Two RFID Privacy Models in Front of a Court

Mohammad Hassan Habibi, Mohammad Reza Aref

ISSL Lab, EE Department, Sharif University of Technology
m.h.habibi@sabamail.com, aref@sharif.edu

Abstract. In ASIACRYPT 2007, Vaudenay proposed a comprehensive privacy model for unilateral RFID schemes. Soon after, in ASIACCS 2008, Paise and Vaudenay presented a new version of the cited model which includes mutual authentication protocols. Recently, Armknecht et al. published two papers in ACNS 2010 and Transactions on Computational Science that examines the Paise-Vaudenay model. They claim that the Paise-Vaudenay model has several inadequacies and prove some results that contradict the Paise-Vaudenay outcomes.
In this paper, we investigate the Armknecht et al.'s papers and show some subtle faults in their works. In particular, our contribution is twofold. First, we show the privacy definition and the adversary goal presented by Armknecht et al. are completely different from the Paise-Vaudenay ones. Therefore, their different results arise from the fundamental differences in their definition of the privacy and their results cannot be valid in the Paise-Vaudenay model. Furthermore, we examine Armknecht et al.'s results and show that by using their methodology, different outcomes are achieved in the same theorems. In fact we prove by using their approach to the privacy that the highest achievable privacy level is narrow-weak privacy, which contradicts most of the theorems proved by Armknecht et al.

Keywords: RFID, privacy model, mutual authentication

1 Introduction

Radio Frequency Identification (RFID) systems are used to identify objects wirelessly. Due to the developing of RFID systems to many applications such as e-passports [14], public transportation [17] and supply chain management [21], providing security and privacy in these systems has been become a major research field in recent years. Although many RFID authentication and identification protocols have been proposed to cover related security and privacy concerns [3,10,24,29,30], large amounts of papers have been published on their weaknesses [15,25,27,28]. However, we need formal models to measure the security and privacy levels of a variety of RFID protocols. Such models give effective tools to examine particular characteristics of the protocols in a comparable way. In attempt to formalise privacy in RFID systems, several works have been proposed in the recent years [4,6,7,11,16,31,32]. In this context one of the most comprehensive privacy models was proposed by Vaudenay at ASIACRYPT 2007 [34] which

defined a privacy and security framework to examine unilateral authentication protocols. This model captures many notions of the previous works in addition to some new concepts. This model was expanded to mutual authentication by Paise and Vaudenay at ASIACCS 2008 [26]. The privacy notion in both models was based on *anonymity* and *unlinkability* concepts. *Anonymity* in RFID context means the confidentiality of a tag's identity, namely an adversary cannot infer the identity of tag, and *unlinkability* means that interactions of a tag cannot be linked.

In 2010, Armknecht et al. published two papers in the proceedings of ACNS [2] and in the journal Transactions on Computational Science [1] where they investigate some notions and results of the Paise-Vaudenay model (denoted hereafter as P-V model) [26]. In these papers they claim that the P-V model has some deficiencies and prove several new results. In this work we scrutinize their papers [1,2] and prove that some of their assumptions and results are incorrect.

1.1 Related Work

One of the first attempts to provide a formal privacy model for RFID systems is due to Avoine [5]. In [5] a range of adversarial abilities are defined and the goal of the adversary is to distinguish two tags. Based on [5], Juels and Weis propose in [16] a new privacy model that includes the concept of *strong privacy* and takes into consideration side channel information. Other works on privacy models were done by Burmester, van Le, and de Medeiros [8], Lim and Kwon [19], van Deursen, Mauw, and Radomirović [31], as well as Canard, Coisel, Etrog, and Girault [9].

All the mentioned models are based on the notion of *indistinguishability* of two tags. Nevertheless, another approach to establish RFID privacy models is based on the notion of *unpredictability* of the output of a protocol. In this direction Ha, Moon, Zhou, and Ha [12] presented a new formal poof model for RFID location privacy, which was later shown by van Deursen and Radomirović to have some defects [33]. The approach in [12] was followed by a few other works [11,18,20].

In conjunction to the *indistinguishability* based approach, Vaudenay proposed a more complete and general model [34] in which the privacy is divided into eight different levels based on given abilities to the adversary, including tag corruption and side channel information. While Vaudenay's model [34] only considers unilateral schemes, Paise and Vaudenay published an evolved version of [34] that defines privacy notions for mutual RFID authentication protocols [26]. They also prove in [26] some possibility and impossibility results on the privacy notions.

In attempt to inquire into Vaudenay [34] and Paise-Vaudenay [26] works, Ng, Susilo, Mu, and Safavi-Naini published two papers at ESORICS 2008 [22] and ESORICS 2009 [23]. In [22] they categorize eight privacy levels of [34] into three levels by introducing the notion of *wise* adversary. This *wise* adversary is restrained in a way that she is not able to access oracles where the results can be precisely predicted. In another approach, Ng et al. [23] examine the highest

achievable privacy levels of synchronized RFID authentication protocols based on [26,34] and show that *forward privacy* is impossible with these synchronized protocols.

