Strengthening Class1 Gen2 RFID Tags

Jihoon Cho
Information Security Group
Royal Holloway University of London
Egham Surrey TW20 0EX, United Kingdom
Jihoon.Cho@rhul.ac.uk

***Abstract*—Refresh techniques can greatly enhance security and privacy of Class-1 Generation-2 RFID tags (Gen2 tags), without requiring any cryptographic capabilities from the tags. We propose a refresh-based RFID system and define a notion of privacy for the system. Privacy analysis investigates a novel security property of public-key encryption schemes, which plays the fundamental role to satisfy the defined privacy requirement. While conventional refresh-based solutions only help enhance privacy, the proposed solution also provides the limited authentication.**

***Keywords*-RFID; Privacy; Cloning; Re-encryption**

I. Introduction

Radio Frequency Identification (RFID) is a technology for automated identification of objects or people. An RFID system basically consists of tags and readers. Radio Signal Transponder, commonly known as *tag*, consists of a chip containing identity information and an antenna for wireless data transmission. Such a tag is typically attached to an object and transmits resident data when the tag passes through a radio frequency (RF) field generated by a compatible *reader*.

Supply chain management can deliver significant savings to businesses, and RFID technology has been introduced as a way of achieving supply chain cost savings. The EPCglobal Network [8] is a standards-based approach designed to help realise RFID-enabled supply chain management. EPCglobal[1], which is leading the development of the EPCglobal Network, specifies the physical and logical requirements for the RFID system, in the Class-1 Generation-2 RFID standard (Gen2 standard) [7]. We use a term 'Gen2 tags' to refer to the RFID tags that conform to Gen2 standard. Gen2 tags are expected to predominate the RFID market in few years.

A. Security Issues of Gen2 Tags

RFID technology poses unique privacy and security concerns. That is, the owner of a tag cannot physically control the communications of the tag; because (i) radio communications are non-contact and non-line-of-sight; and (ii) the tag itself typically maintains no history of past readings. The potentially limited computing capabilities of Gen2 tags, however, render security threats more serious, since standard cryptographic primitives are often beyond the capabilities of Gen2 tags; the most inexpensive Gen2 tags will likely have only between 250 to 1,000 gates available for security features [13]. We summarise the security and privacy threats in Gen2 tags as follows:

Inventorying: Unique identifiers resident in Gen2 tags can permit surreptitious *inventorying* for an object or a person carrying the tags. This is because the field 'object class' in EPCs represents a product code. *Data privacy* (or *confidentiality*) is thus required.

Tracking: Unique identifiers of tags also can be used to *track* an object or a person carrying the tags in time and space. The collected information can be merged and linked to create a person's profile, or generate critical information about inbound and outbound flows of corporate warehouse. *Location privacy* (or *anonymity*) is thus required.

Cloning: Since a Gen2 tag promiscuously emits its EPC to any reader query, an adversary can easily learn it by simply scanning the tag. Furthermore, field-programmable Gen2 tags are available today[2] and readers accept the validity of the EPCs at face value. These features make Gen2 tags vulnerable to elementary cloning attack. *Authenticity* for tags is thus required.

Denial of Service: The Denial of Service (DoS) is a great security concern in RFID-enabled supply chains. *Availability* guarantees that an authorised reader can have constant access to tags.

Key Management: Sharing keys across multiple tags is not desirable, since tags are not assumed to be tamper-resistant and compromising a single tag could make vulnerable all the tags that share the keys. If each tag is assigned a different key, then a reader should be able to efficiently determine which key to use.

B. Related Work

Cryptography can be used to enhance tag privacy even when a tag itself cannot perform any cryptographic operations. For example, an RFID tag could store an encrypted

[1] http://www.epcglobalinc.org

[2] See http://www.ti.com/rfid/docs/manuals/pdfSpecs/epc_inlay.pdf.

978-1-4244-5113-5/09/$25.00

version of its unique identifier, where the encryption is performed by external agents with adequate computational resources. Since a static ciphertext still permits physical tracking, the encrypted identifier needs to be *refreshed* regularly, e.g. using a re-encryption process. Universal re-encryptions [1], [6], in particular, have introduced an attractive idea of allowing any device to perform *refreshing*, but they widely opened possibilities of more serious security and privacy threats, e.g. adversarial writings for malicious tracking [12] or a DoS attack by an adversary who writes garbages into tags and thus makes the tags desynchronised with the system.

The kill-passwords normally authenticate a reader to a tag in order to authorise the deactivation of the tag, but the unique kill-password shared between a tag and a reader can instead serve to authenticate the tag to the reader [9]; when the tag receives a kill command with a valid kill-password, but the received power is insufficient, the tag remains operational and emits an error code. Given the ability to cause Gen2 tags to report insufficient power for the kill command, the tag can be modified to emit *yes* or *no* indicating the validity of a kill-password. This approach, however, is vulnerable to simple eavesdropping attack [9].

C. Contribution and Organisation

Refresh techniques can greatly enhance security and privacy of Gen2 tags, without requiring any cryptographic capabilities from the tags. We propose a refresh-based RFID system and define a notion of privacy for the system. The idea of using ElGamal encryption scheme is proposed in [10], but they do not consider the multiple domain environment. The ElGamal-based universal encryption scheme [6] accommodates multiple domains, but they actually do not prove the security of the their proposed scheme. Our privacy analysis investigates a novel security property of public-key encryption schemes, which plays the fundamental role to satisfy the defined privacy requirement. While conventional refresh-based solutions only help enhance privacy, the proposed solution also provides the authentication feature.

