Effective Protocols for Privacy and Security in RFID Systems Applications

Md. Monzur Morshed

MSc Engineering in Computer Science and Engineering, 1999,

Bangladesh University of Engineering and Technology, Dhaka

Masters in Global Information and Telecommunication Studies, 2007,

Waseda University, Tokyo, Japan

A thesis submitted to the Faculty of Computing, Engineering and Technology, Staffordshire University, in fulfillment of the requirements for the degree of Doctor of Philosophy.

March 2012

Abstract

Radio Frequency Identification (RFID) is a technology to identify objects or people automatically and has received many applications recent years. An RFID tag is a small and low-priced device consisting of a microchip with limited functionality and data storage and antenna for wireless communication with the readers. RFID tags can be passive, active or semi-active depending on the powering technique. In general passive tags are inexpensive. They have no on-board power; they get power from the signal of the interrogating reader. Active tags contain batteries for their transmission. The low-cost passive RFID tags are expected to become pervasive device in commerce. Each RFID tag contains a unique identifier to serve as object identity so that this identity can be used as a link to relate information about the corresponding object. Due to this unique serial number in an RFID tag it is possible to track the tag uniquely. The challenge raised by the RFID systems for certain applications is that the information in it is vulnerable to an adversary. People who carry an object with an RFID tag could be tracked by an adversary without their knowledge. Also, implementation of conventional cryptography is not possible in a low-cost RFID tag due to its limited processing capability and memory limitations.

There are various types of RFID authentication protocols for the privacy and security of RFID systems and a number of proposals for secure RFID systems using one-way hash functions and random number. Few researchers have proposed privacy and security protocols for RFID systems using varying identifiers. These are secured against most of the attacks. Due to varying identifiers they also include the recovery from desynchronization due to incomplete authentication process. However, due to the hash function of the identifier if one authentication process is unsuccessful, an adversary can use the responses in the subsequent phase to break the security. In this case the adversary can use the response for impersonation and replay attack and also can break the location privacy. Some protocols protect privacy and security using static tag identifier with varying responses so that they can work in pervasive computing environment. Most of these protocols work with computationally expensive hash functions and large storage. Since 2001 a number of lightweight protocols have been proposed by several researchers.

This thesis proposes seven protocols for the privacy and security of the RFID systems. Five of them use a hash function and a static identifier such as SUAP1, SUAP2, SUAP3 and EMAP. These

protocols are based on challenge-response method using one-way hash function, hash-address and randomized hash function. The protocols are operable in pervasive environment since the identifier of the tag is static. Another protocol named ESAP also works with static identifier but it updates the timestamp that is used with another random number to make the response unidentifiable. The protocol GAPVI uses varying identifier with hash function to ensure privacy and security of the tag. It is based on challenge-response method using one-way hash function and randomized hash function RFID system. Another proposed protocol EHB-MP is a lightweight encryption protocol which is more suitable for low-cost RFID tag because it does not require comparatively more computationally expensive hash function. Since 2001 Hopper and Blum developed the lightweight HB protocol for RFID systems, a number of lightweight protocols have been proposed by several researchers. This work investigates the possible attacks in the existing light weight protocols HB, HB+ and HB-MP of RFID systems and proposes a new lightweight authentication protocol that improves HB-MP protocol and provides the identified privacy and security in an efficient manner for pervasive computing environment. The validity and performance of the hash-based protocols are tested using analysis; simulation programs and some cases mathematical proofs have been given to prove the protection particularly from the special man-in-the attack in the EHB-MP protocol.

Finally this research work investigates the privacy and security problems in few most potential application areas that are suitable for RFID implementation. The areas are e-passport, healthcare systems and baggage handling in airport. Suitable RFID authentication protocols are also proposed for these systems to ensure the privacy and security of the users.

This thesis uses the symmetric cryptography for privacy and security protocols. In the future asymmetric protocols may be an important research consideration for this area together with ownership transfer of the tag could be a potential work area for research.

Declaration

I declare that this thesis was composed by myself and does not, to the best of my knowledge and belief

(i) contain any material that has been submitted for any other degree qualification except as specified;

(ii) contain any material previously published or written by another person except where due reference is made in the text.

Signed:

Date: 23-03-2012

Acknowledgement

Firstly I would like to express my gratitude to all mighty Allah who always helped me in all the phases of my life. I like to acknowledge my thanks to my principal supervisor Dr. Anthony Atkins for his heartiest cooperation in all the steps during my PhD program. I express my gratitude for his special attention, inspiration, patient guidance and stringent support during the course of the challenging research work. I am also grateful to my second supervisor Professor Hongnian Yu who always loved and supported me from his heart.

I would also express my gratitude to the Faculty of Computing, Engineering and Technology, Staffordshire University, UK for their support in all aspects. It is a great achievement for me to complete this PhD thesis successfully under this faculty. My thanks also go to the members of the research group who are working with Radio Frequency Identification (RFID). Special thanks to the PhD student Lizong Zhang for helping me to test RFID tag recognition using the RFID equipment.

I also thank my friend Professor Mostofa Akbar to encourage me to do PhD and helped me to do the PhD research. I also thank Dr. Sheikh Iqbal Ahamed for his help at any time I asked him about the privacy and security of RFID systems by providing me with study resources and ideas. My special thanks also go to my beloved colleague Dewan Mahboob Hossain who always encouraged me to complete my PhD research abroad.

My special gratitude is for the authority of EU E-link project which provided me with a scholarship to enable me to complete my PhD research in Staffordshire University.

I also thank to my parents who always helped me and encouraged me to do good in my study.

Finally I like to thank my beloved wife Mrs. Shazeda Akter, my daughters Elma Noorain Momo and Naisha Jahin Nisa for their sacrifice for me during my PhD study, which has enabled me to undertake and complete the PhD studies.

Table of Contents

List of Figures

List of Tables

Abbreviation

Term	Description
AC	Administrative Centre
AEA	Association of European Airlines
AES	Advanced Encryption Standard
AIDC	Automatic Identification and Data Collection
CC	Chien-Chen
CPAP	Complete Pervasive Authentication Protocol
CRAP	Challenge-Response based RFID Authentication Protocol
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DoS	Denial-of-Service
DPLK	Duc-Park-Lee-Kim
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EPC	Electronic Product Code
FCC	Federal Communications Commission
EHB-MP	Enhanced HB-MP
EMAP	Efficient Mutual Authentication Protocol
EOHLCAP	Enhanced One-way Hash-based low-cost Authentication Protocol
EPC	Electronic Product Code
ESAP	Efficient and Secure Authentication Protocol
FCC	Federal Communications Commission
GAPVI	Group-based Authentication Protocol using Varying Identifier
HAC	Hash-based Access Control
HB	Hopper and Blum
HB-MP	Hopper, Blum, Munilla and Peinado
HF	High-Frequency
HIDV	Hash-based ID Variation

HL7	Health Level Seven
IATA	International Airport Transport Association
ICAO	International Civil Aviation Organization
ID	Identifier
IoT	Internet of Things
ISO	International Standard Organization
LCAP	Low-cost Authentication Protocol
LK	Lim-Kwon
LF	Low-Frequency
LPN	Learning Parity with Noise
MAC	Message Authentication Code
MitM	Man-in-the-Middle
NDA	Non-Disclosure Agreement
OHLCAP	One-way Hash-based Low-cost Authentication Protocol
PRNG	Pseudorandom Number Generator
RAC	Randomized Access Control
RF	Radio Frequency
RFID	Radio Frequency Identification
RO	Read-only
RSA	Rivest Shamir Adleman
RW	Read-write
SA	Strong Adversary
SUAP	Secure Ubiquitous Authentication Protocol
TAP	Transportes Aéreos Portugueses
THC	Triggered Hash Chains
TID	Tag Identification
TSA	Transportation Security Administration
UHF	Ultra High-Frequency
UPC	Universal Product Code
WA	Weak adversary
YA_TRAP	Yet Another Trivial RFID Authentication Protocol

Chapter 1 Introduction

1.1 Background and Motivations

The objectives of this chapter are to introduce the research area and problem of the research work regarding effective protocols for Privacy and Security in RFID Systems Applications, in terms of the motivation, outline of the deliverables, contributions and to provide an overview of the structure of the thesis.

Radio **F**requency **Id**entification (RFID) is used in many applications such as in automation of automobiles, animal tracking, highway toll collection and supply-chain management [Garfinkel et al. 2005]. Large organizations like Wal-Mart, Procter and Gamble, and the United States Department of Defence are deploying RFID as a tool for automation of their supply chains [Jules 2006] and in civil and mining operations for tracking of equipment [Atkins et al. 2010]. RFID technology is also being used in infant management system. RFID security systems are deployed to locate wandering patients, and protect against infant abduction attempts [Saad and Ahmed 2007] and can also be used in healthcare management for tracking medical waste [Atkins et al. 2009]. The reduction in the cost of RFID and improvement in standardization it is becoming widespread in business use and emerging as the successor of optical barcode.

The main type of RFID tag is known as Electronic Product Code (EPC) tag which is standardized by an organization called EPCglobal Inc. [EPCglobal 2005]. RFID is a technology to identify objects or people automatically. An RFID system consists of three components: tag, reader and back-end database (Want 2005). An RFID tag is a small and extremely low-priced device consisting of a microchip with limited functionality and data storage and antenna for wireless communication with the readers. An RFID tag transmits data in the air in response to the interrogation by an RFID reader. RFID tags can be passive or active or semi-active depending on the powering technique. In general passive tags are inexpensive. They have no on-board power; they get power from the signal of the interrogating reader. Another type of tags called active tags contains batteries, whose batteries power their transmission. Active tags can initiate communications and have read ranges of 100 meters or more. Active tags are comparatively larger in size, more expensive. RFID readers are devices used to read or write data from or to RFID tags.

Low-cost passive RFID tags are expected to become pervasive device in commerce due to its suitability in the application of automation. Each RFID tag contains a unique identifier to serve as object identity so that this identity can be used as a link to relate information about the corresponding object. Due to this unique serial number in an RFID tag it is possible to track the tag uniquely. The challenge raised by the RFID system is that the information in it is vulnerable to an adversary. When a person carries an object which is RFID tagged this could be tracked by an adversary without their knowledge [Garfinkel et al. 2005]. Implementation of conventional cryptography is not possible in a passive RFID tag due to its limited processing capability and memory limitations [Prabhu et al. 2005].

Some researchers have proposed privacy and security protocols for RFID systems using varying identifiers [Henrici and Muller 2004, Lee et al. 2005, Song and Mitchell 2008]. These are secured against most of the attacks. Due to varying identifiers they also include the recovery from desynchronization due to incomplete authentication process. However, due to the hash function of only the identifier alone if one authentication process is unsuccessful, an adversary can use the responses in the subsequent phase to break the security. In this case the adversary can use the response for man-in-the middle attack and also can break the location privacy. Some protocols protect privacy and security using static tag identifiers with varying responses so that they can work in ubiquitous environment. The main challenges using RFID technology are to ensure all the privacy and security protections in the protocols.

The thesis is based on the following motivations:

- Due to the decreased cost of RFID and improvement in standardization it is becoming widespread in business use and emerging as the successor of optical barcode. Due to this unique serial number in an RFID tag it is possible to track the tag uniquely. However, it is infeasible to use conventional cryptography in passive RFID tags due its extremely limited processing and memory limitations. So it is important and challenging to design a new efficient and effective protocol for RFID systems to address the privacy issues.
- The U.S. government has mandated adoption of e-passports by the 27 countries in the Visa-Waiver Program in 2006 [Jules et al. 2005]. Other nations like Japan and most of the nations of Western Europe together with some other countries are involved in this project. These passports follow the guidelines of the International Civil Aviation

Organization (ICAO), an organisation run by the United Nations with a mandate for setting international passport standards from Document 9303 [ICAO 2005]. The guidelines recommend the inclusion of RFID chips, microchips capable of storing data and transmitting it in a wireless manner into a passport. However the RFID data in the e-passport is not fully protected from attacks of adversary.

- In the medical environment, the security and privacy problem will be crucial to RFID based medical applications. The privacy issue with tagged patient cards involves the risk of exposing the information, such as trace of personal location, information of personal health and clinical history. Through the tag the private data of a person can be tracked and the personal information can be captured which could be a violation of privacy under the Data Protection Act 1998. In the standard health level seven (HL7), the standard for customizing and detailed privacy mechanism has not yet been specified (Lee and Kim 2007).
- Many researchers proposed authentication protocols for the protection of privacy and security of the RFID systems. However these protocols require privacy, security and efficiency enhancements.
- The privacy and security of the RFID systems in group-based ubiquitous systems are considered in many authentication protocols. Existing group-based authentication protocols use hash functions and random numbers and have either privacy and security problems or efficiency problems. It is an important research issue to propose new protocols to enhance the systems in both privacy and efficiency.
- Group-based ubiquitous protocols are not suitable for the systems for a small system where there is no group. This also has problems to ensure privacy due to the common secret for all tags in a group as the secret is shared by many people. Therefore it is important to design an authentication protocol to ensure the privacy and security for individual tag with lower storage, computation and communication cost.
- The alternative approach of the ubiquitous protocols use hash function with varying identifier and secret value. However, existing protocols requires privacy, security and efficiency enhancement.
- As the low-cost RFID tags have limited storage, computation and communication capabilities recently light-weight encryption based protocols are being proposed by many researchers. However the challenges in these protocols are to ensure the privacy and security efficiently and effectively with minimum error and lower storages.

1.2 Aim and Objectives

The aim of this research is to investigate the current privacy and security problems of RFID systems and propose protocols with effective and efficient privacy and security properties for the different RFID applications. The objective of the research is to propose new protocols to address the privacy and security issues in RFID systems for low-cost RFID tags and is achieved as follows:

- To identify the challenges through literature review with the relevant fields of RFID systems, application, privacy and security problems and the basic cryptographic techniques that can be used in low-cost RFID systems.
- To investigate the existing protocols for privacy and security of RFID system.
- To develop new protocols for RFID privacy, security and safety to improve efficiency and reliability.
- To develop simulation software and carry out experiment using the simulation software based on the developed protocols.
- To evaluate the performance of the developed protocols against other privacy and security protocols in terms of potential benefits effects to justify the adoption of proposed work.
- To propose architectures for the implementation of the developed protocols in real life application like healthcare systems and e-passport.

1.3 The Design Issues

The design issues of this research are privacy, security and efficiency of the systems. It will consider the privacy and security problems in various applications like healthcare systems, e-passport and luggage handling in airport.

The privacy and security issues: There are several privacy and security issues in RFID systems. These issues are information leakage, location privacy, impersonation and replay attack**,** message interception or denial of services, forward and backward traceability.

The efficiency issues: For efficiency issue storage cost, communication cost and computation cost are considered. For storage cost both the tag and the databases are considered. Typically reader

does not store the database information. In some cases the reader can also have some storage to store the tag information. Communication cost is the size of the information transferred between the reader and the tag. The computation cost refers to the function and mathematical and logical operations required in both the tag and the database.

Another issue is the suitability in the implementation in applications. Different applications have different privacy and security requirements. The structures of the data are also different and used in various applications and this also influences on the design of the privacy and security systems.

The design objective is to propose new authentication protocols to ensure the privacy and security of the RFID systems with less storages and computations.

1.4 Research Outcomes

To achieve the objectives identified in section 1.2, this research leads to the following outcomes:

- A report/survey results on current issues of privacy and security problems in RFID system and in wireless technology.
- A report on the different types of the existing protocols for privacy and security of RFID system indicating their limitations.
- New protocols and systems for RFID privacy and security to improve the existing protocols for use in wireless technology.
- Evaluation of the proposed protocols in terms of efficiency and reliability against other privacy and security protocols. Potential benefits and effects of the adoption of proposed system will also be evaluated using simulation and storage requirement calculations.
- Uses of the proposed protocols in different applications.
- Dissertation
- 5 Conference papers and two journal papers.

1.5 Statement of Ethics

Many ethical issues are considered in any research works. This research work will follow the all ethical guidelines outlined by the ethical guidelines of Staffordshire University. The following guidelines are considered in this research.

- Accreditation: Due accreditation will be given to the individuals and organizations whose work have been cited via proper references. In this research Harvard referencing is used.
- No plagiarism: Plagiarism is the act of using the ideas, thoughts, pictures, theories, words, or stories of some other person as your own. Plagiarism is both an illegal and punishable act. It is ensured that no plagiarism is done in any level in this research.
- Confidentiality: Confidentiality should be maintained when private data are used for any research purpose. No private data are used for this research. So No confidentiality issues were considered for ethical issues.
- Collection of Data: Data collection is an important aspect to conduct a research. When data is collected from any person or an organization it should be taken care that the collected data is essential and pertinent to the research purpose. No data collection is required from any individual(s) or organization(s) for this thesis.
- Informed consent: Informed consent is required if data are required to collect from them from individual (s) or organization(s). This thesis does not require data collection so informed consent is not applicable.
- Non-Disclosure Agreements (NDAs): NDAs are required to sign at the request of industrial collaborations that provide data set(s) for validation purposes or offered professional insights for the research. However this thesis does not require any datasets for validation purposes.

1.6 Research Process

This section presents an overview of research design and methodology. It includes the different research methods, strategies and a technique used in the area of computing and illustrates the

research philosophy and methodology that was adopted in this thesis. All the research works can be viewed as a process which has a number of stages that should be followed to reach the goal of the research. Research process is referred as 'onion' by [Saunders et al. 2007]. It has six layers as shown in Table 1-1. Each layer is presented as a stage in the research process. The research onion and its layers are shown in Figure 1-1. Figure 1-1 also shows the philosophy, approach, strategies, choices and techniques adopted in this research as shown in dotted block.

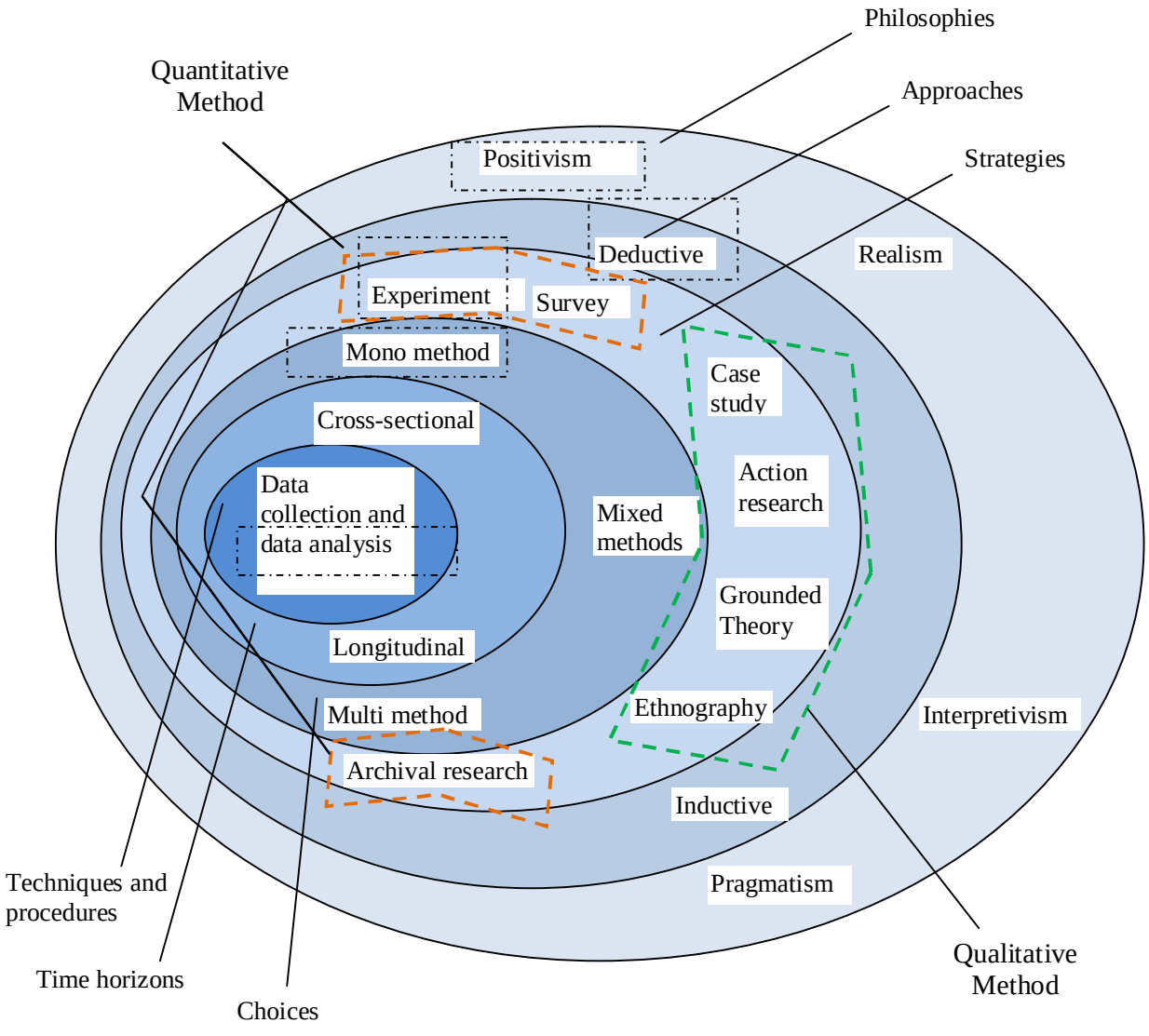

Figure 1-1: The research 'Onion' [Sounders et al. 2007]

Table 1-1 The Research 'onion' in Tabular Form [Saunders et al. 2007]

Layer	Approaches
2. Research philosophy	**Positivism**, Realism, Interpretivism, Pragmatism
3. Research Approaches	**Deductive**, Inductive
4. Research Strategies	**Experiment**, Survey, Case study, Grounded theory, Ethnography, Action research
5. Research Choices	**Mono methods**, Mixed methods, Multi methods
6. Time horizons	Cross-sectional, Longitudinal
7. Techniques and procedures	**Data collections and data analysis**

1.6.1 Research Philosophy

To carry out any research work it is essential to know the essential fundamental assumptions about the way in which one views the world. Research can be explained, measured and classified at different levels. The most basic level is to classify the research from a philosophical view which is described by the research process 'onion' model as depicted in Figure 1-1. There are various types of research philosophies such as positivism, realism, interpretivism and pragmatism [Saunders et al. 2007].

Positivism states that knowledge has to be objectively based from depicting a logical inference from observable, measurable and verifiable facts. Positivism typically implements clear quantitative approach for investigating phenomena based on statistical factors. Positivist approaches include case study research and other research where there exists evidence of formal propositions, quantifiable measures of variables, hypothesis testing and illustration of conjectures about incident from the sample to a known population [Mayer, 1977].

1.6.2 Research Approach

There are various types of approaches to accomplish and evaluate a research work. The approach depends on the research context and nature of the work. There are mainly two types of research approaches: deductive and inductive [Saunders et al. 2007]. The deductive research approach does

in a top-down process where it begins with the development of a theory relating to the research, subsequently by the making of the hypotheses for testing, gathering of observations to deal with the hypotheses, and then the validation of the hypotheses with the utilization of the specific data. On the other hand, inductive research approach performs in a bottom-up fashion, starting with the observation, followed by the detection of patterns and regularities, construction of a tentative hypothesis, and then the development of a general conclusion based on the former analysis. The two approaches are shown in Figure 1-2.

.

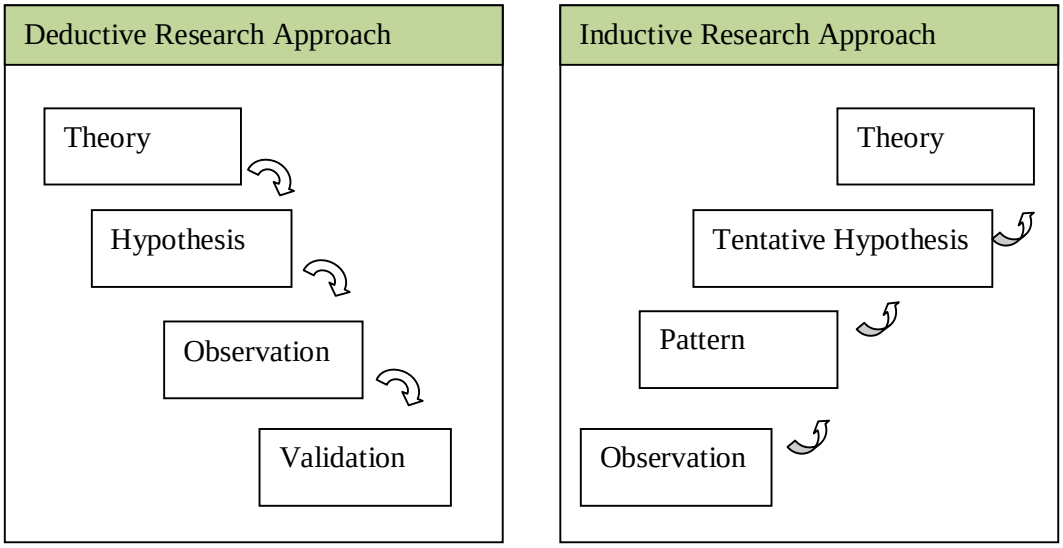

Figure 1-2: Deductive versus Inductive Research [Trochim 2001]

1.6.3 Research Strategy

Research strategies can be classified in different ways. Each strategy can be adopted for exploratory, descriptive and explanatory research [Yin 2003]. Part of these approaches fits into the deductive research approach and other parts in inductive research approach. Literature suggests that the most common categories of research methods are qualitative and quantitative research methods [Kumar 2005]. Qualitative research methods were firstly adopted in the social sciences to facilitate researchers to study social and cultural phenomena [Myers, 1977]. These types of methods look for the collection of data in the shape of written or spoken words, and do not usually include any numerical measurements. Examples of qualitative data sources include documents, texts,

interviews, questionnaires and participants observation. There are four main strategies are in the qualitative research: action research, case study research, ethnography and grounded theory.

Alternatively, quantitative research methods are suitable where quantitative measures of the variables of interest are possible, where hypothesis can be constructed and verified, and where inferences can be made [Moore 2006, Creswell 2003]. Quantitative research methods were at first adopted in the fields of natural sciences for studying natural phenomena [Kumar 2005]. These methods collect data which is in a numerical form and can be analyzed using table, various charts of data and histograms etc. Some of the examples of quantitative data sources are laboratory experiments, statistical returns, census data and structured surveys. There are two main strategies in quantitative research methods: experiments and surveys.

1.6.4 Choices

The way in which one chooses to combine quantitative and qualitative techniques and procedures is referred to as research choice. Typically quantitative and qualitative methods and procedures do not work individually. In selecting the research methods it can use a single data collection technique and corresponding analysis procedure called mono method or use multiple data collection technique and procedure for the answer of the research question (multiple methods). If a mono method is chosen it will combine either a single quantitative data collection technique or a single qualitative data collection technique [Saunders et al. 2007]. The term multi-method refers to combinations of more than one data collection technique with associated analysis techniques, but this restricted within either a quantitative or qualitative research methods. Mixed methods approach is the general term for when both the quantitative and qualitative data collection techniques and analysis procedures are used. For example in a series of semi-structured interview it requires both quantitative and qualitative methods.

1.6.5 Time Horizons

Time is an important issue in any research work. The studies can be classified in two ways: cross-sectional studies and longitudinal studies. Cross-sectional studies happen at a single point in time and including a slice or cross-section. Typically longitudinal studies happen over a period of time.

The research conducted in a longitudinal approach because in order to enable coverage of relevant data and information which a cross-sectional study does not provide. This will likely include a fair analysis of the literature to identify the problems in existing RFID privacy and security systems. A longitudinal time horizon is therefore considered more appropriate for this research.

1.6.6 Techniques and Procedures

Data can be divided into primary and secondary data. Normally in research both primary and secondary data collection methods are used.

The primary data refers to the data which is obtained for the first time and used specially for the current research. Primary data can be collected through surveys, interviews, brainstorming and seminars etc. Primary data are more accommodating as it contains latest information in a convenient way. In fact, the researchers can ask the questions that are set to elicit the data that will help them with their study. The researchers can collect the data for specific purpose.

On the other hand secondary data refers to the collection of data which has been collected and used by other purpose than the current research work. In secondary data information relates to the past periods. Secondary data can be collected from various sources such as academic journals, conference research papers, books, industry library and reports, private or public organizations etc. For example, survey reports or secret records collected before by a business group can offer information that cannot be obtained from original sources.

1.7 Outline of the Chapters

The thesis has eight chapters and Figure 1-3 shows the structure of the chapters. The chapters of the thesis are organized as follows:

Chapter 1 introduces the aim and objectives of the research and introduces the motivations, outcomes and statement of ethics. It also outlines the research methods carried out for different types of research works. It includes research philosophy, research approach, research strategy, techniques etc.

Chapter 2 introduces an overview of the RFID systems. It gives an overview of the components of the RFID Systems RFID tag, reader and database. It classifies the RFID tags according to various physical and logical properties. It also describes the standards of the RFID tags proposed by different organizations. This chapter focuses on some applications of RFID systems for automation. It also identified the privacy, security and performance of RFID systems. It also outlines the general security and cryptographic techniques.

Chapter 3 discusses the existing privacy and security protocols of the RFID systems. There are various approaches to ensure the privacy and security protection of the RFID systems. It explains the various physical and logical approaches for the protection of the RFID systems from the adversary. It also classifies the various RFID authentication protocol according to privacy and security architecture. It identifies the various advantages and problems of the existing authentication protocols in different application scenarios.

Chapter 4 presented the proposed new protocols for privacy and security of RFID Systems. It proposes four protocols using hash function, hash address, random numbers. It uses two random numbers in tag side and the reader side. The protocols of this chapter use static identifiers to implement the privacy and security of RFID systems in the ubiquitous environment. It proposes two types of protocols. It uses group-based protocols for a big system where the tags are classified into the various departments so that it can be easy to manage and control. In this case the privacy and security is also managed in a group. It also proposes authentication protocol for a system where the privacy and security is fully implemented individually in each tag.

Chapter 5 presented a new protocol for the privacy and security of the RFID system using static identifier and hash function. However it uses a timestamp instead of a random number in the reader side and one random number in the tag side. It also compares the advantages of the using the timestamp for a random number in privacy and security of the RFID system.

Chapter 6 proposes a new protocol for the privacy and security of the RFID systems using varying identifier and secret. It also uses hash function and random numbers to ensure privacy and security. It presented the recovery of the identifier due to any incomplete authentication process for any reason.

Chapter 7 proposes a new protocol using light-weight encryption technique. Light-weight encryption technique mostly uses bitwise xor operation or other simple bitwise operations that are suitable for low-cost RFID tag. This chapter identifies the problems in the existing light-weight RFID authentication protocols and proposes a new protocol to overcome the privacy and security problems efficiently and effectively.

Chapter 8 selects three real life scenarios that are potentially important candidates to use RFID systems for automation and improved management. The areas are hospital, e-passport and baggage handling in the airport. This chapter shows the possible privacy and security threats in these applications and proposes RFID authentication protocol suitable for the systems.

Chapter 9 presents the conclusions and summaries of the main findings of this research work. It also recommends future works to improve the privacy and security protection of the RFID system.

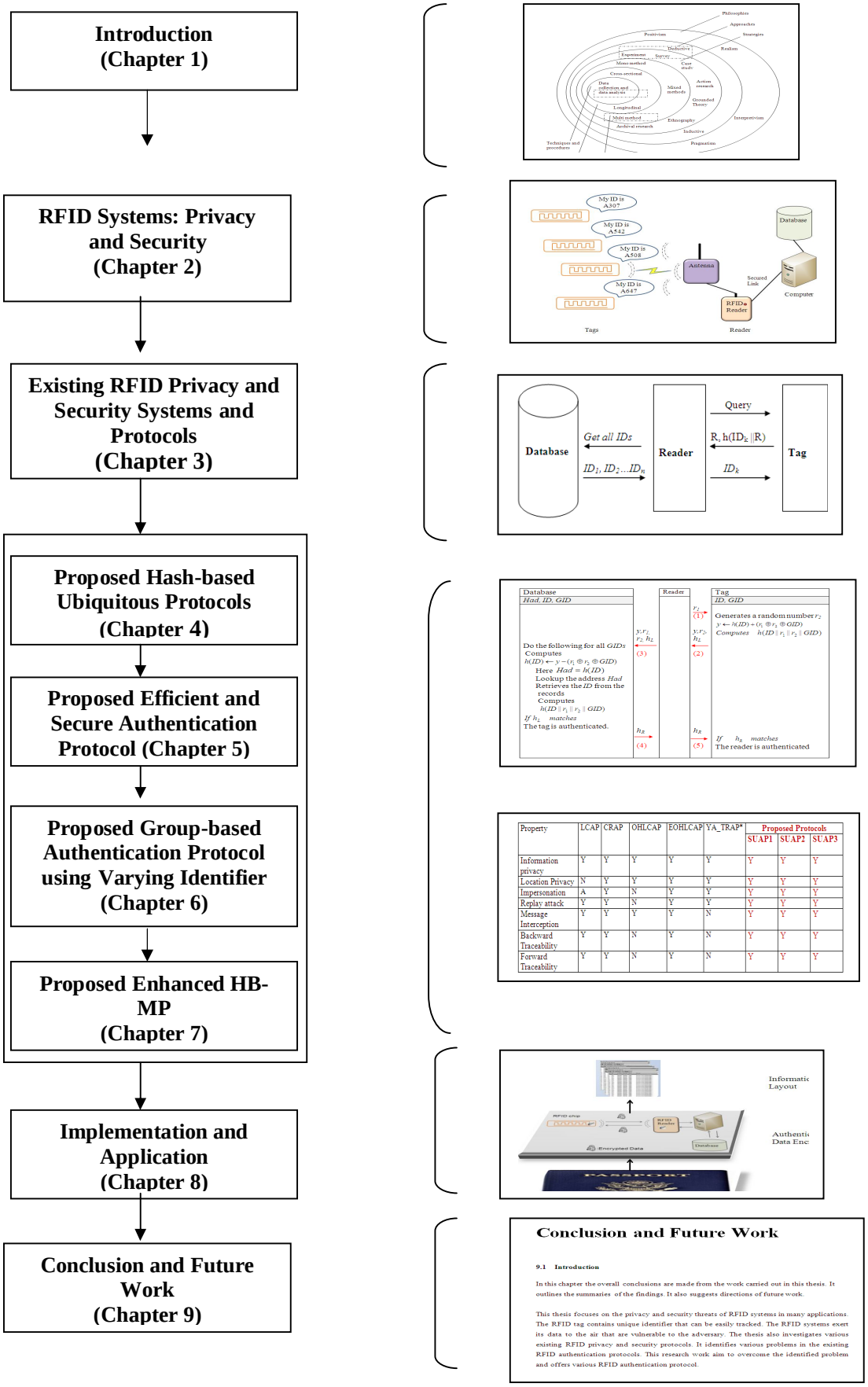

Figure 1-3: Structure of the Thesis

Chapter 2 Introduction to RFID Systems and Privacy and Security Issues

2.1 Introduction to RFID System

The objectives of this chapter are to introduce an overview covering the RFID systems, its privacy and security problems and also that are used in computer networks and information systems. In privacy and security section it includes different types of privacy and security threats in RFID systems.

Radio Frequency Identification is a technology to identify objects or people automatically. An RFID system consists of three components: tag, reader and the back-end database [Want 2005, Lee et al. 2005]. A typical RFID system is shown in Figure. 2-1 and the characteristics of the RFID system outlined as follows:

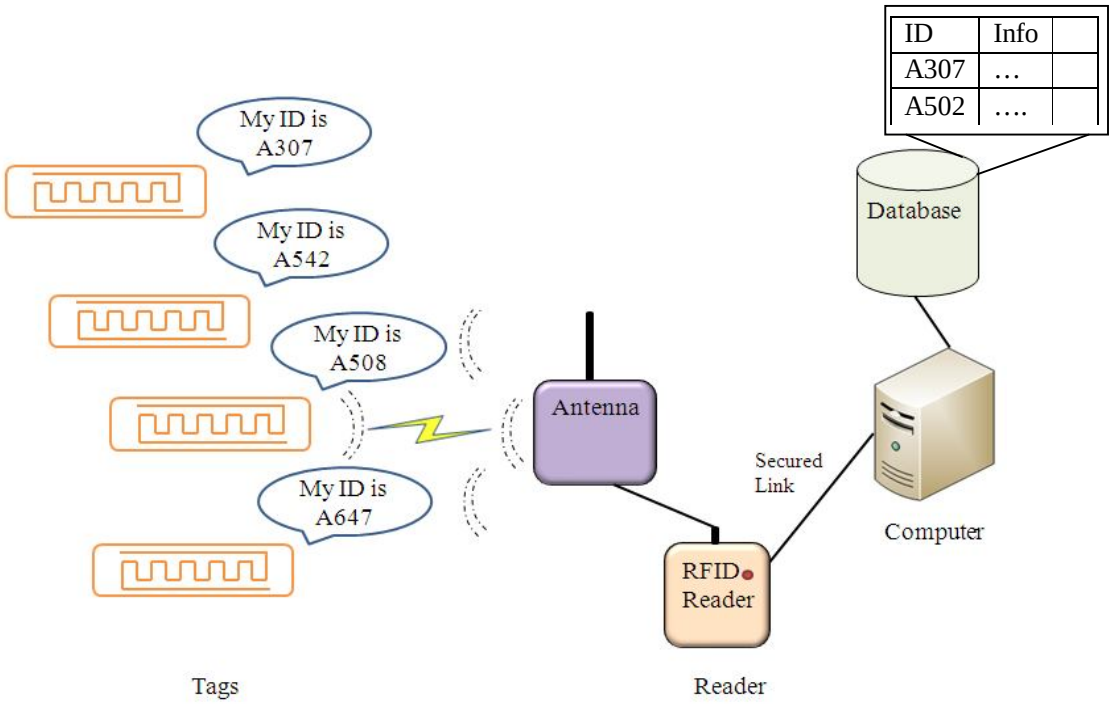

Figure 2-1: Typical RFID System Components

2.1.1 RFID Tag

An RFID tag is a small and extremely low-cost device having a microchip with limited processing capabilities, data storage and antenna for wireless communication with readers. The microchip is used for processing data, to modulate and demodulate radio signals, and to store and processes information and is sometimes referred to as a ‘transponder’. Sometimes the term `tag' is used for its simplicity. An RFID tag transmits data in the air in response to the interrogation by an RFID reader. Memory on tags may be of different types such as read-only, write-once read-many, or fully rewritable [Weis et al. 2004].

2.1.2 RFID Reader

RFID readers are devices to read or write data from or to RFID tags. It is also called a transceiver or interrogator. The readers query to a tag to obtain information from the tag. The readers interrogate tags for their contents using an RF interface. The readers typically contain internal storage, processing power, sometimes an interface to the back-end databases to offer some other additional functionality [Weis et al. 2004]. The readers may use tag data as a look-up key into a database storing product information, tracking logs, or key management data [Weis et al. 2004].

Readers should be able to identify a particular tag, from among a collection of many tags. During this identification process, multiple tags responses may interfere with each other. It requires an anti-collision algorithm. The algorithms may be probabilistic or deterministic. A familiar probabilistic algorithm is the Aloha scheme [Bing 2002, Metcalfe and Boggs 1976] used in Ethernet local area networks. In the case of RFID system, RFID tags avoid collisions with other tags by responding to the queries of the readers at random intervals. At the time of a collision, the perpetrator tags wait for other tags for longer and random interval before trying again. Higher densities of tags will result in a higher collision rate and degraded performance.

