Strong Knowledge Extractors for Public-Key Encryption Schemes

M. Barbosa[1] and P. 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. Completely non-malleable encryption schemes resist attacks which allow an adversary to tamper with both ciphertexts *and* public keys. In this paper we introduce two extractor-based properties that allow us to gain insight into the design of such schemes and to go beyond known feasibility results in this area. We formalise *strong plaintext awareness* and *secret key awareness* and prove their suitability in realising these goals. Strong plaintext awareness imposes that it is infeasible to construct a ciphertext under *any* public key without knowing the underlying message. Secret key awareness requires it to be infeasible to produce a new public key without knowing a corresponding secret key.

Keywords. Secret Key Awareness. Strong Plaintext Awareness. Complete Non-Malleability. Strong Chosen-Ciphertext Attacks.

1 Introduction

Background. Indistinguishability of ciphertexts under chosen-ciphertext attacks (IND-CCA2) is a convenient reformulation of a more intuitive security notion known as *non-malleability*. Roughly speaking, an encryption scheme is non-malleable if, given a challenge ciphertext, it is infeasible to output a new ciphertext encrypting a plaintext related in a "meaningful" or "interesting" way to that enclosed in the challenge. The advantages of the indistinguishability formulation become apparent when one considers various subtleties which arise when defining what a meaningful relation is [22, 10]. Recently, Fischlin [18] has considered the problem of using public key encryption schemes to build non-malleable commitment schemes. It has been shown that the standard definition of non-malleability is not sufficient for this application and that a stronger variant, referred to as *complete non-malleability*, is required. This security definition allows the adversary to maul the challenge public key, as well as the ciphertext. Put differently, the adversary can output a related ciphertext under a new public key of its choice. Unlike standard non-malleability, it has been shown in [18] that completely non-malleable schemes are hard to construct. In particular, such

schemes do not exist for general relations with respect to black-box simulators that cannot access a decryption oracle (i.e. non-assisted simulators).

Complete non-malleability has recently been shown to be equivalent to *indistinguishability under strong chosen-ciphertext attacks* [2, 1]. This model enhances the adversary's capabilities to forge public keys and ask the decryption oracle to provide decryptions under the corresponding (possibly unknown) secret keys. It was also shown that it is possible to construct efficient completely non-malleable schemes using the strong chosen-ciphertext attack model, which is more convenient than performing the proof in the original simulation-based definition. Unfortunately, the equivalence result connecting strong chosen-ciphertext security to complete non-malleability holds only for simulators *assisted* by a strong decryption oracle. It therefore remains an open problem to construct efficient schemes that achieve complete non-malleability in the strongest sense.

The impossibility result from [18] dictates that to construct a scheme that achieves complete non-malleability with respect to *non-assisted* simulators, one must resort to a non-black-box simulator. In this paper we consider extractor-based properties that allow us to gain insight into the design of completely non-malleable schemes and provide a technique to go beyond known feasibility results in this area. We formalise *strong plaintext awareness* and *secret key awareness* and prove their suitability in realising these goals. We show that if such properties are realisable, and one considers non-black-box simulators, then the impossibility result established for non-assisted simulators no longer holds. We also look at how such notions can be realised with and without random oracles.

Strong plaintext awareness. Plaintext awareness formalises the intuition that one can achieve security under chosen-ciphertext attacks by making it infeasible to construct a valid ciphertext without *knowing*, a priori, the message hidden inside it. In fact, it has been shown that the combination of plaintext awareness and semantic security is enough to achieve chosen-ciphertext security [5]. We formulate a natural strengthening of plaintext awareness that requires the existence of a strong plaintext extractor that decrypts ciphertexts, even if they are encrypted under adversarially generated public keys. We prove a fundamental theorem according to which a *strongly plaintext-aware* (SPA) and IND-CPA secure scheme also withstands strong chosen-ciphertext attacks[3]. This implies, through the results in [2], that such a scheme is also completely non-malleable with respect to assisted simulators. We extend this result by showing that strong plaintext awareness allows us to directly build *non-assisted* simulators. The resulting simulators depend on the adversary and hence they are not black-box. This permits going around the impossibility result established by Fischlin [18]. Furthermore, strong plaintext awareness generalises a proof technique used by Fischlin to demonstrate that (a slightly modified version of) RSA-OAEP is completely non-malleable for non-assisted simulators[4].

[3] This result also has applications in certificateless encryption [1].

[4] A corollary of this result is that we obtain a new perspective on the *standard* notion of plaintext awareness. Indeed, a similar proof strategy can be used to construct non-assisted simulators for standard non-malleability.

Secret key awareness. We also propose a new extractor-based security definition that takes a different perspective on how to achieve strong plaintext awareness and complete non-malleability. Roughly speaking, this notion that we call *secret key awareness* (SKA), requires it to be infeasible to generate new valid public keys without knowing their corresponding secret keys. It therefore looks at enhancing the security of key-generation mechanisms. We show that an encryption scheme that is secret key aware and IND-CCA2 is also secure under strong chosen-ciphertext attacks, and therefore completely non-malleable. We derive this result via a stronger indistinguishability security notion, where the adversary has access to a public key inversion oracle[5]. Furthermore, we prove that secret key awareness, together with standard plaintext awareness, implies strong plaintext awareness. Hence, secret key awareness provides all of the benefits of strong plaintext awareness. Additionally, secret key awareness permits the construction of a complete non-malleability simulator that *opens* the secret key associated with the public created by the adversary. This is particularly relevant when the scheme is used in commitment schemes, where to de-commit one reveals a secret key rather a message/randomness pair. Strong plaintext awareness in not sufficient to open a ciphertext in the sense of de-commitment, as it does not guarantee knowledge of the *randomness* used in encryption.

Schemes. We propose a generic transformation that permits transforming any IND-CCA2 scheme into a secret key aware (and still IND-CCA2) scheme in the random oracle model. The resulting schemes are therefore completely non-malleable for non-assisted simulators. We also take first steps towards building fully secret-key-aware schemes without random oracles. We propose a *generic* construction inspired in escrow public-key encryption [12], relying on schemes whose key-generation routines themselves operate as an encryption scheme. We are, however, unable to instantiate this scheme and leave it as an interesting open problem. Next, we move to specific constructions based on knowledge assumptions. A natural candidate for building a secret key aware scheme is the Diffie-Hellman Knowledge assumption [5]. This approach, however, fails once we notice that secret key awareness allows adaptive attacks on the public keys, whereas Diffie-Hellman tuples are malleable. We therefore introduce a new knowledge assumption stating, roughly speaking, that it is impossible to compute integers of the form P^2Q, where P and Q are prime, without knowing the factors and even if provided with another integer of this form. This assumption can be used to demonstrate that variants of RSA satisfy weak forms of secret key awareness.

Organisation. We first review related work. Then, in Section 2 we settle notation and recall the syntax for public-key encryption schemes. We also recall the definition of strong decryption oracles and IND-SCCA2 security. In the same section we also introduce invert and chosen-ciphertext attacks, which we will use later on in the paper. In Section 3 we introduce our extractor-based notions. In Section 4 we discuss constructions of secret key aware schemes.

