

A Modular Analysis of the Fujisaki-Okamoto Transformation

Dennis Hofheinz ¹

Kathrin Hövelmanns ²

Eike Kiltz ²

November 2, 2021

¹ Karlsruhe Institute of Technology

`Dennis.Hofheinz@kit.edu`

² Ruhr Universität Bochum

`{Kathrin.Hoevermanns,Eike.Kiltz}@rub.de`

Abstract

The Fujisaki-Okamoto (FO) transformation (CRYPTO 1999 and Journal of Cryptology 2013) turns any weakly secure public-key encryption scheme into a strongly (i.e., IND-CCA) secure one in the random oracle model. Unfortunately, the FO analysis suffers from several drawbacks, such as a non-tight security reduction, and the need for a perfectly correct scheme. While several alternatives to the FO transformation have been proposed, they have stronger requirements, or do not obtain all desired properties.

In this work, we provide a fine-grained and modular toolkit of transformations for turning weakly secure into strongly secure public-key encryption schemes. All of our transformations are robust against schemes with correctness errors, and their combination leads to several tradeoffs among tightness of the reduction, efficiency, and the required security level of the used encryption scheme. For instance, one variant of the FO transformation constructs an IND-CCA secure scheme from an IND-CPA secure one with a tight reduction and very small efficiency overhead. Another variant assumes only an OW-CPA secure scheme, but leads to an IND-CCA secure scheme with larger ciphertexts.

We note that we also analyze our transformations in the quantum random oracle model, which yields security guarantees in a post-quantum setting.

Keywords: public-key encryption, Fujisaki-Okamoto transformation, tight reductions, quantum random oracle model

Errata

In previous versions of this paper, the theorems stating security of transformations U_m^\perp (Theorem 3.5) and U_m^\times (Theorem 3.6) were incorrect. This was observed by Bernstein and Persichetti [BP18] who also noted that the theorems can be fixed by additionally requiring the underlying deterministic PKE scheme to be rigid. Rigidity means that unless decryption of a ciphertext c fails, decrypting c and then re-encrypting yields c , i.e., $\text{Enc}(pk, \text{Dec}(sk, c)) = c$. This issue does not affect our overall results for the respective Fujisaki-Okamoto transformations ($\text{FO}_m^\times = U_m^\times \circ \text{T}$, $\text{FO}_m^\perp = U_m^\perp \circ \text{T}$) since the rigidity requirement is naturally met by transformation T .

This version furthermore corrects the following counting mistakes: The δ -term in the ROM bounds for T (i.e., the bounds in Theorem 3.1 and 3.2) is $(q_G + q_P) \cdot \delta$ instead of $q_G \cdot \delta$. Similarly, the term in the respective QROM bound (see Theorem 4.4) is $8 \cdot (q_G + q_P + 1)^2 \cdot \delta$ instead of $8 \cdot (q_G + 1)^2 \cdot \delta$. Furthermore, the advantage term in Theorem 3.1 is $(q_G + q_P + 1) \cdot \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\mathbf{A})$ instead of $(q_G + 1) \cdot \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\mathbf{A})$. These corrections do not affect the overall ROM results for the Fujisaki-Okamoto transformations, as the bounds given in Section 3.3 already covered the additional term (because $q_G + q_P$ translates to q_{RO}).

An updated version of this work with an improved presentation of the proofs is given in [Höv21, Sections 2.1 and 2.2].

Contents

1	Introduction	2
1.1	Our contributions	3
1.1.1	Our transformations in detail	4
1.1.2	The resulting FO transformations	5
1.1.3	Example Instantiations	6
1.1.4	Transformation S^ℓ : from OW-CPA to IND-CPA, Tightly	6
1.2	Related work	7
2	Preliminaries	7
2.1	Public-Key Encryption	7
2.2	Key Encapsulation	9
3	Modular FO Transformations	10
3.1	Transformation T : from OW-CPA/IND-CPA to OW-PCVA	10
3.2	Transformations $U^\times, U_m^\times, U^\perp, U_m^\perp$	13
3.2.1	Transformation U^\perp : from OW-PCVA to IND-CCA	13
3.2.2	Transformation U^\times : from OW-PCA to IND-CCA	15
3.2.3	Transformations U_m^\times/U_m^\perp : from OW-CPA/OW-VA to IND-CCA for deterministic Encryption	18
3.3	The resulting KEMs	21
3.4	S^ℓ : from OW-CPA to IND-CPA Security, tightly	22
4	Modular FO Transformation in the QROM	25
4.1	Quantum Computation	25
4.2	Transformation T : from OW-CPA to OW-PCA in the QROM	27
4.3	Transformations QU_m^\perp, QU_m^\times	29
4.3.1	Transformation QU_m^\perp : from OW-PCA to IND-CCA in the QROM	29
4.3.2	Transformation QU_m^\times : from OW-PCA to IND-CCA in the QROM	33
4.4	The resulting KEMs	34

1 Introduction

The notion of INDistinguishability against Chosen-Ciphertext Attacks (IND-CCA) [RS92] is now widely accepted as the standard security notion for asymmetric encryption schemes. Intuitively, IND-CCA security requires that no efficient adversary can recognize which of two messages is encrypted in a given ciphertext, even if the two candidate messages are chosen by the adversary himself. In contrast to the similar but weaker notion of INDistinguishability against Chosen-Plaintext Attacks (IND-CPA), an IND-CCA adversary is given access to a decryption oracle throughout the attack.

GENERIC TRANSFORMATIONS ACHIEVING IND-CCA SECURITY. While IND-CCA security is in many applications the desired notion of security, it is usually much more difficult to prove than IND-CPA security. Thus, several transformations have been suggested that turn a public-key encryption (PKE) scheme with weaker security properties into an IND-CCA one generically. For instance, in a seminal paper, Fujisaki and Okamoto [FO99, FO13] proposed a generic transformation (FO transformation) combining any One-Way (OW-CPA) secure asymmetric encryption scheme with any one-time secure symmetric encryption scheme into a Hybrid encryption scheme that is (IND-CCA) secure in the random oracle model [BR93]. Subsequently, Okamoto and Pointcheval [OP01] and Coron et al. [CHJ+02] proposed two more generic transformations (called REACT and GEM) that are considerably simpler but require the underlying asymmetric scheme to be One-Way against Plaintext Checking Attacks (OW-PCA). OW-PCA security is a non-standard security notion that provides the adversary with a plaintext checking oracle $PCO(c, m)$ that returns 1 iff decryption of ciphertext c yields message m . A similar transformation was also implicitly used in the “Hashed ElGamal” encryption scheme by Abdalla et al. [ABR01].

KEMs. In his “A Designer’s Guide to KEMs” paper, Dent [Den03] provides “more modern” versions of the FO [Den03, Table 5] and the REACT/GEM [Den03, Table 2] transformations that result in

IND-CCA secure key-encapsulation mechanisms (KEMs). Recall that any IND-CCA secure KEM can be combined with any (one-time) chosen-ciphertext secure symmetric encryption scheme to obtain a IND-CCA secure PKE scheme [CS03]. Due to their efficiency and versatility, in practice one often works with such hybrid encryption schemes derived from a KEM. For that reason the primary goal of our paper will be constructing IND-CCA secure KEMs.

We remark that all previous variants of the FO transformation require the underlying PKE scheme to be γ -spread [FO99], which essentially means that ciphertexts (generated by the probabilistic encryption algorithm) have sufficiently large entropy.

SECURITY AGAINST QUANTUM ADVERSARIES. Recently, the above mentioned generic transformations have gathered renewed interest in the quest of finding an IND-CCA secure asymmetric encryption scheme that is secure against quantum adversaries, i.e., adversaries equipped with a quantum computer. In particular, the NIST announced a competition with the goal to standardize new asymmetric encryption systems [NIS17] with security against quantum adversaries. Natural candidates base their IND-CPA security on the hardness of certain problems over lattices and codes, which are generally believed to resist quantum adversaries. Furthermore, quantum computers may execute all “offline primitives” such as hash functions on arbitrary superpositions, which motivated the introduction of the quantum (accessible) random oracle model [BDF⁺11]. Targhi and Unruh recently proved a variant of the FO transformation secure in the quantum random oracle model [TU16]. Helping to find IND-CCA secure KEM with provable (post-quantum) security will thus be an important goal in this paper.

DISCUSSION. Despite their versatility, the above FO and REACT/GEM transformations have a couple of small but important disadvantages.

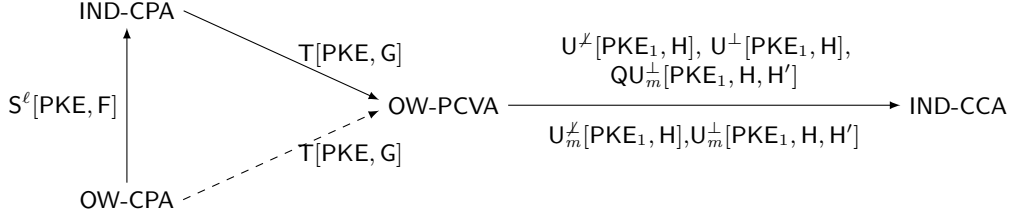
- **Tightness.** The security reduction of the FO transformation [FO99, FO13] in the random oracle model is not tight, i.e., it loses a factor of q_G , the number of random oracle queries. A non-tight security proof requires to adapt the system parameters accordingly, which results in considerably less efficient schemes. The REACT/GEM transformations have a tight security reduction, but they require the underlying encryption scheme to be OW-PCA secure. As observed by Peikert [Pei14], due to their decision/search equivalence, many natural lattice-based encryption schemes are not OW-PCA secure and it is not clear how to modify them to be so. In fact, the main technical difficulty is to build an IND-CPA or OW-PCA secure encryption scheme from an OW-CPA secure one, with a tight security reduction.
- **Correctness error.** The FO, as well as the REACT/GEM transformation require the underlying asymmetric encryption scheme to be perfectly correct, i.e., not having a decryption error. In general, one cannot exclude the fact that even a (negligibly) small decryption error could be exploited by a concrete IND-CCA attack against FO-like transformed schemes. Dealing with imperfectly correct schemes is of great importance since many (but not all) practical lattice-based encryption schemes have a small correctness error, see, e.g., DXL [DXL12], Peikert [Pei14], BCNS [BCNS15], New Hope [ADPS16], Frodo [BCD⁺16], Lizard [CKLS16], and Kyber [BDK⁺17].¹

These deficiencies were of little or no concern when the FO and REACT/GEM transformations were originally devised. Due to the emergence of large-scale scenarios (which benefit heavily from tight security reductions) and the increased popularity of lattice-based schemes with correctness defects, however, we view these deficiencies as acute problems.

1.1 Our contributions

Our main contribution is a modular treatment of FO-like transformations. That is, we provide fine-grained transformations that can be used to turn an OW-CPA secure PKE scheme into an IND-CCA secure one in several steps. For instance, we provide separate OW-CPA \rightarrow OW-PCA and OW-PCA \rightarrow IND-CCA transformations that, taken together, yield the original FO transformation. However, we also provide variants of these individual transformations that achieve different security goals and tightness properties.

¹Lattice-based encryption schemes can be made perfectly correct by putting a limit on the noise and setting the modulus of the LWE instance large enough, see e.g. [BCLV16, HGSW05]. But increasing the size of the modulus makes the LWE problem easier to solve in practice, and thus the dimension of the problem needs to be increased in order to obtain the same security levels. Larger dimension and modulus increase the public-key and ciphertext length.



Transformation	Security implication	QRom?	ROM Tightness?	Requirements
$\text{PKE}_1 = \text{T}[\text{PKE}, \text{G}]$ (§3.1)	$\text{OW-CPA} \Rightarrow \text{OW-PCA}$	✓	—	none
$\text{PKE}_1 = \text{T}[\text{PKE}, \text{G}]$ (§3.1)	$\text{IND-CPA} \Rightarrow \text{OW-PCA}$	✓	✓	none
$\text{PKE}_1 = \text{T}[\text{PKE}, \text{G}]$ (§3.1)	$\text{OW-CPA} \Rightarrow \text{OW-PCVA}$	✓	—	γ -spread
$\text{PKE}_1 = \text{T}[\text{PKE}, \text{G}]$ (§3.1)	$\text{IND-CPA} \Rightarrow \text{OW-PCVA}$	—	✓	γ -spread
$\text{KEM}^x = \text{U}^x[\text{PKE}_1, \text{H}]$ (§3.2)	$\text{OW-PCA} \Rightarrow \text{IND-CCA}$	—	✓	none
$\text{KEM}^\perp = \text{U}^\perp[\text{PKE}_1, \text{H}]$ (§3.2.1)	$\text{OW-PCVA} \Rightarrow \text{IND-CCA}$	—	✓	none
$\text{KEM}_m^x = \text{U}_m^x[\text{PKE}_1, \text{H}]$ (§3.2.3)	$\text{OW-CPA} \Rightarrow \text{IND-CCA}$	—	✓	det. PKE_1
$\text{KEM}_m^\perp = \text{U}_m^\perp[\text{PKE}_1, \text{H}]$ (§3.2.3)	$\text{OW-VA} \Rightarrow \text{IND-CCA}$	—	✓	det. PKE_1
$\text{QKEM}_m^\perp = \text{QU}_m^\perp[\text{PKE}_1, \text{H}, \text{H}']$ (§4.3.1)	$\text{OW-PCA} \Rightarrow \text{IND-CCA}$	✓	✓	none
$\text{PKE}_\ell = \text{S}^\ell[\text{PKE}, \text{F}]$ (§3.4)	$\text{OW-CPA} \Rightarrow \text{IND-PCA}$	—	✓	none

Figure 1: Our modular transformations. Top: solid arrows indicate tight reductions, dashed arrows indicate non-tight reductions. Bottom: properties of the transformations. The tightness row only refers to tightness in the standard random oracle model; all our reductions in the quantum random oracle model are non-tight.

All of our individual transformations are robust against PKE schemes with correctness errors (in the sense that the correctness error of the resulting schemes can be bounded by the correctness error of the original scheme).

The benefit of our modular treatment is not only a conceptual simplification, but also a larger variety of possible combined transformations (with different requirements and properties). For instance, combining two results about our transformations T and U^x , we can show that the original FO transformation yields IND-CCA security from IND-CPA security with a *tight* security reduction. Combining S^ℓ with T and U^x , on the other hand, yields tight IND-CCA security from the weaker notion of OW-CPA security, at the expense of a larger ciphertext. (See Figure 1 for an overview.)

1.1.1 Our transformations in detail

In the following, we give a more detailed overview over our transformations. We remark that all our transformations require a PKE scheme (and not a KEM). We view it as an interesting open problem to construct similar transformations that only assume (and yield) KEMs, since such transformations have the potential of additional efficiency gains.

T: FROM OW-CPA TO OW-PCA SECURITY (“DERANDOMIZATION”+“RE-ENCRYPTION”). T is the Encrypt-with-Hash construction from [BBO07], originally proposed in [BHSV98, Sec. 5]: Starting from an encryption scheme PKE and a hash function G , we build a deterministic encryption scheme $\text{PKE}_1 = \text{T}[\text{PKE}, \text{G}]$ by defining

$$\text{Enc}_1(pk, m) := \text{Enc}(pk, m; \text{G}(m)),$$

where $\text{G}(m)$ is used as the random coins for Enc . Note that Enc_1 is deterministic. $\text{Dec}_1(sk, c)$ first decrypts c into m' and rejects if $\text{Enc}(pk, m'; \text{G}(m')) \neq c$ (“re-encryption”). Modeling G as a random oracle, OW-PCA security of PKE_1 non-tightly reduces to OW-CPA security of PKE and tightly reduces to IND-CPA security of PKE . If PKE furthermore is γ -spread (for sufficiently large γ), then PKE_1 is even OW-PCVA secure.

OW-PCVA security² is PCA security, where the adversary is additionally given access to a validity oracle $\text{Cvo}(c)$ that checks c 's validity (in the sense that it does not decrypt to \perp , see also Definition 2.1).

$\text{U}^\times (\text{U}^\perp)$: FROM OW-PCA (OW-PCVA) TO IND-CCA SECURITY (“HASHING”). Starting from an encryption scheme PKE_1 and a hash function H , we build a key encapsulation mechanism $\text{KEM}^\times = \text{U}^\times[\text{PKE}_1, \text{H}]$ with “implicit rejection” by defining

$$\text{Encaps}(pk) := (c \leftarrow \text{Enc}_1(pk, m), K := \text{H}(c, m)), \quad (1)$$

where m is picked at random from the message space.

$$\text{Decaps}^\times(sk, c) = \begin{cases} \text{H}(c, m) & m \neq \perp \\ \text{H}(c, s) & m = \perp \end{cases}, \quad (2)$$

where $m := \text{Dec}(sk, c)$ and s is a random seed which is contained in sk . Modeling H as a random oracle, IND-CCA security of KEM^\times tightly reduces to OW-PCA security of PKE_1 . In the context of the FO transformation, implicit rejection was first introduced by Persichetti [Per12, Sec. 5.3].

We also define $\text{KEM}^\perp = \text{U}^\perp[\text{PKE}_1, \text{H}]$ with “explicit rejection” which differs from KEM^\times only in decapsulation:

$$\text{Decaps}^\perp(sk, c) = \begin{cases} \text{H}(c, m) & m \neq \perp \\ \perp & m = \perp \end{cases}, \quad (3)$$

where $m := \text{Dec}(sk, c)$. Modeling H as a random oracle, IND-CCA of KEM^\perp security tightly reduces to OW-PCVA security of PKE_1 . We remark that transformation U^\perp is essentially [Den03, Table 2], i.e., a KEM variant of the REACT/GEM transformations.

$\text{U}_m^\times (\text{U}_m^\perp)$: FROM DETERMINISTIC OW-CPA (OW-VA) TO IND-CCA SECURITY (“HASHING”). We consider two more variants of U^\times and U^\perp , namely U_m^\times and U_m^\perp . Transformation $\text{U}_m^\times (\text{U}_m^\perp)$ is a variant of $\text{U}^\times (\text{U}^\perp)$, where $K = \text{H}(c, m)$ from Equations (1)-(3) is replaced by $K = \text{H}(m)$. We prove that IND-CCA security of $\text{KEM}_m^\times := \text{U}_m^\times[\text{PKE}_1, \text{H}]$ ($\text{KEM}_m^\perp := \text{U}_m^\perp[\text{PKE}_1, \text{H}]$) in the random oracle model tightly reduces to IND-CPA (IND-VA³) security of PKE_1 , if encryption of PKE_1 is deterministic.

QU_m^\perp : FROM OW-PCA TO IND-CCA SECURITY IN THE QUANTUM ROM. We first prove that transformation T also works in the quantum random oracle model. Next, to go from OW-PCA to IND-CCA in the QROM, we build a key encapsulation mechanism $\text{QKEM}_m^\perp = \text{QU}_m^\perp[\text{PKE}_1, \text{H}, \text{H}']$ with explicit rejection by defining

$$\text{QEncaps}_m(pk) := ((c \leftarrow \text{Enc}_1(pk, m), d := \text{H}'(m)), K := \text{H}(m)),$$

where m is picked at random from the message space.

$$\text{QDecaps}_m^\perp(sk, c, d) = \begin{cases} \text{H}(m') & m' \neq \perp \\ \perp & m' = \perp \vee \text{H}'(m') \neq d \end{cases},$$

where $m' := \text{Dec}(sk, c)$. QU_m^\perp differs from U^\perp only in the additional hash value $d = \text{H}'(m)$ from the ciphertext and H' is a random oracle with matching domain and image. This trick was introduced in [Unr15] and used in [TU16] in the context of the FO transformation. Modeling H and H' as a quantum random oracles, IND-CCA security of KEM reduces to OW-PCA security of PKE_1 .

1.1.2 The resulting FO transformations

Our final transformations FO^\times (“FO with implicit rejection”), FO^\perp (“FO with explicit rejection”), FO_m^\times (“FO with implicit rejection, $K = \text{H}(m)$ ”), FO_m^\perp (“FO with explicit rejection, $K = \text{H}(m)$ ”), and QFO_m^\perp (“Quantum FO with explicit rejection, $K = \text{H}(m)$ ”) are defined in the following table.

²OW-PCVA security is called OW-CPA⁺ security with access to a PCO oracle in [Den03].

³OW-VA security is OW-CPA security, where the adversary is given access to a validity oracle $\text{Cvo}(c)$ that checks c 's validity (cf. Definition 2.1).

Transformation	QROM?	ROM Tightness?	Requirements
$\text{FO}^\times[\text{PKE}, \text{G}, \text{H}] := \text{U}^\times[\text{T}[\text{PKE}, \text{G}], \text{H}]$	—	✓	none
$\text{FO}^\perp[\text{PKE}, \text{G}, \text{H}] := \text{U}^\perp[\text{T}[\text{PKE}, \text{G}], \text{H}]$	—	✓	γ -spread
$\text{FO}_m^\times[\text{PKE}, \text{G}, \text{H}] := \text{U}_m^\times[\text{T}[\text{PKE}, \text{G}], \text{H}]$	—	✓	none
$\text{FO}_m^\perp[\text{PKE}, \text{G}, \text{H}] := \text{U}_m^\perp[\text{T}[\text{PKE}, \text{G}], \text{H}]$	—	✓	γ -spread
$\text{QFO}_m^\perp[\text{PKE}, \text{G}, \text{H}, \text{H}'] := \text{QU}_m^\perp[\text{T}[\text{PKE}, \text{G}], \text{H}, \text{H}']$	✓	✓	none

As corollaries of our modular transformation we obtain that IND-CCA security of $\text{FO}^\times[\text{PKE}, \text{G}, \text{H}]$, $\text{FO}^\perp[\text{PKE}, \text{G}, \text{H}]$, $\text{FO}_m^\times[\text{PKE}, \text{G}, \text{H}]$, and $\text{FO}_m^\perp[\text{PKE}, \text{G}, \text{H}]$ non-tightly reduces to the OW-CPA security of PKE, and tightly reduces to the IND-CPA security of PKE, in the random oracle model. We remark that transformation FO_m^\perp essentially recovers a KEM variant [Den03, Table 5] of the original FO transformation [FO99]. Whereas the explicit rejection variants FO^\perp and FO_m^\perp require PKE to be γ -spread, there is no such requirement on FO^\times and FO_m^\times . Further, IND-CCA security of $\text{QFO}_m^\perp[\text{PKE}, \text{G}, \text{H}, \text{H}']$ reduces to the OW-CPA security of PKE, in the quantum random oracle model. Our transformation QFO_m^\perp essentially recovers a KEM variant of the modified FO transformation by Targhi and Unruh [TU16]. As it is common in the quantum random oracle model, all our reductions are (highly) non-tight. We leave it as an open problem to derive a tighter security reduction of T, for example to IND-CPA security of PKE.

