# RFID Systems: A Survey on Security Threats and Proposed Solutions

Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda

Computer Science Department, Carlos III University of Madrid,
{pperis, jcesar, jestevez, arturo}@inf.uc3m.es

**Abstract.** Low-cost Radio Frequency Identification (RFID) tags affixed to consumer items as smart labels are emerging as one of the most pervasive computing technology in history. This can have huge security implications. The present article surveys the most important technical security challenges of RFID systems. We first provide a brief summary of the most relevant standards related to this technology. Next, we present an overview about the state of the art on RFID security, addressing both the functional aspects and the security risks and threats associated to its use. Finally, we analyze the main security solutions proposed until date.

**Keywords:** RFID Security, Pervasive Computing, Ubiquitous Computing, Security and Privacy.

## 1 Introduction

At the moment, the most extended identification systems are barcodes. Initially, there were two standards: the Universal Product Code (UPC, United States) and the European Article Number (EAN, Europe). Although, at first, EAN was only taken by twelve European countries, by the end of 2004 more than one hundred countries all over the world had already adopted this standard. Finally, when the United States decided to adopt the European-born standard, UPC and EAN merged, giving rise to what is nowadays known as GS1 [8].

Recently, the mass deployment of Radio Frequency Identification systems (RFID) has taken place. These systems comprise of Radio Frequency (RF) tags or transponders, and RF readers or transceivers. Tag readers broadcast an RF signal to access resistant data stored in tags. One of the main differences with barcodes is that RFID tags provide an unique identifier, or a pseudonym that allows accessing to this unique identifier. The use of RFID tags offers several advantages over barcodes: data can be read automatically, without line of sight, and through a non-conducting material such as cardboard or paper, at a rate of hundreds of times per second, and from a distance of several meters.

Radio frequency identification systems are becoming valuable tools in processes such as manufacturing, provision chain management, and stock control. Around 5 billion barcodes are read daily, so efficiency gains from using RFID tags could substantially lower the cost of tagged items [29]. The penetration of

RFID systems is nowadays mainly limited by privacy concerns and by their cost, which must be between 0.05 and 0.1 € to be considered affordable. Additionally, in order to take full advantage of the potential offered by RFID tags, the identification of an item must be made throughout all its life cycle: production, distribution, sale and recycling.

The low cost demanded for RFID tags causes them to be very resource limited. Typically, they can only store hundreds of bits, roughly have between 5000 and 10000 logic gates, and a maximum communication range of a few meters. Within this gate counting, only between 250 and 3000 gates can be devoted to security functions. It is interesting to recall that for a standard implementation of the Advanced Encryption Standard (AES) between 20000 and 30000 gates are needed. Additionally, power restrictions should be taken into account, since most RFID tags in use are passive. Furthermore, one can not suppose either that these systems are able to store passwords in a secure way, because tags are not resistant against tampering attacks at all.

In spite of all these limitations, the penetration of RFID technology is increasing steadily. Experts believe that both systems will coexist some time and that finally, RFID tags will completely replace classical barcodes. An example of this increasing interest in RFID technology is the project of the European Central Bank about including RFID tags in 500 € bills, along with barcodes.

Nevertheless, the implantation of RFID systems is not being absolutely spotless, as there are some organizations like CASPIAN [4] which are strongly against their massive deployment.

## 2 Overview of RFID Systems

### 2.1 RFID System Components

RFID systems are made up of three main components, that we briefly describe in the following: the transponder or RFID tag, the transceiver or RFID reader, and the back-end database.

1. ***Transponder or RFID Tag***
   In an RFID system, each object will be labeled with a tag. Each tag contains a microchip with some computation and storage capabilities, and a coupling element, such as an antenna coil for communication. Tags can be classified according to two main criteria:
   - The type of memory: read-only, write-once read-many, or fully rewritable.
   - The source of power: active, semi-passive, and passive.
2. ***Transceiver or RFID Reader***
   RFID readers are generally composed of an RF module, a control unit, and a coupling element to interrogate electronic tags via RF communication. Readers may have better internal storage and processing capabilities, and frequently connect to back-end databases. Complex computations, such as all kind of cryptographic operations, may be carried out by RFID readers, as they usually do not have more limitations than those found in modern handheld devices or PDAs.

