On the non-tightness of measurement-based reductions for key encapsulation mechanism in the quantum random oracle model

Haodong Jiang[1,2,4], Zhenfeng Zhang[2,3], and Zhi Ma[1,4]

[1] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan, China
[2] TCA Laboratory, State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, China
[3] University of Chinese Academy of Sciences, Beijing, China
[4] Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, Henan, China
hdjiang13@gmail.com, zfzhang@tca.iscas.ac.cn, ma_zhi@163.com

Abstract. Key encapsulation mechanism (KEM) variants of the Fujisaki-Okamoto (FO) transformation (CRYPTO 1999 and Journal of Cryptology 2013) that turn a weakly-secure public-key encryption (PKE) into an IND-CCA-secure KEM, were proposed by Hofheinz, Hövelmanns and Kiltz (TCC 2017) and widely used among the KEM submissions to the NIST Post-Quantum Cryptography Standardization Project. The security reductions for these variants in the quantum random oracle model (QROM) were given by Hofheinz, Hövelmanns and Kiltz (TCC 2017) and Jiang et al. (Crypto 2018). However, under standard CPA security assumptions, i.e., OW-CPA and IND-CPA, all these security reductions are far from desirable due to the quadratic security loss.

In this paper, for KEM variants of the FO transformation, we show that a typical *measurement-based* reduction in the QROM from breaking standard OW-CPA (or IND-CPA) security of the underlying PKE to breaking the IND-CCA security of the resulting KEM, will *inevitably* incur a quadratic loss of the security, where "measurement-based" means the reduction measures a hash query from the adversary and uses the measurement outcome to break the underlying security of PKE. In particular, all currently known security reductions in (TCC 2017 and Crypto 2018) are of this type, and our results suggest an explanation for the lack of progress in improving the reduction tightness in terms of the degree of security loss. We emphasize that our results do not expose any post-quantum security weakness of KEM variants of FO transformation.

Keywords: non-tightness · quantum random oracle model · key encapsulation mechanism

1 Introduction

Indistinguishability against chosen-ciphertext attacks (IND-CCA) [1] has been considered as a standard security notion for a key encapsulation mechanism (KEM) [2]. For designing efficient cryptographic protocols, an idealized model called random oracle model (ROM) [3] is usually used, where a hash function is idealized to be a publicly accessible random oracle (RO). Generic constructions of an IND-CCA-secure KEM in the ROM were well studied by Dent [4] and Hofheinz, Hövelmanns and Kiltz [5].

Essentially, the generic constructions in [5] are KEM variants of the Fujisaki-Okamoto (FO) transformation [6, 7], including $\mathrm{FO}^{\perp}$, $\mathrm{FO}^{\perp}_{m}$, $\mathrm{FO}^{\not\perp}$, $\mathrm{FO}^{\not\perp}_{m}$, $\mathrm{QFO}^{\perp}_{m}$ and $\mathrm{QFO}^{\not\perp}_{m}$, and KEM variants of the REACT/GEM transformation [8, 9], including $\mathrm{U}^{\not\perp}$, $\mathrm{U}^{\perp}$, $\mathrm{U}^{\not\perp}_{m}$, $\mathrm{U}^{\perp}_{m}$, $\mathrm{QU}^{\not\perp}_{m}$ and $\mathrm{QU}^{\perp}_{m}$, where FO denotes the class of transformations that turn a public-key encryption (PKE) with standard security (one-wayness against chosen-plaintext attacks (OW-CPA) or indistinguishability against chosen-plaintext attacks (IND-CPA)) into an IND-CCA KEM, U denotes the class of transformations that turn a PKE with non-standard security (e.g., OW-PCA, one-way against plaintext checking attack [8, 9]) or a deterministic PKE (DPKE, where the encryption algorithm is deterministic) into an IND-CCA-secure KEM, m (without m) means $K = H(m)$ ($K = H(m, c)$), $\not\perp$ ($\perp$) means implicit (explicit) rejection[5] and Q means an additional Targhi-Unruh hash [10] (a length-preserving hash function that has the same domain and range size) is appended to the ciphertext. The modular analysis of FO transforms by Hofheinz et al. [5] suggests that the FO transform implicitly contains

[5] In implicit (explicit) rejection, a pseudorandom key (an abnormal symbol $\perp$) is returned for an invalid ciphertext.

the GEM/REACT transform at least the proof technique. Thus, in what follows, we just call these variants FO-like KEM constructions for brevity.

In modern cryptography, cryptosystem constructions are usually proposed together with a proof of security. Typically, when proving a security of a cryptographic scheme S under a hardness assumption of an underlying problem P, one usually constructs a reduction algorithm $R^{\mathcal{A}}$ that runs an adversary $\mathcal{A}$ against S as a subroutine to break the underlying hardness assumption of P. Let $(T_{\mathcal{A}}, \epsilon_{\mathcal{A}})$ and (T_R, ϵ_R) denote the running times and advantages of $\mathcal{A}$ and $R^{\mathcal{A}}$, respectively. The reduction is said to be tight if $T_{\mathcal{A}} \approx T_R$ and $\epsilon_{\mathcal{A}} \approx \epsilon_R$. Otherwise, if $T_R \gg T_{\mathcal{A}}$ or $\epsilon_R \ll \epsilon_{\mathcal{A}}$, the reduction is non-tight. Generally, the tightness gap, (informally) defined by $\frac{T_{\mathcal{A}}\epsilon_R}{T_R\epsilon_{\mathcal{A}}}$ [11], is used to measure the quality of a reduction. Tighter reductions with smaller tightness gap are desirable for practice cryptography especially in large-scale scenarios, since the tightness of a reduction determines the strength of the security guarantees provided by the security proof.

In the ROM, if an adversary queries m to a random oracle H, the reduction can see this query and learn m. This is sometimes called extractability. When proving the IND-CCA security of a PKE/KEM under various standard assumptions in the ROM, one usually constructs a *query-based*[6] reduction that uses a hash query from the adversary to beak the underlying hard problem, such as the proofs for FO transformation [6, 7], REACT/GEM transformation [8, 9], Bellare-Rogaway [3], OAEP [13, 14], and the hashed ElGamal encryption scheme [15]. A query-based reduction is also used in getting a tight security proof for a unique signature [12]. In particular, for FO-like KEM constructions from standard CPA assumptions (in what follows, standard CPA assumptions refer to OW-CPA and IND-CPA), currently known security reductions [4, 5, 16–19] in the ROM are all query-based.

Recently, post-quantum security of these FO-like KEM constructions has gathered great interest [5, 16–23] due to their widespread adoption [17, Table 1] in KEM submissions to the NIST Post-Quantum Cryptography Standardization Project [24], of which the goal is to standardize new public-key cryptographic algorithms with security against quantum adversaries. Motivated by the fact that quantum adversaries can execute all offline primitives such as hash functions on arbitrary superpositions, Boneh et al. [25] introduced quantum random oracle model (QROM), where the adversary can query the random oracle with a quantum state, and argued that to prove post-quantum security one needs to prove security in the QROM.

Unfortunately, aforementioned query-based reduction in the ROM can not carry over to the QROM setting offhand due to the fact that the extractability might be problematic [25] when the query is a quantum state, which can be a superposition of exponentially many classical states. In a quantum world, measurement allows us to extract classical information from a quantum state and thus is a way that we can "read out" information. Thus, naturally, a QROM version of aforementioned query-based reduction can be a reduction that measures a hash query from the adversary and uses the measurement outcome to beak the underlying hard problem. In this paper, we call this type of reductions a *measurement-based* reduction.

Particularly, all currently known security reductions in the QROM for FO-like KEM constructions from standard CPA assumptions in [5, 16–19] are of this type, and have the tightness, (1) T_R is about $T_{\mathcal{A}}$; (2) $\epsilon_R \approx \kappa\epsilon_{\mathcal{A}}^{\tau}$, where κ and τ in the following are respectively denoted as the factor and degree of security loss[7]. Let q be the total number of adversarial queries (including quantum and classical) to various oracles.

- In [5], Hofheinz et al. presented security reductions for $\mathrm{QFO}_m^{\not\perp}$ and $\mathrm{QFO}_m^{\perp}$ from the OW-CPA security of the underlying PKE with $\kappa = q^{-6}$ and $\tau = 4$, for $\mathrm{QU}_m^{\not\perp}$ and $\mathrm{QU}_m^{\perp}$ from the OW-PCA security of the underlying PKE with $\kappa = q^{-2}$ and $\tau = 2$.
- In [16], Saito, Xagawa and Yamakawa presented a tight security reduction (i.e., $\kappa = 1$ and $\tau = 1$) for $\mathrm{U}_m^{\not\perp}$ from a new non-standard security called disjoint simulatability (DS) of the underlying DPKE, and also provided a security reduction for a variant of $\mathrm{FO}_m^{\not\perp}$ from standard IND-CPA security of the underlying PKE with $\kappa = q^{-2}$ and $\tau = 2$.
- In [17], Jiang et al. first presented security reductions for $\mathrm{FO}^{\not\perp}$ and $\mathrm{FO}_m^{\not\perp}$ from standard OW-CPA security of the underlying PKE with $\kappa = q^{-2}$ and $\tau = 2$. Then, they presented security reductions for $\mathrm{U}^{\not\perp}$ ($\mathrm{U}^{\perp}$, resp.) from OW-qPCA (OW-qPVCA, resp.) of the underlying PKE, $\mathrm{U}_m^{\not\perp}$ ($\mathrm{U}_m^{\perp}$, resp.) from OW-CPA (OW-VA, resp.) of the underlying DPKE with $\kappa = q^{-2}$ and $\tau = 2$, where OW-qPCA and OW-qPVCA are new non-standard security notions of PKE introduced by [17] and called one-way against

[6] This name comes from Guo et al.'s paper [12].

[7] When comparing the tightness of different reductions, we assume perfect correctness of the underlying scheme for brevity.

quantum plaintext checking attacks and one-way against quantum plaintext and (classical) validity checking attacks respectively, OW-VA is also a non-standard security notion of DPKE called one-way against validity checking attacks in [5].
– In [18, 19], using the semi-classical oracle technique in [26], Jiang et al. improved the tightness of security reductions in [17]. Precisely, from standard IND-CPA security of the underlying PKE, security reductions for $\mathrm{FO}^{\not\perp}$, $\mathrm{FO}^{\not\perp}_m$, and their variants with explicit rejection have tightness with $\kappa = q^{-1}$ and $\tau = 2$. For $\mathrm{U}^{\not\perp}$, $\mathrm{U}^{\perp}$, $\mathrm{U}^{\not\perp}_m$ and $\mathrm{U}^{\perp}_m$, the security reductions are improved with $\kappa = q^{-1}$ and $\tau = 2$ with the same security assumptions as in [17].

As seen above, all currently known security reductions in the QROM for FO-like KEM constructions from standard CPA assumptions, are far from desirable due to the quadratic security loss (at least). This is quite different from the ROM setting, where security reductions with linear security loss [4, 5] can be achieved. Recently, to better assess the security of lattice-based submissions, Ducas and Stehlé [27] suggested 10 questions that NIST should be asking the community. The 10-th question [27, Problem 10] is on this non-tightness of security reductions for FO-like KEM constructions in the QROM. To better understand this non-tightness, they asked that

Is QROM non-tightness an artifact or is it meaningful? Can the tightness of those reductions be improved?

1.1 Our Contributions

In this paper, we consider a "typical" class of reductions that have black-box access to the adversary and run the adversary *once and without rewinding*[8]. Given a real p ($0 \leq p \leq 1$) and a FO-like KEM construcion,

1. We first construct an unbounded quantum adversary $\mathcal{A}$ that breaks the IND-CCA security of the resulting KEM by querying the random oracle with a well-designed *quantum* state and solving a discrimination problem between two *quantum* states (refer to Subsection 1.2 for details). The advantage of $\mathcal{A}$ is at least $\sqrt{p}$, i.e., $\epsilon_{\mathcal{A}} \gtrapprox \sqrt{p}$.
2. Then, using the meta-reduction methodology [29, 30], we bound the advantage ϵ_R of a typical measurement-based reduction $R^{\mathcal{A}}$ that takes above $\mathcal{A}$ as a subroutine to break the OW-CPA (IND-CPA, resp.) security of the underlying PKE. In particular, the advantage ϵ_R can not substantially exceed p, i,e, $\epsilon_R \lessapprox p$, unless there exists an algorithm breaking the OW-CPA (IND-CPA, resp.) security of the underlying PKE efficiently.