[5] This type of oracle has been shown to have numerous applications in the context of adaptive one-way functions [21].

1.1 Related work

Plaintext awareness was originally formulated by Bellare and Rogaway [7] in the random oracle model. Later, Bellare and Palacio [5] gave the first definition of PA in the standard model. It is well known [5, 4] that plaintext awareness together with IND-CPA imply a level of security that is strictly stronger than IND-CCA2. The authors in [24] showed that plaintext awareness is an "all-or-nothing property" in the sense that *one-wayness* (or even a weaker condition called non-triviality) together with PA2 plaintext awareness is enough to guarantee IND-CCA2 security. Birkett and Dent [11] settled the relations between notions of plaintext awareness from [16], and showed that schemes with infinite message spaces that are plaintext-aware and one-way do not exist using techniques from [24].

Non-malleability (as a general notion) was originally introduced in the seminal work of Dolev, Dwork, and Naor [17]. In order to establish relations with other notions of security, non-malleability for public-key encryption was reformulated by Bellare et al. [4] as a comparison-based security model. Bellare and Sahai [10, 9] later fully established the relation between this comparison-based definition and the original simulation-based definition of Dolev et al. Pass, Shelat, and Vaikuntanathan [22] provide a full characterisation of non-malleability, identifying some shortcomings in previous results and considering their robustness under a form of composition where the adversary is provided with a polynomial number of challenge ciphertexts.

Complete non-malleability, was proposed by Fischlin [18]. Here the adversary is allowed to choose the public key under which the target ciphertext is produced. The same author presented impossibility results as to the construction of completely non-malleable schemes with respect to black-box simulators and general relations, and showed that a modified version of RSA-OAEP is completely non-malleable in the random oracle model. Visconti and Ventre [26] proposed a comparison-based definition of complete non-malleability, studied its relation with the simulation-based definition of Fischlin, and also gave a generic construction of completely non-malleable schemes based on NIZK-PoK. The authors in [2] define strong decryption oracles, use this to introduce indistinguishability under strong chosen-ciphertext attacks and establish relations with assisted simulation-based and comparison-based complete non-malleability. A practical and strongly secure scheme (without random oracles) based on the decisional bilinear Diffie-Hellman problem is also given.

Adaptive one-way functions [21], where an adversary has access to an inversion oracle, and extractable one-way functions [13, 14], where one requires knowledge of pre-image, have been recently proposed. Secret key awareness can be seen as a refinement of these notions for public-key encryption.

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 coins chosen uniformly at random, and assigning the result to x. When A is run on specific coins r, we 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 $s \in \mathsf{Sp}$. The function $\mathsf{Sp}(\cdot)$ always exists, although it may not be computable in polynomial time. 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, and we indicate vectors using bold-faced font. We say $f(\lambda)$ is negligible if $f(\lambda) \in \cap_{c \in \mathbb{N}} O(\lambda^{-c})$.

Games. In this paper we will be using code-based game-playing [8]. 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. All algorithms (adversaries, extractors and plaintext/public-key creators) are assumed to run in probabilistic polynomial time (PPT).

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 1^λ and returns the common domain parameter[6] I. $\mathsf{Gen}(\mathsf{I})$ is the probabilistic key-generation algorithm. On input global 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, this algorithm outputs a message m or a special failure symbol $\perp$. The correctness of a public-key encryption scheme requires that for any $\mathsf{I} \leftarrow_\$ \mathsf{Setup}(1^\lambda)$, any $(\mathsf{SK}, \mathsf{PK}) \leftarrow_\$ \mathsf{Gen}()$ and all $\mathsf{m} \in \mathsf{MsgSp}(\mathsf{PK})$ we have $\Pr[\mathsf{Dec}(\mathsf{Enc}(\mathsf{m}, \mathsf{PK}), \mathsf{SK}, \mathsf{PK}) = \mathsf{m}] = 1$.

[6] Although all algorithms are parameterised by I, we often omit I as an explicit input for readability. Furthermore, we assume that the security parameter is included in I.

REMARK. We note that the multi-user syntax permits capturing in the same framework schemes that execute in the standard model, in which case the global parameters are empty; and also schemes which execute in the Common Reference String (CRS) model. All the relations that we establish between the different models apply to 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 $\{0,1\}^\star$.

$$\mathsf{MsgSp}(\mathsf{PK}) := \{\mathsf{m} : \mathsf{MsgSp}(\mathsf{m}, \mathsf{PK})\}$$
$$\mathsf{KeySp} := \{(\mathsf{SK}, \mathsf{PK}) : \exists r\ (\mathsf{SK}, \mathsf{PK}) = \mathsf{Gen}(r)\}$$

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 two valid public keys PK and PK' 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, one can consider the infinite message space $\mathsf{MsgSp}(\mathsf{PK}) = \{0,1\}^\star$ case. 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. [22], 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[7], including the special failure symbol $\perp$. We also assume that the key-pair validity algorithm KeySp is polynomial-time and require that decryption returns $\perp$ if this check fails on the key-pair passed to it. We also assume various algorithms check for structural properties such as correct encoding, membership in a group, etc.

2.1 Strong chosen-ciphertext security

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.

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.

We follow [2] and adopt a generic definition of strong decryption as shown in Figure 1. The oracle proceeds in three steps. The first step models the general

[7] This can be easily achieved for schemes used in practice.

procedure of constructing a set of candidate (valid) decryption results[8]. 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[9]. As discussed in [2] the motivation for having such a general definition is that the notion of *the message encapsulated by the ciphertext* can be defined in a number of ways, depending on the witnesses that are taken to assess the validity of the public key/ciphertext pair. For example, one can define validity via the encryption operation, in which case a message/randomness pair is the witness

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

or via the decryption algorithm, where a message/secret key pair is the witness

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

Note that neither criterion guarantees that, if a message is found to be a valid decryption result, then it will be unique. This 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 by providing a relation R on messages as input to the oracle. For a well-defined and broad class of schemes [2], this general definition collapses into a much simpler one. However, we follow this approach for the sake of generality.

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

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

where game IND-SCCAx is shown in Figure 2. 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. We say a scheme is IND-SCCAx secure if the advantage of any PPT adversary is negligible.

2.2 Security under invert and chosen-ciphertext attacks

We introduce a new security model for encryption that helps us clarify the relations among notions we establish later on. In this model, the adversary has access to an oracle that, given a public key generated by the adversary, provides it with the corresponding secret key. Figure 4 presents the general form of the **Inv** procedure, which is analogous to the **SDec** procedure presented in the previous section. When many secret keys satisfy the validity criterion, the adversary is

[8] Search for messages is over sufficiently long bit strings together with the special symbol $\perp$. Search for random coins is over sufficiently long bit strings.

[9] The state is initialized to some value st_0. A natural use of the state is to make sure that decryption is consistent in different calls.

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

proc. Initialize(λ):
$b \leftarrow_{\$} \{0,1\}$; $\mathsf{I} \leftarrow_{\$} \mathsf{Setup}(1^{\lambda})$
$(\mathsf{SK}^{\star}, \mathsf{PK}^{\star}) \leftarrow_{\$} \mathsf{Gen}()$
$\mathsf{List} \leftarrow []$; $\mathsf{st}[\mathsf{V}] \leftarrow \mathsf{st}_0$
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. 2: 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.

