THE ROMANIAN ACADEMY
The School of Advanced Studies of the Romanian Academy
“Simion Stoilow” Institute of Mathematics of the Romanian Academy

PhD THESIS SUMMARY

Security and Privacy of RFID Schemes in Vaudenay’s Model

SUPERVISOR:
Prof. Dr. Ferucio Laurenţiu Ţiplea

AUTHOR:
Nicolae Cristian Hristea

2024

Contents

Preface

Thesis Goal

This thesis is concerned with the study of RFID security and privacy from a cryptographic perspective. The main element of study in this research domain is the communication protocol between the reader and the tag. In order to perform such a study, one needs a *model* that provides rigorous definitions for security and privacy and for the adversarial powers. The model helps researchers to design protocols and to produce formal security proofs that can be easily verified and are preferrable to ad-hoc analysis. Probably the most complete and mature model for RFID is Vaudenay's model [31,38]. In the model, the adversary can create tags (both legitimate and illegitimate), intercept and forge messages and, depending on its powers, corrupt tags and learn the result of an authentication session. Vaudenay's model classifies adversaries into eight categories which in turn give rise to eight corresponding privacy classes. The *destructive privacy* class defines protocols that achieve privacy against adversaries that can learn whether an authentication session is successful and corrupt tags in order to obtain their internal state. The only restriction on this type of adversary is that a tag is considered destroyed after it has been corrupted.

The goal of this thesis is to perform a study of destructive privacy in Vaudenay's model. We will explore the ways in which destructive privacy can be achieved and highlight model characteristics that can considerably affect the privacy level that a protocol achieves. One such feature is the distinction between corruption and corruption with temporary state disclosure (in the latter the adversary obtains not only the persistent state but also the temporary state resulted from the tag's internal computation). In this regard, we will describe attacks against existing protocols and solutions for obtaining destructive privacy in the context of the tag's exposed temporary state. For each RFID scheme that we propose in this thesis we will present detailed security and privacy proofs. It is our hope that these proofs will contribute to the evolution and better understanding of the model and of the intricacies of designing RFID protocols.

Contributions

The main contributions of the thesis are the following:

1. We propose the first mutual authentication protocol with complete proofs that achieves destructive privacy in Vaudenay's model [17] (preprint [18]) - Chapter 3.
2. We define temporary variables and highlight the role they play in achieving privacy under temporary state disclosure [17, 36] - Chapter 4.
3. We propose a general method of achieving privacy under TSD by protecting the temporary variables that carry information between protocol steps [36] - Chapter 4.
4. We propose two RFID protocols designed according to the reader-first approach that achieve destructive privacy under temporary state disclosure by avoiding the use of temporary variables [37, 39, 40] (preprint [8]) - Chapter 5.
5. We extend the Vaudenay model to allow the analysis of stateful RFID schemes with constant tag identifiers and design a protocol that achieves destructive privacy in the extended model [19] (preprint [20]) - Chapter 6.
6. We analyse a privacy definition proposed for offline RFID schemes in Vaudenay's model and introduce a new privacy notion called offline privacy. We propose an RFID scheme that achieves destructive privacy and offline privacy [16] - Chapter 7.

Outline

The structure of the thesis is focused on the study of the destructive privacy notion from Vaudenay's security and privacy model. This section presents the outline of the thesis.

Chapter 1 introduces the RFID technology and the notions of security and privacy. We first describe RFID by focusing on its goal, benefits, and main components. A brief historical development of RFID is also presented. Then, we outline the cryptographic approach to RFID security and privacy, alongside with a short presentation of what a security and privacy model is and why it is needed. Afterwards, we sketch the main aspects of Physically Unclonable Functions, a new technology that complements RFID. The chapter concludes with design considerations for RFID protocols, concerning the use of random number generators, symmetric or asymetric cryptographic primitives, and identification times on the reader side.

Chapter 2 focuses on the security and privacy model employed in the thesis, namely Vaudenay's model. The chapter debuts with general and RFID specific definitions used in the rest of the thesis. Following this, we explain the Vaudenay model with a focus on the interaction between the adversary and the tags (through vtags) and the oracles available to the adversary. The security and privacy definitions and their corresponding experiments are described in detail. Afterwards, we present the main impossibility results for the model and perform an analysis of the model from the black/gray/white box perspective. We conclude with a general description of how proofs are constructed in the model and some methodological remarks.

Chapter 3 is centered around achieving destructive privacy. First of all, we discuss at length the PUF technology, focusing on its implications for destructive privacy and the formalism that we employ. We discuss how PUFs impact corruption and present a general result that facilitates the construction of privacy proofs when PUFs are used. Afterwards, we present the first protocol that achieved destructive privacy in a unilateral authentication setting. The protocol uses a PRF as the main cryptographic primitive and makes use of PUFs to ensure the tag key is kept protected from invasive adversaries. We then proceed to extend this construction to achieve destructive privacy together with mutual authentication. We provide detailed security and privacy proofs for this solution.

Chapter 4 tackles the problem of achieving more than weak privacy against adversaries that can obtain, through corruption, both the persistent and the temporary state of a tag. Firstly, we explain an impossibility result which states that, in the absence of PUFs, privacy greater than weak cannot be achieved under corruption with TSD. Secondly, we introduce the concept of temporary variables, which can be used to reason about corruption with TSD. With temporary variables in mind, we present two attacks against schemes that employ the double PUF protection technique to prevent adversaries from obtaining information from the intermediary computation of tags. Afterwards, we introduce a general solution, called *PUF protection*, which can be used to enhance protocols that are private in Vaudenay's model, to achieve the same privacy level in Vaudenay's model with TSD. A detailed proof accompanies this result. In the end, the solution is illustrated on two authentication protocols.

