Relations among Notions of Privacy for RFID Authentication Protocols

Daisuke Moriyama, Shin'ichiro Matsuo, and Miyako Ohkubo

National Institute of Information and Communications Technology, Japan
{dmoriyam,smatsuo,m.ohkubo}@nict.go.jp

Abstract. In this paper, we present the relationship between privacy definitions for Radio Frequency Identification (RFID) authentication protocols. The security model is necessary for ensuring security or privacy, but many researchers present different privacy concepts for RFID authentication and the technical relationship among them is unclear. We reconsider the zero-knowledge based privacy proposed by Deng et al. at ESORICS 2010 and show that this privacy is equivalent to indistinguishability based privacy proposed by Juels and Weis. We also provide the implication and separation between these privacy definitions and the simulation based privacy proposed by Paise and Vaudenay at AsiaCCS 2008 based on the *public verifiability* of the communication message.

1 Introduction

Radio Frequency Identification (RFID) technology enables the reader to identify objects. RFID systems consist of a reader and many tags. The reader communicates with the tags over the wireless (insecure) channel and checks the identity. RFID is expected to replace barcodes and is now used in many industries (manufacturing, transportation, logistics, etc.). However, the existing low-cost tags only contain the identity with no protection and respond with their identity directly when the reader provides electric power. Many cryptographers have studied the RFID authentication protocol to overcome the privacy problem. This privacy-preserving RFID authentication protocol improves the reliability of the machine-to-machine network system and also ensures the secure transaction.

In cryptography, the security/privacy of each scheme or protocol is evaluated by the security model. There are several security models for RFID authentication protocols [6,5,9,10,12,15,14,18]. All of which define three components: correctness, security and privacy. The correctness and security definitions are almost the same in these models. Correctness ensures that the reader accepts the tag if the reader and tag correctly communicate with each other. Security requires that if a malicious adversary impersonates a valid tag and interferes the communication, the reader rejects the session. However, the privacy notion is not commonly defined and the relationship between them is unclear. In this paper, we concentrate on the privacy definitions for the RFID authentication protocol and investigate the relationship.

S. Foresti, M. Yung, and F. Martinelli (Eds.): ESORICS 2012, LNCS 7459, pp. 661–678, 2012.

Our Contributions. Our contributions are twofold:

1. We show that the indistinguishability based privacy definition (IND-privacy) proposed by Juels and Weis [12] and zero-knowledge based privacy definition (ZK-privacy) proposed by Deng et al. [9] are equivalent. Though Deng et al. proved that zero-knowledge based privacy is stronger than indistinguishability based privacy, we show that their argument is inadequate and these privacy definitions are proven to be equivalent.
2. We investigate the relationship between indistinguishability based privacy and simulation based privacy (SIM-privacy) proposed by Paise and Vaudenay [18]. There are many existing RFID authentication protocols that are secure in one of the two security models or its slight variants [11,17], but no one investigates whether there exists a technical difference between [12] and [18], except the trivial separation followed by the corruption timing. These privacy definitions are formalized in a different style and it is hard to present the difference directly. Hence, we consider a variant of the zero-knowledge based privacy proposed in [9] in order to reduce the gap between them (this variant is polynomially equivalent to the Juels-Weis security model). We then compare the resulting privacy definition with [18]. We introduce a notion of public and secret verifiability to the RFID authentication. Roughly speaking, the public verifiability holds if anyone can check the authenticity of an entity from the communication message (note that the tag must be secret verifiable from correctness and privacy). Our result is that there is a technical gap between IND-privacy and SIM-privacy if the communication message is publicly verifiable. Otherwise, we prove that these privacy definitions are equivalent (if the restriction for the tag corruption is equivalent).

Related Work. The privacy definition for RFID authentication is roughly divided into the following: indistinguishability [4,12,11], simulatability [21,18], zero-knowledge [9], unpredictability [10,15] and universal composability [6,5,14] (see [8] for more information). The unpredictability based privacy model [10,15] requires that, at least, the tag's response to the reader is indistinguishable from the random string. Ma et al. [15] showed that (1) the unpredictability based privacy model requires strictly stronger privacy than the indistinguishability based privacy model [12], and (2) the existence of an RFID authentication protocol that satisfies the unpredictability based privacy model equals the existence of a pseudo-random function. This function is used in many lightweight RFID authentication protocols, but we consider unpredictability based privacy too strong to satisfy privacy. For example, if both the reader and tag can perform IND-CCA2 secure public key encryption and all communication is encrypted by each party's public key, then the communication reveals none of the secret information. However, the ciphertext usually consists of group elements and is easily distinguishable from random string.

The universal composability based privacy model [6,5,14] requires a simulator to simulate any actions of the malicious adversary and no external environment should be able to distinguish whether it interacts with the adversary or the simulator. The authors did not describe the relationship between their model

and the other privacy model, but Paise and Vaudenay demonstrated the RFID authentication protocol depicted in [6] does not have the narrow-forward privacy present in the Paise-Vaudenay privacy model [18].

2 Existing RFID Security Models

We review security models proposed by Juels-Weis [12], Deng-Li-Yung-Zhao [9] and Paise-Vaudenay [18], respectively. We use the following notations in this paper. We denote by $\mathcal{T}$ the total set of tags in the RFID authentication protocol that is managed by the reader $\mathcal{R}$. The reader runs the Setup algorithm and obtains (pk, sk). The public parameter pk is published and secret key sk is kept as a secret. If the RFID authentication protocol is based on symmetric key cryptography, each tag shares several secret keys with the reader (sk contains the set of these secret keys). In the authentication phase, the reader and the tag communicate with each other via wireless communication. We consider an active adversary $\mathcal{A}$ that can interfere/insert/delete/modify the communication message and its direction. The RFID authentication protocol requires correctness, security and privacy. Roughly speaking, correctness defines that the reader always outputs "accept" if the communication is not modified by the adversary. Security requires that the reader rejects the session if the adversary interferes and modifies the outgoing message. In the following, we concentrate on the privacy definition in the security model and call privacy model.

2.1 Juels-Weis Privacy Model

Juels and Weis proposed a privacy model for RFID authentication protocols based on indistinguishability [12]. We show a slight variant of the privacy model modified by Deng et al. [9]. Based on the IND-CPA definition for public/symmetric key encryption, this model evaluates the probability that an adversary correctly distinguishes the identity of the tag when he interacts with the reader and tags. The privacy game between an adversary $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$ and challenger is defined as follows:

Setup. The challenger runs the Setup algorithm and obtains (pk, sk) to setup the reader $\mathcal{R}$ and set of tags $\mathcal{T}$. The adversary obtains public parameter pk and $(\mathcal{R}, \mathcal{T})$.

Phase 1. The adversary $\mathcal{A}_1$ can issue oracle queries $\mathcal{O} := \{\mathsf{Launch}, \mathsf{SendReader}, \mathsf{SendTag}, \mathsf{Result}, \mathsf{Corrupt}\}$ and interact with the reader and tags:

- $\mathsf{Launch}(1^k)$ — Launch the reader to initiate the session.
- $\mathsf{SendReader}(m)$ — Send arbitrary message m to the reader.
- $\mathsf{SendTag}(t, m)$ — Send arbitrary message m to the tag $t \in \mathcal{T}$.
- $\mathsf{Result}(\mathsf{sid})$ — Output whether the reader accepts the session sid (sid is uniquely determined by the communication message).
- $\mathsf{Corrupt}(t)$ — Output the secret key of the tag t.

