DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

ENHANCING AUTHENTICATION IN RADIO FREQUENCY IDENTIFICATION SYSTEMS BY DESIGNING A FULLY FLEDGED CLASS PROTOCOL

by

Alaauldin KHIDIR IBRAHIM IBRAHIM

June, 2018
IZMIR

ENHANCING AUTHENTICATION IN RADIO FREQUENCY IDENTIFICATION SYSTEMS BY DESIGNING A FULLY FLEDGED CLASS PROTOCOL

A Thesis Submitted to the
Graduate School of Natural and Applied Sciences of Dokuz Eylül University
In Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Computer Engineering

by

Alaauldin KHIDIR IBRAHIM IBRAHIM

June, 2018
IZMIR

Ph.D. THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"ENHANCING AUTHENTICATION IN RADIO FREQUENCY IDENTIFICATION SYSTEMS BY DESIGNING A FULLY FLEDGED CLASS PROTOCOL"** completed by **ALAAULDIN IBRAHIM** under supervision of **ASST. PROF. DR. GÖKHAN DALKILIÇ** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Doctor of Philosophy.

Asst. Prof. Dr. Gökhan DALKILIÇ

Supervisor

Prof. Dr. Yalçın ÇEBİ

Thesis Committee Member

Asst. Prof. Dr. Reyat YILMAZ

Thesis Committee Member

Prof. Dr. Mehmet Ufuk Çağlayan

Examining Committee Member

Assoc. Prof. Dr. Mehmet Ünlütürk

Examining Committee Member

Prof. Dr. Latif SALUM
Director
Graduate School of Natural and Applied Sciences

ACKNOWLEDGMENTS

Primarily, I thank Allah for his bounty, which allowed me to accomplish this work, he has praise first and last.

First of all, I would like to express my deepest appreciation to my advisor Assistant Professor Dr. Gökhan DALKILIÇ for his precious propositions, inducements, motives, patience and support along this study. Besides, I would like to thank him for obliging me to research in various style and illuminate my brain, his assistance was fundamental in achieving this study. It was an honor for me to work with.

I would like to thank my committee members, Professor Dr. Yalçın ÇEBİ, Assistant Professor Dr. Reyat YILMAZ and, not to forget, Assistant Professor Dr. Özlem AKTAŞ for their subscription to this achievement and participating their opinions throughout this study.

I would like to thank my colleague Ömer AYDIN and my friend Samed KARDJILOV for their help and support during this study.

I would like to thank the Turkish government and the Yurtdışı Türkler ve Akraba Topluluklar Başkanlığı for giving me the chance to peruse my dream.

Last but not the least, I would like to thank my wonderful family: my outstanding mother and father, to my brothers and sisters for supporting me spiritually throughout writing this thesis and my whole life. A deep thanks to my wife, without your outstanding support I couldn't reach what I am presenting today.

Alaauldin KHIDIR IBRAHIM IBRAHIM

ENHANCING AUTHENTICATION IN RADIO FREQUENCY IDENTIFICATION SYSTEMS BY DESIGNING A FULLY FLEDGED CLASS PROTOCOL

ABSTRACT

The main topic of this thesis is the security problems of Radio Frequency Identification (RFID) system, one of the most important technologies of recent years. Despite the numerous advantages of RFID technology, it faces a major security and privacy threats. Because of the wireless communication nature between reader and tag, RFID technology is vulnerable to many attacks. Since, authentication adds trust to the identifing process, authentication protocols are first step in protection against wireless attacks and only the authenticated reader can access the contents of the authenticated tags.

As a first step in this thesis, a class related comprehensive survey, review and comparison of the most recent and considerable RFID mutual authentication protocols are made in detail. The significant points of the compare are presented in two tables. The outcome of the comparison revealed that the investigated authentication protocols have adopted various methods to deal with attacks and ensure security and privacy. Due to hardware restriction of the low cost tags, most of the investigated authentication protocols are lie under fully fledged class. Besides, every examined protocols has a particular capability to handle the security and privacy issues.

Secondly, in this thesis an efficient and powerful RFID mutual authentication protocol is proposed named AERMAP-W5. AERMAP-W5 uses both private and public key algorithms, AES and ECC. Two methods are used during the authentication process. Dissimilar the existing schemes, AERMAP-W5 is coded, tested and proven on real devices and could send tag ID and valuable data as well. Moreover, in AERMAP-W5, mutual authentication has been realized in only 2 steps. Finally, the security and performance of AERMAP-W5 is thoroughly analyzed and the results show that it can stand out against almost all common attacks and satisfies the essential security requirements of RFID-based healthcare systems.

Keywords: AERMAP-W5, radio frequency identification, RFID, RFID attacks, RFID authentication protocols, authentication protocols, mutual authentication protocol, healthcare environments, elliptic curve cryptography, wireless identification and sensing platform, WISP, WISP5

TAM TEŞEKKÜLLÜ SINIFINDA BİR PROTOKOL TASARIMIYLA RADYO FREKANSI İLE TANIMLAMA SİSTEMLERİNDE KİMLİK DOĞRULAMAYI GELİŞTİRME

ÖZ

Bu tezin ana konusu, son yılların en önemli teknolojilerinden biri olan Radyo Frekansı ile Tanımlama (RFID) sisteminin güvenlik problemlerini incelemektir. RFID teknolojisinin sayısız avantajlarına rağmen, aşılması zor güvenlik ve gizlilik tehdidi ile karşı karşıyadır.. Okuyucu ve etiket arasındaki kablosuz iletişim yapısı nedeniyle, RFID teknolojisi birçok saldırıya karşı savunmasızdır. Kimlik doğrulama, kimlik doğrulama sürecine güven eklediğinden, kimlik doğrulama protokolleri kablosuz saldırılara karşı korunmada ilk adımdır ve yalnızca kimliği doğrulanmış okuyucu, kimliği doğrulanmış etiketlerin içeriğine erişebilir.

Bu tezde ilk adim olarak, sınıfa bağlı kapsamlı bir araştırma, yeni ve dikkate değer RFID karşılıklı kimlik doğrulama protokollerini ayrıntılı birşekilde inceleme ve karşılaştırma yapılmıştır. Karşılaştırmanın önemli noktaları iki tabloda sunulmuştur. Karşılaştırmanın sonucu, araştırılan kimlik doğrulama protokoller, saldırılar ile başa çıkabilmek, güvenlik ve gizliliği sağlamak için çeşitli doğrulama yöntemleri uygulamıştır. Düşük maliyetli etiketlerin depolama ve işleme kabiliyetleri açısından donanımsal kısıtlığı nedeniyle, araştırılan kimlik doğrulama protokollerinin çoğu tam teşekküllü sınıfı altında yer almaktadır. Ayrıca, incelenen her protokolün güvenlik ve gizlilik konularını ele almak için belirli bir yeteneği vardır.

İkinci olarak, bu tezde, AERMAP-W5 adında, etkin ve güçlü bir RFID karşılıklı kimlik doğrulama protokolü önerilmiştir. Önerilen protokolde, simetrik ve asimetrik şifreleme algoritmalarını, AES ve ECC, kullanılmıştır. Kimlik doğrulamada iki farklı yöntem kullanılmıştır. Mevcut şemalardan farklı olarak, önerimiz gerçek cihazlarda, kodlanmış, test edilmiş ve kanıtlanmıştır ve etiket kimliğine ek olarak değerli verileri de gönderebilir. Ayrıca, sunulan protokol, karşılıklı kimlik doğrulama sadece 2 adımda gerçekleştirilmiştir. Son olarak, protokolümüzün güvenliği ve performansı iyice analiz edildi. Analiz sonuçları, protokolümüzün neredeyse tüm ortak saldırılara karşı

durabileceğini ve RFID tabanlı sağlık sistemlerinin temel güvenlik gereksinimlerini karşıladığını göstermektedir.

Anahtar kelimeler: AERMAP-W5, radyo frekansı ile tanımlama, RFID, RFID saldırıları, RFID kimlik doğrulama protokolleri, kimlik doğrulama protokolleri, karşılıklı kimlik doğrulama protokolü, sağlık ortamları, eliptik eğri kriptografisi, kablosuz tanımlama ve algılama platformu, WISP, WISP5

CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

CHAPTER ONE

INTRODUCTION

In Section 1.1, we are going to give a fast overview of Radio-Frequency Identification (RFID) tag, technology, advantages, systems, communication, daily applications, applications in healthcare environments and Wireless Identification and Sensing Platform (WISP). In Section 1.2, we mentioned about motivation of our Thesis. In section 1.3, we referred to aim of this Thesis. In section 1.4, we talked about our contribution in this Thesis. Finally, Thesis organization is given in Section 1.5.

1.1 Overview

RFID is a relatively new and an emerging technology. It is a wireless data capturing technique from tagged objects and people. This technology has been recognized as one of the most important technologies of these recent years (Ministry of Science and Technology of PRC, 2006). It is a complex technology that is not well known and well understood by the public. RFID tags receive/send signals from/to reader. RFID tags, as seen from the Figure 1.1 (Karmakar, 2011), according to how they are powered, are divided into three types: passive, semi- passive and active tags. Passive tags take their energy from the reader. Semi-passive tags, or semi-active, use batteries only to energize the interior circuit, and use the collected energy from reader's radio signal to generate the reply signal to the reader. Active RFID tags use inner batteries to energize the interior circuit and to generate the reply signal. Furthermore, in terms of frequencies, RFID tags are ranged into three basic frequencies: low frequency (LF) (125–134 kHz), high frequency (HF) (13.56 MHz) and ultra-high frequency (UHF) (860–960 MHz) ranges. Passive (low-cost) RFID tags that operate in ultra-high frequency bands have opened an innovation gate in our variety daily application, such as goods tracking, building access control, supply chain management. Since these two abovementioned tag classifications are related with the topic of this thesis, other tag classification could be examined form Karmakar (2011).

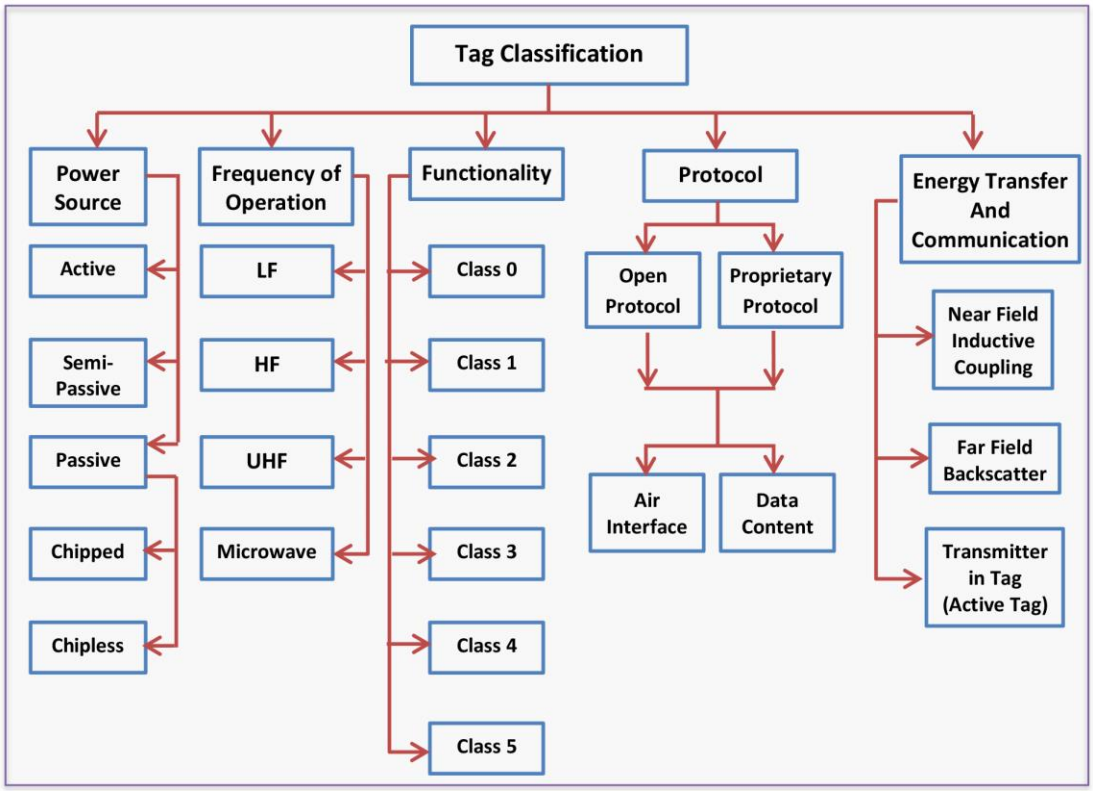

Figure 1.1 Classification of RFID tags (Karmakar, 2011)

As RFID tags can be read in challenging circumstances, they became attractive for considerable tracking and tagging scenarios. In the last years, deployment of RFID applications in supply chain management and access control applications, environmental sensing, electronic toll collection, e-passports, inventory control, automobile identification, theft detection, electronic ticketing, livestock identification, etc. have been increased rapidly. RFID technology offers several advantages over optical barcodes and according to some specialist, the low-cost RFID tag attached to consumer items will replace the barcodes (Vajda & Buttyán, 2003). For instance, the data in RFID technology can be read automatically from a non-conductive material, like cardboard or paper, at a speed of hundreds tags/s and a distance of many meters, without line of sight. Further, in addition to the unique identifier, tag has read/write memory able to store large amount of data, and it is less responsive to adverse conditions like dust, chemicals, physical damage etc. (Vajda & Buttyán, 2003). As seen from Figure 1.2, the tag consists of a microchip connected to an antenna and both put on the package.

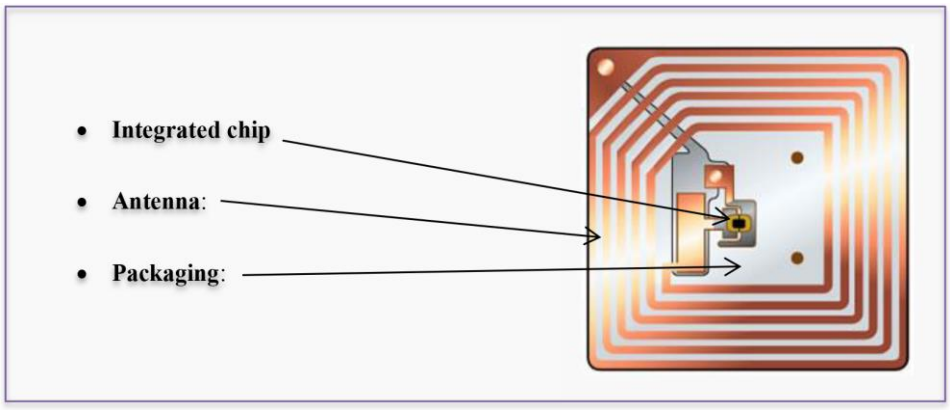

Figure 1.2 RFID tag

RFID systems consist of three essential elements; an RFID reader, a tag and a back-end database server. The reader is a device emits radio frequency (RF) to activate the battery-less tag and queries the tag identity by the means of electromagnetic signals (Figure 1.3) and forwards the tag identity to the back-end server, where information obtained from tags is generally in the form of an index for a back-end database.

Normally, RFID tags are attached to the objects that need to be identified. So, when we query information from an RFID network, such as the number of items or specific information, we need to execute an identification process in a fast and reliable fashion. During a typical identification process, a reader broadcasts a command to request some information from tags. Then, accordingly, the tags send their ID or specific information. Since the RFID networks are wireless, two or more tags could reply the reader simultaneously. Hence, lead to collision in radio frequency channel. This called tag collision that has direct impacts on the performance of the whole system (Bonuccelli, Lonetti, & Martelli, 2007). There are two RFID standards to solve the collisions between tags: ISO18000-7 and Electronic Product Code Class 1 Generation 2 (EPC C1-G2). The first is to solve collisions in active RFID tags, and the second is for solving collisions in passive RFID tags. EPC C1-G2 is the most popular air interface standard related with passive RFID. This standard, is approved by EPCglobal in 2004, provides a number of enhancements that helps solidify the adoption of RFID in the UHF band (EPCGlobal, 2015).

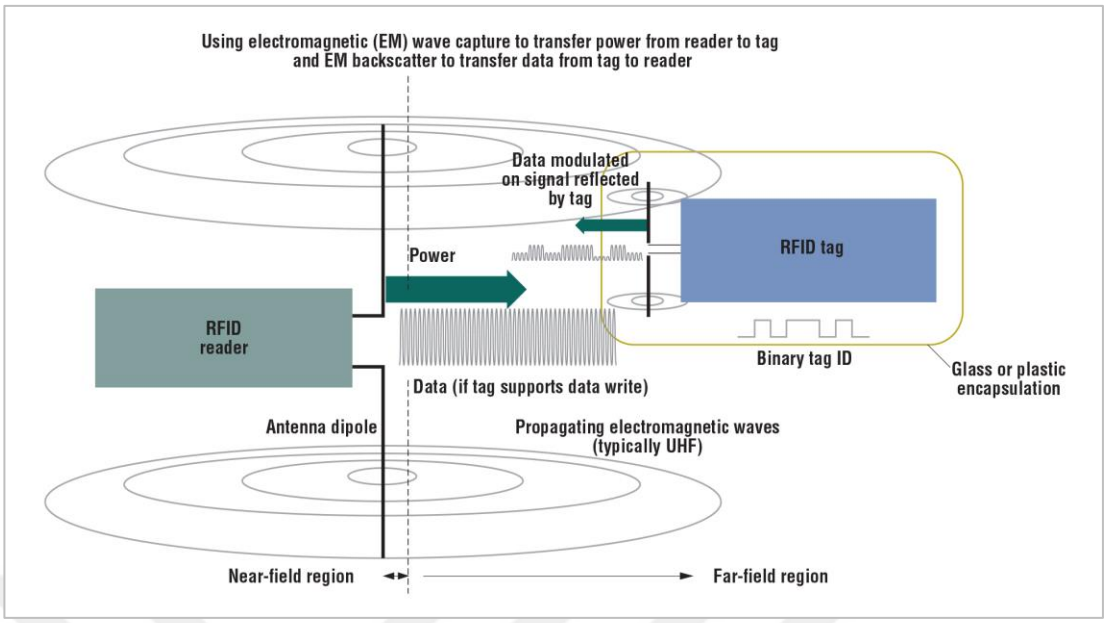

Figure 1.3 Tag and reader communication (Want, 2006)

As the the reader communicate with the tag wirelessly, RFID technology faces a significant security and privacy threatening. Since the authentication verifies the authenticity of an identity and adds trust to the identity process, it is first step in protection against wireless attacks in RFID systems. After authentication, the reader able to access the content of the authenticated tags. Mutual authentication protocols are mainly used for overcoming the security attacks on reader and tags. A lot of research has been done since 2002 and many protocols have been proposed. However, some of these protocols yet need to be improved.

RFID technology is widely used in healthcare environments, where it has been applied to newborn and patient identification (Hung, 2007), tracking medical assets (Najera, Lopez, & Roman, 2011), medical treatment tracking and validation (Katz & Rice, 2009), surgical process management (Yu, Chen, Liao, & Lee, 2008), and patient location and procedure management (Leu, 2010). The legacy systems in hospitals could be integrated with middleware to provide a lot of smart services, such as drug administration, patient identification and asset tracking (Figure 1.4). However, hospitals are open and unsecure environments in which radio waves are used for connections. An eavesdropper could read, modify, or even clone the data stored in patients' tags. Thence, security and privacy are main worries of using RFID systems in healthcare environments.

The US Food and Drug Administration (FDA) declared that “Hospira and an independent researcher confirmed that Hospira’s Symbiq Infusion System could be accessed remotely through a hospital’s network. This could allow an unauthorized user to control the device and change the dosage the pump delivers, which could lead to over- or under-infusion of critical patient therapies” (U.S. Department of Health and Human Services [USDHHS], 2015).

In the future, the FDA may warn about other devices or even RFID-based healthcare systems. For instance, if the blood groups or laboratory test results were modified on the RFID tags attached to blood bags (Siemens, 2010), patients could suffer fatal harm. To prevent and eliminate these potential hazards, rigid mutual authentication protocols must be exploited between the tag and the reader using cryptographic technologies.

Protocols conforming to the EPC C1-G2 standard increasingly inadequate, and there is a demand for stronger protocols. Furthermore, the improvements in integrated circuit techniques made the RFID tags able to support the complicated operations of private and public key cryptography. In this thesis, using the last revision of the WISP, WISP5 (WISP5, 2015), we propose a mutual authentication protocol based on elliptic curve cryptography (ECC) and advanced encryption standard (AES) algorithms. WISP5 is an EPC C1-G2 UHF passive RFID tag that is embedded with AES and sensors. Integrating passive RFID with sensing technologies is widely applicable in many productive sectors.

For instance, some application scenarios of the healthcare systems, as WISP has built-in sensors, it can easily send temperature of WISP tagged blood bag to the system. Checking whether the box that contains glass tubes having specimens taken from the patients in the laboratory has been fallen or not, or measuring the ambient temperature can be achieved via a WISP tagged to the box. Moreover, there are many valuable devices in the hospital and some of these devices are portable. It is possible to get information about the place of the WISP tagged devices and it can be easily determined whether a WISP tagged device has been moved or not. In above scenarios, if the authentication is provided, we can trust that the tags are the legitimate tags. WISP5 is passively powered, obtaining power from the reader rather than a battery. Hence, this is essentially a maintenance-free system.

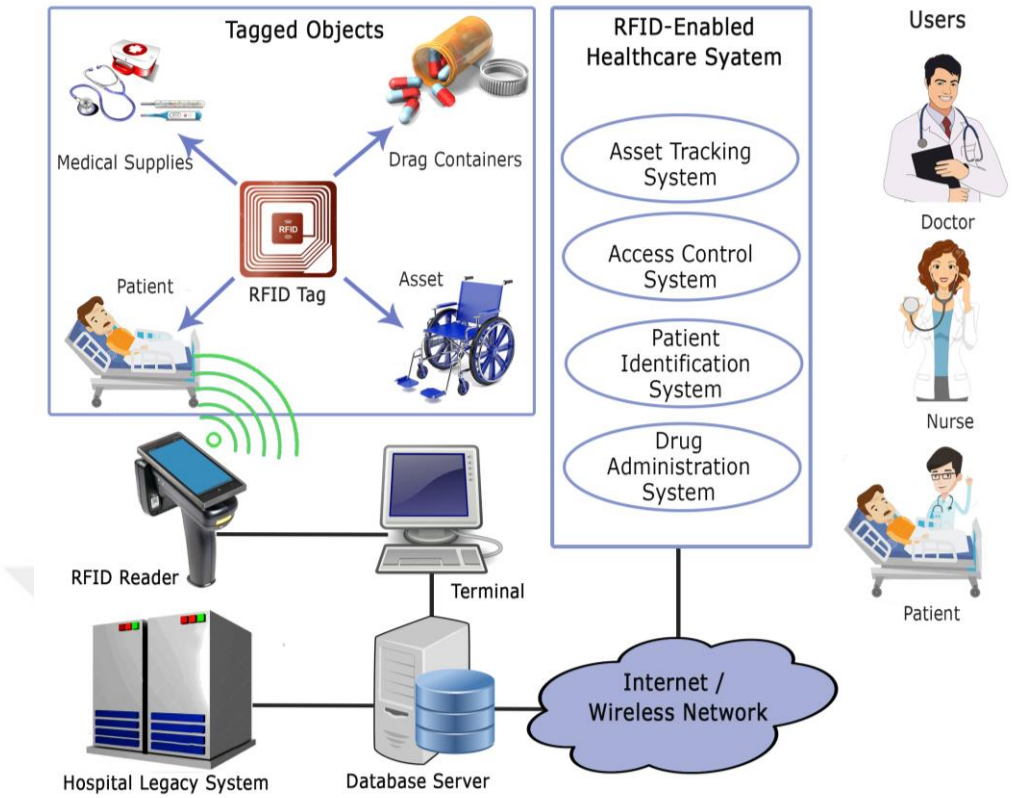

Figure 1.4 RFID-enabled healthcare systems (redrawn from Yao, Chu, & Li (2012))

Compared with other public key algorithms such as Rivest–Shamir–Adleman (RSA), ECC algorithms are smaller, faster, and consume less power, see Table 1.1, (William & Stallings, 2006). Thus, the elliptic curve Diffie–Hellman scheme (ECDH) is used to produce the secret key that will encrypt the tag ID and data. The elliptic curve digital signature algorithm (ECDSA) is used to prevent man-in-the-middle attacks (Blake, Seroussi, & Smart, 2005) and to realize mutual authentication between the tag and the reader.

