INVITED PAPER *Special Section on Trust, Security and Privacy in Computing and Communication Systems*

A Survey on Privacy Frameworks for RFID Authentication

Chunhua SU[†], ***Member***, **Yingjiu LI**[††], **Yunlei ZHAO**[†††a)], **Robert H. DENG**[††], **Yiming ZHAO**[††††], ***and*** **Jianying ZHOU**[†], ***Nonmembers***

SUMMARY Due to rapid growth of RFID system applications, the security and privacy problems become more and more important to guarantee the validity of RFID systems. Without introducing proper privacy protection mechanisms, widespread deployment of RFID could raise privacy concerns to both companies and individuals. As a fundamental issue for the design and analysis of secure RFID systems, some formal RFID privacy frameworks were proposed in recent years to give the principles for evaluating the security and privacy in RFID system. However, readers can be confused with so many proposed frameworks. In this paper, we make a comparative and survey study on the proposed RFID privacy frameworks. We mainly divide the existing models into three categories, the four-oracle framework, eight-oracle framework and Universal Composability framework. We give a brief review on the existing models and describe their abilities to model the adversarial behavior in RFID systems. We then analyze relations among those existing RFID privacy models and make some comparisons among their properties.

key words: *RFID security, authentication protocol, privacy*

1. Introduction

RFID (Radio-Frequency IDentification) is a technology for automated identification of objects and people using the radio wave. It has a lot of applications such as payments, transportation, supply chain and access management. An RFID system usually consists of three kinds of entities (database, readers, and tags) as well as communication channels. Normally, it is assumed that the communication channels between readers and database are secure. RFID reader/tag authentication is the major functionality for RFID system. In such authentication protocols, the RFID tags have to authenticate themselves to a reader, in the case of mutual authentication, the reader needs also to authenticate itself to the tags in such a way that they are assured of each other's identities.

For an RFID protocol, it must be authenticated and identified correctly by legitimate users (the completeness property), and that cloned/counterfeited tags or readers must be detected and rejected (the authentication property). Furthermore, most applications legitimately require that authentications remain anonymous (and even untraceable) for other entities, so that tags cannot be traced (the privacy property). This leads to the notion of privacy-preserving RFID authentication.

For an RFID system, it is important to provide the privacy protection, particularly when a specific tag or a set of tags are associated with a particular person or can cause location disclosure of both person and goods. In recent years, many research papers are published to propose conceptual frameworks and technique (protocol based) solutions for such problems. So many proposals can make people confused. In view of this, in this paper, we are mainly concerned with formal provable privacy models for RFID systems and do some comprehensive analysis on these models.

1.1 Related Works

There are many research papers about RFID privacy-preserving protocols published in last decade, Juels provided a survey of much of the related literature in [11]. For more research papers about RFID privacy protection, the reader can refer to Avoine's current online bibliography at [2]. There are many RFID privacy models proposed to evaluate how strong privacy can be provided by a protocol. Avoine first formalized the adversary model in RFID systems and proposes very general and flexible definitions of RFID privacy [1]. Based on the adversary model of [1], Juels and Weis defined the notion of strong privacy based on indistinguishability of arbitrary selected two tags in RFID systems [12]. Following these works, Ha *et al.* [10] proposed a privacy model which is based on the unpredictability between a real protocol transcript and the randomly generated messages from the same domain. To get a more general privacy model, Ma *et al.* proposed an extended version of the Ha *et al.* [10]'s model, and Lai *et al.* [14] further extended the model in Ma *et al.*.

In Asiacrypt 2007, Vaudernay proposed a new framework and classified the privacy models into eight categories [23], this framework aims at abstracting most previous works of RFID authentication. One year later, Paise and Vaudernay extended Vaudernay's model to the mutual authentication scenario [19]. Very recently, based upon Vaudenay's model, Canard *et al.* proposed an RFID privacy model by focusing upon untraceability of tags. In [9], Deng *et al.* proposed a zero-knowledge based framework for RFID privacy. Universal composability (UC) based frameworks for

Manuscript received March 16, 2011.
Manuscript revised July 14, 2011.

[†] The authors are with Institute for Infocomm Research, Singapore.
[††] The authors are with the School of Information Systems, Singapore Management University, Singapore.
[†††] The author is with Software School, Fudan University, China.
[††††] The author is with the School of Computer Science and Technology, Fudan University, China.
a) E-mail: ylzhao@fudan.edu.cn (Corresponding author)

DOI: 10.1587/transinf.E95.D.2

RFID privacy are considered in [4], [5], [13], [20].

1.2 Our Contributions

In this paper, we make a comparative and survey study on the recent research results of RFID authentication security and privacy models. Our contributions can be summarized as follows:

- We focus on the up-to-date results of RFID authentication security and privacy models, and classified the models into three frameworks: four-oracle based frameworks, eight-oracle based frameworks, and universally composable (UC) framework. We point out their strong points and weak points based on the adversarial behaviors and security and privacy proof techniques.
- We make some summaries on the basic ideas and principles of each privacy model and make them easier to understand. We also pointed out some incompleteness in the current privacy models, which provides a direction to design more reasonable models for evaluating privacy issues for RFID authentication protocols.

2. Preliminaries

Here, we will provide the definition of RFID system and introduce some necessary preliminaries.

2.1 RFID System Modeling

An RFID system can be formulated and modeled as follows:

1. Initiate a reader R with certain keys for verifying tags' identities. Use an algorithm SetupReader (k) where k is the security parameter to generate common input, domain parameters, the key to be used in the authentication for the reader R, and initialize a database.
2. Create a set of n tags, each tag T_i having a unique ID_i, where $1 \leq i \leq n$. Use an algorithm SetupTag (ID) with common input to generate tag-specific secret K and its initial state st. When the tag is a legitimate one, the entry $(ID; K)$ is inserted in the database.
3. Design a 2-party protocol π between the reader and a tag in which the reader protocol uses the common input, the database, and the secret.

