Some (In)Sufficient Conditions for Secure Hybrid Encryption

Javier Herranz[a], Dennis Hofheinz[b], Eike Kiltz[c]

[a] *Dept. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya, Barcelona, Spain*
jherranz@ma4.upc.edu
[b] *Karlsruher Institute für Technologie, Germany*
Dennis.Hofheinz@kit.edu
[c] *Centrum Wiskunde en Informatica, Amsterdam, The Netherlands*
kiltz@cwi.nl

Abstract

In hybrid public key encryption (PKE), first a key encapsulation mechanism (KEM) is used to fix a random session key that is then fed into a highly efficient data encapsulation mechanism (DEM) to encrypt the actual message. A well-known composition theorem states that if *both* the KEM and the DEM have a high enough level of security (i.e. security against chosen-ciphertext attacks), then so does the hybrid PKE scheme. It is not known if these strong security requirements on the KEM and DEM are also necessary, nor if such general composition theorems exist for weaker levels of security.

Using six different security notions for KEMs, ten for DEMs, and six for PKE schemes, we completely characterize in this work which combinations lead to a secure hybrid PKE scheme (by proving a composition theorem) and which do not (by providing counterexamples). Furthermore, as an independent result, we revisit and extend prior work on the relations among security notions for KEMs and DEMs.

Keywords:
Hybrid public key encryption, KEM/DEM paradigm, indistinguishability, non-malleability

1. Introduction

Public key encryption (PKE) schemes (in contrast to symmetric ones) usually have restricted message spaces, meaning that each ciphertext can hide

only a limited number of plaintext bits. This greatly limits their application since in practice one typically wants to efficiently encrypt arbitrary amounts of data. One way of solving this problem is by using a *hybrid encryption scheme* consisting of an (asymmetric) public-key part to encrypt a key plus a (symmetric) secret-key part to encrypt the actual data. For the first part one uses a *key encapsulation mechanism* (KEM) to produce a random symmetric key K together with a ciphertext. For the second part this symmetric key K is then used to encrypt the data using a highly efficient *data encapsulation mechanism* (DEM), such as one based on AES. This popular approach is often referred to as the "KEM/DEM paradigm" and was first formalized by Cramer and Shoup [28, 11].

This KEM/DEM paradigm is a simple way of constructing efficient and practical public key encryption schemes, and so has received a lot of attention in literature. It is incorporated in many new standards and recommendations for encryption (see [29, 25, 12], for example) and many KEMs have been proposed in the literature ([27, 28, 11, 13, 8, 21] and others). A natural question when dealing with this paradigm is how the security of the individual KEM and DEM parts relates to the security of the resulting hybrid public key encryption scheme. This question is quite broad since there are a lot of different security notions for the three components of the paradigm to consider. As an example, the strongest security notion one usually considers is denoted as *indistinguishability under chosen ciphertext attacks* (IND-CCA2) [26]. Cramer and Shoup [11] already proved that chosen-ciphertext security for the KEM and the DEM part is a sufficient condition to obtain a chosen-ciphertext secure hybrid PKE scheme. The first natural question is if one can relax the general security requirements made to the KEM or DEM part and nevertheless obtain a chosen-ciphertext secure hybrid PKE scheme. This question is in particular motivated by the hybrid encryption scheme by Kurosawa and Desmedt [23, 1] which is chosen-ciphertext secure as a hybrid PKE scheme whereas its KEM part alone was shown not to be chosen-ciphertext secure [10]. A more general problem is to study which of the standard/natural security levels of the KEM and DEM parts are enough, and which are not, to obtain a secure hybrid PKE scheme.

1.1. Overview of our main contributions

The main result of this paper is to solve the above open problem. We study the conditions that the KEM and the DEM must satisfy in order to lead to a secure hybrid PKE scheme. Our characterization is complete

with respect to the considered security notions for KEMs, DEMs, and PKE schemes (that will be introduced in the next subsection) and the hierarchies implied by these notions.[1] For fixed security levels of the KEM and the DEM we show which security level for the hybrid PKE scheme can be guaranteed (by proving a corresponding hybrid composition theorem) and which cannot (by presenting a concrete counterexample).

To prove our results, we can in some places make use of established techniques [3, 17], whereas in other cases we need to introduce new proof machinery.

1.2. Security notions for KEMs, DEMs, and PKE schemes

PKE Security Notions. For PKE schemes we consider the six standard notions of $\{\text{NM}, \text{IND}\}$-$\{\text{CPA}, \text{CCA1}, \text{CCA2}\}$ which were classified in [3].

KEM Security Notions. For KEMs, besides the straightforward indistinguishability based security notions, we consider the notion of non-malleability (NM) that was proposed in a paper by Nagao, Manabe, and Okamoto [24]. Our six considered notions for KEMs are therefore

$$\{\text{NM}, \text{IND}\} - \{\text{CPA}, \text{CCA1}, \text{CCA2}\}.$$

The relations between the above notions are the same as in the PKE case (with similar proofs to those in [3]).

DEM Security Notions. For DEMs we consider the standard notions of $\{\text{NM}, \text{IND}\}$-$\{\text{CPA}, \text{CCA1}, \text{CCA2}\}$. Furthermore, we add the two attack forms of one-time (OT) and one-time chosen-ciphertext (OTCCA) security. Adding these new notions (that originate from Cramer and Shoup [11] and do not give an adversary access to an encryption oracle), which we will see later, is motivated by the hybrid PKE approach. The ten considered notions for DEMs are thus $\{\text{NM}, \text{IND}\}$-$\{\text{OT}, \text{OTCCA}, \text{CPA}, \text{CCA1}, \text{CCA2}\}$. Compared to [17] we use a different (and in our opinion more natural) security definition of NM for DEMs. (We do so to avoid intuitively completely insecure schemes which are still non-malleable, see Section 2.3 for a discussion.) As a consequence, we obtain a DEM hierarchy (Figure 3 in Section 2.3) that is

[1] We *do* consider established security notions for KEMs, DEMs, and PKE schemes such as those from [3]. We do *not* consider, in particular, the notion of IND-CCCA [16], which is tailored towards achieving secure hybrid encryption with one specific type of construction.

very different from that established in [17]. In fact, the characterization of the relations among the $\{\mathrm{CPA}, \mathrm{CCA1}, \mathrm{CCA2}\}$ notions is exactly the same as for the PKE case established in [3]. We think that this new characterization may be of independent interest.

Why consider non-malleability? While considering IND type security notions for KEMs, DEMs, and PKE schemes is straightforward, it may seem less interesting to consider NM type security notions for them. For the case of PKE and DEM we refer to [14, 5, 3] and [17] for a motivation. We now motivate NM security for KEMs. First of all, it is a natural theoretical question in the hybrid setting whether it is possible to build NM hybrid encryption from NM KEMs and DEMs. It is known that NM-CPA secure PKE schemes are easier to construct than IND-CCA2 secure ones [9] so in the hybrid setting we can also hope to be able to construct more efficient NM-CPA secure KEMs. Furthermore, and maybe more interestingly, non-malleability for KEMs also seems to be a natural security notion when considering so called related-key attacks [22, 6] on DEMs. In related-key attacks, a DEM is attacked by observing encryptions under "meaningfully related keys" and in the past many popular cryptographic ciphers were successfully broken by such attacks (e.g., [20, 19, 7]). For hybrid encryption, NM security for KEMs exactly prevents such related-key attacks on the DEM part.

1.3. (In)Sufficient Conditions for Hybrid Encryption

We show in Figure 1 which conditions on the KEM and the DEM lead to a hybrid PKE scheme with a certain level of security, and which do not. The symbol "$\geq$" is used for positive implications, meaning that any combination of a KEM and a DEM with the stated levels of security leads to a hybrid PKE scheme with the level of security stated after the symbol "$\geq$". On the other hand, the symbol "$<$" is used for negative results, meaning that there exists some combination of a KEM and a DEM satisfying the stated security notions such that the resulting hybrid PKE scheme does not satisfy the security notion stated after the symbol "$<$". (Usually, these constructions will require some mild complexity assumptions, e.g., the existence of a secure KEM in the first place.)

In the table there are eight key results, those with a number attached in brackets, which refers to the theorem where we prove the corresponding result. We deduce the rest of our results from these by using the security hierarchies of KEMs, DEMs and PKE schemes, that is, the relations between

DEM KEM	IND-OT IND-CPA IND-CCA1	NM-OT NM-CPA NM-CCA1	IND-OTCCA IND-CCA2
IND-CPA	$\geq$ IND-CPA (3.1) $<$ IND-CCA1 $<$ NM-CPA	$\geq$ IND-CPA $<$ IND-CCA1 $<$ NM-CPA	$\geq$ IND-CPA $<$ IND-CCA1 $<$ NM-CPA
NM-CPA	$\geq$ IND-CPA $<$ IND-CCA1 $<$ NM-CPA	$\geq$ NM-CPA (3.3) $<$ IND-CCA1 $<$ IND-CCA1	$\geq$ NM-CPA $<$ IND-CCA1 (4.2) $<$ IND-CCA1 (4.2)
IND-CCA1	$\geq$ IND-CCA1 (3.1) $<$ NM-CPA	$\geq$ IND-CCA1 $<$ NM-CPA	$\geq$ IND-CCA1 $<$ NM-CPA (4.1)
NM-CCA1	$\geq$ IND-CCA1 $<$ NM-CPA	$\geq$ NM-CCA1 (3.2) $<$ IND-CCA2	$\geq$ NM-CCA1 $<$ IND-CCA2 (4.5)
IND-CCA2	$\geq$ IND-CCA1 $<$ NM-CPA (4.3)	$\geq$ NM-CCA1 $<$ IND-CCA2 (4.4)	$\geq$ IND-CCA2 [11]

Figure 1: Sufficient and necessary conditions for hybrid encryption. The results are given in set-notation: all positive results hold with respect to the weakest possible combination of KEM/DEM in the set, whereas negative results hold with respect to the strongest combination. For discussion on how the key results propagate in this diagram, consult the discussion in the text and Figures 2 and 3.

the different security notions for each of these primitives (that are summarized in Figures 2 and 3, respectively). Here positive results propagate to the right and down, whereas negative results propagate to the top and left.

We now turn to a discussion of our results from Figure 1. The first remarkable fact is that it is possible to group notions for DEMs that achieve the same security level for the resulting hybrid scheme, even though the primitives themselves can be separated. For example, with an IND-OT secure DEM one can always reach the same level of security as with an IND-CCA1 DEM.

Extending [11], our main positive result is that an X-Y secure KEM in combination with an X-Y secure DEM also yields an X-Y secure hybrid scheme (Theorems 3.1, 3.2 and 3.3). Furthermore, an IND-CCA1 KEM and an IND-OT DEM already yield an IND-CCA1 hybrid scheme (Theorem 3.1); a NM-CCA1 KEM plus a NM-OT DEM imply a NM-CCA1 hybrid scheme (Theorem 3.2).

Our table also shows that the sufficient conditions on the KEM and the DEM in the composition theorem from [11] are also necessary: an IND-CCA2 secure hybrid scheme can only be guaranteed if both the KEM and the DEM have the highest considered security levels (that is, IND-CCA2 for KEM and IND-$\{$OTCCA, CCA2$\}$ for DEM). Any attempt to weaken the KEM to IND-CCA1/NM-CCA1 or the DEM to NM-CCA1 may yield a hybrid PKE scheme that is no longer IND-CCA2 (Theorems 4.1 / 4.5 and Theorem 4.4, respectively). Furthermore, even the strongest possible KEM in combination with a weak DEM (or vice-versa) only provides a relatively weak hybrid PKE scheme (Theorems 4.3 and 4.2). We stress that our negative results also hold in combination with DEM ciphertext integrity INT-CTXT [18, 4]. Note that IND-CCA2 plus INT-CTXT (also denoted as *authenticated encryption*) is strictly stronger than IND-CCA2 [4].

