SECURITY ANALYSIS OF LIGHTWEIGHT SCHEMES FOR RFID SYSTEMS

Mohammad Reza Sohizadeh Abyaneh

DISSERTATION FOR
THE DEGREE OF PHILOSOPHIAE DOCTOR

THE SELMER CENTER
DEPARTMENT OF INFORMATICS
UNIVERSITY OF BERGEN
NORWAY

JUNE 2012

ABSTRACT

This thesis mainly examines the security analysis of lightweight protocols proposed for providing security and privacy for RFID systems. To achieve this goal, first we give a brief introduction of RFID systems. The introduction includes: the history, system components, applications, standards and related issues of RFID systems. The main issues which are highlighted in the thesis are *security* and *privacy*. One possible solution to provide RFID systems with privacy and security is using cryptography. But conventional cryptography is too big for the highly constrained devices such as RFIDs. The alternative solution is using *lightweight cryptography* which aims at squeezing the cryptographic schemes into the RFID tags. A brief overview of the thesis is illustrated in Figure 1.

This thesis consists of a categorization of the lightweight proposals and related works in the literature. Finally, we try to explain how the security of a lightweight scheme can be analyzed and evaluated. To do so, the security requirements, adversarial models and potential attacks for lightweight schemes are presented. In this part, we mainly focus on the security analysis of the lightweight protocols because the security analysis of the lightweight primitives and algorithms is more or less the same as conventional primitives and has already been widely discussed in the literature.

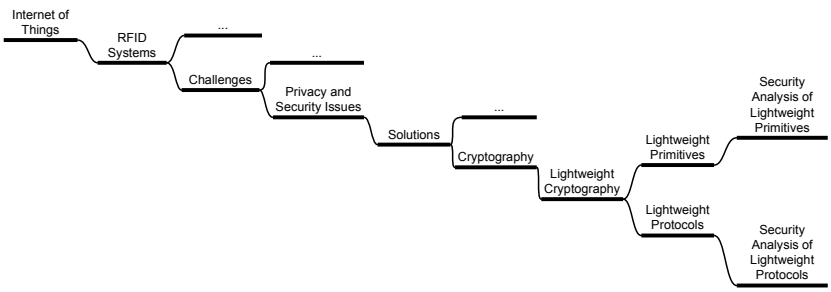

Fig. 1: *Overview of the thesis.*

ACKNOWLEDGEMENTS

First and foremost, I want to thank my supervisors, Professor Tor Hellesth for all his supports and trust, Professor Øyvind Ytrehus for his priceless advices and high standards which motivated me to work harder and also Dr. Alexandre Kholosho. I shall say that it has been an honor for me to be their Ph.D. student and I really appreciate all their contributions of time, ideas, and funding to make my Ph.D. I also would like to thank Professor Matthew Parker for taking the time and energy to organize my defense.

Then, I should thank the all members of the Selmer Center those who have already left the group and those who are still there. They have contributed immensely to my personal and professional time at university of Bergen. The group has been a source of friendship as well as good advices and collaborations. I am especially grateful for conversations with Seyyed Mehdi Mohammad Hassanzadeh, Mohammad Ravanbakhsh, and also Håvard Raddum.

For this dissertation I would like to thank my reading committee members: Gilas Avoine and Matthew Robshaw for their time, interest, and helpful comments.

My time in institute of Informatics at university of Bergen was a part of my life which I am grateful for spending time with my colleagues and the other staffs there. My special thanks for Ida Holen, for all her supports from the first day I came to Bergen.

Lastly, I would like to thank my family for all their love and encouragement, my parents who raised me with a love of science and supported me in all my pursuits. And most of all for my loving, supportive, encouraging, and patient wife Zahra whose faithful support during the final stages of this Ph.D. is so appreciated.

Thank you all.

Mohammad Reza Sohizadeh Abyaneh
University of Bergen
June 2012

CONTENTS

1 Introduction

1.1 Motivation

The advances in wireless and mobile technologies have paved the way for pervasive communication systems to be utilized in billions of terminals in commercial operations. And it is just the beginning for some new wireless technologies such as RFID with a deployment potential of tens of billions of tags and a virtually unlimited application potential. ITU reports predict a scenario of "Internet of things" in which billion of objects and items are able to report information about their location, identity, etc. through a wireless connections. Therefore, technologies which enable unique identification of objects are fundamental parts of Internet of things. This is where RFID technology emerges [6].

Radio frequency identification (RFID) is an automatic identification and data capture technology that uses radio frequency (RF) to identify objects. This can be achieved by three main components in RFID systems: RFID tags, RFID readers and a back-end system. RFID readers communicate with RFID tags via a wireless channel to identify them while the back-end system provides the readers the information required to accomplish the identification process.

Using RFID technology has enabled identifying objects in large scales automatically and in contact-less manner. Correspondingly, this technology is currently being deployed in an extensive variety of applications such as: automatic inventory, asset tracking, transportation payments, entry access control, and electronic passports. In addition, overwhelming increase of demand for automatic inventory and tracking applications draws a bright future for RFIDs.

Nevertheless, every coin has two sides. As mentioned earlier, an RFID reader and RFID tags communicate via a wireless channel. This communication and the messages exchanged in between may be susceptible to eavesdropping or interception. This is the point that some non-trivial concerns such as *security* and *privacy* arise. It is nowadays feasible to read the information of some RFID tags illegitimately and thus obtain some information about their owners. Tracking the tags is also feasible for some RFID tags. That is why RFID technology has not reached the expected wide range of deployments and there exist numerous controversies about the wide-scale deployment of it.

The above-mentioned concerns become more serious when dealing with the inexpensive (low-cost) RFIDs normally used for mass distribu-

tion. The major challenge in tackling to provide security for this kind of RFID tags is that they have very constrained capabilities (storage, circuitry and power consumption), which makes them unable to perform the most common security measures such as cryptography.

In order to find a concrete solution to this problem, a paradigm shift from conventional solutions is required. The schemes which are proposed as solution for providing *low-cost* RFIDs with security and privacy are called *lightweight schemes* in the literature.

A considerable volume of papers have been published so far on lightweight schemes. But the other side of the coin is how secure or privacy-preserving these schemes are. This can be achieved through *security analysis* of the schemes to ensure that they have not sacrificed the security of the scheme for the sake of being lightweight. This is the main subject of this thesis.

1.2 Organization

The remainder of this thesis is organized as follows. Section 2 gives an overview of the RFID systems. In Section 3, the main issues in the RFID systems, which are security and privacy are explored. Section 4 gives a classification of lightweight schemes in the literature and contains some related works of each kind. In Section 5, it is shown how to analyze the security of the lightweight schemes by explaining the models and requirements for the security. The thesis concludes by a brief introduction of our five papers in Section 6 and some future work in Section 7.

2 RFID Systems

2.1 System Components

In general, an RFID system consists of *tags*, *readers*, and a *back-end* system (database) (Fig.2). Typically, an RFID tag is attached to an object and an RFID reader communicates with the tag to identify the object to which the tag is attached. The tag carries information about the object for identification purposes. This information can be a serial number, model number, or other characteristics of the object to identify or distinguish the object. A copy of this information is stored in the back-end system which provides it to the readers on demand. In the

following subsections, the systems components are studied in more details.

2.1.1 RFID TAGS

An RFID tag is a tiny radio device that is also referred to as a *transponder*. It comprises two main parts which are common among all types of tags: *internal circuitry* attached to a small flat onboard *antenna*. However, some types like active tags have an extra part which is a battery.

The tags are attached to different objects and carry the information which can identify those objects. Then, this information can be read contact-lessly by readers. There are different sorts of tags available in the market. These differences between tags will be examined with respect to *power* sources, *frequencies*, *writing* capabilities and the *cost* [5].

- *Passive Tags :* Passive tags do not contain battery. Instead, they absorb their power from the radio wave transmitted by the reader. Passive tags transmit data by reflecting power from the reader. This is also referred to as *backscatter modulation* for systems that operate in the far-field, and *load modulation* for systems that operate in the near-field [2]. The received power is used for two purposes: powering the internal circuitry on the tag and communication through the onboard antenna for responding to the reader interrogations.

  It should be noted that many RFID experts believe that passive tags are the future of RFID and this can be achieved when the cost of individual tags reaches less then five cents [5].

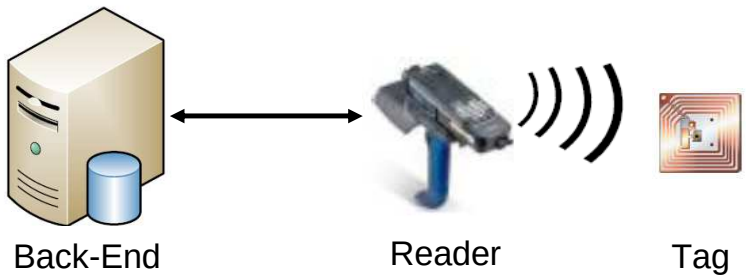

Fig. 2: *RFID system components.*

- *Active Tags*: As their name suggests, active tags include an onboard power source as a battery which provides power for both internal circuitry and the antenna. This imposes additional expenses on manufacturers and correspondingly makes the active tags more expensive than the passive ones. However, the range of active tags is generally far more (Table 1).

- *Semi-Active Tags:* Semi-Active tags are manufactured to retain the advantages while eliminating the disadvantages of passive and active tags. Semi-active tags typically use an internal battery to power internal circuitry. However, the battery power is not used for communication via the antenna. The power for communication is received from the reader as in the passive tags. In this way some battery power can be saved for a longer period of time and correspondingly makes this type of tag more cost-effective comparing to the active tags.

Tags primarily operate at three ranges of frequencies: low frequency (LF), high frequency (HF) or ultra-high-frequency (UHF). Nevertheless, there are some active tags for specialized applications may utilize microwave frequencies as well [14]:

- *Low-Frequency Tags:* This type of tags operate at the frequency of 125/134 KHz and are most commonly used for access control, animal tracking, and asset tracking.

- *High-Frequency Tags:* This type of tags operate at the frequency of 13.56 MHz. At this frequency the interference caused by metals or water is eliminated. The range of communication in HF tags is generally confined to some inches. Thus, HF tags are primarily suitable for inventory or smart card applications where the tagged items are in close proximity to the reader.

- *Ultra High-Frequency Tags:* This type of tags operate at the frequency range of either 850-950 MHz or 2400-2500 MHz. So, they can offer up to about 3 meters communication range at a high speed. The range of UHF tags makes them more applicable to shipping dock type applications.

RFID tags are made of two different types of chips, regarding their writing capabilities: read-only chips and read-write chips [14]:

Specifications	Low-cost RFID Tag	High-cost RFID Tag
Power Source	Passive	Active
Storage	32 - 1K bits	32 KB - 70 KB
Security Capabilities	250 - 4K gates	3DES,SHA-1,RSA
Reading Distance	Up to 3 m	About 10 cm
Price	0.05-0.1 euro	Several euros

Table 1: *Specifications for Low-cost and High-cost RFID Tags [9].*

- *Read-only Tags*: As their name suggests, read-only tags contain some unique information which is stored during the manufacturing process and can not be changed.
- *Read-Write Tags*: The user can either read or write information to a read-write tag when the tag is within range of the reader. Read-Write tags are naturally more expensive that read-only ones.

RFID tags are divided into two categories regarding their price: *low-cost* and *high-cost* RFID tags (Table 1).

- *High-cost tags*: High-cost tags are mostly active tags with more computational and storage capabilities compared to passive ones. While the communication range of the active tags are less.
- *Low-cost tags*: The low-cost tags are mostly passive and their computational and storage capabilities are highly constrained.

A comparison of the specifications in these two types of tags are illustrated in Table 1 [9].

2.1.2 RFID Readers

An RFID reader, also known as an *interrogator* or *transceivers*, is a device that can read and/or write data to an RFID tag. The data is exchanged between a reader and a tag via their antennas by electromagnetic RF waves. In addition to data, the waves transmitted from readers are also the source of power for the passive tags. Readers are generally of two types: simple *scanner* and *complex*(smart) reader.

Simple scanners may be handheld or mounted to mobile equipment such as a forklift. This makes them useful for the situations where

the reader is mobile and moves toward the objects with tags. On the other hand, scanners are mostly used where data verification in the interrogation is also required. Therefore, the rate of data communication by scanners is relatively low. An application that is well suited to scanners is order fulfillment [5].

In more complex or rapidly moving readers, the electromagnetic signal is transmitted by a smart reader.

2.1.3 Back-End System

The data acquired by the readers in tag interrogations is usually passed to a back-end system (e.g. a host computer) to be processed into useful information. The host computer is a system with application specific software. The software can include RFID middleware to set up and control the reader and some type of database software to control the information received from the reader [5].

2.1.4 Communications

Communications in RFID systems can be categorized into two parts: communications between the reader and the tag and communication between the reader and the back-end.

- *Reader and Tags*: The communication between the reader and the tag takes place via an *asymmetric channel*. The *forward* (reader-to-tag) and *backward* (tag-to-reader) channel.

  For passive tags, the forward channel is much stronger than the backward channel because they not only receive data but also the power. As a result the forward channel may be intercepted from a far longer distance than the backward channel. For example, the forward channel of a passive tag operating at 915 MHz may be eavesdropped or intercepted at the range of almost 100 meters, while this range is less than 3 meters for the backward channel for the same tag.

  To make the communication of readers and tags more efficient coding and modulation are necessary. But the coding/modulation method should be chosen differently for forward and backward channels due to different specifications in the channels.

  Readers are able to transmit at greater power; however they suffer from bandwidth limitations in the forward channel. On the other

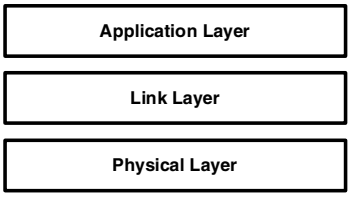

Fig. 3: *ISO/OSI reference model for tag and reader communication.*

hand, in the backward channel, tags can transmit messages only to a short range due to lack of power but the bandwidth limitation is not very strict.

Therefore, Manchester or NRZ (Non-Return-to-Zero) and PPM or PWM coding techniques are used in forward and backward channels respectively. For modulation there are three alternatives: Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK) and Phase Shift Keying (PSK) which are used depending on the application requirements [9].

The communication between tags and readers can be discussed on the basis of a simplified model of ISO/OSI *reference model* in which there are three different layers: *physical layer link layer*, and *application layer* [4] (Fig. 3). At the lowest layer, which is called the physical layer, the transmission over the physical medium, such as: used frequencies, modulation techniques, signal forming, etc., is defined. Above that layer the transmission of data frames is defined in the link layer. The layer which is placed at the top presents the algorithms for multiple accesses to the shared medium and protocol messages for reading and writing the memory of tags or authentication protocol. This layer is called application layer [4].

- *Reader and Back-end*: The communication between the reader and the back-end system is performed in a totally different way. The reader has the capability of communicating to the back-end via different types of communication protocols depending on the distance between the reader and the host, the required data transfer rate, and the system budget. Common types of protocols include RS-232, RS-485, and Ethernet-based systems [5].

2.2 HISTORY

Radio-Frequency Identification (RFID) technology is usually considered to be the next generation of barcode and will replace barcode systems in the very near future. The barcode is currently the most common type of automatic data capture (ADC) technology in use. The history of barcodes goes back to 1932 when Wallace Flint introduced a system which used punch cards to dispensed products to customers automatically. This was the first documented instance of the advantages of an automated checkout and bar codes. Forty years later, Flint, as the vice president of the National Association of Food Chains, played an important role as to support bar code standardization that led to the uniform product code (UPC) [5].

In the case of RFID technology, we can not say that it is a recent technology, although it has been recently become practical for business applications. It is difficult to trace its true history because most research was done behind closed doors for military purposes. But we can say that its history goes back to prior to World War II when Radar was discovered in 1935 by Sir Robert Alexander Watson Watt to identify friend or foe aircraft during the Second World War [13]. However, one of the first major scientific papers on RFID was "Communication by means of reflected power" written by Harry Stockman in 1948. Since then, plenty of research studies and patents have been published in this field. But major events in RFID commercial development can be traced to the 1975 declassification of research by Los Alamos Scientific Labs (LASL) with the published paper "Shortrange radio-telemetry for electronic identification using modulated backscatter" by Koelle et al [3].

In the 1980s, the RFID technology started to be widely deployed in the industry especially in transportation applications and personnel access in US and short-range systems for animal tracking and business applications in Europe. The first commercial toll application of RFID technology began to be used in Europe in 1987 and was soon followed in the United States. [3].

In early 1999, the Uniform Code Council, EAN International, Proctor & Gamble, and Gillette established the Auto-ID Center at the Massachusetts Institute of Technology (MIT). For the first time it was there where, David Brock and Sanjay Sarma, initiated the idea of integrating passive RFID tags in products in order to track items in the supply chain. They suggested the idea of using a unique number (serial number) on

the tags for identification. Data associated with the serial number on the tag would be stored in a back-end system which would be accessible over the Internet [13].

There was increased prominence for passive RFID tagging, as a result of the influence of one hundred or so large end-user companies, and led by the Auto-ID Centre, from 1999 to 2003 [5]. This work was then extended by the Auto-ID research lab to countries such as Australia, the United Kingdom, Switzerland, Japan, and China. In 2003 the tehnology was licensed to the Uniform Code Council (UCC), which created EPC Global, being a combined activity between EAN International and the Auto-ID Centre, and with an aim to commercialize the EPC technology. In 2003, the research activity of the Auto-ID Centre was transferred to Auto-ID labs, and GS1 EPC GLobal is now responsible for the standards associated with such for RFID technologies [13]. Up to now, two generations of standards have been ratified by be the organization for RFID tags.

Today, the industry support is evidenced in the fact that some of the biggest retailers in the world-Albertsons, Metro, Target, Tesco, Wal Mart-and the U.S. Department of Defense have initiated plans to use EPC technology to track goods in their supply chain. The pharmaceutical, tire, defense, and other industries are also moving to adopt the technology [13].

2.3 Applications

Initially, the deployment of RFID technology was confined to some simple applications like inventory and antitheft. However, it has been deployed in more sophisticated areas today, such as in electronic IDs and passports. A sample of applications is shown here [16]:

- *Automotive*: Car manufacturers mostly exploit the RFID technology as anti-theft immobilizers in their products to improve their security.

- *Animal Tracking*: This application of RFID technology is used for either tracking wild animals in scientific studies, or tracking pets when they are lost.

- *Asset Tracking*: Libraries use RFID technology on books to manage them in circulation more efficiently and limit theft. Airlines use

this technology to track the luggage or cargos for better management. These are just two examples of asset tracking applications of RFID technology.

- *Contact-less Payments*: Blue-chip companies such as American Express, ExxonMobil, and MasterCard use RFID technology on their products for contact-less payment.
- *Supply Chain*: Some retailers such as WalMart, Target, BestBuy use RFID technology to keep a record of their products, limit shoplifting, and reduce the check-out time of the costumers.

2.4 STANDARDS

The EPCGlobal and the ISO (International Standards Organization) are both leading figures in issuing standards for RFIDs.

2.4.1 EPCGLOBAL STANDARDS

The objective of EPCGlobal standards is identifying objects through a uniquely formatted number kept on each tag, with associated data stored in a back-end system. To achieve this goal, EPCglobal has introduced the Electronic Product Code (EPC) as a scheme designed for universal object identification.

EPC is a unique naming scheme for objects containing a header and three sets of data (Fig. 4). The header identifies the EPC's version number, allowing for different lengths or types of EPC later on. The second part of the EPC number identifies the EPC manager, most likely the manufacturer of the product. The third, called object class refers to the exact type of product and the fourth is the serial number unique to the item. In the EPCglobal standard, the RFID tags have been divided into five different classes which fulfill different industry's need. Class 0 is a read-only passive tag with 64 bit EPC. Class 1 refers to write-once read-many passive tags that carry unique ID, password-based access control, and a kill switch that can be used in deactivating the tag at a

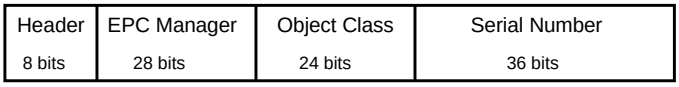

Fig. 4: *Example of an 96-bit EPCGlobal tag.*

point-of-sale. Class 2 extends Class 1 by allowing rewritable memory and authenticated access control. Class 3 refers to semi-active tags that carry an integral power source to supplement captured energy. Finally, Class 4 refers to active tags that enable tag-to-tag communication, more complex protocols, and ad hoc networking. It should be noted that the EPC size in all classes1–4 is 96 bits [1].

The current version of EPCglobal standard is known as UHF Generation 2 (UHF Gen 2) [115]. The EPC Class-1 Generation-2(C1G2) is now considered as the universal standard for low-cost passive RFID tags. Class-1 RFID tags belong to the category of low-cost tags mentioned in Section 2.1.1. Because of its very limited storage and computational capabilities, this class of tag cannot support conventional cryptographic primitives. So there is a lot of research into how to bolster the security level of such tags [6].

In the following the main specifications of EPC Class-1 Generation-2 RFID tag are listed [17]:

- C1G2 RFID tag is passive; it implies that it absorbs the power from readers.
- C1G2 RFID tag communicates at UHF band (800–960 MHz) with the communication range of 2-10m.
- C1G2 's privacy protection mechanism is to render the tag permanently unusable by using the *kill* command. To avoid illegitimate usage of this command a 32-bit *kill PIN* is also required.
- Read/Write to C1G2 RFID tag's memory is allowed only after receiving *access* command with a valid 32-bit *access PIN*.
- C1G2 RFID tag supports on-chip 16-bit Cyclic Redundancy Code (CRC) and 16-bit Pseudo-Random Number Generator (PRNG). The 16-bit PRNG has the following properties:
  - The probability that any 16-bit pseudo random value shows up as the next output is between 0.8×2^{-16} and 1.25×2^{-16}.
  - Among 10000 tags, the probability that any two or more tags generate the same sequence of 16-bit numbers is less than 10^{-3}.
  - The probability of predicting the next pseudo-random number from the previous outputs is less than 2.5×10^{-4}.

The CRC checksum is used to detect error in transmitted data and the corresponding CRC polynomial of degree 16 is [11]:

$$x^{16} + x^{12} + x^5 + 1$$

2.4.2 ISO STANDARDS

The ISO is very active in developing RFID standards for supply chain operations and is nearing completion on multiple standards to identify items and different types of logistics containers. Some examples of ISO Standards in this field are: ISO 14443 for "proximity" cards and ISO 15693 for "vicinity" cards both recommend 13.56 MHz. ISO 11748 / 11785 for standard for animal identification and ISO 17364 for transport units [4].

But the most important one of this kind are the ISO 18000 series which are a set of proposed RFID specifications for air interface communications of item management. The ISO 18000–6C of this series and EPC Class1 Generation2 are harmonized to reach a global standard, and are referred to as ISO 18000–6C.

2.5 CHALLENGES

Despite the incentives in RFID deployment, this technology is facing some non-trivial challenges which some of them are listed below [24]:

- *Large volumes of data*: Reading RFID tags data is currently possible at a very high speed of several times per second. Therefore, in a very short time a large amount of raw data is read by the readers and should be processed by the back-end system. The processing of these large volumes of data is a bottleneck for the system.

- *Product information maintenance*: When a high volume of RFID tags are processed by the back-end system, the readers must the continually retrieve some attributes of the tags from a back-end system which results in scalability challenges for large-scale implementations.

- *Configuration and management of readers and devices*: When a large number of readers and related hardware devices are utilized in multiple facilities, their configuration and management becomes challenging.

- *Data integration across multiple facilities*: When the facilities of an enterprise are geographically distributed, real time management of data on a central back-end system can place a significant burden on the network infrastructure.

- *Data ownership and partner data integration*: During each product's lifecycle its owner might vary several times. When the product is tagged, the owners of that product at each time must be given the associated data of the tag. This is where the challenge pertaining to the ownership and integration of the data emerge.

- *Data security and privacy*: The last but foremost challenge in the field of RFIDs is undoubtedly security and privacy challenges which could have a significant impact on the system. This challenge is investigated in details in the following section.

3 Privacy and Security Issues

There are two main issues in RFID systems which are highlighted in this thesis: *privacy* issues and *security* issues. These issues, although interrelated, are different. With respect to RFID, we define these issues as follows [15]:

- *Privacy*: the ability of the RFID system to keep the meaning of the information transmitted between the tag and the reader secure from non-intended recipients.

- *Security*: the ability of the RFID system to keep the information transmitted between the tag and the reader secure from non-intended recipients.

3.1 Privacy Issues

The major concern which thwarts widespread deployment of RFIDs is the possibility of privacy violation. This issue seems to be very difficult to tackle because it originates from the basic functions of RFID tags.

As mentioned, each RFID tag contains a unique ID which identifies it through an RF wireless interrogation. This results in high risk of identification or tracking of bearers by illegitimate entities unless sufficient protection is used.

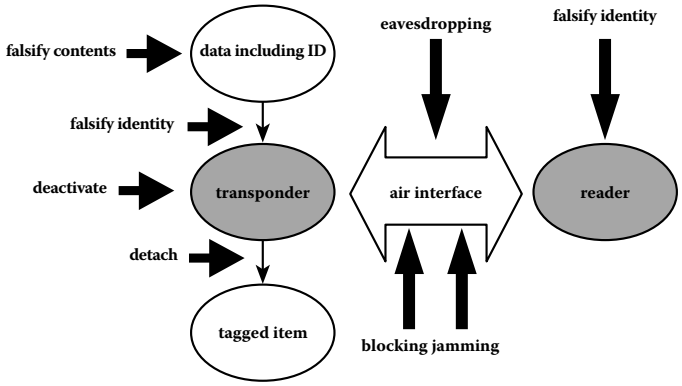

Fig. 5: *Security Issues in RFID systems [6].*

In general, violation of privacy has two forms: *information leakage* and *location tracking*. Information leakage includes obtaining the information from the tag to identify its owner, his preferences or physical condition. For example, if a person carries a bottle of medications with attached RFID tag, obtaining the information of the RFID tag may point to his disease [1]. As RFID tags can be attached to almost every item we use in everyday life, obtaining their information can reveal a vast amount of data about a person's life style and therefore violates his/her privacy.

This kind of information might be interesting for variety of entities e.g. marketers can obtain and use these leaked information to link buyers to specific items and make personal profiles in order to give them specialized sale offers.

On the other hand, even if the tag responses do not leak information about the product it has been attached to, static responses of the tags during interrogations helps with tracking the owners.

3.2 Security Issues

The security issues can exist in all RFID systems' components. In this subsection, we briefly explore some of the security issues related to the tags, readers and the communication between them. These issues are illustrated in Figure 5 regarding the part of system they are targeting [6].

3.2.1 Security Issues of the Tag

Some of the security issues for the tags are [7]:

- *Falsification of ID*: In this security issue, an attacker first obtains/steals the ID or other sensitive data of a tag and uses it to impersonate the tag and deceive the readers in further interrogations. This can be achieved by using an emulator tag or copying the obtained information on another tag (cloning or counterfeiting).

- *Unauthorized deactivation*: Each RFID tag based on EPC C1G2 has a mechanism for deactivation using *kill* command. Unauthorized usage of this command can render the tag unusable in further interrogations and deactivate the tag permanently.

- *Physical destruction*: Tags can be physically destroyed in different ways, for example by using strong electromagnetic fields (e.g. a microwave oven) or by some chemical substances. In the case of active tags, they could also be rendered unusable by removing their battery.

- *Detaching the tag*: A tag can be separated from the tagged item. The detached tag may even subsequently be attached to a different item. This type of attack poses a fundamental security problem because RFID systems are completely dependent on the unambiguous identification of the tags.

- *Falsification of Contents*: If the tags contain some extra data except from ID and security information, the data can be falsified by unauthorized write access to the tag while the ID (serial number) and any other security information (e.g. keys) remain unchanged. In this way, the readers continue to recognize the identity of the tags correctly while their contents have been changed.

3.2.2 Security Issues of the Reader

Readers are also susceptible to falsifying ID attack. In a secure RFID system, the reader must prove its authorization to the tag. If an attacker wants to read the data with his own reader, this reader must fake the identity of an authorized reader. If an attacker accomplishes to falsify the reader's ID, she will be able not only to have access to the tag's information but also to the back-end system.

3.2.3 Security Issues of the Communications

The communications between the components of RFID systems also suffer from security issues. Nevertheless, the level of vulnerability significantly differs from communication between the tag and the reader to communication between the reader and back-end system. While the latter is considered robust and almost secure due to application of standard security measures such as SSL or TLS, the former is the most vulnerable part of the whole system. Some of the security issues in the communication between the tag and the reader are listed below [7].

- *Eavesdropping*: The communication between reader and tags via the air interface can be monitored by intercepting and decoding the radio signals. This is one of the most specific threats to RFID systems. The eavesdropped information could for example be used to collect sensitive information about a person. It could also be used to perform a replay attack.

- *Replay Attack*: The attacker can obtain and save all the exchanged messages between a tag and a reader and either simulate the tag or the reader towards one another.

- *Jamming*: The air interface between reader and tag can be disturbed in order to attack the integrity or the availability (Dos attack) of the communication. This could be achieved by powerful transmitters at a large distance, but also through more passive means such as shielding.

- *Man-in-the-middle*: A man-in-the-middle attack is a form of attack in which the adversary provokes or manipulates the communication between the reader and the tag, where manipulating the communication means relay, withhold, or insert messages.

- *Relay attack*: A relay attack [21] is similar to the well known man-in-the-middle attack. A device is placed in between the reader and the tag such that all communication between reader and tag goes through this device, while both tag and reader think they communicate directly to each other. In the case of payment systems, the attacker is able to charge some one else's payment device (e.g. a smart card with an RFID tag) to buy something for herself.

3.3 SOLUTIONS

Proposed solutions to security and privacy issues in RFID systems include defensive measures that could be taken in two levels: *technical* and *management* levels. To have a concrete solution for RFID system, it requires having a holistic perspective to the problem and adopting a combination of measures in both levels. In the management level, it is required to:

- have an up-to-date *risk assessment* of the whole system to be aware of the possible threats and vulnerabilities in the system.
- establish policies for the security of the data to tackle the risks.
- incorporate security solutions that are transparent.
- realize that security is an ongoing process.

There are quite a few related works in this layer in the literature such as [25] as well as some guidelines and recommendations [26, 27]. One of the first and best known proposals in this context is "RFID Bill of Rights" [18] which proposes five privacy addressed articles for RFID systems: (1) The right to know whether products contain RFID tags, (2) the right to have tags removed or deactivate upon purchase of these products, (3) the right to use RFID-enabled services without RFID tags (i.e. right to opt out without penalty), (4) the right to access an RFID tag's stored data along with the possibility to correct and amend that data, and finally (5) the right to know when, where, and why the tags are being read [4].

In addition, there are plenty of proposals in the technical level which can be categorized in four following groups [3]:

- *Tag Killing Command or Permanent Deactivation*: Using the kill command in RFID tags in an authorized manner (e.g. after shopping the tagged item) makes the tag permanently deactivated and thus renders any subsequent unauthorized reading impossible. It should be noted that although killing tags effectively enforces consumer privacy, it eliminates all of the post-purchase benefits of RFID for the customer [20].
- *A Faraday Cage or Jamming Approach*: Faraday Cage is a metal or foil-lined container that is impenetrable to radio frequency waves. By putting RFID tags inside a Faraday Cage, they can be

made protected from reading by isolating them from any kind of electromagnetic waves.
The reading of RFID tags may also be jammed by devices that emit powerful and disruptive radio signals. But usually such jamming devices violate government regulations on radio emissions [23].

- *Use of Blocker Tags*: A blocker tag is a special RFID tag that prevents unwanted scanning of tags. This idea is first introduced by Juels, Rivest, and Szydlo in [19] to protect privacy.

- *Cryptography*: To achieve privacy in RFID systems, a typical solution can be the adoption of cryptographic techniques. Nevertheless, this can not be achieved through conventional cryptography due to special limitations of passive low-cost RFID tags. In the following section, we will discuss the paradigm shift which took place in cryptography to fulfill these limitations and led to coin the term *lightweight cryptography* in the literature.

4 Lightweight Cryptography for RFIDs

In order to provide security and privacy for low-cost RFID tags which have limitations in terms of memory and power, we must overcome the barrier of adapting the current computationally intensive operations of security countermeasures (e.g. conventional cryptography) to these limitations at an acceptable speed without compromising on security. This is where the new field of *lightweight cryptography* emerges.

There should typically be a trade-off between *cost*, *performance*, and *security* (Fig.6). It is straightforward to optimize for any two of the three design goals, but a trade-off between all three is difficult [10]. That is an underlying research area in search for a proper solution.

The first step towards this goal is having an explicit overview of the low-cost RFID limitations. Today, the EPCglobal Class-1 Gen-2 (ISO 18000-6) standard is a base point. However, the current security mechanisms in this standard are very weak and require amendments e.g. the tag ID (here: Electronic Product Code) can be easily eavesdropped by unauthorized readers and the only protection mechanism is a 16-bit checksum CRC. The desirable security and privacy countermeasures include: authentication, encryption, and message integrity.

To meet these countermeasures, one of the best known ways is using cryptography but with considering the limitations for low-cost RFID

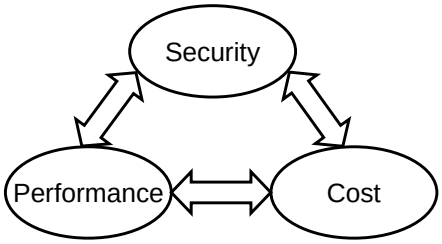

Fig. 6: *Triangle of trade-off among security, cost and performance.*

tags. As mentioned earlier, this is the scope of lightweight cryptography. The attempts to amend the current standard in RFID technology to make them more secure led to publishing the family of ISO/IEC 29192 standards. This standard defines properties of lightweight cryptographic primitives in four parts. In the first part of this standard some general properties of lightweight cryptography based on target platforms are presented. Properties such as chip size and/or energy consumption in hardware implementations and the code and/or RAM size in software implementations. In the second, third and forth parts of this standard, some lightweight algorithms from block ciphers, stream ciphers and public keys are presented respectively.

In this section, we explore the lightweight cryptography in two main categories: *lightweight primitives* or algorithms and *lightweight protocols* (Figure 7) in Section 4.1 and Section 4.2 respectively. In the case of lightweight primitives, we only compare some of the most recent algorithms of each type and their properties in a table. But in the case of lightweight protocols, we provide some well-known examples of each kind.

4.1 Lightweight Primitives

In this section, we explore the most current state-of-art in lightweight primitives or algorithms which are designed to meet the low-cost RFID limitations. Lightweight primitives usually used as building blocks of lightweight protocols presented in Section 4.2 to be deployed on RFID tags.

