Relations among Privacy Notions for Signcryption and Key Invisible "Sign-then-Encrypt"

Yang Wang[1], Mark Manulis[2], Man Ho Au[1], and Willy Susilo[1,⋆]

[1] Centre for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong, Australia
yw990@uowmail.uow.edu.au,
{wsusilo,aau}@uow.edu.au
[2] Department of Computing, University of Surrey, United Kingdom
mark@manulis.eu

Abstract. Signcryption simultaneously offers authentication through unforgeability and confidentiality through indistinguishability against chosen ciphertext attacks by combining the functionality of digital signatures and public-key encryption into a single operation. Libert and Quisquater (PKC 2004) extended this set of basic requirements with the notions of ciphertext anonymity (or key privacy) and key invisibility to protect the identities of signcryption users and were able to prove that key invisibility implies ciphertext anonymity by imposing certain conditions on the underlying signcryption scheme.

This paper revisits the relationship amongst privacy notions for signcryption. We prove that key invisibility implies ciphertext anonymity without any additional restrictions. More surprisingly, we prove that key invisibility also implies indistinguishability against chosen ciphertext attacks. This places key invisibility on the top of privacy hierarchy for public-key signcryption schemes.

On the constructive side, we show that general "sign-then-encrypt" approach offers key invisibility if the underlying encryption scheme satisfies two existing security notions, indistinguishable against adaptive chosen ciphertext attacks and indistinguishability of keys against adaptive chosen ciphertext attacks. By this method we obtain the first key invisible signcryption construction in the standard model.

1 Introduction

Signcryption methods. The concept of signcryption was introduced by Zheng in 1997 [26], with the initial goal to achieve performance increase for simultaneous signing and public-key encryption. His idea was to derive the combined functionality by optimizing computations at the algorithmic level rather than considering joint execution of two different signing and encryption procedures.

⋆ W. Susilo is supported by ARC Future Fellowship FT0991397.

C. Boyd and L. Simpson (Eds.): ACISP 2013, LNCS 7959, pp. 187–202, 2013.

This idea was reflected in various signcryption constructions, including those based on discrete logarithms [4, 21, 25], factoring assumptions [18, 22], and hard problems in groups with bilinear maps [15, 16]. Some of these designs were less successful, e.g. [4, 25] were cryptanalyzed in [21], a problem in [15] was identified in [23] and repaired in [9].

A more general approach to signcryption was initiated by An, Dodis, and Rabin [1]. They considered different methods for obtaining the signcryption functionality through a black-box composition of arbitrary signature and public-key encryption schemes, in particular showing that "encrypt-then-sign" (EtS) and "sign-then-encrypt" (StE) lead to secure singcryption schemes (as opposed to the symmetric-key setting [6]). They also introduced another approach, termed "commit-then-sign-and-encrypt" (CtS&E) that admits parallelization of the signing and encryption operations, motivated by the insecurity of the plain "sign-and-encrypt" (S&E) method. Dent et al. [10] recently proved security of S&E in the setting of high-entropy messages, assuming the confidentiality property of signatures. Alternative generic methods for (parallel) signcryption were introduced by Pieprzyk and Pointcheval [19] based on secret sharing techniques, by Dodis et al. [11] using trapdoor permutations and probabilistic padding schemes, and by Malone-Lee [17] from the hybrid KEM/DEM framework.

Privacy notions for signcryption. The first formal security model for signcryption in the public-key setting was introduced by Baek et al. [3], encompassing the requirements of message confidentiality (indistinguishability against adaptive chosen ciphertext attacks) and unforgeability against chosen-message attacks in the multi-user setting. This model has been strengthened by An, Dodis, and Rabin [1] towards the insider security setting that admits corruptions of senders and receivers, as opposed to the outsider security guarantees from [3] in which all involved parties must remain uncorrupted. The insider security setting became the de facto standard security setting for modern public-key signcryption schemes.

Libert and Quisquater [15], inspired by Boyen's work [7] on identity-based signcryption and the earlier definition of key privacy for public-key encryption schemes by Bellare et al. [5], formalized the notions of ciphertext anonymity (or key privacy) for public-key signcryption. This requirement, modeled within the insider security framework, prevents the adversary that is not in possession of the recipient's decryption key from obtaining information about the sender and the recipient of the signcrypted message. Libert and Quisquater also introduced the notion of key invisibility, for which they could prove that it implies ciphertext anonymity as long as signcryption ciphertexts have uniform distribution for random recipients' public keys.

1.1 Our Contribution

In this paper we focus on privacy notions for signcryption schemes and aim at closing gaps from previous work.

Relations among privacy notions. Using public-key signcryption notions from [15], namely key invisibility (SC-INVK-CCA), ciphertext anonymity (SC-INDK-CCA), and indistinguishability against chosen ciphertext attacks (SC-IND-CCA), we investigate their relationships and come to the following surprising results (cf. Figure 1): first, we show that key invisibility implies ciphertext anonymity without requiring uniformity of ciphertexts for random public keys (as opposed to the proof from [15]). Our proof of this implication involves a two-step approach: we first give a new definition of ciphertext anonymity, which we term SC-ANON-CCA and for which we prove the equivalence to SC-INDK-CCA from [15], before proving that SC-ANON-CCA is implied by SC-INVK-CCA. Even more surprising, we prove that SC-INVK-CCA implies SC-IND-CCA, that is key invisible signcryption schemes readily provide message confidentiality. Our analysis thus implies that key invisibility is strictly stronger than ciphertext anonymity and message confidentiality.

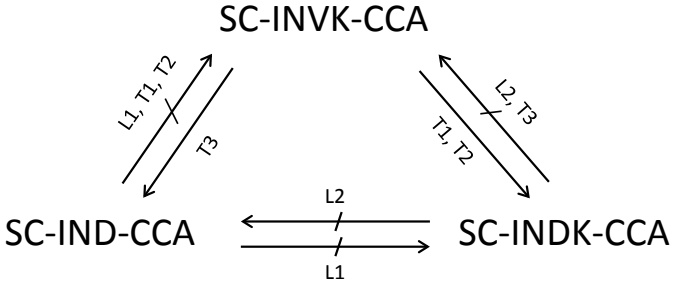

Fig. 1. Relationships among privacy notions for signcryption. An arrow denotes an implication while a barred arrow denotes a separation. T and L stand for Theorem and Lemma, respectively.

Key invisibility of "Sign-then-Encrypt". As observed in [15], parallel signcryption methods (incl. S&E and CtS&E) do not satisfy ciphertext anonymity — the recipient needs to know who is the sender in order to verify the signature. The key invisible signcryption scheme from [15], which has been revised in [9] following the analysis in [23], is a concrete construction based on bilinear maps and random oracles. As a second contribution we explore the key invisibility of the StE signcryption method, showing that it achieves SC-INVK-CCA (and by this SC-INDK-CCA and SC-IND-CCA) provided that the underlying public key encryption scheme satisfies two existing requirements, which are named *indistinguishability against adaptive chosen ciphertext attacks* (IND-CCA) and *indistinguishability of keys against adaptive chosen ciphertext attacks* (IK-CCA), respectively. It is well-known that Cramer-Shoup encryption scheme [8] offers both IND-CCA and IK-CCA security. In this way we readily obtain the first key invisible signcryption scheme in the standard model.