Thus, for FO-like KEM constructions, our results show that a typical measurement-based reduction in the QROM from breaking standard OW-CPA (or IND-CPA) security of the underlying PKE to breaking the IND-CCA security of the resulting KEM, will *inevitably* incur a quadratic loss of the security.

1.2 Technique overview

In FO-like KEM constructions, the (session) key K is derived by $H(m)$ (or $H(m, c)$) and the ciphertext $c = Enc(pk, m; G(m))$ (or $Enc(pk, m)$ if Enc is deterministic) is the corresponding encapsulation of the key K, where Enc is the encryption algorithm of the underlying PKE, m is uniformly picked at random, G and H are random oracles. In this section, for a concise presentation, we just take $\mathrm{KEM} - \mathrm{U}^{\not\perp}_m$ (see Fig. 3 for details) as an example, and thus $K = H(m)$ and $c = Enc(pk, m)$. It is easy to extend the techniques here to other FO-like KEM constructions, see Sec. 6.1.

When attacking the IND-CCA security of $\mathrm{KEM} - \mathrm{U}^{\not\perp}_m$, an adversary $\mathcal{A}(pk, c^*, K_b)$ needs to distinguish $K_0 = H(m^*)$ from a uniformly random key K_1, where $c^* = Enc(pk, m^*)$ for a uniformly random m^*, the coin $b \in \{0, 1\}$ is uniformly random. We note that the random oracle H has a useful property that if m^* has not been queried to H by $\mathcal{A}$, then the value $H(m^*)$ is uniformly random in $\mathcal{A}$'s view. Thus,

[8] At first sight we heavily constrain the class of reductions to that our results apply. However, all currently known security reductions in the QROM for FO-like KEM constructions [5, 16–23] belong to this typical class. Moreover, most reductions of cryptographic security proofs in the QROM are of this type. This seems to be mostly due to the hardness of quantum rewinding [28].

$\mathcal{A}$'s distinguishing advantage is negligible when making no queries to H with m^*. Intuitively, to achieve a non-negligible distinguishing advantage, $\mathcal{A}$ has to query m^* to H.

In the ROM, $\mathcal{A}$ can only make classical queries to H. For any p ($0 \leq p \leq 1$), if $\mathcal{A}$ queries m^* to H with probability p, he will learn $K_0 = H(m^*)$ with probability p and break the IND-CCA security with advantage approximately p by testing whether $K_0 = K_b$. For a reduction $R^{\mathcal{A}}$ against the OW-CPA security of the underlying DPKE, a natural way is to take $\mathcal{A}$'s query as a return. Then, with probability p, $R^{\mathcal{A}}$ will return the m^* and break the OW-CPA security of the underlying DPKE. That is, the advantages of $R^{\mathcal{A}}$ and $\mathcal{A}$ are approximately equal, which is consistent with currently known tight reduction in [5].

Unbounded quantum adversary $\mathcal{A}$. In the QROM, a quantum adversary $\mathcal{A}$ can make a query to H with a quantum state. Consider the following quantum state

$$|\psi_{-1}\rangle := \sqrt{p}|m^*\rangle|0\rangle + \sqrt{1-p}|m'\rangle|\Sigma\rangle,$$

where $m' \neq m^*$, $|\Sigma\rangle = \sum_{k\in\mathcal{K}} \frac{1}{\sqrt{|\mathcal{K}|}}|k\rangle$ and $\mathcal{K}$ is the (session) key space. For a quantum query with $|\psi_{-1}\rangle$, the random oracle H will return

$$|\psi_0\rangle := \sqrt{p}|m^*\rangle|K_0\rangle + \sqrt{1-p}|m'\rangle|\Sigma\rangle.$$

We remark that if the adversary $\mathcal{A}$ directly measures $|\psi_0\rangle$ in standard computational basis, he will obtain K_0 with probability p and break the IND-CCA security with the advantage (approximately) p by testing whether $K_0 = K_b$ as the adversary in the ROM described above.

Here, we construct an unbounded quantum adversary $\mathcal{A}(pk, c^*, K_b)$ that first determines m^* such that $c^* = Enc(pk, m^*)$ by exhaustive search (if none is found, outputs 1) and randomly selects a uniform m' such that $m' \neq m^*$, then queries $|\psi_{-1}\rangle$ to H, lastly guesses b by *testing* whether $|\psi_0\rangle = |\psi_b\rangle$, where

$$|\psi_b\rangle := \sqrt{p}|m^*\rangle|K_b\rangle + \sqrt{1-p}|m'\rangle|\Sigma\rangle.$$

Testing whether $|\psi_0\rangle = |\psi_b\rangle$ can be converted into a discrimination problem between quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$. The advantage of $\mathcal{A}$ against the IND-CCA security is about the distinguishing advantage of a distinguisher D against the discrimination problem between $|\psi_0\rangle$ and $|\psi_1\rangle$.

Quantum state discrimination [31–33] traces a long history of several decades, and underlies various applications in quantum information processing tasks. Although there are several well-known distinguishers [33–35], they do not serve as a satisfactory solution due to the restricted conditions or low distinguishing advantages, see Sec. 3 for details.

Therefore, exploiting the algebraic property of $|\psi_0\rangle$ and $|\psi_1\rangle$, we develop a new distinguisher such that the distinguishing advantage is at least $\sqrt{p}$. Thus, with this new distinguisher, quantum adversary $\mathcal{A}$ can break the IND-CCA security with advantage (approximately) at least $\sqrt{p}$. That is, $\epsilon_{\mathcal{A}} \gtrapprox \sqrt{p}$.

In currently known proofs for $\mathrm{KEM} - \mathrm{U}_m^{\not\perp}$ in [17], the reduction algorithm $R^{\mathcal{A}}$ against the OW-CPA security of the underlying DPKE *just* randomly measures one of $\mathcal{A}$'s queries to H in standard computational basis and takes the measurement outcome as a return. The security bound is given by $\epsilon_{\mathcal{A}} \lessapprox q\sqrt{\epsilon_R}$.

We note that above unbounded quantum adversary $\mathcal{A}$ makes no queries to the decapsulation oracle, and just reveals one quantum query $|\psi_{-1}\rangle$ to H and a guessing of b. Thus, the total number of $\mathcal{A}$'s queries to various oracles is one, i.e., $q = 1$. We also note that the advantage of the reduction algorithm $R^{\mathcal{A}}$ in [17] is exactly the probability of the measurement outputting m^*, which is equal to p. That is, $\epsilon_R = p$. Thus, for above unbounded quantum adversary $\mathcal{A}$, the advantage can match the bound $\epsilon_{\mathcal{A}} \lessapprox q\sqrt{\epsilon_R}$ in [17].

The advantage of a typical measurement-based reduction Here, we consider a typical measurement-based reduction $R^{\mathcal{A}}$ that runs $\mathcal{A}$ (once and without rewinding), measures $\mathcal{A}$'s query $|\psi_{-1}\rangle$ and uses the measurement outcome to break the OW-CPA security of the underlying DPKE. We say a reduction R is

efficient if the running time of R (excluding the running time of the adversary $\mathcal{A}$) is polynomial in the security parameter. We make a convention that $R^{\mathcal{A}}$ measures $|\psi_{-1}\rangle$ in standard computational basis[9].

Meta-reduction methodology. Since the introduction by Boneh and Venkatesan in [29], the meta-reduction methodology has proven to be a versatile tool in deriving impossibility results and tightness bounds of security proofs for many cryptosystem constructions [29, 30, 36–44], please see the review [45, Figure 1]. Let R be a reduction that breaks the underlying hard problem P with access to an adversary $\mathcal{A}$ against a scheme S. Roughly speaking, a meta-reduction MR_R simulates the adversarial part $\mathcal{A}$, runs R as a subroutine, and break the underlying hard problem P directly without reference to an allegedly successful adversary. That is, a meta-reduction MR_R treats the reduction R as an adversary itself and reduce the existence of such a reduction R to a presumably hard problem.

Consider the advantage of $R^{\mathcal{A}}$ in following three cases, where INE (EXI, resp.) is the event that the exhaustive search returns no (a, resp.) m^* such that $Enc(pk, m^*) = c^*$, and GOOD (BAD, resp.) is the event that the measurement outcome is (not, resp.) m^*.

Case 1: INE. In this case, $\mathcal{A}$ just outputs 1 without queries to H. Thus, exhaustive search for m^* in this case is vain, and $\mathcal{A}$ can be replaced by an adversary $\mathcal{A}_1$ that always outputs 1 without the search for m^* and the query to the random oracle H. Therefore, we can easily construct a meta-reduction MR_1^R that simulates $\mathcal{A}_1$ and takes $R^{\mathcal{A}_1}$ as a subroutine to break the OW-CPA security of the underlying DPKE such that the running time of MR_1^R is about the running time of R, and under the condition INE the advantage of MR_1^R is about the advantage of R.

Case 2: EXI $\wedge$ GOOD. Since $\Pr[\text{GOOD}|\text{EXI}] = p$, we can bound the advantage of R in this case by p.

Case 3: EXI $\wedge$ BAD. In this case, R gets $m' \neq m^*$. Let $\mathcal{A}_2$ be an adversary that queries a quantum state $\sum_{m,k} \frac{1}{\sqrt{|\mathcal{M}|\cdot|\mathcal{K}|}}|m\rangle|k\rangle$ and outputs 1 without the search for m^*. Thus, the advantage of R under the condition EXI $\wedge$ BAD remains unchanged when $\mathcal{A}$ is replaced by $\mathcal{A}_2$. As in the case 1, we can also construct a meta-reduction MR_2^R against the OW-CPA security of the underlying DPKE that simulates $\mathcal{A}_2$ and takes $R^{\mathcal{A}_2}$ as a subroutine such that the running time of MR_2^R is about the running time of R, and under the condition EXI $\wedge$ BAD the advantage of MR_2^R is about the advantage of R.

Under the assumption that the advantage of any efficient algorithm breaking the OW-CPA security of the underlying DPKE is negligible, we have that both advantages of MR_1^R and MR_2^R are negligible since the running time of R (excluding the running time of the adversary $\mathcal{A}$) is polynomial in the security parameter. Thus, both advantages of R in Case 1 and Case 3 are negligible, which implies that the upper bound of R's advantage is approximately p. That is, the advantage of a typical measurement-based reduction against the OW-CPA security of the underlying DPKE can not substantially exceed p unless there exists an algorithm breaking the OW-CPA security of the underlying DPKE efficiently.

1.3 Discussion

Although certain quantum cases of rewinding are handled by [46–48], the rewinding problem in general quantum case remains elusive [28]. Thus, it is an interesting open problem for FO-like KEM constructions that whether one can derive tighter QROM security proofs by rewinding, or extend our results to the reductions with rewinding.

We also note that we just consider a measurement-based reduction that measures a hash query from the adversary and uses the measurement outcome to break the underlying hard problem. For $\text{KEM} - \text{U}_m^{\not\perp}$ from a non-standard assumption, DS security, [16] gave a tight non-measurement-based reduction algorithm, where adversary's guessing of the coin b instead is used to break the DS security of the underlying DPKE. Thus, it is also an interesting problem whether one can develop a tight non-measurement-based reduction for FO-like KEM constructions from standard CPA assumptions.

2 Preliminaries

Symbol description. A security parameter is denoted by λ. We use the standard O-notations: O, Θ, Ω and ω. The abbreviation PPT stands for probabilistic polynomial time. A function $f(\lambda)$ is said to be *negligible*

[9] For $|\psi_{-1}\rangle$, the semi-classical measurement in [26] is equivalent to the standard computational basis measurement since $|\psi_{-1}\rangle$ is the superposition of two terms, $|m^*\rangle|0\rangle$ and $|m'\rangle|\Sigma\rangle$.

if $f(\lambda) = \lambda^{-\omega(1)}$. We denote a set of negligible functions by $\mathsf{negl}(\lambda)$. $\mathcal{K}$, $\mathcal{M}$, $\mathcal{C}$ and R are denoted as key space, message space, ciphertext space and randomness space, respectively. Given a finite set X, we denote the sampling of a uniformly random element x by $x \xleftarrow{\$} X$. Denote the sampling from some distribution D by $x \leftarrow D$. $x =? y$ is denoted as an integer that is 1 if $x = y$, and otherwise 0. Denote deterministic (probabilistic) computation of an algorithm A on input x by $y = A(x)$ ($y \leftarrow A(x)$). Let $|X|$ be the cardinality of set X. A^H means that the algorithm A gets access to the oracle H. $\mathsf{Time}(R)$ is the running time of an algorithm R. $\mathsf{Time}(R^{\mathcal{A}}) = \mathsf{Time}(R) + k\mathsf{Time}(\mathcal{A})$ is the running time of an algorithm $R^{\mathcal{A}}$ that takes $\mathcal{A}$ as a subroutine[10], where k is the number of times $\mathcal{A}$ is invoked by R.

