# Low-Cost RFID Technology - an Overview

Annika Karlsson and Anna Sandström,
Department of Information Technology, Uppsala University

**Abstract.** Radio Frequency Identification (RFID) systems are becoming more common. Companies like Wal-Mart are using it to facilitate the tracking of goods, to still be competitive when budget alternatives want to get into the market. But what is exactly RFID and where can it be used?
In this paper we give an overview of RFID technology and the challanges that arises when it is brought into an open environment, the consumer market. Finally we discuss possible solutions when using the low-cost tags that are lacking in both memory and computaional power, but still can provide some level of security and privacy.

## 1 Introduction

The idea of Radio Frequency Identification (RFID) is to remotely be able to register items passing by a reader. The comparison to the optical bar code you can find on almost every item sold in a store, is obvious. With a special reader you can get the information of an item with just a swipe. The difference is the scanning technique. Where the bar code needs line-of-sight between reader and tag, the RFID uses radio frequencies to transmit the information. You can also get the information from many items in significantly less time, because you do not have to put each item before the reader. It is also much easier to automate the readings as the items just have to pass by the reader without the intervention of a person.

The idea have been around ever since the bar codes were first used in the 70's, and have been used for tracking goods during shipping and cattle tracking for some time now. In these applications you put a tag on for example a container and can track the movement of this container in a closed area. The tags used do not have a restricted budget, since the goods it is attached to are very valuable.

When RFID tags are used today, they are taken from the closed environment of a production site and put into the consumer market. RFID will likely be one of the most extensive examples of ubiquitous computing in the coming years. [Sar04], and everywhere we are seeing new examples of where it can be used. The new usage areas and environment results in new risks to privacy and security that was not an issue in the former uses of the technology. In 3 we will describe the technology in more detail.

The tag transmits its identification number when prompted, and every reader in range can hear the reply. When this is done in an non-secure environment, the information must be secured to hide business secrets. As tags are used for cheaper items the need for cheaper tags increase. If you put a $1 tag on an item that will be sold for $1, the price for that item has just been doubled. The cost of simple RFID tags promises to drop to the level of $0.05 per unit in the next years [SWE02], and then they can be used in low-cost applications as well!

Another issue is consumer privacy. Who would want to broadcast the name of the medication you bought at the pharmacy during your lunch break? And what if the shoes and jacket I am wearing makes it possible to track my movements? These type of questions are discussed in section 4. In section 5 and section 6 we present some possible solutions to these problems.

## 2 Where Can RFID be Used?

The possibilities and usage areas for RFID is enormous, the only limitation is made by the human mind. Today you may find that RFID is already used in various applications. Here are some of them:

- Sportident International AB: Verifying and timestamping controls in sports events, for example orienteering contest. [webb] [Mat]
- Kidspotter, Legoland in Billund, Denmark. Parents may rent a Kidspotter wristband and a special map to track their missing child. The wristband is an encapsulated RFID tag. Sending an SMS request trigger a location report back to the mobile phone. [Leg]
- Vasaloppet, RFID tracking of the skiers. The readers are placed under the snow to facilitate easy tracking of each skier. Relatives and friends can subscribe and get an SMS to their mobile phone for each time the skier is passing one of the checkpoints.[web04] [weba]
- Åre Skistar ski-pass. These you can load in advance via Internet and then just start using as soon as you get to the slopes. Since each ski-pass is unique it is easy to load an old ski-pass with new valid days, and also easy to restrict the usage to pre-paid customers. Here the dates for usage or the areas where the card will work is easily limited. Compare this to the manual inspection of day-passes at a nearby amusement park. This day-pass might be a color-coded band to help the employees inspection but not hindering reuse the next day the same color-code is used.

What all these have in common is that the users (except the small kid in the Kidspotter example) are perfectly aware and perhaps even paying an extra fee to get traced or to get the service of a ski lift. It is part of the function of these implementations.

