

Extract-Amplify-Measure: Single-Sided and Tight O2H with Applications to CCA Security in the Quantum Random Oracle Model

Jiangxia Ge¹, Kang Yang², and Yu Yu^{3,4}

¹ China Telecom Quantum Information Technology Group Co., Ltd., Hefei, China
gejiangxia@chinatelecom.cn

² State Key Laboratory of Cryptology, Beijing, China
yangk@sklc.org

³ Shanghai Jiao Tong University, Shanghai, China

⁴ Shanghai Qi Zhi Institute, Shanghai, China
yuyu@yuyu.hk

Abstract. The One-Way-to-Hiding (O2H) theorem is a useful tool for analyzing reprogramming in the quantum random oracle model (QROM). It bounds the distinguishing advantage by the probability ϵ that a one-wayness attacker finds the reprogrammed point. A sequence of works has improved the tightness of this theorem. Currently, the Measure-Rewind-Extract O2H (MRE-O2H) theorem proved by Ge et al. (ASIACRYPT 2024) achieves the tightest known upper bound of $O(\sqrt{q} \cdot \epsilon)$, where q is the number of quantum queries. This theorem follows the Double-Sided idea introduced by Bindel et al. (TCC 2019), which requires the one-wayness attacker to access both the original and reprogrammed random oracles, thereby imposing stronger requirements on the reduction. Moreover, it incurs a q -dependent loss of $O(\sqrt{q})$.

In this paper, we address these limitations by proving two Extract-Amplify-Measure (EAM) O2H theorems. First, we prove a Single-Sided EAM-O2H (SSEAM-O2H) theorem, which achieves the same $O(\sqrt{q} \cdot \epsilon)$ upper bound as the MRE-O2H theorem, while the resulting attacker only needs access to either the original or the reprogrammed random oracle, reducing the requirements on the underlying reduction. Second, we prove a Double-Sided EAM-O2H (DSEAM-O2H) theorem, which retains the Double-Sided idea used in the MRE-O2H theorem but removes the q -dependent loss, yielding a tight $O(\epsilon)$ upper bound.

As applications, we revisit the security of several Fujisaki–Okamoto variants proposed by Hofheinz et al. (TCC 2017) in the QROM, namely $U^\perp$, $FO^\perp$, $FO_m^\perp$, $FO^\perp$, and $FO_m^\perp$, and obtain the following results:

- The IND-CCA security of $U^\perp$ can be reduced to the OW-CPA security of the underlying PKE scheme. Compared with the previous proofs by Bindel et al. (TCC 2019) and Kuchta et al. (EUROCRYPT 2020), we avoid both the square-root loss and the q -dependent loss in the underlying adversary’s OW-CPA advantage.
- The IND-CCA security of $FO^\perp$, $FO_m^\perp$, $FO^\perp$, and $FO_m^\perp$ can be reduced to the IND-CPA security of the underlying PKE scheme. Compared with the previous proofs by Ge et al. (ASIACRYPT 2024), we reduce the q -dependent loss from $O(q^{1.5})$ to $O(q^{0.5})$.

- Assuming unique randomness recoverability, the IND-CCA security of $\text{FO}^\perp$, $\text{FO}_m^\perp$, $\text{FO}^\perp$, and $\text{FO}_m^\perp$ can be reduced to the OW-CPA security of the underlying PKE scheme. Compared with the previous proofs by Ge et al. (ASIACRYPT 2024), we avoid the q -dependent loss in the underlying adversary’s OW-CPA advantage.

Keywords: quantum random oracle model · security proof · Fujisaki-Okamoto transformation · key encapsulation mechanism.

1 Introduction

The Fujisaki–Okamoto (FO) transformation [12] is a generic tool for upgrading a public key encryption (PKE) scheme to achieve indistinguishability under chosen-ciphertext attacks (IND-CCA) in the random oracle model (ROM) [3]. The underlying PKE scheme only needs to satisfy a weaker security notion, such as indistinguishability under chosen-plaintext attacks (IND-CPA) or one-wayness under chosen-plaintext attacks (OW-CPA). Rather than directly constructing an IND-CCA-secure PKE scheme, a common and often more efficient way is to first build an IND-CCA-secure key encapsulation mechanism (KEM) and then obtain an IND-CCA-secure PKE scheme via the KEM-DEM paradigm [8]. Dent [9] proposed the first KEM variant of FO and showed how to construct IND-CCA-secure KEM schemes in the ROM. Later, Hofheinz et al. [16] proposed some KEM variants of FO, including $\text{U}^\perp$, $\text{FO}^\perp$, $\text{FO}_m^\perp$, $\text{FO}^\perp$, and $\text{FO}_m^\perp$, and proved their IND-CCA security in the ROM⁵. These variants are also called the FO-like transformations.

The FO-like transformations have been widely adopted in the NIST post-quantum cryptography standardisation process [24]. In the post-quantum setting, Boneh et al. [5] suggested lifting the ROM to the quantum random oracle model (QROM). Hence, the QROM security of FO-like transformations has become an important research topic. To date, a series of works [26, 18, 19, 4, 21, 17, 13] have proved the IND-CCA security of FO-like transformations in the QROM, where an important tool is the One-Way to Hiding (O2H) theorem and its variants. The original O2H theorem was introduced by Unruh [27] and then restated by Ambainis et al. [1]. Its statement can be informally described as follows.

- **Original O2H theorem.** There are two functions $G, H : X (= \{0, 1\}^m) \rightarrow Y$ and a subset $S \subseteq X$ such that $G(x) = H(x)$ for all $x \notin S$. Thus, G and H differ only on S . There is also a q -query quantum distinguisher $\mathcal{A}$ with the distinguishing advantage $\text{Adv}(\mathcal{A}) := |\Pr[1 \leftarrow \mathcal{A}^H] - \Pr[1 \leftarrow \mathcal{A}^G]|$. The O2H theorem states that $\text{Adv}(\mathcal{A}) \leq 2q \cdot \sqrt{\text{Adv}(\mathcal{B}_{\text{ow}})}$, where $\mathcal{B}_{\text{ow}}$ is a one-wayness attacker that has quantum oracle access to G or H , and $\text{Adv}(\mathcal{B}_{\text{ow}})$ denotes its probability of finding an element in S .

⁵ The notation $\perp$ denotes implicit rejection, whereas $\perp$ denotes explicit rejection. In the former case, decapsulation of an invalid ciphertext returns a pseudorandom value, while in the latter case it returns the failure symbol $\perp$.

For the O2H variants used in [26,18,19,4,21,17,13], we briefly review four representative variants below. By introducing additional constraints, these variants achieve tighter bounds than the original O2H bound $2q \cdot \sqrt{\text{Adv}(\mathcal{B}_{\text{ow}})}$.

- **Semi-Classical O2H (SC-O2H) theorem.** This variant is proved by Ambainis et al. [1]. By allowing $\mathcal{B}_{\text{ow}}$ to access $G \setminus S$, which is an oracle that first queries the semi-classical oracle $\mathcal{O}_S^{SC}$ and then G , this variant proves that $\text{Adv}(\mathcal{A}) \leq 2\sqrt{q+1} \cdot \sqrt{\text{Adv}(\mathcal{B}_{\text{ow}})}$. Intuitively, the introduction of $\mathcal{O}_S^{SC}$ enables $\mathcal{B}_{\text{ow}}$ to determine whether x belongs to S , thereby improving its ability to find an element in S .
- **Double-Sided O2H (DS-O2H) theorem.** This variant is proved by Bindel et al. [4]. By allowing $\mathcal{B}_{\text{ow}}$ to query G and H and assuming $|S| = 1$, this variant proves that $\text{Adv}(\mathcal{A}) \leq 2 \cdot \sqrt{\text{Adv}(\mathcal{B}_{\text{ow}})}$. The "Double-Sided" idea of Bindel et al., namely allowing $\mathcal{B}_{\text{ow}}$ to query both the original and reprogrammed random oracles and thereby improving its ability to find an element in S , is inspired by Zhandry's compressed oracle technique [29].
- **Measure-Rewind-Measure O2H (MRM-O2H) theorem.** This variant is proved by Kuchta et al. [21]. It follows the Double-Sided idea and uses quantum rewinding to improve $\mathcal{B}_{\text{ow}}$'s ability to find an element in S , achieving a bound $\text{Adv}(\mathcal{A}) \leq 4q \cdot \text{Adv}(\mathcal{B}_{\text{ow}})$ without the square-root advantage loss. Here, quantum rewinding means that, roughly speaking, if $\mathcal{A}$ performs the unitary operation U , then $\mathcal{B}_{\text{ow}}$ performs its inverse $U^\dagger$ at some point.
- **Measure-Rewind-Extract O2H (MRE-O2H) theorem.** This variant is proved by Ge et al. [13]. It can be viewed as a variant of MRM-O2H, which tightens the bound to $\text{Adv}(\mathcal{A}) \leq 4\sqrt{q} \cdot \text{Adv}(\mathcal{B}_{\text{ow}})$. This variant also follows the Double-Sided idea and allows $\mathcal{B}_{\text{ow}}$ to rewind $\mathcal{A}$. In addition, it enables $\mathcal{B}_{\text{ow}}$ to query the indicator function 1_S of the set S , where $1_S(x) = 1$ if $x \in S$ and 0 otherwise, further improving $\mathcal{B}_{\text{ow}}$'s ability to find an element in S .

The above four O2H variants improve the original O2H bound in different ways, and MRM-O2H and MRE-O2H theorems further eliminate the square-root advantage loss. Moreover, SC-O2H, MRM-O2H, and MRE-O2H theorems support quantum parallel queries, where the term q in their bounds can be replaced by the query depth d , which provides an additional improvement⁶.

When assessing the post-quantum security of FO-like transformations, tighter security proofs in the QROM are highly desirable, as the tightness determines the flexibility of parameter selection and the strength of the resulting security guarantee. In fact, the goal of the long line of work [26,18,19,4,21,17,13] on tighter O2H variants is to obtain tighter IND-CCA security proofs for FO-like transformations in the QROM. However, the currently tightest MRE-O2H theorem still follows the Double-Sided idea and introduces a loss factor of $4\sqrt{q}$ depending on the number of quantum queries. The former requires the reduction algorithm to simulate both the original and reprogrammed random oracles, which may limit its applicability in settings where the two oracles are difficult to simulate simul-

⁶ For the sake of simplicity, we do not consider quantum parallel queries in this paper.

taneously⁷. Moreover, the latter introduces an additional $4\sqrt{q}$ security loss in the resulting security proof. Hence, a natural question arises:

Can we prove a new O2H theorem that goes beyond the Double-Sided idea or eliminates the q -dependent loss?

1.1 Our Contributions

We address the above question by developing a new Extract-Amplify-Measure (EAM) technique based on amplitude amplification [6] and using it to prove two O2H theorems as follows:

Single-Sided Extract-Amplify-Measure O2H (SSEAM-O2H),
Double-Sided Extract-Amplify-Measure O2H (DSEAM-O2H).

The SSEAM-O2H theorem has the same asymptotic bound as the MRE-O2H theorem, while the resulting one-wayness attacker $\mathcal{B}_{\text{ow}}$ only needs access to either the original or the reprogrammed random oracle, rather than both. Therefore, it provides broader applicability than the MRE-O2H theorem. The DSEAM-O2H theorem retains the Double-Sided idea used in the MRE-O2H theorem, but has a tight upper bound $22 \cdot \text{Adv}(\mathcal{B}_{\text{ow}})$, thereby completely removing the q -dependent loss. In the following Table 1, we also compare our SSEAM-O2H theorem and DSEAM-O2H theorem with previous O2H theorems.

Table 1: Comparison of O2H theorems. The " $\mathcal{B}_{\text{ow}}$ accesses" column shows the oracles quantum accessible to $\mathcal{B}_{\text{ow}}$. The 1_S refers to the indicator function of S , that is, $1_S(x) = 1$ if $x \in S$ and 0 otherwise. The "Running time" column gives the relationship between the running time $\mathcal{T}_{\mathcal{B}_{\text{ow}}}$ of $\mathcal{B}_{\text{ow}}$ and the running time $\mathcal{T}_{\mathcal{A}}$ of $\mathcal{A}$. The $\mathcal{T}_{\mathcal{B}_{\text{ow}}}^{\text{exp}}$ denotes the expected running time of $\mathcal{B}_{\text{ow}}$.

O2H theorem	Bound ($\text{Adv}(\mathcal{A}) \leq$)	$ S $	$\mathcal{B}_{\text{ow}}$ accesses	Running time
SC-O2H [1]	$2\sqrt{q+1} \cdot \sqrt{\text{Adv}(\mathcal{B}_{\text{ow}})}$	Any	$G \setminus S$ or $H \setminus S$	$\mathcal{T}_{\mathcal{B}_{\text{ow}}} \approx \mathcal{T}_{\mathcal{A}}$
DS-O2H [4]	$2 \cdot \sqrt{\text{Adv}(\mathcal{B}_{\text{ow}})}$	One	G and H	$\mathcal{T}_{\mathcal{B}_{\text{ow}}} \approx \mathcal{T}_{\mathcal{A}}$
MRM-O2H [21]	$4q \cdot \text{Adv}(\mathcal{B}_{\text{ow}})$	Any	G and H	$\mathcal{T}_{\mathcal{B}_{\text{ow}}} \lesssim 3 \cdot \mathcal{T}_{\mathcal{A}}$
MRE-O2H [13]	$4\sqrt{q} \cdot \text{Adv}(\mathcal{B}_{\text{ow}})$	Any	G , H and 1_S	$\mathcal{T}_{\mathcal{B}_{\text{ow}}} \lesssim 3 \cdot \mathcal{T}_{\mathcal{A}}$
SSEAM-O2H Thm. 2	$22\sqrt{q+1} \cdot \text{Adv}(\mathcal{B}_{\text{ow}})$	Any	$(G \text{ or } H)$ and 1_S	$\mathcal{T}_{\mathcal{B}_{\text{ow}}}^{\text{exp}} \lesssim (2m+5) \cdot \mathcal{T}_{\mathcal{A}}^a$
DSEAM-O2H Thm. 4	$22 \cdot \text{Adv}(\mathcal{B}_{\text{ow}})$	One	G and H	$\mathcal{T}_{\mathcal{B}_{\text{ow}}}^{\text{exp}} \lesssim (2m+5) \cdot \mathcal{T}_{\mathcal{A}}^a$

^a Recall that $S \subseteq X (= \{0, 1\}^m)$. Hence, m is the bit length of the element in S and X .

⁷ For example, in proving the OW-CPA security of the transformation T [16], the value $H(m^*)$ is embedded in the challenge ciphertext $c^* = \text{Enc}_{pk}(m^*; H(m^*))$. In this case, a reduction algorithm receiving (pk, c^*) can directly simulate the reprogrammed version of H , where $H(m^*)$ is replaced by a fresh random value. However, the reduction algorithm may be unable to perfectly simulate the original random oracle H , since it generally cannot recover $H(m^*)$ from c^* .

Trade-off of our O2H. Although our O2H theorems improve applicability and tightness compared with previous results, they have two trade-offs in the running time of $\mathcal{B}_{\text{ow}}$. We believe these trade-offs are acceptable, as analyzed below.

1. Previous O2H provide a running time bound for $\mathcal{B}_{\text{ow}}$ that is at most $3 \cdot \mathcal{T}_{\mathcal{A}}$. In contrast, our O2H introduces a factor of $2m + 5$, where m is the bit length of the elements in X . Nevertheless, we believe that this is an acceptable trade-off because, in practice, at least for the FO-like transformations considered in this paper, $X = \{0, 1\}^m$ is the message space of underlying PKE schemes, where m is usually fixed to 256. Hence, although $2m + 5 = 517$ is still much larger than 3, it only introduces a constant-factor overhead in $\mathcal{T}_{\mathcal{A}}$.
2. Unlike previous O2H, where the running time of $\mathcal{B}_{\text{ow}}$ is actually bounded in the worst case, we only give an expected running time bound for $\mathcal{B}_{\text{ow}}$. In fact, our $\mathcal{B}_{\text{ow}}$ needs to repeatedly run $\mathcal{A}$ for k times, where k may take exponential values with some probability. Hence, even if $\mathcal{A}$ runs in strict poly-time, the worst case running time of our $\mathcal{B}_{\text{ow}}$ may still be exponential. Fortunately, since the expectation of k can be bounded by $m + 2$, our $\mathcal{B}_{\text{ow}}$ runs in expected poly-time with bound $(2m + 5) \cdot \mathcal{T}_{\mathcal{A}}$. We believe this is an acceptable trade-off. First, expected poly-time QROM security proofs have already appeared in the literature, such as the expected poly-time acHVZK simulator in the EUF-CMA security proof of Dilithium [2]. In addition, assuming $\text{Adv}(\mathcal{A})$ is non-negligible, we can apply the cutoff argument [20, Lemma 1.2] to convert $\mathcal{B}_{\text{ow}}$ into a strict poly-time attacker while preserving the relationship between $\text{Adv}(\mathcal{A})$ and $\text{Adv}(\mathcal{B}_{\text{ow}})$ up to a constant factor. Thus, if $\mathcal{A}$ can distinguish G and H with a non-negligible advantage, we can then design $\mathcal{B}_{\text{ow}}$ to find an element in S in strict poly-time and achieve a similar advantage. So our O2H theorems preserve the essential reduction functionality of O2H theorems.

Moreover, similar to the DS-O2H theorem, our DSEAM-O2H theorem requires $|S| = 1$. Nevertheless, following [4], this restriction can be relaxed by introducing a function f , where S is allowed to contain multiple elements as long as the set $\{f(x) : x \in S\}$ that $\mathcal{B}_{\text{ow}}$ actually guesses still contains only one element.

By using our O2H theorems, we give tighter IND-CCA security proofs for the FO-like transformations $\text{U}^\perp$, $\text{FO}^\perp$, $\text{FO}_m^\perp$, $\text{FO}^\perp$, and $\text{FO}_m^\perp$ in the QROM, and the security bounds are shown in Table 2. For $\text{U}^\perp$, under the η -injective assumption, we give a tight IND-CCA security proof. Moreover, without assuming η -injective, we still prove the IND-CCA security of $\text{U}^\perp$, while avoiding both the square-root loss and the q -dependent loss in ϵ . This comes with a trade-off: replacing the FFC game used in [4, 21] with the COR game defined in [16] and introducing a $\sqrt{q}$ loss⁸. For $\text{FO}^\perp$, $\text{FO}_m^\perp$, $\text{FO}^\perp$, and $\text{FO}_m^\perp$, compared with [13], our bounds reduce the q -dependent loss in ϵ by a factor of $q + q_D$, $(q + q_D)^{0.5}$, q , or $q^{0.5}$.

⁸ Note that the third-round finalist NTRU [25] uses $\text{U}^\perp$ (called SXY in their specification) and has zero decryption error, implying that the corresponding COR advantage δ_{COR} is also zero. Hence, our Theorem 6 in fact gives a tight IND-CCA proof for NTRU based on the standard OW-CPA security. This is also non-trivial, since previous tight IND-CCA proofs for NTRU relied on the non-standard DS-IND security [26].

Table 2: Security bounds in the QROM. Here q is the total number of queries to random oracles and q_D is the total number of queries to the decapsulation oracle. δ and ϵ denote the decryption error and security bound of the underlying PKE scheme. δ_{FFC} and δ_{COR} denote the advantages in the FFC and COR games. Here we abbreviate unique randomness recoverable as URR for simplicity.

Transformation	Underlying security	Assumption	Achieved security	Security bound
$U^\perp$ [4]	OW-CPA	η -injective	IND-CCA	$\sqrt{\epsilon} + \delta_{\text{FFC}} + \eta$
$U^\perp$ [21]	OW-CPA	η -injective	IND-CCA	$q \cdot \epsilon + \delta_{\text{FFC}} + \eta$
$U^\perp$ Thm. 5	OW-CPA	η -injective	IND-CCA	$\epsilon + \delta_{\text{FFC}} + \eta$
$U^\perp$ Thm. 6	OW-CPA	$\backslash$	IND-CCA	$\epsilon + \sqrt{q} \cdot \delta_{\text{COR}}$
$\text{FO}^\perp, \text{FO}_m^\perp$ [13]	IND-CPA	γ -spread	IND-CCA	$(q + q_D)^{1.5} \cdot \epsilon + q \cdot \sqrt{\delta} + q_D \cdot \sqrt{2^{-\gamma}}$
$\text{FO}^\perp, \text{FO}_m^\perp$ Thm. 9	IND-CPA	γ -spread	IND-CCA	$(q + q_D)^{0.5} \cdot \epsilon + q \cdot \sqrt{\delta} + q_D \cdot \sqrt{2^{-\gamma}}$
$\text{FO}^\perp, \text{FO}_m^\perp$ [13]	OW-CPA	URR	IND-CCA	$(q + q_D)^{0.5} \cdot \epsilon + q \cdot \sqrt{\delta}$
$\text{FO}^\perp, \text{FO}_m^\perp$ Thm. 10	OW-CPA	URR	IND-CCA	$\epsilon + q \cdot \sqrt{\delta}$
$\text{FO}^\perp, \text{FO}_m^\perp$ [13]	IND-CPA	$\backslash$	IND-CCA	$q^{1.5} \cdot \epsilon + q^2 \cdot \delta$
$\text{FO}^\perp, \text{FO}_m^\perp$ Thm. 17	IND-CPA	$\backslash$	IND-CCA	$q^{0.5} \cdot \epsilon + q^2 \cdot \delta$
$\text{FO}^\perp, \text{FO}_m^\perp$ [13]	OW-CPA	URR	IND-CCA	$q^{0.5} \cdot \epsilon + q^2 \cdot \delta$
$\text{FO}^\perp, \text{FO}_m^\perp$ Thm. 18	OW-CPA	URR	IND-CCA	$\epsilon + q^2 \cdot \delta$

1.2 Technique Overview

In this section, for clarity, we explain our techniques in the following two steps:

- We first explain how to prove the SSEAM-O2H and DSEAM-O2H theorems. Roughly speaking, the proof first extracts a queried input into an auxiliary register if it is in S , then uses amplitude amplification [6] to amplify the successful-extraction component, and finally measures the auxiliary register to obtain an element in S . This Extract-Amplify-Measure (EAM) technique allows us to design a one-wayness attacker with a higher success probability, thereby yielding tighter bounds.
- Next, we explain how to use our new O2H theorems to give tighter IND-CCA security proofs of $U^\perp$, $\text{FO}^\perp$, $\text{FO}_m^\perp$, $\text{FO}^\perp$, and $\text{FO}_m^\perp$ in the QROM.

Recall that $G, H : X(= \{0, 1\}^m) \rightarrow Y$ are functions such that $G(x) = H(x)$ for all $x \notin S$. For simplicity, we set $S = \{m^*\}$. That is, there is only one point where G and H may differ. We also consider the following simple distinguisher $\mathcal{A}$:

$$\mathcal{A}^G : \mathbb{M}_{\mathcal{A}} \circ U_2 O_G U_1 O_G |\psi\rangle, \mathcal{A}^H : \mathbb{M}_{\mathcal{A}} \circ U_2 O_H U_1 O_H |\psi\rangle, (|\psi\rangle := U_0 |0^a\rangle).$$

Specifically, $\mathcal{A}$ works on a quantum register with a qubits and first performs the unitary operation U_0 on $|0^a\rangle$ to prepare its initial state $|\psi\rangle$. U_1 and U_2 are the

unitary operations performed by $\mathcal{A}$ between its oracle queries O_G/O_H , where $O_G|x, y\rangle = |x, y \oplus G(x)\rangle$ and $O_H|x, y\rangle = |x, y \oplus H(x)\rangle$. $\mathbb{M}_{\mathcal{A}}$ is a binary projective measurement and its outcome is the final output of $\mathcal{A}$.

How to prove SSEAM-O2H theorem. Define $q := 2$ to represent the number of queries made by $\mathcal{A}$. The first step of this proof is to invoke [1, Theorem 1], which introduces the semi-classical oracle $\mathcal{O}_S^{SC}$ (Definition 1) and ensures that

$$|\Pr[1 \leftarrow \mathcal{A}^G] - \Pr[1 \leftarrow \mathcal{A}^H]| \leq 2\sqrt{q+1} \cdot \sqrt{\Pr[\text{Find} : \mathcal{A}^{G \setminus S}]}. \quad (1)$$

Here $G \setminus S$ is an oracle that first queries $\mathcal{O}_S^{SC}$ on the input of G and then queries G . Find is the event that $\mathcal{O}_S^{SC}$ ever has outcome 1.

Note that $\mathcal{O}_S^{SC}$ can be simulated by querying 1_S , where $1_S(x) = 1$ if $x \in S$ and 0 otherwise. Moreover, roughly speaking, if a query to $\mathcal{O}_S^{SC}$ has outcome 1, then the state of its input register is a superposition of elements in S . Hence, $\Pr[\text{Find} : \mathcal{A}^{G \setminus S}]$ naturally corresponds to the success probability of the following one-wayness attacker $\mathcal{B}$: it runs $\mathcal{A}^{G \setminus S}$ by querying G and 1_S , and once a simulation of $\mathcal{O}_S^{SC}$ has outcome 1 (i.e., Find occurs), it stops and measures the input register to obtain an element in S . Here, to facilitate the analysis of probability differences, we design a purified version of $\mathcal{B}$ with additional record registers as:

- $\mathcal{B}^{G, 1_S}$ has auxiliary register BT and initial state $|0^a\rangle|0, 0^m\rangle_{\text{BT}}$. It performs $U_2 O_G U_S^2 U_1 O_G U_S^1 U_0$, then measures BT in the computational basis to obtain (b, t) , and finally outputs t if $b \neq 0$ and outputs $\perp$ otherwise.

The unitary operations U_S^i ($i \in \{1, 2\}$) used by $\mathcal{B}$ are defined as follows and can also be implemented by querying 1_S .

$$U_S^i|x, y\rangle|b, t\rangle_{\text{BT}} := \begin{cases} |x, y\rangle|i, t \oplus x\rangle_{\text{BT}} & x \in S \text{ and } b = 0, \\ |x, y\rangle|0, t \oplus x\rangle_{\text{BT}} & x \in S \text{ and } b = i, \\ |x, y\rangle|b, t\rangle_{\text{BT}} & \text{otherwise.} \end{cases}$$

Compared with $\mathcal{A}$, $\mathcal{B}$ additionally applies U_S^i before the i -th G query ($i \in \{1, 2\}$). Intuitively, U_S^i serves three purposes. First, it records in T the inputs in S queried by $\mathcal{A}$ to G . Second, it records in B the index of the first G query that records the element $x \in S$ in T. Third, if some U_S^j with $j < i$ has already recorded (j, x) in BT, then U_S^i does not make any record in BT again.

Indeed, $\Pr[\text{Find} : \mathcal{A}^{G \setminus S}]$ equals the probability that $\mathcal{B}$ outputs some $t \in S$. This is because Find can be decomposed into two mutually exclusive events: either Find occurs in the first $G \setminus S$ query, or it first occurs in the second one⁹, and these two events correspond respectively to the records $(1, t_1 \in S)$ and $(2, t_2 \in S)$ in the BT register. More precisely, $(1, t_1 \in S)$ means that an element in S is recorded at the first query, whereas $(2, t_2 \in S)$ means that such an element is first recorded at the second query. Hence, $\mathcal{B}$ essentially transforms Find into

⁹ Recall that the distinguisher $\mathcal{A}$ considered here makes only two oracle queries.

the event that measuring the BT registers yields (b, t) satisfying $b \neq 0$ and $t \in S$. Thus, by Eq. (1), we have

$$|\Pr[1 \leftarrow \mathcal{A}^G] - \Pr[1 \leftarrow \mathcal{A}^H]| \leq 2\sqrt{q+1} \cdot \sqrt{\Pr[t \in S : t \leftarrow \mathcal{B}^{G,1_S}]} \quad (2)$$

In addition, an important observation of $\mathcal{B}$ is that the final state of $\mathcal{B}$ before measurement can be decomposed into two orthogonal components according to whether the B register is in state $|0\rangle$. Specifically, define the projectors $\Pi_S := \sum_{x \in S} |x\rangle\langle x| = |m^*\rangle\langle m^*|$ (recall that $S = \{m^*\}$ in our simple case) and $\Pi_\perp := I - \Pi_S$. Then, the final state of $\mathcal{B}$ before measurement can be written as

$$\begin{aligned} |\psi_{\text{final}}\rangle &= \underbrace{U_2 O_G \Pi_\perp U_1 O_G \Pi_\perp |\psi\rangle \otimes |0, 0^m\rangle_{\text{BT}}}_{:= |\psi_{\text{bad}}\rangle} + \\ &\quad \underbrace{U_2 O_G U_1 O_G \Pi_S |\psi\rangle \otimes |1, m^*\rangle_{\text{BT}} + U_2 O_G \Pi_S U_1 O_G \Pi_\perp |\psi\rangle \otimes |2, m^*\rangle_{\text{BT}}}_{:= |\psi_{\text{good}}\rangle} \\ &= |\psi_{\text{bad}}\rangle + |\psi_{\text{good}}\rangle. \end{aligned}$$

Now, we have $\|\psi_{\text{good}}\| = \sqrt{\Pr[t \in S : t \leftarrow \mathcal{B}^{G,1_S}]}$, since by the definition of $\mathcal{B}$, the probability $\Pr[t \in S : t \leftarrow \mathcal{B}^{G,1_S}]$ is exactly $\|\psi_{\text{good}}\|^2$.

The above analysis shows that $\mathcal{B}$ is well suited for applying amplitude amplification [6]: its initial state $|0^a\rangle|0, 0^m\rangle_{\text{BT}}$ is the all-zero state, its success probability is determined by the norm of the state $|\psi_{\text{good}}\rangle$, and $|\psi_{\text{bad}}\rangle$ and $|\psi_{\text{good}}\rangle$ can be distinguished according to whether the B register is in state $|0\rangle$. In fact, by defining $U_B := U_2 O_G U_S^2 U_1 O_G U_S^1 U_0$, Lemma 1 of [6] and the analysis in Eqs. (2)–(8) of the same paper show that the following operation Am can be used to amplify the success probability of $\mathcal{B}^{10}$.

$$Am := U_B \circ (2|0^a\rangle\langle 0^a|_{\text{BT}} - I) \circ U_B^\dagger \circ (2|0\rangle\langle 0|_{\text{B}} - I_{\text{B}}).$$

Since O_G and U_S^i ($i \in \{1, 2\}$) are Hermitian, we have $U_B^\dagger = U_0^\dagger U_S^1 O_G U_1^\dagger U_S^2 O_G U_2^\dagger$. We stress that we do not need to amplify $\Pr[t \in S : t \leftarrow \mathcal{B}^{G,1_S}]$ to a value close to 1; it suffices to amplify it to around $\sqrt{\Pr[t \in S : t \leftarrow \mathcal{B}^{G,1_S}]}$. In other words, based on $\mathcal{B}$ and Am , we aim to design a new one-wayness attacker $\mathcal{B}_{\text{ow}}$ such that

$$\sqrt{\Pr[t \in S : t \leftarrow \mathcal{B}^{G,1_S}]} \leq c \cdot \Pr[t \in S : t \leftarrow \mathcal{B}_{\text{ow}}^{G,1_S}] \quad (3)$$

for some suitable constant c , e.g., $c = 10$. At this point, combining Eq. (3) with Eq. (2), we obtain

$$|\Pr[1 \leftarrow \mathcal{A}^G] - \Pr[1 \leftarrow \mathcal{A}^H]| \leq 2c\sqrt{q+1} \cdot \Pr[t \in S : t \leftarrow \mathcal{B}_{\text{ow}}^{G,1_S}].$$

The above is the core inequality of our SSEAM-O2H theorem, bounding the distinguishing advantage of $\mathcal{A}$ in terms of the success probability of $\mathcal{B}_{\text{ow}}$. Although the above analysis assumes that $\mathcal{B}_{\text{ow}}$ queries G and 1_S , the same argument applies directly when it queries H and 1_S , since the starting point Eq. (1) is actually single-sided and remains valid with $G \setminus S$ replaced by $H \setminus S$.

¹⁰ For completeness, we provide a proof of this claim in the main body (Lemma 1).

Table 3: The distribution $\mathfrak{D}$. Here $T := \sum_{i=0}^m 1/2^i$.

k	2^0	2^1	2^2	$\dots$	2^m
probability	$\frac{1}{T \cdot 2^0}$	$\frac{1}{T \cdot 2^1}$	$\frac{1}{T \cdot 2^2}$	$\dots$	$\frac{1}{T \cdot 2^m}$

Notice that in the previous paragraph, we only described the desired effect of $\mathcal{B}_{\text{ow}}$ without giving its concrete construction. We now provide the construction.

- $\mathcal{B}_{\text{ow}}^{G,1s}$ has auxiliary register BT and initial state $|0^a\rangle|0, 0^m\rangle_{\text{BT}}$. It first samples k according to the distribution $\mathfrak{D}$ defined in Table 3, then performs $(Am)^k U_{\mathcal{B}}$ and measures BT in the computational basis to get (b, t) . $\mathcal{B}_{\text{ow}}^{G,1s}$ outputs t if $b \neq 0$ and outputs $\perp$ otherwise.

The construction of $\mathcal{B}_{\text{ow}}$ is the same as that of $\mathcal{B}$, except that it additionally performs k iterations of Am before the final measurement. Thus, the key is how to choose k . A larger k generally gives stronger amplification but also increases the running time. As mentioned before, our goal is not to amplify the success probability of $\mathcal{B}$ to a value close to 1, but only to around $\sqrt{\Pr[t \in S : t \leftarrow \mathcal{B}^{G,1s}]}$. Hence, we simplify the amplification-iteration distribution used in [6, Theorem 3] to the distribution defined in Table 3. We prove that this distribution is sufficient to achieve our desired amplification effect, and its expectation is at most $m + 2$, where m is the bit length of the elements in S and X . So our theorem introduces a certain trade-off in running time. Nevertheless, as explained in Section 1.1, we believe that this trade-off is acceptable.

