KEM/DEM: Necessary and Sufficient Conditions for Secure Hybrid Encryption

Javier Herranz Dennis Hofheinz Eike Kiltz

August 8, 2006

CWI Amsterdam, The Netherlands
{herranz,hofheinz,kiltz}@cwi.nl

Abstract

The KEM/DEM hybrid encryption paradigm combines the efficiency and large message space of secret key encryption with the advantages of public key cryptography. Due to its simplicity and flexibility, the approach has ever since gained increased popularity and has been successfully adapted in encryption standards. 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 composition theorem states that if *both* the KEM and the DEM have the highest 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 neccessary, nor if such general composition theorems exist for weaker levels of security. In this work we study neccessary and sufficient conditions on the security of the KEM and the DEM in order to guarantee a hybrid PKE scheme with a certain given level of security. More precisely, using nine different security notions for KEMs, ten for DEMs, and six for PKE schemes we completely characterize 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 relation among security notions for KEMs and DEMs.

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 amount of plaintext bits. This greatly limits their application since in practice one typically wants to efficiently encrypt large amounts of data. One way of solving this problem is by using a *hybrid encryption scheme* consisting of a (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 AES. This popular approach is often referred to as the "KEM/DEM paradigm" and was first formalized by Cramer and Shoup [23, 8].

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. Due to his simplicity and flexibility this modular approach is incorporated in many new standards for encryption (see, e.g., [24, 20, 9]) and many KEMs have been proposed in the literature (see, e.g., [22, 23, 8, 10, 6, 15]). 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) [21]. Cramer and Shoup [8] 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 KEM or DEM part and yet still obtain a chosen-ciphertext secure hybrid PKE scheme. This question is in particular motivated by the hybrid encryption scheme by Kurosawa and Desmedt [16, 1] which is chosen-ciphertext secure as a hybrid PKE scheme whereas its KEM part alone was recently shown not to be chosen-ciphertext secure [13]. A more general problem is to study the necessary and sufficient conditions for the KEM and the DEM part to obtain a hybrid PKE scheme that is secure with respect to possibly weaker notions (e.g., IND-CPA, NM-CCA1).

Overview of our main contribution. The main result of this paper is to solve the above open problem. We characterize the necessary and sufficient 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 paragraph) and the hierarchies implied by these notions. 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 not (by presenting a concrete counterexample).

To prove our results, we can in some places make use of established techniques [3, 14], whereas in other cases we need to introduce new proof machinery.

Considered security notions for KEMs, DEMs, and PKE schemes. Correcting problems we encountered in earlier attempts [17, 19], we propose a new notion of non-malleability for KEMs which we call *weak non-malleability* (wNM). In combination with the three standard attacks forms this leads to the respective notions of wNM-CPA, wNM-CCA1, and wNM-CCA2. Furthermore, we also consider a stronger notion of non-malleability that was independently proposed in a recent paper by Nagao, Manabe, and Okamoto [18] which we denote by *strong non-malleability* (sNM). Our nine considered notions for KEMs are therefore $\{\text{wNM}, \text{sNM}, \text{IND}\}$-$\{\text{CPA}, \text{CCA1}, \text{CCA2}\}$. Similar to [3] we provide a complete characterization of the relations between the above 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 [8] 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 $\{\text{NM}, \text{IND}\}$-$\{\text{OT}, \text{OTCCA}, \text{CPA}, \text{CCA1}, \text{CCA2}\}$. We provide a complete characterization of the relations between the above notions. This revisits and extends existing results by Katz and Yung [14] by considering a stronger (and arguably more natural) notion of non-malleability and by adding the attack form of OTCCA.

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].

We now discuss our results in more detail.

DEM KEM	IND-{OT, CPA, CCA1}	NM-{OT, CPA, CCA1}	IND-{OTCCA, CCA2}
{IND-CPA, wNM-CPA}	$\geq$ IND-CPA (5.1) $<$ IND-CCA1, NM-CPA	$\geq$ IND-CPA $<$ IND-CCA1, NM-CPA	$\geq$ IND-CPA $<$ IND-CCA1, NM-CPA
sNM-CPA	$\geq$ IND-CPA $<$ IND-CCA1, NM-CPA	$\geq$ NM-CPA (5.3) $<$ IND-CCA1	$\geq$ NM-CPA $<$ IND-CCA1 (5.7)
{IND-CCA1, wNM-CCA1, wNM-CCA2}	$\geq$ IND-CCA1 (5.1) $<$ NM-CPA	$\geq$ IND-CCA1 $<$ NM-CPA	$\geq$ IND-CCA1 $<$ NM-CPA (5.4)
sNM-CCA1	$\geq$ IND-CCA1 $<$ NM-CPA	$\geq$ NM-CCA1 (5.2) $<$ IND-CCA2	$\geq$ NM-CCA1 $<$ IND-CCA2 (5.8)
IND-CCA2	$\geq$ IND-CCA1 $<$ NM-CPA (5.5)	$\geq$ NM-CCA1 $<$ IND-CCA2 (5.6)	$\geq$ IND-CCA2 [8]

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.

1.1 Sufficient and necessary conditions for hybrid encryption

We give a characterization of the necessary and sufficient conditions required from the KEM and the DEM in order to achieve secure hybrid PKE schemes in Figure 1. 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 "$<$".

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 results from these key results, by using the security hierarchies of KEMs, DEMs and PKE schemes, i.e. the relations between the different security notions for each of these primitives (that are summarized in Figures 2, 3, and 4, respectively). Here positive results propagate to the right and down, whereas negative results propagate to the top and left. E.g., the fact that the PKE scheme resulting from a wNM-CCA1 KEM combined with a NM-CPA DEM is IND-CPA secure, can be deduced from its IND-CCA1 security.[1]

We now turn to a discussion of our main results from Figure 1. The first surprising fact is that it is possible to group notions for DEMs and KEMs that achieve exactly 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 reach the same level of security as with an IND-CCA1 DEM. Naïvely, one may expect that the proof of [8] carries over to show that a X-Y secure KEM in combination with a X-Y secure DEM also yields a X-Y secure hybrid scheme. This intuition is only true for X $\in$ {IND, sNM} (Theorems 5.1, 5.2 and 5.3) but it is wrong for X = wNM (Theorems 5.6 and 5.4). Most importantly, our table shows that the sufficient conditions on the KEM and the DEM in the composition theorem from [8] are also necessary: an

[1] All of our key results are unconditional. However, during propagation, some results may lose their unconditionality: e.g., IND-CPA KEM+IND-CPA DEM $<$ NM-CPA PKE is deduced from IND-CCA2 KEM + IND-CPA DEM $<$ NM-CPA PKE and hence implicitly assumes the existence of an IND-CCA2 secure KEM. This is standard practice, see, e.g., [3].

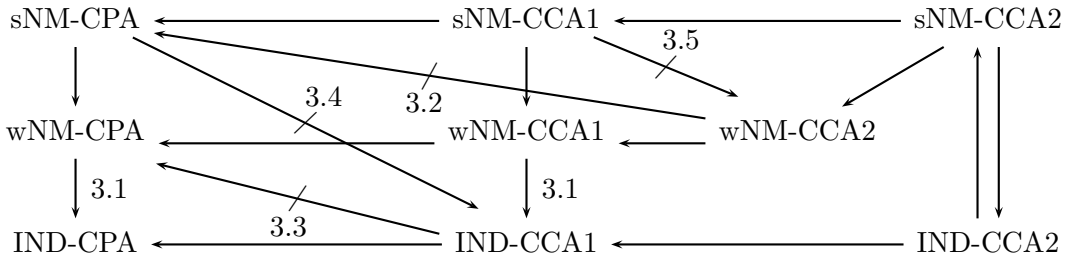

Figure 2: Implications and separations between the various security notions for KEMs. Here "$X \rightarrow Y$" means that X-security implies Y-security, and "$X \not\rightarrow Y$" means that X-security does not necessarily imply Y-security (i.e., that if there is at all a scheme which is X-secure, then there is also one which is X-secure, but not Y-secure). The characterization is complete, i.e. for each two notions either an implication or a separation can be derived from the diagram.

IND-CCA2 secure hybrid scheme can only be guaranteed if both, the KEM and the DEM, have the highest security level (i.e. IND-CCA2 for KEM and IND-OTCCA for DEM). Any attempt to weaken the KEM to wNM-CCA2/sNM CCA1 or the DEM to NM-CCA1 may yield a hybrid PKE scheme that is no longer IND-CCA2 (Theorems 5.4 / 5.8 and Theorem 5.6, 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 5.5 and 5.7).

On the positive side, an IND-CCA1 KEM and an IND-OT DEM already yields an IND-CCA1 hybrid scheme (Theorem 5.1). Furthermore, a sNM-CCA1 KEM plus a NM-OT DEM implies a NM-CCA1 hybrid scheme (Theorem 5.2).

For proving these results, we use new as well as established techniques: e.g., the proof of Theorem 5.5 basically transports a counterexample used in [3] to separate two security notions for public key encryption to the hybrid setting. Conversely, e.g., Theorems 5.7 and 5.8 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".

1.2 Security notions for Key Encapsulation Mechanisms and their relation

We revisit some previous attempts to define non-malleability for KEMs [17, 19] (denoted NM′) which we argue to have certain problems with the treatment of the key-space. (Furthermore we prove one of the main theorems of [17, 19] about the equivalence between the notions of IND-CCA2 and NM′-CCA2 to be wrong: we show that the Cramer-Shoup KEM [8] serves as an example of a KEM that is IND-CCA2 but not NM′-CPA in the sense of [17, 19].) Building on [11, 3] we revisit the security definitions of non-malleability for KEMs. Intuitively, in non-malleability, an adversary is given a challenge ciphertext and is considered to be successful if he is able to come up with a different ciphertext such that its decrypted key is "meaningfully related" to the challenge key [11]. In the concrete security experiment for PKE schemes (and DEMs) [3], an adversary against non-malleability first outputs a distribution of messages where the challenge message (which is later encrypted in the challenge ciphertext) is sampled from. This distribution may well be defined on two messages only. The situation is different for KEMs where the key-space is always implicitly fixed. This is the reason why in our definition of non-malleability for KEMs an adversary is not given control over the key-space (in contrast to what

was done in [17, 19]). These considerations lead to our new definition of non-malleability for KEMs, that we call wNM.

A different and stronger definition of non-malleability for KEMs (which we denote by sNM) has been independently proposed in [18] (also with the goal of correcting [17, 19]). The difference is that, roughly, in the non-malleability experiment the adversary is given some additional information containing the challenge key in clear. We give a complete characterization of the KEM hierarchy providing implications and separations between the nine different security notions $\{\text{IND}, \text{wNM}, \text{sNM}\}$-$\{\text{CPA}, \text{CCA1}, \text{CCA2}\}$. Our resulting hierarchy is depicted in Figure 2. By trivial reasons sNM always implies wNM. On the other hand we show that wNM-CCA2 does not even imply sNM-CPA. Here, a surprising result is that wNM-ATK strictly implies IND-ATK for $\text{ATK} \in \{\text{CPA}, \text{CCA1}\}$ whereas the opposite is the case for $\text{ATK} = \text{CCA2}$. This is analog to the case of DEMs (using the non-malleability definition from [14]) but in contrast to what happens with PKE schemes, where for CCA2 attacks indistinguishability is in fact equivalent to non-mealleability (cf. Figure 4). On the other hand, when the stronger notion sNM is considered, then this equivalence between sNM-CCA2 and IND-CCA2 is also valid for KEMs, as proved in [18].

