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
Email: yw990@uowmail.uow.edu.au
{wsusilo, aau}@uow.edu.au
[2]Department of Computing, University of Surrey, United Kingdom
Email: 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. 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.

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

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.

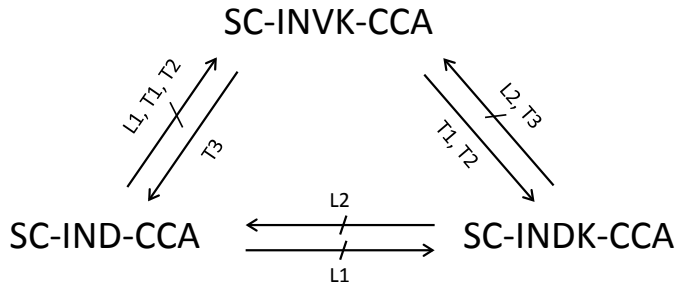

Fig. 1. Relationships among privacy notions for signcryption. An arrow denotes an implication while a barred arrow denotes a separation. T and L stand for Theorem and Lemma, respectively.

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 UF-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 UF-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 IND-CCA, and *indistinguishability of keys against adaptive chosen ciphertext attacks* [5],

denoted by IK-CCA. Intuitively, IND-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

Experiment $\mathsf{Exp}^{\mathsf{IND\text{-}CCA},b}_{\mathcal{E},\mathcal{A}}(k)$:	Experiment $\mathsf{Exp}^{\mathsf{IK\text{-}CCA},b}_{\mathcal{E},\mathcal{A}}(k)$:
$\lambda_{\mathcal{E}} \leftarrow \mathcal{E}.\mathsf{Setup}(1^k)$	$\lambda_{\mathcal{E}} \leftarrow \mathcal{E}.\mathsf{Setup}(1^k)$
$(dk, ek) \leftarrow \mathcal{E}.\mathsf{KGen}(\lambda_{\mathcal{E}})$	$(dk_0, ek_0) \leftarrow \mathcal{E}.\mathsf{KGen}(\lambda_{\mathcal{E}});\ (dk_1, ek_1) \leftarrow \mathcal{E}.\mathsf{KGen}(\lambda_{\mathcal{E}})$
$(m_0, m_1, \omega) \leftarrow \mathcal{A}_1^{\mathcal{D}_{dk}(\cdot)}(\lambda_{\mathcal{E}}, ek, \mathsf{find})$	$(m, \omega) \leftarrow \mathcal{A}_1^{\mathcal{D}_{dk_0}(\cdot),\mathcal{D}_{dk_1}(\cdot)}(\lambda_{\mathcal{E}}, ek_0, ek_1, \mathsf{find})$
$c_b \leftarrow \mathsf{Enc}_{ek}(m_b)$	$c_b \leftarrow \mathsf{Enc}_{ek_b}(m)$
$d \leftarrow \mathcal{A}_2^{\mathcal{D}_{dk}(\cdot)}(c_b, \omega, \mathsf{guess})$	$d \leftarrow \mathcal{A}_2^{\mathcal{D}_{dk_0}(\cdot),\mathcal{D}_{dk_1}(\cdot)}(c_b, \omega, \mathsf{guess})$

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:

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

$\mathcal{E}$ 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 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 $\mathsf{Verify}(m, s, pk_U) = \top$.

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 $\mathit{Query}(\mathcal{A}, \mathsf{SC.S}_{sk_U}(\cdot,\cdot))$ 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

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

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

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

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 Appendix A. □

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 Appendix B, 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* 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* 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* SC *satisfies key invisibility, then it satisfies anonymity.*

Proof of Theorem 2 is presented in Appendix C. □

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* SC *satisfies key invisibility, then it satisfies indistinguishability against chosen ciphertext attacks.*

Proof of Theorem 3 is presented in Appendix D. □

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. 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 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 $\Pr[S_1] = |\Pr[\mathsf{Exp}^{\textbf{Game 1},0}_{\mathsf{SC},\mathcal{A}}(k) = 1] - \Pr[\mathsf{Exp}^{\textbf{Game 1},1}_{\mathsf{SC},\mathcal{A}}(k) = 1]|$, where $\mathsf{Exp}^{\textbf{Game 1},b}_{\mathsf{SC},\mathcal{A}}(k)$ 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 $\mathsf{IK\text{-}CCA}$ 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 $\mathsf{IK\text{-}CCA}$ 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

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

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

Claim 2

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

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 $\mathsf{SC}.\mathsf{S}_{sk_R}(\cdot,\cdot)$, $\mathcal{C}$ 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 $\mathsf{SC}.\mathsf{D}_{sk_R}(\cdot)$, $\mathcal{C}$ 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 $\mathsf{SC}.\mathsf{D}_{sk_R}(\cdot)$, 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 $\mathsf{Adv}^{\mathsf{INVK\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k) \le 2\cdot\mathsf{Adv}^{\mathsf{IK\text{-}CCA}}_{\mathcal{E},\mathcal{B}}(k) + \mathsf{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathcal{E},\mathcal{C}}(k)$. This concludes the proof. □