Chapter 5 handles the authentication order in RFID protocols, tag-first or reader-first. We present the implications of each approach and show that reader-first can be used as an alternative for destructive privacy alongside TSD. Following this approach, we design two protocols that achieve destructive privacy in Vaudenay's model with TSD by avoiding temporary variables between protocol steps. The reader-first approach also allows us to eliminate the random number generator from the tag, which results in more efficient and lightweight protocols. Both solutions employ PUFs as a protection against corruption. As the main cryptographic primitive, the first protocol makes use of a PRF while the second one uses an SKE scheme. The SKE protocol leverages the encryption scheme to obtain constant identification time on the reader. We provide detailed security and privacy proofs for both protocols.

Chapter 6 addresses the class of stateful RFID schemes with constant tag identifiers. After characterising this class of protocols, we show a general result that demonstrates that these protocols cannot achieve any privacy level in Vaudenay's model. Subsequently, we analyse the Refresh model [26], which was proposed for the analysis of stateful protocols, and prove that it is restricted only to unilateral authentication. We also construct an attack against the LAST RFID scheme, which accompanies this model, that proves that the scheme is insecure. Afterwards, we proceed to transform Vaudenay's model in order to allow the study of these protocols. In the end, we propose a mutual authentication RFID scheme that achieves destructive privacy in this model. We accompany the scheme with complete proofs.

Chapter 7 focuses on another class of protocols that cannot be analysed in Vaudenay's model, namely schemes that allow multiple readers in the system (i.e. offline schemes). After introducing these schemes, we discuss model proposals for the formal treatment of these schemes. We prove that such a proposal for Vaudenay's model, *privacy+*, is not adapted to the blinder-based privacy of the model. We propose an alternative notion called *offline privacy*, which comes as an additional analysis, on top of security and privacy. Finally, we propose an RFID scheme that achieves destructive privacy and offline privacy.

Chapter 8 presents the main conclusions that can be drawn from this thesis and summarises the main results that have emerged from this work.

Chapter 1

Introduction

1.1 Radio Frequency Identification

As a technology, Radio Frequency Identification (RFID) provides wireless identification of assets and people. Passports (or other types of IDs), public transport, access control, supply chain logistics or medical care, are domains that already benefit from RFID technology or could be dramatically improved by its use. Some of the advantages of RFID systems over other competing ID technologies (barcode, OCR, smart cards) are high data transfer rates, low operational costs, increased reading range, and independence of direction or position [11]. The central element of the RFID technology is a small transponder device called *tag* that is attached to an object and facilitates its identification. In most cases the tag has no power source and it relies on another device, called *reader* (or *interrogator* [11]), to power it with energy (captured by means of an antenna). The reader is a more powerful device whose main goal is to collect the data stored on the tag and either process it by itself or pass it on to another processing system. Once the tag is powered-up, the reader and the tag will engage in communication and exchange messages according to a *protocol*. The end result of the protocol is *identification*.

The RFID communication model is what sets it apart from other technologies. There are three components in any RFID system: the tag, the reader and the backend server. The tag and the reader form the core of any RFID system. The backend server is an entity with standard computational capabilities that owns (or has access to) a database. The reader communicates with the backend server through a channel that is considered to be secured by regular means (standard encryption). It is the channel between the reader and the tag (especially the authentication protocol) that is of interest to this thesis.

Attacks performed on RFID typically aim at eavesdropping (or "spying out"), impersonating tags or readers, denial of service and privacy breaches [11]. Denial of service is of interest to security enhancement as long as it targets the protocol and it can affect privacy. Otherwise, there is no RFID system that can defend against such attacks (e.g. signal jamming or shielding the tag with metal so that it cannot even be powered on [11]). Another special characteristic of RFID is the potency of invasive attacks. These attacks are mainly directed at tags, but can be aimed at the reader also, although more infrequent and in some special cases (RFID systems with multiple readers [4]). The discrepancy to regular computer systems is evident in this aspect. Physical access to a tag is far more straightforward than for a normal computer and tags lack advanced protection technology such as encrypted storage or tamper-detection mechanisms. Physical attacks can facilitate the recovery of the data stored on the tag and allow an attacker to impersonate the tag defeating the purpose of the RFID system (e.g. an attacker can gain access to a building by cloning an access card). The attacker could also use the data to discover past uses of the tag and breach the user's privacy.

In these circumstances identification alone can not solve RFID security and privacy concerns. Stronger protocols that offer *authentication*, in addition to identification, and prevent user tracking need to be designed. Given the scope of RFID, these protocols need to ensure that manufacturing costs for tags are minimised and the security overhead does not prevent scaling to large RFID applications or increase energy consumption beyond what the tag can provide. One could easily design ultra strong protocols that require an order-of-magnitude increase in tag costs, energy or computation, but that is not the aim. Balancing performance, costs and security turns out to be a significant challenge and a blend between science and art.

Over the last two decades efforts have been undertaken to construct and implement protocols that bring RFID closer to fulfilling its potential. Although the understanding of the field has increased and more adequate protocols have been proposed, there is still a long road ahead.

1.2 Cryptography in RFID

In RFID systems, cryptography plays a central role in mitigating user concerns about the security and user tracking that are inherent in these systems. The main goals that cryptography sets for RFID are *security* and *privacy*. Informally, the goal of security is to guarantee that an attacker cannot impersonate an entity (tag or reader), while the goal of privacy is to prevent an attacker from tracking or tracing a tag.