Our characterization from Figure 1 is complete with respect to all standard security notions for KEM, DEM, and PKE. We stress, on the other hand, that different, less standard security notions for KEMs/DEMs can lead to interesting results. For instance, [16] considers a new security notion for KEMs called "constrained chosen-ciphertext (IND-CCCA) security." IND-CCCA security is a proper relaxation of IND-CCA2 security for KEMs. However, [16] proves that, when combined with a suitably secure DEM, it allows to construct fully IND-CCA2 secure PKE schemes. This paper only considers more established security notions such as CPA, CCA1, and CCA2 security.

For proving our results, we use new as well as established techniques: for instance, the proof of Theorem 4.3 basically transports a counterexample used in [3] to separate two security notions for public key encryption to the hybrid setting. Conversely, Theorems 4.2 and 4.5 use a new DEM modification which introduces new, "weak" DEM keys. This does not harm the stand-alone security of the DEM in any way, but only makes sense in our specific KEM/DEM setting where the DEM keys produced by the KEM may be "vulnerable".

2. Security Definitions

In this section we formally introduce different security notions from PKE schemes, KEMs, and DEMs.

We first need to introduce some common notation. If x is a string, then $|x|$ denotes its length, while if S is a finite set then $|S|$ denotes its size. If $k \in \mathbb{N}$ then 1^k denotes the string of k ones. We write $X||Y$ to denote an encoding of two strings X and Y that allows to uniquely recover both X and Y. If S is a set then $s \xleftarrow{\$} S$ denotes the operation of picking an element s of S uniformly at random. We write $\mathcal{A}(x, y, \ldots)$ to indicate that $\mathcal{A}$ is an algorithm with inputs $x, y, \ldots$ and by $z \xleftarrow{\$} \mathcal{A}(x, y, \ldots)$ we denote the operation of running $\mathcal{A}$ with inputs $(x, y, \ldots)$ and letting z be the output. We write $\mathcal{A}^{\mathcal{O}_1, \mathcal{O}_2, \cdots}(x, y, \ldots)$ to indicate that $\mathcal{A}$ is an algorithm with inputs $x, y, \ldots$ and access to oracles $\mathcal{O}_1, \mathcal{O}_2, \ldots$ and by $z \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_1, \mathcal{O}_2, \cdots}(x, y, \ldots)$ we denote the operation of running $\mathcal{A}$ with inputs $(x, y, \ldots)$ and access to oracles $\mathcal{O}_1, \mathcal{O}_2, \ldots$, and letting z be the output.

2.1. Public Key Encryption

PKE Schemes. A *public key encryption* (PKE) scheme $\mathcal{PKE} = (\mathsf{PKE.Kg}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ consists of three probabilistic polynomial-time (PPT) algorithms. For consistency, we require[2] that for all $k \in \mathbb{N}$, all keypairs (pk, sk) in the range of $\mathsf{PKE.Kg}(1^k)$, and all messages $m \in \{0,1\}^*$, we always have $\mathsf{PKE.Dec}(sk, \mathsf{PKE.Enc}(pk, m)) = m$.

PKE Indistinguishability. For $atk \in \{cpa, cca1, cca2\}$, the notion of *indistinguishable against* ATK *attacks* (IND-ATK) is captured by defining

[2]Some relaxations are possible, see [15, Comments after Def. 5.1.1], for example. Such relaxations do not affect our results.

the advantage of a PPT adversary $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ as

$$\mathbf{Adv}^{pke\text{-}ind\text{-}atk}_{\mathcal{PKE},\mathcal{F}}(k) \;=\; \Big|\Pr\Big[\,\mathbf{Exp}^{pke\text{-}ind\text{-}atk\text{-}1}_{\mathcal{PKE},\mathcal{F}}(k) = 1\,\Big] - \Pr\Big[\,\mathbf{Exp}^{pke\text{-}ind\text{-}atk\text{-}0}_{\mathcal{PKE},\mathcal{F}}(k) = 1\,\Big]\Big|\,,$$

where, for $b \in \{0,1\}$,

Experiment $\mathbf{Exp}^{pke\text{-}ind\text{-}atk\text{-}b}_{\mathcal{PKE},\mathcal{F}}(k)$
$(pk, sk) \xleftarrow{\$} \mathsf{PKE.Kg}(1^k)$; $(St, m_0, m_1) \xleftarrow{\$} \mathcal{F}_1^{\mathtt{DEC}_1(sk,\cdot)}(pk)$, s.t. $|m_0| = |m_1|$;
$C^* \xleftarrow{\$} \mathsf{PKE.Enc}(pk, m_b)$; $b' \xleftarrow{\$} \mathcal{F}_2^{\mathtt{DEC}_2(sk,\cdot)}(C^*, St)$; return b'

and the oracles $\mathtt{DEC}_1$ and $\mathtt{DEC}_2$ are defined as

atk	$\mathtt{DEC}_1(sk,\cdot)$	$\mathtt{DEC}_2(sk,\cdot)$
cpa	ε	ε
cca1	$\mathsf{PKE.Dec}(sk,\cdot)$	ε
cca2	$\mathsf{PKE.Dec}(sk,\cdot)$	$\mathsf{PKE.Dec}(sk,\cdot)$

with the restriction that $\mathcal{F}_2$ is not allowed to query oracle $\mathtt{DEC}_2(sk,\cdot)$ on the target ciphertext C^*. Here ε denotes an oracle which returns an empty string for any input. Note that we use both capital and lower case letters for the same concepts (like *atk*, *cpa*, ...), depending on the expressions, so to improve their readability.

We also require that $\mathcal{F}_1$ outputs two messages m_0 and m_1 of equal length. This can be enforced, e.g., by only allowing $\mathcal{F}_1$ that always output equal-length messages; equivalently, we can truncate m_0 and m_1 to $\min\{|m_0|, |m_1|\}$ bits.

A public key encryption scheme $\mathcal{PKE}$ is said to be *indistinguishable against* ATK *attacks* (IND-ATK) if the advantage function $\mathbf{Adv}^{pke\text{-}ind\text{-}atk}_{\mathcal{PKE},\mathcal{F}}(k)$ is a negligible function in k for all polynomial-time adversaries $\mathcal{F}$. Recall that a function $f(k)$ is negligible in k if there exists $k_0 \in \mathbb{N}$ and $c > 0$ such that $f(k) < 1/k^c$ for all $k \geq k_0$.

VECTOR NOTATION In the following, we will denote vectors in boldface, as in $\mathbf{C}$. We denote by $|\mathbf{C}|$ the number of components in $\mathbf{C}$, and by $\mathbf{C}[i]$ the ith component, such that $\mathbf{C} = (\mathbf{C}[1], \ldots, \mathbf{C}[|\mathbf{C}|])$. We stress that in particular we also consider the *empty vector*. We write $\mathbf{C} = \varepsilon$ if $|\mathbf{C}| = 0$. We use the natural notation $C \in \mathbf{C}$ to indicate $C = \mathbf{C}[i]$ for some $1 \leq i \leq |\mathbf{C}|$. It will also be convenient to extend decryption to vectors where the operation is performed

componentwise, namely by $\mathbf{M} = (\mathbf{M}[1], \ldots, \mathbf{M}[|\mathbf{C}|]) \leftarrow \mathsf{PKE.Dec}(sk, \mathbf{C})$ we mean that $\mathbf{M}[i] \leftarrow \mathsf{PKE.Dec}(sk, \mathbf{C}[i])$ for $1 \le i \le |\mathbf{C}|$. We will consider relations of arity t, where t will be polynomial in the security parameter k. By writing $R(M, \mathbf{M})$ we mean $R(M, \mathbf{M}[1], \ldots, \mathbf{M}[t-1])$.

Formalization of non-malleability. Non-malleability was introduced in [14] and subsequently refined [3, 15]. The goal of an adversary in a non-malleability experiment is, given a ciphertext C, to come up with a vector of ciphertexts $\mathbf{C}$ whose decryption $\mathbf{M}$ is *meaningfully related* to m, where m is the plaintext encrypted in C. Here meaningfully related means that $R(M, \mathbf{M})$ holds for some relation R. The question is how one can exactly measure the advantage of an adversary. We will use the definition from [3] which considers an experiment involving the adversary.

For $atk \in \{cpa, cca1, cca2\}$, the notion of *non-malleable against* ATK *attacks* (NM-ATK) is captured by defining the advantage function of a PPT adversary $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ as

$$\begin{aligned}\mathbf{Adv}^{pke\text{-}nm\text{-}atk}_{\mathcal{PKE},\mathcal{F}}(k) \;=\; \Big|&\Pr\Big[\,\mathbf{Exp}^{pke\text{-}nm\text{-}atk\text{-}1}_{\mathcal{PKE},\mathcal{F}}(k) = 1\,\Big] \\ &- \Pr\Big[\,\mathbf{Exp}^{pke\text{-}nm\text{-}atk\text{-}0}_{\mathcal{PKE},\mathcal{F}}(k) = 1\,\Big]\Big| \,.\end{aligned}$$

Here, for $b \in \{0, 1\}$,

$$\begin{array}{l}\textbf{Experiment } \mathbf{Exp}^{pke\text{-}nm\text{-}atk\text{-}b}_{\mathcal{PKE},\mathcal{F}}(k) \\ \quad (pk, sk) \xleftarrow{\$} \mathsf{PKE.Kg}(1^k)\,;\; (St, \mathcal{M}) \xleftarrow{\$} \mathcal{F}_1^{\mathtt{DEC}_1(sk,\cdot)}(pk)\,; \\ \quad m_0^*, m_1^* \xleftarrow{\$} \mathcal{M}\,;\; C^* \xleftarrow{\$} \mathsf{PKE.Enc}(pk, m_1^*)\,; \\ \quad (R, \mathbf{C}) \xleftarrow{\$} \mathcal{F}_2^{\mathtt{DEC}_2(sk,\cdot)}(C^*, St)\,;\; \mathbf{M} \leftarrow \mathsf{PKE.Dec}(sk, \mathbf{C}) \\ \quad \text{If } C^* \notin \mathbf{C} \text{ and } R(m_b^*, \mathbf{M}) \text{ then return 1 else return 0}\end{array}$$

and the oracles $\mathtt{DEC}_1$ and $\mathtt{DEC}_2$ are defined as above, again with the restriction that $\mathcal{A}_2$ is not allowed to query $\mathtt{DEC}_2$ for C^*. In the experiment $\mathcal{M}$ is a probability distribution on the space of messages, and $m \xleftarrow{\$} \mathcal{M}$ denotes the choice of a message following this distribution. We insist that $\mathcal{M}$ is valid; that is, $|m_0| = |m_1|$ for any m_0, m_1 that are given non-zero probability in $\mathcal{M}$. (See also the discussion after our PKE indistinguishability definitions.)

The relations among all these different security notions for public key encryption schemes were established in [3]. They are summarized in Figure 2.