6 Conclusion

In this paper, we first revisited the existing privacy notions of signcryptions, 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. J. H. An, Y. Dodis, and T. Rabin. On the security of joint signature and encryption. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology*, EUROCRYPT '02, pages 83–107, London, UK, UK, 2002. Springer-Verlag.
2. J. H. Au and T. Rabin. "Security for Signcryption: The Two-User Model". In A. Dent and Y. Zheng, editors, *Practical Signcryption*, Information Security and Cryptography. 2010.
3. J. Baek, R. Steinfeld, and Y. Zheng. Formal proofs for the security of signcryption. In *Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems: Public Key Cryptography*, PKC '02, pages 80–98, London, UK, UK, 2002. Springer-Verlag.
4. F. Bao and R. H. Deng. A Signcryption Scheme with Signature Directly Verifiable by Public Key. In *PKC*, volume 1431 of *LNCS*, pages 55–59. Springer, 1998.
5. M. Bellare, A. Boldyreva, A. Desai, and D. Pointcheval. Key-privacy in public-key encryption. In *Advances in Cryptology - ASIACRAPT '01*, volume 2248 of *LNCS*, pages 566–582. Springer-Verlag, 2001.
6. M. Bellare and C. Namprempre. Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. In *ASIACRYPT*, volume 1976 of *LNCS*, pages 531–545. Springer, 2000.
7. X. Boyen. Multipurpose identity-based signcryption – a Swiss Army knife for identity-based cryptography. In D. Boneh, editor, *Advances in Cryptology—CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 383–399. Berlin: Springer-Verlag, 2003. Available at http://www.cs.stanford.edu/ xb/crypto03/.
8. R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext. In *CRYPTO '98*, pages 13–25, 1998.
9. A. W. Dent and Y. Z. (Eds). *Practical Signcryption*. Springer, 2010.
10. A. W. Dent, M. Fischlin, M. Manulis, M. Stam, and D. Schröder. Confidential Signatures and Deterministic Signcryption. In *PKC 2010*, volume 6056 of *LNCS*, pages 462–479, 2010.
11. Y. Dodis, M. J. Freedman, S. Jarecki, and S. Walfish. Optimal Signcryption from Any Trapdoor Permutation. Cryptology ePrint Archive, Report 2004/020, 2004. http://eprint.iacr.org/.
12. S. Galbraith and W. Mao. Invisibility and anonymity of undeniable and confirmer signatures. In M. Joye, editor, *Topics in Cryptology CT-RSA 2003*, volume 2612 of *Lecture Notes in Computer Science*, pages 80–97. Springer Berlin Heidelberg, 2003.
13. S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.*, 17(2):281–308, Apr. 1988.
14. C. K. Li, G. Yang, D. S. Wong, X. Deng, and S. S. M. Chow. An efficient signcryption scheme with key privacy. In *EuroPKI*, volume 4582, pages 78–93, 2007.
15. B. Libert and J.-J. Quisquater. Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups. In *PKC*, volume 2947 of *LNCS*, pages 187–200. Springer, 2004.
16. B. Libert and J.-J. Quisquater. Improved Signcryption from q-Diffie-Hellman Problems. In *SCN*, volume 3352 of *LNCS*, pages 220–234. Springer, 2004.
17. J. Malone-Lee. A General Construction for Simultaneous Signing and Encrypting. In *IMA Int. Conf.*, volume 3796 of *LNCS*, pages 116–135. Springer, 2005.
18. J. Malone-Lee and W. Mao. Two Birds One Stone: Signcryption Using RSA. In *CT-RSA*, volume 2612 of *LNCS*, pages 211–225. Springer, 2003.
19. J. Pieprzyk and D. Pointcheval. Parallel Authentication and Public-Key Encryption. In *ACISP*, volume 2727 of *LNCS*, pages 387–401. Springer, 2003.
20. C. Rackoff and D. R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '91, pages 433–444, London, UK, UK, 1992. Springer-Verlag.
21. J.-B. Shin, K. Lee, and K. Shim. New DSA-Verifiable Signcryption Schemes. In *ICISC*, volume 2587 of *LNCS*, pages 35–47. Springer, 2002.
22. R. Steinfeld and Y. Zheng. A Signcryption Scheme Based on Integer Factorization. In *ISW*, volume 1975 of *LNCS*, pages 308–322. Springer, 2000.

23. C.-H. Tan. On the security of signcryption scheme with key privacy. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, E88-A(4):1093–1095, Apr. 2005.
24. G. Yang, D. S. Wong, and X. Deng. Analysis and improvement of a signcryption scheme with key privacy. In *Proceedings of the 8th international conference on Information Security*, ISC'05, pages 218–232, Berlin, Heidelberg, 2005. Springer-Verlag.
25. D. H. Yum and P. J. Lee. New Signcryption Schemes Based on KCDSA. In *ICISC*, volume 2288 of *LNCS*, pages 305–317. Springer, 2001.
26. Y. Zheng. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption). In *Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '97, pages 165–179, London, UK, UK, 1997. Springer-Verlag.

A Proof of Theorem 1

Theorem 1 follows from Lemma 3 and Lemma 4. □

Lemma 3. *Let* SC *be a signcryption scheme. If* SC *satisfies anonymity, then it satisfies ciphertext anonymity.*

Proof. Suppose an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ breaks the ciphertext anonymity property with non-negligible advantage. We show how to construct an algorithm $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ that breaks the anonymity property with non-negligible advantage. Recall that $\mathcal{A}_1$ gets $(\lambda_{sc}, pk_{R,0}, pk_{R,1})$ as input and has access to signcryption oracles $\mathsf{SC.S}_{sk_{R,0}}(\cdot,\cdot)$, $\mathsf{SC.S}_{sk_{R,1}}(\cdot,\cdot)$ and unsigncryption oracles $\mathsf{SC.D}_{sk_{R,0}}(\cdot)$, $\mathsf{SC.D}_{sk_{R,1}}(\cdot)$, and at some time submits $(m, sk_{S,0}, sk_{S,1})$ to its challenger. Let $\Pr[(d,d')|(b,b')]$, where $d, d', b, b' \in \{0,1\}$, be the probability that $\mathcal{A}_2$ outputs (d,d') when given the challenge signcryption ciphertext C^* generated with respect to $sk_{S,b}, pk_{R,b'}$. Then we have

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{INDK\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k) &= \big|\Pr[(d,d') = (b,b')] - \frac{1}{4}\big| \\
&= \big|\frac{1}{4}\cdot(\Pr[(0,0)|(0,0)] + \Pr[(0,1)|(0,1)] + \Pr[(1,0)|(1,0)] + \Pr[(1,1)|(1,1)]) - \frac{1}{4}\big| \\
&= \big|\frac{1}{4}\cdot(\Pr[(0,0)|(0,0)] + \Pr[(0,1)|(0,1)] + \Pr[(1,0)|(1,0)] + \Pr[(1,1)|(1,1)]) \\
&\quad - \frac{1}{4}\cdot(\Pr[(0,0)|(0,0)] + \Pr[(0,1)|(0,0)] + \Pr[(1,0)|(0,0)] + \Pr[(1,1)|(0,0)])\big| \\
&= \big|\frac{1}{4}\cdot(\Pr[(0,1)|(0,1)] + \Pr[(1,0)|(1,0)] + \Pr[(1,1)|(1,1)]) \\
&\quad - \frac{1}{4}\cdot(\Pr[(0,1)|(0,0)] + \Pr[(1,0)|(0,0)] + \Pr[(1,1)|(0,0)])\big|.
\end{aligned}$$

Recall that $\mathcal{B}_1$ gets $(\lambda'_{sc}, pk'_{R,0}, pk'_{R,1})$ as input and has access to signcryption oracles $\mathsf{SC.S}_{sk'_{R,0}}(\cdot,\cdot)$, $\mathsf{SC.S}_{sk'_{R,1}}(\cdot,\cdot)$ and unsigncryption oracles $\mathsf{SC.D}_{sk'_{R,0}}(\cdot)$, $\mathsf{SC.D}_{sk'_{R,1}}(\cdot)$. $\mathcal{B}_1$ flips two coins $i, j \in \{0,1\}$ independently. If $i = 1$ and $j = 1$, $\mathcal{B}_1$ sets $\lambda_{sc} := \lambda'_{sc}, pk_{R,0} := pk'_{R,1}, pk_{R,1} := pk'_{R,0}$. Otherwise, $\mathcal{B}_1$ sets $\lambda_{sc} := \lambda'_{sc}, pk_{R,0} := pk'_{R,0}, pk_{R,1} := pk'_{R,1}$. $\mathcal{B}_1$ runs $\mathcal{A}_1$ as a subroutine with input $(\lambda_{sc}, pk_{R,0}, pk_{R,1})$.