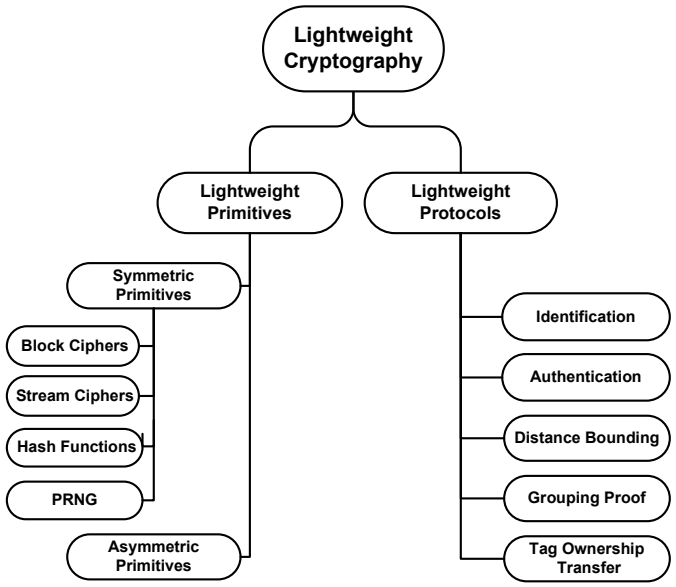

Fig. 7: *Lightweight Cryptography.*

4.1.1 Symmetric Key Primitives

In this subsection, we study block ciphers, stream ciphers, hash functions and random number generators.

- *Block Ciphers:* Block ciphers are one of the most fundamental cryptographic primitives. A typical block cipher E_k is a mapping which maps a binary message of length n as plain text to another binary message of the same length as cipher text i.e. $E_k : \{0,1\}^n \rightarrow \{0,1\}^n$ by using a key k.

  The history of conventional block ciphers goes back to 1977 when the DES algorithm was introduced, but the history of lightweight block ciphers is much more recent. It goes back to 1997 by the introduction of the XTEA block cipher [28]. Since then, there have been plenty of lightweight block cipher proposals. Some of the recent proposals for lightweight block ciphers are compared in Table 2 with their specifications.

  To have a more fair comparison, the ciphers are compared regarding the area required to implement them on hardware in gate

Algorithm	Area (GE)	Block size	Key size	Speed (Kbps)	Technology (μm)
mCRYPTON [35]	2,500	96	64	492.3	0.13
CLEFIA[39]	4,950	128	128	355.6	0.09
AES[39]	3,100	128	128	80.0	0.13
HIGHT[30]	3,048	64	128	188.2	0.25
SEA[40]	3,758	96	96	103	0.13
DESXL[31]	2,168	64	184	44.4	0.18
PRESENT[29]	1,570	64	80	200	0.18
KATAN[33]	1,054	64	80	25.1	0.13
KTANTAN[33]	688	64	80	25.1	0.13
PRINT[34]	402	48	80	3.2	0.18
LED[37]	1,872	64	80	3.4	0.18
KLEIN[38]	1,220	64	80	207	0.18
Piccolo[36]	616	64	80	432	0.13
LBlock[41]	1,320	64	80	200	0.18

Table 2: *Lightweight Block Ciphers*

equivalent(GE), their speed in Kbps at the frequency of 100KHz and their CMOS technology in μm.

As it can be seen the proposed schemes attempt to meet the limitations of passive low-cost RFIDs. From this list, PRESENT and CLEFIA are being standardized in the second part of ISO/IEC 29192 standard as lightweight block ciphers.

- *Stream Ciphers*: Stream ciphers provide an alternative to block ciphers for symmetric encryption. They are sometimes considered as particularly efficient, although this may not generally hold true [2].

  Stream ciphers used as a generator of a pseudo random string of binary bits as *keystream*. The key stream is generated by using a key and an initialization vector at the same length of plaintext. Then, the keystream is simply XORed by the plaintext to give the ciphertext.

  In contrast to block ciphers, there are not many proposals for lightweight stream ciphers. The most prominent ones are two of the hardware-oriented ciphers remained in the eStream project's

Algorithm	**Area** (GE)	**Interface Bits** (bit/cycle)	**Speed** (Kbps)	**Technology** (μm)
Grain[68]	1,294	1	100	0.13
	2,200	8	800	0.13
Trivium [68]	2,599	1	100	0.13
	2,800	8	800	0.13
Enocoro v.2 [70]	2,700	8	800	0.18

Table 3: *Lightweight Stream Ciphers*

portfolio, Grain v1 and Trivium [42] along with Enocoro [70]. These three lightweight stream ciphers are compared in Table 3. The Enocoro and Trivium algorithms are in the process of standardization in the third part of ISO/IEC 29192 as lightweight stream ciphers. It should be noted that some recent lightweight stream ciphers such as WG7 [71] and A2U2 [72] which attempted to improve the efficiency of the lightweight stream ciphers did not prospered due to significant security breaches [73, 74].

There is also a third group of hybrid algorithms in the literature such as Hummingbirds v.1 [43] and v.2 [44] which are more *authentication encryption* schemes.

- *Minimalism in Cryptography*: A major theme in cryptographic research is the analysis of minimal constructions. For example, many papers were published on the minimal cryptographic assumptions which are necessary and sufficient in order to construct various types of secure primitives. To lend clarity to our discussion, we should say that the term *minimal* means a local minima which becomes insecure when any one of their elements is eliminated, not a minimum scheme which is global minima among all the possible constructions [46].
  - *Minimal Stream Cipher*: In the case of stream ciphers, the simplest possible secure scheme is the *one-time pad*. Since any encryption algorithm requires a secret key, and XORing is the simplest conceivable way to mix it with the plain-text bits.
  - *Minimal Block Cipher*: In the case of block ciphers, this problem was first addressed by Even and Mansour in 1991 [45].

They were inspired by the DESX construction proposed to protect DES against exhaustive search attacks by XORing two independent pre-whitening and post-whitening keys to the plaintext and ciphertext (respectively). The Even-Mansour (EM) scheme used such whitening keys, but eliminated the keyed block cipher in the middle, replacing it with a fixed random permutation (F) that everyone can share. The resultant scheme is extremely simple: To encrypt a plaintext (P), XOR it with one key (K_1), apply to it a publicly known permutation (F), and XOR the result with a second key(K_2) [46].

$$C = EM^{\mathcal{F}}_{K_1,K_2}(P) = \mathcal{F}(P \oplus K_1) \oplus K_2 \quad (1)$$

To argue that the Even-Mansour scheme is minimal, its designers noted in [45] that eliminating either one of the two XORed keys makes it easy to invert the known effect of permutation on the plaintext or ciphertext, and thus to recover the other key from a single known plaintext/ciphertext pair. Eliminating the permutation is also disastrous, since it makes the scheme completely linear.

However, Shamir *et al* in [46] showed that, the two-key *EM* block cipher is not minimal in the sense that it can be further simplified into a single-key variant ($K_1 = K_2$) with half as many key bits which has exactly the same provable security.

4.1.2 Hash Functions

Hash functions yield a digest of a message which plays an important role in message authentication, data integrity, and digital signatures.

A hash function denoted by h maps a binary sting x with arbitrary length to an output binary string $y = h(x)$ of fixed length. Using hash functions is also popular in security and privacy protocol proposals for RFID systems.

Table 4 compares some of the recent lightweight hash functions and their specifications. It should be noted that the algorithms listed below may have different variants regarding block size, output size or internal state size; but only one of the variants is presented as a representative. There is also a lightweight message authentication code (MAC) algorithms [52] which is well designed to be suited to RFID-based challenge-response authentication protocols.

Algorithm	**Area**(GE)	**Block size**	**Output size**	**Speed** (Kbps)*	**Technology** (μm)
D-Quark [51]	1,702	160	176	2.27	0.18
Armadillo-C [69]	5,406	160	160	25	0.18
DM-Present [48]	1,600	64	64	14.63	0.18
H-Present[48]	2,330	128	128	11.45	0.18
Keccak[49]	1,300	160	200	1.86	0.13
Photon[50]	1,396	160	160	2.70	0.18
Spongent[47]	2,190	160	176	17.78	0.18

Table 4: *Lightweight Hash Functions.*
**Speed is given for a clock frequency of 100 kHz, assuming a long message.*

4.1.3 Random Number Generators

A Random Number Generator (RNG) is a device or procedure which produces a series of numbers or bits which are statistically independent and identically distributed [2].

To produce random numbers in practical security applications however, a Pseudo Random Number Generator (PRNG) is used. PRNG is an algorithm which generates an output sequence of bits which look like random informally meaning that prediction of any output bit of a PRNG is not be possible by a polynomial time algorithm with the probability of significantly greater than 0.5.

As mentioned in Section 2.4.1, there is already a lightweight 16-bit built-in PRNG on passive RFID tags compliant to EPCGlobal Class1 Gen2 standard. There are also a few proposals for lightweight random number generators in the literature. These schemes attempt to fulfill not only the EPCGlobal standard requirements for PRNG stated in Section 2.4.1, but also NIST requirements for random number generators [96]. Some of the lightweight PRNG schemes are listed in Table 5.

4.1.4 Public Key Primitives

In contrast to symmetric key primitives, public-key or *asymmetric key* primitives provide some security properties such as: non-repudiation, integrity protection, authentication, confidentiality and key exchange without previously established symmetric secret keys.

Algorithm	**Area**(GE)	**Output size**	**Speed** (Kbps)*	**Technology** (μm)
AKARI1A [54]	476	16	24.24	0.09
Mandal *et al*[55]	1,242	16	13.8	-
LAMED [53]	1,566	16	17	-

Table 5: *Lightweight Pseudo random number generator functions.*
* *Speed is given for a clock frequency of 100 kHz.*

RSA encryption as the most well-known public key algorithm has been widely used in various applications. But, due to computationally intensive operations and high memory consumption, it is currently not feasible to implement RSA for a low-cost RFID tags. This problem for the similar public key primitives such as ElGamal [62] and DSA (Digital Signature Algorithm) [63] which exploit exponential operations. However, these primitives can be suitable to be implemented on high-cost RFIDs with microprocessors (e.g. smart cards) or even with built-in cryptographic coprocessor.

On the other hand, there are some advantages in public key primitives which motivate the realizing public-key primitives on RFID tags. For example, by utilizing public key algorithms one can make the tags more resistant against counterfeiting and provide them with high level of privacy (strong privacy) [64]. Researchers have most recently been working on the feasibility of public-key algorithms for RFID tags [56, 58, 59], plus have developed Elliptic Curve Cryptography(ECC) [57, 60], Hyper Elliptic Curve Cryptography (HECC) [65] and NTRU [57] for RFID.

Recently, a hybrid Rabin-based public key encryption cryptosystem called BlueJay [66] has been proposed. BlueJay is a combination of the Hummingbird-2 [44] lightweight authenticated encryption algorithm and Passerine [67] optimized for a 1024-bit public modulus n and 32-bit register size. In Table 6, some of the latest results in the implementation of public key primitives are presented. It should be noted that there are many lightweight implementations of ECC regarding the field size. For example a lightweight implementation of 163-bit ($F_{2^{163}}$) ECC in [61] which is compliant with ISO 15693 and ISO 18000-3. The tag using this implementation is now available in industry mainly for anti-counterfeiting. ECC is also a candidate as a lightweight asymmetric (public key) primitive in the ISO/IEC 29192-4.

Algorithm	Area (GE)	Perf.* (ms)	Technology (μm)	Parameters
BlueJay [57]	$\leq$ 3,000	-	0.18	n = 1024, w = 32
NTRU [57]	3,000	58.45	0.18	N = 167, p = 3, q = 128
ECC [60]	8,104	115	0.18	$F_{2^{131}}, d = 4$
HECC [65]	14,500	456	0.13	$F_{2^{67}}, d = 8$

Table 6: *Lightweight public key primitives.*
* *Speed is given for a clock frequency of 500 kHz.*

4.2 Lightweight Protocols

The lightweight primitives presented in the previous section are utilized by the lightweight protocols to provide low-cost RFID systems with some properties. The main properties are: *identification*, *authentication*, as basic properties, and *delegation and restriction*, *proof of existence* and *distance bounding* as additional properties [2]. These properties are briefly introduced in this section.

- *Identification*: Identification in RFID systems is the process of identifying tags by readers via some identification information such as ID. Identification can be performed without using any secret information. Therefore, no cryptographic techniques are needed to provide identification. This property is fulfilled by the *identification protocols* (Section 4.2.1).

- *Authentication*: As the communication between tags and readers takes place in an open environment via RF signals, there should be a mechanism for both side to ensure validity and authenticity of the messages. This mechanism is called authentication. In contrast to identification, some secret information is needed for authentication. Some proposals for authentication in low-cost RFID tags are discussed in Section 4.2.2.

- *Delegation and Restriction*: The properties called delegation and restriction mainly address the *data ownership and partner data integration* challenge discussed in Section2.5. It happens when a tag's owner changes and the data corresponding to the tag is transferred to a new owner. This should be done while the current owner would not be able to trace the tag any more. The proto-

cols which are designed to address this issue are called *ownership transfer protocols* discussed in Section 4.2.5.

- *Proof of Existence*: Proof of existence guarantees that a particular tag exists in a specific location, at a specific time or with other particular tags. The proposals address this issue, which are called *yoking/grouping proof protocols* in the literature, along with some application of this property are discussed in more details in Section 4.2.3.

- *Distance Bounding*: To raise the security level of RFID systems against the relay attack described in Section 3.2, the accepted distance between any tag and reader must be limited or bounded. Distance bounding techniques are well-known solutions for this purpose. These techniques limit the accepted distance between a tag and a reader by measuring the round trip time of the exchanged messages between them and putting some limitations on the round trip time. The distance bounding proposals for low-cost RFID systems, called *distance bounding protocols*, are described in Section 4.2.4.

It should be noted that all the protocols presented in this section except the distance bounding protocols are executed in the *application layer* according to the ISO/OSI reference model described in Section 2.1.4. But the distance bounding protocols are executed in the *physical layer*.

4.2.1 Identification Protocols

A reader in passive RFID systems initiates the interrogations by broadcasting a *Query* message. If there is only one tag in the neighborhood or only one tag responds to this query, the identification is straightforward. But if more tags respond, the responses collide and thus cannot be correctly received by the reader and so, the identification process fails. The same thing (collision) may happen when one tag responds to the queries of multiple readers in the neighborhood. An effective technique to avoid this collision is using an *anti-collision* protocols in the identification process.

The proposed protocols for tag collision resolution in RFID systems are either *probabilistic* or *deterministic*. Probabilistic anti-collision schemes are mainly Aloha-based protocols which some of them can be found in [75–78]. While deterministic protocols are mostly tree-based

[79–82]. There are also some protocols with hybrid approaches [83, 84] which use randomization in tree-based schemes.

Aloha-based protocols use a time division technique for data transmission i.e. each RFID tag determines a distinct time slot and transmits data in that time slot to avoid collisions. EPCglobal Class 1 Generation 2 exploits a variant of this type.

However, in tree-based protocols, all tags transmit their identification data simultaneously. But if collision occurs, the anti-collision mechanism based on *binary tree* or *binary search tree* structure is invoked within the reader.

4.2.2 Authentication Protocols

Authentication protocols are extensively discussed in the literature in different forms. But one can categorize them in four major classes regarding the fundamental elements used in them: protocols based on *cryptographic primitives*, protocols based on *ultra lightweight operations*, protocols based on the capabilities of *EPCglobal Class1 Generation2* and protocols based on the notion of *physical primitives*.

Among the proposals based on cryptographic primitives, the protocols using hash functions or MACs (Message Authentication Codes) are among the first solutions discussed in the literature [85–87]. There are also some protocols based on PRNGs (Pseudo Random Numbers Generators) [94, 95], stream ciphers [89], block ciphers [88] and even public keys [90–93].

On the other hand, protocols based on *ultra-lightweight* operations attempt to provide authentication without using cryptographic primitives, and involve only simple bitwise and modular arithmetic on-tag operations (e.g. XOR, AND, OR, rotation, etc.). The proposals of this kind are divided into two major groups: protocols based on "*minimalist cryptography*" and protocols based on *NP-hard mathematical problems*.

The set of authentication schemes presented as the MAP-family (LMAP, EMAP, M2AP, etc) [97–99] and later on SASI [101] and Gossamer [102] protocols are inspired by the work minimalist cryptography for low-cost RFID tags [100] in which an ultra lightweight protocol for mutual authentication between tags and readers based on one-time authenticators is suggested. From this category, the SASI protocol is depicted in Figure 8. The most famous class of lightweight authentication protocols based on NP-hard mathematical problems is the HB family authentication protocols. The HB authentication protocol proposed by

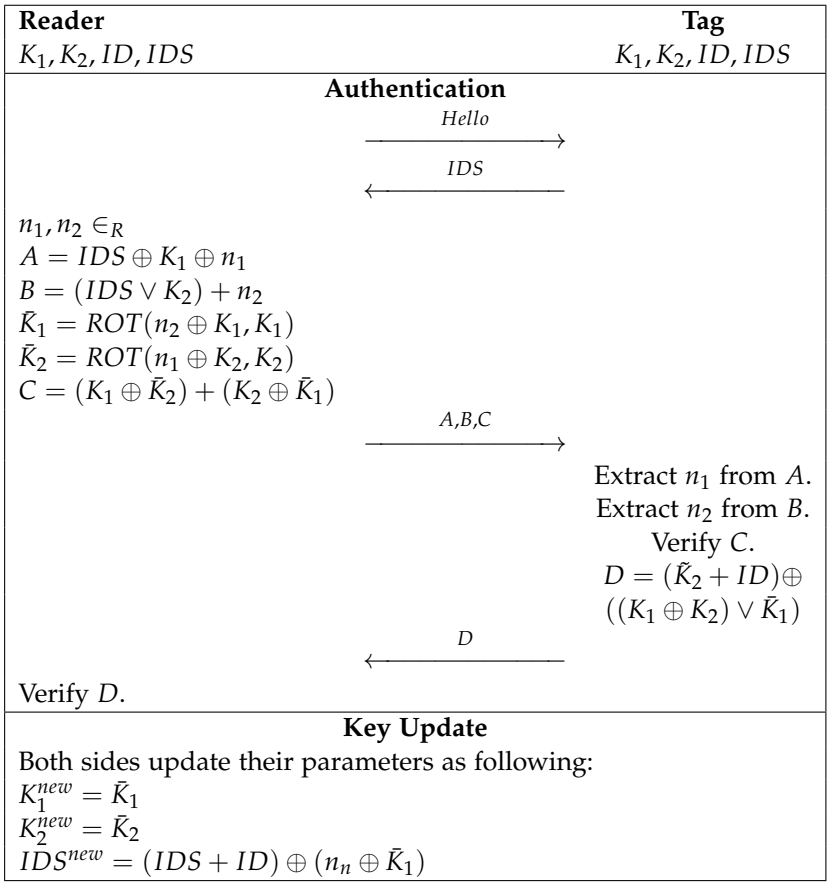

Fig. 8: *SASI ultra lightweight protocol*

Hopper and Blum in 2001 [103](Fig.9) is the first member of this family. This protocol aims at *unilateral* authenticating of an RFID tag to a reader only by lightweight operations. From one perspective, the operations used in this protocol are one matrix multiplication and some XORs. In addition, the security of this algorithm and some others in this family against *passive attacks* is reduced to a well-known NP-hard problem called *Learning with Parity Noise* (LPN) problem [104]. The other members of this family emerged as a result of proposing an attack on the previous one in order to eliminate the weaknesses and render the prior proposed attacks ineffective. Some of other members of this family are:

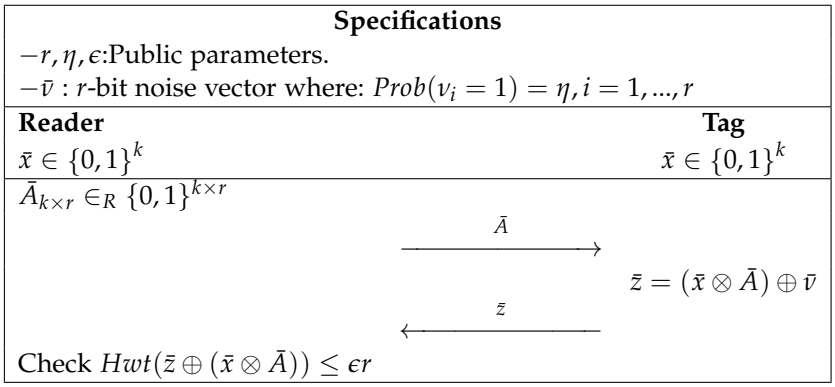

Fig. 9: *Parallelized version of an r-round HB protocol*

HB$^+$ [105], HB^{++} [106], HB* [107], HB-MP [108], HB$^\sharp$ [109] and NLHB [110].

As a possible alternative to HB-family protocols, another class of authentication protocols, called CKK or in general (n, k, L), were introduced in [111]. (n, k, L)-protocols have the advantage that fewer bits need be communicated in comparison to HB-type protocols, and the memory and computational requirements are lower at the tag and appear to be more resistant to *active attacks*. The security of (n, k, L)-protocols can be related to the hardness of a certain learning problem, in this case the Learning Unions of L linear subspaces (LULS) problem [112, 113].

The third category of authentication protocols consists of the schemes designed for conforming to EPCGlobal Class1 Generation2 standard [114–117]. These schemes mainly exploit the 16-bit CRC and 16-bit RNG of the standard to provide authentication.

In the protocols based on *physical primitives*, some properties related to the electronic circuits in RFID tags are exploited to form a primitive to be used in the authentication protocols. One of the most prominent proposals of this kind is Physical Unclonable Function (PUF). Some authentication protocols based on PUFs are presented in [118–120].

4.2.3 Yoking/Grouping Proof Protocols

In 2004, Juels [121] proposed a new security notion called *Yoking Proof*. The yoking proof enables the generation of a proof which shows that a

pair of RFID tags are scanned simultaneously by a reader. Yoking proof are later generalized to *grouping proofs* which indicates that multiple tags participate in the generation of the proof [122, 124].

By adopting grouping proofs, the manufacturer can prove to its customers that the referred products are sold at the same time. For example in a pharmacy store, some drugs must be sold according to the recipe. For inpatients, the medical staffs can guarantee the authentication and integrity of a group of medical items like inpatient bracelets and the containers of drugs [123]. For car industry, a grouping proof ensures that all components of a car are assembled in the same factory [121, 125].

In Figure 10, the yoking proof protocol proposed by Juels is depicted. The reader initiates the interrogation with the left tag (T_A and secret key k_A) by sending "start left". Then, T_A calculates the keyed hash (f) of its internal counter c_A and sends the tuple $a = (c_A, A, m_A)$ back to the reader. The reader initiates the interrogation with the tag on the right (T_B and secret key k_A) by sending it "start right" concatenated with a. T_B computes $m_B = MAC_{k_B}(a, c_B)$, where c_B is the internal counter of T_B and sends the tuple $b = (B, m_B, c_B)$ to the reader and increase its internal counter by one. The reader sends b to T_A and receives $m_{AB} = MAC_{k_A}(a, b)$ in return. The yoking proof is calculated as follows:

$$P_{AB} = (A, B, c_A, c_B, m_{AB})$$

In this way, a verifier (e.g. the database), who has access to the secret key of both tags and given the proof P_{AB}, is able to verify the correctness of the proof by calculating a' and b',

$$\begin{aligned} a' &= (A, c_A, f_{k_A}(c_A)) \\ b' &= (B, c_B, MAC_{k_B}(a', c_B)) \end{aligned}$$

and subsequently checks the equality $m_{AB} = MAC_{k_A}(a', b')$. Grouping proof protocols mainly address the tags sequentially. But in order to make the schemes more practical, Lien *et al*. [127] suggested scanning tags in parallel instead of in a sequential way. Since then, several schemes have been proposed to improve the efficiency of grouping proofs such as [126, 128].

Most of the grouping proof protocols in the literature are based on a hash function or a MAC or they conform to EPC Class-1 Generation2 low-cost RFID tag capabilities. However, there are also some grouping proof protocols based on Elliptic Curve Cryptography(ECC) [129].

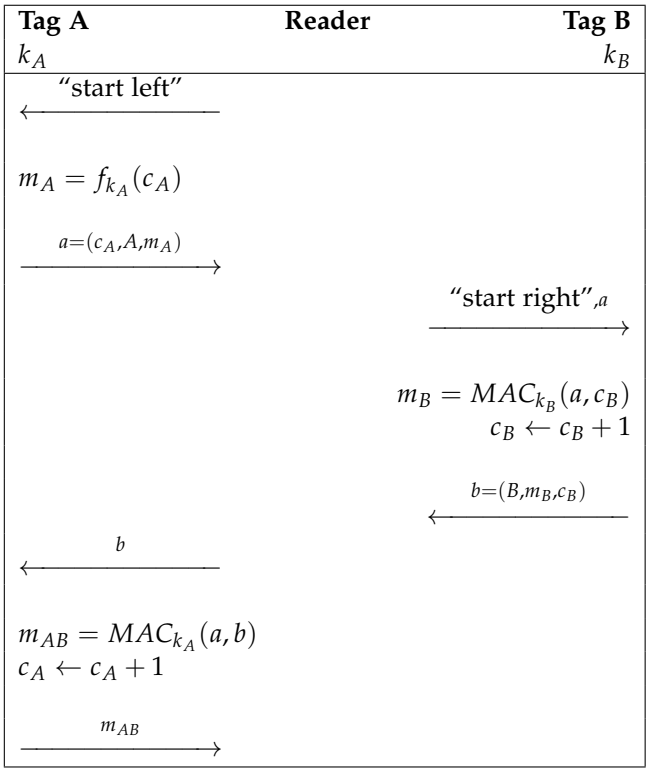

Fig. 10: *Juels's Yoking proof protocol*

4.2.4 Distance Bounding Protocols

Although many schemes have been proposed to secure RFID systems, most of them are still susceptible to relay attack or other different attacks related to locations. These attacks (see Section 5.1) aim at suggesting a wrong assumption of the distance between a tag and a reader and require simpler technical resources than tampering or cryptanalysis, and they cannot be prevented by other lightweight protocols that operate in the *application layer*. The main countermeasure against these attacks is the use of *distance bounding* protocols, which verify not only that the tag knows the cryptographic secret, but also that is within a certain distance. To achieve this goal, distance bounding protocols must be tightly integrated into the *physical layer* [130].

In 1993, Brands and Chaum proposed the first distance bounding protocol [134]. Afterward, in 2005, Hancke and Kuhn [135] proposed the first distance-bounding protocol dedicated to RFID systems.

So far, there have been many schemes proposed either similar to Hancke and Kuhn [131, 136, 139–141] or with different structures [134, 137, 138, 142, 143]. However, they mostly have something in common; they all consist of two major parts: a *slow phase* in the beginning followed by a *fast phase* or *rapid bit exchange* phase. In the fast phase, the round trip time (RTT) of a bitwise challenge and response is measured to estimate the distance i.e. a reader is able to calculate the distance of a tag (d) [8]:

$$d = c \times \frac{(\Delta t - t_d)}{2}; \quad \Delta t = 2t_p + t_d \tag{2}$$

where, c is the propagation speed of light, t_p is the one-way propagation time , Δt is the total elapsed RTT and t_d is the processing delay of the tag.

The Hancke and Kuhn protocol is illustrated in Figure 11. In the first slow phase, the tag and the reader generates a random number each (N_T and N_R respectively) and exchange their random numbers. Then, the reader and the tag compute the hash value $H = h_k(N_R, N_T)$ which is of length $2n$, where n is a security parameter and assign the first n-bit to v^0 and the second n-bit to v^1. In the i^{th} round of the fast phase, the reader chooses a random challenge bit c_i and sends it to the tag. The tag responds with v_i^0. The fast phase is performed for n rounds. It should be noted that in some schemes, there is a third part called *slow phase-II*, which has the role of the final phase or *signature*. Both slow phases consist of the time-consuming operations such as random nonce generations, commitment and signature calculations. On the other hand, the fast phase includes non-time consuming response generations and rapid bit exchanges. In order to decrease the adversary success probability of distance bounding protocols, Munilla and Peinado introduced the concept of *void challenges* in [146]. Such challenges may be 0, 1, or *void*, and the reader and tag agree on those challenges that should be void - void means that no challenge is sent [132]. Some modifications of this idea are introduced recently using *non-uniform* [143] or *mixed challenges* [147]. The idea is that the challenges from the reader to the tag in the fast bit exchanges are divided into two categories, random challenges and predefined challenges. The former are random bits from the reader and the latter are predefined bits known to both the reader and the tag in advance [8].

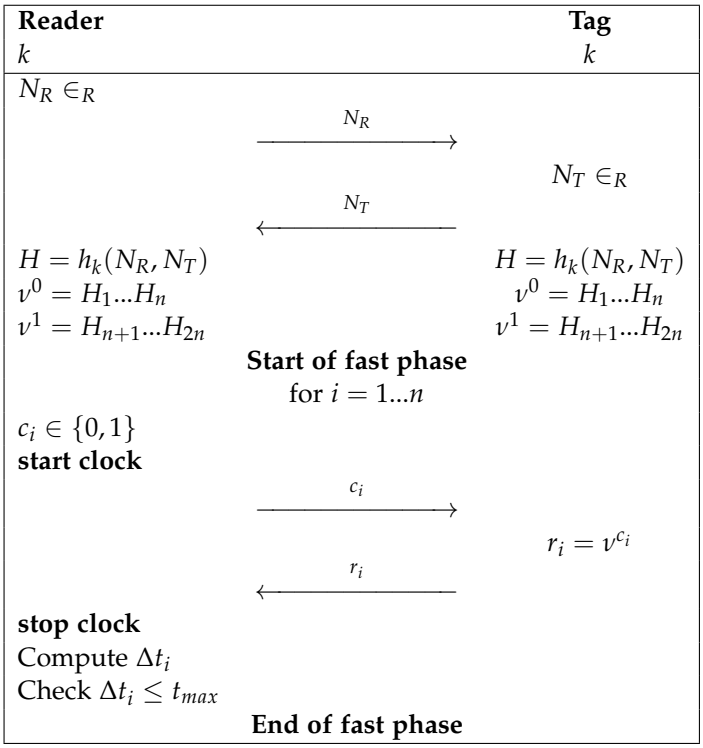

Fig. 11: *Hancke and Kuhn's Distance Bounding Protocol*

One of the well-known schemes which consists of a final signature is the Swiss-knife protocol [137] proposed by Kim *et al*. This protocol attempts not only to resists location related attacks but also tackle the problem of *noisy channels* by using an *error resistance* mechanism. As it can be seen in Figure 12, the tag chooses a random N_T and computes a temporary key $a = f_k(C_T, N_T)$ using its permanent secret key k and N_T (here C_T is just a system-wide constant). The tag splits its permanent secret key k in two shares by computing $R^0 = a$,$R^1 = a \oplus k$. After this first slow phase, the rapid bit exchange phase starts. This phase is repeated n times and the challenge-response delay is measured for each step. But in fact channel errors might occur (either randomly or by action of the attacker) in this phase. Therefore, the challenges and responses are denoted differently (c_i, c_i' and r_i, r_i') at each side of the channel to consider possible noise occurrence. The tag answers by

Reader k, ID		**Tag** k, ID
$N_R \in_R \{0,1\}^n$		
	$\xrightarrow{N_R}$	
		$N_T \in_R \{0,1\}^n$ $a = f_k(N_T, C_T)$ $\begin{cases} R^0 = a \\ R^1 = a \oplus x \end{cases}$
	$\xleftarrow{N_T}$	
	Start of fast phase for $i = 1...n$	
$c_i \in_R \{0,1\}$ **start clock**		
	$\xrightarrow{c_i}$	
		$r'_i = R_i^{c'_i}$
	$\xleftarrow{r_i}$	
stop clock Compute Δt_i		
	End of fast phase	
		$s_T = f_x(ID, N_R,$ $N_T, c'_1, ..., c'_n)$
	$\xleftarrow{s_T}$	
Check ID in the Database Compute R^0, R^1 $err_c = \#\{i : c_i \neq c'_i\}$ $err_r = \#\{i : c_i = c'_i, r_i \neq R_i^{c_i}\}$ $err_t = \#\{i : c_i = c'_i, \Delta t_i > t_{max}\}$ if $err_c + err_r + err_t \geq \tau$ REJECT else $s_R = f_x(N_T)$		
	$\xrightarrow{s_R}$	
		Compute and Compare t_A

Fig. 12: *Swiss knife Distance Bounding*

$r'i = R^{c'_i}$. After the rapid bit exchange phase, the final phase (slow phase II) begins. In this phase, messages s_T and s_R are transmitted from the tag and the reader as a signature respectively. The reader is able to calculate the values R^0 and R^1 by looking up the tags's information in the back-end and then checks the validity of the responses made during rapid bit exchange phase. To render the scheme more resistant against the noise or errors in the channel, the reader computes three kinds of errors (err_c, err_r and err_t) and compare their summation with a predefined threshold τ. The reader continues the protocol unless the summation exceeds the threshold.

4.2.5 Tag Ownership Transfer Protocols

It is usually the case that the RFID tag changes owner many times during its life, and therefore one requires to manage the transfer of ownership, where the tag information must be transferred to the new owner. It is required that the current/old owner cannot track the tag after the transfer of ownership. In this context the idea of ownership transfer protocols is introduced, providing a solution to the requirement to transfer the tag's information in a secure and private way [150].

In ownership transfer protocols, there are mainly three active entities involved: *current/old owner*, *tag* and *new owner*. The owners in an ownership transfer protocols are some readers in practice which take the role of ownership in these kinds of protocols.

Most of the ownership transfer protocols consist of two phases, an *authentication phase* and an *ownership transfer phase*. By the former phase, the tag and two owners are mutually authenticated and the latter phase assures all three entities that the ownership of the tag is transferred securely.

The proposed protocols for ownership transfer protocols are divided into two groups. Some protocols exploit a trusted third party (TTP) which acts as a secure channel to transfer some information between the entities. One of the first solution of this kind was proposed by Saito *et al* [148, 149].

In Figure 13, the Saito *et al*'s ownership transfer protocol is illustrated. This protocol is among the first and simplest protocols of this kind and therefore not very secure. In this protocol, the secret s_n is shared between the current owner and the tag is updated to a new secret s_{n+1}, which is shared between the new owner and the tag.

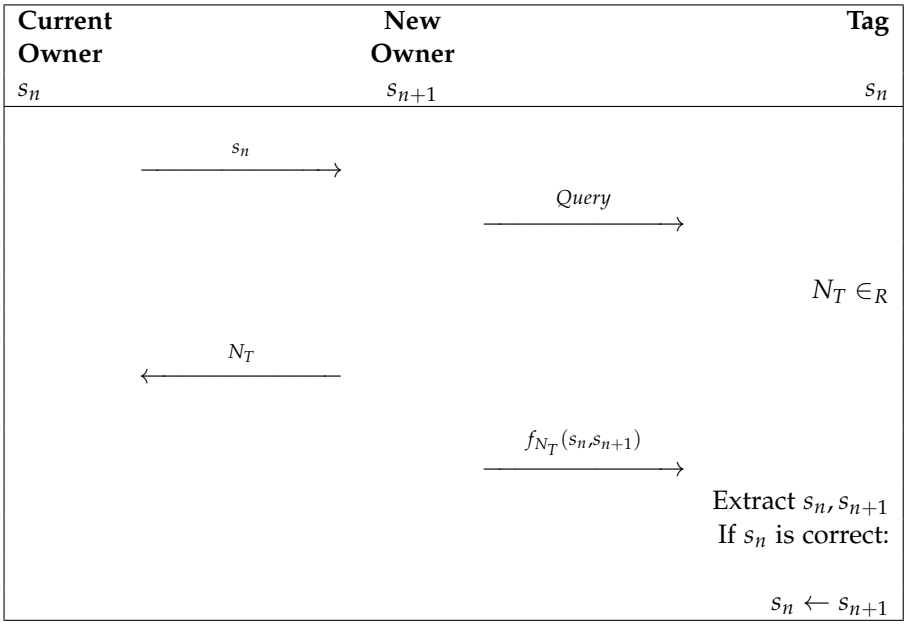

Fig. 13: *Saito* et al*'s ownership transfer phase*

There also exist some *decentralized* proposals without using a TTP. Most of these schemes have two following assumptions. It is assumed that there is a secure channel between the current and new owner to pass the tag's information securely. It is also assumed that the new owner and the tag will be able to execute an authentication session in an isolated environment without presence of the current owner after the ownership transfer is completed in order to update some secret parameters [151–154].

