A Modular Analysis of the Fujisaki-Okamoto Transformation

Dennis Hofheinz[1], Kathrin Hövelmanns[2(✉)], and Eike Kiltz[2]

[1] Karlsruhe Institute of Technology, Karlsruhe, Germany
Dennis.Hofheinz@kit.edu
[2] Ruhr Universität Bochum, Bochum, Germany
{Kathrin.Hoevelmanns,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

1 Introduction

The notion of INDistinguishability against Chosen-Ciphertext Attacks (IND-CCA) [34] 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.

Y. Kalai and L. Reyzin (Eds.): TCC 2017, Part I, LNCS 10677, pp. 341–371, 2017.
https://doi.org/10.1007/978-3-319-70500-2_12

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 [23,24] 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 [7]. Subsequently, Okamoto and Pointcheval [32] and Coron et al. [18] 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 $\textsc{Pco}(c, m)$ 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. [1].

KEMs. In his "A Designer's Guide to KEMs" paper, Dent [20] provides "more modern" versions of the FO [20, Table 5] and the REACT/GEM [20, 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 [19]. 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 [23], 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 [31] 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 resists 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 [11]. Targhi and Unruh recently proved a variant of the FO transformation secure in the quantum random oracle model [38]. 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 [23,24] 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 [33], due to their decision/search equivalence, many natural lattice-based encryption scheme 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 [21], Peikert [33], BCNS [14], New Hope [3], Frodo [13], Lizard [17], and Kyber [12].[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

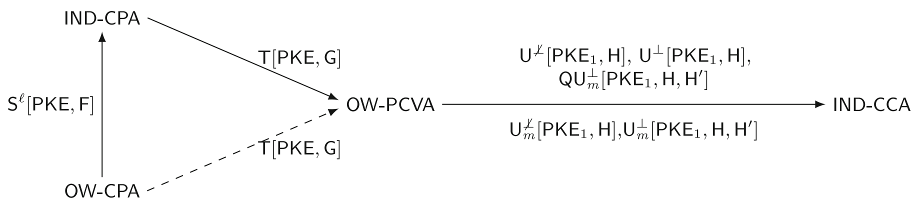
Our main contribution is a modular treatment of FO-like transformations. That is, we provide fine-grained transformations that can be used to turn an OW-CPA secure PKE scheme into an IND-CCA secure one in several steps. For instance, we provide separate OW-CPA $\rightarrow$ OW-PCA and OW-PCA $\rightarrow$ 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. All of our individual transformations are

[1] Lattice-based encryption schemes can be made perfectly correctness by putting a limit on the noise and setting the modulus of the LWE instance large enough, see e.g. [9,27]. 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.

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 $\mathsf{U}^{\not\perp}$, we can show that the original FO transformation yields $\mathsf{IND\text{-}CCA}$ security from $\mathsf{IND\text{-}CPA}$ security with a *tight* security reduction. Combining S^{ℓ} with T and $\mathsf{U}^{\not\perp}$, on the other hand, yields tight $\mathsf{IND\text{-}CCA}$ security from the weaker notion of $\mathsf{OW\text{-}CPA}$ security, at the expense of a larger ciphertext. (See Fig. 1 for an overview.)

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.



Transformation	Security implication	QROM?	ROM Tightness?	Requirements
$\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ (§3.1)	OW-CPA ⇒ OW-PCA	✓	—	none
$\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ (§3.1)	IND-CPA ⇒ OW-PCA	✓	✓	none
$\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ (§3.1)	OW-CPA ⇒ OW-PCVA	✓	—	γ-spread
$\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ (§3.1)	IND-CPA ⇒ OW-PCVA	—	✓	γ-spread
$\mathsf{KEM}^{\not\perp} = \mathsf{U}^{\not\perp}[\mathsf{PKE}_1, \mathsf{H}]$ (§3.2)	OW-PCA ⇒ IND-CCA	—	✓	none
$\mathsf{KEM}^{\perp} = \mathsf{U}^{\perp}[\mathsf{PKE}_1, \mathsf{H}]$ (§3.2)	OW-PCVA ⇒ IND-CCA	—	✓	none
$\mathsf{KEM}_m^{\not\perp} = \mathsf{U}_m^{\not\perp}[\mathsf{PKE}_1, \mathsf{H}]$ (§3.2)	OW-CPA ⇒ IND-CCA	—	✓	det. PKE_1
$\mathsf{KEM}_m^{\perp} = \mathsf{U}_m^{\perp}[\mathsf{PKE}_1, \mathsf{H}]$ (§3.2)	OW-VA ⇒ IND-CCA	—	✓	det. PKE_1
$\mathsf{QKEM}_m^{\perp} = \mathsf{QU}_m^{\perp}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$ (§4.3)	OW-PCA ⇒ IND-CCA	✓	✓	none
$\mathsf{PKE}_{\ell} = \mathsf{S}^{\ell}[\mathsf{PKE}, \mathsf{F}]$ (§3.4)	OW-CPA ⇒ IND-PCA	—	✓	none

Fig. 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.

T: FROM $\mathsf{OW\text{-}CPA}$ TO $\mathsf{OW\text{-}PCA}$ SECURITY ("DERANDOMIZATION" + "RE-ENCRYPTION"). T is the Encrypt-with-Hash construction from [6]: Starting from an encryption scheme PKE and a hash function G, we build a deterministic encryption scheme $\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ by defining

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

where $\mathsf{G}(m)$ is used as the random coins for Enc. Note that Enc_1 is deterministic. $\mathsf{Dec}_1(sk, c)$ first decrypts c into m' and rejects if $\mathsf{Enc}(pk, m'; \mathsf{G}(m') \neq c$ ("re-encryption"). Modeling G as a random oracle, $\mathsf{OW\text{-}PCA}$ security of PKE_1 non-tightly reduces to $\mathsf{OW\text{-}CPA}$ security of PKE and tightly reduces to $\mathsf{IND\text{-}CPA}$ security of PKE. If PKE furthermore is γ-spread (for sufficiently large γ), then PKE_1 is even $\mathsf{OW\text{-}PCVA}$ secure. $\mathsf{OW\text{-}PCVA}$ security[2] 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 1).

$\mathsf{U}^{\not\perp}$ ($\mathsf{U}^{\perp}$): FROM $\mathsf{OW\text{-}PCA}$ ($\mathsf{OW\text{-}PCVA}$) TO $\mathsf{IND\text{-}CCA}$ SECURITY ("HASHING"). Starting from an encryption scheme PKE_1 and a hash function H, we build a key encapsulation mechanism $\mathsf{KEM}^{\not\perp} = \mathsf{U}^{\not\perp}[\mathsf{PKE}_1, \mathsf{H}]$ with "implicit rejection" by defining

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

where m is picked at random from the message space.

$$\mathsf{Decaps}^{\not\perp}(sk, c) = \begin{cases} \mathsf{H}(c, m) & m \neq \perp \\ \mathsf{H}(c, s) & m = \perp \end{cases}, \tag{2}$$

where $m := \mathsf{Dec}(sk, c)$ and s is a random seed which is contained in sk. Modeling H as a random oracle, $\mathsf{IND\text{-}CCA}$ security of $\mathsf{KEM}^{\not\perp}$ tightly reduces to $\mathsf{OW\text{-}PCA}$ security of PKE_1.

We also define $\mathsf{KEM}^{\perp} = \mathsf{U}^{\perp}[\mathsf{PKE}_1, \mathsf{H}]$ with "explicit rejection" which differs from $\mathsf{KEM}^{\not\perp}$ only in decapsulation:

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

where $m := \mathsf{Dec}(sk, c)$. Modeling H as a random oracle, $\mathsf{IND\text{-}CCA}$ of $\mathsf{KEM}^{\perp}$ security tightly reduces to $\mathsf{OW\text{-}PCVA}$ security of PKE_1. We remark that transformation $\mathsf{U}^{\perp}$ is essentially [20, Table 2], i.e., a KEM variant of the REACT/GEM transformations.

$\mathsf{U}^{\not\perp}_m$ ($\mathsf{U}^{\perp}_m$): FROM DETERMINISTIC $\mathsf{OW\text{-}CPA}$ ($\mathsf{OW\text{-}VA}$) TO $\mathsf{IND\text{-}CCA}$ SECURITY ("HASHING"). We consider two more variants of $\mathsf{U}^{\not\perp}$ and $\mathsf{U}^{\perp}$, namely $\mathsf{U}^{\not\perp}_m$ and $\mathsf{U}^{\perp}_m$. Transformation $\mathsf{U}^{\not\perp}_m$ ($\mathsf{U}^{\perp}_m$) is a variant of $\mathsf{U}^{\not\perp}$ ($\mathsf{U}^{\perp}$), where $K = \mathsf{H}(c, m)$ from Eqs. (1)–(3) is replaced by $K = \mathsf{H}(m)$. We prove that $\mathsf{IND\text{-}CCA}$ security of $\mathsf{KEM}^{\not\perp}_m := \mathsf{U}^{\not\perp}_m[\mathsf{PKE}_1, \mathsf{H}]$ ($\mathsf{KEM}^{\perp}_m := \mathsf{U}^{\perp}_m[\mathsf{PKE}_1, \mathsf{H}]$) in the random oracle model tightly reduces to $\mathsf{IND\text{-}CPA}$ ($\mathsf{IND\text{-}VA}$[3]) security of PKE_1, if encryption of PKE_1 is deterministic.

[2] $\mathsf{OW\text{-}PCVA}$ security is called $\mathsf{OW\text{-}CPA}^+$ security with access to a PCO oracle in [20].

[3] $\mathsf{OW\text{-}VA}$ security is $\mathsf{OW\text{-}CPA}$ security, where the adversary is given access to a validity oracle $\text{Cvo}(c)$ that checks c's validity (cf. Definition 1).

$\mathsf{QU}_m^{\perp}$: 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 $\mathsf{QKEM}_m^{\perp} = \mathsf{QU}_m^{\perp}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$ with explicit rejection by defining

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

where m is picked at random from the message space.

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

where $m' := \mathsf{Dec}(sk, c)$. $\mathsf{QU}_m^{\perp}$ differs from $\mathsf{U}^{\not\perp}$ only in the additional hash value $d = \mathsf{H}'(m)$ from the ciphertext and H' is a random oracle with matching domain and image. This trick was introduced in [40] and used in [38] 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.

