J. Math. Cryptol. **6** (2012), 183–227
DOI 10.1515/jmc-2010-0099

New security notions and relations for public-key encryption

Reza Sepahi, Josef Pieprzyk, Siamak F. Shahandashti and Berry Schoenmakers

Communicated by Rainer Steinwandt

Abstract. Since their introduction, the notions of indistinguishability and non-malleability have been changed and extended by different authors to support different goals. In this paper, we propose new flavors of these notions, investigate their relative strengths with respect to previous notions, and provide the full picture of relationships (i.e., implications and separations) among the security notions for public-key encryption schemes. We take into account the two general security goals of indistinguishability and non-malleability, each in the message space, key space, and hybrid message-key space to find six specific goals, a couple of them, namely *complete indistinguishability* and *key non-malleability*, are new. Then for each pair of goals, coming from the indistinguishability or non-malleability classes, we prove either an implication or a separation, completing the full picture of relationships among all these security notions. The implications and separations are respectively supported by formal proofs (i.e., reductions) in the concrete-security framework and by counterexamples.

Keywords. Public-key encryption, notions of security, indistinguishability, non-malleability, complete indistinguishability, key non-malleability.

2010 Mathematics Subject Classification. 11T71, 68P25, 94A60.

1 Introduction

Public-key cryptography emerged in 1976 when Diffie and Hellman showed how two parties can agree on a common secret key via a publicly accessible communication channel [5]. This idea was also proposed by Ellis at the Government Communications Headquarters (GCHQ), under the name 'non-secret encryption' [8]. Shortly after that, in 1977, Rivest, Shamir and Adleman invented the most important public key cryptosystems, namely RSA (essentially, the same scheme was also invented by Cocks at GCHQ in 1973 [4]). Public-key encryption is evaluated

Work partly done while Berry Schoenmakers visiting Macquarie University. Also, at the time of this work, Siamak F. Shahandashti was with the ICT Research Institute, University of Wollongong, Australia.

by security goals that it achieves. The basic goal introduced by Bellare et al. in [2] is confidentiality. It requires that an adversary does not learn any useful information about the plaintext from ciphertext. A different goal formulated by Dolev in [6] is non-malleability. It is defined as inability of the adversary to convert a given ciphertext into another one in such a way that the plaintexts for the two ciphertexts are related in some way. Bellare et al. introduced the so-called *key privacy* or *anonymity* and the notion of *key indistinguishability* in [1]. Fischlin generalized the standard notion of non-malleability to *complete non-malleability* [9] in order to prove security for some higher-level protocols.

In this paper, we propose two new notions of security for public-key encryption, which we call *complete indistinguishability* (IND*) and *key non-malleability* (KNM). The former, complete indistinguishability, asserts that the encryption provides both data and key privacy. In other words, given two public keys pk_0 and pk_1, two messages x_0 and x_1, and the ciphertext $y = \mathcal{E}_{pk_b}(x_c)$, for $b, c \in \{0, 1\}$, no polynomial-time adversary should be able to find which public key and which message have been used to obtain y. The latter, i.e., key non-malleability, states that a ciphertext must not allow an adversary to generate another ciphertext for the same message and a related key. More precisely, given a public key pk and a ciphertext $y = \mathcal{E}_{pk}(x)$, no polynomial-time adversary should be able to find another ciphertext $y^* = \mathcal{E}_{pk^*}(x)$ for the same message x encrypted under a different, yet related, public key pk^*.

In addition to definitional contributions (i.e., complete indistinguishability and key non-malleability), we will compare relative strengths of indistinguishability and non-malleability notions, and derive appropriate implications or separations.

1.1 Motivation

Key non-malleability. To begin with, consider someone wants to send a secret message x to user B. So he encrypts the message x using the public key of B to obtain the ciphertext $y = \mathcal{E}_{pk}(x)$, and sends y to B over an insecure channel. If an eavesdropper A obtains y and transforms it (without decrypting it) to another ciphertext $y^* = \mathcal{E}_{pk^*}(x)$ for which pk^* and pk are related according to a binary relation $R_k(\cdot, \cdot)$, then the owner of the secret key sk^* can decrypt y^* and obtain the secret message x.

Following the point mentioned above, we note that public encryption is often used as the building block for complex protocols whose security depends on properties of the encryption. Fischlin makes this argument in [9] when he considers the possibility of constructing non-malleable commitments on top of NM*-CCA2 secure encryption. He argues that this can be done by assuming that the committing party selects a public key, encrypts the message and sends the encryption

as commitment. The opening is performed by sending the randomness used for encryption. Obviously a man-in-the-middle adversary could select a related public key in order to compute a related encryption and thus a related commitment. The KNM-CCA2 security guarantees the failure of the adversary. Putting all together, we can view KNM security as a stepping-stone toward NM* security and a prerequisite for achieving NM* security.

Complete indistinguishability. The main motivation for introducing the *complete indistinguishability* (IND*) notion is the usage of public-key encryption in multi-user settings where both message and key indistinguishability are required. Message indistinguishability is needed to provide message confidentiality while key indistinguishability guarantees anonymity of the ciphertext receiver. The complete indistinguishability, therefore, is a stronger notion as the adversary gets no information about the message and the receiver (cryptographic key).

Relations between notions. The paper investigates the relations among different indistinguishability and non-malleability notions. This is because in different applications of encryption schemes one needs different primitives with different security levels. So it is important to have a clear picture about which benefits can be provided by each definition. Our results are represented in the form of a diagram with implications and separations. The diagram can be easily used to derive the relations for an instance of public-key encryption once the security strength of the encryption is established.

1.2 Literature review

In the papers of Bellare et al. [2] and of Bellare and Sahai [3], relations between security notions for public-key encryption have been extensively studied. These papers continue the research initiated by Goldwasser and Micali [11] who defined the notion of polynomial security also called indistinguishability or IND for short. Later Naor and Yung [13] and Rackoff and Simon [14] considered stronger scenarios of attacks. This led Dolev, Dwork and Naor [6,7] to propose a stronger security notion that is the non-malleability. Bellare et al. in [1] extended the indistinguishability notion to cover *key privacy* or *ciphertext anonymity*. This notion is called *key indistinguishability* and requires from a ciphertext $y = \mathcal{E}_{pk}(x)$ not to disclose any information about the *public key pk*. Later Zhang et al. examined the relation between the standard notion of indistinguishability and key privacy [19]. They proved *informally* that message indistinguishability (IND) and key indistinguishability (KI) are orthogonal notions, and none of them implies the other. Fischlin [9] introduced the notion of complete non-malleability (NM*). The notion requires

the adversary to get no help from a ciphertext $y = \mathcal{E}_{pk}(x)$ when trying to generate another ciphertext $y^* = \mathcal{E}_{pk^*}(x^*)$ for a message x^* under a public key pk^* (at least one of y^* and pk^* should be different from their original counterparts x and pk). Ventre and Visconti continued this line of research and examined the relation between complete non-malleability and standard non-malleability. They showed *informally* that standard NM does not imply NM* [18].

1.3 Contributions of the paper

New security notions. We present a unified and complete picture of indistinguishability and non-malleability notions for public-key encryption. In particular, we introduce the following two new security notions:

(1) *Complete indistinguishability* (IND*) – this notion states that a ciphertext $y = \mathcal{E}_{pk}(x)$ should not give any information about the corresponding plaintext x or the public key pk. This is a stronger notion compared to message indistinguishability (IND) and key indistinguishability (KI) notions as the adversary gets no information about the message and/or the receiver (cryptographic key). Note that there are other ways that the definition could be strengthened, for example, by increasing the power of the decryption oracle using a definition similar to the strong decryption oracle used in certain certificateless encryption definitions.

(2) *Key non-malleability* (KNM) – this notion requires that a ciphertext $y = \mathcal{E}_{pk}(x)$ should not help the adversary to generate a new ciphertext $y^* = \mathcal{E}_{pk^*}(x)$ for the same plaintext but under a new, yet related, public key pk^*.

Relations between notions. We study the two security notions (indistinguishability and non-malleability) in the two dimensions, namely, message and key spaces. Thus we are considering the six following security notions:

(1) message indistinguishability (IND),

(2) key indistinguishability (KI),

(3) complete indistinguishability (IND*),

(4) message non-malleability (NM),

(5) key non-malleability (KNM), and

(6) complete non-malleability (NM*).

Among these six notions, IND* and KNM are new (see Table 1). In this paper we work out the relations between every pair of notions. So for every pair

Notion	Reference	Notion	Reference
IND	Bellare et al. [2]	NM	Dolev et al. [6]
KI	Bellare et al. [1]	KNM	This paper
IND*	This paper	NM*	Fischlin [9]

Table 1. Notions of security for public-key encryption

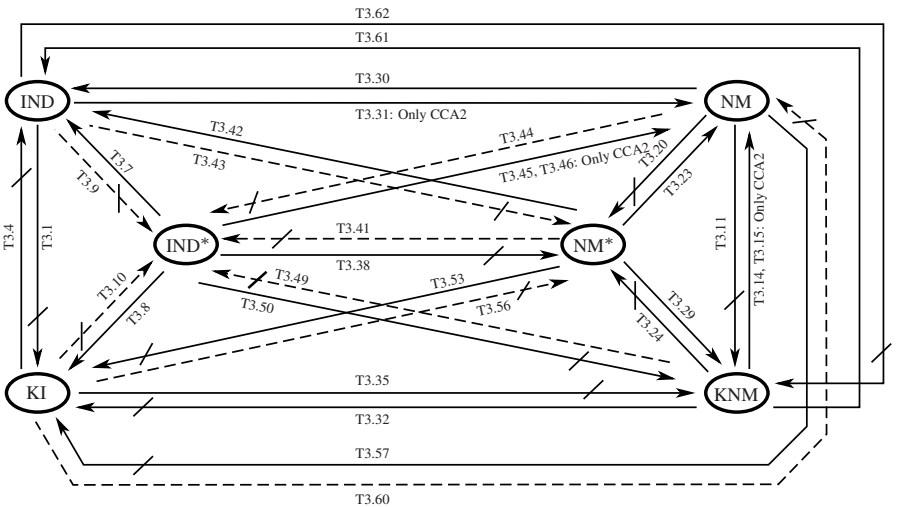

Figure 1. Relations between notions of security. An arrow shows an implication, and a negated arrow represents a separation. Dashed arrows indicate trivial relations while solid arrows represent nontrivial relations. The number above or below any arrow indicate the theorem number which proves the relation.

of notions $N_1, N_2 \in$ {IND-ATK, KI-ATK, IND*-ATK, NM-ATK, KNM-ATK, NM*-ATK}, where ATK ∈ {CPA, CCA1, CCA2}, we show one of the following:

- $N_1 \Rightarrow N_2$: a proof that shows if a public-key encryption $\mathcal{PE}$ meets the security notion N_1 then it also meets the security notion N_2 (implication).
- $N_1 \not\Rightarrow N_2$: a construction for a public-key encryption $\mathcal{PE}$ that meets the security notion N_1 but does not meet the security notion N_2 (separation).

The results are illustrated in Figure 1. We have used arrows to represent implications, and negated arrows to represent separations. The label associated with each arrow indicates the theorem number related to that implication or separation.

The rest of the paper is structured as follows. Section 2 introduces the necessary definitions of the security notions for public-key encryption. Section 3 is the main part of the paper and examines relations, i.e., implications and separations, between different security notions. Section 4 discusses future works and open problems.

2 Definitions of security

The notations and conventions used here are the standard ones for writing probabilistic algorithms and experiments. If A is a probabilistic algorithm, then $A(x_0, x_1, \ldots; r)$ is the result of running algorithm A on inputs $x_0, x_1, \ldots$ and coins r. We use $y \leftarrow A(x_0, x_1, \ldots)$ to denote the experiment of picking r uniformly at random and letting y be the output of $A(x_0, x_1, \ldots; r)$. For a finite set S, we use $x \leftarrow S$ to denote the operation of picking an element uniformly at random from S. For an α neither an algorithm nor a set, $x \leftarrow \alpha$ is used to denote a simple value assignment statement. We say that y can be output by $A(x_0, x_1, \ldots)$ if there is some random r such that $\mathcal{A}(x_0, x_1, \ldots; r) = y$. Also we use $|x|$ to denote the bit-length of string (or message) x, and $\overline{x}$ to denote the bit complement of x. Finally, we use $x \| y$ to denote concatenation of x and y.

Definition 2.1 (Public-key encryption). A public-key encryption scheme, noted as $\mathcal{PE}$, is a triplet $(\mathcal{K}; \mathcal{E}; \mathcal{D})$ with the following polynomial-time algorithms:

- $\mathcal{K}$ is a probabilistic key generation algorithm which, given a security parameter k (usually viewed as a unary input 1^k) produces , from its random source ω, a pair $(pk; sk)$ of public and secret keys.
- $\mathcal{E}$ is a probabilistic encryption algorithm which, given a public key pk generated by $\mathcal{K}$ and a message x, produces y, called the encryption of x under pk.
- $\mathcal{D}$ is a deterministic decryption algorithm which given a secret key sk and a ciphertext y, produces either a message x or a special symbol $\perp$ to state that y is an *invalid* ciphertext. It is required that for every message x and for every pair $(pk; sk)$ output by $\mathcal{K}$, $\mathcal{D}_{sk}(\mathcal{E}_{pk}(x)) = x$. It is possible that $\mathcal{D}_{sk'}(\mathcal{E}_{pk}(x)) = x'$ for some $x' \neq \perp$; this means that using a wrong key may result in a valid message.

Recall that a real-valued function $\varepsilon : \mathbb{N} \to \mathbb{R}$ is *negligible* if for every constant $c \geq 0$ there exists an integer k_c such that $|\varepsilon(k)| \leq k^{-c}$ for all $k > k_c$.

Note. We are assuming that the message and/or public key spaces are closed under bitwise complement. This is just to simplify the proofs though our proofs work for any closed (in the message space or the public key space, respectively), efficiently computable, and length-preserving unary operator put in place of bitwise complement. This operator does not have to be secret, hence can be a publicly defined function. Regarding Lemmas 3.18 and 3.27 which we have used bitwise complement as an involution (i.e., $\overline{\overline{x}} = x$), the only modification needed is replacing the bitwise complement operator in $\mathcal{A}_2$ (i.e., $\overline{m_1}$) with the inverse of the unary operator used in $\mathcal{A}_1$. Therefore, the operator should be reversible as well. This means that some of our results are not completely general.

Regarding the existence of public-key encryption schemes with public key space closed under some unary operator, we argue that some important systems satisfy this condition, e.g. in the "dual" version of Regev's lattice-based system [15], the public key is of the form $u = e * A$ for a small vector e, where $u \in \mathbb{Z}_q^n$, $e \in \mathbb{Z}_q^m$ with m sufficiently larger than $n * \log q$. In this case, every vector $u' \in \mathbb{Z}_q^n$ is a valid key since it has a corresponding secret key e' with $u' = e' * A$ (with very high probability over a random matrix A). In regard to the existence of public-key encryption schemes with message space closed under some unary operator, we insist that an encryption scheme with a k-bit message space $\{0,1\}^k$ would be closed under any length-preserving function f; for a concrete example with 1-bit messages (extendable to k-bit messages), see the completely non-malleable scheme proposed by Sepahi et al. [16].