Here are some more examples where the tags will be used for tracking shipments and tracking items from manufacturing to customer check-out replacing bar code technology:

- Wal-Mart: Uses a passive, cheap, and short range RFID in their products. [Mat] Their goal is that 100 of Wal-Marts biggest suppliers equip all their products with RFID by January 1, 2005, and the next 200 by January 1, 2006. [Walb] [Wala]

- United Colors of Benetton: All clothes and items from the brand will be equipped with a Philips I.CODE RFID chip. [Yos]

In all these cases the different items in the store have an RFID for the purpose of tracking the item. The purpose may be to to speed up the check-out process indicate that non-purchased goods are leaving the store. We have not find an implementation for private use (today) of these tags.

Using an appropriate reader these items could be read outside of the store...

In the future we cannot really imagine all the possible ways of using RFID's to make life easier to humans, but here are some suggestions:

- For the recycling industry. Identifying what bin different unsorted items should end up in, depending on material, letting the sorting be automated.
- Sorting and finding misplaced books in a library. For example a device to scan the bookshelf to be sure the books are in alphabetical order.
- Spare the employees not having to do the tedious job of stock-taking for any store or storage.
- Tracking supplies in a factory.
- Stopping shoplifting and related problems, i.e. "stealing" supply and tools from a construction area.

And here are some examples of some applications where any person has a use of RFID:

- All sorts of situations when you lost a personal thing, misplaced it (for example your keys), or maybe a runaway pet.
- A refrigerator/freezer keeping track of and creating a shopping list from what you need to buy/replace in your fridge, and even suggesting some dinner and provide recipes depending on what you actually have at home.
- A microwave owen that knows how to cook the food. You just have to place the food in it and press start.

## 3 A Brief Introduction to RFID Technology

RFID is promoted as a more intelligent replacement for the optical bar code that has been used since the 70's to scan items. But it can do so much more than just be a placeholder for a product number!

In this section we will describe the basics of RFID technology; the tags and the readers.

RFID is not a new technology. It has been around since at least the 1970'th. The reason why it has become such and advancing research area now is depending on the fact that the tags, the part on the item, has become so small and cheap that it is possible to use RFID for many applications. [Jou]

### 3.1 The Components of a RFID System

The RFID consists of the following parts:

- one or more tags, also called transponders
- a reader, that collects information from the tags in its vicinity
- a database, for translating the information received to more useful data.

**Tags** A tag is attached to the items that should be monitored in the system. A unique id is stored in the memory of the tag.

The original name of a tag is a transponder. The functionality of the tag is that of a transponder. When it receives a request, it transmit some data. In the airline industry transponders have been used since the World War II [Wei03], and almost all aircrafts today are equipped with transponders. The pilot sets a code given by the air traffic controller and then every radar scan shows the active transponders in the air space.

There are a lot of different tags, and they can be ordered into classes depending on their computational power, memory storage and whether or not they contain their own power source (battery) or if they are using the readers request signals to build up enough power to transmit.

*Architecture.* A tag consists of a microchip connected to an antennae. It communicate with a reader using radio frequencies (RF). [Wei03] The range of the communication is dependant on the size of the antennae and the power with which the data is being sent.

Today more advanced tags are already being used in for example "keyless entry" systems. These tags are capable of doing relatively advanced cryptographic calculations. If this type of tag would be attached to a cheap item like a milk carton, the cost of the milk would be too high. If RFID tags are to be used in this application the price of a tag must decrease significantly. Research has been done to develop the new generation of tags, which will only cost about $0.05. [SWE02] This type of tag has a small memory and very limited computing capabilities. A tag without a local power source is not capable to transmit data unless it is charged. This type of tag is called passive.

In this paper we are focusing the techniques to make these small, inexpensive tags and still be able to provide some level of security and privacy protection.

**Readers** While the tags are moving with the item it is attached to, the readers can be both in a fixed position and hand held devices. The reader transmits a request to its vicinity and reads the answer it gets. It could either talk to all tags present or directly to a specific tag. In the latter case it would have to know the unique identifier of the tag.

The reader interacts with a passive tag by creating a magnetic field from which the tag can absorb energy enough to send a reply message back to the sender. The frequencies used in RFID systems are regulated by authorities. 13.56 MHz and 915 MHz are two standardized frequencies.

