Security Requirements for RFID Computing Systems

Xiaolan Zhang[1] and Brian King[2]
(Corresponding author: Xiaolan Zhang)

Coordinated Science Laboratory, University of Illinois[1]
Urbana-Champaign, IL, USA (Email: zhang_xiaolan@ieee.org)
Electrical & Comp. Engineering, Indiana Univ. Purdue Univ. Indianapolis[2]

(Received Mar. 27, 2006; revised and accepted May 25, 2006)

Abstract

Many security and privacy protocols for RFID systems have been proposed [8, 13, 19, 20]. In most cases these protocols are evaluated in terms of security based on some model. Often the model was introduced by the creator of the protocol, in some cases borrowing parameters from the protocol for model parameters. Moreover, the models that are discussed may represent only one aspect of the necessary security services that are needed in an RFID system. Here we describe several of the security requirements that are needed in an RFID system. Further, we model these requirements. These models incorporate security requirements that include privacy of tag data, privacy of ownership, and availability of tag identity. We also construct less restrictive versions of many of these models to reflect the security needed for some less security-intensive RFID applications. Finally, we compare our model to Juels' models [13], Avoine's models [4] and Ohkubo et al.'s models [20].

Keywords: RFID, one-time pad, security model

1 Introduction

Security models play an important role, for they provide tools which allows us to measure the security offered by protocols. Often models are developed as an immediate response to evaluate a protocol. The construction of the model could actually borrow parameters and ideas from the protocol that inspired the development of the model. Clearly security would benefit if there was a disconnect between the development of models and the development of protocols. Further, protocols are often developed for specific applications and may require several security services, thus requiring several security models. Consequently, independent development of a set of security models is essential. More important, RFID systems are utilized for economical reasons, the cost of the tags plays an important role in why the tags can be pervasively implemented. These tags have limited resources, one may be intending to use them as low-cost solutions for a low-cost problems. On the other hand, an RFID system may be used in high-security problems like anti-counterfeiting, pharmaceutical integrity, etc. Many of these applications require a high-level of security. Thus the application often will dictate the security level. So the best models would allow us to adjust the security parameters to fit our needs. Moreover, we should expect to see an increase in the use of RFID systems in the computing mainstream engaging in more sensitive areas. Further, an RFID system has a specific set of security vulnerabilities and so the models should address these vulnerabilities.

In this paper we describe a set of security requirements that are needed in an RFID system and model these requirements. They include privacy of tag data, privacy of ownership, and availability of tag identity. This paper is the complete version of our conference paper [30], including a complete description of our models, as well as three new models and many more examples.

2 Background

RFID stands for Radio Frequency IDentification. RFID tags are small integrated circuits connected to an antenna, which can respond to an interrogating RF signal with simple identifying information, or with more complex signals depending on the size of the IC. They usually have very little memory (around several Kbits), some of which are keyed read or write enabled such as Atmel e5561[3]. One classification is by source of power. Passive tags derive all their transmission and computation power from the RF signal. It is inexpensive and less powerful. Active tags have batteries and are more complex. Semi-active tags use batteries to run local circuitry and derive transmission power from reader's signal. They are able to communicate over a longer distance (over ten feet) than passive ones (just over a foot). A typical RFID system consists of a tag (transponder), a reader (transceiver), and some

means to process information, such as a computer. The reader queries the tag for some information. The tag then responds with the corresponding information. The reader then forwards the information to the data processing device via reader's network. The reader may be a handset device or a computer, which is capable of complex computations, such as public-key algorithm. An RFID system usually operates on 868-956 MHz or 13.56 MHz frequency band. The higher frequency tags have higher transmission range and smaller size. But they are easily blocked by the presence of liquid, intensive mass, even human beings. A RFID tag can respond to multiple readers and a reader can talk to thousands of tags. Their communication, in some applications, should be authenticated and confidential.

Originally, RFID tags were developed as a replacement for bar-codes, providing more efficient inventory over the traditional bar-code because of its remote accessibility. Many other applications are envisioned for RFID beyond the retailing store application. [24] explores the potential of RFID in anti-counterfeiting. Euro banknotes [28] may authenticated by RFID tags embedded in it. U.S. Food and Drug Administration (FDA) has considered using RFID tags to defend counterfeit pharmaceutical products [12]. Passports [18] and driver licenses are other potential uses of RFID for anti-counterfeiting. Hospitals may monitor the consumption of medicine by a patient, this can be achieved by monitoring the tags on bottle which record the name of the patient. As the number of applications grow, new functions and more requirements are imposed on RFID tags. Due to the constraints of current RFID tags, only limited security functions are available. For current RFID applications, as well as future applications, it is important to decide which functions are necessary to be implemented and what are the constraints based on current and/or near future tag technology, in order to drive the technology towards providing the necessary function for all applications.

There has already been a significant amount of discussion concerning the technology on future RFID tags [22], some of these tags will provide greater functionality. Such tags will have greater range and slightly more resources. If manufacturing costs can be contained, then we may find that these tags will be utilized within applications that are more mainstream, applications that will affect the consumer (bearer of the tags). Such applications will be much more sensitive and will require greater security services such as confidentiality, integrity and authentication and it will be even more important to protect the privacy of the consumer.

3 RFID Services and Security Requirements

3.1 Application Services

Generally, current and future RFID applications require one or more of the following of services which we have grouped into three categories: remote identification (tracking/tracing), authentication (anti-counterfeit) and data collection (sensor). Roughly all RFID applications utilize remote identification service which is the primary purpose of RFID tags. But some applications may also require authentication and/or data collection. Three security service groups are described as follows:

1) **Remote identification:** It refers to systems for which when a reader interrogates a tag for the identity and property information of the item this tag is associated with. The reader wants to remotely identify the item by querying the tag. Basically, the RFID tag plays a role as the identifier of items. Examples include: inventory management, distribution, in-store detection, automatic check out, stream-line monitor, Smart House, port inspection, etc.

2) **Authentication:** This is one of the basic tracking functions but applications in this category emphasize the need for authenticity of the identity that the RFID tag reports. It refers to systems where the reader interrogates a tag for verifying the information of the item. The reader may already know the information but may not be sure about its authenticity. RFID tag plays a supportive role to authenticate the information of the item. The information can be identity, origin or property of items. Examples of applications include RFID-enabled banknotes, pharmaceutical products, ID cards, passports, certificates.

3) **Data collection:** It refers to systems for which when a reader interrogates a tag, updated data is collected from the item. In this category, the reader already knows the item and previous data but wants to monitor the change in the data. Tags may be installed at some fixed position for a relatively long time to collect data. Sometimes an item may have many tags embedded in it and each tag may be responsible for a certain portion of data collection. Examples include product quality control, advertising notification, security alarm, sensors.

