Secure passive RFID technology in the Internet of Things

by

Manfred Aigner

A PhD Thesis
Presented to the Faculty of Computer Science in Partial Fulfillment of the Requirements for the PhD Degree

Assessors

Prof. Dr. Karl Christian Posch (TU Graz, Austria)
Prof. Dr. Rafael Pous (Universitat Pompeu Fabra, Spain)

April 2010

Institute for Applied Information Processing and Communications (IAIK)
Faculty of Informatics
Graz University of Technology, Austria

Abstract

The future development of existing technologies like Radio Frequency Identification (RFID) or Wireless Sensor Networks to an emerging and pervasive Internet of Things (IoT) is currently heavily discussed. Industry forecasts a big chance for new markets when everyday things are equipped with communicating chips. The academic community faces a lot of new research challenges in areas like antennae design, network architectures, communication protocols or security. Public bodies like to European Commission got interested in the development, since the expected changes on the society by the technology pose both, a threat or a chance for future society. In the public, privacy for end users is often discussed as the problem of technologies which use contact-less identification devices like passive Radio-Frequency Identification (RFID) tags.

We think that privacy protection is an important issue for this upcoming technology, but it is not the only one. In this thesis we explain why passive RFID technology will play a major role in the IoT and why it requires special attention when protection measures are discussed. We explain why security is an important topic in this context, and give suggestions how it should be addressed. We motivate our research by a service-oriented approach to security that differs from traditional concept of treating security as non-functional requirement. To achieve proper protection, we suggest using established cryptographic methods instead of proprietary and often undisclosed solutions.

In later sections we provide information about realized research activities in the area of secure RFID technology, by describing our initial goals, the most important results, and their impact. Our chronological description additionally illustrates the development of the research group I have been heading since 2003 from highly specialized digital Hardware (HW) designers, to a group which is now actively involved in design and implementation of security concepts and prototypes for future RFID applications. In the final section we give an outlook to activities planned in the near future and exhibit the impact of the achieved results on basis of their publications.

Acknowledgements

I'd like to express special thanks to following persons:

- My wife Gabriela: For staying with me, for bearing up with my grouchy periods while writing this text, and for painful proofreading of early versions of it.
- My parents and brothers: For raising me up and putting me on a very nice track for life.
- All current and former members of the VLSI research group at IAIK: For your motivation, excellent results and the exceptionally good mood during our work. For being a perfect team!
- Karl Christian Posch: For your very special way of teaching and motivating people and for all the important things I learned from you. For motivating me to finally finish this part of my career.
- Reinhard Posch: For giving me a perfect opportunity at IAIK to build up a research group and for your trust in my skills.
- All other colleagues at IAIK: For an interesting working environment with a lot of discussions, opportunities, and fun. For all the competent help and for funny discussions during coffee breaks or after work events.
- All project partners: For accepting the challenges during our research projects and for your motivation to deliver the projects often much better than necessary.
- All my friends: For spending not only the good times and for being there when necessary.

Manfred Aigner
Graz, April 2010

Contents

Abstract i

Acknowledgements iii

List of Figures ix

Acronyms xi

1 Introduction 1
1.1 Organization of this thesis 5

I The role of security and passive RFID in the Internet of Things 7

2 Passive RFID technology and the Internet of Things 9
2.1 The role of passive RFID in the IoT 12
2.1.1 Classification of tags 12
2.1.2 Use of tags in future applications 14
2.2 Components of RFID systems 15
2.3 Security for RFID 17
2.3.1 Kill command 18
2.3.2 Blocker tag 18
2.3.3 Proprietary crypto on tags 19
2.3.4 Pseudonyms for tags 19
2.3.5 Standardized crypto tags 20
2.4 Security for the Internet of Things 21
2.5 Comparison with Wireless Sensor Networks Wireless Sensor Network (WSN) 21

3 Security for passive RFID tags 23
3.1 The privacy discussion 23
3.2 Closed vs. open-loop RFID systems 25
3.3 Added value due to security services 26
3.3.1 Security service: Proof of origin or anti-cloning . . . 27

3.3.2 Security service: Protection against introduction of wrong or fake data 28
3.3.3 Security service: Data-integrity protection for data from tags 28
3.3.4 Security service: Access control for the tag's memory or commands 29
3.3.5 Security service: Protected or encrypted transactions between reader and tag 30
3.4 Wrong assumptions for development of secure RFID tags . 30
3.4.1 First wrong assumption: Implementation of real crypto on tags is technically not possible 30
3.4.2 Second wrong assumption: Hash modules are less power and area consuming than encryption modules 32
3.4.3 Third wrong assumption: A tag with crypto results in a contact-less smart card 32
3.5 Security flaws in existing products 33
3.5.1 Texas Instruments – Digital Signature Transponder (DST) 34
3.5.2 NXP – The Mifare™ incident 35
3.5.3 Keeloq™ – A successful attack using Side-Channel Analysis (SCA) 36
3.5.4 Future attacks 36
3.6 Trade-offs for security implementation on tags 37

II Research activities towards a secure Internet of Things 41

4 Research activities towards secure passive tags 43
4.1 Authentication for Long-Range RFID technology - ART 45
4.1.1 Introduction and project description 45
4.1.2 IAIK goals and objectives for Authentication for Long Range RFID Technology (ART) 46
4.1.3 IAIK results of the project 47
4.1.4 Impact of the project results 50
4.2 Secure NFC applications - SNAP 52
4.2.1 Introduction and project description of SNAP 52
4.2.2 IAIK goals and results of the project 56
4.2.3 Impact of the project results 60
4.3 BRIDGE, a large scale EC research project 62
4.3.1 Introduction and project description 62
4.3.2 Security activities in BRIDGE 63
4.3.3 IAIK goals and results of the project 66

4.3.4 Impact of the project results 70
4.4 Cryptographic protected tags for new RFID applications - CRYPTA 74
4.4.1 Introduction and project description 74
4.4.2 IAIK goals for the project 75
4.4.3 The project results 77
4.5 Workshop on RFID security 79
4.5.1 Introduction and workshop description 80
4.5.2 Goals and development of the workshop 80

III Future developments and conclusions 83

5 Future developments of RFID security research 85
5.1 Integration of passive tags into IP networks 86
5.2 Extended security services for RFID tags 87
5.3 Split computing and pre-computation 89
5.4 Indirect tag-to-tag communication 90
5.5 Protection for sensor-enabled passive tags 91
5.6 Electronic signatures for objects 94
5.7 Computation capabilities depending on reading distance . . 94

6 Conclusions 97

Bibliography 101

List of Figures

2.1 RFID system. 16

4.1 Smallest AES chip for RFID tags by Feldhofer. 47
4.2 Protocol extension proposed in ART. 48
4.3 A semi passive prototype tag. The 1^{st} version of the Demotag. 49
4.4 Left side: Pick-up of a mCoupon. Right side: Delivery at a cashier. 53
4.5 PDA with NFC interface, running the application mWallet. 55
4.6 Setup by Institute for Electrical Measurement and Measurement Signal Processing (EMT) to assess the outdoor eavesdropping distance. 56
4.7 Chip layout of the AES module with SCA countermeasures. 57
4.8 Result comparison of TINA chips. 58
4.9 IAIK HF demotag; a programmable RFID tag. 60
4.10 Early prototype of the semi-passive UHF demotag. 66
4.11 Final version of the IAIK UHF demotag design. 67
4.12 Comparison of different cryptographic primitives by Feldhofer, in respect to their suitability for application on RFID tags. 69
4.13 The architecture of the CRYPTA tag, as specified by the project partners. 76

Acronyms

AES Advanced Encryption Standard

ART Authentication for Long Range RFID Technology

BRIDGE Building Radiofrequency IDentification solutions for the Global Environment

CA Certificate Authority

CERN Conseil Europen pour la Recherche Nuclaire, or European Council for Nuclear Research

CLUART Contact-less Universal Asynchronous Receiver/Transmitter

CMOS Complementary Metal-Oxide Semiconductor

CPU Central Processing Unit

CRYPTA Cryptographic Protected Tags for new RFID Applications

C@R FP6 Project Collaboration Rural

DAA Direct Anonymous Attestation

DST Digital Signature Transponder

DoS Denial of Service

EC European Commission

ECC Elliptic Curve Cryptography

ECDSA Elliptic Curve Digital Signature Algorithm

EM Electro-Magnetic

ECRYPT European Network of Excellence in Cryptology

EMDA Electro-Magnetic Differential Analysis

EMT Institute for Electrical Measurement and Measurement Signal Processing

EPC Electronic Product Code

EPC Gen2 Electronic Product Code Class-1 Generation-2 UHF RFID Protocol

EPCIS EPC Information Service

EPCDS EPC Discovery Service

EPOSS European Technology Platform on Smart Systems Integration

EEPROM Electrically Erasable Programmable Read-only Memory

ETH Eidgenssische Technische Hochschule Zürich

ETSI European Telecommunications Standards Institute

FIPS Federal Information Processing Standard

ftp File Transfer Protocol

FPGA Field-Programmable Gate Array

FP6 IP Sixth Framework Programme, Integrated Project

GPS Girault, Poupard, Stern

GSM Global System for Mobile Communications

HF High Frequency

http Hypertext Transfer Protocol

HW Hardware

IAIK Institut fr angewandte Informationstechnologie und Kommunikationsverarbeitung

IC Integrated Circuit

ID Identifier

IGTE Institute for Fundamentals and Theory in Electrical Engineering

IP Intellectual Property

IPR Intellectual Property Rights

IPSec Internet Protocol Security

IPv6 Internet Protocol Version 6

IPv4 Internet Protocol Version 4

ISO International Standards Organization

IST Information Society Technology

IoT Internet of Things

MIT Massachusetts Institute of Technology

NFC Near Field Communication

ONS Object Name Service

PDA Personal Digital Assistent

PETRA Protocol Evaluation Tool for RFID Applications

PIA Privacy Impact Assessment

PKI Public Key Infrastructure

POS Point of Sale

PROACT Programme for Advanced Contactless Technology

RF Radio Frequency

RFID Radio-Frequency Identification

RFIDSec Workshop for RFID Security

RISC Reduced Instruction Set Computer

RTI Reusable Transport Items

SAML Security Assertion Markup Language

SCA Side-Channel Analysis

SCARD Side-Channel Attacks Resistant Design Flow

SCM Supply-Chain Management

sftp Secure File Transfer Protocol

SHA Secure Hash Algorithm

shttp Secure Hypertext Transfer Protocol

SME Small and Medium Enterprizes

SNAP Secure NFC Applications

ssh Secure Shell

SSL Secure Socket Layer

SW Software

TEA Tiny Encryption Algorithm

TI Texas Instruments

UHF Ultra High Frequency

UMTS Universal Mobile Telecommunications System

UID Unique Identifier

VLSI Very Large Scale Integration

WISP Wireless Identification and Sensing Platform

WSN Wireless Sensor Network

WWW World Wide Web

XACML eXtensible Access Control Markup Language

1 Introduction

This work presents a vision towards a secure Internet of Things. This vision is based on research which has been performed at IAIK's[1] *Very Large Scale Integration (VLSI) and Security* Group. Since the time when the author of this thesis has taken over the responsibility for coordination of the research group (in early 2003), this group has been consequently following a research direction towards secure RFID technology. We were one of the first in the community to argue that proper security means are necessary for proper development of RFID technology. At that time, applications of passive RFID technology were mainly treated as "IT for improvements of Supply-Chain Management (SCM)", or with different words, "RFID as a modern replacement of bar-codes." The improved reading distance and bulk-read performance of RFID tags over bar-codes were considered as the most important features of RFID technology. Most research in RFID technology was dedicated to logistics as application area. Based on assumptions from this application area, a system that neglected protection of the tags due to cost reasons was suggested. This back-end system for RFID applications is known today as Electronic Product Code (EPC) network. The idea was very successful and is today globally accepted as de-facto standard for RFID supported SCM applications. When the EPC network was defined, it was assumed that security issues can be covered at the network layer. Privacy and security issues for the tag-to-reader communication were neglected due to the fact that most supply-chain relevant operations take

[1] Institute for Applied Information Processing and Communications at Graz, University of Technology

place in a controlled environment. The inventors assumed that tags get destroyed or removed from the objects before they get into the hands of the end-customer.

From the beginning of our involvement in RFID research, our view of RFID technology was not restricted to SCM. While SCM is definitely an important application area for RFID, it is by far not the only one. Many assumptions which fit to SCM are not necessarily true for a more generic view on RFID technology. Especially those on security and privacy issues do not hold for other application areas, especially when the objects with the tags are carried by persons.

When we started to develop a protection concept for RFID tags, we considered applications where tags operate in unprotected environments. We looked at scenarios for RFID applications where end-customers and un-trusted parties were also involved. With this we came to the conclusion that proper protection of the tags and the communication between the tags and the readers are essential requirements for proper development of RFID technology. In contrast to other proposals we argued that low-cost protection of the tags will not be sufficient, since this low-cost protection for tags defines the overall security level of the system. A similar protection level as in all other parts of the whole RFID system is required for the tags and for the communication with them as well. Our vision has suggested protection of the communication link between readers and tags on basis of state-of-the-art cryptographic methods.

The feasibility of the implementation of cryptographic primitives under the fierce constraints for RFID tags was then doubted by researchers and industry. Therefore it was our first goal to prove the technical feasibility of implementation of modern encryption algorithms, so that they fulfill the requirements for passive tags. When a tag can execute cryptographic operations, one can build protection mechanisms based on this feature.

A second step was to demonstrate that protected communication is possible on basis of standardized RFID protocols. Our defined goal has been to propose extensions for security that do not require to replace all existing RFID infrastructure. We developed methods that can be implemented on basis of modification of firmware and middleware for existing reader products. Our solution ensures backwards compatibility; this means that protected tags still communicate with readers that do not use the security extension and secure readers still can communicate with unprotected tags. This compatibility is necessary for evolvement of current RFID systems towards protected systems due to economic reasons. A suggestion that requires to build a completely new infrastructure would practically fail due to lack of acceptance of the arising costs for such systems by the operators.

Consequentially, the next step has been to propose applications for secure RFID tags which would be infeasible using unprotected tags. We developed a new system for protected mobile coupons, comparable to a micro-

payment scheme. Alternatively we proposed solutions for anti-cloning and forgery protection for tagged items. The different applications use different RFID standards, (High Frequency (HF) and Ultra High Frequency (UHF) technology), to demonstrate that the protection methods are independent from the underlying communication standard.

Since 2003 a lot of published attacks on RFID applications and an intensive discussion about privacy implications of RFID technology show that our assumptions about the necessity of proper protection of tags have been correct.

Our results raised considerable interest by the academic community, but also by RFID industry. We were invited to contribute actively to standardization of RFID protection mechanisms in International Standards Organization (ISO) bodies. We submitted a suggestion as work item proposal which was accepted in an international ballot. The future ISO standard for protection of RFID communication between tags and readers is currently developed on basis of our suggestion.

Currently, the development towards the IoT is heavily discussed. We see passive RFID technology as a major building block for the future network which foresees communication with items. Protection of the RFID communication is necessary for the development of the Internet of Things. Many future applications will require protection of the data arising from communication with tagged items. Our protection concept which we have developed for passive RFID technology fits to the vision of the IoT.

The contribution of the author to the developments mentioned above is best described as the development and consistent implementation of a vision for a research group. When he has taken over the responsibility for coordination of the group, the small team was highly specialized towards the development of cryptographic modules for smart cards. One of the first tasks were to define the directions for future research.

We defined two main research directions; secure passive RFID and SCA. In a broader context, we refer to the area SCA as implementation security. After definition of the directions, actions for successful development of the group were taken. Based on profound know-how in VLSI implementation of cryptographic modules for smart cards, we investigated how to apply this know-how in new application areas, like RFID. To acquire necessary funding and to improve cross-linking with academic and industrial research groups, we initiated and submitted proposals for cooperative research projects. The author has taken responsibility for proposal development as well as leading roles in national and international cooperative research projects (project coordinator, scientific leader, workpackage leader etc.). While some projects were solely based on internal ideas (ART, SNAP, SCARD), others were initiated by partners, but the *VLSI and Security Group* contributed with their expertise in dedicated work packages. Before and at the beginning of his responsibility as group

leader, the author contributed mainly to technical research and development in the research areas side-channel analysis, SCA-countermeasure development, and hardware implementation of cryptographic algorithms. Results of this implementation-oriented research are publications on implementation of cryptographic primitives and countermeasures against SCA attack. The paper [64] presents results of an efficient hardware implementation of a Secure Hash Algorithm (SHA) primitive for Field-Programmable Gate Array (FPGA) technology. A flexible architecture for Advanced Encryption Standard (AES) implementation in hardware is presented in [50]. Countermeasures against SCA attacks on implementations of asymmetric cryptographic primitives are discussed in [58]. [4] explains the use of high-level models in the design flow to judge about the SCA susceptibility of the final implementation. Two patent applications for inventions resulted from the work in the area of SCA countermeasures [33] [63].

Due to successful acquisition and improved cooperation with RFID industry and academic research groups, the group grew steadily to a team of thirteen full-time researchers by 2008. Beside his work towards implementation oriented results, the author claims the successful development and implementation of the research agenda, for a period of six years, as his personal contribution. We think that our work produced results that significantly contributed to a re-thinking of the early assumptions about security in RFID systems. Visible results of the author's personal work in this respect are accepted national and international project proposals (ART, SNAP, BRIDGE, C@R, CRYPTA), successfully completed cooperative research projects under the coordination of the author (SCARD, ART, SNAP), as well as invitations to talks on conferences organized by academic and industry bodies (RFID Convocation, Odette Conference, EC-EPOSS Workshop). On a more technical level, the author contributed to articles for conferences and workshops. Papers about the authentication of RFID tags to readers [3] [19] and the design of an RFID based coupon system [2] [14] were accepted for presentation on conferences and workshops. The author held lectures on RFID security topics at the PROACT summer school and spring school (2006 and 2007), and as well on the 2^{nd} EURO-NF summer school 2009.

Meanwhile, the research group *VLSI and Security* is internationally accepted in both research directions that where defined and realized under the coordination of the author (Secure RFID and SCA). Although implementation security and SCA will be also an important topic for secure RFID tags, the content of this work is focused on the results of the research area RFID security. The success of the research group is the result of on many valuable contributions by all current and past team members.

Beside the activities in cooperative research projects, the author and his team were promoting and installing a workshop dedicated to the research area of RFID Security. In 2010, the seventh edition of the annual

Workshop for RFID Security will take place. The first, second and fourth edition was organized by the *VLSI and Security* group. Meanwhile, a steering committee of acknowledged researchers was introduced to guarantee further development of the workshop towards the leading workshop for RFID-security topics.

1.1 Organization of this thesis

As initially stated, this work describes a vision towards a secure Internet of Things. The second chapter describes the relationship between passive RFID technology and the communication concept for the future which is currently discussed as the Internet of Things. The third chapter provides details on our view on protection for passive RFID systems. All assumptions and reflections are still valid for the evolvement of the technology towards the IoT. Chapter four deals with successfully conducted projects and the results of our research achieved during the recent years. It documents the advances achieved in the research field of RFID Security and our development as research team. Additionally, we mention the major outcomes of the research projects which we were involved in. Chapter six gives an outlook to future work, which will concentrate on. It describes developments that enable the development of the IoT and it explains how we envision the integration of secure RFID technology into a heterogeneous network without necessarily reducing of the security level. A final section summarizes the contributions of this thesis and draws the conclusions about the presented work.

Part I

The role of security and passive RFID in the Internet of Things

2

Passive RFID technology and the Internet of Things

The "Internet of Things" has meanwhile become a scientific discipline that deals with the interlink of physical objects and the Internet. Various technologies are discussed as building blocks of this development, like RFID, short-range communications, ultra wide band communications, real-time localization, WSN, or ad-hoc networks. In 2008 the first version of the international Conference "The Internet of Things" took place[1]. New business models, technologies and applications were discussed. The European Commission organized a series of workshops[2] to develop a research road-map that should ensure proper development.

Currently there is no clear definition of the term Internet of Things established. In Wikipedia it is simple referred to as *"Network of Objects [...]"* or *"a system [...] that would be able to instantaneously identify any kind of object.* The European Commission explains the Internet of Things[3] as *"one major next step in this development of the Internet, which is to progressively evolve from a network of interconnected computers to a network of interconnected objects*". The authors of [25] describe it as *"number of technologies [...] that enable the Internet to reach out into the real world of physical objects.*

[1] http://www.the-internet-of-things.org/

[2] http://www.smart-systems-integration.org/public/internet-of-things

[3] Commission of the European Communities (18.6.2009). "Internet of Things An action plan for Europe"

The Internet of Things will be characterized by communication between objects without human interaction, rather than data transfer between computers that are operated by persons. In the traditional Internet, as we know it today, most communication is triggered by human interaction, e.g. when we open a web-page or send an email with attachments to the mailbox of a recipient. Communication in the Internet of Things will be enabled when e.g. objects enter into the area that is covered by a reader device. While present within the reading range, it may connect to a server for inventory or object tracing purposes in a supply-chain. An autonomous node in a network of sensor nodes might issue an alarm to a controlling system as soon as it measures a critical value.

Although we can foresee some scenarios for applications using the Internet of Things, it is impossible to correctly predict typical applications or killer applications of this upcoming network. Similar to the development of the Internet we will face new classes of applications that are hard or even impossible to forecast (remember e.g. the development of Web 2.0 that is based on user-generated content). Nevertheless, already today we can foresee that a big number of applications will need security measures as a prerequisite for successful launches. We can easily compare the situation with the World Wide Web (WWW) in its first years. At the beginning the Internet was a network that combined servers from various universities. Facilitated data exchange was the first use case for the network. All involved parties basically trusted each other and first applications did not really require protection, but the goal was to establish a connection for exchange of data. When CERN came up with their first version of the WWW the basic idea was to have a presentation platform for research results to an interested audience. Newspapers started to use the web as platform and companies used it to provide information about their products. More advanced applications like electronic banking or webshops were not possible until protection of the communication was established. Due to the high risk of fraud no company would provide access to critical data via the web without secure authentication of the servers and encrypted communication between server and clients. Looking at current killer applications in the Internet, most of them use some sort of security measures. Especially for commercial services it is necessary to achieve the secure authentication of communication partners and protection of the stored data against attacks. The short history of the Internet has shown that it is necessary to protect any server that hosts valuable data or services, we can assume that this will also account for the Internet of Things. To illustrate this statement, we distinguish three different classes of protection for applications in the Internet:

- *Protection of servers against intrusion and Denial of Service (DoS):* Any server holding valuable data needs to be protected against mod-

ification of its content. Although it is often not visible to a standard user, companies (like Google or Yahoo) need to protect their servers against illicit access and denial of service attacks. Strict access control, firewalls and other measures are used to protect the servers. The main motivation for protection is the commercial value of their service and data. If databases or web-pages were modified by attackers their business would seriously suffer.

- *Authenticated access:* Many applications require authentication of the client to grant access to specific data and services. Typically the end-user needs to log in to receive personalized services or data. As example you can think of web-based email or platforms to share photos. The service provides only the data that the logged-in end user should have access to. On the other hand the authentication protects the end-user's data from access by other, probably unknown users. Nobody would use e.g. a web-based email service that would automatically allow any other users to access personal data. It is therefore necessary for the service provider to protect the servers in a similar way as above, but additionally to demonstrate to the end-users that their personal data is protected from access by others. In some applications like e.g. platforms for sharing photos or videos, end users may grant access to other users or groups of users.

- *Encrypted connection:* The third class of applications requires more protection. In some cases, access control to data is not enough, but the transfer of data is critical. The application needs to make sure that the data is not modified or eavesdropped on its way between the server and the client. Any webshop with payment facility falls into this category. The end-user wants to be sure that information about his credit card is neither eavesdropped nor modified when transferred to the server. Additionally to protection of the servers against illicit access and authentication to grant the proper access rights, these class of applications requires encryption of the transferred data and integrity checks. Before encrypting it is necessary that both communication partners authenticate to each other, otherwise an attacker could easily claim a wrong identity and communicate perfectly encrypted with the victims.

During the development of the Internet, important but insecure services were replaced step by step with functionally equivalent protected versions. Instead of remote login via *telnet* or *rlogin*, nowadays *Secure Shell (ssh)* is typically used to establish a remote connection to a computer. Instead of transferring files via the insecure *File Transfer Protocol (ftp)*, nowadays the protected version *Secure File Transfer Protocol (sftp)* is typically used. Due

to the high number of successful attacks on unprotected services, nearly all firewalls block access to such insecure services by default.

The development of the Internet of Things is currently in an early phase. First applications are currently developed; most of them operate in a closed-loop environment, without public access. Technology to interact with the network is not yet pervasively installed, but already available. Based on the development in the Internet we can foresee similar security requirements for applications in the new network.