When $\mathcal{A}_1$ makes a query (m, pk_R) to $\mathsf{SC.S}_{sk_{R,c}}(\cdot,\cdot)$ where $c \in \{0,1\}$, $\mathcal{B}_1$ forwards (m, pk_R) to its own signcryption oracle $\mathsf{SC.S}_{sk'_{R,c'}}(\cdot,\cdot)$ where $c' = 1 - c$ when $i = j = 1$ and $c' = c$ otherwise, and returns the output to $\mathcal{A}_1$ as the reply. When $\mathcal{A}_1$ makes a query C to $\mathsf{SC.D}_{sk_{R,c}}(\cdot)$ where $c \in \{0,1\}$, $\mathcal{B}_1$ forwards C to its own unsigncryption oracle $\mathsf{SC.D}_{sk'_{R,c'}}(\cdot)$ and returns the output to $\mathcal{A}_1$ as the reply.

At some time, $\mathcal{A}_1$ submits $(m^*, sk_{S,0}, sk_{S,1})$. $\mathcal{B}_1$ sets $sk'_{S,0} := sk_{S,0}$ and $sk'_{S,1} := sk_{S,j}$ (i.e., if the previously flipped coin $j = 0$, $sk'_{S,1} := sk_{S,0}$. If $j = 1$, $sk'_{S,1} := sk_{S,1}$). $\mathcal{B}_1$ submits $(m^*, sk'_{S,0}, sk'_{S,1})$ to

its own challenger, who returns a challenger signcryption ciphertext C^*. $\mathcal{B}_2$ runs $\mathcal{A}_2$ as a subroutine by forwarding C^*, and simulates the oracles in the same way as $\mathcal{B}_1$ did.

Note that $\mathcal{A}_2$ never makes a unsigncryption query C^* to $\mathsf{SC.D}_{sk_{R,c}}(\cdot)$ where $c \in \{0,1\}$, thus $\mathcal{B}_2$ does not make a unsigncryption query C^* to $\mathsf{SC.D}_{sk'_{R,c}}(\cdot)$. The simulation of the environment for $\mathcal{A}$ is perfect. Finally $\mathcal{A}_2$ outputs (d, d').

- When $i = 0, j = 0$. $\mathcal{B}_2$ outputs 1 if $(d, d') = (0, 1)$; otherwise $\mathcal{B}_2$ aborts and returns failure.
- When $i = 0, j = 1$. $\mathcal{B}_2$ outputs 1 if $(d, d') = (1, 1)$; otherwise $\mathcal{B}_2$ aborts and returns failure.
- When $i = 1, j = 0$. $\mathcal{B}_2$ outputs 1 if $(d, d') = (1, 0)$; otherwise $\mathcal{B}_2$ aborts and returns failure.
- When $i = 1, j = 1$. $\mathcal{B}_2$ outputs 1 if $(d, d') = (1, 0)$; otherwise $\mathcal{B}_2$ aborts and returns failure.

We show that the advantage of $\mathcal{B}$ is negligible. Indeed, we have

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{ANON\text{-}CCA}}_{\mathsf{SC},\mathcal{B}}(k) &:= |\Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},0}_{\mathsf{SC},\mathcal{B}}(k) = 1] - \Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},1}_{\mathsf{SC},\mathcal{B}}(k) = 1]| \\
&= \big|\frac{1}{4} \cdot (\Pr[(0,1)|(0,0)] + \Pr[(1,1)|(0,0)] + \Pr[(1,0)|(0,0)] + \Pr[(1,0)|(0,1)]) \\
&\quad - \frac{1}{4} \cdot (\Pr[(0,1)|(0,1)] + \Pr[(1,1)|(1,1)] + \Pr[(1,0)|(0,1)] + \Pr[(1,0)|(1,0)])\big| \\
&= \big|\frac{1}{4} \cdot (\Pr[(0,1)|(0,0)] + \Pr[(1,1)|(0,0)] + \Pr[(1,0)|(0,0)]) \\
&\quad - \frac{1}{4} \cdot (\Pr[(0,1)|(0,1)] + \Pr[(1,1)|(1,1)] + \Pr[(1,0)|(1,0)])\big| \\
&= \mathsf{Adv}^{\mathsf{INDK\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k). \qquad \square
\end{aligned}$$

Lemma 4. *Let* SC *be a signcryption scheme. If* SC *satisfies ciphertext anonymity, then it satisfies anonymity.*

Proof. Suppose an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ breaks the anonymity property with non-negligible advantage. We show how to construct an algorithm $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ that breaks the ciphertext anonymity property with non-negligible advantage. Recall that $\mathcal{A}_1$ gets $(\lambda_{sc}, pk_{R,0}, pk_{R,1})$ as input and has access to signcryption oracles $\mathsf{SC.S}_{sk_{R,0}}(\cdot,\cdot)$, $\mathsf{SC.S}_{sk_{R,1}}(\cdot,\cdot)$ and unsigncryption oracles $\mathsf{SC.D}_{sk_{R,0}}(\cdot)$, $\mathsf{SC.D}_{sk_{R,1}}(\cdot)$.

$\mathcal{B}_1$ gets $(\lambda'_{sc}, pk'_{R,0}, pk'_{R,1})$ as input and has access to signcryption oracles $\mathsf{SC.S}_{sk'_{R,0}}(\cdot,\cdot)$, $\mathsf{SC.S}_{sk'_{R,1}}(\cdot,\cdot)$ and unsigncryption oracles $\mathsf{SC.D}_{sk'_{R,0}}(\cdot)$, $\mathsf{SC.D}_{sk'_{R,1}}(\cdot)$. $\mathcal{B}_1$ sets $\lambda_{sc} := \lambda'_{sc}, pk_{R,0} := pk'_{R,0}, pk_{R,1} := pk'_{R,1}$. $\mathcal{B}_1$ runs $\mathcal{A}_1$ as a subroutine with input $(\lambda_{sc}, pk_{R,0}, pk_{R,1})$.

When $\mathcal{A}_1$ makes a query (m, pk_R) to $\mathsf{SC.S}_{sk_{R,c}}(\cdot,\cdot)$ where $c \in \{0,1\}$, $\mathcal{B}_1$ forwards (m, pk_R) to its own signcryption oracle $\mathsf{SC.S}_{sk'_{R,c}}(\cdot,\cdot)$ and returns the output to $\mathcal{A}_1$ as the reply. When $\mathcal{A}_1$ makes a query C to $\mathsf{SC.D}_{sk_{R,c}}(\cdot)$ where $c \in \{0,1\}$, $\mathcal{B}_1$ forwards C to its own unsigncryption oracle $\mathsf{SC.D}_{sk'_{R,c}}(\cdot)$ and returns the output to $\mathcal{A}_1$ as the reply.

At some time, $\mathcal{A}_1$ submits $(m^*, sk_{S,0}, sk_{S,1})$. $\mathcal{B}_1$ sets $sk'_{S,0} := sk_{S,0}$ and $sk'_{S,1} := sk_{S,1}$, and submits $(m^*, sk'_{S,0}, sk'_{S,1})$ to its own challenger, who returns a challenger signcryption ciphertext C^*. $\mathcal{B}_2$ runs $\mathcal{A}_2$ as a subroutine by forwarding C^*, and simulates the oracles in the same way as $\mathcal{B}_1$ did.