2 Preliminaries

2.1 Digital Signatures

SYNTAX. A signature scheme $\mathcal{S}$ comprises four efficient algorithms: $\mathcal{S} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Sig}, \mathsf{Ver})$. The setup algorithm Setup takes as input a security parameter 1^k and outputs the public parameters $\lambda_{\mathcal{S}}$. The key generation algorithm KGen takes as input $\lambda_{\mathcal{S}}$ and outputs a signing key sk and a verification key vk. The signing algorithm Sig takes as input a signing key sk and a message m from the associated message space $\mathcal{M}$, and outputs a signature $\sigma \leftarrow \mathsf{Sig}_{sk}(m)$. The verification algorithm Ver takes a message m, a signature σ and a verification key pk and outputs either a valid symbol $\top$ or an invalid symbol $\bot$. We require that $\mathsf{Ver}_{vk}(m, \mathsf{Sig}_{sk}(m)) = \top$, for any $m \in \mathcal{M}$.

SECURITY. We consider a standard security notion for signatures: *existential unforgeability under adaptive chosen message attacks* [13], denoted by $\mathsf{UF\text{-}CMA}$. Intuitively, we require that an adversary is not able to generate a signature on a new message on behalf of a target signer. We define the adversary $\mathcal{A}$'s advantage $\mathsf{Adv}^{\mathsf{UF\text{-}CMA}}_{\mathcal{S},\mathcal{A}}(k)$ as

$$\Pr\left[\mathcal{S}.\mathsf{Ver}_{vk}(m,\sigma) = \top \;\middle|\; \begin{array}{l} \lambda_S \leftarrow \mathsf{Setup}(1^k),\ (sk, vk) \leftarrow \mathcal{S}.\mathsf{KGen}(\lambda_S), \\ (m,\sigma) \leftarrow \mathcal{A}^{O_{\mathsf{Sig}}(\cdot)}(vk),\ m \notin \mathrm{Query}(\mathcal{A}, O_{\mathsf{Sig}}(\cdot)) \end{array}\right],$$

where $\mathcal{A}$ is allowed to make a sequence of queries to the signing oracle $O_{\mathsf{Sig}}(\cdot)$, and $\mathrm{Query}(\mathcal{A}, O_{\mathsf{Sig}}(\cdot))$ is the set of queries made by $\mathcal{A}$ to oracle $O_{\mathsf{Sig}}(\cdot)$. $\mathcal{S}$ is said to be $\mathsf{UF\text{-}CMA}$-secure, if the advantage function $\mathsf{Adv}^{\mathsf{UF\text{-}CMA}}_{\mathcal{S},\mathcal{A}}(k)$ is negligible in k for any PPT adversary $\mathcal{A}$.

2.2 Public-Key Encryption

SYNTAX. A public key encryption scheme $\mathcal{E}$ comprises four efficient algorithms: $\mathcal{E} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$. The setup algorithm Setup takes as input a security parameter 1^k and outputs the public parameters $\lambda_{\mathcal{E}}$. The key generation algorithm KGen takes as input $\lambda_{\mathcal{E}}$ and outputs a decryption key dk and an encryption key ek. The encryption algorithm Enc takes as input an encryption key ek and a message m from the associated message space $\mathcal{M}$, and outputs a ciphertext $c \leftarrow \mathsf{Enc}_{ek}(m)$. The decryption algorithm Dec takes a decryption key dk and a ciphertext c to return the corresponding message m; we write $m \leftarrow \mathsf{Dec}_{dk}(c)$. We require that $\mathsf{Dec}_{dk}(\mathsf{Enc}_{ek}(m)) = m$, for any $m \in \mathcal{M}$.

SECURITY. We consider *indistinguishability against adaptive chosen ciphertext attacks* [20], denoted by $\mathsf{IND\text{-}CCA}$, and *indistinguishability of keys against adaptive chosen ciphertext attacks* [5], denoted by $\mathsf{IK\text{-}CCA}$. Intuitively, $\mathsf{IND\text{-}CCA}$ means that given a properly generated encryption key, no adversary $\mathcal{A}$ can distinguish encryptions of any two-equal length messages m_0, m_1 under this key.

IND-CCA security captures strong message (data)-privacy property and guarantees that, given a challenge ciphertext, no valid information about the underlying message (plaintext, or data) will be leaked. On the other hand, IK-CCA captures strong key-privacy property. It means that given two randomly selected encryption keys ek_1 and ek_2, no adversary $\mathcal{A}$ can distinguish encryptions of a same message m under the two different keys. Given a challenge ciphertext, no valid information about the underlying key will be leaked in an IK-CCA-secure encryption scheme. For $b = 0, 1$ and an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, which runs in two stages of find and guess, consider the experiments

$$
\begin{aligned}
&\text{Experiment } \mathsf{Exp}^{\mathsf{IND\text{-}CCA},b}_{\mathcal{E},\mathcal{A}}(k):\\
&\quad \lambda_{\mathcal{E}} \leftarrow \mathcal{E}.\mathsf{Setup}(1^k)\\
&\quad (dk, ek) \leftarrow \mathcal{E}.\mathsf{KGen}(\lambda_{\mathcal{E}})\\
&\quad (m_0, m_1, \omega) \leftarrow \mathcal{A}_1^{\mathcal{D}_{dk}(\cdot)}(\lambda_{\mathcal{E}}, ek, \mathsf{find})\\
&\quad c_b \leftarrow \mathsf{Enc}_{ek}(m_b)\\
&\quad d \leftarrow \mathcal{A}_2^{\mathcal{D}_{dk}(\cdot)}(c_b, \omega, \mathsf{guess})
\end{aligned}
$$

$$
\begin{aligned}
&\text{Experiment } \mathsf{Exp}^{\mathsf{IK\text{-}CCA},b}_{\mathcal{E},\mathcal{A}}(k):\\
&\quad \lambda_{\mathcal{E}} \leftarrow \mathcal{E}.\mathsf{Setup}(1^k)\\
&\quad (dk_0, ek_0) \leftarrow \mathcal{E}.\mathsf{KGen}(\lambda_{\mathcal{E}}\\
&\quad (dk_1, ek_1) \leftarrow \mathcal{E}.\mathsf{KGen}(\lambda_{\mathcal{E}})\\
&\quad (m, \omega) \leftarrow \mathcal{A}_1^{\mathcal{D}_{dk_0}(\cdot),\mathcal{D}_{dk_1}(\cdot)}(\lambda_{\mathcal{E}}, ek_0, ek_1, \mathsf{find})\\
&\quad c_b \leftarrow \mathsf{Enc}_{ek_b}(m)\\
&\quad d \leftarrow \mathcal{A}_2^{\mathcal{D}_{dk_0}(\cdot),\mathcal{D}_{dk_1}(\cdot)}(c_b, \omega, \mathsf{guess})
\end{aligned}
$$

where $|m_0| = |m_1|$, ω is some state information and $\mathcal{A}$ is allowed to invoke the decryption oracle $\mathcal{D}_{dk}(\cdot)$ (or $\mathcal{D}_{dk_1}(\cdot)$ and $\mathcal{D}_{dk_2}(\cdot)$) at any point with the only restriction that c_b is not queried during the guess stage. We define the advantages $\mathsf{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathcal{E},\mathcal{A}}(k)$ and $\mathsf{Adv}^{\mathsf{IK\text{-}CCA}}_{\mathcal{E},\mathcal{A}}(k)$, respectively, as follows:

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathcal{E},\mathcal{A}}(k) &= \left|\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA},0}_{\mathcal{E},\mathcal{A}}(k) = 1] - \Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA},1}_{\mathcal{E},\mathcal{A}}(k) = 1]\right|\\
\mathsf{Adv}^{\mathsf{IK\text{-}CCA}}_{\mathcal{E},\mathcal{A}}(k) &= \left|\Pr[\mathsf{Exp}^{\mathsf{IK\text{-}CCA},0}_{\mathcal{E},\mathcal{A}}(k) = 1] - \Pr[\mathsf{Exp}^{\mathsf{IK\text{-}CCA},1}_{\mathcal{E},\mathcal{A}}(k) = 1]\right|.
\end{aligned}
$$

$\mathcal{E}$ is said to be IND-CCA (resp. IK-CCA) secure, if the advantage function $\mathsf{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathcal{E},\mathcal{A}}(k)$ (resp. $\mathsf{Adv}^{\mathsf{IK\text{-}CCA}}_{\mathcal{E},\mathcal{A}}(k)$) is negligible in k for any PPT adversary $\mathcal{A}$.