2.1 The role of passive RFID in the IoT

The term RFID is not well defined, nor consistently used in the scientific literature. RFID stands for Radio Frequency Identification, so in principle for any technology that transmits an identifying information via radio-frequency. Friend or foe identification systems for aircrafts are presumed to be the predecessors of modern RFID systems. Modern RFID systems consist of tags or transponders which are able to store an identifying number. As soon as they enter the range of a reading device they transfer their Identifier (ID).

2.1.1 Classification of tags

Different classifications for RFID tags exist. Due to the enormous difference of technology used for design and production of different transponders, it is useful to classify them for better understanding. In the following paragraphs we provide classifications of tags which we will use in the remaining parts.

Concerning their communication principles and power supply, transponders are separated into active, passive and semi-passive types:

- *Active tags* use their own power supply, therefore they can actively send information which leads typically to a longer reading distance. The tag's battery limits the lifetime of the tags and increases the costs of such tags significantly.

- *Passive tags* draw all the power they need for operation from the reader's EM-field. The communication from the tag to the reader is performed by modifying the reader's signal passively, by e.g. load modulation of the provided field or back-scattering of signals. High-volume production allows to provide such tags at very low cost. The functionality of passive tags, which can operate in longer distances from a reader is very restricted due to the low power that can be extracted from the surrounding EM-field.

- *Semi-passive tags* are a hybrid of the previously described tags. They communicate passively, but they have their own power supply, typically used for additional functionality. While passive tags only operate when a reader field is available, semi-passive tags can e.g. sample data via attached sensors also when no reader field is available. Currently they do not play an important role but with upcoming applications for sensor tags they will become more relevant in future RFID applications.

In the context of this thesis, passive RFID tags are the most interesting ones. Due to their low production costs they can be attached to basically any object in our surroundings. A variety of different passive RFID transponders exist.

Out of these passive tags, the most powerful class—in terms of computation capabilities—are currently contact-less smart cards. They communicate with readers in a reading distance of up to some centimeters. Often, they are used as security devices for access control systems or as secure token in ticketing systems. The short reading distance is not a restriction, but actually a feature—the user is forced to bring the card close to an access point to trigger deliberately a transaction. Due to the short reading distance, the contact-less device receives more power from the reader, so that even complicated cryptographic operations are possible. The contact-less interface replaces the contact-based smart card interface; instead of sliding the card into the smart card reader it is brought close to the reading point. This improves both, user convenience and transaction speed.

Another sort of tags is designed for longer reading distances. Such tags are typically used in supply chain automation. They are optimized for lowest power consumption and low production cost, since their typical applications use a very high number of tags. Additionally the applications require that all tags in the reader field can be detected in short time. The functionality of such RFID tags is reduced to the execution of a protocol that supports anti-collision of concurrent answers and transmission of a unique identifier.

Those low-cost RFID tags with long reading distance are important devices in the context of the future IoT. They will appear in a high number and new applications will make use of their presence. Although the physical appearance of these tags is very similar to contact-less smart cards, their implementation is very different due to the different design requirements for reading distance and unit costs. In the remainder of this thesis we will refer with the term *RFID tag* or *RFID transponder* to this specific sort of tags which are built to operate in higher reading distances. In case that we mean another sort of tags, we will clearly mention this.

A different classification of RFID tags was published by EPCglobal in [18]. This classification is comminly accepted by the scientific community,

and in this thesis we also refer to this classification, when appropriate. In the following we provide a short description of the defined classes of tags according EPCglobal:

- *Class-1 or Identity Tags:* This sort of tags defines the least-cost tags with minimal functionality. They can provide their Unique Identifier (UID) and the electronic product code identifier (EPC) for the product they are attached to. Typically, they accept a command that permanently kills them. They may provide password-protected access control and additional user memory to write to and read from.

- *Class-2 or Higher-Functionality Tags:* These tags include additionally an extended tag ID, extended user memory and authenticated access control. The specification of this class is not yet completed at the time of writing of this thesis.

- *Class-3 or Battery Assisted Passive Tags:* Class 3 tags communicate passively (they modify a reader field) but might use a battery supply to enable additional functionality, e.g. sensing of environmental effects. The classification of Class-3 tags is still very open, but it matches our description of "semi-passive tags" from above.

- *Class-4 or Active Tags:* Beside an extended tag ID and their own power supply, these tags feature authenticated access control and extended user memory. Additionally, they can be equipped with sensors with and without data-logging. In contrast to Class-3 tags, they use active communication therefore they can initiate communication to a reader or to other tags. Their classification equals the description of "active tags" from above.

2.1.2 Use of tags in future applications

We can assume that the tags of Class-1 and Class-2 will make up the majority of devices in the Internet of Things. Those low cost tags—when attached to a physical object—will provide an electronic identity of objects. The marginal cost increase due to tagging enables that a very high number of things will be tagged for participating in the network.

Class-1 tags are nowadays used in applications for supply chain automation. Currently, around one billion of tags are produced worldwide per year. The costs for such tags are already below € 0.05[4]. The costs of Class-2 tags will be higher, but still in the same cost segment. Class-3 and Class-4 tags will have much higher costs and therefore appear in a much lower number.

[4]information from http://www.rfidjournal.com/faq/20/85

Nowadays, most tags are used in applications in the logistics domain. To optimize processes in the supply chain for retailers, pallets and transport cases are tagged to allow real-time tracking of goods. Portals with readers are placed on important points of such supply chains, e.g. on exit gates of production halls and entry gates of distribution centers and warehouses. The requirements for reading distance and reading rates are very specific. The specification for Class-1 tags was defined to meet the requirements of such applications at minimal tag costs. Most of the currently installed systems operate as closed-loop applications; this means that the readers and servers are operating in a protected environment and by trusted parties and personnel. Currently, we observe a shift towards an open infrastructure that allows access of multiple parties to data on the tags, and the network services.

The future Internet of Things will allow homogenous access to tags from and to the traditional Internet, as well as compatibility to ad-hoc sensor networks and other networks of mobile devices (e.g. devices operating in GSM or UMTS networks). In this network, the passive tags of Class-1 and Class-2 will be the devices with least performance and therefore mark the lower barrier for data throughput. If we compare passive RFID tags with other wireless connected devices like sensor nodes, we realize a dramatic difference in the power consumption of the circuits. With given voltage levels, the power consumption directly translates to the continuous current consumption of the circuits. While battery-operated devices or passive smart cards typically have an average continuous current consumption between 10mA and 100mA, the circuits of passive RFID reset themselves when the power consumption exceeds $10\mu A$ to $20\mu A$. The low level of energy available in the reader's EM field at the maximal reading distance and the minimal size of the chip and the antenna prevents higher power consumption for RFID tags. We observe a difference of power levels of a factor higher that 1000 between passive RFID tags and battery-operated devices or contact-less smart cards. This will not change in the next years, since the given parameters for reading distance and antennae size or chip size will not change in near future. The power consumption of the circuits themselves will be reduced following Moore's Law [53]. Nevertheless, it will take very long until today's RFID tags will provide similar capabilities as today's sensor nodes or similar battery-operated devices.

2.2 Components of RFID systems

An RFID system consist of several components with very different requirements and limitations (see Figure 2.1). Those components will be part of the future IoT or they will be replaced by components provided by the IoT. For better comprehension, we shortly describe those main components as

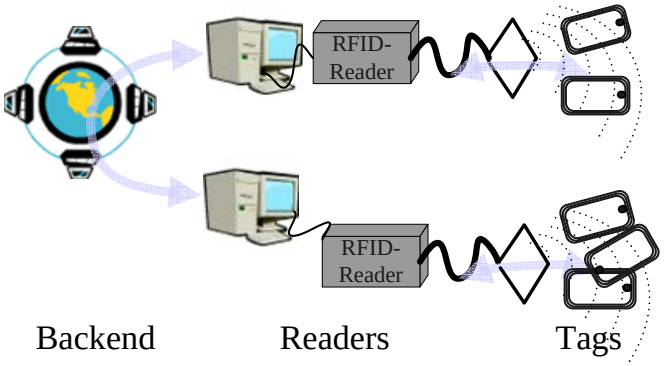

Figure 2.1: RFID system.

they appear in today's systems:

- *Backend*: Depending on the complexity of the application, the backend may consist of a single computer with a database or of a network of computers and databases. Data about RFID tags (typically their ID) are transmitted from the readers to this database. RFID applications make use of the stored information. The computers of the backend have practically unlimited computing capabilities, their communication interfaces are broadband connections with very high communication rates.

- *RFID Reader:* An RFID system contains at least one, but typically several readers. RFID readers are usually peripherals for normal PCs, but there are also mobile RFID readers available. We consider an RFID reader as a combination of the RFID reader peripheral with a PC or a mobile computing device like a Personal Digital Assistent (PDA). The readers can connect via any Internet connection to the backend system. Communication to the tags is performed via the wireless interface. The reader can communicate with the tags that are present within the reading distance. This can be more than one tag at the same time. The reader devices have rather high computing power. Their connection to the backend allows for high speed transmission. Compared to the rather slow contactless channel, the communication with the backend has unlimited bandwidth.

- *Tags:* The tags or transponders are electronic devices with very restricted computing capabilities. They communicate exclusively to readers in a point-to-point manner (only one reader at the same

time). The interface between tags and readers is not suitable for high throughput communication. At any moment one or more tags can be present in the reading distance of a reader.

If all parts of such a system are under control of one party, or of several parties who mutually trust each others, we speak of closed-loop applications. Open-loop applications allow remote data access to the backend for other parties, or include readers that are placed outside a trusted area.

2.3 Security for RFID

Passive tags play an important role when the security in the IoT is discussed. They are the devices with least performance in the overall systems, therefore their computational capabilities and their limited communication bandwidth has to be considered when overall security mechanisms are defined. In this section we look at the development of passive RFID technology in respect of security.

In 1999 the Auto ID Center at MIT started to promote their vision towards "The Networked Physical World" [66]. One of their starting assumption was that only inexpensive tags can enable the development of RFID technology [67]. Automation of supply-chain management by tagging of every produced good was defined as the application for this new network. They developed a system based on very limited functionality provided by the tags, to allow production of such low-cost tags for a price below 5 ¢. All computations and decisions were considered to be executed by the network to keep the chip area, and thus the cost for a tag as low as possible. Security requirements for the tags were not considered, but the tags should hold a permanent ID and EPC, and transfer it whenever requested by a reader.

A consequence of the necessary Unique Identifier (UID) for each tag and each tagged object (EPC), an extensive discussion on privacy implications occurred. When the UID of a tag or an object can be directly or indirectly mapped to a person who carries the object, the data-protection problem is indeed significant because the information available from the tag is then considered as "personal data", which has to be protected against illegal access. In the closed-loop supply-chain application this is not necessarily a problem. In those scenarios an object is often not connected to a specific person. The problem starts at the point of sale, where a customer takes over a tagged object. Together with a potential payment by credit card, the link between identity of the person and the tagged object can easily be performed. Since a low-cost tag—as used in supply chain automation—answers its ID to any reader the person could be identified without knowing it. In such cases, the rights for privacy of end customers are be perpetrated.

2.3.1 Kill command

A straightforward solution to this privacy problem is to disable the tags at the Point of Sale (POS), so that tags are not operating anymore when the end consumer takes over the tagged goods. The so-called *kill command* was introduced in the tag communication protocol and when a tag receives such a command it disables itself unrecoverable. This approach solves the privacy problems for supply-chain application, but it raises others:

- *No after-POS application of tags:* When tags are killed at the POS, they cannot be used in other applications. Often tags are integrated in the objects, so they could be easily used in processes like warranty refund or disposal. Due to the use of the kill command to tackle the privacy problem, we lose a lot of additional benefits of tagged objects.
- *Unwanted execution of the kill command:* A supply-chain management system that relies on the information of the tags can be jammed by executing kill commands for tags while they are still in the supply chain, e.g. during loading or unloading of goods from and to a lorry. For most tags, the kill command can be protected by a password that needs to be sent to the tag before it accepts the command. Managing such passwords is quite complex, if each tag uses a different password. On the other hand, it is easy to eavesdrop and reuse passwords, if a password is used for more than one tag.

2.3.2 Blocker tag

The blocker tag is a suggestion by RSA Security to cope with the privacy problem [42]. It is a tag that can be attached to a shopping bag to protect the end consumer from unwanted reading. As long as the blocker tag is in the same reader field as other tags, the reader is not able to communicate with the tags, because the blocker tag prevents the resolving of collisions. The blocker tag's functionality is comparable with a jamming device that disturbs the communication, but instead of jamming the EM field, the blocker tag blocks the communication at the protocol level. During the anti-collision procedure, the blocker tag appears to the reader as an infinite number of tags. It is therefore impossible to serialize the communication slots. The solution is effective, but has several drawbacks. It might be possible that a tag in the pocket is within the reading distance of a reader while the blocker tag of the bag is not. In this case it might still be possible to read certain tags. For many products it might be impossible or not desirable to put a bag around it (wrist watch) so an end consumer would need to apply a blocker tag near working tags to be protected. Additionally, a blocker tag will also block wanted RFID communication, if it is unintentionally brought into the reader field, of e.g. an automatic

cashier reader. Finally we can observe that the solution to apply blocker tags puts burden and potential costs on the end-consumer to protect his privacy, which is far from ideal. End-users will not accept additional costs or effort as long as no benefit is visible for them.

2.3.3 Proprietary crypto on tags

Due to the very restricted requirements for low-cost RFID tags, it was often proposed to use proprietary protection measures for RFID tags. This argument follows an assumption that published algorithms might use higher resources during execution and that undisclosed encryption algorithms might provide an accepted security level. Very successful RFID-tag products have been produced following this assumption. One example is the first version of Philips' MIFARE tags which used the undisclosed CRYPTO1 algorithm [55], another TI's DST [44] using DST40 as cryptographic primitive. Both approaches were meanwhile broken by academic groups [29] [8]. When proprietary algorithms are used, one needs to consider that the chance for successful attacks gets very high as soon as secret details about the encryption algorithm become public. The decision of such an approach is reasonable for specific application; however application of undisclosed primitives for protection of an open network, as it is considered for the Internet of Things, is not meaningful.

2.3.4 Pseudonyms for tags

A tag pseudonym is a changing ID that appears to a non-authorized reader as random number. Only authorized readers should be able to dissolve the pseudonym to find out the real ID of the tag. Typically, a central computing centre is involved that dissolves the pseudonym for the distributed readers. To fully tackle the privacy problem, it is necessary that the ID changes every time when a tag is read so that tracing for collected pseudonyms gets useless. Various schemes to generate pseudonyms on tags and to find their real ID efficiently were published in the recent years [52]. At the beginning, these approaches suffered from the wrong assumption that hash primitives would be more efficient to compute on tags than encryption primitives. This assumption is meanwhile shown to be wrong [23], but still alive in many scientific publications. So far, only one prototype implementation of a pseudonym scheme that demonstrates the feasibility for implementation with RFID technology was published [72] [73]. The requirements for the tags non-volatile memory are rather high due to a higher number of keys that needs to be stored on the tags. The centralized nature of the computation centre is feasible for e.g. an application in a closed-loop system (e.g. library), but prevents many possible applications in the open Internet of

Things. Additionally, the computational load on the computation centre is very high when a high number of tags is participating in the system.

2.3.5 Standardized crypto tags

Meanwhile it is established as good practice to use standardized cryptographic primitives and protocols for security operations in the Internet. Following Kerckhoffs' principle [47], all parts of the cryptographic system, except the key must not rely on secrets. During the standardization phase of public algorithms or protocols an open evaluation is carried out, so that potential security holes can be detected and corrected. It is very hard to get the same level of confidence for proprietary solutions. The security level of standardized solutions is known and if new attack techniques could harm such algorithms it is normally known well before a practical attack is possible. This allows reaction on new developments before real attacks are feasible.

Design of open systems prevents the application of secret algorithms and protocols, since it would be very likely that attackers would get access to the secret it is know by many parties.

A variety of standards for secure communication exist, driven by bodies like ISO or ETSI. Those standards include cryptographic algorithms (e.g. Federal Information Processing Standard (FIPS)-197 or AES) but also protocols (e.g. ISO/IEC 9796 Information Technology Security Techniques).

Comparing standardized solutions with ad-hoc solutions for a specific application, they often seem to be less efficient. After a closer look, often new flaws are detected in the ad-hoc solutions, and after fixing them the overall performance gain is lost. For many years it was argued that due to the restricted power budget the implementation of standardized cryptographic primitives is not possible on RFID tags. The results from our research projects show that current technology allows the implementation of such algorithms without any restriction of the reading distance. In Chapter 4 we will describe these results in more detail. Comparing the increase of chip area of proprietary algorithms with the one of standardized algorithms we come to the conclusion that the possible benefit of proprietary solutions does not justify the arising security risk.

The possible decrease of chip area by application of proprietary algorithms instead of standardized algorithms does in our opinion not justify the arising security risks.

We think that using established and standardized protection measures are meaningful for RFID tags is the only way towards secure RFID and IoT. If carefully selected and properly implemented, they can be used also on tags. In chapter 3 we will provide more arguments why this approach is meaningful.

2.4 Security for the Internet of Things

For proper establishment of an open Internet of Things we foresee security as a service enabler. As in the Internet there will be still some applications without security requirements. Nevertheless, especially applications with commercial background will require protection of the data that is communicated. With the term protection we do not only refer to encrypted communication, but also other security features. To protect the privacy of people who carry tagged goods, encryption of the tag's communication is certainly an important feature, but it is not the only one.

Data integrity in end-to-end connections with passive tags is certainly an important feature. When an application communicates with a remote tag, via a reader and other servers that are not under own control, it will be important to detect whether the data originating from the tag was not modified on its way. Vice versa, it will be important that data that is supposed to be stored on a tag was not modified on its way to the tag.

As soon as networked readers—which are not under sole control of the application provider—are used in applications, tags will need to check the authenticity of the data that should be stored on the tag. Authentication of tags to readers will be an important feature to protect IoT applications from data introduced by fake tags. To avoid illicit changes of the content or the configuration of tags, reader authentication will be necessary. Tags with signature functionality can ensure the integrity of data originating from them, even if the data is transferred via a non-trusted network.

2.5 Comparison with Wireless Sensor Networks WSN

In many publications, wireless sensor nodes and ad-hoc networks of such nodes are referred to as the most important technology for the Internet of Things. The technology behind sensor nodes and ad-hoc networks is challenging and it is obvious that there will be important future applications which use sensor nodes and ad-hoc networks. We do not consider them as special cases in the context of this work for the following reasons:

- *Number of devices:* The number of devices participating in the Internet of Things will be very high when considering that most of our objects are tagged with passive RFID tags. Due to the costs of sensor nodes and the need for a energy source, we do currently not consider that everyday objects will be tagged with sensor nodes. Comparing the number of devices that will contribute to the network, we can see that sensor nodes will not contribute with a significant number. Currently, about one billion tags are produced per year — most of

them to be used in logistic processes. The number of produced sensor nodes is of a much lower dimension.

- *Computational capabilities of WSN:* Sensor nodes do not operate passively. This means that they have their own power source. Although energy consumption is a critical factor for the lifetime of the nodes, the continuous power consumption has no strict limit. As a consequence, sensor nodes feature very powerful processors compared with the available computing power of passive RFID circuits. Current passive RFID tags use only $\frac{1}{1000}$ and less of the power consumption of battery-powered sensor nodes.

  Although improvements in silicon technology will improve the computational capabilities of tags, it is not foreseeable that an improvement by a factor of 1000 will be achieved in the next years, so that RFID tags would have the same computational capabilities as today's sensor nodes. Sooner it can be expected that the performance of future sensor node processors will be comparable with the one of today's desktop computers. Current state-of-the-art sensor nodes[5] feature 32-bit Reduced Instruction Set Computer (RISC) processors, and run a Java virtual machines for comfortable application development. Complex calculations as required for cryptographic operations can be performed without significant delay. In the context of this thesis we do treat sensor nodes as devices with basically unlimited computing power, as todays desktop PCs or hand-held computers.

- *Network connection and protection:* Sensor nodes operate in ad-hoc network infrastructures, often in peer-to-peer architectures. All nodes communicate actively with other nodes in their range, special gateways or base stations provide a bridge to other networks, e.g. via gateway servers to the Internet. Their communication principle is very different from RFID technology where tags communicate passively in a point-to-point manner with one reader device.

[5] e.g. Sun SPOTS from Sun Microsystems https://spots.dev.java.net/

3 Security for passive RFID tags

In the early years of passive RFID technology, security was not considered as an important topic. Passive RFID tags were considered to replace bar codes for applications in the supply chain. While security measures for smart-card technology were transferred to contact-less smart cards, the primary goal for the design of RFID tags was cost saving, and therefore minimal functionality of the tags themselves. The advantages over bar codes, like improved reading distance, bulk reading, and no need for direct line of sight, were addressed. The resulting security concerns (tag cloning, eavesdropping etc.) were not taken into consideration. This chapter outlines the development of the security topic in the context of RFID applications. We focus on passive RFID technology for longer reading distance without discussing the development of contact-less smart-card technology.

3.1 The privacy discussion

Soon after the presentation of first ideas for applications of RFID technology, an intense public discussion about the technology's privacy implications emerged. This public discussion was mainly driven by privacy activists and consumer advocates and was based on many factoids.

The RFID tag producing industry ignored the discussion for a rather long time. It did not react on the statements, but claimed that RFID technology does not have any privacy implication, as long as RFID tags do not hold personal data. This statement is only true for a very specific selection

of applications. In the closed-loop supply-chain scenario this argument is true; as long as it is guaranteed that the tag is removed or killed when the tagged item is handed over to the end consumer. Over years the discussion was held active, sometimes with strange arguments like *RFID chips are "the mark of the beast" [46] from Biblical prophesies* or wrong statements like *RFID tags can be read from satellites.*

In fact, the ongoing discussions lead to a situation which turned out to be critical for development of the technology. One famous incident was the announcement of a huge RFID project by Benetton. Philips Semiconductors published that Benetton was about to order a very high number of tags to introduce item level tagging for optimization of their garment supply chain. In fact, the project was in a very early stage and far from introduction into the productive system, but vague ideas for use after the point of sale were already discussed (e.g. the RFID enabled washing machine).

No item level tagging was considered in the first stage of the project, pallet level tagging was planned as a start. In the planned scenario no privacy problems would appear for the end customers because the purchased goods would not carry RFID tags. Only when the first stage of the project was considered successful, item level tagging was considered later on. Directly after publication of the story by Philips, Benetton was flooded with a very high number of complaints and requests for statements, but they were not prepared for such a situation at this moment.

No privacy impact evaluation or similar was done at this stage of the project. A group called CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) organized a boycott of Benetton products and got a very high attention in press. Due to the high pressure, Benetton had to back off the project, and obviously also the order of RFID tags. So far, the project has not been implemented or at least no public information about the results and reasons to stop the project are available. It is obvious that Benetton had to stop the project and abstained from RFID technology for the following years as consequence of the story.

In 2006, the European Commission started activities to solve the privacy discussion in RFID technology. A series of public RFID consultations were organized together with a platform for public discussion. During a series of workshops, experts were invited to contribute to the topic. We contributed to this discussion with a presentation about the technical feasibility of cryptographic protection of RFID tags in the academic track of the EU RFID Forum 2007 [1].

In May 2009, the *Commission's Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification* was published. This recommendation provides a basis for the RFID industry to develop and implement applications and gives the end consumers the confidence that their privacy is not violated

by the technology or the applications. According to these regulations, future RFID applications which involve processing of personal data require a Privacy Impact Assessment (PIA) before roll-out.

Requirements for this PIA are currently defined by all stakeholders in close cooperation with the European Commission. RFID industry has also reacted on the ongoing discussion. NXP Semiconductors (successor of Philips Semiconductors) announced already their new generation of RFID tags with built-in support for consumer privacy protection. The privacy topic and discussion is now addressed, and instead of claiming that the technology is free of privacy impact, a new generation of tag-products emerges that supports consumer privacy.

3.2 Closed vs. open-loop RFID systems

When RFID systems are discussed, they are often classified as closed-loop or open-loop systems. For better understanding of the different security requirements it is necessary to point out the difference of these two categories. In the following paragraphs we therefore provide a short description of the characteristics and differences of those two types of RFID systems.

- *Closed-loop RFID applications:* This is the category of independent or autonomous RFID applications, typically used in a single-enterprise environment. They operate as independent systems of tags and readers; when a network is involved then all components (databases, servers) are located in the enterprise network.

  Closed-loop systems are simpler to implement, since they do not require inter-organizational agreements or policies for data access. They are typically used to achieve very specific goals or to solve very specific problems. Typical closed-loop RFID applications are RFID-based car immobilizers or RFID-enabled library management systems. Closed-loop applications often run within the boundaries of a company; therefore security is easier to manage. Ownership of objects (tags) and data is clear, and trust management and access control is relatively easy to manage since no data sharing with external entities is necessary.

