**Marquette University**

**e-Publications@Marquette**

***Mathematics, Statistical and Computer Sciences Faculty Research and Publications/College of Arts and Sciences***

***This paper is NOT THE PUBLISHED VERSION;* but the author’s final, peer-reviewed manuscript.** The published version may be accessed by following the link in th citation below.

*2011 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, (March 21-25, 2011): 102-110. [DOI](https://doi.org/10.1109/PERCOM.2011.5767573). This article is © IEEE and permission has been granted for this version to appear in [e-Publications@Marquette](http://epublications.marquette.edu/). IEEE does not grant permission for this article to be further copied/distributed or hosted elsewhere without the express permission from IEEE.

AnonPri: An Efficient Anonymous Private Authentication Protocol

Md. Endadul Hoque

Department of Mathematics, Statistics, and Computer Science, Marquette University, Milwaukee, WI

Farzana Rahman

Department of Mathematics, Statistics, and Computer Science, Marquette University, Milwaukee, WI

Sheikh Iqbal Ahamed

Department of Mathematics, Statistics, and Computer Science, Marquette University, Milwaukee, WI

# Abstract:

Privacy protection is a very important issue during authentications in RFID systems. In order to achieve high-speed authentication in large-scale RFID systems, researchers propose tree-based approaches, in which any pair of tags share a number of key components. Another technique can be to perform group based private authentication that improves the tradeoff between scalability and privacy by dividing the tags into a number of groups. This is a novel authentication scheme that ensures privacy of the provers. However, one limitation of this technique is that the level of privacy provided by the scheme decreases as more and more tags are compromised Therefore, in this paper, we propose a group based anonymous private authentication protocol (AnonPri) that provides higher level of privacy than the above mention group based scheme and achieves better efficiency than the approaches that prompt the reader to perform an exhaustive search. Our protocol provides unlinkability and thereby preserves privacy. The adversary cannot link the responses with the tags, even if she can learn the identifier that the tags are using to produce the response. To evaluate AnonPri, we have compared both the protocols, AnonPri and the group based authentication. The experiment results establish that the level of privacy provided by AnonPri is higher than that of the group based authentication.

# **SECTION I.** Introduction

RFID systems have been studied actively and frequently in pervasive computing environments for last few years. The inherent capability of precise and reliable identification attracts RFID systems in the area of tracking applications. This potentiality, however, can put individual privacy at a risk. A threat to consumer privacy is one of the major obstacles in the widespread deployment of RFID systems. A field trial of RFID embedded loyalty cards in Europe was cancelled due to consumer protest over privacy concerns.1 Strong authentication can be a solution to the privacy problem. One party *(prover)* has to prove its own identity to another party *(verifier)* in such way that an adversary can neither identify nor track the party (prover). In this paper we will consider only one way authentication where the tag has to authenticate itself to the backend server via the reader. Here the tag is the prover and the reader is the verifier. To address the privacy problem, the tag has to obfuscate its identity from eavesdroppers in such a way that only the valid reader can understand and identify the tag. Encrypting the tag's message can protect its privacy. However, this technique cannot provide any hint to the reader about the key that the tag is using to encrypt its message. Therefore the reader has to search among a set of candidate keys until it finds the right key that correctly decrypts the tag's message. As a result, the reader becomes inefficient in terms of identifying a single tag since it has to search a number of keys. This problem is exacerbated when the number of tags in the system increases.

Several private authentication schemes proposed in2,3,4 provide strong privacy at the cost of the search complexity on the reader's side. Under these protocols, the workload of the reader increases linearly with the number of tags in the system. In other words, the search complexity is , where  is the total number of tags in the system. These approaches become infeasible in some applications, such as tracking each product at every stage of supply chain management or automated display of flight information on smart tickets, where there is a huge of number of tags in the system. Molnar and Wagner5 first proposed a tree based hash protocol for RFID systems to reduce the search complexity of the reader from  to , where α is the branching factor at each level of the tree. The tag has to always perform  encryptions for every authentication. However, for authenticating a single tag, the worst case complexity of the reader is reduced to α logα N. But this approach achieves better scalability at the cost of some privacy loss of the tags.6 Despite the privacy loss, this protocol has been held in great consideration by the RFID community because this is the first private authentication protocol that reduces the complexity of the reader. In fact, this is the only protocol so far that can be practically deployed in large scale applications. Therefore, improving the tradeoff between scalability and privacy of RFID systems has a great significance in reality. In,7 the authors proposed a modified version of the tree based scheme where the branching factors are different at the different levels of the tree. This approach improves privacy protection. The authors also propose an algorithm to determine the optimal key tree for a given number of tags. Later Avoine et al.8 proposed a group based private authentication scheme that improves the tradeoff between scalability and privacy by dividing the tags into a number of groups. A benefit of this approach is that the tag has to perform only two encryptions for every authentication. In addition, this approach provides significant improvement in privacy protection. A serious limitation of this protocol is that whenever any tag is compromised (the group key and the tag's key become known to the adversary), all other tags of the same group lose their complete privacy. The level of privacy provided by the scheme decreases as more and more tags are compromised.

## A. Our Contributions

* In this paper, we provide a new insight on the privacy issue of RFID systems. We use an experiment based definition to formalize RFID privacy from the perspective of unlinkability among different RFID tags. Our idea is to preserve privacy by introducing the notion that adversary cannot break unlinkability or invade privacy with probability better than random guessing.
* We present a group based anonymous private authentication protocol (AnonPri) as a solution to the tradeoff between the scalability and privacy problem of RFID systems. AnonPri provides higher level of privacy than the above mentioned group based scheme and achieves better efficiency than the approaches that prompt the reader to perform an exhaustive search.

Based on the notion of RFID privacy, we prove that AnonPri protects privacy of RFID tags and thereby the privacy of tag holders. We also prove that AnonPri provide unlinkability and thereby preserves privacy. The adversary cannot link the tag responses, even if she can decrypt the first portion of the response and learn the identifier that the tags are using to produce the response.

The rest of the paper is organized as follows. Section II reviews important privacy protection approaches proposed so far in RFID systems. In Section III we discuss the details of our system model. We present the AnonPri protocol in Section IV. The attack model is presented in Section V. Subsequently, we present the privacy model in Section VI. In Section VII, we formally prove that our protocol preserves data privacy and provides unlinkability. In Section VIII, we measure the level of privacy achieved by AnonPri as a function of the total number of compromised tags. In Section IX, we discuss the limitation of AnonPri. We present relevant related work in Section X. Finally, we conclude the paper in Section XI.

# **SECTION II.** Privacy In RFID Systems

## A. Privacy vs. Scalability

Ensuring strong privacy imposes a higher complexity on the reader. Conversely, improving efficiency may hamper some privacy. In this paper we focus on this major problem of between privacy and scalability of RFID systems.

Public key cryptography would be a better candidate to solve the problem between privacy and scalability. In this approach, the tag would encrypt its message using the public key of the reader so that only the real reader would be able to decrypt the message and identify the tag. But public key encryption is too expensive for low cost tags. In this paper we consider the low cost tags which are capable of doing symmetric key encryption, in which keys are shared between the tag and the legitimate readers.

First, we outline how the tree based hash protocol provides scalability but sacrifice some privacy. Then, we describe how the group based protocol provides improved scalability as well as a higher level of privacy. Finally, we point out the privacy problem of this group based protocol.

### 1) Tree based hash protocol

The tree based hash protocol proposed by Molnar and Wagner5 reduces the reader's complexity from  to . Tags are organized in a secret key tree where each tag is assigned to a leaf of the tree. Secret keys are associated with each branch of the tree. Each tag (each leaf) receives all the secret keys along the path from the root to itself. If the tree has  levels, each tag stores  keys. The authors5 proposed the key tree as a balanced tree. So if the branching factor is α, the l will be equal to L. Each tag has only one key that is not shared with any other tag of the system. Fig. 1shows a balanced key tree with  and .