The Resulting FO Transformations. Our final transformations $\mathsf{FO}^{\not\perp}$ ("FO with implicit rejection"), $\mathsf{FO}^{\perp}$ ("FO with explicit rejection"), $\mathsf{FO}_m^{\not\perp}$ ("FO with implicit rejection, $K = \mathsf{H}(m)$"), $\mathsf{FO}_m^{\perp}$ ("FO with explicit rejection, $K = \mathsf{H}(m)$"), and $\mathsf{QFO}_m^{\perp}$ ("Quantum FO with explicit rejection, $K = \mathsf{H}(m)$") are defined in the following table.

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

As corollaries of our modular transformation we obtain that IND-CCA security of $\mathsf{FO}^{\not\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}]$, $\mathsf{FO}^{\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}]$, $\mathsf{FO}_m^{\not\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}]$, and $\mathsf{FO}_m^{\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}]$ 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 $\mathsf{FO}_m^{\perp}$ essentially recovers a KEM variant [20, Table 5] of the original FO transformation [23]. Whereas the explicit rejection variants $\mathsf{FO}^{\perp}$ and $\mathsf{FO}_m^{\perp}$ require PKE to be γ-spread, there is no such requirement on $\mathsf{FO}^{\not\perp}$ and $\mathsf{FO}_m^{\not\perp}$. Further, IND-CCA security of $\mathsf{QFO}_m^{\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}, \mathsf{H}']$ reduces to the OW-CPA security of PKE, in the quantum random oracle model. Our transformation $\mathsf{QFO}_m^{\perp}$ essentially recovers a KEM variant of the modified FO transformation by Targhi and Unruh [38]. 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 Sect. 2.1) derives from the ones previously given in the literature (e.g. [10,22]). The concrete bounds of $\mathsf{FO}^{\not\perp}$, $\mathsf{FO}^{\perp}$, $\mathsf{FO}^{\not\perp}_m$, and $\mathsf{FO}^{\perp}_m$ give guidance on the required correctness error of the underlying PKE scheme. Concretely, for "κ bits security", PKE requires a correctness error of $2^{-\kappa}$.

Example Instantiations. In the context of ElGamal encryption one can apply $\{\mathsf{FO}^{\not\perp}, \mathsf{FO}^{\perp}, \mathsf{FO}^{\not\perp}_m, \mathsf{FO}^{\perp}_m\}$ to obtain the schemes of [4,25,28] whose $\mathsf{IND\text{-}CCA}$ security non-tightly reduces to the CDH assumption, and tightly reduces to the DDH assumption. Alternatively, one can directly use $\mathsf{U}^{\not\perp}/\mathsf{U}^{\perp}$ to obtain the more efficient schemes of [1,18,32,36] whose $\mathsf{IND\text{-}CCA}$ 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 $\mathsf{U}^{\not\perp}/\mathsf{U}^{\perp}$ to obtain schemes mentioned in [20,36] whose $\mathsf{IND\text{-}CCA}$ security tightly reduces to one-way security. Finally, in the context of lattices-based encryption (e.g., [30,35]), one can apply $\mathsf{FO}^{\not\perp}$, $\mathsf{FO}^{\perp}$, $\mathsf{FO}^{\not\perp}_m$, $\mathsf{FO}^{\perp}_m$, and $\mathsf{QFO}^{\perp}_m$ to achieve $\mathsf{IND\text{-}CCA}$ security.

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

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

The reduction (to the $\mathsf{OW\text{-}CPA}$ security of PKE) loses a factor of $q_{\mathsf{G}}^{1/\ell}$, 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 $\mathsf{G}(x_1, \ldots, x_n)$, which requires to find all x_i. The reduction can use this observation to embed an $\mathsf{OW\text{-}CPA}$ challenge as one $\mathsf{Enc}(pk, x_{i^*})$ and hope to learn x_{i^*} from the G-queries of a successful $\mathsf{IND\text{-}CPA}$ 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 $(x_1, \ldots, x_{\ell})$ (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, $\mathsf{FO}^{\perp}_m = \mathsf{U}^{\perp}_m \circ \mathsf{T}$ is essentially a KEM variant of the Fujisaki-Okamoto transform from [20, Table 5]. Further, $\mathsf{U}^{\perp}$ is a KEM variant

[20] of the GEM/REACT transform [1,18,32]. 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 [15,16] 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, [2] considers the IND-CCA security of LIMA which in our notation can be described as $\mathsf{FO}_m^{\perp}[\mathsf{RLWE}, \mathsf{G}, \mathsf{H}]$. Here RLWE is a specific encryption scheme based on lattices associated to polynomial rings from [29], which is IND-CPA secure under the Ring-LWE assumption. As the main result, [2] 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 $\mathsf{FO}_m^{\perp}$. We note that the security reduction of [2] 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 $\mathfrak{D}$ by $x \leftarrow \mathfrak{D}$. For a polynomial $p(X)$ with integer coefficients, we denote by $\mathsf{Roots}(p)$ the (finite) set of (complex) roots of p. By $[\![B]\!]$ 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 $\mathsf{H} : \mathfrak{D}_{\mathsf{H}} \to \mathfrak{I}(\mathsf{H})$ as random oracles. To keep record of the queries issued to H, we will use a hash list $\mathfrak{L}_{\mathsf{H}}$ that contains all tuples $(x, \mathsf{H}(x))$ of arguments $x \in \mathfrak{D}_{\mathsf{H}}$ that H was queried on and the respective answers $\mathsf{H}(x)$. We make the convention that $\mathsf{H}(x) = \perp$ for all $x \notin \mathfrak{D}_{\mathsf{H}}$.

Games. Following [8,37], 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 $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ 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 $c \leftarrow \mathsf{Enc}(pk, m)$ of m under the public key pk. If necessary, we make the used randomness of encryption explicit by writing $c := \mathsf{Enc}(pk, m; r)$, 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 $m = \mathsf{Dec}(sk, c) \in \mathcal{M}$ or a special symbol $\perp \notin \mathcal{M}$ to indicate that c is not a valid ciphertext.

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

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

where the expectation is taken over $(pk, sk) \leftarrow \mathsf{Gen}$. Equivalently, δ-correctness means that for all (possibly unbounded) adversaries A, $\Pr[\mathsf{COR}^{\mathsf{A}}_{\mathsf{PKE}} \Rightarrow 1] \leq \delta$, where the correctness game COR is defined as in Fig. 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. [10,22]) 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 $\mathsf{PKE} = \mathsf{PKE}^{\mathsf{G}}$ 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 $\delta(q_{\mathsf{G}})$-*correct* if for all (possibly unbounded) adversaries A making at most q_{G} queries to random oracle G, $\Pr[\mathsf{COR\text{-}RO}^{\mathsf{A}}_{\mathsf{PKE}} \Rightarrow 1] \leq \delta(q_{\mathsf{G}})$, where the correctness game $\mathsf{COR\text{-}RO}$ is defined as in Fig. 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 $\delta(q_{\mathsf{G}})$ is a constant.

Min-Entropy. [24] For $(pk, sk) \leftarrow \mathsf{Gen}$ and $m \in \mathcal{M}$, we define the *min-entropy* of $\mathsf{Enc}(pk, m)$ by $\gamma(pk, m) := -\log \max_{c \in \mathcal{C}} \Pr_{r \leftarrow \mathcal{R}}[c = \mathsf{Enc}(pk, m; r)]$. We say that PKE is γ-*spread* if, for every key pair $(pk, sk) \leftarrow \mathsf{Gen}$ and every message $m \in \mathcal{M}$, $\gamma(pk, m) \geq \gamma$. In particular, this implies that for every possible ciphertext $c \in \mathcal{C}$, $\Pr_{r \leftarrow \mathcal{R}}[c = \mathsf{Enc}(pk, m; r)] \leq 2^{-\gamma}$.

Security. We now define three security notions for public-key encryption: One-Wayness under Chosen Plaintext Attacks ($\mathsf{OW\text{-}CPA}$), One-Wayness under

[4] For an example why the number of random oracle queries matters in the context of correctness, we refer to Theorem 1.

GAME COR:	**GAME** COR-RO:
$(pk, sk) \leftarrow \mathsf{Gen}$	$(pk, sk) \leftarrow \mathsf{Gen}$
$m \leftarrow \mathsf{A}(sk, pk)$	$m \leftarrow \mathsf{A}^{\mathsf{G}(\cdot)}(sk, pk)$
$c \leftarrow \mathsf{Enc}(pk, m)$	$c \leftarrow \mathsf{Enc}(pk, m)$
return $[\![\mathsf{Dec}(sk, c) = m]\!]$	**return** $[\![\mathsf{Dec}(sk, c) = m]\!]$

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

GAME OW-ATK:	$\textsc{Pco}(m \in \mathcal{M}, c)$
$(pk, sk) \leftarrow \mathsf{Gen}$	**return** $[\![\mathsf{Dec}(sk, c) = m]\!]$
$m^* \xleftarrow{\$} \mathcal{M}$	
$c^* \leftarrow \mathsf{Enc}(pk, m^*)$	$\textsc{Cvo}(c \neq c^*)$
$m' \leftarrow \mathsf{A}^{\mathrm{O}_{\mathsf{ATK}}}(pk, c)$	$m := \mathsf{Dec}(sk, c)$
return $\textsc{Pco}(m', c^*)$	**return** $[\![m \in \mathcal{M}]\!]$

Fig. 3. Games OW-ATK (ATK $\in$ {CPA, PCA, VA, PCVA}) for PKE, where $\mathrm{O}_{\mathsf{ATK}}$ is defined in Definition 1. $\textsc{Pco}(\cdot, \cdot)$ is the Plaintext Checking Oracle and $\textsc{Cvo}(\cdot)$ is the Ciphertext Validity Oracle.

Plaintext Checking Attacks (OW-PCA) and One-Wayness under Plaintext and Validity Checking Attacks (OW-PCVA).