- *Open-loop RFID applications:* Open-loop RFID systems provide a broad basis for a variety of applications. They are based on networked services which provide information about RFID tags in the system via access beyond a company network. The components of such systems are designed without a specific application in mind, but they should fit for a variety of applications.

The EPC network, as promoted by EPCGlobal[1], is one example for such open-loop RFID systems. The open nature of such systems requires complex access control policies and mechanisms. Trust management and data sharing between the participating parters are complex to achieve.

The distributed supply-chain-management scenario is a prototype for open-loop RFID system. Various applications (ePedigree, anti-cloning, product tracing and tracking) can be implemented upon such a system. Early versions of the EPC network did not take security mechanisms into account; this can be one reason why deployment of open-loop supply-chain management systems did not take off like forecast several years ago.

Recent activities in the development of the network have taken also security into account, but problems concerning end-user privacy or secure data sharing are still unsolved.

3.3 Added value due to security services

Often, security requirements for RFID systems are discussed as "non-functional requirement." This approach does not consider benefits to the systems functionality triggered by embedded security features.

We suggest to discuss security functionality as a service that enables new application areas for a system or that raises the value of the system due to its protection. This approach facilitates the justification of the additional costs arising by the protection. When the argumentation demonstrates benefits, the arising costs can be compared with the assumed rise of income.

We claim that a service-oriented approach is necessary for proper development of secure RFID technology. So far, in many discussions towards secure RFID, the drawbacks of security (additional costs, reduced throughput, more complicated interaction) were highlighted. For future discussions we suggest focusing on the benefits a protected system can provide.

In the Internet, the introduction of the Secure Socket Layer (SSL), or the secure version of Hypertext Transfer Protocol (http)—Secure Hypertext Transfer Protocol (shttp)—,enabled a multitude of new applications that were not thinkable before (online banking, eGovernment, eCommerce, and many more). The same can happen as soon as RFID systems can provide an appropriate level of security.

In the following we provide a non-exhaustive description of services for RFID systems that can be achieved when tags with cryptographic capabilities are used. Some of the described services can be established by other means, e.g. by data-mining techniques applied to the data stored on servers

[1] http://www.epcglobalinc.org

of the EPC network, but we think that introduction of cryptographic functionality to tags is the more efficient choice.

3.3.1 Security service: Proof of origin or anti-cloning

Tags with encryption functionality and a stored secret key can perform a challenge-response authentication protocol. To authenticate a tag, a reader queries the tag to receive its UID. Then the reader sends a random number as challenge to the tag, which encrypts the challenge under its secret key. The encryption result is sent back to the reader. Using the claimed UID, the reader can either retrieve a secret key from a database to perform the same encryption. Alternatively, the reader sends the UID and the challenge to a authentication server which stores the key for the transmitted tag UID. The server calculates the expected tag response and sends it to the reader. When the expected challenge is computed, the reader verifies the authenticity of the tag by comparing the expected tag response with the one received from the tag.

When such a tag is attached to a product, this mechanism can be used as protection against product cloning. Companies can personalize the tags in their products with secret keys. An authentication server with public reading access can provide the necessary authentication data to customers or to any other party who intends to check the tags origin.

The tags can still be used for traditional RFID applications, e.g. for supply-chain management or RFID-assisted inventory, without using the authentication feature.

Proof of origin can also be provided by plausibility checks in RFID network services. If a specific UID appears twice at the same time in the system, one must necessarily be a clone. This approach has two significant drawbacks. Firstly, it is a computation intense task to check for duplicates in distributed databases, especially when the number of entries is very high. Unfortunately, this is the case in network-based open RFID systems, like the EPC network. Secondly, it is very hard or impossible to distinguish the clone from the original, once duplicates are detected. The consequence would be to flag both tags as possible clones. This can be very annoying or even produce a financial loss for the owner of the original product.

Additionally, network based checks for proof of origin generate a point of attacks against the system, since valuable original products can be falsely marked as potential clones, by introduction of tags with cloned UIDs into the system.

3.3.2 Security service: Protection against introduction of wrong or fake data

When RFID systems are integrated into automated business or production processes, the data inserted into these system is highly critical. As for any other part of the IT system, protection is necessary to avoid financial loss due to successful attacks.

In closed-loop RFID applications which operate inside the premises of a company, protection against introduction of illicit RFID tags, and wrong or fake data from those tags, can be achieved by physical protection of the space around RFID readers.

As soon as the system expands outside the company, attackers can easily introduce data via the unprotected tag-reader link with either faked RFID tags, or RFID-tag spoofing devices. It is easy to understand that wrong data in IT systems for production or other critical business processes can produce considerable damage. A possible attack got wide attention after its publication [65] under the buzzword *RFID virus*. RFID tags with cryptographic authentication feature can prevent such attacks without the need for physical protection of the space around the readers. The reader can then request an authentication whenever a tag arrives from an unprotected area to check whether it is a genuine one. Data from tags that cannot authenticate can be simply ignored. Within protected areas, authentication of the tags may be omitted.

3.3.3 Security service: Data-integrity protection for data from tags

In current RFID systems the transponders do not hold a lot of data, but their main functionality is to transmit their UID. Future RFID systems will include tags with increased memory, therefore readers will store data on tags, or tags will generate data by themselves (e.g. tags with a temperature or light sensor).

When such tags are read and the data is relevant for the RFID application, it is important to check the integrity of the data coming from the tag. A very illustrative example is a temperature sensor tag which is used to record the permanent temperature characteristic of an object in a cooling chain. In case that anybody can change the temperature logging data coming from the tag, the logging is useless. A sleazy operator of a cooling chain could easily alter the logging data to hide discontinuities under her responsibility. For food products this leads to inconveniences because the goods go bad earlier. For pharmaceutical or chemical products such an interruption can cause severe damage with relatively high compensation claims.

In case of unprotected data on tags, an attacker can harm the system

by simply changing the logging data of correctly reposited goods, which would force a cooling chain operator to dispose non-expired goods due to the forged logging data.

Whenever tags can get in the hands of non-trusted parties, a protection against illicit changes of the data carried by the tags is necessary. In future applications, where tags are read by non-trusted readers and the acquired data is sent via the Internet to a back-end service, it is necessary to protect the data from changes by any node between the tag and the point where the data from the tag is processed.

3.3.4 Security service: Access control for the tag's memory or commands

When data is written to tags, or the configuration of tags can be changed by a reader outside a trusted environment (e.g. execution of the "kill" command), it is necessary to protect from unwanted access.

For current tags, the write commands or the execution of the kill command is protected by passwords (access password or kill password in Gen2 tags). This is only a weak protection due to the rather short length of the password (32 bit) and the possibility to eavesdrop and reuse the password.

In case of the kill command, re-use is not a critical issue (after killing the tag, they do not operate anymore) if every tag is configured with a different kill password. This leads to complex password management.

Especially when write access to tags should be performed outside protected areas, another form of protection is necessary. A tag can request proper authentication of the reader before it grants access to critical memory areas or commands. The reader authentication can be performed on basis of cryptographic protocols so that a eavesdropping attacker does not gain any information about the stored secret key. Re-use of the intercepted communication is then not enough to get access to the tag's memory. In case that only those authenticated and trusted readers get permission to write data to the tag or to execute critical commands, a broad band of attacks is repelled.

In future RFID systems of open and distributed nature it will be additionally necessary to hand over the control of the tag's content. When a tagged object changes its owner, is also necessary to perform a so-called transfer of ownership of the access rights to the tag's memory. After the transfer, only the new owner can alter the tag's data and configuration. This can be performed by exchange of the cryptographic keys used in the reader authentication process. Such transfer-of-ownership protocols will require interaction of the tag, the old, and the new owner.

3.3.5 Security service: Protected or encrypted transactions between reader and tag

To repel eavesdropping attacks on the wireless channel between tag and reader, the exchanged data can be encrypted. A pre-requirement for useful encryption is authentication, because the party who encrypts the data needs to decide which key should be used. Even if a session key for the encryption is generated by so called "key agreement schemes", both parties need to authenticate to avoid man-in-the-middle attacks.

A correctly established encrypted channel between authenticated parties (tags and readers) prevents from illicit tracking and tracing of RFID tags. No information about the content is revealed to an eavesdropper, but the exchanged data seems like a stream of random data.

Privacy protection for the owner of the tagged object is not the only motivation for encryption of RFID transactions. The data transferred between tags and readers during an inventory process can be a interesting target for industrial espionage. Such attacks can also be avoided by storing encrypted data on the tags, which is then sent during a transaction. This has the advantage that the tag itself does not require encryption functionality, but simply stores and sends encrypted data. In such cases, the data delivered by the tag is static; this means an eavesdropper may identify tags by messages that were eavesdropped previously. This can be a problem for the final application when tracking or tracing of tags should be impossible. Encryption functionality on the tag itself can avoid such problems.

3.4 Wrong assumptions for development of secure RFID tags

Some wrong assumptions about the feasibility of cryptographic primitives during the early years of the RFID hype delayed the development of proper protection mechanisms. In this section we discuss these wrong assumptions, we try to correct them and describe the effects that those assumptions had on the work of the research community.

3.4.1 First wrong assumption: Implementation of real crypto on tags is technically not possible

With the idea to use passive RFID tags as bar-code replacement, the first killer application for this technology was born. For this application, maximum reading distance and minimal tag costs are the major requirements. The tag's power consumption determines the reading distance; the area of the chip influences the costs of the tag.

When AUTO-ID labs came up with their vision of automated supply chains on basis if passive RFID tags in 1999, it was still a very challenging task to realize the basic functionality of the tags so that they still operate in the required reading distance. In the early years, it was therefore believed that it is technically infeasible to include cryptographic functionality on the tags without reduction of the maximal reading distance.

This assumption was arising from estimations by downsizing the power and area consumption of existing modules from smart card technology, to newer silicon production technologies. Different throughput requirements of RFID tags and smart card chips were not considered during this estimation.

The results of our research proofed this assumption wrong. In [20], members of the VLSI group have presented for the first time an RFID-tag architecture with an integrated AES module. The crypto module fulfills all requirements for application on passive RFID tags in terms of power consumption and chip area.

Instead of using crypto modules from smart-card technology, a completely new architecture was developed, which considers the special requirements for the tag throughout the whole design process. The main difference beside the limited power consumption is the required data throughput. Application on RFID tags allows for slower computation.

The module was designed in a way to achieve a balanced power profile during a rather long execution time. Although power is a very limited resource for circuits on passive tags, energy consumption is not that restricted, because a tag receives continuously energy as long as it stays in the reader field.

Based on the assumption that crypto modules for tags are not feasible, a lot of alternative solutions for protection measures on the network layer were proposed, which do not require crypto functionality on the tags. Considering the expected high number of tags in RFID applications, such approaches get inefficient, due to the high amount of entries in distributed databases.

Another idea that followed was to equip tags with functionality that obfuscates data from tags. The assumption was that such a weak protection of tags might be enough in the context of the application. This assumption may hold for some applications, but in the general case it does not. One has to consider that solutions that protect a device today in a weak way so that they allow breaking them with mid-range costs, can be broken soon with basically no costs with future standard equipment. During standardization of cryptographic algorithms this natural evolvement of computing devices for attacks is taken into account.

3.4.2 Second wrong assumption: Hash modules are less power and area consuming than encryption modules

When the first researchers started to accept that RFID tags might be able to compute cryptographic functionality, a lot of proposals were made based on hash primitives. It was believed that hardware implementations of hash primitives are less resource consuming than encryption primitives.

This wrong assumption has arisen from the experience with software implementations of hash and encryption primitives. Most hash primitives are optimized and designed for efficient implementation on 32-bit processors. Although they outperform encryption primitives on those platforms, they are less efficient when a dedicated hardware architecture is developed.

For researchers with background in power aware development and implementation of digital circuits in hardware, it was obvious that hash primitives will consume more power and area in dedicated hardware implementations, due to the required storing of rather long initial and chaining values. Although the combinational effort of hash algorithms is usually less than for encryption algorithms, the overall power and area consumption is higher. When Sarma et al. published their assumptions about hash implementations in [68], they did not consider that storing intermediate values requires more power and area than low-power implementation of combinatorial logic.

Based on our research results, the authors of [21] clearly show that "*current standards and state-of-the-art low-power implementation techniques favor the use of block ciphers [...] instead of hash functions [...] for secure RFID protocols.*"

As effect of this wrong assumption, various proposals for pseudonym schemes based on hash functions were developed ([56], [75], [11]). All these concepts can also be implemented using an encryption primitive, as this was shown in [73]. We think that such protocols can be constructed more efficiently, when encryption primitives are considered.

3.4.3 Third wrong assumption: A tag with crypto results in a contact-less smart card

Contact-less smart cards can look very similar to RFID tags. The main difference between those devices is the maximum operation distance. For most applications where contact-less smart cards are used, a very short reading distance with a well-defined operation area is intended. For payment or access-control applications it is required that only cards that are very close to a terminal are accepted.

The shorter reading distance leads to following differences. Firstly, the power available closer to a reader is by a factor of 1000 higher than in the

maximum distance of passive RFID tags. While digital parts of contact-less smart cards consume currents around $20mA$, the available power for digital circuits on an RFID-tag is less than $15\mu A$. Secondly, the possible number of devices in the reader field is very different. In the short field of a contact-less smart card reader, there may be a number of three to five cards in the field for an RFID reader the number of tags in the field is much higher. The throughput requirements for one RFID tag and for a contact-less smart card are therefore very different; an RFID tag stays typically much longer in the (larger) field than a smart card does. For access-control applications of smart cards, the maximal response time for cryptographic operations for the card has to be very short to meet the expectations from the user.

Smart cards, which are used in security-critical operations, must fulfill very high requirements for implementation security. During a certification process it is evaluated that the card's secret does not leak, even if a very high number of cryptographic operations are analyzed with Side-Channel Analysis techniques. Meanwhile, some 10 million samples are a standard value for such attacks. Typical RFID tags do not require to execute a very high number of cryptographic operations in their lifetime, therefore the number of operations a tag performs with one key can be restricted, and the SCA countermeasures can be designed in a way to provide protection for a lower number of measurements.

Chip costs are a critical factor for both technologies, but RFID tags are much more inexpensive than smart cards. While smart cards chips have a size of around $10mm^2$, the silicon area of RFID tag chips is around $\frac{1}{2}mm^2$. Any similar additional component added to the basic functionality influences the RFID tag's overall size—and consequently its costs—with a much higher percentage.

Typically, smart cards provide a powerful set of cryptographic functions, which can be accessed by the application. The useful and error-free combination of different cryptographic functions, in a way that no security hole is generated requires a immense controlling overhead which has to be performed by the card itself. We think that future RFID tags will provide a very restricted and well-chosen set of cryptographic functions that can be implemented with marginal effort for controlling circuits.

3.5 Security flaws in existing products

Already today, RFID tags are used in security critical applications. In difference to our suggestion, most of these applications rely on proprietary cryptographic solutions. To achieve the power requirements for tags, dedicated algorithms that promised to result in a low-power design were developed. In many approaches the used key length does not fulfill established

cryptographic standards and therefore brute force attacks become feasible.

In the following paragraphs we look at recently published attacks on RFID applications with secure tags. We discuss the attacks and try to pinpoint the weakness of the system that made the attack feasible.

3.5.1 Texas Instruments – DST

The DST can perform a cryptographic challenge-response protocol to authenticate tags to a reader. As underlying cryptographic primitive the proprietary custom block cipher DST-40 is used. Those tags were designed for use in an electronic car-immobilizer system, with protected passive tags which are embedded in the car key.

At the time when the tags were designed it was assumed that a 40-bit key provides sufficient protection against car theft. Designers of the system claim that at the time when the tags were developed, it was technically not possible to implement protection measures with longer bit length with the available silicon technology. In a later application, the RFID tags from the car keys were used to authenticate clients at payment terminals of gas stations (*Speedpass by Exxon Mobil*).

In [8], a group of students and researchers from Johns Hopkins University present a hack which exploits severe vulnerabilities of the tag. They used information from a presentation held by one of the developers of DST-40 [43] to reverse-engineer the proprietary and confidential encryption primitive. Knowing the algorithm, they implemented an FPGA-based key-search engine which is able to search the secret key for a given challenge-response pair within an hour. Once they know the secret key, they can copy it to a tag-emulation device to authenticate illicitly to the electronic car-immobilizer system or to a payment terminal. While it is possible to check for duplicate tags in the online system of the payment application and to defeat this attack on this level, the electronic protection of the car key is completely broken by the attack. The researchers produced and published videos where they showed that they could make a purchase on an electronic terminal and start a car using their emulation device. The necessary budget for the devices used in the attack was below US \$10.000.–

This incident was the first published attack on a protected RFID application. It received worldwide press coverage. The researchers demonstrated the weaknesses of an established system with a high number of terminals and tags in the field. With the introduction of electronic car immobilizers with passive RFID tags, the number of stolen cars has significantly decreased. Therefore, one can claim that the application is still useful because the effort for breaking it — together with the problem to circumvent traditional protection measures against car theft — is still too high for car thieves. Nevertheless, the decision to use the same protection in a payment systems was a very critical one, and was taken probably years after the

development of the tags themselves.

This successful attack shows that the application of proprietary custom algorithms for protection is very critical. As soon as details about the implementation become public, attacks become probable. For future tag products we must not scale the security level of the tags to a specific application, since it might be the case that the same tags are used in a different application with very different security requirements, as it happened in this case. It was already clear at the time when the DST was developed that payment systems require a key length that is longer than 40-bit.

3.5.2 NXP – The Mifare™ incident

Mifare™ describes a series of contact-less smart card products from NXP[2]. Although Mifare products are contact-less smart card technology, we decided to include the incident in this section. Especially the low-cost branch of Mifare cards, which are intended for one-way tickets, have similar characteristics (minimal chip area) like RFID tags. Different versions of Mifare with different security levels are available; the one we refer to here in this section is Mifare Classic, which uses the proprietary CRYPTO-1 algorithm as security primitive. Mifare was also licensed to other chip producers. Currently Mifare is the market leader and the de-facto standard for contact-less ticketing system. It was also discussed as protection of RFID applications.

The functionality of CRYPTO-1 was reverse-engineered with home equipment by graduate students. During the 24^{th} Chaos Communication Congress in December 2007 they presented their results. Later on, they published their analysis results as a research paper [54]. During their work, not only the functionality of the proprietary and undisclosed algorithm was revealed, but also other severe weaknesses of the design were detected. Soon after disclosure of CRYPTO-1, a very efficient attack that reveals the secret key within some minutes followed[3].

At the same time, a second academic team was investigating the security of Mifare cards. Soon after the first presentation of successful attacks on Mifare, researchers from Radbound University published a series of papers [13] [28], where successful attacks on Mifare cards and their applications were presented. After these publications it was clear that the protection of Mifare Classic cards was completely broken.

It is out of doubt that Mifare products are a commercial success. When the successful hacks were published, newer versions with stronger, and above all, standardized cryptographic features were already available as products. Nevertheless, Mifare Classic cards are still used in many applications. The incidents show again the risk of using proprietary cryptographic

[2]http://www.nxp.com/

[3]http://www.cs.virginia.edu/ kn5f/Mifare.Cryptanalysis.htm

primitives. As soon as the secret algorithm was disclosed, successful attacks became feasible.

3.5.3 Keeloq™ – A successful attack using SCA

Keeloq™ is available as a product for active (battery powered) and passive transponder devices. The main application area is battery-powered Keeloq transponders for remote key-less entry systems. Due to the lightweight implementation and the similarity of key-less entry applications and possible applications of secure passive RFID tags, recent attacks on Keeloq™ are discussed here.

In early 2008 a cryptanalytic attack on the Keeloq encryption algorithm was presented [38]. This attack requires exhaustive computation but is technically feasible. The impact on practical implementations was considered minor due to the necessary computational effort of an attack.

Shortly after publication of the cryptanalytic attack, researchers from the University of Bochum analyzed several "high secure" key-less entry systems with Keeloq protection by application of SCA methods. This class of attacks uses physical characteristics of the encryption device, e.g. the power consumption of the device during operation, to reveal the secret key. After analysis of several products they completely broke the system [17]. Now they are able to reveal the secret key of remote devices and — even more critical — the manufacturer key, which allows to generate valid key values for cloned remote devices. In a follow-up paper they explain how to reveal the secret key of a remote device after eavesdropping only two cipher-texts from the device [45]. Additionally, this attack allows to prevent access for legitimate devices, while the illegal attacker can still enter. These attacks pose a serious threat for all installed systems which are protected by Keeloq.

This incident is very similar to the previously described attacks on RFID systems. Compared to the value that is protected by the devices, it is possible to break it with rather low effort. Interesting is that this attack relies on an attacking method that was not known when the system was developed. The first public paper of SCA was published in 1996 [48], at a time when Keeloq was already available as product.

It is important to consider this point for future developments. The lifetime of tags in the field is rather long, compared to software products. Again, a proprietary algorithm was used which turned out to be susceptible after profound investigation by independent researchers.

3.5.4 Future attacks

The academic community's interest in breaking RFID systems has just started. We expect more successful attacks on established systems in the

next time. Since successful attacks guarantee very high press coverage, they can boost academic careers. At least such attacks raise the international visibility of the involved researchers significantly.

There is no reason to assume that other protected RFID-tag solutions provide a better protection. The design of currently available tags dates back to a time when the necessary protection level for the applications was underestimated and when silicon technology for tags did not allow better protection. Especially the threat of implementation attacks like SCA is a serious one for current secure RFID products.

Some people see this hacking activity of academic researchers as destructive, because it damages the business case of companies. Companies have invested money to bring their product on the market; a published attack can reduce the sales and therefore lead to a financial damage. Nevertheless, we have to consider that such systems are designed to protect other values, and clients pay for proper protection. In case that the protection is not as good as claimed, due to advances in technology or due to flaws in the protection, this should be publicly known.

One can assume that criminal organizations also analyze protection measures, possibly with higher financial support than academic researchers. In case that a criminal party reveals a security hole they would not publish their findings, but they would try to get as much profit out of the flaw as long as nobody else is aware of it. Such an incident would damage the customer who runs the inadequately protected application. A following legal case poses therefore high risk also for the producer of the protected system. Loss can then be higher than after publication of a security hole. Considering this, it is easier to see the benefit and importance of public analysis of protection measures.

3.6 Trade-offs for security implementation on tags

From the previously described incidents we can see that proper protection is necessary for many applications already. Weak protection on basis of proprietary or confidential methods is not enough. From the experiences in the traditional Internet we learn that secured communication will enable a variety of applications for new technology. We are confident that proper protection of future RFID systems and the IoT requires also protection of passive RFID tags. In this section we discuss the possibilities to provide this protection functionality on future tags. Due to the high restrictions for resources like chip area and power supply, alternative trade-offs are required to come up with proper solutions.

In the remaining part of this section we present ideas and possibilities which can enable cryptographic operation with appropriate protection level

on RFID tags. Those ideas exploit specific characteristics of RFID tags and their application. Focusing on one specific point to implement security primitives on RFID tags will not lead to a competitive solution. For every single primitive one needs to evaluate all available options for optimization to allow deciding for the best choice. During optimization of circuits it has to be considered that over-fulfillment of given requirements can impede the accomplishment of the overall optimization goal. If, for instance, a critical throughput requirement can be fulfilled with a very low clock frequency, it is not useful to introduce a more advanced architecture which would allow even higher throughput than necessary. The decision for the architecture has then to be taken on basis of the power consumption of the two choices.

- *Computation time — clock cycles for computation:* Often, tags are quite long in the field. In some applications tags need to answer rather fast to a initial request of the reader (inventory command); but this is not the general case. For cryptographic operations we can assume that only a very limited amount of data will be encrypted by the tags. Consequently, the required throughput for the cryptographic circuit is quite low; a lot of clock cycles can be used for the operation. Traditionally, throughput optimization is the reason to embed cryptographic hardware primitives, therefore the hardware designers have to re-think their approaches when designing for RFID tags. Optimization for throughput is often an optimization for energy consumption as well, which is important for applications in battery powered devices. This is different for RFID tags, where energy is not a restricted resource, but power consumption is. Developers of cryptographic hardware need to consider this. Hardware developers are trained for throughput optimization; they are challenged to rethink their design suggestions when they design circuits for passive tags. Often the area and power consumption of circuits can be significantly improved when all available time for the required computation is used. Parallel execution or pipelining are typical strategies that are applied to improve throughput of crypto hardware. Both strategies are counterproductive when designing for low-area and low-power consumption. Pipeline structures should be replaced by register files and parallel computation should be avoided wherever possible.

