# Completely Non-Malleable Encryption Revisited

Carmine Ventre and Ivan Visconti

Dipartimento di Informatica ed Applicazioni
Università di Salerno, 84084 Fisciano (SA), ITALY
{ventre, visconti}@dia.unisa.it

**Abstract.** Several security notions for public-key encryption schemes have been proposed so far, in particular considering the powerful adversary that can play a so called "man-in-the-middle" attack.
In this paper we extend the notion of completely non-malleable encryption introduced in [Fischlin, ICALP 05]. This notion immunizes a scheme from adversaries that can generate related ciphertexts under new public keys. This notion is motivated by its powerful features when encryption schemes are used as subprotocols. While in [Fischlin, ICALP 05] the only notion of *simulation-based* completely non-malleable encryption with respect to CCA2 adversaries was given, we present new *game-based* definitions for completely non-malleable encryption that follow the standard separations among NM-CPA, NM-CCA1 and NM-CCA2 security given in [Bellare et al., CRYPTO 98]. This is motivated by the fact that in several cases, the simplest notion we introduce (i.e., NM-CPA*) in several cases suffices for the main application that motivated the introduction of the notion of NM-CCA2* security, i.e., the design of non-malleable commitment schemes. Further the game-based definition of NM-CPA* security actually implies the simulation-based one.
We then focus on constructing encryption schemes that satisfy these strong security notions and show: 1) an NM-CCA2* secure encryption scheme in the shared random string model; 2) an NM-CCA2* secure encryption scheme in the plain model; for this second result, we use interaction and non-black-box techniques to overcome an impossibility result.
Our results clarify the importance of these stronger notions of encryption schemes and show how to construct them without requiring random oracles.

## 1 Introduction

The study of the relations among security notions for public-key encryption is a central question in Cryptography. Several notions for encryption schemes have been defined in order to construct schemes that are secure against strong adversaries. One of the most general and accepted concept is that of non-malleability formalized with the notion of adaptive chosen ciphertext security (shortly referred to as CCA2). Intuitively, a man-in-the-middle adversary should not be able given a public key `pk` and a ciphertext $c$, relative to a message $m$ sampled

from a distribution of its choice, to output a relation $\mathtt{R}$ and a ciphertext $c'$ whose plaintext $m'$ is related through $\mathtt{R}$ with $m$. This task has to be hard even in case that the adversary has access to a decryption oracle. Important constructions (see [1,2]) as well as relations among security notions [3] currently clarify the power of CCA2 security with respect to the weaker notions of CCA1 (where the decryption oracles can be accessed only before the challenge is received) and CPA (where no access to a decryption oracle is possible) security.

Recently, Fischlin presented in [4] a new security notion for public-key encryption, referred to as complete non-malleability. This notion, requires that non-malleability has to be preserved even in case that the man-in-the-middle adversary can also choose a new public key (that thus could be related to the original one). The goal of the adversary is to compute a ciphertext (under the new public key) that corresponds to a plaintext that is related to the original plaintext. Notice that in this more general case the relation considers also the new public key.

The main motivation for considering this new notion is that encryption schemes are often used as building blocks for larger protocols and in [4] it is stressed that completely non-malleable security has much more applications than the standard non-complete security notions for public-key encryption schemes. In particular, in [4] Fischlin discusses possible approaches for the design of non-malleable commitment schemes on top of completely non-malleable encryption schemes.

This new security notion is strong but unfortunately also impossible to achieve in the standard model when non-interactive encryption with simulation-based black-box security is considered (see [4]). Constructions are instead possible [4] in the random oracle model.

### 1.1 Our Results

In this paper we revisit the study of the concept of completely non-malleable encryption schemes initiated in [4]. First we notice that the idea behind complete non-malleability can be extended also to the notions of CPA and CCA1 security, while the original notion of Fischlin only considered CCA2 security. In order to motivate these new definitions, we present separating examples (see Theorem 1) showing that such notions seem to capture more than what the older non-complete definitions actually do. We will refer to these new notions of security for encryption schemes as NM-CPA$^*$, NM-CCA1$^*$ and NM-CCA2$^*$ respectively.

The importance of the new definitions (and thus of our study of the relations among the different notions) follows from the following observation. The main motivation given in [4] for NM-CCA2* security concerned the possibility of constructing non-malleable commitments on top of NM-CCA2* secure encryption schemes[1]. This could be done (under some additional assumption that however

[1] Additionally, in [4] similar powerful attacks are discussed with respect to signature schemes.

we do not stress here) by assuming that the committer selects a public key, encrypts the message and sends the encryption as commitment. Then the opening is performed by sending the randomness used for the encryption. Obviously a man-in-the-middle could select a related public key in order to compute a related encryption and thus a related commitment. NM-CCA2* security should guarantee the failure of the above attack of the man-in-the-middle.

We observe that the role of a decryption oracle is not clear in this context and in particular could not be required in many applications. Indeed, for non-malleable commitments, the man-in-the-middle $\mathcal{A}$ does not have access to oracles that can open challenge commitments, therefore the NM-CCA2* security requirement in some cases can be relaxed to NM-CPA* security. Therefore, in this work we consider the possible variants for complete non-malleability, considering also the potential presences of a decryption oracle.

We stress that while the definitions of [4] follow the simulation-based approach already used in [1], we give definitions that follow the game-based approach of [3]. The choice of this formulation follows from the fact that the game-based definition of NM-CPA* security (our motivating notion) implies its simulation-based variant. Thus, we give a simpler formulation for NM-CPA* security and also show that for a large set of relations, the game-based formulations of NM-CCA1* and NM-CCA2* security imply the simulation-based ones. This implication shows that the impossibility result proved by Fischlin [4] about the design (in the plain model) of public-key encryption schemes that are completely non-malleable can be adapted to the game-based version of the definition of NM-CCA2* security.

We next focus on feasibility results with the goal of overcoming known impossibility results as well as improving the assumptions needed by previous constructions.

1. We first consider the shared random string model. By starting from any IND-CPA secure encryption scheme and by using the non-malleable NIZK proof of knowledge of [5] we obtain an NM-CCA2* secure encryption schemes in the shared random string model. In this construction we enrich the known technique due to [2] in which every ciphertext of the underlying IND-CPA secure encryption scheme is augmented with a NIZK proof of knowledge of the corresponding plaintext. In our construction we also need a proof that the new public key is indeed valid (i.e., the output of the honest key generation algorithm of the underlying encryption scheme). We stress that such a construction improves the assumption (i.e., the existence of random oracles) needed by Fischlin's constructions. Moreover we show that by using robust NIZK [5] (thus strengthening the non-malleable NIZK proof of knowledge), the construction also satisfies the simulation-based notion of NM-CCA2* security.
2. We show a construction of an interactive non-black-box completely non-malleable encryption scheme that works by assuming that oracle queries are asked sequentially. We stress that even this second construction satisfies the simulation-based notion of NM-CCA2* security. Since the impossibility re-

sults proved by Fischlin in [4] only concerned black-box adversaries and non-interactive encryption, the possibility of further improving our construction by relaxing either the non-black-box requirement or the interactiveness of the encryption or the concurrency issue for oracle queries is an interesting open problem. The techniques of [1,6] would potentially avoid the non-black-box techniques, but would produce a non-constant round complexity. We finally stress that the potential drawback due to the interaction could not be an issue when encryption is used as subprotocol in an interactive protocol.

The motivation behind the constructions we present in this work is the proved failure of the random oracle proved in several papers [7,8,9,10]. We therefore show (constructively) that without a random oracle complete non-malleability is achievable in at least two settings.

## 2 New Definitions for Encryption Schemes

In this section we give the first contribution of this work by giving new definitions for completely non-malleable encryption schemes.

### 2.1 Completely Non-Malleable Encryption

We define stronger notions of security against man-in-the-middle attacks following the lead of [4]. Indeed, Fischlin in [4] defined complete non-malleability as a stronger notion of NM-CCA2 security. We will refer to these stronger encryption schemes as NM-CCA2* secure encryption schemes. We here generalize that notion with respect to all the three main variants of security: namely NM-CPA, NM-CCA1 and NM-CCA2.

An important ingredient that we take from the framework introduced in [4] is that of a *complete relation*. A complete relation $\mathtt{R}$ is a (probabilistic) algorithm that takes as inputs: a public key $\mathtt{pk}$, a message $m$, a public key $\mathtt{pk}^*$, a ciphertext vector (under $\mathtt{pk}^*$) $\mathbf{c}^*$ and a plaintext vector $\mathbf{m}^*$ (the decryption of $\mathbf{c}^*$). $\mathtt{R}$ returns either `false` or `true`.

In our definition we will use the notation introduced in [3] based on indistinguishability rather than on the simulation paradigm (used in [4]) as the game-based paradigm simplifies the task of working with non-malleability, moreover it implies the simulation-based approach for the case of NM-CPA* security.