Definition 1 *(*OW-ATK*). Let* PKE = (Gen, Enc, Dec) *be a public-key encryption scheme with message space* $\mathcal{M}$*. For* ATK $\in$ {CPA, PCA, VA, PCVA}*, we define* OW-ATK *games as in Fig. 3, where*

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

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

A few remarks are in place. Our definition of the plaintext checking oracle $\textsc{Pco}(m, c)$ (c.f. Fig. 3) implicitly disallows queries on messages $m \in \mathcal{M}$. (With the convention that $\textsc{Pco}(m \notin \mathcal{M}, c)$ yields $\perp$.) This restriction is important since otherwise the ciphertext validity oracle $\textsc{Cvo}(\cdot)$ could be simulated as $\textsc{Cvo}(m) = \textsc{Pco}(\perp, c)$. Similarly, the ciphertext validity oracle $\textsc{Cvo}(c)$ 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 $\mathsf{Dec}(sk, c^*) = m'$. The two games have statistical difference δ, if PKE is δ-correct.

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

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

We also define $\mathsf{OW\text{-}ATK}$ and $\mathsf{IND\text{-}CPA}$ security in the random oracle 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 $\mathsf{H}(\cdot)$ plus the number of implicit queries to $\mathsf{H}(\cdot)$ made by the experiment.

It is well known that $\mathsf{IND\text{-}CPA}$ security of PKE with sufficiently large message space implies its $\mathsf{OW\text{-}CPA}$ security.

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

2.2 Key Encapsulation

Syntax. A key encapsulation mechanism $\mathsf{KEM} = (\mathsf{Gen}, \mathsf{Encaps}, \mathsf{Decaps})$ 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 $K := \mathsf{Decaps}(sk, c) \in \mathcal{K}$ or a special symbol $\perp \notin \mathcal{K}$ to indicate that c is not a valid encapsulation. We call KEM δ-*correct* if

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

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 ($\mathsf{IND\text{-}CCA}$).

Definition 3 *(*$\mathsf{IND\text{-}CCA}$*). We define the* $\mathsf{IND\text{-}CCA}$ *game as in Fig. 4 and the* $\mathsf{IND\text{-}CCA}$ *advantage function of an adversary* A *(with binary output) against* KEM *as* $\mathrm{Adv}_{\mathsf{KEM}}^{\mathsf{IND\text{-}CCA}}(\mathsf{A}) := |\Pr[\mathsf{IND\text{-}CCA}^{\mathsf{A}} \Rightarrow 1] - 1/2|$.

3 Modular FO Transformations

In Sect. 3.1, we will introduce T that transforms any $\mathsf{OW\text{-}CPA}$ secure encryption scheme PKE into a $\mathsf{OW\text{-}PCA}$ secure encryption scheme PKE_1. If PKE is furthermore $\mathsf{IND\text{-}CPA}$, then the reduction is tight. Furthermore, if PKE is γ-spread, then PKE_1 even satisfied the stronger security notion of $\mathsf{OW\text{-}PCVA}$ security. Next, in Sect. 3.2, we will introduce transformations $\mathsf{U}^{\not\perp}$, $\mathsf{U}_m^{\not\perp}$

GAME IND-CPA	**GAME** IND-CCA	$\textsc{Decaps}(c \neq c^*)$
$(pk, sk) \leftarrow \mathsf{Gen}$	$(pk, sk) \leftarrow \mathsf{Gen}$	$K := \mathsf{Decaps}(sk, c)$
$b \xleftarrow{\$} \{0,1\}$	$b \xleftarrow{\$} \{0,1\}$	**return** K
$(m_0^*, m_1^*, st) \leftarrow \mathsf{A}_1(pk)$	$(K_0^*, c^*) \leftarrow \mathsf{Encaps}(pk)$	
$c^* \leftarrow \mathsf{Enc}(pk, m_b^*)$	$K_1^* \xleftarrow{\$} \mathcal{K}$	
$b' \leftarrow \mathsf{A}_2(pk, c^*, st)$	$b' \leftarrow \mathsf{A}^{\textsc{Decaps}}(c^*, K_b^*)$	
return $[\![b' = b]\!]$	**return** $[\![b' = b]\!]$	

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

($\mathsf{U}^{\perp}$, $\mathsf{U}_m^{\perp}$) that transform any OW-PCA (OW-PCVA) secure encryption scheme PKE_1 into an IND-CCA secure KEM. The security reduction is tight. Transformations $\mathsf{U}_m^{\not\perp}$ and $\mathsf{U}_m^{\perp}$ can only be applied for deterministic encryption schemes. Combining T with $\{\mathsf{U}^{\not\perp}, \mathsf{U}_m^{\not\perp}, \mathsf{U}^{\perp}, \mathsf{U}_m^{\perp}\}$, in Sect. 3.3 we provide concrete bounds for the IND-CCA security of the resulting KEMs. Finally, in Sect. 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 $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ and randomness space $\mathcal{R}$, and random oracle $\mathsf{G} : \mathcal{M} \rightarrow \mathcal{R}$, we associate $\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$. The algorithms of $\mathsf{PKE}_1 = (\mathsf{Gen}, \mathsf{Enc}_1, \mathsf{Dec}_1)$ are defined in Fig. 5. Note that Enc_1 deterministically computers the ciphertext as $c := \mathsf{Enc}(pk, m; \mathsf{G}(m))$.

$\mathsf{Enc}_1(pk, m)$	$\mathsf{Dec}_1(sk, c)$
$c := \mathsf{Enc}(pk, m; \mathsf{G}(m))$	$m' := \mathsf{Dec}(sk, c)$.
return c	**if** $m' = \perp$ **or** $\mathsf{Enc}(pk, m'; \mathsf{G}(m')) \neq c$
	return $\perp$
	else return m'

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

Non-tight Security from OW-CPA. The following theorem establishes that OW-PCVA security of PKE_1 (cf. Definition 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 1 (PKE OW-CPA $\overset{\text{ROM}}{\Rightarrow}$ PKE$_1$ OW-PCVA)**.** *If* PKE *is δ-correct, then* PKE$_1$ *is δ_1-correct in the random oracle model with $\delta_1(q_{\mathsf{G}}) = q_{\mathsf{G}} \cdot \delta$. 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*

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

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

The main idea of the proof is that since Enc_1 is deterministic, the $\mathsf{PCA}(\cdot, \cdot)$ oracle can be equivalently implemented by "re-encryption" and the 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 (Fig. 2) of PKE$_1$ in the random oracle model. Game COR-RO makes at most q_{G} (distinct) queries $\mathsf{G}(m_1), \ldots, \mathsf{G}(m_{q_{\mathsf{G}}})$ to G. We call such a query $\mathsf{G}(m_i)$ *problematic* iff it exhibits a correctness error in PKE$_1$ (in the sense that $\mathsf{Dec}(sk, \mathsf{Enc}(pk, m_i; \mathsf{G}(m_i))) \neq m_i$). Since G outputs independently random values, each $\mathsf{G}(m_i)$ 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 $\mathsf{G}(m_i)$ is problematic is at most $q_{\mathsf{G}} \cdot \delta$. This proves $\Pr[\mathsf{COR\text{-}RO}^{\mathsf{A}} \Rightarrow 1] \leq q_{\mathsf{G}} \cdot \delta$ and hence PKE$_1$ is δ_1-correct with $\delta_1(q_{\mathsf{G}}) = q_{\mathsf{G}} \cdot \delta$.

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 Fig. 6.

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

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

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

Consider a single query Cvo(c) and define $m' := \mathsf{Dec}(sk, c)$. If Cvo$(c) = 1$ in G_1, then $\mathsf{G}(m') = \mathsf{G}(m) = r$ and hence $\mathsf{Enc}(pk, m'; G(m')) = c$, meaning Cvo$(c) = 1$ in G_0. If Cvo$(c) = 1$ in G_0, then we can only have Cvo$(c) = 0$ in G_1 only if $\mathsf{G}(m')$ 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

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

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

```
GAMES G0-G3
01 (pk, sk) ← Gen
02 m* ←$ M
03 c* ← Enc(pk, m*)
04 m' ← B^{G(·),Pco(·,·),Cvo(·)}(pk, c*)
05 return ⟦m' = m*⟧

G(m)
06 if ∃r s. th.(m, r) ∈ 𝔏_G
07    return r
08 if m = m*                                   // G3
09    QUERY := true                            // G3
10    abort                                    // G3
11 r ←$ R
12 𝔏_G := 𝔏_G ∪ {(m, r)}
13 return r

Pco(m ∈ M, c)
14 m' := Dec(sk, c)                            // G0-G1
15 return ⟦m' = m⟧
      and ⟦Enc(pk, m'; G(m')) = c⟧             // G0-G1
16 return ⟦Enc(pk, m, G(m)) = c⟧               // G2-G3

Cvo(c ≠ c*)
17 m' := Dec(sk, c)                            // G0-G1
18 return ⟦m' ∈ M⟧
      and ⟦Enc(pk, m'; G(m')) = c⟧             // G0
19 return ⟦∃(m, r) ∈ 𝔏_G
      and Enc(pk, m; r) = c and m' = m⟧        // G1
20 return ⟦∃(m, r) ∈ 𝔏_G
      and Enc(pk, m; r) = c⟧                   // G2-G3
```

Fig. 6. Games G_0-G_3 for the proof of Theorem 1.

We claim

$$|\Pr[G_2^{\mathsf{B}} \Rightarrow 1] - \Pr[G_1^{\mathsf{B}} \Rightarrow 1]| \leq q_{\mathsf{G}} \cdot \delta. \quad (4)$$

To show Eq. (4), observe that the whole Game G_1 (and also the whole Game G_2) makes at most q_{G} (distinct) queries $\mathsf{G}(m_1), \ldots, \mathsf{G}(m_{q_{\mathsf{G}}})$ to G. Again, we call such a query $\mathsf{G}(m_i)$ *problematic* iff it exhibits a correctness error in PKE_1 (in the sense that $\mathsf{Dec}(sk, \mathsf{Enc}(pk, m_i; \mathsf{G}(m_i))) \neq m_i$). 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 $\mathsf{G}(m_i)$ is problematic is at most $\delta_1(q_{\mathsf{G}}) \leq q_{\mathsf{G}} \cdot \delta$.