The binary tree-walking scheme is a simple deterministic algorithm that can be used in RFID system. In this system, a reader queries all the tags for the next bit of their *ID* number. If the reader detects a collision in any position it implies that at least two tags have different bit values in that position of the *ID*. The reader will then send a response bit to indicate which tags should carry on with the protocol and which should stop giving response. Each selection of bit represents a branch to choose in a binary tree. The leaves of the tree represents thee tag *ID* numbers. Assuming the tags

have unique *ID*s, after walking to a leaf in the tree, a reader has addressed a particular tag. The advantages of binary tree-walking are that it has simple tag operation and can efficiently broadcast only the bits of an *ID* to address any tag.

2.1.3 RFID Middleware and Database

RFID middleware is a new breed of specialized software that sits between the RFID readers and the enterprise applications [Prabhu et al. 2005]. It is in charge of converting low-level RFID hardware information into useable event information. The main purpose of the middleware is to process data from the tags collected by the readers used in the systems, or to write *ID* numbers and data to the tags while the assignment is done of these tags for attaching to the individual items. The middleware is responsible for the translation of machine information into information related to tag events. This event specially indicates that it has detected a tag. The minimum information that the middleware reports, is the tag *ID*. This may contains other information like reader ID, Date/time stamp etc. The middleware give a standard communication mechanism for the readers and the tags. The reason is that it gives a higher-level communication system for the computer information systems and applications with the RFID infrastructure without the knowledge of lower level issues to communicate with the RFID hardware [Banks et al. 2007]. Some RFID systems can handle other events like status of the tag memory, tag sensor information, tag battery level, tag position, tag info zone, tag out of zone etc.

The middleware has other benefits. It can provide a single mechanism to communicate with different RFID infrastructures [Banks et al. 2007]. For example, the system can communicate with both the active tag and passive tag system. This tremendously reduces the IT resources requirements.

2.2 Classification of RFID Tags

RFID tags can be classified in three ways. Classification is based on

1. Powering techniques
2. Processing capacity
3. Operating frequency
4. Memory Type

2.2.1 Powering Techniques

RFID tag can be passive, semi active or active depending on the powering technique.

- Passive Tags: In general passive tags are inexpensive. They have no on-board power; they get power from the signal of the interrogating reader. Power is provided by the reader. The reader creates radio frequency wave that induces in the antenna a tiny but sufficient electrical current to activate the tag [Banks et al. 2007]. When the tag comes near the range of the reader's radio frequency wave field, it uses the energy to power up its internal components. It can then communicate with the reader. The advantages of these types of tags are that they are low cost (3p), very small in size and require no internal power supply. It has drawback that the range of operation is very short for example a few meters. The antenna configurations vary widely based on the application of the tag. Different configurations work differently based on the environment in which the tag will be used. Passive tag can operate in many frequency bands. Low-Frequency (LF) tags operates in 124 kHz to 135 kHz, have a traditional range up to half a meter. High-Frequency (HF) tags operate in 13.56 MHz have range up to a meter or more. Ultra High-Frequency (UHF) tags operate at the frequencies of 860 MHz to 960 MHz; have a read range up to 10 meters.

- Active Tags: Active tags have on-board power. It is powered by its own battery for the operation of the tag over a period of time. The active tags beeps at a specified intervals. The life of the battery in active tags is determined by the frequency of the beeps. The battery life is shorter for the tags having higher beeping frequency. These tags are constantly beeping and so there is no requirement to be within the power field of the reader to be detected. The advantage of these types of tags is that the signal strengths of the active tags are much more than the passive tags and can be read from a further distance [Banks et al. 2007]. An active tag can be detected from 1.5 km away from the reader in an open-field environment with no minimum interference. There are few disadvantages of the active tags. First, the cost of the active tag is much higher than the passive tag. The active tags must have a self-contained power source. Therefore the cost of the tag is depended on the cost of the battery, which is itself is usually more than the cost of a passive tag. Second, the size of the active tag is much bigger that the passive tag. It is because the battery takes space in the active tag. This increases the size of the active tag dramatically. Another problem is that the uses of the

active tags are bounded by the life of the batteries that power them. When batteries go down it cannot communicate with the reader. Active tags can initiate communications and have read ranges of 100 meters or more. Active tags are expensive and costing some $20 or more.

- Semi-Active Tag: The uses of active tags are limited by the life of the batteries and frequent 'beaconing' reduces the life of the battery. A semi active tag overcomes these problems. It is a combination of a passive and an active tag. The passive component of the tag is energized by the reader when they enter into the electromagnetic field of the reader. When it is energized, it triggers the active component of the tag to send an RFID signal. Then battery is only used when it is activated by the passive components of the tag. After a predetermined amount of time it goes to sleep mode thus saving battery life [Banks et al. 2007]. The range of the semi-active tag is higher than the passive tag.

2.2.2 Processing Capacity

According to processing capacity, RFID devices can be classified into two broad categories, 'dumb' and 'smart'.

- Dumb tag: A dumb tag has no significant processing capacity and typically a dumb tag would be considered as a passive tag. The unique identifier of the tag will be a small fixed length value, typically 10 or 16 hexadecimal digits long. The memory capacity is also very small- for example a few hundred bytes to a maximum of around 2KBs [Laurie 2007]. In its simplest implementation, a tag listens for a radio signal, and sends a signal of its own as a reply [Thornton et al. 2006]. More complicated systems may transmit a single letter or digit back to the source, or send multiple strings of letters and numbers [Thornton et al. 2006].

- Smart tag: A smart tag has processing capability and typically this would be a semi or active tag. It has on-board processors and is typically capable of doing cryptographic operations [Laurie 2007]. It usually has larger memory capacity of 32 KBs or more, and is capable of performing authentication before allowing access to the stored data for the valid users [Laurie 2007]. This tag may also have the capabilities to encrypt the data used in communications with session keys to avoid snooping or data injection attacks [Laurie 2007].

2.2.3 Operating Frequency

The operating frequency is the electromagnetic frequency by which a tag communicates with a reader and it also may be used to obtain power. Passive tag can operate in many frequency bands. The electromagnetic spectrum within which RFID systems typically operate is commonly divided into low frequency (LF), high frequency (HF), ultra-high frequency (UHF), and microwave [Glover and Bhatt 2006]. Low-Frequency (LF) tags operates in 124 kHz to 135 kHz, have a traditional range up to half a meter. High-Frequency (HF) tags operate in 13.56 MHz have range up to a meter or more. Ultra High-Frequency tags operates at the frequencies of 860 MHz to 960 MHz, have a read range up to 10 meters. For UHF the dominant standard will be likely to be Class-1 Gen-2.

Due to the different properties of different frequencies these are used in different applications according to the requirements. Lower frequency signals are more suitable to travel through water, while higher frequencies can carry information at higher rates [Glover and Bhatt 2006]. Higher frequency signals are typically also easier to read at a distance.

2.2.4 Memory Type

Another category of RFID tags is that RFID tags may be either read-only (RO) or read-write (RW). The memory space can be used as writable and non-writable data storage. Tags can be manufactured as read-only, write-once read-many, or fully rewritable. Depending on the types of tag, tag programming is done at the manufacturing level or at the application level. The RO tags can only be read by the reader and the communication between the tag and the reader is unidirectional. RW tags provide the capability of both reading information from the tag and writing information to the tag at any time. The tag has a memory space to store information it requires and sent to it from the reader [Banks et al. 2007]. The size of the memory space varies from few bytes to hundreds of KB.

2.3 RFID Standard

There are different vendors for RFID solutions with different methodologies for communications between the readers and the tags. All the vendors had their own mechanism claimed to be the best for their purpose. However, it raises an important problem when they like to communicate with

each other. As a result the readers and tags from different vendors may not communicate with each other. It was a barrier for the growth of a large scalable RFID system. To facilitate the rapid growth of RFID systems several organizations have attempted to create a single standard of communication. Massachusetts Institute of Technology's (MIT) Auto-ID lab and the International Organization for Standardization (ISO) have provided a platform for the RFID providers and the users to create a standard for inter-industry RFID communication. These standards deal with many aspects of the communication of the RFID systems such as how the tags and the readers communicate with each other and what data is given by the RFID system to the consumer applications [Banks et al. 2007].

2.3.1 EPC Standard

The main form of RFID tag is known as Electronic Product Code (EPC) tag which is standardized by an organization called EPCglobal Inc [EPCglobal 2005]. The Electronic Product Code standard was developed by the Auto-ID centre at MIT with the collaboration of academic and industry personnel. It is now administered and managed by EPCglobal Inc. The standard provides a mechanism to uniquely identify every product for manufacturing. The Universal Product Code (UPC) ensures only the mechanism to uniquely identify the type of the product. The EPC ensures the identification of every instance. As there are a large number of products manufactured in the world the protocol must uniquely identify every instance from the large number of diverse products. To do this, the EPC standard divides the manufacturer and product number in a way that is compact and sensible [Banks et al. 2007]. Figure 2-2 shows an example of an EPC coding scheme.

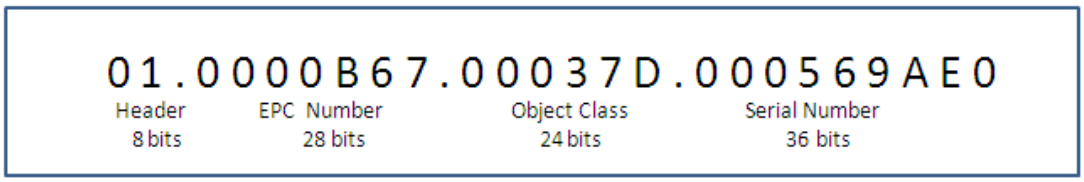

Figure 2-2: EPC-based Information

EPCglobal Inc. has specified six categories of RFID tags class-0 to class-5. Table 2-1 shows an overview of the classification of tags based on their power characteristics, read ranges, memory capabilities, communication protocol, and peripheral systems. Class 0 to Class 3 is usually for

passive tags. Active tags are specified by Class 4. Class 5 is reserved for the reader and the active tag that can read information from other tag.

Table 2-1 EPC Tag Classifications (Reprinted from GS1 US)

Class	Power	Range	Memory	Communication	Peripherals	Cost
0	None	<3 m	1-96 bits Read Only	Backscatter	None	Low
1	None	<3 m	1-96 bits Read/Write Once	Backscatter	None	Low
2	None	<3 m	1-96 bits Read/Write	Backscatter	Security	Medium
3	Battery	< 100 m	< 100 Kilobytes Read/Write	Backscatter	Security, Sensors	High
4	Battery	< 300 m	< 100 Kilobytes Read/Write	Active Transmission	Security, Sensors	High
5	Battery, AC/DC Connection	Unlimited	Unlimited Read/Write	Active Transmission	Security, Sensors Can communicate with other tags	Very High

2.3.2 ISO Standard

International Standard Organization (ISO) provides different types of industry standards. This organization is made up of over 140 members from over 90 nations. ISO also is working with RFID for its standardization. This standard also defines the communication protocol of RFID components, data elements and data interfaces for dealing with RFID information [Banks et al. 2007].

2.4 Passive Tag Memory Layout

Passive tags stores various information like unique identifier, current state and user defined data etc. Tag memory is logically divides into four banks. Each bank has 0 or more memory words as shown in Figure 2-3. The memory banks are reserved, electronic product code, tag identification and user

memory banks. Figure shows the layout of data in a set of four memory banks on the tag. A logical memory map is also shown in Figure 2-4 [EPCglobal, 2005].

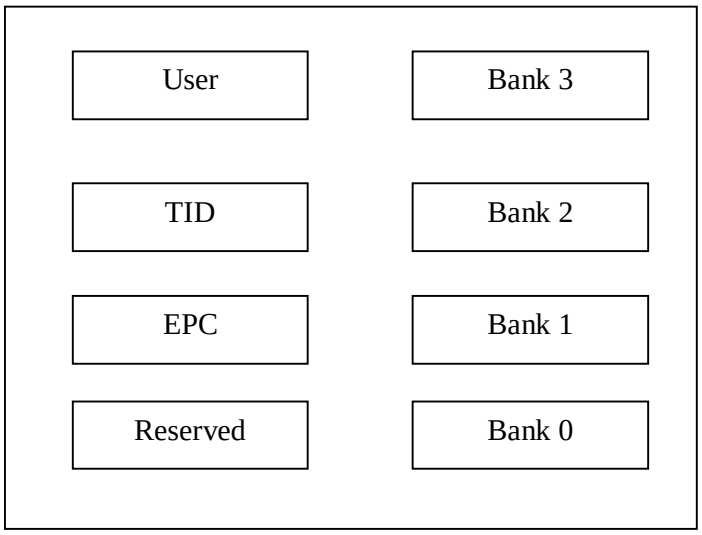

Figure 2-3: Tag Memory Layout

Reserved memory: The reserved memory bank contains the Kill and Access passwords if passwords are implemented on the tag. A reader must know the appropriate password to issue a Kill command. If a tag does not implement Kill or access password, the tag logically operates as zero valued passwords that are permanently locked for read/write.

EPC memory: The EPC memory contains a StoredCRC at memory addresses 00_n to $0F_n$ and a StoredPC at 10_n to $1F_n$. The StoredCRC is 1 16-bit Cyclic Redundancy Check (CRC-16) field. It is used to validate the data in EPC memory bank. StoredPC is the Protocol Control field. For EPC compliant tags, this code is an EPC as defined by EPCglobal. This field can also hold other types of codes by the data format defined by the manufacturer [EPCglobal, 2005].

TID memory: Tag identification (TID) memory banks contain an 8-bit ISO/IEC 15963 allocation class identifier at locations 00_n to 07_n. It associates the tag with the type or manufacturer of the tag. It contains information for an interrogator to uniquely identify the custom commands and optional features that a tag supports [EPCglobal, 2005].

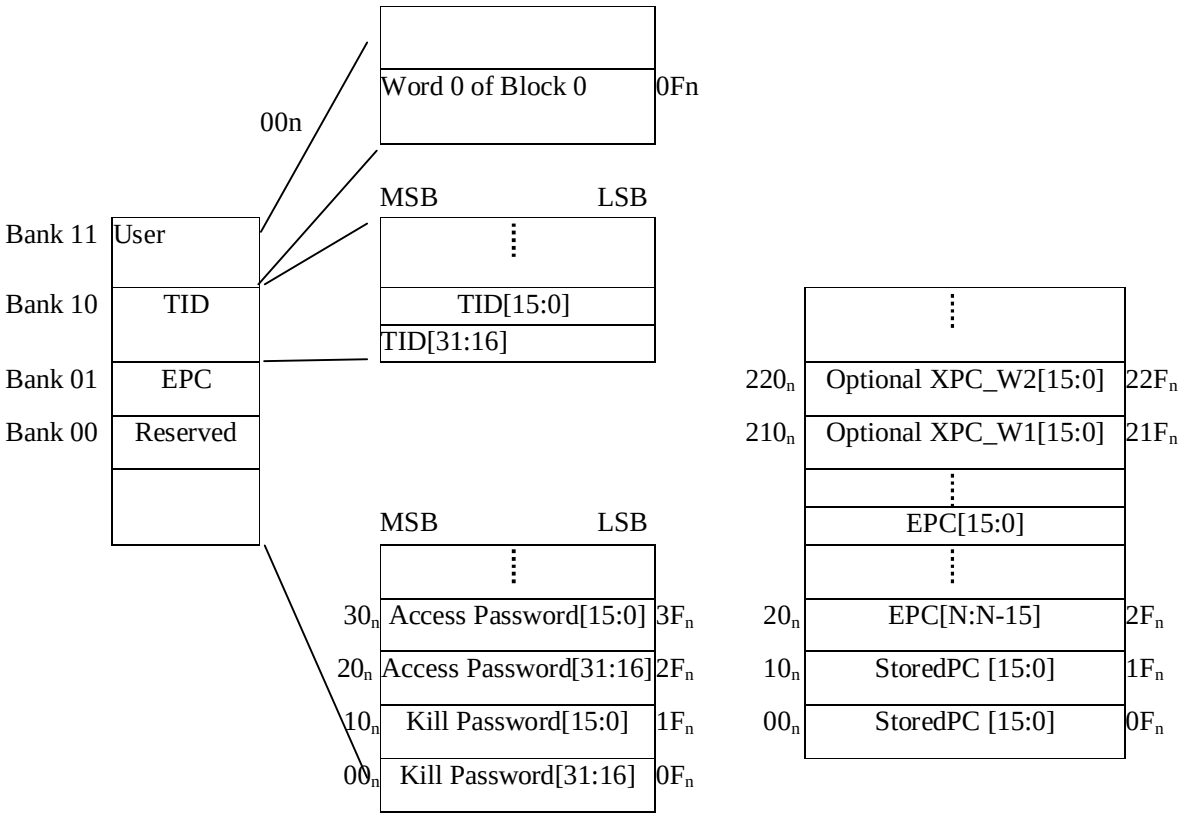

Figure 2-4: Logical Memory Map [EPCglobal, 2005]

User memory: This is user-defined data. It allows user-specific data storage. This is where read or write operations may be performed [Banks et al. 2007]. The size of the memory depends on the requirements and determined by the manufacturer.

2.5 Radio Frequency Regulations

The radio frequency (RF) spectrum used for different applications is not infinite. If multiple devices attempt to use the same frequency or frequencies close to each other, there might be an interference among them. This interference might disrupt the transmissions of all the applications. To avoid the collisions among the radio frequencies it should be regulated. Most countries have a governmental organization to regulate the radio frequency spectrum in their countries. For example in the United States the Federal Communications Commission (FCC) is responsible for RF regulation and in Europe the European Telecommunications Standards Institute oversees the RF regulation. Though the RF frequency is regulated by the countries with their own regulations but there are frequency

ranges that are widely adopted around the world. The spectrum is regulated by the frequency ranges and is sliced into thousand of regulated frequencies for different purpose [Banks et al. 2007].

To regulate the range of frequencies, restriction is imposed for who can use that range. There are rules for most regulated frequencies regarding the maximum broadcasting power in watts, the type and size of the antenna can be used. EPCglobal maintains a living document for the current RF regulations status in the UHF spectrum. Table 2-2 shows a part of the information from that document. It has five columns: "Country", "Frequency", "Power", "Technique" and "Status". The "Status" column means the current state of RF regulation in that country.

Table 2-2 Telecommunications Regulation Status for EPC-Complaint Tags

Country	Frequency	Power	Technique	Status
Australia	920-926 MHz	4W EIRP	Unknown	Agreed
Brazil	902-907.5 MHz 915-928 MHz	4W EIRP	FHSS	Agreed
Canada	902-928 MHz	4W EIRP	FHSS	Agreed
China	917-922 MHz	2W ERP	FHSS	In Progress
France	865.6-867.6 MHz	2W ERP	LBT	Agreed
Germany	865.6-867.6 MHz	2W ERP	LBT	Agreed
Italy	865.6-867.6 MHz	2W ERP	LBT	In Progress
Japan	952-954 MHz	4W EIRP	LBT	Agreed
Russian Federation	865.6-867.6 MHz	2W ERP	LBT	In Progress: LBT License Only
United Kingdom	865.6-867.6 MHz	4W EIRP	LBT	Agreed
United States	902-928 MHz	4W EIRP	FHSS	Agreed

2.6 An RFID Chip and a Barcode

An RFID chip or tag is like a wireless barcode. It contains a silicon microprocessor and an antenna usually in size and form like an ordinary adhesive label. It can be as small as a grain of sand, and can be embedded in a paper [Hitachi 2003]. An RFID tag traditionally used as a label carries no internal source of power. It is simultaneously powered and read by a radio-emitting scanner. In an ideal case, an RFID tag is readable through obstructions at a distance of up to several meters. RFID systems give a powerful advantage over the optical barcode. Barcodes require line-of-sight contact with readers. However, RFID tags do not require line-of-sight contact and can work without precise

positioning (Jules 2006). This characteristic facilitates a new dimension of automated object recognition. RFID readers can read tags at rates of hundreds per second. For instance, an RFID reader in a warehouse door can scan stacks of passing crates with high accuracy. It may eliminate the requirement of the employees at the checkout in supermarkets. Once RFID-tagging is widespread, a customer might be able to roll a shopping cart full of items by a point-of-sale scanner that would ring them up without human intervention – and automatically mediate payment as well. This vision extends to the factory and warehouse as well, where RFID could enable automated inventory-taking and ultimately even robot-guided item selection and assembly.

A barcode specifies the type of object on which it is embedded. For example "This is a pen of X brand." An RFID tag can do more than this. It transmits a unique identification number that can be distinguished from a large number of manufactured objects. For example "It is a pen of X brand, with code number 01546875734." The unique serial number in RFID tags can be used as indexes in a database having much transaction information of individual items.

2.7 Uses of RFID Technology

RFID was first used in the Second World War to detect and distinguish between the aircrafts of friend and foe. Today, RFID is used in a wide variety of applications [Garfinkel et al. 2005] and some examples are outlined as follows:

- **Proximity cards:** RFID is used as contactless card for building access.

- **Automatic toll collection:** One of the most interesting uses of RFID technology is the toll collections by highway authorities in many metropolitan areas from travellers. One example of the most popular systems is E-ZPass. It was first used widely in New York. E-ZPass is based on a 921.75 MHz semi-passive tag. The read range is several meters and it has a shelf life of about five to seven years. The tag in the moving car can be read by the reader to debit accounts. The system can read the tag in the cars moving up to 100 miles per hour. It can be further used for traffic monitoring and other applications. Several million US consumers are now using these tags nationwide [Garfinkel et al. 2005].

- **Automobile Industry:** RFID technology in automobile industry is used for various purposes. The most rapidly grown application of RFID technology is the automobile or vehicle immobilizer. RFID is also very suitable for the assembly and manufacturing process of the automobiles. In manufacturing process RFID can serve in different phases like for flexible and agile production planning, spare parts, and inventory management. It automates the whole assembly process where a significant cost reduction is achieved. It also offers improved services to the automobile users for more efficient replacement part ordering and automated generation of maintenance reminder.

- **Automobile immobilization:** In these systems, the car key contains a passive RFID tag that the steering column authenticates, thereby enabling vehicle operation. A typical antitheft system would flash the headlights and produce a sound if there any unauthorised attempt to open the car without a key [Banks et al. 2007]. The tags are usually programmed by the manufacturer as read only and cannot be altered when in use. Some tags consist of cryptographic information to communicate between the key and the sensor. Typically Immobilizers have a short read range of 5 cm and operate in the low-frequency end of the electromagnetic spectrum between 125 and 134.2 KHz, and cost a few dollars each. This is widely used to reduce auto theft by as much as 50 percent. These systems are perhaps the best-known examples of RFID application that contributes to a measurable end-user benefit [Garfinkel et al. 2005].

- **Payment systems:** RFID tags are used in credit card-like payment tokens that have a unique identification number. A reader transmits the identification number through the network and a server computer adjusted payment in the consumer's account. To protect from unauthorised users, some systems implement a simple challenge–response protocol. Texas Instrument's Speedpass pay-at-the-pump system is one of the popular examples, introduced in Mobil stations in the mid-1990s. Few years ago, the European Central Bank considered using RFID tags into currency [Garfinkel et al. 2005].

- **Animal tracking:** To enable tracking, recovery, and management organizations and individuals are increasingly providing pets, livestock, exotic animals, and endangered species with RFID tags [Garfinkel et al. 2005]. In the US, many owners are implanting RFID chips in their pets. In August 2000, the Los Angeles City Council implemented the

implantation of RFID tag to the pet animals from the city's animal shelters at a cost of US$15 per animal. The shelter has reader and database to store of all the tag information used for the pets. Using this database lost animals can be found easily by a shelter and can be returned to the owners. RFID chips are also being increasingly used into ear tags attached to cattle. Another interesting example is researchers have tracked dolphins and other marine animals using a radio transmitter combining with a GPS receiver that can be picked up by satellite.

- **Manufacturing:** Manufacturing is a very complex process. It requires that the right materials arrive at the right place at right time. It also requires that it receives the right process – and the manufacturing process itself is done correctly. Barcode, RFID and vision systems have been used in manufacturing to identify items, processes and ensure product quality since long time.

- **Security:** Access to secure areas is already being controlled through the use of variety of Automatic Identification and Data Collection (AIDC) technologies. Bar codes, RFID, and biometrics are the main technologies used for this purpose.

- **Inventory management:** RFID is being used in many sections of inventory management [Garfinkel et al. 2005]. RFID tags are being used in packaging of consumer goods at the factory. Subsequently it is being used to track packages when they are put on a truck or boat, travel in a foreign country, pass through the supply chain, distribution, and ultimately arrive at their destinations. Tags can guarantee that products manufactured and sold in one place are not mistakenly placed to another. In addition, "smart shelves" using RFID readers could incorporate with inventory systems, tracking all commodities and informing store personnel when things are misplaced. RFID tags could be used for after sale service to ensure that consumers actually bought the right items that they're trying to return or have serviced.

- **Libraries:** RFID is suitable for fast and automatic tracking of items. This feature is suitable to applications for library automation. The RFID technology is slowly replacing the barcodes on library items such as books, DVDs, CDs etc. The barcodes need line-of-sight contact to be scanned and they are easily deteriorated by use. In addition they cannot perform multiple scan at the same time. On the other hand, RFID technology permits

autonomous checkouts where the patron only passing under library's batters is identified and so are the books that are identified. The system can also automatically check if an individual can borrow the books and updates library's database.

- **Passport:** Different countries are now using RFID-enabled passports. The International Civil Aviation Organization (ICAO) has circulated specifications for RFID-enabled passports and other travel documents [ICAO 2005, Jules et al. 2005].

- **RFID in Hospital:** Healthcare is assumed to be the very big potential area for RFID implementation [Ericson 2004]. In general, the healthcare industry has been investing in the field of Information Technology (IT) to improve patient safety, to reduce operating costs and RFID is expected to become critical to healthcare organizations achieving these two goals. Some medical institutes and hospitals are starting to perform small-scale RFID experiment projects. The application of RFID in healthcare is in its child state. Healthcare industries expect that RFID can help to save costs and improve patient safety. Many of them started at first with tracking and managing their equipment. For automation RFID is being used in many hospitals [Wang et al. 2006].

In future, in a world when RFID tags will be extensively used by most of the shopping items, many remarkable things might be possible with this tag [Jules, 2006] and some possibilities are outlined as follows:

- **Smart appliances:** Nowadays RFID is being used in many shopping items like garments, package of foods and other necessary items. These tags can be further used by the home appliances more smartly. During the washing of cloths in a washing machine it might select wash cycles automatically by using the information in the RFID tag attached with the garments. It may avoid damage to delicate fabrics. Refrigerator might warn when the food has expired and there is only few remaining cartons are there. It could even transmit a shopping list automatically to a home delivery service [Jules, 2006].

- **Shopping:** RFID tag is easier to read and track than barcode. Customers could check out by rolling carts of the shop at the terminals very quickly. It would be possible that these terminals without human intervention count the items, calculate the cost, and charge the

customers' RFID-enabled payment devices. It then also possible that customers could return items using the RFID tag without receipts. Also the tags may be used as indices into database records, and help the retailers to track the pedigrees of defective items [Jules, 2006].

- **Interactive objects:** Recently mobile phones are using RFID tags to interact with different objects. Customers could interact with RFID-tagged objects through their mobile phones to perform many actions. A consumer could scan a movie poster to display show times on her phone. A consumer can also obtain information about the products by waving the phone over it [Jules, 2006].

- **Medication compliance:** In future RFID can be used to facilitate medication compliance. Research at Intel and the University of Washington [Fishkin et al. 2003] used RFID for this purpose. As researchers demonstrated that, an RFID-based medicine cabinet could be used to verify that medications are done timely. RFID assures to bring incredible benefits to hospitals [Fishkin and Lundell 2005].

2.8 Privacy Problems in RFID Application

RFID has unique privacy and security problems because people cannot understand when the tag is read by the adversary. Further the tag and the reader can be covertly embedded in the environment [Garfinkel et al. 2005]. There are various RFID applications that have various types of privacy and security problems. Some of these are outlined as follows:

- **RFID Privacy Problems in Medical Service:** In the medical scenario, privacy and security problems are vital to RFID-enabled medical application. In RFID mobile phone model, the user holds the small RFID reader implanted in the phone. Then the user can use the reader to request information from the tag attached to the patient. The reader then sends the information to the back-end database. The database then gives the requested information to the reader and displays it to user. In case of the location sensitive RFID reader, this can be used for the increased customer safety. This can also be used for negative purpose to break customer privacy [Lee and Kim 2007]. The privacy issue with tagged patient card has the threat of revealing the information, such as trace of individual location, information of

personal clinical and health history. In the standard health level seven (HL7), the standard for customizing and detailed privacy mechanism is not yet provided. HL7 is an international non-profit organization that develops international healthcare informatics interoperability standards. Lee and Kim [2007] propose a privacy mechanism for RFID in healthcare system. The authors analyzed the privacy requirements for the ubiquitous service. In order to ensure privacy in this process, a mechanism of encryptions and decryptions of the outgoing data from tag and server has been proposed. However, these methods may have limitations to give service in the ubiquitous application environment. Additionally, if the information can be decrypted successfully, all information will be available to unauthorised users. For this reason, a method is proposed by the authors that protect the privacy in the ubiquitous system using a personal privacy policy in order to administer information more flexibly and securely as well as overcome the problems discussed previously. In order to protect privacy of the patient, all of the information of the patient should be managed by privacy aware system. In addition, unique serial number in the RFID tag of the patient can be used outside of the hospital for any emergency medical service or other hospital service.

- **RFID Privacy Problems in E-passport:** E-passports are vulnerable to information leakage of their contents without the knowledge of the passport holder. The short read range of the e-passport is also not free from some threats. Clandestine readers could be placed in shops or entrances to buildings. These types of readers would enable for appropriate surveillance of e-passports. E-passport contains personal data that a passport holder does not like to disclose to an unauthorised reader. There are many security threats are identified in e-passport due to the uses of the RFID [Jules et al. 2005]. The identified security threats are clandestine scanning, clandestine tracking, skimming and cloning, eavesdropping, biometric data-leakage, cryptographic weaknesses. The details will be discussed in the application and implementation chapter 8.

- **RFID Privacy Problems in Supply Chain:** RFID enables improved inventory management, better shipping and gaining productivity, reduces levels of the safety stock, and significantly reduces inventory losses due to shrinkage [Dimitriou 2005]. However, RFID technology has also caused major security problems. An industry spying may eavesdrop RFID signals to gather inventory information; cloning of tag which may cause significant loss to supply chain partners. The inventory information has financial significant

for business organization and their competitors. As RFID based supply chains systems are becoming widespread, it is important to solve the security problems in a cost-effective approach without lessening the efficiency of supply chain management due to the introduction of RFID technology. The privacy and security in RFID technology can be classified into corporate information security threats which mainly affect corporations inside the supply chain, and personal privacy threats which mainly affects individual consumer outside the supply chain [Garfinkel et al. 2005]. The security concern in supply chain management is that the inventory of store labelled with unprotected tags may be monitored by the unauthorized readers of the business competitors [Gao et al. 2004]. Another privacy issue is that persons may be tracked by RFID tags attached on the objects carried by the persons. Also, even if the responses of tags are encrypted, the tag carrier can also be identified and tracked by the fixed encrypted code [Gao et al. 2004].

2.9 Privacy, Security and Performance Goals in RFID Systems

The privacy and security concerns are the major drawback of the RFID technology. In RFID systems various types of attacks can be identified. Attacks against the RFID systems opened the door for the construction of traditional and modern security systems, ranging from signal jamming to challenge-response based authentication. It is just as likely that RFID will continue to inspire progress in security and privacy research in the future, as it has done for decades.

This section gives an overview of the primary privacy and security requirements of RFID systems and the traditional mechanisms to fulfil those requirements. It also categorizes the existing weaknesses of RFID systems so that a better understanding of RFID attacks can be achieved.

2.9.1 Objective of the Adversary

In an RFID system the objectives of the adversary and each attack can be different. It is important to identify the potential targets in order to understand all the possible attacks. The target can be to disrupt the complete system or only a section of the entire system. Sometimes just to track any or part of the system. A large number of information systems focus solely on protecting the transmitted data. However, when designing RFID systems, additional objectives, such as tracking or data manipulation should be considered. An adversary may introduce wrong information in the

database to make it inoperative. Some attacks, such as the active jamming attack, are inherent in the wireless technology employed. Other attacks focus on eliminating physical access control, and ignore the data. Some involve identity stealing from legitimate e-passports, and etc.

2.9.2 Privacy and Security Requirements

To provide privacy and security for a system, it is essential to identify the possible threats and risks to that system. These can be used for privacy and security requirements. From this, protection measures to the threats and residual risks can be identified and applied [Aissi et al. 2006]. In this section, two main classes of threats to RFID systems privacy and security are investigated separately.

2. 9.2.1 Privacy in RFID Systems

Privacy is an important concern in RFID systems. The information transmitted between the tag and the reader can be disclosed and at least the location can be tracked by the adversary if the system is unprotected. There are two major privacy issues which are as follows:

- **Tag Information Leakage:** A person can hold different types of tags. Some of the tags could contain personal data and the private information that the tag bearer does not wish to disclose. Examples are diagnostic and health information of an individual, a title of a CD or book and expensive product etc. However, the revelation of information arising during the transmission of various personal data details without the knowledge of the tag bearer [Lee et al. 2005]. In typical RFID system, a tag is a unique identifier that transmits information to the reader. At this stage there is a chance of information leakage and to protect an RFID system there needs to provide privacy control so that unauthorized readers are unable to access the tags [Ohkubo et al. 2003].

- **Tag Tracking:** When a tag transmits any information to a reader, an adversary may try to at least distinguish it from other responses and consequently could determine the location of the user. If the signals of an RFID tag can be linked to each other or can be distinguished from those of other tags, then the tracking of a tag could be possible by the adversaries [Weis et al. 2004].

2.9.2.2 Privacy Requirements

To protect the RFID systems form the privacy attacks from various adversaries the system should meet the following privacy requirements in order to defend from the two threats outlined.

- **Tag Information Privacy:** The tag information can be extremely sensitive for some users. The RFID systems should be able to resist tag information leakage. If the information transmitted is in plaintext and is not authenticated properly there is a chance of information leakage. To protect from such a threat, the RFID systems should be designed in such a way that only the authorised users are able to get the information from a tag.

- **Tag Location Privacy:** If a tag can be tracked from its response then the location of the user can be known and can be tracked. RFID systems should be able to protect the tag from tracking attacks. If responses from tags are anonymous, then the problem of tracking the RFID tag by unauthorized users can be overcome.

2.9.3 Security in RFID Systems

The communication process between a reader and a tag is not reliable due to the possible attacks of an adversary. Communication processes between a tag and a server in an insecure wireless channel are vulnerable to eavesdropping. There are various security threats to RFID systems.

2.9.3.1 Attack Model

The possible attackers are divided into two groups, as follows.

- **Weak adversary (WA):** A weak adversary (WA) is a malicious body that can monitor and manipulate communications between a reader and a tag, but cannot compromise the targeted tag.
- **Strong adversary (SA):** A strong adversary (SA) is a malicious entity that has the ability to compromise a targeted tag, in addition to the capabilities of a weak attacker.

Threats by a strong adversary as well as a weak adversary should be considered in RFID protocol design, because the internal data in a tag memory are liable to exposure as a result of side-channel attacks [Avoine and Oechslin 2005, Lim and Kwon 2006]. These attacks are based on side channel information that can be obtained from a system carrying out cryptographic computations [Bar-El 2002]. Side channels give information on internal computations through measurement, for example by monitoring variations of power consumption, time taken to perform calculations, or from external radiation. Side channel attacks use such information to capture the secret key the system is using [Bar-El 2002]. Security threats to RFID systems can be classified into weak and strong attacks in line with the adversary types.

2.9.3.2 Weak Attacks

There are various attacks that can be classified as weak attacks. The following attacks are some of the weak attacks [Avoine, G 2005, Jules 2006, Weis et al. 2004].

- **Tag Impersonation**: In this attack an adversary without knowing the secrets could impersonate a target tag to a server. It could also communicate with the server rather than the tag and be authenticated as the valid tag [Weis et al. 2004].

- **Cloning:** To detect counterfeit products in RFID application is very important. An adversary can counterfeit a tag to imitate the tag similar to any tag of a valuable item. In order to avoid counterfeiting, RFID tags should be protected from cloning. An adversary can clone a valid tag if it knows the secret value of the tag and its authorized reader [Dimitriou 2005, Duc et al. 2006].

- **Replay attack**: An adversary could replay data exchanged between a tag and a server without being detected, thus accomplishing a successful authentication between a server and a tag [Dimitriou 2005].

- **Man-in-the-Middle** (MitM) attack: An adversary could interfere with the communications transmitted between a tag and a server [Jules 2004].

- **Denial-of-Service (DoS) attack**: An adversary could block the transmission of messages between a tag and a server. This attack could cause the server and the tag to lose synchronisation. An example of DoS attack is that, the server updates its secret values but the tag does not; thus, they would not be able to authenticate each other anymore [Weis et al. 2004].

2.9.3.3 Strong Attacks

There are various attacks that can be classified as strong attacks. A strong adversary may be able to perform both the strong attacks and weak attacks. The following attacks are some of the strong attacks [Avoine, G 2005, Lim and Kwon 2006, Ohkubo et al. 2003].

- **Backward Traceability**: If the internal state of the tag is known then it can help to identify the tag interactions of past communications of the tag. An adversary may trace past transactions between a server and a compromised tag using the known internal state. The past information of a tag may permit tracking of the tag user's past behaviour [Ohkubo et al. 2003].

- **Forward Traceability**: If the internal state of the tag is known then it can help to identify the tag interactions of future communications. An adversary might be able to trace future transactions between a server and a compromised tag using knowledge of the internal state of the tag [Lim and Kwon 2006].

- **Server Impersonation**: In this attack if an adversary knows the internal state it might be able to impersonate a valid server to a tag using this state of the tag. If the adversary could impersonate a server to a tag, it could request the tag for its secrets and to update the secrets. Then the real server and the tag would be desynchronised, and unable of doing successful communications [Song 2008].

2.9.3.4 Security Requirements

The security requirements are identified for RFID systems to protect from the threats of the weak and strong adversary. These are the security goals that should be guaranteed by protocols.

- **Resistance to Tag Impersonation:** Without knowing the internal secrets of the tag an adversary could impersonate the tag to a server. The RFID systems should be designed in such away that without knowing the secret of a tag an adversary should not be able to impersonate a tag.

- **Resistance to Replay attack:** Security must be ensured against replay attacks so that an adversary should not be able to use the information exchanged between a tag and a server, thus accomplishing a successful authentication between the server and the tag.

- **Anti-cloning:** It is important to detect counterfeit objects in RFID systems. To avoid counterfeiting, RFID tags should be unalienable. If an adversary knows the shared secret key of the tag and the authorized reader it can clone the tag. So, to protect the system form cloning attack, protocols should not disclose the secret key.

- **Resistance to MitM attack:** An adversary could intrude into the messages exchanged between a server and a tag to intercept the exchanged data and inject false information. An adversary should not be able to manipulate messages and inject false information sent between a server and a tag without compromising a tag.

- **Resistance to DoS attack:** In DoS attack an authorized entity is prevented from accessing the authorized resources. Blocking of transmitted messages between a tag and a server should not cause the server and the tag unable to communicate successfully. In order to ensure successful communication between a reader and its authorized tags, it should be guaranteed that an adversary cannot desynchronize them.

- **Backward Un-traceability:** The communication between the server and the tag should be backward untraceable. An adversary should not be able to trace past transactions between a server and a tag, even if it compromises the tag.