Finally, Armknecht et al. investigated the P-V model and proved some new results [1,2] that contradict the P-V ones.

1.2 Our Contribution

In this paper, our contribution is twofold.

Firstly, we look at the privacy definition and adversary goal presented by Paise-Vaudenay and Armknecht et al. precisely and show the fundamental differences between them. In particular, we demonstrate that Armknecht et al.'s approach to privacy is completely different from the Paise-Vaudenay one. This leads them to deduce results different than those of Paise and Vaudenay. Therefore, we prove that though their claims on impossibility results for privacy notions may be valid on their assumptions, they cannot be valid in the P-V model.

Secondly, we apply the Armknecht et al.'s privacy approach on the same theorems they proved and obtain different results, demonstrating that their proofs are wrong.

1.3 Organization of the Paper

We first give an abstract of the P-V model [26] in Section 2. Our first contribution is presented in Section 3 in which the fundamental distinctions between the P-V approach and the Armknecht et al. approach to RFID privacy is proved. Then we thoroughly analyse the Armknecht et al.'s theorems and results and point out distinct results on the same theorems and problems in Section 4. Finally we conclude in Section 5.

2 The P-V Model

In this section we briefly review the privacy model proposed by Paise-Vaudenay [26] which is based on [34].

2.1 RFID Scheme

An RFID scheme is defined by:

- A $\mathsf{SetupReader}(1^s)$ algorithm to produce the required system parameters (public key K_P, secret key K_S) based on a security parameter s and initialise a database.
- A $\mathsf{SetupTag}_{K_P}(\mathrm{ID})$ algorithm to generate the tag secret K and the initial tag state S. When a tag is legitimate, the pair (ID, K) is stored in the database.
- An interaction protocol between a tag and the reader to execute the authentication procedure.

2.2 Adversarial Model

To represent the abilities of the adversary, eight oracles are defined as following.

- CreateTag^b(ID): is used to create a free tag, either legitimate ($b = 1$) or not ($b = 0$).
- DrawTag(): this oracle picks a free tag randomly and makes it accessible to the adversary to interact with by returning a handle $vtag$ (unique and one time). DrawTag oracle keeps a hidden table Γ such that $\Gamma(vtag)$ is the ID of $vtag$. This hidden table is not available to the adversary until the last step of the privacy game. DrawTag oracle also returns a bit b which indicates whether the tag is legitimate ($b = 1$) or not ($b = 0$).
- Free($vtag$): makes $vtag$ unavailable by moving it to the set of free tags.
- Launch(): makes the reader to start a new protocol instance π.
- SendReader$(m, \pi) \rightarrow m'$ (resp. SendTag$(m, vtag) \rightarrow m$): sends a message m to a protocol instance π for the reader (resp. to $vtag$) and receives the answer m according to the protocol.
- Result$(\pi) \rightarrow x$: when π is complete, returns 1 if the tag is identified and 0 otherwise.
- Corrupt$(vtag) \rightarrow S$: returns the current internal state S of the tag.

2.3 Privacy Classes

The P-V model defines eight adversarial classes based on the availability of the oracles Corrupt and Result to the adversary.

`Strong` adversaries can use all oracles without limitation. `Destructive` adversaries are the class of adversaries who destroy $vtag$ after a Corrupt($vtag$) query. `Forward` adversaries use Corrupt oracles under the limitation that they can only be followed by other Corrupt oracles. `Weak` adversaries never use Corrupt oracles. The cited adversaries have corresponding `Narrow` classes in which they have no access to the Result oracle.

Each adversarial class corresponds to a privacy class with the same name. The relationship between privacy classes is as following.

$$\begin{array}{ccccccc} \text{strong} & \Rightarrow & \text{destructive} & \Rightarrow & \text{forward} & \Rightarrow & \text{weak} \\ \Downarrow & & \Downarrow & & \Downarrow & & \Downarrow \\ \text{narrow-strong} & \Rightarrow & \text{narrow-destructive} & \Rightarrow & \text{narrow-forward} & \Rightarrow & \text{narrow-weak} \end{array}$$

2.4 Privacy Game

The adversary, a set of tags, a protocol instance π, and the reader participate in the *privacy game*. In this game, the adversary can interact with the tags and the reader by calling a polynomially-bounded times any oracle based on

her class. Once done, the hidden table Γ is revealed to the adversary. Based on $(vtag, ID)$ entries in the table Γ and information obtained from the queries, the adversary outputs $True$ or $False$ for the question whether $\Gamma(vtag) = ID$. The adversary wins the *privacy game* if she outputs $True$ in a *non-trivial* way. An adversary $\mathcal{A}$ is called *trivial* if there is a blinded adversary $\mathcal{A}^{\mathcal{B}}$ such that $\Pr[\mathcal{A}$ wins$] - \Pr[\mathcal{A}^{\mathcal{B}}$ wins$]$ is negligible. Namely, the adversary makes no effective use of protocol messages.