However, conditioned on the event that no query $\mathsf{G}(m_i)$ is problematic, Game G_1 and Game G_2 proceed identically (cf. Fig. 6). Indeed, the two games only differ if B submits a Pco query (m, c) or a Cvo query c together with a G query m such that $\mathsf{G}(m)$ is problematic and $c = \mathsf{Enc}(pk, m; \mathsf{G}(m))$. (In this case, G_1 will answer the query with 0, while G_2 will answer with 1.) This shows Eq. (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 [37],

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

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

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

$\mathsf{C}(pk, c^*)$	$\mathsf{D}(pk, c^*)$
$m' \leftarrow \mathsf{B}^{\mathsf{G}(\cdot),\textsc{Pco}(\cdot,\cdot)}(pk, c^*)$	$m \leftarrow \mathsf{B}^{\mathsf{G}(\cdot),\textsc{Pco}(\cdot,\cdot)}(pk, c^*)$
return m'	$(m', r') \xleftarrow{\$} \mathfrak{L}_G$
	return m'

Fig. 7. Adversaries C and Dagainst OW-CPA for the proof of Theorem 1. Oracles Pco, Cvo are defined as in game G_3, and G is defined as in game G_2 of Fig. 6.

So far we have established the bound

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

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

$$\Pr[\mathrm{QUERY}] \leq q_{\mathsf{G}} \cdot \mathrm{Adv}_{\mathsf{PKE}}^{\mathsf{OW\text{-}CPA}}(\mathsf{D}).$$

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

By definition, OW-PCA security is OW-PCVA security with $q_V := 0$ queries to the validity checking oracle. Hence, the bound of Theorem 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 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 2 (PKE IND-CPA $\overset{\text{ROM}}{\Rightarrow}$ 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*

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

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

Proof. Considering the games of Fig. 6 from the proof of Theorem 1 we obtain by Eq. (5)

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

$\mathsf{D}_1(pk)$	$\mathsf{D}_2(pk, c^*, st)$
$st := (m_0^*, m_1^*) \xleftarrow{\$} \mathcal{M}^2$	$m' \leftarrow \mathsf{B}^{\mathsf{G}(\cdot),\textsc{Pco}(\cdot),\textsc{Cvo}(\cdot)}(pk, c^*)$
return st	$b' := \begin{cases} 0 & \lvert\mathfrak{L}_G(m_0^*)\rvert > \lvert\mathfrak{L}_G(m_1^*)\rvert \\ 1 & \lvert\mathfrak{L}_G(m_1^*)\rvert < \lvert\mathfrak{L}_G(m_0^*)\rvert \\ \xleftarrow{\$} \{0,1\} & \text{otherwise} \end{cases}$
	return b'

Fig. 8. Adversary $\mathsf{D} = (\mathsf{D}_1, \mathsf{D}_2)$ against $\mathsf{IND\text{-}CPA}$ for the proof of Theorem 2. For fixed $m \in \mathcal{M}$, $\mathfrak{L}_G(m)$ is the set of all $(m, r) \in \mathfrak{L}_G$. Oracles Pco, Cvo are defined as in game G_3, and G is defined as in game G_2 of Fig. 6.

where the last inequation uses Lemma 1.

In Fig. 8 we construct an adversary $\mathsf{D} = (\mathsf{D}_1, \mathsf{D}_2)$ 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 $(pk, c^* \leftarrow \mathsf{Enc}(pk, m_b^*), st)$, 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 $\mathsf{IND\text{-}CPA}^{\mathsf{D}}$ 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 $\Pr[\text{BADG}] \le q_{\mathsf{G}}/|\mathcal{M}|$. For the remainder of the proof we assume BADG did not happen, i.e. $|\mathfrak{L}_G(m_{1-b}^*)| = 0$.

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

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

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

With the same argument as in Theorem 1, a tight reduction to OW-PCA security is implied without requiring PKE to be γ-spread.

3.2 Transformations $\mathsf{U}^{\not\perp}$, $\mathsf{U}_m^{\not\perp}$, $\mathsf{U}^{\perp}$, $\mathsf{U}_m^{\perp}$

In this section we introduce four variants of a transformation U, namely $\mathsf{U}^{\not\perp}$, $\mathsf{U}_m^{\not\perp}$, $\mathsf{U}^{\perp}$, $\mathsf{U}_m^{\perp}$, 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
$\mathsf{U}^{\not\perp}$	implicit	$K = \mathsf{H}(m, c)$	OW-PCA
$\mathsf{U}^{\perp}$	explicit	$K = \mathsf{H}(m, c)$	OW-PCVA
$\mathsf{U}_m^{\not\perp}$	implicit	$K = \mathsf{H}(m)$	det. + OW-CPA
$\mathsf{U}_m^{\perp}$	explicit	$K = \mathsf{H}(m)$	det. + OW-VA

Transformation $\mathsf{U}^{\perp}$: From OW-PVCA to IND-CCA. $\mathsf{U}^{\perp}$ transforms an OW-PCVA secure public-key encryption scheme into an IND-CCA secure key encapsulation mechanism. The $^{\perp}$ in $\mathsf{U}^{\perp}$ means that decapsulation of an invalid ciphertext results in the rejection symbol $\perp$ ("explicit rejection").

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

$\mathsf{Encaps}(pk)$	$\mathsf{Decaps}^{\perp}(sk, c)$
01 $m \xleftarrow{\$} \mathcal{M}$	05 $m' := \mathsf{Dec}_1(sk, c)$
02 $c \leftarrow \mathsf{Enc}_1(pk, m)$	06 **if** $m' = \perp$ **return** $\perp$
03 $K := \mathsf{H}(m, c)$	07 **else return**
04 **return** (K, c)	$K := \mathsf{H}(m', c)$

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

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

Theorem 3 (PKE_1 OW-PCVA $\overset{\text{ROM}}{\Rightarrow}$ $\mathsf{KEM}^{\perp}$ IND-CCA)**.** *If* PKE_1 *is* δ_1*-correct, so is* $\mathsf{KEM}^{\perp}$*. For any* IND-CCA *adversary* B *against* $\mathsf{KEM}^{\perp}$*, 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*

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

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 Pco$(\cdot,\cdot)$ provided by the OW-PCVA game. Additionally, the ciphertext validity oracle Cvo$(\cdot)$ is required to reject decapsulation queries with inconsistent ciphertexts.

```
GAMES G_0 - G_2
01 (pk, sk) ← Gen_1
02 m* ←$ M
03 c* ← Enc_1(pk, m*)
04 K*_0 := H(m*, c*)
05 K*_1 ←$ {0,1}^n
06 b ←$ {0,1}
07 b' ← B^{DECAPS^⊥,H}(pk, c*, K*_b)
08 return ⟦b' = b⟧

DECAPS^⊥(c ≠ c*)                          // G_0
09 m' := Dec_1(sk, c)
10 if m' = ⊥ return ⊥
11 return K := H(m', c)

H(m, c)
12 if ∃K such that (m, c, K) ∈ 𝔏_H
13    return K
14 K ←$ 𝒦
15 if Dec_1(sk, c) = m                     // G_1-G_2
16    if c = c*                            // G_2
17       CHAL := true                      // G_2
18       abort                             // G_2
19    if ∃K' such that (c, K') ∈ 𝔏_D       // G_1-G_2
20       K := K'                           // G_1-G_2
21    else                                 // G_1-G_2
22       𝔏_D := 𝔏_D ∪ {(c, K)}             // G_1-G_2
23 𝔏_H := 𝔏_H ∪ {(m, c, K)}
24 return K

DECAPS^⊥(c ≠ c*)                          // G_1-G_2
25 if ∃K s. th. (c, K) ∈ 𝔏_D
26    return K
27 if Dec_1(sk, c) ∉ M
28    return ⊥
29 K ←$ 𝒦
30 𝔏_D := 𝔏_D ∪ {(c, K)}
31 return K
```

Fig. 10. Games G_0 - G_2 for the proof of Theorem 3.

Proof. It is easy to verify the correctness bound. Let B be an adversary against the IND-CCA security of $\mathsf{KEM}^{\perp}$, issuing at most q_D queries to $\textsc{Decaps}^{\perp}$ and at most q_{H} queries to H. Consider the games given in Fig. 10.

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

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

Game G_1. In game G_1, the oracles H and $\textsc{Decaps}^{\perp}$ are modified such that they make no use of the secret key any longer except by testing if $\mathsf{Dec}_1(sk', c) = m$ for given (m, c) in line 15 and if $\mathsf{Dec}_1(sk, c) \in \mathcal{M}$ for given c in line 27. Game G_1 contains two sets: hash list $\mathfrak{L}_H$ that contains all entries (m, c, K) where H was queried on (m, c), and set $\mathfrak{L}_D$ that contains all entries (c, K) where either H was queried on (m', c), $m' := \mathsf{Dec}_1(sk', c)$, or $\textsc{Decaps}^{\perp}$ 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 $m' := \mathsf{Dec}_1(sk', c)$.

- Case 1: $m' \notin \mathcal{M}$. Since $\textsc{Cvo}(c) = 0$ is equivalent to $m' = \perp$, $\textsc{Decaps}^{\perp}(c)$ 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 is ensures $\textsc{Decaps}^{\perp}(c) = \mathsf{H}(m', c)$, where $m' := \mathsf{Dec}_1(sk, c)$, for all

ciphertexts c with $m' \in \mathcal{M}$. We distinguish two sub-cases: B might either first query H on (m', c), then $\text{Decaps}^{\perp}$ on c, or the other way round.

- If H is queried on (m', c) first, it is recognized that $\mathsf{Dec}_1(sk, c) = m$ in line 15. Since Decaps was not yet queried on c, no entry of the form (c, K) can already exist in $\mathfrak{L}_D$. Therefore, besides adding $(m, c, K \xleftarrow{\$} \mathcal{K})$ to $\mathfrak{L}_H$, H also adds (c, K) to $\mathfrak{L}_D$ in line 22, thereby defining $\text{Decaps}^{\perp}(c) := K = \mathsf{H}(m', c)$.
- If $\text{Decaps}^{\perp}$ is queried on c first, no entry of the form (c, K) exists in $\mathfrak{L}_D$ yet. Therefore, $\text{Decaps}^{\perp}$ 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 $\mathsf{Dec}_1(sk, c) = m'$ 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 $\mathsf{H}(m', c) := K = \text{Decaps}^{\perp}(c)$.