Game $\mathsf{IND\text{-}ICAx}_{\Pi}(\lambda)$

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

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

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

Fig. 3: Game defining indistinguishability under invert and 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) R is polynomial-time and, if $\mathsf{x} = 0$ it does not call **Dec** or **Inv**, if $\mathsf{x} = 1$ it does not call **Dec** or **Inv** after calling **LoR**, and if $\mathsf{x} = 2$ it does not call **Dec** with a c in List; and 3) It does not call **Inv** on $\mathsf{PK}^{\star}$.

also allowed to restrict the set of "interesting" secret keys from which the answer is sampled by providing a relation R on secret keys as input to the oracle. A natural validity criteria for this oracle is

$$\mathsf{V}(\mathsf{PK}, \mathsf{SK}, r) := (\mathsf{SK}, \mathsf{PK}) \stackrel{?}{=} \mathsf{Gen}(r)$$

accepting all key-pairs that may be output by the key-generation algorithm[10].

We define the $\mathsf{IND\text{-}ICAx}$ advantage of an adversary $\mathcal{A}$ for $\mathsf{x} = 0, 1, 2$ against encryption scheme Π is defined by

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

where Game $\mathsf{IND\text{-}ICAx}$ is shown in Figure 3. We say a scheme is $\mathsf{IND\text{-}ICAx}$ secure if the advantage of any PPT adversary is negligible. This new model can be related to $\mathsf{IND\text{-}SCCAx}$ as follows. For a given $\mathbf{Inv}_{\mathsf{U},\mathsf{V}}$ procedure, define the associated $\mathbf{SDec}_{\mathsf{U}',\mathsf{V}'}$ procedure through the algorithms shown in Figure 5. The

[10] Another validity criteria, corresponding to a natural stateful invert oracle, will ensure that repeat queries will be answered consistently.

$\underline{\textbf{proc. } \mathbf{Inv}_{\mathsf{U},\mathsf{V}}(\mathsf{PK},\mathsf{R})}$:
$\mathsf{WitSp} \leftarrow \{(\mathsf{SK}, r) : \mathsf{V}(\mathsf{PK}, \mathsf{SK}, r, \mathsf{st}[\mathsf{V}])\}$
$(\mathsf{SK}, r) \leftarrow_{\$} \{(\mathsf{SK}, r) \in \mathsf{WitSp} : \mathsf{R}(\mathsf{SK})\}$
$\mathsf{st}[\mathsf{V}] \leftarrow \mathsf{U}(\mathsf{PK}, \mathsf{R}, \mathsf{SK}, r, \mathsf{st}[\mathsf{V}])$
Return SK

Fig. 4: Generic definition of an invert oracle.

$\underline{\textbf{algorithm } \mathsf{V}'(\mathsf{c}, \mathsf{PK}, \mathsf{m}, r, \mathsf{st}[\mathsf{V}'])}$:
$(\mathsf{st}[\mathsf{V}], (\mathsf{SK}^*, \mathsf{PK}^*)) \leftarrow \mathsf{st}[\mathsf{V}']$
If $\mathsf{PK} = \mathsf{PK}^\star$
  If $\mathsf{m} = \mathsf{Dec}(\mathsf{c}, \mathsf{SK}^*, \mathsf{PK}^*)$
    Return T Else Return F
$(\mathsf{SK}, r') \leftarrow r$
If $\mathsf{V}(\mathsf{PK}, \mathsf{SK}, r', \mathsf{st}[\mathsf{V}]) \wedge \mathsf{m} = \mathsf{Dec}(\mathsf{c}, \mathsf{SK}, \mathsf{PK})$
  Return T Else Return F

$\underline{\textbf{algorithm } \mathsf{U}'(\mathsf{c}, \mathsf{PK}, \mathsf{R}, \mathsf{m}, r, \mathsf{st}[\mathsf{V}'])}$:
$(\mathsf{st}[\mathsf{V}], (\mathsf{SK}^*, \mathsf{PK}^*)) \leftarrow \mathsf{st}[\mathsf{V}']$
$(\mathsf{SK}, r') \leftarrow r$
$\mathsf{R}'(\mathsf{SK}) := \mathsf{R}(\mathsf{Dec}(\mathsf{c}, \mathsf{SK}, \mathsf{PK}))$
$\mathsf{st}[\mathsf{V}] \leftarrow \mathsf{U}(\mathsf{PK}, \mathsf{R}', \mathsf{SK}, r', \mathsf{st}[\mathsf{V}])$
Return $(\mathsf{st}[\mathsf{V}], (\mathsf{SK}^*, \mathsf{PK}^*))$

Fig. 5: U' and V' for $\mathbf{SDec}_{\mathsf{U}',\mathsf{V}'}$ corresponding to $\mathbf{Inv}_{\mathsf{U},\mathsf{V}}$ with $\mathsf{st}_0 = (\mathsf{SK}^\star, \mathsf{PK}^\star)$.

following theorem shows that security under each possible definition of an invert oracle implies IND-SCCAx security under a well-defined version of the strong decryption oracle.

Theorem 1 (IND-ICAx $\Rightarrow$ IND-SCCAx)**.** *Let $\mathcal{A}$ be an* IND-SCCAx *adversary against encryption scheme Π with respect to $\mathbf{SDec}_{\mathsf{U}',\mathsf{V}'}$ associated to $\mathbf{Inv}_{\mathsf{U},\mathsf{V}}$ as defined in Figure 5. Then there exists an* IND-ICAx *adversary $\mathcal{A}_1$ against Π with at least the same advantage as that of $\mathcal{A}$.*

The reduction is constructed by simulating the strong decryption oracle using both the standard decryption oracle (for queries under the challenge public key) and the invert oracle (for adversarially chosen-keys) available in the IND-ICAx game. The details are given in the full version of the paper. The interesting part of the proof is an argument showing that this simulation fits into the generic structure of **SDec** given in Figure 1 and, in particular, that the effect of the relation R passed to the strong decryption oracle can be emulated through a relation R' passed to the invert oracle. The intuition here is that the strong decryption oracle associated with a particular invert oracle maps the relation R that allows the adversary to restrict the set of interesting messages onto a relation R' that selects the set of secret keys that decrypt the queried ciphertext into the same set of interesting messages. Technically, the relation $\mathsf{R}'_{\mathsf{c},\mathsf{PK}}(\mathsf{SK}) := \mathsf{R}(\mathsf{Dec}(\mathsf{c}, \mathsf{SK}, \mathsf{PK}))$ allows us to simulate the oracle in Figure 5 with the correct distribution.

3 Extractor-based properties

The strong chosen-ciphertext security model that was recalled in Section 2 suggests that any secure scheme under this definition must ensure, by construction, that strong decryption queries are of no help to the adversary even when the

associated public keys are chosen adaptively. Plaintext awareness [5] formalises this intuition when a standard decryption oracle is used (and a public key is fixed). We therefore propose strong plaintext awareness as a natural extension for strong security models. This notion, however, is not the only way to render strong decryption oracles ineffective. An alternative approach is to require that any adversary which outputs a new valid public key must know a valid secret key for it. We refer to this property as secret key awareness. In the next two subsections we formalise these extractor-based notions precisely and demonstrate their adequacy for the security analysis of completely non-malleable schemes.