5 Security Analysis of Lightweight Schemes

Security analysis of a scheme can be done in three steps:

1. Defining the security requirements and security margins of the scheme.

2. Defining the adversarial capabilities and the adversarial model.

3. Searching to find an attacking scenario which exploits the adversarial capabilities to violate the security requirements with less computational overhead than the security margins.

If the last step of the security analysis is successful, we can conclude that the scheme lacks security or in other worlds, it is vulnerable against attacks. But there is an underlying bottle neck at the third step of this security analysis process; Searching to find effective attacking scenarios can be heuristic and therefore, if it is not successful, we can not conclude that the scheme is robust. To avoid this problem, formalization of the analysis is a good starting point.

In this section, we study how the security of a lightweight scheme can be analyzed. To do so, we first present some security requirements and potential attacking scenarios for lightweight schemes. Then, we briefly present some of the formal adversarial models in the literature, which implies the capabilities of adversaries to attack the schemes.

5.1 Privacy and Security Requirements

As mentioned in Section 4, there is always a trade-off among performance, cost and security. This implies that for lightweight schemes which are designed for low-cost RFID tags, it is not fair to expect the same security and performance as the conventional ones.

>From security perspective, loosing the security bounds can be an option. This can be achievable in two ways: lowering the desirable security margins or limiting adversarial capabilities.

5.1.1 Requirements for Lightweight Primitives

The security requirements of the lightweight primitives are almost the same as the conventional primitives, which are extensively discussed in the cryptography literature. The main differences between the security requirements of the lightweight primitives and conventional primitives are twofold:

1. The desired security margin for lightweight primitives is 2^{80} instead of 2^{128} which is more common in conventional primitives.

2. The *related-key* attack and the *side channel* attacks (e.g. fault attack) are arguable as adversarial capabilities.

5.1.2 Requirements for Lightweight Protocols

Lightweight protocols should fulfill some security and privacy requirements. In this section, we first study the general requirements which are common for all types of lightweight protocols and then, we present some requirements which are specific for each type.

The same as lightweight primitives, there are some commonsense in the security analysis of the lightweight protocols:

1. Passive attacks which only exploit the information collected via eavesdropping are more welcome.
2. Attacking the lightweight protocols specially those with ultra lightweight operations via tampering or some other side channel attacks is still arguable.

As mentioned earlier, the most important requirements of lightweight protocols are to preserve *privacy* which consists of two parts:

- *Resistant against tag information leakage*: the sensitive information of the tag should not be leaked or revealed to an unauthorized reader.
- *Resistant against tag tracking*: It should be impossible for an adversary to track or distinguish a specific tag by just having its output. As an extension of the second requirement, there is a property called *forward security*. Forward security is defined as follows: if the secret information in a tag becomes known to an adversary, e.g. via *tampering*, the past outputs of the tag should remain indistinguishable.

There are also some general *security* requirements for the lightweight protocols such as resistance against the following attacks [150]:

- *Tag impersonation*: In this attack, an adversary can impersonate a tag without knowing the tag's secret information in advance. Thus, it can communicate with a reader instead of the tag and be authenticated as the tag.
- *Replay attacks :* In this attack, an adversary can intercept messages exchanged between a reader and a tag, and replay them.
- *Man-in-the-middle attacks*: In this attack, an adversary can insert or modify messages sent between a reader and a tag without being detected.

- *Denial-of-service attacks :* In this attack, an adversary can interrupt or impede messages sent between a reader and a tag. Such an attack can cause *desynchronization* between the tag and the other components of the system.

Some of the lightweight protocols need some extra requirements to meet, e.g. yoking/grouping proof protocols need to resist even in the following situations [129]:

- *Compromised tag :* In this situation, the tag is compromised but the reader is non-compromised.
- *Colluding reader and tag :* In this situation, the reader and one of the tags are compromised.
- *Colluding tags :* In this situation, the reader is not compromised but both/a group of tags are compromised. In this situation, the compromised tags can exchange some messages in advance (e.g., via another reader), but do not know each other's private key.

Distance bounding protocols need also to resist against the following attacks [144]:

- *Distance Fraud*: A distance fraud is an attack where a dishonest and lonely tag purports to be in the neighborhood of the reader.
- *Mafia Fraud(relay attack)*: A mafia fraud is an attack where an adversary defeats a distance bounding protocol using a an-in-the-middle between the reader and an honest tag located outside the neighborhood.
- *Terrorist Fraud*: A terrorist fraud is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle between the reader and a dishonest tag located outside of the neighborhood, such that the latter actively helps the adversary to maximize her attack success probability, without giving to her any advantage for future attacks.

Figure 14 illustrates these attacks regarding the position of the adversary. The T^* and R^* represent the adversary in the role of a tag or a reader respectively.

In addition to the general requirements mentioned earlier, the ownership transfer protocols should fulfill the following requirements [155]:

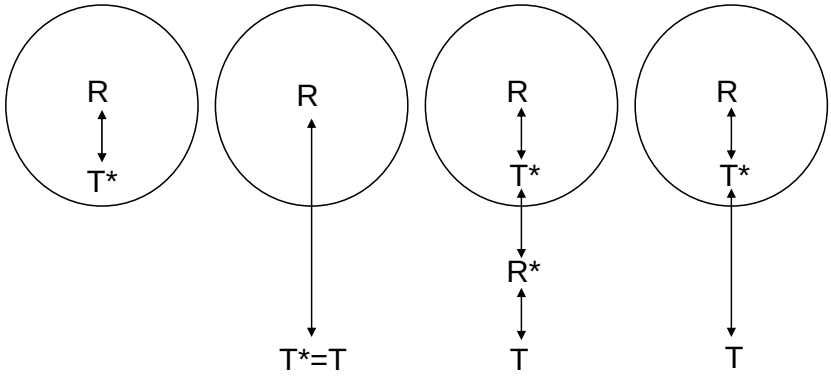

Fig. 14: *From left to right: Impersonation Fraud, Distance Fraud, Mafia and Terrorist Fraud [144].*

- *Previous owner privacy*: No future owners should be able to relate or trace back any previous communication between the previous owner and the RFID tag even though a full history of transmitted messages is eavesdropped and recorded.
- *New owner privacy*: No previous owners should be able to relate or track any current communication between the new owner and the RFID tag even though all the transmission is being eavesdropped.

There are also some other optional requirements for ownership transfer protocols in the literature [155]:

- *Controlled delegation*: The current owner of the RFID tag should have the authority to temporary delegate the access right of the tag to anyone without forfeiting the ownership to the tag. The delegate cannot overtake the ownership while the owner can cancel this delegation at anytime. Moreover, the delegation will automatically expire once a pre-determined number of queries value is reached.
- *Temporary authorization recovery*: The current owner of the RFID tag should be able to allow the previous owner to gain back the access to the RFID tag without going through another instance of the ownership transfer protocol. At the same time, the current owner can cancel the recovered authorization at anytime without the help from the previous owner.

- *Tag assurance*: During the ownership transfer scheme, the buyer should be able to be assured that the RFID tag undergoes the ownership transfer is the tag claimed by the current owner and requested by the buyer. This property guarantees that the current owner cannot randomly pick any tagged product he/she owns and sells it to the buyer.

- *Current ownership proof* : The current owner should be able to prove to any third party that he/she is the current owner of the RFID tagged item.

- *Undeniable ownership transfer* : The current owner should be able to prove to any third party that the RFID tagged item was owned by a previous owner and the previous owner cannot deny ever owning the tag.

- *Owner initiation*: The current owner and only the current owner should be able to initiate an ownership transfer, key change and delegation.

5.2 Adversarial Models

In this section, we explore two formal adversarial models which attempt to model the adversarial capabilities to attack the lightweight protocols' security requirements. In Subsections 5.3.2 the model mainly addresses the privacy requirement and it is mostly used to analyze the lightweight authentication protocols. The privacy models of this kind have been extensively studied in the literature, some of the well-known models of this kind are: Avoine's model [156], Juels-Weis's *et al*'s model [64], Vuadenay's model [158] and Herman *et al*'s model [157].

Furthermore, in Subsection 5.3.3, a formal framework for analyzing the security of distance bounding protocols is studied. It should be noted that there are some other formal models for other kinds of lightweight protocols such as ownership transfer protocols [160].

5.2.1 Notations

We will denote $\mathcal{T}$ as a tag, $\mathcal{R}$ as the reader and $\mathcal{A}$ as the adversary. A tag $\mathcal{T}$ is able to communicate with $\mathcal{R}$, when it enters into $\mathcal{R}$'s electromagnetic field. Then both reader and tag can participate together to a protocol instance π.

5.3 Adversarial Models

In this section, we explore two formal adversarial models which model the adversarial capabilities to attack the lightweight protocols' security requirements. In Subsection 5.3.2 the model mainly addresses the privacy requirement and it is mostly used to analyze the lightweight authentication protocols. The privacy models of this kind have been extensively studied in the literature, some of the well-known models of this kind are: Avoine's model [156], Juels-Weis's *et al*'s model [64], Vuadenay's model [158] and Herman *et al*'s model [157].

Furthermore, in Subsection 5.3.3, a formal framework for analyzing the security of distance bounding protocols is studied. It should be noted that there is also a formal approach to distance-bounding RFID protocols introduced in [145]. This approach gives rigorous cryptographic security models for mafia, terrorist, and distance frauds in distance-bounding protocols.

It should be noted that there are some other formal models for other kinds of lightweight protocols such as ownership transfer protocols [160].

5.3.1 Notations

We will denote $\mathcal{T}$ as a tag, $\mathcal{R}$ as a reader and $\mathcal{A}$ as an adversary. A $\mathcal{T}$ is able to communicate with $\mathcal{R}$, when it enters into $\mathcal{R}$'s electromagnetic field. Then, both reader and tag can participate together to a protocol instance π.

5.3.2 Herman e al's Model

Hermans, Pashalidis, Vercauteren and Preneel present a model based on indistinguishability [157] between two "worlds": it is most commonly called the "left or right" paradigm. This model is mainly inspired by Vaudanay's model.

In this model, the adversary $\mathcal{A}$ is able to interacts with the challenger by means of the following oracles:

- $\mathsf{CreateTag(ID)} \rightarrow \mathcal{T}_i$: on input a tag identifier ID, this oracle registers the new tag with the server.
- $\mathsf{Launch} \rightarrow (\pi, m)$: this oracle launches a new protocol run, according to the protocol specifications. It returns a session identifier π, generated by the reader, together with the first message m that

the reader sends. Note that this implies that this model does not support tag-initiated protocols.

- DrawTag$(\mathcal{T}_i, \mathcal{T}_j) \rightarrow vtag$: on input a pair of tag references, this oracle generates a virtual tag reference, as a monotonic counter, $vtag$ and stores the triple $\mathcal{T}_i, \mathcal{T}_j, vtag$ in a table D. Depending on the value of b, $vtag$ either refers to $\mathcal{T}_i$ or $\mathcal{T}_j$.

- Free(vtag)$_b$: on input $vtag$, this oracle retrieves the triple $(vtag, \mathcal{T}_i, \mathcal{T}_j)$ from the table Tab. If $b = 0$, it resets the tag $\mathcal{T}_i$. Otherwise, it resets the tag $\mathcal{T}_j$. Then it removes the entry $(vtag, \mathcal{T}_i, \mathcal{T}_j)$ from D.

- SendTag$(vtag, m)_b \rightarrow m'$: on input $vtag$, this oracle retrieves the triple $(vtag, \mathcal{T}_i, \mathcal{T}_j)$ from the table D and sends the message m to either $\mathcal{T}_i$ (if $b = 0$) or $\mathcal{T}_j$ (if $b = 1$). It returns the reply from the tag (m').

- SendReader$(\pi, m) \rightarrow m'$: on input π, m this oracle sends the message m to the reader in session π and returns the reply m' from the reader is returned by the oracle.

- Result(π): on input π, this oracle returns a bit indicating whether or not the reader accepted session π as a protocol run that resulted in successful authentication of a tag.

- Corrupt$(\mathcal{T}_i)$: on input a tag reference $\mathcal{T}_i$, this oracle returns the complete internal state of $\mathcal{T}_i$. Note that the adversary is not given control over $\mathcal{T}_i$.

The same as Vaudanay, Hermans *et al* divide adversaries into different classes, depending on restrictions regarding their use of the above the oracles. In particular, a *strong* adversary may use all eight oracles without any restrictions. A *destructive* adversary is not allowed to use a tag after it has been corrupted. This models situations where corrupting a tag leads to the destruction of the tag. A *forward* adversary can only do other corruptions after the first corruption. That is, no protocol interactions are allowed after the first corrupt. A *weak* adversary does not have the ability to corrupt tags. Orthogonal to these four attacker classes there is the notion of *wide* and *narrow* adversary. A wide adversary has access to the result of the verification by the server while a narrow adversary does not. Due to their generality, the above restrictions can be used perfectly in other privacy models.

The attacking scenario using this model for a specific class of adversary, P, is as follows.

1. The challenger initializes the system, chooses a bit b at random presents to the adversary the system where b refers to either the "left" tags $\mathcal{T}_i$ (if $b = 0$) or the right tags $\mathcal{T}_j$ (if $b = 1$).

2. $\mathcal{A}$ interacts with the whole system, limited by her class P.

3. $\mathcal{A}$ outputs a guess bit b'.

A We say that $\mathcal{A}$ wins the privacy game if and only if $g = b$, i.e. if it correctly identifies which of the worlds was active. The advantage of the adversary is defined as:

$$Adv_{\mathcal{A}}(k) = |Pr(b' = b|b = 0) + Pr(b' = b|b = 1) - 1| < \epsilon$$

5.3.3 Avoine *et al*'s Model for Distance Bounding

In this section, a brief overview of Avoine *et al*'s framework [144] for analyzing distance bounding protocol is given.

The adversary model which has been used in the model is the Dolev-Yao model [161]. In this model, the adversary can provoke or manipulate the communication between two parties where manipulating the communication means relay, withhold, or insert messages and she is only limited by the constraints of the cryptographic methods used. However, she cannot perform unbounded computations and cannot obtain the keys of honest parties. The latter assumption is not considered for the distance fraud attacks, where the tag has access to the keys.

The main attacking scenarios to target distance bounding protocols are : distance fraud, mafia fraud and terrorist fraud which are explained in Section 5.1.2. But the adversary can apply these attacks using three following strategies [144]:

1. *Pre-ask strategy*: The adversary relays the messages between the reader and the tag in both slow phases of the protocol, and before the honest reader starts the fast phase, executes the fast phase with the honest tag. Having the responses from the honest tag, the adversary carries on fast phase with the honest reader.

2. *Post-ask strategy*: The adversary relays the messages between the reader and the tag in both slow phases of the protocol. Afterward, she executes the fast phase with the honest reader without asking

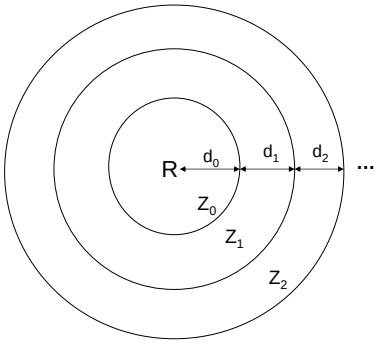

Fig. 15: *Adversary's location zones.*

the tag. Then, she queries the tag with the correct challenges received from the honest reader during the fast phase.

3. *Early-reply strategy*: In this strategy, the adversary, located outside of the neighborhood, relays the first slow phase. During the fast phase, her strategy is to anticipate the challenge and she replies before she is supposed to do so. In this way, the adversary deceives the verifier on his location.

Now, the distance of the adversary from the reader is studied. In the distance fraud attack, depending on how far the adversary is from the reader, she receives the challenges with some delay. This delay may impact the probability of success of the attack. Considering this determining factor, we use a modified version of the model described in [132]. In this model, the adversary can communicate with the reader from one of the spherical zones illustrated in Figure 15. For instance, Z_0 represents the legal authentication region with the diameter d_0, where the adversary accesses to all the challenges and produces valid responses on time. The distance d_0 is calculated by using (2) as:

$$d_0 = c \times \frac{(\Delta t - t_d)}{2}; \quad \Delta t = 2t_p + t_d \tag{3}$$

where, c is the propagation speed of light, t_p is the one-way propagation time, Δt is the total elapsed RTT and t_d is the processing delay of the tag.

When the adversary is located at Z_l, any response from her takes more time to get to the reader, namely

$$t'_p = t_p + \delta_t; \quad \delta_t = \frac{\sum_{i=1}^{l} d_i}{c} \tag{4}$$

In order to have a successful attack, the adversary should send each current response, at least $2\delta_t$ before receiving the current challenge. Moreover, the adversary located in Z_l has access to the challenges up to l^{th} previous round before she generates the response of the current round.

In the distance fraud, the capabilities of the tag as the adversary are of great importance. Considering that whether the tag has full control on the execution of the algorithm or not, we can have two different tampering capability models for the tag, *black-box* and *white-box*.

- *Black-box model*: In a black-box model, the tag cannot observe or tamper with the execution of the algorithm.
- *White-box model*: In a white-box model, the tag has full access to the implementation of the algorithm and a complete control over the execution environment.

In [144], it has been shown that the probability of success for an adversary tag can be remarkably elevated is it has the capabilities in the white-box model.

The model described in this section defines a framework for analyzing the security of a distance bounding protocol against distance fraud, mafia fraud and terrorist fraud attacks. It should be noted that the desired security margin of the distance bounding protocols against the mentioned attacks is $(\frac{1}{2})^n$, where n is the number of challenge and response iterations in the fast phase of the protocol. However, in [132], the authors showed that there are some trade-offs between the security margin of the distance bounding protocols against distance and mafia fraud attacks, for some protocols without final signature. It implies that the security margin against the distance fraud and mafia fraud can not reach the desired bound simultaneously.

6 Summary of Papers

This thesis consists of five papers. In the following sections, a short overview of each paper is given.

6.1 Paper I

The first paper, entitled "On the Security of Non-Linear HB (NLHB) Protocol against Passive Attack" and was presented at *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing* (EUC- TrustCom 2010) in Hong Kong, China.

As a variant of the HB authentication protocol for RFID systems presented in Section 4.2.2, which relies on the complexity of decoding *linear* codes against passive attacks, Madhavan *et al* presented Non-Linear HB (NLHB) protocol. In contrast to HB, NLHB relies on the complexity of decoding a class of *non-linear* codes to render the passive attacks proposed against HB ineffective. Based on the fact that there has been no passive solution for the problem of decoding a random non-linear code, the authors have claimed that NLHB's security margin is very close to its key size.

In this paper, we show that existing passive attacks against HB protocol can still be applicable to NLHB and this protocol does not provide the desired security margin. In our attack, we first linearize the non-linear part of NLHB to obtain a *HB equivalent* for NLHB, and then exploit the passive attack techniques proposed for the HB to evaluate the security margin of NLHB. The results show that although NLHB's security margin is relatively higher than HB against similar passive attack techniques, it has been overestimated especially when the noise vector in the protocol has a low weight.

6.2 Paper II

The second paper, entitled "Passive Cryptanalysis of the UnConditionally Secure Authentication Protocol for RFID Systems" and was presented at *International Conference on Information Security and Cryptology* (ICISC 2010) in Seoul, Korea.

Alomair *et al*. proposed the first *UnConditionally Secure* mutual authentication protocol for low-cost RFID systems(UCS-RFID). The security of the UCS-RFID relies on five dynamic secret keys which are updated at every protocol run using a fresh random number (nonce) secretly transmitted from a reader to tags.

Our results show that, at the highest security level of the protocol (security parameter= 256), inferring a nonce is feasible with the probability of 0.99 by eavesdropping about 90 runs of the protocol. Finding a nonce enables a passive attacker to recover all five secret keys of the protocol. To do so, we propose a three-phase probabilistic attack in this paper. Our attack recovers the secret keys with a probability that increases by accessing more protocol runs. We also show that *tracing* a tag using this protocol is also possible even with less runs of the protocol.

6.3 PAPER III

The third paper, entitled "Security Analysis of two Distance-Bounding Protocols" and was presented at *Workshop on RFID Security and Privacy* (RFIDSec 2011) in Amherst, Massachusetts, USA.

In this paper, we analyze the security of two recently proposed distance bounding protocols called the "Hitomi" and the "NUS" protocols. Our results show that the claimed security of both protocols has been overestimated. Namely, we show that the Hitomi protocol is susceptible to a full secret key disclosure attack which not only results in violating the privacy of the protocol, but also can be exploited for further attacks such as impersonation, mafia fraud and terrorist fraud attacks. Our results also demonstrates that the probability of success in a distance fraud attack against the NUS protocol can be increased up to $(\frac{3}{4})^n$ and even slightly more, if the adversary is furnished with some computational capabilities.

6.4 PAPER IV

The fourth paper, entitled "Colluding Tags Attack on the ECC-based Grouping Proofs for RFIDs" and was presented at *International Conference on Security and Cryptography* (SECRYPT 2011) in Seville, Spain.

A new privacy-preserving Elliptic Curve based grouping proof protocol with *colluding tag prevention*(CTP) has been proposed by Batina *et al*. The notion of this protocol is mainly derived from the latest version of an ECC-based authentication scheme called EC-RAC. The main security concern for this as grouping proof protocols is to prevent forged proof generation.

In this paper, we show that the CTP protocol is vulnerable to some *colluding tag* attacking scenario. In our attack, the involved tags pass some message to one specific tag to qualify it to represent them all in

the grouping proof generation time without revealing any information about their private keys.

In addition, we propose a new elliptic curve based grouping protocol which can fix the problem. Our proposal is based on a formally proved privacy preserving authentication protocol and has the advantage of being resistant against colluding tags attacks with the same amount of computation.

6.5 Paper V

The fifth paper, entitled "On the Privacy of Two Tag Ownership Transfer Protocols for RFIDs" and was presented at *IEEE International Conference for Internet Technology and Secured Transactions* (ICITST2011) in Abu Dhabi, UAE.

In this paper, the privacy of two recent RFID tag ownership transfer protocols are investigated against the tag owners as adversaries. The first protocol called ROTIV is a scheme which provides a privacy-preserving ownership transfer by using an HMAC-based authentication with public key encryption. However, our passive attack on this protocol shows that any legitimate owner which has been the owner of a specific tag is able to trace it either in the past or in the future. Tracing the tag is also possible via an active attack for any adversary who is able to tamper the tag and extract its information.

The second protocol called, *Chen et al*'s protocol, is an ownership transfer protocol for passive RFID tags which conforms EPC Class1 Generation2 standard. Our attack on this protocol shows that the previous owners of a particular tag are able to trace it in future. Furthermore, they are able even to obtain the tag's secret information at any time in the future which makes them capable of impersonating the tag.

7 Future Research

As mentioned earlier, public acceptance of RFIDs as an integral part of "Internet of Things" depends on strong technical and operational security and privacy solutions being in place. Although there have been plenty of efforts to provide a desirable level of security and privacy for RFIDs, there are still some missing pieces in the puzzle, e.g.:

- RFIDs still lack a standard which meets even a minimum level of security and privacy in practice.

- There is still not a unanimous agreement on the desirable security level and requirements in the lightweight cryptography.

The researches have shown that deploying lightweight primitives is possible on the RFID tags, even on the most constrained ones. Therefore, if the security and practical requirements of the RFID systems are clearly defined, the future trend of the research can be towards designing secure lightweight primitives and correspondingly provable lightweight protocols which not only meet the security but also the practical requirements of RFID systems.

REFERENCES

[1] Editors: Kitsos, Paris and Zhang. RFID Security: Techniques, Protocols and System-On-Chip Design. In Springer-Verlag. ISBN 978–1–441–94557–0, 2008.

[2] Editors: Miodrag Bolic, David Simplot-Ryl, and Ivan Stojmenovic. RFID systems : Research trends and challenges. In John Wiley & Sons Ltd. ISBN 978–0–470–74602–8, 2010.

[3] Editors: Pedro M. Reyes. RFID in the Supply Chain. In McGraw-Hill Companies. ISBN 978–0–07–163498–4, 2011.

[4] Dirk Henrici. RFID Security and Privacy Concepts, Protocols, and Architectures. In Springer-Verlag. ISBN 978–0–387–76480–1, 2008.

[5] Erick C. Jones and Christopher A. Chung. RFID in Logistics. In CRC Press. ISBN 978–0–8493–8526–1, 2008.

[6] Editors: Lu Yan, Yan Zhang, Laurence T. Yang, Huansheng Ning. THE INTERNET OF THINGS From RFID to the Next-Generation Pervasive Networked Systems. Auerbach Publications. ISBN 978–1–4200–5281–7, 2008.

[7] Harold F. Tipton, Micki Krause Nozaki. Information Security Management Handbook, Volume 5. CRC Press. 978–1–4398–5345–0, 2012.

[8] Editors: Y. Zhang, P.Kitos. Security in RFID and Sensor Networks. CRC Press. 978–1–4200–6839–9. 2009.

[9] Pedro Peris López. Lightweight Cryptography in Radio Frequency Identification (RFID) Systems. Ph.D. THESIS, 2008.

[10] Axel York Poschmann. Lightweight Cryptography - Cryptographic Engineering for a Pervasive World. Ph.D. THESIS, 2009.

[11] D. N. Duc, J. Park, H. Lee, and K. Kim. Enhancing security of EPCglobal Generation-2 RFID tag against traceability and cloning. In Symposium on Cryptography and Information Security (SCIS), 2006.

[12] EPCglobal Inc., Class1 Generation2 UHF Air Interface Protocol Standard Version 1.09, Available at http://www.epcglobalinc.org/standards_technology/ specifications.html.

[13] http://www.rfidjournal.com/article/view/1338

[14] http://msdn.microsoft.com/en-us/library/aa479355.aspx

[15] http://www.rfidnews.org/2008/05/30/understanding-rfid-part-9-rfid-privacy-and-security

[16] http://www.indiamart.com/twinantennas/rfid-antenna.html

[17] D. N. Duc, H. Lee and K. Kim. Enhancing Security of EPCGlobal Gen-2 RFID against Traceability and Cloning. Auto-ID Labs White Paper WP-SWNET-016, 2006.

[18] Simson L. Garfinkel. An RFID Bill of Rights, Technology Review. October 2002.

[19] A. Juels, R. L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In Proceedings of the 10th ACM Conference on Computer and Communication Security, pp. 103–111, ACM Press, 2003.

[20] Sarah Spiekermann. RFID and privacy: what consumers really want and fear. Journal Personal and Ubiquitous Computing archive. Volume 13 Issue 6, 2009.

[21] Z. Kfir, A.Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. Available at http://eprint.iacr.org/2005/052

[22] http://www.ti.com/rfid/shtml/apps.shtml

[23] http://www.rsa.com/rsalabs/node.asp?id=2120

[24] Marc van Lieshout, M., L. Grossi, et al. RFID Technologies: Emerging Issues, Challenges and Policy Options. Luxembourg, European Commission, Directorate-General Joint Research Centre, Institute for Prospective Technological Studies, 2007.

[25] Alexander Ilic, Trevor Burbridge, Andrea Soppera, Florian Michahelles. A Threat Model Analysis of EPC-based Information Sharing Networks. Building Radio frequency IDentification for the Global Environment, 2007.

[26] Commission of the European Communities. On The Implementation Of Privacy And Data Protection Principles In Applications Supported By Radio-Frequency Identification. Commission Of The European Communities, 2009.

[27] National Institute of Standards and Technology(NIST SP800-98). Guidelines for Securing Radio Frequency Identification (RFID) Systems, 2007.

[28] R.M. Needham, D.J. Wheeler: TEA extensions. Technical report, the Computer Laboratory, University of Cambridge. Archive available at: http://www.cl.cam.ac.uk/ftp/users/djw3/xtea.ps, 1997.

[29] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. Cryptographic Hardware and Embedded Systems (CHES), pp. 450–466. Springer, 2007.

[30] H. Kim, J. Kim, and S. Chee. HIGHT: A new block cipher suitable for low-resource device. Cryptographic Hardware and Embedded Systems (CHES), volume LNCS 4249, pp. 46–59. Springer, 2006.

[31] G. Leander, C. Paar, A. Poschmann, and K. Schramm. New lighweight DES variants. In A. Biryukov, editor, Fast Software Encryption 2007 (FSE), volume LNCS 4593, pp. 196–210, Springer, 2007.

[32] Toru Akishita and Harunaga Hiwatari. Very compact hardware implementations of block cipher CLEFIA. In Selected Areas in Cryptography. Available at http://sac2011.ryerson.ca/SAC2011/AH.pdf.

[33] Christophe De Cannirére, Orr Dunkelman, and Miroslav Knezevìc. KATAN and KTANTAN - a family of small and efficient hardware-oriented block ciphers. CHES, volume 5747 of LNCS, pp. 272–288. Springer, 2009.

[34] Lars R. Knudsen, Gregor Leander, Axel Poschmann, and Matthew J. B. Robshaw. PRINTcipher: A block cipher for IC-printing. CHES, LNCS 6225, pp. 16–32, 2010.

[35] Chae Hoon Lim and Tymur Korkishko. mCrypton - a lightweight block cipher for security of low-cost RFID tags and sensors. WISA2005 , volume 3786 of LNCS, pp. 243–258. Springer, 2005.

[36] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai. Piccolo: An Ultra-Lightweight Blockcipher. In CHES, LNCS 6917, pp. 342–357, 2011.

[37] J. Guo, T. Peyrin, A. Poschmann, M. J. B. Robshaw. The LED Block Cipher., CHES'10, LNCS 6225, pp. 326–341, 2010.

[38] Z. Gong, S. Nikova and Y.-W. Law. KLEIN: A New Family of Lightweight Block Ciphers. In RFIDsec, 2011.

[39] http://www.ecrypt.eu.org/lightweight/index.php/Block_ciphers

[40] F. Mace, F.-X. Standaert, and J.-J. Quisquater. Implementations of the Block Cipher SEA for Constrained Applications. Proceedings of the Third International Conference on RFID Security, RFIDSec 2007, pp.103–114, 2007.

[41] Wenling Wu and Lei Zhang. LBlock: A Lightweight Block Cipher. ACNS 2011, LNCS 6715, pp. 327–344,2011.

[42] S.Babbage, C. De Cannière, A. Canteaut, C. Cid, H. Gilbert, T. Johansson, M. Parker, B. Preneel, V. Rijmen, and M. Robshaw. The eSTREAM Portfolio (rev. 1). eSTREAM, ECRYPT Stream Cipher Project. Available at: http://www.ecrypt.eu.org/stream/portfolio_revision1.pdf

[43] D. Engels, X. Fan, G. Gong, H. Hu, E.M. Smith: Ultra-Lightweight Cryptography for Low-Cost RFID Tags: Hummingbird Algorithm and Protocol, http://www.cacr.math.uwaterloo.ca/techreports/2009/cacr2009-29.pdf

[44] Engels, D., Saarinen, M.J.O., Smith, E.M.: The Hummingbird-2 Lightweight Authenticated Encryption Algorithm, http://eprint.iacr.org/2011/126.pdf

[45] S. Even and Y. Mansour. A construction of a cipher from a single pseudorandom permutation. In Advances in Cryptology , ASIACRYPT '91, volume 739 of LNCS, pp. 210–224. Springer-Verlag,

1992.

[46] Orr Dunkelman, Nathan Keller, and Adi Shamir. Minimalism in Cryptography: The Even-Mansour Scheme Revisited. EUROCRYPT 2012. Available at: www.eprint.iacr.org/2011/541.pdf

[47] Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede. SPONGENT: A lightweight hash function. CHES, volume 6917 of LNCS, pp. 312–325. Springer, 2011.

[48] Andrey Bogdanov, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, and Yannick Seurin. Hash functions and RFID tags: Mind the gap. CHES, volume 5154 of LNCS, pp. 283–299. Springer, 2008.

[49] Guido Bertoni, Joan Daemen, Michäel Peeters, and Gilles Van Assche. Keccak sponge function family main document (version 2.1). Submission to NIST (Round 2), 2010.

[50] Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON family of lightweight hash functions. In CRYPTO, volume 6841 of LNCS, pp. 222–239. Springer, 2011.

[51] Jean Philippe, Aumassony Luca Henzenz, Willi Meierx and Marìa Naya-Plasencia. Quark: a lightweight hash. In CHES , pp. 1–15, 2010.

[52] A. Shamir. SQUASH: A New MAC With Provable Security Properties for Highly Constrained Devices Such as RFID Tags. In Proc. of FSE, 2008.

[53] 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. Journal of Computer Standards & Interfaces, 2008.

[54] Honorio Martín, Enrique San Millán, Luis Entrena, Julio César Hernández Castro and Pedro Peris Lpez. AKARI-X: a pseudorandom number generator for secure lightweight systems. IEEE 17th International On-Line Testing Symposium, 2011.

[55] Kalikinkar Mandal, Xinxin Fan and Guang Gong, A Lightweight Pseudorandom Number Generator for EPC Class 1 Gen2 RFID Tags. RIM Seminar, 2011.

[56] Sandeep Kumar and Christof Paar. Are standards compliant Elliptic Curve Cryptosystems feasible on RFID? Workshop on RFID Security. RFIDSec, 2006.

[57] Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. An elliptic curve processor suitable for RFID-tags. Cryptology ePrint Archive, Report 2006/227, 2006.

[58] Maire McLoone and Matt Robshaw. Public key cryptography and RFID tags. In Masayuki Abe, editor, The Cryptographers' Track at the RSA Conference. CT-RSA, LNCS, Springer-Verlag, 2007.

[59] Kazuo Sakiyama, Lejla Batina, Nele Mentens, Bart Preneel, and Ingrid Verbauwhede. Small-footprint ALU for public-key processors for pervasive security. Workshop on RFID Security. RFIDSec, 2006.

[60] L. Batina, N. Mentens, K. Sakiyama, B. Preneel,and I. Verbauwhede. Low-cost elliptic curve cryptography for wireless sensor networks, in Security and Privacy in Ad-Hoc and Sensor Networks (ESAS), LNCS 4357, pp. 6–17, 2006.

[61] M. Braun, E. Hess, and B. Meyer. Using elliptic curves on RFID tags, International Journal of Computer Science and Network Security, pp. 1–9, 2008.

[62] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms Advances in cryptology: Proceedings of CRYPTO. LNCS. pp. 10–18, Springer-Verlag, 1984.

[63] http://csrc.nist.gov/publications/fips/fips186-3/fips 186-3.pdf

[64] S. Vaudenay. RFID Privacy based on Public-Key Cryptography (Invited Talk). In ICISC. LNCS, vol. 4296, pp. 1–6. Springer, 2006.

[65] K. Sakiyama. Secure Design Methodology and Implementation for Embedded Public-key Cryptosystems. PhD thesis, Katholieke Universiteit Leuven, Belgium, 2007.

[66] Markku-Juhani O. Saarinen. The BlueJay Ultra-Lightweight Hybrid Cryptosystem. available at: www.eprint.iacr.org/2012/195.pdf, 2012.