2.1 Cryptographic Primitives

Definition 2.1 (Public-key encryption). *A public-key encryption scheme* $\mathrm{PKE} = (Gen, Enc, Dec)$ *consists of a triple of polynomial time (in the security parameter* λ*) algorithms and a finite message space* $\mathcal{M}$*.*

- $Gen(1^\lambda) \to (pk, sk)$*: the key generation algorithm, is a probabilistic algorithm which on input* 1^λ *outputs a public/secret key-pair* (pk, sk)*. Usually, for brevity, we will omit the input of Gen.*
- $Enc(pk, m) \to c$*: the encryption algorithm Enc, on input pk and a message* $m \in \mathcal{M}$*, outputs a ciphertext* $c \leftarrow Enc(pk, m)$*. If necessary, we make the used randomness of encryption explicit by writing* $c := Enc(pk, m; r)$*, where* $r \xleftarrow{\$} R$ *(R is the randomness space).*
- $Dec(sk, c) \to m$*: the decryption algorithm Dec, is a deterministic algorithm which on input sk and a ciphertext c outputs a message* $m := Dec(sk, c)$ *or a rejection symbol* $\perp \notin \mathcal{M}$*.*

A PKE is deterministic if *Enc* is deterministic. We denote DPKE to stand for a deterministic PKE.

Definition 2.2 (Correctness). *A public-key encryption scheme* PKE *is* perfectly correct *if for any* $(pk, sk) \leftarrow Gen$ *and* $m \in \mathcal{M}$*, we have that*

$$\Pr[Dec(sk, c) = m | c \leftarrow Enc(pk, m)] = 1.$$

Definition 2.3 (OW-CPA-secure PKE). *Let* $\mathrm{PKE} = (Gen, Enc, Dec)$ *be a public-key encryption scheme with message space* $\mathcal{M}$*. Define* $\mathrm{OW-CPA}$ *game of PKE as in Fig. 1. Define the* $\mathrm{OW-CPA}$ *advantage of an adversary* $\mathcal{A}$ *against PKE as*

$$\mathtt{Adv}^{\text{OW-CPA}}_{\mathrm{PKE}}(\mathcal{A}) := \Pr[\text{OW-CPA}^{\mathcal{A}}_{\mathrm{PKE}} = 1].$$

Game OW-CPA		Game IND-CPA	
1 :	$(pk, sk) \leftarrow Gen; m^* \xleftarrow{\$} \mathcal{M}$	1 :	$(pk, sk) \leftarrow Gen; b \leftarrow \{0, 1\}$
2 :	$c^* \leftarrow Enc(pk, m^*)$	2 :	$(m_0, m_1) \leftarrow \mathcal{A}(pk); c^* \leftarrow Enc(pk, m_b)$
3 :	$m' \leftarrow \mathcal{A}(pk, c^*)$	3 :	$b' \leftarrow \mathcal{A}(pk, c^*)$
4 :	**return** $m' =? m^*$	4 :	**return** $b' =? b$

Fig. 1: Game OW-CPA and game IND-CPA for PKE.

Definition 2.4 (IND-CPA-secure PKE). *Let* $\mathrm{PKE} = (Gen, Enc, Dec)$ *be a public-key encryption scheme with message space* $\mathcal{M}$*. Define* $\mathrm{IND-CPA}$ *game of PKE as in Fig. 1, where* m_0 *and* m_1 *have the same length. Define the* $\mathrm{IND-CPA}$ *advantage* [11] *of an adversary* $\mathcal{A}$ *against PKE as*

$$\mathtt{Adv}^{\text{IND-CPA}}_{\mathrm{PKE}}(\mathcal{A}) := \left| 2 \Pr[\text{IND-CPA}^{\mathcal{A}}_{\mathrm{PKE}} = 1] - 1 \right|.$$

[10] Here, in this paper, $\mathcal{A}$ is forbidden to call R as a subroutine.

[11] The $\mathrm{IND-CPA}$ advantage is also defined by $\left| \Pr[\text{IND-CPA}^{\mathcal{A}}_{\mathrm{PKE}} = 1] - \frac{1}{2} \right|$ in the literature. Here, to make the advantage for OW-CPA and IND-CPA have the same range $[0, 1]$, we choose such a definition.

Definition 2.5 (Key encapsulation). *A key encapsulation mechanism KEM consists of three algorithms Gen, Encaps and Decaps.*

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

Game IND-CCA	DECAPS(sk, c)
1 : $(pk, sk) \leftarrow Gen; b \xleftarrow{\$} \{0,1\}$	1 : **if** $c = c^*$
2 : $(K_0^*, c^*) \leftarrow Encaps(pk); K_1^* \xleftarrow{\$} \mathcal{K}$	2 : **return** $\perp$
3 : $b' \leftarrow \mathcal{A}^{\text{DECAPS}}(pk, c^*, K_b^*)$	3 : **else return**
4 : **return** $b' =? b$	4 : $K := Decaps(sk, c)$

Fig. 2: Game IND-CCA for KEM.

Definition 2.6 (IND-CCA-secure KEM). *We define the* $\text{IND} - \text{CCA}$ *game as in Fig. 2 and the* $\text{IND} - \text{CCA}$ *advantage of an adversary* $\mathcal{A}$ *against* KEM *as*

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

2.2 Quantum Computation

Here, we just briefly review some basics of quantum computation used in this paper. For a more thorough discussion, please refer to [34].

A quantum system A is a complex Hilbert space $\mathcal{H}$ with an inner product $\langle\cdot|\cdot\rangle$. The state of a quantum system is given by a vector $|\Psi\rangle$ of unit norm ($\langle\Psi|\Psi\rangle = 1$). Given quantum systems A and B over spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, we define the joint or composite quantum system through the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$. The product state of $|\varphi_A\rangle \in \mathcal{H}_A$ and $|\varphi_B\rangle \in \mathcal{H}_B$ is denoted by $|\varphi_A\rangle \otimes |\varphi_B\rangle$ or simply $|\varphi_A\rangle|\varphi_B\rangle$. A n-qubit system lives in the joint quantum system of n two-dimensional Hilbert spaces. The standard computational basis $B = \{|x\rangle\}$ for such a system is given by $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$ for $x = x_1 \cdots x_n$. Any (classical) bit string x is encoded into a quantum state by $|x\rangle$.

Quantum measurement. Quantum measurements are usually described by a collection $\{M_x\}$ of *measurement operators*, which satisfy the *completeness equation*, $\sum_x M_x^\dagger M_x = I$. The index x refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\varphi\rangle$ immediately before the measurement then the probability that result x occurs is given by $\Pr(x) = \langle\varphi|M_x^\dagger M_x|\varphi\rangle$, and the state of the system after the measurement is $\frac{M_x|\varphi\rangle}{\sqrt{\Pr(x)}}$. We say a measurement is in the standard computational basis $B = \{|x\rangle\}$ if the measurement operator M_x is $|x\rangle\langle x|$. For a measurement of $|\varphi\rangle$ in standard computational basis B, x is obtained with probability $|\langle x|\varphi\rangle|^2$.

Quantum algorithm. A quantum algorithm A over a Hilbert space $\mathcal{H}$ with a standard orthonormal basis B is specified by unitary transformation U. The input to A is the initial state $|x_0\rangle$. Then U is applied to the system, and the final state is obtained $|\varphi\rangle = \text{U}|x_0\rangle$. At last, A's output is obtained by performing a measurement on $|\varphi\rangle$. We say that a quantum algorithm is efficient if U is composed of a polynomial number of universal basis gates (the Hadamard, CNOT, and phase shift gates are commonly used).

Quantum random oracle model. Following [25, 49], we view a quantum oracle $\mathcal{O} : \{0,1\}^n \to \{0,1\}^m$ as a mapping that takes basis state $|x\rangle|y\rangle$ into basis state $|x\rangle|y \oplus \mathcal{O}(x)\rangle$ for $x \in \{0,1\}^n$ and $y \in \{0,1\}^m$, and model quantum adversaries with access to $\mathcal{O}$ by the sequence $\mathrm{U} \circ \mathcal{O}$, where U is a unitary transformation. The quantum random oracle model (QROM) [25] is an idealized model where hash functions are modeled as quantum random oracles, and the adversaries are given *quantum* access to these random oracles and *classical* access to all other oracles (e.g., decapsulation oracle).

3 Discrimination of quantum states

Quantum state discrimination [31–33] essentially describes the distinguishability of quantum systems in different states, and has many applications in quantum information field, such as quantum key distribution scheme based on discrimination between non-orthogonal quantum states [50, 51], the study on the foundation of quantum theory [52–55].

The best strategy adopted for quantum state discrimination depends largely on the figures of merit used, for instance, see reviews [31–33]. The three most common figures of merit are minimum-error discrimination, unambiguous state discrimination, and maximum confidence discrimination. Optimal quantum state discrimination is generally difficult apart from the case of two state discrimination. Fortunately, here, we focus on minimum-error discrimination between two pure states.

For two pure states (TPS) $|\psi_0\rangle$ and $|\psi_1\rangle$ with algebraic property

$$|\psi_0\rangle = \sqrt{p}|a\rangle + \sqrt{1-p}|c\rangle \text{ and } |\psi_1\rangle = \sqrt{p}|b\rangle + \sqrt{1-p}|c\rangle,$$

such that $\langle a|b\rangle = \langle a|c\rangle = \langle b|c\rangle = 0$, we consider following game.

Discrimination game DIST *for a distinguisher* D.

- Pick a uniform bit b, i.e., $b \xleftarrow{\$} \{0,1\}$,
- The distinguisher D on input $|\psi_b\rangle$ outputs b' as a guessing of b,
- Return $b' =? b$.

Define the distinguishing advantage of a distinguisher D against DIST game as

$$\mathtt{Adv}^{\mathrm{DIST}}_{\mathrm{TPS}}(\mathsf{D}) := \left|2\Pr[\mathrm{DIST}^{\mathsf{D}}_{\mathrm{TPS}} = 1] - 1\right| = \left|\Pr[\mathsf{D} \Rightarrow 1|b=0] - \Pr[\mathsf{D} \Rightarrow 1|b=1]\right|.$$

The goal of minimum-error discrimination here is to maximize above advantage by optimizing the distinguisher.

To discriminate quantum states, one natural approach is to perform a measurement. Let positive operator M_0 and M_1 be two measurement operators associated with a binary measurement M such that $M_0 + M_1 = I$. Let $P_i^j = \langle\psi_i|M_j^\dagger M_j|\psi_i\rangle$ be the probability that the outcome j occurs when measuring $|\psi_i\rangle$. Then, $\mathtt{Adv}^{\mathrm{DIST}}_{\mathrm{TPS}}(\mathsf{D}) = \left|P_0^1 - P_1^1\right|$. According to [34, Theorem 9.1], the upper bound of the distinguishing advantage $\left|P_0^1 - P_1^1\right|$ is exactly the trace distance between $|\psi_0\rangle$ and $|\psi_1\rangle$, $D(|\psi_0\rangle, |\psi_1\rangle)$, and there exists an *optimal* measurement M that attains this bound. For our specific case,

$$D(|\psi_0\rangle, |\psi_1\rangle) = \sqrt{1 - |\langle\psi_0|\psi_1\rangle|^2} = \sqrt{p(2-p)} \geq \sqrt{p}.$$

The *optimal* measurement M attaining above bound can be found by spectral decomposition of operator $X = \frac{1}{2}(|\psi_0\rangle\langle\psi_0| - |\psi_1\rangle\langle\psi_1|)$ into positive and negative parts [33]. Write the spectral decomposition of the operator by $X = \lambda_+ X_+ - \lambda_- X_-$ with positive (negative) projector X_+ (X_-) and positive (negative) eigenvalue λ_+ (λ_-). Then, the *optimal* measurement M can be given by $M_1 = X_+, M_0 = X_-$. We note that such a spectral decomposition requires distinguisher D knowing both $|\psi_0\rangle$ and $|\psi_1\rangle$. However, the distinguisher D used in Sec. 4 can only know $|\psi_0\rangle$ or $|\psi_1\rangle$.