3.2 Security Requirements

Applications discussed previously indicate some of the functional goals that use RFID technology. However, simply integrating RFID technology into some of these applications will not ensure that the needed services are provided adequately, because many RFID systems operate in unknown or untrusted environments, for which adversaries motivated by different purposes may attack the

system. Some attacks may cause tags to return wrong information to readers. Some will block readers from hearing tags. Further, attackers may attempt to hide within a group of authorized users in an attempt to eavesdrop private information. Privacy is an issue that could hinder the wider use of RFID. For example [11] discusses the privacy concerns when using RFID to tag information goods where the secrecy of ownership is legally protected. Similar problems could occur in applications like banknotes, medicines, cloths, etc. In such situations if common items are tagged and actively queried in the mainstream, those parties that possess the tagged items will have their privacy compromised. Furthermore, privacy will become an even more important issue as RFID technology is pervasively applied [27]. To ensure a wider use of RFID technology, security must be included into any design of applications. In some systems one must make sure the communication between tags and readers is confidential and authenticated, in other systems the information in provided by the tags needs to be authenticated and in other systems the access (read or write) to the RFID systems, including tags, readers and other related equipment should be classified against unauthorized parties. Clearly securing an RFID system is a much greater challenge than many other digital systems because of several reasons.

1) Due to the size and cost limits of an RFID tag, they may not able to perform intense computations like public-key cryptography.

2) Tags may be subject to intense physical attacks, such as memory tampering, brute force password attacking or cloning.

3) The communication channels between tags and readers are insecure. Many common computer network attacks, such as eavesdropping, impersonating or DOS (denial-of-service), will possibly migrate to RFID systems.

4) Because the pervasive and invisible natures of tags, privacy protection becomes an important issue.

5) The goals of security, privacy, and performance are contradictory in many ways. The requirements for each application are different and it is hard to find a one-fits-all security model for all RFID systems.

In some specific applications, the level of security that is required may need to be as strong as the security required in a networked computing system. For example, consider an anti-counterfeit system, the loss of integrity of tag data will significantly undermine the trust of system. In such systems, low cost RFID tags should still be able to provide high integrity. How to implement RFID services together with necessary levels of security when designing a protocol becomes a complex problem.

A significant amount of research has focused on the security protocols for various RFID applications. Juels proposed an simple password scheme against cloning tag in [14]. Juels also provided a pseudonym throttling authentication protocol in [13]. Ranasinghe et al. [21] discussed the use of cryptography to solve RFID problems. Feldhofer [8, 9] proposed to use symmetric key encryption to provide authentication solutions. Ohkubo [20] suggested a hash based protocol and Avoine [5] improved its scalability. The Blocking scheme in [16] and kill tag method [1] are other approaches to achieve privacy. Some secure RFID solutions for future applications have been developed: [15] proposed a security model and a protocol for RFID enabled Euro banknotes, [6] presented a model of the lifecycle of RFID tags used in the retail sector and a solution through zero-knowledge protocols, and [19] focused on the security in RFID library systems. More recently [17], Juels and Weiss analyzed RFID security.

With many RFID protocols already designed, a question arises is how to evaluate those protocols. i.e. whether those protocols provide exactly the security as required. To solve this problem, we should first model RFID systems and define those security services for them. Many of the above authors provided a model to evaluate their protocol. The problem is that the protocol tends to be based for a specific application and the model often reflect this.

4 Formal Definitions

In this section, we describe mathematical models for several security services affected by or needing RFID technology. Identification is the most basic function in a remote tracking system. We first define *perfect identification* and later define *authorized perfect identification*. Later we will modify our definitions to define security models for RFID systems. Several RFID parameters are modeled and identification within a RFID system is formalized.

Our security models are constructed with access groups (authorization) in mind. Adversaries are considered as parties (readers) performing operations that they are not authorized for. Such operations can be: interleaving RF communication, querying a tag (impersonating an authorized reader), responding a reader (impersonating a valid tag), tampering a tag physically or performing DOS attacks by any means. Interleaving and querying is modeled as RF signals an adversary obtained from listening/eavesdropping RF communications. Further, adversaries may initiate a session or intercept a session. We consider cloning, disguising or tampering tag problem as an integrity problem. Integrity also deals with the problem concerning readers authenticating tags. In a seperate work [29], we discussed an integrity model. In our model, we required that an authorized reader will be able to determine the authenticity of tags with a high probability. For an authorized party, the tag should always be available to be identified.

In an applied RFID system, since a tag's resources are limited, it is unfair and impractical to require tags to defend against adversaries with unlimited resources.

In our RFID security models, security requirements are conditioned on tag resources and an assumed bound on the adversarial resources as well. We assume adversaries have limited accesses to a tag and computational powers, which are represented by parameters that differ from applications. Our definitions are used to model an RFID system requiring security based on a resource constrained adversary.

4.1 Definition of Identification of Tag Identity

We now consider a model for a general remote identification system. We use the term *item* to represent a physical object that will be remotely identified. It can be money, medicine or cloths. It is the authentic individual information, such as identification number, name, origin, property, distribution pedigree, etc. It is conceptual and physically unalterable. A Toshiba laptop CR300 is an example. Even if someone alters the manufacturer identification on its label or tag to be an IBM laptop T43, the item is still a Toshiba laptop CR300. The goal is to track the authentic identity of an item. *Tag* is the concept used to denote a labelling, it provides information about the item associating with it in form of remote signals. *Identity* is the remote identification information for which the queried tag responds with. *Reader* is a device that receives some/none/all information transmitted from a tag. When a reader queries a tag, the information revealed is the identity but not the item. *Authorized party* is a group of people or organizations that are granted certain permissions to access the identity of an item from remote access. Since any individual in a party accesses a tag through a reader, the reader represents and implements the authorization of its user. For integrity, some data can only be modified by authorized parties, and parties authorized for some tags should be able to recognize the authenticity of this data.

Channel is the source that a tag uses to send information. There are two information channels: public and secret. The two channels are designed to deliver data such that when both channels of information are collected by an authorized party, it provides the desired authenticated identity. The information that the channels provide will vary depending on the authorization group (authorized or unauthorized) the reader belongs to. Informally, we characterize this as a "view" of signals. Given the same channel of the tag at the same time, readers in different authorized groups may have different views of it. We make no formal requirement as to how information is delivered via the secret channel, it could take many forms, for example it could take the form of a ciphertext, or it could take the form of a physical communication that is not available without secret key. In addition to the two remote RF channels of information, the reader could obtain additional information from a third channel when communicating with the tag. For example, the location where the signal is received. The content of this information has a level of uncertainty and varies depending on the situational-aspects of the communication. We define the *environmental channel* as the channel that delivers side information about the tagged item and we will assume that environmental channel itself reveals little information that one can use for identification. Remember that our focus is to construct models to analyze security protocols that are used over remote communication. If the environmental channel alone has provided enough information for identification, it would be meaningless to analyze the security of the protocol as used over the two remote channels. Although the environmental channel exists and can provide identification in real world applications, we carefully construct our models so they do not criticize protocols (during their evaluation) which only yields information where the source comes solely from the environmental channel.

The mathematical model is probabilistic. Our initial definitions are device independent. Later we consider the implication of the limitations of the tag, so then the definitions will incorporate the limited resources. Some variables are defined as follows:

I is a random variable of the identity of a tagged item. It represents any or all of the data pertaining to the tagged item (representation depends on the application).