An RFID system RS can be considered as a tuple $(R, T, InitProcess, \pi)$, where every tag in T exchanges messages with the reader R through a protocol π after some initializing processes. A tag $T_i, 1 \leq i \leq n$, exchanges messages with the reader R through a protocol $\pi(R, T_i)$. Canonically, there are 2 or 3 rounds message exchanged as shown in Fig. 1:

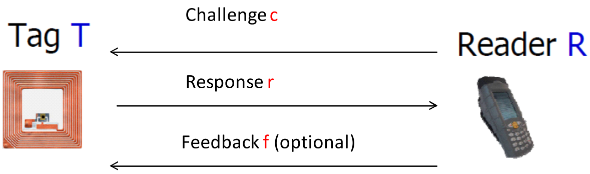


Fig. 1 RFID authentication protocol.

Normally, we assume that in the RFID system, the reader is secure; in other words, the legitimate reader is a "black-box" to an adversary.

2.2 Adversary Modeling and Security Proof

The privacy frameworks for RFID system are based on provable security in cryptography. The security definitions in the existing works for RFID authentication protocols are built on the traditional game-based security model. The inputs to the adversary must be determined, and the behaviors of the adversary are modeled using some oracles to which the adversary can access. The protocol has to give the winning condition: achieving the winning condition is the only way to break the RFID authentication.

The model first sets the goal of the attack in RFID authentication, says, under which conditions the adversary can win, then captures the adversary's attack as a series of queries to some oracles which model the execution of the protocol under the adversarial control of the adversary. The RFID protocol is said to be secure if the probability of adversary's success is negligible. Usually, the adversary $\mathcal{A}$ is modeled as a probabilistic polynomial-time (PPT) concurrent man-in-the-middle (CMIM) against (R, T_i) with tag corruptions.

- The adversary's capabilities: The capabilities are modeled by the oracles to which the adversary can have access.
- The adversary's strategy: all possible combinations of the oracles queries made by the adversary.
- The adversary's goal: The adversary can successfully trace the tags, this can be considered as the winning condition of the adversary.

In this paper, we present the adversary's attacks as privacy experiments which is similar to the classical definition of indistinguishability in provable security. To model the attacks against RFID authentication protocols, we often divide the attacks into two stages. The first stage is learning stage, in which the adversary can eavesdrop and interrupt the communications between reader and tags, and even corrupt the tags to get their internal states st during this stage. The second stage is guessing stage, in which the adversary outputs the results based on what they learned in the former stage. Roughly speaking, we say that the adversary cannot break the security or privacy of the underlying RFID authentication protocol, if the advantage of adversary's guess is no more than choosing a random bit.

3. Privacy Frameworks Based on Four Oracles

There are four oracles that are used to model the adversary's attack. These four oracles model the capability of the adversary in eavesdropping and interrupting the protocol messages being communicated, and in corrupting tags to get their internal states. In the following, we specify *the basic versions* of the four oracles that the adversary $\mathcal{A}$ is permitted to query.

1. InitReader (): It makes the reader R to start a new session of protocol π and generate a session identifier sid and challenge message $c_{sid} \in_R P_{CH}$. The reader returns the session identifier sid and the challenge message c_{sid}.
2. SendTag $(T_i, \mathrm{sid}, c_{sid})$: It invokes tag T_i to start a session of protocol π with session identifier sid and challenge message $c_{sid} \in P_{CH}$. The tag T_i responds with the session identifier sid and a message $r_{sid} \in P_{RS}$.
3. SendReader (sid, c, r): It returns the challenge and response messages c, r with session identifier sid and (in three-round protocol) the reader's final message f_{sid}.
4. Corrupt (T_i): Adversary $\mathcal{A}$ obtains the secret-key and internal state information (as well as the random coins) currently held by T_i. Once a tag T_i is corrupted, all its actions are controlled and performed by the adversary $\mathcal{A}$.

Let O_1, O_2, O_3 and O_4 denote InitReader, SendTag, SendReader and Corrupt oracles, respectively. Denote by $O = \{O_1, O_2, O_3, O_4\}$. Throughout the experiments, the adversary $\mathcal{A}$ is allowed to launch O_1, O_2, O_3 and O_4 oracle queries without exceeding n_1, n_2, n_3 and n_4 overall calls, respectively. The oracles which are used by adversary can be used to model the eavesdropping, alteration of communication messages, replay attacks, corruption of tags, and physical or side-channel attacks to tags.

3.1 Indistinguishability-Based Privacy Model

The indistinguishability-based (Ind) privacy model is proposed by Juels *et al.* [12]. The goal of the adversary in this experiment is to distinguish between two different tags within the limits of its computational power and functionality-call bounds. The adversary uses two algorithms: A_1 to select a pair of target tags together with some state information st collected in the learning stage, and A_2 to interact with the reader and the challenge tag (which is chosen randomly from the pair of target tags) and output the final result in the guessing stage. The adversary's behaviors of attacking the privacy of RFID system can be modeled by the following game:

Remark: The ind-privacy framework [12] works for any RFID protocols, not necessarily limited to the special 3-round protocols as specified by the basic versions of the oracles above. Also, the ind-privacy framework works even if the adversary is allowed to learn the protocol outputs (i.e., whether the reader or the tag is accepted or rejected), which corresponds to the Corrupt (π) oracle in the eight-oracle based frameworks. As noted in [9], requiring the selected target tags to be *clean* is crucial for the ind-privacy formulation to be sound, which is not explicitly addressed in [12]. Also, as noted in [9], the ind-privacy framework is not appropriate to RFID systems consisting of a single (high-value) tag.

Algorithm 1 Adversarial Game in Ind-Privacy Model

1. We assume that there are a reader R and a set of tags T with $|T| = n$ for the RFID system;
2. The adversary eavesdrops and interrupts all the communications between reader and tags. It randomly selects two target tags, and corrupts other tags and gets their states using algorithm A_1 in this learning stage: $\{T_i, T_j, st\} \leftarrow A_1^{O}(R, T)$;
3. The adversary separates the target tags and sets $T' = T - \{T_i, T_j\}$;
4. The challenger flips a coin $b \in_R \{0, 1\}$ to select one challenge tag from the target tags, if $b = 0$ then $T_c = T_i$, else $T_c = T_j$;
5. The adversary further queries the oracles to guess the b as $b' \leftarrow A_2^{O}(R, T', st, T_c)$, with the limitation that either T_i or T_j cannot be corrupted in this guessing stage.
6. The experiment outputs 1 which means it successes in the attack if $b = b'$, 0 otherwise.