Before giving an elaborate measurement, we first present two typical constructions of distinguisher D knowing one of $|\psi_0\rangle$ and $|\psi_1\rangle$. Without loss of generality, assume $|\psi_0\rangle$ is known.

One tests wether $|\psi_b\rangle$ is equal to $|\psi_0\rangle$ by a simple but important procedure known as the swap test introduced by [35]. In the test, take $|\psi_0\rangle$ and $|\psi_b\rangle$ as input, attach an ancilla qubit in state $|0\rangle$, then apply a Hadamard gate to the ancilla, followed by a controlled-SWAP gate (controlled on the ancilla), and another Hadamard gate. Finally, measure the ancilla qubit in standard computational basis. The measurement outputs 1 with probability 0 if $b = 0$ and $\frac{1}{2}(1 - |\langle\psi_0|\psi_1\rangle|^2)$ if $b = 1$. Thus, using this swap test, one can just have distinguishing advantage $\left|\frac{1}{2}(1 - |\langle\psi_0|\psi_1\rangle|^2)\right| = \frac{1}{2}p(2-p)$.

Another distinguisher [34] can be constructed by directly performing a measurement with $M_1 = |\psi_0\rangle\langle\psi_0|$ and $M_0 = I - M_1$. Then, the measurement produces outcome 1 with probability 1 if $b = 0$ and $|\langle\psi_0|\psi_1\rangle|^2$ if $b = 1$. Thus, the distinguishing advantage is $|p(2-p)| = p(2-p)$.

As we have seen, the distinguishing advantages of above two typical distinguishers are far from the trace distance $D(|\psi_0\rangle, |\psi_1\rangle) = \sqrt{p(2-p)}$. Taking the algebraic property into consideration, we give an improved distinguisher of which the distinguishing advantage is at least $\sqrt{p}$.

Lemma 3.1. *Let $|\psi_0\rangle = \sqrt{p}|a\rangle + \sqrt{1-p}|c\rangle$ and $|\psi_1\rangle = \sqrt{p}|b\rangle + \sqrt{1-p}|c\rangle$, where $\langle a|b\rangle = \langle a|c\rangle = \langle b|c\rangle = 0$. Let $M_1 = |\psi\rangle\langle\psi|$ and $M_0 = I - M_1$, where $|\psi\rangle = \sin(x)|a\rangle + \cos(x)|c\rangle$ and $x = \frac{1}{2}\arccos(-\frac{\sqrt{p}}{\sqrt{4-3p}})$ ($\sin(2x) \geq 0$). For a distinguisher D that performs a binary measurement with operators M_0 and M_1, the distinguishing advantage has a lower bound $\sqrt{p}$, i.e., $\mathtt{Adv}^{\mathrm{DIST}}_{\mathrm{TPS}}(\mathsf{D}) \geq \sqrt{p}$.*

Proof. Let $\sin(\theta) = \sqrt{p}$ and $\cos(\theta) = \sqrt{1-p}$. Then $\sin(2\theta) = 2\sqrt{p(1-p)}$ and $\cos(2\theta) = 1 - 2p$. Since $x = \frac{1}{2}\arccos(-\frac{\sqrt{p}}{\sqrt{4-3p}})$ and $\sin(2x) \geq 0$, $\sin(2x) = 2\frac{\sqrt{1-p}}{\sqrt{4-3p}}$ and $\cos(2x) = -\frac{\sqrt{p}}{\sqrt{4-3p}}$. The distinguishing advantage

$$\begin{aligned}
\mathtt{Adv}^{\mathrm{DIST}}_{\mathrm{TPS}}(\mathsf{D}) &= \left|\langle\psi_0|M_1^\dagger M_1|\psi_0\rangle - \langle\psi_1|M_1^\dagger M_1|\psi_1\rangle\right| \\
&= \left|(\sin(x)\sin(\theta) + \cos(x)\cos(\theta))^2 - (\cos(x)\cos(\theta))^2\right| \\
&= \left|\sin^2(x)\sin^2(\theta) + 2\sin(x)\sin(\theta)\cos(x)\cos(\theta)\right| \\
&= \frac{1-\cos(2x)}{2}\cdot\frac{1-\cos(2\theta)}{2} + \frac{1}{2}\sin(2x)\sin(2\theta) \\
&= p\frac{1-\cos(2x)}{2} + \sqrt{p(1-p)}\cdot\sin(2x) \\
&= \sqrt{p}(\frac{\sqrt{p}+\sqrt{4-3p}}{2})
\end{aligned}$$

It is easy to verify that $\sqrt{p} + \sqrt{4-3p} \geq 2$ for $0 \leq p \leq 1$. Thus, we have

$$\mathtt{Adv}^{\mathrm{DIST}}_{\mathrm{TPS}}(\mathsf{D}) \geq \sqrt{p}.$$

□

4 An unbounded quantum adversary against the IND-CCA security of KEM

In this section, we will construct an unbounded quantum adversary against the IND-CCA security of $\mathrm{KEM} - \mathrm{U}^{\not\perp}_m = \mathrm{U}^{\not\perp}_m[\mathrm{DPKE}, H, f]$ shown by Fig. 3, where $\mathrm{DPKE} = (Gen', Enc', Dec')$, a hash function $H : \mathcal{M} \to \mathcal{K}$, and a pseudorandom function (PRF) f with key space $\mathcal{K}^{prf}$. The IND-CCA game of $\mathrm{KEM} - \mathrm{U}^{\not\perp}_m$ is given by Fig. 4.

Let $\mathcal{A}(1^\lambda, pk, c^*, K_b)$ be a quantum adversary against the IND-CCA game of $\mathrm{KEM} - \mathrm{U}^{\not\perp}_m$ that does as follows,

1. Search a $m^* \in \mathcal{M}$ such that $Enc'(pk, m^*) = c^*$. If no one (or more than one) is found, output 1 and terminate the procedure.

2. Pick a real p such that $0 \leq p \leq 1$.

3. Sample a m' according to the uniform distribution over $\{m' \in \mathcal{M} : m' \neq m^*\}$.

4. Query the random oracle H with quantum state $|\psi_{-1}\rangle := \sqrt{p}|m^*\rangle|0\rangle + \sqrt{1-p}|m'\rangle|\Sigma\rangle$, where $|\Sigma\rangle = \sum_{k\in\mathcal{K}} \frac{1}{\sqrt{|\mathcal{K}|}}|k\rangle$ can be derived by $H^{\otimes \log|\mathcal{K}|}|0\rangle$. The random oracle returns $|\psi_0\rangle \overset{(*)}{:=} \sqrt{p}|m^*\rangle|K_0\rangle + \sqrt{1-p}|m'\rangle|\Sigma\rangle$.
5. Perform a binary measurement M on $|\psi_0\rangle$ with operators $M_1 = |\Psi\rangle\langle\Psi|$ and $M_0 = I - M_1$, where $|\Psi\rangle = \sin(x)|m^*\rangle|K_b\rangle + \cos(x)|m'\rangle|\Sigma\rangle$ and $x = \frac{1}{2}\arccos(-\frac{\sqrt{p}}{\sqrt{4-3p}})$ $(\sin(2x) \geq 0)$.
6. Output the measurement outcome.

Gen	$Encaps(pk)$	$Decaps(sk', c)$
$(pk, sk) \leftarrow Gen'$	$m \xleftarrow{\$} \mathcal{M}$	Parse $sk' = (sk, k)$
$k \xleftarrow{\$} \mathcal{K}^{prf}$	$c := Enc'(pk, m)$	$m' := Dec'(sk, c)$
$sk' := (sk, k)$	$K := H(m)$	**if** $Enc'(pk, m') = c$
return (pk, sk')	**return** (K, c)	**return** $K := H(m')$
		else return
		$K := f(k, c)$

Fig. 3: IND-CCA-secure KEM $-$ $\mathrm{U}^{\not\perp}_m = \mathrm{U}^{\not\perp}_m[\mathrm{DPKE}, H, f]$

IND-CCA game of KEM $-$ $\mathrm{U}^{\not\perp}_m$	DECAPS $(c \neq c^*)$
$(pk, sk') \leftarrow Gen; H \xleftarrow{\$} \Omega_H$	Parse $sk' = (sk, k)$
$m^* \xleftarrow{\$} \mathcal{M}; c^* := Enc'(pk, m^*)$	$m' := Dec'(sk, c)$
$K_0^* := H(m^*)$	**if** $Enc'(pk, m') = c$
$K_1^* \xleftarrow{\$} \mathcal{K}; b \xleftarrow{\$} \{0, 1\}$	**return** $K := H(m')$
$b' \leftarrow \mathcal{A}^{H,\mathrm{DECAPS}}(pk, c^*, K_b^*)$	**else return**
return $b' =? b$	$K := f(k, c)$

Fig. 4: IND-CCA game of KEM $-$ $\mathrm{U}^{\not\perp}_m$

Remark: The equation $(*)$ is derived by

$$\begin{aligned}
|\psi_0\rangle = \mathcal{O}_H|\psi_{-1}\rangle &= \sqrt{p}|m^*\rangle|H(m^*)\rangle + \sqrt{1-p}|m'\rangle|(\sum_{k\in\mathcal{K}} \frac{1}{|\mathcal{K}|}|k \oplus H(m')\rangle) \\
&= \sqrt{p}|m^*\rangle|K_0\rangle + \sqrt{1-p}|m'\rangle|(\sum_{k\in\mathcal{K}} \frac{1}{|\mathcal{K}|}|k\rangle) \\
&= \sqrt{p}|m^*\rangle|K_0\rangle + \sqrt{1-p}|m'\rangle|\Sigma\rangle.
\end{aligned}$$

Theorem 4.1 (The advantage of $\mathcal{A}$ in the QROM.). *If the underlying DPKE is perfectly correct, the advantage of $\mathcal{A}$ against the IND-CCA security of* KEM $-$ $\mathrm{U}^{\not\perp}_m$ *is at least* $\sqrt{p}(1 - \frac{1}{|\mathcal{K}|})$.

Proof. In the IND-CCA game of KEM $-$ $\mathrm{U}^{\not\perp}_m$, $c^* = Enc'(pk, m^*)$, where $m^* \xleftarrow{\$} \mathcal{M}$, thus there exists at least one $m^* \in \mathcal{M}$ such that $Enc'(pk, m^*) = c^*$. Since DPKE is perfectly correct, there exists no more than one m^* such that $Enc'(pk, m^*) = c^*$. Thus, the m^* that $\mathcal{A}$ gets is exactly the one chosen by the challenger.

