5-2018

Exploring relationship between indistinguishability-based and unpredictability-based RFID privacy models

Anjia YANG

Yunhui ZHUANG

Jian WENG

Gerhard HANCKE

Duncan S. WONG

See next page for additional authors

Citation

YANG, Anjia; ZHUANG, Yunhui; WENG, Jian; HANCKE, Gerhard; WONG, Duncan S.; and YANG, Guomin. Exploring relationship between indistinguishability-based and unpredictability-based RFID privacy models. (2018). *Future Generation Computer Systems*. 82, 315-326.
Available at: https://ink.library.smu.edu.sg/sis_research/7297

Author
Anjia YANG, Yunhui ZHUANG, Jian WENG, Gerhard HANCKE, Duncan S. WONG, and Guomin YANG

Future Generation Computer Systems 82 (2018) 315–326

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Exploring relationship between indistinguishability-based and unpredictability-based RFID privacy models

Anjia Yang [a], Yunhui Zhuang [b], Jian Weng [a,*], Gerhard Hancke [b], Duncan S. Wong [c], Guomin Yang [d]

[a] Jinan University, Guangzhou, China
[b] City University of Hong Kong, Hong Kong
[c] CryptoBLK Limited, Hong Kong
[d] University of Wollongong, Australia

HIGHLIGHTS

- We show an imperfection of unp*-privacy model.
- We re-investigate the relationship between unp*-privacy and ind-privacy.
- We present a new unpredictability-based privacy model called unp$^\tau$-privacy.
- We explore the relations among the three privacy notions with formal proofs.
- We design a new RFID mutual authentication protocol and prove its security under the unp$^\tau$-privacy model.

ARTICLE INFO

Article history:
Received 26 August 2017
Received in revised form 8 November 2017
Accepted 24 December 2017
Available online 10 January 2018

Keywords:
RFID
Privacy models
Mutual authentication
Cryptographic protocols

ABSTRACT

A comprehensive privacy model plays a vital role in the design of privacy-preserving RFID authentication protocols. Among various existing RFID privacy models, indistinguishability-based (ind-privacy) and unpredictability-based (unp-privacy) privacy models are the two main categories. Unp*-privacy, a variant of unp-privacy has been claimed to be stronger than ind-privacy. In this paper, we focus on studying RFID privacy models and have three-fold contributions. We start with revisiting unp*-privacy model and figure out a limitation of it by giving a new practical traceability attack which can be proved secure under unp*-privacy model. To capture this kind of attack, we improve unp*-privacy model to a stronger one denoted as unp$^\tau$-privacy. Moreover, we prove that our proposed privacy model is stronger than ind-privacy model. Then, we explore the relationship between unp*-privacy and ind-privacy, and demonstrate that they are actually not comparable, which is in contrast to the previous belief. Next, we present a new RFID mutual authentication protocol and prove that it is secure under unp$^\tau$-privacy model. Finally, we construct a RFID mutual authentication model denoted as *MA* model, and show that unp$^\tau$-privacy implies *MA*, which gives a reference to design a privacy-preserving RFID mutual authentication protocol. That is, if we propose a scheme that satisfies unp$^\tau$-privacy, then it also supports mutual authentication.

1. Introduction

Radio Frequency Identification (RFID) allows automatical identification and track of tags attached to objects by utilizing electromagnetic induction. Due to its many attractive features compared with barcodes such as high throughput, not requiring line of light of the reader and supporting cryptographic algorithms to provide security, RFID has been extensively adopted in our daily life like personal identity identification cards, payments, and supply chain management.

While the scope of RFID applications is growing fast nowadays, it may also introduce kinds of serious security and privacy concerns [1–5]. Since each tag may contain some information of its owners or bearers, once the tag is corrupted, its owners' or bearers' privacy will also be disclosed consequently. Moreover, standard cryptographic techniques are too resource-consuming to be implemented on low-cost RFID tags. Therefore, it is desirable to employ less computationally expensive cryptographic functions when designing protocols for RFID systems. In this paper, we mainly look into the privacy issues of RFID tags. Generally, a

* Corresponding author.
E-mail addresses: cryptjweng@gmail.com, twjian@jnu.edu.cn (J. Weng).

https://doi.org/10.1016/j.future.2017.12.044

tag's privacy is guaranteed if the attacker cannot link or trace the tag.

A lot of efforts have been made to address the RFID tags' privacy concerns, which produces two different methods. The first one is designing privacy-preserving RFID authentication protocols, which has attracted a large number of researchers' attention [6–19]. Most of these protocols employ symmetric encryption technique for the sake of efficiency but may lose security, while a few works build secure authentication protocols based on efficient public key cryptography like Elliptic curve cryptography (ECC). Very recently, some nice works for lightweight implementation of ECC protocols on sensor nodes are done [20,21]. It will be interesting to investigate whether those protocols can be employed on low-cost RFID tags. The other one is constructing formal RFID privacy models [22–36]. Among these models, two categories stand out: one based on the indistinguishability of two tags [32], denoted as ind-privacy, and the other one based on the unpredictability of RFID protocol's outputs [26], denoted as unp-privacy. Ind-privacy is reasonably good while it is difficult to apply ind-privacy model to prove whether a given protocol is ind-private. To deal with this issue, Ha et al. [26] proposed the unp-privacy model and it has been rectified to the eunp-privacy model by Ma et al. [23]. Later, Li et al. [24] presented an improved version of the eunp-privacy model called unp*-privacy.

In this paper, we continue studying the privacy models for RFID authentication protocols, beginning with revisiting the unp*-privacy model. After that, we put forward a new RFID privacy model as well as exploring the relations among our model and previous ones. Moreover, we come up with a new RFID mutually authenticated protocol and prove its security under our proposed privacy model. Finally, as an interesting extension, we formalize a mutual authentication model and delve into its relationship with the proposed privacy model. The detailed contributions are as follows.

1.1. Our contributions

(1) We review the unp*-privacy model, and demonstrate a practical attack to a counterexample protocol which can be proved secure under the unp*-privacy model. It indicates that unp*-privacy is not enough for capturing this kind of attacks. In particular, the adversary can utilize the observation of the reactions of the reader and the tag in a concrete protocol to win the security game, while this capability is not considered in unp*-privacy.

(2) We re-investigate the relationship between unp*-privacy and ind-privacy and prove that unp*-privacy is not comparable with ind-privacy, which is in contrast to the previous claim that unp*-privacy was stronger than ind-privacy in [24]. In the original ind-privacy model [32], the adversary has the ability to recognize whether or not the tag is accepted, which can been derived from the implications of the privacy experiment in Juels et al.'s paper [32] after the experiment definition. In our paper, we also suppose the adversary can observe whether or not a tag accepts the reader since we consider a mutual authentication. When giving proof of the fact that unp*-privacy can imply ind-privacy in [24], the authors ignored the adversary's ability of observing those results. Therefore, we can find a counterexample that is unp*-private but not ind-private, which means unp*-privacy cannot imply ind-privacy, either.

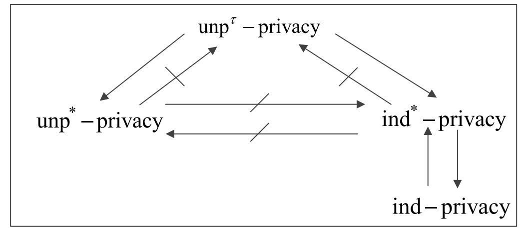


Fig. 1. Relations among privacy models.

(3) We present the unpredictability-based unp$^\tau$-privacy model, and provide a formal analysis of its capability of handling the above mentioned practical attacks.

(4) We revisit the relations among the three notions and formally prove that unp$^\tau$-privacy implies ind-privacy and unp*-privacy while not vice versa. This means that our proposed unp$^\tau$-privacy is stronger than the other two.

(5) We design a new RFID mutual authentication protocol and prove that it is secure under the unp$^\tau$-privacy model.

(6) Upon making further analysis on unp$^\tau$-privacy, we figure out an interesting and useful result, that is, any protocol satisfying unp$^\tau$-privacy must support mutual authentication. To verify that point, we first construct a mutual authentication model, denoted as *MA*, and then prove that unp$^\tau$-privacy implies *MA*. This gives us a reference to design a secure RFID mutual authentication protocol with tag privacy.

In order to make it clearer to see our contributions, we give a figure to depict the relations among three recently proposed privacy models including our new unp$^\tau$-privacy model in Fig. 1. Since it is hard to directly investigate the relationship between ind-privacy and unp$^\tau$-privacy, we build the ind*-privacy model that can be shown equivalent to ind-privacy and act as a "bridge" to discovering the relations.

1.2. Related work

In 2005, Avoine [22] proposed an adversary model for RFID systems and made the first step towards the formalization of the privacy of RFID protocols in terms of traceability. After that, based on Avoine's adversary model, in 2007, Juels and Weis [32] constructed a strong privacy model based on the indistinguishability of two tags, denoted as ind-privacy, for two-round RFID authentication protocols. In Juels and Weis's privacy model, the target tags are chosen by the adversary itself rather than the Challenger, which intuitively gives the adversary more powerful capability. However, it is difficult to apply ind-privacy model in security analysis of an RFID protocol. In ESORICS 2010 [25], Deng et al. proposed a zero-knowledge based privacy model, denoted as ZK-privacy, and they proved that their model is stronger than ind-privacy model; however, Moriyama et al. have shown that ZK-privacy is equivalent to ind-privacy in ESORICS 2012 [34]. In ASIACRYPT 2007 [30], Vaudenay proposed a framework and classified the privacy models into eight categories by considering the side-channel attacks. After this work, Paise and Vaudenay [31] extended Vaudenay's model to address mutual authentication.

Ha et al. [26] proposed a new privacy model based on the unpredictability of the tag's outputs, denoted as unp-privacy. In CCS 2009, Ma et al. [23] refined the unp-privacy to an enhanced version called eunp-privacy. In Ma et al.'s paper, the authors also proved that a pseudorandom function family is the minimal requirement on an RFID tag's computational power to preserve strong privacy. This explains why lots of existing lightweight RFID authentication protocols suffer from privacy problems [6,8–10]. Li et al. [24] improved eunp-privacy to unp*-privacy that can be applied to three round RFID protocols, and investigated the relation between unp*-privacy and ind-privacy and proved that unp*-privacy was stronger than ind-privacy.

This article is an extended version of our previous conference paper [35] in which we revisited unp*-privacy and demonstrated a practical attack to a counterexample protocol that is unp*-privacy secure. This shows that unp*-privacy cannot capture this kind of practical attack. Therefore, we presented a new unpredictability-based privacy model for RFID which can handle the new attacks and has been proved to be stronger than unp*-privacy. Except for these results, we also added sufficient extra work to this article as follows. First, we explored the relationship between unp*-privacy and ind-privacy and proved that unp*-privacy is not comparable with ind-privacy, which is in contrast to the previous claim that unp*-privacy was stronger than ind-privacy in [24]. Moreover, we designed a new RFID mutual authentication protocol and proved that it is secure under the unp$^\tau$-privacy model. Finally, we built a mutual authentication model *MA*, and formally analysed its relationship with unp$^\tau$-privacy.