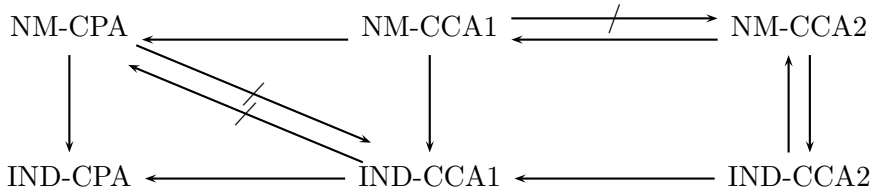

Figure 2: Implications and separations between security notions for PKE schemes from [3]. Note that these implications also hold for the corresponding KEM security notions.

2.2. Public Key Encapsulation Mechanisms

Now a *public-key encapsulation mechanism (KEM)* $\mathcal{KEM} = (\mathsf{KEM.Kg}, \mathsf{KEM.Enc}, \mathsf{KEM.Dec})$ with associated key-space $\mathsf{KeySp}(k)$ (which we assume to be $\mathsf{KeySp}(k) = \{0,1\}^{\ell(k)}$, where $\ell(k)$ is the key-length) consists of three PPT algorithms. For consistency, we require that for all $k \in \mathbb{N}$, and all $(K, C) \xleftarrow{\$} \mathsf{KEM.Enc}(1^k, pk)$ we have $\Pr[\,\mathsf{KEM.Dec}(sk, C) = K\,] = 1$, where the probability is taken over the choice of $(pk, sk) \xleftarrow{\$} \mathsf{KEM.Kg}(1^k)$, and the coins of all the algorithms in the expression above.

KEM Indistinguishability. The notion of indistinguishablity of KEMs against CCA2 attacks was established in [11]. Using the ideas from Section 2.1 it is straightforward to also extend it to CPA and CCA1 attacks.

For $atk \in \{cpa, cca1, cca2\}$, the notion of *indistinguishable against* ATK *attacks* (IND-ATK) is captured by defining the advantage function of a PPT adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ as

$$\begin{aligned}\mathbf{Adv}^{kem\text{-}ind\text{-}atk}_{\mathcal{KEM},\mathcal{A}}(k) \;=\; \Big|&\Pr\Big[\,\mathbf{Exp}^{kem\text{-}ind\text{-}atk\text{-}1}_{\mathcal{KEM},\mathcal{A}}(k) = 1\,\Big] \\ &- \Pr\Big[\,\mathbf{Exp}^{kem\text{-}ind\text{-}atk\text{-}0}_{\mathcal{KEM},\mathcal{A}}(k) = 1\,\Big]\Big|\,,\end{aligned}$$

where, for $b \in \{0,1\}$,

$$\begin{array}{l}\textbf{Experiment } \mathbf{Exp}^{kem\text{-}ind\text{-}atk\text{-}b}_{\mathcal{KEM},\mathcal{A}}(k) \\ \quad (pk, sk) \xleftarrow{\$} \mathsf{KEM.Kg}(1^k)\,;\; St \xleftarrow{\$} \mathcal{A}_1^{\mathtt{DEC}_1(sk,\cdot)}(pk)\,; \\ \quad K_0^* \xleftarrow{\$} \mathsf{KeySp}(k)\,;\; (K_1^*, C^*) \xleftarrow{\$} \mathsf{KEM.Enc}(pk)\,; \\ \quad b' \xleftarrow{\$} \mathcal{A}_2^{\mathtt{DEC}_2(sk,\cdot)}(pk, C^*, K_b^*, St)\,;\; \text{return } b'\end{array}$$

with the restriction that $\mathcal{A}$ is not allowed to query $\mathtt{DEC}_2(sk,\cdot)$ on the target ciphertext C^*. Oracles $\mathtt{DEC}_1$ and $\mathtt{DEC}_2$ are defined as in the case of PKE.

KEM Non-Malleability. In the PKE case, the adversary in the first stage has to output a description of the message space $\mathcal{M}$. This models the situation where an adversary may attack only a specific set of plaintexts such as the two messages "yes" and "no". With a KEM, the situation is different. A KEM is used to create ciphertexts for *random keys*, where the keys are uniformly distributed over some fixed key-space (whose description is contained in the public key). In general there is no efficient way to create a ciphertext for an arbitrary key. Therefore it is unreasonable to let the adversary define a key distribution $\mathcal{K}$ since the challenger would not be able to efficiently sample pairs of keys and ciphertexts where the keys are drawn according to $\mathcal{K}$. We rather define $\mathcal{K}$ to be the sampling algorithm that returns a key uniformly distributed in the key-space, just as $\mathsf{KEM.Enc}(pk)$ should do. We now give the formal definition of NM for KEMs as proposed by Nagao, Manabe, and Okamoto [24].

For $atk \in \{cpa, cca1, cca2\}$, the notion of *non-malleability against* ATK *attacks* (NM-ATK) is captured by defining the advantage function of a PPT adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ as

$$\begin{aligned}\mathbf{Adv}^{kem\text{-}nm\text{-}atk}_{\mathcal{KEM},\mathcal{A}}(k) \;=\; &\Big|\Pr\Big[\,\mathbf{Exp}^{kem\text{-}nm\text{-}atk\text{-}1}_{\mathcal{KEM},\mathcal{A}}(k)=1\,\Big]\\ &-\Pr\Big[\,\mathbf{Exp}^{kem\text{-}nm\text{-}atk\text{-}0}_{\mathcal{KEM},\mathcal{A}}(k)=1\,\Big]\Big|,\end{aligned}$$

where, for $b \in \{0,1\}$,

Experiment $\mathbf{Exp}^{kem\text{-}nm\text{-}atk\text{-}b}_{\mathcal{KEM},\mathcal{A}}(k)$
$(pk, sk) \xleftarrow{\$} \mathsf{KEM.Kg}(1^k)$; $St \xleftarrow{\$} \mathcal{A}_1^{\mathtt{DEC}_1(sk,\cdot)}(pk)$;
$K_0^* \xleftarrow{\$} \mathsf{KeySp}(k)$; $(K_1^*, C^*) \xleftarrow{\$} \mathsf{KEM.Enc}(pk)$; $c \xleftarrow{\$} \{0,1\}$;
$(R, \mathbf{C}) \xleftarrow{\$} \mathcal{A}_2^{\mathtt{DEC}_2(sk,\cdot)}(C^*, (K_c^*, K_{1-c}^*), St)$; $\mathbf{K} \leftarrow \mathsf{KEM.Dec}(sk, \mathbf{C})$
If $C^* \notin \mathbf{C}$ and $R(K_b^*, \mathbf{K})$ then return 1 else return 0.

The relation between the security notions for KEMs is the same as in the PKE case (see Figure 2). The equivalence between IND-CCA2 and NM-CCA2 was shown in [24] and the rest of the relations can be proved with a similar reasoning than in the PKE case studied in [3].

2.3. Data Encapsulation Mechanisms

A *data encapsulation mechanism (DEM)* $\mathcal{DEM} = (\mathsf{DEM.Kg}, \mathsf{DEM.Enc}, \mathsf{DEM.Dec})$ consists of three PPT algorithms. We require that for all $k \in \mathbb{N}$,

and all messages m, we have $\Pr[\,\mathsf{DEM.Dec}(K, \mathsf{DEM.Enc}(K, m)) = m\,] = 1$, where the probability is taken over the choice of $K \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$, and the coins of all the algorithms in the expression above.

DEM Indistinguishability. It is well known how to define indistinguishability against CPA, CCA1, and CCA2 attacks for DEMs [2]. We consider two more attack forms which we call one-time attacks (OT) and one-time (adaptive) chosen-ciphertext attacks (OTCCA).

For $atk \in \{ot, otcca, cpa, cca1, cca2\}$, the notion *indistinguishable against* ATK *attacks* (IND-ATK) is captured by defining the advantage function of a PPT adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ as

$$\mathbf{Adv}^{dem\text{-}ind\text{-}atk}_{\mathcal{DEM},\mathcal{B}}(k) = \left| \Pr\left[\, \mathbf{Exp}^{dem\text{-}ind\text{-}atk\text{-}1}_{\mathcal{DEM},\mathcal{B}}(k) = 1 \,\right] - \Pr\left[\, \mathbf{Exp}^{dem\text{-}ind\text{-}atk\text{-}0}_{\mathcal{DEM},\mathcal{B}}(k) = 1 \,\right] \right|,$$

where, for $b \in \{0, 1\}$,

Experiment $\mathbf{Exp}^{dem\text{-}ind\text{-}atk\text{-}b}_{\mathcal{DEM},\mathcal{B}}(k)$

$K \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$; $(St, m_0, m_1) \xleftarrow{\$} \mathcal{B}_1^{\mathtt{ENC}(\cdot),\mathtt{DEC}_1(sk,\cdot)}(1^k)$, s.t. $|m_0| = |m_1|$;
$C^* \xleftarrow{\$} \mathsf{DEM.Enc}(K, m_b)$; $b' \xleftarrow{\$} \mathcal{B}_2^{\mathtt{ENC}(\cdot),\mathtt{DEC}_2(sk,\cdot)}(C^*, St)$; return b'

and the oracles $\mathtt{ENC}$, $\mathtt{DEC}_1$, and $\mathtt{DEC}_2$ are defined as

	$\mathtt{ENC}(\cdot)$	$\mathtt{DEC}_1(sk, \cdot)$	$\mathtt{DEC}_2(sk, \cdot)$
ot	ε	ε	ε
otcca	ε	ε	$\mathsf{DEM.Dec}(K, \cdot)$
cpa	$\mathsf{DEM.Enc}(K, \cdot)$	ε	ε
cca1	$\mathsf{DEM.Enc}(K, \cdot)$	$\mathsf{DEM.Dec}(K, \cdot)$	ε
cca2	$\mathsf{DEM.Enc}(K, \cdot)$	$\mathsf{DEM.Dec}(K, \cdot)$	$\mathsf{DEM.Dec}(K, \cdot)$

with the restriction that $\mathcal{B}$ is not allowed to query the oracle $\mathtt{DEC}_2(\cdot)$ on the target ciphertext C^*. For clarification we note that in [17] different notation is used for attack forms on DEMs: OT is P0-C0, CPA is P2-C0, CCA1 is P2-C1, and CCA2 is P2-C2, whereas OTCCA was not considered.

DEM Non-Malleability. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be a PPT adversary. For ATK $\in \{ot, otcca, cpa, cca1, cca2\}$, the notion of *non-malleability against* ATK *attacks* (NM-ATK) is captured by defining the advantage of $\mathcal{B}$ as

$$\mathbf{Adv}^{dem\text{-}nm\text{-}atk}_{\mathcal{DEM},\mathcal{B}}(k) = \left| \Pr\left[\, \mathbf{Exp}^{dem\text{-}nm\text{-}atk\text{-}1}_{\mathcal{DEM},\mathcal{B}}(k) = 1 \,\right] - \Pr\left[\, \mathbf{Exp}^{dem\text{-}nm\text{-}atk\text{-}0}_{\mathcal{DEM},\mathcal{B}}(k) = 1 \,\right] \right|,$$

where, for $b \in \{0,1\}$,

Experiment $\mathbf{Exp}^{dem\text{-}nm\text{-}atk\text{-}b}_{\mathcal{DEM},\mathcal{B}}(k)$
$K \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$; $(St, \mathcal{M}) \xleftarrow{\$} \mathcal{B}_1^{\mathtt{ENC}(\cdot),\mathtt{DEC}_1(sk,\cdot)}(1^k)$; $m_0^*, m_1^* \xleftarrow{\$} \mathcal{M}$;
$C^* \xleftarrow{\$} \mathsf{DEM.Enc}(K, m_1^*)$; $(R, \mathbf{C}) \xleftarrow{\$} \mathcal{B}_2^{\mathtt{ENC}(\cdot),\mathtt{DEC}_2(sk,\cdot)}(C^*, St)$;
$\mathbf{M} \leftarrow \mathsf{DEM.Dec}(K, \mathbf{C})$
If $C^* \notin \mathbf{C}$ and $R(m_b^*, \mathbf{M})$ then return 1 else return 0

and the oracles $\mathtt{ENC}$, $\mathtt{DEC}_1$, and $\mathtt{DEC}_2$ are defined as in the IND case.

