Relations among Notions of Complete Non-malleability: Indistinguishability Characterisation and Efficient Construction without Random Oracles

Manuel Barbosa[1] and Pooya Farshim[2]

[1] CCTC/Departamento de Informática, Universidade do Minho,
Campus de Gualtar, 4710-057 Braga, Portugal
mbb@di.uminho.pt
[2] Information Security Group, Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, United Kingdom
Pooya.Farshim@rhul.ac.uk

Abstract. We study relations among various notions of complete non-malleability, where an adversary can tamper with both ciphertexts and public-keys, and ciphertext indistinguishability. We follow the pattern of relations previously established for standard non-malleability. To this end, we propose a more convenient and conceptually simpler indistinguishability-based security model to analyse completely non-malleable schemes. Our model is based on strong decryption oracles, which provide decryptions under arbitrarily chosen public keys. We give the first precise definition of a strong decryption oracle, pointing out the subtleties in different approaches that can be taken. We construct the first *efficient* scheme, which is fully secure against strong chosen-ciphertext attacks, and therefore completely non-malleable, without random oracles.

Keywords: Complete Non-Malleability. Strong Chosen-Ciphertext Attacks. Public-Key Encryption. Provable Security.

1 Introduction

Background. The security of public-key encryption schemes has been formalised according to various goals and attack models. Extensive work has been done in establishing relations between these security notions, and converging towards a core set of standard security definitions. Well-studied goals include semantic security, indistinguishability, and non-malleability; whereas chosen-plaintext and (adaptive) chosen-ciphertext are the most common attack scenarios considered in literature.

An important criterion for selecting security models is the guarantee of *necessary security* for a class of applications with practical relevance. Conversely, it is also expected that one can select a security model that is only as strict as required by a specific application. Otherwise, one might rule out valid solutions without justification, possibly sacrificing other important factors such as

R. Steinfeld and P. Hawkes (Eds.): ACISP 2010, LNCS 6168, pp. 145–163, 2010.

set-up assumptions, computational cost or communications bandwidth. Another important criterion is the conceptual simplicity and ease of use of a model.

Indistinguishability of ciphertexts is the most widely used notion of security for public-key encryption schemes. This notion was proposed by Goldwasser and Micali [15] as a convenient formalisation of the more intuitive notion of semantic security. Other notions of security have been proposed in different contexts. Of particular interest to this work is non-malleability, initially proposed by Dolev, Dwork, and Naor [12]. Roughly speaking, an encryption scheme is non-malleable if giving an encryption of a message to an adversary does not increase its chances of producing an encryption of a related message (under a given public key). This is formalised by requiring the existence of a simulator that performs as well as the adversary but without seeing the original encryption.

The relations between different notions of security for public-key encryption schemes were examined in a systematic way by Bellare et al. [4]. There, the authors compare indistinguishability of ciphertexts and non-malleability under chosen-plaintext and chosen-ciphertext attacks. In doing so, they formalise a comparison-based definition of non-malleability and establish important results based on this: non-malleability implies indistinguishability for an equivalent attack model, there is an equivalence between these notions for CCA2 model, and there are separations between the two notions for intermediate attack models.

Bellare and Sahai [8] established a cycle of equivalence between three definitions of non-malleability: a simulation-based definition similar to that of Dolev, Dwork and Naor, a comparison-based definition as introduced in [4], and a new definition called indistinguishability of ciphertexts under parallel chosen-ciphertext attacks. These equivalence relations essentially establish that the three definitions are alternative formulations of the same notion. Pass, Shelat, and Vaikuntanathan [18] revisit this equivalence result, and clarify several technical aspects in the known equivalence proofs. They consider the important question of composability of definitions, and establish a separation between the simulation-based and comparison-based non-malleability definitions, showing that the former is strictly stronger for *general* schemes.

Besides being theoretically interesting, the above results are also relevant in practice. They permit designers of encryption schemes to base their analysis on the simpler and better understood IND-CCA2 security model. This facilitates the presentation of conceptually simpler proofs, which are less prone to errors, as well as the direct application of a well-known set of proof techniques.

Complete non-malleability. Fischlin [13] introduces a stronger notion of non-malleability, known as *complete*, which requires attackers to have negligible advantage, even if they are allowed to transform the public key under which the related message is encrypted. Put differently, the goal of an adversary is to construct a related ciphertext under a new public key pair, for which the attacker might not even know a valid secret key.

Fischlin shows that well-known encryption schemes such as Cramer-Shoup [10] and RSA-OAEP [14] do *not* achieve even the weakest form of complete non-malleability. Furthermore, he proves a negative results with respect to the

existence of completely non-malleable schemes for general relations: there is a large class of relations for which completely non-malleable schemes do not exist with respect to black-box simulators. On the other hand, Fischlin establishes a positive result for a modified version of RSA-OAEP, with respect to a restricted class of adversaries, in the random oracle model.

Ventre and Visconti [19] later propose a comparison-based definition of this security notion, which is more in line with the well-studied definitions proposed by Bellare et al. [4,8]. For chosen-plaintext attacks the authors prove that (a restricted version of) their definition is equivalent to that of Fischlin. They also establish equivalence for chosen-ciphertext attacks, for a well-defined class of relations that do not depend on the challenge public key (known as lacking relations). The authors also provide additional feasibility results by proposing two constructions of completely non-malleable schemes, one in the common reference string model using non-interactive zero-knowledge proofs, and another using interactive encryption schemes. Therefore, the only previously known completely non-malleable (and non-interactive) scheme in the standard model, is quite inefficient as it relies on generic zero-knowledge techniques.

Motivation. The initial motivation for complete non-malleability resided on constructing *non-malleable commitment* schemes. A commitment scheme can be constructed from an encryption scheme in the following way. To commit to a message, one generates a key pair and encrypts the message under the generated public key. The resulting public key/ciphertext pair forms the commitment. To de-commit, one reveals a valid secret key or the message/randomness pair used in encryption. In this setting, it is clearly desirable that the encryption scheme should be completely non-malleable in order to guarantee non-malleability of the associated commitment scheme.

Furthermore, new notions of security of high practical relevance have been emerging in the literature that closely relate to different flavours of complete non-malleability. The pattern connecting these notions is that adversaries are allowed to tamper with the keys, under which they are challenged, in order to gain extra advantage. *Robust encryption* [1] is one such notion, and it is pitched at applications where ciphertext anonymity is relevant. This notion requires it to be infeasible to construct a ciphertext which is valid under two distinct public keys. Another such notion is security under *related-key attacks* [5], where cipher operations can be executed over perturbed versions of the challenge secret key. This model is of particular relevance in the symmetric encryption setting. Also worth mentioning are concrete attacks on key-agreement protocols and public-key signature schemes, where attackers are able to introduce public keys of their choice in the protocol execution [13].

The relations between these new notions of security are understudied and constitute a novel challenge in theoretical cryptography. A deeper understanding of the relations between these notions of security should permit identifying a core set of security models that facilitate the design and analysis of strongly secure schemes with practical relevance. The main motivation of this work is, therefore, to take an important step in this direction. We aim to expand the

current understanding of complete non-malleability, by establishing relations among notions of complete non-malleability and ciphertext indistinguishability that are akin to those already known for standard non-malleability. To this end, we introduce a new indistinguishability based notion, and demonstrate its applicability by constructing an efficient and completely non-malleable scheme.