3. ***Back-end Database***
   The information provided by tags is usually an index to a back-end database (pointers, randomized IDs, etc.). This limits the information stored in tags to only a few bits, typically 96, which is a sensible choice due to tag severe limitations in processing and storing. It is generally assumed that the connection between readers and back-end databases is secure, because processing and storing constraints are not so tight in readers, and common solutions such as SSL/TLS can be used.

### 2.2 RFID System Interface

In this section, we focus exclusively on passive RFID tags, since we consider that these will be the first to be massively deployed and form part of our daily lives. Additionally, these low-cost RFID systems are very limited on resources, which forces some interesting trade-offs in their designs.

1. ***Transceiver/Transponder Coupling Communication***
   Passive RFID tags obtain their operating power by harvesting energy from the electromagnetic field of the reader communication signal. Two main possibilities exist here: near field ($d < \frac{1}{2\pi f}$) and far field ($d > \frac{1}{2\pi f}$) [2].
   The signal sent from readers to tags must be used simultaneously to transmit both information and energy. However, readers normally operate in Industrial Scientific-Medical (ISM) bands, so there are restrictions in the bandwidth and in the transmitted power. Tags, on the other hand, are not under these limitations.
2. ***Data Coding***
   The exchange of data between the reader and the tag, and vice versa, must be performed efficiently; so both coding and modulation are used. The coding/modulation is defined according to the existing limitations in the backward and the forward channel. Readers will be able to transmit greater power, but will have bandwidth limitations. Tags, which are passive, will not have bandwidth limitations.
   As a coding mechanism, level codes (Non-Return-to-Zero, NRZ; and Return to Zero, RZ) or transition codes (Pulse Pause Modulation, PPM; Pulse Weight Modulation, PWM; and Manchester) are mostly used. These coding techniques are depicted in *Table* 1.

| Channel | Usual Coding |
|---|---|
| Forward Channel | Manchester or NRZ |
| Backward Channel | PPM or PWM |

**Table 1.** Coding Techniques

3. ***Modulation***
   The modulation scheme determines how the bitstream is transmitted between readers and tags, and vice versa. Three possible solutions exist: Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK) and Phase Shift Keying (PSK). The choice of a modulation type is based on power consumption, reliability, and bandwidth requirements.
4. ***Tag Anti-collision***
   Collisions in RFID systems happen when multiple tags simultaneously answer to a reader signal. Methods used to solve this kind of problems, allowing reliable communication between readers and tags, are referred to as anti-collision methods. The anti-collision algorithms used in RFID systems are quite similar to those applied in networks, but they take into account that RFID tags are generally more limited than the average network device. Two approaches are used: probabilistic or deterministic. However, in practice, many solutions are a combination of both.
5. ***Reader Anti-collision***
   In this case, several readers interrogate the same tag at the same time. This is known in the bibliography as the *Reader Collision Problem*. One possible solution to this problem consists of allocating frequencies over time to a set of readers by either a distributed or a centralized approach.
6. ***Frequencies and Regulations***
   Most RFID systems operate in ISM bands [15]. ISM Bands are designated by the International Union of Telecommunications and are freely available to be used by low-power, short-range systems. The most commonly used ISM frequencies for RFID systems are 13.56 MHz and 902-928 MHz (only in the US). Each band has its own radiation power and bandwidth regulations.

## 3 RFID Standards

RFID systems do not lack standards. Those standards typically describe the physical and the link layers, covering aspects such as the air interface, anti-collision mechanisms, communication protocols and security functions. Nevertheless, not everything is well covered, and there is a certain absence of standardization in testing methods and application data (notably in protocols and application programming interfaces).

### 3.1 Contactless Integrated Circuit Cards

ISO 7810 defines a special type of identification cards without contact. According to the communication range, three types of cards can be distinguished:

- Close-coupled cards (ISO 10536). These are cards that operate at a very short distance of the reader ($< 1$ centimeter).
- Proximity cards (ISO 14443). These are cards that operate at an approximated distance of 10 centimeters of the reader. They can be considered as a high-end RFID transponder since they have a microprocessor.

– Vicinity cards (ISO 15693). These are cards that operate at distances greater than one meter. On the contrary to the previous cards (ISO 14443), they usually only incorporate inexpensive machines of states, instead of microprocessors.