Remark 1. We intuitively explain why the distribution $\mathfrak{D}$ in Table 3 achieves the desired amplification effect. Let $|\psi_{\text{good}}^k\rangle$ denote the good component after k amplification iterations. To derive Eq. (3) based on $\mathfrak{D}$, it suffices to prove that, for some suitable constant c , $\|\psi_{\text{good}}\| \leq c \cdot \sum_{i=0}^m (T \cdot 2^i)^{-1} \|\psi_{\text{good}}^{2^i}\|^2$. We consider three cases. When $\|\psi_{\text{good}}\|$ is relatively large, $\|\psi_{\text{good}}^1\|^2$ and $\|\psi_{\text{good}}^2\|^2$ are also relatively large. Hence, for a suitable constant c , the first two terms of the sum already suffice to upper bound $\|\psi_{\text{good}}\|$. When $\|\psi_{\text{good}}\|$ is relatively small but there exists some $0 \leq j \leq m$ such that $1/2^j \approx \|\psi_{\text{good}}\|$. For this j , the 2^j amplification iterations makes $\|\psi_{\text{good}}^{2^j}\|^2$ close to 1, while $1/(T \cdot 2^j)$ is within a constant factor of $\|\psi_{\text{good}}\|$ since $1 \leq T \leq 2$. Hence, for some suitable constant c , the term $c \cdot (T \cdot 2^j)^{-1} \|\psi_{\text{good}}^{2^j}\|^2$ alone suffices to upper bound $\|\psi_{\text{good}}\|$. Finally, when $\|\psi_{\text{good}}\|$ is very small such that $\|\psi_{\text{good}}\| < 1/2^m$, we obviously have $\|\psi_{\text{good}}\| \leq c \cdot \sum_{i=0}^m (T \cdot 2^i)^{-1} \|\psi_{\text{good}}^{2^i}\|^2 + 1/2^m$. Thus, this case can be handled by adding a tail term $1/2^m$ to the desired inequality, which is also acceptable since $1/2^m$ is generally negligible. This gives the desired amplification effect.

How to prove DSEAM-O2H theorem. Our proof starts from [4, Lemma 5], which gives a one-wayness attacker $\mathcal{B}$ with access to both G and H satisfying

$$|\Pr[1 \leftarrow \mathcal{A}^G] - \Pr[1 \leftarrow \mathcal{A}^H]| \leq 2 \cdot \sqrt{\Pr[t \in S : t \leftarrow \mathcal{B}^{G,H}]}. \quad (4)$$

The construction of $\mathcal{B}$ follows that of $\mathcal{A}$, except that the oracle queries O_G/O_H are replaced by $RO_{G,H}R$. Here $R : |x, y\rangle|b, t\rangle_{\text{BT}} \mapsto |x, y\rangle|b, t \oplus (b \cdot x)\rangle_{\text{BT}}$ records information in the BT register, and $O_{G,H} := (|+\rangle\langle+|_{\text{B}} \otimes O_H) + (|-\rangle\langle-|_{\text{B}} \otimes O_G)$ performs a coherent query to G and H controlled by B . The concrete construction of $\mathcal{B}$ is given below.

- $\mathcal{B}^{G,H}$ has auxiliary register BT and initial state $|0^a\rangle|0, 0^m\rangle_{\text{BT}}$. It performs $U_2(RO_{G,H}R)U_1(RO_{G,H}R)U_0$, then measures BT in the computational basis to obtain (b, t) , and finally outputs t if $b \neq 0$ and outputs $\perp$ otherwise.

In our simple case where $S = \{m^*\}$, by defining $P := 1/2 \cdot (U_2O_HU_1O_HU_0 + U_2O_GU_1O_GU_0)$ and $Q := 1/2 \cdot (U_2O_HU_1O_HU_0 - U_2O_GU_1O_GU_0)$, [4, Lemma 5] gives the following final state of $\mathcal{B}$ before measurement:

$$|\psi_{\text{final}}\rangle = P|0^a\rangle \otimes |0, 0^m\rangle_{\text{BT}} + Q|0^a\rangle \otimes |1, m^*\rangle_{\text{BT}}.$$

We can observe that, unlike the proof of the SSEAM-O2H theorem discussed earlier, where we need to construct a one-wayness attacker suitable for amplitude amplification, the attacker $\mathcal{B}$ constructed in [4] already has the desired structure. Specifically, its initial state $|0^a\rangle|0, 0^m\rangle_{\text{BT}}$ is the all-zero state, its success probability is determined by the norm of $Q|0^a\rangle \otimes |1, m^*\rangle_{\text{BT}}$, and $P|0^a\rangle \otimes |0, 0^m\rangle_{\text{BT}}$ and $Q|0^a\rangle \otimes |1, m^*\rangle_{\text{BT}}$ can be distinguished according to whether the B register is in state $|0\rangle$. Hence, applying the same amplitude amplification technique as in our SSEAM-O2H proof, we can construct a new one-wayness attacker $\mathcal{B}_{\text{ow}}$ satisfying

$$\sqrt{\Pr[t \in S : t \leftarrow \mathcal{B}^{G,H}]} \leq c \cdot \Pr[t \in S : t \leftarrow \mathcal{B}_{\text{ow}}^{G,H}] \quad (5)$$

for some suitable constant c . Define $U_{\text{B}} := U_2(RO_{G,H}R)U_1(RO_{G,H}R)U_0$. Then, the amplification operation used by $\mathcal{B}_{\text{ow}}$ is

$$Am := U_{\text{B}} \circ (2|0^a\rangle|0, 0^m\rangle_{\text{BT}}\langle 0^a| \langle 0, 0^m|_{\text{BT}} - I) \circ U_{\text{B}}^\dagger \circ (2|0\rangle\langle 0|_{\text{B}} - I_{\text{B}}).$$

Since R and $O_{G,H}$ are both Hermitian, $U_{\text{B}}^\dagger$ equals $U_0^\dagger(RO_{G,H}R)U_1^\dagger(RO_{G,H}R)U_2^\dagger$. Next, the concrete construction of $\mathcal{B}_{\text{ow}}$ is as follows.

- $\mathcal{B}_{\text{ow}}^{G,H}$ has auxiliary register BT and initial state $|0^a\rangle|0, 0^m\rangle_{\text{BT}}$. It first samples k according to the distribution $\mathfrak{D}$ defined in Table 3, then performs $(Am)^k U_{\text{B}}$ and measures BT in the computational basis to get (b, t) . $\mathcal{B}_{\text{ow}}^{G,H}$ outputs t if $b \neq 0$ and outputs $\perp$ otherwise.

At this point, by combining Eq. (4) with Eq. (5), we obtain

$$|\Pr[1 \leftarrow \mathcal{A}^G] - \Pr[1 \leftarrow \mathcal{A}^H]| \leq 2c \cdot \Pr[t \in S : t \leftarrow \mathcal{B}_{\text{ow}}^{G,H}].$$

The above is the core inequality of our DSEAM-O2H theorem, bounding the distinguishing advantage of $\mathcal{A}$ in terms of the success probability of $\mathcal{B}_{\text{ow}}$. Note that, as in [4], our $\mathcal{B}_{\text{ow}}$ is double-sided, requiring access to both G and H .

QROM security proofs for $\mathbf{U}^\perp$. Here, we briefly explain how to prove the IND-CCA security of $\mathbf{U}^\perp$ in the QROM. When the underlying PKE scheme is η -injective, we follow the proof of [4, Theorem 2], replacing the DS-O2H theorem used there with our tight DSEAM-O2H theorem. When the underlying PKE scheme is not η -injective, however, the random oracle reprogramming argument of [4, Theorem 2] no longer applies. We therefore give a new proof of the reprogramming step using the COR game [16]. Roughly speaking, to keep the reprogramming of random oracle G undetectable, the previous proof requires the encryption algorithm to be injective and the adversary not to query the decapsulation oracle on an error ciphertext c . Instead, we only require the adversary not to query G on an error (m, c) pair¹¹, thereby avoiding the η -injective assumption. To this end, we use the MRE-O2H theorem [13] to transform the probability of detecting the reprogramming into that of guessing an error (m, c) pair, resulting in an adversary against the COR game at the cost of a $\sqrt{q}$ loss¹². The remaining proof follows [4, Theorem 2], with the DS-O2H theorem replaced by our DSEAM-O2H theorem to obtain a tighter bound.

QROM security proofs for $\mathbf{FO}^\perp$, $\mathbf{FO}_m^\perp$, $\mathbf{FO}^\perp$, and $\mathbf{FO}_m^\perp$. The proofs for these transformations are similar, so we briefly explain the case of $\mathbf{FO}_m^\perp$. The first step is to invoke [14, Theorem 2], which shows that, in the QROM, the IND-CPA security of $\mathbf{FO}_m^\perp$ implies its IND-CCA security. We therefore focus on proving the IND-CPA security of $\mathbf{FO}_m^\perp$ using our SSEAM-O2H theorem. In this proof, we first combine the generation of the randomness $r := H(m)$ and the session key $k := G(m)$ by introducing a single random oracle F with $(r, k) := F(m)$. We then follow the idea of [4, Theorem 1] to reduce the IND-CPA security of this reformulated construction to that of the underlying PKE scheme in two steps:

- First, instead of sampling the challenge plaintext as $m^* \leftarrow_{\$} \mathcal{M}$, where $\mathcal{M}$ is the message space, we equivalently sample $m_0 \leftarrow_{\$} \mathcal{M}$, $m_1 \leftarrow_{\$} \mathcal{M} \setminus \{m_0\}$, $c \leftarrow_{\$} \{0, 1\}$, and set $m^* := m_c$. Then, the reprogramming of F at m^* can be covered by a broader reprogramming: we reprogram F at both m_0 and m_1 , and it suffices to show that the adversary cannot distinguish whether F is reprogrammed on $S := \{m_0, m_1\}$. The reason for this approach is that, when only m^* is reprogrammed, a reduction receiving the challenge ciphertext c^* may be unable to test whether an element equals m^* without additional properties of the underlying PKE scheme. With this broader reprogramming on S , however, the reduction against the IND-CPA security of the underlying PKE scheme can sample m_0 and m_1 itself and hence compute 1_S , allowing us to apply our SSEAM-O2H theorem.

¹¹ Here, an error ciphertext c means that there exists some m such that $\text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) \neq m$, and an error (m, c) pair means that $\text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) \neq m$.

¹² Although our SSEAM-O2H could also be used here, we use MRE-O2H because it has a simpler structure and gives the same asymptotic bound. Note that our DSEAM-O2H cannot be directly applied to remove the $\sqrt{q}$ loss, since the set S in this case does not necessarily satisfy $|S| = 1$.

- As in the proof of [4, Theorem 1], after applying the SSEAM-O2H theorem, it remains to bound a tail probability that the reduction outputs m_{1-c} after receiving $\text{Enc}_{pk}(m_c)$. Since m_0 is sampled uniformly from $\mathcal{M}$ and m_1 uniformly from $\mathcal{M} \setminus \{m_0\}$, for either value of c , conditioned on m_c , the value m_{1-c} is uniformly distributed over $\mathcal{M} \setminus \{m_c\}$ from the reduction's view. Thus, following the proof of [4, Theorem 1], this tail probability should be bounded by $q/(|\mathcal{M}| - 1)$, where q is the number of random oracle queries.

Nevertheless, we stress that the bound $q/(|\mathcal{M}| - 1)$ requires some additional care, since the SSEAM-O2H theorem amplifies the success probability of the one-wayness adversary and may also increase the probability of outputting m_{1-c} . Fortunately, as discussed in the proof overview of the SSEAM-O2H theorem, its amplification is actually bounded: the $\Pr[t \in S : t \leftarrow \mathcal{B}^{G,1s}]$ only needs to be amplified to around $\sqrt{\Pr[t \in S : t \leftarrow \mathcal{B}^{G,1s}]}$. We can hence rigorously show that the amplified tail probability is at most $\sqrt{q}/\sqrt{|\mathcal{M}| - 1}$ ¹³. Next, combining this bound with the $\sqrt{q}$ loss introduced by the SSEAM-O2H theorem yields a final bound of $q/\sqrt{|\mathcal{M}| - 1}$. Although larger than $q/(|\mathcal{M}| - 1)$, this bound remains acceptable, and similar terms commonly appear in existing QROM security proofs for FO-like transformations [18,26,22].

2 Preliminaries

2.1 Notation

By $\llbracket w \rrbracket$ we denote a bit that is 1 if w is true and otherwise 0. For a finite set S , $x \leftarrow_{\S} S$ denotes that x is an element uniformly sampled from set S . For a distribution $\mathfrak{D}$, $x \leftarrow \mathfrak{D}$ denotes that x is chosen according to distribution $\mathfrak{D}$. $\Omega_{X \rightarrow Y}$ refers to the set containing all functions from X to Y . For a game $\mathbf{G}$ in the security proof, $1 \leftarrow \mathbf{G}$ denotes that $\mathbf{G}$ finally returns 1. $\Pr[A : B, C]$ (or $\Pr_C[A : B]$, $\Pr_{B,C}[A]$ for short) is the probability that the predicate A holds where all variables in A are conditioned according to predicates B and C . For an algorithm $\mathcal{A}$, we use $\mathcal{T}_{\mathcal{A}}$ to denote its running time. In particular, we use $\mathcal{T}_{\mathcal{A}}^{\text{exp}}$ to denote the expected running time of $\mathcal{A}$.

2.2 Quantum Background

We refer to [23] for basics of quantum computation. In Supplementary Material B, we introduce several important quantum notions and QROM theorems that are used throughout this paper.

3 Single-Sided Extract-Amplify-Measure O2H

Our Single-Sided Extract-Amplify-Measure (SSEAM) O2H focuses on the tuple (G, H, S, z) . Here G, H are functions with domain $X (= \{0, 1\}^m)$ and codomain

¹³ That is, Lemma 6 used in the proof of Theorem 8.

Y , $z \in Z$ is a random bitstring, $S \subseteq X$, and G, H, S satisfy that $G(x) = H(x)$ for all $x \notin S$. The tuple (G, H, S, z) may have arbitrary joint distribution. During our proof, we will frequently use the following three unitary operations.

$$\begin{aligned} O_G : |x, y\rangle &\mapsto |x, y \oplus G(x)\rangle, \quad O_H : |x, y\rangle \mapsto |x, y \oplus H(x)\rangle, \\ U_S^i |x, y\rangle |b, t\rangle_{\text{BT}} &:= \begin{cases} |x, y\rangle |i, t \oplus x\rangle_{\text{BT}} & x \in S \text{ and } b = 0, \\ |x, y\rangle |0, t \oplus x\rangle_{\text{BT}} & x \in S \text{ and } b = i, \\ |x, y\rangle |b, t\rangle_{\text{BT}} & \text{otherwise.} \end{cases} \end{aligned} \quad (6)$$

Here O_G (resp. O_H) is used to simulate G (resp. H) queries of the adversary. B (resp. T) is the quantum register defined over $\{0, 1, \dots, q\}$ (resp. X), where q is a fixed positive integer. The unitary operation U_S^i ($i \in \{1, \dots, q\}$) updates the register B (resp. T) by recording the flag i (resp. the query x) when $x \in S$, and reverses this update when the operation is applied again. One can directly verify that all the unitary operations defined above are Hermitian, i.e., their Hermitian transpose is exactly themselves.

In the following, we first prove the fixed version of the SSEAM-O2H, where the tuple (G, H, S, z) is fixed. Then, we extend the result to the random version, where the tuple follows an arbitrary joint distribution.

Theorem 1 (Fixed SSEAM-O2H). *Let $G, H : X \rightarrow Y$ be fixed functions and $S \subseteq X (= \{0, 1\}^m)$ be a fixed set. Let $z \in Z$ be a fixed bitstring. The tuple (G, H, S, z) satisfies that $\forall x \notin S, G(x) = H(x)$. Let 1_S denote the indicator function of the set S , that is, $1_S(x) = 1$ if $x \in S$ and 0 otherwise. Let $\mathcal{A}$ be a q -query quantum oracle algorithm. Define*

$$P_{\text{left}}^{GHSz} := \Pr[b = 1 : b \leftarrow \mathcal{A}^H(z)], \quad P_{\text{right}}^{GHSz} := \Pr[b = 1 : b \leftarrow \mathcal{A}^G(z)].$$

Then, we can construct an algorithm $\mathcal{D}^{O, 1_S}(z)$ ($O \in \{G, H\}$), which makes an expected $(2m + 5)q$ queries to O and an expected $(4m + 10)q$ queries to 1_S , has running time $\mathcal{T}_{\mathcal{D}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}}$, and satisfies

$$|P_{\text{left}}^{GHSz} - P_{\text{right}}^{GHSz}| \leq 22\sqrt{q+1} \cdot \text{Adv}(\mathcal{D}). \quad (7)$$

Here $\text{Adv}(\mathcal{D})$ can be $\Pr[x \in S : x \leftarrow \mathcal{D}^{G, 1_S}(z)]$ or $\Pr[x \in S : x \leftarrow \mathcal{D}^{H, 1_S}(z)]$.

Proof. By Fact 1 in Supplementary Material B, any quantum oracle algorithm can be transformed into a unitary one with the same query times. Hence, without loss of generality, we assume $\mathcal{A}^O(z)$ ($O \in \{G, H\}$) to be unitary. Next, we suppose that $\mathcal{A}^O(z)$ operates on an a -qubit register with the initial state $|\psi_z\rangle := U_z|0^a\rangle$, and we denote $U_1, \dots, U_q$ as the unitary operations performed by $\mathcal{A}^O(z)$ between its oracle queries.

We first prove Eq. (7) under $\text{Adv}(\mathcal{D}) = \Pr[x \in S : x \leftarrow \mathcal{D}^{G, 1_S}(z)]$. At this point, we define the probability

$$P_{\text{find}}^{GHSz} := \Pr[\text{Find} : \mathcal{A}^{G \setminus S}(z), (G, H, S, z)]. \quad (8)$$

By using Theorem 11 under the fixed (G, H, S, z) we considered, we have

$$|P_{\text{left}}^{GHSz} - P_{\text{right}}^{GHSz}| \leq 2\sqrt{(q+1) \cdot P_{\text{find}}^{GHSz}}. \quad (9)$$

We then define two projectors as:

$$\Pi_S := \sum_{x \in S} |x\rangle\langle x|, \quad \Pi_{\perp} := I - \Pi_S = \sum_{x \in X \setminus S} |x\rangle\langle x|, \quad (10)$$

where I is the identity operator. For $i \in \{1, \dots, q\}$, let Find_i be the event that, during the execution of $\mathcal{A}^{G \setminus S}(z)$, the measurement outcome of $\mathcal{O}_S^{SC}$ is 1 for the first time at the i -th query. One can check that Find_i for different i are mutually exclusive, and $\text{Find} = \bigvee_{i=1}^q \text{Find}_i$. Thus, we can compute

$$\begin{aligned} P_{\text{find}}^{GHSz} &= \Pr \left[\text{Find} : \mathcal{A}^{G \setminus S}(z), (G, H, S, z) \right] \\ &= \Pr \left[\bigvee_{i=1}^q \text{Find}_i : \mathcal{A}^{G \setminus S}(z), (G, H, S, z) \right] \\ &= \sum_{i=1}^q \Pr \left[\text{Find}_i : \mathcal{A}^{G \setminus S}(z), (G, H, S, z) \right] = \sum_{i=1}^q \left\| \Pi_S \prod_{j=1}^{i-1} [U_j O_G \Pi_{\perp}] |\psi_z\rangle \right\|^2. \end{aligned} \quad (11)$$

Here $\prod_{j=1}^0 [U_j O_G \Pi_{\perp}]$ is defined as the identity operator and $\prod_{j=1}^{i-1} [U_j O_G \Pi_{\perp}]$ for $i > 1$ is defined as $U_{i-1} O_G \Pi_{\perp} \dots U_1 O_G \Pi_{\perp}$.

Note that P_{find}^{GHSz} in Eq. (8) denotes only the probability of Find , rather than the probability that the algorithm successfully guesses an element in S . In the following, by using the oracle 1_S , we design a new algorithm $\mathcal{B}^{G, 1_S}(z)$ and then establish a connection between its probability of guessing an element in S and P_{find}^{GHSz} . The detailed construction of $\mathcal{B}^{G, 1_S}(z)$ is as follows:

- $\mathcal{B}^{G, 1_S}(z)$ has initial state $|0^a\rangle|0, 0^m\rangle_{\text{BT}}$ and performs U_z to get $|\psi_z\rangle|0, 0^m\rangle_{\text{BT}}$. Then, $\mathcal{B}^{G, 1_S}(z)$ performs $\prod_{i=1}^q [U_i O_G U_S^i] = U_q O_G U_S^q \dots U_1 O_G U_S^1$ and finally measures the registers BT in the computational basis to get the measurement outcome (b, t) .
- $\mathcal{B}^{G, 1_S}(z)$ outputs $x := t$ if $b \neq 0$ and outputs $\perp$ otherwise.

We note that the U_S^i defined in Eq. (6) for any $i \in \{1, \dots, q\}$ can be implemented by querying 1_S twice. Specifically, on the basis state $|x, y\rangle|b, t\rangle_{\text{BT}}$, we first query 1_S to obtain the membership bit $\llbracket x \in S \rrbracket$ and compute $r := \llbracket x \in S \rrbracket \wedge \llbracket b \in \{0, i\} \rrbracket$; then, according to r , we apply a controlled-XOR operation on the register T and a controlled permutation ($|0\rangle \rightarrow |i\rangle$ and $|i\rangle \rightarrow |0\rangle$) on the register B ; next, since the permutation preserves the predicate $b \in \{0, i\}$, we uncompute r using $\llbracket x \in S \rrbracket$ and $\llbracket b \in \{0, i\} \rrbracket$; finally, we query 1_S again to erase the membership bit $\llbracket x \in S \rrbracket$. Hence, $\mathcal{B}^{G, 1_S}(z)$ queries G for q times and queries 1_S for $2q$ times.

Below, we analyze the probability that $\mathcal{B}^{G, 1_S}(z)$ outputs an x satisfying $x \in S$. Based on the definition of U_S^i in Eq. (6) and the definitions of Π_S and $\Pi_{\perp}$ in

Eq. (10), the final state of $\mathcal{B}^{G,1s}(z)$ before performing the measurement is

$$\begin{aligned}
& \prod_{i=1}^q [U_i O_G U_S^i] |\psi_z\rangle |0, 0^m\rangle_{\text{BT}} \\
&= \prod_{i=1}^q [U_i O_G U_S^i] (\Pi_S + \Pi_\perp) |\psi_z\rangle |0, 0^m\rangle_{\text{BT}} \\
&= \sum_{x \in S} \prod_{i=1}^q [U_i O_G U_S^i] |x\rangle \langle x| |\psi_z\rangle |0, 0^m\rangle_{\text{BT}} + \prod_{i=1}^q [U_i O_G U_S^i] \Pi_\perp |\psi_z\rangle |0, 0^m\rangle_{\text{BT}} \\
&\stackrel{(a)}{=} \sum_{x \in S} \prod_{i=2}^q [U_i O_G U_S^i] U_1 O_G |x\rangle \langle x| |\psi_z\rangle |1, x\rangle_{\text{BT}} + \prod_{i=2}^q [U_i O_G U_S^i] U_1 O_G \Pi_\perp |\psi_z\rangle |0, 0^m\rangle_{\text{BT}} \\
&\stackrel{(b)}{=} \sum_{x \in S} \prod_{i=1}^q [U_i O_G] |x\rangle \langle x| |\psi_z\rangle |1, x\rangle_{\text{BT}} + \prod_{i=2}^q [U_i O_G U_S^i] |\psi'_z\rangle |0, 0^m\rangle_{\text{BT}}.
\end{aligned}$$

Here (a) follows from the facts that $U_S^1 |x\rangle \langle x| |\psi_z\rangle |0, 0^m\rangle_{\text{BT}} = |x\rangle \langle x| |\psi_z\rangle |1, x\rangle_{\text{BT}}$ and U_S^1 does not change the state $\Pi_\perp |\psi_z\rangle |0, 0^m\rangle_{\text{BT}}$. (b) follows from two facts. First, for any $i \in \{2, \dots, q\}$, U_S^i leaves any state of the form $|\phi\rangle |1, x\rangle_{\text{BT}}$ unchanged, and hence the U_S^i can be omitted from the first term. Second, we introduce the notation $|\psi'_z\rangle := U_1 O_G \Pi_\perp |\psi_z\rangle$ and rewrite the second term accordingly. It can be observed that the above equation essentially provides an iterative structure, allowing us to derive

$$\begin{aligned}
& \prod_{i=1}^q [U_i O_G U_S^i] |\psi_z\rangle |0, 0^m\rangle_{\text{BT}} \\
&= \sum_{j=1}^q \sum_{x \in S} \prod_{i=j}^q [U_i O_G] |x\rangle \langle x| \prod_{i=1}^{j-1} [U_i O_G \Pi_\perp] |\psi_z\rangle |j, x\rangle_{\text{BT}} \\
&\quad + \prod_{i=1}^q [U_i O_G \Pi_\perp] |\psi_z\rangle |0, 0^m\rangle_{\text{BT}}.
\end{aligned} \tag{12}$$

Here $\prod_{i=1}^0 [U_i O_G \Pi_\perp]$ is defined as the identity operator and $\prod_{i=1}^{j-1} [U_i O_G \Pi_\perp]$ for $j > 1$ is defined as $U_{j-1} O_G \Pi_\perp \dots U_1 O_G \Pi_\perp$. Define

$$\text{Adv}(\mathcal{B}) := \Pr [x \in S : x \leftarrow \mathcal{B}^{G,1s}(z)]. \tag{13}$$

Thus, based on Eq. (12), the probability $\text{Adv}(\mathcal{B})$ can be computed as

$$\begin{aligned}
\text{Adv}(\mathcal{B}) &= \left\| \sum_{j=1}^q \sum_{x \in S} \prod_{i=j}^q [U_i O_G] |x\rangle \langle x| \prod_{i=1}^{j-1} [U_i O_G \Pi_\perp] |\psi_z\rangle |j, x\rangle_{\text{BT}} \right\|^2 \\
&= \sum_{j=1}^q \sum_{x \in S} \left\| \prod_{i=j}^q [U_i O_G] |x\rangle \langle x| \prod_{i=1}^{j-1} [U_i O_G \Pi_\perp] |\psi_z\rangle |j, x\rangle_{\text{BT}} \right\|^2
\end{aligned}$$

$$\begin{aligned}
&= \sum_{j=1}^q \sum_{x \in S} \left\| |x\rangle\langle x| \prod_{i=1}^{j-1} [U_i O_G \Pi_{\perp}] |\psi_z\rangle \right\|^2 \\
&= \sum_{j=1}^q \left\| \sum_{x \in S} |x\rangle\langle x| \prod_{i=1}^{j-1} [U_i O_G \Pi_{\perp}] |\psi_z\rangle \right\|^2 \\
&= \sum_{j=1}^q \left\| \Pi_S \prod_{i=1}^{j-1} [U_i O_G \Pi_{\perp}] |\psi_z\rangle \right\|^2 \stackrel{(a)}{=} P_{\text{find}}^{GHSz}.
\end{aligned} \tag{14}$$

The equation (a) follows from Eq. (11). Therefore, the probability that the algorithm $\mathcal{B}^{G,1s}(z)$ constructed above outputs an element in S is exactly P_{find}^{GHSz} .

Next, we will apply the amplitude amplification technique to amplify $\text{Adv}(\mathcal{B})$. We first introduce the following notation.

$$\begin{aligned}
U_{\mathcal{B}} &:= \prod_{i=1}^q [U_i O_G U_S^i] U_z, \quad |\psi_{\mathcal{B}}\rangle := \prod_{i=1}^q [U_i O_G \Pi_{\perp}] |\psi_z\rangle |0, 0^m\rangle_{\text{BT}}, \\
|\psi_S\rangle &:= \sum_{j=1}^q \sum_{x \in S} \prod_{i=j}^q [U_i O_G] |x\rangle\langle x| \prod_{i=1}^{j-1} [U_i O_G \Pi_{\perp}] |\psi_z\rangle |j, x\rangle_{\text{BT}}.
\end{aligned} \tag{15}$$

Here $U_{\mathcal{B}}$ denotes the unitary operation implemented by $\mathcal{B}^{G,1s}(z)$. By Eq. (12) and Eq. (14), we have $U_{\mathcal{B}}|0^a\rangle|0, 0^m\rangle_{\text{BT}} = |\psi_{\mathcal{B}}\rangle + |\psi_S\rangle$ and $\text{Adv}(\mathcal{B}) = \|\psi_S\|^2 = P_{\text{find}}^{GHSz}$. Since $|\psi_{\mathcal{B}}\rangle$ and $|\psi_S\rangle$ are orthogonal, $U_{\mathcal{B}}|0^a\rangle|0, 0^m\rangle_{\text{BT}} = |\psi_{\mathcal{B}}\rangle + |\psi_S\rangle$ implies that $\|\psi_{\mathcal{B}}\|^2 + \|\psi_S\|^2 = 1$. Therefore, defining $\theta := \arcsin(\|\psi_S\|)$, we have $0 \leq \theta \leq \pi/2$, $\sin(\theta) = \|\psi_S\|$, $\cos(\theta) = \|\psi_{\mathcal{B}}\|$, and

$$\text{Adv}(\mathcal{B}) = P_{\text{find}}^{GHSz} = \|\psi_S\|^2 = \sin^2(\theta). \tag{16}$$

We next define two new states as:

$$|\psi_{\text{bad}}\rangle := \begin{cases} |\psi_{\mathcal{B}}\rangle / \cos(\theta) & \text{if } \theta \neq \pi/2, \\ \mathbf{0} & \text{if } \theta = \pi/2, \end{cases} \quad |\psi_{\text{good}}\rangle := \begin{cases} |\psi_S\rangle / \sin(\theta) & \text{if } \theta \neq 0, \\ \mathbf{0} & \text{if } \theta = 0, \end{cases} \tag{17}$$

where $\mathbf{0}$ denotes the zero vector. With these definitions, the final state of $\mathcal{B}^{G,1s}(z)$ just before measurement, namely $U_{\mathcal{B}}|0^a\rangle|0, 0^m\rangle_{\text{BT}}$, can be written as

$$U_{\mathcal{B}}|0^a\rangle|0, 0^m\rangle_{\text{BT}} = \cos(\theta) \cdot |\psi_{\text{bad}}\rangle + \sin(\theta) \cdot |\psi_{\text{good}}\rangle. \tag{18}$$

At this point, we introduce the amplitude amplification technique, i.e., following Lemma 1. This lemma follows directly from [6, Lemma 1] together with the analysis in Eq. (2) to Eq. (8) of the same paper. For completeness, we provide a detailed proof of this lemma in Supplementary Material D.1.

Lemma 1. *Let Am be the amplitude-amplification operator, which is defined as*

$$Am := U_{\mathcal{B}} \circ (2|0^a\rangle\langle 0^a|_{\text{BT}} - I) \circ U_{\mathcal{B}}^{\dagger} \circ (2|0\rangle\langle 0|_{\text{B}} - I_{\text{B}}).$$

Here I denotes the identity operator on the whole register while I_B denotes the identity operator on the register B . Then, for any $k \in \mathbb{N}^+$, we have

$$(Am)^k U_B |0^a\rangle |0, 0^m\rangle_{BT} = \cos((2k+1)\theta) \cdot |\psi_{bad}\rangle + \sin((2k+1)\theta) \cdot |\psi_{good}\rangle.$$

For any fixed constant $0 < \epsilon < 1$, we define the following algorithm $\mathcal{C}_\epsilon^{G,1s}(z)$, which aims to amplify the success probability of $\mathcal{B}^{G,1s}(z)$, i.e., the $\text{Adv}(\mathcal{B})$ defined in Eq. (13).

- $\mathcal{C}_\epsilon^{G,1s}(z)$ has initial state $|0^a\rangle |0, 0^m\rangle_{BT}$ and first samples k according to the distribution $\mathfrak{D}_\epsilon$ defined in Table 4. Then, $\mathcal{C}_\epsilon^{G,1s}(z)$ performs $(Am)^k U_B$, and finally measures the registers BT in the computational basis to get the measurement outcome (b, t) .
- $\mathcal{C}_\epsilon^{G,1s}(z)$ outputs $x := t$ if $b \neq 0$ and outputs $\perp$ otherwise.

For the running time, since the time complexity of one application of U_B or $U_B^\dagger$ (Eq. (15)) is close to that of one execution of $\mathcal{A}$, the running time of $\mathcal{C}_\epsilon^{G,1s}(z)$ satisfies $\mathcal{T}_C^{\text{exp}} \lesssim (2\mathbb{E}[\mathfrak{D}_\epsilon] + 1) \cdot \mathcal{T}_A$. For the expectation $\mathbb{E}[\mathfrak{D}_\epsilon]$, we can compute

$$\mathbb{E}[\mathfrak{D}_\epsilon] = \sum_{l=0}^L \frac{2^l}{T \cdot 2^l} = \sum_{l=0}^L \frac{1}{T} = \frac{L+1}{T} \stackrel{(a)}{\leq} L+1 = \left\lceil \log_2 \frac{1}{\epsilon} \right\rceil + 1 \leq \log_2 \frac{1}{\epsilon} + 2. \quad (19)$$

Here (a) uses the fact that $T \geq 1$. Therefore, we have $\mathcal{T}_C^{\text{exp}} \lesssim (5 - 2\log_2 \epsilon) \cdot \mathcal{T}_A$.