Let $|\psi_1\rangle := \sqrt{p}|m^*\rangle|K_1\rangle + \sqrt{1-p}|m'\rangle|\Sigma\rangle$. Let $|a\rangle = |m^*\rangle|K_0\rangle$, $|b\rangle = |m^*\rangle|K_1\rangle$, and $|c\rangle = |m'\rangle|\Sigma\rangle$ Then, $|\psi_0\rangle$, $|\psi_1\rangle$, $|\Psi_0\rangle$ and $|\Psi_1\rangle$ can be rewritten as $|\psi_0\rangle = \sqrt{p}|a\rangle + \sqrt{1-p}|c\rangle$, $|\psi_1\rangle = \sqrt{p}|b\rangle + \sqrt{1-p}|c\rangle$,

$|\Psi_0\rangle = \sin(x)|a\rangle + \cos(x)|c\rangle$ and $|\Psi_1\rangle = \sin(x)|b\rangle + \cos(x)|c\rangle$. The probability $\Pr[\mathcal{A} \Rightarrow 1]$ that $\mathcal{A}$ outputs 1 is $|\langle\psi_0|\Psi_0\rangle|^2$ if $b = 0$, and $|\langle\psi_0|\Psi_1\rangle|^2$ if $b = 1$. Thus,

$$\mathtt{Adv}^{\text{IND-CCA}}_{\text{KEM}-\text{U}^{\not\perp}_m}(\mathcal{A}) = \left| |\langle\psi_0|\Psi_0\rangle|^2 - |\langle\psi_0|\Psi_1\rangle|^2 \right|.$$

When $K_0 = K_1$, $|\Psi_0\rangle = |\Psi_1\rangle$ and the advantage of $\mathcal{A}$ is 0. In the following, we consider the case $K_0 \neq K_1$. It's easy to verify that when $K_0 \neq K_1$, $\langle a|b\rangle = \langle a|c\rangle = \langle b|c\rangle = 0$ since $m^* \neq m'$. Thus, $|\langle\psi_0|\Psi_1\rangle|^2 = |\langle\psi_1|\Psi_0\rangle|^2$. Therefore, the advantage of $\mathcal{A}$ will become

$$\mathtt{Adv}^{\text{IND-CCA}}_{\text{KEM}-\text{U}^{\not\perp}_m}(\mathcal{A}) = \left| |\langle\psi_0|\Psi_0\rangle|^2 - |\langle\psi_1|\Psi_0\rangle|^2 \right|.$$

That is, the advantage function $\mathtt{Adv}^{\text{IND-CCA}}_{\text{KEM}-\text{U}^{\not\perp}_m}(\mathcal{A})$ of $\mathcal{A}$ is exactly the distinguishing advantage $\mathtt{Adv}^{\text{DIST}}_{\text{TPS}}(\mathsf{D})$ of a distinguisher D that distinguishes quantum state $|\psi_0\rangle$ from quantum state $|\psi_1\rangle$ by a binary measurement M' with operators $M'_1 = |\Psi_0\rangle\langle\Psi_0|$ and $M'_0 = I - M'_1$. Thus, according to Lemma 3.1, if $K_0 \neq K_1$, we have $\mathtt{Adv}^{\text{IND-CCA}}_{\text{KEM}-\text{U}^{\not\perp}_m}(\mathcal{A}) \geq \sqrt{p}$. Note that $K_0 \neq K_1$ with probability $1 - \frac{1}{|\mathcal{K}|}$. Thus, we have

$$\mathtt{Adv}^{\text{IND-CCA}}_{\text{KEM}-\text{U}^{\not\perp}_m}(\mathcal{A}) \geq \sqrt{p}(1 - \frac{1}{|\mathcal{K}|}) \approx \sqrt{p}.$$

□

In the ROM, $\mathcal{A}$ can only classically query the random oracle H. That is, before querying H, the input state is measured in standard computational basis. Then, with probability p ($1-p$, resp.), $\mathcal{A}$ will query m^* (m', resp.) to H and get a return hash value $H(m^*)$ ($H(m')$, resp.). Note that classical states (orthogonal quantum states) can be perfectly distinguished. Thus, by testing the equality between the return hash value and K_b, $\mathcal{A}$ can break the IND-CCA security of $\text{KEM} - \text{U}^{\not\perp}_m$ with advantage $1 - \frac{1}{\mathcal{K}}$ if m^* is queried, and 0 if m' is queried. Thus, in the ROM, the advantage of $\mathcal{A}$ will become $p(1 - \frac{1}{|\mathcal{K}|})$.

5 The advantage of a typical measurement-based reduction

In this section, we will bound the advantage of a measurement-based reduction that runs the quantum adversary $\mathcal{A}$ (described in Sec. 4), measures $\mathcal{A}$'s hash query and uses the measurement outcome to break the OW-CPA security of the underlying DPKE. Note that the quantum adversary $\mathcal{A}$ in Sec. 4 just makes a ***single*** query to the random oracle H and no queries to the DECAPS oracle. Thus, the total number q of $\mathcal{A}$'s queries to various oracles is one, i.e., $q = 1$.

First, consider a *natural* measurement-based reduction $R^{\mathcal{A}}(pk, c^*)$ that samples a $k \in \mathcal{K}$, runs $\mathcal{A}(pk, c^*, k)$, measures $\mathcal{A}$'s query to H in computational basis and outputs the measurement outcome. It is apparent that for this natural measurement-based reduction $R^{\mathcal{A}}(pk, c^*)$, the advantage against the OW-CPA security of the underlying DPKE is p, that is $\mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(R^{\mathcal{A}}) = p$. Actually, the proof in [17] for $\text{KEM} - \text{U}^{\not\perp}_m$ from the OW-CPA security of the underlying DPKE exactly adopted this natural measurement-based reduction. Thus, through the adversary $\mathcal{A}$, we have demonstrated that natural measurement-based reduction in [17] ***inevitably*** has a quadratic security loss, $\mathtt{Adv}^{\text{IND-CCA}}_{\text{KEM}-\text{U}^{\not\perp}_m}(\mathcal{A}) \gtrapprox \sqrt{p} = \sqrt{\mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(R^{\mathcal{A}})}$, which matches the bound given by [17].

Next, we will bound the advantage of a typical class of measurement-based reductions. Precisely, we consider a reduction $R^{\mathcal{A}}(pk_1, c_1^*)$ that runs $\mathcal{A}(pk, c^*, K_b)$ once and without rewinding (we do **not** require $(pk, c^*) = (pk_1, c_1^*)$), measures $\mathcal{A}$'s query input in computational basis, use the measurement outcome to break the OW-CPA security of the underlying DPKE.

Theorem 5.1. *If the underlying DPKE is perfectly correct, for any above described measurement-based reduction $R^{\mathcal{A}}$, there exist two meta-reductions MR_1^R and MR_2^R against the OW-CPA security of the underlying*

DPKE such that

$$\mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(R^{\mathcal{A}}) \leq p + \mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(MR_1^R) + \frac{|\mathcal{M}|}{|\mathcal{M}|-1}\mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(MR_2^R),$$

and $\mathsf{Time}(R) \approx \mathsf{Time}(MR_1^R) \approx \mathsf{Time}(MR_2^R)$.

Since the underlying DPKE is perfectly correct, there exists no more than one m^* such that $Enc'(pk, m^*) = c^*$. Let Exi (Ine) be the event that there exists a (no) m^* such that $Enc'(pk, m^*) = c^*$. Thus,

$$\begin{aligned}\mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(R^{\mathcal{A}}) &= \Pr[R^{\mathcal{A}} \Rightarrow m^* \wedge \textsc{Exi}] + \Pr[R^{\mathcal{A}} \Rightarrow m^* \wedge \textsc{Ine}] \\ &\leq \Pr[\textsc{Exi}] \cdot \Pr[R^{\mathcal{A}} \Rightarrow m^* | \textsc{Exi}] + \Pr[R^{\mathcal{A}} \Rightarrow m^* \wedge \textsc{Ine}]. \end{aligned} \tag{1}$$

Denote Good (Bad, resp.) as the event that the measurement of $\mathcal{A}$'s query returns (no, resp.) m^* such that $Enc(pk, m^*) = c^*$. It's apparent that $\Pr[\textsc{Good}|\textsc{Exi}] = p$ and $\Pr[\textsc{Bad}|\textsc{Exi}] = 1 - p$. Thus, we have

$$\begin{aligned}\Pr[R^{\mathcal{A}} \Rightarrow m^* | \textsc{Exi}] &= \Pr[R^{\mathcal{A}} \Rightarrow m^* | \textsc{Exi} \wedge \textsc{Good}] \Pr[\textsc{Good}|\textsc{Exi}] \\ &\quad + \Pr[R^{\mathcal{A}} \Rightarrow m^* | \textsc{Exi} \wedge \textsc{Bad}] \Pr[\textsc{Bad}|\textsc{Exi}] \\ &\leq p + \Pr[R^{\mathcal{A}} \Rightarrow m^* | \textsc{Exi} \wedge \textsc{Bad}]. \end{aligned} \tag{2}$$

Combining the equations (1) and (2), we have

$$\mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(R^{\mathcal{A}}) \leq p + \Pr[R^{\mathcal{A}} \Rightarrow m^* \wedge \textsc{Ine}] + \Pr[\textsc{Exi}] \cdot \Pr[R^{\mathcal{A}} \Rightarrow m^* | \textsc{Exi} \wedge \textsc{Bad}].$$

We give upperbounds of $\Pr[R^{\mathcal{A}} \Rightarrow m^* \wedge \textsc{Ine}]$ and $\Pr[\textsc{Exi}] \cdot \Pr[R^{\mathcal{A}} \Rightarrow m^* | \textsc{Bad} \wedge \textsc{Exi}]$ by following Lemmas 5.1 and 5.2.

Lemma 5.1. *There exists a meta-reduction* MR_1^R *such that* $\Pr[R^{\mathcal{A}} \Rightarrow m^* \wedge \textsc{Ine}] \leq \mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(MR_1^R)$*, and* $\mathsf{Time}(R) \approx \mathsf{Time}(MR_1^R)$.

Proof. Let $\mathcal{A}_1(pk, c^*, K_b)$ be a trivial adversary against the IND-CCA game of $\text{KEM} - \text{U}^{\not\perp}_m$ that always returns 1 and does nothing else. It is obvious that when Ine happens, both $\mathcal{A}$ and $\mathcal{A}_1(pk, c^*, K_b)$ just outputs 1, and $\Pr[R^{\mathcal{A}} \Rightarrow m^* \wedge \textsc{Ine}] = \Pr[R^{\mathcal{A}_1} \Rightarrow m^* \wedge \textsc{Ine}]$.

Construct a meta reduction $MR_1^R(pk_1, c_1^*)$ against the OW-CPA security of DPKE as follows,

1. Run $R^{\mathcal{A}_1}(pk_1, c_1^*)$.
2. Simulate $\mathcal{A}_1(pk, c^*, K_b)$ for $R^{\mathcal{A}_1}(pk_1, c_1^*)$.
3. Return $R^{\mathcal{A}_1}$'s output.

It's easy to see that $\mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(MR_1^R) = \mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(R^{\mathcal{A}_1})$. Since $\mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(R^{\mathcal{A}_1}) \geq \Pr[R^{\mathcal{A}_1} \Rightarrow m^* \wedge \textsc{Ine}]$, we have

$$\Pr[R^{\mathcal{A}} \Rightarrow m^* \wedge \textsc{Ine}] \leq \mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(MR_1^R).$$

Since $\mathsf{Time}(\mathcal{A}_1) \in \mathsf{negl}(\lambda)$, $\mathsf{Time}(MR_1^R) \approx \mathsf{Time}(R) + \mathsf{Time}(\mathcal{A}_1) \approx \mathsf{Time}(R)$. □

Lemma 5.2. *There exists a meta-reduction* MR_2^R *such that*

$$\Pr[\textsc{Exi}] \cdot \Pr[R^{\mathcal{A}} \Rightarrow m^* | \textsc{Exi} \wedge \textsc{Bad}] \leq \frac{|\mathcal{M}|}{|\mathcal{M}|-1}\mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(MR_2^R),$$

and $\mathsf{Time}(R) \approx \mathsf{Time}(MR_2^R)$.

Proof. Let $\mathcal{A}_2(pk, c^*, K_b)$ be an adversary against the IND-CCA game of $\text{KEM} - \text{U}^{\not\perp}_m$ as follows,

1. Pick a real p such that $0 \leq p \leq 1$.
2. Query the random oracle H with quantum state $\psi'_{-1} = \sum_{m,k} \frac{1}{\sqrt{|\mathcal{M}| \cdot |\mathcal{K}|}} |m\rangle|k\rangle$.
3. After the return of the random oracle H, output 1 with probability 1.

We note that under the condition $\text{EXI} \wedge \text{BAD}$, both measurement outcomes of $\mathcal{A}$'s query and $\mathcal{A}_2$'s query obey the uniform distribution over $\{m' \in \mathcal{M} : m' \neq m^*\}$. Thus, $\Pr[R^{\mathcal{A}} \Rightarrow m^* | \text{EXI} \wedge \text{BAD}] = \Pr[R^{\mathcal{A}_2} \Rightarrow m^* | \text{EXI} \wedge \text{BAD}]$ due to the fact that R just uses the information of the measurement outcome to break the OW-CPA sucurity.

Construct a meta reduction $MR_2^R(pk_1, c_1^*)$ against the OW-CPA security of the underlying DPKE as follows,

1. Run $R^{\mathcal{A}_2}(pk_1, c_1^*)$.
2. Simulate $\mathcal{A}_2(pk, c^*, K_b)$ for $R^{\mathcal{A}_2}(pk_1, c_1^*)$.
3. Return $R^{\mathcal{A}_2}$'s output.