- **Forward Un-traceability:** The communication between the server and the tag should be forward untraceable. An adversary should not be able to trace future transactions between a server and a tag, even if it compromises the tag.

- **Resistance to Server Impersonation:** If an adversary could compromise a tag using the knowledge of the internal state it might be able to impersonate a legitimate server to the tag and could request a tag for its secrets to update its shared secrets. An adversary should not be able to impersonate a server to a tag, even if it compromises that tag.

2.9.4 Performance Requirements

An RFID tag is a tiny and extremely low-cost apparatus containing a microchip with very limited functionality and some data storage with antenna for wireless communication with readers. It cannot use complex cryptographic algorithms that require powerful processing capability to provide privacy and security because tight tag cost requirements put limits on the resources in tag-side.

RFID schemes should consider the following performance issues.

- **Storage Capacity:** The tag has a very limited storage capacity. So the volume of data stored in a tag should be minimised because of tight tag cost requirements [Weis et al. 2004].

- **Computation:** The processing capability of a tag is also very limited. Due to the limited power of the tag the complexity of tag computations should be minimised [Weis et al. 2004].

- **Communication:** The bandwidth of the tag is also limited. The volume of data that each tag can transmit per second is also limited. So the number and size of messages exchanged between a tag and a reader should be minimised [Weis et al. 2004].

- **Scalability:** The server should be able to handle increasing amounts of data for a large amount of tags. It should have the capability to handle a large number of tags. It should also be able to identify multiple tags using the same radio channel [Avoine and Oechslin 2005].

2.10 Security and Cryptographic Techniques

2.10.1 Security

This chapter introduces general communications security and cryptographic primitives. It contains the basic concepts of computer security and categories of cryptography.
The computer security means the protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and useful to its valid users. Computer security can be defined in the following ways:

- **Confidentiality:** Confidentiality is a service that prevents the access of information to the unauthorized systems or users. There are many ways of ensuring confidentiality. Confidentiality can be explained in two ways [Stallings 2011]

    - Data confidentiality: It assures that private or confidential information is not disclosed to unauthorized users.
    - Privacy: It assures that individuals can control or influence the information related to them and also can control the system so that information should be revealed only to authorised users. It should have the ability of an individual or group to conceal them and expose them selectively.

- **Integrity:** Integrity means that data cannot be modified by unauthorized users or it cannot be changed undetectably. To ensure data integrity in an unreliable channel, it is essential to detect data manipulation by unauthorised users. Various types of data manipulations are insertion, deletion and substitution. Integrity may be two types [Stallings 2011]
    - Data Integrity: Data integrity assures that information and programs are changed only in a specified and authorized manner.
    - System Integrity: System integrity means a system should perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

- **Availability:** This means the resources should be available for the authorized users. It should work promptly and service is not denied to authorize users.

- **Authenticity:** Authenticity means the genuineness of the origin and being able to be verified and trusted. This also ensures confidence in the validity of a transmission, a message, or message originator.

- **Non-repudiation:** Non-repudiation is a service which prevents either sender or receiver from denying a transmitted message. When the message is received from the sender, the receiver can prove that the alleged sender in fact has sent it. Similarly when any acknowledgement is sent back to the sender, the sender can verify that the alleged receiver in fact received the message.

- **Access control:** Access control provides protection against unauthorised use of resources. It can protect the use of a communications resource: the reading, writing, or deletion of an information resource; or the execution of a processing resource [Stallings 2011].

2.10.2 Introduction to Cryptography

Cryptography is the technique of hiding information and combines the disciplines of mathematics, computer science, and electrical engineering. The many schemes used for encryption constitute the area of study of cryptology. Such a scheme is known as cipher. Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted information without the knowledge of the key and the process normally required. The areas of cryptography and cryptanalysis together are called cryptology. Modern cryptographic techniques can be divided into two main classes, symmetric and asymmetric techniques, depending on the nature of the keys used [Menezes et al. 1996, Mitchell 2003 and Stinson 2002]. Some cryptographic data integrity algorithms are also used for data security. For example, cryptographic hash functions, message authentication codes and digital signatures are the most popular algorithms among them.

2.10.2.1 Symmetric Cipher Model

Symmetric encryption method is a form of cryptosystem in which the sender and the receiver share the same key [Stallings 2011] and it has five elements as shown in Figure 2-5.

- **Plaintext (*X*):** This is the original information used as input into the encryption algorithm.

- **Encryption algorithm (*E*):** The encryption algorithm carry outs various substitution and transformation on the plaintext.

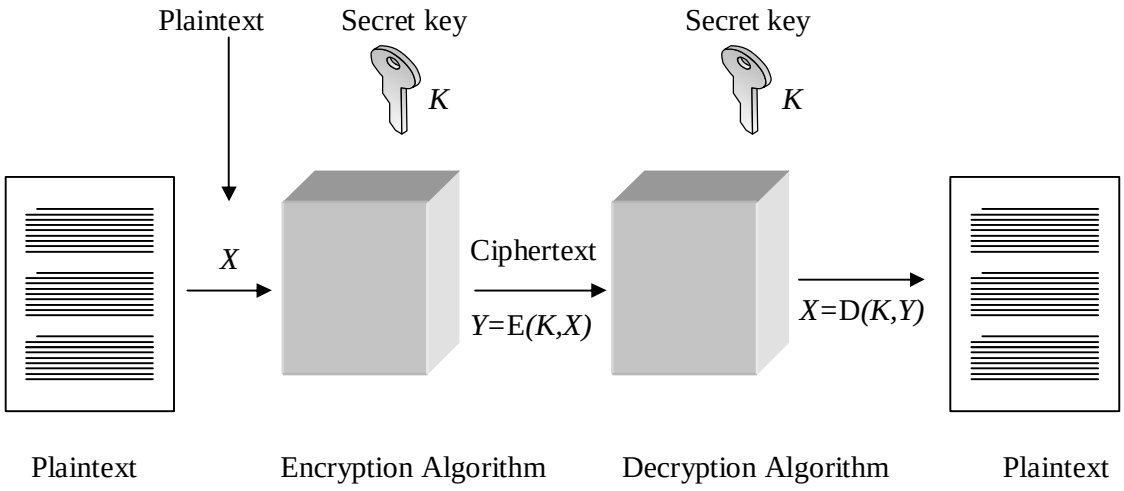

Figure 2-5: Symmetric Encryption

- **Secret key (*K*):** The secret key is a value independent of the plaintext and the algorithm. The algorithm will produce different output for specific key being used at the time.

- **Ciphertext (*Y*):** This is the scrambled unintelligible message produced as output. It depends on the plaintext and the secret key. For a given plaintext two different keys will produce two different ciphertexts.

- **Decryption algorithm (*D*):** Decryption algorithm is the encryption algorithm run in the reverse order. It produces the original plaintext from the ciphertext and the secret key.

2.10.2.2 Asymmetric (Public-Key) Cryptography

In asymmetric-key cryptography two different but mathematically related keys are used for encryption and decryption as shown in Figure 2-6. The two keys used for asymmetric encryption are referred to as the public key and the private key. It is also known as public-key encryption. A public-key encryption has six elements

- **Plaintext (*X*):** This is the original information used as input into the encryption algorithm.

- **Encryption algorithm (*E*):** The encryption algorithm carry outs various substitution and transformation on the plaintext.
- **Public (PU_a) and Private (PR_a) key:** This is the pair of keys used for complementary operations. If one is used for encryption then the other is used for decryption. The transformations done in the algorithm depend on the public key and private key that is given as input.
- **Ciphertext (*Y*):** This is the scrambled unintelligible message produced as output. It depends on the plaintext and the secret key. For a given plaintext two different keys will produce two different ciphertexts.
- **Decryption algorithm (D):** Decryption algorithm is the encryption algorithm run in the reverse order. It produces the original plaintext from the ciphertext and the secret key.

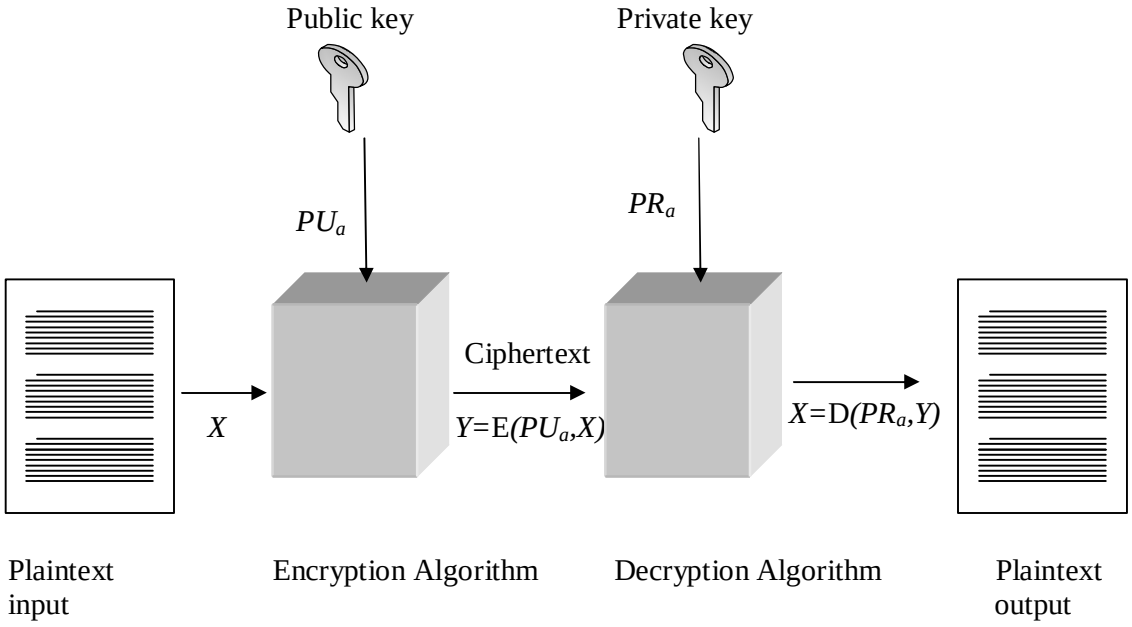

Figure 2-6: Asymmetric Encryption

2.10.3 Other Security Algorithms

There are many other cryptographic security algorithms in the literature. The most well known algorithms will be discussed in this section since the entire region is beyond the scope of this research. Traditional cryptographic algorithms are highly computation and storage intensive which are not suitable for low-cost RFID tags. Some of the examples of traditional cryptographic examples are Data Encryption Standard (DES), Advanced Encryption Standard (AES) etc.

2.10.3.1 Cryptographic Hash Function

A hash function maps a variable-length input message into a fixed-length output message. A hash function takes an arbitrary data as input string and gives a short, fixed-length value as output. The output is known as a hash value or hash code. Any change to the input data will also change the hash value. Hash functions have the one-way property, that is, it is not computationally feasible to find an input string from the output. They must be simple and efficient to compute [Menezes et al. 1996, Mitchell 2003 and Stinson 2002]. For example, $h:\{0,1\}^* \rightarrow \{0,1\}^l$ be a one-way hash function where a hash value space belongs to $\{0,1\}^l$.

It is assumed that a cryptographic hash function is able to withstand all known types of cryptanalytic attack. The basic requirements for a cryptographic hash function are as follows:

- **Preimage resistance:** Given a hash output *y* it is infeasible to find any message *x* such that $h(x) = y$. This is the one-way property of a hash function.

- **Second preimage resistance:** Given an input x_1 it should be difficult to find another input x_2 where $x_1 \neq x_2$ such that $h(x_1) = h(x_2)$. This property is known as weak collision resistance

- **Collision resistance:** It is infeasible to find two different messages x_1 and x_2 such that $h(x_1) = h(x_2)$. This property is known as strong collision resistance.

2.10.3.2 Message Authentication Codes

A Message Authentication Code (MAC) is a short piece of information used to authenticate a message. A MAC algorithm is a cryptographic function that takes a message and a secret key as input, and produces an authentication called a MAC code. The recipient of a MAC equipped with the correct secret key, can re-generate the authentication code to verify the integrity of the message [Menezes et al. 1996, Mitchell 2003 and Stinson 2002]. The MAC value protects both a message's data integrity as well as its authenticity, by allowing the recipients to detect any changes to the message content.

A MAC algorithm is a family of functions *f* parameterised by a secret key *k*, with the following properties [Menezes et al. 1996]:

- **Ease of computation:** For a given a secret value *k* and an input *x*, it is easy to compute the MAC $f_k(x)$.
- **Compression:** The function *f* maps an input string *x* of arbitrary finite length to an output $f_k(x)$ of fixed length *l*.
- **Forgery-resistance:** For a given sequence of text-MAC pairs $(x_1, f_k(x_1))$ for a fixed key *k*, it is computationally infeasible to compute a text-MAC pair $(x_2, f_2(x_2))$ for any $x_1 = x_2$.

2.10.3.3 Pseudorandom Number Generator

A Pseudorandom Number Generator (PRNG) is an algorithm for generating a sequence of unpredictable numbers that approximates the properties of random numbers. PRNGs are used in variety of cryptographic and security applications. The basic requirement when PRNG is used in cryptographic application is that an adversary who does not know the seed cannot determine the pseudorandom string. If the pseudorandom bit stream is used in a stream cipher, then the knowledge of the pseudorandom bit stream would enable the adversary to recover the plaintext from the ciphertext. The general requirements for secrecy of the output of a PRNG are randomness, unpredictability and the characteristics of the seed [Stallings 2011].

- **Randomness:** The requirement of a PRNG is that the generated bit streams appear random even though is deterministic. If the PRNG shows randomness on the basis of multiple tests it will be accepted that it satisfies the requirements of randomness.

- **Unpredictability:** Pseudorandom numbers should show two types of unpredictability – forward unpredictability and backward unpredictability. In forward unpredictability if the seed is unknown the next output bit in the sequence should be unpredictable though the previous bits in the sequence are known. In backward unpredictability it should not be feasible to determine the seed from knowledge of any generated values.

- **Seed requirements:** The PRNG is a deterministic algorithm. This is why in the cryptographic applications the seed of the PRNG needs to be secured. Otherwise, if the adversary can obtain the seed, the output can be determined.

2.11 Conclusions

This chapter gives a review of RFID systems and also discusses the components of RFID systems including the readers, tags and a backend database. RFID systems use radio transmission to communicate, recognize, categorize, locate and track objects. The low-cost tags are attached to the products and can be scanned when these enter the read range of a reader. This chapter also discusses the classification of RFID tags. It outlined RFID standards and the details of different types of EPC classes.

This chapter discusses some application and advantages of RFID systems compared to bar code systems. RFID gives many advantages over the optical barcode. Barcodes require line-of-sight contact with readers. In contrast, RFID tags are readable without line-of-sight contact and without precise positioning. RFID readers can scan tags at rates of hundreds per second. A barcode indicates the type of object on which it is used. An RFID tag emits a unique serial number that distinguishes among many millions of identically manufactured objects. However in RFID systems there are issues regarding privacy and security. The information in these systems is vulnerable to various attacks. This chapter also presented these types of attacks and indicated the security requirements of RFID systems.

This chapter further discusses general cryptographic techniques that are used in network communication and information systems security. Modern cryptographic techniques are divided into two main classes, symmetric and asymmetric techniques. Some cryptographic data integrity algorithms such as cryptographic hash functions, message authentication codes and digital signatures are also discussed for data security.

Chapter 3 Existing RFID Privacy and Security Protocols

3.1 Background of Privacy and Security Protocols

This chapter introduces the existing RFID privacy and security systems and protocols. It also identifies the privacy and security problems of the protocols. There are several attacks in RFID systems that can break the privacy and security of the users carrying the RFID tag. Günther and Spiekermann [2005] conducted research in Germany and found consumers distrust at RFID system implemented to shopping item because of concerns about their privacy. However, researchers have been working for long time to prevent those attacks in RFID systems and to facilitate the expansion of RFID technology. One key research area that focuses on securing RFID systems against major attacks is to design secure authentication techniques. These authentication techniques are designed to execute while a reader communicates with an RFID tag for identification purpose. One extension of RFID tag authentication is known as tag searching. Tag searching means searching for an RFID tag from a large collection of tags. Any RFID authentication protocol which provides security and privacy can be used for this purpose. However, as the number of RFID tags increases, the cost of collecting data can be high. Consequently, more efficient methods for performing RFID tag search are needed. As this is a basic and invaluable tool for sifting through large amounts of data. Though RFID tag searching is an important issue for most RFID systems, the assortment of research literature on RFID searching is inadequate. Therefore, the purpose of this chapter is to discuss some famous authentication techniques along with the proposed search protocols that are currently available.

Many researchers have discussed efficient algorithms and protocols for RFID system authentication. Sharma et al. [2003] pointed out about the resource constrained in an RFID tag as a major challenge in providing privacy and security. There are various types of RFID authentication protocols for the privacy and security of RFID systems. These protocols can be mostly categorized in two ways. Firstly is the hash function based security protocol and secondly is the lightweight XOR based security protocol. There are also few other types of privacy and security protocol for

RFID system but could not attract the attention of the researchers substantially due to the large storage and computation requirements.

There are various ways to protect the privacy and security of the RFID tag and systems. The first approach towards the privacy and security of the RFID tag is the physical approach (Section 3.2) such as kill the tag at the point of sale or using Faraday cage etc to protect the tag physically [Jules et al. 2003]. The second approach in securing RFID systems against major attacks are to use secure various authentication protocols (Section 3.3). These authentication techniques are designed to execute while a reader communicates with an RFID tag for identification purpose.

3.2 Physical Approach

This is the most straight forward approach for the protection of the privacy and security of the users. The physical approaches are Killing and Sleeping (temporary inactive) [Jules 2006], Faraday Cage and Blocker Tag approaches. The approaches are outlined as follows:

3.2.1 Killing and Sleeping

EPC tags address consumer privacy with a simple as well as destructive approach called Tag "killing." When an EPC tag receives a special "kill" command from a reader, it permanently disables itself. To prevent killing tag by unauthorised users the kill command is protected by a PIN code. The PIN is 32 bits long in the EPC Class-1 Gen-2 standard. To kill a tag, a reader must also transmit a tag-specific PIN. As killed tags cannot be activated, it is a highly effective privacy measure. It is expected that once RFID tags become widespread on the items of retailer shop, the devices at point-of-sale would kill the tags on sold items to protect customer privacy. Killing tags protects consumer privacy effectively, but it removes all the benefits of the consumer of post-purchase of RFID. In some cases, such as libraries and rental shops, RFID tags cannot be killed because they must survive over the lifetime of the objects they track. So, it is essential to look at approaches other than killing for more reasonable solutions to consumer privacy.

A related approach to kill a tag, suggested by EPCglobal [2005], is to make RFID tags easily visible and removable to the consumer. For example, Marks and Spencer incorporated RFID into price tags rather than directly into the garments [Collins 2004]. However, this method has the similar disadvantage as the killing of tags. It eliminates the benefits of consumer and the process of tag

removal from the garments invites additional disadvantage of inconvenience. The drawbacks include smart appliances and other useful systems will not work with deactivated tags.

Another approach is to put the tag into sleep mode rather than killing at the point of sale, making them only temporarily inactive and then waking them when they are ready for home use [Jules 2006]. This idea is simple, but would be difficult to handle in practice. It is apparent that, sleeping tags would offer no true privacy protection if any reader could wake them after the sleep duration. Therefore, some form of access control would be required for the waking of tags. This access control might be similar to the tag specific PINs those used for the killing of the RFID tag. To wake a tag from sleeping, a reader could use this PIN.

3.2.2 Faraday Cage

An RFID tag may be protected from the radio signal using a physical approach called Faraday Cage [Jules et al. 2003]. It is a container made up of metal foil that is not penetrable by wireless signals of some specified frequencies. A State of California agency currently implemented this approach by using mylar bags to protect toll-payment transponders from reading when not in use. They offered a way to opt out of state-initiated programs that use such transponders to monitor traffic patterns. However, Faraday cages have limitations in utility since all the useful items cannot be kept inside a Faraday cage for example a wrist-watch. They not only stop reading of RFID tags on privately owned items, but also serve in assisting in-store theft. For this reason, retail shops are not interested to support their extensive use. Faraday cages are likely to be of little use if RFID tags are implanted in a wide range of personal items, such as cloths [Shim 2003]. Faraday cages can be used at best as a very partial solution to consumer privacy.

3.2.3 Blocker Tag

Juels et al. [2003] propose a privacy-protecting scheme called blocking. To protect privacy in a tag it uses a privacy bit. The privacy bit is a modifiable bit into tags can be either ‘0’ or ‘1’. A ‘0’ privacy bit marks a tag to show unrestricted for public scanning; a ‘1’ bit marks a tag to represent it as a private. A blocker tag provides a physical region of privacy protection so that a reader is unable of singulating tags in a scenario of a consumer carrying a tag e.g. purchased item etc. A blocker tag

is a special RFID tag that prevents unwanted scanning of tags by mapping it into the privacy zone. Jules et al. [2003] refer to the part of identifiers with leading '1' bits as a privacy zone.

3.3 Authentication Protocols

Many researchers have proposed authentication protocols for RFID system. This chapter outlines the most well known authentication protocols and these are classified according to the encryption method used. Many works are done using hash function. The advantages of hash function are it is low cost and it has one-way property that makes it secure [Henrici and Muller 2004, Ha et al. 2007]. A hash function using random numbers in tag side and database side can make the protocol anonymous and intractable. Some protocols also use timestamp instead of a random number. Since hash function requires complex calculations many researchers proposed protocols using light-weight xor encryption. Hash-based protocols are further classified according to the nature of the update policy of the identifier and secret after each authentication session. The approaches are hash-based protocols using varying identifier and hash-based protocol using static identifier. The advantages of hash-based protocols using varying identifier are the tracking of the identifier is not possible since it changes in each session [Henrici and Muller 2004]. It ensures the privacy and security of the RFID system effectively. The disadvantage of this approach is that it requires updating of the system that may not be suitable in ubiquitous computing environment. In hash-based protocol using static identifier the identifier is not changed in each authentication process. It is suitable for ubiquitous computing. The classifications of the protocols are as follows:

1. Hash-based protocols using Varying Identifiers (Section 3.3.1)
2. Hash-based Protocols using Static identifiers (Section 3.3.2)
3. Light-weight encryption protocols (Section 3.3.3)

The most well known security protocols are discussed in this Chapter. Some of the protocols are introduced in short to outline the evolution of the research but further details are listed in the Appendix A number 1 to 8 for brevity.

3.3.1 Hash-based Protocols using Varying Identifiers

To protect the privacy and security of the RFID systems efficiently many researchers use the varying identifier approach [Henrici and Muller 2004, Lee et al. 2005]. In his approach the identifier and secret value are updated after each successful authentication protocol. The update process is done in both the tag side and the database side. This ensures synchronization of the information in a distributed environment [Henrici and Muller 2004]. In this approach hash function also uses random number to make the response anonymous [Lee et al. 2005]. However, this approach is less suitable for the ubiquitous environment since it requires synchronization after each session. Some of the most well known protocols with hash-based varying identifiers are discussed as follows:

3.3.1.1 Hash-based ID Variation

Henrici and Muller [2004] proposed a hash-based ID variation scheme (HIDV) using one way hash function to enhance location privacy by changing the ID after each session. The notations are given as follows:

"DB-ID" Database-identifier
"ID" Current ID
"HID" Hash of ID acting as a primary index of the table
"TID" Transaction number
"LST" Last successful transaction number
$\Delta TID = TID - LST$
"AE" Associated DB entry
"DATA" A reference to tag data / user data

It implements all the three main tasks: identification, authentication, and identifier modification. Each tag stores 4 fields:

The tag identifier *ID*,
The database identifier DB-ID,
Transaction or session number *TID*
Last successful transaction number LST.

The backend database stores two records for each tag. Each record in the database needs to contain a table with the following entries:

Hash of current identifier HID, acting as primary index of the table

Current identifier ID

Transaction or session number TID

Last successful transaction number LST

Associated database entry AE

A reference to tag data / user data DATA

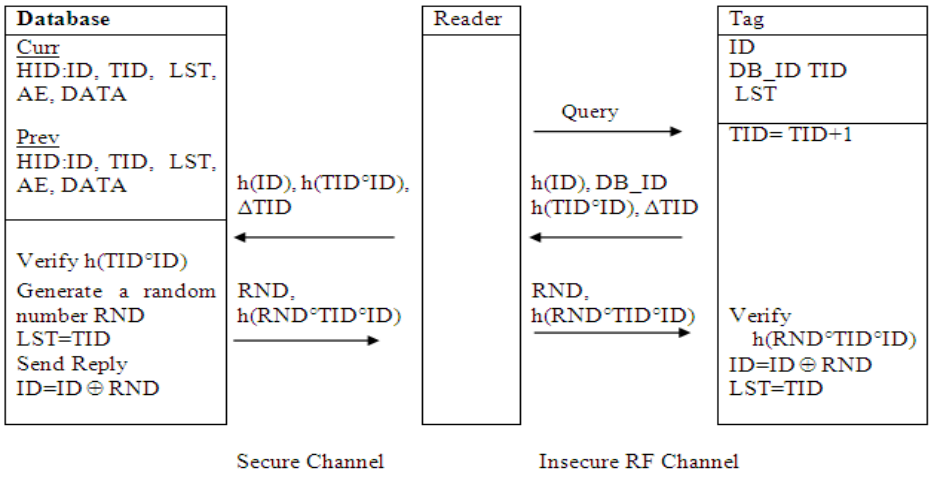

Figure 3-1: Hash-based ID variation protocol [Henrici and Muller 2004]

Initially, the fields in the tag and the backend database are in synchronized and TID (Tag Identification) is equal to LST. The protocol operates as shown in Figure 3-1. The reader starts the authentication process by sending a request to the tag. After receiving the request, the tag increases its current session number TID by one and calculates ΔTID =TID- LST. Then the tag replies with the hashed identifier HID = h(ID), a hash value h(TID o ID) for authenticating the tag, and the calculated ΔTID to give the backend database a hint for calculating TID. Here 'o' is a conjunction operation for example, XOR. Using the received h(ID), the backend database can identify the tag. Using ΔTID and the LST from the database record, the current session number TID of the tag (TID^*) can be recovered. If the TID^* is not current or the received hash value $h(TID^*$ o ID) is wrong, the message is discarded.

If everything is fine the current TID* is stored as TID in the record row. Now a random number "RND" is generated and a new ID (ID*) is updated by ID* =RND o ID and HID is updated by (ID*). The TID of the newly selected row is updated to the TID* value, its last successful transaction ID (LST) gets the same value. Using the random number a reply message h(RND o TID* o ID) is created and is sent to the reader which forwards the message to the tag.

The tag receives the reply from the reader and verifies it. If it is not matched the message is discarded. Otherwise the tag updates its ID to the value RND o ID and sets its last successful transaction number (LST) to the TID value.

In this scheme a tag always replies with the same hashed ID before the next successful authentication and allows a degree of tag tracking [Chien and Chen 2007]. This protocol does not provide backward untraceability because a strong attacker could compute the identifiers used in previous sessions by combining the server's random number and the current identifier [Song 2008].

3.3.1.2 Hash Chain Approach

Ohkubo et al.[2003] proposed a tag identification scheme by modification after each query using hash chains and is referred to OSK (Ohkubo, Suzuki and Kinoshita) protocol. The hash chain approach does not provide authentication because the protocol does not prevent the replay of messages. Each tag has an identifier *ID* that is never revealed to the reader. The hash value *g(ID)* is used for identification. The identifier update is not triggered by the backend entity. The tag modifies the identifier itself without any interaction with the reader and Figure 3-2 shows the complete protocol.

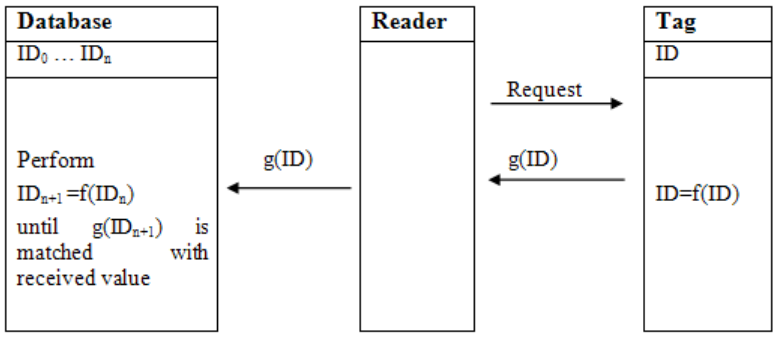

Figure 3-2: Hash Chain Protocol

The tag is initialized with the *ID* and the backend database is initialized with the ID_0 of the tag. The steps of this protocol are given below:

1. After receiving a query from the reader side, the RFID tag replies with a hash response $g(ID)$ and identifier *ID* of the tag by using the function *f*. This guarantees that the tag will provide a new refreshed identifier at the next session.
2. The back-end database tries to identify the tag using the received $g(ID)$. Therefore, the back-end database needs to repeatedly use the function *f* to all ID_0 until $g(ID_{n+1})$ matches the *g(ID)* or a last record is reached. The back-end database does not need to send a reply to the tag.

The function f has a uniformly distributed output and the one-way property of a cryptographic hash function. The scheme gives forward secrecy and therefore if an *ID* is exposed to an adversary at any time, they cannot acquire the previous tag *ID*.

From a security point of view, the approach has some good characteristics. It is also efficient since the tags only require a single variable and only need to perform a single hash calculation. The main drawback of the hash chain scheme is that the backend database requires many hash operations to all the stored tag identifiers to identify a tag. The reason is that if the tag and the database lose synchronization because of unsuccessful identification or update process the database does not know the expected value.

If the number of iterations in the back-end database is kept limited, an adversary can leave a tag unidentifiable by sufficient repeated queries. If no limit is applied, an attacker can run a denial-of-service attack against the back-end database by introducing an invalid tag *ID* into the RFID system. A solution is to incorporate a limit of iterations that a tag performs before it starts with the initial ID_0. In this case the identifiers repeat. This could be misused by an adversary for unwanted identification and tracking. However, the protocol is not scalable since many hash operations are needed to identify a tag. The complexity is expressed as $O(n^2)$, whereby n is the number of tags known to the back-end database. Although the protocol cannot be used in real life, it is a good conceptual base for developing other new protocols.

3.3.1.3 Triggered Hash Chains

In Triggered Hash Chains (THC) the Hash-based *ID* variation and the Hash chain approach are used to take the advantages of the both the protocols [Henrici and Muller 2008]. That means the scheme has the same desirable properties as hash-based *ID* variation like the ability for performing authentication without the inelegant ΔTID and the resulting issue by using the hash chain concept. To achieve this, an update of the inner tag state is done using a hash function similar to the hash chain approach. However, an update is not performed on each tag query as in hash chain approach. Update is performed only when it is triggered by the backend database. Figure 3-3 shows the complete Triggered Hash Chains protocol.

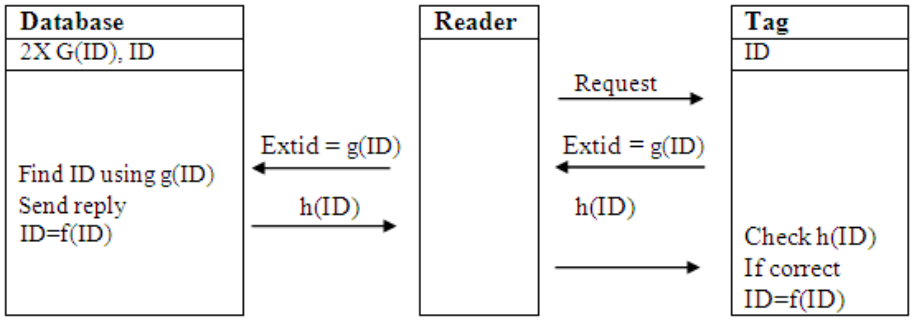

Figure 3-3: Triggered Hash Chains Protocol

Each tag has an identifier *ID* that is never revealed to the reader. The current tag identifier is calculated by using the hash function by Extid = g(*ID*). The backend entity knows the inner state of the tag and can also calculate g(*ID*) and identify the tag successfully. The inner state ID is updated by a hash function *f*. The update is not performed unless the tag receives a message that contains the hash value *h*(*ID*), whereby *h* is another hash function. The steps in the protocol are as follows:

1. After receiving a query, the tag sends $g(ID)$ to the back-end database.
2. The back-end database can recognize the tag and get the current inner state *ID* of the tag.
3. The back-end database computes *Updauth* = *h(*ID*)* using the hash function *h* and sends the result to the tag via the reader.
4. The tag computes *h*(*ID*). If the computed result and the received message match, the inner state of the tag is updated by computing $ID \leftarrow f(ID)$. Otherwise, the received response is rejected by the tag.

The backend database keeps two records for each tag. If an updates message is lost, the backend database can still identify the tag using the old tag identifier.

3.3.1.4 Low-cost Authentication Protocol

Low-cost Authentication Protocol (LCAP) simplifies and enhanced HIDV scheme in both efficiency and security [Lee et al. 2005]. The scheme uses one way hash function to protect the privacy and security of the tag. Figure 3-4 shows the LCAP protocol. The notations and symbols used in LCAP operation are as follows [Lee et al. 2005]:

$h : \{0, 1\}^* \rightarrow \{0, 1\}^l$ is a one-way hash function

ID: *ID* denotes identity of a tag and is a random value in $\{0, 1\}^l$.

HaID: HaID value is the hash value of *ID* used for identifying or addressing the tag.

TD: *TD*-entry is used to trace previous data information of a tag when loss of message occurs in the current session.

DATA: *DATA* stores the information about an accessible tag.

Data fields of a tag and a reader are initialized to the following values:

Tag: The data field of a tag is initialized to its own *ID*.

Reader: A reader picks uniformly a random number *r* in $\{0, 1\}^l$.

The data fields of a back-end database are initialized to *HaID, ID, TD* and *DATA*.

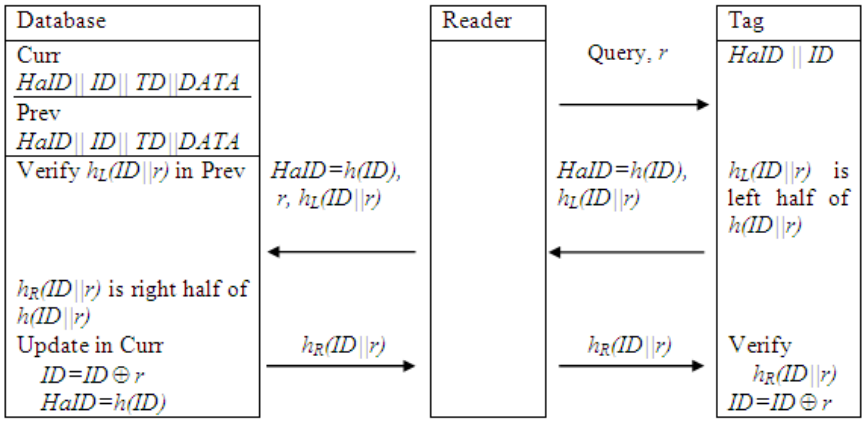

Figure 3-4: LCAP protocol

The back-end database keeps two rows; Prev is for the previous session and Curr is for the current session. Each row consists of *HaID, ID, TD,* and *DATA* fields. The back-end database stores *HaID* and *ID* in the previous session in Prev. In Curr rows, it updates the *HaID* and *ID* of Prev. *TD*-field of the Curr rows has *HaID* value of Prev rows and *TD*-field of Prev rows contains *HaID*-value of Curr rows.

LCAP works as follows:

1. A reader selects a random number r and sends a request and r to the tag.
2. The tag computes $HaID=h(ID)$ and $h(ID||r)$ using r and its ID and sends $h_L(ID||r)$ and *HaID* to the reader, where $h_L(ID||r)$ is the left half of $h(ID||r)$.
3. The reader sends $h_L(ID||r)$, r, and *HaID* to the back-end database.
4. The back-end database then compares if the value of *HaID* in Prev is same as the value of *HaID* received from the reader. If successful, the back-end database calculates $h_R(ID||r)$ using the random number r obtained from the reader and *ID* in Prev, where $h_R(ID||r)$ is the right half of $h(ID||r)$. The back-end database computes and stores $HaID=h(ID\oplus r)$ and $ID=ID\oplus r$ in Curr for next session. *TD*-field of Prev is updated with current $HaID=h(ID\oplus r)$. At last the back-end database sends $h_R(ID||r)$ to the reader.
5. The reader then sends $h_R(ID||r)$ to the tag.
6. The tag checks $h_R(ID||r)$. If it matches, the tag updates its ID to $ID\oplus r$.

It also has the similar problem as in HIDV that a tag always replies with the same hashed *ID* before the next successful authentication which allows tag tracking [Morshed et al. 2010].

3.3.1.5 Song and Mitchell (SM) Mutual Authentication Process

Song and Mitchell [2008] proposed a mutual authentication protocol using varying identifier with hash functions. The protocol is designed for the tags that can generate random strings and perform a hash function and a keyed hash function (for further details Appendix A).

This protocol is claimed to design to have the most security properties in the literature [song 2008]. However, Cai et al. [2009] discovered that the mutual authentication protocol is vulnerable to both

tag impersonation attack and reader impersonation attack. This enables an adversary to impersonate any legitimate reader or tag.

3.3.1.6 The Duc-Park-Lee-Kim (DPLK) Protocol

Duc et al. [2006] proposed an authentication protocol DPLK for EPCglobal Class-1 Gen-2 RFID tags (for further details Appendix A).

The protocol cannot prevent the system from replay attacks until the next successful authentication is done, because Y_1 and Y_2 can be reused by an adversary to impersonate the tag. Another problem of this scheme is that, a DoS attack could permanently desynchronise a server and a tag [Chien and Chen 2007]. The scheme also does not provide backward traceability because EPCs are fixed [Chien and Chen 2007].

3.3.1.7 The Lim-Kwon (LK) Protocol

Lim and Kim [2006] proposed a challenge-response based protocol employing pseudo-random functions (for further details Appendix A).

3.3.1.8 The Chien-Chen (CC) Protocol

Chien and Chen [2007] proposed an RFID mutual authentication protocol based on the EPCglobal Class-1 Gen-2 RFID standard. The scheme uses simple cryptographic primitives for example a PRNG and a cyclic redundancy code (for further details appendix A).

3.3.1.9 The Tsudik Protocols

Tsudik [2006] described an RFID identification scheme that provides a basic level of tag identification using time-stamps. It will be referred to as T1 (for further details Appendix A). This is a famous identification protocol that places little burden on the back-end server and uses a monotonically increasing time-stamp which makes it secure against tracking but unsecure against DoS attack. Tsudik [2007] proposed two further protocols known as the T2 and T3 schemes that also provide tag authentication (for further details Appendix A). The schemes use monotonically

increasing time-stamps for tracking-resistant tag authentication, and employ a keyed hash function *f*. The DoS vulnerability of the T1 and T2 schemes is overcome in T3 scheme by using a hash-chain to generate a so-called epoch token, which allows a tag to ascertain that a time-stamp is not too far into the future. Figure 3-5 summarizes the T3 protocol.