**Definition 1 (NM-CPA*, NM-CCA1*, NM-CCA2*).** *Let $\mathcal{PE} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a public-key encryption scheme, let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary. For* $\mathrm{atk} \in \{\mathrm{cpa}, \mathrm{cca1}, \mathrm{cca2}\}$ *and $k \in \mathbb{N}$ let*

$$\mathbf{Adv}^{\mathrm{nm-atk}^*}_{\mathcal{PE},\,\mathcal{A}}(k) = \left|\mathrm{Prob}\left[\mathtt{Expt}^{\mathrm{nm-atk}^*}_{\mathcal{PE},\,\mathcal{A}}(k)\right] - \mathrm{Prob}\left[\mathtt{Expt}^{\mathrm{nm-atk}^*}_{\mathcal{PE},\,\mathcal{A},\,\$}(k)\right]\right|$$

*where, the experiments $\mathtt{Expt}^{\mathrm{nm-atk}^*}_{\mathcal{PE},\,\mathcal{A}}(k)$, and $\mathtt{Expt}^{\mathrm{nm-atk}^*}_{\mathcal{PE},\,\mathcal{A},\,\$}(k)$ are defined as follows:*

| $\mathtt{Expt}^{\mathrm{nm-atk}^*}_{\mathcal{PE},\ \mathcal{A}}(k)$: | $\mathtt{Expt}^{\mathrm{nm-atk}^*}_{\mathcal{PE},\ \mathcal{A},\ \$}(k)$: |
|---|---|
| $(\mathtt{pk}, \mathtt{sk}) \leftarrow \mathcal{G}(r)$ where $r \leftarrow \{0,1\}^k$ | $(\mathtt{pk}, \mathtt{sk}) \leftarrow \mathcal{G}(r)$ where $r \leftarrow \{0,1\}^k$ |
| $(M, s) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(\mathtt{pk})$ | $(M, s) \leftarrow \mathcal{A}_1^{\mathcal{O}_1}(\mathtt{pk})$ |
| $x \leftarrow M$ | $x, \tilde{x} \leftarrow M$ |
| $c = \mathcal{E}_{\mathtt{pk}}(x)$ | $c = \mathcal{E}_{\mathtt{pk}}(x)$ |
| $(R, \mathtt{pk}^*, \mathbf{c}^*) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(M, \mathtt{pk}, s, c)$ | $(R, \mathtt{pk}^*, \mathbf{c}^*) \leftarrow \mathcal{A}_2^{\mathcal{O}_2}(M, \mathtt{pk}, s, c)$ |
| **return** $\mathtt{true}$ *iff* $\exists\ \mathbf{m}^*$ *such that* | **return** $\mathtt{true}$ *iff* $\exists\ \mathbf{m}^*$ *such that* |
| $(\mathbf{c}^* = \mathcal{E}_{\mathtt{pk}^*}(\mathbf{m}^*)) \wedge$ | $(\mathbf{c}^* = \mathcal{E}_{\mathtt{pk}^*}(\mathbf{m}^*)) \wedge$ |
| $(c \notin \mathbf{c}^* \vee \mathtt{pk} \neq \mathtt{pk}^*) \wedge$ | $(c \notin \mathbf{c}^* \vee \mathtt{pk} \neq \mathtt{pk}^*) \wedge$ |
| $(\mathbf{m}^* \neq \perp) \wedge$ | $(\mathbf{m}^* \neq \perp) \wedge$ |
| $(R(x, \mathbf{m}^*, \mathtt{pk}, \mathtt{pk}^*, \mathbf{c}^*) = \mathtt{true})$ | $(R(\tilde{x}, \mathbf{m}^*, \mathtt{pk}, \mathtt{pk}^*, \mathbf{c}^*) = \mathtt{true})$ |

*Above*

$$\begin{aligned}
&\textit{if } \mathrm{atk} = \mathrm{cpa} \ \ \textit{then } \mathcal{O}_1(\cdot) = \epsilon \qquad\ \ \textit{and } \mathcal{O}_2(\cdot) = \epsilon,\\
&\textit{if } \mathrm{atk} = \mathrm{cca1} \ \textit{then } \mathcal{O}_1(\cdot) = \mathcal{D}_{\mathtt{sk}}(\cdot) \ \textit{and } \mathcal{O}_2(\cdot) = \epsilon,\\
&\textit{if } \mathrm{atk} = \mathrm{cca2} \ \textit{then } \mathcal{O}_1(\cdot) = \mathcal{D}_{\mathtt{sk}}(\cdot) \ \textit{and } \mathcal{O}_2(\cdot) = \mathcal{D}^{(c)}_{\mathtt{sk}}(\cdot),
\end{aligned}$$

*with $\mathcal{D}^{(c)}_{\mathtt{sk}}(\cdot)$ meaning that the oracle decrypts any ciphertext except $c$. We insist, above, that the message space $M$ is valid: $|x| = |x'|$ for any $x, x'$ with non-zero probability in the message space $M$. Moreover, we let $\mathbf{m}^* \neq \perp$ meaning that at least one of the ciphertexts in $\mathbf{c}^*$ is valid, i.e., in $\mathbf{m}^*$ there is at least one message that is different from a special symbol $\perp$.*

*We say that $\mathcal{PE}$ is NM-ATK* secure if for every probabilistic polynomial-time adversary $\mathcal{A}$, $\mathbf{Adv}^{\mathrm{nm-atk}^*}_{\mathcal{PE},\ \mathcal{A}}(\cdot)$ is negligible.*

In the definition above we assume (as in [4,3]) that any a priori information of the adversary, i.e. the history, is in the message space $M$.

*Insecurity of known schemes with respect to complete non-malleability.* In order to motivate his definitions Fischlin showed in [4] that two encryption schemes, namely Cramer-Shoup [11] and RSA-OAEP [12,13], are not NM-CCA2* secure though they are NM-CCA2 secure. We first note that both separations trivially work also under our game-based definitions and further motivate both our definitions and Fischlin's security notion by providing the next two theorems. Below, we let $\mathrm{ATK} \in \{\mathrm{cpa}, \mathrm{cca1}, \mathrm{cca2}\}$.

**Theorem 1.** *For any NM-ATK secure encryption scheme $\mathcal{PE} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ there exists an NM-ATK secure encryption scheme $\mathcal{PE}' = (\mathcal{G}', \mathcal{E}', \mathcal{D}')$ which is not NM-ATK* secure.*

The proof of above result is based on the following simple observation. A bit is appended to the public key of an NM-ATK secure encryption scheme and it is ignored by the encryption and decryption algorithms. Obviously the resulting scheme is still NM-ATK secure but it is not NM-ATK* secure as the

adversary can simply change the appended bit of the public key, thus obtaining a new encryption of the same message with respect to a new public key. It is also possible to show that the NM-CCA2 secure encryption schemes known in literature [2,5] are not NM-CCA2* secure even under our game-based definition.

*Game-Based vs Simulation-Based Definitions.* We next study the relation between the game-based definitions and the simulation-based ones. We start by giving the simulation-based definition for NM-CCA2* [4] security.

**Definition 2 (SNM-CCA2*). ([4])** *Let $\mathcal{PE} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a public key encryption scheme, let $R$ be a complete relation, let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary and let $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ be a pair of algorithms that we call simulator. For $k \in \mathbb{N}$ we define*

$$\mathbf{Adv}^{\mathrm{snm-cca2^*}}_{\mathcal{PE},\,\mathcal{A},\,\mathcal{S},\,R}(k) = \left|\mathrm{Prob}\left[\mathtt{Expt}^{\mathrm{snm-cca2^*}}_{\mathcal{PE},\,\mathcal{A},\,R}(k)\right] - \mathrm{Prob}\left[\mathtt{Expt}^{\mathrm{snm-cca2^*}}_{\mathcal{PE},\,\mathcal{S},\,R}(k)\right]\right|$$