Note that $\mathcal{A}_2$ never makes a unsigncryption query C^* to $\mathsf{SC.D}_{sk_{R,c}}(\cdot)$ where $c \in \{0,1\}$, thus $\mathcal{B}_2$ does not make a unsigncryption query C^* to $\mathsf{SC.D}_{sk'_{R,c}}(\cdot)$. Finally $\mathcal{A}_2$ outputs a bit d (in the case $\mathcal{A}_2$ returns failure, we can safely assume that a random bit d is outputted). $\mathcal{B}_2$ outputs (d, d).

We show that the advantage of $\mathcal{B}$ is negligible. Indeed, we have

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{INDK\text{-}CCA}}_{\mathsf{SC},\mathcal{B}}(k) &= \big|\Pr[(d,d')=(b,b')] - \frac{1}{4}\big| \\
&= \big|\frac{1}{4}\cdot(\Pr[(0,0)|(0,0)] + \Pr[(0,1)|(0,1)] + \Pr[(1,0)|(1,0)] + \Pr[(1,1)|(1,1)]) - \frac{1}{4}\big| \\
&= \big|\frac{1}{4}\cdot(\Pr[(0,0)|(0,0)] + \Pr[(1,1)|(1,1)]) - \frac{1}{4}\big| \\
&= \big|\frac{1}{4}\cdot(\Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k)=0] + \Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k)=1]) - \frac{1}{4}\big| \\
&= \big|\frac{1}{4}\cdot(1-\Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k)=1] + \Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k)=1]) - \frac{1}{4}\big| \\
&= \frac{1}{4}\cdot\big|\mathsf{Adv}^{\mathsf{ANON\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k)\big|. \qquad \square
\end{aligned}
$$

B Proof of Lemmas 1 and 2 (Separating SC-IND-CCA and SC-INDK-CCA)

Proof of Lemma 1: We prove this by giving a counterexample. Let SC' = ($\mathsf{Setup}, \mathsf{KeyGen}$, $\mathsf{SignCrypt}, \mathsf{UnSignCrypt}, \mathsf{Verify}$) be an arbitrary signcryption scheme that is semantically secure against chosen ciphertext attacks. We construct signcryption scheme SC from SC' as follows.

- $\mathsf{Setup}(1^k)$: Output $\lambda_{sc} \leftarrow \mathsf{SC}'.\mathsf{Setup}(1^k)$.
- $\mathsf{KeyGen}(\lambda_{sc})$: Output $(sk_U, pk_U) \leftarrow \mathsf{SC}'.\mathsf{KeyGen}(\lambda_{sc})$.
- $\mathsf{Signcrypt}(m, sk_U, pk_R)$: Let $C' \leftarrow \mathsf{SC}'.\mathsf{SignCrypt}(m, sk_U, pk_R)$. Output $C = C'||pk_U$.
- $\mathsf{UnSignCrypt}(sk_R, C)$: Parse C as $C'||pk'_U$. If $(m, s, pk_U) \leftarrow \mathsf{SC}'.\mathsf{SignCrypt}(sk_R, C')$ and $pk_U = pk'_U$, output (m, s, pk_U). Otherwise output $\perp$.
- $\mathsf{Verify}(m, s, pk_U)$: Output $\mathsf{SC}'.\mathsf{Verify}(m, s, pk_U)$.

Since public keys can readily be extracted from signcryption ciphertext C, the obtained scheme SC does not satisfy ciphertext anonymity. However, we show that SC is semantically secure against chosen ciphertext attacks.

Suppose an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ breaks the indistinguishability against chosen ciphertext attacks of SC with non-negligible advantage. We show how to construct an algorithm $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ that breaks the indistinguishability against chosen ciphertext attacks of SC' with non-negligible advantage. Recall that $\mathcal{B}_1$ gets (λ_{sc}, pk_R) as input and has access to signcryption oracle $\mathsf{SC}.\mathsf{S}_{sk_R}(\cdot,\cdot)$ and unsigncryption oracle $\mathsf{SC}.\mathsf{D}_{sk_R}(\cdot)$. $\mathcal{B}_1$ runs $\mathcal{A}_1$ as a subroutine by forwarding (λ_{sc}, pk_R).

When $\mathcal{A}_1$ makes a signcryption query on (m, pk_U), $\mathcal{B}_1$ submits (m, pk_U) to its own signcryption oracle $\mathsf{SC}.\mathsf{S}_{sk_R}(\cdot,\cdot)$, who returns a reply denoted as C'. $\mathcal{B}_1$ forwards $C'||pk_R$ to $\mathcal{A}_1$. When $\mathcal{A}_1$ makes a unsigncryption query on C, $\mathcal{B}_1$ parses C as $C'||pk'_U$ and submits C' to its own unsigncryption oracle $\mathsf{SC}.\mathsf{D}_{sk_R}(\cdot)$. If the output is (m, s, pk_U) and $pk_U = pk'_U$, $\mathcal{B}_1$ forwards (m, s, pk_U) to $\mathcal{A}_1$. Otherwise, $\mathcal{B}_1$ forwards $\perp$ to $\mathcal{A}_1$.

At some time, $\mathcal{A}_1$ submits (m_0, m_1, sk_S). $\mathcal{B}_1$ submits (m_0, m_1, sk_S) to its own challenger, who returns a challenge signcryption ciphertext $C^* = \tilde{C}||pk_S$ where pk_S is the corresponding public key of sk_S. $\mathcal{B}_2$ runs $\mathcal{A}_2$ as a subroutine by forwarding $\tilde{C}$, and simulates the oracles in the same way as $\mathcal{B}_1$ did, with the exception that $\mathcal{B}_2$ always returns $\perp$ to $\mathcal{A}_2$ when a unsigncryption query is made on C' where C' is of the form $\tilde{C}||pk_U$.

Note that $\mathcal{A}$ is not allowed to ask a decryption query on the challenge ciphertext $C^* = \tilde{C}||pk_S$. In the real attack environment for $\mathcal{A}_2$, when $\tilde{C}||pk_U$ where $pk_U \neq pk_S$ is query, $\perp$ will also be returned as $\perp$, due to the fact that $\mathsf{SC}'.\mathsf{UnSignCrypt}(sk_R, \tilde{C})$ always outputs a tuple (m_b, s, pk_S)

where $b \in \{0,1\}$ and pk_S is the target sender's public key. The simulation is perfect. Finally $\mathcal{A}_2$ outputs a bit d. $\mathcal{B}_2$ outputs d.

We show that the advantage of $\mathcal{B}$ is non-negligible.

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

Since $\mathsf{Adv}^{\mathsf{INVK\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k)$ is non-negligible, so does $\mathsf{Adv}^{\mathsf{INV\text{-}CCA}}_{\mathcal{E},\mathcal{B}}(k)$.

Since there exist signcryption schemes that are semantically secure against chosen ciphertext attacks, the scheme SC served as an an counterexample described above exists. □

Before proving Lemma 2, we first review some notions that will be used in the proof.