Θ is a random variable of the information received from an access to the tagged item. It is a tuple of information from three channels $< U, V, W >$. U is the variable representing the remote information received from a public channel. V represents remote information received from a secret channel. The environment channel W is usually omitted if it is not explicitly discussed.

$\mathcal{I}$ the set of all possible tagged items.

$\mathcal{AR}_i$ the set of parties authorized to obtain the true identity information of item $i \in \mathcal{I}$.

For the identification security model, a suitable level of integrity is assumed. Therefore tag data is authenticated and trusted to represent the identity of the physical item. There is no need to distinguish the terms "item" and "identity".

We say that a protocol is able to identify an item from the tag if the protocol provides identification of the tag from the remote information. Ideally, if a protocol provides the reader the ability to recognize the item with a probability near 1 given the correct remote information and near 0 given the incorrect information, we would consider this identification protocol reliable and accurate. Throughout this paper we will use $\theta =< u, v >$ to represent the correct information of item i, where u belongs to variable U in tuple Θ and v to V. We will use θ' to represent an incorrect information of i. The first equation

defines the availability of identification and the second defines the correctness in the ideal situation. It is modelled after perfect secrecy.

Definition 1 (Perfect Identification of tag Identity (PII)). *A protocol satisfies PII has the property that: (1) a party is able to identify an item i given its correct tag information,* $\Pr(I = i|\Theta = \theta) = 1$. *(2) a party cannot identify i given the incorrect tag information θ',* $\Pr(I = i|\Theta = \theta') = 0$.

In real world applications, perfect identification will most likely not exist because several factors affect the probability. Hardware failure, inconsistent power supplies, or transmission errors may cause a reader to accept or reject a tag incorrectly. The probability in the first equation defines the tolerance of tag acceptance errors and the one in the second equation defines the tolerance of tag rejection errors. For RFID applications, the tolerance in model can be adjusted to fit different requirements. This will be discussed in Section 5. On the other hand, the perfect identification model is not sufficient to describe many applications. Security conditions should be added. Perfect identification is the first step for constructing other definitions that are needed. One of them is *authorized identification*. In remote tracking systems, the security services are provided for authorized parties. Intuitively, it means two things: one is that only a certain group of authorized readers are able to remotely recognize the identity of an item correctly. Another is that unauthorized readers are given so little information about the item that they cannot distinguish it from others remotely. Obviously an authorized reader should be able to identify an item with perfect identification. But given an unauthorized reader, the remote information should not provide any information that improves the chance of identification better than guessing the identity of the item. You can always guess an item based on your knowledge but the remote information should not provide any help. The second part of the definition of perfect authorized identification has constructed to be sufficiently strong, in the sense that an unauthorized reader cannot identify an item better than guessing even when provided a history. The "history" is a finite collection of pairs of information and results obtained from prior remote accesses[1] of a party. For simplicity, we assume that the membership of a reader does not change in one history. A more complex model of various membership history will be discussed in future work.

$\eta(\cdot)$ is a set representing the history information for a party. It consists of finite number of tuples $\{< \Theta(\cdot), J(\cdot) >\}^*$. [2] $J(\cdot)$ represents the result obtained from access the channel $\Theta(\cdot)$ [3]. It is the set of data of the identification information and maintains that $J(\cdot) \in \mathcal{I}$.

A secure protocol will depend on history. If an adversary has unbounded accesses to RFID tags, it may be impractical to expect that the protocol is impervious to attacks. The following definition consists of two parts. The first part states that authorized parties possess perfect identification. It requires availability and correctness for identification. The second states that the remote information does not improve the identification of tag identification for an unauthorized party. It defines the adversary advantage for identification, i.e. the likelihood that one can identify the item with remote information will be the same as without the remote information. Otherwise, the party is able to identify it. The history here is $\eta(\cdot) = \{< \theta_1(\cdot), j_1(\cdot) >, < \theta_2(\cdot), j_2(\cdot) >, \cdots, < \theta_k(\cdot), j_k(\cdot) >\}$. We write $|\eta(\cdot)| = k$ to be the size of history. The size of history is a security parameter. We should point out that our Definition 2 only considers adversaries whose access history is bounded by κ (here κ is a nonnegative integer). That is, if a given protocol allows an unauthorized adversary to be able to identify the tag identification using a history of length κ or less, then that protocol violates our model. However, if the number of history accesses exceeds κ, then the model is indifferent to whether such adversaries should be able to identify the tag identification.

Definition 2 (Authorized Perfect Identification of tag Identity with κ-history (κAPII)). *A protocol satisfies κAPII provided that:*

1) If α is an authorized party of item i, then α has perfect identification of i.

$$\begin{aligned} \Pr(I = i|\Theta = \theta, \alpha \in \mathcal{AR}_i) &= 1 \\ \Pr(I = i|\Theta = \theta', \alpha \in \mathcal{AR}_i) &= 0, \end{aligned}$$

2) or any party α whose access history $\eta(\alpha)$ satisfies that $|\eta(\alpha)| \leq \kappa$, and is NOT an authorized party of i, does not have better chance to identify the item i given any θ'' that is not a correct signal of any tag that party α is authorized for,

$$\begin{aligned} &\Pr(I = i|\Theta = \theta'', \eta(\alpha), \alpha \notin \mathcal{AR}_i) \\ &= \Pr(I = i|\eta(\alpha), \alpha \notin \mathcal{AR}_i). \end{aligned}$$

The above equation states that the probability of party α to identify i will not improve with the current RF channel access. Furthermore this equation addresses the ability of α to use prior accesses to mine information. We know that history may help identification, since history

[1] The access may be such that another part is actually making the query and this party is merely eavesdropping.

[2] In this article, $\cdot$ denotes a specific party. The history of party α would be written as $\eta(\alpha)$.

[3] In the history, $\Theta(\cdot)$ will be represented using all three channels because past results may be determined together with the information from the environmental channel as well. Although we do not have assumption that W channel contains no identification information over past accesses. But we have that assumption thus do not consider that channel for the current access.

includes the knowledge you possess. Basically, a protocol cannot control the source of previous knowledge. Because history includes the environmental channel, the result (identification) may be obtained through social engineering. The model is constructed so that it will evaluate the security of a protocol based on the current channel not how history will help identification.

If a protocol designer sets the parameter $\kappa = 0$ within the security model, then they assume that an adversary does not memorize previous tag accesses. Observe that a statically encrypted ciphertext transmitted from a tag will be secure enough to prevent tracking in the sense that the adversary cannot compare any previous ciphertexts to the current one. Under the model with the assumption that an adversary does not memorize tag accesses, even if the ciphertext does not change, the encryption will appear like a one-time-pad to an adversary. In another model, if we set $\kappa > 0$, then a protocol secure in this model must withstand an adversary who is allowed to have κ recordable previous accesses. We must make sure that any encryption algorithm we choose to encrypt the tag should be secure against chosen ciphertext attack of κ ciphertext-plaintext pairs, or an adversary will have a chance to break the encryption after acquired a history of κ length. Usually, the history size in the model is set higher if the mobility of tags is lower, since a reader has more chances to access the same tag. The history size can be safely lowered if tags have much greater mobility than a reader, since the reader is less likely to encounter the same tag again. Moreover, if the application requires stronger privacy of tag identification, then one should increase the κ parameter.