*where, the experiments $\mathtt{Expt}^{\mathrm{snm-cca2^*}}_{\mathcal{PE},\,\mathcal{A},\,R}(k)$, and $\mathtt{Expt}^{\mathrm{snm-cca2^*}}_{\mathcal{PE},\,\mathcal{S},\,R}(k)$ are defined as follows:*

| $\mathtt{Expt}^{\mathrm{snm-cca2^*}}_{\mathcal{PE},\,\mathcal{A},\,R}(k)$: | $\mathtt{Expt}^{\mathrm{snm-cca2^*}}_{\mathcal{PE},\,\mathcal{S},R}(k)$: |
|---|---|
| $(\mathtt{pk}, \mathtt{sk}) \leftarrow \mathcal{G}(1^k)$ | $(\mathtt{pk}, \mathtt{sk}) \leftarrow \mathcal{G}(1^k)$ |
| $(M, s) \leftarrow \mathcal{A}_1^{\mathcal{D}_{\mathtt{sk}}(\cdot)}(\mathtt{pk})$ | $(M, s) \leftarrow \mathcal{S}_1(\mathtt{pk})$ |
| $m \leftarrow M;\ c = \mathcal{E}_{\mathtt{pk}}(m)$ | $m \leftarrow M$ |
| $(\mathtt{pk}^*, c^*) \leftarrow \mathcal{A}_2^{\mathcal{D}^{(c)}_{\mathtt{sk}}(\cdot)}(c, s)$ | $(\mathtt{pk}', c') \leftarrow \mathcal{S}_2(s)$ |
| **return** `true` *iff* $\exists\ m^*$ *such that* | **return** `true` *iff* $\exists m'$ *such that* |
| $(c^* = \mathcal{E}_{\mathtt{pk}^*}(m^*)) \wedge$ | $(c' = \mathcal{E}_{\mathtt{pk}'}(m')) \wedge$ |
| $((\mathtt{pk}, c) \neq (\mathtt{pk}^*, c^*)) \wedge$ | |
| $(R(m, m^*, \mathtt{pk}, \mathtt{pk}^*, c^*) = \mathtt{true})$ | $(R(m, m', \mathtt{pk}, \mathtt{pk}', c') = \mathtt{true})$ |

*where $\mathcal{D}^{(c)}_{\mathtt{sk}}(\cdot)$ means the oracle that decrypts any ciphertext except $c$. We insist, above, that the message space $M$ is valid: $|x| = |x'|$ for any $x, x'$ with non-zero probability in the message space $M$.*

*We say that $\mathcal{PE}$ is SNM-CCA2* secure if for every probabilistic polynomial-time adversary $\mathcal{A}$ and complete relation $R$ computable in polynomial time, there exists a polynomial-time simulator $\mathcal{S}$ such that $\mathbf{Adv}^{\mathrm{snm-cca2^*}}_{\mathcal{PE},\,\mathcal{A},\,\mathcal{S},\,R}(\cdot)$ is negligible.*

We remark that if we remove both oracle accesses to the adversary $\mathcal{A}$ in the above definition then we have a simulation-based definition of NM-CPA* security (we refer to this notion as SNM-CPA*). To be consistent with Fischlin's definition we slightly change our game-based definitions by not asking for the condition $\mathbf{m}^* \neq \perp$ (see Definition 1). We are now in the position to show that our game-based definition of NM-CPA* security implies the corresponding simulation-based one (see Definition 2).

**Theorem 2.** *If an encryption scheme $\mathcal{PE} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ is NM-CPA* secure according to the game-based definition then $\mathcal{PE}$ is SNM-CPA* secure according to simulation-based definition.*

*Proof.* We next show that given a relation $\mathtt{R}$ and an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ we are able to construct a simulator $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$. The simulator simply runs the adversary $\mathcal{A}$. More formally:

| $S_1(\mathtt{pk})$: | $S_2(\tilde{s})$ where $\tilde{s} = (M, s, \mathtt{pk})$: |
|---|---|
| | $x \leftarrow M$ |
| $(M, s) \leftarrow \mathcal{A}_1(\mathtt{pk})$ | $c \leftarrow \mathcal{E}_{\mathtt{pk}}(x)$ |
| $\tilde{s} \leftarrow (M, s, \mathtt{pk})$ | $(\mathtt{pk}^*, c^*) \leftarrow \mathcal{A}_2(c, s)$ |
| **return** $(M, \tilde{s})$ | **return** $(\mathtt{pk}^*, c^*)$ |

A key point is that the simulator can indeed run $\mathcal{A}$ as $\mathcal{A}$ has not oracle access (and therefore $\mathcal{S}$ does not need to know the secret key corresponding to $\mathtt{pk}$). Now we want to show that $\mathbf{Adv}^{\mathrm{snm-cpa}^*}_{\mathcal{PE},\ \mathcal{A},\ \mathcal{S},\ \mathtt{R}}(\cdot)$ is negligible. We do this using the hypothesis that $\mathcal{PE}$ is secure in the sense of NM-CPA*. To that end, we consider the following adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ attacking $\mathcal{PE}$ in the sense of NM-CPA* security:

| $\mathcal{B}_1(\mathtt{pk})$: | $\mathcal{B}_2(M, \mathtt{pk}, s, c)$: |
|---|---|
| $(M, s) \leftarrow \mathcal{A}_1(\mathtt{pk})$ | $(\mathtt{pk}^*, c^*) \leftarrow \mathcal{A}_2(c, s)$ |
| **return** $(M, s)$ | **return** $(\mathtt{R}, \mathtt{pk}^*, c^*)$ |

It is clear from the definition of $\mathcal{B}$ that

$$\mathrm{Prob}\left[\mathtt{Expt}^{\mathrm{nm-cpa}^*}_{\mathcal{PE},\ \mathcal{B}}(k)\right] = \mathrm{Prob}\left[\mathtt{Expt}^{\mathrm{snm-cpa}^*}_{\mathcal{PE},\ \mathcal{A},\ \mathtt{R}}(k)\right]$$

for all $k \in \mathbb{N}$. Now, let us expand the definition of $\mathtt{Expt}^{\mathrm{snm-cpa}^*}_{\mathcal{PE},\ \mathcal{S},\ \mathtt{R}}(k)$, substituting in the definition of $\mathcal{S}$ given above.

$\mathtt{Expt}^{\mathrm{snm-cpa}^*}_{\mathcal{PE},\ \mathcal{S},\ \mathtt{R}}(k)$:
$(\mathtt{pk}, \mathtt{sk}) \leftarrow \mathcal{G}(1^k)$
$(M, s) \leftarrow \mathcal{A}_1(\mathtt{pk})$
$\tilde{s} \leftarrow (M, s, \mathtt{pk})$
$m \leftarrow M$
$x \leftarrow M$
$c \leftarrow \mathcal{E}_{\mathtt{pk}}(x)$
$(\mathtt{pk}^*, c^*) \leftarrow \mathcal{A}_2(c, s)$
**return** `true` iff there exists $m^*$ such that
$(c^* = \mathcal{E}_{\mathtt{pk}^*}(m^*)) \wedge$
$(\mathtt{R}(m, m^*, \mathtt{pk}, \mathtt{pk}^*, c^*) = \mathtt{true})$

Examining the code above we notice that we can drop instructions $\tilde{s} \leftarrow (M, s, \mathtt{pk})$ (as $\tilde{s}$ is never referred to). The resulting code is equivalent to that of $\mathtt{Expt}^{\mathrm{nm-cpa}^*}_{\mathcal{PE},\ \mathcal{B},\ \$}(k)$ so that:

$$\mathrm{Prob}\left[\mathtt{Expt}^{\mathrm{nm-cpa}^*}_{\mathcal{PE},\ \mathcal{B},\ \$}(k)\right] = \mathrm{Prob}\left[\mathtt{Expt}^{\mathrm{snm-cpa}^*}_{\mathcal{PE},\ \mathcal{S},\ \mathtt{R}}(k)\right]$$

for all $k \in \mathbb{N}$. Thus for all $k \in \mathbb{N}$ we have:

$$\mathbf{Adv}^{\mathrm{snm-cpa}^*}_{\mathcal{PE},\ \mathcal{A},\ \mathcal{S},\ \mathtt{R}} = \mathbf{Adv}^{\mathrm{nm-cpa}^*}_{\mathcal{PE},\ \mathcal{B}}.$$

But $\mathcal{PE}$ is assumed to be secure in the sense of NM-CPA*, so $\mathbf{Adv}^{\mathrm{nm-cpa}^*}_{\mathcal{PE},\ \mathcal{B}}$ is negligible. The above implies that $\mathbf{Adv}^{\mathrm{snm-cpa}^*}_{\mathcal{PE},\ \mathcal{A},\ \mathcal{S},\ \mathtt{R}}$ is negligible too. Therefore, $\mathcal{PE}$ is secure in the sense of SNM-CPA*. □

Using the same technique we can show that the game-based definitions of NM-CCA1* and NM-CCA2* security imply the corresponding simulation-based definitions for a large set of relations. Below we just present discussion for the NM-CCA2* security notion.

We say that an encryption scheme is (S)NM-CCA2* secure with respect to a set of complete relations $\mathcal{R}$ if in Definitions 1 and 2 we require $\mathtt{R} \in \mathcal{R}$ (we require that the scheme is resistant to a set of relations – and not to all relations as demanded by the definition). Further, we call a relation $\mathtt{R}$ *lacking* if $\mathtt{R}$ is a complete relation that ignores the input of the challenge public key: $\mathtt{R}$ is lacking if and only if $\mathtt{R}(m, m^*, pk, pk^*, c^*) = \mathtt{R}(m, m^*, pk^*, c^*)$ where $\mathtt{pk}$ is the challenge public key.