Table 4: Distribution $\mathfrak{D}_\epsilon$ for $0 < \epsilon < 1$. Here $L := \lceil \log_2 \epsilon^{-1} \rceil$ and $T := \sum_{l=0}^L 1/2^l$.

k	2^0	2^1	2^2	$\dots$	2^L
probability	$\frac{1}{T \cdot 2^0}$	$\frac{1}{T \cdot 2^1}$	$\frac{1}{T \cdot 2^2}$	$\dots$	$\frac{1}{T \cdot 2^L}$

According to Lemma 1, for a fixed number of iterations $k \in \{2^0, 2^1, \dots, 2^L\}$, the whole state of $\mathcal{C}_\epsilon^{G,1s}(z)$ before performing the final measurement is

$$(Am)^k U_B |0^a\rangle |0, 0^m\rangle_{BT} = \cos((2k+1)\theta) \cdot |\psi_{bad}\rangle + \sin((2k+1)\theta) \cdot |\psi_{good}\rangle. \quad (20)$$

Define

$$\text{Adv}(\mathcal{C}_\epsilon) := \Pr[x \in S : x \leftarrow \mathcal{C}_\epsilon^{G,1s}(z)].$$

Hence, by the definition of $|\psi_{bad}\rangle$ and $|\psi_{good}\rangle$ in Eq. (17), we have

$$\begin{aligned} \text{Adv}(\mathcal{C}_\epsilon) &:= \sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta) \cdot \|\psi_{good}\|^2 \\ &\stackrel{(a)}{=} \sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta). \end{aligned} \quad (21)$$

Here (a) is derived by considering two cases. If $\theta = 0$, then $\sin((2 \cdot 2^l + 1)\theta) = 0$ for every l and $\|\psi_{good}\| = 0$. Similarly, if $\theta \neq 0$, then $|\psi_{good}\rangle$ is a unit vector, so $\|\psi_{good}\| = 1$. Therefore, the factor $\|\psi_{good}\|^2$ can be directly omitted in either case. In the following lemma, up to an additive error ϵ , we bound $\sin(\theta)$ in terms of the sum $\sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta)$.

Lemma 2. *For any $0 \leq \theta \leq \pi/2$, $\sin(\theta) \leq 10 \cdot \sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta) + \epsilon$.*

Proof. The full proof of this lemma is given in Supplementary Material D.2. $\square$

Recall that $\text{Adv}(\mathcal{B}) = \sin^2(\theta)$ (Eq. (16)). Hence, the previous lemma shows that, up to an additive error ϵ , the algorithm $\mathcal{C}_\epsilon^{G,1s}(z)$ successfully amplifies $\text{Adv}(\mathcal{B})$ from $\sin^2(\theta)$ to at least $\sin(\theta)/10$. That is to say,

$$\sqrt{\text{Adv}(\mathcal{B})} = \sin(\theta) \leq 10 \cdot \text{Adv}(\mathcal{C}_\epsilon) + \epsilon.$$

Combining the above equation with Eq. (9) and Eq. (16), we have

$$|P_{\text{left}}^{GHSz} - P_{\text{right}}^{GHSz}| \leq 2\sqrt{q+1} \cdot (10 \cdot \text{Adv}(\mathcal{C}_\epsilon) + \epsilon). \quad (22)$$

This inequality holds for every $0 < \epsilon < 1$. Set $\epsilon = 2^{-m}$, and define $\mathcal{C}'$ to be the algorithm that samples $x \leftarrow_{\S} \{0,1\}^m$ and outputs x as its guess for an element of S . Then, we have $\text{Adv}(\mathcal{C}') = |S|/2^m$. Moreover, let $\mathcal{D}^{G,1s}(z)$ be an algorithm that runs $\mathcal{C}_\epsilon^{G,1s}(z)$ with probability $10/11$ and $\mathcal{C}'$ with probability $1/11$, and define $\text{Adv}(\mathcal{D}) := \Pr[x \in S : x \leftarrow \mathcal{D}^{G,1s}(z)]$. We then have $11 \cdot \text{Adv}(\mathcal{D}) = 10 \cdot \text{Adv}(\mathcal{C}) + \text{Adv}(\mathcal{C}')$ and

$$|P_{\text{left}}^{GHSz} - P_{\text{right}}^{GHSz}| \leq 22\sqrt{q+1} \cdot \text{Adv}(\mathcal{D}). \quad (23)$$

In fact, the above inequality follows by considering two cases. If $|S| = 0$, then G is the same as H , and hence $P_{\text{left}}^{GHSz} = P_{\text{right}}^{GHSz}$, so the above inequality holds trivially. If $|S| > 0$, the above inequality follows from Eq. (22) and the fact that $\text{Adv}(\mathcal{C}') = |S|/2^m \geq 2^{-m} = \epsilon$. As for the running time, recall that we have $\mathcal{T}_{\mathcal{C}}^{\text{exp}} \lesssim (5 - 2\log_2 \epsilon) \cdot \mathcal{T}_{\mathcal{A}}$, thus we have $\mathcal{T}_{\mathcal{D}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}}$. This completes the proof of Theorem 1 under $\text{Adv}(\mathcal{D}) = \Pr[x \in S : x \leftarrow \mathcal{D}^{G,1s}(z)]$.

As for the case of $\text{Adv}(\mathcal{D}) = \Pr[x \in S : x \leftarrow \mathcal{D}^{H,1s}(z)]$, the proof is completely analogous. Indeed, none of the arguments from Eq. (8) to Eq. (23) relies specifically on G , and the entire analysis can be carried over to H in the same way. This completes the proof of Theorem 1. $\square$

Theorem 2 (Random SSEAM-O2H). *Let $G, H : X \rightarrow Y$ be random functions and $S \subseteq X (= \{0,1\}^m)$ be a random set. Let $z \in Z$ be a random bitstring. The tuple (G, H, S, z) may have arbitrary joint distribution $\mathfrak{D}$ and satisfies that $\forall x \notin S, G(x) = H(x)$. Let 1_S denote the indicator function of the set S , that is, $1_S(x) = 1$ if $x \in S$ and 0 otherwise. Let $\mathcal{A}$ be a q -query quantum oracle algorithm. Define*

$$P_{\text{left}} := \Pr_{(G,H,S,z) \leftarrow \mathfrak{D}} [b = 1 : b \leftarrow \mathcal{A}^H(z)], P_{\text{right}} := \Pr_{(G,H,S,z) \leftarrow \mathfrak{D}} [b = 1 : b \leftarrow \mathcal{A}^G(z)].$$

Then, we can construct an algorithm $\mathcal{D}^{O,1s}(z)$ ($O \in \{G, H\}$), which makes an expected $(2m+5)q$ queries to O and an expected $(4m+10)q$ queries to 1_S , has running time $\mathcal{T}_{\mathcal{D}}^{\text{exp}} \lesssim (2m+5) \cdot \mathcal{T}_A$, and satisfies

$$|P_{\text{left}} - P_{\text{right}}| \leq 22\sqrt{q+1} \cdot \text{Adv}(\mathcal{D}).$$

Here $\text{Adv}(\mathcal{D})$ can be $\Pr[x \in S : x \leftarrow \mathcal{D}^{G,1s}(z)]$ or $\Pr[x \in S : x \leftarrow \mathcal{D}^{H,1s}(z)]$, where the probability is taken over $(G, H, S, z) \leftarrow \mathfrak{D}$.

Proof. Based on Eq. (7) in Theorem 1, we can directly prove this theorem by averaging over $(G, H, S, z) \leftarrow \mathfrak{D}$. $\square$

4 Double-Sided Extract-Amplify-Measure O2H

Our Double-Sided Extract-Amplify-Measure (DSEAM) O2H focuses on the tuple (G, H, S, z) and the function f . Here G, H are functions with domain X and codomain Y , $z \in Z$ is a random bitstring, $S \subseteq X$ and G, H, S satisfy that $G(x) = H(x)$ for all $x \notin S$. The tuple (G, H, S, z) may have arbitrary joint distribution. As for the function f , it has input space X and output space $\{0, 1\}^m$, and satisfies $f(S) = \{w^*\}$ for a single $w^* \in \{0, 1\}^m$, that is, $f(x) = w^*$ for any $x \in S$.

Let $\mathbf{B}$ (resp. $\mathbf{T}$) be the quantum register defined over $\{0, 1\}$ (resp $\{0, 1\}^m$). During our proof, we will frequently use following five unitary operations.

$$\begin{aligned} O_G &: |x, y\rangle \mapsto |x, y \oplus G(x)\rangle, \\ O_H &: |x, y\rangle \mapsto |x, y \oplus H(x)\rangle, \\ T_f &: |x, y\rangle |b, t\rangle_{\mathbf{BT}} \mapsto |x, y\rangle |b, t \oplus (b \cdot f(x))\rangle_{\mathbf{BT}}, \\ O_{G,H} &:= (O_H \otimes |+\rangle\langle +|_{\mathbf{B}}) + (O_G \otimes |-\rangle\langle -|_{\mathbf{B}}), \\ O_{G,H}^f &:= T_f \circ O_{G,H} \circ T_f. \end{aligned} \tag{24}$$

Here O_G (resp. O_H) is used to simulate G (resp. H) queries of the adversary. The T_f acts as the identity when $b = 0$, whereas when $b = 1$, it XORs the tag $f(x)$ into the register $\mathbf{T}$. The $O_{G,H}$ uses $\mathbf{B}$ as the control register, and performs O_H (resp. O_G) if the state of $\mathbf{B}$ is $|+\rangle$ (resp. $|-\rangle$). The $O_{G,H}^f$ is the same as $O_{G,H}$, except that it performs T_f both before and after the performing of $O_{G,H}$.

One can directly verify that all the unitary operations define in Eq. (24) are Hermitian, i.e., their Hermitian transpose is exactly themselves. Now, for $O_{G,H}^f$, we introduce the following lemma, which will be used in later proof.

Lemma 3. *For any initial state $|\phi\rangle$ and any unitary operations $U_0, \dots, U_t$ ($t \in \mathbb{N}^+$) acting on $|\phi\rangle$, we have*

$$\left(\prod_{i=1}^t [U_i O_{G,H}^f] U_0 \right) |\phi\rangle |0, 0^m\rangle_{\mathbf{BT}} = P_t |\phi\rangle \otimes |0, 0^m\rangle_{\mathbf{BT}} + Q_t |\phi\rangle \otimes |1, w^*\rangle_{\mathbf{BT}},$$

where

$$P_t := \frac{1}{2} \left(\prod_{i=1}^t [U_i O_H] U_0 + \prod_{i=1}^t [U_i O_G] U_0 \right),$$

$$Q_t := \frac{1}{2} \left(\prod_{i=1}^t [U_i O_H] U_0 - \prod_{i=1}^t [U_i O_G] U_0 \right).$$

Here $\prod_{i=1}^t [U_i O_{G,H}^f]$ is defined as $U_t O_{G,H}^f U_{t-1} O_{G,H}^f \dots U_1 O_{G,H}^f$, and analogously for $\prod_{i=1}^t [U_i O_H]$ and $\prod_{i=1}^t [U_i O_G]$.

Proof. This lemma was already implicitly used in the proof of [4, Lemma 5], although it was not explicitly stated as a lemma or formally proved. For completeness, we provide a detailed proof in Supplementary Material D.3, which is achieved by induction. We also note that the U_0 used here is not essential, since one may regard $U_0|\phi\rangle$ as a new initial state. We include U_0 here only to facilitate subsequent applications of this lemma. $\square$

In the following, we first prove the fixed version of the DSEAM-O2H, where the tuple (G, H, S, z) is fixed. Then, we extend the result to the random version, where the tuple follows an arbitrary joint distribution.

Theorem 3 (Fixed DSEAM-O2H). *Let $G, H : X \rightarrow Y$ be fixed functions and $S \subseteq X$ be a fixed set. Let $z \in Z$ be a fixed bitstring. The tuple (G, H, S, z) satisfies that $\forall x \notin S, G(x) = H(x)$. Let $f : X \rightarrow \{0, 1\}^m$ be a function such that $f(S) = \{w^*\}$ for a single $w^* \in \{0, 1\}^m$. Let $\mathcal{A}^O$ ($O \in \{G, H\}$) be a q -query quantum oracle algorithm. Define*

$$P_{\text{left}}^{GHSz} := \Pr [b = 1 : b \leftarrow \mathcal{A}^H(z)], \quad P_{\text{right}}^{GHSz} := \Pr [b = 1 : b \leftarrow \mathcal{A}^G(z)].$$

Then we can construct an algorithm $\mathcal{D}^{G,H}(z)$, which makes an expected $(2m + 5)q$ queries to G and an expected $(2m + 5)q$ queries to H , has running time $\mathcal{T}_{\mathcal{D}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}}$, and satisfies

$$|P_{\text{left}}^{GHSz} - P_{\text{right}}^{GHSz}| \leq 22 \cdot \text{Adv}(\mathcal{D}). \quad (25)$$

Here $\text{Adv}(\mathcal{D}) := \Pr[w = w^* : w \leftarrow \mathcal{D}^{G,H}(z)]$.

Proof. The proof of this theorem follows the same high-level idea as that of Theorem 1: both aim to amplify the success probability of the one-wayness attacker constructed in prior work. First, similar to the proof of Theorem 1, we assume $\mathcal{A}^O(z)$ ($O \in \{G, H\}$) to be unitary and suppose that $\mathcal{A}^O(z)$ acts on an a -qubit register with the initial state $|\psi_z\rangle := U_z|0^a\rangle$. We then denote $U_1, \dots, U_q$ as the unitary operations performed by $\mathcal{A}^O(z)$ between its oracle queries.

At this point, by using Theorem 13 under the fixed (G, H, S, z) we considered, we can construct a new algorithm $\mathcal{B}^{G,H}(z)$ such that

$$|P_{\text{left}}^{GHSz} - P_{\text{right}}^{GHSz}| \leq 2\sqrt{\text{Adv}(\mathcal{B})}, \quad (26)$$

where

$$\text{Adv}(\mathcal{B}) := \Pr [w = w^* : w \leftarrow \mathcal{B}^{G,H}(z)].$$

For the sake of simplicity, Theorem 13 does not explicitly describe the construction of $\mathcal{B}^{G,H}(z)$. Here, based on the $O_{G,H}^f$ defined in Eq. (24), we provide the explicit construction of $\mathcal{B}^{G,H}(z)$ given in [4] as follows:

- $\mathcal{B}^{G,H}(z)$ has initial state $|0^a\rangle|0, 0^m\rangle_{\text{BT}}$ and performs U_z to get $|\psi_z\rangle|0, 0^m\rangle_{\text{BT}}$. Then, $\mathcal{B}^{G,H}(z)$ performs $\prod_{i=1}^q [U_i \circ O_{G,H}^f] = U_q O_{G,H}^f \dots U_1 O_{G,H}^f$ and finally measures the registers BT in the computational basis to get the measurement outcome (b, t) .
- $\mathcal{B}^{G,H}(z)$ outputs $w := t$ if $b = 1$ and outputs $\perp$ otherwise.

Since $O_{G,H}^f$ can be implemented using one query to G and one query to H , the algorithm $\mathcal{B}^{G,H}(z)$ makes q queries to G and q queries to H .

Below, we analyze the probability that $\mathcal{B}^{G,H}(z)$ outputs w^* . By using Lemma 3, the final state of $\mathcal{B}^{G,H}(z)$ before performing the measurement is

$$\prod_{i=1}^q [U_i O_{G,H}^f] |\psi_z\rangle |0, 0^m\rangle_{\text{BT}} = P_q |\psi_z\rangle \otimes |0, 0^m\rangle_{\text{BT}} + Q_q |\psi_z\rangle \otimes |1, w^*\rangle_{\text{BT}},$$

where $P_q = 1/2 \prod_{i=1}^q [U_i O_H] + 1/2 \prod_{i=1}^q [U_i O_G]$ and $Q_q = 1/2 \prod_{i=1}^q [U_i O_H] - 1/2 \prod_{i=1}^q [U_i O_G]$. Thus, we have $\text{Adv}(\mathcal{B}) = \|Q_q |\psi_z\rangle \otimes |1, w^*\rangle_{\text{BT}}\|^2$. Next, we will apply the amplitude amplification technique to amplify $\text{Adv}(\mathcal{B})$. We first introduce the following notation.

$$U_{\mathcal{B}} := \prod_{i=1}^q [U_i O_{G,H}^f] U_z, \quad (27)$$

$$|\psi_{0,0^m}\rangle := P_q |\psi_z\rangle \otimes |0, 0^m\rangle_{\text{BT}}, \quad |\psi_{1,w^*}\rangle := Q_q |\psi_z\rangle \otimes |1, w^*\rangle_{\text{BT}}.$$

Here $U_{\mathcal{B}}$ denotes the unitary operation implemented by $\mathcal{B}^{G,H}(z)$. The above two equations show that we have $U_{\mathcal{B}}|0^a\rangle|0, 0^m\rangle_{\text{BT}} = |\psi_{0,0^m}\rangle + |\psi_{1,w^*}\rangle$ and $\text{Adv}(\mathcal{B}) = \|\psi_{1,w^*}\|^2$. Since $|\psi_{0,0^m}\rangle$ and $|\psi_{1,w^*}\rangle$ are orthogonal, $U_{\mathcal{B}}|0^a\rangle|0, 0^m\rangle_{\text{BT}} = |\psi_{0,0^m}\rangle + |\psi_{1,w^*}\rangle$ implies that $\|\psi_{0,0^m}\|^2 + \|\psi_{1,w^*}\|^2 = 1$. Therefore, defining the angle $\theta := \arcsin(\|\psi_{1,w^*}\|)$, we have $0 \leq \theta \leq \pi/2$, $\sin(\theta) = \|\psi_{1,w^*}\|$, $\cos(\theta) = \|\psi_{0,0^m}\|$, and

$$\text{Adv}(\mathcal{B}) = \|\psi_{1,w^*}\|^2 = \sin^2(\theta). \quad (28)$$

We next define two new states as:

$$|\psi_{\text{bad}}\rangle := \begin{cases} |\psi_{0,0^m}\rangle / \cos(\theta) & \text{if } \theta \neq \pi/2, \\ \mathbf{0} & \text{if } \theta = \pi/2, \end{cases} \quad |\psi_{\text{good}}\rangle := \begin{cases} |\psi_{1,w^*}\rangle / \sin(\theta) & \text{if } \theta \neq 0, \\ \mathbf{0} & \text{if } \theta = 0. \end{cases} \quad (29)$$

where $\mathbf{0}$ denotes the zero vector. With these definitions, the final state of $\mathcal{B}^{G,H}(z)$ just before measurement, namely $U_{\mathcal{B}}|0^a\rangle|0, 0^m\rangle_{\text{BT}}$, can be written as

$$U_{\mathcal{B}}|0^a\rangle|0, 0^m\rangle_{\text{BT}} = \cos(\theta) \cdot |\psi_{\text{bad}}\rangle + \sin(\theta) \cdot |\psi_{\text{good}}\rangle.$$

Now, we introduce the amplitude amplification technique, i.e., following Lemma 4. The proof of this lemma is identical to that of Lemma 1, up to the corresponding changes in notation. For simplicity, we omit the detailed proof.

Table 5: Distribution $\mathfrak{D}_\epsilon$ for $0 < \epsilon < 1$. Here $L := \lceil \log_2 \epsilon^{-1} \rceil$ and $T := \sum_{l=0}^L 1/2^l$. This is the same distribution $\mathfrak{D}_\epsilon$ (Table 4) used in the proof of Theorem 1.

k	2^0	2^1	2^2	$\dots$	2^L
probability	$\frac{1}{T \cdot 2^0}$	$\frac{1}{T \cdot 2^1}$	$\frac{1}{T \cdot 2^2}$	$\dots$	$\frac{1}{T \cdot 2^L}$

Lemma 4. *Let Am be the amplitude-amplification operator, which is defined as*

$$Am := U_B \circ (2|0^a\rangle\langle 0|, 0^m)_{BT} \langle 0^a| \langle 0, 0^m|_{BT} - I) \circ U_B^\dagger \circ (2|0\rangle\langle 0|_B - I_B).$$

Here I denotes the identity operator on the whole register while I_B denotes the identity operator on the register B . Then, for any $k \in \mathbb{N}^+$, we have

$$(Am)^k U_B |0^a\rangle\langle 0|, 0^m)_{BT} = \cos((2k+1)\theta) \cdot |\psi_{bad}\rangle + \sin((2k+1)\theta) \cdot |\psi_{good}\rangle.$$

For any fixed constant $0 < \epsilon < 1$, we define the following algorithm $\mathcal{C}_\epsilon^{G,H}(z)$, which aims to amplify the success probability of $\mathcal{B}^{G,H}(z)$, i.e., the $\text{Adv}(\mathcal{B})$.

- $\mathcal{C}_\epsilon^{G,H}(z)$ has initial state $|0^a\rangle\langle 0|, 0^m)_{BT}$ and first samples k according to the distribution $\mathfrak{D}_\epsilon$ defined in Table 5. Then, $\mathcal{C}_\epsilon^{G,H}(z)$ performs $(Am)^k U_B$, and finally measures the registers BT in the computational basis to get the measurement outcome (b, t) .
- $\mathcal{C}_\epsilon^{G,H}(z)$ outputs $w := t$ if $b = 1$ and outputs $\perp$ otherwise.

For the running time, since the time complexity of one application of U_B or $U_B^\dagger$ (Eq. (27)) is close to that of one execution of $\mathcal{A}$, the running time of $\mathcal{C}_\epsilon^{G,H}(z)$ satisfies $\mathcal{T}_C^{\text{exp}} \lesssim (2\mathbb{E}[\mathfrak{D}_\epsilon] + 1) \cdot \mathcal{T}_A$. For the expectation $\mathbb{E}[\mathfrak{D}_\epsilon]$, by Eq. (19) we have $\mathbb{E}[\mathfrak{D}_\epsilon] \leq 2 - \log_2 \epsilon$. Therefore, we have $\mathcal{T}_C^{\text{exp}} \lesssim (5 - 2\log_2 \epsilon) \cdot \mathcal{T}_A$.

According to Lemma 4, for a fixed number of iterations $k \in \{2^0, 2^1, \dots, 2^L\}$, the whole state of $\mathcal{C}_\epsilon^{G,H}(z)$ before performing the final measurement is

$$(Am)^k U_B |0^a\rangle\langle 0|, 0^m)_{BT} = \cos((2k+1)\theta) \cdot |\psi_{bad}\rangle + \sin((2k+1)\theta) \cdot |\psi_{good}\rangle.$$

Define

$$\text{Adv}(\mathcal{C}_\epsilon) := \Pr [w = w^* : w \leftarrow \mathcal{C}_\epsilon^{G,H}(z)].$$

Hence, by the definition of $|\psi_{bad}\rangle$ and $|\psi_{good}\rangle$ in Eq. (29), we have

$$\begin{aligned} \text{Adv}(\mathcal{C}_\epsilon) &:= \sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta) \cdot \|\psi_{good}\|^2 \\ &\stackrel{(a)}{=} \sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta). \end{aligned}$$

Here (a) is derived by considering two cases. If $\theta = 0$, then $\sin((2 \cdot 2^l + 1)\theta) = 0$ for every l and $\|\psi_{good}\| = 0$. Similarly, if $\theta \neq 0$, then $|\psi_{good}\rangle$ is a unit vector, so $\|\psi_{good}\| = 1$. Thus, the factor $\|\psi_{good}\|^2$ can be directly omitted in either case.

Recall that $\text{Adv}(\mathcal{B}) = \sin^2(\theta)$ (Eq. (28)). Hence, Lemma 2 shows that, up to an additive error ϵ , the algorithm $\mathcal{C}_\epsilon^{G,H}(z)$ successfully amplifies $\text{Adv}(\mathcal{B})$ from $\sin^2(\theta)$ to at least $\sin(\theta)/10$. That is to say,

$$\sqrt{\text{Adv}(\mathcal{B})} = \sin(\theta) \leq 10 \cdot \text{Adv}(\mathcal{C}_\epsilon) + \epsilon.$$

Combining the above equation with Eq. (26), we have

$$|P_{\text{left}}^{GHSz} - P_{\text{right}}^{GHSz}| \leq 20 \cdot \text{Adv}(\mathcal{C}_\epsilon) + 2\epsilon.$$

This inequality holds for every $0 < \epsilon < 1$. Set $\epsilon = 2^{-m}$, and define $\mathcal{C}'$ to be the algorithm that samples $x \leftarrow_{\$} \{0,1\}^m$ and outputs x as its guess for w^* . Then, we have $\text{Adv}(\mathcal{C}') = 1/2^m = \epsilon$. Moreover, let $\mathcal{D}^{G,H}(z)$ be an algorithm that runs $\mathcal{C}_\epsilon^{G,H}(z)$ with probability $10/11$ and $\mathcal{C}'$ with probability $1/11$, and define $\text{Adv}(\mathcal{D}) := \Pr[w = w^* : w \leftarrow \mathcal{D}^{G,H}(z)]$. We then have $11 \cdot \text{Adv}(\mathcal{D}) = 10 \cdot \text{Adv}(\mathcal{C}) + \epsilon$ and

$$|P_{\text{left}}^{GHSz} - P_{\text{right}}^{GHSz}| \leq 22 \cdot \text{Adv}(\mathcal{D}).$$

As for the running time, recall that we have $\mathcal{T}_{\mathcal{C}}^{\text{exp}} \lesssim (5 - 2 \log_2 \epsilon) \cdot \mathcal{T}_{\mathcal{A}}$, thus we have $\mathcal{T}_{\mathcal{D}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}}$. This completes the proof of Theorem 3. $\square$

Theorem 4 (Random DSEAM-O2H). *Let $G, H : X \rightarrow Y$ be random functions and $S \subseteq X$ be a random set. Let $z \in Z$ be a random bitstring. The tuple (G, H, S, z) may have arbitrary joint distribution $\mathfrak{D}$ and satisfies that $\forall x \notin S, G(x) = H(x)$. Let $f : X \rightarrow \{0,1\}^m$ be a function such that $f(S) = \{w^*\}$ for a single $w^* \in \{0,1\}^m$. Let $\mathcal{A}$ be a q -query quantum oracle algorithm. Define*

$$P_{\text{left}} := \Pr_{(G,H,S,z) \leftarrow \mathfrak{D}} [b = 1 : b \leftarrow \mathcal{A}^H(z)], P_{\text{right}} := \Pr_{(G,H,S,z) \leftarrow \mathfrak{D}} [b = 1 : b \leftarrow \mathcal{A}^G(z)].$$

Then we can construct an algorithm $\mathcal{D}^{G,H}(z)$, which makes an expected $(2m + 5)q$ queries to G and an expected $(2m + 5)q$ queries to H , has running time $\mathcal{T}_{\mathcal{D}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}}$, and satisfies

$$|P_{\text{left}} - P_{\text{right}}| \leq 22 \cdot \text{Adv}(\mathcal{D}).$$

Here $\text{Adv}(\mathcal{D}) := \Pr[w = w^* : w \leftarrow \mathcal{D}^{G,H}(z), (G, H, S, z) \leftarrow \mathfrak{D}]$.

Proof. Based on Eq. (25) in Theorem 3, we can directly prove this theorem by averaging over $(G, H, S, z) \leftarrow \mathfrak{D}$. $\square$

5 IND-CCA Security Proof of $\mathbf{U}^\perp$ in the QROM

In this section, by using our DSEAM-O2H (Theorem 4), we prove the IND-CCA security of $\mathbf{U}^\perp$ in the QROM. All the relevant security notions can be found in Supplementary Material C.

Transformation $U^\perp$. Let $P = (\text{Gen}, \text{Enc}, \text{Dec})$ be a dPKE scheme with message space $\mathcal{M} (= \{0, 1\}^m)$ and ciphertext space $\mathcal{C}$. For a given key space $\mathcal{K}$, let $G : \mathcal{M} \times \mathcal{C} \rightarrow \mathcal{K}$ be a hash function, and let $F : \mathcal{K}^{\text{prf}} \times \mathcal{C} \rightarrow \mathcal{K}$ be a pseudorandom function (PRF) with key space $\mathcal{K}^{\text{prf}}$. We associate the KEM scheme

$$U^\perp[P, G, F] := (\text{Gen}', \text{Enca}, \text{Deca}).$$

The constituting algorithms of $U^\perp[P, G, F]$ are given in Fig. 1.

Gen'	$\text{Enca}(pk)$	$\text{Deca}(sk' = (pk, sk, s), c)$
1 : $(pk, sk) \leftarrow \text{Gen}$	1 : $m \leftarrow_{\$} \mathcal{M}$	1 : $m' := \text{Dec}_{sk}(c)$
2 : $s \leftarrow_{\$} \mathcal{K}^{\text{prf}}$	2 : $c := \text{Enc}_{pk}(m)$	2 : if $m' \neq \perp \wedge \text{Enc}_{pk}(m') = c$
3 : $sk' := (pk, sk, s)$	3 : $k := G(m, c)$	3 : return $G(m', c)$
4 : return (pk, sk')	4 : return (k, c)	4 : else return $F(s, c)$

Fig. 1: Key encapsulation mechanism $U^\perp[P, G, F]$ with key space $\mathcal{K}$.

Theorem 5 (OW-CPA of $P \stackrel{\text{QROM}}{\Rightarrow} \text{IND-CCA of } U^\perp[P, G, F]$). *For η -injective dPKE scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M} (= \{0, 1\}^m)$, let $\mathcal{A}$ be an IND-CCA adversary against $U^\perp[P, G, F]$, making q_D classical queries to the decapsulation oracle and q_G quantum queries to the random oracle G . Then, we can construct a OW-CPA adversary $\mathcal{A}_{\text{ow}}$ against P , a PRF adversary $\mathcal{A}_{\text{prf}}$ against F , and an adversary $\mathcal{A}_{\text{ffc}}$ of the FFC game of P such that*

$$\begin{aligned} \text{Adv}_{U^\perp[P, G, F]}^{\text{IND-CCA}}(\mathcal{A}) &\leq \text{Adv}_F^{\text{PRF}}(\mathcal{A}_{\text{prf}}) + 22 \cdot \text{Adv}_P^{\text{OW-CPA}}(\mathcal{A}_{\text{ow}}) \\ &\quad + \text{Adv}_P^{\text{FFC}}(\mathcal{A}_{\text{ffc}}) + 24 \cdot \eta. \end{aligned}$$

Here, we have $\mathcal{T}_{\mathcal{A}_{\text{prf}}} \lesssim \mathcal{T}_{\mathcal{A}} + O(q_G + q_D) \cdot (\mathcal{T}_{\text{Enc}} + \mathcal{T}_{\text{Dec}}) + O(q_G^2 + q_D^2)$, $\mathcal{T}_{\mathcal{A}_{\text{ffc}}} \lesssim \mathcal{T}_{\mathcal{A}} + O(q_G) \cdot \mathcal{T}_{\text{Enc}} + O(q_G^2 + q_D^2)$ and $\mathcal{T}_{\mathcal{A}_{\text{ow}}}^{\text{exp}} \lesssim (2m+5) \cdot \mathcal{T}_{\mathcal{A}} + O(mq_G) \cdot \mathcal{T}_{\text{Enc}} + O(mq_G^2 + mq_D^2)$.

Proof. The full proof of Theorem 5 is given in Supplementary Material D.4. $\square$

The above theorem gives a tight IND-CCA security proof of $U^\perp[P, G, F]$ in the QROM, but requires P to be η -injective. In the following, we give a new proof without this requirement, at the cost of replacing the FFC game with the COR game, where the adversary has stronger capabilities¹⁴, and introduce an $O(\sqrt{q_G})$ loss in the term involving $\text{Adv}_P^{\text{COR}}(\mathcal{A}_{\text{cor}})$.

¹⁴ We regard the COR adversary as having stronger capabilities, since it is given both the public and secret keys, while the FFC adversary is given only the public key.

Theorem 6 (OW-CPA of $P \xRightarrow{\text{QROM}} \text{IND-CCA of } U^\perp[P, G, F]$). For dPKE scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M} (= \{0, 1\}^m)$, let $\mathcal{A}$ be an IND-CCA adversary against $U^\perp[P, G, F]$, making q_D classical queries to the decapsulation oracle and q_G quantum queries to the random oracle G . Then, we can construct a OW-CPA adversary $\mathcal{A}_{\text{ow}}$ against P , a PRF adversary $\mathcal{A}_{\text{prf}}$ against F , and an adversary $\mathcal{A}_{\text{cor}}$ of the COR game of P such that

$$\begin{aligned} \text{Adv}_{U^\perp[P, G, F]}^{\text{IND-CCA}}(\mathcal{A}) \leq & \text{Adv}_F^{\text{PRF}}(\mathcal{A}_{\text{prf}}) + 22 \cdot \text{Adv}_P^{\text{OW-CPA}}(\mathcal{A}_{\text{ow}}) \\ & + (4\sqrt{q_G + 1} + 46) \cdot \text{Adv}_P^{\text{COR}}(\mathcal{A}_{\text{cor}}). \end{aligned}$$

Here, we have $\mathcal{T}_{\mathcal{A}_{\text{prf}}}, \mathcal{T}_{\mathcal{A}_{\text{cor}}} \lesssim 3 \cdot \mathcal{T}_{\mathcal{A}} + O(q_G + q_D) \cdot (\mathcal{T}_{\text{Enc}} + \mathcal{T}_{\text{Dec}}) + O(q_G^2 + q_D^2)$ and $\mathcal{T}_{\mathcal{A}_{\text{ow}}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}} + O(mq_G) \cdot \mathcal{T}_{\text{Enc}} + O(mq_G^2 + mq_D^2)$.

Proof. The proof of this theorem closely follows that of Theorem 5, and a detailed proof is given in Supplementary Material D.5. $\square$

6 IND-CCA Security Proofs of FO-like Transformations

In this section, by using our SSEAM-O2H (Theorem 2), we prove the IND-CCA security of FO-like transformations $\text{FO}^\perp$, $\text{FO}_m^\perp$, $\text{FO}^\perp$, and $\text{FO}_m^\perp$ in the QROM. Recall that [4, Theorem 5] has shown that $\text{FO}^\perp$ (resp. $\text{FO}^\perp$) is as secure as $\text{FO}_m^\perp$ (resp. $\text{FO}_m^\perp$) and vice versa. Hence, we only prove the IND-CCA security of $\text{FO}_m^\perp$ and $\text{FO}^\perp$ in the QROM.

6.1 FO-like transformation $\text{FO}_m^\perp$

Transformation $\text{FO}_m^\perp$: Let $P = (\text{Gen}, \text{Enc}, \text{Dec})$ be an rPKE scheme with message space $\mathcal{M} (= \{0, 1\}^m)$ and randomness space $\mathcal{R} (= \{0, 1\}^r)$. For a given set $\mathcal{K} (= \{0, 1\}^k)$, let $H : \mathcal{M} \rightarrow \mathcal{R}$, $G : \mathcal{M} \rightarrow \mathcal{K}$ be hash functions. We associate the KEM scheme

$$\text{KEM}_m^\perp := \text{FO}_m^\perp[P, H, G] = (\text{Gen}', \text{Enca}, \text{Deca}_m^\perp).$$

The constituting algorithms of $\text{KEM}_m^\perp$ are given in Fig. 2.