Protocols The fundamental element in an RFID setup, that allows the technology to be used, is the communication protocol between the reader and the tag. The main goal of this protocol is to allow the reader to perform the identification of the tag. Cryptography helps to transform this protocol into an authentication protocol where the identification is performed but the parties are convinced about the outcome [29]. RFID authentication protocols are typically single-pass when only the tag authenticates to the reader and always multi-pass when both the tag and the reader are authenticated. In general, RFID authentication protocols follow the "challenge - response" approach [29], where the tag or the reader issue a challenge to which the other party replies and proves the knowledge of a pre-shared secret. These authentication protocols can be based on various cryptographic primitives such as public key encryption [38], hash functions [1, 24], symmetric key encryption [37], or pseudorandom functions [17, 38]. Although authentication protocols ensure that the parties cannot be impersonated by a malicious adversary, authentication does not protect the identity of the parties (i.e. the adversary can still learn which tag participated in an authentication session). It is also through cryptography that the privacy goal of RFID protocols is achieved. Authentication protocols that are private are capable of protecting the identity of the tag even when the adversary is intercepting or manipulating the communication.

Security and Privacy Model A key step in designing protocols adapted to the specific RFID requirements is the development of an adequate security and privacy model. Such a model attempts to capture the essence of the real-world system and translates this into precise definitions, a complete description of the adversary's capabilities and the formulation of the security experiments that help develop security proofs. A privacy model brings value not just through the above, but also by offering a framework for comparison between authentication protocols and allows, thus, the possibility of improvement. In RFID there have been proposed various privacy models such as: [5,7,9,14,15,23,31,38].

Arguably, the most prominent model and the one that we follow in this thesis, is the one defined in [31,38], which we will call *Vaudenay's model* or *the Vaudenay model*. In the model the main entities (the tag, the reader and the adversary) are modelled as PPT (Probabilistic Polynomial Time) algorithms. The adversary interacts with the tag and the reader by means of *oracles* that allow it to start protocol sessions, intercept communication, learn whether protocol sessions complete successfully and obtain the internal state (including any secrets it may contain) of the tag. The last capability is called *corruption* and when the adversary obtains the tag state we say that it *corrupts* the tag. The possibility for corruption models the real world lack of physical protection of RFID integrated circuits. Since performing invasive hardware attacks is not trivial, the model distinguishes between multiple types of adversaries with this capability. We have thus *weak* adversaries (that cannot corrupt a tag), *forward* adversaries (that can perform corruption only at the end of their attacks), *destructive* adversaries (that destroy the tag after corruption) and *strong* adversaries (without corruption restrictions). When a protocol is resistant to an adversary class P, we say that the protocol achieves P $privacy$ (or is P $private$).

Chapter 2

Security and Privacy Model

2.1 Vaudenay's Model

The two most important requirements for RFID schemes are *security* and *privacy*. To formalise them, the concept of an *adversary model* is needed. In the literature there have been multiple models proposed, out of which we recall [3,5,7,9,14,15,23,31,38]. The model that we follow in this thesis, is *Vaudenay's model* [31,38].

In the model there is a single reader that is permanently connected to the central database. The reader can communicate with multiple tags at the same time (have multiple sessions open) but a tag can only be involved in a single session. The reader, the tags, and the adversary are all PPT algorithms.

The database of the reader DB is initially empty and tags are added to it as the adversary requests their creation. The adversary can request the creation of *legitimate* or *illegitimate* tags. The latter are created through the same process but they are not inserted in the reader database. Once created, a tag can be either *drawn* or *free*. This models the RFID characteristic that a tag can be powered on for a limited time and only when the reader or the adversary are in its vicinity. The drawn tags are the ones that the adversary can interact with (listen to the communication, send messages or corrupt them), while the free tags are considered outside the reach of the adversary. The adversary does not interact directly with a tag based on its identity but through a unique temporary identifier called *vtag*. Once a tag becomes drawn, it is assigned a vtag that the adversary uses to communicate with or corrupt the tag. If the tag is freed (it is no longer in the proximity of the adversary), the vtag can no longer be used. If the same tag is drawn again in the future it will be given a different vtag.

In Vaudenay's model the adversary is given access to the following oracles: $CreateTag$ (for creating tags), $Corrupt$ (for revealing the internal state of a tag), $SendTag$ and $SendReader$ (for communication), $Result$ (for learning the output of an authentication session), $Free$ and $DrawTag$ (for modelling the interaction with tags), and $Launch$ (for creating a new authentication session).

The model offers granularity by creating different categories of adversaries with different levels of power. The adversaries from the model are classified based on their access to the oracles $Corrupt$ and $Result$. Based on access to the $Corrupt$ oracle we obtain adversaries that are *weak*, *forward*, *destructive*, and *strong*, while based on the access to $Result$ the adversaries can be *narrow* or *wide*. We may now combine these classes to obtain eight adversarial classes: *narrow weak*, *narrow forward*, *narrow destructive*, *narrow strong*, *wide weak*, *wide forward*, *wide destructive*, *wide strong*. For simplicity, we will consider that when an adversary is denoted only as weak, forward, destructive or strong it is implicitly wide.

2.2 Security

The security of RFID schemes in Vaudenay's model can be decomposed in two protocol properties: *tag authentication* and *reader authentication*. Informally, security means that the tag or the reader cannot be impersonated by the adversary. In the view of the model, an adversary that tries to break this property in a protocol session, will have to create some messages that convince the reader/tag that the adversary is the other party.

The tag and reader authentication properties are captured through security experiments, which are built as a game between a strong adversary and a challenger. The adversary can create as many tags as it requires and corrupt any tag except a target tag ID. In this game the goal of the adversary is to impersonate the tag or the reader so that the other party authenticates it but without having a matching conversation. This means that, in order to win, the adversary can not only forward messages between the reader and the tag but must also compute at least a part of the message by itself.