[67] Markku-Juhani O. Saarinen. The PASSERINE public key encryption and authentication mechanism. NORDSEC 2010, Lecture Notes in Computer Science. vol. 7127. pp. 283–288, 2011.

[68] M. Feldhofer, and J. Wolkerstorfer. Hardware implementations of symmetric algorithms for RFID security. In RFID Security, Techniques, Protocols and System-on-Chip-Design. Springer, pp. 373–415, 2009.

[69] Stéphane Badel1, Nilay Dağtekin1, Jorge Nakahara Jr, Khaled Ouafi, Nicolas Reffé, Pouyan Sepehrdad, Petr Sušil1, and Serge Vaudenay. ARMADILLO: A Multi-purpose Cryptographic Primitive Dedicated to Hardware. In CHES, LNCS 6225, pp. 398–412, 2010.

[70] Dai Watanabe, Toru Owada, Kazuto Okamoto,Yasutaka Igarashi and Toshinobu Kaneko. Update on Enocoro Stream Cipher. In IEEE ISITA. pp. 778–783, 2010.

[71] Y. Luo, Q. Chai, G. Gong and X. Lai. WG-7: A lightweight stream cipher with good cryptographic properties. IEEE Global Telecommunications Conference, GLOBE-COM'10, pp. 1–6, 2010.

[72] M. David, D.C. Ranasinghe, and T. Larsen. A2u2: A stream cipher for printed electronics rfid tags. pp. 176–183. IEEE, 2011.

[73] Qi Chai, Xinxin Fan and Guang Gong. An Ultra-Efficient Key Recovery Attack on the Lightweight Stream Cipher A2U2. www.eprint.iacr.org/2011/247.pdf

[74] Mohammad Ali Orumiehchiha, Josef Pieprzyk, and Ron Steinfeld. Cryptanalysis of WG-7:A Lightweight Stream Cipher for RFID Encryption. www.eprint.iacr.org/2011/687.pdf

[75] S.R. Lee, S.-D. Joo, and C.-W. Lee. An enhanced dynamic framed slotted aloha algorithm for RFID tag identification. In Proc. of Mobiquitous, pp. 166–172, 2005.

[76] M. A. Bonuccelli, F. Lonetti, and F. Martelli. Tree slotted aloha: a new protocol for tag identification in RFID networks. In Proc. of IEEE Int. Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 603–608, 2006.

[77] Q. Peng, M. Zhang and W. Wu. Variant Enhanced Dynamic Frame Slotted ALOHA Algorithm for Fast Object Identification in RFID System. In Proc. of IEEE Int. Workshop on Anti-counterfeiting, Security, Identification, pp. 88–91, 2007.

[78] J.R. Cha and J.H. Kim, Dynamic framed slotted ALOHA algorithms using fast tag estimation method for RFID system. In IEEE Con-

sumer Communications and Networking Conf., Vol. 2, pp. 768–772, 2006.

[79] C. Law, K. Lee, and K.-Y. Siu. Efficient memoryless protocol for tag identification (extended abstract). In Proc. 4th Int. workshop on Discrete Algorithms and methods for mobile computing and communications (DIALM), pp. 75–84, 2000.

[80] H.S. Choi, J.R. Cha, and J.H. Kim. Improved bit by bit binary tree algorithm in ubiquitous IDsystem. In LNCS, PCM, No. 3332, pp. 696–703, 2004.

[81] J. Myung, W. Lee and T.K. Shih, An Adaptive Memoryless Protocol for RFID Tag Collision Arbitration. In IEEE Trans. on Multimedia, Vol. 8, pp. 1096–1101, 2006.

[82] J. Myung, W. Lee, J. Srivastava and T.K. Shih. Tag-Splitting: adaptive collision arbitration protocols for RFID tag identification. In IEEE Trans. on Parallel and Distributed Systems, Vol. 18 , pp. 763–775, 2007.

[83] A. Micic, A. Nayac, D. Simplot-Ryl and I. Stojmenovic. A hybrid randomized protocol for RFID tag identification. In 1st IEEE Int. Workshop on Next Generation Wireless Networks (WoNGeN), 2005.

[84] J. Ryu, H. Lee, Y. Seok, T. Kwon and Y. Choi. A Hybrid Query Tree Protocol for Tag Collision Arbitration in RFID systems. In IEEE Int. Conf. on Communications, pp. 5981–5986, 2007.

[85] T. Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks, Conference on Security and Privacy for Emerging Areas in Communication Networks(SecureComm), 2005.

[86] M. Ohkubo, K. Suzuki and S. Kinoshita. Eficient hash-chain based RFID privacy protection scheme, International Conference on Ubiquitous Computing (Ubicomp), Workshop Privacy: Current Status ans Future Directions, 2004.

[87] G. Avoine, P. Oechslin. A scalable and provably secure hash based RFID protocol. Workshop on Pervasive Computing and Communication Security(PerSec), 2005.

[88] M. Feldhofer, S. Dominicus and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm, Proceedings of CHES, LNCS 3156, pp. 357–370, 2004.

[89] Olivier Billet, Jonathan Etrog, and Henri Gilbert. Lightweight Privacy Preserving Authentication for RFID Using a Stream Cipher. Proceedings of FSE, LNCS 6147, pp. 55–74, 2010.

[90] Yong Ki Lee, Lejla Batina, Dave Singelée, and Ingrid Verbauwhede. Low-Cost Untraceable Authentication Protocols for RFID. In Proceedings of the 3rd ACM conference on Wireless network security (WiSec), 2010.

[91] Yong Ki Lee, Lejla Batina, and Ingrid Verbauwhede. EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol. In IEEE International Conference on RFID, pp. 97–104, 2008.

[92] Yong Ki Lee, Lejla Batina, and Ingrid Verbauwhede. Untraceable RFID Authentication Protocols: Revision of EC-RAC. In IEEE International Conference on RFID, pp. 178–185, 2009.

[93] Lejla Batina, Stefaan Seys, Dave Singelée, and Ingrid Verbauwhede. Hierarchical ECC-Based RFID Authentication Protocol. RFIDSec, 2011.

[94] T. van Le, M. Burmester, and B. de Medeiros. Universally Composable and Forward-Secure RFID Authentication and Authenticated Key Exchange. Proc. ACM Symp. on Information, Computer, and Communications Security (ASIACCS), ACM Press, pp. 242–252, 2007.

[95] M. Burmester, T. van Le, and B. de Medeiros, Provably secure ubiquitous systems: Universally composable RFID authentication protocols. Proc. 2nd IEEE CreateNet Int. Conf. on Security and Privacy in Communication Networks (SECURECOMM), 2006.

[96] E. Barker, J. Kelsey, Recommendation for random number generation using deterministic random bit generators (revised). NIST Special publication 800-90 (March 2007), http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90revised March2007.pdf

[97] Peris-Lopez, Hernandez-Castro,Estevez Tapiador, and Ribagorda. LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags. RFIDSec , 2006.

[98] P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda. M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags, in International Conference on Ubiquitous Intelligence and Computing (UIC), vol. 4159 of LNCS, pp.912–923, 2006.

[99] P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda. EMAP: An Efficient Mutual-Authentication Protocol for Low-cost RFID tags , in OTM Federated Conferences and Workshop: IS Workshop, 2006.

[100] A. Juels. Minimalist cryptography for low-cost RFID tags. In Proc. of SCN, volume 3352 of LNCS, pp. 149–164, 2004.

[101] H.Y. Chien. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. IEEE Transactions on Dependable and Secure Computing. pp. 337–340, 2007.

[102] P. Peris-Lopez, J.C.Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda. Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In WISA. LNCS, vol. 5379, pp. 56–68. Springer, 2009.

[103] N.J. Hopper and M. Blum. Secure Human Identifcation Protocols, in Advances in Cryptology ASIACRYPT, Volume 2248, LNCS, pp. 52–66, Springer-Verlag, 2001.

[104] J. Bringer, H. Chabanne, and E. Dottax. HB++: a Lightweight Authentication Protocol Secure Against Some Attacks, IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU), 2006.

[105] Julien Bringer and Herve Chabanne. Trusted-HB: a low-cost version of HB+ secure against man-in-the-middle attacks. CoRR, abs/0802.0603, 2008.

[106] Julien Bringer, Herve Chabanne, and Emmanuelle Dottax. HB++: a lightweight authentication protocol secure against some attacks. In Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU), pp. 28–33. IEEE Computer Society, 2006.

[107] Dang Nguyen Duc and Kwangjo Kim. Securing HB+ against GRS man-in-the-middle attack. In Institute of Electronics, Information and Communication Engineers, Symposium on Cryptography and Information Security, 2007.

[108] J. Munilla and A. Peinado. HB-MP: A further step in the HB-family of lightweight authentication protocols. Computer Networks, 2007.

[109] Henri Gilbert, Matthew J. B. Robshaw, and Yannick Seurin. HB♯: Increasing the security and effciency of HB+. Advances in Cryptology EUROCRYPT, Annual International Conference on the Theory and Applications of Cryptographic Techniques. volume 4965 of LNCS, pp. 361–378. Springer, 2008.

[110] Mukundan Madhavan,Andrew Thangaraj,Yogesh Sankarasubramaniam and Kapali Viswanathan, NLHB : A Non-Linear Hopper Blum Protocol,IEEE National Conference on Communications (NCC),2010, CoRR abs/1001.2140:2010.

[111] J. Cichoń, M. Klonowski, and M. Kuty lowski. Privacy protection for RFID with hidden subset identifiers. In Proceedings of Pervasive, volume 5013 of LNCS, pp. 298–314. Springer, 2008.

[112] Matthias Krause and Matthias Hamann. The Cryptographic Power of Random Selection. ECRYPT Workshop on Lightweight Cryptography. pp. 122–146, 2011.

[113] Matthias Krause and Dirk Stegemann. More on the Security of Linear RFID Authentication Protocols. In SAC, LNCS 5867, pp. 182–196, 2009.

[114] H.Y. Chien, C.H. Chen. Mutual authentication protocol for RFID conforming to EPC Class-1 Generation-2 standards. in Computer Standards & Interfaces,pp. 254–259, 2007.

[115] H.M. Sun, and W.C. Ting. A gen2-based rfid authentication protocol for security and privacy. IEEE Transactions on Mobile Computing, 2009.

[116] D. Seo, J.Baek, and D. Cho. Secure RFID Authentication Scheme for EPC Class Gen2. In Proc. 3rd Int. Conf. on Ubiquitous Information Management and Communication (ICUIMC), pp. 221–227, 2009.

[117] C.-L. Chen, and Y.-Y. Deng. Conformation of EPC Class 1 Generation 2 standards RFID system with mutual authentication and privacy protection. Engineering Applications of Artificial Intelligence, Elsevier, 2009.

[118] R.Bassil, W. El-Beaino, W. Itani, A. Kayssi, A. Chehab. PUMAP: A PUF-Based Ultra-Lightweight Mutual-Authentication RFID Protocol.International Journal of RFID Security and Cryptography (IJRFIDSC), Volume 1, 2012.

[119] P. Tuyls, L. Batina. RFID-tags for anti-counterfeiting. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 115–131. Springer, 2006.

[120] L. Bolotnyy, G. Robins. Physically unclonable function-based security and privacy in rfid systems. In: IEEE International Conference on Pervasive Computing and Communications (PerCom 2007). pp. 211–220, 2007.

[121] Ari Juels. Yoking-Proofs for RFID Tags. In the Proceedings of First International Workshop on Pervasive Computing and Communication Security, IEEE Press, pp.138–143, 2004.

[122] Junichiro Saitoh and Kouichi Sakurai. Grouping Proofs for RFID Tags. In the Proceedings of AINA International Conference, IEEE Computer Society, pp. 621–624, 2005.

[123] C.Y. K. Hsieh Hong Huang. A RFID Grouping Proof Protocol for Medication Safety of Inpatient. Journal of Medical Systems, 2008.

[124] L. Bolotnyy and G. Robins. Generalized Yoking-Proofs for a Group of RFID Tags, in Proc. International Conference on Mobile and Ubiquitous Systems (Mobiquitous), 2006.

[125] Hung-Min Sun, Wei-Chih Ting, Shih-Ying Chang. Offlined Simultaneous Grouping Proof for RFID Tags,The Second International Workshop on Multimedia, Information Privacy and Intelligent Computing Systems(MPIS), 2009.

[126] Hung Yu Chien. Tree-Based RFID Yoking Proof. International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009.

[127] Y. Lien, X. Leng, K. Mayes, and J. Chiu. Reading Order Independent Grouping Proof for RFID Tags. IEEE International Conference

on Intelligence and Security Informatics, ISI, 2008.

[128] Dang Nguyen Duc, Jangseong Kim, Kwangjo Kim. Scalable Grouping-proof Protocol for RFID Tags. The Symposium on Cryptography and Information Security (SCIS), 2010.

[129] Lejla Batina, Yong Ki Lee, Stefaan Seys, Dave Singelee, Ingrid Verbauwhede. Short Paper: Privacy-preserving ECC-based grouping proofs for RFID, In Information Security Conference(ISC), 2010.

[130] Jorge Munilla Fajarado, A. Peinado Dominguez. Security in RFID and Sensor Networks. First Edition, ISBN: 978-1-4200-6839-9, Auerbach publication, 2009.

[131] Gildas Avoine and Aslan Tchamkerten. An efficient distance bounding RFID authentication protocol: balancing false-acceptance rate and memory requirement. In Information Security Conference (ISC), volume 5735 of LNCS, 2009.

[132] Orhun Kara, Süleyman Karda, Muhammed Ali Bingöl, Gildas Avoine: Optimal Security Limits of RFID Distance Bounding Protocols editors Radio Frequency Identification: Security and Privacy Issues (RFIDSec), volume 6370 of LNCS, pp. 220–238, 2010.

[133] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and J. C. A. van der Lubbe. Shedding Some Light on RFID Distance Bounding Protocols and Terrorist Attacks. arXiv.org, Computer Science, Cryptography and Security , 2010.

[134] Stefan Brands and David Chaum. Distance-bounding protocols. In EUROCRYPT: Workshop on the theory and application of cryptographic techniques on Advances in cryptology, pp. 344–359, 1994.

[135] Gerhard Hancke and Markus Kuhn. An RFID Distance Bounding Protocol.In Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm), pp. 67–73, 2005.

[136] Chong Hee Kim and Gildas Avoine. RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks. In 8th International Conference on Cryptology And Network Security (CANS), 2009.

[137] Chong Hee Kim, Gildas Avoine, Francois Koeune, Francois-Xavier Standaert, and Olivier Pereira. The Swiss-Knife RFID Distance Bounding Protocol. In International Conference on Information

Security and Cryptology (ICISC), volume 5461 of LNCS, pp. 98–115, 2008.

[138] Jorge Munilla, Andres Ortiz, and Alberto Peinado. Distance Bounding Protocols with Void-Challenges for RFID. In Workshop on RFID Security(RFIDSec), 2006.

[139] Jorge Munilla and Alberto Peinado. Security Analysis of Tu and Piramuthu's Protocol. In New Technologies, Mobility and Security (NTMS), pp. 1–5, 2008.

[140] Jason Reid, Juan Gonzalez Neito, Tee Tang, and Bouchra Senadji. Detecting relay attacks with timing based protocols. In Feng Bao and Steven Miller, editors, Proceedings of the ACM Symposium on Information, Computer and Communications Security(ASIACCS), pp. 204–213, 2007.

[141] Yu-Ju Tu and Selwyn Piramuthu. RFID Distance Bounding Protocols. In First International EURASIP Workshop on RFID Technology, 2007.

[142] Rolando Trujillo-Rasua, Benjamin Martin, and Gildas Avoine. The Poulidor Distance-Bounding Protocol. In Radio Frequency Identification: Security and Privacy Issues (RFIDSec), volume 6370 of LNCS, page 239–257, 2010.

[143] Ali Özhan Gürel, Atakan Arslan, Mete Akgün . Non-Uniform Stepping Approach to RFID Distance Bounding Problem. Fifth International Workshop on Data Privacy Management(DPM), volume 6370 of LNCS, 2010.

[144] G. Avoine, M. A. Bingol, S. Kardas, C. Lauradoux, and B. Martin. A Formal Framework for Cryptanalyzing RFID Distance Bounding Protocols. Cryptology ePrint Archive, Report 2009/543, 2009.

[145] U. Dürholz, M.Fischlin, M. Kasper, C. Onete. A formal approach to distance bounding RFID protocols. In: Proceedings of the 14th Information Security Conference ISC 2011. pp. 47–62. Lecture Notes in Computer Science, 2011.

[146] J. Munilla and A. Peinado. Distance Bounding Protocols for RFID Enhanced by Using Void-Challenges and Analysis in Noisy Channels. volume 8, pp. 1227–1232, 2008.

[147] Kim, Chong Hee and Avoine, Gildas. Distance Bounding Protocols with Mixed Challenges. IEEE Transactions on Wireless Communications, pp. 1618–1626, 2011.

[148] J. Saito, K. Imamoto, and K. Sakurai. Reassignment scheme of an RFID tags key for owner transfer. Embedded and Ubiquitous Computing, 2005.

[149] D. Molnar, A. Soppera, and D. Wagner. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In Selected Areas in Cryptography. Springer, 2006.

[150] Boyeon Song. RFID Tag Ownership Transfer. In 4th Workshop on RFID Security (RFIDsec 08), 2008.

[151] A. Soppera and T. Burbridge. Secure by default: The RFID acceptor tag (RAT), In 2nd Workshop on RFID Security (RFIDSec), 2006.

[152] E.J. Yoon and K.Y. Yoo. Two security problems of RFID security method with ownership transfer. In Network and Parallel Computing, 2008.

[153] G. Kapoor and S. Piramuthu. Vulnerabilities in some recently proposed RFID ownership transfer protocols. In First International Conference on Networks and Communications. IEEE, 2009.

[154] K. Osaka, T. Takagi, K. Yamazaki, O. Takahashi. An efficient and secure RFID security method with ownership transfer. In Proc. Computational Intelligence and Security, Springer-Verlag pp. 778–787, 2006.

[155] Ching Yu Ng, Willy Susilo, Yi Mua and Rei Safavi-Naini. Practical RFID ownership transfer scheme. Journal of Computer Security, pp. 319–341, 2011.

[156] Gildas Avoine. Adversary Model for Radio Frequency Identification. Cryptology ePrint Archive, Report 2005/049, 2005.

[157] Jens Hermans, Andreas Pashalidis, Frederik Vercauteren, and Bart Preneel. A New RFID Privacy Model. In European Symposium on Research in Computer Security (ESORICS), LNCS, Leuven, 2011.

[158] Serge Vaudenay. On Privacy Models for RFID. In Advances in Cryptology (ASIACRYPT), volume 4833 of LNCS, pp. 68–87, 2007.

[159] Iwen Coisel and Tania Martin. Untangling RFID Privacy Models eprint.iacr.org/2011/636

[160] Ton van Deursen, Sjouke Mauw, Saša Radomirović, and Pim Vullers. Secure ownership and ownership transfer in RFID systems. In Proc. European Symposium On Research In Computer Security (ESORICS), LNCS. Springer, 2009.

[161] D. Dolev and A. C. Yao. On the security of public key protocols. IEEE Transactions on Information Theory. pp. 198–207, 1983.

I

PAPER I

ON THE SECURITY OF NON-LINEAR HB (NLHB) PROTOCOL AGAINST PASSIVE ATTACK *

Mohammad Reza Sohizadeh Abyaneh

*Mohammad Reza Sohizadeh Abyaneh,"On the Security of Non-Linear HB (NLHB) Protocol Against Passive Attack", *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing* (EUC-TrustCom2010) in Hong Kong, China

On the Security of Non-Linear HB (NLHB) Protocol Against Passive Attack

Mohammad Reza Sohizadeh Abyaneh*

Abstract. As a variant of the HB authentication protocol for RFID systems, which relies on the complexity of decoding *linear* codes against passive attacks, Madhavan et al. presented Non-Linear HB(NLHB) protocol. In contrast to HB, NLHB relies on the complexity of decoding a class of *non-linear* codes to render the passive attacks proposed against HB ineffective. Based on the fact that there has been no passive solution for the problem of decoding a random non-linear code, the authors have claimed that NLHB's security margin is very close to its key size.

In this paper, we show that passive attacks against HB protocol can still be applicable to NLHB and this protocol does not provide the desired security margin. In our attack, we first linearize the non-linear part of NLHB to obtain a *HB equivalent* for NLHB, and then exploit the passive attack techniques proposed for the HB to evaluate the security margin of NLHB. The results show that although NLHB's security margin is relatively higher than HB against similar passive attack techniques, it has been overestimated and, in contrary to what is claimed, NLHB is vulnerable to passive attacks against HB, especially when the noise vector in the protocol has a low weight.

Key Words: RFID, Authentication, LPN problem, HB protocols.

*Department of Informatics, University of Bergen

1 INTRODUCTION

Radio Frequency Identification (RFID) tags are forming the next generation technology for identifying objects, and are poised to supplant barcodes in near future. Their advantages such as: more storage and ease of use have caused a universal proliferation of RFID tags in many commercial as well as national security applications; [1] ranging from electronic passports [3, 4], contactless credit cards [2], to supply chain management [5–7].

This widespread deployment of RFID tags has raised some concerns about their security. On the other hand, RFID tag constraints in processing power and memory make them tougher to deal with in security. These kinds of constraints dictate a paradigm shift in security provision for RFIDs which is known as *lightweight cryptography*.

Lightweight authentication protocol is a subset of lightweight cryptography which tackles providing authentication in highly constrained environments (e.g RFID systems) as well as security provision to a reasonable extent [8, 9].

1.1 NOTATIONS

- $G_{a\times b}$: $a \times b$ binary matrix.
- $h_{1\times b}$: $1 \times b$ binary vector.
- $A \otimes B$: matrix multiplication of A and B.
- $\oplus$: XOR operation.
- x_i: i^{th} bit of binary vector x.
- $Hwt(.)$: hamming weight function.
- $h \otimes G$: matrix multiplication of a vector h into matrix G.
- R, T: *Reader* and *Tag* respectively.

1.2 HB FAMILY PROTOCOLS

The HB lightweight authentication protocol proposed by Hopper and Blum in 2001 [10] is the first in the *HB family* of protocols. An overview of a paralleled r-round of the HB protocol is given in Figure 1. This protocol aims at unilateral authenticating of an RFID tag to a reader

Specifications
$-r, \eta, \epsilon$:Public parameters.
$-\nu$: d-bit noise vector where: $Prob(\nu_i = 1) = \eta, i = 1, ..., r$
HB Protocol
- Secret parameter $x \in \{0,1\}^k$ is shared between R and T.
(1) R : Chooses a random $A_{k \times r}$ matrix.
(2) $R \Rightarrow T : A$
(3) T : Computes $z_{1 \times r} = (x \otimes A) \oplus \nu_{1 \times r}$
(4) $T \Rightarrow R : z$
(5) R : ACCEPTS iff $Hwt(z \oplus (x \otimes A) \leq \epsilon r)$

Fig. 1: *Parallelized version of an r-round HB protocol*

only by lightweight operations. The operations used in this protocol are one matrix multiplication and some XORs. On the other hand, The security of this algorithm and some others in this family against passive attacks is reduced to a well-known NP-hard problem called *Learning with Parity Noise* (LPN) problem [11]. The other members of this family emerged as a result of proposing an attack on the previous one in order to eliminate the weaknesses and render the prior proposed attacks ineffective. Some of other members of this family are: HB^+ [12],HB^{++} [13], HB* [14],HB-MP [16],$HB^\sharp$ [21] and NLHB [17]. Attacks which have targeted these authentication protocols consists both *passive* [18–20] and *active* types [21, 22]. In an active attack, the adversary is able to eavesdrop the transcripts between a reader and a tag as well as being able to interact with them and manipulate the messages exchanging in between [23] in order to impersonate either of them. It should be noted that active attacks involve a broad spectrum of attacks which differ in adversary's capabilities (e.g. DET [23] and GRS [21] attack models). On the contrary, in a passive attack, the adversary has only access to the transcripts from an arbitrary number of authentication sessions between a tag and a reader and aims at impersonating either of them.

1.3 LPN Problem

If we see from a passive adversary perspective, who has only access to s number of parallelized r-round HB protocol transcripts(i.e. $A_{k \times n}, z_{1 \times n}, \eta$ where $n = s \times r$) and his goal is to recover secret parameter x, it will be obvious that she faces a decoding problem of a codeword $(x \otimes A)$

generated by a random linear block code A in presence of noise ν [25]. This problem is called *LPN problem* with parameters k, n, η and has been shown to be NP-hard in worst case [25].

1.4 LPN Solvers

In addition to worst case complexity results of the LPN problem, there are numerous studies on average case complexity [20, 26]. These studies has led to finding some algorithms to solve the LPN problem under certain assumptions(*LPN solvers*). Proposition of these algorithms paved the way for applying passive attack against some of HB family protocols.

In [20], the BKW algorithm has been reported which can be considered as an instance of the generalized birthday paradox [27]. In [18], another algorithm(FMICM) has been proposed inspired by fast correlation attack [24] on ciphers. The solution proposed by the FMICM algorithm is under the assumption of having low bit rate($\frac{k}{n}$)and high η. Besides some deterministic LPN solvers such as the two aforementioned algorithms, there are some probabilistic algorithms such as CTIN [19] which accomplish their goal even when the adversary has access to less amount of transcripts comparing to deterministic ones.

As said, applying any passive attack on HB protocol requires to utilize an LPN solver algorithm to solve the LPN problem. Thus, the terms *LPN solver* and *passive attack* against HB protocol point to the same notion and are used interchangeably hereafter.

Using LPN solvers caused a dramatic decrease in security margin of some of HB family protocols against passive attacks [18, 19]. As an attempt to search for a variant of the HB, which relies on the complexity of decoding *linear* codes against passive attacks, Madhavan et al. presented Non-Linear HB(NLHB) protocol. In contrast to HB, NLHB relies on the complexity of decoding a class of *non-linear* codes to render the passive attacks proposed against HB ineffective. Based on this fact that there has been no passive solution for the problem of decoding a random non-linear code, the authors have claimed that NLHB's security margin is very close to its key size.

Our Contribution. In this paper, we present a passive attack on the NLHB protocol. The idea of our attack is the linearization of the non-linear part of the NLHB protocol to convert it to an equivalent of conventional HB protocol. This method has been adopted in order to be able to deploy the passive attack techniques used against HB on NLHB.

Specifications
$-r, \eta, p, \epsilon$:Public parameters $-d = r - p$ $-\nu$: d-bit noise vector where: $Prob(\nu_i = 1) = \eta, i = 1, ..., d$
NLHB Protocol
- Secret parameter $x \in \{0,1\}^k$ is shared between R and T. (1) R : Chooses a random $A_{k \times r}$ matrix. (2) $R \Rightarrow T : A$ (3) T : Computes $z_{1 \times d} = f(x \otimes A) \oplus \nu_{1 \times d}$ (4) $T \Rightarrow R : z$ (5) R : ACCEPTS iff $Hwt(z \oplus f(x \otimes A)) \leq \epsilon d$

Fig. 2: *Parallelized version of an r-round NLHB protocol*

Outline. The remainder of this paper is organized as follows. In Section 2, we give a brief description of the NLHB protocol and Section 3 elaborates on our attack method on it. In Section 4, we display the results of applying our attack on NLHB compared to similar attacks on HB and eventually, Section 5 concludes the paper.

2 Description of the NLHB Protocol

Figure 2 shows one session of a parallelized r-round version of NLHB protocol. The tag and reader share a k-bit secret x in advance. The reader transmits a random $k \times r$ challenge matrix A to the tag. Having A received, the tag computes $f(x \otimes A)$. Subsequently, it also computes $z = f(x \otimes A) \oplus \nu$, where ν is a noise-vector whose bits are all independently distributed according to the Bernoulli distribution with parameter η, just like the noise vector in the HB protocol. $x \otimes A$ is also an r-bit vector similar to HB, but z differs in size. It is a d-bit vector($d = r - p$). On receiving z, the reader checks whether $Hwt(z \oplus f(x \otimes A)) \leq \epsilon d$ Where $0 < \epsilon < \eta < 0.5$. If this is true, reader accepts and this means that the tag has been authenticated successfully.

2.1 Function f

The function f used in the protocol is a non-linear function which maps $\{0,1\}^r$ to $\{0,1\}^d$. Specifically, in [17], the function f is defined as

p	g
2	$x_{i+1}x_{i+2}$
3	$x_{i+1}x_{i+2} \oplus x_{i+1}x_{i+3}$
	$x_{i+1}x_{i+3} \oplus x_{i+2}x_{i+3}$
	$x_{i+1}x_{i+2} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+1}$
4	$x_{i+1}x_{i+4} \oplus x_{i+2}x_{i+3}$
	$x_{i+1}x_{i+4} \oplus x_{i+2}x_{i+4} \oplus x_{i+3}x_{i+4}$
	$x_{i+1}x_{i+4} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+4}$

Table 1: *Proposed g function for NLHB protocol*

following:

$$y = f(x); y \in \{0,1\}^d, x \in \{0,1\}^r \tag{1}$$

and

$$y_i = x_i \oplus g(x_{i+1}, ..., x_{i+p}) \tag{2}$$

where $g : \{0,1\}^p \to \{0,1\}$ is a non linear boolean function. The authors have also proposed some specific functions for g corresponding to parameter p to achieve maximum entropy and lower the complexity of the protocol (see Table 1). In [17], the authors have shown that for a general function of f, the existing passive attacks on the HB protocol family (discussed in section 1.4) do not work on their protocol.

3 Proposed Attacking Method

3.1 Description

In this section, we present our three-phase passive attack on the NLHB protocol. In this passive attack, we assume that the attacker has access to n rounnds of the NLHB protocol where $n = s \times r$ (i.e. s sessions of an r-round protocol) and thus can form matrix A according to (3).

$$A_{k\times n} = (A^1_{k\times r} || \dots || A^s_{k\times r}) \tag{3}$$

where $A^i_{k\times r}$ is random matrix in i^{th} session.

Exploiting the passive attack techniques proposed for the HB protocol, we require to find an *HB equivalent* of the NLHB protocol. This implies that we should first find a linear approximation of its non-linear part and then update its parameters accordingly. Hence, phase I and II of

p	g	$\approx$ g	q
2	$x_{i+1}x_{i+2}$	x_{i+1}	0.75
		x_{i+2}	0.75
3	$x_{i+1}x_{i+2} \oplus x_{i+1}x_{i+3}$	x_{i+1}	0.75
	$x_{i+1}x_{i+3} \oplus x_{i+2}x_{i+3}$	x_{i+3}	0.75
	$x_{i+1}x_{i+2} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+1}$	x_{i+2}	0.75
4	$x_{i+1}x_{i+4} \oplus x_{i+2}x_{i+3}$	x_{i+1}	0.62
	$x_{i+1}x_{i+4} \oplus x_{i+2}x_{i+4} \oplus x_{i+3}x_{i+4}$	x_{i+4}	0.75
	$x_{i+1}x_{i+4} \oplus x_{i+2}x_{i+3} \oplus x_{i+3}x_{i+4}$	$x_{i+2} \oplus x_{i+3} \oplus x_{i+4} \oplus 1$	0.75

Table 2: *Best linear approximation of function g in NLHB protocol and their probabilities*

our attack tackle the former and latter implications and phase III is the utilization of passive attack techniques on the equivalent HB protocol.

Phase I: Linearization

Our objective in this phase is to find a relatively good linear approximation for non-linear part of NLHB to convert the problem of decoding a non-linear random code to LPN problem. To do so, we should find a matrix B such that the probability q in (4) is relatively high.

$$prob(f\,(x \otimes A) = (x \otimes A)_{1\times n} \otimes B_{n\times n^*}) = q; \;\; n^* = n - s \times p \quad (4)$$

To construct matrix B, we require to linearize the whole system and according to (2), the non-linear part of the algorithm is the function g which will be our target for linearization hereafter. We can use the Walsh-Hadamard technique [28] to find the best linear approximation for the boolean function g such that:

$$g(x_{i+1}, ..., x_{i+p}) \approx \sum_{j=i+1}^{i+p} c_j x_j \quad (5)$$

According to Table 2, all functions proposed for NLHB can be linearly approximated with a relatively high probability. A linear approximation of all g functions with their probabilities q are shown in Table 2. Having c_js from linear approximation of g, we can conclude this phase by calculating matrix B. Similar to matrix A in (3), matrix B for s sessions has the following structure:

$$B_{n\times n^*} = (B^1_{n\times d}||\ldots||B^s_{n\times d}) \quad (6)$$

in which,

$$b_{ij}^{l} = \begin{cases} 1 & \text{if } i = j \\ c_j & \text{for } j = i+1, ..., i+p \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

where $i = 1, ..., n;\ j = 1, ..., n^*;\ l = 1, ..., s$ or,

$$B_{n\times d}^{l} = \begin{pmatrix} 1 & 0 & & 0 \\ c_1 & 1 & & 0 \\ c_2 & c_1 & & 0 \\ \vdots & c_2 & & \vdots \\ c_p & \vdots & \dots & \\ 0 & c_p & & 0 \\ 0 & 0 & & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & & c_p \end{pmatrix};\ l = 1, ..., s \tag{8}$$

Phase II: Finding a new linear equivalent protocol
In this phase, we attempt to find an equivalent HB protocol for NLHB using the linear approximation obtained in previous phase. Since our approximation is valid with probability q, we can rewrite (4) as following to formulate the HB equivalent of our NLHB protocol with new parameters denoted by *.

$$\begin{aligned} y &= f(xA) = (x \otimes A) \otimes B \oplus e \\ &= (x \otimes A^*) \oplus e \end{aligned} \tag{9}$$

where:

$$\begin{aligned} A^*_{k\times n^*} &= A_{k\times n} \otimes B_{n\times n^*} \\ Prob(e_i = 1) &= (1-q);\ i = 1, ..., n^* \end{aligned} \tag{10}$$

Now, by adding the noise of protocol to both side of (9) we have:

$$y = f(x \otimes A) \oplus \nu = (x \otimes A^*) \oplus \nu \oplus e = (x \otimes A^*) \oplus \nu^* \tag{11}$$

where $\nu^* = \nu \oplus e$.

As ν and e are independent, the probability of error for the new noise vector can be calculated by (12).

$$\begin{aligned} Prob(\nu_i^* = 1) = \eta^* = Prob(\nu_i = 1) + Prob(e_i = 1) - \\ Prob(\nu_i = 1) \times Prob(e_i = 1) \\ = \eta + (1-q) - (1-q)\eta. \end{aligned} \tag{12}$$

As it is apparent from (12), the noise of the equivalent HB protocol(ν^*) is more than the noise in NLHB protocol. Therefore, in general, the NLHB protocol is more resistant against the passive attacks comparing to the HB protocol with the same parameters. Nevertheless, according to our results in Section 4, this strength is far lower than it has been claimed and desired.

Phase III: Recovering secret parameter x

Up to here, we have accomplished to find an equivalent HB form for the NLHB protocol. From now on, the problem of recovering secret parameter x is an LPN problem with random matrix A^* and parameters k, n^*, η^* (equivalent HB parameters) and therefore can be achieved by using any of LPN solvers discussed in Section 1.4.