According to this protocol, the reader queries a tag with a nonce . Upon the reception of the nonce from the reader, the tag generates another nonce nt and replies to the reader with

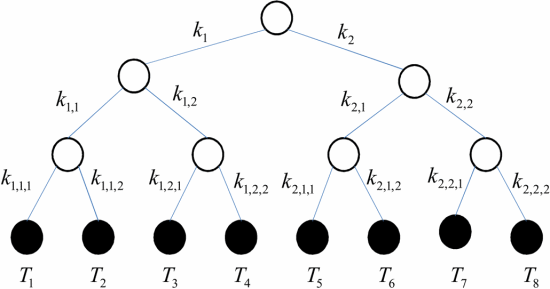
where each  is a hash function and ∥represents concatenation. The nonce produced by the tag provides unlinkability between two consecutive responses from the same tag. One the other side, the nonce from the reader prevents replay attacks. After receiving the response, the reader first finds a match with the first hash value of the response by hashing with all the keys of level 1. Whenever the reader obtains a match, the reader starts to search for the second hash value of the response by hashing with all the keys at the next level of the sub-tree rooted at the node where the reader has found the match. The reader repeats this step until it reaches a leaf. Thus, the reader's complexity is reduced to . In worst case, the reader has to search with all keys at each level of the tree and therefore, the complexity becomes .

The major drawback of this approach is the loss of privacy if any tag is compromised by the adversary. Since the tags share keys with some of the tags in the system, whenever a single tag becomes compromised all the tags that share at least one key with the compromised tag have to sacrifice their privacy. Suppose the tag  in Fig. 1 becomes compromised. All the tags of the system are partitioned into three disjoint sets. The adversary can now uniquely distinguish the tag  and identify the tags  and  as a unique partition. All the remaining tags  form a single partition because the tag  shares no key with them. Therefore each tag of this partition  is anonymous among these four tags. The privacy provided by this scheme diminishes as more and more tags are compromised by the adversary.

## 2) Group based protocol

Avoine et al.8 proposed a group based authentication protocol to address the privacy problem of the tree based hash protocol. According to this protocol, tags are divided into γ disjoint groups of equal size. Each group is associated with a unique key that we refer to as a group key. Every tag shares this group key with other members of the given group. Each tag is assigned a unique key that is known only to the tag and the reader. Fig. 2 shows the group organization of the tags where  and . The  's are the group keys, where . The identifier of the *jth* tag is represented by  (not shown in Fig. 2) and the unique secret key of the same tag is denoted as , where .

According to this protocol, the reader queries the tag with a nonce . The tag, then, replies the following encrypted message (we assume that each tag has the knowledge of the encryption algorithm) with the nonce  produced by the tag.

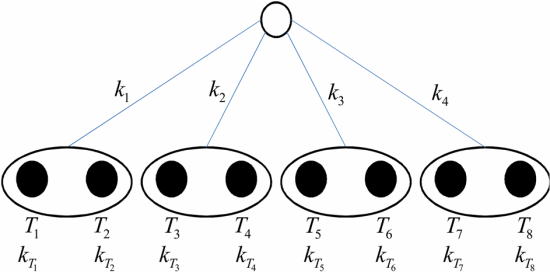
[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/5762825/5767569/5767573/5767573-fig-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/5762825/5767569/5767573/5767573-fig-1-source-large.gif)

**Figure 1.**A secret key tree for the tree based hash protocol with N=8 and α=2

Now the reader tries all the group keys to decrypt the first portion of the message. If the reader finds the right key that correctly decrypts the message, then the reader can learn  and decrypt the following portion of the response with the secret key of the tag . Thus, the reader verifies the tag's legitimacy. This protocol reduces the complexity of both the reader and the tag. The tag always has to perform two encryptions. In the worst case, the reader has to perform encryptions. In addition, each tag needs to store only two keys for the authentication.

The group organization of this protocol improves the level of privacy. If any tag is compromised by the adversary, then this compromised tag affects only the other members of its group. After compromising the tag, the adversary learns the group key and the tag's secret key. Now the adversary can uniquely identify every single tag from the same group since the adversary can discover each tag's identifier by decrypting the first portion of the response from each tag with the learned group key. All the remaining tags that belong to different groups form a single partition so that the adversary cannot distinguish the tags that belong to this partition. For instance, if the tag  is compromised, the adversary can uniquely identify only the tag  (see Fig. 2). The adversary cannot uniquely distinguish the other tags . Each of these tags remains anonymous among these six tags. This is a significant improvement in privacy protection of RFID systems in comparison with other protocols including tree based protocol.

Like other protocols, this protocol also has some limitations. There is a tradeoff between the number of groups and the group size. To address this problem, we propose an efficient anonymous private authentication (AnonPri) scheme that improves the privacy protection by keeping the reader's complexity moderate.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/5762825/5767569/5767573/5767573-fig-2-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/5762825/5767569/5767573/5767573-fig-2-source-large.gif)

**Figure 2.**The group organization of the tags for the group based authentication protocol, with  and

In our approach, each tag is assigned a couple of identifiers. A single tag shares some of its identifiers with some members of its group. Thus this protocol prevents tracking by increasing the uncertainty of the adversary.

## B. Privacy Characterization

In literature several different notions of privacy have been proposed so far. Some authors mention *information privacy* as the privacy of RFID systems. This privacy notion is the act of preventing a tag from disclosing its product information.4,3 But protecting information privacy keeps tags traceable. Therefore it is a weak notion of RFID privacy. Some define *unlinkability* as the strong notion of RFID privacy.6,9 Unlinkability means the inability to distinguish between the responses from the same tag and the responses from different tags of the system. Providing unlinkability ensures strong privacy when the adversary cannot distinguish between two tags with a probability better than random guessing.2 In our protocol, we protect privacy of the tags by providing unlinkability between two tags of the system.

The level of privacy obtained by any protocol can be measured using the *anonymity set. Anonymity* has been proposed in the context of mix-nets in.10 Mix-nets are used to make the sender (and the recipient) of a message anonymous. The anonymity set is defined as the set of all potential senders (recipients) of the message. Anonymity is defined as being not identifiable among a group of entities, i.e., the members of the anonymity set. A higher degree of anonymity is achieved with an anonymity set of larger size. Perfect anonymity is achieved if anonymity set contains all the members capable of sending (receiving) messages in system.

# SECTION III. System Model

Our protocol is based on the group based scheme. Therefore, tags are divided into groups of equal size. Suppose, N is the total number of tags in the system and τ is the number of groups. So, the group size is n=Nτ. In this section, we define the components and parameters of our system.

## Issuer

The issuer initializes each tag during the deployment by writing the tag's information into its memory. The issuer also authorizes the reader access to the tags. Even each group receives its unique group key and a pool of identifiers from the issuer.

## Group

Each group has a n number of tags. The issuer assigns a unique group key kGi to the ith group Gi of the system. This key is shared between the members (tags) of this group. Each group also receives the following pool of identifiers from the issuer

where,  and M is a system parameter. The pools of any two groups do not share any identifier, i.e., . Each tag of the group  is assigned a couple of identifiers from  by the issuer.

## Tag

All the tags of the system are divided into τ groups. Each tag receives the shared group key of the group that the tag belongs to, a unique secret key that is known only to the reader and the tag itself, and a set of identifiers from the pool of identifiers of the group. Suppose, the tag  belongs to the group . This tag possesses the group key , the unique secret key , and a set of identifiers . Each key is of *θ* bits, where *θ* is the security parameter of symmetric key encryption. We define the  as follows

where,

* each   is chosen randomly following uniform distribution from the pool  and , where
* , for all
* m is also a system parameter and .

The identifiers are assigned to the tags in such a way that at least one identifier of a tag is shared with at least two other members of the same group. So, we can say for the tag ,

where  are any two members of  and .