CORRECTNESS ERROR. We stress that all our security reductions also take non-zero correctness error into account. Finding the “right” definition of correctness that is achievable (say, by currently proposed lattice-based encryption schemes) and at the same time sufficient to prove security turned out to be a bit subtle. This is the reason why our definition of correctness (see Section 2.1) derives from the ones previously given in the literature (e.g. [DNR04, ?]). The concrete bounds of FO^\times , FO^\perp , FO_m^\times , and FO_m^\perp give guidance on the required correctness error of the underlying PKE scheme. Concretely, for “ κ bits security”, PKE requires a correctness error of $2^{-\kappa}$.

1.1.3 Example Instantiations

In the context of ElGamal encryption one can apply $\{\text{FO}^\times, \text{FO}^\perp, \text{FO}_m^\times, \text{FO}_m^\perp\}$ to obtain the schemes of [KML03, BLK00, GMMV05] whose IND-CCA security non-tightly reduces to the CDH assumption, and tightly reduces to the DDH assumption. Alternatively, one can directly use $\text{U}^\times/\text{U}^\perp$ to obtain the more efficient schemes of [OP01, CHJ⁺02, ABR01, Sho04a] whose IND-CCA security tightly reduces to the gap-DH (a.k.a. strong CDH) assumption. In the context of deterministic encryption schemes such as RSA, Paillier, etc, one can apply $\text{U}^\times/\text{U}^\perp$ to obtain schemes mentioned in [Sho04a, Den03] whose IND-CCA security tightly reduces to one-way security. Finally, in the context of lattices-based encryption (e.g., [Reg05, LPR13]), one can apply FO^\times , FO^\perp , FO_m^\times , FO_m^\perp , and QFO_m^\perp to achieve IND-CCA security.

1.1.4 Transformation S^ℓ : from OW-CPA to IND-CPA, Tightly

Note that T requires PKE to be IND-CPA secure to achieve a tight reduction. In case one has to rely on OW-CPA security, transformation S^ℓ offers the following tradeoff between efficiency and tightness. It transforms an OW-CPA secure PKE into an IND-CPA secure PKE_ℓ , where ℓ is a parameter. The ciphertext consists of ℓ independent PKE ciphertexts:

$$\text{Enc}_\ell(pk, m) := (\text{Enc}(pk, x_1), \dots, \text{Enc}(pk, x_\ell), m \oplus \text{G}(x_1, \dots, x_\ell)).$$

The reduction (to the OW-CPA security of PKE) loses a factor of $q_G^{1/\ell}$, where q_G is the number of G-queries an adversary makes.

Observe that the only way to gather information about m is to explicitly query $\text{G}(x_1, \dots, x_n)$, which requires to find all x_i . The reduction can use this observation to embed an OW-CPA challenge as one $\text{Enc}(pk, x_{i^*})$ and hope to learn x_{i^*} from the G-queries of a successful IND-CPA adversary. In this, the reduction will know all x_i except x_{i^*} . The difficulty in this reduction is to identify the “right” G-query (that reveals x_{i^*}) in all of the adversary’s G-queries. Intuitively, the more instances we have, the easier it is for the reduction to spot the G-query (x_1, \dots, x_ℓ) (by comparing the x_i for $i \neq i^*$), and the less guessing is necessary. Hence, we get a tradeoff between the number of instances ℓ (and thus the size of the ciphertext) and the loss of the reduction.

1.2 Related work

As already pointed out, $\text{FO}_m^\perp = \text{U}_m^\perp \circ \text{T}$ is essentially a KEM variant of the Fujisaki-Okamoto transform from [Den03, Table 5]. Further, U^\perp is a KEM variant [Den03] of the GEM/REACT transform [OP01, CHJ⁺02, ABR01]. Our modular view suggest that the FO transform implicitly contains the GEM/REACT transform, at least the proof technique. With this more general view, the FO transform and its variants remains the only known transformation from CPA to CCA security. It is an interesting open problem to come up with alternative transformations that get rid of derandomization or that dispense with re-encryption (which preserving efficiency). Note that for the ElGamal encryption scheme, the “twinning” technique [CKS08, CKS09] does exactly this, but it uses non-generic zero-knowledge proofs that are currently not available for all schemes (e.g., for lattice-based schemes).

In concurrent and independent work, [AOP⁺17] considers the IND-CCA security of LIMA which in our notation can be described as $\text{FO}_m^\perp[\text{RLWE}, \text{G}, \text{H}]$. Here RLWE is a specific encryption scheme based on lattices associated to polynomial rings from [LPR10], which is IND-CPA secure under the Ring-LWE assumption. As the main result, [AOP⁺17] provides a tight reduction of LIMA’s IND-CCA security to the Ring-LWE assumption, in the random oracle model. The proof exploits “some weakly homomorphic properties enjoyed by the underlying encryption scheme” and therefore does not seem to be applicable to other schemes. The tight security reduction from Ring-LWE is recovered as a special case of our general security results on FO_m^\perp . We note that the security reduction of [AOP⁺17] does not take the (non-zero) correctness error of RLWE into account.

2 Preliminaries

For $n \in \mathbb{N}$, let $[n] := \{1, \dots, n\}$. For a set S , $|S|$ denotes the cardinality of S . For a finite set S , we denote the sampling of a uniform random element x by $x \xleftarrow{\$} S$, while we denote the sampling according to some distribution \mathcal{D} by $x \leftarrow \mathcal{D}$. For a polynomial $p(X)$ with integer coefficients, we denote by $\text{Roots}(p)$ the (finite) set of (complex) roots of p . By $\llbracket B \rrbracket$ we denote the bit that is 1 if the Boolean Statement B is true, and otherwise 0.

ALGORITHMS. We denote deterministic computation of an algorithm A on input x by $y := A(x)$. We denote algorithms with access to an oracle O by A^{O} . Unless stated otherwise, we assume all our algorithms to be probabilistic and denote the computation by $y \leftarrow A(x)$.

RANDOM ORACLES. We will at times model hash functions $\text{H} : \mathcal{D}_{\text{H}} \rightarrow \mathfrak{S}(\text{H})$ as random oracles. To keep record of the queries issued to H , we will use a hash list \mathfrak{L}_{H} that contains all tuples $(x, \text{H}(x))$ of arguments $x \in \mathcal{D}_{\text{H}}$ that H was queried on and the respective answers $\text{H}(x)$. We make the convention that $\text{H}(x) = \perp$ for all $x \notin \mathcal{D}_{\text{H}}$.

GAMES. Following [Sho04b, BR06], we use code-based games. We implicitly assume boolean flags to be initialized to false, numerical types to 0, sets to \emptyset , and strings to the empty string ϵ . We make the convention that a procedure terminates once it has returned an output.

2.1 Public-Key Encryption

SYNTAX. A public-key encryption scheme $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$ consists of three algorithms and a finite message space \mathcal{M} (which we assume to be efficiently recognizable). The key generation algorithm Gen outputs a key pair (pk, sk) , where pk also defines a randomness space $\mathcal{R} = \mathcal{R}(pk)$. The encryption algorithm Enc , on input pk and a message $m \in \mathcal{M}$, outputs an encryption $c \leftarrow \text{Enc}(pk, m)$ of m under the public key pk . If necessary, we make the used randomness of encryption explicit by writing $c := \text{Enc}(pk, m; r)$, where $r \xleftarrow{\$} \mathcal{R}$ and \mathcal{R} is the randomness space. The decryption algorithm Dec , on input sk and a ciphertext c , outputs either a message $m = \text{Dec}(sk, c) \in \mathcal{M}$ or a special symbol $\perp \notin \mathcal{M}$ to indicate that c is not a valid ciphertext.

INJECTIVITY. We call a public-key encryption scheme PKE *injective* if for all key pairs $(pk, sk) \leftarrow \text{Gen}$, it holds that $\text{Enc}(pk, m; r) = \text{Enc}(pk, m'; r') \Rightarrow (m, r) = (m', r')$ for all $m, m' \in \mathcal{M}$ and $r, r' \in \mathcal{R}$.

CORRECTNESS. We call a public-key encryption scheme PKE δ -correct if

$$\mathbf{E}[\max_{m \in \mathcal{M}} \Pr[\text{Dec}(sk, c) \neq m \mid c \leftarrow \text{Enc}(pk, m)]] \leq \delta,$$

where the expectation is taken over $(pk, sk) \leftarrow \text{Gen}$. In particular, δ -correctness means that for all (possibly unbounded) adversaries A , $\Pr[\text{COR}_{\text{PKE}}^A \Rightarrow 1] \leq \delta$, where the correctness game COR is defined as in Figure 2 (left). That is, an (unbounded) adversary obtains the public and the secret key and wins if it finds a message inducing a correctness error. Note that our definition of correctness slightly derives from previous definitions (e.g. [DNR04, ?]) but it has been carefully crafted such that it is sufficient to prove our main theorems (i.e., the security of the Fujisaki-Okamoto transformation) and at the same time it is fulfilled by all recently proposed lattice-based encryption schemes with correctness error.

If $\text{PKE} = \text{PKE}^G$ is defined relative to a random oracle G , then defining correctness is a bit more subtle as the correctness bound might depend on the number of queries to G .⁴ We call a public-key encryption scheme PKE in the random oracle model $\delta(q_G)$ -correct if for all (possibly unbounded) adversaries A making at most q_G queries to random oracle G , $\Pr[\text{COR-RO}_{\text{PKE}}^A \Rightarrow 1] \leq \delta(q_G)$, where the correctness game COR-RO is defined as in Figure 2 (right). If PKE is defined relative to two random oracles G, H , then the correctness error δ is a function in q_G and q_H .

Note that our correctness definition in the standard model is a special case of the one in the random oracle model, where the number of random oracle queries is zero and hence $\delta(q_G)$ is a constant.

GAME COR:	GAME COR-RO:
01 $(pk, sk) \leftarrow \text{Gen}$	05 $(pk, sk) \leftarrow \text{Gen}$
02 $m \leftarrow A(sk, pk)$	06 $m \leftarrow A^G(sk, pk)$
03 $c \leftarrow \text{Enc}(pk, m)$	07 $c \leftarrow \text{Enc}(pk, m)$
04 return $[\text{Dec}(sk, c) = m]$	08 return $[\text{Dec}(sk, c) = m]$

Figure 2: Correctness game COR for PKE in the standard model (left) and COR-RO for PKE defined relative to a random oracle G (right).

RIGIDITY. Following [BP18], we call a deterministic public-key encryption scheme PKE *rigid* if for all key pairs $(pk, sk) \leftarrow \text{Gen}$, and all ciphertexts c , it holds that either $\text{Dec}(sk, c) = \perp$ or $\text{Enc}(pk, \text{Dec}(sk, c)) = c$.

MIN-ENTROPY. [FO13] For $(pk, sk) \leftarrow \text{Gen}$ and $m \in \mathcal{M}$, we define the *min-entropy* of $\text{Enc}(pk, m)$ by $\gamma(pk, m) := -\log \max_{c \in \mathcal{C}} \Pr_{r \leftarrow \mathcal{R}} [c = \text{Enc}(pk, m; r)]$. We say that PKE is γ -spread if, for every key pair $(pk, sk) \leftarrow \text{Gen}$ and every message $m \in \mathcal{M}$, $\gamma(pk, m) \geq \gamma$. In particular, this implies that for every possible ciphertext $c \in \mathcal{C}$, $\Pr_{r \leftarrow \mathcal{R}} [c = \text{Enc}(pk, m; r)] \leq 2^{-\gamma}$.

SECURITY. We now define three security notions for public-key encryption: One-Wayness under Chosen Plaintext Attacks (OW-CPA), One-Wayness under Plaintext Checking Attacks (OW-PCA) and One-Wayness under Plaintext and Validity Checking Attacks (OW-PCVA).

Definition 2.1 (OW-ATK). Let $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$ be a public-key encryption scheme with message space \mathcal{M} . For $\text{ATK} \in \{\text{CPA}, \text{PCA}, \text{VA}, \text{PCVA}\}$, we define OW-ATK games as in Figure 3, where

$$\text{O}_{\text{ATK}} := \begin{cases} - & \text{ATK} = \text{CPA} \\ \text{PCo}(\cdot, \cdot) & \text{ATK} = \text{PCA} \\ \text{Cvo}(\cdot) & \text{ATK} = \text{VA} \\ \text{PCo}(\cdot, \cdot), \text{Cvo}(\cdot) & \text{ATK} = \text{PCVA} \end{cases}.$$

We define the OW-ATK *advantage function of an adversary A against PKE* as $\text{Adv}_{\text{PKE}}^{\text{OW-ATK}}(A) := \Pr[\text{OW-ATK}_{\text{PKE}}^A \Rightarrow 1]$.

A few remarks are in place. Our definition of the plaintext checking oracle $\text{PCO}(m, c)$ (c.f. Figure 3) implicitly disallows queries on messages $m \in \mathcal{M}$. (With the convention that $\text{PCO}(m \notin \mathcal{M}, c)$ yields \perp .) This restriction is important since otherwise the ciphertext validity oracle $\text{CVO}(\cdot)$ could be simulated as $\text{Cvo}(m) = \text{PCO}(\perp, c)$. Similarly, the ciphertext validity oracle $\text{CVO}(c)$ implicitly disallows queries on the challenge ciphertext c^* .

Usually, the adversary wins the one-way game iff its output m' equals the challenge message m^* . Instead, in game OW-ATK the correctness of m' is checked using the PCO oracle, i.e., it returns 1 iff $\text{Dec}(sk, c^*) = m'$. The two games have statistical difference δ , if PKE is δ -correct.

⁴For an example why the number of random oracle queries matters in the context of correctness, we refer to Theorem 3.1.

GAME OW-ATK:	$\text{PCO}(m \in \mathcal{M}, c)$
09 $(pk, sk) \leftarrow \text{Gen}$	14 return $\llbracket \text{Dec}(sk, c) = m \rrbracket$
10 $m^* \xleftarrow{\$} \mathcal{M}$	
11 $c^* \leftarrow \text{Enc}(pk, m^*)$	$\text{CVO}(c \neq c^*)$
12 $m' \leftarrow \text{A}^{\text{O}_{\text{ATK}}}(pk, c)$	15 $m := \text{Dec}(sk, c)$
13 return $\text{PCO}(m', c^*)$	16 return $\llbracket m \in \mathcal{M} \rrbracket$

Figure 3: Games OW-ATK ($\text{ATK} \in \{\text{CPA}, \text{PCA}, \text{VA}, \text{PCVA}\}$) for PKE, where O_{ATK} is defined in Definition 2.1. $\text{PCO}(\cdot, \cdot)$ is the Plaintext Checking Oracle and $\text{CVO}(\cdot)$ is the Ciphertext Validity Oracle.

Additionally, we define Indistinguishability under Chosen Plaintext Attacks (IND-CPA).

Definition 2.2 (IND-CPA). Let $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$ be a public-key encryption scheme with message space \mathcal{M} . We define the IND-CPA game as in Figure 4, and the IND-CPA advantage function of an adversary $\text{A} = (\text{A}_1, \text{A}_2)$ against PKE (such that A_2 has binary output) as $\text{Adv}_{\text{PKE}}^{\text{IND-CPA}}(\text{A}) := |\Pr[\text{IND-CPA}^{\text{A}} \Rightarrow 1] - 1/2|$.

We also define OW-ATK and IND-CPA security in the random oracle model model, where PKE and adversary A are given access to a random oracle H . We make the convention that the number q_{H} of the adversary's random oracle queries count the total number of times H is executed in the experiment. That is, the number of A explicit queries to $\text{H}(\cdot)$ plus the number of implicit queries to $\text{H}(\cdot)$ made by the experiment.

It is well known that IND-CPA security of PKE with sufficiently large message space implies its OW-CPA security.

Lemma 2.3 *For any adversary B there exists an adversary A with the same running time as that of B such that $\text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\text{B}) \leq \text{Adv}_{\text{PKE}}^{\text{IND-CPA}}(\text{A}) + 1/|\mathcal{M}|$.*

2.2 Key Encapsulation

SYNTAX. A key encapsulation mechanism $\text{KEM} = (\text{Gen}, \text{Encaps}, \text{Decaps})$ consists of three algorithms. The key generation algorithm Gen outputs a key pair (pk, sk) , where pk also defines a finite key space \mathcal{K} . The encapsulation algorithm Encaps , on input pk , outputs a tuple (K, c) where c is said to be an encapsulation of the key K which is contained in key space \mathcal{K} . The deterministic decapsulation algorithm Decaps , on input sk and an encapsulation c , outputs either a key $K := \text{Decaps}(sk, c) \in \mathcal{K}$ or a special symbol $\perp \notin \mathcal{K}$ to indicate that c is not a valid encapsulation. We call KEM δ -correct if

$$\Pr[\text{Decaps}(sk, c) \neq K \mid (pk, sk) \leftarrow \text{Gen}; (K, c) \leftarrow \text{Encaps}(pk)] \leq \delta .$$

Note that the above definition also makes sense in the random oracle model since KEM ciphertexts do not depend on messages.

SECURITY. We now define a security notion for key encapsulation: Indistinguishability under Chosen Ciphertext Attacks (IND-CCA).

Definition 2.4 (IND-CCA). We define the IND-CCA game as in Figure 4 and the IND-CCA advantage function of an adversary A (with binary output) against KEM as $\text{Adv}_{\text{KEM}}^{\text{IND-CCA}}(\text{A}) := |\Pr[\text{IND-CCA}^{\text{A}} \Rightarrow 1] - 1/2|$.

GAME IND-CPA	GAME IND-CCA	DECAPS ($c \neq c^*$)
01 $(pk, sk) \leftarrow \text{Gen}$	07 $(pk, sk) \leftarrow \text{Gen}$	13 $K := \text{Decaps}(sk, c)$
02 $b \xleftarrow{\$} \{0, 1\}$	08 $b \xleftarrow{\$} \{0, 1\}$	14 return K
03 $(m_0^*, m_1^*, st) \leftarrow A_1(pk)$	09 $(K_0^*, c^*) \leftarrow \text{Encaps}(pk)$	
04 $c^* \leftarrow \text{Enc}(pk, m_b^*)$	10 $K_1^* \xleftarrow{\$} \mathcal{K}$	
05 $b' \leftarrow A_2(pk, c^*, st)$	11 $b' \leftarrow A^{\text{DECAPS}}(c^*, K_b^*)$	
06 return $\llbracket b' = b \rrbracket$	12 return $\llbracket b' = b \rrbracket$	

Figure 4: Games IND-CPA for PKE and IND-CCA game for KEM.

3 Modular FO Transformations

In Section 3.1, we will introduce T that transforms any OW-CPA secure encryption scheme PKE into a OW-PCA secure encryption scheme PKE_1 . If PKE is furthermore IND-CPA, then the reduction is tight. Furthermore, if PKE is γ -spread, then PKE_1 even satisfied the stronger security notion of OW-PCVA security. Next, in Section 3.2 (Section 3.2.1), we will introduce transformations U^\perp , U_m^\perp (U^\perp , U_m^\perp) that transform any OW-PCA (OW-PCVA) secure encryption scheme PKE_1 into an IND-CCA secure KEM. The security reduction is tight. Transformations U_m^\perp and U_m^\perp can only be applied for deterministic encryption schemes. Combining T with $\{U^\perp, U_m^\perp, U^\perp, U_m^\perp\}$, in Section 3.3 we provide concrete bounds for the IND-CCA security of the resulting KEMs. Finally, in Section 3.4 we introduce S^ℓ that transforms any OW-CPA secure scheme into an IND-CPA secure one, offering a tradeoff between tightness and ciphertext size.

3.1 Transformation T : from OW-CPA/IND-CPA to OW-PCVA

T transforms an OW-CPA secure public-key encryption scheme into an OW-PCA secure one.

THE CONSTRUCTION. To a public-key encryption scheme $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space \mathcal{M} and randomness space \mathcal{R} , and random oracle $G : \mathcal{M} \rightarrow \mathcal{R}$, we associate $\text{PKE}_1 = T[\text{PKE}, G]$. The algorithms of $\text{PKE}_1 = (\text{Gen}, \text{Enc}_1, \text{Dec}_1)$ are defined in Figure 5. Note that Enc_1 deterministically computes the ciphertext as $c := \text{Enc}(pk, m; G(m))$.

Enc ₁ (pk, m)	Dec ₁ (sk, c)
01 $c := \text{Enc}(pk, m; G(m))$	03 $m' := \text{Dec}(sk, c)$.
02 return c	04 if $m' = \perp$ or $\text{Enc}(pk, m'; G(m')) \neq c$
	05 return \perp
	06 else return m'

Figure 5: OW-PCVA-secure encryption scheme $\text{PKE}_1 = T[\text{PKE}, G]$ with deterministic encryption.

NON-TIGHT SECURITY FROM OW-CPA. The following theorem establishes that OW-PCVA security of PKE_1 (cf. Definition 2.1) non-tightly reduces to the OW-CPA security of PKE, in the random oracle model, given that PKE is γ -spread (for sufficiently large γ). If PKE is not γ -spread, then PKE_1 is still OW-PCA secure.

Theorem 3.1 ($\text{PKE OW-CPA} \xrightarrow{\text{ROM}} \text{PKE}_1 \text{ OW-PCVA}$). *If PKE is δ -correct, then PKE_1 is δ_1 -correct in the random oracle model with $\delta_1(q_G) = q_G \cdot \delta$. Assume PKE to be γ -spread. Then, for any OW-PCVA adversary B that issues at most q_G queries to the random oracle G , q_P queries to a plaintext checking oracle PCO , and q_V queries to a validity checking oracle CVO , there exists an OW-CPA adversary A such that*

$$\text{Adv}_{\text{PKE}_1}^{\text{OW-PCVA}}(B) \leq (q_G + q_P) \cdot \delta + q_V \cdot 2^{-\gamma} + (q_G + q_P + 1) \cdot \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(A)$$

and the running time of A is about that of B . Furthermore, PKE_1 is rigid.

The main idea of the proof is that since Enc_1 is deterministic, the $\text{PCA}(\cdot, \cdot)$ oracle can be equivalently implemented by “re-encryption” and the $\text{CVO}(\cdot)$ oracle by controlling the random oracles. Additional care has to be taken to account for the correctness error.