2.1 Definitions of indistinguishability

Message indistinguishability (IND). *Message indistinguishability*, or briefly indistinguishability, is the first and most important notion for public-key encryption. This notion defines the *data privacy* of public-key encryption and formalizes an adversary's inability to learn any information about the plaintext x from a challenge ciphertext y. In other words, given a public key pk, two messages x_0 and x_1, and a ciphertext $y = \mathcal{E}_{pk}(x_b)$, for $b \in \{0,1\}$, no polynomial-time adversary is able to find which message has been used to obtain the challenge ciphertext y.

Consider a two-step adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ whose goal is to attack indistinguishability of public-key encryption. (1) Algorithm $\mathcal{A}_1$ takes in the public key pk, and returns two plaintext messages x_0 and x_1, plus a string $S_{\mathcal{A}}$ encoding state information to be handed to $\mathcal{A}_2$. (2) A message x_b, for $b \in \{0,1\}$, is chosen uniformly at random from the set $\{x_0, x_1\}$ and encrypted into a challenge ciphertext y. (3) Algorithm $\mathcal{A}_2$ is given the input $(y, S_{\mathcal{A}})$ and has to guess the index b of the plaintext being encrypted. The advantage of $\mathcal{A}$ is measured by the probability that it outputs the correct index bit of the challenge. The scheme is indistinguishable if

no adversary obtains an advantage significantly greater than one would obtain by flipping a coin. The formal definition of this notion is as follows [2]:

Definition 2.2 (Indistinguishability (IND)). Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption and let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary. For ATK $\in$ {CPA, CCA1, CCA2}, $k \in \mathbb{N}$, and b a random value in $\{0, 1\}$, let,

$$\mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \left|2 \cdot \Pr\left[\mathbf{Expt}^{\text{IND-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k) = b\right] - 1\right|$$

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

$$\begin{aligned}&\text{Experiment } \mathbf{Expt}^{\text{IND-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k)\\ &(pk, sk) \leftarrow \mathcal{K}(k);\ (x_0, x_1, S_{\mathcal{A}}) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk);\\ &y \leftarrow \mathcal{E}_{pk}(x_b);\\ &b^* \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}});\ \textbf{return}\ (b^*);\end{aligned}$$

and the oracles $\mathcal{O}_1, \mathcal{O}_2$ are defined as follows:

- if ATK = CPA, then $\mathcal{O}_1 = \varepsilon$ and $\mathcal{O}_2 = \varepsilon$;
- if ATK = CCA1, then $\mathcal{O}_1 = \mathcal{D}_{sk}(\cdot)$ and $\mathcal{O}_2 = \varepsilon$;
- if ATK = CCA2, then $\mathcal{O}_1 = \mathcal{D}_{sk}(\cdot)$ and $\mathcal{O}_2 = \mathcal{D}_{sk}(\cdot)$.

We say that $\mathcal{PE}$ is secure in the sense of IND-ATK if a polynomial-time $\mathcal{A}$ implies that $\mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE},\mathcal{A}}(\cdot)$ is negligible. We assume that $|x_0| = |x_1|$. In the case of CCA2, we further assume that $\mathcal{A}_2$ does not ask its oracle to decrypt the challenge ciphertext y.

Key indistinguishability (KI). Message indistinguishability (IND), as defined before, is about the message privacy of encryption, and does not guarantee that some information about the underlying key is leaking. Another important security notion for public-key encryption is *key indistinguishability* (KI). It is especially crucial for multi-user protocols, where privacy of ciphertexts (anonymity) is required. Key privacy formalizes the inability of an adversary to learn any information about the underlying key from the observed ciphertext(s). Being more specific, given two public keys pk_0 and pk_1, and the ciphertext $y = \mathcal{E}_{pk_b}(x)$ for $b \in \{0, 1\}$, no polynomial-time adversary should be able to find which public key has been used to generate y.

Consider a two-step adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ who is attacking key indistinguishability of public-key encryption. (1) Algorithm $\mathcal{A}_1$ is run on input the two

public keys pk_0, pk_1 and outputs a plaintext message x and the state information $S_{\mathcal{A}}$, to be handed to $\mathcal{A}_2$. (2) A key pk_b, for $b \in \{0,1\}$, is chosen uniformly at random from the set $\{pk_0, pk_1\}$ and used to encrypt the message x into the challenge ciphertext y. (3) Algorithm $\mathcal{A}_2$ is given the input $(y, S_{\mathcal{A}})$, and has to guess the index bit b of the public key used for encryption. The advantage of $\mathcal{A}$ is measured by the probability that it outputs the correct index bit of the challenge. The scheme is key indistinguishable if no adversary obtains an advantage that is significantly greater than random coin flipping. The formal definition of *key indistinguishability* (KI) is as follows [1]:

Definition 2.3 (Key indistinguishability (KI)). Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption and let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary. For ATK $\in$ {CPA, CCA1, CCA2}, $k \in \mathbb{N}$, and b a random value in $\{0,1\}$, let

$$\mathbf{Adv}^{\text{KI-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \left| 2 \cdot \Pr\left[\mathbf{Expt}^{\text{KI-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k) = b\right] - 1 \right|$$

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

$$\begin{aligned}
&\text{Experiment } \mathbf{Expt}^{\text{KI-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k)\\
&\quad (pk_0, sk_0) \leftarrow \mathcal{K}(k);\ (pk_1, sk_1) \leftarrow \mathcal{K}(k);\\
&\quad (x, S_{\mathcal{A}}) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk_0, pk_1);\ y = \mathcal{E}_{pk_b}(x);\\
&\quad b^* \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}});\ \textbf{return } (b^*);
\end{aligned}$$

and the oracles $\mathcal{O}_1, \mathcal{O}_2$ are defined as follows:

- if ATK = CPA, then $\mathcal{O}_1 = \varepsilon$ and $\mathcal{O}_2 = \varepsilon$;
- if ATK = CCA1, then $\mathcal{O}_1 = (\mathcal{D}_{sk_0}(\cdot), \mathcal{D}_{sk_1}(\cdot))$ and $\mathcal{O}_2 = \varepsilon$;
- if ATK = CCA2, then $\mathcal{O}_1 = (\mathcal{D}_{sk_0}(\cdot), \mathcal{D}_{sk_1}(\cdot))$ and $\mathcal{O}_2 = (\mathcal{D}_{sk_0}(\cdot), \mathcal{D}_{sk_1}(\cdot))$.

The scheme $\mathcal{PE}$ is said to be KI-ATK secure if the function $\mathbf{Adv}^{\text{KI-ATK}}_{\mathcal{PE},\mathcal{A}}(\cdot)$ is negligible for any adversary $\mathcal{A}$ whose time complexity is polynomial in k. In the case of CCA2, we assume that $\mathcal{A}_2$ does not ask its oracle to decrypt the challenge ciphertext y.

Complete indistinguishability (IND*). Although message indistinguishability and key indistinguishability reflect two main facets (i.e., data privacy and key privacy) of encryption, for some application we need a stronger notion that covers simultaneously both message and key privacy. *Complete indistinguishability* (IND*) is a notion that combines both requirements. Informally, it requires that

given two public keys pk_0 and pk_1, two messages x_0 and x_1, and the ciphertext $y = \mathcal{E}_{pk_b}(x_c)$, for $b, c \in \{0, 1\}$, there is no polynomial-time adversary who is able to find the public key (i.e., the value of index b) or the message (i.e., the value of index c) that have been used to generate the challenge ciphertext y.

Consider a two-step adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ who is attacking complete indistinguishability of public-key encryption. (1) Algorithm $\mathcal{A}_1$ is run on input of the public keys pk_0, pk_1 and outputs two plaintexts messages x_0 and x_1 plus a string $S_{\mathcal{A}}$ encoding information to be handed to $\mathcal{A}_2$. (2) A key pk_b, $b \in \{0, 1\}$, from the set $\{pk_0, pk_1\}$ and a message x_c, $c \in \{0, 1\}$, from the set $\{x_0, x_1\}$ is chosen uniformly at random, and the message x_c encrypted using the public key pk_b into a challenge ciphertext y. (3) Algorithm $\mathcal{A}_2$ is given the input $(y, S_{\mathcal{A}})$ and has to guess which public key or which plaintext is used to obtain the challenge ciphertext. The advantage of $\mathcal{A}$ is measured by the probability that it outputs at least one correct index bit b or c of the challenge. The scheme is completely indistinguishable if no adversary obtains an advantage significantly greater than random flips of two coins. Formally, we can write it as follows:

Definition 2.4 (Complete indistinguishability (IND*)). Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption and let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary. For ATK $\in$ {CPA, CCA1, CCA2}, $k \in \mathbb{N}$, and b, c two random values in $\{0, 1\}$, let,

$$\mathbf{Adv}^{\text{IND*-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \left| 4 \cdot \Pr\left[\mathbf{Expt}^{\text{IND*-ATK-}(b,c)}_{\mathcal{PE},\mathcal{A}}(k) \simeq (b, c)\right] - 3 \right| \tag{2.1}$$

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

Experiment $\mathbf{Expt}^{\text{IND*-ATK-}(b,c)}_{\mathcal{PE},\mathcal{A}}(k)$

$(pk_0, sk_0) \leftarrow \mathcal{K}(k)$; $(pk_1, sk_1) \leftarrow \mathcal{K}(k)$; $(x_0, x_1, S_{\mathcal{A}}) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk_0, pk_1)$;

$y = \mathcal{E}_{pk_b}(x_c)$; $(b^*, c^*) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$; **return** (b^*, c^*);

in which $(b^*, c^*) \simeq (b, c)$ whenever $(b^* = b) \vee (c^* = c)$, and the oracles $\mathcal{O}_1, \mathcal{O}_2$ are defined exactly as in Definition 2.3.

The scheme $\mathcal{PE}$ is said to be IND*-ATK secure if the function $\mathbf{Adv}^{\text{IND*-ATK}}_{\mathcal{PE},\mathcal{A}}(\cdot)$ is negligible for any adversary $\mathcal{A}$ whose time complexity is polynomial in k. We assume that $|x_0| = |x_1|$. In the case of CCA2, we further assume that $\mathcal{A}_2$ does not ask its oracle to decrypt the challenge ciphertext y.

Note that equation (2.1) can be viewed as the (rescaled) excess of the probability of correct guess by the adversary, i.e., $\Pr[\mathbf{Expt}^{\text{IND*-ATK-}(b,c)}_{\mathcal{PE},\mathcal{A}}(k) \simeq (b, c)]$, over the probability of random guess, i.e., $3/4$.

Note 1. The notion of complete indistinguishability presented here is different from the notion of *recipient anonymity* (RA) introduced by Gentry [10] for identity-based encryption. Firstly, we claim that our notion is more intuitive. Recall that 'a chain is only as strong as its weakest link'. In the context of public-key encryption, this means that such a scheme is insecure if an adversary can break its privacy, i.e., finding c, or its anonymity, i.e., finding b, or both of them. This is exactly our notion of IND*. On the other hand, the notion of RA proposed by Gentry says that a scheme is insecure if an adversary can break both its privacy and its anonymity at the same time. Obviously, this is far from the intuition mentioned above.

Note 2. Our notion of complete indistinguishability is different from a notion with the same name introduced by van Liesdonk [17] as well. The latter notion considers only one index b for both the plaintext and the public key. So, the adversary should distinguish between two pairs (x_0, pk_0) and (x_1, pk_1) in a game similar to ours. Again our notion is more realistic since it considers privacy and anonymity like two separate features, as they are (see Theorems 3.1 and 3.4).

2.2 Definitions of non-malleability

Non-malleability (NM). The indistinguishability is the main security notion for public-key encryption. However, in some applications this is not enough. This observation was made by Dolev et al. [6] who studied bidding protocols. To prove the security of protocols, they had to assume that the encryption used was non-malleable (NM). The encryption is non-malleable if knowing a challenge ciphertext y, the adversary cannot produce another valid ciphertext y^* such that the underlying plaintexts x, x^* are "meaningfully related" (for example, $x^* = x + 1$). In other words, given a public key pk and a ciphertext $y = \mathcal{E}_{pk}(x)$, there is no polynomial-time adversary to find another ciphertext $y^* = \mathcal{E}_{pk}(x^*)$ of a related message x^* encrypted under the same public key pk.

Consider an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ who attacks non-malleability of public-key encryption. (1) The Turing machine $\mathcal{A}_1$ is run with input of a public key pk and outputs the description of a probabilistic polynomial-time Turing machine M as the message sampler, and a state string $S_{\mathcal{A}}$ for further computation. (2) A message x is randomly chosen by running message sampler M, and its encryption y under pk is given to $\mathcal{A}_2$. (3) The goal of $\mathcal{A}_2$ is to output a binary relation $R_x(\cdot, \cdot)$ and a ciphertext $y^* \neq y$ whose decryption x^* is related to x according to $R_x(\cdot, \cdot)$, i.e., $R_x(x^*, x) = \mathbf{true}$. The scheme is non-malleable if for any adversary, the probability that $R(x^*, x)$ holds is not significantly better than the probability that $R(x^*, \tilde{x})$ holds for a random hidden $\tilde{x} \in M$.

The formal definition, due to Dolev et al. [6], is as follows:

Definition 2.5 (Non-malleability (NM)). Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption and let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary. For ATK $\in$ {CPA, CCA1, CCA2} and $k \in \mathbb{N}$ let,

$$\mathbf{Adv}^{\text{NM-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \left|\Pr\left[\mathbf{Expt}^{\text{NM-ATK-1}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right] - \Pr\left[\mathbf{Expt}^{\text{NM-ATK-0}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right]\right|$$

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

$$\begin{aligned}
&\text{Experiment } \mathbf{Expt}^{\text{NM-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k) \qquad (2.2)\\
&\quad (pk, sk) \leftarrow \mathcal{K}(k);\ (M, S_{\mathcal{A}}) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk);\\
&\quad x_0, x_1 \leftarrow M;\ y \leftarrow \mathcal{E}_{pk}(x_1);\\
&\quad (y^*, R_x) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}});\ x^* \leftarrow \mathcal{D}_{sk}(y^*);\\
&\quad \textbf{if } (x^* \neq \perp) \wedge (y^* \neq y) \wedge (R_x(x^*, x_b) = \textbf{true}) \textbf{ then}\\
&\qquad d \leftarrow 1;\\
&\quad \textbf{else}\\
&\qquad d \leftarrow 0;\\
&\quad \textbf{return } (d);
\end{aligned}$$

and the oracles $\mathcal{O}_1, \mathcal{O}_2$ are defined as follows:

- if ATK = CPA, then $\mathcal{O}_1 = \varepsilon$ and $\mathcal{O}_2 = \varepsilon$;
- if ATK = CCA1, then $\mathcal{O}_1 = \mathcal{D}_{sk}(\cdot)$ and $\mathcal{O}_2 = \varepsilon$;
- if ATK = CCA2, then $\mathcal{O}_1 = \mathcal{D}_{sk}(\cdot)$ and $\mathcal{O}_2 = \mathcal{D}_{sk}(\cdot)$.

In Experiment (2.2), $R_x(\cdot, \cdot)$ is a probabilistic polynomial-time Turing machine taking two inputs, say a, b, and producing as output either 0 (if the inputs a and b are not related as required by R_x), or 1 (if the inputs a and b are related as required by R_x).

It is said that $\mathcal{PE}$ is secure in the sense of NM-ATK if any adversary $\mathcal{A}$ whose running time is given by a polynomial $p(k)$ outputs a description of a message space M described by a sampling algorithm M, and a relation $R_x(\cdot, \cdot)$ with a negligible advantage $\mathbf{Adv}^{\text{NM-ATK}}_{\mathcal{PE},\mathcal{A}}(\cdot)$. We assume that M is valid, i.e., $|x| = |x'|$ for any x and x' that are given non-zero probability in the message space M. In the case of CCA2, we further assume that $\mathcal{A}_2$ does not ask its oracle to decrypt the challenge ciphertext y. We insist that the running time of the attacker $\mathcal{A}$ includes the time taken to run M and R_x, and that the combined run time is always bounded by a polynomial in the security parameter.

