6-2013

A new unpredictability-based RFID privacy model

Anjia YANG

Yunhui ZHUANG

Duncan S. WONG

Guomin YANG
Singapore Management University, gmyang@smu.edu.sg

A New Unpredictability-Based RFID Privacy Model

Anjia Yang[1], Yunhui Zhuang[1], Duncan S. Wong[1], and Guomin Yang[2]

[1] City University of Hong Kong, Hong Kong
{ayang3-c,yhzhuang2-c}@my.cityu.edu.hk,
duncan@cityu.edu.hk
[2] University of Wollongong, Australia
gyang@uow.edu.au

Abstract. Ind-privacy and unp-privacy, later refined to unp*-privacy, are two different classes of privacy models for RFID authentication protocols. These models have captured the major anonymity and untraceability related attacks regarding RFID authentication protocols with privacy, and existing work indicates that unp*-privacy seems to be a stronger notion when compared with ind-privacy. In this paper, we continue studying the RFID privacy models, and there are two folds regarding our results. First of all, we describe a new traceability attack and show that schemes proven secure in unp*-privacy may not be secure against this new and practical type of traceability attacks. We then propose a new unpredictability-based privacy model to capture this new type of attacks. Secondly, we show that this new model, where we called it the unp$^\tau$-privacy, is stronger than both unp*-privacy and ind-privacy.

Keywords: RFID, privacy models, mutual authentication protocol.

1 Introduction

RFID (Radio Frequency Identification) technology has been widely applied in many applications such as payments, supply chain management, tracking goods, and electronic passports. Generally speaking, an RFID system comprises a reader, a set of tags and a database. RFID tags authenticate themselves to an RFID reader through an authentication protocol and the reader may also need to authenticate itself to the tags if mutual authentication is required. However, there may exist privacy issues if the authentication protocol is not designed with a proper privacy protection mechanism. We mainly focus on the RFID tags' privacy since once the tags' privacy is disclosed, their owners or bearers will also suffer from privacy problems. To keep the tags' privacy means that the adversary cannot identify, trace or link tag appearances.

There are mainly two ways to deal with the RFID tags' privacy issues. The first one is to construct RFID protocols which can preserve the tags' privacy and the second one is to formalize privacy models for RFID systems. As to the former way, lots of protocols have been proposed in recent years [2,5,8–10,18,19],

J. Lopez, X. Huang, and R. Sandhu (Eds.): NSS 2013, LNCS 7873, pp. 479–492, 2013.

while many of them are claimed to have privacy flaws according to [11]. For the latter way, many privacy models have been proposed [1, 3, 4, 6, 7, 11–17]. Among them, there are two major notions: one based on the indistinguishability of two tags [7], denoted as ind-privacy, and the other one based on the unpredictability of RFID protocol's outputs [4], denoted as unp-privacy. Ind-privacy is reasonably good; however, it is difficult to apply ind-privacy model to prove whether a given protocol is ind-private. To address this problem, Ha *et al.* [4] proposed the unp-privacy model and it has been rectified to eunp-privacy by Ma *et al.* [12]. In [11], Li *et al.* pointed out the limitation of eunp-privacy and proposed a new privacy model called unp*-privacy.

In this paper, we focus on the privacy models for RFID authentication protocols and point out some limitations of unp*-privacy. Then we propose a new privacy model and explore the relations between our proposed model and the previous models.

1.1 Our Contributions

(1) We revisit the unpredictability-based RFID privacy model denoted as unp*-privacy [11], and we point out the limitations of the unp*-privacy model by giving a protocol as a counterexample that is secure under unp*-privacy model while vulnerable to a practical attack given in Section 4.1. In this new attack, the adversary can observe the protocol results, i.e., the reaction of the reader and the tag, in an RFID authentication protocol. Through this attack the adversary can trace RFID tags.
(2) We propose a new unpredictability-based privacy model, denoted as unp$^\tau$-privacy (τ is short for traceability), and prove that our new model can handle the new attack and thus is more appropriate.
(3) We investigate the relationship among ind-privacy, unp*-privacy and unp$^\tau$-privacy and obtain the result that unp$^\tau$-privacy is stronger than both ind-privacy and unp*-privacy.

Fig. 1 illustrates the relations among the previous privacy models and the unp$^\tau$-privacy model that we elaborate in this paper. Note that the ind*-privacy model is a "bridge" which is proven to be equivalent to ind-privacy model and is used to explore the relation between ind-privacy and unp$^\tau$-privacy.

2 RFID Security Architecture

2.1 RFID System Model

We consider an RFID system which consists of n tags belonging to a set $\mathcal{T}$, and a reader R that is connected with a database. The reader and the tags are probabilistic polynomial time (PPT) interactive Turing machines. Each tag $\mathcal{T}_i$ stores an internal secret key k_i which is shared with the reader R, and some optional state information st_i. The reader R has a database to store k_i, st_i, ID_i which is the identifier of $\mathcal{T}_i$, and some other information for each tag $\mathcal{T}_i$.