It is easy to see that for above $\mathcal{A}_2$ and MR_2^R, $\Pr[\text{GOOD}|\text{EXI}] = \frac{1}{|\mathcal{M}|}$ and $\Pr[\text{BAD}|\text{EXI}] = 1 - \frac{1}{|\mathcal{M}|}$. Then, we have

$$\begin{aligned}
\mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(MR_2^R) = \mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(R^{\mathcal{A}_2}) &\geq \Pr[R^{\mathcal{A}_2} \Rightarrow m^* | \text{EXI}] \cdot \Pr[\text{EXI}] \\
&\geq (1 - \frac{1}{|\mathcal{M}|}) \Pr[R^{\mathcal{A}_2} \Rightarrow m^* | \text{EXI} \wedge \text{BAD}] \cdot \Pr[\text{EXI}] \\
&= (1 - \frac{1}{|\mathcal{M}|}) \Pr[R^{\mathcal{A}} \Rightarrow m^* | \text{EXI} \wedge \text{BAD}] \cdot \Pr[\text{EXI}]
\end{aligned}$$

as we wanted. Since $\mathsf{Time}(\mathcal{A}_2) \in \mathsf{negl}(\lambda)$, $\mathsf{Time}(MR_2^R) \approx \mathsf{Time}(R) + \mathsf{Time}(\mathcal{A}_2) \approx \mathsf{Time}(R)$. □

6 Main results

Combing Theorems 4.1 and 5.1, we can directly obtain following main Theorem.

Theorem 6.1. *If the underlying DPKE is perfectly correct, there exists a quantum adversary $\mathcal{A}$ against the IND-CCA security of* $\text{KEM} - \text{U}_m^{\not\perp}$ *such that for any measurement-based reduction $R^{\mathcal{A}}$ that runs $\mathcal{A}$ (once and without rewinding), measures $\mathcal{A}$'s query and uses the measurement outcome to break the OW-CPA security of the underlying DPKE, there exist two meta-reductions MR_1^R and MR_2^R which take R as a subroutine to break the OW-CPA security of the underlying DPKE such that* $\mathtt{Adv}^{\text{IND-CCA}}_{\text{KEM}-\text{U}_m^{\not\perp}}(\mathcal{A}) \geq$

$$(1 - \frac{1}{|\mathcal{K}|}) \sqrt{\mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(R^{\mathcal{A}}) - \mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(MR_1^R) - \frac{|\mathcal{M}|}{|\mathcal{M}| - 1} \mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(MR_2^R)},$$

and $\mathsf{Time}(R) \approx \mathsf{Time}(MR_1^R) \approx \mathsf{Time}(MR_2^R)$.

Assuming that no PPT adversary can break the OW-CPA security of the underlying DPKE with non-negligible probability, we must have that $\mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(MR_1^R) \approx \mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(MR_2^R) \in \mathsf{negl}(\lambda)$ since $\mathsf{Time}(MR_1^R) \approx \mathsf{Time}(MR_2^R) \approx \mathsf{Time}(R)$ is polynomial[12], and the message space $\mathcal{M}$ is exponentially large due to the brute-force attack. For real-world applications, the key space $\mathcal{K}$ is also exponentially large. Thus, $1 - \frac{1}{|\mathcal{K}|} \approx \frac{|\mathcal{M}|}{|\mathcal{M}|-1} \approx 1$.

Informally, Theorem 6.1 shows the existence of a quantum adversary $\mathcal{A}$ against the IND-CCA security of $\text{KEM} - \text{U}_m^{\not\perp}$ with advantage $\epsilon_{\mathcal{A}} = \mathtt{Adv}^{\text{IND-CCA}}_{\text{KEM}-\text{U}_m^{\not\perp}}(\mathcal{A})$ such that for any typical measurement-based reduction $R^{\mathcal{A}}$ that takes $\mathcal{A}$ as a subroutine to break the OW-CPA security of the underlying DPKE, the advantage $\epsilon_R = \mathtt{Adv}^{\text{OW-CPA}}_{\text{DPKE}}(R^{\mathcal{A}})$ is approximately at most ${\epsilon_{\mathcal{A}}}^2$, i.e., $\epsilon_R \lessapprox {\epsilon_{\mathcal{A}}}^2$. Namely, for $\text{KEM} - \text{U}_m^{\not\perp}$ from a OW-CPA-secure PKE, typical measurement-based reductions ***inevitably*** have a quadratic security loss.

As discussed in Sec. 5, the advantage of currently known reductions, like [17], can approximately attain above bound $\epsilon_R \approx {\epsilon_{\mathcal{A}}}^2$. Thus, Theorem 6.1 also suggests an explanation for the lack of progress in improving the reduction tightness in terms of the degree of security loss.

Remark: One way to hiding (OW2H) lemma [56, Lemma 6.2] is a practical tool to prove the indistinguishability between games where the random oracles are reprogrammed. Essentially, the OW2H lemma

[12] We remark that $\mathsf{Time}(R^{\mathcal{A}}) = \mathsf{Time}(R) + \mathsf{Time}(\mathcal{A})$ is exponential since $\mathcal{A}$ is an unbounded adversary.

gives a generic reduction from a hiding-style property (indistinguishability security) to a one-wayness-style property (unpredictability) with quadratic loss. It is not hard to expand the proof of Theorem 6.1 to show that when arguing the indistinguishability between games where the random oracles are reprogrammed, a reduction from a hiding-style property to a one-wayness-style property will ***inevitably*** have a quadratic security loss. That is, the bound derived by the OW2H lemma is optimal in terms of the degree of loss.

6.1 Extension to other (modular) FO transformations

$\mathrm{U}^{\perp}_{m}$, $\mathrm{U}^{\perp}$, $\mathrm{U}^{\not\perp}$, $\mathrm{QU}^{\not\perp}_{m}$ and $\mathrm{QU}^{\perp}_{m}$ are variants of $\mathrm{U}^{\not\perp}_{m}$, where m (without m, resp.) means $K = H(m)$ ($K = H(m, c)$, resp.), $\not\perp$ ($\perp$, resp.) means implicit (explicit, resp.) rejection[13] and Q means adding an additional Targhi-Unruh hash to the ciphertext. It is easy to see that our main results for $\mathrm{U}^{\not\perp}_{m}$ can also apply to above variants from one-wayness security assumption. That is, typical measurement-based reductions for these variants from one-wayness security assumption will ***inevitably*** have a quadratic security loss.

$\mathrm{FO}^{\not\perp}$, $\mathrm{FO}^{\perp}$, $\mathrm{FO}^{\not\perp}_{m}$, $\mathrm{FO}^{\perp}_{m}$, $\mathrm{QFO}^{\not\perp}_{m}$ and $\mathrm{QFO}^{\perp}_{m}$ in [5] are KEM variants of FO transformation [6, 7], and widely used in the NIST KEM submissions. Following the same analysis for $\mathrm{KEM} - \mathrm{U}^{\not\perp}_{m}$, we can also show that for these KEM variants of FO transformation from standard OW-CPA security (and even IND-CPA security) of the underlying PKE, quadratic security loss is also inevitable for typical measurement-based reductions.

Theorem 6.2. *If the underlying PKE is perfectly correct, there exists a quantum adversary $\mathcal{A}$ against the IND-CCA security of* $\mathrm{KEM} - \mathrm{FO}^{\not\perp}_{m}$ *(see Fig. 5)such that for any measurement-based reduction $R^{\mathcal{A}}$ that runs $\mathcal{A}$ (once and without rewinding), measures $\mathcal{A}$'s query in computational basis, and uses the measurement outcome to break the IND-CPA security (OW-CPA security, resp.) of the underlying PKE, there exist two meta-reductions MR^R_1 and MR^R_2 which take R as a subroutine to break the IND-CPA security (OW-CPA security, resp.) of the underlying PKE such that* $\mathtt{Adv}^{\text{IND-CCA}}_{\text{KEM-FO}^{\not\perp}_{m}}(\mathcal{A}) \geq (1 - \frac{1}{|\mathcal{K}|})$

$$\sqrt{\mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(R^{\mathcal{A}}) - \mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(MR^R_1) - \frac{|\mathcal{M}|}{|\mathcal{M}|-1}\mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(MR^R_2) - \frac{1}{|\mathcal{M}|-1}}$$

$$((1 - \tfrac{1}{|\mathcal{K}|})\sqrt{\mathtt{Adv}^{\text{OW-CPA}}_{\text{PKE}}(R^{\mathcal{A}}) - \mathtt{Adv}^{\text{OW-CPA}}_{\text{PKE}}(MR^R_1) - \tfrac{|\mathcal{M}|}{|\mathcal{M}|-1}\mathtt{Adv}^{\text{OW-CPA}}_{\text{PKE}}(MR^R_2)},\ \textit{resp.})$$

and $\mathsf{Time}(R) \approx \mathsf{Time}(MR^R_1) \approx \mathsf{Time}(MR^R_2)$.

Gen	$Encaps(pk)$	$Decaps(sk', c)$
1 : $(pk, sk) \leftarrow Gen'$	1 : $m \xleftarrow{\$} \mathcal{M}$	1 : Parse $sk' = (sk, k)$
2 : $k \xleftarrow{\$} \mathcal{K}^{prf}$	2 : $c = Enc'(pk, m; G(m))$	2 : $m' := Dec'(sk, c)$
3 : $sk' := (sk, k)$	3 : $K := H(m)$	3 : **if** $Enc'(pk, m'; G(m')) = c$
4 : **return** (pk, sk')	4 : **return** (K, c)	4 : **return** $K := H(m')$
		5 : **else return**
		6 : $K := f(k, c)$

Fig. 5: $\mathrm{KEM} - \mathrm{FO}^{\not\perp}_{m} = \mathrm{FO}^{\not\perp}_{m}[\mathrm{PKE}, G, H, f]$, where $\mathrm{PKE} = (Gen', Enc', Dec')$ with message space $\mathcal{M}$ and randomness space R, $G : \mathcal{M} \to R$, $H : \mathcal{M} \to \mathcal{K}$ are hash functions, and f is a PRF with key space $\mathcal{K}^{prf}$.

Remark: It is not hard to extend above results to other KEM variants of the FO transformation, including $\mathrm{FO}^{\not\perp}$, $\mathrm{FO}^{\perp}$, $\mathrm{FO}^{\perp}_{m}$, $\mathrm{QFO}^{\not\perp}_{m}$ and $\mathrm{QFO}^{\perp}_{m}$, we just omit them in this paper.

Proof. The proof of Theorem 6.2 is similar to the proof of Theorem 6.1. We first construct a quantum adversary $\mathcal{A}$ against the IND-CCA security of $\mathrm{KEM} - \mathrm{FO}^{\not\perp}_{m}$ with advantage at least $(1 - \frac{1}{|\mathcal{K}|})\sqrt{p}$, and then bound the advantage of a typical measurement-based reduction against the IND-CPA security (OW-CPA

[13] In implicit (explicit) rejection, a pseudorandom key (an abnormal symbol $\perp$) is returned for an invalid ciphertext.

security, resp.) of the underlying PKE by running $\mathcal{A}$ and measuring $\mathcal{A}$'s query to utilize the measurement outcome.

Let $\mathcal{A}(1^\lambda, pk, c^*, K_b)$ be a quantum adversary against the IND-CCA security of $\mathrm{KEM}-\mathrm{FO}_m^{\not\perp}$ that does as follows,

1. Search a $m^* \in \mathcal{M}$ and $r^* \in R$ such that $Enc'(pk, m^*; r^*) = c^*$. If none (or more than one) is found, output 1 and terminate the procedure.

2. Pick a real p such that $0 \leq p \leq 1$.

3. Sample a m' according to the uniform distribution over $\{m' \in \mathcal{M} : m' \neq m^*\}$.

4. Query the random oracle H with quantum state $|\psi_{-1}\rangle := \sqrt{p}|m^*\rangle|0\rangle + \sqrt{1-p}|m'\rangle|\Sigma\rangle$, where $|\Sigma\rangle = \sum_{k\in\mathcal{K}} \frac{1}{|\mathcal{K}|}|k\rangle$. The random oracle returns $|\psi_0\rangle := \sqrt{p}|m^*\rangle|K_0\rangle + \sqrt{1-p}|m'\rangle|\Sigma\rangle$.
5. Perform a binary measurement M on $|\psi_0\rangle$ with operators $M_1 = |\Psi\rangle\langle\Psi|$ and $M_0 = I - M_1$, where $|\Psi\rangle = \sin(x)|m^*\rangle|K_b\rangle + \cos(x)|m'\rangle|\Sigma\rangle$ and $x = \frac{1}{2}\arccos(-\frac{\sqrt{p}}{\sqrt{4-3p}})$ $(\sin(2x) \geq 0)$.
6. output the measurement outcome.