3.2 Unpredictability Privacy Model

In 2008, Ha *et al.* [10] proposed a privacy model for the RFID location privacy, which is referred to as unpredictability privacy (unp-privacy, in short). Their model focuses on each round of information exchange in the authentication protocol between tag and reader. Roughly speaking, an RFID protocol is of unp-privacy if the exchanged messages are indistinguishable from some dummy message chosen randomly according to some predetermined distributions.

Algorithm 2 Adversarial Game in Unp-Privacy Model

1. We assume that there are a reader R and a set of tags T with $|T| = n$ for the RFID system;
2. The adversary uses an algorithm $A_1$to select a challenge tag T_c from the n tags, and then it gets the challenge message c_0 from reader to T_c and a state: $\{T_c, c_0, st\} \leftarrow A_1^{O_1, O_2, O_4}(R, T)$;
3. The challenger then sets $T' = T - \{T_c\}$, and flips a coin $b \in_R \{0, 1\}$ to select one challenge tag. If $b = 0$ then the challenger generates two pseudorandom message (r', f') from some certain domains which are used in the real protocol. If $b = 1$, then challenger gets $(c_0, r', f') \leftarrow \pi(R, T_c, sid)$ from a real protocol.
4. The challenger sends (r', f') to the adversary. The adversary queries the oracles to guess the b as $b' \leftarrow A^{O_1, O_2, O_3, O_4}(R, T', st, r', f')$, under the limitation that oracle access to T_c is denied.
5. The experiment outputs 1 (which means the adversary successes in the attack) if $b = b'$, 0 otherwise.

In this model, all the messages c, r, f (random generated or from real protocol) must have the same lengths and generated from the same domains, respectively. During the guess stage, the adversary is allowed to query O_1, O_2 and O_3 oracles to the challenge tag T_c in the ind-privacy experiment, while it is not allowed to query any oracle to T_c in the unp-privacy experiment.

3.3 Extended Unpredictability-Based Privacy Model

Ma *et al.* extended and refined the ind-privacy model into so called extended unp-Privacy (eunp-privacy) model in 2009 [15]. Compared to unp-privacy model, the adversary in eunp-privacy is allowed to challenge for w test messages rather than only one test message as in the unp-privacy experiment. The adversary uses two algorithm A_1 and A_2 in the experiment. The eunp-Privacy experiment can be briefly described as follows:

Algorithm 3 Adversarial Game in Extended Unp-Privacy

```
1. There are a reader $R$ and a set of tags $T$ with $|T| = n$ in the system;
2. The adversary $\mathcal{A}$ outputs a challenge tag $T_c$ and the state information using an algorithm $A_1$: it gets $\{T_c, st\} \leftarrow A_1^{O}(R, T)$ and sets $T' = T - \{T_c\}$. Then, let $st_0 = st$ and $M = \{\epsilon\}$, for $i = 1$ to $w$, $(c_i, st_i) \leftarrow A_1^{O}(R, T', st_{i-1}, M)$;
3. The challenger flips the coins, if $b = 0$ then for each $i, 1 \leq i \leq w$, it generates two pseudorandom message $(r'_i, f'_i)$ from some domains, else $(c_i, r_i, f_i) \overset{R}{\leftarrow} \pi(R, T_c, sid_i)$ and sets $(r'_i, f'_i) = (r_i, f_i)$, $M = M \cup \{(r'_i, f'_i)\}$. Finally, the adversary outputs $b' \leftarrow A_2^{O}(R, T', st_w, M)$, under the limitation that oracle access to $T_c$ is denied to $A_2$;
4. The experiment outputs 1 if $b = b'$, 0 otherwise.
```

For all the w test messages, the experiment uses the same coin $b \in_R \{0, 1\}$. If $b = 1$, algorithm A_2 is given challenge messages which are all selected from protocol messages; otherwise, A_2 is given random challenge messages all selected randomly. Later, the eunp-privacy model was further extended by Lai *et al.* [14] into the mutual RFID authentication, but the mutual authentication protocol proposed in [14] was later broken by Ma [16].

Remark: Both the unp-privacy and eunp-privacy models work for a special kind of RFID protocols, i.e., 3-round RFID protocol where the second-round message from tag is indistinguishable from a random string (which is usually achieved by using a pseudorandom function). This limits the applicability of unp-privacy and eunp-privacy models. Moreover, the unp-privacy and eunp-privacy models (implicitly) prohibit the adversary to learn the protocol outputs, which is unrealistic in reality. That is, the adversaries considered within the unp-privacy and eunp-privacy frameworks are actually narrow ones as defined in [23]. This shows that unp-privacy and eunp-privacy are incomparable with ind-privacy in general, as in the ind-privacy experiment the adversary is allowed to learn the protocol outputs.

3.4 Zero-Knowledge Based Model

In 2010, Deng *et al.* [9] proposed a new model call zero knowledge-based (ZK) privacy model for analyzing the privacy of RFID system. The idea of the model comes from the GMW model in the secure multi-party computation and the zero-knowledge formulation. The idea of the model is that a real protocol that is run by RFID reader and tags (in a world where no trusted party exists) is secure, if no adversary can do more harm in a real execution than in an execution that takes place in the ideal world. Their privacy model defines the privacy of RFID system by using two experiments, one is the *real world experiment* and the other is *ideal world experiment*. The adversary $\mathcal{A}$ interacts with the reader R and tags in T via the four oracles in O; At the end of the adversarial experiment, $\mathcal{A}$ outputs a transcript of a session.

$\mathcal{A}$ can use a pair of algorithms (A_1, A_2) and run in two stages. In the first stage, algorithm A_1 is concurrently interacting with R and all the tags in T via the four oracles in O, and is required to output a set C of clean tags, along with some state information st, at the end of the first stage. As formulated in [9], a clean tag is an uncorrupted tag that is currently at the status of waiting for the first-round message from the reader to start a new session. Between the first stage and the second stage, a challenge tag T_c, is taken uniformly at random from C. In the second stage, on input st, A_2 concurrently interacts with the reader R and the tags in $T' = T - C$ via the four oracles in O, and additionally has blind access to T_c via a specialized interface $\mathcal{I}$. Note that $\mathcal{A}$ cannot corrupt any tag in C in the second stage. Finally, $\mathcal{A}$ gets its outputs.