(Strong One-Time Signature): A one-time signature scheme is a signature scheme with the limitation that each key pair is used only once for signature generation. A one-time signature scheme $\mathsf{OTS} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Sig}, \mathsf{Ver})$ is said to be *strongly one-time unforgeable* if no PPT adversary $\mathcal{A}$ wins the following game against the challenger C with non-negligible probability.

1. C generates the public parameter $\lambda_{\mathsf{OTS}} \leftarrow \mathsf{OTS}(1^\kappa)$, produces a one-time signature key pair $(otsk, otvk)$ and forwards $otvk$ to $\mathcal{A}$.
2. $\mathcal{A}$ may select one message m of any length, and request for a signature on it. $\mathcal{C}$ runs the signing algorithm $\mathsf{Sig}_{otsk}(m) \to \sigma$ and returns σ to $\mathcal{A}$.
3. $\mathcal{A}$ outputs a message signature forgery (m^*, σ^*), and wins the game if
   - $\mathsf{Ver}_{otvk}(m^*, \sigma^*) = \top$,
   - $(m^*, \sigma^*) \neq (m, \sigma)$ (if $\mathcal{A}$ has ever made a signature query).

(Collision-Resistant Hash Functions): A hash function H is collision-resistant if it is computationally hard to find two inputs that hash to the same output; that is, two inputs a and b such that $H(a) = H(b)$, and $a \neq b$.

(bilinear pairing): Let $\mathbb{G}$, $\mathbb{G}_T$ be two cyclic groups such that $|\mathbb{G}| = |\mathbb{G}_T| = p$. We say that e is a bilinear map if $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ possesses the following properties.

- For all elements of $g, h \in \mathbb{G}$, $x, y \in \mathbb{Z}_p$, it holds that $e(g^x, h^y) = e(g, h)^{xy}$.
- There exists $g, h \in \mathbb{G}$ such that $e(g, h)$ is not the identity element of $\mathbb{G}_T$.
- There is an efficient algorithm to compute $e(g, h)$ for any $g, h \in \mathbb{G}$.

(Decisional Bilinear Diffie-Hellman Assumption): The DBDH assumption states that, for a given generator $g \in \mathbb{G}$, randomly and independently chosen $x, y, z \in \mathbb{Z}_p$ and $T \in \mathbb{G}_T$, no PPT adversary $\mathcal{A}$ has non-negligible advantage in distinguishing $e(g, g)^{xyz}$ from T. That is, there exists a negligible ϵ such that

$$|\Pr[\mathcal{A}(g, g^a, g^b, g^c, e(g, g)^{abc}) = 1] - \Pr[\mathcal{A}(g, g^a, g^b, g^c, T) = 1]| \leq \epsilon.$$

Proof of Lemma 2: We prove Lemma 2 by giving an counterexample. Let $\mathcal{S} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Sig}, \mathsf{Ver})$ be a signature scheme that is existentially unforgeable under adaptive chosen message attacks, $\mathsf{OTS} = (\mathsf{Setup}, \mathsf{KGen}, \mathsf{Sig}, \mathsf{Ver})$ be a strong one-time signature scheme, $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a bilinear

pairing with g, h being two generators of $\mathbb{G}$, and $H : \{0,1\}^* \to \mathbb{Z}_p$ be a collision-resistant hash function. We construct a signcryption scheme $\mathsf{SC} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{SignCrypt}, \mathsf{UnSignCrypt}, \mathsf{Verify})$ that satisfies ciphertext anonymity 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 $\lambda_{\mathsf{OTS}} \leftarrow \mathcal{E}.\mathsf{Setup}(1^k)$, respectively. The public parameters are set as $\lambda_{sc} := (\lambda_{\mathcal{S}}, \lambda_{\mathsf{OTS}}, e, g, h, X, H)$ where $X = g^x$ and x is randomly chosen from $\mathbb{Z}_p$.
- $\mathsf{KeyGen}(\lambda_{sc})$: The user U_i runs $\mathcal{S}.\mathsf{KGen}(\lambda_{\mathcal{S}}) \to (sk_i, vk_i)$, and randomly chooses $y_i \in \mathbb{Z}_p$. The secret and public key pair is set as $(sk_{U_i}, pk_{U_i}) := ((sk_i, dk_j), (vk_i, ek_j))$ where $(dk_j, ek_j) = (X^{y_j}, g^{y_j})$.
- $\mathsf{SignCrypt}(m, sk_{U_i}, pk_{U_j})$: To signcrypt a message m for the receiver U_j, U_i
  1. produces a signature σ on $m||pk_{U_j}$, i.e., $\sigma \leftarrow \mathcal{S}.\mathsf{Sig}_{sk_i}(m||pk_{U_j})$.
  2. runs $\mathsf{OTS.KGen}(\lambda_{\mathsf{OTS}}) \to (otsk, otvk)$, and sets $c_0 := otvk$.
  3. Denote $\mathcal{F}(u) = X^u h$ for $u \in \mathbb{Z}_p$. U_i decomposes pk_{U_j} as (vk_j, ek_j), randomly chooses $z \in \mathbb{Z}_p$, and sets
  $$c_1 := (C_0, C_1, C_2) = (g^z,\ \mathcal{F}(H(otvk))^z,\ e(X, ek_j)^z \cdot m||\sigma||pk_{U_i}).$$
  Here we implicitly assume an encoding is employed to encode $m||\sigma||pk_{U_i}$ as an element of group $\mathbb{G}_T$.
  4. U_i runs $\mathsf{OTS.Sig}_{otsk}(C_0||C_1||C_2||m) \to c_2$.
  5. The signcryption ciphertext is set as $C := (c_0, c_1, c_2, m)$.
- $\mathsf{UnSignCrypt}(sk_{U_j}, C)$: On receiving a signcryption ciphertext $C = (c_0, c_1, c_2, m)$ where $c_0 = otvk$ and $c_1 = (C_0, C_1, C_2)$, the receiver U_j
  1. verifies whether $\mathsf{OTS.Ver}_{otvk}(C_0||C_1||C_2||m, c_2) = \top$. If not, U_j continues, and otherwise $\perp$ is returned.
  2. randomly chooses $r \in \mathbb{Z}_p$ and computes
  $$(D_0, D_1) := (dk_j \cdot \mathcal{F}(H(otvk))^r,\ g^r).$$
  3. computes $C_2 \cdot e(C_1, D_1)/e(C_0, D_0) = M$.
  4. decomposes M as $m'||\sigma||pk_{U_i}$, and parses pk_{U_i} as (vk_i, ek_i).
  5. outputs $(m, (pk_{U_j}, \sigma), pk_{U_i})$ if $m' = m$ and $\mathcal{S}.\mathsf{Ver}_{vk_i}(m||pk_{U_j}, \sigma) = \top$. Otherwise, $\perp$ is returned.
- $\mathsf{Verify}(m, (pk_{U_j}, \sigma), pk_{U_i})$: Parse pk_{U_i} as (vk_i, ek_i). Outputs $\mathcal{S}.\mathsf{Ver}_{vk_i}(m||pk_{U_j}, \sigma)$.