**Theorem 3.** *Let $\mathcal{R}$ be the set of lacking relations. If an encryption scheme $\mathcal{PE} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ is NM-CCA2* secure (Definition 1) with respect to $\mathcal{R}$ then $\mathcal{PE}$ is SNM-CCA2* secure with respect to $\mathcal{R}$ (Definition 2).*

The proof is similar in spirit to that we gave above (and to the one in [14] where it is shown that the game-based formulation of [3] implies the simulation-based formulation of [1]). However, there is the following technical problem. The proof in [14] consists in designing a simulator that on input a challenge public key $\mathtt{pk}$, runs an adversary $\mathcal{A}$ of the simulation-based notion. The simulator generates a new pair of public and private keys and runs $\mathcal{A}$ on input the new public key. The simulator computes an encryption of a randomly chosen message and uses it as challenge for the adversary $\mathcal{A}$. The simulator uses the secret key to answer to all decryption queries of $\mathcal{A}$ and can decrypt the final ciphertext produced by $\mathcal{A}$. The plaintext obtained is then encrypted under the challenge public key $\mathtt{pk}$ and returned by the simulator. The assumption that the original encryption scheme is secure under the game-based notion is crucially used in [14] as it is possible to show that the simulator has the same probability of succeeding as the adversary $\mathcal{A}$.

In our case, when $\mathcal{A}$ is a completely non-malleable adversary it generates the final ciphertexts under a new public key. Moreover, $\mathcal{A}$'s success depends also on

this new public key and the fake public key generated by the simulator (i.e., the outcome of complete relations does not depend just on plaintexts). This means that such a success of $\mathcal{A}$ does not seem to be easily reproducible by the simulator with respect to the challenge public key $\mathtt{pk}$. Thus the technique exploited in [14] fails, in our case, because we are considering complete relations. Therefore, if we restrict $\mathcal{R}$ to relations that ignore the challenge public key $\mathtt{pk}$, the simulator can use his own pair of keys. Consequently, it can answer to decryption queries of the underlying adversary $\mathcal{A}$ (knowing the secret key) and can return the new public key and ciphertexts given in output by $\mathcal{A}$. If the relation ignores the challenge public key $\mathtt{pk}$ in input to the simulator (as we assume) then such a simulator is successful whenever $\mathcal{A}$ is.

Theorem 6 in [15] shows the impossibility result for simulation-based black-box NM-CCA2* security with respect to a set of relation that contains relations $R_{msg-eq}$: $\mathtt{R} \in R_{msg-eq}$ means that $\mathtt{R}(m, m^*, pk, pk^*, c^*) = 1$ if and only if $m = m^*$. Since $R_{msg-eq}$ is lacking, we have the following corollary.

**Corollary 1.** *Encryption schemes which are game-based NM-CCA2* secure according to black-box adversaries do not exist.*

## 3 NM-CCA2* Secure Encryption with Shared Random Strings

In this section we show an NM-CCA2* secure encryption scheme in the shared random string model.

We stress that the NM-CCA2* security definition easily adapts to the shared random string model by simply feeding each algorithm (and the relation) with the shared random string $\Sigma$ as extra input. We remark that such a string is not under the control of the adversary and is known to all players in the game.

*IND-CPA Secure Encryption Schemes.* In our construction we will make use of encryption scheme satisfying the following classical security notions (see [3]).

**Definition 3 (IND-CPA).** *Let $\mathcal{PE} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a public-key encryption scheme, let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary. For $k \in \mathbb{N}$ let*

$$\mathbf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{PE},\,\mathcal{A}}(k) = \left|\mathrm{Prob}\left[\mathtt{Expt}^{\mathrm{indcpa-0}}_{\mathcal{PE},\,\mathcal{A}}(k) = 0\right] - \mathrm{Prob}\left[\mathtt{Expt}^{\mathrm{indcpa-1}}_{\mathcal{PE},\,\mathcal{A}}(k) = 0\right]\right|$$

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

$\mathtt{Expt}^{\mathrm{indcpa-b}}_{\mathcal{PE},\,\mathcal{A}}(k)$*:*
$(\mathtt{pk}, \mathtt{sk}) \leftarrow \mathcal{G}(r)$ *where* $r \leftarrow \{0,1\}^k$
$(x_0, x_1, s) \leftarrow \mathcal{A}_1(\mathtt{pk})$
$c = \mathcal{E}_{\mathtt{pk}}(x_b)$
$d \leftarrow \mathcal{A}_2(x_0, x_1, s, c)$
**return** $d$

*Above it is mandatory that $|x_0| = |x_1|$. We say that $\mathcal{PE}$ is IND-CPA secure if $\mathcal{A}$ being polynomial-time implies $\mathbf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{PE},\,\mathcal{A}}(\cdot)$ is negligible.*

*Non-Malleable NIZK proof of knowledge.* An important tool of our construction is the following notion defined in [5].

**Definition 4 (Non-Malleable NIZK).** *Let $\Pi = (\ell, \mathcal{P}, \mathcal{V}, \mathcal{S})$ be an unbounded NIZK proof system for the $\mathcal{NP}$ language $L$ with witness relation $W$. We say that $\Pi$ is a* non-malleable (in the explicit witness sense) NIZK proof system *for $L$ if there exists a probabilistic polynomial-time oracle machine $\mathcal{M} = (\mathcal{M}_0, \mathcal{M}_1, \mathcal{M}_2)$ such that:*

*For all non-uniform probabilistic polynomial-time adversaries $\mathcal{A}$ and for all non-uniform polynomial-time relations $R$, there exists a negligible function $\nu(k)$ such that*

$$\left|\mathrm{Prob}\left[\,\mathtt{Expt}^{\mathcal{S}}_{\mathcal{A},R}(k)\,\right] - \mathrm{Prob}\left[\,\mathtt{Expt}'_{\mathcal{A},R}(k)\,\right]\right| \leq \nu(k)$$

*where $\mathtt{Expt}^{\mathcal{S}}_{\mathcal{A},R}(k)$ and $\mathtt{Expt}'_{\mathcal{A},R}$ are the following experiments:*

| $\mathtt{Expt}^{\mathcal{S}}_{\mathcal{A},R}(k)$: | $\mathtt{Expt}'_{\mathcal{A},R}(k)$ |
|---|---|
| $(\Sigma, \tau) \leftarrow \mathcal{S}_1(1^k)$ | |
| $(x, \pi, \mathtt{aux}) \leftarrow \mathcal{A}^{\mathcal{S}_2(\cdot,\Sigma,\tau)}(\Sigma)$ | |
| Let $Q$ be list of pairs $(x, \pi)$ given by $\mathcal{S}_2$ above | $(x, w, \mathtt{aux}) \leftarrow \mathcal{M}^{\mathcal{A}}(1^k)$ |
| **return** `true` iff | |
| $((x, \pi) \notin Q) \wedge$ | **return** `true` iff |
| $(\mathcal{V}(x, \pi, \Sigma) = \mathtt{true}) \wedge$ | $((x, w) \in W) \wedge$ |
| $(R(x, \mathtt{aux}) = \mathtt{true})$ | $(R(x, \mathtt{aux}) = \mathtt{true})$ |

We focus our attention to the construction given in [5] and thus we can rewrite the non-malleability machine $\mathcal{M}$ of the non-malleable NIZK proof of knowledge of [5] as follows. We can state that $\mathcal{M}$ is actually composed of three different algorithms $(\mathcal{G}_\Sigma, \mathcal{M}_1, \mathcal{M}_2)$. In particular we can rewrite $\mathtt{Expt}'_{\mathcal{A},\mathtt{R}}(k)$ above as follows:

$\mathtt{Expt}'_{\mathcal{A},\mathtt{R}}(k)$
Make reference string $\Sigma$
$(\Sigma, \tau) \leftarrow \mathcal{G}_\Sigma(1^k)$
Interact with $\mathcal{A}(\Sigma)$. When asked for a proof of $x$, do:
$\pi_x \leftarrow \mathcal{M}_1(\Sigma, x, \tau)$
Extract witness from some proof $\pi$
$(x, w, \mathtt{aux}) \leftarrow \mathcal{M}_2(\Sigma, \tau, x, \pi)$
**return** `true` *iff* $((x, w) \in W) \wedge (\mathtt{R}(x, \mathtt{aux}) = \mathtt{true})$

*Ingredients of the Construction.* Our scheme $(\mathcal{G}', \mathcal{E}', \mathcal{D}')$ is based on:

1. Any IND-CPA secure encryption scheme $\mathcal{PE} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ in the standard model.
2. A non-malleable NIZK proof of knowledge $\Pi = (\ell, \mathcal{P}, \mathcal{V}, \mathcal{S})$ for the following languages:

$$L_1 = \{\mathtt{pk} : \exists\ r\ s.t.\ |r| = k, (\mathtt{pk}, \mathtt{sk}) \leftarrow \mathcal{G}(r)\},$$
$$L_2 = \{(c, \mathtt{pk}) : \exists\ r, m\ s.t.\ \ c = \mathcal{E}_{\mathtt{pk}}(m; r)\}.$$

   We observe that both languages are in $\mathcal{NP}$. Indeed, for $L_1$, $r$ witnesses the membership in the language, and further, the length of $r$ is polynomial in the size of $\mathtt{pk}$. For $L_2$, $r$ and $m$ witness the membership in the language; the size of $r$ and $m$ is polynomial in the sizes of $c$ and $\mathtt{pk}$.