## Reader

The reader is connected to the backend server. In this paper, we assume the communication channel between the reader and the backend server is secured. From now on, we denote the backend server as the reader. In our system, the tag is the prover and the reader is the verifier. The reader receives all the secret information by the issuer during the deployment. The issuer issues the reader a set of secret information for each group in the system , where  is the secret group key and  is the mapping of the identifiers of the pool  with the secret keys of tags. Formally,

where  is the set of secret keys of tags associated with the  can be defined as an empty set if no tag is associated with the  or it can be a set of size at least one. Formally,

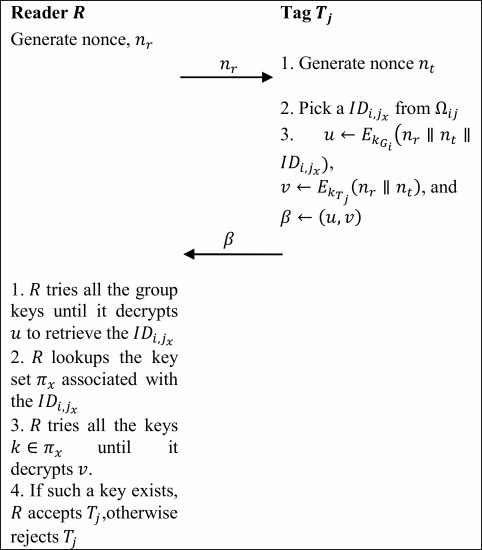
## System parameters

Since each tag receives m identifiers randomly chosen from the pool of  identifiers, according to the  distribution strategy, we can say that each tag has at least one identifier common with at least two group members. The probability that each tag shares at least one identifier with at least two group members is

where . For example, we consider an RFID system of 1000 tags divided in 10 groups. 100 tags are in each group. For simplicity, we assume  and . Then the probability that each tag shares at least one identifier with at least two group members is .

# **SECTION IV.** Our Protocol: Anonpri

In this section, we describe our protocol. The reader starts to query the tag with a nonce . Upon the reception of the query, the tag generates another nonce . Suppose the reader interrogates the tag . In the second step, the tag picks an identifier, say , from . Then the tag computes  as shown in Fig. 3. Here,  denotes symmetric key encryption with key . The tag replies with the . Now the reader searches all the group keys until it finds the correct one that properly decrypts the first part  of the response. If the reader retrieves the identifier  that the tag used in its response, then the reader tries to decrypt the second part  of  with the potential set of secret keys  associated with . After finding the right secret key, the reader can uniquely identify the tag . Sharing some identifiers of a tag with other members of the group provide unlinkability even if any tag is compromised by the adversary. We will discuss this in section VII.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/5762825/5767569/5767573/5767573-fig-3-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/5762825/5767569/5767573/5767573-fig-3-source-large.gif)

**Figure 3.**The efficient anonymous private authentication protocol

# **SECTION V.** Attack Model

One of the major goals of an adversary in any RFID system is to infringe the tags' privacy by means of tracking. In this paper, an adversary is denoted as . We assume  as an active adversary who has full control over all the communications between the tag and the reader. She can not only eavesdrop, but also intercept, modify and even initiate authentication session. The adversary can, for example, impersonate a tag and communicate with the valid reader. Even the adversary can query a valid tag and learn the tag's response. Our assumptions also include that the adversary can control a number of readers and tags. Each reader and tag controlled by the adversary are denoted as  and , respectively.  is unauthorized to have access to any real tags since  has no secret information like the real reader . Similarly,  is not valid as it does not have the secret and identifying information of a valid tag. However, the adversarial reader  can communicate with a valid tag. Even the fake tag  can communicate with a legitimate reader. In both cases, the ultimate goal of the adversary is to track any tag of the RFID system. We assume that the adversary, the adversarial reader, and the adversarial tag have polynomially bounded resources. In addition, the adversary can launch physical attacks. However, the hardware based defenses against physical attacks are beyond the scope of this paper. We also assume that the reader cannot be compromised.

# **SECTION VI.** Privacy Model

At the end of the protocol description, we mention that this protocol provide unlinkability and thereby preserves privacy. The adversary cannot link the responses with the tags, even if she can decrypt the first portion of the response and learn the identifier that the tags are using to produce the response. Like Juels and Weis,2 we use an experiment based definitions to formalize RFID privacy. We conclude that the adversary cannot break unlinkability or invade privacy with probability better than random guessing. The following oracle-like construction exists:

 is an oracle that randomly chooses some tags from all the  tags of the system.

 takes a tag  as an input. Given the nonce , the group key , the secret key  and the set of identifiers , the oracle randomly selects an , generates another nonce and finally produces the response . It outputs the cipher text .

 is an oracle that, provided with a tag , queries the tag and outputs the received response .

 is an oracle that, provided with two tags , randomly chooses  and queries the tag  using Oquery. Then it outputs the response .

## A. Information Privacy Against

Given a tag , the set of identifiers  stored on , and an identifier , an adversary can break the information privacy of our protocol if she can guess whether the tag  is using the . Moreover,  is the security parameter and  is the maximum number of time the adversary can query the tag . In addition, since the oracles of our model are random, the inputs are computationally intractable from the outputs of the oracles.

### Experiment

1. Setup: The issuer initializes the  tags of the system with their corresponding unique secret keys, the group keys, and the sets of identifiers after dividing the tags into  groups. It shares all the secret information with only the reader.
2. Learning:  provides the adversary with a challenged tag  that the adversary queries  times and appends each response  to the list  (initially L is an empty list).
3. Guess: Now the adversary transmits the tag  to the oracle  with a nonce and receives a response  from the oracle. The adversary selects an identifier . Given the list of  responses in  outputs if she guesses that  is produced using , and 0 otherwise.  is successful if her guess is right.

### Definition 1.

*AnonPri is said to preserve information* *privacy with security parameter*  *and*  *representing any polynomial function of* , *if*

## B. Unlinkability Against

The adversary should not be able to distinguish between the two responses from the same tag.

### Experiment

1. **Setup:** The issuer initializes the  tags of the system with their corresponding unique secret keys, the group keys, and the sets of identifiers after dividing the tags into  groups. It shares all the secret information with only the reader.
2. **Learning:**  provides the adversary with two challenged tags  from the same group. The adversary queries each tag  times and appends each response  to the list (initially  is an empty list).
3. **Guess:** The adversary transmits  to the oracle  receives the response  from . Given the list of responses  and the response , the adversary guesses the value of b.  succeeds if her guess is right.

### Definition 2.

*AnonPri is said to provide unlinkability with* *security parameter*  *and poly*  *representing any polynomial function of , if*

# **SECTION VII.** Security and Privacy Analysis

In this section, we formally prove that our protocol preserves data privacy and provides unlinkability. In addition, we analyze the preservation of privacy in some attack scenarios where some of the tags of the system are compromised by the adversary .

## A. Information Privacy

### Theorem 1.

*AnonPri preserves information privacy with* *respect to the adversary* .

### Proof.

Let us assume  provides the adversary  with a tag .  transmits this tag to the oracle  with a nonce . Then  provides  with the response .

Now,  selects a . To break data privacy,  should tell if  is produced using the . This implies that  has to identify the input of the encryption by just learning the cipher text.  can succeed in two cases. First, if she can retrieve the inputs from the output of the random oracle. But this contradicts with our assumption that the inputs of a random oracle are computationally intractable from the output of the oracle. Second, if  knows the secret keys of the tag . Without tampering the tag , if  can determine the keys by learning the cipher texts, this again breaks the semantic security of the symmetric key cryptography. Therefore  can break data privacy with probability no better than random guessing. Thus it proves data privacy property of Definition 1.

# B. Unlinkability

### Theorem 2.

*AnonPri provides unlinkability with respect to* *the adversary* .

### Proof.

Let us assume  provides the adversary  with two tags from the same group. These two tags go into the learning phase.  transmits  to  which outputs the response .