Gen'	Enca(pk)	Deca _m [⊥] (sk, c)
1 : $(pk, sk) \leftarrow \text{Gen}$	1 : $m \leftarrow_{\$} \mathcal{M}$	1 : $m' := \text{Dec}_{sk}(c)$
2 : return (pk, sk)	2 : $c := \text{Enc}_{pk}(m; H(m))$	2 : if $m' = \perp \vee c \neq \text{Enc}_{pk}(m'; H(m'))$
	3 : $k := G(m)$	3 : return $\perp$
	4 : return (k, c)	4 : else return $G(m')$

Fig. 2: Key Encapsulation Mechanism $\text{KEM}_m^\perp$ with key space $\mathcal{K}$.

We first introduce the following theorem, which shows that in the QROM, the IND-CPA security of $\text{KEM}_m^\perp$ implies its IND-CCA security.

Theorem 7 (IND-CPA of $\text{KEM}_m^\perp \xrightarrow{\text{QROM}} \text{IND-CCA of } \text{KEM}_m^\perp$ [14, Thm. 2]). *Let rPKE scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$ be δ_{wc} -worst-correct and weakly γ -spread. Let $\mathcal{A}$ be an IND-CCA adversary against $\text{KEM}_m^\perp = \text{FO}_m^\perp[P, H, G]$, making q_D classical queries to the decapsulation oracle and making q_G (resp. q_H) quantum queries to the random oracle G (resp. H). Then, we can construct an IND-CPA adversary $\mathcal{A}_{\text{ind}}$ (in the QROM) against $\text{KEM}_m^\perp$ such that*

$$\text{Adv}_{\text{KEM}_m^\perp}^{\text{IND-CCA}}(\mathcal{A}) \leq \text{Adv}_{\text{KEM}_m^\perp}^{\text{IND-CPA}}(\mathcal{A}_{\text{ind}}) + 8(q_H + 1)\sqrt{\delta_{wc}} + (64q_H + 2)\delta_{wc} + 40q_D \cdot 2^{-\gamma/2}.$$

Here $\mathcal{A}_{\text{ind}}$ makes at most $q_G + q_D$ (resp. $2q_H$) quantum queries to the random oracle G (resp. H). The running time of $\mathcal{A}_{\text{ind}}$ is $\mathcal{T}_{\mathcal{A}_{\text{ind}}} \lesssim \mathcal{T}_{\mathcal{A}} + O(q_H q_D + q_H^2)$.

Then, by using our SSEAM-O2H (Theorem 2), we prove the following theorem, which shows that the IND-CPA security of $\text{KEM}_m^\perp$ in the QROM can be reduced to the IND-CPA security of P without the square-root advantage loss.

Theorem 8 (IND-CPA of $P \xrightarrow{\text{QROM}} \text{IND-CPA of } \text{KEM}_m^\perp$). *For an rPKE scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M} (= \{0, 1\}^m)$, let $\mathcal{A}$ be an IND-CPA adversary against $\text{KEM}_m^\perp = \text{FO}_m^\perp[P, H, G]$, making q_G (resp. q_H) quantum queries to the random oracle G (resp. H). Then, we can construct an IND-CPA adversary $\mathcal{A}_{\text{ind}}$ against P such that*

$$\text{Adv}_{\text{KEM}_m^\perp}^{\text{IND-CPA}}(\mathcal{A}) \leq 44\sqrt{q_G + q_H + 1} \cdot \text{Adv}_P^{\text{IND-CPA}}(\mathcal{A}_{\text{ind}}) + 1100 \cdot \frac{q_G + q_H + 1}{\sqrt{|\mathcal{M}|} - 1}.$$

Here, we have $\mathcal{T}_{\mathcal{A}_{\text{ind}}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}} + O(mq_G^2 + mq_H^2)$.

Proof. The full proof of this theorem is given in Supplementary Material E. $\square$

Combining Theorem 7 with Theorem 8, we finally obtain the following theorem. This theorem shows that, in the QROM, the IND-CCA security of $\text{KEM}_m^\perp$ can be reduced to the IND-CPA security of the underlying rPKE scheme without the square-root advantage loss.

Theorem 9 (IND-CPA of $P \xrightarrow{\text{QROM}} \text{IND-CCA of } \text{KEM}_m^\perp$). *Let rPKE scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$ be δ_{wc} -worst-correct and weakly γ -spread. Suppose that P has message space $\mathcal{M} (= \{0, 1\}^m)$. Let $\mathcal{A}$ be an IND-CCA adversary against $\text{KEM}_m^\perp = \text{FO}_m^\perp[P, H, G]$, making q_D classical queries to the decapsulation oracle and making q_G (resp. q_H) quantum queries to the random oracle G (resp. H). Then, we can construct an IND-CPA adversary $\mathcal{A}_{\text{ind}}$ against P such that*

$$\begin{aligned} \text{Adv}_{\text{KEM}_m^\perp}^{\text{IND-CCA}}(\mathcal{A}) \leq & 44\sqrt{2q_H + q_G + q_D + 1} \cdot \text{Adv}_P^{\text{IND-CPA}}(\mathcal{A}_{\text{ind}}) \\ & + 1100 \cdot \frac{2q_H + q_G + q_D + 1}{\sqrt{|\mathcal{M}|} - 1} + 8(q_H + 1) \cdot \sqrt{\delta_{wc}} \\ & + (64q_H + 2) \cdot \delta_{wc} + 40q_D \cdot 2^{-\gamma/2}. \end{aligned}$$

Here, we have $\mathcal{T}_{\mathcal{A}_{\text{ind}}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}} + O(mq_G^2 + mq_H^2 + mq_H q_D)$.

If the underlying rPKE scheme P is unique randomness recoverable (Definition 8) with the recover algorithm Rec , we can prove the following theorem. This theorem shows that, in the QROM, the IND-CCA security of $\text{KEM}_m^\perp$ can be reduced to the OW-CPA security of P without the square-root advantage loss.

Theorem 10 (OW-CPA of $P \xrightarrow{\text{QROM}} \text{IND-CCA of } \text{KEM}_m^\perp$). *Let rPKE scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$ be unique randomness recoverable with the recover algorithm Rec . Suppose that P is δ_{wc} -worst-correct and has message (resp. randomness) space $\mathcal{M}(= \{0, 1\}^m)$ (resp. $\mathcal{R}$). Let $\mathcal{A}$ be an IND-CCA adversary against $\text{KEM}_m^\perp = \text{FO}_m^\perp[P, H, G]$, making q_D classical queries to the decapsulation oracle and making q_G (resp. q_H) quantum queries to the random oracle G (resp. H). Then, we can construct a OW-CPA adversary $\mathcal{A}_{\text{ow}}$ against P such that*

$$\begin{aligned} \text{Adv}_{\text{KEM}_m^\perp}^{\text{IND-CCA}}(\mathcal{A}) \leq & 110 \cdot \text{Adv}_P^{\text{OW-CPA}}(\mathcal{A}_{\text{ow}}) + 8(q_H + 1) \cdot \sqrt{\delta_{wc}} \\ & + (64q_H + 200) \cdot \delta_{wc} + 40q_D \cdot |\mathcal{R}|^{-1/2}. \end{aligned}$$

Here, we have $\mathcal{T}_{\mathcal{A}_{\text{ow}}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}} + O(mq_G + mq_H) \cdot (\mathcal{T}_{\text{Enc}} + \mathcal{T}_{\text{Rec}}) + O(mq_G^2 + mq_H^2 + mq_H q_D)$.

Proof. The proof of this theorem is identical to that of [13, Corollary 2] based on the unique-randomness-recoverability, except for the following two differences:

1. The MRE-O2H (Theorem 14) used in [13, Corollary 2] should be replaced by our DSEAM-O2H (Theorem 4).
2. The random oracles should be simulated by $2q$ -wise independent functions before applying the O2H theorem. This is similar to the proof of Theorem 8, where the distribution $\mathfrak{D}$ (Fig. 13) initially samples G as a $2(q_G + q_H)$ -wise independent function. We adopt this approach because the one-wayness attacker designed in DSEAM-O2H requires repeatedly running the distinguisher, possibly for an exponential number of repetitions. Therefore, if we convert the random oracles into $2q$ -wise independent functions only after applying DSEAM-O2H, we need to choose an exponentially large q to ensure a perfect simulation of the random oracle, since the number of random oracle queries at this point may be exponential.

Despite these two differences, the proof of [13, Corollary 2] can still be transferred in a straightforward manner. Hence, we omit the detailed proof. $\square$

6.2 FO-like transformation $\text{FO}^\perp$

Due to space restrictions, the full proofs are given in Supplementary Material F.

Acknowledgments. The core ideas for the two new O2H theorems (Theorems 2 and 4) were proposed by the authors, and GPT-5.6 Sol Ultra and GPT-6 Astra Ultra were then used to help refining the detailed proof strategies. For Lemmas 2 and 7, these models generated proof drafts, and then the authors checked and

revised these drafts before including them in the manuscript. The rest of the manuscript was written by the authors, with GPT-6 Astra Ultra used to check the reasoning, polish the language, and correct typos. The authors verified the consistency and correctness of all content.

References

1. Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. In: *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference*, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II. pp. 269–295. Springer (2019). https://doi.org/10.1007/978-3-030-26951-7_10
2. Barbosa, M., Barthe, G., Doczkal, C., Don, J., Fehr, S., Grégoire, B., Huang, Y.H., Hülsing, A., Lee, Y., Wu, X.: Fixing and mechanizing the security proof of Fiat-Shamir with aborts and Dilithium. In: *Advances in Cryptology – CRYPTO 2023. Lecture Notes in Computer Science*, vol. 14085, pp. 358–389. Springer (2023)
3. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security*, Fairfax, Virginia, USA, November 3-5, 1993. pp. 62–73. ACM (1993). <https://doi.org/10.1145/168588.168596>
4. Bindel, N., Hamburg, M., Hövelmanns, K., Hülsing, A., Persichetti, E.: Tighter proofs of CCA security in the quantum random oracle model. In: *Theory of Cryptography Conference*. pp. 61–90. Springer (2019). https://doi.org/10.1007/978-3-030-36033-7_3
5. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security*, Seoul, South Korea, December 4-8, 2011. Proceedings. pp. 41–69. Springer (2011). https://doi.org/10.1007/978-3-642-25385-0_3
6. Brassard, G., Høyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. In: Samuel J. Lomonaco, J. (ed.) *Quantum Computation and Quantum Information*, Contemporary Mathematics, vol. 305, pp. 53–74. American Mathematical Society (2002). <https://doi.org/10.1090/conm/305/05215>
7. Chen, J., Chen, R., Wang, Y., Jiang, H., Peng, C., Huang, X., He, D., Chen, X.: Tighter proofs for PKE-to-KEM transformations under average-case decryption error and without γ -spread. *Cryptology ePrint Archive*, Paper 2026/468 (2026), <https://eprint.iacr.org/2026/468>
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 (2003). <https://doi.org/10.1137/S0097539702403773>
9. Dent, A.W.: A designer’s guide to kems. In: *IMA International Conference on Cryptography and Coding*. pp. 133–151. Springer (2003). https://doi.org/10.1007/978-3-540-40974-8_12
10. Don, J., Fehr, S., Majenz, C., Schaffner, C.: Online-extractability in the quantum random-oracle model. In: *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III. pp. 677–706. Springer (2022). https://doi.org/10.1007/978-3-031-07082-2_24

11. Duman, J., Hövelmanns, K., Kiltz, E., Lyubashevsky, V., Seiler, G., Unruh, D.: A thorough treatment of highly-efficient NTRU instantiations. In: Public-Key Cryptography - PKC 2023 - 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, Atlanta, GA, USA, May 7-10, 2023, Proceedings, Part I. pp. 65–94. Springer (2023). https://doi.org/10.1007/978-3-031-31368-4_3
12. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. *J. Cryptol.* **26**(1), 80–101 (2013). <https://doi.org/10.1007/s00145-011-9114-1>
13. Ge, J., Liao, H., Xue, R.: Measure-rewind-extract: Tighter proofs of one-way to hiding and CCA security in the quantum random oracle model. In: Chung, K., Sasaki, Y. (eds.) *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security*, Kolkata, India, December 9-13, 2024, Proceedings, Part IV. *Lecture Notes in Computer Science*, vol. 15487, pp. 3–34. Springer (2024). https://doi.org/10.1007/978-981-96-0894-2_1, https://doi.org/10.1007/978-981-96-0894-2_1
14. Ge, J., Shan, T., Xue, R.: Tighter qcca-secure key encapsulation mechanism with explicit rejection in the quantum random oracle model. In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference*, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part V. pp. 292–324. Springer (2023). https://doi.org/10.1007/978-3-031-38554-4_10
15. Ge, J., Yang, K., Yu, Y., Yu, Y.: Fujisaki-okamoto transformation under average-case decryption error: Tighter and more general proofs with applications to PQC. *IACR Cryptology ePrint Archive* p. 1641 (2025), report 2025/1641
16. Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the fujisaki-okamoto transformation. In: *Theory of Cryptography Conference*. pp. 341–371. Springer (2017). https://doi.org/10.1007/978-3-319-70500-2_12
17. Hövelmanns, K., Hülsing, A., Majenz, C.: Failing gracefully: Decryption failures and the fujisaki-okamoto transform. In: *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security*, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part IV. pp. 414–443. Springer (2022). https://doi.org/10.1007/978-3-031-22972-5_15
18. Jiang, H., Zhang, Z., Chen, L., Wang, H., Ma, Z.: Ind-cca-secure key encapsulation mechanism in the quantum random oracle model, revisited. In: *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference*, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III. pp. 96–125. Springer (2018). https://doi.org/10.1007/978-3-319-96878-0_4
19. Jiang, H., Zhang, Z., Ma, Z.: Key encapsulation mechanism with explicit rejection in the quantum random oracle model. In: *Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography*, Beijing, China, April 14-17, 2019, Proceedings, Part II. pp. 618–645. Springer (2019). https://doi.org/10.1007/978-3-030-17259-6_21
20. Klooß, M.: On expected polynomial runtime in cryptography. In: Nissim, K., Waters, B. (eds.) *Theory of Cryptography*. *Lecture Notes in Computer Science*, vol. 13042, pp. 558–590. Springer (2021). https://doi.org/10.1007/978-3-030-90459-3_19, https://doi.org/10.1007/978-3-030-90459-3_19
21. Kuchta, V., Sakzad, A., Stehlé, D., Steinfeld, R., Sun, S.: Measure-rewind-measure: Tighter quantum random oracle model proofs for one-way to hiding and CCA security. In: *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International*

- Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part III. pp. 703–728. Springer (2020). https://doi.org/10.1007/978-3-030-45727-3_24
22. Maram, V., Xagawa, K.: Post-quantum anonymity of Kyber. In: Boldyreva, A., Kolesnikov, V. (eds.) Public-Key Cryptography – PKC 2023. Lecture Notes in Computer Science, vol. 13940, pp. 3–35. Springer (2023). https://doi.org/10.1007/978-3-031-31368-4_1
 23. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information (10th Anniversary edition). Cambridge University Press (2016)
 24. NIST: National institute for standards and technology. post quantum crypto project. <https://csrc.nist.gov/projects/post-quantum-cryptography> (2017)
 25. NTRU: A submission to the nist post-quantum standardization effort. <https://ntru.org/> (2018)
 26. Saito, T., Xagawa, K., Yamakawa, T.: Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In: Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III. pp. 520–551. Springer (2018). https://doi.org/10.1007/978-3-319-78372-7_17
 27. Unruh, D.: Revocable quantum timed-release encryption. J. ACM **62**(6), 49:1–49:76 (2015). <https://doi.org/10.1145/2817206>
 28. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings. pp. 758–775. Springer (2012). https://doi.org/10.1007/978-3-642-32009-5_44
 29. Zhandry, M.: How to record quantum queries, and applications to quantum indistinguishability. In: Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II. pp. 239–268. Springer (2019). https://doi.org/10.1007/978-3-030-26951-7_9

Supplementary Material

A Further Related Work

As discussed in Section 1.1, our SSEAM-O2H and DSEAM-O2H involve two running time trade-offs: the one-wayness attacker $\mathcal{B}_{\text{ow}}$ has a relatively large running time overhead, and we only provide an expected running time bound. Thus, a natural question is whether the distribution $\mathfrak{D}$ in Table 3 can be modified to avoid branches with exponentially large iterations, thereby reducing this overhead and yielding a nontrivial worst case running time bound. In addition, as with DS-O2H, our DSEAM-O2H requires $|S| = 1$, which limits its applicability. For example, in the case discussed in Footnote 12, DSEAM-O2H cannot be used to avoid the $\sqrt{q}$ loss. Hence, another natural question is whether this restriction can be removed to obtain a more general tight O2H theorem.

Regarding applications, this work focuses only on FO-like transformations based on worst-case decryption error. In contrast, recent works consider the weaker average-case decryption error and propose new FO-like transformations with IND-CCA security proofs in the QROM [11, 15, 7]. It is therefore natural to ask whether our SSEAM-O2H and DSEAM-O2H can yield tighter proofs for these transformations.

B Quantum Background

A quantum system (register) Q is a complex Hilbert space $\mathcal{H}_Q$ with an inner product $\langle \cdot | \cdot \rangle$, and notation like $|\cdot\rangle$ or $\langle \cdot |$ is called the Dirac notation. We denote $\mathcal{H}_Q = \mathbb{C}[X]$ if Q is defined over a finite set X . The orthonormal basis of $\mathbb{C}[X]$ is $\{|x\rangle\}_{x \in X}$, where the basis state $|x\rangle$ is labeled by the element x of X . We also refer to $\{|x\rangle\}_{x \in X}$ as the computational basis. The norm of a state $|\psi\rangle$ is defined as $\| |\psi\rangle \| := \sqrt{\langle \psi | \psi \rangle}$, and we say $|\psi\rangle$ is a unit vector if $\| |\psi\rangle \| = 1$.

Composite quantum system. Given quantum systems Q_1 and Q_2 , we call tensor product $Q_1 \otimes Q_2$ is the composite quantum system and the product state is $|\psi_1\rangle \otimes |\psi_2\rangle \in Q_1 \otimes Q_2$, where $|\psi_1\rangle \in Q_1$, $|\psi_2\rangle \in Q_2$. We sometimes also abbreviate $|\psi_1\rangle \otimes |\psi_2\rangle$ into $|\psi_1\rangle |\psi_2\rangle$ for simplicity. If the composite quantum system $Q_1 \otimes Q_2$ is in the state $|\psi\rangle$, we say that the systems Q_1 and Q_2 are entangled if $|\psi\rangle$ cannot be written as a product state $|\psi_1\rangle \otimes |\psi_2\rangle$ (here $|\psi_1\rangle \in Q_1$, $|\psi_2\rangle \in Q_2$). Otherwise, we say that the systems Q_1 and Q_2 are un-entangled.

A single qubit is a quantum system defined over $\{0, 1\}$. A single qubit in superposition is a linear combination vector $|b\rangle = \alpha|0\rangle + \beta|1\rangle$ of two computational basis states $|0\rangle$ and $|1\rangle$ with $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$, α, β are the probability amplitudes of $|b\rangle$. An n -qubit system is $Q^{\otimes n}$ where Q is single qubit system.

Evolution of quantum systems. A pure state $|\psi\rangle$ can be manipulated by performing a unitary operation U , and the resulting state can be denoted as $|\psi'\rangle = U|\psi\rangle$. For any unitary operation U , we have $UU^\dagger = I$, where $U^\dagger$ is the

Hermitian transpose of U and I is the identity operator.

Projector on the quantum system. We introduce a special operation called projector. For the state $|\psi\rangle$ of a quantum system defined over finite set X , a projector M_y ($y \in X$) applies the operation $|y\rangle\langle y|$ to $|\psi\rangle$ to get the new state $|y\rangle\langle y|\psi\rangle$. M_y can also be generalized to a new projector M_S ($S \subseteq X$) which applies the operation $\sum_{y \in S} |y\rangle\langle y|$. We stress that any projector M is Hermitian (i.e., we have $M^\dagger = M$) and idempotent (i.e., we have $M^2 = M$).

Basic measurement. The state $|\psi\rangle$ in a quantum system can be measured in the computational basis. For example, suppose $|\psi\rangle = \sum_{x \in X} \alpha_x |x\rangle$ ($\sum_{x \in X} |\alpha_x|^2 = 1$) with computational basis $\{|x\rangle\}_{x \in X}$, if we measure $|\psi\rangle$ in basis $\{|x\rangle\}_{x \in X}$, we obtain the measurement result x with probability $|\langle x|\psi\rangle|^2 = |\alpha_x|^2$. Given that result x obtained, the state $|\psi\rangle$ collapses to the state $|x\rangle$. Moreover, we explain an important special class of measurements known as projective measurement. Indeed, a projective measurement $\mathbb{M}$ is defined by a set of projectors $M_1, \dots, M_n$ where M_i are mutually orthogonal and $\sum_{i=1}^n M_i = I$. Upon measuring the state $|\psi\rangle$, the probability of obtaining measurement result i ($i \in \{1, \dots, n\}$) is $\langle \psi | M_i | \psi \rangle$ ($= \|M_i |\psi\rangle\|^2$). Given that result i obtained, the state $|\psi\rangle$ collapses to the state $M_i |\psi\rangle / \sqrt{\langle \psi | M_i | \psi \rangle}$.

Quantum oracle algorithm. A quantum oracle algorithm $\mathcal{A}^H(z)$ has a classical input z and quantum oracle access to H . It can perform a combination of classical and quantum operations. In this paper, without loss of generality, we default that $\mathcal{A}$'s final output is a single bit $b \in \{0, 1\}$.

Unitary quantum oracle algorithm. We say that $\mathcal{A}^H(z)$ is a unitary quantum oracle algorithm if its entire execution can be described as:

$$\mathbb{M}_{\mathcal{A}} U_q O_H U_{q-1} O_H \dots U_2 O_H U_1 O_H |\psi_z\rangle.$$

Here $|\psi_z\rangle$ is an initial pure state that may depend on input z , $U_1, \dots, U_q$ are the fixed unitary operations applied between oracle queries, O_H is the unitary operation used to implement the oracle H . $\mathbb{M}_{\mathcal{A}} := \{M_0^{\mathcal{A}}, M_1^{\mathcal{A}}\}$ is the final binary projective measurement performed by $\mathcal{A}$. The measurement result of $\mathbb{M}_{\mathcal{A}}$ (0 or 1) is the final output of $\mathcal{A}$. Assume that $\mathcal{A}$ works on a quantum register with a qubits. Then, we denote the unitary operation preparing the initial state $|\psi_z\rangle$ by U_z , where U_z may depend on the input z , and we have $U_z |0^a\rangle = |\psi_z\rangle$.

Next, following [1], we introduce a well-known fact about the quantum oracle algorithm.

Fact 1 *Any quantum oracle algorithm can be transformed into a unitary quantum oracle algorithm with constant factor computational overhead and the same query times.*

The above fact implies that, without loss of generality, we can directly assume the quantum oracle algorithms to be unitary.

B.1 Quantum Random Oracle Model

The random oracle model (ROM) is an ideal model in which a uniformly random function H is selected, and all parties have access to H . In real schemes, the random oracle is implemented using a suitable hash function. In the quantum setting, the ROM should be lifted into the quantum random oracle model (QROM) [5], where all parties have quantum access to the random oracle. In the QROM, we take the random oracle H as a unitary operation $O_H : |x, y\rangle \mapsto |x, y \oplus H(x)\rangle$.

Definition 1 (Semi-Classical Oracle [1]). *For a subset $S \subseteq \mathcal{X}$, the indicator function 1_S from $\mathcal{X}$ to $\{0, 1\}$ equals 1 iff its input $x \in S$. The semi-classical oracle, $\mathcal{O}_S^{SC}$, is a quantum accessible oracle that performs the following two operations on its query state $\sum_{x \in \mathcal{X}} \alpha_x |x\rangle$:*

1. Initialize a single qubit register B with the state $|0\rangle_B$.
2. Transform $\sum_{x \in \mathcal{X}} \alpha_x |x\rangle |0\rangle_B$ into $\sum_{x \in \mathcal{X}} \alpha_x |x\rangle |1_S(x)\rangle_B$ and then measure B .

During the execution of quantum oracle algorithm $\mathcal{A}^{\mathcal{O}_S^{SC}}$, let Find be the classical event that the measurement of $\mathcal{O}_S^{SC}$ (on B) ever has outcome 1.

Theorem 11 (Semi-Classical O2H [1, Theorem 1]). *Let $G, H : X \rightarrow Y$ be random functions and $S \subseteq X$ be a random set. Let $z \in Z$ be a random bitstring. The tuple (G, H, S, z) may have arbitrary joint distribution $\mathfrak{D}$ and satisfies that $\forall x \notin S, G(x) = H(x)$. Let $G \setminus S$ be an oracle that first queries $\mathcal{O}_S^{SC}$ on the input of G and then queries G . Let $\mathcal{A}$ be a q -query quantum oracle algorithm. Define*

$$\begin{aligned} P_{\text{left}} &:= \Pr [b = 1 : b \leftarrow \mathcal{A}^H(z), (G, H, S, z) \leftarrow \mathfrak{D}], \\ P_{\text{right}} &:= \Pr [b = 1 : b \leftarrow \mathcal{A}^G(z), (G, H, S, z) \leftarrow \mathfrak{D}], \\ P_{\text{find}} &:= \Pr [\text{Find} : \mathcal{A}^{G \setminus S}(z), (G, H, S, z) \leftarrow \mathfrak{D}]. \end{aligned}$$

Then we have $P_{\text{find}} = \Pr [\text{Find} : \mathcal{A}^{H \setminus S}(z), (G, H, S, z) \leftarrow \mathfrak{D}]$ and

$$|P_{\text{left}} - P_{\text{right}}| \leq 2\sqrt{(q+1) \cdot P_{\text{find}}} \text{ and } \left| \sqrt{P_{\text{left}}} - \sqrt{P_{\text{right}}} \right| \leq 2\sqrt{(q+1) \cdot P_{\text{find}}}.$$

Remark 2. There are several other definitions of P_{right} in [1, Theorem 1]. In this paper, we only need the above definition of P_{right} .

Theorem 12 (Search in Semi-Classical Oracle [1, Theorem 2]). *Let $S \subseteq \mathcal{X}$ be random and z be a random bitstring. (S, z) may have an arbitrary joint distribution $\mathfrak{D}$. Let $\mathcal{A}$ be any quantum oracle algorithm making at most q queries to a semi-classical oracle with domain $\mathcal{X}$.*

Let $\mathcal{B}$ be an algorithm that on input z , chooses $i \leftarrow_{\$} [q]$; runs $\mathcal{A}^{\mathcal{O}_S^{SC}}(z)$ until (just before) the i -th query, measures the input register and outputs the measurement outcome x . Then,

$$\Pr [\text{Find} : \mathcal{A}^{\mathcal{O}_S^{SC}}(z), (S, z) \leftarrow \mathfrak{D}] \leq 4q \cdot \Pr [x \in S : x \leftarrow \mathcal{B}(z), (S, z) \leftarrow \mathfrak{D}].$$

Theorem 13 (Double-Sided O2H [4, Lemma 5]). Let $G, H : X \rightarrow Y$ be random functions and $S \subseteq X$ be a random set. Let $z \in Z$ be a random bitstring. The tuple (G, H, S, z) may have arbitrary joint distribution $\mathfrak{D}$ and satisfies that $\forall x \notin S, G(x) = H(x)$. Let $f : X \rightarrow \{0, 1\}^m$ be a function such that $f(S) = \{w^*\}$ for a single $w^* \in \{0, 1\}^m$. Let $\mathcal{A}$ be a q -query quantum oracle algorithm. Define

$$P_{\text{left}} := \Pr_{(G, H, S, z) \leftarrow \mathfrak{D}} [b = 1 : b \leftarrow \mathcal{A}^H(z)], P_{\text{right}} := \Pr_{(G, H, S, z) \leftarrow \mathfrak{D}} [b = 1 : b \leftarrow \mathcal{A}^G(z)].$$

Then, we can construct an algorithm $\mathcal{B}^{G, H}(z)$, which makes at most q queries to G and H respectively and

$$|P_{\text{left}} - P_{\text{right}}| \leq 2\sqrt{\text{Adv}(\mathcal{B})} \text{ and } \left| \sqrt{P_{\text{left}}} - \sqrt{P_{\text{right}}} \right| \leq 2\sqrt{\text{Adv}(\mathcal{B})}.$$

Here $\text{Adv}(\mathcal{B}) := \Pr[w = w^* : w \leftarrow \mathcal{B}^{G, H}(z), (G, H, S, z) \leftarrow \mathfrak{D}]$. The running time of $\mathcal{B}^{G, H}(z)$ is $\mathcal{T}_{\mathcal{B}} \approx \mathcal{T}_{\mathcal{A}}$.

Theorem 14 (MRE-O2H [13, Theorem 4]). Let $G, H : X \rightarrow Y$ be random functions, $S \subseteq X$ be a random set and $z \in Z$ be a random bitstring. The tuple (G, H, S, z) may have arbitrary joint distribution $\mathfrak{D}$ and satisfies that $\forall x \notin S, G(x) = H(x)$. Let 1_S denote the indicator function of the set S , that is, $1_S(x) = 1$ if $x \in S$ and 0 otherwise. Let $\mathcal{A}$ be a q -query quantum oracle algorithm. Define

$$P_{\text{left}} := \Pr_{(G, H, S, z) \leftarrow \mathfrak{D}} [b = 1 : b \leftarrow \mathcal{A}^H(z)], P_{\text{right}} := \Pr_{(G, H, S, z) \leftarrow \mathfrak{D}} [b = 1 : b \leftarrow \mathcal{A}^G(z)].$$

Then, we can construct an algorithm $\mathcal{B}^{G, H, 1_S}(z)$, which makes at most $3q$ queries to G , H , and 1_S , respectively, and satisfies

$$|P_{\text{left}} - P_{\text{right}}| \leq 4\sqrt{q} \cdot \text{Adv}(\mathcal{B}).$$

Here $\text{Adv}(\mathcal{B}) := \Pr[x \in S : x \leftarrow \mathcal{B}^{G, H, 1_S}(z), (G, H, S, z) \leftarrow \mathfrak{D}]$. The running time of $\mathcal{B}^{G, H, 1_S}(z)$ is $\mathcal{T}_{\mathcal{B}} \lesssim 3 \cdot \mathcal{T}_{\mathcal{A}}$.

C Cryptographic Primitives and Security Definitions

Definition 2 (Public key encryption). A public key encryption (PKE) scheme $\mathsf{P} = (\text{Gen}, \text{Enc}, \text{Dec})$ consists of three polynomial time algorithms (in the security parameter λ) with a finite message space $\mathcal{M}$ such that

1. **Gen**, the key generation algorithm, is a probabilistic algorithm that on input 1^λ outputs a public/secret key pair (pk, sk) .
2. **Enc**, the encryption algorithm, on input pk and a message $m \in \mathcal{M}$, it chooses $r \xleftarrow{\$} \mathcal{R}$ ($\mathcal{R}$ is the randomness space), computes $\text{Enc}_{pk}(m; r) \in \mathcal{C}$ ($\mathcal{C}$ is the ciphertext space) and outputs ciphertext $c := \text{Enc}_{pk}(m; r)$. If **Enc** does not use randomness r to compute c , **Enc** is a deterministic algorithm and outputs $c := \text{Enc}_{pk}(m)$.

3. **Dec**, the decryption algorithm, is a deterministic algorithm that on input ciphertext $c \in \mathcal{C}$ outputs a message $m := \text{Dec}_{sk}(c)$, or a special symbol $\perp \notin \mathcal{M}$ to indicate that c is not a valid ciphertext.

We say $\mathbf{P}$ is a randomized PKE (rPKE) scheme if **Enc** uses randomness r to compute ciphertext c . Otherwise, we say $\mathbf{P}$ is a deterministic PKE (dPKE) scheme.

Definition 3 (Decryption error [11]). We say an rPKE scheme $\mathbf{P} = (\text{Gen}, \text{Enc}, \text{Dec})$ with message/randomness space $\mathcal{M}/\mathcal{R}$ is δ_{wc} -worst-correct or has worst-case decryption error δ_{wc} if

$$\mathbb{E} \left[\max_{m \in \mathcal{M}} \Pr [\text{Dec}_{sk}(c) \neq m : c = \text{Enc}_{pk}(m; r), r \leftarrow_{\$} \mathcal{R}] \right] \leq \delta_{wc}.$$

where the expectation is taken over $(pk, sk) \leftarrow \text{Gen}$ and the choice of the random oracles involved (if any). Similarly, we say an rPKE or dPKE scheme $\mathbf{P} = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M}$ is δ_{ac} -average-correct or has average-case decryption error δ_{ac} if

$$\Pr [\text{Dec}_{sk}(c) \neq m : c = \text{Enc}_{pk}(m), (pk, sk) \leftarrow \text{Gen}, m \leftarrow_{\$} \mathcal{M}] \leq \delta_{ac}.$$

Definition 4 (Correctness (COR) game [16]). For an rPKE or dPKE scheme $\mathbf{P} = (\text{Gen}, \text{Enc}, \text{Dec})$, we define the correctness (COR) game of $\mathbf{P}$ with the adversary $\mathcal{A}$ in Fig. 3. We then define the advantage of $\mathcal{A}$ as $\text{Adv}_{\mathbf{P}}^{\text{COR}}(\mathcal{A}) := \Pr[1 \leftarrow \mathbf{G}_{\mathcal{A}, \mathbf{P}}^{\text{COR}}]$. Notice that the adversary $\mathcal{A}$ receives both pk and sk .

$\mathbf{G}_{\mathcal{A}, \mathbf{P}}^{\text{COR}}$
1 : $(pk, sk) \leftarrow \text{Gen}$
2 : $m \leftarrow \mathcal{A}(pk, sk)$
3 : $c := \text{Enc}_{pk}(m)$
4 : return $\mathbb{I}[\text{Dec}_{sk}(c) \neq m]$

Fig. 3: The correctness game of $\mathbf{P}$ with the adversary $\mathcal{A}$.