Strong chosen-ciphertext attacks. Our search for a suitable indistinguishability-based definition of complete non-malleability resulted in a natural extension of the standard IND-CCA2 security model, in which the adversary can get decryptions of ciphertexts under arbitrary public keys of its choice. We call this a *strong chosen-ciphertext attack* scenario, and say that the adversary is given access to a *strong decryption oracle*. This, in turn, brings together two fields which previously remained unrelated in provable security, namely complete non-malleability and certificateless cryptography [2,11]. Indeed, strong CCA attacks model multi-user scenarios where public keys might not be authenticated, and were initially proposed as a natural attack model for certificateless schemes that aimed to do away with public-key certificates.

The question of whether the weakness captured by such a strong model should be seen as a real vulnerability of public-key encryption schemes has caused some discussion [11]. Arguments against this approach are based on the fact that such an attack model is not realistic, since it is highly unlikely that the adversary is able to get such assistance in a practical scenario. Another way to put this objection is that security models should be defined through experiments that are guaranteed to execute in polynomial time: providing decryptions under unknown secret keys assists the adversary through a super-polynomial time oracle.

The results we present in this paper show that the strength of the complete non-malleability notion is comparable to that of the strong chosen-ciphertext attack scenario. This connection allows us to take a more constructive view of strong decryption oracles, and argue that they can indeed be useful to analyse the security of practical schemes. To support this view, we show that *indistinguishability under strong CCA attacks is a convenient formalisation to establish that a scheme is completely non-malleable*. Furthermore, by proposing a concrete scheme, we also show that both notions are realisable without random oracles.

Finally, we note that strong decryption oracles are closely related to the recently proposed paradigm of adaptive one-way functions [17], which can be used to construct a number of cryptographic protocols that previously remained open in the literature. Indeed, the assumptions that underlie the proposed constructions of adaptive one-way functions rely on similar "magic" oracles. It would be interesting to investigate whether the techniques that we use can be useful in constructing adaptive one-way functions based on standard assumptions. Conversely, the public-key encryption scheme given in [17] seems to achieve strong chosen-ciphertext security. The relationship between adaptive one-way functions and strong security models are left for future work.

Contributions. The first contribution of our paper is a general definition of a strong decryption oracle, which unifies previous definitional approaches. Our

definition is flexible and expressive in the sense that it allows identifying the exact power of the decryption oracle that is provided to an adversary in security analysis. We also show that variants of the strong decryption oracle definition map to interesting properties of encryption schemes. We establish a connection with the validity checks that an encryption scheme performs (message validity, ciphertext validity, public key validity, etc.). More precisely, *we identify a simple and very convenient definition of the strong decryption oracle, which can be used to analyse schemes that incorporate a well-defined and natural set of validity checks*. For schemes that fail to perform these checks, care must be taken to identify the exact strength of the strong decryption oracle under which the scheme can be proven secure.

We then extend the standard indistinguishability and non-malleability models using strong decryption oracles, and examine the relations between the resulting notions. Our approach is consistent with that proposed by Bellare et al. [8,4], which allows us to naturally describe the relation between these stronger models and the more established ones. We also identify the relation between the strong chosen-ciphertext models we propose and the existing notions of complete non-malleability. To the best of our knowledge, this relation was not previously known. It permits fully characterising how these independently proposed models relate to the more standard definitions of non-malleability. The relation we establish between strong decryption oracles and complete non-malleability *provides the first convincing argument that the strong CCA models are useful in analysing the security of practical encryption schemes*.

Finally, we propose a concrete scheme that *efficiently achieves strong chosen-ciphertext security* based on the decisional bilinear Diffie-Hellman assumption. The scheme is secure under a very general definition of the strong decryption oracle, which is made possible by the insights regarding validity checks we described above. The scheme is derived from Waters' identity-based encryption scheme [20] using techniques previously employed in constructing certificateless public-key encryption schemes [11]. Our equivalence result also establishes our scheme as the first efficient completely non-malleable scheme without random oracles. We stress that our scheme is based on a standard and well-known problem and does *not* rely on interactive assumptions or "magic" oracles.

Organisation. In the next section we fix notation by defining public-key encryption schemes and various algorithms associated to them. In Section 3 we discuss different approaches in defining strong decryption oracles and propose a new generic definition. In Section 4 we look at indistinguishability and non-malleability security models for encryption schemes where adversaries have access to strong decryption oracles. We establish relations between these models and also to models existing literature. We present our scheme in the final section.

2 Preliminaries

Notation. We write $x \leftarrow y$ for assigning value y to variable x, and $x \leftarrow_{\$} X$ for sampling x from set X uniformly at random. If X is empty, we set $x \leftarrow \perp$, where

$\perp \notin \{0,1\}^\star$ is a special failure symbol. If A is a probabilistic algorithm, we write $x \leftarrow_\$ A(I_1, I_2, \ldots)$ for the action of running A on inputs $I_1, I_2, \ldots$ with random coin chosen uniformly at random, and assigning the result to x. Sometimes we run A on specific coins r and write $x \leftarrow A(I_1, I_2, \ldots; r)$. We denote boolean values, namely the output of checking whether a relation holds, by T (true) and F (false). For a space $\mathsf{Sp} \subseteq \{0,1\}^\star$, we identify Sp with its characteristic function. In other words, $\mathsf{Sp}(s) = \mathsf{T}$ if and only if $s \in \mathsf{Sp}$. We say s is valid with respect to Sp if and only if $\mathsf{Sp}(s) = \mathsf{T}$. When this is clear from the context, we also use Sp for sampling uniformly from Sp. Unless stated otherwise, the range of a variable s is assumed to be $\{0,1\}^\star$. The symbol : is used for appending an element to a list. We indicate vectors using bold font.

Games. We will be using the code-based game-playing language [7]. Each game has an **Initialize** and a **Finalize** procedure. It also has specifications of procedures to respond to an adversary's various oracle queries. A game Game is run with an adversary $\mathcal{A}$ as follows. First **Initialize** runs and its outputs are passed to $\mathcal{A}$. Then $\mathcal{A}$ runs and its oracle queries are answered by the procedures of Game. These procedures return $\perp$ if queried on $\perp$. When $\mathcal{A}$ terminates, its output is passed to **Finalize** which returns the outcome of the game y. This interaction is written as $\mathsf{Game}^{\mathcal{A}} \Rightarrow y$. In each game, we restrict attention to *legitimate* adversaries. Legitimacy is defined specifically for each game.

Public-key encryption. We adopt the standard multi-user syntax with the extra Setup algorithm [3], which we believe is the most natural one for security models involving multiple public keys. A public-key encryption scheme $\Pi = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{MsgSp}, \mathsf{Enc}, \mathsf{Dec})$ is specified by five polynomial-time algorithms (in the length of their inputs) as follows. Setup is the probabilistic setup algorithm which takes as input the security parameter and returns the common parameters I (we fix the security parameter implicitly, as we will be dealing with concrete security). Although all algorithms are parameterised by I, we often omit I as an explicit input for readability. $\mathsf{Gen}(\mathsf{I})$ is the probabilistic key-generation algorithm. On input common parameters I, this algorithm returns a secret key SK and a matching public key PK. Algorithm $\mathsf{MsgSp}(\mathsf{m}, \mathsf{PK})$ is a deterministic message space recognition algorithm. On input m and PK this algorithm returns T or F. $\mathsf{Enc}(\mathsf{m}, \mathsf{PK}; r)$ is the probabilistic encryption algorithm. On input a message m, a public key PK, and possibly some random coins r, this algorithm outputs a ciphertext c or a special failure symbol $\perp$. Finally, $\mathsf{Dec}(\mathsf{c}, \mathsf{SK}, \mathsf{PK})$ is the deterministic decryption algorithm. On input of a ciphertext c and keys SK and PK, it outputs a message m or a special failure symbol $\perp$. The correctness of a public-key encryption scheme requires that for any $\mathsf{I} \leftarrow_\$ \mathsf{Setup}()$, any $(\mathsf{SK}, \mathsf{PK}) \leftarrow_\$ \mathsf{Gen}()$, all $\mathsf{m} \in \mathsf{MsgSp}(\mathsf{PK})$, and any random coins r we have $\mathsf{Dec}(\mathsf{Enc}(\mathsf{m}, \mathsf{PK}; r), \mathsf{SK}, \mathsf{PK}) = \mathsf{m}$.