2.3 Signcryption Syntax

We will review the signcryption syntax used in [14, 15, 24]. A signcryption scheme is formalized by five PPT algorithms SC = (Setup, KeyGen, SignCrypt, UnSignCrypt, Verify). The setup algorithm generates public parameters $\lambda_{sc} \leftarrow$

$\mathsf{Setup}(1^k)$. Taking as input the public parameters λ_{sc}, the key-generation algorithm outputs a key pair $(sk_U, pk_U) \leftarrow \mathsf{KG_s}(\lambda_{sc})$. On input a message m from the associated message space $\mathcal{M}$, a private key sk_U, and a public key pk_R, the signcryption algorithm outputs a signcryption ciphertext $C \leftarrow \mathsf{SC.SignCrypt}(m, sk_U, pk_R)$. On input a private key sk_R and a signcryption ciphertext C, the unsigncryption algorithm $\mathsf{UnSignCrypt}$ (sk_R, C) outputs either a tuple (m, s, pk_U) where $m \in \mathcal{M}$, s is auxiliary non-repudiation information (allowing to convince a third party of the origin of the message) and pk_U is a public key, or a special symbol $\perp$ indicating failure. The verification algorithm $\mathsf{Verify}(m, s, pk_U)$ taking as input a message m, additional information s, and a public key pk_U, outputs either $\top$ if the additional information s authenticates the message m for the sender pk_U, or $\perp$ otherwise. The correctness requires that for any $m \in \mathcal{M}$, any correctly generated key pairs (sk_U, pk_U) and (sk_R, pk_R), we have $(m, s, pk_U) \leftarrow \mathsf{UnSignCrypt}(sk_R, \mathsf{SignCrypt}(m, sk_U, pk_R))$ and $\mathsf{Verify}(m, s, pk_U) = \perp$.

Remark 1. Note the slightly different syntax in comparison to [1]. The difference is that the unsigncryption algorithm takes as input sender's public key pk_S, receiver's secret key sk_R, and signcryption ciphertext C, and outputs either message m or $\perp$. In this paper, we will adopt the signcryption syntax reviewed above since we intend to study various privacy notions in which the sender's identity may be unknown prior to the execution of the unsigncryption algorithm.

3 Security Notions for Signcryption Schemes

The existing security notions cover four aspects: existential unforgeability against chosen-message attacks, indistinguishability against chosen ciphertext attacks, ciphertext anonymity and key invisibility, which we recall in the following.

3.1 Unforgeability

A fundamental notion for signcryption schemes is existential unforgeability against chosen-message attacks [1]. This property prevents the adversary from forging a signcryption ciphertext on a new message or with respect to a new receiver on behalf of the target sender, and is formalized in the following experiment

$$
\begin{aligned}
&\text{Experiment } \mathsf{Exp}^{\mathsf{UF\text{-}CMA}}_{\mathsf{SC},\mathcal{A}}(k):\\
&\quad \lambda_{sc} \leftarrow \mathsf{SC.Setup}(1^k)\\
&\quad (sk_U, pk_U) \leftarrow \mathsf{SC.KeyGen}(\lambda_{sc})\\
&\quad (C, sk_R, pk_R) \leftarrow \mathcal{A}^{\mathsf{SC.S}_{sk_U}(\cdot,\cdot),\mathsf{SC.D}_{sk_U}(\cdot)}(\lambda_{sc}, pk_U)\\
&\quad \text{success of } \mathcal{A} := [(m, s, pk_U) \leftarrow \mathsf{SC.UnSignCrypt}(sk_R, C)\\
&\qquad\qquad \wedge\ \mathsf{Verify}(m, s, pk_U) = \top\\
&\qquad\qquad \wedge\ (m, pk_R) \notin \mathit{Query}(\mathcal{A}, \mathsf{SC.S}_{sk_U}(\cdot,\cdot))]
\end{aligned}
$$

where the signcryption oracle $\mathsf{SC.S}_{sk_U}(\cdot,\cdot)$ takes as input (m', pk'_R) and outputs a signcryption ciphertext, the unsigncryption oracle $\mathsf{SC.D}_{sk_U}(\cdot)$ takes as input a signcryption ciphertext and outputs either $\perp$ or a tuple (m', s', pk'_U) such that $\mathsf{Verify}(m', s', pk'_U) = \top$, and $Query(\mathcal{A}, \mathsf{SC.S}_{sk_U}(\cdot,\cdot))$ is the set of queries made by $\mathcal{A}$ to oracle $\mathsf{SC.S}_{sk_U}(\cdot,\cdot)$.

Definition 1. *A signcryption scheme is existentially unforgeable against chosen-message attacks* (SC-UF-CMA)*, if for all PPT adversaries $\mathcal{A}$ the following advantage function is negligible in k:*

$$\mathsf{Adv}^{\mathsf{UF\text{-}CMA}}_{\mathsf{SC},\mathcal{A}}(k) := \Pr[\mathcal{A} \text{ success}].$$

We remark existence of a stronger notion named strong existentially unforgeability against chosen-message attacks (SC-SUF-CMA), c.f. [14, 15, 24], which requires that the challenge signcryption ciphertext C was not previously output by the signcryption oracle $\mathsf{SC.S}_{sk_U}(\cdot,\cdot)$ on input (m, pk_R). However, as pointed out in [1] and similar to the signature setting in [13], the conventional (i.e. non-strong) unforgeability is sufficient for most scenarios in practice.