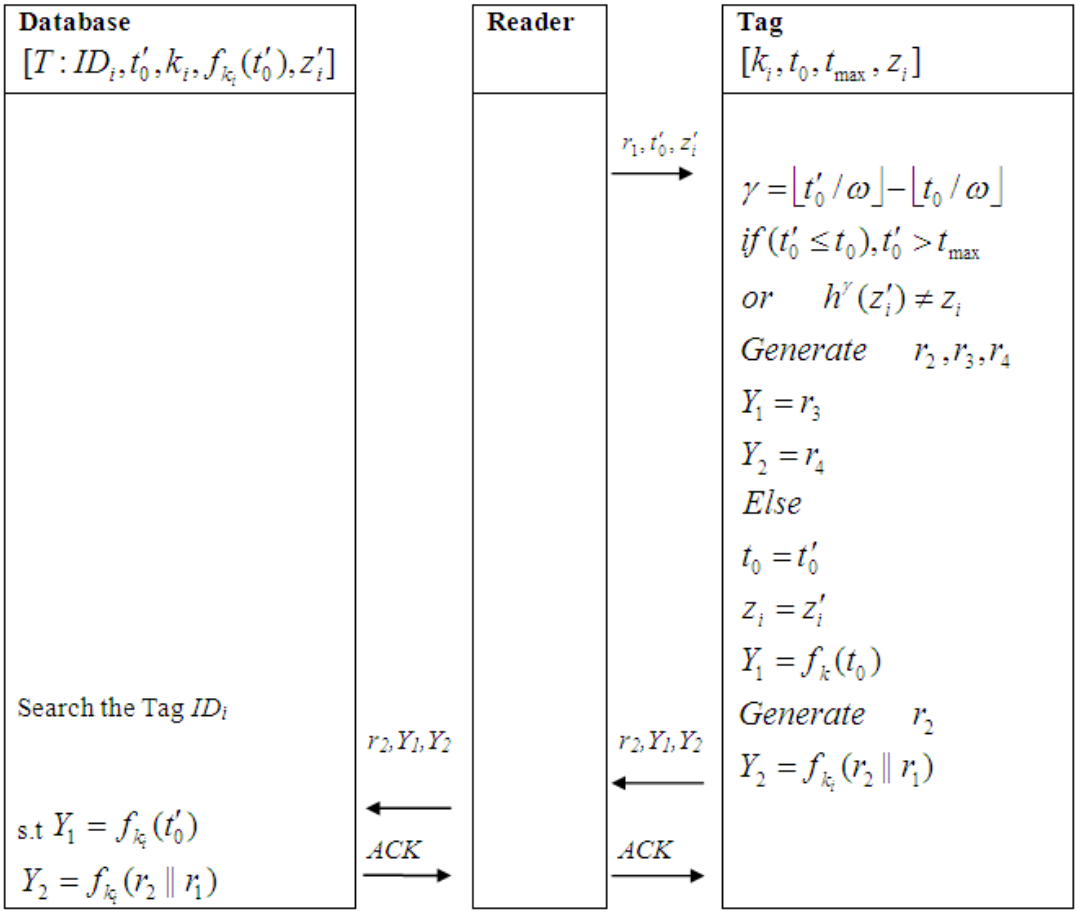

Figure 3-5: The Tsudik T3 protocol

A server makes a hash-chain of length *v* by starting with an initial value *X* and repeatedly hashing it *v* times to generate a root $h^v(X)$, where $v = \lfloor t_{max} / \omega \rfloor$ and ω is the epoch duration. Initially each tag stores an epoch token z_i as a root of the hash-chain, $h^v(X)$.

A server generates a random number r_1 and sends t_0', r_1 and its epoch token z_i' to a tag. The tag checks the received values of t_0' and z_i' by verifying that $t_0' \ge t_0$ and $t_0' < t_{max}$ and that $z_i' = h^{\gamma}(z_i')$, where $\gamma = \lfloor t_0'/\omega \rfloor - \lfloor t_0/\omega \rfloor$. If the validations are successful, the tag updates t_0

and z_i to t_0' and z_i', respectively. The tag then computes $Y_1 = f_{k_i}(t_0)$, generates r_2, computes $Y_2 = f_{k_i}(r_1 \| r_2)$, and sends Y_1, Y_2, and r_2 as its reply. Otherwise, the tag generates pseudo-random numbers r_2, r_3 and r_4, and sends them instead. The server identifies the tag by finding Y_1 in its look-up table for the time-stamp t_0', and authenticates the tag by checking that $Y_2 = f_{k_i}(r_2 \| r_1)$. Figure summarises the T_3 protocol.

The server only requires $O(1)$ operations to identify and authenticate a tag, if the tag reply is valid. Otherwise, the server requires $O(n)$ time to authenticate a tag. For T_3, DoS attacks is still existed as a threat, because an adversary can make the tag inactive for the epoch duration ω, if it queries the tag with the current epoch token and the maximum possible t_0' within the current epoch [Tsudik 2007]. Additionally, for both T_2 and T_3, the adversary can distinguish between synchronised and desynchronised the tags by timing the server responses, because a synchronised tag only requires a server to perform a quick look-up in the table, whereas a desynchronised tag requires performing an extensive search. Furthermore, all the Tsudik schemes have backward traceability, because of their use of a fixed key k_i [Tsudik 2007].

3.3.2 Hash-based Protocols using Static Identifiers

To protect the privacy and security of the RFID systems many researchers use the static identifier approach so that it can work better in ubiquitous computing environment [Choi et al. 2005, Ha et al. 2007]. In his approach the identifier and secret are static and update is not done in the authentication process. The hash function uses random numbers in the tag side and the database side to make the response anonymous. A few researchers also use monotonically increasing timestamp instead of a random number in the reader or database side to make the response unpredictable. This approach eliminates the problem of lack of synchronization since the identifiers are always same.

3.3.2.1 Hash-Based Access Control

Weis at el. [2004] proposed a Hash-based Access Control (HAC) scheme to lock a tag outlined in Figure 3-6. They consider the resource limitations of low-cost tags and offer a simple security scheme based on one-way hash functions [Menezes et al. 1996]. Each hash-enabled tag in this

design will have a part of memory reserved for a temporary *metaID*. It will operate in either a locked or unlocked state. To lock a tag, the tag owner stores the hash of the key at its metaID given as follows:

$$metaID \leftarrow hash(Key)$$

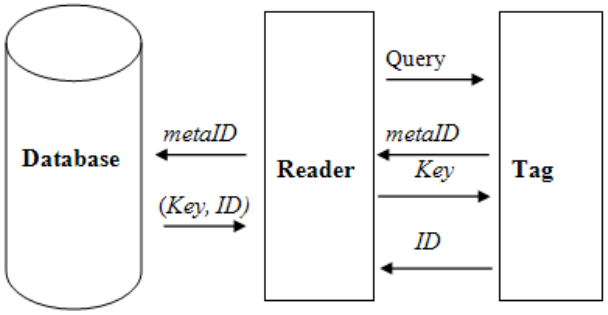

Figure 3-6: Hash-Locking: A Reader Unlocks a Hash-locked Tag

The back-end-database stores both the key and *metaID*. The tag enters its locked state with the *metaID*. In locked state, a tag responds to all queries with only its *metaID* and offers no other functionality. To authenticate a tag the owner needs to unlock the tag first. To accomplish this, the owner queries the tag. The tag replies with the *metaID* to the reader. The reader forwards it to the database and the database looks up the appropriate key for the *metaID* and finally transmits it to the tag. The tag hashes the key and compares with its *metaID*. If the values match, it authenticates the reader and unlocks itself to perform required function before it is locked again.

Due to the one-way hash function the adversary cannot retrieve the contents of the tag from the hash value. Also spoofing attack may be detected but cannot be protected. An adversary may query a tag to get the *metaID*. Later the adversary may spoof the tag to a legitimate reader by a replay attack. The reader will send the key to the spoofed tag. However, to detect spoofing, the reader may check the information of the tag with the back-end database with the proper *metaID*. If any inconsistency is detected, the reader may be alarmed that, a spoofing attack may have occurred. As it always uses the same *metaID*, it can be easily tracked by an adversary. Another problem in this approach is that the key is sent in plain text over the forward channel which can be easily eavesdropped.

3.3.2.2 Randomized Access Control

Weis et al. [2004] also suggested an extended approach called Randomized Access Control (RAC), which uses a random number to prevent location privacy. In each session the tag generate a random number to produce a response as a hash function with this number concatenated with ID. Then it sends the response and the random number to the reader.

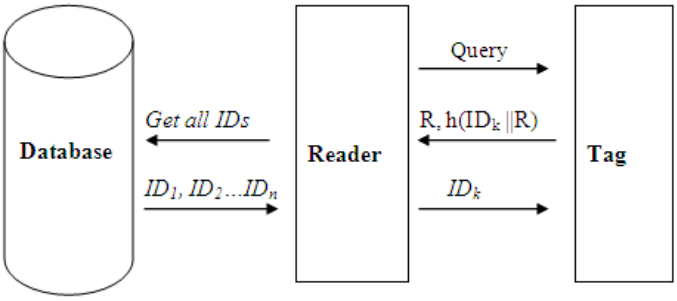

Figure 3-7: Randomized Hashed Locking

A legitimate reader takes all the IDs from the database and computes the hash function with the random number with each ID and compares this value with the tag response to find a match. If it finds a match for any ID then it sends the ID to the tag for authentication (Figure 3-7).

It needs a large number of hash calculations for each tag search. It is impractical for retailers where there are a large number of tags being used and may be feasible for retailers with a relatively small number of tags [Weis et al. 2004]. However, it cannot protect the system from tag impersonation attack and cannot guarantee location privacy since a reader always responses with static tag ID in plain text obtained from its back-end database [Song 2008 and Lee et al. 2005].

3.3.2.3 One-way Hash-based low-cost Authentication Protocol (OHLCAP)

In the schemes where ID is changed in each authentication the protocols do not work well in ubiquitous environment. In ubiquitous computing environment, components of the RFID systems can exist anywhere. If the components of a tag are changed it may not be synchronized with every system [Choi et al. 2005]. The authors proposed a One-way Hash-based low-cost Authentication Protocol (OHLCAP). OHLCAP uses static ID and secrets and works in ubiquitous environment. It

also uses a one-way hash function for privacy and security of the tag. Notations used in the OHLCAP protocol are as follows:

h A one-way hash function, $h:\{0,1\}^* \rightarrow \{0,1\}^l$

l The length of an identifier

r Random number in $\{0,1\}^l$

ID Tag identifier

GI Group index

GI_i ith group index

K Secret in all tags.

S Tag secret

B_L Left half of the message B

B_R Right half of the message B

c Counter

$\oplus$ XOR operator

$\|$ Concatenation operator

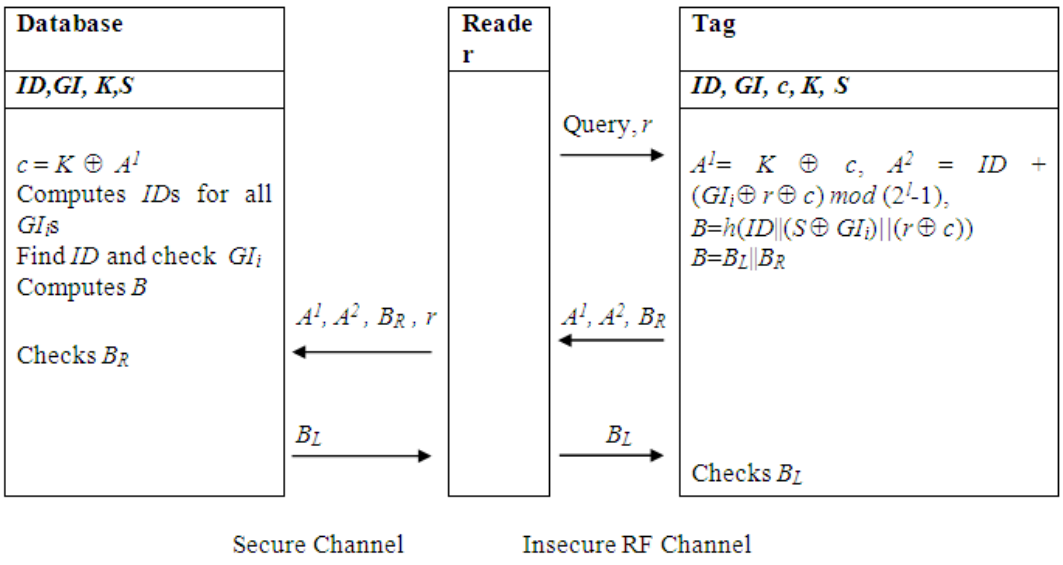

Figure 3-8: The OHLCAP Protocol

The OHLCAP protocol is shown in Figure 3-8 and the steps in the protocol are as follows [Choi et al. 2005]:

Step 1 A reader selects a random value r and sends a request with r to a tag.

Step 2 The tag verifies a random value r if it is all zero or not.

1. If the value of r is all zero, the tag sends stop message to the reader to terminate the process.
2. Else the tag performs as follows:
   - Calculates $A^1 = K \oplus c$, $A^2 = ID + (GI_i \oplus r \oplus c) \bmod (2^l-1)$, $B=h(ID||(S \oplus GI_i)||(r \oplus c))$ and sends A^1, A^2 and B_R to the reader, where B_R is a right half of B,
   - Then, the tag increases the counter c until it exceeds 2^l-1 and is initialized.

Step 3 After receiving from the tag,

1. The reader forwards A^1, A^2, B_R and r to the back-end database.
2. The database computes $c' = A^1 \oplus K$ and $ID_j^{/} = A^2 - (GI_j \oplus r + c') \bmod (2^l - 1)$ for all groups GI_j, $j \in \{1,.....,n\}$
3. The database checks if any $ID_{j(\in\{1.....n\})}^{/}$ matches to one of the stored IDs in the database for same GI_j.
   - If this is successful, the database computes $h(ID||(S \oplus GI_i)||(r \oplus c))$
   - Else, the database terminates this process.
4. Then, the database authenticates the tag by matching the received value B_R.
5. The database sends B_L to the reader, where B_L is a left half of B. The reader forwards B_L to the tag.

Step 4 The tag authenticates the reader by comparing the received value B_L.

OHLCAP is an efficient approach in ubiquitous environment that uses one-way hash function for privacy and security. However, Ha et al. [2007] find its security weakness and proposes an enhanced OHLCAP (EOHLCAP) scheme. The authors showed that this protocol is vulnerable to traceability attack and impersonation attack because of its special property, namely, $c_c=c_p+1$ for two successive sessions. The adversary eavesdrops the messages transmitted between the tag and the reader and obtains the successive $A^1{}_p$ and $A^1{}_c$ where $A^1{}_p = K \oplus c_p$, $A^1{}_c = K \oplus c_c$. Then, it computes $A = A^1{}_p \oplus A^1{}_c = c_p \oplus c_c = c_p \oplus (c_p+1)$ and removes the secret key K in this equation. In this way, the adversary can trace the tag's holder. Similarly, the adversary can implement impersonation attack by selecting special random number $r_c = r_p+1$. If $r_c \oplus c_c = r_p \oplus c_p$ then the value of B_p is equal to B_c since $B=h(ID||(S \oplus GI_i)||(r \oplus c))$. To overcome the security weakness, Ha et al. [2007] adds a pseudo

random number generator (PRNG) to generate a random number and removes the counter in the tag to prevent traceability attack.

3.3.2.4 EOHLCAP Approach

In the EOHLCAP approach to prevent traceability a random number is used in a tag in place of a counter information. However, this protocol requires a random number generator in a tag. Due to this random number in place of a counter value, the tracing attack and impersonation attack by maliciously updating the random number becomes impossible. In contrast to OHLCAP, the proposed protocol removes the data fields, the secret key S_{ij} and counter c due to their uselessness. The system setup is as follows [Ha et al. 2007]:

System Set-up

Tag: A tag is initialized by a data field, including *ID, GI, K*.
Back-end database: Divides all the tags into *n* groups. The data fields are GI_i, K, ID_{ij}.

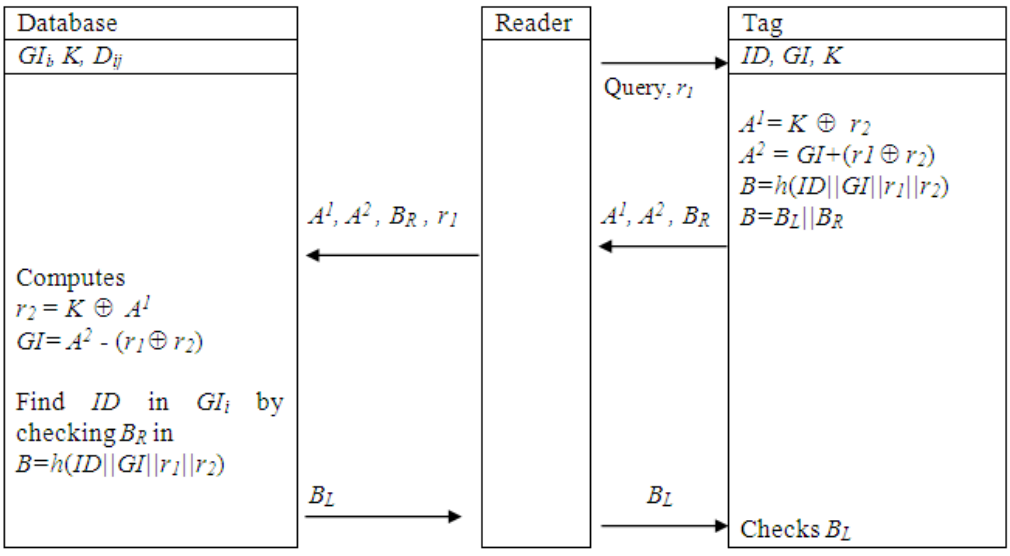

Figure 3-9: The EOHLCAP Protocol

The protocol is shown in Figure 3-9 and the steps are given as follows:

Step 1. The reader sends a request and r_1 to a tag.

Step 2. The tag generates a random number r_2 and computes $A^1 = K \oplus r_2$, $A^2 = GI+(r1 \oplus r_2)$, and $B=h(ID||GI||r_1||r_2)$.

It then sends A^1, A^2, and B_R to the reader.

Step 3. The reader then sends A^1, A^2, and B_R with r_1 to the back-end database.

Step 4. The back-end database computes $r_2 = K \oplus A^1$ and $GI = A^2 - (r_1 \oplus r_2)$, then finds the *ID* in the *GI* by checking the B_R. The back-end database authenticates the tag by checking that the computed B_R equals the received one, and then sends the B_L to the reader.

Step 5. The reader sends the B_L to the tag.

Step 6. The tag also authenticates the reader by checking if the received B_L equals the computed one as in Step 2.

The EOHLCAP overcomes the problems in OHLCAP and protects the RFID system from most of the attacks but it requires many complex hash operations in the database side.

3.3.2.5 Molnar and Wagnar (MW) Protocol

Molnar and Wagner [2004] proposed a mutual authentication scheme to provide privacy and security for library RFID systems. The scheme uses a shared secret and pseudo-random number function to protect the messages communicated between the tag and the reader.

In the basic authentication protocol, a reader R and a tag T share a shared secret *s*, that is used as a key for a pseudo-random number function *f*. The reader queries a tag by sending it a random number r_1. The tag generates a random number r_2, computes $Y_1 = ID_i \oplus f_s(0 \| r_1 \| r_2)$, and sends them both to the reader. The reader sends it to the server. The server finds the value ID_i for the tag using the received values of r_2 and Y_1, and sends $Y_2 = ID_i \oplus f_s(1 \| r_1 \| r_2)$ back to the reader and the reader sends it to the tag to complete server authentication. Figure 3-10 shows the steps of the protocol.

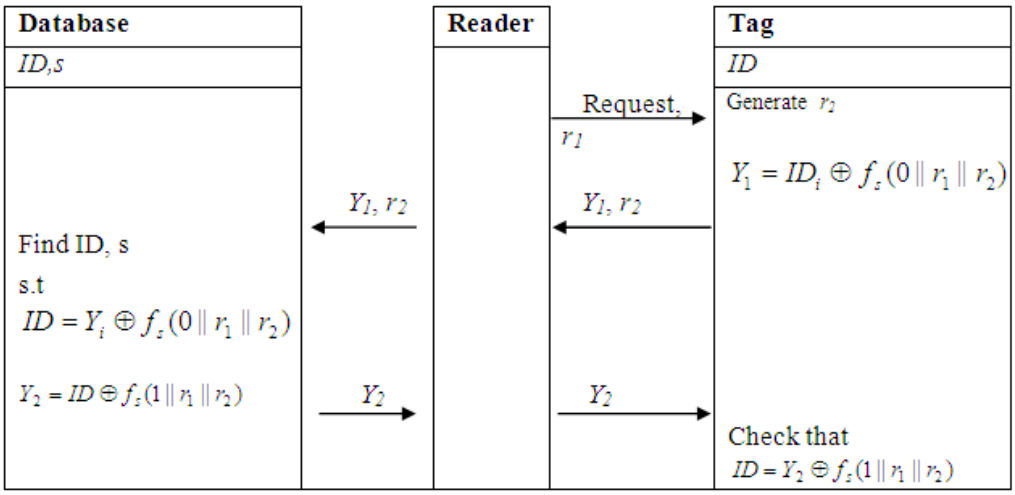

Figure 3-10: MW Protocol

This scheme uses a tree-based technique to search a tag in the database. This reduces the complexity of tag identification from O(*n*) to O(log*n*). The *n* tags are regarded as leaves in a balanced binary tree, and each edge is linked with a secret in the tree structure. A server knows all the secret values, and each tag stores the log*n* secrets corresponding to the path from the root to the tag.

However, this protocol could hamper privacy if an adversary tampers with a tag, because in this case the adversary is able to trace other tags in a probabilistic way [Avoine et al. 2005b]. Also, this protocol uses a static secret *s* for each tag T, and therefore it cannot resist backward traceability; once a tag is compromised, the adversary can trace the past communications of the tag.

3.3.2.6 The Molnar-Soppera-Wagner (MSW) Protocol

Molnar et al. [2005] proposed an RFID pseudonym protocol that employs pseudo-random number functions. The authors claim that, the scheme provides two new features not seen in prior RFID protocols, namely time-limited delegation and ownership transfer (for further details Appendix A).

3.3.2.7 Challenge-Response Based RFID Authentication Protocol

Rhee et al. [2005] proposed challenge response based RFID authentication protocol (CRAP) which is designed to use in pervasive computing.

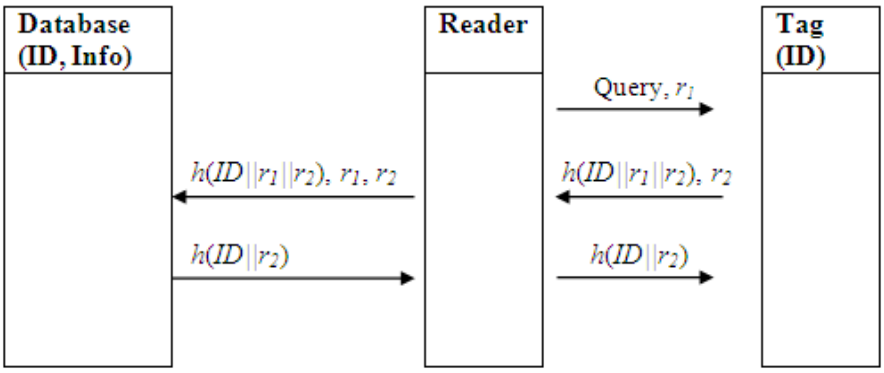

Figure 3-11: CRAP Protocol

The protocol is shown in Figure 3-11 and the steps are given as follows:

Step 1. The reader sends a *Query* and r_1 to a tag.

Step 2. The tag generates a random number r_2 and computes $h(ID||r_1||r_2)$.

It then sends $h(ID||r_1||r_2)$ and r_2 to the reader.

Step 3. The reader forwards $h(ID||r_1||r_2)$ and r_2 with r_1 to the back-end database.

Step 4. The back-end database computes $h(ID||r_1||r_2)$ for all *ID*s and compares with the received $h(ID||r_1||r_2)$ from the reader. If the authentication is successful then the back-end database sends $h(ID||r_2)$ to the reader.

Step 5. The reader forwards the $h(ID||r_2)$ to the tag.

Step 6. The tag computes $h(ID||r_2)$ and compares with the received $h(ID||r_2)$ for successful authentication.

The proposed protocol is secure against the replay attack, spoofing attack and so on. However, this scheme requires $(\frac{N}{2}+1)$ hash functions computations which is impractical for large number of tags in ubiquitous computing (Choi et al. 2005).

3.3.3 Light-weight Encryption Protocols

Recently a number of lightweight encryption authentication protocols are proposed for the privacy and security protections of RFID systems. For this purpose simple light weight encryption for example bitwise XOR is used [Jules and Weis 2005, Goldreich and Levin 1989]. These are suitable for low-cost RFID tags than hash-based protocols since hash functions are computationally

more expensive than bitwise logical operations. The details of this technology are discussed in the next Section 3.3.3.1.

3.3.3.1 The Learning Parity with Noise (LPN) Problem and HB Protocol

The LPN problem works with binary inner product of two numbers. It is assumed that each number is *k*-bit long and two *k*-bit numbers $a = (a_0 a_1 ....(a_{k-1})_2$ and $x = (x_0 x_1 .....x_{k-1})_2$. The inner product of *a* and *x* is denoted by *a.x* and it can be evaluated as $a.x = (a_0 \wedge x_0) \oplus (a_1 \wedge x_1) \oplus ..... \oplus (a_{k-1} \wedge x_{k-1})$. It is easy to implement in low cost hardware such as an RFID tag and is also possible to compute one bit at a time [Jules and Weis 2005]. This means it is not necessary to store all *k* bits of *a* and *x* when computing. Goldreich and Levin [1989] proved that *a.x* is unpredictable if only *a* or *x* is given.

The HB protocol proposed by Hopper and Blum is a cryptographic protocol based on binary inner product. It was a human authentication protocol because human can evaluate one binary inner product operation, and generate a random bit. This HB protocol is claimed to be secure under the assumption that Learning Parity with Noise problem is intractable.

In HB protocol both human and machine shares a common secret *x* of *k*-bit long. In this case the human plays the role of a tag and the reader plays the role of a machine.

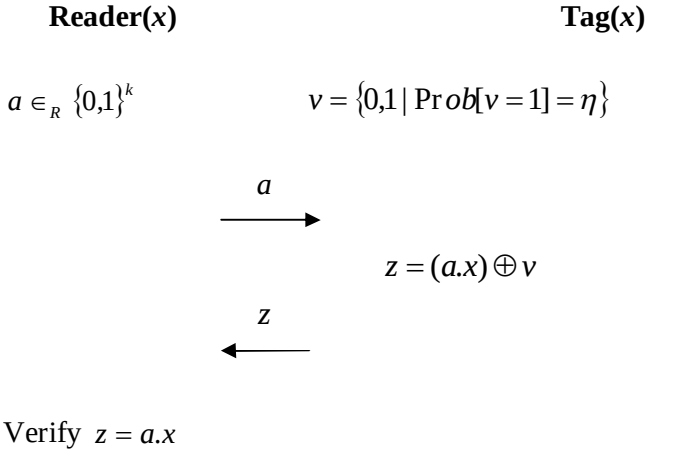

Figure 3-12: One Round of HB Protocol.

The HB protocol is depicted in Figure 3-12 and the steps in this protocol for one round are given as follows:

1. The reader generate a random number *a* and sends it to the tag.
2. The tag receives the random number and computes $z = a.x$ and introduces a noise factor *v* with it. Here *v* =1 with probability $\eta = (0,0.5)$.
3. The tag then sends $z = (a.x) \oplus v$ to the reader.
4. The reader then verifies $z = a.x$ if tag produces fewer errors than ηr in *r* round.

The purpose of *v* is to protect *x* from the passive eavesdropper after observing *k* pairs (*a*, *z*). The noise bit is generated in each round with a value 1 with probability η.

The HB protocol is secure only from passive attackers. It is not secure against active attacks where a reader can be malicious. Jules and Weis [2005] proposed an extended version of the HB protocol to protect against active attack and this new protocol is referred to as HB+.

3.3.3.2 The HB+ Protocol

The HB+ protocol is an improved version of HB protocol and gives better privacy and security protection. In the HB+ protocol the reader and the tag both share two secrets (*x*, *y*) of *k*-bit long. In the HB+ protocol the tag also generates a random number *b* as a blinding factor. The purpose of the blinding factor *b* is to protect the tag from the malicious reader from extracting secret by repeatedly querying the tag with the same random number *a*. The HB+ protocol is depicted in Figure 3-13 and the steps in this protocol are as follows:

1. The tag generates a random number *b* as a blinding factor and sends it to the reader.
2. The reader generates a random number *a* and sends it to the tag.
3. The tag receives the random number *a* and computes $z = (a.x) \oplus (b.y) \oplus v$. Here *v* is a noise factor of value 1 with probability $\eta = (0,0.5)$.
4. The tag then sends $z = (a.x) \oplus (b.y) \oplus v$ to the reader.
5. The reader verifies $z = (a.x) \oplus (b.y)$ if the tag produces fewer errors than ηr in *r* round.

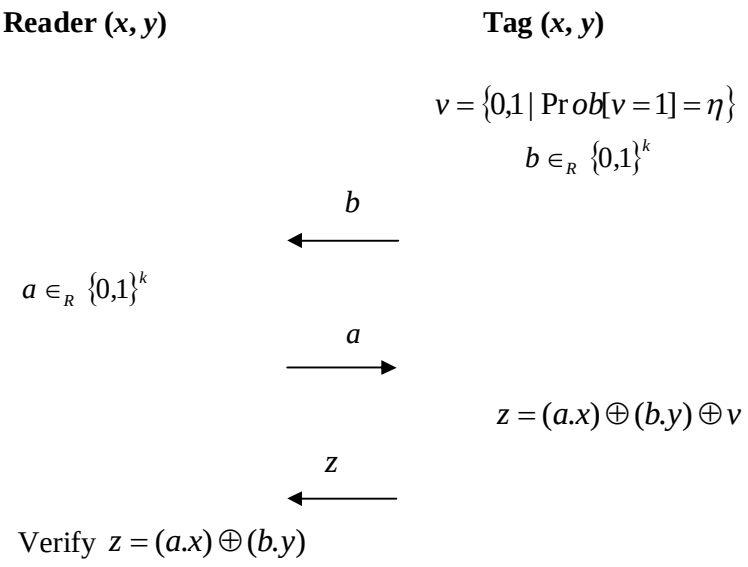

Figure 3-13: One Round of HB+ Protocol.

In the HB+ protocol the purpose of *v* is same as in the HB protocol. It is to protect *x* from passive eavesdropper after observing *k* pairs (*a*, *z*). The noise bit is generated in each round with a value 1 with probability η as in HB protocol.

Though it is claimed that the HB+ protocol is free from an active attack however, Gilbert et al. [2005] has described an attack on HB+ protocol. The authors proved that it is not secure against the man-in-the-middle attack. The adversary chooses a *k*-bit vector δ and introduces it by doing XOR with a in each round and sends the result $a \oplus \delta$ to the tag in place of a shown in Figure 3-14. The tag will compute $z' = (a \oplus \delta).x \oplus (b.y) \oplus v$ and send it to the reader. It is obvious that if authentication process is successful then $\delta.x = 0$ otherwise $\delta.x = 1$ with a high probability. So, one can recover one bit of *x* by using same δ in all *r* round. To retrieve the *k*-bit secret *x* it is sufficient to repeat the whole protocol *k* times by changing the value of δ linearly independently.

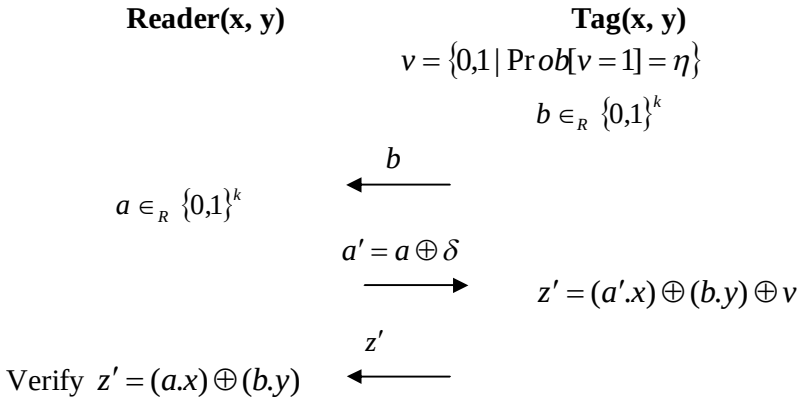

Figure 3-14 Attack in one Round of HB+ Protocol.

3.3.3.3 HB-MP Protocol

Munilla and Peinado [2007] proposed a new protocol named HB-MP, derived from HB+ to improve efficiency and resist active attacks to the HB-family. The authors proposed the protocol in two phases. First one is called HB-MP$^{/}$ which exchanges only two messages. The second protocol HB-MP is defined applying a modification to the previous HB-MP$^{/}$ protocol. It can resistant the simple man-in-the-middle attacks.

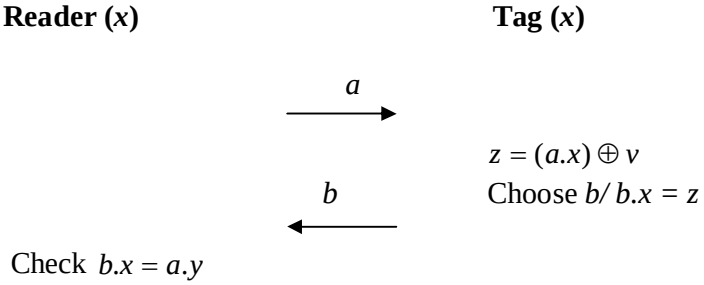

Figure 3-15: One Round of HB-MP$^{/}$ Protocol.

The HB-MP$^{/}$ protocol is composed of r rounds, one of which is depicted in Figure 3-15. The protocol can be described as follows:

1. The reader generates a k-bit random binary vector a, and sends it to the tag.
2. The tag then computes the z as follows:

   $z = (a.x) \oplus v$

It searches for a *k*-bit binary vector b such that

$a.x = z$

3. The tag then sends *b* to the reader.
4. The reader verifies $b.x = a.y$

It is easy to prove that the problem of finding *x* with the known vectors *a* and *b* is at least as difficult as solving the LPN problem. For example if the adversary picks a = 000..... 000 for all the rounds he would obtain the following system of linear equations:

$$0 = b_i.x_0 \leq 0 \leq q$$

where b_i is the vector *b* in the *i*th round. The system incorporated noise in the bitstring b_i. From the adversary point of view, the system is a linear equation where the b_i are right and some of the 0's in the part to the left of equation are wrong; that means this is the LPN problem. However, a checking to avoid that the challenge could be 0 would make solving this problem even more difficult.

The step-2 seems to be very complex in the protocol. This step can be carried out very easily for $\eta = \frac{1}{4}$ without resorting to any noise generator. The following algorithm efficiently performs this step in the HB-MP$^{/}$.

Algorithm 1. Input: *a*, *x*. Output: *b* such that $b.x = a.x \oplus v$, where $v = 1$ with probability 1/4.

Computes $z = a.x$

Generates *k*-bit random binary vector *b*

If $b.x = z$

Sends *b*

else

Generates a new random k-bit vector *b*

end

HB-MP$^{/}$ protocol is secured against passive attack but vulnerable to man-in-the-middle attack proposed by Gilbert et al. [2005]. To protect from the attack the HB-MP$^{/}$ protocol is modified. It is called HB-MP. The HB-MP protocol uses two shared secrets as in HB+ protocol. The lengths of the

secret keys do not coincide with length of the exchanged messages for example keys of 64 bits for the messages of 60 bits.

Notation

k: length of the secret keys.

m: length of the messages exchanged between the parties.

x,y: secret keys shared by the reader and the tag.

xm: *m* less significant bits of x.

a,b: random m-bit binary vectors.

v: noise bit; $v = 1$ with probability $\eta \in [0, 1/2]$

$\oplus$: XOR operation.

Rotate (*p,w*): Bitwise left rotate operator. The operand *p* is rotated *w* positions.

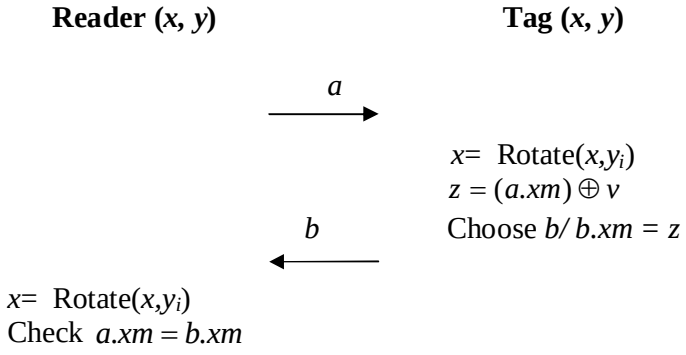

Figure 3-16: One Round of HB-MP Protocol.

This protocol is also composed of *r* rounds and is depicted in Figure 3-16. The protocol can be described as follows:

1. The reader generates a *m*-bit random binary vector *a*, and sends it to the tag.
2. The tag then computes $x = \text{Rotate}(x, y_i)$, where y_i is the *i*th bit of *y*.
3. The tag also computes z:

$$z = a.x \oplus v$$

and looks for a *k*-bit binary vector *b* such that $b.xm = z$, using the previous algorithm

4. The tag then sends *b* to the reader.
5. The reader computes the secret key as $x = \text{Rotate}(x, y_i)$ where y_i is the *i*th bit of the key *y*.

6. The reader verifies $a.xm = b.xm$

3.3.3.4 HB-MP$^+$ Protocol

Leng et al. [2008] propose an improved version of the HB-MP authentication protocol, referred to as the HB-MP$^+$ scheme. The HB-MP$^+$ protocol overcomes the man-in-the-middle attack to which the basic HB-MP protocol is vulnerable. Protection against the man-in-the-middle attack as proposed by Gilbert et al. [2005] has been considered in the HB-MP protocol. The rotation of *xm* is used to protect from the attack. However, this rotation has its own weakness. In the HB-MP protocol, for every new session, *xm* needs to be identical in the *i*th round. It is not mentioned clearly about when to start and end an authentication session. It is assumed that when the tag enters the range and starts to communicate with the reader, an authentication session begins and when the *q*-round is finished or the tag leaves from the range of the reader, the session ends. Since $x = Rotate(x, y_i)$, the value of *xm* in the first round of all the authentication sessions have to be the same. The adversary can commence recurring authentication sessions, initially confined to the first round. Then the techniques of the Section 3.3.3.3 can be used to reveal the *xm* of first round of the tag. If the adversary monitors the *i*th round, he is able to expose the *xm* value used in *i*th round.

The scheme ought to use the same value *xm* between the authentication sessions to evade the synchronisation problem. The value of *x* is fixed. If the value of *x* is changed after each session on both the tag and the reader side, a new reader will not be capable of verifying the tag with updated value and cannot authenticate the new tag. It is possible only if all the tags and the readers are updated simultaneously after each authentication session, which is very expensive and difficult to implement. Even if the synchronization problem is removed and the value of *x* is altered in each successful authentication session there is still a way to carry out the special man-in-the-middle attack. As the size of secrets *x* and *y* is *k* if in any authentication session, the scheme runs *k* rounds, the value of *x* will be rotated by *p* bits, where *p* is the number of '1s' in *y*, so if the adversary runs the scheme for *k* number of times, that is k^2 rounds, the *x* is to be rotated $p \cdot k$ times and finally it comes to its initial value. As a result a repeat of the value *xm* takes place again. As the proposed value of *x* is 512 bits, 262144 rounds will generate a repeated *xm* which is an inexpensive attack.

To overcome the weakness coming from the predictable repetition of xm, Leng et al.[2008] use some additional random bits generated by the reader to randomize the rotation. The objective of HB-MP+ scheme is to use a random secret value in each round.