Table 1.1 Comparable key sizes in terms of computational effort for cryptanalysis

RSA-based asymmetric scheme (modulus size in bits)	***ECC-based asymmetric scheme (size of n in bits)***
512	112
1024	160
2048	224
3072	256
7680	384
15360	512

1.2 Motivation

RFID is an up-and-coming technology in the area of ubiquitous computing. It is offering many features compared to other identification systems like barcodes. For example, the data could be read automatically without line of vision at a distance and high rate. More, RFID tags have read/write memory and are less sensitive to dust, chemicals, physical damages.

However, advantages of RFID systems are accompanied with disadvantages too. Due to the wireless communication nature between reader and tag, the RFID system faces a significant security risks, like privacy and tracking. Yet, there are more risks need to be considered like, man-in-the-middle, denial-of-service (DoS), eavesdropping, impersonation attacks, etc.

No matter how efficient a technology is, the cost still the major concern instead of security. Besides, RFID tag's cost is ahead of its technological progress. In the other words, to replace RFID tags with barcodes, the cost of the first should be around 1 or 2 cents. For this reason, instead of increasing cost of the tags physically, cryptographic solutions are required to ensure sufficient security.

Since 2002, much research has been conducted and numerous protocols are proposed but factually much of them do not address the severe restriction of these tags. Theoretically, much of these proposals meaningful, but practically are not possible to apply them to a large number of low cost tags.

Notwithstanding the above, in last years, RFID systems are started to be used widely in healthcare environments. For instant, it has been applied on patient identification, tracking patient location and medical assets, medical treatment tracking and validation, etc. However, hospitals are open and unsecure environments and an eavesdropper could read, modify, or even clone the data stored in patients' tags. After FDA declaration and improvements in integrated circuit techniques, protocols conforming to the EPC C1-G2 standard became inadequate, and a demand for stronger protocols become obvious.

In this thesis, to prevent and eliminate the potential hazards, we propose a stable and powerful AES and ECC based RFID mutual authentication protocol suitable for RFID-based healthcare systems. The proposed protocol could send the valuable data within tag ID securely and achieves mutual authentication in only two steps. Moreover, integrating passive RFID with sensing technologies would be widely applicable in many sectors.

1.3 Aim of Thesis

The aim of this thesis is examining authentication protocols for RFID systems and proposing a stable and powerful mutual authentication protocol suitable for RFID-based healthcare systems. Through the enormous published paper in last years, it is obvious that RFID security is a significant searching topic. Some articles point to RFID system's attack, yet, no precise work have been done on the subject.

To form secure mechanisms, the first stage is knowing the attacks. due to the wireless connection nature between RFID reader and tag, RFID system faces a significant security risks, like privacy and tracking. The popularity of RFID technology and being unsecure called for inflowing of mutual authentication protocols. For this reason, in this thesis, classes of authentication protocols are defined and to help and give the reader a fast information and quick knowledge about RFID authentication protocols, as literature review, class related well-known authentication protocols are examined and compared in detail.

RFID systems are started to be used widely in healthcare environments. However, (1) being hospitals open and unsecure environments and an eavesdropper could read, modify, or even clone the valuable data stored in patients' tags, (2) after FDA declaration (abovementioned), (3) protocols conforming to the EPC C1-G2 standard became inadequate for RFID-based healthcare systems, in this thesis, we propose a stable and powerful AES and ECC based RFID mutual authentication protocol suitable for RFID-based healthcare systems. The protocol is coded and tested on WISP5. As WISP could be built with different type of sensors, the sensing data could be exploited. Thus, integrating passive RFID with sensing technologies would be widely applicable in healthcare and many other sectors.

1.4 Contribution of Thesis

Our contributions in this thesis can be summarized in three main points:

1. **Comprehensive Survey:** In order to protect a system and construct a secure and an impervious mechanism, the first issue is knowing the attacks on the system. Since reader contacts with the tags wirelessly, RFID system will be faced with significant security risks, like privacy, tracking, cloning, etc. The importance of RFID technology on one hand and being assailable on the other, got the researchers into the action. As authentication is the first step in protecting RFID systems against wireless attacks, hundreds of authentications protocol has been proposed. Accordingly, in Chapter Two, we defined classes of authentication protocols and the security threats and services. To better understanding of the reader, we made a class related comprehensive survey for the most well-known authentication protocols and made an exhaustive comparison among them. This work accepted to be published in Journal of Wireless Networks (Ibrahim & Dalkılıc, 2017a) by Springer, a Science Citation Indexed (SCI) paper. In this comprehensive survey paper, 158 references have been used. Worth mentioning also, that in this thesis 184 references have been cited.
2. **Designing a stable and powerful RFID mutual authentication protocol:** RFID systems are deployed exceedingly in healthcare environments. Nevertheless, being hospitals open environments for attackers, and after FDA declaration that some systems could be accessed remotely via hospital's network, and being protocols conforming to the EPC C1-G2 standard inadequate for RFID-based healthcare systems, in Chapter Four of this thesis, we propose a stable and powerful AES and ECC based RFID mutual authentication protocol suitable for RFID-based healthcare systems called *"AES and ECC Based RFID Mutual Authentication Protocol Proven on WISP5"*. In Chapter Five of this thesis, the security and performance of the proposed protocol is analyzed and compared with 4 latest and well-known proposed protocols. This work led to publication of a SCI paper in Journal of Sensors (Ibrahim & Dalkılıc, 2017b) published by Hindawi.

3. **Our contribution in the proposed protocol:** First of all, it is worth mentioning that, in our design both symmetric, and asymmetric algorithms have been employed. Our main contributions in designing the proposal could be listed as:
    a. Unlike the existing schemes that used simulation tools, the proposed scheme is coded, tested and proven on real devices (WISP5).
    b. As WISP could be built with different type of sensors, the sensing data could be exploited. Thus, integrating passive RFID with sensing technologies would be applicable in healthcare and many other sectors.
    c. Unlike the existing schemes that try to send only tag ID securely, in our design, taking advantage of opportunity that AES is embedded in WISP5 we use it to encrypt both tag's ID and valuable sensors' data and send them to the reader securely (encrypted by AES).
    d. Unlike the existing schemes that realize the mutual authentication at least in 3 steps, our work realizes the mutual authentication in only 2 steps.
    e. Unlike the existing schemes, like study of Jin, Xu, Zhang, & Zhao (2015) where uses precomputed method for private and public keys, in our design the private and public keys are not static, but they are refreshing after each communication and this strengthens the security of the protocol and makes the keys untraceable and unpredictable.
    f. ECDH is used to produce and exchange the secret key that will be used in AES to encrypt both tag's ID and valuable sensed data stored in the tag.
    g. ECDSA is used to prevent man-in-the-middle attack that ECDH suffers from, and to realize the mutual authentication.
    h. The standard ECC almost is not applicable on resource constrained systems. So, the tiny ECC (Liu & Ning, 2008) has been used in during coding the scheme.
    i. As it is well-known that the most time-consuming operation is point multiplications. Since ECC includes numerous time-consuming point multiplications, Shamir's trick optimization is used to compute ($u_1G + u_2R'$) that is used in ECDSA verification, pieces of code are given in Appendix 1. Straight execution needs two scalar multiplications and a

point addition, but with Shamir's trick, the cost is close to one scalar multiplication (Hankerson, Vanstone, & Menezes, 2004).

j. Furthermore, to increase the efficiency of point multiplication, Montgomery's ladder with co-Z coordinates (Rivain, 2011) is used also.

1.5 Thesis Organization

This thesis is organized in 6 chapters. In Chapter Two, we gave basic definitions, defined classes of authentication protocols, and the security threats and services and we made a class related comprehensive survey and made an exhaustive comparison. In Chapter Three, we tried to refresh reader's memory and give a brief preliminary of some important topics that will be used in our proposed protocol, Like, ECDH, ECDSA, AES and WISP5. In Chapter Four, we propose a stable and powerful AES and ECC based RFID mutual authentication protocol suitable for RFID-based healthcare systems and discusses details of our proposed protocol. In Chapter Five, the security and performance of the proposed protocol and compared it with 4 latest and well-known proposed protocols experiments and results are discussed. Finally, in Chapter Six, we concluded the thesis with our major findings on experiments that we obtained and works mentioned along the thesis.

CHAPTER TWO

BASIC DEFINITIONS AND LITERATURE REVIEW

In this chapter we aimed to deepen on authentication protocols and give a detailed literature review. We can divide this chapter into three parts; in the first part, we define classes of authentication protocols and mention about the goals of authentication protocols that must fulfill in terms of security threats and services. In the second part, we examine and compare some well-known authentication protocols including class related literature review in detail. The last parts evaluate the examination and comparison of the well-known authentication protocols.

2.1 Authentication Protocols

Authentication is the first step in defending against wireless attacks on RFID systems. Once the server validates the identity of the RFID tag, it begins trusting the tag. After authentication, the reader can access the contents of the authenticated tags.

2.1.1 Classes of Authentication Protocols

Chien (2007) stated that authentication protocols are divided into four classes with accordance to the tag's computational cost and supported operations:

- *Fully fledged protocols:* Protocols that support symmetric and asymmetric encryption, and a one-way function. Examples are in (Tuyls & Batina, 2006; Feldhofer, Dominikus, & Wolkerstorfer, 2004).

- *Simple protocols:* Protocols that support hash function and random number generator (RNG). Examples of this class are given in (Tsudik, 2006; Weis, Sarma, Rivest, & Engels, 2004).

- *Lightweight protocols:* Protocols that support cyclic redundancy check (CRC) and RNG. Examples are given in (Bringer, Chabanne, & Dottax, 2006; Chien & Chen, 2007; Duc, Park, & Lee, 2006; Gilbert, Robshaw, & Sibert, 2005).

- *Ultra-lightweight protocols:* Protocols that are tailored specially to extremely constrained devices. These protocols involve only simple bitwise operations (like AND, OR, XOR) on tags. Examples are given in (Li & Deng, 2007; Li & Wang, 2007).

2.1.2 Goals of Authentication Protocols

Considering the variety of potential threats, an authentication protocol, whatever the class, should address all or most of the following security threats and services.

2.1.2.1 Security Threats

- *Tracking attack:* is the most suspenseful attack must be taken into account as it yields a serious privacy loss to human and institutions. Any data linked to a particular tag, it would be easy to track.

- *Denial-of-service (DoS) attack*: just as tracking attack, DoS is source of concern in RFID systems. It is simple to achieve and hard to protect against. The attacker tries to breakdown tags by using sinister readers and overlay them more information than they could manage. At the same time, such attack could cause de-synchronization between the reader and tag.

- *Desynchronization attack:* is attempt of making the reader and tag to be out of synchronization. In the other words, the objective of the attack, is to prevent starting the link between the tag and reader.

- *Man-in-the-middle attack:* is attempt of an attacker to control flow of message by replaying and altering messages between a tag and reader, cheating them to thought that each of them speaks to another.

- *Impersonation attack:* is counterfeiting an authenticated tag and pretending to be a legitimate tag.

- *Cloning attack:* is attempt of fooling the reader to believe that it is getting data from a legal tag. This could be happening by printing properly formed data on empty RFID tag and create an authentic tag.

- *Full-disclosure attack:* is compromising of all secret information of the tags by the attacker.

- *Eavesdropping:* is a communal issue of wireless communication, which is listening an illegitimate party to private connection channel because tag and reader.

- *Replay attack:* is attempting of eavesdropping a transmitted message between two communicated parties, tag and reader, during authentication process and retransmitting it illegitimately to cheat a legitimate party and passing the authentication.

2.1.2.2 Security Services

- *Mutual authentication:* is the prime necessity because it is the first step towards protecting RFID systems against wireless attacks. Herein, both the tag and the reader are verified to each other. Thereafter, only the authenticated readers can access contents of the tag.

- *Confidentiality:* is a necessity that all private data must transferred safely throughout all transmissions. Means, that the tag must sends its data in encrypted manner only the server could distinguish it.

- *Availability:* is property that the authentication process between the server and tag have to be operate all the time. In the other words, authenticating parties must keep synchronized along communication.

- *Forward/backward security:* Inability of an attacker to expose the previous/current private data even though it could get the current/previous private data .

- *Ownership transferable:* The privacy of the current and future owner should not be violated even if the current owner gives essential info to the next owner.

- *Tag anonymity:* is the most significant security demand for privacy. It is the feature that the tag cannot be tracked via tapping the line. Otherwise, an attacker with the same reader could constantly monitor the owner of a particular tag.

- *Traceability:* is attempt of tracing a tag holder via using location and information privacy stored in the tag.

- *Location privacy:* Location privacy of a tag must be protected and untraceable. It is property that the attacker cannot track a tag using the location information of the tag.

- *Information privacy:* is property that tag information must be only accessible by legitimate reader and server. Otherwise, the tag could be vulnerable for tracking, privacy cloning, and other attacks.

2.2 Examination and Comparisons of Authentication Protocols

Unlike the study of Soos (2017) where protocols are categorized according to the services provided and the employed algorithms, this section presents 22 recently proposed RFID authentication protocols with respect to their class; some protocols are examined and explained in detail while others are given in the tables. The first column of Table 2.1 lists the 22 protocols in terms of their class starting from fully fledged protocols and ending with ultra-lightweight protocols. The second column gives the function that the protocol is based on. The third column gives the verification tool used for the authentication. The EPC column lists whether the protocol is compatible with EPC C1-G2. The ‘compared with’ column lists the other protocols that the protocol is compared with. The last column gives the class of the authentication protocol. The protocols comparison in terms of security threats and security services in Table 2.2.

Whilst, Table 2.3 presents the examined paper names and publishing year along with their references.

2.2.1 Fully Fledged Protocols

The fully-fledged class involves cryptographic algorithms that are divided mainly into two groups: symmetric algorithms and asymmetric algorithms. Asymmetric algorithms based on ECC are strong in terms of security and the services they provide. Compared with the RSA scheme, ECC-based systems are smaller, faster and consume less power. Hereby, for resource constrained systems, the ECC-based algorithm is a better choice than the RSA algorithm. It is noted that the RSA scheme has an ECC-based variant. Many ECC-based authentication protocols have thus been proposed to satisfy severely constrained tags.

In 2006, Tuyls & Batina (2006), using the Schnorr identification protocol, proposed an ECC-based RFID identification protocol. They asserted that the protocol is resistant against tag counterfeiting. However, in 2008, Lee, Batina, & Verbauwhede (2008) showed that protocol of Tuyls & Batina (2006) is defenseless against a location tracking, does not insure forward security nor mutual authentication and lacks scalability. In 2007, Batina et al. (2007), based on Okamoto's authentication protocol, proposed an RFID identification protocol based on ECC and mentioned their proposal could avoid active attacks. Yet, Lee et al. (2008) stated that the protocol is vulnerable in terms of forward security and location tracking attack and lacks scalability. Lee et al. (2008) claimed to have solved these three issues, but studies (Van Deursen & Radomirovic, 2008; Bringer, Chabanne, & Icart, 2008) showed that proposal of Lee et al. (2008) is defenseless against tracking and forgery attacks and does not provide mutual authentication.

In 2009, by reconstructing the three components of elliptic curve discrete logarithm problem based randomized access control (EC-RAC) (Lee et al., 2008); transfer schemes for secure ID and the secure password, and the server's authentication according to the system requirements and security properties, Lee, Batina, & Verbauwhede (2009) proposed 6 different protocols to minimize the computation amount on tags. In 2010, Lee, Batina, Singelee, Preneel, & Verbauwhede (2010) came

up with an ECC-based authentication protocol that addressed the existing tracking problems for the protocols presented in (Tuyls & Batina, 2006; Batina et al., 2007). This scheme considers only tag to reader identification and excludes reader to tag authentication. In 2011, Zhang, Li, Wu, & Zhang (2011) proposed a randomized key protocol based on ECC that is an improvement on the schemes of Lee et al. (2010). and Tuyls & Batina (2006). This protocol is safe against some relevant attacks, but still does not provide mutual authentication.

In 2014, to achieve mutual authentication, Liao & Hsiao (2014) proposed a secure authentication protocol based on the strength of ECC with an ID-verifier transfer protocol. However, studies (He, Kumar, Chilamkurti, & Lee, 2014; Moosavi, Nigussie, Virtanen, & Isoaho, 2014; Zhao, 2014) showed that proposal of Liao & Hsiao (2014) suffers from security flaws and lacks performance efficiency. Later in the same year, using ECC, Chou (2014) proposed an authentication protocol and informed that their proposal can resist different attacks. Nevertheless, Zhang & Qi (2014) showed that Chou's proposal faces problems in terms of tag information privacy and backward and forward traceability. Then, in 2015, Jin et al. (2015) suggested a secure mutual authentication protocol for healthcare environments based on ECC and asserted that their proposal can resist different attacks and performs better than schemes presented in (He et al., 2014; Zhang & Qi, 2014; Zhao, 2014).

In 2016, Farash, Nawaz, Mahmood, Chaudhry, & Khan (2016) showed that scheme of Zhang & Qi (2014) does not provide forward privacy. Very recent, in 2017, Ibrahim & Dalkılıc (2017b), proposed a strong and powerful mutual authentication protocol based on ECC and proven on WISP5. In the proposal, mutual authentication is proceeded in only two steps and withstands almost all common attacks and fulfills the RFID systems' security requirements.

Table 2.1 Techniques, verifications and classes of authentication protocols (C: class, F: fully fledged, S: simple, L: lightweight, UL: ultra-lightweight)

Protocol	Function Based on	Verificated by	EPC	Compared with	C
(Zhang & Qi, 2014)	ECC	……	X	(He et al., 2014; Zhang & Qi, 2014; Zhao, 2014)	F
Rostampour, Namin, & Hosseinzadeh, 2014)	Public Key Cryptography	BAN logic	X	(Chen & Deng, 2009; Han, Potdar, & Chang, 2007; Qian, Chen, You, & Lu, 2012; Qingling, Yiju, & Yonghua, 2008; Tian, Chen, & Li, 2012)	F
(Farash et al., 2016)	ECC	Random oracle model	X	(Chou, 2014; Liao & Hsiao, 2014; Zhang & Qi, 2014; Zhao, 2014)	F
(Ibrahim & Dalkılıc,2017b)	ECC & AES	Tested and realized on real devices	X	(Chou, 2014; Liao & Hsiao, 2014; Zhao, 2014; Zhang & Qi, 2014)	F
(Dalkiliç, Özcanhan, & Çakir, 2014)	Increasing key space using nonces	AVISPA	X	(Ha, Moon, Nieto, & Boyd, 2007; Liu, 2008; Toiruul & Lee, 2006)	F
(Özcanhan, Dalkılıç, & Utku, 2014)	Cryptographically supported NFC tags in Medication	Manually as in (Peris-Lopez, Safkhani, Bagheri, & Naderi, 2013)	X	(Peris-Lopez et al., 2013)	F
(Hakeem, Raahemifar, & Khan, 2013)	One-way hash function and semi randomized encryption keys	Manually as in (Changqing, Jixiong, Zhengyan, & Shengye, 2008)	X	(Changqing et al., 2008; Chatmon, van Le, & Burmester, 2006; Tsudik, 2007; Tuyls & Batina, 2006; Weis et al., 2004)	F
(Srivastava, Awasthi, Kaul, & Mittal, 2015)	Hash based	….	X	(Chatmon et al., 2006; Cho, Yeo, & Kim, 2011; Tsudik, 2007)	S
(Shen, Tan, Moh, Chung, & Wang, 2016)	Hash based	Manually	X	(Chien, 2007; He, Jin, Zhang, & Li, 2009; Peris-Lopez, Hernandez-Castro, Estevez-Tapiador, & Ribagorda, 2006a; Peris-Lopez, Hernandez-Castro, Estevez-Tapiador, & Ribagorda, 2006b; Peris-Lopez, Hernandez-Castro, Estevez-Tapiador, & Ribagorda, 2006c; Rahman, Soshi, & Miyaji, 2009; Tan, Sheng, & Li, 2008)	S
(Li, Zhou, & Wang, 2017)	Hash and PRNG based	GNY logic (Zhu, Yang, & Zhang, 2007)	√	(Cho, Jeong, & Park, 2012; Jeon & Yoon, 2013b; Mujahid, Najam-ul-Islam, & Shami, 2015)	S
(Kardaş, Celik, Arslan, & Levi, 2013)	Constant-time complexity	Byzantine adversarial model (Changqing et al., 2008)	X	Kardas, Levi, & Murat, 2011)	S
(Fan, Li, Li, Liang, Shen, & Yang, 2014)	Hash operation & RNG	GNY logic (Zhu et al, 2007)	X	(Gao et al., 2004; Henrici & Muller, 2004; Li & Ding, 2007; Molnar & Wagner, 2004; Ohkubo, Suzuki, & Kinoshita, 2004; Sarma, Weis, & Engels, 2003; Weis et al., 2004)	S
(Ren, Xu, & Li, 2013)	One-way Hash Function	GNY logic (Zhu et al, 2007)	X	(Ning, Liu, Mao, & Zhang, 2011; Song & Mitchell, 2008; Weis et al., 2004)	S
(Maarof, Labbi, Senhadji, & Belkasmi, 2016)	XOR, PRNG and CRC based	Manually	√	(Chen & Deng, 2009; Huang & Jiang, 2012).	L
(Zhang, Liu, Wang, Yi, & Wu, 2017)	XOR and PRNG based	Manually as (Zhang et al., 2016)	√	(Alomair, Clark, Cuellar, & Poovendran, 2012; Ha, Ha, Moon, & Boyd, 2006; Habibi, Alagheband, & Aref, 2011; Xiao, Zhou, Zhou, & Niu, 2013)	L
(Pang, Li, He, Alramadhan, & Wang, 2014)	Fast tag indexing, CRC & PRNG	A Simulation Program	√	(Choi, Lee, & Lee, 2005; Dimitriou, 2005; Henrici & Muller, 2004; Song & Mitchell, 2008; Weis et al., 2004; Zhang, Zhou, & Luo, 2008; Zhou, Zhang, Luo, & Wong, 2010)	L
(Lin, & Song, 2013)	Learning parity with noise	Manually as in (Juels & Weis, 2005)	√	(Hopper & Blum, 2001; Juels & Weis, 2005; Leng, Mayes, & Markantonakis, 2008; Munilla & Peinado, 2007)	L
Tounsi, Cuppens-Boulahia, Garcia-Alfaro, Chevalier, & Cuppens, 2014)	A Pseudo Random Generator Shared Between Readers and Tags	AVISPA	√	(Asadpour & Dashti, 2011; Burmester & Munilla, 2011; Brusó, Chatzikokolakis, & Den Hartog, 2010; HanataniI, Ohkubo, Matsuo, Sakiyama, & Ohta, 2012; Kim, Oh, Kim, Jeong, & Choi, 2008; Van Le, Burmester, & De Medeiros, 2007)	L
(Gao, Ma, Shu, & Wei, 2014)	CRC and permutation	Simple Promela Interpreter (SPIN)	√	(Chien, 2007; Peris-Lopez et al., 2006a; Peris-Lopez, Hernandez-Castro, Tapiador, & Ribagorda, 2009; Tian et al., 2012)	L
(Luo, Wen, Su, & Huang, 2016)	A security ultralightweight bitwise conversion	Manually	√	(Chien, 2007; Mujahid et al., 2015; Peris-Lopez et al., 2006b; Peris-Lopez et al., 2006c; Peris-Lopez et al., 2009; Tian et al., 2012; Zhuang, Zhu, & Chang, 2014)	UL
(Tewari & Gupta, 2017)	XOR bitwise rotation based	Manually	√	(Chien, 2007; Peris-Lopez et al., 2006a; Peris-Lopez et al., 2006b; Peris-Lopez et al., 2006c; Peris-Lopez et al., 2009 ; Tian et al., 2012)	UL
(Kardaş et al., 2015	Physically Uncloneable Functions PUF	….	√	(Bassil, El-Beaino, Itani, Kayssi, & Chehab, 2012; Ranasinghe, Engels, & Cole, 2004; Tuyls, & Batina, 2006)	UL

Asymmetric algorithms are not the only choice for RFID systems because they are time consuming. Moreover, their implementation to RFID systems remains considerably challenging. Some researchers have thus directed their attention towards symmetric schemes, which are divided mainly into two groups: block ciphers and stream ciphers. Stream ciphers are faster and easier to implement but are weaker comparing with block ciphers. Block ciphers are thus preferable, and the most popular block cipher encryption algorithm is AES.