### 3.2 RFID in Animals

ISO 11784, ISO 11785, and ISO 14223 standardize tags for animal identification in the frequency band below 135 KHz. Initially, standards define an identifier of 64 bits. In ISO 14223, greater blocks for reading and writing, as well as blocks of protected writing, are allowed. There are hardly any differences between the communication protocols defined in ISO 14223 and ISO 18000-2.

### 3.3 Item Management

ISO 18000 defines the air interface, collision detection mechanisms, and the communication protocol for item tags in different frequency bands.

– Part 1 describes the reference architecture.
– Parts 2-7 specify the system in different frequency bands (<135KHz, 13.56 MHz, 2.45 GHz, 5.8 GHz, 900 MHz, and 433 MHz).

### 3.4 Near-Field Communication (NFC)

1. ***NFCIP-1***
   NFC is designed for interactions between tags and electronic devices in close proximity (< 10 cm). The standards ETSI TS 102.190, ISO 18092, and ECMA 340 identically define the Near Field Communications Interface and Protocol-1 (NFCIP-1).
   These protocols describe the air interface, initialization, collision avoidance, a frame format, and a block-oriented data-exchange protocol with error handling. Additionally, they describe two different communication modes: active and passive.
2. ***NFCIP-2***
   The Near Field Communication Interface and Protocol-2 (NFCIP-2) specifies the communication mode selection mechanism (ECMA 352). NFCIP-2 compliant devices can enter in three different communication modes: NFCIP-1, ISO 14443, and ISO 15693. All these modes operate at 13.56 MHz and are designed not to disturb other RF fields at the same frequency.

### 3.5 Electronic Product Code (EPC)

The Auto-ID (Automatic Identification) Center was created in October 1999 at the MIT Department of Mechanical Engineering, by a number of leading figures. At the beginning, EPC was developed by the Auto-ID Center. The Auto-ID Center officially closed the 26th October, 2003. The center had completed

its work and transferred his technology to EPCglobal [9]. EPCglobal is a joint venture between EAN International and the Uniform Code Council (UCC). The so-called EPC network is composed of five functional elements:

- The Electronic Product Code is a 96-bit number with 4 distinct fields: identifying the EPC version number, domains, object classes, and individual instances.
- An Identification System which consists of RFID tags and readers. Tags can be of three different kinds (Class 0, 1, and 2). The Auto-ID Center published a protocol specification for Class 1 tags in the HF band (compatible with ISO 15693 and ISO 18000-3), and Class 0 and 1 tags in the UHF band.
- The Savant Middleware offers processing modules or services to reduce load and network traffic within the back-end systems.
- The Object Naming Service (ONS) is a network service similar to the Domain Name Service (DNS), which is a technology capable of handling the volumes of data expected in an EPC RFID system.

## 4 Risks and Threats

Although RFID systems may emerge as one of the most pervasive computing technologies in history, there are still a vast number of problems that need to be solved before their massive deployment. One of the fundamental issues still to be addressed is privacy. Products labeled with tags reveal sensitive information when queried by readers, and they do it indiscriminately.

A problem closely related to privacy is tracking, or violations of location privacy. This is possible because the answers provided by tags are usually predictable: in fact, most of the times, tags provide always the same identifier, which will allow a third party to easily establish an association between a given tag and its holder or owner. Even in the case in which tags try not to reveal any kind of valuable information that could be used to identify themselves or their holder, there are many situations where, by using an assembly of tags (constellation), this tracking will still be possible.

Although the two aforementioned problems are the most important security questions that arise from RFID technology, there are some others worth to mention:

1. ***Physical Attacks***
   In order to mount these attacks, it is necessary to manipulate tags physically, generally in a laboratory. Some examples of physical attacks are probe attacks, material removal through shaped charges or water etching, radiation imprinting, circuit disruption, and clock glitching, among others. RFID tags offer little or none resilience against these attacks.
2. ***Denial of Service (DoS)***
   A common example of this type of attack in RFID systems is the signal jamming of RF channels.

3. ***Counterfeiting***
   There are attacks that consist in modifying the identity of an item, generally by means of tag manipulation.
4. ***Spoofing***
   When an attacker is able to successfully impersonate a legitimate tag as, for example, in a man-in-the-middle attack.
5. ***Eavesdropping***
   In this type of attacks, unintended recipients are able to intercept and read messages.
6. ***Traffic analysis***
   Describes the process of intercepting and examining messages in order to extract information from patterns in communication. It can be performed even when the messages are encrypted and can not be decrypted. In general, the greater the number of messages observed, the more information can be inferred from the traffic.