**Database** To be able to get useful information from a tag that only contain an identifier, a back-end database is often used. Here it is possible to store more information about an item. If the database and the reader is separated the channel between them must be safe. [Wei03]

## 4 Presentation of Privacy and Security Problems

In the previous chapters we have given some examples where RFID is very useful. At the same time as the technology is very good for business and customers, it also introduces new problems. In this section we will present some security and privacy risks.

First we will define what we mean by security and privacy in RFID systems.

*Security.* Security refers to the communication between reader and tag. It must be possible to prove that the message has not been compromised and that the sender of a messages is authenticated. The availability of a system is also very important. There is a risk that someone can disturb the connection and hence stop the system from performing its task. [REC04]

Another issue is the information stored on the tag. This must be protected from unauthorized readings and updates.

*Privacy.* Unprotected tags may be vulnerable to eavesdropping, traffic analysis, spoofing and denial-of-service attacks. [WSRE03] If the data on the tags reveal personal information there is a threat to privacy that the data might be read by others. But even though the protected tags may have secure message passing and content, it could pose a threat to the privacy of the customer carrying the tag. If it is possible to relate a RFID tag to a person, it is possible to trace this person.

*Example 1.* Consider the scenario of a huge shopping mall. When a person has bought an item in one shop (or even is carrying a tag already when he enters the mall) readers in the area can register where and when this person goes by one of the readers. This information could be gathered to give a view of how this person moves from shop to shop, perhaps of interest to the shop-owners.

*Example 2.* Another possible scenario is when a customer leaves his newly-bought expensive mp3-player in the car while doing other errands, and a high-tech thief is out on the parking lot scanning cars for valuable items.

This was two different types of problems. In the first, we have the problem of traceability (privacy), that a person can be identified by the item he is carrying even if the information itself is encrypted. The second is information leakage [OSK03] (security), that an unauthorized person can read information from a tag.

In this we can see that the same feature that is the strength of some RFID systems is the vulnerability of another when applying it to a different market.

The original use of RFID tags for tracking goods and cattle is the same that violates the privacy of the customers. In this paper we are focused on low-cost RFID tags that are cheap enough to be embedded into small items. They should not only be useful for the stores, keeping track of all items, but there are a lot of emerging uses for the customer. Hence it is important to find a technology that is adjustable to fit both the producer and the consumer needs!

### 4.1 Identified Threats to Security and Privacy

Here we will try to summarize the most important threats to security and privacy that the researchers in the RFID area have covered. [WSRE03][OSK03] [Wei03]

- Unprotected data can be read by anyone, who is close enough. The tag is sending its information when a reader asks for it. Who wants to display the type of items you have in your bag? Or what if it will be possible to read the amount of money you are carrying if RFID tags are embedded into bank notes?
- As mentioned above, tags can be traced. [WSRE03] calls this "location privacy". An item can be traced when it passes nearby readers. The threat to personal privacy is when this tracing is done on items that can in some way be connected to an individual.
- Fraud is definitely a threat to businesses. If you can copy the information on a tag you can use this to produce new tags. The act of making someone believe you are someone you're not, is called spoofing. Spoofing of tags can make it look like the item is still in the store, even if a customer has taken it through the gates. [WSRE03] If the tag is shielded the readers cannot see it. Shielding is easily done by creating your own Faradays cage (see 5).
  Changing the information on a tag i also fraud. If you can access the pricing information of an item, you can set it lower (if you are the buyer) or raise the price to cause dissatisfaction among the customer of the competing store.
- Similar to the previous point, the placement of the tag is also important to consider. A customer that does not want to pay for an item may find the tag and remove it physically. In this case it can be good to put the tag inside the packet instead of on the outside.
- Sabotage is also an option, where an adversary who has access to the system can corrupt information and disturb communication.
- Denial-of-Service attacks. A malicious blocker tag can be used for denial-of-service attacks. [JRS03] The tag could be disrupting the reading of tags, for example when performing inventory on stock. Blocker tags are described in 5.1.

## 5 Solutions to the Privacy Problem

Below you will find some different solutions to the privacy problem:

*Faradays Cage/Foil Bag Solution* A foil bag or a bag of paper containing metal can prevent readers to notice RFID tags. Shoplifters could bring a bag covered on the inside with foil, but a person not wanting to expose the RFID in his clothes or belongings might still have problems.

