View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Georg-August-University Göttingen

Georg-August-Universität Göttingen
Faculty of Mathematics and Computer Science

PHD THESIS

Towards a Lightweight, Secure, and Untraceable RFID Authentication Protocol

Dissertation
for the award of the degree
"Doctor rerum naturalium" (Dr.rer.nat.)
of the Georg-August-Universität Göttingen
within the doctoral Program in Computer Science (PCS)
of the Georg-August University School of Science
(GAUSS)

Submitted by
Sviatoslav Edelev
from Leningrad (Russia)

Göttingen
2015

Thesis Committee:

Prof. Dr. Dieter Hogrefe
Institute for Computer Science, Georg-August-University Göttingen

Prof. Dr. Xiaoming Fu
Institute for Computer Science, Georg-August-University Göttingen

Prof. Dr. Konrad Rieck
Institute for Computer Science, Georg-August-University Göttingen

Members of the Examination Board:

Prof. Dr. Dieter Hogrefe (First Reviewer)
Institute for Computer Science, Georg-August-University Göttingen

Prof. Dr. Xiaoming Fu (Second Reviewer)
Institute for Computer Science, Georg-August-University Göttingen

Prof. Dr. Konrad Rieck
Institute for Computer Science, Georg-August-University Göttingen

Prof. Dr. Florentin Wörgötter
Institute for Computer Science, Georg-August-University Göttingen

Prof. Dr. Carsten Damm
Institute for Computer Science, Georg-August-University Göttingen

Prof. Dr. Ramin Yahyapour
Institute for Computer Science, Georg-August-University Göttingen

Date of the oral examination: 4th September 2015

Towards a Lightweight, Secure, and Untraceable RFID Authentication Protocol

Abstract: This dissertation tackles the problem of user privacy and security of transactions in the authentication protocols of the technology of Radio-frequency identification (RFID).

Radio-frequency identification is ubiquitously used for automatic identification of objects over the distance. Numerous applications include access control using contactless ID cards, contactless payments in the public transportation, payments using contactless credit cards, toll payments, etc. To identify an item, RFID tags are used. In several other applications, mostly for automatic checkout and fraud control, tags are embedded into books, clothes, packs of medicines, goods. Such a widespread of the technology caused that almost everyone carry an item with an RFID tag inside.

However, many users do not realize that those small chips can reveal valuable privacy information about them or break the security of the information system. From the privacy side, RFID-enabled objects make their owners vulnerable to illegal tracing. This is mainly possible due to eavesdropping and unauthorized querying, which allows attackers to monitor transactions and link them to objects and places. The current state-of-art suggests considering an assumption that attackers can compromise a tag, read its internal state, and use information stored on the tag's memory to link the tag with its previous and future transactions. Moreover, an insecure channel allows attackers to learn, what object one is carrying, thus breaking anonymity. From the security side, RFID communications are vulnerable to replay and desynchronization attacks. In the former attack, an adversary targets to reuse the tag's response in order to impersonate it and illegally obtain the benefits. In the latter attack, the adversary targets to desynchronize identification records between a tag and a valid server so that a valid tag cannot be identified anymore.

Existing RFID authentication protocols demonstrate a lot of progress covering the above-mentioned issues. However, they still suffer from limitations and are vulnerable to certain security and privacy attacks. Moreover, due to their complexity, most of the schemes do not conform to the EPC Class-1 Gen-2 (C1G2) Standard and thus cannot be implemented on passive low-cost RFID tags.

In this dissertation, we aim to comply with the EPC C1G2 Standard and present a minimalist RFID Authentication protocol based on the Rabin scheme. Through the detailed security and privacy analysis, we show that the presented scheme overcomes the flaws of the previous works, provides anonymity, location privacy, achieves both backward and forward untraceability, and is secure against impersonation and desynchronization attacks. The proposed protocol also supports ownership transfer that can be performed over the insecure environment for tags. The performance comparison shows that our scheme outperforms the existing works in the amount of communication rounds, calculations on tags and on the server, and achieves the complexity for database loading of *O(1)* in the worst case. The use of lightweight functions makes the scheme efficient, scalable, and feasible for implementation on simple low-cost tags. To the best of our knowledge, this is the first lightweight protocol that provides forward and backward untraceability at the same time, and is robust against security and privacy attacks generally considered in RFID systems.

Keywords: RFID; authentication; privacy; forward-untraceability; backward-untraceability; ownership transfer.

Acknowledgments

First and foremost, I would like to sincerely thank my principal supervisor Prof. Dr. Dieter Hogrefe for the given opportunity to work in his group, for the support throughout my studies, his expertise, and valuable advice during especially challenging periods of research. Prof. Hogrefe has always provided opportunities for the development and participation in both internal and external activities, which has played a big role for me in becoming an independent researcher. Particularly noteworthy are his kindness and openness to our needs.

I express my gratitude to my Co-Supervisors Prof. Dr. Xiaoming Fu and Prof. Dr. Konrad Rieck for their guidance, insightful discussions, and valuable help during PhD Committee meetings and spontaneous occasions.

My gratitude goes to the further members of the examination board: Prof. Dr. Florentin Wörgötter, Prof. Dr. Carsten Damm, and Prof. Dr. Ramin Yahyapour. It is a great pleasure for me to have them in the committee.

I would like to acknowledge Dr. Lei Xie for hosting me in the Nanjing University, China, during the 2-months research visit. His high professionalism, active involvement, and sincere interest have caused a big step forward in my research. It was one of the most efficient periods of my studies and in general unforgettable experience of the Chinese culture.

I gratefully thank Dr. Somayeh Taheri for the exceptionally positive discussions about the topic of this research and her excellent contribution to this work. I owe her a lot for the progress this work has reached.

My deepest thanks go to current and former members of Telematics Group for their help, kindness, and support: Hang Zhang, Betty Mayeku, Dr. Parisa Memarmoshrefi, Dr. Ansgar Kellner, Salke Hartung, Dr. Maimun Rizal, Dr. Roman Seibel, Dr. Youssef El Hajj Shehadeh, and Dr. Saleh Al-Shadly.

I am very thankful to the administrative and technical staff: Carmen Scherbaum de Huamán, Annette Kadziora, and Udo Burghardt. They have helped in the every aspect of the everyday life, making all the things easier. They are the angels who carry everything on their shoulders and do the magic that makes things work.

In addition, I am grateful to the Education, Audiovisual and Culture Executive Agency of the European Commission for the provided Grant in the framework of the Erasmus Mundus Programme.

My deepest gratitude goes to my parents and grandparents who have raised me in love and care, given me excellent education, and fostered an attitude towards knowledge, development, and high-quality performance. They have given me everything they could in order to form, enrich, and realize my potential.

This work would never face its end without constant love, care, and inspiration from my wife Evgeniia. It is impossible to express how much she has done to support me. She is my everything.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Contents

1.1 Background

Radio-frequency identification (RFID) deals, as the name suggests, with identification of objects through the radio interface. Surprisingly, the technology was born and for the first time used long before the era of wireless networks and personal computers – it was initially applied during the World War II in the "Friend-or-Foe" identification systems to distantly recognize friendly military targets such as aircraft, vehicles, or forces.

The widespread of RFID starts from 1990s when the technology had been actively used in the supply management for tracking of goods and inventory purposes, in public transportation payment systems (e.g., in buses, metro, or ski-lifts), and for animal identification. In RFID, the role of identifier serves a transponder, called a tag, which contains a unique identification number of the object to which it is attached. The identifier (ID) of an item is transmitted wirelessly to the interrogator, or a reader.

The technology is also considered as an enhancement over optically recognizable barcodes. Indeed, in addition to the increased storage capacity and the ability to be reprogrammed (unlike barcodes), RFID tags do not need to be within the line-of-sight to perform identification. Thus, the technology enables automatic and wireless identification of objects without physical contact to them or manual intervention. Moreover, a small size of tags makes it possible to embed them into consumer items (such as shoes or clothes, watches, etc.), credit cards, and even implant them into humans and animals. Unlike barcodes that contain information about the manufacturer and type of a product, RFID tags often come with the Electronic Product Code (EPC), which contains additionally a globally unique identifier of the item.

Thanks to the features of automated and wireless identification and low cost of tags, RFID has faced ubiquitous use in the variety of applications: supply-chain management, access control systems, theft detection, wireless payments, intelligent transportation systems, tracking of humans and animals, electronic documents (e-passports).

All these examples have shifted the problem of identification towards the problems of sophisticated information systems that use identification as a primary operation. These systems operate with sensitive data and provide highly important services being constantly under increased attention of adversaries. Therefore, they have to be secure and reliable.

Since RFID was designed to provide fast identification of objects, the technology itself does not provide means to authenticate the parties of a communication – tags and readers. In particular, tags automatically reveal their identities to every reader that queries them. Moreover, the open broadcast nature of wireless communications allows eavesdroppers to intercept messages and, thus, break the confidentiality of communications. It opens the potential to serious security and privacy attacks that aim to obtain illegal access to resources, impersonate the object of identification, or collect private information about it, including the type of object, its location, and location patterns of its holder.

By placing malicious readers in various locations and hearing the same tag's ID at different places, an adversary can track users without their knowledge or consent. Moreover, from the knowledge of items that a person carries it is possible to obtain such personal information as one's interests, political attitude (from the books one buys, for example) or illnesses (from the medicines). Until protected, the information transmitted during RFID series of communication (transactions) remains easy-to-access. Thus, *the disclosure of the user location and data* from tags is considered as the main privacy problem in RFID.

In addition to user tracking through eavesdropping or unauthorized querying, strong attacker models assume that an adversary can compromise a tag and extract information from its memory in order to link it with previous or future transactions.

Protocols that are resistant to such privacy attacks are called backward-untraceable or forward-untraceable, respectively. Lim and Kwon proved [1] that forward-untraceability is possible to achieve only if an adversary misses at least one valid transaction between the target tag and a valid server after the compromise.

Another notion closely related to privacy in RFID is *ownership transfer*. In its life cycle, a tag may change its physical owners: for example, in the supply chains goods move between various business partners, are stored in the warehouse, appear on the supermarket shelf, and finally reach the end consumer. On each step, once the physical owner is changed, the old owner should have no means to access a previously owned item. In particular, an old owner should be able neither to access the content of the tag nor to trace it. Therefore, an RFID authentication protocol should provide a mechanism to transfer the ownership.

The following security issues are mainly considered in RFID: *impersonation* and *denial-of-service*. Impersonation is usually realized by performing *replay attacks*, the target for impersonation is a tag as a bearer of the secret identification information. Having impersonated a tag, an adversary will be able to illegally obtain the benefits of the victim tag. This is indeed a serious security problem as, in this case, an adversary gets access to the resources of the victim such as a bank account or entrance to the restricted areas. Thus, one of the fundamental properties of authentication is violated – *soundness* – meaning that an illegal entity will be authenticated.

The denial-of-service in regards to the authentication protocols in RFID is represented by *desynchronization attacks*. The goal of these attacks is to cause the mismatch of the identification records on tags and on the authentication server. Desynchronization attacks are possible to mount in those authentication protocols that update a tag's ID to preserve its privacy. An incorrect flow of the protocol caused by malicious attacker's actions or transmission errors can lead to desynchronization of identifiers between a tag and a server. This will lead to a situation when a valid tag will not be authenticated in the following transactions by a valid server. In this case, another fundamental property of authentication is violated – *completeness* – meaning that a legal entity will not be authenticated by a valid server.

Apart from security and privacy challenges, another restriction for the developers are technical capabilities of tags. Current research in RFID authentication is targeted towards low-cost EPC tags, which are embedded into consumer items. The low cost of tags brings with it severely restricted capabilities of tags. It is commonly considered that EPC tags supply only 2000 Gate Equivalents (GE[1]) for security purposes and 10000 GE for the overall gate budget [2]. Such tags are unable to compute hash functions or complex encryption/decryption operations. They support only simple arithmetical and logical operations and have a pseudo-random number generator (PRNG).

Security and privacy issues are one of the main reasons why RFID has not yet replaced barcodes on the shelves of supermarkets. Another reason is that every tag, no matter how cheap it is, requires additional costs in comparison with barcodes, which are produced by printing only. Moreover, privacy advocates have raised their concerns regarding RFID tags being embedded into clothes, banknotes, and other belongings and implanted into humans.

In order to foster the rapid development of consumer applications, a strong attention has been paid to security and privacy issues of RFID in the last decade. Scientists and research organizations are working towards a secure way of identification that would protect the privacy of users and be strong against illegal usage. However, as we will show later in the analysis of existing works (see Sect. 5 below), there is still no perfect solution: the proposed so far authentication protocols are subjected to security and privacy attacks.

1.2 Thesis Contribution

In this dissertation, we discuss in details privacy and security requirements for RFID authentication protocols and requirements imposed by technical capabilities of the technology such as storage, computational, and power resources. We identify flaws in the existing solutions and propose a secure RFID Authentication protocol with strong privacy protection. In particular, the contribution of this dissertation to the field of research is twofold:

1. We have developed an RFID Authentication Protocol that satisfies security and privacy requirements commonly considered in the field of RFID authentication. In particular, through an extensive formal analysis we have shown that the proposed protocol achieves the following properties: data anonymity, tag location privacy, backward-untraceability, forward-untraceability as well as protection against replay and desynchronization

[1] 1 GE is the silicon area of a one two-input logical Not-AND gate.

attacks. Moreover, the protocol uses only lightweight functions in its design: logical XOR, pseudo-random number generator, and modular squaring. Thus, the protocol is suitable for implementation on low-cost EPC tags. In addition, thanks to the Rabin cryptosystem used as a lightweight apparatus for encryption/decryption, the server requires only *O(1)* operations to find the tag ID. The conducted qualitative comparison shows that the proposed scheme outperforms in security and privacy protection as well as in efficiency and scalability.

2. Based on the proposed authentication scheme, we have also developed an ownership transfer protocol. The result of this protocol is that the ownership will be transferred from the old owner to the new owner. Once the ownership is transferred, an old owner is neither able to access nor trace that tag anymore.

The contribution of this dissertation has been published in the following international conference:

- S. Edelev, S. Taheri, and D. Hogrefe, "A Secure Minimalist RFID Authentication and an Ownership Transfer Protocol Compliant to EPC C1G2", in *Proceedings of the 6th IEEE Conference on RFID Technology and Applications (RFID-TA 2015)*, Tokyo, Japan, September 2015.

1.3 Thesis Organization

This dissertation is organized as follows:

Chapter 2 provides fundamentals of the RFID technology. In particular, it describes the main components of RFID – tags and readers, their main physical characteristics, a communication model, and standards used in different applications of RFID. This chapter concludes with the summary of the practical benefits of RFID as an identification technology in contrast to barcodes.

Chapter 3 gives a detailed overview of privacy and security issues in RFID. We first list the basic security services of information systems. We then identify the original flaws of the technology that give an opportunity for the attacker to perform malicious actions. Finally, we investigate the security and privacy threats of RFID and their influence on business processes and end-users.

Chapter 4 is dedicated to the requirements for RFID Authentication protocols. In this chapter, we describe in details an attacker model, define security and privacy requirements as well as feasibility requirements for EPC C1G2 tags. In the attacker model, we specify the particular capabilities of an attacker, the queries it can issue, the attacks it can perform as well as the difference between a strong and a weak attacker.

Chapter 5 gives a detailed overview of the related works. In particular, we have investigated four existing authentication protocols that attempted to achieve security and privacy in RFID using lightweight functions only. For every protocol, we give a description of the authentication scheme, list security and privacy properties claimed by authors, show vulnerabilities, and analyze the performance of the protocols in terms of functions used, amount of computations, and storage requirements.

Chapter 6 describes the proposed authentication protocol in details. We first formulate main principles that we use in the design of this protocol. Formulated principles are the result of the analysis of the existing works and they can be reused in the design of other RFID authentication protocols. In particular, we formulate our conclusions about how to achieve protection against various security and privacy attacks, what influences the protocol complexity, and how to protect against desynchronization. Second, we describe the core idea and a general approach followed by the lightweight mathematical apparatus used to perform encryption and decryption. Third, we explain the specific steps of the proposed protocol. Forth, we augment the proposed authentication protocol with the ownership transfer phase. Afterwards, we provide a detailed formal security & privacy analysis. The chapter ends with the performance analysis and comparison of the proposed protocol with the existing works in terms of the security and privacy provided as well as in terms of computational complexity.

Chapter 2

Components of RFID

Contents

2.1 RFID System

RFID systems consist of two essential and two optional components:

1. Tags, or transponders, which store identifiers of the objects.
2. Readers, or transceivers, which query tags, receive, and read data from them.
3. Databases that associate identification data from tags with business-related information.
4. Actuators, or external mechanisms, that are managed by the RFID system and implement the result of the communication session between tags and readers.

The first two components form a core of every RFID system. Tags are attached to the objects of identification and contain an identification number of the object. They transmit the identifiers to readers upon a query through radio

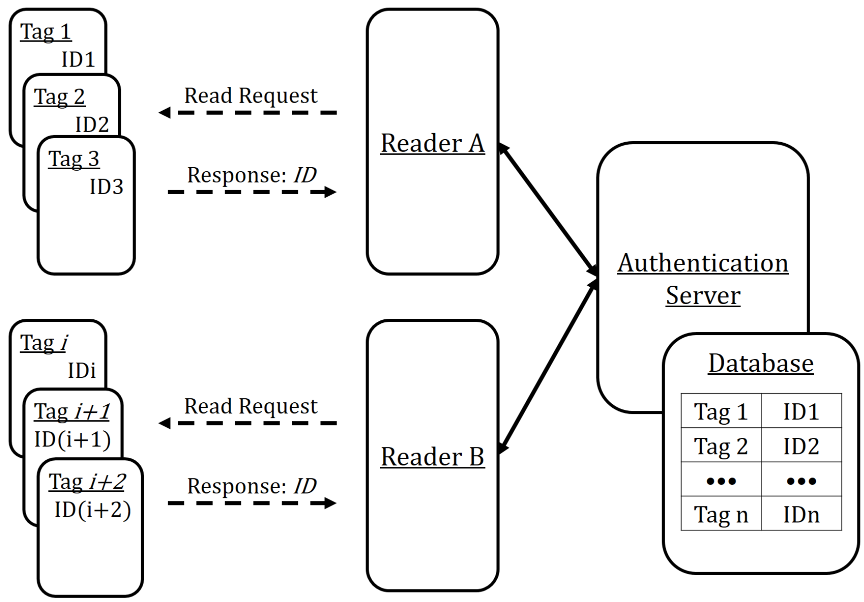


Figure 2.1: Components of the RFID system and their interactions.

waves. Depending on the setting, readers may work in an offline mode, meaning that they do not have a connection to the database, and in the online mode, when there exists a connection to the database. A connection between readers and a database is considered to be secure (e.g., based on the TLS/SSL protocol).

In the offline mode, readers authenticate tags using either the database from its local memory or based on the particular features of tags' IDs. In the online mode, readers are connected to the authentication server with the database of valid identifiers and serve as "hops" only, meaning that information processing and the decision regarding authentication of the tag takes place on the server side. The result of authentication is later transmitted to the reader, and a separate signal is sent that indicates the corresponding action, for example, the item is found in the database, the door opens, the credit card transaction happens, etc. The scheme of an RFID system is shown on Fig. 2.1.

Weis in his paper [3] describes physical principles and details of RFID components. This section summarizes this article as well as other sources: [4, 5, 6, 7].

2.2 Tags

RFID tags are small electronic devices composed of a microchip connected to an integrated antenna. The microchip provides storage and in some cases computational capabilities. Antenna provides communicating capabilities with the reader. Depending on the power source, tags can be passive, semi-passive, or active. Passive tags use energy emitted from the reader to generate a response, while active tags are supplied with an internal battery and periodically broadcast messages containing their IDs. Semi-passive, or battery-assisted, tags are also provided with a small battery on-board but they respond only upon a request from the reader, similar to passive tags.

The power source is a primary property of a tag, since it determines a tag's potential reading range, lifetime, cost, functionalities, and therefore applications where tags can be used. The power source also causes what form-factor a tag may have.

Active tags are the only type of tags that can initiate communication with the reader. Indeed, active tags constantly beacon their IDs. More advanced active tags can even communicate with other active tags, thus forming ad-hoc networks. This can be used, for example, to detect an integrity of shipping containers: if items within one container are supplied with active RFID tags and one of the items is suddenly missing, the other surrounding tags could be aware of it, log this action, and indicate it with an alarm signal. Since active tags have their own power resource, they operate over longer distances (more than 100m) and have better computational capabilities than passive tags; however, their lifetime is limited by the time of the battery, which drains rapidly due to constant beaconing. Active tags are used for cattle localization over large distances, live tracking of high-value assets (e.g. medical and electronic equipment, shipment containers), and others. Active tags are reasonably bigger in size and more expensive than other types of tags.