## 5 Proposed Solutions

In this section we present the best solutions proposed so far to solve the security problems and threats associated with the use of RFID systems. Our objective is not to give a detailed explanation of each solution, but to provide the reader with the fundamental principles and a critical review of every proposal, as well as the bibliography to be checked in case someone wishes to deepen on some aspects of this subject.

### 5.1 Kill Command

This solution was proposed by the Auto-ID Center [5] and EPCglobal. In this scheme, each tag has a unique password, for example of 24 bits, which is programmed at the time of manufacture. Upon receiving the correct password, the tag will deactivate forever.

### 5.2 The Faraday Cage Approach

Another way of protecting the privacy of objects labeled with RFID tags is by isolating them from any kind of electromagnetic waves. This can be made using what is known as a Faraday Cage (FC), a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies). There are currently a number of companies that sell this type of solution [24].

### 5.3 The Active Jamming Approach

Another way of obtaining isolation from electromagnetic waves, and an alternative to the FC approach, is by disturbing the radio channel, a method which is known as active jamming of RF signals. This disturbance may be done with a device that actively broadcasts radio signals, so as to completely disrupt the radio channel, thus preventing the normal operation of RFID readers.

### 5.4 Blocker Tag

If more than one tag answers a query sent by a reader, it detects a collision. The most important singulation protocols are ALOHA (13.56 MHz) and the tree-walking protocol (915 MHz). Juels [19] used this feature to propose a passive jamming approach based on the tree-walking singulation protocol, called blocker tag. A blocker tag simulates the full spectrum of possible serial numbers for tags. In [17], Juels and Brainard propose a weaker privacy-protection mechanism, soft blocking. Soft blockers simply show the privacy preferences of their owners to RFID readers.

### 5.5 Bill of Rights

In [11], Garfinkel proposed a so-called RFID Bill of Rights that should be upheld when using RFID systems. He does not try to turn these rights into Law, but to offer it as a framework that companies voluntarily and publicly should adopt.

### 5.6 Classic Cryptography

1. ***Rewritable Memory***
   In 2003, Kinoshita [22] proposed an anonymous-ID scheme. The fundamental idea of his proposal is to store an anonymous ID, $E(\mathrm{ID})$, of each tag, so that an adversary can not know the real ID of the tag. $E$ may represent a public or a symmetric key encryption algorithm, or a random value linked to the tag ID. In order to solve the tracking problem, the anonymous ID stored in the tag must be renewed by re-encryption as frequently as possible.
2. ***Symmetric Key Encryption***
   Feldhofer [10] proposed an authentication mechanism based on a simple two-way challenge-response algorithm. The problem with this approach is that it requires to have AES implemented in an RFID tag. In [21] we can find a state of the art on AES implementations in RFID systems.
3. ***Public Key Encryption***
   There are solutions that use public-key encryption, based on the cryptographic principle of re-encryption. The reader interested in the precise details can read the paper of Juels [18]. Other two interesting papers that tackle the subject of re-encryption are [12] and [28].

### 5.7 Schemes Based on Hash Functions

One of the more widely used proposals to solve the security problems that arise from RFID technology (privacy, tracking, etc.) is the use of hash functions.

1. ***Hash Lock Scheme***
   Weis [32] proposed a simple security scheme based on one-way hash functions. Each tag has a portion of memory reserved to store a temporary *metaID* and operates in either a locked or an unlocked state. The reader

hashes a key $k$ for each tag, and each tag holds a *metaID* (*metaID = hash(k)*). While locked, a tag answers all queries with his *metaID* and offers no other functionality. To unlock a tag, the owner queries the back-end database with the *metaID* from the tag, looks up the appropriate key and sends the key to the tag. The tag hashes the key and compares it to the stored *metaID*.

2. ***Randomized Hash Lock Scheme***
   One of the problems of the previous solution is that it allows the tracking of individuals. To avoid this, the *metaID* should be changed repeatedly in an unpredictable way. In order to solve this problem, Weis [32] proposed an extension of the hash lock scheme. It requires that tags have a hash function and a pseudo-random number generator.
3. ***Hash-Chain Scheme***
   Ohkubo, in [27], suggested a list of five points that must be satisfied in all security designs of RFID schemes: keep complete user privacy, eliminate the need for extraneous rewrites of the tag information, minimize the tag cost, eliminate the need for high power of computing units, and provide forward security. In [27], a hash-chain scheme was proposed, in which two hash functions ($G$ and $H$) are embedded in the tag.