Key non-malleability (KNM). As in the case of indistinguishability, we can extend the notion of non-malleability to cover key non-malleability. In other words, given a public key pk and a ciphertext $y = \mathcal{E}_{pk}(x)$, there is no polynomial-time adversary who is able to find another $y^* = \mathcal{E}_{pk^*}(x)$ of the same message x encrypted under a related public key pk^*.

Consider a two-step adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ who attacks key non-malleability of public-key encryption. (1) The Turing machine $\mathcal{A}_1$ is run with input of a public key pk and outputs the description of a probabilistic polynomial-time Turing machine M as the message sampler, and a state string $S_{\mathcal{A}}$ for further computation handed to $\mathcal{A}_2$. (2) A message x is randomly chosen by running the message sampler M, and its encryption y is given to $\mathcal{A}_2$. (3) The goal of $\mathcal{A}_2$ is to output a binary relation $R_k(\cdot,\cdot)$, a public key pk^*, and a new ciphertext $y^* = \mathcal{E}_{pk^*}(x)$ whose decryption using the associated secret key sk^* is exactly x, but pk^* is related to the original public key pk according to $R_k(\cdot,\cdot)$. The scheme is key non-malleable if for any adversary the probability that $y^* = \mathcal{E}_{pk^*}(x) \wedge R_k(pk^*, pk)$ holds is not significantly better than the probability that $y^* = \mathcal{E}_{pk^*}(\tilde{x}) \wedge R_k(pk^*, pk)$ holds for a random hidden $\tilde{x} \in M$. The formal definition is as follows:

Definition 2.6 (Key non-malleability (KNM)). Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption and let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary. For ATK $\in$ {CPA, CCA1, CCA2} and $k \in \mathbb{N}$, let

$$\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \left|\Pr\left[\mathbf{Expt}^{\text{KNM-ATK-1}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right] - \Pr\left[\mathbf{Expt}^{\text{KNM-ATK-0}}_{\mathcal{PE},\mathcal{A},\$}(k) = 1\right]\right|$$

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

Experiment $\mathbf{Expt}^{\text{KNM-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k)$

$(pk, sk) \leftarrow \mathcal{K}(k)$; $(M, S_{\mathcal{A}}) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;

$x_0, x_1 \leftarrow M$; $y = \mathcal{E}_{pk}(x_1)$;

$(y^*, pk^*, R_k) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$;

if $(y^* = \mathcal{E}_{pk^*}(x_b)) \wedge (pk^* \neq pk) \wedge (R_k(pk^*, pk) = \textbf{true})$ **then**

  $d \leftarrow 1$;

else

  $d \leftarrow 0$;

return (d);

in which the oracles $\mathcal{O}_1, \mathcal{O}_2$ are defined exactly as in Definition 2.2, and $R_k(\cdot,\cdot)$ is a probabilistic polynomial-time Turing machine taking two inputs, and producing

as output either 0 or 1. Also, the equality check $y^* = \mathcal{E}_{pk^*}(x_b)$ in the "if" clause means that there should exist random coins such that $\mathcal{E}_{pk^*}(x_b)$ outputs y^*.

It is said that $\mathcal{PE}$ is secure in the sense of KNM-ATK if any polynomial-time adversary $\mathcal{A}$ outputs description of a message space described by a sampling algorithm M, and a relation $R_k(\cdot,\cdot)$ with a negligible advantage $\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE},\mathcal{A}}(\cdot)$. We assume that M is valid, i.e., $|x| = |x'|$ for any x and x' that are given non-zero probability in the message space M. In the case of CCA2, we further assume that $\mathcal{A}_2$ does not ask its oracle to decrypt the challenge ciphertext y. We insist that the running time of the attacker $\mathcal{A}$ includes the time taken to run M and R_k, and that the combined run time is always bounded by a polynomial in the security parameter.

Complete non-malleability (NM*). Fischlin [9] defined the notion of complete non-malleability (NM*) in order to evaluate security of commitments protocols. In his proof, he required encryption to be non-malleable for both the message and key spaces. After that, Ventre and Visconti [18] re-defined this notion using the game-based scenario. Based on [18], the complete non-malleability is defined as follows. Given a public key pk and a ciphertext $y = \mathcal{E}_{pk}(x)$, there is no polynomial-time adversary who is able to find another ciphertext $y^* = \mathcal{E}_{pk^*}(x^*)$ of a related message x^* encrypted under a related public key pk^* (note that at least one of y^* or pk^* should be different from their original counterparts y and pk).

Consider a two-step adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ who attacks complete non-malleability of public-key encryption. (1) The Turing machine $\mathcal{A}_1$ is run with input of a public key pk and outputs the description of a probabilistic polynomial-time Turing machine M to run it at next step as message sampler, and a state string $S_{\mathcal{A}}$ for further computation to be handed to $\mathcal{A}_2$. (2) A message x is randomly chosen by running the message sampler M and its encryption y under pk is given to $\mathcal{A}_2$. (3) The goal of $\mathcal{A}_2$ is to output description of a relation $R(\cdot,\cdot,\cdot,\cdot,\cdot)$, a public key pk^*, and a ciphertext $y^* = \mathcal{E}_{pk^*}(x^*)$ for which the relation $R(x^*, x, y^*, pk^*, pk)$ is satisfied. The scheme is completely non-malleable if for any adversary the probability that $y^* = \mathcal{E}_{pk^*}(x^*) \wedge (y^* \neq y \vee pk^* \neq pk) \wedge R(x^*, x, y^*, pk^*, pk)$ holds is not significantly better than the probability that $y^* = \mathcal{E}_{pk^*}(x^*) \wedge (y^* \neq y \vee pk^* \neq pk) \wedge R(x^*, \tilde{x}, y^*, pk^*, pk)$ holds for a random $\tilde{x} \in M$. The formal game-based definition of this notion, due to Ventre and Visconti [18], is as follows:

Definition 2.7 (Complete non-malleability (NM*)). Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary. For ATK $\in$ {CPA, CCA1, CCA2} and $k \in \mathbb{N}$ let

$$\mathbf{Adv}^{\text{NM*-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \left|\Pr\left[\mathbf{Expt}^{\text{NM*-ATK-1}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right] - \Pr\left[\mathbf{Expt}^{\text{NM*-ATK-0}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right]\right|$$

where, for $b \in \{0,1\}$, the experiment $\mathbf{Expt}^{\text{NM*-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k)$ is defined as follows:

Experiment $\mathbf{Expt}^{\text{NM*-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k)$

$(pk, sk) \leftarrow \mathcal{K}(k)$; $(M, S_{\mathcal{A}}) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk)$;

$x_0, x_1 \leftarrow M$; $y = \mathcal{E}_{pk}(x_1)$; $(y^*, pk^*, R) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$;

if $\exists x^*$s.t. $(y^* = \mathcal{E}_{pk^*}(x^*)) \wedge (y^* \neq y \vee pk^* \neq pk) \wedge$

$(x^* \neq \perp) \wedge R(x^*, x_b, y^*, pk^*, pk) =$ **true then**

$d \leftarrow 1$;

else

$d \leftarrow 0$;

return (d);

in which the oracles $\mathcal{O}_1, \mathcal{O}_2$ are defined in the same manner as for Definition 2.2, and R is a probabilistic polynomial-time Turing machine taking 5 inputs, and producing as output either 0 or 1.

It is said that $\mathcal{PE}$ is secure in the sense of NM*-ATK if any polynomial-time adversary $\mathcal{A}$ outputs a description of a message space, described by a sampling algorithm M, and a relation R with a negligible advantage $\mathbf{Adv}^{\text{NM*-ATK}}_{\mathcal{PE},\mathcal{A}}(\cdot)$. We assume that M is valid, i.e., $|x| = |x'|$ for any x and x' that are given non-zero probability in the message space M. In the case of CCA2, we further assume that $\mathcal{A}_2$ does not ask its oracle to decrypt the challenge ciphertext y. We insist that the running time of the attacker $\mathcal{A}$ includes the time taken to run M and R, and that the combined run time is always bounded by a polynomial in the security parameter.

3 Security model

In Section 2 we considered six notions of security for public-key encryption. In this section we extensively study relative strengths of different notions. Result of this section is the full picture of relationships (i.e., implications and separations) among the security notions for public-key encryption schemes, shown in Figure 1.

3.1 Indistinguishability proofs

In this section we examine relative strengths of all indistinguishability notion. To this end, for every two notions of indistinguishability we prove a theorem that shows an implication or a separation.

Zhang et al. [19] *informally* showed that standard message indistinguishability and key indistinguishability are *orthogonal* notions and none of them implies the other. Below we formally prove this result.

Theorem 3.1. *IND-ATK* $\not\Rightarrow$ *KI-ATK for ATK* $\in \{$*CPA, CCA1, CCA2*$\}$.

Proof. Assume there exists some IND-ATK secure encryption $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is meaningless. To prove the theorem, based on $\mathcal{PE}$ we construct a new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$, which is IND-ATK secure but not secure in the sense of KI-ATK.

The new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ is defined as follows:

Algorithm $\mathcal{K}'(k)$	**Algorithm** $\mathcal{E}'_{pk'}(x)$	**Algorithm** $\mathcal{D}'_{sk'}(y \| pk')$
$(pk, sk) \leftarrow \mathcal{K}(k)$	$y \leftarrow \mathcal{E}_{pk'}(x)$	parse sk' as $sk \| pk$
$pk' \leftarrow pk$	**return** $(y \| pk')$	**if** $pk' = pk$ **then**
$sk' \leftarrow sk \| pk$		**return** $(\mathcal{D}_{sk}(y))$
return (pk, sk)		**else return** $(\perp)$

In other words, a ciphertext in the new scheme $\mathcal{PE}'$ is a pair $y \| pk$ consisting of the encryption of the message and the public key used for the encryption process. The second component is ignored during decryption.

Lemma 3.2. $\mathcal{PE}'$ *is not secure in the KI-ATK sense.*

Proof. It is intuitively obvious that the scheme $\mathcal{PE}'$ is not secure in the sense of KI-ATK since given any ciphertext $y = y' \| pk'$ of $\mathcal{PE}'$, the adversary can detect which key has been used to encrypt the corresponding plaintext.

Formally, consider the following KI-CPA adversary: On input (pk_0, pk_1) the algorithm $\mathcal{A}_1$ outputs $(x, S_{\mathcal{A}})$ where x is a random plaintext and $S_{\mathcal{A}} = (pk_0, pk_1)$. On input $(y \| pk, S_{\mathcal{A}})$ the algorithm $\mathcal{A}_2$ outputs $b^* = 0$ if $pk = pk_0$, and $b^* = 1$ otherwise. For this adversary we always have $y = \mathcal{E}'_{pk_{b^*}}(x)$ and hence $\mathbf{Adv}^{\text{KI-CPA}}_{\mathcal{PE}',\mathcal{A}}(k) = 1$. This shows that $\mathcal{PE}'$ is KI-CPA insecure and hence KI-ATK insecure in general. □

On the other hand, we prove that $\mathcal{PE}'$ retains the IND-ATK security of $\mathcal{PE}$:

Lemma 3.3. $\mathcal{PE}'$ *is secure in the sense of IND-ATK.*

Proof. We want to prove that if $\mathcal{PE}$ is IND-ATK secure, then $\mathcal{PE}'$ is IND-ATK secure, as well. To this end, Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be a polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of IND-ATK. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the IND-ATK sense, as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$(x_0, x_1, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}'_1}(pk)$	$b^* \leftarrow \mathcal{B}_2^{\mathcal{O}'_2}(y \| pk, S_{\mathcal{B}})$
$S_{\mathcal{A}} := (pk, S_{\mathcal{B}})$	**return** (b^*)
return $(x_0, x_1, S_{\mathcal{A}})$	

where $\mathcal{O}'_1$ and $\mathcal{O}'_2$ are defined based on the decryption oracle $\mathcal{D}'_{sk}(\cdot)$ which itself is defined based on the provided decryption oracle $\mathcal{D}_{sk}(\cdot)$ as follows: for any input $y\|pk$ we have $\mathcal{D}'_{sk}(y\|pk) := \mathcal{D}_{sk}(y)$.

Now note that $\mathcal{A}$ succeeds if $\mathcal{B}$ succeeds, hence

$$\begin{aligned}\mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE},\mathcal{A}}(k) &= \left|2 \cdot \Pr\left[\mathbf{Expt}^{\text{IND-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k) = b\right] - 1\right| \\ &= \left|2 \cdot \Pr\left[\mathbf{Expt}^{\text{IND-ATK-}b}_{\mathcal{PE}',\mathcal{B}}(k) = b\right] - 1\right| = \mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE}',\mathcal{B}}(k).\end{aligned}$$

This completes the proof of Lemma 3.3. □

Lemmas 3.2 and 3.3 together complete the proof of Theorem 3.1. □

Theorem 3.4. *KI-ATK* $\not\Rightarrow$ *IND-ATK for ATK* $\in$ {*CPA, CCA1, CCA2*}.

Proof. Assume that there exists some KI-ATK secure public-key encryption $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is insignificantly true. We now construct a new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ based on $\mathcal{PE}$ that is KI-ATK secure but not secure in the sense of IND-ATK.

The new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ is constructed as follows:

Algorithm $\mathcal{K}'(k)$	**Algorithm** $\mathcal{E}'_{pk}(x)$	**Algorithm** $\mathcal{D}'_{sk}(y\|x)$
$(pk, sk) \leftarrow \mathcal{K}(k)$	$y \leftarrow \mathcal{E}_{pk}(x)$	**return** $(\mathcal{D}_{sk}(y))$
return (pk, sk)	**return** $(y\|x)$	

In other words, a ciphertext in $\mathcal{PE}'$ is a pair $y\|x$ consisting of the encryption of the message, and the message itself. The second component is ignored during decryption.

Lemma 3.5. $\mathcal{PE}'$ *is not secure in the IND-ATK sense.*

Proof. It is obvious that the scheme $\mathcal{PE}'$ is not secure in the sense of IND since for two messages $x_0 = m\|0$ and $x_1 = m\|1$, the adversary can distinguish which message has been used to obtain the ciphertext $y\|x_b$, for $b \in \{0, 1\}$. □

On the other hand, we prove that the new encryption scheme $\mathcal{PE}'$ retains the KI-ATK security of $\mathcal{PE}$:

Lemma 3.6. *$\mathcal{PE}'$ is secure in the sense of KI-ATK.*

Proof. We show that if $\mathcal{PE}'$ is insecure in the sense of KI-ATK, then $\mathcal{PE}$ is insecure in the sense of KI-ATK. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be a polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of KI-ATK. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the KI-ATK sense, as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk_0, pk_1)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$(x, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}'_1}(pk_0, pk_1)$	$y_B := y\|x$
$S_{\mathcal{A}} := (x, S_{\mathcal{B}})$	$b^* \leftarrow \mathcal{B}_2^{\mathcal{O}'_2}(y_B, S_{\mathcal{B}})$
return $(x, S_{\mathcal{A}})$	**return** (b^*)

where $\mathcal{O}'_1$ and $\mathcal{O}'_2$ are defined based on the decryption oracles $\mathcal{D}'_{sk_i}(\cdot)$ for $i \in \{0, 1\}$ which in turn are defined based on the provided decryption oracles $\mathcal{D}_{sk_i}(\cdot)$ as follows: for any input $y\|x$ we have $\mathcal{D}'_{sk_i}(y\|x) := \mathcal{D}_{sk_i}(y)$.