The rest of the paper is organised as follows. In section 2, we propose a refresh-based RFID system. We then provide privacy and other security analysis in sections 3 and 4, respectively.

II. Definition of RFID System (RFID-R)

We use the following notational conventions: for variables or values a and b, "$a \leftarrow b$" denotes the assignment of value b to a; "$\mathcal{A} \rightarrow \mathcal{B}$:" indicates a command or data flow from entity $\mathcal{A}$ to entity $\mathcal{B}$; "$\mathcal{A}$:" indicates an operation performed locally by $\mathcal{A}$; "$\mathcal{A} \leftrightarrow \mathcal{B}$:" indicates a protocol execution between $\mathcal{A}$ and $\mathcal{B}$; $\in_{\mathsf{R}}$ indicates a uniform random selection from a finite set.

A. Entities

We introduce a notion of *domain*, which is a logical entity that initiates and identifies tags using its own key material. An RFID-R system then consists of the following entities.

- A *tag*, denoted by $\mathcal{T}$, is a passive transponder and belongs to a specific domain. Its memory is logically separated into ϕ-cell and φ-cell: ϕ-cell is *universally readable* and *keyed writable*, and stores a pseudonym c corresponding to the identifier of $\mathcal{T}$; φ-cell stores a tag-access key *ak* and becomes neither readable nor writable once *ak* has been written into.[3]
- A *reader*, denoted by $\mathcal{R}$, represents a specific domain. It initiates, refreshes, and identifies/verifies a tag $\mathcal{T}$. It consists of one or more transceivers and a back-end server, and transceivers read $\mathcal{T}$ and send the captured data to the back-end server for the further process.

We then define the two protocols which describe the basic communication interface between $\mathcal{R}$ and $\mathcal{T}$.

Protocol: Tag-read

1. $\mathcal{R} \rightarrow \mathcal{T}$: *tag-read* (ϵ)
2. $\mathcal{T} \rightarrow \mathcal{R}$: c

For the *tag-read* query, a tag $\mathcal{T}$ simply returns the pseudonym c stored in ϕ-cell. The *tag-read* query carries no message, denoted by ϵ, but supplies $\mathcal{T}$ with the sufficient power for engaging the subsequent protocols.

Protocol: Tag-write(c', ak)

1. $\mathcal{R} \rightarrow \mathcal{T}$: *tag-write* (c', ak)
2. $\mathcal{T}$: if $ak_{\mathcal{T}} = ak$, then $c \leftarrow c'$
3. $\mathcal{T} \rightarrow \mathcal{R}$: c

The *tag-write* query includes a pseudonym c' along with a tag-access key *ak*. A tag $\mathcal{T}$ replaces a pseudonym c in ϕ-cell with c', only if the received *ak* is equal to $ak_{\mathcal{T}}$ stored in φ-cell.

B. Basic Algorithms

The algorithms of an RFID-R system make use of the message authentication code (MAC) algorithm [11] and the ElGamal encryption scheme PE = (G,K,E,D) [4]; the public-parameter[4] generation algorithm G, the key-generation algorithm K, the encryption algorithm E, and the decryption algorithm D. An RFID-R system then consists of a set of the following polynomial-time algorithms, denoted by **P**.

- SetupReader takes as input a security parameter τ and returns the system parameter $parm$ and a master key $K = (K_{\mathsf{PE}}, K_{\mathsf{MAC}})$, where $K_{\mathsf{PE}} = (pk, sk) \leftarrow \mathsf{K}(\tau)$; it also initialises database D that contains tag-related data; we write $\mathsf{SetupReader}(\tau) \rightarrow \mathcal{R}(parm, K, D)$.

[3]Gen2 tags support rewritable memory and access-control based on access-keys.

[4]It includes a message space $\langle g \rangle = \mathbb{G}$, where $\mathbb{G} \subset \mathbb{Z}_p^*$ and $|\mathbb{G}| = q$.

- InitiateTag is a two-party protocol between $\mathcal{R}$ and $\mathcal{T}$, which takes as input $K_{\mathsf{int}} = (pk, K_{\mathsf{MAC}})$ and database D from $\mathcal{R}$ and a tag identifier $id \in \{0,1\}^{l_1}$ from $\mathcal{T}$; $\mathcal{R}$ initiates $\mathcal{T}$ as follows:
  1. $\mathcal{R}$: $ct \leftarrow 0;\ m \leftarrow id||ct;$ $\tilde{m} \leftarrow \mathsf{MAC}(K_{\mathsf{MAC}}, m);\ M \leftarrow m||\tilde{m};$ $c \leftarrow \mathsf{E}(pk, M); ak \in_{\mathsf{R}} \{0,1\}^{l_2};$ $D \leftarrow D \cup \{(id, ak, ct)\}$
  2. $\mathcal{R} \rightarrow \mathcal{T}$: *tag-initiate*(c, ak)
  3. $\mathcal{T}$: store c in ϕ-cell and ak in φ-cell