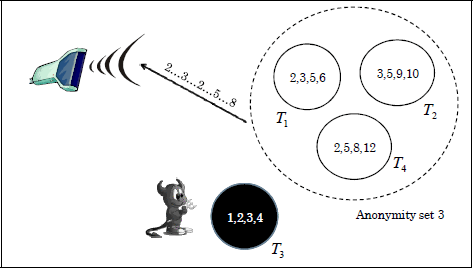
Now, to break unlinkability, the adversary   has to tell the value of . We assume that the adversary's guess is right. In other words, the adversary can determine whether the response  is produced by  or , given the learned responses from both the tags. The responses of a tag cannot be a signature of the tag because according to our protocol, a nonce on the tag side makes each response different from all the previous responses originated from the same tag. Therefore, we can say that the guess is right because the adversary knows the keys (the group key and the secret key) stored on these two tags. Without tampering the tags , the adversary has to determine the keys stored on these tags by just observing the cipher texts. But this contradicts with the semantic security of symmetric key cryptography. Therefore the adversary can break unlinkability with no better approach than random guessing. Thus it proves the unlinkability property of Definition 2. ■

## C. Physical Attack

Under this attack, we consider that the adversary  can compromise any tag with a probability of . Whenever a tag  becomes compromised, the adversary learns all private information stored on the tag . Therefore, the adversary can now decrypt  of each response  originated from the other members of the group . Thus,  can learn the identifier that a tag is using to produce its response by decrypting the . We discuss the aftereffect of this attack with an example and demonstrate how AnonPri provides unlinkability even if the adversary realizes the identifiers used in the responses.

We consider a group Gi of four tags , and . Suppose the adversary compromised the tag  as shown in Fig. 4. Now the adversary learns the group key , the tag secret key and a set of identifiers . From now on, the adversary can decrypt u part of all the responses originated from , and  with the group key . But, the adversary still cannot decrypt  part of these responses since she does not possess the secret keys of these tags. With this learned information (and ), the adversary tries to track the other tags of this group. Since the adversary can decrypt  of each responses, she can learn the identifier underlying the cipher text . In other words, she can discover which identifier has been used to produce a response. The arrow in the Fig. 4 represents that the responses of the authentication sessions (after  is compromised) are transmitted from the tags  to the reader. The identifiers used in these responses are shown on above the arrow. Each identifier is shown in plaintext since the adversary can retrieve the identifier by decrypting  of  using .

According to our protocol, even if the adversary comes to know about the identifier used in a response, she cannot conclude which of the potential tags is the sender of this response. In our example, the adversary discovers the identifier 2 is used two times, but she cannot be certain which of these tags  is the originator(s) of these responses. Though  shares the identifier 2 with only  and , however, the adversary has no knowledge about the parties with whom  is sharing which of its identifiers. Even the adversary does not know how many of the identifiers of  are being shared. So, under this scenario, the anonymity set of the potential senders of a given response seems to be 3 to the adversary. Therefore, when the adversary compromises one tag from the group of  uncorrupted tags, AnonPri forms an anonymity set of size 1 and another anonymity set of size  from the group instead of  anonymity sets of size 1 like the group based authentication.8 This is the noticeable partition that improves the level of privacy provided by AnonPri. Because, the remaining  tags of the system forms the other anonymity set which is same under both the protocols. Thus AnonPri prevents adversary benefit from tracking by compromising a tag.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/5762825/5767569/5767573/5767573-fig-4-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/5762825/5767569/5767573/5767573-fig-4-source-large.gif)

**Figure 4.**Aftereffect of a physical attack on AnonPri, where  is compromised by the adversary

We now consider the case of compromising multiple tags of the same group. In the above scenario, even if  compromises either  or  after compromising , the adversary cannot be certain whether  has identifier 2 in Ω2 or not. Therefore, the size of anonymity set is still 2, i.e., , where c is the number of compromised tags of the group. If  compromises  instead of  or , the size of anonymity set is still 2 (i.e., ). Therefore, we conclude that the anonymity set, formed from a group that is under physical attack, is of size , where  is the group size and  is the number of compromised tags of the given group.

AnonPri provides protocol-level privacy only. In real world, there are many possible side channels. If tags emit distinct “radio-fingerprint”, then no protocol-level privacy countermeasures can prevent privacy infringement.11

# **SECTION VIII.** Measurement of Privacy

In this section, we measure the level of privacy achieved by AnonPri as a function of the total number of compromised tags. We consider two privacy metrics for the measurement of privacy. First, our privacy measurement technique is based on anonymity set like the privacy metric used by Avoine et al.8 Second, we identify the amount of information disclosed by a scheme as another metric presented in.6 This metric is based on Shannon's information theorem.12

## A. Measurement of Privacy Based on Anonymity Set

The level of privacy of an RFID system, achieved by a scheme, at a given time, is a function of the total number of compromised tags at that time. When some tags are compromised, the set of all tags are partitioned such that the adversary cannot distinguish the tags belong to the same partition, but she can distinguish the tags that belong to different partitions. So, these partitions become the anonymity sets of their members. The level of privacy based on anonymity set, ℘, can be measured as the average anonymity set size.8

where  denotes the size of partition  and  is the probability that a randomly chosen tag belongs to partition .

According to AnonPri, a similar kind of partitions is formed when tags become compromised. If  is the number of compromised tags within group , then the set of the tags within this group is partitioned into ci anonymity sets of size 1 and another anonymity set of size . If  is the total compromised tags within  is the set of compromised groups,  is the total number of compromised groups, and  is the total number of compromised tags, the level of privacy  achieved by AnonPri can be expressed as

where  total number of tags in the system

* total number of tags within a group
* total number of groups in the system.

## B. Measurement of Privacy Based on Information Leakage

We measure the information leakage in bits based on Shannon's information theorem.12 If we have a group of tags of size  and the adversary divides this group into two disjoint subgroups of size , then 1 bit of information is disclosed out of log2S bits. Extending this concept from two subgroups of equal size to two subgroups of different sizes, where  tags are in one subgroup and the remaining tags  are in another subgroup, we can measure the average amount of information disclosed in bits as follows

In general, if the adversary splits  tags of the system into  disjoint partitions, then

where  denotes the size of partition .

According to our protocol, if  is the total compromised tags within  is the set of compromised groups,  is the total number of compromised groups, and  is the total number of compromised tags, the amount of information leakage in bits  can be expressed as

where,  total number of tags in the system

* total number of tags within a group
* total number of groups in the system.

## C. Experimental Results

We have compared both the protocols, AnonPri and the group based authentication, using a Matlab simulation. The experiment results establish that the level of privacy provided by AnonPri is higher than that of the group based authentication. Our comparison is based on the two metrics presented above, the level of privacy (based on anonymity set) and information leakage. We have come up with a conclusion same as6 that the information leakage describes the privacy threats better than the anonymity set.

In our simulation, we have considered two systems with  and . Tags are selected to be compromised with a uniform random distribution. The number of compromised tags ranges from 0 to 160. We have run the simulation for 100 times and computed the average  achieved by AnonPri and the group based authentication as a function of the total number of compromised tags  (see Fig. 5(a)-(b)). The small increase in the level of privacy achieved by AnonPri is visible when the total number of compromised tags becomes more than 30.

During the simulation, we have also computed the average amount of information leakage , for both the protocols, as a function of the total number of compromised tags  (see Fig. 5(c)-(d)). The plots depict that a significant amount of improvement in privacy protection is achieved by AnonPri. With the increase in the total number of compromised tags , the average amount of information disclosed by the group based authentication is quite higher than the information disclosed by AnonPri. In Fig. 5(c) , when  becomes 160, the group based authentication discloses about 15 bits out of 16 bits of information, while AnonPri discloses about 6 bits of information. The group based authentication discloses 56.25% more information than AnonPri in a similar setup. Fig. 5(d)  shows that the group based authentication reveals almost 19 bits out of 20 bits of information and AnonPri reveals around 6 bits of information. This time the group based authentication discloses 65% more information than AnonPri. Based on the simulation results, we can conclude that the information disclosed by the group based authentication increases with the size of the system; however, AnonPri shows consistency in the information leakage in both the cases.