3.2 Complexity of the Attack

Complexity of our attack consists of three parts corresponding to each phase. For phase I, we need to find the best linear approximation for boolean function g with p variables. This can be done by finding Walsh-Hadamard coefficients of g with complexity of $O(p2^p)$. In phase II, we just have a matrix multiplication of $A_{k\times n}$ and $B_{n\times n^*}$ to form A^*. This process has the compexity of $O(knn^*)$ in general. But due to sparse form of matrix B in (8), this complexity is reduced to $O(kpn^*)$. Finally, the complexity of phase III relies on the complexity of the LPN solver algorithm. So, the complexity of our attack is calculated by (13) in which the complexity of phases I, II and III are denoted by C_I, C_{II} and C_{III} respectively.

$$C = C_I + C_{II} + C_{III} = O(p2^p) + O(kpn^*) + C_{III} \approx O(kpn^*) + C_{III}, n^* >> p \quad (13)$$

It should be noted that the complexity which computed in(13) is the *time complexity* of our attack. To be more precise, we should calculate the *data complexity* of our attack in terms of the amount of protocol rounds required to apply the attack(n^*) as well. Phase I and II are applied on the number of rounds of the protocol which are determined in phase III and these two phases do not impose any additional data complexity to our attack. Therefore, data complexity of our attack only relies on the data complexity of LPN solvers discussed in [18–20].

4 RESULTS

In this section, we demonstrate the results of applying our passive attack using three LPN solvers BKW,FMICM and CTIN on NLHB and compare the security margins of NLHB(i.e. its equivalent HB) with HB protocol with the same parameters. Our motivation to do such an unfair comparison is to demonstrate that security margin of the NLHB is not far more than th HB protocol with the same parameters.

Tables 3, 4 and 5 show a comparative time and data complexity of applying passive attacks on NLHB and HB protocol for three different but low noise probability ($\eta = 0.15, 0.10, 0.05$ for HB and correspondent $\eta^* = 0.36, 0.32, 0.29$ in NLHB respectively) as well as the number of rounds of the protocol required to apply the attack (data complexity). As the results show, not only are the passive attacks on HB applicable to NLHB, but also the security margin of NLHB protocol is not far more than HB protocol. It is manifest that the results of our attack using FMICM are remarkably better in comparison with BKW and CTIN. Furthermore, we can have better results when the noise vector in the protocol has a lower weights(Table 5).

5 CONCLUSIONS

We presented a passive attack against NLHB protocol by finding an HB equivalent of it and then using some LPN solver techniques. Our results not only negate the authors claim that their protocol is resistant to passive attacks on the HB protocol but also show that the NLHB has not elevated the security margin of the HB remarkably and this is mainly due to the poor design of the non-linear part of the NLHB.

In summary, what we did is as follows. We:

- targeted Non-Linear HB protocol for passive attack.
- found a linear approximation of the non linear part of the protocol and converted the protocol to an equivalent HB protocol with higher noise.
- applied three well-known LPN solver techniques as a passive attack to the equivalent protocol.
- calculated the complexity of our attack on NLHB.

Key Length	**Time Complexity**						**Data Complexity**					
	CTIN		**BKW**		**FMICM**		**CTIN**		**BKW**		**FMICM**	
	HB	NLHB	HB	NLHB	HB	NLHB	HB	NLHB	HB	NLHB	HB	NLHB
32	2^{21}	2^{26}	2^{3}	2^{15}	2^{8}	2^{12}	2^{3}	2^{11}	2^{3}	2^{15}	2^{8}	2^{12}
64	2^{9}	2^{36}	2^{31}	2^{40}	2^{19}	2^{22}	2^{13}	2^{14}	2^{31}	2^{40}	2^{19}	2^{22}
128	2^{23}	2^{78}	2^{47}	2^{62}	2^{35}	2^{45}	2^{13}	2^{15}	2^{47}	2^{62}	2^{35}	2^{45}
192	2^{39}	2^{118}	2^{63}	2^{83}	2^{52}	2^{67}	2^{13}	2^{16}	2^{63}	2^{83}	2^{52}	2^{67}
256	2^{56}	2^{162}	2^{76}	2^{99}	2^{71}	2^{88}	2^{14}	2^{16}	2^{76}	2^{99}	2^{71}	2^{88}

Table 3. Time complexity and Data complexity passive attacks on HB and NLHB $\eta = 0.15$,$\eta^* = 0.36$

Key Length	**Time Complexity**						**Data Complexity**					
	CTIN		**BKW**		**FMICM**		**CTIN**		**BKW**		**FMICM**	
	HB	NLHB	HB	NLHB	HB	NLHB	HB	NLHB	HB	NLHB	HB	NLHB
32	2^{1}	2^{13}	2^{20}	2^{25}	2^{8}	2^{10}	2^{10}	2^{13}	2^{20}	2^{25}	2^{8}	2^{10}
64	2^{4}	2^{30}	2^{28}	2^{37}	2^{17}	2^{19}	2^{10}	2^{13}	2^{28}	2^{37}	2^{17}	2^{19}
128	2^{13}	2^{66}	2^{44}	2^{59}	2^{35}	2^{38}	2^{13}	2^{15}	2^{44}	2^{59}	2^{35}	2^{38}
192	2^{24}	2^{102}	2^{57}	2^{78}	2^{54}	2^{63}	2^{13}	2^{15}	2^{57}	2^{78}	2^{54}	2^{63}
256	2^{31}	2^{140}	2^{70}	2^{94}	2^{71}	2^{85}	2^{14}	2^{16}	2^{70}	2^{94}	2^{71}	2^{85}

Table 4. Time complexity and Data complexity passive attacks on HB and NLHB $\eta = 0.1$,$\eta^* = 0.32$

Key Length	**Time Complexity**						**Data Complexity**					
	CTIN		**BKW**		**FMICM**		**CTIN**		**BKW**		**FMICM**	
	HB	NLHB	HB	NLHB	HB	NLHB	HB	NLHB	HB	NLHB	HB	NLHB
32	2^{1}	2^{10}	2^{17}	2^{23}	2^{6}	2^{8}	2^{11}	2^{13}	2^{17}	2^{23}	2^{6}	2^{8}
64	2^{2}	2^{26}	2^{24}	2^{35}	2^{12}	2^{16}	2^{11}	2^{13}	2^{24}	2^{35}	2^{12}	2^{16}
128	2^{5}	2^{57}	2^{37}	2^{57}	2^{25}	2^{36}	2^{14}	2^{15}	2^{37}	2^{57}	2^{25}	2^{36}
192	2^{9}	2^{88}	2^{50}	2^{73}	2^{42}	2^{54}	2^{14}	2^{16}	2^{50}	2^{73}	2^{42}	2^{54}
256	2^{14}	2^{120}	2^{60}	2^{89}	2^{58}	2^{76}	2^{14}	2^{16}	2^{60}	2^{89}	2^{58}	2^{76}

Table 5. Time complexity and Data complexity passive attacks on HB and NLHB $\eta = 0.05$,$\eta^* = 0.29$

6 ACKNOWLEDGEMENTS

We would like to thank prof. Øyvind Ytrehus for his review and helpful comments to improve our manuscript. We also appreciate anonymous reviewers' time and their valuable feedbacks.

REFERENCES

[1] Raphael C.-W. Phan: *Cryptanalysis of a New Ulteralightweight RFID Authentication Protocol-SASI*, IEEE Transaction on Dependable and Secure Computing, 2008.

[2] T.S. Heydt-Benjamin, D.V. Bailey, K. Fu, A. Juels, and T. O'Hare: Vulnerabilities in First-Generation RFID-Enabled Credit Cards, Proc. 11th Int'l Conf. Financial Cryptography and Data Security (FC '07), pp. 2–14, 2007.

[3] D.Carluccio, K.Lemke, C.Paar: E-passport:*the Global Traceability or How to feel like a UPS package*, Proceeding of WISA'06, LNCS 4298, Springer, pp.391–404, 2007.

[4] J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R.W. Schreur, Crossing Borders: *Security and Privacy Issues of the European e-Passport*, Proc. First Int'l Workshop Security (IWSEC '06), pp.152–167,2006.

[5] CASPIAN, Boycott Benetton: http://www.boycottbenetton.com,2007.

[6] Mitsubishi Electric Asia Switches on RFID: www.rfidjournal.com/article/articleview/2644/,2006.

[7] Target, Wal-Mart Share EPC Data: http://www.rfidjournal.com/article/articleview/642/1/1/,2005.

[8] G. Avoine and P. Oechslin. *RFID Traceability: A Multilayer Problem*, Financial Cryptography - FC'05, LNCS, Springer, 2005.

[9] T. Dimitriou. *A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks*,Proceedings of the IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks, SECURECOMM, 2005.

[10] N.J. Hopper and M. Blum. *Secure Human Identifcation Protocols*, in C. Boyd (ed.) Advances in Cryptology - ASIACRYPT 2001, Volume

2248, Lecture Notes in Computer Science, pp. 52–66, Springer-Verlag, 2001.

[11] J. Bringer, H. Chabanne, and E. Dottax. *HB++: a Lightweight Authentication Protocol Secure Against Some Attacks*, IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing SecPerU, 2006.

[12] Julien Bringer and Herve Chabanne. *Trusted-HB: a low-cost version of HB+ secure against man-in-the-middle attacks*. CoRR, abs/0802.0603, 2008.

[13] Julien Bringer, Herve Chabanne, and Emmanuelle Dottax. *HB++: a lightweight authentication protocol secure against some attacks*. In Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2006), 29 June 2006, Lyon, France, pages 28–33. IEEE Computer Society, 2006.

[14] Dang Nguyen Duc and Kwangjo Kim. *Securing HB+ against GRS man-in-the-middle attack*. In Institute of Electronics, Information and Communication Engineers, Symposium on Cryptography and Information Security, 2007.

[15] Henri Gilbert, Matthew J. B. Robshaw, and Yannick Seurin. *HB♯: Increasing the security and effciency of HB+*. Advances in Cryptology EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13–17, 2008. Proceedings, volume 4965 of Lecture Notes in Computer Science, pages 361–378.Springer, 2008.

[16] J. Munilla and A. Peinado. *HB-MP: A further step in the HB-family of lightweight authentication protocols.* Computer Networks, 2007.

[17] Mukundan Madhavan,Andrew Thangaraj,Yogesh Sankarasubramaniam and Kapali Viswanathan,*NLHB : A Non-Linear Hopper Blum Protocol*,IEEE National Conference on Communications (NCC),2010, CoRR abs/1001.2140:2010.

[18] M. Fossorier, M. Mihaljevi, H. Imai, Y. Cuiz, K. Matsuura. *A Novel Algorithm for Solving the LPN Problem and its Application to Security Evaluation of the HB Protocol for RFID Authentication*. Lecture Notes in Computer Science, vol. 4329, pp. 48–62, Dec. 2006.

[19] J. Carrijo, R. Tonicelli, H. Imai, and A. C. A. Nascimento, *A Novel Probabilistic Passive Attack on the Protocols HB and HB+, IEICE Trans-*

actions, pp. 658–662, 2009.

[20] A. Blum, A. Kalai and H. Wasserman, *Noise-Tolerant Learning, the Parity Problem, and the Statistical Query Model*, Journal of the ACM, vol. 50, no. 4, pp. 506–519, July 2003.

[21] H. Gilbert, M. Robshaw, and H. Sibert, *Active attack against HB+: A Provably-Secure Lightweight Authentication Protocol*, IEE Electronics Letters, vol. 41, no. 21, pp. 1169–1170, Oct. 2005.

[22] K. Ouafi, R. Overbeck, and S. Vaudenay, *On the Security of HB♯ against a Man-in-the-Middle Attack*, in Proceedings of ASIACRYPT 2008, ser. LNCS, vol. 5350. Springer, 2008, pp. 108–124.

[23] J. Katz and A. Smith, *Analyzing the HB and HB+ Protocols in the Large Error Case*, Available from http://eprint.iacr.org/2006/326.pdf.

[24] P. Chose, A. Joux and M. Mitton, *Fast Correlation Attacks: An Algorithmic Point of View*, EUROCRYPT2002, Lecture Notes in Computer Science, vol. 2332, pp. 209–221, 2002.

[25] E.R. Berlekamp, R.J. McEliece, and H.C.A. van Tilborg, *On the Inherent Intractability of Certain Coding Problems*, IEEE Trans. Info. Theory, vol. 24, pp. 384–386, 1978.

[26] A. Blum, M. Furst, M. Kearns, and R. Lipton, *Cryptographic Primitives Based on Hard Learning Problems*, CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 278–291, 1994.

[27] D. Wagner, *A Generalized Birthday Problem*, CRYPTO '02, Lecture Notes in Computer Science, vol. 2442, pp. 288–304, 2002.

[28] J. L. Massey and S. Serconek, *A Fourier Transform Approach to the Linear Complexity of Nonlinearly Filtered Sequences Advances in Cryptology*-CRYPTO 94, Springer, pp. 322–340, 1994.

PAPER II

II

PASSIVE CRYPTANALYSIS OF THE UNCONDITIONALLY SECURE AUTHENTICATION PROTOCOL FOR RFID SYSTEMS *

Mohammad Reza Sohizadeh Abyaneh

*Mohammad Reza Sohizadeh Abyaneh, "Passive Cryptanalysis of the UnConditionally Secure Authentication Protocol for RFID Systems", *International Conference on Information Security and Cryptology* (ICISC 2010) in Seoul, Korea.

PASSIVE CRYPTANALYSIS OF THE UNCONDITIONALLY SECURE AUTHENTICATION PROTOCOL FOR RFID SYSTEMS

Mohammad Reza Sohizadeh Abyaneh*

Abstract. Recently, Alomair et al. proposed the first *Un-Conditionally Secure* mutual authentication protocol for low-cost RFID systems(UCS-RFID). The security of the UCS-RFID relies on five dynamic secret keys which are updated at every protocol run using a fresh random number (nonce) secretly transmitted from a reader to tags.

Our results show that, at the highest security level of the protocol (security parameter= 256), inferring a nonce is feasible with the probability of 0.99 by eavesdropping(observing) about 90 runs of the protocol. Finding a nonce enables a passive attacker to recover all five secret keys of the protocol. To do so, we propose a three-phase probabilistic approach in this paper. Our attack recovers the secret keys with a probability that increases by accessing more protocol runs. We also show that tracing a tag using this protocol is also possible even with less runs of the protocol.

Key Words: RFID, Authentication Protocol, Passive Attack.

*Department of Informatics, University of Bergen

1 INTRODUCTION

As of today, RFID (Radio Frequency Identification) is referred to as the next technological revolution after the Internet. A typical RFID system involves a *reader*, a number of *tags*, which may range from the battery-powered, to the low-cost ones with even no internal power, and a *database*. RFID systems enable the identification of objects in various environments. They can potentially be applied almost everywhere from electronic passports[19, 20], contactless credit cards[18], to supply chain management[21–23].

Keeping RFID systems secure is imperative, because they are vulnerable to a number of malicious attacks. For low-cost RFID systems, security problems become much more challenging, as many traditional security mechanisms are inefficient or even impossible due to resource constraints. Some existing solutions utilize traditional cryptographic primitives such as hash or encryption functions, which are often too expensive to be implemented on low-cost RFID tags.

Another method of securing RFID systems has been the lightweight approach. These solutions base themselves on mostly lightweight operations (e.g. bitwise or simple arithmetic operations) instead of more expensive cryptographic primitives. The HB-family(HB^{+},HB^{++}, HB*,etc.) [1–7] and the MAP-family(LMAP,EMAP,M2AP,etc)[8–10] authentication protocols, are some examples of this kind. However, proposed lightweight protocols so far have been targeted to various successful attacks and therefore, the search for a concrete lightweight solution for authentication in low-cost RFID tags still continues.

Recently, Alomair et al. embarked on the notion of UnConditionally Secure mutual authentication protocol for RFID systems (UCS-RFID)[16]. UCS-RFID's security relies mainly on the freshness of five secret keys rather than the hardness of solving mathematical problems. Freshness in the keys is guaranteed with a *key updating* phase at every protocol run by means of a fresh random number (nonce). This nonce is generated at the reader side due to low-cost tags constraints, and delivered to the tag secretly. This allows the tags to benefit from the functionalities of random numbers without the hardware to generate them.

Our Contribution. In this paper, we present a three-phase probabilistic passive attack against the UCS-RFID protocol to recover all the secret keys in the protocol. Our attack is mainly based on a weakness observed in the protocol(section 3). To put in a nutshell, the weakness

implies that the more outputs we have from consecutive runs of the protocol, the more knowledge we will obtain on the nonces in these protocol runs. In other words, having more number of protocol run outputs observed, we are able to determine some of the nonces (*victim* nonces) with higher probability. It should be noted that this weakness has also been tackled by the authors in [16]. Nevertheless we will show that the security margin they expected from the protocol has been overestimated. Finding the victim nonce in the protocol paves the way toward adopting an attacking scenario to achieve all of the five secret keys in the system.

Outline. The remainder of this paper is organized as follows. In section 2, we briefly describe the UCS-RFID protocol. In section 3 the weakness of the protocol is investigated thoroughly. Section 4 and 5 describes our attacking scenario to recover the keys, and trace the tag in the protocol. Finally, section 6 concludes the paper.

2 Description of the UCS-RFID Protocol

The UCS-RFID authentication protocol consists of two phases: the *mutual authentication phase* and the *key updating phase*. The former phase mutually authenticates an RFID reader and a tag. In the latter phase both the reader and the tag update their dynamic secret keys for next protocol runs.

In this protocol, first the security parameter, N, is specified and a $2N$-bit prime integer, p, is chosen. Then, each tag T is loaded with an N-bit long identifier, $A^{(0)}$, and five secret keys, $k_a^{(0)}, k_b^{(0)}, k_c^{(0)}, k_d^{(0)}$ and $k_u^{(0)}$ chosen independently and uniformly from $\mathbb{Z}_{2^N}, \mathbb{Z}_p, \mathbb{Z}_p \backslash \{0\}, \mathbb{Z}_{2^N}$ and $\mathbb{Z}_p \backslash \{0\}$ respectively.

2.1 Notations

- N: security parameter.
- p: a prime number in $\mathbb{Z}_{2^N}$
- A^x, B^x, C^x, D^x: observable outputs of x^{th} protocol run
- $n = n_l || n_r$: random number in $\mathbb{Z}_{2^N}$
- n_l, n_r: left and right *half-nonces*

Specifications
- Public parameters: p, N.
- Secret parameters(shared between R and T): $k_a^{(0)}, k_b^{(0)}, k_c^{(0)}, k_d^{(0)}, k_u^{(0)}$.
Mutual Authentication Phase
(1) $R \Rightarrow T : Hello$
(2) $T \Rightarrow R : A^{(i)}$
(3) $R \Rightarrow T : B^{(i)}, C^{(i)}$
(4) $T \Rightarrow R : D^{(i)}$

Fig. 1: *i^{th} run of the mutual authentication phase in the UCS-RFID protocol*

2.2 Mutual Authentication Phase

Figure 1 shows one instance run of the mutual authentication phase in the UCS-RFID protocol. The reader starts the interrogation with a "Hello" message which is responded by tag's dynamic identifier $A^{(i)}$. The reader then looks up in the database for a set of five keys(k_a, k_b, k_c, k_d, and k_u) which corresponds to $A^{(i)}$. If this search is successful, it means that the tag is authentic. Having the tag authenticated, the reader generates a $2N$-bit random nonce $n^{(i)}$ uniformly drawn from $\mathbb{Z}_p^*$, calculates messages $B^{(i)}$, $C^{(i)}$ by (2),(3) and sends them to the tag.

$$A^{(i)} \equiv n_l^{(i-1)} + k_a^{(i)} \ mod \ 2^N \tag{1}$$

$$B^{(i)} \equiv n^{(i)} + k_b^{(i)} \ mod \ p \tag{2}$$

$$C^{(i)} \equiv n^{(i)} \times k_c^{(i)} \ mod \ p \tag{3}$$

The tag first checks the integrity of the received messages by (4):

$$(B^{(i)} - k_b^{(i)}) \times k_c^{(i)} \equiv C^{(i)} \ mod \ p \tag{4}$$

This check implies the authenticity of the reader as well. Then, the tag extracts the nonce $n^{(i)}$ by (5.)

$$n^{(i)} \equiv (B^{(i)} - k_b^{(i)}) \ mod \ p \tag{5}$$

To conclude the mutual authentication phase, the tag transmits $D^{(i)}$ as a receipt of obtaining $n^{(i)}$.

$$D^{(i)} = n_l^{(i)} \oplus k_d^{(i)} \tag{6}$$

2.3 KEY UPDATING PHASE

After a successful mutual authentication, both the reader and the tag update their keys and dynamic identifier ($A^{(i)}$) for the next protocol run.

$$k_a^{(i+1)} = n_r^{(i)} \oplus k_a^{(i)} \quad (7)$$

$$k_b^{(i+1)} \equiv k_u^{(i)} + (n^{(i)} \oplus k_b^{(i)}) \ mod \ p \quad (8)$$

$$k_c^{(i+1)} \equiv k_u^{(i)} \times (n^{(i)} \oplus k_c^{(i)}) \ mod \ p \quad (9)$$

$$k_d^{(i+1)} = n_r^{(i)} \oplus k_d^{(i)} \quad (10)$$

$$k_u^{(i+1)} \equiv k_u^{(i)} \times n^{(i)} \ mod \ p \quad (11)$$

$$A^{(i+1)} \equiv n_l^{(i)} + k_a^{(i+1)} \ mod \ 2^N \quad (12)$$

It should be noted that the dynamic values have been proved to preserve their properties of independency and uniformity after updating[16].

3 OBSERVATION

In this section, we shed more light on a weakness in the UCS-RFID protocol which becomes the origin of our proposed attack presented in the subsequent section. By xoring (7) and (10), we have:

$$k_a^{i+1} \oplus k_d^{i+1} = k_a^i \oplus k_d^i \quad (13)$$

Equation (13) shows that the difference between k_a and k_d remains the same for two consecutive runs of the protocol. This statement can also be generalized for every r arbitrary run of the protocol the as following:

$$k_a^{r+1} \oplus k_d^{r+1} = k_a^r \oplus k_d^r = \ldots = k_a^0 \oplus k_d^0 = L \quad (14)$$

By using (14), for outputs A and D in m consecutive runs of the protocol, we have:

$$A^{(i)} \equiv n_l^{(i-1)} + k_a^{(i)} \ mod\ 2^N \tag{15}$$

$$D^{(i)} = n_l^{(i)} \oplus (k_a^{(i)} \oplus L) \tag{16}$$

$$A^{(i+1)} \equiv n_l^{(i)} + (k_a^{(i)} \oplus n_r^{(i)}) \ mod\ 2^N \tag{17}$$

$$D^{(i+1)} = n_l^{(i+1)} \oplus (k_a^{(i)} \oplus L \oplus n_r^{(i)}) \tag{18}$$

$$\vdots$$

$$A^{(i+m-1)} \equiv n_l^{(i+m-2)} + (k_a^{(i)} \bigoplus_{j=i}^{i+m-2} n_r^{(j)}) \ mod\ 2^N \tag{19}$$

$$D^{(i+m-1)} = n_l^{(i+m-1)} \oplus (k_a^{(i)} \oplus L \bigoplus_{j=i}^{i+m-2} n_r^{(j)}) \tag{20}$$

It is apparent that we have a set of $2m$ equations with $2m+2$ variables. These variables can be divided into two groups:
1. $2m$ half-nonces: $n_l^{(i-1)}, \ldots, n_l^{(i+m-1)}, n_r^{(i)}, \ldots, n_r^{(i+m-2)}$
2. L and $k_a^{(i)}$.

So, if we fix the value of variables L and $k_a^{(i)}$, we end up with $2m$ equations and $2m$ half-nonce variables. This implies that the $2m$ half-nonces can not be chosen independently and fulfil the above equations simultaneously. In other words, if we observe the outputs of m consecutive runs of the protocol, it is only necessary to search over all possible sequences of $k_a^{(i)}$ and L, which is 2^{2N}, and then it will be possible to find all $2m$ half-nonces uniquely. As we will see, this weakness is the result of introduction of a tighter bound for the half-nonces while we keep observing more runs of the protocol.

By the randomness nature of the generated half-nonces, the total number of possible sequences for them(2^{2N}) is uniformly distributed over them. This implies that each of the $2m$ half-nonces is expected to have a bound of $\sqrt[2m]{2^{2N}}$ possible values (comparing to its previous bound which was N). Therefore, for m consecutive protocol runs, the total number of possible values distributed over the $2m$ half-nonces is $2m\sqrt[2m]{2^{2N}}$ [16].

Now, if we exclude the value which half-nonces has taken already ($2m\sqrt[2m]{2^{2N}} - 2m$), we can calculate the probability that at least one half-nonce does not receive another possible value (remains constant). To do

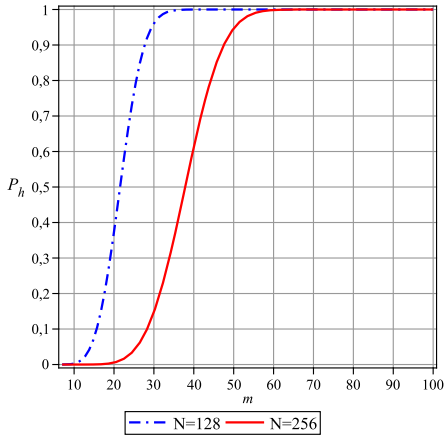

Fig. 2: *The number of consecutive protocol runs an adversary must observe(m) in order to infer at least one half-nonce for* $N = 128, 256$

so, we utilize the well-known problem in probability theory(i.e. Given r balls thrown uniformly at random at b bins, the probability that at least one bin remains empty which is calculated by (21))[17]:

$$\Pr(\text{at least one bin remains empty}) = 1 - \frac{\binom{r-1}{b-1}}{\binom{b+r-1}{b-1}} \tag{21}$$

Now, it only requires to substitute $b = 2m$ and $r = 2m.\sqrt[2m]{2^{2N}} - 2m$ in (21) and then we will have (22). The result is plotted in Figure 2.

$$P_h = \Pr(\text{at least one half-nonce remains constant}) = 1 - \frac{\binom{2m.\sqrt[2m]{2^{2N}}-2m-1}{2m-1}}{\binom{2m.\sqrt[2m]{2^{2N}}-1}{2m-1}} \tag{22}$$

Figure 2 shows the probability of inferring at least one half-nonce in terms of the number of consecutive runs of the protocol required to be observed to do so. For example, if we observe 35 runs of the protocol runs with N=256, we will be able to determine at least one of the 70 transmitted half-nonces with the probability of more than 0.99.

We will use the term "*victim* half-nonce" for inferred half-nonce and notation m_h instead of m for the number of consecutive runs of the protocol required to infer one half-nonce hereafter.

4 Our Attack Scenario

In the previous section, we presented a probabilistic approach to find the number of consecutive runs of the protocol to infer one half-nonce. But in our attack, we need to have a complete nonce(left and right corresponding half-nonces) to recover all secret keys. To achieve this goal, we propose an attacking scenario which consists of the three following phases:

1. Finding the total number of necessary consecutive runs of the protocol to find a complete victim nonce (m_t).
2. Finding the victim nonce.
3. Recovering the secret keys.

4.1 Phase I: Finding m_t

In section 3, we proposed a probabilistic way to calculate the number of consecutive runs that must be observed by an adversary to infer a half-nonce(m_h). It is obvious that if we keep observing more runs of the protocol(i.e. more than m_h), after each extra observation, another half-nonce can be inferred. This is simply possible by eliminating the two equations which contain the first victim half-nonce and adding two newly observed equations to the set of equations (15-20) and then, we again have $2m_h$ equations and $2m_h + 2$ variables which yield another half-nonce inference.

If we intend to find a complete nonce, we must continue observing the runs of the protocol until we infer two corresponding victim half-nonces to form a complete nonce. To do so, we should first calculate the probability that the inferred half-nonce at $(m_e + m_h)^{th}$ run matches one of the previously victim half-nonces.

As we know, after m_h runs of the protocol, we accomplish to find one victim half-nonce, after m_e extra runs of the protocol, we have $\beta = 2m_h + 2m_e$ equations and β half-nonces which $m_e + 1$ of them can be inferred. The probability that none of these $m_e + 1$ half-nonces match is:

$$\begin{aligned} \Pr(\text{Having no pair after } m_h + m_e \text{ runs}) &= \frac{(\beta-1)}{\beta} \times \ldots \times \frac{(\beta-m_e)}{\beta} \\ &= \frac{\prod_{i=1}^{m_e}(\beta-i)}{\beta^{(m_e)}} \end{aligned} \tag{23}$$

Consequently, the probability of having at least one pair after observing m_e runs is simply calculated by (24).

$$\begin{aligned} P_e &= \Pr(\text{Having at least one pair of matching half-nonces after } m_h + m_e \text{ runs}) \\ &= 1 - \frac{\prod_{i=1}^{m_e}(\beta - i)}{\beta^{(m_e)}} \end{aligned} \tag{24}$$

By using (22) and (24) the total number of protocol runs to have at least one complete victim nonce ($m_t = m_h + m_e$) can be calculated by (25) and is plotted in Figure 3.

$$\begin{aligned} P_t &= \Pr(\text{Having at least one complete nonce after } m_t \text{ runs}) \\ &= (P_e | m_h = h) \times Pr(m_h = h) = (P_e | m_h = h) \times P_h(h) \end{aligned} \tag{25}$$

Remark The authors of [16] have also calculated m_t by using some other protocol outputs (B and C). Figure 3 compares our results with what the authors "Expected". This comparison has been conducted for two different security parameters N=128,N=256 which are plotted on the left and right respectively.

The results show that the security margin of the protocol in terms of the number of consecutive runs that must be observed to infer one nonce is less than what the designers of the protocol expected. In other words, we need less number of protocol runs to infer at least one nonce. For example a passive adversary is able to infer a complete nonce with high probability of 0.99 by eavesdropping less that 60 and 90 runs of the protocol for the key size of 128 and 256 bits respectively. These numbers were expected to be 110 and 200 respectively.

4.2 Phase II: Finding the constant nonce

Having m_h consecutive runs of the protocol observed, we have one constant half-nonce or one half-nonce with only one possible value. In order to find this half-nonce, we adopt the following algorithm.

Algorithm Inputs :$A^{(i)}, \ldots, A^{(i+m_t-1)}, D^{(i)}, \ldots, D^{(i+m_t-1)}$

1. Determine a level of confidence(probability) for the final results.
2. Find the m_h, m_t related to the determined probability from Figures 1,2 respectively.
3. Calculate $m_e = m_t - m_h$

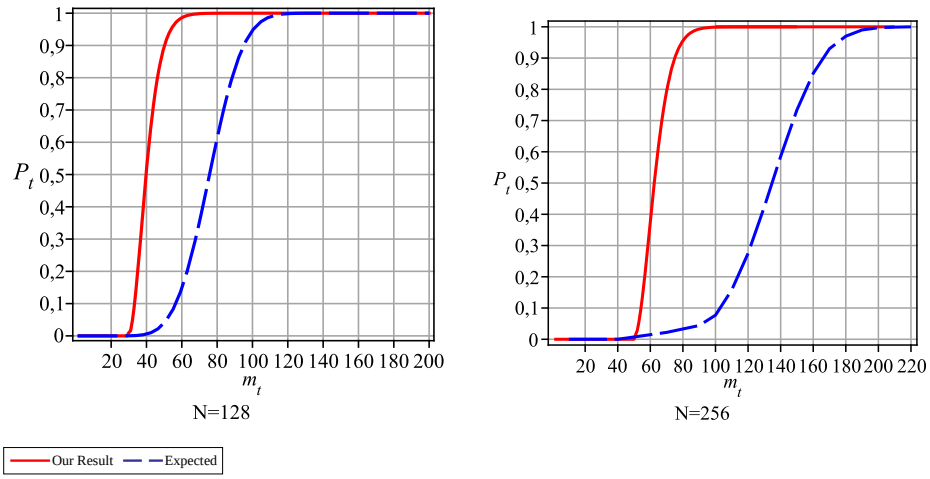

Fig. 3: *Comparison of expected security margin of the UCS-RFID protocol and our results in terms of the number of consecutive protocol runs an adversary must observe in order to infer at least one nonce.*

4. Choose two random numbers from $\mathbb{Z}_{2^N}$ and assign them to $L, k_a^{(i)}$ respectively.

5. Find $2m$ nonces $(n_l^{(i-1)}, \ldots, n_l^{(i+m_h-1)}, n_r^{(i)}, \ldots, n_r^{(i+m_h-2)})$ as follows.

   Find $n_l^{(i-1)}$ from (15) i.e. $n_l^{(i-1)} \equiv A^{(i)} - k_a^{(i)} \ mod\ 2^N$.

   Find $n^{(i)}$ from (16) i.e. $n_l^{(i)} = D^{(i)} \oplus (k_a^{(i)} \oplus L)$.

   Find $n_r^{(i)}$ from (17) i.e. $n_r^{(i)} \equiv (A^{(i+1)} - n_l^{(i)} \ mod\ 2^N) \oplus k_a^{(i)}$.

   $\vdots$

   Find $n_r^{(i+m_h-2)}$ from (19) i.e. $n_r^{(i+m_h-2)} \equiv (A^{(i+m_h-1)} - n_l^{(i+m_h-2)} \ mod\ 2^N) \oplus (k_a^{(i)} \bigoplus_{j=i}^{i+m_h-2} n_r^{(j)})$.

   Find $n_l^{(i+m_h-1)}$ from (20) i.e. $n_l^{(i+m_h-1)} = D^{(i+m_h-1)} \oplus (k_a^{(i)} \oplus L) \bigoplus_{j=i}^{i+m_h-2} n_r^{(j)}$.

6. Repeat 4 and 5 as many times as we observe that only one half-nonce keeps its value for all of the repetitions.
7. Save the constant(victim) half-nonce.
8. Observe another run of the protocol.
$$A^{(i+m_h)} \equiv n_l^{(i+m_h-1)} + (k_a^{(i)} \bigoplus_{j=i}^{i+m_h-1} n_r^{(j)}) \ mod\ 2^N$$
$$D^{(i+m_h)} = n_l^{(i+m_h)} \oplus (k_a^{(i)} \oplus L \bigoplus_{j=i}^{i+m_h-1} n_r^{(j)}).$$
9. Replace the equations corresponding to the found victim half-nonce with two newly observed equations in the equation set (15-20).
10. Repeat 4,5,6,7,8 for m_e times.
11. Match two corresponding victim half-nonces(e.g. $n_l^{(j)}, n_r^{(j)}$).
12. Output the victim nonce ($n^{(j)} = n_l^{(j)} || n_r^{(j)}$).