Algorithm 4 Adversarial Output in Real World of ZK-privacy

```
1. There are a reader $R$ and a set of tags $T$ with $|T| = n$;
2. At first, the adversary uses $A_1$ to output a set of clean tags and the state information: $\{C, st\} \leftarrow A_1^{O}(R, T)$, where $C = \{T_1, T_2, \ldots, T_m\} \in T$ is a set of clean tags, $1 \leq m \leq n$;
3. $g \overset{R}{\leftarrow} \{1, \ldots, m\}$, set the challenge tag $T_c = T_g$ and $T' = T - C$;
4. Then the adversary uses another algorithm $A_2$ to interact with $R, T'$ and $T_g$ via four oracles and gets: $view_{\mathcal{A}} \leftarrow A_2^{O}(R, T', \mathcal{I}(T_g), st)$;
5. The experiment outputs $(g, view_{\mathcal{A}})$, where $view_A$ includes the public parameters $para$, the random coins of $A$ and all answers from the oracles in $O$.
```

Note that $view_A$ does not explicitly include the oracle queries made by $\mathcal{A}$ and $\mathcal{A}$'s output at the first stage, as all these values are implicitly determined by the system public parameter $para$, $\mathcal{A}$'s coins and all oracle answers to A's queries. Recall that a clean tag is an uncorrupted tag that is currently at the status of waiting for the first-round message from the reader to start a new session.

Algorithm 5 Simulator in Ideal World

```
1. Setup the reader $R$ and a set of tags $T$ with $|T| = n$;
2. The simulator queries the oracles and uses an algorithm $S_1$ to output a set of clean tag and gets $\{C, st\} \leftarrow S_1^{O}(R, T)$, where $C = \{T_1, T_2, \ldots, T_m\} \in T$ is a set of clean tags, $1 \leq m \leq n$;
3. The simulator randomly selects a tag as $g \overset{R}{\leftarrow} 1, \ldots, m$, and sets $T' = T - C$;
4. Then simulator uses another algorithm to interact with the reader and tags in $T$ via the four oracles, and gets $view_{\mathcal{S}} \leftarrow S_2^{O}(R, T', st)$, where $view_{\mathcal{S}}$ particularly includes all oracle answers to queries made by $\mathcal{S} = (S_1, S_2)$;
5. output $(g, view_{\mathcal{S}})$.
```

The simulation by the simulator $\mathcal{S} = (S_1, S_2)$ is depicted with Algorithm 5. In the second stage of $\mathcal{S}$, on input st, S_2 concurrently interacts with the reader R and the tags in $T \setminus T_c$, and outputs a simulated view, denoted $view_{\mathcal{S}}$, at the end of the second stage.

Informally speaking, if the outputs of real world adversary and ideal world simulator are computationally indistinguishable, the protocol satisfies the ZK-privacy. The definition of ZK-privacy implies that the adversary $\mathcal{A}$ cannot distinguish any challenge tag T_g from any set C of tags; otherwise, $\mathcal{A}$ can figure out the identity of T_g from its view $view_{\mathcal{A}}$, while this tag's identity cannot be derived from any simulator's view $view_{\mathcal{S}}$.

In the zk-privacy model, it is explicitly specified that the output bits of protocol participants (which indicate authentication success or failure) are publicly accessible to the adversary. Note that, in reality, such outputs can be publicly observed from the behaviors of protocol participants during/after the protocol run or can be learnt by some other side channels. Also, zk-privacy model applies to RFID protocols in general, without limitation to special 3-round or pseudorandom tag-message protocols. It is shown in [9] that zk-privacy is *strictly* stronger than ind-privacy. As clarified in [9], the zk-privacy model can also be extended to capture forward/backward privacy notions.

4. Privacy Frameworks Based on Eight Oracles

In this section, we review the frameworks of [8], [19], [23] that use eight oracles in capturing adversarial capability. For presentation simplicity, we refer to the frameworks proposed in [19], [23] as the Paise-Vaudenay (PV) model.

4.1 The PV Model

Vaudenay *et al.* [23] proposed the first comprehensive privacy framework that uses eight oracles to capture the capability of adversary, which is further extended into the mutual authentication scenarios in [19]. Their additional four oracles to which adversaries can have access are as follows, while other four oracles are the same as in four-oracle based framework. Note that the Result oracle is also allowed in the models of ind-privacy and zk-privacy, but is prohibited in the models of unp-privacy and eunp-privacy. In particular, it is noted in [9] that the zk-privacy framework can be generalized into the eight-oracle setting, where the zk-privacy formulation with four orales (with the Result oracle embeded) is mainly for presentation simplicity there.

- CreateTagb (ID): creates a free tag, either legitimate ($b = 1$) or not ($b = 0$), with unique identifier *ID*.
- DrawTag (distr) → $(vtag_1, b_1, \ldots, vtag_n, b_n)$: moves from the set of free tags to the set of drawn tags a tuple of tags at random following the probability distribution distr. The oracle returns a vector of fresh identifiers $(vtag_1, \ldots, vtag_n)$ which allows to anonymously designate these tags. This oracle keeps a hidden table T such that $T(vtag)$ is the ID of *vtag*.
- Free (tag): The adversary moves the virtual tag *vtag* back to the set of the free tags. This makes *vtag* unreachable
- Result (π): The adversary sends it a request, when authentication is complete and correct, it returns 1 and 0 otherwise. As mentioned, this oracle is implicitly allowed in the ind-privacy model, and is explicitly rendered in the zk-privacy model (but is prohibited in the models of unp-privacy and eunp-privacy).

The PV model defines the authentication between RFID tags and readers, and several privacy notions that correspond to adversaries with different tag corruption abilities. In the PV model there are two adversaries, one is an adversary $\mathcal{A}$ who aims to break the privacy of the real RFID authentication, the other is a blinded adversary $\mathcal{B}$ who cannot make Launch, SendReader, SendTag, and Result queries. In the eight-oracle based framework, the blinded adversary $\mathcal{B}$ for an adversary $\mathcal{A}$ is a polynomial-time algorithm which sees the same messages as $\mathcal{A}$ and simulates the Launch, SendReader, SendTag, and Result oracles to $\mathcal{A}$. A blinded adversary $\mathcal{A}^{\mathcal{B}}$ is itself an adversary who does not use the Launch, SendReader, SendTag, and Result oracles. Informally speaking, an RFID protocol is private against an efficient adversary $\mathcal{A}$ within the PV-model, if there exists another efficient $\mathcal{B}$ such that $|\Pr[A\ wins] - \left[A^B\ wins\right]|$ is negligible.