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

$$\Pr[G_1^{\mathsf{B}} \Rightarrow 1] = \Pr[G_0^{\mathsf{B}} \Rightarrow 1]|.$$

Game G_2. From game G_2 on we proceed identical to the proof of Theorem 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,

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

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

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

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

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

Collecting the probabilities yields the required bound.

Transformation $\mathsf{U}^{\not\perp}$: From OW-PCA to IND-CCA. $\mathsf{U}^{\not\perp}$ is a variant of $\mathsf{U}^{\perp}$ with "implicit rejection" of inconsistent ciphertexts. It transforms an $\mathsf{OW\text{-}PCA}$ secure public-key encryption scheme into an $\mathsf{IND\text{-}CCA}$ secure key encapsulation mechanism.

The Construction. To a public-key encryption scheme $\mathsf{PKE}_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ with message space $\mathcal{M}$, and a random oracle $\mathsf{H} : \{0,1\}^* \to \mathcal{M}$ we associate $\mathsf{KEM}^{\not\perp} = \mathsf{U}^{\not\perp}[\mathsf{PKE}_1, \mathsf{H}] = (\mathsf{Gen}^{\not\perp}, \mathsf{Encaps}, \mathsf{Decaps}^{\not\perp})$. The algorithms of $\mathsf{KEM}^{\not\perp}$ are

```
A^{Pco(·,·)}(pk, c*)
  K* <-$ 𝒦
  b' <- B^{Decaps^⊥(·), H(·,·)}(pk, c*, K*)
  if ∃(m', c', K') ∈ 𝔏_H
        s. th. Pco(m', c*) = 1
     return m'
  else
     abort

H(m, c)
  if ∃K such that (m, c, K) ∈ 𝔏_H
     return K
  K <-$ 𝒦
  if Pco(m, c) = 1
     if ∃K' such that (c, K') ∈ 𝔏_D
        K := K'
     else
        𝔏_D := 𝔏_D ∪ {(c, K)}
  𝔏_H := 𝔏_H ∪ {(m, c, K)}
  return K
```

Fig. 11. Adversary A against OW-PCVA for the proof of Theorem 3, where $\text{Decaps}^{\perp}$ is defined as in Game G_2 of Fig. 10.

```
Gen^⊥̸
  (pk', sk') <- Gen_1
  s <-$ ℳ
  sk := (sk', s)
  return (pk', sk)

Encaps(pk)
  m <-$ ℳ
  c <- Enc_1(pk, m)
  K := H(m, c)
  return (K, c)

Decaps^⊥̸(sk, c)
  Parse sk = (sk', s)
  m' := Dec_1(sk', c)
  if m' ≠ ⊥
     return K := H(m', c)
  else return K := H(s, c)
```

Fig. 12. IND-CCA-secure key encapsulation mechanism $\mathsf{KEM}^{\not\perp} = \mathsf{U}^{\not\perp}[\mathsf{PKE}_1, \mathsf{H}]$.

defined in Fig. 12, Encaps is the same as in $\mathsf{KEM}^{\perp}$ (Fig. 9). Note that $\mathsf{U}^{\perp}$ and $\mathsf{U}^{\not\perp}$ essentially differ in decapsulation: $\mathsf{Decaps}^{\perp}$ from $\mathsf{U}^{\perp}$ rejects if c decrypts to $\perp$, whereas $\mathsf{Decaps}^{\not\perp}$ from $\mathsf{U}^{\not\perp}$ returns a pseudorandom key K.

Security. The following theorem establishes that IND-CCA security of $\mathsf{KEM}^{\not\perp}$ tightly reduces to the OW-PCA security of PKE_1, in the random oracle model.

Theorem 4 (PKE_1 OW-PCA $\overset{\text{ROM}}{\Rightarrow}$ KEM IND-CCA)**.** *If* PKE_1 *is* δ_1*-correct, then* $\mathsf{KEM}^{\not\perp}$ *is* δ_1*-correct in the random oracle model. For any* IND-CCA *adversary* B *against* $\mathsf{KEM}^{\not\perp}$*, issuing at most* q_D *queries to the decapsulation oracle* $\text{Decaps}^{\not\perp}$ *and at most* q_{H} *queries to the random oracle* H*, there exists an* OW-PCA *adversary* A *against* PKE_1 *that makes at most* q_{H} *queries to the* Pco *oracle such that*

$$\text{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathsf{KEM}^{\not\perp}}(\mathsf{B}) \leq \frac{q_{\mathsf{H}}}{|\mathcal{M}|} + \text{Adv}^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(\mathsf{A})$$

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

The proof is very similar to the one of Theorem 3. The only difference is the handling of decapsulation queries with inconsistent ciphertexts. Hence, we defer the proof to the full version [26].

Transformations $\mathsf{U}^{\not\perp_m}/\mathsf{U}^{\perp_m}$: From OW-CPA/OW-VA to IND-CCA for deterministic Encryption. Transformation $\mathsf{U}^{\perp}_m$ is a variant of $\mathsf{U}^{\perp}$ that derives the KEM key as $K = \mathsf{H}(m)$, instead of $K = \mathsf{H}(m, c)$. It transforms a OW-VA secure public-key encryption scheme with deterministic encryption (e.g., the ones obtained via T from Sect. 3.1) into an IND-CCA secure key encapsulation mechanism. We also consider an implicit rejection variant $\mathsf{U}^{\not\perp}_m$ that only requires OW-CPA security of the underlying encryption scheme PKE.

The Construction. To a public-key encryption scheme $\mathsf{PKE}_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ with message space $\mathcal{M}$, and a random oracle $\mathsf{H} : \{0,1\}^* \to \{0,1\}^n$, we associate $\mathsf{KEM}^{\not\perp}_m = \mathsf{U}^{\not\perp}_m[\mathsf{PKE}_1, \mathsf{H}] = (\mathsf{Gen}^{\not\perp}, \mathsf{Encaps}_m, \mathsf{Decaps}^{\not\perp}_m)$ and $\mathsf{KEM}^{\perp}_m = \mathsf{U}^{\perp}_m[\mathsf{PKE}_1, \mathsf{H}] = (\mathsf{Gen}_1, \mathsf{Encaps}_m, \mathsf{Decaps}^{\perp}_m)$. Algorithm $\mathsf{Gen}^{\not\perp}$ is given in Fig. 12 and the remaining algorithms of $\mathsf{KEM}^{\not\perp}_m$ and $\mathsf{KEM}^{\perp}_m$ are defined in Fig. 13.

$\mathsf{Encaps}_m(pk)$	$\mathsf{Decaps}^{\not\perp}_m(sk, c)$	$\mathsf{Decaps}^{\perp}_m(sk, c)$
$m \xleftarrow{\$} \mathcal{M}$	Parse $sk = (sk', s)$	$m' := \mathsf{Dec}_1(sk, c)$
$c := \mathsf{Enc}_1(pk, m)$	$m' := \mathsf{Dec}_1(sk', c)$	**if** $m' = \perp$ **return** $\perp$
$K := \mathsf{H}(m)$	**if** $m' \neq \perp$	**else return**
return (K, c)	**return** $K := \mathsf{H}(m')$	$K := \mathsf{H}(m')$
	else return $K := \mathsf{H}(s, c)$	

Fig. 13. IND-CCA-secure key encapsulation mechanisms $\mathsf{KEM}^{\not\perp}_m = \mathsf{U}^{\not\perp}_m[\mathsf{PKE}_1, \mathsf{H}]$ and $\mathsf{KEM}^{\perp}_m = \mathsf{U}^{\perp}_m[\mathsf{PKE}_1, \mathsf{H}]$.

Security of $\mathsf{KEM}^{\perp}_m$. The following theorem establishes that IND-CCA security of $\mathsf{KEM}^{\perp}_m$ tightly reduces to the OW-VA security of PKE_1, in the random oracle model. Again, the proof is similar to the one of Theorem 3 and can be found in [26].

Theorem 5 (PKE_1 OW-VA $\stackrel{\text{ROM}}{\Rightarrow}$ $\mathsf{KEM}^{\perp}_m$ IND-CCA)**.** *If PKE_1 is δ_1-correct, then so is $\mathsf{KEM}^{\perp}_m$. Let G denote the random oracle that PKE_1 uses (if any), and let $q_{\mathsf{Enc}_1,\mathsf{G}}$ and $q_{\mathsf{Dec}_1,\mathsf{G}}$ 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 $\mathsf{KEM}^{\perp}_m$, issuing at most q_D queries to the decapsulation oracle $\textsc{Decaps}^{\perp}_m$ and at most q_{G}, resp. q_{H} queries to its random oracles G and H, there exists an OW-VA adversary A against PKE_1 that makes at most q_D queries to the* Cvo *oracle such that*

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

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

Security of $\mathsf{KEM}^{\not\perp}_m$. The following theorem establishes that IND-CCA security of $\mathsf{KEM}^{\not\perp}_m$ 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 Theorems 4 and 5.