To have currency notes with RFID to have governments track movement of large numbers of bills will then be ridiculous. It will be easy to cover the money with aluminum foil or a metal bag.

*A Kill Tag Solution/Self Destruct Function.* Another solution would be to have the tags self destruct on the users request. A secret key is used to execute the command on the tag, and this function is implemented in a trial system at Auto-ID Center. Because of the secret key, the self destruct command can only be performed on one tag at a time. This command "electricically and permanently destroy the tag".[SWE02]

*Active Jamming.* [JRS03] The user could carry around an active RFID broadcasting radio signals at random to disrupt the functionality of readers close-by. This is close to the blocker tag solution (5.1). To create an Aloha blocker tag using active jamming is easy (7.1).

*Throttling/Pseudonym Mechanism.* This solution complicate for a malicious reader that tries to trace users. The solution is to change id's in different ways, for example by using the so called throttling/pseudonym mechanism [Jue04]. This solves the traceability problem, but is not a solution to id-hijacking. It is not preventing malicious readers to scan it's id and then reuse it later. Eventually the tag will run out of more id's and one would need to reuse the list of id's or a function to replace them.

*Hash-Function/Hash Chain Technique* This solution intend to do the same thing as the previous, except that the id's are not contained in a list on the RFID, but rather it is "computed" as a function from an original id, but changed for each time a read request is performed. [OSK03]

*External Physical Damage.* Destroying the tag physically by extern physical damage. This could maybe be done by the user by removing the antenna from the RFID-chip.

*Licensing of the Readers.* Readers must be licensed. As a user you have to trust that the readers only read what they are allowed/licensed for. You also have to rely on that no unauthorized readers are present. Each reader is licensed and may have restrictions on what it is allowed to read. [JB04]

Another solution that we will explore more closely using a blocker tag (5.1) to hinder unwanted reading of personal tags.

Find more about this in [HM04].

### 5.1 Blocker Tag

The blocker tag is merely interacting with the singulation protocol (7.2), so that the reader thinks there are lots of tags (actually all possible tags) present, making it impossible for the reader to get useful information from reading tags. This is called a "full blocker" or a "universal blocker" [JRS03]. A blocker tag could be denying access to a certain part of the tree (see 7.2), allowing public tags or private tags ("selective blocker" or "partial blocker"), and further be "polite blocking". [JRS03] Polite blocking will not congest the reader, instead of simulating all possible tags in a subtree, it simply tells the reader that part of the tree is blocked, sparing the reader lots of unnecessary work.

Here follows some examples of usage areas for blocker tags:

*Example 1.* Packed into the plastic in the shopping bags that you get in the grocery store is a blocker tag. It is provided for free by the grocery store, and is no more expensive than the regular plastic bags. This idea was tested earlier this year by RSA Security, of course a negative effect is that shoplifters also can use a it. [GVH04]

*Example 2.* A user who wants to hinder readers to scan the tags of her clothes and the contents of her handbag could wear one or several blocker tags, one that was included when she bought her handbag.

*Example 3.* Malicious blocker tags could be spread out in a grocery store to hinder taking inventory/disrupt checkout for a certain brand, etc.

*Example 4.* During checkout, the customer tells the cashier that his/her previously defined profile will be used, moving the items defined as private from the public to the private part of the tree (i.e. changing the prefix of the identifiers).

The user might have problems relying on that the blocker tag actually works, and that he is protected. Another issue of discussion could be if it should be the user's problem to remember to get and wear the blocker tag.

*Implementation:* The blocker tag could be just a regular tag, but sending out both one and zero when answering requests from readers that are trying to use the binary tree-walking algorithm. A blocker tag might be almost as simple as the low-cost tag, maybe containing two antennas to be able to send out two signals at once. If a simple five cent tag exist, then it should be possible to create a blocker tag that might not exceed ten cents. [JRS03]

### 5.2 Using Cryptography

If one could encrypt everything sent between the tag and the reader safely, the whole problem with privacy could be solved. The problem with low-cost tags is that one cannot implement any kind of cryptography. Using a more sophisticated and equipped RFID-tag one could implement more functions, perhaps one could even use public key cryptography, but then the cost of the tag may prevent it from being used. [SWE02]