All adversaries are polynomial-time. According to the limitation of using the Corrupt and Result oracles, the adversaries can be classified into five classes (or eight types by considering whether the underlying adversary is narrow or not) within the framework of eight oracles.

1. Strong Adversaries: The adversaries who have access to all of the oracles during the attack.
2. Destructive Adversaries: The adversaries who never use *vtag* again after a Corrupt (*vtag*) query, which means the adversaries destroy the tag after the corruption.
3. Forward Adversaries: The adversaries who once make the Corrupt query can only make other Corrupt queries.
4. Weak Adversaries: The adversaries who cannot make the Corrupt query.
5. Narrow Adversaries: The adversaries who cannot make the Result query.

It was proven in [19], [23] that public-key cryptography can assure the highest level of feasible privacy in RFID: narrow-strong and forward privacy, even with stateless protocols. [19], [23] also showed narrow-destructive privacy for an hash chain-like protocol in the random oracle model, and weak privacy for a simple challenge-response protocol. But, the problem of achieving destructive privacy or forward privacy without public-key techniques are left open there.

As it is impossible to reach the strongest privacy property against strong adversary with the capability of arbitrary corruption within the PV-model, Ng *et al.* have introduced in [17] the notion of wise adversaries. These adversaries are restrained (compared to those of Vaudenay) such that they are not able to access twice the same oracle with the same input, and they are also not able to access oracles where the results can be precisely predicted. Under these assumptions, they prove that it is indeed possible that a scheme ensures the strong privacy property against wise adversary. Furthermore, the work of [17] proved the equivalence between some of the eight privacy properties of Vaudenay and thus reduce them to three different properties.

Remark: As noted in [9], in the PV-model the simulator is not required to handle corruption queries made by the adversary, and it is not clear how such a simulator acts upon tag corruption queries made by an adversary. The PV-model allows the strong adversary arbitrary corruption at any point of protocol run, but this way forward/backward privacy may not be achievable in this case. In formulating authentication from reader to tag, the PV-model only considered matching sessions of identical session transcripts, and did not take the cutting-last-message attack (as clarified in [9]) into account. Also, the PV-model did not formulate adaptive completeness, with no adversarial desynchronizing attacks being taken into account. As a consequence, the PV-model and the ind-privacy are incomparable *in general*, while zk-privacy is provably strictly stronger than ind-privacy.

4.2 Untraceability Model

In 2010, Canard *et al.* proposed a so-called untraceability model [8] which is based on Vaudenay's model. They introduced a new notion called non-obvious link. A link is a couple of pseudonyms associated to the same identifier inside a tag. Links are chronologically ordered in their model, where the notation (t_i, t_j) means that t_i has been freed before that t_j has been drawn. Informally, a non-obvious link (n.o.l.) is a link between two pseudonyms which cannot be defined without using some hidden (or not) information in the sent messages.

The untraceability experiment is defined as follows, where the adversary class P belongs to strong, destructive, weak as in the PV-model. The adversary in [8] is equivalent to the blinded adversary of Vaudenay. Although this latter has access to the remaining oracles (Execute, Launch, SendReader, SendTag, Result), all the answers of these oracles are simulated by a Blinder who does not know any secret values of both tags and reader.

Algorithm 6 Adversarial Behavior in Untracability Model

```
1. The challenger $C$ initializes the system and sends the public parameters to $\mathcal{A}$.
2. $\mathcal{A}$ interacts with the whole system using the eight oracles, limited by the adversary classes in PV-model.
3. The adversary $\mathcal{A}$ output one link of $(t_i, t_j)$.
```

In the model of [8], a tag can have multiple different pseudonyms in different sessions. Informally, an RFID scheme is private, if for any pair (t_i, t_j), no probabilistic polynomial-time algorithm can tell whether t_i, t_j correspond to the same tag or not, where t_i, t_j are two pseudonyms used in two sessions in chronological order. That is, any polynomial-time adversary $\mathcal{A}$ is not able to make the link between several authentications of a same tag [8]. [8] classified three privacy classes: (1) Standard untraceability: the adversary does not make any corruption query. (2) Past untraceability: the adversary corrupts t_j and use the internal state information of t_j to trace back t_i. (3) Future untraceability: the adversary corrupts t_i and use the internal information of t_i to trace forward t_j. The work [8] didn't prove that their future-untraceability implies the Vaudenay's destructive privacy, while it is proved that the opposite is false. It is left as an interesting open question there to prove that future-untraceability implies the narrow-strong privacy.

Remark: As noted in [9], the framework of [8] assumes that only the secret-key of the tag is revealed to the adversary upon corruption of a tag; while most other framework assume that, upon corruption of a tag, both its secret-key and internal state (*including random coins*) are revealed to the adversary. The security analysis of the RFID protocols proposed in [8], based on public-key cryptosystems, implicitly relies upon this assumption on tag corruption (i.e., no random coins are revealed upon tag corruption). In the framework of [8], no internal state updating mechanism is given. But, without an appropriate internal state updating mechanism, symmetric-key encryption and/or message authentication code alone are almost useless in achieving past or future privacy in accordance with the framework in [8].

5. Universal Composability Based Framework

Game-based privacy frameworks used in Sect. 3 and Sect. 4 have the advantages of easy-to-understand and simple-to-apply in the formalization of RFID authentication protocols. The inputs to the adversary must be determined at the beginning of the adversarial experiment, and the behaviors of the adversary are modeled using some oracles to which the adversary has access. These models give the winning condition: achieving the winning condition is the only way to break the RFID authentication. Unfortunately, such game-based security modes are insufficient to analyze the security of an RFID protocol when it is used as a sub-protocol in a composite setting.