Semi-passive tags also contain a power source on-board, but they are not able to initiate communication with the reader or other tags. Instead, they generate a response when interrogated by the reader only. In contrast to active tags, it allows to save power and, thus, to provide a longer lifetime. The presence of an internal battery, from the one side, allows semi-passive tags to operate on the distances comparative with that of active tags and provide good computational and storage characteristics. From the other side, it makes semi-passive tags more expensive and bigger in form than passive tags. Since semi-passive tags contain an own power source, they are often used in connection with the sensing functionality. In this case, a sensor is incorporated into the tag's unit or is directly attached to it with the wire. The sensor takes energy from the tag's battery and when queried by the reader the sensor value together with the tag's ID are sent in response. Semi-passive tags are also often used in road tollbooth applications. In this case, the tag is located on the inner side of the car window and works in the slip mode. Once the car is approaching the tollbooth, the tag is activated and it transmits information needed for payment (for example, an account number of the driver).

Passive tags are the cheapest and the most common type of RFID tags. They do not contain any power source; instead, to generate a response they harvest energy from the incoming electromagnetic signal from the reader. For this, the reader should be located in the relatively close proximity, which causes a short-range operating distance (typically 10 cm). Since passive tags are powered by the external source, they might be fairly considered just as a piece of long-term memory and, thus, in contrast to the other two types of tags, have almost unlimited lifetime. The lack of battery also allows flexibility in the design of tags, making it possible to apply convenient form-factors to passive tags for their better incorporation into items: from rice-grain-sized RFID chips implanted into pets to flat, thin, and flexible RFID labels integrated into packing material and paper. The functionalities of passive tags are limited to the storage of an ID-number and simple arithmetic operations. Low manufacturing costs of passive tags and small to no maintenance requirements caused their widespread in the variety of applications: wireless payments, electronic documents (e-passports), supply chain management, animal identification, access control systems, theft detection, and many others. Often passive tags are attached to low-cost consumer items or packaging material and are meant to be disposed with them.

The comparison of the main characteristics of different types of RFID tags is summarised in Table 2.1.

Apart from different types of power sources, RFID systems operate at different radio spectrum. The spectrum defines radio frequencies at which readers and tags communicate. The radio frequencies, in turn, define the operating distance, power requirements, performance in terms of signal strength and tolerance to obstacles of different nature, the physical size of the tag, and finally the areas of applications. The following five classes of radio bands are used in RFID systems:

1. Low Frequency (LF): 30–300 kHz

Property \Tag Type	Passive	Semi-active	Active
Power source	Harvesting energy from the reader	Battery	Battery
Communication mode	Response only	Response only	Response or Initiate (Beaconing)
Relative computational and storage capacities	Simple	More advanced	Most advanced
Maximum operating range	10 meters	>100 meters	>100 meters
Relative lifetime	Unlimited	Less	Least
Relative costs	Cheapest	More expensive	Most expensive

Table 2.1: Main characteristics of different types of RFID tags.

2. Medium Frequency (MF): 300 kHz – 3 MHz
3. High Frequency (HF): 3–30 MHz
4. Ultra-High Frequency (UHF): 300 MHz – 3 GHz
5. Microwave: 2,45 GHz & 5,8 GHz
6. Ultra-Wide Band (UWB): 3–30 GHz

In general, the following consequences exist depending on the operating frequency:

1. The higher the frequency, the more energy is required for transmission.
2. With higher frequencies, the signal strength is higher, which makes the propagation distance longer.
3. Higher frequencies increase the data read rate.

Due to energy requirements, passive tags operate in low, high and ultra-high frequencies. The longest operating distance may be achieved working on UHF – up to 12 m, while the reading distance for HF tags is limited by 1 m, and for LF tags – by 20 cm [8]. Table 2.2 summarizes operating distances, bandwidths, and application areas by different wavebands.

However, low-frequency tags have better performance in terms of propagation in proximity to liquids, metal, or dirt. It makes them more appropriate for complex environments and, thus, they are typically used as implants for animal identification or as laundry tags. The short reading distance often serves as a

Waveband	Application	Bandwidth	Distance
Low Frequency (LF): 30–300 kHz	Animal Identification	< 10 kb/s	0,1–0,2 m
Medium Frequency (MF): 300 kHz – 3 MHz	Contactless Payments	< 50 kb/s	0,2–0,8 m
High Frequency (HF): 3–30 MHz	Access Control	< 100 kb/s	0,05–1 m
Ultra-High Frequency (UHF): 300 MHz – 3 GHz	Range Counting	< 200 kb/s	3–12 m
Ultra-Wide Band (UWB): 3–30 GHz	Vehicle Identification	< 200 kb/s	ca. 15 m

Table 2.2: Application, bandwidth, and operating distance by wavebands [9].

security advantage when tags are used in automobile immobilizers and access cards.

High-frequency tags operate on a narrow frequency band and thus may cause distortions working in sensitive environments with equipment operating on similar frequencies. This is a typical problem for medical settings. Since HF tags are often placed into a foil inlay or have a credit card form-factor, they are mainly used for access control, wireless payments, and asset-tracking applications, for example, for baggage handling or for books tracking in libraries.

Ultra-high-frequency tags are the cheapest to manufacture and have the longest reading range among passive tags. It makes them especially popular in item tracking and supply-chain management applications. However, this type of tags experiences interference in proximity with metals or liquids, which makes them infeasible for many applications such as animal tracking, metal container tracking, or access control systems.

Tags operating on microwave frequencies have a longer reading range and consume more energy than previously described types. That is why this type of tags is typically presented by semi-active and active tags. Unfortunately, the operating frequencies (2,45 GHz and 5,8 GHz) may cause conflicts between RFID tags and other wireless devices working on IEEE 802.11 (Wi-Fi) and 802.15 (ZigBee) standards.

Ultra-wide band tags do not propagate a signal on a particular frequency, they rather send low-power signals on a broad band of frequencies. It means that a

Class	Name	Memory	Power Source	Features
A	Electronic Article Surveillance (EAS)	None	Passive	Article Surveillance
B	Read-only EPC	Read-Only	Passive	Identification Only
C	EPC	Read/Write	Passive	Data Logging
D	Sensor Tags	Read/Write	Semi-Passive	Environmental Sensors
E	Motes	Read/Write	Active	Ad Hoc Networking

Table 2.3: Tag functionality classes.

signal on a particular frequency is very weak but an aggregated signal from the overall range of frequencies is strong and robust. This way of operation allows avoiding interference with the sensitive equipment and, as a consequence, finds its application in the medical environment. Moreover, UWB systems have the longest operating range – up to 200 m and more.

Weis in [3] classifies tags depending on their functionalities into five classes (see Table 2.3):

The first class of tags are Electronic Article Surveillance (EAS) tags. The do not contain a unique identification number but they simply announce their presence to the reader. EAS tags broadcast a single bit of information – 'Someone is here'.

EPC (Electronic Product Code) tags contain a unique identification number of the item. They are used mainly in supply chains and item tracking applications. EPC tags of class B have a single identifier that is set at the time of manufacture and cannot be later updated. On the contrary, EPC tags of class C have a re-writable memory, which allows tags to update their identification numbers or any other data they carry. EPC tags are typically passive. EPC Class C tags are the most common type of tags in particular due to their relatively low cost and sufficient computational and storage characteristics. Their abilities to update an identifier and to generate random numbers serve as a basis in many authentication protocols to provide security and privacy properties. *We particularly focus on this class of tags in this work.*

Class D is represented by Sensor Tags. Sensor Tags offer more than only identification functionality, they possess a sensor board capable of making environmental measurements, for example, light, temperature, sound, orientation, and other measurements. Sensor tags can log information about measurements and transmit it upon a query from the reader. This class of tags necessary contains an own power source, thus, these tags are either semi-passive or active.

Class E tags are also called Motes or Smart Dust because they are able to form ad-hoc networks and communicate with their peers. These tags are more complex than common EPC tags. Since they are able to initiate communication, they are presented by active tags.

2.3 Readers

RFID Readers are devices that establish a wireless connection with RFID tags, query, and identify them. They are the interaction points between tags and the overall system that collects and analyzes data gathered by readers. Identification procedure is defined by the authentication protocol used in a particular RFID environment: it can be a simple request-reply exchange or a multi-round protocol. Independently on the authentication protocol used, to receive tag's ID, the reader broadcasts a message and waits for a reply from the tag. In case several tags are located in the reader's vicinity, they all reply simultaneously on the same frequency and, thus, cause a collision in the communication.

In the environments where multiple tags can be present at the same time, RFID readers use special anti-collision protocols (for example, ALOHA [10] and Slotted-ALOHA [11], Binary-tree protocols [12, 13], overview of anti-collision protocols: [14]). With anti-collision protocols readers can simultaneously communicate with multiple tags and sequentially identify them.

Readers generate energy to power passive tags. Since passive tags have no battery, they use energy from the reader to generate a response. Depending on the protocol, tags can also delegate readers to perform computational and energy-costly operations.

RFID Readers may be stationary or mobile. Stationary readers are usually located at the gates of supermarkets or warehouses. Mobile readers are often produced in a form of a hand-held device or integrated into modern mobile phones.

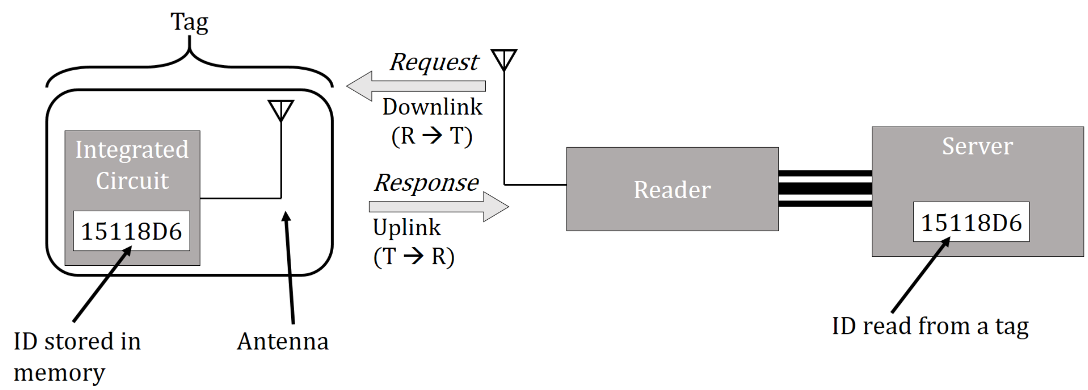


Figure 2.2: The communication process in RFID.

2.4 Communication Model and Security of Communications

The communication in RFID normally starts with the reader's request to read data from the tag. The communication link with the request from the reader to the tag is called a **forward channel**. The request is sent on the frequency and in the format defined by the standard used in the particular application (see Sect. 2.5 for details). Upon receiving the request from the reader, the tag sends its identification number (ID) in the format defined by the authentication protocol. The response from the tag back to the reader is sent over the **backward channel**. Upon receiving the reply from the tag, the reader processes it and extracts the tag's ID. The tag's ID is later checked in the database with the set of valid IDs, upon which a decision is made whether the tag is authorized. This communication process is represented on Fig. 2.2.

The normal operating range of RFID systems depend on various parameters: a type of tags, sensibility, and power of the reader, the presence of obstacles in the environment, the nature of the environment, used protocols and standards. Based on the review from Juels [15], we outline the following read ranges of passive RFID systems in the increasing order:

1. **Nominal read range** is specified by the product manufacturer or by the standard. This is the maximum distance at which a reader conforming to the standard can reliably read tag data. For example, for contactless

smart-cards, the respective standard ISO 14443 [16] specifies a nominal reading range of 10 cm.

2. **Rouge scanning rage** is the maximum range at which a powerful (rouge) reader can power and read a tag. This range exceeds the nominal read range because rouge readers can use much more powerful and sensitive antennas (or antenna arrays) and thus output power beyond the legal limits. Kfir and Wool [17] in their work have demonstrated that a battery-powered reading device can potentially scan ISO 14443 tags at a range of 50 cm, i.e., five times longer than the nominal range.
3. **Tag-to-reader eavesdropping range (backward channel)**: This is the range at which the passive rouge reader can eavesdrop the signal sent from the tag to the valid reader. Since the rouge reader applies its own power to the existing signal from the valid reader, it increases the reading range in comparison to the rouge scanning range.
4. **Reader-to-Tag eavesdropping range (forward channel)**: The signal from the reader to the tag is stronger than the signal back from the tag to the reader. Therefore, the rouge reader can eavesdrop this channel from rather far distances. The eavesdropper, who has access to the tag-to-reader channel, has also access to the reader-to-tag channel, which makes him/her able to get the full access to the communication between the tag and reader.
5. **Detection range**: This is the range at which the rouge reader can detect the presence of the tag or reader. Though the adversary cannot extract useful information from their communication, the adversary is able to locate an item. This information can be especially harmful in the military applications.

The model of communications in RFID between tags and readers can be represented using the Open Systems Interconnection (OSI) layer model [18]. The overall interactions in RFID are based on three layers: *Physical*, *Data Link*, and *Application* ([6, 19, 20]). Each level is a target for particular attacks. Below we list the levels of communications in RFID with the description of relative security issues.

1. **Physical Layer.** This layer consists of the RFID devices (tags and readers) and describes the physical air interface between them, in particular, transmission frequency, modulation, data encoding, and data rate. Since tags are resource-constrained devices due to their cost and size limitations, they are not able to provide a proper level of the physical security. In particular, they are vulnerable to tampering, compromise, cloning, and other physical attacks. One should assume that readers could be compromised as well,

because they are usually located in the environment with public access. This layer corresponds to Layer 1 of the model OSI.

2. **Data Link Layer.** This layer defines the communication interface between tags and readers in terms of data framing, collision avoidance, error detection and correction, point-to-point addressing, link control, and commands for the reading and writing of tags on the low level. The Data Link layer in RFID deals with the exchange of information in the wireless medium. Thus, due to the open and insecure nature of the radio links, they become a prominent target for attacks – the adversary can intercept communications, modify, or jam the signals. This layer corresponds to Layer 2 of the model OSI.
3. **Application Layer.** This layer specifies the organization and structure of data on tags and readers and describes the flow of the application-specific RFID authentication protocols. This layer specifies how the data are analysed and stored. In particular, the protocols on this layer provide authentication rules applied to tags and readers. Therefore, this layer is subjected to attacks applied to authentication protocols, such as impersonation, replay, and desynchronization attacks (these attacks are described in more details in Sect. 3.2). *This research concerns and is limited particularly by the Application Layer.* This layer corresponds to Layer 7 of the OSI model.

Layers Three to Six of the OSI Model are not required in RFID because all links in RFID are point-to-point (without intermediate switches). Therefore, there is no need for routing or complex transport functions described in Layers Three and Four of the OSI Model. Functions of establishing communication between tags and readers as well as functions of data representation (OSI Layers Four and Five) are implemented on the Data Link Level.

The communication model of RFID is depicted on Fig. 2.3.

2.5 Standardization

In order to insure that tags and readers from different vendors and countries are compatible with each other and do not interfere with other electronic objects, standardization is required. In the field of RFID standardization, the major players are the International Organization for Standardization (ISO) [21], International Electrotechnical Commission (IEC) [22], and EPCglobal [23].

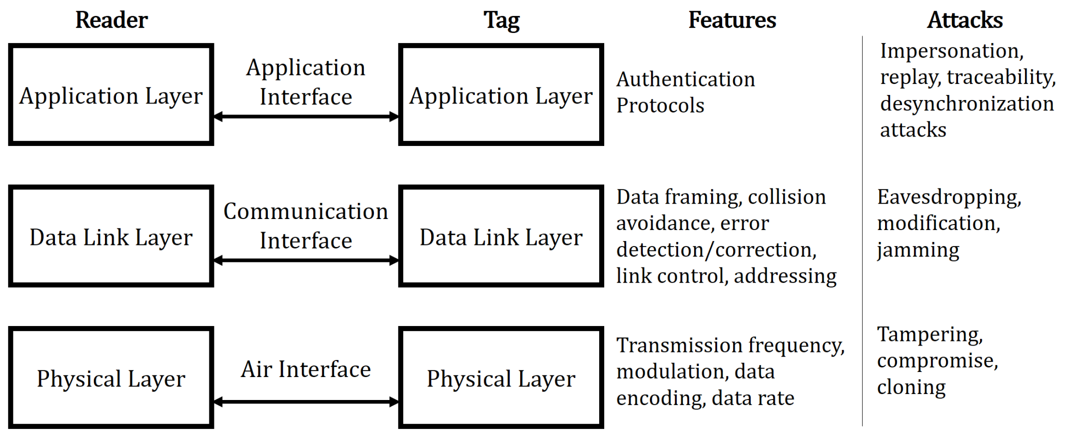


Figure 2.3: The communication model in RFID and attacks of each layer.

2.5.1 ISO Standards

To describe briefly, ISO/IEC mainly regulates physical aspects of the technology, including air interfaces, data protocols, and applications. Various ISO Standards related to the RFID field and their short descriptions are given in Table 2.4.

Item management in RFID is regulated by the ISO/IEC 18000 standard [24], with the following parts regarding different frequency ranges:

1. Part 1 – Reference architecture and definition of parameters to be standardized
2. Part 2 – Parameters for air interface communications below 135 kHz (low frequency)
3. Part 3 – Parameters for air interface communications at 13.56 MHz (high frequency)
4. Part 4 – Parameters for air interface communications at 2.45 GHz (microwave)
5. Part 5 – Parameters for air interface communications at 5.8 GHz (microwave), withdrawn
6. Part 6 – Parameters for air interface communications at 860–960 MHz (ultra-high frequency)
7. Part 7 – Parameters for active air interface communications at 433 MHz (ultra-high frequency)

More information can be found in [6] and in the respective standards.

Standard	Targeted Applications
ISO/IEC 11784, 11785, and 14223	Animal Identification
ISO/IEC 10536, 14443, 15693, and 10373	Contactless Smart Cards (credit cards, RFID-enabled passports, NFC-devices)
ISO/IEC 69873	Data Carriers for Tools and Clamping Devices
ISO/IEC 10374	Container Identification
ISO 18185	Electronic seals for tracking cargo containers

Table 2.4: ISO Standards for RFID and their description.

2.5.2 EPCglobal

The goal of the EPCglobal organisation [23] is to create a network between trading partners in order to exchange business-related information about consumer products, if possible, in real time. It allows authorized partners to track goods through supply chains and get access to previously registered data about products and their location. The EPCglobal defines standards and procedures regarding storage and processing capabilities of transponders and readers, data formats, procedures for discovery, exchange, and security of data. An overview of the EPCglobal network architecture can be found in [25].

EPCglobal also covers the question of the object name space. In particular, for the means of the identification, every transponder attached to goods possesses a *globally unique identification number* – an Electronic Product Code (EPC). Depending on the application, the format of the EPC is different and is defined by the header (the overview of different formats can be found in [26]). The total length of the identifier can be either 64 bits or 96 bits.

A typical format of the 96-bit EPC tags is depicted on Fig. 2.4. The leading 8 bit is a header that sets an EPC type and defines the length, structure, version, generation of the whole EPC record. The next 28 bit represent a so called “EPC Manager”. This field represents a Manufacturer ID or in general an entity responsible for the product. The first two fields are assigned by the EPCglobal. The following 24 bit form a field “Object Class”, which contains an ID of the Product Type, i.e., it identifies a class of objects. The last 36 bit are a Serial

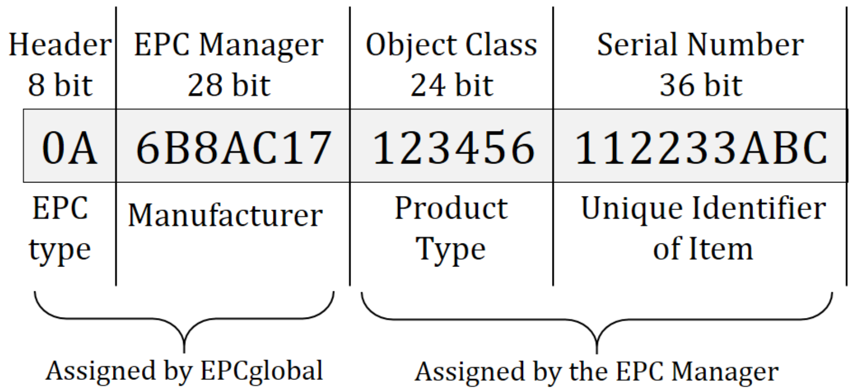


Figure 2.4: Format of the 96-bit EPC tag.

Number of the particular item – this number uniquely identifies an object. The last two fields are assigned by the EPC Manager, i.e. the Owner of the object.

