TECHNISCHE
UNIVERSITÄT
WIEN

VIENNA
UNIVERSITY OF
TECHNOLOGY

MASTERARBEIT

Practical Vulnerability and Threat Evaluation on Security and Privacy Aspects of RFID and Contactless Smart Cards

Ausgeführt am Institut für

Softwaretechnik und interaktive Systeme

der Technischen Universität Wien

unter der Anleitung von

O.Univ.Prof. Dipl.-Ing. Dr.techn. A Min Tjoa

durch

Stefan Pöchlinger

Wilhelminenstrasse 39/16

1160 Wien

Wien, am

Eidesstattliche Erklärung

Ich erkläre an Eides statt, daß ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Wien, am

Abstract

Radio Frequency Identification (RFID) provides the basis for the envisioned "internet of things" and ubiquitous computing. Numerous publications, exposing new potential threats or providing safeguards to them, appear every year, creating a diverse research field. We study this available literature in the RFID field and give an overview of the trends in RFID research and provide a number of observations on RFID.

The first part of this thesis gives an introduction to RFID and describes the basic functions of RFID. The following part examines available literature reviews on either RFID or security. Subsequently, we will study the current state of the art in RFID research and observe a number of facts that influence RFID research. Finally, this thesis gives a small statistical overview and a simple classification of the examined literature.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Radio Frequency Identification (RFID) is a technology for wireless information exchange over short distances. This work examines the current state of the art in RFID security and privacy and contributes a literature review based on over 150 publications. It features an overview of other literature reviews on both RFID and security. Moreover, this work contains a number of observations on the current knowledge on RFID security and privacy and studies different threats to RFID as well as approaches to protect RFID systems from these threats. In that chapter, we will also analyze new threats like RFID viruses and security case studies on the new RFID equipped e-passports. In addition, this work also contains a small statistical part on available RFID literature and a classification of the examined publications based on the presented observations.

Even though the RFID technology itself was developed during the last 50 years, recent developments in the field of low cost RFID devices began to finally show its ultimate potential [77]. The possibility of adding (minimal) computing capabilities to everyday objects will most certainly make RFID ubiquitous in the near future [166]. RFID transponders will then be added to clothes, supermarket products, medicine and many other items, creating an ever present computing environment, in all parts of everyday life. Even today, RFID commerce already constitutes a vital and expanding market [80].

Judging by evidence from recent years, RFID industry will continue its rapid growth during the following years (see figure 1.1).

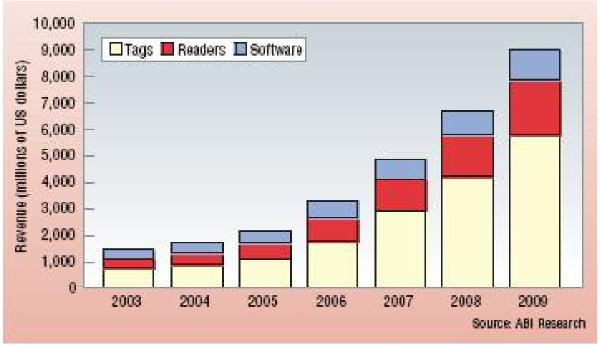

Figure 1.1: RFID sales growth (from [80])

Most obviously, a technology, so promising and potent, raises vast concerns about security and privacy. Spreading news about major economic players adopting RFID has caused initiatives by data protection activists[1]. Today, RFID receives enormous attention from both the media and on the web[2]. Criticism sometimes even takes rather hysterical forms, as some critics use theological arguments against RFID. They cite a passage from the New Testament's "Book of Revelation", saying that "[the Beast] causes all [...] to receive a mark on their right hand or on their foreheads..." ([179] page 31). This is where RFID implants are placed in the human body. While most of these implants are strictly for medical reasons (i.e. notifying medical personnel of the patients individual needs), some RFID implants are used by nightclubs as some sort of "cool" payment system[3]. This causes another correlation with the "Mark of the Beast", which the bible describes as a prerequisite to buy or sell any goods ("...so that no one could buy or sell unless he had the mark."). For this reason, a small group of religiously motivated RFID critics sees RFID as a tool of the "antichrist".

[1] see, for example http://www.boycottgillette.com

[2] See http://www.rfidjournal.com

[3] See http://www.theregister.co.uk/2004/05/19/veripay/

1.1 Why RFID

RFID offers a cheap and efficient way to add automatically processable data to objects without requiring physical or optical contact. Therefore, RFID enables automated data collection without causing unnecessary delays or sacrificing customer convenience. Because of this, RFID is used in automated supply chain management, where it enables automatic scanning of goods on entering or leaving factories, automatically adjusting logistics and thereby reducing out of stock times. In addition, RFID is used for access control, animal tagging and is envisioned to replace the bar code as point of sale technology [179]. All of these applications increase consumer convenience. People only have to wave their wallet, containing an RFID transponder, close to a reader to pass secured gates, animal shelters can inform owners about impounded tagged pets and supermarket customers experience less out-of-stock items, through automated reordering.

While all of these ideas are excellent in theory, in practice they show their shortcomings. Contact less access control is vulnerable to some of the attacks presented later in this work and therefore not yet applicable to high security areas. Item level tagging in supermarkets is still to cost intensive [161], as obviously, it is economically ridiculous to embed tags, of about 50 cents to one dollar cost, in products of roughly the same price. Last, the animal tagging system suffers from the diversity of standards and suppliers. Thornton et al. ([179] page 12) present a story about pet, being euthanized, because the shelter was unable to detect its tag. This happened because the tag came from a different supplier than the shelters reader. Therefore, a lot of work is required on cost factors, standardization and security before RFID finally becomes a truly ubiquitous technology in everyday life.

1.2 History of RFID

Even though RFID is a fairly new technology, it has a rich history. Landt [107] traces the ancestry of RFID back to the beginning of time. The electromagnetic remnant of the Big Bang, the scientific explanation for the creation of the universe, is the energetic background of RFID. With the advance of radio transmission technologies at the beginning of the twentieth century and the invention of radar during World War II, the real history of RFID was about to begin.

Landt dates the appearance of RFID back to October 1948, the publication date of Harry Stockman's landmark paper [176]. The following years saw several RFID related technologies, like the "identification, friend or foe (IFF)" system for airplanes. The IFF was a form of long range transponder system, invented to ease the identification of airplanes in armed conflicts.

In the 1960s several other important papers and inventions [185] were published that fostered the development of RFID. First commercial uses, like EAS (electronic article surveillance) systems appeared. These are simple anti-theft devices, mostly only capable of revealing the presence or absence of cheap 1-bit tags.

The 1970s saw an increasing development speed for RFID, as more and more governmental and academic institutions began to actively work on RFID applications. Furthermore, several large companies like Philips and General Electric became active in the new market. Landt sees a conference in 1973, sponsored by the International Bridge Turnpike and Tunnel Association (IBTTA) and the United States Federal Highway Administration, as one of the most important events of this decade. It concluded "there was no national interest in developing a standard for electronic vehicle identification", thus encouraging companies to develop a variety of systems. According to Landt, this was extremely important for the RFID technology in its infant stages.

Increased industry investments and new technologies like integrated circuits, microprocessors and better communication networks allowed the development of what we today know as RFID until the 1990s. The invention of systems, like the EZ-Pass, an automated toll collection system, marks the beginning of a new era in the development of RFID. With the increased adoption efforts made by companies and the development of new technologies that caused a continuous decrease of RFID cost, new applications begun to spread at a very fast rate. New uses for RFID, including item management, and the bar code replacement EPC (Electronic Product Code), caused lots of companies to enter the market, creating a vivid and ever expanding marketplace. In addition, lots of inventions have been made in this field. At the publication date of Landt's paper [107], in October 2001, over 350 RFID related patents existed, in the US alone.

Decade	**Event**
1940 - 1950	Radar refined and used, major World War II development effort. RFID invented in 1948.
1950 - 1960	Early exploration of RFID technology, laboratory experiments.
1960 - 1970	Development of the theory of RFID. Start of application field trials.
1970 - 1980	Explosion of RFID development. Test of RFID accelerate. Very early adopter implementations of RFID.
1980 - 1990	Commercial applications of RFID enter mainstream.
1990 - 2000	Emergence of standards. RFID widely deployed. RFID becomes a part of everyday life.

Table 1.1: RFID timetable (from [107])

Chapter 2

RFID Basics

Here we will present an overview on the components and functions of an RFID System. Subsections will include a discussion of major RFID standards and some basic malicious operations feasible on such systems. In addition, we will present important facts for discussing RFID security and privacy, like the difference between forward and backward communication channels or the different collision avoidance mechanisms in RFID environments.

2.1 RFID architecture

The typical RFID system consists of three parts: Readers, tags and a data-processing subsystem. These components will now be discussed in detail.

2.1.1 RFID transponder (tag)

An RFID transponder is most of the time referred to as *tag*. Other possible names, mentioned in [179] include *label* or *chip*. For this work, we will subsequently refer to it as tag. Tags receive radio signals and automatically transmit appropriate responses.

They roughly consist of two parts. A microchip, for all computational purposes, and a coupling element (antenna), for communicating with other devices. To discuss their functionality, the following categories of tags have to be distinguished:

passive tags Passive tags rely on energy transmitted by the reader. On being queried they collect enough energy to compute and transmit the response. To do so they have to be inside the reader's *near field*. The near field is a physical phenomenon based on the device's frequency. For a RFID reader operating on 13.56 MHz, one of the most common RFID frequencies, the near field is 3.5 meters [179]. Regardless of the nominal range, the reader-to-tag distance can never exceed this range.

active tags These tags have their own power source. Therefore, they can communicate over far greater distances, but are a lot more costly than passive tags.

semi-passive tags Semi-passive tags contain their own power source, but need to be in a reader's near field to be activated.

2.1.2 RFID transceiver (reader)

The term *transceiver* is a combination of *transmitter* and *receiver*, while the commonly used term *reader* originates from the fact that they can be seen as "reading" tags. Handheld readers usually have an integrated antenna; stationary ones tend to have separate (and bigger) antennas. Readers are usually placed on strategic positions (e.g. entrances) to read all passing tags. Obviously, they are less cost critical than tags, as far less of them are needed to create a useful system.

Readers serve as connection between the data-carrying tags and the data-processing subsystem.

2.1.3 Excursus: communication channels

When discussing RF communications, it is important to distinguish between the *forward-* and *backward* channels. The first one denotes reader-to-tag transmissions, while the second represents the other way round. Forward channel communications are a lot easier to eavesdrop for adversaries than those over the backward channel, especially in combination with passive tags. This is due to the fact that readers a more powerful (bigger antenna and more energy supply) and therefore transmit clearer signals over greater distances.

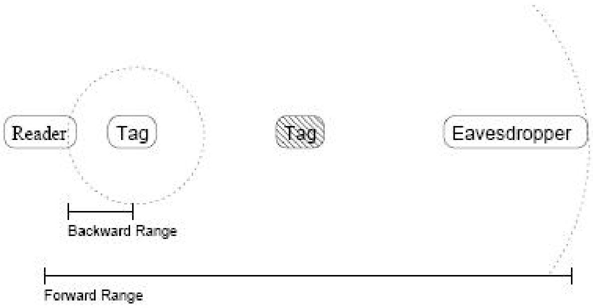

Figure 2.1: The eavesdropper is unable to monitor the backward channel, while the reader can not recognize the shaded tag. (from [187])

2.1.4 Excursus: anti-collision behavior

When talking about anti-collision behavior, there are basically two approaches. First, tags with *deterministic* anti-collision behavior contain an individual unique meta-identifier, in addition to their usual application level identifier. If a reader receives more than one answer at a time, it queries the responding tags for their meta-identifiers, to single out the tag, it intends to communicate with. This process is sometimes referred to as "singulation" [89]. The second approach, is called *probabilistic* anti-collision behavior. The term describes all methods aimed at decreasing the probability of collisions, like transmitting messages at random intervals.

A typical protocol implementing probabilistic anti-collision behavior, is the slotted ALOHA protocol, utilized by the ISO-14443 standard. The name originates from the ALOHANET, a hawaiian communications network, for witch the original ALOHA protocol was developed. ALOHA based tokens cease transmission if a collision occurs and retransmit after randomly chosen intervals. The protocol's success is based on the fact that the probability of two colliding tags, retransmitting at the same delay, is quite low. In the *ALOHA protocol*, two types of collision are possible. Depending on how much the messages overlap, one talks of full or partial collisions.

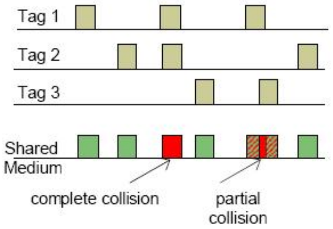

Figure 2.2: An example for collisions in the Aloha protocol (from [21])

The *slotted ALOHA protocol*, being used now, is an improvement of the original protocol, using fixed time slots for communication. Obviously, if tags can only transmit at fixed intervals, no partial collisions do occur.

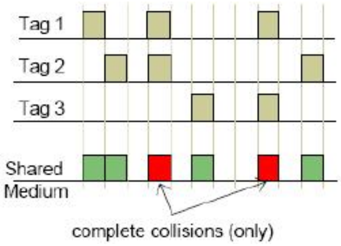

Figure 2.3: Collisions in the slotted Aloha protocol (from [21])

2.1.5 Data-processing subsystem

The data-processing subsystem is, roughly spoken, some sort of computer. It consists of a back-end database, for storing the read information, and the *middleware*, responsible for exchanging data between the reader and the database. In addition, middleware performs any necessary transformations on the received data. Depending on the system, back-end and middleware can be either placed on a single, stand-alone machine or distributed over a whole network [179].

2.2 Relevant RFID technologies

There are several important standards inside the RFID domain. Here we will present the ISO-14443 (Vicinity Cards), the ISO-15693 (Proximity Cards) and the EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol standards. In the latter case, we will focus on the functionality of the EPCglobal network, for which the standard was invented.

2.2.1 ISO standards for contactless smart cards

Under the title "Identification cards - Proximity integrated circuit(s) cards", the ISO-14443 standard describes contactless smart cards with a range of approximately 15cm. According to Finkenzeller [56], these are predominantly used for "ticketing" purposes. The norm consists of four parts, defining values like card size and operation frequencies. An interesting remark is that the standards body was unable to agree on a single communications interface [56]. Therefore, the ISO-14443 standard defines two entirely different signal interfaces, type A and B, using individual modulation. In addition and even more important in the given context, type A and B differ in their anti-collision behavior. While type A uses a deterministic approach, based on the cards identifier, type B utilizes slotted ALOHA protocol.

The ISO-15693 standard is called "Identification cards - contactless integrated circuit(s) cards - Vicinity cards". Such vicinity - coupling cards are contactless smart cards of around 1 m range. Finkenzeller [56] sees their archetypical usage in access control, as they can be read without being taken out of the pocket or bag in which they are carried.

2.2.2 The EPC network

The EPCglobal Network is a technology which allows real-time documentation and discovery of particular goods in a supply chain. To exchange information, it uses the ever expanding internet.

Initially, the EPCglobal network was invented by the Auto-ID-Center, which was founded to develop a global, cost efficient system based on open standards. Nowadays the Auto-ID-Center serves as research division for the EPCglobal Inc., a non-profit organization for global implementation of the EPCglobal network. EPCglobal Inc. has taken over the development of standards and published the Generation 2 protocol. This protocol is globally valid, but not backward compatible to the first generation by the Auto-ID-Center. Of course, it does offer certain advantages over its predecessor [56]:

- Dense reader mode: Prevents disturbance of neighboring readers.
- Separation of memory into four independent sectors, eases storage of individual data on a product.
- Tags are handled like bar codes, several tags are allowed to carry the same EPC (eases barcode migration)
- Better bit-encoding for increased tag detection rate

The EPCglobal Network defines five basic services:

Electronic Product Code (EPC) A unique number to identify products in the supply chain.

Identification System The system of tags and readers used together with the EPC.

EPCglobal Middleware Administrates data sent by the readers and serves as software interface to the EPCglobal network's internet based services.

Discovery Service (DS) Group of services that allows finding data on particular EPCs. The Object Naming Service (ONS) is one of them.

EPC Information Service (EPCIS) Allows exchange of EPC related data over the EPCglobal network.

World Wide Web	**EPCglobal Network**
DNS	ONS
Web Sites	EPC Information Services
Search Engines	EPC Discovery Service
Security Services	EPC Trust Services

Table 2.1: This table compares the services of the EPCglobal Network to those of the World Wide Web (from [56])

For a practical implementation of the EPC network, further reduction of its most central cost factor is required. This is obviously the production cost of EPC tags, as vast numbers of these are necessary to tag all items by an RFID adopting manufacturer. Typical EPC transponders are cheap tags, with a minimum functionality, which are placed on any manufactured unit of a good. They contain the EPC, along with some optional information about the product. At the same time, only few readers, on strategic positions, e.g. at the entrance and exit of production facilities, are required to record any change of information on the tags.

The Electronic Product Code

The EPCs themselves are license plate type numbers stored on every EPC tag to identify the accompanying product. As a fundamental difference to bar codes EPCs can identify individual pieces of goods. Technically, they are stored on the EPC tags memory as bit strings of individual length, consisting of a header and various data fields defined by it. Current definitions cover EPCs with 64 - 96 bits. The EPC is stored in one of the memory sectors of the tag, mentioned earlier. Two of the other sectors, or banks, are reserved for vendor specific information and optional *kill* and *access* passwords. The fourth bank is reserved for user defined input. On presentation of the 32-bit access password a tag transitions into *secured* state, a prerequisite for executing any critical query like the *kill* command. The *access* functionality is optional, so a zero value in the password field indicates that *secured* state is not required for such queries. To physically disable the tag, a 32-bit *kill* password must be provided. If the value of this field is zero, the tag does not execute kill statements [77].

How the EPC network works

Finkenzeller ([56] p. 313) presents a nice overview on the procedures inside the EPC network. Every company handles information regarding EPC tagged objects individually and all of the information should be available solely on the EPC network. When an object is tagged, all related information is stored in the manufacturers EPCIS (EPC Information Service). The EPCIS then registers this entry with the global DS (Discovery Service). After a tagged object is subsequently shipped to another company, the new owner updates his EPCIS with a corresponding entry and again registers it with the DS. To get all information about the object, the new owner now must look up the original manufactures EPCIS IP. To do so, she first queries the EPC network's root ONS for the manufacturer's local ONS, then the local one for the IP of the manufacturer's EPCIS. The required manufacturer ID is a substring of the object's EPC. Finally, the user can now query the manufacturer's EPCIS for all information related to the EPC on the tagged object.

2.3 Basic attacks

In this section we will discuss some of the most basic attacks feasible on RFID systems. Only "protecting the data" is not enough to prevent them, as serious damage can be inflicted to such systems without ever changing data [179].

2.3.1 Spoofing

Spoofing means supplying false information that looks valid and is therefore accepted by the system. An example for spoofing in an RFID environment would be broadcasting incorrect EPCs (Electronic Product Codes).

2.3.2 Replay

If an adversary intercepts and records a valid transmission, she can perform a replay attack. In such an attack the recorded data is transmitted to the reader later on. Because this data appears valid, the system will accept it. Replay attacks can be defeated by adding encrypted timestamps to queries. As these require computational capacities, they are hardly feasible with low cost tags.

2.3.3 Denial of service (DOS)

A DOS attack takes place, when an adversary "floods" (hence, its second name: *flooding*) a system with more data than it can handle. By doing so, the system is prevented from performing necessary operations and answering real requests. An RF significant variant of this attack is *RF jamming*, when the communications channel is blocked by radio noise [179].

2.3.4 Track and trace

The terms "tracing" and "tracking" are often used interchangingly. For scientific precision, we will subsequently use the term "tracking". Tracking means that adversaries can identify tags they read before (e.g. by a static identifier). This can be used to for several malicious practices. In the most harmless case, a merchant could use this to target advertisement individually at wealthy passersby. Of course, if the same technology is used by thieves to identify potential victims, the situation looks a lot less harmless. In addition, automatically collected data about a person's whereabouts is available to RFID implementers. In the future, the fact that a tag was read at a particular time and place could be used in court.

Tracking is also the threat that customers are most aware and afraid of. According to Thornton et al. [179] this results from a vast number of highly speculative and misleading media reports. For the same reason, tracking has received a lot of attention by the scientific community. Numerous proposals on enhanced privacy [4, 89, 157] have been presented to mitigate the tracking problem. However, some findings by Avoine and Oechslin [10] indicate that tracing will remain a problem for some time.

2.4 Practical RFID examples

Thornton et al. [179] present several case studies on applied RFID. They try to separate success stories from failures, but have to admit that there are no real examples for the latter case. This is due to companies, regarding their RFID initiatives as to premature to be considered a failure. However, Thornton et al. decided to present Benetton, which planned to tag clothes, and the Metro Group, which issued RFID equipped loyalty cards, as failure examples. Both companies had to back down after privacy advocates organized protests against their plans. From those examples, Thornton et al. take some important lessons for RFID deployment:

- Anticipate privacy concerns
- Take steps to mitigate privacy intrusion issues
- Demonstrate the steps being taken to protect consumer privacy, and put control in the consumer's hands
- Make full disclosure of any initiative that "touches" consumers with RFID

More successful examples of RFID deployment are Walmart and the US Department of Defense (DoD). Walmart requires its suppliers to tag palettes of goods. By doing so they were able to significantly reduce the number of out-of-stock items and the time to replace them. In addition, the DoD applied RFID to "solve the US military's logistic challenges" [179]. At first, the DoD´s adoption of RFID was bound to very strict deadlines. However, these caused so much problems that they soon had to be extended. Nevertheless, the two "marketplace giants" [179], adopting RFID technology, force hundreds of suppliers to invest into RFID. Thornton et al. expect this, to have serious impact on the growth rate of the RFID market. Other early adoptions of RFID are Exon-Mobile's Speed-Pass contactless payment system and the EZ-Pass, a toll payment system. Both of them have been proven to be insecure [179], but provide so much convenience that they find widespread acceptance among consumers. Therefore, Thornton considers both of them as success stories.

Chapter 3

Related Work

Comparative literature reviews have been presented on all types of scientific topics. A simple search via a scientific search engine (in our case: scholar google) will reveal the broad variety of available work using this approach to literature. However there are not many literature reviews on our intended topic. We had to resort to other topics to provide an accurate overview on literature reviews and to find examples that can serve as starting point for our own investigations. Therefore, we decided to present work form both contexts we deal with, namely RFID and security/privacy. In the second field we will focus predominantly on works, we believe to have some relevance in the RFID context.