In many applications, we are not only concerned with the information concerning a single item that an unauthorized party can gather from an access, but also we are concerned with is whether this adversarial party can distinguish two items without necessarily identifying their identities. Remember if an unauthorized party can distinguish item i from other items, then it is a serious violation of privacy. Indistinguishability is an important security property when we analyze applications. It is derived directly from the definition of authorized identification.

Definition 3 (Indistinguishability of tag Identity with κ-history (κINDI)). *A protocol satisfies κINDI provided that: for any party α whose access history $\eta(\alpha)$ satisfies that $|\eta(\alpha)| \leq \kappa$, if α is an unauthorized party for items i and i', then α cannot distinguish item i from i'.*

$$\forall i' \in \mathcal{I} \quad , \Pr(I = i' | \Theta = \theta, \eta(\alpha), \alpha \notin \mathcal{AR}_i \cup \mathcal{AR}_{i'}) = \Pr(I = i' | \eta(\alpha), \alpha \notin \mathcal{AR}_i \cup \mathcal{AR}_{i'}).$$

Theorem 1. *If a protocol satisfies κAPII then it satisfies κINDI.*

This result is trivial to establish.

4.2 Definition of Identification of Tag Ownership (the Bearer of the Tag)

In an application, some side information is itself enough to violate bearer privacy. That is, you may be able identify and distinguish bearers even if you do not know the identity of an item. For example, Alice has an RFID tagged purse and she always brings it with her. The purse is broadcasting its static encrypted identification number to any reader. Only Alice's reader has the decryption key. Betty is Alice's competitor. She once used her reader to get the ciphertext. Although she could not decrypt it, she recognized it as a purse, and she was able to determine that it was from Alice. Next time, she captured that ciphertext outside a local store. She was able to determine that Alice was shopping at that store.

Attacks on the confidentiality of bearers could be unauthorized tracking of either an bearer or transaction between two bearers (depending on if the bearer of the tag has just changed). To understand the problem of tracking, one should first consider the identification of a bearer.

O is a random variable as the bearer of item i.

$\mathcal{O}$ is a set of all bearers or owners.

A bearer's information may be available to the adversary in two possible ways.

1) One way is that the bearer information is included as part of the tag identification information. Remember that identification information i, as we have defined earlier, is a set of all data pertaining to a tagged item. Thus, in this case, the security/privacy of the bearer has already incorporated into the analysis of the perfect identification of tag information. For this case, the bearer o of i should satisfy the following equation as a precondition which implies the incorporation of bearer's information in the identification information.

$$\Pr(I = i) \leq \Pr(O = o).$$

2) The other case is such that the bearer is not included as part of the tag identification. Thus, the bearer's information is obtained from RF channels together with the environmental channel. It is possible that the bearer may be derived totally from environmental channel as a social engineering attack. Since the security model will be used to measure the effectiveness of a protocol, the model should reflect the violation of the privacy of a bearer due to the use of both RF and environmental channels. However, a protocol cannot prevent a stand alone successful social engineering attack. Thus in this second case, we assume the environmental channel only provides partial information about the bearer but not all. The party is able to get information from channels $\theta =< u, v, w >$ (this includes the environmental channel w, on condition that the environmental channel only provides partial information about the bearers). To this end

$$\forall o \in \mathcal{O}, 0 \leq \Pr(O = o | \Theta =< w >, \eta(\alpha), \alpha \notin \mathcal{AR}_i) < 1.$$

Observe our use of $\Theta =< w >$, this implies that the only channel considered is the environmental channel, i.e. one is only being provided information from the environmental channel.

Definition 4 (Authorized Perfect Identification of tag Bearers with κ-history (κAPIB)). *A protocol satisfies κAPIB provided that:*

1) *All parties α authorized for item i have perfect identification of bearers o.*

$$\Pr(O = o|\Theta = \theta, \alpha \in \mathcal{AR}_i) = 1 \quad (1)$$
$$\Pr(O = o|\Theta = \theta', \alpha \in \mathcal{AR}_i) = 0. \quad (2)$$

2) *All parties α whose access history $\eta(\alpha)$ satisfies that $|\eta(\alpha)| \leq \kappa$, and is NOT authorized for item i should not have better chance to identify the item i, given any $\theta'' =< u'', v'', w'' >$ that is not a correct information of any tag the party authorized for,*

$$\Pr(O = o|\Theta = \theta'', \eta(\alpha), \alpha \notin \mathcal{AR}_i) = \Pr(O = o|\Theta =< w'' >, \eta(\alpha), \alpha \notin \mathcal{AR}_i). \quad (3)$$

Equation (1) implies that authorized readers with correct signal can identify bearers, whereas Equation (2) states that authorized readers with an incorrect signal will not incorrectly identify bearers. Equation (3) implies that unauthorized readers with any signal that they are not authorized for and possess a history of accesses which is bounded by κ have no better chance of identifying the bearer than if they possess a history of accesses which is bounded by κ and a signal consisting solely of the environmental channel.

One can define Indistinguishability of Tag Bearers with κ-history (κINDB), much like we defined Indistinguishability of Tag Identity with κ-history (κINDI).

Definition 5 (Indistinguishability of tag Bearers with κ-history (κINDB)). *A protocol satisfies κINDB provided that: for any party α whose access history $\eta(\alpha)$ satisfies that $|\eta(\alpha)| \leq \kappa$, and is not authorized for item i and item i' (i' can be the same as i) cannot distinguish the bearers o of i from o' of i'*

$$\Pr(O = o'|\Theta = \theta, \eta(\alpha), \alpha \notin \mathcal{AR}_i \cup \mathcal{AR}_{i'}) = \Pr(O = o'|\eta(\alpha), \alpha \notin \mathcal{AR}_i \cup \mathcal{AR}_{i'}) \quad \forall i' \in \mathcal{I}.$$

5 Security Model for RFID Systems

RFID system imposes additional constraints on tracking. An RFID tag has physical limitations and application constraints. Some of these limitations will enhance the security but others will undermine it. It is not fair to require perfect authorized identification and integrity for all RFID systems. One needs to consider the RFID limitations, and incorporate the limitations within the definition of security services for RFID. First we define:

Tag's access limitation: $\phi_{Ta}(\cdot) =< D_T, B_T(\cdot) >$

D_T the reader's range (meters).