Proof. To prove correctness, consider an adversary A playing the correctness game COR-RO (Figure 2) of PKE_1 in the random oracle model. Game COR-RO makes at most q_G (distinct) queries $G(m_1), \dots, G(m_{q_G})$ to G . We call such a query $G(m_i)$ *problematic* iff it exhibits a correctness error in PKE_1 (in the sense that $\text{Dec}(sk, \text{Enc}(pk, m_i; G(m_i))) \neq m_i$). Since G outputs independently random values, each $G(m_i)$ is problematic with probability at most δ (averaged over (pk, sk)), since we assumed that PKE is δ -correct. Hence, a union bound shows that the probability that at least one $G(m_i)$ is problematic is at most $q_G \cdot \delta$. This proves $\Pr[\text{COR-RO}^A \Rightarrow 1] \leq q_G \cdot \delta$ and hence PKE_1 is δ_1 -correct with $\delta_1(q_G) = q_G \cdot \delta$.

To prove security, let B be an adversary against the OW-PCVA security of PKE_1 , issuing at most q_G queries to G , at most q_P queries to PCO , and at most q_V queries to CVO . Consider the sequence of games given in Figure 6.

<p>GAMES G_0-G_3</p> <p>01 $(pk, sk) \leftarrow \text{Gen}$</p> <p>02 $m^* \xleftarrow{\\$} \mathcal{M}$</p> <p>03 $c^* \leftarrow \text{Enc}(pk, m^*)$</p> <p>04 $m' \leftarrow \text{B}^{\text{G}(\cdot), \text{PCO}(\cdot, \cdot), \text{CVO}(\cdot)}(pk, c^*)$</p> <p>05 return $\llbracket m' = m^* \rrbracket$</p> <p>$\text{G}(m)$</p> <p>06 if $\exists r$ s. th. $(m, r) \in \mathcal{L}_G$</p> <p>07 return r</p> <p>08 if $m = m^*$ $\llbracket G_3$</p> <p>09 QUERY := true $\llbracket G_3$</p> <p>10 abort $\llbracket G_3$</p> <p>11 $r \xleftarrow{\\$} \mathcal{R}$</p> <p>12 $\mathcal{L}_G := \mathcal{L}_G \cup \{(m, r)\}$</p> <p>13 return r</p>	<p>$\text{PCO}(m \in \mathcal{M}, c)$</p> <p>14 $m' := \text{Dec}(sk, c)$ $\llbracket G_0$-G_1</p> <p>15 return $\llbracket m' = m \rrbracket$ and $\llbracket \text{Enc}(pk, m'; G(m')) = c \rrbracket$ $\llbracket G_0$-G_1</p> <p>16 return $\llbracket \text{Enc}(pk, m, G(m)) = c \rrbracket$ $\llbracket G_2$-G_3</p> <p>$\text{CVO}(c \neq c^*)$</p> <p>17 $m' := \text{Dec}(sk, c)$ $\llbracket G_0$-G_1</p> <p>18 return $\llbracket m' \in \mathcal{M} \rrbracket$ and $\llbracket \text{Enc}(pk, m'; G(m')) = c \rrbracket$ $\llbracket G_0$</p> <p>19 return $\llbracket \exists (m, r) \in \mathcal{L}_G \text{ and } \text{Enc}(pk, m; r) = c \text{ and } m' = m \rrbracket$ $\llbracket G_1$</p> <p>20 return $\llbracket \exists (m, r) \in \mathcal{L}_G \text{ and } \text{Enc}(pk, m; r) = c \rrbracket$ $\llbracket G_2$-G_3</p>
---	---

Figure 6: Games G_0 - G_3 for the proof of Theorem 3.1.

GAME G_0 . This is the original OW-PCVA game. Random oracle queries are stored in set \mathcal{L}_G with the convention that $G(m) = r$ iff $(m, r) \in \mathcal{L}_G$. Hence,

$$\Pr[G_0^B \Rightarrow 1] = \text{Adv}_{\text{PKE}_1}^{\text{OW-PCVA}}(B) .$$

GAME G_1 . In game G_1 the ciphertext validity oracle $\text{CVO}(c \neq c^*)$ is replaced with one that first computes $m' = \text{Dec}(sk, c)$ and returns 1 iff there exists a previous query (m, r) to G such that $\text{Enc}(pk, m; r) = c$ and $m = m'$.

Consider a single query $\text{CVO}(c)$ and define $m' := \text{Dec}(sk, c)$. If $\text{CVO}(c) = 1$ in G_1 , then $G(m') = G(m) = r$ and hence $\text{Enc}(pk, m'; G(m')) = c$, meaning $\text{CVO}(c) = 1$ in G_0 . If $\text{CVO}(c) = 1$ in G_0 , then we can only have $\text{CVO}(c) = 0$ in G_1 only if $G(m')$ was not queried before. This happens with probability $2^{-\gamma}$, where γ is the parameter from the γ -spreadness of PKE . By the union bound we obtain

$$|\Pr[G_1^B \Rightarrow 1] - \Pr[G_0^B \Rightarrow 1]| \leq q_V \cdot 2^{-\gamma} .$$

GAME G_2 . In game G_2 we replace the plaintext checking oracle $\text{PCO}(m, c)$ and the ciphertext validity oracle $\text{CVO}(c)$ by a simulation that does not check whether $m = m'$ anymore, where $m' = \text{Dec}(sk, c)$

We claim

$$|\Pr[G_2^B \Rightarrow 1] - \Pr[G_1^B \Rightarrow 1]| \leq (q_G + q_P) \cdot \delta . \quad (4)$$

To show Equation (4), observe that the whole Game G_1 (and also the whole Game G_2) makes at most q_G (distinct) queries $G(m_1), \dots, G(m_{q_G})$ to G . Again, we call such a query $G(m_i)$ *problematic* iff it exhibits a correctness error in PKE_1 (in the sense that $\text{Dec}(sk, \text{Enc}(pk, m_i; G(m_i))) \neq m_i$). Clearly, if B makes a problematic query, then there exists an adversary F that wins the correctness game COR-RO in the random oracle model. Hence, the probability that at least one $G(m_i)$ is problematic is at most $\delta_1(q_G) \leq q_G \cdot \delta$.

However, conditioned on the event that no query $G(m_i)$ is problematic, Game G_1 and Game G_2 proceed identically (cf. Figure 6). Indeed, the two games only differ if B submits a PCO query (m, c) or a

$C(pk, c^*)$	$D(pk, c^*)$
01 $m' \leftarrow \mathbf{B}^{\mathbf{G}(\cdot), \mathbf{PCO}(\cdot, \cdot)}(pk, c^*)$	03 $m \leftarrow \mathbf{B}^{\mathbf{G}(\cdot), \mathbf{PCO}(\cdot, \cdot)}(pk, c^*)$
02 return m'	04 $(m', r') \xleftarrow{\$} \mathfrak{L}_G$
	05 return m'

Figure 7: Adversaries C and D against OW-CPA for the proof of Theorem 3.1. Oracles PCO, CVO are defined as in game G_3 , and G is defined as in game G_2 of Figure 6.

CVO query c together with a G query m such that $\mathbf{G}(m)$ is problematic and $c = \mathbf{Enc}(pk, m; \mathbf{G}(m))$. (In this case, G_1 will answer the query with 0, while G_2 will answer with 1.) This shows Equation (4).

GAME G_3 . In Game G_3 , we add a flag QUERY in line 09 and abort when it is raised. Hence, G_2 and G_3 only differ if QUERY is raised, meaning that B made a query G on m^* , or, equivalently, $(m^*, \cdot) \in \mathfrak{L}_G$. Due to the difference lemma [Sho04b],

$$|\Pr[G_3^B \Rightarrow 1] - \Pr[G_2^B \Rightarrow 1]| \leq \Pr[\text{QUERY}].$$

We first bound $\Pr[G_3^B \Rightarrow 1]$ by constructing an adversary C in Figure 7 against the OW-CPA security of the original encryption scheme PKE. C inputs $(pk, c^* \leftarrow \mathbf{Enc}(pk, m^*))$ for random, unknown m^* , perfectly simulates game G_3 for B, and finally outputs $m' = m^*$ if B wins in game G_3 .

$$\Pr[G_3^B \Rightarrow 1] = \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\text{C}) .$$

So far we have established the bound

$$\text{Adv}_{\text{PKE}_1}^{\text{OW-PCVA}}(\text{B}) \leq (q_G + q_P) \cdot \delta + q_V \cdot 2^{-\gamma} + \Pr[\text{QUERY}] + \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\text{C}) . \quad (5)$$

Finally, in Figure 7 we construct an adversary D against the OW-CPA security of the original encryption scheme PKE, that inputs $(pk, c^* \leftarrow \mathbf{Enc}(pk, m^*))$, perfectly simulates game G_3 for B. If flag QUERY is set in G_3 then there exists an entry $(m^*, \cdot) \in \mathfrak{L}_G$ and D returns the correct $m' = m^*$ with probability at most $1/q_G$. We just showed

$$\Pr[\text{QUERY}] \leq (q_G + q_P) \cdot \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\text{D}) .$$

Combining the latter bound with Equation (5) and folding C and D into one single adversary A against OW-CPA yields the required bound of the theorem. \square

By definition, OW-PCA security is OW-PCVA security with $q_V := 0$ queries to the validity checking oracle. Hence, the bound of Theorem 3.1 shows that PKE_1 is in particular OW-PCA secure, without requiring PKE to be γ -spread.

TIGHT SECURITY FROM IND-CPA. Whereas the reduction to OW-CPA security in Theorem 3.1 was non-tight, the following theorem establishes that OW-PCVA security of PKE_1 tightly reduces to IND-CPA security of PKE, in the random oracle model, given that PKE is γ -spread. If PKE is not γ -spread, then PKE_1 is still OW-PCA secure.

Theorem 3.2 (PKE IND-CPA $\xrightarrow{\text{ROM}}$ PKE_1 OW-PCVA). *Assume PKE to be δ -correct and γ -spread. Then, for any OW-PCVA adversary B that issues at most q_G queries to the random oracle G, q_P queries to a plaintext checking oracle PCO, and q_V queries to a validity checking oracle CVO, there exists an IND-CPA adversary A such that*

$$\text{Adv}_{\text{PKE}_1}^{\text{OW-PCVA}}(\text{B}) \leq (q_G + q_P) \cdot \delta + q_V \cdot 2^{-\gamma} + \frac{2q_G + 1}{|\mathcal{M}|} + 3 \cdot \text{Adv}_{\text{PKE}}^{\text{IND-CPA}}(\text{A})$$

and the running time of A is about that of B.

Proof. Considering the games of Figure 6 from the proof of Theorem 3.1 we obtain by Equation (5)

$$\begin{aligned} \text{Adv}_{\text{PKE}_1}^{\text{OW-PCVA}}(\text{B}) &\leq (q_G + q_P) \cdot \delta + q_V \cdot 2^{-\gamma} + \Pr[\text{QUERY}] + \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\text{C}) \\ &\leq (q_G + q_P) \cdot \delta + q_V \cdot 2^{-\gamma} + \Pr[\text{QUERY}] + \frac{1}{|\mathcal{M}|} + \text{Adv}_{\text{PKE}}^{\text{IND-CPA}}(\text{C}) , \end{aligned}$$

$\begin{array}{l} \underline{D_1(pk)} \\ 06 \text{ } st := (m_0^*, m_1^*) \xleftarrow{\$} \mathcal{M}^2 \\ 07 \text{ } \mathbf{return } st \end{array}$	$\begin{array}{l} \underline{D_2(pk, c^*, st)} \\ 08 \text{ } m' \leftarrow \mathbf{B}^{\mathbf{G}(\cdot), \mathbf{PCo}(\cdot), \mathbf{Cvo}(\cdot)}(pk, c^*) \\ 09 \text{ } b' := \begin{cases} 0 & \mathcal{L}_G(m_0^*) > \mathcal{L}_G(m_1^*) \\ 1 & \mathcal{L}_G(m_1^*) < \mathcal{L}_G(m_0^*) \\ \xleftarrow{\$} \{0, 1\} & \text{otherwise} \end{cases} \\ 10 \text{ } \mathbf{return } b' \end{array}$
---	--

Figure 8: Adversary $D = (D_1, D_2)$ against IND-CPA for the proof of Theorem 3.2. For fixed $m \in \mathcal{M}$, $\mathcal{L}_G(m)$ is the set of all $(m, r) \in \mathcal{L}_G$. Oracles PCO, CVO are defined as in game G_3 , and G is defined as in game G_2 of Figure 6.

where the last inequation uses Lemma 2.3.

In Figure 8 we construct an adversary $D = (D_1, D_2)$ against the IND-CPA security of the original encryption scheme PKE that wins if flag QUERY is set in G_3 . The first adversary D_1 picks two random messages m_0^*, m_1^* . The second adversary D_2 inputs $(pk, c^* \leftarrow \text{Enc}(pk, m_b^*), st)$, for an unknown random bit b , and runs B on (pk, c^*) , simulating its view in game G_3 . Note that by construction message m_b^* is uniformly distributed.

Consider game IND-CPA^D with random challenge bit b . Let BADG be the event that B queries random oracle G on m_{1-b}^* . Since m_{1-b}^* is uniformly distributed and independent from B 's view, we have $\Pr[\text{BADG}] \leq q_G/|\mathcal{M}|$. For the remainder of the proof we assume BADG did not happen, i.e. $|\mathcal{L}_G(m_{1-b}^*)| = 0$.

If QUERY happens, then B queried the random oracle G on m_b^* , which implies $|\mathcal{L}_G(m_b^*)| > 0 = |\mathcal{L}_G(m_{1-b}^*)|$ and therefore $b = b'$. If QUERY does not happen, then B did not query random oracle G on m_b^* . Hence, $|\mathcal{L}_G(m_b^*)| = |\mathcal{L}_G(m_{1-b}^*)| = 0$ and $\Pr[b = b'] = 1/2$ since A picks a random bit b' . Overall, we have

$$\begin{aligned} \text{Adv}_{\text{PKE}}^{\text{IND-CPA}}(D) + \frac{q_G}{|\mathcal{M}|} &\geq \left| \Pr[b = b'] - \frac{1}{2} \right| \\ &= \left| \Pr[\text{QUERY}] + \frac{1}{2} \Pr[\neg\text{QUERY}] - \frac{1}{2} \right| \\ &= \frac{1}{2} \Pr[\text{QUERY}]. \end{aligned}$$

Folding C and D into one single IND-CPA adversary A yields the required bound of the theorem. \square

With the same argument as in Theorem 3.1, a tight reduction to OW-PCA security is implied without requiring PKE to be γ -spread.

3.2 Transformations U^\neq , U_m^\neq , U^\perp , U_m^\perp

In this section we introduce four variants of a transformation U , namely U^\neq , U_m^\neq , U^\perp , U_m^\perp , that convert a public-key encryption scheme PKE_1 into a key encapsulation mechanism KEM. Their differences are summarized in the following table.

Transformation	Rejection of invalid ciphertexts	KEM key	PKE ₁ 's requirements
U^\neq	implicit	$K = H(m, c)$	OW-PCA
U^\perp	explicit	$K = H(m, c)$	OW-PCVA
U_m^\neq	implicit	$K = H(m)$	det. + OW-CPA
U_m^\perp	explicit	$K = H(m)$	det. + OW-VA

3.2.1 Transformation U^\perp : from OW-PCVA to IND-CCA

U^\perp transforms an OW-PCVA secure public-key encryption scheme into an IND-CCA secure key encapsulation mechanism. The \perp in U^\perp means that decapsulation of an invalid ciphertext results in the rejection symbol \perp (“explicit rejection”).

THE CONSTRUCTION. To a public-key encryption scheme $\text{PKE}_1 = (\text{Gen}_1, \text{Enc}_1, \text{Dec}_1)$ with message space \mathcal{M} , and a hash function $\text{H} : \{0, 1\}^* \rightarrow \{0, 1\}^n$, we associate $\text{KEM}^\perp = \text{U}^\perp[\text{PKE}_1, \text{H}]$. The algorithms of $\text{KEM}^\perp = (\text{Gen}_1, \text{Encaps}, \text{Decaps}^\perp)$ are defined in Figure 9.

<u>Encaps(pk)</u>	<u>Decaps[⊥](sk, c)</u>
01 $m \xleftarrow{\$} \mathcal{M}$	05 $m' := \text{Dec}_1(sk, c)$
02 $c \leftarrow \text{Enc}_1(pk, m)$	06 if $m' = \perp$ return \perp
03 $K := \text{H}(m, c)$	07 else return
04 return (K, c)	$K := \text{H}(m', c)$

Figure 9: IND-CCA-secure key encapsulation mechanism $\text{KEM}^\perp = \text{U}^\perp[\text{PKE}_1, \text{H}]$.

SECURITY. The following theorem establishes that IND-CCA security of KEM^\perp tightly reduces to the OW-PCVA security of PKE_1 , in the random oracle model.

Theorem 3.3 (PKE_1 OW-PCVA $\stackrel{\text{ROM}}{\Rightarrow}$ KEM^\perp IND-CCA). *If PKE_1 is δ_1 -correct, so is KEM^\perp . For any IND-CCA adversary B against KEM^\perp , issuing at most q_D queries to the decapsulation oracle DECAPS^\perp and at most q_H queries to the random oracle H , there exists an OW-PCVA adversary A against PKE_1 that makes at most q_H queries both to the PCO oracle and to the CVO oracle such that*

$$\text{Adv}_{\text{KEM}^\perp}^{\text{IND-CCA}}(\text{B}) \leq \text{Adv}_{\text{PKE}_1}^{\text{OW-PCVA}}(\text{A})$$

and the running time of A is about that of B .

The main idea of the proof is to simulate the decapsulation oracle without the secret-key. This can be done by answering decryption queries with a random key and then later patch the random oracle using the plaintext checking oracle $\text{PCO}(\cdot, \cdot)$ provided by the OW-PCVA game. Additionally, the ciphertext validity oracle $\text{CVO}(\cdot)$ is required to reject decapsulation queries with inconsistent ciphertexts.

Proof. It is easy to verify the correctness bound. Let B be an adversary against the IND-CCA security of KEM^\perp , issuing at most q_D queries to DECAPS^\perp and at most q_H queries to H . Consider the games given in Figure 10.

GAME G_0 . Since game G_0 is the original IND-CCA game,

$$\left| \Pr[G_0^{\text{B}} \Rightarrow 1] - \frac{1}{2} \right| = \text{Adv}_{\text{KEM}^\perp}^{\text{IND-CCA}}(\text{B}) .$$

GAME G_1 . In game G_1 , the oracles H and DECAPS^\perp are modified such that they make no use of the secret key any longer except by testing if $\text{Dec}_1(sk', c) = m$ for given (m, c) in line 15 and if $\text{Dec}_1(sk, c) \in \mathcal{M}$ for given c in line 27. Game G_1 contains two sets: hash list \mathcal{L}_H that contains all entries (m, c, K) where H was queried on (m, c) , and set \mathcal{L}_D that contains all entries (c, K) where either H was queried on (m', c) , $m' := \text{Dec}_1(sk', c)$, or DECAPS^\perp was queried on c . In order to show that the view of B is identical in games G_0 and G_1 , consider the following cases for a fixed ciphertext c and $m' := \text{Dec}_1(sk', c)$.

- Case 1: $m' \notin \mathcal{M}$. Since $\text{CVO}(c) = 0$ is equivalent to $m' = \perp$, $\text{DECAPS}^\perp(c)$ returns \perp as in both games.
- Case 2: $m' \in \mathcal{M}$. We will now show that H in game G_1 is “patched”, meaning that it ensures $\text{DECAPS}^\perp(c) = \text{H}(m', c)$, where $m' := \text{Dec}_1(sk, c)$, for all ciphertexts c with $m' \in \mathcal{M}$. We distinguish two sub-cases: B might either first query H on (m', c) , then DECAPS^\perp on c , or the other way round.
 - If H is queried on (m', c) first, it is recognized that $\text{Dec}_1(sk, c) = m$ in line 15. Since DECAPS was not yet queried on c , no entry of the form (c, K) can already exist in \mathcal{L}_D . Therefore, besides adding $(m, c, K \xleftarrow{\$} \mathcal{K})$ to \mathcal{L}_H , H also adds (c, K) to \mathcal{L}_D in line 22, thereby defining $\text{DECAPS}^\perp(c) := K = \text{H}(m', c)$.

GAMES $G_0 - G_2$	$H(m, c)$	
01 $(pk, sk) \leftarrow \text{Gen}_1$	12 if $\exists K$ such that $(m, c, K) \in \mathfrak{L}_H$	
02 $m^* \xleftarrow{\$} \mathcal{M}$	13 return K	
03 $c^* \leftarrow \text{Enc}_1(pk, m^*)$	14 $K \xleftarrow{\$} \mathcal{K}$	
04 $K_0^* := H(m^*, c^*)$	15 if $\text{Dec}_1(sk, c) = m$	$\parallel G_1 - G_2$
05 $K_1^* \xleftarrow{\$} \{0, 1\}^n$	16 if $c = c^*$	$\parallel G_2$
06 $b \xleftarrow{\$} \{0, 1\}$	17 $\text{CHAL} := \text{true}$	$\parallel G_2$
07 $b' \leftarrow \text{B}^{\text{DECAPS}^\perp, H}(pk, c^*, K_b^*)$	18 abort	$\parallel G_2$
08 return $\llbracket b' = b \rrbracket$	19 if $\exists K'$ such that $(c, K') \in \mathfrak{L}_D$	$\parallel G_1 - G_2$
	20 $K := K'$	$\parallel G_1 - G_2$
	21 else	$\parallel G_1 - G_2$
	22 $\mathfrak{L}_D := \mathfrak{L}_D \cup \{(c, K)\}$	$\parallel G_1 - G_2$
	23 $\mathfrak{L}_H := \mathfrak{L}_H \cup \{(m, c, K)\}$	
	24 return K	
$\text{DECAPS}^\perp(c \neq c^*)$	$\parallel G_0$	$\text{DECAPS}^\perp(c \neq c^*)$
09 $m' := \text{Dec}_1(sk, c)$	25 if $\exists K$ s. th. $(c, K) \in \mathfrak{L}_D$	$\parallel G_1 - G_2$
10 if $m' = \perp$ return \perp	26 return K	
11 return $K := H(m', c)$	27 if $\text{Dec}_1(sk, c) \notin \mathcal{M}$	
	28 return \perp	
	29 $K \xleftarrow{\$} \mathcal{K}$	
	30 $\mathfrak{L}_D := \mathfrak{L}_D \cup \{(c, K)\}$	
	31 return K	

Figure 10: Games $G_0 - G_2$ for the proof of Theorem 3.3.

- If DECAPS^\perp is queried on c first, no entry of the form (c, K) exists in \mathfrak{L}_D yet. Therefore, DECAPS^\perp adds $(c, K \xleftarrow{\$} \mathcal{K})$ to \mathfrak{L}_D , thereby defining $\text{DECAPS}^\perp(c) := K$. When queried on (m', c) afterwards, H recognizes that $\text{Dec}_1(sk, c) = m'$ in line 15 and that an entry of the form (c, K) already exists in \mathfrak{L}_D in line 19. By adding (m, c, K) to \mathfrak{L}_H and returning K , H defines $H(m', c) := K = \text{DECAPS}^\perp(c)$.