**Construction 4** *The scheme $(\mathcal{G}', \mathcal{E}', \mathcal{D}')$ is defined as follows:*

- $\mathcal{G}'(1^k)$*: randomly pick* $r \leftarrow \{0,1\}^*$*, call* $\mathcal{G}(r)$ *to obtain a valid pair of keys* $(\mathtt{pk}, \mathtt{sk})$*. Use* $\mathcal{P}, r$ *and* $\Sigma$ *to generate a proof of knowledge* $\pi_1$ *that* $\mathtt{pk} \in L_1$ *using* $r$ *as witness. The public key is* $PK = (\mathtt{pk}, \pi_1)$*. The private key is* $SK = \mathtt{sk}$*.*
- $\mathcal{E}'_{PK}(m)$*: Use* $\mathcal{V}$ *to verify the correctness of the proof* $\pi_1$ *in* $PK$*. If* $\pi_1$ *is valid then compute (using randomness* $r$*)* $c = \mathcal{E}_{\mathtt{pk}}(m)$*. Use* $\mathcal{P}, r, m$ *and* $\Sigma$ *to generate a proof of knowledge* $\pi_2$ *that* $(c, \mathtt{pk}) \in L_2$ *using* $r$ *and* $m$ *as witnesses. Output* $(c, \pi_2)$*.*
- $\mathcal{D}'_{SK}(c)$*: Use* $\mathcal{V}$ *to verify the correctness of the proof* $\pi_2$ *in* $c$*. If* $\pi_2$ *is valid then output* $\mathcal{D}_{\mathtt{sk}}(c)$*.*

We next give an informal argument supporting the complete non-malleability of our scheme. Since the component encryption scheme is IND-CPA in the standard model then every IND-CPA adversary for $\mathcal{PE}$ has a negligible advantage. We define one of such IND-CPA adversaries $\mathcal{A}$ in the standard model by means of an NM-CCA2* adversary $\mathcal{B}$ in the shared random string model. The adversary $\mathcal{A}$, on input the challenge ciphertext $c$, starts by creating a random string using the algorithm $\mathcal{G}_\Sigma$ (thus allowing $\mathcal{A}$ to know a trapdoor for $\Sigma$). $\mathcal{B}$, with such a random string and on input the challenge $c$ returns a relation $\mathtt{R}$, a new public key $PK^*$ (i.e., a component public key $\mathtt{pk}^*$ and the proof of knowledge of a corresponding secret key $\mathtt{sk}^*$) and a vector of ciphertexts $\mathbf{c}^*$ under the new public key $PK^*$. If $\mathcal{B}$ is a winning adversary then the probability that the plaintext encrypted in $c$, the ciphertext vector $\mathbf{c}^*$ and the corresponding plaintexts are in relation $\mathtt{R}$ is noticeable. The adversary $\mathcal{A}$ then uses the trapdoor to extract the secret key $\mathtt{sk}^*$ and then evaluates the relation $\mathtt{R}$. This leads to a noticeable advantage for $\mathcal{A}$ distinguishing the plaintext behind the challenge $c$ contradicting the IND-CPA security of $\mathcal{PE}$. Since we augmented the encryption of a message $m$ by a proof of knowledge of $m$, $\mathcal{A}$ can answer the decryption queries the NM-CCA2* adversary $\mathcal{B}$ will ask for, due to the fact that $\mathcal{A}$ knows the trapdoor for $\Sigma$.

**Theorem 5.** *The encryption scheme $(\mathcal{G}', \mathcal{E}', \mathcal{D}')$ above is NM-CCA2* secure in the shared random string model.*

*Proof.* The main idea is to transform a strong NM-CCA2* attack against the new encryption scheme $\mathcal{PE}' = (\mathcal{G}', \mathcal{E}', \mathcal{D}')$ into an IND-CPA attack against the component encryption scheme $\mathcal{PE}$. In particular, let $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ be an NM-CCA2* adversary attacking the new encryption scheme. We must show that $\mathbf{Adv}^{\mathrm{nm-cca2}^*}_{\mathcal{PE}',\mathcal{B}}(\cdot)$ is negligible. Towards this end we describe an IND-CPA adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ attacking the component encryption scheme $\mathcal{PE}$.

$\mathcal{A}_1(\mathtt{pk})$:
$(\Sigma, \tau) \leftarrow \mathcal{G}_\Sigma(1^k)$
$\pi \leftarrow \mathcal{M}_1(\Sigma, \mathtt{pk}, \tau)$
Run $B_1^{\mathcal{D}\mathtt{sk}(\cdot)}$ on input $((\mathtt{pk}, \pi), \Sigma)$:
  When $B_1$ asks $\mathcal{D}_{\mathtt{sk}}(\cdot)$ for a ciphertext $(c', \pi')$, do:
    If $\mathcal{V}((c', \mathtt{pk}), \pi', \Sigma) = \mathtt{false}$ **return** $\perp$ to $\mathcal{B}_1$
    $(r, m) \leftarrow \mathcal{M}_2(\Sigma, \tau, (c', \mathtt{pk}), \pi')$
    **return** $m$ to $\mathcal{B}_1$
  Let $(M, s)$ the output of $\mathcal{B}_1$
$x_0, x_1 \leftarrow M$
**return** $(x_0, x_1, (s, \tau, (\mathtt{pk}, \pi), \Sigma, M))$

$\mathcal{A}_2(x_0, x_1, s', c)$: where $s' = (s, \tau, PK, \Sigma, M)$
Run $B_2^{\mathcal{D}^{(c)}\mathtt{sk}(\cdot)}$ on input $(M, PK, s, c, \Sigma)$:
  When $B_2$ asks $\mathcal{D}^{(c)}_{\mathtt{sk}}(\cdot)$ for a ciphertext $(c', \pi')$, do:
    If $\mathcal{V}((c', \mathtt{pk}), \pi', \Sigma) = \mathtt{false}$ **return** $\perp$ to $\mathcal{B}_2$
    $(r, m) \leftarrow \mathcal{M}_2(\Sigma, \tau, (c', \mathtt{pk}), \pi')$
    **return** $m$ to $\mathcal{B}_2$
  Let $(\mathtt{R}, (\mathtt{pk}^*, \pi^*), \mathbf{c}^*)$ the output of $\mathcal{B}_2$
$r^* \leftarrow \mathcal{M}_2(\Sigma, \tau, \mathtt{pk}^*, \pi^*)$
$(\mathtt{pk}^*, \mathtt{sk}^*) \leftarrow \mathcal{G}(r^*)$; $\mathbf{x} = \mathcal{D}_{\mathtt{sk}^*}(\mathbf{c}^*)$
$f = (c \notin \mathbf{c}^* \vee \mathtt{pk} \neq \mathtt{pk}^*)$
**if** $(f \wedge (\mathbf{x} \neq \perp) \wedge \mathtt{R}(x_0, \mathbf{x}, (\mathtt{pk}, \pi), (\mathtt{pk}^*, \pi^*), \mathbf{c}^*, \Sigma))$ **then** $d \leftarrow 0$
**else** $d \leftarrow \{0, 1\}$
**return** $d$

Notice $\mathcal{A}$ is polynomial time given that the running time of $\mathcal{B}$, the time to compute $\mathtt{R}$, the time to sample from $M$ and the running time of $\mathcal{M}$ are all bounded by a fixed polynomial.

Observe that in the adversary above we use three different kind of proofs: $\pi$ is the (non-malleable NIZK) proof (of knowledge) that $\mathtt{pk} \in L_1$, $\pi'$ is the (non-malleable NIZK) proof (of knowledge) that the ciphertext $c'$ for which $\mathcal{B}_j$

$(j = 1, 2)$ is asking for the decryption is valid – i.e., $(c', \mathtt{pk}) \in L_2$ –, and $\pi^*$ is the (non-malleable NIZK) proof (of knowledge) that $\mathtt{pk}^* \in L_1$. We use the proofs $\pi'$ along with the trapdoor $\tau$ to allow $\mathcal{A}$ to answer to the decryption queries. Indeed, up to a negligible factor, $\mathcal{M}_2$ extracts the witnesses $r, m$ and therefore $\mathcal{A}$ can correctly return $m$ to the NM-CCA2* adversary.