Definition 1 (Blinder). *A blinder $\mathcal{B}$ is a simulator which simulates the* Launch, SendReader, SendTag, *and* Result *oracles without having access to the secret keys and the database. When a blinded adversary $\mathcal{A}^{\mathcal{B}}$ makes the* Launch, SendReader, SendTag, *and* Result *queries, she is answered through the blinder $\mathcal{B}$.*

3 Different Approaches

In this section we present the basic differences between Armknecht et al.'s approach and the P-V one. First we show that the privacy definition presented in [1,2] is conceptually different from the one presented in the P-V [26] and Vaudenay [34] models. This difference leads Armknecht et al. to reach new results on privacy notions that contradict P-V ones. Then, we point out that Armknecht et al.'s viewpoint on temporary state disclosure causes them to achieve new outcomes.

This means the P-V statements are right and correct in their model and the new results obtained by Armknecht et al. are caused by their new approach to the privacy notions.

3.1 Different Approaches to Privacy

To show the fundamental differences between the viewpoint of Armknecht et al. on one side [1,2] and Vaudenay and Paise on the other side [34,26], we first review their privacy definitions. We then explain why they are different.

The Armknecht et al. Approach They define privacy of an RFID scheme based on a *privacy experiment* $\mathbf{Exp}^{prv-b}_{\mathcal{A}_{prv}}$which has two phases. In this experiment, $\mathcal{A}_{prv}$ is an adversary who performs the *privacy experiment* and the bit b is randomly chosen from the set $\{0, 1\}$. In the first phase, the reader is initialized by SetupReader algorithm and then the public key pk_R is given to $\mathcal{A}_{prv}$ and $\mathcal{B}$. Now $\mathcal{A}_{prv}$ is allowed to make queries according to her class. If $b = 0$, all queries are answered by real oracles, but if $b = 1$, all Launch, SendReader, SendTag, and Result queries are answered by the blinder $\mathcal{B}$ and other queries are answered by the real oracles. After a polynomial number of queries, the second phase is started in which the adversary cannot interact with the oracles and the hidden table Γ is released to her. Finally she returns a bit b' that is shown by $\mathbf{Exp}^{prv-b}_{\mathcal{A}_{prv}} = b'$. A formal definition of the privacy is given below.

Privacy Definition(Def. 6 of [1,2]). Let C be one of the adversary classes. An RFID scheme is $C-private$ if for every adversary $\mathcal{A}_{prv}$ of C there exists a blinder $\mathcal{B}$ such that the advantage $\mathbf{Adv}^{prv}_{\mathcal{A}_{prv}}$=|Pr[$\mathbf{Exp}^{prv-0}_{\mathcal{A}_{prv}}$= 1]−Pr[$\mathbf{Exp}^{prv-1}_{\mathcal{A}_{prv}}$= 1]| of $\mathcal{A}_{prv}$ is negligible.

The Paise-Vaudenay Approach The privacy in the P-V model is defined by a *privacy game* in which an adversary participates. The adversary tries to identify target tags (break *anonymity*) or link their interactions (break *unlinkability*) based on information obtained from the oracles. In fact if an adversary can exploit the information obtained from the oracles to trace a target tag, the privacy notion is broken. In this direction they defines two kinds of adversaries including the adversary $\mathcal{A}$ and the blinded adversary $\mathcal{A}^B$ who are different in accessing to the oracles. In the *privacy game* the adversary $\mathcal{A}$ is free to access any oracles in her oracle collection, thus access to the messages produced by tags and the reader. However, the blinded adversary $\mathcal{A}^B$ does not have access to the protocol transcript and its queries to LAUNCH, SEND, and RESULT oracles are answered by the *blinder* $\mathcal{B}$ that does not have access to the secrets of tags or the reader. Now if the adversary $\mathcal{A}$ takes more advantage than $\mathcal{A}^B$ in winning the *privacy game*, it means the protocol messages leak some information that has been exploited by $\mathcal{A}$. Thus the protocol is not private. More information on P-V approach has been given in the Section 2.

Different Comprehension By the first look at to the privacy definitions presented by Armknecht et al. and P-V model, it seems that both of them give the same definition, and Armknecht et al. just paraphrase the model from Paise and Vaudenay by changing the notations only. Because they use the same oracles and set up algorithms as the P-V model, as well as utilize the most concepts given by Paise and Vaudenay.

But, a careful analysis of the privacy definitions presented by Armknecht et al. [1,2] and Paise-Vaudenay [26], allows to highlight the deep and basic differences between them. Indeed, the privacy definition gave by Paise and Vaudenay is based on the *anonymity* of tags and *unlinkability* of their interactions. In the definitions presented by Vaudenay [34] and Paise-Vaudenay [26], it is clear that the most important components of the privacy are the tags, their *anonymity* and *unlinkability* of their interactions (*untraceability*). Consequently, the privacy of an RFID scheme is broken when an adversary can identify a target tag or link its interactions. Vaudenay says: "we define privacy in terms of ability to infer non-trivial ID (tag) relations from protocol message" [34](page.7). However, in the privacy definition presented by Armknecht et al. the *anonymity* of the tags and the *unlinkability* of their interactions are not very important. Instead, in their approach the key factor is the adversary ability to distinguish between the real oracles and the *blinder* $\mathcal{B}$. If so, the privacy is broken. Consequently, in theorems 1, 2 of [1] and 1, 2, 3 of [2], the adversary interacts with one tag only and her goal is not to identify it among a group or link its interactions, but is to recognise the blinder *blinder* $\mathcal{B}$ from the real oracles.