3.1 Strong plaintext awareness

We follow the approach adapted in [5] to define strong plaintext awareness in the standard model. We run an adversary in two possible environments and require that its behaviour does not change in any significant way. In the first world, the adversary has access to a real strong decryption oracle while in the second the oracle executes a polynomial-time extractor. Furthermore, in these environments, the adversary may obtain ciphertexts on "unknown-but-controlled" plaintexts though an encryption oracle, fed with messages produced by a plaintext creator. More formally, the SPAx advantage of an adversary, for $\mathsf{x} = 1, 2$, against encryption scheme Π with respect to plaintext creator $\mathcal{P}$ (mapping bit strings to messages), strong plaintext extractor $\mathcal{K}$, and distinguisher $\mathcal{D}$, is defined by

$$\mathbf{Adv}^{\mathsf{spax}}_{\Pi,\mathcal{P},\mathcal{D},\mathcal{K},\mathcal{A}}(\lambda) := \Pr\left[\mathsf{Dec\text{-}SPAx}^{\mathcal{A}}_{\Pi,\mathcal{P},\mathcal{D}}(\lambda) \Rightarrow \mathsf{T}\right] - \Pr\left[\mathsf{Ext\text{-}SPAx}^{\mathcal{A}}_{\Pi,\mathcal{P},\mathcal{D},\mathcal{K}}(\lambda) \Rightarrow \mathsf{T}\right]$$

where games $\mathsf{Dec\text{-}SPAx}$ and $\mathsf{Ext\text{-}SPAx}$ are shown in Figure 6. We say a scheme is SPAx if, for every PPT adversary $\mathcal{A}$, there exists an efficient strong plaintext extractor $\mathcal{K}$ such that, for all distinguishers[11] and plaintext creators, advantage is negligible.

The next theorem, which is proved in the full version of the paper, shows that the above formulation of strong plaintext-awareness, together with semantic security is enough to achieve strong chosen-ciphertext security.

Theorem 2 ($\mathsf{SPAx} \wedge \mathsf{IND\text{-}CPA} \Rightarrow \mathsf{IND\text{-}SCCAx}$)**.** *Fix a definition of* $\mathbf{SDec}_{\mathsf{U},\mathsf{V}}$ *and let* $\mathcal{A}$ *be an* $\mathsf{IND\text{-}SCCAx}$ *adversary against* Π *in the resulting model. Then there exist an* SPAx *ciphertext creator* $\mathcal{A}_1$*, an* $\mathsf{IND\text{-}CPA}$ *adversary* $\mathcal{A}_2$*, plaintext creators* $\mathcal{P}_0$*,* $\mathcal{P}_1$*, and distinguishers* $\mathcal{D}_0$*,* $\mathcal{D}_1$ *such that*

$$\mathbf{Adv}^{\mathsf{ind\text{-}sccax}}_{\Pi,\mathcal{A}}(\lambda) \leq \mathbf{Adv}^{\mathsf{spax}}_{\Pi,\mathcal{P}_0,\mathcal{D}_0,\mathcal{K},\mathcal{A}_1}(\lambda) + \mathbf{Adv}^{\mathsf{spax}}_{\Pi,\mathcal{P}_1,\mathcal{D}_1,\mathcal{K},\mathcal{A}_1}(\lambda) + \mathbf{Adv}^{\mathsf{ind\text{-}cpa}}_{\Pi,\mathcal{A}_2}(\lambda),$$

where $\mathcal{K}$ *is the plaintext extractor for* $\mathcal{A}_1$ *implied by the* SPAx *property of* Π*.*

As we mentioned in the introduction, the equivalence between indistinguishability under strong chosen-ciphertext security and simulation-based complete non-malleability is established for *assisted* simulators [2]. The next theorem shows that using strong plaintext awareness one can strengthen this result to non-assisted simulators[12].

[11] If unbounded distinguishers are allowed, we get statistical strong plaintext awareness.

[12] Due to space constraints, we refer the interested reader to [2] for the SNM definitions.

Game $\mathsf{Dec\text{-}SPAx}_{\Pi,\mathcal{P},\mathcal{D}}(\lambda)$

proc. Initialize(λ):
$\mathsf{I} \leftarrow_\$ \mathsf{Setup}(1^\lambda)$
$(\mathsf{SK}^\star, \mathsf{PK}^\star) \leftarrow_\$ \mathsf{Gen}()$
Choose coins $\mathsf{Rnd}[\mathcal{A}]$ for $\mathcal{A}$
$\mathsf{st}[\mathcal{P}] \leftarrow \epsilon$; $\mathsf{List} \leftarrow []$; $\mathsf{st}[\mathsf{V}] \leftarrow \mathsf{st}_0$
Return $(\mathsf{I}, \mathsf{PK}^\star, \mathsf{Rnd}[\mathcal{A}])$

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

proc. Enc(Q):
$(\mathsf{m}, \mathsf{st}[\mathcal{P}]) \leftarrow_\$ \mathcal{P}(Q, \mathsf{st}[\mathcal{P}])$
$\mathsf{c} \leftarrow_\$ \mathsf{Enc}(\mathsf{m}, \mathsf{PK}^\star)$
$\mathsf{List} \leftarrow (\mathsf{c}, \mathsf{PK}^\star) : \mathsf{List}$
Return c

proc. Finalize(x):
Return $\mathcal{D}(x)$

Game $\mathsf{Ext\text{-}SPAx}_{\Pi,\mathcal{P},\mathcal{D},\mathcal{K}}(\lambda)$

proc. Initialize(λ):
$\mathsf{I} \leftarrow_\$ \mathsf{Setup}(1^\lambda)$
$(\mathsf{SK}^\star, \mathsf{PK}^\star) \leftarrow_\$ \mathsf{Gen}()$
Choose coins $\mathsf{Rnd}[\mathcal{A}]$ for $\mathcal{A}$; $\mathsf{List} \leftarrow []$
$\mathsf{st}[\mathcal{P}] \leftarrow \epsilon$; $\mathsf{st}[\mathcal{K}] \leftarrow (\mathsf{I}, \mathsf{PK}^\star, \mathsf{Rnd}[\mathcal{A}])$
Return $(\mathsf{I}, \mathsf{PK}^\star, \mathsf{Rnd}[\mathcal{A}])$

proc. SDec$(\mathsf{c}, \mathsf{PK}, \mathsf{R})$:
$(\mathsf{m}, \mathsf{st}[\mathcal{K}]) \leftarrow_\$ \mathcal{K}(\mathsf{c}, \mathsf{PK}, \mathsf{R}, \mathsf{List}, \mathsf{st}[\mathcal{K}])$
Return m

proc. Enc(Q):
$(\mathsf{m}, \mathsf{st}[\mathcal{P}]) \leftarrow_\$ \mathcal{P}(Q, \mathsf{st}[\mathcal{P}])$
$\mathsf{c} \leftarrow_\$ \mathsf{Enc}(\mathsf{m}, \mathsf{PK}^\star)$
$\mathsf{List} \leftarrow (\mathsf{c}, \mathsf{PK}^\star) : \mathsf{List}$
Return c

proc. Finalize(x):
Return $\mathcal{D}(x)$

Fig. 6: The Dec-SPAx and Ext-SPAx games for defining the strong plaintext-awareness of encryption scheme Π. An adversary $\mathcal{A}$ is legitimate if: 1) R is polynomial-time and if $\mathsf{x} = 1$ it never calls **Enc**; and 2) It never calls **SDec** with a tuple $(\mathsf{c}, \mathsf{PK})$ in List.