Challenge. The adversary $\mathcal{A}_1$ sends two tags t_0^* and t_1^* ($t_0^* \neq t_1^*$) to the challenger and outputs state information st_1. st_1 contains all information obtained by $\mathcal{A}_1$ including internal coin tosses of $\mathcal{A}_1$. Then the challenger flips a coin $b \xleftarrow{\mathsf{U}} \{0,1\}$ and sets $\mathcal{T}' := \mathcal{T} \setminus \{t_0^*, t_1^*\}$.

Phase 2. The adversary $\mathcal{A}_2$ obtains st_1 and interacts with the reader $\mathcal{R}$ and tags $(t_b^*, \mathcal{T}')$ with the oracle queries. However, when the adversary interacts with the challenge tag t_b^*, we consider special algorithm $\mathcal{I}$. $\mathcal{I}$ relays the message between $\mathcal{A}$ and t_b^* so that the adversary communicates with t_b^* anonymously.

Guess. The adversary $\mathcal{A}_2$ outputs a guess b'.

We say that the adversary wins the game if $b' = b$ holds and (t_0^*, t_1^*) is not corrupted. The advantage of the adversary in the above game is defined as $\mathsf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{A}}(k) := |2 \cdot \Pr[b' = b] - 1|$. The following experiment also evaluates this advantage.

$\underline{\mathsf{Exp}^{\mathsf{IND}\text{-}b}_{\Pi,\mathcal{A}}(k)}$
$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k)$;
$(t_0^*, t_1^*, st_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}}(pk, \mathcal{R}, \mathcal{T})$;
$b \xleftarrow{\mathsf{U}} \{0,1\}, \mathcal{T}' := \mathcal{T} \setminus \{t_0^*, t_1^*\}$;
$b' \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}}(\mathcal{R}, \mathcal{T}', \mathcal{I}(t_b^*), st_1)$:
Output b'

We have $\mathsf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{A}}(k) = |\Pr[\mathsf{Exp}^{\mathsf{IND}\text{-}0}_{\Pi,\mathcal{A}}(k) \to 1] - \Pr[\mathsf{Exp}^{\mathsf{IND}\text{-}1}_{\Pi,\mathcal{A}}(k) \to 1]|$.

Definition 1. *An RFID authentication protocol Π satisfies the privacy in the Juels-Wies security model if for any probabilistic polynomial time (PPT) adversary $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{A}}(k)$ is negligible.*

2.2 Deng-Li-Yung-Zhao Privacy Model

The privacy model proposed by Deng et al. is based on a zero-knowledge formulation [9]. The intuition behind this model is that when the communication message does not reveal any tag's identity or secret key, the messages should be simulated even if an algorithm cannot interact with the tag.

We consider two experiments $\mathsf{Exp}^{\mathsf{ZK}\text{-}0}_{\mathcal{A},\mathcal{D}}(k)$ and $\mathsf{Exp}^{\mathsf{ZK}\text{-}1}_{\mathcal{S},\mathcal{D}}(k)$. In the former , the adversary $\mathcal{A}$ interacts with the reader and tags. $\mathcal{A}$ outputs an arbitrary subset of tags $\mathcal{C} \subseteq \mathcal{T}$ and the challenger uniformly chooses a challenge tag $t^* \xleftarrow{\mathsf{U}} \mathcal{C}$ at random. The adversary can then interact with $\mathcal{R}$, tags $\mathcal{T}' := \mathcal{T} \setminus \mathcal{C}$ and the challenge tag t^* anonymously. When the adversary sends message m to $\mathcal{I}$, this algorithm passes m to t^* and responds with the output from t^*. Finally the adversary outputs its view and a distinguisher outputs a bit b with the view. The latter experiment is the same as the former except that the simulator $\mathcal{S}$ cannot interact with the challenge tag. We note that the adversary and simulator cannot issue any corrupt queries to the tags in $\mathcal{C}$ in the experiment. These experiments are depicted as follows:

$\underline{\mathsf{Exp}^{\mathsf{ZK\text{-}0}}_{\Pi,\mathcal{A},\mathcal{D}}(k)}$
$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k)$;
$(\mathcal{C}, st_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}}(pk, \mathcal{R}, \mathcal{T})$;
$t^* \xleftarrow{\mathsf{U}} \mathcal{C}, \mathcal{T}' := \mathcal{T} \setminus \mathcal{C}$;
$view_{\mathcal{A}} \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}}(\mathcal{R}, \mathcal{T}', \mathcal{I}(t^*), st_1)$;
$b \xleftarrow{\mathsf{R}} \mathcal{D}(\mathcal{C}, t^*, view_{\mathcal{A}})$:
Output b

$\underline{\mathsf{Exp}^{\mathsf{ZK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{D}}(k)}$
$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k)$;
$(\mathcal{C}, st_1) \xleftarrow{\mathsf{R}} \mathcal{S}_1^{\mathcal{O}}(pk, \mathcal{R}, \mathcal{T})$;
$t^* \xleftarrow{\mathsf{U}} \mathcal{C}, \mathcal{T}' := \mathcal{T} \setminus \mathcal{C}$;
$view_{\mathcal{S}} \xleftarrow{\mathsf{R}} \mathcal{S}_2^{\mathcal{O}}(\mathcal{R}, \mathcal{T}', st_1)$;
$b \xleftarrow{\mathsf{R}} \mathcal{D}(\mathcal{C}, t^*, view_{\mathcal{S}})$:
Output b

The advantage of the adversary in this model is defined by $\mathsf{Adv}^{\mathsf{ZK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D}}(k) = |\Pr[\mathsf{Exp}^{\mathsf{ZK\text{-}0}}_{\Pi,\mathcal{A},\mathcal{D}}(k) \to 1] - \Pr[\mathsf{Exp}^{\mathsf{ZK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{D}}(k) \to 1]|$.

Definition 2. *An RFID authentication protocol Π satisfies the privacy in the Deng et al. security model if for any PPT adversary $\mathcal{A}$, there exists a PPT algorithm $\mathcal{S}$, for any PPT distinguisher $\mathcal{D}$, $\mathsf{Adv}^{\mathsf{ZK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D}}(k)$ is negligible.*

2.3 Paise-Vaudenay Privacy Model

Vaudenay [21] proposed a simulation based privacy model for two-pass RFID authentication protocols. Paise and Vaudenay [18] extended this to satisfy reader authentication. The intuition behind these privacy models is that if the protocol messages are completely simulated by a third party, the privacy of the RFID tag is preserved since the adversary obtains no private information. The privacy game of their model is slightly similar to the Deng et al. privacy model, but the game flow is not explicitly defined. Instead, the adversary can additionally issue the following queries:

$\mathsf{CreateTag}$(ID,s) — Register a free tag to the reader. If the tag is legitimate ($s = 1$), the reader assigns the secret key for this tag and updates the database.
$\mathsf{DrawTag}(\mathcal{C}, \mathsf{Dist})$ — According to the distribution Dist and the arbitrary sets of tags $\mathcal{C} \subseteq \mathcal{T}$, the oracle responds with drawn tags $\mathcal{V} := \{\mathsf{vtag}_1, \ldots\}$. The oracle keeps a list list that maps the drawn tags to the real identity.
$\mathsf{Free}(\mathsf{vtag})$ — Change the drawn tag vtag to the free tag.

In their model, the challenger assigns a temporal identity to each drawn tag. The adversary can issue the $\mathsf{SendTag}$ query to the drawn tags only, and free tags do not execute the communication to the reader.

Paise and Vaudenay classifies the adversary's capacity into 2×4 categories.

1. Result query for the reader:
   (a) *Wide* — Adversary can issue the result query.
   (b) *Narrow* — Adversary cannot issue the result query.
2. Corrupt query for the tag:
   (a) *Strong* — No restriction for the corrupt query.
   (b) *Destructive* — If the adversary issues the corrupt query to a drawn tag, the tag is destroyed and unusable.