Two different notions of non-malleability. There are two different definitions of non-malleability, wNM and sNM, and a priori it is not clear which one should be prefered over the other. We think that our definition of non-malleability (wNM) follows closer the original motivation from [11, 3]. On the other hand, the stronger definition from [18] seems to be more useful in practice: if we use the security of hybrid encryption as a natural assesment of a "good security notion" for non-malleability it seems desirable to have that non-malleability of the KEM and DEM implies non-malleability of the hyrbid PKE scheme. One of our results is that this is the case for the stronger definition sNM, whereas this is not true for wNM.

1.3 Security notions for Data Encapsulation Mechanisms and their relation

Katz and Yung [14] define 18 different security notions for DEMs and give a complete hierarchy of their relations. We consider eight of their notions ($\{\text{IND}, \text{NM}\}$-$\{\text{OT}, \text{CPA}, \text{CCA1}, \text{CCA2}\}$) and additionally add two more notions ($\{\text{IND}, \text{NM}\}$-OTCCA) where IND-OTCCA was originally introduced in [8]. The motivation of considering the additional notions comes from hybrid encryption paradigm: as showed in [8], IND-OTCCA security is sufficient for a DEM to yield an IND-CCA2 secure hybrid scheme when combined with an IND-CCA2 secure KEM. Here we consider a different and stronger notion of non-malleability which we think does more capture the original idea behind non-malleability [11] than the one from [14]. (In fact the scheme from [14, Proof of Theorem 7] whose ciphertext simply consist of the "authenticated plaintext" is non-malleable in the sense of [14] but is intuitively completely insecure.) We remark that this stronger notion of non-malleability is already mentioned (but not used) in [14].

We give a complete characterization of the DEM hierarchy providing implications and separations between the different security notions. Our resulting hierarchy is depicted in Figure 3. We remark that by using a stronger notion of non-malleability our hierarchy looks different from the one obtained in [14] (where NM-CCA2 was shown to be strictly weaker than IND-CCA2).

Even though the main result of this work is the characterization of the necessary and sufficient conditions for the security of hybrid PKE schemes, we think that our results concerning definitions and security hierarchies of KEMs and DEMs may be of independent interest.

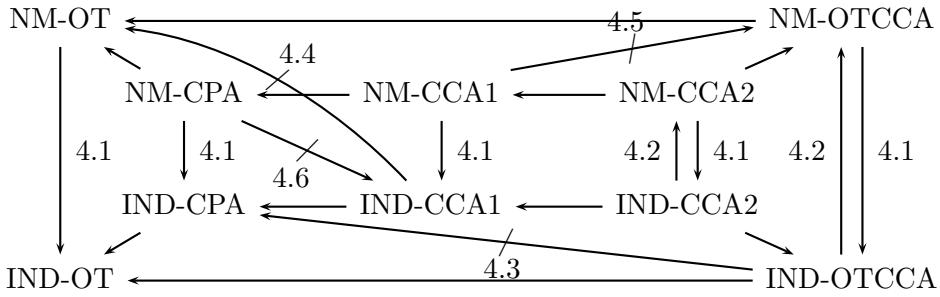

Figure 3: Implications and separations between the various security notions for DEMs.

1.4 Further results

There are many subtle issues to take into account when defining non-malleability [11, 4, 3]. For non-malleability one intuitively requires that, given a challenge ciphertext, the adversary can not come up with another vector of ciphertexts such that the plaintext vector relates to the challenge plaintext. Compared to the definition originally given in [3] we consider a stronger definition of non-malleability for PKE schemes, where the vector of ciphertexts may also contain invalid ciphertexts, that was also used in a recent update [5] of the electronic version of [4]. As an additional result we show a separation between the two notions of non-malleability for PKE schemes. In fact, (an extension of) our separation result has recently been integrated into [5].

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 set then $|S|$ denotes its size. If $k \in \mathbb{N}$ then 1^k denotes the string of k ones. 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

A *public key encryption* (PKE) scheme $\mathcal{PKE} = (\mathsf{PKE.Kg}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ consists of three polynomial-time algorithms. Via $(pk, sk) \xleftarrow{\$} \mathsf{PKE.Kg}(1^k)$ the randomized key-generation algorithm produces keys for security parameter $k \in \mathbb{N}$; via $C \xleftarrow{\$} \mathsf{PKE.Enc}(pk, m)$ a message m is encrypted under public key pk, producing a ciphertext C; via $\{m, \perp\} \leftarrow \mathsf{PKE.Dec}(sk, C)$ the possessor of secret key sk decrypts ciphertext C to get back a message or receives the special symbol $\perp$ that stands for rejection.

For consistency, we require $\Pr[\,\mathsf{PKE.Dec}(sk, \mathsf{PKE.Enc}(pk, m)) = m\,] = 1$ for all $k \in \mathbb{N}$ and all message m, where the probability is taken over the choice of $(pk, sk) \xleftarrow{\$} \mathsf{PKE.Kg}(1^k)$ and the

coins of all the algorithms in the expression above.[2]

2.1.1 PKE Indistinguishability

Definition 2.1 Let $\mathcal{PKE} = (\mathsf{PKE.Kg}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ be a public-key encryption scheme and let $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ be an adversary. For $atk \in \{cpa, cca1, cca2\}$, we define the advantage of $\mathcal{F}$ as

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

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

$$\begin{array}{l}\textbf{Experiment } \mathbf{Exp}^{pke\text{-}ind\text{-}atk\text{-}b}_{\mathcal{PKE},\mathcal{F}}(k)\\ \quad (pk, sk) \xleftarrow{\$} \mathsf{PKE.Kg}(1^k)\\ \quad (St, m_0, m_1) \xleftarrow{\$} \mathcal{F}_1^{\mathtt{DEC}_1(\cdot)}(pk)\\ \quad C^* \xleftarrow{\$} \mathsf{PKE.Enc}(pk, m_b)\\ \quad b' \xleftarrow{\$} \mathcal{F}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)\\ \quad \text{Return } b'\end{array}$$

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

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

with the restriction that $\mathcal{F}_2$ is not allowed to query the oracle $\mathtt{DEC}_2(\cdot)$ on the target ciphertext C^*.

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 $\mathcal{F}$.

2.1.2 PKE Non-Malleability

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 $1 \le i \le |\mathbf{C}|$. 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 [11] and subsequently refined [3, 12]. The goal of an adversary in an 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 K, where K is the key that corresponds to 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

[2] Relaxations are possible, see, e.g., [12, Comments after Def. 5.1.1], and do not affect our results.

of an adversary. We will use the definition from [3] which considers an experiment involving the adversary.

Let $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ be an adversary. In the first stage of the attack $\mathcal{F}_1$ gets the public key pk and returns a description of a message space, described by a *message sampling algorithm* $\mathcal{M}$. (The message space must be valid, i.e. it gives non-zero probability only to strings of one particular length.) In the second stage of the attack $\mathcal{F}_2$ obtains an encryption C of a message M_1 which is drawn randomly using the message sampling algorithm $\mathcal{M}$. Then adversary $\mathcal{F}_2$ returns a ciphertext vector $\mathbf{C}$ together with a relation R. The adversary hopes that $R(M_1, \mathbf{M})$ is different from $R(M_0, \mathbf{M})$ for an independently uniformly chosen $M_0 \in \mathcal{M}$, where $\mathbf{M} \leftarrow \mathsf{PKE.Dec}(sk, \mathbf{C})$. We thus say that $\mathcal{F}$ is successful if $R(M_1, \mathbf{M})$ holds with probability significantly different than $R(M_0, \mathbf{M})$. The restriction to $\mathcal{F}$'s output is that $C \notin \mathbf{C}$ and that R is polynomial-time computable.

Definition 2.2 Let $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ be an adversary. For $atk \in \{cpa, cca1, cca2\}$, we define the advantage of $\mathcal{F}$ as

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

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

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

and the oracles $\mathtt{DEC}_1$ and $\mathtt{DEC}_2$ are defined as in Definition 2.1, again with the restriction that $\mathcal{A}_2$ is not allowed to query $\mathtt{DEC}_2$ for C^*. In the experiment $\mathcal{M}$ is again a probability distribution on the space of messages, and $m \xleftarrow{\$} \mathcal{M}$ denotes the choice of a message following this distrubtion. We insist that $\mathcal{M}$ is valid, i.e. that $|M_0| = |M_1|$ for any M_0, M_1 that are given non-zero probability in $\mathcal{M}$.

A public key encryption scheme $\mathcal{PKE}$ is said to be *non-malleable against* ATK *attacks* (NM-ATK) if the advantage function $\mathbf{Adv}^{pke\text{-}nm\text{-}atk}_{\mathcal{PKE},\mathcal{F}}(k)$ is a negligible function in k for all polynomial-time adversaries $\mathcal{F}$.

Differences to the definition from [3]. In contrast to [3] (and following [12]) we do not require the ciphertexts in $\mathbf{C}$ to be valid. In particular this also includes the case where all ciphertexts $\mathbf{C}[i]$ may decrypt to $\perp$. If some ciphertexts are valid and others are not, the adversary may be taking some action on the valid ones. This makes the definition (strictly) stronger and captures more the intuitive idea behind non-malleability.

The recent update [5] of the electronic version of [4] also considers and relates two definitions of non-malleability, each of them in a version in which the adversary automatically "loses" if $\mathbf{C}$ contains an invalid ciphertext (these notions are called SNM-ATK* resp. CNM-ATK* in [5]), and in more relaxed versions like the one we focus on here (called SNM-ATK resp. CNM-ATK in [5]). With these formalizations, we can prove that actually CNM-CPA is strictly stronger

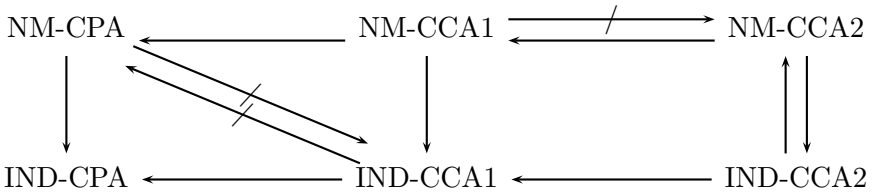

Figure 4: Implications and separations between the various security notions for PKE schemes from [3].

---

than CNM-CPA*, using the example in Appendix A. Actually, [5] gives an extension to the example from Appendix A that shows that not even CNM-CCA1* implies CNM-CPA.

We stress that all the results from [3] are still valid with respect to our stronger non-malleability notion. Furthermore we also allow the adversary to output empty ciphertext vectors $\mathbf{C} = \varepsilon$. Since an adversary is given the possibility to encrypt this is clearly equivalent to not allowing empty ciphertext vectors in the public-key setting. But it will turn out to be a crucial detail for the case of symmetric encryption.

The relations among all these different security notions for public key encryption schemes were established in [3]. They are summarized in Figure 4.