Universal composability (UC) is a powerful notion proposed by Canetti [6] to describe cryptographic protocols that behave like ideal functionality, and can be composed *in arbitrary way*. The salient feature of UC secure protocols is that their security preserves even when it is composed with any arbitrary protocols (captured by unpredictable environment) concurrently in asynchronous networks (like the Internet). In such settings, a protocol execution may run concurrently with an unknown number of other protocols.

UC framework aims for designing protocol that meet the security requirements in the composite setting. It is based on simulation proof and guarantees quite strong secu-

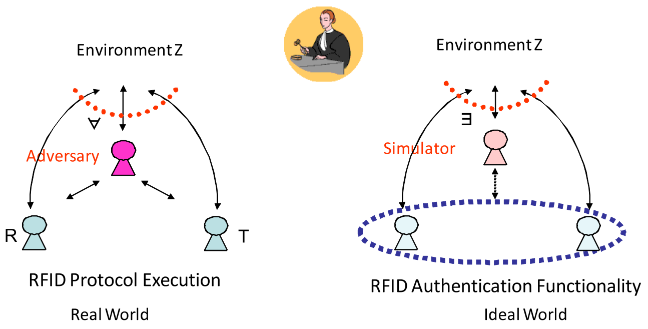


Fig. 2 Universal composability.

The Functionality of RFID Mutual Authentication

The functionality $\mathcal{F}_{\text{RMA}}$ is parameterized by a security parameter k, some public parameters *para* and an $\mathcal{NP}$-relation $\mathcal{R}$. It interacts with an adversary $\mathcal{S}$ and a set of RFID tags and a reader.

1. Upon receiving the identifier (`ReaderIden`, sid, U) from reader, store (sid, U) and send (`ReaderIden`, sid) to $\mathcal{S}$.
2. Upon receiving (`TagIden`, sid, V, ID_i) from tag T_i of identity ID_i, store (sid, V) and send (`TagIden`, sid) to $\mathcal{S}$ if $\mathcal{R}(k, para, U, V) = 1$, where U (resp., V) is some private values held by the reader (resp., the tag) such that the authentication is successful if and only if U and V match (i.e., satisfying the relation $\mathcal{R}$).
3. Upon receiving (`Output`, sid, R) from $\mathcal{S}$, retrieve (sid, U, V) and output ID_i to reader and send `OK` to tag T_i if and only if $\mathcal{R}(k, para, U, V) = 1$.

Fig. 3 The ideal functionality of RFID mutual authentication, $\mathcal{F}_{\text{RMA}}$.

rity and composability properties. The UC framework considers the indistinguishability between the real world protocol execution with an arbitrary adversary and the simulation in an ideal world. There is a so-called environment $\mathcal{Z}$ who can set inputs to all parties and can interact with the adversary. In the ideal world, both the reader and the tags send inputs to a trusted party that is modeled as a functionality, which executes the RFID mutual authentication protocol and sends the outputs to corresponding parties. In the real world, the reader and the tags run a real mutual authentication protocol without the trusted party. Informally speaking, we say that a protocol is UC secure, if for any efficient adversary $\mathcal{A}$ in the real world there exists a simulator, which corresponds to an adversary in the ideal world, such that no efficient environment $\mathcal{Z}$ can distinguish whether it is interacting with protocol players and $\mathcal{A}$ in the real world or protocols players and the simulator S in the ideal world (See Fig. 2.).

Some RFID authentication protocols under the UC framework have been proposed [4], [5], [13], [20]. The ideal functionality of RFID mutual authentication $\mathcal{F}_{\text{RMA}}$ w.r.t. an $\mathcal{NP}$ relation $\mathcal{R}$ is described in Fig. 3. In the UC framework, the adversary can corrupt both reader and tags in the authentication protocol. Different from other frameworks, the simulator has to simulate the reader in the ideal world.

Remark: Though the original goal of UC framework aims for strong composability against arbitrary external protocols, the actual security guarantee of UC is quite subtle. As clarified in [7], [24], [25], the UC security implicitly assumes that the external arbitrary protocols, with which the protocol in question is to be composed, are "independent" of the protocol in question in the sense that they do not share common states.[†] This requirement is quite strong and can be unrealistic for protocol composition in reality. For this reason, UC security does not necessarily imply concurrent non-malleability by definition, which means that UC RFID authentication does not necessarily imply ZK RFID authentication. Another point is, due to the high system complexity of UC framework, the security analysis in accordance with the UC framework is usually more complex.

6. Conclusion and Comparisons

In this section, we compare the existing RFID privacy models and clarify the same and different features among the models. At first, we present the basic ideas of some existing privacy model as follows:

- Ind-privacy model: It defines the privacy as adversaries cannot distinguish one tag to another from any two tags.
- Unp-privacy model: The adversaries cannot distinguish the messages sent between tags and reader in the authentication from random generated strings of the same length.
- Eunp-privacy model: This model extends the unp-privacy by enabling the adversaries w times oracle queries.
- ZK-privacy model: The simulator can simulate the tag in the real world authentication, so it means any efficient adversary cannot distinguish any challenge tag from any set of tags.
- Untracability model: Given two transcripts t_i and t_j, which appeared in the RFID authentications, and a specific tag identify ID, no efficient adversary can decide whether t_i and t_j correspond to the same tag of ID.
- UC model: It considers the indistinguishability between the execution of an RFID protocol in the real world and the execution in the ideal world w.r.t. an ideal functionality. Its goal is for securely deploying an RFID protocol (as a building module) in a high-level more complex system.

Secondly, we present a table to compare the merits of each model as follows (also as seen in Table 1).

6.1 Relations Among Four-Oracle Based Frameworks

- The eunp-privacy model implies the unp-privacy, and unp-privacy also implies the eunp-privacy. Thus, unp-privacy and eunp-privacy are equivalent [15].
- ZK-privacy implies ind-privacy, which holds unconditionally. On the other hand, there exist RFID protocols

[†] Some stronger version of UC framework allows limited state sharing via some specified interfaces.

Table 1 The comparison of privacy models.