(c) *Forward* — After the corrupt query, the adversary cannot issue any other queries in the experiment.
(d) *Weak* — The adversary cannot issue the corrupt query.

For example, wide-strong privacy is defined as follows. Consider the two sets of the oracle queries $\mathcal{O}_1 := \{\mathsf{CreateTag}, \mathsf{DrawTag}, \mathsf{Free}, \mathsf{Corrupt}\}$ and $\mathcal{O}_2 := \{\mathsf{Launch}, \mathsf{SendReader}, \mathsf{SendTag}, \mathsf{Result}\}$. The wide-strong privacy game in this model is defined by the following experiments:

$\underline{\mathsf{Exp}^{\mathsf{SIM\text{-}0}}_{\Pi,\mathcal{A}}(k)}$	$\underline{\mathsf{Exp}^{\mathsf{SIM\text{-}1}}_{\Pi,\mathcal{A},\mathcal{S}}(k)}$
$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k)$;	$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k)$;
$b \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathcal{O}_1,\mathcal{O}_2}(pk, \mathcal{R})$:	$b \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathcal{O}_1,\mathcal{S}(pk)}(pk)$:
Output b	Output b

In the SIM-0 experiment, adversary $\mathcal{A}$ can create tags and interact with the reader and tags through $\mathcal{O}_2$ query. On the contrary, the SIM-1 experiment requires that simulator $\mathcal{S}$ responds to the adversary's oracle queries which correspond to $\mathcal{O}_2$ query. $\mathcal{S}$ can learn any information $\mathcal{A}$ obtains with $\mathcal{O}_1$ query. The advantage of the adversary is defined by $\mathsf{Adv}^{\mathsf{SIM}}_{\Pi,\mathcal{A},\mathcal{S}}(k) := |\Pr[\mathsf{Exp}^{\mathsf{SIM\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1] - \Pr[\mathsf{Exp}^{\mathsf{SIM\text{-}1}}_{\Pi,\mathcal{A},\mathcal{S}}(k) \to 1]|$. Of course, we can formalize the other types of adversary in the same fashion.

Definition 3. *An RFID authentication protocol Π satisfies the (wide/ narrow)-(strong/destructive/forward/weak) privacy in the Paise- Vaudenay security model if for any PPT adversary $\mathcal{A}$, there exists a PPT algorithm $\mathcal{S}$, $\mathsf{Adv}^{\mathsf{SIM}}_{\Pi,\mathcal{A},\mathcal{S}}(k)$ is negligible.*

In this paper, we slightly modify the restriction on the DrawTag query and assume that the adversary can only input legitimate tags for this query[1].

3 Equivalence between IND and ZK Privacy

The previous section described the three privacy models. Deng et al. [9] showed that their ZK-privacy is stronger than IND-privacy; that is, there exist two examples of the RFID authentication protocols that are secure in the Juels-Weis privacy model but insecure in the zero-knowledge based privacy model. However, we will show that these privacy models are proven to be equivalent. To justify our result, we first review their examples and point out the *flaw* of their argument.

The former example is constructed by a digital signature scheme. In the setup phase, a reader generates signing/verification key pair $(sk_{\mathsf{SIG}}, vk_{\mathsf{SIG}})$ and sends the signature of the tag's identity $\sigma_i \xleftarrow{\mathsf{R}} \mathsf{Sign}(sk_{\mathsf{SIG}}, t_i)$ as a secret key. To authenticate the tag, the reader outputs a request message and the tag responds with

[1] Otherwise, the wide-destructive privacy implies the existence of the simulator that can predict the coin tosses of the adversary [21]. To avoid such an unusual situation, Ng et al. formalized another approach s.t. the adversary does not issue oracle queries where the result is predetermined [16].

σ_i itself. Deng et al. argued that *"If the system has only one tag, it is clear to satisfy the IND-privacy but the simulator cannot simulate the signature at Phase 2 in the ZK-privacy"*. But we note that this implication does not make sense. As we explicitly describe in Section 2.1, IND-privacy assumes that the adversary must output two different tags (which is also implicitly assumed in the IND-CPA security for public key encryption). Thus their instantiation is inadequate in considering the IND-privacy. If we consider there are more than two tags in the system, it is clear that the adversary against IND-privacy can distinguish the message since the output of the tag's message is deterministically defined.

The building block of the latter example is the public key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ and an RFID authentication protocol Π that holds IND-privacy. Following [9], we assume that when the reader sends a to the tag, it responds with b to the reader in Π. They described the following RFID authentication protocol Π'. In the setup phase, a reader generates a public/secret key pair $(pk_{\mathsf{PKE}}, sk_{\mathsf{PKE}}) \xleftarrow{\mathsf{R}} \mathsf{Gen}(1^k)$ and sends sk_{PKE} to the tags (we remark that all tags in this protocol shares this unique secret key) as a secret key for Π'. When the reader authenticates the tag, it generates a and sends encrypted message $c \xleftarrow{\mathsf{R}} \mathsf{Enc}(pk_{\mathsf{PKE}}, a)$. If the tag receives the message, it decrypts as $a := \mathsf{Dec}(sk_{\mathsf{PKE}}, c)$, generates b with Π and responds $a \| b$ to the reader. Deng et al. said that Π' satisfies IND-privacy and does not satisfy ZK-privacy since no simulator can output the decryption of the ciphertext. However, we found that this argument is also wrong and Π' still holds ZK-privacy. Since the communication message is indistinguishable, simulator $\mathcal{S}_1$ can internally run zero-knowledge adversary $(\mathcal{A}_1, \mathcal{A}_2)$. It is easy to see that $\mathcal{S}_1$ simulates all communication message for $\mathcal{A}_1$. When $\mathcal{A}_1$ outputs $(\mathcal{C}, st_1)$, $\mathcal{S}_1$ uniformly chooses $t_1^* \xleftarrow{\mathsf{U}} \mathcal{C}$ and runs $\mathcal{A}_2$ with input $(pk, \mathcal{R}, \mathcal{T} \setminus \mathcal{C}, \mathcal{I}(t_1^*), st_1)$. Note that t_1^* may not be identical to the challenge tag, but IND-privacy ensures that no adversary can distinguish whether it interacts with the challenge tag or t_1^*. If $\mathcal{A}_2$ sends a message to the challenge tag, $\mathcal{S}_1$ simply sends it to t_1^* and responds with its message. When $\mathcal{A}_2$ outputs $view_{\mathcal{A}}$, then $\mathcal{S}_1$ sets $st_1' := view_{\mathcal{A}}$ and outputs $(\mathcal{C}, st_1')$. Finally, $\mathcal{S}_2$ outputs st_1' as its view regardless of the choice of challenge tag. Since the simulator can continue Phase 1 until the adversary outputs the view (Phase 1 and 2 for the adversary), these outputs are indistinguishable for any distinguisher $\mathcal{D}$. Of course, if we try to simulate the response of the $\mathsf{SendTag}$ query issued by $\mathcal{A}_2$ with $\mathcal{S}_2$, it is difficult to construct such a simulator since $\mathcal{S}_2$ must break the security for public key encryption. The key point here is that IND-privacy allows $\mathcal{S}_1$ to simulate the whole behavior of the ZK-privacy adversary $(\mathcal{A}_1, \mathcal{A}_2)$.

We now show that IND-privacy is equivalent to ZK-privacy.

Theorem 1. *The indistinguishability based privacy model is equivalent to the zero-knowledge based privacy model.*

Lemma 1. *If an RFID authentication protocol Π holds IND-privacy, it implies ZK-privacy.*

Proof. We prove the above lemma via the following sequence of games. We gradually change the ZK-0 experiment to ZK-1 experiment which is bounded by IND-privacy. Especially, we show that if for any IND-privacy adversary $\mathcal{B}$, $\mathsf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{B}}(k)$ is negligible, then for any ZK-privacy adversary $\mathcal{A}$, there exists a simulator $\mathcal{S}$, for any distinguisher $\mathcal{D}$, $\mathsf{Adv}^{\mathsf{ZK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D}}(k)$ is negligible.