Now note that $\mathcal{A}$ succeeds if $\mathcal{B}$ succeeds, hence

$$\begin{aligned}\mathbf{Adv}^{\text{KI-ATK}}_{\mathcal{PE},\mathcal{A}}(k) &= \left|2 \cdot \Pr\left[\mathbf{Expt}^{\text{KI-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k) = b\right] - 1\right| \\ &= \left|2 \cdot \Pr\left[\mathbf{Expt}^{\text{KI-ATK-}b}_{\mathcal{PE}',\mathcal{B}}(k) = b\right] - 1\right| = \mathbf{Adv}^{\text{KI-ATK}}_{\mathcal{PE}',\mathcal{B}}(k).\end{aligned}$$

This completes the proof of Lemma 3.6. □

Lemmas 3.5 and 3.6 together complete the proof of Theorem 3.4. □

Theorem 3.7. *IND*-ATK ⇒ IND-ATK for ATK ∈ {CPA, CCA1, CCA2}.*

Proof. We prove the contrapositive; assume that $\mathcal{PE}$ is an IND-ATK insecure encryption. So there is an adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE},\mathcal{B}}(\cdot)$ is non-negligible. We construct an IND*-ATK adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{IND*-ATK}}_{\mathcal{PE},\mathcal{A}}(\cdot)$ is non-negligible.

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk_0, pk_1)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$(x_0, x_1, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk_0)$	$c^* \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$S_{\mathcal{A}} := S_{\mathcal{B}}$	$b^* \leftarrow 1$
return $(x_0, x_1, S_{\mathcal{A}})$	**return** (b^*, c^*)

Now we calculate the advantage of $\mathcal{A}$:

$$\begin{aligned}
\mathbf{Adv}^{\text{IND*-ATK}}_{\mathcal{PE},\mathcal{A}}(k) &= \left|4 \cdot \Pr\left[\mathbf{Expt}^{\text{IND*-ATK-}(b,c)}_{\mathcal{PE},\mathcal{A}}(k) \simeq (b,c)\right] - 3\right| \\
&= \left|4 \cdot \Pr[(b^*, c^*) \simeq (b,c)] - 3\right| \\
&= \left|4 \cdot \Pr[b^* = b \vee c^* = c] - 3\right| \\
&= \left|4 \cdot \Pr[b^* = b] + 4 \cdot \Pr[c^* = c \wedge b^* \neq b] - 3\right| \\
&= \left|4 \cdot \Pr[b^* = b] + 4 \cdot \Pr[c^* = c | b^* \neq b] \cdot \Pr[b^* \neq b] - 3\right| \\
&= \left|4 \cdot \Pr[b = 1] + 4 \cdot \Pr[c^* = c | b = 0] \cdot \Pr[b = 0] - 3\right| \\
&= \left|4 \cdot \frac{1}{2} + 4 \cdot \frac{1}{2} \cdot \left(\mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE},\mathcal{B}}(k) + 1\right) \cdot \frac{1}{2} - 3\right| \\
&= \mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE},\mathcal{B}}(k).
\end{aligned}$$

Therefore if $\mathcal{PE}$ is an insecure public-key scheme in the sense of IND-ATK, then $\mathcal{PE}$ will be insecure in the sense of IND*-ATK as well. This completes the proof of Theorem 3.7. □

Theorem 3.8. *IND*-ATK* $\Rightarrow$ *KI-ATK for ATK* $\in$ {*CPA, CCA1, CCA2*}.

Proof. We prove the contrapositive; assume that $\mathcal{PE}$ is a KI-ATK insecure encryption. Therefore there is an adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{KI-ATK}}_{\mathcal{PE},\mathcal{B}}(\cdot)$ is non-negligible. We construct an IND*-ATK adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{IND*-ATK}}_{\mathcal{PE},\mathcal{A}}(\cdot)$ is non-negligible.

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk_0, pk_1)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$(x, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk_0, pk_1)$	$b^* \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$x_0 \leftarrow x;\ x_1 \leftarrow \overline{x}$	$c^* \leftarrow 1$
$S_{\mathcal{A}} := S_{\mathcal{B}}$	**return** (b^*, c^*)
return $(x_0, x_1, S_{\mathcal{A}})$	

Now a calculation similar to the proof of Theorem 3.7 shows that

$$\mathbf{Adv}^{\text{IND*-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \mathbf{Adv}^{\text{KI-ATK}}_{\mathcal{PE},\mathcal{B}}(k).$$

This completes the proof of Theorem 3.8. □

Theorem 3.9. *IND-ATK $\not\Rightarrow$ IND*-ATK for ATK $\in$ {CPA, CCA1, CCA2}.*

Proof. Assume that IND-ATK $\Rightarrow$ IND*-ATK. According to Theorem 3.8 we have IND*-ATK $\Rightarrow$ KI-ATK. Hence we should have IND-ATK $\Rightarrow$ KI-ATK. But this contradicts Theorem 3.1. Consequently, IND-ATK $\not\Rightarrow$ IND*-ATK. □

Theorem 3.10. *KI-ATK $\not\Rightarrow$ IND*-ATK for ATK $\in$ {CPA, CCA1, CCA2}.*

Proof. Assume that KI-ATK $\Rightarrow$ IND*-ATK. According to Theorem 3.7, we have IND*-ATK $\Rightarrow$ IND-ATK. Therefore we should have KI-ATK $\Rightarrow$ IND-ATK. But this contradicts Theorem 3.4 and we can conclude that KI-ATK $\not\Rightarrow$ IND*-ATK. □

3.2 Non-malleability proofs

In this section we examine the relations between different notions of non-malleability. To achieve this goal, for every two notions of non-malleability we prove a theorem that shows an implication or a separation.

Theorem 3.11. *NM-ATK $\not\Rightarrow$ KNM-ATK for ATK $\in$ {CPA, CCA1, CCA2}.*

Proof. Assume there exists some NM-ATK secure encryption $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is true in a meaningless manner. We now modify $\mathcal{PE}$ to a new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ which is also NM-ATK secure but not secure in the sense of KNM-ATK.

The new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ is constructed as follows:

Algorithm $\mathcal{K}'(k)$	**Algorithm** $\mathcal{E}'_{pk\|b}(x)$	**Algorithm** $\mathcal{D}'_{sk}(y)$
$(pk, sk) \leftarrow \mathcal{K}(k)$	**return** $(\mathcal{E}_{pk}(x))$	**return** $(\mathcal{D}_{sk}(y))$
$b \leftarrow \{0, 1\}$		
return $(pk\|b, sk)$		

In other words, a public key in the new scheme is a pair $pk\|b$ consisting of the original public key pk and a random bit b. During encryption, the second component is ignored.

Lemma 3.12. *$\mathcal{PE}'$ is not secure in the KNM-ATK sense.*

Proof. It is intuitively clear that the scheme $\mathcal{PE}'$ is not KNM-ATK secure since for a given $y = \mathcal{E}_{pk\|b}(x)$, the adversary can output y as the encryption of the same message x under a different yet related public key $pk\|\overline{b}$.

Formally, let a KNM-CPA adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be defined as follows: on input $pk\|b$ the algorithm $\mathcal{A}_1$ outputs the plaintext space M and the state $S_{\mathcal{A}} = pk\|b$; on input $(y, S_{\mathcal{A}})$ the algorithm $\mathcal{A}_2$ outputs $(y, pk\|\overline{b}, R_k)$ where, for any public keys pk^* and pk, and any two bits b^* and b, $R_k(pk^*\|b^*, pk\|b)$ is defined to be true if and only if $pk^* = pk$. $\mathcal{A}_2$ always outputs a different but related public key, therefore the probability that the experiment $\mathbf{Expt}^{\text{KNM-CPA-}b}_{\mathcal{PE}',\mathcal{A}}(k)$ outputs 1 is equal to the probability that $y = \mathcal{E}_{pk\|\overline{b}}(x_b)$. Since $\mathcal{E}_{pk\|b}(x) = \mathcal{E}_{pk\|\overline{b}}(x)$ for any x, pk, and b, this probability is 1 for $\mathbf{Expt}^{\text{KNM-CPA-1}}_{\mathcal{PE}',\mathcal{A}}(k)$ and 0 for $\mathbf{Expt}^{\text{KNM-CPA-0}}_{\mathcal{PE}',\mathcal{A}}(k)$. Hence we have $\mathbf{Adv}^{\text{KNM-CPA}}_{\mathcal{PE}',\mathcal{A}}(k) = 1$ and therefore $\mathcal{PE}'$ is not KNM-CPA secure and in general not KNM-ATK secure. □

On the other hand, we prove that $\mathcal{PE}'$ retains the NM-ATK security of $\mathcal{PE}$:

Lemma 3.13. *$\mathcal{PE}'$ is secure in the sense of NM-ATK.*

Proof. We prove that if $\mathcal{PE}'$ is insecure in the sense of NM-ATK, then $\mathcal{PE}$ is insecure in the sense of NM-ATK. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be a polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of NM-ATK. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the NM-ATK sense. The adversary $\mathcal{A}$ works as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$b \leftarrow \{0,1\}$	$(y^*, R_x) \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$pk' := pk\|b$	**return** (y^*, R_x)
$(M, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk')$	
$S_{\mathcal{A}} := S_{\mathcal{B}}$	
return $(M, S_{\mathcal{A}})$	

Note that $\mathcal{A}$ succeeds whenever $\mathcal{B}$ does, hence

$$\begin{aligned}
\mathbf{Adv}^{\text{NM-ATK}}_{\mathcal{PE},\mathcal{A}}(k) &= \left|\Pr\left[\mathbf{Expt}^{\text{NM-ATK-1}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right] - \Pr\left[\mathbf{Expt}^{\text{NM-ATK-0}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right]\right| \\
&= \left|\Pr\left[\mathbf{Expt}^{\text{NM-ATK-1}}_{\mathcal{PE}',\mathcal{B}}(k) = 1\right] - \Pr\left[\mathbf{Expt}^{\text{NM-ATK-0}}_{\mathcal{PE}',\mathcal{B}}(k) = 1\right]\right| \\
&= \mathbf{Adv}^{\text{NM-ATK}}_{\mathcal{PE}',\mathcal{B}}(k).
\end{aligned}$$

This completes the proof of Lemma 3.13. □

Lemmas 3.12 and 3.13 together complete the proof of Theorem 3.11. □

Theorem 3.14. *KNM-CCA2 ⇒ NM-CCA2.*

Proof. We prove the contrapositive; assume that $\mathcal{PE}$ is an insecure encryption scheme in the sense of NM-CCA2. Therefore there is an adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{NM-CCA2}}_{\mathcal{PE},\mathcal{B}}(\cdot)$ is non-negligible. We construct a KNM-CCA2 adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{KNM-CCA2}}_{\mathcal{PE},\mathcal{A}}(\cdot)$ is non-negligible as well.

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$(M_{\mathcal{B}}, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk)$	$(\hat{y}, R_x) \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$x_0 \leftarrow M_{\mathcal{B}};\ x_1 \leftarrow M_{\mathcal{B}}$	$\hat{x} \leftarrow \mathcal{D}_{sk}(\hat{y})$
$M_{\mathcal{A}} := \{x_0, x_1\}$	find the original plaintext x from $\hat{x}$ and R_x
$S_{\mathcal{A}} := (pk, S_{\mathcal{B}})$	$y^* \leftarrow \mathcal{E}_{\overline{pk}}(x)$
return $(M_{\mathcal{A}}, S_{\mathcal{A}})$	**return** $(y^*, \overline{pk}, R_k)$

where $R_k(\cdot,\cdot)$ is the complement relation, i.e., $R_k(a,b) = \mathbf{true}$ if and only if $a = \overline{b}$.

Now we calculate the advantage of $\mathcal{A}$:

$$\begin{aligned}
\mathbf{Adv}^{\text{KNM-CCA2}}_{\mathcal{PE},\mathcal{A}}(k) &= \left|\Pr\left[\mathbf{Expt}^{\text{KNM-CCA2-1}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right] - \Pr\left[\mathbf{Expt}^{\text{KNM-CCA2-0}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right]\right| \\
&= \left|\Pr\left[\mathbf{Expt}^{\text{NM-CCA2-1}}_{\mathcal{PE},\mathcal{B}}(k) = 1\right] - \Pr\left[\mathbf{Expt}^{\text{NM-CCA2-0}}_{\mathcal{PE},\mathcal{B}}(k) = 1\right]\right| \\
&= \mathbf{Adv}^{\text{NM-CCA2}}_{\mathcal{PE},\mathcal{B}}(k).
\end{aligned}$$

This completes the proof of Theorem 3.14. □

Theorem 3.15. *KNM-ATK ⇏ NM-ATK for ATK ∈ {CPA, CCA1}.*

Proof. Assume that there exists some KNM-ATK secure encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is insignificantly true. We now modify $\mathcal{PE}$ to a new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ which is also KNM-ATK secure but not secure in the NM-ATK sense. This will prove the theorem.

The new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ is defined as follows:

Algorithm $\mathcal{K}'(k)$	**Algorithm** $\mathcal{E}'_{pk}(x)$	**Algorithm** $\mathcal{D}'_{sk}(y_1 \| y_2)$
$(pk, sk) \leftarrow \mathcal{K}(k)$	$y_1 \leftarrow \mathcal{E}_{pk}(x)$	$x_1 \leftarrow \mathcal{D}_{sk}(y_1)$
return (pk, sk)	$y_2 \leftarrow \mathcal{E}_{pk}(\overline{x})$	$x_2 \leftarrow \mathcal{D}_{sk}(y_2)$
	return $(y_1 \| y_2)$	**if** $x_1 = \overline{x_2}$ **then**
		return (x_1)
		else return $(\perp)$

In other words, a ciphertext in the new scheme is a pair $y_1 \| y_2$ consisting of the encryption of the message, and the encryption of the message complement. We prove in the following that $\mathcal{PE}'$ is KNM-ATK secure but not NM-ATK secure.

Lemma 3.16. *$\mathcal{PE}'$ is not secure in the NM-ATK sense.*

Proof. Given a ciphertext $y_1 \| y_2$ of a message x under public key pk, it is easy to create a ciphertext of $\overline{x}$ under the same public key pk: just output $y_2 \| y_1$. Thus the scheme is not non-malleable. □

On the other hand, we prove that $\mathcal{PE}'$ retains the KNM-ATK security of $\mathcal{PE}$:

Lemma 3.17. *$\mathcal{PE}'$ is secure in the sense of KNM-ATK.*

Proof. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be some polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of KNM-ATK. We want to show that $\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE}',\mathcal{B}}$ is negligible. To this end, consider the following probability, defined for $i, j \in \{0, 1\}$:

$$
\begin{aligned}
p_k(i, j) := \Pr\Big[& (pk', sk') \leftarrow \mathcal{K}'(k);\ (M_{\mathcal{B}}, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}'_1}(pk'); \\
& (x_0, x_1) \leftarrow_R M_{\mathcal{B}};\ y_1 \leftarrow \mathcal{E}_{pk}(x_i);\ y_2 \leftarrow \mathcal{E}_{pk}(\overline{x_j}); \\
& y' \leftarrow y_1 \| y_2;\ (y'^*, pk'^*, R'_k) \leftarrow \mathcal{B}_2^{\mathcal{O}'_2}(y', S_{\mathcal{B}}) : \\
& y'^* = \mathcal{E}'_{pk'^*}(x_0) \wedge pk'^* \neq pk' \wedge R'_k(pk'^*, pk') \Big].
\end{aligned}
$$

We know that $\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE}',\mathcal{B}} = |p_k(1,1) - p_k(0,0)|$. The following lemmas state that, under our assumption, i.e., KNM-ATK security of $\mathcal{PE}$, the differences $p_k(1,1) - p_k(1,0)$ and $p_k(1,0) - p_k(0,0)$ must be both negligible. This will complete the proof since

$$\begin{aligned}\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE}',\mathcal{B}} &= \left|p_k(1,1) - p_k(0,0)\right| \\ &= \left|[p_k(1,1) - p_k(1,0)] + [p_k(1,0) - p_k(0,0)]\right|\end{aligned}$$

being the sum of two negligible functions, will be negligible.