1.3. Organization

We organize the remainder of this paper as follows. In Section 2, we give definitions of the RFID system model, the adversary model and some mathematical notations used in the paper. In Section 3, we revisit existing privacy models, i.e., ind-privacy and unp*-privacy, and we also explored the relation between ind-privacy and unp*-privacy. In Section 4, we present our new privacy model unp$^\tau$-privacy and establish its relation with ind-privacy and unp*-privacy. In Section 5, we propose a new RFID mutual authentication protocol with unp$^\tau$-privacy. In Section 6, we construct a mutual authentication model *MA* and explore the relation between unp$^\tau$-privacy and *MA*. Finally, in Section 7, we make a conclusion of this paper.

2. Definitions

2.1. RFID system model

An RFID system is constituted of a set of tags $\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_n$, a database and a reader R connected to the database. A tag $\mathcal{T}_i$ with an identity $I\!D_i$ shares a secret key k_i and possibly some state information st_i with R. The database stores $(k_i, st_i, I\!D_i)$ for $\mathcal{T}_i$ and R.

Definition 1. An RFID authentication system RAS consists of a tuple $(R, \mathcal{T}$, SetupReader, SetupTag, ReaderStart, TagCompute, ReaderCompute, $\pi)$, where

SetupReader: the initialization algorithm to set up the reader with system parameters π.

SetupTag: the initialization algorithm to set up the tag such as the identity, the secret key and the initial state information.

ReaderStart: the algorithm run by the reader to generate a session identifier of a fresh session, denoted as *sid*, and a fresh challenge message c_{sid} of this session.

TagCompute$(\mathcal{T}_i, sid, c_{sid})$: the algorithm run by the tag $\mathcal{T}_i$ to calculate the response r_{sid}, with inputs of *sid* and c_{sid}.

ReaderCompute(sid, c_{sid}, r_{sid}): the algorithm run by the reader to calculate the final information f_{sid}, with inputs of *sid*, c_{sid} and r_{sid}.

Protocol $\pi(R, \mathcal{T}_i)$: a polynomial time interactive protocol run by the reader R and the tag $\mathcal{T}_i$. Upon running the protocol, the algorithms of ReaderStart, TagCompute, ReaderCompute may be invoked.

A protocol $\pi(R, \mathcal{T}_i, sid)$ is executed successfully if and only if the reader and the tag accept each other.

We define the completeness and soundness of RAS in accordance with Li et al. [24]. In particular, a RAS is complete if legitimate parties including tags and reader can always pass the protocol. Suppose $(c_{sid}, r_{sid}, .)$ is the output of session *sid*, where r_{sid} is correctly generated by a legitimate tag, then completeness means that the reader R and the tag accepts each other with probability 1 for any such session. A RAS is sound if only legitimate tags/reader can pass the protocol, that is, any adversary cannot impersonate a tag or a reader successfully. Actually, in a practical RFID protocol, soundness means this protocol should provide tag/reader authentication. Li et al. only considered the soundness for tag authentication which requires an adversary cannot impersonate a tag. In our paper, we also consider the soundness for reader authentication, that is we consider the mutual authentication of RFID protocols. We will design a general model for mutual authentication in Section 6.

Remark 1. In this paper, we assume that at any time a tag can only involve one protocol session and it will remove its old secret key and state information upon updating them.

2.2. Adversary model

The adversary $\mathcal{A}$ has computation capability of probabilistic polynomial time (PPT), and can control the wireless communication channel which means it can intercept or modify messages transmitted in the air. It can also observe the protocol results, i.e. the reaction of the reader or the tag ('accept' or 'reject'). To sum up, the adversary can adaptively query the following oracles.

InitReader. This oracle allows the adversary to know the initialization result of the reader for a new protocol session, and it will return a fresh *sid* and a fresh c_{sid}.

SendTag $(\mathcal{T}_i, sid, c_{sid})$. On input of a tag $\mathcal{T}_i$, a session identifier *sid* and a challenge message c_{sid}, this oracle returns a message r_{sid}.

SendReader (sid, c_{sid}, r_{sid}). On input of a session identifier *sid*, a challenge message c_{sid}, and the message r_{sid}, this oracle returns a message f_{sid}.

Result (sid, f_{sid}). On input of a session identifier *sid* and a message f_{sid}, this oracle returns the reaction of the tag ('reject' or 'accept').

SetTag $(\mathcal{T}_i)$. On input of a tag $\mathcal{T}_i$, this oracle returns the tag's secret key and internal state information.

Hereafter, for simplicity, we use O_1, O_2, O_3, O_4, O_5 to denote **InitReader, SendTag, SendReader, Result, SetTag** oracles respectively. And the following are some parameters:

κ: security parameter;
n: the number of tags in $\mathcal{T}$;
q: the number of **InitReader** queries allowed;
s: the number of **SendTag** queries allowed;
u: the number of **SendReader** queries allowed;
v: the number of **Result** queries allowed;
w: the number of **SetTag** queries allowed;

Experiment $\mathbf{Exp}_T^{PTT}(F, m, n, p)$

1. Select $b \in_R \{0, 1\}$;
2. If $b = 1$, select a random $k \in \mathcal{K}$ and set $f = F_k$; else if $b = 0$, select a random $f' \in RF(\cdot)$ and set $f = f'$;
3. $b' \leftarrow T^{O_f}$;
4. The experiment outputs 1 if $b' = b$, 0 otherwise.

Fig. 2. Polynomial time test for F.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{ind}[\kappa, n, q, s, u, w]$

1. Initialize the RFID system with a reader R and a set of tags $\mathcal{T}$ with $|\mathcal{T}| = n$;
2. $\{\mathcal{T}_i, \mathcal{T}_j, st\} \leftarrow \mathcal{A}^{O_1,O_2,O_3,O_5}(R, \mathcal{T})$;//learning stage
3. set $\mathcal{T}' = \mathcal{T} - \{\mathcal{T}_i, \mathcal{T}_j\}$;
4. $b \in_R \{0, 1\}$;
5. If b=0, let $\mathcal{T}_c = \mathcal{T}_i$, else $\mathcal{T}_c = \mathcal{T}_j$;
6. $b' \leftarrow \mathcal{A}^{O_1,O_2,O_3,O_5}(R, \mathcal{T}', st, \mathcal{T}_c)$;//guess stage
7. the experiment outputs 1 if $b' = b$, 0 otherwise.

Fig. 3. Ind-privacy experiment.

2.3. Mathematical notations

Definition 2. A function f is negligible if for every polynomial $p(.)$ there exists an integer N such that for all integers $n > N$ it holds that $f(n) < \frac{1}{p(n)}$.

Let $F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$ be a family of functions, where $\mathcal{K}$ is the set of indexes of F, $\mathcal{D}$ is the domain of F and $\mathcal{R}$ is the range of F. Let $|\mathcal{K}| = m$, $|\mathcal{D}| = n$, $|\mathcal{R}| = p$. Let $RF : \mathcal{D} \rightarrow \mathcal{R}$ be the family of all functions with domain $\mathcal{D}$ and range $\mathcal{R}$. A polynomial time test (*PTT*) for F is an experiment, where a probabilistic polynomial time algorithm T with inputs m, n, p and access to an oracle O_f, guesses that the function f is chosen from whether $F(.)$ or $RF(.)$. $b \in_R \{0, 1\}$ means that b is chosen uniformly at random from $\{0, 1\}$. We illustrate the *PTT* experiment in Fig. 2.

Definition 3. An algorithm T passes the *PTT* experiment for the function family F if the advantage that it guesses the correct value of bit b is non-negligible, where the advantage of T is defined as $Adv_T(m, n, p) = |Pr[b' = b] - \frac{1}{2}|$, k and f are chosen uniformly at random from $\mathcal{K}$ and $RF(.)$, respectively.

Definition 4. A function family $F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$ is a pseudorandom function family (PRF) if there is no probabilistic polynomial time algorithm which can pass the *PTT* experiment for F with non-negligible advantage.

3. Revision of Ind-privacy and unp*-privacy

3.1. Ind-privacy

Juels and Weis [32] proposed the first indistinguishability-based RFID privacy model (ind-privacy). The intuitive idea of this model is that there is no adversary with the ability to distinguish two different tags with limited computational power and functionality-call bounds.

The ind-privacy experiment is briefly illustrated in Fig. 3. In the initialization phase, a reader and n tags are set up with the system parameters, where for each tag $\mathcal{T}_i$, the identifier, the secret key and optionally the internal state are created and shared with the reader R. During the learning phase, the adversary $\mathcal{A}$ is allowed to query O_1, O_2, O_3, and O_5 oracles within q, s, u and w times, respectively. Then $\mathcal{A}$ is required to choose two tags ($\mathcal{T}_i$, $\mathcal{T}_j$) that have not been compromised, i.e., have not been queried with O_5 oracle. In the challenge phase, the experiment randomly picks a bit b and determines the challenge tag according to the value of b, i.e., $\mathcal{T}_c = \mathcal{T}_i$ if $b = 0$, and $\mathcal{T}_c = \mathcal{T}_j$ otherwise. In the guessing stage, $\mathcal{A}$ is allowed to query O_1, O_2, O_3, and O_5 oracles on the set of tags again within q, s, u and w times in total, respectively, except for that it cannot query O_5 on the challenge tag $\mathcal{T}_c$. Finally, $\mathcal{A}$ outputs a bit b'.

Let $\mathbf{Exp}_{\mathcal{A}}^{ind}$ stand for the ind-privacy experiment. Let

$$\mathbf{Adv}_{\mathcal{A}}^{ind}[\kappa, n, q, s, u, w] = |Pr[\mathbf{Exp}_{\mathcal{A}}^{ind} = 1] - \frac{1}{2}|.$$

Definition 5. An RFID authentication system RAS is said to be ind-private if for any PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{ind}[\kappa, n, q, s, u, w]$ is negligible.

Discussion. Juels and Weis's experiment [32] did not explicitly state the adversary's capability of observing whether the reader and the tag accept or reject each other, while they discussed this kind of attack after their description of the experiment. Therefore, their model can actually capture this attack.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{unp*}[\kappa, n, q, s, u, w]$

1. Initialize the RFID system with a reader R and a set of tags $\mathcal{T}$ with $|\mathcal{T}| = n$;
2. $\{T_c, st\} \leftarrow \mathcal{A}^{O_1,O_2,O_3,O_5}(R, \mathcal{T})$; //learning stage
3. $b \in_R \{0, 1\}$
4. $b' \leftarrow \mathcal{A}^{O_1,O_2,O_3}(R, T_c, st)$ //guess stage
   - 4.1 When $\mathcal{A}$ queries O_1, O_2, O_3 oracles, if b=1, run the algorithm **ReaderStart, TagCompute, ReaderCompute** respectively, and return the results (c, r, f);
   - 4.2 else b=0 pick c, r, f randomly from their respective domains and return them to $\mathcal{A}$.
5. the experiment outputs 1 if $b' = b$, 0 otherwise.