Apart from the information about an object, the EPC serves also as a pointer to database records associated with this product. Database entries provide reach history of the object's life cycle, for example, time and location of the object in the supply chain as well as corresponding operation with the object (*transaction*). To perform a search of these data, EPCglobal has developed a public lookup system, called Object Name Service (ONS), similar to the Domain Name System (DNS) in the web-domain context. The goal of the ONS is to route queries containing tags' IDs to the corresponding database records [15].

EPC tags are small passive tags that can be manufactured in various form-factors depending on the object to which tags are attached and the type of application. With the goal to have a minimal price (generally considered no more than 5 US-cents [2]) and due to the efficiency of their operation, EPC tags are supposed to replace barcodes in the nearest future.

2.6 Benefits of RFID

Though RFID Systems are more costly in comparison to another popular identification technique – barcodes, which are produced by printing only, RFID has still major advantages and properties that barcodes do not provide [27]:

1. **Unique identification.** In contrast to barcodes, which identify a type of the product only (e.g., "a bar of chocolate, 100 g, brand XYZ"), an RFID tag emits a unique serial number that specifies a particular item among millions of identically manufactured objects (e.g. "a bar of chocolate, 100 g, brand XYZ, SERIAL NO. 123 456 789") [15].
2. **No line-of-sight required.** Since technology uses radio waves to transmit identification information about objects, it does not require direct visibility of an object. In particular, this property makes it possible to perform identification in difficult environments when tags are unexpectedly covered due to weather conditions (with ice, snow, or dirt) or are located inside a package/container.
3. **Simultaneous identification of multiple objects.** To prevent collisions in cases when multiple tags are present in the vicinity of a reader, RFID systems utilize singulation protocols (such as ALOHA and others, see Chap. 2.3 for references). The usage of these protocols makes it possible to perform fast and reliable identification of multiple tags at the same time. Together with the previous property, it automatizes the identification processes.
4. **Fast response time.** RFID tags respond typically in less than 100 milliseconds, which, in particular, makes them appropriate for identification of movable objects, for example, in the toll payments applications or finish detection on sport events.
5. **Bidirectional communication.** In case of RFID, tags and readers are indeed two communicating parties, where communication is pre-defined by the particular protocol. The protocol, in turn, allows protecting security and privacy of transactions. It is opposite to other optical recognition systems, where a particular identification mark (a barcode, QR-code, etc.) is a piece of information only without any processing power.
6. **Tags can be re-written and can store supplementary information.** On different stages of goods production, shipping, and supply, it is beneficial for the business purposes to add or modify information stored on tags. In addition, the ability of tags to update their IDs is the basic property for privacy protection. In Chap. 5, we will discuss how various protocols use this property and what level of privacy they achieve.

Due to the ability to recognize objects distantly without being on the line-of-sight, the field of supply management was influenced greatly by the use of radio-frequency identification and since long time has been considered as the major application area in RFID. As discussed in [28], the usage of RFID reduces expensive manual operations, increases speed and accuracy of operations, making the overall distribution process more reliable and cheaper.

Juels et al. in [29] and in [15] in particular point the following benefits of using RFID tags on the item-level in the retail field:

1. **Automatic checkout.** Given that all items in the store have an RFID tag attached, the checkout system could automatically identify all the items in the customer's basket and calculate the total price within seconds. Perhaps, the system could also automatically charge the customer by contacting his/her RFID-enabled credit card or another payment device with wireless connectivity.

2. **Receiptless item returns and post-purchase benefits.** Thanks to unique identification numbers of RFID tags, the particular item can be linked with the shop where it was bought and even with the buyer, if he/she had used a credit card (or other means of identification) at the moment of purchase. In case the customer wants to return the product or request the guarantee service, the seller will be able to check that this item was indeed bought from this shop by looking for a corresponding record of the purchase in the database. The customer is not required to present a receipt in this case because the item can be allocated to the shop using its unique identification number. Current use of barcodes does not allow it since barcodes represent a type of an item (for example, a bar of chocolate) but do not identify a particular item (e.g., a bar of chocolate ID: XYZ).

3. **Smart appliances.** Smart refrigerators could control an expiry date of food products with RFID tags and create a shopping list when something is over or, perhaps, make an order in the food delivery service. Washing machines could analyse RFID-tagged items of apparel to choose an appropriate washing mode. Microwave ovens could scan RFID tags on the packages of food items to use appropriate temperature and heating mode.

4. **Localisation of lost items.** RFID has been shown in the literature as a way to localise objects in the environment (for example, [30, 31]). This would allow people to localise lost items, which has a special meaning for people with memory disabilities. Moreover, the ability of objects to recognise their location in the environment plays an important role in the field of

context-aware ubiquitous computing, especially when other localisation technologies are not available.

5. **Recycling.** RFID tags embedded in the packaging material of goods could provide information regarding the type of material and, thus, permit fast and automatic sorting process for further recycling.

6. **Improved customer experience.** Modern smartphones support reading of RFID-labels, which opens perspectives for new applications and improved customer experience. For example, instead of reading small text from the packaging, people could read information about the product in a convenient for them way. Such "Shopping-advisor" App could also notify if the product contains any ingredients to which the customer is allergic.

Chapter 3

Security and Privacy in RFID

Contents

3.1 Authentication and Other Security Properties

Before explaining the security flaws and requirements for RFID authentication protocols, in this section, we give definitions for general security properties that information systems should normally provide [32].

3.1.1 Identification, Authentication, Authorization

Authentication is a security mechanism that provides a proof that the entity is indeed the one it claims to be. This process takes place after *identification* of the entity and is followed by the authorization. Identification of the entity is made when the entity gives its name or other identifier. During *authorization* (often called as *access control*), the system checks if the entity wishing to get access to the particular object has necessary access rights and privileges.

The overall process can be described on the following example. Alice wants to enter the office Z. She tells the guard Bob her name – by this name Bob can *identify* the coming person. Bob asks for the secret phrase that only Alice can know – if Alice gives the correct phrase, she is *authenticated* by Bob. Then Bob checks if Alice has privileges to access the office Z. If she has access rights, she is *authorized* to enter the office and Bob lets her in.

Authentication methods can be based on the following three factors [33]:

1. *Something you know* (Knowledge factor) – this is the most often used authentication factor. Examples include passwords, pin-codes, and answers to security questions (like "Where did you meet your partner?"). The knowledge of this secret information distinguishes one entity from another. Unfortunately, this factor has several limitations. First, due to human memory limitations, users tend to use simple passwords, apply the same password to different systems, or record the password somewhere. Each of this points lead to the increased vulnerability that the password becomes known for the attacker. Moreover, attackers can apply techniques of social engineering to get this secret information from the victim.

2. *Something you have* (Possession factor) – this authentication factor can be used to prevent the problem of forgetting secret information in the previous case. In this case, the authentication can be performed using a security token, physical key, proximity card, cryptographic calculator, and other authentication devices. However, once the authentication device is stolen, the adversary will get illegal access. This is especially dangerous when the same device (e.g., a smart-card) is used for access to different systems.

3. *Something you are* (Inherence factor) – this factor includes physical or behavioral characteristic of the entity, for example, fingerprints of retina, fingers, hands, voice, or a signature. An example of such property in RFID is a radio fingerprint of the tag. However, costs, accuracy, and reliability of these authentication factors are still being discussed.

To improve the security of authentication, information systems tend to use two- or multiple-way authentication. For example, it is becoming more common nowadays to use a pin-code sent by SMS in addition to the password to log-in or to perform a bank transaction.

3.1.2 Confidentiality

Confidentiality concerns the protection of data from being accessed by unauthorized entities. For example, in wireless communications, the typical attack against confidentiality is eavesdropping. It should also be noted that confidentiality deals not only with the content of communications but also with the fact that such communication takes place. In particular, the protective measures should be considered against traffic analysis, i.e., for the adversary it should be hard to determine the sender, the receiver, the length of the message, and other parameters. The typical measure to protect data from unauthorized disclosure is encryption. Encryption can be symmetric when the same key is used by two parties to encrypt and decrypt the messages and asymmetric when such keys are different.

3.1.3 Anonymity

Anonymity can be represented as a sub-set of the confidentiality. In particular, the communication can be considered as anonymous when it is not possible for the unauthorized party to define the sender and the receiver of the message. This can be achieved when, for example, the identifiers of the sender and the receiver are updated in the probabilistic manner. Anonymity and confidentiality form a base for privacy in communications.

3.1.4 Integrity

Integrity of communications guarantees that the message was transmitted from the sender to the intended receiver without modifications, duplications, reordering, or errors. This security property deals with active attacks such as man-in-the-middle, relay, and replay attacks as well as with accidental data transmission errors.

3.1.5 Availability

Availability refers to the ability of the system to provide resources and services required by the authorized party. This property relates in general to the ability of the system to resist attacks against its functionality. Attacks that cause the system breakdown are called denial-of-service attacks. Availability also relates to the fair distribution of the resources in wireless networks.

3.1.6 Non-repudiation

Non-repudiation is the property that provides a proof that the message was indeed sent or received by the particular entity. In the result, the sender (or the receiver) cannot claim that it did not send (or did not receive) the message. This property is especially important in e-commerce or other networks with sensitive information.

3.2 Flaws of RFID

The technology of radio-frequency identification was initially developed to provide fast and automatic identification of objects. In particular, the aim of RFID is to establish a mechanism of the communication between readers (transceivers) and tags (transponders). This mechanism allows readers to query tags and tags – to respond to the queries with the identification information.

Being fast and simple, the technology, however, possesses vulnerabilities making it an attractive goal for attackers. Indeed, several original qualities of the RFID technology bear an opportunity for an adversary to violate security and privacy in RFID-based communications:

1. Communication between tags and readers is performed through a **wireless channel.** Consequently, the open nature of radio communications allows attackers to eavesdrop communications.

2. Moreover, the RFID technology originally involves **no authentication** procedures between the communicating parties.

3. Next, due to the low computational capabilities of tags (given their low costs), the data transmitted during RFID communications are **unencrypted**.

4. Tags are **not tamper-proof** devices, which allows adversaries to corrupt tags. In the result, the adversary gets access to the internal information of the tag, including its ID and secret keys. Moreover, in a number of applications, it is possible to obtain the current state of a tag even without corrupting it, because there exists a third party with delegated access to the tag ID. For example, the initial tag ID is always known to an RFID integrator, or in the approach proposed for the RFID-enabled banknotes [34], a merchandiser can update the tag ID.

5. Lastly, tags respond with **unique** and **static** IDs.

Adversaries use above-mentioned traits of the RFID technology, which leads to serious security and privacy attacks. Specifically, the features of RFID give the following means for adversaries:

1. **Eavesdropping**. Eavesdropping in RFID communications is defined as surreptitiously listening and intercepting messages transferred between legitimate RFID entities [35]. An adversary can overhear the transmitted information between tags and readers, because information in RFID communications is transmitted through the wireless channel, which has an open and insecure broadcast nature. Though passive RFID tags normally have a short operating range, the signal broadcasted from the reader is strong enough to be monitored up to 1000 meters. Moreover, the adversary can use high-powerful antennas to monitor communications from a large distance. By eavesdropping, the adversaries are able to follow the execution of the protocol that may reveal the secret exchange or an update of the tag's ID. This information will help the adversary to launch further security and privacy attacks.

2. **Unauthorized tag reading**. An adversary can query tags and receive identifiers in response. This becomes possible, because originally the RFID technology does not involve any authentication procedures between the communicating parties. Thus, tags respond automatically to the requests of every, including malicious, reader.

Consequently, eavesdropping and unauthorized tag reading violate anonymity and confidentiality of RFID communications. In this sight, researchers (e.g., [15, 35, 36, 37, 38]) raise two major privacy problems in RFID: (1) leakage of information about user belongings and (2) tracking the user behaviour. We explain these concerns in more details. The former concerns *data/user privacy*, while the latter concerns *location privacy*.

3.2.1 Privacy Concerns

Leakage of information about user belongings (violation of data/user privacy). With the rapid deployment of RFID systems in various spheres of the everyday life, people are carrying more and more items that contain RFID tags inside. It can be quite personal items, the existence of which the person does not wish to disclose. The examples of such items include expensive products and accessories, books, or medicines. Once the adversaries are able to learn the content of the tag, they discover private information about the holder. For example, the brand of clothes or watches would indicate the material status of a person; the medicines indicate a particular disease; books reveal political and personal interests. Indeed, it is possible to associate an identification number from the EPC tag with a particular class of an object because EPC tags include a field "Object class" (see Sect. 2.5.2 for more details). Since the allocation rules are freely available from the EPC standard, this is an easy task. Even if allocation is done randomly, the adversary can establish a visual contact with the items in the shop, build a database of the identifiers and corresponding objects, and discover the patterns for allocation of IDs. This privacy concern is also often called *inventorying*.

Tracking the user behavior (violation of location privacy). As was discussed earlier, in contrast to barcodes, RFID tags emit unique identifiers of the objects. Therefore, when the adversary is located in the vicinity enough either to eavesdrop communications between tags and valid readers or to query tags on his/her own, he/she is able to obtain identifiers of tags. Even if the identifier does not possess any meaningful data regarding the object, to which it is attached, the static character of the tag's replies leads to illegal tracking of tags and, therefore, to tracking of people and objects that are carrying tags. More generally, if adversaries located at different places are able to recognize transactions belonging to the same tag, it violates the location privacy of the tag's owner. This concern is motivated by the fact that it is highly possible that people carry RFID-enabled objects with them on the regular basis. Example of such objects include RFID-enabled passports (e-passports [39]), contactless credit-cards, toll payment cards attached to car windshields, or even implanted RFID-tags.

Froward and backward tracing. Since RFID tags are not tamper-resistant devices, the current state-of-the-art assumes that attackers can compromise tags, extract information stored in the tag's memory, and use it to link the tag with its previous and future transactions. In particular, the strong adversary with the ability to compromise a tag is considered in privacy models by Avoine [40], Vaudenay [41], Juels and Weis [42], and others. Lim and Kwon [1] introduced the strongest privacy notion of untraceability in RFID, namely, *backward- and forward-untraceability*. These notions deal with the case when adversaries are able to compromise a tag during its life cycle, extract secret data from its memory, and return the tag to the normal operation. *Forward tracing* means that the adversary is able to recognize future transactions of the target tag. *Backward tracing* means that the adversary is able to recognize previous transactions of the target tag. These notions extend the tracking capabilities of the adversaries.

3.2.2 Security Concerns

Impersonation. The security of transactions is mainly vulnerable due to the ability to execute replay attacks, thus impersonating tags. Security issues are especially important in access control and payment applications. If the adversary is able to impersonate a valid tag, then he/she is able to obtain benefits provided by the valid tag, for example, access to the building or access to the payment account.

Violation of the integrity of communications. Integrity of communications is violated typically using man-in-the-middle attacks. In these attacks, the adversary acts as the intermediate party between the tag and the reader with the ability to modify and block the transferred information. The possible goals of this attack are to impersonate a valid reader or a valid tag, to make the tag traceable for the attacker, or to desynchronize the tags and the server in case the authentication protocol assumes update of the identifiers.

Desynchronization. The desynchronization attack concerns RFID authentication protocols that involve the update of the tag's identifier. The approach to update the tag's ID is used for privacy protection. However, in order to keep the correct execution of the further protocol runs, the ID should be updated properly on both the server and the tag. If the attacker prevents the correct execution of the protocol that causes the incorrect update of the identifier, the identification data on the server and on the tag are desynchronized. This makes the tag unidentifiable for the valid server, which does not allow a tag's holder to use his/her benefits (e.g. to pay in the shop). As another consequence, this attack can make the tag traceable for the attacker.

The complete overview of the attacks and defenses classified based on the communication levels and security principles are described by Mitrokotsa in [43]. The summary of the attacks on the application level and possible countermeasures are shown in Table 3.1.

3.2.3 Threats in Supply Chain Environments

Apart from the raw data about the object itself and its location, clandestine monitoring leads to various further consequences in the supply chain/retailer environments. Simson et al. [44] give an overview of such threats inside supply chains grouping them into corporate and personal threats.

3.2.3.1 Corporate Threats

1. **Corporate espionage threat.** Commercial privacy is subjected to violation due to clandestine monitoring of goods of the company by the competitor. For example, the competitor can locate powerful readers near the warehouse of the company and query the tags attached to the stored objects. Alternatively, the competitor can query objects being transported. This will reveal confidential business information about kinds and quantity of goods stored in warehouses and being transported.

2. **Competitive marketing threat.** Competitors are able to gather data about customer's preferences and use it in their marketing scenarios.

3. **Infrastructure threat.** RFID, being an infrastructural technology, strongly influences business processes. Therefore, due to any failure in the technology, caused either by unexpected events or by illegal competitor's actions, this will seriously affect the organizational actions.

4. **Trust perimeter threat.** Since business networks share data between each other, Simson et al. raise concerns regarding trust to such sharing mechanisms.

Attack name	Type of attack	Result of Attack	Possible countermeasures
Eavesdropping	Privacy	The content of communications is revealed (confidentiality is broken)	Encryption
Unauthorized tag reading	Privacy	Tag's identifier is revealed to adversary	Encryption, Reader authentication
Tracing (without tag compromise)	Privacy	The item's/user's location is being tracked	Randomize the tag's response
Forward/backward tracing (given the compromise of the tag)	Privacy	Adversary accesses the secret information stored in the tag's memory, which leads to extended tracking possibilities	Use one-way encryption functions, update tag's secret parameters after every transaction with authorized readers
Replay attacks	Security	A malicious entity impersonates an entity and gets its rights and privileges	Use nonces – one-time valid parameters (e.g., a random number or a timestamp)
Message blocking/ modification	Security	A valid tag is not authenticated; an invalid tag is authenticated; a tag is desynchronized from the server	Apply means to control the integrity of communications, e.g. digital signatures
Desynchronization	Security	A valid tag is not authenticated due to mismatch of the credentials on the tag and on the server	Prevent desynchronization by design or apply means to restore synchronization

Table 3.1: Possible security and privacy attacks on the application level and respective countermeasures.

3.2.3.2 Personal Threats

In addition to the inventorying and tracking threats described earlier, Simson et al. [44] express the following personal threats:

1. **Action threat.** Anti-theft detection systems may detect a sudden disappearance of tags attached to the expensive items. This could infer that a person is going to shoplift, which would activate the alarm. However, this can also happen if the person accidentally knocks the shelf with items.

2. **Transaction threat.** Not only can the location of the tag's owner be monitored but also transactions with other individuals. This is possible in particular due to the exchange of items.

3. **Breadcrumb threat**. Once the person purchases an item in the shop, an information system builds a link between the item and the person. However, when the person discards an item, this moment may not be monitored and, thus, the link in the system will still be kept. The threat arises when the item is used to commit a crime: in this case, the only identity associated with the item is an initial owner.

Chapter 4

Requirements for RFID Authentication Protocols – Problem Formulation

Contents

As any authentication protocol, RFID authentication protocols should satisfy the general requirements such as soundness and completeness. Soundness means that the protocol should authenticate valid entities, while completeness means that illegal entities should not be authenticated except with the negligible probability. In addition, RFID authentication protocols should satisfy specific security, privacy, and technical requirements described below.

4.1 Security and Privacy Requirements

RFID authentication protocols should achieve the following **security and privacy properties** [1, 38, 45]:

4.1.1 Privacy Properties

1. **Data privacy (tag anonymity):** The protocol should prevent the leakage of information that allows an adversary to recognize the real identifier of the tag. This makes an adversary unable to learn what object of identification is. If disclosed, the data about user's belongings can reveal sensitive information such as user's interests, social status, political attitude, and others.

2. **Tag location privacy:** The protocol should ensure that located at different places adversaries are not able to recognize transactions belonging to the same tag. Otherwise, this is the way to trace the tag and, therefore, its owner. Violation of the location privacy leads to the disclosure of the social activities of the private person and confidential business information. To achieve this as well as the previous property, there should be no computational link between tag's replies (the formal definitions are described below in Sect. 6.8)

3. **Backward- and forward-untraceability** [1]: The protocol should ensure that, if the tag was compromised and the information from its memory became known to the attacker, the attacker still cannot trace previous and future transactions of the tag. These notions deal with the case when the adversary corrupts the tag T_i and reveals its internal state at time t. *Backward-untraceability* means that the adversary cannot determine if a transaction at time $t'<t$ involves the tag T_i. *Forward-untraceability* means that the adversary cannot determine if a transaction at time $t'>t$ involves the tag T_i. Lim and Kwon [1] proved that *forward-untraceability* is achievable only if the adversary misses at least one successful transaction between the tag T_i and the valid server/reader at time t'' such that: $t<t''<t'$. To achieve this property, tag's previous and future replies should not depend on the currently stored on the tag data.