Due to the correctness of a signature scheme and that of a one-time signature scheme and that

$$C_2 \frac{e(C_1, D_1)}{e(C_0, D_0)} = \frac{C_2 \cdot e(\mathcal{F}(H(otvk))^z, g^r)}{e(g^z, g^{xy_j}\mathcal{F}(H(otvk))^r)} = \frac{C_2 \cdot e(\mathcal{F}(H(otvk)), g)^{rz}}{e(g,g)^{xy_j z} e(\mathcal{F}(H(otvk)), g)^{rz}} = \frac{C_2}{e(X, ek_j)^z},$$

it is easy to verify that the correctness of the proposed signcryption scheme holds.

Next we show that the proposed signcryption scheme satisfies ciphertext anonymity. We shall use anonymity instead of ciphertext anonymity in our analysis, as these two are equivalent by Theorem 1.

Suppose an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ breaks the ciphertext anonymity of SC with non-negligible advantage. We show how to construct an algorithm $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ that breaks the DBDH assumption. Recall that $\mathcal{B}_1$ gets $(e, g, g_1 = g^x, g_2 = g^y, g_3 = g^z, T)$ as input where e is a bilinear pairing and T is either a random element in group $\mathbb{G}_T$ or $e(g,g)^{xyz}$.

$\mathcal{B}_1$ runs $\lambda_{\mathcal{S}} \leftarrow \mathcal{S}.\mathsf{Setup}(1^k)$, $\lambda_{\mathsf{OTS}} \leftarrow \mathsf{OTS.Setup}(1^k)$, $\mathcal{S}.\mathsf{KGen}(\lambda_{\mathcal{S}}) \to (sk_0, vk_0)$, $\mathcal{S}.\mathsf{KGen}(\lambda_{\mathcal{S}}) \to (sk_1, vk_1)$ and $\mathsf{OTS.KGen}(\lambda_{\mathsf{OTS}}) \to (otsk^*, otvk^*)$ respectively. $\mathcal{B}_1$ randomly chooses $v, a \in \mathbb{Z}_p$ and

a collision-resistant hash function H, and sets $u^* := H(otvk^*), X := g_1, h := X^{-u^*}g^v, ek_0 := g_2, ek_1 := g_2 g^a, pk_{R,0} := (vk_0, ek_0), pk_{R,1} := (vk_1, ek_1)$.

$\mathcal{B}_1$ further sets $\lambda_{sc} := (\lambda_{\mathcal{S}}, \lambda_{\mathsf{OTS}}, e, g, h, X, H)$, and runs $\mathcal{A}_1$ as a subroutine by forwarding $(\lambda_{sc}, pk_{R,0}, pk_{R,1})$.

When $\mathcal{A}_1$ makes a signcryption query on (m, pk_U) to its signcryption oracle $\mathsf{SC.S}_{sk_{R,c}}(\cdot,\cdot)$ where $c \in \{0,1\}$, $\mathcal{B}_1$ runs $\mathsf{SignCrypt}(m, sk_{R,c}, pk_U) \to C$ and forwards C to $\mathcal{A}_1$ as the reply. The reason that $\mathcal{B}_1$ can do so is that only the signature signing key is used in the generation of a signcryption ciphertext.

When $\mathcal{A}_1$ makes a unsigncryption query $C = (c_0, c_1, c_2, m)$ to $\mathsf{SC.D}_{sk_{R,c}}(\cdot)$ where $c_0 = otvk \neq otvk^*$, $c_1 = (C_0, C_1, C_2)$ and $c \in \{0,1\}$, $\mathcal{B}_1$

- verifies whether $\mathsf{OTS.Ver}_{otvk}(C_0||C_1||C_2||m, c_2) = \top$. If not, U_j continues, and otherwise $\perp$ is returned.
- sets $u = H(otvk)$ and $\Delta = u - u^*$. Note that $\Delta \in \mathbb{Z}_p^*$ when $otvk \neq otvk^*$ due to the collision resistant property of H.
- randomly selects $t \in \mathbb{Z}_p$ and computes

$$D_0 := (g_2(g^a)^c)^{-\frac{v}{\Delta}}\mathcal{F}(u)^t, D_1 := (g_2(g^a)^c)^{-\frac{1}{\Delta}}g^t.$$

- computes $C_2 \cdot e(C_1, D_1)/e(C_0, D_0) = M$.
- decomposes M as $m'||\sigma||pk_{U_i}$, and parses pk_{U_i} as (vk_i, ek_i).
- outputs $(m, (pk_{R,c}, \sigma), pk_{U_i})$ if $m' = m$ and $\mathcal{S}.\mathsf{Ver}_{vk_i}(m||pk_{R,c}, \sigma) = \top$. Otherwise, $\perp$ is returned.

Denote $r = -\frac{y+ac}{\Delta} + t$. Note that $\mathcal{F}(u) = X^u h = g^{x(u-u^*)+v} = g^{x\Delta+v}$. Then it is clear that

$$D_0 = (g_2(g^a)^c)^{-\frac{v}{\Delta}}\mathcal{F}(u)^t = X^{y+ac}g^{-\frac{y+ac}{\Delta}(x\Delta+v)}\mathcal{F}(u)^t = X^{y+ab}\mathcal{F}(u)^{-\frac{y+ab}{\Delta}}\mathcal{F}(u)^t = X^{y+ac}\mathcal{F}(u)^r,$$

$$D_1 = g^{-\frac{y+ac}{\Delta}+t} = g^r.$$

This matches what a real challenger would do in answering the unsigncryption queires.

In the challenge phase, $\mathcal{A}_1$ submits $(m^*, sk_{S,0}, sk_{S,1})$. $\mathcal{B}_2$

- parses $sk_{S,0}$ and $sk_{S,1}$ as (sk'_0, dk'_0) and (sk'_1, dk'_1) respectively.
- randomly chooses a bit $b \in \{0,1\}$ and produces a signature σ^* on $m^*||pk_{R,b}$ using the signing key sk'_b, i.e., $\sigma^* \leftarrow \mathcal{S}.\mathsf{Sig}_{sk'_b}(m^*||pk_{R,b})$.
- computes $c_1^* = (C_0^*, C_1^*, C_2^*) = (g_3,\ g_3^v,\ T \cdot e(g_1, g_3)^{ab} \cdot m^*||\sigma^*||pk_{S,b})$ where $pk_{S,b}$ is the corresponding public key of $sk_{S,b}$.
- sets $c_0^* = otvk^*$ and runs $\mathsf{OTS.Sig}_{otsk^*}(C_0^*||C_1^*||C_2^*||m^*) \to c_2$.
- The challenge signcryption ciphertext is set as $C^* := (c_0^*, c_1^*, c_2^*, m^*)$.

