

RFID-AP

DWP1.2

RFID Security: State of the Art

CEA-LETI (F. Vacherand, O. Savry)
 Eurecom (R. Molva, E. Blass)
 INRIA (M. Soos, C. Castelluccia)
 Orange Labs (M. Robshaw, Olivier Billet, Jonathan Etrog, Iwen Coisel)

First deliverable for RFID-AP (ANR SESUR)

Date: 30.01.2009	Version: 1.0	DCIS/SASTI/ 09-014
-------------------------	---------------------	--------------------

RFID-AP	30/01/2009	1.0	2/44
Project	Date	Version	page

Table of contents

1 INTRODUCTION5

2 RFID SYSTEM COMPONENTS.....7

 2.1 TAGS, READERS, AND DATABASES 7

 2.1.1 *Tags* 8

 2.1.2 *Readers*..... 9

 2.1.3 *Databases* 9

 2.2 RFID PRINCIPLES 10

 2.2.1 *Powering a Tag*..... 10

 2.2.2 *Communicating with a Tag*..... 10

 2.2.3 *Tag Functionality*..... 13

 2.2.4 *Examples of EPC tags* 16

3 SECURITY THREATS.....21

 3.1 PHYSICAL LAYER ATTACKS..... 21

 3.1.1 *Eavesdropping* 21

 3.1.2 *Skimming*..... 22

 3.1.3 *Denial of service*..... 22

 3.1.4 *Side channel attacks on the contactless interface*..... 25

 3.2 COMMUNICATION LAYER ATTACKS..... 25

 3.2.1 *Relay Attack* 25

 3.2.2 *Man-in-the-middle attack*..... 26

 3.3 HIGHER LAYER ATTACKS..... 26

4 FORMALISED SECURITY REQUIREMENTS.....28

 4.1 SECURITY NOTIONS AND GOALS IN RFID SYSTEMS..... 28

 4.1.1 *Identification* 28

 4.1.2 *Authentication*..... 28

 4.1.3 *Untraceability*..... 29

 4.1.4 *Unlinkability* 29

 4.1.5 *Anonymity*..... 29

 4.1.6 *Forward-secrecy* 29

5 CURRENT SECURITY SOLUTIONS 30

 5.1 PHYSICAL LAYER SOLUTIONS 30

 5.1.1 *The “Kill” Tag Approach* 30

 5.1.2 *The Faraday Cage* 30

 5.1.3 *Active Jamming*..... 30

 5.1.4 *Noisy Tags* 31

 5.1.5 *The Blocker Tag*..... 31

RFID-AP	30/01/2009	1.0	3/44
Project	Date	Version	page

5.1.6	<i>The RFID Guardian</i>	31
5.1.7	<i>Distance bounding protocol</i>	31
5.2	CRYPTOGRAPHIC SOLUTIONS.....	32
5.2.1	<i>Symmetric Cryptography</i>	34
5.2.2	<i>Asymmetric Cryptography</i>	37
5.3	PRIVACY-PRESERVING AUTHENTICATION PROTOCOLS.....	38
5.3.1	<i>YA-TRAP</i>	39
5.3.2	<i>Hash Locks</i>	39
5.3.3	<i>Tree-based shared Keys</i>	39
5.3.4	<i>HB</i>	39
5.3.5	<i>DPM</i>	39
6	CONCLUSIONS	41
7	REFERENCES	42

RFID-AP	30/01/2009	1.0	4/44
Project	Date	Version	page

1 Introduction

Today *Radio-Frequency-Identification* (RFID) is used for a variety of applications, ranging from simple library borrowing systems, building access-control, through to complete supply-chain management solutions. In many applications there are clear advantages in having an RFID-enabled solution, with such advantages being measured in terms of convenience and cost.

In *supply-chain management* large quantities of goods can be individually equipped with tags so as to monitor and track their movement. This gives the advantage of easily detecting losses during shipment and also, since tags are scanned during checkout, can allow stores to manage their stocks and shelf displays leading to savings which can be passed on to the consumer.

Access control allows certain areas to be controlled so that only those authorized people carrying appropriate tags can enter a given areas. Instead of keys employees receive RFID-tags and instead of classical door locks, doors are equipped with RFID-readers connected to databases. The doors only open if a legitimate tag is wiped next to the reader. This application of RFID-tags has many advantages in terms of cost and dynamic management since tags can easily be issued to open multiple doors and can also be electronically revoked without the need to change the door lock.

Public-transport ticketing, where paper-tickets are replaced by electronic-tickets, is now commonplace in many cities around the world. While the tags in this case are often more powerful contactless smart cards (this is a spectrum of devices that is quite difficult to classify) this kind of application helps to motivate some of the security and privacy issues that are typical in most RFID-based applications. For instance, every time a passenger enters or leaves a metro, they pass readers that identify their tags and this gives the passenger access to certain services that can have a substantial monetary value. From a security perspective, the issues of RFID-tags need to ensure that they will function correctly to avoid customer fraud such as the (re-)charging of tags. From a privacy perspective, it is not necessarily a pleasant thought for the user to know that their movements through the system could be tracked and collated. This would be worse if it could be done by a third party with equipment that eavesdrops on the wireless communication between tags and readers.

As RFID-systems are entering our daily life and becoming more ubiquitous, their security and our privacy gain importance. Indeed, the concepts of authentication and privacy are relevant to both suppliers and consumers and it can be claimed that industrial RFID deployment can only be successful if all participating parties are convinced that the deployed system respects their respective demands for authentication and privacy.

RFID-enabled applications are generally split into two different domains:

- Systems that are dedicated to persons that use contactless smartcards with the well-known size of a credit card. They can be found of course in banking system but also in secured access applications, in transportation, in public health systems or with new generation passports.
- Systems that are dedicated to objects that allow their traceability: these devices are then named "RFID tags". Since there are many objects to track, this necessarily implies that the tags should be ultra-low-cost devices.

RFID-AP	30/01/2009	1.0	5/44
Project	Date	Version	page

While much of what we discuss in RFID-AP applies to both application fields, our focus will typically be on the second class of ultra-low-cost devices. And the main goal of the project will be to propose and prototype cryptographic algorithms and secure protocols that might be used for RFID deployment. These algorithms and protocols may be used individually or in combination, and we anticipate that they will potentially contribute to the authentication and/or privacy that might be needed in an RFID-enabled system. One particular feature of our research in the RFID-AP project is that contributions must be practical. Many academic proposals can be deeply flawed in practice since too little attention has been paid to the realities of implementation and deployment. This project will therefore be notable for the way theoretical work will be closely intertwined with the task of development and deployment.

In this first document of RFID-AP, however, we give an introduction to RFID-systems and their applications. In particular we focus on some current industrial solutions as exemplified by EPCglobal. We will also give an overview of the current state of the art of RFID-security and privacy, and we will also highlight some current research results on the possible threats and attacks on RFID-systems as well as some solutions.

After this introduction we will, in Section 2, introduce the essential components of an RFID-system. We present some of the basic physical properties of basic RFID tags as well as details of the low-level communication between tags and readers and the low-level services that tags can offer. In Section 3, we consider the range of potential security threats typical to RFID-systems, from simple attacks such as eavesdropping on a wireless communication through to more sophisticated counterfeiting attacks. As a common theme to these attacks, we see that two fundamental security requirements - authentication and privacy - are frequently prominent. Section 4 introduces some attempts at a more formal approach to understanding different security demands, while Section 5 consider some current (often partial) solutions that might be available to help protect the authentication and privacy of devices and/or communications in an RFID-enabled application.

RFID-AP	30/01/2009	1.0	6/44
Project	Date	Version	page

2 RFID System Components

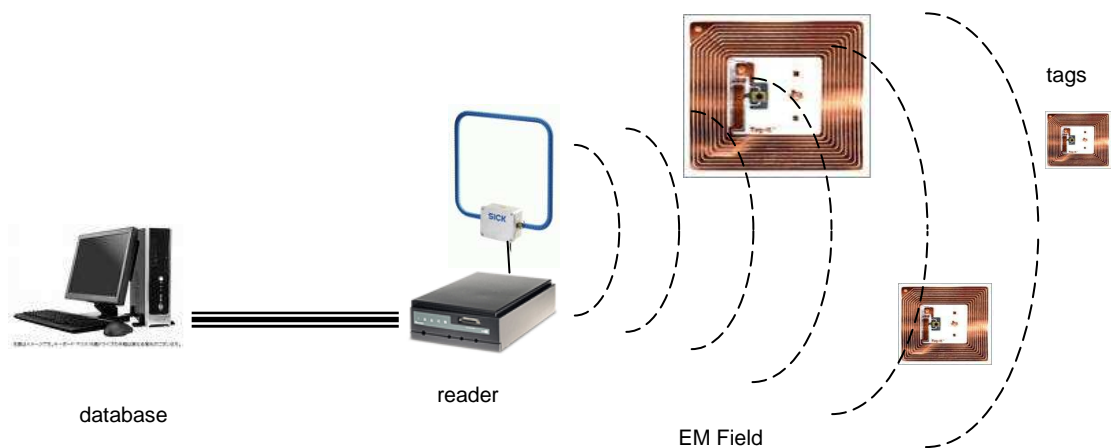
To understand the background to this report, and to the RFID-AP project in general, it is important to describe the basic fundamentals of an RFID-based system. This will include descriptions of how tags are powered, how they communicate, and what they do.

To start we need to describe the essential components.

2.1 Tags, Readers, and Databases

There is a vast range of RFID-enabled systems that can differ in many ways. However, despite the fact each system is highly tailored to its application and environment, there are several features that are common to all systems.

Put simply, an RFID-system consists of *tags*, *readers* and *backend-databases*. Reality can be much more complex [GB06] and in a more nuanced world there can be additional components as well as the “*enterprise application*” that oversees the entire deployment. However, the essential security issues encountered in RFID-enabled applications can be illustrated by a very simple and general security application that consists of a single database, one reader and some tags. Thus for the sake of clarity, within RFID-AP we will typically be concerned with the case of a *single reader* connected to a *single database* and being used in a population of *many tags*. This basic RFID system is illustrated below.



RFID-AP	30/01/2009	1.0	7/44
Project	Date	Version	page

2.1.1 Tags

There are different understandings of the term RFID-“tags” which range from tiny chips that can be swallowed or implanted into a human body through to smart-cards containing micro-controllers.

In RFID-AP we assume a “tag” to be physically small device, e.g. less than a square-centimetre, consisting of at most a very primitive processing unit and a radio interface. The tags of interest to us are passive; they do not have an autonomous power source such as a battery. Instead tags are powered by the electromagnetic field of the reader. As long as the tag is inside the reader’s electromagnetic-field, it can do (some rudimentary) processing and communication.

A tag is often read-only in the sense that its executable program or algorithm once stored on it cannot be overwritten after manufacturing of the tag. It might, however, be the case that tags have, besides volatile memory, also a non-volatile kind of memory available which can be repeatedly changed from the tag and “survives” power-losses. The benefits of such a feature for authenticity and privacy will be studied within the project.

A tag can have access to some source of “true randomness”. This might either be a random seed that is issued during a tag’s manufacturing and which’s state is updated using the above-mentioned non-volatile memory, or there might be random noise available from, e.g., the radio interface.

The physical size of a tag is the main criteria of its possible capabilities. The larger a tag and the more money are available, the more logic gates, or “gate equivalents”, can be stored on it. Both, storing data and executable algorithms on a tag require gate equivalents. The exact capabilities of a given tag for a given cost is open to considerable debate, and it is something that is considered later in this report, see Section 5, with particular reference to the use of cryptography on RFID tags and the deployment of protocols for authentication and identification.

Typically, simple tags are “stateless”. As soon as such a tag leaves the reader’s electro-magnetic field, all state information on the tag is erased. It is however possible, implying higher production costs, to implement “non-volatile”, electrical erasable memory on the tag. As a result, subsequent identification instances between tag and reader can generally depend on previous ones. In RFID-AP, we want to analyze potential benefits, e.g., in terms of additional security, privacy or performance of tag authentication with “stateful” tags compared to today’s stateless tags.

As soon as a tag is in a reader’s wireless communication range, the reader tries to identify the tag using information from the database. Typically, a palette passes next to or a human wipes his tag/passport close a reader. The reader now sends some information to the tag to initiate the process of identification. The tag replies to the transmission with some data that is used by the reader, together with the database, to identify the tag.

RFID-AP	30/01/2009	1.0	8/44
Project	Date	Version	page

2.1.2 Readers

A reader is an electronic device, wirelessly and constantly *scanning* its environment for tags.

Similar to tags, readers will differ depending on their application, environment, and requirements. Readers might be small, electronic devices attached to a laptop- or desktop-size computer with the only purpose of carrying out the wireless communication to the tag. All further processing, e.g. together with the database, is done on the computer. This setup might be used in applications or scenarios where many objects on a palette are passing the checkout at a supermarket.

In other scenarios readers might be small, embedded computers, featuring only a microcontroller, some communication facility and some memory to store the database in it. This might be realistic for access control, where a reader is placed next to a door only opening if and only if a legitimate tag is in communication range. Another setup, e.g. if there are multiple readers, would be to use small, embedded readers that are connected to a network. Readers can access this network to give to and retrieve data from a central database. This setup might be used in the public transport systems.

So depending on the setup, readers will not only realize the communication with the tag to receive information for identification, but readers might also be involved in the process of the actual identification of tags. In RFID-AP, we assume readers to small, embedded electronic devices with resource restrictions. While they will typically be more powerful than tags, we assume the existence of only one reader with a “built-in” database. The implications of multiple, connected, and networking readers sharing one database or different parts of a database will also be studied during the project, but secure and private identification protocols for RFID-systems are likely to become more complex as a result.