Lemma 3.18. *$p_k(1,1) - p_k(1,0)$ is negligible.*

Proof. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the KNM-ATK sense, as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$(M_{\mathcal{B}}, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}'_1}(\overline{pk}, pk)$	$y_1 \leftarrow \mathcal{E}_{pk}(\overline{m_1});\ y_2 \leftarrow y$
$(x_0, x_1) \leftarrow M_{\mathcal{B}}$	(y'^*, pk'^*, R'_k)
$m_0 \leftarrow \overline{x_0};\ m_1 \leftarrow \overline{x_1};\ M_{\mathcal{A}} \leftarrow \{m_0, m_1\}$	$\quad \leftarrow \mathcal{B}_2^{\mathcal{O}'_2}(y_1 \| y_2, S_{\mathcal{B}})$
$S_{\mathcal{A}} \leftarrow S_{\mathcal{B}} \| (m_0, m_1)$; **return** $(M_{\mathcal{A}}, S_{\mathcal{A}})$	**return** (y^*, pk^*, R_k)

We observe that

$$\begin{aligned}&\Pr\Big[(pk, sk) \leftarrow \mathcal{K}(k);\ (M_{\mathcal{A}}, S_{\mathcal{A}}) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk); \\ &\quad m_0, m_1 \leftarrow M_{\mathcal{A}};\ y = \mathcal{E}_{pk}(m_1); \\ &\quad (y^*, pk^*, R_k) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}}) : \\ &\quad y^* = \mathcal{E}_{pk^*}(x_b) \wedge pk^* \neq pk \wedge R_k(pk^*, pk)\Big] = p_k(1,1), \\ &\Pr\Big[(pk, sk) \leftarrow \mathcal{K}(k);\ (M_{\mathcal{A}}, S_{\mathcal{A}}) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk); \\ &\quad x_0, x_1 \leftarrow M_{\mathcal{A}};\ y = \mathcal{E}_{pk}(m_0); \\ &\quad (y^*, pk^*, R_k) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}}) : \\ &\quad y^* = \mathcal{E}_{pk^*}(x_b) \wedge pk^* \neq pk \wedge R_k(pk^*, pk)\Big] = p_k(1,0).\end{aligned}$$

Thus $\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE},\mathcal{B}} = p_k(1,1) - p_k(1,0)$. The assumed security of $\mathcal{PE}$ in the KNM-ATK sense now implies that the latter difference is negligible. □

Lemma 3.19. *$p_k(1,0) - p_k(0,0)$ is negligible.*

Proof. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the KNM-ATK sense, as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$(M_{\mathcal{B}}, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}'_1}(pk, \overline{pk})$	$y_2 \leftarrow y;\ y_1 \leftarrow \mathcal{E}_{\overline{pk}}(\overline{x_0});$
$(x_0, x_1) \leftarrow M_{\mathcal{B}}$	$(y'^*, pk'^*, R'_k) \leftarrow \mathcal{B}_2^{\mathcal{O}'_2}(y_1 \| y_2, S_{\mathcal{B}})$
$M_{\mathcal{A}} \leftarrow \{\overline{x_0}, \overline{x_1}\}$	**return** (y^*, pk^*, R_k)
$S_{\mathcal{A}} \leftarrow S_{\mathcal{B}} \| M_{\mathcal{A}}$	
return $(M_{\mathcal{A}}, S_{\mathcal{A}})$	

We observe that

$$\begin{aligned}
&\Pr\Big[(pk, sk) \leftarrow \mathcal{K}(k);\ (M_{\mathcal{A}}, S_{\mathcal{A}}) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk);\\
&\quad x_0, x_1 \leftarrow M_{\mathcal{A}};\ y = \mathcal{E}_{pk}(x_1);\\
&\quad (y^*, pk^*, R_k) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}}) :\\
&\quad y^* = \mathcal{E}_{pk^*}(x_b) \wedge pk^* \neq pk \wedge R_k(pk^*, pk)\Big] = p_k(1, 0),\\
&\Pr\Big[(pk, sk) \leftarrow \mathcal{K}(k);\ (M_{\mathcal{A}}, S_{\mathcal{A}}) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk);\\
&\quad x_0, x_1 \leftarrow M_{\mathcal{A}};\ y = \mathcal{E}_{pk}(x_0);\\
&\quad (y^*, pk^*, R_k) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}}) :\\
&\quad y^* = \mathcal{E}_{pk^*}(x_b) \wedge pk^* \neq pk \wedge R_k(pk^*, pk)\Big] = p_k(0, 0).
\end{aligned}$$

Thus $\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE},\mathcal{B}} = p_k(1,0) - p_k(0,0)$. The assumed security of $\mathcal{PE}$ in the KNM-ATK sense now implies that the latter difference is negligible. □

Therefore if $\mathcal{PE}'$ is an insecure public-key scheme in the sense of KNM-ATK, then $\mathcal{PE}$ will be insecure in the sense of KNM-ATK as well. This completes the proof of Lemma 3.17. □

Lemmas 3.16 and 3.17 together complete the proof of Theorem 3.15. □

The following theorem was stated as Theorem 1 in [18] and the authors gave an informal proof sketch for it. We prove the theorem formally below.

Theorem 3.20. *NM-ATK ⇏ NM*-ATK for ATK ∈ {CPA, CCA1, CCA2}.*

Proof. Assume there exists NM-ATK secure encryption $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is true in a meaningless manner. To prove the theorem, we modify $\mathcal{PE}$ to a new encryption $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ (exactly similar to the

scheme $\mathcal{PE}'$ used in the proof of Theorem 3.11 with $pk' = pk\|b$) which is also NM-ATK secure but not secure in the sense of NM*-ATK.

Lemma 3.21. *$\mathcal{PE}'$ is not secure in the NM*-ATK sense.*

Proof. It is obvious that the scheme $\mathcal{PE}'$ is not secure in the sense of KNM since given any ciphertext $y = \mathcal{E}_{pk\|0}(x)$ of $\mathcal{PE}'$, the adversary can generate a new ciphertext $y^* = \mathcal{E}_{pk\|1}(x)$ of the same plaintext under another related public key $pk\|1$. □

Now, we prove that $\mathcal{PE}'$ retains the NM-ATK security of $\mathcal{PE}$.

Lemma 3.22. *$\mathcal{PE}'$ is secure in the sense of NM-ATK.*

Proof. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be a polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of NM-ATK. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the NM-ATK sense. The adversary $\mathcal{A}$ is defined as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$b \leftarrow \{0,1\}$	$(y^*, R_x) \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$pk' := pk\|b$	**return** (y^*, R_x)
$(M, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk')$	
$S_{\mathcal{A}} := S_{\mathcal{B}}$	
return $(M, S_{\mathcal{A}})$	

Note that $\mathcal{A}$ is successful whenever $\mathcal{B}$ is; hence, similar to the proof of Lemma 3.13, we obtain

$$\mathbf{Adv}^{\text{NM-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \mathbf{Adv}^{\text{NM-ATK}}_{\mathcal{PE}',\mathcal{B}}(k).$$

This completes the proof of Lemma 3.22. □

Lemmas 3.21 and 3.22 together complete the proof of Theorem 3.20. □

Theorem 3.23. *NM*-ATK ⇒ NM-ATK for ATK ∈ {CPA, CCA1, CCA2}.*

Proof. We prove the contrapositive; assume that $\mathcal{PE}$ is an insecure encryption in the sense of NM-CCA2. Therefore there is an adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{NM-CCA2}}_{\mathcal{PE},\mathcal{B}}(\cdot)$ is non-negligible. To this end, we describe an NM*-CCA2 adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{NM*-CCA2}}_{\mathcal{PE},\mathcal{A}}(\cdot)$ is non-negligible.

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$(M, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk)$	$(y^*, R_x) \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$S_{\mathcal{A}} := S_{\mathcal{B}}$	**return** (y^*, pk, R)
return $(M, S_{\mathcal{A}})$	

where the quinary relation R is simply defined based on the relation R_x as follows: $R(x^*, x, y^*, pk^*, pk) = \textbf{true}$ if and only if $R_x(x^*, x) = \textbf{true}$.

Now note that $\mathcal{A}$ succeeds whenever $\mathcal{B}$ does, hence

$$\begin{aligned}\mathbf{Adv}^{\text{NM*-CCA2}}_{\mathcal{PE},\mathcal{A}}(k) &= \left|\Pr\left[\mathbf{Expt}^{\text{NM*-CCA2-1}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right] - \Pr\left[\mathbf{Expt}^{\text{NM*-CCA2-0}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right]\right| \\ &= \left|\Pr\left[\mathbf{Expt}^{\text{NM-CCA2-1}}_{\mathcal{PE},\mathcal{B}}(k) = 1\right] - \Pr\left[\mathbf{Expt}^{\text{NM-CCA2-0}}_{\mathcal{PE},\mathcal{B}}(k) = 1\right]\right| \\ &= \mathbf{Adv}^{\text{NM-CCA2}}_{\mathcal{PE},\mathcal{B}}(k).\end{aligned}$$

This completes the proof of Theorem 3.23. □

Theorem 3.24. *KNM-ATK* $\not\Rightarrow$ *NM*-ATK for ATK* $\in$ *{CPA, CCA1, CCA2}.*

Proof. Assume that there exists some KNM-ATK secure encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is true in a meaningless manner. We now modify $\mathcal{PE}$ to a new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ which is also KNM-ATK secure but not secure in the NM*-ATK sense. This will prove the theorem.

The new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ is defined as follows:

Algorithm $\mathcal{K}'(k)$	**Algorithm** $\mathcal{E}'_{pk_1 \| pk_2}(x)$	**Algorithm** $\mathcal{D}'_{sk_1 \| sk_2}(y_1 \| y_2)$
$(pk_1, sk_1) \leftarrow \mathcal{K}(k)$	$y_1 \leftarrow \mathcal{E}_{pk_1}(x)$	$x_1 \leftarrow \mathcal{D}_{sk_1}(y_1)$
$(pk_2, sk_2) \leftarrow \mathcal{K}(k)$	$y_2 \leftarrow \mathcal{E}_{pk_2}(\overline{x})$	$x_2 \leftarrow \mathcal{D}_{sk_2}(y_2)$
$pk' \leftarrow (pk_1, pk_2)$	**return** $(y_1 \| y_2)$	**if** $x_1 = \overline{x_2}$ **then**
$sk' \leftarrow (sk_1, sk_2)$		**return** (x_1)
return (pk', sk')		**else return** $(\perp)$

In other words, a ciphertext in the new scheme is a pair $y_1 \| y_2$ consisting of the encryption of the message using the first part of the public key, and the encryption of the message complement using the second part of the public key. We prove in the following that $\mathcal{PE}'$ is KNM-ATK secure but not NM*-ATK secure.

Lemma 3.25. *$\mathcal{PE}'$ is not secure in the NM*-ATK sense.*

Proof. Given a ciphertext $y_1 \| y_2$ of a message x under public key $pk_1 \| pk_2$, it is easy to create a ciphertext of $\overline{x}$ under public key $pk_2 \| pk_1$: just output $y_2 \| y_1$. Thus the scheme is not completely non-malleable. □

On the other hand, we prove that $\mathcal{PE}'$ retains the KNM-ATK security of $\mathcal{PE}$:

Lemma 3.26. *$\mathcal{PE}'$ is secure in the sense of KNM-ATK.*

Proof. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be some polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of KNM-ATK. We want to show that $\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE}',\mathcal{B}}$ is negligible. To this end, consider the following probability, defined for $i, j \in \{0, 1\}$:

$$
\begin{aligned}
p_k(i,j) := \Pr\Big[& (pk', sk') \leftarrow \mathcal{K}'(k);\ (M_{\mathcal{B}}, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}'_1}(pk'); \\
& (x_0, x_1) \leftarrow_R M_{\mathcal{B}};\ y_1 \leftarrow \mathcal{E}_{pk_1}(x_i);\ y_2 \leftarrow \mathcal{E}_{pk_2}(\overline{x_j}); \\
& y' \leftarrow y_1 \| y_2;\ (y'^*, pk'^*, R'_k) \leftarrow \mathcal{B}_2^{\mathcal{O}'_2}(y', S_{\mathcal{B}}) : \\
& y'^* = \mathcal{E}'_{pk'^*}(x_0) \wedge pk'^* \neq pk' \wedge R'_k(pk'^*, pk') \Big].
\end{aligned}
$$

We know that $\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE}',\mathcal{B}} = p_k(1,1) - p_k(0,0)$. The following lemmas state that, under our assumption, i.e., KNM-ATK security of $\mathcal{PE}$, the differences $p_k(1,1) - p_k(1,0)$ and $p_k(1,0) - p_k(0,0)$ must be both negligible. This will complete the proof since

$$
\begin{aligned}
\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE}',\mathcal{B}} &= p_k(1,1) - p_k(0,0) \\
&= [p_k(1,1) - p_k(1,0)] + [p_k(1,0) - p_k(0,0)]
\end{aligned}
$$

being the sum of two negligible functions, will be negligible.