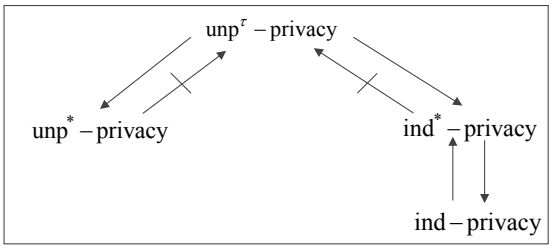

Fig. 1. Relations among privacy models

To start an authentication session, the reader R first sends a fresh challenge message c to a tag $\mathcal{T}_i$. Then $\mathcal{T}_i$ responds with a message r computed based on its secret key k_i, c, st_i, and random coins cn_i. We write r as $r = F_T(k_i, cn_i, st_i, c)$, where F_T denotes the function used by the tag. Upon receiving r, the reader verifies the response and will output either 'accept' or 'reject' as its reaction. If there is a third round (i.e. for mutual authentication), R will respond to $\mathcal{T}_i$ with a final message f which is computed according to the tag's response r, k_i, c, the reader's own state information st_R and random coins cn_R. We write it as $f = F_R(k_i, cn_R, st_R, c, r)$, where F_R is the function used by the reader. Similarly, when the tag receives f, it will verify whether f is valid or not and will output either 'accept' or 'reject' as its reaction, and terminate the session. Typically, in this paper, we focus on three-round RFID authentication protocols.

Definition 1. *An RFID system RS is composed of a tuple (R,$\mathcal{T}$,SetupReader, SetupTag, ReaderStart, TagCompute, ReaderCompute,π), where*

SetupReader. It is a function used to initialize the system with some system parameters and make the reader R ready to work.

SetupTag. It is a function used to generate the secret keys and set the initial state information for the tags. It also associates each tag with an unique *ID*.

ReaderStart. It is a function for R to generate a session identifier of a fresh session, denoted as *sid*, and a fresh challenge message c_{sid} of this session.

TagCompute$(\mathcal{T}_i, sid, c_{sid})$. It is a function for $\mathcal{T}_i$ to compute its response message r_{sid}, with *sid* and c_{sid} as inputs.

ReaderCompute(sid, c_{sid}, r_{sid}). It is a function for R to compute the final message f_{sid}, with sid, c_{sid} and r_{sid} as inputs.

Protocol $\pi(R, \mathcal{T}_i)$. It is a polynomial time interactive protocol between R and $\mathcal{T}_i$. When executing the protocol, it will invoke the functions of ReaderStart,TagCompute, ReaderCompute.

We say a protocol $\pi(R, \mathcal{T}_i, sid)$ is successful if R and $\mathcal{T}_i$ accept each other.

For the completeness and soundness of RFID systems, we adopt the definitions by Li *et al.* [11]. Informally, completeness means that valid tags should always be accepted by a legitimate reader and soundness means that only valid tags/reader should be accepted. In the following sections, when we mention an RFID system, we mean it is complete and sound.

Remark 1. We assume any tag $\mathcal{T}_i$ can be involved in only one protocol session at a time and it will overwrite the old k_i and st_i when updating them.

2.2 Adversary Model

We consider a PPT adversary $\mathcal{A}$ who has the ability to eavesdrop, intercept, modify and remove messages transmitted between the reader and the tag. $\mathcal{A}$ also can generate its own messages. We assume that $\mathcal{A}$ can obtain the reaction of the reader and tag, i.e. $\mathcal{A}$ will know if the reader or any tag makes a decision ('accept' or 'reject'). In a word, we allow the adversary to adaptively query the following oracles.

InitReader. It invokes the reader R to start a new protocol session. R generates and returns a fresh session identifier sid and challenge message c_{sid}.

SendTag$(\mathcal{T}_i, sid, c_{sid})$. It invokes the tag $\mathcal{T}_i$ to start a new protocol session with the inputs sid and c_{sid}, and return a message r_{sid}.

SendReader(sid, c_{sid}, r_{sid}). It invokes R to compute and return the final message f_{sid} with the inputs sid, c_{sid} and r_{sid}.

Result(sid, f_{sid}). $\mathcal{A}$ queries the reaction of the tag in the session sid with the message f_{sid}.

SetTag$(\mathcal{T}_i)$. $\mathcal{A}$ obtains the secret key and internal state information of $\mathcal{T}_i$.

For convenience, we use O_1, O_2, O_3, O_4, O_5 to denote **InitReader, SendTag, SendReader, Result, SetTag** oracles respectively. We define some parameters for the adversary as follows. κ is the security parameter and n is the number of tags in $\mathcal{T}$, and q, s, u, v, and w are the number of O_1, O_2, O_3, O_4 and O_5 queries respectively allowed for the adversary in one game.