4.3 Phase III: Key Recovery

In the previous two phases of our attack, we accomplished to find a complete victim nonce $n^{(j)}$,with a certain probability, by observing m_t consecutive runs of the protocol. Now, we present how an adversary is able to recover all five secret keys of the protocol. To find $k_a^{(j)}, k_b^{(j)}, k_c^{(j)}$ and $k_d^{(j)}$, we should follow(26-29).

$$k_a^{(j)} \equiv (A^{(j+1)} - n_l^{(j)}) \oplus n_r^{(j)} mod\ 2^N \quad (26)$$
$$k_b^{(j)} \equiv B^{(j)} - n^{(j)}\ mod\ p \quad (27)$$
$$k_c^{(j)} \equiv (\frac{1}{n^{(j)}}\ mod\ p) \times C^{(j)}\ mod\ p \quad (28)$$
$$k_d^{(j)} = n_l^{(j)} \oplus D^{(j)} \quad (29)$$

To recover $k_u^{(j)}$, we need to find the nonce in the next run ($n^{(j+1)}$), thus we should calculate the updated keys for the $(j+1)^{th}$ run using (7) and (10).

$$k_a^{(j+1)} = k_a^{(j)} \oplus n_r^{(j)} \quad (30)$$
$$k_d^{(j+1)} = k_d^{(j)} \oplus n_r^{(j)} \quad (31)$$

Then we have:

$$n_l^{(j+1)} = D^{(j+1)} \oplus k_d^{(j+1)} \quad (32)$$

$$k_a^{(j+2)} = A^{(j+2)} \oplus n_l^{(j+1)} \quad (33)$$

Using (30) and (33), we can write:

$$n_r^{(j+1)} = k_a^{(j+2)} \oplus k_a^{(j+1)} \quad (34)$$

Finally, by using (27),(32) and,(34) we can find $k_u^{(j)}$.

$$k_u^{(j)} \equiv B^{(j+1)} - n^{(j+1)} - (k_b^{(j)} \oplus n^{(j+1)}) \ mod \ p \quad (35)$$

The procedure above provides us with our objective to recover all of the secret keys with a certain probability(P_t). This probability can be increased by paying the price of having more protocol run outputs available.

Furthermore, as it can be seen from the (32) and (34), next nonce is also achievable. This implies that the secret keys of the next run can also be calculated by using (26-35) for the next run. This is an ongoing procedure which yields the keys of any arbitrary run of the protocol(r) which $r > j$. Being able to generate the future secret keys, an adversary is capable of either impersonating both the reader and the tag or tracing the tag.

5 On the Traceability of the UCS-RFID

In the previous section, we presented a probabilistic key recovery attack against the UCS-RFID protocol. We mentioned that according to Figure 3, we need to have about 90 runs of the protocol to be almost sure that our found keys are correct. But with less number of protocol run outputs, we still can apply an attack against the traceability of the protocol. In this section, we formally investigate the *untraceability* of the UCS-RFID based on the formal description in [11].

5.1 Adversarial Model

According to [11], the means that are accessible to an attacker are the following: We denote a tag and a reader in i^{th} run of the protocol by $\mathcal{T}_i$ and $\mathcal{R}_i$, respectively.

- Query($\mathcal{T}_i, m_1, m_3$): This query models the attacker $\mathcal{A}$ sending a message m_1 to the tag and sending the m_3 after receiving the response.
- Send($\mathcal{R}_i, m_2$): This query models the attacker $\mathcal{A}$ sending a message m_2 to the Reader and being acknowledged.
- Execute($\mathcal{T}_i, \mathcal{R}_i$): This query models the attacker $\mathcal{A}$ executing a run of protocol between the Tag and Reader to obtain the exchanged messages.
- Reveal($\mathcal{T}_i$): This query models the attacker $\mathcal{A}$ obtaining the information on the Tag's memory.

A *Passive Adversary*, $\mathcal{A}_\mathcal{P}$, is capable of eavesdropping all communications between a tag and a reader and accesses only to the Execute($\mathcal{T}_i, \mathcal{R}_i$): .

5.2 Attacking Untraceability

The result of application of an oracle for a passive attack $\mathcal{O}_\mathcal{P} \subseteq \{Execute(.)\}$ on a tag T in the run i is denoted by $w_i(T)$. Thus, a set of I protocol run outputs, $\Omega_I(T)$, is:
$\Omega_I(T) = \{w_i(T)|i \in I\}; I \subseteq N$;($N$ denotes the total set of protocol runs).
The formal description of attacking scenario against untraceability of a protocol is as following:
1. $\mathcal{A}_\mathcal{P}$ requests the *Challenger* to give her a target T.
2. $\mathcal{A}_\mathcal{P}$ chooses I and calls $Oracle(T, I, \mathcal{O}_\mathcal{P})$ where $|I| \leq l_{ref}$ receives $\Omega_I(T)$.
3. $\mathcal{A}_\mathcal{P}$ requests the *Challenger* thus receiving her challenge T_1, T_2 ,$I_1$and I_2
4. $\mathcal{A}_\mathcal{P}$ calls $Oracle(T_1, I_1, \mathcal{O}_\mathcal{P})$, $Oracle(T_2, I_2, \mathcal{O}_\mathcal{P})$ then receives $\Omega_{I_1}(T_1)$, $\Omega_{I_2}(T_2)$.
5. $\mathcal{A}_\mathcal{P}$ decides which of T_1 or T_2 is T, then outputs her guess T'.

For a security parameter,k, if $Adv^{UNT}_{\mathcal{A}_\mathcal{P}}(k) = 2Pr(T' = T) - 1 > \epsilon$ then we can say that the protocol is traceable.

For UCS-RFID case, as Figure 3 implies, an adversary $\mathcal{A}_\mathcal{P}$ needs only to access to about 40 and 65 consecutive runs of the protocol to be able to determine $n^{(j)}$ with a probability of more than 0.5 (e.g. 0.6) for k =128 and 256 respectively and then according to section 4.3, she will

be able to recover the keys of subsequent runs. After, key recovery, the adversary can easily distinguish a target tag with any other challenge tag given by the challenger. So we have:
$\forall l_{ref} \geq 40$, $Adv^{UNT}_{\mathcal{A}_\mathcal{P}}(128) = 2Pr(T' = T) - 1 = 0.1 > \epsilon$.
$\forall l_{ref} \geq 65$,$Adv^{UNT}_{\mathcal{A}_\mathcal{P}}(256) = 2Pr(T' = T) - 1 = 0.1 > \epsilon$.

6 Conclusions

The design of suitable lightweight security protocols for low-cost RFID tags is still a big challenge due to their severe constraints. Despite of interesting proposals in the literature, this field still lacks a concrete solution.

Recently, Alomair *et al* have proposed the first authentication protocol based on the notion of unconditional security. Regardless of some inefficiencies in UCS-RFID authentication protocol, such as: large key sizes, using modular multiplication ,etc ,which makes this protocol an unsuitable nominate for low-cost RFID tag deployment, we presented a passive attack which showed that even the security margin which was expected to be yielded by UCS-RFID has also been overestimated.

In our attack, we showed that a passive adversary is able to achieve the all secret keys of the system with a high probability of 0.99 by eavesdropping less that 60 and 90 runs of the protocol for the key size of 128 and 256 bits respectively. Tracing the tag in the protocol is also feasible even by less number of runs of the protocol (e.g. 40, 65).

Our results suggest a major rethink in the design of the authentication protocols for RFID systems based on unconditional security notion. Drastic changes are necessary to fulfil both technological constraints and security concerns in RFID systems.

References

[1] N.J. Hopper and M. Blum. : Secure Human Identifcation Protocols , in C. Boyd (ed.) Advances in Cryptology - ASIACRYPT 2001, Volume 2248, Lecture Notes in Computer Science, pp. 52–66, Springer-Verlag, (2001).

[2] J. Bringer, H. Chabanne, and E. Dottax.: HB++: a Lightweight Authentication Protocol Secure Against Some Attacks, IEEE International Conference on Pervasive Services, Workshop on Security,

Privacy and Trust in Pervasive and Ubiquitous Computing SecPerU, (2006).

[3] Julien Bringer and Herve Chabanne.: Trusted-HB: a low-cost version of HB+ secure against man-in-the-middle attacks. CoRR, abs/0802.0603, (2008).

[4] Julien Bringer, Herve Chabanne, and Emmanuelle Dottax.: HB++: a lightweight authentication protocol secure against some attacks, In Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2006), pages 28–33. IEEE Computer Society, (2006).

[5] Dang Nguyen Duc and Kwangjo Kim.: Securing HB+ against GRS man-in-the-middle attack, In Institute of Electronics, Information and Communication Engineers, Symposium on Cryptography and Information Security, (2007).

[6] Henri Gilbert, Matthew J. B. Robshaw, and Yannick Seurin: HB♯: Increasing the security and effciency of HB+, Advances in Cryptology EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings, volume 4965 of Lecture Notes in Computer Science, pages 361–378.Springer, (2008).

[7] J. Munilla and A. Peinado.: HB-MP: A further step in the HB-family of lightweight authentication protocols. Computer Networks, (2007).

[8] Peris-Lopez, Hernandez-Castro,Estevez Tapiador, and Ribagorda: LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags , RFIDSec 06, (2006).

[9] P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda: M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags, in International Conference on Ubiquitous Intelligence and Computing (UIC06), vol. 4159 of LNCS, pp.912–923 (2006).

[10] P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda: EMAP: An Efficient Mutual-Authentication Protocol for Low-cost RFID tags , in OTM Federated Conferences and Workshop: IS Workshop, (2006).

[11] Avoine G. :Adversarial Model for Radio Frequency Identification. Cryptology ePrint Archive, Report 2005/049, (2005).

[12] M. Ohkubo, K. Suzuki, and S. Kinoshita: Cryptographic Approach to Privacy-Friendly Tags, in RFID Privacy Workshop, (2003).

[13] D. Henrici, and P. Muller: Hash-based Enhancement of Location Privacy for Radio Frequency Identification Devices using Varying Identifiers, in Proceedings of PerSec04,IEEE PerCom, pp.149-153, (2004).

[14] D. Henrici, and P. Muller: Providing Security and Privacy in RFID Systems Using Triggered Hash Chains, in PerCom'08, 50–59, (2008).

[15] L.S. Kulseng: Lightweight Mutual Authentication, Owner Transfer, and Secure Search Protocols for RFID Systems , Master Thesis, Iowa State University,Ames, (2009).

[16] B. Alomair, L. Lazos , R. Poovendran: Securing Low-cost RFID Systems: an Unconditionally Secure Approach , RFIDsec'10 Asia, Singapore, (2010).

[17] W. Feller: An Introduction to Probability Theory and its Applications, Wiley India Pvt. Ltd., (2008).

[18] T.S. Heydt-Benjamin, D.V. Bailey, K. Fu, A. Juels, and T. O'Hare: Vulnerabilities in First-Generation RFID-Enabled Credit Cards, Proc. 11th Int'l Conf. Financial Cryptography and Data Security (FC '07), pp. 2–14, (2007).

[19] D.Carluccio, K.Lemke, C.Paar: E-passport: The Global Traceability or How to feel like a UPS package, Proceeding of WISA'06, LNCS 4298, Springer, pp.391–404, (2007).

[20] J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R.W. Schreur, Crossing Borders: Security and Privacy Issues of the European e-Passport, Proc. First Int'l Workshop Security (IWSEC '06), pp.152–167 (2006).

[21] CASPIAN, Boycott Benetton: http://www.boycottbenetton.com (2007).

[22] Mitsubishi Electric Asia Switches on RFID: www.rfidjournal.com/article/articleview/2644/ (2006).

[23] Target, Wal-Mart Share EPC Data: http://www.rfidjournal.com/article/articleview/642/1/1/ (2005).

PAPER III

SECURITY ANALYSIS OF TWO DISTANCE-BOUNDING PROTOCOLS *

Mohammad Reza Sohizadeh Abyaneh

III

*Mohammad Reza Sohizadeh Abyaneh, "Security Analysis of two Distance-Bounding Protocols", *Workshop on RFID Security and Privacy* (RFIDSec 2011) in Amherst, Massachusetts, USA.

SECURITY ANALYSIS OF TWO DISTANCE-BOUNDING PROTOCOLS

Mohammad Reza Sohizadeh Abyaneh*

Abstract. In this paper, we analyze the security of two recently proposed distance bounding protocols called the "Hitomi" and the "NUS" protocols. Our results show that the claimed security of both protocols has been overestimated. Namely, we show that the Hitomi protocol is susceptible to a full secret key disclosure attack which not only results in violating the privacy of the protocol but also can be exploited for further attacks such as impersonation, mafia fraud and terrorist fraud attacks. Our results also demonstrates that the probability of success in a distance fraud attack against the NUS protocol can be increased up to $(\frac{3}{4})^n$ and even slightly more, if the adversary is furnished with some computational capabilities.

Keywords: RFID, Privacy, Distance bounding protocol, Distance fraud

1 INTRODUCTION

Radio frequency identification (RFID) technology is widely being deployed today in many applications which require security, such as payment and access control applications. Although many solutions have been proposed to secure RFID systems, most of them are still susceptible to different attacks related to location such as: *distance fraud, mafia fraud* and *terrorist fraud* attacks. All of these attacks aim at suggesting a wrong assumption of the distance between a tag and a reader.

*Department of Informatics, University of Bergen

In distance fraud attack, a tag operates from out of the range where it is supposed to be. Mafia fraud attack, is a kind of man-in-the-middle attack in which a rogue tag circumvents the security mechanisms by getting right answers from the legitimate tag via a rogue reader, while both legitimate entities (legitimate reader and tag) remain unaware. In the terrorist attack, a legitimate tag colludes with the adversary, giving her the necessary information to access the system by impersonating it for a limited number of times.

The described attacks require simpler technical resources than tampering or cryptanalysis, and they cannot be prevented by ordinary security protocols that operate in the high layers of the protocol stack. The main countermeasure against these attacks is the use of *distance bounding* protocols, which verify not only that the tag knows the cryptographic secret, but also that is within a certain distance. To achieve this goal, distance bounding protocols must be tightly integrated into the physical layer [1].

In 1993, Brands and Chaum proposed the first distance bounding protocol [5]. Afterward, in 2005, Hancke and Kuhn [6] proposed the first distance-bounding protocol dedicated to RFID systems. This protocol has the drawback of giving the adversary this chance to succeed with the probability of $(\frac{3}{4})^n$ rather than $(\frac{1}{2})^n$ in distance and mafia fraud attacks, where n is a security parameter. Since then, there have been many solutions proposed either similar to Hancke and Kuhn [2, 7, 8, 10–12] or with different structures [5, 8, 9, 13–15]. However, they mostly have something in common; they all consist of three phases, the first and the last ones called *slow phases*, and the second one called the *fast phase*. The round trip time (RTT) of a bitwise challenge and response is measured n times during the fast phase to estimate the distance, while the slow phases include all the time-consuming operations.

Recently, two distance bounding protocols have been proposed by Lopez *et al* and Gürel *et al* called Hitomi [4] and Non-Uniform Stepping (NUS) [15] distance bounding protocols respectively. These protocols are claimed to provide privacy and resistance against distance, mafia and terrorist fraud attacks.

Our Contribution. In this paper, we apply a key disclosure attack to the Hitomi protocol and a distance fraud attack on the NUS protocol. Our analysis is framed in the formal framework introduced in [16].

Outline. The remainder of this paper is organized as follows. Section 2 includes a succinct description of the framework we do our security analysis within. In Sections 3, we describe the Hitomi protocol, its

security claims and our key disclosure attack on it. In Section 4, we explain the NUS protocol and explain our distance fraud attack against it, and finally, Section 5 concludes the paper.

2 PRELIMINARIES

See Section 5.2.3 of the thesis.

2.1 NOTATIONS

Here, we explain the notations used hereafter.

- x: Secret key of the tag.
- $f_x(.)$: Pseudo-Random Function operation with secret key x.
- $hw(.)$: Hamming Weight calculation function.
- N_R, N_T: Random numbers generated by the reader and the tag respectively.
- n: The length of registers considered as a security parameter.

2.2 ASSUMPTIONS

The protocols described in this paper are executed under following assumptions:

- The tag and the reader share a long-term secret key x.
- Each tag has a unique identifier ID.
- The tag's capabilities supports a Pseudo-Random Function (f) and can perform bitwise operations.
- The reader and the tag agree on:
  - a security parameter n.
  - a public pseudo random function f with length of n bits.
  - a timing bound t_{max}
  - a fault tolerance threshold τ.

3 THE HITOMI PROTOCOL

3.1 DESCRIPTION

As stated in Section 1, being a distance bounding protocol, the Hitomi protocol (Figure 1) consists of three phases, two *slow phases* which are carried out at the first and final part of the protocol called *preparation phase* and *final phase* respectively. And the fast phase which is executed in between, called *rapid bit exchange phase*.

In the preparation phase, the reader chooses a random nonce (N_R) and transmits it to the tag. In return, the tag chooses three random numbers N_{T_1}, N_{T_2} and N_{T_3} and computes two temporary keys (k_1 and k_2) as (1) and (2).

$$k_1 = f_x(N_R, N_{T_1}, W) \tag{1}$$

$$k_2 = f_x(N_{T_2}, N_{T_3}, W') \tag{2}$$

where W and W' represent two constant parameters. By using these keys, the tag splits its permanent secret key x into two shares as *response registers*(i.e. $R^0 = k_1$ and $R^1 = k_2 \oplus x$). Finally, the tag transmits the 3-tuple $\{N_{T_1}, N_{T_2}, N_{T_3}\}$ to the reader.
The rapid bit exchange phase is a challenge and response phase with n rounds. In its i^{th} round, the reader generates a random challenge bit c_i and sends it to the tag while initializing a clock to zero. The tag receives c_i' which may not be equal to c_i due to errors or alterations in the channel. Immediately upon receiving c_i', the tag responses with $r_i' = R_i^{c_i}$. The reader stops the clock after receiving r_i, which may not be equal to r_i' due to errors or alterations in the channel, and computes the round trip time (RTT) of this challenge and response transaction and stores it as Δt_i.

The final phase starts with computing and sending two following messages from the tag to the reader.

$$m = \{c_1', ..., c_n', r_1', ..., r_n'\} \tag{3}$$

$$t_B = f_x(m, ID, N_R, N_{T_1}, N_{T_2}, N_{T_3}) \tag{4}$$

Finally, the reader computes three kinds of errors and checks whether their summation is below a fault tolerance threshold as following.

- *errc*: the number of times that $c_i \neq c_i'$.
- *errr*: the number of times that $c_i = c_i'$ but $r_i \neq R_i^{c_i}$.

- *errt*: the number of times that $c_i = c'_i$ but the response delay Δt_i is more than a timing bound threshold $t_{max}(\Delta t_i > t_{max})$.

If the reader authentication is also demanded, the reader computes $t_A = f_x(N_R, k_2)$ and transmits it to the tag. Once the tag checks its correctness, the two entities are mutually authenticated.

The authors claim that the Hitomi protocol provides mutual authentication between the tag and the reader and also guarantees privacy protection. The authors argue that the success probability of the mafia and distance fraud attacks against their scheme is bounded by $(\frac{1}{2})^n$.

3.2 Key Disclosure Attack

In this section, we present an attacking scenario to the Hitomi protocol which leads to tag's secret key disclosure. Our main assumption in this attack is that the reader authentication is not demanded and so the protocol is executed without the optional message t_A. This allows an unauthorized reader(adversary) to query the tag several times without being detected.

Algorithm 1 portrays how an adversary is able to extract Δ bits of the tag's secret key by querying the tag m times.

The algorithm starts with the preparation phase in which at mth run, the adversary first generates a new random number N_R, sends it to the tag and receives the 3-tuple of $\{N_{T_1}, N_{T_2}, N_{T_3}\}$ in return.
The rapid bit exchange phase of the algorithm starts with generation of a challenge vector by the adversary which contains Δ bits of 1 and $n - \Delta$ bits of 0 ($c^{(m)}$). By sending the bits of this challenge vector to the tag in n rounds of the rapid bit exchange phase and receiving the responses, the adversary obtains $n - \Delta$ bits of $R^0 = k_1$ and Δ bits of $R^1 = k_2 \oplus x$.

We know that if the adversary is able to find k_1, she will be able to calculate k_2 by (2). Now, the adversary requires to search over all possible 2^Δ values for k_1. If we observe the output of $f_{k_1}(N_{T_2}^{(m)}, N_{T_3}^{(m)}, W')$ in the mth run of the protocol for 2^Δ times, each time with one different possible value of k_1, we will see that the number of values for the first Δ bits of k_2 ($k_{2(1)}, ..., k_{2(\Delta)}$) is less than 2^Δ. This can be calculated by a well-known problem in probability theory described in Remark 1.

Each k_2 nominates one $X_\Delta = (x_{(1)}, ..., x_{(\Delta)})$ for Δ bits of the tag's secret key (Line 16 of the Algorithm 1). So, each time the adversary queries the tag, she will obtain a set of potential candidates for X_Δ.

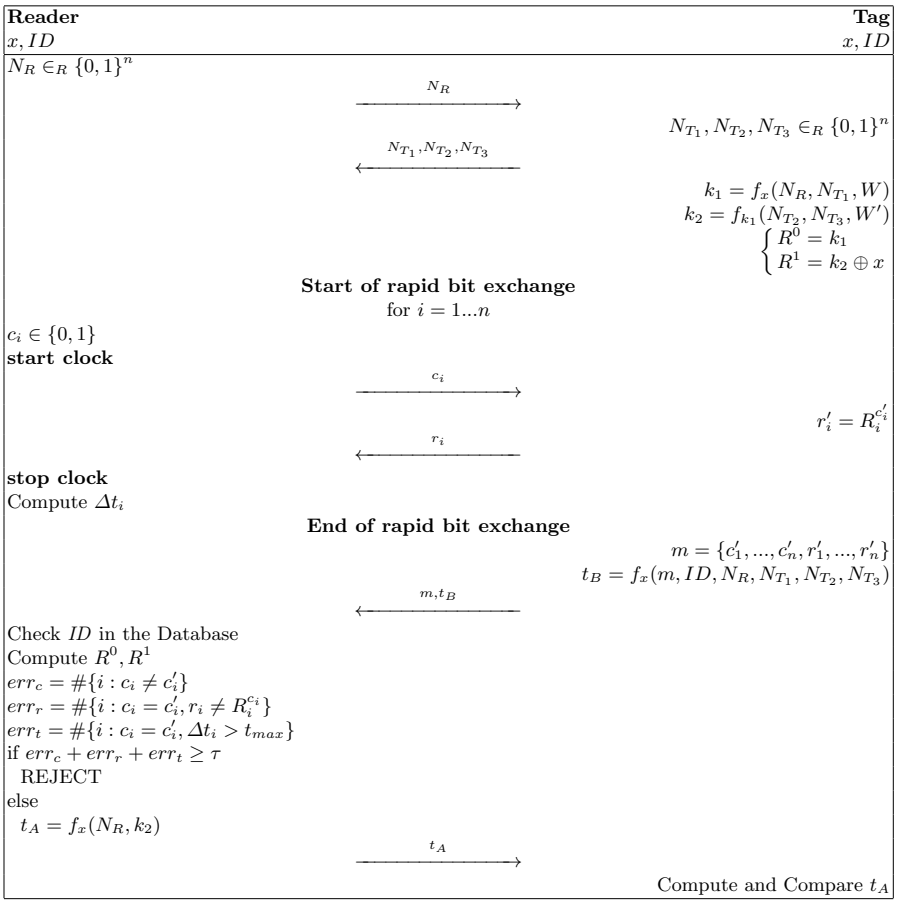

Fig. 1: *Hitomi Distance Bounding Protocols.*

If she continues querying the tag, each time she will obtain a set of different candidates.
These candidates can be removed from the list by further querying, unless they are nominated in the other runs. And the final candidate is the one which has been in the candidate list in all the queries. The number of times that the adversary must query the tag to be left with only one candidate is calculated by (7) and plotted in Figures 2 and 3.

Remark 1. Consider the process of tossing b balls into b bins. The tosses are uniformly at random and independent of each other. The

Algorithm 1 Δ bit secret key disclosure

Inputs: n, Δ, W, W'

Outputs: m, Δ bits of secret key x $(x_1, ..., x_\Delta)$

1: $m \leftarrow 1$ {number of required runs of the protocol}
2: **repeat**
3: $NumberofCandidates \leftarrow 0$
4: $FinalCandidate \leftarrow 0$
5: $\{counter(1), ..., counter(2^\Delta)\} \leftarrow \{0x0, ..., 0x0\}$
6: $\{CandidateFlag(1), ..., CandidateFlag(2^\Delta)\} \leftarrow \{0x0, ..., 0x0\}$
7: Generate $N_R^{(m)}$ and Send to the tag.
8: Receive $N_{T_1}^{(m)}, N_{T_2}^{(m)}, N_{T_3}^{(m)}$
9: $c^{(m)} \leftarrow (\underbrace{1, ..., 1}_{\Delta}, \underbrace{0, ..., 0}_{n-\Delta})$
10: send the challenges to the tag in n rounds and receive the responses.
11: $r^{(m)} \leftarrow (r_{(1)}^{(m)}, ..., r_{(n)}^{(m)})$
12: $(k_{1(\Delta+1)}, ..., k_{1(n)}) \leftarrow (r_{(\Delta+1)}^{(m)}, ..., r_{(n)}^{(m)})$
13: **for** $i = 0$ **to** $2^\Delta - 1$ **do**
14: $(k_{1(1)}, ..., k_{1(\Delta)}) \leftarrow Decimal2Binary(i)^*$
15: $(k_{2(1)}, ..., k_{2(n)}) \leftarrow f_{k_1}(N_{T_2}^{(m)}, N_{T_3}^{(m)}, W')$
16: $(x_{(1)}, ..., x_{(\Delta)}) \leftarrow (k_{2(1)}, ..., k_{2(\Delta)}) \oplus (r_{(1)}^{(m)}, ..., r_{(\Delta)}^{(m)})$
17: $l \leftarrow Binary2Decimal(x_{(1)}, ..., x_{(\Delta)})^{**}$
18: **if** $CandidateFlag(l) = 0$ **then**
19: $counter(l) \leftarrow counter(l) + 1$
20: $CandidateFlag(l) \leftarrow 1$
21: **end if**
22: **end for**
23: **for** $j = 1$ **to** 2^Δ **do**
24: **if** $counter(j) = m$ **then**
25: $NumberofCandidates \leftarrow NumberofCandidates + 1$
26: $FinalCandidate \leftarrow j$
27: **end if**
28: **end for**
29: $m \leftarrow m + 1$
30: **until** $NumberofCandidates = 1$
31: $(x_{(1)}, ..., x_{(\Delta)}) \leftarrow Decimal2Binary(FinalCandidate)$
32: **return** $m, (x_{(1)}, ..., x_{(\Delta)})$

* Decimal2Binary(.) outputs the binary representation of a given decimal number.

** Binary2Decimal(.) outputs the decimal representation of a given binary number.

probability of not falling any ball into a particular bin can be calculated by (5) [17].

$$\Pr(\text{one particular bin remains empty}) = p_0 = \left(1 - \frac{1}{b}\right)^b \approx \frac{1}{e},\ b \gg 1 \tag{5}$$

Hence, the probability that a ball does not remain empty is simply $p_1 = 1 - p_0$. Due to independency, if we repeat the same experiment for m trials, the probability that one particular bin remains empty at least in one of m trials is $1 - p_1^m$. Now, we can calculate the probability that all bins experience to be empty at least in one of m trials ($Pr(Success)$) by (6).

$$\begin{aligned} Pr(Success) &= (1 - p_1^m)^b = \left(1 - \left(1 - \left(1 - \frac{1}{b}\right)^b\right)^m\right)^b \\ &\approx \left[1 - \left(1 - \frac{1}{e}\right)^m\right]^b,\ b \gg 1 \end{aligned} \tag{6}$$

For our problem it is only required to substitute b with 2^Δ and we will have:

$$P_{Succ} = Pr(Success) = \left(1 - \left(1 - \left(1 - \frac{1}{2^\Delta}\right)^{2^\Delta}\right)^m\right)^{2^\Delta} \tag{7}$$

Figure 2 illustrates the probability of success calculated in (7) while the number of protocol runs are increased. The figures have been plotted for $\Delta = 4$,8,16 and 32, which should be chosen according to computational constraints. So far, we have accomplished to find the first Δ bits of the tag's secret key with a certain probability. In a similar vein, one can find other bits of the secret key by choosing a different challenge vector (e.g. for finding $(x_{(\Delta+1)}, ..., x_{(2\Delta)})$ the challenge should be chosen like (8) and the above algorithm should be executed another time).

$$c = (\underbrace{0, ..., 0}_{\Delta}, \underbrace{1, ..., 1}_{\Delta}, \underbrace{0, ..., 0}_{n-2\Delta}) \tag{8}$$

In this way, the adversary accomplishes to find the whole tag's secret key, if she can query the tag for enough times. Figure 3 illustrates the number of runs of the protocol which an adversary must query the tag and its probability of success to find the entirety of tags's secret

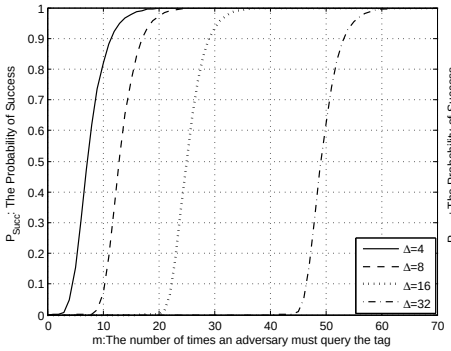

Fig. 2: *Adversary success probability to find Δ bits of the secret key.*

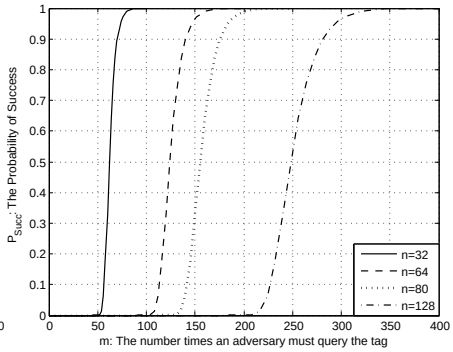

Fig. 3: *Adversary success probability to find the whole secret key for* $\Delta = 16$.

key, assuming that her computational capability is limited to $2^{\Delta} = 2^{16}$ computations. The computations include: searching over 2^{Δ} values of k_1, finding k_2 for each k_1 and candidate one X_{Δ}.
The graphs have been plotted for four different key sizes $n = 32$, 64, 80 and 128. For instance, the adversary is required to query the tag about 70, 140, 175 and 280 times to find the tag's secret keys of size 32, 64, 80 and 128 bits with the probability of about 0.9 respectively.

It is obvious that having this attack accomplished, the adversary is able to easily either track or impersonate the tag in further interrogations. The information elicited in this attack also paves the way for performing other attacks such as mafia or terrorist fraud attacks.

4 The NUS Protocol

4.1 Description

The NUS protocol (Figure 4) also consists of three phases, two *slow phases* a fast called *rapid bit exchange phase*.
In the first slow phase, the reader chooses a random nonce(N_R) and transmits it to the tag. In return, the tag chooses another random number(N_T) and computes the response register $R = f_x(N_R, N_T)$, which is of length $2n$. The tag then initializes the variables $j1, j2, k1$ and $k2$ to $1, n, 0$ and $2n + 1$ respectively and sends back N_T to the reader.

In the i^{th} round of the rapid bit exchange phase, the reader generates a random challenge bit c_i and sends it to the tag while initializing a clock to zero. The tag receives c_i' which may not be equal to c_i due to errors or alterations in the channel. Immediately upon receiving c_i', the tag sends the bit r_i', computed according to the procedure shown in Figure 4.

The final phase concludes with sending the message m which consists of all challenges the tag has received, from the tag to the reader and finally, the error computation which is almost the same as in the Hitomi protocol.

The authors claim that the success probability of the distance, mafia and terrorist fraud attacks against the NUS protocol is bounded by $(\frac{1}{2})^n$.

4.2 Distance fraud attack

In this section, we present a distance fraud attack on the NUS protocol in two different forms in white-box model: *restricted adversary* and *powerful adversary*. The main assumption we have is that the adversary is located at zone Z_1, i.e. at the i^{th} round of the rapid bit exchange phase, the adversary accesses to the value of the challenge bit in previous round c_{i-1}, before generating current response r_i. This assumption implies that the adversary is able to update the registers $j1, j2, k1$ and $k2$ and she is aware of their correct current values, before she generates the response.

Restricted adversary
The adversary is allowed to run only once the pseudo-random function f function to compute R and observe its content before any response. The probability of success for the distance fraud attack in this model can be calculated by (9).

$$\begin{aligned} P_{dis} &= Pr(\text{Success}|x_{j1}x_{j2} = 00)Pr(x_{j1}x_{j2} = 00) \\ &+ Pr(\text{Success}|x_{j1}x_{j2} = 01)Pr(x_{j1}x_{j2} = 01) \\ &+ Pr(\text{Success}|x_{j1}x_{j2} = 10)Pr(x_{j1}x_{j2} = 10) \\ &+ Pr(\text{Success}|x_{j1}x_{j2} = 11)Pr(x_{j1}x_{j2} = 11) \end{aligned} \tag{9}$$

If $x_{j1}x_{j2} = 00$ and without knowing c_i, the adversary should anticipate the right response(r_i) between R_{k1+1} and R_{k2-1}. Let us define the probability of equality of these two bits by (10).

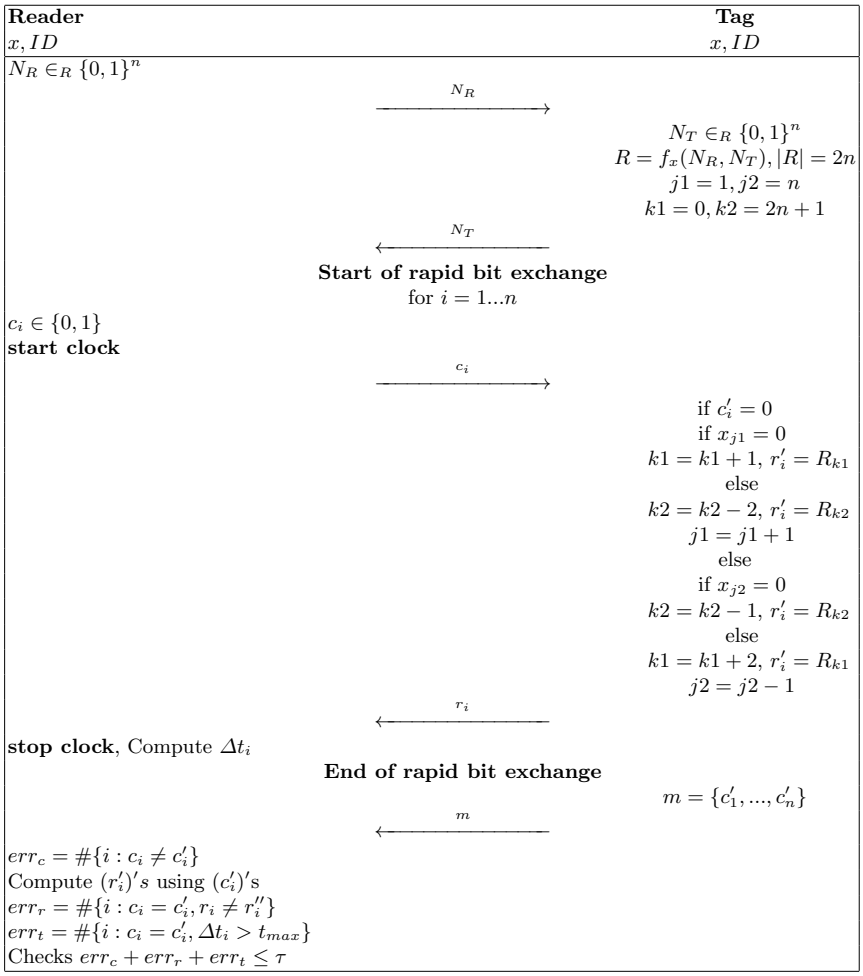

Fig. 4: *The NUS Distance Bounding Protocol*

$$P_{eq} = \Pr(R_{k1+1} = R_{k2-1}) \tag{10}$$

So, we have,

$$\begin{aligned} Pr(\text{Success}|x_{j1}x_{j2} = 00) &= Pr(\text{Success}|x_{j1}x_{j2} = 00, R_{k1+1} = R_{k2-1})(P_{eq}) \\ &+ Pr(\text{Success}|x_{j1}x_{j2} = 00, R_{k1+1} \neq R_{k2-1})(1 - P_{eq}) \end{aligned}$$

If $R_{k1+1} = R_{k2-1}$, the adversary can simply outputs either of these two bits and succeeds with the probability 1. Otherwise, she outputs a random bit and she will have the success probability of $\frac{1}{2}$. So,

$$Pr(\text{Success}|x_{j1}x_{j2} = 00) = 1 \times P_{eq} + \frac{1}{2} \times (1 - P_{eq}) = \frac{(1 + P_{eq})}{2} \quad (11)$$

We can do similar calculations for other three possibilities of $x_{j1}x_{j2}$. Since all four possibilities of $x_{j1}x_{j2}$ are equally likely, we have the probability of success for a distance fraud attack in one round as (12).

$$P_{dis} = \frac{(1 + P_{eq})}{2} \quad (12)$$

In a similar vein, one can show that due to independency of the n rounds, the adversary obtains the success probability of $(\frac{1+P_{eq}}{2})^n$ for n rounds. If we assume that zeros and ones are equally likely, P_{eq} equals to $\frac{1}{2}$ and for n rounds we have:

$$P_{dis} = (\frac{3}{4})^n \quad (13)$$

Powerful adversary

Our main assumptions in this attack are as following. We assume that, there is a 1-second latency between the preparation and rapid bit exchange phases of the protocol. It implies that the adversary can run the pseudo-random function f for c times between the preparation and the rapid bit exchange phases, where c the number of a simple random number function like a hash function that can be computed per second on a single PC [16].