To understand properly the features of an RFID system, the physical layer of the EPC standard will be detailed. This standard is now well deployed in the UHF radio band, but a HF standard is being finalized which is of particular interest because of the improved propagation properties through liquids. To simplify the development of the tags and readers, however, manufacturers have chosen the same fundamental mechanisms for communication in both UHF and HF.

2.1.3 Databases

For our purposes in RFID-AP the database will often consist simply of the list of all known tag IDs plus some additional information. This additional information can sometimes be a cryptographic key which allows for some more sophisticated applications to be developed. Typically such databases contain a couple of thousands, potentially hundreds of thousands of entries. However, much of what we cover in RFID-AP is somewhat orthogonal to the exact form and deployment of the database.

RFID-AP	30/01/2009	1.0	9/44
Project	Date	Version	page

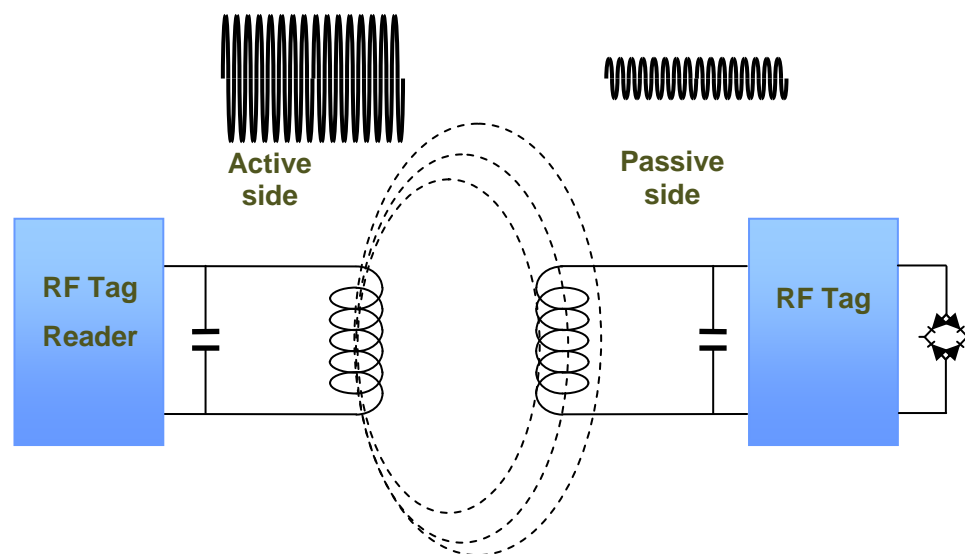
2.2 RFID principles

In an RFID system a tag cannot power itself. So, when a tag is close to a reader, we need to support three basic functions: powering the tag by the reader, transferring data between the reader and the tag (in both directions), and providing some limited functionality to the tag.

2.2.1 Powering a Tag

To supply power to a tag, the reader-tag system can be seen as a *transformer* with the antenna coil of the reader acting as the primary and the antenna coil of the tag acting as the secondary.

However, in contrast to a classical transformer, the transfer of the magnetic flux is not ensured by some ferrite core but rather by the air itself. The consequence is that the strength of the coupling is not so high, but it is sufficiently powerful to power a tag in what is termed the *near field* when a sinusoidal current is injected in the primary coil. A sinusoidal voltage is induced in the tag, and this can be rectified with an onboard rectifier to provide power to the on-tag chip. The sinusoidal wave, termed the *carrier*, can also be used by the tag to generate a clock and this helps to synchronize the answers of the tag as well as its logical circuit.

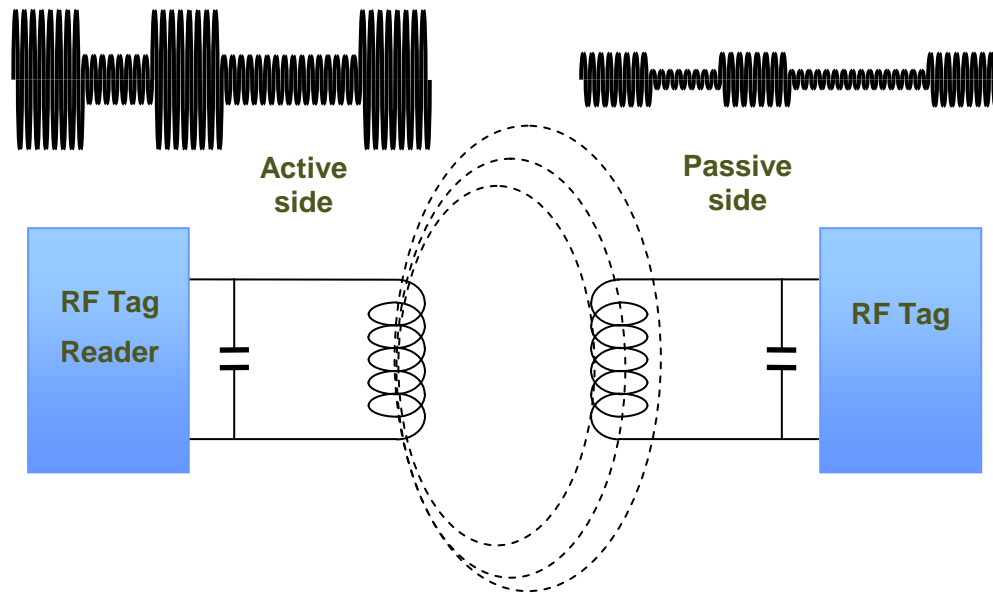


2.2.2 Communicating with a Tag

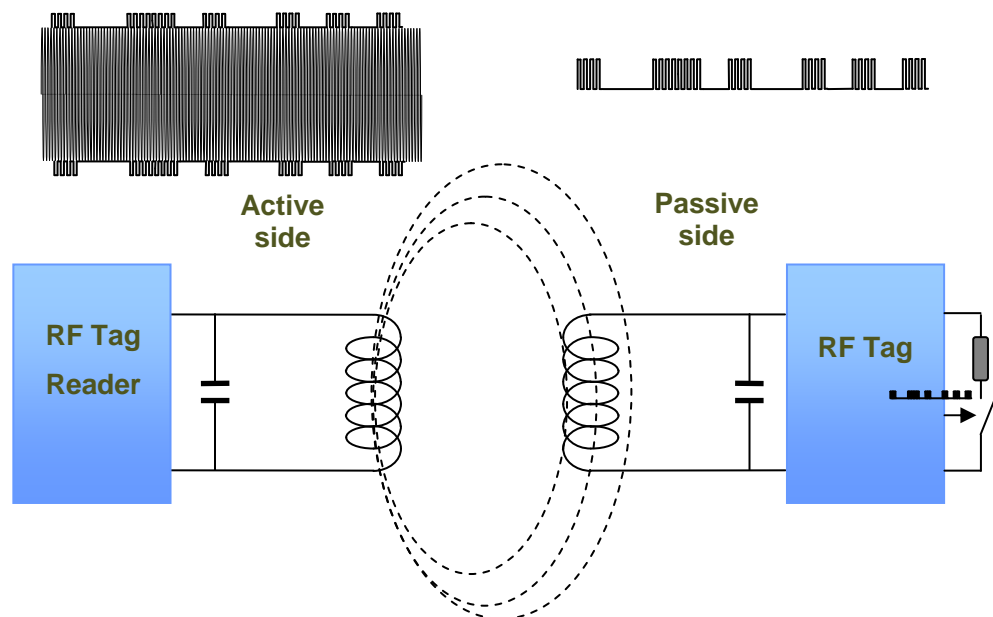
It should be immediately clear, but once we have a current being generated by the reader that induces some current in the tag, then we essentially have a means of communication between the reader and the tag.

RFID-AP	30/01/2009	1.0	10/44
Project	Date	Version	page

Indeed, data transfer from the reader to the tag is carried out by *modulating* the sinusoidal wave, what we termed the carrier, and this modulation is a direct function of the binary message we wish to transmit. While there are different ways of doing this, the basic principle remains the same.

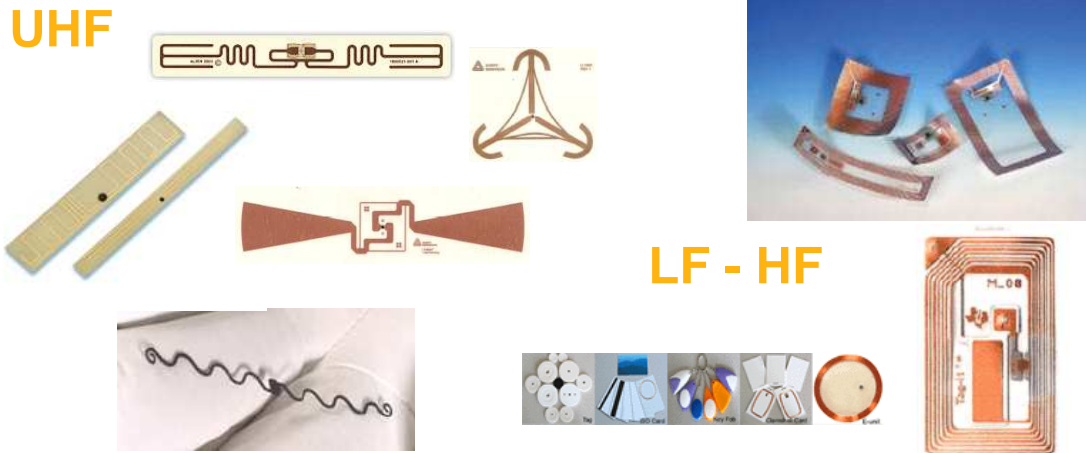


Passing data from the tag to the reader is a little harder. Since the ensemble of the reader and the tag can be viewed as a transformer, the RFID system can take advantage of the following fact. If we change the *impedance* of the secondary coil, that is the tag, then we will also see an impedance variation at the primary coil (the reader). As a consequence, to transfer data the tag modulates the load at the terminals of its antenna, and it does this as a function of the binary message it wishes to transmit. The reader is able to detect an impedance change at the terminals of its antenna and can then demodulate the message. To detect this modulation more easily, the tag uses a *sub-carrier* and a different set of bit-encodings to the reader-tag direction.



RFID-AP	30/01/2009	1.0	11/44
Project	Date	Version	page

From the description given above, it should be clear that fundamental performance of an RFID system will depend on the antennas that are used in the tag and the reader. The tag antenna for a UHF system is often a *bipolar wire* while it is a coil for LF and HF applications that is printed on a plastic substrate.



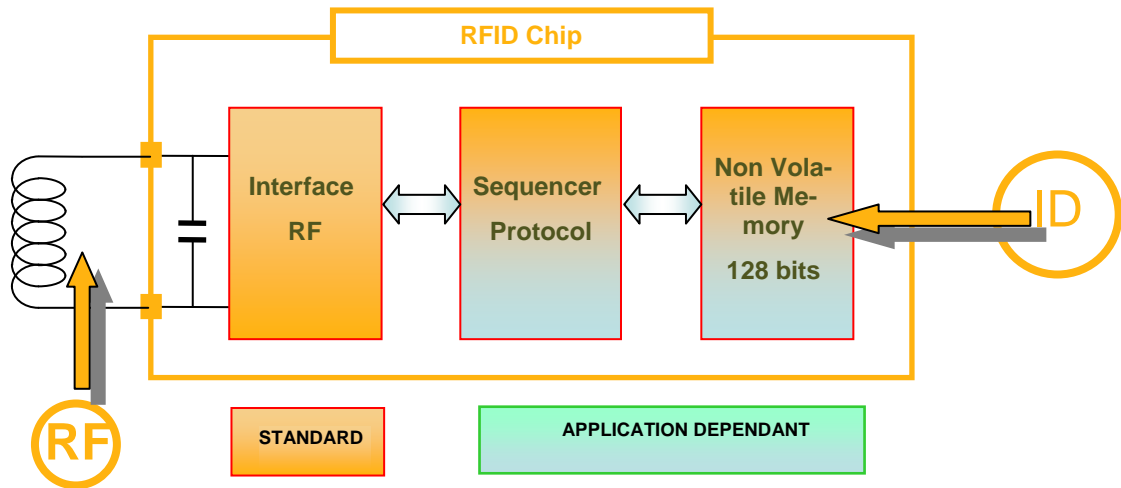
The reader and especially the reader antenna can also take a wide variety of forms.



An RFID tag should be low cost and as a consequence it will have a low number of logical gates. This is something that will be explored later in this document and also in the project, but around 2000 to 3000 logical gates is a typical number at the very low end of the tag eco-system. The tag itself will be composed of several components such as an RF front-end, a logical sequencer that implements the

RFID-AP	30/01/2009	1.0	12/44
Project	Date	Version	page

protocol of the RFID standards and, typically, non-volatile memory with space for a minimum of 128 bits which enables it to store a unique identifier for the tag. More expensive tags will boast more features and greater functionality, though at a cost.



2.2.3 Tag Functionality

RFID tags can be manufactured to have a wide-range of specifications. Our interest naturally lies with the most basic, but a range of functionalities have been proposed. This can be illustrated by the taxonomy provided by EPCglobal where EPC tags are classified into different classes according to the amount of memory they have, their READ/WRITE capability, and their power supply (passive or battery assisted).