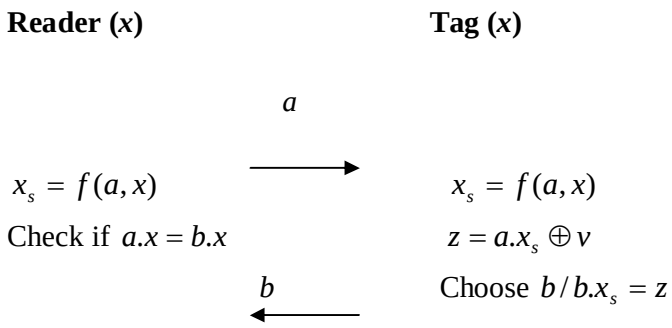

Figure 3-17: A Single Round of HB-MP^{+} Protocol

The HB-MP+ protocol is shown in Figure 3-17 and the steps are given as follows:

1. The reader picks at random a *m*-bit binary vector a and sends it to the tag.
2. The reader and tag computes the round key $x_s = f(a, x)$. *f*(.) is a one-way function.
3. The tag computes z as follows $z = a.x_s \oplus v$ and looks for a *m*-bit binary vector b such that $b.x_s = z$
4. The tag sends b to the reader
5. The reader computes the $x_s = f(\alpha, x)$, using the secret *x* and random number *a*
6. The reader checks if $a.x_s = b.x_s$

The round key x_s is obtained by a random number a and the shared secret *x*. There is no need for another secret *y* because the value of *x* is not altered. There is no problem of synchronization between tag and reader. Since the rotation is a linear operation, the output of *f*(.) should be less predictable. Using the simple bit operations, it is very easy to apply a low-cost non-linear function *f*(.). Since *f*(.) does not inevitably use rotation operation, the bits in *x* are not need to be mentioned.

3.3.3.5 HB-MP^{++} Protocol

The nonlinear one-way function used in HB-MP+ is abstract. So it is not possible to prove the validity of the protocol for RFID systems. Also, as the tag's response has the same number of bits,

the protocol is still vulnerable to traceability [Weste and Harris 2005, Garg 2000]. Yoon et al. [2009] proposed the HB-MP++ protocol that uses the LSFR that has two consecutive two-stage memory or storage stage and feedback logic (See appendix A).

3.4 Conclusion

This chapter has reviewed a number of recently proposed RFID authentication protocols. This chapter also classified the authentication protocols according to their implementation. Advantages and disadvantages of the protocols are also outlined for each protocol. The protocols are classified based on hash-based varying identifier, static identifier and light-weight encryption based protocols for RFID systems. The protocols with hash-based varying identifiers ensure privacy and security of the information by updating it after every authentication session so that the response is unpredictable. In this case the adversary cannot use any response in future to authenticate the system since the identifier and the secret value are no longer similar. However it requires synchronization in the tag side and the database side which involves computational and storage overheads. This approach is not suitable in the ubiquitous computing environment since the synchronization of the updated values is difficult to ensure in the distributed environment. The protocols with static identifiers are suitable for ubiquitous computing environment but it requires more storage. Finally this chapter discusses a number of well known light-weight encryption authentication protocols and their advantages and disadvantages. The light-weight encryption protocols require less complex operations than hash-based protocols since hash functions are complex and computation intensive.

The privacy, security and efficiency problems in different existing protocols are also identified in this chapter. It is a challenge to ensure all the identified privacy and security threats effectively and efficiently. In the following chapters a number of novel authentication protocols are proposed to protect the privacy and security of the RFID systems to overcome the problems of existing protocols. The proposed protocols attempt to protect from the following privacy and security threats: information leakage, location privacy, impersonation attack, man-in-the-middle attack, replay attack, DoS attack, forward privacy and backward privacy. The concepts of the existing protocols are used as the foundation for the proposed protocols. The protocols combined the advantages of various existing protocols to overcome the privacy and security problems in RFID

systems. It also effectively uses the hash function, hash address, random numbers and timestamp in the proposed protocols.

Chapter 4 Proposed Hash-based Ubiquitous Protocols

4.1 Secure Ubiquitous Authentication Protocols

In this chapter, the possible privacy and security threats to the Radio Frequency Identification (RFID) systems are investigated and four novel group-based authentication protocols are proposed which provide the identified privacy and security in an efficient manner for a ubiquitous computing environment. The approach utilizes the concepts of two very different, widely known RFID protocols, i.e. the Low-Cost Authentication Protocol (LCAP) approach and the One-way Hash based Low-Cost Authentication Protocol (OHLCAP) approach. The resulting protocols combine the advantages of both protocols and eliminate the existing privacy and security problems from these. The approaches are evaluated using a variety of criteria that are relevant in practice. The proposed protocols use random numbers and a hash function to encrypt the key to protect the RFID system from the adversary attacks. The protocols also use the hash value as a hash address to reduce the search time to locate the tag in the database from a large number of records. The analysis shows that it requires low tag-side storage and computation. A simulation experiment is also conducted to verify some of the privacy and security properties of the proposed protocol.

4.1.1 Related Workd

The proposed protocols combine the concepts of two different prominent protocols LCAP [Lee et al. 2005] and OHLCAP [Choi et al. 2005] and join the advantages to solve the existing privacy and security problems.

The detail of the LCAP protocol is given in Section 3.3.1.4. The LCAP scheme uses one way hash function to protect the privacy and security of the tag. The hash function $h(ID)$ is also used to denote the address or index of the tag in the database. To authenticate each other it generates $h(ID||r)$ and uses two halves $h_L(ID||r)$ and $h_R(ID||r)$ to authenticate in two ends. In LCAP scheme

ID is changed in each authentication. So it does not work in ubiquitous environment. As mentioned earlier (Section 3.3.1.4), it does not overcome the traceability problem.

The OHLCAP uses a static identifier and secrets and is suitable for ubiquitous environment. The detail of the OHLCAP protocol is given in section 3.3.2.3. It also uses a one-way hash function for privacy and security of the tag. OHLCAP requires an *ID* and a hash function *h* as in LCAP. Some additional fields are also required. *GI* is used as a group index. *K* is a common secret used in all tags, *S* is a tag secret. B_L and B_R are the left and right half of *B* respectively. *c* is used as a counter and initialized to an arbitrary value. It is increased every time a reader sends a query to the tag. The notation $\oplus$is used for xor operation and || is used for concatenation operation.

OHLCAP is an efficient approach in ubiquitous environment that uses one-way hash function for privacy and security. However, Ha et al.[2007] found its security weakness and proposes an enhanced OHLCAP (EOHLCAP) scheme. The authors showed that this protocol is vulnerable to traceability attack and impersonation attack because of its special property, namely, $c_c=c_p+1$ for two successive sessions. The detail of the attack is given in section 3.3.2.3. To overcome the security weakness, Ha et al.[2007] adds a pseudo random number generator (PRNG) to generate a random number and removes the counter in the tag to prevent traceability attack.

4.1.2 The Proposed Secure Ubiquitous Authentication Protocols

OHLCAP is not protected against traceability and impersonation attacks. It requires considerable storage on the tag side and database side. EOHLCAP eliminates the privacy problem in OHLCAP with reduced amount of storages in the tag side and the database side but it takes many hash operations to locate the tag in the database [Ha et al. 2007]. LCAP requires less storage in the tag and reduces search time in the database but it is not suitable for ubiquitous computing environment as the *ID* is updated after each authentication process. To overcome these problems, three Secure Ubiquitous Authentication Protocols SUAP1, SUAP2 and SUAP3 for RFID systems are proposed in this section. The SUAP1 is a simple RFID authentication protocol that will work in a system where the numbers of tags are small (several thousands). Some aspects of the work of the SUAP1 was published in [Morshed et al. 2010]. In this section the SUAP1 protocol has been improved with additional privacy and security enhancement. This also added privacy and security comparison, simulation results with an extensive analysis and evaluations. The SUAP2 and SUAP3 are the

extension of SUAP1 and work in a large group-based system where RFID tags are divided into several groups. These protocols are low-cost and secure based on challenge-response method using a one-way hash function, hash-address as a search index. The proposed protocols combine the features of the hash address and hash function of the LCAP protocol and the ubiquitous property of OHLCAP protocol and overcome the existing privacy and security problems in these two schemes. The advantage of hash address is to reduce the search time in the database. The notations used in the SUAP1, SUAP2 and SUAP3 protocols are as follows:

Notations

h A one-way hash function, $h:\{0,1\}^* \rightarrow \{0,1\}^l$

ID Tag identifier

GID Group identifier

Had Hash address *h(ID)*

N Number of tags

n Number of groups

m_i Number of tags in the i^{th} group

l The length of an identifier. The value of l is assumed 96 bits.

r_1 Random number in $\{0,1\}^l$

r_2 Random number in $\{0,1\}^l$

$\oplus$ XOR operator

|| Concatenation operator

$\leftarrow$ Assignment operator

$+$ Modular addition by *mod* $(2^l - 1)$

4.1.2.1 SUAP1

The SUAP1 protocol uses a static identifier and a secret number, hash function and two random numbers. This protocol also uses the hash function value as an address to search the tags in the database. The objective of the SUAP1 protocol is to preserve the ubiquitous property of the protocol and is suitable for a small number of tags. In this case a common secret is stored in all the tags. Two random numbers make the hash response unpredictable so that it is impossible to perform

impersonation and tracing attack by a malicious reader. The system set-up of the SUAP1 protocol is as follows:

System Set-up

Tag: Each tag contains the following fields:

ID: Tag Identifier

x: Common secret number

Reader: Reader does not contain any fields.

Back-end Database: Back-end database contains the following fields:

ID: Tag identifier

x: Common secret number

Had: Hash address *h(ID)*

When a tag enters into the range of a reader, the reader can initiate the authentication protocol. The steps in the authentication protocol are as follows.

1. The reader generates a random number r_1 and sends it to the tag.
2. Receiving the number r_1 the tag generates another random number r_2.

   if r_1 *or* r_2 *is* 0 *stop protocol*

   otherwise performs the following computations

   $y \leftarrow h(ID) + (r_1 \oplus r_2)$

   $t = r_2 \oplus x$

   Computes $h(ID \| r_1 \| r_2)$

   The tag then sends the value of *y*, *t*, h_L to the reader.

   Where h_L is the left half of $h(ID \| r_1 \| r_2)$
3. The reader then sends the value of *y*, *t*, h_L and r_1 to the back-end database.
4. The back-end database will calculate the following

   $r_2 = t \oplus x$

   $h(ID) \leftarrow y - (r_1 \oplus r_2)$

   $h(ID)$ is the address of the record containing the *ID* where $Had = h(ID)$

   Access the address *Had*

   Retrieves the *ID* from the record

   Then the back-end database *Computes* $h(ID \| r_1 \| r_2)$

If h_L matches the tag is authenticated

Sends h_R to the reader

Where h_R is the right half of $h(ID \| r_1 \| r_2)$

5. The reader forwards the h_R to the tag
6. If the received h_R matches the reader is authenticated.

The protocol is shown in the Figure 4-1.

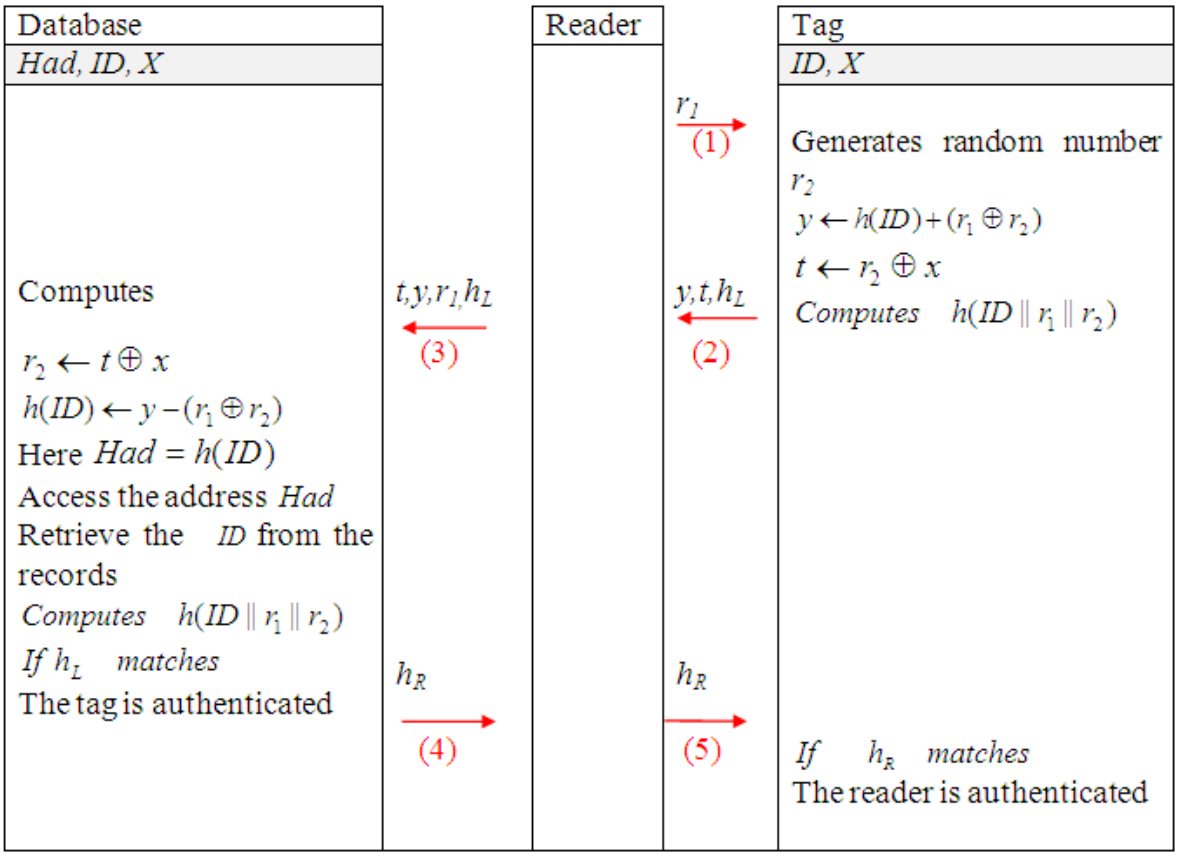

Figure 4-1: The Proposed SUAP1 Protocol

The protocol is simple and works for an organization having small number of tags (several thousands). Two random numbers make the response anonymous. The problem in this simple protocol is that it maintains a common secret for all the tags in the database. It can be a problem to manage this secret in a large organization having different departments. Having only a single secret for all the tags it cannot ensure privacy and security for a large organization having millions of tags in many departments.

4.1.2.2 SUAP2

To overcome the problem in SUAP1 of having only one secret for all the tags the SUAP2 maintains groups for the different departments and different types of products. In addition to the *ID* and secrets in the SUAP1, one extra variable *GID* is needed in the tag side and the database side. It represents a group identifier. This is also a secret number. The database divides the tags into *n* groups and the protocol is shown in the Figure 4-2. The only difference between the SUAP1 and SUAP2 is that SUAP2 maintains the groups of the tags and there is a common secret for each group like OHLCAP and EOHLCAP. In this case one secret value *x* is used for all the tags in a group. It will reduce the tag search time in the database. This is suitable for the case where the tags of the same group are not distributed in various places. It ensures better security but requires less computation and search times in the database. The system set-up of the SUAP2 protocol is as follows:

System Set-up

The system setup for the tag, reader and database for the SUAP2 protocol are as follows:

Tag: Each tag contains the following fields:

ID: Tag Identifier

x: Secret number

GID: Group identifier

Reader: Reader does not contain any fields.

Back-end Database: Back-end database contains the following fields:

ID: Tag identifier

x: Secret number

Had: Hash address *h*(*ID*)

GID: Group identifier

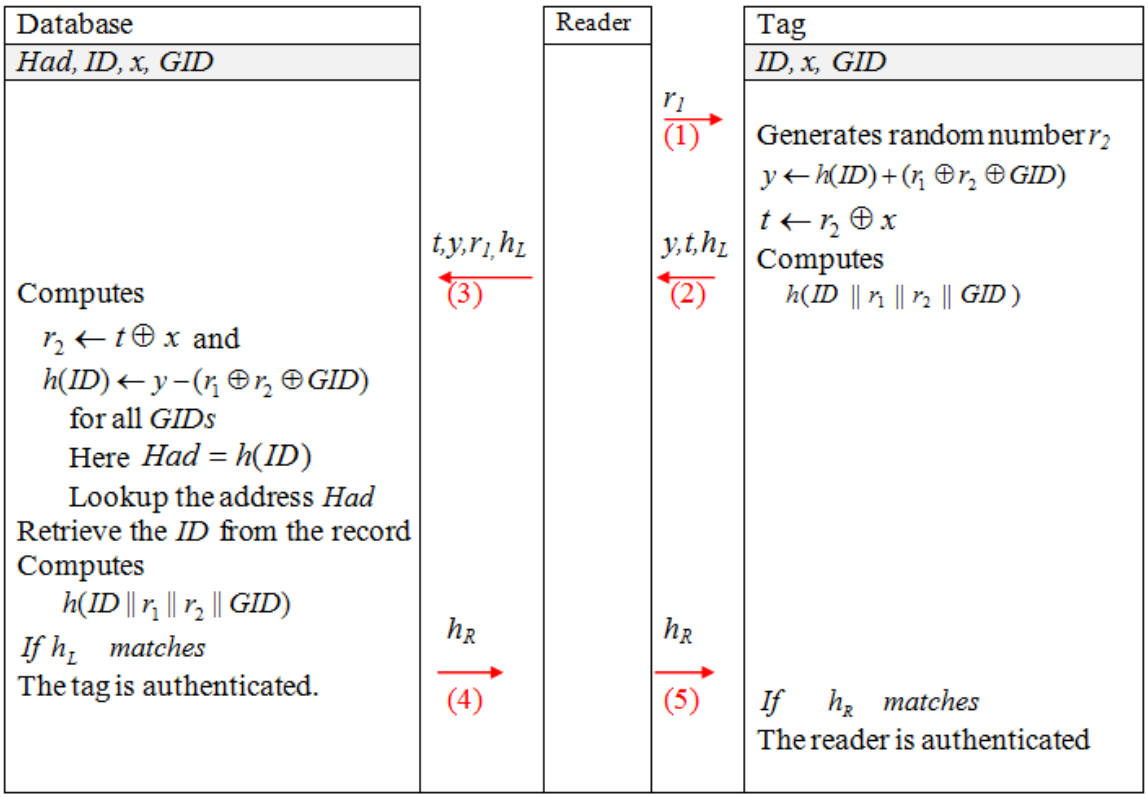

Figure 4-2: The Proposed SUAP2 Protocol

The steps in the authentication protocol are as follows.

1. The reader generates a random number r_1 and sends it to the tag.
2. Receiving the number r_1 the tag generates another random number r_2.

   if r_1 *or* r_2 *is* 0 *stop protocol*

   otherwise performs the following computations

   $y \leftarrow h(ID) + (r_1 \oplus r_2 \oplus GID)$

   $t = r_2 \oplus x$

   Computes $h(ID \| r_1 \| r_2 \| GID)$

   The tag then sends the value of y, t, h_L to the reader.

   Where h_L is the left half of $h(ID \| r_1 \| r_2 \| GID)$
3. The reader then sends the value of y, t, h_L and r_1 to the back-end database.
4. The back-end database calculates the following for all *GID*s

   $r_2 = t \oplus x$

$h(ID) \leftarrow y - (r_1 \oplus r_2 \oplus GID)$

$h(ID)$ is the address of the record containing the *ID* where $Had = h(ID)$

Lookup the address *Had*

Retrieves the *ID* from the record

Then the back-end database *Computes* $h(ID \| r_1 \| r_2 \| GID)$

If h_L matches the tag is authenticated

Sends h_R to the reader

Where h_R is the right half of $h(ID \| r_1 \| r_2 \| GID)$

5. The reader forwards the h_R to the tag
6. If the received h_R matches the reader is authenticated.

The SUAP2 protects the RFID systems from all the identified privacy and security problems in large organization but requires more storages than SUAP1.

4.1.2.3 SUAP3

The SUAP3 enhances the SUAP2 in efficiency by removing the secret *x* from the tag and the database. It also requires the group variable *GID* in the tag and the database as in SUAP2. It represents a group identifier and also a secret number. The database divides the tags into *n* groups. The protocol is shown in the Figure 4-3. The only difference between the SUAP2 and SUAP3 is that SUAP3 does not use the secret *x* for the tag and the database. The group based structure is used for the searching tags in the database. The privacy will not be hampered due to the elimination of the secret *x* because the *GID* works as an *l* bits secret which is also difficult to guess by the adversary. It reduces the number of searches significantly. Since the hash function is one-way it still gives the same security protection to the *ID*. The system set-up of the SUAP3 protocol is as follows:

System Set-up

Tag: Each tag contains the following fields:

ID: Tag Identifier

GID: Group identifier

Reader: Reader does not contain any fields.

Back-end Database: Back-end database contains the following fields:

ID: Tag identifier

Had: Hash address *h*(*ID*)

GID: Group identifier

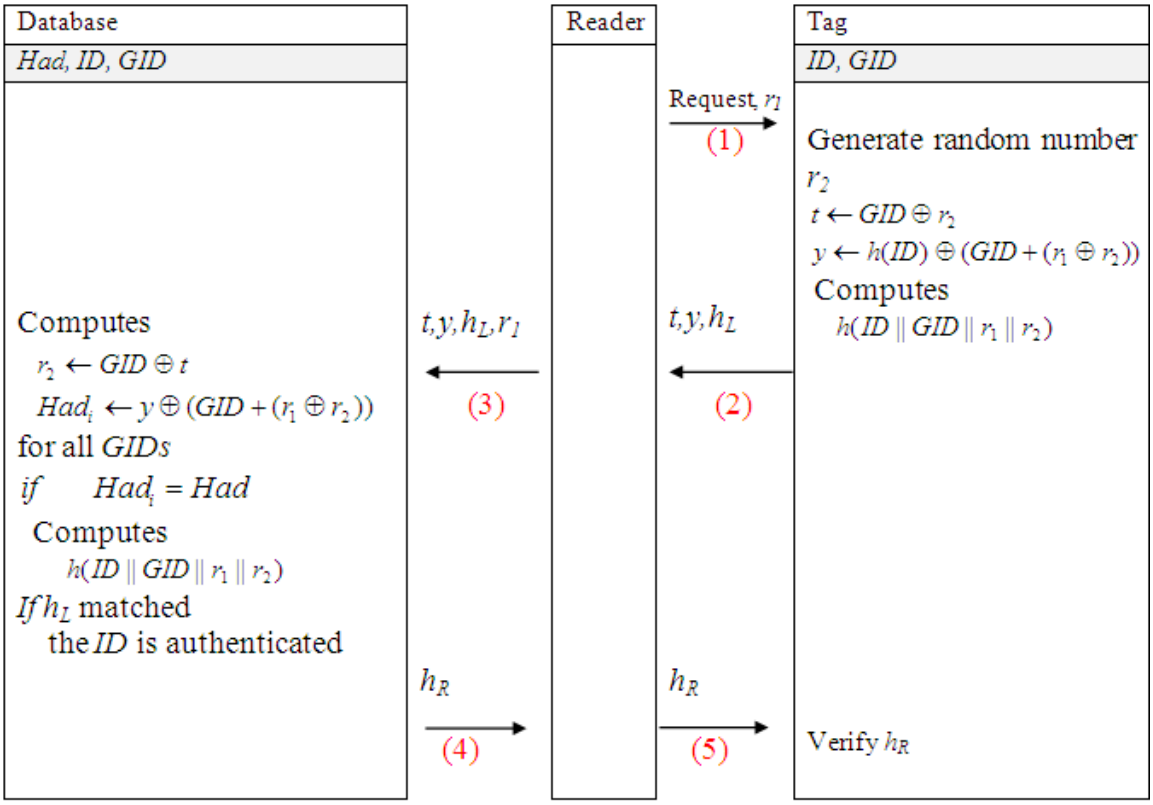

Figure 4-3: The Proposed SUAP3 Protocol

The steps in the authentication protocol are as follows.

1. The reader generates a random number r_1 and sends it to the tag.
2. Receiving the number r_1 the tag generates another random number r_2.

   if r_1 *or* r_2 *is* 0 *stop protocol*

   otherwise performs the following computations

   $t \leftarrow GID \oplus r_2$

   $y \leftarrow h(ID) \oplus (GID + (r_1 \oplus r_2))$ *Computes* $h(ID \| GID \| r_1 \| r_2)$

   The tag then sends the value of *y*, *t* and h_L to the reader.

   Where h_L is the left half of $h(ID \| r_1 \| r_2 \| GID)$

3. The reader then sends the value of y, r_1, h_L and t to the back-end database.
4. The back-end database calculates the following for all *GID*s

   $r_2 \leftarrow GID \oplus t$

   $Had_i \leftarrow y \oplus (GID + (r_1 \oplus r_2))$

   $h(ID)$ is the address of the record containing the *ID* where $Had_i = h(ID)$

   Lookup the address Had_i in the database

   If $Had_i = Had$ for any *ID* retrieves the *ID* from the record

   Then the back-end database *Computes* $h(ID \| r_1 \| r_2 \| GID)$

   If h_L matches the tag is authenticated

   Sends h_R to the reader

   Where h_R is the right half of $h(ID \| r_1 \| r_2 \| GID)$
5. The reader forwards the h_R to the tag
6. If the received h_R matches, the reader is authenticated.

4.1.3 Analysis

To evaluate the proposed protocol this can be analyzed in two ways. Firstly is privacy and security analysis and secondly is its efficiency analysis. The privacy and security analysis includes information leakage, location privacy, impersonation and replay attack, Denial of Service (DoS) and traceability. In efficiency analysis the storage, computation and communication costs are compared with existing related protocols.

4.1.3.1 Privacy and Security Analysis

The privacy and security of the proposed protocol is analyzed against the identified threats as follows.

- **Information Leakage:** In SUAP1 protocol, the adversary must be authenticated to access any sensitive information from a tag. To authenticate the systems an adversary must know *ID*, x and r_2 to access any information from the tag. The SUAP2 protocol has additional *GID* secret to make the response more unpredictable. The SUAP3 uses the *GID* as a secret

instead of x. The combination of r_1 and r_2 makes the response y so unpredictable that the adversary can only guess the value of h_R and h_L. The advantage of an adversary is at most $\frac{1}{2^l}$, which is negligible for l=96 or more.

- **Location Privacy:** The responses from the tags are always changing in every new session. The value of t, y and h_L cannot be linked with any particular tag in the SUAP1 and SUAP2. In the SUAP3 the value of y and h_L also cannot be linked with any particular tag. The protocols ensure location privacy by using new values of r_1 and r_2 each time. Even if a malicious reader sends a same random value r_1 all the times, a tag transmits the refreshed values that are refreshed by r_2 and x.

- **Impersonation and Replay attack:** The protocols work in a complete challenge-response fashion by mutual authentication. When a tag reaches within the range of a reader, the reader queries with a random value to the tag. An adversary may also request a tag with a random number. Without knowing *ID*, hash function, secret x and random number r_2 generated by the tag, the adversary cannot find $h(ID)$. In SUAP2 and SUAP3 the group identifier *GID* also makes the response more unidentifiable. For each session the tag gives new value of y that is totally indistinguishable and different from other sessions. So impersonation and replay attack is nearly impossible in practical scenario. Impersonation and replay attack could be possible if the attacker waits for a matched response (same h_L) from the tag and replays the h_R to authenticate itself. Such repeating hash response could only be reproduced once in 2^l responses (where the responses are uniformly random in nature) as the length of the hash response is l.

- **Denial of Service (DoS):** Since the *ID* and the secret are never changed in the proposed protocols, if the attacker prevents the last flow to the tag from the reader it will not cause any problem of desynchronization. Consequently the DoS attack cannot break the synchronization of the system.

- **Traceability:** Attacker cannot identify the past and future interactions. The schemes SUAP1, SUAP2 and SUAP3 are fully protected from future forward and backward traceability. The attacker has no access over r_2, and the combination of r_1, r_2 and hash function. The responses are always anonymous and the attacker does not know about the *ID* and the secret *x* or *GID*. So the previous, present and future interactions are all indistinguishable. The attacker cannot identify the past and future interactions.

4.1.3.2 Efficiency Analysis

For efficiency analysis the storage, communication and computation cost of the proposed protocols are compared with other protocols. The storage cost indicates the storage requirements in the tag, database and the reader. The communication cost means the length of bits the tag and the reader send during the authentication process. The computation cost is the maximum computations require in the tag and the database during the execution of the authentication protocol. Various existing authentication protocols are selected to compare with the proposed protocols in Table 4-1.

Table 4-1 Efficiency Analysis

Efficiency Criteria		**LCAP**	**CRAP**	**OHLCAP**	**EOHLCAP**	**Proposed Protocols**		
						SUAP1	**SUAP2**	**SUAP3**
Storage	Tag	$1l$	$1l$	$5l$	$3l$	$2l$	$3l$	$2l$
	Reader	-	-	-	-	-	-	-
	Database	$6l$	$1l$	$4l$	$3l$	$3l$	$4l$	$3l$
Computation	Tag	$2h$	$3h$	$1h(+A_1)$	$1h(+A_2)$	$2h$ $(+A_2)$	$2h$ $(+A_3)$	$2h$ $(+A_3)$
	Reader	-	-	-	-	-	-	-
	Database	$1h$	$(\frac{N}{2}+1)h$	$1h+\varepsilon_1$	$(\frac{m_i+1}{2})h+\varepsilon_2$	$1h+\varepsilon_3$	$1h+\varepsilon_4$	$1h+\varepsilon_5$
Communication	Tag-to-Reader	$1.5l$	$2l$	$2.5l$	$2.5l$	$2.5l$	$2.5l$	$2.5l$
	Reader-to-tag	$0.5l$	$0.5l$	$0.5l$	$0.5l$	$0.5l$	$0.5l$	$0.5l$

A_1,A_2,A_3: Additional XOR and Add operations in the tag ε_1, ε_2, ε_3, ε_4, ε_5: Small operations in the database

In Table 4-1 the LCAP [Lee et al. 2005] performs better than other protocols for almost all criteria but it suffers from traceability problem and it is not suitable for ubiquitous computing. The proposed protocols show better performance because it requires less tag side and database side storage and gives protection from all known attacks. The storage requirement for tag and the

database are 2*l*, and 3*l* respectively in SUAP1 and SUAP3, whereas OHLCAP [Choi et al. 2005] requires 5*l* and 4*l* respectively. CRAP [Rhee et al. 2005] uses only 1*l* storage for tag but it needs $(\frac{N}{2}+1)$ hash operations which is practically unsuitable because in ubiquitous environment the value of *N* is extremely high and does not divide the tag in groups. It needs many hash operations and hence requires long search time to obtain the tag information in the database. Similarly the EOHLCAP [Ha et al. 2007] requires 3*l* storages in the tag side and 3*l* storages in the database side but requires a large number of hash operations for a group. This is also high for a group having a large number of tags. The main computation costs in the tags are the hash operations. OHLCAP requires 1 hash operations and additional operations A_1 which are four xor operations in the tag. EOHLCAP also requires 1 hash operation and additional operations A_2 which are two xor operations in the tag. The proposed protocols require two one-way hash operations in each tag. SUAP1 requires additional operations A_2 which are two xor-operations. Both SUAP2 and SUAP3 require additional operations A_3 which are three xor-operations in the tag. In each protocol the tag requires one addition operation. Since both xor-operation and addition operation are very simple bits operation, hardware embodiment of these operations is simpler than one-way Hash function. Therefore, the proposed protocols are suitable to a low-cost RFID tag systems. ε_1, ε_2, ε_3, ε_4 and ε_5 are additional operations other than hash functions in the corresponding databases as shown in Table4-1.

4.1.4 Simulation Experiment and Evaluation

To validate the proposed protocols, simulation experiments have been conducted. The privacy and security protections are ensured with the hash functions and random numbers. A hash function is a one-way function for which information leakage is not possible from the hash response. Mathematically the probability of success to guess the value of a response using a brute-force technique is at most $\frac{1}{2^l}$. In this experiment the value of *l* takes different values i.e. 16, 32, 64 and 96. However, many combinations of the hash inputs can give the same response that can be used by the adversary to impersonate the RFID systems. This is the main reason to conduct the simulation program. The objective of the simulation program is to verify the protection for impersonation, replay attack and location privacy. It checks the response *y* if it recurs more than once for one tag during the attacks by an adversary in a given number of attempts. If the same response is generated

for any given random number pair it can be used by the adversary for impersonation and replay attack and the location privacy of the tag may be broken.

The impersonation and replay attack are simulated using Monte Carlo simulation method. To replay the hash value h (h_L|| h_R) for a particular *ID* and *GID*, hash responses are generated for 10^{11} times with the same *ID* and *GID* and different set of r_1 and r_2. The hash value generated at ith attempt h_i is considered vulnerable for impersonation and replay attack if h_i=h. The generated random sequences for r_1 and r_2 are tested for uniform random distribution using chi square test to ensure the validity of the simulation using Monte Carlo method. The number of matches found is recorded to generate the performance results. For a particular data length 10 simulations are executed using different set of random numbers and the possible impersonation and replay attacks are observed in the simulation. The averages of the successful replay attacks are reported in Table 4-2.

Table 4-2 Attacker's Success for one Tag

No.	Number of Attempts	Data Length l (bits)	Expected Number of Matches	Average Number of Matches (Attacker's Success)			
				EOHLCAP	SUAP1	SUAP2	SUAP3
1	10^{11}	16	1525878.91	1532979.81	1536442.83	1535009.84	1526520.77
2	10^{11}	32	23.28	21.34	20.30	21.20	20.81
3	10^{11}	64	$5.42\text{x}10^{-9}$	0	0	0	0
4	10^{11}	96	$1.26\text{x}10^{-18}$	0	0	0	0

A simulation program in Turbo C++ compiler has developed. It runs in a desktop computer of Intel (R) Core 2 Duo. Processor speed is 2.93GHz and memory 3.46 GB. The operating System was Windows XP professional. The objective of the simulation program was to check the anonymity of the response for one tag.

The output of a hash function is the same for the same random number pair. Some different random number pairs may also give the same response. The objective is to ensure unique response for different inputs of random number pair so that an adversary is unable to use any response at later stage to access the tag or the reader. We select one tag and generate a response for two random numbers as in SUAP1, SUAP2, SUAP3 and EOHLCAP. Then the program attempts 10^{11} times to check that how many times the same response is generated. This is the role of an adversary. In each attempt a new response is generated with a new pair of random number. The average number of times a similar response generated in SUAP1, SUAP2, SUAP3 and EOHLCAP are given in Table 4-2. The expected number of matches is also reported in a column to compare the obtained result.

The value of the expected number of matches are calculated using the analysis of repeating hash response presented for replay attack in Section 4.1.3.1 and it is calculated as $10^{11}/2^{l}$. All the selected protocols show almost similar results. The number of matches represents the success of the adversary to attack the tag. The experiment was conducted for 16, 32, 64 and 96 bits of secrets, random number and *ID*. The success of the adversary is found for 16 and 32 bits since many occurrences of the same response are found. For 64 and 96 bits the adversary cannot break the privacy and security of the tag for an extremely large number of attempts. There was no recurrence of the same response for 64 bits and 96 bits for the specified number of attempts, i.e. 10^{11} times. The summary of the result for SUAP1, SUAP2 and SUAP3 and EOHLCAP is shown in Table 4-3. Simulation experiments were not performed for LCAP, OHLCAP and YA_TRAP* (T3) protocols since these are not protected against all the privacy threats [Choi et al. 2005, Ha et al. 2007, Tsudik 2007]. CRAP is also not included since it requires many hash operations [Choi et al. 2005].

The results shown in Table 4-3 indicated that for 64 and 96 bits there is no matching response and the results were always dissimilar for the different sessions. If the result is unique the adversary cannot use it for replay attack, impersonation attack and location tracking. For 16 and 32 bits there were some recurrences of the same response which was due to two reasons. Firstly it produces the same random number pairs and secondly it produced similar responses for some other combination of random number pairs. With 64 and 96 bits the tag produced unique response for a tag.

Table 4-3 Attacker's Success Summary for SUAP1, SUAP2, SUAP3 and EOHLCAP

No. of Queries	Attacker's Success (Number of matches)		
	Data length (16 bits)	Data length (32 bits)	Data length (64/96 bits)
10^{11}	>0	>=0	0

According to the privacy and security analysis in the Section 4.1.3.1 and the simulation results the summary of the privacy and security properties are given in Table 4-4.

Table 4-4 Privacy and Security Comparisons

Property	LCAP	CRAP	OHLCAP	EOHLCAP	YA_TRAP*	Proposed Protocols		
						SUAP1	SUAP2	SUAP3
Information privacy	Y	Y	Y	Y	Y	Y	Y	Y
Location Privacy	N	Y	Y	Y	Y	Y	Y	Y
Impersonation	A	Y	N	Y	Y	Y	Y	Y
Replay attack	Y	Y	N	Y	Y	Y	Y	Y
Message Interception	Y	Y	Y	Y	N	Y	Y	Y
Backward Traceability	Y	Y	N	Y	N	Y	Y	Y
Forward Traceability	Y	Y	N	Y	N	Y	Y	Y

Y: Provided A: provided under assumption N: Not Provided

The privacy and security properties of the proposed protocols are compared with five other schemes. The five schemes were chosen because all of these protocols involved tag authentication. LCAP and YA_TRAP* involves secret update process but the other three protocols CRAP, OHLCAP and EOHLCAP do not support secret updates. Proposed protocols are more similar to CRAP, OHLCAP, EOHLCAP than LCAP and YA_TRAP* since all these protocols support authentication in ubiquitous computing environment and do not update the identifier and the secret value. Table 4-4 shows that, the proposed protocols provided protections from the identified privacy and security threats.

4.2 Efficient Mutual Authentication Protocol

In group-based security protocol the privacy and security of the RFID system is managed by group secrets. In practical it is difficult to ensure the privacy protection of a secret value that is managed by a group in some distributed environment since it is handled by various groups of interests. This section proposes a novel Efficient Mutual Authentication Protocol (EMAP) which provides the privacy and security in an efficient manner using individual secret for each tag. The evaluation also indicates that it requires low storage and computation but offers larger ranges of security protection.

This research aims to propose Efficient Mutual Authentication Protocol for RFID Systems to address the privacy and security issues using static identifier and secret for ubiquitous computing

environment. The OHLCAP and the proposed SUAP1, SUAP2 and SUAP3 in Section 4.1 use static identifiers and common secret for a group. In this section the proposed EMAP uses individual tag secret for each tag to ensure the privacy and security more particularly and efficiently.

This proposed EMAP protocol is related to two popular works OHLCAP and Enhanced OHLCAP. OHLCAP works in ubiquitous environment. It also uses a one-way hash function for privacy and security of the tag. Ha et al.[2007] indicated its security weakness and proposes an enhanced OHLCAP (EOHLCAP) scheme. The authors showed that this protocol is vulnerable to traceability attack and impersonation attack because of its counter for two successive sessions. In EOHLCAP to prevent traceability a random number is used in a tag instead of a counter value. Due to this random number instead of a counter, the tracing attack and impersonation attack by maliciously updating the random number become impossible.

4.2.1 The Propsoed Efficient Mutual Authentication Protocol

In this section, a new Efficient Mutual Authentication Protocol (EMAP) is proposed using a one-way hash function, static identifier, an individual secret and the randomized hash function in the RFID systems. The protocol works in ubiquitous computing environment suitably since it uses the static identifier and does not change any secrets in authentication process. It offers a design with low storage using only two data fields in the tag side by eliminating the group index *GI*, group secret value *k* and the counter value *c* used in OHLCAP from the tag and the database side. The proposed protocol ensures protections from all the identified privacy and security threats and also avoids the large number of hash computations that might incur due to the introduction of an individual secret value in each tag.