2.3 Mathematical Notations

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

Let $F : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$ be a family of functions, where $\mathcal{K}$ is the set of indices 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 $RF : \mathcal{D} \to \mathcal{R}$ 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 whether the function f is chosen from whether $F(\cdot)$ or $RF(\cdot)$. $b \in_R \{0, 1\}$ 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 $Adv_T(m, n, p) = \left|\Pr[b' = b] - \frac{1}{2}\right|$, k and f chosen uniformly at random from $\mathcal{K}$ and $RF(\cdot)$, respectively.*

Definition 4. *A function family $F : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$ 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.*

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 $f = F_k$; otherwise, select a random $f' \in RF(.)$ 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

3 Ind-Privacy and Unp*-Privacy

3.1 Ind-Privacy

Fig. 3 describes the ind-privacy experiment, denoted by $\mathbf{Exp}_{\mathcal{A}}^{ind}[\kappa, n, q, s, u, w]$. At first, the experiment sets up the RFID system by initializing a reader R and a set of tags $\mathcal{T} = (\mathcal{T}_1, \mathcal{T}_2, \cdots, \mathcal{T}_n)$ according to the system security parameter κ. It associates each tag $\mathcal{T}_i$ with a secret key k_i and an internal state information st_i, and also stores these keys and state information in the database connected with R. Then in the learning stage, the adversary can issue O_1, O_2, O_3, O_5 oracle queries at most q, s, u and w overall calls, respectively. The adversary also selects two uncorrupted tags $(\mathcal{T}_i, \mathcal{T}_j)$, which it has not sent SetTag (O_5) queries to, and outputs the state information st which will be used in the guess stage. Next, the experiment randomly selects a bit b and sets the challenge tag $\mathcal{T}_c = \mathcal{T}_i$ if $b = 0$, and $\mathcal{T}_c = \mathcal{T}_j$ otherwise. Finally, in the guessing stage, the adversary $\mathcal{A}$ is required to guess the random bit b by outputting a bit b'. During the guessing stage, $\mathcal{A}$ can issue O_1, O_2, O_3, O_5 oracle queries on $\mathcal{T}_c \cup (\mathcal{T} - \{\mathcal{T}_i, \mathcal{T}_j\})$ at most q, s, u and w overall calls respectively, with the restriction that it cannot query SetTag($\mathcal{T}_c$). We use $\mathbf{Exp}_{\mathcal{A}}^{ind}$ to represent the ind-privacy experiment.

Let

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

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

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

Discussion. In Juels and Weis' ind-privacy experiment [7], we cannot conclude directly whether the adversary has the ability to observe the reaction of the reader, that is, either accepts or rejects a tag. Nevertheless, in their following Section 3.1 where the OSK/AO protocols are analyzed, they described a kind of attack in which the adversary can observe the reaction of the reader. We believe they presume the adversary has this ability. In addition, Juels and Weis considered two-round RFID authentication protocols. However, Li *et al.* [11] proved Juels and Weis' ind-privacy model also works for three-round protocols. In this paper, we consider ind-privacy for three-round RFID authentication protocols, which support mutual authentication.

3.2 Unp*-Privacy

Fig. 4 illustrates unp*-privacy experiment, denoted by $\mathbf{Exp}_{\mathcal{A}}^{unp^*}[\kappa, n, q, s, u, v, w]$. In the learning stage, the adversary $\mathcal{A}$ selects an uncorrupted challenge tag $\mathcal{T}_c$ which it has not sent SetTag queries to. Next, the challenger picks a random bit b. When receiving an oracle query, the challenger will decide what to respond to $\mathcal{A}$ according to the value of b. $\mathcal{A}$ is required to guess the value of b. We use $\mathbf{Exp}_{\mathcal{A}}^{unp^*}$ to represent unp*-privacy experiment. Let