- *Clock frequency:* Clock frequency is a critical factor for the power consumption of the digital circuit. The lower the clock frequency, the lower is the overall power consumption of the circuit since the CMOS structures use most of the energy during the moments when the clock signal changes. Different clock domains can be defined for the overall RFID tag. The clock frequency for the digital circuits of the tag is derived from the carrier of the RF signal (in HF systems) or an

on-chip oscillator is used to generate the tag's clock signal (in UHF systems). Therefore, the clock frequency value is not a completely free choice of the designer. Separating clock domains of circuits with high computational activity from those of register files can help to meet the limits for the overall power consumption. Nevertheless, separation of clock domains requires additional effort for synchronization and clock generation, which adds up to the overall chip area. Especially when asymmetric cryptographic algorithms are implemented for RFID tags, different clock domains should be considered.

- *Silicon area is becoming less critical:* Production technology for silicon chips is steadily improving. Newer production processes allow smaller on-chip structures leading to lower area and power consumption for the same functionality. Production on newer process facilities is more expensive, but the expected high number of tag chips justifies to migrate to newer production technologies. The chip alone does not yet make up the tag; the single tag chips need to be cut from the die and every single chip is then mounted to the package with the antenna. The smaller the chips get, the more expensive is the handling of them before and during the connection with the packages and antennae. The percentage of area loss during the cutting of the tags from the die increases, because the active chip area shrinks, but the loss from cutting stays constant. Recent estimations forecast that a chip area around $\frac{1}{2}mm^2$ results in minimum overall costs. Currently, tag chips are just below $1mm^2$; with the next migration to a newer technology the standard functionality will be possible on a silicon area close to $0.5mm^2$. Making the chips even smaller would then result in higher effort during handling costs and increased loss during cutting.

  For improving the power consumption, moving to newer technologies still makes sense. This development will then lead to a situation that additional functionality can be implemented without resulting cost increase during production. The area overhead due to cryptographic functionality will then be less critical.

- *Pre-computation:* When a tag enters a reader field, it is automatically powered by the EM field. As completely passive device it stays idle until the reader sends a request. Whenever multiple tags are in the field and the reader detects a collision during the time when the tags are supposed to answer, it deselects a certain number of tags so that the probability of a further collision in the next try is reduced. This operation is repeated until all collisions are resolved. For further operation with one specific tag, a single tag is selected by direct addressing. All other tags are then disabled. While this procedure can be rather intense for the reader, the tags themselves are mainly

idle, actively operating only in a rather short time interval. This idle time could be used for cryptographic operations. Random numbers can be derived from a pre-stored seed value with a pseudo-random number generator. Pre-computations can be done for computation-intense operations. Clearly, the protocols and algorithms need to be designed in a way so that this pre-computation is possible. So far this was not considered during development and design of RFID protocols.

- *Computation charging and split computing:* RFID tags are powered by the surrounding EM field from the reader. The reader additionally performs modulation of the carrier to communicate with the tags. The tag's answers are de-modulated by the reader. Whenever a tag receives the carrier signal with enough field strength, it is powered up and waits for communication which is initiated by the reader. In principle it is possible that a tag starts computation without trigger from outside. Instead of starting computation-intense operations after a request from the reader, the tag can pre-compute intermediate values before getting the input value. Clearly, the used protocol and underlying primitives need to support this feature. Some security solutions (e.g. GPS [30]) allows pre-computation of so called coupons. Some signature scheme also allow pre-computation of parts of the algorithm. In case those protocols allow pre-computation, computation-charging stations can be introduced on the application level. These stations would be reduced readers that only provide an RF-field in situations where tags are placed stationary for a longer time (e.g. in warehouses). The tags start computing new coupons when they are supplied with the EM field, and they store the newly generated coupons when they have finished computing. More advanced tags could even store intermediate values of computation-intense operations so that they do not have to start the whole operation when they get interrupted before finishing (split computation). Again, this principle has to be considered during selection and design of the cryptographic primitives and protocols.

Part II

Research activities towards a secure Internet of Things

4

Research activities towards secure passive tags

The *VLSI and Security* group at IAIK has been active in various research projects in the area of RFID security. Some of the projects were initiated by the author based on the vision and ideas of the group. In other projects we participated as research partner, mainly responsible for secure tags and the integration of security measures into tags-to-reader protocols.

All mentioned projects have been of co-operative nature. Industry partners typically provide inputs for our research that are based on their experience and information about market trends and needs. To follow our principle of applied research, we base our work on the requirements given by real-world applications and trends. Therefore, it is useful to define the requirements in close co-operation with industry partners. Sole technical feasibility is not necessarily the primary motivation for such research. Instead, we try to find new or alternative solutions which provide the required functionality and comply with given limitations like chip-size, power consumption, reading distance, compatibility, and so on. The innovative parts of such projects are normally the tasks of the academic partner. Starting from given requirements, we suggest alternative and new approaches, evaluate them, choose the most promising one and implement them as prototype. In case that the assessment of the results and the prototypes is positive, the solutions might be used by the commercial partners as part of future products. Sometimes, the results are directly exploited by IAIK itself, e.g. as hardware Intellectual Property (IP) modules.

Scientific dissemination of achievements is of major importance of any academic research group. Our co-operations are defined in a way, such that publication of our results is not restricted due to commercial interests. To avoid problems of conflicting interests of academic groups and industry (the first want to publish their results and the second wants to keep the major achievements undisclosed, at least as long Intellectual Property Rights (IPR) protection is established) we consider this issue during the definition of the project. As long as the activity of the academic researchers is not directly connected with "product development", usually no problems arise. In case that ongoing research activity leads to directly exploitable results, motivation of the academic researchers to protect their IP is the same as for an industry partner.

All described projects have a similar focus for the dissemination and exploitation of the results. Commercial exploitation of the results is planned in a time-frame of five to eight years after start of the project. Dissemination of the project results in an academic sense is integral part of all projects and has been accepted by all partners as important activity. Our publication list of the recent years demonstrates our motivation for scientific publication.

In the following we give a more detailed description of each single project and the evolution of the Workshop for RFID Security (RFIDSec). The projects are presented in a chronological order. The research of later projects is based on the results of earlier projects, therefore the project descriptions document the development of the research activities in the RFID area within IAIK's *VLSI and Security* group.

In parallel with the research projects, a new series of workshops was initiated. We realized that the topic "Secure RFID" was tackled as side-topic in many distributed events, relevant papers were therefore presented in various conferences with RFID or security focus. A focused event where a core group of active researchers could meet on a regular basis was missing. Our idea was to establish a yearly workshop where the academic researchers can discuss relevant topics together with representatives from industry. This was the starting point for the RFIDSec workshop. Meanwhile, the yearly RFIDSec is established as meeting point for the community. A steering committee for further development has been established, proceedings are published, and an Asian branch was initiated.

4.1 Authentication for Long-Range RFID technology - ART

The project ART marks the starting point of our RFID-related research. After gaining experience in development of cryptographic modules in close cooperation with the smart-card industry, we started to explore further areas to contribute with the gained expertise. At that time, MIT's Auto-ID Labs came up with their vision about pervasive RFID technology combined with the EPC network as backend system. Auto-ID Lab's vision for RFID forecast non-intelligent tags and a powerful backend network where the gathered information is used and analyzed. Lowest possible cost for the tags was the most important criteria during development of the system. Security or privacy was not considered as major issue at that time. This idea was very successful. Meanwhile the subsidiaries of MIT's Auto-ID Lab are established all over the globe. The major result of their activities is the EPC-Gen2 standard (Electronic Product Code, Generation 2) which is currently the most important standard of UHF RFID tags of supply chain applications. The EPC numbering system, the development of the communication standard as well as the EPCglobal Network is managed by GS1.

The initial idea for ART did not follow the vision of Auto-ID Labs. The researchers from MIT claimed that available resources on low-cost RFID tags for symmetric or asymmetric encryption primitives are "far below what is feasible" [75]. This was actually our starting point. Our main motivation during the definition of the project ART was to show that implementation of modern cryptographic primitives is feasible for low-cost and long-range RFID tags.

4.1.1 Introduction and project description

In the project Authentication for Long Range RFID Technology, we investigated the design possibilities and use of cryptographically protected tags. Strong symmetric cryptographic algorithms were considered as protection method, which was at that time seen as infeasible by many players in the RFID community. We considered our approach as successful if we were able to include symmetric crypto to tags without resulting reduction of the reading distance. An additional goal of the project was to increase the reading distance by re-design of the RFID reader's receiver parts, which is basically independent for the tag's implementation.

The consortium of ART was composed of four partners. The project was initiated and coordinated by IAIK's *VLSI and Security* group. Beside coordination, we were responsible for all security related parts of the project. NXP Semiconductors Styria and Siemens AG participated as industrial

partners, mainly during requirement definition for the tag and reader development. NXP provided the production facility for the AES chips. The research team Industrial Electronics from FH Joanneum Kapfenberg was the second academic partner in ART. They investigated the possibility of noise reduction in the reader by application of advanced DSP methods.

ART was accepted for funding during the second call for proposals by the Austrian FIT-IT program line "Embedded Systems". The project started in September 2003 and was successfully completed after 26 months. Following objectives were defined in the project proposal:

- To raise existing protocol standards for RFID technology with respect to security features.
- Designing and implementing tags with strong cryptographic algorithms, and to implement a prototype tag and a reader.
- To improve long-range readers by using innovative architectures.
- Investigation of the potential of new application fields, and
- to research the role of secure smart tags as part of a world of ambient intelligence.

4.1.2 IAIK goals and objectives for ART

Together with our industrial partners we defined the requirements for the cryptographic modules of future RFID tags. To come up with usable suggestions, it was necessary to derive the requirement from experiences of already existing applications. The tags cost (thus, the chip area of the cryptographic modules) was an important factor, but turned out not to be the most important one. Even more important for most applications is that the tag's reading distance is not reduced due to the extended functionality. As outcome of this discussion we defined as goal to come up with implementations of an AES module with a maximal continuous power consumption that is below the consumption of the tag's EEPROM.

To ensure the practical feasibility of the results, we defined compatibility to current existing RFID infrastructure and communication standards as necessary requirement for our developments. Together with our industrial project partners we came to the conclusion that incompatible solutions will not be accepted by the industry due to the expectable high costs during migration to protected versions. Additionally, a compatible solution has the benefit that protected and unprotected tags can be used together within the same infrastructure.

It was considered as necessary that we were able to demonstrate the cryptographic features together with commercial RFID readers, without

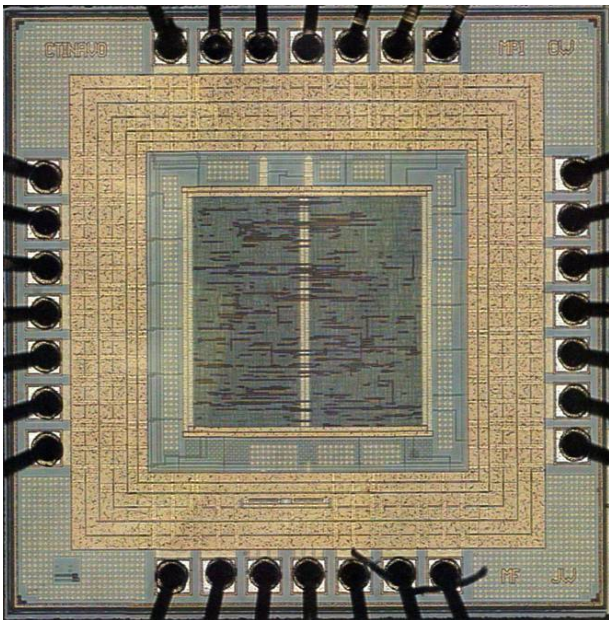

Figure 4.1: Smallest AES chip for RFID tags by Feldhofer.

modification of the reader hardware. Modification of the reader's firmware (to execute protocol extensions) was considered as meaningful.

Wherever possible we agreed to apply established security mechanisms, with accepted security level. AES as standardized symmetric primitive together with the authentication protocols according security standards [39] were considered as first choice.

We agreed on concentrated dissemination and demonstration of the results in the RFID community. Development of application-like prototypes which could be demonstrated to audiences without strong security background was defined as important task of IAIK in ART.

4.1.3 IAIK results of the project

Important results have been achieved by our project partners on the reader-related part of the project. To improve the operating range between reader and tag, NXP and FH Joanneum developed innovative antenna concepts with improved characteristics which were verified in laboratory experiments. The reading distance in laboratory environment was improved by the new reader design by about 20% through application of advanced digital signal processing methods. Environmental noise signals of typical RFID operational areas have been studied and classified to design specialized dig-

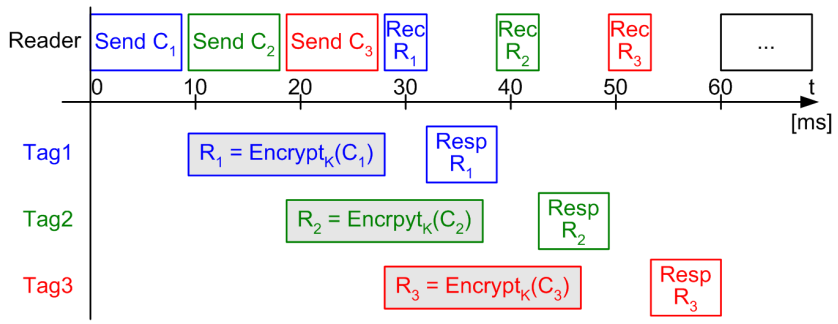

Figure 4.2: Protocol extension proposed in ART.

ital filters. Important improvements of the reading distance were achieved by improving the analog receiver components of existing reader designs.

The project share of IAIK was the security-relevant part of the project. Our archived results were beyond the initial expectations.

In the security domain we've shown that implementation of a standardized cryptographic functionality is feasible without reduction of the reading distance. Successful implementation and production of the so far smallest reported hardware implementation of AES is a proof of our starting assumption. The fully functional silicon implementation is optimized for use in RFID systems [24] and fulfills all requirements for application on low-cost RFID tags. Figure 4.1 shows a photo of the chip.

For development and analysis of protocol extensions, simulation is a standard approach. Unfortunately, no simulation engine was available for the chosen communication protocol between readers and tags. We implemented a Java-based Protocol Evaluation Tool for RFID Applications (PETRA), a simulator for the ISO/IEC-15693 communication standard. The user can implement own applications by using mandatory reader requests (which are already implemented) or custom requests (which have to be defined by the user) and can define the behavior of tags when receiving custom requests. The simulated output provides the exact timing and internal behavior of reader and tags as well as all exchanged data during execution of a command or a sequence of commands.

Especially in cases where more than one tag is in the field, simulation is the only reasonable way to determine average values for the timing at reasonable costs. Due to the dependence of the anti-collision procedure on the UIDs of the involved tags, the effect of changes in the protocol is hard to assess with analytic methods. Testing in a reference lab would be possible but very expensive, because the test setup would require a high number of tags with extended functionality. For protocol assessment, the testing approach is impractical. Long delay would arise because testing is

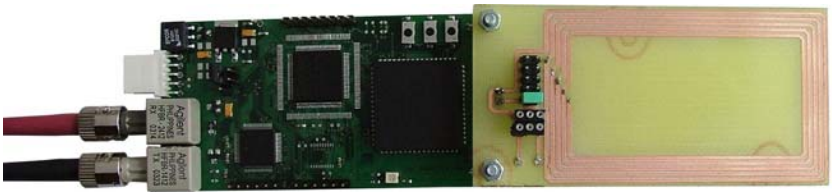

Figure 4.3: A semi passive prototype tag. The 1^{st} version of the Demotag.

only possible after production of tags with the new functionality. In case of errors or changes, long re-production cycles would arise. Simulation with PETRA turned out to be a good choice.

Because tags were not able to perform encryption operations, security was never considered in detail during the design and development of communication-protocol standards before ART. We proposed a security layer for authentication of tags and readers, as well as for mutual authentication of tags and readers [3] [19] [20] [16]. This security layer was suggested as extension of the existing standard ISO/IEC-15693 [40]. Figure 4.2 shows a snapshot how the suggested protocol for tag authentication is executed when more than one tag is present in the field. PETRA was used during design and analysis of the protocol extensions. Accurate simulation helped to find the optimal parameters for the protocol extension. For demonstration, the suggested custom commands were implemented on the prototype tags and in the reader firmware.

A fully configurable semi-passive HF tag was implemented as prototyping platform. This platform is basically a combination of an analogue-frontend chip and an FPGA that implements the digital components of an RFID tag. Compared to an implementation of the full tag as single chip solution, this approach is more flexible because it allows configuration and reprogramming of its functionality after production. Cost-saving was another argument for this choice. Production of a full-tag chip with analogue front-end and memory structures was not feasible with the available budget. On the other hand, the stand-alone front-end chip and the FPGA consume much more power than available. The prototype requires therefore an energy source. The final prototype was used for demonstration of the results in a setup that allowed tag authentication to a commercial reader. Figure 4.3 shows a picture of the semi-passive prototype tag.

In terms of academic dissemination, the results of ART were published as eight peer-reviewed scientific articles on international level as conference papers and journal papers. The articles were presented by IAIK's researchers on international and national workshops or conferences. We were invited to present our results at the 1^{st} academic RFID convocation at MIT [5]. At that time, the convocation was probably the most im-

portant dissemination event, because it was the most important scientific meeting in the RFID area worldwide. Before that, our results were mainly acknowledged by the IT-security community.

4.1.4 Impact of the project results

TINA, the resulting AES chip marks a major milestone in the research towards secure RFID technology. Not only for the research at IAIK, but also for the international community. For the first time it was shown that standardized cryptographic methods can be implemented in a way, so that they comply with the fierce requirements of passive RFID tags. Our results correct the wrong assumption that standardized cryptographic functionality would be infeasible for RFID tags (see Section 3.4). The resulting publications of the implementation results [24] [22] [20] proofed this assumption wrong.

Together with the proof that symmetric cryptography is feasible on passive RFID tags, we proposed security extensions for the communication between readers and tags [19][15][3]. The focus of our work in ART was put on authentication of the tag to a reader; nevertheless we also suggested extensions for reader and mutual authentication. We did not implement a full RFID application, but we suggested an application scenario in the area of supply-chain management. We suggested to use cryptographic tag authentication as proof of origin for items, to protect from introduction of cloned items into the supply chain. Our proposal was made at a time when most reaserchers considered the network-based checks for cloning, together with the UID of RFID tags as secure enough. Meanwhile, the opinion of the community has changed in this respect [51]. The community became aware that the uniqueness of the UID cannot be guaranteed in practice. Results of ART are for sure not the sole reason for this development, but a visible contribution of our project results to this development cannot be denied.

For the development of the research area RFID Security at IAIK, ART was the first visible starting point. The successful achievement of the ambitious goals and the high visibility of the results in the international research community opened up many possibilities for further research. Basically all projects and activities described later are a direct result of ART.

The Programme for Advanced Contactless Technology (PROACT)[1] was initiated by the author. Our project partner NXP sponsored the activity, a decision that was taken after assessment of our results in the cooperative project. We initiated a teaching and research platform for RFID related topics at Graz University of Technology. During the first period of PROACT, the research focus was put on security. IAIK was responsi-

[1] http://proact.tugraz.at

ble for coordination of the activities during this period. We organized two RFID summer schools, a variety of student projects and other activities to increase the interest of students in the research field RFID in general, and security in particular. During the second period, the coordination of PROACT has been given over to the Institute for Fundamentals and Theory in Electrical Engineering (IGTE). The project had therefore not only an impact on the following research and teaching activities at IAIK, but boosted also the RFID related activities at other research units of TU Graz.

In terms of commercial exploitation the project also achieved direct results. The resulting IP module for AES is available for commercial licensing. Meanwhile it was licensed by several clients for chip designs in contact-less applications.

4.2 Secure NFC applications - SNAP

The results of the project ART boosted our interest in the research area RFID Security. The motivation for ART was technology oriented, towards the development of the necessary components to build secure RFID systems. Within the project, supply-chain management was considered as application area. The requirements for the developments were derived having this application area in mind, but no demonstrator was built. While the significance of our results was rapidly understood by the security community, we learned during the project that it is hard to explain the need for secure components and the security requirements to non-security audience, without referring to an illustrative application.

For a follow-up project we wanted to motivate our further developments with an application that does not need additional argumentation to understand the security requirements. Additionally, we wanted to broaden the application area of our developments. Due to the success and impact of AUTO-ID's activities, the focus for RFID application was logistics. Our view for application of RFID was broader. To demonstrate the potential for applications of secure RFID in other areas, we wanted to suggest an application without supply-chain context. The upcoming communication standard Near Field Communication (NFC) provided a good basis for our next proposal.

4.2.1 Introduction and project description of SNAP

Short introduction to NFC

NFC is a short-range communication standard for mobile phones and other embedded systems like PDAs, cameras, electronic picture frames and similar devices. The applications using NFC follow the principle of "touching" communicating devices. This means that in contradiction to other contactless communication technologies, NFC stands for communication between devices that are brought closely together to share data. NFC applications can be seen as virtual counterpart to direct communication between two persons standing close together to share information.

NFC allows for easy connectivity between devices without any complex setup procedure for the connection. The standard additionally enables communication of mobile devices with passively powered devices (passive RFID tags) that do not have an internal power source. Main applications are bootstrapping of other connections, like Bluetooth, rapid and easy data exchange between e.g. a camera and a picture frame or payment and access control, where a mobile phone replaces the smart card as security token. The principle of communication of devices that are brought closely together provides the user with the imagination that the communication is private

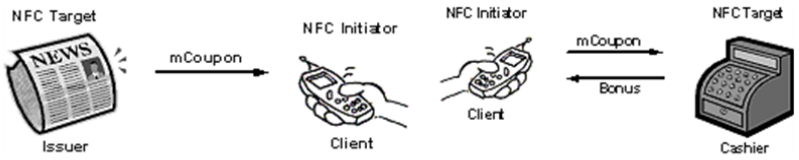

Figure 4.4: Left side: Pick-up of a mCoupon. Right side: Delivery at a cashier.

and secure. In principle, a mobile phone with an NFC interface is a mobile RFID reader, which can also act as RFID tag.

Fixing a tag (passively or actively powered) to a certain location can provide information whether a mobile NFC device (or its user) has been at that location. NFC can serve as direct link between data in a virtual network and data about the location in the real world by means of placing inexpensive passive tags on dedicated geographical locations. Business applications that exploit this characteristic require protection of the tag's content and the data that is exchanged to prevent illicit use.

Coupons and mobile coupons

Coupons are a well-established way to improve business by providing a benefit to a customer for a specific activity (e.g. looking at an advertisement). Often, coupons are given out to collect some information about customers. For example, the filled-out coupon contains the address of the client which can be used for subsequent advertisement. Both parties benefit from the coupon, the client by receiving a gift or a discount, the merchant by getting more information that can be valuable for further business.

The coupons represent a small value, but a high number of uncontrolled copies of coupons can result in a significant loss. Electronic or virtual coupons are codes or numbers which can be used in web stores to get a discount. Compared to paper-based coupons, systems of electronic or virtual coupons differ significantly by the fact that unprotected data is easily copied or modified without significant costs by anyone.

Mobile Coupons (mCoupons) are a special form of electronic coupons. They are not bound to any fixed host system; a client does not need online connection to receive or to store them. mCoupons can be picked up with mobile electronic devices from terminals or passive low-cost tags that do not require their own power supply. The owner of the mobile device can carry the mCoupon around (as stored data on the device) like a traditional paper coupon and can deliver them to a cashier where a bonus is handed over in exchange of the coupon. The client has full control over the data that is delivered together with the mCoupon. Additionally, user-relevant data like the email address or other personal information can be filled-

out by the user. The mCoupons themselves require protection against illicit modification of its value, unwanted transfer to other devices or illegal duplication by the users. Figure 4.4 illustrates the necessary actions to pick-up and to deliver a mCoupon.

Project consortium and defined goals

The objective of SNAP was to develop appropriate protection mechanisms for NFC communication and to develop a demonstrator application that relies on those protection mechanisms. An mCoupon system, which allows users to collect electronic coupons from passive tags, was designed and implemented as demonstrator.

The consortium of SNAP was composed of four partners. IAIK's *VLSI and Security* group initiated and coordinated the project. Besides coordination, we were responsible for the system design, design and implementation of the security protocols, development of the prototyping platform and for the design and implementation of an AES module that is protected against SCA attacks. Basically the overall system design and all security related parts of the project were performed by IAIK. NXP Semiconductors Styria participated as industrial partner, mainly during requirement definition for the tag and the assessment of the SCA countermeasures. Additionally, they provided NFC development kits and libraries. The researchers from Industrial Electronics at FH Joanneum Kapfenberg developed an energy aware approach to detect tags in the neighborhood of an NFC antenna. To evaluate the feasibility to eavesdrop communication between NFC devices, experts from the Institute for Electrical Measurement and Measurement Signal Processing participated in the project.