It is worth mentioning that Feldhofer, et al., 2004 introduced an efficient implementation of AES in 2004. However, Kaps (2008) noted that the implementation of the extended tiny encryption algorithm (XTEA) needs less power and fewer resources than that of the AES. Furthermore, searches that use the AES mostly refer to the number of gates rather than the security goals of the authentication protocol, which is beyond the scope of our thesis.

2.2.2 Simple Protocols

The simple protocol class includes protocols that support RNG and a one-way hash function. Ohkubo, Suzuki, & Kinoshita (2003) came up with a strong protocol, as an example of a hash-based protocol, in 2003. However, the tag searching cost by the server is high for this protocol. In the same year, the proposal was updated by Weis et al. (2001) under the name of the hash-lock protocol. Although the hash-lock protocol performs well in tag implementation and effectiveness of the server, it performs poorly in terms of security. In 2006, Tsudik claimed that yet another trivial RFID authentication protocol (YA-TRAP) (Tsudik, 2006) resists the tracing attack.

In 2007, however, Tsudik noted the flaws of his previous protocol and proposed a new protocol (Tsudik, 2007), even though his new protocol does not reflect his original purpose and is vulnerable to a reply attack. In 2011, Chien, Yang, Wu, & Lee, (2011) showed that the scheme presented in (Tsudik, 2007) is vulnerable to replay attacks and DoS and proposed a secured version. In the same year, Peris-Lopez, Orfila, Mitrokotsa, & Van der Lubbe (2011) claimed that the proposal of Chien et al. (2011) is defenseless against impersonation and replay attacks and proposed a new concept called inpatient safety RFID system (IS-RFID).

In 2012, Yen, Lo, & Wu (2012) noted that medication evidence generated by an IS-RFID system can be modified by a hospital easily. Chen, Huang, Tsai, & Jan (2012) suggested a forge resistant protocol that withstands impersonation, desynchronization and traceability attacks. In 2012, Cho et al. (2012) came up with a hash function based mutual authentication protocol that was inspired from his previous work (Cho et al., 2011). In the years 2012 and 2013, the scheme of Cho et al. (2012) was analyzed by (Kim, 2012, 2013) and found to be most vulnerable to a desynchronization attack.

In 2014, Safkhani et al. (2014) also analyzed the scheme of Cho et al. (2012) and showed that it is vulnerable to desynchronization, tag and reader impersonation. Moreover, the scheme introduced in (Kim, 2012, 2013) based on the work presented in (Cho et al., 2012) was analyzed (Safkhani, Peris-Lopez, Castro, & Bagheri, 2014) and found to have the same security faults. In 2015, a new mutual authentication protocol based on hash function proposed by Srivastava et al. (2015) was qualitatively compared with protocols proposed in (Chatmon et al., 2006; Cho et al., 2011; Tsudik, 2007) and found to be superior. In 2016, Shen et al. (2016) proposed an efficient RFID authentication protocol (ERAP) and claimed that compared with the previous researches, their protocol withstands different types of attacks with low cost, which satisfies the requirement of highly resource constrained RFID tags. Finally, Li et al. (2017) pointed out that the lightweight mutual authentication protocol (LMAP) (Peris-Lopez et al., 2006b) is vulnerable to some attacks and data integrity. To improve the security and the privacy of LMAP, they proposed an improved version of LMAP and claimed that their protocol meets all the requirements of RFID applications and resists common attacks.

Other protocols that may fall into this class and be worthy of mention are the Hopper and Blum (HB) family of protocols. In 2001, Hopper and Blum proposed an extraordinarily lightweight protocol that uses only the AND and XOR operations on binary vectors and a noise bit called the HB bit (Hopper & Blum, 2001) that can be generated from a physical event. To resist passive attacks, the protocol depends on the computational complexity of the learning parity with the noise problem.

The HB protocol was not designed for RFID or categorized as being lightweight or ultra-lightweight. Afterwards, the lightweight authentication protocol family based on

the HB protocol was proposed. As the HB protocol resists passive attacks, Juels and Weis proposed in 2005 a modified protocol, named the HB+ protocol (Juels & Weis, 2005), to resist active attacks. They claimed that their protocol is lightweight but may not be directly applied to RFID tags, and their use of a two-round version may not be secure. Also, in 2005, Gilbert et al. (2005) mentioned that the HB+ protocol is defenseless against a linear time active attack.

In 2006, Bringer et al. (2006) modified the HB+ protocol to develop the HB++ protocol, which avoids the attack of Gilbert et al. (2005). However, to detect attacks, it requires universal hash functions and additional secret key material. In 2007, Munilla & Peinado (2007) introduced the idea of a round and proposed a new protocol, named as the HB-MP protocol, to resist man-in-the-middle and active attacks that are effective against HB and HB+ protocols.

In 2008, Gilbert, Robshaw, & Seurin (2008a) revealed that it is possible for a simple passive attack to impersonate a valid tag by eavesdropping on communication. In 2008, the HB# protocol was introduced as an improvement on the Random-HB# protocol that was described in the same work (Gilbert, Robshaw, & Seurin, 2008b). The HB# protocol is resistant against an extended class of active attacks embracing the active attack of Gilbert et al. (2008a) on HB+ and HB-MP protocols and, unlike the HB++ protocol (Bringer et al., 2006), the HB# protocol does not require additional hardware that would increase the complexity of the HB protocol. Also, in 2008, Leng et al. (2008) improved on the HB-MP protocol by proposing the HB-MP+ protocol. However, Yoon, Sung, Yeon, & Oh (2009) noted that the HB-MP+ protocol does not have a real function with which to defend against an advanced active attack or strong methods for preventing the tracking problem, and they subsequently proposed the HB-MP++ protocol. Again in 2008, Ouafi, Overbeck, & Vaudenay (2008) conducted a man-in-the-middle attack on the HB# protocol and retrieved a secret shared by communicating parties.

In 2011, Halevi, Saxena, & Halevi (2011) indicated that PRF-based protocols, such as HB+ and HB# protocols, are not applicable to low-cost tags, and announced Tree-HB+ and Tree-HB# protocols. In 2012, the GHB# (Rizomiliotis & Gritzalis, 2012)

protocol was developed and claimed to resist a man-in-the-middle attack, which is an effective attack on the HB# protocol. With the proposal of the Tree-LSHB+ protocol

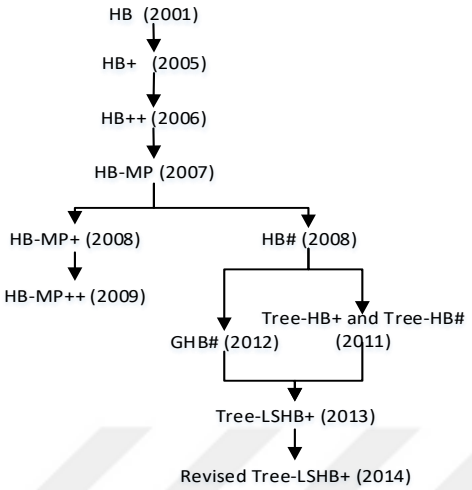

Figure 2.1 Evolution of the HB family

of Deng, Li, Zhang, & Wang (2013), they claimed that tree-based and regular HB protocols provide only one-way authentication, only tag is authenticated by the reader, and they added mutual authentication. Finally, Qian, Liu, Yang, & Zuo (2014) mentioned the Tree-LSHB+ protocol cannot resist disclosure, desynchronization and traceability attacks. Moreover, in (Qian et al., 2014), a revised Tree-LSHB+ protocol was developed and claimed to have advantages over the past Tree-LSHB+ protocol. The evolution of the HB family protocols is shown in Figure 2.1. Other examined protocols of this class are presented in Tables 2.1 and 2.2.

2.2.3 Lightweight Protocols

The lightweight protocol class includes protocols that require simple functions, such as CRC code, and an RNG and broadly involves protocols conforming to the EPC C1-G2 standard. Operations supporting EPC C1-G2 might not be ideal for security purposes and it is thus important to improve them. Moreover, it is usual to face new problems when trying to solve expected problems. In protocols conforming to the EPC C1-G2 standard, the main security problem is CRC-16 (owing to the algebraic weakness of CRC (a $\oplus$ b) = CRC (a) $\oplus$ CRC (b)).

In 2005, Juels (2005) was among the first to propose a solution that conforms to the EPC C1-G2 and was claimed to resist cloning and spoofing. In the same year, Karthikeyan & Nesterenko (2005) proposed a protocol and used XOR and matrix operations not to be tracked and used timer and key updating to achieve mutual authentication. However, their protocol is vulnerable to DoS and replay attacks. In 2006, Duc et al. (2006) showed that scheme of Juels (2005) suffers from privacy and information leakage. Moreover, they proposed a new protocol that uses CRC, XOR and a pseudorandom-number generator (PRNG) to guarantee interactive information security, achieving mutual authentication and synchronous updating of the secret key. However, their protocol is vulnerable in terms of a DoS attack and forward security.

In 2007, Chien & Chen (2007) embellished on both the works of Karthikeyan & Nesterenko (2005) and Duc et al. (2006) in proposing a new protocol called the Chien & Chen (CC) protocol and claimed that they had achieved forward security and resistance against DoS and reply attacks; however, the claimed security objectives were later shown to be false owing to the linear property of the CRC operation used in the protocol. In the same year, Lo & Yeh (2007) improved the CC protocol (Chien & Chen, 2007) in terms of data security, privacy and efficiency, but the CC protocol is still vulnerable to eavesdropping and location tracking.

In 2009, Peris-Lopez, Hernandez-Castro, Estevez-Tapiador, & Ribagorda (2009) noted the CC protocol cannot hold tag and reader impersonation, desynchronization and tracing attacks. In 2010, Yeh, Wang, Kuo, & Wang (2010) asserted a new protocol, referred to as the secure remote password (SRP) protocol, which is easy and convenient to implement and which they claimed not only resolved the flaws of the CC protocol but also enhanced the overall performance efficiently. However, Habibi et al. (2011) and Habibi, Gardeshi, & Alaghband (2011) noted that the SRP protocol is defenseless to a tracking attack and information leakage and that the complexity of a successful attack is only 2^{16}, and they improved SRP and suggested this new version.

In 2014, Mohammadi, Hosseinzadeh, & Esmaeildoust (2014) studied the scheme proposed in (Habibi et al., 2011) and showed that it is vulnerable to an attack that reveals secret parameters, a tag impersonation attack, a data desynchronization attack and a traceability attack. Additionally, they improved the scheme proposed in (Habibi

Table 2.2 Comparison of authentication protocols in terms of security threats and security services (F: fully fledged, S: simple, L: lightweight, UL: ultra-lightweight)

Protocol	Zhang & Qi, 2014	Rostampour et al. 2014)	Farash et al., 2016)	Ibrahim & Dalkılıc, 2017b	Dalkiliç et al., 2014)	Özcanhan et al., 2014	Hakeem et al., 2013	Srivastava et al., 2015	Shen et al., 2016	Li et al. 2017	Kardaş et al., 2013	Fan et al., 2014	Ren et al., 2013	Maarof et al., 2016	Zhang et al., 2017	Pang et al., 2014	Lin, & Song, 2013	Tounsi et al., 2014	Gao et al., 2014	Luo et al., 2016	Tewari & Gupta, 2017	Kardaş et al., 2015
SECURITY THREATS																						
Tracking attack				√			√		√		√	√		√					√	√		
DoS	√	√		√	√	√	√						√	√			√		√			√
De- Synchronize	√	√		√	√	√	√	√	√		√	√			√	√	√			√		
Man-In-The-Middle	√	√	√	√	√	√	√	√							√		√				√	
Impersonation attack	√		√	√		√	√		√	√		√		√	√		√					√
Cloning attack	√			√		√			√			√	√	√		√						
Full disclosure attack				√		√			√										√	√	√	
Eaves dropping		√		√				√									√	√				
Replay attack	√	√	√	√	√	√		√		√	√	√	√	√	√	√	√		√		√	√
SECURITY SERVICES																						
Mutual authentication	√	√	√	√	√	√	√	√			√		√	√	√			√			√	√
Confidentiality	√	√		√	√	√	√			√		√					√		√		√	
Availability	√			√																		
Forward security	√	√	√	√		√	√		√	√	√	√		√		√		√				
Backward security			√	√						√	√					√		√				√
Ownership transferable											√											
Tag anonymity	√			√																	√	
Traceability	√	√	√	√		√		√		√	√	√										
Location privacy			√	√			√									√						√
Information privacy	√			√			√									√		√				
CLASS																						
Class	**F**	**F**	**F**	**F**	**F**	**F**	**F**	**S**	**S**	**S**	**S**	**S**	**S**	**L**	**L**	**L**	**L**	**L**	**L**	**UL**	**UL**	**UL**

et al., 2011) and proposed a new protocol called the improved lightweight mutual authentication protocol (ILMAP). Later, in 2014, Alavi, Baghery, & Abdolmaleki (2014) investigated the ILMAP protocol and showed that it is vulnerable to an attack that reveals secret parameters, a data integrity attack, a reader forward compromise attack, a traceability attack and backward and forward traceability attacks. Additionally, by altering processes of the ILMAP, they proposed a strengthened version of the ILMAP. In 2013, based on the SRP protocol, Pang, He, Pei, & Wang (2013) suggested an authentication protocol, named SRP+, and they argued that they had overcome the weaknesses of the SRP protocol and increased the complexity of a successful attack to 2^{23}.

In 2015, however, Wang, Liu, & Chen (2015) analyzed the SRP+ protocol and showed that it is vulnerable to a desynchronization attack because of the well-known security defect of the CRC function and a passive disclosure attack with a complexity of O (2^{16}). Furthermore, an updated version of the SRP+, called the SRP++, has been proposed and it has been asserted that this proposal can withstand disclosure attack with a complexity reaching O (2^{32}), thus providing better security than its predecessors.

In 2016, Maarof et al. (2016) suggested a new mutual authentication scheme that is compliant with EPC C1-G2 standard. They demonstrated that their scheme resists against security attacks, is better than the previous schemes and is easy to implement in low cost RFID systems because the simple operators (XOR, CRC and PRNG) are used. Finally, Zhang et al. (2017) proposed a lightweight RFID authentication protocol with strong trajectory privacy protection (LAP-STP). They informed their protocol can withstand different attacks and warrant the strong trajectory privacy. Other examined protocols of this class are given in Tables 2.1 and 2.2.

2.2.4 Ultra-lightweight Protocols

Ultra-lightweight protocols are tailored specially to extremely constrained devices in which only simple bit-wise operations (e.g., XOR, AND, OR) are implemented. After Gen-2 was released in 2006, (Peris-Lopez et al., 2006a, 2006b, 2006c). proposed ultra-lightweight RFID protocols named the ultralightweight mutual authentication protocols (UMAPs) and comprising the minimalist mutual authentication protocol

Table 2.3 Examined protocols' reference numbers and names

Ref.	Paper Name and Publishing Year
(Zhang & Qi, 2014)	A secure RFID mutual authentication protocol for healthcare environments using elliptic curve cryptography (2015)
(Rostampour et al. 2014)	A novel mutual RFID authentication protocol with low complexity and high security (2014)
(Farash et al., 2016)	A provably secure RFID authentication protocol based on elliptic curve for healthcare environments (2016)
(Ibrahim & Dalkılıc, 2017b)	An advanced encryption standard powered mutual authentication protocol based on elliptic curve cryptography for RFID, proven on WISP (2017)
(Dalkiliç et al., 2014)	Increasing key space at little extra cost in RFID authentications (2014)
(Özcanhan et al., 2014)	Cryptographically supported NFC tags in medication for better inpatient safety (2014)
(Hakeem, et al., 2013)	HPAP: A novel authentication scheme for RFID systems (2013)
(Srivastava et al., 2015)	A hash based mutual RFID tag authentication protocol in telecare medicine information system (2015)
(Shen et al., 2016)	An efficient RFID authentication protocol providing strong privacy and security (2016)
(Li et al., 2017)	Cryptanalysis of the LMAP protocol: A low-cost RFID authentication protocol. (2017)
(Kardaş et al., 2013)	An efficient and private RFID authentication protocol supporting ownership transfer (2013)
(Fan et al., 2014)	RSEL: revocable secure efficient lightweight RFID authentication scheme (2014)
(Ren et al., 2013)	An one-way hash function based lightweight mutual authentication rfid protocol (2013)
(Maarof et al., 2016)	A novel mutual authentication scheme for low-cost RFID systems (2016)
(Zhang et al., 2017)	An efficient lightweight RFID authentication protocol with strong trajectory privacy protection (2017)
(Pang et al., 2014)	Secure and efficient lightweight RFID authentication protocol based on fast tag indexing (2014)
(Lin, & Song, 2013)	An improvement in HB-family lightweight authentication protocols for practical use of RFID system (2013)
(Tounsi et al., 2014)	KEDGEN2: A key establishment and derivation protocol for EPC Gen2 RFID systems (2014)
(Gao et al., 2014)	An ultralightweight RFID authentication protocol with CRC and permutation (2014)
(Luo et al., 2016)	SLAP: Succinct and lightweight authentication protocol for low-cost RFID system (2016)
(Tewari & Gupta, 2017)	Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags (2017)
(Kardaş et al., 2015)	k-strong privacy for radio frequency identification authentication protocols based on physically unclonable functions (2014)

(M^2AP) (Peris-Lopez et al., 2006a), LMAP (Peris-Lopez et al., 2006b) and efficient mutual authentication protocol (EMAP) (Peris-Lopez et al., 2006c), which use only triangular functions (∨, ∧, ⊕) and addition (Özcanhan, Dalkılıç, & Utku (2014). This family is efficient for low-cost RFID tags in terms of the computation cost and storage cost.

In 2007, however, (Li & Deng, 2007; Li & Wang, 2007) presented several attacks on the M^2AP, LMAP and EMAP. In the same year, Chien (2007) pointed out the UMAPs were vulnerable to many attacks, introduced the rotation operation and proposed the strong authentication and strong integrity (SASI) protocol. However, owing to its use of triangular functions (∨, ⊕), only a limited number of rotations and addition, SASI protocol is defenseless against various kinds of attacks and this was shown by (Hernandez-Castro, Tapiador, Peris-Lopez, & Quisquater, 2009; Phan, 2009). Later, in 2009, (Peris-Lopez et al., 2009), used XOR encapsulated in nested rotation functions and addition and produced Gossamer protocol, which is inspired from the SASI protocol.

In 2010, however, Tagra, Rahman, & Sampalli (2010) conducted a desynchronization attack on Gossamer. After Gossamer, in 2009, Peris-Lopez, Hernandez-Castro, Estevez-Tapiador, & Ribagorda (2009) slightly improved the LMAP and produced the ultra-lightweight authentication protocol (ULAP), which uses only addition and triangular functions, to overcome passive attacks. Meanwhile, in 2010, a passive attack on ULAP was conducted by Wang & Wang (2010).

In 2012, Tian et al. (2012) proposed an interesting ultra-lightweight RFID authentication protocol, named the RFID authentication protocol with permutation (RAPP), have only bit-wise eXclusive OR, left circular rotation and permutation. However, because the Hamming weight of rotation and permutation is invariant (i.e., the Hamming weight output of two operations is the same as that of the first parameter) and because of permutation properties, Zhuang, Wang, Chang, & Zhu (2013) applied two attacks on the RAPP that can cause a tag to fall into the DoS state in addition to desynchronization and replay attacks.

Also, in 2013, Jeon & Yoon (2013a) by using merge (merging two-bit strings) and separation (inverse of merging) operations suggested a new authentication protocol called the efficient ultra-lightweight RFID authentication protocol (EURFID). In the same year, however, the same authors (Jeon & Yoon, 2013b) found that EURFID protocol does not serve correctly in the case of collision between tags and they improved EURFID protocol and proposed the RFID authentication protocol for low-cost tags (RAPLT) that is a new merge and separation operations based ultra-lightweight protocol. Nevertheless, RAPLT is vulnerable in terms of replay and desynchronization attack, protecting data integrity and user privacy according to Zhuang, Zhu, & Chang (2013). In 2015, Wang et al. (2015) applied a passive disclosure attack on the RAPLT using the linear property of the merge operation and applied de-synchronization attack on SRP+ (Pang et al., 2013) using the linearity feature of CRC operation. They presented a modified and efficient version of SRP+ protocol that is EPC C1-G2 standard compliant, denoted by SRP++. They claimed for this protocol that exhaustive search attack could be resisted.

In 2016, Luo et al. (2016) presented a new secure ultra-lightweight bitwise conversion based ultra-lightweight mutual authentication protocol. The aim was to improve the ultra-lightweight authentication against the weak security resistance in recent protocols described in references (Zhuang et al., 2014) and (Mujahid et al., 2015). Their protocol employed only three bitwise operations; XOR, left rotation and conversion. They claimed that their protocol is more secure than other compared protocols, can resist various existing attacks and preferable in a low-cost RFID system than other compared protocols. Finally, in 2017, Tewari & Gupta (2017) presented an ultra-lightweight mutual authentication protocol that uses bitwise XOR and left-rotation. They pointed out that their protocol ensures data confidentiality, integrity, tag anonymity, and has resistance against tracking and various attacks. Other examined protocols of this class are given in Tables 2.1 and 2.2.

2.2.5 Less Traditional Forms of Authentication

It is worth mentioning that less traditional forms of authentication such as using exhaustive searches to enable privacy-preservation, are also used. The mechanism of randomizing a tag identifier to protect its privacy was firstly proposed in 2003 by Sarma et al. (2003). By using a nonce generated by a tag and secret value, they computed the identifier. In the same year, Ohkubo et al. (2003) and in 2005 Avoine & Oechslin (2005) improved this idea by a different approach; the key that produced the identifier continually changes, where the new key was the message digest of the former.

In 2008, Henrici & Müller (2008) used the same approach of Ohkubo et al. (2003) and Avoine & Oechslin (2005), but the new key was triggered by the hash chains of the former. The main problem of randomized tag identifier is on the server side where the identifier has to be searched among a bulk of data. A solution to this problem is a tree search structure approach used by Molnar & Wagner (2004), Molnar, Soppera, & Wagner (2005) and Dimitriou (2006). In this proposal, branches have specific keys and each tag has set of keys. To identify a tag, the keys on each level and on a specific branch are used.

However, in 2010, Avoine, Coisel, & Martin (2010) mentioned that protocols that use exhaustive searches are vulnerable to a timeful attack. In 2014, Figueiredo, Zúquete & e Silva (2014) proposed a protocol where RFID tags are used on vehicles. The tag, uses the stored secret key with two random values generated by the reader and the tag itself to generate the pseudo-random identifier. The identification application makes an exhaustive search to discover the tag that generated the identifier.

2.3 Comparison Evaluation

In Table 2.2, the protocols are compared in terms of security threats and services. Each of the examined protocols has a specific ability to cope with security and privacy issues. When the number of checks counted from the table, the class that overcomes most threats and provides more services is the fully fledged and the class that overcomes least threats and provides least services is the ultra-lightweight. The protocol presented in (Ibrahim & Dalkılıc, 2017b), which provides the best security is

fully fledged, and has overcome (9) threats and provides (9) services. The protocol presented in (Luo et al., 2016), which provides the least security is ultra-lightweight, and has overcome (3) threats and provides (0) service. This is to be expected considering the definitions of authentication classes.

In other words, less can be achieved with an authentication protocol when the hardware capability of a tag is low. Not surprisingly, most of the practical RFID-based applications such as building access control (Rohr, Nohl, & Plötz, 2010), e-passports (Kumar & Srinivasan, 2012), electronic toll collection (Hwang, Su, & Tsai, 2010) and electronic ticketing (Nair, Arun, & Joseph, 2015) are using fully fledged class. Moreover, the widely-used technology in this field, such as Calypso Secure (2014) and most generations of MIFARE (Schalk, 2013) (Table 2.4) are using fully fledged class. When the matter is the life of a person and privacy, this is to be expected. However, the cost must be reduced and a need for more and stronger light and ultra-lightweight authentication protocols is obvious. For the readers who want to deepen on other specific features, please check UCODE (2017).