Theorem 6 (PKE_1 OW-CPA $\overset{\text{ROM}}{\Rightarrow}$ $\mathsf{KEM}_m^{\not\perp}$ IND-CCA)**.** *If* PKE_1 *is* δ_1*-correct, then so is* $\mathsf{KEM}_m^{\not\perp}$*. Let* G *denote the random oracle that* PKE_1 *uses (if any), and let* $q_{\mathsf{Enc}_1,\mathsf{G}}$ *and* $q_{\mathsf{Dec}_1,\mathsf{G}}$ *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* $\mathsf{KEM}_m^{\not\perp}$*, issuing at most* q_D *queries to the decapsulation oracle* $\textsc{Decaps}_m^{\not\perp}$ *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*

$$\mathrm{Adv}_{\mathsf{KEM}_m^{\not\perp}}^{\mathsf{IND\text{-}CCA}}(\mathsf{B}) \leq \mathrm{Adv}_{\mathsf{PKE}_1}^{\mathsf{OW\text{-}CPA}}(\mathsf{A}) + \frac{q_D}{|\mathcal{M}|} + \delta_1(q_\mathsf{G} + (q_\mathsf{H} + q_D)(q_{\mathsf{Enc}_1,\mathsf{G}} + q_{\mathsf{Dec}_1,\mathsf{G}}))$$

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

3.3 The Resulting KEMs

For completeness, we combine transformation T with $\{\mathsf{U}^{\not\perp}, \mathsf{U}^{\perp}, \mathsf{U}_m^{\not\perp}, \mathsf{U}_m^{\perp}\}$ from the previous sections to obtain four variants of the FO transformation $\mathsf{FO} := \mathsf{U}^{\not\perp} \circ \mathsf{T}$, $\mathsf{FO}^{\perp} := \mathsf{U}^{\perp} \circ \mathsf{T}$, $\mathsf{FO}_m^{\not\perp} := \mathsf{U}_m^{\not\perp} \circ \mathsf{T}$, and $\mathsf{FO}_m^{\perp} := \mathsf{U}_m^{\perp} \circ \mathsf{T}$. To a public-key encryption scheme $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ and randomness space $\mathcal{R}$, and hash functions $\mathsf{G} : \mathcal{M} \to \mathcal{R}$, $\mathsf{H} : \{0,1\}^* \to \{0,1\}^n$ we associate

$$\begin{aligned}
\mathsf{KEM}^{\not\perp} &= \mathsf{FO}^{\not\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}] := \mathsf{U}^{\not\perp}[\mathsf{T}[\mathsf{PKE}, \mathsf{G}], \mathsf{H}] = (\mathsf{Gen}^{\not\perp}, \mathsf{Encaps}, \mathsf{Decaps}^{\not\perp})\\
\mathsf{KEM}^{\perp} &= \mathsf{FO}^{\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}] := \mathsf{U}^{\perp}[\mathsf{T}[\mathsf{PKE}, \mathsf{G}], \mathsf{H}] = (\mathsf{Gen}, \mathsf{Encaps}, \mathsf{Decaps}^{\perp})\\
\mathsf{KEM}_m^{\not\perp} &= \mathsf{FO}_m^{\not\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}] := \mathsf{U}_m^{\not\perp}[\mathsf{T}[\mathsf{PKE}, \mathsf{G}], \mathsf{H}] = (\mathsf{Gen}^{\not\perp}, \mathsf{Encaps}_m, \mathsf{Decaps}_m^{\not\perp})\\
\mathsf{KEM}_m^{\perp} &= \mathsf{FO}_m^{\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}] := \mathsf{U}_m^{\perp}[\mathsf{T}[\mathsf{PKE}, \mathsf{G}], \mathsf{H}] = (\mathsf{Gen}, \mathsf{Encaps}_m, \mathsf{Decaps}_m^{\perp})\ .
\end{aligned}$$

Their constituting algorithms are given in Fig. 14.

The following table provides (simplified) concrete bounds of the IND-CCA security of $\mathsf{KEM} \in \{\mathsf{KEM}^{\not\perp}, \mathsf{KEM}^{\perp}, \mathsf{KEM}_m^{\not\perp}, \mathsf{KEM}_m^{\perp}\}$, directly obtained by combining Theorems 1–6. Here $q_{\mathsf{RO}} := q_\mathsf{G} + q_\mathsf{H}$ counts the total number of B's queries

$\mathsf{Gen}^{\not\perp}$
$(pk, sk) \leftarrow \mathsf{Gen}$
$s \xleftarrow{\$} \mathcal{M}$
$sk' := (sk, s)$
return (pk, sk')

$\mathsf{Decaps}^{\perp}(sk, c)$ [$\mathsf{Decaps}_m^{\perp}(sk, c)$]
$m' := \mathsf{Dec}(sk, c)$
if $c \neq \mathsf{Enc}(pk, m'; \mathsf{G}(m'))$ **or** $m' = \perp$
  return $\perp$
else return $K := \mathsf{H}(m', c)$ [$K := \mathsf{H}(m')$]

$\mathsf{Encaps}(pk)$ [$\mathsf{Encaps}_m(pk)$]
$m \xleftarrow{\$} \mathcal{M}$
$c := \mathsf{Enc}(pk, m; G(m))$
$K := \mathsf{H}(m, c)$ [$K := \mathsf{H}(m)$]
return (K, c)

$\mathsf{Decaps}^{\not\perp}(sk' = (sk, s), c)$ [$\mathsf{Decaps}_m^{\not\perp}(sk'(sk, s), c)$]
$m' := \mathsf{Dec}(sk, c)$
if $c \neq \mathsf{Enc}(pk, m'; G(m'))$ **or** $m' = \perp$
  return $K := \mathsf{H}(s, c)$ [$K := \mathsf{H}(m')$]
else return $K := \mathsf{H}(m', c)$ [$K := \mathsf{H}(m')$]

Fig. 14. IND-CCA secure Key Encapsulation Mechanisms $\mathsf{KEM}^{\not\perp} = (\mathsf{Gen}^{\not\perp}, \mathsf{Encaps}, \mathsf{Decaps}^{\not\perp})$, $\mathsf{KEM}^{\perp} = (\mathsf{Gen}, \mathsf{Encaps}, \mathsf{Decaps}^{\perp})$, $\mathsf{KEM}_m^{\not\perp} = (\mathsf{Gen}^{\not\perp}, \mathsf{Encaps}_m, \mathsf{Decaps}_m^{\not\perp})$, and $\mathsf{KEM}_m^{\perp} = (\mathsf{Gen}, \mathsf{Encaps}_m, \mathsf{Decaps}_m^{\perp})$ obtained from $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

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.

KEM	Concrete bounds on $\mathrm{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathsf{KEM}}(\mathsf{B}) \leq$	
$\mathsf{KEM}^{\not\perp}$	$q_{\mathsf{RO}} \cdot \delta + \frac{2q_{\mathsf{RO}}}{\lvert\mathcal{M}\rvert} + 2q_{\mathsf{RO}} \cdot \mathrm{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A})$	$q_{\mathsf{RO}} \cdot \delta + \frac{3q_{\mathsf{RO}}}{\lvert\mathcal{M}\rvert} + 3 \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A}')$
$\mathsf{KEM}^{\perp}$	$q_{\mathsf{RO}} \cdot (\delta + 2^{-\gamma}) + 2q_{\mathsf{RO}} \cdot \mathrm{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A})$	$q_{\mathsf{RO}} \cdot \left(\delta + 2^{-\gamma}\right) + \frac{3q_{\mathsf{RO}}}{\lvert\mathcal{M}\rvert} + 3 \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A}')$
$\mathsf{KEM}^{\not\perp}_m$	$(2q_{\mathsf{RO}} + q_D) \cdot \delta + \frac{2q_{\mathsf{RO}}}{\lvert\mathcal{M}\rvert} + 2q_{\mathsf{RO}} \cdot \mathrm{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A})$	$(2q_{\mathsf{RO}} + q_D) \cdot \delta + \frac{3q_{\mathsf{RO}}}{\lvert\mathcal{M}\rvert} + 3 \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A}')$
$\mathsf{KEM}^{\perp}_m$	$(2q_{\mathsf{RO}} + q_D) \cdot \delta + q_{\mathsf{RO}} \cdot 2^{-\gamma} + 2q_{\mathsf{RO}} \cdot \mathrm{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A})$	$(2q_{\mathsf{RO}} + q_D) \cdot \delta + q_{\mathsf{RO}} \cdot 2^{-\gamma} + 3 \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A}')$

Concrete parameters. For "κ bits of security" one generally requires that for all adversaries B with advantage $\mathrm{Adv}(\mathsf{B})$ and running in time $\mathrm{Time}(\mathsf{B})$, we have

$$\frac{\mathrm{Time}(\mathsf{B})}{\mathrm{Adv}(\mathsf{B})} \geq 2^{\kappa}.$$

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
$q_{\mathsf{RO}} \cdot \delta$	$\delta \leq 2^{-\kappa}$
$q_{\mathsf{RO}} \cdot 2^{-\gamma}$	$\gamma \geq \kappa$
$q_{\mathsf{RO}}/\lvert\mathcal{M}\rvert$	$\lvert\mathcal{M}\rvert \geq 2^{\kappa}$

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

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

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 trade-off 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 $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M} = \{0,1\}^n$ and a hash function $\mathsf{F} : \mathcal{M}^{\ell} \to \mathcal{R}$, we associate $\mathsf{PKE}_{\ell} = \mathsf{S}^{\ell}[\mathsf{PKE}, \mathsf{F}]$. The algorithms of PKE_{ℓ} are defined in Fig. 15.

Security. The following theorem shows that PKE_{ℓ} is IND-CPA secure, provided that PKE is OW-CPA secure. The proof (sketched in the introduction) is postponed to [26].

$\mathsf{Enc}_\ell(pk, m)$	$\mathsf{Dec}_\ell(sk, c = (c_0, \dots, c_\ell))$
$\mathbf{x} := (x_1, \dots, x_\ell) \xleftarrow{\$} (\{0,1\}^n)^\ell$	**for** $i = 1$ **to** ℓ **do**
$c_0 := m \oplus \mathsf{F}(\mathbf{x})$	$\quad x_i := \mathsf{Dec}(sk, c_i)$
for $i = 1$ **to** ℓ **do**	$\mathbf{x} := (x_1, \dots, x_\ell)$
$\quad c_i := \mathsf{Enc}(pk, x_i)$	**return** $c_0 \oplus \mathsf{F}(\mathbf{x})$
return $c := (c_0, \dots, c_\ell)$	

Fig. 15. Tightly $\mathsf{IND\text{-}CPA}$ secure encryption PKE_ℓ obtained from PKE.