2.2 Public Key Encapsulation Mechanisms

A *public-key encapsulation mechanism* $\mathcal{KEM} = (\mathsf{KEM.Kg}, \mathsf{KEM.Enc}, \mathsf{KEM.Dec})$ with associated key-space $\mathsf{KeySp}(k)$ (which we assume to be $\mathsf{KeySp}(k) = \{0,1\}^{kl(k)}$, where $kl(k)$ is the key-length) consists of three polynomial-time algorithms. Via $(pk, sk) \xleftarrow{\$} \mathsf{KEM.Kg}(1^k)$ the randomized key-generation algorithm produces keys for security parameter $k \in \mathbb{N}$; via $(K, C) \xleftarrow{\$} \mathsf{KEM.Enc}(1^k, pk)$, a key $K \in \mathsf{KeySp}(k)$ together with a ciphertext C is created; via $\{K, \perp\} \leftarrow \mathsf{KEM.Dec}(sk, C)$ the possessor of secret key sk decrypts ciphertext C to get back a key or the rejection symbol $\perp$. 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.

2.2.1 KEM Indistinguishability

The notion of indistinguishablity of KEMs against CCA2 attacks was established in [8]. Using the ideas from Section 2.1 it is straightforward to also extend it to CPA and CCA1 attacks.

Definition 2.3 Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary. For $atk \in \{cpa, cca1, cca2\}$, we define the advantage of $\mathcal{A}$ as

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

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

Experiment $\mathbf{Exp}^{kem\text{-}ind\text{-}atk\text{-}b}_{\mathcal{KEM},\mathcal{A}}(k)$

$(pk, sk) \xleftarrow{\$} \mathsf{KEM.Kg}(1^k)$
$St \xleftarrow{\$} \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$
$K_0^* \xleftarrow{\$} \mathsf{KeySp}(k)\ ;\ (K_1^*, C^*) \xleftarrow{\$} \mathsf{KEM.Enc}(pk)$
$K^* \leftarrow K_b^*$
$b' \xleftarrow{\$} \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(pk, C^*, K^*, St)$
Return b'

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

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

with the restriction that $\mathcal{A}$ is not allowed to query $\mathtt{DEC}_2(\cdot)$ on the target ciphertext C^*.

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

2.2.2 KEM Non-Malleability

Defining non mealleability for KEMs needs some care and it turns out that an existing definition from [17, 19] has a problem in the treatment of the key-space (more details are given in Appendix B). 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 over $\{0,1\}^k$, just as $\mathsf{KEM.Enc}(pk)$ should do.

Definition 2.4 Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary. For $atk \in \{cpa, cca1, cca2\}$, we define the advantage of $\mathcal{A}$ as

$$\mathbf{Adv}^{kem\text{-}wnm\text{-}atk}_{\mathcal{KEM},\mathcal{A}}(k) \;=\; \left|\Pr\left[\mathbf{Exp}^{kem\text{-}wnm\text{-}atk\text{-}1}_{\mathcal{KEM},\mathcal{A}}(k) = 1\right] - \Pr\left[\mathbf{Exp}^{kem\text{-}wnm\text{-}atk\text{-}0}_{\mathcal{KEM},\mathcal{A}}(k) = 1\right]\right| ,$$

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

Experiment $\mathbf{Exp}^{kem\text{-}wnm\text{-}atk\text{-}b}_{\mathcal{KEM},\mathcal{A}}(k)$

$(pk, sk) \xleftarrow{\$} \mathsf{KEM.Kg}(1^k)$
$St \xleftarrow{\$} \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$
$K_0^* \xleftarrow{\$} \mathsf{KeySp}(k)\ ;\ (K_1^*, C^*) \xleftarrow{\$} \mathsf{KEM.Enc}(pk)$
$(R, \mathbf{C}) \xleftarrow{\$} \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$
$\mathbf{K} \leftarrow \mathsf{KEM.Dec}(sk, \mathbf{C})$
If $C^* \notin \mathbf{C}$ and $R(K_b^*, \mathbf{K})$ then return 1 else return 0

and the oracles $\texttt{DEC}_1$ and $\texttt{DEC}_2$ are defined as in Definition 2.3.

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

A stronger definition of non-malleability for KEMs. Nagao, Manabe, and Okamoto [18] independently proposed a different and stronger definition of non-malleability. The difference is that in the non-mealleability security experiment the adversary $\mathcal{A}_2$ is given additional information in form of the tuple X, where X consists of the elements K_0^* and K_1^* in a random order. More precisely, the input of adversary $\mathcal{A}_2$ is replaced with (C^*, X, St), where $X \xleftarrow{\$} (K_c^*, K_{1-c}^*)$ for a random bit c that is hidden from $\mathcal{A}$. We call the resulting notion *strong non-malleability against* ATK *attacks* (sNM-ATK). Trivially, we have that sNM-ATK security implies wNM-ATK security, for ATK $\in \{\text{CPA}, \text{CCA1}, \text{CCA2}\}$.

2.3 Data Encapsulation Mechanisms

A (stateless) *data encapsulation mechanism* $\mathcal{DEM} = (\mathsf{DEM.Kg}, \mathsf{DEM.Enc}, \mathsf{DEM.Dec})$ consists of three polynomial-time algorithms. Via $K \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$ the randomized key-generation algorithm produces a uniformly distributed key $K \in \{0,1\}^k$ for security parameter $k \in \mathbb{N}$; via $C \xleftarrow{\$} \mathsf{DEM.Enc}(K, m)$ a message m is encrypted under the key K; via $\{M, \perp\} \leftarrow \mathsf{DEM.Dec}(K, C)$ a possessor of the key K decrypts the ciphertext C to get back a message or the special rejection symbol $\perp$. For consistency, we require that for all $k \in \mathbb{N}$, and all message 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.

2.3.1 DEM Indistinguishability

It is well known how to define indistinguishability against CPA, CCA1, and CCA2 attacks for DEMs [2]. The important fact to notice is that in the security definition of CPA for DEMs an adversary is also given access to an encryption oracle. This models the ability of the adversary to encrypt arbitrary messages under the (unknown) symmetric key. Note that this encryption oracle was not neccessary for the case of public-key encryption since there the knowledge of the public key is sufficient to perform encryption of arbitrary messages.

We consider two more attack forms which we call one-time attacks (OT) and one-time (adaptive) chosen-ciphertext attacks (OTCCA). OT attacks correspond to *passive attacks* and OTCCA attacks correspond to *adaptive chosen-ciphertext attacks* in [8, Sec 7.2.1]. More concretely, OT attacks are CPA attacks where the adversary is not given an encryption oracle. OTCCA attacks are OT attacks where in the second stage the adversary is given access to a decryption oracle. Note that in one-time attacks the adversary is not given an encryption oracle, nor is he given any oracle access in the first stage.

Definition 2.5 Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be an adversary. For $atk \in \{ot, otcca, cpa, cca1, cca2\}$, define the advantage of $\mathcal{B}$ 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 $\mathbf{Exp}^{\textit{dem-ind-atk-b}}_{\mathcal{DEM},\mathcal{B}}(k)$
$K \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$
$(St, M_0, M_1) \xleftarrow{\$} \mathcal{B}_1^{\mathtt{ENC}(\cdot),\mathtt{DEC}_1(\cdot)}(1^k)$
$C^* \xleftarrow{\$} \mathsf{DEM.Enc}(K, M_b)$
$b' \xleftarrow{\$} \mathcal{B}_2^{\mathtt{ENC}(\cdot),\mathtt{DEC}_2(\cdot)}(C^*, St)$
Return b'

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

	$\mathtt{ENC}(\cdot)$	$\mathtt{DEC}_1(\cdot)$	$\mathtt{DEC}_2(\cdot)$
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^*.

A data encapsulation mechanism $\mathcal{DEM}$ is said to be *indistinguishable against* ATK *attacks* (IND-ATK) if the advantage function $\mathbf{Adv}^{\textit{dem-ind-atk}}_{\mathcal{DEM},\mathcal{B}}(k)$ is a negligible function in k for all polynomial-time adversaries $\mathcal{B}$.

For clarification we note that in [14] different natation 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.

2.3.2 DEM Non-Malleability

Definition 2.6 Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be an adversary. For $\textit{atk} \in \{\textit{ot}, \textit{otcca}, \textit{cpa}, \textit{cca1}, \textit{cca2}\}$, we define the advantage of $\mathcal{B}$ as

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

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

Experiment $\mathbf{Exp}^{\textit{dem-nm-atk-b}}_{\mathcal{DEM},\mathcal{B}}(k)$
$K \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$
$(St, \mathcal{M}) \xleftarrow{\$} \mathcal{B}_1^{\mathtt{ENC}(\cdot),\mathtt{DEC}_1(\cdot)}(1^k)$
$m_0^*, m_1^* \xleftarrow{\$} \mathcal{M}\,;\; C^* \xleftarrow{\$} \mathsf{DEM.Enc}(K, m_1^*)$
$(R, \mathbf{C}) \xleftarrow{\$} \mathcal{B}_2^{\mathtt{ENC}(\cdot),\mathtt{DEC}_2(\cdot)}(C^*, St)$
$\mathbf{M} \leftarrow \mathsf{DEM.Dec}(K, \mathbf{C})$
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 Definition 2.5. 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.

Note that as in the previous definitions, we allow invalid ciphertexts in $\mathbf{C}$ as well as an empty $\mathbf{C}$. This leads to a relatively strict definition of non-malleability, but we think that this best reflects the intuition behind. 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, e.g., 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 w.r.t. a non-malleability notion that requires the adversary to come up with a valid, non-empty ciphertext vector. (In fact, this is precisely the example from [14, Proof of Theorem 7].) We believe that this "security" is intuitively not justified.

A data encapsulation mechanism $\mathcal{DEM}$ is said to be *non-malleable against* ATK *attacks* (NM-ATK) if the advantage function $\mathbf{Adv}^{dem\text{-}nm\text{-}atk}_{\mathcal{DEM},\mathcal{B}}(k)$ is a negligible function in k for all polynomial-time adversaries $\mathcal{B}$.

Existence of DEMs. It is well known that a one-time pad [25] is an IND-OT DEM that therefore exist unconditionally. Also, by adding a one-time MAC to an arbitrary IND-OT DEM, we obtain an IND-OTCCA DEM [8]. Thus, IND-OTCCA DEMs also exist unconditionally. See also [14] for a direct construction of a DEM unconditionally secure in the sense of IND-OTCCA.

On the other hand, IND-CPA/IND-CCA2 secure DEMs are only known to exist on the assumption that one-way functions exist. This was first explicitly noted in [11].

3 Relations among Key Encapsulation Mechanisms

We state more formally the results summarized in Figure 2 and provide proofs. One would expect that all proofs from the PKE setting carry more or less over to the KEM setting. This is only the case for the stronger notion sNM of non-malleability, but not if we consider the weaker notion of wNM (recall that sNM-ATK security implies wNM-ATK security, for ATK $\in$ $\{\text{CPA}, \text{CCA1}, \text{CCA2}\}$). Namely, as it happens in the PKE setting, sNM-CCA2 and IND-CCA2 are equivalent notions, as it has been proved in [18]. On the other hand, we will show that wNM-CCA2 security does not even imply sNM-CPA security. These two results directly imply that wNM-CCA2 is strictly weaker than IND-CCA2 for KEMs.

Our first results shows that for KEMs, wNM implies IND for CPA and CCA1 attacks. Interestingly the proof from [11, 3] does not carry over to the case of KEMs. The proof of the following is in Section 3.1 and uses techniques different from [3].

Theorem 3.1 [wNM-CPA $\Rightarrow$ IND-CPA, wNM-CCA1 $\Rightarrow$ IND-CCA1] If a KEM is secure in the sense of wNM-ATK then it is secure in the sense of IND-ATK, for ATK $\in \{\text{CPA}, \text{CCA1}\}$.