3.2 Confidentiality

The notion of indistinguishability against chosen ciphertext attacks [15] captures confidentiality of messages. That is, given a signcryption ciphertext, no valid information about the message that was signcrypted will be exposed to an adversary without the designated receiver's private key. Formally, for $b = 0, 1$ we consider the following experiments

$$\begin{aligned}
&\text{Experiment } \mathsf{Exp}^{\mathsf{IND\text{-}CCA},b}_{\mathsf{SC},\mathcal{A}}(k):\\
&\quad \lambda_{sc} \leftarrow \mathsf{SC.Setup}(1^k)\\
&\quad (sk_U, pk_U) \leftarrow \mathsf{SC.KeyGen}(\lambda_{sc})\\
&\quad (m_0, m_1, sk_S, \omega) \leftarrow \mathcal{A}_1^{\mathsf{SC.S}_{sk_U}(\cdot,\cdot),\mathsf{SC.D}_{sk_U}(\cdot)}(\lambda_{sc}, pk_U)\\
&\quad C_b \leftarrow \mathsf{SC.SignCrypt}(m_b, sk_S, pk_U)\\
&\quad d \leftarrow \mathcal{A}_2^{\mathsf{SC.S}_{sk_U}(\cdot,\cdot),\mathsf{SC.D}_{sk_U}(\cdot)}(C_b, \omega)
\end{aligned}$$

where $|m_0| = |m_1|$, ω is some state information, and oracles $\mathsf{SC.S}_{sk_U}(\cdot,\cdot)$ and $\mathsf{SC.D}_{sk_U}(\cdot)$ are the same as in the previous experiment $\mathsf{Exp}^{\mathsf{UF\text{-}CMA}}_{\mathsf{SC},\mathcal{A}}(k)$ with the only limitation of $\mathcal{A}_2$ not querying the challenge ciphertext C_b to the unsigncryption oracle $\mathsf{SC.D}_{sk_U}(\cdot)$.

Definition 2. *A signcryption scheme is semantically secure against chosen ciphertext attacks* (SC-IND-CCA)*, if for all PPT adversaries $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ the following advantage function is negligible in k:*

$$\mathsf{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k) := |\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k) = 1] - \Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k) = 1]|.$$

3.3 Ciphertext Anonymity

Intuitively, a signcryption scheme has ciphertext anonymity property [15] if signcryption ciphertexts reveal no information about the identities of the sender and receiver. Formally, consider the following experiment

$$
\begin{aligned}
&\text{Experiment } \mathsf{Exp}^{\mathsf{INDK\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k):\\
&\quad \lambda_{sc} \leftarrow \mathsf{SC.Setup}(1^k)\\
&\quad (sk_{R,0}, pk_{R,0}) \leftarrow \mathsf{SC.KeyGen}(\lambda_{sc})\\
&\quad (sk_{R,1}, pk_{R,1}) \leftarrow \mathsf{SC.KeyGen}(\lambda_{sc})\\
&\quad \mathcal{O} := \{\mathsf{SC.S}_{sk_{R,0}}(\cdot,\cdot), \mathsf{SC.S}_{sk_{R,1}}(\cdot,\cdot), \mathsf{SC.D}_{sk_{R,0}}(\cdot), \mathsf{SC.D}_{sk_{R,1}}(\cdot)\}\\
&\quad (m, sk_{S,0}, sk_{S,1}, \omega) \leftarrow \mathcal{A}_1^{\mathcal{O}}(\lambda_{sc}, pk_{R,0}, pk_{R,1})\\
&\quad (b, b') \leftarrow \{0,1\}\\
&\quad C \leftarrow \mathsf{SC.SignCrypt}(m, sk_{S,b}, pk_{R,b'})\\
&\quad (d, d') \leftarrow \mathcal{A}_2^{\mathcal{O}}(C, \omega)
\end{aligned}
$$

where ω is some state information and $\mathcal{A}$ can have access to the signcryption and unsigncryption oracles at any point with the two limitations that $\mathcal{A}_2$ does not query C to the unsigncryption oracles $\mathsf{SC.D}_{sk_{R,0}}(\cdot)$ and $\mathsf{SC.D}_{sk_{R,1}}(\cdot)$.

Definition 3. *A signcryption scheme is said to satisfy ciphertext anonymity* (SC-INDK-CCA)*, if for all PPT adversaries* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *the following advantage function is negligible in* k*:*

$$\mathsf{Adv}^{\mathsf{INDK\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k) := |\Pr[(d,d') = (b,b')] - \frac{1}{4}|.$$

3.4 Key Invisibility

The notion of key invisibility for signcryption was formalized by Libert and Quisquater in [15]. It can be viewed as an extension of the invisibility concept proposed by Galbraith and Mao [12] for undeniable signatures. Intuitively, this notion captures that given a receiver, a specific signcryption ciphertext generated with respect to a chosen message, a chosen sender and a given receiver is indistinguishable to a random ciphertext uniformly chosen from the signcryption ciphertext space. Formally, for $b = 0, 1$ we consider the following experiments

$$
\begin{aligned}
&\text{Experiment } \mathsf{Exp}^{\mathsf{INVK\text{-}CCA},b}_{\mathsf{SC},\mathcal{A}}(k):\\
&\quad \lambda_{sc} \leftarrow \mathsf{SC.Setup}(1^k)\\
&\quad (sk_R, pk_R) \leftarrow \mathsf{SC.KeyGen}(\lambda_{sc})\\
&\quad (m, sk_S, \omega) \leftarrow \mathcal{A}_1^{\mathsf{SC.S}_{sk_R}(\cdot,\cdot), \mathsf{SC.D}_{sk_R}(\cdot)}(\lambda_{sc}, pk_R)\\
&\quad C_0 \leftarrow \mathsf{SC.SignCrypt}(sk_S, pk_R, m)\\
&\quad C_1 \leftarrow \mathcal{C}\\
&\quad d \leftarrow \mathcal{A}_2^{\mathsf{SC.S}_{sk_R}(\cdot,\cdot), \mathsf{SC.D}_{sk_R}(\cdot)}(C_b, \omega)
\end{aligned}
$$

where ω is some state information, $\mathcal{C}$ is the signcryption ciphertext space, C_1 is uniformly chosen at random from $\mathcal{C}$, and $\mathcal{A}$ can have access to the signcryption and unsigncryption oracles at any point with the two limitations that $\mathcal{A}_2$ does not query C_b to the unsigncryption oracle $\mathsf{SC.D}_{sk_R}(\cdot)$.

Definition 4. *A signcryption scheme is said to satisfy key invisibility* (SC-INVK-CCA)*, if for all PPT adversaries* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *the following advantage function is negligible in* k*:*

$$\mathsf{Adv}^{\mathsf{INVK\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k) := |\Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k) = 1] - \Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k) = 1]|.$$

4 Relations among Privacy Notions for Signcryption

We now define *anonymity*, an equivalent notion for ciphertext anonymity of signcryption schemes. This notion is conceptually simpler in comparison to *ciphertext anonimity* from [15] in that the adversary only needs to distinguish between two cases, depending on a single bit $b = 0, 1$, rather than between four cases in [15]. Formally, we consider the following experiments

$$\begin{aligned}
&\text{Experiment } \mathsf{Exp}^{\mathsf{ANON\text{-}CCA},b}_{\mathsf{SC},\mathcal{A}}(k):\\
&\quad \lambda_{sc} \leftarrow \mathsf{SC.Setup}(1^k)\\
&\quad (sk_{R,0}, pk_{R,0}) \leftarrow \mathsf{SC.KeyGen}(\lambda_{sc})\\
&\quad (sk_{R,1}, pk_{R,1}) \leftarrow \mathsf{SC.KeyGen}(\lambda_{sc})\\
&\quad \mathcal{O} := \{\mathsf{SC.S}_{sk_{R,0}}(\cdot,\cdot), \mathsf{SC.S}_{sk_{R,1}}(\cdot,\cdot), \mathsf{SC.D}_{sk_{R,0}}(\cdot), \mathsf{SC.D}_{sk_{R,1}}(\cdot)\}\\
&\quad (m, sk_{S,0}, sk_{S,1}, \omega) \leftarrow \mathcal{A}_1^{\mathcal{O}}(\lambda_{sc}, pk_{R,0}, pk_{R,1})\\
&\quad C_b \leftarrow \mathsf{SC.SignCrypt}(m, sk_{S,b}, pk_{R,b})\\
&\quad d \leftarrow \mathcal{A}_2^{\mathcal{O}}(C_b, \omega)
\end{aligned}$$

where ω is some state information and $\mathcal{A}$ can have access to the signcryption and unsigncryption oracles at any point with the two limitations that $\mathcal{A}_2$ does not query C_b to the unsigncryption oracles $\mathsf{SC.D}_{sk_{R,0}}(\cdot)$ and $\mathsf{SC.D}_{sk_{R,1}}(\cdot)$.