- Class 0: Passive tags that are programmed at manufacture and have no dynamic functionality.
- Class 1: Passive tags with very limited memory that can be programmed once after manufacture, and no dynamic functionality.
- Class 2: Passive tags that have extended memory, some dynamic features, and a read/write functionality.
- Class 3: Semi-passive tags that might have some battery-assistance, read/write functionality and a greater range, perhaps up to 30m.
- Class 4: Semi-passive tags with an enhanced range, for instance up to 100m.

However, work on Class 2 tags is only just beginning, and additional functionality beyond that is some way in the future. That said there are semi-passive and even so-called active tags in use today; however they are far more expensive than the simple passive tags that we consider in RFID-AP and we consider them out of our scope.

RFID-AP	30/01/2009	1.0	13/44
Project	Date	Version	page

While our focus is on tags, it should be observed that EPCglobal in fact produces standard specifications for the entirety – or more accurately for the interfaces – of the components in an RFID application. This includes specifying the interface between readers and the controlling software, specifying how an application can formulate query commands for a reader to interrogate a tag, and ways in which information on the tag can be incorporated with business information at the database level.

The details of the communication and encoding mechanism in EPCglobal – while following the top-level scheme outlined above – is too complex to consider in this document. It will however be vital for our future work, particularly in the construction of the prototypes and the test-bed which will be based around EPCglobal. We therefore summarise some of the vital aspects of the tag functionality, and instead refer the reader to either the EPCglobal standards [EPC], to the Annex where extracts from the EPCglobal specifications are presented, or to work later in the project for more detailed issues.

Regarding the functionality of the tag itself, newer tags have extended capabilities as is evidenced by the available memory, which is illustrated below. There are several different types of memory:

- **Reserved memory:** This is used for storing passwords for access to other parts of the memory or to kill a tag.

- **EPC memory:** This is used to store the EPC code which identifies the tag (and hence the item). This memory is locked.

- **TID memory:** This is used to store information that identifies the tag and its functionality.

- **User memory:** This is optional, but increasingly users are seeking tags that have some additional functionality, often so that information about the tag and the products can be added as the item makes its way through the supply chain.

The amounts of different types of memory on a tag will be a function of the cost of the tag, the cost of deployment and the application advantages that such additional memory will provide.

The EPC standard implements a restricted number of mandatory commands. These are in fact sufficient for the basic functionality of an RFID-enabled application as is found in the supply chain. One of the goals of RFID-AP, however, is to see what security features can be implemented using this basic set of commands. Then, on the assumption that more commands would be needed for a security solution, what is the minimum set of additional commands, or extended functionality, that would be required to achieve our security goal.

The set of existing operations available can be listed as follows:

- **Select:** This command is used by the reader to select a subset of the tag population.

RFID-AP	30/01/2009	1.0	14/44
Project	Date	Version	page

- **Inventory:** These commands are used to establish communications between different tags and the reader. The process by which this is done is somewhat more complicated than is needed for this survey report. However this process can be seen as the core of the EPCglobal process – without inventory nothing is possible – and this will feature prominently in later work in the RFID-AP project and in the design of the demonstrator and test-bed.

- **Access:** This is a set of operations or commands that allow the reader to functionally interact with a tag. For EPCglobal the commands consist of :
 - **Req_RN:** Request the tag to return a 16-bit random number
 - **Read:** Reading the memory on the tag.
 - **Write:** Writing to the memory on the tag.
 - **Kill:** Permanently disable the tag.
 - **Lock:** Lock the memory.

With this set of commands and specifications, the entirety of the EPCglobal system can be launched. One of the goals of RFID-AP is to see how many of the different security features that we might like to see within an RFID-enabled system can be integrated into EPCglobal with as few changes or additions to the protocol as possible.

RFID-AP	30/01/2009	1.0	15/44
Project	Date	Version	page

2.2.4 Examples of EPC tags

The market for tags supporting EPCglobal is now reasonably-well developed. We illustrate this by replicating some public product specifications for a variety of tags. More information can be found at the web-sites referenced.

Philips Semiconductors Product Specification Revision 3.0 2004 January 30

I-CODE UID

SL2 ICS11

1 FEATURES

Integrated Circuit for Contactless Radio Frequency Identification Smart Label
 Integrated resonance capacitor of 23.5 pF with $\pm 5\%$ tolerance over full production.

1.1 I-CODE UID RF Interface Features

- Contactless transmission of data and supply energy (no battery needed)
- Operating distance: up to 1.5 m (depending on antenna geometry)
- Operating frequency: 13.56 MHz (ISM, world-wide licence free available)
- Modulation Read/Write Device \rightarrow Label: 10 % ASK
- Fast data transfer: up to 53 kbit/s
- High data integrity: 16-bit CRC, framing
- Anticollision with high identification speed (approx. 200 I-CODE UID smart labels per second)
- Label DESTROY command with 24-bit Destroy Code protection

1.2 Memory Features

- 192 bits, organised in 24 blocks of 1 byte each
- Data retention of 5 years

13.56 MHz I CODE chip from NXP: Information available via
http://www.nxp.com/acrobat_download/other/identification/SL080530.pdf



RI-UHF-IC116-00

www.ti.com

SCBS874-JULY 2008

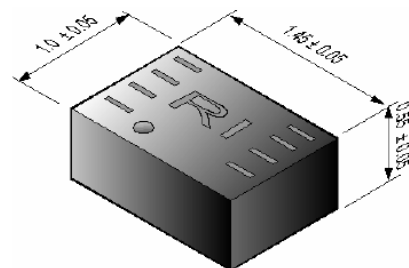
SMT EPC Gen2 IC

FEATURES

- Meets EPCglobal™ Gen2 (v1.0.9) and ISO/IEC 18000-6C
- Global Frequency Operability: 840 MHz to 960 MHz
- Supports Optional Gen2 Commands: Block Write and Block Erase
- 192-bit Memory: 96-bit Electronic Product Code™ (EPC), 32-bit Access Password, 32-bit KILL Password, 32-bit TID Memory
- Designed for High Performance and Low Power Consumption, Based on the Most Advanced Silicon Node for RFID (130 nm)
- Fast Tag Singulation Using Most Advanced Anticollision Scheme
- Green (RoHS and No Sb/Br) Compliant

APPLICATIONS

- PCB Tracking
- Specialized Tag Designs



Dimensions in mm

UHF SMT EPC gen2 chip from Texas Instruments: Information available via
<http://focus.ti.com/lit/ds/symlink/ri-uhf-ic116.pdf>

RFID-AP	30/01/2009	1.0	16/44
Project	Date	Version	page

2. Features

2.1 Key features

Interface fully compatible with UHF EPC G2 standard
 Long-range solutions
 Suitable for UHF RFID, allowing one IC to be used worldwide
 Fast data rate
 Forward link: 40 to 160 kbits/s
 Return link: 40 to 640 kbits/s
 512-bit of on-chip memory
 96-bit EPC
 64-bit tag Identifier
 224-bit programmable user memory
 32-bit access password
 32-bit kill password
 Runs on the same hardware infrastructure as the UCODE HSL and the UCODE EPC1.19

2.2 Key benefits

Tags/labels and readers available from various suppliers
 First UHF EPC product operating worldwide
 Highly advanced anti-collision resulting in highest identification speed
 Reliable and robust RFID technology suitable for dense reader and noisy environment
 Secure UHF communication; readers do not transmit EPC data
 Broadest industry back-up - EPCglobal and ISO 18000-6C
 Reader portfolio covers all regional demands

2.3 RF Interface Features

Contact-less transmission of data and supply energy (no battery needed)
 Long-range operating distance
 Operating frequency within the released operating bands from 860 MHz to 960 MHz
 High data integrity: 16-bit CRC, framing
 High anti-collision and inventory speed
 Data rates:
 R -> T: 40 to 160 kbps,
 T -> R: 40 to 465 kbps (Divide ratio DR = 8) or 95 to 640 kbps (DR = 64/3)
 Uses a slotted random anti-collision algorithm where the UCODE EPC G2 IC loads a random (or pseudo-random) number into a slot counter, decrement this slot counter based on interrogator commands, and reply to the interrogator when their slot counter reaches zero. Supports the full mandatory command set as well as optional and Customer commands according to the standard

UHF UCODE EPC G2 chip from NXP: Information available via
http://www.nxp.com/acrobat_download/other/identification/SFS129430.pdf

RFID-AP	30/01/2009	1.0	17/44
Project	Date	Version	page



XRA00

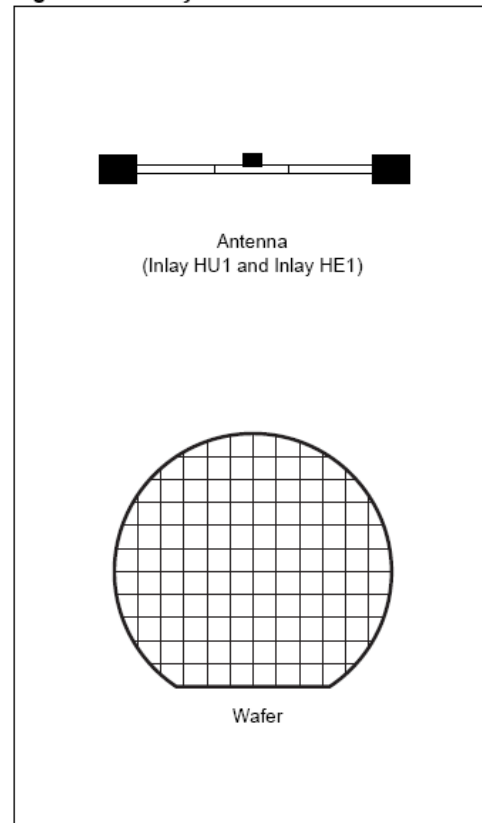
UHF, Auto-ID Class 1b, Contactless Memory IC 96 bit ePC with Inventory and Kill Function

DATA BRIEFING

FEATURES SUMMARY

- Auto-ID Class-1b fully compliant
- UHF Carrier Frequencies
 - 868MHz ISM Band
 - 915MHz ISM Band
- To the XRA00:
 - Asynchronous 50% to 100% ASK modulation using PWM pulse coding (up to 70 kbit/s)
- From the XRA00:
 - Back-scattered answers using Bi-phase Space coding (up to 140 kbit/s)
- 128 bits EEPROM with Lock Function
- 96 bits ePC
- Inventory, Read, Program and Erase functions
- Kill Command
- 30ms Programming Time (typical)
- More than 10000 Write/Erase cycles
- More than 40 Year Data Retention

Figure 1. Delivery Forms



UHF XRA00 chip from ST Microelectronics: Information available via
http://www.datasheetcatalog.org/datasheets/134/285161_DS.pdf

RFID-AP	30/01/2009	1.0	18/44
Project	Date	Version	page

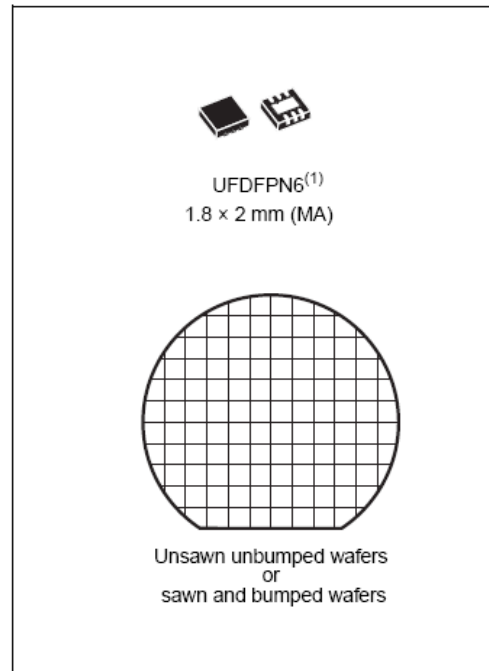


XRAG2

432-bit UHF, EPCglobal Class1 Generation2 and ISO 18000-6C, contactless memory chip with user memory

Features

- EPCglobal class 1 generation 2 RFID UHF specification (revision 1.0.9)
- Passive operation (no battery required)
- UHF carrier frequencies from 860 MHz to 960 MHz ISM band
- To the XRAG2:
 - Asynchronous 90% SSB-ASK, DSB-ASK or PR-ASK modulation using pulse interval encoding (Up to 128Kbit/s)
- From the XRAG2:
 - Backscattered reflective answers using FM0 or Miller bit coding (up to 640 Kbits/s)
- 432-bit memory with two possible configurations:
 - 3 memory banks to store up to 256-bit EPC code: 64-bit TID, 304-bit EPC and 64-bit reserved banks
 - 4 memory banks to store up to 128-EPC code: 128-bit user, 64-bit TID, 176-bit EPC and 64-bit reserved banks
- Supports EPC and ISO TID
- Multisession protocol
- Anti-collision functionality
- Inventory, Read, Write and Erase features
- Kill command
- 100 ms programming time (max) for 288-bit (EPC code, Protocol Control bits and CRC16) programming
- More than 10,000 Write/Erase cycles
- More than 40 years' data retention
- Packages
 - ECOPACK® (RoHS compliant)



1. Preliminary data.



950110126000000216

UHF XRAG2 chip from ST Microelectronics: Information available via
http://www.datasheetcatalog.org/datasheets/134/285161_DS.pdf

RFID-AP	30/01/2009	1.0	19/44
Project	Date	Version	page



EM MICROELECTRONIC - MARIN SA

SWATCH GROUP ELECTRONIC SYSTEMS

Fact Sheet EM4444

512 bit, Read/Write UHF Identification Device

Description

The EM4444 is used in passive UHF Read/Write transponder applications. It is powered up by an RF beam transmitted by the reader, which is received and rectified to generate a supply voltage for the chip.