  We write $\mathsf{InitiateTag}(\mathcal{R}(K_{\mathsf{int}}, D), \mathcal{T}(id)) \rightarrow \mathcal{T}(c, ak)$.
- IdentifyTag is two-party protocol between $\mathcal{R}$ and $\mathcal{T}$, which takes as input $K_{\mathsf{idt}} = sk$ and D from $\mathcal{R}$ and a ciphertext c from $\mathcal{T}$; $\mathcal{R}$ determines the identifier of $\mathcal{T}$ as follows:
  1. $\mathcal{R} \leftrightarrow \mathcal{T}$: Tag-Read
  2. $\mathcal{R}$: $M = M_{id}||M_{ct}||M_{\mathsf{MAC}} \leftarrow \mathsf{D}(sk, c);$ if $\mathsf{IDLookup}(M_{id}, D) = 1,$ then return M_{id}; else, return $\perp$

  We write $\mathsf{IdentifyTag}(\mathcal{R}(K_{\mathsf{idt}}, D), \mathcal{T}(c)) \rightarrow z$.
- RefreshTag is a two-party protocol between $\mathcal{R}$ and $\mathcal{T}$, which takes as input $K_{\mathsf{ref}} = K_{\mathsf{PE}}$ and D from $\mathcal{R}$, and c and ak from $\mathcal{T}$, where $c = (\alpha, \beta) = (M(pk)^k, g^k)$ for $k \in \mathbb{Z}_q^*$; $\mathcal{R}$ refreshes c in $\mathcal{T}$ as follows:
  1. $\mathcal{R} \leftrightarrow \mathcal{T}$: $\mathsf{IdentifyTag}(\mathcal{R}(sk, D), \mathcal{T}(c))$
  2. $\mathcal{R}$: if $z \neq \perp,$ then $ak \leftarrow \mathsf{KeyLookup}(z, D);$ $k' \in_{\mathsf{R}} \mathbb{Z}_q^*;$ $c' = (\alpha', \beta') \leftarrow (\alpha(pk)^{k'}, \beta g^{k'})$
  3. $\mathcal{R} \leftrightarrow \mathcal{T}$: $\mathsf{Tag\text{-}write}(c', ak)$

  We write $\mathsf{RefreshTag}(\mathcal{R}(K_{\mathsf{ref}}, D), \mathcal{T}(c, ak)) \rightarrow \mathcal{T}(c, ak)$.

Given id and D, we define the following algorithms: $\mathsf{IDLookup}(id, D)$ returns "1" if D contains a tag identifier *id* or "0" otherwise; $\mathsf{KeyLookup}(id, D)$ returns the corresponding tag-access key *ak*; $\mathsf{CntLookup}(id, D)$ returns the current count ct. Due to the homomorphic property of ElGamal encryption scheme, we formally define an RFID-R system as follows.

Definition 1 *An RFID-R system consists of a tuple* $(\mathcal{T}, \mathcal{R}, \boldsymbol{P})$*, as defined above, satisfying the following viability condition, i.e. for the following experiment and for any* $n \in \mathbb{N}$*:*

$\mathcal{R}(parm, K, D) \leftarrow$ *SetupReader*(τ)*;*
$id \in_R \{0,1\}^{l_1}$;
$\mathcal{T}(c_0, ak) \leftarrow$ *InitiateTag*$(\mathcal{R}(K_{int}, D), \mathcal{T}(id))$;
For $i = 0, \ldots, n-1$ *do*
  $\mathcal{T}(c_{i+1}, ak) \leftarrow$ *RefreshTag*$(\mathcal{R}(K_{ref}, D), \mathcal{T}(c_i, ak))$
EndFor;

we have $Pr[$*IdentifyTag*$(\mathcal{R}(K_{idt}, D), \mathcal{T}(c_n)) = id] = 1$.

Protocol: Tag-Auth$(\mathcal{R}(K, D), \mathcal{T}(c, ak))$

1. $\mathcal{R} \leftrightarrow \mathcal{T}$: Tag-Read
2. $\mathcal{R}$: $M = M_{id}||M_{ct}||M_{\mathsf{MAC}} \leftarrow \mathsf{D}(sk, c);$
3. if $\mathsf{IDLookup}(M_{id}, D) = 0,$
4. then output $\perp$ and halt;
5. else, $ct \leftarrow \mathsf{CntLookup}(M_{id}, D);$
6. $M'_{\mathsf{MAC}} \leftarrow \mathsf{MAC}(K_{\mathsf{MAC}}, M_{id}||M_{ct});$
7. if $M_{ct} \neq ct$ or $M_{\mathsf{MAC}} \neq M'_{\mathsf{MAC}},$
8. then output "*invalid*";
9. else, $ct \leftarrow ct + 1; m \leftarrow id\,||\,ct;$
10. $\tilde{m} \leftarrow \mathsf{MAC}(K_{\mathsf{MAC}}, m);$
11. $M \leftarrow m||\tilde{m};\ c' \leftarrow \mathsf{E}(pk, M);$
12. $ak \leftarrow \mathsf{KeyLookup}(M_{id}, D);$
13. $(p, \{ak^{(\omega)}\}_{\omega=1}^{q}) \leftarrow \mathsf{GenKeySet}(q, ak);$
14. $\lambda \leftarrow$ "*valid*";
    for $k = 1$ to q do
15. $\mathcal{R} \leftrightarrow \mathcal{T}$: Tag-Write $(c', ak^{(k)})$
16. $\mathcal{R}$: if $c = c'$ and $k \neq p,$
17. then $\lambda \leftarrow$ "*invalid*"
18. if $c \neq c'$ and $k = p,$
19. then $\lambda \leftarrow$ "*invalid*"
20. $\mathcal{R}$: output λ;
21. if $\lambda =$ "*valid*",
22. then $D \leftarrow \mathsf{CntUpdate}(M_{id}, ct, D)$

Figure 1. Authentication protocol

C. Adding Authentication

We propose to use a tag-access key as a mechanism not only for writing access control but also for authentication, i.e. $\mathcal{R}$ can authenticate $\mathcal{T}$ by simply checking if $\mathcal{T}$ is written using its corresponding access key *ak*.