Theorem 7 (PKE $\mathsf{OW\text{-}CPA} \Rightarrow \mathsf{PKE}_\ell$ $\mathsf{IND\text{-}CPA}$). *If* PKE *is* δ*-correct (in the ROM), then* PKE_ℓ *is* $\ell \cdot \delta$*-correct. Moreover, for any* $\mathsf{IND\text{-}CPA}$ *adversary* B *that issues at most* q_F *queries to random oracle* F*, there exists an* $\mathsf{OW\text{-}CPA}$ *adversary* A *such that*

$$\mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}_\ell}(\mathsf{B}) \le q_\mathsf{F}^{1/\ell} \cdot \mathrm{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A})$$

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

4 Modular FO Transformation in the QROM

In this section, we will revisit our transformations in the quantum random oracle model. In Sect. 4.1, we give a short primer on quantum computation and define the quantum random oracle model (QROM). In Sect. 4.2, we will state that transformation T from Fig. 5 (Sect. 3.1) is also secure in the quantum random oracle model. Next, in Sect. 4.3 we will introduce $\mathsf{QU}^\perp_m$ ($\mathsf{QU}^{\not\perp}_m$), a variant of $\mathsf{U}^\perp_m$ ($\mathsf{U}^{\not\perp}_m$), which has provable security in the quantum random oracle model. Combining the two above transformations, in Sect. 4.4 we provide concrete bounds for the $\mathsf{IND\text{-}CCA}$ security of $\mathsf{QKEM}^\perp_m = \mathsf{QFO}^\perp_m[\mathsf{PKE}, \mathsf{G}, \mathsf{H}, \mathsf{H}']$ and $\mathsf{QKEM}^{\not\perp}_m = \mathsf{QFO}^{\not\perp}_m[\mathsf{PKE}, \mathsf{G}, \mathsf{H}, \mathsf{H}']$ 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 $\sum_{(b_1,\cdots,b_n)\in\{0,1\}^n} \alpha_{b_1\cdots b_n} \cdot |b_1 \cdots b_n\rangle$, where $\alpha_{b_1,\cdots,b_n} \in \mathbb{C}^n$, with the additional restriction that $\sum_{(b_1,\cdots,b_n)\in\{0,1\}^n} |\alpha_{b_1\cdots b_n}|^2 = 1$. As in the one-dimensional case, we call the basis $\{|b_1 \cdots b_n\rangle\}_{(b_1,\cdots,b_n)\in\{0,1\}^n}$ 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 MEASURE($\cdot$), where the outcome of 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 $\sum_{b_1,\cdots,b_n \in \{0,1\}} \alpha_{b_1 \cdots b_n} \cdot |b_1 \cdots b_n\rangle$ will be $|b_1 \cdots b_n\rangle$ with probability $|\alpha_{b_1 \cdots b_n}|^2$. 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 [5,11], we view a quantum oracle as a mapping

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

where $\mathrm{O} : \{0, 1\}^n \to \{0, 1\}^m$, $x \in \{0, 1\}^n$ and $y \in \{0, 1\}^m$, and model quantum adversaries A with access to O by the sequence $U \circ \mathrm{O}$, where U is a unitary operation. We write $\mathsf{A}^{|\mathrm{O}\rangle}$ 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 [41] proved that no quantum algorithm $\mathsf{A}^{|f\rangle}$, issuing at most q quantum queries to $|f\rangle$, can distinguish between a random function $f : \{0, 1\}^m \to \{0, 1\}^n$ 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 $|\mathsf{H}\rangle$ 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 $\mathsf{PKE} = \mathsf{PKE}^{\mathsf{G}}$ is defined relative to a random oracle $|\mathsf{G}\rangle$, then again the correctness bound might depend on the number of queries to $|\mathsf{G}\rangle$. We call a public-key encryption scheme PKE in the quantum random oracle model $\delta(q_{\mathsf{G}})$-*correct* if for all (possibly unbounded, quantum) adversaries A making at most q_{G} queries to quantum random oracle $|\mathsf{G}\rangle$, $\Pr[\mathsf{COR\text{-}QRO}^{\mathsf{A}}_{\mathsf{PKE}} \Rightarrow 1] \leq \delta(q_{\mathsf{G}})$, where the correctness game COR-QRO is defined as in Fig. 16.

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

Recall transformation T from Fig. 5 of Sect. 3.1.

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

GAME COR-QRO:
$(pk, sk) \leftarrow \mathsf{Gen}$
$m \leftarrow \mathsf{A}^{|\mathsf{G}\rangle}(sk, pk)$
return $[\![\mathsf{Dec}(sk, \mathsf{Enc}(pk, m; \mathsf{G}(m))) \neq m]\!]$

Fig. 16. Correctness game COR-QRO for PKE_1 in the quantum random oracle model.

It can be shown that $\delta_1(q_{\mathsf{G}})$ can be upper bounded by the success probability of an (unbounded, quantum) adversary against a generic search problem. For more details, refer to the full version [26].

The following theorem (whose proof is loosely based on [38]) establishes that IND-PCA security of PKE_1 reduces to the OW-CPA security of PKE, in the quantum random oracle model.

Theorem 8 (PKE OW-CPA $\overset{\text{QROM}}{\Rightarrow}$ 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* $|\mathsf{G}\rangle$ *and* q_P *(classical) queries to the plaintext checking oracle* Pco*, there exists an* OW-CPA *quantum adversary* A *such that*

$$\mathrm{Adv}_{\mathsf{PKE}_1}^{\mathsf{OW\text{-}PCA}}(\mathsf{B}) \leq 8 \cdot \delta \cdot (q_{\mathsf{G}} + 1)^2 + (1 + 2q_{\mathsf{G}}) \cdot \sqrt{\mathrm{Adv}_{\mathsf{PKE}}^{\mathsf{OW\text{-}CPA}}(\mathsf{A})},$$

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

Similar to the proof of Theorem 1, the proof first implements the PCA oracle via "re-encryption". Next, we apply an algorithmic adaption of OW2H from [39] to decouple the challenge ciphertext $c^* := \mathsf{Enc}(pk, m^*; \mathsf{G}(m^*))$ from the random oracle G. The decoupling allows for a reduction from OW-CPA security. Again, we defer to [26] for details.

4.3 Transformations $\mathsf{QU}_m^{\perp}$, $\mathsf{QU}_m^{\not\perp}$

Transformation $\mathsf{QU}_m^{\perp}$: From OW-PCA to IND-CCA in the QROM. $\mathsf{QU}_m^{\perp}$ transforms an OW-PCA secure public-key encryption scheme into an IND-CCA secure key encapsulation mechanism with explicit rejection.

The Construction. To a public-key encryption scheme $\mathsf{PKE}_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ with message space $\mathcal{M} = \{0,1\}^n$, and hash functions $\mathsf{H} : \{0,1\}^* \rightarrow \{0,1\}^n$ and $\mathsf{H}' : \{0,1\}^n \rightarrow \{0,1\}^n$, we associate $\mathsf{QKEM}_m^{\perp} = \mathsf{QU}_m^{\perp}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$. The algorithms of $\mathsf{QKEM}_m^{\perp} = (\mathsf{QGen} := \mathsf{Gen}_1, \mathsf{QEncaps}_m, \mathsf{QDecaps}_m^{\perp})$ are defined in Fig. 17. We stress that hash function H' has matching domain and range.

Security. The following theorem (whose proof is again loosely based on [38] and is postponed to [26]) establishes that IND-CCA security of $\mathsf{QKEM}_m^{\perp}$ reduces to the OW-PCA security of PKE_1, in the quantum random oracle model.

Theorem 9 (PKE_1 OW-PCA $\overset{\text{QROM}}{\Rightarrow}$ $\mathsf{QKEM}_m^{\perp}$ IND-CCA)**.** *If* PKE_1 *is* δ_1*-correct, so is* $\mathsf{QKEM}_m^{\perp}$*. For any* IND-CCA *quantum adversary* B *issuing at most* q_D *(classical) queries to the decapsulation oracle* $\mathrm{QDecaps}_m^{\perp}$*, at most* q_{H} *queries to the*

$\mathsf{QEncaps}_m(pk)$	$\mathsf{QDecaps}^{\bot}_m(sk, c, d)$
$m \xleftarrow{\$} \mathcal{M}$	$m' := \mathsf{Dec}_1(sk, c)$
$c \leftarrow \mathsf{Enc}_1(pk, m)$	**if** $m' = \bot$ **or** $\mathsf{H}'(m') \neq d$
$d := \mathsf{H}'(m)$	**return** $\bot$
$K := \mathsf{H}(m)$	**else return** $K := \mathsf{H}(m')$
return (K, c, d)	

Fig. 17. IND-CCA-secure key encapsulation mechanism $\mathsf{QKEM}^{\bot}_m = \mathsf{QU}^{\bot}_m[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$.

quantum random oracle $|\mathsf{H}\rangle$ *and at most* $q_{\mathsf{H}'}$ *queries to the quantum random oracle* $|\mathsf{H}'\rangle$*, there exists an* OW-PCA *quantum adversary* A *issuing* $2q_D q_{\mathsf{H}'}$ *queries to oracle* PCO *such that*

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

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

Transformation $\mathsf{QU}^{\not\bot}_m$: From OW-PCA to IND-CCA in the QROM. $\mathsf{QU}^{\not\bot}_m$ 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 $\mathsf{PKE}_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ with message space $\mathcal{M} = \{0,1\}^n$, and hash functions $\mathsf{H} : \{0,1\}^* \to \{0,1\}^n$ and $\mathsf{H}' : \{0,1\}^n \to \{0,1\}^n$, we associate $\mathsf{QKEM}^{\not\bot}_m = \mathsf{QU}^{\not\bot}_m[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}'] = (\mathsf{QGen} := \mathsf{Gen}^{\not\bot}, \mathsf{QEncaps}_m, \mathsf{QDecaps}^{\not\bot}_m)$. Algorithm $\mathsf{Gen}^{\not\bot}$ is given in Fig. 12 and the remaining algorithms of $\mathsf{QKEM}^{\not\bot}_m$ are defined in Fig. 18. We stress again that hash function H' has matching domain and range.

$\mathsf{QEncaps}_m(pk)$	$\mathsf{QDecaps}^{\not\bot}_m(sk' = (sk, s), c, d)$
$m \xleftarrow{\$} \mathcal{M}$	$m' := \mathsf{Dec}_1(sk, c)$
$c \leftarrow \mathsf{Enc}_1(pk, m)$	**if** $m' = \bot$ **or** $\mathsf{H}'(m') \neq d$
$d := \mathsf{H}'(m)$	**return** $K := \mathsf{H}(s, c, d)$
$K := \mathsf{H}(m)$	**else return** $K := \mathsf{H}(m')$
return (K, c, d)	

Fig. 18. IND-CCA-secure key encapsulation mechanism $\mathsf{QKEM}^{\not\bot}_m = \mathsf{QU}^{\not\bot}_m[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$.