A pre-programmed ID code or other data is transmitted back to the reader by varying the amount of energy that is reflected back to the reader.

It implements the robust and fast anti-collision protocol full compliant with the EM Microelectronic UHF read-only and read/write tags. Data is written to the tag in 64 bit blocks by commanding the chip after its presence had been detected.

ID only or ID and one or more EEPROM data pages is transmitted continuously in a Tag-Talks-Only (TTO) mode. Alternatively data can be read from the tag in 64 bit blocks by commanding the chip after its presence had been detected.

The reading range depends on the reader power allowed by local spectrum regulations, but in excess of 6 m can be achieved in the USA (license free) and 20 m (site licensed). More than 2 m can be attained in Europe. ID reading rates of 120 tags per second can be attained.

The chip is compatible with the EM4222/EM4122 read-only chips and readers. It can be used in mixed populations of read/write and read only RFID tags.

Features

- Compatible with UHF read-only and read/write tags (EM4222, EM4122, EM4442)
- Factory programmed 64 bit serial ID number
- 7 pages of user programmable and lockable memory (64-bit pages)
- EEPROM data pages can be transmitted with ID in Tag-Talks-only (TTO) mode.
- Can be used as OTP device
- High reading data rate up to 256 kbit/s
- Frequency independent: typically used at 315 MHz, 433 MHz, 869 MHz, 902 - 928 MHz and 2.45 GHz
- On-chip oscillator
- Low voltage operation down to 1.3V
- 40 to +85°C temperature range

Applications

The EM4444 is ideal for applications where long range, high-speed item identification is required:

- Supply chain management
- Tracking and tracing
- Smart labelling
- Airline baggage

Typical Operating Configuration

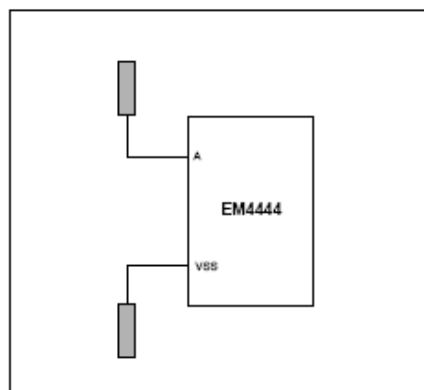


Fig. 1

UHF EM4444 chip from EM Microelectronic: Information available via http://www.emmicroelectronics.com/webfiles/product/RFID/ds/EM4444_FS.pdf

RFID-AP	30/01/2009	1.0	20/44
Project	Date	Version	page

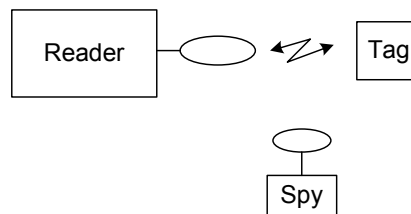
3 Security Threats

The security issues that are associated with RFID tags are by now well-known. However, as we will see, this does not make the task of finding solutions any easier. The different kind of attacks can be grouped together according to where the attacker is active.

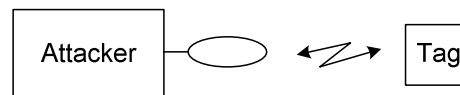
3.1 Physical Layer Attacks

Attacks on what is termed the physical layer of an RFID-enabled system can be classified into two types:

- **Passive attacks:** which consist of **listening** on transactions between an authentic reader and a tag.



- **Active attacks:** which consist of interacting with the reader and/or the tag during an attack.



3.1.1 Eavesdropping

Some initial publications with practical results about eavesdropping were mentioned at the National Institute of Technology (NIST) demonstration at the National Biometric Security Project Facility in 2004. There it was claimed that using a reader equipped with a specific antenna, the testing team was able to lift "an exact copy of digitally signed private data" from a contactless e-passport chip from 30 feet (9 m) away. No precision was given about experimental conditions and real performances and so this leads to different interpretations. It seems likely that only the reader-to-card communication had been intercepted, but it is interesting nevertheless. Of course, the e-passport is not the cheap RFID tag that we are interested in during RFID-AP, but it is indicative of the kind of adversary we need to consider.

More results in the same vein include the following. At *Cartes 2005* Kroniger suggested that a reader could be successfully listened to from a few meters while the listening distance for contactless card would be far more restricted, perhaps to 80 cm. This distinction between the reader and the card is also present in the BSI report [R1] but with a larger (tens of meters) listening distance for the reader. The suggested listening distance for contactless cards remains restricted to about 5 times the nominal distance given by manufacturer, that is to say to about 1 meter.

RFID-AP	30/01/2009	1.0	21/44
Project	Date	Version	page

In [FK04], it is demonstrated through experimentations that reader-to-card and card-to-reader communications could be intercepted over a distance of up to 2 meters. Hancke [H08] provides a variety of details on means and methods (antennas, instrumentations, tunings...) to perform eavesdropping on contactless transactions. Experiments with an AGC reader and ISO14443 A/B [ISO14443] and ISO15693 [ISO15693] cards were performed and, according to his measurements, the performances of different cards were such that reader-to-card communication could be eavesdropped over 10 meters for ISO14443 A and ISO15693 and up to 3 meters for ISO14443 B. By contrast the card-to-reader communication could be eavesdropped up to a distance of only 1 meter for ISO14443 A and ISO15693 and up to 3 meters for ISO14443 B.

It should be noted that for all this figures, the attacker is only interested in listening to the communication. To actively participate is much harder and a particularly delicate problem to solve. Not least, we need to be able to power the tag and then to send commands by modulating the field and this is not so easy.

3.1.2 Skimming

As opposed to eavesdropping, which requires the attacker to listen in to a genuine tag-reader interaction, the attacker in skimming will actively interrogate a tag, perhaps from a distance. The goal is to recover information from the tag (or in the case of a contactless smart card, the card) perhaps so that the information can be used to provision another device.

Skimming requires two capabilities that are usually in conflict: we need an antenna with a high quality factor for generating a high magnetic field with the minimum of dissipated power. However, at the same time, we need a large bandwidth for modulating the field and sending commands to the tag. These two operations can be made with separated devices that are equipped with distinct antennas, but they must operate with the same clock.

In the Kroniger study, energizing a contactless card at 50 cm distance is barely feasible; however energizing a contactless card – or in the scenarios of interest to RFID-AP a tag – at 1 meter is impossible because the dissipated power grows with the cube of distance. If we need only 0.5 W for energizing a contactless card at a distance of 5 cm, we need 500 W at 50 cm, which is not easily achieved using portable power appliances. At 5 meters we would need 500 kW, which would not only be a problem of portable power generation, but also a hazardous exercise for the attacker!

We can also find practical values in publications describing the realization of relay attacks. Z. Kfir and A. Wool, University of Tel Aviv, evaluate a simulated reading distance of 40 to 50 cm. From this study, I. Kirchenbaum and A. Wool build a demonstrator, easily made for less than 100\$, which is able to read a contactless card from a distance of 35 cm.

3.1.3 Denial of service

The goal of denial of service attacks is to disrupt the application that is being used by valid users. Since they merely aim to disrupt rather than to do anything necessarily precise, the denial of service attack is reasonably easy to accomplish and rather difficult to guard against.

They might be divided into three categories:

RFID-AP	30/01/2009	1.0	22/44
Project	Date	Version	page

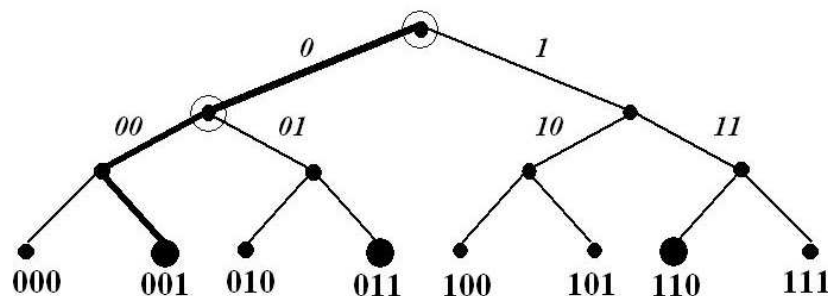
- Interference in the anti-collision protocols,
- Reader and/or tag jamming, and
- Tag destruction.

3.1.3.1 Anti-collision protocols

When we have many tags in the range of a single reader, we need to have some mechanism for the reader to sort out how to talk to each tag individually. This is the role of the inventory instructions that were given earlier. Generally speaking, there are two different solutions to managing the collision of tags: one is a deterministic protocol and the second is probabilistic.

In the deterministic protocol, the main principle is that the algorithm implemented in the reader explores the identifying number of a tag, the UID, bit-by-bit like a tree-walking protocol. This protocol is simple to implement and is very time efficient. However from a privacy point of view, this protocol is not secure since the reader calls the different tags using their unique UIDs and this request from the reader has a much greater range than that responses emitted from the tag. Thus the UIDs of any tags in the vicinity are easy to intercept. By contrast, in the probabilistic algorithm, only the tag emits the UID and so the UID becomes much more difficult to intercept by a third party.

An example of the tree-walking algorithm is given by Juels [JRS03] where the figure below appears. Consider a tree of depth three which can therefore support eight tag serial numbers (represented at the tree leaves) and suppose that three tags are present, the 001, 011, and the 110 tags. The tree-walking algorithm singulates the 001 tag by following the bold-edged path but at two nodes, the root of the tree and the root for all tags with a '0' prefix, there will be collisions because there are tags present in the left and right sub-trees [JRS03].



The goal of the well-known blocker tag is to create these collisions. Juels et al. [JRS03] developed a device that blocks this tree-walking singulation protocol – by emitting both a zero and one at a branch point – and thereby hides the tag UIDs that lie at the leaves of the tree.

It is interesting to note that the blocker tag can be viewed as a privacy solution against unauthorized scanning as well as a denial-of-service threat. Also the blocker tag is essentially a passive tag and so it will need to be powered by the reader field for it to work, and will therefore only protect tags that are close to itself.

RFID-AP	30/01/2009	1.0	23/44
Project	Date	Version	page

Probabilistic protocol

In the probabilistic protocol, sometimes called ALOHA and which in the 13.56 MHz range is implemented by all standards (ISO 14443B, ISO 15693, ISO 18000 [ISO18000]) tags select a random communication slot in which to reply to a reader query. The maximum number of slots is typically set in the tag as a default value. Once the tag selects a slot, the reader signals the start of each slot so that the tag can communicate and after responding at the correct slot, the tag goes quiet. If tag responses collide, then the tags keep trying by cycling round different slot positions until all tags enter a quiet state

The RFID Guardian has been proposed [R05a,R05b,R06a,R06b] as a device that might be used to prevent unauthorized reading by sending a jamming signal. Clearly, such a device could be a useful privacy tool, though in the same way it might also be viewed as a device to carry out a denial of service attack. Whereas the blocker tag is a passive device, the RFID guardian requires batteries and emits its own signal. It will therefore have a much greater blocking range than the blocker tag, though at greater cost. The Guardian creates fake tag responses by selectively generating properly-encoded responses in a way that they are recognized by the RFID tag reader. Thus in an ALOHA anti-collision protocol, the RFID Guardian can determine the time-slot where specific tags will answer and then emit a jamming signal to create a collision and to hide a given tag UID.

3.1.3.2 Reader and card jamming

The jamming attack is often mentioned though it is not frequently detailed. The obvious idea is to emit a signal in the same bandwidth as the reader or the tag in order to obfuscate the transmission between the reader and the tag. This can therefore be seen as a rather unsophisticated relative of the blocker tag. Since the attack requires no ingenuity, the only goal is to drown the reader or tag signal in a higher level of noise. Since the maximal level of emitted magnetic field is restricted in international agreements, and while be adhered to by legitimate tags and readers, any attacker able to pass this limitation is sure to efficiently jam an RFID reader. Note that exceeding the standard does not necessarily require a lot of power. If the noisy emission is in the exact bandwidth of the reader signal, then it could be that only a few watts (1 to 2 W) of power are enough. To spoil the tag signal is of course even easier since its signal is at a much lower level than that of the reader.

3.1.3.3 Tag destruction and deactivation

Again, not a particularly sophisticated attack, but the destruction of a tag is an irreversible form of denial of service attack. Note that it is also a particularly effective form of privacy protection if the tag is destroyed with the consent of the holder, or by the holder, as is sometimes proposed.

One might distinguish between destruction being carried out at a distance and that carried out directly. For example mechanisms for generating electromagnetic pulses to destroy a contactless chip at short range have been proposed. However the opportunities for destroying a tag at a distance are not so wide-spread, even though we might observe that EAS, or in-store anti-theft devices, share features with this kind of scenario when they are deactivated at the point-of-sale. Instead it seems to be more likely that an individual will destroy his own tags, for instance by breaking the antenna. Importantly, EPCglobal specifies the use of a *kill* command that will render an EPC tag inoperable. It is envisaged that this could be used at the point-of-sale, or at other points in the supply chain.

RFID-AP	30/01/2009	1.0	24/44
Project	Date	Version	page

3.1.4 Side channel attacks on the contactless interface

The idea of using physical information – such as power consumption or timing analysis – to recover secret information from a chip is by now very widespread. Certainly in the case of contact smart cards such attacks, i.e. Simple Power Analysis (SPA) and Differential Power Analysis (DPA) are well-known. However, in the case of contactless smart cards, and then in our case of RFID tags, account needs to be taken of the communication aspects of the application.