Theorem 3 (SPAx $\wedge$ SNM-CPA $\Rightarrow$ Non-Assisted SNM-SCCAx). *Fix a definition of* $\mathbf{SDec}_{\mathsf{U},\mathsf{V}}$ *and let* $\mathcal{A}$ *be a* Real-SNM-SCCAx *adversary against* Π*. Then there exist an* SPAx *ciphertext creator* $\mathcal{A}_1$*, a* Real-SNM-CPA *adversary* $\mathcal{A}_2$*, a plaintext creator* $\mathcal{P}$*, a distinguisher* $\mathcal{D}$*, and a (non-assisted) simulator* $\mathcal{S}$ *such that for all* R

$$\mathbf{Adv}^{\mathsf{snm\text{-}sccax}}_{\Pi,\mathsf{R},\mathcal{S},\mathcal{A}}(\lambda) \leq \mathbf{Adv}^{\mathsf{spax}}_{\Pi,\mathcal{P},\mathcal{D},\mathcal{K},\mathcal{A}_1}(\lambda) + \mathbf{Adv}^{\mathsf{snm\text{-}cpa}}_{\Pi,\mathsf{R},\mathcal{S}_2,\mathcal{A}_2}(\lambda),$$

where $\mathcal{K}$ *is the strong plaintext extractor for* $\mathcal{A}_1$ *implied by the* SPAx *property of* Π *and* $\mathcal{S}_2 = \mathcal{S}$ *is the simulator for* $\mathcal{A}_2$ *implied by the* SNM-CPA *security of* Π*.*

The proof of this theorem, included in the full version of the paper, proceeds in a different way than that in [10] for standard security models. There, a new key-pair is generated to enable the simulator to answer decryption queries, whereas in our proof this is not necessary. As pointed out by Pass et al. [22], the proof in [10] relies on the existence of an algorithm for efficiently encrypting all possible outputs of decryption, including special symbol $\perp$. Plaintext awareness in general does not imply that this must be the case, and so our results extend the results in [22]: schemes that do not have the property identified in [22] may still be plaintext aware, and therefore achieve simulation-based non-malleability for non-assisted simulators. However, as shown in [11, Theorem 2], if an encryption scheme is PA2 and has an infinite message space, then it is not OW-CPA. This

also applies to strong plaintext awareness, and hence no scheme with an infinite message space will be captured by the above theorem.

REMARK. In the above theorem we do not need to restrict the class of relations, in particular to those which are independent of the challenge public key (called lacking relations in [26]). This means that through strong plaintext awareness one can improve on the results in [26], where this security level can only be achieved at the cost of relation being independent of the common parameters.

REMARK. Using the techniques introduced by Dent [16], the scheme in [2] might satisfy strong plaintext awareness under an appropriate (bilinear) Diffie-Hellman knowledge assumptions. We leave this and constructing a strongly plaintext-aware scheme in the standard model as an open problem.

3.2 Secret key awareness

We now formalise secret key awareness as an alternative route to achieve strong security guarantees. We take a similar approach to plaintext awareness and give an adversary access to an oracle which is either a real *inversion* oracle (as defined in Section 2) or one which uses a polynomial-time secret key extractor. Once again, our requirement is that the behaviour of the adversary is computationally indistinguishable in the two environments. We also provide the adversary with a decryption and a controlled encryption oracle which model the extra auxiliary information that might be useful in producing a new public key. Formally, the SKAx advantage of an adversary $\mathcal{A}$ against encryption scheme Π with respect to secret key extractor $\mathcal{K}$, plaintext creator $\mathcal{P}$, and distinguisher $\mathcal{D}$ is defined by

$$\mathbf{Adv}^{\mathsf{skax}}_{\Pi,\mathcal{P},\mathcal{D},\mathcal{K},\mathcal{A}}(\lambda) := \Pr\left[\mathsf{Inv\text{-}SKAx}^{\mathcal{A}}_{\Pi,\mathcal{P},\mathcal{D}}(\lambda) \Rightarrow \mathsf{T}\right] - \Pr\left[\mathsf{Ext\text{-}SKAx}^{\mathcal{A}}_{\Pi,\mathcal{P},\mathcal{D},\mathcal{K}}(\lambda) \Rightarrow \mathsf{T}\right]$$

where games Inv-SKA and Ext-SKA are shown in Figure 7. We say a scheme is SKAx secure if, for every PPT adversary $\mathcal{A}$, there exists an efficient secret key extractor $\mathcal{K}$ such that, for all distinguishers[13] and plaintext creators, advantage is negligible.

We are now ready to state the main theorem of this section, which permits concluding that secret key awareness combined with IND-CCA2 is strong enough to guarantee IND-SCCA2 security. The proof is analogous to that of Theorem 2 and is included in the full version of the paper.

Theorem 4 (SKAx $\wedge$ IND-CCAx $\Rightarrow$ IND-ICAx)**.** *Fix a definition of* $\mathbf{Inv}_{\mathsf{U},\mathsf{V}}$ *and let* $\mathcal{A}$ *be an* IND-ICAx *adversary against* Π*. Then, there exist an* SKAx *public key creator* $\mathcal{A}_1$*, an* IND-CCAx *adversary* $\mathcal{A}_2$*, plaintext creators* $\mathcal{P}_0$*,* $\mathcal{P}_1$*, and distinguishers* $\mathcal{D}_0$*,* $\mathcal{D}_1$ *such that*

$$\mathbf{Adv}^{\mathsf{ind\text{-}icax}}_{\Pi,\mathcal{A}}(\lambda) \leq \mathbf{Adv}^{\mathsf{skax}}_{\Pi,\mathcal{P}_0,\mathcal{D}_0,\mathcal{K},\mathcal{A}_1}(\lambda) + \mathbf{Adv}^{\mathsf{skax}}_{\Pi,\mathcal{P}_1,\mathcal{D}_1,\mathcal{K},\mathcal{A}_1}(\lambda) + \mathbf{Adv}^{\mathsf{ind\text{-}ccax}}_{\Pi,\mathcal{A}_2}(\lambda),$$

where $\mathcal{K}$ *is the secret key extractor for* $\mathcal{A}_1$ *implied by the* SKAx *property of* Π*.*

[13] If unbounded distinguishers are allowed, we get statistical secret key awareness.