Remark. We note that the multi-user syntax permits capturing in a single framework schemes that execute in the plain model, in which case the global parameters are empty, as well as those which execute in the CRS model. The relations that we establish between different models hold in both cases.

Validity checking algorithms. The following spaces (and associated functions) will be used throughout the paper. All of these spaces are parameterised by I and are subsets of $\{0,1\}^\star$.

$$\begin{aligned}
&\mathsf{MsgSp}(\mathsf{PK}) := \{\mathsf{m} : \mathsf{MsgSp}(\mathsf{m}, \mathsf{PK})\}\\
&\mathsf{KeySp} := \{(\mathsf{SK}, \mathsf{PK}) : \exists r\ (\mathsf{SK}, \mathsf{PK}) = \mathsf{Gen}(r)\}\\
&\mathsf{PKSp} := \{\mathsf{PK} : \exists r, \mathsf{SK}\ (\mathsf{SK}, \mathsf{PK}) = \mathsf{Gen}(r)\}\\
&\mathsf{SKSp} := \{\mathsf{SK} : \exists r, \mathsf{PK}\ (\mathsf{SK}, \mathsf{PK}) = \mathsf{Gen}(r)\}
\end{aligned}$$

Validity assumptions. We assume throughout the paper that the encryption and decryption algorithms check if $\mathsf{m} \in \mathsf{MsgSp}(\mathsf{PK})$ and return $\perp$ if it does not hold. Often the algorithm MsgSp does not depend on PK in the sense that for any $\mathsf{PK}, \mathsf{PK}' \in \mathsf{PKSp}$ and any $\mathsf{m} \in \{0,1\}^\star$ we have $\mathsf{MsgSp}(\mathsf{m}, \mathsf{PK}) = \mathsf{MsgSp}(\mathsf{m}, \mathsf{PK}')$. For general schemes, case one can consider the infinite message space $\mathsf{MsgSp}(\mathsf{PK}) = \{0,1\}^\star$. However, given that in this paper we will often consider the set of all valid messages and sample from it, we restrict our attention to schemes with finite message spaces. As pointed out by Pass et al. [18], this means that to avoid degenerate cases we must also restrict our attention to schemes for which all the elements in the range of decryption can be efficiently encrypted, including the special failure symbol $\perp$. A distribution M on messages is *valid* with respect to a public key PK if it is computable in polynomial time and its support contains strings of equal length which lie in $\mathsf{MsgSp}(\mathsf{PK})$. We also assume that key-pair validity KeySp is efficiently implementable and require that decryption returns $\perp$ if this check fails on the keys passed to it (note that this can easily be achieved for general public key encryption schemes, by including the input randomness to Gen in SK). We also assume various algorithms check for structural properties such as correct encoding, membership in a group, etc.

3 Defining Strong Decryption Oracles

The idea behind a strong chosen-ciphertext attack is to give the adversary access to an oracle that decrypts ciphertexts of the adversary's choice with respect to arbitrary public keys. There are a number technicalities involved in defining such an oracle precisely, which we now discuss.

proc. $\mathbf{SDec}_{\mathsf{U},\mathsf{V}}(\mathsf{c}, \mathsf{PK}, \mathsf{R})$:
$\mathsf{WitSp} \leftarrow \{(\mathsf{m}, r) : \mathsf{V}(\mathsf{c}, \mathsf{PK}, \mathsf{m}, r, \mathsf{st}[\mathsf{V}])\}$
$(\mathsf{m}, r) \leftarrow_{\$} \{(\mathsf{m}, r) \in \mathsf{WitSp} : \mathsf{R}(\mathsf{m})\}$
$\mathsf{st}[\mathsf{V}] \leftarrow \mathsf{U}(\mathsf{c}, \mathsf{PK}, \mathsf{R}, \mathsf{m}, r, \mathsf{st}[\mathsf{V}])$
Return m

Fig. 1. Generic definition of a strong decryption oracle. In the first step the search is performed over sufficiently long bit strings and, for messages, it also includes the special symbol $\perp$. The state $\mathsf{st}[\mathsf{V}]$ is initialised to some value st_0.

We will base our presentation on the generic definition of a strong decryption oracle presented in Figure 1, which we thoroughly explain and justify in the discussion that follows. The oracle proceeds in three steps. The first step models the general procedure of constructing a set of candidate (valid) decryption results. The second step consists of choosing one of these candidate solutions to return to the adversary. The final step updates the state of the oracle, if it keeps one.

More precisely, in the first step, the oracle constructs a set of possible decryption results WitSp using a polynomial-time validity relation V[1]. Note that the search for messages includes the special failure symbol $\perp$. This permits making the subtle distinction of returning $\perp$ when a candidate decryption result has not been found[2], or when it has been established that the oracle may return $\perp$ when queried on a given $(\mathsf{c}, \mathsf{PK})$ pair. In the second step, it selects the message to return from WitSp. To make sure the security model is not restricting the adversary by choosing the decryption result in a particular way, we allow the adversary to provide a polynomial-time relation R to characterise a set of messages of interest to her. The oracle then samples a message at random from this set and returns it to the adversary. In the third and final step, the oracle updates any state it may have stored from previous queries. We require that the update procedure to be polynomial in the size of its inputs, excluding the state[3].

Although we have constrained the algorithms in our definition (i.e. V, R and U) to be polynomial-time, the calculations carried out in the first two steps may not be computable in polynomial time and may require an exponential number of executions of these algorithms. Nevertheless, we emphasise that the search space must be finite. This is guaranteed by the assumption that the message space of the encryption scheme is finite, and by the fact that the algorithms associated with the scheme run in polynomial time in their inputs.

The motivation for having such a general definition is that the notion of *the message encapsulated by the ciphertext* can be defined in various ways. For concreteness, let us fix U so that $\mathsf{st}[\mathsf{V}]$ is empty throughout the game execution, and look at two alternative definitions of V. These derive from two interpretations as to which message(s) might be encapsulated in a public key/ciphertext pair: they can be seen as alternative witnesses to the validity of the public key/ciphertext pair. Concretely one can define validity via the encryption operation, in which case a message/randomness pair is the witness or via the decryption algorithm, in which case the natural witness is a message/secret key pair[4]:

$$\mathsf{V}(\mathsf{c}, \mathsf{PK}, \mathsf{m}, r) := \mathsf{c} \stackrel{?}{=} \mathsf{Enc}(\mathsf{m}, \mathsf{PK}; r) \tag{1}$$

[1] This constitutes an NP-relation for the language of valid decryption results.

[2] Recall that we assume that sampling from an empty set returns $\perp$.

[3] Discarding the state size ensures that the run-time of this procedure does not increase exponentially with queries.