Moreover, observe that since we are using a non-malleable NIZK PoK proof system then $\mathcal{M}_2(\cdot,\cdot,\cdot,\cdot)$ must extract (up to a negligible factor) the plaintext used by $\mathcal{B}_2(\cdot,\cdot,\cdot,\cdot)$ in the proof $\pi^*$. If it was not the case, then we could use $\mathcal{B}_2(\cdot,\cdot,\cdot,\cdot)$ to break the properties of the non-malleable NIZK proof system. Thus the operation of using the output of $\mathcal{M}_2(\cdot,\cdot,\cdot,\cdot)$ to generate the secret key $\mathtt{sk}^*$ corresponding to $\mathtt{pk}^*$ is well defined. The decryption with $\mathtt{sk}^*$ will thus give the actual plaintext vector behind $\mathbf{c}^*$.

The advantage of $\mathcal{A}$ is given by $\mathbf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{PE},\,\mathcal{A}}(k) = |p_k(0) - p_k(1)|$ where, for $b \in \{0,1\}$, we let

$$p_k(b) = \mathrm{Prob}\left[(\mathtt{pk},\mathtt{sk}) \leftarrow \mathcal{G}(1^k); (x_0, x_1, s') \leftarrow \mathcal{A}_1(\mathtt{pk}); c \leftarrow \mathcal{E}_{\mathtt{pk}}(x_b) : \mathcal{A}_2(x_0, x_1, s', c) = 0\right].$$

Also for $b \in \{0,1\}$ we let[2]

$$\begin{aligned} p'_k(b) = \mathrm{Prob}\Big[&(\mathtt{pk},\mathtt{sk}) \leftarrow \mathcal{G}(1^k); (\Sigma,\tau) \leftarrow \mathcal{G}_\Sigma(1^k); \pi \leftarrow \mathcal{M}_1(\Sigma,\mathtt{pk},\tau);\\ &(M,s) \leftarrow \mathcal{B}_1^{\mathcal{D}_{\mathtt{sk}}(\cdot)}((\mathtt{pk},\pi),\Sigma); x_0, x_1 \leftarrow M; c \leftarrow \mathcal{E}_{\mathtt{pk}}(x_b);\\ &(\mathtt{R},(\mathtt{pk}^*,\pi^*),\mathbf{c}^*) \leftarrow \mathcal{B}_2^{\mathcal{D}^{(c)}_{\mathtt{sk}}(\cdot)}(M,PK,s,c,\Sigma); r^* \leftarrow \mathcal{M}_2(\Sigma,\tau,\mathtt{pk}^*,\pi^*);\\ &(\mathtt{pk}^*,\mathtt{sk}^*) \leftarrow \mathcal{G}(r^*); \mathbf{x} = \mathcal{D}_{\mathtt{sk}^*}(\mathbf{c}^*); f = (c \notin \mathbf{c}^* \vee \mathtt{pk} \neq \mathtt{pk}^*) :\\ &f \wedge (\mathbf{x} \neq \perp) \wedge\ \mathtt{R}(x_0,\mathbf{x},(\mathtt{pk},\pi),(\mathtt{pk}^*,\pi^*),\mathbf{c}^*,\Sigma)\Big]. \end{aligned}$$

Now observe that $\mathcal{A}_2$ may return 0 either when $\mathbf{x}$ is $\mathtt{R}$-related to $x_0$ or as a result of the coin flip. Thus we have:

$$\mathbf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{PE},\,\mathcal{A}}(k) = |p_k(0) - p_k(1)| = \frac{1}{2}\left|p'_k(0) - p'_k(1)\right|.$$

We now observe that the experiment of $\mathcal{B}_2$ being given a ciphertext of $x_1$ and $\mathtt{R}$-relating $\mathbf{x}$ to $x_0$ is exactly $\mathtt{Expt}^{\mathrm{nm-cca2}^*}_{\mathcal{PE}',\,\mathcal{B},\,\$}(k)$. On the other hand, in the case in which $\mathcal{B}_2$ works on the ciphertext of $x_0$, we are looking at the experiment $\mathtt{Expt}^{\mathrm{nm-cca2}^*}_{\mathcal{PE}',\,\mathcal{B}}(k) = 1$. Therefore we obtain the following.

$$\mathbf{Adv}^{\mathrm{nm-cca2}^*}_{\mathcal{PE}',\,\mathcal{B}}(k) = |p'_k(0) - p'_k(1)| = 2 \cdot \mathbf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{PE},\,\mathcal{A}}(k).$$

[2] To simplify our notation, in the definition of $p'_k(b)$ we do not specify that the decryption queries of $\mathcal{B}$ are replied as in the description of the IND-CPA adversary $\mathcal{A}$.

Since $\mathcal{PE}$ is IND-CPA secure then $\mathbf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{PE},\,\mathcal{A}}(\cdot)$ is negligible. It follows that $\mathbf{Adv}^{\mathrm{nm-cca2}^*}_{\mathcal{PE}',\,\mathcal{B}}(\cdot)$ is negligible. □

We stress that we cannot use just one of the two languages above. Indeed, $L_2$ is needed because it allows an IND-CPA adversary to answer to the queries of an NM-CCA2* adversary. Moreover, we need $L_1$ to enforce the NM-CCA2* adversary to output a valid new public key $\mathtt{pk}^*$ (i.e., $\mathtt{pk}^*$ is the output of the key generation algorithm of $\mathcal{PE}$) for the component IND-CPA secure encryption scheme. One would be tempted to use the proof of knowledge contained in $\mathbf{c}^*$ – the ciphertext output of the NM-CCA2* adversary – to extract the corresponding plaintext and use it to evaluate the relation. This approach fails when $\mathtt{pk}^*$ is not valid since the NMNIZK PoK extractor returns one of the messages for which $\mathbf{c}^*$ is the corresponding encryption but not necessarily the one that satisfies the relation.

*Simulation-based NM-CCA2* security.* We now discuss that our construction can be adapted to achieve the simulation-based notion of NM-CCA2* security. In particular, we will consider the following tool. We start by giving the definition of same-string ZK.

**Definition 5 (Same-String Zero Knowledge).** *We say that an NIZK argument system is* same-string *NIZK if the (unbounded) zero knowledge requirement above is replaced with the following requirement: there exists a negligible function $\nu$ such that for all $k$ the following property holds.*
Same-string Zero Knowledge*: For all non-uniform probabilistic polynomial-time adversaries $\mathcal{A}$ we have that*
$|\mathrm{Prob}[X=1]-\mathrm{Prob}[Y=1]|\leq\nu(k)$*, where $X$ and $Y$ are as defined in (and all probabilities are taken over) the experiment* $\mathtt{Expt}(k)$ *below:*

$\mathtt{Expt}(k)$ :
$(\Sigma,\tau)\leftarrow\mathcal{S}_1(1^k)$
$X\leftarrow\mathcal{A}^{\mathcal{P}(\cdot,\cdot,\Sigma)}(\Sigma)$
$Y\leftarrow\mathcal{A}^{\mathcal{S}'(\cdot,\cdot,\Sigma,\tau)}(\Sigma)$

*where* $\mathcal{S}'(x,w,\Sigma,\tau)\stackrel{\mathrm{def}}{=}\mathcal{S}_2(x,\Sigma,\tau)$*. The distribution on $\Sigma$ produced by $\mathcal{S}_1(1^k)$ is the uniform distribution over $\{0,1\}^{\ell(k)}$.*

We refer to NIZK arguments that are both non-malleable and same-string as *robust NIZK* (as in [5]). We denote a robust NIZK $\Pi$ as the following tuple: $\Pi=(\ell,\mathcal{P},\mathcal{V},\mathcal{S})$. We remark that the authors of [5] give a construction of a robust NIZK starting from a same-string NIZK proof of knowledge given that one-way functions exist.

*The construction.* We now show that in the above scheme by simply replacing the non-malleable NIZK proof of knowledge $\Pi = (\ell, \mathcal{P}, \mathcal{V}, \mathcal{S})$ by a robust NIZK $\Pi' = (\ell', \mathcal{P}', \mathcal{V}', \mathcal{S}')$ we obtain a scheme that satisfies the simulation-based definition of [4] (see Definition 2) adapted to the shared random string model.