The characteristics of the privacy game in P-V model

1. Although it is not mentioned explicitly in the P-V model, as $\mathcal{A}$ should identify a tag among a group, the adversary in the *privacy game* deals with at least two tags or their corresponding states which can be legitimate or not (This can be verified in theorem 1, subsections 5.1, and 5.2 of [26], and theorems 9, 11, 12, 13, 15, 19, and notes 10, and 18 of [34]).
2. In the attack phase of the *privacy game*, in one time the adversary interacts with `known` tags (that she knows their identity) or their corresponding states, and makes queries based on her class. In another time during this phase, $\mathcal{A}$ interacts with `unknown` tags and makes queries based on her class (to identify an `unknown` tag or make any link).
3. The capability of the adversary is evaluated based on her ability in making any link between the `known` and `unknown` tags she interacted with. Any ability of the adversary in making this link violates the notions of *anonymity* and *unlinkability*, so breaks the privacy.

The characteristics of the privacy experiment in Armknecht et al. model

1. The adversary can interact with only one tag (e.g. algorithms 2, 3 of [2] and 2, 4, 6 of [1]).
2. In the attack phase of the *privacy experiment*, the adversary can interact with only a `known` tag (e.g. algorithms mentioned in step 1). As a result, when the adversary deals with just one `known` tag, there is no room to evaluate the notions of *anonymity* and *unlinkability*.
3. The capability of the adversary is evaluated based on her ability in distinguishing between the `blinder` $\mathcal{B}$ and the `real oracles`. The goal of the adversary is not to violate the *anonymity* or *unlinkability*.

This distinctive approach to the privacy, adversary and her goals leads the authors of [1,2] to derive new outcomes that are inconsistent with [26].

Besides, the concept of privacy in the P-V model is based on distinguishing between `different tags`, while in the Armknecht et al.'s model the privacy is defined based on the notion of (`left-or-right`) or (`0-or-1`) indistinguishability. In fact, the adversary's goal in [1,2] is to distinguish between the `0's world` (including the real oracles) and the `1's world` (including the *blinder* $\mathcal{B}$). This implies that we consider the model introduced in [1,2] as a new model that differs from P-V one. Similar to this approach, Hermans, Pashalidis, Vercauteren, and Preneel [13] introduce a new RFID privacy model, but they state that their model is a new one, in contrast with Armknecht et al.

3.2 Different Approaches to Temporary State Disclosure

Another basic difference between [1,2] and [26] is the concept of temporary state disclosure.

At first, it should be pointed that in [1,2] some new concepts on temporary state disclosure are added to ones in [26] that are noticeable, and we do not

discuss these new notes. In this subsection we focus on different approaches on the concept of temporary state disclosure in the P-V and Armknecht et al.'s models.

In [26] a tag in the set of *drawn tags* means that it is in the reader range and accessible to the adversary. So CORRUPT reveals temporary and permanent tag states. When a drawn tag becomes *free*, this means out of the reader range and is unavailable to the adversary. In this situation Paise and Vaudenay consider two cases. In the first case, when a *drawn* tag is put to the set of *free* tags and then put back again to the set of *drawn* tags, its temporary state can be revealed by CORRUPT. In this case they prove (Theorem.1 of [26]) no RFID scheme providing secure reader authentication is *narrow-forward* private in their model. In the second case, they assume that temporary tag memory is automatically erased as soon as the tag is put back to the set of *free* tags. Hence when a tag is drawn again, its temporary state is not revealed by CORRUPT. In the P-V model there is no discussion on temporary state disclosure when a tag is in the set of *drawn* tags for the first time, instead they discuss the situation of *drawn*, *free*, *drawn* tags (a tag is *drawn* first, then it is released, and finally it is *drawn* again).

However, the authors of [1,2] present a distinctive definition of temporary state disclosure. In their papers there is no discussion about *drawn*, *free*, *drawn* tags. They just consider *drawn* tags and discuss whether CORRUPT reveals the temporary state of a tag when it is drawn for the first time.

Clearly, the temporary state disclosure is differently addressed in [26] and [1,2]: the temporary memory may be erased when the tag becomes free in [26], while Armknecht et al. do not consider this situation at all.

4 Different Results

Besides the differences between Armknecht et al.'s approach and P-V one, another problem is the fact that Armknecht et al.'s approach has some defects by itself. Namely if the privacy level of the RFID schemes is examined by applying Armknecht et al.'s approach, then the results will be variable. In precise, we show if we apply their methodology to the same problems and the same theorems, we obtain different results.