Fig. 4. Unp*-privacy experiment.

3.2. Unp*-privacy

The idea of ind-privacy is quite appealing; however, it is very difficult to apply the ind-privacy model to prove whether a given RFID protocol is ind-private. To address this issue, Ha et al. [26] proposed the unp-privacy model. After several modification, unp-privacy model is improved to unp*-privacy model by Li et al. [24].

The unp*-privacy experiment is briefly illustrated in Fig. 4. The initialization phase and the learning phase are the same as that of the ind-experiment, except that after the learning phase, $\mathcal{A}$ chooses a challenge tag $\mathcal{T}_c$ which has not been queried for O_5. In the challenge phase, the experiment selects a random bit b. During this phase, $\mathcal{A}$ can query O_1, O_2, O_3 oracles on R and $\mathcal{T}_c$ without exceeding q, s and u overall calls, respectively. Upon receiving an oracle query, the challenger will respond to $\mathcal{A}$ with different strings according to the value of b as shown in Fig. 4.

Let

$$\mathbf{Adv}_{\mathcal{A}}^{unp^*}[\kappa, n, q, s, u, w] = |Pr[\mathbf{Exp}_{\mathcal{A}}^{unp^*} = 1] - \frac{1}{2}|.$$

Reader R		Tag $\mathcal{T}_i$
$\{(k_i, ctr_i, ID_i)\}$		(k_i, ctr_i, s_i)
	$c \in_R \{0,1\}^{l_c}$ →	
		$r_2 \in_R \{0,1\}^{l_r}$,
		If $s_i = 0$
		$r_1 = F_{k_i}(c\|\|pad) \oplus ctr_i$;
		Else
	← r_1, r_2	$r_1 = F_{k_i}(c\|\|r_2) \oplus ctr_i$;
If find (k_i, ctr'_i, ID_i), so that		$ctr_i = ctr_i + 1$,
$ctr'_i = F_{k_i}(c\|\|pad) \oplus r_1$, then		$s_i = 1$.
$ctr'_i = ctr'_i + 1$,		
$f = F_{k_i}(c\|\|ctr'_i\|\|r_2)$ and accept $\mathcal{T}_i$,		
Else if $\exists(k_i, ctr'_i, ID_i)$ so that	f →	
$ctr'_i = F_{k_i}(c\|\|r_2) \oplus r_1$, then		
$ctr'_i = ctr'_i + 1$,		**If** $f = F_{k_i}(c\|\|ctr_i\|\|r_2)$,
$f = F_{k_i}(c\|\|ctr'_i\|\|r_2)$ and accept $\mathcal{T}_i$,		$s_i = 0$ and accept R.
Else		**Else**
$f \in_R \{0,1\}^{l_r}$ and reject $\mathcal{T}_i$.		reject R.

Fig. 5. A counterexample.

Definition 6. An RFID authentication system RAS is said to be unp*-private if for any PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{unp^*}[\kappa, n, q, s, u, w]$ is negligible.

3.3. *Revisiting unp*-privacy*

As we have mentioned before, the adversary in the unp*-privacy experiment has no idea of the reactions of the reader and the tag, whereas it is practical and easy to obtain this capability in most of RFID applications. For instance, a student with a student card can go into the library if the card is successfully authenticated; otherwise the student cannot enter if the card authentication fails. We will demonstrate a practical attack to a counterexample that is provably secure under the unp*-privacy mode. This implies that unp*-privacy is not enough to capture this kind of attacks against RFID authentication protocols.

3.3.1. *A counterexample*

Let $F : \{0,1\}^{l_k} \times \{0,1\}^{l_d} \to \{0,1\}^{l_r}$ be a PRF family, $ctr \in \{0,1\}^{l_r}$ be a counter, and $pad \in \{0,1\}^{l_{pad}}$ be a padding so that $l_r + l_{pad} = l_d$. The values of ctr_i and s_i are initialized to be 1 and 0, respectively. The protocol works as follows depicted in Fig. 5.

(1) The reader R randomly produces a challenge c and sends it to the tag $\mathcal{T}_i$.
(2) The tag randomly generates a string $r_2 \in \{0,1\}^{l_r}$ and calculates r_1 depending on the state information s_i that is initialized to be 0 at the setup phase.
(3) The tag returns the response r_1, r_2 to the reader, while meantime updating the values of ctr_i and s_i.
(4) Upon receiving the response from the tag, the reader calculates and compares to find the matching tag according to the information stored in the database.
(5) The final message from the reader will be verified by the tag. If the message is valid, the tag will update s_i and accept the reader; otherwise, the reader will be rejected.

Theorem 1. *The counterexample is unp*-private, given that the function family* $F : \{0,1\}^{l_k} \times \{0,1\}^{l_d} \to \{0,1\}^{l_r}$ *is a PRF family.*

Proof. To prove the proposed counterexample in Fig. 5 is secure, we first assume it is not unp*-private. Namely, a PPT adversary $\mathcal{A}$ has the ability to pass the unp*-privacy game with an advantage of more than ϵ within time t. Then, we try to build an algorithm $\mathcal{B}$ which invokes $\mathcal{A}$ as a subroutine in order to win the *PTT* game defined for F. Due to the condition that F is a secure PRF family, there is supposed to be no PPT adversary that can pass the *PTT* game. Therefore, as long as we can reduce the problem of $\mathcal{A}$ in unp*-privacy experiment to the problem of $\mathcal{B}$ in *PTT* experiment, then the proof is completed. In the following, we describe how $\mathcal{B}$ simulates the unp*-privacy game with $\mathcal{A}$.

Simulate the initialization phase. To simulate the setup phase, $\mathcal{B}$ randomly chooses an index $i \in [1, n]$ that will be considered as the index of the challenge tag, and initializes the value of $ctr_i = 1$ and $s_i = 0$, respectively. Note that tag $\mathcal{T}_i$'s secret key k_i is set up implicitly, i.e., $\mathcal{B}$ has no idea of k_i. For the secret keys of the rest $n-1$ tags in $\{\mathcal{T} - \mathcal{T}_i\}$, they are randomly generated by $\mathcal{B}$ according to the secret key space.

Simulate the learning phase. In the learning phase, to simulate the answers of queries $O_1 \sim O_3$ and O_5 by $\mathcal{A}$, $\mathcal{B}$ queries the oracle O_f in *PTT* experiment game and utilizes the keys $\{k_j\}_{1\le j\le n, j\ne i}$ to respond. If $\mathcal{A}$ enquires O_5 on the tag $\mathcal{T}_i$, then $\mathcal{B}$ aborts the simulation.

Simulate the challenge phase. In the challenge phase, $\mathcal{A}$ is required to submit a challenge tag $\mathcal{T}_c$ that has not been queried with O_5 (i.e., has not been corrupted). As in the initialization phase, $\mathcal{B}$ has designated $\mathcal{T}_i$ as the challenge tag, thus if $\mathcal{T}_c \ne \mathcal{T}_i$, then $\mathcal{B}$ will abort the simulation.

Simulate the guess phase. To simulate the guess phase, $\mathcal{B}$ utilize O_f query in the *PTT* game and the secret keys $\{k_j\}_{1\le j\le n, j\ne i}$ to respond the queries of $O_1 \sim O_3$ by $\mathcal{A}$ as shown in the following steps:

① Upon $\mathcal{A}$ enquiring O_1, $\mathcal{B}$ randomly generates a session identifier *sid* and a challenge message c and returns (sid, c) to $\mathcal{A}$.
② Upon $\mathcal{A}$ enquiring O_2, $\mathcal{B}$ first randomly generates $r_2 \in_R \{0,1\}^{l_r}$. According to the value of the state s_i, $\mathcal{B}$ computes r_1 with different methods, respectively. In particular, if $s_i = 0$, then $\mathcal{B}$ queries O_f with the input of $x = c\|\|pad$, obtaining the result y and computing $r_1 = y \oplus ctr_i$; else $\mathcal{B}$ queries O_f with the input of $x = c\|\|r_2$, obtaining the result y and computing $r_1 = y \oplus ctr_i$. Finally, $\mathcal{B}$ increases ctr_i by 1, updates s_i to be 1, and sends (r_1, r_2) to $\mathcal{A}$.

③ Upon $\mathcal{A}$ enquiring O_3, $\mathcal{B}$ queries O_f with input of $c||ctr_i||r_2$, obtains the result f and returns f to $\mathcal{A}$.

Output. Finally, $\mathcal{A}$ submits a bit b' as its output, and meantime $\mathcal{B}$ also sets b' as its output.

It is not hard to see that if $O_f = F_{k_i}$, the simulation equals the unp*-privacy game in the case of $b = 1$; if $O_f = RF$, the simulation equals the unp*-privacy game in the case of $b = 0$. Therefore, if the simulation is not aborted by $\mathcal{B}$ specifically, then it is a perfect one. Note that the simulation will be aborted only if $\mathcal{A}$ queries O_5 on $\mathcal{T}_c$ or submits a tag that is not $\mathcal{T}_i$ as the challenge tag. Thus the probability that the simulation is not aborted can be calculated by $(1 - \frac{w}{q+s+u+v+w}) \cdot \frac{1}{n}$. This indicates that if $\mathcal{A}$ can win the unp*-privacy game with the advantage of more than ϵ, then $\mathcal{B}$ can win the *PTT* game with the advantage of more than $(1 - \frac{w}{q+s+u+v+w}) \cdot \frac{\epsilon}{n}$. Moreover, the running time of $\mathcal{B}$ is approximate to that of $\mathcal{A}$. This contradicts the condition that F is a PRF family. And thus the proof is completed. □

3.3.2. A traceability attack

Although we have formally proved that the counterexample is secure under the unp*-privacy model, we can demonstrate a practical traceability attack against it. Suppose the adversary $\mathcal{A}$ can observe the protocol results, i.e., whether the reader and the tag accept each other, which is a common capability as we have stated before, then $\mathcal{A}$ can obtain the state s_i of the tag $\mathcal{T}_i$ trivially, since according to the protocol, if s_i equals 0, then $r_1 = F_{k_i}(c||pad) \oplus ctr_i$ which indicates that the calculation of r_1 does not depend on r_2. By this way, $\mathcal{A}$ can intercept and modify r_2 which will be transmitted to the reader R. Next, $\mathcal{A}$ observes the result of the protocol. If $\mathcal{T}_i$ is still accepted by R, then it shows that s_i is equivalent to 0; and else it shows that s_i is equivalent to 1. This attack can be used to trace the tag since normally each tag's state is initialized to be 0, and thus an active adversary could first flag a target tag's state by interfering with the final message sent from the reader, and then trace the tag.