3.1 Related work on RFID

Our initial search on "scholar google" yielded no result. Concluding that our search terms *"comparative literature review" RFID* and *"comparative literature survey" RFID* were to strong, we started a new search for *comparative "literature review" RFID*. This time, we found at least some results. For sake of completeness, we repeated this search on the ACM portal site and the IEEE Xplore digital library, but experienced exactly the same situation. Only the weaker, less strict search terms discovered some results at all. However, most of the reviews, we found in the RFID field, are not true comparative literature reviews. They simply feature a short literature review, prior to some empirical survey. In addition, the literature reviews [68, 113] on our core topic, the privacy and security topics of RFID, were not among this results. We found them, using Avoine's online bibliography [7], a good and actual source for RFID security related papers. The following sections describe the most interesting examples for literature reviews related to RFID, divided in two parts: One for papers combining a literature review and another approach and one for "pure" literature reviews.

3.1.1 Literature reviews as starting points

Many authors combine literature reviews with other scientific methods like case studies or interviews, to prove their point. A typical example for this approach is [125]. Masters and Michaels identify a gap in literature, between technological development and future humancentric possibilities. Therefore, they conducted a study on the current state of humancentric RFID applications using usability context analysis. For their literature review, they identify three different contexts, and analyze the corresponding literature separately: *control*, *convenience* and *care*. In a critical response to the existing literature they state that only few articles on humancentric RFID are based on case studies or interviews. The rest of them are news type, reporting a particular event and subsequently speculating about utopian future developments.

Another work in the healthcare context is presented by Lee, who wrote a doctoral dissertation [109] about a survey on the adoption of RFID in US hospitals. His literature review mostly covers studies and surveys on the adoption of technological innovations. In addition, his interest is on the relationship between information technology and the healthcare industry, as well as on previous studies on RFID in healthcare. However, the main part of his review deals with reasons and inhibitors for technology adoption in general and not with RFID. Lee does provide a rough overview on RFID costs in healthcare stating that RFID will reach a volume of 8.8 billion Dollars in 2010, as many hospitals hope to establish RFID systems in the near future. Furthermore, he enumerates known application areas in healthcare. These include tracking medical supplies and medicine, patient tracking and locating medical staff. One hospital has also tested tagged beds to improve maintenance procedures. Nevertheless Lee's literature review is mainly a starting point for his survey and subsequent data analysis. He concludes that unlike expected, vendor advertising and financial readiness are minor factors for RFID adoption in healthcare. Instead, rather small hospitals with significant IT knowledge are most likely to adopt RFID.

Apart from healthcare, RFID's adoption for various purposes has already been considered. For example, Hou and Huang [75] combine a literature review and an industry survey to identify the important issues for RFID's adoption by the printing industry. Furthermore they provide quantitative cost and benefit analysis to provide supporting information on RFID adoption for decision makers. Therefore, they feature a number of equation models, together with tables revealing cost and efficiency factors to evaluate an RFID implementation's feasibility.

3.1.2 Pure RFID literature reviews

A fully RFID concerned review is presented by Matta and Moberg [126], who develop a research framework for RFID in the supply chain. Their work is based on the claim that "given the positive hype of RFID often found in the trade press and at conferences there is a surprisingly scarce number of conceptual and empirical research articles on RFID in the supply chain and technology literature" [126]. An interesting aspect of their investigation is the differentiation between coerced and free-will adoption of RFID. Which one is the driving principle in RFID adoption, remains a question to be answered. Matta and Moberg find indications for both scenarios. Companies adopting RFID for performance gains indicate free will, while Walmart's suppliers are obviously coerced to adopt RFID.

RFID product authentication techniques

Up to now, all mentioned reviews were fairly unconcerned with privacy and security aspects of RFID. Lehtonen et al. [113] present a literature review on RFID in a security and privacy context. However, they limit the scope of their examination to product authentication. Depending on the functional base of each identified approach, Lehtonen et al. divide them into four categories.

The first two of them imply no tag authentications, while the other two do either authenticate tags or tag data respectively. *Unique serial numbers* are a basic approach, adding a serial to every product. Comparing numbers on products to a list of valid identifiers will then expose counterfeits. An extension of this approach is a *track and trace based plausibility check*. By storing information on a product's movement, illicit products become identifiable. For example a product, being shipped to Norway, can hardly be on sale in the US at the same time. This approach requires a lot of collaboration from business partners, but is a natural complement to the EPC network. The third approach makes use of cryptography to provide *secure object authentication*. Lehtonen et al. analyze several different proposals in this field. Their findings show that it is by far the best covered of the four. The last approach, examined by Lehtonen et al. is the use of *product specific features* to create a digital signature stored on the tag. Product specific features could be physical or chemical characteristics, for example the exact weight.

In addition, Lehtonen et al. [113] discuss relevant elements of RFID authentication methods. All of them provide a trade-off between complexity and security. Both factors are therefore of integrative importance, when evaluating different approaches. For such an evaluation, the survey identifies a number of important factors. These are *cloning resistance* and *detection*, *resistance against removal and reapplying* to other products and the two cost factors *complexity of check* and *tag cost*.

Lethonen et al. conclude there is currently no perfect solution in RFID authentication.

Approach	**Complexity of check**	**Cost of tag**	**cloning resistance**	**clone detection**	**tag reapplying resistance**
Serial numbering	Low	Low	No	No	No
Track and trace	Medium	Low	No	Yes	Yes
Secure authentication	Medium-High	Low-High	Yes	No	No
Product specific features	High	Low	Yes	No	Yes

Table 3.1: Lethonen et al.'s comparison of product authentication categories (from [113])

Especially, there is no proper way to provide offline authentication, as most of the analyzed approaches require server access.

Juels' RFID survey

To the best of our knowledge, Juels [84] presents the most accurate and complete survey on RFID security and privacy. It features not only explanations of functionality and areas of application, but also an appropriate summary of actual security and privacy concerns.

It is noteworthy that Juels makes a fundamental distinction between basic tags (mostly denoted low or lowest cost tags in this work), which lack the resources for any conventional cryptography and symmetric key tags, which support some standard cryptography. Addressing basic tags, Juels speaks of inability "to perform true cryptographic operations" [84]. He views this necessity to provide security without standard cryptography as an exciting challenge, especially because he believes that RFID vendors will choose the cheapest of these tags as potential bar code replacement. Therefore, only privacy protection mechanisms that do not increase the tag's price have a reasonable chance to be integrated. Moreover, he presents some of the most popular scientific solutions to this dilemma like blocking (see section 4.2.1) and solutions for minimal authentication algorithms and key distribution.

Symmetric key tags include standard cryptography and by that standard privacy protection. Therefore, Juels examines more complex attacks which are only interesting to acquire sensitive information or to incorporate the legitimate owner of such a tag. These attacks include cloning via side channel vulnerabilities, relay attacks (see section 4.2.4) and the few available countermeasures, like distance bounding protocols [68]. Other issues addressed by Juels include key management and effective implementations of symmetric key primitives (see section 4.2.3).

He concludes that, as RFID systems will involve massive server infrastructures, many data security problems will look familiar to professionals in that domain. Nevertheless, he emphasizes that RFID systems will also create some new problems through their unique characteristics. RFID tags can be expected to change ownership more often than other, more expensive computational devices. Therefore, the EPCnetwork's ONS (Object Name Service, see section 2.2.2) will face bigger challenges than the Internet's DNS (Domain Name Service). Additionally, as there will be lots of tags in the hands of non-professional users, individual security and privacy perceptions will be especially important.

3.2 Related work on security and privacy

Even though there is only a single literature review on privacy and security in combination with RFID technology, this topic has received extended attention in different contexts. There are numerous reviews on security and privacy in fields like health care, e-commerce and data mining. The latter two are especially interesting, as essential privacy questions in these fields, like "What data is collected?" and "How is data secured during transmission?" apply to RFID as well. The central factor underlying these topics in e-commerce is trust, a question that can easily be anticipated in an RFID context. When RFID tagged object hit the end-user market at a large scale, consumers' willingness to provide data will likely depend on individual perceptions of trustworthiness, just as it does in e-commerce. Therefore this section will present a number of literature reviews on the role and importance of privacy and trust.

3.2.1 Privacy and trust - consumer and employee perceptions by means of e-commerce

Belanger, Hiller and Smith [15] analyze the influence of security and privacy on trustworthiness in electronic commerce. Their study features a literature review about definitions for electronic commerce and a survey on the implications of security and privacy on consumer acceptance of e-commerce websites. Additionally, they present statistical analysis of their survey results, covering trustworthiness perceptions of their study's subjects, US university students.

The importance of individuals' perceptions on privacy in e-commerce is another interesting question. Gauzente [61] examines the different privacy views of merchants and customers. As a starting point for her questionnaire, she conducts a review of existing literature in the privacy field, comparing selected privacy definitions. Additionally, she emphasizes the importance of mutual trust. Customers are far less skeptical if merchants do not request information prior to usage, that is, all personal information must only be provided at the latest possible point. This allows merchants and customers to gradually develop a trust relationship.

Another researcher who has examined privacy in e-commerce is Luo [123]. He exemplifies the role of trust as solution for consumers' privacy concerns. In his study he examines literature from the field of relationship marketing and social exchange theory to identify and demonstrate trust raising mechanisms. Based on recent studies, Luo claims that trust plays a key role in expanding the size of electronic commerce and strengthening the role of the internet as market place.

Furthermore, he presents a trust producing framework based on three different trust building mechanisms. *Characteristics-based* trust focuses on something people have in common. This can be fairly general features like nationality or ethnicity. Everything that indicates similar cultural values creates a sense of community and therefore a feeling of trust toward each other. For example, companies could adopt technologies in a similar way to create inter-organizational trust. *Process-based* trust results from past and expected future exchange. It builds on reputation, gift giving and brand names. This is especially valuable in the business to business context, where purchases repeat at a very fast rate. *Institution-based* trust is more general than characteristics-based or process-based trust, as it is not narrowed down to specific transactions or partners. A typical example for that type of trust is a digital certificate, issued by a trusted third party. Any owner of such a certificate receives trust, based on consumers' perceptions of the trusted third party's reliability. According to Luo, this approach's "formal marketable structure" is best suited for resolving the privacy concerns of the internet. Characteristics and process-based trust can only do this to a limited extent.

3.2.2 The impact of employees' awareness on privacy - policies and organizational structures

The role and importance of policies and regulations together with individuals' awareness and knowledge of them is another factor in any privacy discussion. This topic has therefore found attention in scientific circles and, as a consequence, been subject of literature reviews. For example, Monday and Rudge [133] present descriptive research on e-mail policy, in an Australian winery. They examine literature on e-mail policies, as well as on legal issues and the security and privacy implications of e-mail. Again, this review merely serves as a starting point for their case study. Through this study, Monday and Rudge find that one third of the examined winery employees were not aware of the organizations e-mail policy and even less knew about their privacy options.

In particular environments, where a lot of private information is available, values like awareness and responsibility are even more important. Earp and Payton [47] examine such an environment by performing a survey on privacy perceptions by university employees. Although their main contribution is the survey, they do additionally present a brief literature review on current practices in data protection. In it, they analyze the development of the privacy topic and the corresponding legal situation. Based on this overview, Earp and Payton develop a hypothesis on university employees' privacy perception, which serves as starting point for their survey instrument. They state "academic settings are largely data warehouses of student information, dispersed through numerous autonomous departments". Finally, their survey reveals that university employees are well aware of their responsibility to a large degree. Nevertheless, Earp and Payton identify problems with organizational policies on performance issues and workers' experienced practices. In this context, they demand better articulation of responsibilities in cooperation with organizational policies to resolve these conflicts.

3.2.3 Technological and mathematical approaches to privacy

The technological approach to privacy is taken by Argyrakis et al. [3], who present a short review on privacy enhancing technologies (PETs). Their focus is on the e-government relevance of these PETs. In the analysis, they investigate the PETs on three different aspects: *Confronted security threats*, *applied technological issues* and *satisfied user demands*. The first category is mostly self explanatory, listing typical threats like eavesdropping or malicious collaborators. The technological issues cover reliability, performance and installation complexity. The final category contains typical user interests like anonymity, usability and cost. Following their comparison, Argyrakis et al. conclude there is no dominant solution. Each of the reviewed PETs offers different advantages over its competitors.

A somewhat different and more mathematical view on the privacy topic is presented by Yu et al. [194], who provide statistical analysis on the relationship between consumer attitudes toward e-commerce and a number of demographic and social variables. Their literature review is mainly a starting point for their empirical analysis. Consequently, they analyze literature concerned with privacy perceptions of both business and consumers. In their conclusion Yu et al. state social factors have significant impact on individual privacy perceptions.

3.2.4 The security context

An enumeration and comparison of security-enabling technologies is given by Skoularidou and Spinellis [170], who analyze architectures, implemented in current hard- or software (i.e. firewalls, virtual machines), and theoretical concepts that have never been recognized outside the research community alike. Their work consists of a description of the analyzed concepts, together with a fairly short comparison in tabular form. Skoularidou and Spinellis show how good these concepts protect against the well known security threats *leakage (disclosure)*, *tampering (modification)*, *resource stealing* and *repudiation*. Furthermore, they added two additional serious threats, *malware* and *user ignorance*, because of their practical relevance. In addition, Skoularidou and Spinellis provide non-functional characteristics on the reviewed technologies, like incorporation into existing applications, ease of use and complexity. All of them are fundamental factors for user acceptance. A combination of different reviewed security architectures can offer a finer grained protection.

The adoption of new technologies is likely to raise concerns among both companies and customers. An example of typical concerns on the companies' side is given in [149]. Ratnasingham and Swatman review existing literature on security in the EDI (Electronic Data Interchange) context. By providing an extensive overview of EDI security, together with an evaluation of EDI specific risks and security features, they attempt to give a good starting point for future research. As expected, they find that technological adoption faces a number of barriers: *lack of awareness*, *difficult quantification of Return on Investment* and *high initial capital expense*. In addition, security and legal issues, as well as multiple standards and missing interconnections between them, raise concerns among possible adopters. While these facts on EDI have been stated in 1997, they remind surprisingly of the situation RFID adopters face nowadays. Even the main rationale for adoption, increased efficiency and better performance, reminds of RFID.

Allendorfer and Pai [2] discuss human factors in user identification for the US Federal Aviation Administration. They review the existing literature on *knowledge-*, *token-based* and *biometric* identification systems. All of them have some human factor issues. Users of knowledge-based systems face extended cognitive and social pressures. First, it might be hard to comply with all requirements of a strong password (length, frequency of change etc.). Second, people tend to avoid everything that would be seen negatively among their colleagues. Therefore, they might not protect their passwords well or give them away when asked, in order to not appear paranoid. Apart from that, passwords can be forgotten, but neither damaged nor misplaced nor lost, which is an enormous advantage over the other systems. Token-based systems are especially damaged by loss. If a lost token can not be invalidated, securing the system might inflict serious costs (e.g. replacing locks if a key was lost). Damaged tokens represent another, yet less serious problem. Biometric identification systems have their own human factors. While the identification-factor can not be lost or forgotten, these systems face product maturity issues, resulting in identification problems, when persons change physically, as well as acceptance problems among users. People might feel that their physical characteristics are private and refuse to provide this data. A final remark, this work bears a short note on RFID in the token-based identification section, again showing the spread of this topic.

3.2.5 Privacy concerns on data collection - the data mining case

RFID is certainly not the first example for an advancement that supplies merchants with enormous potential to acquire information. Data mining, for example, is one of these potent technologies. Recent developments in this field encourage Verykios et al. [184] to provide an overview on research in the context of privacy preserving data mining and a classification hierarchy to categorize it. They identify five different dimensions in privacy preserving data mining: *data distribution*, ranging from centralized to distributed data and in the latter case from horizontal to vertical data distribution, *data modification*, distinguishing several methods of modification, *data mining algorithm*, not to be mistaken for the privacy preserving algorithm, *data or rule hiding*, deciding what users are allowed to see, and finally *privacy preservation.* The last dimension is obviously most important in the given context.

Verykios et al. present three different approaches, to avoid jeopardizing privacy in case of modification: *heuristics-based*, *cryptography-based* and *reconstruction-based.* First, as selective data sanitization is an NP-Hard problem, the arisen efficiency problems can be addressed through heuristics. The issue with cryptography based approaches is the Secure Multiparty Computation (SMC) problem. In other words, how can two parties conduct a computation with private inputs, without disclosing them? Finally, reconstruction-based data-mining operates on perturbed and reconstructed data, to prevent privacy intrusions. Verykios et al. give formal definitions for this fact, as well as several possible solutions, but these would go far beyond the scope of this chapter.

Moreover, they discuss the quality of privacy preserving algorithms in four dimensions: *performance*, *data utility*, representing the loss of information or data functionality, the *level of uncertainty* at which hidden information can still be predicted, and *resistance* to data mining. Following their review, they conclude that the diversity of data mining algorithms makes it almost impossible to assess the value of privacy preserving algorithms for more than one data mining algorithm.

All data collection technologies are especially privacy critical when targeted at minors and systems where minors represent the majority of users. Such a scenario is presented in [37]. Chung and Grimes examine data mining and information management practices on online entertainment sites for children. They utilized a multidisciplinary search on scholarly databases to acquire available papers on this topic as well as current market research trends. In addition, they combined their findings with data from a case study on children's online gaming communities. In doing so, they provide both quantitative and qualitative analysis alongside a historical overview on corporate actions. Chung and Grimes analyze literature about hard facts, like the privacy implications of data mining and companies' corresponding practices, but also on ethical implications of privacy and tradeoffs to site access. Their findings show some rather disturbing facts.

First, they describe a practice called "cool hunting", in which interviewers "get kids talking about their taste-worlds". Many sites do this by awarding some form of online credits for participating in surveys or supplying private information. This is especially noteworthy, when one regards the usual "End User License Agreements" that have to be accepted prior to using a service. According to Chung and Grimes, it is common that users have to give the site owner the irrevocable permission to use any material or data submitted. By a simple mouse click, users therefore give up a number of important rights. This is even more disturbing in an environment where the typical audience consists predominantly of minors.

Another questionable practice is "digital redlining". The term denotes the case when marketers sort populations based on their spending patterns. This can be easily done by linking postal codes acquired from a child's subscription form to surveys in which the child participated. Again this is disturbing when done among minors.

Furthermore, Chung and Grimes present privacy protection frameworks and guidelines for developers. They conclude this privacy protection attempts can only be the first step. Given the technological complexity and the adaptive strategies of marketers, such topics require continuous research and innovation. In addition, these practices are certainly not limited to traditional online offers.

3.3 Other related work

Some literature reviews we found were rather unconcerned with RFID or security and privacy topics. For the sake of accuracy, all papers mentioned in this section would have had to be omitted, but were kept to exemplify differing approaches to literature and the widespread impact of RFID on other topics.

Apart from classical literature reviews, other approaches to examine the broadness of a theoretical field have been taken. For example, Møller et al. [129] describe the development of a comprehensive bibliography for ERP research. This bibliography lists numbers of appearing papers grouped by journals or publishers. The authors claim that, though a comprehensive bibliography does not necessarily provide any better views on existing literature than classical literature reviews, the different approach it offers may enrich traditional views on literature. One of its shortcomings is its inability to explicitly consider paper quality and impact. Only the fact that Møller et al. limit their bibliography to reviewed and published papers can serve as implicit quality indicator. To the best of our knowledge, there is only one comparable service in the RFID field: Avoine's online bibliography [7].

Felstead [55] examines the literature available on integrated library management systems. In 2003 the "Library Systems Review Working Party of Oxford University Library Services" began investigating the library systems market. The original survey was published as part of the group's final report. Felstead analyzes new complementary technologies for library systems. In addition, her focus is on trends in integrated library systems and individual supplier's products. She states that there are nearly no comparisons of the reviewed library management systems available. Most information in the field comes from brief press releases about new products or features. However, according to Felstead, there are some longer best practice articles available to interested readers.

Although this paper does contain a brief mention of RFID, it can not be reasonably seen as a literature review on RFID.

Tetther and Ferreira [178] present a framework to evaluate e-business investments in the railway industry, based on a literature review and a series of interviews. Their literature review deals with three different topics. First they investigate available background information on IT adoption and e-business budgets. In addition, Tetther and Ferreira review the state-of-the-art in cost and benefit quantification, together with current methods for cost evaluation. The paper contains a single mention of RFID in the results section. Most interestingly, the privacy concerns arisen by RFID appear as one of the four most important technology inhibitors in this review. This may at least serve as strong indicator for broad public interest RFID related privacy concerns receive nowadays.

Gunasekaran and Ngai [64] review literature on the build-to-order supply chain management (BOSC), a new development in operations management. They divide the reviewed literature into four categories, based on major areas of decision-making: *organizational competitiveness*, the *development and implementation of BOSC*, the *operations of BOSC* and *information technology in BOSC* . Among the discussion of the last point, there is a subsection on RFID. In it, Gunasekaran and Ngai present literature on the opportunities offered by the combination of RFID and BOSC. The flexibility and efficiency offered by contactless technologies like RFID add perfect to BOSC's "global and dynamic nature". However, the authors conclude that the impact and opportunities of RFID on BOSC need to be examined further. In addition, they present a framework for the development of BOSC, integrating the four categories, mentioned above. Although this is strictly spoken not a literature review on RFID, it shows a key area of RFID application, the supply chain, and the value of RFID for item tracking.

Chapter 4

Literature Review

4.1 Methodology

For this survey we selected papers from both journals and conferences. Concentrating on only one of them would narrow the presented views down in an unacceptable manner. However, papers on RFID security or privacy appeared in various journals or conference proceedings. Examples include, but are certainly not limited to IEEE's International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM), the IEEE International Conference on Pervasive Computing and Communications (PERCOM), the Australasian Conference on Information Security and Privacy and many others. While conferences on pervasive computing or secure communications are rather typical places for new RFID publications, some important papers appeared on conferences, one would not suspect at first. For example, Rieback et al.'s [156] presentation of their RFID Guardian prototype appeared on the USENIX/SAGE Large Installation System Administration conference. Therefore, limiting sources to conferences or journals with particular topics would again introduce unacceptable constraints and limit our review's quality. Searching papers by checking the table of contents of selected journals and conferences, an otherwise well suited starting point for a literature review [124] is therefore not applicable in our case. Hence, we had to use a different approach to find appropriate literature.

Initially, we acquired publications from different scientific search engines and libraries, i.e. ACM Portal, IEEE Xplore, SpringerLink or Goggle's scholar search. At this point, we utilized abstract reading to assess paper qualities and ensure that they cover appropriate topics for this literature review. During this selection process publications from respected scientific sources like ACM, IEEE or SpringerLink were chosen preferably, for the quality standards they represent. During this process we found out that many publications referred to Avoine's online bibliography [7] as an accurate source of overview. Hence, we visited this website and realized that almost all our previously selected articles where referenced there. Additionally, the narrow topic of this source allowed us to discover publications with unconventional titles that we could have missed in terms-based search engines. Therefore, we added Avoine's bibliography to our list of sources.