Definition 5. *A signcryption scheme is said to satisfy anonymity* (SC-ANON-CCA)*, if for all PPT adversaries* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$*, the advantage function is negligible in* k*:*

$$\mathsf{Adv}^{\mathsf{ANON\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k) := |\Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k) = 1] - \Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k) = 1]|.$$

We now show that ciphertext anonymity and anonymity are equivalent.

Theorem 1 (SC-INDK-CCA $\Leftrightarrow$ SC-ANON-CCA). *For signcryption schemes, anonymity is equivalent to ciphertext anonymity.*

Proof of Theorem 1 is presented in the full version of this paper. □

4.1 Separation between Ciphertext Anonymity and SC-IND-CCA

Intuitively, ciphertext anonymity captures identity privacy and indistinguishability against chosen ciphertext attacks captures message privacy. The goals of ciphertext anonymity and indistinguishability against chosen ciphertext attacks are orthogonal. Formally, Lemmas 1 and 2 proven in the full version of this paper, separate the two notions.

Lemma 1 (SC-IND-CCA $\not\Rightarrow$ SC-INDK-CCA). *Let* $\mathsf{SC} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{SignCrypt}, \mathsf{UnSignCrypt})$ *be a signcryption scheme. If the scheme* SC *satisfies indistinguishability against chosen ciphertext attacks, then it may not satisfy ciphertext anonymity.*

Lemma 2 (SC-INDK-CCA $\not\Rightarrow$ SC-IND-CCA). *Let* $\mathsf{SC} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{SignCrypt}, \mathsf{UnSignCrypt})$ *be a signcryption scheme. If the scheme* SC *satisfies ciphertext anonymity, then it may not satisfy indistinguishability against chosen ciphertext attacks.*

4.2 Relationship between Key Invisibility and Ciphertext Anonymity

Next, we investigate the relationship between key invisibility and ciphertext anonymity. We shall use anonymity instead of ciphertext anonymity in our analysis, as these two are equivalent by Theorem 1.

Theorem 2 (SC-INVK-CCA $\Rightarrow$ SC-ANON-CCA). *Let* SC *be a signcryption scheme. If the scheme* SC *satisfies key invisibility, then it satisfies anonymity.*

Proof of Theorem 2 is presented in the full version of this paper. □

Note that Libert and Quisquater [15] were only able to prove implication of ciphertext anonymity by key invisibility for a class of signcryption schemes satisfying a particular property, namely that for a given message and a given sender's private key, the output of the signcryption algorithm must be uniformly distributed in the ciphertext space when the receiver's public key is random. Our results in Theorems 1 and 2 lift this restriction.

4.3 Relationship between Key Invisibility and SC-IND-CCA

Our next result shows that key invisibility, which originally was viewed as a notion for protecting privacy of user identities [15], is in fact a much stronger notion that implies indistinguishability against chosen ciphertext attacks.

Theorem 3 (SC-INVK-CCA $\Rightarrow$ SC-IND-CCA). *Let* SC *be a signcryption scheme. If the scheme* SC *satisfies key invisibility, then it satisfies indistinguishability against chosen ciphertext attacks.*

Proof of Theorem 3 is presented in the full version of this paper. □

From Theorem 1, Lemma 1, Lemma 2, Theorem 2 and Theorem 3, we can safely conclude that key invisibility is strictly stronger than both indistinguishability against chosen ciphertext attacks and ciphertext anonymity.

5 Sign-then-Encrypt Generic Construction

In this section, we revisit the generic construction of signcryption schemes based on the sign-then-encrypt method [1, 2]. We show that the resulting signcryption schemes can achieve key invisibility when appropriate encryption schemes are employed.

5.1 Scheme

Let $\mathcal{S} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Sig}, \mathsf{Ver})$ be a signature scheme and $\mathcal{E} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme. Signcryption schemes based on the sign-then-encrypt method can be constructed as follows:

- $\mathsf{Setup}(1^k)$: On input a security parameter k, this algorithm runs $\lambda_{\mathcal{S}} \leftarrow \mathcal{S}.\mathsf{Setup}(1^k)$ and $\lambda_{\mathcal{E}} \leftarrow \mathcal{E}.\mathsf{Setup}(1^k)$, respectively. The public parameters are set as $\lambda_{sc} := (\lambda_{\mathcal{S}}, \lambda_{\mathcal{E}})$.
- $\mathsf{KeyGen}(\lambda_{sc})$: The user U_i runs $\mathcal{S}.\mathsf{KGen}(\lambda_{\mathcal{S}}) \rightarrow (sk_i, vk_i)$ and $\mathcal{E}.\mathsf{KGen}(\lambda_{\mathcal{E}}) \rightarrow (dk_i, ek_i)$, respectively. The secret and public key pair is set as $(sk_{U_i}, pk_{U_i}) := ((sk_i, dk_i), (vk_i, ek_i))$.
- $\mathsf{SignCrypt}(m, sk_{U_i}, pk_{U_j})$: To signcrypt a message m for the receiver U_j, U_i first produces a signature σ on $m||pk_{U_j}$, i.e., $\sigma \leftarrow \mathcal{S}.\mathsf{Sig}_{sk_i}(m||pk_{U_j})$, and then encrypts $m||\sigma||pk_{U_i}$ under receiver U_j's encryption key, i.e. $c \leftarrow \mathcal{E}.\mathsf{Enc}_{ek_j}(m||\sigma||pk_{U_i})$. The signcryption ciphertext is set as $C := c$.
- $\mathsf{UnSignCrypt}(sk_{U_j}, C)$: On receiving a signcryption ciphertext C, receiver U_j firstly decrypts it using its own decryption key dk_j, i.e., $m||\sigma||pk_{U_i} \leftarrow \mathcal{E}.\mathsf{Dec}_{dk_j}(C)$, and then checks if $\mathcal{S}.\mathsf{Ver}_{vk_i}\ (m||pk_{U_j}, \sigma) = \top$. If so, it outputs (m, s, pk_{U_i}) where $s = (pk_{U_j}, \sigma)$; otherwise, it returns $\perp$.
- $\mathsf{Verify}(m, s, pk_{U_i})$: This algorithm parses s and pk_{U_i} as (pk_{U_j}, σ) and (vk_i, ek_i), respectively, and outputs $\mathcal{S}.\mathsf{Ver}_{vk_i}(m||pk_{U_j}, \sigma)$.