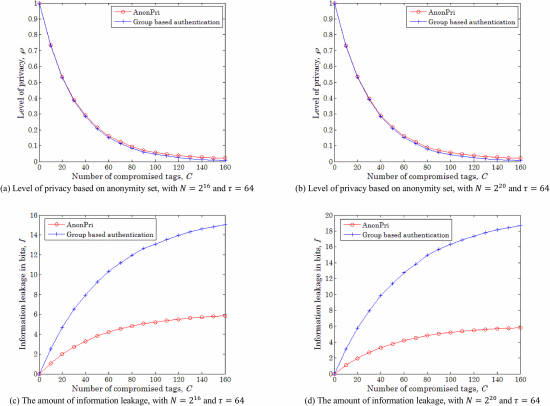
Information leakage is a better metric to demonstrate the privacy threats in RFID systems than anonymity set. Though the improvement in ℘ provided by AnonPri against the group based authentication is not significant, however, we can say that AnonPri provides better privacy protection than the group based authentication, based on the results of the amount of information disclosed by these two protocols.

# SECTION IX. Discussion

In this section, we discuss the limitations of AnonPri.

## A. Search Complexity

According to AnonPri, the reader's complexity is slightly increased than the group based scheme.8 After receiving the response  from a tag , the reader searches for the correct group key to decrypt u. In the worst case, the reader has to perform this operation τ times. If such a group key exists, the reader can retrieve the identifier  from . Now, the reader has to search for the tag's secret key to identify  by decrypting ν properly. The reader searches a key space of size . Therefore, in the worst case, the reader's total complexity is . In the best case, the size of  is 3 and in the worst case, it can be , size of the group. But in the group based scheme, the reader's complexity in worst case is .

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/5762825/5767569/5767573/5767573-fig-5-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/5762825/5767569/5767573/5767573-fig-5-source-large.gif)

**Figure 5.**Experimental results of AnonPri against the group based authentication

Nevertheless, AnonPri is much better than the other schemes where the worst case reader's complexity is , the number of total tags in the system. To provide improvement in privacy protection, we have to sacrifice this small increase in the complexity of the reader. Since readers are more powerful than tags, they can handle this increase in search complexity.

## B. Memory Complexity

According to AnonPri, tags need to store m number of identifiers along with the group key and the unique secret key. Though tags have limited resources, however, the increase in memory requirement is acceptable than the increase in computation and communication complexity. A smart RFID tags have memory capacity of 32kBytes or more.13 Even RFID tags with extended memory capacity are available at the market.14 All these tags can store the information required for AnonPri.

# **SECTION X.** Related Work

Private authentication techniques proposed to protect user privacy in RFID systems can be classified into two categories, non-tree-based approaches and tree-based approaches. Non-tree-based protocols usually perform linear search to find out a tag. The search complexity is , where  is the number of tags. Obviously, the linear search is not efficient in large-scale RFID systems that may have millions of tags [24].

Another non-tree-based approach, Hash-lock4 method uses the hash value of a key to identify a tag. A variation of Hash-lock needs exhaustive search through all IDs to identify a tag. Molnar and Wagner proposed a tree based approach in5 that reduces the complexity of authentication from  to . This reduction is made possible by using a key-tree instead of a flat key space. The level of privacy provided by the scheme is decreases quickly as more and more tags are compromised. Numbers of research have been conducted to find out a trade-off between the complexity and the level of privacy provided by the key-tree based scheme. This trade-off is identified and analyzed by Avoine et al. in,15 by Buttyan, Holczer, and Vajda in,7 and more recently by Nohl and Evans in.6 These papers introduce privacy metrics and quantify the level of privacy provided by the key-tree based scheme when some tags are compromised.

Avoine et al. proposed a group based private authentication scheme in8 that improves the tradeoff between scalability and privacy by dividing the tags into a number of groups. One major limitation of this protocol is that the level of privacy provided by the scheme decreases as more and more tags are compromised.

Nohara et al. discuss the unlinkability and the real world constraints in RFID systems in.16 They define a link expression with real world constraints and propose a location tracking model. The simulation results show the real world constraints have possibility that break the unlinkability. However, the authors did not consider the unlinkability issue from privacy violation perspective.

A lightweight RFID private authentication protocol, RWP, have been proposed in,17 based on the random walk concept. The analysis results show that RWP effectively enhances the security protection for RFID private authentication, and increases the authentication efficiency from  to . However, this technique is suitable for tags with high computational power as the technique requires tags to perform randomized hash functions.

In the recent past, significant research has been conducted in developing RFID systems to ease the everyday life of human.18–19,20,21 Even recently some research has been performed to devise accurate ways of determining indoor location.22,23 But all of these researches mainly focused on developing the system itself, rather than focusing to consider the privacy impacts of installing those RFID systems in practical environment.

# SECTION XI. Conclusions

RFID systems will be useful for many applications if the system can guarantee consumer privacy as well as improve scalability. To address the tradeoff between privacy and scalability, we have proposed an efficient anonymous private authentication protocol (AnonPri) in this paper. We have presented a brief comparison between the tree based hash protocol and the group based authentication for RFID systems. Then we have presented a privacy definition that an RFID system should consider. A detail security and privacy analysis of AnonPri establishes that AnonPri preserves information privacy as well as unlinkability. In addition, AnonPri provides higher level of privacy than the group based scheme when some of the tags are compromised by the adversary. However, according to AnonPri, the reader faces a slight increase in the search complexity, which is much better than performing linear search in the database to identify a single tag. Finally, we can say that AnonPri is suitable for many applications where privacy violation is a major point-of-failure.

Our future work includes further reducing the costs of complexity, storage, increasing scalability. Another future work can be to determine an optimal tradeoff between the authentication complexity and storage required.

# References

1. *CASPIAN Press Release. Metro's decision to drop the loyalty card 2004*.

2. A. Juels, S. Weis, "Defining strong privacy for RFID", *Proc. of Pervasive Computing and Communications Workshops (PerComW 2007)*, pp. 342-347, 2007.

3. M. Ohkubo, K. Suzuki, S. Kinoshita, "Cryptographic approach to privacy friendly tags", *Proc. of RFID Privacy Workshop*, 2003.

4. S. Weis, S. Sarma, R. Rivest, D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", *Proc. of Security in Pervasive Computing (SPC 2003)*, vol. 2802, pp. 454-469, 2003.

5. D. Molnar, D. Wagner, "Privacy and security in library RFID: Issues practices and architectures", *Proc. of Computer and Communications Security. USA 2004*, pp. 210-219.

6. K. Nohl, D. Evans, "Quantifying information leakage in tree-based hash protocols", *Proc. of Information and Communications Security (ICICS 2006). USA. 2006*, pp. 228-237.

7. L. Buttyan, T. Holczer, I. Vajda, "Optimal key-trees for tree-based private authentication", *Proc. of Privacy Enhancing Technologies Workshop (PET 2006)*, pp. 332-350, 2006.

8. G. Avoine, L. Buttyan, T. Holczer, I. Vajda, "Group-based private authentication", *Proc. of World of Wireless Mobile and Multimedia Networks (WoWMoM 2007). Finland. 2007*, pp. 1-6.

9. C. Chatmon, T. V. Le, M. Burmester, "Secure anonymous RFID authentication protocols", *Technical report*, 2006.

10. C. Diaz, S. Seys, J. Claessens, B. Preneel, "Towards measuring anonymity", *Privacy Enhancing Technologies Workshop (PET 2002). USA. 2002*, pp. 54-68.

11. G. Avoine, P. Oechslin, "A scalable and provably secure hash based RFID protocol", *Proceedings of the IEEE International Workshop on Pervasive Computing and Communication Security (PerSec 2005). USA. 2005*, pp. 110-114.