### 5.3 A Hash-Lock Solution

The tag can be locked the user giving the tag a metaID to prevent unauthorized reading. Only if a key is given to the tag, which encrypted will result in the metaID, then the tag will be unlocked. The tag has to be unlocked to let the reader know any data from the tag, or to change the data in the tag. [WSRE03]

## 6 Solutions to the Security Problem

In previous chapters, we have described the threat to security when taking an RFID system from a closed environment, such as a production line at a factory, and introducing it to an open environment where anyone can be listening to the traffic. Here we have the need to secure our communication to prevent information leakage.

One more problem is the fact that if you are to afford to put RFID tags on cheap items to facilitate the handling of them, then the RFID tags must be cheap. In electronics, the more you put in an IC the more it cost, hence the low-cost RFID tags of the future will have only limited amount of memory and computing power. The tags with these characteristics will be less capable of performing ordinary cryptographic calculations. [Jue04] introduces a security model and a protocol for low-cost RFID tags that will still be able to achieve “good-enough” security.

Below you will find some different solutions to the security problem:

- Close range. One advantage of RFID system is the physical limitations of the transmissions. The tag uses low power to send its data, and a person who wants to listen in must be relatively close to be able to pick up the transmission. In the 13.56 MHz band, which is one of the dedicated frequencies for RFID, the distance is about 1 m.
- The low computing power of the tag reduces the brute-force attack where an adversary “guesses” the key. It is not possible to run all possible key by the tag, because the response time is to long for this to be successful during the short time period when the tag is in range.
- The assumed power of the adversary can also be considerable less than that of an adversary of a wired network. [Jue04] proposes a model where the adversary is assumed to be portable.
- The aspect of fraud, that someone can change the data on a tag, is easily stopped by using write-protected tags. But what if the operation of the system is relying on the function that the reader can add or change information

on the tags? Then the formerly proposed solution is not an option. In this case, there is a need for a protocol that authenticates the reader to the tag before updating. [Jue04] proposes a minimalistic protocol that achieves this.
- The problem of information leakage can be reduced if the tag only transmits its id number. Then the adversary must have access to the system database to get some useful information from the eavesdropping. The reader and the database are assumed to have a secure channel [WSRE03], relying on security protocols for larger systems.
- Hash-based access control. If a tag is storing some data, and this is not supposed to be open to everybody, one solution is to lock it by a security schema based on a one-way hash-function. When a tag is locked a metaID, which is a hashed key, is stored at a specific place in memory. The owner of the tag stores the ID and meta ID of the tag in its database. To unlock the tag, the owner (reader) queries the metaID from the tag, looks up the appropriate key in the database, and the transmits the the key to the tag. [WSRE03] Only the one who has the key can read the data stored on the tag. The hashing functionality is a relatively low-cost operation and may be implementable in the coming low-cost tags.
- Silent tree walking. In the singulation process where a reader determines the id's of the present tags, the tree walking algorithm (7.2 can be used. An adversary can listen to the broadcasts of the reader from a much greater distance than it can listen to the tag. To force an adversary to be close, and therefore maybe cancel the possibility to spy, a shared secret between the reader and the tags can be sent from the tags to the reader. In the tree walking algorithm, the reader sends a prefix, and queries the tags for their next bit. For a given setup, the tags already may share a prefix, and then this may not need to be transmitted in the queries at all. Another reader will not get the whole picture.
- Detecting false read attempts in the system. The difference between the reader and tag transmission is great, and therefore it is possible to detect false active readers in the tag frequencies. If a false reader tries to kill tags, it could be possible to use tags that "screams" when being killed, and in that way notice any attempt to destroy tags.

This was a taste of the techniques for securing the RFID, and there are more. We refer to the references at the end of this paper for further reading.

## 7 Anti-Collision Solutions

Imagine that you have a customer checking out a shopping-cart filled with lots of items. The shopping-cart is passing the TAG-reader and the TAG-reader calls out to find out what goods are in the cart. Chances are that all the tags call out their id's at the same time and there will be reading collisions.