[4] Note that we have assumed Dec always performs the key-pair validity check, and so this is redundant in V'. We include it for the sake of clarity: for schemes which do not perform the key-pair validity check, this issue must be considered.

$$\mathsf{V}'(\mathsf{c}, \mathsf{PK}, \mathsf{m}, r) := (\mathsf{SK}, \mathsf{PK}) \stackrel{?}{=} \mathsf{Gen}(r) \wedge \mathsf{m} \stackrel{?}{=} \mathsf{Dec}(\mathsf{c}, \mathsf{SK}, \mathsf{PK}). \quad (2)$$

The first observation to make on these validity criteria is that neither of them guarantees that if a message is found to be a valid decryption result, it will be unique. This is because the correctness restriction only guarantees unique decryptability for correctly constructed $(\mathsf{c}, \mathsf{PK})$ pairs: it says nothing about the result of decryption when an invalid public key and/or an invalid ciphertext are provided as inputs. In particular, the validity criterion in Equation 1 could accept multiple messages as valid, when run on an invalid public key. Ambiguity can also occur for the validity criterion in Equation 2, when multiple valid secret keys correspond to the queried public key, and decrypt an invalid ciphertext inconsistently. This discussion justifies the need for the second step in the definition we propose: there could be many valid decryption results to choose from, and it is left to the adversary to control how this is done. In the simplest scenario, where there is only one candidate decryption result, one can assume without loss of generality that the adversary will choose to retrieve that result by passing in the trivial relation T.

The need for the first step of the definition is justified by observing that the two witness sets associated with the above validity algorithms do not always coincide. To see this, consider an encryption scheme where decryption does not necessarily fail when run on a ciphertext that falls outside the range of the encryption algorithm. Then the first witness set will be empty whereas the second may not be. A concrete example is the Cramer-Shoup [10] encryption scheme. For other schemes, such as RSA-OAEP [14], it may happen that the encryption algorithm produces apparently valid ciphertexts for invalid public keys. When this is the case, the first witness set may not be empty, whereas the second one will surely contain no messages, given that no valid secret key exists.

We note that the above issues do not arise in the standard definition of a decryption oracle, in which decryption is always carried out with a fixed secret key. In other words, the decryption oracle is stateful. To allow capturing this sort of behaviour in strong decryption oracles, we add the last step to the oracle definition. This manages the decryption oracle state, and ensures that the validity checking algorithm can access it in each query.

Specific definitions. Previous attempts to define strong decryption oracles have been introduced for certificateless public-key encryption, where public keys are not authenticated [2,11]. These definitions implicitly adopt validity criteria which are adequate only for the concrete schemes discussed in the referred works.

In the definition proposed in [2] the authors simply describe the oracle as providing "correct decryptions" even though the secret key could be unknown. A close analysis of the presentation in this work indicates that "correct decryption" is defined through a search for a message/randomness pair in the domain of the encryption, similarly to the first validity criterion presented above. However, the unique decryptability issue is implicit in the definition, since the concrete scheme the authors consider ensures that the encryption algorithm fails when queried

with an invalid public key. Extending this definition to encryption schemes in general results in the following validity criterion:

$$\mathsf{V}_{\mathsf{PK}}(\mathsf{c}, \mathsf{PK}, \mathsf{m}, r||r') := \mathsf{c} \stackrel{?}{=} \mathsf{Enc}(\mathsf{m}, \mathsf{PK}; r) \wedge (\star, \mathsf{PK}) \stackrel{?}{=} \mathsf{Gen}(r').$$

Note that this is equivalent to the validity relation in Equation 1 for schemes which check for public key validity in the encryption algorithm. Alternatively, a solution adopted in literature [13] is to restrict the class of adversaries to those which query only valid public keys. In our view, such a restriction on the adversary's behaviour is unjustified, and we will look for alternatives which guarantee stronger security.

In a more recent work [11], the strong decryption oracle is described as constructing a private key that corresponds to the queried valid public key, and then using that key to decrypt the ciphertext. The oracle then stores the extracted secret key to be reused in subsequent queries under the same public key. This definition is more in line with the intuition that a decryption oracle should reflect the behaviour of the decryption algorithm, and it is also consistent with the stateful operation of the standard decryption oracle. We can capture this definition through the algorithms presented in Figure 2. Note that, for those schemes in which there is a unique valid private key per public key or for those schemes where all valid secret keys behave consistently for all possible, even invalid, ciphertexts, the oracle resulting from these algorithms will be identical to the one using the criterion in Equation 2.

The previous discussion indicates that different definitions of a strong decryption oracle can be seen as natural for particular classes of schemes. However, we can also consider other approaches, which are not so easy to characterise. For example, a straightforward fix to the ambiguity problem described above is to have the oracle simply return $\perp$ when it arises. Agreeably, this approach addresses the problem of ambiguity directly, but it is hardly intuitive with respect to the operation of public-key encryption schemes. In particular, this definition is best suited for the class of encryption schemes for which the ambiguity never occurs. However, there is no natural characterisation of this class of schemes.

As a final motivation for a general definition of a strong decryption oracle, let us look at RSA-OAEP [14]. The non-malleability properties of (a modified version of) this scheme are analysed by Fischlin [13] using a model related to the

proc. $\mathsf{V}(\mathsf{c}, \mathsf{PK}, \mathsf{m}, r, \mathsf{st}[\mathsf{V}])$:	**proc.** $\mathsf{U}(\mathsf{c}, \mathsf{PK}, \mathsf{R}, \mathsf{m}, r, \mathsf{st}[\mathsf{V}])$:
$(\mathsf{SK}', \mathsf{PK}') \leftarrow \mathsf{Gen}(r)$	$(\mathsf{SK}', \mathsf{PK}') \leftarrow \mathsf{Gen}(r)$
If $((\mathsf{SK}, \mathsf{PK}) \in \mathsf{st}[\mathsf{V}] \wedge \mathsf{SK}' \neq \mathsf{SK})$	If $\mathsf{PK}' \neq \mathsf{PK} \vee (\mathsf{SK}, \mathsf{PK}) \in \mathsf{st}[\mathsf{V}]$
$\mathsf{PK}' \neq \mathsf{PK}$ Return F	Return $\mathsf{st}[\mathsf{V}]$
If $\mathsf{m} = \mathsf{Dec}(\mathsf{c}, \mathsf{SK}', \mathsf{PK}')$ Return T	$\mathsf{st}[\mathsf{V}] \leftarrow (\mathsf{SK}', \mathsf{PK}') : \mathsf{st}[\mathsf{V}]$
Return F	Return $\mathsf{st}[\mathsf{V}]$

Fig. 2. Update and validity algorithms for a stateful strong decryption oracle with initial state $\mathsf{st}_0 = (\mathsf{SK}^\star, \mathsf{PK}^\star)$

decryption oracle associated with Equation 1. However, the analysis is restricted to adversaries that only query valid public keys. For such adversaries, the resulting oracle is identical to that resulting from Equation 2, as the decryption algorithm of the scheme checks for key-pair validity and recovers the random coins used in encryption. However, once this restriction is dropped, the oracles are no longer equivalent. Security with respect to Equation 2 is still implied by Fischlin's analysis but, with respect to Equation 1 it remains an open issue.

Simplification. We now characterise a class of schemes for which the above variants of strong decryption oracle collapse into a simpler definition. This class consists of encryption schemes which perform checks both at encryption and decryption stages. They check for public key validity upon encryption, returning a failure symbol if the key is invalid. Furthermore, in decryption, they check both key-pair validity and that the input ciphertext lies in the range of the encryption algorithm. Note that for such schemes, whenever encryption and decryption do not fail, then correctness ensures that the set of messages which can be obtained using any of the validity criteria above coincide, and have cardinality 1. The simplified version of the strong decryption oracle that we arrive at is shown in Figure 3. The scheme that we present in Section 5 has been designed so that it belongs to this class of encryption schemes, and could therefore be analysed using this simpler oracle. Indeed, this observation is central to our argument that *we propose a simpler and more convenient security model in which to analyse schemes that aim to achieve complete non-malleability.*

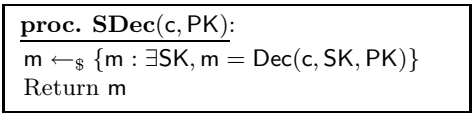

Fig. 3. Simplified definition of strong decryption for schemes which perform all checks. The search over m excludes $\perp$.