The next result (proved in Section 3.2) shows that wNM-CCA2 does not even imply sNM-CPA. This in particular shows that for KEMs IND-CCA2 is strictly stronger than wNM-CCA2. This is in sharp contrast to PKE schemes and DEMs (cf. Figure 4 and Figure 3).

Theorem 3.2 [wNM-CCA2 $\not\Rightarrow$ sNM-CPA] If there exists a scheme $\mathcal{KEM}$ which is secure in the sense of wNM-CCA2, then there exists a scheme $\mathcal{KEM}'$ which is secure in the sense of wNM-CCA2 but which is not secure in the sense of sNM-CPA.

The following shows that IND-CCA1 does not imply wNM-CPA for KEMs. The proof of the following uses a modified version of the separation example from [3, Theorem 3.5] and is given in Section 3.3.

Theorem 3.3 [IND-CCA1 $\not\Rightarrow$ wNM-CPA] If there exists a scheme $\mathcal{KEM}$ which is secure in the sense of IND-CCA1, then there exists a scheme $\mathcal{KEM}'$ which is secure in the sense of IND-CCA1 but which is not secure in the sense of wNM-CPA.

The proof of the following uses (an adaptation of) the separation example from [3, Theorem 3.6] for PKE schemes and is omitted here.

Theorem 3.4 [sNM-CPA $\not\Rightarrow$ IND-CCA1] If there exists a scheme $\mathcal{KEM}$ which is secure in the sense of sNM-CPA, then there exists a scheme $\mathcal{KEM}'$ which is secure in the sense of sNM-CPA but which is not secure in the sense of IND-CCA1.

The proofs of the following theorem uses (an adaptation to the KEM setting of) the separation example from [3, Theorem 3.7] for PKE schemes, and is omitted here.

Theorem 3.5 [sNM-CCA1 $\not\Rightarrow$ wNM-CCA2] If there exists a scheme $\mathcal{KEM}$ which is secure in the sense of sNM-CCA1, then there exists a scheme $\mathcal{KEM}'$ which is secure in the sense of sNM-CCA1 but which is not secure in the sense of wNM-CCA2.

3.1 Proof of Theorem 3.1: wNM-CPA $\Rightarrow$ IND-CPA, wNM-CCA1 $\Rightarrow$ IND-CCA1

Assume $\mathcal{KEM}$ is secure in thewNM-ATK sense for ATK $\in \{\text{CPA}, \text{CCA1}\}$. 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 $\mathcal{KEM}$. We have to show that $\mathbf{Adv}^{\textit{kem-ind-atk}}_{\mathcal{KEM},\mathcal{B}}(\cdot)$ is negligible. To this end we will describe a wNM-ATK adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ attacking $\mathcal{KEM}$.

The intuition is that adversary $\mathcal{A}_2$ defines its relation $R(\cdot)$ using adversary $\mathcal{B}_2$ as a (black-box) algorithm. More precisely, the relation is defined on the empty key vector $\mathbf{K} = \varepsilon$ and only takes one key K as input. $R(K, \varepsilon)$ is defined as the output of $\mathcal{B}_2$ on key K, where $\mathcal{A}_2$'s challenge ciphertext C^*, as well as the public key pk, and $\mathcal{A}_2$'s randomness are hard-coded into $\mathcal{B}_2$.

Alg. $\mathcal{A}_1^{\mathtt{DEC}_1}(pk)$	**Alg.** $\mathcal{A}_2(pk, C^*, St)$
$St \xleftarrow{\$} \mathcal{B}_1^{\mathtt{DEC}_1}(pk)$	Define $R(K) = \mathcal{B}_2(pk, C^*, K, St)$
Return St	Return $(\mathbf{C} = \varepsilon, R)$

In the CCA1 case, adversaries $\mathcal{A}_1$ and $\mathcal{B}_1$ have access to an oracle $\mathtt{DEC}_1$, where $\mathcal{A}_1$ forwards $\mathcal{B}_1$'s oracle queries to its oracle $\mathtt{DEC}_1$.

Note that $\mathcal{A}_2$ outputs an empty ciphertext vector $\mathbf{C} = \varepsilon$. In the definition of the relation R made by $\mathcal{A}_2$ the values pk, C^*, St, and some randomness are hardcoded into R. Note that $R(K)$ is only defined on the challenge key K and the target ciphertext vector returned by $\mathcal{A}_2$ is empty. If $\mathcal{B}$ is a PPT adversary then the relation $R(\cdot)$ is polynomial time computable.

Claim 3.6 For $b \in \{0, 1\}$, $\Pr\left[\mathbf{Exp}^{\textit{kem-wnm-atk-b}}_{\mathcal{KEM},\mathcal{A}}(k) = 1\right] = \Pr\left[\mathbf{Exp}^{\textit{kem-ind-atk-b}}_{\mathcal{KEM},\mathcal{B}}(k) = 1\right]$

Proof: Consider the output of $\mathcal{A}_2$. Note that the relation over K_b holds if and only if $\mathcal{B}_2$ returns one, i.e. if $\mathcal{B}_2$ thinks that $K^* = K_b$ fits to the challenge ciphertext C^*. This exactly coincides with the non-malleability experiment of $\mathcal{A}$. In case $b = 1$, $\mathcal{B}$ does this correctly with probability $\Pr\left[\mathbf{Exp}^{\textit{kem-ind-atk-1}}_{\mathcal{KEM},\mathcal{B}}(k) = 1\right]$ and therefore the relation holds with exactly the same probability showing that $\Pr\left[\mathbf{Exp}^{\textit{kem-wnm-atk-1}}_{\mathcal{KEM},\mathcal{A}}(k) = 1\right] = \Pr\left[\mathbf{Exp}^{\textit{kem-ind-atk-1}}_{\mathcal{KEM},\mathcal{B}}(k) = 1\right]$. The same argument holds for the case $b = 0$. ∎

Now we can apply the claim to obtain $\mathbf{Adv}^{\textit{kem-ind-atk}}_{\mathcal{KEM},\mathcal{B}}(k) = \mathbf{Adv}^{\textit{kem-wnm-atk}}_{\mathcal{KEM},\mathcal{A}}(k)$. Since $\mathcal{KEM}$ is secure in the sense of wNM-ATK we know that $\mathbf{Adv}^{\textit{kem-wnm-atk}}_{\mathcal{KEM},\mathcal{A}}(k)$ is negligible and hence $\mathbf{Adv}^{\textit{kem-ind-atk}}_{\mathcal{KEM},\mathcal{B}}(k)$ is negligible, too.

3.2 Proof of Theorem 3.2: wNM-CCA2 $\not\Rightarrow$ sNM-CPA

As a technical tool, we first provide an equivalent formulation of the sNM notion for $\mathcal{KEM}$s. This notion of *non-malleability under parallel chosen-ciphertext attacks* was introduced in [4] for the PKE setting, and extended to the KEM setting in [18].

Definition 3.7 Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ be an adversary. For $atk \in \{cpa, cca1, cca2\}$, we define the advantage of $\mathcal{A}$ as

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

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

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

and the oracles $\mathtt{DEC}_1$ and $\mathtt{DEC}_2$ are defined as in Definition 2.3.

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 [18] that (a slightly different but equivalent formulation of) PNM-ATK is equivalent to sNM-ATK for ATK $\in \{\text{CPA}, \text{CCA1}, \text{CCA2}\}$. In the current proof, we are going to use therefore the PNM-CPA notion instead of the equivalent sNM-CPA notion.

Assume there exists a wNM-CCA2 secure scheme $\mathcal{KEM} = (\mathsf{KEM.Kg}, \mathsf{KEM.Enc}, \mathsf{KEM.Dec})$ with key-space $\{0,1\}^c$ for some function $c = c(k)$ such that the length of the key-space 2^c is super-polynomial in k.

We modify $\mathcal{KEM}$ into a new KEM $\mathcal{KEM}' = (\mathsf{KEM'.Kg}, \mathsf{KEM'.Enc}, \mathsf{KEM'.Dec})$ which is still secure in the sense of wNM-CCA2 but not secure in the sense of PNM-CPA. We split the keys generated by $\mathsf{KEM.Enc}$ in two parts of the same length $c/2$ (we assume c to be even for simplicity), denoting this fact as $K = K_1||K_2$. Concretely, we set $\mathsf{KEM'.Kg} = \mathsf{KEM.Kg}$ and

Alg. $\mathsf{KEM'.Enc}(pk)$	**Alg.** $\mathsf{KEM'.Dec}(sk, C_1'||C_2')$
$(K_1||K_2, C_1) \xleftarrow{\$} \mathsf{KEM.Enc}(pk)$	$K_1||K_2 \xleftarrow{\$} \mathsf{KEM.Dec}(sk, C_1')$
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

Claim 3.8 $\mathcal{KEM}'$ is not secure in the sense of PNM-CPA.

Proof: In the PNM-CPA game the adversary $\mathcal{A}_2$ gets the challenge ciphertext $C^* = C_1^*||\perp$, together with a key $K^* = K_1||K_2$. The goal of the adversary is to guess if the key K^* is the

one encapsulated in C^* (i.e. $d = 1$) or if it is a random key (i.e. $d = 0$). To do this, the adversary can choose a vector of ciphertexts $\mathbf{C}$ to be decrypted. In this case, $\mathcal{A}_2$ chooses a single ciphertext to be decrypted, which is $C_1^*||K_2$. The result of decrypting this ciphertext, $K' = \mathsf{KEM}'.\mathsf{Dec}(sk, C_1^*||K_2)$, is taken as input by $\mathcal{A}_3$. If $K' = \perp$ then $\mathcal{A}_3$ returns $d' = 0$; otherwise, $\mathcal{A}_3$ returns $d' = 1$.

Note that the final output of $\mathcal{A}_3$ is incorrect only if the key $K^* = K_1||K_2$ received by $\mathcal{A}_2$ is not the key encapsulated in C^* (that is, if K^* is a random key, independent from C^*) but on the other hand the second half of the key, K_2, is equal to the second half of the key encapsulated in C^*. This happens with negligible probability; therefore, we have that the advantage $\mathbf{Adv}^{kem\text{-}pnm\text{-}atk}_{\mathcal{KEM}',\mathcal{A}}(k)$ is almost 1 in this case, meaning that $\mathcal{KEM}'$ is not PNM-CPA secure. ∎

Claim 3.9 $\mathcal{KEM}'$ is secure in the sense of wNM-CCA2.

Proof: Assume to the contrary that there exists a successful wNM-CCA2 adversary $\mathcal{A}' = (\mathcal{A}'_1, \mathcal{A}'_2)$ against $\mathcal{KEM}'$. Then we can use it to construct a successful wNM-CCA2 adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ against $\mathcal{KEM}$ (leading therefore to a contradiction), as follows. In the first stage $\mathcal{A}_1$ receives a public key pk, then it initializes $\mathcal{A}'$ by sending the same pk to $\mathcal{A}'_1$. When $\mathcal{A}'$ makes a decapsulation query to the oracle $\mathsf{KEM}'.\mathsf{Dec}(sk, \cdot)$ for a ciphertext $C' = C'_1||C'_2$, adversary $\mathcal{A}_1$ makes the query $C = C'_1$ to its oracle $\mathsf{KEM}.\mathsf{Dec}(sk, \cdot)$, obtaining as answer $K_1||K_2$. If $C'_2 = K_2$ or $C'_2 = \perp$, then $\mathcal{A}_1$ sends $K_1||K_2$ to $\mathcal{A}'_1$; otherwise it sends $\perp$ to $\mathcal{A}'_1$. We now describe $\mathcal{A}_2$ and $\mathtt{DEC}'_2$.