The selected publications give us an appropriate overview on the current state-of-the-art in RFID related privacy and security. From this starting point, we will use these facts to present a number of observations on the topic made during the literature review. Alongside this, we intend to discuss central factors for RFID's further development and to summarize central perceptions.

Apart from papers on state-of-the-art security for RFID tags, we included papers on the use of RFID systems as security tokens in our review. Obviously, exploitable security leaks in an RFID system intended to provide security itself, would automatically compromise the security of the protected assets. Such applications of RFID will therefore require especially strong security.

Like in [124], we too did find and read a number of worthy articles outside of our core article sample and will cite them throughout this review. While the entirety of our articles is surely representative of the current situation in RFID research, it is by no means exhaustive or nor complete. The mere magnitude of the subject, the enormous numbers of newly published articles and the impressive rate at which those papers appear make such a claim impossible (Avoine's bibliography [7] provides good evidence of the increase in RFID research).

4.2 State of the art in RFID security and privacy preservation

In this section we will examine the current state-of-the-art in RFID security and privacy research and develop the theoretical base for our subsequent observations.

4.2.1 Common RFID security proposals

Some proposals on enhanced RFID security and better privacy protection have received widespread acceptance and several subsequent improvements to adapt them to the increasing requirements in the RFID field and keep them state.of-the-art. Typical examples for such popular proposals are Weis et al.'s hash locks and Juels et al.'s blocker tag, which are introduced in this section.

Hash locks

Proposed by Weis et al. [187], the hash lock offers a simple way to protect RFID tags from unauthorized read operations. It is based on one way hash functions and therefore appropriate on low cost tags. Each hash-enabled tag has to store a meta-ID, calculated by hashing a random key. On being queried, the tag reveals only this meta-ID. The reader then has to fetch the corresponding key from a database. The key is sent to the tag, which hashes it and and compares it to the stored meta-ID. Weis et al.'s schematic description of the hash lock is shown in figure 4.1. If the values match, the tag offers its full content and functionality. Since the key is only available on legitimate systems

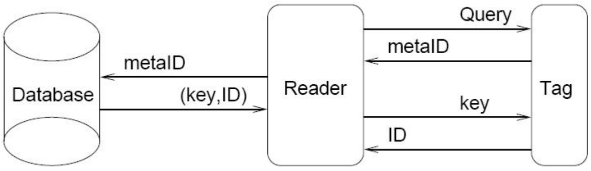

Figure 4.1: Function of hash locks (from [187])

hash locks limit tag access to authorized readers. However, hash locks do explicitly not prevent tracking.

To address tracking, Weis et al. introduce an additional mode of operation. This time the tag also computes a random number. On being queried the tag responds with the random number together with the hash value. A reader then has to brute-force identify its own tags by fetching all IDs from the database and calculating hash values for all of them with the received random number. Obviously, this method is only feasible for small numbers of tags.

Blocker Tags

In [89], Juels, Rivest and Szydlo describe their concept of a blocker tag, which allows for selective blocking of particular tags. For example, it could block every tag, whose key contains a leading "1" bit. Figure 4.2 shows how a tag is selected with a tree walking algorithm. This standard procedure is where the blocker tag interferes. As Juels et al. state, this concept of blocker tags is superior to technically simpler approaches like the *kill*-command, because the tags themselves remain in function, which allows to use the ubiquitous computing potential of RFID later on. The blocker tags could be embedded in bags and only prevent reading of purchased items on the consumers way home from the shop. Blocking would start at purchase time, by switching the leading bit on the tag and end by deactivating the blocker or removing it from the tag's perimeter.

Juels et al. also envision potential misuse of their proposal. By blocking legitimate readers, an adversary could use the technology for shoplifting, or other malicious purposes.

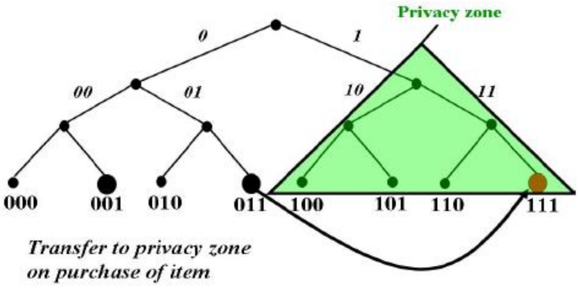

Figure 4.2: Demonstration of blocking inside the tree-walking algorithm. (from [84])

While they believe such attempts can be overcome by using several readers together to detect the blocker, which could also be used to threaten privacy if used by adversaries against legitimate blockers. However, Juels et al. do not view readers as a serious problem, because they believe that the true threat for consumer privacy originates from cheap standard readers. Therefore, the blocker tag can be a potent tool to protect privacy interests.

4.2.2 Several proposed RFID protocols

In this section, we will take a look at some of the available protocols, schemes and security measures in the RFID environment. Whilst there is a wide range of publications on this topic, we will only examine a few of these in detail, in order to keep this section short. For an exhaustive list of protocols visit the tables in the discussions section 4.4. All of these protocols are a lot less common than the proposals listed in section 4.2.1.

A security scheme for RFID equipped money

Some of the proposed uses for RFID have especially high security implications. One of the best examples for this fact is the ECB's rumored plan to introduce RFID tagged Euro banknotes. Juels and Pappu [88] describe the privacy problems arisen by tagged currency and propose their own public/private key security scheme for RFID money.

They point out that such a scheme has to offer reasonable consumer privacy protection based on the capabilities of the current generation of RFID tags. First of all, they state that re-encryption is a necessary feature for such an application of RFID. Without this feature, the encrypted serial numbers would serve as meta-identifiers, automatically compromising their bearers privacy. Another fact, which has to be taken into account, is that RFID equipped money differs from other RFID systems as it should allow tracking for law enforcing purposes.

Juels and Pappu identify four different roles in such a system. The *central bank* creates and issues the banknote and is mainly interested in preventing forgery. *Law enforcement* agencies want to track banknotes and limit other parties tracking capabilities. *Merchants* will take banknotes as payment and possibly anonymize them. Merchants are supposed to seek compliance with law enforcement and report suspicious readings, but might have an interest in compromising consumer privacy (e.g. for targeting advertisements). The last and biggest group are the *consumers*, who have interests in protecting their privacy. Some of them might follow this line up to a degree where they violate law enforcement regulations.

In addition, Juels and Pappu provide a rough enumeration of properties a banknote-tracking system has to provide. To protect *consumer privacy*, tracking must only be possible when owning the private key, even with law-enforcement field monitoring equipment. It should support *strong tracking*. Given the valid RFID information, law-enforcement agencies must be able to determine the associated serial number. The system has to be based on a *minimalist infrastructure* to ensure a broad public acceptance. Therefore, consumers should require no additional material to use the banknote and merchants and banks should only need to install few, inexpensive devices. Moreover, the system has to provide an appropriate level of *forgery resistance* i.e. the system must not give away information(e.g. serial numbers, signatures) that could be used for forgery. To prevent information tampering, the banknotes must support *privilege separation*, to distinguish write operations that require optical contact from read operations that should be possible over radio channels alone. At last, the system needs *fraud* *protection* and any invalid information should be widely noticeable, especially by the merchants that handle the banknote.

Juels and Pappu state that their scheme has shortcomings, which could be exploited by knowledgeable attackers. For example an adversary can easily prevent (lawful) tracking by putting banknotes into a faraday cage. Another problem is that tags give away the presence of banknotes on a bearer. This could be overcome by issuing cheap spoofing tags. A potential drawback of this approach lies in the fact that persons who do not possess much money have indeed very little reason to use such tags, thus rendering them fairly useless. Anyone using spoofing tags is likely to posses sufficient money to be a potential victim.

The weaknesses of the Juels/Pappu scheme and several attacks which are nevertheless possible are presented by Avoine [5]. He argues that on the one hand if not all banknotes are tagged, attackers would easily discover victims for pickpocketing. On the other hand if all denominations would be tagged, merchants might refuse to reencrypt low denominations as this operation takes time. This would result in a serious compromisation of consumer privacy. Same does apply if the re-encryption takes place too infrequently. According to Avoine, Ciphertext tracking would still be possible. Furthermore, attackers can acquire the read access key by eavesdropping the forward channel when a merchant re-encrypts the tag. Then they can exploit a weakness of the encryption method to extract further information. In addition the read access key is static and as a consequence useful for tracking.

Avoine presents two types of denial of service (DoS) attacks. The first targets the central bank, which has to restore the destroyed information on valid banknotes. By using the attack mentioned above, an adversary could invalidate tags, therefore flooding the central bank with angry customers. The second DoS-attack is even stronger. It is based on the assumption that the key, protecting the kill command, is likely to be to short on cheap tags. Therefore, an adversary will be able to easily destroy large numbers of tags. This would force the central bank to replace the affected banknotes.

We have seen that Avoine shows significant weaknesses in the Juels/Pappu scheme. However, there have been no further rumors on tagged money and therefore considerations on such a protocol have only limited practical relevance at the current time.

Ateniese et al.'s scheme - insubvertible encryption

Ateniese et al. [4] describe a new cryptographic primitive called *insubvertible encryption*, to solve the tracking problem of RFID systems. Different from other proposed solutions to that topic, this approach requires no functions that are off limits for todays tags, as the already proposed hash-functions and public key encryption schemes are according to Ateniese et al. [4]. Also Ateniese et al. claim that their ciphertexts produced by this protocol contain implicit proof of their legitimacy, allowing reencrypters to overwrite possibly malicious content by safe but meaningless information. This solution prevents tracking by having legitimate readers storing randomized marks on tags, therefore limiting traceability to only until the next interaction with a legitimate reader. These marks will be re-randomized by honest readers and might be destroyed by malicious participants, but can not be used for unintended purposes.

Even though the security scheme provides strong privacy features and tracking resistance, the drawback of this solution is that it requires tags to be rewritable, which makes them vulnerable to cloning. To counter this Ateniese et al. invent the idea of "dual core" tags where one is read only and killed on point of sale, while the other is reencryptable and used for post-sale customer care.

Juels' parallel yoking proof

Juels [82] presents a way in which two tags can establish proof that they have been scanned simultaneously. He calls that a "yoking proof". As this shall provide a way to maintain supply chain integrity, it is important that this is done in an offline verifiable way. Juels shows how tags can establish the *yoking proof*, using a reader as communications device. In addition, he proves that this communication can be shielded against adversaries controlling the reader. To establish a yoking proof, tags need to exchange message authentication codes (MAC). However, Juels is aware that such standard cryptographic applications are not executable on current low cost tags. For this reason, he presents a minimum MAC of decreased computational complexity in [82].

Minimal security on lowest cost tags

Based on the assumption that even symmetric keys are beyond the reach of current low cost RFID tags, Juels [81] presents his views on minimalist cryptography. His aim is to prove that security is improvable, even though standard cryptography might not be feasible on such tags. To break passwords, the adversary has to issue queries to guess important values. In order to lower the rate at which an adversary can successfully execute such queries, Juels proposes a scheme he calls *pseudonym throttling*. In this scheme, a tag cycles through a number of random identifiers or pseudonyms. In addition, tags are forced to answer queries at a low rate, using hardware delays. Adversaries can therefore only track the tag, if they uphold contact for some time. However, pseudonym throttling has a shortcoming. Caused by the low amount of memory available to them, low cost tags can only store a limited number of pseudonyms, which might not be sufficient to prevent tracking.

Juels assumes that a real world adversary faces a number of constraints. First he will only be able to interact with a tag a few times, before the tag can interact with a legitimate reader that will replace the pseudonyms in a secure manner (refresh). Therefore, the adversary can only issue a small number of queries before his findings become void. In addition, as tags are mobile and utilize throttling, this number is decreased further, because an adversary will not be able to follow his victim limitless. It is important to note that Juels does not claim to eliminate all vulnerabilities, only to limit them in a plausible way. In that respect, there are some noteworthy facts in regard to readers. First, they should refuse to initiate sessions with particular tags rapidly to limit the feasibility of successful relay attacks. Second, following Juels scheme, readers should never transmit any tag identifiers.Therefore, eavesdropping the powerful forward channel is useless for any adversary.

Another important aspect of this scheme is the authentication of tags and readers. If tags would directly use a pseudonym for authentication, the whole scheme would be vulnerable to cloning. Therefore, Juels proposes a "challenge response protocol [...] carefully interwoven with pseudonym rotation" [81]. That is, every pseudonym has two additional values associated with it. One is the key used for reader to tag authentication and the other one is the tag to reader key, issued only when the first authentication step was successful.

To update the pseudonyms (and the associated key), Juels utilizes a one time pad, composed across multiple reader-tag sessions. This limits the danger of eavesdropping and is nevertheless no more computationally complex than XOR-ing.

Juels believes that pseudonym lengths around 80 to 100 bits and key lengths around 20 bits should be sufficient for low cost systems. This scheme could be easily integrated into existing standards, as changing from identifiers like the EPC to pseudonyms should be straightforward. According to Juels, this scheme is only vulnerable to denial of service attacks against tags. As there are far easier ways to disable tags (by electromechanical means), this is very unlikely to be a problem.

A security layer for EPC tags

Bailey and Juels [12] present a way to add security to the EPCglobal Class 1 Generation 2 standard [77], the upcoming worldwide specification for inexpensive tags. They present functions, which they claim circumvent the intended behavior, defined in the standard, but provide formal compliance. For their examinations, Bailey and Juels divide authentication into three categories: *device authentication*, *device-binding authentication* and *data-origin authentication.* The first denotes the most straightforward security measure in the RFID field. RFID devices, namely tags and readers, should be able to authenticate each other in order to prevent data disclosure to illicit parties. However, the best authentication is futile, if the tag is removed from the object it was originally attached to. An adversary could attach stolen EPCs to counterfeit goods, to make them appear valid. Therefore, *device-binding authentication* is required to detect tag removal. Finally, as we have seen in section 2.2.2, EPC tags do carry additional data about the object they are attached to. *Data-origin authentication* ensures that this information remains unchanged since the original encoding. Tags could either receive data with a digital signature or compute one their self if they are computationally strong enough. Bailey and Juels first show a simple challenge response authentication, using 32-64 bits of the EPC field´s 512 bits to embed a key. As this might not be sufficient for all cases Bailey and Juels see need for another approach. Instead of inventing new formats, they use an existing tool, the ISO-7816 standard to their advantage. However, the EPCglobal Class 1 Generation 2 standard limits payload field sizes to extremely low levels of around sixteen bits. Obviously, this is not enough to provide reasonable security. Therefore, Bailey and Juels rely on *protocol convergence.* This term describes the use of one protocol to carry the protocol data frames of another. By transporting all required data in form of *application protocol data units* over standard compliant *Read* or *BlockWrite* commands far more complex authentication algorithms can be feasibly done. To further increase the feasibility of their approach, Bailey and Juels try to compress the ISO-7816 messages and present new commands, to save as much bits over the air as possible.

4.2.3 Adapting modern cryptography to RFID systems

In this section we will examine efforts to adapt well known cryptographic solutions to the limited computational resources of RFID tags. This includes the current standard encryption algorithm AES (Advanced Encryption Standard) and existing considerations on the feasibility of public key cryptography on RFID hardware.

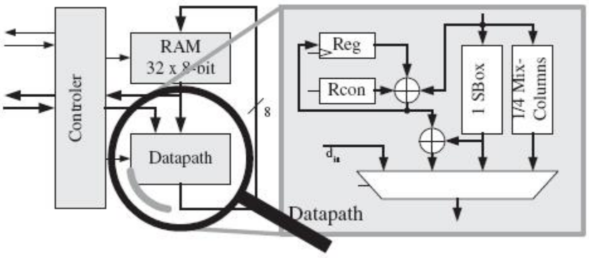

Figure 4.3: Feldhofer et al.'s AES module (from [54])

AES on low-cost tags

In [54], Feldhofer, Dominikus and Wolkerstorfer present an AES (Advanced Encryption Standard) module for RFID tags. As they state, most existing AES implementations are designed for high speed computations and gigabyte throughput, which is not applicable to the strictly constrained RF environment. By rescaling the AES algorithm from 128 bit to 8 bit operations, they decrease the computational complexity to a level that is feasible on passive RFID tags. Even though this increases the overall power consumption and computation time, the average power consumption goes down. In an environment, where power supply faces stern limitations, this is far more important than all the presented shortcomings. In addition, this rescaling also limits the hardware requirements of AES, which is another important prerequisite for encryption algorithms on RFID tags. A model of Feldhofer et al.'s AES module is shown in figure 4.3.

Elliptic Curve Cryptography on RFID

Batina et al. [14] discuss the feasibility of public key based secure identification protocols for RFID systems. In particular their focus is on using them for anti-counterfeiting measures. To realistically asses the feasibility of public key cryptography (PKC) in an RFID environment, Batina et al. apply some restrictions to their scenario and assume that tag manufacturers are trustworthy. Furthermore, their theoretical attacker knows the tag's position on a product and can therefore analyze tags in detail or launch any kind of physical attack against it. Such an adversary attempts to reproduce tag contents

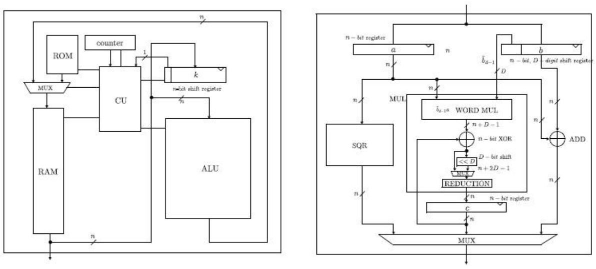

Figure 4.4: Batina et al.'s ECC hardware (from [14])

in order to deploy counterfeit goods with valid RF information. Under this assumptions Batina et al. examine the PKC implementations based on elliptic curve cryptography (ECC) for two RFID protocols by Schorr [168] and Okamoto [138]. Batina et al. find both the presented algorithms feasible for ECC implementation. Figure 4.4 shows Batina et al's elliptic curve processor (left) and its arithmetic logic unit (right).

4.2.4 RFID specific attacks and problems

In this section we will summarize publications that address either RF specific problems or attacks that can solely be launched against RFID systems. Rieback et al.'s RFID virus is a more specialized case. While a (computer) virus is by no means limited to RFID, the corresponding section shows the individual implications and constraints of applying such malware to RFID.

Tracking as multilayer problem

RFID can be divided into three layers, comparable to the OSI model [42] for networks. Avoine and Oechslin [10] demonstrate that tracking problems must be addressed on each of the three RFID layers separately. In network security, confidentially, integrity and authentication can be ensured by a protocol, independent of the characteristics of lower levels. Unlike this, RFID privacy is compromised if a single layer fails to be tracking-resistant. These layers are:

1. The *application layer* is responsible for all user defined information. In most of the cases this will be an identifier to fetch related information from a database.
2. The *communication layer* controls the collision avoidance behavior of tags.
3. The *physical layer* defines the radio characteristics, timing, data encoding and so on.

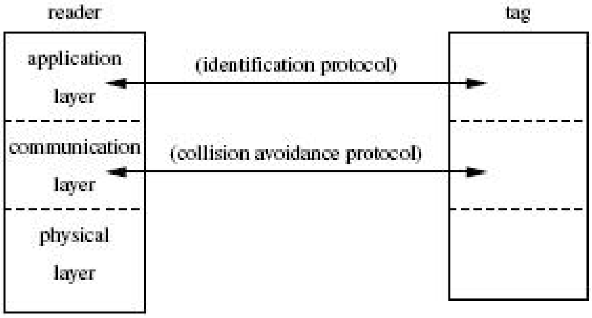

Figure 4.5: RFID layers (from [10])

As we see in figure 4.5, the first two of these layers utilize protocols. Furthermore, traceability has only been well examined on the application layer [10]. Almost all protocols in this domain depend on changing the identifier upon identification. To prevent tracking, the information transmitted by the reader (either a new identifier or material to compute one) must appear random to any adversary. Therefore, using the same rationale as with one-time pads, the information must be used only once.

On the communication layer, traceability is connected to the anti-collision behavior. A deterministic collision avoidance algorithm, together with a static identifier would automatically compromise the users privacy. All that is left to do for an adversary is to create a collision to acquire the identifier. Using dynamic identifiers is a more complex issue. If the identifier is modified during the singulation process, singulation becomes impossible. To address this, Avoine and Oechslin introduce the concept of a singulation session, which denotes all steps of process. The identifier could then be changed after each session. While this would be straightforward to implement, as many readers do already send signals at the beginning and end of the singulation process, Avoine and

Oechslin admit that this concept is still vulnerable. A malicious reader, which does not send the stop signal, could track the unchanged identifier.

Furthermore, probabilistic anti-collision schemes are vulnerable as well. During singulation, a reader notifies all tags that need to retransmit, either by sending identifiers or specifying the slots, where the collision appeared. When the session stays open, the first case allows tracking directly. The second case allows adversaries to execute the following attack, described by Avoine and Oechslin. [10]. An adversary queries a single tag, which responds at a randomly chosen slot. Again, if the session stays open and the adversary stores the slot, privacy is compromised. The adversary can later on transmit a query to a group of tags, asking those that responded at the recorded slot to retransmit. Only tags with an open session which transmitted at the corresponding slot will reply. The probability is very high that this will be exactly the tag queried before. Therefore, independent of the used algorithm, it is imperative that the session end signal is an internal feature of the tag, to ensure that no session remains open.

Another source of vulnerability emphasized by Avoine and Oechslin is lacking randomness. If identifiers, in case of a deterministic protocol, or slots, in a probabilistic one, are not chosen uniformly at random an adversary can gain useful information for launching an attack. Unfortunately, as Avoine and Oechslin state, this is the case with many existing protocols. To exemplify their point, they cite the EPCglobal Inc. draft on class0 tags [76]. This draft uses dynamic random identifiers for singulation, but for efficiency reasons, these are very short. If they cannot support singulation, every tag carries an additional static identifier embedded by the manufacturer. Therefore, the advantages of the random identifier become void.

On the physical layer, an adversary can use signal characteristics to recognize tags [10]. The easiest way to do this, is to differentiate tags according to their standard. These differ widely in their characteristics (frequency, modulation, timing). Anyone, carrying more than one tag, can be vulnerable to tracking by the individual mix of standards. The best countermeasure would be further integration of standards, up to the level of a single global RFID standard. Of course, Avoine and Oechslin admit that this is highly unlikely to happen. In addition, even if such an integration of standards would take place, every time a new standard emerges, tracking would again be possible. The second possibility for tracking on the physical layer, is called radio fingerprinting. Every radio device can be identified by minimal variations in its transmission behavior. In case of RFID, Avoine and Oechslin believe that there will be to many tags to singulate one particular tag form all others of the same production series. However, tags by different manufacturers are likely to have bigger differences, depending on the manufacturing process. Again, the individual mix of tags in a person's possession could allow tracking. Preventing radio fingerprint tracking appears to be a difficult task. Getting all manufacturers to adopt the same manufacturing process seems almost impossible, as they would surely prefer to use different approaches in order to gain business advantages over their competitors.