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

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

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

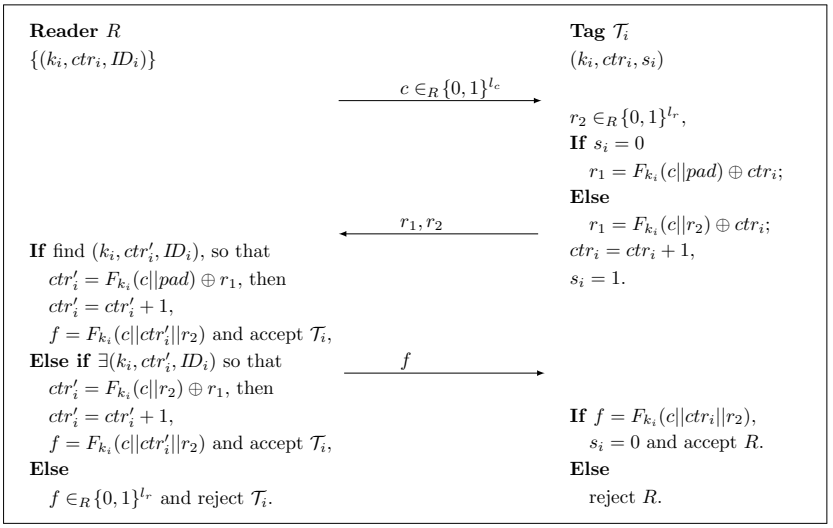

Fig. 5. A Counterexample

4 Limitation of Unp*-Privacy

Note that in unp*-privacy experiment, the adversary $\mathcal{A}$ can not observe the reaction of R and $\mathcal{T}_i$. However, in practice, for most RFID tag applications, this ability is easily obtainable. For example, a staff card either opens a door when authenticated successfully or fails to open a door when failed to be authenticated to the reader equipped in the door; a payment card is either accepted or rejected by a sale device. In the following section, we will show a counterexample which is secure under unp*-privacy model, while vulnerable to a kind of attack that is easy to launch in our daily life. This example implies a limitation of unp*-privacy when it is applied to RFID authentication protocols.

4.1 A Counterexample

Let $F : \{0,1\}^{l_k} \times \{0,1\}^{l_d} \to \{0,1\}^{l_r}$ be a PRF family. Let $ctr \in \{0,1\}^{l_r}$ be a counter, and $pad \in \{0,1\}^{l_{pad}}$ be a padding such that $l_r + l_{pad} = l_d$. When the system calls SetupTag($\mathcal{T}_i$), it will initialize $ctr_i = 1$ and set $s_i = 0$. After the initialization phase, the system will go on as the following steps.

(1) The reader R generates a random challenge message c to the tag $\mathcal{T}_i$.
(2) $\mathcal{T}_i$ randomly selects r_2 and computes r_1 according to the value of s_i: $r_1 = F_{k_i}(c||pad) \oplus ctr_i$ if $s_i = 0$, else $r_1 = F_{k_i}(c||r_2) \oplus ctr_i$.
(3) $\mathcal{T}_i$ sends the response r_1, r_2 to R, updates $ctr_i = ctr_i + 1$, and sets $s_i = 1$.
(4) R searches from the database for the tuple (k_i, ctr'_i, ID_i) such that $ctr'_i = F_{k_i}(c||pad) \oplus r_1$ or $ctr'_i = F_{k_i}(c||r_2) \oplus r_1$. If such a tuple exists, then update $ctr'_i = ctr'_i + 1$, compute $f = F_{k_i}(c||ctr'_i||r_2)$, send it to $\mathcal{T}_i$ and accept $\mathcal{T}_i$; else response with $f \in_R \{0,1\}^{l_r}$ and reject $\mathcal{T}_i$.

(5) Upon receiving f, $\mathcal{T}_i$ checks if $f = F_{k_i}(c||ctr_i||r_2)$. If yes, $\mathcal{T}_i$ accepts R and sets $s_i = 0$, else $\mathcal{T}_i$ rejects R.

A Traceability Attack. Now we launch a traceability attack against this protocol. We consider an adversary $\mathcal{A}$ who has the ability to know whether R accepts $\mathcal{T}_i$ or not and vice versa. $\mathcal{A}$ can find out the value of a tag's state s_i easily, for if $s_i = 0$, then $r_1 = F_{k_i}(c||pad) \oplus ctr_i$ which means the value of r_1 is not related with r_2. Therefore, $\mathcal{A}$ can change the value of r_2 that is sent by $\mathcal{T}_i$ and observe whether R will accept $\mathcal{T}_i$. If R accepts $\mathcal{T}_i$, then it means $s_i = 0$; otherwise, it means $s_i = 1$. Note that under normal circumstances the value of s_i is 0. Thus, an active attacker can flag a tag by setting its state $s_i = 1$ and then trace the tag. However, we can prove this counterexample is secure under unp*-privacy model.

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. Assume the counterexample in Fig. 5 is not unp*-private. That is, there exists an adversary $\mathcal{A}$ who can win the unp*-privacy game with advantage at least ϵ, and the running time at most t. We construct an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ as a subroutine and can pass the PTT experiment for PRF family F. Algorithm $\mathcal{B}$ can simulate unp*-privacy experiment for $\mathcal{A}$ as follows.

Simulate the learning stage. At the beginning, $\mathcal{B}$ selects a random index $i \in [1, n]$ and sets $ctr_i = 1, s_i = 0$. The key of $\mathcal{T}_i$ is set as k_i implicitly, which is unknown to $\mathcal{B}$. For any tag $\mathcal{T}_j \in \{\mathcal{T} - \mathcal{T}_i\}$, $\mathcal{B}$ sets $ctr_j = 1, s_j = 0$ and sets the secret key of $\mathcal{T}_j$ as k_j which is selected randomly from the secret key space. When $\mathcal{A}$ queries O_1, O_2, O_3, O_5, $\mathcal{B}$ invokes O_f and the keys k_1, k_2, $\cdots$, k_{i-1}, k_{i+1}, $\cdots$, k_n to respond. Note that when $\mathcal{A}$ queries O_5 on tag $\mathcal{T}_i$, $\mathcal{B}$ aborts and randomly outputs a bit.