An error message $\perp$ denotes that $\mathcal{T}$ does not belong to the domain (line 4). Spurious tag-access keys are used to prevent a round-about attack, where illegitimate tags always send back the updated ciphertext c'. $\mathsf{GenKeySet}(q, ak)$ randomly generates a set of q spurious access keys, and replace $ak^{(p)}$ for $p \in_{\mathsf{R}} \{1, 2, \ldots, q\}$ with a true access key *ak* (line 13). The output "*invalid*" or "*valid*" indicates that $\mathcal{T}$ is counterfeit or legitimate, respectively. For the efficiency, the computation of c' (line 9–11) and the generation of spurious keys (line 13) can be performed in advance.

III. Privacy Analysis

A. Definition of Privacy

In order to define the notion of privacy in RFID systems, we must construct a formal model that characterises the capabilities of a potential adversary. In cryptography, such a model takes a form of an *experiment* (or an *attack game*), which specifies the actions that a potential adversary can perform (i.e. the *oracles* an adversary can query), the goal of the attack (i.e. the *game* the adversary plays), and the way

in which the adversary interact with system components (i.e. the *rules* of the game).

In most cryptographic security models, an adversary is assumed to have more-or-less unfettered access to system components. Such an access, however, will be a sporadic event in most RFID systems, e.g. in order to scan a tag, an adversary must have physical proximity to the tag. Moreover, because Gen2 tags cannot perform standard cryptographic functions, they cannot provide a meaningful level of security against too strong an adversary. We thus need to formulate a weakened security model which accurately reflects real-world threats and tag capabilities.

We roughly define the privacy of an RFID-R system as follows: An RFID-R system is said to provide privacy if the adversary cannot link a tag between two reads whenever the tag has been refreshed outside the eavesdropping range of the adversary. The proposed notion of privacy is designed to capture *location privacy* and *data privacy*.

We assume that tags have an identical *radio finger print*; for example, all the tags must use the same frequency for communication. Avoine and Oechslin [2] point out multi-layer privacy issues; if a tag has a distinct radio fingerprint (e.g. due to its use of a different underlying standard at the communication/physical layer), then the best cryptographic privacy-preserving identification protocol running at the application layer may be of no use.

1) Adversarial capability: An adversary $\mathcal{A}$ is a probabilistic polynomial-time (PPT) algorithm, which can make the following types of oracle queries.

- $\texttt{RevIdt}(\mathcal{T})$: which returns the identifier *id* of $\mathcal{T}$.
- $\texttt{RevPdn}(\mathcal{T})$: which returns the current pseudonym c resident in $\mathcal{T}$.
- $\texttt{RefTag}(\mathcal{T})$: which refreshes the pseudonym resident c in $\mathcal{T}$ into c', and returns a pair (c, c').

A RevPdn query reflects the greatest privacy threat in RFID systems, i.e. $\mathcal{A}$ can obtain the data resident in $\mathcal{T}$ by either eavesdropping tag-reader communication or querying $\mathcal{T}$ without the tag owner's permission. A RevIdt query, however, reflects the special event that $\mathcal{A}$ could obtain a tag identifier id from the tag itself or an object the tag is attached. In the RFID-enabled banknote scheme [10], for example, a tag identifier (serial number) is written in a banknote. A RefTag query reflects the adversarial capability which eavesdrops the communications when tags are refreshed.

2) Privacy experiment: Assuming that the define RFID system is used across multiple domains, which is a likely case in reality, we define the *privacy experiment* for $n \in \mathbb{N}$ and $b \in \{0, 1\}$. We define $\mathsf{SetupReaders}(1^n, m)$ to run $\mathsf{SetupReader}(1^n)$ m times.

Experiment $\mathbf{Exp}^{\text{privacy}}_{\mathcal{A},\mathsf{RFID\text{-}R}}(n, b)$

Setup: $\{\mathcal{R}_j(parm, K, D)\}_{j=1}^{m} \leftarrow \mathsf{SetupReaders}(1^n, m)$

Select: For $i = 0$ and 1,
$\mathcal{R}_i(K, D) \in_{\mathsf{R}} \{\mathcal{R}_j(K, D)\}_{j=1}^{m}$;
$id_i \in_{\mathsf{R}} \{0, 1\}^b$;
$\mathcal{T}_i(c, ak) \leftarrow \mathsf{InitiateTag}(\mathcal{R}_i(K_{\mathsf{int}}, D), \mathcal{T}_i(id_i))$

Learn: $(state, \mathcal{T}_0, \mathcal{T}_1) \leftarrow \mathcal{A}^{\mathcal{O}(\mathcal{T}_0, \mathcal{T}_1)}$

Guess: $\mathcal{T}_b(c', ak) \leftarrow \mathsf{RefreshTag}(\mathcal{R}_b(K_{\mathsf{ref}}, D), \mathcal{T}_b(c, ak))$;
$d \leftarrow \mathcal{A}(state, c')$; return d

In the 'Setup' stage, we take as input a security parameter 1^n and setups m domain readers by running the algorithm $\mathsf{SetupReaders}(1^n, m)$.