Table 2.4 MIFARE products overview (DES: Data Encryption Standard)

Products	**Authentication**	**Confidentiality**
MIFARE Classic EV1	CRYPTO1	CRYPTO1
MIFARE Plus	AES	CRYPTO1 + AES
MIFARE Plus SE	AES	CRYPTO1 + AES (Optional)
MIFARE Plus EV1	AES	AES
MIFARE Ultralight C	3DES	-
MIFARE Ultralight EV1	-	-
MIFARE Ultralight Nano	-	-
MIFARE DESFire EV1	AES + 3DES + DES	AES + 3DES + DES
MIFARE DESFire EV2	AES + 3DES + DES	AES + 3DES + DES

CHAPTER THREE

PRELIMINARIES

After the comprehensive survey that we did in the previous chapter, Chapter Two, we deduced that there is a need for a strong mutual authentication protocol. Particularly, after FDA' declaration and being protocols conforming to EPC C1 G2 inadequate for healthcare environments. Taking the advantage of having a real experimental tag, WISP5, and taking the opportunity that AES is embedded in WISP5, we proposed a stable and powerful mutual authentication protocol exploiting both symmetric (AES) and asymmetric (ECC) algorithms. We used the ECDH to produce the secret key that will be used to in AES to encrypt tag ID. Furthermore, we used the ECDSA to maintain message integrity, prevent man-in-the-middle attacks that ECDH suffer from, and achieve authentication between the tag and the reader. So, in this chapter, we tried to refresh reader's memory and give a brief preliminary of some important topics that will stay with us until end of this thesis.

3.1 Advance Encryption Standard (AES)

As DES become insufficient to today's technology, it replaced with AES by US National Institute of Standards and Technology (NIST). The AES is 128-bit Rijndael block cipher and accept three different key lengths 128, 192 and 256 bits (Figure 3.1), where x is the plaintext, y is the ciphertext, k is key and n_r is the number of rounds.

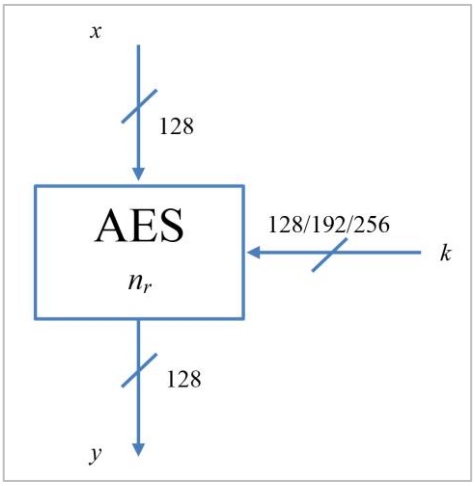

Figure 3.1 AES input/output

The AES is the most commonly used symmetric-key algorithm in industry standards and many commercial applications for today and expected for the next decades. Since AES encrypts 128 bits in a single iteration, it has comparatively few rounds. Rounds number of the cipher is varied from 10 to 14 according the key length, see Table 3.1 (Paar & Pelzl, 2009).

Since AES encrypts 128 bits in a single iteration, it has comparatively few rounds. AES consists of three different types of layers that each handle all 128 bits of the data.

Table 3.1 AES key lengths and rounds number

key lengths	Rounds number (n_r)xu
128 bit	10
192 bit	12
256 bit	14

As shown in Figure 3.2, each round consists of the three layers except the first which consists of Key Addition Layer only. Furthermore, the last round n_r do not apply the MixColumn sublayer making the encryption and decryption schemes symmetrical. For decryption scheme, see Figure 3.3. Code sample for both encryption and decryption are given in Appendix 2.

An explanation of each layer is given below:

- *Key Addition layer:* Is XORing the 128-bit round key with a portion of the expanded key.

- *Byte Substitution layer (S-Box):* Using lookup tables, each element is converted in nonlinear manner.

- *Diffusion layer*: It consists of two sublayers that perform linear operations:

    - The ShiftRows sublayer : is a simple permutation
    - The MixColumn sublayer: is mixing blocks of four bytes.

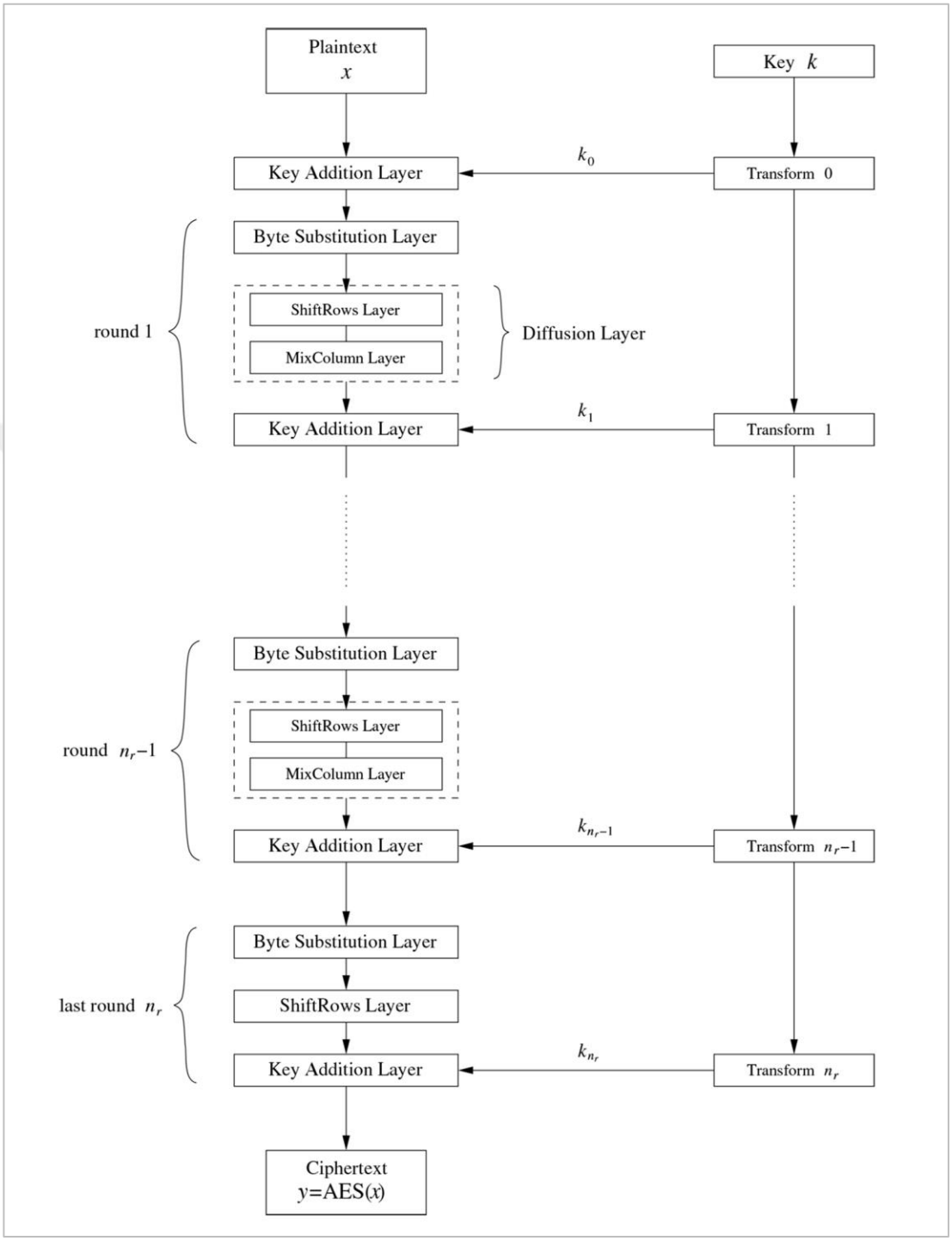

Figure 3.2 AES encryption block diagram (Paar & Pelzl, 2009)

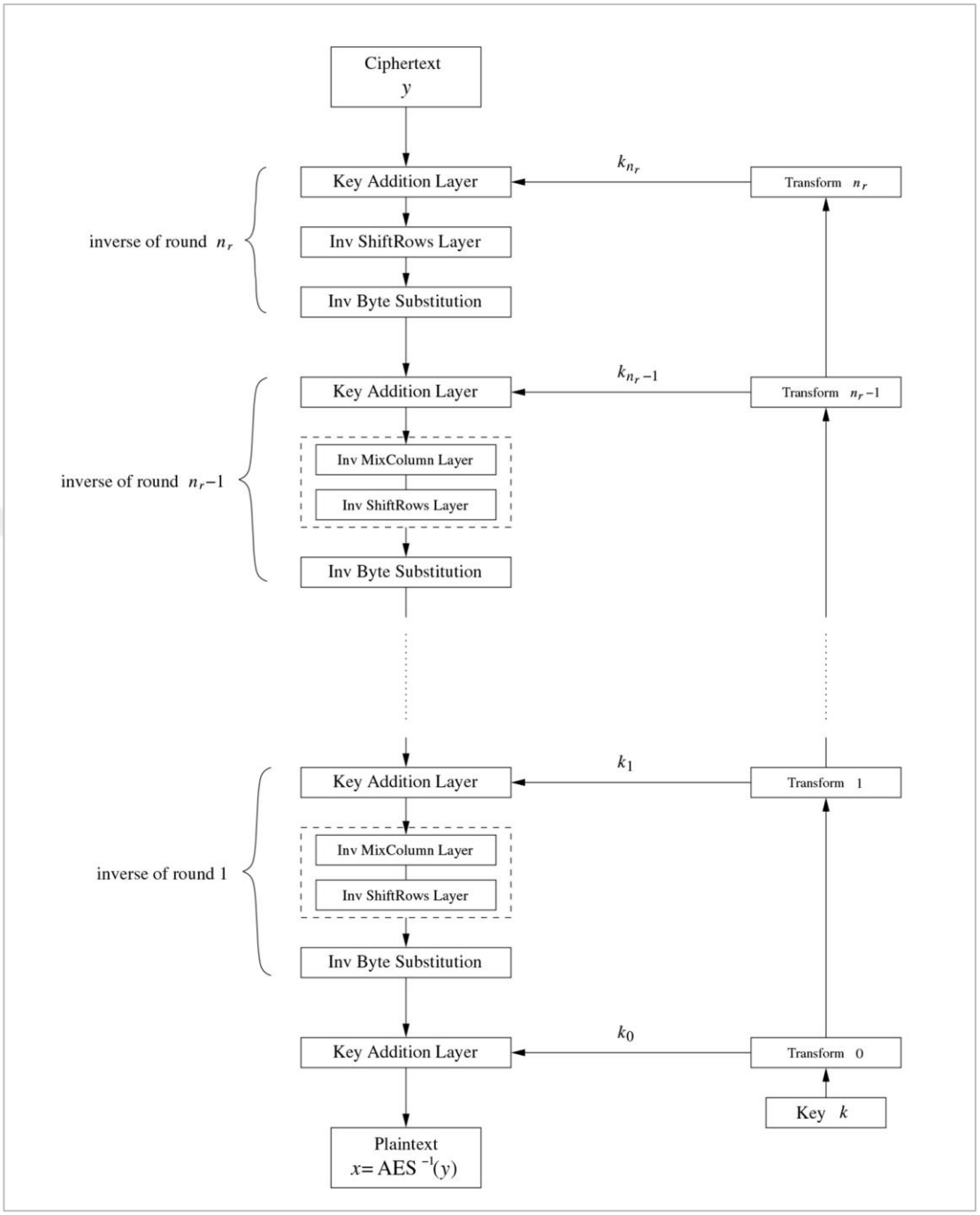

Figure 3.3 AES decryption block diagram (Paar & Pelzl, 2009)

3.2 Elliptic Curve Cryptography (ECC)

ECC is an asymmetric key cryptography that unlike other asymmetric key cryptography techniques, uses much smaller key sizes and ensures higher levels of security. ECC is very strong in terms of security and the services that provide.

Compared to RSA, ECC is smaller and faster consumes less power, fewer memory and CPU resources. For instance, as shown in Table 1.1, to secure a 256-bit AES key, 512-bit ECC can be expected to be on average 400 times faster than 15360-bit RSA (William & Stallings, 2006). Hereby, for resource constrained systems, ECC-based algorithm is a better choice than RSA algorithm.

Elliptic curves that used in cryptography could be identified over two finite fields: prime fields F_p, p is a large prime number, and binary fields F_2m (Hankerson, Menezes, & Vanstone, 2006). Our focus, in this thesis, is on elliptic curves over Fp. The equation of the elliptic curve over prime fields F_p is defined by $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$. Values a and b are constants $\in F_p$. Each value constitutes a variant elliptic curve. The points (x, y) that fulfill the above equation and a point at infinity O (that could be found by adding a point on the curve repeatedly to itself), are lies on the elliptic curve. For any G (G is generator point of elliptic curve) on an elliptic curve, the set {O, G, 2G, 3G,...} is a cyclic group (Hankerson et al., 2006). The public key Q is a point on the curve, and the private key P is a randomly selected integer number. The public key is calculated by multiplying P with G, e.g. Q=PG. This calculation called a scalar multiplication. The generator point G, the large prime number p and constants a and b with order of the elliptic curve n (number of times a point can be doubled until it reaches infinity O) and cofactor h (number of points on the curve divided by n ideally h = 1) are constitute the domain parameters of ECC that must be agreed by both parties during communication.

3.2.1 Group Operations on Elliptic Curves

For cryptographic usage, our focus is on the curve over a prime field. However, for better understanding, it can be plotting an elliptic curve equation over the set of real numbers. For Example, the elliptic curve $y^2 = x^3 - 3x + 3$ is shown over the real numbers (Figure 3.4).

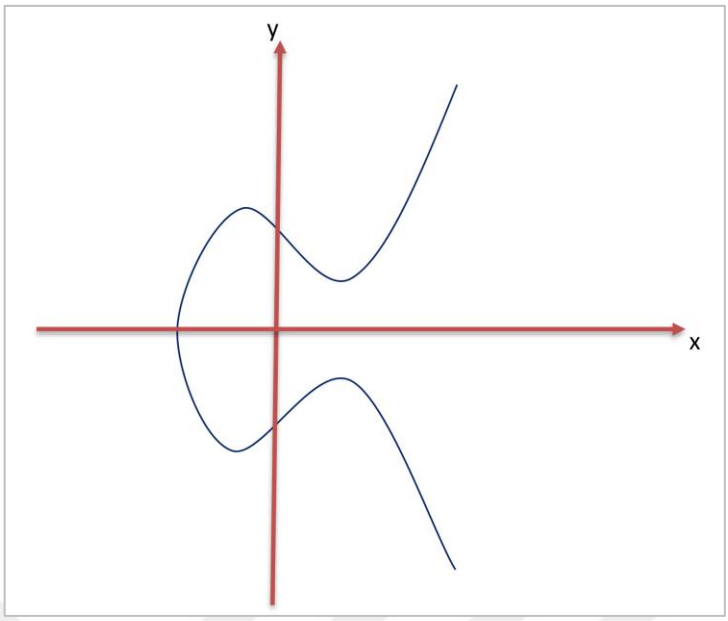

Figure 3.4 An example curve of elliptic curve

3.2.1.1 Point Addition

Adding points J and K to get point L on the curve, for example, L = J + K. The forming works as follows: draw a line from J passing K till intersect with the curve. Mirroring the intersection point along x-axis gives the point L (Figure 3.5).

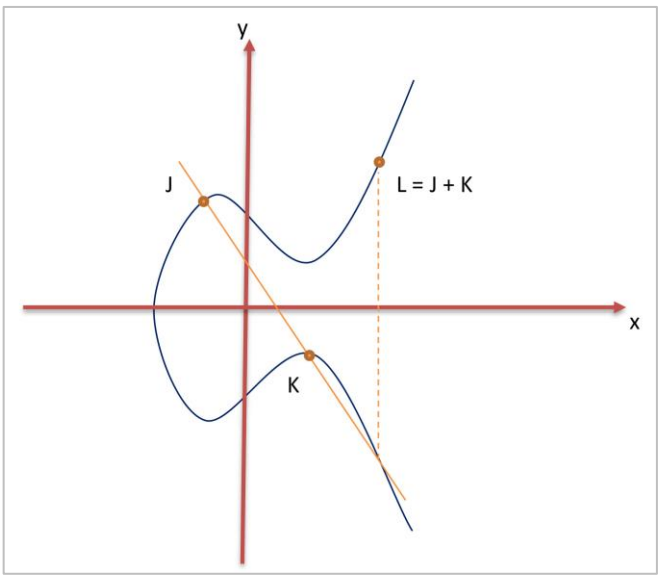

Figure 3.5 An example of point addition

3.2.1.2 Point Doubling

Adding point J to itself to get point L on the curve, for example, J + J = L. The forming works as follows: draw a tangent line through J till intersect with the curve. Mirroring the intersection point along x-axis gives the point L, the doubling of J (Figure 3.6).

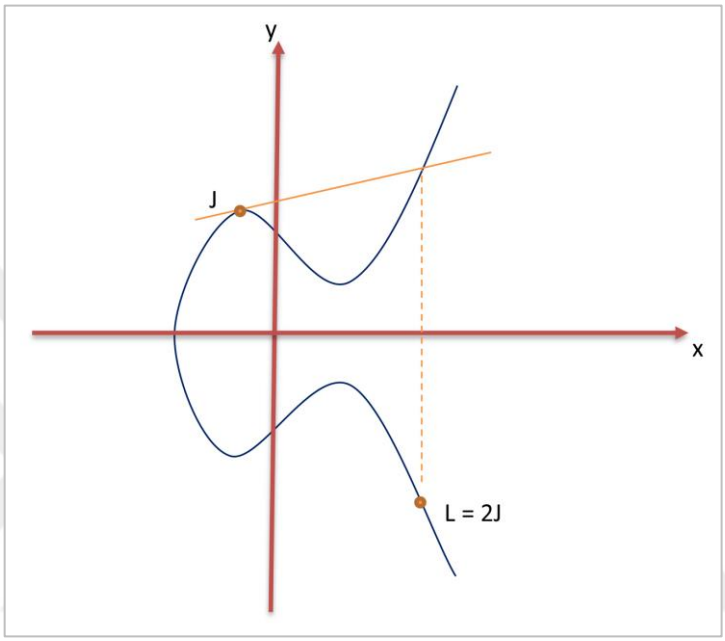

Figure 3.6 An example of point doubling

3.2.1.3 Point Multiplication

Multiplying P, which is a point on the curve, with a scalar k to get the point Q that lies on the same curve, i.e. Q = kP. Actually, point multiplication is a repeated point addition and point doubling operations, for example:

Q = kP. If k = 23 then kP = 23.P = 2(2(2(2P) + P) + P) + P (Caelli, Dawson, & Rea, 1999).

The most time-consuming operation in ECC is point multiplication because it includes multiple point addition and point doubling which in turn involves a multiplicative inverse. Hence finding a multiplicative inverse is a costly operation (Hankerson et al., 2006).

3.2.2 Elliptic Curve Discrete Logarithm Problem (ECDLP)

ECDLP could be defined as follow: Suppose P and Q be two points on an elliptic curve such that Q = kP (i.e. adding P, k times to itself) where k is number of effectively hopping on the. Given P and Q, for a large k, finding k is computationally infeasible. Means, an attacker to break the cryptosystem, he has to find how often it has been hopped on the curve. The number of hops represents the private key, k. So, k is the discrete logarithm of Q to the base P. Herewith, the main operation included in ECC is point multiplication (Hankerson et al., 2006). All ECC Protocols depend on the hardness of the ECDLP.

3.2.3 Elliptic Curve Diffie-Hellman Scheme (ECDH)

ECDLP is very hard one-way function and it is the fundamental principle behind the ECDH key agreement and exchange protocol that let both parties to construct a shared secret key that could be used for symmetric key algorithms. The two parties share some data publicly and by using this public information with their own private info they will calculate the secret key. Any other party, that does not have the private information of communicated party, will not be capable to figure out the secret key. As seen in Figure 3.7, the process flows as: For generating a shared secret using ECDH between communicated parties T and R, both parties publicly will agree on elliptic curve domain parameters. The two parties have a pair of keys, private key P (a randomly selected integer number) and public key Q=PG (G is generator point). Let (P_T, Q_T) are private – public key of T and (P_R, Q_R) are private – public key of R.

- T computes $S_T = P_T Q_R$
- R computes $S_R = P_R Q_T$
- Seeing that $P_T Q_R = P_T P_R G = P_R P_T G = P_R Q_T$.

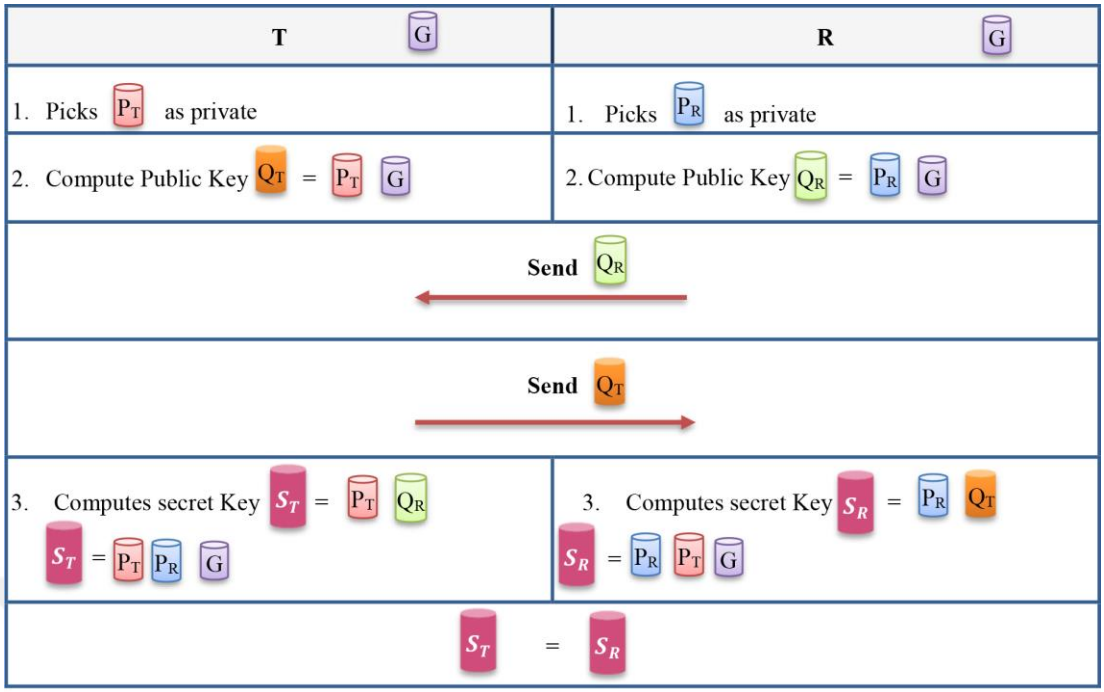

Figure 3.7 Elliptic curve Diffie-Hellman scheme

3.2.4 Elliptic Curve Digital Signature Algorithms (ECDSA)

A digital signature presents identification along with integrity and non-repudiation. Signature algorithms used for authentication purposes. ECDSA is a version of the digital signature algorithm (DSA) which works on elliptic curves. In order to send a signed message from T to R, they have to deal on elliptic curve domain parameters (G, p, a, b, n, h). The sender T have a key pair, a randomly selected integer private key P_T and public key $Q_T = P_T$ G. i.e., to authenticate a message sent by T (Figure 3.8), T signs the message via its private key P_T and sends it and its signature to R. Using the public key of the sender, Q_T, the signature could be verified. Hence, since the R has T's public key, Q_T, it can verify if the message is really send by T or not (Hankerson et al., 2006).

R	T
Both agree on domain parameters p, a, b, G, n and h	Both agree on domain parameters p, a, b, G, n and h
	Signing m: 1. e = Hash(m). 2. Select k randomly 3. r = x_1 mod n, where (x_1, y_1) = kG. If r = 0, go to (2). 4. s = k^{-1}(e + P_T r) mod n. If s = 0, go to (2). 5. Signature pair is (r, s).
Send m, (r, s) ←	
Verifying m: 1. Check whether r and s are integers in the range [1, n−1]. If not, the signature is invalid 2. e = Hash (m), 3. w = s^{-1} mod n. 4. u_1 = ew mod n and u_2 = rw mod n. 5. (x_1, y_1) = u_1G + u_2 Q_T 6. The T is authenticated if x_1 = r mod n; otherwise is invalid.	

Figure 3.8 Elliptic curve digital signature algorithm scheme

- *Signature Generation:* to sign the message m by sender T, using T's private key P_T
    1. Compute e = Hash(m), where the Hash is hash function.
    2. Select randomly an integer k [1, n−1]
    3. Compute r = x_1 mod n, where (x_1, y_1) = kG. If r = 0, go to (2).
    4. Compute s = k^{-1}(e + P_T r) mod n. If s = 0, go to (2).
    5. Signature pair is (r, s).