Some other recent published works on the use of hash functions are [6, 7, 14, 23, 34].

### 5.8 A Basic PRF Private Authentication Scheme

Molar [26] proposed a scheme for mutual authentication between tags and readers, with privacy for the tag. This protocol uses a shared secret $s$ and a Pseudo-Random Function (PRF) to protect the messages exchanged between the tag and the reader.

### 5.9 Tree-Based Private Authentication and Delegation Tree

One of the main drawbacks of the hash schemes already proposed is that the load of the server (for identifying tags) is proportional to the number of tags. Molnar [26] has proposed a new scheme to reduce this load, which is named *Tree-Based Private Authentication*. This new protocol reduces the load to $O(\log n)$ but introduces the use of a Trust Center (TC). In order to reduce the burden on the TC, an offline delegation has been proposed [25]. Another interesting proposal is the work of Gildas and Oechslin [1], where a time-space trade-off is proposed.

### 5.10 Human Protocols

In [31], Weis introduced the concept of human computer authentication protocol due to Hopper and Blum, adaptable to low-cost RFIDs. This concept has been recently extended in an article by Weis and Juels [20], where they propose a lightweight symmetric-key authentication protocol named $HB^+$.

The security of both the $HB$ and the $HB^+$ protocols is based on the *Learning Parity with Noise Problem*, whose hardness over random instances still remains as an open question.

### 5.11 Non-Cryptographic Primitives

There are some solutions which do not use true cryptographic operations. The authors in [30] proposed a set of extremely-lightweight challenge-response authentication protocols. These protocols can be used for authenticating tags, but they can be broken by a powerful adversary. In [16], Juels proposed a solution based on pseudonyms without using hash functions at all. The RFID tags store a short list of random identifiers or pseudonyms (known by authorized verifiers to be equivalent). When tag is queried, it emits the next pseudonym in the list.

## 6 Conclusions

RFID technology is one of the most promising technologies in the scope of ubiquitous computing. For it to become a reality, two kinds of problems must be solved: on one hand, *technological problems* and, on the other, *social problems.*

1. ***Technological Problems***
   Mark Weiser [33] (an early visionary of ubiquitous computing) announced (in 1991!) that one of the main problems that ubiquitous computing would have to solve was privacy. Deeply associated with it is the problem of tracking, or violations of location privacy.
   We have presented some of the most relevant solutions which try to address the fundamental security problems of RFID technology (privacy and tracking). Most of the proposed solutions rely on schemes based on the implementation of cryptographic hash functions in the tag. Although it is true that this could be possible in a short period of time, we consider that the current state of the art is still far from this point, so schemes based in hashing are not currently feasible. Alternatively, new lightweight hashing schemes especially suitable for RFID implementations, have not been scrutinized enough to be considered secure, a notable example is the ASHF used in SecurID [3].
2. ***Social Problems***
   Even considering that technological problems could eventually be solved, the implantation of RFID systems to a great scale will not be a reality if *we don't educate* people about their potential benefits, and if we cannot offer a guaranteed level of security. For example, a recent report [13] showed the numbers of a study made on *RFID and Perception of Control* pointing out that a 73.4% of those polled preferred to deactivate tags after buying a product. This clearly shows that, although advances in technological problems have been made, this is not yet reflected in the society, on the average citizen, which is, after all, who has the last word in deciding the future of a given technology.