For each game, $\Pr[T_j]$ denotes the probability that the distinguisher outputs 1 in Game j.

Game 0: Game 0 is the same as the original ZK-privacy game between a challenger and $\mathcal{A}$D Without loss of generality, we assume that $t_0^* \xleftarrow{\mathsf{U}} \mathcal{C}$ is chosen as the challenge tag. It is clear that $\Pr[T_0] = \Pr[\mathsf{Exp}^{\mathsf{ZK\text{-}0}}_{\Pi,\mathcal{A},\mathcal{D}}(k) \to 1]$.

Game 1: We modify Game 1 by changing the challenge tag. In addition to t_0^*, we select $t_1^* \xleftarrow{\mathsf{U}} \mathcal{C}$ and the adversary (anonymously) interacts with t_1^* instead of t_0^*.

Game 2: Game 2 is the original ZK-privacy game between a challenger and $\mathcal{S}$ under the condition that $\mathcal{S}$ runs $\mathcal{A}$ as in Fig. 1. Note that the challenge tag is chosen as Game 0 and the input to the distinguisher is t_0^*.

$\underline{\mathcal{S}_1^{\mathcal{O}}(pk, \mathcal{R}, \mathcal{T})}$	$\underline{\mathcal{S}_2(\mathcal{R}, \mathcal{T}', st_1')}$
$(\mathcal{C}, st_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}}(pk, \mathcal{R}, \mathcal{T})$;	$view_{\mathcal{S}} := view_{\mathcal{A}}$:
$t_1^* \xleftarrow{\mathsf{U}} \mathcal{C}, \mathcal{T}' := \mathcal{T} \setminus \mathcal{C}$;	Output $view_{\mathcal{S}}$
$view_{\mathcal{A}} \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}}(\mathcal{R}, \mathcal{T}', \mathcal{I}(t_1^*), st_1)$;	
$st_1' := view_{\mathcal{A}}$:	
Output $(\mathcal{C}, st_1')$	

Fig. 1. Simulation in Game 2

We evaluate the gaps between pairs of advantages with the following claims.

Claim. There exists a PPT algorithm $\mathcal{B}$ such that

$$|\Pr[T_1] - \Pr[T_0]| \leq \mathsf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{B}}(k).$$

Proof. If $(\mathcal{A}, \mathcal{D})$ distinguishes Game 0 and Game 1 with non-negligible probability, we construct an algorithm $\mathcal{B} := (\mathcal{B}_1, \mathcal{B}_2)$ that can break the IND-privacy. $\mathcal{B}$ internally runs $(\mathcal{A}, \mathcal{D})$ in the IND-privacy game as follows:

$\underline{\mathcal{B}_1^{\mathcal{O}}(pk, \mathcal{R}, \mathcal{T})}$	$\underline{\mathcal{B}_2^{\mathcal{O}}(pk, \mathcal{I}(t_b^*), st_1')}$
$(\mathcal{C}, st_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}}(pk, \mathcal{R}, \mathcal{T})$;	$view_{\mathcal{A}} \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}}(\mathcal{R}, \mathcal{T}', \mathcal{I}(t_b^*), st_1)$;
$t_0^*, t_1^* \xleftarrow{\mathsf{U}} \mathcal{C},\ \mathcal{T}' := \mathcal{T} \setminus \mathcal{C}$;	$b' \xleftarrow{\mathsf{R}} \mathcal{D}(\mathcal{C}, t_0^*, view_{\mathcal{A}})$:
$st_1' := (\mathcal{T}', t_0^*, st_1)$:	Output b'
Output (t_0^*, t_1^*, st_1')	

When the adversary $\mathcal{A}_1$ outputs $\mathcal{C}$, $\mathcal{B}_1$ chooses two tags (t_0^*, t_1^*) in $\mathcal{C}$ and sends it to the challenger. Since the challenger chooses a coin $b \xleftarrow{U} \{0,1\}$ and $\mathcal{B}_2$ can access $\mathcal{I}(t_b^*)$, the $\mathsf{SendTag}$ query that $\mathcal{A}_2$ issues to the challenge tag can be completely simulated. If the flipped coin is $b = 0$, the output distribution is the same as Game 0. Otherwise, this simulation is equivalent to Game 1. Therefore, we obtain

$$\begin{aligned} |\Pr[T_1] - \Pr[T_0]| &\leq \left| \mathsf{Adv}^{\mathsf{IND\text{-}1}}_{\Pi,\mathcal{B}}(k) - \mathsf{Adv}^{\mathsf{IND\text{-}0}}_{\Pi,\mathcal{B}}(k) \right| \\ &= \mathsf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{B}}(k). \end{aligned}$$

Claim. We have $\Pr[T_2] = \Pr[T_1]$.

Proof. We show that the output distribution of $\mathcal{A}$ in Game 1 is equivalent to that of $\mathcal{S}$ in Game 2. Recall that $\mathcal{S}_2$ cannot interact with the challenge tag in the original ZK-privacy experiment. Nevertheless, the previous claim shows that the anonymous interaction between $\mathcal{A}_2$ and t_0^* can be changed by another tag t_1^*. This means that even if $\mathcal{S}_1$ chooses another tag $t_1^* \in \mathcal{C}$ and replaces the anonymous interaction by $\mathcal{I}(t_1^*)$, $\mathcal{A}_2$ cannot distinguish between the games. Therefore $\mathcal{S}_1$ can simulate $(\mathcal{A}_1, \mathcal{A}_2)$ as in Fig.1 and obtain the view of the adversary $view_{\mathcal{A}}$. Any oracle queries made by $(\mathcal{A}_1, \mathcal{A}_2)$ can be simulated correctly since $\mathcal{S}_1$ can send the same query to $\mathcal{O}$. Thus $\mathcal{A}_2$'s output in Game 1 is equivalent to $\mathcal{S}_2$'s output in Game 2 and it is (information theoretically) indistinguishable for any distinguisher $\mathcal{D}$. Therefore we have $\Pr[T_2] = \Pr[T_1]$.

It is clear that $\Pr[T_2] = \Pr[\mathsf{Exp}^{\mathsf{ZK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{D}}(k) \to 1]$ and finally we have

$$\begin{aligned} \mathsf{Adv}^{\mathsf{ZK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D}}(k) &= |\mathsf{Exp}^{\mathsf{ZK\text{-}0}}_{\Pi,\mathcal{A},\mathcal{D}}(k) - \mathsf{Exp}^{\mathsf{ZK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{D}}(k)| \\ &= |\Pr[T_2] - \Pr[T_0]| \\ &\leq \mathsf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{B}}(k). \end{aligned}$$

Remark. If the zero-knowledge adversary sets $\mathcal{C}$ as only one tag, then we can directly transform Game 0 to Game 2. The strategy of the simulator is the same as in Fig. 1. The simulator issues the $\mathsf{SendTag}$ query in Phase 1 until the zero-knowledge adversary finishes the experiment.

Lemma 2. *If an RFID authentication protocol Π holds ZK-privacy, it implies IND-privacy.*

Remark that this lemma has been provided by Deng et al. [9], but their proof is *informal*. So we give the rigorous security proof based on the game transformation technique.