The above described application, a system of mCoupons, clearly demonstrates the need for proper data protection of all involved components. Our main expertise, protection of passive RFID tags is a crucial part of such a system. The proposal for SNAP was accepted for funding by the Austrian FIT-IT programm line "Embedded Systems". Additionally the proposal received an award for the best proposal submission during the 5^{th} "Embedded Systems"-call of FIT-IT. The project started in February 2006 and ended in April 2008. The following goals were defined for SNAP:

- A profound investigation of the threat eavesdropping for NFC communication between an active and a passive device.
- Accurate investigation of SCA attacks on RFID devices operating in the reader field.
- Development and implementation of protocols for protected mobile coupons that comply with the requirements of passive mCoupon issuers and NFC.

Figure 4.5: PDA with NFC interface, running the application mWallet.

- Implementation of a neighborhood detector prototype that enables RFID readers and NFC devices to detect nearby tags with low-energy consumption.

- Implementation of two AES chip prototypes for passive RFID devices, one with and one without SCA countermeasures.

- Accurate evaluation of the costs and the efficiency of SCA countermeasures, on basis of two chips — a protected and an unprotected one — with identical functionality and interface.

- Design of an mCoupon demo system based on Windows CE. The demo system uses semi-passive tag prototypes and a laptop with NFC interface.

With completion of the project, all major goals have been met. In February 2008 the final application prototype of the mCoupon system was selected by peer-review for demonstration at the "NFC Developer's Competition" during the NFC Congress, at the University of Applied Sciences Upper Austria, Hagenberg. Together with our partners from FH Joanneum Kapfenberg we presented our results and received an award in the NFC developer's competition.

Figure 4.6: Setup by EMT to assess the outdoor eavesdropping distance.

4.2.2 IAIK goals and results of the project

The tasks of the project were defined in a way to enable independent work by the four research teams. NXP as industrial partner provided important inputs during the specification phase. They accurately analyzed the results of the AES chip development, to prepare the decision of later integration into RFID tag products. As inventor of NFC, they supported us during development and implementation of the demonstrator with valuable know-how as well as development tools and devices.

The team of EMT evaluated the threat of eavesdropping the NFC communication between a passive tag and a reader. Figure 4.6 shows one of the various setups that were built up for the measurements. Previously published results [32], which show that eavesdropping is possible from a distance of several meters, have been fully confirmed by SNAP. Under special conditions, the results have been surpassed. EMT observed that due to effects like crosstalk and diversion of susceptible signals to nearby wires or tubes of the heating system, the achievable eavesdropping distance can be enlarged heavily. A clever attacker who exploits those effects could easily set up eavesdropping equipment out of sight of his victims. After intense discussion with the commercial partner, those results were not published. In later publications [34] our results were confirmed. Independent from the question whether publication of such findings is useful or not, the experiments delivered the affirmation of our initial assumption that NFC communication needs to be protected in case that sensible data is transferred. This was an important result for our following work, since it demonstrates the need for integration of cryptographic mechanisms, whenever crucial or private data are transferred via NFC in an unprotected environment.

The goals and tasks of the *VLSI and Security* group at IAIK during the project were following:

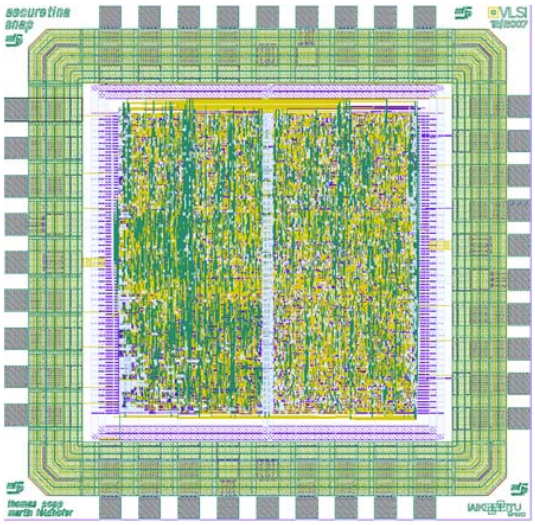

Figure 4.7: Chip layout of the AES module with SCA countermeasures.

- Demonstrate feasibility of SCA attacks: A passive tag which executes a cryptographic algorithm is a target for implementation attacks. The tags are mounted in unprotected areas and since they are inexpensive, attackers can experiment and tamper with them at very low costs. To justify the need for protection against this sort of attacks, we wanted to provide a proof that those attacks are practically feasible. In [37] and [62] it is shown that the attacks are possible on HF tags. Different measurement techniques and also post-processing of acquired traces have been applied to improve the attacks. However, our results show that the attacks are practically feasible with standard lab equipment; therefore RFID tags with cryptographic functionality need to implement countermeasures against those attacks.

- Mobile Coupons as application for secure RFID Tags: With this application we have shown that application of RFID tags is reasonable also in other areas than logistics and supply-chain management (SCM). Application of tags as coupon-issuing devices requires a high number of inexpensive tags so that they can be placed e.g. in magazines or billboards. In contrast to classical SCM scenarios the security requirements are transparent, also for people without security background. The provider of the coupon system would directly be harmed by an successful attack, therefore the motivation to spend costs for protection is higher than in the SCM scenario.

- System design and prototype implementation: Within SNAP we did

Design	Technology	Chip area SYNTH [GEs]	I_{mean} [µA @,100kHz]
TINAold	0.35µm, NXP	3400	3 (1.5V)
TINAnew	0.35µm, AMS	3650	2.9 (1.5V)
secureTINA	0.35µm, AMS	19,500	13.8 (1.5V)
FACTOR	SecureTina/TINAnew	x 5.3	x 4.8
TINA014	0.14µm, NXP	3519	0.35 (0.9V)

Figure 4.8: Result comparison of TINA chips.

not limit our developments to technology that supports applications. Instead we wanted to provide an application prototype as illustrative example to show how the technology can be used. The mCoupon system was defined by IAIK and all components were implemented by FH Joanneum and IAIK. As replacement for the cryptographic RFID tags, semi-passive tags were applied. A PDA with NFC interface was used as device for the client. We implemented the necessary application mWallet which picks-up the electronic coupons from passive tags, and delivers them later to a cashier. Additionally we have implemented an attacker's mode which allows to modify the mCoupon data stored on the phone. Figure 4.5 shows the PDA running the prototype application. The required protocols for pick-up and delivery of coupons were designed and implemented as security layers compatible to ISO [41]. A cashier application was implemented to receive mCoupons from a PDA via an attached NFC interface. Additionally, we have designed an issuer application that configures the tags to issue specific mCoupons and which initialized the databases for the cashier application. The components have been implemented as prototype for demonstration on workshops and fairs. We are fully aware that for a commercial exploitation significant parts are missing. Nevertheless, our demonstrator received considerable attention by industrial and academic players in the NFC community.

- SCA protection for RFID tags: The goals described earlier were planned to provide a motivation for this task. The eavesdropping investigation provided the evidence that cryptographic methods are necessary to avoid eavesdropping. The SCA investigations made clear that implementation attacks are a practical threat. The next logical step was to provide a solution that deals with those issues. An AES module for RFID tags was an important outcome of the project ART. Within SNAP we wanted to develop an encryption IP module that implements protection against implementation attacks. Known countermeasures on logic and architecture level produce overhead of chip

area, power consumption and reduce the throughput of the module. To come up with a usable solution, the available resources had to be specified. Power consumption can be used up to a critical level, area is a cost driver, and reduction of throughput is less a problem, as long as the given requirements from the protocol can be met. The goal of SNAP was to provide maximal protection under given restrictions for the design. On the chosen target technology we agreed on a maximal power consumption of $15\mu A$. The allowed area overhead was defined by factor six. A minimal throughput by factor two smaller than for the unprotected module was considered affordable. The metric for the level of protection was chosen as necessary number of samples for a successful attack. We defined our minimum goal for protection with a factor of 200 more necessary samples for a successful attack. Figure 4.8 shows a comparison of the different chip designs. TINAold is the chip produced in ART. TINAnew is the same design produced on a different process of similar structure size. This chip was the reference design for the assessment of the SCA-protection level. SecureTINA is the chip with the SCA countermeasures, designed and developed in SNAP. The column TINA014 provides results on basis of synthesis, place and route and simulation of the same design on a modern production process. The values provide a reliable estimation for SecureTINA on such a process. With the combination of all implemented countermeasures we have achieved an increased protection level of factor 5800. The value is derived from analysis results with a very powerful attacker who knows all details of the implementation and the countermeasures. This result is a good value compared with the initially defined goal of 200. Nevertheless, it turned out that the combination of the chosen countermeasures for SecureTINA was maybe not the ideal choice. After the implementation and the analysis, the question if such a protection level could be achieved with less overhead remains open.

- Semi-passive HF Demotag without proprietary devices: A first version of a semi-passive RFID tag was developed and produced in ART. It was successfully used for prototyping but this version had one significant drawback. The use of a front-end chip from our research partner restricted publication of results using the tag. Especially publications which could leak characteristics of the analogue front-end were considered critical. To avoid those problems designing a new version was defined as goal for SNAP. A short marked research revealed that no front-end chip was available without those or similar restrictions. We therefore decided to design the analogue font-end for the new version with discrete components. Additionally, the controller platform was changed to a commonly used platform. The ex-

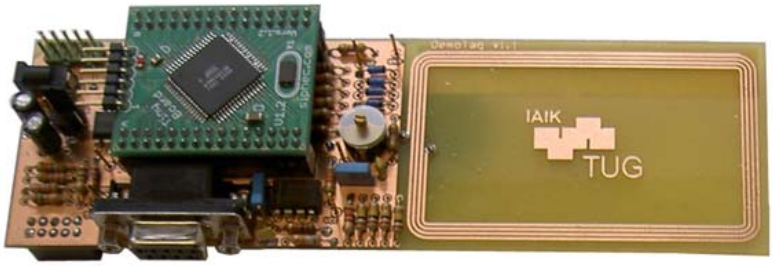

Figure 4.9: IAIK HF demotag; a programmable RFID tag.

isting firmware with the implementation of the protocol was extended to be compatible to NFC. Figure 4.9 shows the current version of the resulting prototyping device. The demonstrator system used these semi-passive tags. They were also used for the setup for SCA attacks of the SecureTINA chip.

4.2.3 Impact of the project results

NFC is discussed as a new communication method that should simplify interaction between mobile devices. Many possible applications are suggested, like easy data exchange between camera and display, bootstrapping of Bluetooth connections, or as replacement of security tokens (smart cards). The fact that the operation works only when the devices are close together, gives the user the impression that the connection is secure, similar to the natural behavior of people who tend to stand closely together when discussing secret information. SNAP revealed that the impression that "near automatically means protected" is wrong. We have shown that protection of the communication is necessary. The mCoupon-system prototype helped to exemplify the need for protection in a broader audience.

Before we presented our SCA results, it was not clear if such attacks are feasible when the tags are in the rather strong reader field. In [10] it was shown before that it is possible to separate the chip from the antenna and perform the actual attack on the device without the disturbing reader field. Such an attack requires physical tampering with the device under attack, which might not be useful in many applications. Countermeasures which prevent separation of antennae from the chip can prevent this sort of attacks. Our successful attack was the first one to show that the effects of the strong reader field can be eliminated with standard lab equipment. A lot of proposals to counteract SCA attacks by solutions that make physical tampering with tags useless are meaningless after presentation of our

attack. Surprisingly, we were able to mount the attack without detailed specialized expertise in measurement techniques. It was not necessary to involve experts for EM field measurement. We can therefore expect that the results can still be improved when more advanced measurement methods are applied.

With the new SecureTINA module we have shown that protection against SCA for symmetric cryptographic modules is possible, even when applied on RFID tags. SecureTINA was not only the basis for scientific publications. Meanwhile, the design has been released as commercial IP module, and has been licensed for commercial use to companies. We consider this directly exploitable IP module as an extraordinary result of a research project which proofs that the defined requirements for the project are based on realistic assumptions. The fact that the outcome of a research project is directly exploitable as IP module proofs that our design methods and tool chain complies with the quality of commercial products.

SNAP received not only an award for the project proposal by the funding body FIT-IT. The final demonstrator received the award for the 3^{rd} place of the Austrian NFC Developer Competition in 2008. This was a surprising result for us, since NFC-technology was not the main research focus of the project but the application area to demonstrate the achieved results. During the event we had a chance to discuss our outcome with audience from other application fields and found out that many other interesting application areas could benefit from the achievements (e.g. NFC-based building inspection on basis of mobile phones and fixed tags on defined control points.)

In terms of scientific dissemination, the project achieved remarkable results. Altogether, the team of IAIK published fifteen peer-reviewed articles in workshop proceedings or journals. The team members contributed to three book chapters with project relevant topics and 19 presentations were given on workshops, conferences or other public events.

The developed prototyping platform, the IAIK HF Demotag was further improved after the project. We extended the firmware to support more protocols and started to ship the device to research partners. Meanwhile, it is sold on a regular basis to developers of RFID systems. It is used in teaching activities at Graz University of Technology, but also in other universities. Companies use it for evaluation of security holes of RFID systems and to develop new solutions.

4.3 BRIDGE, a large scale EC research project

Through the results of ART and our contacts from the first RFIDSec workshop we got in contact with big players in the RFID community. Due to our first results in national projects and our following dissemination efforts through publication and presentation at international workshops and conferences, we were invited to join as tag security specialists in international cooperative research projects. In the following we present our involvement in the Sixth Framework Programme, Integrated Project (FP6 IP) Building Radiofrequency IDentification solutions for the Global Environment (BRIDGE). It was organized by GS1, a leading global organization dedicated to the design and implementation of global standards with special interest in RFID[2].

4.3.1 Introduction and project description

The project proposal for BRIDGE was submitted in May 2005 to the 5^{th} call for the Information Society Technology (IST) research programme of the European Commission (EC). The three year project started in July 2006. The consortium of 32 project partners included five universities, 19 companies and seven national GS1 organizations.

Research, development and implementation of technology and tools for proper deployment of RFID applications in Europe were the main objectives. When the project was defined, the topic security was not considered as major point, but it was considered as one of 15 defined work packages. The European business community should benefit from the project results by increasing the effectiveness and efficiency of their supply chains.

Within business-oriented work packages, trials were performed in different application sectors like manufacturing, textile and pharmaceuticals. Horizontal activities provided dissemination and training activities to improve the adoption of RFID on a large scale in Europe. The work packages dedicated to research and development investigated various aspects of the underlying technology like RFID hardware, software, network and security.

Eleven partners were involved in the activities of the security work package of BRIDGE. Three of those were universities; two were from end-user organizations, three of them were technology providers, like reader manufactures and the rest (three) were solutions providers. Only few of the partners could be described as "security experts", some partners (CAEN or Confidex) started their security activities with the start of BRIDGE while others could provide security experts although the core business of the company was not security (e.g. SAP or BT). IAIK was the only partner with strong security focus in the team.

[2] http://www.gs1.org/

The work package was defined as a technical work package, dedicated to research and development activities. As major goals of the work package we wanted to provide secure building blocks for future applications of the industry partners. The focus of the work was put on application of emerging industry standards like AES, Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML) rather on development of new security mechanisms. Technology development as well as definition and enforcement of proper use policies were considered as necessary to enable secure applications.

BRIDGE was a very large project with a lot of different aspects and technological areas. IAIK was involved exclusively in security-related parts of the project, therefore we will focus in the following description on the work and results of the security work package.

4.3.2 Security activities in BRIDGE

The overall effort of the security work package in BRIDGE was similar as the overall project size of the previously described projects. About 115 person months overall effort was available to perform the tasks. The distribution of workload to the various partners was imbalanced, with only 2 person months for GS1 and about 20 person months for ETH. With 14 planned person months, IAIK was among the three most important parties. The contribution of work package 4 was split into seven independent tasks:

- Task 4.1: Security Analysis and Requirements: Definition of threats and security-related requirements were planned in this task. The needs of all stakeholders in an SCM scenario were considered. An important point was to discuss the security challenges under the assumptions that security can raise the value of the data and thus the RFID applications. The work of WP4.1 provided that basis and motivation for the other parts of the work package. The special requirements of Small and Medium Enterprizes (SME)s were considered throughout the whole work.

- Task 4.2: RFID Tag Security: In opposition of the initial security assumptions of the EPC community (see 3.4), task 4.2 developed technology to protect future RFID tags by application of symmetric cryptographic measures. The aim of the task was to develop lightweight implementations of standardized cryptographic protection measures, to establish secure authentication of tags to readers, readers to tags or to achieve mutual authentication and a following encrypted communication between them. Within the context of BRIDGE the importance of standardization and compatibility was very high; therefore we proposed a security layer on top of the Electronic Product Code

Class-1 Generation-2 UHF RFID Protocol (EPC Gen2) which is fully backward compatible to unprotected RFID infrastructure. The possibilities of using asymmetric cryptography on future tags were additionally investigated in this task. Task 4.2 was coordinated by IAIK and the performed work based on the results of earlier projects. A first important task was to get full commitment from all involved partners by convincing them of the usefulness of the approach. Due to budget restrictions, development of new tag chips was not feasible. We developed semi-passive tag prototypes for UHF technology and used them for prototyping. The results of task 4.2 provided the basis for the work in T4.3.

- Task 4.3: Anti-cloning of RFID Tags: The main goal was to develop an anti-cloning prototype to demonstrate a use case for security enabled tags. To do so, the protocol extensions were simulated to evaluate the impact of the communication overhead. An existing reader product was modified so that the required custom commands could be executed by the prototype implementation. We defined a prototype scenario to protect Reusable Transport Items (RTI) like pallets against cloning. Using the results of task 4.2, we implemented a prototype application with open interfaces to EPC Information Service (EPCIS) services. The developed security layer was the basis for a suggestion to ISO for standardization of security services. Our suggestion was promoted as suggested work item by the Austrian ISO committee and was then accepted by the international ISO working group. IAIK was responsible for coordination of this task.

- Task 4.4: RFID Trusted Network: A trusted RFID network requires that all components of the network can be trusted. The readers have been identified as critical parts of the whole network. The protection of tags and the data they carry was investigated in the tasks task 4.2 and task 4.2. The security framework of task 4.5 deals with the protection of the network components EPCIS and EPC Discovery Service (EPCDS). Protection mechanisms for readers, which may be placed in remote locations were not considered in earlier work. On the other hand, the RFID reader is the first device connected to an organizations internal network and information system. Therefore it forms a key security barrier and it is essential in operating many earlier proposed security schemes. Enabling secure access of readers to key databases, or to enable proper accesses control to critical databases requires a proper protection of the readers. To allow secure enforcement of policies, we require assertion and attestation. The trusting computing concept promises to provide those characteristics, the objective of this task was therefore to develop a new

trusted RFID reader which builds on the trusted-computing principle [31]. The aim was to offer a solution that allows solution providers to control and trust the information entering the SCM application via the readers.

- Task 4.5: Network Confidentiality: Protection of the network services was the focus of this task. The main goals were development of a security framework for protection of EPCIS and Object Name Service (ONS) together with prototype implementations to prevent unwanted access to critical business information. A layered design should allow participation of trusted local operators and scalable global federation of the network services. The major goal of the task was to define a framework for access control for the data stored in EPCIS and EPCDS. Participation of dynamic parties in a supply chain is a crucial issue in the respect. Especially the assumption that parties without prior business relationship should have access is impossible to fulfill, because access control requires specification of the parties who claim access rights.

- Task 4.6: Supply Chain Integrity: The integrity of data stored in the EPC network services is of major importance for applications which rely on this data. Based on the stored events, applications derive assumptions about the physical objects in the supply chain. E.g. theft can be detected, if an object disappears between two checkpoints. Violations of the data integrity can arise by unintentional communication errors or by intended modification through attackers. The task dealt with investigation of methods to recognize such problems. Close cooperation with other work packages (e.g. WP5 Anti-Counterfeiting Business Application) was planned.

- Task 4.7: Roadmap and Dissemination: The main outcome of this task was to provide a technology roadmap for the results of the work package. Together with an assessment of the maturity of the developed solution we have discussed the necessary additional activities towards practical application of the outcome. The goal of this task was to disseminate the key results to a broader public, to outline the additional research needs and to identify the opportunities for commercialization of the results. The work was performed with special focus on the EPCglobal network architecture. Organization of a workshop for academics and industry was also planned as important dissemination activity.

As a starting activity of the work package we discussed the need for security in SCM scenarios under a general view. Privacy was a major topic in those discussions; nevertheless we decided to motivate our work by other

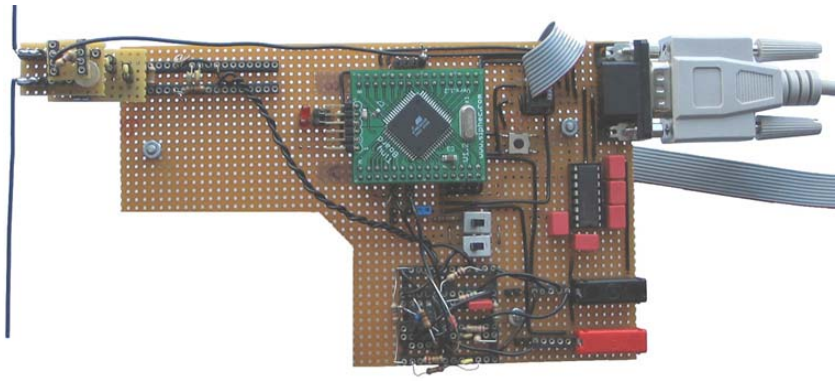

Figure 4.10: Early prototype of the semi-passive UHF demotag.

arguments. This decision was taken due to of two main reasons. Firstly, the work package was defined as technology and research oriented. The privacy implications arise from the final applications; therefore it is hard to address the problems without having a specific application in mind. Secondly, when the main motivation for security is privacy protection of the end-consumer, the arising costs are a blocking criterion. None of the involved shareholders feels responsible to take over the arising costs. By providing an alternative motivation for introduction of security measures, we tried to avoid this deadlock. Logically we wanted to develop a solution that can also be used to improve the privacy protection. The overall motivation was still to provide more than "just" privacy protection, but additional services which justify also additional costs.

Serious attacks came up during the life time of the project (Speedpass, Mifare, Keeloq, see 3.5). They helped us to gain acceptance for our chosen approach. Referring to the real life attacks, it was easier to convince people without security background that ad-hoc solutions without proper protection level are not enough.

4.3.3 IAIK goals and results of the project

The tag-oriented tasks were coordinated by IAIK. The work performed in those two tasks was our major research contribution to the project BRIDGE. In this subsection we will refer only to the results achieved by TU Graz researchers. Some of the results were performed in close cooperation with project partners, others alone by IAIK employed researchers.

- *Secure UHF tag prototype - the IAIK UHF demotag:* Since the semi-passive prototyping platform of the previous projects ART and SNAP was very useful, we suggested to develop a similar device also for UHF

Figure 4.11: Final version of the IAIK UHF demotag design.

technology. Due to the budget restrictions, this was the only way to implement working prototypes to demonstrate our methods. We used the same design approach and micro-controller platform as the HF prototypes. Due to our limited experience in design for UHF the implementation of the device was a challenging task. Figure 4.10 shows a early prototype of the design, Figure 4.11 illustrates the final version of the UHF demotag.

- *Implementation of a pseudonym scheme:* A variety of pseudonym schemes was proposed by the international research community. None of these was implemented due to a lack of tags with cryptographic capabilities. Most of the published schemes use hash primitives as basic building block, a direction we did not follow in this project. The scheme was modified to use AES as cryptographic primitive. This version of the scheme was implemented in close cooperation with BT by a master student of TU Graz. We used our existing HF Demotags, since the UHF version was not yet available when the implementation was done. A complete pseudonym demo was implemented, consisting of tags, readers, a mobile reader terminal on a laptop and a computing centre. The system was presented at the conference Internet of Things 2008 in Zürich and at RFIDSec 2008 in Budapest. To our knowledge it is still the only existing implementation of a pseudonym scheme on RFID technology. Most of the papers on this topic are theoretic concepts or stand-alone prototype implementations of the computing centre to assess the effort of resolving a received pseudonym. The influence of the scheme on the tag-to-reader communication and the tag's operations has not been evaluated before in practice. The demo proofs the feasibility of the approach and shows the possibilities but also the drawbacks of such schemes.