In the following in each case we first mention the theorems proved by Armknecht et al. in [1,2]. Then by applying their approach to the privacy we prove new results and theorems that are completely different from the ones in [1,2]. These differences indicate that the method in which Armknecht et al. evaluate the privacy of RFID schemes is not a standard method.

In addition, we prove with the privacy definition presented in [1,2], that the highest achievable privacy, in both assumptions temporary state disclosure and without temporary state disclosure, is *narrow-weak* privacy. This result contradicts the results of [1,2] and shows their definition of the privacy and the adversary success criteria is not complete.

4.1 Case 1

THEOREM 1 of [1] and THEOREM 2 of [2] state: There is no RFID scheme that achieves both *reader authentication* and `narrow-forward` privacy under temporary tag state disclosure.

To prove these theorems, the authors construct a security adversary $\mathcal{A}_{sec}$ in ALG.1 that uses a *blinder* $\mathcal{B}$ internally to violate *reader authentication*. Then they present a *narrow-forward* adversary in ALG.2 and show if an adversary cannot win the *privacy experiment*, it means the scheme is *narrow-forward* private. So the *blinder* $\mathcal{B}$ is perfect and $\mathcal{A}_{sec}$ can use *blinder* $\mathcal{B}$ in ALG.1 to violate *reader authentication*.

By applying the Armknecht et al.'s approach, we prove the following theorem.

Theorem 1. *There is no RFID scheme that achieves both reader authentication and* `weak privacy`.

Proof. The proof methodology is similar to [1,2]. We just modify ALG.2 of [1,2] and change *narrow-forward* adversary to *weak* adversary. In fact, if we omit the CORRUPT($vtag$) query in the step 12 of ALG.2, and instead use SetupTag($m_{2q_R-1}, vtag$) and Result($vtag$) queries in the steps 12, 13 of the *Modified* ALG.2, we get a *weak* adversary. By having this *weak* adversary, the proof is done according to the proof of THEOREM 1 of [1]. □

Modified ALG.2. *weak adversary*

```
 − : ...
11 : ...
12 : SetupTag(m_{2q_R−1},vtag)
13 : out_TID ← Result(vtag)
14 : if out_TID = ok then return 0
15 : else  return 1
16 : end if
```

4.2 Case 2

Corollary 1 of [1,2] says: In the P-V model there is no RFID scheme that achieves both *reader authentication* and any privacy notion that is different from `weak` and `narrow-weak` privacy under temporary state disclosure.
The authors conclude this corollary as a result of THEOREM 1 of [1] and THEOREM 2 of [2].

As a result of the our Theorem 1 that we proved and THEOREM 1 of [1], we conclude the following corollary.

Corollary 1. *In the P-V model there is no RFID scheme that achieves both reader authentication and any privacy notion that is different from* `narrow-weak` *privacy under temporary state disclosure.*

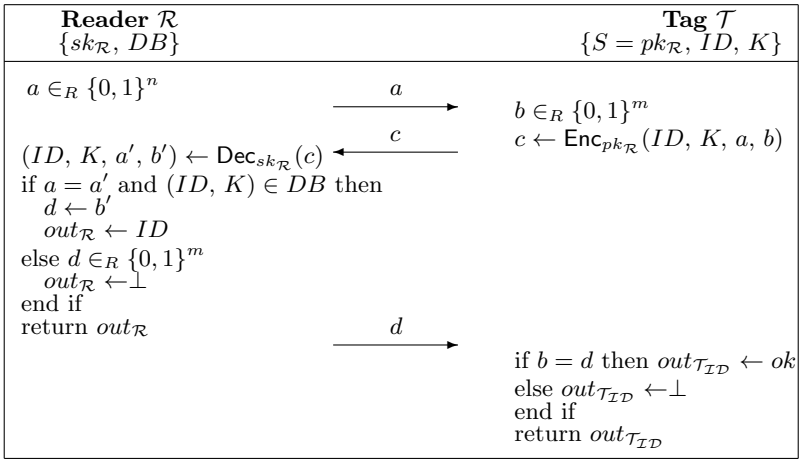

Fig. 1. Figure 2 of [2]

4.3 Case 3

THEOREM1 of [2] states: The RFID protocol shown in Figure 1 does not achieve `narrow-strong` privacy, *reader authentication* and *correctness* at the same time.

The authors construct a *narrow-strong* adversary $\mathcal{A}_{prv}$ which corrupts tag $\mathcal{T}_{ID}$ right before it receives d (d authenticates the reader to $\mathcal{T}_{ID}$) and obtains the complete state of $\mathcal{T}_{ID}$ including its temporary state b. Thus $\mathcal{A}_{prv}$ can perform the computation of $\mathcal{T}_{ID}$ and check whether $b = d$. Now, if this computation leads to the acceptance of the reader, she realises interacting with the real oracles, otherwise she recognises the *blinder* $\mathcal{B}$. As a result, $\mathcal{A}_{prv}$ can distinguish between the real oracles and the simulation by the *blinder* $\mathcal{B}$, so violates *narrow-strong* privacy.

By using the definition of the adversary's success criteria, we state the following theorem.