At least in principle, the use of a radio frequency signal to supply energy to a contactless device would certainly give a way to recover information about the inner activity of a chip. To see this we note that the electromagnetic load constituted by the RFID device will change as a function of the energy supplied to the chip. Thus, depending on the activity of the chip, it should be possible to recover information from the radio frequency signal measured around the reader and tags.

Some preliminary work has taken place, but measurement of the power consumption or the local electromagnetic field emanation requires the attacker to be very close to the device under attack. Further, the simple tags of interest to us do not carry long-term cryptographic secrets (though they may store passwords) and so the value of such an attack is not clear. However, if RFID tags are developed that use cryptographic primitives then the possibilities of side-channel cryptanalysis will become an important factor in the security they offer and potentially increase the cost of a deployment if counter-measures are required.

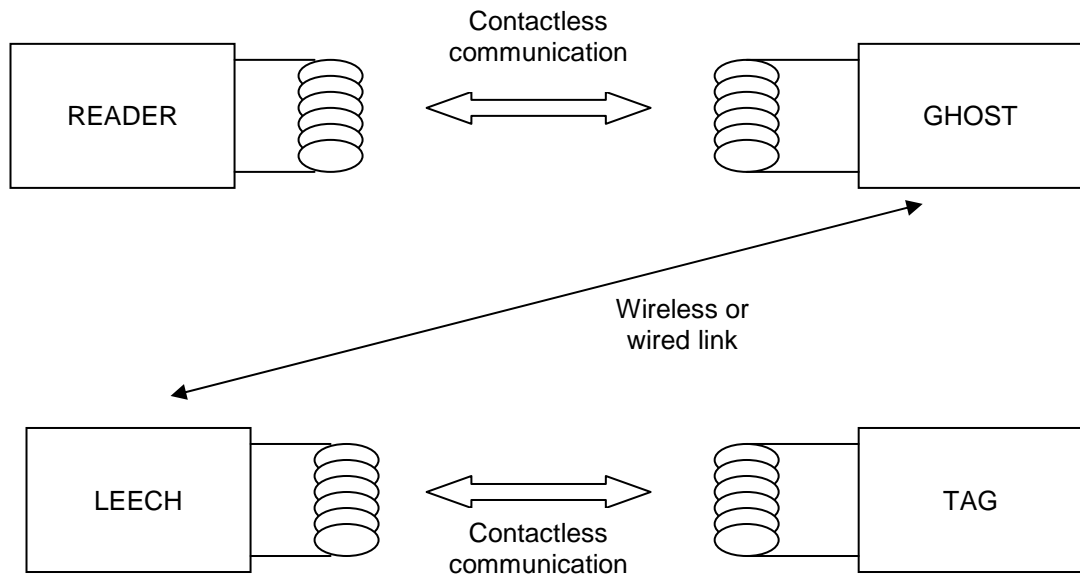
3.2 Communication Layer Attacks

Moving higher up the stack, we now consider attacks that aim to exploit the communication process between a tag and a reader.

3.2.1 Relay Attack

Relay attacks involve two different devices and this must be quite carefully coordinated. One device, that will interact with the target device under attack is named the *leech* though the term *mole* is also sometimes used. The leech is then linked via some relay to a *ghost* that will reproduce the data to a legitimate reader. The scenario – and the threat – is in fact more suitable to contactless smart cards, particularly ones involved in some transaction. But the scenario can still be applied to the idea of a rogue reader being used to interrogate a legitimate tag and using the responses gained to impersonate that tag with a legitimate reader elsewhere.

RFID-AP	30/01/2009	1.0	25/44
Project	Date	Version	page



Note that the leech must activate and power the target tag so as to communicate with it. Skimming a card is an attack in itself and is already discussed in this document. The ghost is able to use this information to communicate with a genuine reader. As is common in this field, there is much speculation about the maximum distances that can be considered for this kind of attack, and some of this has already been considered in the document. It's interesting to also place the RFID Guardian (see earlier) in the context of a relay attack.

One issue with the relay attack is the timing required and the difficult interaction this can have with higher-level communication protocols. However there is much work on showing how such an attack could be plausibly applied. We note however, that most applications of this attack are in the realm of contactless smart cards, and for tag deployments that we consider in RFID-AP, it is very difficult to see the exact attack scenario that would make a relay attack a serious threat.

3.2.2 Man-in-the-middle attack

The man-in-the-middle attack is similar to the relay attack, but with the distinctive feature that the communication might be modified during the relay. Such an attack will inherit all the physical problems of powering and timing that we saw for a relay attack, but apart from that this is an attack that is potentially common to all modern communication systems. The typical solution is to add some form of authentication mechanism to the communication channel, but this requires cryptography and can be – see later – a substantial overhead for the cheapest RFID tags.

3.3 Higher Layer Attacks

Once we are above the tag communication layer we are entering attacks on the RFID tag application itself. Here the attacks are a bit harder to quantify – given the wide range of attacks that might apply to a given application – though it is often at the tag or protocol level that solutions can be deployed.

RFID-AP	30/01/2009	1.0	26/44
Project	Date	Version	page

The possibility of copying the information on a tag and to create fake tags is an important issue in the fight against counterfeit goods. Even tracking batch numbers and the EPC codes used on – say – a batch of medicines need not provide full protection against the substitution or introduction of fake goods into the supply chain. For example a skimming attack could allow the contents of the tag memory to be read and then copied into a blank substitute tag.

The best protection against counterfeiting is provided by cryptographic solutions. However deciding the full cost-benefit for the use of cryptography in RFID tags is not always so easy, as we will see later.

A more disruptive kind of threat – perhaps best viewed as a denial of service attack mounted at the application – is posed by the possibility of viruses and worms.

The announcement of the possibility of viruses and worms in RFID systems unsettled the community in 2006 [Rie06c]. This kind of denial of service attack would not be based on a weakness of the physical contactless link but instead pointed out that faults in the middleware could have an equally devastating effect on a system. However it should be pointed out that vulnerabilities in the middleware or backend databases of an RFID system are vulnerabilities that might appear in any IT deployments and they are not specific to RFID-tag deployments. They can also be avoided by adhering to good software programming practices. In addition, while it might sound quite dramatic to have viruses and worms linked to RFID tags, the very limited resources on a tag coupled with their very specific role mean that such a possibility is very remote.

RFID-AP	30/01/2009	1.0	27/44
Project	Date	Version	page

4 Formalised Security Requirements

Generally, RFID systems deal with the identification of a tag by a reader. Using a wireless communication protocol, the tag and reader exchange data so that at the end the reader is convinced that it was communicating with a certain tag. In RFID-AP, tags will be used for so called “private identification”. In private identification, the goal is for party A to reveal its identity to party B – and only to party B. So, a tag should reveal its identity, and thereby the owner of a tag, to a reader, but not, e.g., to an eavesdropper. Generally, it is of importance that neither with passive, nor with active attacks a tag’s identity can be revealed to any other, non-authorized party. Also, an adversary should not be able to impersonate himself as a valid tag, i.e., to make the reader believe that it is communicating with and falsely identifying a tag. The latter security requirement is called authentication.

There are a number of recent publications on the subject of formally defining the meaning and notions of RFID-specific private identification and authentication, cf., [V07, JW07, JW05].

4.1 Security Notions and Goals in RFID Systems

In the following, we will present an overview of work that appears in [V07, JW07, JW05] so as to help understand the notions of identification, authentication, and privacy in RFID systems. Therewith, we identify the different security goals we will aim at within project RFID-AP.

4.1.1 Identification

With RFID tag identification, a reader gets to know the identity associated with a tag or the owner of a tag. Typically, identities are represented as serial numbers, therewith uniquely identifying the owner of a tag or the object a tag is attached to by plain numbers. However, all kinds of computerized representations of identities are imaginable. With this respect, the notion of identity of an RFID-tag is comparable to the identity of classical barcode labels. Real-world examples for tag identification are the aforementioned EPC codes, which allow for a quick scanning of all tag’s serial numbers within wireless communication range of a reader. Identification as such does not contain any notion of “security” or an “adversary”, yet

4.1.2 Authentication

In many scenarios, an adversary might be interested in spoiling identification by trying to impersonate, e.g., another tag. The goal of the adversary is to successfully identify himself as any valid or one specific tag to the reader. An authentication protocol identifies a tag or the owner of a tag towards a reader such that the reader is sure that it was really the valid tag the reader was talking to.

Authentication may be **unidirectional** (a reader might authenticate a tag, but also a tag might authenticate a reader making sure it is communicating with the “correct” reader) or **mutual** (the tag authenticates to the reader and the reader also authenticates to the tag). Generally, authentication requires a challenge to prevent so called “replay attacks” where an adversary might eavesdrop on the communication between reader and tag, store the communication, and later replay the communication to impersonate a tag. Sending a challenge from the reader to the tag before further communication ensures the “freshness” of the communication to the reader and helps in making subsequent data exchanged dependent on the challenge. In general, freshness could also be achieved using synchronized (between tag and reader) clocks. However, this is difficult to realize on today’s tags as they typically do not have an on-board battery to power a clock.

RFID-AP	30/01/2009	1.0	28/44
Project	Date	Version	page

Identifying or authenticating a tag to a reader is, however, not sufficient. An adversary should not be able to identify any tag and only valid readers should be able to do so. Also, an adversary should not be in the position to link different executions of an identification protocol to a single tag: even if the adversary does not know which tag or which owner of a tag is currently doing executing an identification protocol run, he should in addition not be able to recognize a tag, i.e., be able to deduce that he has seen the tag before. Such notions of privacy are presented in the following.

4.1.3 Untraceability

Suppose that an adversary is able to accumulate logs of tag-reader interactions, i.e., a (partially) successful protocol executions. Further, suppose that an adversary has accumulated a set L_1 of execution logs of a protocol between various tags and readers, and the adversary has access to the set L_2 of execution logs of the same identification protocol between one specific tag T and various readers. The identification protocol is said to provide untraceability, if the adversary cannot decide whether some of the logs in L_1 relate to T with a higher probability than just guessing.

4.1.4 Unlinkability

Suppose that, again, an adversary has access to the set L_1 of logs of the execution of an identification protocol between various tags and readers. The protocol is said to provide unlinkability, if the adversary is unable to select any pair of logs that relate to one and the same tag – with higher probability than guessing.

4.1.5 Anonymity

An identification protocol can be called anonymous, if no adversary is able to derive the (secret) identity of the tag.

4.1.6 Forward-secrecy

Suppose that an adversary has access to the inner state of a tag T , e.g., by physically compromising T , reading out all its memory etc. Also, the adversary has collected a set L_1 of past execution logs of the protocol between various tags and various readers. Then, an authentication protocol is said to provide **forward-secrecy**, if an adversary is unable to tell which execution of the authentication protocol relates to T (other than with negligible advantage over a random guess).

Among the above notions of privacy, the following implications can be identified [V07]:

Forward Secrecy \Rightarrow Unlinkability \Rightarrow Untraceability \Rightarrow Anonymity

RFID-AP	30/01/2009	1.0	29/44
Project	Date	Version	page

5 Current Security Solutions

Just as there are a wide variety of threats to an RFID-enabled system, there are a wide variety of proposed solutions to cope with some attack. We will see, however, that few are entirely satisfactory.

5.1 Physical Layer Solutions

5.1.1 The “Kill” Tag Approach

This solution consists of creating a new command, the “kill” command, that enables the destruction of the tag so that it can never be re-activated. Deactivation can be implemented by a fuse on the power supply of the chip or on the antenna, or by erasing of the memory. This command could be used, e.g., after checkout at a store. This approach ultimately solves all the problems of privacy. But outside a supply chain, all the advantages of an RFID-enabled application disappear. Thus, with the destruction of the tag all of the proposed future benefits of Ambient Intelligence are substantially reduced: no more possibility to make fridges interact with food packaging or washing-machines with clothes. Even the control of a part of the supply chain is removed: tracking of items for recycling or for after-sale services is not feasible anymore. With such an approach, RFID only remains a tool to improve logistics of manufacturers and distributors. The implementation of the “kill” command implies also the use of a basic cryptographic algorithm to avoid the destroying of all the tags in the shop by a hacker [SA02, JRS03].

5.1.2 The Faraday Cage

A basic solution to protect tags against malicious, unwanted wireless communication is to protect our RFID tags by a metallic sheet or metallic mesh; for contactless smart cards this is often in the form of a wallet, but one can also imagine store bags being protected in a similar manner to provide tags on clothing being read in the street while the buyer returns home. Such packaging makes a simple Faraday cage blocking the HF and UHF radio signals of readers. To be efficient against HF electromagnetic waves, the thickness of the metallic sheet should be greater than 20 μm for a metal with a good conductivity like copper or aluminium. Considering the metallic mesh, the periodicity of the grid (that is the unit scale on which the mesh repeats) should be around half of the wavelength. This solution is cheap and efficient and is not based on a complex technology. As a consequence, it is a very reliable way to ensure the security of contactless devices while not in use. There are a large number of suppliers for such wallets, though for RFID tags there are fewer targeted solutions.

Generally speaking, the Faraday cage gives good protection against malicious communication, but the approach clearly has its limits. For larger tagged objects that cannot be placed easily in an adequate Faraday cages there is no easy solution. Another problem is raised by the fact that the RFID tags will soon be so small – and often integrated into clothing – so that we will not know where they are in the first place.