In the 'Select' stage, we first selects two readers, $\mathcal{R}_0$ and $\mathcal{R}_1$, uniformly at random. We allow either two different readers to be selected or the same reader to be selected twice. The experiment then consider the case that a single key pair is used in the system (as in the RFID-enabled banknote system [10]), as well as the case that multiple key pairs are used (as in [1], [6]). We then let two readers, $\mathcal{R}_0$ and $\mathcal{R}_1$, initiate two tags, $\mathcal{T}_0$ and $\mathcal{T}_1$, respectively.

In the 'Learn' stage, $\mathcal{A}$ makes all the permitted queries to $\mathcal{T}_0$ and $\mathcal{T}_1$, denoted by $\mathcal{O}(\mathcal{T}_0, \mathcal{T}_1)$, and returns the two tags along with *state*, which is the summary of computations or logics concerning the two tags.

In the 'Guess' stage, one of the two tags, denoted by $\mathcal{T}_b$, is refreshed. Given *state* and a pseudonym c' in $\mathcal{T}_b$, $\mathcal{A}$ outputs a guess $d \in \{0, 1\}$, which implies that c' belongs to the tag $\mathcal{T}_d$. The experiment finally outputs d.

3) Defining privacy: We define privacy to require that every adversary *behaves the same way* whether it sees c' refreshed from the pseudonym in a tag $\mathcal{T}_0$ or it sees c' refreshed from the pseudonym in a tag $\mathcal{T}_1$. Since the adversary $\mathcal{A}$ outputs a single bit, "behaving the same way" means that it outputs "1" with almost the same probability in each case. For the experiment defined above, the advantage of $\mathcal{A}$, $\mathbf{Adv}^{\text{privacy}}_{\mathcal{A},\mathsf{RFID\text{-}R}}(n)$, then can be defined as

$$\left|\Pr\left[\mathbf{Exp}^{\text{privacy}}_{\mathcal{A},\mathsf{RFID\text{-}R}}(n, 1) = 1\right] - \Pr\left[\mathbf{Exp}^{\text{privacy}}_{\mathcal{A},\mathsf{RFID\text{-}R}}(n, 0) = 1\right]\right|.$$

The following definition then states that the adversary $\mathcal{A}$ cannot determine whether it is running the experiment $\mathbf{Exp}^{\text{privacy}}_{\mathsf{RFID\text{-}R},\mathcal{A}}(n, 0)$ or the experiment $\mathbf{Exp}^{\text{privacy}}_{\mathcal{A},\mathsf{RFID\text{-}R}}(n, 1)$.

Definition 2 *An RFID-R system is said to provide privacy if the function* $\mathbf{Adv}^{\text{privacy}}_{\mathcal{A},\mathsf{RFID\text{-}R}}$ *is negligible.*

B. Privacy Analysis for RFID-R System

Semantic security is not sufficient to guarantee meaningful security when multiple key pairs are used within the system, since an adversary could exploit the use of different public keys to break semantic security. We thus introduce a novel security notion, namely *universal semantic security* (USS). Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme and $\mathcal{A}$ be an adversary. We consider the following

experiment for a security parameter $n \in \mathbb{N}$ and a fixed single bit $b \in \{0,1\}$.

Experiment $\mathbf{Exp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n,b)$

1) $\mathsf{Gen}(1^n)$ is run to obtain two pairs (pk_0, sk_0) and (pk_1, sk_1).
2) $\mathcal{A}$ is given (pk_0, pk_1) as well as oracle access to $\mathsf{Enc}(pk_0, \cdot)$ and $\mathsf{Enc}(pk_1, \cdot)$. $\mathcal{A}$ outputs a pair of messages (m_0, m_1) of the same length, where these messages must be in the plaintext space associated with (pk_0, pk_1).
3) A ciphertext $c \leftarrow \mathsf{Enc}(pk_b, m_b)$ is given to $\mathcal{A}$.
4) $\mathcal{A}$ continues to have access to $\mathsf{Enc}(pk_0, \cdot)$ and $\mathsf{Enc}(pk_1, \cdot)$, and outputs a bit b'.
5) The output of the experiment is b'.

We then define the advantage of $\mathcal{A}$, $\mathbf{Adv}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n)$, as

$$\left|\Pr\left[\mathbf{Exp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n,1)=1\right] - \Pr\left[\mathbf{Exp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n,0)=1\right]\right|.$$

We now formally define the *universal semantic security*.

Definition 3 *A public-key encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *has universal semantic security* (*or has USS property*) *if the function* $\mathbf{Adv}^{uss}_{\mathcal{A},\Pi}$ *is negligible for all probabilistic polynomial-time adversary* $\mathcal{A}$.

The above security property involves the traditional two security properties; *semantic security* (or *indistinguishability of encryptions under chosen-plaintext attack* (IE-CPA)) [5] and *key privacy* (or *indistinguishability of keys under chosen plaintext attack* (IK-CPA)) [3]. Semantic security requires that an adversary should not gain advantage or information from having seen the ciphertext output by the encryption algorithm. On the other hand, key privacy requires that an adversary should not make use of differences in public keys to defeat the semantic security of an encryption scheme.
The following lemma provides an essential property to prove the privacy of the proposed RFID-R system.

Lemma 1 *If a public-key encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *satisfies both IE-CPA and IK-CPA, then the public-key encryption scheme* Π *has USS property.*

Proof. We first construct a hybrid experiment which effectively interpolates between the experiments for IE-CPA security and IK-CPA security, by the standard hybrid argument. For $b \in \{0,1\}$ and $\tau \in \mathbb{N}$, we define the following experiment.