Simulate the challenge stage. $\mathcal{A}$ submits an uncorrupted challenge tag $\mathcal{T}_c$. Note that if $\mathcal{T}_c \neq \mathcal{T}_i$, $\mathcal{B}$ aborts and randomly outputs a bit.

Simulate the guess stage. Every time when $\mathcal{A}$ queries about O_1, O_2, O_3, $\mathcal{B}$ will answer $\mathcal{A}$ using O_f and the keys k_1, k_2, $\cdots$, k_{i-1}, k_{i+1}, $\cdots$, k_n as follows.

① When $\mathcal{A}$ queries O_1, $\mathcal{B}$ selects a random session sid and a random challenge message c and returns sid, c to $\mathcal{A}$.
② When $\mathcal{A}$ queries O_2, $\mathcal{B}$ selects a random string $r_2 \in_R \{0,1\}^{l_r}$. If $s_i = 0$, $\mathcal{B}$ queries O_f on $x = c||pad$, gets the response y and sets $r_1 = y \oplus ctr_i$; else queries O_f on $x = c||r_2$, gets the response y and sets $r_1 = y \oplus ctr_i$. Then update $ctr_i = ctr_i + 1$ and $s_i = 1$, and return r_1, r_2 to $\mathcal{A}$.
③ When $\mathcal{A}$ queries O_3, $\mathcal{B}$ queries O_f on $c||ctr_i||r_2$, gets the response f and sends f to $\mathcal{A}$.

Output. When $\mathcal{A}$ outputs a bit b', $\mathcal{B}$ also takes b' as its output.

We can see that when $O_f = F_{k_i}$, then the simulation is identical to the experiment with $b = 1$; otherwise, if $O_f = RF$, then the simulation is identical to the experiment with $b = 0$. Thus, if $\mathcal{B}$ does not abort during the simulation,

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

$\mathcal{B}$'s simulation is perfect. The probability that $\mathcal{B}$ does not abort during the simulation is $\frac{1}{n}$. Thus, if the adversary $\mathcal{A}$ can pass unp*-privacy experiment with the advantage at least ϵ, then the advantage that $\mathcal{B}$ passes the PTT experiment is at least $\frac{\epsilon}{n}$. In addition, the running time of $\mathcal{B}$ is approximate to that of $\mathcal{A}$. This completes the proof. □

5 Our Proposed Privacy Model: Unp$^{\tau}$-Privacy

Fig. 6 illustrates the unp$^{\tau}$-privacy experiment, denoted by $\mathbf{Exp}_{\mathcal{A}}^{unp^{\tau}}[\kappa, n, q, s, u, v, w]$. In this experiment the adversary $\mathcal{A}$ can query O_4. Note that when $b = 1$ and O_3 is queried, the challenger will return f as well as the reaction of the reader, and when $b = 0$ and O_3 is queried, the challenger needs to send the reader's reaction to $\mathcal{A}$, since it's in accordance with the situation when $b = 1$ so that $\mathcal{A}$ can not distinguish $b=0$ or $b=1$ only according to the reaction of the reader R.

We use $\mathbf{Exp}_{\mathcal{A}}^{unp^{\tau}}$ to represent the unp$^{\tau}$-privacy experiment. Let

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

Definition 7. *An RFID system RS 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.*

Note that the counterexample in Fig. 5 does not satisfy our privacy model. In unp$^{\tau}$-privacy experiment, when the adversary modifies the second message r_2

randomly, if $b = 1$, the reader R will accept the tag $\mathcal{T}_c$ with overwhelming probability, since the value of r_1 is not related with r_2 under normal circumstances; otherwise, if $b = 0$, the reader R will reject the tag $\mathcal{T}_c$. That is, the adversary can distinguish the two cases with overwhelming probability. Hence the counterexample is not unp$^{\tau}$-private.

5.1 Relation between Unp$^{\tau}$-Privacy and Ind-Privacy

In order to explore the relation between unp$^{\tau}$-privacy and ind-privacy, we first introduce a restricted ind-privacy model, denoted as ind*-privacy, as a "bridge", which is equivalent to ind-privacy.

Ind*-Privacy Fig. 7 illustrates the ind*-privacy experiment, denoted by $\mathbf{Exp}_{\mathcal{A}}^{ind^*}[\kappa, n, q, s, u, v, w]$, which is identical to the ind-privacy experiment given in Fig. 3 except that the adversary $\mathcal{A}$ in ind*-privacy experiment is not allowed to query oracles on other tags except for $\mathcal{T}_c$ in the guess stage. Since we have showed that the adversary in the ind-privacy model has the ability to know the result of the reader's reaction, we explicitly allow $\mathcal{A}$ to query O_4 in ind*-privacy experiment. We use $\mathbf{Exp}_{\mathcal{A}}^{ind^*}$ to simply represent ind*-privacy experiment. Let

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

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

Definition 8. *An RFID system RS 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.*