5.1.3 Active Jamming

It is possible to create a device that emits signals in the same bands as RFID readers to jam their communications with RFID tags. However such a device would broadcast signals with a higher amplitude than the different standards permit and, as a consequence, would probably not be legal. The use of jamming has already been mentioned before as a form of denial of service attack. Indeed, most denial of service attacks can be viewed as more-or-less efficient countermeasures to the problem of malicious interrogation.

RFID-AP	30/01/2009	1.0	30/44
Project	Date	Version	page

5.1.4 Noisy Tags

To prevent from eavesdropping on the communication, C. Castelluccia and G. Avoine [CA06] developed a solution named the "noisy tag". A special tag shares a key with the reader to create a secure communication channel. Then the noisy tag emits some bits generated with this key known only by the reader during the reply of the tag to the reader. The noise created by the noisy tag should prevent eavesdropping. Yes still the communication can be understood by the reader since it is able to subtract the noise. This approach however, introduces some major drawbacks. First of all, it requires a key agreement that is not always easy to implement. Secondly, the noise generated is digital (bits are sent), so it will be really unlikely that a spying probe close by sees the signal from the noisy tag and from the original tag with the same amplitude. Consequently, it will be always possible to see a difference that is enough to retrieve the message from the tag.

5.1.5 The Blocker Tag

The blocker tag [JRS03] is already well documented in the previous chapter where it was presented as a tool for denial of service. The main drawbacks of the blocker tag to protect the user are that it cannot be selective (it will blur all tags). Also it is a passive device that must be powered by the reader to work.

5.1.6 The RFID Guardian

The RFID Guardian [R06a,R06b,R05a,R05b] is also aforementioned as a denial of service attack. In principle it can offer a large panel of services to protect the user: secret key management, authentication, access control, monitoring of the RFID environment, creation of collisions. It does not have the main drawbacks of the blocker tag, since the Guardian can be active. However, the selectivity can only be realized with ALOHA type anti-collision protocols, which would not necessarily be the mechanism in use.

5.1.7 Distance bounding protocol

An adversary might try to impersonate a valid tag with a "relay attack". The adversary starts identification with a reader and forwards all communication from the reader to a valid tag. This valid tag might be physically far away from the reader, so the adversary might require an additional communication channel to reach it. As the tag cannot detect whether the ongoing communication is a "relay attack" or a legitimate communication, it will respond to the relayed communication. The adversary can now relay the tag's response to the reader and has now successfully identified himself as a valid tag.

To protect against such a threat, "distance bounding protocols" are typically used. The principle of distance bounding protocols is to detect unusual propagation times during wireless communication. To monitor this [H05] we can imagine inserting delays that depend on a cryptographic function and a key that is known only to the reader and the tag. This information can be sent using a second communication channel and so changes in the anticipated delays can be detected by the reader and the tag, thereby confirming that the channel is not safe. The drawback of such a solution is the requirement of an additional communication channel and the implementation of a cryptographic function on the tag.

RFID-AP	30/01/2009	1.0	31/44
Project	Date	Version	page

5.2 Cryptographic Solutions

In Section 3, we saw a great variety of different attacks that might be mounted against an RFID-enabled application. It turns out that countermeasures to many threats – but certainly not all – can be provided by cryptography.

However deploying any cryptographic mechanisms involves several overheads. Not only is there a performance overhead, which in the case of the cheapest RFID tags can be a very substantial one, but there are also issues in how to support the provisioning and distribution of key material, a problem that is often referred to as providing the cryptographic infrastructure.

For instance, one solution to guard against eavesdropping or replay attacks could be the encryption of data and the use of cryptographic signatures. Symmetric keys could be used with algorithms like DES or AES, and asymmetric keys with algorithms like RSA or elliptic curves. However, those algorithms require a lot of computing resources on an RFID tag and this has led to some new and active research directions.

In particular, over recent years there have been tremendous advances in the field of *low-cost* or *light-weight cryptography*. While many research-oriented protocols call upon cryptographic techniques, it is often assumed that only the simplest and marginally secure cryptographic methods can be implemented on the cheap tags we associate with RFID-based applications. However this is no longer the case and instead new, trusted algorithms offering full security are becoming available.

In this section we will make a non-technical survey of the current state of the art. (More details will follow in the deliverable DWP2.2 later in the RFID-AP project.) For this survey, we adopt the typical classification in the literature [MvOV96] and we separate classes of cryptographic algorithms according to how they use key material.

Symmetric (secret-key) Algorithms	Asymmetric (public-key) Algorithms
Block ciphers	Encryption schemes
Stream ciphers	Digital signature schemes
Hash functions (keyless algorithms)	Identification schemes
Message authentication codes	

When considering the performance of a cryptographic algorithm – particularly for use in highly constrained environments such as RFID tags – then we are typically concerned about the following performance attributes:

- The size of an implementation, as measured by *equivalent gates* (GEs).
- The peak and the average power consumption.
- The time required to complete a computation.

These attributes are now addressed in more detail.

RFID-AP	30/01/2009	1.0	32/44
Project	Date	Version	page

The notion of *equivalent gates*, more familiarly referred to as *gate equivalents (GE)*, allows us to compare different implementations and different algorithms. We use the NAND gate as the basic unit of size and we give the area of an implementation in terms of the number of NAND gates that would occupy the same area. While there will still be some minor variance in the area quoted for the same implementation when different fabrication technologies are used, when the same manufacturing techniques are used this gives a reasonable way of comparing algorithms.

The power consumption is particularly important for passive devices (e.g. the classical RFID tags) since they derive their power from a reader. As it moves past a reader, a tag will benefit from a short power exposure that increases as the tag approaches a reader and falls away as it moves away. Algorithms, therefore, that are particularly power hungry – especially at the start or the end of an interaction – might not be so suitable. For other applications such as sensor networks, where nodes might be self-powered but difficult or expensive to replace, then reduced power consumption is essential. However, the power consumption of an algorithm depends heavily on the implementation and it is almost impossible to compare the power consumption in any meaningful way across the work of different implementation teams or even the work of the same researchers across different fabrication technologies. For this reason we avoid giving power consumption figures in the tables that follow, though we do highlight specific data points in the accompanying text.

Many algorithms offer a range of implementation options and one common hardware implementation technique is to trade space for time. By this we mean that a more compact design, for instance a serial rather than a parallel implementation, can often be derived at the cost of a more time-consuming operation. While no-one is expecting to do significant amounts of cryptography on an RFID tag, and therefore timing might be seen as a secondary issue, passive RFID tags are often used in high-speed multi-tag and multi-reader environments. In such situations, higher-level protocols determine how tags and readers communicate and these can pose significant demands on the amount of time available for performing some computation.

Taken together, these three attributes pose considerable problems for the cryptographic designer.

RFID-AP	30/01/2009	1.0	33/44
Project	Date	Version	page

5.2.1 Symmetric Cryptography

In symmetric cryptography the users – e.g. the senders and the receivers – both share the same key material. This can pose difficult infrastructure problems since the correct key needs to be securely delivered to the correct participants at the right time. However, it is typically the case that symmetric primitives can offer improved performance over asymmetric alternatives.

5.2.1.1 *Block Ciphers*

Block ciphers are first and foremost encryption primitives and they operate on fixed blocks of data. The size of the data block – m bits – is termed the block size and the key size (in bits) is often denoted by k . As we change the key through all the 2^k possible alternatives, the block cipher instantiates different permutations of the set of 2^m possible input blocks, and it does so in a seemingly random manner. Today, the state of the art of block cipher design is very well developed and there are a variety of block ciphers that are claimed to be suitable to low-cost implementation. The performance of a range of these block ciphers is given in [BKL+07] and reproduced here.

		Key Size	Block Size	Cycles / Byte	Throughput @ 100KHz	Logic μ m	Area GE
PRE-SENT	[RPL+08]	80	64	563	11	0.18	1080
PRE-SENT	[BKL+07]	80	64	32	200	0.18	1570
DESXL	[LPP+07]	184	64	144	44.4	0.18	2168
DES	[LPP+07]	56	64	144	44.4	0.18	2309
mCrypton	[LK05]	96	64	13	492.3	0.13	2681
HIGHT	[DSH+06]	128	64	1	6400	0.25	3048
AES-128	[FDW04]	128	128	1032	12.4	0.35	3400

As can be observed, the most promising block cipher in the table is PRESENT and this is confirmed by a power consumption of 5 μ W for the implementation and architecture described in [BKL+07]. More recently, an implementation of PRESENT was announced which required little more than 1000 GE and 3 μ W though the throughput suffered as a result with an encryption rate of 11 Kbps at 100 KHz [RPL+08].

While block ciphers are typically viewed as an encryption primitive, they can be used in a natural way as the basis for a challenge-response authentication protocol; the reader would send a challenge c to the tag which then encrypts and sends back the encryption challenge to the reader. Since both tag and reader share the same key, the response can be verified. Block ciphers can also be used to build examples of the remaining symmetric algorithms that we consider in the following sections.

5.2.1.2 *Stream Ciphers*

Stream ciphers of a dedicated design are commonly viewed as being more efficient (in some sense) than block ciphers. Stream ciphers operate by continually updating some cipher *state* and sampling

RFID-AP	30/01/2009	1.0	34/44
Project	Date	Version	page

the *state* in a complex way to generate what is termed *keystream*. A secure design will generate a keystream that is indistinguishable from a random string and which reveals no information about the state of the cipher. The cipher state is initialised using a user-supplied key and (typically) a publicly-known initialisation vector. By varying the value of the initialisation vector, different keystreams can be generated without the need to re-negotiate a new secret key.

Perhaps the two most cited stream ciphers in the literature are Rivest's RC4 and SNOW 2.0 [EJ03]. However they both have very large cipher states and a large cipher state translates directly into a significant area cost. To illustrate, estimates for the cost of implementing RC4 exceed 12000 GE while those for SNOW 2.0 exceed 7000 GE. Clearly these are entirely unsuitable for low-cost applications such as RFID tags. There are two ways forward.

First, it is well-known that a block cipher can be used as the basis for a stream cipher. This is done by using one of the standardized modes of use of a block cipher such as *counter* mode, *output feedback* mode, or *cipher feedback* mode [N01b]. Each mode has its advantages and disadvantages, but the resultant performance of the derived stream cipher will be close to that of the underlying block cipher.

A more satisfying second approach, and one which is more likely to yield better results, is to design a new hardware efficient stream cipher from scratch. The multi-year eSTREAM project [E04] finished in 2008 and one of the goals was to identify some new stream cipher designs that might be suitable for implementation in constrained hardware environments. Three ciphers are supported in the latest version of the portfolio [BdCC+08]: MICKEY v2 [BD08], Grain v1 [HJM08] and Trivium [dCP08].

A full overview of the hardware implementation costs of these algorithms is given in [GB08], and all three ciphers can be implemented in a couple of thousand gate equivalents with Grain v1 offering a particularly compact implementation of under 1500 GE and a very modest power consumption. However, it is worth observing that all three ciphers are new and so cryptanalytic advances in the coming months cannot be ruled out.

5.2.1.3 Hash Functions

The case of hash functions is a particularly challenging one. Not only are most commonly cited hash functions cryptographically compromised in some way, but they are very large when implemented in hardware. Much of this is due to the fact that they were explicitly designed for 32-bit processors and the operations they use are not particularly hardware friendly. The implementation characteristics of some common hash functions are given in [FR06, BLP+08] and reproduced here.

		Block Size	Cycles / Block	Throughput @ 100KHz	Logic μ m	Area GE
MD4	[R91]	128	456	112	0.13	7350
MD5	[R92]	128	612	84	0.13	8400
SHA-1	[N02]	160	1274	40	0.35	8120
SHA-256	[N02]	256	1128	45	0.35	10868

When the area available to security features is often estimated to be around 2000 GE, it is immediately apparent that none of the standard hash functions – irrespective of their cryptanalytic status – is suitable for deployment. Indeed, there are a variety of properties of hash functions that mean that their use in low-cost environments is likely to be problematic no matter which algorithm we choose.

RFID-AP	30/01/2009	1.0	35/44
Project	Date	Version	page

The most important point when using a hash function is to understand the exact security goals and why we are using a hash function in the first place. Classically, hash functions are described as having three properties:

- Collision-resistance; *i.e.* it is hard to find two inputs that hash to the same output.
- Pre-image resistance; *i.e.* given an output it is hard to find an input that gives this value.
- 2nd pre-image resistance; *i.e.* given an input-output pair, it is hard to find a second input that gives the same output value.

In the absence of any structural defect¹, the security of a hash function with regards to all three properties depends on the length of the hash output n (in bits). If we need collision-resistance, then a security level of 2^t is only attained if $n \geq 2t$. For pre-image and second pre-image resistance – properties that capture the notion of being one-way – if we desire a security level of 2^t then this can only be attained if $n \geq t$. Since increases to the output size n immediately increase the amount of state in the hash function and therefore the cost of an implementation, we can immediately see that n will be larger when we desire collision-resistance. If instead our application only requires one-wayness then we have the chance for a much more compact hash function.

Thankfully, in many applications we genuinely don't need collision-resistance. Instead we are using the hash function for its one-way properties and so we are often satisfied with a shorter hash output. That said we still have an absence of any real candidates. This problem was partially addressed in [BLP+08] where hash functions were constructed in an accepted way from the AES [N01a] and PRESENT [BKP+07]. While the results were partially successful, with the results being given below, this work serves instead to demonstrate just how difficult the field of hash functions – particularly compact hash functions – really is.