Lemma 3.27. *$p_k(1,1) - p_k(1,0)$ is negligible.*

Proof. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the KNM-ATK sense, as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$(pk', sk') \leftarrow \mathcal{K}(k)$	$y_1 \leftarrow \mathcal{E}_{pk}(\overline{m_1});\ y_2 \leftarrow y$
$(M_{\mathcal{B}}, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}'_1}(\overline{pk}, pk)$	(y'^*, pk'^*, R'_k)
$(x_0, x_1) \leftarrow M_{\mathcal{B}}$	$\quad \leftarrow \mathcal{B}_2^{\mathcal{O}'_2}(y_1 \| y_2, S_{\mathcal{B}})$
$m_0 \leftarrow \overline{x_0};\ m_1 \leftarrow \overline{x_1};\ M_{\mathcal{A}} \leftarrow \{m_0, m_1\}$	**return** (y^*, pk^*, R_k)
$S_{\mathcal{A}} \leftarrow S_{\mathcal{B}} \| (m_0, m_1)$; **return** $(M_{\mathcal{A}}, S_{\mathcal{A}})$	

We observe that

$$\Pr\Big[(pk,sk)\leftarrow\mathcal{K}(k);\ (M_{\mathcal{A}},S_{\mathcal{A}})\leftarrow\mathcal{A}_1^{\mathcal{O}_1}(pk);\ m_0,m_1\leftarrow M_{\mathcal{A}};\ y=\mathcal{E}_{\overline{pk}}(m_1);\ (y^*,pk^*,R_k)\leftarrow\mathcal{A}_2^{\mathcal{O}_2}(y,S_{\mathcal{A}}):\ y^*=\mathcal{E}_{pk^*}(x_b)\wedge pk^*\neq pk\wedge R_k(pk^*,pk)\Big]=p_k(1,1),$$

$$\Pr\Big[(pk,sk)\leftarrow\mathcal{K}(k);\ (M_{\mathcal{A}},S_{\mathcal{A}})\leftarrow\mathcal{A}_1^{\mathcal{O}_1}(pk);\ x_0,x_1\leftarrow M_{\mathcal{A}};\ y=\mathcal{E}_{\overline{pk}}(m_0);\ (y^*,pk^*,R_k)\leftarrow\mathcal{A}_2^{\mathcal{O}_2}(y,S_{\mathcal{A}}):\ y^*=\mathcal{E}_{pk^*}(x_b)\wedge pk^*\neq pk\wedge R_k(pk^*,pk)\Big]=p_k(1,0).$$

Thus $\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE},\mathcal{B}}=p_k(1,1)-p_k(1,0)$. The assumed security of $\mathcal{PE}$ in the KNM-ATK sense now implies that the latter difference is negligible. □

Lemma 3.28. *$p_k(1,0)-p_k(0,0)$ is negligible.*

Proof. We construct an adversary $\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the KNM-ATK sense, as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y,S_{\mathcal{A}})$
$(pk',sk')\leftarrow\mathcal{K}(k)$	$y_2\leftarrow y;\ y_1\leftarrow\mathcal{E}_{\overline{pk}}(\overline{x_0});$
$(M_{\mathcal{B}},S_{\mathcal{B}})\leftarrow\mathcal{B}_1^{\mathcal{O}_1'}(pk,\overline{pk})$	$(y'^*,pk'^*,R_k')\leftarrow\mathcal{B}_2^{\mathcal{O}_2'}(y_1\|y_2,S_{\mathcal{B}})$
$(x_0,x_1)\leftarrow M_{\mathcal{B}}$	**return** (y^*,pk^*,R_k)
$M_{\mathcal{A}}\leftarrow\{\overline{x_0},\overline{x_1}\}$	
$S_{\mathcal{A}}\leftarrow S_{\mathcal{B}}\|M_{\mathcal{A}}$	
return $(M_{\mathcal{A}},S_{\mathcal{A}})$	

We observe that

$$\Pr\Big[(pk,sk)\leftarrow\mathcal{K}(k);\ (M_{\mathcal{A}},S_{\mathcal{A}})\leftarrow\mathcal{A}_1^{\mathcal{O}_1}(pk);\ x_0,x_1\leftarrow M_{\mathcal{A}};\ y=\mathcal{E}_{pk}(x_1);\ (y^*,pk^*,R_k)\leftarrow\mathcal{A}_2^{\mathcal{O}_2}(y,S_{\mathcal{A}}):\ y^*=\mathcal{E}_{pk^*}(x_b)\wedge pk^*\neq pk\wedge R_k(pk^*,pk)\Big]=p_k(1,0),$$

$$\Pr\Big[(pk, sk) \leftarrow \mathcal{K}(k);\ (M_{\mathcal{A}}, S_{\mathcal{A}}) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(pk);$$
$$x_0, x_1 \leftarrow M_{\mathcal{A}};\ y = \mathcal{E}_{pk}(x_0);$$
$$(y^*, pk^*, R_k) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}}) :$$
$$y^* = \mathcal{E}_{pk^*}(x_b) \wedge pk^* \neq pk \wedge R_k(pk^*, pk)\Big] = p_k(0,0).$$

Thus $\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE},\mathcal{B}} = p_k(1,0) - p_k(0,0)$. The assumed security of $\mathcal{PE}$ in the KNM-ATK sense now implies that the latter difference is negligible. □

Therefore if $\mathcal{PE}'$ is an insecure public-key scheme in the sense of KNM-ATK, then $\mathcal{PE}$ will be insecure in the sense of KNM-ATK as well. This completes the proof of the Lemma 3.26. □

Lemmas 3.25 and 3.26 together complete the proof of Theorem 3.24. □

Theorem 3.29. *NM*-ATK ⇒ KNM-ATK for ATK ∈ {CPA, CCA1, CCA2}.*

Proof. We prove the contrapositive; assume that $\mathcal{PE}$ is an insecure encryption in the sense of KNM-ATK. Therefore there is an adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE},\mathcal{B}}(\cdot)$ is non-negligible. To this end, we describe an NM*-ATK adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{NM*-ATK}}_{\mathcal{PE},\mathcal{A}}(\cdot)$ is non-negligible.

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$(M, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk)$	$(y^*, R_k) \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$S_{\mathcal{A}} := (pk, S_{\mathcal{B}})$	**return** (y^*, pk, R)
return $(M, S_{\mathcal{A}})$	

where the relation R is defined based on R_k as follows: $R(x^*, x, y^*, pk^*, pk) =$ **true** if and only if $R_k(pk^*, pk) =$ **true**.

Now note that $\mathcal{A}$ succeeds whenever $\mathcal{B}$ does, hence

$$\mathbf{Adv}^{\text{NM*-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE},\mathcal{B}}(k).$$

This completes the proof of Theorem 3.29. □

3.3 IND-NM inter-relation proofs

In this section we prove relation (i.e., implication or separation) between notions of indistinguishability and notions of non-malleability.

Theorem 3.30. *NM-ATK* $\Rightarrow$ *IND-ATK for ATK* $\in$ {*CPA, CCA1, CCA2*}.

Proof. For a complete proof refer to [2]. □

Theorem 3.31. *IND-CCA2* $\Rightarrow$ *NM-CCA2.*

Proof. Refer to [2] for a complete proof. □

Theorem 3.32. *KNM-ATK* $\not\Rightarrow$ *KI-ATK.*

Proof. Assume that there exists some KNM-ATK secure encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is meaninglessly true. We now modify $\mathcal{PE}$ to a new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ (identically as the scheme $\mathcal{PE}'$ used in the proof of Theorem 3.1 with $y' = y \| pk$) which is also KNM-ATK secure but not secure in the KI-ATK sense. This will prove the theorem.

Lemma 3.33. $\mathcal{PE}'$ *is not secure in the KI-ATK sense.*

Proof. It is intuitively clear that the scheme $\mathcal{PE}'$ is not secure in the sense of KI since given any ciphertext $y' = y \| pk$ of $\mathcal{PE}'$, the adversary can find out which key has been used to encrypt the corresponding plaintext.

Formally, consider the following KI-CPA adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$: on the input (pk_0, pk_1), the algorithm $\mathcal{A}_1$ chooses a random plaintext x, sets $S_{\mathcal{A}} := (pk_0, pk_1)$, and outputs $(x, S_{\mathcal{A}})$; the ciphertext will be in the form $y \| pk_b$ for some $b \in \{0, 1\}$; then on the input $(y \| pk_b, S_{\mathcal{A}})$, the algorithm $\mathcal{A}_2$ outputs b. For such an adversary we always have $\mathbf{Expt}^{\text{KI-CPA-}b}_{\mathcal{PE}',\mathcal{A}}(k) = b$ and hence $\mathbf{Adv}^{\text{KI-CPA}}_{\mathcal{PE}',\mathcal{A}}(k) = 1$. This shows that $\mathcal{PE}'$ is insecure in the sense of KI-CPA and hence insecure in the sense of KI-ATK generally. □

On the other hand, we prove that $\mathcal{PE}'$ retains the KNM-ATK security of $\mathcal{PE}$:

Lemma 3.34. $\mathcal{PE}'$ *is secure in the sense of KNM-ATK.*

Proof. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be a polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of KNM-ATK. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the KNM-ATK sense, as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y_{\mathcal{A}}, S_{\mathcal{B}})$
$(M, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}'_1}(pk)$	$y_{\mathcal{B}} := y_{\mathcal{A}} \| pk$
return $(M, S_{\mathcal{B}})$	$(y^*_{\mathcal{B}}, pk^*, R_k) \leftarrow \mathcal{B}_2^{\mathcal{O}'_2}(y_{\mathcal{B}}, S_{\mathcal{B}})$
	Parse $y^*_{\mathcal{B}}$ as $y^*_{\mathcal{A}} \| pk^{**}$
	return $(y^*_{\mathcal{A}}, pk^*, R_k)$

where $\mathcal{O}'_1$ and $\mathcal{O}'_2$ are defined based on the decryption oracle $\mathcal{D}'_{sk}(\cdot)$ which itself is defined based on the provided decryption oracle $\mathcal{D}_{sk}(\cdot)$ as follows: for any input $y\|pk$ it queries $\mathcal{D}_{sk}(\cdot)$ on the first component of the ciphertext and returns $\mathcal{D}'_{sk}(y\|pk) := \mathcal{D}_{sk}(y)$.

Note that for any $y^*_{\mathcal{B}}$, pk^*, and x_b, based on our definition of $\mathcal{E}'$, we have $y^*_{\mathcal{B}} = \mathcal{E}'_{pk^*}(x_b)$ if and only if $y^*_{\mathcal{A}} = \mathcal{E}_{pk^*}(x_b)$ and $pk^{**} = pk^*$. We can assume that $pk^{**} = pk^*$ always holds because otherwise the advantage of $\mathcal{B}$ would automatically be zero. Hence, for such an adversary $\mathbf{Expt}^{\text{KNM-ATK-}b}_{\mathcal{PE}',\mathcal{B}}(k) = \mathbf{Expt}^{\text{KNM-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k)$ for any $b \in \{0, 1\}$. This means that

$$\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE}',\mathcal{B}}(k).$$

Hence if $\mathcal{PE}'$ is insecure in the sense of KNM-ATK, then $\mathcal{PE}$ will be insecure in the sense of KNM-ATK, too. This completes the proof of the lemma. □

Lemmas 3.33 and 3.34 together complete the proof of Theorem 3.32. □

Theorem 3.35. *KI-ATK ⇏ KNM-ATK for ATK* ∈ {*CPA, CCA1, CCA2*}.

Proof. Assume there exists some KI-ATK secure encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is meaningless though true. We now modify $\mathcal{PE}$ to a new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ (analogous to the scheme $\mathcal{PE}'$ used in the proof of Theorem 3.11 with $pk' = pk\|b$) which is also KI-ATK secure but not secure in the KNM-ATK sense. This will prove the theorem.

Lemma 3.36. *$\mathcal{PE}'$ is not secure in the KNM-ATK sense.*

Proof. See the proof of Lemma 3.12. □

On the other hand, we prove that $\mathcal{PE}'$ retains the KI-ATK security of $\mathcal{PE}$:

Lemma 3.37. *$\mathcal{PE}'$ is secure in the sense of KI-ATK.*

Proof. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be some polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of KI-ATK. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the KI-ATK sense, as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk_0, pk_1)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$b_0, b_1 \leftarrow \{0,1\}$	$b^* \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$(x, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk_0 \| b_0, pk_1 \| b_1)$	**return** (b^*)
return $(x, S_{\mathcal{B}})$	

Now note that, based on our definition of $\mathcal{E}'$, we have $y = \mathcal{E}'_{pk_{b^*}\|b_{b^*}}(x)$ if and only if $y = \mathcal{E}_{pk_{b^*}}(x)$. This means that

$$\mathbf{Expt}^{\text{KI-ATK-}b}_{\mathcal{PE}',\mathcal{B}}(k) = b \text{ if and only if } \mathbf{Expt}^{\text{KI-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k) = b.$$

Hence we deduce

$$\mathbf{Adv}^{\text{KI-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \mathbf{Adv}^{\text{KI-ATK}}_{\mathcal{PE}',\mathcal{B}}(k).$$

This completes the proof of Lemma 3.37. □

Lemmas 3.36 and 3.37 together complete the proof of Theorem 3.35. □

Theorem 3.38. *IND*-ATK ⇏ NM*-ATK for ATK ∈ {CPA, CCA1, CCA2}.*

Proof. Assume there exists IND*-ATK secure encryption $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is true, but meaningless. To prove the theorem, we modify $\mathcal{PE}$ to a new encryption $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ (precisely similar to the scheme $\mathcal{PE}'$ used in the proof of Theorem 3.11 with $pk' = pk\|b$) which is still IND*-ATK secure but not secure in the sense of NM*-ATK.

Lemma 3.39. *$\mathcal{PE}'$ is not secure in the NM*-ATK sense.*

Proof. It is obvious that the scheme $\mathcal{PE}'$ is not secure in the sense of NM*-ATK since given any ciphertext $y = \mathcal{E}_{pk\|b}(x)$ of $\mathcal{PE}'$, the adversary can output the ciphertext $y = \mathcal{E}_{pk\|\overline{b}}(x)$ of the same plaintext under a new related public key $pk\|\overline{b}$.

Formally, consider the following NM*-CPA adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$: on input $pk\|b$ the algorithm $\mathcal{A}_1$ outputs $(M, pk\|b)$ where M is the plaintext space; on input $(y, pk\|b)$ the algorithm $\mathcal{A}_2$ outputs $(y, pk\|\overline{b}, R)$ where for any x^*, x_b, y^*, $pk^*\|b^*$, and $pk\|b$: $R(x^*, x_b, y^*, pk^*\|b^*, pk\|b)$ is defined to be true if and only if $x^* = x_b$ and $pk^* = pk$. Now note that for $\mathcal{A}_2$'s output we always have $pk\|\overline{b} \neq pk\|b$. Also if $y = \mathcal{E}'_{pk\|b}(x_1)$ then for $x^* = x_1$ both $y = \mathcal{E}'_{pk\|\overline{b}}(x_1)$ and R are true, but if $y = \mathcal{E}'_{pk\|b}(x_0)$ then both $y = \mathcal{E}'_{pk\|\overline{b}}(x^*)$ and R can only be true at the

same time if $x_0 = x_1$ because the former requires $x^* = x_1$ and the latter requires $x^* = x_0$. The event $x_0 = x_1$ only happens with probability $1/|M|$. Hence we have $\mathbf{Adv}^{\text{NM*-ATK}}_{\mathcal{PE}',\mathcal{A}}(k) = 1 - 1/|M|$ which is a considerable advantage. Therefore $\mathcal{PE}'$ is not NM*-CPA secure and hence not NM*-ATK secure in general. □

Now, we prove that $\mathcal{PE}'$ retains the IND*-ATK security of $\mathcal{PE}$.