Katz and Yung [17] already provide security definitions for $\{\mathrm{OT}, \mathrm{CPA}, \mathrm{CCA1}, \mathrm{CCA2}\}$) attacks which we extend (motivated by the KEM/DEM apporach [11]) by adding OTCCA attacks. We stress that, in contrast to the original definition of Katz and Yung [17], we allow invalid ciphertexts in $\mathbf{C}$ as well as an empty $\mathbf{C}$. This leads to a relatively strict definition of non-malleability,[3] but we think that this best reflects the underlying intuition. It should not be possible to have a "secure" system which is only secure because the adversary cannot come up with a valid encryption of anything. Consider, for instance, a DEM which in every encryption leaks the complete plaintext, but authenticates every encryption so that no adversary can come up with a valid ciphertext without knowing the secret key. This scheme is trivially secure with respect to a non-malleability notion from [17] that requires the adversary to come up with a valid, non-empty ciphertext vector. (In fact, this is precisely the example from [17, Proof of Theorem 7].) We believe that this "security" is intuitively not justified.

Relations. Figure 3 shows the relations among the different security notions for DEMs. Due to our alternative security notion of NM, the proofs from [3] relating $\{\mathrm{IND}, \mathrm{NM}\} - \{\mathrm{CPA}, \mathrm{CCA1}, \mathrm{CCA2}\}$) for PKE schemes carry over the DEM setting.[4] Therefore the center diagram in Figure 3 exactly coincides with the relations for PKE schemes and KEMs (Figure 2).

The only thing that remains to prove is to extend a result from [3] showing that NM is strictly stronger than IND for all attacks forms. For CCA2

[3] We remark that this stronger notion of non-malleability is already mentioned (but not used) in [17].

[4] Concretely, for PKE schemes [3, Theorem 3.3] shows IND-OTCCA $\Rightarrow$ NM-OTCCA and IND-CCA2 $\Rightarrow$ NM-CCA2; [3, Theorem 3.5] shows IND-CCA1 $\not\Rightarrow$ NM-CPA; [3, Theorem 3.7] shows NM-CCA1 $\not\Rightarrow$ NM-CCA2; [3, Theorem 3.6] shows NM-CPA $\not\Rightarrow$ IND-CCA1. All these results carry over to the DEM setting.

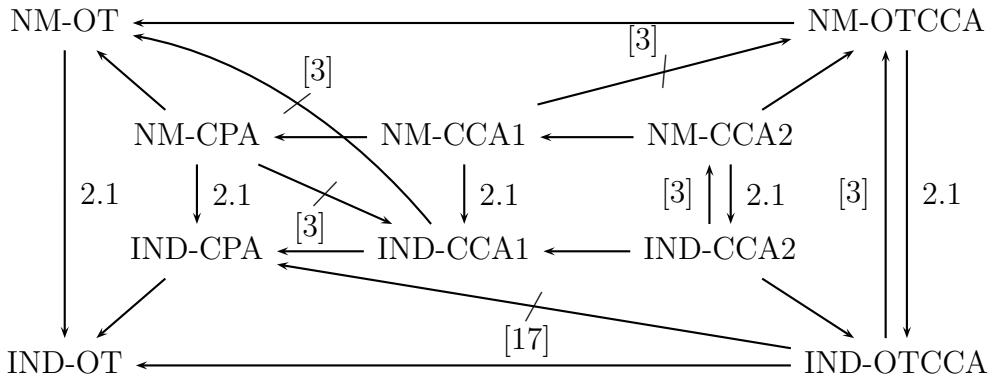

Figure 3: Implications and separations between the security notions for DEMs.

---

attacks this is in contrast to [17] (recall that [17] uses a weaker notion of non-malleability).

Theorem 2.1. [NM-ATK ⇒ IND-ATK] If a DEM is secure in the sense of NM-ATK then it is secure in the sense of IND-ATK, for any ATK ∈ {OT, OTCCA, CPA, CCA1, CCA2}.

Proof. For ATK ∈ {CPA, CCA1, CCA2} this is essentially Theorem 3.1 from [3]. We focus on the case ATK ∈ {OT, OTCCA}.

Assume $\mathcal{DEM}$ is secure in the NM-ATK sense for ATK ∈ {OT, OTCCA}. We will show it is also secure in the sense of IND-ATK. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be an IND-ATK adversary attacking $\mathcal{DEM}$. We have to show that $\mathbf{Adv}^{dem\text{-}ind\text{-}atk}_{\mathcal{DEM},\mathcal{B}}(\cdot)$ is negliglible. To this end we will describe a NM-ATK adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ attacking $\mathcal{DEM}$.

Alg. $\mathcal{A}_1(1^{\mathsf{k}})$	**Alg**. $\mathcal{A}_2^{\mathtt{DEC}_2(sk,\cdot)}(C^*, St, m_0, m_1)$
$(m_0, m_1, St) \xleftarrow{\$} \mathcal{B}_1(1^k)$	$c \xleftarrow{\$} \mathcal{B}_2^{\mathtt{DEC}'_2(sk,\cdot)}(m_0, m_1, C^*, St)$
$\mathcal{M} \leftarrow \{m_0, m_1\}$	Define $R(m_0) := 1 - c$, $R(m_1) := c$
Return $(\mathcal{M}, St, m_0, m_1)$	Return $(\mathbf{C} = \varepsilon, R)$

In the OTCCA case, adversary $\mathcal{B}_2$ has access to an oracle $\mathtt{DEC}'_2$ which is simulated by $\mathcal{A}_2$ using its own oracle $\mathtt{DEC}_2$. Note that $\mathcal{A}_2$ outputs an empty ciphertext vector $\mathbf{C} = \varepsilon$.

It is easy to verify that adversary $\mathcal{A}$ perfectly simulates $\mathcal{B}$'s view in the IND-ATK game. Furthermore, it holds

$$\Pr\left[\mathbf{Exp}^{\textit{dem-nm-atk-1}}_{\mathcal{DEM},\mathcal{A}}(k)=1\right]=\Pr\left[\mathbf{Exp}^{\textit{dem-ind-atk-b}}_{\mathcal{DEM},\mathcal{B}}(k)=b\right].$$

In effect, by [3, Proposition 3.8] we may assume here, without loss of generality, that we have $m_0 \neq m_1$ for the two messages output by $\mathcal{B}_1$. Adversary $\mathcal{A}$ returns a relation $R : \{m_0, m_1\} \to \{0, 1\}$ such that $R(m) = 1$ if $m = m_c$ and $R(m) = 0$, otherwise. In the IND-ATK game we have $\mathsf{DEM.Dec}(K, C^*) = m_b$ and therefore by definition of R, we have $R(m_b) = 1$ if and only if $b = c$.

Finally, we have that $\Pr\left[\mathbf{Exp}^{\textit{dem-nm-atk-0}}_{\mathcal{DEM},\mathcal{A}}(k)=1\right] = 1/2$. This follows from an information theoretic argument since $\mathcal{A}$ does not have any information about the message $\tilde{m} \in \{m_0, m_1\}$ in which the relation R is evaluated.

Applying the claims yields $\mathbf{Adv}^{\textit{dem-ind-atk}}_{\mathcal{DEM},\mathcal{B}}(k) = 2 \cdot \mathbf{Adv}^{\textit{dem-nm-atk}}_{\mathcal{DEM},\mathcal{A}}(k)$. Since $\mathcal{DEM}$ is secure in the sense of IND-ATK, $\mathbf{Adv}^{\textit{dem-nm-atk}}_{\mathcal{DEM},\mathcal{A}}(\cdot)$ and hence $\mathbf{Adv}^{\textit{dem-ind-atk}}_{\mathcal{DEM},\mathcal{B}}(k)$ is negliglible, too. □

2.4. Hybrid Encryption

Let $\mathcal{KEM} = (\mathsf{KEM.Kg}, \mathsf{KEM.Enc}, \mathsf{KEM.Dec})$ be a public-key encapsulation mechanism (KEM) and $\mathcal{DEM} = (\mathsf{DEM.Kg}, \mathsf{DEM.Enc}, \mathsf{DEM.Dec})$ be a data encapsulation mechanism (DEM). For simplicity we assume that the two schemes are compatible in the sense that for all security parameters k, we have that the KEM's and the DEM's key-space are equal. (If that is not the case we can apply a suitable *key-derivation function* [11] that maps the KEM's key-space to the DEM's key-space.) Then we can consider the *hybrid* public key encryption scheme $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}} = (\mathsf{PKE.Kg}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ which is constructed by combining $\mathcal{KEM}$ and $\mathcal{DEM}$ as follows:

Alg. $\mathsf{PKE.Kg}(1^k)$	**Alg**. $\mathsf{PKE.Enc}(pk, M)$	**Alg**. $\mathsf{PKE.Dec}(sk, (C_1, C_2))$
$(pk, sk) \xleftarrow{\$} \mathsf{KEM.Kg}(1^k)$	$(K, C_1) \xleftarrow{\$} \mathsf{KEM.Enc}(pk)$	$K \xleftarrow{\$} \mathsf{KEM.Dec}(sk, C_1)$
Return (pk, sk)	$C_2 \xleftarrow{\$} \mathsf{DEM.Enc}(K, M)$	$M \xleftarrow{\$} \mathsf{DEM.Dec}(K, C_2)$
	Return (C_1, C_2)	Return M

3. Sufficient Conditions for Secure Hybrid Encryption

3.1. Claims

We state more formally the positive results summarized in Figure 1 and provide proofs. The following three results can be considered as the

main composition theorems for hybrid encryption. They show that, for $X \in \{IND, NM\}$ and $Y \in \{OT, OTCCA, CPA, CCA1, CCA2\}$, an X-Y secure KEM and a X-Y secure DEM imply an X-Y secure hybrid PKE scheme. Interestingly, in some cases we have that for the DEM part a weaker attack form than Y is already sufficient.

Theorem 3.1. [IND-ATK KEM + IND − ATK′ DEM ⇒ IND-ATK PKE] For $ATK \in \{CPA, CCA1, CCA2\}$, if $\mathcal{KEM}$ is a secure KEM under IND-ATK attacks and $\mathcal{DEM}$ is a secure DEM under IND − ATK′ attacks, then $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}}$ is a secure PKE scheme under IND-ATK attacks, where for $ATK \in \{CPA, CCA1\}$, ATK′ = OT and for ATK = CCA2, ATK′ = OTCCA.

The CCA2 version of the proof can be found in Theorem 5 of [11]. The proofs for the other two cases are almost identical and omitted here.

The following two results are proved in Section 3.2.