Definition 5 (η -injective [21]). We say a dPKE scheme $\mathbf{P} = (\text{Gen}, \text{Enc}, \text{Dec})$ is η -injective if $\Pr[\text{Enc}_{pk}(\cdot)$ is not injective : $(pk, sk) \leftarrow \text{Gen}, H \leftarrow_{\$} \Omega_{X \rightarrow Y}] \leq \eta$. Here the $H \leftarrow_{\$} \Omega_{X \rightarrow Y}$ represents the random oracle that may be used by $\mathbf{P}$.

Definition 6 (Weakly γ -spread [10]). We say a randomized PKE scheme $\mathbf{P} = (\text{Gen}, \text{Enc}, \text{Dec})$ with message/ciphertext space $\mathcal{M}/\mathcal{C}$ is weakly γ -spread if

$$\mathbb{E}_{(pk, sk) \leftarrow \text{Gen}} \left[\max_{m \in \mathcal{M}, c \in \mathcal{C}} \Pr[c = \text{Enc}_{pk}(m)] \right] \leq 2^{-\gamma},$$

where the probability is over the randomness of the encryption.

Definition 7 (Find failing ciphertext (FFC) game [4]). For a dPKE scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$, we define the find failing ciphertexts (FFC) game with the adversary $\mathcal{A}$ in Fig. 4, and define its advantage as $\text{Adv}_P^{\text{FFC}}(\mathcal{A}) := \Pr[1 \leftarrow \mathbf{G}_{\mathcal{A},P}^{\text{FFC}}]$.

$\mathbf{G}_{\mathcal{A},P}^{\text{FFC}}$
1 : $(pk, sk) \leftarrow \text{Gen}$
2 : $L \leftarrow \mathcal{A}(pk)$
3 : return $\llbracket \exists(m, c) \in \mathcal{M} \times L : \text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) \neq m \rrbracket$

Fig. 4: The FFC game of P with the adversary $\mathcal{A}$.

Definition 8 (Unique randomness recoverable [13]). We say a randomized PKE scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$ with message/randomness space $\mathcal{M}/\mathcal{R}$ is unique randomness recoverable if there exists a deterministic (recover) algorithm Rec such that for all $m \in \mathcal{M}$ and $r \in \mathcal{R}$,

$$\Pr[\text{Rec}(pk, m, \text{Enc}_{pk}(m; r)) \neq r] = 0,$$

where the probability is taken over $(pk, sk) \leftarrow \text{Gen}$. For the pair (m, c) , if $\nexists r \in \mathcal{R}$ such that $c = \text{Enc}_{pk}(m; r)$, $\text{Rec}(pk, m, c)$ returns the symbol $\perp \notin \mathcal{R}$.

Remark 3. Since Rec is a deterministic algorithm, a unique randomness recoverable PKE scheme must satisfy that, for any $(m, r) \in \mathcal{M} \times \mathcal{R}$, there does not exist $r' \neq r$ such that $\text{Enc}_{pk}(m; r) = \text{Enc}_{pk}(m; r')$. This is why we call this property as unique randomness recoverable.

Definition 9 (Security notions for PKE schemes). For any polynomial time quantum adversary $\mathcal{A}$, we define its OW-CPA and IND-CPA advantage against PKE scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$ as follows:

$$\begin{aligned} \text{Adv}_P^{\text{OW-CPA}}(\mathcal{A}) &:= \Pr[1 \leftarrow \mathbf{G}_{\mathcal{A},P}^{\text{OW-CPA}}], \\ \text{Adv}_P^{\text{IND-CPA}}(\mathcal{A}) &:= \left| \Pr[1 \leftarrow \mathbf{G}_{\mathcal{A},P}^{\text{IND-CPA}}] - \frac{1}{2} \right|. \end{aligned}$$

Here games $\mathbf{G}_{\mathcal{A},P}^{\text{OW-CPA}}$ and $\mathbf{G}_{\mathcal{A},P}^{\text{IND-CPA}}$ are shown in Fig. 5. We say scheme P is OW-CPA-secure/IND-CPA-secure, if for any polynomial time quantum adversary $\mathcal{A}$, the $\text{Adv}_P^{\text{OW-CPA}}(\mathcal{A})/\text{Adv}_P^{\text{IND-CPA}}(\mathcal{A})$ is negligible.

Definition 10 (Key encapsulation mechanism). A key encapsulation mechanism $\text{KEM} = (\text{Gen}, \text{Enca}, \text{Deca})$ consists of three polynomial time algorithms with the key space $\mathcal{K}$ and the ciphertext space $\mathcal{C}$ such that

$\mathbf{G}_{\mathcal{A},\mathcal{P}}^{\text{OW-CPA}}$	$\mathbf{G}_{\mathcal{A},\mathcal{P}}^{\text{IND-CPA}}$
1 : $(pk, sk) \leftarrow \text{Gen}$	1 : $(pk, sk) \leftarrow \text{Gen}$
2 : $m^* \xleftarrow{\$} \mathcal{M}$	2 : $b \xleftarrow{\$} \{0, 1\}$
3 : $c^* := \text{Enc}_{pk}(m^*)$	3 : $(m_0^*, m_1^*) \leftarrow \mathcal{A}(pk)$
4 : $m' \leftarrow \mathcal{A}(pk, c^*)$	4 : $c^* := \text{Enc}_{pk}(m_b^*)$
5 : return $\llbracket m' = m^* \rrbracket$	5 : $b' \leftarrow \mathcal{A}(pk, c^*)$
	6 : return $\llbracket b' = b \rrbracket$

Fig. 5: Games $\mathbf{G}_{\mathcal{A},\mathcal{P}}^{\text{OW-CPA}}$ and $\mathbf{G}_{\mathcal{A},\mathcal{P}}^{\text{IND-CPA}}$.

1. **Gen**, the key generation algorithm, is a probabilistic algorithm that on input 1^λ outputs a public/secret key pair (pk, sk) .
2. **Enca**, the encapsulation algorithm, is a probabilistic algorithm that on input pk outputs a key $k \in \mathcal{K}$ and a ciphertext $c \in \mathcal{C}$.
3. **Deca**, the decapsulation algorithm, is a deterministic algorithm that on input ciphertext c outputs a key $k := \text{Deca}(sk, c)$ or a special symbol $\perp \notin \mathcal{K}$ to indicate that c is not a valid ciphertext.

$\mathbf{G}_{\mathcal{A},\text{KEM}}^{\text{IND-CPA}}$	$\mathbf{G}_{\mathcal{A},\text{KEM}}^{\text{IND-CCA}}$	$\text{oDeca}(c)$
1 : $(pk, sk) \leftarrow \text{Gen}$	1 : $(pk, sk) \leftarrow \text{Gen}$	1 : if $c = c^*$
2 : $b \xleftarrow{\$} \{0, 1\}$	2 : $b \xleftarrow{\$} \{0, 1\}$	2 : return $\perp$
3 : $(k_0, c^*) \leftarrow \text{Enca}(pk)$	3 : $(k_0, c^*) \leftarrow \text{Enca}(pk)$	3 : else return $\text{Deca}(sk, c)$
4 : $k_1 \xleftarrow{\$} \mathcal{K}$	4 : $k_1 \xleftarrow{\$} \mathcal{K}$	
5 : $b' \leftarrow \mathcal{A}(pk, c^*, k_b)$	5 : $b' \leftarrow \mathcal{A}^{\text{oDeca}}(pk, c^*, k_b)$	
6 : return $\llbracket b' = b \rrbracket$	6 : return $\llbracket b' = b \rrbracket$	

Fig. 6: Games $\mathbf{G}_{\mathcal{A},\text{KEM}}^{\text{IND-CPA}}$ and $\mathbf{G}_{\mathcal{A},\text{KEM}}^{\text{IND-CCA}}$.

Definition 11 (Security notions for KEM schemes). For any polynomial time quantum adversary $\mathcal{A}$, we define its IND-CPA and IND-CCA advantage against KEM scheme $\text{KEM} = (\text{Gen}, \text{Enca}, \text{Deca})$ as follows:

$$\text{Adv}_{\text{KEM}}^{\text{IND-CPA}}(\mathcal{A}) := \left| \Pr [1 \leftarrow \mathbf{G}_{\mathcal{A},\text{KEM}}^{\text{IND-CPA}}] - \frac{1}{2} \right|,$$

$$\text{Adv}_{\text{KEM}}^{\text{IND-CCA}}(\mathcal{A}) := \left| \Pr [1 \leftarrow \mathbf{G}_{\mathcal{A},\text{KEM}}^{\text{IND-CCA}}] - \frac{1}{2} \right|.$$

Here games $\mathbf{G}_{\mathcal{A}, \text{KEM}}^{\text{IND-CPA}}$ and $\mathbf{G}_{\mathcal{A}, \text{KEM}}^{\text{IND-CCA}}$ are shown in Fig. 6. We say scheme KEM is IND-CPA-secure/IND-CCA-secure, if for any polynomial time quantum adversary $\mathcal{A}$, the advantage $\text{Adv}_{\text{KEM}}^{\text{IND-CPA}}(\mathcal{A})/\text{Adv}_{\text{KEM}}^{\text{IND-CCA}}(\mathcal{A})$ is negligible.

We also define OW-CPA/IND-CPA security of PKE schemes and IND-CPA/IND-CCA security of KEM schemes in the QROM, where the adversary $\mathcal{A}$ can make quantum queries to random oracles.

D Some Missing Proofs

D.1 Proof of Lemma 1

Proof. We first explain the definition of Am . The operator $2|0\rangle\langle 0|_{\mathbf{B}} - I_{\mathbf{B}}$ used by Am acts on the register $\mathbf{B}$, and it leaves the state $|b\rangle$ unchanged if $b = 0$, while mapping it to $-|b\rangle$ if $b \in \{1, \dots, q\}$. The operator $2|0^a\rangle\langle 0^a|_{\mathbf{BT}} - I_{\mathbf{BT}}$ used by Am is similar, except that it focuses on the whole register and maps $|w, b, t\rangle$ into $-|w, b, t\rangle$ for any $(w, b, t) \neq (0^a, 0, 0^m)$. Now, for any angle η , we can compute

$$\begin{aligned} & Am(\cos(\eta) \cdot |\psi_{bad}\rangle + \sin(\eta) \cdot |\psi_{good}\rangle) \\ \stackrel{(a)}{=} & \left[U_{\mathbf{B}} \circ (2|0^a\rangle\langle 0^a|_{\mathbf{BT}} - I_{\mathbf{BT}}) \circ U_{\mathbf{B}}^\dagger \right] (\cos(\eta) \cdot |\psi_{bad}\rangle - \sin(\eta) \cdot |\psi_{good}\rangle) \\ = & \left[2U_{\mathbf{B}}|0^a\rangle\langle 0^a|_{\mathbf{BT}}(U_{\mathbf{B}}|0^a\rangle\langle 0^a|_{\mathbf{BT}} - I)^\dagger - I \right] (\cos(\eta) \cdot |\psi_{bad}\rangle - \sin(\eta) \cdot |\psi_{good}\rangle). \end{aligned}$$

Here (a) is because $2|0\rangle\langle 0|_{\mathbf{B}} - I_{\mathbf{B}}$ maps $|\psi_{bad}\rangle$ into itself and maps $|\psi_{good}\rangle$ into $-|\psi_{good}\rangle$ ¹⁵. By substituting $U_{\mathbf{B}}|0^a\rangle\langle 0^a|_{\mathbf{BT}}$ with $\cos(\theta) \cdot |\psi_{bad}\rangle\langle \psi_{bad}| + \sin(\theta) \cdot |\psi_{good}\rangle\langle \psi_{good}|$, and using the properties that $\langle \psi_{bad} | \psi_{good} \rangle = 0$ and $\langle \psi_{good} | \psi_{bad} \rangle = 0$, the above equation can be further computed as

$$\begin{aligned} & Am(\cos(\eta) \cdot |\psi_{bad}\rangle + \sin(\eta) \cdot |\psi_{good}\rangle) \\ = & \left[\begin{aligned} & 2\cos^2(\theta)\cos(\eta)\langle \psi_{bad} | \psi_{bad} \rangle \\ & - 2\cos(\theta)\sin(\theta)\sin(\eta)\langle \psi_{good} | \psi_{good} \rangle - \cos(\eta) \end{aligned} \right] \cdot |\psi_{bad}\rangle \\ & + \left[\begin{aligned} & 2\sin(\theta)\cos(\theta)\cos(\eta)\langle \psi_{bad} | \psi_{bad} \rangle \\ & - 2\sin^2(\theta)\sin(\eta)\langle \psi_{good} | \psi_{good} \rangle + \sin(\eta) \end{aligned} \right] \cdot |\psi_{good}\rangle. \end{aligned} \quad (30)$$

Note that the coefficient above contains the terms $\langle \psi_{bad} | \psi_{bad} \rangle$ and $\langle \psi_{good} | \psi_{good} \rangle$. This is because, by the definitions of $|\psi_{bad}\rangle$ and $|\psi_{good}\rangle$ in Eq. (17), their norms are not always fixed.

¹⁵ According to the definitions of $|\psi_{bad}\rangle$ and $|\psi_{good}\rangle$ in Eq. (17), one of these vectors is the zero vector $\mathbf{0}$ in each boundary case. Hence, here we actually use the fact that every linear operator maps $\mathbf{0}$ to itself and that $\mathbf{0} = -\mathbf{0}$.

We first consider the case that $\theta = \pi/2$, which implies $\langle \psi_{bad} | \psi_{bad} \rangle = 0$ and $\langle \psi_{good} | \psi_{good} \rangle = 1$. Thus, Eq. (30) can be simplified as

$$\begin{aligned}
& Am(\cos(\eta) \cdot |\psi_{bad}\rangle + \sin(\eta) \cdot |\psi_{good}\rangle) \\
&= [-2 \cos(\theta) \sin(\theta) \sin(\eta) - \cos(\eta)] \cdot |\psi_{bad}\rangle + [-2 \sin^2(\theta) \sin(\eta) + \sin(\eta)] \cdot |\psi_{good}\rangle \\
&= -\cos(\eta) \cdot |\psi_{bad}\rangle - \sin(\eta) \cdot |\psi_{good}\rangle \\
&= \cos\left(\eta + 2 \cdot \frac{\pi}{2}\right) \cdot |\psi_{bad}\rangle + \sin\left(\eta + 2 \cdot \frac{\pi}{2}\right) \cdot |\psi_{good}\rangle \\
&= \cos(\eta + 2\theta) \cdot |\psi_{bad}\rangle + \sin(\eta + 2\theta) \cdot |\psi_{good}\rangle.
\end{aligned}$$

For the case that $\theta = 0$, which implies $\langle \psi_{bad} | \psi_{bad} \rangle = 1$ and $\langle \psi_{good} | \psi_{good} \rangle = 0$. Thus, Eq. (30) can be simplified as

$$\begin{aligned}
& Am(\cos(\eta) \cdot |\psi_{bad}\rangle + \sin(\eta) \cdot |\psi_{good}\rangle) \\
&= [2 \cos^2(\theta) \cos(\eta) - \cos(\eta)] \cdot |\psi_{bad}\rangle + [2 \sin(\theta) \cos(\theta) \cos(\eta) + \sin(\eta)] \cdot |\psi_{good}\rangle \\
&= \cos(\eta) \cdot |\psi_{bad}\rangle + \sin(\eta) \cdot |\psi_{good}\rangle \\
&= \cos(\eta + 2\theta) \cdot |\psi_{bad}\rangle + \sin(\eta + 2\theta) \cdot |\psi_{good}\rangle.
\end{aligned}$$

As for the case $0 < \theta < \pi/2$, we have $\langle \psi_{bad} | \psi_{bad} \rangle = \langle \psi_{good} | \psi_{good} \rangle = 1$ and thus the Eq. (30) can be further computed as

$$\begin{aligned}
& Am(\cos(\eta) \cdot |\psi_{bad}\rangle + \sin(\eta) \cdot |\psi_{good}\rangle) \\
&= [2 \cos^2(\theta) \cos(\eta) - 2 \cos(\theta) \sin(\theta) \sin(\eta) - \cos(\eta)] \cdot |\psi_{bad}\rangle \\
&\quad + [2 \sin(\theta) \cos(\theta) \cos(\eta) - 2 \sin^2(\theta) \sin(\eta) + \sin(\eta)] \cdot |\psi_{good}\rangle \\
&\stackrel{(a)}{=} \cos(\eta + 2\theta) \cdot |\psi_{bad}\rangle + \sin(\eta + 2\theta) \cdot |\psi_{good}\rangle.
\end{aligned}$$

Here (a) is obtained through a straightforward trigonometric calculation. At this point, the above three equations show that for any angle η , we always have

$$Am(\cos(\eta) \cdot |\psi_{bad}\rangle + \sin(\eta) \cdot |\psi_{good}\rangle) = \cos(\eta + 2\theta) \cdot |\psi_{bad}\rangle + \sin(\eta + 2\theta) \cdot |\psi_{good}\rangle.$$

Since $U_B|0^a\rangle|0, 0^m\rangle_{BT}$ is exactly $\cos(\theta) \cdot |\psi_{bad}\rangle + \sin(\theta) \cdot |\psi_{good}\rangle$ (Eq. (18)), the above equation implies that for any $k \in \mathbb{N}^+$,

$$(Am)^k U_B|0^a\rangle|0, 0^m\rangle_{BT} = \cos((2k+1)\theta) \cdot |\psi_{bad}\rangle + \sin((2k+1)\theta) \cdot |\psi_{good}\rangle.$$

This completes the proof of Lemma 1. $\square$

D.2 Proof of Lemma 2

Proof. If $\sin(\theta) \leq \epsilon$, this lemma holds trivially. As for the case of $\sin(\theta) > \epsilon$, since it implies $\sin(\theta) > 0$ and thus $\theta > 0$, in this proof we can only consider $0 < \theta < \frac{1}{2}$ and $\frac{1}{2} \leq \theta \leq \pi/2$.

If $0 < \theta < \frac{1}{2}$, let $R = 2^k$ be the smallest power of two satisfying $R \geq \frac{1}{2\theta}$. By the minimality of R , we have $\frac{R}{2} < \frac{1}{2\theta}$, and thus

$$\frac{1}{2\theta} \leq R < \frac{1}{\theta}. \quad (31)$$

Since $L = \lceil \log_2 \frac{1}{\epsilon} \rceil$ and $\sin(\theta) > \epsilon$ implies $\theta > \epsilon$, we have $R < \frac{1}{\theta} < \frac{1}{\epsilon} \leq 2^L$. Thus $k \leq L$, and hence the summation $\sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta)$ necessarily contains the term $\frac{1}{T \cdot R} \sin^2((2R + 1)\theta)$. From Eq. (31), we have

$$1 + \theta \leq (2R + 1)\theta < 2 + \theta < \frac{5}{2}.$$

For every $x \in [1, 5/2]$, we have $\sin^2 x \geq \sin^2(\frac{5}{2})$. Consequently,

$$\begin{aligned} \sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta) &\geq \frac{1}{T \cdot R} \sin^2((2R + 1)\theta) \\ &\geq \frac{1}{T \cdot R} \sin^2\left(\frac{5}{2}\right) \\ &\geq \frac{1}{2 \cdot R} \sin^2\left(\frac{5}{2}\right) \\ &> \frac{\theta}{2} \sin^2\left(\frac{5}{2}\right) > \frac{\sin(\theta)}{2} \sin^2\left(\frac{5}{2}\right) > \frac{\sin(\theta)}{10}. \end{aligned}$$

Here we use $T = \sum_{l=0}^L \frac{1}{2^l} \leq 2$, $R < 1/\theta$ (Eq. (31)), and $\frac{1}{2} \sin^2(\frac{5}{2}) \approx 0.179 > \frac{1}{10}$.

Next, we consider the case $\frac{1}{2} \leq \theta \leq \pi/2$. Since $0 < \epsilon < 1$, we have $L = \lceil \log_2 \frac{1}{\epsilon} \rceil \geq 1$. Hence the summation $\sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta)$ necessarily contains the term $\frac{1}{T} \sin^2(3\theta) + \frac{1}{2T} \sin^2(5\theta)$. One can directly verify that the minimum of the function $\sin^2(3x) + \frac{1}{2} \sin^2(5x)$ over the interval $x \in [1/2, \pi/2]$ is greater than $\frac{1}{5}$, and thus we have

$$\begin{aligned} \sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta) &\geq \frac{1}{T} \sin^2(3\theta) + \frac{1}{2T} \sin^2(5\theta) \\ &= \frac{1}{T} \left(\sin^2(3\theta) + \frac{1}{2} \sin^2(5\theta) \right) \\ &\geq \frac{1}{2} \left(\sin^2(3\theta) + \frac{1}{2} \sin^2(5\theta) \right) > \frac{1}{10} \geq \frac{\sin(\theta)}{10}. \end{aligned}$$

Here we use $T = \sum_{l=0}^L \frac{1}{2^l} \leq 2$ and $\sin(\theta) \leq 1$. Now, for $\sin(\theta) > \epsilon$, we have $\sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta) > \sin(\theta)/10$, which implies $10 \sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta) + \epsilon > \sin(\theta)$. This completes the proof of Lemma 2. $\square$

D.3 Proof of Lemma 3

Proof. We first consider the case of $t = 1$, i.e., we need to prove

$$(U_1 \circ O_{G,H}^f \circ U_0)|\phi\rangle|0, 0^m\rangle_{\text{BT}} = P_1|\phi\rangle|0, 0^m\rangle_{\text{BT}} + Q_1|\phi\rangle|1, w^*\rangle_{\text{BT}}, \quad (32)$$

where

$$P_1 := \frac{U_1 \circ O_H \circ U_0 + U_1 \circ O_G \circ U_0}{2}, \quad Q_1 := \frac{U_1 \circ O_H \circ U_0 - U_1 \circ O_G \circ U_0}{2}. \quad (33)$$

In fact, for the state $(U_1 \circ O_{G,H}^f \circ U_0)|\phi\rangle|0, 0^m\rangle_{\text{BT}}$, we can directly compute

$$\begin{aligned} & (U_1 \circ O_{G,H}^f \circ U_0)|\phi\rangle|0, 0^m\rangle_{\text{BT}} \\ &= (U_1 \circ O_{G,H}^f)U_0|\phi\rangle|0, 0^m\rangle_{\text{BT}} \\ &\stackrel{(a)}{=} (U_1 \circ T_f \circ O_{G,H} \circ T_f)U_0|\phi\rangle|0, 0^m\rangle_{\text{BT}} \\ &\stackrel{(b)}{=} (U_1 \circ T_f \circ O_{G,H})U_0|\phi\rangle|0, 0^m\rangle_{\text{BT}} \\ &\stackrel{(c)}{=} (U_1 \circ T_f \circ O_{G,H}) \left(\frac{1}{\sqrt{2}}U_0|\phi\rangle|+, 0^m\rangle_{\text{BT}} + \frac{1}{\sqrt{2}}U_0|\phi\rangle|-, 0^m\rangle_{\text{BT}} \right) \\ &\stackrel{(d)}{=} (U_1 \circ T_f) \left(\frac{1}{\sqrt{2}}O_H \circ U_0|\phi\rangle|+, 0^m\rangle_{\text{BT}} + \frac{1}{\sqrt{2}}O_G \circ U_0|\phi\rangle|-, 0^m\rangle_{\text{BT}} \right) \\ &= (U_1 \circ T_f) \left(\frac{1}{2}O_H \circ U_0|\phi\rangle|0, 0^m\rangle_{\text{BT}} + \frac{1}{2}O_H \circ U_0|\phi\rangle|1, 0^m\rangle_{\text{BT}} \right. \\ &\quad \left. + \frac{1}{2}O_G \circ U_0|\phi\rangle|0, 0^m\rangle_{\text{BT}} - \frac{1}{2}O_G \circ U_0|\phi\rangle|1, 0^m\rangle_{\text{BT}} \right) \\ &= (U_1 \circ T_f) \left(\frac{1}{2}(O_H \circ U_0 + O_G \circ U_0)|\phi\rangle|0, 0^m\rangle_{\text{BT}} \right. \\ &\quad \left. + \frac{1}{2}(O_H \circ U_0 - O_G \circ U_0)|\phi\rangle|1, 0^m\rangle_{\text{BT}} \right) \\ &\stackrel{(e)}{=} U_1 \left(\frac{1}{2}(O_H \circ U_0 + O_G \circ U_0)|\phi\rangle|0, 0^m\rangle_{\text{BT}} \right. \\ &\quad \left. + \frac{1}{2}(O_H \circ U_0 - O_G \circ U_0)|\phi\rangle|1, w^*\rangle_{\text{BT}} \right) \\ &= \frac{1}{2}(U_1 \circ O_H \circ U_0 + U_1 \circ O_G \circ U_0)|\phi\rangle|0, 0^m\rangle_{\text{BT}} \\ &\quad + \frac{1}{2}(U_1 \circ O_H \circ U_0 - U_1 \circ O_G \circ U_0)|\phi\rangle|1, w^*\rangle_{\text{BT}} \\ &\stackrel{(f)}{=} P_1|\phi\rangle|0, 0^m\rangle_{\text{BT}} + Q_1|\phi\rangle|1, w^*\rangle_{\text{BT}}. \end{aligned} \quad (34)$$

Here (a) (resp. (b)) follows from the definition of $O_{G,H}^f$ (resp. T_f) given in Eq. (24), (c) uses $|0\rangle = 1/\sqrt{2}|+\rangle + 1/\sqrt{2}|-\rangle$, (d) follows from the definition of $O_{G,H}$ given in Eq. (24), and (f) follows from Eq. (33). As for the (e), it follows from the definition of T_f and the following fact:

for any state $|\psi\rangle$, $(O_H - O_G)|\psi\rangle$ must be a superposition in the form of $\sum_{x \in S, y, z} \alpha_{x,y}^z |x, y, z\rangle$.

Now, the above equation shows that Eq. (32) holds, and thus Lemma 3 holds for $t = 1$.

Next, we assume that Lemma 3 holds for $t = k$ and then based on this assumption to consider the case of $t = k + 1$. At this point, we have

$$\left(\prod_{i=1}^k [U_i \circ O_{G,H}^f] \circ U_0 \right) |\phi\rangle |0, 0^m\rangle_{\text{BT}} = P_k |\phi\rangle |0, 0^m\rangle_{\text{BT}} + Q_k |\phi\rangle |1, w^*\rangle_{\text{BT}}.$$

Then we can compute

$$\begin{aligned} & \left(\prod_{i=1}^{k+1} [U_i \circ O_{G,H}^f] \circ U_0 \right) |\phi\rangle |0, 0^m\rangle_{\text{BT}} \\ &= U_{k+1} \circ O_{G,H}^f \left(\prod_{i=1}^k [U_i \circ O_{G,H}^f] \circ U_0 \right) |\phi\rangle |0, 0^m\rangle_{\text{BT}} \\ &= U_{k+1} \circ O_{G,H}^f P_k |\phi\rangle |0, 0^m\rangle_{\text{BT}} + U_{k+1} \circ O_{G,H}^f Q_k |\phi\rangle |1, w^*\rangle_{\text{BT}}. \end{aligned} \tag{35}$$

For the first part $U_{k+1} \circ O_{G,H}^f P_k |\phi\rangle |0, 0^m\rangle_{\text{BT}}$, similar to Eq. (34), we have

$$\begin{aligned} & U_{k+1} \circ O_{G,H}^f P_k |\phi\rangle |0, 0^m\rangle_{\text{BT}} \\ &= U_{k+1} \circ T_f \circ O_{G,H} \left(\frac{1}{\sqrt{2}} P_k |\phi\rangle |+, 0^m\rangle_{\text{BT}} + \frac{1}{\sqrt{2}} P_k |\phi\rangle |-, 0^m\rangle_{\text{BT}} \right) \\ &= U_{k+1} \circ T_f \left(\frac{1}{\sqrt{2}} O_H \circ P_k |\phi\rangle |+, 0^m\rangle_{\text{BT}} + \frac{1}{\sqrt{2}} O_G \circ P_k |\phi\rangle |-, 0^m\rangle_{\text{BT}} \right) \\ &= U_{k+1} \circ T_f \left(\frac{1}{2} O_H \circ P_k |\phi\rangle |0, 0^m\rangle_{\text{BT}} + \frac{1}{2} O_H \circ P_k |\phi\rangle |1, 0^m\rangle_{\text{BT}} \right. \\ & \quad \left. + \frac{1}{2} O_G \circ P_k |\phi\rangle |0, 0^m\rangle_{\text{BT}} - \frac{1}{2} O_G \circ P_k |\phi\rangle |1, 0^m\rangle_{\text{BT}} \right) \\ &= U_{k+1} \circ T_f \left(\frac{1}{2} (O_H \circ P_k + O_G \circ P_k) |\phi\rangle |0, 0^m\rangle_{\text{BT}} \right. \\ & \quad \left. + \frac{1}{2} (O_H \circ P_k - O_G \circ P_k) |\phi\rangle |1, 0^m\rangle_{\text{BT}} \right) \\ &= U_{k+1} \left(\frac{1}{2} (O_H \circ P_k + O_G \circ P_k) |\phi\rangle |0, 0^m\rangle_{\text{BT}} \right. \\ & \quad \left. + \frac{1}{2} (O_H \circ P_k - O_G \circ P_k) |\phi\rangle |1, w^*\rangle_{\text{BT}} \right) \\ &= \frac{1}{2} (U_{k+1} \circ O_H \circ P_k + U_{k+1} \circ O_G \circ P_k) |\phi\rangle |0, 0^m\rangle_{\text{BT}} \\ & \quad + \frac{1}{2} (U_{k+1} \circ O_H \circ P_k - U_{k+1} \circ O_G \circ P_k) |\phi\rangle |1, w^*\rangle_{\text{BT}}. \end{aligned} \tag{36}$$

For the second part $U_{k+1} \circ O_{G,H}^f Q_k |\phi\rangle |1, w^*\rangle_{\text{BT}}$, also similar to Eq. (34) and denote $Q_k |\phi\rangle := \sum_{x,y,z} \beta_{x,y}^z |x, y, z\rangle$, we can compute

$$\begin{aligned} & U_{k+1} \circ O_{G,H}^f Q_k |\phi\rangle |1, w^*\rangle_{\text{BT}} \\ &= U_{k+1} \circ T_f \circ O_{G,H} \circ T_f \sum_{x,y,z} \beta_{x,y}^z |x, y, z\rangle |1, w^*\rangle_{\text{BT}} \\ &= U_{k+1} \circ T_f \circ O_{G,H} \sum_{x,y,z} \beta_{x,y}^z |x, y, z\rangle |1, w^* \oplus f(x)\rangle_{\text{BT}} \\ &= U_{k+1} \circ T_f \circ O_{G,H} \sum_{x,y,z} \beta_{x,y}^z \left(\frac{1}{\sqrt{2}} |x, y, z\rangle |+, w^* \oplus f(x)\rangle_{\text{BT}} \right. \\ & \quad \left. - \frac{1}{\sqrt{2}} |x, y, z\rangle |-, w^* \oplus f(x)\rangle_{\text{BT}} \right) \end{aligned}$$

$$\begin{aligned}
&= U_{k+1} \circ T_f \sum_{x,y,z} \beta_{x,y}^z \left(-\frac{1}{\sqrt{2}} |x, y \oplus H(x), z\rangle |+, w^* \oplus f(x)\rangle_{\text{BT}} \right. \\
&\quad \left. -\frac{1}{\sqrt{2}} |x, y \oplus G(x), z\rangle |-, w^* \oplus f(x)\rangle_{\text{BT}} \right) \\
&= U_{k+1} \circ T_f \sum_{x,y,z} \beta_{x,y}^z \left(\begin{aligned} &+\frac{1}{2} |x, y \oplus H(x), z\rangle |0, w^* \oplus f(x)\rangle_{\text{BT}} \\ &+\frac{1}{2} |x, y \oplus H(x), z\rangle |1, w^* \oplus f(x)\rangle_{\text{BT}} \\ &-\frac{1}{2} |x, y \oplus G(x), z\rangle |0, w^* \oplus f(x)\rangle_{\text{BT}} \\ &+\frac{1}{2} |x, y \oplus G(x), z\rangle |1, w^* \oplus f(x)\rangle_{\text{BT}} \end{aligned} \right) \\
&= U_{k+1} \sum_{x,y,z} \beta_{x,y}^z \left(\begin{aligned} &+\frac{1}{2} |x, y \oplus H(x), z\rangle |0, w^* \oplus f(x)\rangle_{\text{BT}} \\ &+\frac{1}{2} |x, y \oplus H(x), z\rangle |1, w^* \rangle_{\text{BT}} \\ &-\frac{1}{2} |x, y \oplus G(x), z\rangle |0, w^* \oplus f(x)\rangle_{\text{BT}} \\ &+\frac{1}{2} |x, y \oplus G(x), z\rangle |1, w^* \rangle_{\text{BT}} \end{aligned} \right) \\
&\stackrel{(a)}{=} U_{k+1} \sum_{x,y,z} \beta_{x,y}^z \left(\begin{aligned} &+\frac{1}{2} |x, y \oplus H(x), z\rangle |0, w^* \oplus f(x)\rangle_{\text{BT}} \\ &-\frac{1}{2} |x, y \oplus G(x), z\rangle |0, w^* \oplus f(x)\rangle_{\text{BT}} \end{aligned} \right) \\
&\quad + \frac{1}{2} (U_{k+1} \circ O_H \circ Q_k + U_{k+1} \circ O_G \circ Q_k) |\phi\rangle |1, w^*\rangle_{\text{BT}} \tag{37} \\
&\stackrel{(b)}{=} U_{k+1} \sum_{x \in S, y, z} \beta_{x,y}^z \left(\begin{aligned} &+\frac{1}{2} |x, y \oplus H(x), z\rangle |0, w^* \oplus f(x)\rangle_{\text{BT}} \\ &-\frac{1}{2} |x, y \oplus G(x), z\rangle |0, w^* \oplus f(x)\rangle_{\text{BT}} \end{aligned} \right) \\
&\quad + \frac{1}{2} (U_{k+1} \circ O_H \circ Q_k + U_{k+1} \circ O_G \circ Q_k) |\phi\rangle |1, w^*\rangle_{\text{BT}} \\
&\stackrel{(c)}{=} U_{k+1} \sum_{x \in S, y, z} \beta_{x,y}^z \left(\begin{aligned} &+\frac{1}{2} |x, y \oplus H(x), z\rangle |0, 0^m\rangle_{\text{BT}} \\ &-\frac{1}{2} |x, y \oplus G(x), z\rangle |0, 0^m\rangle_{\text{BT}} \end{aligned} \right) \\
&\quad + \frac{1}{2} (U_{k+1} \circ O_H \circ Q_k + U_{k+1} \circ O_G \circ Q_k) |\phi\rangle |1, w^*\rangle_{\text{BT}} \\
&\stackrel{(d)}{=} \frac{1}{2} (U_{k+1} \circ O_H \circ Q_k - U_{k+1} \circ O_G \circ Q_k) |\phi\rangle |0, 0^m\rangle_{\text{BT}} \\
&\quad + \frac{1}{2} (U_{k+1} \circ O_H \circ Q_k + U_{k+1} \circ O_G \circ Q_k) |\phi\rangle |1, w^*\rangle_{\text{BT}}.
\end{aligned}$$

Here (a) uses $Q_k|\phi\rangle = \sum_{x,y,z} \beta_{x,y}^z |x, y, z\rangle$, (b) follows from $G(x) = H(x)$ for any $x \notin S$, (c) follows from $f(x) = w^*$ for any $x \in S$, and (d) uses the fact that

$$O_H \circ Q_k |\phi\rangle - O_G \circ Q_k |\phi\rangle = \sum_{x \in S, y, z} \beta_{x,y}^z (|x, y \oplus H(x), z\rangle - |x, y \oplus G(x), z\rangle),$$

which is obvious under the definition $Q_k|\phi\rangle = \sum_{x,y,z} \beta_{x,y}^z |x, y, z\rangle$ and the fact that $G(x) = H(x)$ for any $x \notin S$. Now, by combining Eq. (35) to Eq. (37), we obtain

$$\begin{aligned}
&\left(\prod_{i=1}^{k+1} [U_i \circ O_{G,H}^f] \circ U_0 \right) |\phi\rangle |0, 0^m\rangle_{\text{BT}} \\
&= \frac{1}{2} (U_{k+1} \circ O_H \circ P_k + U_{k+1} \circ O_G \circ P_k) |\phi\rangle |0, 0^m\rangle_{\text{BT}} \\
&\quad + \frac{1}{2} (U_{k+1} \circ O_H \circ P_k - U_{k+1} \circ O_G \circ P_k) |\phi\rangle |1, w^*\rangle_{\text{BT}}
\end{aligned}$$

$$\begin{aligned}
& + \frac{1}{2}(U_{k+1} \circ O_H \circ Q_k - U_{k+1} \circ O_G \circ Q_k)|\phi\rangle|0, 0^m\rangle_{\text{BT}} \\
& + \frac{1}{2}(U_{k+1} \circ O_H \circ Q_k + U_{k+1} \circ O_G \circ Q_k)|\phi\rangle|1, w^*\rangle_{\text{BT}} \\
& = \frac{1}{2}(U_{k+1} \circ O_H \circ (P_k + Q_k) + U_{k+1} \circ O_G \circ (P_k - Q_k))|\phi\rangle|0, 0^m\rangle_{\text{BT}} \\
& + \frac{1}{2}(U_{k+1} \circ O_H \circ (P_k + Q_k) - U_{k+1} \circ O_G \circ (P_k - Q_k))|\phi\rangle|1, w^*\rangle_{\text{BT}}.
\end{aligned} \tag{38}$$

According to the definition of P_t and Q_t given in Lemma 3, we have

$$P_k + Q_k = \prod_{i=1}^k [U_i \circ O_H] \circ U_0, \quad P_k - Q_k = \prod_{i=1}^k [U_i \circ O_G] \circ U_0.$$

This further implies that

$$\begin{aligned}
U_{k+1} \circ O_H \circ (P_k + Q_k) &= \prod_{i=1}^{k+1} [U_i \circ O_H] \circ U_0, \\
U_{k+1} \circ O_G \circ (P_k - Q_k) &= \prod_{i=1}^{k+1} [U_i \circ O_G] \circ U_0.
\end{aligned} \tag{39}$$

Combining Eq. (38) with Eq. (39) we finally obtain

$$\left(\prod_{i=1}^{k+1} [U_i \circ O_{G,H}^f] \circ U_0 \right) |\phi\rangle|0, 0^m\rangle_{\text{BT}} = P_{k+1}|\phi\rangle|0, 0^m\rangle_{\text{BT}} + Q_{k+1}|\phi\rangle|1, w^*\rangle_{\text{BT}}.$$

In fact, the above equation shows that, if Lemma 3 holds with $t = k$, then this lemma also holds with $t = k + 1$. Since we have proved that this lemma holds with $t = 1$ in the beginning, by induction we can prove this lemma. $\square$

D.4 Proof of Theorem 5

Proof. To prove this theorem, we define a sequence of games $\mathbf{G}_0$ to $\mathbf{G}_6$ (Fig. 7).