Block cipher based hash functions	Block Size	Cycles / Block	Throughput @ 100KHz	Logic μm	Area GE
PRESENT-based	64	547	15	0.18	1600
PRESENT-based	64	33	388	0.18	2530
PRESENT-based	128	559	11	0.18	2320
PRESENT-based	128	32	200	0.18	4256
AES-based	128	>1032	<12	<i>estimate</i>	> 4400

5.2.1.4 Message Authentication Codes

With regards to Message Authentication Codes (MACs) there are few dedicated proposals in wide-spread use. One can always use a block cipher in an appropriate mode of use, *e.g.* [N05] and so we could use a lightweight block cipher such as PRESENT. We can also build a MAC from a hash function [N08], but then this brings us back to the underlying problems with finding a suitable hash function. One recent dedicated proposal – called SQUASH [S08] – is certainly of some interest, but no specific details have been given except for a small, toy example for research purposes. Given this situation, it seems that lightweight message authentication codes might best be designed from a lightweight block cipher, in which case the performance characteristics of PRESENT, for instance, would be a good guide to what is possible, even if there might be some slight implementation overheads.

¹ Which unfortunately is not the case for MD4, MD5, and SHA-1.

RFID-AP	30/01/2009	1.0	36/44
Project	Date	Version	page

5.2.2 Asymmetric Cryptography

In asymmetric cryptography, the users – e.g. the senders and the receivers or the signers and the verifiers – use different key material. Depending on the application, this can help to simplify some of the key distribution problems encountered when using symmetric cryptography. However, since asymmetric primitives are built around hard mathematical problems, they are rarely amenable to compact implementation. We will however see one exception to this rule.

5.2.2.1 General Techniques: Encryption and Signatures

Asymmetric techniques are typically used in two ways. The first is as an encryption primitive and typically a session key that will be used for bulk symmetric encryption is exchanged between participants. The second use is as a signing primitive and a document or – as is more likely in the case of RFID-based applications – a challenge or a short string is signed using the private key of the owner. The correctness of the signature can be verified using a publicly-available public or verifying key.

There are typically three classes of asymmetric primitives available:

- Those based on the difficulty of factoring large numbers, such as RSA [RSA78].
- Those based on the difficulty of taking discrete logarithms, such as DSA [N00].
- Those based on the difficulty of taking elliptic curve discrete logarithms, such as ECDSA [N00].

Of the three types of hard problem, it is generally recognized that the most promising for compact implementation is that of elliptic curve discrete logarithms and there has been considerable effort in trying to provide the most compact implementation possible. The field of elliptic curves is complicated by the fact that there are different types of curves and different fields that one might be choose for an implementation. As a result, the field of results is large and growing all the time. That said, a brief survey of the most promising results [BGK+06, KP06] reveal that even the most compact implementations of the basic elliptic curve operations require of the order of 10,000 gate equivalents.

One asymmetric scheme that doesn't fall under the simple classification given above is called NTRU. Unfortunately the NTRU algorithms have not had the most trouble-free gestation and there are some doubts as to the security offered by the signature scheme. The encryption scheme is perhaps a bit more stable, and from publicly-available implementation figures it appears that a compact implementation of encryption might be attainable for several thousand gates [GKO+05]. However this is achieved at such a severe cost to the computation time that the implementation would be unusable.

However, despite this rather negative prognosis for asymmetric cryptography in RFID-tag applications, there is one technique that is very suitable and which has received increased attention and prototype implementation. Indeed, there are variants of the *cryptoGPS* identification scheme [GPS06] for which the *on-tag* memory and power consumption is less than that required by most symmetric techniques. At the same time the computational effort for the reader remains reasonable.

5.2.2.2 Dedicated Techniques: ID schemes

A public key identification scheme [MvOV] allows the possessor of a secret key to prove possession of that secret by means of an interactive protocol. Thus, in the case of an RFID deployment, the tag

RFID-AP	30/01/2009	1.0	37/44
Project	Date	Version	page

would *prove* that it contains a tag-specific secret to a reader and the reader is thereby assured that the tag is genuine. Only a device possessing the key could provide the necessary responses during interaction with the reader. While at first sight this might appear to be quite a specialised functionality, for instance we don't have the conventional public key services of encryption or digital signatures – though identification schemes can be converted to signature schemes in a standard way [MvOV] – interactive identification schemes have been deployed widely.

Among the family of identification schemes the *cryptoGPS* scheme allows a particularly compact implementation on the tag. An exposition of the scheme, its security and that of numerous variants, appears in a range of papers [G92, GPS06, PS98] and it is standardised within ISO/IEC 9798-5 [ISO9798-5]. There are many variants and optimisations of the scheme, but the variant using elliptic curve operations allows smaller keys.

Of particular practical interest are a series of optimisations that are designed to ease the computation and storage costs. One important optimisation is the use of *coupons*. These are a form of pre-computation and they are described in [G00]. Some storage optimisations are described in [GS94, ISO9798-5], and a particularly useful proposal termed the *Low Hamming Weight (LHW)* challenge is described in [GL04]. It is the combination of coupons with the LHW challenge that yields the best performance profile for implementation in resource-constrained environments.

The performance of *cryptoGPS* has been studied in a range of papers. An FPGA-based prototype exists [GJR07] and ASIC estimates from [McR07a, McR07b] are given below. Recall that the most compact implementation of the AES requires around 3400 GE while PRESENT requires 1000-1500 GE, though it should be observed that they would be used in a very different way to *cryptoGPS*.

	Datapath (bits)	Current μA	Cycles	Logic μm	Area GE
<i>cryptoGPS</i> (core computation)	1	0.61	1088	0.18	317
<i>cryptoGPS</i> (core computation)	8	0.67	136	0.18	431
<i>cryptoGPS</i> (core computation)	16	1.43	68	0.18	900

The accuracy of these estimates, along with a better understanding of the requirements for a fully-supported version will become clearer in time. In particular, the estimates given above are for the core *cryptoGPS* computation and any fully-functioning implementation will incur additional overheads. Nevertheless, asymmetric cryptography is within reach of the cheaper RFID-tags and its utility will depend much on the environment and application in mind.

5.3 Privacy-Preserving Authentication Protocols

In the following section, we present some prominent examples of recently proposed protocols that offer authentication and privacy for RFID-systems. Besides giving an overview about these proposals, we will point out their main disadvantages or weaknesses. Many recently proposed protocols for RFID-authentication and –privacy require usage of a strong, but expensive cryptographic hash function on the tag. Also, most of these protocols have been shown to be insecure or leak privacy. In conclusion, you can note that there is still a lack of lightweight, feasible protocol solutions for RFID that yet offer good protection of authenticity and privacy.

RFID-AP	30/01/2009	1.0	38/44
Project	Date	Version	page

5.3.1 YA-TRAP

In [T06], the tag sends the HMAC of the reader's challenge, keyed with a pairwise secret key, back to the reader. To protect against replay attacks, reader's challenges are numbers of ascending order. Therefore, the tag can reject old challenges. So in addition to an HMAC, a non-volatile state is required on the tag which, in many scenarios, might not be feasible or simply too expensive for a tag. This protocol is also prone against DoS-attacks and has been shown to leak privacy, see [JW07].

5.3.2 Hash Locks

The protocol of [WSRE03] uses a strong hash function and an HMAC-like computation for identification of a tag. Simply, for each authentication, the tag sends a random number together with the HMAC of this random number and the tag's ID to the reader. This, however, does not protect against replay attacks from the adversary: as there is no nonce from the reader involved in the protocol, an adversary receives always the same response on subsequent protocol instances with the same tag. This gives the adversary the opportunity to identify a single tag, thus breaking privacy, cf., [MW04].

5.3.3 Tree-based shared Keys

Using a tree-based setup, [MW04] hands out $O(\log n)$ secret keys to each tag. Each tag represents a leaf in a complete binary tree and receives a secret for each edge on the way towards the root of the tree. Authentication between reader and tag is then a "walking down" the tree of secrets until one tag, is uniquely defined. Yet, besides requiring a complex hash function, the amount of memory required on a tag to store the secret keys of this scheme might be infeasible in many scenarios. Also, privacy of this scheme is weak, as shown in [AO05]. To overcome these weaknesses, [AO05] proposes the OSK/AO protocol using hash-chains, an idea originally proposed in [AO05]. Yet, OSK/AO is also known to leak privacy, cf., [JW07], requires an expensive hash function and a state on the tag.

5.3.4 HB

Also within the HB+ protocol of [JW05], the tag shares a secret with the reader. After a receiving a challenge from the reader, the tag XORs a not completely randomly drawn, but biased "noise" vector to the challenge and sends the result back to the reader. The reader can then compute the tag's response by solving the Learning Parity with Noise (LPN) problem. Yet, this scheme and also many variants are known to be insecure or leak privacy, cf., [GRS05]. Also note that with HB+ and all variants based on LPN-schemes [W08], there will always be a potentially non-negligible probability that a valid tag gets rejected by the reader. This might not be acceptable in many scenarios

5.3.5 DPM

In [DM05], the authors propose a round-based communication setup. In each round, the tag computes the XOR of a secret key, again shared only by the tag and the reader, together with a per-round random number and sends the result ("alpha") to the reader. Additionally in each round, the tag computes the "DPM"-function of the round's random number. The DPM-function can be understood as a simplified, lightweight hash-function. This function computes the majorities of subsequent groups of three bits of the random number. Then, all computed majorities are XORed, and the resulting bit ("beta") is also sent to the reader.

RFID-AP	30/01/2009	1.0	39/44
Project	Date	Version	page

After transmitting the alphas and betas, the tag computes a keyed hash, using the secret key, and some initially exchanged nonces and sends the result to the reader. The reader computes for every key in its database, whether the DPM function applied to the XOR of each key and the received alpha equals beta. If this is not the case, this entry in the database is removed from the database, otherwise the reader continues with the next entry in the database. After many rounds, the database converges to a single key. This key is finally used to compute a keyed hash and to compare with the keyed hash received from the tag.

Again, this scheme requires an additional, but expensive hash function to protect against replay-attacks. Also, it has been shown in [vDR08] and [S08] that there exist attacks not only spoiling privacy, but also computation of 2/3 of the secret key.

RFID-AP	30/01/2009	1.0	40/44
Project	Date	Version	page

6 Conclusions

As more and more RFID-enabled systems enter our daily life, new security and privacy challenges arise. The identification of tags should be reliable so that adversaries cannot impersonate tags. At the same time the owners of tags want their privacy to be protected, so many users would prefer not to have their identity revealed either directly or by the linking of different events in the identification process.

In this report, we have presented a brief overview of the current state of the art for basic RFID systems as well as some of the security aspects. Different levels of abstraction have been considered, such as the physical aspects of communication and identification, the feasibility of cryptographic primitives, and also some of the higher-level protocols for authentication and privacy.

It is clear that the restricted hardware features of basic RFID tags allow a number of physical attacks that could be a hazard for privacy. These threats have been pointed out and detailed. However we have seen that there are several possibilities, besides pure cryptographic solutions, to protect the privacy of users and these require further study to see how easily they can be adapted to RFID tags. This will be subject to research in RFID-AP.

If we are to try and use cryptography, then we also run into some problems. While most commonly-used cryptographic solutions may run very well on PCs and servers, and some may even be suitable for smart cards with dedicated cryptographic co-processors, very few techniques are at all suitable for the highly constrained environments that we find in RFID tags. This has therefore been a very active area of research over the last years and there has been much progress. While some of the new techniques are inevitably somewhat immature, there is now a range of algorithms that could be suitable for different applications and which might help provide security solutions in pervasive low-cost deployments. It is one of the goals of the RFID-AP project to identify how easy it might be to integrate cryptographic technologies into existing application infrastructures such as that offered by EPCglobal.

Finally, as a dual to not having appropriate cryptographic primitives available, there are additional difficulties and challenges for the design of new identification or authentication protocols. In the context of RFID, the “new” security property of privacy plays an important and vital role. It is not sufficient anymore that an adversary cannot impersonate the owner of a valid tag; rather the privacy of the legitimate tag owner should be protected during the process of identification. In the world of RFID tags, the term privacy carries different nuances and meanings such as “anonymity”, “unlinkability”, or “untraceability”. Current work already provides first steps towards these formal notions of privacy and authentication properties in RFID. However, solutions so far fail to provide both, authentication and privacy at the same time, while also using lightweight primitives suited for today’s simple and low-cost tags.

The major goal of RFID-AP, therefore, is to try and bridge this gap and to focus on the design of identification protocols, providing both privacy and authentication, in such a way that they might be suitable for deployment on lightweight RFID tags.