In the IND-CCA game of $\mathrm{KEM}-\mathrm{FO}_m^{\not\perp}$, $c^* = Enc'(pk, m^*; G(m^*))$ for some $m^* \in \mathcal{M}$, thus there exists at least one $m^* \in \mathcal{M}$ and $r^* = G(m^*)$ such that $Enc'(pk, m^*; r^*) = c^*$. Since the underlying PKE is perfectly correct, there exist no more than one m^* such that $Enc'(pk, m^*; r^*) = c^*$ for some r^*. Thus, the m^* that $\mathcal{A}$ gets is exactly the one chosen by the challenger. Then, following the proof of Theorem 4.1, we have

$$\mathtt{Adv}^{\text{IND-CCA}}_{\text{KEM-FO}_m^{\not\perp}}(\mathcal{A}) \geq \sqrt{p}(1 - \frac{1}{|\mathcal{K}|}). \tag{3}$$

Then, we use Lemma 6.1 to bound the advantage of a typical measurement-based reduction R which runs $\mathcal{A}$ once without rewinding, measures $\mathcal{A}$'s query input in computational basis and uses the measurement outcome to break the underlying security assumption. Collecting the inequalities (3), (4) and (5) in Lemma 6.1, we can derive the bound as we want in Theorem 6.2.

Lemma 6.1. *If PKE is perfectly correct, for any above typical measurement-based reduction $R^{\mathcal{A}}$, there exist two meta-reductions MR_1^R and MR_2^R that break the IND-CPA (OW-CPA) security of PKE such that* $\mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(R^{\mathcal{A}}) \leq$

$$p + \mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(MR_1^R) + \frac{|\mathcal{M}|}{|\mathcal{M}|-1}\mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(MR_2^R) + \frac{1}{|\mathcal{M}|-1}, \tag{4}$$

$$(\mathtt{Adv}^{\text{OW-CPA}}_{\text{PKE}}(R^{\mathcal{A}}) \leq p + \mathtt{Adv}^{\text{OW-CPA}}_{\text{PKE}}(MR_1^R) + \frac{|\mathcal{M}|}{|\mathcal{M}|-1}\mathtt{Adv}^{\text{OW-CPA}}_{\text{PKE}}(MR_2^R)), \tag{5}$$

and $\mathsf{Time}(R) \approx \mathsf{Time}(MR_1^R) \approx \mathsf{Time}(MR_2^R)$.

Proof of Lemma 6.1 The proof for the case of OW-CPA security is the same as the one of Theorem 5.1. Here, we just consider the reductions $R^{\mathcal{A}}$ against the IND-CPA security of PKE, see Fig. 6.

Game IND-CPA for PKE	
1 :	$(pk_1, sk_1) \leftarrow Gen; \bar{b} \leftarrow \{0,1\}; (m_0, m_1) \leftarrow R^{\mathcal{A}}(pk_1)$
2 :	$c_{\bar{b}}^* \leftarrow Enc(pk_1, m_{\bar{b}}); \bar{b}' \leftarrow R^{\mathcal{A}}(pk_1, c_{\bar{b}}^*);$ **return** $\bar{b}' =? \bar{b}$

Fig. 6: IND-CPA game for PKE.

Since the underlying PKE is perfectly correct, there exists no more than one m^* such that $Enc'(pk, m^*; r^*) = c^*$ for some $r^* \in R$. Let INE (EXI, resp.) be the event that there exists no (a, resp.) m^* such that

$Enc'(pk, m^*; r^*) = c^*$ for some $r^* \in R$. Thus,

$$\begin{aligned}
&\mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(R^{\mathcal{A}}) = \left|2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}] - 1\right| \\
&= \left|\Pr[\textsc{Exi}](2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi}] - 1) + \Pr[\textsc{Ine}](2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Ine}] - 1)\right| \\
&\leq \left|\Pr[\textsc{Exi}](2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi}] - 1)\right| + \left|\Pr[\textsc{Ine}](2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Ine}] - 1)\right| \qquad (6)
\end{aligned}$$

Denote Good (Bad, resp.) as the event that the measurement of $\mathcal{A}$'s query returns (no, resp.) m^* such that $Enc(pk, m^*; r^*) = c^*$ for some $r^* \in R$. It's apparent that

$$\Pr[\textsc{Good}|\textsc{Exi}] = p \text{ and } \Pr[\textsc{Bad}|\textsc{Exi}] = 1 - p.$$

Thus, we have

$$\begin{aligned}
&\left|2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi}] - 1\right| \\
&= |\ (2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Good}] - 1)\Pr[\textsc{Good}|\textsc{Exi}] \\
&\quad +(2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Bad}] - 1)\Pr[\textsc{Bad}|\textsc{Exi}]\ | \\
&\leq p\left|2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Good}] - 1\right| + \left|2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Bad}] - 1\right| \\
&\leq p + \left|2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Bad}] - 1\right|. \qquad (7)
\end{aligned}$$

Combining the equations (6) and (7), we have $\mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(R^{\mathcal{A}}) \leq$

$$p + |\ \Pr[\textsc{Ine}](2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Ine}] - 1)\ | + |\ \Pr[\textsc{Exi}](2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Bad}] - 1)|.$$

By Lemmas 6.2 and Lemma 6.3, we bound $\left|\Pr[\textsc{Ine}](2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Ine}] - 1)\right|$ and $|\ \Pr[\textsc{Exi}](2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Bad}] - 1)\ |$.

Lemma 6.2. *There exists a meta-reduction MR_1^R such that*

$$|\ \Pr[\textsc{Ine}](2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Ine}] - 1)\ | \leq \mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(MR_1^R),$$

and $\mathsf{Time}(R) \approx \mathsf{Time}(MR_1^R)$.

Proof. Define $\mathcal{A}_1(pk, c^*, K_b)$ as a trivial adversary that always returns 1 and does nothing else. It is obvious that when Ine happens, both $\mathcal{A}$ and $\mathcal{A}_1$ just outputs 1, and $\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Ine}] = \Pr[R^{\mathcal{A}_1} \Rightarrow \bar{b}|\textsc{Ine}]$.

Construct a meta reduction $MR_1^R(pk_1)$ against the IND-CPA security of PKE as follows,

1. Run $R^{\mathcal{A}_1}(pk_1)$.
2. Simulate $\mathcal{A}_1(pk, c^*, K_b)$ for $R^{\mathcal{A}_1}(pk_1)$.
3. Output $R^{\mathcal{A}_1}$'s output (m_0, m_1).
4. Send the challenge ciphertext c_b^* to $R^{\mathcal{A}_1}$.
5. Return $R^{\mathcal{A}_1}$'s output $\bar{b}'$.

Since the output of $\mathcal{A}_1$ is independent of Exi and Ine, $\Pr[R^{\mathcal{A}_1} \Rightarrow \bar{b}|\textsc{Exi}] = \Pr[R^{\mathcal{A}_1} \Rightarrow \bar{b}|\textsc{Ine}]$. Then we have

$$\begin{aligned}
&\mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(MR_1^R) = \mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(R^{\mathcal{A}_1}) = \left|2\Pr[R^{\mathcal{A}_1} \Rightarrow \bar{b}] - 1\right| \\
&= \left|\Pr[\textsc{Exi}](2\Pr[R^{\mathcal{A}_1} \Rightarrow \bar{b}|\textsc{Exi}] - 1) + \Pr[\textsc{Ine}](2\Pr[R^{\mathcal{A}_1} \Rightarrow \bar{b}|\textsc{Ine}] - 1)\right| \\
&\overset{(*)}{\geq} \left|\Pr[\textsc{Ine}](2\Pr[R^{\mathcal{A}_1} \Rightarrow \bar{b}|\textsc{Ine}] - 1)\right| \\
&= \left|\Pr[\textsc{Ine}](2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Ine}] - 1)\right|.
\end{aligned}$$

The inequality $(*)$ uses the fact for any reals $a \cdot b \geq 0$, we have $|a + b| \geq |a|$.

Since $\mathsf{Time}(\mathcal{A}_1) \in \mathsf{negl}(\lambda)$, $\mathsf{Time}(MR_1^R) \approx \mathsf{Time}(R) + \mathsf{Time}(\mathcal{A}_1) \approx \mathsf{Time}(R)$. □

Lemma 6.3. *There exists a meta-reduction MR_2^R such that* $|\ \Pr[\textsc{Exi}](2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Bad}] - 1)\ | \leq \frac{|\mathcal{M}|}{|\mathcal{M}|-1}\mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(MR_2^R) + \frac{1}{|\mathcal{M}|-1}$, *and $\mathsf{Time}(R) \approx \mathsf{Time}(MR_2^R)$.*

Proof. Define $\mathcal{A}_2(pk, c^*, K_b)$ as follows,

1. Pick a real p such that $0 \leq p \leq 1$.
2. Query the random oracle H with quantum state $\psi'_{-1} = \sum_{m,k} \frac{1}{\sqrt{|\mathcal{M}|\cdot|\mathcal{K}|}}|m\rangle|k\rangle$.
3. After the return of the random oracle H, return 1 with probability 1.

It is apparent that $\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Bad}] = \Pr[R^{\mathcal{A}_2} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Bad}]$ due to the fact that R just uses the measurement outcome to break the IND-CPA sucurity.

Construct a meta reduction $MR_2^R(pk_1)$ against the IND-CPA security of the underlying PKE as follows,

1. Run $R^{\mathcal{A}_2}(pk_1)$.
2. Simulate $\mathcal{A}_2(pk, c^*, K_b)$ for $R^{\mathcal{A}_2}(pk_1)$.
3. Output $R^{\mathcal{A}_2}$'s output (m_0, m_1).
4. Send the received challenge ciphertext $c^*_{\bar{b}}$ to $R^{\mathcal{A}_2}$.
5. Return $R^{\mathcal{A}_2}(pk_1, c^*_{\bar{b}})$'s output $\bar{b}'$.

Since the output of $\mathcal{A}_2$ is independent of $\textsc{Exi}$ and $\textsc{Ine}$, $\Pr[R^{\mathcal{A}_2} \Rightarrow \bar{b}|\textsc{Exi}] = \Pr[R^{\mathcal{A}_2} \Rightarrow \bar{b}|\textsc{Ine}]$. It is easy to see that for above $\mathcal{A}_2$ and MR_2^R, $\Pr[\textsc{Good}|\textsc{Exi}] = \frac{1}{|\mathcal{M}|}$ and $\Pr[\textsc{Bad}|\textsc{Exi}] = 1 - \frac{1}{|\mathcal{M}|}$. Thus, we have

$$
\begin{aligned}
& \mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(MR_2^R) = \mathtt{Adv}^{\text{IND-CPA}}_{\text{PKE}}(R^{\mathcal{A}_2}) = \left|2\Pr[R^{\mathcal{A}_2} \Rightarrow \bar{b}] - 1\right| \\
= \; & \left|\Pr[\textsc{Exi}](2\Pr[R^{\mathcal{A}_2} \Rightarrow \bar{b}|\textsc{Exi}] - 1) + \Pr[\textsc{Ine}](2\Pr[R^{\mathcal{A}_2} \Rightarrow \bar{b}|\textsc{Ine}] - 1)\right| \\
\overset{(**)}{\geq} \; & \left|\Pr[\textsc{Exi}](2\Pr[R^{\mathcal{A}_2} \Rightarrow \bar{b}|\textsc{Exi}] - 1)\right| \\
= \; & \Pr[\textsc{Exi}] \mid \Pr[\textsc{Good}|\textsc{Exi}](2\Pr[R^{\mathcal{A}_2} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Good}] - 1) \\
& \qquad + \Pr[\textsc{Bad}|\textsc{Exi}](2\Pr[R^{\mathcal{A}_2} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Bad}] - 1) \mid \\
\overset{(***)}{\geq} \; & \Pr[\textsc{Exi}]\left|\Pr[\textsc{Bad}|\textsc{Exi}](2\Pr[R^{\mathcal{A}_2} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Bad}] - 1)\right| \\
& \qquad - \Pr[\textsc{Exi}]\left|\Pr[\textsc{Good}|\textsc{Exi}](2\Pr[R^{\mathcal{A}_2} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Good}] - 1)\right| \\
\geq \; & \Pr[\textsc{Exi}](1 - \frac{1}{|\mathcal{M}|})\left|2\Pr[R^{\mathcal{A}_2} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Bad}] - 1\right| - \frac{1}{|\mathcal{M}|} \\
= \; & (1 - \frac{1}{|\mathcal{M}|})\left|\Pr[\textsc{Exi}](2\Pr[R^{\mathcal{A}} \Rightarrow \bar{b}|\textsc{Exi} \wedge \textsc{Bad}] - 1)\right| - \frac{1}{|\mathcal{M}|}
\end{aligned}
$$

as we wanted, where the inequality $(**)$ uses the fact $|a + b| \geq |a|$ for any reals $a \cdot b \geq 0$, and the inequality $(***)$ uses the fact $|a + b| \geq |a| - |b|$ for any any reals a, b.