Note that if T is a random element in group $\mathbb{G}_T$, then C^* is independent of b in the adversary $\mathcal{A}$'s view. Whereas if $T = e(g,g)^{xyz}$, then $C_1^* = g_3^v = g^{zv} = g^{z(x\cdot 0+v)} = \mathcal{F}(H(otvk^*))^z$ and $C_3^* = T \cdot e(X, g_3)^{ab} \cdot M^* = e(g,g)^{x(y+ab)z} \cdot M^* = e(X, ek_b)^z \cdot M^*$ where $M^* := m^*||\sigma^*||pk_{S,b}$ are correctly generated, and C^* is a valid challenge signcryption ciphertext that a real challenger may output.

$\mathcal{B}_2$ then simulates the signcryption and unsigncryption oracles in the same way as $\mathcal{B}_1$ did. We argue that $\mathcal{A}_2$ is not able to ask a unsigncryption query on $C = (c_0, c_1, c_2, m)$ where $c_0 = otvk^*$ and $c_1 = (C_0, C_1, C_2)$.

Remember that $\mathcal{A}$ is not allowed to ask a decryption query on the challenge ciphertext C^*. When an unsigncryption query on $C \neq C^*$ with $c_0 = c_0^* = otvk^*$ is made, it means that $(C_1||C_2||C_3||m, c_2) \neq$

$(C_1^*||C_2^*||C_3^*||m^*, c_2^*)$. The probability that this case happens is negligible, guaranteed by the strong one-time unforgeability of OTS.

Finally, $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$. Algorithm $\mathcal{B}$ concludes its own game by outputting a guess as follows. If $b = b'$ then $\mathcal{B}$ output 1 meaning $T = e(g,g)^{xyz}$. Otherwise, it outputs 0 meaning T is a random element in group $\mathbb{G}_T$.

When $T = e(g,g)^{xyz}$, then $\mathcal{A}$'s view is indistinguishable to its view in a real attack game. On the other hand, when T is random, $\Pr[b' = b] = 1/2$. Thus we have

$$\begin{aligned}
&\big|\Pr[\mathcal{B}(g, g^x, g^y, g^z, e(g,g)^{xyz}) = 1] - \Pr[\mathcal{B}(g, g^a, g^b, g^c, T) = 1]\big| \\
&= \big|\frac{1}{2} \cdot (\Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k) = 0] + \Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k) = 1]) - \frac{1}{2} \cdot (\frac{1}{2} + \frac{1}{2})\big| \\
&= \big|\frac{1}{2} \cdot (\Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k) = 1] - \Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k) = 1])\big| \\
&= \frac{1}{2} \cdot \mathsf{Adv}^{\mathsf{INVK\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k).
\end{aligned}$$

Therefore, we can safely arrive to the conclusion that the proposed scheme SC satisfies ciphertext anonymity under the DBDH assumpiton. However, since the message can readily be extracted from a signcryption ciphertext C, SC is not semantically secure against chosen ciphertext attacks. This completes the proof. □

C Proof of Theorem 2

Suppose an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ breaks anonymity with non-negligible advantage. We show how to construct an algorithm $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ that breaks key invisibility with non-negligible advantage. Recall that $\mathcal{B}_1$ gets (λ_{sc}, pk_R) as input and has access to signcryption oracle $\mathsf{SC.S}_{sk_R}(\cdot,\cdot)$ and unsigncryption oracle $\mathsf{SC.D}_{sk_R}(\cdot)$. $\mathcal{B}_1$ firstly generates randomly $(sk'_R, pk'_R) \leftarrow \mathsf{SC.KeyGen}(\lambda_{sc})$, flips a coin $\tilde{b} \in \{0,1\}$ and sets $pk_{R,\tilde{b}} := pk_R, pk_{R,1-\tilde{b}} := pk'_R$. $\mathcal{B}_1$ runs $\mathcal{A}_1$ as a subroutine by forwarding $(\lambda_{sc}, pk_{R,0}, pk_{R,1})$.

When $\mathcal{A}_1$ makes a query (m, pk_U) to $\mathsf{SC.S}_{sk_{R,c}}(\cdot,\cdot)$ where $c \in \{0,1\}$, if $sk_{R,c} = sk'_R$, $\mathcal{B}_1$ runs $\mathsf{SC.SignCrypt}$ (m, sk'_R, pk_U) and forwards the output to $\mathcal{A}_1$ as the reply. Otherwise, $\mathcal{B}_1$ forwards (m, pk_U) to its own signcryption oracle $\mathsf{SC.S}_{sk_R}(\cdot,\cdot)$ and returns the output to $\mathcal{A}_1$ as the reply. When $\mathcal{A}_1$ makes a query C to $\mathsf{SC.D}_{sk_{R,c}}(\cdot)$ where $c \in \{0,1\}$, if $sk_{R,c} = sk'_R$, $\mathcal{B}_1$ runs $\mathsf{SC.UnSignCrypt}$ (sk'_R, C) and forwards the output to $\mathcal{A}_1$ as the reply. Otherwise, $\mathcal{B}_1$ submits C to its own unsigncryption oracle $\mathsf{SC.D}_{sk_R}(\cdot)$ and returns the output of its own oracle to $\mathcal{A}_1$ as the reply.

At some time, $\mathcal{A}_1$ submits $(m^*, sk_{S,0}, sk_{S,1})$. $\mathcal{B}_1$ sets $sk_S := sk_{S,\tilde{b}}$ and submits (m^*, sk_S) to its own challenger, who returns a challenge signcryption ciphertext C^*. $\mathcal{B}_2$ runs $\mathcal{A}_2$ as a subroutine by forwarding C^*, and simulates the oracles in the same way as $\mathcal{B}_1$ did.

Note that $\mathcal{A}_2$ never makes a unsigncryption query C^* to $\mathsf{SC.D}_{sk_{R,c}}(\cdot)$ where $c \in \{0,1\}$, thus $\mathcal{B}_2$ does not make a unsigncryption query C^* to $\mathsf{SC.D}_{sk_R}(\cdot)$. Finally $\mathcal{A}_2$ outputs a bit d (in the case $\mathcal{A}_2$ returns failure, we can safely assume that a random bit d is returned). $\mathcal{B}_2$ outputs d if $\tilde{b} = 0$; otherwise it outputs $1 - d$.

Let $\mathsf{Exp}^*_{\mathsf{SC},\mathcal{A}}(k)$ be the experiment that is the same as $\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},b}_{\mathsf{SC},\mathcal{A}}(k)$ where $b \in \{0,1\}$ with the exception that the challenge signcryption ciphertext C^* is randomly and uniformly chosen from

the signcryption ciphertext space $\mathcal{C}$. We show that the advantage of $\mathcal{B}$ is non-negligible.