12. C. Shannon, "A mathematical theory of communication", *Bell System Technical Journal*, vol. 27, pp. 379-423, 1948.

13. A. Laurie, "Practical attacks against RFID", *Network Security*, no. 9, pp. 4-7, 2007.

14. *Fujitsu develops world's first 64KByte high-capacity FRAM RFID tag for aviation applications 2008*.

15. G. Avoine, E. Dysli, P. Oechslin, B. Preneel, S. Tavares, "Reducing time complexity in RFID systems" in Selected Areas in Cryptography, Springer, pp. 291-306, 2005.

16. Y. Nohara, S. Inoue, H. Yasuura, "Unlinkability and real world constraints in RFID systems", *Proc. of Pervasive Computing and Communications Workshop (PerCom Workshops 2007)*, pp. 371-376, 2007.

17. Q. Yao, Y. Qi, J. Han, J. Zhao, X. Li, Y. Liu, "Randomizing RFID private authentication", *Proc. of Pervasive Computing and Communications Workshop (PerCom Workshops 2009)*, pp. 1-10, 2009.

18. S. Hinske, "Determining the Position and Orientation of Multi-Tagged Objects Using RFID Technology", *Proc. of Pervasive Computing and Communications Workshops (PerCom Workshops 2007)*, pp. 377-381, 2007.

19. G. Zecca, P. Couderc, M. Banatre, R. Beraldi, "Swarm robot synchronization using RFID tags", *Proc. of Pervasive Computing and Communications (PerCom 2009)*, pp. 1-4, 2009.

20. V.P. Munishwar, S. Singh, C. Mitchell, W. Xiaoshuang, K. Gopalan, N.B Abu-Ghazaleh, "RFID based localization for a miniaturized robotic platform for wireless protocols evaluation", *Proc. of Pervasive Computing and Communications (PerCom 2009)*, pp. 1-3, 2009.

21. Ilic, F. Michahelles, E. Fleisch, "Dual ownership: access management for shared item information in RFID-enabled supply chains", *Proc. of Pervasive Computing and Communications Workshops (PerCom Workshops 2007)*, pp. 337-341, 2007.

22. A. Saxena, S. Ganguly, S. Bhatnagar, R. Izmailov, "RFInD: an RFID-based system to manage virtual spaces", *Proc. of Pervasive Computing and Communications Workshops (PerCom Workshops 2007)*, pp. 382-387, 2007.

23. L.M. Ni, L. Yunhao, C. L. Yiu, A.P. Patil, "LANDMARC: indoor location sensing using active RFID", *Proc. of Pervasive Computing and Communications (PerCom 2003)*, pp. 407-415, 2003.

24. G. Roussos, V. Kostakos, "RFID in pervasive computing: ctate-of-the-art and outlook", *Pervasive and Mobile Comp.*, 2008.

Citation Map

**1.** *CASPIAN Press Release. Metro's decision to drop the loyalty card 2004*.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.jtitle=CASPIAN%20Press%20Release.%20Metro%27s%20decision%20to%20drop%20the%20loyalty%20card,%202004&rft.date=2010&rft.au=&rft.aulast=)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.jtitle=CASPIAN%20Press%20Release.%20Metro%27s%20decision%20to%20drop%20the%20loyalty%20card,%202004&rft.date=2010&rft.au=&rft.aulast=)[Google Scholar](https://scholar.google.com/scholar?as_q=CASPIAN+Press+Release.+Metro%27s+decision+to+drop+the+loyalty+card%2C+2004&as_occt=title&hl=en&as_sdt=0%2C31)

**2.** A. Juels, S. Weis, "Defining strong privacy for RFID", *Proc. of Pervasive Computing and Communications Workshops (PerComW 2007)*, pp. 342-347, 2007.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOMW.2007.37&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Defining%20strong%20privacy%20for%20RFID&rft.spage=342&rft.epage=347&rft.au=A.%20Juels&rft.aulast=A.%20Juels)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOMW.2007.37&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Defining%20strong%20privacy%20for%20RFID&rft.spage=342&rft.epage=347&rft.au=A.%20Juels&rft.aulast=A.%20Juels)[Google Scholar](https://scholar.google.com/scholar?as_q=Defining+strong+privacy+for+RFID&as_occt=title&hl=en&as_sdt=0%2C31)

**3.** M. Ohkubo, K. Suzuki, S. Kinoshita, "Cryptographic approach to privacy friendly tags", *Proc. of RFID Privacy Workshop*, 2003.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Cryptographic%20approach%20to%20privacy%20friendly%20tags&rft.au=M.%20Ohkubo&rft.aulast=M.%20Ohkubo)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Cryptographic%20approach%20to%20privacy%20friendly%20tags&rft.au=M.%20Ohkubo&rft.aulast=M.%20Ohkubo)[Google Scholar](https://scholar.google.com/scholar?as_q=Cryptographic+approach+to+privacy+friendly+tags&as_occt=title&hl=en&as_sdt=0%2C31)

**4.** S. Weis, S. Sarma, R. Rivest, D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", *Proc. of Security in Pervasive Computing (SPC 2003)*, vol. 2802, pp. 454-469, 2003.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Security%20and%20privacy%20aspects%20of%20low-cost%20radio%20frequency%20identification%20systems&rft.volume=2802&rft.spage=454&rft.epage=469&rft.au=S.%20Weis&rft.aulast=S.%20Weis)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Security%20and%20privacy%20aspects%20of%20low-cost%20radio%20frequency%20identification%20systems&rft.volume=2802&rft.spage=454&rft.epage=469&rft.au=S.%20Weis&rft.aulast=S.%20Weis)[Google Scholar](https://scholar.google.com/scholar?as_q=Security+and+privacy+aspects+of+low-cost+radio+frequency+identification+systems&as_occt=title&hl=en&as_sdt=0%2C31)

**5.** D. Molnar, D. Wagner, "Privacy and security in library RFID: Issues practices and architectures", *Proc. of Computer and Communications Security. USA 2004*, pp. 210-219.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1145/1030083.1030112&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Privacy%20and%20security%20in%20library%20RFID:%20Issues,%20practices,%20and%20architectures&rft.spage=210&rft.epage=219&rft.au=D.%20Molnar&rft.aulast=D.%20Molnar)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1145/1030083.1030112&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Privacy%20and%20security%20in%20library%20RFID:%20Issues,%20practices,%20and%20architectures&rft.spage=210&rft.epage=219&rft.au=D.%20Molnar&rft.aulast=D.%20Molnar)[Access at ACM](https://doi.org/10.1145/1030083.1030112)[Google Scholar](https://scholar.google.com/scholar?as_q=Privacy+and+security+in+library+RFID%3A+Issues%2C+practices%2C+and+architectures&as_occt=title&hl=en&as_sdt=0%2C31)

**6.** K. Nohl, D. Evans, "Quantifying information leakage in tree-based hash protocols", *Proc. of Information and Communications Security (ICICS 2006). USA. 2006*, pp. 228-237.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Quantifying%20information%20leakage%20in%20tree-based%20hash%20protocols&rft.spage=228&rft.epage=237&rft.au=K.%20Nohl&rft.aulast=K.%20Nohl)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Quantifying%20information%20leakage%20in%20tree-based%20hash%20protocols&rft.spage=228&rft.epage=237&rft.au=K.%20Nohl&rft.aulast=K.%20Nohl)[Google Scholar](https://scholar.google.com/scholar?as_q=Quantifying+information+leakage+in+tree-based+hash+protocols&as_occt=title&hl=en&as_sdt=0%2C31)

**7.** L. Buttyan, T. Holczer, I. Vajda, "Optimal key-trees for tree-based private authentication", *Proc. of Privacy Enhancing Technologies Workshop (PET 2006)*, pp. 332-350, 2006.