3.4. Relation between unp-privacy and Ind-privacy*

In last section, we show the counterexample is secure under the unp*-privacy model. In this section, we will demonstrate that it is not secure under the ind-privacy model and thus obtain the result that unp*-privacy does not imply ind-privacy, which is in contrast to the previous belief that unp*-privacy is stronger.

We have discussed that the adversary $\mathcal{A}$ in the ind-privacy game can observe the protocol results. And $\mathcal{A}$ can also flag a tag's state by an active attack. To win the ind-privacy game, $\mathcal{A}$ has to distinguish two tags $\mathcal{T}_i$ and $\mathcal{T}_j$. Before outputting the result, $\mathcal{A}$ can flag one of the tags' state (say $\mathcal{T}_i$) s_i to be 1 by modifying f. Then $\mathcal{A}$ can tell apart $\mathcal{T}_i$ from $\mathcal{T}_j$ trivially adopting the strategy used in the traceability attack. This indicates that $\mathcal{A}$ can pass the ind-privacy game and the counterexample is not ind-private. Therefore, a protocol that can be proved secure under the unp*-privacy model does not have to be proved secure under the ind-privacy model, that is, unp*-privacy does not imply ind-privacy. Moreover, Li et al. [24] has proved that ind-privacy does not imply unp*-privacy, either. According to the above results, we obtain the following claim.

Claim 1. *Unp*-privacy does not imply ind-privacy, and vice versa.*

4. The proposed privacy model: unp$^\tau$-privacy

According to the counterexample in Fig. 5, we know that unp*-privacy cannot capture the traceability attack which is easily to be launched in practice. We propose a new RFID privacy model, denoted as unp$^\tau$-privacy, which can address this issue.

The unp$^\tau$-privacy experiment is briefly illustrated in Fig. 6. The initialization phase, the learning phase and the challenge phase are the same as that of the unp*-privacy experiment, except that in the unp$^\tau$-privacy experiment, the adversary can query one more oracle (O_4). In the guess phase, $\mathcal{A}$ can query $O_1 \sim O_4$ oracles on R and $\mathcal{T}_c$ without exceeding q, s, u and v overall calls, respectively. Upon receiving an oracle query, the challenger will respond to $\mathcal{A}$ with different ways according to the value of b as shown in Fig. 6.

Let

$$\mathbf{Adv}_{\mathcal{A}}^{unp^\tau}[\kappa, n, q, s, u, v, w] = |Pr[\mathbf{Exp}_{\mathcal{A}}^{unp^\tau} = 1] - \frac{1}{2}|.$$

Definition 7. An RFID authentication system RAS is said to be unp$^\tau$-private if for any PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{unp^\tau}[\kappa, n, q, s, u, v, w]$ is negligible.

Discussion. Our proposed unp$^\tau$-privacy model can capture the practical traceability attack, that is, the given counterexample is not secure under the unp$^\tau$-privacy model, since the adversary with the ability of querying O_4 can identify the value of b trivially. In particular, $\mathcal{A}$ can manipulate the value of r_2, where in the case of $b = 1$, the challenge tag $\mathcal{T}_c$ will be accepted with overwhelming probability due to the fact that the calculation of r_1 is independent on r_2, whereas in the case of $b = 0$, $\mathcal{T}_c$ will be rejected definitely. This means the counterexample is not secure under the unp$^\tau$-privacy model.

4.1. Relation between unp$^\tau$-privacy and Ind-privacy

Before studying the relationship between unp$^\tau$-privacy and ind-privacy, we first construct a variant of ind-privacy, named ind*-privacy, which will be proved to equal ind-privacy and acts as a "bridge" that will be used for making the formal security proof.

4.1.1. Ind-privacy*

The ind*-privacy experiment is briefly depicted in Fig. 7. It is obvious that the ind*-privacy experiment is the same as the ind-privacy experiment except that in the ind*-privacy game, the adversary $\mathcal{A}$ can only enquire oracles on the challenge tag $\mathcal{T}_c$ in the guess phase. In addition, as we have discussed before, $\mathcal{A}$ can actually observe the protocol results in the ind-privacy experiment. Here, we directly grant the right to query O_4 to $\mathcal{A}$ in the ind*-privacy experiment. Essentially, the adversary in the ind-privacy has this capability, too.

Let

$$\mathbf{Adv}_{\mathcal{A}}^{ind^*}[\kappa, n, q, s, u, v, w] = |Pr[\mathbf{Exp}_{\mathcal{A}}^{ind^*} = 1] - \frac{1}{2}|.$$

Definition 8. An RFID authentication system RAS is said to be ind*-private if for any PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{ind^*}[\kappa, n, q, s, u, v, w]$ is negligible.

4.1.2. Ind-privacy $\Longleftrightarrow$ Ind-privacy*

We first prove that ind*-privacy is actually identical to ind-privacy. Intuitively, the only difference between these two experiments is that in the guess phase, the adversary in the ind-privacy game is allowed to enquire oracles on all tags including $\mathcal{T}_c$, whereas the adversary in the ind*-privacy game is only allowed to enquire oracles on $\mathcal{T}_c$. Namely, ind*-privacy is essentially a restricted version of ind-privacy and hence it is trivial to see that ind-privacy implies ind*-privacy. Nevertheless, the adversary in the ind*-privacy game can enquire O_5 on all tags except $\mathcal{C}$ before the guess phase so that it can get all the secret keys and internal state of tags in $\mathcal{T}' = \{\mathcal{T} - \mathcal{T}_c\}$ and store them in a list **TagKey-List**. This means that the adversary in the ind*-privacy game has the same power as that of the ind-privacy game.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{unp^{\tau}}[\kappa, n, q, s, u, v, w]$

1. Initialize the RFID system with a reader R and a set of tags $\mathcal{T}$ with $|\mathcal{T}| = n$;
2. $\{\mathcal{T}_c, st\} \leftarrow \mathcal{A}^{O_1,O_2,O_3,O_4,O_5}(R, \mathcal{T})$; //learning stage
3. $b \in_R \{0, 1\}$
4. $b' \leftarrow \mathcal{A}^{O_1,O_2,O_3,O_4}(R, \mathcal{T}_c, st)$ //guess stage
   - 4.1 When $\mathcal{A}$ queries O_1, O_2, O_3, O_4 oracles, if b=1, run the algorithm **ReaderStart, TagCompute, ReaderCompute, Result** respectively, and return the results; the challenger also returns the reaction of the reader R to $\mathcal{A}$, either *accept* or *reject*, when O_3 is queried.
   - 4.2 else b=0
     - 4.2.1 when $\mathcal{A}$ queries O_1, O_2 oracles, pick random elements sid, c and r from their respective domains, and return them to $\mathcal{A}$;
     - 4.2.2 when $\mathcal{A}$ queries O_3, the challenger compares whether r is equal to the output of $O_2(\mathcal{T}_c, sid, c)$. If yes, the challenger returns a random element f from its domain, and returns the reader's reaction as *accept*; else it returns a random element f from its domain and returns the reader's reaction as *reject*;
     - 4.2.3 when $\mathcal{A}$ queries O_4, the challenger checks whether f is equal to the output of $O_3(sid, c, r)$ and the reaction of the reader for this session sid is *accept*. If yes, the challenger returns the tag's reaction as *accept*; else it returns the tag's reaction as *reject*;
5. the experiment outputs 1 if $b' = b$, 0 otherwise.

Fig. 6. Unp$^{\tau}$-privacy experiment.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{ind^{*}}[\kappa, n, q, s, u, v, w]$

1. Initialize the RFID system with a reader R and a set of tags $\mathcal{T}$ with $|\mathcal{T}| = n$;
2. $\{\mathcal{T}_i, \mathcal{T}_j, st\} \leftarrow \mathcal{A}^{O_1,O_2,O_3,O_4,O_5}(R, \mathcal{T})$; //learning stage
3. set $\mathcal{T}' = \mathcal{T} - \{\mathcal{T}_i, \mathcal{T}_j\}$;
4. $b \in_R \{0, 1\}$;
5. If b=0, let $\mathcal{T}_c = \mathcal{T}_i$, else $\mathcal{T}_c = \mathcal{T}_j$;
6. $b' \leftarrow \mathcal{A}^{O_1,O_2,O_3,O_4}(R, \mathcal{T}_c, st)$; //guess stage
7. the experiment outputs 1 if $b' = b$, 0 otherwise.

Fig. 7. Ind*-privacy experiment.

Theorem 2. *Ind*-privacy is identical to ind-privacy for an RAS.*

Proof. On the one hand, according to our above analyzation, it is trivial to see that ind*-privacy $\Longleftarrow$ ind-privacy. On the other hand, we will formally prove that ind*-privacy $\Longrightarrow$ ind-privacy.

Employing the same proof technique of Theorem 1, we first assume that *RAS* is not secure under the ind-privacy model. Namely, a PPT adversary $\mathcal{A}$ has the ability to pass the ind-privacy game with an advantage of more than ϵ within time t. Then we try to build an algorithm $\mathcal{B}$ which invokes $\mathcal{A}$ as a subroutine in order to win the ind*-privacy game. Due to the condition that *RAS* is ind*-private, there is supposed to be no PPT adversary that can pass the ind*-privacy game. Therefore, as long as we can reduce the problem of $\mathcal{A}$ in the ind-privacy experiment to the problem of $\mathcal{B}$ in the ind*-privacy experiment, then the proof is completed. In the following, we illustrate how $\mathcal{B}$ simulates the ind-privacy game with $\mathcal{A}$.

Simulate the initialization phase The same as the proof in Theorem 1, except for that in this experiment two candidate challenge tags $\mathcal{T}_i$ and $\mathcal{T}_j$ are randomly designated, since the indistinguishability-based privacy model requires the adversary to distinguish two tags.

Simulate the learning phase. To simulate the answers of queries $O_1 \sim O_3$ and O_5 by $\mathcal{A}$, $\mathcal{B}$ enquires these oracles in the ind*-privacy game and returns the received responses to $\mathcal{A}$. If $\mathcal{A}$ queries O_5 on $\mathcal{T}_i$ or $\mathcal{T}_j$, then $\mathcal{B}$ aborts the simulation.

Simulate the challenge phase. In the challenge phase, $\mathcal{A}$ is required to submit two tags $\mathcal{T}_{c1}, \mathcal{T}_{c2}$ which have not been queried with O_5. If $\mathcal{T}_{c1}$ and $\mathcal{T}_{c2}$ are not the same tags as $\mathcal{T}_i$ and $\mathcal{T}_j$, then $\mathcal{B}$ aborts the simulation. $\mathcal{B}$ will also submit $\mathcal{T}_i$ and $\mathcal{T}_j$ to the challenger in the ind*-privacy game, obtain the result: the challenge tag $\mathcal{T}_c \in \{\mathcal{T}_i, \mathcal{T}_j\}$, and send $\mathcal{T}_c$ as the challenge tag to $\mathcal{A}$. Next, $\mathcal{B}$ enquires O_5 on all the tags except $\mathcal{T}_i$ and $\mathcal{T}_j$, and records these results in **TagKey-List**.