In [16], Avoine *et al* has presented an instance of a distance fraud attack against a white-box-modeled tag in Hancke and Kuhn protocol. They have devoted the white-box modeled tag's capabilities to minimize the hamming weight difference of n-bit response registers in the Hancke and Kuhn protocol($hw(R^0 \oplus R^1)$). They have proved that if $P_i = Pr(success|(hw(R^0 \oplus R^1) = i))$, the probability of success in the distance fraud attack can be calculated by (14).

$$P_{dis} = \left(\frac{1}{2}\right)^{cn} \times \left(\sum_{i=0}^{i=n-1} (P_i) \left[\left(\sum_{j=i}^{j=n} \binom{n}{j} \right)^c - \left(\sum_{j=i+1}^{j=n} \binom{n}{j} \right)^c \right] + 1 \right) \quad (14)$$

	n=32	n=64	n=80	n=128
Claimed Security	2.3283E-10	5.4210E-20	8.2718E-25	2.9387E-39
Restricted Adversary	1.0045E-4	1.0090E-8	1.0113E-10	1.0183E-16
Powerful Adversary	0.0035	4.5101E-7	4.7459E-9	5.1498E-15

Table 1: *Comparison of the probability of success for distance fraud attack against the NUS protocol for $c = 2^{23} \approx E6$.*

In order to utilize (14) for our purpose, we define $P_i = Pr(Success|hw(R) = i)$. This implies that, we devote the tag's capability to minimize the hamming weight of the response register R in the NUS protocol. Having this in mind and by using (12), we can calculate P_i for n rounds as following.

$$\begin{aligned} P_{eq} &= (\frac{i}{2n})^2 + (\frac{2n-i}{2n})^2 = 1 + \frac{i^2 - 2in}{2n^2} \\ P_i &= P_{dis} = \left[\frac{(1+P_{eq})}{2}\right]^n = \left(1 + \frac{i^2 - 2in}{4n^2}\right)^n \end{aligned} \tag{15}$$

As the response register R in the NUS protocol is of length $2n$, we only need to substitute n by $2n$ and P_i by (15) in (14). Table 1 compares the claimed security of the NUS protocol and our results in restricted and powerful adversary models in terms of the probability of success of an adversary in the distance fraud attack. For example, for $n = 32$, the probability of success in the distance fraud attack in a restricted adversary model is 1.0045E-4. This probability improves to 0.0035 in a powerful adversary model for $c = 2^{23}$ which roughly represents the number of hashes that can be computed today per second on a single PC [16]. These probabilities are remarkably beyond the claimed security $(\frac{1}{2})^{32} = 2.3283\text{E-}10$.

5 Conclusions

The design of a secure distance bounding protocol which can resist against the existing attacks for RFID systems is still challenging. Despite

of interesting proposals in the literature, this field still lacks a concrete solution.

Recently, two solutions have been proposed for this purpose called the Hitomi and the NUS distance bounding protocols. We presented a secret key disclosure attack on the former and a distance fraud attack on the latter protocol. Our results showed that the security margins which was expected to be yielded by them have been overestimated.

We showed that the Hitomi protocol is vulnerable to a full secret key disclosure attack by querying the tag several times. In addition, the probability of success in a distance fraud attack against the NUS protocol was shown to be able to be increased up to $(\frac{3}{4})^n$, if the adversary gets close enough to the reader. This probability can even be slightly improved, if the tag has some computational capabilities.

REFERENCES

[1] Jorge Munilla Fajarado, A. Peinado Dominguez. Security in RFID and Sensor Networks. First Edition, ISBN:978-1-4200-6839-9, Auerbach publication, 2009.

[2] Gildas Avoine and Aslan Tchamkerten. An efficient distance bounding RFID authentication protocol: balancing false-acceptance rate and memory requirement. *In Information Security Conference - ISC'09*, volume 5735 of Lecture Notes in Computer Science, Pisa, Italy, September 2009.

[3] Orhun Kara, Süleyman Karda, Muhammed Ali Bingöl, Gildas Avoine: Optimal Security Limits of RFID Distance Bounding Protocols editors *Radio Frequency Identification: Security and Privacy Issues - RFIDSec10*, volume 6370 of Lecture Notes in Computer Science, pages 220–238, Istanbul, Turkey, June 2010.

[4] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and J. C. A. van der Lubbe. Shedding Some Light on RFID Distance Bounding Protocols and Terrorist Attacks. arXiv.org, Computer Science, Cryptography and Security, June , 2010.

[5] Stefan Brands and David Chaum. Distance-bounding protocols. *In EUROCRYPT'93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 344–359, Secaucus, NJ, USA, 1994.

[6] Gerhard Hancke and Markus Kuhn. An RFID Distance Bounding Protocol. *In Conference on Security and Privacy for Emerging Areas in Communication Networks - SecureComm 2005*, pages 67–73, Athens, Greece, September 2005.

[7] Chong Hee Kim and Gildas Avoine. RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks. *In 8th International Conference on Cryptology And Network Security - CANS'09*, Japan, December 2009.

[8] Chong Hee Kim, Gildas Avoine, Francois Koeune, Francois-Xavier Standaert, and Olivier Pereira. The Swiss-Knife RFID Distance Bounding Protocol. *In P.J. Lee and J.H. Cheon, editors, International Conference on Information Security and Cryptology - ICISC, volume 5461 of Lecture Notes in Computer Science*, pages 98–115, Seoul, Korea, December 2008.

[9] Jorge Munilla, Andres Ortiz, and Alberto Peinado. Distance Bounding Protocols with Void-Challenges for RFID. *In Workshop on RFID Security - RFIDSec'06*, Graz, Austria, July 2006.

[10] Jorge Munilla and Alberto Peinado. Security Analysis of Tu and Piramuthu's Protocol. *In New Technologies, Mobility and Security - NTMS'08*, pages 1–5, Tangier, Morocco, November 2008.

[11] Jason Reid, Juan Gonzalez Neito, Tee Tang, and Bouchra Senadji. Detecting relay attacks with timing based protocols. *In Feng Bao and Steven Miller, editors, Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security - ASIACCS '07*, pages 204–213, Singapore, Republic of Singapore, March 2007.

[12] Yu-Ju Tu and Selwyn Piramuthu. RFID Distance Bounding Protocols. In First International EURASIP Workshop on RFID Technology, Vienna, Austria, September 2007.

[13] Rolando Trujillo-Rasua, Benjamin Martin, and Gildas Avoine. The Poulidor Distance-Bounding Protocol. *In Radio Frequency Identification: Security and Privacy Issues - RFIDSec10, volume 6370 of Lecture Notes in Computer Science*, page 239–257, Istanbul, Turkey, June 2010.

[14] Pedro Peris-Lopez and Julio C. Hernandez-Castro and Juan M. E. Tapiador and Esther Palomar and Jan C.A. van der Lubbe. Cryptographic Puzzles and Distance-bounding Protocols: Practical Tools for RFID Security. *In IEEE International Conference on RFID*, Orlando,

2010.

[15] Ali Özhan Gürel, Atakan Arslan, Mete Akgün . Non-Uniform Stepping Approach to RFID Distance Bounding Problem. *Fifth International Workshop on Data Privacy Management - DPM'10*, volume 6370 of Lecture Notes in Computer Science, Athens, Greece, September 2010.

[16] G. Avoine, M. A. Bingol, S. Kardas, C. Lauradoux, and B. Martin. A Formal Framework for Cryptanalyzing RFID Distance Bounding Protocols. Cryptology ePrint Archive, Report 2009/543, 2009.

[17] W. Feller, An Introduction to Probability Theory and its Applications, Wiley India Pvt. Ltd., 2008.

[18] D. Dolev and A. C.-C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory, 29(2)*:pages 198–207, 1983.

PAPER IV

COLLUDING TAGS ATTACK ON THE ECC-BASED GROUPING PROOFS FOR RFIDS *

Mohammad Reza Sohizadeh Abyaneh

IV

*Mohammad Reza Sohizadeh Abyaneh, "Colluding Tags Attack on the ECC-based Grouping Proofs for RFIDs", *International Conference on Security and Cryptography* (SECRYPT 2011) in Seville, Spain.

COLLUDING TAGS ATTACK ON THE ECC-BASED GROUPING PROOFS FOR RFIDS

Mohammad Reza Sohizadeh Abyaneh*

Abstract. Recently, a new privacy-preserving elliptic curve based grouping proof protocol with *colluding tag prevention*(CTP) has been proposed. The CTP protocol is claimed to be resistant against colluding tags attacks in which the involved tags can exchange some messages via another reader before the protocol starts without revealing their private keys.
In this paper, we show that the CTP protocol is vulnerable to some colluding tag attacking scenario. In addition, we propose a new elliptic curve based grouping protocol which can fix the problem. Our proposal is based on a formally proved privacy preserving authentication protocol and has the advantage of being resistant against colluding tags attacks with the same amount of computation.

Keywords: RFID, Grouping Proofs, Elliptic Curve, Privacy.

1 INTRODUCTION

In 2004, Juels [1] proposed a new security notion called *Yoking Proofs*. The proposed scheme enables the generation of a proof which shows that a pair of RFID tags are scanned simultaneously by a reader. Yoking proofs were later generalized to *grouping proofs* which indicates that multiple tags participate in the generation of a proof [2, 8].

*Department of Informatics, University of Bergen

By adopting grouping proofs, the manufacturer can prove to its customers that the referred products are sold at the same time. For example in a pharmacy store, some drugs must be sold according to the recipe. For inpatients, the medical staffs can guarantee the authentication and integrity of a group of medical items like inpatient bracelets and the containers of drugs [6]. For car industry, a grouping proof ensures that all components of a car are assembled in the same factory [1, 9].

Recently, Batina *et al* have proposed a new privacy-preserving elliptic curve based grouping-proof protocol with *colluding tag prevention* (denoted by CTP protocol)[13]. The protocol is claimed to be resistant against all active attacks applied on the previous grouping proof protocols and also fulfil the privacy against a narrow-strong adversary. The notion of the CTP protocol is mainly derived from the latest version of their elliptic curve based authentication protocols called EC-RAC III [20].

Remark1. With elliptic curve cryptography emerging as a serious alternative, the desired level of security can be attained with significantly smaller key sizes. This makes ECC very attractive for devices with limited computational capabilities. On the feasibility of implementing ECC on RFID tags, one may argue that it is too heavy to be deployed on low-cost tags such as EPCglobal Class-1 Generation-2 standard tags. Nevertheless, there have been many proposals so far such as [13–17].

Our Contribution. In this paper, we present a colluding attack against the CTP protocol. We show that two colluding tags are able to complete a run of the CTP protocol successfully and generate a valid grouping proof with the presence of only one of the tags. Then, we propose a new grouping proof protocol based on elliptic curves which fixes the problem.

Outline. The remainder of this paper is organized as follows. In Section 2, we describe the CTP protocol and its security claims, then Section 3 presents a colluding attack scenario against the CTP protocol. In order to fix the problem, a new grouping protocol is proposed in Section 4 with its security analysis. In Section 5, we compare our proposal with the CTP protocol from security and computation perspectives and finally Section 6 concludes the paper.

2 THE CTP PROTOCOL

In this section, we describe the CTP protocol. But first we explain the notations and assumptions used hereafter.

- P: Elliptic curve base point.
- T_A, T_B: Tag A and tag B respectively.
- R: Reader.
- V: Verifier.
- $y, Y = yP$: Verifier's private and public keys respectively.
- s_a, s_b: Tag A and tag B's private keys respectively.
- $x(T)$: x-coordinate of point T on the elliptic curve.
- P_{AB} : grouping proof of tag A and tag B.

2.1 Assumptions

It should be noted that the CTP protocol is executed under following assumptions:

- There are three entities involved in the protocol: some *tags*, a *reader* and a *verifier*.
- The task of the reader is to coordinate the execution of the protocol, collect the grouping proof and forward it to the verifier. The reader is not necessarily trusted by the tags or the verifier.
- The verifier is trusted and the public-key Y of the verifier is a publicly known system parameter. Only the verifier knows the corresponding private-key y.
- Knowledge of y is a necessary requirement to check the correctness of a grouping proof. The result of a verification claim is failure, or it reveals the identities of the involved tags.
- It is hard to solve the Discrete Logarithm (DL) problem, i.e. given P and aP in Elliptic Curve with a randomly chosen in $\mathbb{Z}_q = [0, q-1]$, it is hard to compute a.
- It is hard to solve the Decisional Diffie-Hellman (DDH) problem, i.e. given P, aP, bP with a and b randomly chosen in $\mathbb{Z}_q$ and given $cP = abP$ with probability $\frac{1}{2}$ and $cP = dP$ with probability $\frac{1}{2}$ with d randomly chosen in $\mathbb{Z}_q$, it is hard to decide whether abP equals cP .

2.2 DESCRIPTION

Without loss of generality, we explain the two-party version of the CTP protocol. This protocol can be easily extended to more than two tags as described in [13].
The two-party version of the CTP protocol is shown in Fig.1. The reader initiates the interrogation by sending the messages "start left" to one of the tags (T_A). Then, T_A generates a random number r_a and computes its corresponding Elliptic curve point ($T_{a,1} = r_a P$) and sends it back to the reader. The reader then initiates a simultaneous interrogation with another tag (T_B) by transmitting the "start right" message following by a random challenge generated by the reader r_s and $T_{a,1}$ received from T_A. T_B computes $T_{b,1} = r_b P$ and $T_{b,2} = (r_b + x(r_s T_{a,1}) s_b) Y$. Then, both of the generated messages are transmitted to the reader. The reader passes $T_{b,2}$ to T_A and the protocol concludes by transmission of $T_{a,2} = (r_a + x(T_{b,2}) s_a) Y$ from T_A to the reader.
The grouping proof, collected by the reader, consists of the tuple in (1).

$$P_{AB} = \{T_{a,1}, T_{a,2}, r_s, T_{b,1}, T_{b,2}\} \tag{1}$$

This tuple is sent to the verifier to verify the grouping proof constructed by T_A and T_B. The verifier checks whether the following equations hold.

$$S_a = s_a P = (y^{-1} T_{a,2} - T_{a,1}) x(T_{b,2})^{-1} \tag{2}$$
$$S_b = s_b P = (y^{-1} T_{b,2} - T_{b,1}) x(r_s T_{a,1})^{-1} \tag{3}$$

where S_a and S_b are the public keys of T_A and T_B respectively and are registered in the database of the verifier. If so, the grouping proof is accepted.

2.3 SECURITY CLAIMS

Due to its construction, the CTP grouping-proof protocol is claimed to inherit the security properties of the EC-RAC III authentication protocol [20]. The EC-RAC III latter is designed to provide secure entity authentication against an active adversary, and was informally shown to be equivalent to the Schnorr protocol [18].
The security claims on the CTP protocol can be divided into to two different security issues, *Privacy* and *Forgery prevention* of the grouping proof.

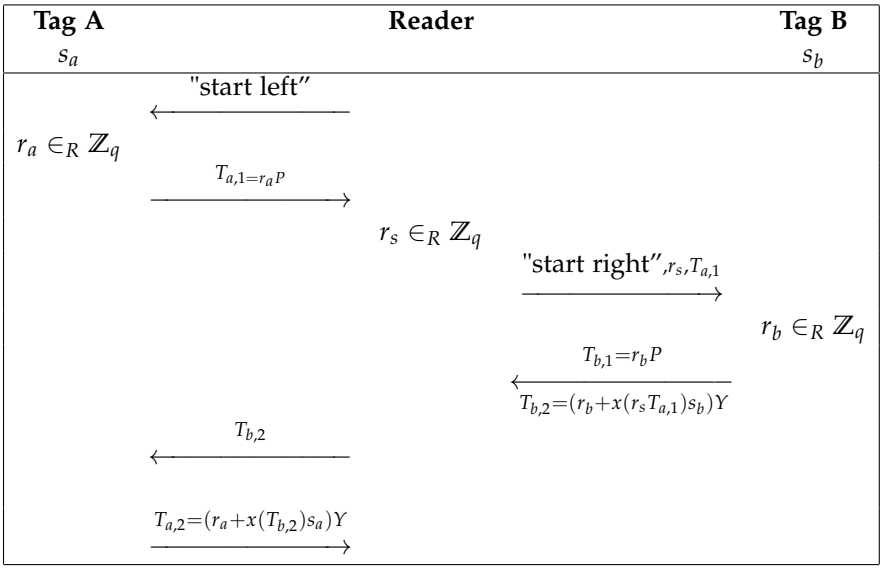

Fig. 1: *Two-party version of the CTP protocol*

2.3.1 Privacy

In [22], Vaudenay has presented a classification of privacy in RFID systems. Vaudenay's model defines eight classes of adversarial capabilities. These capabilities are in two orthogonal parts:

1. Four different types of tag corruptions: *strong*, *forward*, *destructive* and *weak*.

2. Two modes of observations: *wide* and *narrow*.

Referring to this classification, the CTP protocol is claimed to be *narrow-strong* private, although no formal proof for this is given in the original paper. This claim has been recently invalidated [23]. However, verification of this claim has not been addressed in this paper.

2.3.2 Forgery Prevention

Being a grouping proof protocol, the CTP must prevent the generation of a valid grouping proof without the involved tags actually participating

in the protocol. This implies that the protocol must resist against the following potential attack scenarios:

- *Compromised tag:* One tag is compromised, the reader is non-compromised.
- *Man-in-the-middle attack*: The reader is compromised (the tags are honest).
- *Colluding reader and tag:* The reader and one of the tags are compromised.
- *Colluding tags:* The reader is non-compromised, both tags are compromised. The tags can exchange some messages in advance (e.g., via another reader), but do not know each other's private key.
- *Replay attack performed by an outsider:* An eavesdropper scans two non-compromised tags simultaneously and replays the copied message-flow to impersonate the two tags.

The CTP protocol is claimed to be resistant against the impersonation of a tag in all of the above attack scenarios. Namely,an adversary needs to either know the private-key of that particular tag or be able to solve the Decisional Diffie-Hellman (DDH) problem to impersonate it in this protocol. This claim has been addressed through this paper and an attack, which negates this claim, will be described in the next section.

3 Our colluding tags attack

In this section, we elaborate an attacking scenario against the CTP protocol. In our attack, we take the colluding tags scenario which implies that the reader is trusted, but both tags are compromised, and tags can exchange some messages in advance (e.g. via another reader), but they do not know each other's private key.
Our attacking scenario is divided into two phases: *conspiracy* phase and *deceit* phase. In the conspiracy phase, the two tags secretly negotiate via a rogue reader (Reader*). In this negotiation, as Figure 2 shows, one of the tags (e.g. tag B) sends $H = s_b Y$ to tag A. H is the point multiplication operation of tag B's private key (s_b) and verifier's public key (Y) on the Elliptic Curve group. It should be mentioned that message H does not reveal any information on s_b due to discrete logarithm (DL) problem.

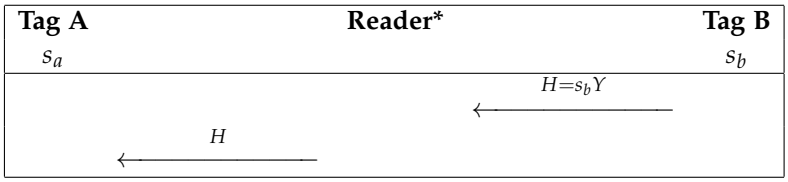

Fig. 2: *Phase I: Conspiracy Phase*

Having H known, tag A is able to impersonate tag B in the CTP protocol.

Figure 3 shows the detail of a successful completion of the CTP protocol run with inclusion of only one of the tags. The only message of the CTP protocol, which includes tag B's private key, is $T_{b,2}$ which can be easily forged by (5) if a tag accesses H.

$$T_{b,2} = (r_b + x(r_s T_{a,1})s_b)Y \tag{4}$$

$$T_{b,2} = (r_b Y + x(r_s T_{a,1})s_b Y) = (r_b Y + x(r_s T_{a,1})H) \tag{5}$$

As it can be seen, knowing $H = s_b Y$ is adequate to impersonate tag B in the CTP protocol without revealing any information about its private key s_b.

4 Proposed Protocol

In Section 3, we showed that the CTP protocol is vulnerable to some colluding tags attacks. In this section, we propose a new scheme based on elliptic curve notion with the same security level from privacy perspective but resistant against colluding attacks from forgery prevention perspective.

4.1 Description

Our proposal is based on an authentication protocol proposed by Bringer *et al*. called "Randomized Schnorr"(Figure 4 [19]. This protocol has been formally proved to be narrow-strong private.

The two-party version of our proposed protocol is shown in Figure 5. The reader initiates the interrogation by sending the messages "start left" to one of the tags (T_A). Then, T_A generates two random numbers α_a and β_a and computes their point multiplication on P and Y Elliptic curve

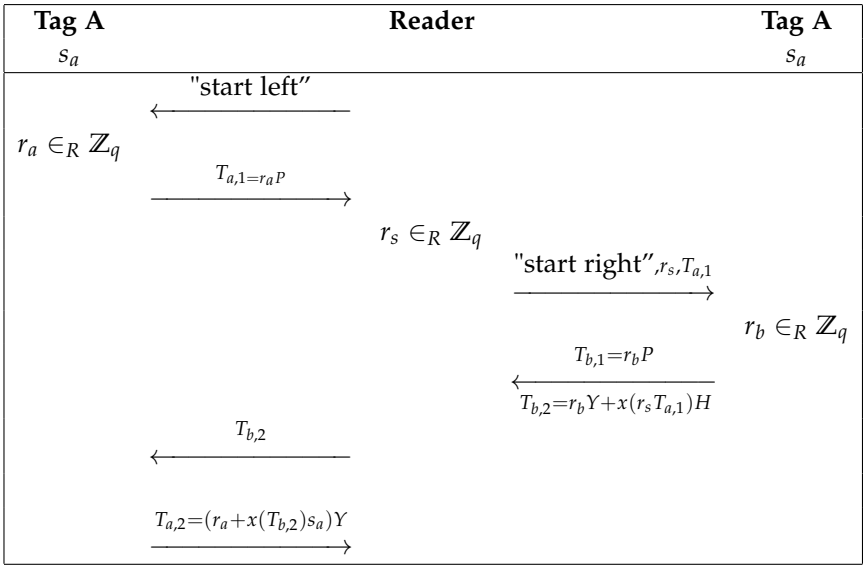

Fig. 3: *Phase II: Deceit Phase*

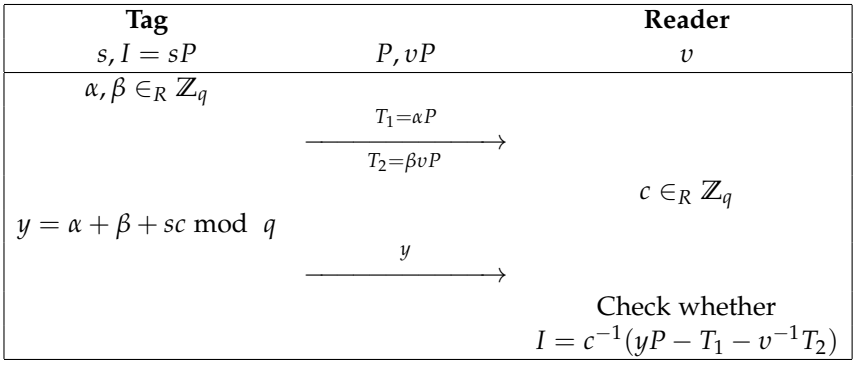

Fig. 4: *Randomized Schnorr protocol*

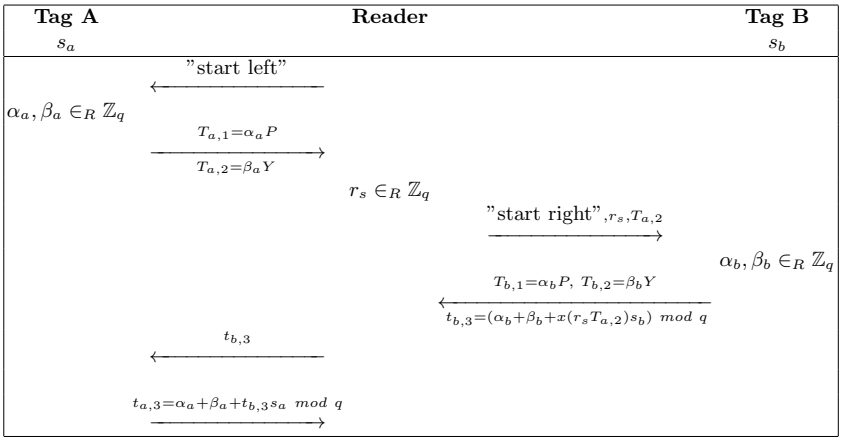

Fig. 5: *Proposed grouping protocol*

points respectively ($T_{a,1} = \alpha_a P$, $T_{a,2} = \beta_a Y$) and sends it to the reader in return. The reader then initiates a simultaneous interrogation with another tag (T_B) by transmitting the "start right" message following by a random challenge generated by the reader r_s and $T_{a,2}$ received from T_A. T_B computes $T_{b,1} = \alpha_b P$ and $T_{b,2}\beta_b Y$, the same as T_A did. In addition, it also generates a scalar number $t_{b,3} = (\alpha_b + \beta_b + x(r_s T_{a,2})s_b)$ mod q. Then, all of the three generated messages are transmitted to the reader. The reader passes $t_{b,3}$ to T_A and the protocol concludes by transmission of scalar $t_{a,3} = \alpha_a + \beta_a + t_{b,3}s_a$ from T_A to the reader. The grouping proof, collected by the reader, consists of the tuple (6).

$$P_{AB} = \{T_{a,1}, T_{a,2}, T_{a,3}, r_s, T_{b,1}, T_{b,2}, T_{b,3}\} \tag{6}$$

To verify the grouping proof constructed by T_A and T_B, the verifier checks whether the Equations (7) and (8) hold.

$$S_a = s_a P = x^{-1}(T_{b,3})(t_{a,3}P - T_{a,1} - y^{-1}T_{a,2}) \tag{7}$$

$$S_b = s_b P = x^{-1}(r_s T_{a,2})(t_{b,3}P - T_{b,1} - y^{-1}T_{b,2}) \tag{8}$$

4.2 Security Analysis

In this section, we analyze the security of our protocol in the same security framework used for the CTP protocol.

4.2.1 Privacy

Theorem 1. *Assume the hardness of the DDH problem, then Randomized Schnorr is narrow-strong private.*

Proof: [19]

Theorem 2. *Assume that the Randomized Schnorr is narrow-strong private, our proposed protocol is privacy-preserving against narrow-strong adversary.*

Proof: As explained, to prove the privacy, it is necessary to prove that we can simulate the tags outputs. In the following, we construct a simulation and we show that an adversary who is able to distinguish between this simulation and the outputs of genuine tags in the proposed protocol will be able to do the same for the Randomized Schnorr protocol.

The outputs of the tags in the proposed are as following:

T_A: $T_{a,1} = \alpha_a P, T_{a,2} = \beta_a Y, t_{a,3} = \alpha_a + \beta_a + t_{b,3} s_a$

T_B: $T_{b,1} = \alpha_b P,\ T_{b,2} = \beta_b Y, t_{b,3} = (\alpha_b + \beta_b + x(r_s T_{a,2}) s_b)$

The outputs of each tag is easily mapped on the outputs of a generic tag in the Randomized Schnorr protocol, namely $T_1 = \alpha P, T_2 = \beta v P, y = \alpha + \beta + sc$. In other words, the proposed protocol is simply two runs of the Randomized Schnorr protocol regarding the tags outputs. This simply proves the privacy attribute inheritance of the proposed protocol from the Randomized Schnorr protocol.

4.2.2 Forgery Prevention

Theorem 3. *Assume the Schnorr scheme is secure against active impersonation attacks, then Randomized Schnorr is secure against active impersonation attacks.*

Proof: [19]

Theorem 4. *Assume the randomized Schnorr scheme is secure against active impersonation attacks, then our proposed protocol is secure against active impersonation attacks.*

Proof: It is obvious that interrogation of T_A in the proposed protocol is a complete run of the Randomized Schnorr protocol and inherits the security attribute of the Randomized Schnorr protocol stated in

Theorem 3. The interrogation of T_B, however, is slightly different from a normal run of the Randomized Schnorr protocol. So, in our proof we focus on the right part of the protocol runs between the reader and T_B.

In order to proof the theorem, we devise a *proof by contradiction* approach. Assume there exists an active adversary $\mathcal{A}$ against the proposed protocol. Given a system of tags $\mathcal{T}$ and a reader executing the Randomized Schnorr protocol, we transform the tags' normal outputs to simulate tags' outputs in the proposed protocol. So doing, we convert $\mathcal{A}$ into an adversary against the Randomized Schnorr protocol.

First, when $\mathcal{A}$ interrogates T_B, she sends r_s and $T_{a,2}$ to the tag. We intercept this message. Then, tag outputs $T_1 = T_{b,1}$ and $T_2 = T_{a,2}$. We intercept these two messages and send back $c = x(r_s T_{a,2})$ to the tag. The tag responses $y = (\alpha_b + \beta_b + cs_b)$. We forward this message to the adversary as $t_{b,3} = y$. Clearly, from $\mathcal{A}$'s point of view, T_A is using the proposed protocol.

Now, $\mathcal{A}$ tries to impersonate T_B by interacting with the reader. First, we pick a random number r'_s and one random Elliptic curve point $T'_{a,2}$ and send them to $\mathcal{A}$. As $\mathcal{A}$ is able to impersonate T_B against the proposed protocol then she is able to compute a couple tuple $T'_{b,1} = \alpha'_b P, T'_{b,2} = \beta'_b Y$ and $t'_{b,3} = (\alpha'_b + \beta'_b + x(r'_s T'_{a,2})s'_b)$ on receiving the challenges such that there exists an S_b verifying $S'_b = s'_b P = x^{-1}(r_s T_{a,2})(t_{b,3}P - T_{b,1} - y^{-1}T_{b,2})$.

For this reason, we are able to uniquely compute T_1 and T_2, to receive a challenge c and to compute y such that there exists an I with $I = c^{-1}(yP - T_1 - v^{-1}T_2)$. In this way, we showed that by using $\mathcal{A}$, we are able to impersonate T_B against the Randomized Schnorr protocol which negates our assumption.

One can demonstrate that to impersonate a tag in either of the attack scenarios stated in Section 2.3, the adversary needs to know the private-key of that particular tag (or be able to solve the DDH problem).

5 Comparison

Table 2 summarizes the comparison between the CTP and our proposed protocol in terms of security and computation.

Security wise, our proposed protocol has accomplished to yield the same but formally proved privacy level and higher security from forgery prevention perspective, due to formally proved resistance against the colluding tags attack.

	Security		Computation	
	Privacy	**Forgery Prevention**	**# of EC point multiplications for the verifier**	**# of EC point multiplications for each tag**
CTP	narrow-strong (Not formally proved)	Not Secure	4	2
Proposed Protocol	narrow-strong (Formally proved)	Secure	6	2

Table 1. Comparison of the CTP protocol and the proposed protocol

From computational perspective, the forth column of the table compares the number of EC point multiplications(ECPM) required for the verifier to verify the grouping proofs. This number is four for the CTP protocol as it can be seen in (2) and (3). On the other hand, (7) and (8) show that this number is six in our protocol. This implies that our proposed protocol imposes more computational overhead to the verifier than the CTP protocol. But this is trivial due to higher computational capabilities of the verifier in comparison to the tags. On the tag side, the fifth column shows the number of ECPM needed for a tag during one run of the protocol. This number is the same for both protocols as they both impose two EC point multiplications on each tag, e.g. tag A needs to do two EC point multiplications for both protocols to calculate $T_{a,1}$ and $T_{a,2}$.

6 CONCLUSIONS

In this paper, we have presented a successful colluding tag attack on the CTP grouping proof protocol. This implies that the CTP protocol is not able to prevent colluding tags attacks as claimed. The main weakness in the protocol that we have exploited is that the necessary information required to impersonate a tag in the protocol is not structurally restricted to be its private key. It was shown that the point multiplication of a tag's private key and the verifier's public key, which does not reveal any information about the tag's private key, can be exploited by colluding tags to generate a grouping proof with presence of only one of the tags. In order to fix this problem, we proposed a new grouping protocol based on elliptic curves which prevents the colluding attacks and proved its security properties. In summary, compared to the CTP protocol, our proposal has the following properties:

- Formally provable narrow-strong privacy.
- Formally provable prevention against forged proof generation.
- The same amount of computational overhead on tag sides.

REFERENCES

[1] Ari Juels, Yoking-Proofs for RFID Tags, In the Proceedings of First International Workshop on Pervasive Computing and Communication Security, IEEE Press, pp.138–143, (2004).

[2] Junichiro Saitoh and Kouichi Sakurai, Grouping Proofs for RFID Tags, In the Proceedings of AINA International Conference, IEEE Computer Society, pp. 621–624, (2005).

[3] Selwyn Piramuthu, On Existence Proofs for Multiple RFID Tags, In the Proceedings of ACS/IEEE International Conference on Pervasive Services, IEEE Computer Society, pp. 317–320, (2006).

[4] Chih-Chung Lin, Yuan-Cheng Lai, J. D. Tygar, Chuan-Kai Yang and Chi-Lung Chiang, Coexistence Proof using Chain of Timestamps for Multiple RFID Tags, In the Proceedings of APWeb/WAIM International Workshop, Springer-Verlag LNCS 5189, pp. 634–643, (2007).

[5] Mike Burmester, Breno de Medeiros, and Rossana Motta, Provably Secure Grouping-Proofs for RFID Tags, In the Proceedings of CARDIS International Conference, Springer-Verlag LNCS 5189, pp. 176–190, (2008).

[6] C.-Y. K. Hsieh-Hong Huang, A RFID Grouping Proof Protocol for Medication Safety of Inpatient, Journal of Medical Systems, (2008).