Proof. Again, we prove the above lemma via the following sequence of games. We show that if for any ZK adversary $\mathcal{B}$, there exists a simulator $\mathcal{S}$, for any distinguisher $\mathcal{D}$, $\mathsf{Adv}^{\mathsf{ZK}}_{\Pi,\mathcal{B},\mathcal{S},\mathcal{D}}(k)$ is negligible, then for any IND adversary $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{A}}(k)$ is negligible. For each game, $\Pr[T_j]$ denotes the probability that the experiment outputs 1 in Game j.

Game 0: Game 0 is the same as the original IND-0 privacy game between a challenger and $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$D We consider $\mathcal{A}_1$ outputs two tags (t_0^*, t_1^*) and t_0^* is chosen as the challenge tag in this game. It is clear that $\Pr[T_0] = \Pr[\mathsf{Exp}^{\mathsf{IND\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 1]$.

Game 1: We modify Game 1 by changing the challenge tag from t_0^* to t_1^*. It is clear that $\Pr[T_1] = \Pr[\mathsf{Exp}^{\mathsf{IND\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1]$.

Using $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, we construct the following ZK-privacy adversary $\mathcal{B} := (\mathcal{B}_1, \mathcal{B}_2)$ and distinguisher $\mathcal{D}$.

$\underline{\mathcal{B}_1^{\mathcal{O}}(pk, \mathcal{R}, \mathcal{T})}$	$\underline{\mathcal{B}_2^{\mathcal{O}}(\mathcal{R}, \mathcal{T}', \mathcal{I}(t^*), st_1')}$	$\underline{\mathcal{D}(\mathcal{C}, t^*, view_{\mathcal{B}})}$
$(t_0^*, t_1^*, st_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}}(pk, \mathcal{R}, \mathcal{T})$;	$b' \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}}(\mathcal{R}, \mathcal{T}', \mathcal{I}(t^*), st_1)$;	$t^* = view_{\mathcal{B}} \iff b := 1$;
$\mathcal{C} := \{t_0^*, t_1^*\}$;	$view_{\mathcal{B}} := t_{b'}$:	$t^* \neq view_{\mathcal{B}} \iff b := 0$:
$st_1' := (st_1, t_0^*, t_1^*)$:	Output $view_{\mathcal{B}}$	Output b
Output $(\mathcal{C}, st_1')$		

The adversary $\mathcal{B}_1$ sets two tags (t_0^*, t_1^*) as $\mathcal{C}$ and one of the two tags can be accessed by $\mathcal{B}_2$. If t_0^* is chosen from $\mathcal{C}$, it is equivalent to Game 0 with respect to $\mathcal{A}$ and we obtain

$$\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}0}}_{\Pi,\mathcal{A}}(k) \to 0] = 1 - \Pr[T_0] = \Pr[\mathsf{Exp}^{\mathsf{ZK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{D}}(k) \to 1 \mid \mathcal{C} \to t_0^*].$$

Otherwise, it can be viewed as Game 1 and

$$\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}1}}_{\Pi,\mathcal{A}}(k) \to 1] = \Pr[T_1] = \Pr[\mathsf{Exp}^{\mathsf{ZK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{D}}(k) \to 1 \mid \mathcal{C} \to t_1^*].$$

Of course, the challenger uniformly selects the challenge tag and $\Pr[\mathcal{C} \to t_0^*] = \Pr[\mathcal{C} \to t_1^*] = 1/2$. Thus we obtain

$$\Pr[\mathsf{Exp}^{\mathsf{ZK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{D}}(k) \to 1] = \frac{1}{2} + \frac{1}{2} \cdot (\Pr[T_1] - \Pr[T_0]).$$

Recall that we have assumed that Π is ZK-privacy. Thus, for any adversary $\mathcal{B}$, there exists an algorithm $\mathcal{S}$ such that for any distinguisher $\mathcal{D}$, $|\Pr[\mathsf{Exp}^{\mathsf{ZK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{D}}(k) \to 1] - \Pr[\mathsf{Exp}^{\mathsf{ZK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{D}}(k) \to 1]|$ is negligible. However, $\mathcal{S}$ has no information about the flipped coin in the experiment and we have $\Pr[\mathsf{Exp}^{\mathsf{ZK\text{-}1}}_{\Pi,\mathcal{S},\mathcal{D}}(k) \to 1] = 1/2$. Finally, we obtain

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{A}}(k) &= |\Pr[T_1] - \Pr[T_0]| \\
&= |2 \cdot \Pr[\mathsf{Exp}^{\mathsf{ZK\text{-}0}}_{\Pi,\mathcal{B},\mathcal{D}}(k) \to 1] - 1| \\
&= 2 \cdot \mathsf{Adv}^{\mathsf{ZK}}_{\Pi,\mathcal{B},\mathcal{S},\mathcal{D}}(k).
\end{aligned}$$

□

4 Relation between SIM and IND Privacy

4.1 Constraint for Corrupt Query

We revisit the privacy relation between SIM-privacy and IND-privacy. Many researchers have informally analyzed these models and several papers conclude

that SIM-privacy is stronger than IND-privacy since a wide-strong adversary can corrupt all tags in the experiment (recall that in the IND-privacy, the adversary must output uncorrupted tags for the challenge phase). However, there are four wide adversaries for SIM-privacy and it is meaningful to consider the other privacy notions. Vaudenay recently showed that the IND-privacy game can be written by the wide-destructive SIM-privacy game [22]. Of course, the condition for the corrupt query in the IND-privacy game is different from that in the SIM-privacy game and we can say that wide-forward SIM-privacy does not imply IND-privacy in the sense of adaptive corruption[2]. However, whether IND-privacy implies wide-weak SIM-privacy is unclear. We can also consider two variants for IND-privacy:

1. Strong IND-privacy — Challenge tags can be corrupted in Phase 1, and
2. Weak IND-privacy — The adversary is prohibited to issue the corrupt query.

Then Strong/weak IND-privacy is comparable to wide-strong/wide-weak SIM-privacy. The actual procedure of the IND experiment is of course different from that of the SIM experiment, but the restriction for the corrupt query in strong (resp. weak) IND-privacy is the same as for wide-strong (resp. wide-weak) SIM-privacy. One can also define these variants for ZK-privacy that are equivalent to the strong/weak IND-privacy, respectively.

One may think that the adaptive registration of the tag is allowed in SIM-privacy through the SetupTag query, but it is not a technical point since we can easily add this query to IND-privacy and ZK-privacy.

4.2 Anonymous Communication with Many Tags in ZK-Privacy

We modify ZK-privacy to minimize the difference between ZK-privacy and SIM-privacy. For simplicity, we consider weak ZK-privacy in the following.

First, we consider a slight variant of weak ZK-privacy such that the adversary can anonymously access any tags in $\mathcal{C}$ in Phase 2. This is done by a slight modification for the intermediate algorithm $\mathcal{I}$. When the adversary outputs $\mathcal{C}$, the challenger randomizes and indexes each tag in $\mathcal{C}$. The challenger keeps the list $\{(i, \mathrm{ID}_j)\}_{i,j}$ where $i \in \{1, \ldots, |\mathcal{C}|\}$ and $\mathrm{ID}_j \in \mathcal{C}$ which is initially empty. When the adversary issues the SendTag query to $\mathcal{I}$ with input (i, m), the challenger checks the list. If the list does not contain index i, the new identity ID in $\mathcal{C}$ is uniformly chosen and the tuple (i, ID) is inserted into the list. The message is sent to the corresponding identity and its response is returned to the adversary. This is a quite natural extension for ZK-privacy but we note that this modification partially interpolates the DrawTag query in SIM-privacy to allow anonymous access. We call the modified privacy as ZK′-privacy. Consider that $\mathcal{O}' := (\mathsf{Launch}, \mathsf{SendReader}, \mathsf{SendTag}, \mathsf{Result})$. Then weak ZK′-privacy is described as follows:

[2] If an RFID authentication protocol specifies that the secret key of each tag is initially correlated and always updated, the adversary can obtain the challenge tag's secret key in Phase 1 of the IND-privacy game. However, this protocol can hold wide-forward SIM-privacy due to the key update algorithm.