Simulate the guess phase. To simulate the guess phase, upon $\mathcal{A}$ enquiring $O_1 \sim O_3$ and O_5 oracles on $\mathcal{T}_c$, $\mathcal{B}$ queries the oracles $O_1 \sim O_3$ in the ind*-privacy game, and combines the list **TagKey-List** to respond $\mathcal{A}$. If $\mathcal{A}$ queries O_5 on $\mathcal{T}_c$, then $\mathcal{B}$ aborts the simulation.

Output. Finally, $\mathcal{A}$ submits a bit b' as its output, and meantime $\mathcal{B}$ also sets b' as its output.

According to the above description, if the simulation is not aborted by $\mathcal{B}$ specifically, then it is a perfect one. Note that the simulation will be aborted only if $\mathcal{A}$ queries O_5 on the candidate challenge tags or submits wrong candidate challenge tags. Thus the probability that the simulation is not aborted can be calculated by $(1 - \frac{2w}{q+s+u+v+w}) \cdot \frac{2}{n(n-1)}$. This indicates that if $\mathcal{A}$ can win the ind-privacy game with the advantage of more than ϵ, then $\mathcal{B}$ can win the ind*-privacy game with the advantage of more than $(1 - \frac{2w}{q+s+u+v+w}) \cdot \frac{2\epsilon}{n(n-1)}$. Moreover, the running time of $\mathcal{B}$ is approximate to that of $\mathcal{A}$. This contradicts the condition that *RAS* is ind*-private and thus the proof is completed. □

4.1.3. Unp$^{\tau}$-privacy $\Longrightarrow$ Ind*-privacy

Theorem 3. *Given an RFID authentication system RAS, if RAS is unp$^{\tau}$-private, then it is ind*-private.*

Proof. We first assume that *RAS* is not secure under the ind*-privacy model. Namely, a PPT adversary $\mathcal{A}$ has the ability to pass the ind*-privacy game with an advantage more than ϵ within time t. Then we try to build an algorithm $\mathcal{B}$ which invokes $\mathcal{A}$ as a subroutine in order to win the unp$^{\tau}$-privacy game. Due to the condition that *RAS* is unp$^{\tau}$-private, there is supposed to be no PPT adversary that can pass the unp$^{\tau}$-privacy game. Therefore, as long as we can reduce the problem of $\mathcal{A}$ in the ind*-privacy game to the problem of $\mathcal{B}$ in the unp$^{\tau}$-privacy game, then the proof is completed. In the following, we depict how $\mathcal{B}$ simulates the ind*-privacy game with $\mathcal{A}$.

Simulate the initialization phase The same as the proof in Theorem 2.

Simulate the learning phase. To simulate the answers of queries $O_1 \sim O_5$ by $\mathcal{A}$, $\mathcal{B}$ enquires these oracles in the unp$^\tau$-privacy game and returns the received responses to $\mathcal{A}$. If $\mathcal{A}$ queries O_5 on $\mathcal{T}_i$ or $\mathcal{T}_j$, then $\mathcal{B}$ aborts the simulation.

Simulate the challenge phase. In the challenge phase, $\mathcal{A}$ is required to submit two tags $\mathcal{T}_{c1}, \mathcal{T}_{c2}$ which have not been queried with O_5. If $\mathcal{T}_{c1}$ and $\mathcal{T}_{c2}$ are not the same tags as $\mathcal{T}_i$ and $\mathcal{T}_j$, then $\mathcal{B}$ aborts the simulation. $\mathcal{B}$ selects a random bit b to determine the challenge tag $\mathcal{T}_c = \mathcal{T}_i$ if $b = 0$ and $\mathcal{T}_c = \mathcal{T}_j$ otherwise. Next, $\mathcal{B}$ transmits the challenge tag $\mathcal{T}_c$ to $\mathcal{A}$ and also sets $\mathcal{T}_c$ as its own challenge tag the in unp$^\tau$-privacy game.

Simulate the guess phase. Upon $\mathcal{A}$ enquiring $O_1 \sim O_4$ oracles on $\mathcal{T}_c$, $\mathcal{B}$ queries these oracles on $\mathcal{T}_c$ in the unp$^\tau$-privacy experiment and forwards the received responses to $\mathcal{A}$

Output. Finally, $\mathcal{A}$ submits a bit b' as its output and meantime $\mathcal{B}$ outputs 1 if $b' == b$, otherwise $\mathcal{B}$ outputs 0.

According to the above description, if the simulation is not aborted by $\mathcal{B}$ specifically, then it is a perfect one. The probability that the simulation is not aborted can be calculated by $(1 - \frac{2w}{q+s+u+v+w}) \cdot \frac{2}{n(n-1)}$. We will explain why it is a perfect simulation if there is no abortion. Suppose the challenger in the unp$^\tau$-privacy experiment selects a random bit b_0 in the challenge phase. If b_0 is 0, $\mathcal{T}_c$ is essentially a virtual tag in the perspective of $\mathcal{A}$ because in this case $\mathcal{A}$ will always receive random responses upon enquiring $O_1 \sim O_3$ during the guess phase. Therefore, the probability that $b' == b$ is $\frac{1}{2}$. On the other hand, if b_0 equals 1, the probability that $b' == b$ becomes $\frac{1}{2} + \epsilon$. This indicates that the advantage that $\mathcal{B}$ wins the unp$^\tau$-privacy experiment is $|\frac{1}{2} - (\frac{1}{2} + \epsilon)| = \epsilon$. This is exactly the same advantage as that of $\mathcal{A}$. Above all, if $\mathcal{A}$ can win the ind*-privacy game with the advantage of more than ϵ, then $\mathcal{B}$ can win the unp$^\tau$-privacy game with the advantage of more than $(1 - \frac{2w}{q+s+u+v+w}) \cdot \frac{2\epsilon}{n(n-1)}$. Moreover, the running time of $\mathcal{B}$ is approximate to that of $\mathcal{A}$. This contradicts the condition that *RAS* is unp$^\tau$-private and thus the proof is completed. □

4.1.4. Unp$^\tau$-privacy $\Longrightarrow$Ind-privacy

According to Theorem 2 and Theorem 3, we can directly derive Theorem 4:

Theorem 4. *Given an RFID authentication system RAS, if RAS is unp$^\tau$-private, then it is ind-private.*

4.1.5. Unp$^\tau$ -privacy$\not\Longleftarrow$ Ind-privacy

Intuitively, ind-privacy requires it is hard for the adversary to distinguish two tags according to their transcripts in spite of the distribution of the transcripts, while unp$^\tau$-privacy stipulates that the transcripts should be randomly distributed.

Theorem 5. *An RFID authentication system RAS with ind-privacy does not imply that it is unp$^\tau$-private.*

Proof. (sketch). We employ the similar technique with Li et al. [24] and build an RFID authentication system in which the protocol transcripts have format of $(c, r||r, f)$. On one hand, in the ind-privacy game, two tags with two different transcripts $r_1||r_1$ and $r_2||r_2$ are indistinguishable since r_1 and r_2 are randomly chosen. Thus, the designed *RAS* is ind-private. On the other hand, in the unp$^\tau$-privacy game, the adversary is required to distinguish whether $r_1||r_2$ is from a real protocol transcript or randomly selected by the challenger. If they are randomly selected by the challenger, then $r_1 \neq r_2$ with overwhelming probability; otherwise, r_1 is equivalent to r_2 since this is how the real protocol works. This means that *RAS* is not secure under the unp$^\tau$-privacy model. Above all, the proof is completed. □

4.2. Relation between unp$^\tau$-privacy and unp-privacy*

In Section 3.3.1 we have shown that the counterexample protocol in Fig. 5 is provably secure under the unp*-privacy model but not in the unp$^\tau$-privacy model. This means unp*-privacy does not imply unp$^\tau$-privacy. In the following, we will prove that unp$^\tau$-privacy implies unp*-privacy, which indicates that unp$^\tau$-privacy is stronger than unp*-privacy.

Theorem 6. *Given an RFID authentication system RAS, if RAS is unp$^\tau$-private, then it is unp*-private.*

Proof. We first assume that *RAS* is not secure under the unp*-privacy model. Namely, a PPT adversary $\mathcal{A}$ has the ability to pass the unp*-privacy game with an advantage of more than ϵ within time t. Then we try to build an algorithm $\mathcal{B}$ which invokes $\mathcal{A}$ as a subroutine in order to win the unp$^\tau$-private game. Due to the condition that *RAS* is unp$^\tau$-private, there is supposed to be no PPT adversary that an pass the unp$^\tau$-privacy game. Therefore, as long as we can reduce the problem of $\mathcal{A}$ in the unp*-privacy experiment to the problem of $\mathcal{B}$ in the unp$^\tau$-privacy experiment, then the proof is completed. In the following, we illustrate how $\mathcal{B}$ simulates the unp*-privacy game with $\mathcal{A}$.

Simulate the initialization phase. The same as that in Theorem 1.

Simulate the learning phase. To simulate the answers of queries $O_1 \sim O_3$ and O_5 by $\mathcal{A}$, $\mathcal{B}$ enquires these oracles in the unp$^\tau$-privacy game and returns the received responses to $\mathcal{A}$. If $\mathcal{A}$ enquires O_5 on the tag $\mathcal{T}_i$, then $\mathcal{B}$ aborts the simulation.

Simulate the challenge phase. In this phase, $\mathcal{A}$ is required to submit a challenge tag $\mathcal{T}_c$ that has not been queried with O_5. $\mathcal{B}$ sets $\mathcal{T}_c$ as the challenge tag in the unp$^\tau$-privacy game, too. If $\mathcal{T}_c \neq \mathcal{T}_i$, then $\mathcal{B}$ aborts the simulation.

Simulate the guess phase. Upon $\mathcal{A}$ enquiring $O_1 \sim O_3$ oracles on $\mathcal{T}_c$, $\mathcal{B}$ queries these oracles on $\mathcal{T}_c$ in the unp$^\tau$-privacy game and returns the received responses to $\mathcal{A}$.

Output. Finally, $\mathcal{A}$ submits a bit b' as its output, and meantime $\mathcal{B}$ also sets b' as its output.