We have shown that B 's view is identical in both games and

$$\Pr[G_1^B \Rightarrow 1] = \Pr[G_0^B \Rightarrow 1] .$$

GAME G_2 . From game G_2 on we proceed identical to the proof of Theorem 3.4. That is, we abort immediately on the event that B queries H on (m^*, c^*) . Denote this event as CHAL . Due to the difference lemma,

$$|\Pr[G_2^B \Rightarrow 1] - \Pr[G_1^B \Rightarrow 1]| \leq \Pr[\text{CHAL}] .$$

In game G_2 , $H(m^*, c^*)$ will not be given to B ; neither through a hash nor a decryption query, meaning bit b is independent from B 's view. Hence,

$$\Pr[G_2^B] = \frac{1}{2} .$$

It remains to bound $\Pr[\text{CHAL}]$. To this end, we construct an adversary A against the OW-PCVA security of PKE_1 simulating G_2 for B as in Figure 11. Note that the simulation is perfect. Since CHAL implies that B queried $H(m^*, c^*)$ which implies $(m^*, c^*, K') \in \mathfrak{L}_H$ for some K' , and A returns $m' = m^*$. Hence,

$$\Pr[\text{CHAL}] = \text{Adv}_{\text{PKE}}^{\text{OW-PCVA}}(A) .$$

Collecting the probabilities yields the required bound. \square

3.2.2 Transformation U^\perp : from OW-PCA to IND-CCA

U^\perp is a variant of U^\perp with “implicit rejection” of inconsistent ciphertexts. It transforms an OW-PCA secure public-key encryption scheme into an IND-CCA secure key encapsulation mechanism.

$A^{\text{PCO}(\cdot, \cdot)}(pk, c^*)$ 01 $K^* \xleftarrow{\$} \mathcal{K}$ 02 $b' \leftarrow \mathbf{B}^{\text{DECAPS}^\perp(\cdot), \mathbf{H}(\cdot, \cdot)}(pk, c^*, K^*)$ 03 if $\exists(m', c', K') \in \mathfrak{L}_H$ s. th. $\text{PCO}(m', c^*) = 1$ 04 return m' 05 else 06 abort	$\mathbf{H}(m, c)$ 07 if $\exists K$ such that $(m, c, K) \in \mathfrak{L}_H$ return K 08 09 $K \xleftarrow{\$} \mathcal{K}$ 10 if $\text{PCO}(m, c) = 1$ 11 if $\exists K'$ such that $(c, K') \in \mathfrak{L}_D$ 12 $K := K'$ 13 else 14 $\mathfrak{L}_D := \mathfrak{L}_D \cup \{(c, K)\}$ 15 $\mathfrak{L}_H := \mathfrak{L}_H \cup \{(m, c, K)\}$ 16 return K
--	--

Figure 11: Adversary A against OW-PCVA for the proof of Theorem 3.3, where DECAPS^\perp is defined as in Game G_2 of Figure 10.

THE CONSTRUCTION. To a public-key encryption scheme $\text{PKE}_1 = (\text{Gen}_1, \text{Enc}_1, \text{Dec}_1)$ with message space \mathcal{M} , and a random oracle $\mathbf{H} : \{0, 1\}^* \rightarrow \mathcal{M}$ we associate $\text{KEM}^\perp = \mathbf{U}^\perp[\text{PKE}_1, \mathbf{H}] = (\text{Gen}^\perp, \text{Encaps}, \text{Decaps}^\perp)$. The algorithms of KEM^\perp are defined in Figure 12, Encaps is the same as in KEM^\perp (Figure 9). Note that \mathbf{U}^\perp and \mathbf{U}^\perp essentially differ in decapsulation: Decaps^\perp from \mathbf{U}^\perp rejects if c decrypts to \perp , whereas Decaps^\perp from \mathbf{U}^\perp returns a pseudorandom key K .

Gen^\perp 01 $(pk', sk') \leftarrow \text{Gen}_1$ 02 $s \xleftarrow{\$} \mathcal{M}$ 03 $sk := (sk', s)$ 04 return (pk', sk)	$\text{Encaps}(pk)$ 05 $m \xleftarrow{\$} \mathcal{M}$ 06 $c \leftarrow \text{Enc}_1(pk, m)$ 07 $K := \mathbf{H}(m, c)$ 08 return (K, c)	$\text{Decaps}^\perp(sk, c)$ 09 Parse $sk = (sk', s)$ 10 $m' := \text{Dec}_1(sk', c)$ 11 if $m' \neq \perp$ 12 return $K := \mathbf{H}(m', c)$ 13 else return $K := \mathbf{H}(s, c)$
--	---	---

Figure 12: IND-CCA-secure key encapsulation mechanism $\text{KEM}^\perp = \mathbf{U}^\perp[\text{PKE}_1, \mathbf{H}]$.

SECURITY. The following theorem establishes that IND-CCA security of KEM^\perp tightly reduces to the OW-PCA security of PKE_1 , in the random oracle model.

Theorem 3.4 (PKE_1 OW-PCA $\xrightarrow{\text{ROM}}$ KEM IND-CCA). *If PKE_1 is δ_1 -correct, then KEM^\perp is δ_1 -correct in the random oracle model. For any IND-CCA adversary \mathbf{B} against KEM^\perp , issuing at most q_D queries to the decapsulation oracle DECAPS^\perp and at most q_H queries to the random oracle \mathbf{H} , there exists an OW-PCA adversary \mathbf{A} against PKE_1 that makes at most q_H queries to the PCO oracle such that*

$$\text{Adv}_{\text{KEM}^\perp}^{\text{IND-CCA}}(\mathbf{B}) \leq \frac{q_H}{|\mathcal{M}|} + \text{Adv}_{\text{PKE}_1}^{\text{OW-PCA}}(\mathbf{A})$$

and the running time of \mathbf{A} is about that of \mathbf{B} .

The proof is very similar to the one of Theorem 3.3. The difference is the handling of decapsulation queries with inconsistent ciphertexts. Since the OW-PCA experiment does not provide a CVO oracle, the simulation of such queries has to be integrated into the random oracle patching technique.

Proof. It is easy to verify the correctness bound. Let \mathbf{B} be an adversary against the IND-CCA security of KEM , issuing at most q_D queries to DEC and at most q_H queries to \mathbf{H} . Consider the games given in Figure 13.

GAME G_0 . Since game G_0 is the original IND-CCA game,

$$\left| \Pr[G_0^{\mathbf{B}} \Rightarrow 1] - \frac{1}{2} \right| = \text{Adv}_{\text{KEM}^\perp}^{\text{IND-CCA}}(\mathbf{B}) .$$

GAME G_1 . In game G_1 we make two changes. First, we raise flag QUERY and abort if $\mathbf{H}(s, \cdot)$ is queried (lines 18 and 19). Second, we make the pseudorandom keys output by DECAPS^\perp perfectly random.

<p>GAMES $G_0 - G_3$</p> <p>01 $(pk', sk') \leftarrow \text{Gen}_1$</p> <p>02 $s \xleftarrow{\\$} \mathcal{M}$</p> <p>03 $sk := (sk', s)$</p> <p>04 $m^* \xleftarrow{\\$} \mathcal{M}$</p> <p>05 $c^* \leftarrow \text{Enc}_1(pk, m^*)$</p> <p>06 $K_0^* := \text{H}(m^*, c^*)$</p> <p>07 $K_1^* \xleftarrow{\\$} \{0, 1\}^n$</p> <p>08 $b \xleftarrow{\\$} \{0, 1\}$</p> <p>09 $b' \leftarrow \mathbf{B}^{\text{DECAPS}^\perp(\cdot), \text{H}(\cdot)}(pk', c^*, K_b^*)$</p> <p>10 return $\llbracket b' = b \rrbracket$</p> <p>$\text{DECAPS}^\perp(c \neq c^*)$</p> <p>11 $m' := \text{Dec}_1(sk', c)$</p> <p>12 if $m' = \perp$ return $K := \text{H}(s, c)$</p> <p>13 if $m' = \perp$ return $K := \text{H}'(c)$</p> <p>14 if $m' = s$ return $K := \text{H}'(c)$</p> <p>15 return $K := \text{H}(m', c)$</p>	<p>$\text{H}(m, c)$</p> <p>16 if $\exists K$ s. th. $(m, c, K) \in \mathcal{L}_H$ return K</p> <p>17 $K \xleftarrow{\\$} \mathcal{K}$</p> <p>18 if $m = s$ // $G_1 - G_3$</p> <p>19 QUERY := true; abort // $G_1 - G_3$</p> <p>20 if $\text{Dec}_1(sk', c) = m$ // $G_2 - G_3$</p> <p>21 if $c = c^*$ // G_3</p> <p>22 CHAL := true; abort // G_3</p> <p>23 if $\exists K'$ such that $(c, K') \in \mathcal{L}_D$ // $G_2 - G_3$</p> <p>24 $K := K'$ // $G_2 - G_3$</p> <p>25 else // $G_2 - G_3$</p> <p>26 $\mathcal{L}_D := \mathcal{L}_D \cup \{(c, K)\}$ // $G_2 - G_3$</p> <p>27 $\mathcal{L}_H := \mathcal{L}_H \cup \{(m, c, K)\}$</p> <p>28 return K</p> <p>$\text{DECAPS}^\perp(c \neq c^*)$ // $G_0 - G_1$ $\text{DECAPS}^\perp(c \neq c^*)$ // $G_2 - G_3$</p> <p>29 if $\exists K$ s. th. $(c, K) \in \mathcal{L}_D$</p> <p>30 return K</p> <p>31 else</p> <p>32 $K \xleftarrow{\\$} \mathcal{K}$</p> <p>33 $\mathcal{L}_D := \mathcal{L}_D \cup \{(c, K)\}$</p> <p>34 return K</p>
--	--

Figure 13: Games $G_0 - G_3$ for the proof of Theorem 3.4 . H' (lines 13 and 14) is an independent internal random oracle that cannot be accessed by \mathbf{B} .

That is, in $\text{DECAPS}^\perp(c)$, we replace $K = \text{H}(s, c)$ by $K = \text{H}'(c)$ if $m' = \text{Dec}_1(sk', c) = \perp$ (lines 13) or if $m' = \text{Dec}_1(sk', c) = s$ (line 14), where H' is an independent internal random oracles that cannot be accessed by \mathbf{B} . The latter remains unnoticed by \mathbf{B} unless $\text{H}(s, \cdot)$ is queried, in which case G_1 aborts. (Also note that $m' := \text{Dec}_1(sk, c)$ is unique.) Since \mathbf{B} 's view is independent of (the uniform secret) s unless G_1 aborts,

$$|\Pr[G_1^{\mathbf{B}} \Rightarrow 1] - \Pr[G_0^{\mathbf{B}} \Rightarrow 1]| \leq \frac{q_{\text{H}}}{|\mathcal{M}|} .$$

GAME G_2 . In game G_2 , the oracles H and DECAPS^\perp are modified such that DECAPS^\perp does not make use of the secret key any longer except by testing if $\text{Dec}_1(sk', c) = m$ for given (m, c) in line 20. In game G_2 we will use two lists, \mathcal{L}_H and \mathcal{L}_D , for bookkeeping. $(m, c, K) \in \mathcal{L}_H$ indicates that H was queried on (m, c) and $\text{H}(m, c) = K$ holds; $(c, K) \in \mathcal{L}_D$ indicates that $\text{DECAPS}^\perp(c) = K$ holds and either H was queried on $(m := \text{Dec}_1(sk', c), c)$ or DECAPS^\perp was queried on c . In order to show that the view of \mathbf{B} is identical in games G_1 and G_2 , consider the following cases for a fixed ciphertext c and $m' := \text{Dec}_1(sk', c)$.

- Case 1: $m' \in \{\perp, s\}$. Since H cannot be queried on (m', c) (i.e., $\text{H}(\perp, \cdot)$ is not allowed and $\text{H}(s, c)$ results in abort), the simulation of H can never add a tuple of the form (c, K) to \mathcal{L}_D . Hence, querying $\text{DECAPS}^\perp(c)$ in game G_2 will return a uniformly random key, as in Game G_1 .
- Case 2: $m' \notin \{\perp, s\}$. We will now show that H in game G_2 is “patched”, meaning that it is ensured $\text{DECAPS}^\perp(c) = \text{H}(m', c)$, where $m' := \text{Dec}_1(sk', c)$, for all valid ciphertexts c with $\text{Dec}_1(sk', c) \neq s$. We distinguish two sub-cases: \mathbf{B} might either first query H on (m', c) , then DECAPS^\perp on c , or the other way round.
 - If H is queried on (m', c) first, it is recognized that $\text{Dec}_1(sk', c) = m'$ in line 20. Since DECAPS^\perp was yet not queried on c , no entry of the form (c, K) already exists in \mathcal{L}_D . Therefore, besides adding $(m', c, K \xleftarrow{\$} \mathcal{K})$ to \mathcal{L}_H , H also adds (c, K) to \mathcal{L}_D in line 26, thereby defining $\text{DECAPS}^\perp(c) := K = \text{H}(m', c)$.
 - If DECAPS^\perp is queried on c first, no entry of the form (c, K) exists in \mathcal{L}_D yet. Therefore, DECAPS^\perp adds $(c, K \xleftarrow{\$} \mathcal{K})$ to \mathcal{L}_D thereby defining $\text{DECAPS}^\perp(c) := K$. When queried on (m', c) afterwards, H recognizes that $\text{Dec}_1(sk', c) = m'$ in line 20 and that an entry of the form

$A^{\text{PCO}(\cdot)}(pk, c^*)$	$H(m, c)$
01 $K^* \xleftarrow{\$} \mathcal{K}$	08 if $\exists K$ s. th. $(m, c, K) \in \mathcal{L}_H$ return K
02 $s \xleftarrow{\$} \mathcal{M}$	09 $K \xleftarrow{\$} \mathcal{K}$
03 $b' \leftarrow \mathbf{B}^{\text{DECAPS}^\mathcal{L}(\cdot), H(\cdot)}(pk, c^*, K^*)$	10 if $m = s$
04 if $\exists(m', c', K') \in \mathcal{L}_H$	11 abort
s. th. $\text{PCO}(m', c^*) = 1$	12 if $\text{PCO}(m, c) = 1$
05 return m'	13 if $\exists K'$ s. th. $(c, K') \in \mathcal{L}_D$
06 else	14 $K := K'$
07 abort	15 else
	16 $\mathcal{L}_D := \mathcal{L}_D \cup \{(c, K)\}$
	17 $\mathcal{L}_H := \mathcal{L}_H \cup \{(m, c, K)\}$
	18 return K

Figure 14: Adversary A against OW-PCA for the proof of Theorem 3.4. Oracle $\text{DECAPS}^\mathcal{L}$ is defined as in game G_3 of Figure 13.

(c, K) already exists in \mathcal{L}_D in line 23. By adding (m', c, K) to \mathcal{L}_H and returning K , H defines $H(m', c) := K = \text{DECAPS}^\mathcal{L}(c)$.

We have shown that B's view is identical in both games and

$$\Pr[G_2^{\mathbf{B}} \Rightarrow 1] = \Pr[G_1^{\mathbf{B}} \Rightarrow 1] .$$

GAME G_3 . In game G_3 , we abort immediately (and raise flag CHAL) on the event that B queries H on (m^*, c^*) , where m^* is the challenge message. Due to the difference lemma,

$$|\Pr[G_3^{\mathbf{B}} \Rightarrow 1] - \Pr[G_2^{\mathbf{B}} \Rightarrow 1]| \leq \Pr[\text{CHAL}] .$$

In game G_3 , $H(m^*, c^*)$ will not be given to B; neither through a hash nor a decryption query, meaning bit b is independent from B's view. Hence,

$$\Pr[G_3^{\mathbf{B}}] = \frac{1}{2} .$$

It remains to bound $\Pr[\text{CHAL}]$. To this end, we construct an adversary A against the OW-PCA security of PKE_1 simulating G_3 for B as in Figure 14. Note that the simulation is perfect. Since CHAL implies that B queried $H(m^*, c^*)$ which implies $(m^*, c^*, K') \in \mathcal{L}_H$ (for some K'), A returns $m' = m^*$ and wins its OW-PCA game. Hence,

$$\Pr[\text{CHAL}] = \text{Adv}_{\text{PKE}}^{\text{OW-PCA}}(\text{A}) .$$

Collecting the probabilities yields the required bound. \square

3.2.3 Transformations $U_m^\mathcal{L}/U_m^\perp$: from OW-CPA/OW-VA to IND-CCA for deterministic Encryption

Transformation U_m^\perp is a variant of U^\perp that derives the KEM key as $K = H(m)$, instead of $K = H(m, c)$. It transforms a OW-VA secure public-key encryption scheme with deterministic encryption (e.g., the ones obtained via T from Section 3.1) into an IND-CCA secure key encapsulation mechanism. We also consider an implicit rejection variant $U_m^\mathcal{L}$ that only requires OW-CPA security of the underlying encryption scheme PKE.

THE CONSTRUCTION. To a public-key encryption scheme $\text{PKE}_1 = (\text{Gen}_1, \text{Enc}_1, \text{Dec}_1)$ with message space \mathcal{M} , and a random oracle $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$, we associate $\text{KEM}_m^\mathcal{L} = U_m^\mathcal{L}[\text{PKE}_1, H] = (\text{Gen}^\mathcal{L}, \text{Encaps}_m, \text{Decaps}_m^\mathcal{L})$ and $\text{KEM}_m^\perp = U_m^\perp[\text{PKE}_1, H] = (\text{Gen}_1, \text{Encaps}_m, \text{Decaps}_m^\perp)$. Algorithm $\text{Gen}^\mathcal{L}$ is given in Figure 12 and the remaining algorithms of $\text{KEM}_m^\mathcal{L}$ and KEM_m^\perp are defined in Figure 15.

SECURITY OF KEM_m^\perp . The following theorem establishes that IND-CCA security of KEM_m^\perp tightly reduces to the OW-VA security of PKE_1 , in the random oracle model.

$\text{Encaps}_m(pk)$	$\text{Decaps}_m^\perp(sk, c)$	$\text{Decaps}_m^\perp(sk, c)$
01 $m \xleftarrow{\$} \mathcal{M}$	05 Parse $sk = (sk', s)$	10 $m' := \text{Dec}_1(sk, c)$
02 $c := \text{Enc}_1(pk, m)$	06 $m' := \text{Dec}_1(sk', c)$	11 if $m' = \perp$ return \perp
03 $K := \text{H}(m)$	07 if $m' \neq \perp$	12 else return
04 return (K, c)	08 return $K := \text{H}(m')$	$K := \text{H}(m')$
	09 else return $K := \text{H}(s, c)$	

Figure 15: IND-CCA-secure key encapsulation mechanisms $\text{KEM}_m^\perp = \text{U}_m^\perp[\text{PKE}_1, \text{H}]$ and $\text{KEM}_m^\perp = \text{U}_m^\perp[\text{PKE}_1, \text{H}]$.

GAMES $G_0 - G_2$	$\text{H}(m)$	
01 $(pk, sk) \leftarrow \text{Gen}_1$	12 if $\exists K$ such that $(m, K) \in \mathcal{L}_H$	
02 $m^* \xleftarrow{\$} \mathcal{M}$	13 return K	
03 $K_0^* := \text{H}(m^*)$	14 if $m = m^*$ and c^* defined	// G_2
04 $K_1^* \xleftarrow{\$} \{0, 1\}^n$	15 CHAL := true	// G_2
05 $c^* := \text{Enc}_1(pk, m^*)$	16 abort	// G_2
06 $b \xleftarrow{\$} \{0, 1\}$	17 $c' := \text{Enc}_1(pk, m)$	// $G_1 - G_2$
07 $b' \leftarrow \mathcal{B}^{\text{DECAPS}_m^\perp, \text{H}}(pk, c^*, K_b^*)$	18 $K \xleftarrow{\$} \mathcal{K}$	
08 return $\llbracket b' = b \rrbracket$	19 if $\exists K'$ such that $(c', K') \in \mathcal{L}_D$	// $G_1 - G_2$
	20 $K := K'$	// $G_1 - G_2$
	21 else	// $G_1 - G_2$
	22 $\mathcal{L}_D := \mathcal{L}_D \cup \{(c', K)\}$	// $G_1 - G_2$
	23 $\mathcal{L}_H := \mathcal{L}_H \cup \{(m, K)\}$	
	24 return K	
$\text{DECAPS}_m^\perp(c \neq c^*)$	// G_0	$\text{DECAPS}_m^\perp(c \neq c^*)$
09 $m' := \text{Dec}_1(sk, c)$	25 if $\exists K$ s. th. $(c, K) \in \mathcal{L}_D$	// $G_1 - G_2$
10 if $m' = \perp$ return \perp	26 return K	
11 return $K := \text{H}(m')$	27 if $\text{Dec}_1(sk, c) \notin \mathcal{M}$	
	28 return \perp	
	29 $K \xleftarrow{\$} \mathcal{K}$	
	30 $\mathcal{L}_D := \mathcal{L}_D \cup \{(c, K)\}$	
	31 return K	

Figure 16: Games $G_0 - G_2$ for the proof of Theorem 3.5

Theorem 3.5 (PKE_1 det., OW-VA $\xrightarrow{\text{ROM}}$ KEM_m^\perp IND-CCA). *If PKE_1 is δ_1 -correct, then so is KEM_m^\perp . Furthermore, assume PKE_1 to be rigid. Let \mathcal{G} denote the random oracle that PKE_1 uses (if any), and let $q_{\text{Enc}_1, \mathcal{G}}$ and $q_{\text{Dec}_1, \mathcal{G}}$ denote an upper bound on the number of \mathcal{G} -queries that Enc_1 , resp. Dec_1 makes upon a single invocation. If Enc_1 is deterministic then, for any IND-CCA adversary \mathcal{B} against KEM_m^\perp , issuing at most q_D queries to the decapsulation oracle DECAPS_m^\perp and at most q_G , resp. q_H queries to its random oracles \mathcal{G} and H , there exists an OW-VA adversary \mathcal{A} against PKE_1 that makes at most q_D queries to the CVO oracle such that*

$$\text{Adv}_{\text{KEM}_m^\perp}^{\text{IND-CCA}}(\mathcal{B}) \leq \text{Adv}_{\text{PKE}_1}^{\text{OW-VA}}(\mathcal{A}) + \delta_1(q_G + (q_H + q_D)(q_{\text{Enc}_1, \mathcal{G}} + q_{\text{Dec}_1, \mathcal{G}}))$$

and the running time of \mathcal{A} is about that of \mathcal{B} .