5.2 Security of the Generic Construction

From the relations discussed in Section 4, we only need to show that the above generic construction results in signcryption schemes that are existentially unforgeable against chosen-message attacks and satisfy key invisibility. The former requirement has already been proven in [1], who stated the following theorem:

Theorem 4 ([1]). *Let* SC *be the above generic signcrypiton scheme. If the signature scheme* $\mathcal{S}$ *is* UF-CMA*-secure, then* SC *is existentially unforgeable against chosen-message attacks.*

We thus focus on key invisibility, for which we need to specify how to uniformly sample signcryption ciphertexts from the ciphertext space. Here we will adopt the very natural method for uniform sampling, i.e., uniformly and independently choosing a message $m \in M$, a sender's secret key sk_{U_i}, and a receiver's public key pk_{U_j}, and returning a signcryption ciphertext $C \leftarrow \mathsf{SC.SignCrypt}(m, sk_{U_i}, pk_{U_j})$.

Theorem 5. *Let $\mathcal{S}$ be a signature scheme, $\mathcal{E}$ be a public-key encryption scheme that is both* IND-CCA*-secure and* IK-CCA*-secure. Then the above generic signcrypiton scheme* SC *satisfies key invisibility.*

Proof. To show the security, we first define two games, and then show in Claims 1 and 2 that no adversary $\mathcal{A}$ can break the key invisibility property of SC.

Game 0. This is the real experiment between the challenger and an adversary $\mathcal{A}$. This means that the challenger firstly correctly generates the target receiver's key pairs $(sk_R, pk_R) := ((sk_0, dk_0), (vk_0, ek_0))$, forwards pk_R to the adversary $\mathcal{A}$, and then provides accesses to signcryption oracle $\mathsf{SC.S}_{sk_R}(\cdot,\cdot)$ and unsigncryption oracle $\mathsf{SC.D}_{sk_R}(\cdot)$. In the challenge phase, after $\mathcal{A}$ submits $(m^*, sk_S = (sk_1, dk_1))$, the challenger randomly flips a coin $b \in \{0,1\}$. If $b = 0$, the challenger produces a signature σ_0 on $m^*||pk_R$ under the signing key sk_1, i.e., $\sigma_0 \leftarrow \mathcal{S}.\mathsf{Sig}_{sk_1}(m^*||pk_R)$, encrypts $m^*||\sigma_0||pk_S$ under the receiver's encryption key, i.e. $C_0 \leftarrow \mathcal{E}.\mathsf{Enc}_{ek_0}(m^*||\sigma_0||pk_S)$, and returns C_0 to $\mathcal{A}$. If $b = 1$, the challenger independently and uniformly chooses $m' \in \mathcal{M}$, a sender's secret key $sk'_S := (sk'_1, dk'_1)$ and a receiver's public key $pk'_R := (vk'_0, ek'_0)$, produces a signature σ_1 on $m'||pk'_R$, i.e., $\sigma_1 \leftarrow \mathcal{S}.\mathsf{Sig}_{sk'_1}(m'||pk'_R)$, encrypts $m'||\sigma_1||pk'_S$ under the receiver's encryption key, i.e. $C_1 \leftarrow \mathcal{E}.\mathsf{Enc}_{ek'_0}(m'||\sigma_1||pk'_S)$, and returns C_1 to $\mathcal{A}$. Besides, the challenger provides access to signcryption oracle $\mathsf{SC.S}_{sk_R}(\cdot,\cdot)$ and unsigncryption oracle $\mathsf{SC.D}_{sk_R}(\cdot)$.

Game 1. This is the same as Game 0, with the exception that in the challenge phase, the challenger computes $C_1 \leftarrow \mathcal{E}.\mathsf{Enc}_{ek_0}(m'||\sigma_1||pk'_S)$, and returns C_1 to $\mathcal{A}$ when $b = 1$.

Next we link the probability that $\mathcal{A}$ wins in Game 0 and Game 1. Let S_1 be the advantage that $\mathcal{A}$ wins in Game 1. Thus $\Pr[S_1] = |\Pr[\mathsf{Exp}^{\mathbf{Game\ 1},0}_{\mathsf{SC},\mathcal{A}}(k) = 1] - \Pr[\mathsf{Exp}^{\mathbf{Game\ 1},1}_{\mathsf{SC},\mathcal{A}}(k) = 1]|$, where $\mathsf{Exp}^{\mathbf{Game\ 1},b}_{\mathsf{SC},\mathcal{A}}(k)$ is the output of $\mathcal{A}$ in Game 1 when the challenge ciphertext is C_b.

Claim 1

$$|\mathsf{Adv}^{\mathsf{INVK\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k) - \Pr[S_1]| = 2 \cdot \mathsf{Adv}^{\mathsf{IK\text{-}CCA}}_{\mathcal{E},\mathcal{B}}(k), \tag{1}$$

where $\mathsf{Adv}^{\mathsf{IK\text{-}CCA}}_{\mathcal{E},\mathcal{B}}(k)$ is the advantage of an adversary $\mathcal{B}$ that breaks the IK-CCA security of the encryption scheme $\mathcal{E}$.

We show that any difference between $\mathsf{Adv}^{\mathsf{INVK\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k)$ and $\Pr[S_1]$ can be parlayed into an algorithm $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ that breaks the IK-CCA security of the encryption scheme $\mathcal{E}$. Recall that $\mathcal{B}_1$ gets $(\lambda_{\mathcal{E}}, ek, ek')$ as input and has access to decryption oracles $\mathcal{D}_{dk}(\cdot)$ and $\mathcal{D}_{dk'}(\cdot)$. $\mathcal{B}_1$ runs $\lambda_{\mathcal{S}} \leftarrow \mathcal{S}.\mathsf{Setup}(1^k)$, $\mathcal{S}.\mathsf{KGen}(\lambda_{\mathcal{S}}) \rightarrow$

(sk_0, vk_0) and sets $\lambda_{sc} := (\lambda_{\mathcal{S}}, \lambda_{\mathcal{E}})$ and $pk_R := (vk_0, ek)$. $\mathcal{B}_1$ runs $\mathcal{A}_1$ as a subroutine by forwarding (λ_{sc}, pk_R).

When $\mathcal{A}_1$ makes a signcryption query $(m, pk_U = (vk_U, ek_U))$ to $\mathsf{SC.S}_{sk_R}(\cdot,\cdot)$, $\mathcal{B}_1$ first produces a signature σ on $m||pk_U$ under the signing key sk_0, i.e., $\sigma \leftarrow \mathcal{S}.\mathsf{Sig}_{sk_0}(m||pk_U)$, and then encrypts $m||\sigma||pk_R$ under the encryption key ek_U, i.e. $c \leftarrow \mathcal{E}.\mathsf{Enc}_{ek_U}(m||\sigma||pk_R)$. The signcryption ciphertext is set as $C := c$, and returned to $\mathcal{A}_1$ as the reply. When $\mathcal{A}_1$ makes a unsigncryption query C to $\mathsf{SC.D}_{sk_R}(\cdot)$, $\mathcal{B}_1$ submits C to its own decryption oracle $\mathcal{D}_{dk}(\cdot)$. If the reply is not of the form $m||\sigma||pk_U$ where pk_U is a public key, then $\mathcal{B}_1$ returns $\perp$ to $\mathcal{A}_1$. Otherwise, $\mathcal{B}_1$ decomposes pk_U as (vk_U, ek_U), and further checks whether $\mathcal{S}.\mathsf{Ver}_{vk_U}(m||pk_R, \sigma) = \top$. If so, $\mathcal{B}_1$ returns $(m, (pk_R, \sigma), pk_U)$ to $\mathcal{A}_1$, and otherwise $\perp$ is returned.