Notations

The notations used in this protocol are as follows:

- h A one-way hash function, $h:\{0,1\}^* \rightarrow \{0,1\}^l$
- l The length of an identifier
- r_1 Random number in $\{0,1\}^l$

r_2 Random number in $\{0,1\}^l$

ID Tag identifier

S Secret of the individual tag

Had Hash address h(*ID*), acting as an index

$\oplus$ XOR operator

|| Concatenation operator

$\leftarrow$ Assignment operator

+ Modular addition by *mod* $(2^l - 1)$

System Set-up

The EMAP also uses the static identifier and secret. It uses only one secret *S* in the tag and the database. The protocol uses the hash function *h*(*ID*) to encrypt the *ID*. The hash response is also used as a hash address for the tags in the database. The system setup of the EMAP protocol is as follows:

Tag: Each tag contains the following fields:

ID: Tag Identifier

S: Secret value of a tag

Reader: Reader does not contain any fields.

Back-end Database: Back-end database contains the following fields:

ID: Tag Identifier

S: Secret value of a tag

Had: Hash address *h*(*ID*), acting as an index

EMAP Operations

The EMAP protocol shown in Figure 4-4 reduces the number of fields in the tag by removing three data fields *GI, c* and *K* from the OHLCAP and uses only two data fields *ID* and *S* in the tag side. The database uses three data fields *Had, ID* and *S*. The proposed protocol uses the hash value *Had* as the hash address in the database to search the tag information. However, this hash address is sent to the reader with an encryption so that an adversary cannot track the tag. For authentication

between the reader and the tag it uses a different hash value $h(ID \| r_1 \| r_2 \| S)$ so that the information in the tag is always secure and the valid tag is identified correctly. The random number r_1 is transmitted in plaintext but the r_2 is transmitted by encrypting with the secret value S.

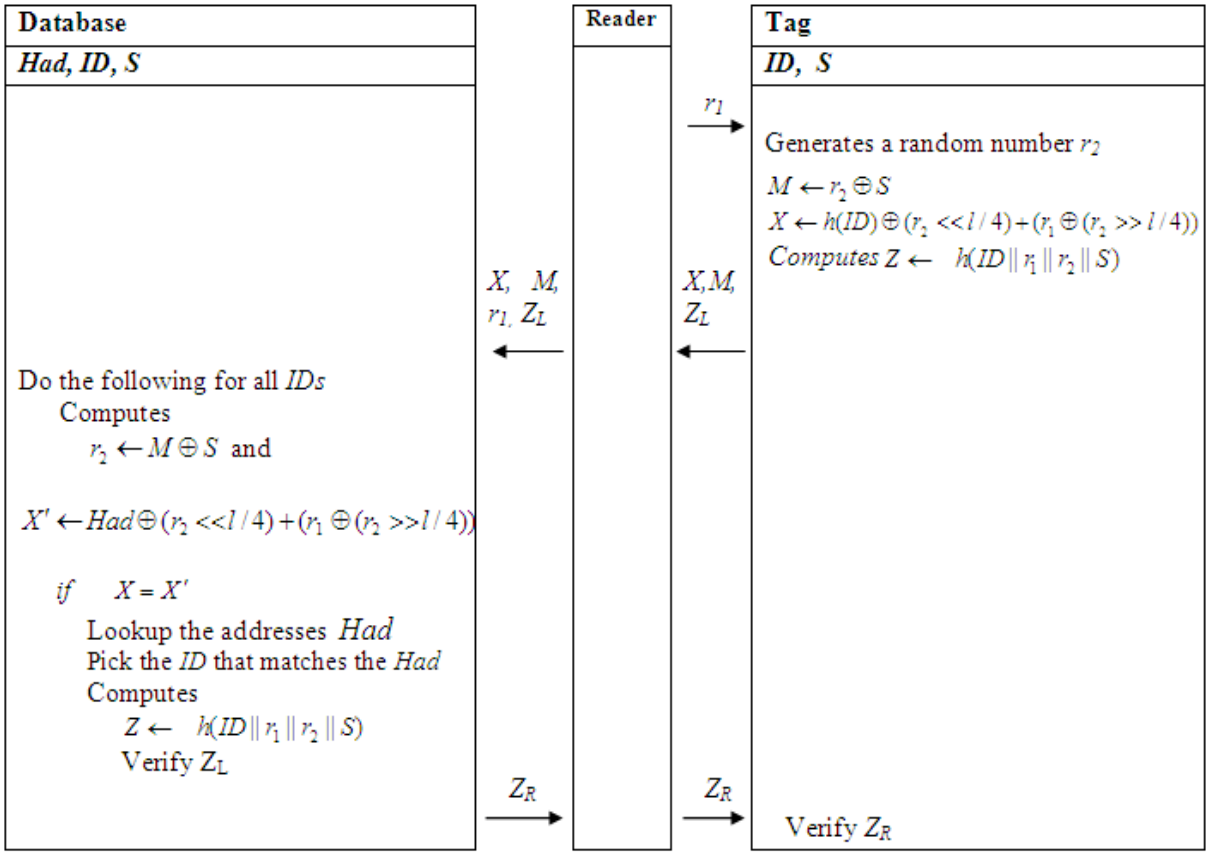

Figure 4-4: The Proposed EMAP Protocol

The steps in the authentication protocol are as follows:

1. A reader selects a random number r_1 and sends a request with r_1 to the tag.
2. After receiving the random number r_1 the tag will generate another random number r_2.

The tag computes $M \leftarrow r_2 \oplus S$

$$X \leftarrow h(ID) \oplus (r_2 << l/4) + (r_1 \oplus (r_2 >> l/4))$$

$$Z \leftarrow h(ID \| r_1 \| r_2 \| S)$$

and sends the values of M, X and Z_L to the reader. Z_L is the left half of Z.

3. The reader then sends r_1, M, X and Z to the back-end database.
4. The back-end database then computes for all IDs in database

$r_2 \leftarrow S \oplus M$.

$X \leftarrow had \oplus (r_2 << l/4) + (r_1 \oplus (r_2 >> l/4))$

if $X = X'$

Lookup the addresses *Had*

Pick the *ID* that matches the *Had*

Computes $Z \leftarrow h(ID \| r_1 \| r_2 \| S)$

Verifies Z_L

If the *ID* is authenticated the database sends Z_R to the reader. Z_R is the right half of *Z*.

5. The reader forwards Z_R to the tag.
6. The tag verifies Z_R.

Comparing with the security scheme OHLCAP, the proposed EMAP protocol has the following advantages (see Tables 4-5 and 4-6):

1. Uses less storage in both tag side and database side.
2. Improves privacy and security due to that the proposed protocol has removes the counter field used in OHLCAP and uses a random number.
3. Insures the individual security using the individual tag secret value instead of the group secret value.

Comparing with the security scheme EOHLCAP, the proposed EMAP protocol has the following advantages (see Tables 4-5 and 4-6):

1. Uses the less storage in the tag side.
2. Insures the individual security using the individual tag secret value instead of the group secret value.
3. Reduces the hash computation.

4.2.2 Evaluation

To evaluate the proposed protocol privacy, security and efficiency are analysed. Firstly is privacy and security analysis and secondly is efficiency analysis. The privacy and security analysis includes information leakage, location privacy, impersonation and replay attack, Denial of Service (DoS)

and traceability. In efficiency analysis the storage, computation and communication costs are compared with existing related protocols.

4.2.2.1 Privacy and Security Analysis

The attack model is defined in the following way:

A : An adversary

R: Reader

T: Tag

It is assumed that the adversary disguises as a reader R_A and ID_A, S_A will be used by the adversary as fake *ID* and secret. $h_L(ID \| r_1 \| r_2 \| S)$ will be used as the left half Z_L and $h_R(ID \| r_1 \| r_2 \| S)$ as the right half Z_R of *Z*. The proposed protocols have the following privacy and security properties:

Information Leakage: In the proposed protocol authentication is required to obtain any sensitive information from a tag. In EMAP the adversary must know the *ID* and *S* to authenticate the system. The *ID* is never sent in plaintext. The combination of r_1 and r_2 with *S* and *ID* make the hash response unpredictable so that the adversary does not have any information about the secret. The adversary disguises as a reader R_A and tries to extract the ID_A and S_A. After receiving the response Z_L from the tag or Z_R from the reader the adversary can try to compute the secrets and send the request to the tag and failed, where Z_L is the left half and Z_R is the right half of $Z \leftarrow h(ID \| r_1 \| r_2 \| S)$. The adversary A may also collect the responses from the tag and the readers to use them for next session but due to two random numbers the responses are always unpredictable and authentication is not possible. For example the adversary takes the responses from the tag as follows:

$$T \Rightarrow A(R_A): \quad M \leftarrow r_2 \oplus S,\ X \leftarrow h(ID) \oplus (r_2 << l/4) + (r_1 \oplus (r_2 >> l/4)),\ Z_L$$

It is not possible for the adversary to extract the value *S* from the responses since r_2 is never sent in plain text. The value of *ID* is always sent in a hash function. So the information leakage is not possible.

Location Privacy: The response cannot be linked with any particular tag. The protocol ensures location privacy by using new values of r_1, r_2 each time. The EMAP refreshed the value using the r_1, r_2 and *S*. The adversary A can receive the following response from the tag in one session.

$$T \Rightarrow \mathrm{A} : h_L(ID \| r_1 \| r_2 \| S)$$

In the next session the adversary A will receive a different response from the tag since the r_1 and r_2 are changed and the response is also changed. Therefore, the new response shown below is not matched with the previous one.

$$T \Rightarrow \mathrm{A} : h_L(ID \| r_1' \| r_2' \| S)$$

The adversary can send fixed query with fixed r_1. In that case the response is refreshed by r_2 by the tag and the response is still anonymous.

$$T \Rightarrow \mathrm{A} : h_L(ID \| r_1 \| r_2' \| S)$$

In subsequent all sessions the response from the tag are anonymous hence location privacy is protected and tracking is not possible. The adversary may also try to use the value of *M* and *X* to extract the secret *S*. Since the random number r_2 is passed secretly the value of *M* and *X* are always unpredictable.

Impersonation and Replay Attack: The protocol works in a complete challenge-response method by mutual authentication. When a tag reaches within the range of a reader, the reader sends a query request with a random value to the tag. An adversary may also make a request to a tag with a random number. However, without knowing the *ID*, the hash function, secret *S* an adversary is unable to impersonate. For each session the tag generates a new response which is totally indistinguishable and different from other session and subsequently the impersonation and replay attacks are not possible.

The adversary A can receive the responses from the tag and the reader in one session for impersonation and replay attack.

$$T \Rightarrow \mathrm{A} : h_L(ID \| r_1 \| r_2 \| S)$$

$$R \Rightarrow \mathrm{A} : h_R(ID \| r_1 \| r_2 \| S)$$

In the next session the adversary A may try to use this response to attack the tag. The adversary A can have two approaches. It can use the same response to attack the tag or it can try to guess the value of *ID* and *S*. Since the r_1, and r_2 are all changed and the secret is also unknown the response will not match. Both the attacks are shown as follows:

(i) First approach

The random number r_1 is sent in plain text. It is assumed that the adversary A can track and receive it.

$A(R_A) \Rightarrow T : h_L(ID \| r_1 \| r_2' \| S)$

T: Verify. $r_2 \neq r_2'$

$T \Rightarrow$ Authentication fail.

(ii) Second approach

The adversary can try to assume the values *ID* and *S* and use fake ID_A and S_A.

$A(R_A) \Rightarrow T : h(ID_A \| r_1 \| r_2' \| S_A)$

T: Verify. $ID_A \neq ID, \quad S_A \neq S, r_2 \neq r_2'$

$T \Rightarrow$ Authentication fail.

Message Interception or DoS Attack: The protocol uses static identifier and secret. Since the values are not changed in the authentication process the protocol does not face any update anomalies. If the adversary is able to prevent the last transmission to the tag from the reader it will not face any synchronization problem.

Traceability: An adversary is unable to identify the tag from its response because each time it gives a different value which is non traceable from other responses. Alternatively, for traceability an adversary needs to know the secret *ID* or *S*. *ID* is secure due to the one-way hash function $h(ID \| r_1 \| r_2 \| S)$ and the secret *S* is also sent by encryption with a new random number r_2 in each session. Both the schemes are fully protected from the future forward and backward traceability. It is also not possible to trace the expression $X \leftarrow h(ID) \oplus (r_2 << l/4) + (r_1 \oplus (r_2 >> l/4))$ since r_2 is passed in secret and changed in every session. The summary of privacy and security comparisons are given in Table 4-5.

Table 4-5 Privacy and Security Comparisons

Property	LCAP	CRAP	OHLCAP	EOHLCAP	**Proposed EMAP**
Information privacy	Y	Y	Y	Y	Y
Location Privacy	N	Y	Y	Y	Y
Impersonation	A	Y	N	Y	Y
Replay attack	Y	Y	N	Y	Y
Message Interception	Y	Y	Y	Y	Y
Backward Traceability	Y	Y	N	Y	Y
Forward Traceability	Y	Y	N	Y	Y

Y: Provided A: provided under assumption N: Not Provided

4.2.2.2 Efficiency Analysis

Storage, communication and computation cost are considered for efficiency analysis. Various existing authentication protocols are compared with the proposed protocols. LCAP requires less storage in the tag side but it does not work in a ubiquitous environment since the identifier is updated after every authentication process. It also has location privacy problem. The EMAP protocol shows improved performance as shown in Table 4-6 because it requires less tag side and database side storage than OHLCAP and EOHLCAP protocols and gives protection from all the identified threats.

The storage requirements for the tag and the database are 2l and 3l respectively in EMAP which is the lowest in all the protocols except CRAP. CRAP gives protections from all the attacks but it needs $(\frac{N}{2}+1)$ hash operations for N tags, which is costly because the value of N may be extremely high and many hash computations will make the protocol slower. EOHLCAP also gives protections from all the identified threats but it also requires (m_i +1)/2 hash operations for a number of tags in a group. m_i is the number of tags in the ith group and this number also may be very high.

Table 4-6 Efficiency Analysis

Efficiency Criteria		**LCAP**	**CRAP**	**OHLCAP**	**EOHLCAP**	**Proposed EMAP**
Storage	Tag	1l	1l	5l	3l	2l
	Reader	-	-	-	-	-
	Database	6l	1l	4l	3l	3l
Computation	Tag	2h	3h	1h+A	1h+A	2h+A
	Reader	-	-	-	-	-
	Database	1h	$(\frac{N}{2}+1)h$	1h+ε	$(\frac{m_i+1}{2})h+\varepsilon$	1h+ ε
Communication	Tag-to-Reader	1.5l	2l	2.5l	2.5l	2.5l
	Reader-to-tag	0.5l	0.5l	0.5l	0.5l	0.5l

A: Additional XOR and Add operations in tag ε: Small operation in back-end database

4.2.3 Simulation Experiment

Though the proposed protocols are logically and mathematically secret from various attacks the adversary can go for repeated replay attack to take the advantage of generation of similar response for a number of different inputs. If the adversary can match any response it can be used for

impersonation and replay attack and can break the location privacy. To validate the proposed protocol, simulation experiments have been conducted. A simulation program in Turbo C++ compiler was developed for desktop computer of Intel (R) Core 2 Duo with processor speed of 2.93GHz and memory of 3.46 GB. Windows XP Professional was used as the operating system. The objective of the simulation program was to check the anonymity of the response for one tag. The output of a hash function is the same for the same random number pair. The objective is to ensure unique response for different inputs of random number pair so that an adversary is unable to use any responses at later stage to access the tag or the reader. The program checks to match a response of a tag with the responses of different sets of random numbers. Two protocols EMAP and EOHLCAP were selected for the experiment. The number of times a similar response is generated is given in Table 4-7 for 10^{11} attempts. The summary result is shown in Table 4-8.

Table 4-7 Attacker's Success for one Tag

Exp No.	Number of attempts	Data Length	Number of Matches (Attacker's success)	
			EOHLCAP	**Proposed EMAP**
1	10^{11}	16	1539054	1545003
2	10^{11}	16	1536078	1537687
3	10^{11}	16	1536965	1535689
4	10^{11}	32	0	0
5	10^{11}	32	40	0
6	10^{11}	32	0	42
7	10^{11}	32	43	0
8	10^{11}	32	0	39
9	10^{11}	32	0	0
10	10^{11}	32	0	0
11	10^{11}	32	0	0
12	10^{11}	64	0	0
13	10^{11}	64	0	0
14	10^{11}	64	0	0
15	10^{11}	64	0	0
16	10^{11}	96	0	0
17	10^{11}	96	0	0
18	10^{11}	96	0	0
19	10^{11}	96	0	0
20	10^{11}	96	0	0

The summary results of the simulation experiments were same for both the proposed protocol EMAP and the selected protocol EOHLCAP. The experiments were conducted for 12, 16, 32, 64

and 96 bits of secrets, random number and *ID*. The results shown in Table 4-8 indicated that for 64 and 96 bits there is no matching for a response of a tag. It means the response were always unique. If the result is unique the adversary cannot use it for replay or any other attack. For 12, 16 and 32 bits there were some recurrences of the same response.

Table 4-8 Attacks and success of an adversary on one tag for EMAP and EOHLCAP

No. of Attempts	Attacker's Success		
	Response length (16 bits)	Response length (32 bits)	Response length (64/96 bits)
10^{11}	>0	>=0	0

The recurrence of the same response was due to two reasons. Firstly, it produces the same random number pairs and hence the same response. Secondly, it produces similar responses for some other combination of random number pairs. If an adversary uses this response for any of these combinations of random number pairs it may impersonate as a valid reader.

Any simulation experiments for LCAP, CRAP and OHLCAP protocols were not performed since it is already mentioned that logically and mathematically the LCAP, OHLCAP are not protected against all the privacy threats [Choi et al. 2005, Ha et al. 2007]. CRAP is also protected from all the threats but it requires a large number of hash operations. The response of EOHLCAP is also similar in nature as in the proposed protocols and shows the same results.

4.2.4 Hospital Case Study

This section presents a case study of a hospital RFID System to explain how the proposed EMAP can be implemented to ensure privacy and security. In the medical environment, the security and privacy problem will be crucial to RFID based medical application. The privacy issue with tagged patient cards involves the risk of exposing the information, such as trace of personal location, information of personal health and clinical history. Through the tag the private data of a person can be tracked and the personal information can be captured which could be a violation of privacy under the Data Protection Act 1998. Many security threats are identified in RFID system in hospitals [Jules et al. 2005]. The details of the hospital privacy and security scenario are given in Chapter 8. In this case it is assumed that there are *K* readers are connected to the database. There are *N* tags. It

is assumed that there is no classification in the tag side. The database may classify the tag according to the patient disease or other criteria. The Figure 4-5 shows the tag, reader and the database architecture for the hospital system. The database only shows the basic part of the tags. This can be used to link with other information of the patient and hospital. All the readers read the tags and verify the tag information with the database.

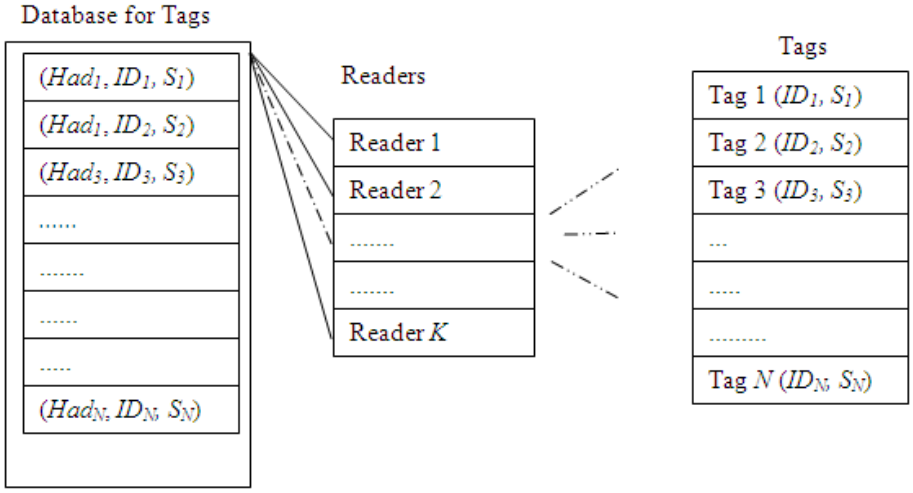

Figure 4-5: Security Architecture of the Hospital RFID Systems

It is assumed a reader $Reader_i$ initiates authentication protocol with Tag_j.

1. $Reader_i$ generates a random number r_1 and sends a request with r_1 to the tag.
2. After receiving the random number r_1 the tag Tag_j generates another random number r_2.

The tag computes M, X and Z and sends the values of M, X and Z_L to the reader. Z_L is the left half of Z.

3. The reader then sends r_1, M, X and Z to the back-end database.
4. The database verifies the tag. If the response from the tag is forged by the adversary the database can recognise it. If it does not match with the tag records stored in the database then the database recognize the tag as a forged or external tag. To do it the database also computes the X and Z using the database field S and Had with received M. The database then sends the Z_R to the reader, where Z_R is the right half of Z.
5. The reader forwards Z_R to the tag.
6. The tag verifies Z_R. If any adversary forges the response the tag can also recognise it.

There are several readers are connected in the network systems of the hospital to communicate with the database server. The reader and tag authenticate each other using the hash responses Z_L and Z_R. The information is fully secured in this protocol. The *ID* is never transmitted in plaintext and the one way hash function with two random numbers makes the response *Z* fully unpredictable. Only the valid reader can authenticate the tag using the information stored in a secured database. An authorized reader cannot track or authenticate any tag related to patient, doctor or nurse etc.

4.3 Conclusion

Three group-based efficient and secure authentication protocols are proposed to protect privacy for the low-cost RFID system in ubiquitous computing environment. The privacy and security problem of OHLCAP is overcome in these protocols. SUAP1 is suitable for the organization having small number of tags. SUAP2 and SUAP3 are for medium and large organizations having many departments. All the proposed schemes require only two one-way hash function operations that make them very efficient. The tag search time in the database is reduced by using the hash value as the address of the corresponding tag. EOHLCAP also overcomes the problem in OHLCAP and protects the RFID system from most of the attacks but it requires many complex hash operations. In the proposed protocols the number of hash operations has been reduced in database side and ensure privacy and security protections from the identified threats. The storage requirements in SUAP1 and SUAP3 are also less than OHLCAP and EOHLCAP protocols. The comparison shows that the proposed protocols are both secure and efficient than other schemes and have practical advantages over them because these are simple and provide greater number of privacy and security protection for less storages and computations.

A new efficient and secure authentication protocol EMAP is also proposed using an individual secret value for each tag to protect privacy for low-cost RFID systems. It also uses static identifier so that it can work in a ubiquitous computing system. The proposed EMAP requires only one one-way hash function in the database and two one-way hash functions in the tag side. The storage requirements for the tag and database are also low i.e. $2l$ and $3l$ respectively. Due to two random numbers, one generated in the reader and the other generated in the tag, a tracing attack and impersonation attack become impossible. It has practical advantages over other protocols because it is simple and provides a larger range of privacy and security protections. The proposed protocol is

robust to the identified threats, such as information leakage, an impersonation attack, replay attack, DoS attack and location tracing problem.

Part of the substance of this chapter has been published in the following journal:

Morshed, M.M., Atkins, A.S., Yu H. 2010, 'Secure Ubiquitous Authentication Protocols for RFID System', EURASIP Journal on Wireless Communications and Networking.

Part of the substance of this chapter has been accepted in the following journal:

Morshed, M.M., Atkins, A.S., Yu, H. 2011, 'Efficient Mutual Authentication Protocol for RFID Systems', IET Communications.

Chapter 5 Proposed Efficient and Secure Authentication Protocol (ESAP)

5.1 Introduction

This chapter proposes a hash-based Efficient and Secure Authentication Protocol (ESAP) protocol using a monotonically increasing timestamp and a random number to protect the privacy and security of the RFID systems effectively and efficiently. It also identifies different advantages of using the timestamp to ensure the privacy and the security of the RFID systems.

The use of RFID tags may cause privacy violation of users carrying an RFID tag because of the unique identification number of the RFID tag. This can result possible privacy threats such as information leakage of a tag, traceability of the consumer, denial of service attack, replay attack and impersonation of a tag. There are some challenges in providing privacy and security in the RFID tags due to the extremely limited computation, storage and communication ability of passive RFID tags. Many research works have already been conducted using hash functions and random numbers. As the same random number can recur many times the adversary can use the response derived from the same random number for replay attack and it can cause a break in location privacy. This section proposes an RFID authentication protocol ESAP using a monotonically increasing timestamp, a tag side random number and a hash function to protect the RFID system from adversary attacks. The proposed protocol also indicates that it requires less storage and computation than previous existing RFID authentication protocols but offers a larger range of security protection. A simulation experiment is also conducted to verify some of the privacy and security properties of the proposed protocol.

5.2 Related Works

In most of the RFID authentication protocol to make the response unidentifiable one or two random number are used with hash function. Tsudik [2006] described an RFID identification protocol that provides a basic level of tag identification using time-stamps. It will be referred to as T1. This is a widely acknowledged authentication protocol that places only a small burden on the back-end

server and uses monotonically increasing timestamp which makes it secure against tracking but unsecure against DoS attack. Tsudik [2007] proposed two further schemes T2 and T3 to provide tag authentication. The schemes use monotonically increasing time-stamps for tracking-resistant tag authentication, and employ a keyed hash function *f*. However, these protocols are not protected from privacy and security threats. The detail of the protocol is given in Section 3.3.1.9.

It is an important research consideration to develop a privacy and security protocol for the RFID system that addresses these privacy and security issues and overcomes these problems with the limited storage and computational capacity of an RFID tag. The next section presents the proposed Efficient and Secure Authentication Protocol (ESAP) to overcome the present privacy and security problems.

5.3 The Propsoed Efficient and Secure Authentication Protocol

In this section, a new protocol (ESAP) is proposed. This is based on the challenge-response method using the one-way hash randomized hash function for the RFID systems. This protocol uses a monotonically increasing timestamp to make the response more unidentifiable and anonymous. The notations used in this protocol are as follows:

5.3.1 Notations

h A one-way hash function, $h:\{0,1\}^* \rightarrow \{0,1\}^l$

l The length of an identifier

r_1 Random number in $\{0,1\}^l$

ID Tag identifier

X Shared secret value

IDX $ID \oplus X$; it is the search index of the records

T_r Time stamp generated by the reader

T_t Last timestamp stored in a tag

f_t Tag response

f_r Reader response

$\oplus$ XOR operator

$\|$ Concatenation operator

$\leftarrow$ Assignment operator

5.3.2 System Set-up

The system setup of this protocol is given below:

Tag: Each tag contains the following fields:

ID: Tag identifier

X: Shared secret value

T_t: Last timestamp

Reader: Reader does not contain any fields.

Back-end Database: Back-end database contains the following fields:

IDX: $ID \oplus X$; Search index

ID: Tag identifier

5.3.3 ESAP Operations

When a tag enters into the range of the reader, this can initiate the authentication protocol. The protocol is shown in Figure 5-1.

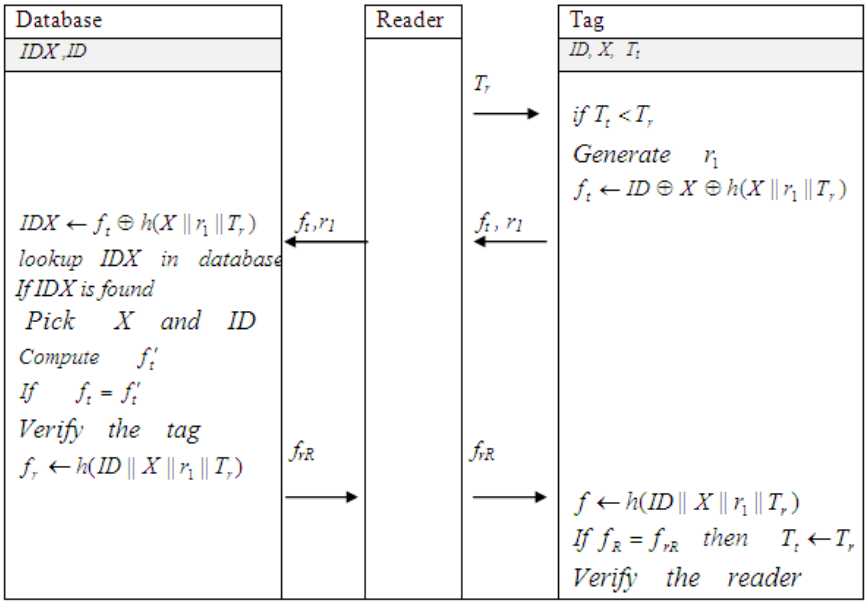

Figure 5-1: The Proposed ESAP Protocol

The steps in the authentication protocol are as follows.

1. **Reader:** The reader generates a time stamp T_r and sends the timestamp to the tag.

2. **Tag:** *if* $T_t < T_r$ *then*

The tag generates a random number r_1

The tag computes $f_t \leftarrow ID \oplus X \oplus h(X \| r_1 \| T_r)$

It sends the value of r_1 and f_t to the reader. The reader then sends r_1 and f_t to the back-end database.

3. **Database:** The back-end database then finds X and computes $h(X \| r_1 \| T_r)$ and then it finds $IDX \leftarrow f_t \oplus h(X \| r_1 \| T_r)$.

The database lookups *IDX*, *ID* in the database and computes $f_t' \leftarrow ID \oplus X \oplus h(X \| r_1 \| T_r)$

if $f_t = f_t'$ *match*

Then the database authenticates the tag and

computes $f_r \leftarrow h(ID \| X \| r_1 \| T_r)$

Finally the back-end database sends

f_{rR} to the reader. f_{rR} is the right half part of the f_r.

4. **Reader:** The reader forwards f_{rR} to the tag.

5. **Tag:** The tag also computes f_r and check f_{rR}. If it matches it authenticates the reader and updates $T_t \leftarrow T_r$.

Next, how the protocol works will be discussed. In this protocol the reader starts authentication by generating a new timestamp T_r and sends it to the tag. If the timestamp $T_t < T_r$ then the tag generates a random number r_1 to make the authentication process reliable. The tag then computes the response $f_t \leftarrow ID \oplus X \oplus h(X \| r_1 \| T_r)$ and sends f_t and r_1 to the reader. The reader sends the response and the random number r_1 to the database. The database finds X and at first computes $h(X \| r_1 \| T_r)$ and then it computes $IDX \leftarrow f_t \oplus h(X \| r_1 \| T_r)$. If *IDX* is found in the database it uses the *ID* to calculate the secret X. The database then calculate f_t with this values. If it matches with the f_t received from the tag then authenticate the tag. The database then computes $f_r \leftarrow h(ID \| X \| r_1 \| T_r)$ and sends the right half f_{rR} to the reader. The protocol uses one monotonically increasing timestamp to keep the response unidentifiable or anonymous. The tag then computes the $f \leftarrow h(ID \| X \| r_1 \| T_r)$. If the right half of this value matches with the received one then the reader is authenticated. The proposed protocol uses a random number for the tag side and a timestamp from the reader side. It makes the

response more unpredictable. Moreover the monotonically increasing timestamp also makes the input combination unique and intractable.

5.4 Analysis of the Proposed Protocol

To evaluate the proposed protocol this can be analyzed in two ways. Firstly is privacy and security analysis and secondly is efficiency analysis. The privacy and security analysis includes information leakage, location privacy, impersonation and replay attack, Denial of Service (DoS) and traceability. In efficiency analysis the storage, computation and communication costs are compared with existing related protocols.

5.4.1 Privacy and Security Analysis

The privacy and security of the proposed protocol are analysed against the threats discussed in Chapter 2. The identified privacy and security threats are information leakage, location privacy, impersonation and replay attack, Denial of Service (DoS) and traceability are outlined as follows:

- **Information Leakage:** To be able to obtain any sensitive information from a tag a protocol must be authenticated. In this protocol, to authenticate the system and to receive any information from the tags an adversary must know *ID*, *X* and the hash function. The combination of r_1 , T_r and *ID* makes the responses so unpredictable that the adversary can only guess the value or use a brute-force technique with an advantage of only $(1/2^l)$, which is negligible for data length of 96 bits or more.

- **Location Privacy:** The value of f_r and f_t cannot be linked with any particular tag. The protocol ensures location privacy by using new values of r_1 and T_r each time. Even if a malicious reader sends the same timestamp T_r all the times, a tag transmits the refreshed value using r_1 , *X* and *ID*.

- **Impersonation and Replay Attack:** When a tag reaches within the range of a reader, the reader queries with a random value to the tag. An adversary may also make a request to a tag with a timestamp. However, without knowing the *ID*, *X* and the hash function an adversary is unable to impersonate. For each session the tag generates new values of f_t and f_r which are totally

indistinguishable and different from other session and subsequently the impersonation and replay attacks are not possible.

- **Message Interception or DoS attack:** It is not possible to detect all the types of DoS attacks. The objective of the protocol is to take action against the vulnerability of a DoS attack and the system should not be desynchronized. The proposed protocol uses a static identifier for the authentication process. If the adversary is able to prevent the last transmission to the tag from the reader then the tag will not authenticate the reader in that session. In the next authentication phase it will use a new random number to authenticate and the reader will send a new timestamp and the process will be continued.

- **Traceability:** An adversary is unable to identify the tag from its response because each time it gives a different value which is non-traceable from other responses. This scheme is fully protected from the future forward and backward traceability. The adversary has no control over r_1, and the combination of r_1, T_r and hash function and also does not know the *ID* and secret *X*. Consequently, the previous, present and future interactions are all indistinguishable.

5.4.2 Efficiency Analysis

Storage, communication and computation cost were considered for efficiency analysis. Two existing authentication protocols OHLCAP [Choi et al. 2005] and T3 [Tsudik 2007] were compared with the proposed ESAP authentication protocol. These protocols were selected for efficiency comparison since all of them work in ubiquitous environment. OHLCAP and T3 require a larger storage and computations than other protocols. OHLCAP is also vulnerable to impersonation attack. The ESAP protocol shows improved performance as shown in Table 5-1 because it requires less tag side and database side storage than other protocols. The storage requirement for the tag and the database are $3l$ and $2l$ respectively. The protocol requires less hash functions in both tag and database. T3 cannot give protections from all the identified attacks and it requires (N/2+1) complex functions operations which is costly because the value of *N* may be very high and it requires many function computations that will make the protocol slower [Tsudik 2007]. Table 5-1 gives an overall comparison of the different protocols compared to the proposed ESAP. Another advantage of the proposed protocol is that it requires less data to be communicated from the reader to the tag.

Table 5-1 Efficiency Analysis

Efficiency Criteria		**OHLCAP**	**T3**	**ESAP**
Storage	Tag	5*l*	*4l*	*3l*
	Reader	-	-	-
	Database	*4l*	*5l*	*2l*
Computation	Tag	1*h*	*2h*	*2h*
	Reader	-	-	-
	Database	1*h*+ε	(N/2+1)*h*	*2h*
Communication	Tag-to-Reader	2.5*l*	3*l*	*2l*
	Reader-to-tag	0.5*l*	3*l*	*0.5l*

ε: Small operation in back-end database

5.5 Experiment Results and Evaluation

To validate the proposed protocol ESAP, simulation work has been conducted. The privacy and security protections are ensured with the hash functions, timestamp and random number. A hash function is a one-way function for which information leakage is not possible from the hash response. The simulation is to further verify the protection for impersonation attack, replay attack and location privacy. It is assumed that the adversary will capture a response from the tag or the reader and then subsequently use this response 10^{11} times to impersonate the tag or the reader. It checks the responses f_t and f_r if any of them recur more than once for one tag during the attacks by an adversary. If the same response is generated it can be used by the adversary for impersonation and replay attack and the location privacy of the tag may be broken. A simulation program in Turbo C++ compiler is developed. It runs in a desktop computer of Intel (R) Core 2 Duo. Processor speed is 2.93GHz and memory 3.46 GB. The operating System was Windows XP professional.

The objective of the simulation program was to check the response for one tag if the response is anonymous. The output of a hash function is the same for the same random number and timestamp. The objective is to ensure unique response for different inputs of random number and timestamp so that attacker cannot use any response it collected and attack later to access the tag or the reader. The program checks to match a response with subsequent responses for a set of random numbers and time stamps. The number of times the same response generated for the tag response f_t and the reader response f_r is given in the Table 5-2. It represents the success of the adversary for 10^{11} attempts of attacks for different sizes of secret numbers and data. The experiment was conducted for 16 bits, 32 bits, 64 bits and 96 bits of secret and data length. In this experiment there was no match

of the response for 64 bits and 96 bits. For 16 bits and 32 bits there were some recurrences of the same response. The reason is that it produced the same response for some other combination of random number and the timestamp. The recurrence of the response for 16, 32, 64 and 96 bits are shown in the table for 10^{11} attempts.

Table 5-2 Attacker's success table

Exp No	Number of Queries to the Tag	Attacker's Success for different data length		
		Data length	Number of Matches	
			f_t	f_r
1	10^{11}	16	1538360	1538360
2	10^{11}	16	1550799	1550799
3	10^{11}	16	1527728	1527728
4	10^{11}	32	20	20
5	10^{11}	32	15	15
6	10^{11}	32	0	0
7	10^{11}	32	0	0
8	10^{11}	32	25	25
9	10^{11}	32	23	23
10	10^{11}	64	0	0
11	10^{11}	64	0	0
12	10^{11}	64	0	0
13	10^{11}	64	0	0
14	10^{11}	64	0	0
15	10^{11}	96	0	0
16	10^{11}	96	0	0
17	10^{11}	96	0	0
18	10^{11}	96	0	0
19	10^{11}	96	0	0
20	10^{11}	96	0	0

This experiment shows that during the attempt with 64 and 96 bits of data and secret the tag and the reader produced unique response for a tag *ID* and the adversary cannot break the privacy and security of the RFID systems by using the same response.

In this experiment the attacker only tries to track the response in passive mode. It cannot use the previous timestamp and the response to attack the tag, since the tag always checks if the new timestamp is larger than its stored one. The tag does not modify its timestamp until an authentication process is successful. This experiment showed that the protocol is secure for at least 64 bits of data and secrets in 10^{11} attempts and the following Table 5-3 shows the evaluation summary.

Table 5-3 Attacker's Success Summary

Number of Queries	Attacker's Success					
	Data length (16 bits)		Data length (32 bits)		Data length (64/96 bits)	
	f_t	f_r	f_t	f_r	f_t	f_r
10^{11}	>0	>0	>=0	>= 0	0	0

f_t: Tag Response, f_r: Reader Response

In this authentication system it is not possible to perform an active attack by the adversary to the tag by using the same or fake timestamp. The reason is that the tag always stores the last timestamp and it does not allow any authentication process until it receives a timestamp greater than the previous one. Due to this monotonically increasing timestamp, impersonation and replay attack is not possible. Another advantage of this protocol is that the adversary cannot be successful with arbitrary big fake timestamp since the tag does not update its timestamp unless a successful authentication is performed. This prevents the protocol from DoS attack.

The summary of the privacy and security properties is given in Table 5-4. The privacy and security properties of ESAP are compared with four other schemes [Lee et al. 2005, Choi et al. 2005, Chien and Chen 2004, Ha et al. 2007. Tsudik 2007]. The four schemes were chosen because all of these protocols involved tag authentication. HIDV and LCAP involve secret update process and other two protocols OHLCAP and T3 do not support secret update. ESAP is similar to OHLCAP and T3 since ESAP does not support secret update and all these protocols support authentication in ubiquitous environment. Another reason to select T3 is that it also uses timestamp to make the response unpredictable. The table shows that the proposed protocol provided protections from all the identified privacy and security threats.