- *Protocol extension of ISO-18000-6c:* To implement the anti-cloning prototype, tag authentication was performed between tag and readers. The necessary commands were integrated as "custom commands" into the communication protocol between tags and readers. To allow the execution of such custom commands, the firmware of a commer-

cial RFID reader was extended by a generic interface for custom commands. Before specification of this protocol extension and fixing of all its parameters, the approach was modeled in RFIDSim, a simulation framework for EPC Gen2 [27] [26]. We extended the simulator by the security commands according [59] and tested different approaches in a variety of different scenarios to define the parameters in the best fitting way. The suggested approach was the basis for our standardization activities together with ISO. The semi-passive prototype tags were configured to execute the protocol and the security commands. In the prototype scenario they represented specific RTIs. We also defined clones with the same ID, but with different cryptographic keys to be able to demonstrate naive cloning attempts.

- *Comparison of cryptographic primitives:* At the beginning of the activity we decided to focus on AES as cryptographic primitive. This decision was based on our results of earlier projects. Nevertheless, it took us quite some time in discussion to convince our partners that AES is a good choice. While it was clear that an efficient implementation of AES can fulfill the requirements, our earlier results have not excluded all doubts that there might be a better choice. Before deciding for AES, we have made estimations about implementations of other possible candidates, but to explain all reasons and arguments to non-specialists on basis of those estimations took rather long. Therefore we decided to implement other cryptographic algorithms under similar design assumptions to be able to compare the results in a fair manner. Figure 4.12 shows the results for a metric that is important for RFID technology. It includes the current consumption, the required clock cycles and the resulting chip area for each implemented candidate. The result shows that the new stream-chiphers GRAIN and TRIVIUM are interesting candidates. They are fast, small, and – most important – use least power. Those algorithms are rather new, their security level is currently still under investigation. We concluded that they might be a good choice for the future. Tiny Encryption Algorithm (TEA) was suggested as candidate by our Chinese project partners. Our results show that a low-power implementation is three times faster than a comparable AES implementation. The requirements are comparable but TEA uses more power. Additionally, the security level of TEA is doubted by the security experts. We think that the gain in throughput is not worth the risk of a security hole when using TEA. The result also shows that low-power implementations of the hash functions MD-5 or SHA-1 have marginal inferior characteristics compared with AES. We want to note here that MD5 is already broken [74]. SHA-1 is expected to be broken soon, since significant vulnerabilities have been published [12]. The

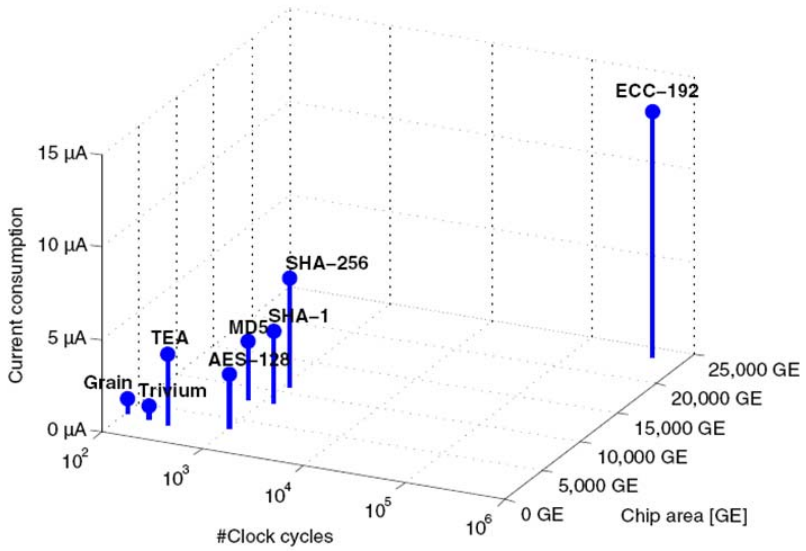

Figure 4.12: Comparison of different cryptographic primitives by Feldhofer, in respect to their suitability for application on RFID tags.

newer hash function SHA-256 achieves comparable security level as AES, but our results show that the power and area requirements are more than double. To be able to compare the results with efficient primitives for asymmetric cryptography, we additionally included an Elliptic Curve Cryptography (ECC) module with comparable security level. Due to more complex computations and the much longer parameters, the consumption of area, power and clock cycles are significantly higher. The analysis and the result helped us to convince all partners that the chosen approach is meaningful. It was also very useful for discussion with external contacts to justify our decision for AES.

- *Implementation attacks (EMDA)*: To assess the threat for this class of attacks we performed Electro-Magnetic Differential Analysis (EMDA) attacks on the semi-passive prototypes and on real world RFID tags. The result of the attacks for the semi-passive prototypes was as expected; we were able to attack the devices successfully. This was no surprise since the AES implementation was not protected and the controller of the Demotag has been attacked many times before in our lab. From previous projects we had experience of filtering the EM field to get the best results for an attack. In UHF systems,

the UHF carrier frequency and the frequency range of the emanated signal which is used in the attack are quite different. The filtering turned out to be more efficient than for HF systems. The results on commercial RFID tags were indeed a surprise. The directly emanated signal from the tag was small enough so that we could not perform a reasonable attack, but it turned out that a major leakage occurs due to a parasitic in the backscatter signal. The results of the attack were more effective than for passive HF tags, although the UHF tags have less power available for operation. The results were published in [60]. This was not the first EM-based SCA attack on RFID tags; one year before a simple EM-attack was presented in [57]. Our attack is of differential nature, which is significant for the design of countermeasures. While ad-hoc solutions are enough to avoid the simple EM attacks on tags by Oren and Shamir, the differential attacks are more complicated to repel. In [61], the limitations of suggested countermeasures in [69] and [70] are shown by researchers from IAIK's BRIDGE team. With our results we have shown that protection against SCA is an important requirement for cryptographic primitives on RFID tags.

- *Tag Security Whitepaper:* The main results of the security work package were described a Whitepaper publication by BRIDGE; the results of IAIK mentioned above made up a substantial part of it. In difference to the scientific papers we have produced for the research community, this publication was written with an audience in mind that does not have detailed security or technical knowledge. Professional business managers from GS1 assisted to publish our results in an adequate format for this audience. The release of the Whitepaper was a success, an article was issued on the online portal of the RFID Journal[3]. RFID Journal is currently probably the most important information resource for business people for understanding how RFID can help their companies to improve supply chain efficiencies.

4.3.4 Impact of the project results

The project BRIDGE was the first chance for us to promote our approach for security in the RFID community. Since our results were acknowledged by the security community more or less immediately, this was a big chance for us to achieve higher visibility for our results. In the project we were in a new situation when working together with people from another discipline. This situation required to explain our suggestions for a different audience, RFID-trained engineers and researchers without detailed security background. During the starting phase, this situation lead to some

[3] http://www.rfidjournal.com/article/articleview/5074/1/1/

hindrances, but soon the hole team became used to each other and productive.

The privacy discussion at the beginning of the project helped us to get closer cooperation with other work packages. We achieved to persuade the whole project that security on tags can help to improve the privacy implications, but also to raise the value of the whole system. During discussions with other work packages we also came to the common agreement that technology can support protection of end-user privacy, but the evaluation of privacy impacts need to be performed on application level. Although this outcome seems logical or trivial, it took a while until the partners from the application-focused work packages agreed that the team of the security work package cannot provide a solution for the privacy-protection issue by a technological approach.

Beside privacy protection, the topic anti-cloning and anti-counterfeiting got high importance on project level. Work package 5 was dedicated to anti-counterfeiting, but worked on a network-based approach. We have shown that protection on tags can improve the currently possible solutions. At the start of the project it was still believed by the majority that the UIDs which are permanently programmed into the tags are a suitable security characteristic. In numerous discussions we have emphasized the fact that although currently no tags with programmable UID are available, they can be available in future. Especially when a lot of anti-cloning systems rely on the uniqueness of the tag IDs, the market for programmable tags is becoming more interesting. In this discussion it was important to mention that the cost calculations for tags with programmable UIDs are not comparable with the cost calculations for normal tags. Their price can still reasonable, although much more than normal tags, because in many scenarios forging can still pay off. If a tag with programmable UID helps to get a cloned product into an official supply chain, the value of the tag can be much higher. The network-based solutions additionally suffer from the effect that it is a very hard problem to distinguish the original product from the cloned one, in case that a UID appears twice in the information system. In such cases, the legitimate owner of the cloned item can be harmed because it can happen that the SCM system could mark it as potential clone.

Throughout the project we came to the conclusion that networked-based systems for anti-cloning have limited use. With our programmable Demotag we could also show that producing tag-cloning devices is not a very cost intensive task. As long as cryptographic tags are not available the network-based solutions provide a reasonable alternative. Nevertheless, for future needs they do not compensate cryptographic functionality on the tags.

Our experience gained in protocol extensions received attention by the standardization bodies. through activity on the project we got in contact with working groups in ISO that were established to push standardization

of security in RFID protocols. We were invited to present our approach; especially ideas to extend the current protocols by security mechanisms were interesting for the working group. We promoted a solution that is service oriented and that allows application of different algorithms and security protocols to achieve a service. Clearly, such a solution adds extra overhead, since before a secure operation can take place, the reader and the tag need to negotiate the protection methods used. On the other hand such a generic way facilitates standardization since it allows for different approaches to achieve a service. In case that the two communication devices do not share the necessary cryptographic functionality to communicate securely, they can still exchange data that is not susceptible to attacks. Our suggested approach is still followed by the current draft of the standard[4].

Our comparison for implementations of cryptographic primitives helped to suggest encryption primitives rather than hash primitives for tags. It turned out that explaining our decision for AES was much easier using the resulting picture. Abstract and thus complex argumentation on basis of estimations without illustration is less efficient. The work of Sarma et al. [68] had a very high impact and especially in the RFID community there was no doubt that their assumptions about hash modules were correct. With the direct comparison of (outdated and insecure) hash functions (MD-5 and SH-1) and AES it was much easier to convince involved persons. We think that future suggestions for secure protocols will take our results into account, rather than basing developments on wrong assumptions like e.g. [6] and [49].

The SCA attacks have shown that this sort of attacks will become a threat for cryptographic RFID tags. Design of tags without keeping this problem in mind leads to attacks like published in [57]. We have also shown that naive ad-hoc solutions to deal with the attack might lead to insufficient protection [61]. The smart-card community has already built up expertise for efficient protection against those attacks. This work needs to be done also for protected RFID tags. Due to the fact that tags are rather inexpensive and that it will be easy for attackers to get them, invasive attacks need to be considered in the risk analysis. Our results raised awareness in the RFID community who did not have to deal with the topic before. Although some involved companies like NXP or Infineon do have advantages because of synergies with their smart card business lines, other major players did not consider the topic yet.

Our semi-passive UHF Demotags are meanwhile exploited as commercial products. They were shipped to companies and universities in a similar number as the HF Demotags. To raise our sales and contacts to US based researcher units, we are currently considering to provide a new version that

[4]Working Draft of ISO/IEC JTC 1/SC31N for "Information technology - Automatic identification and data capture techniques - Air Interface for file management and security services for RFID"

supports the frequencies specified for US (915MHz carrier instead of the 868MHz carrier used in Europe).

As the following paragraph shows, the project reviewers were quite pleased with our results. We did not get any negative feedback for the overall results of WP4. The text below is a specific fraction, taken directly from the official project review report provided by the EC:

[. . .] Since 2006 it has become clear that there is a security requirement for RFID there is a new mind set beyond "privacy". This WP work has influenced ISO Standardization in Austria on how security can be enabled in tag-reader RFID communication. – Furthermore, integrity of RFID attacks was taken as a key challenge, because read-failures due to attacks are looking the same as normal network failures; therefore a mechanism needs to be developed that identifies attacks. [. . .]

From our perspective we have achieved all results as planned and expected. We built two demonstrators to prove that our starting assumptions were correct. Although there were some delays due to misunderstandings and misalignment of tasks in the work package, we have met all defined goals. Such delays and the resulting communication overhead within the project team are probably normal in such big consortia. We underestimated those issues when starting the project, because before we were working in rather small projects with a very small and specialized selection of partners. In that sense, BRIDGE was a new experience for us. On the other hand, we realized that once the approach is accepted in a bigger group, the impact of the results is much higher and therefore justifies the resulting overhead. Especially the result that our suggestions are on the way to become an important part of an ISO standard are motivating for future activities. The experience of cooperation with partners with very different technical background was demanding and inspiring as well.

4.4 Cryptographic protected tags for new RFID applications - CRYPTA

CRYPTA is ongoing at the time of writing this thesis. It is a project funded by the Austrian FIT-IT programme, in that sense a follow-up of ART and SNAP. While the previous projects of this format dealt with symmetric cryptographic functionality for RFID tags, CRYPTA is our first step towards asymmetric cryptography for passive tags. The proposal was submitted to the third call for proposals of FIT-IT's programm line "Trust in IT Systems". The idea was developed by IAIK's VLSI team which also initiated and coordinated the proposal development. The project was accepted for funding without major changes and in the following proposal award ceremony we received an award for the second-best submission. Austriamicrosystems and RFiT Solutions are the commercial partners of the project. RFiT Solutions is a Graz based company which specializes in RFID software and solutions and is therefore interested in exploitation of the research results on application level. They bring in experience in design of RFID applications and middleware. Austriamicrosystems is a semiconductor developing and producing company specializing in high-performance analog Integrated Circuit (IC) designs for specific markets. Recently, they entered the UHF and HF RFID market. Together with their existing reader IC products, they are interested in the development of RFID tags with additional functionality. Within the project they provide experience in design and production of tags, especially the analogue parts like front-end or memory structures. They also provide production facilities for the prototype chips. Their exploitation interest is focused on the results of the chip development activities. They bring in valuable experience in specification and design of chip design for low-power applications like passive RFID.

4.4.1 Introduction and project description

CRYPTA aims at protection of objects against cloning by providing a proof of origin. Earlier solutions to this problem focus on network-based solutions which search for clones of the unique ID in the relevant data bases. When a tag ID appears in two different locations at the same time, one must be a fake. This protection might be enough for the very specific case of supply chains for retailers where tagged objects are scanned quite often along their way in the supply chain. The starting assumption that the unique tag ID provides protection does not hold in a general case.

To provide an alternative, we suggest in CRYPTA cryptographic protection of the tags themselves. The tags store a cryptographic key that cannot be read from outside, but is used exclusively by the cryptographic operation. A faked product cannot reveal the key from original tags and

therefore it is impossible to transfer the key to a faked tag. Still, it is possible to include successful or unsuccessful authentication procedures in central databases to trace routes of fakes, but it is not necessary to do this for detecting fakes. Depending on the class of cryptographic algorithms, a verifier needs access to the secret key of the tags (or a central service that verifies tag responses) or a public key, that can be distributed without a security problem. To bind the public key with the correct tag, Public Key Infrastructure (PKI) is applied. Within CRYPTA we research protection of tags with asymmetric cryptographic solutions. It is our goal to integrate standardized cryptographic primitives with a key length that provides protection according the current state of the art. Application of asymmetric cryptographic functionality on passive tags is the main difference to the projects previously described, and much more than a logical step of development. The necessary amount of computation to execute asymmetric cryptographic primitives is much higher than for symmetric primitives like AES. This fact requires new approaches for the development of the digital circuits parts the tags.

CRYPTA builds its protection on tags that are capable to compute the fully standardized Elliptic Curve Digital Signature Algorithm (ECDSA). Once personalized, they carry a private key and a signed certificate (their public key signed by a Certificate Authority (CA)). Our main goal is to provide proof of origin for a tagged product, development of a prototype application for this proof is part of the project. Integration of additional security services like reader authentication, encrypted communication, key exchange etc. is considered during system design and protocol specification, but not necessarily integrated into the prototype.

The project was started at the beginning of 2009; the planned project duration is 26 months. The overall workload available by the whole consortium is approximately 110 person months. IAIK had the initial idea and prepared the project, we also coordinate the project.

4.4.2 IAIK goals for the project

When the project was started, several prototype implementations with asymmetric cryptographic modules for RFID were available [35] [36]. Even a product-like implementation by Siemens was available when the project was started [7]. The main difference, and also the main challenge of CRYPTA was to develop and implement a module that is capable to compute a digital signature of a received message, according to a standardized asymmetric method. Development and implementation of this module was defined as task for the VLSI team, after joint specification with the industrial partners. Instead of optimizing the cryptographic method so that a minimum of operations is left for the tag, we planned to implement ECDSA in a way that fully complies with the given requirements for passive tags.

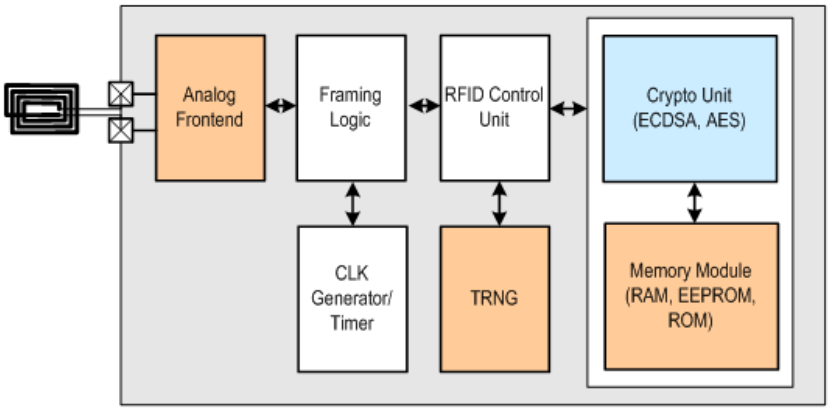

Figure 4.13: The architecture of the CRYPTA tag, as specified by the project partners.

The cryptographic module for ECDSA is expected to use considerably more logical gates and storage than chips with symmetric primitives. To achieve best chances for exploitation we decided for additional integration of an AES, which adds only a small percentage of additional area. Result is a cryptographic module that is capable to perform ECDSA, SHA-1 (which is part of ECDSA signatures) and AES encryption as well as decryption. It is a dedicated goal of CRYPTA to develop, implement and produce a passive RFID tag with antennae. This adds front-end design and non-volatile memory modules to the chip, instead of designing a pure digital stand-alone crypto IP module. The integration of the digital hardware into a mix-signal prototype is a challenge we have not faced in earlier projects. Our partners work on the analogue front-end the Contact-less Universal Asynchronous Receiver/Transmitter (CLUART) and the storage modules (volatile and non-volatile memory). Nevertheless, the required effort for integration must not be underestimated. The architecture of the tag is illustrated in figure 4.13. Similar to SNAP, we have chosen NFC for the application area, therefore the analogue front-end will be an HF front-end operating with a 13.56 MHz carrier frequency.

Due to the powerful cryptographic functions the tag will build on a new controller concept instead of hardwired state machines. Those finite state machines for protocol execution are state-of-the-art technology applied on RFID tags. A drawback of this approach is that complete re-design and testing of the circuit is necessary even in the case of very small changes of the protocol or tag functionality. Instead, we will apply a small micro-controller for execution of the protocol execution and controlling of the cryptographic module. We will develop and implement a completely new

tag architecture on basis of a programmable controller which facilitates integration of additional modules and which can handle necessary protocol extensions easier. Instead of re-development of the digital hardware by re-design and extension of the state-machines, our approach allows for modification of the functionality on basis of modification of the microcode.

The tag prototype will demonstrate the technical feasibility of ECDSA computation on tags. Together with the tag we will provide an application demonstrator that uses the tag for a proof-of-origin application. The asymmetric cryptographic capability of the tags will allow off-line authentication of the products. This means that the verifier does not need a connection to a verification service at the time of verification. A trusted public key from the issuer's certificate will be sufficient to perform secure verification. At the time of writing of this thesis, development of the final application demonstrator has not yet been started.

Together with the tag prototype we will provide a Java reference model of the overall system, which will serve as executable specification. The model will include a simple PKI for generation of valid key pair and certificates. Those parts can be directly used by the application demonstrator. This reference model will serve as the reference during application development, so that development can start before the tags are available. The same model will also be used for testing of the tag chips and for personalization of the tag chips.

4.4.3 The project results

At the time of writing this thesis the project has been running for one year. This is approximately half of the overall project duration. After an initial phase of system specification, requirement definition and chip specification, the majority of development and implementation tasks are currently ongoing. The expected project results are still under development. Nevertheless, some results are already visible and are therefore mentioned here. We will not describe the impact of the results as we did in earlier sections. We expect that our tag design achieves similar acknowledgement as the TINA chip; but quite a few tasks, from chip development and production to successful testing are to be done until we can present the results.

The signature-creating tags will be the main outcome of CRYPTA. We expect that they will be the first fully passive RFID tags with ECDSA functionality. The fact that fully assembled tags will be produced will facilitate demonstration and exploitation activities of the results.

The tag architecture and the low-power controller design is not only usable for passive RFID tags, but is an interesting approach for other control intensive digital designs with rigid power or energy restrictions. We have noticed interest from our commercial partner on this new approach for on-chip controlling already during the specification phase of CRYPTA.

After the first year of the project, five presentations about specific topics of the project were held on international conferences or workshops, three of them peer-reviewed, the others invited. Two papers have been published in proceedings. This shows that already after the first year the project achieved international visibility by the academic community. We will go on with our dissemination activity and expect more publications on conferences and proceedings on subtopics of the research performed within the project.

4.5 Workshop on RFID security

When beginning our RFID activities, we realized that the combination of the subjects *security* and *RFID* were mentioned as side topic in several RFID-related conferences and workshops, but there was no event that served as meeting point for people interested in the combination of both topics.

Due to the starting privacy discussion in RFID technology, there were quite a lot of suggestions to deal with the security topic, but since there was no dedicated workshop it was seldom the case to meet researchers with the same interest. Due to the special requirements for tags and RFID systems, general purpose approaches did not provide a good starting point for a satisfying solution. Soon it became clear that high specialization was necessary to deal with RFID security. Researchers from different directions, IT-security specialists from one direction, and communications or microelectronics experts from the other direction got involved with very different starting suggestions. While the researchers from the security area trifled with the power limitations and throughput requirements of tags, the experts from non-security areas started with suggestions that neglected well-established security principles. Without a central meeting point, there was little chance that a common understanding of the topic would arise. Depending on the community present on the workshop, either the one or the other direction was favored during discussions, without considering inputs from the other direction. Observing this situation, we formulated our goal to start a new workshop series dedicated to RFID security and to establish it as the main event for the growing RFID security community. It was a dedicated goal to generate an environment that enables cooperation of experts from the security area with specialists with background in communications and microelectronics and to attract academic researchers and industry representatives.

In 2005 we were asked to organize the European Network of Excellence in Cryptology (ECRYPT)[5] *"Workshop for Lightweight Crypto"*, as planned in the work programme for the network. We used this opportunity and slightly renamed the workshop to *"Workshop on RFID and Lightweight Crypto"*. Mainly members from the ECRYPT network participated at this event in Graz. In the introductory talks of the workshop we defined the term *"lightweight crypto"* as *"lightweight implementation of state-of-the-art crypto"*. We illustrated the technological requirements for tags with a strong focus on passive tags with long reading distance. Additionally, we tried to point out that RFID security involves more topics than just privacy protection.

Already during the first occurrence it became clear that this event has a

[5] http://www.ecrypt.eu.org/

good chance to provide the central meeting point for researchers and industry interested in RFID security research. We agreed to organize a second edition in the following year, which should also attract participants not involved in ECRYPT. The RFIDSec workshop was born with this decision. The second workshop was already announced under the name *"Workshop on RFID Security 2006"*. By organizing the first two workshops, the *VLSI and Security* group, together with the *KRYPTO group* at IAIK were the initiators of the RFIDSec workshop series.

4.5.1 Introduction and workshop description

Meanwhile, the workshop for RFID Security is the reference workshop in the field of RFID security.

After the initial phase of two workshops in Graz, we wanted to involve more institutions for further development towards an open community of researchers. Rather than a yearly event in Graz, we called on other groups to organize the workshop, so that it took place in different venues. Although Graz is undoubtedly an important place for RFID technology and well known in the RFID community, we thought that a fixed location of the workshop might reduce the appeal for participation by the involved persons. After 2005, it was therefore organized in different places like Malaga (Spain), Budapest (Hungary) and Leuven (Belgium). 2010 the workshop will take place in Istanbul (Turkey). In 2008, the Asian edition of the workshop was started, which is an independent workshop that is strongly aligned with the original. In 2010 the second Asian RFIDSec workshop was held in Singapore. In the future closer cooperation is planned through combined workshops, cross invitations of best-papers presentations and joint proceedings.

To enable a development towards an internationally acknowledged scientific workshop, we invited recognized personalities to join the steering committee. Together they discuss ideas for the future development of the workshop and take decisions for further successful development. In 2010 we will publish for the first time official proceedings in Springer's Lecture Notes in Computer Science.

4.5.2 Goals and development of the workshop

When we started with our activity, our primary goal was to create a yearly event that congregates the academic researchers and leading industry players with interest in the technical security and privacy issues arising with RFID. Looking back at the participant lists from past events, we can state that this goal was achieved. Participants from RFID companies which are market leaders, as well as recognized professors from security research are regular visitors of the workshop. Meanwhile, side events with similar topics

come along with the workshop; they are often organized at the same location directly before or after RFIDSec, to attract workshop participants to stay a day longer and attend an additional event. In the last years typically 70 to 100 persons participated, many of them attending not only once.