$B_T(\cdot)$ resource bound for readers. It is a tuple, one for readability $R_b(\cdot)$, one for writability $W_b(\cdot)$ and another for computational power $C_b(\cdot)$ (number of gates). Readability is the maximal number of inquiries that a party is allowed to utilize on a tag. Writability is the maximal size of memory that a party is allowed to make to one tag. $\forall \alpha \in \mathcal{AR}_T, R_b(\alpha) = \infty, C_b(\alpha) = \infty$, $\forall \alpha \in \mathcal{AW}_T, W_b(\alpha) =$ modifiable size for this party, $C_b(\alpha) = \infty$. Otherwise $R_b(\alpha), W_b(\alpha), C_b(\alpha)$ are some fixed value.

Tag's resource: $\phi_{Ts} =< P_T, C_T, M_T >$.

P_T the physical condition (boolean). '0' means that it is physically unremoveable from the host item. '1' means removeable.

C_T the computational power limitation (number of gates).

M_T the memory limitation (number of bits).

For most tags, D_T will be a few meters (often this limitation D_T is used as a mechanism that prevents eavesdropping). P_T is assumed to be 0. C_T is often limited to 400-4000 of gates (this hardly meets the requirements to allow one to use symmetric key encryption). M_T is around 1Kbits.

Given a fixed tag, readers may access the tag in various conditions. We define reader's access limitation as a tuple of distance and resources to one tag. $\phi_r(\cdot) =< D, B(\cdot) >$. Our definition is satisfied whenever the reader's access limitation is smaller than tag's. For authorized readers, their B will be always smaller than B_T. However, for unauthorized readers, their B is some set of resources that are mostly affected by money and time available to an adversary. Due to the cost-limitation of tags, it is almost impossible to design a protocol resistant to adversaries with unlimited resource.

In a real-world application, many other factors may affect the ability to recognize an item correctly, such as encryption errors, communication errors, and hardware errors. However, if these errors occur with a small probability, then a final decision would be correct according to an acceptable error rate. Define δ be the acceptable error tolerance for an authorized party to accept an incorrect tag. Define ϵ be the rejection error tolerance for an authorized party to reject a correct tag. Similarly, a system could still be considered secure, if the maximum advantage an unauthorized party can gain to identify a tag is acceptably small. Define γ to be the maximal adversary advantage that an unauthorized party is allowed to obtain to identify a tag correctly. δ, ϵ, γ are small nonnegative numbers between 0 and 1 (including the endpoints),

and the choice of these parameters depend on the application. Our previous security models are now modified to incorporate those parameters.

Suppose the tag of an item i has limitations $\phi_{Ta}(\cdot) =< D_T, B_T(\cdot) >, \phi_{Ts} =< P_T, C_T, M_T >$. The party has a history $\eta(\alpha) = \{< \theta_1(\alpha), j_1(\alpha) >, < \theta_2(\alpha), j_2(\alpha) >, \cdots, < \theta_k(\alpha), j_k(\alpha) >\}$.

Definition 6 ($(\delta, \epsilon, \gamma, \kappa)$ RFID APII). *An RFID protocol satisfies $(\delta, \epsilon, \gamma, \kappa)$ APII provided that:*

1) An authorized party α of item i has perfect identification.

$$\Pr(I = i|\Theta = \theta\, \phi_r(\alpha) \leq \phi_{Ta}(\alpha), \phi_{Ts}, \alpha \in \mathcal{AR}_i) \geq 1 - \delta$$
$$\Pr(I = i|\Theta = \theta', \phi_r(\alpha) \leq \phi_{Ta}(\alpha), \phi_{Ts}, \alpha \in \mathcal{AR}_i) \leq \epsilon.$$

2) For all parties α whose access history $\eta(\alpha)$ satisfies that $|\eta(\alpha)| \leq \kappa$, and is not authorized for item i, α does not have better chance to identify the item i, given θ'' that is not a correct signal of any tag that party α is authorized for,

$$\Pr(I = i|\Theta = \theta'', \eta(\alpha), \phi_r(\alpha) \leq \phi_{Ta}(\alpha), \phi_{Ts}, \alpha \notin \mathcal{AR}_i) \leq \Pr(I = i|\eta(\alpha), \alpha \notin \mathcal{AR}_i) + \gamma.$$

Similarly, indistinguishability of tag identity in RFID can be introduced.

Definition 7 ((γ, κ)RFID INDI). *An RFID protocol satisfies (γ, κ) INDI provided that: for any party α whose access history $\eta(\alpha)$ satisfies that $|\eta(\alpha)| \leq \kappa$, and is not an authorized party α of item i or any item i' (i' can be the same as i) cannot distinguish item i from i'*

$$\begin{aligned} & \Pr(I = i'|\Theta = \theta, \eta(\alpha), \phi_r(\alpha) \\ \leq\ & \phi_{Ta}(\alpha), \phi_{Ts}, \alpha \notin \mathcal{AR}_i \cup \mathcal{AR}_{i'}) \\ \leq\ & \Pr(I = i'|\eta(\alpha), \alpha \notin \mathcal{AR}_i \cup \mathcal{AR}_{i'}) + \gamma \qquad \forall i' \in \mathcal{I}. \end{aligned}$$

We now consider the privacy of the bearer.

Definition 8 ($(\delta, \epsilon, \gamma, \kappa)$ RFID APIB). *An RFID protocol satisfies $(\delta, \epsilon, \gamma, \kappa)$ APIB provided that:*

1) An authorized party α of item i has perfect identification of bearers o.

$$\Pr(O = o|\Theta = \theta, \phi_r(\alpha) \leq \phi_{Ta}(\alpha), \phi_{Ts}, \alpha \in \mathcal{AR}_i) \geq 1 - \delta$$
$$\Pr(O = o|\Theta = \theta', \phi_r(\alpha) \leq \phi_{Ta}(\alpha), \phi_{Ts}, \alpha \in \mathcal{AR}_i) \leq \epsilon.$$

2) For all parties α whose access history $\eta(\alpha)$ satisfies that $|\eta(\alpha)| \leq \kappa$, and is not authorized for item i does not have better chance to identify the bearer o, given $\theta'' =< u'', v'', w'' >$ that is not a correct information of any tag that party α is authorized for,

$$\begin{aligned} & \Pr(O = o|\Theta = \theta'', \eta(\alpha), \phi_r(\alpha) \\ \leq\ & \phi_{Ta}(\alpha), \phi_{Ts}, \alpha \notin \mathcal{AR}_i) \\ \leq\ & \Pr(O = o|\Theta =< w'' >, \eta(\alpha), \alpha \notin \mathcal{AR}_i) + \gamma. \end{aligned}$$

Similarly we can define (γ, κ) indistinguishability of bearers.