If the simulation is not aborted by $\mathcal{B}$ specifically, then it is a perfect one. The probability that the simulation is not aborted can be calculated by $(1 - \frac{w}{q+s+u+v+w}) \cdot \frac{1}{n}$. This indicates that if $\mathcal{A}$ can win the unp*-privacy game with the advantage of more than ϵ, then $\mathcal{B}$ can win the unp$^\tau$-privacy game with the advantage of more than $(1 - \frac{w}{q+s+u+v+w}) \cdot \frac{\epsilon}{n}$. Moreover, the running time of $\mathcal{B}$ is approximate to that of $\mathcal{A}$. This contradicts the condition that *RAS* is unp$^\tau$-private. And thus the proof is completed. □

By far, we have studied the relationship among all ind-privacy, unp*-privacy and unp$^\tau$-privacy. According to these work, we can get the claim:

Claim 2. *Unp$^\tau$-privacy is stronger than both unp*-privacy and ind-privacy.*

5. Our new RFID authentication protocol

Now we design a new RFID mutual authentication protocol with unp$^\tau$-privacy as shown in Fig. 8. F is the same PRF family as in the counterexample and $pad \in \{0, 1\}^{l_{pad}}$ is a padding so that $l_c + l_r + l_{pad} = l_d$. The protocol works as follows depicted in Fig. 8.

(1) The reader R randomly produces a challenge c and sends it to the tag $\mathcal{T}_i$.

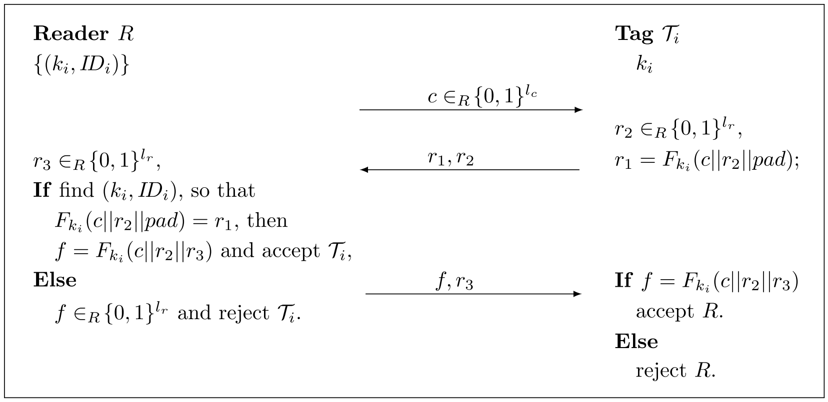


Fig. 8. Our new RFID mutual authentication protocol with unp$^\tau$-privacy.

(2) The tag randomly generates a string $r_2 \in \{0, 1\}^{l_r}$, calculates r_1, and returns r_1, r_2 to the reader.
(3) Upon receiving the response from the tag, the reader calculates and compares to find the matching tag according to the information stored in the database.
(4) The final message from the reader will be verified by the tag. If the message is valid, the tag will accept the reader; otherwise, the reader will be rejected.

Theorem 7. *The mutual authentication protocol in Fig. 8 is unp$^\tau$-private, given that the function family $F : \{0, 1\}^{l_k} \times \{0, 1\}^{l_d} \to \{0, 1\}^{l_r}$ is a PRF family.*

Proof. The proof is similar with that in Theorem 1. We first assume that the authentication protocol in Fig. 8 is not unp$^\tau$-private. Namely, a PPT adversary $\mathcal{A}$ has the ability to pass the unp$^\tau$-privacy game with an advantage of more than ϵ within time t. Then we try to build an algorithm $\mathcal{B}$ which invokes $\mathcal{A}$ in order to win the *PTT* game. Due to the condition that F is a secure PRF family, there is supposed to be no PPT adversary that can pass the *PTT* game. Therefore, as long as we can reduce the problem of $\mathcal{A}$ in the unp$^\tau$-privacy experiment to the problem of $\mathcal{B}$ in *PTT* experiment, then the proof is completed. In the following, we depict how $\mathcal{B}$ simulates the unp$^\tau$-privacy game with $\mathcal{A}$.

Simulate the initialization phase. The same as the proof in Theorem 1, except for that in this simulation there is no ctr_i and s_i.

Simulate the learning phase. To simulate answers of queries $O_1 \sim O_5$ by $\mathcal{A}$, $\mathcal{B}$ enquires O_f in *PTT* experiment game and utilizes the keys $\{k_j\}_{1 \le j \le n, j \ne i}$ to respond. If $\mathcal{A}$ enquires O_5 on $\mathcal{T}_i$, then $\mathcal{B}$ aborts the simulation.

Simulate the challenge phase. $\mathcal{A}$ is required to submit a challenge tag $\mathcal{T}_c$ that has not been queried with O_5. If $\mathcal{T}_c \ne \mathcal{T}_i$, then $\mathcal{B}$ aborts the simulation.

Simulate the guess phase. To simulate the guess phase, $\mathcal{B}$ utilizes O_f query in the *PTT* game and the secret keys $\{k_j\}_{1 \le j \le n, j \ne i}$ to respond the queries of $O_1 \sim O_4$ on $\mathcal{T}_c$ by $\mathcal{A}$ as shown in the following steps.

① Upon $\mathcal{A}$ enquiring O_1, $\mathcal{B}$ randomly generates a session identifier *sid* and a challenge c and returns (sid, c).
② Upon $\mathcal{A}$ enquiring O_2, $\mathcal{B}$ randomly generates $r_2 \in_R \{0, 1\}^{l_r}$, and queries O_f with the input of $x = c||r_2||pad$, obtaining the result y which is assigning to r_1. Finally, $\mathcal{B}$ sends (r_1, r_2) to $\mathcal{A}$.
③ Upon $\mathcal{A}$ enquiring O_3, $\mathcal{B}$ selects a random string $r_3 \in_R \{0, 1\}^{l_r}$, queries O_f with input of $c||r_2||r_3$, and obtains the result f. Then it sends f and r_3, as well as the reaction of the reader R to $\mathcal{A}$. Note that in order to obtain the reaction of R, $\mathcal{B}$ also queries O_f with input of $x = c||r_2||pad$, and compares the answer returned by O_f with the value provided by the adversary $\mathcal{A}$ in the query. If they are equal, then $\mathcal{B}$ returns the reaction of R as 'accept', else, it returns 'reject'.
④ Upon $\mathcal{A}$ enquiring O_4, $\mathcal{B}$ queries O_f with input of $c||r_2||r_3$ and compares the answer returned by O_f with the value provided by the adversary $\mathcal{A}$ in the query, and whether the reaction of R is 'accept' for this session. If both of the checking results are yes, then it returns 'accept' as the reaction of $\mathcal{T}_i$, else it returns 'reject'.

Output. Finally, $\mathcal{A}$ submits a bit b' as its output, and meantime $\mathcal{B}$ also sets b' as its output.

We can see that when $O_f = RF$, then the simulation is identical to the experiment with $b = 0$; otherwise, if $O_f = F_{k_i}$, then the simulation is identical to the experiment with $b = 1$ except for a little difference that in the experiment the challenger will not check the reaction of R when answering the query of O_4 from $\mathcal{A}$. Nevertheless, we can show that this difference is negligible. The only difference that the adversary $\mathcal{A}$ may observe is: upon receiving O_4 from $\mathcal{A}$, in the simulated game, if O_3 outputs 'reject', then O_4 will always output 'reject'; while in the real experiment, if O_3 outputs 'reject', then O_4 may output 'accept' if and only if $\mathcal{A}$ is able to forge a valid input for O_4. It is obvious that the difference between the real game and the simulated game is negligible since the probability for the adversary to forge a valid reply f is negligible.

Therefore, if the simulation is not aborted by $\mathcal{B}$ specifically, then it is a perfect one. The probability that the simulation is not aborted can be calculated by $(1 - \frac{w}{q+s+u+v+w}) \cdot \frac{1}{n}$. This indicates that if $\mathcal{A}$ can win the unp$^\tau$-privacy game with the advantage of more than ϵ, then $\mathcal{B}$ can win the *PTT* game with the advantage of more than $(1 - \frac{w}{q+s+u+v+w}) \cdot \frac{\epsilon}{n}$. Moreover, the running time of $\mathcal{B}$ is approximate to that of $\mathcal{A}$. This contradicts the condition that F is a PRF family and thus the proof is completed. □

6. Relation between unp$^\tau$-privacy and *MA* model

By far, when we talk about an RFID authentication system *RAS*, we assume that *RAS* is sound, which means given a three round protocol $\mathcal{P}$, we presume $\mathcal{P}$ provides mutual authentication. Now, we want to eliminate these preconditions. Intuitively, we expect that given any protocol $\mathcal{P}$, if it satisfies our proposed unp$^\tau$-privacy model, then it must provide mutual authentication. This offers us a reference to design a mutual authentication protocol with tag privacy. In order to achieve this, we first construct a general model for mutual authentication and then we will explore the relationship between the unp$^\tau$-privacy model and the mutual authentication model.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{MA}[\kappa, n, q, s, u, v, w]$

1. Initialize the RFID system with a reader R and a set of tags $\mathcal{T}$ with $|\mathcal{T}| = n$;
2. $\{\mathcal{T}_c, st\} \leftarrow \mathcal{A}^{O_1,O_2,O_3,O_4,O_5}(R, \mathcal{T})$;
3. $\{(c_{sid}, r_{sid}, f_{sid})\} \leftarrow \mathcal{A}^{O_1,O_2,O_3,O_4}(R, st, \mathcal{T}_c)$;
4. The experiment outputs 1 if the reader R accepts $\mathcal{T}_c$ in a session sid whose transcript is $(c_{sid}, r_{sid}, f_{sid})$ and r_{sid} is not in the returned values of O_2 in session sid, or if $\mathcal{T}_c$ accepts R in a session sid whose transcript is $(c_{sid}, r_{sid}, f_{sid})$ and f_{sid} is not in the returned values of O_3 in session sid; otherwise, the experiment outputs 0.

Fig. 9. Mutual authentication model.

6.1. Mutual authentication model: MA

The *MA* experiment is briefly depicted in Fig. 9. At the beginning, a reader and n tags are set up with the system parameters. During the learning phase, the adversary $\mathcal{A}$ is allowed to query $O_1 \sim O_5$ oracles within q, s, u, v and w times in total, respectively. Then $\mathcal{A}$ is required to choose a challenge tag $\mathcal{T}_c$ that has not been queried with O_5. Then in the challenge phase, $\mathcal{A}$ is required to generate a new transcript tuple $(c_{sid}, r_{sid}, f_{sid})$. Meantime, $\mathcal{A}$ can issue $O_1 \sim O_4$ oracle queries within q, s, u, v times in total, respectively. The experiment outputs 1 if the reader R accepts $\mathcal{T}_c$ in a session *sid* whose transcript is $(c_{sid}, r_{sid}, f_{sid})$ and r_{sid} is not in the returned values of O_2 in session *sid*, or if $\mathcal{T}_c$ accepts R in a session *sid* whose transcript is $(c_{sid}, r_{sid}, f_{sid})$ and f_{sid} is not in the returned values of O_3 in session *sid*; otherwise, the experiment outputs 0. We use $\mathbf{Exp}_{\mathcal{A}}^{MA}$ to represent the *MA* experiment. Let

$$\mathbf{Adv}_{\mathcal{A}}^{MA}[\kappa, n, q, s, u, v, w] = Pr[\mathbf{Exp}_{\mathcal{A}}^{MA} = 1]$$

Definition 9. Given any mutual authentication protocol $\mathcal{P}$, $\mathcal{P}$ is said to be *MA*-secure if for any PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{MA}[\kappa, n, q, s, u, v, w]$ for $\mathcal{P}$ is negligible.