4 Security under Strong Chosen-Ciphertext Attacks

In this section, we use the general definition of a strong decryption oracle in Figure 1 to extend different security models for encryption schemes. This allows for a uniform treatment of strong security models, some of which have been independently proposed in literature. Then, we investigate the relations among the resulting security notions, as well as those in [13,19].

4.1 Indistinguishability of Ciphertexts

We now introduce ciphertext indistinguishability under strong chosen-ciphertext attacks as the natural extension of the standard notions of security for public-key encryption schemes. The IND-SCCAx advantage of an adversary $\mathcal{A}$ for $\mathsf{x} = 0, 1, 2$ against a public-key encryption scheme Π is defined by

$$\mathbf{Adv}^{\mathsf{ind\text{-}sccax}}_{\Pi}(\mathcal{A}) := 2 \cdot \Pr\left[\mathsf{IND\text{-}SCCAx}^{\mathcal{A}}_{\Pi} \Rightarrow \mathsf{T}\right] - 1,$$

where game IND-SCCAx is shown in Figure 4. Implicit in this definition are the descriptions of the U and V algorithms, which are fixed when analysing a scheme in the resulting IND-SCCAx model. As seen in the previous section, *one can make general claims of security and still use a simple definition for the strong decryption oracle (Figure 3) by showing that the scheme satisfies a well-defined set of natural properties.*

Game $\mathsf{IND\text{-}SCCAx}_{\Pi}$

proc. Initialize():
$b \leftarrow_{\$} \{0,1\}$; $\mathsf{I} \leftarrow_{\$} \mathsf{Setup}()$
$(\mathsf{SK}^{\star}, \mathsf{PK}^{\star}) \leftarrow_{\$} \mathsf{Gen}()$
$\mathsf{List} \leftarrow []$; $\mathsf{st}[\mathsf{V}] \leftarrow \mathsf{st}_0$
Return $(\mathsf{I}, \mathsf{PK}^{\star})$

proc. LoR$(\mathsf{m}_0, \mathsf{m}_1)$:
$\mathsf{c} \leftarrow_{\$} \mathsf{Enc}(\mathsf{m}_b, \mathsf{PK}^{\star})$
$\mathsf{List} \leftarrow (\mathsf{c}, \mathsf{PK}^{\star}) : \mathsf{List}$
Return c

proc. SDec$(\mathsf{c}, \mathsf{PK}, \mathsf{R})$:
Return $\mathbf{SDec}_{\mathsf{U},\mathsf{V}}(\mathsf{c}, \mathsf{PK}, \mathsf{R})$

proc. Finalize(b'):
Return $(b' = b)$

Fig. 4. Game defining indistinguishability under strong chosen-ciphertext attacks. An adversary $\mathcal{A}$ is legitimate if: 1) It calls **LoR** only once with $\mathsf{m}_0, \mathsf{m}_1 \in \mathsf{MsgSp}(\mathsf{PK})$ such that $|\mathsf{m}_0| = |\mathsf{m}_1|$; and 2) R is polynomial-time and, if $\mathsf{x} = 0$ it does not call **SDec**, if $\mathsf{x} = 1$ it does not call **SDec** after calling **LoR**, and if $\mathsf{x} = 2$ it does not call **SDec** with a tuple $(\mathsf{c}, \mathsf{PK})$ in List.

Strong parallel attacks. Bellare and Sahai [8] define a security notion known as indistinguishability under parallel chosen-ciphertext attacks. Here the adversary can query a vector of ciphertexts to a parallel decryption oracle exactly once and after its left-or-right query, receiving the corresponding component-wise decryptions. It is proved in [8] that parallel security maps well to non-malleability of encryption schemes. We extend this model to incorporate strong attacks by defining the IND-SPCAx advantage of an adversary $\mathcal{A}$ against an encryption scheme Π similarly to above, where game IND-SPCAx is shown in Figure 5. Note that under this definition, and consistently with previous results, IND-SPCA2 is equivalent to IND-SCCA2: the parallel oracle is subsumed by the strong decryption oracle that the adversary is allowed to call adaptively after the challenge phase. We remark that a stronger definition can be adopted, whereby the adversary is allowed to query the parallel oracle with a relation that takes all the ciphertexts simultaneously. We will return to this issue in the next section.

KEM/DEM composition. The standard proof technique [10] to establish the security of hybrid encryption schemes consisting of a secure keys encapsulation mechanism (KEM) and a secure data encryption mechanism (DEM), fails to extend to the strong chosen-ciphertext models (strong security for KEMs can be defined in the natural way). This failure is due to the non-polynomial nature of the decryption oracle, which cannot be simulated even if one generates the

Game $\mathsf{IND\text{-}SPCAx}_{\Pi}$

proc. Initialize():
$b \leftarrow_{\$} \{0,1\}$; $\mathsf{I} \leftarrow_{\$} \mathsf{Setup}()$
$(\mathsf{SK}^{\star}, \mathsf{PK}^{\star}) \leftarrow_{\$} \mathsf{Gen}()$
$\mathsf{List} \leftarrow []$; $\mathsf{st}[\mathsf{V}] \leftarrow \mathsf{st}_0$
Return $(\mathsf{I}, \mathsf{PK}^{\star})$

proc. SDec$(\mathsf{c}, \mathsf{PK}, \mathsf{R})$:
Return $\mathbf{SDec}_{\mathsf{U},\mathsf{V}}(\mathsf{c}, \mathsf{PK}, \mathsf{R})$

proc. LoR$(\mathsf{m}_0, \mathsf{m}_1)$:
$\mathsf{c} \leftarrow_{\$} \mathsf{Enc}(\mathsf{m}_b, \mathsf{PK}^{\star})$
$\mathsf{List} \leftarrow (\mathsf{c}, \mathsf{PK}^{\star}) : \mathsf{List}$
Return c

proc. PSDec$(\mathbf{c}, \mathbf{PK}, \mathbf{R})$:
For i from 1 to $\#\mathbf{c}$ do
  $\mathbf{m}[i] \leftarrow_{\$} \mathbf{SDec}_{\mathsf{U},\mathsf{V}}(\mathbf{c}[i], \mathbf{PK}[i], \mathbf{R}[i])$
Return $\mathbf{m}$

proc. Finalize(b'):
Return $(b' = b)$

Fig. 5. Game defining indistinguishability under strong parallel chosen-ciphertext attacks. An adversary $\mathcal{A}$ is legitimate if: 1) It calls **LoR** only once with $\mathsf{m}_0, \mathsf{m}_1 \in \mathsf{MsgSp}(\mathsf{PK})$ such that $|\mathsf{m}_0| = |\mathsf{m}_1|$; 2) It calls **PSDec** exactly once and after calling **LoR**, on a tuple $(\mathbf{c}, \mathbf{PK}, \mathbf{R})$ such that for $i = 1, \ldots, \#\mathbf{c}$, the tuples $(\mathbf{c}[i], \mathbf{PK}[i])$ do not appear in List and $\mathbf{R}[i]$ are polynomial-time; and 3) R is polynomial-time and, if $\mathsf{x} = 0$ it does not call **SDec**, or if $\mathsf{x} = 1$ it does not call **SDec** after calling **LoR**, or if $\mathsf{x} = 2$ it does not call **SDec** with a tuple $(\mathsf{c}, \mathsf{PK})$ in List.

challenge public key. One way to go around this obstacle is to build schemes which permit embedding an *escrow* trapdoor in the common parameters, enabling decryption over *all* public keys.