The relay attack

Kfir and Wool [98] describe the theory of a relay attack which, as the name indicates, allows to relay information from the victim card to a reader. This takes place without the user noticing anything and over far greater distances than nominal communication covers (Details depend on the channel and will be discussed later on). To perform a relay attack, an adversary needs two devices called *ghost* and *leech*. The ghost emulates a tag and takes care of communicating with the legitimate reader, while the leech is a reader that queries the victim tag. Data transfer between them takes place via fast digital communication, so they need not necessarily be placed close to each other.

Range limitations of normal RFID systems can easily be overcome. First, the main source of range limitation is the passive nature of RFID tags. An attacker could easily construct an active ghost that operates over far greater distances to bypass this restrictions. Using the NEDAP model[1], Kfir et al. calculated the possible distances between ghost and reader in ISO-14443 environments. Assuming only man made radio noise is

[1] available at http://www.rfid-handbook.de/downloads

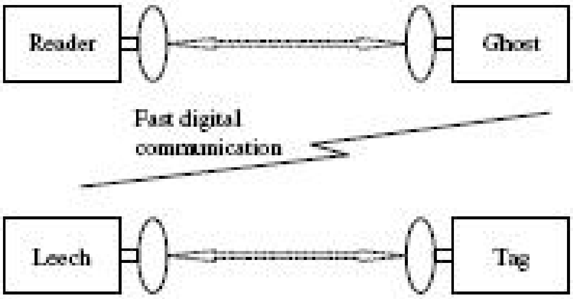

Figure 4.6: Basic relay attack (from [98])

present, the distance can be up to 50 meters. They also state that, if there are concurrent RFID systems close, the targeted reader has to be three times closer to the ghost than the interfering device. The leech to tag distance can be improved as well. To do so, the leech has to transmit more power to activate the tag over a greater distance. Another improvement can be made taking advantage of the characteristics of the ISO-14443 standard, which allows countless retransmissions of message frames. This allows the leech to order retransmissions until the tags response was properly received. Again using the NEDAP model, Kfir et al. calculated that the possible leech to tag range is around 40 - 50cm. Timing constraints are not an inhibiting factor on current systems. The ISO-14443 standard specifies the data transfer time-out to be up to five seconds. This restriction should be easily met by any system developed by attackers.

In [67], Hancke describes an actual implementation of the relay attack on an ISO-14443 system. The vocabulary is different, as the ghost is referred to as *Proxy* and the leech is referred to as *Mole*. Hancke claims that he executed the attack successfully over 50 meters, thus proving Kvir et al.s calculation. A most interesting discovery is that the timing constraints on the attacked system were in fact less strict than what is specified by the ISO-14443 standard. The only problem Hancke reports is that additional tags, other than the proxy, in the legitimate readers vicinity introduces a delay (via collision-avoidance) that violates the timing constraints.

Hancke points out that the relay attack is not strictly a failure in the cryptographic protocol and is therefore difficult to defend against. In addition, it is invisible on the application layer and for that reason countermeasures against the relay attack have to be placed on the physical layer. Kfir et al. show two possible approaches. One possibility is a faraday cage approach, which means shielding the tag against radio waves when it is not in use. The other one is that developers could implement some kind of activation mechanism. In that case, users would activate their cards only on purpose, making unknown relaying a lot more difficult.

An RFID Virus

Rieback et al. [155] presented the first RFID Virus. They proved that RFID malware and exploits are possible and that RFID tag data should not be trusted without proof. In addition, Rieback et al. state that RFID malware is highly probable to appear "in the wild" as RFID systems have five characteristics that make them outstanding targets [155]: They have *lots of source code.* The back-end databases, application servers and reader interfaces are likely to contain million lines of code. Moreover, RFID developers adopt *generic protocols and facilities*, therefore importing several known vulnerabilities. As an example, Rieback et al. present the EPCglobal networks adoption of XML (Extensible Markup Language), DNS (Domain Name System) and URIs (Uniform Resource Identifiers). Automated data collection is essential for RFID. Unluckily, *back-end databases* have their own sets of individual exploits. In addition, RFID systems are interesting to criminals, because of the *high value data* and RFID users have a *false sense of security*, due to RFID's characteristic resource limitations. According to Rieback et al. no one is really expecting the appearance of RFID malware, at least no one was expecting it until the publication of [155].

Furthermore, they show that RFID environments allow several types of well-known exploits. *Buffer overflows* are one of the most common security vulnerabilities. They are applicable to any system that is based on a not "memory-safe" programming language. As RFID implementations are based on ordinary computers, which are likely to have scripting languages installed, *code insertions* are often possible. A special form of code insertion, *SQL injection* is possible because of the automated data-collection in RFID systems, which is usually done with SQL based relational databases. Rieback et al. based their proof of concept on a virus spreading via such an SQL injection. In detail, they implemented it using a SQL injection in Oracle and opened a command shell on the PHP-based management interface.

To protect systems against such attacks, Rieback et al. advise using well known precautions. This includes *bounds checking* to ensure all indexes are inside the range of an array. All *input has to be rigorously sanitized.* This is best done by allowing only standard character input and using "built-in" data-sanitizing functions where available. Another important step is to *disable back-end scripting languages* wherever possible. Its important to *limit database permissions and segregate users* and most critical to disable multiple commands in a single query. As constructing SQL on the fly is dangerous, *parameter binding* using the PREPARE is recommended. Furthermore, when implementing a RFID system it is best to *isolate the RFID middleware server*, so that compromising the RFID infrastructure does not compromise the entire computing environment. Last, *code reviews* should be applied to any code.

Rieback et al. state that RFID malware has the potential of causing several subsequent threats and countermeasures to appear in RFID environments. They anticipate topics like RFID phishing, RFID wardriving and RFID honeypots.

4.2.5 Security models for RFID

To compare the pros and contras of different RFID security protocols, we can use formal descriptions of RFID security and privacy parameters. There are several such descriptions of RFID security and privacy available. There are however, some formalized RFID security models by Avoine [6], Juels and Weis [92] as well as Van Le et al. [108]. In this section we will provide a presentation of the most important models and their central attributes. A short comparison of these models is given in table 4.1.

Avoine's adversary model

Avoine claims that "designing and analyzing RFID protocols is still a real problem, because no universal model has been defined" [6]. Therefore, he presents a formal adversary model for RFID.

For this model, Avoine identifies three vulnerable channels in RFID environments. The first two, namely the well known *forward channel* and *backward channel*, are treated individually, as "some protocols benefit from the asymmetry" [6]. In addition, Avoine treats the memory as a third channel, because from a theoretical viewpoint, all three can be accessible for read and/or write operations, or not accessible at all.

Every adversary model consists of the means and goals of the adversary. For his model, Avoine describes means as follows:

	Avoine [6]	**Juels and Weis [92]**	**Van Le et al. [108]**
Functional Base	Adversary Approach	Adversary Approach	Universal Composability (UC) framework
Goal	Generality in capturing adversarial operations	Simple definition of strong adversary	Using UC advantages
Tested at	Published protocols	Published protocols	Own Protocols
Found	Protocols unsecure	Protocols unsecure	Protocols secure
Authors see need for improvement	Yes	Yes (side channels)	Yes (side channels)

Table 4.1: Comparison of RFID security models

Query The adversary sends a message over the forward channel and a subsequent message after receiving the answer.

Send The adversary sends a message over the backward channel and receives the answer.

Execute The adversary initiates a communication between both legitimate tag and reader, obtaining messages from the forward and backward channel.

Execute* Same as with "Execute", but the adversary only obtains messages from the forward channel.

Reveal The adversary obtains the content of a tags memory channel. As the adversary has corrupted the tag, other operations are no longer possible.

Regarding the goals of the adversary, Avoine introduces a formalization for the RF relevant term *untraceability*. More important, he divides into *existential* and *universal* untraceability. The first denotes the fact that an adversary cannot succeed with any tracking attack, the second one describes a scenario where an adversary can only succeed under particular circumstances. After presenting his definitions, Avoine applies them to several proposed RFID protocols and concludes that most of them did not respect the minimum expected security criteria. The few that did suffered from high computation complexity. Finally, Avoine emphasizes that his work is just a first step in formalizing RFID security and untraceability.

The Juels and Weis model

Juels and Weis present their own security model [92]. Compared to the Avoine model, they claim that their model is less flexible, but more specific and simple. However, as they state, their model is more general in one respect. It allows adversarial interactions with more than two tags, thus covering the security aspects of RFID systems based on correlated secrets. Moreover, the Juels/Weis model is explicitly aimed at next generation EPC tags and similar tags, which are capable of performing symmetric cryptography. In their views, systems are composed by a single reader and an arbitrary number of

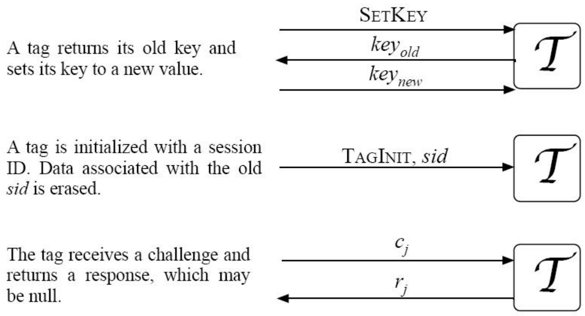
A tag returns its old key and sets its key to a new value.
SETKEY
key_{old}
key_{new}
$\mathcal{T}$
A tag is initialized with a session ID. Data associated with the old *sid* is erased.
TAGINIT, *sid*
$\mathcal{T}$
The tag receives a challenge and returns a response, which may be null.
c_j
r_j
$\mathcal{T}$

Figure 4.7: Juels' formalized tag interface (from [92])

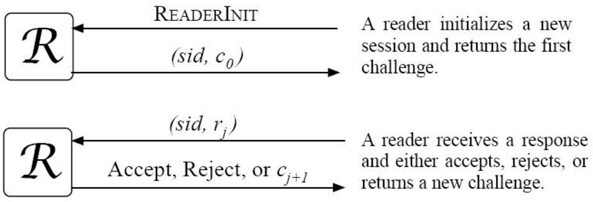
$\mathcal{R}$
READERINIT
(sid, c_0)
A reader initializes a new session and returns the first challenge.
$\mathcal{R}$
(sid, r_j)
Accept, Reject, or c_{j+1}
A reader receives a response and either accepts, rejects, or returns a new challenge.

Figure 4.8: Juels' formalized reader interface (from [92])

tags. All of them are viewed as "functionalities" with well defined interfaces [92]. These interfaces are shown in figures 4.7 and 4.8. They may receive messages and respond with their own. Especially, they do not necessarily provide deterministic output.

The model defines tags to store two values, a key and a session identifier (*sid*). Both of them have related messages, new keys are set via SETKEY message and new *sid*s are received together with a TAGINIT message. In response to a SETKEY message a tag sends its current key. Other exchanged messages are challenges (c) and responses (r). Upon receipt of a READERINIT message, the reader creates a *sid* and the first challenge c_0 of the challenge-response protocol. These are sent as TAGINIT messages to the reader. In addition, *sid*s are stored in the back-end database together with some state information ("open" or "closed") to identify incoming queries.

An adversary in the Juels/Weis model can issue all kinds of messages (SETKEY, TAGINIT, READERINIT, c, r). If she is able to successfully issue a SETKEY command, she can both obtain the tag's key plus embed an arbitrary new one. Therefore, Juels and Weis view any tag, receiving an adversarial SETKEY message, as corrupted. In addition to this definition, their work features a privacy experiment, based on the above parameters, and a formal definition of privacy, derived from it.

In this definition, privacy is not depending on single asset, but on the entire system [92]. If generated keys are not random, or the reader does not treat all tags equally, privacy, according to the definition, is unachievable. In addition, the Juels/Weis definition is strictly protocol-level based. Physical tag identification, for example by their radio characteristics, is not covered by it. The initial definition requires all readers to "own" their tags, i.e. assumes a closed system, which is extremely unlikely for a real world scenario. In such a realistic scenario, users can be expected to carry tags of different types. As readers will reject all incompatible tags, any adversary, capable of performing a man in the middle attack, compromises formal privacy by identifying tag types. The information gathered this way can be used for tracking individual sets of tags. Juels and Weis address this by defining a variant of their definition aimed on what they call *cross-reader privacy*. Again, this definition is limited the protocol level. In case, the tag types are physically distinguishable, for example by their frequency, the best achievable formal privacy is indistinguishability between tags of the same type.

Juels and Weis use their definitions to test several protocols. For example, they show that the Weis et al. hash-lock system (see section 4.2.1 or [187]) is only private for the closed system assumption. Therefore, they present an improvement to the initial hash-lock scheme, using nonces (one time numbers), but do not provide a formal analysis for this.

Juels and Weis conclude that their definition is just a starting point and further research is needed in two directions. On the one hand, there is need for even *stronger definitions*. For example, side channel information, like the radio behavior of tags, is not covered by their current approach. On the other hand, Juels and Weis admit that some of their definitions are to strong and only practically feasible using public-key encryption. Symmetric key encryption would require a brute-force search for tag keys, which would scale poorly on large systems. Therefore, Juels and Weis declare *weaker definitions*, which are more practicable, a fertile area for research.

The UC model

Another security model is presented by Burmester, Van Le and Medeiros [22] and refined by Van Le, Burmester and Medeiros [108]. Unlike the others, this model is based on the universal composability (UC) framework [26] instead of the classical adversary approach. This approach defines security in terms of indistinguishability between real and ideal protocol simulation. Therefore, the UC model requires three elements: models of both the real and ideal protocol execution and a proof of indistinguishability between them. To formalize their model, Van Le et al. assume that all malicious participants are under control of a central adversary.

The central agenda of this model is to provide *forward security* for RFID communications. This means that sessions cannot be corrupted by the adversary at a later point. However the Van Le ideal world model does only provide this value for completed sessions. An adversary, corrupting a tag (reader and back-end are considered incorruptible), can link all incomplete sessions up to the last completed one. Further on, Van Le et al. use their model to prove the correctness of two new protocols they present. They admit, however, that they do not address side-channel attacks which are likely to corrupt protected tags. As such attacks are not restricted to the protocol level this is beyond their intended scopes. Nevertheless, their model includes a brief formalization of ideal wireless communication which can serve as a starting point for further examination of lower communication layers, beyond the protocol level.

4.2.6 Integration of different approaches - RFID Guardian

In the previous sections we have seen that there are various ways to address the security and privacy concerns of RFID. However, most of them are either not feasible on low cost tags or address only a small subset of RFID security issues. To integrate the various approaches, Melanie R. Rieback, Bruno Crispo and Andrew S. Tanenbaum proposed a device called RFID Guardian [157] in 2005. They observed that most security proposals require high-end RFID tags, leaving the majority of applications, which are based on cheap tags, unprotected. In addition, they state that many solutions are not compatible to each other, but have complimentary features (e.g. blocker tags and hash locks, described in section 4.2.1). Therefore, they introduce the RFID Guardian as first centralized platform for managing individual user's security and privacy. They propose an actively powered, portable device. Because of the prerequisite of portability, Rieback et al. planned their RFID Guardian, to be no more than the size of a PDA. Alternatively, the device could be directly integrated into a handheld computer or a cellphone. The main benefit of the RFID Guardian is that it integrates auditing, key management, access control and authentication into a single device. To accomplish this, it has to be able to read tags, but also emulate them to communicate with readers.

The RFID Guardian supports two forms of auditing. It logs RFID scans and therefore allows discovering illicit behavior. This enables users to resolve this activities later on and report them to the authorities. In addition, the guardian can perform regular scans to discover RFID tags in its owners possession, which prevents the user from carrying unknown and unwanted tags. It is noteworthy that these scans involve a trade-of between scanning often, which offers strong protection but will drain huge amounts of battery power and might result in false positives and scanning infrequently, which is less resource consuming, but leaves the user unprotected for some time.

Another function Rieback et al. included into the RFID guardian is key management, which is required for several RFID security mechanisms. Being a two way RFID device, able to communicate with both tag and reader, the RFID Guardian is perfectly suited to serve as key management system without having to rely on additional infrastructure. Its features include activation and deactivation of security measures and key updates on-demand. This is especially valuable on low cost tags, which cannot create random material for keys by themselves.

On behalf of access control, Rieback et al. introduce three new features to the RFID security context. First, *coordination of security primitives* means that the RFID Guardian coordinates the use of different access control mechanisms in appropriate situations. While this need not be done by a device, most RFID users will surely lack the patience or knowledge to do this manually. Second, *context-awareness* relates to the fact that the amount of risk differs from place to place. For example, some tags that contain private information are meant to be readable at home, to offer additional benefits. If such a tag is readable in public places it might represent a serious privacy threat. As context is a somewhat imprecise fact and might be hard to determine, Rieback et al. propose two ways how the Guardian acquires context information. It could either be linked to some sort of GPS to calculate its position, or it could receive context updates by certain readers for example on leaving the user's house. The main problem is that the RFID Guardian has to be in a readers vicinity to be notified of context changes. Finally, *tag-reader mediation* means that the RFID Guardian works as man-in-the-middle for any negotiation between tags and readers. It takes care of encryption, forwards queries and manages which readers get answers to their queries. This is done by jamming the tags if the readers are not permitted to access.

Furthermore, the RFID Guardian can serve as of tag authorization device when communicating with "guardian aware" readers, therefore automatically enforcing the previously mentioned access control mechanisms accordingly. The remaining problem is that RFID queries are not easily linkable to the readers that issued them. Rieback et al. address this problem by recommending further standardization to solve this problem. Until then, they propose to make readers announce their queries prior to execution.

In 2006, Rieback et al. finally presented a prototype for their device in [156]. They designed their device to be integrated in a handheld computer. For implementing the reader function they used a fully ISO-15693 compliant RFID reader. The standards based tag emulation hardware allows to actively spoof tag responses up to half a meter and additionally serves as hardware basis for distributing the RFID Guardian's jamming signal. This jamming signal of the current prototype is optimized for ISO-15693 tags with slotted aloha anti collision scheme (see section 2.1.4). The RFID Guardian decodes incoming queries an blocks exactly the timeslot, in which the tag responds. A disadvantage of this system is that, as the RFID Guardian emulates a tag, it is unable to initiate communication with a reader. Instead, it always has to wait for reader requests.

The software for the RFID Guardian consists of a central real-time operating system and several libraries implementing the required functionality. These include device drivers for the hardware components, an implementation of the ISO-15693 communication protocol to enable it to understand RFID communication and a journaling file system for storing persistent data into the integrated flash memory. The main functions are realized by four tasks, which share the system resources. All of them wait for invocation in infinite loops and activate appropriate routines from the software stack. The timer task performs regular activities, the UI task handles user input, the tag task takes care of tag emulation and the reader task issues RFID queries. In addition, Rieback et al. plan that the RFID Guardian will communicate with "guardian aware" readers using a so-called "guardian language", but this topic remains theoretic, as no such readers exist at the time being.

An interesting aspect of [156] are the initial considerations on the security of the RFID Guardian itself. Exploits like buffer overflows should be preventable by cautious programming of the guardian's software. In addition, Rieback et al. see no real threat in DOS attacks against the RFID Guardian. Most attacks that could confuse the guardian would also confuse the tag. This would prevent it from answering, therefore eliminating the reason why anyone should want to take down the RFID Guardian in the first place. Exactly the same arguments apply to completely jamming the communications channel. A variation of a classical DOS attack would be to take down the guardian's auditing functions by filling up the RFID Guardian's limited storage space. While this would be a possible way to destroy evidence, it will take enough time for the guardian to notify its owner of this threat. Nevertheless there are some attacks that will be successful against the guardian. For example, by tracking the collision space, readers can discover the IDs of guardian-protected tags. Rieback et al. see the biggest problem of the RFID Guardian in its inability to block reader queries. While it may block tags from answering the query, the guardian cannot prevent readers from executing malicious queries to kill tags or overwrite content. Another drawback of the guardian until this point is that it is unable to handle tags working with different standards or frequencies.

Despite this restrictions the RFID Guardian is a powerful privacy protection tool that integrates several different functionalities and RFID security proposals. In their conclusion, Rieback et al. compare their RFID Guardian to a life raft in an upcoming sea of RFID systems that will help users to regain a bit of privacy lost to the ubiquitous RFID environment.

4.2.7 Actual and potential uses of RFID

RFID is a potent technology for various areas of application, some of which can already be seen in practice while others remain somewhat theoretic at this point. For example, RFID is currently used in several libraries throughout the US [132] and for linking goods to identifiers in the supply chain. The latter one offers an interesting possibility when combined with the upcoming worldwide EPCnetwork [174].

RFID in anti-counterfeiting

RFID tags can be used to replace or support existing anti-counterfeiting technologies. This was examined by Staake et al. [174], who show the use of the EPC (Electronic Product Code) Network to keep track of legitimate products. Anti-counterfeiting measures consist of four parts: legislation, law enforcement, policies and technical measures. Technical measures are again divided into three categories. *Optical anti-counterfeiting technologies* include solutions like the famous holograms or microprinting. However, they are not forgery resistant and because of their widespread use, customers tend to pay little to no attention to them. *Biotechnology* shows a growing potential for anti-counterfeiting by using the unique characteristics of DNA. By adding minimal doses to certain products, producers can confirm their legitimacy through biochemical tests.

Another growing section is *microelectronics*, which is best suited for automated checks. Obviously, RFID tags belong to the last branch. Staake et al. exemplify how the EPC-network presented in section 2.2.2 can be used to prevent counterfeiting of tagged goods. Anti-counterfeiting uses the possibility of worldwide tracking, which is normally viewed as privacy threat in RFID, to check goods in a fully automated way. According to Staake et al. [174], RFID has the potential to circumvent all shortcomings of current measures and become a flexible and secure tool for anti-counterfeiting.

RFID in libraries

Apart from theoretical considerations, valuable lesson can be learned from RFID applications in practical use. Molnar and Wagner [132] do this by analyzing RFID based library systems, which are already in use in the USA. They describe actual implementations of library services and show what concerns remain in current systems. A typical practical problem they describe is that RFID systems and the employed tags will rarely be altered or replaced once attached to a book, as the environment for RFID is still cost intensive, even though the tags are not. Therefore, many flaws remain in working systems and malicious contents will stay present on tags undetected, as long as they do not trigger any alerts on check-out or check-in of the book. According to Molnar and Wagner, this would only happen if the malicious changes affect the ID of the tag or information like a so-called "security bit". This term is somewhat odd in the given context, as the bit is not concerned with RFID security, it only keeps the status of the book (e.g. checked-in or -out) in some implementations. In other implementations, readers acquire this information by querying a database with the tag's identity instead of asking the tag directly.