The proof is similar to the one of Theorem 3.3. A naive adaptation would reduce to PKE_1 's OW-PCVA security and make $O(q_H q_D)$ queries to the PCO oracle. Instead, we exploit the deterministic Enc_1 to (implicitly) simulate our own PCO oracle via re-encryption during the proof.

Proof. It is easy to verify the correctness bound. (Note that the correctness error δ_1 of KEM_m^\perp is independent of the number of H -queries that an adversary on KEM_m^\perp 's correctness makes.)

To show security of KEM_m^\perp , let \mathcal{B} be an adversary against the IND-CCA security of KEM_m^\perp , issuing at most q_D queries to DECAPS_m^\perp and at most q_H queries to H . Consider the games given in Figure 16.

GAME G_0 . Since game G_0 is the original IND-CCA game,

$$\left| \Pr[G_0^{\mathbf{B}} \Rightarrow 1] - \frac{1}{2} \right| = \text{Adv}_{\text{KEM}_m^{\text{IND-CCA}}}(\mathbf{B}) .$$

GAME G_1 . In game G_1 , the oracles \mathbf{H} and DECAPS_m^\perp are changed such that they make no use of the secret key any longer except for testing if $\text{Dec}_1(sk, c) \in \mathcal{M}$ for given c in line 27. Game G_1 contains two sets: hash list \mathfrak{L}_H which contains all entries (m, K) where \mathbf{H} was queried on m , and set \mathfrak{L}_D which contains all entries (c, K) where either DECAPS_m^\perp was queried on c , or \mathbf{H} was queried on some message m such that $c = \text{Enc}_1(pk, m)$.

Let QUERY denote the event that \mathfrak{L}_H contains an entry (m, K) with $\text{Dec}_1(sk, \text{Enc}_1(pk, m)) \neq m$. Intuitively, QUERY denotes the event that a correctness error of PKE_1 actually occurs. We will show that the view of \mathbf{B} is identical in games G_0 and G_1 unless a query to \mathbf{H} occurs on a plaintext that induces a correctness error, i.e., we show that the view only differs if QUERY happens.

To do so, we have to examine if DECAPS_m^\perp and \mathbf{H} handle queries consistently in game G_1 : In game G_0 , it holds that $\text{DECAPS}_m^\perp(c) = \mathbf{H}(\text{Dec}_1(sk, c))$ for all ciphertexts c such that $\text{Dec}_1(sk, c) \neq \perp$. To analyze game G_1 , let c be a query to DECAPS_m^\perp , and let $m' := \text{Dec}_1(sk, c)$.

We first show that before the query to DECAPS_m^\perp on c and the query to \mathbf{H} on m' , no entry of the form (c, K) could already exist in \mathfrak{L}_D yet unless QUERY happened: Since neither DECAPS was yet queried on c nor \mathbf{H} was yet queried on m' , existence of an entry (c, K) in \mathfrak{L}_D implies that \mathbf{H} was queried on some message $m \neq m'$ such that $\text{Enc}_1(pk, m) = c$. Hence, $\text{Dec}_1(sk, \text{Enc}_1(pk, m)) = \text{Dec}_1(sk, c) = m' \neq m$, meaning that m induces a correctness error and QUERY happened.

We will now analyze the games' behaviour in the case that \mathbf{H} was not queried on such an error-inducing message, i.e., conditioned on $\neg\text{QUERY}$. If $\text{Dec}_1(sk, c) = \perp$, $\text{DECAPS}_m^\perp(c)$ returns \perp in both games. It remains to show that $\text{DECAPS}_m^\perp(c) = \mathbf{H}(m')$ if $m' \neq \perp$. We distinguish two sub-cases: \mathbf{B} might either first query \mathbf{H} on m' , then DECAPS_m^\perp on c , or the other way round.

- If \mathbf{H} is queried on m' first, no entry of the form (c, K) already exists in \mathfrak{L}_D . Hence, besides adding $(m', K \stackrel{\$}{\leftarrow} \mathcal{K})$ to \mathfrak{L}_H , \mathbf{H} also computes $c' := \text{Enc}_1(pk, m')$, where $c' = c$ due to PKE_1 's rigidity. By adding (c, K) to \mathfrak{L}_D in line 22, \mathbf{H} defines $\text{DECAPS}_m^\perp(c) := K = \mathbf{H}(m')$.
- If DECAPS_m^\perp is queried on c first, it adds $(c, K \stackrel{\$}{\leftarrow} \mathcal{K})$ to \mathfrak{L}_D , thereby defining $\text{DECAPS}_m^\perp(c) := K$. When queried on m' afterwards, \mathbf{H} computes $\text{Enc}_1(pk, m') = c$, and recognizes that an entry of the form (c, K) already exists in \mathfrak{L}_D in line 19. By adding (m', K) to \mathfrak{L}_H and returning K , \mathbf{H} defines $\mathbf{H}(m') := K = \text{DECAPS}_m^\perp(c)$.

We have shown that \mathbf{B} 's view is identical in both games unless a correctness error (in the form of QUERY) occurs.

$$|\Pr[G_1^{\mathbf{B}} \Rightarrow 1] - \Pr[G_0^{\mathbf{B}} \Rightarrow 1]| \leq \Pr[\text{QUERY}] .$$

We can bound $\Pr[\text{QUERY}]$ with a straightforward reduction to the δ_1 -correctness of PKE_1 . In this reduction, an adversary on PKE_1 's correctness simulates Game G_0 and additionally checks for QUERY upon every DECAPS_m^\perp and every \mathbf{H} query. In total, this takes $q_G + (q_H + q_D)(q_{\text{Enc}_1, G} + q_{\text{Dec}_1, G})$ queries to \mathbf{G} : q_G queries from \mathbf{B} , and $q_{\text{Enc}_1, G} + q_{\text{Dec}_1, G}$ additional queries upon each query to \mathbf{H} and DECAPS_m^\perp (in order to check for QUERY). Hence,

$$\Pr[\text{QUERY}] \leq \delta_1(q_G + (q_H + q_D)(q_{\text{Enc}_1, G} + q_{\text{Dec}_1, G})) .$$

GAME G_2 . In game G_2 , we abort (with uniformly random output) immediately on the event that \mathbf{B} queries \mathbf{H} on m^* . Denote this event as CHAL . Due to the difference lemma,

$$|\Pr[G_2^{\mathbf{B}} \Rightarrow 1] - \Pr[G_1^{\mathbf{B}} \Rightarrow 1]| \leq \Pr[\text{CHAL}] .$$

In game G_2 , $\mathbf{H}(m^*)$ will not be given to \mathbf{B} ; neither through a hash nor a decryption query, meaning bit b is independent from \mathbf{B} 's view. Hence,

$$\Pr[G_2^{\mathbf{B}}] = \frac{1}{2} .$$

$A^{\text{Cvo}(\cdot)}(pk, c^*)$ 01 $K^* \xleftarrow{\$} \mathcal{K}$ 02 $b' \leftarrow \mathbf{B}^{\text{DECAPS}_m^\perp(\cdot), \text{H}(\cdot)}(pk, c^*, K^*)$ 03 if $\exists(m', K') \in \mathcal{L}_H$ s. th. $\text{Enc}_1(pk, m') = c^*$ 04 return m' 05 else 06 abort	$\text{DECAPS}_m^\perp(c \neq c^*)$ 07 if $\exists K$ s. th. $(c, K) \in \mathcal{L}_D$ 08 return K 09 if $\text{Cvo}(c) = 0$ 10 return \perp 11 $K \xleftarrow{\$} \mathcal{K}$ 12 $\mathcal{L}_D := \mathcal{L}_D \cup \{(c, K)\}$ 13 return K
--	--

Figure 17: Adversary A against OW-VA for the proof of Theorem 3.5, where H is defined as in Game G_2 of Figure 16.

It remains to bound $\Pr[\text{CHAL}]$. To this end, we construct an adversary A against the OW-VA security of PKE_1 simulating G_2 for B as in Figure 17.

Note that the simulation is perfect until CHAL occurs. Furthermore, CHAL implies that B queried $\text{H}(m^*)$, which implies that $(m^*, K') \in \mathcal{L}_H$ for some K' . In this case, we have $\text{Enc}_1(pk, m^*) = c^*$ (since Enc_1 is deterministic), and thus A returns m^* . Hence,

$$\Pr[\text{CHAL}] = \text{Adv}_{\text{PKE}}^{\text{OW-VA}}(\text{A}) .$$

Collecting the probabilities yields the required bound. \square

SECURITY OF KEM_m^\times . The following theorem establishes that IND-CCA security of KEM_m^\times tightly reduces to the OW-CPA security of PKE_1 , in the random oracle model. Its proof is easily obtained by combining the proofs of Theorem 3.4 and Theorem 3.5.

Theorem 3.6 (PKE_1 OW-CPA $\stackrel{\text{ROM}}{\Rightarrow}$ KEM_m^\times IND-CCA). *If PKE_1 is δ_1 -correct, then so is KEM_m^\times . Furthermore, assume PKE_1 to be rigid. Let G denote the random oracle that PKE_1 uses (if any), and let $q_{\text{Enc}_1, G}$ and $q_{\text{Dec}_1, G}$ denote an upper bound on the number of G -queries that Enc_1 , resp. Dec_1 makes upon a single invocation. If Enc_1 is deterministic then, for any IND-CCA adversary B against KEM_m^\times , issuing at most q_D queries to the decapsulation oracle DECAPS_m^\times and at most q_G , resp. q_H queries to its random oracles G and H , there exists an OW-CPA adversary A against PKE_1 such that*

$$\text{Adv}_{\text{KEM}_m^\times}^{\text{IND-CCA}}(\text{B}) \leq \text{Adv}_{\text{PKE}_1}^{\text{OW-CPA}}(\text{A}) + \frac{q_D}{|\mathcal{M}|} + \delta_1(q_G + (q_H + q_D)(q_{\text{Enc}_1, G} + q_{\text{Dec}_1, G}))$$

and the running time of A is about that of B.

3.3 The resulting KEMs

For completeness, we combine transformation T with $\{\text{U}^\times, \text{U}^\perp, \text{U}_m^\times, \text{U}_m^\perp\}$ from the previous sections to obtain four variants of the FO transformation $\text{FO} := \text{U}^\times \circ \text{T}$, $\text{FO}^\perp := \text{U}^\perp \circ \text{T}$, $\text{FO}_m^\times := \text{U}_m^\times \circ \text{T}$, and $\text{FO}_m^\perp := \text{U}_m^\perp \circ \text{T}$. To a public-key encryption scheme $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space \mathcal{M} and randomness space \mathcal{R} , and hash functions $G : \mathcal{M} \rightarrow \mathcal{R}$, $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ we associate

$$\begin{aligned} \text{KEM}^\times &= \text{FO}^\times[\text{PKE}, G, H] := \text{U}^\times[\text{T}[\text{PKE}, G], H] = (\text{Gen}^\times, \text{Encaps}, \text{Decaps}^\times) \\ \text{KEM}^\perp &= \text{FO}^\perp[\text{PKE}, G, H] := \text{U}^\perp[\text{T}[\text{PKE}, G], H] = (\text{Gen}, \text{Encaps}, \text{Decaps}^\perp) \\ \text{KEM}_m^\times &= \text{FO}_m^\times[\text{PKE}, G, H] := \text{U}_m^\times[\text{T}[\text{PKE}, G], H] = (\text{Gen}^\times, \text{Encaps}_m, \text{Decaps}_m^\times) \\ \text{KEM}_m^\perp &= \text{FO}_m^\perp[\text{PKE}, G, H] := \text{U}_m^\perp[\text{T}[\text{PKE}, G], H] = (\text{Gen}, \text{Encaps}_m, \text{Decaps}_m^\perp) . \end{aligned}$$

Their constituting algorithms are given in Figure 18.

The following table provides (simplified) concrete bounds of the IND-CCA security of $\text{KEM} \in \{\text{KEM}^\times, \text{KEM}^\perp, \text{KEM}_m^\times, \text{KEM}_m^\perp\}$, directly obtained by combining Theorems 3.1–3.6. Here $q_{\text{RO}} := q_G + q_H$ counts the total number of B's queries to the random oracles G and H and q_D counts the number of B's decryption queries. The left column provides the bounds relative to the OW-CPA advantage, the right column relative to the IND-CPA advantage.

Gen^ℓ 01 $(pk, sk) \leftarrow \text{Gen}$ 02 $s \leftarrow_{\mathcal{S}} \mathcal{M}$ 03 $sk' := (sk, s)$ 04 return (pk, sk')	Encaps(pk) Encaps_m(pk) 09 $m \leftarrow_{\mathcal{S}} \mathcal{M}$ 10 $c := \text{Enc}(pk, m; G(m))$ 11 $K := \text{H}(m, c)$ $K := \text{H}(m)$ 12 return (K, c)
Decaps[⊥](sk, c) Decaps_m[⊥](sk, c) 05 $m' := \text{Dec}(sk, c)$ 06 if $c \neq \text{Enc}(pk, m'; G(m'))$ or $m' = \perp$ 07 return \perp 08 else return $K := \text{H}(m', c)$ $K := \text{H}(m')$	Decaps^ℓ(sk' = (sk, s), c) Decaps_m^ℓ(sk'(sk, s), c) 13 $m' := \text{Dec}(sk, c)$ 14 if $c \neq \text{Enc}(pk, m'; G(m'))$ or $m' = \perp$ 15 return $K := \text{H}(s, c)$ 16 else return $K := \text{H}(m', c)$ $K := \text{H}(m')$

Figure 18: IND-CCA secure Key Encapsulation Mechanisms $\text{KEM}^{\ell} = (\text{Gen}^{\ell}, \text{Encaps}, \text{Decaps}^{\ell})$, $\text{KEM}^{\perp} = (\text{Gen}, \text{Encaps}, \text{Decaps}^{\perp})$, $\text{KEM}_m^{\ell} = (\text{Gen}^{\ell}, \text{Encaps}_m, \text{Decaps}_m^{\ell})$, and $\text{KEM}_m^{\perp} = (\text{Gen}, \text{Encaps}_m, \text{Decaps}_m^{\perp})$ obtained from $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$.

KEM	Concrete bounds on $\text{Adv}_{\text{KEM}}^{\text{IND-CCA}}(\mathbf{B}) \leq$	
KEM^{ℓ}	$q_{\text{RO}} \cdot \delta + \frac{2q_{\text{RO}}}{ \mathcal{M} } + 2q_{\text{RO}} \cdot \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\mathbf{A})$	$q_{\text{RO}} \cdot \delta + \frac{3q_{\text{RO}}}{ \mathcal{M} } + 3 \cdot \text{Adv}_{\text{PKE}}^{\text{IND-CPA}}(\mathbf{A}')$
KEM^{\perp}	$q_{\text{RO}} \cdot (\delta + 2^{-\gamma}) + 2q_{\text{RO}} \cdot \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\mathbf{A})$	$q_{\text{RO}} \cdot (\delta + 2^{-\gamma}) + \frac{3q_{\text{RO}}}{ \mathcal{M} } + 3 \cdot \text{Adv}_{\text{PKE}}^{\text{IND-CPA}}(\mathbf{A}')$
KEM_m^{ℓ}	$(2q_{\text{RO}} + q_D) \cdot \delta + \frac{2q_{\text{RO}}}{ \mathcal{M} } + 2q_{\text{RO}} \cdot \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\mathbf{A})$	$(2q_{\text{RO}} + q_D) \cdot \delta + \frac{3q_{\text{RO}}}{ \mathcal{M} } + 3 \cdot \text{Adv}_{\text{PKE}}^{\text{IND-CPA}}(\mathbf{A}')$
KEM_m^{\perp}	$(2q_{\text{RO}} + q_D) \cdot \delta + q_{\text{RO}} \cdot 2^{-\gamma} + 2q_{\text{RO}} \cdot \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\mathbf{A})$	$(2q_{\text{RO}} + q_D) \cdot \delta + q_{\text{RO}} \cdot 2^{-\gamma} + 3 \cdot \text{Adv}_{\text{PKE}}^{\text{IND-CPA}}(\mathbf{A}')$

CONCRETE PARAMETERS. For “ κ bits of security” one generally requires that for all adversaries \mathbf{B} with advantage $\text{Adv}(\mathbf{B})$ and running in time $\text{Time}(\mathbf{B})$, we have

$$\frac{\text{Time}(\mathbf{B})}{\text{Adv}(\mathbf{B})} \geq 2^{\kappa}.$$

The table below gives recommendations for the information-theoretic terms δ (correctness error of PKE), γ (γ -spreadness of PKE), and \mathcal{M} (message space of PKE) appearing the concrete security bounds above.

Term in concrete bound	Minimal requirement for κ bits security
$q_{\text{RO}} \cdot \delta$	$\delta \leq 2^{-\kappa}$
$q_{\text{RO}} \cdot 2^{-\gamma}$	$\gamma \geq \kappa$
$q_{\text{RO}}/ \mathcal{M} $	$ \mathcal{M} \geq 2^{\kappa}$

For example, if the concrete security bound contains the term $q_{\text{RO}} \cdot \delta$, then with $\delta \leq 2^{-\kappa}$ one has

$$\frac{\text{Time}(\mathbf{B})}{\text{Adv}(\mathbf{B})} \geq \frac{q_{\text{RO}}}{q_{\text{RO}} \cdot \delta} = \frac{1}{\delta} \geq 2^{\kappa},$$

as required for κ bits security.

3.4 S^{ℓ} : from OW-CPA to IND-CPA Security, tightly

S^{ℓ} transforms an OW-CPA secure public-key encryption scheme into an IND-CPA secure scheme. The security reduction has a parameter ℓ which allows for a tradeoff between the security loss of the reduction and the compactness of ciphertexts.

THE CONSTRUCTION. Fix an $\ell \in \mathbb{N}$. To a public-key encryption scheme $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M} = \{0, 1\}^n$ and a hash function $\text{F} : \mathcal{M}^{\ell} \rightarrow \mathcal{R}$, we associate $\text{PKE}_{\ell} = S^{\ell}[\text{PKE}, \text{F}]$. The algorithms of PKE_{ℓ} are defined in Figure 19.

SECURITY. The following theorem shows that PKE_{ℓ} is IND-CPA secure, provided that PKE is OW-CPA secure.

$\text{Enc}_\ell(pk, m)$	$\text{Dec}_\ell(sk, c = (c_0, \dots, c_\ell))$
01 $\mathbf{x} := (x_1, \dots, x_\ell) \xleftarrow{\$} (\{0, 1\}^n)^\ell$	06 for $i = 1$ to ℓ do
02 $c_0 := m \oplus F(\mathbf{x})$	07 $x_i := \text{Dec}(sk, c_i)$
03 for $i = 1$ to ℓ do	08 $\mathbf{x} := (x_1, \dots, x_\ell)$
04 $c_i := \text{Enc}(pk, x_i)$	09 return $c_0 \oplus F(\mathbf{x})$
05 return $c := (c_0, \dots, c_\ell)$	

Figure 19: Tightly IND-CPA secure encryption PKE_ℓ obtained from PKE.

Theorem 3.7 (PKE OW-CPA \Rightarrow PKE_ℓ IND-CPA). *If PKE is δ -correct (in the ROM), then PKE_ℓ is $\ell \cdot \delta$ -correct. Moreover, for any IND-CPA adversary \mathbf{B} that issues at most q_F queries to random oracle F , there exists an OW-CPA adversary \mathbf{A} such that*

$$\text{Adv}_{\text{PKE}_\ell}^{\text{IND-CPA}}(\mathbf{B}) \leq q_F^{1/\ell} \cdot \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\mathbf{A})$$

and the running time of \mathbf{A} is about that of \mathbf{B} .

Proof. We first sketch correctness. Consider a public key pk and an encryption $c = (c_0, \dots, c_\ell)$ of generated by Enc_ℓ . Let x_i denote the respective value chosen by Enc_ℓ when generating c . Furthermore, let QUERY_i denote the event that, when decrypting c , the partial ciphertext c_i is decrypted to a value $x'_i \neq x_i$. If no QUERY_i occurs (for any i), then this implies that c is decrypted correctly. Hence, we have

$$\Pr[c \text{ decrypts incorrectly}] \leq \Pr\left[\bigvee_{i=1}^{\ell} \text{QUERY}_i\right] \leq \sum_{i=1}^{\ell} \Pr[\text{QUERY}_i] \stackrel{(*)}{=} \ell \cdot \delta,$$

where the probability is over the random coins of Gen_ℓ , Enc_ℓ , and Dec_ℓ , and $(*)$ follows from the δ -correctness of PKE. We note that this argument also applies verbatim in the ROM.

As for security, let $\mathbf{B} = (\mathbf{B}_1, \mathbf{B}_2)$ be an adversary against the IND-CPA security of PKE_ℓ , issuing at most q_F queries to F . Consider the games given in Figure 20.