An RFID scheme $\mathcal{S}$ achieves *tag authentication* if the advantage of $\mathcal{A}$ winning the tag authentication experiment is negligible, for any strong adversary $\mathcal{A}$.

An RFID scheme $\mathcal{S}$ achieves *reader authentication* if the advantage of $\mathcal{A}$ winning the reader authentication experiment is negligible, for any strong adversary $\mathcal{A}$.

2.3 Privacy

Privacy for RFID systems [31] captures anonymity and untraceability. Informally, privacy in this model means that an adversary cannot learn anything new from intercepting the communication between a tag and the reader. This concept is modelled through the use of a special algorithm called *blinder*. This method of formalising privacy is different from the usual method of defining privacy in RFID systems [14, 15, 22] based on the indistinguishability between two challenge tags (left-or-right indistinguishability).

A *blinder* for an adversary $\mathcal{A}$ that belongs to some class P of adversaries is a PPT algorithm $\mathcal{B}$ that simulates the $Launch$, $SendReader$, $SendTag$, and $Result$ oracles for $\mathcal{A}$, without having access to the tag and reader secrets, and passively observes the communication between $\mathcal{A}$ and the other oracles allowed for the class P.

When the adversary $\mathcal{A}$ interacts with the RFID scheme by means of a blinder $\mathcal{B}$, we say that $\mathcal{A}$ is *blinded by* $\mathcal{B}$ and denote this by $\mathcal{A}^{\mathcal{B}}$. We emphasize that $\mathcal{A}^{\mathcal{B}}$ is allowed to query the oracles $Launch$, $SendReader$, $SendTag$, and $Result$ only by means of $\mathcal{B}$; all the other oracles are queried as a standard adversary.

Privacy states that a protocol is private with respect to a class of adversaries if all adversaries from that class are *trivial*. A trivial adversary is basically an adversary that does not make use of the oracles that are simulated by blinder. In the privacy game, the adversary interacts with the RFID scheme and is allowed to query all oracles according to its class. This is denoted as the *learning phase*. At the end of this phase the adversary receives the secret table Γ of the $DrawTag$ oracle that contains the mappings between the tag identifiers and the vtags. Having this extra information the adversary enters an *analysis phase*, at the end of which it outputs whether it interacted with the blinder or the real oracles. We provide below two equivalent formulations for the privacy experiment in Vaudenay's model.

An RFID scheme $\mathcal{S}$ achieves privacy for a class V of adversaries if for any adversary $\mathcal{A} \in V$ there exists a blinder $\mathcal{B}$ such that the advantage of $\mathcal{A}$ of distinguishing the blinder simulated oracles from the real oracles is negligible.

Chapter 3

Destructive Privacy

3.1 Physically Unclonable Functions

Compared to RFID, the Physically Unclonable Functions (PUFs) are a technology that is relatively new. The first description of the notion of PUF, although by the name of *physical random function*, was presented in [32] in the early 2000s. The first reference with the exact terminology was first stated in [13]. Since then, the domain has gained momentum and a variety of PUF constructions have been proposed. The knowledge base of what a PUF is and what properties are desirable for PUFs, has matured as well.

PUFs [6, 27, 28] are hardware constructions capable of uniquely identifying the device on which they are implemented. In this regard, PUFs have been compared with human unique biometric features and have been considered the fingerprint of a device. The design process of a PUF aims to enhance the imperfections inherent to the manufacturing process in order to produce a differentiable and consistent unique trait of a circuit. This goes contrary to regular hardware manufacturing where these distinctions between objects are minimised. As the name suggests, the main feature of a PUF should be unclonability. This means that even with extensive knowledge of a PUF's design and behaviour, it should not be feasible to produce another PUF with the same behaviour (i.e. clone it).

3.2 Unilateral Authentication and Destructive Privacy

The first use of PUFs in the context of Vaudenay's model was the introduced in the paper from [34, 35]. In this paper, the PRF-based weak protocol from [38] was enhanced with a PUF to achieve destructive privacy in Vaudenay's model, which was an open problem until that moment. This is the first protocol to achieve this privacy level, as in [38] there was no protocol proposed for this level. The PUF was used in the tag as a secure key generator with tamper-evident behaviour.

3.3 Destructive Privacy with Mutual Authentication

In this section we make a step further to obtain the first RFID scheme that achieves destructive privacy and mutual authentication in Vaudenay's model [17]. The main idea is to start with the scheme in [34,35] and to extend it with one more step to achieve mutual authentication, as it was done in [31]. An alternative way of thinking about this scheme, is to consider that the PRF-based weak private scheme from [31] is enhanced with a PUF.

Each tag is equipped with a (unique) PUF P and has the capacity to compute the PRF F. A random number generator is also required on the tag. The reader maintains a database DB with entries for all legitimate tags. The protocol is started by the reader who sends a random number x to the tag. After receiving it, the tag generates a random y, computes $K = P(s)$ and $z = F_K(0, x, y)$, and answers with (y, z). The reader checks its database for a pair (ID, K) such that $z = F_K(0, x, y)$. If such a pair is found, it outputs ID; otherwise, outputs $\perp$ and randomly chooses a key K No matter of the two cases (K is found in the database or is randomly generated), the reader computes $w = F_K(1, x, y)$ and sends it to the tag. Upon receiving it, the tag computes $w' = F_K(1, x, y)$, where K is the one computed in the second step. Finally, it outputs OK or $\perp$ depending on the equality $w = w'$.