- *Signature Verification:* To authenticate T's signature, R must have T's public key Q_T
    1. Check whether signature pair is r and s are integers in the range [1, n−1]. If not, the signature is invalid
    2. Compute e = Hash(m), where the Hash is the same hash function used in the signature generation.
    3. Compute w = s^{-1} mod n.
    4. Compute u_1 = ew mod n and u_2 = rw mod n.
    5. Compute (x_1, y_1) = u_1G + u_2 Q_T
    6. The T is authenticated if x_1 = r mod n; otherwise is invalid.

3.3 Wireless Identification and Sensing Platform5 (WISP5)

The WISP is an open source, open architecture EPC C1-G2 UHF RFID tag. It includes a fully programmable 16-bit microcontroller (central processing unit (CPU) MSP430 16Mhz, 64KB Non-volatile memory and 66KB of RAM for more details see (Instruments, 2012)) and construct with light and temperature sensors, and strain gauges (Figure 3.9). WISP is powered by harvested energy from UHF RFID readers. The aggregated energy operates the 16-bit microcontroller that could realize a set of computation and report the sensed data to the RFID reader. WISPs can write to flash and perform cryptographic computations. Unlike traditional tags, WISP can execute computer programs and supports sensors. WISP5 is the last revision of the Wireless Identification and Sensing Platform projects that started in 2006. WISP5 can operate at 8 meters from a reader. The prime feature of WISP5 is being embedded with AES.

Up to now, most of the work done on the WISP involves a single WISP that performs detection or computation functions. The next stage of the WISP studies may involve interactions of many WISPs so that they can discover a new batteryless form of wireless sensor network.

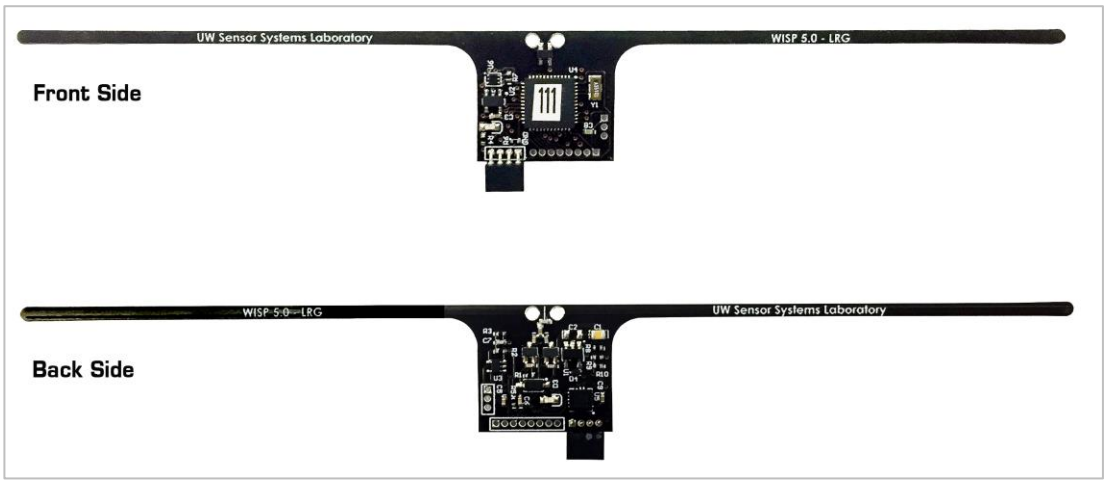

Figure 3.9 Front and back sides of WISP5 (Personal archive, 2017)

3.3.1 Random Number Generator

The REFGEN subsystem of the reference module (REF) of MSP430 consists of bandgap, bandgap bias and noninverting buffer stage. The bandgap voltage is used to generate the three references voltages (1.2 V, 2.0 V, and 2.5 V) that are required for

an analog to digital convertor (ADC) subsystem. Further, the REFGEN subsystem is includes the temperature sensor circuitry that is used by an ADC to measure a voltage proportional to temperature (1).

To enable and use the inbuilt temperature sensor, the user has to enable its input channel (A30) by setting the ADC12TCMAP bit = 1 in the ADC12CTL3 register and selecting the analog input channel ADC12INCHx = 0x1E (11110), (Figure 3.10).

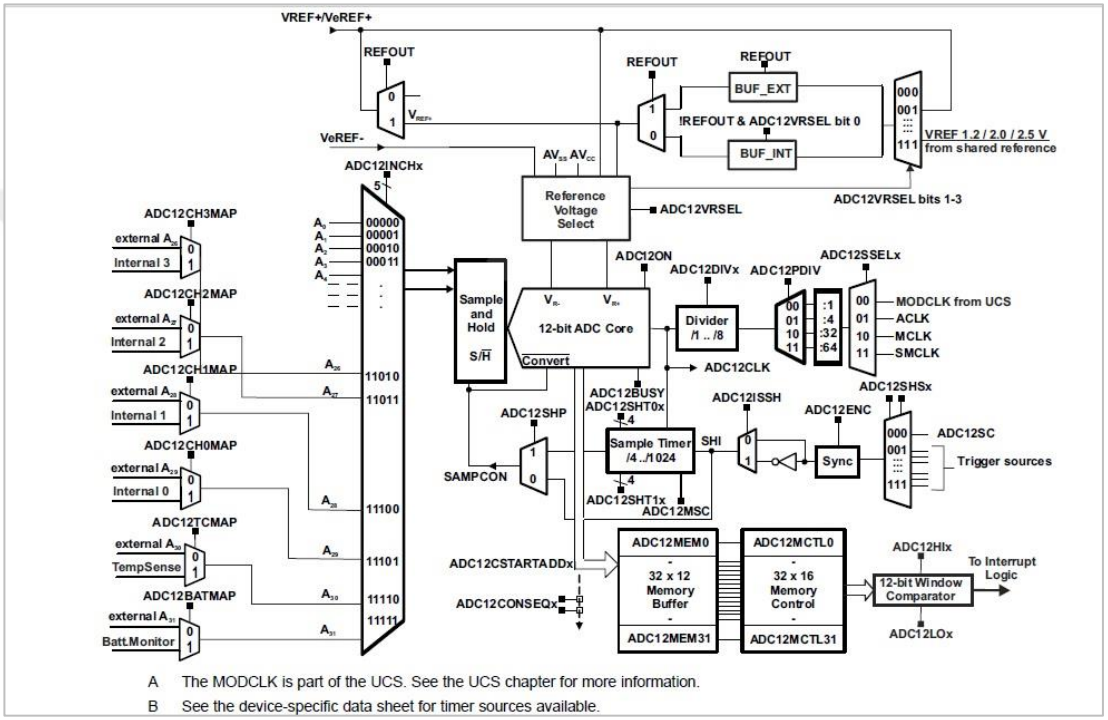

Figure 3.10 ADC12_B Block diagram (Instruments, 2016)

The MSP430 on-chip temperature sensor could be exploit as Random Number Generator. Using 12-bit ADC in repeat-single-sample mode, the 16-bit random number generator could be produced by sampling the least significant bit (LSB) (b0) of the temperature sensor 16 times. In each sampling and holding process, the b0 of ADC12 is kept then shifted left by 1, the next sampled b0 will be assembled from end (to the right of the previous b0). This process will proceed until 16-bit RNG is formed. A code sample for acquiring 16 measurements of ADC12 is given in Appendix 3.

CHAPTER FOUR

AES AND ECC BASED RFID MUTUAL AUTHENTICATION PROTOCOL

In this chapter, based on advanced encryption standard and elliptic curve cryptography, a stable and powerful RFID mutual authentication protocol is proposed coded and tested on WISP5 named "*AES and ECC Based RFID Mutual Authentication Protocol Proven on WISP5 (AERMAP-W5)*". Which not only send the tag ID securely, it could also send the valuable data stored in the tag in an encrypted pattern. Moreover, achieves mutual authentication in just two steps. See Appendix 4 for a Code sample.

AERMAP-W5, after initial RFID system setup, it continues with authentication phase. Authentication phase is introduced in two different methods. First, called reader signing method, in which, only reader signs the message and tag verifies the signature. Second, called reader and tag signing method, in which, both reader and tag sign the message, and both verify the signature of each other.

4.1 Discussion of AERMAP-W5

In this section, AERMAP-W5 will be discussed in detail. This section will be divided into five subsections; Assumptions, Used Tools, Used Notations, Initial RFID System Setup and Authentication Phase. The explanation of each subsection is below:

4.1.1 Assumptions

It has been assumed that the communication channel between the reader and the back-end database server is done through a secure channel, while communication channel between the tags and the readers is not secure. The readers assumed to be fully equipped and connected directly to a power supply.

4.1.2 Used Tools

In the proposed scheme and to use the WISP5 the following tools are used:

- *The WISP5 itself:* WISP5 developed at the laboratories of the University of Washington and is the last member of the WISP device family. It includes a fully programmable 16-bit microcontroller (CPU MSP430 16Mhz, 64KB Non-

volatile memory and 66KB of RAM) and constructed with light and temperature sensors, and strain gauges. The WISP5 tag that used in our study is acquired from Washington University.

- *An Impinj Speedway reader:* WISP5 has not been tested for use with another RFID reader model or with R420 or R1000 versions sold outside the US. Moreover, aligning WISP5 with other readers is not an easy process. However, several workings are proceeding to solve the matter (WISP5, 2015).

- *An MSP-FET430UIF debugging tool:* Not to forget that the low-price debugging tools may not works with the MSP430FR5969 microcontroller used by WISP5. It must be sure to use MSP-FET430UIF and the compatible debugging tool.
- *The WISP5 programming adapter:* This adapter used to connect the 14-pin connector of the MSP-FET430UIF to the 4-pin Spy-Bi-Wire (SBW) programming head of the WISP5.

- *Code Composer Studio:* Not to forget that Code Composer Studio prior to version 6 is not convenient to with the MSP430FR5969 of the WISP5. In AERMAP-W5 it has been used the version 6.1.0.

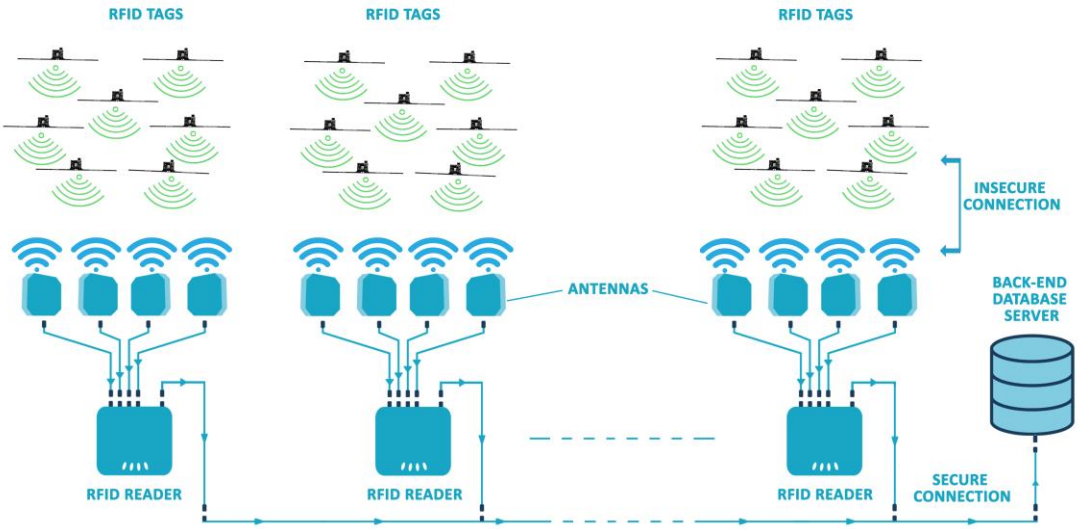

Figure 4.1 AERMAP-W5's modality

4.1.3 Used Notations

In this subsection, we would like to list the used notations in the initial RFID system setup and authentication phase:

- *Domain parameters of prime field* (F_p) *elliptic curve are*:
  - *p:* big prime number defined for finite field F_p
  - *a, b:* defines the elliptic curve $E(F_p)$
  - *G:* generator point
  - *n:* order of G (order of the curve)
  - *h:* cofactor = $\#E(F_p)/n$, $\#E(F_p)$ is no of points on elliptic curve $E(F_p)$

- K_{TR}: The produced secret key by ECDH key exchange that will be used in AES to encrypt/decrypt tag ID (and the sent/received data).

- *t, T:* Private & public keys (at the same time considered as a message during signing *T* in ECDSA) of a tag used in ECDH to produce Secret key K_{TR}

- *t', T':* Private & public keys of the tag used in ECDSA

- *(h, g):* Signature pair of *T* (the tag's public key)

- *r, R:* Private & public key (at the same time considered as a message during signing *R* in ECDSA) of a reader used in ECDH to produce Secret key K_{TR}

- *(z, s):* Signature pair of *R* (the reader's public key)

- *r', R':* Private & public keys of the reader used in ECDSA.

- ID_i: ID of the i^{th} tag

- *k:* a random integer used during *R* (the reader's public key) signing in ECDSA.

- *l:* a random integer used during *T* (the tag's public key) signing in ECDSA.

4.1.4 Initial RFID System Setup

In the initial RFID system setup, the readers and tags agree on the elliptic curve domain parameters p, a, b, G, n, and h. Elliptic curve secp160r1, recommended by the NIST, is used for the domain parameter values (Brown, 2010). After agreeing on the elliptic curve domain parameters, the initial RFID system setup will be completed after these following steps:

1. All tags' identifiers (*IDi*) are stored in the back-end-database server.
2. Each tag selects an integer t' at random as its private key for ECDSA, where $1 \leq t' \leq n-1$ and computes its public key T' that will be used in ECDSA, where $T' = t'G$. Then, the public key T' of the tag is stored in the back-end-database server.
3. Each reader selects an integer r' at random as its private key for ECDSA, where $1 \leq r' \leq n-1$ and computes its public key R' that will be used in ECDSA, where $R' = r'G$. Then, the public key R' of the reader is set on all the tags manually.

4.1.5 **Authentication Phase**

During the authentication phase both symmetric, and asymmetric algorithms have been exploited. The ECDH is used to produce the secret key K_{TR} that will be used to in AES to encrypt the tag ID. The ECDSA is used to maintain message integrity and provide authentication. So, according to the usage of ECDSA, this phase will be discussed in two different methods:

4.1.5.1 Reader Signing Method

In this method, after reader computes its public key (*R*), reader signs *R* and sends it with its signature pair to the tag. Once the tag receives *R* and its signature pair, it verifies the signature and hence authenticates the reader. Then the tag computes it public key (*T*) and produce secret key K_{TR}. Using AES, the tag will encrypt its *ID* and sends the ciphered text and *T* to the reader. Once the reader receives *T*, it will produce the secret key K_{TR} and uses it to decrypt the received ciphered text to get tag's *ID*. Finally, the reader compares the received *ID* with the already stored ID_i. If matches, this means that this is a legitimate tag. Hence, the reader authenticates the tag. Briefly, at the end of this phase, the public keys *R* and *T* are produced, *R* is signed and verified,

and *R* and *T* are exchanged. The secret key K_{TR} is produced and mutual authentication is achieved in only two steps (see Figure 4.2). The details are as follows:

1. The reader picks an integer random number *r* as its private key used in ECDH, where $1 \leq r \leq n-1$, and computes its public key *R* that will be used in ECDH (*R* at the same time considered as a message for ECDSA), where $R = rG$.
2. Before starting ECDH key exchange and sending *R* to the tag, the reader signs *R* using ECDSA as follows:
    a. e = Hash(*R*), where the hashing algorithm is SHA-3 (256).
    b. Select randomly the integer k [$1, n-1$]
    c. Compute $z = x_1 \bmod n$, where $(x_1, y_1) = kG$. If $z = 0$, go to (b).
    d. Compute $s = k^{-1}(e + r'z) \bmod n$. If $s = 0$, go to (b).
    e. Signature pair is (z, s).
3. The reader sends *R* and its signature pair (*z, s*) to the tag.
4. Once the tag receives *R* and its signature (*z, s*), it verifies *R* as follows:
    a. Check whether *z* and *s* are integers in the range [$1, n-1$]. If not, the signature is invalid, and the session is rejected.
    b. e = Hash (*R*), where the hash algorithm is SHA-3 (256).
    c. Compute $w = s^{-1} \bmod n$.
    d. Compute $u_1 = ew \bmod n$ and $u_2 = zw \bmod n$.
    e. Compute $(x_1, y_1) = u_1G + u_2R'$.
    f. The reader is authenticated if $x_1 = z \bmod n$; otherwise, the tag rejects the session.
5. If the reader is authenticated, the tag picks a random integer *t* as its private key used in ECDH, where $1 \leq t \leq n-1$, and computes its public key $T = tG$.
6. The tag computes the secret key $K_{TR} = tR = t(rG) = trG$.
7. The tag encrypts its ID using AES: $C = AES_{K_{TR}}(ID)$.
8. The tag sends its public key *T* and *C* to the reader.
9. Once the reader receives *T* and *C*, it computes the secret key $K_{TR} = rT = r(tG)$
10. To get the tag *ID*, the reader decrypts AES by $ID = AES^{-1}_{K_{TR}}(C)$.
11. The server will compare the *ID* with ID_i from its database. If $ID = ID_i$, the tag is authenticated, otherwise is not and reader rejects the session.

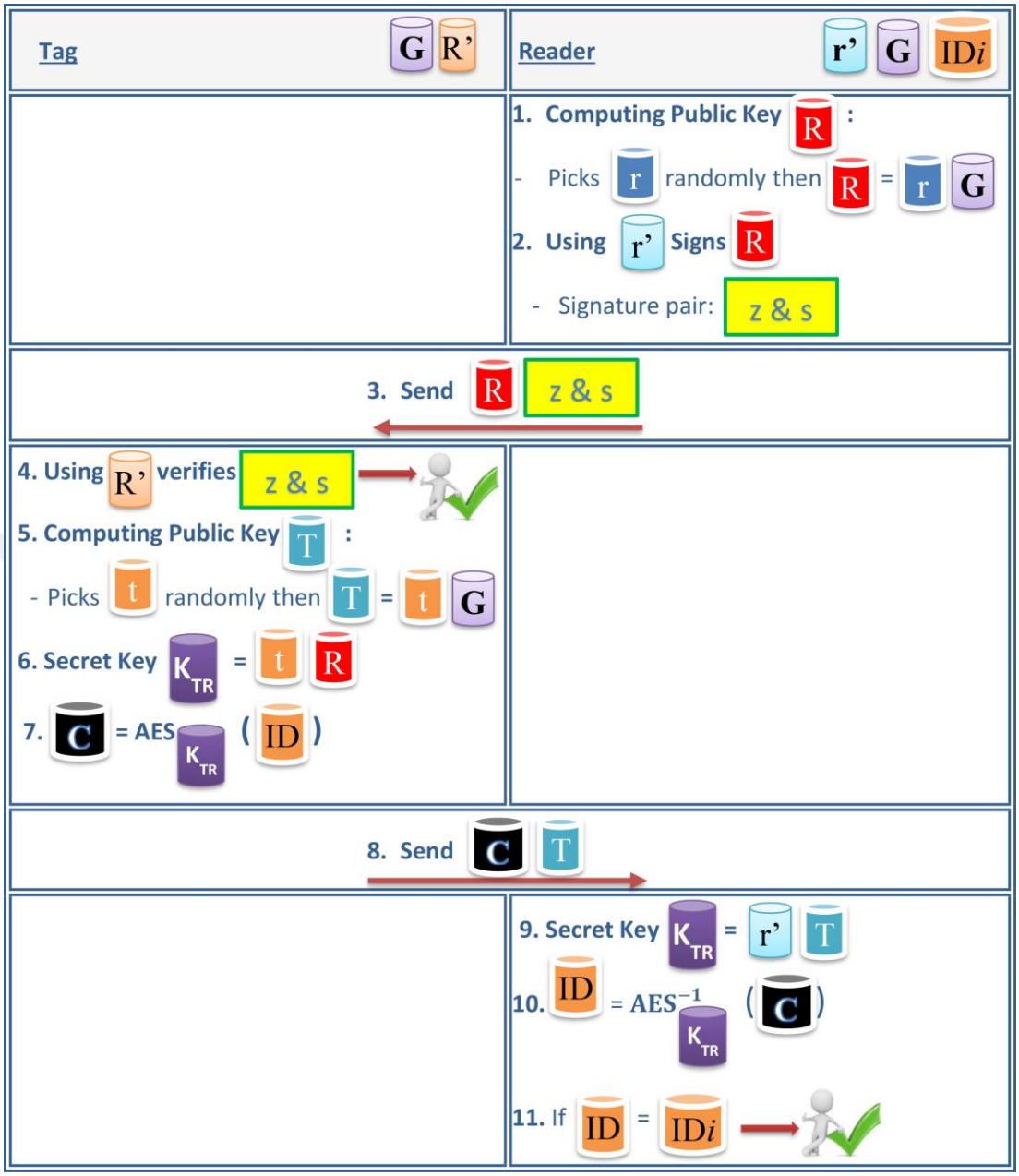

Figure 4.2 AERMAP-W5's scheme (reader signing method)

4.1.5.2 Reader and Tag Signing Method

In this method, after reader computes its public key (*R*), reader sign *R* and send it with its signature pair to the tag. Once the tag receives *R* and its signature pair, it verifies the signature and hence authenticates the reader. Then the tag computes it public key (*T*), Sign *T* and produce secret key K_{TR}. Using AES, the tag will encrypt its *ID* and send *T* and its signature pair, and ciphered text to the reader. Once the reader receives *T* and its signature pair, it verifies the signature and hence authenticates the

tag. Then the reader will produce the secret key K_{TR} and use it to decrypt the received ciphered text to get tag's *ID*. Finally, the reader compares the received *ID* with the already stored ID_i. If matches, this means that this is a legitimate tag. Actually, in this method, the reader authenticates the tag two times; one through verifying tag's signature, and one through comparing the received *ID* with the already stored ID_i. Briefly, at the end of this phase, the public keys *R* and *T* are produced, *R* and *T* are signed and verified, and *R* and *T* are exchanged. The secret key K_{TR} is produced and mutual authentication is achieved in two steps also (see Figure 4.3). The details are as follows:

1. The reader picks an integer random number *r* as its private key used in ECDH, where $1 \leq r \leq n-1$, and computes its public key *R* that will be used in ECDH (*R* at the same time considered as a message for ECDSA), where $R = rG$.
2. Before starting ECDH key exchange and sending *R* to the tag, the reader signs *R* using ECDSA as follows:
    a. e = Hash(*R*), where the hashing algorithm is SHA-3 (256).
    b. Select randomly the integer k $[1, n-1]$
    c. Compute $z = x_1 \bmod n$, where $(x_1, y_1) = kG$. If $z = 0$, go to (b).
    d. Compute $s = k^{-1}(e + r'z) \bmod n$. If $s = 0$, go to (b).
    e. Signature pair is (z, s).
3. The reader sends *R* and its signature pair (*z, s*) to the tag.
4. Once the tag receives *R* and its signature (*z, s*), it verifies *R* as follows:
    a. Check whether *z* and *s* are integers in the range $[1, n-1]$. If not, the signature is invalid, and the session is rejected.
    b. e = Hash(*R*), where the hash algorithm is SHA-3 (256).
    c. Compute $w = s^{-1} \bmod n$.
    d. Compute $u_1 = ew \bmod n$ and $u_2 = zw \bmod n$.
    e. Compute $(x_1, y_1) = u_1G + u_2R'$.
    f. The reader is authenticated if $x_1 = z \bmod n$; otherwise, the tag rejects the session.
5. If the reader is authenticated, the tag picks a random integer *t* as its private key used in ECDH, where $1 \leq t \leq n-1$, and computes its corresponding public key $T = tG$.