At some time, $\mathcal{A}_1$ submits $(m^*, sk_S = (sk_1, dk_1))$. B_1 randomly flips a coin $\tilde{b} \in \{0, 1\}$. If $\tilde{b} = 0$, $\mathcal{B}$ first produces a signature σ_0 on $m^*||pk_R$ under the signing key sk_1, i.e., $\sigma_0 \leftarrow \mathcal{S}.\mathsf{Sig}_{sk_1}(m^*||pk_R)$, encrypts $m^*||\sigma_0||pk_S$ under the receiver's encryption key, i.e. $C_0 \leftarrow \mathcal{E}.\mathsf{Enc}_{ek}(m^*||\sigma_0||pk_S)$, and returns C_0 to $\mathcal{A}$. If $\tilde{b} = 1$, $\mathcal{B}$ independently and uniformly chooses $m' \in \mathcal{M}$, a sender's secret key $sk'_S := (sk'_1, dk'_1)$ and a public verification key vk'_0, sets $pk'_R := (vk'_0, ek')$, produces a signature σ_1 on $m'||pk'_R$ using the signing key sk'_1, i.e., $\sigma_1 \leftarrow \mathcal{S}.\mathsf{Sig}_{sk'_1}(m'||pk'_R)$, and submits $m'||\sigma_1||pk'_S$ where pk'_S is the corresponding public key of sk'_S to its own challenger. Let C_1 denote the reply of $\mathcal{B}$'s own challenger. $\mathcal{B}$ returns C_1 to $\mathcal{A}$. $\mathcal{B}_2$ simulates the oracles in the same way as $\mathcal{B}_1$ did.

Note that $\mathcal{A}_2$ never makes an unsigncryption query C_b where $b \in \{0, 1\}$ to $\mathsf{SC.D}_{sk_R}(\cdot)$, thus $\mathcal{B}_2$ does not make the query C_b to its decryption oracles $\mathcal{D}_{dk}(\cdot)$ or $\mathcal{D}_{dk'}(\cdot)$. Finally $\mathcal{A}_2$ outputs a bit d. $\mathcal{B}_2$ outputs d when $\tilde{b} = 1$, and returns failure when $\tilde{b} = 0$. When C_1 is the encryption of $m'||\sigma_1||pk'_S$ under ek, the environment simulated by $\mathcal{B}$ is exactly the same as in Game 1. While C_1 is the encryption of $m'||\sigma_1||pk'_S$ under ek', the environment simulated by $\mathcal{B}$ is exactly the same as in Game 0. Thus we have

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{IK\text{-}CCA}}_{\mathcal{E},\mathcal{B}}(k) &= \big|\Pr[\mathsf{Exp}^{\mathsf{IK\text{-}CCA},0}_{\mathcal{E},\mathcal{B}}(k) = 1] - \Pr[\mathsf{Exp}^{\mathsf{IK\text{-}CCA},1}_{\mathcal{E},\mathcal{B}}(k) = 1]\big| \\
&= \big|\Pr[\tilde{b} = 1] \cdot \Pr[\mathsf{Exp}^{\mathbf{Game\ 1},1}_{\mathsf{SC},\mathcal{A}}(k) = 1] \\
&\quad - \Pr[\tilde{b} = 1] \cdot \Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k) = 1]\big| \\
&= \big|(\frac{1}{2} \cdot \Pr[\mathsf{Exp}^{\mathbf{Game\ 1},0}_{\mathsf{SC},\mathcal{A}}(k) = 1] - \frac{1}{2} \cdot \Pr[\mathsf{Exp}^{\mathbf{Game\ 1},1}_{\mathsf{SC},\mathcal{A}}(k) = 1]) \\
&\quad - \frac{1}{2} \cdot \Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k) = 1] \\
&\quad + \frac{1}{2} \cdot \Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k) = 1]\big| \qquad (2) \\
&= \frac{1}{2} \cdot \big|\Pr[S_1] - \mathsf{Adv}^{\mathsf{INVK\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k)\big|.
\end{aligned}
$$

Equation (2) follows from the fact that $\Pr[\mathsf{Exp}^{\mathbf{Game\ 1},0}_{\mathsf{SC},\mathcal{A}}(k) = 1]$ equals to $\Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k) = 1]$, as the experiments are exactly the same.

Claim 2

$$\Pr[S_1] \leq \mathsf{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathcal{E},\mathcal{C}}(k), \tag{3}$$

where $\mathsf{Adv}^{\mathsf{IK\text{-}CCA}}_{\mathcal{E},\mathcal{C}}(k)$ is the advantage of an adversary $\mathcal{C}$ that breaks the IND-CCA security of the encryption scheme $\mathcal{E}$.

To show this, we build an algorithm $\mathcal{C}$ that employs the adversary $\mathcal{A}$ in Game 1 to break the IND-CCA security of the encryption scheme $\mathcal{E}$. Recall that $\mathcal{C}$ gets $(\lambda_{\mathcal{E}}, ek)$ as input and has access to a decryption oracle $\mathcal{D}_{dk}(\cdot)$. $\mathcal{C}$ runs $\lambda_{\mathcal{S}} \leftarrow \mathcal{S}.\mathsf{Setup}(1^k)$, $\mathcal{S}.\mathsf{KGen}(\lambda_{\mathcal{S}}) \rightarrow (sk_0, vk_0)$ and sets $\lambda_{sc} := (\lambda_{\mathcal{S}}, \lambda_{\mathcal{E}})$ and $pk_R := (vk_0, ek)$. $\mathcal{C}$ runs $\mathcal{A}_1$ as a subroutine by forwarding (λ_{sc}, pk_R).

When $\mathcal{A}_1$ makes a signcryption query $(m, pk_U = (vk_U, ek_U))$ to $\mathsf{SC.S}_{sk_R}(\cdot,\cdot)$, $\mathcal{C}$ first produces a signature σ on $m||pk_U$, i.e., $\sigma \leftarrow \mathcal{S}.\mathsf{Sig}_{sk_0}(m||pk_U)$, and then encrypts $m||\sigma||pk_R$ under the encryption key ek_U, i.e. $c \leftarrow \mathcal{E}.\mathsf{Enc}_{ek_U}(m||\sigma||pk_R)$. The signcryption ciphertext is set as $C := c$, and returned to $\mathcal{A}_1$ as the reply. When $\mathcal{A}_1$ makes a unsigncryption query C to $\mathsf{SC.D}_{sk_R}(\cdot)$, $\mathcal{C}$ submits C to its own decryption oracle $\mathcal{D}_{dk}(\cdot)$. If the reply is not of the form $m||\sigma||pk_U$ where pk_U is a public key, then $\mathcal{C}$ returns $\perp$ to $\mathcal{A}_1$. Otherwise, $\mathcal{C}$ decomposes pk_U as (vk_U, ek_U), and further checks whether $\mathcal{S}.\mathsf{Ver}_{vk_U}(m||pk_R, \sigma) = \top$. If so, $\mathcal{C}$ returns $(m, (pk_R, \sigma), pk_U)$ to $\mathcal{A}_1$, and otherwise $\perp$ is returned.