$\underline{\mathsf{Exp}^{\mathsf{ZK'\text{-}0}}_{\Pi,\mathcal{A},\mathcal{D}}(k)}$	$\underline{\mathsf{Exp}^{\mathsf{ZK'\text{-}1}}_{\Pi,\mathcal{S},\mathcal{D}}(k)}$
$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k)$;	$(pk, sk) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^k)$;
$(\mathcal{C}, st_1) \xleftarrow{\mathsf{R}} \mathcal{A}_1^{\mathcal{O}'}(pk, \mathcal{R}, \mathcal{T})$;	$(\mathcal{C}, st_1) \xleftarrow{\mathsf{R}} \mathcal{S}_1^{\mathcal{O}'}(pk, \mathcal{R}, \mathcal{T})$;
$\mathcal{T}' := \mathcal{T} \setminus \mathcal{C}$;	$\mathcal{T}' := \mathcal{T} \setminus \mathcal{C}$;
$view_{\mathcal{A}} \xleftarrow{\mathsf{R}} \mathcal{A}_2^{\mathcal{O}'}(\mathcal{R}, \mathcal{T}', \mathcal{I}(\mathcal{C}), st_1)$;	$view_{\mathcal{S}} \xleftarrow{\mathsf{R}} \mathcal{S}_2^{\mathcal{O}'}(\mathcal{R}, \mathcal{T}', st_1)$;
$b \xleftarrow{\mathsf{R}} \mathcal{D}(\mathcal{C}, \{i, \mathrm{ID}_j\}_{i,j}, view_{\mathcal{A}})$:	$b \xleftarrow{\mathsf{R}} \mathcal{D}(\mathcal{C}, \{i, \mathrm{ID}_j\}_{i,j}, view_{\mathcal{S}})$:
Output b	Output b

In this privacy model, the advantage of the adversary is defined by

$$\mathsf{Adv}^{\mathsf{ZK'}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D}}(k) = \left| \begin{array}{l} \Pr[\mathsf{Exp}^{\mathsf{ZK'\text{-}0}}_{\Pi,\mathcal{A},\mathcal{D}}(k) \to 1] - \\ \quad \Pr[\mathsf{Exp}^{\mathsf{ZK'\text{-}1}}_{\Pi,\mathcal{S},\mathcal{D}}(k) \to 1] \end{array} \right|.$$

Definition 4. *An RFID authentication protocol Π satisfies the ZK′-privacy if for any PPT adversary $\mathcal{A}$, there exists a PPT algorithm $\mathcal{S}$, for any PPT distinguisher $\mathcal{D}$, $\mathsf{Adv}^{ZK'}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D}}(k)$ is negligible.*

Theorem 2. *ZK′-privacy is an equivalent privacy notion to ZK-privacy.*

Proof. It is clear that ZK′-privacy implies ZK-privacy. We prove that if an RFID authentication protocol Π satisfies ZK-privacy, Π is also ZK′-privacy. This proof follows from the standard hybrid argument. Assume that the adversary against ZK′-privacy issues the $\mathsf{SendTag}$ query at most q_s. Based on the ZK′-0 experiment, we change the output from the $\mathsf{SendTag}$ query in Phase 2. The response is simulated by $\mathcal{S}$ for ZK-privacy until j-th invocation and executed by the real tag after j-th invocation. When the adversary issues j-th $\mathsf{SendTag}$ query, the challenger flips a coin $b \xleftarrow{\mathsf{U}} \{0, 1\}$. If $b = 1$, the challenger activates the real tag, and otherwise it runs the simulator to output the response. The difference between $b = 1$ and $b = 0$ is clearly bounded by $\mathsf{Adv}^{\mathsf{ZK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D}}(k)$. For $1 \leq j \leq q_s$, we can apply the same argument and finally we obtain an experiment that is identical to the ZK′-1 experiment. Therefore we have $\mathsf{Adv}^{\mathsf{ZK'}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D}}(k) \leq q_s \cdot \mathsf{Adv}^{\mathsf{ZK}}_{\Pi,\mathcal{A},\mathcal{S},\mathcal{D}}(k)$. □

Now, recall the simulation strategy in Lemma 1. The simulator $\mathcal{S}$ chooses an arbitrary tag to simulate the anonymous access for the adversary if the RFID authentication holds IND-privacy. ZK′-privacy implies that the simulator can simulate the message between the reader and all tags in $\mathcal{C}$ without any communication with these tags. Even when particular tags are chosen by a distribution (i.e. $\mathsf{DrawTag}$ query in SIM-privacy), the tag's behavior is indistinguishable from another tag and simulated by the simulator. Therefore, if the RFID authentication protocol satisfies ZK′-privacy (= IND-privacy), any specific information that corresponds to the tag's identity is not revealed.

4.3 Verifiability in the RFID Authentication Protocols

From the above argument, we can say that the only technical differences between ZK′-privacy and SIM-privacy are: (a) the simulator has the opportunity

to interact with the tag, and (b) the simulator can obtain reader's output or not[3]. We explicitly wrote that the simulator takes as input $\mathcal{R}$ and can issue the SendReader and Result queries in ZK′-privacy. On the other hand, SIM-privacy requires that the simulator must simulate the SendReader and Result queries along with the SendTag query. Thus the simulator against SIM-privacy must generate all reader's output which is indistinguishable from the real execution. Whether the output is simulatable or not depends on the protocol, so we define the *verifiability* to classify the protocol:

- Public verifiability: a third party who does not participate in the communication can check the validity of the message with the public parameter
- Secret verifiability: only the party who participates in the communication can check the validity of the message.

In the RFID authentication protocol, any message from the tag must satisfy the secret verifiability. In addition, the reader's output must satisfy at least the secret verifiability if the protocol provides reader authentication. However, we can consider the public verifiability of the reader/tag since any anonymity is not required for the reader and the tag may produce additional message which is not related to its identity. In the following, we provide the relationship among the privacy definitions based on the verifiability of the message.

4.4 Separation in the Presence of Public Verifiability

Theorem 3. *Strong ZK′-privacy does not imply wide-weak SIM-privacy if an RFID authentication protocol provides public verifiability of the communication message.*

Proof. Let Π be an RFID authentication protocol that satisfies strong ZK′-privacy. For simplicity, we assume that $(m_1, m_2, m_3, \ldots)$ is the communication message exchanged by the reader and a tag in this protocol. We describe three examples to clarify the essence of the public verifiability.

First Example Π'_1:

Let $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ be a digital signature algorithm. The reader runs Π to obtain (pk, sk) and shares secret keys with each tag in some cases. Run KeyGen algorithm and obtain signing/verification key pair $(sk_{\mathsf{SIG}}, vk_{\mathsf{SIG}})$. The reader publishes $pk' := (pk, vk_{\mathsf{SIG}})$ and sends sk_{SIG} to all tags in Π'_1. The authentication is executed as follows:

1. The reader obtains m_1 from Π and sends it to the tag.
2. When the tag receives the message, it generates m_2 with Π and signs the message as $\sigma \xleftarrow{\mathsf{R}} \mathsf{Sign}(sk_{\mathsf{SIG}}, m_2)$. Then the tag responds (m_2, σ) to the reader.

[3] Though the SIM-privacy allows the adversary to activate an illegitimate tag which is not registered to the database of the reader, we can also consider such a tag in the IND/ZK-privacy when the adversary activates a tag $t \notin \mathcal{T}$.