6. Before starting ECDH key exchange and sending T to the reader, the tag signs T using ECDSA as follows:
    a. e = Hash(T), where the hashing algorithm is SHA-3 (256).
    b. Select randomly the integer l [1, n−1]
    c. Compute $g = x_2 \bmod n$, where $(x_2, y_2) = lG$. If $g = 0$, go to (b).
    d. Compute $h = l^{-1}(e + t'g) \bmod n$. If $h = 0$, go to (b).
    e. Signature pair is (g, h).
7. The tag computes the secret key $K_{TR} = tR = t(rG) = trG$.
8. The tag encrypts its ID using AES: $C = AES_{K_{TR}}(ID)$.
9. The tag sends its public key T and its signature pair (g, h), and C to the reader.
10. Once the reader receives T and its signature (g, h), it verifies T as follows:
    a. Check whether g and h are integers in the range $[1, n-1]$. If not, the signature is invalid, and the session is rejected.
    b. e = Hash(T), where the hash algorithm is SHA-3 (256).
    c. Compute $i = h^{-1} \bmod n$.
    d. Compute $j_1 = ei \bmod n$ and $j2 = gi \bmod n$.
    e. Compute $(x_2, y_2) = j_1G + j_2T'$.
    f. $x_2 = g \bmod n$; otherwise, the reader rejects the session.
11. The reader computes the secret key $K_{TR} = rT = r(tG) = rtG$.
12. To get the tag ID, the reader decrypts AES by $ID = AES^{-1}_{K_{TR}}(C)$.
13. The server will compare the ID with ID_i from its database. If $x_2 = g \bmod n$ and $ID = ID_i$, the tag is authenticated, otherwise is not and reader rejects the session.

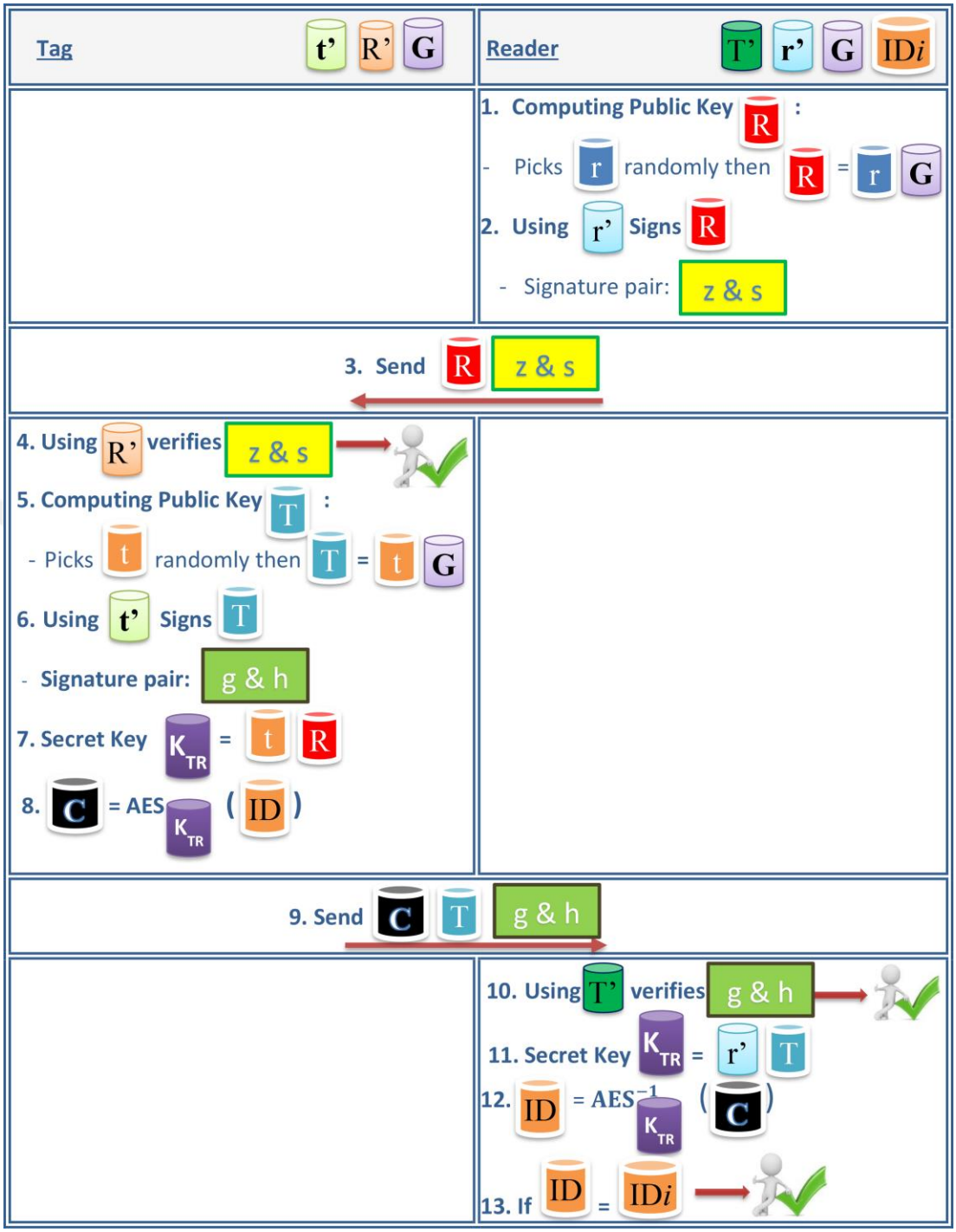

Figure 4.3 AERMAP-W5's scheme (reader and tag signing method)

As shown in Figure 4.3, the mutual authentication has been achieved in only two steps. In this point, we would like to mention, if sensing properties of WISP wanted to be exploited, data related to the sensors' readings can be sent within the tag ID.

CHAPTER FIVE

SECURITY AND PERFORMANCE ANALYSIS OF AERMAP-W5

In this chapter, it will be analyzed the security and performance of AERMAP-W5. As will be shown thereafter, in the following subsection, the security analysis reveals that both authentication methods, that explained in pervious chapter, are carrying out the same security threats and services. Then, a security comparison between AERMAP-W5 and some related ECC-based RFID authentication schemes (hereinafter referred to as "others") are made. In subsection 5.2, the performance analysis reveals that reader signing method is lighter that the other method in terms of RAM usage, communication cost and time response costs. In this point, it is worth to mention that in the both authentication methods, the code size, RAM usage, and response times of AERMAP-W5 is not optimum but considering the used algorithm, indeed, this should be predictable. A performance comparison between AERMAP-W5 and the others is made. Finally, in subsection 5.3 an evaluation of AERMAP-W5 is made.

5.1 Security Analysis and Comparison

In this section, it will be analyzed the security of our proposed protocol in both abovementioned authentication methods and it will be compared with some well-known related ECC-based RFID authentication schemes. As it will be clear hereafter that our proposed protocol in both authentication methods is resistant to the main security concept that includes the following known attacks and services:

- Mutual authentication
- Tracking attack, traceability, location and information privacy
- De-synchronization attack, denial-of-service (DoS) attack, and availability
- Tag anonymity
- Eavesdropping and man-in-the-middle
- Tag impersonation and reader spoofing attacks
- Cloning attacks
- Full disclosure attacks

- Replay attacks
- Confidentiality
- Integrity, modification attack, and unforgeability
- Forward/backward security

5.1.1 Security Analysis of Reader Signing Method

In this subsection, it will be analyzed the foregoing security attacks and services in reader signing method, in which, only reader signs the message, the public key (*R*) and tag verifies the signature.

- *Mutual authentication:* Using the signature pair (*z, s*) and the reader's public key used in ECDSA (*R'*), the tag can verify the signed public key (*R*), herewith, the reader can be authenticated. Since, (1) the unique IDs of all tags are stored formerly in the back-end-database server (2) the tag IDs are sent in an AES encrypted form, (3) each session uses a different secret key K_{TR}, (4) the reader could decrypt AES and gets the ID, (5) the received ID matches the stored ID_i, the reader authenticates the tag. Hence, AERMAP-W5 provides mutual authentication.

- *Tracking attack, traceability, location and information privacy:* Because the ID and confidential information on the tag are encrypted by AES using K_{TR}, an attacker has to break AES or obtain K_{TR} to access the ID or confidential information, which is computationally infeasible. Moreover, K_{TR} is dynamic, meaning that, after each session, a new and different key is produced. Accordingly, the tag cannot be tracked, and the attacker cannot obtain the location and private information stored in the tag. Hence, it cannot be traced.

- *De-synchronization attack, denial-of-service (DoS) attack, and availability*: In the proposed scheme, neither the tag ID nor any critical data that can cause de-synchronization is updated after each execution. Therefore, AERMAP-W5 can withstand de-synchronization attacks, and both the tag and reader remain

synchronized and available to communicate. Thus, DoS attacks can be withstood, and availability is maintained.

- *Tag anonymity*: An adversary who intercepts R, z, s, T, and C between the reader and the tag and attempts to obtain the tag ID cannot get the session key K_{TR}, because this is computationally infeasible under the Diffie–Hellman problem and the elliptic curve discrete logarithm problem (ECDLP). Thence, AERMAP-W5 protects tag anonymity.

- *Eavesdropping and man-in-the-middle*: Even if an adversary eavesdrops messages transmitted between the reader and the tag, the data are useless without the private keys (t and r). When trying to obtain t, r, or any valuable information, the attacker faces the computational Diffie–Hellman problem and ECDLP. Any modification on the messages will be detected, because R is signed by private keys r', and the received ID is compared with the stored IDi. Thus, AERMAP-W5 is resistant to eavesdropping and man-in-the-middle attacks.

- *Tag impersonation and reader spoofing attacks*: To impersonate a tag, an attacker must produce K_{TR} or break AES, which is computationally infeasible under the Diffie–Hellman problem and ECDLP. As, tag ID is encrypted via AES and the received tag ID by reader match with the unique ID of the tag that stored formerly in the back-end-database server, an attacker cannot impersonate the tag. Similarly, attackers cannot spoof the reader, because this would require the signature pair (z, s) and to produce K_{TR}, all of which are unattainable without knowing t and r. Thence, AERMAP-W5 can face tag impersonation and reader spoofing attacks.

- *Cloning attacks:* To clone a tag, attackers must obtain the ID of the tag they wish to clone. Obtaining the tag ID requires the computation of K_{TR}, which is computationally infeasible under the Diffie–Hellman problem and ECDLP, or the breaking of AES. Hence, AERMAP-W5 is resistant to cloning attacks.

- *Full disclosure attacks*: The sent messages R, z, s, T, and C do not disclose any secrets. Hence, even if an adversary could intercept these messages, she would be unable to progress without the random private keys t and r. Furthermore, any attempt to calculate t and r will encounter the computational Diffie–Hellman problem and ECDLP or AES. Thus, the scheme resists full disclosure attacks.

- *Replay attacks:* Intercepting R, z, and s and replaying them to the tag will not produce K_{TR} from the previous session, because the tag chooses a new private key that is used to form the new session key K_{TR}. Similarly, replaying T and C from the previous session will not cause the reader to produce K_{TR} from the previous session. Thus, the scheme resists reply attacks.

- *Confidentiality*: As the tag ID is transmitted as ciphertext, and the K_{TR} changes for every session, an attacker cannot achieve any progress. Thus, unauthorized users cannot obtain the tag ID or other valuable information without computing K_{TR} or breaking of AES.

- *Integrity, modification attack, and unforgeability*: Since ECDSA is used by reader, modifications to the signature pair (z, s) will be detected by the tag and any modifications to T, will produce wrong K_{TR} and accordingly wrong ID. Hence, AERMAP-W5 provides integrity, rejects any modifications, and provides unforgeability.

- *Forward/backward security:* An adversary cannot compromise the previous/current confidential information, because the transferred messages R, z, s, T, and C change after each execution according to the random private keys t and r. Adversaries cannot obtain the tag ID, because it is sent as ciphertext with a different K_{TR} in each session.

5.1.2 Security Analysis of The Reader and Tag Signing Method

In this subsection, the foregoing security attacks and services in the reader and tag signing method has been analyzed, in which, both reader and tag sign the messages *R* and *T* respectively, and both verify the signature of each other.

- *Mutual authentication:* Using the signature pair (*z, s*) and the reader's public key used in ECDSA (*R'*), the tag can verify the signed public key (*R*), herewith, the reader can be authenticated. Tag authentication passes through two stages: stage one, using the signature pair (*g, h*) and the tag's public key used in ECDSA (*T'*), the reader can verify the signed public key (*T*) and hence authenticate the tag; stage two, since, (1) the unique IDs of all tags are stored formerly in the back-end-database server (2) the tag IDs are sent in an AES encrypted form, (3) each session uses a different secret key K_{TR}, (4) the reader could decrypt AES and gets the ID, (5) the received ID matches the stored ID_i, the reader authenticates the tag. Hence, AERMAP-W5 provides mutual authentication.

- *Tracking attack, traceability, location and information privacy:* Because the ID and confidential information on the tag are encrypted by AES using K_{TR}, an attacker has to break AES or obtain K_{TR} to access the ID or confidential information, which is computationally infeasible. Moreover, K_{TR} is dynamic, meaning that, after each session, a new and different key is produced. Accordingly, the tag cannot be tracked, and the attacker cannot obtain the location and private information stored in the tag. Hence, it cannot be traced.

- *De-synchronization attack, denial-of-service (DoS) attack, and availability*: In the proposed scheme, neither the tag ID nor any critical data that can cause de-synchronization is updated after each execution. Therefore, AERMAP-W5 can withstand de-synchronization attacks, and both the tag and reader remain synchronized and available to communicate. Thus, DoS attacks can be withstood, and availability is maintained.

- *Tag anonymity*: An adversary who intercepts R, z, s, T, g, h and C between the reader and the tag and attempts to obtain the tag ID cannot get the session key K_{TR}, because this is computationally infeasible under the Diffie–Hellman problem and the ECDLP. Thus, AERMAP-W5 protects tag anonymity.

- *Eavesdropping and man-in-the-middle*: Even if an adversary eavesdrops messages transmitted between the reader and the tag, the data are useless without the private keys (t and r). When trying to obtain t, r, or any valuable information, the attacker faces the computational Diffie–Hellman problem and ECDLP. Any modification on the messages will be detected, because R and T are signed by private keys r' and t' respectively, and the received ID is compared with the stored IDi. Thus, AERMAP-W5 is resistant to eavesdropping and man-in-the-middle attacks.

- *Tag impersonation and reader spoofing attacks*: To impersonate a tag, an attacker must produce K_{TR} or break AES, which is computationally infeasible under the Diffie–Hellman problem and ECDLP. As, the public key of the tag (T) is signed by the private key t' and verified by the public key T' of the tag, an attacker cannot impersonate the tag. Similarly, attackers cannot spoof the reader, because this would require the signature pair (z, s) and to produce K_{TR}, all of which are unattainable without knowing t and r. Thus, AERMAP-W5 can cope with tag impersonation and reader spoofing attacks.

- *Cloning attacks:* To clone a tag, attackers must obtain the ID of the tag they wish to clone. Obtaining the tag ID requires the computation of K_{TR}, which is computationally infeasible under the Diffie–Hellman problem and ECDLP, or the breaking of AES. Hence, AERMAP-W5 is resistant to cloning attacks.

- *Full disclosure attacks*: The sent messages R, z, s, T, g, h and C do not disclose any secrets. Hence, even if an adversary could intercept these messages, she would be unable to progress without the random private keys t and r. Furthermore, any attempt to calculate t and r will encounter the computational

Diffie–Hellman problem and ECDLP or AES. Thus, the scheme resists full disclosure attacks.

- *Replay attacks:* Intercepting R, z, and s and replaying them to the tag will not produce K_{TR} from the previous session, because the tag chooses a new private key that is used to form the new session key K_{TR}. Similarly, replaying T, g, h and C from the previous session will not cause the reader to produce K_{TR} from the previous session.

- *Confidentiality*: As the tag ID is transmitted as ciphertext, and the K_{TR} changes for every session, an attacker cannot achieve any progress. Thus, unauthorized users cannot obtain the tag ID or other valuable information without computing K_{TR} or breaking of AES.

- *Integrity, modification attack, and unforgeability*: Since ECDSA is used by reader, modifications to the signature pair (z, s) will be detected by the tag and any modifications to T, g and h will fail the verification and cause to produce wrong K_{TR} and accordingly wrong ID. Hence, AERMAP-W5 provides integrity, rejects any modifications, and provides unforgeability.

- *Forward/backward security:* An adversary cannot compromise the previous/current confidential information, because the transferred messages R, z, s, T, g, h and C change after each execution according to the random private keys t and r. Adversaries cannot obtain the tag ID, because it is sent as ciphertext with a different K_{TR} in each session

5.1.3 Security Comparison of Both Authentication Methods

As it is clear from the foregoing two subsection, 5.1.1 and 5.1.2, that both authentication methods fulfill the same security attacks and services. Accordingly, a security comparison of our proposed scheme and other ECC-based schemes are made and the results are shown in Table 5.1. As it is visible from the table, that AERMAP-W5 has additional security features than the related schemes and withstands the

common attacks and satisfies the essential security requirements of RFID-based healthcare systems which make AERMAP-W5 more applicable than other related protocols in the field of healthcare systems.

Table 5.1 Security comparison (√: Provide, X: do not provide and —: not mentioned)

Security Services and attacks	Liao & Hsiao, 2014	Zhao, 2014	Chou, 2014	Zhang & Qi, 2014	AERMAP-W5
Mutual authentication	X	√	X	√	√
Tracking attack	X	—	—	—	√
Traceability	X	—	X	—	√
Location privacy	X	√	X	—	√
Information privacy	X	—	X	√	√
De-synchronization attack	—	—	—	√	√
Denial-of-service (DoS) attack	√	√	√	√	√
Availability	√	√	—	—	√
Tag anonymity	√	X	—	√	√
Eavesdropping	—	—	—	—	√
Man-in-the-middle	—	—	X	√	√
Impersonation attack	X	√	X	√	√
Reader spoofing attack	X	√	—	√	√
Cloning attacks	√	√	—	—	√
Full disclosure attacks	—	—	—	—	√
Replay attacks	√	√	√	√	√
Confidentiality	√	—	—	—	√
Integrity	—	—	—	—	√
Modification attack	—	—	—	√	√
Unforgeability attack	—	—	—	—	√
Forward security	X	X	X	X	√
Backward security	X	X	X	X	√

5.2 Performance Analysis

The performance of the proposed method is analyzed in terms of code size, communication cost, and tag response time (the reader is assumed to be fully equipped). The results are obtained based on the secp160r1 curve. The following first two subsections analyzes the performance of our proposed protocol in both authentication methods. In the third subsection, a performance comparison among AERMAP-W5 and other related ECC-based RFID authentication protocols is made.

5.2.1 Performance Analysis of Reader Signing Method

A total of 28330 (code) and 3147 (data) bytes are written to the tag FLASH/FRAM, and RAM usage is 1537 bytes. The communication cost (Table 5.2) from reader to tag involves transmitting the 320-bit reader public key and 320-bit reader signature (= 640 bits), and the communication cost from tag to reader involves transmitting the 320-bit tag public key and 128-bit encrypted tag ID (= 448 bits). Unlike the proposal in (Jin et al., 2015), which used the pairing-based cryptography library with an embedding degree of 2 on an Intel Pentium(R) Dual-Core processor with 2.69 GHz and 2048 MB of RAM, and the proposal in (He et al., 2014), which assumed a hardware platform of a Pentium-IV 3 GHz processor with 512 MB memory and Windows XP (Cao, Kou, & Du, 2010), our proposed protocol is realized on a passive tag with a 16 MHz MSP430, 64 KB non-volatile memory, and 66 KB RAM. As shown in Table 5.3, computing K_{TR} requires 1.4578926250 s (= 23,326,282 CPU cycles/16 MHz). However, adopting the same system used by Jin et al. (2015), computing K_{TR} would require 0.00867148 s (=23,326,282 CPU cycles/2.69 GHz). Previous ECC-based protocols have been adopted under simulation scenarios, whereas AERMAP-W5 has been realized on a real device.

Table 5.2 Communication cost in reader signing method

Communication	Cost (bit)
Reader - Tag	640 (320-bit reader public key + 320-bit signature)
Tag - Reader	448 (320-bit tag public key + 128-bit encrypted tag ID)
Total	1088

Table 5.3 Response times in reader signing method

Operation	Resp. time (ms) (Real)	Resp. time (CPU cycles) (Real)	Resp. time (ms) (Simulation)
Generating 16-bit RNG	0.1356875	2171	0.0008070
Hashing R	18.5743125	297,189	0.0001104
Verification of R	1805.2265625	28,883,625	10.7374070
Generating t	12.1121250	193,794	0.0720423
Computing T	1470.9932500	23,535,892	8.7494022
Computing K_{TR}	1457.8926250	23,326,282	8.6714802
Encrypting tag ID (AES)	0.0471875	755	0.0002806

5.2.2 Performance Analysis of Reader and Tag Signing Method

A total of 29450 (code) and 3296 (data) bytes are written to the tag FLASH/FRAM, and RAM usage is 1595 bytes. The communication cost (Table 5.4) from reader to tag involves transmitting the 320-bit reader public key and 320-bit reader signature (= 640 bits), and the communication cost from tag to reader involves transmitting the 320-bit tag public key, 320-bit tag signature and 128-bit encrypted tag ID (= 768 bits). In this method, as shown in in Table 5.5, in addition to the response times of the reader signing method, time of signing tag's public key (T) has been added. Hence, the tags response time at all increased.

Table 5.4 Communication cost in reader and tag signing method

Communication	Cost (bit)
Reader - Tag	640 (320-bit reader public key + 320-bit signature)
Tag - Reader	768 (320-bit tag public key + 320-bit signature + 128-bit encrypted tag ID)
Total	1408

Table 5.5 Response times in reader and tag signing method

Operation	Resp. time (ms) (Real device)	Resp. time (CPU cycles) (Real device)	Resp. time (ms) (Simulation)
Generating 16-bit RNG	0.1356875	2171	0.0008070
Hashing R	18.5743125	297,189	0.0001104
Verification of R	1805.2265625	28,883,625	10.7374070
Generating t	12.1121250	193,794	0.0720423
Computing T	1470.9932500	23,535,892	8.7494022
Signing T	1626.8456250	26,029,530	9.6764452
Computing K_{TR}	1457.8926250	23,326,282	8.6714802
Encrypting tag ID (AES)	0.0471875	755	0.0002806

Although the proposed scheme uses the tiny ECC (Liu & Ning, 2008) and has AES embedded in the WISP5 platform, its heaviness is apparent from the results of both methods. However, taking the algorithms used in AERMAP-W5, the results reported by Marin, Jara, & Gomez (2013) indicate that each point addition and point doubling on MSP430 require 22,981.05 and 25,743.13 CPU cycles, respectively. Marin, Jara, & Skarmeta (2011) found that producing a signature tiny ECC requires 19308 bytes ROM and 1510 bytes RAM, generating a signature requires 2 s, and verifying the

signature requires 2.43 s. Considering these facts, our results are reasonable. Indeed, some enhancements have been achieved. In worst case, according to Moore's Law (2017), using the same codes the response times may decrease to half within maximum two years.

5.2.3 Performance Comparison

In this subsection, a performance comparison of both authentication methods is made between AERMAP-W5 and the others.

5.2.3.1 Performance Comparison of Reader Signing Method

Table 5.6 shows the communication cost of AERMAP-W5 and related schemes. As seen from the table, despite of AERMAP-W5 achieves mutual authentication in just two steps, its communication cost is less than the other schemes.

Table 5.6 Performance comparison in reader signing method

Communication Cost	**Liao & Hsiao, 2014**	**Zhao, 2014**	**Chou, 2014**	**Zhang & Qi, 2014**	**AERMAP-W5**
# of Steps	3	3	3	3	2
Bytes	168	168	184	160	136

5.2.3.2 Security and Performance of The Reader and Tag Signing Method

Table 5.7 shows the communication cost of our proposed and related schemes. As seen from the table, although AERMAP-W5 achieves mutual authentication in just two steps, its communication cost is less than study (Chou, 2014) and very close to the other compared schemes.