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{INVK\text{-}CCA}}_{\mathsf{SC},\mathcal{B}}(k) &= \big|\Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},0}_{\mathsf{SC},\mathcal{B}}(k)=1] - \Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},1}_{\mathsf{SC},\mathcal{B}}(k)=1]\big| \\
&= \big|\Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},0}_{\mathsf{SC},\mathcal{B}}(k)=1|\tilde{b}=0]\Pr[\tilde{b}=0] + \Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},0}_{\mathsf{SC},\mathcal{B}}(k)=1|\tilde{b}=1]\Pr[\tilde{b}=1] \\
&\quad - \Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},1}_{\mathsf{SC},\mathcal{B}}(k)=1|\tilde{b}=0]\Pr[\tilde{b}=0] - \Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},1}_{\mathsf{SC},\mathcal{B}}(k)=1|\tilde{b}=1]\Pr[\tilde{b}=1]\big| \\
&= \big|\frac{1}{2}\cdot\Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k)=1] + \frac{1}{2}\cdot\Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k)=0] \\
&\quad - \frac{1}{2}\cdot\Pr[\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)=1] - \frac{1}{2}\cdot\Pr[\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)=0]\big| \\
&= \big|\frac{1}{2}\cdot\Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k)=1] + \frac{1}{2}\cdot(1-\Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k)=1]) \\
&\quad - \frac{1}{2}\cdot(\Pr[\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)=1] + \Pr[\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)=0])\big| \\
&= \big|\frac{1}{2}\cdot(\Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k)=1] - \Pr[\mathsf{Exp}^{\mathsf{ANON\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k)=1])\big| \qquad (4) \\
&= \frac{1}{2}\cdot\mathsf{Adv}^{\mathsf{ANON\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k).
\end{aligned}
$$

Equation (4) follows from the fact that $\mathcal{A}$ outputs either 0 or 1 and thus $\Pr[\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)=1] + \Pr[\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)=0] = 1$. Since $\mathsf{Adv}^{\mathsf{ANON\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k)$ is non-negligible, so does $\mathsf{Adv}^{\mathsf{INVK\text{-}CCA}}_{\mathsf{SC},\mathcal{B}}(k)$. This completes the proof. □

D Proof of Theorem 3

Suppose an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ breaks indistinguishability against chosen ciphertext attacks with non-negligible advantage. We show how to construct an algorithm $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ that breaks key invisibility with non-negligible advantage. Recall that $\mathcal{A}_1$ gets (λ_{sc}, pk_R) as input and has access to signcryption oracle $\mathsf{SC.S}_{sk_R}(\cdot,\cdot)$ and unsigncryption oracle $\mathsf{SC.D}_{sk_R}(\cdot)$.

$\mathcal{B}_1$ gets (λ'_{sc}, pk'_R) as input and has access to signcryption oracle $\mathsf{SC.S}_{sk'_R}(\cdot,\cdot)$ and unsigncryption oracle $\mathsf{SC.D}_{sk'_R}(\cdot)$. $\mathcal{B}_1$ sets $\lambda_{sc} := \lambda'_{sc}, pk_R := pk'_R$ and runs $\mathcal{A}_1$ as a subroutine with input (λ_{sc}, pk_R).

When $\mathcal{A}_1$ makes a signcryption query (m, pk_U) to $\mathsf{SC.S}_{sk_R}(\cdot,\cdot)$, $\mathcal{B}_1$ forwards (m, pk_U) to its own signcryption oracle $\mathsf{SC.S}_{sk'_R}(\cdot,\cdot)$ and returns the output 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 unsigncryption oracle $\mathsf{SC.D}_{sk'_R}(\cdot)$ and returns the output to $\mathcal{A}_1$ as the reply.

At some time, $\mathcal{A}_1$ submits (m_0, m_1, sk_S). $\mathcal{B}_1$ flips a coin $\tilde{b} \in \{0,1\}$, and submits $(m_{\tilde{b}}, sk_S)$ to its own challenger, who returns a challenge signcryption ciphertext C^*. $\mathcal{B}_2$ runs $\mathcal{A}_2$ as a subroutine by forwarding C^*, and simulates the oracles in the same way as $\mathcal{B}_1$ did.

Note that $\mathcal{A}_2$ never makes a unsigncryption query C^* to $\mathsf{SC.D}_{sk_R}(\cdot)$, thus $\mathcal{B}_2$ does not make a unsigncryption query C^* to $\mathsf{SC.D}_{sk'_R}(\cdot)$. Finally $\mathcal{A}_2$ outputs a bit d (in the case $\mathcal{A}_2$ returns failure, we can safely assume that a random bit d is returned). $\mathcal{B}_2$ outputs d if $\tilde{b} = 0$; otherwise it outputs $1 - d$.

Let $\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)$ be the experiment that is the same as $\mathsf{Exp}^{\mathsf{IND\text{-}CCA},b}_{\mathsf{SC},\mathcal{A}}(k)$ where $b \in \{0,1\}$ with the exception that the challenge signcryption ciphertext C^* is randomly and uniformly chosen from

the signcryption ciphertext space $\mathcal{C}$. We show that the advantage of $\mathcal{B}$ is non-negligible.

$$
\begin{aligned}
\mathsf{Adv}^{\mathsf{INVK\text{-}CCA}}_{\mathsf{SC},\mathcal{B}}(k) &= \big|\Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},0}_{\mathsf{SC},\mathcal{B}}(k)=1] - \Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},1}_{\mathsf{SC},\mathcal{B}}(k)=1]\big| \\
&= \big|\Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},0}_{\mathsf{SC},\mathcal{B}}(k)=1|\tilde{b}=0]\Pr[\tilde{b}=0] + \Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},0}_{\mathsf{SC},\mathcal{B}}(k)=1|\tilde{b}=1]\Pr[\tilde{b}=1] \\
&\quad - \Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},1}_{\mathsf{SC},\mathcal{B}}(k)=1|\tilde{b}=0]\Pr[\tilde{b}=0] - \Pr[\mathsf{Exp}^{\mathsf{INVK\text{-}CCA},1}_{\mathsf{SC},\mathcal{B}}(k)=1|\tilde{b}=1]\Pr[\tilde{b}=1]\big| \\
&= \big|\frac{1}{2}\cdot\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k)=1] + \frac{1}{2}\cdot\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k)=0] \\
&\quad - \frac{1}{2}\cdot\Pr[\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)=1] - \frac{1}{2}\cdot\Pr[\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)=0]\big| \\
&= \big|\frac{1}{2}\cdot\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k)=1] + \frac{1}{2}\cdot(1-\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k)=1]) \\
&\quad - \frac{1}{2}\cdot(\Pr[\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)=1] + \Pr[\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)=0])\big| \\
&= \big|\frac{1}{2}\cdot(\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA},0}_{\mathsf{SC},\mathcal{A}}(k)=1] - \Pr[\mathsf{Exp}^{\mathsf{IND\text{-}CCA},1}_{\mathsf{SC},\mathcal{A}}(k)=1])\big| \qquad (5) \\
&= \frac{1}{2}\cdot\mathsf{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k).
\end{aligned}
$$

Equation (5) follows from the fact that $\mathcal{A}$ outputs either 0 or 1 and thus $\Pr[\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)=1] + \Pr[\mathsf{Exp}^{*}_{\mathsf{SC},\mathcal{A}}(k)=0] = 1$. Since $\mathsf{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathsf{SC},\mathcal{A}}(k)$ is non-negligible, so does $\mathsf{Adv}^{\mathsf{INVK\text{-}CCA}}_{\mathsf{SC},\mathcal{B}}(k)$. The proof is done. □