Lemma 3.40. *$\mathcal{PE}'$ is secure in the sense of IND*-ATK.*

Proof. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be a polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of IND*-ATK. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the IND*-ATK sense. The adversary $\mathcal{A}$ is defined as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk_0, pk_1)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$b_0, b_1 \leftarrow \{0,1\}$	$(b^*, c^*) \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$(x_0, x_1, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk_0 \| b, pk_1 \| b)$	**return** (b^*, c^*)
return $(x_0, x_1, S_{\mathcal{B}})$	

Now note that, based on our definition of $\mathcal{E}'$, for any b^* and c^*, we have $y = \mathcal{E}'_{pk_{b^*}\|b_{b^*}}(x_{c^*})$ if and only if $y = \mathcal{E}_{pk_{b^*}}(x_{c^*})$. This means that

$$\mathbf{Expt}^{\text{IND*-ATK-}(b,c)}_{\mathcal{PE}',\mathcal{B}}(k) \simeq (b,c) \text{ if and only if } \mathbf{Expt}^{\text{IND*-ATK-}(b,c)}_{\mathcal{PE},\mathcal{A}}(k) \simeq (b,c).$$

Hence we have

$$\begin{aligned}
\mathbf{Adv}^{\text{IND*-ATK}}_{\mathcal{PE},\mathcal{A}}(k) &= \left|4 \cdot \Pr\left[\mathbf{Expt}^{\text{IND*-ATK-}(b,c)}_{\mathcal{PE},\mathcal{A}}(k) \simeq (b,c)\right] - 3\right| \\
&= \left|4 \cdot \Pr\left[\mathbf{Expt}^{\text{IND*-ATK-}(b,c)}_{\mathcal{PE}',\mathcal{B}}(k) \simeq (b,c)\right] - 3\right| \\
&= \mathbf{Adv}^{\text{IND*-ATK}}_{\mathcal{PE}',\mathcal{B}}(k).
\end{aligned}$$

This completes the proof of Lemma 3.40. □

Lemmas 3.39 and 3.40 together complete the proof of Theorem 3.38. □

Theorem 3.41. *NM*-ATK $\not\Rightarrow$ IND*-ATK for ATK $\in$ {CPA, CCA1, CCA2}.*

Proof. Assume we have NM*-ATK $\Rightarrow$ IND*-ATK. According to Theorem 3.8 we have IND*-ATK $\Rightarrow$ KI-ATK. Then we should have NM*-ATK $\Rightarrow$ KI-ATK. But this is in contradiction with Theorem 3.53. Therefore NM*-ATK $\not\Rightarrow$ IND*-ATK. □

Theorem 3.42. *NM*-ATK ⇒ IND-ATK for ATK ∈ {CPA, CCA1, CCA2}.*

Proof. We prove the equivalent relation IND-ATK insecurity implies NM*-ATK insecurity. Assume that $\mathcal{PE}$ is an insecure encryption scheme in the sense of IND-ATK. Hence there exists an adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE},\mathcal{B}}(\cdot)$ is non-negligible. We construct an NM*-ATK adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ attacking $\mathcal{PE}$ as follows, such that $\mathbf{Adv}^{\text{NM*-ATK}}_{\mathcal{PE},\mathcal{A}}(\cdot)$ is also non-negligible.

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$(x_0, x_1, s) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk)$	$b^* \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$M := \{x_0, x_1\}$	$y^* \leftarrow \mathcal{E}_{\overline{pk}}(\overline{x_{b^*}})$
$S_{\mathcal{A}} := (M, pk, S_{\mathcal{B}})$	**return** $(y^*, \overline{pk}, R)$
return $(M, S_{\mathcal{A}})$	

where, for any x^*, x_b, y^*, pk^*, and pk: $R(x^*, x_b, y^*, pk^*, pk)$ is defined to be true if and only if $x^* = \overline{x_b}$ and $pk^* = \overline{pk}$.

Now note that for $\mathcal{A}_2$'s output the following hold: for $\overline{x_{b^*}}$ we have

$$y^* = \mathcal{E}_{\overline{pk}}(\overline{x_{b^*}}), \quad \overline{pk} \neq pk, \quad \text{and} \quad \overline{\overline{pk}} = pk.$$

Therefore $\mathbf{Expt}^{\text{NM*-ATK-1}}_{\mathcal{PE},\mathcal{A}}(k) = 1$ if and only if $\overline{x_{b^*}} = \overline{x_b}$ or equivalently $x_{b^*} = x_b$. Hence we have

$$\Pr\left[\mathbf{Expt}^{\text{NM*-ATK-1}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right] = \Pr\left[\mathbf{Expt}^{\text{IND-ATK-}b}_{\mathcal{PE},\mathcal{B}}(k) = b\right].$$

Similarly $\mathbf{Expt}^{\text{NM*-ATK-0}}_{\mathcal{PE},\mathcal{A}}(k) = 1$ if and only if $x_{b^*} = x_{\overline{b}}$. This event happens exactly half of the time since $x_{\overline{b}}$ is chosen randomly from $\{x_0, x_1\}$. Hence we have

$$\Pr\left[\mathbf{Expt}^{\text{NM*-ATK-0}}_{\mathcal{PE},\mathcal{A}}(k) = 1\right] = \frac{1}{2}.$$

Combining the above two results we get the following:

$$\mathbf{Adv}^{\text{NM*-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE},\mathcal{B}}(k).$$

Therefore if $\mathcal{PE}'$ is insecure in the sense of IND-ATK, then $\mathcal{PE}$ will be insecure in the sense of NM*-ATK. This completes the proof of Theorem 3.42. Note that this can be deduced from the two already-proved Theorems 3.23 and 3.30 as well. □

Theorem 3.43. *IND-ATK ⇏ NM*-ATK for ATK ∈ {CPA, CCA1, CCA2}.*

Proof. According to Theorem 3.30 we have NM-ATK $\Rightarrow$ IND-ATK. Now if we assume that IND-ATK $\Rightarrow$ NM*-ATK then we should have NM-ATK $\Rightarrow$ NM*-ATK; but this is in contradiction with Theorem 3.20. Therefore IND*-ATK $\not\Rightarrow$ NM*-ATK. □

Theorem 3.44. *NM-ATK $\not\Rightarrow$ IND*-ATK for ATK $\in$ {CPA, CCA1, CCA2}.*

Proof. Assume we have NM-ATK $\Rightarrow$ IND*-ATK. According to Theorem 3.8 we have IND*-ATK $\Rightarrow$ KI-ATK. Then we should have NM-ATK $\Rightarrow$ KI-ATK. But this is in contradiction with Theorem 3.57. Therefore NM-ATK $\not\Rightarrow$ IND*-ATK. □

Theorem 3.45. *IND*-CCA2 $\Rightarrow$ NM-CCA2.*

Proof. According to Theorem 3.7 we have IND*-ATK $\Rightarrow$ IND-ATK. Also according to Theorem 3.31 we have IND-CCA2 $\Rightarrow$ NM-CCA2. Hence IND*-CCA2 $\Rightarrow$ NM-CCA2. □

Theorem 3.46. *IND*-ATK $\not\Rightarrow$ NM-ATK for ATK $\in$ {CPA, CCA1}.*

Proof. Assume there exists NM-ATK secure encryption $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is true in a meaningless manner. To prove the theorem, we modify $\mathcal{PE}$ to a new encryption $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ which is also NM-ATK secure but not secure in the sense of IND*-ATK.

The new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ is defined as follows:

Algorithm $\mathcal{K}'(k)$	**Algorithm** $\mathcal{E}'_{pk}(x)$	**Algorithm** $\mathcal{D}'_{sk}(y\|b)$
$(pk, sk) \leftarrow \mathcal{K}(k)$	$b \leftarrow \{0,1\}$	**return** $(\mathcal{D}_{sk}(y))$
return (pk, sk)	**return** $(\mathcal{E}_{pk}(x)\|b)$	

In other words, a ciphertext in the new scheme is a pair $y\|b$ consisting of $\mathcal{E}_{pk}(x)$ and a random bit b. During encryption, the second component is ignored.

Lemma 3.47. *$\mathcal{PE}'$ is not secure in the NM-ATK sense.*

Proof. It is obvious that the scheme $\mathcal{PE}'$ is not secure in the sense of NM since given any ciphertext $y' = \mathcal{E}_{pk}(x)\|b$ of $\mathcal{PE}'$, the adversary can generate a new ciphertext $y^* = \mathcal{E}_{pk}(x)\|\overline{b}$ of the same plaintext under the same public key. □

Now, we prove that $\mathcal{PE}'$ retains the IND*-ATK security of $\mathcal{PE}$.

Lemma 3.48. *$\mathcal{PE}'$ is secure in the sense of IND*-ATK.*

Proof. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be a polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of IND*-ATK. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the IND*-ATK sense. The adversary $\mathcal{A}$ is defined as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk_0, pk_1)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$(x_0, x_1, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk_0, pk_1)$	$d \leftarrow \{0,1\}$
return $(x_0, x_1, S_{\mathcal{B}})$	$(b^*, c^*) \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y \| d, S_{\mathcal{B}})$
	return (b^*, c^*)

Now note that, based on our definition of $\mathcal{E}'$, for any d, b^* and c^*, we have $y\|d = \mathcal{E}'_{pk_{b^*}}(x_{c^*})$ if and only if $y = \mathcal{E}_{pk_{b^*}}(x_{c^*})$. This means that

$$\mathbf{Expt}^{\text{IND*-ATK-}(b,c)}_{\mathcal{PE}',\mathcal{B}}(k) \simeq (b,c) \text{ if and only if } \mathbf{Expt}^{\text{IND*-ATK-}(b,c)}_{\mathcal{PE},\mathcal{A}}(k) \simeq (b,c).$$

Hence, similar to the proof of Lemma 3.40, we have

$$\mathbf{Adv}^{\text{IND*-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \mathbf{Adv}^{\text{IND*-ATK}}_{\mathcal{PE}',\mathcal{B}}(k).$$

This completes the proof of Lemma 3.48. □

Lemmas 3.47 and 3.48 together complete the proof of Theorem 3.46. □

Theorem 3.49. *KNM-ATK $\not\Rightarrow$ IND*-ATK for ATK $\in$ {CPA, CCA1, CCA2}.*

Proof. Assume we have KNM-ATK $\Rightarrow$ IND*-ATK. According to Theorem 3.8 we have IND*-ATK $\Rightarrow$ KI-ATK. Then we should have KNM-ATK $\Rightarrow$ KI-ATK. But this is in contradiction with Theorem 3.32. Therefore KNM-ATK $\not\Rightarrow$ IND*-ATK. □

Theorem 3.50. *IND*-ATK $\not\Rightarrow$ KNM-ATK for ATK $\in$ {CPA, CCA1, CCA2}.*

Proof. Assume there exists IND*-ATK secure encryption $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is true, but meaningless. To prove the theorem, we modify $\mathcal{PE}$ to a new encryption $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ (just as the scheme $\mathcal{PE}'$ used in the proof of Theorem 3.11 with $pk' = pk\|b$) which is also IND*-ATK secure but not secure in the sense of KNM-ATK.

Lemma 3.51. *$\mathcal{PE}'$ is not secure in the KNM-ATK sense.*

Proof. See the proof of Lemma 3.12. □

Now, we prove that $\mathcal{PE}'$ retains the IND*-ATK security of $\mathcal{PE}$.

Lemma 3.52. *$\mathcal{PE}'$ is secure in the sense of IND*-ATK.*

Proof. We prove that if $\mathcal{PE}'$ is insecure in the sense of IND*-ATK, then $\mathcal{PE}$ is insecure in the sense of IND*-ATK. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be a polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of IND*-ATK. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the IND*-ATK sense. The adversary $\mathcal{A}$ is defined as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk_0, pk_1)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$b_0, b_1 \leftarrow \{0,1\}$	$(b^*, c^*) \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$(x_0, x_1, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk_0 \| b_0, pk_1 \| b_1)$	**return** (b^*, c^*)
return $(x_0, x_1, S_{\mathcal{B}})$	

Now note that, based on our definition of $\mathcal{E}'$, for any b^* and c^*, we have $y = \mathcal{E}'_{pk_{b^*} \| b_{b^*}}(x_{c^*})$ if and only if $y = \mathcal{E}_{pk_{b^*}}(x_{c^*})$. This means that

$$\mathbf{Expt}^{\text{IND*-ATK-}(b,c)}_{\mathcal{PE}',\mathcal{B}}(k) \simeq (b,c) \text{ if and only if } \mathbf{Expt}^{\text{IND*-ATK-}(b,c)}_{\mathcal{PE},\mathcal{A}}(k) \simeq (b,c).$$

Hence, by a simple calculation similar to the proof of Lemma 3.40 we obtain

$$\mathbf{Adv}^{\text{IND*-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \mathbf{Adv}^{\text{IND*-ATK}}_{\mathcal{PE}',\mathcal{B}}(k).$$

This completes the proof of Lemma 3.40. □

Lemmas 3.51 and 3.52 together complete the proof of Theorem 3.50. □

Theorem 3.53. *NM*-ATK $\not\Rightarrow$ KI-ATK for ATK $\in$ {CPA, CCA1, CCA2}.*

Proof. Assume that there exists some NM*-ATK secure encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is meaningless though true. We now modify $\mathcal{PE}$ to a new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ (just like the scheme $\mathcal{PE}'$ used in the proof of Theorem 3.1 with $y' = y \| pk$) which is also NM*-ATK secure but not secure in the KI-ATK sense. This will prove the theorem.

Lemma 3.54. *$\mathcal{PE}'$ is not secure in the KI-ATK sense.*

Proof. See the proof of Lemma 3.2. □

On the other hand, we prove that $\mathcal{PE}'$ retains the NM*-ATK security of $\mathcal{PE}$:

Lemma 3.55. *$\mathcal{PE}'$ is secure in the sense of NM*-ATK.*

Proof. We prove that if $\mathcal{PE}$ is secure in the sense of NM*-ATK, then $\mathcal{PE}'$ is also secure in the sense of NM*-ATK. We do so by proving that if $\mathcal{PE}'$ is insecure in the sense of NM*-ATK, then $\mathcal{PE}$ is also insecure in the sense of NM*-ATK. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be some polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of NM*-ATK. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the NM*-ATK sense, as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y_{\mathcal{A}}, S_{\mathcal{A}})$
$(M, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}'_1}(pk)$	$y_{\mathcal{B}} := y_{\mathcal{A}} \| pk$
$S_{\mathcal{A}} := (M, pk, S_{\mathcal{B}})$	$(y^*_{\mathcal{B}}, pk^*, R) \leftarrow \mathcal{B}_2^{\mathcal{O}'_2}(y_{\mathcal{B}}, S_{\mathcal{B}})$
return $(M, S_{\mathcal{A}})$	Parse $y^*_{\mathcal{B}}$ as $y^*_{\mathcal{A}} \| pk^{**}$
	if $pk^{**} = pk$ **then**
	$R' := R$
	else define $R'(\ldots) = 0$
	return $(y^*_{\mathcal{A}}, pk^*, R')$

where $\mathcal{O}'_1$ and $\mathcal{O}'_2$ are defined based on the decryption oracle $\mathcal{D}'_{sk}(\cdot)$ which itself is defined based on the provided decryption oracle $\mathcal{D}_{sk}(\cdot)$ as follows: for any input $y\|pk$ it queries $\mathcal{D}_{sk}(\cdot)$ on the first component of the ciphertext and returns $\mathcal{D}'_{sk}(y\|pk) := \mathcal{D}_{sk}(y)$. Also, $R'(x^*, x_b, y^*\|pk^*, pk^*, pk)$ is defined to be true if and only if the relation $R'(x^*, x_b, y^*, pk^*, pk)$ is true.

We assume that $pk^{**} = pk^*$ because otherwise the advantage of $\mathcal{B}$ would automatically be zero. Now note that, based on our definitions, $y^*_{\mathcal{B}} = \mathcal{E}'_{pk}(x^*)$ if and only if $y^*_{\mathcal{A}} = \mathcal{E}_{pk}(x^*)$, $y^*_{\mathcal{B}} \neq y_{\mathcal{B}} \wedge pk^* \neq pk$ is true if and only if $y^*_{\mathcal{A}} \neq y_{\mathcal{A}} \wedge pk^* \neq pk$ is true, and $R'(x^*, x_b, y^*\|pk^*, pk^*, pk)$ is true if and only if $R'(x^*, x_b, y^*, pk^*, pk)$ is true. Therefore, $\mathbf{Expt}^{\text{NM*-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k)$ outputs 1 if and only if $\mathbf{Expt}^{\text{NM*-ATK-}b}_{\mathcal{PE}',\mathcal{B}}(k)$ outputs 1. Hence we have

$$\mathbf{Adv}^{\text{NM*-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \mathbf{Adv}^{\text{NM*-ATK}}_{\mathcal{PE}',\mathcal{B}}(k).$$

This completes the proof of Lemma 3.55. □

Lemmas 3.54 and 3.55 together complete the proof of Theorem 3.53. □

Theorem 3.56. *KI-ATK ⇏ NM*-ATK for ATK ∈ {CPA, CCA1, CCA2}.*

Proof. Assume that KI-ATK ⇒ NM*-ATK. According to Theorem 3.29 we can write NM*-ATK ⇒ KNM-ATK. Therefore we should have KI-ATK ⇒ KNM-ATK; but this is in contradiction with Theorem 3.35. Hence KI-ATK ⇏ NM*-ATK. □

Theorem 3.57. *NM-ATK $\not\Rightarrow$ KI-ATK for ATK $\in$ {CPA, CCA1, CCA2}.*

Proof. Assume there exists some NM-ATK secure encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is vacuously true. We now modify $\mathcal{PE}$ to a new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ which is also NM-ATK secure but not secure in the KI-ATK sense. This will prove the theorem.