Game $\mathsf{Inv\text{-}SKAx}_{\Pi,\mathcal{P},\mathcal{D}}(\lambda)$

proc. Initialize(λ):
$\mathsf{I} \leftarrow_\$ \mathsf{Setup}(1^\lambda)$
$(\mathsf{SK}^\star, \mathsf{PK}^\star) \leftarrow_\$ \mathsf{Gen}()$
Choose coins $\mathsf{Rnd}[\mathcal{A}]$ for $\mathcal{A}$
$\mathsf{st}[\mathcal{P}] \leftarrow \epsilon$; $\mathsf{st}[\mathsf{V}] \leftarrow \mathsf{st}_0$
$\mathsf{List} \leftarrow []$
Return $(\mathsf{I}, \mathsf{PK}^\star, \mathsf{Rnd}[\mathcal{A}])$

proc. Dec(c):
$\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{c}, \mathsf{SK}^\star, \mathsf{PK}^\star)$
Return m

proc. Enc(Q):
$(\mathsf{m}, \mathsf{st}[\mathcal{P}]) \leftarrow_\$ \mathcal{P}(Q, \mathsf{st}[\mathcal{P}])$
$\mathsf{c} \leftarrow_\$ \mathsf{Enc}(\mathsf{m}, \mathsf{PK}^\star)$
$\mathsf{List} \leftarrow (\mathsf{c}, \mathsf{PK}^\star) : \mathsf{List}$
Return c

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

proc. Finalize(x):
Return $\mathcal{D}(x)$

Game $\mathsf{Ext\text{-}SKAx}_{\Pi,\mathcal{P},\mathcal{D},\mathcal{K}}(\lambda)$

proc. Initialize(λ):
$\mathsf{I} \leftarrow_\$ \mathsf{Setup}(1^\lambda)$
$(\mathsf{SK}^\star, \mathsf{PK}^\star) \leftarrow_\$ \mathsf{Gen}()$
Choose coins $\mathsf{Rnd}[\mathcal{A}]$ for $\mathcal{A}$
$\mathsf{st}[\mathcal{K}] \leftarrow (\mathsf{I}, \mathsf{PK}^\star, \mathsf{Rnd}[\mathcal{A}])$
$\mathsf{st}[\mathcal{P}] \leftarrow \epsilon$; $\mathsf{List} \leftarrow []$; $\mathsf{List}' \leftarrow []$
Return $(\mathsf{I}, \mathsf{PK}^\star, \mathsf{Rnd}[\mathcal{A}])$

proc. Dec(c):
$\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{c}, \mathsf{SK}^\star, \mathsf{PK}^\star)$
$\mathsf{List}' \leftarrow \mathsf{m} : \mathsf{List}'$
Return m

proc. Enc(Q):
$(\mathsf{m}, \mathsf{st}[\mathcal{P}]) \leftarrow_\$ \mathcal{P}(Q, \mathsf{st}[\mathcal{P}])$
$\mathsf{c} \leftarrow_\$ \mathsf{Enc}(\mathsf{m}, \mathsf{PK}^\star)$
$\mathsf{List} \leftarrow (\mathsf{c}, \mathsf{PK}^\star) : \mathsf{List}$
Return c

proc. Inv$(\mathsf{PK}, \mathsf{R})$:
$(\mathsf{SK}, \mathsf{st}[\mathcal{K}]) \leftarrow_\$ \mathcal{K}(\mathsf{PK}, \mathsf{R}, \mathsf{List}, \mathsf{List}', \mathsf{st}[\mathcal{K}])$
Return SK

proc. Finalize(x):
Return $\mathcal{D}(x)$

Fig. 7: The Inv-SKAx and Ext-SKAx games for defining secret key awareness. An adversary $\mathcal{A}$ is legitimate if: 1) R is polynomial-time and, if $\mathsf{x} = 0$ it never calls **Dec** or **Enc** and if $\mathsf{x} = 1$ it never calls **Enc**; 2) It never queries $\mathsf{PK}^\star$ to **Inv**; and 3) It never calls **Dec** with a ciphertext c such that $(\mathsf{c}, \mathsf{PK}^\star) \in \mathsf{List}$.

To further justify the definition of secret key awareness, we show that it can be used to achieve strong plaintext awareness. The next theorem, proved in in the full version of the paper, states that secret key awareness combined with standard plaintext awareness gives rise to strong plaintext awareness.

Theorem 5 ($\mathsf{SKAx} \wedge \mathsf{PAx} \Rightarrow \mathsf{SPAx}$)**.** *Fix a definition of* $\mathbf{Inv}_{\mathsf{U},\mathsf{V}}$ *and let* $\mathcal{A}$ *be an* SPAx *ciphertext creator against* Π*, with respect to the* $\mathbf{SDec}_{\mathsf{U}',\mathsf{V}'}$ *procedure associated to* $\mathbf{Inv}_{\mathsf{U},\mathsf{V}}$ *as defined in Figure 5. Then there exists an* SKAx *public key creator* $\mathcal{A}_1$*, a* PAx *ciphertext creator* $\mathcal{A}_2$*, and an* SPAx *plaintext extractor* $\mathcal{K}$ *such that for any plaintext creator* $\mathcal{P}$*, and any distinguisher* $\mathcal{D}$ *we have*

$$\mathbf{Adv}^{\mathsf{spax}}_{\Pi,\mathcal{P},\mathcal{D},\mathcal{K},\mathcal{A}}(\lambda) \leq \mathbf{Adv}^{\mathsf{skax}}_{\Pi,\mathcal{P},\mathcal{D},\mathcal{K}_1\mathcal{A}_1}(\lambda) + \mathbf{Adv}^{\mathsf{pax}}_{\Pi,\mathcal{P},\mathcal{D},\mathcal{K}_2,\mathcal{A}_2}(\lambda),$$

where $\mathcal{K}_1$ *is the a secret key extractor for* $\mathcal{A}_1$ *implied by the* SKAx *property of* Π*, and* $\mathcal{K}_2$ *is the plaintext extractor for* $\mathcal{A}_2$ *implied by the* PAx *property of* Π*.*

The intuition behind this theorem is the following. Secret key awareness ensures that a strong plaintext awareness adversary cannot come up with a ciphertext under a *new* public key, for which it does not know the underlying message (as

it must know the decryption key). However, no such guarantee is provided for the *challenge* public key, and this justifies the plaintext awareness requirement.

REMARK. An extra feature that comes with secret key awareness is the ability to open ciphertexts via the secret key[14]. In other words, one can convert a non-malleability simulator that only returns $(\mathbf{PK}^\star, \mathbf{c}^\star)$ to another one[15] which also outputs the corresponding opening $(\mathbf{SK}^\star, \mathbf{m}^\star)$. This means that the output of the simulator can indeed be seen as a de-commitment. The same observation does not apply to strong plaintext awareness, as this notion does not guarantee the knowledge of the *randomness* used in encryption.