Definition 9 ((γ, κ)RFID INDB). *An RFID protocol satisfies (γ, κ)INDB provided that: for any party α whose access history $\eta(\alpha)$ satisfies that $|\eta(\alpha)| \leq \kappa$, and is not an authorized party of item i or any item i' (i' can be the same as i) cannot distinguish the bearers o of i from o' of i':*

$$\begin{aligned} & \Pr(O = o'|\Theta = \theta, \eta(\alpha), \phi_r(\alpha) \\ \leq\ & \phi_{Ta}(\alpha), \phi_{Ts}, \alpha \notin \mathcal{AR}_i \cup \mathcal{AR}_{i'}) \\ \leq\ & \Pr(O = o'|\eta(\alpha), \alpha \notin \mathcal{AR}_i \cup \mathcal{AR}_{i'}) + \gamma \qquad \forall i' \in \mathcal{I}. \end{aligned}$$

Errors are usually caused by hardware failures, weak power supply, or poor transmission. Low quality hardware of tags or readers, high mobility during communication, electromagnetic noisy environment can all increase the error rate. According to [25], tag read or write error rate may range from 0% in a controlled environment to exceeding 5% in a non-controlled environment. On the other hand, some protocols are probabilistic. i.e. They derive a correct result with a certain probability. Error tolerance should vary depending on applications. δ determines the error tolerance for tag acceptance. If a system is very restrictive in accepting tags correctly, then δ should be set smaller in the model. ϵ is the error tolerance for rejection. If a system requires that rejection only occurs when their is clear evidence of improper tag information then ϵ would be smaller. γ is the security bound for adversary advantage. If a system requires higher privacy, γ should be reduced. These parameters in our model should be chosen independently for each system and becomes a guideline that helps determine the quality of hardware, communication environment and algorithm used in protocols.

In the following we provide several examples demonstrating how to apply the apply parameter configuration within our models to assess security of protocols. We assume, within these examples, the hardware, software and all communications are 100% reliable, since our immediate focus is to assess the security protocol only.

Example 1. (Static and cleartext on tag)

> *Data is stored on a tag in cleartext with read-only. This is the most commonly used RFID technology today. When a reader interrogates a tag, the tag simply responds with its data.*

Let's consider several different ways to assess the protocol. First, suppose one assigns $\delta, \epsilon, \gamma, \kappa$ to all be zero. The implication of these assignments are as follows: The model for RFID system does not allow errors (with respect to rejection nor acceptance), the model for RFID system does not allow an adversarial advantage, and the model for RFID system is oblivious to prior communications and attempts of communication (i.e. history). The ignoring of any history, implies that the designers, who would have selected these parameter requirements based

on the application, have high confidence that, in their application of the RFID system, history poses no security risk. If there exist unauthorized readers, then the protocol violates (0, 0, 0, 0)RFID APII since every reader (authorized or unauthorized) is able to get the cleartext data to identify the tag. However, if the bearer's information is not included in the identity, the protocol is secure for (0, 0, 0, 0)RFID APIB because there is no way for an unauthorized reader to track tags or users without previous access record. If we assign κ to be one, then the protocol will no longer be secure for (0, 0, 0, 1)RFID APIB because they can track tags or users based on the static data on tag. If we assign δ to be one or ϵ to be one, then the model does not allow authorized readers to identify or reject a tag correctly. The protocol will never satisfy (1, 0, 0, 0)RFID APII or (0, 1, 0, 0)RFID APII because an authorized user can identify or reject a tag correct. If we assign γ to be one, then the protocol always satisfies (0, 0, 1, 1)RFID APIB because the system allows unauthorized readers to identity a tag by 100% accuracy which is exactly what the protocol has provided.

Example 2. (Static one-time-pad encrypted ciphertext on tag)

> *Data is stored in static ciphertext by one-time-pad encryption. The decryption key is delivered to the authorized parties in a secure manner. When a reader interrogates a tag, a tag simply replies with the ciphertext.*

The protocol satisfies (0, 0, 0, k)RFID APII for all $k \geq 0$ because unauthorized readers cannot decrypt the ciphertext to identify the tag whatever number of history they have. But this protocol is insecure in terms of protecting the bearer's privacy. The protocol does not satisfy (0, 0, 0, 1)RFID APIB because the ciphertext is static and could be used to track.

Example 3. (One-time-pad re-encrypted ciphertext on tag)

> *We now consider the case where the tag data is modified by a cryptographic tool called re-encryption [15]. The ciphertext stored on tag is refreshed by encrypting the plaintext with a new randomly chosen key. The protocol is: Data is stored in ciphertext by one-time-pad encryption. The decryption key is assumed to be delivered to the authorized parties securely. When a reader interrogates a tag, a tag simply replies the ciphertext. After each access, the ciphertext is re-encrypted, by a new randomly chosen key.*

The protocol satisfies (0, 0, 0, k)RFID APII for all k because unauthorized readers cannot decrypt the ciphertext to identify the tag whatever number of history she has. This protocol satisfies (0, 0, 0, k)RFID APIB for all k because the ciphertext appears new to an unauthorized reader in every access. One problem that must be overcome to use this protocol is how will future readers know what the latest key is. This can be solved if the number of authorized readers that require the key is small, in particular if it is one. A solution that can be used when the number of authorized readers is sufficiently large, the reader who selected the latest re-encryption key, can store this key on the tag by encrypting it with a public key and storing the ciphertext on the tag. The collection of authorized readers would need to share the corresponding private-key. However, key distribution and re-encryption protocols will incur many security problems related to integrity which may undermine the overall security of the protocol [29].

Example 4. (Password protection of tag data by authorized parties)

> *Suppose that the tag data is password protected. The problem is that the password must be transmitted over the RF channel. There are several possible ways to handle this. (i) First suppose that the transmission is made over an unencrypted channel. (ii) Second, suppose we encrypt the channel using a fixed channel key, which is delivered securely to all authorized parties. (iii) Third, suppose that during manufacturing, the manufacturer has prestored k keys, and that the order of the keys order has been set. When the tag is queried with a encrypted password, it will use the current key and then will toggle the next key to be set as the current key.*

Clearly Example 4.-(i) does not satisfy (0,0,0,0)APII since the password is transmitted in the clear. This is a common mechanisms that is used today, the argument for its use is that the D_T distance in ϕ_{Ta}, is limited, thus eavesdropping is limited. For example, suppose that the application has been analyzed, and due to the mobility of the tags, authorized readers and the distance D_T, the protocol designers have modeled the probability of an unauthorized reader being able to get within D_T communication distance between an authorized reader and tag to be q_1. Then the protocol satisfies $(0, 0, q_1, 0, 0)$APII. Example 4.-(ii) will violate (0,0,0,0)APIB since the key is fixed. Consequently the encrypted password forms a static ciphertext that allows the tracing of the bearer. The analysis for Example 4.-(iii) is slightly more complex then the above. if one assumes that an adversary has stored κ accesses where $\kappa \geq k$ and one assumes that the accesses are such that each of the prestored keys was equally likely stored then clearly this protocol would violate (0,0,0,κ)APIB. For the case where κ satisfies $0 < \kappa < k$, and again one assumes that each of the k keys were equally likely to be accessed as the current key, then clearly we would still violate (0,0,0,κ)APIB. This protocol would only satisfy the security model of (0,0,γ,κ)APIB where γ is suitably large enough.