Alg. $\mathcal{A}_2^{\mathtt{DEC}_2}(C^*, St)$
- $(\mathbf{C}', R') \xleftarrow{\$} \mathcal{A}_2'^{\mathtt{DEC}'_2}(C^*||\perp, St)$
- For $i \in \{1, \ldots, |\mathbf{C}'|\}$ do
  - Parse $\mathbf{C}'[i]$ as $C_i||T_i$
  - $\mathbf{C}[i] \leftarrow C_i$ if $C_i \neq C^*$
  - $\mathbf{C}[i] \leftarrow \perp$ otherwise
- Define $R(K, \mathbf{K})$ as $R'(K, \mathbf{K}')$, where
  - $\mathbf{K}'[i] \leftarrow \mathbf{K}[i]$ if $C_i \neq C^*$,
  - $\mathbf{K}'[i] \leftarrow \perp$ otherwise.
- Return $(\mathbf{C}, R)$

Alg. $\mathtt{DEC}_2'^{\mathtt{DEC}_2}(C')$
- Parse $C' = C'_1||C'_2$
- If $C'_1 = C^*$ then $K \leftarrow \perp$
  - else $K \xleftarrow{\$} \mathtt{DEC}_2(C'_1)$
- return K

After this first phase, $\mathcal{A}_2$ receives a challenge ciphertext C^*, which encapsulates some key $K^* = (K_1^*, K_2^*)$. We define the two events in the above execution of adversary $\mathcal{A}'$.

$$\mathbf{E_1}: \quad C'_2 = K_2^* \text{ for a query } C' = C'_1||C'_2 \text{ to } \mathtt{DEC}'_2(\cdot).$$
$$\mathbf{E_2}: \quad T_i = K_2^* \text{ for an index } 1 \leq i \leq |\mathbf{C}'|.$$

Let $\mathbf{E} = \mathbf{E_1} \vee \mathbf{E_2}$.

We claim that unless event $\mathbf{E}_1$ happens adversary $\mathcal{A}$ perfectly simulates the view of $\mathcal{A}'$. To verify this consider a query $C' = C'_1||C'_2$ made to $\mathtt{DEC}'_2$. The interesting case to consider is $C'_1 = C^*$. Note that $C' \neq C'^*$ and $C'_1 = C^*$ imply $C'_2 \neq \perp$. Therefore the only case where the answer $\perp$ is invalid would be $C'_2 = K_2^*$.

Furthermore it is easy to verify that unless $\mathbf{E_2}$ happens, adversary $\mathcal{A}$ translates a correct ciphertext/relation pair $(\mathbf{C}', R')$ for $\mathcal{KEM}'$ into a correct ciphertext/relation pair $(\mathbf{C}, R)$ for $\mathcal{KEM}$, i.e. we have $R'(\mathbf{K}') \Leftrightarrow R(\mathbf{K})$.

Thus,

$$\Pr\left[\mathbf{Exp}^{\textit{kem-wnm-cca2-b}}_{\mathcal{KEM}',\mathcal{A}'}(k)=1|\neg\mathbf{E}\right]=\Pr\left[\mathbf{Exp}^{\textit{kem-wnm-cca2-b}}_{\mathcal{KEM},\mathcal{A}}(k)=1|\neg\mathbf{E}\right] \quad (1)$$

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

Lemma 3.10 There exists a PPT adversary $\mathcal{B}$ against the wNM-CCA2 security of $\mathcal{KEM}$ such that $\mathbf{Adv}^{\textit{kem-wnm-cca2}}_{\mathcal{KEM},\mathcal{B}}\geq \Pr[\mathbf{E}]/q(k)-2^{-c/2}$ for some polynomial $q(k)$.

Proof: Adversary $\mathcal{B}$ is defined like $\mathcal{A}$ with the difference that $\mathcal{B}$ uses the K_2^* part of the output of $\mathcal{A}$ (from either the queries to $\mathtt{DEC}_2'$ or from $\mathbf{C}'$) to break the non-malleability of $\mathcal{KEM}$. More precisely, $\mathcal{B}$ chooses in the beginning a random integer $j\in\{1,\ldots,q(k)\}$, where $q(k)=q_1(k)+q_2(k)$ and $q_1(k)$ is an upper bound on the number of decapsulation queries $\mathcal{A}'$ makes and $q_2(k)$ is an upper bound on the length of the ciphertext vector $\mathbf{C}'$ output by $\mathcal{A}'$.
The integer j corresponds to the (guessed) appearance of K_2^* in the queries of $\mathcal{A}'$. If $i\leq q_1$ then it uses the C_2' of the ith decapsulation query to break the wNM-CCA2 security of $\mathcal{KEM}$. If $i>q_1$ then it uses T_{i-q_1} from $\mathbf{C}'$ returned by $\mathcal{A}'$ to break the wNM-CCA2 security of $\mathcal{KEM}$. By definition of event $\mathbf{E}$ and since i is chosen uniformly and independently, we have that K_2^* is guessed correctly with probability at least $\Pr[\mathbf{E}]/q(k)$. Finally adversary $\mathcal{B}$ returns $(\mathbf{C},R)$, where $\mathbf{C}=\epsilon$ and $R(K)$ returns true iff $K=K_2^*$. This implies $\Pr\left[\mathbf{Exp}^{\textit{kem-wnm-cca2-1}}_{\mathcal{KEM},\mathcal{B}}(k)=1\right]\geq \Pr[\mathbf{E}]/q(k)$ and $\Pr\left[\mathbf{Exp}^{\textit{kem-wnm-cca2-0}}_{\mathcal{KEM},\mathcal{B}}(k)=1\right]=2^{-c/2}$. This proves the lemma by observing

$$\begin{aligned}\mathbf{Adv}^{\textit{kem-wnm-cca2}}_{\mathcal{KEM},\mathcal{B}} &= \Pr\left[\mathbf{Exp}^{\textit{kem-wnm-cca2-1}}_{\mathcal{KEM},\mathcal{B}}(k)=1\right]-\Pr\left[\mathbf{Exp}^{\textit{kem-wnm-cca2-0}}_{\mathcal{KEM},\mathcal{B}}(k)=1\right]\\ &\geq \Pr[\mathbf{E}]/q(k)-2^{c/2}\,.\end{aligned}$$

∎

Using the previous lemma and (1), we complete the proof with

$$\begin{aligned}\mathbf{Adv}^{\textit{kem-wnm-cca2}}_{\mathcal{KEM}',\mathcal{A}'} &\leq |\Pr\left[\mathbf{Exp}^{\textit{kem-wnm-cca2-1}}_{\mathcal{KEM}',\mathcal{A}'}(k)=1|\neg\mathbf{E}\right]-\Pr\left[\mathbf{Exp}^{\textit{kem-wnm-cca2-0}}_{\mathcal{KEM}',\mathcal{A}'}(k)=1|\neg\mathbf{E}\right]|+\Pr\left[\mathbf{E}\right]\\ &\leq \mathbf{Adv}^{\textit{kem-wnm-cca2}}_{\mathcal{KEM},\mathcal{A}}+q(k)\cdot\left(\mathbf{Adv}^{\textit{kem-wnm-cca2}}_{\mathcal{KEM},\mathcal{B}}+2^{-c/2}\right)\,,\end{aligned}$$

where the two terms on the right hand side are negligible by the security of $\mathcal{KEM}$ and since $q(k)$ is a polynomial and 2^{-c} is negligible by assumption. ∎

Theorem 3.2 in particular implies the interesting separation wNM-CCA2 $\not\Rightarrow$ IND-CCA2. We stress that this is only due to the fact that the size of the key-space $\{0,1\}^c$ of $\mathcal{KEM}$ is assumed to be super-polynomial (resembled by the additive factor $2^{-c/2}$ in Lemma 3.10). On the other hand, if the size of the key-space is only polynomial in k then we actually can prove wNM-CCA2 $\Rightarrow$ IND-CCA2.

3.3 Proof of Theorem 3.3: IND-CCA1 $\not\Rightarrow$ wNM-CPA

Assume there exists an IND-CCA1 secure scheme $\mathcal{KEM}=(\mathsf{KEM.Kg},\mathsf{KEM.Enc},\mathsf{KEM.Dec})$ (since otherwise the theorem is vacuously true). We modify $\mathcal{KEM}$ into a new KEM $\mathcal{KEM}'=(\mathsf{KEM'.Kg},\mathsf{KEM'.Enc},\mathsf{KEM'.Dec})$ which is still secure in the sense of IND-CCA1 but not in the sense of wNM-CPA. Namely, we set $\mathsf{KEM'.Kg}=\mathsf{KEM.Kg}$ and

Alg. $\mathsf{KEM}'.\mathsf{Enc}(pk)$	**Alg.** $\mathsf{KEM}'.\mathsf{Dec}(sk, C')$
$(K, C) \xleftarrow{\$} \mathsf{KEM}.\mathsf{Enc}(pk)$	Parse C' as $P \| C$
$C' \leftarrow 0^k \| C$	$K \xleftarrow{\$} \mathsf{KEM}.\mathsf{Dec}(sk, C)$
Return (C', K)	Return $K \oplus P$

Now $\mathcal{KEM}'$ inherits the IND-CCA1 security of $\mathcal{KEM}$, since any IND-CCA1 attack on $\mathcal{KEM}'$ can be simulated in the IND-CCA1 attack setting on $\mathcal{KEM}$ (note that in the first phase, the $\mathcal{KEM}$ decapsulation oracle is not restricted in any way, and thus, decapsulation of any $\mathcal{KEM}'$ ciphertext can be performed using such a $\mathcal{KEM}$ decapsulation oracle).

However, $\mathcal{KEM}'$ is not secure in the sense of wNM-CPA: an attacker receiving a challenge ciphertext $0^k \| C$ can submit a forged ciphertext $1^k \| C$ (which decrypts to the bitwise complement of the challenge message) together with the relation $R(K_1, K_2)$ that is fulfilled iff K_2 is the bitwise complement of K_1.

4 Relations among Data Encapsulation Mechanisms

We state more formally the results summarized in Figure 3 and provide proofs.

We first show that NM is strictly stronger than IND for all attacks forms. For CCA2 attacks this is in contrast to [14] (recall that [14] uses a weaker notion of non-malleability). The proof of the following is in Section 4.1.

Theorem 4.1 [NM-ATK $\Rightarrow$ 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 $\in \{\mathrm{OT}, \mathrm{OTCCA}, \mathrm{CPA}, \mathrm{CCA1}, \mathrm{CCA2}\}$.

The proof of the following goes along the lines of [3, Theorem 3.3] (showing IND-CCA2 $\Rightarrow$ NM-CCA2) and is omitted here.

Theorem 4.2 [IND-OTCCA $\Rightarrow$ NM-OTCCA, IND-CCA2 $\Rightarrow$ NM-CCA2] If a DEM is secure in the sense of IND-ATK then it is secure in the sense of NM-ATK for any ATK $\in \{\mathrm{OTCCA}, \mathrm{CCA2}\}$.

Not too surprisingly even the stronger notion without access to an encryption oracle (IND-OTCCA) does not imply the weakest notions with access to an encryption oracle (IND-CPA). The following theorem follows from [14, Theorem 6].

Theorem 4.3 [IND-OTCCA $\not\Rightarrow$ IND-CPA] There exists a DEM which is secure in the sense of IND-OTCCA but which is not secure in the sense of IND-CPA.