Theorem 2. *The RFID protocol shown in Figure 1 does not achieve* ***`narrow-destructive`*** *privacy, reader authentication and correctness at the same time.*

Proof. The proof is similar to the THEOREM1 of [2] and the discussion given in Subsection 4.3. We do not change the adversary nor do the attack strategy introduced in THEOREM1 of [2]. We construct a *narrow-destructive* adversary $\mathcal{A}_{prv}$ which corrupts tag $\mathcal{T}_{ID}$ right before it receives d and obtains the complete state of $\mathcal{T}_{ID}$. Therefore, $\mathcal{A}_{prv}$ can perform the computation of $\mathcal{T}_{ID}$ and check whether $b = d$. Now, if this computation leads to the acceptance of the reader, she realises interacting with the real oracles, otherwise she recognises the *blinder* $\mathcal{B}$. Consequently, $\mathcal{A}_{prv}$ can distinguish between the real oracles and the simulation by the *blinder* $\mathcal{B}$, so violates *narrow-destructive* privacy. Since $\mathcal{A}_{prv}$ does not use any SENDTAG queries after a CORRUPT query, she is a *destructive* one. □

Modified ALG.4. *weak adversary*

```
1 : CreateTag(ID)
2 : vtag ← DrawTag(Pr[ID]=1)
3 : π ←LUNCH()
4 : m1 ← SendReader(−, π)
5 : t ∈ {1, ..., qT}
6 : i ← 1
7 : while i < t do
8 :    m2i ←SendTag(m2i−1, vtag)
9 :    if i < qR then m2i+1 ← SendReader(m2i, π)
10 :   end if
11 :   i ← i + 1
12 : end while
13 : SendTag(m2t−1, vtag)
14 : out_TID ← result(vtag)
15 : if out_TID = ok then return 0
16 : else return 1
17 : end if
```

4.4 Case 4

THEOREM 2 of [1] and THEOREM 5 of [2] state: In the P-V model there is no RFID scheme that fulfils both *reader authentication* and `narrow-strong` privacy.

In these theorems the authors consider situation in which CORRUPT query does not reveal the temporary state of a tag. To prove the theorems the authors construct a *narrow-strong* adversary $\mathcal{A}_{prv}$ (ALG.4 of [1]) and state that if the scheme in ALG.4 provides *narrow-strong* privacy, then there should be a *blinder* $\mathcal{B}$ that cannot be distinguished by $\mathcal{A}_{prv}$. Consequently, they construct a security adversary $\mathcal{A}_{sec}$ (ALG.3 of [1]) that uses $\mathcal{B}$ internally to violate *reader authentication*.

By using the same methodology as Armknecht et al., we prove the following theorem.

Theorem 3. *In the PV-Model there is no RFID scheme that fulfils both reader authentication and* `weak` *privacy.*

Proof. The methodology to prove our Theorem 2 is the same as THEOREM 2 of [1]. We just modify ALG.4 of [1] to change the *narrow-strong* adversary into *weak* adversary. In fact, we omit CORRUPT($vtag$) query in the step 3 of ALG.4. Instead we use SENDTAG($m_{2i-1}, vtag$), SENDTAG($m_{2t-1}, vtag$) and Result($vtag$) queries in the steps 8, 13, 14 of the *Modified* ALG.4 to obtain a *weak* adversary. If the scheme provides *weak* privacy, then there should be a *blinder* $\mathcal{B}$ that is perfect. Now, $\mathcal{A}_{sec}^{\mathcal{B}}$ uses $\mathcal{B}$ to violate *reader authentication.* □

4.5 Case 5

THEOREM4 of [1] says: There is no stateless RFID scheme that achieves `destructive` privacy.

The authors establish a destructive adversary $\mathcal{A}_{prv}$(ALG.7 of [1]) and assume the scheme in ALG.7 is *destructive* private. Thus there exists a *blinder* $\mathcal{B}$ which $\mathcal{A}_{prv}$ cannot distinguish from the real oracles. After that, they construct a *narrow-forward* adversary $\mathcal{A}_{prv}^{\mathcal{B}_D}$ in ALG.8 that uses $\mathcal{B}$ internally to break the *narrow-forward* privacy. Clearly, this contradicts the hypothesis which states that the scheme is *destructive*-private. Thus the authors conclude *destructive* privacy is not achievable.

By using the privacy definition presented in [1,2], we prove a new theorem.

Theorem 4. *There is no stateless RFID scheme that achieves* `weak` *privacy.*

Proof. We construct a *weak* adversary $\mathcal{A}_{prv}$ that takes overwhelming advantage in distinguishing between the real oracles and the *blinder* $\mathcal{B}$ in the stateless RFID schemes, so breaks the notion of *weak* privacy. The adversary and the attack strategy are presented in Algorithm 1.