Ind*-Privacy $\Longleftrightarrow$ Ind-Privacy On the one hand, the adversary in ind-privacy experiment can query oracles on any tag from $\mathcal{T}' \cap \mathcal{T}_c$ in the guess stage, while the adversary in ind*-privacy experiment can only query oracles on $\mathcal{T}_c$ in the guess stage. There is no any other difference between ind-privacy and ind*-privacy. That is, there are more restrictions on the adversary in ind*-privacy experiment, and thus ind-privacy implies ind*-privacy. On the other hand, the adversary in ind*-privacy experiment can launch O_5 queries on all tags in $\mathcal{T}'$

before the guess stage in order to obtain the secret keys and internal state information of all the tags in $\mathcal{T}'$ and then store them in a list **TagKey-List**. Then in the guess stage when the adversary queries those oracles on any tag in $\mathcal{T}'$, the adversary itself can obtain the corresponding answers using the list **TagKey-List**. That is, the adversary's power in ind*-privacy experiment is not weakened compared with that in ind-privacy experiment.

Theorem 2. *Ind*-privacy is equivalent to ind-privacy for an RFID system RS.*

Proof. First, it is obvious that ind-privacy $\Longrightarrow$ ind*-privacy as what we have analyzed above. In the following, we will prove ind-privacy $\Longleftarrow$ ind*-privacy.

Assume that RS is not ind-private. That is, there exists an adversary $\mathcal{A}$ which can win the ind-privacy game with advantage at least ϵ, and the running time at most t. We construct an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ as a subroutine and can pass ind*-privacy experiment. Algorithm $\mathcal{B}$ can simulate ind-privacy experiment for $\mathcal{A}$ as follows.

Simulate the learning stage. When $\mathcal{A}$ queries O_1, O_2, O_3, O_5 oracles, algorithm $\mathcal{B}$ queries these oracles in ind*-privacy experiment and sends the results it receives to $\mathcal{A}$. Actually, we have shown that in ind-privacy experiment, the adversary $\mathcal{A}$ also has the ability to observe the protocol results, which means it can query O_4 (can be seen in ind*-privacy experiment).

Simulate the challenge stage. When $\mathcal{A}$ outputs two uncorrupted tags $\mathcal{T}_i, \mathcal{T}_j$, algorithm $\mathcal{B}$ will also submit $\mathcal{T}_i$ and $\mathcal{T}_j$ to the challenger in ind*-privacy experiment, and get the response with a challenge tag $\mathcal{T}_c \in \{\mathcal{T}_i, \mathcal{T}_j\}$. Then $\mathcal{B}$ sends O_5 oracles on all the tags in $\mathcal{T}' = \mathcal{T} - \{\mathcal{T}_i, \mathcal{T}_j\}$ and stores the results in **TagKey-List**. Then $\mathcal{B}$ forwards $\mathcal{T}_c$ to $\mathcal{A}$.

Simulate the guess stage. When $\mathcal{A}$ queries O_1, O_2, O_3, O_5 oracles on $\mathcal{T}' \cup \mathcal{T}_c$, $\mathcal{B}$ also uses the oracles O_1, O_2, O_3, together with the list **TagKey-List** to answer $\mathcal{A}$.

Output. When $\mathcal{A}$ outputs a bit b', $\mathcal{B}$ also takes b' as its own output.

We can see the simulation of $\mathcal{B}$ is perfect. Thus if $\mathcal{A}$ can pass ind-privacy experiment with the advantage at least ϵ, then the advantage that $\mathcal{B}$ passes ind*-privacy experiment is at least ϵ, too. In addition, the running time of $\mathcal{B}$ is approximate to that of $\mathcal{A}$. This completes the proof. □

Unp$^\tau$-Privacy $\Longrightarrow$Ind*-Privacy

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

Proof. Assume that RS is not ind*-private. That is, there exists an adversary $\mathcal{A}$ which can win ind*-privacy game with advantage at least ϵ, and the running time at most t. We construct an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ as a subroutine and can pass unp$^\tau$-privacy experiment. Algorithm $\mathcal{B}$ can simulate ind*-privacy experiment for $\mathcal{A}$ as follows.

Simulate the learning stage. When $\mathcal{A}$ queries O_1, O_2, O_3, O_4, O_5 oracles, algorithm $\mathcal{B}$ queries these oracles in unp$^\tau$-privacy experiment and sends the results it receives to $\mathcal{A}$.

Simulate the challenge stage. When $\mathcal{A}$ outputs two uncorrupted tags $\mathcal{T}_i, \mathcal{T}_j$ which it has not queried O_5 oracle on, algorithm $\mathcal{B}$ will pick a random bit b and set the challenge tag $\mathcal{T}_c = \mathcal{T}_i$ if $b = 0$ and $\mathcal{T}_c = \mathcal{T}_j$ otherwise. Then $\mathcal{B}$ sends $\mathcal{T}_c$ to $\mathcal{A}$ as its challenge tag and $\mathcal{B}$ also submits $\mathcal{T}_c$ as its own challenge tag to the challenger in unp$^\tau$-privacy experiment.