Table 5.7 Performance comparison in reader and tag signing method

Communication Cost	**Liao & Hsiao, 2014**	**Zhao, 2014**	**Chou, 2014**	**Zhang & Qi, 2014**	**AERMAP-W5**
# of Steps	3	3	3	3	2
Bytes	168	168	184	160	176

5.3 Evaluation

Actually, planning and proposing a new protocol is a difficult subject, where, various alternative has been composed till a final version is defined. Nevertheless, AERMAP-W5 is achieved in two different alternatives; first, only reader signs the message and tag verifies and second, both reader and tag are sign messages and both verify the message of each other. After the design is completed, a deep security analysis has to be achieved. In our status, AERMAP-W5, in its both authentication methods, is analyzed and showed its strength to the main security concept that includes the following known attacks and services:

- Mutual authentication
- Tracking attack, traceability, location and information privacy
- De-synchronization attack, denial-of-service (DoS) attack, and availability
- Tag anonymity
- Eavesdropping and man-in-the-middle
- Tag impersonation and reader spoofing attacks
- Cloning attacks
- Full disclosure attacks
- Replay attacks
- Confidentiality
- Integrity, modification attack, and unforgeability
- Forward/backward security

Once the security analysis is accomplished, the performance of AERMAP-W5 is coded, tested on real devices and found acceptable. This was the most significant achievement because the acceptability of the protocol would be depending on the performance results. Finally, AERMAP-W5 is compared with the most well-known protocols from our literature review. In terms of security, AERMAP-W5 proved that it has additional security features than the related schemes and withstands the common attacks and satisfies the essential security requirements of RFID-based healthcare systems.

In term of performance, communication overhead of AERMAP-W5's reader signing authentication method is less than the other schemes. However, the communication overhead of AERMAP-W5's reader and tag signing authentication method is less than study of Chou (2014) and very close to the other compared schemes. In term of time response, code size and RAM usage, it is not optimal but taking into account the MSP430 and the used algorithms, actually, this is to be anticipated. After all, worth mentioning that AERMAP-W5 achieves mutual authentication in just two steps. In this point, it is worth mentioning that a list of abbreviations is given in Appendix 5.

CHAPTER SIX

CONCLUSION

RFID technology is one of the most up-and-coming progresses in pervasive infrastructures that permit the untouched identification of tagged objects and people. For being readable in adverse conditions, RFID tags could be a well replacement of optical barcodes and attractive for considerable tracking and tagging scenarios. As the reader communicate with the tag in a wireless manner, RFID technology faces a considerable security and privacy threats. The contrast of RFID technology to be popular but insecure has led to an influx of mutual authentication protocols. Because authentication protocols are first step in prevention wireless attacks and adds confidence to the identification process. According to the computations and operations supported by tag, authentication protocols are divided into four classes. Vast majority of the mutual authentication protocol proposed has not pointed out for which class the protocol is belong to. Moreover, many proposals claimed to be convenient for low-cost RFID tags but actually they are not literal about tag hardware restrictions, which is very critical points and security level will vary accordingly.

In Chapter Two, we made a class based comprehensive survey. The most recent and worthy RFID mutual authentication protocols are reviewed and compared minutely. The key points of comparison collected in Table 2.1 and Table 2.2. From Table 2.1, it could be concluded that each examined protocol adopted different method to cope with attacks and ensure security and privacy. Moreover, various verification tools are used to verify the proposal. Owing to the severe hardware construction fact of low-cost RFID, utmost of the surveyed protocols take place under fully fledged class and slight of them take place under fully fledged class. From Table 2.2, it could be deduced that each examined protocol has a certain talent to face security and privacy issues. From the comparison as all, it could be concluded that the less hardware restriction of a tag, the less goal realized by authentication protocol and there is a necessity for more and stronger ultra-lightweight mutual authentication protocol.

Information in patients' medical histories is exposed to varied security and privacy concerns. whereas, any alteration in patient's medical data may lead to severe and even

mortal harm. To prevent such alteration, RFID systems have been vastly applied in healthcare systems in many hospitals. However, because of the open and unsecure wireless communication environments, the security and privacy become major concerns of using RFID systems in healthcare environments. Especially, after FDA's declaration and becoming the protocols conforming to EPC C1-G2 standard inadequate for RFID-based healthcare systems, in Chapter Four, we proposed a stable and powerful RFID mutual authentication protocol named AERMAP-W5. In which, both symmetric and asymmetric algorithms have been exploited, AES and ECC.

Unlike the existing schemes, firstly, AERMAP-W5 did not simulated it is coded, tested and proven on real devices, WISP5. Secondly, in addition to send tag ID in a secured manner, AERMAP-W5 can send valued sensed data also. Thirdly, AERMAP-W5 realize mutual authentication in only 2 steps. After initial RFID system setup, AERMAP-W5 continues with authentication phase. Authentication phase, achieved in two different methods. As foregoing in Chapter Five, although, both methods fulfil the same security threats and services, the reader and tag signing method is relatively heavier than reader signing method in terms of RAM usage and timing cost. The analysis results of AERMAP-W5 show that it can overcomes almost all common attacks and meets the essential security demands of RFID-based healthcare systems. In terms of performance, in both methods, when taking a glance at the code size, RAM usage, and response times of AERMAP-W5, clearly, it will be found not optimal. However, taking into account using MSP430 with SHA3, ECDH, and ECDSA algorithms, actually, this is to be anticipated.

As a future work, firstly, as it is well-known, ECC includes numerous time-consuming point multiplications. Reducing the time-consuming of point multiplications using some methods that increase the efficiency, reducing the code size and decreasing the response times could be considered as a future work.

Secondly, worth to mention, that most works on WISP have included only a single unit. Using the sensing features of WISP5 with multiple WISPs will open a gate of a batteryless form of wireless sensor networks in the field of healthcare systems. So, using multiple WISPs with sensing feature could be considered as a future work also.

REFERENCES

Alavi, S. M., Baghery, K., & Abdolmaleki, B. (2014). Security and privacy flaws in a recent authentication protocol for EPC C1 G2 RFID tags. *Advances in Computer Science: an International Journal (ACSIJ), 3*(5), 44-52.

Alomair, B., Clark, A., Cuellar, J., & Poovendran, R. (2012). Scalable RFID systems: a privacy-preserving protocol with constant-time identification. *IEEE Transactions on Parallel and Distributed Systems*, *23*(8), 1536-1550.

Asadpour, M., & Dashti, M. T. (2011). A privacy-friendly RFID protocol using reusable anonymous tickets. In *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),* 206-213. IEEE.

Avoine, G., & Oechslin, P. (2005). A scalable and provably secure hash-based RFID protocol. In *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops,*110-114. IEEE.

Avoine, G., Coisel, I., & Martin, T. (2010). Time measurement threatens privacy-friendly RFID authentication protocols. In *International Workshop on Radio Frequency Identification: Security and Privacy Issues,*138-157. Springer Berlin Heidelberg.

Bassil, R., El-Beaino, W., Itani, W., Kayssi, A., & Chehab, A. (2012). PUMAP: A PUF-based ultra-lightweight mutual authentication RFID protocol. *International Journal of RFID Security and Cryptography, 1*(1/2), 58-66.

Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., & Verbauwhede, I. (2007). Public-key cryptography for RFID-tags. In *Pervasive Computing and Communications Workshops, 2007. Fifth Annual IEEE International Conference on PerCom Workshops' 07.,* 217-222. IEEE.

Blake, I. F., Seroussi, G., & Smart, N. P. (Eds.). (2005). *Advances in elliptic curve cryptography* (Vol. 317). Cambridge University Press.

Bonuccelli, M. A., Lonetti, F., & Martelli, F. (2007). Instant collision resolution for tag identification in RFID networks. *Ad Hoc Networks*, *5*(8), 1220-1232.

Bringer, J., Chabanne, H., & Dottax, E. (2006). HB^{++}: a Lightweight Authentication Protocol Secure against Some Attacks. In *Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006. Second International Workshop on SecPerU 2006*. 28-33. IEEE.

Bringer, J., Chabanne, H., & Icart, T. (2008). Cryptanalysis of EC-RAC, a RFID identification protocol. In *International Conference on Cryptology and Network Security*, 149-161. Springer, Berlin, Heidelberg.

Brown, D. R. (2010). Sec 2: Recommended elliptic curve domain parameters. *Standars for Efficient Cryptography*.

Brusó, M., Chatzikokolakis, K., & Den Hartog, J. (2010). Formal verification of privacy for RFID systems. In *23rd IEEE Computer Security Foundations Symposium*, 75-88. IEEE.

Burmester, M., & Munilla, J. (2011). Lightweight RFID authentication with forward and backward security. *ACM Transactions on Information and System Security (TISSEC)*, *14*(1), 11 – 16.

Caelli, W. J., Dawson, E. P., & Rea, S. A. (1999). PKI, elliptic curve cryptography, and digital signatures. *Computers & Security*, *18*(1), 47-66.

Calypso Secure (2014). Retrieved March 09, 2017, from https://www.calypsonet asso.org/secure.

Cao, X., Kou, W., & Du, X. (2010). A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. *Information Sciences*, *180*(15), 2895-2903.

Changqing, O., Jixiong, W., Zhengyan, L., & Shengye, H. (2008). An enhanced security authentication protocol based on hash-lock for low-cost RFID. In *Anti-*

counterfeiting, Security and Identification, 2008. 2nd International Conference on ASID 2008, 416-419. IEEE.

Chatmon, C., van Le, T., & Burmester, M. (2006). Secure anonymous RFID authentication protocols. *Florida State University, Department of Computer Science, Tech. Rep*.

Chen, C. L., & Deng, Y. Y. (2009). Conformation of EPC Class 1 Generation 2 standards RFID system with mutual authentication and privacy protection. *Engineering Applications of Artificial Intelligence*, *22*(8), 1284-1291.

Chen, Y. Y., Huang, D. C., Tsai, M. L., & Jan, J. K. (2012). A design of tamper resistant prescription RFID access control system. *Journal of Medical Systems*, *36*(5), 2795-2801.

Chien, H. Y. (2007). Sasi: A new ultralightweight rfid authentication protocol providing strong authentication and strong integrity. *IEEE transactions on dependable and secure computing*, *4*(4), 337-340.

Chien, H. Y., & Chen, C. H. (2007). Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. *Computer Standards & Interfaces*, *29*(2), 254-259.

Chien, H. Y., Yang, C. C., Wu, T. C., & Lee, C. F. (2011). Two RFID-based solutions to enhance inpatient medication safety. *Journal of Medical Systems*, *35*(3), 369-375.

Cho, J. S., Jeong, Y. S., & Park, S. O. (2012). Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol. *Computers & Mathematics with Applications*, 1 -8.

Cho, J. S., Yeo, S. S., & Kim, S. K. (2011). Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. *Computer communications*, *34*(3), 391-397.

Choi, E. Y., Lee, S. M., & Lee, D. H. (2005). Efficient RFID authentication protocol for ubiquitous computing environment. *In Embedded and Ubiquitous Computing–EUC 2005 Workshops*, 945-954. Springer Berlin Heidelberg.

Chou, J. S. (2014). A secure RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. *J. Supercomput*.

Chou, J. S. (2014). An efficient mutual authentication RFID scheme based on elliptic curve cryptography. *The Journal of Supercomputing*, *70*(1), 75-94.

DALKILIÇ, G., ÖZCANHAN, M. H., & ÇAKIR, H. Ş. (2014). Increasing key space at little extra cost in RFID authentications. *Turkish Journal of Electrical Engineering & Computer Sciences*, *22*(1), 155-165.

Deng, G., Li, H., Zhang, Y., & Wang, J. (2013). Tree-LSHB+: An LPN-based lightweight mutual authentication RFID protocol. *Wireless Personal Communications*, *72*(1), 159-174.

Dimitriou, T. (2005). A lightweight RFID protocol to protect against traceability and cloning attacks. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, 59-66. IEEE.

Dimitriou, T. (2006). A secure and efficient RFID protocol that could make big brother (partially) obsolete. In *Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, 6-pp. IEEE.

Duc, D., Park J., & Lee, H. (2006). Enhancing security of EPCglobal gen-2 RFID tag against traceability and cloning. In *2006 Symposium on Cryptography and Information Security*, 17 – 20.

EPCglobal, (2015). EPC radio frequency identity protocols Class-1 Generation-2 UHF RFID protocol for communications at 860–960 MHz, Technical report, Version 2.0.1, *Retrieved September, 03, 2017*, from https://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf.

Fan, K., Li, J., Li, H., Liang, X., Shen, X. S., & Yang, Y. (2014). RSEL: revocable secure efficient lightweight RFID authentication scheme. *Concurrency and Computation: Practice and Experience*, *26*(5), 1084-1096.

Farash, M. S., Nawaz, O., Mahmood, K., Chaudhry, S. A., & Khan, M. K. (2016). A provably secure RFID authentication protocol based on elliptic curve for healthcare environments. *Journal of medical systems*, *40*(7), 165.

Feldhofer, M., Dominikus, S., & Wolkerstorfer, J. (2004). Strong authentication for RFID systems using the AES algorithm. In *International Workshop on Cryptographic Hardware and Embedded Systems*, 357-370. Springer, Berlin, Heidelberg.

Figueiredo, R., Zúquete, A., & e Silva, T. O. (2014). Massively parallel identification of privacy-preserving vehicle RFID tags. *In International Workshop on Radio Frequency Identification: Security and Privacy Issues*, 36-53. Springer International Publishing.

Gao, L., Ma, M., Shu, Y., & Wei, Y. (2014). An ultralightweight RFID authentication protocol with CRC and permutation. *Journal of Network and Computer Applications*, 41, 37-46.

Gao, X., Xiang, Z., Wang, H., Shen, J., Huang, J., & Song, S. (2004). An approach to security and privacy of RFID system for supply chain. In *IEEE International Conference on E-Commerce Technology for Dynamic E-Business*, 164-168. IEEE.

Gilbert, H., Robshaw, M. J., & Seurin, Y. (2008a). Good variants of HB+ are hard to find. *In Financial Cryptography and Data Security*, 156-170. Springer Berlin Heidelberg.

Gilbert, H., Robshaw, M. J., & Seurin, Y. (2008b).: HB#: Increasing the Security and Efficiency of HB+. In *Advances in Cryptology–EUROCRYPT 2008*, 361-378. Springer Berlin Heidelberg.

Gilbert, H., Robshaw, M., & Sibert, H. (2005). Active attack against HB+: a provably secure lightweight authentication protocol. *Electronics Letters*, 41(21), 1169-1170.

Ha, J. C., Ha, J. H., Moon, S. J., & Boyd, C. (2006). LRMAP: Lightweight and resynchronous mutual authentication protocol for RFID system. In *International Conference on Ubiquitous Convergence Technology ,4412,* 80–89. Springer.

Ha, J., Moon, S., Nieto, J. M. G., & Boyd, C. (2007). Low-cost and strong-security RFID authentication protocol. In *International Conference on Embedded and Ubiquitous Computing,* 795-807. Springer, Berlin, Heidelberg.

Habibi, M. H., Alagheband, M. R., & Aref, M. R. (2011). Attacks on a lightweight mutual authentication protocol under EPC C-1 G-2 standard. In *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication,* 254-263. Springer Berlin Heidelberg.

Habibi, M. H., Gardeshi, M., & Alaghband, M. R. (2011). Practical attacks on a RFID authentication protocol conforming to EPC C-1 G-2 standard. *arXiv preprint arXiv:1102.0763*.

Hakeem, M. J., Raahemifar, K., & Khan, G. N. (2013). HPAP: A novel authentication scheme for RFID systems. In *2013 26th Annual IEEE Canadian Conference on Electrical and Computer Engineering (CCECE),* 1-6. IEEE.

Halevi, T., Saxena, N., & Halevi, S. (2011). Tree-based HB protocols for privacy-preserving authentication of RFID tags. *Journal of Computer Security*, *19*(2), 343-363.

Han, S., Potdar, V., & Chang, E. (2007). Mutual authentication protocol for RFID tags based on synchronized secret information with monitor. In *International Conference on Computational Science and its Applications,* 227-238. Springer, Berlin, Heidelberg.

HanataniI, Y., Ohkubo, M., Matsuo, S. I., Sakiyama, K., & Ohta, K. (2012). A study on computational formal verification for practical cryptographic protocol: the

case of synchronous RFID authentication. In *Financial Cryptography and Data Security*, 70-87. Springer Berlin Heidelberg.

Hankerson, D., Menezes, A. J., & Vanstone, S. (2006). *Guide to elliptic curve cryptography*. Springer Science & Business Media.

Hankerson, D., Vanstone, S., & Menezes, A. (2004). Elliptic Curve Arithmetic. *Guide to Elliptic Curve Cryptography*, 75-152.

He, D., Kumar, N., Chilamkurti, N., & Lee, J. H. (2014). Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. *Journal of Medical Systems*, *38*(10), 116.

He, L., Jin, S. H., Zhang, T., & Li, N. N. (2009). An enhanced 2-pass optimistic anonymous RFID authentication protocol with forward security. In *5th International Conference on Wireless Communications, Networking and Mobile Computing*, 1-4. IEEE.

Henrici, D., & Muller, P. (2004). Hash-based enhancement of location privacy for radio frequency identification devices using varying identifiers. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*,149-153. IEEE.

Henrici, D., & Müller, P. (2008). Providing security and privacy in RFID systems using triggered hash chains. In *Proceedings of the Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, 50-59. IEEE.

Hernandez-Castro, J. C., Tapiador, J. M., Peris-Lopez, P., & Quisquater, J. J. (2009). Cryptanalysis of the SASI ultralightweight RFID authentication protocol with modular rotations. *International Workshop on Coding and Cryptography*.

Hopper, N. J., & Blum, M. (2001). Secure human identification protocols. *In Advances in cryptology—ASIACRYPT 2001*, 52-66. Springer Berlin Heidelberg.

Huang, Y. C., & Jiang, J. R. (2012). An ultralightweight mutual authentication protocol for EPC C1G2 RFID tags. In *2012 Fifth International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, 133-140. IEEE.

Hung, Y. K. (2007). The study of adopting RFID technology in medical institute with the perspectives of cost benefit. In *International Medical Informatics Symposium in Taiwan, Taiwan*.

Hwang, R. J., Su, F. F., & Tsai, Y. C. (2010). Efficient electronic toll collection protocol for intelligent transport system. *Journal of Computer Science, 21*(3), 18-26.

Ibrahim, A., & Dalkılıc, G. (2017a). Review of different classes of RFID authentication protocols. *Wireless Networks*, 1-14.

Ibrahim, A., & Dalkılıç, G. (2017b). An advanced encryption standard powered mutual authentication protocol based on elliptic curve cryptography for RFID, proven on WISP. *Journal of Sensors, 2017* (2017), 1-10.

Instruments, T. (2012). MSP430FR59xx Mixed Signal Microcontroller Datasheet.

Instruments, T. (2016). MSP430FR58xx, MSP430FR59xx, MSP430FR68xx, and MSP430FR69xx Family User's Guide.(May 2016). *Retrieved May, 29*, 2016.

Jeon, I. S., & Yoon, E. J. (2013a). Cryptanalysis and improvement of a new ultralightweight rfid authentication protocol with permutation. *Applied Mathematical Sciences, 7*, 3433 – 3444.

Jeon, I. S., & Yoon, E. J. (2013b). A new ultralightweight RFID authentication protocol using merge and separation operations. *International Journal of Mathematical Analysis, 7*(52), 2583-2593.

Jin, C., Xu, C., Zhang, X., & Zhao, J. (2015). A secure RFID mutual authentication protocol for healthcare environments using elliptic curve cryptography. *Journal of medical systems, 39*(3), 24.

Juels, A. (2005). Strengthening EPC tags against cloning. In *Proceedings of the 4th ACM workshop on Wireless security*, 67-76. ACM.

Juels, A., & Weis, S. A. (2005). Authenticating pervasive devices with human protocols. *In Advances in Cryptology–CRYPTO 2005*, 293-308. Springer Berlin Heidelberg.

Kaps, J. P. (2008). Chaitea, cryptographic hardware implementations of xtea. I*n Progress in Cryptology-INDOCRYPT 2008*, 363-375. Springer Berlin Heidelberg.

Kardas, S., Levi, A., & Murat, E. (2011). Providing resistance against server information leakage in RFID systems. In *New Technologies, 4th IFIP International Conference on Mobility and Security (NTMS), 2011*, 1-7. IEEE.

Kardaş, S., Celik, S., Arslan, A., & Levi, A. (2013). An efficient and private RFID authentication protocol supporting ownership transfer. In *International Workshop on Lightweight Cryptography for Security and Privacy*, 130-141. Springer, Berlin, Heidelberg.

Kardaş, S., Çelik, S., Bingöl, M. A., Kiraz, M. S., Demirci, H., & Levi, A. (2015). K-strong privacy for radio frequency identification authentication protocols based on physically unclonable functions. *Wireless Communications and Mobile Computing*, *15*(18), 2150-2166.

Karmakar, N. C. (Ed.). (2011). *Handbook of smart antennas for RFID systems*. John Wiley & Sons.

Karthikeyan, S., & Nesterenko, M. (2005). RFID security without extensive cryptography. In *Proceedings of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks*, 63-67. ACM

Katz, J. E., & Rice, R. E. (2009). Public views of mobile medical devices and services: A US national survey of consumer sentiments towards RFID healthcare technology. *International journal of medical informatics*, *78*(2), 104-114.

Kim, H. (2012). Enhanced hash-based RFID mutual authentication protocol. In *Computer Applications for Security, Control and System Engineering*, 70-77. Springer Berlin Heidelberg.

Kim, H. (2013). RFID mutual authentication protocol based on synchronized secret. *International Journal of Security and Its Applications*, *7*(4), 37-50.

Kim, H. S., Oh, J. H., Kim, J. B., Jeong, Y. O., & Choi, J. Y. (2008). Formal verification of cryptographic protocol for secure RFID system. In *Fourth International Conference on Networked Computing and Advanced Information Management, 2*, 470-477. IEEE.

Kumar, V. N., & Srinivasan, B. (2012). Evolution of electronic passport scheme using cryptographic protocol along with biometrics authentication system. *International Journal of Computer Network and Information Security*, *4*(2), 50.

Lee, Y. K., Batina, L., & Verbauwhede, I. (2008). EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol. In *2008 IEEE International Conference on RFID, ,* 97-104. IEEE.

Lee, Y. K., Batina, L., & Verbauwhede, I. (2009). Untraceable RFID authentication protocols: Revision of EC-RAC. *IEEE International Conference on RFID, 2009,* 178-185. IEEE.

Lee, Y. K., Batina, L., Singelee, D., Preneel, B., & Verbauwhede, I. (2010). Anti-counterfeiting, untraceability and other security challenges for RFID systems: Public-key-based protocols and hardware. In *Towards Hardware-Intrinsic Security*, 237-257. Springer, Berlin, Heidelberg.

Leng, X., Mayes, K., & Markantonakis, K. (2008). HB-MP+ protocol: An improvement on the HB-MP protocol. In *2008 IEEE International Conference on RFID,* 118-124. IEEE.

Leu, J. G. (2010). The benefit analysis of RFID use in the health management center—The experience in Shin Kong Wu Ho-Su Memorial Hospital. *National Taiwan University*.

Li, J., Zhou, Z., & Wang, P. (2017). Cryptanalysis of the LMAP protocol: A low-cost RFID authentication protocol. In *29th Chinese Control and Decision Conference (CCDC)*, 7292-7297. IEEE.

Li, T., & Deng, R. (2007). Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol. In *Availability, Reliability and Security, The Second International Conference on ARES 2007*, 238-245. IEEE.

Li, T., & Wang, G. (2007). Security analysis of two ultra-lightweight RFID authentication protocols. In *IFIP International Information Security Conference*, 109-120. Springer, Boston, MA.

Li, Y., & Ding, X. (2007). Protecting RFID communications in supply chains. In *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, 234-241. ACM.

Liao, Y. P., & Hsiao, C. M. (2014). A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. *Ad Hoc Networks*, *18*, 133-146.

Lin, Z., & Song, J. S. (2013). An improvement in HB-family lightweight authentication protocols for practical use of RFID system. *Journal of Advances in Computer Networks*, *1*(1), 61-65.

Liu, A., & Ning, P. (2008). TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In *Proceedings of the 7th international conference on Information processing in sensor networks*, 245-256. IEEE Computer Society.

Liu, Y. (2008). An efficient RFID authentication protocol for low-cost tags. In *Embedded and Ubiquitous Computing, 2008. IEEE/IFIP International Conference on EUC'08, 2*, 180-185. IEEE.

Lo, N. W., & Yeh, K. H. (2007). An efficient mutual authentication scheme for EPCglobal class-1 generation-2 RFID system. In *Emerging Directions in Embedded and Ubiquitous Computing*, 43-56. Springer Berlin Heidelberg.

Luo, H., Wen, G., Su, J., & Huang, Z. (2016). SLAP: Succinct and lightweight authentication protocol for low-cost RFID system. *Wireless Networks*, 1-10.

Maarof, A., Labbi, Z., Senhadji, M., & Belkasmi, M. (2016). A novel mutual authentication scheme for low-cost RFID systems. In *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 240-245. IEEE.