GAMES $G_0 - G_1$	$F(\mathbf{x})$
01 $(pk, sk) \leftarrow \text{Gen}()$	11 if $\exists r$ s.t. $(\mathbf{x}, r) \in \mathcal{L}_F$
02 $b \xleftarrow{\$} \{0, 1\}$	12 return r
03 $(m_0, m_1, st) \xleftarrow{\$} \mathbf{B}_1(pk)$	13 if $\mathbf{x} = \mathbf{x}^*$ // G_1
04 $\mathbf{x}^* := (x_1^*, \dots, x_\ell^*) \xleftarrow{\$} (\{0, 1\}^n)^\ell$	14 $\text{QUERY} := \text{true}$ // G_1
05 $c_0^* := m_b \oplus F(\mathbf{x}^*)$	15 abort // G_1
06 for $i = 1$ to ℓ do	16 $r \xleftarrow{\$} \mathcal{R}$
07 $c_i^* := \text{Enc}(pk, x_i)$	17 $\mathcal{L}_F := \mathcal{L}_F \cup \{(\mathbf{x}, r)\}$
08 $c^* := (c_0^*, \dots, c_\ell^*)$	18 return r
09 $b' \xleftarrow{\$} \mathbf{B}_2(pk, c^*, st)$	
10 return $\llbracket b' = b \rrbracket$	

Figure 20: Games $G_0 - G_1$ for the proof of Theorem 3.7

GAME G_0 . Since game G_0 is the original IND-CPA game,

$$|\Pr[G_0^{\mathbf{B}} \Rightarrow 1] - 1/2| = \text{Adv}_{\text{PKE}_\ell}^{\text{IND-CPA}}(\mathbf{B}) . \quad (6)$$

GAME G_1 . In Game G_1 , we add lines 13-15, and in particular a flag QUERY in line 14, and abort (such that the game outputs an independently random bit) when QUERY is raised. QUERY is raised whenever random oracle F is queried with the vector \mathbf{x}^* that was chosen during the generation of the challenge ciphertext c^* . Games G_0 and G_1 proceed identically until QUERY occurs. Hence, we have

$$|\Pr[G_0^{\mathbf{B}} \Rightarrow 1] - \Pr[G_1^{\mathbf{B}} \Rightarrow 1]| \leq \Pr[\text{QUERY}] . \quad (7)$$

Moreover, observe that in Game G_1 , \mathbf{B} 's view is independent of the bit b chosen by the game: b is only used in the computation of c_0^* , which in turn is blinded by $F(\mathbf{x}^*)$. But since the game aborts (with a

$A(pk, \widehat{c})$:	$F(\mathbf{x})$
01 $(m_0, m_1, st) \xleftarrow{\$} B_1^F(pk)$	15 if $\exists r$ s. th. $(\mathbf{x}, r) \in \mathcal{L}_F$
02 $c_0^* \xleftarrow{\$} \{0, 1\}^n$	16 return r
03 for $i = 1$ to ℓ with $i \neq i^*$	17 $r \xleftarrow{\$} \mathcal{R}$
04 $x_i^* \xleftarrow{\$} \{0, 1\}^n$	18 $\mathcal{L}_F := \mathcal{L}_F \cup \{(\mathbf{x}, r)\}$
05 $c_i^* \xleftarrow{\$} \text{Enc}(pk, x_i^*)$	19 parse $\mathbf{x} = (x_1, \dots, x_\ell)$
06 $i^* \xleftarrow{\$} [\ell]$	20 if $\forall i < i^* : x_i = x_i^*$
07 $c_{i^*}^* := \widehat{c}$	21 $\mathcal{L}_{i^*} := \mathcal{L}_{i^*} \cup \{x_{i^*}\}$
08 $c^* := (c_0^*, \dots, c_\ell^*)$	22 return r
09 $b' \xleftarrow{\$} B_2^F(pk, c^*, st)$	
10 if \mathcal{L}_{i^*} empty	
11 $x = \perp$	
12 else	
13 $x \xleftarrow{\$} \mathcal{L}_{i^*}$	
14 return x	

Figure 21: Adversary A against IND-CPA from B against OW-PCA for Lemma 3.8. Note that the sampling operation in line 13 refers to the *list* (not the *set*) \mathcal{L}_{i^*} (such that multiple F queries with the same x_{i^*} may raise the probability that that x_{i^*} is sampled).

random output) as soon as B queries $F(\mathbf{x}^*)$, this means that c_0^* is independently random in B's view. This means that also B's output b' and b are independent, which implies that the game's output $\llbracket b' = b \rrbracket$ is a uniformly random bit in case no abort occurs. But since the game also outputs a random bit upon an abort, we get that

$$\Pr[G_1^B \Rightarrow 1] = 1/2. \quad (8)$$

Taking (6-8) together, we thus get

$$\text{Adv}_{\text{PKE}_\ell}^{\text{IND-CPA}}(\text{B}) \leq \Pr[\text{QUERY}] ,$$

and the theorem follows from the next lemma. \square

Lemma 3.8 *In the situation of Game G_1 , we have*

$$\Pr[\text{QUERY}] \leq q_F^{1/\ell} \cdot \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\text{A})$$

for an adversary A (of roughly the same complexity as Game G_1).

Proof. We may assume that $\Pr[\text{QUERY}] > 0$ (so that it is possible to condition on QUERY). We describe adversary A in Figure 21.

To analyze B, let $\mathbf{x}^* := (x_1^*, \dots, x_\ell^*)$, where $x_{i^*}^*$ is the value encrypted in A's own challenge \widehat{c} , and, for $i \neq i^*$, the x_i^* are defined in line 4 in Figure 21. (That is, up to decryption errors, $x_i^* = \text{Dec}(sk, c_i^*)$ for all i .) Now observe that B's views in Game G_1 and in the simulation inside A are identical *until* B queries $F(\mathbf{x}^*)$. In this latter case, Game G_1 would abort, while A would simply continue the simulation. In particular, if we let QUERY denote the event that B queries $F(\mathbf{x}^*)$, then the probability of QUERY is the same in Game G_1 and in A's simulation. We can thus show the lemma by bounding the probability for QUERY in A's simulation.

To this end, for each $i \in [\ell]$, consider the probability

$$p_i := \Pr[x_i = x_i^* \mid (x_1, \dots, x_{i-1}) = (x_1^*, \dots, x_{i-1}^*) \wedge \text{QUERY}]$$

in an execution with A, where the probability is over a uniform choice of $\mathbf{x} = (x_1, \dots, x_\ell)$ among the set of all of F-queries from B. (Note that the condition QUERY guarantees that at least one such \mathbf{x} exists.) Intuitively, p_i denotes the probability that a F-query matches the challenge message in the i -th component when they already match in the first $i - 1$ components (assuming that QUERY occurs).

It will be helpful to first note a useful property of the p_i : namely, we have

$$\prod_{i=1}^{\ell} p_i \stackrel{(i)}{=} \Pr[\mathbf{x} = \mathbf{x}^* \mid \text{QUERY}] \stackrel{(ii)}{=} 1/q_F , \quad (9)$$

where (i) follows by using $\Pr[A | B] \cdot \Pr[B] = \Pr[A \wedge B]$ for arbitrary events A, B (such that B is possible), and (ii) follows by definition of QUERY.

Furthermore, we can connect the p_i to A 's output as follows. Observe that B 's view in A 's simulation does not depend on i^* , and thus, that the p_i do not change when conditioning on a specific choice of i^* . Now by construction of A and the list \mathfrak{L}_{i^*} , for each fixed choice of i^* , and assuming that QUERY occurs, we have that $x = x_{i^*}^*$ is sampled in line 13 with probability p_{i^*} . Note that in this case, A wins its own OW-CPA game. Formally:

$$\begin{aligned} \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(A) &= \Pr[A \Rightarrow x_{i^*}^*] = \frac{1}{\ell} \sum_{i=1}^{\ell} \Pr[A \Rightarrow x_i^* | i^* = i] \\ &= \frac{\Pr[\text{QUERY}]}{\ell} \sum_{i=1}^{\ell} \Pr[A \Rightarrow x_{i^*}^* | i^* = i \wedge \text{QUERY}] = \frac{\Pr[\text{QUERY}]}{\ell} \sum_{i=1}^{\ell} p_i \\ &\stackrel{(*)}{\geq} \Pr[\text{QUERY}] \cdot \left(\prod_{i=1}^{\ell} p_i \right)^{1/\ell} \stackrel{(9)}{=} \Pr[\text{QUERY}] \cdot \frac{1}{q_{\mathbb{F}}^{1/\ell}}, \end{aligned}$$

where (*) follows by the inequality between the arithmetic and geometric means. Rearranging terms yields the lemma. \square

4 Modular FO Transformation in the QROM

In this section, we will revisit our transformations in the quantum random oracle model. In Section 4.1, we give a short primer on quantum computation and define the quantum random oracle model (QROM). In Section 4.2, we will prove that transformation T from Figure 5 (Section 3.1) is also secure in the quantum random oracle model. Next, in Section 4.3 we will introduce QU_m^\perp (QU_m^\times), a variant of U_m^\perp (U_m^\times), which has provable security in the quantum random oracle model. Combining the two above transformations, in Section 4.4 we provide concrete bounds for the IND-CCA security of $\text{QKEM}_m^\perp = \text{QFO}_m^\perp[\text{PKE}, \text{G}, \text{H}, \text{H}']$ and $\text{QKEM}_m^\times = \text{QFO}_m^\times[\text{PKE}, \text{G}, \text{H}, \text{H}']$ in the QROM.

4.1 Quantum Computation

QUBITS. For simplicity, we will treat a *qubit* as a vector $|b\rangle \in \mathbb{C}^2$, i.e., a linear combination $|b\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ of the two *basis states* (vectors) $|0\rangle$ and $|1\rangle$ with the additional requirement to the probability amplitudes $\alpha, \beta \in \mathbb{C}$ that $|\alpha|^2 + |\beta|^2 = 1$. The basis $\{|0\rangle, |1\rangle\}$ is called *standard orthonormal computational basis*. The qubit $|b\rangle$ is said to be *in superposition*. Classical bits can be interpreted as quantum bits via the mapping ($b \mapsto 1 \cdot |b\rangle + 0 \cdot |1 - b\rangle$).

QUANTUM REGISTERS. We will treat a quantum register as a collection of multiple qubits, i.e. a linear combination $\sum_{(b_1, \dots, b_n) \in \{0,1\}^n} \alpha_{b_1 \dots b_n} \cdot |b_1 \dots b_n\rangle$, where $\alpha_{b_1, \dots, b_n} \in \mathbb{C}^n$, with the additional restriction that $\sum_{(b_1, \dots, b_n) \in \{0,1\}^n} |\alpha_{b_1 \dots b_n}|^2 = 1$. As in the one-dimensional case, we call the basis $\{|b_1 \dots b_n\rangle\}_{(b_1, \dots, b_n) \in \{0,1\}^n}$ the *standard orthonormal computational basis*.

MEASUREMENTS. Qubits can be measured with respect to a basis. In this paper, we will only consider measurements in the standard orthonormal computational basis, and denote this measurement by $\text{MEASURE}(\cdot)$, where the outcome of $\text{MEASURE}(|b\rangle)$ is a single qubit $|b\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ will be $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$, and the outcome of measuring a qubit register

$\sum_{b_1, \dots, b_n \in \{0,1\}} \alpha_{b_1 \dots b_n} \cdot |b_1 \dots b_n\rangle$ will be $|b_1 \dots b_n\rangle$ with probability $|\alpha_{b_1 \dots b_n}|^2$. Note that the amplitudes

collapse during a measurement, this means that by measuring $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$, α and β are switched to one of the combinations in $\{\pm(1, 0), \pm(0, 1)\}$. Likewise, in the n -dimensional case, all amplitudes are switched to 0 except for the one that belongs to the measurement outcome and which will be switched to 1.

QUANTUM ORACLES AND QUANTUM ADVERSARIES. Following [BDF⁺11, BBC⁺98], we view a quantum oracle as a mapping

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

where $O : \{0, 1\}^n \rightarrow \{0, 1\}^m$, $x \in \{0, 1\}^n$ and $y \in \{0, 1\}^m$, and model quantum adversaries A with access to O by the sequence $U \circ O$, where U is a unitary operation. We write $A^{(O)}$ to indicate that the oracles are quantum-accessible (contrary to oracles which can only process classical bits).

QUANTUM RANDOM ORACLE MODEL. We consider security games in the quantum random oracle model (QROM) as their counterparts in the classical random oracle model, with the difference that we consider quantum adversaries that are given **quantum** access to the random oracles involved, and **classical** access to all other oracles (e.g., plaintext checking or decapsulation oracles). Zhandry [Zha12b] proved that no quantum algorithm $A^{(f)}$, issuing at most q quantum queries to $|f\rangle$, can distinguish between a random function $f : \{0, 1\}^m \rightarrow \{0, 1\}^n$ and a $2q$ -wise independent function. It allows us to view quantum random oracles as polynomials of sufficient large degree. That is, we define a quantum random oracle $|H\rangle$ as an oracle evaluating a random polynomial of degree $2q$ over the finite field \mathbb{F}_{2^n} .

CORRECTNESS OF PKE IN THE QROM. Similar to the classical random oracle model, we need to define correctness of encryption in the quantum random oracle model. If $\text{PKE} = \text{PKE}^G$ is defined relative to a random oracle $|G\rangle$, then again the correctness bound might depend on the number of queries to $|G\rangle$. We call a public-key encryption scheme PKE in the quantum random oracle model $\delta(q_G)$ -correct if for all (possibly unbounded, quantum) adversaries A making at most q_G queries to quantum random oracle $|G\rangle$, $\Pr[\text{COR-QRO}_{\text{PKE}}^A \Rightarrow 1] \leq \delta(q_G)$, where the correctness game COR-QRO is defined as in Figure 22.

GAME COR-QRO:
23 $(pk, sk) \leftarrow \text{Gen}$
24 $m \leftarrow A^{(G)}(sk, pk)$
25 $c \leftarrow \text{Enc}(pk, m)$
26 **return** $\llbracket \text{Dec}(sk, c) \neq m \rrbracket$

Figure 22: Correctness game COR-QRO for PKE in the quantum random oracle model.

ALGORITHMIC ONEWAY TO HIDING. To a quantum oracle $|H\rangle$ and an algorithm A (possibly with access to other oracles) we associate the following extractor algorithm $\text{EXT}[A, |H\rangle]$ that returns a measurement x' of a randomly chosen query to $|H\rangle$.

EXT $[A, |H\rangle](inp)$
01 $i \xleftarrow{\$} [q_H]$
02 Run $A^{(|H\rangle)}(inp)$ until the i th query $|\hat{x}\rangle$ to $|H\rangle$
03 **if** $i >$ number of queries to $|H\rangle$
04 **return** \perp
05 **else**
06 $x' \leftarrow \text{MEASURE}(|\hat{x}\rangle)$
07 **return** x'

Figure 23: Extractor algorithm $\text{EXT}[A, |H\rangle](inp)$ for OW2H.

The following statement is an algorithmic adaption of OW2H from [Unr14] and will be used heavily during our security proofs.

Lemma 4.1 (*Algorithmic Oneway to hiding (AOW2H)*) *Let $|H\rangle : \{0, 1\}^n \rightarrow \{0, 1\}^m$ be a quantum random oracle, and let A be a quantum algorithm issuing at most q_H queries to $|H\rangle$ that, on input $x \in \{0, 1\}^n$, $y \in \{0, 1\}^m$ outputs either 0 or 1. Then, for all (probabilistic) algorithms F that input bit-strings in $\{0, 1\}^{n+m}$ (and do not make any hash queries to $|H\rangle$),*

$$\left| \Pr \left[1 \leftarrow A^{(|H\rangle)}(inp) \mid x \xleftarrow{\$} \{0, 1\}^n; inp \leftarrow F(x, H(x)) \right] - \Pr \left[1 \leftarrow A^{(|H\rangle)}(inp) \mid (x, y) \xleftarrow{\$} \{0, 1\}^{n+m}; inp \leftarrow F(x, y) \right] \right| \leq 2q_H \cdot \sqrt{\Pr[x \leftarrow \text{EXT}[A, |H\rangle](inp) \mid (x, y) \xleftarrow{\$} \{0, 1\}^{n+m}; inp \leftarrow F(x, y)]} .$$

Note that the original OWTH lemma can be obtained by applying Lemma 4.1 to $F(x, y) := (x, y)$.

GENERIC QUANTUM SEARCH. For $\lambda \in [0, 1]$ let B_λ be the Bernoulli distribution, i.e., $\Pr[b = 1] = \lambda$ for the bit $b \leftarrow B_\lambda$. Let X be some finite set. The generic quantum search problem GSP [HRS16, Thm. 1], [Zha12a], is to find an $x \in X$ satisfying $F(x) = 1$ given quantum access to an oracle $F : X \rightarrow \{0, 1\}$, such that for each $x \in X$, $F(x)$ is distributed according to B_λ . We will need the following slight variation of GSP that is given in [KLS17]. The Generic quantum Search Problem with Bounded probabilities GSPB is like the quantum search problem with the difference that the Bernoulli parameter $\lambda(x)$ may depend on x but it is upper bounded by a global λ .

Lemma 4.2 (*Generic Search Problem with Bounded Probabilities*) *Let $\lambda \in \{0, 1\}$. For any (unbounded, quantum) algorithm A issuing at most q quantum queries to $|F\rangle$, $\Pr[\text{GSPB}_\lambda^A \Rightarrow 1] \leq 8 \cdot \lambda \cdot (q + 1)^2$, where Game GSPB_λ is defined in Figure 24.*

GAME GSPB_λ
01 $(\lambda(x))_{x \in X} \leftarrow A_1$
02 **if** $\exists x \in X$ s.t. $\lambda(x) > \lambda$ **return** 0
03 **For** all $x \in X$
04 $F(x) \leftarrow B_{\lambda(x)}$
05 $x \leftarrow A_2^{F(\cdot)}$
06 **return** $F(x)$

Figure 24: The generic search game GSPB_λ with bounded maximal Bernoulli parameter $\lambda \in [0, 1]$.

4.2 Transformation T: from OW-CPA to OW-PCA in the QROM

Recall transformation T from Figure 5 of Section 3.1.

Lemma 4.3 *Assume PKE to be δ -correct. Then $\text{PKE}_1 = \text{T}[\text{PKE}, \text{G}]$ is δ_1 -correct in the quantum random oracle model, where $\delta_1 = \delta_1(q_G) \leq 8 \cdot (q_G + 1)^2 \cdot \delta$.*

Proof. Consider an (unbounded, quantum) adversary A in the quantum random oracle correctness game COR-QRO. For fixed (pk, sk) and message $m \in \mathcal{M}$, let

$$\mathcal{R}_{\text{bad}}(pk, sk, m) := \{r \in \mathcal{R} \mid \text{Dec}(sk, \text{Enc}(pk, m; r)) \neq m\}$$

denote the set of “bad” randomness. Further, define

$$\delta(pk, sk, m) := |\mathcal{R}_{\text{bad}}(pk, sk, m)| / |\mathcal{R}| \tag{10}$$

as the fraction of bad randomness and $\delta(pk, sk) := \max_{m \in \mathcal{M}} \delta(pk, sk, m)$. Note that with this notation $\delta = \mathbf{E}[\delta(pk, sk)]$, where the expectation is taken over $(pk, sk) \xleftarrow{\$} \text{Gen}$.

To upper bound $\Pr[\text{COR-QRO}^A \Rightarrow 1]$, we construct an (unbounded, quantum) adversary B in Figure 25 against the generic search problem with bounded probabilities GSPB_λ defined in Figure 24. B runs $(pk, sk) \xleftarrow{\$} \text{Gen}$ and computes the Bernoulli parameters $\lambda(m)$ of the generic search problem as $\lambda(m) := \delta(pk, sk, m)$ which are bounded by $\lambda := \delta(pk, sk) := \max_{m \in \mathcal{M}} \Pr[\text{Dec}(sk, \text{Enc}(pk, m)) \neq m]$.

To analyze B, we first fix (pk, sk) . For each $m \in \mathcal{M}$, by the definition of game GSPB_λ , the random variable $F(m)$ is distributed according to $B_{\lambda(m)} = B_{\delta(pk, sk, m)}$. By construction, the random variable $G(m)$ defined in line 09 if $F(m) = 0$ and in line 11 if $F(m) = 1$ is uniformly distributed in \mathcal{R} meaning G is a (quantum) random oracle.

A wins its game COR-QRO iff it returns a message m such that $G(m) \in \mathcal{R}_{\text{bad}}(pk, sk, m)$ or, equivalently, $F(m) = 1$ in which case B wins game GSP_λ . To summarize, conditioned on a fixed (pk, sk) we obtain by Lemma 4.2

$$\Pr[\text{COR-QRO}^A \Rightarrow 1 \mid (pk, sk)] \leq \Pr[\text{GSP}_{\delta(pk, sk)}^B \Rightarrow 1] \leq 8 \cdot \delta(pk, sk) \cdot (q_G + 1)^2.$$

By averaging over $(pk, sk) \xleftarrow{\$} \text{Gen}$ we finally obtain

$$\delta_1(q_G) = \Pr[\text{COR-QRO}^A \Rightarrow 1] \leq 8 \cdot \delta \cdot (q_G + 1)^2.$$

This completes the proof. □

B₁	B₂^{F(·)}	G(m)
01 $(pk, sk) \leftarrow \text{Gen}$	05 Pick $2q_H$ -wise hash f	08 if $F(m) = 0$
02 for $m \in \mathcal{M}$	06 $m \leftarrow \text{A}^{ \mathbf{G}(\cdot) }(pk, sk)$	09 $\mathbf{G}(m) := \text{Sample}(\mathcal{R} \setminus \mathcal{R}_{\text{bad}}(pk, sk, m); f(m))$
03 $\lambda(m) := \delta(pk, sk, m)$	07 return m	10 else
04 return $(\lambda(m))_{m \in \mathcal{M}}$		11 $\mathbf{G}(m) := \text{Sample}(\mathcal{R}_{\text{bad}}(pk, sk, m); f(m))$
		12 return $\mathbf{G}(m)$

Figure 25: Adversary **B** executed in game $\text{GSPB}_{\delta(pk, sk)}$ with access to $|F(\cdot)|$ for the proof of Theorem 4.4. $\delta(pk, sk, m)$ is defined in Equation (10). f (lines 09 and 11) is an internal $2q_G$ -wise independent hash function that cannot be accessed by **A**. $\text{Sample}(Y)$ is a probabilistic algorithm that returns a uniformly distributed $y \leftarrow_{\$} Y$. $\text{Sample}(Y; f(m))$ denotes the deterministic execution of $\text{Sample}(Y)$ using explicitly given randomness $f(m)$.

The following theorem (whose proof is loosely based on [TU16]) establishes that IND-PCA security of PKE_1 reduces to the OW-CPA security of PKE, in the quantum random oracle model.

Theorem 4.4 (PKE OW-CPA $\xrightarrow{\text{QROM}}$ PKE_1 OW-PCA). *Assume PKE to be δ -correct. For any OW-PCA quantum adversary **B** that issues at most q_G queries to the quantum random oracle $|\mathbf{G}\rangle$ and q_P (classical) queries to the plaintext checking oracle PCO, there exists an OW-CPA quantum adversary **A** such that*

$$\text{Adv}_{\text{PKE}_1}^{\text{OW-PCA}}(\mathbf{B}) \leq 8 \cdot (q_G + q_P + 1)^2 \cdot \delta + (1 + 2q_G) \cdot \sqrt{\text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\mathbf{A})},$$

and the running time of **A** is about that of **B**.

Similar to the proof of Theorem 3.1, in game G_1 the proof first implements the PCA oracle via “re-encryption”. Next, we apply AOW2H to decouple the challenge ciphertext $c^* := \text{Enc}(pk, m^*; \mathbf{G}(m^*))$ from the random oracle \mathbf{G} . The decoupling allows for a reduction from OW-CPA security.

Proof. Let **B** be an adversary against the OW-PCA security of PKE_1 , issuing at most q_G queries to $|\mathbf{G}\rangle$ and at most q_P queries to PCO. Consider the games given in Figure 26, where \mathbf{G} is modeled as a random $2q_G$ -wise independent hash function.