	Ind	E/Unp	ZK	PV	Untra	UC
Multiple tag	Yes	No	Yes	Yes	Yes	Yes
Full corruption	No	No	Yes	No	No	Yes
Arbitrary composition	No	No	No	No	No	No

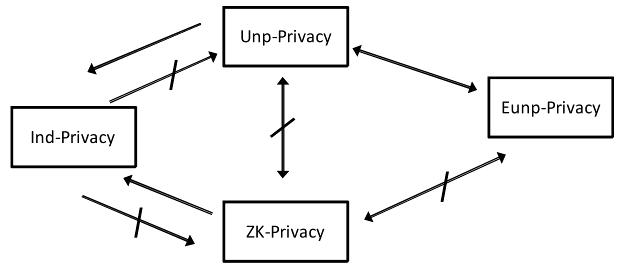


Fig. 4 Relations among four-oracle based models.

that are of ind-privacy but not of zk-privacy. Thus, zk-privacy is strictly stronger than ind-privacy [9].

- It is proved in [15] that unp-privacy implies ind-privacy. We remark that this result is imprecise. What is proved in [15] is that unp-privacy implies a special weakened version of ind-privacy, where adversary cannot learn protocol outputs (which are unrealistic in reality). As ind-privacy does not pose this restriction, ind-privacy and unp-privacy are incomparable in general. But, the reader should remind that the security guarantee of UC is not absolute, which implicitly assumes the external protocols (being composed with the protocol in question) are essentially independent of the protocol at hand. Figure 4 illuminates the relations among four-oracle base models.

6.2 Analyzing the Eight-Oracle Based Frameworks

By rendering more oracles to which adversary can have access, the eight-oracle based frameworks can be more flexible. However, the models in eight oracles-based framework are not required to deal with full corruption in the simulation. It is not clear how such a simulator acts upon tag corruption.

In comparison, the models in [19], [23] pose no restriction on tag corruption (though it is not clear how the simulator handles such adversaries), which implies that an adversary can corrupt any tag at any time (possibly in the middle of session). However, in such a case, forward/backward privacy may not be achievable if the challenge tag is corrupted in the middle of a session; this is the reason why it is required in [9] that the challenge tag T_g must remain clean at the moment of corruption.

The framework of [8] considers a much weak tag corruption, in the sense that upon corruption only secret-key is leaked to the adversary. In reality, both secret-key and some private internal state (e.g., random coins) can be revealed to adversary upon corruption. Also, no internal state update mechanism is given in the framework of [8]. This implies that symmetric encryptions or MACs alone are almost useless for achieving past or future privacy (without appropriate internal state update mechanisms). Indeed, all the authentication protocols proposed in [8] are based upon public-key cryptosystems, and the security proofs there implicitly rely upon the assumption on tag corruption (i.e., only secret-key can be revealed upon tag corruption). Also, in the framework of [8], only authentication from tag to reader is formulated.

6.3 Limitations of Some Privacy Models

- Unp-privacy and eunp-privacy have much limitations: (1) Both of them work only for special 3-round RFID protocol, with *pseudorandom* second-round message from tag. This particularly implies that public key cryptosystems can hardly be used for achieving unp-privacy and eunp-privacy. (2) Both models require that the adversary cannot learn the protocol outputs, which are unrealistic in reality. (3) These two models can only model the privacy of one tag, they can not be used to analyze the relations among a sets of tags.
- The ind-privacy model does not apply to RFID systems of a single (e.g., high valued) tag.
- PV model is not well appropriate to be used for the evaluation of practical protocols where adversary can corrupt tags.
- The untraceability model of [8] does not allow full tag corruption, and may also not be well appropriate for achieving RFID authentication protocols without using public-key cryptographic techniques.
- The UC privacy model requires the external protocols composing with the RFID authentication protocol are "independent" of the RFID protocol at hand. The formulation of UC privacy is more abstract and less easy to apply than oracle-based frameworks.

It remains an open problem to design a more reasonable Protocol. We need to consider more practical attack scenarios, which has more flexibility and stronger privacy.

Acknowledgements

This work is partly supported by A*Star SERC Grant No. 082 101 0022 in Singapore, and also supported in part by the Office of Research, Singapore Management University and Chunhua Su was supported by this grant when he was a postdoctoral fellow in Singapore Management University. Yunlei Zhao is partly supported by a grant from the Major State Basic Research Development (973) Program of China (No. 2007CB807901) and a grant from the National Natural Science Foundation of China NSFC (No. 61070248) and the QiMingXing Program of Shanghai.

References

[1] G. Avoine, "Adversary Model for Radio Frequency Identification,"

Technical Report LASEC-REPORT- 2005-001," Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC), 2005.

[2] G. Avoine, "RFID Security & Privacy Lounge," http://www.avoine.net/rfid/

[3] M. Blum, P. Feldman, and S. Micali, "Non-Interactive Zero-Knowledge and Its Applications," (Extended Abstract), Proc. 20th STOC, pp.103–112, 1988.

[4] M. Burmester, T. Le, and B. Medeiros, "Provably secure ubiquitous systems: Universally composable RFID authentication protocols," Proc. 2nd IEEE CreateNet International Conference on Security and Privacy in Communication Networks, 2006.

[5] M. Burmester, T.V. Le, B. Medeiros, and G. Tsudik, "Universally composable RFID identification and authentication protocols," ACM Trans. Information and System Security, vol.12, no.4, pp.1–33, 2009.

[6] R. Canetti, "Universally Composable Security: A new paradigm for cryptographic protocols," Proc. 42nd FOCS, pp.136–145, 2001.

[7] R. Canetti, Y. Dodis, R. Pass, and S. Walfish, "Universal composable security with global setup," Theory of Cryptography (TCC) 2007, LNCS 4392, pp.61–85, Springer-Verlag, 2007.

[8] S. Canard, I. Coisel, J. Etrog, and M. Girault, "Privacy-Preserving RFID Systems: Models and Constructions," Cryptology ePrint Archive, Report no.2010/405, 2010.

[9] R.H. Deng, Y. Li, M. Yung, and Y. Zhao, "A new framework for RFID privacy," Proc. 15th European conference on Research in computer security (ESORICS10), pp.1–18, 2010.

[10] J. Ha, S. Moon, J. Zhou, and J. Ha, "A new formal proof model for RFID location privacy," Proc. European Symposium on Research in Computer Security (ESORICS) 2008, vol.5283 of LNCS, pp.267–281, 2008.