4. **Ownership transfer** [46]: Ownership is defined from the one side by the ability of the owner to interact with the tag, modify it, and transfer the ownership, and by the ability of the tag to be authenticated by its owner from the other side. In its life cycle, a tag may change its owners, for example, in supply chains when goods are moved between different parties or when one buys an object or receives it as a present. Thus, in secure protocols, an old owner must have no means of accessing the tag and tracing it after the ownership has been transferred.

4.1.2 Security Properties

1. **Replay attacks:** The protocol should assume that the communication channel between tags and readers is insecure and can be eavesdropped. Therefore, the protocol should ensure that the messages transmitted during the authentication protocol cannot be reused (=replayed) by the adversary to impersonate any of the communicating parties. To protect against replay attacks, protocol messages should contain the freshly generated nonce.

2. **Tag Impersonation attacks:** An adversary should not be able to generate the correct response of the tag without knowing the tag's internal secrets.

3. **Desynchronization attacks:** Desynchronization attacks can be launched against the protocols that update the tag ID after every transaction. Common ways to perform desynchronization attacks are: (1) to query the tag in order to cause an update of its ID so many times that it cannot be identified on the server side, (2) to block/modify messages in the protocol run (i.e., to cause an incorrect execution of the protocol), or (3) to impersonate the reader/server.

4.2 Technical Requirements for Low-cost EPC Tags

Apart from the above security and privacy requirements, in order to be applied to the real-world RFID systems, the protocols should satisfy the feasibility requirements. EPC Class-1 Genereation-2 (EPC C1G2) has become an industrial standard for low cost tags with limited storage and computational capabilities. It limits the use of cryptographic primitives to 16-bit cyclic redundancy checks (CRCs) and 16-bit pseudo random number generators (PRNGs) only [47]. More details about the EPC C1G2 standard and related implementation challenges can be found in Picazo-Sanchez et al. [48]. It is also commonly considered that simple tags have at most 2000 Gate Equivalents (GE) for security purposes [2]. This is certainly not enough for the classical implementations of the public-key cryptography (e.g., RSA) or hash functions (e.g., SHA-1, MD-5) on tags. In addition, the protocol construction should have only one round of the "request-reply" message exchange between tags and readers (i.e., one "request"-message from the reader and one "reply"-message from the tag).

To be precise, it is commonly considered that lightweight protocols should target low-cost tags in the range of 0,05-0,1 USD production price [2]. This cost limitation influences on the physical capabilities of tags in terms of computational power and storage. Consequently, the design of the lightweight authentication protocol has become a crucial subject among researcher in the last years. Armknecht et al. [49] gathered the set of technical conditions to be met.

1. **Timing**: The whole communication process should take no longer than 150 msec.

2. **Operating Frequency and Transmission Bandwidth**: The operating frequency depends on the application and varies from Low Frequency (LF), 30-300 kHz to Super-High Frequency (SHF), 3-30 GHz (see Table 2.2). The higher the waveband, the higher the bandwidth. The largest transmission bandwidth is limited to 200 kbit/s, while 100 kbit/s is the limit for one of the most popular applications – access control. Taking the limit for the duration of the authentication process, this implies that 30,000 bit is the maximum transmission size of the whole transaction.

3. **Chip Area**: Juels and Weis in [2] have determined the upper bound for the chip area as 2000 Gate Equivalents (GE) for security purposes and 10000 GE for the overall gate budget (where 1GE is the silicon area of a one two-input logical Not-AND gate). This number was later confirmed by Armknecht et al. [49] in the result of discussions with industrial experts. Existing works on designing the light-weight cryptographic functions (such as pseudo-random number generators, hash functions, symmetric cryptography) for low-cost RFID tags also target this limit (e.g. [50, 51, 52, 53]).

4. **Power**: Since passive RFID tags use the power emitted by the reader, it strongly limits the amount of power required for operations on tags. The maximum amount of power allowed to be generated by the reader is specified in the respective communication standard used in the particular application. For example, the EPC Gen 2 regulations define a power limit in 2W EIRP (Equivalent isotropically radiated power) in Germany and 4W EIRP in the USA [54]. The power consumed by the tag influences the maximum reading distance – the more power it requires, the less is the operating distance. In addition, Juels and Weis [2] define the general upper bound of 10 μW.

5. **Clock Speed and Clock Cycles**. The upper bound of the amount of clock cycles for computations on tags is defined by the time limit of the

transaction time and by the clock speed. The clock speed, in turn, is limited by the power consumption limits. The higher the clock speed, the more clock cycles can be performed within the same time interval. However, the more the clock speed, the more the power consumption. Therefore, researchers and industry experts consider 100 kHz as the prevalent clock speed feasible on constrained RFID tags. Assuming an upper bound of 150 msec for executing a full authentication instance, a clock speed of 100 kHz gives a limit of 15,000 clock cycles for tags to perform all the necessary computations during the authentication.

6. **Memory**: Juels and Weis [2] have stated that 128-512 bits are available for the read-only-storage and 32-128 bits are available for the volatile read-write memory on low-cost RFID tags.

4.3 Attacker Model

For the attacker model, we reuse the definition of the *powerful adversary* from the Vaudenay model [41]. In addition, the attacker is based on the Dolev-Yao intruder model [55]. We assume that the powerful adversary can:

1. monitor all communications between tags and readers,
2. store the eavesdropped transactions in an unlimited manner,
3. modify and block messages,
4. inject his own messages making them look like they were sent by the tag or reader,
5. query tags and readers,
6. corrupt tags,
7. and get side channel information about the result of the tag's authentication (i.e. observe the result of the authentication).

This adversary model also satisfies the formal models proposed by Avoine [40] and Juels and Weis [42].

The adversary who monitors communications is called an *eavesdropper*; the adversary who queries valid tags is called a *malicious reader*; the adversary who queries valid readers/servers is called a *malicious tag*. The adversary can use the collected information in order to trace tags. Malicious readers are considered more powerful than valid readers and, therefore, can operate over larger distances [56].

For the simplicity of further explanations, we follow the style of the formal definitions from [57, 58]. The adversary A is formally defined by the ability to issue the following queries:

Execute *(S, T, i)*: This query represents passive attacks, where an adversary A eavesdrops the honest session i between the tag T and the server S.
SendTag *(T, i, m)* $\rightarrow$ *m'*: This query sends a message m to the tag T in the protocol session i and receives the tag's response *m'*.
Modify *(m, i, m'):* With this query, A modifies the message m in the protocol session i to the message *m'*. If *m'* is Null, the message m is considered blocked by A.
Corrupt *(T)* $\rightarrow$ *Data*: With this query, A compromises the tag T and retrieves the data from T's internal memory (e.g., T's *ID*, a secret key, an internal state of PRNG). The query captures strong privacy notions of backward-untraceability or forward-untraceability depending on the time when this query is called.

Definition 1 (Attacks). *We define six type of attacks as follows:*

Anonymity attack: The adversary plays as a malicious reader and eavesdropper who attempts to discover the tag (tag's ID) that is communicating with the valid server or with the adversary. The adversary cannot corrupt the tag in this attack.
Location privacy attack: This attack captures the notion of the tag traceability. With this attack, the adversary attempts to link the particular responses in different sessions with the particular tag. The adversary cannot corrupt the tag in this attack.
Impersonation attack: The adversary plays as a malicious reader or as a malicious tag who attempts to successfully authenticate itself as a valid reader or as a valid tag, respectively. The adversary cannot use *corrupt* query in this attack.
Desynchronization attack: With this attack, the adversary attempts to make the tag unidentifiable for the valid server in the future transactions by mismatching the records of the tag's ID on the server's and on the tag's sides.
Backward attack: The adversary plays as a malicious reader and eavesdropper who attempts to trace the tag's previous communications.
Forward attack: The adversary plays as a malicious reader and eavesdropper who attempts to trace the tag's future communications.

The review of the related works showed us that not every work clearly says whether their attacker model assumes message blocking/modification by the active adversary, which makes it difficult to fully analyse the properties achieved by the protocol. We explicitly state that the attacker in our model can modify and block messages during the protocol session between the protocol parties.

Note: we do not consider server impersonation attacks because the tag does not authenticate the server in the proposed protocol.

Definition 2 (Strong and weak adversaries). *A strong adversary can access all the above queries and launch all the above attacks, while a weak adversary cannot access the* ***Corrupt*** *(T) query.*

Chapter 5

Overview of Related Works

Contents

To achieve privacy and security in RFID-based systems, numerous RFID authentication protocols have been recently proposed and analysed. Piramuthu [59]

Symbol	Description
T	Tag
S	Server
$\oplus$, XOR	Exclusive-Or operator
$\gg$	Right-bit shift operator
$\leftarrow$	Assignment operator
$\|$	Concatenation operator

Table 5.1: Used notations in the description of related works.

has made an extensive survey of the different approaches used to design RFID authentication protocols and identified privacy flaws and security vulnerabilities in all of the discussed schemes. We refer the reader to this work for more details. In addition to security and privacy vulnerabilities, most of the schemes use complex computations (e.g., hash functions, encryption and decryption functions) that do not conform to the EPC C1G2 standard and, therefore, cannot be implemented on low-cost tags.

In this section, we will describe several existing works that attempted to achieve security and privacy in RFID using lightweight functions only. In other words, we have considered the studies that aimed at not only achieving security and privacy properties in RFID authentication protocols but also at making the solution practical for implementation on simple passive low-cost RFID tags. We review each protocol, describe the claimed properties, and analyse vulnerabilities. Although numerous protocols have been developed for the lightweight authentication in RFID, we will review the following four works: Jin et al. [60], Le et al. [61], Lee et al. [62], and Doss et al. [63]. While describing the protocols we will highlight only those parameters and steps that are important for authentication. We use the notations from Table 5.1. The functions and parameters specific for each scheme are described in the respective section.

In the following sections, we first provide a description of the scheme including the properties claimed by the authors, after which we show its vulnerabilities, and finally we make a performance analysis in terms of functions used, amount of computations, and storage requirements.

5.1 Jin et al., 2011

5.1.1 Description

Jin et al. [60] proposed a lightweight RFID authentication protocol that uses a PRNG, XOR function, right-bit shift operator, and a lightweight encryption based on the SQUASH scheme [64]. The SQUASH scheme is an implementation of the Rabin scheme [65] for RFID tags based on the Quadratic residues property (see Sect. 6.5 for more details about the Rabin scheme).

In this protocol, every tag T_i is assigned an identifier t_i. The set of tags' identifiers is stored in the database on the server side. The server also stores the previously known ID of each tag s_i. Tags and the server share a big integer n, which is a product of two large primes.

The authentication scheme works on the following algorithm (Fig. 5.1):

1. The tag generates a random number r_T and calculates the following expressions:
   $M = t_i\ XOR\ r_T$
   $N' = {r_T}^2\ mod\ n$
   $N = [N']_t$, where t is a length of the substring N' assigned to N.
2. The tag transmits M and N to the server
3. The server makes an exhaustive search and looks for such t_i that
   $[N']_t = N$, where
   $N' = (M\ XOR\ t_i)^2\ mod\ n$
4. The server updates the new and the old tag's identifiers:
   $s_i' = t_i$
   $t_i = (s_i')^2\ mod\ n$
   $s_i = t_i$
5. The server calculates
   $r_T = M\ XOR\ t_i$,
   $P = s_i\ XOR\ (r_T \gg l/2)$, where l is the length of t_i,
   and sends r_T and P.
6. The tag calculates s_i (its previous ID) from received P:
   $s_i = P\ XOR\ (r_T \gg l/2)$
   and checks
   if $t_i = {s_i}^2\ mod\ n$ then
   $t_i \leftarrow {t_i}^2\ mod\ n$.

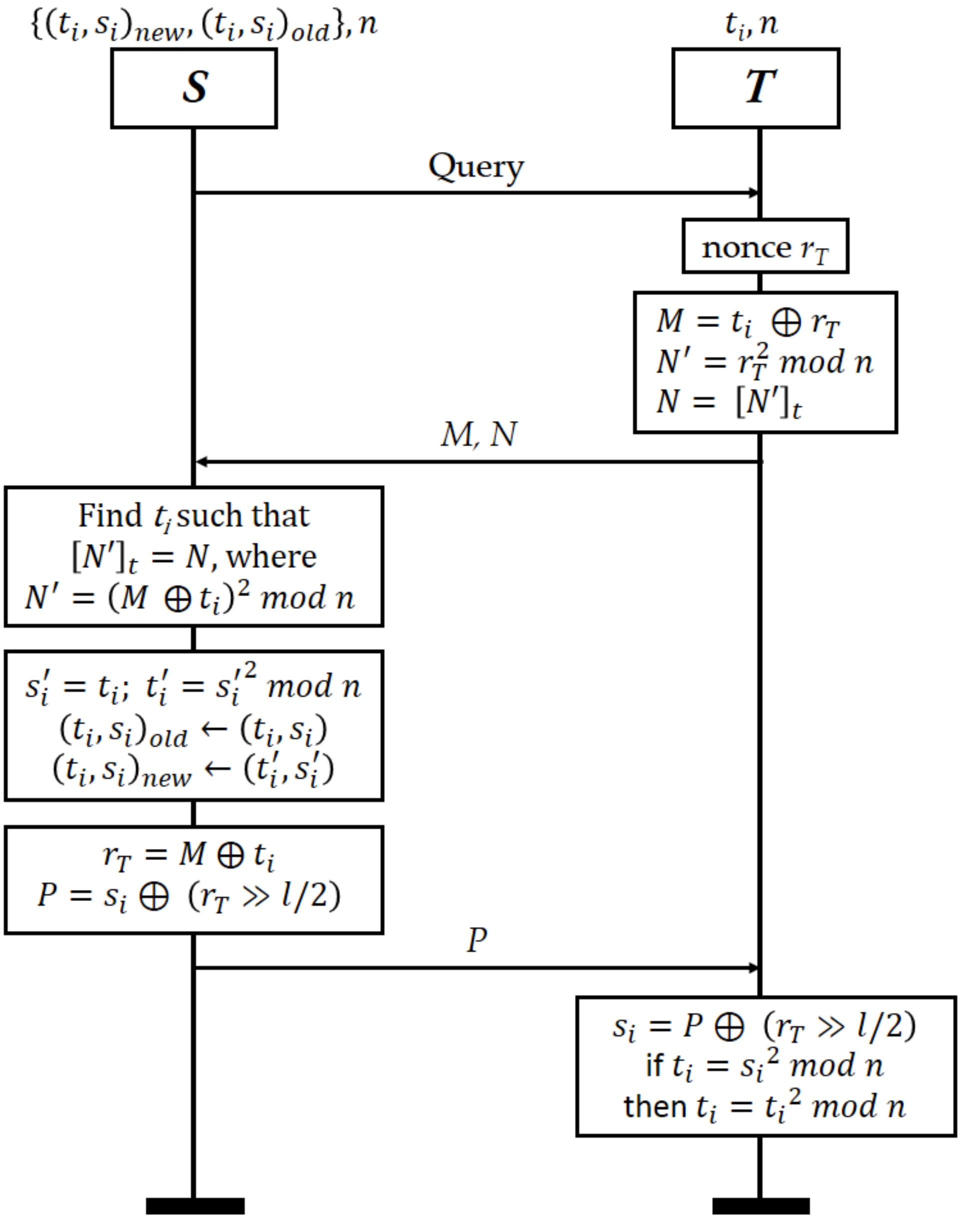


Figure 5.1: The protocol by Jin et al. [60].

To protect against desynchronization, the authors propose to store the old (unupdated) identifiers of tags on the server and check them as well during the authentication phase.

5.1.2 Claimed Properties

Jin et al. have claimed that their scheme satisfies the following properties:

1. Resistance against Replay Attacks,
2. Resistance against Desynchronization Attacks,
3. Resistance against Man in the Middle Attacks,
4. Backward-untraceability,
5. Forward-untraceability.

5.1.3 Vulnerability Analysis

Vulnerability to Replay attacks

The design of the protocol assumes that the identification message of the tag is based on the following values:

- Tag's ID t_i;
- a random number generated by the tag r_T;
- a shared parameter n.

The authors' statement about the protection against replay attacks is based on the assumption that the tag's ID will be updated at the end of the transactions, which means that it will not be valid anymore. However, in the situations when the message from the tag is not transmitted (due to transmission errors or malicious behaviour of the attacker), the identification message can be reused. The reason for this flaw is that the tag's reply does not contain the randomness generated by the server. The replayed message will be identified as valid by the server because the server also stores old (unupdated) identifiers of tags and checks them as well during the authentication phase. This is in particular a result of the protection against desynchronization attacks.

Vulnerability to Desynchronization

As can be seen from the protocol design, on the last step, the tag authenticates the reader. Only if the reader is authenticated, the tag updates its ID. However, Sohrabi-Bonab et al. [66] showed a Server Impersonation Attack on this protocol that causes authentication of the malicious attacker as a server. As a result, the tag will consider the attacker's response as correct and will update its ID. This, in turn, will cause desynchronization between the tag and the valid server.

Vulnerability to Traceability attacks

Moreover, it was shown in Sohrabi-Bonab et al. [66] that the tags become traceable when the session is not complete (i.e., when the message from the valid server is not received by the tag). In particular, they have shown that in case of two incomplete sessions the following expression will be hold:

$M_{i+1} \oplus \left(P_{i+1} \gg \frac{l}{2}\right) = M_i \oplus \left(P_i \gg \frac{l}{2}\right)$, where index i shows the session number.

Forward-traceable

The Tag's ID is updated by the modular squaring of the current ID:

$t_i \leftarrow {t_i}^2 \ mod \ n$

It allows the attacker to restore the current ID of the tag on the x-th transaction after the tag had been compromised even if the attacker missed one transaction in the meanwhile.

In other words, let us denote t_0 as the tag's ID stored in its memory. t_0 is known to the attacker at the moment when the tag was compromised. The attacker puts the tag back to the normal operation and misses one transaction, where t_0 is updated to t_1.

The attacker eavesdrops the second transaction, where the tag sends $M = t_1 \ XOR \ r_T$, and $N = {r_T}^2 \ mod \ n$, where t_1 was derived as $t_1 = {t_0}^2 \ mod \ n$.

The attacker computes:

$t_1 = {t_0}^2 \ mod \ n$

$N' = (M \ XOR \ t_i)^2 \ mod \ n$

If $[N']_t = N$, the attacker concludes that the observed transaction occurs with the previously compromised tag. Consequently, the protocol is forward-traceable.

5.1.4 Performance Analysis

Tag side

The following computational functions are called on the tag side:

1. PRNG – 1 call
2. XOR – 2 calls
3. Modular squaring – 3 calls

4. Right bit-shift – 1 call

Storage requirements:

1. Non-volatile memory: $2L$ bit, where L is the maximum size of integer n (in bits).
2. Volatile memory: $5L$ bit.

Server side

The following computational functions are called on the server side:

1. XOR – 2 calls
2. Modular squaring – 2 calls
3. Right bit-shift – 1 call

Storage requirements:

1. Non-volatile memory: $4L \cdot N + L$, where N is the number of tags in the system.
2. Volatile memory: $7L$

Database look-up complexity in the worst case: *O(N)*. The protocol consists of three communication flows.

5.2 Le et al., 2007

Le et al. [61] proposed two lightweight protocols O-FRAP and O-FRAKE that use a pseudo-random function only for computations on tags and readers. O-FRAKE is an extension of O-FRAP and both of them possess the same security properties. That is why for the simplicity, we will describe O-FRAP in the following section. The discussion given is also valid for O-FRAKE.