Security. The following theorem (whose proof is deferred to [26]) establishes that IND-CCA security of $\mathsf{QKEM}^{\not\bot}_m$ reduces to the OW-PCA security of PKE_1, in the quantum random oracle model.

Theorem 10 (PKE_1 OW-PCA $\overset{\text{QROM}}{\Rightarrow}$ $\mathsf{QKEM}^{\not\bot}_m$ IND-CCA)**.** *If* PKE_1 *is* δ*-correct, so is* $\mathsf{QKEM}^{\not\bot}_m$*. For any* IND-CCA *quantum adversary* B *issuing at most* q_D *(classical) queries to the decapsulation oracle* $\mathrm{QDecaps}^{\not\bot}_m$*, at most* q_{H} *queries to the* *quantum random oracle* $|\mathsf{H}\rangle$ *and at most* $q_{\mathsf{H}'}$ *queries to the quantum random oracle* $|\mathsf{H}'\rangle$*, there exists an* OW-PCA *quantum adversary* A *issuing* $2q_D q_{\mathsf{H}'}$ *queries to oracle* PCO *such that*

$$\mathrm{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathsf{QKEM}^{\perp}_{m}}(\mathsf{B}) \le (2q_{\mathsf{H}'} + q_{\mathsf{H}}) \cdot \sqrt{\mathrm{Adv}^{\mathsf{OW\text{-}PCA}}_{\mathsf{PKE}_1}(\mathsf{A})},$$

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

4.4 The Resulting KEMs

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

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

Algorithm $\mathsf{Gen}^{\not\perp}$ is given in Fig. 12 and the remaining algorithms are given in Fig. 19.

$\mathsf{QEncaps}_m(pk)$	$\mathsf{QDecaps}^{\perp}_m(sk, c, d)$
$m \xleftarrow{\$} \mathcal{M}$	$m' := \mathsf{Dec}(sk, c)$
$c := \mathsf{Enc}(pk, m; \mathsf{G}(m))$	**if** $c = \mathsf{Enc}(pk, m', \mathsf{G}(m'))$ **and** $\mathsf{H}'(m') = d$
$K := \mathsf{H}(m)$	**return** $K := \mathsf{H}(m')$
$d := \mathsf{H}'(m)$	**else return** $\perp$
return (K, c, d)	
	$\mathsf{QDecaps}^{\not\perp}_m(sk' = (sk, s), c, d)$
	$m' := \mathsf{Dec}(sk, c)$
	if $c = \mathsf{Enc}(pk, m', \mathsf{G}(m'))$ **and** $\mathsf{H}'(m') = d$
	return $K := \mathsf{H}(m')$
	else return $K := \mathsf{H}(s, c, d)$

Fig. 19. IND-CCA secure $\mathsf{QKEM}^{\perp}_{m}$ and $\mathsf{QKEM}^{\not\perp}_{m}$ obtained from PKE.

The following table provides (simplified) concrete bounds of the IND-CCA security of $\mathsf{KEM} \in \{\mathsf{QKEM}^{\not\perp}_{m}, \mathsf{QKEM}^{\perp}_{m}\}$ in the quantum random oracle model, directly obtained by combining Theorems 8–10. Here $q_{\mathsf{RO}} := q_{\mathsf{G}} + q_{\mathsf{H}} + q'_{\mathsf{H}}$ counts the total number of (implicit and explicit) queries to the quantum random oracles G, H and H′.

KEM	Concrete bound on $\text{Adv}_{\text{KEM}}^{\text{IND-CCA}}(\text{B}) \leq$
$\text{QKEM}_m^{\not\perp}$, $\text{QKEM}_m^{\perp}$	$8q_{\text{RO}}\sqrt{\delta \cdot q_{\text{RO}}^2 + q_{\text{RO}} \cdot \sqrt{\text{Adv}_{\text{PKE}}^{\text{OW-CPA}}(\text{A})}}$

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 Sect. 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

1. Abdalla, M., Bellare, M., Rogaway, P.: The oracle Diffie-Hellman assumptions and an analysis of DHIES. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 143–158. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45353-9_12
2. Albrecht, M.R., Orsini, E., Paterson, K.G., Peer, G., Smart, N.P.: Tightly secure Ring-LWE based key encapsulation with short ciphertexts. Cryptology ePrint Archive, Report 2017/354 (2017). http://eprint.iacr.org/2017/354
3. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange - a new hope. In: 25th USENIX Security Symposium, USENIX Security 2016, Austin, TX, USA, pp. 327–343, 10–12 August 2016
4. Baek, J., Lee, B., Kim, K.: Secure length-saving ElGamal encryption under the computational Diffie-Hellman assumption. In: Dawson, E.P., Clark, A., Boyd, C. (eds.) ACISP 2000. LNCS, vol. 1841, pp. 49–58. Springer, Heidelberg (2000). https://doi.org/10.1007/10718964_5
5. Beals, R., Buhrman, H., Cleve, R., Mosca, M., Wolf, R.: Quantum lower bounds by polynomials. In: 39th FOCS, pp. 352–361. IEEE Computer Society Press, November 1998
6. Bellare, M., Boldyreva, A., O'Neill, A.: Deterministic and efficiently searchable encryption. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 535–552. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74143-5_30
7. Bellare, M., Rogaway, P.: Random oracles are practical: a paradigm for designing efficient protocols. In: Ashby, V. (ed.) ACM CCS 1993, pp. 62–73. ACM Press, November 1993
8. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (2006). https://doi.org/10.1007/11761679_25
9. Bernstein, D.J., Chuengsatiansup, C., Lange, T., van Vredendaal, C.: NTRU prime. Cryptology ePrint Archive, Report 2016/461 (2016). http://eprint.iacr.org/2016/461
10. Bitansky, N., Vaikuntanathan, V.: A note on perfect correctness by derandomization. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10211, pp. 592–606. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56614-6_20

11. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_3
12. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Stehlé, D.: Crystals - Kyber: a CCA-secure module-lattice-based KEM. Cryptology ePrint Archive, Report 2017/634 (2017). http://eprint.iacr.org/2017/634
13. Bos, J.W., Costello, C., Ducas, L., Mironov, I., Naehrig, M., Nikolaenko, V., Raghunathan, A., Stebila, D.: Frodo: take off the ring! Practical, quantum-secure key exchange from LWE. In: Weippl, E.R., Katzenbeisser, S., Kruegel, C., Myers, A.C., Halevi, S. (eds.) ACM CCS 2016, pp. 1006–1018. ACM Press, October 2016
14. Bos, J.W., Costello, C., Naehrig, M., Stebila, D.: Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In: 2015 IEEE Symposium on Security and Privacy, pp. 553–570. IEEE Computer Society Press, May 2015
15. Cash, D., Kiltz, E., Shoup, V.: The twin Diffie-Hellman problem and applications. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 127–145. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78967-3_8
16. Cash, D., Kiltz, E., Shoup, V.: The twin Diffie-Hellman problem and applications. J. Cryptol. **22**(4), 470–504 (2009)
17. Cheon, J.H., Kim, D., Lee, J., Song, Y.: 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
18. Coron, J.S., Handschuh, H., Joye, M., Paillier, P., Pointcheval, D., Tymen, C.: GEM: a generic chosen-ciphertext secure encryption method. In: Preneel, B. (ed.) CT-RSA 2002. LNCS, vol. 2271, pp. 263–276. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45760-7_18
19. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput. **33**(1), 167–226 (2003)
20. Dent, A.W.: A designer's guide to KEMs. In: Paterson, K.G. (ed.) Cryptography and Coding 2003. LNCS, vol. 2898, pp. 133–151. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-40974-8_12
21. Ding, J., Xie, X., Lin, X.: 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
22. Dwork, C., Naor, M., Reingold, O.: Immunizing encryption schemes from decryption errors. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 342–360. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_21
23. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_34
24. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. J. Cryptol. **26**(1), 80–101 (2013)
25. Galindo, D., Martín, S., Morillo, P., Villar, J.L.: Fujisaki-Okamoto hybrid encryption revisited. Int. J. Inf. Secur. **4**(4), 228–241 (2005)
26. Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the Fujisaki-Okamoto transformation. Cryptology ePrint Archive, Report 2017/604 (2017). https://eprint.iacr.org/2017/604

27. Howgrave-Graham, N., Silverman, J.H., Whyte, W.: Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 118–135. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-30574-3_10
28. Kiltz, E., Malone-Lee, J.: A general construction of IND-CCA2 secure public key encryption. In: Paterson, K.G. (ed.) Cryptography and Coding 2003. LNCS, vol. 2898, pp. 152–166. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-40974-8_13
29. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_1
30. Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for Ring-LWE cryptography. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 35–54. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_3
31. NIST: National institute for standards and technology. Postquantum crypto project (2017). http://csrc.nist.gov/groups/ST/post-quantum-crypto
32. Okamoto, T., Pointcheval, D.: REACT: rapid enhanced-security asymmetric cryptosystem transform. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 159–174. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-45353-9_13
33. Peikert, C.: Lattice cryptography for the internet. Cryptology ePrint Archive, Report 2014/070 (2014). http://eprint.iacr.org/2014/070
34. Rackoff, C., Simon, D.R.: Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 433–444. Springer, Heidelberg (1992). https://doi.org/10.1007/3-540-46766-1_35
35. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) 37th ACM STOC, pp. 84–93. ACM Press, May 2005
36. Shoup, V.: ISO 18033–2: An emerging standard for public-key encryption, December 2004. http://shoup.net/iso/std6.pdf. Final Committee Draft
37. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs. Cryptology ePrint Archive, Report 2004/332 (2004). http://eprint.iacr.org/2004/332
38. Targhi, E.E., Unruh, D.: Post-quantum security of the Fujisaki-Okamoto and OAEP transforms. In: Hirt, M., Smith, A. (eds.) TCC 2016. LNCS, vol. 9986, pp. 192–216. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53644-5_8
39. Unruh, D.: Revocable quantum timed-release encryption. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 129–146. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_8
40. Unruh, D.: Non-interactive zero-knowledge proofs in the quantum random oracle model. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 755–784. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_25
41. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 758–775. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_44