The separating example from [3, Theorem 3.5] (showing IND-CCA1 $\not\Rightarrow$ NM-CPA) extends to show the following:

Theorem 4.4 [IND-CCA1 $\not\Rightarrow$ NM-OT] If there exists a scheme $\mathcal{DEM}$ which is secure in the sense of IND-CCA1, then there exists a scheme $\mathcal{DEM}'$ which is secure in the sense of IND-CCA1 but not secure in the sense of NM-OT.

The separating example from [3, Theorem 3.7] (showing NM-CCA1 $\not\Rightarrow$ NM-CCA2) extends to show the following:

Theorem 4.5 [NM-CCA1 $\not\Rightarrow$ NM-OTCCA] If there exists a scheme $\mathcal{DEM}$ which is secure in the sense of NM-CCA1, then there exists a scheme $\mathcal{DEM}'$ which is secure in the sense of NM-CCA1 but not secure in the sense of NM-OTCCA.

For completing the picture, we finally need to formulate a result from [3] for the secret key case (however, the proof from [3] still applies):

Theorem 4.6 [NM-CPA $\not\Rightarrow$ IND-CCA1] If there exists a scheme $\mathcal{DEM}$ which is secure in the sense of NM-CPA, then there exists a scheme $\mathcal{DEM}'$ which is secure in the sense of NM-CPA but not secure in the sense of IND-CCA1.

4.1 Proof of Theorem 4.1: NM-ATK $\Rightarrow$ IND-ATK

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

Assume $\mathcal{DEM}$ is secure in the NM-ATK sense for ATK $\in \{\text{OT}, \text{OTCCA}\}$. 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 $\mathbf{Adv}^{\textit{dem-ind-atk}}_{\mathcal{DEM},\mathcal{B}}(\cdot)$ 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.** $\mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St, m_0, m_1)$
$(m_0, m_1, St) \xleftarrow{\$} \mathcal{B}_1(1^k)$	$c \xleftarrow{\$} \mathcal{B}_2^{\mathtt{DEC}'_2(\cdot)}(m_0, m_1, C^*, St)$
$\mathcal{M} \leftarrow \{m_0, m_1\}$	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.

Claim 4.7 $\Pr\left[\mathbf{Exp}^{\textit{dem-nm-atk-1}}_{\mathcal{DEM},\mathcal{A}}(k) = 1\right] = \Pr\left[\mathbf{Exp}^{\textit{dem-ind-atk-b}}_{\mathcal{DEM},\mathcal{B}}(k) = b\right]$.

Proof: 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 $R(m_b) = 1$ iff $b = c$. ∎

Claim 4.8 $\Pr\left[\mathbf{Exp}^{\textit{dem-nm-atk-0}}_{\mathcal{DEM},\mathcal{A}}(k) = 1\right] = 1/2$.

Proof: 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. ∎

Now we may apply the claims to obtain $\mathbf{Adv}^{\textit{dem-ind-atk}}_{\mathcal{DEM},\mathcal{B}}(k) = 2 \cdot \mathbf{Adv}^{\textit{dem-nm-atk}}_{\mathcal{DEM},\mathcal{A}}(k)$. Since $\mathcal{DEM}$ is secure in the sense of IND-ATK we know that $\mathbf{Adv}^{\textit{dem-nm-atk}}_{\mathcal{DEM},\mathcal{A}}(\cdot)$ and hence $\mathbf{Adv}^{\textit{dem-ind-atk}}_{\mathcal{DEM},\mathcal{B}}(k)$ is negliglible, too.

5 Necessary and Sufficient Conditions for 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).

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. 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

We state more formally the 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, sNM} security, a X-Y secure KEM and a X-Y' secure DEM implies a X-Y secure hybrid PKE scheme. Interestingly, in same cases we have that for Y$'$ a weaker attack form than Y is sufficient.

Theorem 5.1 [IND-ATK KEM + IND-ATK' DEM $\Rightarrow$ 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 [8]. The proofs for the other two cases are almost identical and omitted here.

The following results are proved in Section 5.1

Theorem 5.2 [sNM-CCA1 KEM + NM-OT DEM $\Rightarrow$ NM-CCA1 PKE] If $\mathcal{KEM}$ is a secure KEM under sNM-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 5.3 [sNM-CPA KEM + NM-OT DEM $\Rightarrow$ NM-CPA PKE] If $\mathcal{KEM}$ is a secure KEM under sNM-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.

Now we turn to negative results.

Theorem 5.4 [wNM-CCA2 KEM + IND-CCA2 DEM $\not\Rightarrow$ NM-CPA PKE] Assume there exist a scheme $\mathcal{KEM}$ which is secure in the sense of wNM-CCA2 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 wNM-CCA2 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 5.5 [$*$ 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 5.6 [$*$ 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 5.7 [sNM-CPA KEM + IND-CCA2 DEM $\not\Rightarrow$ IND-CCA1 PKE] Assume there exist a scheme $\mathcal{KEM}$ which is secure in the sense of sNM-CPA and a scheme $\mathcal{DEM}$ which is secure in the sense of IND-CCA2. Then there exist a scheme $\mathcal{DEM}'$ which is secure in the sense of sNM-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 5.8 [sNM-CCA1 KEM + IND-CCA2 DEM $\not\Rightarrow$ IND-CCA2 PKE] Assume there exist a scheme $\mathcal{KEM}$ which is secure in the sense of sNM-CCA1 and a scheme $\mathcal{DEM}$ which is secure in the sense of IND-CCA2. Then there exist a scheme $\mathcal{DEM}'$ which is secure in the sense of sNM-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.

5.1 Proof of Theorem 5.2 and Theorem 5.3: sNM-CCA1 KEM + NM-OT DEM $\Rightarrow$ NM-CCA1 PKE, and sNM-CPA KEM + NM-OT DEM $\Rightarrow$ NM-CPA PKE

For this proof we will use the notion of PNM-ATK security (equivalent to sNM-ATK security) described in Section 3.2. So first assume $\mathcal{KEM}$ to be sNM-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^b_0.

In G^b_0, 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^b_1, 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:

$$\Pr\left[\, G^b_0 \to 1 \,\right] \approx \Pr\left[\, G^b_1 \to 1 \,\right] \tag{2}$$

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^b_0 resp. G^b_1 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^b_{1-d} when run with $\mathcal{F}$. Since $\mathcal{KEM}$ is PNM-CCA1 secure, (2) follows.

Next we simulate G^b_1 (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 $(C^i_1, C^i_2) \in \mathbf{C}$ has $C^i_1 \neq C^*_1$, it is decrypted using the prepared keypair and hardcoded into R. But all C^i_2 with $C^i_1 = C^*_1$ 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^b_1 (with adversary $\mathcal{F}$). By the NM-OT security of $\mathcal{DEM}$, we thus have

$$\Pr\left[\, G^0_1 \to 1 \,\right] \approx \Pr\left[\, G^1_1 \to 1 \,\right],$$

and hence, using (2),

$$\Pr\left[\, G_0^0 \to 1 \,\right] \approx \Pr\left[\, G_0^1 \to 1 \,\right],$$

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-CPA secure.

5.2 Proof of Theorem 5.4: wNM-CCA2 KEM + IND-CCA2 DEM $\not\Rightarrow$ NM-CPA PKE

Assume there exists a wNM-CCA2 secure scheme $\mathcal{KEM}$. We use the same modification $\mathcal{KEM}'$ as in the proof of Theorem 3.2, where it was shown that $\mathcal{KEM}'$ is still wNM-CCA2 secure.

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 $\{0,1\}^k$. We modify $\mathcal{DEM}$ into a new DEM $\mathcal{DEM}' = (\mathsf{DEM'.Kg}, \mathsf{DEM'.Enc}, \mathsf{DEM'.Dec})$ (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. $\mathsf{DEM'.Kg}(1^k)$	**Alg.** $\mathsf{DEM'.Enc}(K, M)$	**Alg.** $\mathsf{DEM'.Dec}(K, C')$
$K_1 \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$	Parse K as $K_1\|\|K_2$	Parse C' as $C'_1\|\|C'_2$ and K as $K_1\|\|K_2$
$K_2 \xleftarrow{\$} \{0,1\}^k$	$C'_1 \xleftarrow{\$} \mathsf{DEM.Enc}(K_1, M)$	If $C'_2 = K_2$ then $M \leftarrow \mathsf{DEM.Dec}(K_1, C'_1)$
Return $K = K_1\|\|K_2$	$C'_2 \leftarrow K_2$	else $M \leftarrow \perp$
	Return $C' = C'_1\|\|C'_2$	Return M

Claim 5.9 $\mathcal{DEM}'$ is secure in the sense of IND-CCA2.

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

Here, oracle $\mathtt{ENC}'_2(M)$ returns $\mathtt{ENC}_2(M)||K_2$. Oracle $\mathtt{DEC}'_2(C'_1||C'_2)$ returns $\mathtt{DEC}_2(C'_1)$ 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 scheme $\mathcal{DEM}'$. Hence

$$\mathbf{Adv}^{\mathit{dem\text{-}ind\text{-}atk}}_{\mathcal{DEM}',\mathcal{B}'}(k) = \mathbf{Adv}^{\mathit{dem\text{-}ind\text{-}atk}}_{\mathcal{DEM},\mathcal{B}}(k)$$

and thus, $\mathcal{DEM}'$ inherits the IND-CCA2 security of $\mathcal{DEM}$. ▌

Claim 5.10 $\mathcal{PKE}_{\mathcal{KEM}',\mathcal{DEM}'}$ is not secure in the sense of NM-CPA.

Proof: We construct 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 the uniform distribution on the message space. Then, in the second phase, $\mathcal{F}_2$ receives a challenge ciphertext for the hybrid PKE scheme, i.e. $C^* = (C_1^*||C_2^*, C_3^*||C_4^*)$ where $(K_1||K_2, C) \xleftarrow{\$} \mathsf{KEM.Enc}(pk)$, $C_1^* = C$, $C_2^* = 0^{l/2}$, $C_3^* = \mathsf{DEM.Enc}(K_1, M^*)$ and $C_4^* = K_2$, for some challenge message M^*.

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 $R(m_1, m_2) = 1$ iff $m_1 = m_2$. In the experiment with $b = 1$, where message M_1 in the evaluation of the relation is the challenge message M^*, the relation holds with probability one (message M_2 is in both experiments $M_2 = \mathsf{PKE.Dec}(sk, C) = M^*$); on the other hand, in the experiment with $b = 0$, where message M_1 in the evaluation of the relation is a uniform message, chosen independently from M^*, the relation only holds with probability one over the cardinality of the message space. Therefore the adversary $\mathcal{F}$ is successful. ∎

This proof makes use of a malleability attack in which the adversary outputs the identity relation. Although fine in our setting, the original non-malleability formulation [11] disallows this. However, our example can be adapted such that instead of the identity relation, the "bitwise complement" relation can be used. We omit the somewhat tedious proof, which requires further modifications to both the KEM and the DEM part. (The idea is to have $\mathcal{KEM}$' output a key $\overline{K_1}||K_2$ upon decapsulation of ciphertexts (C_1, K_2), such that $\overline{K_1}$ is equal to K_1 except for, say, the most significant bit. On the other hand, $\mathcal{DEM}$' now uses this most significant bis of K_1 to determine whether to invert the plaintext upon decryption or not.)