Example 5. (Integrity)

> *[15] described a RFID enabled banknote protocol that uses the RFID tag to allow law enforce-*

ment to trace banknotes while at the same time trying to preserve the privacy of the bearer. In [29] it was shown that if all parties possessed the reader (capable of performing all functions used in the protocol), then there exists an attack on the banknote protocol [15]. This attack would allow an adversary to maliciously substitute alternate banknote information into any given banknote, which would fool law enforcement. Here law enforcement is an authorized party. Thus this protocol does NOT satisfy $(0, \rho, 0, 0)$*APII for all* ρ *satisfying* $0 < \rho < 1$.

Example 6. (CCA2 resistant within m-ciphertext-plaintext pairs cryptosystem re-encrypted ciphertext on tag) *Suppose the cryptosystem is resistant to adaptive chosen ciphertext attack (CCA2) if at most m ciphertext-plaintext pairs are obtained. However, if more than m pairs are obtained by the adversary, let's assume that the cryptosystem can be broken with some probability, which we demote by* p_1.

Data is stored in ciphertext encrypted by the cryptosystem described above. The decryption key is assumed to be delivered to authorize parties safely. When a reader interrogates a tag, a tag simply replies with the ciphertext. After each access, the ciphertext is re-encrypted. Assume that re-encryption process is secure and the collision of key is ineligible.

The protocol satisfies (0, 0, 0, k)RFID APII for $k \leq m - 1$ *because unauthorized readers cannot decrypt the ciphertext to identify the tag whatever number of history she has. But this protocol is weakened if the adversary is allowed to record more accesses. For* $k > m - 1$, *the protocol does not satisfy (0, 0, 0, k)RFID APII because the ciphertext could be broken in a probability of* p_1. *However, if the system allows at most* $p_1 + \rho$, *for some* $\rho > 0$, *adversary advantage, then the protocol will satisfy (0, 0,* $p_1 + \rho$, *k)RFID APII for all k because the probability of breaking the ciphertext is tolerated by the system. Similarly, the protocol satisfies (0, 0, 0, k)RFID APII for* $k \leq m - 1$ *or (0, 0,* $p_1 + \rho$, *k) for all k.*

Example 7. (Atmel e5561 [3] security) *Atmel e5561 is a standard read/write crypto identification tag. It provides password read/write protection and challenge response authentication by AUT64 crypto algorithm. First, we discuss the password function:*

The password function is a protection mechanism to prevent a reader from reading or writing data blocks of the e5561 memory without knowing the password. The reader needs to send password before enabling any other operations. They use a 28bit static password for each tag.

This protection is fairly insecure because a static password could be stolen or replayed to identify the same tag. However, for applications which require low security, our model could be configured low to meet the standard. Obviously, the protocol satisfies (0, 0, 0, 0)RFID APII and (0, 0, 0, 0)RFID APIB. It does not satisfy (0, 0, 0, 1)RFID APII or APIB because the old password can be used to identify or track the tag.
We now discuss the challenge response authentication used by a reader to authenticate tags:

The tag and the authorized reader share the cryptographic key for the symmetric encryption algorithm AUT64. We assume the level of security of AUT64 is high. As the tag sends its identification to the reader, the reader will generate a challenge by encrypting a random number with the tag's encryption key. After the tag receives the challenge, it will decrypt it and transmit the checksum of plaintext. Then, both the reader and the tag will take the plaintext as input value to AUT64 to calculate the response. When the tag finished calculation, it will transmit the response back to the reader. The reader will compare the response with its own calculation to determine the authenticity of the tag.

Unauthorized readers need to identify an authenticate tag. Therefore, they need to authenticate the tag even if the tag has already sent out its identification. Unauthorized readers don't have the correct encryption for the tag so they cannot generate a correct challenge. However, if they are able to eavesdrop a session between the tag and an authorized reader, they could authenticate the tag by replaying the challenge and check the response since the tag will always provide the same response to the same challenge. Like password protection, AUT64 authentication protocol becomes viewed as weak by the formal models as the size of history grows.

6 Previous Work and Comparison

Juels developed models for authentication security and privacy in [13]. Ohkubo et al. [20] proposed two security requirements for RFID systems: indistinguishability and forward security. Avoine defined existential and universal untraceability under five kinds of oracle access modes [4] and derived logical implications among them. In some ways Juels' models, Ohkubo's models, Avoine's models and our models are very similar, but they are different in many aspects like building blocks, adversary assumptions and security services provided. We will compare and discuss the merits of each work in this section.

Juels' model focuses on defining the advantage of adversaries in tag authentication and privacy attacks. Similarly, Ohkubo's model also defines the advantage of adversaries in indistinguishability and forward security. Avoine's model has named his work, adversary model, in the title. Their work focused on finding the adversary advantage of various security problems. However, definitions in our model cover availability, and confidentiality

Table 1: Compare security services between models

	Juels' model [13]	Ohkubo et al. model [20]	Avoine's model [4]	Ours model
Availability of tag identities	NP	NP	NP	P
Indistinguishability of tags via RF access only	P	P	P	P
Indistinguishability of tags via RF and environmental access	NP	NP	P	P
Indistinguishability of a tag from random variable via RF access	NP	P	NP	NP
Bearer's privacy	NP	NP	NP	P
Considers resource limitations	P	NP	P	P

Note: NP stands for "not provided". P stands for "provided".

services that may provide in a RFID protocol. The security goal in Juels', Ohkubo's and Avoine's models are to reduce the advantage of the adversaries to be as low as possible. But our model suggests setting security parameters for specific applications. Moreover, Juels' and Ohkubo's models were constructed closely to the protocols (Minimalist cryptography protocol [13] and privacy protection scheme [20]) they created. In Juels' models, some parameters in the models are borrowed from his protocol. In contrast, we constructed our models directly from analyzing security services required in a remote identification system (RFID system is a instance) rather than from any current protocol. Avoine's model is constructed from a broader picture of untraceability as well. His model has been applied on many existing protocols from a neutral point of view. Adversary assumptions in four models are similar. Access to RF channels and tag memory are both considered.

The security services provided by the models are compared in Table 1. Generally, Juels', Avoine's and Ohkubo's models focus on the privacy of tags data and the RF access within the protocol. But, as we have demonstrated in previous discussion, even the perfect privacy protection protocol will fail when RF information is combined with some environmental information, or if the privacy of bearers is not considered. Therefore, we have a more complex assumption on the sources of information and a separate model for bearers' privacy. All four models provide indistinguishability but their meanings are different. Ohkubo's model defines indistinguishability between tag data and random value. Ohkubo's privacy model is very strong and may be impractical for some RFID systems. Juels' privacy definition and Avoine's untraceability is essentially indistinguishability one while Juels', Avoine's and ours are close in the perspective that we all describe indistinguishability between two tags. One difference between Juels' model and ours is the definition of ideal privacy value. He uses 1/2 as the ideal guessing probability for adversaries who have no advantage. However, the guessing probability depends on the past knowledge (history) an adversary has, i.e. it could differ from 1/2 in some situations due to the existence of the environmental channel in past accesses (history). Avoine has a more detailed model on indistinguishability (untraceability in his notion). He classified untraceability in three levels and five kinds of oracle accesses. Our model, comparably, has three channels: RF public, RF secret, and environmental, which covers a broader range of situation.