[11] A. Juels, "RFID security and privacy: A research survey," IEEE J. Sel. Areas Commun., vol.24, no.2, pp.381–395, Feb. 2006.

[12] A. Juels and S. Weis, "Defining strong privacy for RFID," Proc. International Conference on Pervasive Computing and Communications (PerCom 2007), 2007.

[13] T. Van Le, M. Burmester, and B. Medeiros, "Universally composable and forward secure RFID authentication and authenticated key exchange," Proc. ACM Symposium on Information, Computer and Communications Security (ASIACCS 2007), pp.242–252, Singapore, 2007.

[14] J. Lai, R.H. Deng, and Y. Li, "Revisiting unpredictability-Based RFID privacy models," Proc. ACNS 2010, pp.475–492, 2010.

[15] C. Ma, Y. Li, R. Deng, and T. Li, "RFID privacy: Relation between two notions, minimal condition, and efficient construction," Proc. 16th ACM Conference on Computer and Communications Security (CCS 2009), pp.54–65, Chicago, US, Nov. 2009.

[16] C. Ma, "An Improved Privacy-Preserving RFID Protocol," (in Chinese), Chinese Journal of Computer, no.8, pp.1387–1398, 2011.

[17] C. Ng, W. Susilo, Y. Mu, and R. Safavi-Naini, "Practical RFID ownership transfer scheme," Proc. Workshop on RFID Security (RFIDSec Asia'10). Volume 4 of Cryptology and Information Security, Singapore, Feb. 2010.

[18] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Efficient hash-chain based RFID privacy protection scheme," International Conference on Ubiquitous Computing - Ubicomp, Workshop Privacy: Current Status and Future Directions, 2004.

[19] R. Paise and S. Vaudenay, "Mutual authentication in RFID: Security and privacy," Proc. 2008 ACM symposium on Information, computer and communications security (ASIACSS2008). pp.292–299, Japan, 2008.

[20] C. Su, Y. Li, T. Li, and R.H. Deng, "RFID mutual authentication protocal with universally composable security," Proc. 2011 Workshop on RFID Security (RFIDsec'11 Asia), pp.35–49, Wuxi, China, April 2011.

[21] G. Tsudik, "A Family of dunces: Trivial RFID identification and authentication protocols," Proc. Privacy Enhancing Technologies 2007 (PET 2007), volume 4776 of Lecture Notes in Computer Science, pp.45–61, Canada, 2007.

[22] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," Proc. Topics in Cryptology-CT-RSA 2006. Springer Verlag, Lecture Notes in Computer Science, 2006.

[23] S. Vaudenay, "On privacy models for RFID," Proc. Asiacrypt 2007, vol.4833 of Lecture Notes in Computer Science, pp.68–87, Kuching, Malaysia, Dec. 2007.

[24] A.C. Yao, F.F. Yao, and Y. Zhao, "A note on the feasibility of generalised universal composability," Mathematical Structures in Computer Science, vol.19, no.1, pp.193–205, 2009.

[25] A.C. Yao, F.F. Yao, and Y. Zhao, "A note on universal composable zero-knowledge in the common reference string model," Theor. Comput. Sci., vol.410, no.11, pp.1099–1108, 2009.

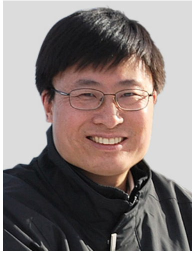
Chunhua Su received the B.S. degree for Beijing Electronic Science and Technology Institute in 2003 and recieved his M.S. and PhD of computer science from Faculty of Engineering, Kyushu University in 2006. He is currently working as Scientist in Cryptography & Security Department of the Institute for Infocomm Research, Singapore. His research areas include algorithm, cryptography, data mining and the security and privacy of RFID.

Yingjiu Li is currently an Associate Professor in the School of Information Systems at Singapore Management University. He received his Ph.D. degree in Information Technology from George Mason University in 2003. His research interests include RFID security and privacy, applied cryptography, and data applications security and privacy. He has published over 80 technical papers in international conferences and journals. He has served in the program committees for over 50 international conferences and workshops. Yingjiu Li is a senior member of the ACM and a member of the IEEE. The URL for his web page is http://www.mysmu.edu/faculty/yjli/

Yunlei Zhao is currently an Associate Professor in Software School at Fudan University, Shanghai, China. He received his Ph.D. degree in Software and Theory from Fudan University. His research interests include: Foundations of cryptography (particularly, zero-knowledge, commitments, coin-tossing, concurrent non-malleability, etc), authenticated key-exchange, public-key encryptions, cryptography applications (particularly, RFID security and privacy, smart grid security and privacy, cloud computing security and privacy, etc), and computational complexity and randomized computation.

Robert H. Deng received his Bachelor from National University of Defense Technology, China, his MSc and PhD from the Illinois Institute of Technology, USA. He has been with the Singapore Management University since 2004, and is currently Professor, Associate Dean for Faculty & Research, School of Information Systems. Prior to this, he was Principal Scientist and Manager of Infocomm Security Department, Institute for Infocomm Research, Singapore. He has 26 patents and more than 200 technical publications in international conferences and journals in the areas of computer networks, network security and information security. He received the University Outstanding Researcher Award from the National University of Singapore in 1999 and the Lee Kuan Yew Fellow for Research Excellence from the Singapore Management University in 2006. He was named Community Service Star and Showcased Senior Information Security Professional by $(ISC)^2$ under its Asia-Pacific Information Security Leadership Achievements program in 2010.

Yiming Zhao is currently an Associate Professor and associate dean in Software School at Fudan University, Shanghai, China. His research areas are cryptography, information security, and discrete mathematics.



Jianying Zhou is a senior scientist at Institute for Infocomm Research, and heads the Network Security Group. He received PhD in Information Security from University of London, MSc in Computer Science from Chinese Academy of Sciences, and BSc in Computer Science from University of Science and Technology of China. His research interests are in computer and network security, mobile and wireless communications security. He has served over 150 times in international conference committees as general chair, program chair, and PC member. He has published over 150 referred papers at international conferences and journals, of which the top 10 publications received over 1200 citations. He is a co-founder and steering committee member of International Conference on Applied Cryptography and Network Security (ACNS). He is also a cofounder and coordinating editor of Cryptology and Information Security Series (CIS).