Molnar and Wagner prove that an adversary can pose a threat without having access to such a bibliographical database, a fact that has beforehand been denied by some library RFID proponents [132]. None of the systems they analyzed used any type of read access controls and the IDs are currently persistent throughout the tag's lifetime.

This has mainly practical reasons, because it prevents tags from a particular library from triggering readers elsewhere. As Molnar and Wagner indicate, this privacy leak could even raise racial issues. People, who possess books from libraries in minority areas, could become preferred targets of RFID using authorities. The static ID itself is a problem as well, because it allows tracking of books and if combined with other surveillance technologies allows to link books to certain groups of people. For example if a book (without knowing its title, topic or author) was beforehand found in the hands of suspected criminals, it could arise suspicion around everyone who reads it. Oversuspicious authorities could construct lists of suspicious books and search for people who check out this books. Molnar and Wagner describe this "hotlisting" as a major problem of RFID enabled libraries.

Moreover, they show that even if tags would be upgraded to support access control, many of them would still be identifiable, because of their collision avoidance behavior. This behavior is often based on globally unique, static collision IDs, which can be used exactly like normal identifiers (see section 2.1.4). Because this is hardcoded on a low layer it is impossible to subsequently provide an appropriate level of privacy on such systems.

Another problem Molnar and Wagner emphasize is that actual and coming RFID standards like the EPC standard [77] and the ISO-18000-3 standard implement a *lock* command, but no *unlock*. This *lock* command prevents further memory changes. As the security bit, mentioned earlier, needs to be changed quite often, it is impossible to lock library RFID tags on deployment. Therefore, any attacker could *lock* the bit afterward to make the book, it is attached to, unavailable. Molnar and Wagner claim that this "security bit Denial of Service" was possible in any ISO-15693 environment they examined. In addition, as empty tag space on RFID tags is usually writable, an attacker can easily store his own identifier and bypass security measures like ID changes. Molnar and Wagner recommend that at least this part of memory should be locked.

Furthermore, they state that until now write passwords are the only security measure used in actual implementations. Passwords are currently transmitted unencrypted and therefore simple eavesdropping allows attackers to discover all they need to execute any kind of query. Moreover, if the system is based on using the same password for all tags, discovering one password compromises the entire system. Else, if the system utilizes different passwords for tags, they require some sort of identifier sent from the tags, which would again allow hotlisting.

In the second part of [132], Molnar and Wagner describe necessary prerequisites for improved privacy in RFID based libraries. One of their proposals is some kind of private anti-collision for tags, to prevent their identification by the used collision avoidance behavior, mentioned above. They suggest to replace all data on a tag by a random number at check-out and recover it from a database on check-in. Books leaving the library will then only contain a random number, which allows no hotlisting.

Molnar's and Wagner's second improvement is some minimum encryption for transmitted passwords. They propose a simple protocol, where the tag transmits a random number to the reader, which is then used to encrypt the password. The security advantage is gained by the fact that tag to reader transmissions are harder to eavesdrop than the opposite direction. If an eavesdropper misses the random number, he cannot exploit the password transmission. Currently though, the generation of the required random numbers is beyond the capabilities of available tags. Furthermore, Molnar and Wagner present their plan to solve the dilemma between readers, which can only authenticate a tag using the tag's symmetric key if they know the tag's identity, and the tag, which can only reveal its identity after authenticating the reader. The exact description is beyond the scope of this work and can be read in [132].

According to their findings current library RFID systems do not and cannot protect consumer privacy. Therefore, Molnar ans Wagner conclude that adopting all required security properties will take a lot of time, money and effort. Apart from its use in anti-counterfeiting or library check-outs, RFID is also included in contactless identification tokens like the e-passports that we will examine in the following section.

4.2.8 RFID passport security analysis

In 2006, the USA and the European Union issued the first generation of new RFID equipped Passports. Subsequently, several authors analyzed the security and privacy aspects of this so-called *e-passport*. The *International Civil Aviation Organization* (ICAO), responsible for passport standards, calls these passports *Machine Readable Travel Documents* (MRTD). The privacy aspects of these new passports have gotten a lot of attention, not only on the web. Several security related websites and blogs have already dealt with this topic[2] and there are also some scientific contributions. During our literature review we acquired three publications on e-passports by Juels et al. [87], Hoepman et al. [74] and Carluccio et al. [29]. Avoine's online bibliography [7] mentions a fourth paper on e-passports, but we were not able to retrieve anything more than a citation of this document [102]. After several unsuccessful tries, we finally found the article on Springer's website[3], but had to note that the Vienna University of Technology's access rights did not permit us to access this document. Therefore, we could not include it in our literature review.

Juels, Molnar and Wagner

Juels et al. [87] explore the security and privacy implications of the "worldwide experiment" represented by the e-passport. They examine clandestine scanning and tracking, skimming and cloning, eavesdropping and biometric data-leakage as well as cryptographic weaknesses in the current ICAO guidelines. Wherever appropriate, they also examine the case of the Malaysian e-passport, whose deployment in 1998 predates the ICAO specification. Juels et al. stress the importance of data leakage threats as MRTDs contain especially sensitive information. Acquiring such information will allow criminals to create fake identities and create fraudulent documents. Moreover, tracking and hotlisting are potentially even more dangerous. While any static identifier allows to track

[2] see, for example http://www.schneier.com/blog/archives/2006/08/hackers_clone_r.html

[3] http://www.springerlink.com/content/b50183536414k401/?p=2fc16a31d217468abc717507c1113133pi=41

a person's movement, hotlisting allows to target specific individuals and therefore yields unpleasant prospects as the infamous "American-sniffing bomb" explicitly mentioned by Juels et al.

Additionally, MRTDs contain high quality biometric data. Currently this is only a digital image, which alone could allows identity theft. Juels et al. mention that some supporters of biometrics argue that such images are public knowledge and do therefore not require secrecy. However, this argument ignores a fundamental aspect of passport pictures: image quality. They are usually taken under highly regulated circumstances and are consequently significantly better than anything made under casual circumstances. An attacker will likely be unable to create pictures of similar quality without the intended victim's notice. Therefore, digital image information is not public record [87] and should be kept secret. This is even more the case with iris scans and fingerprints, which could also be stored in ICAO conform e-passports. Biometrics related security is even more critical, as Juels et al. identify two typical factors in the e-passport context threatening it. First, the intended automation of passport checks leads to a relaxation of human oversight, which eases spoofing of certain attributes. Second, there is a potential and highly probable spillover effect as biometrics can also be used as authentication tokens in other context. Juels et al. exemplify this by showing [87] how spillovers could be used to defeat a recent scheme for fingerprint randomization.

Subsequently to their threat survey, Juels et al. examine the ICAO specification's mandatory and optional cryptographic features. Most noteworthy, the mandatory feature in this specification is passive authentication, ensuring only that the given data is authentic and not the data container (namely the e-passport). To ensure the tokens authenticity, basic or active authentication should be employed.

Moreover, Juels et al. propose several security measures to strengthen actual e-passport deployments. First, their most basic precaution is to construct the passport cover out of some sort of blocking material to create a faraday cage. This would prevent any clandestine scans, and allows the passport bearer to regain control over whom he shows his data. Moreover, they advise to use larger (128-bit) secrets for key derivation and a switch from the standard UID based ISO-14443 anti-collision algorithm to private collision avoidance. Furthermore, Juels et al. state that optically readable keys fit neatly in the passport context, but will not be usable for other contactless ID cards. Regarding future issues they envision problems resulting from writable e-passports, which might be desired to store visas electronically [87], and a potential function creep, when e-passports are used for additional purposes like e-commerce.

Juels et al. conclude that e-passports are only the first of a whole new generation of identification devices and may provide valuable information on building more secure systems.

Hoepman, Hubbers, Jacobs, Oostdijk and Wichers Schreur

Hoepman et al. [74] analyze the first generation of e-passports conforming with the ICAO specification. They examine the main security factors based on the Dutch e-passport and especially put their focus on the specific European perspective, emphasizing the development of *extended access control*. To precisely assess the needs of e-passports, they formulate three basic security goals: First, terminals (readers) should always authenticate themselves first to prevent information disclosure. Second, the passport holder's consent should be required before any identity information is released. Finally, anyone who receives such data should be able to verify this information's integrity and authenticity.

Regarding the fulfillment of this goals in the current e-passport generation, Hoepman et al. state that the first goal, namely reader first authentication, is not satisfied. Basic access control only requires readers to know the passport's machine readable zone (MRZ) information i.e. to have optical access to the passport and enforces no reliable authentication. The second goal is theoretically satisfied as passport holders must open their passports before the reader acquires the MRZ information. The action of opening the passport implies at least some sort of consent. However, in practice there are some side channels that leak out data without prior authentication. Finally, Hoepman et al. regard the third goal of verifiable integrity and authenticity as satisfied by the secure messaging service used after the basic authentication.

An additional focus of their publication is on special identity management issues of e-passports. For situations which require only simple proofs, like in Hoepman et al.'s example where a person has to proof only that she is over 18, the e-passport is certainly an "overkill" [74]. Therefore, the authors give basic rules for more flexible identification tokens. Mainly, they advise an environment authentication first strategy to protect user privacy, which they see as most important for security. Furthermore, they propose that authentication should be split into small portions. Regarding the prior example, this means that there should be a reliable way to transmit small information pieces like "The owner of this token is over 18".

Finally, they advise a fundamental redesign for the second generation of e-passports. Their most outstanding advice is to redesign e-passports as a smart card with contacts, to avoid a whole set of clandestine operations possible in RFID environments. Moreover, they advise a network that connects all passport terminals to a back office, which handles identification of terminals using public key cryptography and determines their access rights on the fly. Subsequently this back office would give the terminal access to the passport by fetching the required information from a server in the passport's issuing country.

Carluccio, Lemke-Rust, Paar and Sadeghi

Carluccio et al. [29] focus on the basic access control features of the ICAO specification and in particular its German implementation. Moreover, they contribute a distributed hardware platform for eavesdropping and cracking e-passport data to the current scientific discussion. Basically they summarize the functionality of basic access control and describe two attacks on privacy. This attacks would allow eavesdroppers to build up an adversarial tracking database. Their first attack is based on a direct key search. MRTDs have no failure counter, which allows adversaries to run limitless brute-force attacks at check-in desks or airport restaurants. As Carluccio et al. point out, the odds of such an attack can be increased greatly by guessing some information about victims like date of birth or city of residence.

Additionally, Carluccio et al. describe their device architecture. For an ISO-14443 environment they explain that nominal operating distances can be exceeded greatly and communications over 2 meters distance are possible. Moreover, they envision that with some setup optimizations distances around 10 meters should be possible [29]. As the threat scenario they foresee is a online tracking database, Carluccio et al. see a potential for MRTD cracking in distributed environments, using idle computing capacities of machines connected via the internet to break passport encryption. Alternatively, they advise using optimized special purpose hardware. For their examinations they used a system called COPACABANA, with optimized code breaking hardware.

Finally they conclude that e-passports offer strong mechanisms for authenticity, while confidentiality and access control mechanics are still weak.

4.3 Observations

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" [188]. This quote from Mark Weiser, who was the first to use the term "ubiquitous computing", illustrates the potential of RFID tags. But, as long as consumers have serious privacy concerns against RFID [179], we do not expect the technology to become truly "invisible" in the sense of the quotation above. Therefore, we present the observations we made during our literature review of RFID security and privacy, as we are convinced that strong security can solve many of these pressing concerns. An overview on our observations is given in table 4.2. Part of this work is going to appear in [160].

4.3.1 Observation 1: RFID security is a complex topic comprised of several severe, interconnected problems

Much of RFID's characteristic complexity comes from its composed nature, implying several interconnected problems. We found an adequate example for this fact in Avoine's and Oechslin's [10] findings on tracking as a multilayer problem. Tracking or tracing is an RFID significant security threat. It means that adversaries can identify tags they read before (e.g. by a static identifier). This represents a serious violation of confidentiality as well as privacy.

According to Thornton et al., misleading and speculative media reports have made tracking the threat that customers are most aware and afraid of [179]. Furthermore, tracking is a well known RFID specific problem, and has therefore received a lot of attention by the scientific community. This led to the publication of numerous privacy protection proposals [4, 89, 156] to mitigate it. Among them, there is the previously

Observation 1	RFID security is a complex topic comprised of several severe, interconnected problems.
Observation 2	There is no commonly accepted holistic security model.
Observation 3	Papers on new protocols and publications on weaknesses in them appear increasingly fast.
Observation 4	Perceptions on RFID differ widely depending on the participating stakeholders.
Observation 5	Available trusted and proven cryptographic solutions are not applicable to the current generation of low cost tags.
Observation 6	There are a few main development streams in the RFID security and privacy complex that drive the technology forward.
Observation 7	RFID equipped e-passports are considered insecure.

Table 4.2: Observations on RFID security

mentioned work by Avoine and Oechslin on tracking's multilayered nature [10] (see section 4.2.4). Unlike the OSI layers [42] in networking, the three RFID layers have to be secured independently. If privacy protection fails on only one of these layers the whole system is automatically compromised.

However, RFID's complexity is not caused by its multilayered nature alone. We see another source for the topic's complexity in the broad range of possible attacks. RFID has its own specific set of vulnerabilities [98], as it can be seen in the tracking complex. However, for some time people shared the convenient view that the obvious resource limitations faced by (cheap) RFID tags would implicitly secure them against more complex malware like viruses and worms. This was pointed out by Rieback et al. and immediately disproved in the same publication [158] (see section 4.2.4). In their impressive paper, they showed on an exemplary virus that complex exploit based malware is possible despite the previously mentioned limitations. Therefore, we see that RFID implementers should not limit their views on core RFID topics, but be aware of all vulnerabilities discovered in information and communication technologies.

4.3.2 Observation 2: There is no commonly accepted holistic security model

In [6], Avoine points out the importance of a universal RFID security model for designing secure RFID protocols. Even though, he and several subsequent authors put forward their models [6, 92, 108] (see the corresponding section for a comparison), none of these seems to have the potential to arise as a standard model. This can be exemplified using several common points. First, all of these presented models are limited to the protocol level. Therefore, lower level characteristics like radio behavior are not covered by them. As an initial effort in this direction, Van Le et al. [108] present a formalization of ideal wireless communication, which may serve as a possible starting point. Second, the intended range of such a protocol is not beyond doubt. As Juels and Weis [92] showed in their conclusion, there are arguments in favor of both stronger and weaker formal models.

Nevertheless, we should not yet talk of exhaustive research in this area, the existing models do already prove their value, as they can be used to uncover weaknesses in existing protocols. Avoine, Juels and Weis, use their models to examine existing protocols and show that most of them do not provide formal security under them. Juels and Weis highlight that many systems do only provide security under their practically unrealistic closed system assumption [92]. The Van Le et al. model represents a little exception, as the authors analyze their own, newly presented protocols. It is not surprisingly that they find them secure.

As Gilbert et al. highlighted, a too restrictive model can make protocols look secure that are nevertheless vulnerable to realistic attacks [62]. Therefore, the lack of a standard security model for RFID shifts attention and resources from protocol comparisons to model assessments. As none of the presented RFID security models covers all aspects of RFID, we think that they will not arise as a standard to test new protocols, but they can provide valuable input for the future development of such a model. Until an agreed standard model arises, we believe that claims on mathematically provable security should be treated with care, as models and the protocols, tested against them, are often defined by the same persons. Therefore, testing and comparing new protocols and applications remains a complex task. Further efforts in this research direction could benefit the improvement of RFID security as such, by sparing researchers a lot of side efforts.

4.3.3 Observation 3: Papers on new protocols and publications on weaknesses in them appear increasingly fast

As RFID itself is a rather young research field, it is undergoing fast development and change. In 2005, Avoine and Oechslin [10] cited six publications on new protocols and only two that uncovered weaknesses in such protocols [5,163]. Therefore, they concluded that only little work has been done on computationally simple protocols. Now, we can see that this situation is changing rapidly, as numerous publications address the issue of new protocols and their weaknesses.

Examples for this fact include, but are certainly not limited to, Li and Deng's [116] attack against "EMAP: An Efficient Mutual Authentication Protocol" [143], Li and Wang's [117] attacks against the recently proposed LMAP [140] and M^{2}AP [141] and Gilbert et al.'s [62] active attack against the so-called "HB$^+$" [91]. Moreover, Defend, Fu and Juels [43] present lightweight attacks on two protocols by Vajda and Buttyán [182], which uncover the session keys.

Three of these four examples appeared within less than a year's time. In addition, from fourteen sources added to Avoine's bibliography [7] in 2007, eight dealt with new protocols and four exposed weaknesses in existing protocols. We can see from this evidence that the lack of attention on protocol weaknesses Avoine and Oechslin experienced [10] does no longer exist. Therefore, we believe that RFID development has entered a new era where new protocols appear at a fast rate and are disproved (or sometimes improved) quite as fast.

4.3.4 Observation 4: Perceptions on RFID differ widely depending on the participating stakeholders.

Among the topics of the emerging RFID trust complex, we find the debate on further governmental or voluntary vendor regulations especially interesting. A summary of the different points of involved parties, namely customers, vendors, researchers and governments, can be found in the results of a public consultation on RFID privacy by the European Union's Article 29 Data Protection Working Party. A year earlier this advisory body published its views on RFID technology and privacy aspects [50] and asked for comments. In their report on the results of this consultation [49], the members of the working party state that they got results from eight private individuals, nine universities and think tanks, sixteen corporations or trade organizations, and one consumer association. Corporation in this context refers to both RFID vendors and retailers. One point of the results we find noteworthy is that most corporations see self-regulation as the adequate tool to complement the current European data protection directive in RFID related privacy issues, whereas most of the other parties suggest a need for additional guidance like RFID specific rules in the directive. The only exception from this pattern are companies providing security solutions themselves, as they do not view self-regulation as an appropriate measure. Nevertheless, the situation is not always that clear and the opinions are not always as different as it appears in that case. This can be seen in our next example.

Comparing the proposed "RFID Bill of Rights"[4] by Garfinkel to its business counterpart, the EPCglobal guidelines[5] for RFID, we can easily see the fundamental differences between them. These are exemplified in in table 4.3. When examining this fact, it is important to note that Garfinkel opposes regulation. He proposed a voluntary vendor self regulation to prevent strict mandatory regulation by governmental institutions, which would delay the further economic adoption of RFID. If the self regulation rules and sanctions are not strict enough to prevent misuse of the technology, this could lead to a public outcry with exactly the foreseen negative result. In Garfinkel's view the EPCglobal version of his proposals is too weak to have the intended result. In fact, Garfinkel called these guidelines "significantly watered down"[6] and showed that we can tell from the wording how thin these rights really are. For example, instead of guaranteeing users the right to have tags deactivated, EPCglobal Inc. simply advises that customers should be informed about the choices they have for future removal or deactivation of the tag.

Even though, the situation cannot be explained by labeling private individuals regulation proponents and corporations opponents, there are fundamental differences in the views of RFID and the corresponding privacy needs by this two groups. To conclude, there is a tradeoff between governmental regulation which might ensure privacy but will delay

[4] see http://www.technologyreview.com/Infotech/12953/

[5] see http://www.epcglobalinc.org/public/ppsc_guide/

[6] see http://www.technologyreview.com/Infotech/13902/

RFID's widespread adoption and limit its technological diversity and voluntary self regulation which will ensure fast economic success through flexibility but might sacrifice customer privacy to achieve this goal.

4.3.5 Observation 5: Available trusted and proven cryptographic solutions are not applicable to the current generation of low cost tags

RFID's resource limitations in processing capacity and memory prevent tags from using conventional cryptographic like other platforms do. Especially, these cryptographic solutions are not applicable on the current generation of low cost tags. This view was quite common in our reviewed literature. For example, Juels [81] sees PIN controlled data ac-

RFID Bill of Rights[4] Consumers should have...	**EPCglobal Guidelines**[5]
...the right to know whether products contain RFID tags.	Tagged products should be marked with an EPC sticker.
...the right to have RFID tags removed or deactivated when they purchase products.	Consumers will be informed of the choices available to discard or remove the tag.
...the right to use RFID-enabled services without RFID tags.	Consumers shall be informed of the advantages RFID offers.
...the right to know when, where and why the tags are being read.	Companies should publish policies addressing the use of collected data.
...the right to access an RFID tag's stored data.	(Not covered by the EPCglobal guidelines)

Table 4.3: RFID Bill of Rights vs. EPCglobal Guidelines (first published in [160])

cess as the best providable security on upcoming five cent tags, as they will only perform simple computational operations, excluding conventional cryptography. Other examples for this view include Sarma et al., who explicitly call strong symmetric key encryption "a challenge in short term" [166] and Juels' work on "yoking proofs" [82] in which he claims MD5 hash functions are beyond reach for low cost RFID tags for the coming years. Furthermore, even downscaled variants of common cryptographic algorithms like the AES implementation by Feldhofer et al. [54] will exceed the computational restrictions of the quintessential cheap RFID token, the EPC tag [12].

These samples indicate that this opinion is common in the RFID context and shared among the involved parties. Nevertheless, it is an important fact, as this absence of profen cryptographic solutions has the potential to cause further consumer concerns and seriously delay RFID's further development. Some of the already deployed RFID applications find widespread acceptance despite their proven lack of security [179], which indicates a weaker connection between security and consumer concerns than we believe. Nonetheless, this observation serves as our starting point for our examination of the current main development streams in RFID research, as it provides an explanation for the driving issues in this research direction.

4.3.6 Observation 6: There are a few main development streams in the RFID security and privacy complex that drive the technology forward

As we have seen, the fact that RFID tags cannot execute conventional cryptography is a common one. This makes computationally less complex algorithms an important research issue. Juels formulated the notion of "minimalist cryptography" [81], which basically means that standard cryptography is not a necessary prerequisite for providing security. The new cryptographically simple protocols mentioned in Observation 3 [140, 141,143,182] can be seen in this context. This race for computationally simpler solutions constitutes the biggest quantity of RFID security publications.

Even though standard cryptography is not feasible for the current generation of RFID tags, implementations of such more complex algorithms still present a valuable research field. This is due to the fact that RFID tags can be expected to provide more resources in the future. Additionally, in less cost critical applications using tags with more resources is economically justifiable. Such systems, for example banking systems containing mandatory sensitive information, usually employ far less tags than typical EPC applications. Typical publications in this research complex include efforts to adapt standard cryptography to RFID limitations, like Feldhofer et al.'s previously mentioned AES implementation [54] or initial efforts to make public key cryptography (PKC) available on RFID systems. Typical examples for the latter topic are recent publications on elliptic curve cryptography (ECC) on RFID. For example, Batina et al. present an elliptic curve generator for RFID tags in [13] and adaptations of RFID protocols for elliptic curve cryptography in [14]. However, to the best of our knowledge, there are no experimental implementations of this technology. Therefore, these advancements have yet to prove their practical feasibility.