Table 2: Compare security parameters

Constraints Constraints	Juels' model	Avoine's model	Ours model
Memory	l, q		M_t
Computational power	s		C_t
Reader's rang			D_t
Alterability			P_t
Adversary limitation	q, r, s	l_{ref}, l_{chal}	B_t, κ
Error tolerance			δ, ϵ

Juels', Avoine's and our models all provide security parameters to bound tags resources and adversary resources, yet Ohkubo's model does not. In the instance of an RFID system, we provide many explicit security parameters to limit the resources of tags and adversaries assumed in the models. See Table 2 for a comparison of security parameters.

7 Conclusion

We have discussed the necessary security requirements that current and future RFID systems will need. The security requirements for RFID include: availability of identity information, privacy of tag information and privacy of ownership. In order to evaluate whether an RFID application protocol provides the necessary security requirements one measures the protocol against the necessary model. In addition to constructing strong versions of these models, we have constructed versions of many of these models which have less-restrictive requirements, and these models have been developed with security parameters that can be adjusted to fit the application. These models may be more practical for the security within an RFID systems, which use limited resource tags that are low-cost in an application where security needs are not as great. In [29] we discussed an integrity model for RFID systems. Future work will focus on developing a less restrictive model for integrity that can be used in RFID applications whose integrity requirements are not as strict. Lastly, we have compared our models to Juels' models [13], Avoine's models [4] and Ohkubo et al.'s models [20].

References

[1] *860MHzC930MHz Class I Radio Frequency Identification Tag: radio frequency and logical communication interface specification*, Technical report, Auto-ID Center, 2002.

[2] *900 MHz Class 0 Radio Frequency Identification Tag*, Draft protocol specification, Technical report, Auto-ID Center, 2003.

[3] Atmel Corporation, *Atmel e5561 data sheet*, 2003.

[4] G. Avoine, *Adversarial Model for Radio Frequency Identification*, Cryptology ePrint Archive, Report 2005/098, 2005. (http://eprint.iacr.org/)

[5] G. Avoine and P. Oechslin, "A scalable and provably secure hash based RFID protocol," in *The 2nd IEEE International Workshop on Pervasive Computing and Communication Security (PerSec'05)*, pp. 110-114, 2005.

[6] S. Engberg, M. Harning, and C. D. Jensen, "Zero-knowledge device authentication: Privacy and security enhanced RFID preserving business value and consumer convenience," in *The Second Annual Conference on Privacy, Security and Trust (PST'04)*, pp. 47-58, 2004.

[7] EPCglobal Inc, *The EPCglobal Network: Overview of Design, Benefits, and Security*, 2004.

[8] M. Feldhofer, *A proposal for Authentication Protocol in a Security Layer for RFID Smart Tags*, 2003.

[9] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004*, LNCS 3156, pp. 357-370, Springer-Verlag, 2004.

[10] "Gillette confirms RFID purchase," *RFID Journal*, 2003.

[11] N. Good, J. Han, E. Miles, D. Molnar, D. Mulligan, L. Quilter, J. Urban, and D. Wagner, "Radio frequency identification and privacy with information goods," in *De Capitani di Vimercati*, pp. 41-42, 2004.

[12] G. Harris, *Tiny Antennas to Keep Tabs on U.S. Drugs*, New York Times, 2004.

[13] A. Juels, "Minimalist cryptography for low-cost RFID tags," in *The Fourth International Conference on Security in Communication Networks (SCN'04)*, LNCS 3352, pp. 149-164, Springer-Verlag, 2004.

[14] A. Juels, *Strengthening EPC Tags Against Cloning*, Manuscript, 2004.

[15] A. Juels, and R. Pappu, "Squealing euros: Privacy-protection in RFID-enabled banknotes," in *Financial Cryptography*, pp. 103-121, Springer-Verlag, 2003.

[16] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy," in *Proceedings of the 10th ACM Conference on Computer and Communication Security*, pp. 103-111, 2003.

[17] A. Juels and S. Weiss, *Defining Strong Privacy for RFID*, Manuscript, 2006.

[18] M. Kanellos, "E-passports to put new face on old documents," CNET News.com, 2004.

[19] D. Molnar and D. Wagner, "Privacy and security in library RFID: Issues, practices, and architectures," in *ACM Conference on Computer and Communications Security (CCS'04)*, pp. 210-219, 2004.

[20] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to "privacy-friendly" tags," in *RFID Privacy Workshop*, MIT, 2003. (http://citeseer.ist.psu.edu/ohkubo03cryptographic.html)

[21] D. Ranasinghe, D. Engels, and P. Cole, "Low-cost RFID systems: Confronting security and privacy," in *Auto-ID Labs Research Workshop*, Zurich, Switzerland, 2004. (http://citeseer.ist.psu.edu/716801.html)

[22] S. E. Sarma and D. W. Engels, *On the Future of RFID Tags and Protocols*, Technical Report MIT-AUTOID-TR-018, AUTO-ID Center, 2003.

[23] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID systems and security and privacy implications," in *Workshop on Cryptographic Hardware and Embedded Systems*, pp. 454-470, 2002.

[24] T. Staake, F. Thiesse, and E. Fleisch, "Extending the EPC network – The potential of RFID in anti-counterfeiting," in *Proceedings of the 2005 ACM symposium on Applied computing*, pp. 1607-1612, 2005.

[25] G. D. Sutton, *Radio Frequency Identification - Basics for Manufacturing*, 1993.

[26] "Wal-Mart details RFID requirement," *RFID Journal*, 2003.

[27] R. Want, "RFID: A key to automating everything," *Scientific American*, pp. 56-65, 2004.

[28] J. Yoshida, *Euro Bank Notes to Embed RFID Chips by 2005*, EE Times, 2001.

[29] X. Zhang and B. King, "Integrity improvements to an RFID privacy protection protocol for anti-counterfeiting," in *8th International Conference on Information Security (ISC'05)*, LNCS 3650, pp. 474-481, Springer-Verlag, 2005.

[30] X. Zhang and B. King, "Modeling RFID security," in *First SKLOIS Conference on Information Security and Cryptology (CISC'05)*, LNCS 3822, pp. 75-90, Springer-Verlag, 2005.

Xiaolan Zhang received the B.S. degree in information engineering from Shanghai Jiao Tong University in 2003 and the M.S. degree in computer engineering from Purdue University at Indianapolis in 2005. Now she is a Ph.D. candidate in electrical and computer engineering at the University of Illinois at Urbana-Champaign. She is currently a Research Assistant in the Coordinated Science Laboratory at the University of Illinois at Urbana-Champaign. Her research interests are in optical networking, computer security and privacy.

Brian King received a Ph.D. in mathematics (1990) and a Ph.D. in Computer Science (2000). He is currently an assistant professor of Electrical and Computer Engineering at Indiana Univ. Purdue Univ. Indianapolis (IUPUI). Prior to joining IUPUI he worked in the Security Technologies La at Motorola Research Labs. His research interests include: wireless security, cryptography, threshold cryptography and low-complexity cryptosystems.