Theorem 3.2. [NM-CCA1 KEM + NM-OT DEM ⇒ NM-CCA1 PKE] If $\mathcal{KEM}$ is a secure KEM under NM-CCA1 attacks and $\mathcal{DEM}$ is a secure DEM under NM-OT attacks, then $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}}$ is a secure PKE scheme under NM-CCA1 attacks.

Theorem 3.3. [NM-CPA KEM + NM-OT DEM ⇒ NM-CPA PKE] If $\mathcal{KEM}$ is a secure KEM under NM-CPA attacks and $\mathcal{DEM}$ is a secure DEM under NM-OT attacks, then $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}}$ is a secure PKE scheme under NM-CPA attacks.

We remark that the reductions are tight; that is, adversarial advantage and running times are preserved during the reduction.

3.2. Proof of Thms 3.2 and 3.3

These theorems state that NM-CCA1 KEM + NM-OT DEM ⇒ NM-CCA1 PKE, and NM-CPA KEM + NM-OT DEM ⇒ NM-CPA PKE. We will detail the first result, and will briefly comment the second result in the last paragraph of this section.

As a technical tool, we first provide an equivalent formulation of the NM notion for $\mathcal{KEM}$s. This notion of *non-malleability under parallel chosen-ciphertext attacks* was introduced in [5] for the PKE setting, and extended to the KEM setting in [24].

For $atk \in \{cpa, cca1, cca2\}$, the notion of *non-malleability under parallel* ATK *attacks* (PNM-ATK) is captured by defining the advantage function of a PPT adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ as

$$\begin{aligned}\mathbf{Adv}^{kem\text{-}pnm\text{-}atk}_{\mathcal{KEM},\mathcal{A}}(k) \;= \Big|&\Pr\Big[\,\mathbf{Exp}^{kem\text{-}pnm\text{-}atk\text{-}1}_{\mathcal{KEM},\mathcal{A}}(k) = 1\,\Big] \\ &- \Pr\Big[\,\mathbf{Exp}^{kem\text{-}pnm\text{-}atk\text{-}0}_{\mathcal{KEM},\mathcal{A}}(k) = 1\,\Big]\Big|\,,\end{aligned}$$

where, for $d \in \{0,1\}$,

Experiment $\mathbf{Exp}^{kem\text{-}pnm\text{-}atk\text{-}d}_{\mathcal{KEM},\mathcal{A}}(k)$
$(pk, sk) \xleftarrow{\$} \mathsf{KEM.Kg}(1^k)$; $St_1 \xleftarrow{\$} \mathcal{A}_1^{\mathtt{DEC}_1(sk,\cdot)}(pk)$;
$K_0^* \xleftarrow{\$} \mathsf{KeySp}(k)$; $(K_1^*, C^*) \xleftarrow{\$} \mathsf{KEM.Enc}(pk)$; $K^* \leftarrow K_d^*$;
$(St_2, \mathbf{C}) \xleftarrow{\$} \mathcal{A}_2^{\mathtt{DEC}_2(sk,\cdot)}(C^*, K^*, St_1)$; $\mathbf{K} \xleftarrow{\$} \mathsf{KEM.Dec}(\mathbf{C})$; $d' \xleftarrow{\$} \mathcal{A}_3(\mathbf{K}, St_2)$
If $(C^* \notin \mathbf{C})$ then return d' else return 0

and the oracles $\mathtt{DEC}_1$ and $\mathtt{DEC}_2$ are defined as in Section 2.1.

A key encapsulation mechanism $\mathcal{KEM}$ is said to be PNM *against* ATK *attacks* if the advantage function $\mathbf{Adv}^{kem\text{-}pnm\text{-}atk}_{\mathcal{KEM},\mathcal{A}}(k)$ is a negligible function in k for all polynomial-time adversaries $\mathcal{A}$.

It has been proved in [24] that (a slightly different but equivalent formulation of) PNM-ATK is tightly equivalent to NM-ATK for ATK $\in$ {CPA, CCA1, CCA2}. In the following proof, we are going to use therefore the PNM notion instead of the equivalent NM notion.

Proof of Theorems 3.2 and 3.3. First, to prove Theorem 3.2, assume $\mathcal{KEM}$ to be NM-CCA1 secure (and thus PNM-CCA1 secure), and $\mathcal{DEM}$ to be NM-OT secure. Consider an adversary $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ on the NM-CCA1 security of $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}}$. Denote the NM-CCA1 experiment $\mathbf{Exp}^{pke\text{-}nm\text{-}atk\text{-}b}_{\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}},\mathcal{F}}(k)$ by G_0^b.

In G_0^b, the challenge ciphertext C^* is generated as $C^* = (C_1^*, C_2^*)$ for $(K^*, C_1^*) \xleftarrow{\$} \mathsf{KEM.Enc}(pk)$ and $C_2^* \xleftarrow{\$} \mathsf{DEM.Enc}(K^*, m_1^*)$. In experiment G_1^b, we modify the generation of the challenge ciphertext as follows: $C^* = (C_1^*, C_2^*)$ for $(K^*, C_1^*) \xleftarrow{\$} \mathsf{KEM.Enc}(pk)$ and $C_2^* \xleftarrow{\$} \mathsf{DEM.Enc}(K^-, m_1^*)$ with an independently chosen key $K^- \xleftarrow{\$} \{0,1\}^k$. During the decryption of the ciphertext vector $\mathbf{C}$ for evaluating the relation R, the KEM ciphertext C_1^* is always decapsulated as K^- (without even running $\mathsf{KEM.Dec}$). We claim:

$$\Pr\big[\,G_0^b \to 1\,\big] \approx \Pr\big[\,G_1^b \to 1\,\big] \tag{1}$$

for $b = 0, 1$ (denoting by $X \approx Y$ that $|X - Y|$ is negligible in k). To see this (for fixed b), construct an adversary $\mathcal{A}$ on the PNM-CCA1 security of $\mathcal{KEM}$, so that $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ simulates the setting of game G_0^b resp. G_1^b for an internal simulation of $\mathcal{F}$. As a public key, $\mathcal{A}_1$ relays its own public key (for $\mathcal{KEM}$) to $\mathcal{F}_1$, and oracle queries from $\mathcal{F}_1$ are answered using $\mathcal{A}_1$'s own oracle. The key point is that $\mathcal{A}_2$ presents to $\mathcal{F}_2$ a challenge ciphertext $C^* = (C_1^*, C_2^*)$ that is built from $\mathcal{A}_2$'s own challenge (K^+, C^+) as $C_1^* \leftarrow C^+$ and $C_2^* \xleftarrow{\$} \mathsf{DEM.Enc}(K^+, m_1^*)$.

Once $\mathcal{F}_2$ outputs a ciphertext vector $\mathbf{C}$ along with a relation R, $\mathcal{A}_2$ translates this into a ciphertext vector $\mathbf{C}'$ for its own PNM-CCA1 setting and relays R along with K^+ as state information to $\mathcal{A}_3$. Specifically, $\mathbf{C}'$ contains all KEM ciphertexts of $\mathbf{C}$ which are not equal to the challenge KEM ciphertext C^+. Finally, $\mathcal{A}_3$, on input $(K^+, R, \mathbf{K}')$, where $\mathbf{K}'$ is the decapsulation of $\mathbf{C}'$, outputs $R(m_b^*, \mathbf{M})$. Here, $\mathbf{M}$ is generated by decapsulating $\mathbf{C}$ with the keys in $\mathbf{K}'$ and using K^+ as the decapsulation of C^+.

Now if $\mathcal{A}$ itself is run in $\mathbf{Exp}^{kem\text{-}pnm\text{-}cca1\text{-}d}_{\mathcal{KEM},\mathcal{A}}$, its output is that of G_{1-d}^b when run with $\mathcal{F}$. Since $\mathcal{KEM}$ is PNM-CCA1 secure, (1) follows.

Next we simulate G_1^b (with adversary $\mathcal{F}$) inside a NM-OT adversary $\mathcal{B}$ on $\mathcal{DEM}$. Here, $\mathcal{B}$ chooses a $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}}$ keypair on its own for the experiment and answers all oracle queries from $\mathcal{F}$ using this secret key. $\mathcal{B}$ relays $\mathcal{F}$'s choice of message space and then uses its own NM-OT challenge $C^\times$ in $\mathcal{F}$'s challenge ciphertext $C^* = (C_1^*, C_2^*)$ as C_2^*. Relation R and ciphertext vector $\mathbf{C}$ from $\mathcal{F}$ are translated as follows: if a ciphertext $(C_1^i, C_2^i) \in \mathbf{C}$ has $C_1^i \neq C_1^*$, it is decrypted using the prepared keypair and hardcoded into R. But all C_2^i with $C_1^i = C_1^*$ are collected and output by $\mathcal{B}$ as its own ciphertext vector (as ciphertexts encrypted by the same unknown key as $C_2^* = C^\times$).

Now the experiment $\mathbf{Exp}^{dem\text{-}nm\text{-}atk\text{-}b}_{\mathcal{DEM},\mathcal{B}}$ is simply a reformulation of G_1^b (with adversary $\mathcal{F}$). By the NM-OT security of $\mathcal{DEM}$, we thus have $\Pr[\, G_1^0 \to 1\,] \approx \Pr[\, G_1^1 \to 1\,]$, and hence, using (1), $\Pr[\, G_0^0 \to 1\,] \approx \Pr[\, G_0^1 \to 1\,]$, which shows $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}}$ secure.

The only difference in the CPA case is that $\mathcal{F}$ has no oracle access in the first phase; but then the reductions above work fine with a KEM that is PNM-CPA secure and a DEM which is NM-OT secure. □

4. Insufficient Conditions for Secure Hybrid Encryption

4.1. Claims

Now we turn to negative results from Figure 1. The following results are successively proved in Section 4.2

Theorem 4.1. [IND-CCA1 KEM + IND-CCA2 DEM $\not\Rightarrow$ NM-CPA PKE] Assume there exist a scheme $\mathcal{KEM}$ which is secure in the sense of IND-CCA1 and a scheme $\mathcal{DEM}$ which is secure in the sense of IND-CCA2. Then there exist a scheme $\mathcal{KEM}'$ which is secure in the sense of IND-CCA1 and a scheme $\mathcal{DEM}'$ which is secure in the sense of IND-CCA2, such that the hybrid scheme $\mathcal{PKE}_{\mathcal{KEM}',\mathcal{DEM}'}$ is not secure in the sense of NM-CPA.

Theorem 4.2. [NM-CPA KEM + IND-CCA2 DEM $\not\Rightarrow$ IND-CCA1 PKE] Assume there exist a scheme $\mathcal{KEM}$ which is secure in the sense of NM-CPA and a scheme $\mathcal{DEM}$ which is secure in the sense of IND-CCA2. Then there exist a scheme $\mathcal{KEM}'$ which is secure in the sense of NM-CPA and a scheme $\mathcal{DEM}'$ which is secure in the sense of IND-CCA2, such that the hybrid scheme $\mathcal{PKE}_{\mathcal{KEM}',\mathcal{DEM}'}$ is not secure in the sense of IND-CCA1.

Theorem 4.3. [$*$ KEM + IND-CCA1 DEM $\not\Rightarrow$ NM-CPA PKE] Assume there exists a scheme $\mathcal{DEM}$ which is secure in the sense of IND-CCA1. Then there exists a scheme $\mathcal{DEM}'$ which is also secure in the sense of IND-CCA1, such that for any $\mathcal{KEM}$ (independently of its security level), the hybrid scheme $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}'}$ is not secure in the sense of NM-CPA.