Usually, the workshop consists of several invited talks and tracks with scientific presentations, which are selected by peer review of submitted research papers. The invited talks allow the organizers to put a focus on a specific sub topic. The list of topics of the yearly published call for papers is quite constant. It covers a variety of research activities, from security primitives and security protocols for RFID, over attacks and countermeasures, to applications of secure RFID technology. The first two editions had a strong focus on the awareness for the security requirements as well as the given requirements and limitations by the technology. This topic was selected to bridge the gap between activities in the cryptographic community and the RFID community with microelectronics background. In later editions we shifted the focus to different aspects like data protection in the context of RFID technology, or on the implications of successful attacks by academic researchers on commercial RFID-security products.

Nowadays, security is referred to as a hot topic when RFID technology is discussed and much more people and institutions are involved in research activities than several years ago. Together with the development towards a heterogeneous Internet of Things, and with the suggested integration of sensors into passive RFID tags, the interest in security topics for RFID will still rise. Therefore, we expect a successful further development of the workshop.

Part III

Future developments and conclusions

5

Future developments of RFID security research

Due to the fast development of RFID, sensor networks and similar technologies one should come to the conclusion that it would be better not trying to forecast future developments. The often predicted hype in RFID technology did not happen as assumed; at least, the development was not that fast as predicted. Although sensor networks are available at the moment they are not yet ubiquitously existent, but still niche applications or research projects. We should not think that our current predictions would be much more accurate. This chapter focuses therefore not on global developments of the IoT or its technologies, but discusses the future activities expected to happen in the *VLSI and Security* group at IAIK.

Our research is motivated by a vision towards a secure IoT. Each single research activity or project is a small step towards realization of this vision which itself is adjusted continuously by the achieved results and the ongoing developments. To allow for a proper development of the group it is necessary to continually generate new ideas and plans for future activities. The following sections inform about our plans and ideas for upcoming projects. Some of the ideas presented are logical follow-up activities of running or completed projects. Others are maybe less apparent, but we consider them as interesting approaches for the future. In some cases, the topics mentioned are suggestions of submitted proposals for projects. Plans to investigate these topics are quite precise and realistic plans exist to start the activities. Other presented ideas are less elaborated but mentioned here

because they appear challenging, necessary and interesting so that we will consider them soon in upcoming proposals.

In general it is visible that our activities move towards higher levels, from sole chip development to system architectures, protocols and application design. During the starting phase of our RFID activities they were concentrated on hardware implementation activities. We still try to focus our research on chip development activities, but often it is not enough to scrutinize only low-level technology issues. Meanwhile, our activities involve protocol extensions, system architecture development, and more. The wider picture helps to see possibilities for further optimization and is therefore often necessary to achieve major steps. Nevertheless, the majority of our activities will deal with implementation of optimized security hardware, which is the core expertise of the team.

5.1 Integration of passive tags into IP networks

Many of the security issues discussed arise due to the connection of RFID applications to the Internet. In other words, the combination of RFID applications and the Internet is an effect of the evolvement from closed-loop architectures to open-loop applications. Not all future applications will require an open-loop architecture, but a variety of new and innovative application scenarios for RFID builds on open-loop architectures. Although this is not a big issue for most current applications, it seems a natural step for us to integrate tags seamlessly into the IP network, so that the tags and the readers can be addressed like any other node in the Internet.

The current EPC network is designed to make data from tags available from a "server" or a distributed network of servers. It defines interfaces and services for data exchange for RFID applications, with a strong focus on logistics. The main services are the EPCDS to locate where the information associated to a specific tag is stored, and the EPCIS, which stores and provides the relevant data for every tag. During the design of the EPC network it was assumed that the tags send their ID and nothing else. Additional tag features, like storage of data on the tags or cryptographic services were not really considered.

IPv6 provides a 128-bit address space, which is enough for the expected number of participating devices in the IoT. The slow adoption of this new protocol is an issue in many publications. Still, the migration to Internet Protocol Version 6 (IPv6) is still behind expectations. The number of available addresses in IPv4 is nearly exhausted, therefore we can assume that the migration to IPv6 will take place faster in the years ahead. There is no other promising approach to deal with the shortage of addresses. IPv6 has improved support of security protocols compared to its predecessor

(IPv4). It includes Internet Protocol Security (IPSec), a recognized way to establish secure connections in the Internet. The standard includes improved concepts to include mobile nodes, it even allows point-to-point communication between two mobile nodes.

The integration of passive tags into IPv6 networks would allow for enhanced communication to and from tags from any other node in the network. We think that future tags will be able to store or generate data; therefore we do not consider to limit the data flow into one direction from the tags to the servers only. Once addressed, the tags should also be able to receive data packages from any authorized node in the network.

Logically, IPv6 will add quite a communication overhead for the tag-reader link; but especially for scenarios where tagged objects are mainly static, this is not necessarily a drawback. We think it is an interesting challenge to investigate integration of tags via IPv6 home agents as foreseen in the concept for mobile nodes. A first step could be an addressing mechanism for tags. It will be necessary to modify the reader firmware in a way that they inform the respective home agents about the presence of 'their' tags in the reader's neighborhood. The tag-to-reader protocol needs to be extended or modified to allow the transfer of IPv6 packets. In a second step we want to investigate the feasibility of security mechanism according to IPSec. This is the point where our specialization in security can be taken into account. The final goal would be to use the already designed security primitives for tags, like AES or SHA-1 and ECDSA in an IPv6 communication secured by IPSec mechanisms. This would be a way to guarantee the compatibility of future tags to other parts of the Internet.

The planned activities will be performed on basis of protocol simulation tools and network simulators. If the simulation delivers acceptable results, so that we think an implementation of real readers and tags is meaningful, we will consider a prototype implementation on basis of our semi-passive programmable tags. It is probably not meaningful to produce tag chips as long as the concept can be demonstrated on basis of less expensive prototypes. We will disseminate our results and suggestions by scientific papers to analyse the feedback from reviewers and the community.

5.2 Extended security services for RFID tags

Our suggestions to security in RFID technology from the projects ART (see section 4.1), BRIDGE (section 4.3) and SNAP (section 4.2) follow already this approach. We started to suggest tag authentication as security service a cryptographic tag can provide. We want to point out that cryptography on tags is not the only way to provide security services. Our approach has been taken up by the Austrian ISO body for a "work-item proposal" towards a standard for security extension for tag-to-reader communication.

The advantage of this approach is that it opens the way for a variety of different implementations and therefore it has good chances to get common agreement in the standardization procedure. In our future activities we try to investigate more cryptographic services. Within the currently running project CRYPTA (Section 4.4) we implement a signature generating primitive on a passive tag and use this for tag authentication. The application uses this service for a proof of origin of the tagged good. The signature service can be used also to provide "data integrity" for data that was generated by the tags themselves. Data from integrated sensors can be signed by the tags, which assures that modification of this data on its way to a central application can be detected. A cooling-chain operator who uses sensor tags on goods can then be sure that the received data was not modified by a sleazy distributor who might have the idea to modify the received data after an incident that could affect his income.

With a cryptographic signature, trusted tags can sign data that was sent from un-trusted readers to the tag. The signed data can then be delivered back to the reader. An application can use such a signature to check whether a reader have been communicating with a trusted tag, a feature that, for example, is useful in scenarios where mobile reading devices want to prove their presence at defined locations.

Beside cryptographic services that can be established using already existing and implemented primitives we have further ideas for future activities. Often we observe problems with control over data when tagged goods are handed over to new owners. The privacy discussion results from such an ownership transfer. Consumers often do not accept that retailers might still control the data on the tags attached to goods belonging to the customers. The current solution is execution of the the kill command at the POS, where the tagged good changes ownership. This is not an ideal solution. We discuss the problems with the kill command in subsection 2.3.1. To get control of the data on the tags, a secure change of the key material can be useful. Such a key exchange would allow the end-user to deny future access for the retailer while keeping the tag's features available for own applications. Such procedures are referred to as transfer of ownership, which involves typically interaction of the old and the new owner and in some suggestions a trusted third party. Cryptographic functionality can help to achieve secure transfer of ownership, which means that the new owner can be sure that the old one (or any eavesdropper) has no chance to get information about the new key material. End-user privacy is not the only motivation for such procedures. Whenever tagged objects change their ownership the new owner wants to ensure full control for the involved data and guarantee that the old owner does not get any critical information.

Access control is currently the most important application area for passive contact-less security tokens. An often discussed problem of current solutions is that during the authentication process the party who asks for

access needs to identify, so that the verifying party can decide to grant or deny access. We think that better privacy protection can help to raise the acceptance of contact-less devices and open new markets for this technology. The trusted-computing community has developed methods to solve this problem. Direct Anonymous Attestation (DAA) [9] is a promising approach to provide anonymous authentication. In an access control system this means that a party can demonstrate its right to get access, without the need to reveal her identity to the prover. The current suggestion for DAA is very complex and too complex for passive devices. Our planned activities involve the investigation of modification of used cryptographic principle to ECC and development of prototypes to assess the performance. We plan to investigate the possibilities to modify the methods in a way so that the necessary computation on the tag is reduced without reducing the security. This activity will be performed in close cooperation with the trusted-computing specialists from IAIK.

5.3 Split computing and pre-computation

Passively powered devices suffer from limited computation capabilities. Security primitives, especially asymmetric ones include computation intensive operations. These two statements describe the principal problem we face when proposing security mechanisms for the Internet of Things. There are several ways to solve this problem. So far we have tried to use optimized silicon processes and to implement the digital circuits as efficient as possible so that computation of selected algorithms becomes feasible. On the other side, we observe that passive tags are mainly idle. When they enter a reader field, they wait passively for a request of the reader. Once selected, they reply with their ID or additional information. Depending on the application, the idle time is long compared to the active time. This observation lead us to the idea that tags could start activity before they get addressed. First steps in this directions were published in [36]. The idea of the authentication scheme GPS was to allow pre-computation of so-called coupons and to store them on low-resource devices. During each authentication procedure the device uses a coupon which then expires. When all coupons are used, the device cannot authenticate anymore. We extended the idea in a way that the device can compute coupons by itself. Assuming that the tag is sufficiently long in an RF field, the performance requirements for this coupon pre-computation are rather low, which allows optimization of the necessary arithmetic path. Clearly, the described approach is not useful for all applications, but it opens new directions for optimization. GPS was designed with this pre-computation in mind, therefore it was a logical first step. In the future we want to analyze whether pre-computation is also feasible for other security schemes, or in a next step how existing schemes

need to be modified such that pre-computation becomes feasible. The approach can be analyzed on algorithmic as well as protocol level. So far we have first ideas to apply the approach to other schemes like ECDSA, but we did not yet have the chance to investigate the approach in more detail.

An extension of this idea is split computation. Tags enter and leave reader fields unpredictably, so they might be interrupted in their pre-computations before coming to a result. The more the computation circuit is optimized (resulting in longer computation time), the higher is the chance to be interrupted when the tagged objects moves out of the reader field. Under the term split computation we understand an approach to define points during the computation for storing intermediate results. In case that the operation is interrupted, the tag can resume the operation using the stored intermediate result. Finding viable points for storing intermediate results is an intricate task, because storing intermediate value adds overhead. Cryptographic protocols and primitives need to be scrutinized to evaluate whether the approach provides enough benefits. As far as we know, this area is completely unexplored in the context of cryptographic primitives. We think that together with pre-computation, this approach may allow the application of more complex security mechanisms for passive devices in the future. If all additional options for tradeoffs due to pre-computation and split computation are considered and exploited on all levels (from chip design, security algorithm design, the security protocol and the communication protocol) a variety of extended security services might become feasible without noticeable overhead or limitation for the final application.

5.4 Indirect tag-to-tag communication

So far, tags and readers communicate in a direct point-to-point connection. After the anti-collision procedure the reader selects a tag to communicate with. The selected tag answers in the defined time-slot to the reader's request directly afterwards. All other tags listen passively to the reader commands and stay idle until they are addressed. The tag's demodulator allows all other tags to eavesdrop the commands issued to the tags in their neighborhood; however, a typical tag cannot de-modulate the messages of the tags to the reader. Listening to the commands of a reader, a tag can already get some information. E.g. it can find out what tags are in their neighborhood by decoding the address of the reader commands, a process they need to do anyway to find out whether they are addressed themselves. We can consider advanced tags that behave differently in case they detect that certain tags are in the field. This behavior can be exploited in applications where assembled objects carry more than one tag. The product might consist of various parts, each tagged with its own tag. As example we can

consider a small portable computer that consists of a tagged CPU, a tagged display and a tagged hard disk. If this components appear together close to a reader, it would be nice for the RFID application to get the information that the portable computer was detected directly. Once disassembled, the detailed information about the computer's components can be interesting. A decision that can be taken by the tags themselves, listening just to the communication sent by the reader. If e.g. the hard disk finds out that the display and the CPU are in the field, then it assumes that it is integrated within a computer and stays quiet during an inventory request. This example is not only one application idea we had so far, we consider this approach is very promising for the future development. Thinking further, we can provide additional extensions of the tag-reader protocol. This would allow the tags to communicate with each other, although they cannot de-modulate the signals of tags. We can define commands for the message from tags, which tell the reader to forward the content to another tag in the field. Clearly, this procedure is not practicable for tags moving fast through a reader field, but only useful for static situations where tags remain in the field for a longer time. Once we can provide connection between passive tags via a reader as relay, the next challenge is to protect this channel. We can consider situations where tags in a field trust each other, but the reader is an un-trusted device. Using the tag's cryptographic capabilities, we can protect the indirect tag-to-tag communication against illicit modifications by a rouge reader of even against unwanted eavesdropping by the reader that acts as relay. Especially during transfer of ownership of tags such protection is useful. In [71] the authors present an idea to use an additional device to enable a secure transfer of ownership. Considering protected indirect tag-to-tag communication, such approaches become much more practicable, because this additional device can also operate fully passively. The interesting feature of our concept is that it would not require a modification of installed reader hardware. The protocol extensions can be integrated through firmware modifications of the readers. This makes adoption of our suggestion much more likely.

So far the idea hass not been further elaborated. We suggested investigation of the topic in proposals for future cooperative projects, but we did not yet get acceptance. We are not aware of any other academic research group following this direction. Our results from previous projects (protocol simulators, programmable tags, protocol extensions, cryptographic modules) provide a good basis for future research in this direction.

5.5 Protection for sensor-enabled passive tags

Currently, tags equipped with sensors are a hot topic in the research community. Researchers investigate the possibilities of adding various sensors

to passive RFID devices. In contrast to wireless sensor nodes, such sensor-enabled tags communicate passively, they can operate without own energy source, and they can be produced inexpensively. This means, they qualify for mass applications with a very high number of distributed sensors at reasonable overall costs. So far, prototypes have been demonstrated e.g. by Intel. They achieved to build passive programmable tags that featuring three different sensors. The tags are called Wireless Identification and Sensing Platform (WISP)[1]. The WISP is an interesting platform and even more powerful devices can be expected in the near future. They use a standardized UHF RFID protocol (ISO-18000-6c) to communicate with readers. An ISO subgroup is already actively working on an extension of the current standard to provide a standardized way for communication of sensor data.

So far, most proposals for applications of sensor nodes assume that the sensors communicate with a trusted reader in a secure environment. We think that the sensor-enabled tags will have no chance on the market as high-volume products, as long as no proper protection for the tags is available. Following our vision for the Internet of Things as an open network, sensor tags will communicate with non-trusted readers in completely unprotected environments. Applications running on central servers will collect data from distributed tags via mobile or stationary readers. In addition to all security problems known in the traditional Internet, we face additional ones due to the special characteristics of passive sensor nodes. To point out the importance of data protection when tags are equipped with sensors, we illustrate some vulnerabilities:

- *Fake or virtual sensors:* When distributed sensors communicate with standardized readers which send their data to central servers, it is easy for attackers to spoof the ID of tags or simulate entire tags. Replacing "official" tags by modified ones allows attackers to insert arbitrary data into the system. We suggest proper authentication mechanisms for tags with sensors, so that applications can rely on the data they receive.

- *Modified sensor data:* As a typical application for passive sensor tags, often inspection of cooling-chains in grocery logistics is mentioned. We think that the application of sensor tags in this context is only useful when proper protection of the tags themselves and the data they send are guaranteed. Otherwise it is simple to hide any interruption in the cold chain by modifying the stored data on the tags themselves, or on the way to the central server. It is therefore important to provide a proof of data integrity for the values coming from the tags.

[1] http://seattle.intel-research.net/wisp/

- *Sensor configuration:* Sensor-enabled tags will be more complex than simple RFID tags. Not every application will use every feature, nevertheless, mass production will be necessary to produce them at a competitive price. A possibility to deal with this is to produce a generic platform which can be configured for a specific purpose. The access to such configuration data needs to be protected, otherwise attackers might re-configure distributed tags in a way that was not foreseen.

- *Implementation attacks on sensor tags:* We assume that such sensor tags will be rather inexpensive devices which will be pervasively available in our environment. Due to the fact that they will not have continuous connection to readers, but only sporadic communication, such tags will get lost regularly. At least, the issuers will have no measure to get a status report of their tags when they are outside a reading spot. This means that they are easily available as targets for attackers. They can take tags in their lab and experiment with them. We have a similar situation with smart cards, where attackers can tamper with them at rather low costs, but the situation is even worse with tags. While your bank or phone operator might get suspicious if an attacker orders regularly new cards because they did not survive an attack, it will be very hard to find out when inexpensive sensor tags disappear. This makes such devices very interesting targets for any kind of implementation attack, like for instance SCA. An accurate investigation of the threat should be done and proper countermeasures need to be designed before commercial products can use the technology.

The above list is most likely not complete. We are not informed of any activity to investigate attack scenarios and associated risks for applications with passive sensors, but this is not the main direction we want to go. With these examples we simply want to illustrate the need for protection of the sensors. In our opinion, this is an important area, but we do not see a lot of activity in the research community. At the same time, we want to suggest protection mechanisms that fit to the technology. We think that especially protection against implementation attacks is an important topic. As the first step we got in contact with Intel's research group that developed the WISPs and suggested to investigate the possibilities to implement AES on a tag. Additionally, we want to investigate their susceptibility against SCA. In a next step we hope to get in closer cooperation for a more detailed investigation of security mechanisms for passive sensor nodes.

5.6 Electronic signatures for objects

Asymmetric cryptographic primitives can be used to generate signatures for digital content by application of the private key. Verifiers can check the signature using the public key of the signing party. Together with the appropriate legal framework and digital certificates it is nowadays possible to lawfully sign digital content electronically. Such electronic signatures will probably not replace hand-written signatures in all cases, but they are very useful in electronic business processes to avoid additional paperwork. In some countries it is meanwhile possible to replace handwritten signatures by electronic ones with equivalent legal status. IAIK is actively involved in this research area. Many applications, from eGovernment to eBusiness (e.g. electronic banking) benefit from electronic signatures.

Also in the context of the Internet of Things, electronic signatures may become an interesting topic. So far, in the Internet, the electronic signature is bound to a person as legal identity. It can be seen as the transformation of the handwritten signature on paper documents to virtual documents. Still, the sender and the recipient of the data or documents are natural persons. In the IoT, objects or things will trigger communication of data, not only to persons, but also to other objects. It is clear that from a legal perspective a signature is probably meaningless in this context, since objects cannot be made liable for their actions. Nevertheless, it would be an interesting task to investigate if the concept of digital signatures is meaningful or useful for processes and transaction which will happen in the IoT. We can imagine that objects sign data they receive to allow for later verification. We have shown already that it is technically feasible to compute digital signatures on passive tags with the same key-length and security parameters as electronic signatures according to the Austrian law. Although an electronic signature performed by objects will not reach the same legal status as an electronic signature issued by a person, compatibility of both is meaningful. Existing back-end infrastructures, like implementations of CAs, revocation services, verification services, could be directly ported to applications for the IoT.

So far no activities have been started in this direction. We think that an illustrative application scenario is necessary to motivate further research in this direction. We are still in a brainstorming phase, but soon we will come up with a good suggestion to move forward in this direction.

5.7 Computation capabilities depending on reading distance

We have shown that implementation of cryptographic primitives is possible on passive tags, and that still more possibilities for trade-offs for implementation of more complex algorithms exist (such as pre-computation).

Nevertheless, in all cases we trade the time for computation with the reduction of power during calculation to deal with the scarce resources available on tags. For applications, where tags move rapidly through reader fields (which is typically the case in logistics) the ideas described above might not fit. Additionally we need to take into account that the tag chips suffer from a variation of parameters during production, and they are designed to operate in the maximum reading distance. This means that the requirements for digital circuitry on tags are specified in a way, so that they still operate in maximum reading distance, even when the actual chip comes from a production run with worst-case parameters. Production variances and full functionality in maximum reading distance make therefore the problem for the designer even harder. We do not see a big chance to heavily reduce the production variances, especially due to the fact that the price for tag chips needs to be very low to be competitive on the market. On the other hand, we can assume that tags are not always operating in the maximum reading distance, or that the application might accept that the functionality of the chip varies with the strength of the EM signals the tags receive. Although not yet considered, it would be possible for the receiver circuits on a tag to detect the signal strength of the EM field and to activate specific parts of the tag only when enough power is available. Such tags would provide basic functionality in the maximum reading distance, and extended features when brought closer to the reader antenna.

6 Conclusions

In the first part of this thesis we start with explaining the reasons why we think that passive RFID tags play an important role for the development of the Internet of Things. Estimating the future number of tags on behalf of current production, we expect that the number of passive tags will soon surpass by far the number of any other devices contributing to the future network. The fact that they can operate without own power supply in addition to their low price will make the integration of day-to-day things or items into the future networks possible. Their strong limitations in terms of computation and communication capabilities require special attention when security concepts are considered. We mention early solution for protection of RFID tags and provide reasons why such currently existing approaches are not sufficient for the future evolution of the technology. In addition we suggest an approach that is based on standardized cryptographic primitives and established security protocols to enable proper development. This approach is considered good practice in the IT-security community and is e.g. followed during the design and implementation of security tokens like smart cards. In a dedicated section we explain how it may become feasible to implement this approach also on passive RFID tags.

In part two of this thesis we report on research projects with RFID relevance which took place at IAIK. The description of our most relevant research projects ordered chronologically and also documents the development of the research activities. We started with projects that were mainly oriented towards our expertise in the development of efficient digital circuits for cryptographic computations (project ART). Shortly after we were

able to show our first results, a proof in silicon that it is possible to compute AES on passive RFID tags. In follow-up projects, we got involved in research and development tasks towards security concepts for specific application scenarios (project SNAP), in development of prototyping and simulation tools, and in standardization activities (BRIDGE). In the latest project (CRYPTA) we investigate the potential of asymmetric cryptography for RFID application scenarios and propose a security concept based on tags with ECDSA functionality.

In the third part, we inform about our ideas for future activities in the area of security research for the IoT. We present what we have in mind for future research. Some of the suggestions are quite elaborated, so that start of the activity is very probable or has been already decided, while other ideas are not yet more than results of brainstorming sessions or coffee-break discussions.

The content of this work should be more than just a documentation of performed research tasks. Therefore we do not go in too much technical detail. Most of the work is documented in project deliverables[1] or research papers. Instead, we wanted to document the development of a research group along a defined vision. Throughout our work we had a clear vision in mind. Step by step we achieved enough results so that meanwhile our publications are regularly cited when other researchers publish their new approaches. While it was quite complicated in the beginning to find partners from the RFID industry for collaborative research projects we get now regularly invited to join new project proposals.

When we started to design cryptographic modules for RFID technology in 2004, our first proposals to include standardized security primitives into passive tags did not earn a lot of positive feedback from the community. Meanwhile, we can refer to more than 800 citations of our most important publications[2] in the area (see Annex for a list of citations). We think that this proofs the relevance of our results. This result is not the work of one person; such a visibility is only possible when all members of a team are working together. Beside careful investigation and specialized expertise to implement the prototypes, also less technical tasks like dissemination of results, project coordination, and active involvement in the research community is necessary. In addition to our research we tried to involve our topics into teaching activities, so that motivated students get in contact with the topic throughout their curriculum. Beside student projects with RFID-security focus, we organized a summer school and a spring school dedicated to RFID technology[3] for 150 students altogether.