Game $\mathbf{G}_0$: This is the IND-CCA game of $\mathcal{U}^\mathcal{L}[\mathbf{P}, G, F]$ with the adversary $\mathcal{A}$ in the QROM. Obviously, we have

$$\text{Adv}_{\mathcal{U}^\mathcal{L}[\mathbf{P}, G, F]}^{\text{IND-CCA}}(\mathcal{A}) = \left| \Pr[1 \leftarrow \mathbf{G}_0] - \frac{1}{2} \right|. \tag{40}$$

Game $\mathbf{G}_1$: In this game, the pseudorandom function F used in the decapsulation oracle Deca is changed into a fresh uniformly random function $R \leftarrow_{\S} \Omega_{\mathcal{C} \rightarrow \mathcal{K}}$.

We define a PRF adversary $\mathcal{A}_{\text{prf}}$ with oracle access to $O \in \{F(s, \cdot), R(\cdot)\}$ as:

- By using a $2(q_G + q_D)$ -wise independent function [28] to simulate G , $\mathcal{A}_{\text{prf}}$ runs the adversary $\mathcal{A}$ in game $\mathbf{G}_0$. If $\mathcal{A}$ makes a $\text{Deca}(c)$ query that failed to decapsulate, $\mathcal{A}_{\text{prf}}$ returns $O(c)$ to $\mathcal{A}$ by querying O . $\mathcal{A}_{\text{prf}}$ finally outputs 1 if game $\mathbf{G}_0$ returns 1 and 0 otherwise.

GAMES $\mathbf{G_0-G_6}$		$G(m, c)$ $// \mathbf{G_4, G_6}$
1 : $(pk, sk) \leftarrow \text{Gen}$	$// \mathbf{G_0-G_6}$	1 : if $\text{Enc}_{pk}(m) = c$
2 : $G_1 \leftarrow_{\$} \Omega_{\mathcal{M} \times \mathcal{C} \rightarrow \mathcal{K}}$	$// \mathbf{G_0-G_6}$	2 : return $R(c)$
3 : $s \leftarrow_{\$} \mathcal{K}^{prf}$	$// \mathbf{G_0}$	3 : else return $G_1(m, c)$
4 : $R \leftarrow_{\$} \Omega_{\mathcal{C} \rightarrow \mathcal{K}}$	$// \mathbf{G_1-G_6}$	
5 : $m^* \leftarrow_{\$} \mathcal{M}$	$// \mathbf{G_0-G_6}$	$G(m, c)$ $// \mathbf{G_5}$
6 : $c^* := \text{Enc}_{pk}(m^*)$	$// \mathbf{G_0-G_6}$	1 : if $(m, c) = (m^*, c^*)$
7 : $b \leftarrow_{\$} \{0, 1\}$	$// \mathbf{G_0-G_6}$	2 : return k_0^*
8 : $k_0^* := G(m^*, c^*)$	$// \mathbf{G_0-G_4}$	3 : else if $\text{Enc}_{pk}(m) = c$
9 : $k^* \leftarrow_{\$} \mathcal{K}, k_0^* := k^*$	$// \mathbf{G_5-G_6}$	4 : return $R(c)$
10 : $k_1^* \leftarrow_{\$} \mathcal{K}$	$// \mathbf{G_0-G_6}$	5 : else return $G_1(m, c)$
11 : $b' \leftarrow \mathcal{A}^{G, \text{Deca}}(pk, c^*, k_b^*)$	$// \mathbf{G_0-G_6}$	
12 : return $\llbracket b' = b \rrbracket$	$// \mathbf{G_0-G_6}$	$\text{Deca}(c \neq c^*)$
$G(m, c)$ $// \mathbf{G_0-G_1}$		1 : $m' := \text{Dec}_{sk}(c)$ $// \mathbf{G_0-G_2}$
1 : return $G_1(m, c)$		2 : if $m' \neq \perp \wedge \text{Enc}_{pk}(m') = c$ $// \mathbf{G_0-G_2}$
$G(m, c)$ $// \mathbf{G_2-G_3}$		3 : return $G(m', c)$ $// \mathbf{G_0-G_2}$
1 : if $\text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) = m$		4 : else return $F(s, c)$ $// \mathbf{G_0}$
2 : return $R(c)$		5 : else return $R(c)$ $// \mathbf{G_1-G_2}$
3 : else return $G_1(m, c)$		$\text{Deca}(c \neq c^*)$ $// \mathbf{G_3-G_6}$
		1 : return $R(c)$

Fig. 7: Games $\mathbf{G_0-G_6}$ for the proof of Theorem 5. Note that the oracle G can be quantumly accessed in those games. In this figure, we just write the classical description of G for brevity.

Since the pseudorandom function F is only used by Deca , $\mathcal{A}_{\text{prf}}$ makes at most q_D classical queries to its oracle O and its running time can be bounded as $\mathcal{T}_{\mathcal{A}_{\text{prf}}} \lesssim \mathcal{T}_A + q_D \cdot (\mathcal{T}_{\text{Enc}} + \mathcal{T}_{\text{Dec}}) + O(q_G^2 + q_D^2)$. By the definition of $\mathcal{A}_{\text{prf}}$, we have $\Pr[1 \leftarrow \mathcal{A}_{\text{prf}}^{F(s, \cdot)}] = \Pr[1 \leftarrow \mathbf{G_0}]$ and $\Pr[1 \leftarrow \mathcal{A}_{\text{prf}}^{R(\cdot)}] = \Pr[1 \leftarrow \mathbf{G_1}]$. Thus

$$|\Pr[1 \leftarrow \mathbf{G_0}] - \Pr[1 \leftarrow \mathbf{G_1}]| = \text{Adv}_F^{\text{PRF}}(\mathcal{A}_{\text{prf}}). \quad (41)$$

Game $\mathbf{G_2}$: This game is the same as game $\mathbf{G_1}$, except that the $G(m, c)$ is replaced with $R(c)$ if $\text{Enc}_{pk}(m) = c$ and $\text{Dec}_{sk}(c) = m$.

In game $\mathbf{G_1}$, the adversary $\mathcal{A}$ can obtain $R(c)$ only through a $\text{Deca}(c)$ query for which decryption fails or the re-encryption check fails. Hence, the $R(c)$ used to reprogram G in game $\mathbf{G_2}$ remains uniformly random from $\mathcal{A}$'s view. Moreover, since Dec is a deterministic algorithm, there do not exist $m_1 \neq m_2$ and c such

that both $(m = m_1, c)$ and $(m = m_2, c)$ pass the check that $\text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) = m$. These two observations imply that, from $\mathcal{A}$'s view, the oracle G reprogrammed using R in game $\mathbf{G}_2$ is equivalent to the original one in game $\mathbf{G}_1$. Consequently,

$$\Pr[1 \leftarrow \mathbf{G}_1] = \Pr[1 \leftarrow \mathbf{G}_2]. \quad (42)$$

Game $\mathbf{G}_3$: This game is the same as game $\mathbf{G}_2$, except that the decapsulation oracle Deca is changed as it directly returns $R(c)$ for any $c \neq c^*$. Therefore, the answer of Deca in this game no longer uses the secret key sk .

Since we have already reprogrammed $G(m, c)$ to $R(c)$ whenever $\text{Enc}_{pk}(m) = c$ and $\text{Dec}_{sk}(c) = m$, the value $G(m, c)$ returned by Deca in game $\mathbf{G}_2$ is in fact exactly $R(c)$. Therefore, game $\mathbf{G}_3$ is an equivalent rewriting of game $\mathbf{G}_2$. Thus

$$\Pr[1 \leftarrow \mathbf{G}_2] = \Pr[1 \leftarrow \mathbf{G}_3]. \quad (43)$$

Game $\mathbf{G}_4$: In this game, the reprogramming of $G(m, c)$ no longer checks whether $\text{Dec}_{sk}(c) = m$, and directly returns $R(c)$ if $\text{Enc}_{pk}(m) = c$.

The only difference between game $\mathbf{G}_4$ and game $\mathbf{G}_3$ is that, for any (m, c) satisfying $\text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) \neq m$, $G(m, c)$ is set to $G_1(m, c)$ in game $\mathbf{G}_3$ and to $R(c)$ in game $\mathbf{G}_4$. Note that, in game $\mathbf{G}_3$, whenever the adversary $\mathcal{A}$ obtains a value $R(c)$ through a G query, there must exist some m such that $\text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) = m$. Hence, as long as $\mathcal{A}$ does not make a Deca query on a $c \in L$, where

$$L := \{c \mid \exists m \in \mathcal{M} \text{ s.t. } \text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) \neq m\},$$

all values $R(c)$ with $c \in L$ remain uniformly random from $\mathcal{A}$'s view. Moreover, if $\text{Enc}_{pk}(\cdot)$ is injective, there do not exist $m_1 \neq m_2$ and c such that both $(m = m_1, c)$ and $(m = m_2, c)$ satisfy $\text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) \neq m$. This means that, as long as $\mathcal{A}$ does not make a Deca query on $c \in L$ and $\text{Enc}_{pk}(\cdot)$ is injective, for every (m, c) satisfying $\text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) \neq m$, the responses $G_1(m, c)$ and $R(c)$ to G on (m, c) are indistinguishable to $\mathcal{A}$. Thus, by the definitions of FFC game and η -injective, we have

$$|\Pr[1 \leftarrow \mathbf{G}_3] - \Pr[1 \leftarrow \mathbf{G}_4]| \leq \text{Adv}_P^{\text{FFC}}(\mathcal{A}_{\text{ffc}}) + \eta. \quad (44)$$

Here, $\mathcal{A}_{\text{ffc}}$ runs $\mathcal{A}$ in game $\mathbf{G}_4$, simulates G_1 by a $2q_G$ -wise independent function and R by a $2(q_G + q_D)$ -wise independent function, and finally outputs the list of Deca queries made by $\mathcal{A}$. Obviously, $\mathcal{T}_{\mathcal{A}_{\text{ffc}}} \lesssim \mathcal{T}_{\mathcal{A}} + O(q_G) \cdot \mathcal{T}_{\text{Enc}} + O(q_G^2 + q_D^2)$.

Game $\mathbf{G}_5$: This game is the same as game $\mathbf{G}_4$, except that k_0^* is replaced with a fresh uniformly random value k^* and G directly returns k^* if its input is (m^*, c^*) .

Game $\mathbf{G}_5$ actually reprograms G at (m^*, c^*) to a fresh uniformly random value k^* before G is queried. Hence, as long as $G(m^*, c^*)$ in game $\mathbf{G}_4$ is uniformly random and $G(m^*, c^*)$ is independent of $G(m, c)$ for every $(m, c) \neq (m^*, c^*)$, the

adversary $\mathcal{A}$ cannot detect the modification made in game $\mathbf{G}_5$. We next justify these two properties of $G(m^*, c^*)$. For the first property, since $G(m^*, c^*) = R(c^*)$ in game $\mathbf{G}_4$, $G(m^*, c^*)$ is indeed uniformly random. For the second property, note that, as long as the $\text{Enc}_{pk}(\cdot)$ is injective, there is no $(m, c) \neq (m^*, c^*)$ such that $\text{Enc}_{pk}(m) = c$ and $c = c^*$. This implies that, during the simulation of G in game $\mathbf{G}_4$, the value $R(c^*)$ is used only to answer the $G(m^*, c^*)$. Therefore, $G(m^*, c^*)$ is independent of $G(m, c)$ for every $(m, c) \neq (m^*, c^*)$, establishing the second property as well. Thus, we have

$$|\Pr[1 \leftarrow \mathbf{G}_4] - \Pr[1 \leftarrow \mathbf{G}_5]| \leq \eta. \quad (45)$$

Game $\mathbf{G}_6$: This game is the same as game $\mathbf{G}_5$, except that the simulation of $G(m, c)$ no longer additionally checks whether $(m, c) = (m^*, c^*)$.

As long as the adversary $\mathcal{A}$ does not query G on (m^*, c^*) , the modification made in game $\mathbf{G}_6$ cannot be detected by $\mathcal{A}$, and we need to use the O2H theorem to formalize this argument. To this end, we first define a distribution $\mathfrak{D}$ over the tuple $(G, H, S, z = (pk, c^*, b, k_b^*, R))$ as shown in Fig. 8. We then define a quantum oracle algorithm $\mathcal{B}^O(z)$ ($O \in \{G, H\}$), which runs $\mathcal{A}^{O, \text{Deca}}(pk, c^*, k_b^*)$ to get b' and then outputs $\llbracket b = b' \rrbracket$. During the running, $\mathcal{B}^O(z)$ answers each $\text{Deca}(c)$ query with $R(c)$.

1. Sample $(pk, sk) \leftarrow \text{Gen}$, $m^* \leftarrow_{\S} \mathcal{M}$, $b \leftarrow_{\S} \{0, 1\}$, $k^* \leftarrow_{\S} \mathcal{K}$, and $k_1^* \leftarrow_{\S} \mathcal{K}$.
Sample G_1 (resp. R) as a $2q_G$ -wise (resp. $2(q_G + q_D)$ -wise) independent function.
2. Define $c^* := \text{Enc}_{pk}(m^*)$, $S := \{(m^*, c^*)\}$, $k_0^* := k^*$, $z := (pk, c^*, b, k_b^*, R)$.
3. Let H be a function that $H(m, c) = R(c)$ if $\text{Enc}_{pk}(m) = c$
and $H(m, c) = G_1(m, c)$ if $\text{Enc}_{pk}(m) \neq c$.
4. The function G is the same as H , except $G(m^*, c^*) := k^*$.

Fig. 8: The distribution $\mathfrak{D}$ of $(G, H, S, z := (pk, c^*, b, k_b^*, R))$. Here, the R in z is not represented by its value table, but by a description of a $2(q_G + q_D)$ -wise independent function.

Observe that $\mathcal{B}^O(z)$ makes q_G queries to O and $\mathcal{T}_B \lesssim \mathcal{T}_A + O(q_G^2 + q_D^2)$. By the definitions of G and H in the above distribution $\mathfrak{D}$, we have

$$\begin{aligned} \Pr[1 \leftarrow \mathcal{B}^G(z) : (G, H, S, z) \leftarrow \mathfrak{D}] &= \Pr[1 \leftarrow \mathbf{G}_5], \\ \Pr[1 \leftarrow \mathcal{B}^H(z) : (G, H, S, z) \leftarrow \mathfrak{D}] &= \Pr[1 \leftarrow \mathbf{G}_6]. \end{aligned}$$

Then, by using Theorem 4 and setting f as the function that maps $(m, c) \in \mathcal{M} \times \mathcal{C}$ to m , we can construct an algorithm $\mathcal{C}$ such that

$$|\Pr[1 \leftarrow \mathbf{G}_5] - \Pr[1 \leftarrow \mathbf{G}_6]| \leq 22 \cdot \text{Adv}(\mathcal{C}),$$

where

$$\text{Adv}(\mathcal{C}) := \Pr [m = m^* : m \leftarrow \mathcal{C}^{G,H}(z), (G, H, S, z) \leftarrow \mathfrak{D}].$$

Recall that $\mathcal{M} = \{0, 1\}^m$. Thus, $\mathcal{C}$ makes an expected $(2m + 5)q_G$ queries to G and an expected $(2m + 5)q_G$ queries to H , and $\mathcal{T}_{\mathcal{C}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{B}}$.

At this point, we can equivalently transform $\mathcal{C}$ into an adversary $\mathcal{A}_{\text{ow}}$ against the OW-CPA security of $\mathbf{P}$ as follows:

- $\mathcal{A}_{\text{ow}}$ gets the challenge ciphertext $c^* := \text{Enc}_{pk}(m^*)$ and public key pk , where m^* is the challenge plaintext uniformly sampled from $\mathcal{M}$ by the challenger and pk is sampled by $(pk, sk) \leftarrow \text{Gen}$.
- $\mathcal{A}_{\text{ow}}$ samples b, k^*, k_b^*, G_1 , and R according to the distribution $\mathfrak{D}$ in Fig. 8, and then uses $z := (pk, c^*, b, k_b^*, R)$ as input to run $\mathcal{C}^{G,H}(z)$ and simulates the oracles G and H for $\mathcal{C}$:
 1. When $\mathcal{C}$ queries G with input (m, c) :
 - (a) If $\text{Enc}_{pk}(m) = c^* \wedge c = c^*$, $\mathcal{A}_{\text{ow}}$ answers k^* .
 - (b) If $\text{Enc}_{pk}(m) \neq c^* \vee c \neq c^*$, but $\text{Enc}_{pk}(m) = c$, $\mathcal{A}_{\text{ow}}$ answers $R(c)$.
 - (c) Otherwise, $\mathcal{A}_{\text{ow}}$ answers $G_1(m, c)$.
 2. When $\mathcal{C}$ queries H with input (m, c) , $\mathcal{A}_{\text{ow}}$ answers $R(c)$ if $\text{Enc}_{pk}(m) = c$, and answers $G_1(m, c)$ otherwise.
- After $\mathcal{C}$ returns m , $\mathcal{A}_{\text{ow}}$ outputs m .

One can check that the running time of $\mathcal{A}_{\text{ow}}$ is $\mathcal{T}_{\mathcal{A}_{\text{ow}}}^{\text{exp}} \lesssim \mathcal{T}_{\mathcal{C}}^{\text{exp}} + O(mq_G) \cdot \mathcal{T}_{\text{Enc}} + O(mq_G^2 + mq_D^2)$. In the above construction, since $\mathcal{A}_{\text{ow}}$ cannot get the challenge plaintext m^* directly, it checks whether m equals m^* by testing whether $\text{Enc}_{pk}(m)$ equals c^* during the simulation of oracle G for $\mathcal{C}$. In fact, as long as the $\text{Enc}_{pk}(\cdot)$ is injective, $\mathcal{A}_{\text{ow}}$ simulates the oracle G for $\mathcal{C}$ perfectly¹⁶. Thus,

$$\text{Adv}(\mathcal{C}) \leq \text{Adv}_{\mathbf{P}}^{\text{OW-CPA}}(\mathcal{A}_{\text{ow}}) + \eta.$$

Combining the above analysis and three equations, we have $\mathcal{T}_{\mathcal{A}_{\text{ow}}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}} + O(mq_G) \cdot \mathcal{T}_{\text{Enc}} + O(mq_G^2 + mq_D^2)$ and

$$|\Pr[1 \leftarrow \mathbf{G}_5] - \Pr[1 \leftarrow \mathbf{G}_6]| \leq 22 \cdot \text{Adv}_{\mathbf{P}}^{\text{OW-CPA}}(\mathcal{A}_{\text{ow}}) + 22 \cdot \eta. \quad (46)$$

As for the probability $\Pr[1 \leftarrow \mathbf{G}_6]$, since the adversary $\mathcal{A}$'s view in game $\mathbf{G}_6$ is independent of b , we have

$$\Pr[1 \leftarrow \mathbf{G}_6] = \frac{1}{2}. \quad (47)$$

By combining Eq. (40) to Eq. (47), we finally have

$$\begin{aligned} \text{Adv}_{\mathbf{U}^\perp[\mathbf{P}, G, F]}^{\text{IND-CCA}}(\mathcal{A}) &\leq \text{Adv}_{\mathbf{F}}^{\text{PRF}}(\mathcal{A}_{\text{prf}}) + 22 \cdot \text{Adv}_{\mathbf{P}}^{\text{OW-CPA}}(\mathcal{A}_{\text{ow}}) \\ &\quad + \text{Adv}_{\mathbf{P}}^{\text{FFC}}(\mathcal{A}_{\text{ffc}}) + 24 \cdot \eta. \end{aligned}$$

This completes the proof of Theorem 5. $\square$

¹⁶ Here the "perfectly" means that, in $\mathcal{C}$'s view, the oracle G simulated by $\mathcal{A}_{\text{ow}}$ is perfectly indistinguishable with the oracle G obtained by sampling (G, H, S, z) according to the distribution $\mathfrak{D}$ in Fig. 8.

D.5 Proof of Theorem 6

Proof. To prove this theorem, we define a sequence of games $\mathbf{G}_0$ to $\mathbf{G}_6$ (Fig. 9).

Game $\mathbf{G}_0$: This is the IND-CCA game of $\mathcal{U}^\perp[\mathbf{P}, G, \mathbf{F}]$ with the adversary $\mathcal{A}$ in the QROM. Obviously, we have

$$\text{Adv}_{\mathcal{U}^\perp[\mathbf{P}, G, \mathbf{F}]}^{\text{IND-CCA}}(\mathcal{A}) = \left| \Pr[1 \leftarrow \mathbf{G}_0] - \frac{1}{2} \right|. \quad (48)$$

GAMES $\mathbf{G}_0$ - $\mathbf{G}_6$	$G(m, c)$ // $\mathbf{G}_4, \mathbf{G}_6$
1 : $(pk, sk) \leftarrow \text{Gen}$ // $\mathbf{G}_0$ - $\mathbf{G}_6$	1 : if $\text{Enc}_{pk}(m) = c$
2 : $G_1 \leftarrow_{\$} \Omega_{\mathcal{M} \times \mathcal{C} \rightarrow \mathcal{K}}$ // $\mathbf{G}_0$ - $\mathbf{G}_6$	2 : return $R(c)$
3 : $s \leftarrow_{\$} \mathcal{K}^{prf}$ // $\mathbf{G}_0$	3 : else return $G_1(m, c)$
4 : $R \leftarrow_{\$} \Omega_{\mathcal{C} \rightarrow \mathcal{K}}$ // $\mathbf{G}_1$ - $\mathbf{G}_6$	
5 : $m^* \leftarrow_{\$} \mathcal{M}$ // $\mathbf{G}_0$ - $\mathbf{G}_6$	$G(m, c)$ // $\mathbf{G}_5$
6 : $c^* := \text{Enc}_{pk}(m^*)$ // $\mathbf{G}_0$ - $\mathbf{G}_6$	1 : if $(m, c) = (m^*, c^*)$
7 : $b \leftarrow_{\$} \{0, 1\}$ // $\mathbf{G}_0$ - $\mathbf{G}_6$	2 : return k_0^*
8 : $k_0^* := G(m^*, c^*)$ // $\mathbf{G}_0$ - $\mathbf{G}_4$	3 : else if $\text{Enc}_{pk}(m) = c$
9 : $k^* \leftarrow_{\$} \mathcal{K}, k_0^* := k^*$ // $\mathbf{G}_5$ - $\mathbf{G}_6$	4 : return $R(c)$
10 : $k_1^* \leftarrow_{\$} \mathcal{K}$ // $\mathbf{G}_0$ - $\mathbf{G}_6$	5 : else return $G_1(m, c)$
11 : $b' \leftarrow \mathcal{A}^{G, \text{Deca}}(pk, c^*, k_b^*)$ // $\mathbf{G}_0$ - $\mathbf{G}_6$	$\text{Deca}(c \neq c^*)$
12 : return $\llbracket b' = b \rrbracket$ // $\mathbf{G}_0$ - $\mathbf{G}_6$	1 : $m' := \text{Dec}_{sk}(c)$ // $\mathbf{G}_0$ - $\mathbf{G}_2$
$G(m, c)$ // $\mathbf{G}_0$ - $\mathbf{G}_1$	2 : if $m' \neq \perp \wedge \text{Enc}_{pk}(m') = c$ // $\mathbf{G}_0$ - $\mathbf{G}_2$
1 : return $G_1(m, c)$	3 : return $G(m', c)$ // $\mathbf{G}_0$ - $\mathbf{G}_2$
$G(m, c)$ // $\mathbf{G}_2$ - $\mathbf{G}_3$	4 : else return $\mathbf{F}(s, c)$ // $\mathbf{G}_0$
1 : if $\text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) = m$	5 : else return $R(c)$ // $\mathbf{G}_1$ - $\mathbf{G}_2$
2 : return $R(c)$	
3 : else return $G_1(m, c)$	$\text{Deca}(c \neq c^*)$ // $\mathbf{G}_3$ - $\mathbf{G}_6$
	1 : return $R(c)$

Fig. 9: Games $\mathbf{G}_0$ - $\mathbf{G}_6$ for the proof of Theorem 6. Note that the oracle G can be quantumly accessed in those games. In this figure, we just write the classical description of G for brevity.

Game $\mathbf{G}_1$: In this game, the pseudorandom function $\mathbf{F}$ used in the decapsulation oracle Deca is changed into a fresh uniformly random function $R \leftarrow_{\$} \Omega_{\mathcal{C} \rightarrow \mathcal{K}}$.

We define a PRF adversary $\mathcal{A}_{\text{prf}}$ with oracle access to $O \in \{\mathbf{F}(s, \cdot), R(\cdot)\}$ as:

- By using a $2(q_G + q_D)$ -wise independent function [28] to simulate G , $\mathcal{A}_{\text{prf}}$ runs the adversary $\mathcal{A}$ in game $\mathbf{G}_0$. If $\mathcal{A}$ makes a $\text{Deca}(c)$ query that failed to decapsulate, $\mathcal{A}_{\text{prf}}$ returns $O(c)$ to $\mathcal{A}$ by querying O . $\mathcal{A}_{\text{prf}}$ finally outputs 1 if game $\mathbf{G}_0$ returns 1 and 0 otherwise.

Since the pseudorandom function F is only used by Deca , $\mathcal{A}_{\text{prf}}$ makes at most q_D classical queries to its oracle O and its running time can be bounded as $\mathcal{T}_{\mathcal{A}_{\text{prf}}} \lesssim \mathcal{T}_{\mathcal{A}} + q_D \cdot (\mathcal{T}_{\text{Enc}} + \mathcal{T}_{\text{Dec}}) + O(q_G^2 + q_D^2)$. By the definition of $\mathcal{A}_{\text{prf}}$, we have $\Pr[1 \leftarrow \mathcal{A}_{\text{prf}}^{F(s, \cdot)}] = \Pr[1 \leftarrow \mathbf{G}_0]$ and $\Pr[1 \leftarrow \mathcal{A}_{\text{prf}}^{R(\cdot)}] = \Pr[1 \leftarrow \mathbf{G}_1]$. Thus

$$|\Pr[1 \leftarrow \mathbf{G}_0] - \Pr[1 \leftarrow \mathbf{G}_1]| = \text{Adv}_F^{\text{PRF}}(\mathcal{A}_{\text{prf}}). \quad (49)$$

Game $\mathbf{G}_2$: This game is the same as game $\mathbf{G}_1$, except that the $G(m, c)$ is replaced with $R(c)$ if $\text{Enc}_{pk}(m) = c$ and $\text{Dec}_{sk}(c) = m$.

In game $\mathbf{G}_1$, the adversary $\mathcal{A}$ can obtain $R(c)$ only through a $\text{Deca}(c)$ query for which decryption fails or the re-encryption check fails. Hence, the $R(c)$ used to reprogram G in game $\mathbf{G}_2$ remains uniformly random from $\mathcal{A}$'s view. Moreover, since Dec is a deterministic algorithm, there do not exist $m_1 \neq m_2$ and c such that both $(m = m_1, c)$ and $(m = m_2, c)$ pass the check that $\text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) = m$. These two observations imply that, from $\mathcal{A}$'s view, the oracle G reprogrammed using R in game $\mathbf{G}_2$ is equivalent to the original one in game $\mathbf{G}_1$. Consequently,

$$\Pr[1 \leftarrow \mathbf{G}_1] = \Pr[1 \leftarrow \mathbf{G}_2]. \quad (50)$$

Game $\mathbf{G}_3$: This game is the same as game $\mathbf{G}_2$, except that the decapsulation oracle Deca is changed as it directly returns $R(c)$ for any $c \neq c^*$. Therefore, the answer of Deca in this game no longer uses the secret key sk .

Since we have already reprogrammed $G(m, c)$ to $R(c)$ whenever $\text{Enc}_{pk}(m) = c$ and $\text{Dec}_{sk}(c) = m$, the value $G(m, c)$ returned by Deca in game $\mathbf{G}_2$ is in fact exactly $R(c)$. Therefore, game $\mathbf{G}_3$ is an equivalent rewriting of game $\mathbf{G}_2$. Thus

$$\Pr[1 \leftarrow \mathbf{G}_2] = \Pr[1 \leftarrow \mathbf{G}_3]. \quad (51)$$

Game $\mathbf{G}_4$: In this game, the reprogramming of $G(m, c)$ no longer checks whether $\text{Dec}_{sk}(c) = m$, and directly returns $R(c)$ if $\text{Enc}_{pk}(m) = c$.

Define $S := \{(m, c) : \text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) \neq m\}$. It is obvious that, as long as G has never been queried on any $(m, c) \in S$, the modification made in game $\mathbf{G}_4$ cannot be detected. However, since G can be quantumly accessed, we need to use the O2H theorem to formalize this argument. In particular, we reduce the distinguishing advantage between games $\mathbf{G}_3$ and $\mathbf{G}_4$ to the probability of guessing an element in S . To this end, we first define a distribution $\mathfrak{D}$ over the tuple $(G_1, G_2, S, z := (pk, sk, m^*, c^*, b, k_1^*, R))$ as shown in Fig. 10.