The new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ is defined as follows:

Algorithm $\mathcal{K}'(k)$	**Algorithm** $\mathcal{E}'_{pk}(x)$	**Algorithm** $\mathcal{D}'_{sk\|pk}(y\|pk')$
$(pk, sk) \leftarrow \mathcal{K}(k)$	$y \leftarrow \mathcal{E}_{pk}(x)$	if $pk = pk'$ **then**
return $(pk, sk\|pk)$	**return** $(y\|pk)$	**return** $(\mathcal{D}_{sk}(y))$
		if $pk \neq pk'$ **then**
		return $\perp$

In other words, a ciphertext in the new scheme is a pair $y\|pk$ consisting of the encryption of the message under $\mathcal{E}$ and the public key used for the encryption process. In decryption, the second component is ignored.

Lemma 3.58. *$\mathcal{PE}'$ is not secure in the KI-ATK sense.*

Proof. The proof is similar to that of Lemma 3.54. □

On the other hand, we prove that $\mathcal{PE}'$ retains the NM-ATK security of $\mathcal{PE}$:

Lemma 3.59. *$\mathcal{PE}'$ is secure in the sense of NM-ATK.*

Proof. We prove that if $\mathcal{PE}$ is secure in the sense of NM-ATK, then $\mathcal{PE}'$ is secure in the sense of NM-ATK too. We do so by proving that if $\mathcal{PE}'$ is insecure in the sense of NM-ATK, then $\mathcal{PE}$ is insecure in the sense of NM-ATK too. Let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be some polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of NM-ATK. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the NM-ATK sense, as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y_{\mathcal{A}}, S_{\mathcal{A}})$
$(M, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}'_1}(pk)$	$y_{\mathcal{B}} := y_{\mathcal{A}} \| pk$
$S_{\mathcal{A}} := (pk, S_{\mathcal{B}})$	$(y^*_{\mathcal{B}}, R_x) \leftarrow \mathcal{B}_2^{\mathcal{O}'_2}(y_{\mathcal{B}}, S_{\mathcal{B}})$
return $(M, S_{\mathcal{A}})$	parse $y^*_{\mathcal{B}}$ as $y^*_{\mathcal{A}} \| pk^*$
	if $pk^* = pk$ **then**
	$R' := R$
	else define $R'(\ldots) = 0$
	return (y^*_A, R_x)

where $\mathcal{O}'_1$ and $\mathcal{O}'_2$ are defined based on the decryption oracle $\mathcal{D}'_{sk\|pk}(\cdot)$ which itself is defined based on the provided decryption oracle $\mathcal{D}_{sk}(\cdot)$ and the public key pk as follows: for any input $y\|pk'$, if $pk' \neq pk$ then $\mathcal{D}'_{sk\|pk}(\cdot)$ outputs $\perp$, but if $pk' = pk$ it queries $\mathcal{D}_{sk}(\cdot)$ on the first component of the ciphertext and returns $\mathcal{D}'_{sk\|pk}(y\|pk) := \mathcal{D}_{sk}(y)$.

We assume that $pk^* = pk$ because otherwise $\mathcal{D}'_{sk\|pk}(y^*_{\mathcal{B}}) = \perp$ and hence the advantage of $\mathcal{B}$ would automatically be zero. Now note that, based on our definitions and the fact that $pk^* = pk$, $\mathcal{D}'_{sk\|pk}(y^*_{\mathcal{B}}) \neq \perp$ if and only if $\mathcal{D}_{sk}(y^*_{\mathcal{A}}) \neq \perp$ and $y^*_{\mathcal{B}} \neq y_{\mathcal{B}}$ if and only if $y^*_{\mathcal{A}} \neq y_{\mathcal{A}}$. Therefore, $\mathbf{Expt}^{\text{NM-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k)$ outputs 1 if and only if $\mathbf{Expt}^{\text{NM-ATK-}b}_{\mathcal{PE}',\mathcal{B}}(k)$ outputs 1. Hence, we have

$$\mathbf{Adv}^{\text{NM-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \mathbf{Adv}^{\text{NM-ATK}}_{\mathcal{PE}',\mathcal{B}}(k).$$

This completes the proof of Lemma 3.59. □

Lemmas 3.58 and 3.59 together complete the proof of Theorem 3.57. □

Theorem 3.60. *KI-ATK $\not\Rightarrow$ NM-ATK for ATK $\in$ {CPA, CCA1, CCA2}.*

Proof. Assume that KI-ATK $\Rightarrow$ NM-ATK. According to Theorem 3.30 we know that NM-ATK $\Rightarrow$ IND-ATK. Therefore we should have KI-ATK $\Rightarrow$ IND-ATK; but this is in contradiction with Theorem 3.4. Hence KI-ATK $\not\Rightarrow$ NM-ATK. □

Theorem 3.61. *KNM-ATK $\Rightarrow$ IND-ATK for ATK $\in$ {CPA, CCA1, CCA2}.*

Proof. We prove the equivalent statement that if a scheme is IND-ATK insecure then it is KNM-ATK insecure. Assume that $\mathcal{PE}$ is an insecure encryption scheme in the sense of IND-ATK. There is an adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE},\mathcal{B}}(\cdot)$ is non-negligible. We construct a KNM-ATK adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ attacking $\mathcal{PE}$ such that $\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE},\mathcal{A}}(\cdot)$ is non-negligible too.

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{A}})$
$(x_0, x_1, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk)$	$b^* \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$M := \{x_0, x_1\}$	$y^* \leftarrow \mathcal{E}_{\overline{pk}}(x_{b^*})$
$S_{\mathcal{A}} := (M, pk, S_{\mathcal{B}})$	**return** $(y^*, \overline{pk}, R_k)$
return $(M, S_{\mathcal{A}})$	

where, for any pk^* and pk: $R_k(pk^*, pk)$ is defined to be true if and only if $pk^* = \overline{pk}$.

Now note that for $\mathcal{A}_2$'s output the following hold: for x_{b^*} we have

$$y^* = \mathcal{E}_{\overline{pk}}(x_{b^*}), \quad \overline{pk} \neq pk, \quad \text{and} \quad \overline{\overline{pk}} = pk.$$

Therefore $\mathbf{Expt}^{\text{KNM-ATK-1}}_{\mathcal{PE},\mathcal{A}}(k) = 1$ if and only if $x_{b^*} = x_b$. Hence we have

$$\Pr\big[\mathbf{Expt}^{\text{KNM-ATK-1}}_{\mathcal{PE},\mathcal{A}}(k) = 1\big] = \Pr\big[\mathbf{Expt}^{\text{IND-ATK-}b}_{\mathcal{PE},\mathcal{B}}(k) = b\big].$$

Similarly $\mathbf{Expt}^{\text{KNM-ATK-0}}_{\mathcal{PE},\mathcal{A}}(k) = 1$ if and only if $x_{b^*} = x_{\overline{b}}$. This event happens exactly half of the time since $x_{\overline{b}}$ is chosen randomly from $\{x_0, x_1\}$. Hence we have

$$\Pr\big[\mathbf{Expt}^{\text{KNM-ATK-0}}_{\mathcal{PE},\mathcal{A}}(k) = 1\big] = \frac{1}{2}.$$

Combining the above two results we get the following:

$$\mathbf{Adv}^{\text{KNM-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \frac{1}{2} \cdot \mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE},\mathcal{B}}(k).$$

This completes the proof of Theorem 3.61. □

Theorem 3.62. *IND-ATK $\not\Rightarrow$ KNM-ATK for ATK $\in$ {CPA, CCA1, CCA2}.*

Proof. Assume there exists some IND-ATK secure encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is vacuously true. We now modify $\mathcal{PE}$ to a new encryption scheme $\mathcal{PE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ (just like the scheme $\mathcal{PE}'$ used in the proof of Theorem 3.11 with $pk' = pk \| b$) which is also IND-ATK secure but not secure in the KNM-ATK sense. This will prove the theorem.

Lemma 3.63. *$\mathcal{PE}'$ is not secure in the KNM-ATK sense.*

Proof. See the proof of Lemma 3.51. □

On the other hand, we prove that $\mathcal{PE}'$ retains the IND-ATK security of $\mathcal{PE}$:

Lemma 3.64. *$\mathcal{PE}'$ is secure in the sense of IND-ATK.*

Proof. We prove by contrapositive; let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be some polynomial-time adversary attacking $\mathcal{PE}'$ in the sense of IND-ATK. We construct an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that attacks the scheme $\mathcal{PE}$ in the IND-ATK sense, as follows:

Algorithm $\mathcal{A}_1^{\mathcal{O}_1}(pk)$	**Algorithm** $\mathcal{A}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$b \leftarrow \{0,1\}$	$b^* \leftarrow \mathcal{B}_2^{\mathcal{O}_2}(y, S_{\mathcal{B}})$
$(x_0, x_1, S_{\mathcal{B}}) \leftarrow \mathcal{B}_1^{\mathcal{O}_1}(pk \| b)$	**return** (b^*)
return $(x_0, x_1, S_{\mathcal{B}})$	

Now note that based on our definition of $\mathcal{PE}'$, $y = \mathcal{E}'_{pk\|b}(x_{b^*})$ if and only if $y = \mathcal{E}_{pk}(x_{b^*})$. Hence

$$\mathbf{Expt}^{\text{IND-ATK-}b}_{\mathcal{PE}',\mathcal{B}}(k) = b \text{ if and only if } \mathbf{Expt}^{\text{IND-ATK-}b}_{\mathcal{PE},\mathcal{A}}(k) = b.$$

Hence we have

$$\mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE},\mathcal{A}}(k) = \mathbf{Adv}^{\text{IND-ATK}}_{\mathcal{PE}',\mathcal{B}}(k).$$

This completes the proof of Lemma 3.64. □

Lemmas 3.63 and 3.64 together complete the proof of Theorem 3.62. □

4 Conclusion and open problems

In this paper we proposed two new notions of security, namely *complete indistinguishability* and *key non-malleability*, and proved relative strength of every two notions of indistinguishability and non-malleability. Many papers studied constructing concrete cryptosystem for the notions IND, NM, KI and NM*. Regarding KNM, Theorem 3.29 shows that we can use a completely non-malleable scheme instead (see, for example, [9, 12, 16, 18]) though it may not be as efficient as a newly designed KNM-secure encryption. Hence, we put constructing practical cryptosystems for IND* and KNM as open problems.

Acknowledgments. We thank the anonymous reviewers, and also Ron Steinfeld and Hassan Jameel Asghar for their helpful and constructive comments. Reza Sepahi was supported by a Macquarie University MQRES scholarship and Josef Pieprzyk was supported by the Australian Research Council grant DP0987734. Siamak F. Shahandashti would like to thank the Macquarie University Department of Computing and Josef Pieprzyk for hosting him during part of this work.

Berry Schoenmakers is grateful to the Centre for Advanced Computing – Algorithms and Cryptography (ACAC) at Macquarie University, and in particular to Prof. Pieprzyk's group, for their financial support and hospitality during his sabbatical stay in 2009.

Bibliography

[1] M. Bellare, A. Boldyreva, A. Desai and D. Pointcheval, Key-privacy in public-key encryption, in: *Advances in Cryptology* (Asiacrypt 2001), Lecture Notes in Comput. Sci. 2248, Springer (2001), 566–582.

[2] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, Relations among notions of security for public-key encryption schemes, in: *Advances in Cryptology* (Crypto '98), Springer (1998), 26–46.

[3] M. Bellare and A. Sahai, Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization, in: *Advances in Cryptology* (Crypto '99), Springer (1999), 78.

[4] C. Cocks, *A note on non-secret encryption*, CESG Report, November 1973.

[5] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Inform. Theory* **22** (1976), 644–654.

[6] D. Dolev, C. Dwork and M. Naor, Non-malleable cryptography, in: *Proc. of the 23rd STOC*, ACM Press, New York (1991), 542–552.

[7] D. Dolev, C. Dwork and M. Naor, Non-malleable cryptography, *SIAM J. Comput.* **30** (2000), 391–437.

[8] J. Ellis, *The possibility of secure non-secret digital encryption*, CESG Report, January 1970.

[9] M. Fischlin, Completely non-malleable schemes, in: *Proc. of ICALP*, Springer (2005), 779–790.

[10] C. Gentry, Practical identity-based encryption without random oracles, in: *Advances in Cryptology* (Eurocrypt 2006), Lecture Notes in Comput. Sci. 4004, Springer (2006), 445–464.

[11] S. Goldwasser and S. Micali, Probabilistic encryption, *J. Comput. System Sci.* **28** (1984), 270–299.

[12] B. Libert and M. Yung, Efficient completely non-malleable public key encryption, in: *Proceedings of the 37th International Colloquium Conference on Automata, Languages and Programming* (ICALP'10), Springer (2010), 127–139.

[13] M. Naor and M. Yung, Public-key cryptosystems provably secure against chosen ciphertext attacks, in: *Proc. of the 22nd STOC*, ACM Press, New York (1990), 427–437.

[14] C. Rackoff and D. Simon, Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack, in: *Advances in Cryptology* (Crypto '91), Lecture Notes in Comput. Sci. 576, Springer (1992), 433–444.

[15] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, in: *Proceedings of the 37th annual ACM symposium on Theory of computing* (STOC '05), ACM, New York (2005), 84–93.

[16] R. Sepahi, R. Steinfeld and J. Pieprzyk, Lattice-based completely non-malleable public-key encryption in the standard model, *Des. Codes Cryptogr.* (2012), DOI 10.1007/s10623-012-9732-0.

[17] P. van Liesdonk, *Anonymous and fuzzy identity-based encryption*, Master's thesis, Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, 2007.

[18] C. Ventre and I. Visconti, Completely non-malleable encryption revisited, in: *Public Key Cryptography* (PKC 2008), Springer (2008), 65–84.

[19] R. Zhang, G. Hanaoka and H. Imai, Orthogonality between key privacy and data privacy, revisited, in: *Information Security and Cryptology*, Springer (2008), 313–327.

Received August 19, 2010; revised August 13, 2012; accepted October 19, 2012.

Author information

Reza Sepahi, Computing Department, Macquarie University, Sydney, Australia.
E-mail: reza.sepahi@mq.edu.au

Josef Pieprzyk, Computing Department, Macquarie University, Sydney, Australia.
E-mail: josef.pieprzyk@mq.edu.au

Siamak F. Shahandashti, Département d'Informatique, École Normale Supérieure, Paris, France.
E-mail: fshahand@di.ens.fr

Berry Schoenmakers, Coding and Crypto Group, Technische Universiteit Eindhoven, Eindhoven, Netherlands.
E-mail: berry@win.tue.nl