Theorem 4.4. [$*$ KEM + NM-CCA1 DEM $\not\Rightarrow$ IND-CCA2 PKE] Assume there exists a scheme $\mathcal{DEM}$ which is secure in the sense of NM-CCA1. Then there exists a scheme $\mathcal{DEM}'$ which is also secure in the sense of NM-CCA1, such that for any $\mathcal{KEM}$ (independently of its security level), the hybrid scheme $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}'}$ is not secure in the sense of IND-CCA2.

Theorem 4.5. [NM-CCA1 KEM + IND-CCA2 DEM $\not\Rightarrow$ IND-CCA2 PKE] Assume there exist a scheme $\mathcal{KEM}$ which is secure in the sense of NM-CCA1 and a scheme $\mathcal{DEM}$ which is secure in the sense of IND-CCA2. Then there exist a scheme $\mathcal{KEM}'$ which is secure in the sense of NM-CCA1 and a scheme $\mathcal{DEM}'$ which is secure in the sense of IND-CCA2, such that the hybrid scheme $\mathcal{PKE}_{\mathcal{KEM}',\mathcal{DEM}'}$ is not secure in the sense of IND-CCA2.

4.2. Proof of Thm 4.1: IND-CCA1 *KEM* + IND-CCA2 *DEM* $\not\Rightarrow$ NM-CPA *PKE.*

Assume there exists an IND-CCA1 secure scheme $\mathcal{KEM}$. We modify $\mathcal{KEM}$ into a scheme $\mathcal{KEM}' = (\mathsf{KEM}'.\mathsf{Kg}, \mathsf{KEM}'.\mathsf{Enc}, \mathsf{KEM}'.\mathsf{Dec})$ which is still secure in the sense of IND-CCA1. For that, we split the keys generated by $\mathsf{KEM}.\mathsf{Enc}$ in two parts of the same length k (we assume that the key length of $\mathsf{KEM}.\mathsf{Dec}$ is $2k$), denoting this fact as $K = K_1||K_2$. Concretely, we set $\mathsf{KEM}'.\mathsf{Kg} = \mathsf{KEM}.\mathsf{Kg}$ and

Alg. $\mathsf{KEM}'.\mathsf{Enc}(pk)$	**Alg**. $\mathsf{KEM}'.\mathsf{Dec}(sk, C_1'||C_2')$
$(K_1||K_2, C_1) \xleftarrow{\$} \mathsf{KEM}.\mathsf{Enc}(pk)$	$K_1||K_2 \xleftarrow{\$} \mathsf{KEM}.\mathsf{Dec}(sk, C_1')$
Return $(K_1||K_2, C_1||\perp)$	If $C_2' \in \{\perp, K_2\}$ then $K = K_1||K_2$ else $K = \perp$
	Return K

Note that $\mathcal{KEM}'$ inherits the IND-CCA1 security of $\mathcal{KEM}$: any IND-CCA1 adversary $\mathcal{A}'$ on $\mathcal{KEM}'$ can be reduced to an IND-CCA1 adversary on $\mathcal{KEM}$ by straightforwardly translating the challenge ciphertext and the decryption queries in the first phase to the $\mathcal{KEM}'$ setting that $\mathcal{A}'$ expects.

With respect to the DEM part, assume now that there exists an IND-CCA2 secure scheme $\mathcal{DEM} = (\mathsf{DEM}.\mathsf{Kg}, \mathsf{DEM}.\mathsf{Enc}, \mathsf{DEM}.\mathsf{Dec})$, with key-space $\{0,1\}^k$. We modify $\mathcal{DEM}$ into a new DEM $\mathcal{DEM}' = (\mathsf{DEM}'.\mathsf{Kg}, \mathsf{DEM}'.\mathsf{Enc}, \mathsf{DEM}'.\mathsf{Dec})$ (with key-space $\{0,1\}^{2k}$ so as to be compatible with $\mathcal{KEM}'$) which is still secure in the sense of IND-CCA2. Again we split the keys $K = K_1||K_2$ used by $\mathcal{DEM}$ in two parts of the same length.

Alg. $\mathsf{DEM}'.\mathsf{Kg}(1^k)$	**Alg**. $\mathsf{DEM}'.\mathsf{Enc}(K, M)$
$K_1 \xleftarrow{\$} \mathsf{DEM}.\mathsf{Kg}(1^k)$	Parse K as $K_1||K_2$
$K_2 \xleftarrow{\$} \{0,1\}^k$	$C_1' \xleftarrow{\$} \mathsf{DEM}.\mathsf{Enc}(K_1, M)$
Return $K = K_1||K_2$	$C_2' \leftarrow K_2$
	Return $C' = C_1'||C_2'$

Alg. $\mathsf{DEM}'.\mathsf{Dec}(K, C')$
Parse C' as $C_1'||C_2'$ and K as $K_1||K_2$
If $C_2' = K_2$ then $M \leftarrow \mathsf{DEM}.\mathsf{Dec}(K_1, C_1')$
else $M \leftarrow \perp$
Return M

Claim 4.6. If $\mathcal{DEM}$ is secure in the sense of IND-CCA2, then so is $\mathcal{DEM}'$.

Proof. We reduce an adversary $\mathcal{B}' = (\mathcal{B}'_1, \mathcal{B}'_2)$ on the IND-CCA2 security of $\mathcal{DEM}'$ to an adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ on the IND-CCA2 security of $\mathcal{DEM}$. The idea is that $\mathcal{B}$ internally runs $\mathcal{B}$ and simply translates challenge ciphertext and oracle queries:

Alg. $\mathcal{B}_1^{\mathtt{ENC}_1,\mathtt{DEC}_1}(1^k)$	**Alg.** $\mathcal{B}_2^{\mathtt{ENC}_2,\mathtt{DEC}_2}(C^*, St\|\|K_2)$
$K_2 \xleftarrow{\$} \{0,1\}^k$; $St \xleftarrow{\$} \mathcal{B}_1'^{\mathtt{ENC}'_1,\mathtt{DEC}'_1}(1^k)$	$b \xleftarrow{\$} \mathcal{B}_2'^{\mathtt{ENC}'_2,\mathtt{DEC}'_2}(C^*, St)$
Return $St\|\|K_2$	Return b

Here, oracle $\mathtt{ENC}'_2(M)$ returns $\mathtt{ENC}_2(M)||K_2$. Oracle $\mathtt{DEC}'_2(sk, C'_1||C'_2)$ returns $\mathtt{DEC}_2(sk, C'_1)$ if $C'_2 = K_2$ and $\perp$ otherwise. (Similarly for $\mathtt{ENC}'_2$ and $\mathtt{DEC}'_2$.) Note that this implies that $\mathcal{B}$ never queries $\mathtt{DEC}'_2$ on its target ciphertext.

Now $\mathcal{B}'$ gets identical views in the simulation inside $\mathcal{B}$ and in the IND-CCA2 experiment with $\mathcal{DEM}'$. Hence $\mathbf{Adv}^{dem\text{-}ind\text{-}atk}_{\mathcal{DEM}',\mathcal{B}'}(k) = \mathbf{Adv}^{dem\text{-}ind\text{-}atk}_{\mathcal{DEM},\mathcal{B}}(k)$ and thus, $\mathcal{DEM}'$ inherits the IND-CCA2 security of $\mathcal{DEM}$. □

Note that $\mathcal{DEM}'$ also inherits a possible ciphertext integrity property [18, 4] from $\mathcal{DEM}$. That is, if an adversary cannot produce fresh ciphertexts for $\mathcal{DEM}$ that are valid (in the sense that they do not get rejected by the decryption algorithm), then the same holds for $\mathcal{DEM}'$. The idea is that an adversary producing a valid $\mathcal{DEM}'$ ciphertext (C'_1, C'_2) (with $C'_2 = K_2$) must already produce a valid $\mathcal{DEM}$ ciphertext C'_1.

Claim 4.7. $\mathcal{PKE}_{\mathcal{KEM}',\mathcal{DEM}'}$ is not secure in the sense of NM-CPA.

Proof. We build a successful adversary $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ against $\mathcal{PKE}_{\mathcal{KEM}',\mathcal{DEM}'}$. In the first phase, $\mathcal{F}_1$ receives a public key pk and chooses as $\mathcal{M}$ the uniform distribution in a set of two messages m_0, m_1. Then, in the second phase, $\mathcal{F}_2$ receives a challenge ciphertext for the hybrid PKE scheme: $C^* = (C_1^*||C_2^*, C_3^*||C_4^*)$ where $(K_1||K_2, C) \xleftarrow{\$} \mathsf{KEM.Enc}(pk)$, $C_1^* = C$, $C_2^* = \perp$, $C_3^* = \mathsf{DEM.Enc}(K_1, M^*)$ and $C_4^* = K_2$, for some challenge message $m^* \in \{m_0, m_1\}$.

Now, the ciphertext $C = (C_1^*||C_4^*, C_3^*||C_4^*)$ is also a valid ciphertext for $\mathcal{PKE}_{\mathcal{KEM}',\mathcal{DEM}'}$ which encrypts the same message m^*. Therefore, $\mathcal{F}_2$ can output (R, C), where $R(m, m') = 1$ if and only if $m = m'$. In the experiment with $b = 1$, where message m in the evaluation of the relation is the challenge message m^*, the relation holds with probability one (message m' is in both experiments $m' = \mathsf{PKE.Dec}(sk, C) = m^*$); on the other hand, in the experiment with $b = 0$, where message m in the evaluation of the relation is message taken uniformly (and independently from m^*) from the

set $\{m_0, m_1\}$, the relation only holds with probability 1/2. Therefore the adversary $\mathcal{F}$ is successful.

Note that the use of the identity relation in a non-malleability attack is explicitly disallowed in [14]; however, our attack from above can be adapted to use a "bitwise complement" relation at the price of a more complicated KEM and DEM modification. □

4.3. Proof of Thm 4.2: NM-CPA *KEM* + IND-CCA2 *DEM* $\not\Rightarrow$ IND-CCA1 *PKE*

Assume there exists an NM-CPA secure scheme $\mathcal{KEM} = (\mathsf{KEM.Kg}, \mathsf{KEM.Enc}, \mathsf{KEM.Dec})$. Once again, it will be useful to assume that $\mathcal{KEM}$ has a key-space of $\{0,1\}^{2k}$. Also we assume that the secret keys sk of $\mathcal{KEM}$ are of the form $sk = sk_1||\ldots||sk_{p(k)}$ for $sk_i \in \{0,1\}^k$ and $p(k)$ a fixed polynomial. Both of these assumptions are without loss of generality.

We modify $\mathcal{KEM}$ into a KEM $\mathcal{KEM}' = (\mathsf{KEM'.Kg}, \mathsf{KEM'.Enc}, \mathsf{KEM'.Dec})$ which is still secure in the sense of NM-CPA. The modification is very similar to the one proposed in Section 3.6 of [3] for the case of PKE schemes.