GAME G_0, G_2, H	PCO ($m \in \mathcal{M}, c$)
01 $(pk, sk) \leftarrow \text{Gen}$	09 $m' := \text{Dec}(sk, c)$ // G_0
02 $m^* \leftarrow_{\$} \mathcal{M}$	10 return $\llbracket m' = m \rrbracket$ and $\llbracket \text{Enc}(pk, m'; \mathbf{G}(m')) = c \rrbracket$ // G_0
03 $r^* := \mathbf{G}(m^*)$ // G_0, G_1	11 return $\llbracket \text{Enc}(pk, m; \mathbf{G}(m)) = c \rrbracket$ // G_1, G_2, H
04 $r^* \leftarrow_{\$} \mathcal{R}$ // G_2, H	
05 $c^* := \text{Enc}(pk, m^*; r^*)$	
06 $m' \leftarrow \text{B}^{ \mathbf{G}(\cdot) , \text{PCO}(\cdot, \cdot)}(pk, c^*)$ // G_1, G_2	
07 $m' \leftarrow \text{EXT}[\text{B}^{\text{PCO}(\cdot, \cdot)}, \mathbf{G}(\cdot)](pk, c^*)$ // H	
08 return $\llbracket m' = m^* \rrbracket$	

Figure 26: Games G_0, G_1, G_2, H for the proof of Theorem 4.4.

GAME G_0 . Since game G_0 is the original OW-PCA game,

$$\Pr[G_0^{\mathbf{B}} \Rightarrow 1] = \text{Adv}_{\text{PKE}_1}^{\text{OW-PCA}}(\mathbf{B}).$$

GAME G_1 . In game G_1 the plaintext checking oracle $\text{PCO}(\cdot, \cdot)$ is replaced with a simulation that doesn't make use of the secret key anymore. We claim

$$|\Pr[G_1^{\mathbf{B}} \Rightarrow 1] - \Pr[G_0^{\mathbf{B}} \Rightarrow 1]| \leq 8 \cdot (q_G + q_P + 1)^2 \cdot \delta. \quad (11)$$

To show Equation (11), first note that both Game G_0 and Game G_1 proceed identically until the event that **B** submits a PCO query (m, c) such that $c = \text{Enc}(pk, m; \mathbf{G}(m))$ and $\text{Dec}(sk, c) \neq m$. We call this

event BADR. Since both Game G_0 and Game G_1 proceed identically conditioned on the event that BADR does not happen,

$$|\Pr[G_1^B \Rightarrow 1] - \Pr[G_0^B \Rightarrow 1]| \leq \Pr[\text{BADR}] .$$

Similar to the proof of Theorem 3.1 one can again show that there exists an adversary F against COR-QRO that perfectly simulates games G_0 and G_1 and wins iff BADR happens. Applying Lemma 4.3, we see that

$$\Pr[\text{BADR}] \leq \Pr[\text{COR-QRO}^F] \leq 8 \cdot (q_G + q_P + 1)^2 \cdot \delta .$$

GAME G_2 . In game G_2 , we replace $r^* := G(m^*)$ with uniform randomness r^* in line 03. We apply Lemma 4.1 (AOW2H) to $x := m^*$, $y := r^*$, and algorithm F given in Figure 27. We obtain

$$|\Pr[G_2^B \Rightarrow 1] - \Pr[G_1^B \Rightarrow 1]| \leq 2 \cdot q_G \cdot \sqrt{\Pr[H^B \Rightarrow 1]} ,$$

where the extractor algorithm EXT of game H is defined in Figure 23.

<p>Algorithm $F(m^*, r^*)$ 01 $(pk, sk) \leftarrow \text{Gen}$ 02 $c^* := \text{Enc}(pk, m^*; r^*)$ 03 $inp = (pk, c^*)$ 04 return inp</p>

Figure 27: Algorithm F for the application of AOW2H in the proof of Theorem 4.4.

Now that r^* is uniformly random we trivially construct an adversary C in Figure 28 against the OW-CPA security of the original encryption scheme PKE simulating game G_2 for B that outputs $m' = m^*$ if B wins in game G_2 .

$$\Pr[G_2^B \Rightarrow 1] = \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(C) \leq \sqrt{\text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(C)} .$$

Finally, we construct another trivial adversary D in Figure 28 against the OW-CPA security of the original encryption scheme PKE simulating game H for B with Advantage

$$\Pr[H^B \Rightarrow 1] = \text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(D) .$$

Collecting the probabilities and combining adversaries C and D into one single adversary A proves the theorem. \square

4.3 Transformations QU_m^\perp , QU_m^\neq

4.3.1 Transformation QU_m^\perp : from OW-PCA to IND-CCA in the QROM

QU_m^\perp transforms an OW-PCA secure public-key encryption scheme into an IND-CCA secure key encapsulation mechanism with explicit rejection.

THE CONSTRUCTION. To a deterministic public-key encryption scheme $\text{PKE}_1 = (\text{Gen}_1, \text{Enc}_1, \text{Dec}_1)$ with message space $\mathcal{M} = \{0, 1\}^n$, and hash functions $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ and $H' : \{0, 1\}^n \rightarrow \{0, 1\}^n$, we associate $\text{QKEM}_m^\perp = \text{QU}_m^\perp[\text{PKE}_1, H, H']$. The algorithms of $\text{QKEM}_m^\perp = (\text{QGen} := \text{Gen}_1, \text{QEncaps}_m, \text{QDecaps}_m^\perp)$ are defined in Figure 29. We stress that hash function H' has matching domain and range.

<p>C(pk, c^*) 01 $m' \leftarrow \mathbf{B}^{ \mathbf{G}(\cdot) , \text{Pco}(\cdot, \cdot)}(pk, c^*)$ 02 return m'</p>	<p>D(pk, c^*) 03 $m' \leftarrow \text{EXT}[\mathbf{B}^{\text{Pco}(\cdot, \cdot)}, \mathbf{G}(\cdot)](pk, c^*)$ 04 return m'</p>
--	--

Figure 28: Adversaries C (left) and D (right) for the proof of Theorem 4.4. Oracle PCO is defined as in game G_2 of Figure 26.

<u>QEncaps_m(pk)</u>	<u>QDecaps_m[⊥](sk, c, d)</u>
01 $m \xleftarrow{\$} \mathcal{M}$	06 $m' := \text{Dec}_1(sk, c)$
02 $c := \text{Enc}_1(pk, m)$	07 if $m' = \perp$ or $H'(m') \neq d$
03 $d := H'(m)$	08 return \perp
04 $K := H(m)$	09 else return $K := H(m')$
05 return (K, c, d)	

Figure 29: IND-CCA-secure key encapsulation mechanism $\text{QKEM}_m^\perp = \text{QU}_m^\perp[\text{PKE}_1, H, H']$.

SECURITY. The following theorem (whose proof is again loosely based on [TU16]) establishes that IND-CCA security of QKEM_m^\perp reduces to the OW-PCA security of PKE_1 , in the quantum random oracle model, given that PKE_1 is rigid.

Theorem 4.5 (PKE_1 OW-PCA $\xrightarrow{\text{QROM}}$ QKEM_m^\perp IND-CCA). *If PKE_1 is δ_1 -correct, so is QKEM_m^\perp . Furthermore, assume PKE_1 to be rigid. For any IND-CCA quantum adversary B issuing at most q_D (classical) queries to the decapsulation oracle QDECAPS_m^\perp , at most q_H queries to the quantum random oracle $|H\rangle$ and at most $q_{H'}$ queries to the quantum random oracle $|H'\rangle$, there exists an OW-PCA quantum adversary A issuing $2q_D q_{H'}$ queries to oracle PCO such that*

$$\text{Adv}_{\text{QKEM}_m^\perp}^{\text{IND-CCA}}(B) \leq (2q_{H'} + q_H + 2q_D) \cdot \sqrt{\text{Adv}_{\text{PKE}_1}^{\text{OW-PCA}}(A) + \delta_1} ,$$

and the running time of A is about that of B .

Proof. Let B be an adversary against the IND-CCA security of QKEM_m^\perp , issuing at most q_D queries to QDECAPS_m^\perp , at most q_H queries to $|H\rangle$ and at most $q_{H'}$ queries to $|H'\rangle$. Consider the games G_0 - G_3 given in Figure 30.

GAMES $G_0 - G_3$		<u>QDECAPS_m[⊥]((c, d) ≠ (c*, d*))</u>
01 $b \xleftarrow{\$} \{0, 1\}$	// G_0 - G_2	10 if $c = c^*$
02 $(pk, sk) \leftarrow \text{Gen}_1$		11 return \perp // G_1 - G_3
03 $m^* \xleftarrow{\$} \{0, 1\}^n$; $c^* := \text{Enc}_1(pk, m^*)$		12 $m' := \text{Dec}_1(sk, c)$
04 $K_0^* := H(m^*)$; $K_1^* \xleftarrow{\$} \{0, 1\}^n$	// G_0 - G_2	13 if $m' = m^*$
05 $d^* := H'(m^*)$; $K^* := K_0^*$	// G_3	14 ABORT // G_2 - G_3
06 $d^* \xleftarrow{\$} \{0, 1\}^n$; $K^* \xleftarrow{\$} \{0, 1\}^n$		15 if $m' \neq \perp$ and $H'(m') = d$
07 $b' \leftarrow \text{B}^{\text{QDECAPS}_m^\perp, H\rangle, H'\rangle}(pk, (c^*, d^*), K^*)$	// G_0 - G_2	16 return $K := H(m')$
08 return $[[b' = b]]$	// G_0 - G_2	17 else return \perp
09 return b'	// G_3	

Figure 30: Games $G_0 - G_3$ for the proof of Theorem 4.5.

GAME G_0 . Since $G_0 = \text{IND-CCA}$,

$$\text{Adv}_{\text{QKEM}_m^\perp}^{\text{IND-CCA}}(B) = |\Pr[G_0^B \Rightarrow 1] - 1/2| .$$

The next two steps are preparation steps to ensure that no query to QDECAPS_m^\perp can trigger a query to H' on m^* .

GAME G_1 . In game G_1 , we change QDECAPS_m^\perp in line 11 such that it always returns \perp if queried on a ciphertext of the form (c^*, d) . We argue that this change is only conceptual unless m^* triggers a correctness error: Since query (c^*, d) is explicitly forbidden in both games G_0 and G_1 , we only have to consider the case that $d \neq d^*$. Let $m' := \text{Dec}_1(sk, c^*)$. If $m' = m^*$, $d \neq d^*$ implies that $H'(m') = H'(m^*) = d^* \neq d$, hence G_0 also returns \perp . Therefore, game G_1 only differs from game G_0 if $m' \neq m^*$ and

$$|\Pr[G_1^B \Rightarrow 1] - \Pr[G_0^B \Rightarrow 1]| \leq \delta_1 .$$

GAME G_2 . In game G_2 , we let QDECAPS_m^\perp abort in line 14 if queried on a ciphertext (c, d) such that $c \neq c^*$, but $\text{Dec}_1(sk, c) = m^*$. We claim that no such query is possible due to PKE_1 's rigidity: Take

any ciphertext c such that $\text{Dec}_1(sk, c) = m^*$. Since PKE_1 is rigid and $\text{Dec}_1(sk, c) \neq \perp$, it holds that $c = \text{Enc}_1(pk, \text{Dec}_1(sk, c)) = \text{Enc}_1(pk, m^*) = c^*$.

We just have shown that $\Pr[\text{ABORT}] = 0$, hence

$$\Pr[G_2^{\text{B}} \Rightarrow 1] = \Pr[G_1^{\text{B}} \Rightarrow 1] .$$

Note that from game G_2 on, no query to QDECAPS_m^\perp can possibly trigger a query on m^* to either of the random oracles H and H' .

GAME G_3 . In game G_3 , we replace $(d^* := \text{H}'(m^*), K^* := K_b^*)$ with uniform random (d^*, K^*) in line 06, and instead of returning whether B 's bit was the right guess, game G_3 just returns B 's bit, see line 09. Since

$$\begin{aligned} \Pr[G_2^{\text{B}} \Rightarrow 1] &= \frac{1}{2} (\Pr[G_2^{\text{B}} \Rightarrow 1 \mid b = 1] + \Pr[G_2^{\text{B}} \Rightarrow 1 \mid b = 0]) \\ &= \frac{1}{2} (\Pr[G_2^{\text{B}} \Rightarrow 1 \mid b = 1] - \Pr[G_2^{\text{B}} \Rightarrow 0 \mid b = 0]) + \frac{1}{2} , \end{aligned}$$

$$\begin{aligned} |\Pr[G_2^{\text{B}} \Rightarrow 1] - \frac{1}{2}| &= \frac{1}{2} |\Pr[G_2^{\text{B}} \Rightarrow 1 \mid b = 1] - \Pr[G_2^{\text{B}} \Rightarrow 0 \mid b = 0]| \\ &\leq \frac{1}{2} (|\Pr[G_2^{\text{B}} \Rightarrow 1 \mid b = 1] - \Pr[G_3^{\text{B}} \Rightarrow 1]| + |\Pr[G_2^{\text{B}} \Rightarrow 0 \mid b = 0] - \Pr[G_3^{\text{B}} \Rightarrow 1]|) . \end{aligned}$$

To upper bound $|\Pr[G_2^{\text{B}} \Rightarrow 1 \mid b = 1] - \Pr[G_3^{\text{B}} \Rightarrow 1]|$ and $|\Pr[G_2^{\text{B}} \Rightarrow 0 \mid b = 0] - \Pr[G_3^{\text{B}} \Rightarrow 1]|$, we will make use of Lemma 4.1 (OWTH), where we let $F(m^*, d^*) = (m^*, d^*)$ for $b = 1$, and $F(m^*, d^*, K^*) = (m^*, d^*, K^*)$ for $b = 0$. Consider the adversaries D_b and games H_b given in Figure 31. D_1 issues at most $q_{\text{H}'} + q_D$ queries to H' , and perfectly simulates game G_2 for bit $b = 1$ if run on input $(m^*, d^* = \text{H}'(m^*))$, and game G_3 if run on uniformly random input $(m^*, d^*) \xleftarrow{\$} \{0, 1\}^{n+m}$, hence

$$\begin{aligned} |\Pr[G_2^{\text{B}} \Rightarrow 1 \mid b = 1] - \Pr[G_3^{\text{B}} \Rightarrow 1]| &= |\Pr[m^* \xleftarrow{\$} \{0, 1\}^n, d^* = \text{H}'(m^*), b \leftarrow \text{D}_1(m^*, d^*) : b = 1] \\ &\quad - \Pr[(m^*, d^*) \xleftarrow{\$} \{0, 1\}^{n+m}, b \leftarrow \text{D}_1(m^*, d^*) : b = 1]| \\ &\leq 2(q_{\text{H}'} + q_D) \cdot \sqrt{\Pr[H_1^{\text{D}_1} \Rightarrow 1]} . \end{aligned}$$

Likewise, D_0 issues at most $q_{\text{H}'} + q_{\text{H}} + q_D$ queries to $\text{H}' \times \text{H}$, and perfectly simulates game G_2 for bit $b = 0$ if run on input $(m^*, (d^*, K^*) = \text{H}' \times \text{H}(m^*))$, and game G_3 if run on uniformly random input $(m^*, d^*, K^*) \xleftarrow{\$} \{0, 1\}^{2n+m}$, hence

$$|\Pr[G_2^{\text{B}} \Rightarrow 0 \mid b = 0] - \Pr[G_3^{\text{B}} \Rightarrow 1]| \leq 2(q_{\text{H}'} + q_{\text{H}} + q_D) \cdot \sqrt{\Pr[H_0^{\text{D}_0} \Rightarrow 1]} .$$

So far, we established

$$|\Pr[G_2^{\text{B}} \Rightarrow 1] - 1/2| \leq (q_{\text{H}'} + q_D) \cdot \sqrt{\Pr[H_1^{\text{D}_1} \Rightarrow 1]} + (q_{\text{H}'} + q_{\text{H}} + q_D) \cdot \sqrt{\Pr[H_0^{\text{D}_0} \Rightarrow 1]} .$$

To upper bound $\Pr[H_b^{\text{D}_b} \Rightarrow 1]$, consider the sequence of games given in Figure 32.

GAMES $G_{4,b}$. Games $G_{4,b}$ are reformulations of games H_b that do not use the helper adversaries D_b anymore. Game $G_{4,b}$ differs from H_b only in the following way: Game H_b randomly picks one of the queries to H' (or, respectively, $\text{H}' \times \text{H}$) that D_b issued, including all implicit queries, i.e., the classical queries that were triggered by B 's queries to QDECAPS_m^\perp . Game $G_{4,b}$ excludes those implicit queries and picks only amongst the explicit queries to H' ($\text{H}' \times \text{H}$) that B issued.

Note, however, that D_b loses in game H_b if the game randomly picks one of the queries that were triggered by B 's queries to QDECAPS_m^\perp : D_b rejects queries to QDECAPS_m^\perp on ciphertexts of the form (c^*, d) , and aborts if QDECAPS_m^\perp is queried on a ciphertext $(c, d) \neq (c^*, d^*)$ such that $\text{Dec}_1(sk, c) = m^*$, hence no query to QDECAPS_m^\perp could possibly trigger a query to H' ($\text{H}' \times \text{H}$) on m^* , and

$$\Pr[H_b^{\text{D}_b} \Rightarrow 1] \leq \Pr[G_{4,b}^{\text{B}} \Rightarrow 1] .$$

$\underline{D_1^{ \mathbf{H}' , \mathbf{H}' }}(m^*, d^*)$ 01 $(pk, sk) \leftarrow \text{Gen}_1$ 02 $c^* := \text{Enc}_1(pk, m^*)$ 03 $K^* \xleftarrow{\$} \{0, 1\}^n$ 04 $b' \leftarrow \mathbf{B}^{\text{QDECAPS}_m^\perp, \mathbf{H}' , \mathbf{H}' }(pk, (c^*, d^*), K^*)$ 05 return b'	GAME H_1 06 $(m^*, d^*) \xleftarrow{\$} \{0, 1\}^{n+m}$ 07 $i \xleftarrow{\$} [q_{\mathbf{H}'} + q_D]$ 08 Run $\underline{D_1^{ \mathbf{H}' , \mathbf{H}' }}(m^*, d^*)$ until the i th query $ \hat{m}\rangle$ to $ \mathbf{H}'\rangle$ 09 if $i >$ number of queries to $ \mathbf{H}'\rangle$ 10 return 0 11 else 12 $m' \leftarrow \text{MEASURE}(\hat{m}\rangle)$ 13 return $\llbracket m' = m^* \rrbracket$
$\underline{D_0^{ \mathbf{H}' , \mathbf{H}' }}(m^*, d^*, K^*)$ 14 $(pk, sk) \leftarrow \text{Gen}_1$ 15 $c^* := \text{Enc}_1(pk, m^*)$ 16 $b' \leftarrow \mathbf{B}^{\text{QDECAPS}_m^\perp, \mathbf{H}' , \mathbf{H}' }(pk, (c^*, d^*), K^*)$ 17 return b'	GAME H_0 18 $(m^*, d^*, K^*) \xleftarrow{\$} \{0, 1\}^{2n+m}$ 19 $i \xleftarrow{\$} [q_{\mathbf{H}'} + q_{\mathbf{H}'} + q_D]$ 20 Run $\underline{D_0^{ \mathbf{H}' , \mathbf{H}' }}(m^*, d^*, K^*)$ until the i th query $ \hat{m}\rangle$ to $ \mathbf{H} \times \mathbf{H}'\rangle$ 21 if $i >$ number of queries to $ \mathbf{H} \times \mathbf{H}'\rangle$ 22 return 0 23 else 24 $m' \leftarrow \text{MEASURE}(\hat{m}\rangle)$ 25 return $\llbracket m' = m^* \rrbracket$

Figure 31: Adversaries D_b and games H_b ($b \in \{0, 1\}$) for the proof of Theorem 4.5. QDECAPS_m^\perp is defined as in game G_2 , see Figure 30.

GAMES $G_{4,1}, G_{5,1}$ 01 $(m^*, d^*, K^*) \xleftarrow{\$} \{0, 1\}^{2n+m}$ 02 $i \xleftarrow{\$} [q_{\mathbf{H}'}]$ 03 $(pk, sk) \leftarrow \text{Gen}_1$ 04 $c^* := \text{Enc}_1(pk, m^*)$ 05 Run $\mathbf{B}^{\text{QDECAPS}_m^\perp, \mathbf{H}' , \mathbf{H}' }(pk, (c^*, d^*), K^*)$ until the i th query $ \hat{m}\rangle$ to $ \mathbf{H}'\rangle$ 06 if $i >$ number of queries to $ \mathbf{H}'\rangle$ 07 return 0 08 else 09 $m' \leftarrow \text{MEASURE}(\hat{m}\rangle)$ 10 return $\llbracket m' = m^* \rrbracket$	$\underline{\text{QDECAPS}_m^\perp((c, d) \neq (c^*, d^*))}$ // $G_{4,b}$ 21 if $c = c^*$ 22 return \perp 23 $m' := \text{Dec}_1(sk, c)$ 24 if $m' = m^*$ 25 ABORT 26 if $m' \neq \perp$ and $\mathbf{H}'(m') = d$ 27 return $K := \mathbf{H}(m')$ 28 else return \perp
GAMES $G_{4,0}, G_{5,0}$ 11 $(m^*, d^*, K^*) \xleftarrow{\$} \{0, 1\}^{2n+m}$ 12 $i \xleftarrow{\$} [q_{\mathbf{H}'} + q_{\mathbf{H}'}]$ 13 $(pk, sk) \leftarrow \text{Gen}_1$ 14 $c^* := \text{Enc}_1(pk, m^*)$ 15 Run $\mathbf{B}^{\text{QDECAPS}_m^\perp, \mathbf{H}' , \mathbf{H}' }(pk, (c^*, d^*), K^*)$ until the i th query $ \hat{m}\rangle$ to $ \mathbf{H} \times \mathbf{H}'\rangle$ 16 if $i >$ number of queries to $ \mathbf{H} \times \mathbf{H}'\rangle$ 17 return 0 18 else 19 $m' \leftarrow \text{MEASURE}(\hat{m}\rangle)$ 20 return $\llbracket m' = m^* \rrbracket$	$\underline{\text{QDECAPS}_m^\perp((c, d) \neq (c^*, d^*))}$ // $G_{5,b}$ 29 if $c = c^*$ 30 return \perp 31 $m' := \text{Dec}_1(sk, c)$ 32 if $m' = m^*$ 33 ABORT 34 if $\exists m \in \text{Roots}(\mathbf{H}'(X) - d)$ s.t. $\text{Dec}_1(sk, c) = m$ 35 return $K := \mathbf{H}(m)$. 36 else return \perp

Figure 32: Games $G_{4,b}$ and $G_{5,b}$ ($b \in \{0, 1\}$) for the proof of Theorem 4.5.