5.3 Proof of Theorem 5.5: $*$ KEM + IND-CCA1 DEM $\not\Rightarrow$ NM-CPA PKE

For this, we can use the ideas in the proof of [3, Theorem 3.5]. Assume that there exists an IND-CCA1 secure scheme $\mathcal{DEM} = (\mathsf{DEM.Kg}, \mathsf{DEM.Enc}, \mathsf{DEM.Dec})$. We modify $\mathcal{DEM}$ into a new DEM $\mathcal{DEM}' = (\mathsf{DEM'.Kg}, \mathsf{DEM'.Enc}, \mathsf{DEM'.Dec})$ 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. $\mathsf{DEM'.Kg}(1^k)$	**Alg.** $\mathsf{DEM'.Enc}(K, m)$	**Alg.** $\mathsf{DEM'.Dec}(K, C')$
$K \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$	$C_1 \xleftarrow{\$} \mathsf{DEM.Enc}(K, m)$	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].

Claim 5.11 $\mathcal{DEM}'$ is still secure in the sense of IND-CCA1.

Proof: Assume to the contrary that there exists a successful IND-CCA1 adversary $\mathcal{B}' = (\mathcal{B}_1', \mathcal{B}_2')$ against $\mathcal{DEM}'$, and let us use it to construct a successful IND-CCA1 adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ against $\mathcal{DEM}$, contradicting the fact that $\mathcal{DEM}$ is IND-CCA1 secure.

A challenger generates $K \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$, then $\mathcal{B}$ initializes adversary $\mathcal{B}'$. In the first stage, $\mathcal{B}_1'$ can make encryption and decryption queries, which are answered by $\mathcal{B}_1$ as follows:

- To answer an encryption query for a message m, adversary $\mathcal{B}_1$ makes two queries to its encryption oracle $\mathsf{DEM.Enc}(K, \cdot)$, for messages m and $\overline{m}$. The concatenation of the two obtained ciphertexts is the ciphertext that $\mathcal{B}_1$ sends back to $\mathcal{B}_1'$.

- To answer a decryption query for a ciphertext $C' = C_1||C_2$, adversary $\mathcal{B}_1$ sends C_1 to its decryption oracle, obtaining $m \leftarrow \mathsf{DEM.Dec}(K, C_1)$. The message is sent back to $\mathcal{B}'_1$.

Now $\mathcal{B}'_1$ outputs two messages m_0 and m_1 of the same length. $\mathcal{B}_1$ chooses at random a bit $\delta \in \{0,1\}$ and asks to its encryption oracle for the encryption of $\overline{m_\delta}$, obtaining $C_2^* \leftarrow \mathsf{DEM.Enc}(K, \overline{m_\delta})$. $\mathcal{B}_1$ outputs the same messages m_0 and m_1 to its challenger, who then computes $C_1^* \leftarrow \mathsf{DEM.Enc}(K, m_b)$ and gives it as input to $\mathcal{B}_2$, depending on the experiment $b \in \{0,1\}$. The resulting challenge ciphertext that $\mathcal{B}_2$ gives to $\mathcal{B}'_2$ is $C'^* = (C_1^*, C_2^*)$. At the end, $\mathcal{B}'_2$ outputs a bit b'. If $b' = \delta$, then the output of $\mathcal{B}_2$ is also this bit δ; otherwise, the output of $\mathcal{B}_2$ is simply a random bit.

It is not difficult to see that $\mathbf{Adv}^{\textit{dem-ind-cca1}}_{\mathcal{DEM},\mathcal{B}} \geq \frac{1}{2}\mathbf{Adv}^{\textit{dem-ind-cca1}}_{\mathcal{DEM}',\mathcal{B}'}$, which leads to the desired contradiction. ▮

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

Claim 5.12 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: $\mathcal{F}$ receives a public key pk, resulting from $(pk, sk) \leftarrow \mathsf{KEM.Kg}(1^k)$; then it chooses the uniform distribution on the message space, and receives a challenge ciphertext $C^* = (C_1, C_2||C_3)$, where $(K, C_1) \stackrel{\$}{\leftarrow} \mathsf{KEM.Enc}(1^k, pk)$, $C_2 = \mathsf{DEM.Enc}(K, m^*)$ and $C_3 = \mathsf{DEM.Enc}(K, \overline{m^*})$, for some uniform message m^*. It is evident that $C = (C_1, C_3||C_2)$ is a valid encryption of message $\overline{m^*}$ under the scheme $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}'}$. Therefore the adversary $\mathcal{F}$ 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; on the other hand, in the $b = 0$ experiment we have that R is evaluated on a uniform message m, independent from m^*, and in $\overline{m^*}$, so the relation holds only with probability one over the cardinality of the message space. ▮

5.4 Proof of Theorem 5.6: $*$ KEM + NM-CCA1 DEM $\not\Rightarrow$ 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 $\mathcal{DEM}' = (\mathsf{DEM'.Kg}, \mathsf{DEM'.Enc}, \mathsf{DEM'.Dec})$ 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 $F_K : \{0,1\}^k \rightarrow \{0,1\}^k$, 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. $\mathsf{DEM'.Kg}(1^k)$
$K_1 \stackrel{\$}{\leftarrow} \mathsf{DEM.Kg}(1^k)$
$K_2 \stackrel{\$}{\leftarrow} \{0,1\}^k$
Return $K = K_1||K_2$

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

Alg. $\mathsf{DEM'.Dec}(K, C')$
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 in Section 3.7 of [3].

Claim 5.13 $\mathcal{DEM}'$ is secure in the sense of NM-CCA1.

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; one can always use a KEM with key-space $\{0,1\}^{k'}$ with "stretched security" parameter $k' = 2k$.) 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 5.5, the attack from [3, Claim 3.14] on $\mathcal{DEM}$ can be transported to the hybrid setting.

Claim 5.14 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. ∎

5.5 Proof of Theorem 5.7: sNM-CPA KEM + IND-CCA2 DEM ⇏ IND-CCA1 PKE

Assume there exists a sNM-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 new 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. $\mathsf{KEM'.Dec}(sk', C')$
Write $sk' = (sk, v)$ 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 new DEM $\mathcal{DEM}' = (\mathsf{DEM'.Kg}, \mathsf{DEM'.Enc}, \mathsf{DEM'.Dec})$ which is still secure in the sense of IND-CCA2.

Alg. $\mathsf{DEM'.Kg}(1^k)$
$K \xleftarrow{\$} \mathsf{DEM.Kg}(1^k)$
Return K

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

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

Claim 5.15 $\mathcal{PKE}_{\mathcal{KEM}', \mathcal{DEM}'}$ 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. ▌

5.6 Proof of Theorem 5.8: sNM-CCA1 KEM + IND-CCA2 DEM $\not\Rightarrow$ IND-CCA2 PKE

Assume there exists an sNM-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 5.6. Namely, if F is a family of pseudo-random functions, we define:

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

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

Alg. $\mathsf{KEM'.Dec}(sk', C')$
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, techniques from Section 3.7 of [3] show

Claim 5.16 $\mathcal{KEM}'$ is secure in the sense of sNM-CCA1.

Combined with the IND-CCA2 secure DEM $\mathcal{DEM}'$ from the proof of Theorem 5.7, 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 5.6 can be carried out "through" the DEM $\mathcal{DEM}'$ just like in the proof of Theorem 5.7. We omit the details.

Acknowledgements

We thank Tatsuaki Okamoto for providing us with a preliminary version of [18] and Mihir Bellare for interesting discussions. The work of the first author has been carried out during the tenure of an ERCIM fellowship. The third author was 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.

References

[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 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 128–146, Aarhus, Denmark, May 22–26, 2005. Springer-Verlag, Berlin, Germany. 2

[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. 11

[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. 2, 3, 4, 5, 6, 7, 8, 9, 13, 14, 18, 19, 23, 24, 25, 27

[4] 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, 8, 15

[5] Mihir Bellare and Amit Sahai. Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization. IACR ePrint Archive, June 2006. Manuscript, available online at `http://eprint.iacr.org/2006/228.ps`. 6, 8, 9, 29

[6] Xavier Boyen, Qixiang Mei, and Brent Waters. Direct chosen ciphertext security from identity-based techniques. In *ACM CCS 05: 12th Conference on Computer and Communications Security*, pages 320–329, Alexandria, Virginia, USA, November 7–11, 2005. ACM Press. 1

[7] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, *Advances in Cryptology – CRYPTO'98*, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25, Santa Barbara, CA, USA, August 23–27, 1998. Springer-Verlag, Berlin, Germany. 31

[8] 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. 1, 2, 3, 4, 5, 9, 11, 13, 20

[9] CRYPTREC (cryptography research & evaluation committees): The cryptographic technique evaluation project, August 2003. `http://www.ipa.go.jp/security/enc/CRYPTREC/`. 1

[10] A. W. Dent. A designer's guide to KEMs. In *Cryptography and Coding: 9th IMA International Conference*, volume 2898 of *LNCS*, pages 133–151, 2003. 1

[11] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. In *23rd Annual ACM Symposium on Theory of Computing*, pages 542–552, New Orleans, Louisiana, USA, May 6–8, 1991. ACM Press. 4, 5, 6, 7, 13, 23

[12] Oded Goldreich. *Foundations of Cryptography: Basic Applications*, volume 2. Cambridge University Press, Cambridge, UK, 2004. 7, 8

[13] D. Hofheinz, J. Herranz, and E. Kiltz. The Kurosawa-Desmedt key encapsulation is not chosen-ciphertext secure. Cryptology ePrint Archive, Report 2006/207, 2006. `http://eprint.iacr.org/`. 2

[14] J. Katz and M. Yung. Characterization of security notions for probabilistic private-key encryption. *Journal of Cryptology*, 19(1):67–96, 2006. 2, 5, 12, 13, 18

[15] Eike Kiltz. Chosen-ciphertext security from tag-based encryption. In Shai Halevi and Tal Rabin, editors, *TCC 2006: 3rd 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. 1

[16] Kaoru Kurosawa and Yvo Desmedt. A new paradigm of hybrid encryption scheme. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 426–442, Santa Barbara, CA, USA, August 15–19, 2004. Springer-Verlag, Berlin, Germany. 2

[17] Waka Nagao, Yoshifumi Manabe, and Tatsuaki Okamoto. A universally composable secure channel based on the KEM-DEM framework. In Joe kilian, editor, *TCC 2005: 2nd Theory of Cryptography Conference*, volume 3378 of *Lecture Notes in Computer Science*, pages 426–444, Cambridge, MA, USA, February 10–12, 2005. Springer-Verlag, Berlin, Germany. 2, 4, 5, 10, 31

[18] Waka Nagao, Yoshifumi Manabe, and Tatsuaki Okamoto. On the equivalence of several security notions of key encapsulation mechanism. Cryptology ePrint Archive, Report 2006/xxx (to appear), 2006. http://eprint.iacr.org/. 2, 5, 11, 13, 15, 27

[19] Waka Nagao, Yoshifumi Manabe, and Tatsuaki Okamoto. A universally composable secure channel based on the KEM-DEM framework. *IEICE Trans Fundamentals*, E89-A(1):28–38, 2006. 2, 4, 5, 10, 31

[20] NESSIE Final report of European project IST-1999-12324: New European Schemes for Signatures, Integrity, and Encryption, April 2004. Working draft. 1

[21] 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. 2

[22] Victor Shoup. Using hash functions as a hedge against chosen ciphertext attack. In Bart Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 275–288, Bruges, Belgium, May 14–18, 2000. Springer-Verlag, Berlin, Germany. 1