Alg. $\mathsf{KEM'.Kg}(1^k)$
$(pk, sk) \xleftarrow{\$} \mathsf{KEM.Kg}(1^k)$
$v \xleftarrow{\$} \{0,1\}^k$
$pk' \xleftarrow{\$} pk$; $sk' \xleftarrow{\$} (sk, v)$
Return (pk', sk')

Alg. $\mathsf{KEM'.Enc}(pk')$
$(K, C) \xleftarrow{\$} \mathsf{KEM.Enc}(pk')$
Define $C' = 0||C$
Return (K, C')

Alg. $\mathsf{KEM'.Dec}(sk', C')$
Parse $sk' = (sk, v)$ and $C' = b||C$
If $b = 0$ return $\mathsf{KEM.Dec}(sk, C)$
else if $C = v||i$ for $1 \le i \le p(k)$ then
return $0^k||sk_i$ else return $0^k||v$

Using the same techniques as in Section 3.6 of [3] for the case of PKE schemes, $\mathcal{KEM}'$ can be proved to be secure in the sense of NM-CPA, whereas it is obviously insecure in the sense of IND-CCA1.

With respect to the DEM part, assume now that there exists an IND-CCA2 secure scheme $\mathcal{DEM} = (\mathsf{DEM.Kg}, \mathsf{DEM.Enc}, \mathsf{DEM.Dec})$ (with key-space $\{0,1\}^{2k}$, so that we can write $K = K_1||K_2$ for keys $K_1, K_2 \in \{0,1\}^k$). We modify $\mathcal{DEM}$ into a DEM $\mathcal{DEM}' = (\mathsf{DEM'.Kg}, \mathsf{DEM'.Enc}, \mathsf{DEM'.Dec})$ which is still secure in the sense of IND-CCA2.

Alg. $\mathsf{DEM}'.\mathsf{Kg}(1^k)$	**Alg.** $\mathsf{DEM}'.\mathsf{Enc}(K, m)$	**Alg.** $\mathsf{DEM}'.\mathsf{Dec}(K, C)$
$K \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$	Write $K = K_1 \| K_2$	Write $K = K_1 \| K_2$
Return K	If $K_1 = 0^k$ then $C = K \oplus m$	If $K_1 = 0^k$ then $m = K \oplus C$
	Else $C \xleftarrow{\$} \mathsf{DEM.Enc}(K, m)$	Else $m \leftarrow \mathsf{DEM.Dec}(K, C)$
	Return C	Return m

Now $\mathcal{DEM}'$ inherits $\mathcal{DEM}$'s IND-CCA2 security, since the only difference between the two schemes appears when $\mathsf{DEM.Kg}$ produces a $2k$-bit key K such that the first k bits of K are all zero (which happens only with negligible probability). Except for this negligible probability, the advantages of an adversary against $\mathcal{DEM}$ and an adversary against $\mathcal{DEM}'$ are exactly the same. For similar reasons, $\mathcal{DEM}'$ enjoys ciphertext integrity [18, 4] if $\mathcal{DEM}$ does.

Claim 4.8. $\mathcal{PKE}_{\mathcal{KEM}',\mathcal{DEM}'}$ is not secure in the sense of IND-CCA1.

Proof. An adversary $\mathcal{F}$ against the IND-CCA1 property of $\mathcal{PKE}_{\mathcal{KEM}',\mathcal{DEM}'}$ receives a public key pk' resulting from $(pk', sk') \leftarrow \mathsf{KEM.Kg}'(1^k)$. Recall that $sk' = (sk, v)$, where $(pk', sk') \leftarrow \mathsf{KEM.Kg}(1^k)$ and we write $sk = sk_1 || \ldots || sk_{p(k)}$.

In the first phase, $\mathcal{F}$ can ask decryption queries to an oracle; in particular, it can first ask for the decryption of the hybrid ciphertext $(1||0||0, 0^{2k})$. By definition of $\mathcal{KEM}'$, the key encapsulated in $C' = 1||0||0$ is $K = K_1||K_2 = 0^k||v$; by definition of $\mathcal{DEM}'$, since $K_1 = 0^k$, we have that the decrypted message obtained from this query is $m = K \oplus 0^{2k} = K = 0^k||v$. Once $\mathcal{F}$ has obtained the secret value of v, it can ask for the decryption of the ciphertexts $(1||v||i, 0^{2k})$, obtaining as answers the messages $0^k||sk_i$. Therefore, $\mathcal{F}$ is able to obtain the whole secret key sk' of the hybrid encryption scheme, even before receiving the challenge ciphertext. This means in particular that $\mathcal{PKE}_{\mathcal{KEM}',\mathcal{DEM}'}$ is not IND-CCA1 secure. □

4.4. Proof of Thm 4.3: ∗ KEM + IND-CCA1 *DEM ⇏* NM-CPA *PKE*

For this, we can use the ideas in the proof of [3, Theorem 3.5]. Say there exists an IND-CCA1 secure DEM $\mathcal{DEM} = (\mathsf{DEM.Kg}, \mathsf{DEM.Enc}, \mathsf{DEM.Dec})$. We modify $\mathcal{DEM}$ into a new DEM $\mathcal{DEM}' = (\mathsf{DEM}'.\mathsf{Kg}, \mathsf{DEM}'.\mathsf{Enc}, \mathsf{DEM}'.\mathsf{Dec})$ which is still secure in the sense of IND-CCA1. The new DEM $\mathcal{DEM}'$ is defined as follows. Here we denote by $\overline{m}$ the bitwise complement of the string m, namely the string obtained by flipping each bit of m.

Alg. $\mathsf{DEM}'.\mathsf{Kg}(1^k)$	**Alg.** $\mathsf{DEM}'.\mathsf{Enc}(K, m)$	**Alg.** $\mathsf{DEM}'.\mathsf{Dec}(K, C')$
$K \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$	$C_1 \xleftarrow{\$} \mathsf{DEM.Enc}(K, m)$	Parse C' as $C_1 \| C_2$
Return K	$C_2 \xleftarrow{\$} \mathsf{DEM.Enc}(K, \overline{m})$	$m \leftarrow \mathsf{DEM.Dec}(K, C_1)$
	Return $C' = C_1 \| C_2$	Return $\perp$

The following was already proved in [3, Claim 3.10] for the PKE case. (The proof holds literally, apart from obvious syntactic adaptations, in our case.)

Claim 4.9. If $\mathcal{DEM}$ is secure in the sense of IND-CCA1, then so is $\mathcal{DEM}'$.

However, the attack from [3, Claim 3.9] carries over to the hybrid setting:

Claim 4.10. For any scheme $\mathcal{KEM}$, $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}'}$ is not secure in the sense of NM-CPA.

Proof. Consider an arbitrary scheme $\mathcal{KEM} = (\mathsf{KEM.Kg}, \mathsf{KEM.Enc}, \mathsf{KEM.Dec})$. In effect, we can easily construct a successful adversary $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ against the NM-CPA property of the hybrid scheme: $\mathcal{F}_1$ receives a public key pk, resulting from $(pk, sk) \leftarrow \mathsf{KEM.Kg}(1^k)$; then it chooses the uniform distribution on a set $\{m_0, m_1\}$ of two messages, and receives a challenge ciphertext $C^* = (C_1, C_2 || C_3)$, where $(K, C_1) \xleftarrow{\$} \mathsf{KEM.Enc}(1^k, pk)$, $C_2 = \mathsf{DEM.Enc}(K, m^*)$ and $C_3 = \mathsf{DEM.Enc}(K, \overline{m^*})$, for some uniform message $m^* \in \{m_0, m_1\}$. It is evident that $C = (C_1, C_3 || C_2)$ is a valid encryption of message $\overline{m^*}$ under the scheme $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}'}$.

The adversary $\mathcal{F}_2$ can output $(R, \mathbf{C})$, where $\mathbf{C} = C$ contains only one ciphertext, and the relation is defined as $R(m, m') = 1$ if and only if $m' = \overline{m}$. In the real experiment (with $b = 1$), where $m = m^*$ in the evaluation of R, the relation holds with probability one (message m' is in both experiments $m' = \mathsf{PKE.Dec}(sk, C) = \overline{m^*}$). On the other hand, in the $b = 0$ experiment we have that R is evaluated on a uniform message $m \in \{m_0, m_1\}$ (chosen independently from m^*), and in $\overline{m^*}$, so the relation holds only with probability $1/2$. Therefore the adversary $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ is successful in breaking NM-CPA of this hybrid scheme. □

4.5. Proof of Thm 4.4: ∗ KEM + NM-CCA1 *DEM ⇏* IND-CCA2 *PKE*

Assuming that there exists a NM-CCA1 secure scheme $\mathcal{DEM} = (\mathsf{DEM.Kg}, \mathsf{DEM.Enc}, \mathsf{DEM.Dec})$, we modify $\mathcal{DEM}$ into a new DEM $\mathcal{DEM}' = (\mathsf{DEM}'.\mathsf{Kg}, \mathsf{DEM}'.\mathsf{Enc}, \mathsf{DEM}'.\mathsf{Dec})$ which is still secure in the sense of NM-CCA1. This modification is the same as the one proposed in Section 3.7 of [3] in order to

prove that there exist (public key) encryption schemes which are NM-CCA1 secure but not NM-CCA2. Let $F = \{F^k : k \geq 1\}$ be a family of pseudo-random functions (this is no extra assumption): each $F^k = \{F_K : K \in \{0,1\}^k\}$ is a finite collection of particular functions $F_K : \{0,1\}^k \to \{0,1\}^k$, indexed by a key K. We denote as ε the empty string. Again we split the keys $K = K_1||K_2$ used by $\mathcal{DEM}$ in two parts of the same length. The new scheme $\mathcal{DEM}'$ is defined as follows.

Alg. $\mathsf{DEM}'.\mathsf{Kg}(1^k)$
$K_1 \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$
$K_2 \xleftarrow{\$} \{0,1\}^k$
Return $K = K_1||K_2$

Alg. $\mathsf{DEM}'.\mathsf{Enc}(K, m)$
Parse K as $K_1||K_2$
$C = \mathsf{DEM.Enc}(K_1, m)$
Return $C' = 0||C||\varepsilon$

Alg. $\mathsf{DEM}'.\mathsf{Dec}(K, C')$
Write $K = K_1||K_2$ and $C' = b||C||z$
If $b = 0$ and $z = \varepsilon$, return $\mathsf{DEM.Dec}(K_1, C)$
Else if $b = 1$ and $z = \varepsilon$, return $F_{K_2}(C)$
Else if $b = 1$ and $z = F_{K_2}(C)$,
return $\mathsf{DEM.Dec}(K_1, C)$
Else return $\perp$

The following has been proved as [3, Claim 3.15].

Claim 4.11. If $\mathcal{DEM}$ is secure in the sense of NM-CCA1, then so is $\mathcal{DEM}'$.

Again, $\mathcal{DEM}$ uses keys of length $2k$, hence we need a KEM with key-space $\{0,1\}^{2k}$. (We stress again that this is without loss of generality.)So for the rest of this proof, we assume that $\mathcal{KEM}$ is any KEM with key-space $\{0,1\}^{2k}$.

Similar to the proof of Theorem 4.3, the attack from [3, Claim 3.14] on $\mathcal{DEM}$ can be transported to the hybrid setting.

Claim 4.12. For any scheme $\mathcal{KEM}$, $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}'}$ is not secure in the sense of IND-CCA2.

Proof. Consider an arbitrary KEM $\mathcal{KEM} = (\mathsf{KEM.Kg}, \mathsf{KEM.Enc}, \mathsf{KEM.Dec})$ and consider the hybrid public key encryption scheme $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}'}$. We are going to show that this hybrid scheme is not secure in the sense of IND-CCA2. An adversary $\mathcal{F}$ against the IND-CCA2 property of $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}'}$ receives

a public key pk resulting from $(pk, sk) \leftarrow \mathsf{KEM.Kg}(1^k)$; after the first phase, it receives a challenge ciphertext $C^* = (C_1, 0||C_2||\varepsilon)$, where $(K_1, C_1) \xleftarrow{\$} \mathsf{KEM.Enc}(1^k, pk)$ and $C_2 = \mathsf{DEM.Enc}(K_1, m_b)$, for some message m_b (with $b = 0, 1$ depending on the IND experiment) between two messages m_0, m_1 chosen by $\mathcal{F}$. In the following phase, the adversary $\mathcal{F}$ has access to a decryption oracle for ciphertexts different from C^*.