6.2. Unp$^\tau$-privacy $\Longrightarrow$ MA

In the *MA* experiment, if any adversary $\mathcal{A}$ can forge a valid response r or f without querying for them from the oracles O_2 or O_3 respectively, then $\mathcal{A}$ can win the game. While if $\mathcal{A}$ can win the *MA* game, then it can also win the unp$^\tau$-privacy game. This is because $\mathcal{A}$ can forge a valid r or f, and observe the reactions of the reader and the tag. Take the reader's reaction for example, $\mathcal{A}$ first forges a valid r, and then queries O_3 to get the reaction of the reader. If the reader outputs 'accept' then it indicates the random bit b selected by the challenger in the unp$^\tau$-privacy game is 1; otherwise, it means $b = 0$, since when $b = 0$, the challenger compares whether r is equal to the output of O_2 according to the unp$^\tau$-privacy experiment. Since $\mathcal{A}$ has never queried O_2 for r, the forged r is different from any outputs of O_2 with an overwhelming probability, which means the reader will reject the tag with an overwhelming probability. Therefore, the adversary $\mathcal{A}$ can distinguish $b = 0$ or $b = 1$, which means $\mathcal{A}$ can also win the unp$^\tau$-privacy game. In the following, we will give a theorem and prove it formally.

Theorem 8. *Given any mutual authentication protocol $\mathcal{P}$, if $\mathcal{P}$ satisfies the unp$^\tau$-privacy model, then it satisfies the MA-model, too.*

Proof. We first assume that $\mathcal{P}$ is not *MA*-secure. Namely, a PPT adversary $\mathcal{A}$ has the ability to pass the *MA* game with an advantage of more than ϵ within time t. Then we try to build an algorithm $\mathcal{B}$ which invokes $\mathcal{A}$ in order to win the unp$^\tau$-privacy game. Due to the condition that $\mathcal{P}$ is unp$^\tau$-private, there is supposed to be no PPT adversary that can pass the unp$^\tau$-privacy game. Therefore, as long as we can reduce the problem of $\mathcal{A}$ in the *MA* game to the problem of $\mathcal{B}$ in the unp$^\tau$-privacy game, then the proof is completed. In the following, we depict how $\mathcal{B}$ simulates the *MA* game with $\mathcal{A}$.

Simulate the initialization phase. To simulate the setup phase, $\mathcal{B}$ randomly chooses an index $i \in [1, n]$ that will be considered as the index of the challenge tag. Note that tag $\mathcal{T}_i$'s secret key k_i is set up implicitly, i.e., $\mathcal{B}$ has no idea of k_i. For the secret keys of the rest $n-1$ tags in $\{\mathcal{T} - \mathcal{T}_i\}$, they are randomly generated by $\mathcal{B}$ according to the secret key space.

Simulate the learning phase. Upon $\mathcal{A}$ enquiring $O_1 \sim O_5$ oracles, $\mathcal{B}$ queries these oracles in the unp$^\tau$-privacy game and forwards the received responses to $\mathcal{A}$. If $\mathcal{A}$ queries O_5 on $\mathcal{T}_i$, then $\mathcal{B}$ aborts the simulation. After learning, $\mathcal{A}$ outputs the challenge tag $\mathcal{T}_c$ which has not been queried with O_5, $\mathcal{B}$ also sets $\mathcal{T}_c$ as its own challenge tag in the unp$^\tau$-privacy experiment. If $\mathcal{T}_c$ is not $\mathcal{T}_i$, $\mathcal{B}$ aborts the simulation.

Simulate the challenge phase. Upon $\mathcal{A}$ enquiring $O_1 \sim O_4$ on $\mathcal{T}_c$, $\mathcal{B}$ queries these oracles on $\mathcal{T}_c$ in the unp$^\tau$-privacy game and forwards the received responses to $\mathcal{A}$.

Output. Finally, $\mathcal{A}$ outputs a tuple $(c_{sid}, r_{sid}, f_{sid})$. $\mathcal{B}$ checks whether R accepts $\mathcal{T}_c$ and r_{sid} is not in the returned values of O_2 in session *sid*, or $\mathcal{T}_c$ accepts R and f_{sid} is not in the returned values of O_3. If yes, $\mathcal{B}$ outputs 1; otherwise it outputs 0.

We can see that if the simulation is not aborted by $\mathcal{B}$ specifically, then it is a perfect one. Now we will explain why $\mathcal{B}$ can win the unp$^\tau$-privacy game if $\mathcal{A}$ can win the *MA* game. Let b_0 be the random bit selected in the unp$^\tau$-privacy experiment. Let $\mathbf{Adv}_{\mathcal{B}}$ be the advantage of $\mathcal{B}$ in the unp$^\tau$-privacy experiment in the case that the simulation is not aborted. According to the definition of unp$^\tau$-privacy, we have

$$\begin{aligned}
\mathbf{Adv}_{\mathcal{B}} &= P_r[\mathcal{B}\ wins\ the\ unp^\tau{-}privacy\ game] - \frac{1}{2} \\
&= P_r[\mathcal{B}\ outputs\ 1|b_0 = 1]P_r[b_0 = 1] \\
&\quad + P_r[\mathcal{B}\ outputs\ 0|b_0 = 0]P_r[b_0 = 0] - \frac{1}{2} \\
&= \frac{1}{2}P_r[\mathcal{B}\ outputs\ 1|b_0 = 1] \\
&\quad + \frac{1}{2}(1 - P_r[\mathcal{B}\ outputs\ 1|b_0 = 0]) - \frac{1}{2} \\
&= \frac{1}{2}(P_r[\mathcal{B}\ outputs\ 1|b_0 = 1] - P_r[\mathcal{B}\ outputs\ 1|b_0 = 0]) \\
&= \frac{1}{2}(\epsilon - P_r[\mathcal{B}\ outputs\ 1|b_0 = 0])
\end{aligned}$$

When $b_0 = 0$, the outputs of O_2 are random strings, and O_3 will output 'accept' only when r_{sid} is equal to the output of O_2 in session *sid* according to the unp$^\tau$-privacy experiment for $b_0 = 0$. Then the probability that "O_2 has never been queried in session *sid* (that is, r_{sid} is not in the returned values of O_2 in session *sid*), but r_{sid} provided by $\mathcal{A}$ is equal to the output of O_2" is $(\frac{1}{2})^{l_r}$ (assume the length of r_{sid} is l_r). By a union bound, the probability that such an event happens in any session is at most $\frac{s}{2^{l_r}}$, where s is the number of O_2 queries allowed in the *MA* experiment.

Similarly, the probability that "O_3 has never been queried in session *sid* but f_{sid} provided by $\mathcal{A}$ is equal to the output of O_3" is $(\frac{1}{2})^{l_f}$ (assume the length of f_{sid} is l_f) and by a union bound, the probability that such an event happens in any session is at most $\frac{u}{2^{l_f}}$, where u is the number of O_3 queries allowed in the *MA* experiment.

Now, we can obtain $P_r[\mathcal{B}\ outputs\ 1|b_0 = 0] = \frac{s}{2^{l_r}} + \frac{u}{2^{l_f}}$. Since s, u, l_r, l_f are polynomial in the secret key k (in general, l_r and l_f are several times longer than k in bit string form), $P_r[\mathcal{B}\ outputs\ 1|b_0 = 0]$ is negligible. Therefore, if ϵ is non-negligible, then the advantage of $\mathcal{B}$, i.e. $\mathbf{Adv}_{\mathcal{B}} = \frac{1}{2}(\epsilon - (\frac{s}{2^{l_r}} + \frac{u}{2^{l_f}}))$, is also non-negligible. Above all, if we consider the case that the simulation could be aborted, then the final advantage of $\mathcal{B}$ become $(1 - \frac{w}{q+s+u+v+w}) \cdot \frac{1}{n} \cdot \mathbf{Adv}_{\mathcal{B}}$, which is also non-negligible. Moreover, the running time of $\mathcal{B}$ is approximate to that of $\mathcal{A}$. Thus the proof is completed. □

7. Conclusion

In this paper, we reviewed unp*-privacy and showed that it cannot capture a new practical attack. At the meantime, we re-investigated the relationship between unp*-privacy and ind-privacy and proved that unp*-privacy is not comparable with ind-privacy. Then we presented a new unpredictability-based privacy model: unp$^\tau$-privacy which can handle the above mentioned practical attacks and we revisited the relations among ind-privacy, unp*-privacy and unp$^\tau$-privacy. Then we proposed a mutual authentication protocol and proved its security under the unp$^\tau$-privacy model. Finally, we constructed a new mutual authentication model *MA* and proved that unp$^\tau$-privacy implies *MA*. This gives us a reference to design a secure RFID mutual authentication protocol with tag privacy.

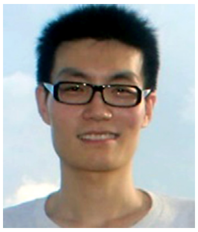
Acknowledgements

This work was supported by National Key R&D Plan of China (Grant No. 2017YFB0802203), National Natural Science Foundation of China (Grant Nos. U173620045, 61702222, 61732021, 61472165 and 61373158), China Postdoctoral Science Foundation funded project (Grant No. 2017M612842), Guangdong Provincial Engineering Technology Research Center on Network Security Detection and Defence (Grant No. 2014B090904067), Guangdong Provincial Special Funds for Applied Technology Research and development and Transformation of Important Scientific and Technological Achieve (Grant No. 2016B010124009), the Zhuhai Top Discipline-Information Security, Guangzhou Key Laboratory of Data Security and Privacy Preserving, and Guangdong Key Laboratory of Data Security and Privacy Preserving.