 Show Context [CrossRef](https://doi.org/10.1007/11957454_19)[[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1007/11957454_19&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Optimal%20key-trees%20for%20tree-based%20private%20authentication&rft.spage=332&rft.epage=350&rft.au=L.%20Buttyan&rft.aulast=L.%20Buttyan)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1007/11957454_19&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Optimal%20key-trees%20for%20tree-based%20private%20authentication&rft.spage=332&rft.epage=350&rft.au=L.%20Buttyan&rft.aulast=L.%20Buttyan)[Google Scholar](https://scholar.google.com/scholar?as_q=Optimal+key-trees+for+tree-based+private+authentication&as_occt=title&hl=en&as_sdt=0%2C31)

**8.** G. Avoine, L. Buttyan, T. Holczer, I. Vajda, "Group-based private authentication", *Proc. of World of Wireless Mobile and Multimedia Networks (WoWMoM 2007). Finland. 2007*, pp. 1-6.

 Show Context [View Article](https://ieeexplore.ieee.org/document/4351808)[Full Text: PDF](https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4351808) (3361KB) [Google Scholar](https://scholar.google.com/scholar?as_q=Group-based+private+authentication&as_occt=title&hl=en&as_sdt=0%2C31)

**9.** C. Chatmon, T. V. Le, M. Burmester, "Secure anonymous RFID authentication protocols", *Technical report*, 2006.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Secure%20anonymous%20RFID%20authentication%20protocols&rft.jtitle=Technical%20report&rft.date=2006&rft.au=C.%20Chatmon&rft.aulast=C.%20Chatmon)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Secure%20anonymous%20RFID%20authentication%20protocols&rft.jtitle=Technical%20report&rft.date=2006&rft.au=C.%20Chatmon&rft.aulast=C.%20Chatmon)[Google Scholar](https://scholar.google.com/scholar?as_q=Secure+anonymous+RFID+authentication+protocols&as_occt=title&hl=en&as_sdt=0%2C31)

**10.** C. Diaz, S. Seys, J. Claessens, B. Preneel, "Towards measuring anonymity", *Privacy Enhancing Technologies Workshop (PET 2002). USA. 2002*, pp. 54-68.

 Show Context [CrossRef](https://doi.org/10.1007/3-540-36467-6_5)[[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1007/3-540-36467-6_5&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Towards%20measuring%20anonymity&rft.spage=54&rft.epage=68&rft.au=C.%20Diaz&rft.aulast=C.%20Diaz)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1007/3-540-36467-6_5&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Towards%20measuring%20anonymity&rft.spage=54&rft.epage=68&rft.au=C.%20Diaz&rft.aulast=C.%20Diaz)[Google Scholar](https://scholar.google.com/scholar?as_q=Towards+measuring+anonymity&as_occt=title&hl=en&as_sdt=0%2C31)

**11.** G. Avoine, P. Oechslin, "A scalable and provably secure hash based RFID protocol", *Proceedings of the IEEE International Workshop on Pervasive Computing and Communication Security (PerSec 2005). USA. 2005*, pp. 110-114.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOMW.2005.12&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=A%20scalable%20and%20provably%20secure%20hash%20based%20RFID%20protocol&rft.spage=110&rft.epage=114&rft.au=G.%20Avoine&rft.aulast=G.%20Avoine)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOMW.2005.12&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=A%20scalable%20and%20provably%20secure%20hash%20based%20RFID%20protocol&rft.spage=110&rft.epage=114&rft.au=G.%20Avoine&rft.aulast=G.%20Avoine)[Google Scholar](https://scholar.google.com/scholar?as_q=A+scalable+and+provably+secure+hash+based+RFID+protocol&as_occt=title&hl=en&as_sdt=0%2C31)

**12.** C. Shannon, "A mathematical theory of communication", *Bell System Technical Journal*, vol. 27, pp. 379-423, 1948.

 Show Context [CrossRef](https://doi.org/10.1002/j.1538-7305.1948.tb01338.x)[[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1002/j.1538-7305.1948.tb01338.x&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=A%20mathematical%20theory%20of%20communication&rft.jtitle=Bell%20System%20Technical%20Journal&rft.date=1948&rft.volume=27&rft.spage=379623&rft.epage=423656&rft.au=C.%20Shannon&rft.aulast=C.%20Shannon)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1002/j.1538-7305.1948.tb01338.x&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=A%20mathematical%20theory%20of%20communication&rft.jtitle=Bell%20System%20Technical%20Journal&rft.date=1948&rft.volume=27&rft.spage=379623&rft.epage=423656&rft.au=C.%20Shannon&rft.aulast=C.%20Shannon)[Google Scholar](https://scholar.google.com/scholar?as_q=A+mathematical+theory+of+communication&as_occt=title&hl=en&as_sdt=0%2C31)

**13.** A. Laurie, "Practical attacks against RFID", *Network Security*, no. 9, pp. 4-7, 2007.

 Show Context [CrossRef](https://doi.org/10.1016/S1353-4858(07)70080-6)[[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1016/S1353-4858(07)70080-6&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Practical%20attacks%20against%20RFID&rft.jtitle=Network%20Security&rft.date=2007&rft.issue=9&rft.spage=4&rft.epage=7&rft.au=A.%20Laurie&rft.aulast=A.%20Laurie)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1016/S1353-4858(07)70080-6&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Practical%20attacks%20against%20RFID&rft.jtitle=Network%20Security&rft.date=2007&rft.issue=9&rft.spage=4&rft.epage=7&rft.au=A.%20Laurie&rft.aulast=A.%20Laurie)[Google Scholar](https://scholar.google.com/scholar?as_q=Practical+attacks+against+RFID&as_occt=title&hl=en&as_sdt=0%2C31)

**14.** *Fujitsu develops world's first 64KByte high-capacity FRAM RFID tag for aviation applications 2008*.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.jtitle=Fujitsu%20develops%20world%27s%20first%2064KByte%20high-capacity%20FRAM%20RFID%20tag%20for%20aviation%20applications,%202008&rft.date=2010&rft.au=&rft.aulast=)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.jtitle=Fujitsu%20develops%20world%27s%20first%2064KByte%20high-capacity%20FRAM%20RFID%20tag%20for%20aviation%20applications,%202008&rft.date=2010&rft.au=&rft.aulast=)[Google Scholar](https://scholar.google.com/scholar?as_q=Fujitsu+develops+world%27s+first+64KByte+high-capacity+FRAM+RFID+tag+for+aviation+applications%2C+2008&as_occt=title&hl=en&as_sdt=0%2C31)

**15.** G. Avoine, E. Dysli, P. Oechslin, B. Preneel, S. Tavares, "Reducing time complexity in RFID systems" in Selected Areas in Cryptography, Springer, pp. 291-306, 2005.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.jtitle=Selected%20Areas%20in%20Cryptography&rft.date=2005&rft.spage=291&rft.epage=306&rft.au=G.%20Avoine&rft.aulast=G.%20Avoine)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.jtitle=Selected%20Areas%20in%20Cryptography&rft.date=2005&rft.spage=291&rft.epage=306&rft.au=G.%20Avoine&rft.aulast=G.%20Avoine)[Google Scholar](https://scholar.google.com/scholar?as_q=Reducing+time+complexity+in+RFID+systems&as_occt=title&hl=en&as_sdt=0%2C31)

**16.** Y. Nohara, S. Inoue, H. Yasuura, "Unlinkability and real world constraints in RFID systems", *Proc. of Pervasive Computing and Communications Workshop (PerCom Workshops 2007)*, pp. 371-376, 2007.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOMW.2007.122&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Unlinkability%20and%20real%20world%20constraints%20in%20RFID%20systems&rft.spage=371&rft.epage=376&rft.au=Y.%20Nohara&rft.aulast=Y.%20Nohara)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOMW.2007.122&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Unlinkability%20and%20real%20world%20constraints%20in%20RFID%20systems&rft.spage=371&rft.epage=376&rft.au=Y.%20Nohara&rft.aulast=Y.%20Nohara)[Google Scholar](https://scholar.google.com/scholar?as_q=Unlinkability+and+real+world+constraints+in+RFID+systems&as_occt=title&hl=en&as_sdt=0%2C31)