5.2.1 Description

In the O-FRAP (Optimistic Forward-secure RFID Authentication Protocol), the tags and the server share a key-pair $\{r_i,\ K_i\}$. This pair uniquely identifies a tag in the system. The protocol executes in the following way (Fig. 5.2):

1. The server generates a random number r and sends it to the tag.
2. The tag calculates:
   $v1 \parallel v2 \parallel v3 \parallel v4 \parallel v5 = F(K_i, r \parallel r_i)$, where $\parallel$ is a concatenation operator,

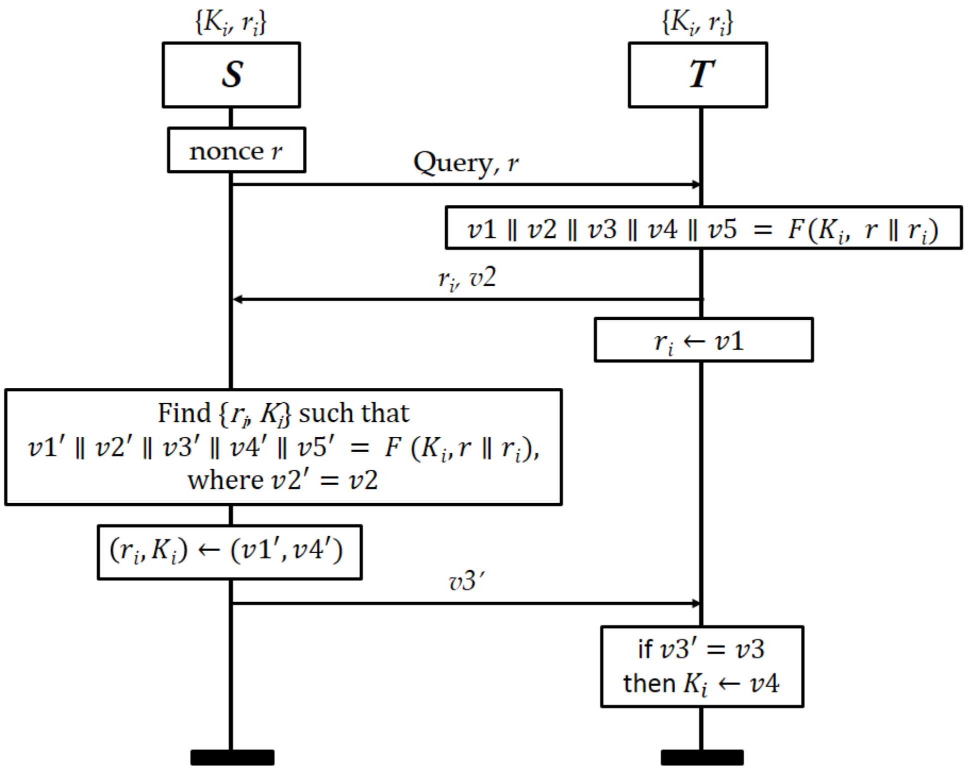


Figure 5.2: O-FRAP protocol by Le et al. [61].

F() is a pseudo-random function.

3. The tag sends r_i and *v2* to the server and updates r_i:
   $r_i \leftarrow v1$
4. The server makes an exhaustive search in the database and for every pair $\{r_i,\ K_i\}$, it calculates:
   $v1' \parallel v2' \parallel v3' \parallel v4' \parallel v5' = F(K_i, r \parallel r_i)$
5. The server checks: If *v2'=v2*, then the tag is identified and authenticated.
6. The server updates r_i and K_i:
   $(r_i,\ K_i) \leftarrow (v1',\ v4')$
   and sends *v3'* to the tag.
7. The tag checks: if *v3'=v3* then it updates:
   $K_i \leftarrow v4$

5.2.2 Claimed Properties

Le et al. in the analysis of the proposed protocols [61] have claimed the following properties:

1. Anonymity,
2. Authenticity,
3. Backward untraceability.

5.2.3 Vulnerability Analysis

The protocols by Le et al. [61] indeed provide anonymity because the information associated with the tag ID $(r_i,\ K_i)$ is never transmitted in the clear text. In addition, since r_i is updated in the random manner after every query, the messages r_i and *v2* transmitted from the tag to the server have no computational link with the messages transmitted in previous and future transactions until the secret K_i is known. However, the protocol is vulnerable to desynchronization attacks and is backward-traceable.

Vulnerable to Desynchronization attacks

Unfortunately, the protocol by design is vulnerable to simple desynchronization attacks. If a malicious reader queries the tag, the tag updates the value r_i. This value is used to identify the tag to the valid reader. The unauthorised queries by attackers cause the update of r_i on the tag's side, while this value will not be updated on the server side. As the result, the tag will not be authenticated by the valid server during the next transaction. This attack is shown in details by Ouafi and Phan [67].

Backward-traceable

To demonstrate that the protocol is backward-traceable, we present the following attack:

Learning: The adversary queries the tag T_i by sending an arbitrary random number r and stops the execution of the protocol once the tag's response is received. Thus, the adversary receives $\widetilde{r}_i$ and $\widetilde{v2}$. The adversary queries other tags as well.
Challenge: The adversary is given a tag T_0. Adversary compromises T_0 and extracts a secret K_0. The adversary calculates:
$v1 \parallel v2 \parallel v3 \parallel v4 \parallel v5 = F(K_0,\ r \parallel \widetilde{r}_i)$.

Guess: If $v2 = \widetilde{v2}$, the adversary concludes that the compromised tag T_0 is the eavesdropped tag T_i. Therefore, the protocol is backward-traceable.

Forward-untraceable

Interestingly, this protocol is forward-untraceable because the tag will update its secrets r_i, K_i when the adversary misses at least one transaction after the tag was compromised. The nature of such an update is random and depends on the random number sent by the valid server in the request message. Therefore, for the adversary it is not possible to restore the current secrets of the tag when one transaction is missed. Based on these assumptions, the protocol is forward-untraceable.

5.2.4 Performance Analysis

Tag side

The following computational functions are called on the tag side:

1. PRNG – 1 call

Storage requirements:

1. Non-volatile memory: $2L$ bit, where L is the maximum size of a tag's key (in bits).
2. Volatile memory: $6L$ bit.

Server side

The following computational functions are called on the server side:

1. PRNG – 1 call

Storage requirements:

1. Non-volatile memory: $2L \cdot N$, where N is the number of tags in the system.
2. Volatile memory: $7L$

Database look-up complexity in the worst case: *O(N)*. The protocol consists of three communication flows.

5.3 Lee et al., 2009

Lee et al. [62] presented an Ultralightweight RFID Protocol with Mutual Authentication that uses the following lightweight functions: XOR, AND, OR, and bit rotation Rot (A, B)[1]. The random number generator is used by the server only. Similar to the previously described protocols, this protocol consists of two phases: authentication and key updating.

5.3.1 Description

Every tag T_i shares its dynamic temporary identifier IDT_i and a secret key K_i with the server S. The protocol executes in the following way (Fig. 5.3):

1. The server sends a request to the tag.
2. The tag immediately replies with its identifier IDT_i.
3. Based on the IDT_i received, the server finds a corresponding K_i in the database.
4. The server generates a random number N_i and calculates the following:
   $A = K_i \bigoplus N_i$
   $\overline{K_i} = Rot(K_i,\ K_i)$
   $\overline{N_i} = Rot(N_i,\ N_i)$
   $B = \overline{K_i} \bigoplus \overline{N_i}$
5. The server transmits A and B to the tag.
6. The tag derives N_i from A: $N_i = A \bigoplus K_i$
7. The tag calculates $\overline{K_i}$, $\overline{N_i}$, and B in the same way and compares the calculated value B with the received B from the server. On this step, the tag authenticates the sever:
   $\overline{K_i} = Rot(K_i,\ K_i)$
   $\overline{N_i} = Rot(N_i,\ N_i)$
   $B = \overline{K_i} \bigoplus \overline{N_i}$
   Verify B.
8. The tag calculates C as:
   $C = \left(K_i \vee \overline{N_i}\right) \bigoplus \left(\overline{K_i} \wedge N_i\right)$
   and transmits C to the server.
9. The tag updates IDT_i and K_i:

[1] $Rot(A,\, B)$ denotes to left rotate the value of A with n bits, where n is the number of “1” in B

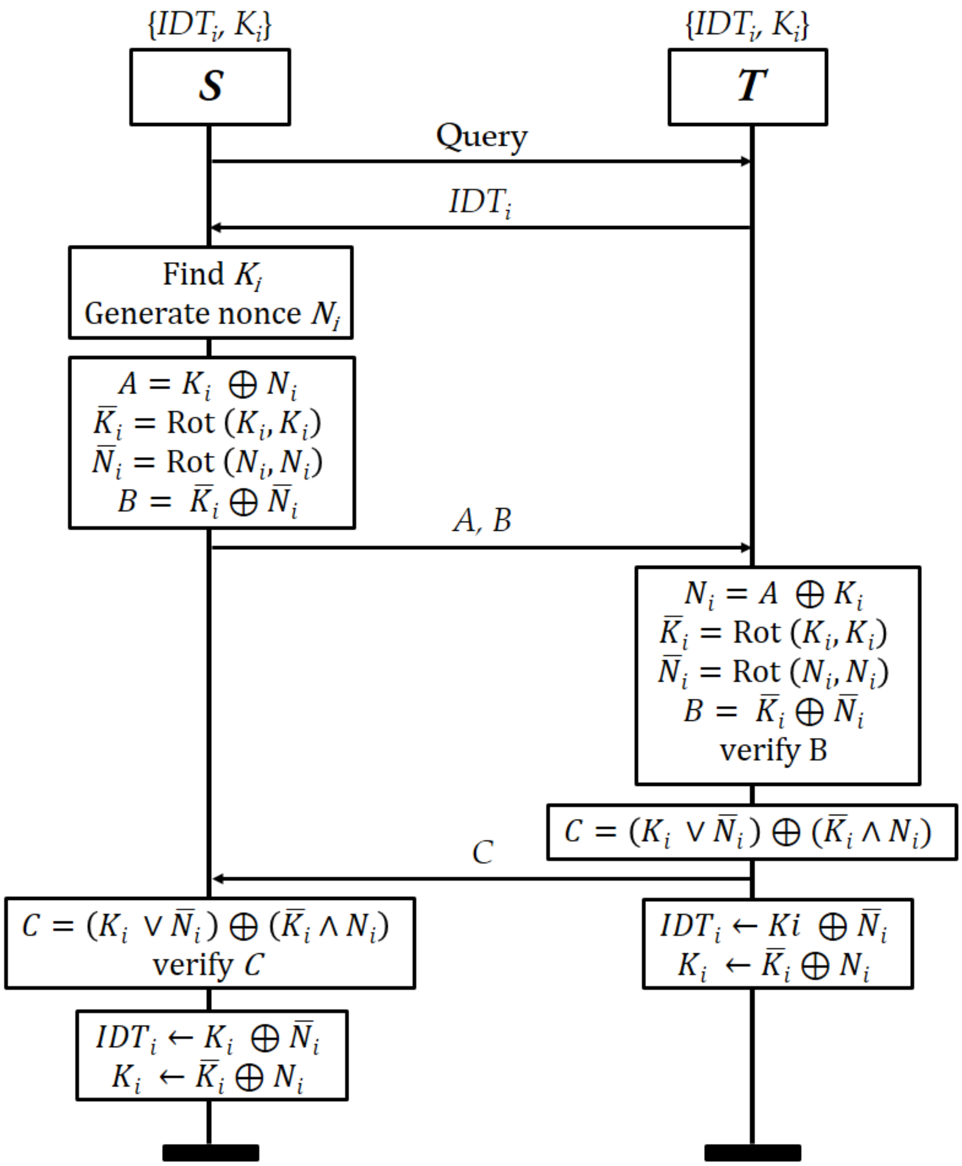


Figure 5.3: The protocol by Lee et al. [62].

$IDT_i \leftarrow K_i \bigoplus \overline{N_i}$
$K_i \leftarrow \overline{K_i} \bigoplus N_i$

10. The server calculates C in the same way and compares it with the received C:
$C = \left(K_i \vee \overline{N_i}\right) \bigoplus \left(\overline{K_i} \wedge N_i\right)$
Verify C.
On this step, the server authenticates the tag.
11. Once the tag is authenticated, the server updates IDT_i and K_i in the database (in the same fashion as on step 9).
$IDT_i \leftarrow K_i \bigoplus \overline{N_i}$
$K_i \leftarrow \overline{K_i} \bigoplus N_i$

5.3.2 Claimed Properties

Lee at al. in the analysis of the proposed protocol have claimed the following security and privacy properties:

1. Anonymity,
2. Resistance against Impersonation attacks,
3. Resistance against Replay attacks,
4. Resistance against Desynchronization attacks,
5. Backward-untraceability.

5.3.3 Vulnerability Analysis

Vulnerability to Replay and (Backward-)Traceability attacks

The main drawback of this protocol is that the tag replies with a static response if the previous transaction occurred unsuccessfully, i.e., if during the last transaction a tag could not authenticate a server. This is the case when (1) the tag was queried by a malicious reader or (2) when the messages from the server to the tag (A and B) were transmitted with errors (transmission errors or due to the malicious actions of the adversary). This makes the protocol vulnerable to replay and traceability (including Backward-traceability) attacks.

Vulnerability to Desynchronization attacks and loss of anonymity

Furthermore, the blocking of the last message from the valid tag to the server desynchronizes the tag's ID between the tag and the server. In addition to these attacks, Peris-Lopez et al. [68] conducted a detailed analysis of this scheme and found out that the protocol does not provide anonymity. They have shown how the protocol design makes it possible for the adversary to disclose the secret key K_i of the tag by eavesdropping several transactions.

Forward-untraceable

As shown by Lim and Kwon [1], when analysing forward-untraceability attacks, one should assume that at least one complete and valid transaction happens between the tag and the valid server after the tag had been compromised. In the case of the protocol by Lee et al., the tag's secrets are updated using the random number generated by the server. As per our analysis, for the adversary it is impossible to link the compromised parameters IDT_i and K_i with the messages A, B, and C eavesdropped after at least one complete unheard transaction. Therefore, the protocol by Lee et al. is forward untraceable.

Consequently, in contrast to the claimed statements by the authors, the proposed protocol is vulnerable to Impersonation, Desynchronization, Replay attacks, is traceable, and is not anonymous.

5.3.4 Performance Analysis

Tag side

The following computational functions are called on the tag side:

1. XOR – 5 calls
2. Bit rotation – 2 calls
3. 1 AND, 1 OR

Storage requirements:

1. Non-volatile memory: $2L$ bit, where L is the maximum size of a tag's key (in bits).
2. Volatile memory: $7L$ bit.

Server side

The following computational functions are called on the server side:

1. PRNG – 1 call
2. XOR – 5 calls
3. Bit rotation – 2 calls
4. 1 AND, 1 OR

Storage requirements:

1. Non-volatile memory: $2L \cdot N$, where N is the number of tags in the system.
2. Volatile memory: $8L$

Database look-up complexity in the worst case: *O(1)*. The protocol consists of four communication flows.

5.4 Doss et al., 2012

Doss et al. in [63] proposed "A minimum disclosure approach to authentication and privacy in RFID systems" (MDA protocol for short). The protocol aims to be suitable for low-cost EPC tags with the small computational power. For this purpose, the MDA protocol uses PRNG, XOR, and Quadratic residues as cryptographic primitives to provide mutual authentication.

5.4.1 Description

This protocol uses a minimal disclosure property to authenticate the tag. This approach is similar to the "zero-knowledge authentication" paradigm, where the prover proves that it knows a secret but the secret itself is not revealed to the verifier. We describe the minimal disclosure property below based on the description from [63].

5.4.1.1 Minimal Disclosure Property

Let n be a product of two large prime numbers g and q. We assume that A has a secret V represented by a sequence of numbers $\{v_1, v_2, v_3, \dots, v_m\}$,where $1 \leq v_j < n$. A wants to convince the verifier B that it has a secret V. For that, A shares with B a sequence of integers $\{s_1, s_2, s_3, \dots, s_m\}$, where $s_j \equiv v_j^{-2}\ mod\ n$, $1 \leq s_j < n$. A generates a random number r and computes $x \equiv r^2\ mod\ n$ and $y \equiv r \prod_{j \in S} v_j (mod\ n)$, $0 \leq y < n$, where S is a subset of the set $\{1, 2, \dots, m\}$. With the knowledge of x and y, B can verify that $x \equiv y^2 z\ mod\ n$, where $z \equiv \prod_{j \in S} s_j\ (mod\ n)$, $0 \leq z < n$. This congruence holds because: $y^2 z \equiv r^2 \prod_{j \in S} v_j^2 \prod_{j \in S} s_j \equiv r^2\ (mod\ n)$ [69].

5.4.1.2 Protocol Description

The MDA protocol has two phases: initialization and authentication (see Fig. 5.4).

Initialization

In the initialization phase, the server generates two large primes p and q and computes $n = g * q$. Each tag is assigned an identification number *TID* and a secret $K_{TID} = v_1 \| v_2 \| v_3 \| \ldots \| v_m$. The server generates a random number r and computes the following values:

$s_j \equiv v_j^{-2}\ mod\ n$

$R_{TID} = h(TID) \bigoplus r$

$R_{TID}^{-1} = h\,(TID) \bigoplus r^{-1}$, where r^{-1} is the previous value of r (initially r=r^{-1}), *h()* is a hash-function.

Each tag is initialised with the following record:

$$\{TID, h(TID), K_{TID}, n, r\}.$$

For each tag in the system, the server stores a record with the following parameters:

$$\{R_{TID},\ R_{TID}^{-1},\ TID,\ h(TID),\ K_{TID},\ r,\ r^{-1}\}.$$

Authentication

1. The authentication phase starts with the query from the server to the tag supplied with a random number s.
2. The tag generates a random number r_t and calculates:
   $M = TID\ \bigoplus r_t \bigoplus s$
   $x = M^2\ mod\ n$
   $c = x \bigoplus h(TID) \parallel s \bigoplus r$
   $R_t = h\,(TID) \bigoplus v_p \bigoplus r,$
   where v_p is chosen at random from K_{TID},
   $y = (M \cdot v_p \cdot v_{p+1} \cdots v_{p+l})\ \ mod\ n$, where $l = m - p$.
3. The tag sends $c,\ y,\ R_t,\ p$ to the server.
4. Based on received R_t and p, the server searchers R_{TID} or R_{TID}^{-1} such that:
   $R_t \oplus v_p = R_{TID}\ or\ R_{TID}^{-1}$
5. Based on the found R_{TID}, the server retrieves corresponding *TID, h(TID),* $K_{TID},\ r$.
   Note: for the equation above, R_{TID}^{-1} is used in case the previous transaction

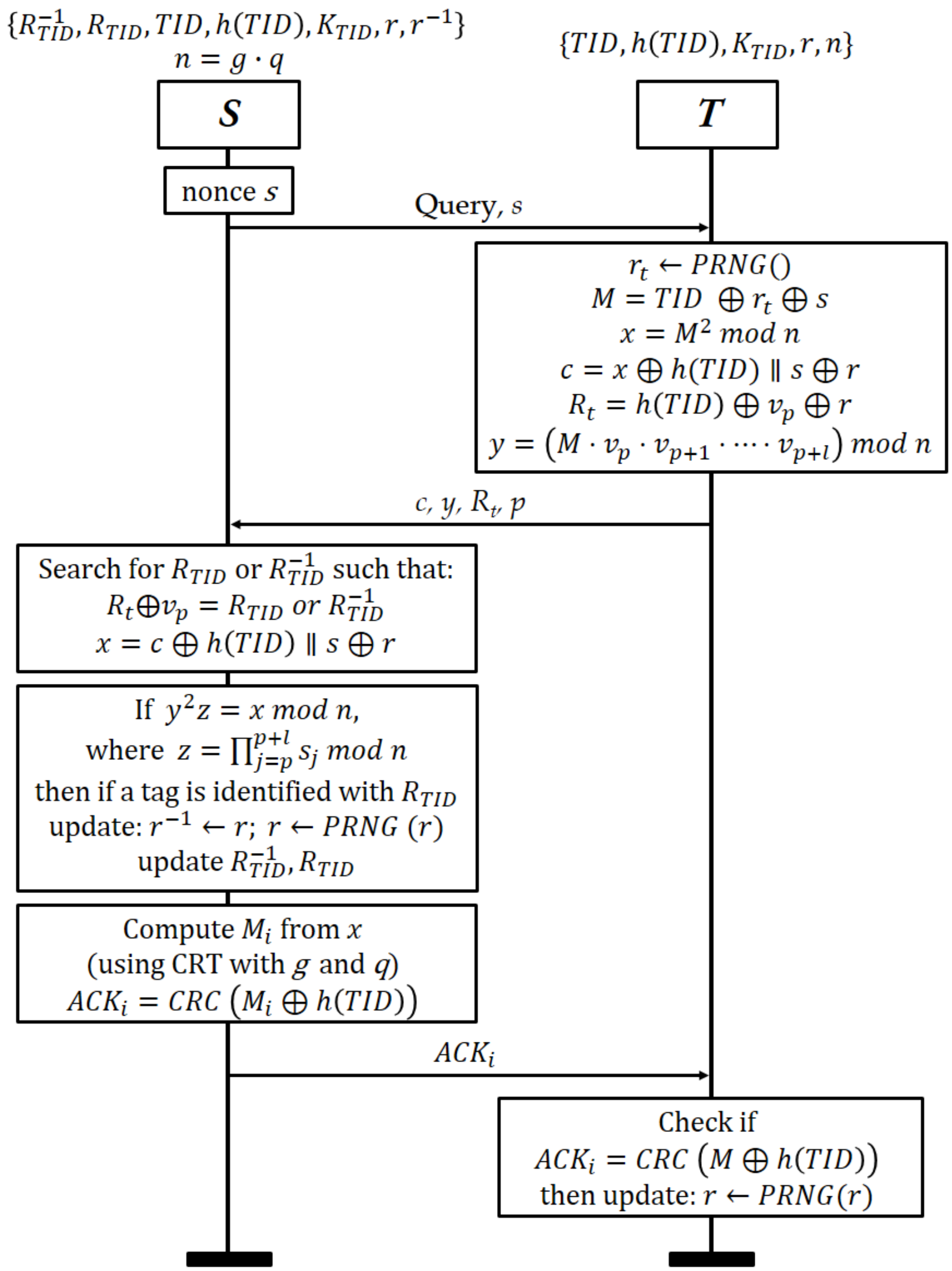


Figure 5.4: The MDA Protocol by Doss et al. [63].

had been incomplete and the tag had not updated r (see below). If $R_t \oplus v_p = R^{-1}_{TID}$, then r^{-1} is used in the calculations below instead of r.