First of all we argue why Construction 4 does not seem to be sufficient. The simulator $S$ receives as input a pair $(\mathtt{pk} = (\mathtt{pk}', \pi), \Sigma)$ generates a fake SRS $\Sigma'$ along with a trapdoor $\tau'$, and computes a new proof $\pi'$ so that $\mathtt{pk}'' = (\mathtt{pk}', \pi')$ is a valid public key with respect to $\Sigma'$. Then $S$ runs $\mathcal{A}$ on input $(\mathtt{pk}'', \Sigma')$ and can obviously answer to all its queries since knowledge of $\tau'$ allows $S$ to decrypt all valid ciphertexts. Moreover $S$ feeds to $\mathcal{A}$ the encryption $c$ of a random message $m$ as challenge. Finally $\mathcal{A}$ outputs a pair $(c^\star, \mathtt{pk}^\star)$ that corresponds to the encryption of a messages $\tilde{m}$ related to $m$. However, the relation $\mathtt{R}$ receives as input also the public keys $\mathtt{pk}'', \mathtt{pk}^\star$ and $\Sigma'$. $S$ could obviously decrypt the message $\tilde{m}$ encrypted in $c^\star$ and could compute an encryption of $\tilde{m}$ with respect to a new public key $\tilde{\mathtt{pk}}$ and shared random string $\Sigma$ (notice that $S$ can not simply output the pair $(c^\star, \mathtt{pk}^\star)$ since this is valid only with respect to $\Sigma'$ while $S$ needs to output a valid pair with respect to $\Sigma$). However even though the same message has been encrypted, the relation could not be satisfied as $\Sigma \neq \Sigma'$ and $\mathtt{pk}^\star \neq \tilde{\mathtt{pk}}$.

We fix this problem by strengthening the ingredient that we use in the construction: we replace the non-malleable NIZK by a robust NIZK. Robust NIZK considers non-malleable zero-knowledge arguments (i.e., computationally sound proofs) of knowledge where the simulator works using the same shared random string of the real game, still having a trapdoor that will allow it to compute simulated proofs and to extract witnesses from accepting proofs.

Concretely, $S$ will run $\mathcal{A}$ precisely on input $(\mathtt{pk}, \Sigma)$ and will feed it the encryption $c$ of a random message $m$. $S$ decrypts $A$'s queries by using $\tau$ and finally outputs the pair $(c^\star, \mathtt{pk}^\star)$ given in output by $\mathcal{A}$. The indistinguishability of the output of the stand-alone $S$ with respect to the man-in-the-middle $\mathcal{A}$ can be proved by using standard hybrid arguments.

We finally stress that the above simulator does not require access to a decryption oracle, therefore it satisfies the stronger notion of stand-alone simulation discussed in [4].

## 4 Interactive Non-Black-Box Complete Non-Malleability

In this section we present a completely non-malleable encryption scheme using interaction and non-black-box techniques. Our construction can be compared to Fischlin's impossibility result. Indeed, that impossibility proof holds for black-box non-interactive encryption schemes, therefore it is still possible to relax either the need of interaction or the need of non-black-box techniques[3]. The construction we give is NM-CCA2$^*$ secure under both our game-based definition and under the simulation-based definition. Moreover, it is *stand-alone* (i.e.,

[3] We stress that the techniques of [1,6] would potentially avoid the non-black-box techniques, but would produce a non-constant round complexity.

the simulator does not access to a decryption oracle) and requires sequential decryption queries (i.e., the decryption oracle sends its answers one-by-one, sequentially). We construct a non-black-box constant-round interactive completely non-malleable encryption scheme in the standard model using the recent technique by Pass and Rosen [16,17] that produced a constant-round NMZK argument of knowledge in the standard model. On top of this tool they showed also how to construct constant-round concurrent non-malleable commitments in the standard model by composing a commitment scheme with the NMZK argument of knowledge of the committed message. The same approach has been recently used in [18] where non-malleable witness indistinguishable argument systems are achieved by committing to an $\mathcal{NP}$ witness and then using the NMZK argument of knowledge to prove that the committed message satisfies an $\mathcal{NP}$ relation. We notice that by following the same approach, it is possible to first encrypt a message using an IND-CPA encryption scheme and then prove knowledge of the encrypted message with the NMZK argument of knowledge. While this gives NM-CPA$^*$ security, extra work is required to claim NM-CCA1$^*$ and NM-CCA2$^*$ security as in these last two cases, queries to a decryption oracle have to be taken into account.

*Definitions for interactive encryption.* The definitions for NM-ATK$^*$-secure encryption for ATK $\in$ {CPA, CCA1, CCA2} given in Section 2 assume that an encryption and a decryption (oracle answer) is computed non-interactively by an efficient algorithm. An interactive encryption is instead a two-party protocol. Therefore, in order to recycle all the previous definitions we have to specify the role of the parties in all the steps described in Definition 1.

An *interactive encryption* is a protocol played between a sender `sen` and a receiver `rec`. At the end of the protocol, if both parties behave correctly, the exchanged transcript corresponds to an encryption of a message computed by `sen` for `rec` under a public key `pk`.

Non-malleable interactive encryption concerns a man-in-the-middle adversary $\mathcal{A}$ that controls the communication between `sen` and `rec` (e.g., he can delay, discard, scramble, and update the messages, as defined for non-malleable protocols in [1]). $\mathcal{A}$ aims at computing encryptions for `rec` of messages that are related to the message encrypted by `sen`. The goal of a non-malleable interactive encryption scheme is to preserve security against such man-in-the-middle attacks, thus making useless the attack of $\mathcal{A}$. Different definitions of interactive non-malleable encryption can be given by possibly giving to $\mathcal{A}$ access to decryption oracles, thus producing the variations CPA, CCA1 and CCA2. In order to have a definition of interactive encryption following the standard non-interactive Definition 1, we consider the framework used by Katz in [19,20]. We sketch here the setting on which we base our protocol, more details can be in the full version of the paper.

$\mathcal{A}$ has access to an encryption oracle $\mathcal{O}_E = \mathcal{E}_{\mathtt{pk}}(\cdot)$ that plays as sender while $\mathcal{A}$ plays as receiver. The goal of $\mathcal{A}$ is to produce the description of a relation `R`, a new public key `pk`$^*$ and encryptions of messages that are related through `R` to the message encrypted by $\mathcal{O}_E$. In order to do that, $\mathcal{A}$ plays the protocol with

honest receivers potentially interleaving (even concurrently) these interactions and the one with $\mathcal{O}_E$.

The above sketched discussion only concerns NM-CPA* security given in Definition 1 but adapted for interactive encryption. Instead, for the notions of NM-CCA1* and NM-CCA2* security the adversary $\mathcal{A}$ has to include the capability of accessing to a decryption oracle. Such accesses (e.g., oracle queries) are interactive encryptions where the adversary acts as a sender and the decryption oracle $\mathcal{O}_D = \mathcal{D}_{\mathtt{sk}}(\cdot)$ plays the role of a receiver. Indeed, an oracle query is an encryption sent by the adversary (and thus the interactive encryption protocol is played) plus an answer of the oracle. Each time a given interactive encryption with $\mathcal{O}_D$ is completed, the decryption oracle computes the decryption (using the secret key) and sends the resulting message (or a special symbol, if the transcript was invalid) to the adversary.

The definition of NM-CCA1* security assumes that $\mathcal{A}$ has first access to the decryption oracle $\mathcal{O}_D$ and then, once all interactions with $\mathcal{O}_D$ have been completed, $\mathcal{A}$ starts the game above, choosing the messages distribution $M$ and receiving an encryption from $\mathcal{O}_E$ while computing encryptions for honest receivers. For the case of NM-CCA1* security we therefore assume a time barrier between all decryption queries and the remaining protocols. These accesses to $\mathcal{O}_D$ correspond to queries to $\mathcal{O}_1$ in Definition 1.

The definition of NM-CCA2* security instead allows $\mathcal{A}$ to run decryption queries even during and/or after receiving the challenge encryption from $\mathcal{O}_E$. Obviously some limitations must be placed on the adversary access to the decryption oracle or else the adversary may simply forward messages between $\mathcal{O}_E$ and $\mathcal{O}_D$ and therefore trivially succeeds in computing encryptions of messages that are related to the challenge plaintext. We therefore require that the transcript of the encryptions of $\mathcal{O}_E$ must be different from the ones of the decryption queries. These additional accesses to $\mathcal{O}_D$ correspond to queries to $\mathcal{O}_2$ in Definition 1.

The above definition gives to the adversary $\mathcal{A}$ the power of controlling the communication channel and thus of deciding the schedule of the messages of different interactions involving different parties (different honest receivers, the encryption oracle and the decryption oracle). It is therefore obvious to assume that interactions with different parties can be run concurrently. The only restriction we have is on the interactions with the decryption oracle that we required to be sequential. Notice that this is also applicable in practice since $\mathcal{O}_D$ is a stateful algorithm that can simply manage a queue of requests to satisfies them one by one.

We finally say that an encryption scheme is self-certifiable, if there exists an efficient algorithm that on input a public key outputs 1 if it holds that any valid ciphertext corresponds to only one plaintext and 0 otherwise.