Marin, L., Jara, A. J., & Skarmeta, A. F. (2011). Shifting primes: extension of pseudo-mersenne primes to optimize ECC for MSP430-based future internet of things devices. In *International Conference on Availability, Reliability, and Security*, 205-219. Springer, Berlin, Heidelberg.

Marin, L., Jara, A., & Gomez, A. S. (2013). Shifting primes: Optimizing elliptic curve cryptography for 16-bit devices without hardware multiplier. *Mathematical and Computer Modelling*, *58*(5-6), 1155-1174.

Ministry of Science and Technology of PRC (2006). Fifteen Ministries and Commissions White Paper on RFID Technology Policy in China.

Mohammadi, M., Hosseinzadeh, M., & Esmaeildoust, M. (2014). Analysis and improvement of the lightweight mutual authentication protocol under EPC C-1 G-2 standard. *Advances in Computer Science: an International Journal*, *3*(2), 10-16.

Molnar, D., & Wagner, D. (2004). Privacy and security in library RFID: Issues, practices, and architectures. In *Proceedings of the 11th ACM conference on Computer and Communications Security*, 210-219. ACM.

Molnar, D., Soppera, A., & Wagner, D. (2005). A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In *International Workshop on Selected Areas in Cryptography*, 276-290. Springer Berlin Heidelberg.

Moore's Law (2017). Retrieved January 27, 2017, from http://www.mooreslaw.org/.

Moosavi, S. R., Nigussie, E., Virtanen, S., & Isoaho, J. (2014). An elliptic curve-based mutual authentication scheme for RFID implant systems. *Procedia Computer Science*, *32*, 198-206.

Mujahid, U., Najam-ul-Islam, M., & Shami, M. A. (2015). RCIA: a new ultralightweight rfid authentication protocol using recursive hash. *International Journal of Distributed Sensor Networks*, *11*(1), Article ID 642180.

Munilla, J., & Peinado, A. (2007). HB-MP: A further step in the HB-family of lightweight authentication protocols. *Computer Networks*, *51*(9), 2262-2267.

Nair, L. S., Arun, V. S., & Joseph, S. (2015). Secure e-ticketing system based on mutual authentication using RFID. In *Proceedings of the Third International Symposium on Women in Computing and Informatics*, 673-677. ACM.

Najera, P., Lopez, J., & Roman, R. (2011). Real-time location and inpatient care systems based on passive RFID. *Journal of Network and Computer Applications*, *34*(3), 980-989.

Ning, H., Liu, H., Mao, J., & Zhang, Y. (2011). Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems. *IET Communications*, *5*(12), 1755-1768.

Ohkubo, M., Suzuki, K., & Kinoshita, S. (2003). Cryptographic approach to "privacy-friendly" tags. In *RFID privacy workshop* (Vol. 82).

Ohkubo, M., Suzuki, K., & Kinoshita, S. (2004). Hash-chain based forward-secure privacy protection scheme for low-cost RFID. In *Proceedings of the SCIS, 2004*, 719-724.

Ouafi, K., Overbeck, R., & Vaudenay, S. (2008). On the Security of HB# against a Man-in-the-Middle Attack. *In Advances in Cryptology-ASIACRYPT 2008*, 108-124. Springer Berlin Heidelberg.

Özcanhan, M. H., Dalkılıç, G., & Utku, S. (2014). Cryptographically supported NFC tags in medication for better inpatient safety. *Journal of medical systems*, *38*(8), 61.

Özcanhan, M. H., Dalkılıç, G., & Utku, S. (2014). Cryptographically supported NFC tags in medication for better inpatient safety. *Journal of Medical Systems, 38*(8), 1-15.

Paar, C., & Pelzl, J. (2009). *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media.

Pang, L., He, L., Pei, Q., & Wang, Y. (2013). Secure and efficient mutual authentication protocol for RFID conforming to the EPC C-1 G-2 standard. In *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, 1870-1875. IEEE.

Pang, L., Li, H., He, L., Alramadhan, A., & Wang, Y. (2014). Secure and efficient lightweight RFID authentication protocol based on fast tag indexing. *International Journal of Communication Systems, 27*(11), 3244-3254.

Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2006a). M2AP: A minimalist mutual authentication protocol for low-cost RFID tags. In *Ubiquitous Intelligence and Computing*, 912-923. Springer Berlin Heidelberg.

Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2006b). LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. In *Workshop on RFID security*, 12-14.

Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2006c). EMAP: An efficient mutual-authentication protocol for low-cost RFID tags. In *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, 352-361. Springer Berlin Heidelberg

Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2009). Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard. *Computer Standards & Interfaces, 31*(2), 372-380.

Peris-Lopez, P., Hernandez-Castro, J. C., Tapiador, J. M., & Ribagorda, A. (2009). Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In *Information security applications*, 56-68. Springer Berlin Heidelberg.

Peris-Lopez, P., Hernandez-Castro, J., Estevez-Tapiador, J., & Ribagorda, A. (2009). An ultra-light authentication protocol resistant to passive attacks under the Gen-2 specification. *Journal of Information Science and Engineering, 25*(1), 33-57.

Peris-Lopez, P., Orfila, A., Mitrokotsa, A., & Van der Lubbe, J. C. (2011). A comprehensive RFID solution to enhance inpatient medication safety. *International Journal of Medical Informatics, 80*(1), 13-24.

Peris-Lopez, P., Safkhani, M., Bagheri, N., & Naderi, M. (2013). RFID in eHealth: How to combat medication errors and strengthen patient safety. *J. Med. Biol. Eng, 33*, 363-372.

Phan, R. C. W. (2009). Cryptanalysis of a new ultralightweight RFID authentication protocol—SASI. *IEEE Transactions on Dependable and Secure Computing*, *6*(4), 316-320.

Qian, X., Liu, X., Yang, S., & Zuo, C. (2014). Security and privacy analysis of tree-LSHB+ protocol. *Wireless Personal Communications, 77*(4), 3125-3141.

Qian, Z., Chen, C., You, I., & Lu, S. (2012). ACSP: A novel security protocol against counting attack for UHF RFID systems. *Computers & Mathematics with Applications*, *63*(2), 492-500.

Qingling, C., Yiju, Z., & Yonghua, W. (2008). A minimalist mutual authentication protocol for RFID system & BAN logic analysis. In *2008 ISECS International*

Colloquium on Computing, Communication, Control, and Management, 2008. CCCM'08. 2, 449-453. IEEE.

Rahman, M. S., Soshi, M., & Miyaji, A. (2009). A secure RFID authentication protocol with low communication cost. In *International Conference on Complex, Intelligent and Software Intensive Systems, 2009. CISIS'09*, 559-564. IEEE.

Ranasinghe, D., Engels, D., & Cole, P. (2004). Security and privacy: modest proposals for low-cost RFID systems. In *Auto-ID Labs Research Workshop, Zurich, Switzerland*.

Ren, X., Xu, X., & Li, Y. (2013). An One-way Hash Function Based Lightweight Mutual Authentication RFID Protocol. *JCP*, *8*(9), 2405-2412.

Rivain, M. (2011). Fast and Regular Algorithms for Scalar Multiplication over Elliptic Curves. *IACR Cryptology ePrint Archive*, *2011*, 338.

Rizomiliotis, P., & Gritzalis, S. (2012). GHB#: A provably secure HB-like lightweight authentication protocol. In *Applied Cryptography and Network Security*, 489-506. Springer Berlin Heidelberg.

Rohr, A., Nohl, K., & Plötz, H. (2010). Establishing Security Best Practices in Access Control. Berlin, Germany: Security Research Labs.

Rostampour, S., Namin, M. E., & Hosseinzadeh, M. (2014). A novel mutual RFID authentication protocol with low complexity and high security. *International Journal of Modern Education and Computer Science*, *6*(1), 17.

Safkhani, M., Peris-Lopez, P., Castro, J.C. H., & Bagheri, N. (2014). Cryptanalysis of Cho et al.'s Protocol, A Hash-Based Mutual Authentication Protocol for RFID Systems. *Journal of Computational and Applied Mathematics*, *259*, 571–577.

Sarma, S. E., Weis, S. A., & Engels, D. W. (2003). RFID systems and security and privacy implications. *In Cryptographic Hardware and Embedded Systems CHES 2002*, 454-469. Springer Berlin Heidelberg.

Schalk, G. H. (2013). RFID: MIFARE and contactless cards in application. Limbricht. Elektor Publishing.

Shen, J., Tan, H., Moh, S., Chung, I., & Wang, J. (2016). An efficient RFID authentication protocol providing strong privacy and security. *Journal of Internet Technology*, *17*(3), 443-455.

Siemens, (2010). Blood bags with RFID chips. Retrieved December 23, 2015, from http://www.siemens.com/press/en/presspicture/picturesphotonews/2010/pn201005.php.

Song, B., & Mitchell, C. J. (2008). RFID authentication protocol for low-cost tags. In *Proceedings of the First ACM Conference on Wireless Network Security*, 140-147. ACM.

Soos, M. (2017). *An overview of RFID security protocols* (Doctoral dissertation, Ph. D. Thesis. https://www. msoos. org/wordpress/wp-content/uploads/2012/03/soos_thesis_v3. pdf. Accessed 01 Sept).

Srivastava, K., Awasthi, A. K., Kaul, S. D., & Mittal, R. C. (2015). A hash based mutual RFID tag authentication protocol in telecare medicine information system. *Journal of medical systems*, *39*(1), 153.

Tagra, D., Rahman, M., & Sampalli, S. (2010). Flaws in a recent ultralightweight RFID protocol. In *International Conference on Software Telecommunications and Computer Networks, Croatia*, 6 – 10.

Tan, C. C., Sheng, B., & Li, Q. (2008). Secure and serverless RFID authentication and search protocols. *IEEE Transactions on Wireless Communications*, *7*(4), 1400-1407.

Tewari, A., & Gupta, B. B. (2017). Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *The Journal of Supercomputing*, *73*(3), 1085-1102.

Tian, Y., Chen, G., & Li, J. (2012). A new ultralightweight RFID authentication protocol with permutation. *IEEE Communications Letters*, *16*(5), 702-705.

Toiruul, B., & Lee, K. (2006). An advanced mutual-authentication algorithm using AES for RFID systems. *International Journal of Computer Science and Network Security*, *6*(9), 156-162.

Tounsi, W., Cuppens-Boulahia, N., Garcia-Alfaro, J., Chevalier, Y., & Cuppens, F. (2014). KEDGEN2: A key establishment and derivation protocol for EPC Gen2 RFID systems. *Journal of Network and Computer Applications, 39*, 152-166.

Tsudik, G. (2006). YA-TRAP: Yet another trivial RFID authentication protocol. In *2006 Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006*, 4-pp. IEEE.

Tsudik, G. (2007). A family of dunces: Trivial RFID identification and authentication protocols. In *International Workshop on Privacy Enhancing Technologies*, 45-61. Springer, Berlin, Heidelberg.

Tuyls, P., & Batina, L. (2006). RFID-tags for Anti-Counterfeiting. In *Topics in Cryptology–CT-RSA 2006,* 115-131. Springer Berlin Heidelberg.

U.S. Department of Health and Human Services (2015). Retrieved December 23, 2015, from http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm.

UCODE (2017). Retrieved March 20, 2017, from http://www.nxp.com/products/identification-and-security/smart-label-and-tag-ics/ucode:MC_50483.

Vajda, I., & Buttyán, L. (2003). Lightweight authentication protocols for low-cost RFID tags. In *Second Workshop on Security in Ubiquitous Computing–Ubicomp* (Vol. 2003), 1-10.

Van Deursen, T., & Radomirovic, S. (2008). Attacks on RFID Protocols. *IACR Cryptology EPrint Archive*, *2008*(310), 1-56.

Van Le, T., Burmester, M., & De Medeiros, B. (2007). Universally composable and forward secure RFID authentication and authenticated key exchange. In *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security*, 242-252. ACM.

Wang, S., Liu, S., & Chen, D. (2015). Security analysis and improvement on two RFID authentication protocols. *Wireless Personal Communications, 82*(1), 21-33.

Wang, S.H., & Wang, G.L. (2010). Analysis of passive attack on RFID authentication protocol ULAP. *Networks and Communications*, *36,* 17–19.

Want, R. (2006). An introduction to RFID technology. *IEEE pervasive computing*, *5*(1), 25-33.

Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2004). Security and privacy aspects of low-cost radio frequency identification systems. In *Security in pervasive computing*, 201-212. Springer, Berlin, Heidelberg.

WISP5, (2015). Wiki, "Welcome to the WISP 5 Wiki!," Retrieved December 23, 2015, from http://wisp5.wikispaces.com/WISP+Home, 2015.

William, S., & Stallings, W. (2006). Cryptography and Network Security: For VTU, 4/e. Pearson Education India.

Xiao, F., Zhou, Y. J., Zhou, J. X., & Niu, X. X. (2013). Provable secure mutual authentication protocol for RFID in the standard model. *Journal on Communications*, *34*(4), 82-87.

Yao, W., Chu, C. H., & Li, Z. (2012). The adoption and implementation of RFID technologies in healthcare: a literature review. *Journal of medical systems*, *36*(6), 3507-3525.

Yeh, T. C., Wang, Y. J., Kuo, T. C., & Wang, S. S. (2010). Securing RFID systems conforming to EPC Class 1 Generation 2 standard. *Expert Systems with Applications*, *37*(12), 7678-7683.

Yen, Y. C., Lo, N. W., & Wu, T. C. (2012). Two RFID-based solutions for secure inpatient medication administration. *Journal of medical systems*, *36*(5), 2769-2778.

Yoon, B., Sung, M. Y., Yeon, S., & Oh, H. S. (2009). HB-MP++ Protocol: An ultraLightweight authentication protocol for RFID system. In *Proceedings of IEEE International Conference on RFID*, 86 – 191. IEEE.

Yu, C., Chen, C., Liao, P., & Lee, Y. (2008). RFID-based operation room and medicare system for patient safety enhancement—a case study of keelung branch. *J. Inf. Manag*, *15*, 97-122.

Zhang, W., Liu, S., Wang, S., Yi, B., & Wu, L. (2017). An efficient lightweight RFID authentication protocol with strong trajectory privacy protection. *Wireless Personal Communications*, *96*(1), 1215-1228.

Zhang, W., Wu, L., Liu, S., Huang, T., Guo, Y., & Hsu, C. (2016). A trajectory privacy model for radio-frequency identification system. *Wireless Personal Communications*, *90*(3), 1121-1134.

Zhang, X., Li, L., Wu, Y., & Zhang, Q. (2011). An ECDLP-based randomized key RFID authentication protocol. In *2011 International Conference on Network Computing and Information Security (NCIS), 2011*, *2*, 146-149. IEEE.

Zhang, Z., & Qi, Q. (2014). An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. *Journal of medical systems*, *38*(5), 47.

Zhang, Z., Zhou, S., & Luo, Z. (2008). Design and analysis for RFID authentication protocol. In *IEEE International Conference on e-Business Engineering*, 574-577). IEEE.

Zhao, Z. (2014). A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem. *Journal of medical systems*, *38*(5), 46.

Zhou, S., Zhang, Z., Luo, Z., & Wong, E. C. (2010). A lightweight anti desynchronization RFID authentication protocol. *Information Systems Frontiers, 12*(5), 521-528.

Zhu, S., Yang, B., & Zhang, M. (2007). Research on RFID protocols and security. *Information Security and Confidentiality of Communications*, 168 – 170.

Zhuang, X., Wang, Z.H., Chang, C.C., & Zhu, Y. (2013). Security analysis of a new ultralightweight RFID protocol and its improvement. *Journal of Information Hiding and Multimedia Signal Processing*, *4*(3), 165–180.

Zhuang, X., Zhu, Y., & Chang, C. C. (2013). Security analysis of ultralightweight RFID protocols. *Technique Report.*

Zhuang, X., Zhu, Y., & Chang, C. C. (2014). A new ultralightweight RFID protocol for low-cost tags: R^2AP. *Wireless Personal Communications*, *79*(3), 1787-1802.

APPENDICES

APPENDIX 1: Code Sample of Shamir's Trick

```
/* Use Shamir's trick to calculate u1*G + u2*Q */
points[0] = 0;
points[1] = &curve_G;
points[2] = &public;
points[3] = ∑
numBits = smax(vli_numBits(u1, uECC_N_WORDS), vli_numBits(u2, uECC_N_WORDS));
point = points[(!!vli_testBit(u1, numBits - 1)) | ((!!vli_testBit(u2, numBits - 1)) << 1)];
vli_set(rx, point->x);
vli_set(ry, point->y);
vli_clear(z);
z[0] = 1;
for (i = numBits - 2; i >= 0; --i) {
uECC_word_t index;
EccPoint_double_jacobian(rx, ry, z);
index = (!!vli_testBit(u1, i)) | ((!!vli_testBit(u2, i)) << 1);
point = points[index];
if (point) {
vli_set(tx, point->x);
vli_set(ty, point->y);
apply_z(tx, ty, z);
vli_modSub_fast(tz, rx, tx); /* Z = x2 - x1 */
XYcZ_add(tx, ty, rx, ry);
vli_modMult_fast(z, z, tz);
}
}
vli_modInv(z, z, curve_p); /* Z = 1/Z */
apply_z(rx, ry, z);
```

APPENDIX 2: Code Sample for Both AES Encryption and Decryption

```
  void aes_encrypt(uint8_t data[16], uint8_t key[16])
  {
    uint8_t i = 0;
    // software reset
    AESACTL0 |= AESSWRST;
    // disable interrupt
    AESACTL0 &= ~AESRDYIE;
    // set encryption
    AESACTL0 &= ~(AESOP0 | AESOP1);
    // load key
    for (i = 0; i < 16; i++) {
                                AESAKEY_L = key[i];
                                }
    // load data
    for (i = 0; i < 16; i++) {
                                AESADIN_L = data[i];
                                }
    // wait till complete
    while (AESASTAT & AESBUSY);
    // read data
    for (i = 0; i < 16; i++) {
                                data[i] = AESADOUT_L;
                                }
  }
```

****

```
void aes_decrypt(uint8_t data[16], uint8_t key[16])
{
    uint8_t i = 0;
    // software reset
    AESACTL0 |= AESSWRST;
    // disable interrupt
    AESACTL0 &= ~AESRDYIE;
    // set decryption
    AESACTL0 &= ~AESOP1;
    AESACTL0 |= AESOP0;
    // load key
    for (i = 0; i < 16; i++) {
                                AESAKEY_L = key[i];
                                }
        // load data
    for (i = 0; i < 16; i++) {
                                AESADIN_L = data[i];
                                }
        // wait till complete
    while (AESASTAT & AESBUSY);
    // read data
    for (i = 0; i < 16; i++) {
                                data[i] = AESADOUT_L;
                                }
}
```

APPENDIX 3: A Code Sample for Acquiring 16 Measurements of ADC12

```
ADC12CTL0 |= ADC12ENC+ADC12SC;

while (ADC12CTL1 & ADC12BUSY);

returnVal = 0;

for(i=0;i<15;i++) {

returnVal = (returnVal<<1) | (ADC12MEM0 & BIT0);

ADC12CTL0 |= ADC12SC;

while (ADC12CTL1 & ADC12BUSY);

                }
```

APPENDIX 4: Sample Code of AERMAP-W5

```
void main(void) {
WISP_init();
// Set rng fonction
uECC_set_rng(&RAND_adcRand16);
.
.
.
// ECDH
printf("*********************************************************************\n");
printf("ECDH : \n");
printf("*********************************************************************\n");

.
.
.
// ECDSA
printf("*********************************************************************\n");
printf("ECDSA : \n");
printf("*********************************************************************\n");
.
.
.
// Key used for sign
printf("Key used for sign : "); vli_print(private_ECDSA, sizeof(private_ECDSA));
.
.
.

// Generate Hash of public key used in ECDH using SHA 256
uint32_t dataToHash[32];
uint32_t hash32[8];
memcpy(dataToHash, public_key, sizeof(public_key));
SHA_3(dataToHash, sizeof(dataToHash), hash32, SHA_256);
memcpy(hash, hash32, sizeof(hash));
printf("Hash of data : "); vli_print(hash, sizeof(hash));
.
.
.

// Generate data signature
uECC_sign(private_ECDSA, hash, signature);
printf("Signature : "); vli_print(signature, sizeof(signature));
.
.
.
// Check signature, generate secret key is success
printf("Check signature :\n");
if (!uECC_verify(public_ECDSA, hash, signature))

{
printf("uECC_verify() failed, secret key not genereted\n");

}
```

```
else
{
printf("uECC_verify() success, secret key generetion\n");

.
.
.


//Generate secret key
uECC_shared_secret(foreign_public, private_key, secret_key);
printf("Secret key : "); vli_print(secret_key, 16*sizeof(uint8_t));
 }
.
.
.
// AES
printf("*********************************************************************\n");
printf("AES : \n");
printf("*********************************************************************\n");
.
.
.
//Secret key
printf("Secret key : "); vli_print(secret_key, 16*sizeof(uint8_t));
.
.
.
//Data before encryption
printf("Data before encryption (%s) : ", data); vli_print(data, sizeof(data));
.
.
.
//Encrypt data
aes_encrypt(data, secret_key);
.
.
.
//Data after encryption
printf("Data after encryption (%s) : ", data); vli_print(data, sizeof(data));
.
.
.
while (FOREVER) { }
```

APPENDIX 5: Abbreviations

ADC	:Analog to Digital Convertor
AERMAP-W5	:AES and ECC Based RFID Mutual Authentication Protocol Proven on WISP5
AES	:Advanced Encryption Standard
AVISPA	:Automated Validation of Internet Security Protocols and Applications
BAN	:Burrows–Abadi–Needham
CC	:Chien & Chen
CPU	:Central Processing Unit
CRC	:Cyclic Redundancy Check
DES	:Data Encryption Standard
DoS	:Denial-of-Service
DSA	:Digital Signature Algorithm
EC	:Elliptic Curve
ECC	:Elliptic Curve Cryptography
ECDH	:Elliptic Curve Diffie-Hellman Scheme
ECDLP	:Elliptic Curve Discrete Logarithm Problem
ECDLP	:Elliptic Curve Discrete Logarithm Problem
ECDSA	:Elliptic Curve Digital Signature Algorithms
EC-RAC	:Elliptic Curve Discrete Logarithm Problem Based Randomized Access Control
EMAP	:Efficient Mutual Authentication Protocol

EPC C1-G2	:Electronic Product Code Class 1 Generation 2
ERAP	:Efficient Rfıd Authentication Protocol
EURFID	:Efficient Ultra-Lightweight Rfıd Authentication Protocol
FDA	:US Food and Drug Administration
FRAM	:Ferroelectric Random Access Memory
GNY	:Gong, Needham and Yahalom
HB	:Hopper and Blum
HF	:High Frequency
ID	:Identifier
ILMAP	:Improved Lightweight Mutual Authentication Protocol
IS-RFID	:Inpatient Safety RFID System
KEDGEN2	:A Key Establishment And Derivation Protocol For Epc Gen2
LAP-STP	:Lightweight Rfıd Authentication Protocol With Strong Trajectory Privacy Protection
LF	:Low Frequency
LMAP	:Lightweight Mutual Authentication Protocol
LSB	:least significant bit
M^2AP	:Minimalist Mutual Authentication Protocol
NIST	:National Institute of Standards and Technology
PRNG	:Pseudorandom-Number Generator
RAM	:Random Access Memory
RAPLT	:RFID Authentication Protocol For Low-Cost Tags

RAPP	:RFID Authentication Protocol With Permutation
REF	:Reference Module
RF	:Radio Frequency
RFID	:Radio Frequency Identification
RNG	:Random Number Generator
RSA	:Rivest–Shamir–Adleman
SASI	:Strong Authentication And Strong Integrity
SBW	:Spy-Bi-Wire
SCI	:Science Citation Indexed
SLAP	:Succinct And Lightweight Authentication Protocol
SPIN	:Simple Promela Interpreter
SRP	:Secure Remote Password
ucode	:Ucode System
UHF	:Ultra-High Frequency
ULAP	:Ultra-Lightweight Authentication Protocol
UMAPs	:Ultralightweight Mutual Authentication Protocols
USDHHS	:U.S. Department of Health and Human Services
WISP	:Wireless Identification and Sensing Platform
WISP5	:latest revision of Wireless Identification and Sensing Platform
XTEA	:Extended Tiny Encryption Algorithm
YA-TRAP	:Yet Another Trivial Rfid Authentication Protocol