Apart from these two main development streams there are some side developments usually consisting of only few publications. Such "one paper" research areas include malware and exploits [158], non protocol specific attacks [98] and integration of different solutions [156]. We believe that the last topic will grow in importance when the current solutions for security issues are incorporated into the next generation of RFID tags. Furthermore, there is little work on RFID in practical use, like for example Molnar's and Wagner's research on library RFID systems [132]. Such work can show important elements in the lifecycle of typical RFID applications and provide valuable lessons for further RFID deployment.

	Juels et al. [87]	**Hoepman et al. [74]**	**Carluccio et al. [29]**
Regional focus	Malaysia	European Union (especially Dutch)	Germany
Threats	Identity theft, tracking, hotlisting, biometric feature erosion due to automation and spillovers	Guessing the access key, tracking	concentrates on tracking
Function Creep	e-commerce	ubiquitous identification and tracking	ubiquitous tracking, only implicitly mentioned
Conclusion on security	Threatened through unauthorized reading	Threatened through unauthorized reading and irrevocable certificates	Threatened through weak access control and confidentiality mechanisms
Conclusion on privacy	Threatened through unauthorized reading	Threatened via sidechannels and possible information disclosure	Threatened through possibility of tracking
Improvements	Faraday cages, private collision avoidance, larger secrets	No RFID, Online authentication, on tag template check	none, but negative vision of tracking database

Table 4.4: Comparison of e-passport analysis

4.3.7 Observation 7: RFID equipped e-passports are considered insecure

Recently, as mentioned above several researchers focused on RFID equipped *e-passports* also called MRTDs following the ICAO specification. Juels et al. [87], Hoepman et al. Hoepman et al. [74] and Carluccio et al. Carluccio et al. [29] all focused on passports from different countries and more or less independently found that the security and privacy features of actual passport implementations raise serious concerns. Main issues in this context are a potential function creep when the e-passports and their environment are used for additional purposes like for example e-commerce. This, especially in combination with other trends like automatized passport checks, has a tendency to erode existing security mechanics. Moreover, privacy appears to have been of minor importance when designing the specification. All authors find the privacy protection of e-passports weaker than the security features. This allows tracking and hotlisting up to a global level. Carluccio et al. [29] explicitly describe the construction of a global tracking database by an adversary, able to break the basic access control features of e-passports.

Along with their security discussions, the various authors also give some recommendations for possible improvements. For example, Juels et al. advise to put passport check terminals inside a faraday cage installation to prevent adversaries from eavesdropping on the communication. Moreover, they see private collision avoidance as a necessary improvement to keep other layers (see section 4.2.4) of RFID systems from compromising passport bearer privacy. Hoepman et al. take an even more rigid approach to privacy protection and advise to redesign e-passports without RFID, based on smart card technology. Because legitimate e-passport checks require optical access, this would only limit the amount of potential misuse, but not the intended use.

Another, rather sensational misuse of RFID equipped e-passports are RFID-bombs, often referred to as "American-sniffing bombs". By attaching an RFID reader to a bomb, terrorists could easily discover victims of the intended nationality, most likely

Americans. Such bombs are mentioned in two of the examined publications [74, 87]. In addition, the information leaking from e-passports could be used by criminals to identify potential victims from wealthy countries.

4.4 Discussion and statistics

In this section we will examine how the current publications on RFID security and privacy are connected to our observations and assert our positions. tables 4.5 to 4.11 list the publications in our literature review. You may note that they are mostly identical with the papers listed in Avoine's bibliography. This is due to the fact that after discovering this site, we have added almost all publications listed there to our list of references, because of their relevance for our research field. Subsequently, in table 4.15 we will see in detail, which publication corresponds with our observations referring to statistical facts.

Now we will take a look at the meaning of each of the columns in tables 4.5 to 4.11. The first one gives each publication's author(s) and reference, the next two columns state to which of the development steams (if any) in Observation 6 (see section 4.3.6) the paper belongs in our view. These are either the low cost topic for typical EPC tags or any attempts to make "high tech", namely conventional cryptography feasible on RFID. The third column shows if the paper contains a new protocol (or improvements to an existing one), while the fourth column tells whether it contains material on security models. Finally, the last column shows papers, demonstrating successful attacks or present formal mistakes in the protocol. Papers in this last category often automatically falsify the claim on provable security made by protocol inventors.

In the context of this section it is important to note that some protocols are presented in more than one publication, therefore not every single entry in the corresponding columns of the tables denotes a new protocol. An entry to the column "analysis/attack" does not always mean that a protocol has been proven insecure, in some cases publications marked there only show possible attacks that might even have been foreseen by the protocol inventors. The authors of subsequent publications sometimes only put more emphasis on the importance and damage potential of such an attack. Moreover, you will note that some entries are between brackets. This denotes the fact that a publication does not conform fully with the intended meaning of this category. For example some authors present minor refinements to existing protocols, which do not constitute a new protocol but do nevertheless add to our knowledge in this category.

When studying tables 4.5 to 4.11 you will further notice that some of the listed publications are not corresponding with any of our selected categories. To briefly explain the value and relevance of these papers for our review the subsequent tables 4.12 to 4.14 feature some short notes on their contents. This table is comprised of the publications citation, its title and a note which gives the previously mentioned explanation.

Finally, table 4.15 will give a rough overview on our empirical findings. Here you can see the numbers of publications corresponding with each category in the overview tables as well as those without any category in this review.

Of the 157 publications we selected for this literature review, we found more than hundred that deal with low cost issues, new cryptographically simple protocols or are in any other way connected to our identified low cost development stream. Although we found only 18 publications conforming with our second identified development stream, the possibility to integrate conventional cryptography like AES or even simple public key cryptography into RFID environments is fairly new. Most of the publications listed in this category appeared only recently, therefore we expect to see much more such publications in the near future.

Moreover, the growing importance of RFID identification and authentication protocols is quite obvious regarding the fact that we found 75 publications out of the 157 to be at least somehow connected to RFID protocols. Even though, a considerable number of these papers contain only minor refinements to already known protocols, we still see that a remarkable amount of the examined literature is concerned with cryptographic solutions and RFID protocols of all sorts. Lately, we see a beginning and growing correspondence between publications on conventional cryptography and protocols in the RFID context. This shows that the attempts to adapt well known cryptographic solutions to RFID have developed far enough to allow their incorporation into all sorts of formalized protocols. Furthermore, this fact indicates that researcher's interest moved from theoretical resource considerations to more practical implementation issues recently (see section 4.3.3).

Regarding Avoine's and Oechslin's early statement that there are only very few authors who provide formal security analysis of RFID protocols, we have already outlined the changes RFID research undergoes at the moment in section 4.3.6. Here we can see that 15 papers of our literature review offer such formal analysis or describe detailed attacks against protocols. As you can see in the detailed overview tables 4.5 to 4.11 most of them appeared only recently.

Our seventh observation (see section 4.3.7) addressed only three publications of our literature base. However, we discovered references to a fourth publication, but were unable to receive a copy of this paper. Therefore, we had to base our observation on only the three papers we were able to retrieve. Nevertheless, these three do already give an overview on the popular topic of e-passports and their potential misuse.

	Low Cost topic	**High Tech**	**Protocol**	**Model**	**Analysis / attack**
Landt [107]	0	0	0	0	0
Sarma et al. [166]	x	0	0	0	0
Feldhofer [52]	x	0	(x)	0	0
Juels and Pappu [88]	x	0	(x)	0	0
Weis et al. [187]	x	0	x	0	0
Sarma et al. [167]	x	0	0	0	0
Vajda and Buttyán [182]	x	0	x	0	0
Juels et al. [89]	x	0	0	0	0
Ohkubo et al. [137]	x	0	x	0	0
Kumar [103]	0	0	0	0	0
Inoue and Yasuura [78]	x	0	0	0	0
Feldhofer [53]	x	0	x	0	0
Good et al. [63]	0	0	0	0	0
Brito [20]	0	0	0	0	0
Juels [82]	x	0	(x)	0	0
Henrici and Müller [71]	x	0	x	0	0
Spiekermann and Berthold [173]	x	0	0	0	0
Henrici and Müller [72]	x	0	(x)	0	0
Saito et al. [163]	x	0	x	0	x
Fishkin et al. [57]	x	0	0	0	0
Feldhofer et al. [54]	0	x	0	0	0
Avoine [5]	x	0	0	0	x
Ranasinghe et al. [148]	x	0	0	0	0

Table 4.5: Enumeration of Publications in the literature review (Part 1)

	Low Cost topic	**High Tech**	**Protocol**	**Model**	**Analysis / attack**
Ranasinghe et al. [147]	0	0	0	0	0
Juels [81]	x	0	x	0	0
Molnar and Wagner [132]	x	0	(x)	0	0
Juels and Brainard [86]	x	0	0	0	0
Hennig et al. [70]	x	0	0	0	0
Engberg et al. [48]	x	0	x	0	0
Floerkemeier et al. [58]	x	0	0	0	0
Hanke [66]	x	0	0	0	0
Juels [83]	0	0	0	0	0
Avoine and Oechslin [10]	x	0	0	0	0
Saito and Sakurai [164]	x	0	(x)	0	0
Weis [186]	x	0	(x)	0	0
Juels [85]	x	0	0	0	0
Staake et al. [174]	x	0	0	0	0
Avoine and Oechslin [9]	x	0	x	0	0
Aigner and Feldhofer [1]	0	x	0	0	0
Rhee et al. [151]	x	0	x	0	0
Ayoade et al. [11]	0	0	0	0	0
Rieback et al. [152]	x	0	0	0	0
Kinoshita et al. [100]	0	x	x	0	0
Lee et al. [111]	x	0	x	0	0
Rieback et al. [153]	0	0	0	0	0
Garfinkel et al. [60]	0	0	0	0	0
Juels et al. [90]	0	x	0	0	0

Table 4.6: Enumeration of Publications in the literature review (Part 2)

	Low Cost topic	**High Tech**	**Protocol**	**Model**	**Analysis / attack**
Spiekermann [172]	0	0	0	0	0
Rieback et al. [157]	x	0	0	0	0
Yeo and Kim [192]	x	0	x	0	0
Kwak et al. [105]	x	0	x	0	0
Kang and Nyang [93]	x	0	x	0	0
Fabian et al. [51]	x	0	0	0	0
Chang [32]	x	0	x	0	0
Bono et al. [17]	0	0	0	0	(x)
Yang et al. [191]	x	0	x	0	0
Wolkerstorfer [189]	0	x	0	0	0
Molnar et al. [131]	x	0	x	0	0
Dominikus et al. [46]	0	x	x	0	0
Chabanne and Fumaroli [31]	x	0	(x)	0	0
Carluccio et al. [28]	0	0	0	0	0
Juels and Weis [91]	x	0	x	0	0
Avoine et al. [8]	x	0	(x)	0	0
Gilbert et al. [62]	x	0	0	0	x
Lim and Korkishko [118]	x	0	0	0	0
Gao et al. [59]	x	0	(x)	0	0
Kfir and Wool [98]	x	0	0	0	0
Juels et al. [87]	0	0	0	0	0
Hancke and Kuhn [68]	0	(x)	0	0	0
Dimitriou [44]	x	0	x	0	0
Zhang and King [196]	x	0	(x)	(x)	(x)

Table 4.7: Enumeration of Publications in the literature review (Part 3)

	Low Cost topic	**High Tech**	**Protocol**	**Model**	**Analysis / attack**
Juels [84]	0	0	0	0	0
Avoine [6]	0	0	0	x	0
Ateniese [4]	x	0	x	0	0
Molnar et al. [130]	0	0	0	0	0
Karjoth and Moskowitz [94]	x	0	0	0	0
Nohara et al. [135]	x	0	(x)	0	0
Lee and Verbauwhede [112]	x	0	x	0	0
Choi et al. [35]	x	0	x	0	0
Zhang and King [197]	x	0	0	x	0
Karthikeyan and Nesterenko [95]	x	0	x	0	0
Stapleton-Gray [175]	0	0	0	0	0
Roussos [161]	(x)	0	0	0	0
Nguyen et al. [134]	x	0	x	0	0
Lee et al. [110]	x	0	x	0	0
Liu and Peng [120]	0	x	0	0	0
Israsena [79]	x	0	(x)	0	0
Tuyls and Batina [181]	0	(x)	0	0	0
Dimitrou [45]	x	0	x	0	0
Tsudik [180]	x	0	x	0	0
Kirschenbaum and Wool [101]	x	0	0	0	0
Reid et al. [150]	0	x	(x)	0	0
Rieback et al. [158]	(x)	0	0	0	0
Rieback et al. [159]	(x)	0	0	0	0

Table 4.8: Enumeration of Publications in the literature review (Part 4)

	Low Cost topic	**High Tech**	**Protocol**	**Model**	**Analysis / attack**
Rieback et al. [154]	0	0	0	0	0
Lohman et al. [121]	0	0	0	0	0
Castelluccia and Avoine [30]	x	0	x	0	0
Calmels et al. [25]	0	x	x	0	0
Kim et al. [99]	x	0	0	0	0
Juels and Weis [92]	x	0	0	x	0
Whong et al. [190]	x	0	x	0	0
Katz and Sun Shin [97]	x	0	(x)	0	0
Bringer et al. [19]	x	0	(x)	0	0
Chatmon et al. [33]	x	0	x	0	0
Piramuthu [145]	x	0	(x)	0	0
Piramuthu [144]	x	0	(x)	0	x
Halamka et al. [65]	0	0	0	0	0
Hoepman et al. [74]	0	0	0	0	0
Hancke [67]	x	0	0	0	0
Zhai et al. [195]	x	0	x	0	0
Choi and Roh [36]	x	0	x	0	0
Park et al. [139]	x	0	x	0	0
Buttyan et al. [24]	x	0	(x)	0	0
Carluccio et al. [29]	0	0	0	0	0
Carluccio et al. [27]	0	0	0	0	0
Peris-Lopez et al. [140]	x	0	x	0	0
Yu et al. [193]	0	0	0	0	0
Lehtonen et al. [113]	x	0	0	0	0

Table 4.9: Enumeration of Publications in the literature review (Part 5)

	Low Cost topic	**High Tech**	**Protocol**	**Model**	**Analysis / attack**
Kumar and Paar [104]	0	x	0	0	0
Sakiyama et al. [165]	0	x	0	0	0
Haselsteiner and Breitfuss [69]	0	0	0	0	0
Poschmann et al. [146]	0	x	0	0	0
Seo and Kim [169]	x	0	x	0	0
Kwon et al. [106]	x	0	0	0	x
Batina et al. [13]	0	x	0	0	0
Damgard and Østergaard [41]	0	0	0	(x)	0
Burmester et al. [23]	0	0	0	x	0
Burmester et al. [22]	0	0	(x)	(x)	0
Bringer and Chabanne [18]	x	0	(x)	0	(x)
Peris-Lopez et al. [142]	0	0	0	0	0
Peris-Lopez et al. [141]	x	0	x	0	0
Bailey and Juels [12]	x	0	0	0	0
Roussos and Moussouri [162]	x	0	0	0	0
Rieback et al. [156]	x	0	0	0	0
Peris-Lopez et al. [143]	x	0	x	0	0
Nohl and Evans [136]	x	0	0	0	x
Lim and Kwon [119]	x	0	x	0	0
Katz and Smith [96]	x	0	0	0	x
Lehtonen et al. [114]	0	0	0	0	0
Heydt et al. [73]	0	0	0	0	0
Vaudenay [183]	0	x	x	0	0
McLoone and Robshaw [127]	0	x	(x)	0	0

Table 4.10: Enumeration of Publications in the literature review (Part 6)

	Low Cost topic	**High Tech**	**Protocol**	**Model**	**Analysis / attack**
Cui et al. [40]	0	x	x	0	0
Conti et al. [39]	x	0	x	0	0
Batina [14]	0	x	x	0	(x)
Defend et al. [43]	x	0	0	0	x
Cichon et al. [38]	x	0	(x)	0	0
Tan et al. [177]	x	0	x	0	0
Bolotnyy and Robins [16]	x	0	x	0	0
Lu et al. [122]	x	0	x	0	0
Solanas et al. [171]	x	0	x	0	0
Li and Deng [116]	x	0	0	0	x
Li and Wang [117]	x	0	0	0	x
Le et al. [108]	x	0	x	(x)	0
Mirowski and Hartnett [128]	x	0	0	0	0
Chien and Chen [34]	x	0	x	0	x
Lemieux and Tang [115]	x	0	x	0	0

Table 4.11: Enumeration of Publications in the literature review (Part 7)

	Title	**Note**
[107]	Shrouds of Time: The history of RFID	RFID timeline and development decades
[103]	Interaction of RFID Technology and Public Policy	proposes RFID policy based on "10 Commandments of computer ethics"
[63]	Radio Frequency Id and Privacy with Information Goods	Threat and best practicy overview, advocating use of technical solutions
[20]	Relax, don't do it: Why RFID Privacy Concerns are Exaggerated and Legislation is premature	Opposes RFID regulation and doubts the relevance of tracking threats
[147]	Low-Cost RFID Systems: Confronting Security and Privacy	Gives an early overview on proposed solutions
[83]	RFID Privacy: A Technical Primer for the Non-Technical Reader	Overview on some aspects of RFID security
[11]	A prototype System of the RFID Authentication Processing Framework	Framework for an online authentication scenario
[153]	Uniting Legislation with RFID Privacy-Enhancing Technologies	Predecessor of guardian papers, emphasizes legal requirements for RFID and necessities to fulfill them
[60]	RFID Privacy: An Overview of Problems and Proposed Solutions	Overview on technologies and threats
[172]	Perceived Control: Scales for Privacy in Ubiquitous Computing Environments	Scales to measure "perceived" privacy by users
[28]	Electromagnetic side channel analysis of a contactless smart card: first results	Initial results of an attempt to recover ciphers physically

Table 4.12: List of Publications without Category (Part 1)

	Title	**Note**
[87]	Security and Privacy Issues in E-passports	Analysis of the International Civil Aviation Organization (ICAO) specification on Machine Readable Travel Documents (MRTD)
[84]	RFID Security and Privacy: A research Survey	literature review (see section 3.1.2)
[130]	Privacy for RFID Through Trusted Computing	Trusted computing on RFID readers - splitting core functionality, policy engine and user auditing engine
[175]	Would Macy's Scan Gimbels? Competitive Intelligence and RFID	Considerations about RFID based business intelligence
[154]	The Evolution of RFID Security	RFID's history and its influence on further development
[121]	Analysis of power constraints for cryptographic algorithms in mid-cost RFID tags	Compares RFID resources to power requirements of several cryptographic algorithms
[65]	The Security Implications of VeriChip Cloning	Analysis of RFID body implants
[74]	Crossing Borders: Security and Privacy Issues of the European e-Passport	analysis and fundamental improvement suggestions
[29]	E-passport: the global traceability or how to feel like an UPS package	privacy discussion using german passports as case study
[27]	Implementation details of a multi purpose ISO 14443 RFID-tool	Presents fake devices for RFID testing
[193]	Securing RFID with Ultra-wideband Modulation	new communication channel to provide security

Table 4.13: List of Publications without Category (Part 2)

	Title	**Note**
[69]	Security in Near Field Communication (NFC)	Use Cases for NFC
[142]	RFID Systems: A Survey on Security Threats and Proposed Solutions	overview on different security approaches
[114]	Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices	Blocking illicit scanning of RFID devices by limiting some information to an optical channel
[73]	Vulnerabilities in first-generation RFID-enabled credit cards	vulnerabilities of RFID-enabled credit cards in practice

Table 4.14: List of Publications without Category (Part 3)

Category	**Number of Publications**
Low Cost topic	103(3)
High Tech	16(2)
Protocol	52(23)
Model	4(4)
Analysis / Attack	11(4)
None	26
Total	157

Table 4.15: The literature review in numbers

Chapter 5

Conclusion and Additional Issues

In this section we will look at some conclusions to our RFID literature review and point out some points for future research we have seen during our examination. Finally, we will use this chapter to give some final remarks.

5.1 Summary

In this work we have seen that RFID we have examined the state-of-the-art in RFID research and also discussed some observations on it. Initially, we considered the use of RFID and its history, which dates back for quite some time. Following an anecdotic line of arguments, it can be dated back to the Big Bang (see section 1.2) but realistically to the Identification Friend or Foe System, invented in the middle of the 20th century. Nevertheless, the development we were interested in only took place in recent years.

Therefore, we subsequently discussed the structure and functionality of modern RFID systems. In addition to the basic parts of an RFID system (reader, tag, data processing subsystem), we also examined the differences of the forward and backward communications channels and the possible anti-collision behavior alternatives available for RFID. Moreover, we looked at the relevant standards in the RFID field, namely the ISO-14443 and ISO-15693 standards for contactless smart cards and the standards for EPC tags. The latter were examined by looking into the general functionality of the EPCglobal Network, the functional base for the famous "internet of things" [179]. Moreover, we examined common attacks possible in RFID environments and some examples of RFID systems already in use.

In the next chapter, we took a look at other literature reviews in both the RFID and the security complex. We have seen that only few literature reviews provide insight into our particular topic. Nevertheless, both aspects of the topic, namely security and RFID, have received attention from authors of literature reviews. Therefore, we did examine some reviews dealing with only one of our two topics in that chapter.

Afterwards, we started our actual literature review by specifying our methodology. In the following section, we gave an overview on the current state-of-the-art in RFID security and privacy. There, we examined literature on RFID specific attacks and problems, common RFID security proposals and ways to adapt conventional cryptography to RFID. Moreover, we took a look on publications addressing RFID security models and e-passport security. To cover some emerging topics in RFID, we also included publications on RFID in use and the integration of different approaches to security and privacy in this section. Subsequently, we gave our observations based on the literature on these topics. In the final section of this chapter, we discussed our findings in a statistical context and showed what publications correspond with which observation.

5.2 Possible research directions

During our literature review, we identified a number of open questions in this field. Apart from designing new protocols and conducting security analysis of their properties, interested researchers might find rewarding open questions like the construction of a holistic RFID security model. Until now, no presented model offers a way to analyze security and privacy aspects of all three RFID layers explained in section 4.2.4.

Furthermore, publications on ways to integrate different RFID security proposals into a holistic set of security measures like in [157] are needed to provide practical relieve to some of the pressing concerns potential RFID users have.

5.3 Final remarks

Finally, it is noteworthy that RFID is still a technology under development, which can be expected to change significantly during the coming years. We have previously seen that RFID is an emerging technology and that publications in the various related research areas arise increasingly fast. The range and types of these publications change significantly and new protocols for secure RFID communications appear at an fast rate. We believe that this trend will not change for some time, as even in the time needed for the creation of this work the RFID landscape underwent considerable change.