**Theorem 6.** *Under the assumption that there exists a family of claw-free permutations and that self-certifiable IND-CPA secure encryption schemes exist, there exists an interactive (constant-round) non-black-box NM-CCA2* secure encryption scheme with sequential decryption queries.*

For lack of space we show the construction in Fig. 1 (where we let $\Pi_{\mathtt{tag}} = \langle P_{\mathtt{tag}}, V_{\mathtt{tag}} \rangle$ be the tag-based constant-round one-left many-right concurrent non-malleable statistical zero-knowledge argument of knowledge of [16,17] and $SS = (\mathtt{SG}, \mathtt{Sig}, \mathtt{SVer})$ be a one-time secure signature scheme of [21]). The proof can be found in the full version of the paper, where we also show in a separate theorem that the same protocol also satisfies the simulation-based notion of complete non-malleability. We remark that the proof exploits the power of the simulator and the extractor of the statistical non-malleable zero knowledge argument of knowledge of [17,16]. In particular the extractor will be used for answering to the decryption queries, and, since it requires rewinds, we assume that decryption queries are answered sequentially, so that we do not need to face the known problems of concurrent zero knowledge [22].

We stress that a public key of our scheme is the public key of a self-certifiable IND-CPA secure encryption scheme.

1. $\mathtt{sen}$ sets $c \leftarrow \mathcal{E}_{\mathtt{pk}}(w)$ where $w$ is the $k$-bit message to encrypt.
2. $\mathtt{sen}$ sets $(\mathtt{ssk}, \mathtt{spk}) \leftarrow \mathtt{SG}(1^n)$.
3. $\mathtt{sen}$ sends the pair $(c, \mathtt{spk})$ to $\mathtt{rec}$.
4. $\mathtt{sen}$ and $\mathtt{rec}$ run protocol $\Pi_{\mathtt{spk}} = \langle P_{\mathtt{spk}}, V_{\mathtt{spk}} \rangle$ where $\mathtt{sen}$ proves knowledge of $w$ such that $c \leftarrow \mathcal{E}_{\mathtt{pk}}(w)$.
5. $\mathtt{sen}$ computes a signature $\tau \leftarrow \mathtt{Sig}(\mathtt{pk} \circ \mathtt{trans}, \mathtt{ssk})$ where $\mathtt{trans}$ is the transcript exchanged so far and sends it to $\mathtt{rec}$.
6. $\mathtt{rec}$ accepts the encryption iff $\mathtt{SVer}(\mathtt{pk} \circ \mathtt{trans}, \tau, \mathtt{spk}) = 1$ and $V_{\mathtt{spk}}$ outputs 1.

**Fig. 1.** Constant-Round Completely Non-Malleable Encryption.

We now only give an intuition of the proof.

*Proof's sketch.* Assume by contradiction that an adversary $\mathcal{A}$ succeeds in computing encryptions of related messages under a new public and a new relation of its choice. Therefore $\mathcal{A}$ has non-negligible success of generating an encryption $c_0^\star$ of a message $m_0^\star$ related to $m_0$ on input an encryption $c_0$ of $m_0$ and an encryption $c_1^\star$ of a message $m_1^\star$ related to $m_1$ on input an encryption $c_1$ of $m_1$.

Let $\mathtt{Expt}_0$ and $\mathtt{Expt}_3$ the two above experiments, we can consider two hybrid experiments $\mathtt{Expt}_1, \mathtt{Expt}_2$ where instead of running $\mathcal{A}$, we run the simulator $S$ associated to the statistical non-malleable zero knowledge argument of knowledge of [17,16] giving it access to $\mathcal{A}$ and $c_0$ in $\mathtt{Expt}_1$ and access to $\mathcal{A}$ and $c_1$ in $\mathtt{Expt}_2$.

By the statistical zero-knowledge property of this tool, we have that experiment $\mathtt{Expt}_1$ in indistinguishable with respect to $\mathtt{Expt}_0$.

A distinguisher between $\mathtt{Expt}_1$ and $\mathtt{Expt}_2$ can be used for breaking the semantic security of the (non-interactive) encryption scheme used as subprotocol. This can be done by feeding to $\mathcal{A}$ a challenge $c$ that can be either an encryption

of $m_0$ or an encryption of $m_1$ under the encryption scheme used as subprotocol. Then the extractor of [17,16] obtains the encrypted message and can therefore be used to break with non-negligible advantage the semantic security of the encryption scheme.

Finally, $\texttt{Expt}_2$ and $\texttt{Expt}_3$ are indistinguishable for the same reason that make indistinguishable $\texttt{Expt}_0$ and $\texttt{Expt}_1$.

The full proof considers other issues as concurrency and adaptiveness. Moreover it is shown that the protocol satisfies also the simulation-based definition, as a simulator can be designed by simply sending an encryption of any message (say $0^k$) and then using the simulator of the NMZK argument of knowledge. □

*Concluding Remarks.* In this paper we explored the notion of complete non-malleability for public-key encryption schemes. We have given new definitions and proved relations among these notions. Finally, we have shown new constructions that achieve these security notions without using random oracles.

## 5 Acknowledgments

We wish to thank Alex Dent for his useful comments on an early draft of this paper. Moreover we thank the anonymous reviewers for their accurate suggestions and Pino Persiano for useful discussions about non-malleability.

The work of the authors has been supported in part through the FP6 program under contract FP6-1596 AEOLUS and in part by the European Commission through the IST program under Contract IST-2002-507932 ECRYPT.

## References

1. Dolev, D., Dwork, C., Naor, M.: Non-malleable cryptography. In: Proc. of STOC. (1991) 542–552
2. Sahai, A.: Non-Malleable Non-Interactive Zero Knowledge and Adaptive Chosen-Ciphertext Security. In: 40th Symposium on Foundations of Computer Science, (FOCS '99), 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, IEEE Computer Society Press (1999) 543–553
3. Bellare, M., Desai, A., Pointcheval, D., Rogaway, P.: Relations among notions of security for public-key encryption schemes. In: Proc. of CRYPTO. Volume 1462. (1998) 26–45
4. Fischlin, M.: Completely non-malleable schemes. In: Proc. of ICALP. Volume 3580. (2005) 779–790
5. De Santis, A., Di Crescenzo, G., Ostrovsky, R., Persiano, G., Sahai, A.: Robust non-interactive zero knowledge. In: Proc. of CRYPTO. Volume 2139. (2001) 566–598
6. Barak, B., Prabhakaran, M., Sahai, A.: Concurrent non-malleable zero knowledge. In: 47th, IEEE Computer Society Press (2006)
7. Bellare, M., Boldyreva, A., Palacio, A.: An uninstantiable random-oracle-model scheme for a hybrid-encryption problem. In: EUROCRYPT. Volume 3027. (2004) 171–188

8. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited (preliminary version). In: STOC. (1998) 209–218
9. Nielsen, J.B.: Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case. In: CRYPTO. Volume 2442. (2002) 111–126
10. Goldwasser, S., Kalai, Y.T.: On the (in)security of the fiat-shamir paradigm. In: FOCS. (2003)
11. Cramer, R., Shoup, V.: A Practical Public-Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack. In Krawczyk, H., ed.: Advances in Cryptology – Crypto '98. Volume 1462 of Lecture Notes in Computer Science., Springer-Verlag (1998) 13–25
12. Bellare, M., Rogaway, P.: Optimal asymmetric encryption. In: Proc. of EUROCRYPT. Volume 765. (1994) 92–111
13. Fujisaki, E., Okamoto, T., Pointcheval, D., Stern, J.: Rsa-oaep is secure under the rsa assumption. In: CRYPTO. (2001) 260–274
14. Bellare, M., Sahai, A.: Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization. In: Advances in Cryptology – Crypto '99. Volume 1666 of Lecture Notes in Computer Science., Springer Verlag (1999) 519–536
15. Fischlin, M.: Completely non-malleable schemes. Technical report (2005) Full version of [4].
16. Pass, R., Rosen, A.: New and improved constructions of non-malleable cryptographic protocols. In: Proc. of STOC. (2005) 533–542
17. Pass, R., Rosen, A.: Concurrent non-malleable commitments. In: Proc. of FOCS. (2005) 563–572
18. Ostrovsky, R., Persiano, G., Visconti, I.: Concurrent non-malleable witness indistinguishability and its applications. Technical Report TR06-095, ECCC (2006)
19. Katz, J.: Efficient Cryptographic Protocols Preventing Man-in-the-Middel Attacks, Ph.D. Thesis. Columbia University (2002)
20. Katz, J.: Efficient and Non-Malleable Proofs of Plaintext Knowledge and Applications. In: Advances in Cryptology – Eurocrypt '03. Volume 2045 of Lecture Notes in Computer Science., Springer-Verlag (2003) 211–228
21. Rompel, J.: One-way functions are necessary and sufficient for secure signatures. In: Proc. of STOC. (1990) 387–394
22. Dwork, C., Naor, M., Sahai, A.: Concurrent Zero-Knowledge. In: 30th ACM Symposium on Theory of Computing (STOC '98), ACM (1998) 409–418