Experiment $\mathbf{HybExp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n,b)$

1) $\mathsf{Gen}(1^n)$ is run to obtain two pairs (pk_0, sk_0) and (pk_1, sk_1).
2) $\mathcal{A}$ is given (pk_0, pk_1) as well as oracle access to $\mathsf{Enc}(pk_0, \cdot)$ and $\mathsf{Enc}(pk_1, \cdot)$. $\mathcal{A}$ outputs a pair of messages (m_0, m_1), where the message must be in the plaintext space associated with (pk_0, pk_1).
3) A ciphertext $c \leftarrow \mathsf{Enc}(pk_{1-b}, m_b)$ is given to $\mathcal{A}$.
4) $\mathcal{A}$ continues to have access to $\mathsf{Enc}(pk_0, \cdot)$ and $\mathsf{Enc}(pk_1, \cdot)$, and outputs a bit b'.

We then have the following result.

$$\begin{aligned}
&\mathbf{Adv}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n)\\
&= \left|\Pr\left[\mathbf{Exp}^{uss}_{\mathcal{A},\Pi}\ (\tau,1)=1\right] - \Pr\left[\mathbf{Exp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(\tau,0)=1\right]\right|\\
&= \left|\Pr\left[\mathbf{Exp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n,1)=1\right] - \Pr\left[\mathbf{HybExp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n,1)=1\right]\right.\\
&+\ \left.\Pr\left[\mathbf{HybExp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n,1)=1\right] - \Pr\left[\mathbf{Exp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n,0)=1\right]\right|\\
&\le \left|\Pr\left[\mathbf{Exp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n,1)=1\right] - \Pr\left[\mathbf{HybExp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n,1)=1\right]\right|\\
&+\ \left|\Pr\left[\mathbf{HybExp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n,1)=1\right] - \Pr\left[\mathbf{Exp}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n,0)=1\right]\right| \quad (*)
\end{aligned}$$

We now considering the following experiment for $b \in \{0,1\}$ and $n \in \mathbb{N}$:

Experiment $\mathbf{Exp}^{\mathsf{ie\text{-}cpa}}_{\mathcal{A},\Pi}(n,b)$	Experiment $\mathbf{Exp}^{\mathsf{ik\text{-}cpa}}_{\mathcal{A},\Pi}(n,b)$
$pk_0 \leftarrow \mathsf{Gen}(1^n)$;	$(pk_0, pk_1) \leftarrow \mathsf{Gen}(1^n)$;
$(m_0, m_1) \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(pk_0)$;	$m_1 \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(pk_0, pk_1)$;
$c \leftarrow \mathsf{Enc}(m_b, pk_0)$;	$c \leftarrow \mathsf{Enc}(m_1, pk_b)$;
$b' \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(c)$; return b'	$b' \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}(c)$; return b'

$\mathcal{A}^{\mathcal{O}(\cdot)}$ denotes that $\mathcal{A}$ is given an permitted oracle access, i.e. $\mathcal{O}(\cdot)$ denotes $\mathsf{Enc}(pk_0, \cdot)$ in $\mathbf{Exp}^{\mathsf{ie\text{-}cpa}}_{\mathcal{A},\Pi}$ and $\mathcal{O}(\cdot)$ denotes $\mathsf{Enc}(pk_0, \cdot)$ and $\mathsf{Enc}(pk_1, \cdot)$ in $\mathbf{Exp}^{\mathsf{ik\text{-}cpa}}_{\mathcal{A},\Pi}$ We then have the following result.

$$\begin{aligned}
(*) &= \left|\Pr\left[\mathbf{Exp}^{\mathsf{ik\text{-}cpa}}_{\mathcal{A},\Pi}(n,1)=1\right] - \Pr\left[\mathbf{Exp}^{\mathsf{ik\text{-}cpa}}_{\mathcal{A},\Pi}(n,0)=1\right]\right|\\
&+\ \left|\Pr\left[\mathbf{Exp}^{\mathsf{ie\text{-}cpa}}_{\mathcal{A},\Pi}(n,1)=1\right] - \Pr\left[\mathbf{Exp}^{\mathsf{ie\text{-}cpa}}_{\mathcal{A},\Pi}(n,0)=1\right]\right|\\
&= \mathbf{Adv}^{\mathsf{ik\text{-}cpa}}_{\mathcal{A},\Pi}(n)\ +\ \mathbf{Adv}^{\mathsf{ie\text{-}cpa}}_{\mathcal{A},\Pi}(n).
\end{aligned}$$

Since the sum of two negligible functions is negligible, $\mathbf{Adv}^{\mathsf{uss}}_{\mathcal{A},\Pi}(n)$ is negligible. This completes the proof. □.

Lemma 2 *ElGamal encryption scheme* $\mathsf{PE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is USS secure under DDH assumption.*

Proof. ElGamal encryption scheme satisfies both IE-CPA and IK-CPA under the DDH assumption, as proved in [3], [14]. By Lemma 1, the PE scheme is USS secure under the DDH assumption. □

Theorem 1 *An RFID-R system satisfies privacy under the DDH assumption.*

Proof. By Lemma 2, we are left to prove that privacy of an RFID-R system can be reduced to either USS property or IE-CPA property of the PE scheme. This is because we have two cases in 'Select' stage in the experiment $\mathbf{Exp}^{\text{privacy}}_{\mathcal{A},\mathsf{RFID\text{-}R}}$; either two different readers are selected (Case I), or; the same reader is selected twice (Case II).