Simulate the guess stage. When $\mathcal{A}$ queries O_1, O_2, O_3, O_4 oracles on $\mathcal{T}_c$, $\mathcal{B}$ also queries these oracles on $\mathcal{T}_c$ in unp$^\tau$-privacy experiment and sends the results it receives to $\mathcal{A}$

Output. When $\mathcal{A}$ outputs a bit b', if $b' = b$, $\mathcal{B}$ outputs 1, otherwise it outputs 0.

We can see the simulation of $\mathcal{B}$ is perfect. Let b_0 be the random bit selected in unp$^\tau$-privacy experiment. If $b_0 = 0$, then the challenge tag $\mathcal{T}_c$ is in fact a virtual tag in $\mathcal{A}$'s view since $\mathcal{A}$ will always obtain the random responses when it queries O_1, O_2, O_3 in the guess stage. Hence, in this case, the probability of $b' = b$ is equal to $\frac{1}{2}$. Otherwise, if $b_0 = 1$, the probability of $b' = b$ is $\frac{1}{2} + \epsilon$. That means the advantage of $\mathcal{B}$ in unp$^\tau$-privacy experiment is equal to $|\frac{1}{2} - (\frac{1}{2} + \epsilon)| = \epsilon$, which is the same as that of $\mathcal{A}$ in ind*-privacy experiment. Thus if $\mathcal{A}$ can pass ind*-privacy experiment with the advantage at least ϵ, then the advantage that $\mathcal{B}$ passes unp$^\tau$-privacy experiment is at least ϵ, too. In addition, the running time of $\mathcal{B}$ is approximate to that of $\mathcal{A}$. This completes the proof. □

Unp$^\tau$-Privacy $\Longrightarrow$Ind-Privacy From Theorem 2 and Theorem 3, we can obtain the following Theorem 4:

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

Unp$^\tau$-Privacy$\not\Longleftarrow$ Ind-Privacy

Theorem 5. *Given an RFID system RS, if RS is ind-private, then it does not imply RS is unp$^\tau$-private.*

Proof. (Sketch) We can use the same RFID system as in Li *et al.*'s paper [11]: $RS = \{R, \mathcal{T}, SetupReader, SetupTag, \pi\}$ such that the protocol transcripts will have the format $(c, r||r,\ f)$. Then we can show that RS is ind-private since for any PPT adversary, $r_1||r_1$ and $r_2||r_2$ are just two independent random strings. However, in unp$^\tau$-privacy experiment, the adversary can easily distinguish if the output $r_1||r_2$ comes from a real protocol transcript or it is chosen randomly by the challenger. If $r_1||r_2$ is chosen by the challenger randomly, then we know $r_1 \neq r_2$ with overwhelming probability; otherwise, if it is from the real protocol transcript, then $r_1 = r_2$ definitely. That is to say, RS is not unp$^\tau$-private. This completes the proof. □

5.2 Relation between Unp$^\tau$-Privacy and Unp*-Privacy

According to the counterexample in Fig. 5, we have known that unp*-privacy does not imply unp$^\tau$-privacy. Since the adversary are more powerful in unp$^\tau$-privacy experiment than in unp*-privacy experiment, intuitively we can understand that unp$^\tau$-privacy implies unp*-privacy.

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

Proof. Assume that RS is not unp*-private. That is, there exists an adversary $\mathcal{A}$ which can win the unp*-privacy game with advantage at least ϵ, and the running time at most t. We construct an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ as a subroutine and can pass the unp$^\tau$-private experiment. Algorithm $\mathcal{B}$ can simulate the unp*-private experiment for $\mathcal{A}$ as follows.

Simulate the learning stage. When $\mathcal{A}$ queries O_1, O_2, O_3, O_5 oracles, algorithm $\mathcal{B}$ queries these oracles in unp$^\tau$-privacy experiment and sends the results it receives to $\mathcal{A}$.

Simulate the challenge stage. When $\mathcal{A}$ outputs one uncorrupted tag $\mathcal{T}_c$ as its challenge tag, algorithm $\mathcal{B}$ also makes $\mathcal{T}_c$ as its own challenge tag in unp$^\tau$-privacy experiment.

Simulate the guess stage. When $\mathcal{A}$ queries O_1, O_2, O_3 oracles on $\mathcal{T}_c$, $\mathcal{B}$ also queries these oracles on $\mathcal{T}_c$ in unp$^\tau$-privacy experiment and sends the results it receives to $\mathcal{A}$.

Output. When $\mathcal{A}$ outputs a bit b', $\mathcal{B}$ also takes b' as its output.