RFID-AP	30/01/2009	1.0	41/44
Project	Date	Version	page

7 References

- [AO05] G. Avoine and P. Oechslin. RFID traceability: A multilayer problem. In A. Patrick and M. Yung, editors, *Financial Cryptography – FC ’05*, volume 3570 of *Lecture Notes in Computer Science*, pages 125–140. Springer-Verlag, 2005.
- [BdCC+08] S. Babbage, C. de Cannière, A. Canteaut, C. Cid, H. Gilbert, T. Johansson, M. Parker, B. Preneel, V. Rijmen, M. Robshaw. The eSTREAM Portfolio (rev. 1). September 2008. Available via www.ecrypt.eu.org/stream.
- [BD08] S. Babbage and M. Dodd. The MICKEY Stream Ciphers. In M. Robshaw and O. Billet, editors, *New Stream Cipher Designs: The eSTREAM Finalists*, volume 4986 of *LNCS*, pages 191-209. Springer-Verlag, 2008.
- [BGK+06] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls and I. Verbauwhede. An Elliptic Curve Processor Suitable for RFID-Tags. *IACR eprint*, July 2006. Available at <http://eprint.iacr.org/2006/227>.
- [BKL+07] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe. Present: An Ultra-Lightweight Block Cipher. In P. Paillier and I. Verbauwhede, editors, *Proceedings of CHES 2007*, volume 4727 of *LNCS*, pages 450-466. Springer-Verlag, 2007.
- [BLP+08] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, and Y. Seurin. RFID Tags and Hash Functions: Mind the Gap. In E. Oswald and P. Rohatgi, editors, *Proceedings of CHES 2008*, volume 5154 of *LNCS*, pages 283-299. Springer-Verlag, 2008.
- [dCP08] C. de Cannière and B. Preneel. Trivium. In M. Robshaw and O. Billet, editors, *New Stream Cipher Designs: The eSTREAM Finalists*, volume 4986 of *LNCS*, pages 244-266. Springer-Verlag, 2008.
- [CA06] Castelluccia, C., Avoine, G.: Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags. In: *Proceedings of CARDIS 2006*, pp. 289–299 (2006)
- [DM05] R. Di Pietro and R. Molva, Refik. Information confinement, privacy, and security in RFID systems, *European Symposium On Research In Computer Security*, September 24- 26, 2007, Dresden, Germany , pp 187-202.
- [DSH+06] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee. HIGHT: A New Block Cipher Suitable for Low-Resource Device. In L. Goubin and M. Matsui, editors, *Proceedings of CHES 2006*, volume 4249 of *LNCS*, pages 46-59, Springer-Verlag, 2006.
- [E04] ECRYPT Network of Excellence. The Stream Cipher Project: eSTREAM. Available via www.ecrypt.eu.org/stream.
- [EJ03] H. Englund and T. Johansson. A New Version of the Stream Cipher Snow. In K. Nyberg and H. Heyes, editors, *Proceedings of SAC 2002*, volume 2595 of *LNCS*, pages 47-61, Springer, 2003.
- [EPC] EPC Class-1 Generation 2 UHF RFID Conformance Requirements Specification.
- [FDW04] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems Using the AES Algorithm. In M. Joye and J.-J. Quisquater, editors, *Proceedings of CHES 2004*, volume 3156 of *LNCS*, pages 357-370. Springer-Verlag, 2004.
- [FR06] M. Feldhofer and C. Rechberger. A Case Against Currently Used Hash Functions in RFID Protocols. In *First International Workshop on Information Security (IS’06)*, volume 4277 of *LNCS*, pages 372-381, Springer-Verlag, 2006.
- [FK04] T. Finke, H. Kelter, (BSI): RFID - eavesdropping of communication between a reader and a transponder in case of ISO14443 system, Bonn 2004
- [GKO+05] G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar. State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks. In F. Stajano and R. Thomas, editors, *Proceedings of PerSec 2005*, IEEE Press, 2005.
- [G92] M. Girault. Self-certified Public Keys. In D. Davies, editor, *Proceedings of Eurocrypt ’91*, volume 547 of *LNCS*, pages 490-497, Springer-Verlag, 1992.
- [GRS05] Henri Gilbert, Matthew Robshaw, and Hervé Sibert. An Active Attack Against HB⁺ - A Provably Secure Lightweight Authentication Protocol. *IEE Electronics Letters*, volume 41, number 21, pages 1169-1170, 2005.
- [GRS08] Henri Gilbert, Matthew J. B. Robshaw, Yannick Seurin: HB#: Increasing the Security and Efficiency of HB. *EU-ROCRYPT 2008*:361-378
- [G00] M. Girault. Low-size Coupons for Low-cost IC Cards. In J. Domingo-Ferrer, D. Chan, and A. Watson, editors, *Proceedings of Cardis 2000*, *IFIP Conference Proceedings 180*, pages 39-50, Kluwer Academic Publishers, 2000.
- [GL04] M. Girault and D. Lefranc. Public Key Authentication With One (On-line) Single Addition. In M. Joye and J.J. Quisquater, editors, *Proceedings of CHES ’04*, volume 3156 of *LNCS*, pages 413-427, Springer-Verlag, 2004.

RFID-AP	30/01/2009	1.0	42/44
Project	Date	Version	page

- [GPS06] M. Girault, G. Poupard and J. Stern. On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order. *Journal of Cryptology*, pages 463-488, volume 19, number 4, 2006.
- [GS94] M. Girault and J. Stern. On the Length of Cryptographic Hash-values Used in Identification Schemes. In Y. Desmedt, editor, *Proceedings of Crypto '94*, volume 839 of LNCS, pages 202-215, Springer-Verlag, 1994.
- [GJR07] M. Girault, L. Juniot, and M.J.B. Robshaw. The Feasibility of On-the-Tag Public Key Cryptography. Presentation at Workshop on RFID Security – RFIDSec 07, July 2007.
- [GB06] B. Glover and H. Bhatt. *RFID Essentials*, O'Reilly, 2006, ISBN 0-596-00944-5.
- [GB08] T. Good and M. Benaissa. ASIC Hardware Performance. In M. Robshaw and O. Billet, editors, *New Stream Cipher Designs: The eSTREAM Finalists*, volume 4986 of LNCS, pages 267-294. Springer-Verlag, 2008.
- [H08] G. Hancke, University of Cambridge: Eavesdropping Attacks on High-Frequency RFID Tokens; July 11 2008
- [H05] Gerhard P. Hancke and Markus G. Kuhn, an RFID distance bounding protocol, March 2005. *IEEE SecureComm 2005*.
- [HJM08] M. Hell, T. Johansson and W. Meier. The Grain Family of Stream Ciphers. In M. Robshaw and O. Billet, editors, *New Stream Cipher Designs: The eSTREAM Finalists*, volume 4986 of LNCS, pages 179-190. Springer-Verlag, 2008.
- [ISO9798-5] ISO/IEC. International Standard ISO/IEC 9798 Part 5: Mechanisms Using Zero-knowledge Techniques. December, 2004
- [ISO14443] ISO 14443 Identification cards - Contactless integrated circuit cards - Proximity cards
- [ISO15693] ISO 15693 Identification cards - Contactless integrated circuit cards - Vicinity cards
- [JRS03] A. Juels, R.L. Rivest, M. Szydlo: Selective blocking of RFID tags for consumer privacy. In 10th Annual ACM CCS 2003, May 2003
- [JW05] Ari Juels, Stephen A. Weis: Authenticating Pervasive Devices with Human Protocols. *CRYPTO 2005*: 293-308
- [JW07] A. Juels and S. Weis. Defining strong privacy for RFID, *Proceedings of Percom Workshops 2007*, 342-347, 2007.
- [KP06] S. Kumar and C. Paar. Are Standards Compliant Elliptic Curve Cryptosystems Feasible on RFID? Presentation at Workshop on RFID Security – RFIDSec 06, July 2006.
- [LK05] C. Lim and T. Korkishko. mCrypton - A Lightweight Block Cipher for Security of Low-cost RFID Tags and Sensors. In J. Song, T. Kwon, and M. Yung, editors, *Proceedings of WISA'05*, volume 3786 of LNCS, pages 243-258, Springer-Verlag, 2005.
- [LPP+07] G. Leander, C. Paar, A. Poschmann, and K. Schramm. A Family of Lightweight Block Ciphers Based on DES Suited for RFID Applications. In A. Biryukov, editor, *Proceedings of FSE 2007*, volume 4593 of LNCS, pages 196-210, Springer-Verlag, 2007.
- [MW04] D. Molnar and D. Wagner, Privacy and security in library RFID: issues, practices, and architectures.
- [McR07a] M. McLoone and M.J.B. Robshaw. Public Key Cryptography and RFID. In M. Abe, editor, *Proceedings of CT-RSA2007*, volume 4377 of LNCS, pages 372-384, Springer, 2007.
- [McR07b] M. McLoone and M.J.B. Robshaw. New Architectures for Low-Cost Public Key Cryptography on RFID Tags. *IEEE International Symposium on Circuits and Systems, 2007 (ISCAS 2007)*, pages 1827-1830, ISBN: 1-4244-0921-7.
- [MvOV96] A. Menezes, P.C. van Oorschot, and S. Vanstone. *The Handbook of Applied Cryptography*. CRC Press, 1996.
- [N00] National Institute of Standards and Technology. FIPS 186-2: Digital Signature Standard (DSS), January 2000. Available from <http://csrc.nist.gov>.
- [N01a] National Institute of Standards and Technology. FIPS 197: Advanced Encryption Standard (AES), November 2001. Available from <http://csrc.nist.gov>.
- [N01b] National Institute of Standards and Technology. SP800-38A: Recommendations for Block Cipher Modes of Operation, December 2001. Available from <http://csrc.nist.gov>.
- [N02] National Institute of Standards and Technology. FIPS 180-2: Secure Hash Standard, August 2002. Available from <http://csrc.nist.gov>.
- [N05] National Institute of Standards and Technology. SP800-38B: Recommendations for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005. Available from <http://csrc.nist.gov>.

RFID-AP	30/01/2009	1.0	43/44
Project	Date	Version	page

- [N08] National Institute of Standards and Technology. FIPS 198-1: The Keyed-Hash Message Authentication Code, July 2008. Available from <http://csrc.nist.gov>.
- [PS98] G. Poupard and J. Stern. Security Analysis of a Practical "On the Fly" Authentication and Signature Generation. In K. Nyberg, editor, Proceedings of Eurocrypt '98, volume 1403 of LNCS, pages 422-436, Springer-Verlag, 1998.
- [R06a] M.R. Rieback, G.N. Gaydadjiev, B. Crispo, R.F.H. Hofman, A.S. Tanenbaum. "A Platform for RFID Security and Privacy Administration" 20th USENIX/SAGE Large Installation System Administration conference (LISA 2006), Washington DC, December 2006.
- [R06b] M.R. Rieback, Patrick N.D. Simpson, B. Crispo, A.S. Tanenbaum. "RFID Malware: Design Principles and Examples" Pervasive and Mobile Computing (PMC) Journal, vol. 2(4): 405-426, Elsevier, 2006.
- [R06c] M.R. Rieback, B. Crispo, A.S. Tanenbaum. "Is Your Cat Infected with a Computer Virus?" Proc. 4th IEEE Intl. Conf. on Pervasive Computing and Communications. (PerCom 2006), Pisa, Italy, March 2006.
- [R05a] M.R. Rieback, B. Crispo, A.S. Tanenbaum. "RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management." Proc. 10th Australasian Conference on Information Security and Privacy. (ACISP 2005), Brisbane, Australia, July 2005
- [R05b] M.R. Rieback, B. Crispo, A.S. Tanenbaum. Uniting Legislation with RFID Privacy-Enhancing Technologies. Proc. 3rd Conference on Security and Protection of Information. (SPI 2005), Brno, Czech Republic, May 2005.
- [R1] Rikcha study: Security Aspects and Prospective Applications of RFID Systems. Federal Office for Information Security (BSI) 2004.
- [RSA78] R.L. Rivest, A. Shamir, and L.M. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems, Communications of the ACM, pages 120-126, volume 21, number 2, 1978.
- [R91] R.L. Rivest. The MD4 Message-Digest Algorithm. In A. Menezes and S. Vanstone, editors, Proceedings of Crypto 1990, volume 537 of LNCS, pages 303-311, Springer-Verlag, 1991.
- [R92] R.L. Rivest. RFC 1321: The MD5 Message-Digest Algorithm, April 1992. Available from www.ietf.org/rfc/rfc1321.txt.
- [RPL+08] C. Rolfes, A. Poschmann, G. Leander, and C. Paar. Ultra-Lightweight Implementations for Smart Devices - Security for 1000 Gate Equivalents. In Proceedings of CARDIS 2008, to appear. Springer.
- [SA02] S. E. Sarma, S. A. Weis, and D.W. Engels. Radio-frequency identification systems. In Burton S. Kaliski Jr., C. etin Kaya Ko, c, and Christof Paar, editors, CHES '02, pages 454-469. Springer-Verlag, 2002. LNCS no. 2523.
- [S08] A. Shamir. SQUASH - a New MAC With Provable Security Properties for Highly Constrained Devices Such As RFID Tags. In K. Nyberg, editor, Proceedings of FSE 2008, to appear. Springer
- [So08] M. Soos. Analysing the Molva and Di Pietro Private RFID Authentication Scheme, Workshop on RFID Security, Budapest, Hungary, 2008, <http://events.iaik.tugraz.at/RFIDSec08/>
- [W08] S.A. Weiss, HB+ Protocol Information Page, <http://saweis.net/hbplus.shtml>, 2008.
- [vDR08] T. van Deursen and S. Radomirovic. Attacks on RFID Protocols, Cryptology ePrint Archive: Report 2008/310, 2008, <http://eprint.iacr.org/2008/310>
- [T06] G. Tsudik. YA-TRAP: yet another trivial RFID authentication protocol, Proceedings of Pervasive Computing and Communications Workshops (PerCom), 2006, ISBN: 0-7695-2520-2.
- [V07] S. Vaudenay. On Privacy Models for RFID. In K. Kurosawa, editor, Proceedings of Asiacrypt 2007, volume 4833 of LNCS, pages 68-87, Springer, 2007.
- [WSRE03] S.A. Weis, S.E. Sarma, R.L. Rivest and D.W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, Proceedings of Security in Pervasive Computing (SPC), LNCS, vol. 2802, pp. 201 – 212, 2003, ISBN 3-540-20887-9.

RFID-AP	30/01/2009	1.0	44/44
Project	Date	Version	page