Table 5-4 Privacy and Security Comparisons

Property	HIDV	LCAP	OHLCAP	T3	**ESAP**
Information privacy	Y	Y	Y	Y	Y
Location Privacy	N	N	Y	Y	Y
Impersonation	N	A	N	Y	Y
Replay attack	N	Y	N	Y	Y
Message Interception	Y	Y	Y	N	Y
Backward Traceability	N	Y	N	N	Y
Forward Traceability	N	Y	N	N	Y

Y: Protected A: provided under assumption N: Not Provided

Figure 5-2 shows the storage comparison with two other ubiquitous RFID privacy and security protocols. Storage requirement in ESAP is less than other protocols. Storage requirements are presented as *l* bits. The HIDV and LCAP protocols are not included in storage comparison since they update their *ID* after each authentication phase.

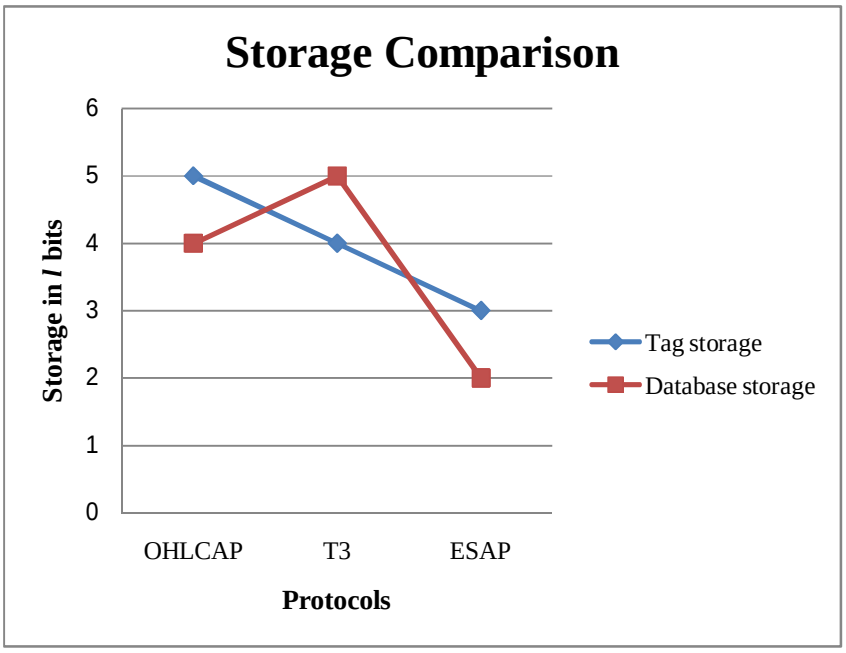

Figure 5-2: Storage Comparison

The simulation experiment successfully authenticates the tag and the reader without any privacy and security failure.

5.6 Application

This protocol will be suitable for hospital scenario where the privacy of the patient is important. In this case the patient identification number will be used as *ID* for an RFID tag.

Through the tag *ID* the private data of a person can be tracked [Lee and Kim 2007]. The privacy issue with tagged patient cards involves the risk of exposing the information, such as trace of personal location and the information of their personal health and clinical treatment. Many security threats are identified in RFID system that can also be threats in hospitals.

To protect the private data in the hospital environment the ESAP protocol can be used in the tag and the database. A hospital database will keep information about the patient. The information contains

personal detail of the patient. It also linked with other information related to the patient like disease, medicine and diagnostic information. It will additionally keep secret number for the tag. In this case any unauthorised user cannot track a patient or cannot extract any information from the patient tag. Figure. 5-3 shows that the encrypted value f_t and f_r cannot be extracted by the unauthorised user.

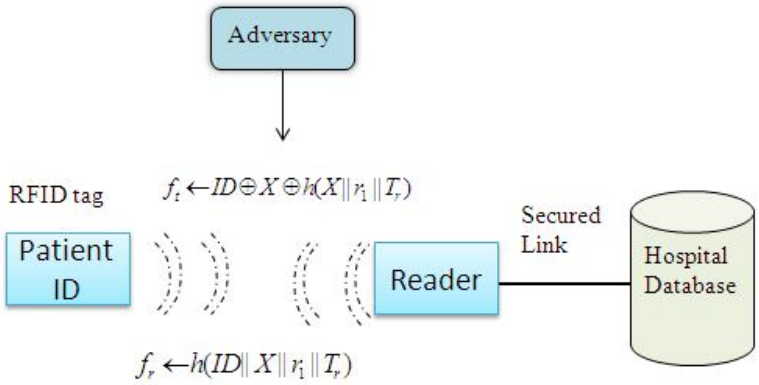

Figure 5-3: Protection of the Patient Data

Similarly the proposed protocol can also be used in a shopping mall to protect the product information from the unauthorised users. In this case all the items will be assigned a unique *ID* and keep a secret shared by the database. The customer may buy products that are private for them such as cloths, drugs or any items they do not like to disclose about the items.

5.7 Conclusion

A new efficient and secure authentication protocol ESAP has been presented in this chapter to protect privacy for low-cost RFID systems. The protocol uses a static identifier to provide effective privacy and security in a ubiquitous environment using hash functions, a timestamp and a random number. The strength of this protocol is the use of a monotonically increasing timestamp and a random number to make the response more unidentifiable. This protocol stores the current timestamp after each successful authentication. This protocol uses the search index *IDX* to search the tag records in the database. It reduces the tag search time substantially in the database. The simulation experiment also proved that, the responses during the experiment were unique for both the 64 and 96 bits long secret and data length. It is secured from an adversary from all the

identified attacks discussed in Chapter 2. Specific privacy and security protections from an adversary appropriate to simulation experiment were tested and found to be satisfactory. The privacy and security protections were also analyzed and the analysis verified that this protocol is protected from the identified threats. The proposed scheme requires only two one-way hash functions making it highly efficient. The storage requirements for the tag and database are also cost efficient. The comparison outlined in the analysis and experiment result shows that the proposed protocol is secure and efficient in compared to the other protocols. It has practical advantages over these protocols because it is simple and provides a larger range of privacy and security protections. This protocol will be suitable in the RFID systems of healthcare industry, supply chain management etc.

Aspects of this chapter have been published in the following journals or conferences. This paper was awarded as the Best Student Paper in the area of Computing and Networking.

1. Morshed, M.M., Atkins, A.S., Yu, H. 2011, An Efficient and Secure Authentication Protocol for RFID Systems, 17th International Conference on Automation and Computing (ICAC'11), 10 September, University of Huddersfield, Huddersfield, UK

An extended version of this paper is accepted for the journal International Journal for Automation and Computing (IJAC) as it is awarded as the Best Student Paper.

Chapter 6 A Group-based Authentication Protocol using Varying Identifiers (GAPVI)

6.1 Introduction

This chapter proposes a Group-based Authentication Protocol using Varying Identifier (GAPVI) to protect the privacy and security of the RFID systems effectively and efficiently. To ensure the privacy and security it updates the identifier after each successful authentication.

The use of RFID tags may cause privacy violation of users carrying an RFID tag. Due to the unique identification number of the RFID tag, the possible privacy threats are information leakage of a tag, traceability of the consumer, denial of service attack, and impersonation of a tag. Some RFID systems protect privacy and security by changing its identifier and other secret numbers. In that case some unexpected scenario like synchronization may be broken due to incomplete authentication process between the tag and the reader for unsuccessful communication or any other reasons like message interception or blocking. This GAPVI protocol provides the privacy and security in a more efficient manner. The protocol recovers from unexpected lack of synchronization due to incomplete authentication process or abnormal termination of communication. Analysis of the proposed protocol also indicates that it requires less storage and computation than some RFID authentication protocols but offers larger ranges of security protection.

6.2 Related Works

To protect the RFID tags and the reader in an efficient and effective way varying identifiers are used in many authentication protocols [Henrici and Muller 2004, Lee et al. 2005, Song and Mitchell 2008]. This section focuses on some of the protocols using varying identifiers and secret numbers for the authentication and is outlined as follows:

Chien and Chen [2007] proposed a challenge-response based authentication protocol to prevent a replay attack. This protocol uses a database in a server which maintains new and old tag keys to protect a DoS attack. To prevent a traceability authentication key and access keys are updated. However, this scheme is still vulnerable to backward and forward traceability [Peris-Lopez et al. 2009]. If an active adversary compromise a tag can identify the tag's past interactions from previous transactions and the fixed identifier of the tag. Using the past transaction and fixed identifier it would be able to identify any future transaction.

Ohkubo et al. [2003] proposed an RFID privacy scheme using a hash chain (HC) mechanism. This method used two hash functions to protect the privacy and security. It is also not suitable in practical use because the back-end database requires a large number of hash chains.

Henrici and Muller [2004] proposed a scheme which is called the hash-based identifier variation scheme (HIDV). It uses one way hash function to protect location privacy by changing the ID after each session. However if any authentication session is unsuccessful it replies with the same hashed ID again for which it opens up the vulnerability for impersonation attack like spoofing.

Lee et al. [2005] proposed a low-cost authentication protocol (LCAP) which simplifies and enhances the HIDV scheme in both efficiency and security. It also has the similar problems as HIDV that a tag always replies with the same hashed ID before the next successful authentication which allows tag tracking.

Dimitriou [2005] proposed an RFID authentication scheme that preserves user privacy and also protects against tag cloning. This protocol uses the hash of its identifier as a response to a reader query to maintain scalability at the server, and the back-end server sends a message using the updated identifier to the tag after getting the tag response. This scheme is also having problems of tracking between valid sessions as the tag identifier remains the same.

Song and Mitchell [2008] proposed an RFID authentication protocol and an ownership transfer protocol [Song 2008] to prevent all the attacks discussed. Though these protocols are efficient in terms of storage and computation requirements but are vulnerable to both tag impersonation attack and reader impersonation attack.

Hoque et al. [2009] proposed a Robust Authentication Protocol (RoAP) that supports not only security and privacy but also recovery in RFID systems. The protocol can get back the desynchronized tags and readers to their normal state, and thus provides robustness. It requires a large number of functions and hash computations.

Cai et al.[2009] proposed a revised authentication protocol of Song and Mitchell [2008] to eliminate the problems in it without violation of any other security properties. The storage and computation requirements are also comparable with the existing protocol.

The protocols discussed remove most of the privacy and security threats but fail to remove the threat of location privacy of the tag with reasonable storage and computation costs. Some of them are vulnerable to impersonation attack and tracing problem [Henrici and Muller 2004, Lee et al. 2005, Song and Mitchell 2008, Chien and Chen 2007]. These protocols do not consider a large system that may divide the tags in many groups. This is an important research consideration to develop a privacy and security protocol for the RFID system that addresses these issues and overcome these problems using limited storage and computational capacity of an RFID tag. This chapter proposes a new group-based authentication protocol which provides the privacy and security in a more efficient manner using varying identifiers. To enhance the privacy and security protection of the RFID systems we propose a new protocol in the next section with the following features:

1. It is a group-based authentication protocol using varying identifier that reduces computation and search time.
2. It uses hash function and two random numbers.
3. It eliminates the existing privacy and security problems.
4. It requires low storages, computation and communication costs that are suitable for low-cost RFID tags.

6.3 The Proposed GAPVI Protocol

In this section, a new protocol (GAPVI) is proposed. This is based on the challenge-response method using the one-way hash function and the randomized hash function in RFID systems. This

protocol supports recovery in case of desynchronization due to incomplete authentication process with less computations and protecting location privacy effectively. Relying on the same prerequisites as the one-way hash function and key management at the back-end, a scheme is proposed that not only provides data privacy but location privacy as well. The general idea is to change the *ID* of a tag on every read attempt in a secure manner. Any attempts like eavesdropping, spoofing, modification, replay attacks, or man-in-the-middle attacks cannot compromise the scheme.

6.3.1 Preliminaries

The hash function h is defined as $y = h(x)$, where $h(x)$ is a cryptographic one-way function. Ideally, besides the function being difficult to invert, the output y should not reveal any substantial information on its preimage x [Menezes et al. 1996]. A hash function h is an efficiently computable function which maps an arbitrary length input to a fixed length output;

$$h : \{0,1\}^* \rightarrow \{0,1\}^l$$

A cryptographic hash function has the following properties [Menezes et al. 1996]:

- Preimage resistance: For any output y, it is computationally infeasible to find an input x such that $h(x) = y$.
- Second-preimage resistance: Given x, it is computationally infeasible to find x, x' where $x \neq x'$ such that $h(x) \neq h(x')$

6.3.2 Notations

The notations used in this protocol are as follows:

h	A one-way hash function, $h : \{0,1\}^* \rightarrow \{0,1\}^l$
l	The length of an identifier
r_1	Random number in $\{0,1\}^l$
r_2	Random number in $\{0,1\}^l$
ID	Tag identifier
ID_{Prev}	Previous tag identifier
HID	Hash address
HID_{Prev}:	Previous value of the hash address

GI Secret group index

$\oplus$ XOR operator

$\|$ Concatenation operator

$\leftarrow$ Assignment operator

$+$ Modular addition by $mod\ (2^l - 1)$

6.3.3 System Set-up

The system setup for the tag, reader and the database are as follows:

Tag: Each tag contains the following fields:

ID: Tag Identifier

GI: Secret group index

Reader: Reader does not contain any fields.

Back-end Database: Back-end database contains the following fields:

ID: Tag identifier

HID: Hash address

GI: Secret group index

HID_{Prev}: Previous value of the hash address

ID_{prev}: *ID* in previous phase

6.3.4 GAPVI Operations

When a tag enters into the range of the reader, this can initiate the authentication protocol. The protocol is shown in Figure 6-1.

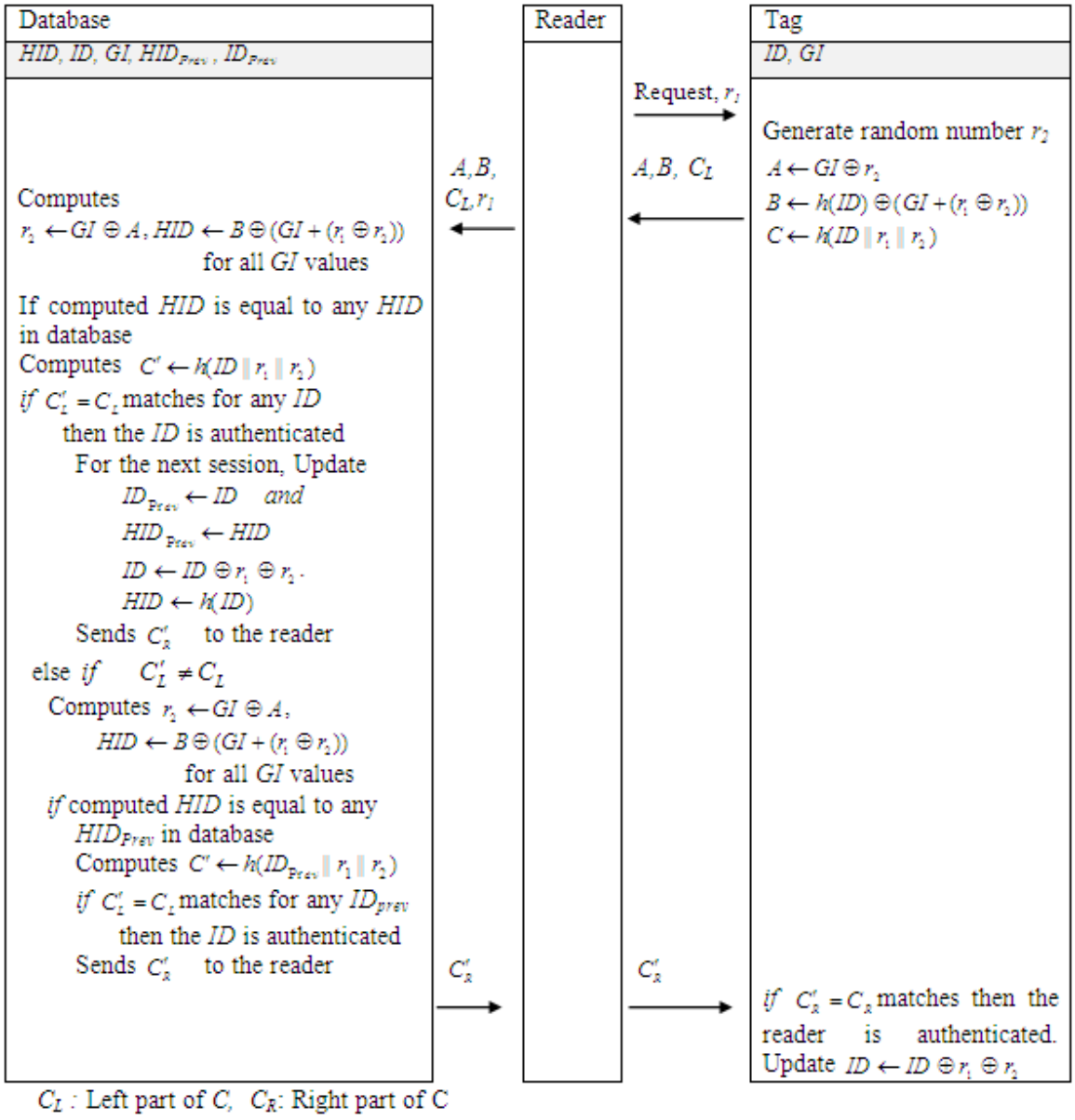

Figure 6-1: GAPVI Protocol

The steps in the authentication protocol are as follows:

1. A reader selects a random number r_1 and sends a request with r_1 to the tag.
2. After receiving the random number r_1 the tag will generate another random number r_2.

The tag computes $A \leftarrow GI \oplus r_2$

$B \leftarrow h(ID) \oplus (GI + (r_1 \oplus r_2))$

$C \leftarrow h(ID \| r_1 \| r_2)$, and sends the value of A,B, C_L to the reader.

3. The reader then sends A,B,C_L,r_1 to the back-end database.

4. The database computes $r_2 \leftarrow GI \oplus A, HID \leftarrow B \oplus (GI + (r_1 \oplus r_2))$ for all *GI* values

If computed *HID* is equal to any *HID* in the database then pick the *ID* and computes $C' \leftarrow h(ID \| r_1 \| r_2)$

if $C'_L = C_L$ matches for any *ID* then the *ID* is authenticated

For the next session, update

$ID_{Prev} \leftarrow ID$

$HID_{Prev} \leftarrow HID$

$ID \leftarrow ID \oplus r_1 \oplus r_2$.

$HID \leftarrow h(ID)$

Sends C'_R to the reader

else *if* $C'_L \neq C_L$

Computes $r_2 \leftarrow GI \oplus A, HID \leftarrow B \oplus (GI + (r_1 \oplus r_2))$ for all *GI* values

if computed *HID* is equal to any HID_{Prev} in database computes $C' \leftarrow h(ID_{Prev} \| r_1 \| r_2)$

if $C'_L = C_L$ matches for any ID_{Prev} then the *ID* is authenticated

Sends C'_R to the reader

5. The reader forwards C'_R to the tag.

6. *if* $C'_R = C_R$ matches then the reader is authenticated. Update $ID \leftarrow ID \oplus r_1 \oplus r_2$

The description and applications of the proposed algorithm will be presented in the next section.

6.3.5 Protocol Description and Example

To understand the update procedure of GAPVI operations and synchronization operation in the tag and the database in each authentication process the protocol descriptions are outlined as follows:

Assume in the initial state the database and the tag has the following values

Database (*HID,ID, GI,* HID_{Prev} *,* ID_{prev}**)**	**Tag(***ID, GI)*
HID_0, ID_0, *GI,* HID_0 , ID_0	ID_0, *GI*

In case of successful authentication process the tag sends *A*, *B* and C_L to the reader to forward these values to the database. The database after authentication updates its parameters and sends the C'_R to

the tag. The tag also authenticates and updates its parameter to synchronous with the database. After successful authentication process it has the following state:

Database (*HID, ID, GI, HID_{Prev} , ID_{prev}***)**	**Tag(***ID, GI)*
HID_1, ID_1, GI, HID_0 , ID_0	ID_1, GI

If the authentication process is unable to complete because of some abnormal situation (e.g. loss of transmission) in this case the tag is unable to authenticate and update the parameter *ID* and is then holding the previous value. The scenario is shown as follows:

Database (*HID,ID, GI, HID_{Prev} , ID_{prev}***)**	**Tag(***ID, GI)*
HID_1, ID_1, GI, HID_0 , ID_0	ID_0, GI

For the next authentication phase of the tag the database cannot authenticate with current value of HID_1 and ID_1 and hence will authenticate the tag with the HID_{Prev} and ID_{Prev} which are now HID_0 and ID_0 . After this it will synchronize the values as follows:

Database (*HID, ID, GI, HID_{Prev} , ID_{prev}***)**	**Tag(***ID, GI)*
HID_1, ID_1, GI, HID_0 , ID_0	ID_1, GI

The scenarios are shown with some examples as follows:

Initial state:

We assume h(100)=10 and h(117)=12 and the fields are initialized with the following values:

HID_0=10, ID_0=100, GI=1, HID_0=10, ID_0=100

Database (*HID,ID, GI, HID_{Prev} , ID_{prev}***)**	**Tag(***ID, GI)*
10, 100, 1, 10, 100	*100, 1*

Next states:

We also assume that the next value of the *ID* will be 117. If a successful authentication is performed the database and tag will update the values as follows:

Database (*HID,ID, GI, HID_{Prev} , ID_{prev}*)	**Tag(*ID, GI)***
12, 117, 1, 10, 100	*117, 1*

The subsequent successful authentication process will be continued in the same way.

If the authentication is not successful we assume only the database updated the values successfully but the tag failed to update. In that case the values will be as follows:

Database (*HID,ID, GI, HID_{Prev} , ID_{prev}*)	**Tag(*ID, GI)***
12, 117, 1, 10, 100	*100, 1*

After this state if a successful authentication is performed with the previous values of HID_{Prev}=10 and ID_{Prev}=100 the database and tag will be again synchronized as follows:

Database (*HID,ID, GI, HID_{Prev} , ID_{prev}*)	**Tag(*ID, GI)***
12, 117, 1, 10, 100	*117, 1*

6.4 Experiment Result and Discussion

To validate the proposed protocol GAPVI, simulation experiments have been conducted. A simulation program in Turbo C++ compiler was developed in a desktop computer of Intel (R) Core 2 Duo with processor speed of 2.93GHz and memory of 3.46 GB. Windows XP Professional was used as the operating system. The objective of the simulation program was to check the anonymity of the response for one tag. The output of a hash function is the same for the same random number pair. The objective is to ensure unique response for different inputs of random number pair so that an adversary is unable to use any responses at later stage to access the tag or the reader. The program checks to match a response for different sets of random numbers. EOHLCAP is selected which uses static identifier to protect the privacy and security of the RFID systems with our proposed protocol. The number of times a similar response is generated is given in Table 6-1. The experiment was conducted for 16, 32 and 64 bits for secrets, random number and data. The results shown in Table 6-1 indicated that for 32 and 64 bits there is no matching response and the results are always unique for the proposed protocol but for EOHLCAP this unique response is obtained only for 64 bits and the secure zones for the two protocols are shown in the shaded cells. For 16 bits

there were some recurrences of the same response for both the protocols. The recurrence of the same response is due to two reasons. Firstly it produces the same random number pairs and secondly it produces similar responses for some other combination of random number pairs.

Table 6-1 Attacker's Success Table

Exp No	Number of Queries to the Tag	Data/ Secret Size (bits)	Attacker's Success	
			EOHLCAP[18] (Static ID)	GAPVI (Varying ID)
1	10^{11}	16	1539054	1511114
2	10^{11}	16	1536078	1505568
3	10^{11}	16	1536965	1526852
4	10^{11}	32	0	0
5	10^{11}	32	40	0
6	10^{11}	32	0	0
7	10^{11}	32	0	0
8	10^{11}	32	0	0
9	10^{11}	32	43	0
10	10^{11}	64	0	0
11	10^{11}	64	0	0
12	10^{11}	64	0	0
13	10^{11}	64	0	0
14	10^{11}	64	0	0
15	10^{11}	64	0	0
16	10^{11}	64	0	0
17	10^{11}	64	0	0
18	10^{11}	64	0	0
19	10^{11}	64	0	0
20	10^{11}	64	0	0

The Table 6-2 shows the summary of the evaluation.

Table 6-2 Attacker's success table

Data/Secret size	EOHLCAP[18] (Static ID)	GAPVI (Varying ID)
16 bits	Not secured	Not secured
32 bits	Not secured	**Secured**
64 bits	**Secured**	**Secured**

This experiment showed that the protocol is secure for 32 and 64 bits in 10^{11} attempts. For 16 bits there were some recurrences of the same response that can be used by an adversary. However, the EOHLCAP is not secure for 32 bits of data and secret values.

6.5 Analysis

To evaluate the proposed protocol privacy, security and efficiency will be analysed. The identified privacy and security are information leakage, location privacy, information and replay attack, message interception and tracing. In efficiency analysis storage, computation and communication costs are considered. The attack model is defined in the following way:

Γ:An adversary

R: Reader

T: Tag

It is assumed that the adversary disguises as a reader R_Γ and ID_Γ, GI_Γ will be used by the adversary as fake *ID* and secret *GI* respectively.

6.5.1 Privacy and Security Analysis

The privacy and security of the proposed protocol is analysed against various threats such as information leakage of a tag, location privacy, and impersonation of a tag, Denial of Service attack and traceability and are outlined as follows:

Information Leakage: In this protocol to be able to obtain any sensitive information from a tag the adversary Γ must be authenticated. To authenticate the system an adversary Γ must know *ID, GI* and the hash function to get any information from the tags. The combination of r_1 and r_2 with *GI* and *ID* makes the response *C* so unpredictable that the adversary can only guess the value or use a brute-force technique with an advantage of only $\frac{1}{2^l}$, which is negligible. From the responses $B \leftarrow h(ID) \oplus (GI + (r_1 \oplus r_2))$ and $C \leftarrow h(ID \| r_1 \| r_2)$ of the tag the adversary cannot extract the value of *ID*.

Location Privacy: The value of *B* and *C* cannot be linked with any particular tag. The protocol ensures location privacy by using new values of r_1, r_2 each time. The identifier *ID* is also updated after each authentication session. Even if a malicious reader sends the same random value r_1 all the times, a tag transmits the refreshed value using r_2 and *GI*. The adversary Γ can receive the following response from the tag in one session.

$$T \Rightarrow \Gamma : h(ID \| r_1 \| r_2)$$

In the next session the adversary Γ will receive a different response from the tag since the *ID*, r_1, and r_2 are all changed the responses are not matched.

In subsequent all sessions the responses from the tag are anonymous hence location privacy is protected and tracking is not possible.

Impersonation and Replay Attack: When a tag reaches within the range of a reader, the reader queries with a random value to the tag. An adversary may also make a request to a tag with a random number. However, without knowing the *ID*, the hash function, secret *GI* an adversary is unable to impersonate. After each session the *ID* is updated internally to a new value. The value of secret *GI* is passed always secretly. For each session the tag generates a new value of the responses *A, B and C* which are totally indistinguishable and different from other sessions and subsequently the impersonation and replay attacks are not possible.

Message Interception: The protocol recovers from the abnormal interruption of the authentication process. If the adversary is able to prevent the last transmission to the tag from the reader then the tag will not authenticate the reader in that session. In the next authentication phase it will use a new random number to authenticate and the database will use the previous ID_{prev} to authenticate and synchronous the system. For example the database will use HID_0, ID_0 instead of HID1, ID_1 to authenticate the tag as shown as follows:

Database (*HID,ID, GI,* HID_{Prev} *,* ID_{prev}**)**	**Tag(***ID, GI)*
HID_1,ID_1, *GI,* HID_0 , ID_0	ID_0, *GI*

Traceability: An adversary is unable to identify the tag from its response because each time it gives a different value which is non traceable from other responses. This scheme is fully protected from

the future forward and backward traceability. The adversary has no control over r_2, and the combination of r_1, r_2 and hash function and also does not know the *ID* and group secret value *GI*. Consequently, the previous, present and future interactions are all indistinguishable.

Table 6-3 Privacy and Security Comparisons

Property	HIDV (Varying ID)	LCAP (Varying ID)	RoAP (Varying ID)	EOHLCAP (Static ID)	GAPVI (Varying ID)
Information privacy	Y	Y	Y	Y	Y
Location Privacy	N	N	Y	Y	Y
Impersonation	N	A	Y	Y	Y
Replay attack	N	Y	Y	Y	Y
Message Interception	Y	Y	Y	Y	Y
Backward Traceability	N	Y	Y	Y	Y
Forward Traceability	N	Y	Y	Y	Y

Y: Protected A: provided under assumption N: Not Provided

The summary of the privacy and security properties is given in Table 6-3. The privacy and security properties of GAPVI are compared with four other schemes HIDV, LCAP, RoAP and EOHLCAP. The three schemes HIDV, LCAP, RoAP were chosen because all of these protocols involved tag authentication and involve secret update process after each successful authentication. The protocol EOHLCAP was chosen from static *ID* group since it offers better privacy and security options. The table shows that the proposed protocol provided protections from all the identified privacy and security threats. Some of the privacy and security properties are further tested by simulation program and outlined in Section 6-4.

6.5.2 Efficiency Analysis

Storage, communication and computation cost are considered for efficiency analysis. Various existing authentication protocols are compared with the proposed GAPVI authentication protocol. HIDV [Henrici and Muller 2004] requires a larger storage and computations than other protocols and suffers from location privacy issues. It is also vulnerable to impersonation attack. LCAP appears to be better in performance however, it has location privacy problem [Lee et al. 2005]. The GAPVI protocol shows improved performance as shown in Table 6-4 because it requires less tag side and database side storage than some protocols and gives protection from the all attacks [Lee et al. 2005]. The storage requirement for the tag and the database are 2*l*, and 5*l* respectively. The

protocol requires less hash function in both tag and database in simulation experiments. RoAP [Hoque et al. 2009] gives protections from all the attacks but it needs $\frac{N}{2}$ functions and 2 hash operations which is costly because the value of N may be very high and require many hash computations that will make the protocol slower. Table 6-4 gives an overall comparison of the different protocols compared to the proposed GAPVI. It shows that the proposed protocol requires much less hash function than the secured RoAP protocol. As the hash functions computations on the database side is less the proposed protocol requires less computation time.

Table 6-4 Efficiency Analysis

Efficiency Criteria		HIDV (Varying ID)	LCAP (Varying ID)	RoAP (Varying ID)	EOHLCAP (Static ID)	GAPVI (Varying ID)
Storage	Tag	$3l$	$1l$	$2l$	$3l$	$2l$
	Reader	-	-	-	-	-
	Database	$10l$	$6l$	$3l$	$3l$	$5l$
Computation	Tag	$3h$	$2h$	$2h + f$	$1h+\mu$	$2h$
	Reader	-	-	-	-	-
	Database	$3h+\varepsilon$	$2h+\varepsilon$	$(\frac{N}{2}f + 2h) + \varepsilon$	$(\frac{m_i + 1}{2})h + \varepsilon$	$1h+\varepsilon$
Communication	Tag-to-Reader	$3l$	$1.5l$	$2l$	$2.5l$	$2.5l$
	Reader-to-tag	$2l$	$0.5l$	l	$0.5l$	$0.5l$

ε: Small operation in back-end database μ: small operation in the tag side h: hash operation f: Function operation N: Total number of tags, m_i: number of tags in the i^{th} group

6.6 Conclusion

A new efficient and secure authentication protocol GAPVI is proposed to protect privacy for low-cost RFID systems. The protocol uses a varying identifier to provide effective privacy and security with recovery of the identifier to maintain synchronization. Due to the group-based design it requires less computation and search time to authenticate a tag. Due to the new updated identifier after each authentication process the response is more unpredictable and consequently more secure. It is also secured from an adversary by maintaining location privacy in case the authentication process is interrupted, since it always uses new random number pairs to generate the hash response. The new random number pairs in each session make the hash response unidentifiable. It also protects the systems from an adversary for both privacy and security attacks as it was tested in the simulation experiment and analysis. The proposed scheme requires only two one-way hash

functions in the tag and only one hash computation in the database making it highly efficient. The storage requirement for the tag and database is also cost efficient for an authentication protocol using varying identifiers. The comparison outlined in the analysis of the protocol is both secure and efficient compared to the other protocols outlined. It has practical advantages over these protocols because it is simple and provides a larger range of privacy and security protections. In future the intention is to perform more comparisons related to privacy, security and performance with other protocols using experiments by simulation software.

Part of the substance of this chapter has been published in the proceedings of the following conference.

1. Morshed, M.M., Atkins, A.S. , Yu, H., Ahmed, S.I. , Akbar, M.M. 2010, 'A Novel Authentication Protocol using Varying Identifier for RFID System', IEEE 4th International Conference on Advanced Computing & Communication Technologies (ICACCT), India, pp.1-6.

Chapter 7 Privacy and Security Enhancements of the HB-MP Protolcols

7.1 Introduction

This chapter proposes a different approach to ensure privacy and security of the RFID systems instead of using hash function. It uses lightweight cryptographic techniques to ensure the privacy and security of the low-cost resource- constraint RFID systems.

It is essential to ensure privacy and security protections in RFID systems. However, implementation of conventional cryptography is not possible in a passive RFID tag due to its limited processing capability and memory limitations [Parbhu et al. 2005]. This chapter analyzes the privacy and security problems in HB, HB+ and HB-MP protocols and a new authentication protocol Enhanced HB-MP (EHB-MP) is presented, to overcome their limitations. HB was suitable against a passive attack but vulnerable to an active attack. HB+ and HB-MP were designed to protect against the active attack. However, it is found that these protocols are not safe against some active attacks such as the man-in-the-middle attack. In this chapter, the possible attacks in the existing light weight protocols of Radio Frequency Identification System (RFID) systems are investigated and new lightweight authentication protocol related to HB+ and HB-MP protocols is proposed which provide the identified privacy and security in an efficient manner for pervasive computing environment. More precisely, the proposed protocol is enhanced version of HB-MP protocol. It is shown that storage and computation require to implement these protocols are almost similar to HB+, HB-MP protocols. A mathematical proof is presented to show that the Enhanced HB-MP protocol is protected from the man-in-the-middle attack.

Various privacy and security goals are identified in the RFID systems. Some of the privacy and security objectives are to protect the RFID systems form information leakage, location privacy, man-in-the-middle and replay attack, backward and forward traceability and cloning. In typical RFID system there is a chance of information leakage. For the protection from such information leakage, an RFID system needs to provide privacy control so that unauthorized readers cannot access the tags. Location privacy is another important issue for a tag holder. An unauthorized user

may try to know the location of the tag holder. When a tag transmits any information to a reader, an adversary may try to distinguish it from other responses and can find the location of the user. An unauthorized reader may initiate man-in-the-middle and replay attack. When a tag responds to a reader, an adversary can collect the information from the tag and can modify the response of the tag. Adversary can also impersonate the tag using this information and replay in future. Message interception or Denial of Service (DoS) may make the RFID system inoperable. An adversary may try to block communication between the tag and the reader and can cause the server and the tag to lose synchronization. It is possible to identify a tag using backward and forward traceability**.** If the internal stage of a tag is known then it can help to identify the tag interactions of past and future. Cloning a tag is a very common threat for an RFID system. To protect from counterfeiting, the RFID systems need to be unclonable. An adversary can clone a tag if it knows the secrets of the tag. If the response of a tag is always the same then an adversary can mimic this response as a valid signal.

This is an important research consideration to develop a privacy and security protocol for the RFID system that addresses these issues and overcome these problems using limited storage and computational capacity of an RFID tag. The goal is to use lightweight encryption that is easy to implement in low-cost RFID tag. The proposed EHB-MP enhanced the HB-MP protocol and protect from the identified privacy and security threats. A mathematical analysis is presented to prove that the man-in-the-middle attack described in Gilbert et al.[2005] cannot break the privacy and security of the EHB-MP protocol.

7.2 Related Works

The proposed new protocol is an extension of HB-MP protocol and is protected from the security attacks discussed in this section. The short review of HB, HB+ and HB-MP protocols and man-in-the-middle attack described by Gilbert et al. [2005] are given below.

The details of the LPN problem and HB protocol are discussed in Section 3.3.3.1. The LPN problem works with binary inner product of two numbers. It is assumed that each number is *k*-bit long and two *k*-bit numbers $a = (a_0 a_1 ....(a_{k-1})_2$ and $x = (x_0 x_1 .....x_{k-1})_2$. The inner product of *a* and *x* is denoted by *a.x* and it can be evaluated as $a.x = (a_0 \wedge x_0) \oplus (a_1 \wedge x_1) \oplus ..... \oplus (a_{k-1} \wedge x_{k-1})$. It is

easy to implement in low cost hardware such as an RFID tag and is also possible to compute one bit at a time [Jules and Weis 2005]. So it is not necessary to store all *k* bits of *a* and *x* when computing. Goldreich and Levin [1989] proved that *a.x* is unpredictable if only *a* or *x* is given.

The HB protocol proposed by Hopper and Blum [2001] is a cryptographic protocol based on binary inner product. It was a human authentication protocol because human can evaluate one binary inner product operation, and generate a random bit. This HB protocol is claimed to be secure under the assumption that Learning Parity with Noise problem is intractable.

In HB protocol both human and machine shares a common secret *x* of *k*-bit long. In this case the human plays the role of a tag and the reader plays the role of a machine.

The HB protocol is secure only from passive attackers. It is not secure against active attacks where a reader can be malicious. Jules and Weis [2005] proposed an extended version of the HB protocol to protect against active attack and this new protocol is referred to as HB+.

The detail of the HB+ protocol is given in Section 3.3.3.2. The HB+ protocol is an improved version of HB protocol and gives better privacy and security protection. In the HB+ protocol the reader and the tag both share two secrets (*x*, *y*) of *k*-bit long. In the HB+ protocol the tag also generates a random number *b* as a blinding factor. The purpose of the blinding factor *b* is to protect the tag from the malicious reader from extracting secret by repeatedly querying the tag with the same random number *a*.

In the HB+ protocol the purpose of *v* is same as in the HB protocol. It is to protect *x* from passive eavesdropper after observing *k* pairs (*a, z*). The noise bit is generated in each round with a value 1 with probability η as in HB protocol.

Though it is claimed that the HB+ protocol is free from an active attack but an attack has been described against this protocol by Gilbert et al. [2005]. The authors proved that it is not secure against the man-in- the-middle attack. The adversary chooses a *k*-bit vector δ and introduces it by doing XOR with a in each round and sends the result $a \oplus \delta$ to the tag in place of a. The tag will compute $z' = (a \oplus \delta).x \oplus (b.y) \oplus v$ and send it to the reader. It is obvious that if authentication process is successful then $\delta.x = 0$ otherwise $\delta.x = 1$ with a high probability. So, one can recover

one bit of x by using same δ in all r round. To retrieve the k- bit secret x it is sufficient to repeat the whole protocol k times by changing the value of δ linearly independently.

The HB-MP protocol is explained in Section 3.3.3.3. The authors proposed the protocol in two phases. First one is called HB-MP$^{/}$ which exchanges only two messages. HB-MP$^{/}$ protocol is secured against passive attack but vulnerable to man-in-the-middle attack [Leng et al. 2008]. To protect from the attack the HB-MP$^{/}$ protocol is modified and the second one is called HB-MP. The HB-MP protocol uses two shared secrets as in HB+ protocol.