4 Secret key aware schemes

4.1 Generic construction with a random oracle

We have defined strong plaintext and secret key awareness in the standard model, but the definitions can be adapted to the random oracle model [6] in the natural way[16]. Interestingly, in the random oracle model, there is a simple transformation that turns any encryption scheme into one which is secret key aware without any loss in security: one just changes the key-generation algorithm by attaching the hash of the key-pair to the public key. More formally, the transformed set-up algorithm Setup' is identical to Setup except that it also specifies a new independent hash function H (i.e. one which is not used by the scheme), which will be modelled as a random oracle in the security analysis. The remaining algorithms are shown in Figure 8.

proc. $\mathsf{Gen}'(\mathsf{I})$:	**proc.** $\mathsf{Enc}'(\mathsf{m}, \mathsf{PK}')$:	**proc.** $\mathsf{Dec}'(\mathsf{c}, \mathsf{SK}', \mathsf{PK}')$:
$(\mathsf{SK}, \mathsf{PK}) \leftarrow_\$ \mathsf{Gen}()$	$(\mathsf{PK}, h) \leftarrow \mathsf{PK}'$	$(\mathsf{PK}, h) \leftarrow \mathsf{PK}'$; $\mathsf{SK} \leftarrow \mathsf{SK}'$
$\mathsf{PK}' \leftarrow (\mathsf{PK}, \mathsf{H}(\mathsf{SK}, \mathsf{PK}))$	$\mathsf{c} \leftarrow_\$ \mathsf{Enc}(\mathsf{m}, \mathsf{PK})$	If $h \neq \mathsf{H}(\mathsf{SK}, \mathsf{PK})$ Return $\perp$
Return $(\mathsf{SK}, \mathsf{PK}')$	Return c	Return $\mathsf{Dec}(\mathsf{c}, \mathsf{SK}, \mathsf{PK})$

Fig. 8: Generic transformation to a secret-key-aware scheme Π' in the ROM.

It can be easily shown that the scheme obtained through the above transformation is secret key aware, as long as the range of H is large enough to ensure that the transformed scheme has only one valid secret key for each valid public key with overwhelming probability. The idea behind the proof is that adversarially created public keys will be invalid with high probability, unless the random

[14] Although not considered in this paper, the secret key awareness property can also be used in composition theorems where direct access to secret keys is required. This could be useful, for example, in signcryption.

[15] This new simulator must be given the secret key for the challenge public key, which is consistent with the notion of a non-malleable commitment.

[16] Furthermore, the standard stronger definition requiring the existence of a universal extractor may also be easily formulated [4].

oracle has already been queried on the corresponding secret key. In this case the (unique) secret key can be recovered using the extractability property of the random oracle. Note that simply attaching $\mathsf{H}(\mathsf{SK})$ is not enough, as extraction will fail in case the challenge public key is malleable. See the details in the full version of the paper. From this result, together with Theorems 1 and 4, we can deduce that if Π is IND-CCAx-secure then Π' is IND-SCCAx-secure.

Remark. The previous generic construction can be applied to RSA-OAEP. In the random oracle model, this new version of RSA-OAEP is SKA2 because of the modified keys, and it preserves the original PA2 and IND-CPA security of RSA-OAEP. It follows that this scheme is completely non-malleable with respect to non-assisted simulators. Note that we do not need to restrict the adversary to querying only valid public keys, as is the case in [18], since the secret key extractor implied by the SKA2 property will permit detecting such invalid queries.

4.2 Towards secret-key-aware schemes without random oracles

We present two approaches to constructing secret key aware schemes without random oracles. Both are intended as stepping stones towards achieving the strongest forms of secret key awareness. We first introduce a new knowledge-based assumption and use it to construct a concrete scheme, which is "weakly" secret key aware. Then we propose a generic construction inspired by techniques used in encryption schemes with key escrow [12]. We leave it as an interesting open problem to instantiate this generic construction or show its unrealisability.

The knowledge of factor assumption. We take advantage of the fact that k-bit integers of the form $N = P^2Q$ have a negligible density in the set of all k-bit integers (note that this is *not* the case for the integers of the form PQ), and we postulate that the only way to generate such integers is to start with the two prime factors and calculate N. This assumption is similar to Diffie-Hellman knowledge type assumptions [5] where one exploits the sparse image of the $r \mapsto (g^r, (g^a)^r)$ map. Our assumption, however, has the extra property of being "non-malleable" in the sense that there does not seem to be any way to use the knowledge of one (or in fact many) integers of this form to find an alternative way to construct new ones. Diffie-Hellman tuples on the other hand are malleable. For concreteness, we now present a formal definition of our *knowledge of factorisation assumptions*.

Take $\mathcal{G}_e$ to be the algorithm that, for a given value of the security parameter, generates numbers of the form P^2Q, with P and Q random primes of the appropriate size such that[17] $\gcd(e, \varphi(P^{\star 2}Q^{\star})) = 1$. Figure 9 depicts the KFAx game for $\mathsf{x} = 0, 1, 2$, where an adversary is required to construct a new integer of the same form *without knowing* the factorization. We define the KFAx advantage of an adversary against $\mathcal{G}_e$, with respect to knowledge extractor $\mathcal{K}$ as:

$$\mathbf{Adv}^{\mathsf{kfax}}_{\mathcal{G}_e,\mathcal{K},\ell,\mathcal{A}}(\lambda) := \Pr[\mathsf{KFAx}^{\mathcal{A}}_{\mathcal{G}_e,\mathcal{K},\ell}(\lambda) \Rightarrow \mathsf{T}].$$

[17] We use φ to denote Euler's totient function.

The KFAx assumption states that, for every PPT adversary, there exists an efficient knowledge extractor such that advantage is negligible.

Game $\mathsf{KFAx}_{\mathcal{G}_e,\mathcal{K},\ell}(\lambda)$

proc. Initialize(λ):
$(P^\star, Q^\star) \leftarrow_\$ \mathcal{G}_e(1^\lambda)$; $N^\star \leftarrow P^{\star 2}Q^\star$
$d \leftarrow 1/e \pmod{\varphi(N^\star)}$; $\mathsf{List} \leftarrow []$
Choose $\mathsf{Rnd}[\mathcal{A}]$ for $\mathcal{A}$; $\mathsf{Flag} \leftarrow \mathsf{F}$
$\mathsf{st}[\mathcal{K}] \leftarrow (N^\star, \mathsf{Rnd}[\mathcal{A}])$
Return $(N^\star, \mathsf{Rnd}[\mathcal{A}])$

proc. Root(y):
$t \leftarrow y^d \pmod{N^*}$; $(x, x') \leftarrow t$
$\mathsf{List} \leftarrow (x, y) : \mathsf{List}$
Return x

proc. Fact(N):
$((P, Q), \mathsf{st}[\mathcal{K}]) \leftarrow_\$ \mathcal{K}(N, \mathsf{List}, \mathsf{st}[\mathcal{K}])$
If $P^2Q = N \wedge P \neq 1$ Return (P, Q)
If $\exists P', Q'$ s.t. $P'^2Q' = N$
  Set $\mathsf{Flag} \leftarrow \mathsf{T}$
Return $(\perp, \perp)$

proc. Finalize():
Return Flag

Fig. 9: Game defining the knowledge of factor assumption. An adversary $\mathcal{A}$ is legitimate if: 1) If $\mathsf{x} = 0$ it queries **Fact** once, and if $\mathsf{x} = 0, 1$ it does not query **Root**; and 2) It never queries **Fact** on $N^\star$. **Root** returns the first ℓ bits of t, i.e. $|x| = \ell$.