3. Upon receiving m_2, the reader generates m_3 and sends it to the reader.

The output message from the tag is publicly verifiable since anyone can check $\mathsf{Verify}(vk_{\mathsf{SIG}}, m_2, \sigma) = 1$ holds or not. However, all tags share the secret key sk_{SIG} and no information about the identity is revealed from this signature.

Second Example Π_2':

Let $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ be a digital signature algorithm. The reader run Π to obtain (pk, sk) and shares secret keys with each tag in some cases. Run KeyGen algorithm and obtain signing/verification key pair $(sk_{\mathsf{SIG}}, vk_{\mathsf{SIG}})$. The reader publishes $pk' := (pk, vk_{\mathsf{SIG}})$ and holds sk_{SIG} as its own secret key of the reader in Π_2'. The authentication is executed as follows:

1. The reader obtains m_1 from Π and sends it to the tag.
2. When the tag receives the message, it generates m_2 with Π and responds m_2 to the reader.
3. Upon receiving m_2, the reader generates m_3 and signs the message as $\sigma \xleftarrow{\mathsf{R}} \mathsf{Sign}(sk_{\mathsf{SIG}}, m_3)$. Then the reader responds (m_3, σ) to the tag.

It is easy to see that the output message from the reader is publicly verifiable because anyone can check $\mathsf{Verify}(vk_{\mathsf{SIG}}, m_3, \sigma) = 1$ holds or not.

Third Example Π_3':

Let $f : \mathcal{X} \to \mathcal{Y}$ be a one-way function. The reader runs Π to obtain (pk, sk) and shares secret keys with each tag in some cases. Choose $x \xleftarrow{\mathsf{U}} \mathcal{X}$ and compute $y := f(x)$. The reader publishes $pk' := (pk, f, y)$ and holds x as a special secret key of the reader in Π_3'. The authentication is executed as follows:

1. The reader obtains m_1 from Π and sends it to the tag.
2. When the tag receives the message, it generates m_2 with Π and responds $m_2' := 1 \| m_2$ to the reader.
3. When the reader receives the message m_2', it is parsed as $b \| m_2$. If $b = 1$, the reader generates m_3 and sends it to the tag (this is the same as the honest execution of Π). If $b = 0$, the reader outputs x as the third message.

It is clear that the above RFID authentication protocols satisfy strong ZK′-privacy. The simulator against ZK′-privacy can issue the $\mathsf{SendReader}$ query to obtain reader's signature and internal secret x, respectively. The output from the tag in Π_1' can be simulated based on the proof strategy for Lemma 1. The other messages are trivially simulated by the assumption that Π is strong ZK′-privacy.

In contrast, we can show that these protocols do not satisfy wide-weak SIM-privacy. The SIM adversary $\mathcal{A}$ can obtain the actual message from the party with the $\mathsf{SendReader}$ and $\mathsf{SendTag}$ query, so we consider the adversary who outputs 1 iff the signature verification holds in Π_1' and Π_2'. On the other hand, the simulator in SIM-privacy cannot output any valid signature to the adversary. If it happens, we can build a forger against the signature algorithm .

In the case of Π_3', the SIM adversary $\mathcal{A}$ launches the reader and sends $0 \| m_2$ to the reader to obtain x. $\mathcal{A}$ sets $b := 1$ iff $y = f(x)$ and terminates the experiment

by outputting b. It is obvious that $\Pr[\mathsf{Exp}^{\mathsf{SIM}\text{-}0}_{\Pi'_3,\mathcal{A}}(k) \rightarrow 1] = 1$. However, it is infeasible for any simulator to output x' such that $y = f(x')$ from the assumption that f is a one-way function. Therefore we have $\Pr[\mathsf{Exp}^{\mathsf{SIM}\text{-}1}_{\Pi'_3,\mathcal{A},\mathcal{S}}(k) \rightarrow 1] \leq \varepsilon$ for a negligible fraction ε. Thus we have $\mathsf{Adv}^{\mathsf{SIM}}_{\Pi'_3,\mathcal{A},\mathcal{S}}(k)$ is not negligible. □

The third example is originally described in Pass, Shelat and Vaikuntanathan to show the gap between their variants of non-malleability definition for public key encryption [19]. We think that it is interesting to show the gap between IND-privacy and SIM-privacy based on the same idea. The main feature of the public verifiability is that the adversary can decide whether the communication message is generated by the actual reader/tag in the protocol.

4.5 Relationship in the Absence of Public Verifiability

We now consider that there is no public verifiability on the communication message. To provide the secret verifiability of the tag, we can think the following two classes:

A1. The consistency of the message (from the tag) is verifiable with the secret key of the tag.
A2. The consistency of the message (from the tag) is not verifiable with the secret key of the tag.

Many previous RFID authentication protocols based on the symmetric key primitives are classified in **A1**. Though, if we add another mechanism like a physically unclonable function, the anonymity of the tag can be ensured after the corruption of the tag [20,13].

Note that we assume the restriction for the corrupt query is the same (unfortunately, we cannot provide any equivalence from the original ZK/IND-privacy [12]) [4] .

Theorem 4. *Assume that an RFID authentication protocol Π satisfies security and the communication message in the protocol is not publicly verifiable. Then weak ZK′-privacy is equivalent to wide-weak SIM-privacy. Moreover, if the protocol is classified in A1, strong ZK′-privacy is equivalent to wide-strong SIM-privacy.*

Proof. It is easy to show wide-strong/wide-weak SIM-privacy implies strong/weak ZK′-privacy (see Section 4.3). For simplicity, we prove that weak ZK′-privacy implies wide-weak SIM-privacy. That is, if for any ZK′ adversary $\mathcal{A}_1$, there exists $\mathcal{S}_1$, for any $\mathcal{D}$, the protocol Π is weak ZK′-privacy, then we show that for any SIM adversary $\mathcal{A}_2$, there exists $\mathcal{S}_2$ such that Π is also wide-weak SIM-privacy.

Consider that $\mathcal{A}_1$ internally runs $\mathcal{A}_2$ and relays all oracle queries issued by $\mathcal{A}_2$ to the challenger. Since we now assume weak ZK′-privacy, the response to

[4] Recall that we assume that the adversary cannot convert any illegitimate tags to the virtual tag. Hence the wide-strong SIM-privacy is achievable (see [16,11]).

the SendTag query is surely simulated by $\mathcal{S}_1$. Therefore $\mathcal{S}_2$ can run $\mathcal{S}_1$ and send the output to $\mathcal{A}_2$ which is indistinguishable from any adversary. The remaining task for $\mathcal{S}_2$ is simulating the SendReader query and Result query. We recall that the output from the reader is not publicly verifiable in this setting and the adversary cannot check the validity of the message. Therefore $\mathcal{S}_2$ can choose arbitrary message which the distribution is identical to the protocol specification and respond it to $\mathcal{A}_2$ as the output of the SendReader query. The simulation for the Result query is as follows. If the communication message between the reader and tag is not modified, $\mathcal{S}_2$ consider that the reader accepts the session. $\mathcal{S}_2$ can consider the remaining sessions are rejected from the reader. Whenever $\mathcal{A}_2$ modifies the communication, these sessions are always rejected by the actual reader until $\mathcal{A}_2$ obtains the secret key of the tag. Otherwise, this contradicts to the fact that the RFID authentication protocol holds security. Remark that in case of the simulation between strong ZK′-privacy and wide-strong SIM-privacy, $\mathcal{S}_2$ can also obtain the tag's secret key along with $\mathcal{A}_2$. Therefore $\mathcal{S}_2$ can correctly simulate the behavior of the corrupted tag and check the validity of the message sent from the adversary, since we now concentrate on the case **A1**.