References

[1] A. Juels, RFID security and privacy: A research survey, IEEE J. Sel. Areas Commun. J-SAC'06 24 (2) (2006) 381–394.
[2] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, RFID systems: A survey on security threats and proposed solutions, Proceedings of the 11th IFIP International Conference on Personal Wireless Communications, PWC'06, in: LNCS, Vol. 4217, Springer, 2006, pp. 159–170.
[3] L. Francis, G. Hancke, K. Mayes, K. Markantonakis, On the security issues of nfc enabled mobile phones, Int. J. Internet Technol. Secur. Trans. 2 (3/4) (2010) 336–356.
[4] C.A. Opperman, G.P. Hancke, Using nfc-enabled phones for remote data acquisition and digital control, in: AFRICON, 2011, September 2011, pp. 1–6.
[5] A. Yang, G.P. Hancke, RFID and Contactless Technology, Springer International Publishing, Cham, 2017, pp. 351–385.
[6] M. Ohkubo, K. Suzuki, S. Kinoshita, Cryptographic approach to privacy-friendly tags, in: RFID Privacy Workshop, 2003.
[7] A. Yang, E. Pagnin, A. Mitrokotsa, G. Hancke, D.S. Wong, Two-hop distance-bounding protocols: keep your friends close, IEEE Trans. Mob. Comput. PP (99) (2017).
[8] A. Juels, R.L. Rivest, M. Szydlo, The blocker tag: Selective blocking of RFID tags for consumer privacy, in: ACM Conference on Computer and Communications Security, CCS'03, ACM, 2003, pp. 103–111.
[9] S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels, Security and privacy aspects of low-cost radio frequency identification systems, 1st International Conference on Security in Pervasive Computing, SPC'03, in: LNCS, Vol. 2802, Springer, 2003, pp. 201–212.
[10] S.M. Lee, Y.J. Hwang, D.H. Lee, J.I. Lim, Efficient authentication for low-cost RFID systems, Proceedings of the 2005 International Conference on Computational Science and Its Applications, Part I, ICCSA'05, in: LNCS, Vol. 3480, Springer, 2005, pp. 619–627.
[11] C.H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, O. Pereira, The swiss-knife RFID distance bounding protocol, Proceedings of the 8th International Conference on Information Security and Cryptology, ICISC '08, in: LNCS, Vol. 5461, Springer, 2008, pp. 98–115.
[12] T.V. Le, M. Burmester, B. de Medeiros, Universally composable and forward-secure RFID authentication and authenticated key exchange, in: Proceedings of the 2th ACM Symposium on Information, Computer and Communications Security-ASIACCS'07, ACM, 2007, pp. 242–252.
[13] M. Burmester, T.V. Le, B. de Medeiros, G. Tsudik, Universally composable RFID identification and authentication protocols, ACM Trans. Inf. Syst. Secur. TISSEC'09 12 (4) (2009).
[14] A. Yang, Y. Zhuang, D.S. Wong, An efficient single-slow-phase mutually authenticated RFID distance bounding protocol with tag privacy, Proceedings of the 14th International Conference on Information and Communications Security, ICICS'12, in: LNCS, Vol. 7618, Springer, 2012, pp. 285–292.
[15] Y. Zhuang, A. Yang, D.S. Wong, G. Yang, Q. Xie, A highly efficient RFID distance bounding protocol without real-time PRF evaluation, Proceedings of the 7th International Conference on Network and System Security, NSS'13, in: LNCS, Vol. 7873, Springer, 2013, pp. 451–464.
[16] E. Pagnin, A. Yang, G. Hancke, A. Mitrokotsa, Short: Hb+db, mitigating man-in-the-middle attacks against hb+ with distance bounding, in: Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec'15. ACM.
[17] E. Pagnin, A. Yang, Q. Hu, G. Hancke, A. Mitrokotsa, Hb+db: distance bounding meets human based authentication, Future Gener. Comput. Syst. (2016).
[18] H. Kılınç, S. Vaudenay, Efficient Public-Key Distance Bounding Protocol, Springer Berlin Heidelberg, Berlin, Heidelberg, 2016, pp. 873–901.
[19] Y. Zhuang, A. Yang, G.P. Hancke, D.S. Wong, G. Yang, Energy-efficient distance-bounding with residual charge computation, IEEE Trans. Emerg. Top. Comput. (2017).
[20] Z. Liu, J. Großschädl, Z. Hu, K. Järvinen, H. Wang, I. Verbauwhede, Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things, IEEE Trans. Comput. 66 (5) (2017) 773–785.
[21] Z. Liu, X. Huang, Z. Hu, M.K. Khan, H. Seo, L. Zhou, On emerging family of elliptic curves to secure internet of things: Ecc comes of age, IEEE Trans. Dependable Secure Comput. 14 (3) (2017) 237–248.
[22] G. Avoine, Adversarial model for radion frequency identification. Cryptology ePrint Archive, Report 2005/049, 2005. http://eprint.iacr.org/.
[23] C. Ma, Y. Li, R.H. Deng, T. Li, Relation between two notions, minimal condition, and efficient construction, in: ACM Conference on Computer and Communications Security, CCS'09, ACM, 2009, pp. 54–65.
[24] Y. Li, R.H. Deng, J. Lai, C. Ma, On two RFID privacy notions and their relations, ACM Trans. Inf. Syst. Secur. TISSEC'11 14 (4) (2011).
[25] R.H. Deng, Y. Li, M. Yung, Y. Zhao, A new framework for RFID privacy, Proceedings of the 15th European Symposium on Research in Computer Security, ESORICS'10, in: LNCS, Vol. 6345, Springer, 2010, pp. 1–18.
[26] J. Ha, S. Moon, J. Zhou, J. Ha, A new formal proof model for RFID location privacy, Proceedings of the 13th European Symposium on Research in Computer Security, ESORICS'08, in: LNCS, Vol. 5283, Springer, 2008, pp. 267–281.
[27] J. Lai, R.H. Deng, Y. Li, Revisiting unpredictability-based RFID privacy models, Proceedings of the 8th International Conference on Applied Cryptography and Network Security, ACNS'10, in: LNCS, Vol. 6123, Springer, 2010, pp. 475–492.
[28] K. Ouafi, R.C.-W. Phan, Traceable privacy of recent provably-secure RFID protocols, Proceedings of the 6th International Conference on Applied Cryptography and Network Security, ACNS'08, in: LNCS, Vol. 5037, Springer, 2008, pp. 479–489.
[29] C. Ng, W. Susilo, Y. Mu, R. Safavi-Naini, RFID privacy models revisited, Proceedings of the 13th European Symposium on Research in Computer Security, ESORICS'08, in: LNCS, Vol. 5283, Springer, 2008, pp. 251–266.
[30] S. Vaudenay, On privacy models for RFID, Advances in Cryptology - ASIACRYPT'07, in: LNCS, Vol. 4833, Springer, 2007, pp. 68–87.
[31] R.-I. Paise, S. Vaudenay, Mutual authentication in RFID: Security and privacy, in: Proceedings of the 3th ACM Symposium on Information, Computer and Communications Security - ASIACCS'08, ACM, 2008, pp. 292–299.
[32] A. Juels, S.A. Weis, Defining strong privacy for RFID, in: Proceedings of the 5th IEEE International Conference on Pervasive Computing and Communications - Workshops, PerCom Workshops 2007, IEEE Computer Society, 2007, pp. 342–347. Also appears in ACM Transaction on Information and System Security, TISSEC 2009, vol. 13(1):7, 2009.
[33] J. Hermans, A. Pashalidis, F. Vercauteren, B. Preneel, A new RFID privacy model, Proceedings of the 16th European Symposium on Research in Computer Security, ESORICS'11, in: LNCS, Vol. 6879, Springer, 2011, pp. 568–587.
[34] D. Moriyama, S. Matsuo, M. Ohkubo, Relations among notions of privacy for RFID authentication protocols, Proceedings of the 17th European Symposium on Research in Computer Security, ESORICS'12, in: LNCS, Vol. 7459, Springer, 2012, pp. 661–678.
[35] A. Yang, Y. Zhuang, D.S. Wong, G. Yang, A new unpredictability-based RFID privacy model, Proceedings of the 7th International Conference on Network and System Security, NSS'13, in: LNCS, Vol. 7873, Springer, 2013, pp. 479–492.

[36] A. Yang, K. Liang, Y. Zhuang, D.S. Wong, X. Jia, A new unpredictability-based radio frequency identification forward privacy model and a provably secure construction. security and communication networks, SCN'15, 8 (16) (2015) 2836–2849.



Anjia Yang received the B.S. degree from Jilin University, China, in 2011, and the Ph.D. degree from the City University of Hong Kong, Hong Kong, in 2015. Currently he is a postdoctoral fellow in the Jinan University, Guangzhou, China. His research interests include RFID security and privacy, applied cryptography, and cloud computing.

Yunhui Zhuang received both Ph.D. and M.Sc. degrees in computer science from City University of Hong Kong (CityU) in 2016 and 2010, respectively. He is now a postdoctoral fellow in the Department of Information Systems of College of Business in CityU. His research interests lie at the intersection of economics and information security. In particular, he is interested in applied cryptography, security and privacy of mobile payment, blockchain, business analytics, e-Learning, and applied econometrics. He has served as the Co-Chair or the Program Committee member for some prestigious international conferences in applied cryptography, information security, and e-Learning.

Jian Weng received the B.S. and M.S. degrees in computer science and engineering from the South China University of Technology, in 2000 and 2004, respectively, and the Ph.D. degree in computer science and engineering from Shanghai Jiao Tong University, in 2008. From 2008 to 2010, he held a post-doctoral position with the School of Information Systems, Singapore Management University. He is currently a Professor and the Dean with the School of Information Technology, Jinan University. He has authored over 50 papers in cryptography conferences and journals, such as CRYPTO, Eurocrypt, TCC, and Asiacrypt. He served as the PC co-chairs or PC member for over 10 international conferences, such as the ISPEC 2011, the RFIDsec 2013 Asia, and the ISC 2011, IWSEC 2012.

Gerhard P. Hancke received the B.Eng. and M.Eng. degrees from the University of Pretoria, Pretoria, South Africa, in 2002 and 2003, respectively, and the Ph.D. degree from the Computer Laboratory, University of Cambridge, Cambridge, U.K., in 2008. He is an Assistant Professor with the Department of Computer Science, City University of Hong Kong. His main research interests revolve around advanced sensing and security, especially for RFID/contactless, mobile and other pervasive technologies.

Duncan S. Wong received the B.Eng. degree from the University of Hong Kong in 1994, the M.Phil. degree from the Chinese University of Hong Kong in 1998, and the Ph.D. degree from Northeastern University in Boston, USA in 2002. He was with the City University of Hong Kong for 12 years, and was the Vice President of Financial Technologies in ASTRI since 2014. He is the Co-Founder and CEO of CryptoBLK Limited. He has authored over 200 research papers in international journals and conferences, and served as a member, including the Chair of the Program Committee for over 90 prestigious international conferences in cryptography and information security. His research interests include applied cryptography, information security, and blockchain.

Guomin Yang received his Ph.D. degree from the Computer Science Department at City University of Hong Kong in 2009. Formerly, he worked as a research scientist in the Temasek Laboratories at National University of Singapore. He is currently a Senior Lecturer at the School of Computing and Information Technology, University of Wollongong, Australia. He has been awarded a prestigious Australian Research Council DECRA fellowship award. His research interests are cryptography and network security.