Appendix A

Bibliography

[1] Manfred Aigner and Martin Feldhofer. Secure Symmetric Authentication for RFID Tags. In *Telecommunication and Mobile Computing – TCMC 2005*, Graz, Austria, March 2005.

[2] Kenneth Allendorfer and Shantanu Pai. Human factors considerations for passwords and other user identification techniques. Technical Report DOT/FAA/CT-05/20, Federal Aviation Administration William J. Hughes Technical Center, Atlantic City International Airport, New Jersey, USA, 2005. Available online at http://hf.tc.faa.gov/technotes/dot_faa_ct_05_20.pdf.

[3] John Argyrakis, Stefanos Gritzalis, and Chris Kioulafas. Privacy enhancing technologies: A review. In R. Traunmüller, editor, *Electronic Government*, volume 2739 of *Lecture Notes in Computer Science*, pages 82–287. Springer-Verlag, 2003.

[4] Giuseppe Ateniese, Jan Camenisch, and Breno de Medeiros. Untraceable RFID Tags via Insubvertible Encryption. In *Conference on Computer and Communications Security – CCS '05*, pages 92–101, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.

[5] Gildas Avoine. Privacy Issues in RFID Banknote Protection Schemes. In Jean-Jacques Quisquater, Pierre Paradinas, Yves Deswarte, and Anas Abou El Kadam,

editors, *International Conference on Smart Card Research and Advanced Applications – CARDIS*, pages 33–48, Toulouse, France, August 2004. IFIP, Kluwer Academic Publishers.

[6] Gildas Avoine. Adversary model for radio frequency identification. Technical Report LASEC-REPORT-2005-001, Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC), Lausanne, Switzerland, September 2005.

[7] Gildas Avoine. Bibliography on security and privacy in RFID systems. Available Online at http://lasecwww.epfl.ch/˜gavoine/rfid/, 2006.

[8] Gildas Avoine, Etienne Dysli, and Philippe Oechslin. Reducing time complexity in RFID systems. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography – SAC 2005*, volume 3897 of *Lecture Notes in Computer Science*, pages 291–306, Kingston, Canada, August 2005. Springer-Verlag.

[9] Gildas Avoine and Philippe Oechslin. A Scalable and Provably Secure Hash Based RFID Protocol. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2005*, pages 110–114, Kauai Island, Hawaii, USA, March 2005. IEEE, IEEE Computer Society Press.

[10] Gildas Avoine and Philippe Oechslin. RFID Traceability: A Multilayer Problem. In Andrew Patrick and Moti Yung, editors, *Financial Cryptography – FC'05*, volume 3570 of *Lecture Notes in Computer Science*, pages 125–140, Roseau, The Commonwealth Of Dominica, February–March 2005. IFCA, Springer-Verlag.

[11] John Ayoade, Osamu Takizawa, and Koji Nakao. A prototype System of the RFID Authentication Processing Framework. In *International Workshop in Wireless Security Technologies, available at http://www.iwwst.org.uk/Files/2005/Proceedings2005.pdf*, London, UK, April 2005.

[12] Daniel Bailey and Ari Juels. Shoehorning Security into the EPC Standard. In Roberto De Prisco and Moti Yung, editors, *International Conference on Security in Communication Networks – SCN 2006*, volume 4116 of *Lecture Notes in Computer Science*, pages 303–320, Maiori, Italy, September 2006. Springer-Verlag.

[13] Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. An Elliptic Curve Processor Suitable For RFID-Tags. Cryptology ePrint Archive, Report 2006/227, 2006.

[14] Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. Public-key cryptography for RFID-tags. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 217–222, New York, USA, March 2007. IEEE, IEEE Computer Society Press.

[15] France Belanger, Janine S. Hiller, and Wanda J. Smith. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems, Volume 11*, pages 245–270, 2002.

[16] Leonid Bolotnyy and Gabriel Robins. Physically Unclonable Function-Based Security and Privacy in RFID Systems. In *International Conference on Pervasive Computing and Communications – PerCom 2007*, pages 211–220, New York, USA, March 2007. IEEE, IEEE Computer Society Press.

[17] Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Avi Rubin, and Michael Szydlo. Security analysis of a cryptographically-enabled RFID device. In *USENIX Security Symposium*, pages 1–16, Baltimore, Maryland, USA, July-August 2005. USENIX.

[18] Julien Bringer and Hervé Chabanne. On the wiretap channel induced by noisy tags. In *European Workshop on Security and Privacy in Ad hoc and Sensor Networks – ESAS'06*, Lecture Notes in Computer Science, Hamburg, Germany, September 2006. Springer-Verlag.

[19] Julien Bringer, Hervé Chabanne, and Emmanuelle Dottax. HB^{++}: a lightweight authentication protocol secure against some attacks. In *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU 2006*, Lyon, France, June 2006. IEEE, IEEE Computer Society Press.

[20] Jeremy Brito. Relax, don't do it: Why RFID privacy concerns are exaggerated and legislation is premature. *Journal of Law and Technology*, volume 8(number 2), 2004.

[21] L. Burdet. RFID multiple access methods. Technical report, ETH Zürich, Zürich, Switzerland, 2005. Available online at http://www.cs.rutgers.edu/~badri/553dir/papers/06_rfid-mac_report.pdf.

[22] Mike Burmester, Tri van Le, and Breno de Medeiros. Provably Secure Ubiquitous Systems: Universally Composable RFID Authentication Protocols. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm*, Baltimore, Maryland, USA, August-September 2006. IEEE.

[23] Mike Burmester, Tri van Le, and Breno de Medeiros. Towards provable security for ubiquitous applications. In Lynn Margaret Batten and Reihaneh Safavi-Naini, editors, *Australasian Conference on Information Security and Privacy – ACISP'06*, volume 4058 of *Lecture Notes in Computer Science*, pages 295–312, Melbourne, Australia, July 2006. Springer-Verlag.

[24] Levente Buttyán, Tamás Holczer, and István Vajda. Optimal Key-Trees for Tree-Based Private Authentication. In *Workshop on Privacy Enhancing Technologies - PET 2006*, Cambridge, United Kingdom, June 2006.

[25] Benoit Calmels, Sébastien Canard, Marc Girault, and Hervé Sibert. Low-cost cryptography for privacy in RFID systems. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *International Conference on Smart Card Research*

and Advanced Applications – CARDIS, Lecture Notes in Computer Science, Tarragona, Spain, April 2006. IFIP, Springer-Verlag.

[26] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS '01: Proceedings of the 42nd IEEE symposium on Foundations of Computer Science*, pages 136–145, Washington, DC, USA, 2001. IEEE Computer Society.

[27] Dario Carluccio, Timo Kasper, and Christof Paar. Implementation details of a multi purpose ISO 14443 RFID-tool. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[28] Dario Carluccio, Kerstin Lemke, and Christof Paar. Electromagnetic side channel analysis of a contactless smart card: first results. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.

[29] Dario Carluccio, Kerstin Lemke-Rust, Christof Paar, and Ahmad-Reza Sadeghi. E-passport: the global traceability or how to feel like an UPS package. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[30] Claude Castelluccia and Gildas Avoine. Noisy tags: A pretty good key exchange protocol for RFID tags. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *International Conference on Smart Card Research and Advanced Applications – CARDIS*, volume 3928 of *Lecture Notes in Computer Science*, pages 289–299, Tarragona, Spain, April 2006. IFIP, Springer-Verlag.

[31] Hervé Chabanne and Guillaume Fumaroli. Noisy cryptographic protocols for low cost RFID tags. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.

[32] Gwo-Ching Chang. A feasible security mechanism for low cost RFID tags. In *International Conference on Mobile Business – ICMB'05*, pages 675–677, Sydney, Australia, July 2005. IEEE, IEEE Computer Society.

[33] Christy Chatmon, Tri van Le, and Mike Burmester. Secure anonymous RFID authentication protocols. Technical Report TR-060112, Florida State University, Department of Computer Science, Tallahassee, Florida, USA, 2006.

[34] Hung-Yu Chien and Che-Hao Chen. Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards. *Computer Standars & Interfaces, Elsevier Science Publishers*, 29(2):254–259, February 2007.

[35] Eun Young Choi, Su Mi Lee, and Dong Hoon Lee. Efficient RFID authentication protocol for ubiquitous computing environment. In Tomoya Enokido, Lu Yan, Bin Xiao, Daeyoung Kim, Yuanshun Dai, and Laurence Yang, editors, *International Workshop on Security in Ubiquitous Computing Systems – secubiq 2005*, volume 3823 of *Lecture Notes in Computer Science*, pages 945–954, Nagasaki, Japan, December 2005. Springer-Verlag.

[36] Wonjoon Choi and Byeong-hee Roh. Backward channel protection method for RFID security schemes based on tree-walking algorithms. In Marina L. Gavrilova, Osvaldo Gervasi, Vipin Kumar, Chih Jeng Kenneth Tan, David Taniar, Antonio Laganà, Youngsong Mun, and Hyunseung Choo, editors, *International Conference on Computational Science and its Applications - ICCSA 2006, Proceedings, Part IV*, volume 3983 of *Lecture Notes in Computer Science*, pages 279–287, Glasgow, Scotland, May 2006. Springer-Verlag.

[37] Grace Chung and Sara M. Grimes. Cool hunting the kids' digital playground: Datamining and the privacy debates in children's online entertainment sites. In *Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS)*, volume 07, Los Alamitos, CA, USA, 2005. IEEE Computer Society.

[38] Jacek Cichon, Marek Klonowski, and Miroslaw Kutylowski. Privacy Protection in Dynamic Systems Based on RFID Tags. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 235–240, New York, USA, March 2007. IEEE, IEEE Computer Society Press.

[39] Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, and Angelo Spognardi. RIPP-FS: an RFID identification, privacy preserving protocol with forward secrecy. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 229–234, New York, USA, March 2007. IEEE, IEEE Computer Society Press.

[40] Yang Cui, Kazukuni Kobara, Kanta Matsuura, and Hideki Imai. Lightweight asymmetric privacy-preserving authentication protocols secure against active attack. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 223–228, New York, USA, March 2007. IEEE, IEEE Computer Society Press.

[41] Ivan Damgård and Michael Østergaard. RFID security: Tradeoffs between security and efficiency. Cryptology ePrint Archive, Report 2006/234, 2006.

[42] John D. Day and Hubert Zimmermann. The OSI reference model. *Proceedings of the IEEE, vol. 71, no. 12*, pages 1334–1340, 1983.

[43] Benessa Defend, Kevin Fu, and Ari Juels. Cryptanalysis of Two Lightweight RFID Authentication Schemes. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 211–216, New York, USA, March 2007. IEEE, IEEE Computer Society Press.

[44] Tassos Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm*, Athens, Greece, September 2005. IEEE.

[45] Tassos Dimitriou. A secure and efficient RFID protocol that could make big brother (partially) obsolete. In *International Conference on Pervasive Computing and Communications – PerCom 2006*, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press.

[46] Sandra Dominikus, Elisabeth Oswald, and Martin Feldhofer. Symmetric authentication for RFID systems in practice. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.

[47] J. B. Earp and F. C. Payton. Data protection in the university setting: employee perceptions of student privacy. In *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, Los Alamitos, CA, USA, 2001. IEEE Computer Society.

[48] Stephan Engberg, Morten Harning, and Christian Damsgaard Jensen. Zero-knowledge device authentication: Privacy & security enhanced RFID preserving business value and consumer convenience. In *Conference on Privacy, Security and Trust – PST*, New Brunswick, Canada, October 2004.

[49] European Union ARTICLE 29 Data Protection Working Party. Results of the public consultation on article 29 working document 105 on data protection issues related to RFID technology. *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf*, 2005.

[50] European Union ARTICLE 29 Data Protection Working Party. Working document on data protection issues related to RFID technology. *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf*, 2005.

[51] Benjamin Fabian, Oliver Günther, and Sarah Spiekermann. Security analysis of the object name service for RFID. In *International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU'05*, Santorini Island, Greece, July 2005. IEEE, IEEE Computer Society Press.

[52] Martin Feldhofer. A Proposal for Authentication Protocol in a Security Layer for RFID Smart Tags, 2003.

[53] Martin Feldhofer. An authentication protocol in a security layer for RFID smart tags. In *MELECON 2004: Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference*, volume 2, pages 759–762. IEEE, May 2004.

[54] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. Strong Authentication for RFID Systems using the AES Algorithm. In Marc Joye and Jean-Jacques Quisquater, editors, *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370, Boston, Massachusetts, USA, August 2004. IACR, Springer-Verlag.

[55] Alison Felstead. The library systems market: a digest of current literature. *Program: electronic library and information systems; Volume: 38 Issue: 2*, pages 88–96, 2004.

[56] Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification.* Hanser, München, Germany, 2002. German version.

[57] Kenneth Fishkin, Sumit Roy, and Bing Jiang. Some methods for privacy in RFID communication. In Claude Castelluccia, Hannes Hartenstein, Christof Paar, and Dirk Westhoff, editors, *European Workshop on Security in Ad-hoc and Sensor Networks – ESAS 2004*, volume 3313 of *Lecture Notes in Computer Science*, pages 42–53, Heidelberg, Germany, August 2005. Springer-Verlag.

[58] Christian Floerkemeier, Roland Schneider, and Marc Langheinrich. Scanning with a purpose – supporting the fair information principles in RFID protocols. In Hitomi Murakami, Hideyuki Nakashima, Hideyuki Tokuda, and Michiaki Yasumura, editors, *International Symposium on Ubiquitous Computing Systems – UCS 2004*, volume 3598 of *Lecture Notes in Computer Science*, pages 214–231, Tokyo, Japan, November 2004. Springer-Verlag.

[59] Xingxin (Grace) Gao, Zhe (Alex) Xiang, Hao Wang, Jun Shen, Jian Huang, and Song Song. An approach to security and privacy of RFID system for supply

chain. In *Conference on E-Commerce Technology for Dynamic E-Business – CEC-East'04*, pages 164–168, Beijing, China, September 2005. IEEE, IEEE Computer Society.

[60] Simson Garfinkel, Ari Juels, and Ravi Pappu. RFID privacy: An overview of problems and proposed solutions. *IEEE Security and Privacy*, 3(3):34–43, May-June 2005.

[61] Claire Gauzente. Web merchants' privacy and security statements: How reassuring are they for consumers? a two-sided approach. *Journal of Electronic Commerce Research, VOL. 5, NO.3*, pages 181 – 198, 2004.

[62] Henri Gilbert, Matthew Robshaw, and Hervé Sibert. An active attack against HB$^+$ – a provably secure lightweight authentication protocol. Manuscript, July 2005.

[63] Nathan Good, David Molnar, Jennifer M. Urban, Deirdre Mulligan, Elizabeth Miles, Laura Quilter, and David Wagner. Radio frequency Id and privacy with information goods. In *WPES '04: Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, pages 41–42, New York, NY, USA, 2004. ACM Press.

[64] A. Gunasekaran and E.W.T. Ngai. Build-to-order supply chain management: a literature review and framework for development. *Journal of Operations Management, Volume 23, Issue 5*, pages 423–451, 2005.

[65] John Halamka, Ari Juels, Adam Stubblefield, and Jonathan Westhues. The security implications of verichip$^{\mathrm{TM}}$cloning. Manuscript in submission, March 2006.

[66] Gerhard Hancke. A Practical Relay Attack on ISO-14443 Proximity Cards. Manuscript, February 2005.

[67] Gerhard Hancke. Practical attacks on proximity identification systems (short paper). In *IEEE Symposium on Security and Privacy*, Oakland, California, USA, May 2006. IEEE, IEEE Computer Society Press.

[68] Gerhard Hancke and Markus Kuhn. An RFID distance bounding protocol. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, Athens, Greece, September 2005. IEEE.

[69] Ernst Haselsteiner and Klemens Breitfuss. Security in Near Field Communication (NFC). Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[70] Jan Hennig, Peter Ladkin, and Bernd Sieker. Privacy enhancing technology concepts for RFID technology scrutinised. Research Report RVS-RR-04-02, University of Bielefeld, Bielefeld, Germany, October 2004.

[71] Dirk Henrici and Paul Müller. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In Ravi Sandhu and Roshan Thomas, editors, *International Workshop on Pervasive Computing and Communication Security – PerSec 2004*, pages 149–153, Orlando, Florida, USA, March 2004. IEEE, IEEE Computer Society.

[72] 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.

[73] Thomas S. Heydt-Benjamin, Dan V. Bailey, Kevin Fu, Ari Juels, and Tom O'Hare. Vulnerabilities in First-Generation RFID-enabled Credit Cards. Manuscript, October 2006.

[74] Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur. Crossing borders: Security and privacy issues of the european e-passport. In Hiroshi Yoshiura, Kouichi Sakurai, Kai Rannenberg, Yuko Murayama, and Shin-ichi Kawamura, editors, *Advances in Information and Computer Security, First International Workshop on Security – IWSEC*, volume 4266 of *Lecture Notes in Computer Science*, pages 152–167, Kyoto, Japan, October 2006. Springer-Verlag.

[75] Jiang-Liang Hou and Chih-Hao Huang. Quantitative performance evaluation of RFID applications in the supply chain of the printing industry. *Industrial Management Data Systems; Volume 106 Number 1*, pages 96–120, 2006.

[76] EPCglobal Inc. Draft protocol specification for a 900 MHz class 0 radio frequency identification tag, 2003. http://www.epcglobalinc.org/standards/specs/900_MHz_Class_0_RFIDTag_Specification.pdf.

[77] EPCglobal Inc. EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz - 960 MHz version 1.0.9, 2005.

[78] Sozo Inoue and Hiroto Yasuura. RFID privacy using user-controllable uniqueness. In *RFID Privacy Workshop*, MIT, Massachusetts, USA, November 2003.

[79] Pasin Israsena. Securing ubiquitous and low-cost RFID using tiny encryption algorithm. In *International Symposium on Wireless Pervasive Computing*, Phuket, Thailand, January 2006. IEEE, IEEE Press.

[80] Sixto Ortiz Jr. How secure is RFID? *Computer, Volume39, Number 7*, pages 17–19, 2006.

[81] Ari Juels. Minimalist Cryptography for Low-Cost RFID Tags. In Carlo Blundo and Stelvio Cimato, editors, *International Conference on Security in Communication Networks – SCN 2004*, volume 3352 of *Lecture Notes in Computer Science*, pages 149–164, Amalfi, Italia, September 2004. Springer-Verlag.

[82] Ari Juels. "Yoking-Proofs" for RFID Tags. In Ravi Sandhu and Roshan Thomas, editors, *International Workshop on Pervasive Computing and Communication Security – PerSec 2004*, pages 138–143, Orlando, Florida, USA, March 2004. IEEE, IEEE Computer Society.

[83] Ari Juels. *Privacy and Technologies of Identity, A Cross-Disciplinary Conversation (Eds K. Strandburg and D. Stan Raicu)*, chapter RFID Privacy: A Technical Primer for the Non-Technical Reader. Springer-Verlag, 2005.

[84] Ari Juels. RFID security and privacy: A research survey. Manuscript, September 2005.

[85] Ari Juels. Strengthening EPC Tags Against Cloning. Manuscript, March 2005.

[86] 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.

[87] Ari Juels, David Molnar, and David Wagner. Security and privacy issues in e-passports. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm*, Athens, Greece, September 2005. IEEE.

[88] Ari Juels and Ravikanth Pappu. Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In Rebecca N. Wright, editor, *Financial Cryptography – FC'03*, volume 2742 of *Lecture Notes in Computer Science*, pages 103–121, Le Gosier, Guadeloupe, French West Indies, January 2003. IFCA, Springer-Verlag.

[89] Ari Juels, Ronald L. 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 '03*, pages 103–111, Washington, DC, USA, October 2003. ACM, ACM Press.

[90] Ari Juels, Paul Syverson, and Dan Bailey. High-power proxies for enhancing RFID privacy and utility. In *Workshop on Privacy Enhancing Technologies - PET 2005*, Dubrovnik, Croatia, May-June 2005.

[91] Ari Juels and Stephen Weis. Authenticating pervasive devices with human protocols. In Victor Shoup, editor, *Advances in Cryptology – CRYPTO'05*, volume 3126 of *Lecture Notes in Computer Science*, pages 293–308, Santa Barbara, California, USA, August 2005. IACR, Springer-Verlag.

[92] Ari Juels and Stephen Weis. Defining strong privacy for RFID. Cryptology ePrint Archive, Report 2006/137, 2006.

[93] Jeonil Kang and Daehun Nyang. RFID authentication protocol with strong resistance against traceability and denial of service attacks. In Refik Molva, Gene Tsudik, and Dirk Westhoff, editors, *European Workshop on Security and Privacy in Ad hoc and Sensor Networks – ESAS'05*, volume 3813 of *Lecture Notes in Computer Science*, pages 164–175, Visegrad, Hungary, July 2005. Springer-Verlag.

[94] Günter Karjoth and Paul Moskowitz. Disabling RFID tags with visible confirmation: Clipped tags are silenced. In *Workshop on Privacy in the Electronic Society – WPES*, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.

[95] Sindhu Karthikeyan and Mikhail Nesterenko. RFID security without extensive cryptography. In *Workshop on Security of Ad Hoc and Sensor Networks – SASN'05*, pages 63–67, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.

[96] Jonathan Katz and Adam Smith. Analyzing the HB and HB+ protocols in the "large error" case. Cryptology ePrint Archive, Report 2006/326, 2006.

[97] Jonathan Katz and Ji Sun Shin. Parallel and concurrent security of the HB and HB$^+$ protocols. In Serge Vaudenay, editor, *Advances in Cryptology – EUROCRYPT'06*, Lecture Notes in Computer Science, Saint Petersburg, Russia, May-June 2006. IACR, Springer-Verlag.

[98] Ziv Kfir and Avishai Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, pages 47–58, Athens, Greece, September 2005. IEEE.

[99] Soo-Cheol Kim, Sang-Soo Yeo, and Sung Kwon Kim. MARP: Mobile agent for rfid privacy protection. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *International Conference on Smart Card Research and Advanced Applications – CARDIS*, Lecture Notes in Computer Science, Tarragona, Spain, April 2006. IFIP, Springer-Verlag.

[100] Shingo Kinoshita, Miyako Ohkubo, Fumitaka Hoshino, Gembu Morohashi, Osamu Shionoiri, and Atsushi Kanai. Privacy Enhanced Active RFID Tag. In *International Workshop on Exploiting Context Histories in Smart Environments – ECHISE'05*, Munich, Germany, May 2005.

[101] Ilan Kirschenbaum and Avishai Wool. How to build a low-cost, extended-range RFID skimmer. Cryptology ePrint Archive, Report 2006/054, 2006.