From the above argument, $\mathcal{S}_2$ can simulate SendTag, SendReader and Result queries whose outputs are indistinguishable from the real interaction. Therefore we can conclude that strong/weak ZK′-privacy is equivalent to wide-strong/wide-weak SIM-privacy, respectively. □

Theorem 5. *Assume that the communication message of an RFID authentication protocol Π is not publicly verifiable and the protocol is classified in A2. Then the strong ZK′-privacy does not imply the wide-strong SIM-privacy.*

Proof. Contrary to Theorem 4, we cannot provide the equivalence when we consider the case **A2**. We consider the following adversary to show the gap between them.

1. Activate the reader with the Launch query.
2. Obtain the secret key of the tag t with the Corrupt query.
3. Generate a valid message m_1 using the secret key of the tag and a random message m_0 which the distribution is same as the protocol specification whenever the reader waits for the tag's response.
4. Choose a random coin $c \xleftarrow{\mathsf{U}} \{0,1\}$ and send m_c to the reader with the SendReader query.
5. Obtain the authentication result c' of the session with the Result query after the session is finished and output 1 iff $c' = c$ holds.

In the strong ZK′-0 and wide-strong SIM-1 experiments, the adversary always outputs 1. Since the simulator in the strong ZK′-1 experiment can issue the same query as the adversary, Π holds the strong ZK′-privacy. On the other hand, the simulator in the wide-strong SIM-1 experiment cannot issue the Result query. This simulator must guess the authentication result for the adversary, but it is impossible since we now assume that the validity of the message m_c cannot be checked by the tag's secret key. Therefore Π does not satisfy the wide-strong SIM-privacy. □

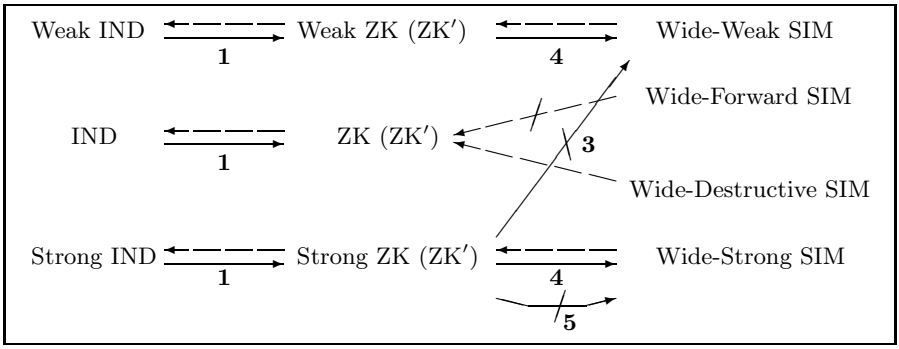

Fig. 2. A implies B if and only if there is a path from A to B, and the hatched arrows represent separations. Our result is represented by the solid arrow, and the dashed arrows represent results from prior works. The number on an arrow refers to the theorem in this paper. Recall that the relationship between ZK-privacy and SIM-privacy depends on the public verifiability of the reader and how to verify the tag's message.

We summarize the relationship the privacy notions in Figure 2.

5 Conclusion

We analyzed the three privacy models for RFID authentication protocols. Contrary to the discussion in Deng et al. [9], we showed that IND-privacy is equivalent to ZK-privacy. We also provided a polynomially equivalent variant of ZK-privacy to consider the relation between IND-privacy and SIM-privacy. Depending on the existence of reader's public verifiability, we showed the separation/equivalence between these privacy definitions.

References

1. Avoine, G.: Adversarial model for radio frequency identification. ePrint Archive, 2006/049 (2005)
2. Bellare, M., Desai, A., Pointcheval, D., Rogaway, P.: Relations among Notions of Security for Public-Key Encryption Schemes. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 26–45. Springer, Heidelberg (1998)
3. Bellare, M., Sahai, A.: Non-malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-Based Characterization. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 519–536. Springer, Heidelberg (1999)
4. Billet, O., Etrog, J., Gilbert, H.: Lightweight Privacy Preserving Authentication for RFID Using a Stream Cipher. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 55–74. Springer, Heidelberg (2010)
5. Burmester, M., Le, T.V., Medeiros, B.D., Tsudik, G.: Universally composable RFID identification and authentication protocols. ACM TISSEC 2009 12(4), 21:1–21:33 (2009)

6. Burmester, M., van, Le, T., de Medeiros, B.: Provably secure ubiquitous systems: Universally composable RFID authentication protocols. In: SecureComm 2006, pp. 1–9. IEEE (2006)
7. Canard, S., Coisel, I.: Data synchronization in privacy-preserving RFID authentication schemes. In: RFIDSec 2008 (2008)
8. Coisel, I., Martin, T.: Untangling RFID privacy models. ePrint Archive 2011/636 (2011)
9. Deng, R.H., Li, Y., Yung, M., Zhao, Y.: A New Framework for RFID Privacy. In: Gritzalis, D., Preneel, B., Theoharidou, M. (eds.) ESORICS 2010. LNCS, vol. 6345, pp. 1–18. Springer, Heidelberg (2010)
10. Ha, J., Moon, S.-J., Zhou, J., Ha, J.C.: A New Formal Proof Model for RFID Location Privacy. In: Jajodia, S., Lopez, J. (eds.) ESORICS 2008. LNCS, vol. 5283, pp. 267–281. Springer, Heidelberg (2008)
11. Hermans, J., Pashalidis, A., Vercauteren, F., Preneel, B.: A New RFID Privacy Model. In: Atluri, V., Diaz, C. (eds.) ESORICS 2011. LNCS, vol. 6879, pp. 568–587. Springer, Heidelberg (2011)
12. Juels, A., Weis, S.A.: Defining strong privacy for RFID. ACM Transactions on Information and System Security 13(1) (2009)
13. Kardaş, S., Kiraz, M.S., Bingöl, M.A., Demirci, H.: A Novel RFID Distance Bounding Protocol Based on Physically Unclonable Functions. In: Juels, A., Paar, C. (eds.) RFIDSec 2011. LNCS, vol. 7055, pp. 78–93. Springer, Heidelberg (2012)
14. van Le, T., Burmester, M., de Medeiros, B.: Universally composable and forward-secure RFID authentication and authenticated key exchange. In: ASIACCS 2007, pp. 242–252. ACM (2007)
15. Ma, C., Li, Y., Deng, R.H., Li, T.: RFID privacy: Relation between two notions, minimal condition, and efficient construction. In: ACMCCS 2009, pp. 54–65. ACM (2009)
16. Ng, C.Y., Susilo, W., Mu, Y., Safavi-Naini, R.: RFID Privacy Models Revisited. In: Jajodia, S., Lopez, J. (eds.) ESORICS 2008. LNCS, vol. 5283, pp. 251–266. Springer, Heidelberg (2008)
17. Ouafi, K., Phan, R.C.-W.: Traceable Privacy of Recent Provably-Secure RFID Protocols. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 479–489. Springer, Heidelberg (2008)
18. Paise, R.I., Vaudenay, S.: Mutual authentication in RFID. In: ASIACCS 2008, pp. 292–299. ACM (2008)
19. Pass, R., Shelat, A., Vaikuntanathan, V.: Relations Among Notions of Non-malleability for Encryption. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 519–535. Springer, Heidelberg (2007)
20. Sadeghi, A.R., Visconti, I., Wachsmann, C.: PUF-enhanced RFID security and privacy. In: SECSI 2010 (2010)
21. Vaudenay, S.: On privacy models for RFID. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 68–87. Springer, Heidelberg (2007)
22. Vaudenay, S.: Privacy Models for RFID Schemes. In: Ors Yalcin, S.B. (ed.) RFIDSec 2010. LNCS, vol. 6370, pp. 65–65. Springer, Heidelberg (2010)