We can see the simulation of $\mathcal{B}$ is perfect. Thus if $\mathcal{A}$ can pass unp*-privacy experiment with the advantage at least ϵ, then the advantage that $\mathcal{B}$ passes unp$^\tau$-privacy experiment is at least ϵ, too. In addition, the running time of $\mathcal{B}$ is approximate to that of $\mathcal{A}$. This completes the proof. □

Up to now, we have explored all these relations among ind-privacy, unp*-privacy and our newly proposed unp$^\tau$-privacy. As shown in Fig. 1, we can obtain the following claim:

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

6 Conclusion

In this paper, we revisited the unp*-privacy model which is based on the unp-privacy and pointed out its limitations by giving a counterexample and demonstrating a new traceability attack on it. Then we proposed a new unpredictability-based privacy model, denoted as unp$^\tau$-privacy. We investigated the relationship among ind-privacy, unp*-privacy and unp$^\tau$-privacy and formally proved that our unp$^\tau$-privacy is stronger than both ind-privacy and unp*-privacy.

References

1. Avoine, G.: Adversarial model for radion frequency identification. Cryptology ePrint Archive, Report 2005/049 (2005), `http://eprint.iacr.org/`
2. Burmester, M., Le, T.V., de Medeiros, B., Tsudik, G.: Universally composable RFID identification and authentication protocols. ACM TISSEC 2009 12(4) (2009)
3. Deng, R.H., Li, Y., Yung, M., Zhao, Y.: A new framework for RFID privacy. In: Gritzalis, D., Preneel, B., Theoharidou, M. (eds.) ESORICS 2010. LNCS, vol. 6345, pp. 1–18. Springer, Heidelberg (2010)

4. Ha, J., Moon, S., Zhou, J., Ha, J.: A new formal proof model for RFID location privacy. In: Jajodia, S., Lopez, J. (eds.) ESORICS 2008. LNCS, vol. 5283, pp. 267–281. Springer, Heidelberg (2008)
5. Henrici, D., Müller, P.: Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In: IEEE PerCom Workshops 2004, pp. 149–153 (2004)
6. Hermans, J., Pashalidis, A., Vercauteren, F., Preneel, B.: A new RFID privacy model. In: Atluri, V., Diaz, C. (eds.) ESORICS 2011. LNCS, vol. 6879, pp. 568–587. Springer, Heidelberg (2011)
7. Juels, A., Weis, S.A.: Defining strong privacy for RFID. In: IEEE PerCom Workshops 2007, pp. 342–347 (2007); Also appears in ACM TISSEC 2009 13(1), 7 (2009)
8. Kim, C.H., Avoine, G., Koeune, F., Standaert, F.-X., Pereira, O.: The Swiss-Knife RFID distance bounding protocol. In: Lee, P.J., Cheon, J.H. (eds.) ICISC 2008. LNCS, vol. 5461, pp. 98–115. Springer, Heidelberg (2009)
9. Le, T.V., Burmester, M., de Medeiros, B.: Universally composable and forward-secure RFID authentication and authenticated key exchange. In: ASIACCS 2007, pp. 242–252 (2007)
10. Lee, S.M., Hwang, Y.J., Lee, D.-H., Lim, J.-I.: Efficient authentication for low-cost RFID systems. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganá, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3480, pp. 619–627. Springer, Heidelberg (2005)
11. Li, Y., Deng, R.H., Lai, J., Ma, C.: On two RFID privacy notions and their relations. ACM TISSEC 2011 14(4) (2011)
12. Ma, C., Li, Y., Deng, R.H., Li, T.: Relation between two notions, minimal condition, and efficient construction. In: ACM CCS 2009, pp. 54–65 (2009)
13. Moriyama, D., Matsuo, S., Ohkubo, M.: Relations among notions of privacy for RFID authentication protocols. In: Foresti, S., Yung, M., Martinelli, F. (eds.) ESORICS 2012. LNCS, vol. 7459, pp. 661–678. Springer, Heidelberg (2012)
14. Ng, C.Y., Susilo, W., Mu, Y., Safavi-Naini, R.: RFID privacy models revisited. In: Jajodia, S., Lopez, J. (eds.) ESORICS 2008. LNCS, vol. 5283, pp. 251–266. Springer, Heidelberg (2008)
15. Ouafi, K., Phan, R.C.-W.: Traceable privacy of recent provably-secure RFID protocols. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 479–489. Springer, Heidelberg (2008)
16. Paise, R.-I., Vaudenay, S.: Mutual authentication in RFID: Security and privacy. In: ASIACCS 2008, pp. 292–299 (2008)
17. Vaudenay, S.: On privacy models for RFID. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 68–87. Springer, Heidelberg (2007)
18. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and privacy aspects of low-cost radio frequency identification systems. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) Security in Pervasive Computing 2003. LNCS, vol. 2802, pp. 201–212. Springer, Heidelberg (2004)
19. Yang, A., Zhuang, Y., Wong, D.S.: An efficient single-slow-phase mutually authenticated RFID distance bounding protocol with tag privacy. In: Chim, T.W., Yuen, T.H. (eds.) ICICS 2012. LNCS, vol. 7618, pp. 285–292. Springer, Heidelberg (2012)