[7] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, Solving the Simultaneous Scanning Problem Anonymously: Clumping Proofs for RFID Tags, in Security, Privacy and Trust in Pervasive and Ubiquitous Computing, SECPerU (2007).

[8] L. Bolotnyy and G. Robins, Generalized Yoking-Proofs for a Group of RFID Tags, in Proc. International Conference on Mobile and Ubiquitous Systems (Mobiquitous), (2006).

[9] Hung-Min Sun, Wei-Chih Ting, Shih-Ying Chang, Offlined Simultaneous Grouping Proof for RFID Tags,The Second International

Workshop on Multimedia, Information Privacy and Intelligent Computing Systems(MPIS),(2009).

[10] Y. Lien, X. Leng, K. Mayes, and J. Chiu, Reading Order Independent Grouping Proof for RFID Tags, IEEE International Conference on Intelligence and Security Informatics,ISI 2008. , (2008).

[11] Hung-Yu Chien, Tree-Based RFID Yoking Proof, International Conference on Networks Security, Wireless Communications and Trusted Computing, (2009).

[12] Dang Nguyen Duc, Jangseong Kim, Kwangjo Kim, Scalable Grouping-proof Protocol for RFID Tags, SCIS 2010 The Symposium on Cryptography and Information Security, (2010).

[13] Lejla Batina, Yong Ki Lee, Stefaan Seys, Dave Singelee, Ingrid Verbauwhede, *Short Paper: Privacy-preserving ECC-based grouping proofs for RFID*, In Information Security - 13th International Conference, ISC 2010 , Boca Raton, Florida, Oct. 25–28,(2010).

[14] Sandeep S. Kumar, Christof Paar. *Are standards compliant Elliptic Curve Cryptosystems feasible on RFID?*.Workshop on RFID Security , Graz, Austria, July (2006).

[15] Franz Furbass, Johannes Wolkerstorfer. *ECC Processor with Low Die Size for RFID Applications*, IEEE International Symposium on Circuits and Systems (ISCAS), (2007).

[16] Yong Ki Lee Sakiyama, K. Batina, L. Verbauwhede. *Elliptic-Curve-Based Security Processor for RFID*, IEEE Transactions on Computers, 1514 –1527 ,(2008).

[17] Daniel Hein, Johannes Wolkerstorfer, Norbert Felber,*ECC Is Ready for RFID - A Proof in Silicon*, SAC 2008, LNCS , pp. 401–413, (2008).

[18] C. P. Schnorr. Efficient Identification and Signatures for Smart Cards. In G. Brassard, editor, Advances in Cryptology (CRYPTO '89), Lecture Notes in Computer Science, LNCS 435, pages 239–252. Springer-Verlag, (1989).

[19] Julien Bringer, Herv´e Chabanne, and Thomas Icart. *Cryptanalysis of EC-RAC, a RFID identification protocol.* In CANS, volume 5339 of Lecture Notes in Computer Science, (2008).

[20] Yong Ki Lee, Lejla Batina, Dave Singelee, and Ingrid Verbauwhede. *Low-Cost Untraceable Authentication Protocols for RFID*. In Proceed-

ings of the 3rd ACM conference on Wireless network security (WiSec 2010),(2010).

[21] Fan, J., Hermans, J., Vercauteren, F.: *On the claimed privacy of EC-RAC III*. Cryptology ePrint Archive, Report 2010/132,, http://eprint.iacr.org, (2010).

[22] Serge Vaudenay. *On privacy models for RFID*. In ASIACRYPT, (2007).

[23] C. Lv and H. Li and J. Ma and B. Niu and H. Jiang. *Security Analysis of a Privacy-preserving ECC-based Grouping-proof Protocol*. Journal of Convergence Information Technology,(2011).

PAPER V

ON THE PRIVACY OF TWO TAG OWNERSHIP TRANSFER PROTOCOLS FOR RFIDS *

Mohammad Reza Sohizadeh Abyaneh

*Mohammad Reza Sohizadeh Abyaneh, "On the Privacy of Two Tag Ownership Transfer Protocols for RFIDs", *IEEE International Conference for Internet Technology and Secured Transactions* (ICITST2011) in Abu Dhabi, UAE.

V

ON THE PRIVACY OF TWO TAG OWNERSHIP TRANSFER PROTOCOLS FOR RFIDS

Mohammad Reza Sohizadeh Abyaneh*

Abstract. In this paper, the privacy of two recent RFID tag ownership transfer protocols are investigated against the tag owners as adversaries.
The first protocol called ROTIV is a scheme which provides a privacy-preserving ownership transfer by using an HMAC-based authentication with public key encryption. However, our passive attack on this protocol shows that any legitimate owner which has been the owner of a specific tag is able to trace it either in the past or in the future. Tracing the tag is also possible via an active attack for any adversary who is able to tamper the tag and extract its information.

The second protocol called, *Chen et al.*'s protocol, is an ownership transfer protocol for passive RFID tags which conforms EPC Class1 Generation2 standard. Our attack on this protocol shows that the previous owners of a particular tag are able to trace it in future. Furthermore, they are able even to obtain the tag's secret information at any time in the future which makes them capable of impersonating the tag.

Key Words: RFID, Ownership Transfer, Privacy.

1 INTRODUCTION

Radio frequency identification(RFID) is currently considered as the next generation technology that mainly used to identify massive objects

*Department of Informatics, University of Bergen

in an automated way and will substitute traditional optical barcode system in near future. The RFID advantages such as reducing supply chain inefficiencies and improving inventory flow leaves no doubt that the dominant deployment of barcodes nowadays in supply chain will be promptly taken over by RFID tags. But it has its own drawbacks too.

As products flow through a supply chain, their ownership is transferred from one partner to the next. This transfer of ownership extends to the RFID tags attached to these products. Thus all information associated with the tag will need to be passed from the current to the new owner. However, at the moment of tag ownership transfer, both the current and new owners have the information necessary to authenticate a tag, and this fact may cause an infringement of tag *owner privacy* [5].

To handle this problem, tag ownership transfer protocols are proposed to transfer the ownership of a tag from one owner to another securely. The proposed schemes for ownership transfer protocols are divided into two groups. Some schemes exploit a trusted third party(TTP) which acts as a secure channel to transfer some information between the entities. One of the first solution of this kind was proposed by Saito *et al.*[6]. However, the security of their scheme is only based on the short read range of the backward channel (tag to reader communication) by assuming that it is hard for adversaries to eavesdrop on this channel. Another scheme with TTP is proposed by Molnar *et al.* [7]. They exploit the TTP to manage tag keys by a tree structure. But in this protocol one key is shared by several tags which makes this protocol vulnerable. The privacy of the whole system decreases quickly when more tags are compromised [8].

There also exist some *decentralized* proposals without a using TTP. Most of these schemes have two following assumptions: there is a secure channel between the current and new owner to pass the tag's information securely. They also assume that the new owner and the tag will be able to execute an authentication session in an isolated environment without presence of the current owner after the ownership transfer is completed in order to update some secret parameters.

For instance, Soppera and Burbridge [9] adopt the scheme of Molnar *et al*. by replacing the TTP with some distributed local devices called RFID *acceptor* tag. In [13], the authors have also proposed a decentralized protocol relying on the assumption that owners are able to change the tag key in an isolated environment. However, this protocol has security vulnerabilities well described in [14]. Song *et al.* [11] proposed a scheme with introduction of a new property called *authorization recovery*

which facilitates the ownership transfer of a tag to its previous owner. But Pedro *et al.* [12] showed that their schemes has some vulnerabilities as well.

Recently, two other tag ownership transfer protocols have been proposed. The first scheme is called an RFID ownership transfer with issuer verification (ROTIV) [16] which provides a constant-time, privacy-preserving tag ownership transfer. The ROTIV's main idea is to combine an HMAC-based authentication with public key encryption. The second scheme which is proposed by Chen *et al.* [17], proposes an RFID ownership transfer systems which conforms the requirements of EPCglobal Class-1 Generation-2 Standard.

Our Contribution. In this paper, we investigate the privacy of two aforementioned ownership transfer protocols. The investigation includes some attacks to violate the forward and backward privacy as well as previous and new owner privacy properties of the schemes.

Outline. The remainder of this paper is organized as follows. Section 2 describes the privacy issues and properties required for tag ownership transfer protocols as well as system and adversary modelings. In Sections 3 and 4 the description of the the ROTIV and Chen *et al.* protocols and our attack on them are presented respectively, and finally, Section 5 concludes the paper.

2 Preliminaries

To lend clarity to our discussions in the subsequent sections, in this section, we outline the models and properties used in ownership transfer protocol.

2.1 System Model

In ownership transfer protocols, there are mainly three active entities involved: *current owner*, *tag* and *new owner*. The owners in an ownership transfer protocols are some readers in practice which take the role of ownership in these kinds of protocols. The ownership transfer protocols typically provide a solution to transfer the tag's information from the current owner to the new owner.

Most of the ownership transfer protocols consist of two phases, an *authentication phase* and a *ownership transfer phase*. By the former phase, the tag and two owners are mutually authenticated and the latter phase

assures all three entities that the ownership of the tag is transferred in a proper and privacy-preserving way.

2.2 Privacy Properties

Generic privacy properties and how to formalize them for RFID systems have been extensively explored in the literature [1–4]. The two generic privacy property we address in this paper are:

- *Backward Privacy*: an adversary should not be able to to trace past transactions between an owner and a tag, even if it compromises/tamper the tag.
- *Forward Privacy*: an adversary should not be able to to trace future transactions between an owner and a tag, even if it compromises/tamper the tag.

On the other hand, in tag ownership transfer protocols changes of tag owner could occur frequently and at the moment of tag ownership transfer, both the current and new owners have the information necessary to authenticate a tag, and this fact may cause an infringement of tag *owner privacy*. Therefore, there are two extra privacy issues dedicated for ownership transfer protocols in the literature [10, 15]:

- *New owner privacy*: Once ownership of a tag has been transferred to a new owner, only the new owner should be able to identify and control the tag. The previous owner of the tag should no longer be able to identify or *trace* the tag.
- *Current/previous owner privacy*: When ownership of a tag has been transferred to a new owner, the new owner of a tag should not be able to *trace* past interactions between the tag and its previous owner.

2.3 Adversary Model

In [3], Juels and Weis give a formal model of the privacy in RFID systems. In this model, tags ($\mathcal{T}$) and readers/owners ($\mathcal{R}$) interact in protocol sessions. During this interaction there is also an adversary entity $\mathcal{A}$ which passively or actively interacts with them. The adversary may have access to an oracle which can be queried by the following queries:

- `Execute`$(\mathcal{T}, \mathcal{R}, i)$: This query is responded by the information of $\mathcal{T}$ and $\mathcal{R}$ interactions in an honest protocol session at time instance i.
- `Send`$(\mathcal{P}_1, \mathcal{P}_2, i, m)$: This query models active attacks by allowing the adversary $\mathcal{A}$ to impersonate some entity, a tag or a reader, $\mathcal{P}_1$ in some protocol session i and send a message m of its choice to an instance of some other entity $\mathcal{P}_2$.
- `Corrupt`$(\mathcal{T})$: This query allows the adversary $\mathcal{A}$ to tamper the tag to learn the stored secret information of the tag $\mathcal{T}$
- `Test`$(i, \mathcal{T}_0, \mathcal{T}_1)$: This query is responded by a random bit $b \in \{0, 1\}$ and the interaction information of the tag $\mathcal{T}_0$ and $\mathcal{T}_1$ with the reader/owner at i^{th} time instance.

2.4 Attack Scenario

In [3], the adversary $\mathcal{A}$ aims at tracing a specific target tag T. To do so, she,

- absorbs the information she requires about the target tag T by the means of queries previously described.
- choose two test tags T_0 and T_1 where one of them is T, and asks the oracle for the challenge by `Test` query. The response will be the interactions between the T_0 and T_1 tags with the reader R at a specific time instance.

The adversary succeeds to violate the privacy of the tag by tracing it, if she is able to distinguish the tag T between the two tested tags by outputting 0 or 1.

2.5 Notations

Here, we explain the notations used hereafter.

- $E_k(.)$: Symetric/asymetric encryption function operation with the key k.
- pk_X, sk_X: Public and private key of entity X respectively.
- $h_k(.)$: Keyed hash function with key k.
- $h(.)$: Hash functions.

- $PRNG(.)$: Pseudo random number generator.
- T, O_n, O_{n+1}: Tag, current owner and new owner.
- ID_X: The identification (ID) of entity X.
- N_X: Random numbers generated by entity X.
- m_i: dynamic value m at time instance i.

3 ROTIV PROTOCOL

ROTIV is a decentralized scheme which does not require a trusted third party to perform tag ownership transfer. This protocol provides issuer verification that allows prospective owners to check the identity of the entity which has issued the tag. The authors have claimed that their scheme ensures both forward and backward privacy and it also preserves current and new owner privacy.

There are four entities involved in the protocol, a tag T, current owner O_n, new owner O_{n+1} and issuer I which initializes the tag and owners.

In ROTIV, the T stores a symmetric key k, a *state parameter* s, where k is a key shared between the tag and its owner and s is an Elgamal encryption of T's identification information.

3.1 PRELIMINARIES

Bilinear pairing
Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be groups, such that $\mathbb{G}_1$ and $\mathbb{G}_2$ have the same prime order q. Pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is a bilinear pairing if has the following properties:

1. *bilinear*: $\forall a, b \in \mathbb{Z}_q$, $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$, $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.
2. *computable*: there is an efficient algorithm to compute $e(g_1, g_2)$ for any $(g_1, g_2) \in \mathbb{G}_1 \times \mathbb{G}_2$;
3. *non-degenerate*: if g_1 is a generator of $\mathbb{G}_1$ and g_2 is a generator of $\mathbb{G}_2$, then $e(g_1, g_2)$ is a generator $\mathbb{G}_T$.

3.2 DESCRIPTION

Setup: The issuer I outputs $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$, where $\mathbb{G}_1$, $\mathbb{G}_T$ are subgroups of prime order q, g_1 and g_2 are random generators of $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is a bilinear pairing.
The issuer chooses $x \in \mathbb{Z}_q^*$ and computes the pair (g_1^x, g_2^x). The I's public and secret keys are:

$$sk_I = (x, g_1^x),\ pk_I = g_2^x \tag{1}$$

I randomly selects $\alpha_n \in \mathbb{Z}_q^*$ and provides each owner O_n with a secret key $sk_{O_n} = \alpha_n$ and a public key $pk_{O_n} = (g_1^{\alpha_n^2}, g_2^{\alpha_n})$. All owners know each other's public keys.

Tag Initialization: The issuer I picks a random number $t \in \mathbb{F}_q$, where $\mathbb{F}_q$ is the finite field with q elements. Using a cryptographic hash function $h : \mathbb{F}_q \rightarrow \mathbb{G}_1$, I computes $u_0 = 1$ and $v_0 = h^x(t)$. Finally, I chooses randomly a key $k_0 \in \mathbb{F}_q$ and stores: (k_0, s_0), where $s_0 = (u_0, v_0)$ into the tag. I also provides O_n with T's information ref^{O_n}. This information includes two *dynamic* values k_{old}, k_{new} which are updated after each successful transaction and two *static* values $\delta = t, \psi = h^x(t)$ which represent the identification of the issuer of the tag.

$$ref^{O_n} = (k_{old}, k_{new}, \delta, \psi) = (k_0, k_0, t, h^x(t)) \tag{2}$$

Before accepting the tag, the owner can read the tag and checks the authenticity of the static values of the tag:

$$e(h(\delta), pk_I) = e(\psi, g_2) \tag{3}$$

Ownership Transfer: The ROTIV ownership transfer protocol (Fig.1) is a combination of two mutual authentication sessions between the tag and current and new owners with the ownership transfer protocol between the current owner O_n and the new owner O_{n+1}.
In i^{th} time instance of the ROTIV protocol:
1. New owner O_{n+1} generates a random nonce $N_{O_{n+1}}$ and sends it to the tag and the current owner simultaneously.
2. The tag T also generates a random number N_T and send it with its status parameter $s_i = (u_i, v_i)$ and a hash $m_i = h_{k_i}(N_{O_{n+1}}, N_T, s_i)$ to the new owner.
3. O_{n+1} selects a random number r_v and computes $A_v = u_i^{r_v}$. Then, it

sends $N_{O_{n+1}}, N_T, s_i, m_i$ and A_v to the current owner O_n. In this way, O_n is able to authenticate the tag by computing,

$$\psi = \frac{v_i}{(u_i)^{\alpha_n^2}} \tag{4}$$

Then, it searches in the database to see if ψ is in the database or not. If not, it aborts authentication. Otherwise, it looks up T's ownership references ref^{O_n} in the database to checks if $m_i = h_{k_i^{new}}(N_{O_{n+1}}, N_T, s_i)$ or $m_i = h_{k_i^{old}}(N_{O_{n+1}}, N_T, s_i)$. For the former case $k_i = k_i^{new}$ and for the latter case $k_i = k_i^{old}$.

4. If the authentication process succeeds O_n gives O_{n+1} the following information via a secure channel:

$$ref^V = (A, B, C) = (t, h^x(t), A_v^{\alpha_n}) \tag{5}$$

$$ref^{O_n} = (k_{old}, k_{new}, \delta, \psi) = (k_i, k_{i+1}, t, h^x(t)) \tag{6}$$

The new owner O_{n+1} check the validity of the provided information by (3).

Now, the new owner can verify whether the issuer of the tag T is I by checking whether the following equations hold:

$$e(h(A), pk_I) = e(B, g_2) \tag{7}$$

$$e(C, g_2) = e(A_v, g_2^{\alpha_n}) \tag{8}$$

$$e(v_i, g_2)^{r_v} = e(B, g_2)^{r_v} e(C, g_2^{\alpha_n}) \tag{9}$$

5. If the verification succeeds, O_{n+1} chooses a new random number r_{i+1} and computes:

$$s_{i+1} = (u_i, v_i) = (g_1^{r_{i+1}}, h^x(t).g_1^{\alpha_n^2 r_{i+1}}) \tag{10}$$

$$m_{i+1} = h_{k_i}(N_T, s_{i+1}) \tag{11}$$

and sends s_{i+1}, m_{i+1} to the tag and updates its database. Now, T authenticates O_{n+1} by checking the content of m_{i+1}. If the authentication succeeds T updates its state parameter to s_{i+1} and its symmetric key to the new key k_{i+1} where,

$$k_{i+1} = PRNG(k_i, N_{O_{n+1}}) \tag{12}$$

In order to prevent the current owner from tracing the tag later in the future, the new owner has to run a mutual authentication with the tag outside the range of the current owner after the ownership transfer is complete.

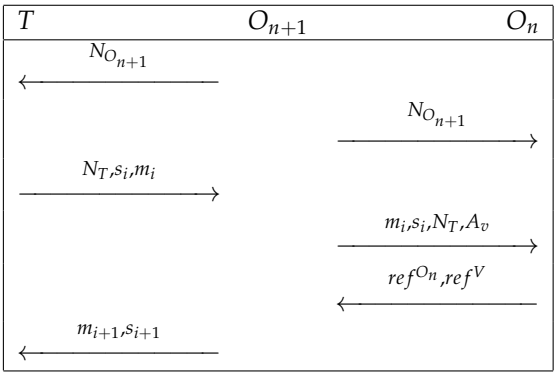

Fig. 1: *Ownership transfer in ROTIV*

3.3 Our Attacks

In this attack, we target mainly the *ownership privacy* including current and new owner privacy of the ROTIV protocol. Correspondingly, the adversary $\mathcal{A}$ has been one of the owners of the tag T at least once. For example, without loss of generality, we can assume that $\mathcal{A} = O_n$. Therefore, at a time instance e.g. i, she has had access to the tags's information ref^{O_n}. We also assume that the adversary is passive and thus has access only to `Execute` and `Test` queries.

According to the attacking scenario described in Section 2.4, the adversary follows the procedure below to trace the tag T via distinguishing that which of the two test tags, T_0 and T_1, are T.

1. $\mathcal{A}$ retrieves the static information of the tag T, $\delta = t, \psi = h^x(t)$, from the information she has been give at time i, ref^{O_n}.

2. $\mathcal{A}$ queries $\texttt{Test}(j, \mathcal{T}_0, \mathcal{T}_1)$ and obtains (13) and (14).

$$\{N_{O_l}, N_{T_0}, m_j, m_{j+1}, s_j, s_{j+1}\} \tag{13}$$

$$\{N_{O'_l}, N_{T_1}, m'_j, m'_{j+1}, s'_j, s'_{j+1}\} \tag{14}$$

   which are the messages exchanged between the owner O_l and tags T_0 and T_1 respectively.

3. $\mathcal{A}$ saves $s_j = (u_j, v_j)$ and $s'_i = (u'_j, v'_j)$.

4. $\mathcal{A}$ checks whether (15) or (16) holds,

$$e(v_j, g_2) = e(h(\delta), pk_I)e\left((\frac{v_j}{\psi}), g_2\right) \quad (15)$$

$$e(v'_j, g_2) = e(h(\delta), pk_I)e\left((\frac{v'_j}{\psi}), g_2\right) \quad (16)$$

5. If (15) is correct then $\mathcal{A}$ outputs 0 i.e. $T = T_0$, otherwise she outputs 1 i.e. $T = T_1$.

Note that we can write (15) because according to bilinear pairing properties of e, we have:

$$\begin{aligned} e(v_i, g_2) &= e(h^x(t).g^{\alpha_l^2 r_i}, g_2) \\ &= e(\psi.g^{\alpha_l^2 r_i}, g_2) \\ &= e(\psi, g_2)e(g_1^{\alpha_l^2 r_i}, g_2) \\ &= e(h(\delta), g_2^x)e(g_1^{\alpha_l^2 r_i}, g_2) \\ &= e(h(\delta), pk_I)e(g_1^{\alpha_l^2 r_i}, g_2) \\ &= e(h(\delta), pk_I)e\left((\frac{v_i}{\psi}), g_2\right) \end{aligned}$$

Using the scenario above, any owner in the protocol which has had the ownership of the tag T is able to trace it. It is worth mentioning that since the update procedure of state values s are performed independent of their previous values (step 5 of ownership transfer), the aforementioned tracing scenario can be applied both on the state values of the past and the future. Hence any owner who has accessed to the static values of a tag is able to trace it at any time in the past or future by only eavesdropping state parameter of the tag s. It implies that the ROTIV protocol lacks both previous owner and new owner privacy properties.

Remark 1. It should be noted that if an adversary $\mathcal{A}'$ has access to `Corrupt` query which gives her this privilege to tamper the tag and access to the tag's static information $t, h^x(t)$, her state of knowledge about the tag is exactly the same as that the adversary $\mathcal{A}$ in the stated attack. Hence, she will also be able to exploit (15) to trace T in any time in the past and future. This implies that the ROTIV protocol lacks forward and backward privacy as well.

4 CHEN *et al*'S PROTOCOL

Chen *et al.*'s protocol is designed to meet the requirements of EPC Class1 Generation2 standard (ISO18000-6C) for passive RFID tags. According to this standard, RFID tags's computation capabilities is restricted to only performing a 16-bit Cyclic Redundancy Code (CRC) and 16-bit Pseudo-Random Number Generator (PRNG). The authors have claimed that their scheme ensures both forward and backward privacy and it also preserves current and new owner privacy.

There are four entities involved in the protocol, a tag T, current owner O_n, new owner O_{n+1} and issuer I which issues a new issuer identification to be stored into the tags after each ownership transfer phase.

4.1 DESCRIPTION

Chen *et al.*'s ownership transfer protocol consist of three phases: *requiring phase*, *authentication phase* and *ownership transfer phase*. In Chen *et al.*'s protocol, the T stores two dynamic symmetric keys k_i, k_i^* and the $h(t_i)$ which is the hash of the issuer identification. In addition to the tag's information the owner has the issuer identification t_i.
In the i^{th} time instance of requiring phase (Fig.2), the current owner first signs the tag's certificate t_i and the identification of the new owner:

$$SG_{O_n} = Sign_{sk_{Ok}}(t_i, ID_{O_{n+1}}) \tag{17}$$

After that, it encrypts this message with the next owner's public key to get C_i:

$$C_i = E_{pk_{O_{n+1}}}(t_i, SG_{O_n}) \tag{18}$$

and transfers the message (ID_{O_k}, C_i) to the new owner O_{n+1}.
In authentication phase (Fig.3), the current owner first generates a random number N_{O_n} and then computes A_i:

$$A_i = CRC(k_i \oplus N_{O_n}) \tag{19}$$

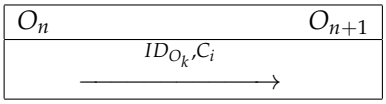

Fig. 2: *Requiring phase*

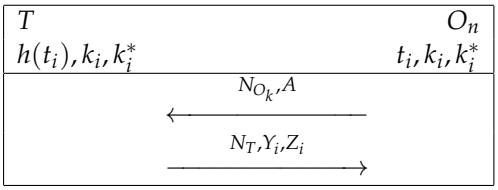

Fig. 3: *Authentication phase*

and sends it with N_{O_n} to the tag. Upon receiving these messages, the tag verifies the content of the message A_i. If the verification succeeds, the tag generates a new random value N_T, and computes the X_i, Y_i and Z_i as following.

$$X_i = CRC(N_T \oplus k_i^*) \quad (20)$$
$$Y_i = k_i^* \oplus ID_T \oplus X_i \oplus k_{i+1} \quad (21)$$
$$Z_i = CRC(X_i \oplus k_i \oplus Y_i) \quad (22)$$

Moreover, the tag updates its keys as:

$$k_{i+1} = (k_i^* \oplus ID_T \oplus N_T \oplus Y_i) \quad (23)$$
$$k_{i+1}^* = PRNG(k_i^*) \quad (24)$$

and transfers (N_T, Y_i, Z_i) to the current owner. Upon receiving the message, O_n checks the content of X_i and Z_i. If this verification succeeds, it obtains k_{i+1} and updates its values accordingly.

In the ownership transfer phase (Fig.4), the new owner O_{n+1} uses its own private key to decrypt C_i received in the requiring phase and obtains SG_{O_k} and t_i. Then, it uses the O_n's public key pk_{O_n} to verify the correction of SG_{O_k}. If the signature is verified successfully, the new owner signs the ID of its own as well as the current owner's:

$$SG_{O_{n+1}} = Sign_{sk_{Ok+1}}(ID_{O_k}, ID_{O_{n+1}}) \quad (25)$$

And sends the tuple $\{ID_{O_i}, ID_{O_{i+1}}, SG_{O_i}, SG_{O_{i+1}}, t_i\}$ to the issuer I to issue a new issuer identification for the tag.

The issuer checks the content of this message and if it is correct, it issues the t_{i+1} and computes $t_{i+1} \oplus k_{i+1}$ and $h(t_{i+1})$ and transmits them to O_n. Upon receiving this message, O_n sends the former message to

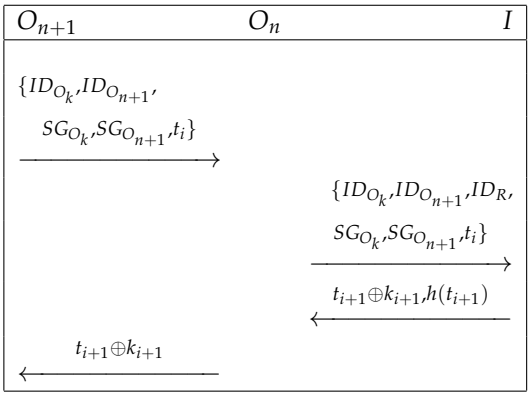

Fig. 4: *Ownership transfer phase*

the new owner and writes the latter one into the tag's memory. The new owner can also obtain the t_{i+1} by XORing the message received from the current owner and the new key stored in the memory.

$$t_{i+1} = (t_{i+1} \oplus k_{i+1}) \oplus k_{i+1} \tag{26}$$

4.2 Our Attack

The adversary $\mathcal{A}$ in our attack is one of the previous owners of the tag T. Therefore, she has had access to ID_T, k_i and k_i^*, where the ID_T is the static ID of the tag T or the tag's electronic product code(EPC) and k_i and k_i^* are the dynamic keys of the tag at time instance i when the tag has been in the possession of $\mathcal{A}$ as the owner.

Being given the messages exchanged between two tags T_0, T_1, which one of them is the tag T, and another owner O_l at two consecutive time instance j and $j+1$, the adversary follows the procedure below to distinguish which of the test tags is the tag T.

1. $\mathcal{A}$ retrieves the static identity of the tag T, ID_T.

2. $\mathcal{A}$ queries $\texttt{Test}(j, \mathcal{T}_0, \mathcal{T}_1)$,$\texttt{Test}(j+1, \mathcal{T}_0, \mathcal{T}_1)$ and obtain

$\{A_j, N_{T_0}, N_{O_l}, Y_j, Z_j\}$,$\{A_{j+1}, N'_{T_0}, N'_{O_l}, Y_{j+1}, Z_{j+1}\}$

$$\begin{aligned} Y_j &= k_j^* \oplus ID_{T_0} \oplus X_j \oplus k_j && (27)\\ Y_{j+1} &= k_{j+1}^* \oplus ID_{T_0} \oplus X_{j+1} \oplus k_{j+1} && (28)\\ Z_j &= CRC(X_j \oplus k_{j+1} \oplus Y_j) && (29)\\ Z_{j+1} &= CRC(X_{j+1} \oplus k_j \oplus Y_{j+1}) && (30) \end{aligned}$$

From (27), we have:

$$k_j = k_j^* \oplus Y_j \oplus ID_{T_0} \oplus X_j \quad (31)$$

By substituting k_j from (31) in (30), we can write:

$$Z_{j+1} = CRC(k_j^* \oplus ID_{T_0} \oplus X_j \oplus X_{j+1} \oplus Y_j \oplus Y_{j+1}) \quad (32)$$

3. Now the adversary $\mathcal{A}$ defines the maximum number of iterations as τ and follows the following steps to determine whether T_0 is the tag T. It should be noted that the same process can be used to determine whether T_1 is the tag T.
   a) $c = 1$
   b) computes:
   $k^* = PRNG^c(k_i^*) = \underbrace{PRNG(PRNG(...(k_i^*)..))}_{c \text{ times}}$.
   c) computes
   $X_j = CRC(k^* \oplus N_{T_0})$,
   $X_{j+1} = CRC(PRNG(k^*) \oplus N'_{T_0})$.
   d) computes $\Delta_X = X_j \oplus X_{j+1}$,$\Delta_Y = Y_j \oplus Y_{j+1}$.
   e) If $Z_{j+1} \neq CRC(k^* \oplus ID_T \oplus \Delta_X \oplus \Delta_Y)$ and $c < \tau$ then $c = c + 1$ and go to b
   f) Else $\mathcal{A}$ outputs 0 i.e. $T_0 = T$ and $k_j^* = k^*$.

This attack shows that the current owner of tag T will be able to trace it at any time in future. Therefore, we can conclude that Chen *et al.*'s protocol lacks new owner privacy.

Remark 2. It should be noted that the procedure above will work when the number of iterations τ is less than the all possible values for the key k_j^*. This implies that if the length of key k_j^* is n, $\tau << 2^n$. So,

the tracing process will work efficiently unless the number of passed sessions are comparable to 2^n.

Remark 3. Any adversary of this kind who has already obtained k_j^* from the above procedure is also able to calculate k_{j+1} by (23). Then she will be able to extract t_{i+1} from the last message of the tag ownership transfer protocol by using (26). This results in a more dangerous attack in which the current owner is able to even *impersonate* the tag for future interrogations.

5 Conclusion

In this paper, we investigated the privacy of two ownership transfer protocols. The investigation included the attacks to target the forward and backward privacy as well as previous and new owner privacy properties. Our results showed both protocols are vulnerable to the attacks where the adversary is one of the owners in the system.

Any owner in the system as well as any adversary with the capability of tampering the tag are able to trace the tag in the previous and future interrogations in the ROTIV protocol. Therefore, this protocol lacks four stated privacy properties, forward privacy, backward privacy, previous owner privacy and new owner privacy.

Chen *et al.*'s protocol was also shown to be susceptible to the attacks in which the adversary is one of the previous owners of the tag and thus not to fulfil the forward privacy and new owner privacy. This protocol also revealed the whole tag's information to any previous owner and makes the adversary capable of impersonating the tag in further interrogations.

References

[1] G. Avoine, *Adversarial model for radio frequency identification*,Cryptology ePrint Archive, Report 2005/049, 2005.

[2] S. 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, Berlin, Heidelberg,2007.

[3] A. Juels and S.A. Weis. *Defining Strong Privacy for RFID*. In PerCom Workshops, White Plains, USA, 2007.

[4] J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel, *A New RFID Privacy Model*, In European Symposium on Research in Computer Security (ESORICS 2011), Lecture Notes

[5] A. Fernàndez-Mir, R. Trujillo-Rasua, J. Castellà-Roca, and J. Domingo-Ferrer, *A Scalable RFID Authentication Protocol Supporting Ownership Transfer and Controlled Delegation*, In the proceeding of RFIDSec2011, Amherst, USA, June 2011.

[6] J. Saito, K. Imamoto, and K. Sakurai. *Reassignment scheme of an RFID tags key for owner transfer*. Embedded and Ubiquitous Computing, 2005.

[7] D. Molnar, A. Soppera, and D. Wagner. *A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags*. In Selected Areas in Cryptography. Springer, 2006.

[8] G. Avoine, E. Dysli, and P. Oechslin. *Reducing Time Complexity in RFID Systems*. In Bart Preneel and Stafford Tavares, editors, Selected Areas in Cryptography (SAC) 2005, volume 3897 of Lecture Notes in Computer Science, Kingston, Canada, August 2005.

[9] A. Soppera and T. Burbridge. *Secure by default: The RFID acceptor tag (RAT)*, In: 2nd Workshop on RFID Security - RFIDSec, Graz, Austria, July 2006, IAIK TU Graz.

[10] K. Osaka, T. Takagi, K. Yamazaki, and O. Takahashi. *An Efficient and Secure RFID Security Method with Ownership Transfer*. In Computational Intelligence and Security, 2006.

[11] B. Song. *RFID Tag Ownership Transfer*. In Workshop on RFID Security - RFIDSec'08, Budapest, Hungary, July 2008.

[12] P. Peris-Lopez, J. C. Hernandez-Castro, J. M.E. Tapiador, T. Li, and Y. Li. *Vulnerability analysis of rfid protocols for tag ownership transfer*. Computer Networks, 2010.

[13] E.J. Yoon and K.Y. Yoo. *Two security problems of RFID security method with ownership transfer*. In Network and Parallel Computing, 2008.

[14] G. Kapoor and S. Piramuthu. *Vulnerabilities in some recently proposed RFID ownership transfer protocols*. In 2009 First International Conference on Networks and Communications. IEEE, 2009.

[15] B. Song and C.J. Mitchell. *Scalable RFID security protocols supporting tag ownership transfer*. Computer Communications, 2010.

[16] K. Elkhiyaoui, E. Blass, R. Molva. *ROTIV: RFID Ownership Transfer with Issuer Verification*, In the proceeding of RFIDSec2011, Amherst, USA, June 2011.

[17] C. Chen, Y. Lai, C.Cheng Chen, Y. Deng,Y. Hwang, *RFID Ownership Transfer Authorization Systems Conforming EPCglobal Class-1 Generation-2 Standards*, International Journal of Network Security, Vol.13, No.1, July 2011.