It is clear if $\mathcal{A}_{prv}$ interacts with the real oracles, then the last message sent by the reader is accepted by *vtag* with overwhelming probability, and it returns 0. Therefore, $\Pr[\mathbf{Exp}^{prv-0}_{\mathcal{A}_{prv}}=1]$ is negligible. On the other hand if $\mathcal{A}_{prv}$ interacts with the *blinder* $\mathcal{B}$, then the last message sent by the *blinder* $\mathcal{B}$ is rejected by *vtag* with the probability of $\frac{1}{2}$, therefore $\Pr[\mathbf{Exp}^{prv-1}_{\mathcal{A}_{prv}}=1]=\frac{1}{2}$. Hence the advantage by $\mathbf{Adv}^{prv}_{\mathcal{A}_{prv}}=|\Pr[\mathbf{Exp}^{prv-0}_{\mathcal{A}_{prv}}=1]-\Pr[\mathbf{Exp}^{prv-1}_{\mathcal{A}_{prv}}=1]|$ of $\mathcal{A}_{prv}$ is overwhelming. □

Algorithm 2. *weak adversary*

```
1 : CreateTag(ID)
2 : vtag ← DrawTag(Pr[ID]=1)
3 : π ←lunch()
4 : m_1 ← SendReader(−, π)
5 : while i < q_R do
6 :     if i < q_T then m_{2i} ← SendTag(m_{2i−1}, vtag)
7 :     end if
8 :     m_{2i+1} ←SendReader(m_{2i}, π)
9 :     i ← i + 1
10 : end while
11 : SendTag(m_{2q_R−1}, vtag)
12 : out_{T_ID} ← result(vtag)
13 : if out_{T_ID} = ok then return 0
14 : else return 1
15 : end if
```

5 Conclusion

In this paper we investigated Armknecht et al.'s works [1,2] in detail and showed their results were not valid in the P-V model [26]. In particular, at first we proved there were fundamental differences between Armknecht et al.'s approach to the privacy and the P-V one. Then we showed that the adversary goals and her success criteria were completely different in [1,2] and [26], as well as the concept

of temporary state disclosure. From all these reasons we can conclude that the results of [1,2] cannot be valid in the P-V model.

Also, we showed that Armknecht et al. use a method to prove their results that is not robust because the calculation of "$\mathbf{Exp}^{prv-b}_{\mathcal{A}_{prv}}$=1" is adopted to reach the expected result. So we proved that if we change the method of achieving "1" from "$\mathbf{Exp}^{prv-b}_{\mathcal{A}_{prv}}$" in the same theorem and the same attack strategy, the opposed outcome can be achieved. Finally, using Armknecht et al.'s approach, we obtained new results in Theorem 1, Corollary 1, Theorem 2, Theorem 3, and Theorem 4, by which proved that the highest achievable privacy level is *narrow-weak* privacy, which contradicts most of their results.

Acknowledgement

We are indebted to Gildas Avoine for his useful comments to improve this work.

References

1. Armknecht, F., Sadeghi, A.R., Scafuro, A., Visconti, I., Wachsmann, C.: Impossibility results for RFID privacy notions. In M.L. Gavrilova et al. (Eds.) Transactions on Computational Science. XI, LNCS, vol. 6480, pp. 39-63. Springer-Verlag Berlin Heidelberg (2010)
2. Armknecht, F., Sadeghi, A.R., Visconti, I., Wachsmann, C.: On RFID privacy with mutual authentication and tag corruption. In: Zhou, J. (ed.) ACNS 2010. LNCS, vol. 6123, pp. 493-510. Springer, Heidelberg (2010)
3. Avoine, G., Oechslin, P.: A scalable and provably secure hash based RFID protocol. In IEEE International Workshop on Pervasive Computing and Communication Security - PerSec 2005, Kauai Island, Hawaii, USA, March 2005. IEEE, IEEE Computer Society Press (2005)
4. Avoine, G.: Radio Frequency Identification: Adversary model and attacks on existing protocols. Technical Report, LASEC-REPORT-2005-001, September (2005)
5. Avoine, G.: Adversarial model for radio frequency identification. Cryptology ePrint Archive, report 2005/049, http://eprint.iacr.org/2005/049 (2005)
6. Bocchetti, S.: Security and privacy in RFID protocols. Master Thesis (2006)
7. Burmester, M., van Le, T., de Medeiros, B.: Provably secure ubiquitous systems: Universally composable RFID authentication protocols. Referenced 2006 at http://eprint.iacr.org/2006/131.pdf
8. Burmester, M., van Le, T., de Medeiros, B.: Universally composable and forward-secure RFID authentication and authenticated key exchange. In: Proc. of ASIACCS, pp. 242-252. ACM Press, New York (2007)
9. Canard, S., Coisel, I., Etrog, J., Girault. M.: Privacy preserving RFID systems: Model and constructions. Cryptology ePrint Archive, Report 2010/405, http://eprint.iacr.org/2010/405 (2010)
10. Chien, H.Y.: SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. IEEE Transactions on Dependable and Secure Computing 4(4), 337-340 (2007)
11. Deng, R.H., Li, Y., Yao, A.C., Yung, M., Zhao, Y.: A new framework for RFID privacy. In: D. Gritzalis, B. Preneel, and M. Theoharidou (Eds.): ESORICS 2010. LNCS, vol. 6345, pp. 1-18. Springer, Heidelberg (2010)