Case I. *We have two distinct readers* $\mathcal{R}_0$ *and* $\mathcal{R}_1$.

We show that, assuming the existence of an adversary $\mathcal{A}$ which breaks privacy of the RFID-R system, we construct another adversary $\mathcal{B}$ which breaks USS property of the PE scheme. More specifically, suppose that we have an adversary $\mathcal{A}$ whose advantage $\mathbf{Adv}^{\text{privacy}}_{\mathcal{A},\mathsf{RFID\text{-}R}}$ for the experiment $\mathbf{Exp}^{\text{privacy}}_{\mathcal{A},\mathsf{RFID\text{-}R}}$ is non-negligible. By constructing an adversary $\mathcal{B}$ which engages in the experiment $\mathbf{Exp}^{\mathsf{uss}}_{\mathcal{B},\mathsf{PE}}$ using $\mathcal{A}$ as a subroutine, we show that $\mathcal{B}$ can guess a correct a bit b with non-negligible advantage.

$\mathcal{B}$ runs the experiment $\mathbf{Exp}^{\mathsf{uss}}_{\mathcal{B},\mathsf{PE}}$, simulating $\mathbf{Exp}^{\text{privacy}}_{\mathcal{A},\mathsf{RFID\text{-}R}}$ for $\mathcal{A}$ as follows.

1. $\mathsf{Gen}(1^n)$ is run to obtain two pairs (pk_0, sk_0) and (pk_1, sk_1).
2. When given (pk_0, pk_1), $\mathcal{B}$ then simulates $\mathbf{Exp}^{\text{privacy}}_{\mathcal{A},\mathsf{RFID\text{-}R}}$ for $\mathcal{A}$:
   - $\mathcal{B}$ simulates 'Setup' stage by running $\mathsf{SetupReaders}(1^n, m)$.
   - $\mathcal{B}$ simulates 'Select' stage by choosing $id_i \in_{\mathsf{R}} \{0,1\}^b$ $(i = 0, 1)$ and also randomly selecting two readers $\mathcal{R}_0$ and $\mathcal{R}_1$, but replacing the public/secret key pairs, i.e. K_{PE} of $\mathcal{R}_i$, with $(pk_i, \perp)$ for $i = 0, 1$.

2′. $\mathcal{B}$ outputs a pair of messages (m_0, m_1) of the same length, where $m_i = \mathsf{Encode\text{-}to\text{-}Group}(K_{\mathsf{MAC}}, id_i, ct)$ for $i = 0, 1$. $\mathcal{B}$ sends oracle queries $\mathsf{Enc}(pk_i, m_i)$ and receives c_i for $i = 0, 1$.
   - $\mathcal{B}$ continues to simulate 'Select' stage by initiating two tags $\mathcal{T}_i(c_i, ak)$ for $i = 0, 1$.
   - $\mathcal{B}$ simulates 'Learn' stage as follows, where $i = 0, 1$:
     - For $\mathtt{RevIdt}(\mathcal{T}_i)$ query, $\mathcal{B}$ returns id_i.
     - For $\mathtt{RevPdn}(\mathcal{T}_i)$ query, $\mathcal{B}$ returns c_i currently resident in $\mathcal{T}_i$.
     - For $\mathtt{RefTag}(\mathcal{T}_i)$ query, $\mathcal{B}$ (i) sends an oracle query $\mathsf{Enc}(pk_i, m_i)$ and receives c_i', (ii) updates c_i currently resident in $\mathcal{T}_i$ with c_i', and (iii) finally returns (c_i, c_i').
3. Given a ciphertext $c \leftarrow \mathsf{Enc}(pk_b, m_b)$, $\mathcal{B}$ simulates 'Guess' stage:
   - $\mathcal{B}$ sends c to $\mathcal{A}$, and receives a guess bit d.
4. $\mathcal{B}$ outputs a bit d.

It is true that the advantage $\mathbf{Adv}^{\mathsf{uss}}_{\mathcal{B},\mathsf{PE}}$ for the experiment $\mathbf{Exp}^{\mathsf{uss}}_{\mathcal{B},\mathsf{PE}}$ is non-negligible.

Case II. *Two readers $\mathcal{R}_0$ and $\mathcal{R}_1$ are the same.*

We show that, assuming the existence of an adversary $\mathcal{A}$ which breaks privacy of the RFID-R system, we construct another adversary $\mathcal{B}$ which breaks USS property of the PE scheme. The detailed proof is similar to Case I. □

IV. Other Security Analysis

A. Tag Authenticity

Precisely, the Tag-Auth protocol cannot exclude cloning attacks, but only can detect that such attacks have been attempted. The proposed protocol, however, provides a strong cloning-free mechanism to inexpensive tags, in which any standard *challenge-response* authentication protocols are beyond their functionalities.