Chapter 4

Destructive Privacy with Temporary State Disclosure

4.1 Mutual Authentication Impossibility

The corruption capability is fundamental in all RFID security and privacy models. In this regard, the $Corrupt$ oracle is designed in a specific manner in each model. In Vaudenay's model, $Corrupt$ gives rise to the model's privacy granularity and its main privacy classes. Originally, the definition of $Corrupt$ stated that it returns the internal state of a tag, which is stored in the tag's memory. This was only specified later, in [30]. However, a tag's memory could be classified into persistent and temporary. The *persistent memory* stores data in non-volatile physical memory that persists between tag power-on sessions. The *temporary memory* is used to store data in volatile physical memory. The data stored in this memory is part of the tag computations and does not persist once the tag is powered off. We may refer to the persistent data as the non-volatile or persistent state and to the temporary data as the volatile state.

Let us consider two cases for the $Corrupt$ oracle:

1. Corruption returns only the persistent state of the tag;

2. Corruption returns both the persistent and temporary state of the tag;

4.2 Corruption with Temporary State Disclosure

The temporary memory of a tag can be viewed as a set of *volatile/temporary variables* used to store and perform the computations required by the authentication protocol. We distinguish between two types of temporary variables:

- *local* - temporary variables used by tags to perform computations only in a given protocol step;

- *global* - temporary variables that store values from a given protocol step and are used in another protocol step. These variables have, therefore, a longer lifetime than local temporary variables.

4.3 Attacks against Destructive Privacy

In the search for the stronger destructive privacy from Vaudenay's model with temporary state disclosure, a number of protocols have been proposed [1, 24]. These protocols use PUFs and rely on a technique called the *double PUF evaluation* in order to overcome the impossibility result from [2]. This was developed to mitigate a practical attack called the *cold boot attack* for PUFs [25]. This attack provides a method to freeze the tag's state and recover the PUF value (if it was just computed). When formalised in Vaudenay's model, this attack falls in the category of corruption with temporary state disclosure. The essence of this technique consists of evaluating the same PUF twice at different computation steps. If the attack is applied immediately after the first PUF evaluation, the value of the second PUF evaluation will not be obtained, and vice-versa.

Although, the double PUF evaluation technique suggests that the authors considered a stronger adversary for the protocols, we will analyse them in a scenario where the adversary cannot obtain PUF values unless they are stored as global temporary variables, and show that they display privacy vulnerabilities.

4.4 The PUF Protection Solution

Temporary variables cannot be protected by keyless cryptographic primitives or keyed cryptographic primitives with the key stored in clear on the tag. This is because Theorem 1 from [2] will also apply (at least for RFID schemes that do not contain PUFs). As a consequence, if keyed cryptographic primitives are used to protect temporary variables, then the key must be protected as well. The protection should not be of a cryptographic nature but rather of a physical one.

In such a context, PUFs seem to be an excellent candidate. In its present form, Theorem 1 from [2] cannot generally be applied to PUF-tags because corruption destroys the tag and the PUF value cannot be recovered (assuming that PUF values are not stored in the internal memory of tags). Following this observation we arrive at the idea of protecting temporary variables by PUFs. This can be done as follows. Given a tag T_{ID} and a temporary variable v from the tag computations, we endow the tag with a dedicated PUF P and a seed s_v (if the tag has already a PUF, then we only add a randomly chosen dedicated seed s_v). Then, to protect v we may encrypt its value by a keyed cryptographic primitive with the key $P(s_v)$.

Chapter 5

Reader First Authentication

5.1 Authentication Order in RFID

The design of RFID schemes with mutual authentication can the thought of in two distinct approaches: *tag-first* and *reader-first* authentication [33].

The reader-first authentication [33] requires that the reader is the first one to authenticate to the tag. The main benefit of this approach can be considered the limitation in attack surface for an attacker. In this way the tag will release sensitive information only after it is confident of the reader's identity. As a consequence, it is only in the presence of a valid reader that the adversary can obtain tag messages meant for authentication. Another interesting use-case for the reader-first approach is in schemes where the tag is designed only for a limited number of authentications since it prevents a form of the denial of service attack that would "consume" all the tag's authentication answers (sometimes called coupons [33]). With this approach comes also a challenge, the reader needs to authenticate itself to an unknown tag. Therefore one must design a method so that the reader can first identify and then authenticate the tag.

We are interested in an alternative design for obtaining privacy in Vaudenay's model with TSD that is more efficient than the PUF protection solution from Chapter 4.4. The straightforward solution is to avoid the use of temporary variables on the in RFID schemes. We consider that the reader-first approach accomplishes this in a natural and efficient way that eliminates temporary variables.

5.2 Destructive Privacy using PUFs and PRFs

In this section we address the problem of constructing a mutual authentication RFID scheme that achieves destructive privacy in Vaudenay's model with temporary state disclosure. The scheme [39, 40] is based on a PRF and it is more efficient than schemes that were enhanced using PUF-protection. The main design goal of this scheme is to completely avoid the use of global temporary variables (recall Section 4.2) that carry information from one step of the protocol to another, instead of protecting them through encryption. The scheme is designed following the reader-first approach. Each tag will be endowed with a PUF and a random number generator. The main cryptographic primitive used in the scheme is a PRF.

5.3 Destructive Privacy with Constant Time Identification

The PKE-based RFID scheme proposed in [31] achieves forward privacy and mutual authentication. Moreover, it allows constant-time identification of tags in the reader's database. This is because the reader has a public key that is distributed to all tags, with the private key being kept secret. Therefore, each tag can safely send its identity encrypted by the reader's public key.

However, this approach has an important drawback as it cannot be implemented in practice: the size of PKE implementation does not fit on most RFID chips. In order to obtain the same advantages in a more efficient scheme one would need to design it using symmetric primitives such as SKE schemes. This idea cannot be put into practice only by SKE because the secret key is used for both encryption and decryption. Sharing the secret key to all tags and the reader raises serious security and privacy problems: corruption of a tag reveals the secret key and the entire system is compromised. The solution to this problem is again the use of PUFs: if the secret key is protected by PUFs, then it will act as a master key known only to tags and reader. Trying to extract the key from the tags by corruption destroys the tags without disclosing the key.