4.2 Complete Non-malleability

Turning our attention to strong notions of non-malleability, or so-called complete non-malleability, we shall see in this section how strong decryption oracles can be used to bring coherence to existing definitional approaches. In particular, we introduce new definitions using strong decryption oracles that can be used to establish clear relations with the strong indistinguishability notion introduced above. We also clarify how the definitions we propose relate to those previously described in literature.

Simulation-based definition. The first definition of complete non-malleability was introduced by Fischlin in [13]. We propose an alternative definition. We define the SNM-SCCAx advantage of an adversary $\mathcal{A}$ with respect to a polynomial-time relation R and a polynomial-time simulator $\mathcal{S}$ against a public-key encryption scheme Π by

$$\mathbf{Adv}^{\mathsf{snm\text{-}sccax}}_{\Pi,\mathsf{R},\mathcal{S}}(\mathcal{A}) := \Pr\left[\mathsf{Real\text{-}SNM\text{-}SCCAx}^{\mathcal{A}}_{\Pi,\mathsf{R}} \Rightarrow \mathsf{T}\right] - \Pr\left[\mathsf{Ideal\text{-}SNM\text{-}SCCAx}^{\mathcal{S}}_{\Pi,\mathsf{R}} \Rightarrow \mathsf{T}\right]$$

where games Real-SNM-SCCAx and Ideal-SNM-SCCAx are as shown in Figure 6. The syntax of public-key encryption that we use includes a Setup procedure and hence we explicitly include the common parameters I as an input to the malleability relation. This approach is consistent with the explicit inclusion of the challenge public key, which is shown in [13] to strictly strengthen the definition. Additionally, for backward compatibility with [8], our relations also include the state information st_{R}. For strong decryption oracles that behave consistently

Game $\mathsf{Real\text{-}SNM\text{-}SCCA}_{\mathsf{x},\Pi,\mathsf{R}}$

proc. Initialize():
$\mathsf{I} \leftarrow_{\$} \mathsf{Setup}()$
$(\mathsf{SK}^\star, \mathsf{PK}^\star) \leftarrow_{\$} \mathsf{Gen}()$
$\mathsf{List} \leftarrow []$; $\mathsf{st}[\mathsf{V}] \leftarrow \mathsf{st}_0$
Return $(\mathsf{I}, \mathsf{PK}^\star)$

proc. SDec$(\mathsf{c}, \mathsf{PK}, \mathsf{R}')$:
Return $\mathbf{SDec}_{\mathsf{U},\mathsf{V}}(\mathsf{c},\mathsf{PK},\mathsf{R}')$

proc. Enc$(\mathrm{M}, \mathsf{st}_\mathsf{R})$:
$\mathsf{m} \leftarrow_{\$} \mathrm{M}()$
$\mathsf{c} \leftarrow_{\$} \mathsf{Enc}(\mathsf{m}, \mathsf{PK}^\star)$
$\mathsf{List} \leftarrow (\mathsf{c}, \mathsf{PK}^\star) : \mathsf{List}$
Return c

proc. Finalize$(\mathbf{c}, \mathbf{PK}, \mathbf{R})$:
For i from 1 to $\#\mathbf{c}$ do
  $\mathbf{m}[i] \leftarrow_{\$} \mathbf{SDec}_{\mathsf{U},\mathsf{V}}(\mathbf{c}[i],\mathbf{PK}[i],\mathbf{R}[i])$
Return $\mathsf{R}(\mathsf{I},\mathsf{m},\mathbf{m},\mathbf{c},\mathsf{PK}^\star,\mathbf{PK},\mathrm{M},\mathsf{st}_\mathsf{R})$

Game $\mathsf{Ideal\text{-}SNM\text{-}SCCA}_{\mathsf{x},\Pi,\mathsf{R}}$

proc. Initialize():
$\mathsf{I} \leftarrow_{\$} \mathsf{Setup}()$
$(\mathsf{SK}^\star, \mathsf{PK}^\star) \leftarrow_{\$} \mathsf{Gen}()$
$\mathsf{st}[\mathsf{V}] \leftarrow \mathsf{st}_0$
Return $(\mathsf{I}, \mathsf{PK}^\star)$

proc. SDec$(\mathsf{c}, \mathsf{PK}, \mathsf{R}')$:
Return $\mathbf{SDec}_{\mathsf{U},\mathsf{V}}(\mathsf{c},\mathsf{PK},\mathsf{R}')$

proc. Finalize$(\mathbf{c}, \mathbf{PK}, \mathbf{R}, \mathrm{M}, \mathsf{st}_\mathsf{R})$:
For i from 1 to $\#\mathbf{c}$ do
  $\mathbf{m}[i] \leftarrow_{\$} \mathbf{SDec}_{\mathsf{U},\mathsf{V}}(\mathbf{c}[i],\mathbf{PK}[i],\mathbf{R}[i])$
$\mathsf{m} \leftarrow_{\$} \mathrm{M}()$
Return $\mathsf{R}(\mathsf{I},\mathsf{m},\mathbf{m},\mathbf{c},\mathsf{PK}^\star,\mathbf{PK},\mathrm{M},\mathsf{st}_\mathsf{R})$

Fig. 6. Games defining simulation-based complete non-malleability under strong chosen-ciphertext attacks. An adversary $\mathcal{A}$, playing the real game, is legitimate if: 1) It calls **Enc** once with a valid M; 2) R' queried to **SDec** is computable in polynomial time; if $\mathsf{x} = 0$ it does not call **SDec**; if $\mathsf{x} = 1$ it does not call **SDec** after calling **LoR**; and if $\mathsf{x} = 2$ it does not call **SDec** with a tuple in List; and 3) It calls **Finalize** with a tuple such that all relations in $\mathbf{R}$ are computable in polynomial time and, for $i = 1, \ldots, \#\mathbf{c}$, the tuples $(\mathbf{c}[i], \mathbf{PK}[i])$ do not appear in List. A *non-assisted* simulator, playing the ideal game, $\mathcal{S}$ is legitimate if: 1) It calls **Finalize** with a valid M; and 2) It does not call **SDec**. An *assisted* simulator, playing the ideal game, is legitimate if: 1) It calls **Finalize** with a valid M; 2) R' queried to **SDec** is computable in polynomial time; and 3) If $\mathsf{x} = 0$ it does not call **SDec**.

with the standard one for $\mathsf{PK}^\star$, and for a class of relations that matches those in the original definition, our definition implies standard assisted and non-assisted simulation-based non-malleability as defined in [8].

A similar line of reasoning does not permit concluding that our definition also implies Fischlin's complete non-malleability. A legitimate adversary under Fischlin's definition is also a legitimate adversary under the definition in 6. However, we cannot identify a concrete version of the strong decryption oracle that captures the environment under which such an adversary should run. This is because Fischlin's model implicitly uses two definitions of decryption oracle: one during the interactive stages of the game, where the adversary has access to a standard decryption oracle that decrypts using the challenge secret key, and a second one in the **Finalize** stage, where the ciphertext produced by the adversary is decrypted by searching through the message/randomness space. We justify our modelling choice with two arguments. Firstly, the construction of **Finalize** in Fischlin's definition makes it impossible to prove that this security model is stronger than the apparently weaker definition of non-malleability

proposed in [8], which uses the standard decryption oracle to recover messages from the ciphertexts output by the adversary (recall the particular case of invalid ciphertexts under a valid public key, for which the two interpretations of valid decryption results do not coincide). This suggests that using a consistent definition of a (strong) decryption oracle in all stages of the game is a better approach. Secondly, if this change were introduced in Fischlin's definition, then this would simply be a special case of our more general definition.