Several solutions to this problem exist, but we will present two solutions that could be used; one probabilistic solution that might be "good enough" for many implementations, and a deterministic solution that will find all tags. The problem to keep in mind when looking at solutions is that most of the implementation must be in the reader due to low computing capacity of the low-cost tags.[Wei03]

The Aloha algorithm is more commonly used by systems operating under the 13.56 MHz band and the binary tree-walking algorithm under the 915 MHz band. [SWE02]

### 7.1 Aloha/Slotted Aloha

The Aloha algorithm is often used as an example but it is also used, for example in Ethernet. If all the RFID-tags answers the reader at the same time, there will be a collision. If a collision is detected, the tag will resend within a random time. The random time will result in that fewer collisions occur.

The slotted Aloha algorithm is the same algorithm with a slight modification; time is divided into slots and sending can only begin in the beginning of a slot.

This algorithm works fine with systems that are not so highly loaded; for example a sorting mechanism for luggage where the luggage is appearing at a certain pace, one or just a few at a time. The problem with this algorithm arise when increasing the number of items that may respond, i.e. the tags, there will also be more collisions. For implementations in the case of a shopping-cart the binary tree-walking algorithm (below) would be more suitable.

*Implementation:* The tags must be able to generate random numbers, and also either one of these solutions:

- have the possibility to detect collisions (and understand that it has to resend) or
- to be able to be "checked" and told to be quiet if the detection of collision is only done by the reader

### 7.2 Binary Tree-Walking Algorithm

This algorithm solves the problem of having a lot of responses. It can manage to identify a huge amount of tags.

*Implementation:* We assume that the tags answer to a ping if they hear the beginning of their tag's id, and the answer they send back is the next bit of their id.

*Algorithm* The reader traverses the tree starting at the root. In this case all tags will answer giving the next bit in their id-number, resulting in a collision if they have different prefixes. If there is a collision, the reader traverses both subtrees, adding “0” to the end of the prefix if it is a left subtree and “1” if it is a right subtree, and now asking again if there are tags with this new prefix. In the case of an answer from only one of the subtrees, the reader walks down this branch. When the reader reaches a leaf in the tree, the prefix is the same as the id of the tag. This process is also referred to as “singulation”. [Wei03]

*Implementation:* To know if you are at a leaf we have two suggestions:

- the tags id-number are of a certain length or
- the reader has to walk down the branch one more level, testing for the same prefix+”1”, or prefix+”0”, getting no answer from any tags, and therefor the prefix must be a leaf in the tree, i.e. a single tag.

## 8 Proposals for a Low-Cost RFID Solution

Tags could be devided into groups of functionality depending on the usage. Here is our proposal of this division.

*Low-Level Identification [of Groceries]* In this level the simplest and cheapest tag available should be used. The only functionality of the tag is to indicate it’s id-number. No cryptography is used. A solution to the privacy problem using this type of tag is that the user (read customer) has to use a blocker tag if she does not want the tag to be visible.

*Identification of Items* The difference to the prior tag is that this tag should not force the user to wear a blocker tag.

These tags could still be low-cost, but need some more hardware/software solutions to be able to implement some privacy and security solutions. Identifying what parts we would like to have in this solution, this would be:

- selective blocking
- encryption of data
- kill function

Why both selective blocking and kill function? As a user, you should also be presented with other fail-proof solutions at different levels; such as kill tag/self destruct, physical remove (it feel more safe to do it physically yourself), external physical damage (breaking), blocker tag (jamming) solution, or a combination of these.

The solution where you can move the tags from public to private zones as presented in 5.1, and a “partial blocker”-solution, requires some more logic in the tag to be able to implement.

*Higher Level Tags* More expensive tags will of course co-exist in parallell with the low-cost tags. These will implement the same functions as the more simple tags, and have more functions in addition to these. The biggest difference is the ability to perform cryptography, due to the larger computing power and memory.

### 8.1 The Supermarket Example

Remember the supermarket example. The store uses RFID to track the goods and have an automated stock-taking and ordering of new supplies continuously.

In the future the customer may want to use the tags in her own home, as suggested in 2. In the meantime the customer must be able to feel secure and to be sure that her privacy is not compromised.