12. 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)
13. Hermans, J, Pashalidis, A., Vercauteren, F., Preneel, B.: A new RFID privacy model. To appear in the proceeding of 16th European Symposium on Research in Computer Security (ESORICS 2011), 12-14 September 2011, Leuven, Belgium (2011)
14. Hoepman, J.-H., Hubbers, E., Jacobs, B., Oostdijk, M., Schreur, R.W.: Crossing borders: security and privacy issues of the European epassport. In: Yoshiura, H., Sakurai, K., Rannenberg, K., Murayama, Y., Kawamura, S.-i. (eds.) IWSEC 2006. LNCS, vol. 4266, pp. 152-167. Springer, Heidelberg (2006)
15. Juels, A.: RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communications 24(2), 381-394 (2006)
16. Juels, A., Weis, S.A.: Defining strong privacy for RFID. In: Proceedings of PerCom 2007, pp. 342-347, http://eprint.iacr.org/2006/137 (2007)
17. Konomi, S., Roussos, G.: Ubiquitous computing in the real world: lessons learnt from large scale RFID deployments. Personal and Ubiquitous Computing, Volume 11, Issue 7, pp. 507-521 (2007)
18. Lai, J., Deng, R., Li, Y.: Revisiting unpredictability-based RFID privacy models. In: J. Zhou and M. Yung (Eds.): ACNS 2010. LNCS, vol. 6123, pp. 475-492. Springer, Heidelberg (2010)
19. Lim, C.H., Kwon, T.: Strong and robust RFID authentication enabling perfect ownership transfer. In: P. Ning, S. Qing, and N. Li (Eds.): ICICS 2006. LNCS, vol. 4307, pp. 1-20. Springer, Heidelberg (2006)
20. Ma, C., Li, Y., Deng, R., Li, T.: RFID privacy: Relation between two notions, minimal condition, and efficient construction. In: ACM CCS (2009)
21. Karkkainen, M.: Increasing efficiency in the supply chain for short shelf life goods using RFID tagging. International Journal of Retail & Distribution Management 31(10), 529-536 (2003)
22. Ng, C.Y., Susilo, W., Mu, Y., Safavi-Naini, R.: New privacy results on synchronized RFID authentication protocols against tag tracing. In: Backes, M., Ning, P. (eds.) ESORICS 2009. LNCS, vol. 5789, pp. 321-336. Springer, Heidelberg (2009)
23. 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. 251-256. Springer, Heidelberg (2008)
24. Ohkubo, M., Suzuki, K., Kinoshita, S.: Efficient hash-chain based RFID privacy protection scheme. In: Davies, N., Mynatt, E.D., Siio, I. (eds.) UbiComp 2004. LNCS, vol. 3205, Springer, Heidelberg (2004).
25. Ouafi, K., Phan, R.C.-W.: Privacy of recent RFID authentication protocols. In: L. Chen, Y. Mu, and W. Susilo (Eds.): ISPEC 2008. LNCS, vol. 4991, pp. 263-277. Springer, Heidelberg (2008)
26. Paise, R.I., Vaudenay, S.: Mutual authentication in RFID: Security and privacy. In: Proc. of ASIACCS 2008, pp. 292-299. ACM Press, New York (2008)
27. Phan, R.C.-W.: Cryptanalysis of a new ultra lightweight RFID authentication protocol - SASI. IEEE Transactions on Dependable and Secure Computing 6(4), 316-320 (2009)
28. Rizomiliotis, P., Rekleitis, E., Gritzalis, S,: Security analysis of the Song-Mitchell authentication protocol for low-cost RFID tags. Comm. Letters. 13, 4 (April 2009), 274-276 (2009)
29. Song, B., Mitchell, C.J.: RFID authentication protocol for low-cost tags. In: Proc. of Wisec 2008, pp. 140-147 (2008)

30. Tsudik, G.: YA-TRAP: Yet another trivial RFID authentication protocol. In: Proceedings of International Conference on Pervasive Computing and Communications - PerCom 2006, pp. 640-643. IEEE Computer Society Press, Los Alamitos (2006)
31. van Deursen, T., Mauw, S., Radomirović, S.: Untraceability of RFID protocols. In: J.A. Onieva et al. (Eds.): WISTP 2008. LNCS, vol. 5019, pp. 1-15. Springer, Heidelberg (2008)
32. van Deursen, T., Mauw, S., Radomirović, S., Vullers, P.: Secure ownership and ownership transfer in RFID Systems. In: M. Backes and P. Ning (Eds.): ESORICS 2009. LNCS, vol. 5789, pp. 637-654. Springer, Heidelberg (2009)
33. van Deursen, T., Radomirović, S.: On a new formal proof model for RFID location privacy. Information Processing Letters, 110 (2009) 57-61 (2009)
34. Vaudenay, S.: On privacy models for RFID. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 68-87. Springer, Heidelberg (2007)