6. The server calculates:
   $x = c \bigoplus h\,(TID) \parallel s \bigoplus r$
   and verifies: if $y^2 z = x \ mod\ n$, where $z = \prod_{j=p}^{p+l} s_j \ mod\ n$, then the tag is authenticated (otherwise, the protocol is aborted).
7. If $R_t \oplus v_p = R_{TID}$, the server updates:
   $r^{-1} \leftarrow r$
   $r \leftarrow PRNG\ (r)$
8. The server applies Chinese Reminder Theorem with the knowledge of p and q to find M as a Quadratic residue of x *modulo* n. There are four possible solutions M_i, $0<i\leq 4$. The server forwards each of these solutions in the response ACK_i:
   $ACK_i = CRC\ (M_i \bigoplus h\,(TID))$, where *CRC()* is a Cyclic Redundancy Check.
9. The tag checks if $ACK_i = CRC\ (M\ \bigoplus h\,(TID))$, then it updates r:
   $r \leftarrow PRNG(r)$

5.4.2 Claimed Properties

Doss et al. have analysed the proposed protocol and have claimed the following properties of their scheme:

1. Tag anonymity,
2. Tag location privacy,
3. Backward-untraceability,
4. Protection against Replay attacks,
5. Protection against Desynchronization attacks.

5.4.3 Vulnerability Analysis

Traceability attacks

Sohrabi-Bonab et al. [66] showed that traceability of the MDA protocol is possible based on two facts: (1) the parameter r remains unchanged when the transaction is incomplete (meaning that the tag does not receive ACK_i from the server or if ACK_i is not valid) and (2) the insignificant size of the tag's secret K_{TID} due to the memory limitations of EPC tags. Though the tag transmits only a random part of K_{TID} in R_t, it was proved in [66] that given *m=16* for the adversary it is sufficient to query the tag only 5 times in order to be able to link the tag with the previously recorded responses with the probability of 66% (i.e. 16% advantage over the random guess).

Backward-traceability

To demonstrate that the protocol is backward-traceable, we present the following attack:

Learning: The adversary queries the tag T_0 and receives in response c^0, y^0, ${R_t}^0$, p^0.
Challenge: The adversary is randomly given a tag T_b, where $b=\{0;\ 1\}$. The adversary compromises T_b and extracts *h(TID)*, K_{TID}, and r.
Guess: Based on ${R_t}^0$ and p^0, the adversary verifies:
if $R_t^0 = h\,(TID) \bigoplus v_{p^0} \bigoplus r$ then *b=0*, otherwise *b=1*.

Therefore, the MDA protocol is backward-traceable.

Forward-traceability

To show that the protocol is forward-traceable, we provide the following attack:

Learning: The adversary compromises the tag T_0 and extracts all information from its memory, in particular, $h(TID)^0$, ${K_{TID}}^0$, r^0, and a state of the PRNG.
Challenge: The adversary returns the tag T_0 to its normal operation and misses one transaction between T_0 and a valid server. Afterwards, the adversary queries a tag T_b or eavesdrops a transaction between T_b and a valid server. Consequently, the adversary gets messages ${R_t}^b$ and p^b.
Guess: The adversary calculates $r=PRNG\ (r^0)$ and verifies: if $h\,(TID)^0 \bigoplus v_{p^b} \bigoplus r = R_t^b$, then *b=0*, i.e., the eavesdropped transaction belongs to the previously compromised tag.

Therefore, the MDA protocol is forward-traceable.

5.4.4 Performance Analysis

Tag side

The following computational functions are called on the tag side:

1. PRNG – 2 calls
2. XOR – 7-10 calls

3. Cyclic redundancy check – 1-4 call(s)
4. Modular squaring – 1 call
5. Modular multiplication – (*l+1*) calls, where l – is a parameter in the protocol

Storage requirements:

1. Non-volatile memory: $(1L + 4M)$ bit, where L is the maximum size of a tag's *ID*, M is the maximum size of the integer n (in bits).
2. Volatile memory: $(3L + 5M)$ bit.

Server side

The following computational functions are called on the server side:

1. PRNG – 2 calls
2. XOR – 4-7 calls
3. Cyclic redundancy check – 1-4 call(s)
4. Modular squaring – 1 call
5. Modular multiplication – *(l+1)* calls
6. Solve quadratic residues – 1 call

Storage requirements:

1. Non-volatile memory: $(1L + 6M) \cdot N + 3M$, where N is the number of tags in the system.
2. Volatile memory: 7*M*+*L*

Database look-up complexity in the worst case: *O(N)*. The protocol consists of three to six communication flows.

Chapter 6

Proposed Lightweight Authentication Protocol

Contents

6.1 System Model

In this section, we describe the entities of the RFID system that take part in the authentication protocols in RFID. As shown earlier in Chap. 2, the RFID system is composed of Tags, Readers, and a Server:

Tag T_i: An RFID tag is a small device composed of a microchip connected to an integrated antenna. It stores a unique identifier (ID) of the object to which it is attached. Identification data of the tag are transmitted through radio waves to an RFID reader, hence the tag and the reader do not necessarily have to be on the line of sight. Tags have little storage and computational capabilities and are not temper-resistant. We consider passive EPC (Electronic Product Code) tags. The example specification regarding the EPC tags can be found in Sect. 4.2.

Reader $\boldsymbol{R}_i$: RFID readers are devices that serve as the interaction points between tags and an authentication server. They establish a wireless connection with RFID tags, query them, receive a reply, and transmit the reply to the server. A separate protocol is established between the readers and sever that authorizes readers to communicate with the authentication server. We assume that communication channels between tags and readers and between readers and the server are not secure and can be eavesdropped and manipulated.

Server $\boldsymbol{S}$: The server adds/removes tags to/from the system and manages a database with the identification information about the tags. It collects and analyzes data gathered by readers, and authenticates the tags depending on the authentication protocol used in a particular RFID environment.

Since Readers work as "hops" only, transmitting the information from tags to the server and back, we define that a protocol party is a $\mathrm{T}_i \in$ Tags or S $\in$ Server, where $0<i<n$, and n – is the number of tags in the system. The protocol parties interact in the polynomial-time protocol according to the algorithm below. Each party is a probabilistic interactive Turing machine with a sufficient internal storage.

The model of communications between these entities is described in Sect. 2.4.

6.2 Motivation & Overview

During the rigorous review of the existing RFID authentication protocols, we looked at the gist of each protocol to understand what exactly provides protection against particular attacks and why the protocols were later shown vulnerable to other security and privacy attacks. We have also noted that a majority of the protocols do not consider restricted storage and computational capabilities of tags as well as the scalability properties in terms of computational costs and the complexity for the database look-up. With this work, we aim to design a minimalist protocol that, from the one side, achieves the set of security and privacy requirements under the common attacker model and, from the other side, is efficient, scalable, and feasible for implementation on simple low-cost tags. We believe that complex protocols are incompatible with simple tags.

In particular, we have come to the following conclusions:

1. To resist replay attacks on the tag's response, the response should be a function of the reader's "request" message containing a freshly generated nonce.
2. To provide tag location privacy, the tag's response should contain a nonce generated by the tag.
3. To provide data privacy, the tag's *ID* should be transmitted in the encrypted form. The corresponding decryption function should be available to the valid server only.
4. Since the tag corruption is an assumed attacker's capability, the tag should not store any secret data shared with other entities in the RFID system. In particular, it means that symmetric-key cryptography should not be used as the tag corruption will reveal a key used by the server to decrypt messages. As a result, this will lead to the server impersonation attack.
5. To achieve forward- and backward-untraceability, the tag's response in each transaction should include some parameter that is not known to the attacker at the moment of the tag's corruption and that is not possible to calculate for the particular transaction in the past or future based on the data at the moment of corruption.
6. The use of hash functions for data encryption is not recommended as it increases the complexity of the database look-up at least to $O(N)$.
7. It is better to avoid desynchronization than to create means for re-synchronization. A possible solution is to use static IDs for tags.

6.3 Core Idea

As in any RFID authentication protocol, the main challenge is to transmit the tag's identifier so that only authorized readers can correctly understand it and hide it from eavesdroppers. Therefore, the transmitted information should be encrypted. As discussed above, in case of symmetric encryption, the compromise of the tag will reveal the secret key used. This will break the security of the whole RFID system as the attacker will be able to decrypt all the communications. The use of the one-way encryption (e.g., hash-functions) is not appreciated because it will make the server do the same encryption operation in order to validate the tag's response, thus increasing the complexity of the protocol in terms of computations, time, and scalability.

Therefore, we propose to use lightweight asymmetric cryptography with the easy-to-perform encryption operation for execution on the tag's side. The message sent from the tag to the server should encrypt the tag's *ID*, the nonce generated by the server, and the nonce generated by the tag. Once the server receives the message from the tag, it decrypts the message, removes the nonce, and finally extracts the tag's *ID*. As the result, the tag does not change its *ID* after every transaction, which avoids possible desynchronization. It is important to mention that for the server it is not necessarily to know the tag's nonce to check the validity of the message – the resistance against replay attacks is guaranteed by the nonce generated by the server. In other words, there is no need to transmit the tag's nonce in clear text to the server. The purpose of the tag's nonce is to provide protection against tracing. Since the nonce generated by the tag is not transmitted in clear text, there is no possibility for the attacker to reconstruct the valid tag's reply, even if the tag was compromised earlier. This nonce remains known to the tag only and only in the moment of the transaction.

The only way to generate a nonce for the tag is to use the built-in pseudo-random number generator (PRNG). Unfortunately, true random number generators still remain an expensive solution. In general, the generation of the pseudo-random number can be represented as:

$$Rand = PRNG\ \ (Seed),$$

where *PRNG()* is a deterministic function.

This means that for the known *Seed* the output of the PRNG will also be known if the attacker knows the construction of PRNG. Thus, it is of special importance because the current state of PRNG becomes known to the attacker once the tag is compromised. Consequently, this would allow the attacker to reconstruct the pseudo-random numbers generated by the tag in the following transactions after the compromise, thus, violating the location privacy (see *Forward-untraceability* property earlier in Sect. 3.2). This problem is described in details in Phan et al. [57].

As a solution, we propose to generate the *Seed* based on the previously generated pseudo-random number and the nonce from the server, i.e.,:

$$Seed = Rand\ XOR\ Nonce$$

$$Rand = PRNG\ (Seed),$$

where *Nonce* is generated by the server.

Based on the proof from Lim and Kwon [1] that forward-untraceability is possible to achieve only if the attacker misses at least one valid transaction with the valid sever after the time of the compromise, the proposed scheme of the PRNG provides forward-untraceability. Indeed, the loss of one valid transaction will not allow the attacker to reconstruct the current state of PRNG and thus will not allow tracing the tag.

This approach is described more detailed in the next section.

6.4 General Approach

The proposed above approach has two phases: initialization and authentication. Below is the description of each of them.

Initialization.

1. The Server generates a pair of Public and Private keys $\{Kpub,\ Kpriv\}$. Both keys are kept on the server.
2. The Server generates an identifier ID_i of the tag T_i as a new random number not used before. The length of the identifier is l. The server assigns ID_i to the tag T_i and transmits *Kpub* to the tag.

Authentication

1. The Server generates a random number *R1* with the length l and transmits it to the Tag.
2. The Tag computes a new seed and generates a random number *R2*:

$$Seed = R2\ XOR\ R1$$

$$R2 = PRNG\ \ (Seed)$$

3. The Tag computes the response M using the encryption function with the public key *Kpub* as follows:

$$M = Enc_{Kpub}((ID\ XOR\ R1)\ \|\ R2)$$

and sends M to the Server.

4. The Server decrypts M using the private key *Kpriv*:

$$P = Dec_{Kpriv}(M),$$

and removes l right bits, the result is P_{left}.

5. The Server computes:

$$ID' = P_{left}\ XOR\ R1$$

and looks for *ID'* in its database. Once *ID'* is found and is legal, the server authorizes the tag.

6.5 Mathematical Apparatus for Low-cost PKC

The approach described above is general and lacks details about the implementation of the asymmetric encryption/decryption. Since there have been common doubts about the feasibility of public-key cryptography (PKC) on RFID tags [70, 71, 72], it is essential to provide a possible realization of the proposed approach suitable for low-computational RFID tags.

In our approach, the only complex on-tag computation is encryption. The decryption operation is performed on the powerful server side. Therefore, we were looking for the implementation of the public-key cryptography where encryption is easy to perform. Thus, we propose to use the Rabin cryptosystem, which has been shown to be as secure as the integer factorization problem [73].

In the Rabin scheme, p and q are two large distinct primes that serve as the private key; $z = p * q$ serves as the public key. Let A be a plaintext, then a ciphertext c is produced by squaring A modulo z:

$c = A^2\ mod\ z$

In order to decrypt c, i.e., to find A given c and z, knowledge of p and q is required. Due to the difficulty of factoring z, it is computationally infeasible to find x, satisfying $x^2 = R\ mod\ n$, without knowing p and q. However, the decryption phase using the Chinese Remainder Theorem [74] gives four candidates *A'*, satisfying $c = (A')^2\ mod\ z$. Therefore, an indicator must exist in order for the decryptor to choose the correct value A. Without a loss of generality, if A is replaced with A^2, the ciphertext is produced as:

$c = (A^2)^2\ mod\ z,\ where\ A^2 < z.$

Among the decrypted values, there is only one solution that is a prefect square [69]. The square root of this value is the original plaintext A. This approach was shown in [75]. A detailed description of the Rabin scheme can be found in [65].

From the efficiency point of view, encryption requires only two *"square modulo z"* operations, which is suitable for computation on tags. A practical realization of the Rabin scheme suitable for low-resource tags (also known as the WIPR scheme) was shown in [76, 77] with the total area of 4,184 GE, including RAM, which fits into the overall gate budget of 10,000 GE for passive RFID tags. The efficient implementation is achieved by replacing a memory-expensive modular reduction step by an addition of a large random multiple of z, i.e.

$c = A^2 + r * z$,

where r is at least 80 bits larger than z.

It is important to mention that a possible alternative low-cost implementation of the public key cryptography could be the Elliptic Curve Cryptography (ECC). However, as evaluated by Wenger et al. [78], the complete implementation of the ECC on the microcontrollers requires between 16,786 and 32,034 GE including RAM, which is beyond the limit of the EPC tags.

The resulting implementation of the proposed RFID authentication protocol using the Rabin scheme is shown in the next section.

6.6 Proposed Protocol

In this section, we provide the formal definition of the proposed protocol. We use the notations from Table 6.1. The protocol has three polynomial time algorithms: server key generation (*SetupServer*), tag ID generation (*SetupTag*), and tag authentication (*Auth*). The algorithm is depicted on Fig. 6.1.

- *SetupServer(τ) $\rightarrow$ (Kpriv, Kpub, N)*: The server generates a name space (N) for tag identifiers and a private/public key pair (*Kpriv, Kpub*) for the server depending on a security parameter τ. The private key (*Kpriv*) consists of a pair of two large prime numbers p and q and is stored on the server side. The public key (*Kpub*) is equal to z=p*q and is distributed among every tag T_i belonging to the system.

- *SetupTag(N, i) $\rightarrow$ (ID_i)*: The server picks a unique tag identifier ID_i from

Notation	Description
T, T_i	Tag
R, R_i	Reader
S	Server
$Kpub = z = p * q$	Public key
$Kpriv = \{p, q\}$	Private key
ID_i	Identifier of Tag i
$r1, r2$	Random numbers
l	Bit-length of *ID*, *r1*, *r2*
T_R	The set of tags in the system
N	Namespace for the tags in the system
$\bigoplus$, XOR	Exclusive OR
$\leftarrow$	Assignment operator
$\|$	Concatenation operator

Table 6.1: Notations and their description.

the name space N and assigns it to T_i. ID_i is stored on S and T_i. Each assigned ID_i becomes a member of the set $\boldsymbol{T}_R$.

- *Auth (Kpriv,* $\boldsymbol{T}_R$*, M)* $\rightarrow$ *(Output)*: The server authenticates the tag T_i, whereby they interact as follows:

1. Server: S generates $r1 \leftarrow PRNG()$ and sends it to T_i.
2. Tag: The tag T_i generates $r2 \leftarrow PRNG(r2' \bigoplus r1)$ as a temporary secret for the session (for the very first session, $r2'$ is initially equal to 0), assigns $r2' \leftarrow r2$, and sends the server

$$M \equiv \left(\left(\left(ID_i \bigoplus r1\right) \| r2\right)^2\right)^2 mod\ z$$

3. Server:
   (a) Upon receiving M, the server finds four candidates X', satisfying $M \equiv X'^2\ mod\ z$, using the Chinese Reminder Theorem (CRT) [74] with the knowledge of *Kpriv: {p, q}*. Only one of these solutions would be a perfect square. The square root of this solution would be a quadratic residue X satisfying $M \equiv (X^2)^2\ mod\ z$.
   (b) Next, the server removes l right bits (where l – is the length of $r2$) from X and XORs the resulted value with $r1$. Let the result of these operations be ID_i'.

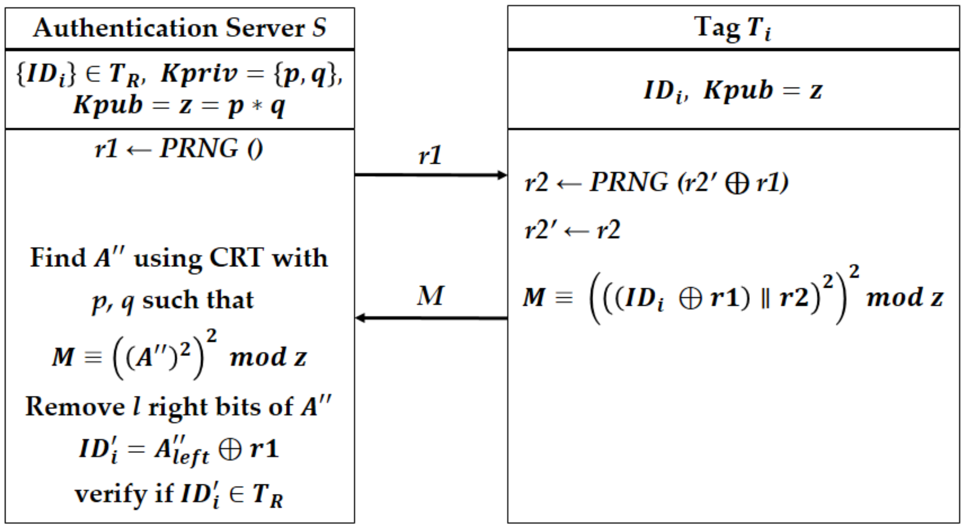


Figure 6.1: The proposed authentication protocol.

Finally, the server looks for the value ID_i' in the database (set $\boldsymbol{T}_R$). If ID_i' is found, the algorithm returns **Output** = True. Otherwise, the algorithm returns $\perp$.