Comparison-based definition. The simulation-based definition due to Fischlin was later reformulated by Ventre and Visconti [19] as a comparison-based notion. We introduce an alternative definition based on the CNM-SCCAx game shown in Figure 7 and define CNM-SCCAx advantage of an adversary $\mathcal{A}$ against an encryption scheme Π as

$$\mathbf{Adv}^{\mathsf{cnm\text{-}sccax}}_{\Pi}(\mathcal{A}) := \Pr\left[\mathsf{CNM\text{-}SCCAx}^{\mathcal{A}}_{\Pi} \Rightarrow \mathsf{T} \,\middle|\, b=1\right] - \Pr\left[\mathsf{CNM\text{-}SCCAx}^{\mathcal{A}}_{\Pi} \Rightarrow \mathsf{T} \,\middle|\, b=0\right]$$

Our definition differs from that given in [19] in the following aspects. We provide the adversary with strong decryption oracles in various stages of the attack. In both models the adversary is allowed to return a vector of ciphertexts, although in [19] it is restricted to returning a single public key. Also, procedure **Finalize** does not automatically return F if any of the ciphertexts is invalid. The definition in [19] would therefore be weaker than ours, were it not for our modelling choice in the **Finalize** procedure. In Ventre and Visconti's definition, the relation R is evaluated by a complete search over $(\mathbf{m}[1], r_1) \times \ldots \times (\mathbf{m}[\#\mathbf{c}], r_{\#\mathbf{c}})$. In our definition we have constrained the adversary to performing the search using the strong decryption oracle independently for *each component* in $\mathbf{c}$, before evaluating R. This option is, not only consistent with the standard notions of non-malleability for encryption schemes [8], but is also essential to proving equivalence among the different notions we propose.

proc. Initialize():	**proc. Enc**(M):	Game $\mathsf{CNM\text{-}SCCAx}_{\Pi}$
$b \leftarrow_{\$} \{0,1\}$; $\mathsf{I} \leftarrow_{\$} \mathsf{Setup}()$	$\mathsf{m}_0, \mathsf{m}_1 \leftarrow_{\$} \mathrm{M}()$	
$(\mathsf{SK}^\star, \mathsf{PK}^\star) \leftarrow_{\$} \mathsf{Gen}()$	$\mathsf{c} \leftarrow_{\$} \mathsf{Enc}(\mathsf{m}_1, \mathsf{PK}^\star)$	
$\mathsf{List} \leftarrow []$; $\mathsf{st}[\mathsf{V}] \leftarrow \mathsf{st}_0$	$\mathsf{List} \leftarrow \mathsf{List} : (\mathsf{c}, \mathsf{PK}^\star)$	**proc. Finalize**($\mathbf{c}, \mathbf{PK}, \mathbf{R}, \mathsf{R}$):
Return $(\mathsf{I}, \mathsf{PK}^\star)$	Return c	For i from 1 to $\#\mathbf{c}$ do
proc. SDec($\mathsf{c}, \mathsf{PK}, \mathsf{R}'$):		$\mathbf{m}[i] \leftarrow_{\$} \mathbf{SDec}(\mathbf{c}[i], \mathbf{PK}[i], \mathbf{R}[i])$
Return $\mathbf{SDec}_{\mathsf{U},\mathsf{V}}(\mathsf{c}, \mathsf{PK}, \mathsf{R}')$		Return $\mathsf{R}(\mathsf{I}, \mathsf{m}_b, \mathbf{m}, \mathbf{c}, \mathsf{PK}^\star, \mathbf{PK})$

Fig. 7. Game defining comparison-based complete non-malleability under strong chosen-ciphertext attacks. An adversary $\mathcal{A}$ is legitimate if: 1) It calls **Enc** once with a valid M; 2) It always queries **SDec** with R' computable in polynomial time; if $\mathsf{x} = 0$ it does not call **SDec**; if $\mathsf{x} = 1$ it does not call **SDec** after calling **LoR**; and if $\mathsf{x} = 2$ it does not call **SDec** with a tuple $(\mathsf{c}, \mathsf{PK})$ in List; 3) It calls **Finalize** with a tuple $(\mathbf{c}, \mathbf{PK}, \mathbf{R}, \mathsf{R})$ such that R and all the elements of $\mathbf{R}$ are computable in polynomial time and, for $i = 1, \ldots, \#\mathbf{c}$, the tuples $(\mathbf{c}[i], \mathbf{PK}[i])$ do not appear in List.

Remark. Recall that Ventre and Visconti's proof [19] of equivalence between comparison and (non-assisted) simulation-based complete non-malleability holds (for $\mathsf{x} \neq 0$) for a restricted class of relations, called *lacking* relations, which do not depend on the challenge public key given to the adversary. We note that our equivalence proof for assisted simulators does not restrict the class of relations under which equivalence holds. Furthermore, such a restriction would be pointless in our definitions for non-assisted simulators, since the proof technique of generating a new key-pair is no longer sufficient to guarantee that the simulator can answer *strong* decryption queries under arbitrary public keys.

4.3 Relations among Notions of Security

We now present our main theorem that establishes equivalence between the security notions we have proposed above. The proof, which can be found in the full version of the paper, follows the strategy used by Bellare and Sahai [8]. We note that our result holds for *any* instantiation of the strong decryption oracle as given in Figure 1, providing further evidence that the security models we are relating are, in fact, the same notion presented using different formalisms.

Theorem 1 (Equivalence). *The* IND-SPCAx*,* CNM-SCCAx *and* SNM-SCCAx *notions of security are equivalent, for any* $\mathsf{x} \in \{0, 1, 2\}$.

Using a standard hybrid argument one can show that IND-SPCAx self-composes. Together with our equivalence result, we conclude that our notions of complete non-malleability also self-compose [18].

5 An Efficient Completely Non-Malleable Scheme

The only completely non-malleable scheme (without random oracles) known prior to this work, was that of Ventre and Visconti [19], which relied on generic (and hence inefficient) zero-knowledge techniques. In this section, we will present an efficient and strongly secure scheme based on standard assumptions.

Our scheme, which is shown in Figure 8, uses a computational bilinear group scheme Γ and a family of collision resistant hash functions Σ mapping $\mathbb{G}_T \times \mathbb{G} \times \mathbb{G}^2$ to bit strings of size n. Our scheme relies on the decisional bilinear Diffie-Hellman assumption which requires the distributions $(g, g^a, g^b, g^c, \mathbf{e}(g,g)^{abc})$ and $(g, g^a, g^b, g^c, \mathbf{e}(g,g)^d)$, for random a, b, c, and d, to be computationally indistinguishable. The scheme's design is based on the certificateless encryption scheme of [11], which in turn is based on Water's identity-based encryption scheme [20]. The construction also uses Waters' hash [20], defined by $\mathsf{WH}(w) := u_0 \prod_{i=1}^{n} u_i^{[w]_i}$.