We then define a new quantum oracle algorithm $\mathcal{B}^O(z)$ ($O \in \{G_1, G_2\}$), which first sets $k_0^* := G(m^*, c^*)$, then runs $\mathcal{A}^{G, \text{Deca}}(pk, c^*, k_b^*)$ to get b' , and

- | |
|--|
| <ol style="list-style-type: none"> 1. Sample $(pk, sk) \leftarrow \text{Gen}$, $m^* \leftarrow_{\\$} \mathcal{M}$, $b \leftarrow_{\\$} \{0, 1\}$, and $k_1^* \leftarrow_{\\$} \mathcal{K}$.
 Sample G_1 as a $2(q_G + 1)$-wise independent function.
 Sample R as a $2(q_G + q_D + 1)$-wise independent function. 2. Define $c^* := \text{Enc}_{pk}(m^*)$ and $S := \{(m, c) : \text{Enc}_{pk}(m) = c \wedge \text{Dec}_{sk}(c) \neq m\}$.
 Define $z := (pk, sk, m^*, c^*, b, k_1^*, R)$.
 The function G_2 is the same as G_1, except $G_2(m, c) := R(c)$ for every $(m, c) \in S$. |
|--|

Fig. 10: The distribution $\mathfrak{D}$ of $(G_1, G_2, S, z := (pk, sk, m^*, c^*, b, k_1^*, R))$. Here, the R in z is not represented by its value table, but by a description of a $2(q_G + q_D + 1)$ -wise independent function.

finally outputs $\llbracket b = b' \rrbracket$. During the running, for each $G(m, c)$ query, $\mathcal{B}^O(z)$ returns $R(c)$ if $\text{Enc}_{pk}(m) = c$ and $\text{Dec}_{sk}(c) = m$. Otherwise, $\mathcal{B}^O(z)$ queries O and returns $O(m, c)$. Observe that $\mathcal{B}^O(z)$ makes $q_G + 1$ queries to O and $\mathcal{T}_B \lesssim \mathcal{T}_A + q_G \cdot (\mathcal{T}_{\text{Enc}} + \mathcal{T}_{\text{Dec}}) + O(q_G^2 + q_D^2)$. By the definitions of G_1 and G_2 in the distribution $\mathfrak{D}$, we have

$$\begin{aligned} \Pr[1 \leftarrow \mathcal{B}^{G_1}(z) : (G_1, G_2, S, z) \leftarrow \mathfrak{D}] &= \Pr[1 \leftarrow \mathbf{G}_3], \\ \Pr[1 \leftarrow \mathcal{B}^{G_2}(z) : (G_1, G_2, S, z) \leftarrow \mathfrak{D}] &= \Pr[1 \leftarrow \mathbf{G}_4]. \end{aligned}$$

Then, by using Theorem 14, we can construct an algorithm $\mathcal{C}$ such that

$$|\Pr[1 \leftarrow \mathbf{G}_3] - \Pr[1 \leftarrow \mathbf{G}_4]| \leq 4\sqrt{q_G + 1} \cdot \text{Adv}(\mathcal{C}),$$

where

$$\text{Adv}(\mathcal{C}) := \Pr[(m, c) \in S : (m, c) \leftarrow \mathcal{C}^{G_1, G_2, 1_S}(z), (G_1, G_2, S, z) \leftarrow \mathfrak{D}].$$

Here, $\mathcal{C}$ makes at most $3(q_G + 1)$ queries to G_1 , G_2 , and 1_S , respectively, and $\mathcal{T}_C \lesssim 3 \cdot \mathcal{T}_B$. By the definition of the COR game (Definition 4), we can equivalently transform $\mathcal{C}$ into an adversary $\mathcal{A}_{\text{cor}}$ of the COR game of $\mathbf{P}$. That is, $\mathcal{A}_{\text{cor}}(pk, sk)$ samples G_1, G_2 , and z according to the distribution $\mathfrak{D}$ (Fig. 10) with the key pair (pk, sk) fixed to its input, runs $\mathcal{C}^{G_1, G_2, 1_S}(z)$ to get (m, c) , and finally outputs m ¹⁷. Now we have $\mathcal{T}_{\mathcal{A}_{\text{cor}}} \lesssim \mathcal{T}_C + O(q_G) \cdot (\mathcal{T}_{\text{Enc}} + \mathcal{T}_{\text{Dec}}) + O(q_G^2 + q_D^2)$ and

$$\text{Adv}(\mathcal{C}) \leq \text{Adv}_{\mathbf{P}}^{\text{COR}}(\mathcal{A}_{\text{cor}}).$$

Combining the above analysis and three equations, we have $\mathcal{T}_{\mathcal{A}_{\text{cor}}} \lesssim 3 \cdot \mathcal{T}_A + O(q_G) \cdot (\mathcal{T}_{\text{Enc}} + \mathcal{T}_{\text{Dec}}) + O(q_G^2 + q_D^2)$ and

$$|\Pr[1 \leftarrow \mathbf{G}_3] - \Pr[1 \leftarrow \mathbf{G}_4]| \leq 4\sqrt{q_G + 1} \cdot \text{Adv}_{\mathbf{P}}^{\text{COR}}(\mathcal{A}_{\text{cor}}). \quad (52)$$

Game $\mathbf{G}_5$: This game is the same as game $\mathbf{G}_4$, except that k_0^* is replaced with a fresh uniformly random value k^* and G directly returns k^* if its input is (m^*, c^*) .

¹⁷ Note that $\mathcal{A}_{\text{cor}}$ can directly simulate G_1, G_2 , and 1_S for $\mathcal{C}$ since it knows sk .

Game $\mathbf{G}_5$ actually reprograms G at (m^*, c^*) to a fresh uniformly random value k^* before G is queried. Hence, as long as $G(m^*, c^*)$ in game $\mathbf{G}_4$ is uniformly random and $G(m^*, c^*)$ is independent of $G(m, c)$ for every $(m, c) \neq (m^*, c^*)$, the adversary $\mathcal{A}$ cannot detect the modification made in game $\mathbf{G}_5$. We next justify these two properties of $G(m^*, c^*)$. For the first property, since $G(m^*, c^*) = R(c^*)$ in game $\mathbf{G}_4$, $G(m^*, c^*)$ is indeed uniformly random. For the second property, observe that, as long as the following event **Bad** does not occur, there is no $(m, c) \neq (m^*, c^*)$ such that $\text{Enc}_{pk}(m) = c$ and $c = c^*$:

$$\text{Bad: } \exists m \neq m^* \text{ s.t. } \text{Enc}_{pk}(m) = \text{Enc}_{pk}(m^*), m^* \leftarrow_{\$} \mathcal{M}, (pk, sk) \leftarrow \text{Gen}. \quad (53)$$

This implies that, during the simulation of G in game $\mathbf{G}_4$, the value $R(c^*)$ is used only to answer the $G(m^*, c^*)$. Therefore, $G(m^*, c^*)$ is independent of $G(m, c)$ for every $(m, c) \neq (m^*, c^*)$, establishing the second property as well. Thus, we have

$$|\Pr[1 \leftarrow \mathbf{G}_4] - \Pr[1 \leftarrow \mathbf{G}_5]| \leq \Pr[\text{Bad}]. \quad (54)$$

As for the probability $\Pr[\text{Bad}]$, the following Lemma 5 ensures that

$$\Pr[\text{Bad}] \leq 2 \cdot e_{ac}, \quad (55)$$

Lemma 5 ([15, Lemma G1]). *Let $P = (\text{Gen}, \text{Enc}, \text{Dec})$ be a dPKE scheme with message space $\mathcal{M}$. For a fixed (pk, sk) , we define two sets $S_{pk,sk}^{\text{coll}} := \{m \in \mathcal{M} \mid \exists m' \in \mathcal{M} \text{ s.t. } m' \neq m \wedge \text{Enc}_{pk}(m') = \text{Enc}_{pk}(m)\}$ and $S_{pk,sk}^{\text{error}} := \{m \in \mathcal{M} \mid \text{Dec}_{sk}(\text{Enc}_{pk}(m)) \neq m\}$. Define $e_{ac} := \Pr[m \in S_{pk,sk}^{\text{error}} : m \leftarrow_{\$} \mathcal{M}, (pk, sk) \leftarrow \text{Gen}]$. Then we have $\Pr[m \in S_{pk,sk}^{\text{coll}} : m \leftarrow_{\$} \mathcal{M}, (pk, sk) \leftarrow \text{Gen}] \leq 2 \cdot e_{ac}$.*

Remark 4. Although the claim of [15, Lemma G1] is $\Pr[m \in S_{pk,sk}^{\text{coll}} : m \leftarrow_{\$} \mathcal{M}, (pk, sk) \leftarrow \text{Gen}] \leq 2 \cdot \delta_{ac}$, where δ_{ac} is the average-case decryption error of P , their proof actually first establishes $\Pr[m \in S_{pk,sk}^{\text{coll}} : m \leftarrow_{\$} \mathcal{M}, (pk, sk) \leftarrow \text{Gen}] \leq 2 \cdot e_{ac}$, and then derives the result from $e_{ac} \leq \delta_{ac}$. Therefore, the above lemma still follows from [15, Lemma G1]. Here, $e_{ac} \leq \delta_{ac}$ follows directly from the definition of δ_{ac} (Definition 3).

Game $\mathbf{G}_6$: This game is the same as game $\mathbf{G}_5$, except that the simulation of $G(m, c)$ no longer additionally checks whether $(m, c) = (m^*, c^*)$.

Similar to the game hop $\mathbf{G}_3$ to $\mathbf{G}_4$, as long as the adversary $\mathcal{A}$ does not query G on (m^*, c^*) , the modification made in game $\mathbf{G}_6$ cannot be detected by $\mathcal{A}$, and we also need to use the O2H theorem to formalize this argument. To this end, we first define a distribution $\mathfrak{D}$ over the tuple $(G, H, S, z = (pk, c^*, b, k_b^*, R))$ as shown in Fig. 11. We then define a quantum oracle algorithm $\mathcal{B}^O(z)$ ($O \in \{G, H\}$), which runs $\mathcal{A}^{O, \text{Deca}}(pk, c^*, k_b^*)$ to get b' and then outputs $\llbracket b = b' \rrbracket$. During the running, $\mathcal{B}^O(z)$ answers each $\text{Deca}(c)$ query with $R(c)$.

Observe that $\mathcal{B}^O(z)$ makes q_G queries to O and $\mathcal{T}_B \lesssim \mathcal{T}_A + O(q_G^2 + q_D^2)$. By the definitions of G and H in the above distribution $\mathfrak{D}$, we have

$$\begin{aligned} \Pr[1 \leftarrow \mathcal{B}^G(z) : (G, H, S, z) \leftarrow \mathfrak{D}] &= \Pr[1 \leftarrow \mathbf{G}_5], \\ \Pr[1 \leftarrow \mathcal{B}^H(z) : (G, H, S, z) \leftarrow \mathfrak{D}] &= \Pr[1 \leftarrow \mathbf{G}_6]. \end{aligned}$$

1. Sample $(pk, sk) \leftarrow \text{Gen}$, $m^* \leftarrow_{\$} \mathcal{M}$, $b \leftarrow_{\$} \{0, 1\}$, $k^* \leftarrow_{\$} \mathcal{K}$, and $k_b^* \leftarrow_{\$} \mathcal{K}$.
Sample G_1 (resp. R) as a $2q_G$ -wise (resp. $2(q_G + q_D)$ -wise) independent function.
2. Define $c^* := \text{Enc}_{pk}(m^*)$, $S := \{(m^*, c^*)\}$, $k_0^* := k^*$, $z := (pk, c^*, b, k_b^*, R)$.
3. Let H be a function that $H(m, c) = R(c)$ if $\text{Enc}_{pk}(m) = c$
and $H(m, c) = G_1(m, c)$ if $\text{Enc}_{pk}(m) \neq c$.
4. The function G is the same as H , except $G(m^*, c^*) := k^*$.

Fig. 11: The distribution $\mathfrak{D}$ of $(G, H, S, z := (pk, c^*, b, k_b^*, R))$. Here, the R in z is not represented by its value table, but by a description of a $2(q_G + q_D)$ -wise independent function.

Then, by using Theorem 4 and setting f as the function that maps $(m, c) \in \mathcal{M} \times \mathcal{C}$ to m , we can construct an algorithm $\mathcal{C}$ such that

$$|\Pr[1 \leftarrow \mathbf{G}_5] - \Pr[1 \leftarrow \mathbf{G}_6]| \leq 22 \cdot \text{Adv}(\mathcal{C}),$$

where

$$\text{Adv}(\mathcal{C}) := \Pr[m = m^* : m \leftarrow \mathcal{C}^{G, H}(z), (G, H, S, z) \leftarrow \mathfrak{D}].$$

Recall that $\mathcal{M} = \{0, 1\}^m$. Thus, $\mathcal{C}$ makes an expected $(2m + 5)q_G$ queries to G and an expected $(2m + 5)q_G$ queries to H , and $\mathcal{T}_{\mathcal{C}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_B$.

At this point, we can equivalently transform $\mathcal{C}$ into an adversary $\mathcal{A}_{\text{ow}}$ against the OW-CPA security of $\mathbf{P}$ as follows:

- $\mathcal{A}_{\text{ow}}$ gets the challenge ciphertext $c^* := \text{Enc}_{pk}(m^*)$ and public key pk , where m^* is the challenge plaintext uniformly sampled from $\mathcal{M}$ by the challenger and pk is sampled by $(pk, sk) \leftarrow \text{Gen}$.
- $\mathcal{A}_{\text{ow}}$ samples b, k^*, k_b^*, G_1 , and R according to the distribution $\mathfrak{D}$ in Fig. 11, and then uses $z := (pk, c^*, b, k_b^*, R)$ as input to run $\mathcal{C}^{G, H}(z)$ and simulates the oracles G and H for $\mathcal{C}$:
 1. When $\mathcal{C}$ queries G with input (m, c) :
 - (a) If $\text{Enc}_{pk}(m) = c^* \wedge c = c^*$, $\mathcal{A}_{\text{ow}}$ answers k^* .
 - (b) If $\text{Enc}_{pk}(m) \neq c^* \vee c \neq c^*$, but $\text{Enc}_{pk}(m) = c$, $\mathcal{A}_{\text{ow}}$ answers $R(c)$.
 - (c) Otherwise, $\mathcal{A}_{\text{ow}}$ answers $G_1(m, c)$.
 2. When $\mathcal{C}$ queries H with input (m, c) , $\mathcal{A}_{\text{ow}}$ answers $R(c)$ if $\text{Enc}_{pk}(m) = c$, and answers $G_1(m, c)$ otherwise.
- After $\mathcal{C}$ returns m , $\mathcal{A}_{\text{ow}}$ outputs m .

One can check that the running time of $\mathcal{A}_{\text{ow}}$ is $\mathcal{T}_{\mathcal{A}_{\text{ow}}}^{\text{exp}} \lesssim \mathcal{T}_{\mathcal{C}}^{\text{exp}} + O(mq_G) \cdot \mathcal{T}_{\text{Enc}} + O(mq_G^2 + mq_D^2)$. In the above construction, since $\mathcal{A}_{\text{ow}}$ cannot get the challenge plaintext m^* directly, it checks whether m equals m^* by testing whether $\text{Enc}_{pk}(m)$ equals c^* during the simulation of oracle G for $\mathcal{C}$. In fact, since m^* is uniformly sampled from $\mathcal{M}$ by the challenger, $\mathcal{A}_{\text{ow}}$ simulates the oracle G for $\mathcal{C}$

perfectly¹⁸ if the event **Bad** (Eq. (53)) does not occur. Thus we have

$$\text{Adv}(\mathcal{C}) \leq \text{Adv}_{\mathbf{P}}^{\text{OW-CPA}}(\mathcal{A}_{\text{ow}}) + \Pr[\text{Bad}] \stackrel{\text{Lem. 5}}{\leq} \text{Adv}_{\mathbf{P}}^{\text{OW-CPA}}(\mathcal{A}_{\text{ow}}) + 2 \cdot e_{ac}.$$

Combining the above analysis and three equations, we have $\mathcal{T}_{\mathcal{A}_{\text{ow}}}^{\text{exp}} \lesssim (2m+5) \cdot \mathcal{T}_{\mathcal{A}} + O(mq_G) \cdot \mathcal{T}_{\text{Enc}} + O(mq_G^2 + mq_D^2)$ and

$$|\Pr[1 \leftarrow \mathbf{G}_5] - \Pr[1 \leftarrow \mathbf{G}_6]| \leq 22 \cdot \text{Adv}_{\mathbf{P}}^{\text{OW-CPA}}(\mathcal{A}_{\text{ow}}) + 44 \cdot e_{ac}. \quad (56)$$

As for the probability $\Pr[1 \leftarrow \mathbf{G}_6]$, since the adversary $\mathcal{A}$'s view in game $\mathbf{G}_6$ is independent of b , we have

$$\Pr[1 \leftarrow \mathbf{G}_6] = \frac{1}{2}. \quad (57)$$

By combining Eq. (48) to Eq. (52) and Eq. (54) to Eq. (57), we finally have

$$\begin{aligned} \text{Adv}_{\mathcal{U}^{\perp}[\mathbf{P}, \mathbf{G}, \mathbf{F}]}^{\text{IND-CCA}}(\mathcal{A}) &\leq \text{Adv}_{\mathbf{F}}^{\text{PRF}}(\mathcal{A}_{\text{prf}}) + 22 \cdot \text{Adv}_{\mathbf{P}}^{\text{OW-CPA}}(\mathcal{A}_{\text{ow}}) \\ &\quad + 4\sqrt{q_G + 1} \cdot \text{Adv}_{\mathbf{P}}^{\text{COR}}(\mathcal{A}_{\text{cor}}) + 46 \cdot e_{ac}. \end{aligned}$$

We point out that the term e_{ac} can be absorbed into $\text{Adv}_{\mathbf{P}}^{\text{COR}}(\mathcal{A}_{\text{cor}})$. By the definition of the **COR** game (Definition 4), e_{ac} equals the advantage of a particular adversary $\mathcal{A}_{\text{cor}}^1$ against the **COR** game. This adversary simply outputs a uniformly sampled m . Therefore, let $\mathcal{A}_{\text{cor}}^2$ be a new adversary that runs $\mathcal{A}_{\text{cor}}$ with probability $4\sqrt{q_G + 1}/(4\sqrt{q_G + 1} + 46)$ and runs $\mathcal{A}_{\text{cor}}^1$ with probability $46/(4\sqrt{q_G + 1} + 46)$. We then have $(4\sqrt{q_G + 1} + 46) \cdot \text{Adv}(\mathcal{A}_{\text{cor}}^2) = 4\sqrt{q_G + 1} \cdot \text{Adv}(\mathcal{A}_{\text{cor}}) + 46 \cdot e_{ac}$. Thus, by renaming $\mathcal{A}_{\text{cor}}^2$ as $\mathcal{A}_{\text{cor}}$, we obtain

$$\begin{aligned} \text{Adv}_{\mathcal{U}^{\perp}[\mathbf{P}, \mathbf{G}, \mathbf{F}]}^{\text{IND-CCA}}(\mathcal{A}) &\leq \text{Adv}_{\mathbf{F}}^{\text{PRF}}(\mathcal{A}_{\text{prf}}) + 22 \cdot \text{Adv}_{\mathbf{P}}^{\text{OW-CPA}}(\mathcal{A}_{\text{ow}}) \\ &\quad + (4\sqrt{q_G + 1} + 46) \cdot \text{Adv}_{\mathbf{P}}^{\text{COR}}(\mathcal{A}_{\text{cor}}). \end{aligned}$$

This completes the proof of Theorem 6. $\square$

E Proof of Theorem 8

Proof. To prove Theorem 8, we define a sequence of games $\mathbf{G}_0$ to $\mathbf{G}_4$ (Fig. 12).

Game $\mathbf{G}_0$: This is the IND-CPA game of $\text{KEM}_m^{\perp}$ with the adversary $\mathcal{A}$ in the QROM. Obviously, we have

$$\text{Adv}_{\text{KEM}_m^{\perp}}^{\text{IND-CPA}}(\mathcal{A}) = \left| \Pr[1 \leftarrow \mathbf{G}_0] - \frac{1}{2} \right|. \quad (58)$$

Game $\mathbf{G}_1$: In this game, a new random oracle $F : \mathcal{M} \rightarrow \mathcal{R} \times \mathcal{K}$ is introduced, where $\mathcal{R} = \{0, 1\}^r$ and $\mathcal{K} = \{0, 1\}^k$. Then, the r^* and k_0^* is generated as $(r^*, k_0^*) = F(m^*)$ and the adversary $\mathcal{A}$ is replaced by a new adversary $\mathcal{A}_1$, which runs $\mathcal{A}$ and simulates G and H for $\mathcal{A}$ by querying F as follows:

¹⁸ Here the "perfectly" means that, in $\mathcal{C}$'s view, the oracle G simulated by $\mathcal{A}_{\text{ow}}$ is perfectly indistinguishable with the oracle G obtained by sampling (G, H, S, z) according to the distribution $\mathfrak{D}$ in Fig. 11.

- For a G query $\sum_{x,y} \alpha_{x,y} |x, y\rangle$ ¹⁹, $\mathcal{A}_1$ queries F on $\sum_{x,y,z \in \mathcal{R}} \alpha_{x,y} / \sqrt{2^r} |x, z, y\rangle$. Here, x denotes the value in the input register, while (z, y) denotes the values in the output register. Similarly, for an H query $\sum_{x,y} \alpha_{x,y} |x, y\rangle$, $\mathcal{A}_1$ queries F on $\sum_{x,y,z \in \mathcal{K}} \alpha_{x,y} / \sqrt{2^k} |x, y, z\rangle$. Here, x denotes the value in the input register, while (y, z) denotes the values in the output register.

Clearly, $\mathcal{A}_1$ makes $q_G + q_H$ queries to F . Note that game $\mathbf{G}_1$ essentially combines the two random oracles G and H into a single F , using the basic properties of random oracles. Hence, game $\mathbf{G}_1$ is equivalent to game $\mathbf{G}_0$. Thus

$$\Pr[1 \leftarrow \mathbf{G}_0] = \Pr[1 \leftarrow \mathbf{G}_1]. \quad (59)$$

GAMES $\mathbf{G}_0$ - $\mathbf{G}_4$		$F(m)$ // $\mathbf{G}_1$ - $\mathbf{G}_2$
1 : $(pk, sk) \leftarrow \text{Gen}$	// $\mathbf{G}_0$ - $\mathbf{G}_4$	1 : return $F_1(m)$
2 : $H \leftarrow_{\$} \Omega_{\mathcal{M} \rightarrow \mathcal{R}}, G \leftarrow_{\$} \Omega_{\mathcal{M} \rightarrow \mathcal{K}}$	// $\mathbf{G}_0$	
3 : $F_1 \leftarrow_{\$} \Omega_{\mathcal{M} \rightarrow \mathcal{R} \times \mathcal{K}}$	// $\mathbf{G}_1$ - $\mathbf{G}_4$	$F(m)$ // $\mathbf{G}_3$
4 : $m^* \leftarrow_{\$} \mathcal{M}$	// $\mathbf{G}_0$ - $\mathbf{G}_1$	1 : if $m = m_0$
5 : $m_0 \leftarrow_{\$} \mathcal{M}, m_1 \leftarrow_{\$} \mathcal{M} \setminus \{m_0\}$	// $\mathbf{G}_2$ - $\mathbf{G}_4$	2 : return (r_0, k_0)
6 : $c \leftarrow_{\$} \{0, 1\}, m^* := m_c$	// $\mathbf{G}_2$ - $\mathbf{G}_4$	3 : else if $m = m_1$
7 : $(r^*, k_0^*) := (H(m^*), G(m^*))$	// $\mathbf{G}_0$	4 : return (r_1, k_1)
8 : $(r^*, k_0^*) := F(m^*)$	// $\mathbf{G}_1$ - $\mathbf{G}_2$	5 : else return $F_1(m)$
9 : $(r_0, k_0) \leftarrow_{\$} \mathcal{R} \times \mathcal{K}, (r_1, k_1) \leftarrow_{\$} \mathcal{R} \times \mathcal{K}$	// $\mathbf{G}_3$ - $\mathbf{G}_4$	
10 : $(r^*, k_0^*) := (r_c, k_c)$	// $\mathbf{G}_3$ - $\mathbf{G}_4$	$F(m)$ // $\mathbf{G}_4$
11 : $c^* := \text{Enc}_{pk}(m^*; r^*)$	// $\mathbf{G}_0$ - $\mathbf{G}_4$	1 : return $F_1(m)$
12 : $b \leftarrow_{\$} \{0, 1\}, k_1^* \leftarrow_{\$} \mathcal{K}$	// $\mathbf{G}_0$ - $\mathbf{G}_4$	
13 : $b' \leftarrow \mathcal{A}^{G,H}(pk, c^*, k_b^*)$	// $\mathbf{G}_0$	
14 : $b' \leftarrow \mathcal{A}_1^F(pk, c^*, k_b^*)$	// $\mathbf{G}_1$ - $\mathbf{G}_4$	
15 : return $\llbracket b' = b \rrbracket$	// $\mathbf{G}_0$ - $\mathbf{G}_4$	

Fig. 12: Games $\mathbf{G}_0$ - $\mathbf{G}_4$ for the proof of Theorem 8. Note that the oracle F can be quantumly accessed in those games. In this figure, we just write the classical description of F for brevity.

Game $\mathbf{G}_2$: This game is the same as game $\mathbf{G}_1$, except that it samples $m_0 \leftarrow_{\$} \mathcal{M}$, $m_1 \leftarrow_{\$} \mathcal{M} \setminus \{m_0\}$, $c \leftarrow_{\$} \{0, 1\}$, and then sets $m^* := m_c$. Observe that the m^* sampled in this game is still uniformly distributed over $\mathcal{M}$. Hence,

$$\Pr[1 \leftarrow \mathbf{G}_1] = \Pr[1 \leftarrow \mathbf{G}_2]. \quad (60)$$

¹⁹ Here for simplicity, we omit the values that may be entangled with x and y .

Game $\mathbf{G_3}$: This game first samples $(r_0, k_0) \leftarrow_{\$} \mathcal{R} \times \mathcal{K}$ and $(r_1, k_1) \leftarrow_{\$} \mathcal{R} \times \mathcal{K}$. Then, it reprograms F at m_0 and m_1 to (r_0, k_0) and (r_1, k_1) , respectively, and accordingly sets $(r^*, k_0^*) := (r_c, k_c)$.

Since game $\mathbf{G_3}$ reprograms F at m_0 and m_1 with fresh uniformly random values before any query to F is made, it is equivalent to game $\mathbf{G_2}$. Hence,

$$\Pr[1 \leftarrow \mathbf{G_2}] = \Pr[1 \leftarrow \mathbf{G_3}]. \quad (61)$$

Game $\mathbf{G_4}$: This game is the same as game $\mathbf{G_3}$, except that the reprogramming of F at m_0 and m_1 is removed. Namely, during the simulation of F , it no longer checks whether m equals m_0 or m_1 and directly returns $F_1(m)$.

It is obvious that, as long as the adversary $\mathcal{A}_1$ does not query F on m_0 or m_1 , the modification made in game $\mathbf{G_4}$ cannot be detected by $\mathcal{A}_1$. However, since F can be quantumly accessed, we need to use the O2H theorem to formalize this argument. To this end, we first define a distribution $\mathfrak{D}$ over the tuple $(G, H, S, z := (pk, c^*, b, k_b^*))$ as shown in Fig. 13.

1. Sample $(pk, sk) \leftarrow \text{Gen}$, $m_0 \leftarrow_{\$} \mathcal{M}$, $m_1 \leftarrow_{\$} \mathcal{M} \setminus \{m_0\}$, $b \leftarrow_{\$} \{0, 1\}$, and $c \leftarrow_{\$} \{0, 1\}$.
 Sample $(r_0, k_0) \leftarrow_{\$} \mathcal{R} \times \mathcal{K}$, $(r_1, k_1) \leftarrow_{\$} \mathcal{R} \times \mathcal{K}$, and $k_1^* \leftarrow_{\$} \mathcal{K}$.
 Sample G as a $2(q_G + q_H)$ -wise independent function.
2. Define $k_0^* := k_c$, $c^* := \text{Enc}_{pk}(m_c; r_c)$, $S := \{m_0, m_1\}$, and $z := (pk, c^*, b, k_b^*)$.
 The function H is the same as G , except $H(m_0) := (r_0, k_0)$ and $H(m_1) := (r_1, k_1)$.

Fig. 13: The distribution $\mathfrak{D}$ of $(G, H, S, z := (pk, c^*, b, k_b^*))$.

We then define a new quantum oracle algorithm $\mathcal{A}_2^O(z)$ ($O \in \{G, H\}$), which runs $\mathcal{A}_1^O(pk, c^*, k_b^*)$ to get b' and then outputs $\llbracket b = b' \rrbracket$. Note that $\mathcal{A}_2^O(z)$ makes $q_G + q_H$ queries to O and $\mathcal{T}_{\mathcal{A}_2} \approx \mathcal{T}_{\mathcal{A}}$. By the definitions of G and H in the distribution $\mathfrak{D}$, we have

$$\begin{aligned} \Pr[1 \leftarrow \mathcal{A}_2^H(z) : (G, H, S, z) \leftarrow \mathfrak{D}] &= \Pr[1 \leftarrow \mathbf{G_3}], \\ \Pr[1 \leftarrow \mathcal{A}_2^G(z) : (G, H, S, z) \leftarrow \mathfrak{D}] &= \Pr[1 \leftarrow \mathbf{G_4}]. \end{aligned} \quad (62)$$

Now, by using Theorem 2, we can construct an algorithm $\mathcal{D}^{G, 1_S}(z)$ such that

$$\begin{aligned} &|\Pr[1 \leftarrow \mathbf{G_3}] - \Pr[1 \leftarrow \mathbf{G_4}]| \\ &\leq 22\sqrt{q_G + q_H + 1} \cdot \Pr_{(G, H, S, z) \leftarrow \mathfrak{D}}[x \in S : x \leftarrow \mathcal{D}^{G, 1_S}(z)] \\ &\stackrel{(a)}{\leq} 22\sqrt{q_G + q_H + 1} \cdot \Pr_{(G, H, S, z) \leftarrow \mathfrak{D}}[x \in \{m_c, m_{1-c}\} : x \leftarrow \mathcal{D}^{G, 1_S}(z)] \end{aligned}$$

$$\begin{aligned}
&\stackrel{(b)}{=} 22\sqrt{q_G + q_H + 1} \cdot \Pr_{(G,H,S,z) \leftarrow \mathfrak{D}} [x = m_c : x \leftarrow \mathcal{D}^{G,1_S}(z)] \\
&\quad + 22\sqrt{q_G + q_H + 1} \cdot \Pr_{(G,H,S,z) \leftarrow \mathfrak{D}} [x = m_{1-c} : x \leftarrow \mathcal{D}^{G,1_S}(z)].
\end{aligned} \tag{63}$$

Here (a) is because $S = \{m_0, m_1\}$ and (b) is because $m_0 \neq m_1$. Since $\mathcal{M} = \{0, 1\}^m$, $\mathcal{D}^{G,1_S}(z)$ makes an expected $(2m+5)(q_G+q_H)$ (resp. $(4m+10)(q_G+q_H)$) queries to G (resp. 1_S), and has running time $\mathcal{T}_{\mathcal{D}}^{\text{exp}} \lesssim (2m+5) \cdot \mathcal{T}_{\mathcal{A}_2}$.

For the probability $\Pr[1 \leftarrow \mathbf{G}_4]$, since k_0^* is sampled uniformly at random from the two independent uniformly random values k_0 and k_1 , k_0^* remains uniformly random. This implies that both k_0^* and k_1^* in game $\mathbf{G}_4$ are uniformly random, and hence the view of the adversary $\mathcal{A}_1$ is independent of b . Thus,

$$\Pr[1 \leftarrow \mathbf{G}_4] = \frac{1}{2}. \tag{64}$$

In the following, based on the algorithm $\mathcal{D}^{G,1_S}(z)$, we define an IND-CPA adversary $\mathcal{A}_{\text{ind}}$ against $\mathbf{P}$ as follows:

- After getting the public key pk , $\mathcal{A}_{\text{ind}}$ samples $m_0 \leftarrow_{\$} \mathcal{M}$, $m_1 \leftarrow_{\$} \mathcal{M} \setminus \{m_0\}$ and then sends (m_0, m_1) to the challenger.
- The challenger returns the challenge ciphertext $c^* := \text{Enc}_{pk}(m_c; r^*)$ to $\mathcal{A}_{\text{ind}}$, where $c \leftarrow_{\$} \{0, 1\}$ and $r^* \leftarrow_{\$} \mathcal{R}$.
- $\mathcal{A}_{\text{ind}}$ samples G as a $2(q_G + q_H)$ -wise independent function, samples $b \leftarrow_{\$} \{0, 1\}$ and $k_b^* \leftarrow_{\$} \mathcal{K}$, and then runs $\mathcal{D}^{G,1_S}(z)$ with $z := (pk, c^*, b, k_b^*)$. Since $\mathcal{A}_{\text{ind}}$ samples G itself and knows both m_0 and m_1 , it can directly simulate the oracles G and 1_S for $\mathcal{D}^{G,1_S}(z)$.
- After $\mathcal{D}^{G,1_S}(z)$ returns x , $\mathcal{A}_{\text{ind}}$ outputs $c' := 1$ (resp. $c' := 0$) if $x = m_0$ (resp. $x = m_1$), and outputs a random bit as c' otherwise.