Since $\mathsf{Time}(\mathcal{A}_2) \in \mathsf{negl}(\lambda)$, $\mathsf{Time}(MR_2^R) \approx \mathsf{Time}(R) + \mathsf{Time}(\mathcal{A}_2) \approx \mathsf{Time}(R)$. □

Acknowledgements. We thank Dominique Unruh for the interesting discussions on the one way to hiding lemma, which motivates this work. In particular, this work is supported by the National Key Research and Development Program of China (No. 2017YFB0802000), the National Natural Science Foundation of China (No. U1536205, 61472446, 61701539), and the National Cryptography Development Fund (mmjj20180107, mmjj20180212).

References

1. Rackoff, C., Simon, D.: Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In Feigenbaum, J., ed.: Advances in Cryptology – CRYPTO 1991. Volume 576 of LNCS., Springer (1992) 433–444
2. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing **33**(1) (2003) 167–226
3. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In Denning, D.E., Pyle, R., Ganesan, R., Sandhu, R.S., Ashby, V., eds.: Proceedings of the 1st ACM Conference on Computer and Communications Security – CCS 1993, ACM (1993) 62–73

4. Dent, A.W.: A designer's guide to KEMs. In Paterson, K.G., ed.: Cryptography and Coding: 9th IMA International Conference. Volume 2898 of LNCS., Springer-Verlag (2003) 133–151
5. Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the Fujisaki-Okamoto transformation. In Kalai, Y., Reyzin, L., eds.: Theory of Cryptography - 15th International Conference – TCC 2017. Volume 10677 of LNCS., Springer (2017) 341–371
6. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In Wiener, M.J., ed.: Advances in Cryptology – CRYPTO 1999. Volume 99 of LNCS., Springer (1999) 537–554
7. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. Journal of cryptology **26**(1) (2013) 1–22
8. Okamoto, T., Pointcheval, D.: REACT: Rapid enhanced-security asymmetric cryptosystem transform. In Naccache, D., ed.: Topics in Cryptology – CT-RSA 2001. Volume 2020 of LNCS., Springer (2001) 159–174
9. Jean-Sébastien, C., Handschuh, H., Joye, M., Paillier, P., Pointcheval, D., Tymen, C.: GEM: A generic chosen-ciphertext secure encryption method. In Preneel, B., ed.: Topics in Cryptology – CT-RSA 2002. Volume 2271 of LNCS., Springer (2002) 263–276
10. Targhi, E.E., Unruh, D.: Post-quantum security of the Fujisaki-Okamoto and OAEP transforms. In Hirt, M., Smith, A.D., eds.: Theory of Cryptography Conference – TCC 2016-B. Volume 9986 of LNCS., Springer (2016) 192–216
11. Menezes, A.: Another look at provable security (2012) Invited Talk at EUROCRYPT 2012, `https://www.iacr.org/cryptodb/archive/2012/EUROCRYPT/presentation/24260.pdf`.
12. Guo, F., Chen, R., Susilo, W., Lai, J., Yang, G., Mu, Y.: Optimal security reductions for unique signatures: Bypassing impossibilities with a counterexample. In Katz, J., Shacham, H., eds.: Advances in Cryptology – CRYPTO 2017. Volume 10402 of LNCS., Springer (2017) 517–547
13. Bellare, M., Rogaway, P.: Optimal asymmetric encryption. In Santis, A.D., ed.: Advances in Cryptology – EUROCRYPT 1994. Volume 950 of LNCS., Springer (1994) 92–111
14. Fujisaki, E., Okamoto, T., Pointcheval, D., Stern, J.: RSA-OAEP is secure under the RSA assumption. In Kilian, J., ed.: Advances in Cryptology – CRYPTO 2001. Volume 2139 of LNCS., Springer (2001) 260–274
15. Abdalla, M., Bellare, M., Rogaway, P.: The oracle Diffie-Hellman assumptions and an analysis of DHIES. In Naccache, D., ed.: CT-RSA 2001. Volume 2020 of LNCS., Springer (2001) 143–158
16. Saito, T., Xagawa, K., Yamakawa, T.: Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In Nielsen, J.B., Rijmen, V., eds.: Advances in Cryptology – EUROCRYPT 2018. Volume 10822 of LNCS. (2018) 520–551
17. Jiang, H., Zhang, Z., Chen, L., Wang, H., Ma, Z.: IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited. In Shacham, H., Boldyreva, A., eds.: Advances in Cryptology – CRYPTO 2018. Volume 10993 of LNCS. (2018) 96–125 `https://eprint.iacr.org/2017/1096`.
18. Jiang, H., Zhang, Z., Ma, Z.: Key encapsulation mechanism with explicit rejection in the quantum random oracle model. In Lin, D., Sako, K., eds.: Public-Key Cryptography - PKC 2019. Volume 11443 of LNCS., Springer (2019) 618–645
19. Jiang, H., Zhang, Z., Ma, Z.: Tighter security proofs for generic key encapsulation mechanism in the quantum random oracle model. Post-Quantum Cryptography - 5th International Workshop – PQCrypto 2019 (to appear) (2019)
20. Bernstein, D.J., Persichetti, E.: Towards KEM unification. Cryptology ePrint Archive, Report 2018/526 (2018) `https://eprint.iacr.org/2018/526`.
21. Szepieniec, A., Reyhanitabar, R., Preneel, B.: Key encapsulation from noisy key agreement in the quantum random oracle model. Cryptology ePrint Archive, Report 2018/884 (2018) `https://eprint.iacr.org/2018/884`.
22. Hövelmanns, K., Kiltz, E., Schäge, S., Unruh, D.: Generic authenticated key exchange in the quantum random oracle model. Cryptology ePrint Archive, Report 2018/928 (2018) `https://eprint.iacr.org/2018/928`.
23. Xagawa, K., Yamakawa, T.: (tightly) QCCA-secure key-encapsulation mechanism in the quantum random oracle model. Post-Quantum Cryptography – PQCrypto 2019 (to appear) (2019) `https://eprint.iacr.org/2018/838`.
24. NIST: National institute for standards and technology. Post quantum crypto project (2017) `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.
25. Boneh, D., Dagdelen, O., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In Lee, D.H., Wang, X., eds.: Advances in Cryptology – ASIACRYPT 2011. Volume 7073 of LNCS., Springer (2011) 41–69
26. Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. Cryptology ePrint Archive, Report 2018/904 (2018) `https://eprint.iacr.org/2018/904`.
27. Ducas, L., Stehlé, D.: Assessing the security of lattice-based submissions: the 10 questions that NIST should be asking the community (2018) `http://prometheuscrypt.gforge.inria.fr/2018-06-04.assessing-security.html`.

28. Ambainis, A., Rosmanis, A., Unruh, D.: Quantum attacks on classical proof systems: The hardness of quantum rewinding. In: 55th IEEE Annual Symposium on Foundations of Computer Science – FOCS 2014, IEEE (2014) 474–483
29. Boneh, D., Venkatesan, R.: Breaking rsa may not be equivalent to factoring. In Nyberg, K., ed.: Advances in Cryptology – EUROCRYPT 1998. Volume 1403 of LNCS., Springer (1998) 59–71
30. Coron, J.S.: Optimal security proofs for PSS and other signature schemes. In Knudsen, L.R., ed.: Advances in Cryptology – EUROCRYPT 2002. Volume 2332 of LNCS., Springer (2002) 272–287
31. Chefles, A.: Quantum state discrimination. Contemporary Physics **41**(6) (2000) 401–424
32. Barnett, S.M., Croke, S.: Quantum state discrimination. Advances in Optics and Photonics **1**(2) (2009) 238–278
33. Bae, J., Kwek, L.C.: Quantum state discrimination and its applications. Journal of Physics A: Mathematical and Theoretical **48**(8) (2015) 083001
34. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Number 2. Cambridge University Press (2000)
35. Buhrman, H., Cleve, R., Watrous, J., De Wolf, R.: Quantum fingerprinting. Physical Review Letters **87**(16) (2001) 167902
36. Dodis, Y., Oliveira, R., Pietrzak, K.: On the generic insecurity of the full domain hash. In Shoup, V., ed.: Advances in Cryptology – CRYPTO 2005. Volume 3621 of LNCS., Springer (2005) 449–466
37. Garg, S., Bhaskar, R., Lokam, S.V.: Improved bounds on security reductions for discrete log based signatures. In Wagner, D.A., ed.: Advances in Cryptology – CRYPTO 2008. Volume 5157 of LNCS., Springer (2008) 93–107
38. Seurin, Y.: On the exact security of Schnorr-type signatures in the random oracle model. In Pointcheval, D., Johansson, T., eds.: Advances in Cryptology – EUROCRYPT 2012. Volume 7237 of LNCS., Springer (2012) 554–571
39. Fischlin, M., Fleischhacker, N.: Limitations of the meta-reduction technique: The case of Schnorr signatures. In Johansson, T., Nguyen, P.Q., eds.: Advances in Cryptology – EUROCRYPT 2013. Volume 7881 of LNCS., Springer (2013) 444–460
40. Dagdelen, Ö., Fischlin, M., Gagliardoni, T.: The Fiat-Shamir transformation in a quantum world. In: Advances in Cryptology – ASIACRYPT 2013, Springer (2013) 62–81
41. Fleischhacker, N., Jager, T., Schröder, D.: On tight security proofs for Schnorr signatures. In Sarkar, P., Iwata, T., eds.: Advances in Cryptology – ASIACRYPT 2014. Volume 8873 of LNCS., Springer (2014) 512–531
42. Lewko, A., Waters, B.: Why proving HIBE systems secure is difficult. In Nguyen, P.Q., Oswald, E., eds.: Advances in Cryptology – EUROCRYPT 2014. Volume 8441 of LNCS., Springer (2014) 58–76
43. Bader, C., Jager, T., Li, Y., Schäge, S.: On the impossibility of tight cryptographic reductions. In Fischlin, M., Coron, J., eds.: Advances in Cryptology – EUROCRYPT 2016. Volume 9666 of LNCS., Springer (2016) 273–304
44. Kakvi, S.A., Kiltz, E.: Optimal security proofs for Full Domain Hash, revisited. Journal of Cryptology **31**(1) (2018) 276–306
45. Fischlin, M.: Black-box reductions and separations in cryptography. In Mitrokotsa, A., Vaudenay, S., eds.: Progress in Cryptology - AFRICACRYPT 2012. Volume 7374 of LNCS., Springer (2012) 413–422
46. Watrous, J.: Zero-knowledge against quantum attacks. SIAM Journal on Computing **39**(1) (2009) 25–58
47. Unruh, D.: Quantum proofs of knowledge. In Pointcheval, D., Johansson, T., eds.: Advances in Cryptology – EUROCRYPT 2012. Volume 7237 of LNCS., Springer (2012) 135–152
48. Unruh, D.: Post-quantum security of Fiat-Shamir. In Takagi, T., Peyrin, T., eds.: Advances in Cryptology – ASIACRYPT 2017. Volume 10624 of LNCS., Springer (2017) 65–95
49. Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. In: 39th FOCS
50. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Theor. Comput. Sci. **560**(P1) (2014) 7–11
51. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Physical Review Letters **68**(21) (1992) 3121
52. Pusey, M.F., Barrett, J., Rudolph, T.: On the reality of the quantum state. Nature Physics **8**(6) (2012) 475
53. Bae, J., Hwang, W.Y., Han, Y.D.: No-signaling principle can determine optimal quantum state discrimination. Physical Review Letters **107**(17) (2011) 170403
54. Brunner, N., Navascués, M., Vértesi, T.: Dimension witnesses and quantum state discrimination. Physical Review Letters **110**(15) (2013) 150501
55. Konig, R., Renner, R., Schaffner, C.: The operational meaning of min-and max-entropy. IEEE Transactions on Information theory **55**(9) (2009) 4337–4347
56. Unruh, D.: Revocable quantum timed-release encryption. Journal of the ACM **62**(6) (2015) 49:1–49:76