6.7 Adding Ownership Transfer

In our protocol, the ownership is defined by the possession of a private key, corresponding to the public key. Indeed, only the owner can decrypt communications using the private key. Therefore, in order to transfer ownership, the following steps have to be performed (see Fig. 6.2):

1. The current authentication sever (S_{old}) sends a request to the tag.
2. The tag generates $X \leftarrow PRNG()$.
3. The tag sends M to the server:
$$M = (X^2)^2 \ mod\ z$$
4. The server finds X' – the square root of the quadratic residue of M using its current private key *Kpriv (p, q)*.
5. S_{old} generates a new pair of public/private keys *(Kpub, Kpriv)*: $(z', \{p', q'\})$, where p', q' – two large primes, $z' = p' * q'$, and sends back the decrypted value X' concatenated with the new public key z':
$$response = X' \parallel z'$$

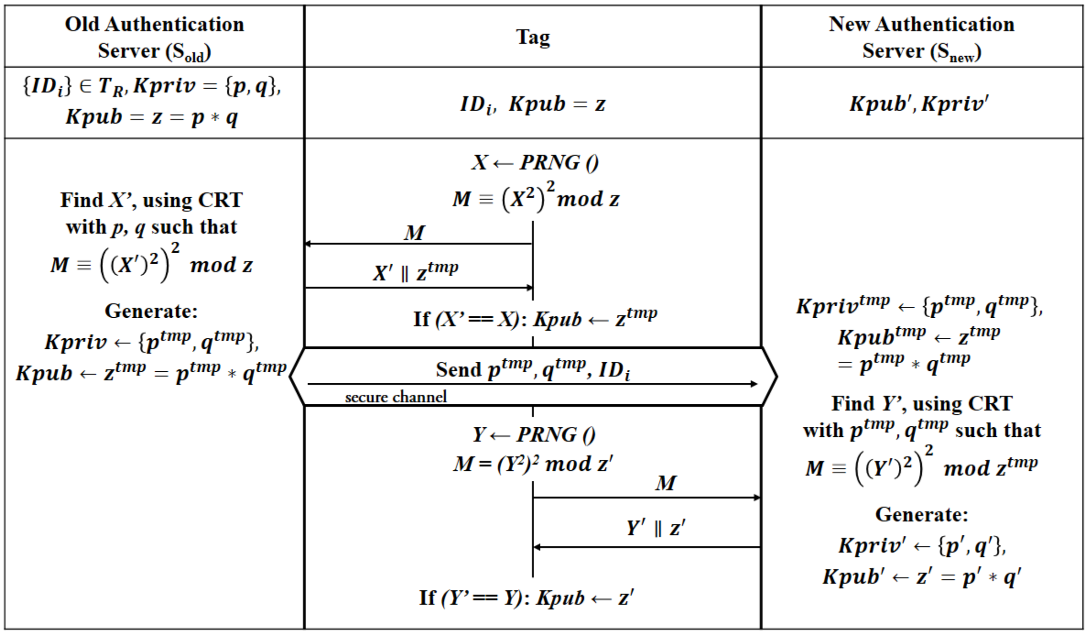


Figure 6.2: The proposed protocol for the ownership transfer.

6. If the left half of the response matches X, the server is authenticated and the tag accepts the new public key (the right half of the response). The tag replaces the old key with the new one.
7. The current server transmits the new *Kpriv* and ID_i to the new authentication server. This operation is performed in a secure environment.
8. The new authentication server runs the first transaction with the tag and changes *Kpub* and *Kpriv*, performing steps 1–6 described here.

Step 8 has to be performed to cause the update of the key pair (*Kpub, Kpriv*) in order to avoid using the keys that are known to the previous authentication server.

In the result of the ownership transfer protocol, the new owner is the only entity that holds a new private key. Hence, the old owner has no access to the tag and can no longer decrypt messages with the old key. Therefore, the ownership is transferred to the new owner.

Note: During the ownership transfer phase, we consider that the attacker can neither modify nor block messages. However, the attacker can eavesdrop the channel between the tag and the server. The communication between the current and the new server is considered protected from eavesdropping.

6.8 Formal Analysis

Formal analysis is performed by analysing the possible attacker's behaviour given the attacker model and the attacks described in Chap. 4. The respective attacks are represented using the game approach. We separate the analysis to Privacy and Security properties.

6.8.1 Privacy Analysis

Theorem 1. *The proposed scheme provides anonymity.*

Proof. To break anonymity, the goal of A is to extract T's *ID* from T's response m. This goal cannot be achieved due to the one-way property of the Rabin encryption. ■

Definition 3 (Backward-untraceability game). *A Backward-untraceability game is defined as a privacy game G between a strong adversary A and a collection of server and tag instances. This game allows the adversary A to launch the Backward attack:*

Phase 1 (Learning): The adversary randomly selects two valid tags T_0 and T_1 and calls any of the following queries at her wish to these tags for the next *(i-1)*-sessions: *Execute*, *SendTag*, *Modify*. I.e., the adversary can eavesdrop communications, query tags, modify/block messages at any of the following *(i-1)*-sessions.

Phase 2 (Challenge):

1. At the session i during G, A randomly chooses a bit $b \in$ *{0, 1}*. A is given a tag T_b from the set $\{T_0, T_1\}$.
2. A makes a *Corrupt* (T_b) query.

Phase 3 (Guess): A terminates the game and outputs a bit *b'* as its guess of the value b. A wins the game if *b'=b*.

Definition 4 (Backward-untraceability). An RFID authentication scheme provides backward-untraceability if there is no A who wins the Backward-untraceability game with the probability $\Pr[b' = b] \geq \frac{1}{2} + e$, where e is negligible.

Theorem 2. *The proposed authentication protocol provides backward untraceability.*

Proof. Let A compromise T_0 at time i (i.e., A chooses a bit b=*0* during the Challenge phase). The adversary is given the message exchange between S and T_0 at time *(i-1)* denoted as

ME_{i-1}=*{Request, M}*,

where *Request* is the message sent by S, M is the message sent by T_0 back to S.

The goal of the adversary is to link M with the data on T_0, i.e., ID_0 and *Kpub*. Thus, the adversary attempts (1) to extract ID_0 from M or (2) to compute M given the knowledge of ID_0 and *Kpub* only. The former is computationally infeasible due to the one-way encryption property of the Rabin scheme: without the knowledge of *Kpriv*, it is not possible to find the pre-image of M. The latter is not possible because M contains a random number, freshly generated by T_0. The random number generated by T_0 is unknown to A because it is never transmitted in plain text. ∎

Definition 5 (Location privacy game). *A Location privacy game is defined as a privacy game G between a weak adversary A and a collection of server and tag instances. This game allows the adversary A to launch the Location privacy attack.*

The description of the Location privacy game is similar to the Backward-untraceability game with the exception that during the Phase 2 (Challenge), Step 2, instead of *Corrupt* query, A makes any of the following queries: *Execute*, *SendTag*.

Definition 6 (Location privacy). An RFID authentication scheme provides location privacy if there is no A who wins the Location privacy game with the probability $\Pr[b' = b] \geq \frac{1}{2} + e$, where e is negligible.

Theorem 3. *The proposed authentication protocol provides location privacy.*

Proof. Let A choose a bit b=*0* during the Challenge phase. The adversary is given the message exchange between S and T_0 at time *(i-1)* denoted as ME_{i-1}=*{Request, M}*, where *Request* is the message sent by S, M is the message sent by T_0 back to S. Let A send the same *Request* to T_0 at time i: *SendTag* (T_0, *i, Request*) $\rightarrow$ *m'*. A has a goal to link M with *m'*. This goal is not achieved because *Reply* and *m'* are encrypted using different random numbers generated by T_0. The random number generated by T_0 is unknown to A because it is never transmitted in plain text. ■

Definition 7 (Forward-untraceability game). *A Forward-untraceability game is defined as a privacy game G between a strong adversary A and a collection of server and tag instances. This game allows the adversary A to launch the Forward attack.*

Phase 1 (Challenge):

1. At the session i, the adversary A randomly selects two valid tags T_0 and T_1 and randomly chooses a bit $b \in \{0, 1\}$. A is given a tag T_b from the set $\{T_0, T_1\}$.
2. A makes a *Corrupt* (T_b) query.

Phase 2 (Learning): A calls any of the following queries at her wish to T_0 and T_1 for the next $(i+j-1)$-sessions: *Execute*, *SendTag*, *Modify*. I.e., the adversary can eavesdrop communications, query tags, modify/block messages at any of the following $(i+j-1)$-sessions. <u>A misses at least one session</u>, during which A does not eavesdrop and does not call any queries (see the assumption by Lim-Kwon [1]).

Phase 3 (Guess): A terminates the game and outputs a bit b' as its guess of the value b. A wins the game if $b'=b$.

Definition 8 (Forward-untraceability). An RFID authentication scheme provides Forward-untraceability if there is no A who wins the Forward-untraceability game with the probability $\Pr[b' = b] \geq \frac{1}{2} + e$, where e is negligible.

Theorem 4. *The proposed authentication protocol provides forward-untraceability.*

Proof. Let A compromise T_0 at time i (i.e., A chooses a bit $b=0$ during the Challenge phase). The adversary is given the message exchange between S and T_0 at time $(i+j)$ denoted as

$ME_{i+j}=\{Request,\ M\}$,

where *Request* is the message sent by S, M is the message sent by T_0 back to S.

A misses the session(s) at time p, where $0<p<j$. The goal of A is to link M with the data on T_0, i.e., ID_0, *Kpub*, and internal state of PRNG. Since A misses at least one valid session with S, during which T_0 updates the internal state of its

PRNG based on the Request from S, A is unaware of the next random numbers, generated by T_0, and thus cannot compute the T_0's reply in the session at time $(i+j)$ based on the compromised data at time i. ■

6.8.2 Security Analysis

In this section, we analyse security protection properties of the proposed protocol against Impersonation and Desynchronization attacks as per Definition 1.

Theorem 5. *The proposed scheme is secure against Impersonation attacks.*

Proof. As per Definition 1, A calls any of the queries *Execute*, *SendTag*, *Modify* with the goal to impersonate T. A can impersonate T in two ways: (1) to find T's *ID* from T's reply M or (2) to replay M on the Server's query Q. The former is not possible due to the one-way encryption function of the Rabin scheme. The latter is not possible since the correct tag's response depends on the random number generated by S, which is included in the encrypted reply by T. The probability of seeing the same query Q twice depends on the bit-length k of the random number generated by S.

The probability P of seeing the same request Q of the bit-length k at least twice during the total number of transactions N is

$$P = 1 - \frac{2^{\mathrm{k}} * \left(2^{\mathrm{k}} - 1\right) * \cdots * (2^{\mathrm{k}} - (\mathrm{N} - 1))}{(2^k)^{\mathrm{N}}}$$

The fraction converges to *1* when 2^k is significantly larger in comparison to a reasonable number of transactions N observed by the attacker. Therefore, the probability P converges to *0*. ■

Theorem 6. *The proposed scheme is secure against Desynchronization attacks.*

Proof. As per Definition 1, A calls any of the queries *Execute*, *SendTag*, *Modify*, *Corrupt* with the goal to make S output $\perp$ at the end of the authentication protocol *Auth*. In other words, A's goal is to make a legitimate tag rejected by the authentication server. Since tags do not update their IDs in the proposed protocol, desynchronization is avoided. ■

6.9 Performance Analysis

Similar to the performance analyses of the existing works, we analyse the performance of the proposed protocol in terms of computational and storage requirements, database look-up complexity as well as the amount of communication flows.

Tag side

The following computational functions are called on the tag side:

1. PRNG – 1 call
2. XOR – 2 calls
3. Modular squaring – 2 calls

Storage requirements:

1. Non-volatile memory: $(1L + 1M)$ bit, where L is the maximum size of a tag's *ID*, M is the maximum size of the integer n (in bits).
2. Volatile memory: $(2L + 1M)$ bit.

Server side

The following computational functions are called on the server side:

1. PRNG – 1 call
2. XOR – 1 call
3. Solve quadratic residues – 1 call

Storage requirements:

1. Non-volatile memory: $L \cdot N + 3M$, where N is the number of tags in the system.
2. Volatile memory: $4L$+M

Database look-up complexity in the worst case: *O(1)*. The protocol consists of only two communication flows – the minimum for the challenge-response protocols.

6.10 Comparison

We compare the proposed protocol with the described existing works based on the security and privacy properties they provide and based on their performance characteristics.

	Scheme				
Property	Jin et al. [60]	Le et al. [61]	Lee et al. [62]	Doss et al. [63]	Our work
Anonymity	Yes	Yes	No	Yes	Yes
Location privacy	No	Yes	No	No	Yes
Impersonation attack	No	Yes	No	Yes	Yes
Desynchronization attack	No	No	No	Yes	Yes
Backward-untraceability	Yes	No	No	No	Yes
Forward-untraceability	No	Yes	Yes	No	Yes

Table 6.2: Comparison of Privacy and Security Properties. Yes: Property/protection is provided/secured; No: property/protection is not provided.

We first compare privacy and security properties. Table 6.2 summarizes security and privacy properties of the described above existing protocols as well as the properties of the proposed protocol. This summary is based on the analysis of vulnerabilities of the existing works presented in Chap. 5 and on the full formal security and privacy analyses of the proposed protocol.

As can be seen from Table 6.2, our proposed protocol satisfies all the security and privacy properties required from RFID authentication protocols. It provides anonymity, location privacy, is resistant to impersonation and desynchronization attacks, is backward- and forward-untraceable.

Finally, we compare the protocols based on their performance. In particular, we compare the amount and form of computations, amount of communication flows, and complexity of database look-up. We summarize the performance characteristics in Table 6.3.

The performance comparison shows that our scheme outperforms the existing works in the amount of communication flows, calculations on tags and on the server, and achieves the complexity for database loading of $O(1)$ in the worst case. The use of the lightweight functions and a low complexity of the protocol design makes it suitable for the implementation on low-cost EPC tags.

Scheme	**Flows**	**Computations on Tag**	**Computations on Server**	**Database loading**
Jin et al. [60]	3	1PRNG, 2XOR, 3ModSquaring, 1BitShift	2XOR, 2ModSquaring, 1BitShift	*O(N)*
Le et al. [61]	3	1PRNG	1PRNG	*O(N)*
Lee et al. [62]	4	5XOR, 1AND, 1OR, 2BitShift	1PRNG, 5XOR, 2BitShift, 1AND, 1OR	*O(1)*
Doss et al. [63]	3-6	1ModSquaring, 2PRNG, 7-10XOR, 1-4CRC, (l+1)ModMultiply	1SqRootSolving, 2PRNG, 1-4CRC, 4-7XOR, 1ModSquaring, (l+1)ModMultiply	*O(N)*
Our work	2	1PRNG, 2XOR, 1ModSquaring	1PRNG, 1XOR, 1SqRootSolving	*O(1)*

Table 6.3: Performance Comparison.

Chapter 7
Conclusion

In this dissertation, we have investigated the problem of the secure and privacy-friendly authentication in the technology of Radio-frequency identification.

Indeed, RFID was developed in order to provide cheap, fast, and automatic identification of objects. This has resulted in the variety of fields where RFID is applied: tracking of items during the transportation, identification of objects in warehouses, contactless payments, and many others. RFID has made identification of items faster and more reliable in comparison to traditional barcodes. One of the main advantages of RFID is that it does not require line-of-sight in order to identify an object. This, in particular, means that an RFID tag can be in any position on or inside an object; the packaging material or dirt will not disturb the process of identification. We have summarised the fundamentals and benefits of RFID in Chapter 2.

However, to provide fast identification, the technology applies a minimalistic approach: the bearers of identification information are simple low-cost tags that transmit their IDs to every reader that queries them. Originally, RFID does not provide any means for tags to authenticate the reader. Moreover, due to their simplicity, tags respond with unencrypted messages. This, in turn, violates security and privacy of communications. The following security and privacy threats are generally considered in RFID: absence of anonymity, traceability, impersonation attacks, desynchronization attacks, forward- and backward-traceability. We review these threats and their influence on users and business processes in Chapter 3. Based on them, we present an attacker model and formulate security and privacy requirements for RFID authentication protocols in Chapter 4.

In addition to the attacker model, in Chapter 4, we provide feasibility requirements for RFID authentication protocols that aim to be compatible with the EPC Class-1 Gen-2 Standard. This standard is applied for those low-cost tags that are going to replace barcodes on the item level. Due to the low computational and storage capabilities of EPC tags, the standard limits the use of computations to simple arithmetic operations in addition to the PRNG on-board. The standard makes the following general restriction: the upper bound for the chip area is 2000 Gate Equivalents (GE) for security purposes and 10000 GE – for the overall gate budget.

In Chapter 5, we have investigated four existing authentication protocols that attempted to achieve security and privacy in RFID using lightweight functions only. Conducted vulnerability analyses has shown that none of these schemes satisfies all the security and privacy requirements for RFID authentication protocols.

Based on the vulnerability analyses of the existing works, in Chapter 6, we have formulated conclusions on how to design a secure and privacy-friendly authentication protocol in RFID. In particular, we formulate our conclusions concerning how to achieve protection against various security and privacy attacks, what influences the protocol complexity, and how to protect against desynchronization.

As a contribution of this dissertation, we have proposed a minimalist RFID authentication protocol based on Quadratic residues. The proposed approach addresses two challenges – (1) to design a robust secure and private authentication protocol and (2) to achieve compliance with EPC Class-1 Gen-2. In particular, the scheme uses modular squaring (which is replaced by addition and multiplication in the practical implementation [77]), XOR, and PRNG functions that meet computational constraints of EPC Class-1 Gen-2 passive RFID tags.

Privacy and Security analysis of the proposed scheme shows that it overcomes the flaws of the previous works and achieves the required properties of the tag anonymity, location privacy, backward- and forward-untraceability while being resistant to impersonation and desynchronization attacks. In addition, we have presented an ownership transfer protocol that allows tags to change owners so that the old owner can neither authenticate nor trace the tag anymore.

The performance comparison shows that our scheme outperforms the existing works in the amount of communication rounds, calculations on tags and on the server, and achieves the complexity for database loading of *O(1)* in the worst case. To the best of our knowledge, this is the first lightweight protocol for RFID authentication that provides forward- and backward-untraceability at the same time, and is robust against security and privacy attacks generally considered in RFID systems. The implementation of this scheme has the potential to strongly enhance privacy and security of RFID-based transactions insuring that the privacy of users is not violated.

Our future work will target the following directions of research:

1. Verification of the security and privacy properties of proposed protocol with the compliance to the recently proposed Untraceability model by Avoine et al. [79].

2. Simulation of the proposed protocol in the network simulation environment, e.g., NS-3. This simulation would allow us to evaluate the authentication delay and other performance parameters. The example of the modelling of RFID entities and their communications on different layers in NS-3 is the work by El Moustaine [80].

3. Design and implementation of the proposed protocol on EPC C1G2-compatible tags. This could verify the compatibility of the proposed protocol with the EPC C1G2 standard. The starting point for this direction can be a study by Arbit et al. [77].

Bibliography

[1] C. H. Lim and T. Kwon, "Strong and robust RFID authentication enabling perfect ownership transfer," in *Information and Communications Security*. Springer, 2006, pp. 1–20. (Cited on pages 3, 31, 35, 36, 56, 67 and 75.)

[2] A. Juels and S. Weis, "Authenticating Pervasive Devices with Human Protocols," in *Advances in Cryptology – CRYPTO 2005 SE – 18*, ser. Lecture Notes in Computer Science, V. Shoup, Ed. Springer Berlin Heidelberg, 2005, vol. 3621, pp. 293–308. (Cited on pages 4, 20, 37, 38 and 39.)

[3] S. A. Weis, "RFID (radio frequency identification): Principles and applications," 2007. (Cited on pages 8 and 13.)

[4] D. Sen, P. Sen, and A. M. Das, *RFID for energy & utility industries*. Pennwell Books, 2009. (Cited on page 8.)

[5] Cisco Systems, "RFID Tag Considerations," in *Wi-Fi Location-Based Services 4.1 Design Guide*, San Jose, USA, 2008, ch. Chapter 6. (Cited on page 8.)

[6] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. John Wiley & Sons, 2010. (Cited on pages 8, 16 and 18.)

[7] S. A. Ahson and M. Ilyas, *RFID handbook: applications, technology, security, and privacy*. CRC press, 2008. (Cited on page 8.)

[8] SkyRFID Inc., "RFID Tag Maximum Read Distance." [Online]. Available: http://skyrfid.com/RFID_Tag_Read_Ranges.php (Cited on page 11.)

[9] J. Susini, H. Chabanne, and P. Urien, *RFID and the Internet of Things*. ISTE - John Wiley & Sons, 2011, ch. RFID and t, p. 304. (Cited on page 12.)

[10] N. Abramson, "THE ALOHA SYSTEM: another alternative for computer communications," in *Proceedings of the November 17-19, 1970, fall joint computer conference*. ACM, 1970, pp. 281–285. (Cited on page 14.)

[11] L. G. Roberts, "ALOHA packet system with and without slots and capture," *ACM SIGCOMM Computer Communication Review*, vol. 5, no. 2, pp. 28–42, 1975. (Cited on page 14.)

[12] J. Myung, W. Lee, and J. Srivastava, “Adaptive binary splitting for efficient RFID tag anti-collision,” *IEEE Communications Letters*, vol. 10, no. 3, pp. 144–146, 2006. (Cited on page 14.)

[13] J.-R. Cha and J.-H. Kim, “Novel anti-collision algorithms for fast object identification in RFID system,” in *Parallel and Distributed Systems, 2005. Proceedings. 11th International Conference on*, vol. 2. IEEE, 2005, pp. 63–67. (Cited on page 14.)