RSA-BASED SECRET-KEY-AWARE SCHEMES. The KFA1 assumption immediately implies that an RSA-based scheme with P^2Q modulus [23] is SKA1. Random padding before encryption allows one to construct an IND-CPA secure scheme. In order to extend this to IND-CCA1 security, a non-adaptive **Root** oracle is added to the RSA problem. As a result, we arrive at an IND-SCCA1 secure encryption scheme without random oracles and with no setup assumptions. We refer the reader to the full version of the paper for the details on this concrete scheme and a proof of the secret key awareness property.

The only factorisation/RSA-based IND-CCA2 secure encryption scheme in the standard model is a recent scheme of Hofheinz and Kiltz [19]. This scheme, with appropriately modified public keys is a candidate for achieving IND-SCCA2 security under the KFAx assumptions through secret key awareness. Such a construction would also admit a (non-black-box) non-assisted complete non-malleability simulator *with no set-up assumptions*. This would solve the open problem [18] of constructing an encryption scheme that is suitable for the implementation of non-malleable commitment schemes in the plain model.

REMARK. The KFAx assumptions lead to a construction of extractable one-way functions analogous to that obtained using the knowledge-of-exponent assumptions [13, 14]. However, we can use even the weakest form KFA0 to go beyond. Indeed, this assumption states that one cannot come up with an N of the correct form, even if *given another* integer of this form as auxiliary information. Under this assumption the function $f(P, Q) = P^2Q$, where P and Q are k-bit primes, is an extractable one-way function with *dependent* auxiliary information.

REMARK. We note that knowledge assumptions seem necessary to establish plaintext and secret key awareness. It remains an open problem to construct

plaintext-aware schemes without relying on extractor-based assumptions such as Diffie-Hellman Knowledge. NIZK techniques do not provide an answer to this problem, as extractors should work with the *provided* common reference string.

A generic technique based on schemes with key escrow. Consider a public-key encryption scheme Π where the key-generation procedure first generates a secret key in the appropriate range, and then encrypts it under an auxiliary encryption scheme[18] Π_{PK}. Then, the plaintext awareness property of Π_{PK} naturally maps to (a weak form of) secret key awareness for Π. The caveat to this design technique is that plaintext awareness is an all-or-nothing notion [24], which could render this construction unrealisable. Indeed, full plaintext awareness in key-generation would imply a form of indistinguishability for secret keys that is contradicted by the correctness of the scheme[19]. However, by restricting the plaintext awareness property of Π_{PK} to the class of plaintext creators that return a random message from the message space, we can show that Π achieves $\mathsf{SKA0}$ if the auxiliary scheme Π_{PK} is $\mathsf{PA2}$.

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. Research was sponsored by US Army Research laboratory and the UK Ministry of Defence and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the US Army Research Laboratory, the U.S. Government, the UK Ministry of Defense, or the UK Government. The US and UK Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

References

1. S. S. Al-Riyami and K. G. Paterson. Certificateless public key cryptography. In C.-S. Laih, editor, *ASIACRYPT*, vol. 2894 of *LNCS*, pp. 452–473. Springer, 2003.
2. M. Barbosa and P. Farshim. Relations among notions of complete non-malleability: Indistinguishability characterisation and efficient construction without random oracles. Pre-print (accepted for ACISP 2010), 2010.
3. M. Bellare, A. Boldyreva, and S. Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In B. Preneel, editor, *EUROCRYPT*, vol. 1807 of *LNCS*, pp. 259–274. Springer, 2000.
4. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In Krawczyk [20].
5. M. Bellare and A. Palacio. Towards plaintext-aware public-key encryption without random oracles. In P. J. Lee, editor, *ASIACRYPT*, vol. 3329 of *LNCS*, pp. 48–62. Springer, 2004.

[18] This means, of course, that a public key for the auxiliary scheme Π_{PK} must be fixed in the global parameters for Π.

[19] Given a public key and two secret keys one can check which secret key is valid through the encryption and decryption algorithms.

6. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM Conference on Computer and Communications Security*, pp. 62–73, 1993.
7. M. Bellare and P. Rogaway. Optimal asymmetric encryption. In A. D. Santis, editor, *EUROCRYPT*, vol. 950 of *LNCS*, pp. 92–111. Springer, 1994.
8. M. Bellare and P. Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In Vaudenay [25], pp. 409–426.
9. M. Bellare and A. Sahai. Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization. In M. J. Wiener, editor, *CRYPTO*, vol. 1666 of *LNCS*, pp. 519–536. Springer, 1999.
10. M. Bellare and A. Sahai. 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`.
11. J. Birkett and A. W. Dent. Relations among notions of plaintext awareness. In Cramer [15], pp. 47–64.
12. J. Brown, J. M. G. Nieto, and C. Boyd. Efficient and secure self-escrowed public-key infrastructures. In *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pp. 284–294, New York, NY, USA, 2007. ACM.
13. R. Canetti and R. R. Dakdouk. Extractable perfectly one-way functions. In L. Aceto, I. Damgård, L. A. Goldberg, M. M. Halldórsson, A. Ingólfsdóttir, and I. Walukiewicz, editors, *ICALP*, vol. 5126 of *LNCS*, pp. 449–460. Springer, 2008.
14. R. Canetti and R. R. Dakdouk. Towards a theory of extractable functions. In O. Reingold, editor, *TCC*, vol. 5444 of *LNCS*. Springer, 2009.
15. R. Cramer, editor. *Public Key Cryptography - PKC 2008*, vol. 4939 of *LNCS*. Springer, 2008.
16. A. W. Dent. The cramer-shoup encryption scheme is plaintext aware in the standard model. In Vaudenay [25], pp. 289–307.
17. D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography (extended abstract). In *STOC*, pp. 542–552. ACM, 1991.
18. M. Fischlin. Completely non-malleable schemes. In L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, editors, *ICALP*, vol. 3580 of *LNCS*, pp. 779–790. Springer, 2005.
19. D. Hofheinz and E. Kiltz. Practical chosen ciphertext secure encryption from factoring. In A. Joux, editor, *EUROCRYPT*, vol. 5479 of *LNCS*, pages 313–332. Springer, 2009.
20. H. Krawczyk, editor. *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, vol. 1462 of *LNCS*. Springer, 1998.
21. O. Pandey, R. Pass, and V. Vaikuntanathan. Adaptive one-way functions and applications. In D. Wagner, editor, *CRYPTO*, vol. 5157 of *LNCS*, pages 57–74. Springer, 2008.
22. R. Pass, A. Shelat, and V. Vaikuntanathan. Relations among notions of non-malleability for encryption. In *ASIACRYPT*, pp. 519–535, 2007.
23. T. Takagi. Fast RSA-type cryptosystem modulo $p^k q$. In Krawczyk [20].
24. I. Teranishi and W. Ogata. Relationship between standard model plaintext awareness and message hiding. *IEICE Transactions*, 91-A(1):244–261, 2008.
25. S. Vaudenay, editor. *Advances in Cryptology - EUROCRYPT 2006*, vol. 4004 of *LNCS*. Springer, 2006.
26. C. Ventre and I. Visconti. Completely non-malleable encryption revisited. In Cramer [15], pp. 65–84.