GAME $G_{5,b}$. In games $G_{5,b}$, the oracle QDECAPS_m^\perp is changed such that it does not make use of the secret key any longer (except for line 34 by testing if $\text{Dec}_1(sk, c) = m$ for given c and messages m). Recall that $\mathbf{H}' = \mathbf{H}(X)$ is a random polynomial of degree $2q_{\mathbf{H}'}$ over \mathbb{F}_{2^n} . Therefore, given that (c, d) is a valid encapsulation (i.e., $m' \in \mathcal{M}$ and $d = \mathbf{H}'(m')$, for $m' := \text{Dec}_1(sk, c)$), m' lies within the roots of $\mathbf{H}'(X) - d$. In order to show that QDECAPS_m^\perp returns the same output in games $G_{4,b}$ and $G_{5,b}$ for every

query $(c, d) \neq (c^*, d^*)$, we only need to consider the cases where $c \neq c^*$ and $m' := \text{Dec}_1(sk, c) \neq m^*$.

- Case 1: $\text{QDECAPS}_m^\perp(c, d)$ returns \perp in Game $G_{5,b}$, meaning that $m' \notin \text{Roots}(\mathbf{H}'(X) - d)$. That latter happens iff $\mathbf{H}'(m') \neq d$ or $m' = \perp$, which is exactly the condition that $\text{QDECAPS}_m^\perp(c, d)$ returns \perp in Game $G_{4,b}$.
- Case 2: $\text{QDECAPS}_m^\perp(c, d)$ does not return \perp in Game $G_{5,b}$, meaning that $m' \in \text{Roots}(\mathbf{H}'(X) - d)$ and $\text{Dec}_1(sk, c) = m'$. Consequently, $\mathbf{H}'(m') = d$ and $\text{QDECAPS}_m^\perp(c, d)$ returns $K = \mathbf{H}(m')$ in Games $G_{5,b}$. The latter is again exactly the condition that $\text{QDECAPS}_m^\perp(c, d)$ returns $K = \mathbf{H}(m')$ in Game $G_{4,b}$.

It is easy to verify that the equivalence of QDECAPS_m^\perp in the two games follows by negation and combining both cases. We have just shown

$$\Pr[G_{5,b}^{\text{B}} \Rightarrow 1] = \Pr[G_{4,b}^{\text{B}} \Rightarrow 1] .$$

For $b \in \{0, 1\}$, we give adversaries A_b against the OW-PCA security of PKE_1 in Figure 33, simulating games $G_{5,b}$ for B .

We stress that while both adversaries do not check whether $\text{Dec}_1(sk, c) = m^*$ during their simulation of $\text{QDECAPS}_m^\perp(c, d)$, this does not change B 's view since $G_{5,b}^{\text{B}} \Rightarrow 1$ implies that no such query exists. Hence,

$$\Pr[G_{5,b}^{\text{B}} \Rightarrow 1] = \text{Adv}_{\text{PKE}_1}^{\text{OW-PCA}}(A_b) .$$

Note that both adversaries issue at most $2q_D q_{H'}$ PCO-queries: For each query of B to QDECAPS_m^\perp on $(c \neq c^*, d)$, both A_0 and A_1 compute the set $\text{Roots}(\mathbf{H}'(X) - d)$ of complex roots, which has $2q_{H'} - 1$ elements since $\mathbf{H}'(X) - d$ is a polynomial of degree $2q_{H'} - 1$. In the worst case, they need to check for every element m' of $\text{Roots}(\mathbf{H}'(X) - d)$ whether $\text{PCO}(m', c) = 1$.

$A_1^{\text{PCO}}(pk, c^*)$	$A_0^{\text{PCO}}(pk, c^*)$
01 $(d^*, K^*) \xleftarrow{\$} \{0, 1\}^{n+m}$	09 $(d^*, K^*) \xleftarrow{\$} \{0, 1\}^{n+m}$
02 $i \xleftarrow{\$} [q_{H'}]$	10 $i \xleftarrow{\$} [q_{H'} + q_{H'}]$
03 Run $B^{\text{QDECAPS}_m^\perp, \mathbf{H}' , \mathbf{H}' }(pk, (c^*, d^*), K^*)$ until the i th query $ \hat{m}\rangle$ to $ \mathbf{H}'\rangle$	11 Run $B^{\text{QDECAPS}_m^\perp, \mathbf{H}' , \mathbf{H}' }(pk, (c^*, d^*), K^*)$ until the i th query $ \hat{m}\rangle$ to $ \mathbf{H} \times \mathbf{H}'\rangle$
04 if $i >$ number of queries to $ \mathbf{H}'\rangle$	12 if $i >$ number of queries to $ \mathbf{H} \times \mathbf{H}'\rangle$
05 return \perp	13 return 0
06 else	14 else
07 $m' \leftarrow \text{MEASURE}(\hat{m}\rangle)$	15 $m' \leftarrow \text{MEASURE}(\hat{m}\rangle)$
08 return m'	16 return m'
<hr/>	
$\text{QDECAPS}_m^\perp((c, d) \neq (c^*, d^*))$	
17 if $c = c^*$	
18 return \perp	
19 if $\exists m \in \text{Roots}(\mathbf{H}'(X) - d)$ s.t. $\text{PCO}(m, c) = 1$	
20 return $K := \mathbf{H}(m)$.	
21 else return \perp	

Figure 33: Adversaries A_b ($b \in \{0, 1\}$) against OW-PCA for the proof of Theorem 4.5.

Collecting the probabilities and folding adversaries A_0 and A_1 into one single adversary A proves the theorem. \square

4.3.2 Transformation QU_m^\perp : from OW-PCA to IND-CCA in the QROM

QU_m^\perp transforms an OW-PCA secure public-key encryption scheme into an IND-CCA secure key encapsulation mechanism with implicit rejection.

THE CONSTRUCTION. To a public-key encryption scheme $\text{PKE}_1 = (\text{Gen}_1, \text{Enc}_1, \text{Dec}_1)$ with message space $\mathcal{M} = \{0, 1\}^n$, and hash functions $\mathbf{H} : \{0, 1\}^* \rightarrow \{0, 1\}^n$ and $\mathbf{H}' : \{0, 1\}^n \rightarrow \{0, 1\}^n$, we associate $\text{QKEM}_m^\perp = \text{QU}_m^\perp[\text{PKE}_1, \mathbf{H}, \mathbf{H}'] = (\text{QGen} := \text{Gen}^\perp, \text{QEncaps}_m, \text{QDecaps}_m^\perp)$. Algorithm Gen^\perp is given in

Figure 12 and the remaining algorithms of QKEM_m^χ are defined in Figure 34. We stress again that hash function H' has matching domain and range.

$\text{QEncaps}_m(pk)$	$\text{QDecaps}_m^\chi(sk' = (sk, s), c, d)$
01 $m \xleftarrow{\$} \mathcal{M}$	06 $m' := \text{Dec}_1(sk, c)$
02 $c \leftarrow \text{Enc}_1(pk, m)$	07 if $m' = \perp$ or $H'(m') \neq d$
03 $d := H'(m)$	08 return $K := H(s, c, d)$
04 $K := H(m)$	09 else return $K := H(m')$
05 return (K, c, d)	

Figure 34: IND-CCA-secure key encapsulation mechanism $\text{QKEM}_m^\chi = \text{QU}_m^\chi[\text{PKE}_1, H, H']$.

SECURITY. The following theorem establishes that IND-CCA security of QKEM_m^χ reduces to the OW-PCA security of PKE_1 , in the quantum random oracle model.

Theorem 4.6 (PKE_1 OW-PCA $\stackrel{\text{QROM}}{\Rightarrow} \text{QKEM}_m^\chi$ IND-CCA). *If PKE_1 is δ_1 -correct, so is QKEM_m^χ . Furthermore, assume PKE_1 to be rigid. For any IND-CCA quantum adversary B issuing at most q_D (classical) queries to the decapsulation oracle QDECAPS_m^χ , at most q_H queries to the quantum random oracle $|H\rangle$ and at most $q_{H'}$ queries to the quantum random oracle $|H'\rangle$, there exists an OW-PCA quantum adversary A issuing $2q_D q_{H'}$ queries to oracle PCO such that*

$$\text{Adv}_{\text{QKEM}_m^\chi}^{\text{IND-CCA}}(B) \leq (2q_{H'} + q_H + 2q_D) \cdot \sqrt{\text{Adv}_{\text{PKE}_1}^{\text{OW-PCA}}(A) + \delta_1},$$

and the running time of A is about that of B .

The proof is almost the same as the one of Theorem 4.5. The crucial observation is that in all games of the proof of Theorem 4.5, the simulation of QDECAPS_m^χ always knows if a given ciphertext (c, d) is valid or not. If it is not valid, it returns \perp . So for the proof of Theorem 4.6 one can simply replace \perp by $H(s, c, d)$. (The difference to the proof of Theorem 3.3 is the value d in the ciphertext that throughout the proof helps with the recognition of invalid ciphertexts.)

4.4 The resulting KEMs

For concreteness, we combine transformations T and $\{\text{QU}_m^\perp, \text{QU}_m^\chi\}$ from the previous sections to obtain $\text{QFO}_m^\perp = T \circ \text{QU}_m^\perp$ and $\text{QFO}_m^\chi = T \circ \text{QU}_m^\chi$. To a public-key encryption scheme $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M} = \{0, 1\}^n$ and randomness space \mathcal{R} , and hash functions $G : \mathcal{M} \rightarrow \mathcal{R}$, $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ and $H' : \{0, 1\}^n \rightarrow \{0, 1\}^n$, we associate

$$\begin{aligned} \text{QKEM}_m^\perp &= \text{QFO}_m^\perp[\text{PKE}, G, H, H'] := \text{QU}_m^\perp[T[\text{PKE}, G], H, H'] = (\text{Gen}, \text{QEncaps}_m, \text{QDecaps}_m^\perp) \\ \text{QKEM}_m^\chi &= \text{QFO}_m^\chi[\text{PKE}, G, H, H'] := \text{QU}_m^\chi[T[\text{PKE}, G], H, H'] = (\text{Gen}^\chi, \text{QEncaps}_m, \text{QDecaps}_m^\chi). \end{aligned}$$

Algorithm Gen^χ is given in Figure 12 and the remaining algorithms are given in Figure 35.

The following table provides (simplified) concrete bounds of the IND-CCA security of $\text{KEM} \in \{\text{QKEM}_m^\chi, \text{QKEM}_m^\perp\}$ in the quantum random oracle model, directly obtained by combining Theorems 4.4–4.6. Here $q_{\text{RO}} := q_G + q_H + q_{H'}$ counts the total number of (implicit and explicit) queries to the quantum random oracles G , H and H' .

KEM	Concrete bound on $\text{Adv}_{\text{KEM}}^{\text{IND-CCA}}(B) \leq$
$\text{QKEM}_m^\chi, \text{QKEM}_m^\perp$	$8q_{\text{RO}} \left(\sqrt{q_{\text{RO}}^2 \cdot \delta + q_{\text{RO}} \cdot \sqrt{\text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(A) + q_{\text{RO}} \cdot \delta}} \right)$

<p>QEncaps_m(pk)</p> 01 $m \xleftarrow{\$} \mathcal{M}$ 02 $c := \text{Enc}(pk, m; \mathbf{G}(m))$ 03 $K := \mathbf{H}(m)$ 04 $d := \mathbf{H}'(m)$ 05 return (K, c, d)	<p>QDecaps_m[⊥](sk, c, d)</p> 06 $m' := \text{Dec}(sk, c)$ 07 if $c = \text{Enc}(pk, m'; \mathbf{G}(m'))$ and $\mathbf{H}'(m') = d$ 08 return $K := \mathbf{H}(m')$ 09 else return \perp <p>QDecaps_m[≠](sk' = (sk, s), c, d)</p> 10 $m' := \text{Dec}(sk, c)$ 11 if $c = \text{Enc}(pk, m'; \mathbf{G}(m'))$ and $\mathbf{H}'(m') = d$ 12 return $K := \mathbf{H}(m')$ 13 else return $K := \mathbf{H}(s, c, d)$
---	---

Figure 35: IND-CCA secure QKEM_m^\perp and QKEM_m^\neq obtained from PKE.

Acknowledgments

We would like to thank Andreas Hülsing, Christian Schaffner, and Dominique Unruh for interesting discussions on the FO transformation in the QROM. We are also grateful to Krzysztof Pietrzak and Victor Shoup for discussions on Section 3.4. The first author was supported in part by ERC project PREP-CRYPTO (FP7/724307) and by DFG grants HO4534/4-1 and HO4534/2-2. The second author was supported by DFG RTG 1817/1 UbiCrypt. The third author was supported in part by ERC Project ERCC (FP7/615074) and by DFG SPP 1736 Big Data.

References

- [ABR01] Michel Abdalla, Mihir Bellare, and Phillip Rogaway. The oracle Diffie-Hellman assumptions and an analysis of DHIES. In David Naccache, editor, *CT-RSA 2001*, volume 2020 of *LNCS*, pages 143–158. Springer, Heidelberg, April 2001. (Cited on page 2, 6, 7.)
- [ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - A new hope. In *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 327–343, 2016. (Cited on page 3.)
- [AOP⁺17] Martin R. Albrecht, Emmanuela Orsini, Kenneth G. Paterson, Guy Peer, and Nigel P. Smart. Tightly secure ring-lwe based key encapsulation with short ciphertexts. *Cryptology ePrint Archive*, Report 2017/354, 2017. <http://eprint.iacr.org/2017/354>. (Cited on page 7.)
- [BBC⁺98] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. In *39th FOCS*, pages 352–361. IEEE Computer Society Press, November 1998. (Cited on page 25.)
- [BBO07] Mihir Bellare, Alexandra Boldyreva, and Adam O’Neill. Deterministic and efficiently searchable encryption. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 535–552. Springer, Heidelberg, August 2007. (Cited on page 4.)
- [BCD⁺16] Joppe W. Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *ACM CCS 16*, pages 1006–1018. ACM Press, October 2016. (Cited on page 3.)
- [BCLvV16] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. Ntru prime. *Cryptology ePrint Archive*, Report 2016/461, 2016. <http://eprint.iacr.org/2016/461>. (Cited on page 3.)
- [BCNS15] Joppe W. Bos, Craig Costello, Michael Naehrig, and Douglas Stebila. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In *2015 IEEE*

- Symposium on Security and Privacy*, pages 553–570. IEEE Computer Society Press, May 2015. doi:10.1109/SP.2015.40. (Cited on page 3.)
- [BDF⁺11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Heidelberg, December 2011. (Cited on page 3, 25.)
- [BDK⁺17] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, and Damien Stehlé. Crystals – kyber: a cca-secure module-lattice-based kem. Cryptology ePrint Archive, Report 2017/634, 2017. <http://eprint.iacr.org/2017/634>. (Cited on page 3.)
- [BHSV98] Mihir Bellare, Shai Halevi, Amit Sahai, and Salil P. Vadhan. Many-to-one trapdoor functions and their relation to public-key cryptosystems. In Hugo Krawczyk, editor, *CRYPTO’98*, volume 1462 of *LNCS*, pages 283–298. Springer, Heidelberg, August 1998. (Cited on page 4.)
- [BLK00] Joonsang Baek, Byoungcheon Lee, and Kwangjo Kim. Secure length-saving ElGamal encryption under the computational Diffie-Hellman assumption. In Ed Dawson, Andrew Clark, and Colin Boyd, editors, *ACISP 00*, volume 1841 of *LNCS*, pages 49–58. Springer, Heidelberg, July 2000. doi:10.1007/10718964_5. (Cited on page 6.)
- [BP18] Daniel J. Bernstein and Edoardo Persichetti. Towards kem unification, 2018. <https://cr.y.p.to/papers/tightkem-20180528.pdf>. (Cited on page 1, 8.)
- [BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In V. Ashby, editor, *ACM CCS 93*, pages 62–73. ACM Press, November 1993. (Cited on page 2.)
- [BR06] Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 409–426. Springer, Heidelberg, May / June 2006. (Cited on page 7.)
- [CHJ⁺02] Jean-Sébastien Coron, Helena Handschuh, Marc Joye, Pascal Paillier, David Pointcheval, and Christophe Tymen. GEM: A generic chosen-ciphertext secure encryption method. In Bart Preneel, editor, *CT-RSA 2002*, volume 2271 of *LNCS*, pages 263–276. Springer, Heidelberg, February 2002. (Cited on page 2, 6, 7.)
- [CKLS16] Jung Hee Cheon, Duhyeong Kim, Joohee Lee, and Yongsoo Song. Lizard: Cut off the tail! practical post-quantum public-key encryption from lwe and lwr. Cryptology ePrint Archive, Report 2016/1126, 2016. <http://eprint.iacr.org/2016/1126>. (Cited on page 3.)
- [CKS08] David Cash, Eike Kiltz, and Victor Shoup. The twin Diffie-Hellman problem and applications. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 127–145. Springer, Heidelberg, April 2008. (Cited on page 7.)
- [CKS09] David Cash, Eike Kiltz, and Victor Shoup. The twin Diffie-Hellman problem and applications. *Journal of Cryptology*, 22(4):470–504, October 2009. (Cited on page 7.)
- [CS03] Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM Journal on Computing*, 33(1):167–226, 2003. (Cited on page 3.)
- [Den03] Alexander W. Dent. A designer’s guide to KEMs. In Kenneth G. Paterson, editor, *9th IMA International Conference on Cryptography and Coding*, volume 2898 of *LNCS*, pages 133–151. Springer, Heidelberg, December 2003. (Cited on page 2, 5, 6, 7.)
- [DNR04] Cynthia Dwork, Moni Naor, and Omer Reingold. Immunizing encryption schemes from decryption errors. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 342–360. Springer, Heidelberg, May 2004. (Cited on page 6, 8.)

- [DXL12] Jintai Ding, Xiang Xie, and Xiaodong Lin. A simple provably secure key exchange scheme based on the learning with errors problem. Cryptology ePrint Archive, Report 2012/688, 2012. <http://eprint.iacr.org/2012/688>. (Cited on page 3.)
- [FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 537–554. Springer, Heidelberg, August 1999. (Cited on page 2, 3, 6.)
- [FO13] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *Journal of Cryptology*, 26(1):80–101, January 2013. doi:10.1007/s00145-011-9114-1. (Cited on page 2, 3, 8.)
- [GMMV05] David Galindo, Sebastià Martín, Paz Morillo, and Jorge L. Villar. Fujisaki-okamoto hybrid encryption revisited. *Int. J. Inf. Sec.*, 4(4):228–241, 2005. (Cited on page 6.)
- [HGSW05] Nick Howgrave-Graham, Joseph H. Silverman, and William Whyte. Choosing parameter sets forwithand. In Alfred Menezes, editor, *CT-RSA 2005*, volume 3376 of *LNCS*, pages 118–135. Springer, Heidelberg, February 2005. (Cited on page 3.)
- [Höv21] Kathrin Hövelmanns. *Generic constructions of quantum-resistant cryptosystems*. PhD thesis, 2021. URL: <http://hss-opus.ub.ruhr-unibochum.de/opus4/frontdoor/index/index/docId/7758>, doi:10.13154/294-7758. (Cited on page 1.)
- [HRS16] Andreas Hülsing, Joost Rijneveld, and Fang Song. Mitigating multi-target attacks in hash-based signatures. In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *PKC 2016, Part I*, volume 9614 of *LNCS*, pages 387–416. Springer, Heidelberg, March 2016. doi:10.1007/978-3-662-49384-7_15. (Cited on page 27.)
- [KLS17] Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of fiat-shamir signatures in the quantum random-oracle model. Manuscript, 2017. (Cited on page 27.)
- [KML03] Eike Kiltz and John Malone-Lee. A general construction of IND-CCA2 secure public key encryption. In Kenneth G. Paterson, editor, *9th IMA International Conference on Cryptography and Coding*, volume 2898 of *LNCS*, pages 152–166. Springer, Heidelberg, December 2003. (Cited on page 6.)
- [LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, Heidelberg, May 2010. (Cited on page 7.)
- [LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-LWE cryptography. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 35–54. Springer, Heidelberg, May 2013. doi:10.1007/978-3-642-38348-9_3. (Cited on page 6.)
- [NIS17] NIST. National institute for standards and technology. postquantum crypto project, 2017. <http://csrc.nist.gov/groups/ST/post-quantum-crypto/>. (Cited on page 3.)
- [OP01] Tatsuaki Okamoto and David Pointcheval. REACT: Rapid Enhanced-security Asymmetric Cryptosystem Transform. In David Naccache, editor, *CT-RSA 2001*, volume 2020 of *LNCS*, pages 159–175. Springer, Heidelberg, April 2001. (Cited on page 2, 6, 7.)
- [Pei14] Chris Peikert. Lattice cryptography for the internet. Cryptology ePrint Archive, Report 2014/070, 2014. <http://eprint.iacr.org/2014/070>. (Cited on page 3.)
- [Per12] Edoardo Persichetti. *Improving the efficiency of code-based cryptography*. PhD thesis, 2012. URL: <http://persichetti.webs.com/Thesis%20Final.pdf>. (Cited on page 5.)
- [Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005. (Cited on page 6.)

- [RS92] Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 433–444. Springer, Heidelberg, August 1992. (Cited on page 2.)
- [Sho04a] Victor Shoup. ISO 18033-2: An emerging standard for public-key encryption. <http://shoup.net/iso/std6.pdf>, December 2004. Final Committee Draft. (Cited on page 6.)
- [Sho04b] Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. Cryptology ePrint Archive, Report 2004/332, 2004. <http://eprint.iacr.org/2004/332>. (Cited on page 7, 12.)
- [TU16] Ehsan Ebrahimi Targhi and Dominique Unruh. Post-quantum security of the fujisaki-okamoto and OAEP transforms. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B, Part II*, volume 9986 of *LNCS*, pages 192–216. Springer, Heidelberg, October / November 2016. [doi:10.1007/978-3-662-53644-5_8](https://doi.org/10.1007/978-3-662-53644-5_8). (Cited on page 3, 5, 6, 28, 30.)
- [Unr14] Dominique Unruh. Revocable quantum timed-release encryption. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 129–146. Springer, Heidelberg, May 2014. [doi:10.1007/978-3-642-55220-5_8](https://doi.org/10.1007/978-3-642-55220-5_8). (Cited on page 26.)
- [Unr15] Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 755–784. Springer, Heidelberg, April 2015. [doi:10.1007/978-3-662-46803-6_25](https://doi.org/10.1007/978-3-662-46803-6_25). (Cited on page 5.)
- [Zha12a] Mark Zhandry. How to construct quantum random functions. In *53rd FOCS*, pages 679–687. IEEE Computer Society Press, October 2012. (Cited on page 27.)
- [Zha12b] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, Heidelberg, August 2012. (Cited on page 26.)