[14] D.-H. Shih, P.-L. Sun, D. C. Yen, and S.-M. Huang, “Taxonomy and survey of RFID anti-collision protocols,” *Computer communications*, vol. 29, no. 11, pp. 2150–2166, 2006. (Cited on page 14.)

[15] A. Juels, “RFID security and privacy: a research survey,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, Feb. 2006. (Cited on pages 15, 20, 21, 22 and 29.)

[16] ISO/IEC, “ISO/IEC 14443-1:2008,” *Identification cards – Contactless integrated circuit cards – Proximity cards*, 2008. (Cited on page 16.)

[17] Z. Kfir and A. Wool, “Picking virtual pockets using relay attacks on contactless smartcard,” in *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on.* IEEE, 2005, pp. 47–58. (Cited on page 16.)

[18] I. Recommendation, “ISO/IEC 7498-1: 1994,” *Information technology–Open systems interconnection–Basic reference model: The basic model*, 1994. (Cited on page 16.)

[19] H. Knospe and H. Pohl, “RFID security,” *Information Security Technical Report*, vol. 9, no. 4, pp. 39–50, Dec. 2004. (Cited on page 16.)

[20] S. Shepard, *RFID: radio frequency identification.* McGraw Hill Professional, 2005. (Cited on page 16.)

[21] “The International Organization for Standardization (ISO).” [Online]. Available: http://www.iso.org/ (Cited on page 17.)

[22] “International Electrotechnical Commission (IEC).” [Online]. Available: http://www.iec.ch/ (Cited on page 17.)

[23] “EPCglobal.” [Online]. Available: http://www.gs1.org/epcglobal (Cited on pages 17 and 19.)

[24] "ISO/IEC 18000. Information technology – Radio frequency identification for item management." (Cited on page 18.)

[25] Verisign Inc., "EPCglobal Network Architecture Overview," 2008. [Online]. Available: https://www.verisign.com/static/DEV044097.pdf (Cited on page 19.)

[26] EPCglobal, "GS1 Identification Keys." [Online]. Available: http://www.gs1.org/id-keys (Cited on page 19.)

[27] Brooks Automation Inc., "RFID Advantages." [Online]. Available: http://www.brooks.com/applications-by-industry/semiconductor/rfid/rfid-basics/rfid-advantages (Cited on page 20.)

[28] RFID Arena, "Benefits of implementing RFID in Supply Chain Management." [Online]. Available: http://rfidarena.com/2013/11/14/benefits-of-implementing-rfid-in-supply-chain-management.aspx (Cited on page 22.)

[29] A. Juels, P. Syverson, and D. Bailey, "High-Power Proxies for Enhancing RFID Privacy and Utility," in *Privacy Enhancing Technologies SE - 14*, ser. Lecture Notes in Computer Science, G. Danezis and D. Martin, Eds. Springer Berlin Heidelberg, 2006, vol. 3856, pp. 210–226. (Cited on page 22.)

[30] Z. Zhang, Z. Lu, V. Saakian, X. Qin, Q. Chen, and L.-R. Zheng, "Item-Level Indoor Localization With Passive UHF RFID Based on Tag Interaction Analysis," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 4, pp. 2122–2135, Apr. 2014. (Cited on page 22.)

[31] J. Zhou and J. Shi, "RFID localization algorithms and applications – a review," *Journal of Intelligent Manufacturing*, vol. 20, no. 6, pp. 695–707, 2009. (Cited on page 22.)

[32] L. Buttyan and J.-P. Hubaux, *Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing*. Cambridge University Press, 2007. (Cited on page 25.)

[33] F. B. Schneider, "Something You Know, Have, or Are." [Online]. Available: https://www.cs.cornell.edu/courses/cs513/2005fa/nnlauthpeople.html (Cited on page 26.)

[34] A. Juels and R. Pappu, "Squealing Euros: Privacy protection in RFID-enabled banknotes," *Computer Aided Verification*, pp. 103–121, 2003. (Cited on page 29.)

[35] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID attacks and defenses," *Information Systems Frontiers*, vol. 12, no. 5, pp. 491–505, 2010. (Cited on page 29.)

[36] J. Kim, "Comparison of Attacks and Security Analyses for Different RFID Protocols," in *IT Convergence and Security 2012 SE - 22*, ser. Lecture Notes in Electrical Engineering, K. J. Kim and K.-Y. Chung, Eds. Springer Netherlands, 2013, vol. 215, pp. 189–196. (Cited on page 29.)

[37] M. Ohkubo, K. Suzuki, S. Kinoshita, and Others, "Cryptographic approach to 'privacy-friendly' tags," in *RFID privacy workshop*, vol. 82. Cambridge, USA, 2003. (Cited on page 29.)

[38] J. Lim, H. Oh, and S. Kim, "A new hash-based RFID mutual authentication protocol providing enhanced user privacy protection," in *Information security practice and experience*. Springer, 2008, pp. 278–289. (Cited on pages 29 and 35.)

[39] A. Juels, D. Molnar, and D. Wagner, "Security and Privacy Issues in E-passports," in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*. IEEE, pp. 74–88. (Cited on page 30.)

[40] G. Avoine, "Adversarial Model for Radio Frequency Identification." *IACR Cryptology ePrint Archive*, vol. 2005, p. 49, 2005. (Cited on pages 31 and 39.)

[41] S. Vaudenay, "On Privacy Models for RFID," in *Advances in Cryptology – ASIACRYPT 2007 SE – 5*, ser. Lecture Notes in Computer Science, K. Kurosawa, Ed. Springer Berlin Heidelberg, 2007, vol. 4833, pp. 68–87. (Cited on pages 31 and 39.)

[42] A. Juels and S. A. Weis, "Defining strong privacy for RFID," in *Proceedings - Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2007*, 2007, pp. 342–347. (Cited on pages 31 and 39.)

[43] A. Mitrokotsa, M. Beye, and P. Peris-Lopez, "Classification of RFID Threats based on Security Principles." [Online]. Available: http://lasecwww.epfl.ch/~katerina/papers/RFIDthreats.pdf (Cited on page 32.)

[44] L. SIMSON, A. Juels, and R. Pappu, "RFID privacy: An overview of problems and proposed solutions," in *IEEE Symposium on Security & Privacy*, 2005, pp. 34–43. (Cited on pages 32 and 34.)

[45] K. Osaka, T. Takagi, K. Yamazaki, and O. Takahashi, "An Efficient and Secure RFID Security Method with Ownership Transfer," in *2006 International Conference on Computational Intelligence and Security*, vol. 2. IEEE, Nov. 2006, pp. 1090–1095. (Cited on page 35.)

[46] T. van Deursen, S. Mauw, S. Radomirović, and P. Vullers, "Secure Ownership and Ownership Transfer in RFID Systems," in *Computer Security – ESORICS 2009 SE – 39*, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds. Springer Berlin Heidelberg, 2009, vol. 5789, pp. 637–654. (Cited on page 36.)

[47] EPCGlobal, "Class-1 generation 2 UHF air interface protocol standard version 1.2.0, Gen2, 2008," 2008. [Online]. Available: http://www.epcglobalinc.org/standards/ (Cited on page 37.)

[48] P. Picazo-Sanchez, L. Ortiz-Martin, P. Peris-Lopez, and J. C. Hernandez-Castro, "Security of EPC Class-1," *Security and Trends in Wireless Identification and Sensing Platform Tags: Advancements in RFID: Advancements in RFID*, p. 34, 2012. (Cited on page 37.)

[49] F. Armknecht, M. Hamann, and V. Mikhalev, "Lightweight Authentication Protocols on Ultra-Constrained RFIDs-Myths and Facts," in *Radio Frequency Identification: Security and Privacy Issues*. Springer, 2014, pp. 1–18. (Cited on page 38.)

[50] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "LAMED–A PRNG for EPC Class-1 Generation-2 RFID specification," *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 88–97, 2009. (Cited on page 38.)

[51] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varıcı, and I. Verbauwhede, "SPONGENT: A lightweight hash function," in *Cryptographic Hardware and Embedded Systems–CHES 2011*. Springer, 2011, pp. 312–325. (Cited on page 38.)

[52] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON family of lightweight hash functions," in *Advances in Cryptology–CRYPTO 2011*. Springer, 2011, pp. 222–239. (Cited on page 38.)

[53] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, *PRESENT: An ultra-lightweight block cipher*. Springer, 2007. (Cited on page 38.)

[54] C. A. Repec., “Regulatory status for using RFID in the EPC Gen 2 band (860 to 960 MHz) of the UHF spectrum,” 2014. [Online]. Available: http://www.gs1.org/docs/epc/UHF_Regulations.pdf (Cited on page 38.)

[55] D. Dolev and A. C. Yao, “On the security of public key protocols,” *Information Theory, IEEE Transactions on*, vol. 29, no. 2, pp. 198–208, 1983. (Cited on page 39.)

[56] P. H. Cole and D. C. Ranasinghe, “Networked RFID systems and lightweight cryptography,” *Springer*, vol. 10, pp. 973–978, 2008. (Cited on page 39.)

[57] R. C.-W. Phan, J. Wu, K. Ouafi, and D. R. Stinson, “Privacy analysis of forward and backward untraceable RFID authentication schemes,” *Wireless Personal Communications*, vol. 61, no. 1, pp. 69–81, 2011. (Cited on pages 40 and 66.)

[58] N. Li, Y. Mu, W. Susilo, F. Guo, and V. Varadharajan, “Privacy-Preserving Authorized RFID Authentication Protocols,” in *Radio Frequency Identification: Security and Privacy Issues - 10th International Workshop, RFIDSec 2014, Oxford, UK, July 21-23, 2014, Revised Selected Papers*, ser. Lecture Notes in Computer Science, N. Saxena and A.-R. Sadeghi, Eds., vol. 8651. Springer, 2014, pp. 108–122. (Cited on page 40.)

[59] S. Piramuthu, “Protocols for RFID tag/reader authentication,” *Decision Support Systems*, vol. 43, no. 3, pp. 897–914, 2007. (Cited on page 43.)

[60] Y. Jin, H. Sun, W. Xin, S. Luo, and Z. Chen, “Lightweight RFID Mutual Authentication Protocol against Feasible Problems,” in *Information and Communications Security SE – 6*, ser. Lecture Notes in Computer Science, S. Qing, W. Susilo, G. Wang, and D. Liu, Eds. Springer Berlin Heidelberg, 2011, vol. 7043, pp. 69–77. (Cited on pages 44, 45, 46, 78 and 79.)

[61] T. Van Le, M. Burmester, and B. de Medeiros, “Universally composable and forward-secure RFID authentication and authenticated key exchange,” in *Proceedings of the 2nd ACM symposium on Information, computer and communications security - ASIACCS ’07*. New York, New York, USA: ACM Press, Mar. 2007, p. 242. (Cited on pages 44, 49, 50, 51, 78 and 79.)

[62] Y.-C. Lee, Y.-C. Hsieh, P.-S. You, and T.-C. Chen, “A New Ultralightweight RFID Protocol with Mutual Authentication,” in *2009 WASE International Conference on Information Engineering*, vol. 2. IEEE, Jul. 2009, pp. 58–61. (Cited on pages 44, 53, 54, 78 and 79.)

[63] R. Doss, W. Zhou, S. Sundaresan, S. Yu, and L. Gao, "A minimum disclosure approach to authentication and privacy in RFID systems," *Computer Networks*, vol. 56, no. 15, pp. 3401–3416, Oct. 2012. (Cited on pages 44, 57, 59, 78 and 79.)

[64] A. Shamir, "SQUASH–A new MAC with provable security properties for highly constrained devices such as RFID tags," in *Fast Software Encryption*. Springer, 2008, pp. 144–157. (Cited on page 45.)

[65] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Rabin public-key encryption," in *Handbook of Applied Cryptography*. CRC Press, ch. 8.3, pp. 292–294. (Cited on pages 45 and 69.)

[66] Z. Sohrabi-Bonab, M. R. Alagheband, and M. R. Aref, "Traceability analysis of quadratic residue-based RFID authentication protocols," in *2013 Eleventh Annual Conference on Privacy, Security and Trust*. IEEE, Jul. 2013, pp. 61–68. (Cited on pages 47, 48, 60 and 61.)

[67] K. Ouafi and R. C.-W. Phan, "Traceable privacy of recent provably-secure RFID protocols," in *Applied Cryptography and Network Security*. Springer, 2008, pp. 479–489. (Cited on page 51.)

[68] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. E. Tapiador, and J. C. A. van der Lubbe, "Security flaws in a recent ultralightweight RFID protocol," *arXiv preprint arXiv:0910.2115*, 2009. (Cited on page 56.)

[69] K. H. Rosen, *Elementary number theory and its applications*, 4th ed. Addison-Wesley, 1999. (Cited on pages 57 and 69.)

[70] G. Avoine, E. Dysli, and P. Oechslin, "Reducing time complexity in RFID systems," in *Selected Areas in Cryptography*. Springer, 2006, pp. 291–306. (Cited on page 68.)

[71] G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," in *Third IEEE International Conference on Pervasive Computing and Communications Workshops*. IEEE, 2005, pp. 146–150. (Cited on page 68.)

[72] M. Girault, L. Juniot, and M. Robshaw, "The feasibility of on-the-tag public key cryptography," in *Conference on RFID Security*. Citeseer, 2007. (Cited on page 68.)

[73] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Jan. 1979. (Cited on page 68.)

[74] K. Ireland and M. Rosen, "The Chinese Remainder Theorem," in *A Classical Introduction to Modern Number Theory*, 2nd ed. New York, USA: Springer-Verlag, 1990, ch. 3.4, pp. 34–38. (Cited on pages 68 and 70.)

[75] S. Sundaresan, R. Doss, and W. Zhou, "Offline grouping proof protocol for RFID systems," in *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, Oct. 2013, pp. 247–252. (Cited on page 69.)

[76] Y. Oren and M. Feldhofer, "A low-resource public-key identification scheme for RFID tags and sensor nodes," in *Proceedings of the second ACM conference on Wireless network security - WiSec '09*. New York, New York, USA: ACM Press, Mar. 2009, p. 59. (Cited on page 69.)

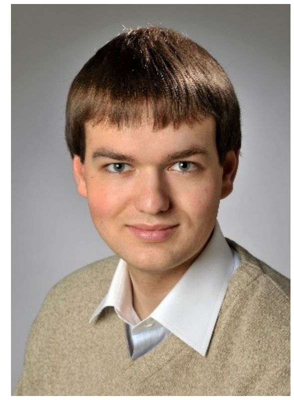
[77] A. Arbit, Y. Livne, Y. Oren, and A. Wool, "Implementing public-key cryptography on passive RFID tags is practical," *International Journal of Information Security*, Apr. 2014. (Cited on pages 69, 82 and 83.)

[78] E. Wenger, T. Unterluggauer, and M. Werner, "8/16/32 shades of elliptic curve cryptography on embedded processors," in *Progress in Cryptology–INDOCRYPT 2013*. Springer, 2013, pp. 244–261. (Cited on page 69.)

[79] G. Avoine, I. Coisel, and T. Martin, "Untraceability Model for RFID," *IEEE Transactions on Mobile Computing*, vol. 13, no. 10, pp. 2397–2405, Oct. 2014. (Cited on page 83.)

[80] E. El Moustaine, "Authentication issues in low-cost RFID," Ph.D. dissertation, Institut National des Télécommunications, 2013. (Cited on page 83.)

Sviatoslav Edelev



Personal Information

Birthday: September 22, 1990
Birthplace: Leningrad, Russia
Marital status: Married
Address: Robert-Koch-Str. 38, App.531, 37075 Göttingen
E-mail: slava.edelev@gmail.com
Mobile: +49 176/554-194-95

Education

Aug 2012 – Sep 2015 — **PhD in Computer Science** — *Göttingen, Germany*
GEORG-AUGUST UNIVERSITÄT GÖTTINGEN
Institute of Applied Computer Science, Telematics Group
PhD Project: "Enhancing Security & Privacy of RFID Authentication Protocols"

Oct 2015 – Nov 2015 — **Foreign Academic Visit** — *Nanjing, China*
NANJING UNIVERSITY,
Department of Computer Science, Distributed Computing Lab
Research Project: "RFID as Enabler of Authentication to Mobile Clouds"

Sep 2007 – Jun 2012 — **Diploma in Automated Systems and Computer Software Support (with excellence)** — *St.-Petersburg, Russia*
ST. PETERSBURG UNIVERSITY OF TELECOMMUNICATIONS
Faculty of Communication Networks, Commutation Systems and Computing Equipment
Diploma Project: "Client-Server Mobile Software for Authentication to the Objects of Restricted Access"

Sep 2010 – Dec 2010 — **Exchange Student** — *Jyväskylä, Finland*
THE UNIVERSITY OF JYVÄSKYLÄ, Department of Information Science
International Master Program: "Mobile Telecommunications and Business"

Awards

Aug 2012 – April 2015	**PhD grant,** Erasmus Mundus Action 2 Strand 1, European Mobility Program
Sep 2011	**Prize for Excellence in Studies,** Saint-Petersburg City Government
Sep 2007 – Jun 2012	**State Scholarship for Diploma Studies,** Russian Ministry of Education
Sep 2007 – Jun 2012	**Scholarship for Diploma Studies,** Sakhalin Energy Investment Company Ltd.
April 2011	**Winner,** IVth All-Russian Student Contest "IT in the world of communications"
May 2008	**Laureate "Leader of the XXI century",** Saint-Petersburg City Government

Experience

Jan 2010 – Dec 2012
ST. PETERSBURG UNIVERSITY OF TELECOMMUNICATIONS

Teaching Assistant
- Conducted practical lessons for undergraduate and part-time students on the basics of programming using C and Pascal: Explained the theory of computer science on practice.

Engineer-Programmer
- Assisted the System Administrator: technical support of the local computer network containing 25 Workstations and a server.
- Software development using C, Python, Visual Basic, Visual Basic for Applications, PHP, MySQL, HTML, JavaScript.
- User support: consulted and provided trainings for students, faculty, and staff on the use of software and hardware.

Teaching:

- Seminar on Network Security and Privacy: SS 2013, WS 2013/14, SS 2014, SS2015
- Exercises & Lectures, Security and Cooperation in Wireless Networks: WS2013/14, WS 2014/15
- Sessions on Security, Mobile Communications: SS 2014

Supervision:

- 3 Master Research Projects
- 1 Master Thesis

Article Reviewer:

- IEEE Mobile Cloud Computing 2014
- Journal of Computer Science and Technology

Skills

- **Technology** — Network Protocols, Network Security, Network Administration, Programming: C/C++, JavaScript, PHP, Visual Basic, MySQL, Python.
- **Key Competences** — Project Management, Goal Formulation, Process Optimization, Conflict Resolution, Team Work, Collaborative, Critical Thinking
- **Languages** — English (advanced), German (intermediate), Russian (native)

Publications

1. S. Edelev, S. Taheri, and D. Hogrefe, "A Secure Minimalist RFID Authentication and an Ownership Transfer Protocol Compliant to EPC C1G2", in *Proceedings of the 6th IEEE Conference on RFID Technology and Applications (RFID-TA 2015)*, Tokyo, Japan, September 2015.
2. B. Mayeku, S. Edelev, S. Prasad, H. Karnal, and D. Hogrefe, "PECALE: An Environment for Enhancing Personalization and Learner Engagement in an Online Learning Platform", poster, *in the 15th International Conference on Advanced Learning Technologies (IEEE ICALT-2015)*, Hualien, Taiwan, July 2015.
3. S. Edelev, S. Taheri, and D. Hogrefe, "Show Me Your ID and I Will Show You Mine: A Mutual Authentication Protocol Against Traceability in RFID", poster, in *Proceedings of the 9th IEEE International Conference on RFID (IEEE RFID-2015)*, San Diego, USA, April 2015.
4. S. Edelev, S. N. Prasad, H. Karnal, and D. Hogrefe, "Knowledge-assisted Location-adaptive Technique for Indoor-Outdoor Detection in E-Learning", in *Proceedings of the 13th IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, St. Louis, USA, March 2015.
5. V. Petrov, S. Edelev, M. Komar, and Y. Koucheryavy, "Towards the Era of Wireless Keys: How the IoT Can Change Authentication Paradigm", in *Proceedings of the 1st IEEE World Forum on Internet of Things (IEEE WF-IoT 2014)*, Seoul, Korea, March 2014.

Certifications

January 2011 – current — **Intel Mobile Programming Professional**
issued by Intel Co., License IMPP-2-029

April 2009 – current — **System Administrator**
issued by Joint-Stock Company "Das kleine Rechenzentrum", License ABF No. 170

Göttingen, 06.08.2015