[23] Victor Shoup. A proposal for an ISO standard for public key encryption (version 2.1). manuscript, 2001. Available on http://shoup.net/papers/. 1, 31

[24] Victor Shoup. ISO 18033-2: An emerging standard for public-key encryption. http://shoup.net/iso/std6.pdf, December 2004. Final Committee Draft. 1

[25] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the American Institute of Electrical Engineers*, 45:109–115, 1926. 13

A Poof that CNM-CPA* does not imply CNM-CPA

Let $\mathcal{PKE} = (\mathsf{PKE.Kg}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ be a CNM-CPA* secure public key encryption scheme. (The notion of CNM-CPA* security is informally defined in Section 2.1, for a formal definition cf. [5].) W.l.o.g., we can assume that the secret keys of $\mathcal{PKE}$ always have length $p(k)$ for a polynomial p. We construct a scheme $\mathcal{PKE}' = (\mathsf{PKE.Kg}', \mathsf{PKE.Enc}', \mathsf{PKE.Dec}')$ as follows:

Alg. $\mathsf{PKE.Kg}'(1^k)$
$(pk, sk) \xleftarrow{\$} \mathsf{PKE.Kg}(1^k)$
Pick pairwise distinct $i_1, \ldots, i_k \in \{1, \ldots, 2k\}$
$j_1, \ldots, j_{k-1} \xleftarrow{\$} \{0,1\}^{p(k)}$
$j_k \leftarrow sk \oplus \bigoplus_{\ell=1}^{k-1} j_\ell$
$sk' \leftarrow ((i_\ell, j_\ell)_{\ell=1}^{k}, sk)$
Return $(pk' = pk, sk')$

Alg. $\mathsf{PKE.Dec}(sk', C')$
Parse sk' as $((i_\ell, j_\ell)_{\ell=1}^{k}, sk)$
Parse C' as $b||C$
If $b = 0$ then $M' \xleftarrow{\$} \mathsf{PKE.Dec}(sk, C)$
else if $C = i_\ell$ for some ℓ then $M' \leftarrow j_\ell$
else $M' \leftarrow \perp$
Return M'

and $\mathsf{PKE.Enc}'(pk', M) = 0||\mathsf{PKE.Enc}(pk', M)$. It is clear that $\mathcal{PKE}'$ is a public key encryption scheme. The idea of $\mathcal{PKE}'$ is to let decryptions of a special form leak information on the decryption key. In particular, a CNM-CPA adversary can, after receiving a challenge ciphertext C'^*, choose a ciphertext vector $\mathbf{C}'$ with $\mathbf{C}'[\ell] = (1, \ell)$ (for $\ell = 1, \ldots, 2k$). The relation R' can

then, using the decryption of $\mathbf{C}'$, recover the secret key sk and, e.g., decrypt the (hardwired) challenge ciphertext C'^* and compare the decryption M'^* to the relation's first argument.

However, such an attack is obviously not possible with the CNM-CPA* notion, since such a $\mathbf{C}'$ contains invalid ciphertexts (in the sense that they decrypt to $\perp$). More generally, we prove that $\mathcal{PKE}'$ inherits the CNM-CPA* security of $\mathcal{PKE}$, which shows the overall statement.

Claim A.1 If $\mathcal{PKE}$ is CNM-CPA* secure, then so is the scheme $\mathcal{PKE}'$ built from $\mathcal{PKE}$ as described above.

Proof: Let $\mathcal{F}' = (\mathcal{F}'_1, \mathcal{F}'_2)$ be a CNM-CPA* adversary on $\mathcal{PKE}'$. We construct a CNM-CPA* adversary $\mathcal{F} = (\mathcal{F}_1, \mathcal{F}_2)$ on $\mathcal{PKE}$ from $\mathcal{F}'$ such that $\mathcal{F}$ is successful if $\mathcal{F}'$ is.

The idea is that $\mathcal{F}$ internally runs $\mathcal{F}'$ and only needs to translate to and from the different interface of $\mathcal{PKE}'$. For this, $\mathcal{F}'_1$ can be left unchanged (i.e., $\mathcal{F}_1 = \mathcal{F}'_1$), and $\mathcal{F}_2$ is defined as follows:

Alg. $\mathcal{F}_2(C^*, St)$
  $C'^* \leftarrow 0||C^*$
  $(R', \mathbf{C}') \xleftarrow{\$} \mathcal{F}'_2(C'^*, St)$
  Pick pairwise distinct $i_1, \ldots, i_k \in \{1, \ldots, 2k\}$
  $j_1, \ldots, j_k \xleftarrow{\$} \{0,1\}^{p(k)}$
  For $\nu \in \{1, \ldots, |\mathbf{C}'|\}$ do
    Parse $\mathbf{C}'[\nu]$ as $b_\nu||C_\nu$
    If $b_\nu = 0$ then $\mathbf{C}[\nu] \leftarrow C_\nu$
    else If $C_\nu = i_\ell$ for some ℓ, then $\mathbf{C}[\nu] \xleftarrow{\$} \mathsf{PKE.Enc}(pk, j_\ell)$
    else $\mathbf{C}[\nu] \xleftarrow{\$} \mathsf{PKE.Enc}(pk, \perp)$
  Return $(St, \mathcal{M})$

By definition of $\mathcal{F}$, the view of $\mathcal{F}'$ in the CNM-CPA* experiment for scheme $\mathcal{PKE}'$ and in $\mathcal{F}$'s simulation of the CNM-CPA* experiment for scheme $\mathcal{PKE}$ is the same. Hence, by definition of the CNM-CPA* experiment, the output distribution of the experiment with adversary $\mathcal{F}'$ and scheme $\mathcal{PKE}'$ is the same as that of the CNM-CPA* experiment with $\mathcal{F}$ and $\mathcal{PKE}$, provided that either

- $\mathbf{C}'$ contains an invalid ciphertext (in which case the experiment output is forced to `false`), or that
- $\mathbf{C}'$ does not contain all ciphertexts $(1, i_\ell)$ for $i = 1, \ldots, k$ (in which case the decryption of $\mathbf{C}'$ is identically distributed in both experiments).

But since the i_ℓ are chosen independently from $\mathcal{F}'$ in both experiments, $\mathcal{F}'$ has negligible chance of coming up with a ciphertext vector $\mathbf{C}'$ that contains only valid ciphertexts, but all the $(1, i_\ell)$. (For this, $\mathcal{F}'$ would have to guess $\{i_\ell\}_{\ell=1}^k$.)

So the experiment output with adversary $\mathcal{F}'$ and scheme $\mathcal{PKE}'$ and that of the experiment with $\mathcal{F}$ and $\mathcal{PKE}$ differ only negligibly. In other words, $\mathcal{F}$ is successful if $\mathcal{F}'$ is. ∎

B The notion of non-malleability for KEMs from [17, 19]

Definition B.1 Weak non-malleability in the sense of Nagao, Manabe, and Okamoto [17, 19] (that we will denote as NM′) is defined as in Definition 2.4 where the security experiment $\mathbf{Exp}^{kem\text{-}wnm\text{-}atk\text{-}b}_{\mathcal{KEM},\mathcal{A}}(k)$ is modified as follows (all changes are marked with a framed box).

$$
\begin{array}{l}
\textbf{Experiment } \mathbf{Exp}^{kem\text{-}wnm\text{-}atk\text{-}b}_{\mathcal{KEM},\mathcal{A}}(k) \\
\quad (pk, sk) \xleftarrow{\$} \mathsf{KEM.Kg}(1^k) \\
\quad \boxed{(St, \mathcal{K}) \xleftarrow{\$} \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)} \\
\quad \boxed{K_0^* \xleftarrow{\$} \mathcal{K}\,;\ (K_1^*, C^*) \xleftarrow{\$} \mathsf{KEM.Enc}(pk) \wedge K_1^* \in \mathcal{K}} \\
\quad (R, \mathbf{C}) \xleftarrow{\$} \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St) \\
\quad \mathbf{K} \leftarrow \mathsf{KEM.Dec}(sk, \mathbf{C}) \\
\quad \text{If } C^* \notin \mathbf{C} \text{ and } R(K_b^*, \mathbf{K}) \text{ then return 1 else return 0}
\end{array}
$$

Again, a key encapsulation mechanism $\mathcal{KEM}$ is said to be NM′ *against* ATK *attacks* if the respective advantage function is a negligible function in k for all polynomial-time adversaries $\mathcal{A}$.

Actually the definition from [17, 19] is ambiguous and leaves some room for interpretation. In particular it is not clear how the statement "$(K_1^*, C^*) \xleftarrow{\$} \mathsf{KEM.Enc}(pk) \wedge K_1^* \in \mathcal{K}$" should be understood. Our interpretation is that the encapsulation algorithm is run with the additional requirement that the generated random key should be chosen according to the distribution $\mathcal{K}$.

One of the main theorems in [17, 19] is that in the case of CCA2 adversaries, the notions of NM′ and IND are equivalent, i.e. that IND-CCA2 $\Leftrightarrow$ NM′-CCA2. For the proof, [19] refers to the second author's master thesis but we now explain some difficulties one encounters proving this result by showing a counterexample separating IND-CCA2 from NM′-CCA2.

As a separating example we use the Cramer-Shoup key encapsulation mechanism [7] which is well-known to be IND-CCA2 [23]. We assume a cyclic group $\mathbb{G}$ of prime order p and two generators $g_1, g_2 \in \mathbb{G}$. Furthermore let $\mathsf{TCR} : \mathbb{G} \times \mathbb{G} \to \mathbb{Z}_p$ be a target collision-resistant hash function [7].

Alg. $\mathsf{KEM.Kg}(pk)$	**Alg.** $\mathsf{KEM.Enc}(pk)$	**Alg.** $\mathsf{KEM.Dec}(sk, C)$
$x_1, x_2, y_1, y_2, z \xleftarrow{\$} \mathbb{Z}_p$	$r \leftarrow \mathbb{Z}_p\,;\ c_1 \leftarrow g_1^r\,;\ c_2 \leftarrow g_2^r$	Write $C = (c_1, c_2, c_3)$
$c \leftarrow g_1^{x_1} g_2^{x_2}\,;\ d \leftarrow g_1^{y_1} g_2^{y_2}$	$t \leftarrow \mathsf{TCR}(c_1, c_2)\,;\ c_3 \leftarrow (c^t d)^r$	$t \leftarrow \mathsf{TCR}(c_1, c_2)$
$h \leftarrow g_1^z$	$C \leftarrow (c_1, c_2, c_3)\,;\ K \leftarrow h^r$	Check if $c_1^{x_1+ty_1} c_2^{x_2+ty_2} = c_3$
$pk = (g_1, g_2, c, d, h)$	Return (C, K)	If not, return $\perp$
$sk = (x_1, x_2, y_1, y_2, z)$		Else return $K \leftarrow c_1^z$
Return (pk, sk)		

As the following attack shows, the Cramer Shoup key-encapsulation scheme is not NM′-CPA secure (and therefore in particular not NM′-CCA2). The idea is that, given the public-key (containing the value $h = g_1^z$), an attacker can choose the key distribution $\mathcal{K}$ as $\{h, h^2\}$ (both chosen with probability 1/2) which limits the randomness used for the challenge ciphertext C^* to either $r = 1$ or $r = 2$. The result is that the element $c_1 = g_1^r$ of the challenge ciphertext is in the set $\{g_1, g_1^2\}$. This can clearly be used by an adversary to break the NM′ − CPA security of the scheme.