The solution that we propose is to use the "Identification of Items"-tags, where the user always can use the kill function or selective blocking as default. It is important that the solution does not force the user to use some special tag/actively choose every time he is shopping. This new way of handling items should be transparent to the user and not having to do lots of extra work. When a user wants to use the tags outside of the store she can apply at the supermarket to be able to choose which items that should not be de-activated by default.

# References

[GVH04] Thomas Claburn George V. Hulme. Rfid's security challenge, security – and its high cost – appears to be the next hurdle in the widespread adoption of rfid., November 2004. http://www.informationweek.com/story/showArticle.jhtml?articleID=52601030.

[HM04] Dirk Henrici and Paul Müller. Tackling security and privacy issues in radio frequency identification devices. In Alois Ferscha and Friedemann Mattern, editors, *Pervasive Computing*, volume 3001 of *Lecture Notes in Computer Science*, pages 219–224, Vienna, Austria, April 2004. Springer-Verlag.

[JB04] Ari Juels and John Brainard. Soft blocking: Flexible blocker tags on the cheap. In Sabrina De Capitani di Vimercati and Paul Syverson, editors, *Workshop on Privacy in the Electronic Society – WPES*, pages 1–7, Washington, DC, USA, October 2004. ACM, ACM Press.

[Jou] RFID Journal. RFID Journal, 2004-11-25, http://www.rfidjournal.com/.

[JRS03] Ari Juels, Ronald Rivest, and Michael Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In Vijay Atluri, editor, *Conference on Computer and Communications Security – ACM CCS*, pages 103–111, Washington, DC, USA, October 2003. ACM, ACM Press.

[Jue04] Ari Juels. Minimalist cryptography for low-cost RFID tags. In *The Fourth International Conference on Security in Communication Networks – SCN 2004 (to appear)*, Lecture Notes in Computer Science, Amalfi, Italia, September 2004. Springer-Verlag.

[Leg] Lego Kidspotter. 2004-11-25. http://www.lego.com/legoland/billund/whatsnew/?locale=2057.

[Mat] Mattias Allared, Software Engineer at Sportident. Phone Interview, 2004-11-25. http://www.sportident.se/.

[OSK03] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. Cryptographic approach to "privacy-friendly" tags. In *RFID Privacy Workshop*, MIT, MA, USA, November 2003.

[REC04] Damith Ranasinghe, Daniel Engels, and Peter Cole. Low-cost rfid systems: Confronting security and privacy. In *Auto-ID Labs Research Workshop*, Zurich, Switzerland, September 2004.

[Sar04] Sanja Sarma. Integrating rfid, October 2004.

[SWE02] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels. RFID Systems and Security and Privacy Implications. In *Workshop on Cryptographic Hardware and Embedded Systems*, volume 2523 of *Lecture Notes in Computer Science*, pages 454–470, 2002. http://citeseer.ist.psu.edu/sarma02rfid.html.

[Wala] Wal-Mart to Expand RFID in 2005. http://www.rfidgazette.org/2004/07/.

[Walb] Wal-Mart RFID Deadline Won't Be Met. http://www.reed-electronics.com/electronicnews/article/CA481710.html.

[weba] IBM webpage. Så mäts din tid, 2004-11-25, http://www-5.ibm.com/se/info/vasaloppet/tech.html.

[webb] Sportident webpage. 2004-11-25. http://www.sportident.se/.

[web04] Vasaloppet webpage. Beställ resultat som SMS, 2004-11-25, http://www.vasaloppet.se, 2004.

[Wei03] Stephen Weis. Security and privacy in radio-frequency identification devices (master thesis), May 2003.

[WSRE03] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels. Security and privacy aspects of low-cost radio frequency identification systems. In Dieter Hutter, Günter Müller, Werner Stephan, and Markus Ullmann, editors, *International Conference on Security in Pervasive Computing – SPC 2003*, volume 2802 of *Lecture Notes in Computer Science*, pages 454–469, Boppard, Germany, March 2003. Springer-Verlag.

[Yos] Junko Yoshida. Clothier Benetton adopts Philips' RFID technology for 'smart' labels, 03-11-03. 2004-11-25, http://www.embedded.com/story/OEG20030311S0028.