[102] Eleni Kosta, Martin Meints, Marit Hensen, and Mark Gasson. An analysis of security and privacy issues relating to RFID enabled epassports. In Hein Venter, Mariki Eloff, Les Labuschagne, Jan Eloff, and Rossouw Von Solms, editors, *IFIP International Federation for Information Processing, New approaches for Security, Privacy and Trust in Complex Environments*, volume 232, pages 467–472, Sandton, Gauteng, South Africa, May 2007. IFIP, Springer.

[103] Rakesh Kumar. Interaction of RFID technology and public policy. In *RFID Privacy Workshop*, MIT, MA, USA, November 2003.

[104] Sandeep Kumar and Christof Paar. Are standards compliant elliptic curve cryptosystems feasible on RFID? Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[105] Jin Kwak, Keunwoo Rhee, Soohyun Oh, Seungjoo Kim, and Dongho Won. RFID system with fairness within the framework of security and privacy. In Refik Molva, Gene Tsudik, and Dirk Westhoff, editors, *European Workshop on Security and Privacy in Ad hoc and Sensor Networks – ESAS'05*, volume 3813 of *Lecture Notes in Computer Science*, pages 142–152, Visegrad, Hungary, July 2005. Springer-Verlag.

[106] Daesung Kwon, Daewan Han, Jooyoung Lee, and Yongjin Yeom. Vulnerability of an RFID authentication protocol proposed at secubiq 2005. In *International Workshop on Security in Ubiquitous Computing Systems – Secubiq 2006*, Lecture Notes in Computer Science, Seoul, Korea, August 2006. Springer-Verlag.

[107] Jeremy Landt. Shrouds of time: The history of RFID. *An AIM Publication*, 2001. Available online at http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf.

[108] Tri van Le, Mike Burmester, and Breno de Medeiros. Forward-secure RFID authentication and key exchange. Cryptology ePrint Archive, Report 2007/051, 2007.

[109] Cheon-Pyo Lee. *An empirical study of organisational ubiquitious computing technology adoption: the case of Radio Frequency Identification (RFID) in the healthcare industry.* PhD thesis, Mississippi State University, Mississippi State, Mississippi, USA, 2006. Available online at http://sun.library.msstate.edu/ETD-db/theses/submitted/etd-11032006-120137/restricted/Lee.pdf.

[110] Sangshin Lee, Tomoyuki Asano, and Kwangjo Kim. RFID mutual authentication scheme based on synchronized secret information. In *Symposium on Cryptography and Information Security*, Hiroshima, Japan, January 2006.

[111] Su-Mi Lee, Young Ju Hwang, Dong Hoon Lee, and Jong In Lim. Efficient Authentication for Low-Cost RFID Systems. In Osvaldo Gervasi, Marina Gavrilova, Vipin Kumar, Antonio Laganaà, Heow Pueh Lee, Youngsong Mun, David Taniar, and Chih Jeng Kenneth Tan, editors, *International Conference on Computational Science and its Applications - ICCSA 2005, Proceedings, Part I*, volume 3480 of *Lecture Notes in Computer Science*, pages 619–627, Singapore, May 2005. Springer-Verlag.

[112] Yong Ki Lee and Ingrid Verbauwhede. Secure and low-cost RFID authentication protocols. In *International Workshop on Adaptive Wireless Networks – AWiN*, Saint Louis, Missouri, USA, November-December 2005. IEEE.

[113] Mikko Lehtonen, Thorsten Staake, Florian Michahelles, and Elgar Fleisch. From Identification to Authentication - A Review of RFID Product Authentication Techniques. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[114] Mikko Lehtonen, Thorsten Staake, Florian Michahelles, and Elgar Fleisch. Strengthening the security of machine readable documents by combining RFID and optical memory devices. In *Ambient Intelligence Developments Conference – AmI.d*, Sophia-Antipolis, France, September 2006.

[115] Stépahne Lemieux and Adrian Tang. Clone resistant mutual authentication for low-cost RFID technology. Cryptology ePrint Archive, Report 2007/170, 2007.

[116] Tieyan Li and Robert H. Deng. Vulnerability analysis of EMAP - an efficient RFID mutual authentication protocol. In *Second International Conference on Availability, Reliability and Security – AReS 2007*, Vienna, Austria, April 2007.

[117] Tieyan Li and Guilin Wang. Security analysis of two ultra-lightweight RFID authentication protocols. In *IFIP SEC 2007*, Sandton, Gauteng, South Africa, May 2007. IFIP.

[118] Chae Hoon Lim and Tymur Korkishko. mcrypton - a lightweight block cipher for security of low-cost rfid tags and sensors. In *Workshop on Information Security Applications – WISA'05*, Lecture Notes in Computer Science, Jeju Island, Korea, August 2005. Springer-Verlag.

[119] Chae Hoon Lim and Taekyoung Kwon. Strong and robust RFID authentication enabling perfect ownership transfer. In *Conference on Information and Communications Security – ICICS'06*, Lecture Notes in Computer Science, Raleigh, North Carolina, USA, December 2006. Springer-Verlag.

[120] Zhaoyu Liu and Dichao Peng. True random number generator in RFID systems against traceability. In *IEEE Consumer Communications and Networking Conference – CCNS*, volume 1, pages 620–624, Las Vegas, Nevada, USA, January 2006. IEEE, IEEE.

[121] Tobias Lohmann, Mattias Schneider, and Christoph Ruland. Analysis of power constraints for cryptographic algorithms in mid-cost RFID tags. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *International Conference*

on Smart Card Research and Advanced Applications – CARDIS, Lecture Notes in Computer Science, Tarragona, Spain, April 2006. IFIP, Springer-Verlag.

[122] Li Lu, Yunhao Liu, Lei Hu, Jinsong Han, and Lionel Ni. A Dynamic Key-Updating Private Authentication Protocol for RFID Systems. In *International Conference on Pervasive Computing and Communications – PerCom 2007*, pages 13–22, New York, USA, March 2007. IEEE, IEEE Computer Society Press.

[123] Xueming Luo. Trust production and privacy concerns on the internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management, Volume 31*, pages 111 – 118, 2002.

[124] Jing Ma and Jeffrey V. Nickerson. Hands-on, simulated, and remote laboratories: A comparative literature review. *ACM Comput. Surv.*, 38(3):7, 2006.

[125] A. Masters and K. Michael. Humancentric applications of RFID implants: The usability contexts of control, convenience and care. In *The Second IEEE International Workshop on Mobile Commerce and Services (WCMS '05)*, pages 32– 41, Los Alamitos, CA, USA, 2005. IEEE Computer Society.

[126] Vic Matta and Christopher Moberg. The development of a research agenda for RFID adoption and effectiveness in supply chains. *Issues in Information Systems (IIS); Volume VII, No. 2*, pages 246–251, 2006.

[127] Maire McLoone and Matt Robshaw. Public Key Cryptography and RFID Tags. In Masayuki Abe, editor, *The Cryptographers' Track at the RSA Conference – CT-RSA*, Lecture Notes in Computer Science, San Francisco, California, USA, February 2007. Springer-Verlag.

[128] Luke Mirowski and Jacky Hartnett. Deckard: A system to detect clone RFID tags. Manuscript, April 2007.

[129] Charles Møller, Pernille Kræmmergaard, Pall Rikhardsson, Per Møller, Torben N. Jensen, and Lasse Due. A comprehensive ERP bibliog-

raphy 2000-2004 - working paper no. 129. Available Online at http://www.hha.dk/afl/wp/inf/related_wp_I/WP_129.pdf, 2004.

[130] David Molnar, Andrea Soppera, and David Wagner. Privacy for RFID through trusted computing. In *Workshop on Privacy in the Electronic Society – WPES*, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.

[131] David Molnar, Andrea Soppera, and David Wagner. A scalable, delegatable, pseudonym protocol enabling ownership transfer of RFID tags. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.

[132] David Molnar and David Wagner. Privacy and Security in Library RFID: Issues, Practices, and Architectures. In Birgit Pfitzmann and Peng Liu, editors, *Conference on Computer and Communications Security – ACM CCS '04*, pages 210–219, Washington, DC, USA, October 2004. ACM, ACM Press.

[133] Ann Monday and Jamie Rudge. Email Policy Enforcement: Choice or Chance - A Case Study at an Australian Winery. In *Proceedings of the 10th Australasian Conference on Information Systems*, pages 634–644, Wellington, New Zealand, 1999.

[134] Dang Nguyen Duc, Jaemin Park, Hyunrok Lee, and Kwangjo Kim. Enhancing security of epcglobal gen-2 RFID tag against traceability and cloning. In *Symposium on Cryptography and Information Security*, Hiroshima, Japan, January 2006.

[135] Yasunobu Nohara, Sozo Inoue, Kensuke Baba, and Hiroto Yasuura. Quantitative evaluation of unlinkable id matching schemes. In *Workshop on Privacy in the Electronic Society – WPES*, pages 55–60, Alexandria, Virginia, USA, November 2006. ACM, ACM Press.

[136] Karsten Nohl and David Evans. Quantifying information leakage in tree-based hash protocols. Technical Report UVA-CS-2006-20, University of Virginia, Department of Computer Science, Charlottesville, Virginia, USA, 2006.

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

[138] Tatsuaki Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In *CRYPTO '92: Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology*, pages 31–53, London, UK, 1993. Springer-Verlag.

[139] Jeong Su Park, Su Mi Lee, Eun Young Choi, and Dong Hoon Lee. Self reencryption protocol providing strong privacy for low cost RFID system. In Marina L. Gavrilova, Osvaldo Gervasi, Vipin Kumar, Chih Jeng Kenneth Tan, David Taniar, Antonio Laganà, Youngsong Mun, and Hyunseung Choo, editors, *International Conference on Computational Science and its Applications - ICCSA 2006*, volume 3983 of *Lecture Notes in Computer Science*, pages 316–325, Glasgow, Scotland, May 2006. Springer-Verlag.

[140] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan Estevez-Tapiador, and Arturo Ribagorda. LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[141] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan Estevez-Tapiador, and Arturo Ribagorda. M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags. In *International Conference on Ubiquitous Intelligence and Computing – UIC06*, volume 4159 of *Lecture Notes in Computer Science*, pages 912–923. Springer-Verlag, September 2006.

[142] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan Estevez-Tapiador, and Arturo Ribagorda. RFID systems: A survey on security threats and proposed solutions. In *11th IFIP International Conference on Personal Wireless Communications – PWC06*, volume 4217 of *Lecture Notes in Computer Science*, pages 159–170. Springer-Verlag, September 2006.

[143] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. EMAP: An efficient mutual authentication protocol for low-cost RFID tags. In *OTM Federated Conferences and Workshop: IS Workshop – IS'06*, volume 4277 of *Lecture Notes in Computer Science*, pages 352–361. Springer-Verlag, November 2006.

[144] Selwyn Piramuthu. HB and related lightweight authentication protocols for secure RFID tag/reader authentication. In *Collaborative Electronic Commerce Technology and Research – CollECTeR 2006*, Basel, Switzerland, June 2006.

[145] Selwyn Piramuthu. On existence proofs for multiple RFID tags. In *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU 2006*, Lyon, France, June 2006. IEEE, IEEE Computer Society Press.

[146] Axel Poschmann, Gregor Leander, Kai Schramm, and Christof Paar. A family of light-weight block ciphers based on DES suited for RFID applications. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[147] 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.

[148] Damith Ranasinghe, Daniel Engels, and Peter Cole. Security and Privacy: Modest Proposals for Low-Cost RFID Systems. In *Auto-ID Labs Research Workshop*, Zurich, Switzerland, September 2004.

[149] Pauline Ratnasingham and Paul A. Swatman. Security in the EDI context. In *First Pacific-Asia Workshop in Electronic Commerce (PAWEC)*, 1997.

[150] Jason Reid, Juan Gonzalez Neito, Tee Tang, and Bouchra Senadji. Detecting relay attacks with timing based protocols. QUT ePrint, Report 3264, 2006.

[151] Keunwoo Rhee, Jin Kwak, Seungjoo Kim, and Dongho Won. Challenge-Response based RFID Authentication Protocol for Distributed Database Environment. In

Dieter Hutter and Markus Ullmann, editors, *International Conference on Security in Pervasive Computing – SPC 2005*, volume 3450 of *Lecture Notes in Computer Science*, pages 70–84, Boppard, Germany, April 2005. Springer-Verlag.

[152] Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags. In *International Workshop on Security Protocols – IWSP'05*, Lecture Notes in Computer Science, Cambridge, England, April 2005. Springer-Verlag.

[153] Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. Uniting legislation with RFID privacy-enhancing technologies. In *Security and Protection of Information*, Brno, Czech Republic, May 2005.

[154] Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. The evolution of RFID security. *IEEE Pervasive Computing*, 5(1):62–69, January–March 2006.

[155] Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. Is your cat infected with a computer virus? In *Pervasive Computing and Communications*, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press.

[156] Melanie Rieback, Georgi Gaydadjiev, Bruno Crispo, Rutger Hofman, and Andrew Tanenbaum. A Platform for RFID Security and Privacy Administration. In *USENIX/SAGE Large Installation System Administration conference – LISA'06*, pages 89–102, Washington DC, USA, December 2006. http://www.rfidguardian.org/papers/lisa.06.pdf.

[157] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. In Colin Boyd and Juan Manuel González Nieto, editors, *10th Australasian Conference on Information Security and Privacy – ACISP'05*, volume 3574 of *Lecture Notes in Computer Science*, pages 184–194, Brisbane, Australia, July 2005. Springer-Verlag. http://www.rfidguardian.org/papers/acisp.05.pdf.

[158] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. Is your cat infected with a computer virus? In *PERCOM '06: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, pages 169–179, Washington, DC, USA, 2006. IEEE Computer Society.

[159] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. RFID malware: Truth vs. myth. *IEEE Security and Privacy*, 4(4):70–72, 2006.

[160] Bernhard Riedl, Gernot Goluch, Stefan Pöchlinger, and Edgar Weippl. A Comparative Literature Review on RFID Security and Privacy. In *9th International Conference on Information Integration and Web-based Applications Services (iiWAS2007)*, to appear.

[161] George Roussos. Enabling RFID in Retail. *Computer*, 39(3):25–30, 2006.

[162] George Roussos and Theano Moussouri. Consumer perceptions of privacy, security and trust in ubiquitous commerce. *Personal Ubiquitous Comput.*, pages 416–429, 2004.

[163] Junichiro Saito, Jae-Cheol Ryou, and Kouichi Sakurai. Enhancing Privacy of Universal Re-encryption Scheme for RFID Tags. In Laurence Jang, Minyi Guo, Guang Gao, and Niraj Jha, editors, *Embedded and Ubiquitous Computing – EUC 2004*, volume 3207 of *Lecture Notes in Computer Science*, pages 879–890, Aizu-Wakamatsu City, Japan, August 2004. Springer-Verlag.

[164] Junichiro Saito and Kouichi Sakurai. Grouping Proof for RFID Tags. In *Conference on Advanced Information Networking and Applications – AINA*, volume 2, pages 621–624, Taiwan, March 2005. IEEE.

[165] Kazuo Sakiyama, Lejla Batina, Nele Mentens, Bart Preneel, and Ingrid Verbauwhede. Small-footprint ALU for public-key processors for pervasive security. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[166] Sanjay Sarma, Stephen Weis, and Daniel Engels. RFID Systems and Security and Privacy implications. In Burton Kaliski, Çetin Kaya ço, and Christof Paar,

editors, *Cryptographic Hardware and Embedded Systems – CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 454–469, Redwood Shores, CA, USA, August 2002. Springer-Verlag.

[167] Sanjay Sarma, Stephen Weis, and Daniel Engels. Radio-frequency identification: security risks and challenges. *Cryptobytes, RSA Laboratories*, 6(1):2–9, Spring 2003.

[168] Claus P. Schnorr. Efficient identification and signatures for smart cards. In *CRYPTO '89: Proceedings on Advances in cryptology*, pages 239–252, New York, NY, USA, 1989. Springer-Verlag New York, Inc.

[169] Youngjoon Seo and Kwangjo Kim. Scalable and untraceable authentication protocol for RFID. In *International Workshop on Security in Ubiquitous Computing Systems – Secubiq 2006*, Lecture Notes in Computer Science, Seoul, Korea, August 2006. Springer-Verlag.

[170] Victoria Skoularidou and Diomidis Spinellis. Security architectures for network clients. *Information Management & Computer Security; Volume 11 Number 2*, pages 84–91, 2003.

[171] Agusti Solanas, Josep Domingo-Ferrer, Antoni Martínez-Ballesté, and Vanesa Daza. A Distributed Architecture for Scalable Private RFID Tag Identification. *Computer Networks, Elsevier*, 51(9), January 2007.

[172] Sarah Spiekermann. Perceived control: Scales for privacy in ubiquitous computing environments. In *Conference on User Modeling – UM'05*, Edinburgh, Scotland, July 2005.

[173] Sarah Spiekermann and Oliver Berthold. Maintaining privacy in RFID enabled environments – proposal for a disable-model. In *Workshop on Security and Privacy, Conference on Pervasive Computing*, Vienna, Austria, April 2004.

[174] Thorsten Staake, Frédéric Thiesse, and Elgar Fleisch. Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting. In Hisham Haddad, Lorie

Liebrock, Andrea Omicini, and Roger Wainwright, editors, *Symposium on Applied Computing – SAC*, pages 1607–1612, Santa Fe, New Mexico, USA, March 2005. ACM, ACM Press.

[175] Ross Stapleton-Gray. Would Macy´s Scan Gimbels? Competitive Intelligence and RFID. In *RFID: Applications, Security, and Privacy*, pages 283–290. Addison-Wesley, 2003.

[176] Harry Stockman. Communication by means of reflected power. In *Proceedings of the IRE (Institute of Radio Engineers)*, pages 1196–1204, Los Alamitos, CA, USA, 1948. IEEE Computer Society.

[177] Chiu C. Tan, Bo Sheng, and Qun Li. Serverless Search and Authentication Protocols for RFID. In *International Conference on Pervasive Computing and Communications – PerCom 2007*, pages 3–12, New York, USA, March 2007. IEEE, IEEE Computer Society Press.

[178] C. Tetther and L. Ferreira. The evaluation of e-business related technologies in the railway industry. In *In Proceedings The 27th Australian Transport Research Forum*, Adelaide, Australia, 2004.

[179] Frank Thornton, Brad Haines, Anand M. Das, Hersh Bhargava, and Anita Campbell. *RFID Security.* Syngress Publishing, Inc., Rockland, MA, USA, 2006.

[180] Gene Tsudik. YA-TRAP: Yet another trivial RFID authentication protocol. In *International Conference on Pervasive Computing and Communications – PerCom 2006*, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press.

[181] Pim Tuyls and Lejla Batina. Rfid-tags for anti-counterfeiting. In David Pointcheval, editor, *Topics in Cryptology - CT-RSA 2006, The Cryptographers' Track at the RSA Conference 2006*, Lecture Notes in Computer Science, San Jose, California, USA, February 2006. Springer-Verlag.

[182] István Vajda and Levente Buttyán. Lightweight Authentication Protocols for Low-Cost RFID Tags. In *Second Workshop on Security in Ubiquitous Computing – Ubicomp 2003*, Seattle, WA, USA, October 2003.

[183] Serge Vaudenay. RFID Privacy Based on Public-Key Cryptography (Abstract). In Min Surp Rhee and Byoungcheon Lee, editors, *Information Security and Cryptology – ICISC 2006*, volume 4296 of *Lecture Notes in Computer Science*, pages 1–6, Busan, Korea, November-December 2006. Springer-Verlag.

[184] Vassilios S. Verykios, Elisa Bertino, Igor Nai Fovino, Loredana Parasiliti Provenza, Yucel Saygin, and Yannis Theodoridis. State-of-the-art in privacy preserving data mining. *SIGMOD Rec., Volume 33, Number 1*, pages 50–57, 2004.

[185] V. P. Vinding. Interrogator-responder identification system, 1969. Patent found at http://www.google.at/patents?hl=de&lr=&vid=USPAT3440633&id=GT1WAAAAEBAJ&oi=fnd&dq=%22Interrogator-responder+identification+system.

[186] Stephen Weis. Security Parallels Between People and Pervasive Devices. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2005*, pages 105–109, Kauai Island, Hawaii, USA, March 2005. IEEE, IEEE Computer Society Press.

[187] 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.

[188] Marc Weiser. The computer for the 21st century. *Scientific American Volume 265, Number 3*, pages 94–104, 1991.

[189] Johannes Wolkerstorfer. Is elliptic-curve cryptography suitable to secure RFID

tags? Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.

[190] Kirk Wong, Patrick Hui, and Allan Chan. Cryptography and authentication on RFID passive tags for apparel products. *Computers in Industry*, May 2006.

[191] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, and Kwangjo Kim. Mutual authentication protocol for low-cost RFID. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.

[192] Sang-Soo Yeo and Sung-Kwon Kim. Scalable and flexible privacy protection scheme for RFID systems. In Refik Molva, Gene Tsudik, and Dirk Westhoff, editors, *European Workshop on Security and Privacy in Ad hoc and Sensor Networks – ESAS'05*, volume 3813 of *Lecture Notes in Computer Science*, pages 153–163, Visegrad, Hungary, July 2005. Springer-Verlag.

[193] Pengyuan Yu, Patrick Schaumont, and Dong Ha. Securing RFID with Ultra-wideband Modulation. Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[194] Tyler T. Yu, Miranda M. Zhang, Lloyd Southern, and Carl Joiner. E-commerce safety and security: a statistical analysis of consumers' attidues. *Issues in Information Systems (IIS); Volume II*, pages 494–500, 2001.

[195] Jia Zhai, Chang Mok-Park, and Gi-Nam Wang. Hash-based RFID security protocol using randomly key-changed identification procedure. In Marina L. Gavrilova, Osvaldo Gervasi, Vipin Kumar, Chih Jeng Kenneth Tan, David Taniar, Antonio Laganà, Youngsong Mun, and Hyunseung Choo, editors, *International Conference on Computational Science and its Applications - ICCSA 2006*, volume 3983 of *Lecture Notes in Computer Science*, pages 296–305, Glasgow, Scotland, May 2006. Springer-Verlag.

[196] Xiaolan Zhang and Brian King. Integrity improvements to an RFID privacy protection protocol for anti-counterfeiting. In Jianying Zhou, Javier Lopez, Robert

Deng, and Feng Bao, editors, *Information Security Conference – ISC 2005*, volume 3650 of *Lecture Notes in Computer Science*, pages 474–481, Singapore, September 2005. Springer-Verlag.

[197] Xiaolan Zhang and Brian King. Modeling RFID security. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, *Conference on Information Security and Cryptology – CISC 2005*, volume 3822 of *Lecture Notes in Computer Science*, pages 75–90, Beijing, China, December 2005. Springer-Verlag.