In particular, it can first ask for the decryption of $(C_1, 1||C_2||\varepsilon)$, obtaining the value of $F_{K_2}(C)$. Then it can ask for the decryption of $(C_1, 1||C_2||F_{K_2}(C))$, obtaining $\mathsf{DEM.Dec}(K_1, C) = m_b$ and thus breaking not only the IND security of the hybrid scheme, but also its one-wayness. Note that none of these two submitted ciphertexts is equal to C^*, as required. □

4.6. Proof of Thm 4.5: NM-CCA1 *KEM* + IND-CCA2 *DEM* $\not\Rightarrow$ IND-CCA2 *PKE*

Assume there exists a NM-CCA1 secure scheme $\mathcal{KEM} = (\mathsf{KEM.Kg}, \mathsf{KEM.Enc}, \mathsf{KEM.Dec})$, where we again assume that the key-space of $\mathcal{KEM}$ is $\{0,1\}^{2k}$. We start off by modifying $\mathcal{KEM}$ into $\mathcal{KEM}'$ along the lines of the modification of the DEM in the proof of Theorem 4.4. Namely, if F is a family of pseudo-random functions, we define:

Alg. $\mathsf{KEM}'.\mathsf{Kg}(1^k)$
$(pk, sk) \xleftarrow{\$} \mathsf{KEM.Kg}(1^k)$
$u \xleftarrow{\$} \{0,1\}^k$
$sk' \leftarrow sk||u$
Return (pk, sk')

Alg. $\mathsf{KEM}'.\mathsf{Enc}(pk)$
$(K, C) = \mathsf{KEM.Enc}(pk')$
$C' \leftarrow 0||C||\varepsilon$
Return (K', C')

Alg. $\mathsf{KEM}'.\mathsf{Dec}(sk', C')$
Write $sk' = sk||u$ and $C' = b||C||z$
If $b = 0$ and $z = \varepsilon$, return $\mathsf{KEM.Dec}(sk, C)$
else if $b = 1$ and $z = \varepsilon$, return $0^k||F_u(C)$
else if $b = 1$ and $z = 0^k||F_u(C)$ then
return $\mathsf{KEM.Dec}(sk, C)$
else return $\perp$

Again, a trivial syntactic adaptation of [3, Claim 3.15] shows

Claim 4.13. If $\mathcal{KEM}$ is secure in the sense of NM-CCA1, then so is $\mathcal{KEM}'$.

Combined with the IND-CCA2 secure DEM $\mathcal{DEM}'$ from the proof of Theorem 4.2, we get a hybrid encryption scheme $\mathcal{PKE} = \mathcal{PKE}_{\mathcal{KEM}',\mathcal{DEM}'}$. Now $\mathcal{PKE}$ is not IND-CCA2 secure. Namely, a CCA2 attack on $\mathcal{KEM}$' along the lines of the CCA2 attack on $\mathcal{DEM}$' in the proof of Theorem 4.4 can be carried out "through" the DEM $\mathcal{DEM}'$ just like in the proof of Theorem 4.2. We omit the details.

Acknowledgements

We thank Tatsuaki Okamoto for providing us with a preliminary version of [24] and Mihir Bellare for interesting discussions.

The work of the first two author was partially carried out while they were working at CWI. The work of Javier Herranz is partially supported by Spanish program CONSOLIDER-INGENIO 2010, under project ARES (CSD2007-00004). He also enjoys a *Ramón y Cajal* grant, partially funded by the European Social Fund (ESF), from Spanish MICINN Ministry. Eike Kiltz is supported by the research program Sentinels (`http://www.sentinels.nl`). Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs.

[1] Masayuki Abe, Rosario Gennaro, Kaoru Kurosawa, and Victor Shoup. Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT'05*, volume 3494 of Lecture Notes in Computer Science, pages 128–146, Aarhus, Denmark, May 22–26, 2005. Springer-Verlag, Berlin, Germany.

[2] Mihir Bellare, Anand Desai, Eric Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *38th Annual Symposium on Foundations of Computer Science*, pages 394–403, Miami Beach, Florida, October 19–22, 1997. IEEE Computer Society Press.

[3] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. In Hugo Krawczyk, editor, *Advances in Cryptology – CRYPTO'98*, volume 1462 of Lecture Notes in Computer Science, pages 26–45, Santa Barbara, CA, USA, August 23–27, 1998. Springer-Verlag, Berlin, Germany. Full version available at `http://eprint.iacr.org/1998/021`.

[4] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In Tatsuaki Okamoto, editor, *Advances in Cryptology – ASIACRYPT 2000*, volume 1976 of Lecture Notes in Computer Science, pages 531–545, Kyoto, Japan, December 3–7, 2000. Springer-Verlag, Berlin, Germany.

[5] Mihir Bellare and Amit Sahai. Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization. In Michael J. Wiener, editor, *Advances in Cryptology – CRYPTO'99*, volume 1666 of Lecture Notes in Computer Science, pages 519–536, Santa Barbara, CA, USA, August 15–19, 1999. Springer-Verlag, Berlin, Germany.

[6] Eli Biham. New types of cryptoanalytic attacks using related keys (extended abstract). In Tor Helleseth, editor, *Advances in Cryptology – EUROCRYPT'93*, volume 765 of Lecture Notes in Computer Science, pages 398–409, Lofthus, Norway, May 23–27, 1993. Springer-Verlag, Berlin, Germany.

[7] Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. Cryptology ePrint Archive, Report 2009/317, 2009. `http://eprint.iacr.org/`.

[8] Xavier Boyen, Qixiang Mei, and Brent Waters. Direct chosen ciphertext security from identity-based techniques. In *ACM 12th Conference on Computer and Communications Security*, pages 320–329, Alexandria, Virginia, USA, November 7–11, 2005. ACM Press.

[9] Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, and Hoeteck Wee. Black-box construction of a non-malleable encryption scheme from any semantically secure one. In Ran Canetti, editor, *Theory of Cryptography Conference*, volume 4948 of Lecture Notes in Computer Science, pages 427–444, New York, NY, USA, March 19–21, 2008. Springer-Verlag, Berlin, Germany.

[10] Seung Geol Choi, Javier Herranz, Dennis Hofheinz, Jung Yeon Hwang, Eike Kiltz, Dong Hoon Lee, and Moti Yung. The Kurosawa-Desmedt key encapsulation is not chosen-ciphertext secure. *Information Processing Letters*, 109(16):897–901, 2009.

[11] Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM Journal on Computing*, 33(1):167–226, 2003.

[12] CRYPTREC (cryptography research & evaluation committees): The cryptographic technique evaluation project, August 2003. `http://www.ipa.go.jp/security/enc/CRYPTREC/`.

[13] Alex Dent. A designer's guide to KEMs. In Kenneth G. Paterson , editor, *Cryptography and Coding: 9th IMA International Conference*, volume 2898 of Lecture Notes in Computer Science, pages 133–151, Cirencester, UK, December 16–18, 2003. Springer-Verlag, Berlin, Germany.

[14] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. In *23rd ACM Symposium on Theory of Computing*, pages 542–552, New Orleans, Louisiana, USA, May 6–8, 1991. ACM Press.

[15] Oded Goldreich. *Foundations of Cryptography: Basic Applications*, volume 2. Cambridge University Press, Cambridge, UK, 2004.

[16] Dennis Hofheinz and Eike Kiltz. Secure hybrid encryption from weakened key encapsulation. In Alfred Menezes, editor, *Advances in Cryptology – CRYPTO'07*, volume 4622 of Lecture Notes in Computer Science, pages 553–571, Santa Barbara, CA, USA, August 19–23, 2007. Springer-Verlag, Berlin, Germany.

[17] Jonathan Katz and Moti Yung. Characterization of security notions for probabilistic private-key encryption. *Journal of Cryptology*, 19(1):67–96, 2006.

[18] Jonathan Katz and Moti Yung. Unforgeable encryption and chosen-ciphertext-secure modes of operation. In Bruce Schneier, editor, *Proceedings of FSE 2000*, volume 1978 of Lecture Notes in Computer Science, pages 284–299, New York, NY, USA, April 10–12, 2000. Springer-Verlag, Berlin, Germany.

[19] John Kelsey, Bruce Schneier, Chris Hall, and David Wagner. Secure applications of low-entropy keys. In *Proceedings of ISW*, pages 121–134, 1997.

[20] John Kelsey, Bruce Schneier, and David Wagner. Key-schedule cryptoanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In Neal Koblitz, editor, *Advances in Cryptology – CRYPTO'96*, volume 1109 of Lecture Notes in Computer Science, pages 237–251, Santa Barbara, CA, USA, August 18–22, 1996. Springer-Verlag, Berlin, Germany.

[21] Eike Kiltz. Chosen-ciphertext security from tag-based encryption. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography Conference*, volume 3876 of Lecture Notes in Computer Science, pages 581–600, New York, NY, USA, March 4–7, 2006. Springer-Verlag, Berlin, Germany.

[22] Lars R. Knudsen. Cryptanalysis of LOKI91. In Jennifer Seberry and Yuliang Zheng, editors, *Proceedings of AUSCRYPT 1992*, volume 718 of Lecture Notes in Computer Science, pages 196–208, Queensland, Australia, December 13–16, 1992. Springer-Verlag, Berlin, Germany.

[23] Kaoru Kurosawa and Yvo Desmedt. A new paradigm of hybrid encryption scheme. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO'04*, volume 3152 of Lecture Notes in Computer Science, pages 426–442, Santa Barbara, CA, USA, August 15–19, 2004. Springer-Verlag, Berlin, Germany.

[24] Waka Nagao, Yoshifumi Manabe, and Tatsuaki Okamoto. On the equivalence of several security notions of key encapsulation mechanism. Cryptology ePrint Archive, Report 2006/268, 2006. `http://eprint.iacr.org/`.

[25] NESSIE Final report of European project IST-1999-12324: New European Schemes for Signatures, Integrity, and Encryption, April 2004. Available at `https://www.cosic.esat.kuleuven.be/nessie/Bookv015.pdf/`.

[26] Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In Joan Feigenbaum, editor, *Advances in Cryptology – CRYPTO'91*, volume 576 of Lecture Notes in Computer Science, pages 433–444, Santa Barbara, CA, USA, August 11–15, 1992. Springer-Verlag, Berlin, Germany.

[27] Victor Shoup. Using hash functions as a hedge against chosen ciphertext attack. In Bart Preneel, editor, *Advances in Cryptology – EUROCRYPT'00*, volume 1807 of Lecture Notes in Computer Science, pages

275–288, Bruges, Belgium, May 14–18, 2000. Springer-Verlag, Berlin, Germany.

[28] Victor Shoup. A proposal for an ISO standard for public key encryption (version 2.1). manuscript, 2001. Available on `http://shoup.net/papers/`.

[29] Victor Shoup. ISO 18033-2: An emerging standard for public-key encryption. `http://shoup.net/iso/std6.pdf`, December 2004. Final Committee Draft.