The first attempt to design a destructive private and mutual authentication RFID scheme by using PUF protected secret keys was proposed in [1]. Unfortunately, the scheme in [1] does not achieve destructive privacy in Vaudenay's model with temporary state disclosure. This is because the scheme uses temporary variables to carry crucial information from one protocol step to another, and this information can be obtained by corruption.

However, combining the idea in [1] of using PUF protected secret keys with the reader-first design approach to avoid the use of temporary variables, leads to an RFID scheme that achieves destructive privacy and mutual authentication in Vaudenay's model with temporary state disclosure, together with constant-time identification of tags in the back-end database.

Chapter 6

Randomized Privacy

6.1 General Description

Increasing the applicability of RFID technology in large-scale systems requires efficient identification and authentication of RFID tags. This led to the proposal of various RFID schemes with identification time varying from constant to linear. Clearly, getting a better identification time is done at a certain price, and most of the times with a sacrifice of privacy. Finding a good balance between the tag identification time and the privacy level, is very important. To achieve this, constant tag identifier protocols must benefit from the same security and privacy analysis as other types of RFID protocols.

The goal of this section is to introduce a class of RFID schemes that allows a reasonable identification time with a reasonable loss of privacy. This is the class of *stateful RFID schemes with constant tag identifiers* [19]. In these schemes, the first message sent by the tag has a constant part (tag identifier) that allows the reader to efficiently identify the tag in its database. A tag identifier should not necessarily be thought of as the tag's identity or some fixed message. It may change after the identification process (but not before).

6.2 Impossibility Result

In stateful RFID schemes with constant tag identifiers the tag updates its permanent state after it is identified or authenticated by the reader. This delay in updating the tag's state can be exploited by an adversary especially to trace tags. The adversary can open a protocol session with the tag, obtain the tag identifier, and then close the session without allowing the tag to update its state. Having obtained the tag identifier, the adversary can open a new protocol session to trace the tag until it has a successful authentication with the reader. Therefore, this class of RFID schemes loses privacy in Vaudenay's model.

6.3 Model Extension

The analysis of the stateful RFID schemes with constant tag identifiers proposed so far has been made either informally, as in the case of [10] , or in restricted models, as in the case of the Refresh model [26]. Thus, it is impossible to compare such schemes in terms of privacy. It becomes then imperative to have a unitary privacy model for stateful schemes with constant tag identifiers. As Vaudenay's model is, arguably, the most general and widely used privacy model for RFID systems, it is natural to try to adapt it to this class of protocols [19]. What we have to do is to check the privacy of stateful schemes with constant tag identifiers against a limited class of adversaries, namely against adversaries that can draw a tag at most once in between two complete protocol sessions. This is because we already know that stateful schemes with constant tag identifiers are not even weak private in Vaudenay's model if the adversary draws a tag more than once in between two complete executions of the protocol.

Perhaps the simplest way to use Vaudenay's model with a restricted class of adversaries as mentioned above is to modify one of the oracles $DrawTag$ or $Free$: when a tag is drawn or freed, respectively, its state is randomized by at least one complete protocol session. The Refresh model implements a randomization similar to the first type: the challenge tags are randomized first and then are made available to the adversary. The HPVP model [15] suggests a randomization of the second type in order to deal with stateful RFID schemes (please see Section IV(C) in [15]).

Whether we modify the oracle $DrawTag$ or $Free$ as discussed above, such a change captures the idea that Vaudenay's model is restricted to consider privacy only against adversaries that can draw a tag at most once in between two complete protocol sessions. However, to be in line with the approaches in [15, 21], we prefer to change the oracle $Free$. Therefore, let us proceed now to the detailed description of the new oracle $Free$.

6.4 Destructive Privacy in rVM

In this section we design an RFID scheme with constant tag identifiers that provides mutual authentication and destructive privacy in the randomized Vaudenay model. The scheme is designed following the reader-first approach.

Each tag is equipped with an ideal PUF and a PRF. Instead of using a random number generator, the tag will share with the reader a state chosen uniformly at random. When presented with a challenge from the reader, the tag will evaluate the PUF to obtain the tag key, and then will apply the PRF to the state and the reader challenge. The reader has to maintain a database with two versions of the tag state because a desynchronisation of at most one step can occur between the reader and the tag. The first stage in the protocol is used as an identification so the reader can find the right pair of state and key that matches the tag answer. When the reader finds the right value, it will resynchronise with the tag and it will compute the answer that authenticates it to the tag. If the reader does not update the tag state (because it rejects the tag), then it will do so in the second step of the next protocol session (with the same tag). Therefore, the desynchronisation between the reader and tag can be at most one step.

Chapter 7

Offline Destructive Privacy

7.1 Offline RFID Schemes

The RFID schemes described in Section **??**, which we will call online schemes from now on, are composed of a reader, multiple tags, and a central server that provides the database of the system. In order to focus on the protocol between the reader and the tag, the communication between the server and the reader is assumed to be secure. Furthermore, this communication can never fail. In such conditions it is natural to consider the server and the reader as a single entity (e.g. the reader from Vaudenay's model).