It is straightforward to verify that $\mathcal{A}_{\text{ind}}$ perfectly simulates the environment of $\mathcal{D}^{G,1_S}(z)$ ²⁰ and $\mathcal{T}_{\mathcal{A}_{\text{ind}}}^{\text{exp}} \lesssim \mathcal{T}_{\mathcal{D}}^{\text{exp}} + O(mq_G^2 + mq_H^2)$. The advantage of $\mathcal{A}_{\text{ind}}$ against the IND-CPA security of $\mathbf{P}$ can be computed as:

$$\begin{aligned}
\text{Adv}_{\mathbf{P}}^{\text{IND-CPA}}(\mathcal{A}_{\text{ind}}) &= \left| \Pr[c' = c : c' \leftarrow \mathcal{A}_{\text{ind}}] - \frac{1}{2} \right| \\
&= \frac{1}{2} |\Pr[c' = c : c' \leftarrow \mathcal{A}_{\text{ind}}] - \Pr[c' \neq c : c' \leftarrow \mathcal{A}_{\text{ind}}]| \\
&= \frac{1}{2} \left| \Pr_{(G,H,S,z) \leftarrow \mathfrak{D}} [x = m_c : x \leftarrow \mathcal{D}^{G,1_S}(z)] - \Pr_{(G,H,S,z) \leftarrow \mathfrak{D}} [x = m_{1-c} : x \leftarrow \mathcal{D}^{G,1_S}(z)] \right|.
\end{aligned}$$

²⁰ This is because the values m_c , r_c , k_c , and k_1^* sampled in the distribution $\mathfrak{D}$ are all uniformly distributed over their respective sets. Therefore, the c^* generated according to $\mathfrak{D}$ has the same distribution as that generated by the IND-CPA challenger, while the k_b^* generated according to $\mathfrak{D}$ is also a uniformly random value over $\mathcal{K}$.

Combining the above equation with Eq. (63), we obtain

$$\begin{aligned}
& |\Pr[1 \leftarrow \mathbf{G}_3] - \Pr[1 \leftarrow \mathbf{G}_4]| \\
& \leq 44\sqrt{q_G + q_H + 1} \cdot \text{Adv}_{\mathbf{P}}^{\text{IND-CPA}}(\mathcal{A}_{\text{ind}}) \\
& \quad + 44\sqrt{q_G + q_H + 1} \cdot \Pr_{(G,H,S,z) \leftarrow \mathfrak{D}}[x = m_{1-c} : x \leftarrow \mathcal{D}^{G,1s}(z)].
\end{aligned} \tag{65}$$

For the final probability $\Pr_{(G,H,S,z) \leftarrow \mathfrak{D}}[x = m_{1-c} : x \leftarrow \mathcal{D}^{G,1s}(z)]$, we can prove the following lemma. The detailed proof is given in Supplementary Material E.1.

Lemma 6. *We have $\Pr_{(G,H,S,z) \leftarrow \mathfrak{D}}[x = m_{1-c} : x \leftarrow \mathcal{D}^{G,1s}(z)] \leq 25\sqrt{\frac{q_G + q_H}{|\mathcal{M}| - 1}}$.*

Finally, by combining Eq. (58) to Eq. (61), Eq. (64), Eq. (65), and Lemma 6, we obtain

$$\text{Adv}_{\text{KEM}_m^\perp}^{\text{IND-CPA}}(\mathcal{A}) \leq 44\sqrt{q_G + q_H + 1} \cdot \text{Adv}_{\mathbf{P}}^{\text{IND-CPA}}(\mathcal{A}_{\text{ind}}) + 1100 \cdot \frac{q_G + q_H + 1}{\sqrt{|\mathcal{M}| - 1}}.$$

This completes the proof of Theorem 8. $\square$

E.1 Proof of Lemma 6

Proof. We first give the detailed construction of $\mathcal{D}^{G,1s}(z)$ based on the algorithm $\mathcal{A}_2^O(z)$ used in Eq. (62) and the proofs of Theorems 1 and 2. By denoting the initial state of $\mathcal{A}_2^O(z)$ as $|\psi_z\rangle := U_z|0^a\rangle$ and then denoting $U_1, \dots, U_q$ ($q := q_G + q_H$) as the unitary operations performed by $\mathcal{A}_2^O(z)$ between its oracle queries, the detailed construction of $\mathcal{D}^{G,1s}(z)$ is as follows:

- With probability $1/11$, $\mathcal{D}^{G,1s}(z)$ directly samples $x \leftarrow_{\S} \mathcal{M}$ and outputs x .
- With probability $10/11$, $\mathcal{D}^{G,1s}(z)$ sets $\epsilon := 1/2^m$ and then runs $\mathcal{C}_\epsilon^{G,1s}(z)$, which performs the following operations:
 1. Initialize the state $|0^a\rangle|0, 0^m\rangle_{\text{BT}}$ and sample k according to the distribution $\mathfrak{D}_\epsilon$ defined in Table 4.
 2. Perform $(Am)^k U_{\mathcal{B}}$, where $U_{\mathcal{B}} := \prod_{i=1}^q [U_i O_G U_S^i] U_z$ and

$$Am := U_{\mathcal{B}} \circ (2|0^a\rangle|0, 0^m\rangle_{\text{BT}} \langle 0^a| \langle 0, 0^m|_{\text{BT}} - I) \circ U_{\mathcal{B}}^\dagger \circ (2|0\rangle\langle 0|_{\text{B}} - I_{\text{B}}).$$

The $O_G : |x, y\rangle \mapsto |x, y \oplus G(x)\rangle$ used by $U_{\mathcal{B}}$ can be implemented with a single query to G . The U_S^i used by $U_{\mathcal{B}}$ is defined in Eq. (6) and can be implemented with two queries to 1_S ²¹.

3. Measure BT in the computational basis to get the measurement outcome (b, t) . If $b \neq 0$, output t . Otherwise, output $\perp$.

²¹ This point has already been explained in the proof of Theorem 1 when constructing the algorithm $\mathcal{B}^{G,1s}(z)$; see the analysis after Eq. (11).

Therefore, we have

$$\begin{aligned} & \Pr_{(G,H,S,z) \leftarrow \mathfrak{D}} [x = m_{1-c} : x \leftarrow \mathcal{D}^{G,1S}(z)] \\ &= \frac{1}{11} \cdot \frac{1}{|\mathcal{M}|} + \frac{10}{11} \cdot \Pr_{(G,H,S,z) \leftarrow \mathfrak{D}} [x = m_{1-c} : x \leftarrow \mathcal{C}_\epsilon^{G,1S}(z)]. \end{aligned} \quad (66)$$

Next, for an arbitrary fixed tuple (G, H, S, z) in the support of the distribution $\mathfrak{D}$ (Fig. 13), we analyze the probability $\Pr[x = m_{1-c} : x \leftarrow \mathcal{C}_\epsilon^{G,1S}(z)]$. First, since $S = \{m_0, m_1\}$ and $m_0 \neq m_1$, the state $|\psi_S\rangle$ defined in Eq. (15) in the proof of Theorem 1 becomes

$$\begin{aligned} |\psi_S\rangle &= \sum_{j=1}^q \prod_{i=j}^q [U_i O_G] |m_c\rangle \langle m_c| \prod_{i=1}^{j-1} [U_i O_G \Pi_\perp] |\psi_z\rangle |j, m_c\rangle_{\text{BT}} \\ &\quad + \sum_{j=1}^q \prod_{i=j}^q [U_i O_G] |m_{1-c}\rangle \langle m_{1-c}| \prod_{i=1}^{j-1} [U_i O_G \Pi_\perp] |\psi_z\rangle |j, m_{1-c}\rangle_{\text{BT}}, \end{aligned}$$

where $\Pi_\perp = I - |m_c\rangle \langle m_c| - |m_{1-c}\rangle \langle m_{1-c}|$. We define

$$\begin{aligned} |\psi_{m_c}\rangle &:= \sum_{j=1}^q \prod_{i=j}^q [U_i O_G] |m_c\rangle \langle m_c| \prod_{i=1}^{j-1} [U_i O_G \Pi_\perp] |\psi_z\rangle |j, m_c\rangle_{\text{BT}}, \\ |\psi_{m_{1-c}}\rangle &:= \sum_{j=1}^q \prod_{i=j}^q [U_i O_G] |m_{1-c}\rangle \langle m_{1-c}| \prod_{i=1}^{j-1} [U_i O_G \Pi_\perp] |\psi_z\rangle |j, m_{1-c}\rangle_{\text{BT}}. \end{aligned} \quad (67)$$

Then, $|\psi_{m_c}\rangle$ and $|\psi_{m_{1-c}}\rangle$ are orthogonal whenever they are nonzero and

$$|\psi_S\rangle = |\psi_{m_c}\rangle + |\psi_{m_{1-c}}\rangle. \quad (68)$$

Define $\theta := \arcsin(\| |\psi_S\rangle \|)$. At this point, according to Eq. (17) and Eq. (20), for a fixed number of iterations k sampled from $\mathfrak{D}_\epsilon$, the whole state of $\mathcal{C}_\epsilon^{G,1S}(z)$ before performing the final measurement on the registers BT is

$$\begin{aligned} & \cos((2k+1)\theta) \cdot |\psi_{bad}\rangle + \sin((2k+1)\theta) \cdot |\psi_{good}\rangle \\ &= \begin{cases} \prod_{i=1}^q [U_i O_G \Pi_\perp] |\psi_z\rangle |0, 0^m\rangle_{\text{BT}} & \text{if } \theta = 0, \\ \frac{\sin((2k+1)\theta)}{\sin(\theta)} (|\psi_{m_c}\rangle + |\psi_{m_{1-c}}\rangle) & \text{if } \theta = \pi/2, \\ \frac{\cos((2k+1)\theta)}{\cos(\theta)} \prod_{i=1}^q [U_i O_G \Pi_\perp] |\psi_z\rangle |0, 0^m\rangle_{\text{BT}} \\ \quad + \frac{\sin((2k+1)\theta)}{\sin(\theta)} (|\psi_{m_c}\rangle + |\psi_{m_{1-c}}\rangle) & \text{if } 0 < \theta < \pi/2. \end{cases} \end{aligned}$$

Thus, by the definition of $\mathcal{C}_\epsilon^{G,1s}(z)$ given at the beginning of the proof, we can compute

$$\Pr[x = m_{1-c} : x \leftarrow \mathcal{C}_\epsilon^{G,1s}(z)] = \begin{cases} 0 & \text{if } \theta = 0, \\ \sum_{l=0}^L \frac{1}{T \cdot 2^l} \frac{\sin^2((2 \cdot 2^l + 1)\theta)}{\sin^2(\theta)} \|\psi_{m_{1-c}}\|^2 & \text{if } 0 < \theta \leq \pi/2. \end{cases} \quad (69)$$

When $\theta \neq 0$, we sum over l because in $\mathcal{C}_\epsilon^{G,1s}(z)$ the iteration number k is sampled according to the distribution $\mathfrak{D}_\epsilon$ (Table 4). Next, to derive an upper bound on $\Pr[x = m_{1-c} : x \leftarrow \mathcal{C}_\epsilon^{G,1s}(z)]$, we introduce the following lemma. The proof of this lemma is given in Supplementary Material E.2.

Lemma 7. *For any $0 < \theta \leq \pi/2$, $\sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta) \leq 12 \sin(\theta)$.*

If $\theta = 0$, then $\|\psi_S\| = 0$, and hence $|\psi_S\rangle = \mathbf{0}$. By Eq. (67), the states $|\psi_{m_c}\rangle$ and $|\psi_{m_{1-c}}\rangle$ are orthogonal whenever they are nonzero. Hence, by Eq. (68), when $\theta = 0$, we must have $|\psi_{m_c}\rangle = |\psi_{m_{1-c}}\rangle = \mathbf{0}$, and thus $\|\psi_{m_{1-c}}\| = 0$. That is to say, when $\theta = 0$, we have $\Pr[x = m_{1-c} : x \leftarrow \mathcal{C}_\epsilon^{G,1s}(z)] = 0$ (Eq. (69)) and $\|\psi_{m_{1-c}}\| = 0$, which obviously implies

$$\Pr[x = m_{1-c} : x \leftarrow \mathcal{C}_\epsilon^{G,1s}(z)] \leq 12 \cdot \|\psi_{m_{1-c}}\|.$$

If $0 < \theta \leq \pi/2$, by using Eq. (69) and Lemma 7, we can compute

$$\begin{aligned} \Pr[x = m_{1-c} : x \leftarrow \mathcal{C}_\epsilon^{G,1s}(z)] &= \sum_{l=0}^L \frac{1}{T \cdot 2^l} \frac{\sin^2((2 \cdot 2^l + 1)\theta)}{\sin^2(\theta)} \|\psi_{m_{1-c}}\|^2 \\ &\leq 12 \cdot \frac{\|\psi_{m_{1-c}}\|^2}{\sin(\theta)} \\ &= 12 \cdot \frac{\|\psi_{m_{1-c}}\|^2}{\|\psi_S\|} \stackrel{(a)}{\leq} 12 \cdot \|\psi_{m_{1-c}}\|. \end{aligned}$$

Here (a) follows from $\|\psi_S\| \geq \|\psi_{m_{1-c}}\|$, which can be derived by Eq. (68) and the fact that the states $|\psi_{m_c}\rangle$ and $|\psi_{m_{1-c}}\rangle$ defined in Eq. (67) are orthogonal whenever they are nonzero.

The above analysis shows that we always have $\Pr[x = m_{1-c} : x \leftarrow \mathcal{C}_\epsilon^{G,1s}(z)] \leq 12 \cdot \|\psi_{m_{1-c}}\|$. Hence, by averaging over $(G, H, S, z) \leftarrow \mathfrak{D}$ and using the Jensen's inequality, we have

$$\begin{aligned} \Pr_{(G,H,S,z) \leftarrow \mathfrak{D}}[x = m_{1-c} : x \leftarrow \mathcal{C}_\epsilon^{G,1s}(z)] &\leq 12 \cdot \mathbb{E}_{(G,H,S,z) \leftarrow \mathfrak{D}} \|\psi_{m_{1-c}}\| \\ &= 12 \cdot \mathbb{E}_{(G,H,S,z) \leftarrow \mathfrak{D}} \sqrt{\|\psi_{m_{1-c}}\|^2} \\ &\leq 12 \cdot \sqrt{\mathbb{E}_{(G,H,S,z) \leftarrow \mathfrak{D}} \|\psi_{m_{1-c}}\|^2}. \end{aligned} \quad (70)$$

In the following, for an arbitrary fixed tuple (G, H, S, z) in the support of the distribution $\mathfrak{D}$ (Fig. 13), we construct an algorithm $\mathcal{D}_1$ that queries the semi-classical oracle $\mathcal{O}_{\{m_{1-c}\}}^{SC}$ (Definition 1) as follows:

- In addition to the input $z = (pk, c^*, b, k_b^*)$, $\mathcal{D}_1$ is also given m_c and G generated when (G, H, S, z) is sampled according to $\mathfrak{D}$.
- $\mathcal{D}_1$ initializes the state $|0^a\rangle$, applies U_z to obtain $|\psi_z\rangle$, and then performs $\prod_{i=1}^q [U_i O_G \mathbb{M}_c \mathbb{M}_{1-c}]$.
 1. The unitary operation $O_G : |x, y\rangle \mapsto |x, y \oplus G(x)\rangle$ can be implemented by $\mathcal{D}_1$ since it is given G as input.
 2. The measurement $\mathbb{M}_c := \{\Pi_1 := |m_c\rangle\langle m_c|, \Pi_0 := I - \Pi_1\}$ acts on the input register of O_G and can be implemented by $\mathcal{D}_1$ since it is given m_c as input.
 3. The measurement $\mathbb{M}_{1-c} := \{\tilde{\Pi}_1 := |m_{1-c}\rangle\langle m_{1-c}|, \tilde{\Pi}_0 := I - \tilde{\Pi}_1\}$ acts on the input register of O_G and can be implemented using one query to $\mathcal{O}_{\{m_{1-c}\}}^{SC}$.
- Measure all registers in the computational basis and output the measurement outcome.²²

Note that $\mathcal{D}_1$ queries $\mathcal{O}_{\{m_{1-c}\}}^{SC}$ q times, where $q = q_G + q_H$. Next, we define the following events that may occur during the execution of $\mathcal{D}_1$:

- **Find**: The measurement $\mathbb{M}_{1-c}$, which is implemented by querying $\mathcal{O}_{\{m_{1-c}\}}^{SC}$, ever has outcome 1.
- **Find _{i}** ($i \in \{1, \dots, q\}$): The first $i - 1$ measurements $\mathbb{M}_{1-c}$ have outcome 0, while the i -th measurement $\mathbb{M}_{1-c}$ has outcome 1.
- **$\neg$ Find _{i} ^c** ($i \in \{0, 1, \dots, q\}$): The first i measurements $\mathbb{M}_c$ have outcome 0. For $i = 0$, we define $\neg$ Find₀^c to be the sure event.

For any $i \in \{1, \dots, q\}$, the event **Find _{i}** $\wedge$ $\neg$ Find _{$i-1$} ^c means that, the first $i - 1$ measurements $\mathbb{M}_c$ and the first $i - 1$ measurements $\mathbb{M}_{1-c}$ all have outcome 0, while the i -th measurement $\mathbb{M}_{1-c}$ has outcome 1. Therefore, we have

$$\begin{aligned} \Pr \left[\text{Find}_i : \mathcal{D}_1^{\mathcal{O}_{\{m_{1-c}\}}^{SC}}(z, m_c, G) \right] &\geq \Pr \left[\text{Find}_i \wedge \neg \text{Find}_{i-1}^c : \mathcal{D}_1^{\mathcal{O}_{\{m_{1-c}\}}^{SC}}(z, m_c, G) \right] \\ &= \left\| |m_{1-c}\rangle\langle m_{1-c}| \prod_{j=1}^{i-1} [U_j O_G \Pi_{\perp}] |\psi_z\rangle \right\|^2. \end{aligned}$$

Here, $\Pi_{\perp} = I - |m_c\rangle\langle m_c| - |m_{1-c}\rangle\langle m_{1-c}|$, and $\prod_{j=1}^0 [U_j O_G \Pi_{\perp}]$ is defined as the identity operator. Since the events **Find _{i}** are mutually exclusive for distinct i and

²² In fact, the subsequent analysis does not depend on the output of $\mathcal{D}_1$; it only focuses on the measurement outcomes of $\mathbb{M}_c$ and $\mathbb{M}_{1-c}$. We therefore adopt this simple output rule for $\mathcal{D}_1$.

$\text{Find} = \vee_{i=1}^q \text{Find}_i$, based on the above equation we can compute

$$\begin{aligned} \Pr \left[\text{Find} : \mathcal{D}_1^{\mathcal{O}_{\{m_{1-c}\}}^{SC}}(z, m_c, G) \right] &= \sum_{i=1}^q \Pr \left[\text{Find}_i : \mathcal{D}_1^{\mathcal{O}_{\{m_{1-c}\}}^{SC}}(z, m_c, G) \right] \\ &\geq \sum_{i=1}^q \left\| |m_{1-c}\rangle \langle m_{1-c}| \prod_{j=1}^{i-1} [U_j O_G \Pi_{\perp}] | \psi_z \rangle \right\|^2 \\ &\stackrel{(a)}{=} \| | \psi_{m_{1-c}} \rangle \|^2. \end{aligned}$$

Here (a) follows from the definition of $| \psi_{m_{1-c}} \rangle$ given in Eq. (67). Combining the above equation with Eq. (70), we obtain

$$\begin{aligned} &\Pr_{(G, H, S, z) \leftarrow \mathfrak{D}} [x = m_{1-c} : x \leftarrow \mathcal{C}_{\epsilon}^{G, 1S}(z)] \\ &\leq 12 \cdot \sqrt{\Pr_{(G, H, S, z) \leftarrow \mathfrak{D}} \left[\text{Find} : \mathcal{D}_1^{\mathcal{O}_{\{m_{1-c}\}}^{SC}}(z, m_c, G) \right]}. \end{aligned}$$

By the definition of the distribution $\mathfrak{D}$ (Fig. 13), it is easy to see that the input (z, m_c, G) of $\mathcal{D}_1$ depends only on m_c and does not directly reveal m_{1-c} . Therefore, according to the sampling procedure of m_0 and m_1 in $\mathfrak{D}$, after $\mathcal{D}_1$ receives the input (z, m_c, G) , the value m_{1-c} remains uniformly distributed over $\mathcal{M} \setminus \{m_c\}$ from its point of view. Recall that $\mathcal{D}_1$ makes $q = q_G + q_H$ queries to $\mathcal{O}_{\{m_{1-c}\}}^{SC}$. Then, by Theorem 12, we have

$$\Pr_{(G, H, S, z) \leftarrow \mathfrak{D}} \left[\text{Find} : \mathcal{D}_1^{\mathcal{O}_{\{m_{1-c}\}}^{SC}}(z, m_c, G) \right] \leq \frac{4(q_G + q_H)}{|\mathcal{M}| - 1}.$$

Combining the above two equations yields

$$\Pr_{(G, H, S, z) \leftarrow \mathfrak{D}} [x = m_{1-c} : x \leftarrow \mathcal{C}_{\epsilon}^{G, 1S}(z)] \leq 24 \sqrt{\frac{q_G + q_H}{|\mathcal{M}| - 1}}.$$

Furthermore, by combining the above equation with Eq. (66), we obtain

$$\Pr_{(G, H, S, z) \leftarrow \mathfrak{D}} [x = m_{1-c} : x \leftarrow \mathcal{D}^{G, 1S}(z)] \leq 25 \sqrt{\frac{q_G + q_H}{|\mathcal{M}| - 1}}.$$

This completes the proof of Lemma 6. $\square$

E.2 Proof of Lemma 7

Proof. Let $\sigma := \sin(\theta)$. Recall that $T = \sum_{l=0}^L 2^{-l} \geq 1$ (Table 4). For every $l \in \{0, \dots, L\}$, the inequality $|\sin(n\theta)| \leq n \sin(\theta)$ for $n \in \mathbb{N}$, together with the inequality $2 \cdot 2^l + 1 \leq 3 \cdot 2^l$, gives

$$\sin^2((2 \cdot 2^l + 1)\theta) \leq \min \{1, 9 \cdot 2^{2l} \sigma^2\}.$$

If $\sigma \geq 1/3$, then we have

$$\sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta) \leq \frac{1}{T} \sum_{l=0}^L 2^{-l} = 1 \leq 3\sigma \leq 12\sigma = 12 \sin(\theta).$$

It remains to consider $0 < \sigma < 1/3$. Partition the indices as

$$L_{\text{low}} := \left\{ l \in \{0, \dots, L\} : 2^l \leq \frac{1}{3\sigma} \right\}, \quad L_{\text{high}} := \left\{ l \in \{0, \dots, L\} : 2^l > \frac{1}{3\sigma} \right\}.$$

Since $0 < \sigma < 1/3$, the set L_{low} is nonempty. Let l_* be its largest element. Then

$$\sum_{l \in L_{\text{low}}} 2^l = \sum_{l=0}^{l_*} 2^l = 2^{l_*+1} - 1 < 2^{l_*+1} \leq \frac{2}{3\sigma}.$$

Consequently,

$$\sum_{l \in L_{\text{low}}} \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta) \leq \frac{9\sigma^2}{T} \sum_{l \in L_{\text{low}}} 2^l \leq 9\sigma^2 \cdot \frac{2}{3\sigma} = 6\sigma.$$

If $L_{\text{high}} = \emptyset$, its contribution is zero. Otherwise, let l^* be its smallest element. Since $2^{l^*} > 1/(3\sigma)$, we have

$$\sum_{l \in L_{\text{high}}} \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta) \leq \frac{1}{T} \sum_{l=l^*}^L 2^{-l} \leq \sum_{l=l^*}^{\infty} 2^{-l} = 2^{1-l^*} < 6\sigma.$$

Combining the two contributions yields

$$\sum_{l=0}^L \frac{1}{T \cdot 2^l} \sin^2((2 \cdot 2^l + 1)\theta) \leq 12\sigma = 12 \sin(\theta),$$

which proves Lemma 7. $\square$

F Security proofs for the FO-like transformation $\text{FO}^\perp$

FO-like transformation $\text{FO}^\perp$. Let $\text{P} = (\text{Gen}, \text{Enc}, \text{Dec})$ be an rPKE scheme with message space $\mathcal{M}$, randomness space $\mathcal{R}$ and ciphertext space $\mathcal{C}$. For a given set $\mathcal{K}$, let $H : \mathcal{M} \rightarrow \mathcal{R}$, $G : \mathcal{M} \times \mathcal{C} \rightarrow \mathcal{K}$ be hash functions, let $F : \mathcal{K}^{\text{prf}} \times \mathcal{C} \rightarrow \mathcal{K}$ be a pseudorandom function (PRF) with key space $\mathcal{K}^{\text{prf}}$. We associate KEM scheme

$$\text{KEM}^\perp := \text{FO}^\perp[\text{P}, H, G, F] = (\text{Gen}^\perp, \text{Enca}, \text{Deca}^\perp)$$

that has key space $\mathcal{K}$. The constituting algorithms of $\text{KEM}^\perp$ are given in Fig. 14.

We first introduce the following theorem. It shows that in the QROM, the IND-CPA security of $\text{KEM}^\perp$ implies its IND-CCA security.

$\text{Gen}^\perp$	$\text{Enc}(pk)$	$\text{Deca}^\perp(sk' = (sk, s), c)$
1: $(pk, sk) \leftarrow \text{Gen}$	1: $m \leftarrow_{\mathcal{S}} \mathcal{M}$	1: $m' := \text{Dec}_{sk}(c)$
2: $s \leftarrow_{\mathcal{S}} \mathcal{K}^{prf}$	2: $c := \text{Enc}_{pk}(m; H(m))$	2: if $m' = \perp \vee c \neq \text{Enc}_{pk}(m'; H(m'))$
3: $sk' := (sk, s)$	3: $k := G(m, c)$	3: return $F(s, c)$
4: return (pk, sk')	4: return (k, c)	4: else return $G(m', c)$

Fig. 14: Key Encapsulation Mechanism $\text{KEM}^\perp$.

Theorem 15 (IND-CPA of $\text{KEM}^\perp \xrightarrow{\text{QROM}} \text{IND-CCA of } \text{KEM}^\perp$ [13, Thm. 5]). Let $r\text{PKE}$ scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$ be δ_{wc} -worst-correct. Let $\mathcal{A}$ be an IND-CCA adversary against $\text{KEM}^\perp = \text{FO}^\perp[P, H, G, F]$, making q_D classical queries to the decapsulation oracle and making q_G (resp. q_H) quantum queries to the random oracle G (resp. H). Then, we can construct a PRF adversary $\mathcal{A}_{\text{prf}}$ against F and an IND-CPA adversary $\mathcal{B}$ (in the QROM) against $\text{KEM}^\perp$ such that

$$\text{Adv}_{\text{KEM}^\perp}^{\text{IND-CCA}}(\mathcal{A}) \leq \text{Adv}_F^{\text{PRF}}(\mathcal{A}_{\text{prf}}) + \text{Adv}_{\text{KEM}^\perp}^{\text{IND-CPA}}(\mathcal{B}) + 16(2q_H + 2q_G + 1)^2 \cdot \delta_{wc}.$$

Here, $\mathcal{B}$ makes at most q_G (resp. $q_G + q_H$) quantum queries to the random oracle G (resp. H). The running time of $\mathcal{A}_{\text{prf}}$ and $\mathcal{B}$ is $\mathcal{T}_{\mathcal{A}_{\text{prf}}} \lesssim \mathcal{T}_{\mathcal{A}} + q_D \cdot (\mathcal{T}_{\text{Enc}} + \mathcal{T}_{\text{Dec}}) + O(q_H^2 + q_G^2)$ and $\mathcal{T}_{\mathcal{B}} \lesssim \mathcal{T}_{\mathcal{A}} + O(q_G) \cdot \mathcal{T}_{\text{Enc}} + O(q_G^2 + q_D^2)$, respectively.

Then, we prove the following theorem, which shows that the IND-CPA security of $\text{KEM}^\perp$ in the QROM can be reduced to the IND-CPA security of P without the square-root advantage loss.

Theorem 16 (IND-CPA of $P \xrightarrow{\text{QROM}} \text{IND-CPA of } \text{KEM}^\perp$). For an $r\text{PKE}$ scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M} (= \{0, 1\}^m)$, let $\mathcal{A}$ be an IND-CPA adversary against $\text{KEM}^\perp = \text{FO}^\perp[P, H, G, F]$, making q_G (resp. q_H) quantum queries to the random oracle G (resp. H). Then, we can construct an IND-CPA adversary $\mathcal{A}_{\text{ind}}$ against P such that

$$\text{Adv}_{\text{KEM}^\perp}^{\text{IND-CPA}}(\mathcal{A}) \leq 44\sqrt{q_G + q_H + 1} \cdot \text{Adv}_P^{\text{IND-CPA}}(\mathcal{A}_{\text{ind}}) + 1100 \cdot \frac{q_G + q_H + 1}{\sqrt{|\mathcal{M}| - 1}}.$$

Here, we have $\mathcal{T}_{\mathcal{A}_{\text{ind}}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}} + O(mq_G^2 + mq_H^2)$.

Proof. Since we only consider IND-CPA security, where the adversary has no access to the decapsulation oracle, the proof of this theorem is almost identical to that of Theorem 8, and we omit the details. In fact, before following the proof of Theorem 8, we only need to use the indistinguishability argument from [4, Theorem 5] to replace the $G(m, c)$ used in key derivation with $G(m)$. $\square$

Combining Theorem 15 with Theorem 16, we finally obtain the following theorem. This theorem shows that, in the QROM, the IND-CCA security of $\text{KEM}^\perp$ can be reduced to the IND-CPA security of the underlying $r\text{PKE}$ scheme without the square-root advantage loss.

Theorem 17 (IND-CPA of $P \xrightarrow{\text{QROM}} \text{IND-CCA of } \text{KEM}^\perp$). *Let rPKE scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$ be δ_{wc} -worst-correct. Suppose that P has message space $\mathcal{M} (= \{0, 1\}^m)$. Let $\mathcal{A}$ be an IND-CCA adversary against $\text{KEM}^\perp = \text{FO}^\perp[P, H, G, F]$, making q_D classical queries to the decapsulation oracle and making q_G (resp. q_H) quantum queries to the random oracle G (resp. H). Then, we can construct a PRF adversary $\mathcal{A}_{\text{prf}}$ against F and an IND-CPA adversary $\mathcal{A}_{\text{ind}}$ against P such that*

$$\begin{aligned} \text{Adv}_{\text{KEM}^\perp}^{\text{IND-CCA}}(\mathcal{A}) &\leq \text{Adv}_F^{\text{PRF}}(\mathcal{A}_{\text{prf}}) + 44\sqrt{2q_G + q_H + 1} \cdot \text{Adv}_P^{\text{IND-CPA}}(\mathcal{A}_{\text{ind}}) \\ &\quad + 1100 \cdot \frac{2q_G + q_H + 1}{\sqrt{|\mathcal{M}| - 1}} + 16(2q_H + 2q_G + 1)^2 \cdot \delta_{wc}. \end{aligned}$$

Here, we have $\mathcal{T}_{\mathcal{A}_{\text{prf}}} \lesssim \mathcal{T}_{\mathcal{A}} + q_D \cdot (\mathcal{T}_{\text{Enc}} + \mathcal{T}_{\text{Dec}}) + O(q_H^2 + q_G^2)$ and $\mathcal{T}_{\mathcal{A}_{\text{ind}}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}} + O(mq_G) \cdot \mathcal{T}_{\text{Enc}} + O(mq_G^2 + mq_H^2 + mq_D^2)$.

If the underlying rPKE scheme P is unique randomness recoverable (Definition 8) with the recover algorithm Rec , we can prove the following theorem. This theorem shows that, in the QROM, the IND-CCA security of $\text{KEM}^\perp$ can be reduced to the OW-CPA security of P without the square-root advantage loss.

Theorem 18 (OW-CPA of $P \xrightarrow{\text{QROM}} \text{IND-CCA of } \text{KEM}^\perp$). *Let rPKE scheme $P = (\text{Gen}, \text{Enc}, \text{Dec})$ be unique randomness recoverable with the recover algorithm Rec . Suppose that P is δ_{wc} -worst-correct and has message space $\mathcal{M} (= \{0, 1\}^m)$. Let $\mathcal{A}$ be an IND-CCA adversary against $\text{KEM}^\perp = \text{FO}^\perp[P, H, G, F]$, making q_D classical queries to the decapsulation oracle and making q_G (resp. q_H) quantum queries to the random oracle G (resp. H). Then, we can construct a PRF adversary $\mathcal{A}_{\text{prf}}$ against F and a OW-CPA adversary $\mathcal{A}_{\text{ow}}$ against P such that*

$$\begin{aligned} \text{Adv}_{\text{KEM}^\perp}^{\text{IND-CCA}}(\mathcal{A}) &\leq \text{Adv}_F^{\text{PRF}}(\mathcal{A}_{\text{prf}}) + 110 \cdot \text{Adv}_P^{\text{OW-CPA}}(\mathcal{A}_{\text{ow}}) \\ &\quad + 16(2q_H + 2q_G + 1)^2 \cdot \delta_{wc} + 198 \cdot \delta_{wc}. \end{aligned}$$

Here, we have $\mathcal{T}_{\mathcal{A}_{\text{prf}}} \lesssim \mathcal{T}_{\mathcal{A}} + q_D \cdot (\mathcal{T}_{\text{Enc}} + \mathcal{T}_{\text{Dec}}) + O(q_H^2 + q_G^2)$ and $\mathcal{T}_{\mathcal{A}_{\text{ow}}}^{\text{exp}} \lesssim (2m + 5) \cdot \mathcal{T}_{\mathcal{A}} + O(mq_G + mq_H) \cdot (\mathcal{T}_{\text{Enc}} + \mathcal{T}_{\text{Rec}}) + O(mq_G^2 + mq_H^2 + mq_D^2)$.

Proof. The proof of this theorem is identical to that of [13, Corollary 1] based on the unique-randomness-recoverability, except for the following two differences:

1. The MRE-O2H (Theorem 14) used in [13, Corollary 1] should be replaced by our DSEAM-O2H (Theorem 4).
2. The random oracles should be simulated by $2q$ -wise independent functions before applying the O2H theorem. This is similar to the proof of Theorem 8, where the distribution $\mathfrak{D}$ (Fig. 13) initially samples G as a $2(q_G + q_H)$ -wise independent function. We adopt this approach because the one-wayness attacker designed in DSEAM-O2H requires repeatedly running the distinguisher, possibly for an exponential number of repetitions. Therefore, if we

convert the random oracles into $2q$ -wise independent functions only after applying DSEAM-O2H, we need to choose an exponentially large q to ensure a perfect simulation of the random oracle, since the number of random oracle queries at this point may be exponential.

Despite these two differences, the proof of [13, Corollary 1] can still be transferred in a straightforward manner. Hence, we omit the detailed proof. $\square$