Validity algorithms. We examine which of the validity algorithms exists for this scheme. We assume that Γ specifies algorithms to check for group membership, which are used implicitly throughout the scheme. The MsgSp algorithm is the same as checking membership in $\mathbb{G}_T$. The SKSp algorithm checks membership in $\mathbb{Z}_p$. The KeySp algorithm checks if $g^{\mathsf{SK}} = X$ and $\alpha^{\mathsf{SK}} = Y$ where

proc. $\mathsf{Setup}_{\Gamma,\Sigma,n}()$:
$\mathsf{k} \leftarrow_{\$} \mathsf{Key}()$;
$(\alpha,\beta,u_0,\ldots,u_n) \leftarrow_{\$} \mathbb{G}^{\star} \times \mathbb{G}^{n+2}$
$\mathsf{I} \leftarrow (\Gamma, \mathsf{H}_{\mathsf{k}}, \alpha, \beta, u_0, \ldots, u_n)$
Return I

proc. $\mathsf{Gen}()$:
$x \leftarrow_{\$} \mathbb{Z}_p$; $X \leftarrow g^x$; $Y \leftarrow \alpha^x$
$\mathsf{PK} \leftarrow (X, Y)$; $\mathsf{SK} \leftarrow x$
Return $(\mathsf{SK}, \mathsf{PK})$

proc. $\mathsf{Enc}(\mathsf{m}, \mathsf{PK})$:
$t \leftarrow_{\$} \mathbb{Z}_p$; $(X, Y) \leftarrow \mathsf{PK}$
If $\mathbf{e}(X, \alpha) \neq \mathbf{e}(g, Y)$
  Return $\perp$
$C_1 \leftarrow \mathsf{m} \cdot \mathbf{e}(Y, \beta^t)$;
$C_2 \leftarrow \alpha^t$
$w \leftarrow \mathsf{H}_{\mathsf{k}}(C_1, C_2, \mathsf{PK})$
$C_3 \leftarrow \mathsf{WH}(w)^t$
$\mathsf{c} \leftarrow (C_1, C_2, C_3)$
Return c

proc. $\mathsf{Dec}(\mathsf{c}, \mathsf{SK}, \mathsf{PK})$:
$(X, Y) \leftarrow \mathsf{PK}$
If $g^{\mathsf{SK}} \neq X \vee \alpha^{\mathsf{SK}} \neq Y$
  Return $\perp$
$(C_1, C_2, C_3) \leftarrow \mathsf{c}$
$w \leftarrow \mathsf{H}_{\mathsf{k}}(C_1, C_2, \mathsf{PK})$
If $\mathbf{e}(C_2, \mathsf{WH}(w)) \neq \mathbf{e}(\alpha, C_3)$
  Return $\perp$
$\mathsf{m} \leftarrow C_1 / \mathbf{e}(C_2, \beta^x)$
Return m

Fig. 8. A strongly secure public-key encryption scheme without random oracles

$(X, Y) = \mathsf{PK}$. The PKSp algorithm checks if $\mathbf{e}(X, \alpha) = \mathbf{e}(g, Y)$. Finally, we show that decryption rejects all ciphertexts outside the range of encryption. Let (C_1, C_2, C_3) be a ciphertext. Then, there exists a message m and a t such that this ciphertext can be written as $(\mathsf{m} \cdot \mathbf{e}(Y, \beta)^t, \alpha^t, C_3)$. If this ciphertext is outside the range of encryption, then $C_3 = \mathsf{WH}(w)^{t'}$ for some $t' \neq t$. But then $\mathbf{e}(C_2, \mathsf{WH}(w)) = \mathbf{e}(\alpha, \mathsf{WH}(w))^t \neq \mathbf{e}(\alpha, \mathsf{WH}(w))^{t'} = \mathbf{e}(\alpha, C_3)$ and the equality check in decryption fails.

The next theorem states the security properties of our scheme. Its proof uses technique recently proposed by Bellare and Ristenpart [6] and is given in the full version of the paper.

Theorem 2 (Informal). *Under the decisional bilinear Diffie-Hellman assumption in* Γ *and the collision resistance of the hash function family* Σ*, the above scheme is* $\mathsf{IND\text{-}SCCA2}$ *secure (with respect to* **SDec** *oracle defined in Figure 3).*

Although our equivalence theorems imply that this scheme admits a black-box assisted simulator, it does not contradict Fischlin's impossibility results on black-box simulation [13]. First note that Fischlin's impossibility result is in the plain model whereas our scheme has a setup procedure. Furthermore, our definitions do not require the opening of message/randomness pairs, whereas Fischlin requires this to derive his impossibility result for *assisted* simulators. We can indeed construct a non-assisted simulator for our scheme through a direct proof, but this requires modifying the common parameters in an essential way to simulate the strong decryption oracle. Hence this result does not hold for general relations, but only for those which ignore the I presented at their inputs (consistently with [19] we call these I-lacking relations). Furthermore, using a similar technique, we are also able to show (through a direct proof) that the zero-knowledge-based construction in [19] is completely non-malleable with respect to black-box simulators for a class of relations that are I-lacking (I in this case comprises the common reference string). We note that this is a better result than that obtained in [19], since there the class of relations must be both I-lacking and PK-lacking (i.e. they must also ignore the PK at their inputs).

Acknowledgments. The authors were funded in part by eCrypt II (EU FP7 - ICT-2007-216646) and FCT project PTDC/EIA/71362/2006. The second author was also funded by FCT grant BPD-47924-2008.

References

1. Abdalla, M., Bellare, M., Neven, G.: Robust encryption. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 480–497. Springer, Heidelberg (2010)
2. Al-Riyami, S.S., Paterson, K.G.: Certificateless public key cryptography. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003)
3. Bellare, M., Boldyreva, A., Micali, S.: Public-key encryption in a multi-user setting: Security proofs and improvements. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 259–274. Springer, Heidelberg (2000)
4. Bellare, M., Desai, A., Pointcheval, D., Rogaway, P.: Relations among notions of security for public-key encryption schemes. In: Krawczyk [16], pp. 26–45
5. Bellare, M., Kohno, T.: A theoretical treatment of related-key attacks: Rka-prps, rka-prfs, and applications. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 491–506. Springer, Heidelberg (2003)
6. Bellare, M., Ristenpart, T.: Simulation without the artificial abort: Simplified proof and improved concrete security for waters' ibe scheme. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 407–424. Springer, Heidelberg (2010)
7. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (2006)
8. Bellare, M., Sahai, A.: Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization. Cryptology ePrint Archive, Report 2006/228 (2006), `http://eprint.iacr.org/2006/228`
9. Cramer, R. (ed.): PKC 2008. LNCS, vol. 4939. Springer, Heidelberg (2008)
10. Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk [16], pp. 13–25
11. Dent, A.W., Libert, B., Paterson, K.G.: Certificateless encryption schemes strongly secure in the standard model. In: Cramer [9], pp. 344–359
12. Dolev, D., Dwork, C., Naor, M.: Nonmalleable cryptography. SIAM J. Comput. 30(2), 391–437 (2000)
13. Fischlin, M.: Completely non-malleable schemes. In: Caires, L., Italiano, G.F., Monteiro, L., Palamidessi, C., Yung, M. (eds.) ICALP 2005. LNCS, vol. 3580, pp. 779–790. Springer, Heidelberg (2005)
14. Fujisaki, E., Okamoto, T., Pointcheval, D., Stern, J.: Rsa-oaep is secure under the rsa assumption. J. Cryptology 17(2), 81–104 (2004)
15. Goldwasser, S., Micali, S.: Probabilistic encryption. J. Comput. Syst. Sci. 28(2), 270–299 (1984)
16. Krawczyk, H. (ed.): CRYPTO 1998. LNCS, vol. 1462. Springer, Heidelberg (1998)
17. Pandey, O., Pass, R., Vaikuntanathan, V.: Adaptive one-way functions and applications. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 57–74. Springer, Heidelberg (2008)

18. Pass, R., Shelat, A., Vaikuntanathan, V.: Relations among notions of non-malleability for encryption. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 519–535. Springer, Heidelberg (2007)
19. Ventre, C., Visconti, I.: Completely non-malleable encryption revisited. In: Cramer [9], pp. 65–84
20. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)