Suppose that an adversary attempts to counterfeit a tag $\mathcal{T}$. The adversary can obtain the pseudonym c and tag-access key ak of $\mathcal{T}$, e.g. by eavesdropping on the TagRefresh protocol, and counterfeits a tag $\mathcal{T}^*$ by writing c and ak into an empty tag. Once $\mathcal{T}$ engages in the Tag-Auth protocol, however, $\mathcal{T}^*$ is de-synchronised with $\mathcal{R}$ due to the use of ct; the pseudonym c' is an encryption on $\big(id||ct''||\mathsf{Mac}(K_{\mathsf{MAC}}, id||ct'')\big)$, where ct'' is an incremented counter. When $\mathcal{R}$ authenticates $\mathcal{T}^*$ via the Tag-Auth protocol, the counter embedded in the pseudonym in $\mathcal{T}^*$ is now less than the one in $\mathcal{T}$ (line 7). Without knowledge of K_{MAC}, the adversary cannot construct the updated pseudonym with the incremented ct when a secure MAC algorithm is used. It is, of course, possible that $\mathcal{T}$ becomes de-synchronised when $\mathcal{T}^*$ runs the Tag-Auth protocol with $\mathcal{R}$ earlier than $\mathcal{T}$. In this case, $\mathcal{T}$ will be determined as a cloned tag. Whenever the Tag-Auth protocol outputs "*invalid*", we thus can classify the identifier of the tag as *tainted*.

For a large value of q, the protocol can be time-consuming, but small values, even $q = 2$, would suffice to detect casual introduction of cloned tags. Counterfeit medicines, for example, would be distributed in boxes, and the detection of a single counterfeit tag among several such tags would be sufficient.

The Tag-Auth protocol also refreshes the pseudonyms in tags, but the refreshed pseudonyms are the encryption on an updated counter. The Tag-Auth protocol, however, still preserves the *viability* condition when used in place of the RefreshTag algorithm, since the identifers in the refreshed pseudonyms do not change.

B. Availability and Efficient Key Management

RFID systems can be easily disturbed by frequency jamming like all wireless devices, but this is not an issue specific to RFID systems. By implementing the access-control on tag writings, the proposed system resists against malicious writings or DoS attacks introduced in universal re-encryption schemes [1], [6]. This approach, however, requires efficient key management for such access keys. The current standard [7] takes an apparent approach to this; a tag sends an index, i.e. EPC, into a table of passwords shared with a reader. This globally identifiable static identity, however, leads to violate a location privacy (and even a data privacy). The proposed system efficiently finds tag-access keys by simply decrypting pseudonyms and recovering the corresponding keys using the KeyLookup algorithm.

V. Conclusion

An RFID-R system cannot provide privacy and authenticity against a strong adversary who is capable of eavesdropping on all communications between tags and readers. Such events, however, will be sporadic in most RFID systems. Moreover, because low-cost Gen2 tags cannot perform standard cryptographic functions, they cannot provide a meaningful level of security against too strong an adversary. Our proposed work provides the pragmatic approach of working within Gen2 tags to achieve practical security goals.

References

[1] G. Ateniese, J. Camenisch, and B. Medeiros. Untraceable RFID tags via insubvertible encryption. In V. Atluri, C. Meadows, and A. Juels, editors, *Proceedings of the 12th ACM Conference on Computer and Communications Security* (CCS 2005), pages 92–101. ACM, 2005.

[2] G. Avoine and P. Oechslin. RFID traceability: A multilayer problem. In A. S. Patrick and M. Yung, editors, *Financial Cryptography 2005*, volume 3570 of *LNCS*, pages 125–140. Springer, 2005.

[3] M. Bellare, A. Boldyreva, A. Desai, and D. Pointcheval. Key-privacy in public-key encryption. In C. Boyd, editor, *Proceedings of Advances in Cryptology — ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 566–582. Springer, 2001.

[4] T. E. Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[5] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[6] P. Golle, M. Jakobsson, A. Juels, and P. F. Syverson. Universal re-encryption for mixnets. In T. Okamoto, editor, *Proceedings of Topics in Cryptology — CT-RSA 2004*, volume 2964 of *LNCS*, pages 163–178. Springer, 2004.

[7] EPCglobal Inc. Specification for RFID air interface. Available at http://www.epcglobalinc.org/standards/uhfc1g2/uhfc1g2_1_1_0-standard-20071017.pdf, December 2005.

[8] EPCglobal Inc. The EPCglobal architecture framework. Available at http://www.epcglobalinc.org/standards/architecture/architecture_1_2-framework-20070910.pdf, September 2007.

[9] A. Juels. Strengthening EPC tags against cloning. In M. Jakobsson and R. Poovendran, editors, *Proceedings of the ACM Workshop on Wireless Security* (WiSe 2005), pages 67–76. ACM, 2005.

[10] A. Juels and R. Pappu. Squealing Euros: Privacy protection in RFID-enabled banknotes. In R. N. Wright, editor, *Financial Cryptography 2003*, volume 2742 of *LNCS*, pages 103–121. Springer, 2003.

[11] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 2001. Available at http://www.cacr.math.uwaterloo.ca/hac/.

[12] J. Saito, J. Ryou, and K. Sakurai. Enhancing privacy of universal re-encryption scheme for RFID tags. In L. T. Yang, M. Guo, G. R. Gao, and N. K. Jha, editors, *Proceedings of International Conference on Embedded and Ubiquitous Computing* (*EUC 2004*), volume 3207 of *LNCS*, pages 879–890. Springer, 2004.

[13] S. E. Sarma, S. A. Weis, and D. W. Engels. Radio Frequency Identification: Security risks and challenges. *CryptoBytes*, 6(1):2–9, 2003.

[14] Y. Tsiounis and M. Yung. On the security of ElGamal based encryption. In H. Imai and Y. Zheng, editors, *Proceedings of First International Workshop on Practice and Theory in Public Key Cryptography* (PKC 1998), volume 1431 of *LNCS*, pages 117–134. Springer, 1998.