**17.** Q. Yao, Y. Qi, J. Han, J. Zhao, X. Li, Y. Liu, "Randomizing RFID private authentication", *Proc. of Pervasive Computing and Communications Workshop (PerCom Workshops 2009)*, pp. 1-10, 2009.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Randomizing%20RFID%20private%20authentication&rft.spage=1&rft.epage=10&rft.au=Q.%20Yao&rft.aulast=Q.%20Yao)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Randomizing%20RFID%20private%20authentication&rft.spage=1&rft.epage=10&rft.au=Q.%20Yao&rft.aulast=Q.%20Yao)[Google Scholar](https://scholar.google.com/scholar?as_q=Randomizing+RFID+private+authentication&as_occt=title&hl=en&as_sdt=0%2C31)

**18.** S. Hinske, "Determining the Position and Orientation of Multi-Tagged Objects Using RFID Technology", *Proc. of Pervasive Computing and Communications Workshops (PerCom Workshops 2007)*, pp. 377-381, 2007.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOMW.2007.38&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Determining%20the%20Position%20and%20Orientation%20of%20Multi-Tagged%20Objects%20Using%20RFID%20Technology&rft.spage=377&rft.epage=381&rft.au=S.%20Hinske&rft.aulast=S.%20Hinske)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOMW.2007.38&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Determining%20the%20Position%20and%20Orientation%20of%20Multi-Tagged%20Objects%20Using%20RFID%20Technology&rft.spage=377&rft.epage=381&rft.au=S.%20Hinske&rft.aulast=S.%20Hinske)[Google Scholar](https://scholar.google.com/scholar?as_q=Determining+the+Position+and+Orientation+of+Multi-Tagged+Objects+Using+RFID+Technology&as_occt=title&hl=en&as_sdt=0%2C31)

**19.** G. Zecca, P. Couderc, M. Banatre, R. Beraldi, "Swarm robot synchronization using RFID tags", *Proc. of Pervasive Computing and Communications (PerCom 2009)*, pp. 1-4, 2009.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOM.2009.4912788&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Swarm%20robot%20synchronization%20using%20RFID%20tags&rft.spage=1&rft.epage=4&rft.au=G.%20Zecca&rft.aulast=G.%20Zecca)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOM.2009.4912788&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Swarm%20robot%20synchronization%20using%20RFID%20tags&rft.spage=1&rft.epage=4&rft.au=G.%20Zecca&rft.aulast=G.%20Zecca)[Google Scholar](https://scholar.google.com/scholar?as_q=Swarm+robot+synchronization+using+RFID+tags&as_occt=title&hl=en&as_sdt=0%2C31)

**20.** V.P. Munishwar, S. Singh, C. Mitchell, W. Xiaoshuang, K. Gopalan, N.B Abu-Ghazaleh, "RFID based localization for a miniaturized robotic platform for wireless protocols evaluation", *Proc. of Pervasive Computing and Communications (PerCom 2009)*, pp. 1-3, 2009.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOM.2009.4912794&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=RFID%20based%20localization%20for%20a%20miniaturized%20robotic%20platform%20for%20wireless%20protocols%20evaluation&rft.spage=1&rft.epage=3&rft.au=V.P.%20Munishwar&rft.aulast=V.P.%20Munishwar)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOM.2009.4912794&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=RFID%20based%20localization%20for%20a%20miniaturized%20robotic%20platform%20for%20wireless%20protocols%20evaluation&rft.spage=1&rft.epage=3&rft.au=V.P.%20Munishwar&rft.aulast=V.P.%20Munishwar)[Google Scholar](https://scholar.google.com/scholar?as_q=RFID+based+localization+for+a+miniaturized+robotic+platform+for+wireless+protocols+evaluation&as_occt=title&hl=en&as_sdt=0%2C31)

**21.** Ilic, F. Michahelles, E. Fleisch, "Dual ownership: access management for shared item information in RFID-enabled supply chains", *Proc. of Pervasive Computing and Communications Workshops (PerCom Workshops 2007)*, pp. 337-341, 2007.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Dual%20ownership:%20access%20management%20for%20shared%20item%20information%20in%20RFID-enabled%20supply%20chains&rft.spage=337&rft.epage=341&rft.au=Ilic,%20F.%20Michahelles&rft.aulast=Ilic,%20F.%20Michahelles)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=Dual%20ownership:%20access%20management%20for%20shared%20item%20information%20in%20RFID-enabled%20supply%20chains&rft.spage=337&rft.epage=341&rft.au=Ilic,%20F.%20Michahelles&rft.aulast=Ilic,%20F.%20Michahelles)[Google Scholar](https://scholar.google.com/scholar?as_q=Dual+ownership%3A+access+management+for+shared+item+information+in+RFID-enabled+supply+chains&as_occt=title&hl=en&as_sdt=0%2C31)

**22.** A. Saxena, S. Ganguly, S. Bhatnagar, R. Izmailov, "RFInD: an RFID-based system to manage virtual spaces", *Proc. of Pervasive Computing and Communications Workshops (PerCom Workshops 2007)*, pp. 382-387, 2007.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOMW.2007.99&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=RFInD:%20an%20RFID-based%20system%20to%20manage%20virtual%20spaces&rft.spage=382&rft.epage=387&rft.au=A.%20Saxena&rft.aulast=A.%20Saxena)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOMW.2007.99&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=RFInD:%20an%20RFID-based%20system%20to%20manage%20virtual%20spaces&rft.spage=382&rft.epage=387&rft.au=A.%20Saxena&rft.aulast=A.%20Saxena)[Google Scholar](https://scholar.google.com/scholar?as_q=RFInD%3A+an+RFID-based+system+to+manage+virtual+spaces&as_occt=title&hl=en&as_sdt=0%2C31)

**23.** L.M. Ni, L. Yunhao, C. L. Yiu, A.P. Patil, "LANDMARC: indoor location sensing using active RFID", *Proc. of Pervasive Computing and Communications (PerCom 2003)*, pp. 407-415, 2003.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOM.2003.1192765&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=LANDMARC:%20indoor%20location%20sensing%20using%20active%20RFID&rft.spage=407&rft.epage=415&rft.au=L.M.%20Ni&rft.aulast=L.M.%20Ni)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&rft_id=info:doi/10.1109/PERCOM.2003.1192765&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=LANDMARC:%20indoor%20location%20sensing%20using%20active%20RFID&rft.spage=407&rft.epage=415&rft.au=L.M.%20Ni&rft.aulast=L.M.%20Ni)[Google Scholar](https://scholar.google.com/scholar?as_q=LANDMARC%3A+indoor+location+sensing+using+active+RFID&as_occt=title&hl=en&as_sdt=0%2C31)

**24.** G. Roussos, V. Kostakos, "RFID in pervasive computing: ctate-of-the-art and outlook", *Pervasive and Mobile Comp.*, 2008.

 Show Context [[Findit@MU](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=RFID%20in%20pervasive%20computing:%20ctate-of-the-art%20and%20outlook&rft.au=G.%20Roussos&rft.aulast=G.%20Roussos)](http://libus.csd.mu.edu:4550/resserv?url_ver=Z39.88-2004&rfr_id=info:sid/IEEE.org:XPLORE&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.atitle=RFID%20in%20pervasive%20computing:%20ctate-of-the-art%20and%20outlook&rft.au=G.%20Roussos&rft.aulast=G.%20Roussos)[Google Scholar](https://scholar.google.com/scholar?as_q=RFID+in+pervasive+computing%3A+ctate-of-the-art+and+outlook&as_occt=title&hl=en&as_sdt=0%2C31)