However, this setup is not adequate for applications that require multiple readers that can function disconnected from the database. Applications that fit this descriptions are access control systems where many individual rooms are equipped with electronic locks [11], sporting events or public transportation [4]. For example, bus readers connect to the central database only at the end of the day. Thus, it is natural to consider the privacy implications of the attacker compromising a reader, and to analyse security and privacy in these circumstances. Offline RFID schemes represent an extension of online schemes (i.e. an online system is an offline system with a single reader that is always connected to the database). In offline RFID schemes we assume that the reader is connected to the central database only at certain moments. Since most or all of the reader's activity must be conducted without access to the server, the reader must accommodate a partial (or full) database with tag information.

7.2 Model Modifications

Vaudenay's model has been constructed for analysing online RFID schemes. In this paper we propose to extend Vaudenay model for offline RFID schemes with modifications inspired from [24] and [15]. The essence of the transformation is to grant the adversary the ability to create multiple readers and to corrupt readers. Corruption will be modelled similar with destructive privacy: after a reader is corrupted it is considered destroyed. However, we will restrict these abilities to a special privacy experiment and we will continue to analyse the scheme with the security and privacy experiments defined in Chapter 2. That is, we will model the offline analysis as an additional analysis to the security and privacy. In this chapter we will perform all analyses under corruption without temporary state disclosure.

7.3 Offline Destructive Privacy

In this section we build upon the efforts of [12, 24] and upon the protocol from Section 3.3, and we propose an RFID scheme that offers offline privacy, mutual authentication, and destructive privacy. The main idea of the scheme is to design a mechanism that allows each tag to store a single key, shared only with the central server, and to derive reader specific keys based on this key and the reader identity. In this manner the tag does not need to be updated in order to support additional readers or to recover privacy. In order to protect the information stored on the reader, we encrypt each reader-tag key with a specific key. For the protection of this key we make use of PUFs.

Chapter 8

Conclusions

The research for this thesis has been concentrated on the study of privacy in Vaudenay's RFID model, more specifically on achieving destructive privacy. Vaudenay's model is one of the first security and privacy models and can be considered to be the most mature model. To better understand the need for privacy in RFID systems we have performed an introduction into RFID domain from both a technological and a cryptographic perspective. We have also taken a look into the PUF technology, which has been proven to be an essential building block for achieving destructive privacy in Vaudenay's model. The tamper-evident nature of the PUF, modelled under the form of the ideal PUF hardware primitive, is highly suited to the destructive privacy definition.

Privacy has been marked as a major impediment to RFID progress more than a decade ago. Since then, the research community has gotten a better understanding of this field and new promising technologies have emerged (PUFs, lightweight cryptographic primitives) that can bring privacy closer to practice. This thesis has provided a deeper comprehension of privacy, as it is modelled in Vaudenay's model, by studying the implications of corruption with temporary state disclosure, by extending Vaudenay's model to other classes of schemes, and by constructing RFID schemes with detailed proofs. However, privacy still continues to be a challenge and a central topic for RFID systems.

Bibliography

[1] Mete Akgün and M. Ufuk Çaglayan. Providing destructive privacy and scalability in RFID systems using PUFs. *Ad Hoc Netw.*, 32(C):32–42, September 2015.

[2] Frederik Armknecht, Ahmad-Reza Sadeghi, Alessandra Scafuro, Ivan Visconti, and Christian Wachsmann. In Marina L. Gavrilova, C. J. Kenneth Tan, and Edward David Moreno, editors, *Transactions on Computational Science XI*, chapter Impossibility Results for RFID Privacy Notions, pages 39–63. Springer-Verlag, Berlin, Heidelberg, 2010.

[3] Gildas Avoine, Iwen Coisel, and Tania Martin. A privacy-restoring mechanism for offline rfid systems. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, pages 63–74, 2012.

[4] Gildas Avoine, Cédric Lauradoux, and Tania Martin. When compromised readers meet rfid. In *International Workshop on Information Security Applications*, pages 36–50. Springer, 2009.

[5] Jens-Matthias Bohli and Andreas Pashalidis. Relations among privacy notions. *ACM Trans. Inf. Syst. Secur.*, 14(1):4:1–4:24, June 2011.

[6] Christoph Böhm and Maximilian Hofer. *Physical unclonable functions in theory and practice*. Springer Science & Business Media, 2012.

[7] Sébastien Canard, Iwen Coisel, Jonathan Etrog, and Marc Girault. Privacy-preserving RFID systems: Model and constructions. https://eprint.iacr.org/2010/405.pdf, 2010.

[8] Ferucio Laurenţiu Ţiplea and Cristian Hristea. Privacy and reader-first authentication in Vaudenay's RFID model with temporary state disclosure. Cryptology ePrint Archive, Report 2019/113, 2019. https://eprint.iacr.org/2019/113.

[9] Robert H. Deng, Yingjiu Li, Moti Yung, and Yunlei Zhao. A new framework for RFID privacy. In *Proceedings of the 15th European Conference on Research in Computer Security*, ESORICS'10, pages 1–18, Berlin, Heidelberg, 2010. Springer-Verlag.

[10] Tassos Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, SECURECOMM '05, pages 59–66, Washington, DC, USA, 2005. IEEE Computer Society.

[11] Klaus Finkenzeller. *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John wiley & sons, 2010.

[12] Flavio D Garcia and Peter Van Rossum. Modeling privacy for off-line rfid systems. In *International Conference on Smart Card Research and Advanced Applications*, pages 194–208. Springer, 2010.

[13] Blaise Gassend, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. Silicon physical random functions. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 148–160, 2002.

[14] Jens Hermans, Frederik Pashalidis, Andreasand Vercauteren, and Bart Preneel. A new RFID privacy model. In Vijay Atluri and Claudia Diaz, editors, *Computer Security – ESORICS 2011*, pages 568–587, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[15] Jens Hermans, Roel Peeters, and Bart Preneel. Proper RFID privacy: Model and protocols. *IEEE Transactions on Mobile Computing*, 13(12):2888–2902, Dec 2014.