At some time, $\mathcal{A}_1$ submits $(m^*, sk_S = (sk_1, dk_1))$. $\mathcal{C}$ first produces a signature σ_0 on $m^*||pk_R$ under the signing key sk_1, i.e., $\sigma_0 \leftarrow \mathcal{S}.\mathsf{Sig}_{sk_1}(m^*||pk_R)$. Then $\mathcal{C}$ independently and uniformly chooses $m' \in \mathcal{M}$, a sender's secret key $sk'_S := (sk'_1, dk'_1)$ and a receiver's public pk'_R, produces a signature σ_1 on $m'||pk'_R$ under the signing key sk'_1, i.e., $\sigma_1 \leftarrow \mathcal{S}.\mathsf{Sig}_{sk'_1}(m'||pk'_R)$. $\mathcal{C}$ sets $\bar{m}_0 := m^*||\sigma_0||pk_S$, $\bar{m}_1 := m'||\sigma_1||pk'_S$ where pk_S and pk'_S are the corresponding public keys of sk_S and sk'_S respectively, and submits $\bar{m}_0$ and $\bar{m}_1$ to its own challenger. Let C_b denote the reply of $\mathcal{C}$'s own challenger. $\mathcal{C}$ returns C_b to $\mathcal{A}$. $\mathcal{C}$ then simulates the oracles in the same way as it did before.

Note that $\mathcal{A}_2$ never makes an unsigncryption query C_b to $\mathsf{SC.D}_{sk_R}(\cdot)$, thus $\mathcal{B}_2$ does not make the query C_b to its decryption oracle $\mathcal{D}_{dk}(\cdot)$. Finally $\mathcal{A}_2$ outputs a bit d. $\mathcal{C}$ outputs d. The environment simulated by $\mathcal{C}$ is exactly the same as in Game 1. Thus we have $\mathsf{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathcal{E},\mathcal{C}}(k) = \Pr[S_1]$.

As a sequence of equations (1), (3) gained above, we have $\mathsf{Adv}^{\mathsf{INVK\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k) \leq 2 \cdot \mathsf{Adv}^{\mathsf{IK\text{-}CCA}}_{\mathcal{E},\mathcal{B}}(k) + \mathsf{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathcal{E},\mathcal{C}}(k)$. This concludes the proof. □

6 Conclusion

In this paper, we first revisited the existing privacy notions of signcryption schemes, namely indistinguishability against chosen ciphertext attacks, ciphertext anonymity and key invisibility. We demonstrated the separation between indistinguishability against chosen ciphertext attacks and ciphertext anonymity, and showed that both notions are implied by key invisibility. Finally we proposed the first generic construction for key invisible signcryption schemes in the standard model.

References

1. An, J.H., Dodis, Y., Rabin, T.: On the security of joint signature and encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 83–107. Springer, Heidelberg (2002)
2. Au, J.H., Rabin, T.: Security for Signcryption: The Two-User Model. In: Dent, A., Zheng, Y. (eds.) Practical Signcryption, Information Security and Cryptography. Springer (2010)
3. Baek, J., Steinfeld, R., Zheng, Y.: Formal proofs for the security of signcryption. In: Naccache, D., Paillier, P. (eds.) PKC 2002. LNCS, vol. 2274, pp. 80–98. Springer, Heidelberg (2002)
4. Bao, F., Deng, R.H.: A Signcryption Scheme with Signature Directly Verifiable by Public Key. In: Imai, H., Zheng, Y. (eds.) PKC 1998. LNCS, vol. 1431, pp. 55–59. Springer, Heidelberg (1998)
5. Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-privacy in public-key encryption. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 566–582. Springer, Heidelberg (2001)
6. Bellare, M., Namprempre, C.: Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 531–545. Springer, Heidelberg (2000)
7. Boyen, X.: Multipurpose identity-based signcryption – a Swiss Army knife for identity-based cryptography. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 383–399. Springer, Heidelberg (2003), `http://www.cs.stanford.edu/~xb/crypto03/`
8. Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13–25. Springer, Heidelberg (1998)
9. Dent, A.W., Zheng, Y. (eds.): Practical Signcryption. Springer (2010)
10. Dent, A.W., Fischlin, M., Manulis, M., Stam, M., Schröder, D.: Confidential Signatures and Deterministic Signcryption. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 462–479. Springer, Heidelberg (2010)
11. Dodis, Y., Freedman, M.J., Jarecki, S., Walfish, S.: Optimal Signcryption from Any Trapdoor Permutation. Cryptology ePrint Archive, Report 2004/020 (2004), `http://eprint.iacr.org/`
12. Galbraith, S.D., Mao, W.: Invisibility and anonymity of undeniable and confirmer signatures. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 80–97. Springer, Heidelberg (2003)
13. Goldwasser, S., Micali, S., Rivest, R.L.: A digital signature scheme secure against adaptive chosen-message attacks. SIAM J. Comput. 17(2), 281–308 (1988)
14. Li, C.K., Yang, G., Wong, D.S., Deng, X., Chow, S.S.M.: An efficient signcryption scheme with key privacy. In: López, J., Samarati, P., Ferrer, J.L. (eds.) EuroPKI 2007. LNCS, vol. 4582, pp. 78–93. Springer, Heidelberg (2007)
15. Libert, B., Quisquater, J.-J.: Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 187–200. Springer, Heidelberg (2004)
16. Libert, B., Quisquater, J.-J.: Improved Signcryption from q-Diffie-Hellman Problems. In: Blundo, C., Cimato, S. (eds.) SCN 2004. LNCS, vol. 3352, pp. 220–234. Springer, Heidelberg (2005)
17. Malone-Lee, J.: A General Construction for Simultaneous Signing and Encrypting. In: Smart, N.P. (ed.) Cryptography and Coding 2005. LNCS, vol. 3796, pp. 116–135. Springer, Heidelberg (2005)

18. Malone-Lee, J., Mao, W.: Two Birds One Stone: Signcryption Using RSA. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 211–225. Springer, Heidelberg (2003)
19. Pieprzyk, J., Pointcheval, D.: Parallel Authentication and Public-Key Encryption. In: Safavi-Naini, R., Seberry, J. (eds.) ACISP 2003. LNCS, vol. 2727, pp. 387–401. Springer, Heidelberg (2003)
20. Rackoff, C., Simon, D.R.: Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 433–444. Springer, Heidelberg (1992)
21. Shin, J.-B., Lee, K., Shim, K.: New DSA-Verifiable Signcryption Schemes. In: Lee, P.J., Lim, C.H. (eds.) ICISC 2002. LNCS, vol. 2587, pp. 35–47. Springer, Heidelberg (2003)
22. Steinfeld, R., Zheng, Y.: A Signcryption Scheme Based on Integer Factorization. In: Okamoto, E., Pieprzyk, J.P., Seberry, J. (eds.) ISW 2000. LNCS, vol. 1975, pp. 308–322. Springer, Heidelberg (2000)
23. Tan, C.-H.: On the security of signcryption scheme with key privacy. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E88-A(4), 1093–1095 (2005)
24. Yang, G., Wong, D.S., Deng, X.: Analysis and improvement of a signcryption scheme with key privacy. In: Zhou, J., López, J., Deng, R.H., Bao, F. (eds.) ISC 2005. LNCS, vol. 3650, pp. 218–232. Springer, Heidelberg (2005)
25. Yum, D.H., Lee, P.J.: New Signcryption Schemes Based on KCDSA. In: Kim, K.-C. (ed.) ICISC 2001. LNCS, vol. 2288, pp. 305–317. Springer, Heidelberg (2002)
26. Zheng, Y.: Digital signcryption or how to achieve cost (Signature & encryption) << cost(Signature) + cost(Encryption). In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 165–179. Springer, Heidelberg (1997)