## References


1. G. Avoine and P. Oechslin. A scalable and provably secure hash-based RFID protocol. In *PERSEC'05*, pages 110–114. IEEE Computer Society Press, 2005.
2. C.A. Balanis. *Antenna theory: analysis and design.* John Wiley and Sons, 1997.
3. A. Biryukov, J. Lano, and B. Preneel. Recent attacks on alleged securid and their practical implications. *Computers and Security*, 24(5):364–370, 2005.
4. CASPIAN. http://www.nocards.org/, 2005.
5. Auto-ID Center. 900 MHz class 0 radio frequency (RF) identification tag specification. Draft, March 2003.
6. E.Y. Choi, S.M. Lee, and D.H. Lee. Efficient RFID authentication protocol for ubiquitous computing environment. In *Proc. of SECUBIQ'05*, LNCS, 2005.
7. T. Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In *Proc. of SECURECOMM'05*, 2005.
8. GS1 - EAN International. http://www.ean-int.org/, June 2005.
9. EPCglobal. http://www.epcglobalinc.org/, June 2005.
10. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In *Proc. of CHES'04*, volume 3156 of *LNCS*, pages 357–370, 2004.
11. S. Garfinkel. Bill of Rights. http://www.technologyreview.com, October 2002.
12. P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets. In *CT-RSA'04*, volume 2964 of *LNCS*, pages 163–178. Springer-Verlag, February 2004.
13. O. Gunther and S. Spiekermann. RFID and the perception of control: the consumer's view. *Commun. ACM*, 48(9):73–76, 2005.
14. D. Henrici and P. Müller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In *PERSEC'04*, pages 149–153. IEEE Computer Society, 2004.
15. ITU page on definitions of ISM bands. http://www.itu.int/ITU-R/terrestrial/faq/index.html, September 2005.
16. A. Juels. Minimalist cryptography for low-cost RFID tags. In *SCN'04*, volume 3352 of *LNCS*, pages 149–164. Springer-Verlag, 2004.
17. A. Juels and J. Brainard. Soft blocking: Flexible blocker tags on the cheap. In *WPES'04*, pages 1–7. ACM, ACM Press, October 2004.
18. A. Juels and R. Pappu. Squealing euros: Privacy protection in RFID-enabled banknotes. In *FC'03*, volume 2742 of *LNCS*, pages 103–121. IFCA, Springer-Verlag, January 2003.
19. A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In *ACM CCS'03*, pages 103–111. ACM, ACM Press, October 2003.
20. A. Juels and S. Weis. Authenticating pervasive devices with human protocols. In *CRYPTO'05*, volume 3126 of *LNCS*, pages 293–308. IACR, Springer-Verlag, 2005.
21. M. Jung, H. Fiedler, and R. Lerch. 8-bit microcontroller system with area efficient AES coprocessor for transponder applications. Ecrypt Workshop on RFID and Lightweight Crypto, 2005.
22. S. Kinoshita, F. Hoshino, T. Komuro, A. Fujimura, and M. Ohkubo. Low-cost RFID privacy protection scheme. In *IPS Journal 45, 8*, pages 2007–2021, 2003.
23. S.M. Lee, Y.J. Hwang, D.H. Lee, and J.I.L. Lim. Efficient authentication for low-cost RFID systems. In *Proc. of ICCSA'05*, volume 3480 of *LNCS*, pages 619–627. Springer-Verlag, 2005.

24. mCloak for RFID tags. *http://www.mobilecloak.com/rfidtag/rfid.tag.html*, September 2005.
25. D. Molnar, A. Soppera, and D. Wagner. A scalable, delegatable, pseudonym protocol enabling ownership transfer of RFID tags. Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.
26. D. Molnar and D. Wagner. Privacy and security in library RFID: Issues, practices, and architectures. In *ACM CCS'04*, pages 210–219. ACM, ACM Press, October 2004.
27. M. Ohkubo, K. Suzuki, and S. Kinoshita. Cryptographic approach to "privacy-friendly" tags. In *RFID Privacy Workshop*, 2003.
28. J. Saito, J.-C. Ryou, and K. Sakurai. Enhancing privacy of universal re-encryption scheme for RFID tags. In *EUC'04*, volume 3207 of *LNCS*, pages 879–890. Springer-Verlag, August 2004.
29. W. Sean and L. Thomas. Automatic identification and data collection technologies in the transportation industry: BarCode and RFID. Technical report, 2001.
30. I. Vajda and L. Buttyán. Lightweight authentication protocols for low-cost RFID tags. In *UBICOMP'03*, 2003.
31. S. Weis. Security parallels between people and pervasive devices. In *PERSEC'05*, pages 105–109. IEEE Computer Society Press, 2005.
32. S.A. Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *Security in Pervasive Comp.*, volume 2802 of *LNCS*, pages 201–212, 2004.
33. M. Weiser. The computer for the 21st century. *Scientific American*, 265(3):94–104, September 1991.
34. J. Yang, J. Park, H. Lee, K. Ren, and K. Kim. Mutual authentication protocol for low-cost RFID. Ecrypt Workshop on RFID and Lightweight Crypto, 2005.