[16] Cristian Hristea. Reliable RFID Offline Privacy. In *Innovative Security Solutions for Information Technology and Communications: 13th International Conference, SecITC*

2020, Bucharest, Romania, November 19–20, 2020, Revised Selected Papers 13, pages 212–226. Springer International Publishing, 2021.

[17] Cristian Hristea and Ferucio Laurenţiu Ţiplea. Destructive privacy and mutual authentication in Vaudenay's RFID model. Cryptology ePrint Archive, Report 2019/073, 2019. https://eprint.iacr.org/2019/073.

[18] Cristian Hristea and Ferucio Laurenţiu Ţiplea. Destructive privacy and mutual authentication in Vaudenay's RFID model. Cryptology ePrint Archive, Report 2019/073, 2019. https://eprint.iacr.org/2019/073.

[19] Cristian Hristea and Ferucio Laurenţiu Ţiplea. Privacy of stateful RFID systems with constant tag identifiers. *IEEE Transactions on Information Forensics and Security*, 15:1920–1934, 2019.

[20] Cristian Hristea and Ferucio Laurentiu Tiplea. Privacy of stateful rfid systems with constant tag identifiers. *Cryptology ePrint Archive*, 2019.

[21] Cristian Hristea and Ferucio LaurenŢiu Ţiplea. A PUF-based destructive private mutual authentication RFID protocol. In Jean-Louis Lanet and Cristian Toma, editors, *Innovative Security Solutions for Information Technology and Communications*, pages 331–343, Cham, 2019. Springer International Publishing.

[22] Ari Juels and Stephen A Weis. Authenticating pervasive devices with human protocols. In *Annual international cryptology conference*, pages 293–308. Springer, 2005.

[23] Ari Juels and Stephen A. Weis. Defining strong privacy for RFID. *ACM Trans. Inf. Syst. Secur.*, 13(1):7:1–7:23, November 2009.

[24] Süleyman Kardaş, Serkan Çelik, Muhammet Yildiz, and Albert Levi. PUF-enhanced offline RFID security and privacy. *J. Netw. Comput. Appl.*, 35(6):2059–2067, November 2012.

[25] Süleyman Kardaş, Mehmet Sabir Kiraz, Muhammed Ali Bingöl, and Hüseyin Demirci. A novel RFID distance bounding protocol based on physically unclonable functions. In

Ari Juels and Christof Paar, editors, *RFID. Security and Privacy*, pages 78–93, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[26] Li Lu, Yunhao Liu, and Xiang-Yang Li. Refresh: Weak privacy model for RFID systems. In *Proceedings of the 29th Conference on Information Communications*, INFOCOM'10, pages 704–712, Piscataway, NJ, USA, 2010. IEEE Press.

[27] Roel Maes. *Physically Unclonable Functions: Constructions, Properties and Applications*. Springer Verlag, 2013.

[28] Roel Maes and Ingrid Verbauwhede. Physically unclonable functions: A study on the state of the art and future research directions. *Towards Hardware-Intrinsic Security: Foundations and Practice*, pages 3–37, 2010.

[29] Tania Martin. *Privacy in RFID systems*. PhD thesis, Ph. D. Thesis. Universite catholique de Louvain, Belgium, 2013.

[30] Khaled Ouafi and Serge Vaudenay. Strong privacy for rfid systems from plaintext-aware encryption. In Josef Pieprzyk, Ahmad-Reza Sadeghi, and Mark Manulis, editors, *Cryptology and Network Security*, pages 247–262, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[31] Radu-Ioan Paise and Serge Vaudenay. Mutual authentication in RFID: Security and privacy. In *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security*, ASIACCS '08, pages 292–299, New York, NY, USA, 2008. ACM.

[32] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. Physical one-way functions. *Science*, 297(5589):2026–2030, 2002.

[33] Roel Peeters, Jens Hermans, and Junfeng Fan. IBIHOP: Proper privacy preserving mutual RFID authentication. In Changshe Ma and Jian Weng, editors, *The 2013 Workshop on Radio Frequency Identification/Internet of Things Security (RFIDsec'13 Asia)*, volume 11 of *Cryptology and Information Security Series*. IOS Press, 2013.

[34] Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. *Enhancing RFID Security and Privacy by Physically Unclonable Functions*, pages 281–305. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[35] Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. PUF-enhanced RFID security and privacy. In *Workshop on secure component and system identification (SECSI)*, volume 110, 2010.

[36] Ferucio Laurenţiu Ţiplea and Cristian Hristea. PUF protected variables: a solution to RFID security and privacy under corruption with temporary state disclosure. *IEEE Transactions on Information Forensics and Security*, 16:999–1013, 2020.

[37] Ferucio Laurentiu Tiplea and Cristian Hristea. Practically Efficient RFID Scheme with Constant-time Identification. In *SECRYPT*, pages 495–506, 2021.

[38] Serge Vaudenay. On privacy models for RFID. In *Proceedings of the Advances in Crypotology 13th International Conference on Theory and Application of Cryptology and Information Security*, ASIACRYPT'07, pages 68–87, Berlin, Heidelberg, 2007. Springer-Verlag.

[39] Ferucio Laurențiu Țiplea, Cristian Hristea, and Rodica Bulai. Privacy and reader-first authentication in Vaudenay's RFID model with temporary state disclosure. *Computer Science Journal of Moldova*, 90(3):335–359, 2022.

[40] Ferucio Laurențiu Țiplea, Cristian Hristea, and Rodica Bulai. Privacy and mutual authentication under temporary state disclosure in RFID Systems. In *Electronics, Communications and Computing*, pages 119–124, 2023.