[1] In case that they are publicly available, they can be accessed via the respective project web sites

[2] Harzing, A.W. (2009) Publish or Perish, version (2.8.3644), available at www.harzing.com/pop.htm

[3] PROACT summer school 2006 and spring school 2007; see http://proact.tugraz.at/

The author of this thesis does not claim that his sole contribution was the reason for the development. It is an achievement of the overall VLSI team at IAIK and probably also a result of a good portion of luck starting with a research topic at the right time. On the other hand, researching successfully in an academic team requires a clear vision towards the goals and a clearly visible motivation with enough freedom for every individual researcher, so that every member can identify with the team's vision but still follow her personal research interests. Such an environment does not develop by itself, but requires careful selection of new team members, coordination, ongoing assessment and quite an amount of project acquisition and project management tasks. The author of this thesis claims that the development of the RFID research at IAIK happened under his sole responsibility as group coordinator. Although well supported by the head of the institute, and the other group leaders it was his decision to research in this direction and to put even more focus on it after the first visible results.

It was not only our work that forced the community to re-think the early approaches. Attacks on RFID applications like the Mobile Speedpass system by researchers from Johns Hopkins University, or the attack on NXP's Mifare tags helped us definitely to promote our approach. A very recent attack on *Legic Prime*, presented by Karsten Nohl and Henryk Ploetz at the 26^{th} Chaos Communication Congress in December 2009[4], gives additional evidence that the approach of undisclosed proprietary protection measures is not secure. Interesting about this attack is that the *Legic Prime* system was advertised as "high-secure technology" and is said to be used for access control in German airports and power plants. Those attacks all got high press coverage and helped us promoting our suggestions to use standardized security primitives and protocols. In our lab we also perform analyzes of crypto chips, but at the beginning we decided not to analyze (or break) existing products. The reason for this decision was not only the close cooperation with research partners from industry who were definitely not interested in accurate analysis of their products with later publications of the results. Our decision against analysis was also taken in favor of suggesting innovative solutions rather than (quite work intensive) reverse-engineering of proprietary and secret solutions. We hoped that our suggestion to follow good practice in IT security (meaning not to rely on undisclosed proprietary measures), together with the proof that it is technically feasible, would suffice to convince others. A hope that was just partly fulfilled. But when the first attacks appeared we used the references as good arguments for proper protection.

We think that currently compatibility of the suggested protection measures for RFID to other network layers and already installed RFID infrastructure is an important issue. We think further that suggestions that

[4]http://events.ccc.de/congress/2009/Fahrplan/events/3709.en.html

would require a complete re-design of installed systems will fail, because system operators would refuse to adopt when they cannot re-use already existing components. On the other hand, we think that without meaningful protection the development of the current technology to an pervasive and ubiquitous Internet of Things can be blocked when security bottlenecks are not eliminated. Nowadays the discussion of end-user privacy protection is apparent and considered a major roadblock. It is no surprise that companies are still precautious when open-loop RFID services and connection to the Internet are suggested. As long as it is not clear how all level of such system can be protected against attacks, the transformation of closed-loop applications to more open architectures will be postponed.

In his very early paper about ubiquitous computing [76], Mark Weiser mentioned that cryptographic techniques will be necessary to protect the communication of distributed computing devices. This is also true for passive tags, and we think that one reason for the lag in the development of ubiquitous computing was the absent protection for wireless communication channels of low-cost devices. We think that our work during the last years was an important contribution in this direction and for the development of the current state of the art in RFID security. Following our prospects about the importance of passive tags, our contribution is valuable for the future development of the Internet of Things. We are aware that still a lot of issues are open and much more research is necessary. Nevertheless, we are on the way to provide feasible solutions for secure applications in the future of the Internet of Things.

Bibliography

[1] M. Aigner. Seven reasons for application of standardized crypto functionality on low cost tags. http://www.rfidconvocation.eu/Convocation.htm, 03 2007.

[2] M. Aigner, S. Dominikus, and M. Feldhofer. A System of Secure Virtual Coupons Using NFC Technology. In *Workshop on Pervasive RFID/NFC Technology and Applications (PerTec07), New York, USA, March 19, 2007, Proceedings*, pages 362–366. IEEE, March 2007.

[3] M. Aigner and M. Feldhofer. Secure Symmetric Authentication for RFID Tags. In *Conference on Telecommunication and Mobile Computing – TCMC 2005, Graz, Austria, March 2005, Proceedings*. Graz University of Technology, March 2005.

[4] M. Aigner and E. Oswald. Softwaremodelle zur Festellung der DPA-Anfälligkeit von Hardwaremodulen. In W. Mayerwieser and K. C. Posch, editors, *Proceedings of Austrochip 2000, October 13, 2000, Graz, Austria*, pages 39–46, October 2000.

[5] M. J. Aigner. Crypto implementations for RFID tags; learnings from smart card security.", 2006. Presentation.

[6] G. Avoine and P. Oechslin. A Scalable and Provably Secure Hash-Based RFID Protocol. In *3rd IEEE Conference on Pervasive Computing and Communications Workshops (PerCom 2005 Workshops), Kauai Island, HI, USA, 8-12 March 2005, Proceedings*, pages 110–114. IEEE Computer Society, March 2005.

[7] H. Bock, M. Braun, M. Dichtl, E. Hess, J. Heyszl, W. Kargl, H. Koroschetz, B. Meyer, and H. Seuschek. A Milestone Towards RFID Products Offering Asymmetric Authentication Based on Elliptic Curve Cryptography. Invited talk at RFIDsec 2008, July 2008.

[8] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security Analysis of a Cryptographically-Enabled RFID Device. In *USENIX Security Symposium, Baltimore, Maryland, USA, July-August, 2005, Proceedings*, pages 1–16. USENIX, 2005.

[9] E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, pages 132–145, New York, NY, USA, 2004. ACM.

[10] D. Carluccio, K. Lemke, and C. Paar. Electromagnetic Side Channel Analysis of a Contactless Smart Card: First Results. In E. Oswald, editor, *Workshop on RFID and Lightweight Crypto (RFIDSec05), July 13-15, Graz, Austria*, pages 44–51, 2005.

[11] C. Chatmon, T. van Le, and M. Burmester. Secure Anonymous RFID Authentication Protocols. Technical report, FSU Computer Science, March 2006.

[12] C. De Cannière, F. Mendel, and C. Rechberger. Collisions for 70-step sha-1: On the full cost of collision search. In M. J. W. Carlisle M. Adams, Ali Miri, editor, *Selected Areas in Cryptography*, volume 4876 of *LNCS*, pages 56 – 73. Springer, 2007.

[13] G. de Koning Gans, J.-H. Hoepman, and F. Garcia. A practical attack on the MIFARE Classic. In *8th Smart Card Research and Advanced Application Workshop (CARDIS 2008)*, volume 5189 of *Lect. Notes Comp. Sci.*, pages 267–282. Springer, 2008.

[14] S. Dominikus and M. J. Aigner. mCoupons: An application for Near Field Communication (NFC). In *AINA Workshops (2)*, volume AINA Workshops (2), pages 421–428. IEEE Computer Society, 2007.

[15] S. Dominikus, E. Oswald, and M. Feldhofer. Symmetric authentication for RFID systems in practice. In *Workshop on RFID and Lightweigth Crypto, July 13-15, 2005, Graz, Austria*, 2005.

[16] S. Dominikus, E. Oswald, and M. Feldhofer. Practical Security for RFID: Strong Authentication Protocols. In P. Horster, editor, *Proceedings of D.A.C.H. Mobility 2006, October 17-18, 2006, Graz, Austria*, pages 187–200. Syssec, 2006. ISBN 3-00-019635-8.

[17] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani. On the power of power analysis in the real world: A complete break of the KEELOQ code hopping scheme. In *CRYPTO*, pages 203–220, 2008.

[18] EPCglobal. EPCglobal tag class structure, Whitepaper:tag class definitions v1.0. http://www.epcglobalinc.org/standards/, 11 2007.

[19] M. Feldhofer, M. Aigner, and S. Dominikus. An Application of RFID Tags using Secure Symmetric Authentication. In P. Georgiadis,

S. Gritzalis, and G. F. Marias, editors, *1st International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU 2005, Santorini Island, Greece, July 14, 2005, Proceedings*, pages 43–49. Diavlos Publications, July 2005. In conjunction with the IEEE ICPS'05.

[20] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems using the AES Algorithm. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems – CHES 2004, 6th International Workshop, Cambridge, MA, USA, August 11-13, 2004, Proceedings*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370. Springer, August 2004.

[21] M. Feldhofer and C. Rechberger. A Case Against Currently Used Hash Functions in RFID Protocols. In S. Dominikus, editor, *Workshop on RFID Security 2006 (RFIDSec06), July 12-14, Graz, Austria*, pages 109–122, July 2006.

[22] M. Feldhofer and J. Wolkerstorfer. Low-power Design Methodologies for an AES Implementation in RFID Systems. In *Workshop on Cryptographic Advances in Secure Hardware 2005 (CRASH05), September 6-7, Leuven, Belgium*, September 2005.

[23] M. Feldhofer and J. Wolkerstorfer. Strong Crypto for RFID Tags - Comparison of Low-Power Hardware Implementations. In *IEEE International Symposium on Circuits and Systems (ISCAS 2007), New Orleans, USA, May 27-30, 2007, Proceedings*, pages 1839–1842. IEEE, May 2007.

[24] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen. AES Implementation on a Grain of Sand. *IEE Proceedings on Information Security*, 152(1):13–20, October 2005.

[25] C. Floerkemeier, M. Langheinrich, E. Fleisch, F. Mattern, and S. E. Sarma, editors. *The Internet of Things, First International Conference, IOT 2008, Zürich, Switzerland, March 26-28, 2008. Proceedings*, volume 4952 of *Lecture Notes in Computer Science*. Springer, 2008.

[26] C. Floerkemeier and R. Pappu. Evaluation of RFIDSim - a Physical and Logical Layer RFID Simulation Engine. In *Proceedings of IEEE International Conference on RFID 2008*, 2008.

[27] C. Floerkemeier, M. Wille, and S. Sarma. RFIDSim - A Physical and Logical Layer Simulation Engine for Passive RFID. *IEEE Transactions on Automation - Special Issue RFID*, 2008.

[28] F. D. Garcia, G. de Koning Gans, R. Muijrers, P. van Rossum, R. Verdult, R. Wichers Schreur, and B. Jacobs. Dismantling MIFARE classic. In S. Jajodia and J. Lopez, editors, *13th European Symposium on Research in Computer Security (ESORICS 2008)*, volume 5283 of *Lect. Notes Comp. Sci.*, pages 97–114. Springer, 2008.

[29] F. D. Garcia, G. Koning Gans, R. Muijrers, P. Rossum, R. Verdult, R. W. Schreur, and B. Jacobs. Dismantling mifare classic. In *ESORICS '08: Proceedings of the 13th European Symposium on Research in Computer Security*, pages 97–114, Berlin, Heidelberg, 2008. Springer-Verlag.

[30] M. Girault, G. Poupard, and J. Stern. On the fly authentication and signature schemes based on groups of unknown order. *J. Cryptology*, 19(4):463–487, 2006.

[31] D. Grawrock. *The Intel Safer Computing Initiative*. Intel Press, 4 2006. ISBN-13 978-0976483267.

[32] J. Guerrieri and D. Novotny. HF RFID eavesdropping and jamming tests. Electronics and Electrical Engineering Laboratory, Electromagnetics Division, National Institute of Standards and Technology, Report No. 818-7-71, 2006.

[33] B. H. and A. M. J. Device and method for the calculation of encrypted data from unencrypted data or unencrypted data from encrypted data. Patent EP000001588518, January 2004.

[34] G. Hancke. Eavesdropping Attacks on High-Frequency RFID Tokens. In *Workshop on RFID Security 2008 (RFIDSec08), July 9-11, Budapest, Hungary*, RFIDsec 2008, pages 100–113, July 2008.

[35] D. Hein, J. Wolkerstorfer, and N. Felber. ECC is Ready for RFID - A Proof in Silicon. In *Workshop on RFID Security 2008 (RFIDsec08)*, July 2008.

[36] G. Hofferek and J. Wolkerstorfer. Coupon Recalculation for the GPS Authentication Scheme. In G. Grimaud and F.-X. Standaert, editors, *Proceedings of the Eight Smart Card Research and Advanced Application Conference, CARDIS '08, September 8-11, 2008, London, UK, Proceedings*, volume 5189 of *Lecture Notes in Computer Science*, pages 162–175. Springer, September 2008.

[37] M. Hutter, S. Mangard, and M. Feldhofer. Power and EM attacks on passive 13.56 MHz RFID devices. In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September*

10-13, 2007, Proceedings, volume 4727 of *Lecture Notes in Computer Science (LNCS)*, pages 320 – 330. Springer, 2007.

[38] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel. A practical attack on KEELOQ. In N. P. Smart, editor, *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2008.

[39] International Organisation for Standardization (ISO). ISO/IEC 9798-2: Information technology – Security techniques – Entity authentication – Mechanisms using symmetric encipherment algorithms, 1999.

[40] International Organisation for Standardization (ISO). ISO/IEC 15693-3: Identification cards - Contactless integrated circuit(s) cards - Vicinity cards – Part 3: Anticollision and transmission protocol, 2001.

[41] International Organisation for Standardization (ISO). ISO/IEC 18092: Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol, April 2004.

[42] A. Juels, R. L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In *10th ACM Conference on Computer and Communication Security, Washington, DC, USA, October 27-30, 2003, Proceedings*, pages 103–111. ACM Press, October 2003.

[43] U. Kaiser. Universal immobilizer crypto engine. Guest Presentation during Fourth Conference on the Advanced Encryption Standard (AES), 2004. The presentation slides were available via the conference web, they were removed after publication of the attack.

[44] U. Kaiser. *RFID Security, Techniques Protocols and System-on-Chip Design*, chapter Digital Signal Transponder, pages 177–190. Springer, 2008.

[45] M. Kasper, T. Kasper, A. Moradi, and C. Paar. Breaking keeloq in a flash: On extracting keys at lightning speed. In B. Preneel, editor, *Progress in Cryptology - AFRICACRYPT 2009, Second International Conference on Cryptology in Africa, Gammarth, Tunisia, June 21-25, 2009. Proceedings*, volume 5580 of *Lecture Notes in Computer Science*, pages 403–420. Springer, 2009.

[46] L. M. Katherine Albrecht. *The Spychips Threat: Why Christians Should Resist RFID and Electronic Surveillance*. Nelson Current, 2006.

[47] A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:pp. 538, Jan 1883.

[48] P. C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In N. Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, number 1109 in Lecture Notes in Computer Science, pages 104–113. Springer, 1996.

[49] S.-M. Lee, Y. J. Hwang, D. H. Lee, and J. I. Lim. Efficient Authentication for Low-Cost RFID Systems. In O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar, and C. J. K. Tan, editors, *Computational Science and Its Applications - ICCSA 2005, International Conference, Singapore, May 9-12, 2005, Proceedings, Part I*, volume 3480 of *Lecture Notes in Computer Science*, pages 619–627. Springer, May 2005. Available online at `http://dx.doi.org/10.1007/11424758_65`.

[50] S. Mangard, M. Aigner, and S. Dominikus. A Highly Regular and Scalable AES Hardware Architecture. *IEEE Transactions on Computers*, 52(4):483–491, April 2003.

[51] M. Mikka Lehtonen, A. Ruhanen, F. Michahelles, and E. Fleisch. Serialized tid numbers a headache or a blessing for rfid crackers? *In 2009 IEEE International Conference on RFID*, pages 233–240, 2009.

[52] D. Molnar. Security and Privacy in Two RFID Deployments, With New Methods For Private Authentication and RFID Pseudonyms. Master's thesis, University of California Berkeley, 2006.

[53] G. E. Moore. Cramming more components onto integrated circuits. *Electronics Magazine*, 1965.

[54] K. Nohl, D. Evans, S. Starbug, and H. Plötz. Reverse-engineering a cryptographic RFID tag. In *SS'08: Proceedings of the 17th conference on Security symposium*, pages 185–193, Berkeley, CA, USA, 2008. USENIX Association.

[55] NXP Austria GmbH. Website mifare.net - contactless smart cards. `http://www.mifare.net`.

[56] M. Ohkubo, K. Suzuki, and S. Kinoshita. Cryptographic Approach to "Privacy-Friendly" Tags. RFID Privacy Workshop, November 2003. Available online at `http://lasecwww.epfl.ch/~gavoine/download/papers/OhkuboSK-2003-mit-paper.pdf`.

[57] Y. Oren and A. Shamir. Remote Password Extraction from RFID Tags. *IEEE Transactions on Computers*, 56(9):1292–1296, September 2007.

[58] E. Oswald and M. Aigner. Randomized Addition-Subtraction Chains as a Countermeasure against Power Attacks. In Çetin Kaya Koç, D. Naccache, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, volume 2162 of *Lecture Notes in Computer Science*, pages 39–50. Springer, 2001.

[59] T. Plos. Implementation of a Security-Enhanced Semi-Passive UHF RFID Tag. Master's thesis, Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria, May 2007.

[60] T. Plos. Susceptibility of UHF RFID Tags to Electromagnetic Analysis. In T. Malkin, editor, *Topics in Cryptology - CT-RSA 2008, The Cryptographers' Track at the RSA Conference 2008, San Francisco, CA, USA, April 8-11, 2008, Proceedings*, volume 4964 of *Lecture Notes in Computer Science*, pages 288–300. Springer, April 2008.

[61] T. Plos. Evaluation of the Detached Power Supply as Side-Channel Analysis Countermeasure for Passive UHF RFID Tags. In M. Fischlin, editor, *Topics in Cryptology - CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009, Proceedings*, volume 5473 of *Lecture Notes in Computer Science*, pages 444–458. Springer, April 2009.

[62] T. Plos, M. Hutter, and M. Feldhofer. On Comparing Side-Channel Preprocessing Techniques for Attacking RFID Devices. In H. Y. Youm and M. Yung, editors, *Information Security Applications, 10th International Workshop, WISA 2009, Busan, Korea, August 25-27, 2009, Revised Selected Papers*, volume 5932 of *Lecture Notes in Computer Science*, pages 163–177. Springer, December 2009.

[63] T. Popp, S. Mangard, and M. J. Aigner. [DE] Verfahren und Schaltung zur abhörsicheren Durchführung von Rechenoperationen, [EM] Method and circuit for carrying out calculation operations secure from bugging, [FR] Procede et circuit permettant l'execution d'operations de calcul. Patent WO002007012102A3, May 2007.

[64] N. Pramstaller and M. Aigner. A Universal and Efficient SHA-256 Implementation for FPGAs. In E. Ofner and M. Ley, editors, *Proceedings of Austrochip 2004, October 8, 2004, Villach, Austria*, pages 89–93, October 2004. ISBN 3-200-00211-5.

[65] M. R. Rieback, B. Crispo, and A. S. Tanenbaum. Is Your Cat Infected with a Computer Virus? In *4th Anual IEEE International Conference on Pervasive Computing and Communications – PerCom 2006, Pisa,*

Italy, 13-17 March, 2006, Proceedings, pages 169–179. IEEE Computer Society, March 2006.

[66] D. L. B. . K. A. Sanjay Sarma. White paper: The networked physical world. MIT-AUTOID-WH-001.pdf, 10 2000.

[67] S. Sarma. White paper: Towards the 5 cent tag. http://www.autoidlabs.org/single-view/dir/article/6/197/page.html, 11 2001.

[68] S. E. Sarma, S. A. Weis, and D. W. Engels. RFID Systems and Security and Privacy Implications. In B. S. K. Jr., Çetin Kaya Koç, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, volume 2523 of *Lecture Notes in Computer Science*, pages 454–470. Springer, August 2003.

[69] A. Shamir. Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies. In Çetin Kaya Koç and C. Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2000, Second International Workshop, Worcester, MA, USA, August 17-18, 2000, Proceedings*, volume 1965 of *Lecture Notes in Computer Science*, pages 71–77. Springer, 2000.

[70] A. Shamir. Method and Apparatus for Protecting RFID Tags from Power Analysis. Patent Number WO 2008/019246 A2, February 2008. Available online at `http://www.freepatentsonline.com/`.

[71] A. Soppera and T. Burbridge. Off by default - RAT: RFID acceptor tag. *Printed handout of Workshop on RFID Security RFIDSec 06*, pages 151–166, 2006.

[72] C. Tutsch. Privacy in RFID - implementing a private and secure pseudonym-based RFID system. Master's thesis, Telematik, Graz, University of Technology, 2008.

[73] C. Tutsch, A. Soppera, T. Burbridge, and M. Aigner. RFID tag pseudonyms with efficient reading and scalable management. Poster at IOT 2008 - Internet of Things 2008, Zürich, March 2008.

[74] X. Wang and H. Yu. How to Break MD5 and Other Hash Functions. In R. Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*, pages 19–35. Springer, 2005.

[75] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In D. Hutter, G. Müller, W. Stephan, and M. Ullmann, editors, *Security in Pervasive Computing, 1st Annual Conference on Security in Pervasive Computing, Boppard, Germany, March 12-14, 2003, Revised Papers*, volume 2802 of *Lecture Notes in Computer Science*, pages 201–212. Springer, March 2003.

[76] M. Weiser. The computer for the 21st century. *Scientific American*, 265(3):94–104, 1991. http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html.

Appendix

Citation statistics for RFID publications of IAIK's VLSI Group (01/2010)

Cites	Authors	Title	Year	Source
4	S Dominikus, M Feldhofer, J Wolkerstorfer	Strong Authentication for RFID Systems Using the AES Algorithm	2004	CHES 2004
67	M Feldhofer	A proposal for an authentication protocol in a security layer for RFID smart	2004	The 12th IEEE Mediterranean Electrotechnical …
339	M Feldhofer, S Dominikus, J Wolkerstorfer	Strong authentication for RFID systems using the AES algorithm	2004	Lecture notes in computer …
5	M Feldhofer, J Wolkerstorfer	Low-power Design Methodologies for an AES Implementation in RFID …	2005	ECRYPT Workshop on Cryptographic Advances in …
16	M Feldhofer, M Aigner, S Dominikus	An application of RFID tags using secure symmetric authentication	2005	Proceedings of 1st International Workshop on …
23	S Dominikus , E Oswald, M Feldhofer	Symmetric authentication for RFID systems in practice	2005	ECRYPT Workshop on …
26	J Wolkerstorfer	Scaling ECC hardware to a minimum	2005	ECRYPT workshop-Cryptographic Advances in Secure …
27	J Wolkerstorfer	Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags?	2005	Workshop on RFID and Lightweight Cryptography, …
36	M Aigner, M Feldhofer	Secure symmetric authentication for RFID tags	2005	Telecommunication and Mobile Computing …
127	M Feldhofer, J Wolkerstorfer, V Rijmen	AES implementation on a grain of sand	2005	IEE Proceedings-Information …
3	M Feldhofer, C Rechberger	A case against currently used hash functions in RFID protocols. Printed …	2006	ECRYPT Network of Excellence, July
75	M Feldhofer, C Rechberger…	A case against currently used hash functions in RFID protocols	2006	LECTURE NOTES IN COMPUTER …
2	M Feldhofer	Comparing the Stream Ciphers Trivium and Grain for their Feasibility …	2007	Proceedings of Austrochip
4	M Aigner, S Dominikus, M Feldhofer	A System of Secure Virtual Coupons Using NFC Technology	2007	Pervasive Computing and …
5	M Feldhofer	Comparison of low-power implementations of Trivium and Grain	2007	State of the Art of Stream Ciphers Workshop (…
18	M Hutter, S Mangard, M Feldhofer	Power and EM attacks on passive 13.56 MHz RFID devices	2007	Lecture Notes in Computer Science
22	M Feldhofer, J Wolkerstorfer	Strong Crypto for RFID Tags-A Comparison of Low-Power Hardware …	2007	IEEE International Symposium …
2	M Hutter, JM Schmidt, T Plos	RFID and Its Vulnerability to Faults	2008	Lecture Notes in Computer Science
4	T Plos, M Hutter, M Feldhofer	Evaluation of Side-Channel Preprocessing Techniques on Cryptographic- …	2008	Workshop on RFID Security
5	Y Oren, M Feldhofer	WIPR-a public key implementation on two grains of sand	2008	Conference on RFID Security, Budapest, Hungary
8	T Plos	Susceptibility of UHF RFID Tags to Electromagnetic Analysis	2008	Lecture Notes in Computer Science
5	Y Oren, M Feldhofer	A low-resource public-key identification scheme for RFID tags and sensor n	2009	Proceedings of the second ACM conference …
823				

Statistics produced with Harzing, A.W. (2009) Publish or Perish, version (2.8.3644), available at www.harzing.com/pop.htm

Deutsche Fassung:
Beschluss der Curricula-Kommission für Bachelor-, Master- und Diplomstudien vom 10.11.2008
Genehmigung des Senates am 1.12.2008

EIDESSTATTLICHE ERKLÄRUNG

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

Graz, am …… ……..
(Unterschrift)

Englische Fassung:

STATUTORY DECLARATION

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

…… ……..
date (signature)