The *Rotate()* function is supposed to protect the HB-MP protocol form the-man-in-the-middle attack. However, this has its own weakness since x=*Rotate*(x, y_i), it gives a same value of *xm* in the first round of all authentication session [Leng et al. 2008]. If the attacker observes the *i*th round, he is able to reveal the *xm* used in the *i*th round. Hence the protocol is not protected from the man-in-the-middle attack [Leng et al. 2008].

7.3 The Propsoed Enhanced HB-MP Protocol

In this section, a new protocol related to HB+ and HB-MP based on challenge-response method is proposed. The proposed protocol utilizes the blinding process of HB+ protocol and the new idea from HB-MP protocol.

The notations and symbols used in this protocol are:

x	Secret number
y	Secret number
k	The length of an identifier
$f_0(p_1,p_2)$	Shift-left p_1 for every 0 in p_2
$f_1(p_1,p_2)$	Shift-left p_1 for every 1 in p_2
a	Random number in $\{0,1\}^k$
b	Random number in $\{0,1\}^k$
δ	k-bit vector used for attack
$\oplus$	XOR operator

$\wedge$ AND operator

z Result of the inner products

z' Changed result of the inner products

The proposed protocol that enhanced HB-MP is as follows:

7.3.1 EHB-MP Protocol

The proposed protocol enhanced HB-MP protocol. It uses one-way shift-left functions $f_0(p_1,p_2)$ and $f_1(p_1,p_2)$ in place of the rotate function in HB-MP, HB-MP+ protocols. The objective of the one-way function is that it makes impossible to get the value of the input from the output. It uses the two random numbers a and b to change the value of x and y in each round. The changed values u and v are used to compute the inner product z. The value of u and v are obtained using a one-way shift left operation. This will give a new value in all the rounds to make the response non identifiable. It is not possible to obtain the secret x and y from u and v.

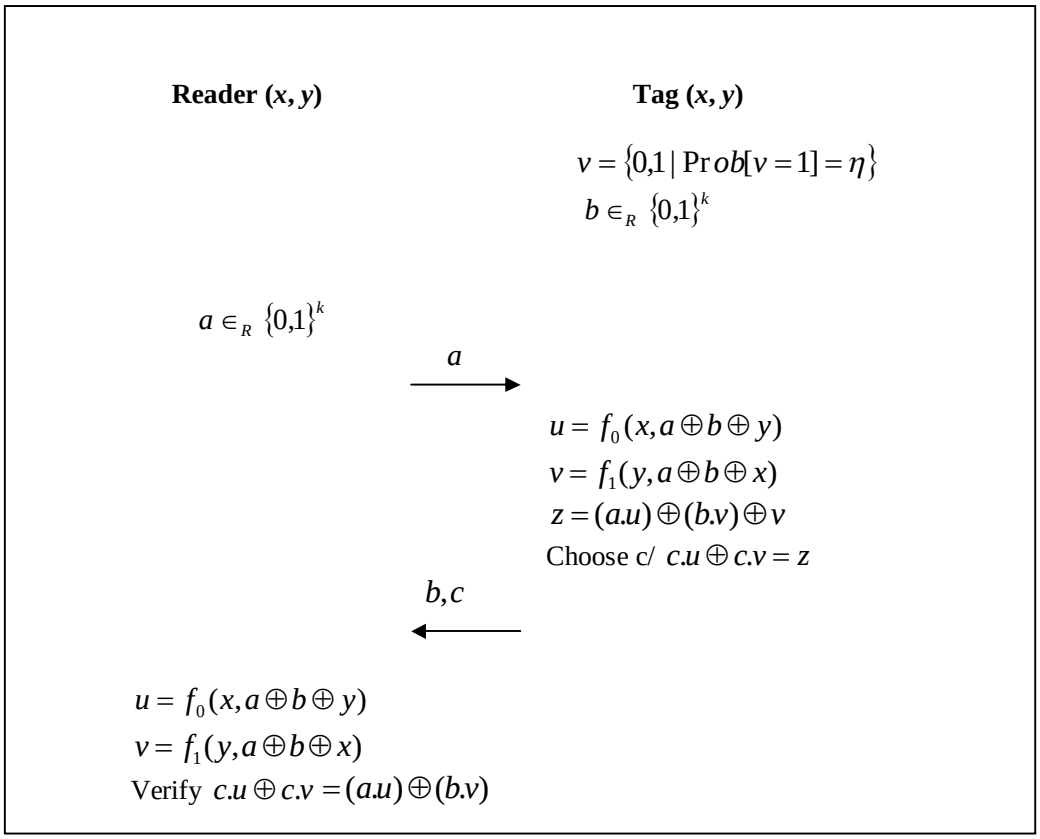

Figure 7-1: One Round of the Proposed EHB-MP Protocol.

The EHB-MP protocol is depicted in Figure7-1 and the steps in the protocols are given as follows:

There are six steps in this protocol.

1. The reader generates a random number *a* and sends it to the tag.
2. The tag receives *a* from the reader and generates a random number *b* as a blinding factor and computes

   $u = f_0(x, a \oplus b \oplus y)$

   $v = f_1(y, a \oplus b \oplus x)$
3. The tag computes

   $z = (a.u) \oplus (b.v) \oplus v$

   and looks for k-bit binary vector *c* such that $c.u \oplus c.v = z$. Here *v* is a noise factor of value 1 with probability $\eta = (0,0.5)$.
4. The tag sends *b* and *c* to the reader.
5. The reader computes

   $u = f_0(x, a \oplus b \oplus y)$

   $v = f_1(y, a \oplus b \oplus x)$
6. The reader checks $c.u \oplus c.v = (a.u) \oplus (b.v)$

7.3.2 Protection Against the Man-in-the-middle Attack

If a man-in-the-middle attack is done according to Gilbert et al. [2005] using δ then the reader will use ($c+\delta$) for *c*. The response reduces to

$$\begin{aligned} & (c+\delta).u \oplus (c+\delta).v \\ = \ & (c+\delta).(u \oplus v) \\ = \ & c.(u \oplus v) + \delta.(u \oplus v) \end{aligned}$$

It is obvious that if authentication process is successful then $\delta.(u \oplus v) = 0$ otherwise $\delta.(u \oplus v) = 1$ with a high probability. The adversary cannot get any idea about *x* and *y* because *u* and *v* are always changing using the random numbers *a* and *b*. Due to the one-way property of the functions

$f_0(x, a \oplus b \oplus y)$ and $f_1(y, a \oplus b \oplus x)$ it is not possible to link between *x*, *y* with *u*, *v* pairs. From the inner product of $\delta.(u \oplus v)$ it is not possible to retrieve the bits of the secret *x* and *y*.

7.4 Analysis

The previous protocols HB, HB+ and HB-MP have several privacy and security problems. The HB protocol is only protected from passive attacks. The HB+ and HB-MP are vulnerable to man-in-the-middle attack. The proposed EHB-MP protocol is protected from the man-in-the middle attack shown in the Section 7.3.2. The other privacy and security analysis are given as follows:

7.4.1 Privacy and Security Analysis

The privacy and security of the proposed protocol are analyzed against the threats discussed in Section 7.1. The responses are computed considering the LPN problem; a passive attacker has to solve the LPN problem to reveal the secret of the tag. The strength of the proposed EHB-MP protocol is that *x* and *y* are replaced by *u* and *v* respectively with two random numbers *a* and *b* before the inner operation is performed. Two random numbers *a* and *b* change the secret *x* and *y* to make the attacks impossible. The proposed EHB-MP protocol is protected against the identified threats.

The proposed protocol is resistant to information leakage. In this protocol, adversary must be authenticated to get any sensitive information from a tag. To authenticate an adversary must know *x* and *y* to get any information from the tag. The combination of *a* and *b* makes the response so unpredictable that adversary cannot extract the value of *x* or *y* from *c* since *x* and *y* are replaced by *u* and *v* respectively. The functions $f_0(x, a \oplus b \oplus y)$ and $f_1(y, a \oplus b \oplus x)$ make the secret *x* and *y* protected from information leakage due to the one-way property of these functions.

The proposed protocol ensures location privacy. The responses from the tags are unidentifiable by the adversary. The value of *z* cannot be linked with any particular tag. This protocol ensures location privacy by using new values of *a*, *b* each time. Even if a malicious reader sends a same random value *a* all the times, a tag transmits the refreshed value that are refreshed by *b*, *x* and *y*.

The proposed protocol is resistant against all passive attacks since the information obtained by an attacker is equivalent to the information obtained by HB and HB+ protocols. It is also resistant against active attacks applied to HB, HB+ because the shared secret keys *x* and *y* are modified by two random numbers *a* and *b* at every round before the computation of the inner product. It makes the response random and unpredictable.

The protocol is protected from the man-in-the-middle and replay attack. Without knowing *x*, *y* adversary cannot be authenticated by the tag. In every round tag generates new value of *z* generated from *x* and *y* that is totally indistinguishable. It sends a new value *c* generated from *z* in each round. It protects the protocol from the man-in-the-middle attack applied to HB+ and HB-MP protocols Gilbert et al.[2005].

The EHB-MP protocol does not suffer from DoS attack. The secrets in our protocol are never changed. The adversary has no access to the secret value of the tag and the reader. If an adversary modifies the responses in any authentication process, the authentication cannot be performed and an active attack is detected.

The proposed protocol is also resistant against the backward and forward traceability. In the proposed protocol the same challenge does not produce the same response from the tag. Two random numbers *a* and *b* make the response more intractable by changing the *x* and *y* to *u* and *v* respectively. The previous, present and future interactions are all indistinguishable. So the backward and forward traceability are not possible.

In the proposed protocol the adversary will not be successful to clone a tag. In the protocol the secrets are never passed in plain text and the responses are always different due to the random numbers *a* and *b*. The same challenge does not produce the same response from the tag.

7.4.2 Efficiency Analysis

The storage cost, communication cost and computation cost of the propose protocols are considered to compare with the protocols in the HB-family for efficiency analysis. The proposed EHB-MP protocol was compared with HB, HB-MP$^{/}$, HB+, HB++ and HB-MP protocols. The proposed protocol gives protection against the active attacks and also against passive attacks using the same

storage and resources as in HB+ and HB-MP protocols. Storage comparison is shown in the Table 7-1. The Proposed EHB-MP requires two secret each like HB+ and HB-MP. HB protocol uses less storage but they are not secured against active attacks. It is secured against passive attacks only.

Table 7-1 Storage Comparison

Protocols	HB	HB-MP/	HB+	HB++	HB-MP	EHB-MP
Tag	k	k	$2k$	$4k$	$2k$	$2k$
Reader	k	k	$2k$	$4k$	$2k$	$2k$

The fundamental operations used in the proposed protocol are similar as in HB, HB+ and HB-MP except HB++ and the proposed protocol require extra functions that make these protocols little more complex [Munilla and Peinado 2007]. There are two message transmissions in each round in our protocol like HB-MP. HB+ protocol requires 3 message transmissions in each round. HB+ and HB-MP protocols are vulnerable against man-in-the middle attack described by Gilbert et al.[2005]. We show that our protocol is secure against the man-in-the-middle attack with same tag and reader storage.

7.5 Application

Recently many researchers are working on Internet of Things (IoT). The main idea of IoT is the pervasive presence of RFID tags, sensors, actuators, mobile phones etc around us can be interacted using their unique identifiers [Giusto et al. 2010]. From the point of the private users, the most obvious effects of the IoT will be in everywhere of domestic and working fields. Security and privacy are two of the important issues in the IoT, since this technology is widely used in the physical world. Many living processes like online payment, transportation and transaction will depend on the application of the IoT. People will reject the IoT if there is no public confidence that it will not be a threat for privacy. There RFID tags are the important assets in the IoT applications. The problem is that when RFID tags are used in the IoT they spend most of the times unattended [Giusto et al. 2010]. Data can be scanned or modified by the adversary. To protect the RFID data from various attacks researchers suggested various RFID authentication protocols. Due to the suitability of the lightweight encryption technology HB+ protocol is suggested by many researchers in IoT. Since this protocol is not secure from man-in-the-middle attack the information in the tags can be vulnerable to the adversary (Gilbert et al. 2005). The proposed protocol EHB-MP is secured

from the identified threats and can be used to protect the RFID tags in the application of IoT. The proposed protocol is also a light weight protocol and it would be suitable in the IoT application.

7.6 Conclusion

A new efficient and secure authentication protocol EHB-MP using light-weight encryption technique is proposed to protect privacy for low-cost RFID system for ubiquitous environment. The HB+ and the HB-MP protocols are suppose to protect from both the passive and the active attack. However they are not protected from the special man-in-the middle attack. The proposed EHB-MP protocol derived from HB+ and HB-MP protocols by removing the existing privacy and security problems. It is protected from the man-in-the-middle attack as well as other attacks discussed in the privacy analysis section. The storage requirements for tag and the reader are also low. The proposed protocol requires the same storage as the HB+ and EHB-MP protocols and less than HB++ protocol.

The proposed scheme requires only lightweight cryptography which is suitable for low-cost RFID tag that makes it more efficient. It takes less storage and computation costs than hash-based RFID authentication protocol. Only drawback of the lightweight authentication protocols like HB+, HB-MP and EHB-MP are the number of iteration takes in data transmission between the tag and the reader. The comparison outlined in Section 7.4.1 and shown in Table 7.1 indicates that the protocol is both secure and efficient than HB+ and HB-MP protocols. A mathematical proof is given to show that the proposed EHB-MP protocol is fully protected from the man-in-the-middle attack.

Chapter 8 Implementation and Application

8.1 Introduction

The applications of RFID technology introduce many privacy and security threats in various commercial operations. The potential areas for RFID applications include e-passport, supply chain, automation, healthcare systems and baggage handling in aviation industry etc. In this chapter the privacy and security problems are identified in three most potential applications areas and architectures are proposed to use the developed protocols in these applications. Other systems also may use the same technologies as well. The application areas are:

- RFID in e-passport
- RFID in healthcare systems
- RFID in baggage handling in airport

8.2 RFID in e-Passport

An e-passport is a biometric passport that combines both paper and electronic chip. It includes biometrics information and *ID* using RFID chip. The goal of e-passport is to provide strong authentication through documents that unambiguously identify the passport holder. An e-passport can protect forging of *ID* and can make rapid progress in immigration. An e-passport is a machine readable passport, which is a biometrically-enabled and globally interoperable. The number of forged passports is increasing worldwide. Therefore, to strengthen national security against international terrorism or crime, nations all over the world are now proposing the use of electronic passports. The e-passport is difficult to forge and increases stability by intensifying the personal verification procedure [Schouten and Jacobs 2009].

An e-passport represents a bold initiative in the deployment of two technologies: biometrics and RFID. The U.S. government has mandated adoption of e-passports by the 27 countries in the Visa-Waiver Program in 2006 [Jules et al. 2005]. Other nations like Japan and most of the nations of Western Europe together with some other countries are involved in this project. These passports follow the guidelines of the International Civil Aviation Organization (ICAO), an organisation run by the United Nations with a mandate for setting international passport standards from Document

9303[ICAO 2004a]. The guidelines recommend the inclusion of RFID chips, microchips capable of storing data and transmitting it in a wireless manner into a passport. ICAO standard specifies face recognition for biometric identity verification. The e-passport will contain digitized photographic images of the passport holder's face. Additionally the standard specifies fingerprints and iris data as an optional biometrics. The goal of ICAO is the strong authentication through documents that unequivocally identify the passport holders.

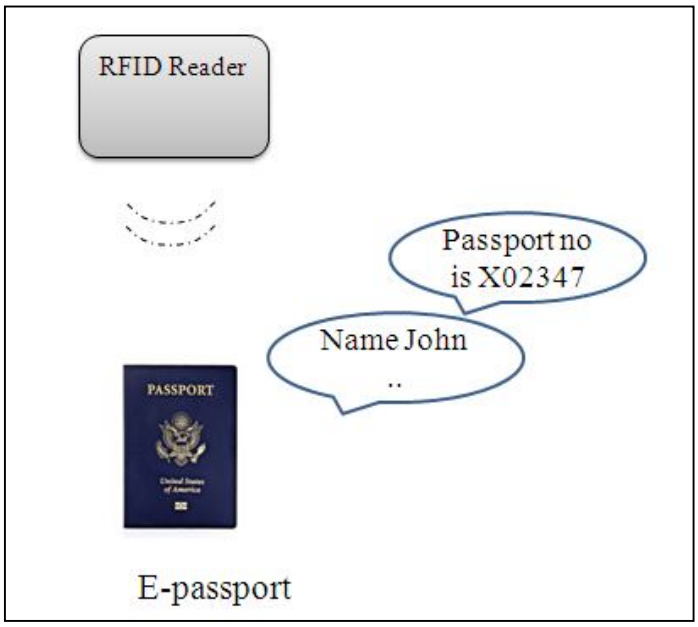

Figure 8-1: Unique Identification of a Passport Holder

The ICAO standard specifies face recognition for identity verification as the globally interoperable biometric. The US-VISIT program in fact requires visitors to provide two fingerprint images in addition to a headshot.

Malaysia has already implemented e-passports in a project before the ICAO standard. Since 1998, Malaysian passports have incorporated a chip consisting of an image of a thumbprint of the passport holder; a second generation e-passports introduced in 2003 that contains extracted fingerprint information only. In Kuala Lumpur International Airport, when a Malaysian passport holder passes through the automated gate that reads the thumb print from the chip and compares this thumb print to the thumb print given on a scanner [Jules et al. 2005].

However, the use of RFID tags used in an e-passport may cause privacy violation of users. Due to the unique identification number of the RFID tag, this is subjected to different privacy and security threats such as information leakage of a tag, traceability of the consumer, denial of service attack, and impersonation of a tag etc. This section investigates different privacy and security problems in RFID systems used in e-passport and proposes the implementation of a proposed authentication protocol to overcome those privacy and security problems. Simulation experiments show that the protocol is secure for larger entropy. There are many security threats are identified in e-passport due to the uses of the RFID [Jules et al. 2005]. A summary of the major general privacy and security issues in e-passport are outlined as follows:

- **Clandestine scanning**: Clandestine scanning is possible in RFID tags. The ICAO guidelines do not require authenticated transmissions between readers and passports. Consequently, an insecure e-passport is subject to short-range clandestine scanning (< 1 m), with attendant leakage of sensitive private information including the date of birth and place of birth.

- **Clandestine tracking:** According to the standard for e-passport, RFID chips (ISO 14443) emits the chip ID without authentication on protocol initiation. If this *ID* is unique for every passport, it could enable tracking the movements of the passport holder by unauthorized parties. Tracking is possible even if the data on the chip cannot be read.

- **Skimming and cloning:** Baseline ICAO regulations need digital signatures on e-passport. According to the regulations, such signatures allow the reader to verify the correct passport-issuing authority. In e-passport digital signatures do not bind the data to a particular passport or chip. They offer no defence against passport cloning.

- **Eavesdropping**: Faraday cage is a physical approach for countermeasure to clandestine RFID scanning. In an e-passport, a Faraday cage can be used in a form of metallic cover that prevents the scanning of RFID signals. Passports equipped with Faraday cages can be scanned only when the passport holders expressly presented them, and would allow most privacy concerns without knowing. Faraday cages, however, do not prevent eavesdropping on legitimate passport-to-reader communications, like those taking place in airports.

- **Biometric data-leakage**: E-passports also include biometric images. According to the ICAO standard, these will initially be digitized headshots. If the physical setting were controlled strongly, these images need to be secret to carry authentication. However, if the proposed uses of e-passports support automation, this may put some risk of biometric data leakage.

- **Cryptographic weaknesses:** ICAO guidelines specify an optional means for authenticating and encrypting the passport-to-reader communications. That is a reader reads the name, date of birth, and passport number to obtain a cryptographic key *K*. The key permits the passport to verify that if the reader is authentic before releasing RFID tag information. It is also used to encrypt all data transmitted between the passport and the reader. Once a reader knows the key *K*, it is revealed to the country's Customs agents forever. The cryptography relied upon by the ICAO standard itself has some minor flaws [Jules et al. 2005].

8.2.1 Biometrics

Biometric information is concerned about a specific person's aspect such as iris, finger print etc. It is physical characteristic or personal behavioural trait used to recognise the identity. With an ever increasing awareness of security and identity theft, there is a need to have a method to identify specific individuals uniquely and accurately. Biometrics is being used as a technology to provide the accurate identification. There are many biometrics in use today, with the most popular being [Jules et al. 2005] as follows:

- **Fingerprints:** A fingerprint is defined by the patterns found on a fingertrip [Jules et al. 2005]. It is unique to an individual. There are a number of methods for using fingerprints to recognize an individual. Some follow the traditional method used by police of visually matching minutiae. Other approaches use pattern-matching techniques.

- **Iris:** The iris is the coloured ring of tissue surrounding the pupil of the eye [Jules et al. 2005]. The iris is also unique for an individual. It needs to be scanned to use the iris as a biometric. The scanned value then can be matched with the templates to recognize or authenticate an individual.

- **Retina:** The retina biometric analyses the blood vessels at the back of the eye. This is also unique to an individual.

- **Voice:** The voice biometric is based on the frequency and/or time analysis of the voice. A template of the user's voice is taken by effectively recording the voice. As with most other biometrics the recording can be compared with a series of templates to perform the biometric check.

- **Face:** The face can be analysed by geometry of facial characteristics. The geometry is captured by taking a digital image of the face and then using software to analyse the characteristics.

- **Hand Geometry:** The geometry of a user's hand can be analysed in the same way as the face.

- **Signature:** A signature biometric is based on the image of the signature [Jules et al. 2005]. Signature biometric may be two types static and dynamic. A static signature biometric is solely based on image comparison, whilst dynamic analysis uses both the image and the dynamics of the signature.

Biometric authentication is the verification of human identity using biometric information [Jules et al. 2005]. It is the main mechanism by which human beings authenticate one another. When a person recognizes a friend by his or her voice or face, he or she is performing biometric authentication. Computers can do the same thing with increasing efficiency, and biometric authentication is gaining popularity as a means for people to authenticate themselves to computing systems. Typically, biometrics refers to the human-to-computer authentication. In practical biometrics for computing systems is different than for human-to-human authentication. Popular computer-oriented biometrics are fingerprints, face recognition, and irises. These are the three biometrics are selected for e-passport deployments.

The process of biometric authentication is almost similar in most of the systems. An authenticated user enrols by giving an initial, biometric image to the sensor. The system databse stores related information at the time of enrolment in a template. This template works as the reference for the

subsequent authentication of the individual. To prove identity during the time of authentication, the user again gives the biometric information to a verifying device. The verifying device checks the presented biometric information with biometric of the template for matching. The template and the image are matched successfully if they are mostly similar according to some defined metric [Jules et al. 2005].

8.2.2 Data Leakage Threats in E-passport

E-passports are vulnerable to clandestine reading of their contents without protection mechanism [Jules et al. 2005]. The short read range of the e-passport is also not free from some threats. It is possible to install RFID readers in doorways; tags can then be read from anyone passing through the doorway. These types of readers could be installed as checkpoints at airports, concerts and sporting events. On the other hand, clandestine readers could be installed in shops or to the entrances of buildings. These readers are mostly like the anti-theft gates at present used in thousands of retail stores. These types of readers would enable for appropriate surveillance of e-passports. E-passport contains personal data that a passport holder does not like to disclose to an unauthorised reader such as name, date of birth, passport number etc.

The RFID schemes of an e-passport may expose information when it is in operation. To avoid collisions the ISO 14443 protocol of ICAO and Malaysian second generation e-passports uses a unique *ID*. If the unique *ID* is static for each e-passport, then it gives a static response for tracking the movement of the e-passports. Due to the static identifier it can also enable hotlisting. In hotlisting, the adversary can construct a database matching identifiers to persons of interest. After this, the adversary can identify the person and extract information without needing to directly access the e-passport contents.

8.2.3 Cryptography in E-passports

The ICAO guidelines give varieties of mandatory and optional data elements. To guarantee the authenticity of this information, the guidelines contain many cryptographic techniques. The ICAO standard specifies one mandatory cryptographic feature for e-passports [ICAO 2004a, ICAO 2004b].

8.2.3.1 Passive Authentication

The data in an e-passport will be provided and approved by the authority of the issuing nation [ICAO 2004b]. The signature algorithms RSA, DSA and ECDSA are permitted for this. The passive authentication system shows only that the data is authentic and does not verify that the e-passport itself is authentic. The guidelines of ICAO indicate two additionally optional cryptographic aspects for better security in e-passports.

8.2.3.2 Basic Access Control and Secure Messaging

To protect the RFID tag data from the unauthorised readers, Basic Access Control stores a pair of secret cryptographic keys (K_{ENC},K_{MAC}) in the e-passport [Jules et al. 2005]. When a reader tries to scan the passport, it encounters in a challenge response protocol that requires the knowledge of the pair of keys and generates a session key. If authentication is successful, the passport gives its data contents. An unauthorised reader cannot access the passport. The keys K_{ENC} and K_{MAC} derive from optically scannable data printed on the passport such as the passport number, the date of birth of the passport holder, the expiry date and three check digits, one for each of the three preceding values. E-passports use the ISO 11770-2 Key Establishment Mechanism 6 as shown in Figure 8-2 [Jules et al. 2005]:

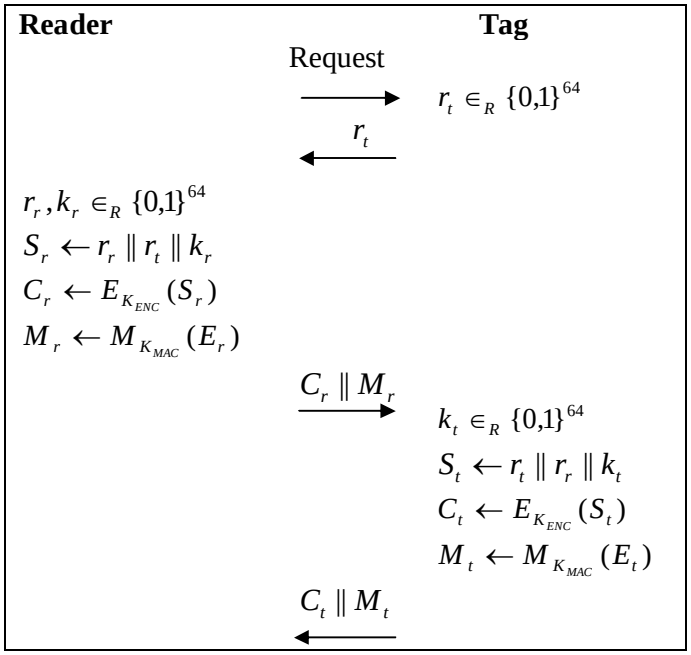

Figure 8-2: ISO 11770-2 Key Establishment Mechanism 6

E is two-key triple-DES in CBC mode with an all-0 IV, and *M* is the ANSI "retail MAC" [ISO algorithm, 1999].

1. In this protocol, the reader at first computes the MAC M_r the value C_r as described in the figure and sends to the tag.
2. The tag first verifies the MAC M_r and then decrypts the value C_r. The Tag then verifies that the r_t in the decrypted value matches the r_t which it previously sent. If any one of the verifications fails, the tag discards the values.
3. The tag then computes C_t and M_t and sends to the reader.
4. The Reader receives C_t and M_t and at first checks the MAC M_t and then decrypts C_t . The Reader then verifies that the correct r_r appears in the decryption of C_t. If any one of the verifications fails, the Reader discards the values.
5. If all the verifications are done correctly the reader and the tag derive a shared session key from the "key seed" $k_r \oplus k_t$, by using the key derivation mechanism described in the ICAO PKI report [ICAO 2004b].

The objective of the Basic Access Control is that the ability to scan the passport information should be only available when a passport owner wants to demonstrate the passport. However, the protocol has drawbacks to achieve this objective due to two reasons.

The first problem identified is that the entropy of the keys is too small [Jules et al. 2005]. The ICAO PKI Technical Report warns that the entropy of the key is at most 56 bits. Moreover, it further acknowledges that some of these bits may be guessable in some circumstances.

Second problem is that, a single fixed key is used for the lifetime of the e-passport [Jules et al. 2005]. As a result, it is impossible to withdraw the access of a reader to the e-passport once it has been scanned. If a visitor visits a foreign country, the visitor must give the key for Basic Access Control to the border authority. As the key is always fixed, this enables that nation to know the e-passport information in perpetuity. This information may be abused in the future

In spite of the limitations, Basic Access Control is better than no privacy measure at all [Jules et al. 2005]. The United States planned not to incorporate Basic Access Control in its e-passport

deployment. On the contrary, the Netherlands and Germany both plan to incorporate this Basic Access Control in the ICAO e-passport deployments.

8.2.3.3 Active Authentication

The ICAO guidelines specify another optional security feature which is referred to as "Active Authentication." The Active Authentication is an anti-cloning feature where as the Basic Access Control is a confidentiality feature. It does not protect information scanning from e-passport by the unauthorized parties [Jules et al. 2005].

The protection of the Active Authentication is based on public-key cryptography. The e-passport has the private key. The associated public key is also stored on the passport. In the ICAO guidelines specification an integer factorization based signature such as Rabin-Williamsis or RSA is presented. To authenticate the e-passport, it obtains an 8-byte challenge from the reader. It then digitally signs this message using the private key, and sends back the result. The reader also can check the validity of the message with the public key of the passport. The ICAO guidelines demonstrate the use of the ISO/IEC-7816 Internal Authenticate mechanism, with ISO 9796-2 Signature Scheme 1 padding for the underlying signature as shown in Figure 8-3:

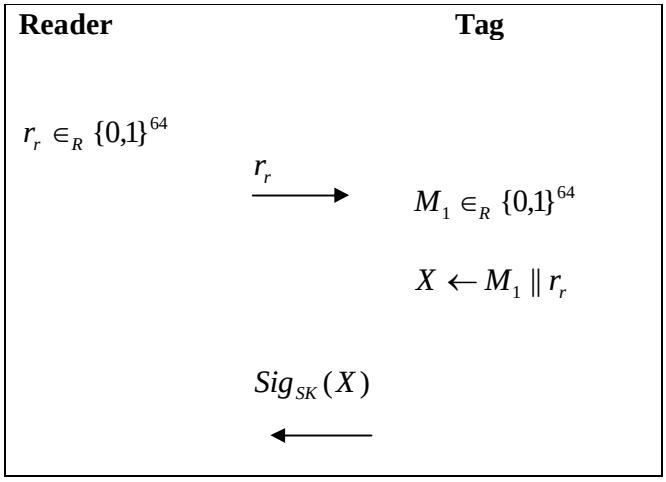

Figure 8-3: Signature

$Sig_{SK}(X)$ is an RSA or Rabin-Williams signature with 9796-2 padding signed with the secret key *SK* of the e-passport. *X* uses both the random number generated by the tag and a challenge from the

reader. This may be used to neutralize padding attacks [Coron et al. 1999]. The 9796-2 padding uses a hash function for example SHA-1 or other suitable hash function. The signature can then be verified with the public key which is stored in the passport. If the signature verifies, the reader assumes that the bearer's passport is supposed to hold the valid biometric data. It is further recommended that e-passport chips must support that data cannot be overwritten on the chip after personalization (U. S. Department 2004). Signing the chip's public key means the corresponding secret key is reliable to implement the security policy.

To avoid the man-in-the-middle attack the public key used for Active Authentication must be tied to the specific e-passport and biometric data presented [Jules et al. 2005]. Using a man-in-the-middle attack it is possible to one passport is presented, but a different passport is used to answer Active Authentication queries. This threat is recognized by the ICAO specification and mandates that Active Authentication occur in conjunction with an optical scan by the reader of the machine-readable zone of the e-passport. Therefore, every reader additionally has the hardware capability necessary for Basic Access Control with Active Authentication and compliant with the ICAO specification. Without this part is implemented properly the systems open themselves to a risk of cloned e-passports.

For effectiveness, the private key of Active Authentication must not leave a particular e-passport. The guidelines about this in the ICAO PKI report are not clear [Jules et al. 2005]. It only mentions that the keys shall be generated "in a secure way" and then stating that "no Key Management is applicable for these keys." In particular, the report does not prevent these keys from being read by a remote reader which is supposedly not the intention of the standard. The U.S. Concept of Operations document is also not clear. It does not also specify that Active Authentication keys cannot be scanned after personalization. The e-passports must also resist the same range of side channel and fault injection attacks traditionally found in the smart cards [Jules et al. 2005].

Active Authentication has another issue with Basic Access Control and privacy when they interact with each other. The certificate used for the verification of Active Authentication must be kept secret because it contains enough information to derive a key for Basic Access Control. In addition, when Active Authentication is used with RSA or Rabin-Williams signatures, responses from different e-passports can be distinguished. Consequently, Active Authentication allows tracking and hotlisting attacks even if the passive Basic Access Control is used. It is recommended that Active

Authentication should be applied only in a secure session after Basic Access Control has been used and session keys derived because Active Authentication needs an optical read of the e-passport, just as Basic Access Control does [Jules et al. 2005].

8.2.3.4 Related Works

Privacy and security issues are recognized by numerous media reports [Singel 2005]. Some issues are technical in nature and have seen less exposition. Pattinson outlines the privacy problems with e-passports that could be readable by anyone and argues for Basic Access Control (Pattinson 2004). Jacobs highlights the issues in e-passport use in the Netherlands and reports on work with a prototype Netherlands biometric passport [Jacobs 2005]. Jacobs also points out the importance of Basic Access Control and also investigates the issues surrounding a national database of biometric identifiers.

Various types of RFID authentication protocols have been proposed for typical RFID systems. Sharma et al.[2003] indicated the resource constrained in RFID tag as a main challenge to provide privacy and security. Weis at el.[2004] proposed a Hash-based Access Control (HAC) approach to protect a tag using a one-way hash function. The tag stores the hash of a random key as metaID. As the metaID is same for the tag all the times, it always transmits the same metaID, which can be easily tracked by an adversary [Singel 2005]. Another problem in this system is that the information is transmitted in plain text which could be easily eavesdropped.

Weis et al. [2004] also suggested another approach that is extended from HAC and referred to as a Randomized Access Control (RAC). It uses a random number to prevent location privacy. In each session the tag produces a response with a newly generated random number and its ID using a hash function. However, it cannot protect the system from replay attack and is not suitable in real life system where a large number of tags would be used because it requires many hash operations at the back-end.

Several researchers proposed RFID authentication protocol for pervasive computing environment. Rhee et al. [2005] proposed challenge response based RFID authentication protocol (CRAP) which is designed for use in pervasive computing. However, this scheme requires $(\frac{N}{2}+1)$ hash functions

computations which is impractical for large number of tags in ubiquitous computing. Choi et al.[2005] proposed a one-way hash based low-cost authentication protocol (OHLCAP), which is suitable for ubiquitous environment. Ha et al. [2007] claims that OHLCAP suffers from traceability and impersonation attack. They also propose a solution of using hash function to protect from traceability attack.

The researchers also proposed authentication protocol using varying identifiers. If a tag always replies with the same hashed ID before the next successful authentication it allows the tag to be tracked [Choi et al. 2005].

However, RFID authentication for pervasive computing environment is preferred for e-passport. The reason for this is that, the passport holder travels many countries and places can be authenticated anywhere when it is required.

8.2.3.5 E-Passport and RFID Chip

The ICAO standard for e-passports mandates that the RFID chip contains the passport holder's name, date of birth and passport number [ICAO 2004a]. For biometric information the e-passports will contain digitized photographic images of the faces of their bearers. The standard additionally specifies fingerprints and iris data as optional biometrics. The ICAO specification for e-passports depends on the specification given by the International Organization for Standardization (ISO) 14443 standard. It specifies a radio frequency of 13.56MHz. Tags in the ISO 14443 standard are passive, meaning that they carry no on-board source of power, and instead derive power indirectly from the interrogating signal of a reader. The intended read range of tags in this standard is about 10 centimetres.

Many large organizations like WalMart, Procter and Gamble, and the United States Department of Defence are deploying RFID as a tool for automation of their Supply Chains Management (SCM) [Jules 2006]. The RFID used for e-passports is not the same as the RFID used by WalMart and others for supply chain management. Supply chain tags are designed to be as simple and cheap as possible, with no support for cryptography and minimal additional features beyond holding a single identifier. The only privacy feature in the tags is a special "kill" command that renders the tag permanently inoperative. These supply chain tags operate at a frequency of 915MHz and have an

intended read range of 5 meters. On the contrary, e-passport RFID devices have a shorter intended read range. It also includes other features such as tamper resistance and cryptography.

The passport number in the passports of United States issued since 1981 is 9-digit long [Jules et al. 2005]. The first two digits encode the passport issuing offices. The remaining 7 digits are assigned arbitrarily. The passport number is unique for a country. It may help to identify the traveller uniquely. An RFID chip can contain the passport holder's name, date of birth, passport number of passport holder.

The ICAO guidelines specify a large range of mandatory and optional data elements. To ensure the authenticity and privacy of this data, the guidelines incorporate several cryptographic measures. The ICAO standard specifies passive authentication as a mandatory cryptographic feature for e-passports [ICAO 2004a, ICAO 2004b]. In passive authentication the data in an e-passport will be signed by the authority of the issuing nation [ICAO 2004b]. The passive authentication demonstrates only that the data is authentic. It does not prove that the e-passport is authentic. The ICAO guidelines specify two additionally optional cryptographic features for improved security in e-passports: Basic Access Control and Secure Messaging, Active Authentication. The next Section 8.2.4 presents the proposed cryptographic authentication protocol for e-passport.

8.2.4 Cryptographic Protection using a Complete Pervasive Authentication Protocol

In this section, the low-cost complete pervasive authentication protocol (CPAP) referred as SUAP1 based on challenge-response method using one-way hash function, hash-address and randomized hash function RFID system is presented [Morshed et al. 2010].

8.2.4.1 System Setup

The tag identifier *ID* represents the passport number or the passport *ID*. The protocol uses a one-way has function *h*. Database also contains the hash address *Had= h(ID)*. If the authentication is successful the RFID tag of the passport will expose its other information to the reader. The reader generates a random number r_1 and the tag generates a random number r_2. All the data fields *ID*, *x* and random numbers have the same *l* bits length. The hash function *h* also produces *l* bits response. The symbol $\oplus$ means exclusive-or (xor) operation and the symbol || means concatenation operation.

The secret number x is common in all the tags in this protocol. This can be implemented for the e-passport of one country.

8.2.4.2 CPAP Operation

When a tag enters into the range of a reader, the reader can initiate the authentication protocol. The protocol is shown in the Figure 8-4. The steps in the authentication protocol are as follows.

1. The reader generates a random number r_1 and sends it to the tag.
2. Receiving the number r_1 the tag generates another random number r_2.

   if r_1 *or* r_2 *is* 0 *stop protocol*

   otherwise perform the following computations

   $y = h(ID) + (r_1 \oplus r_2) \bmod (2^l - 1)$

   $c = r_2 \oplus x$

   $A = h(ID \| r_1 \| r_2)$

   The tag then sends the value of y, c and A_L to the reader. In this protocol c is used as a temporary variable to transmit the random number r_2 to the reader secretly. A_L is the left half of A.
3. The reader then sends the value of y, c and r_1, A_L to the back-end database.
4. The back-end database will calculate the following

   $r_2 = c \oplus x$

   $h(ID) = y - (r_1 \oplus r_2) \bmod (2^l - 1)$

   $h(ID)$ is the address of the record containing the ID where $Had = h(ID)$

   Access the address Had

   Retrieve the ID from the record

   Then the back-end database *Computes* $A = h(ID \| r_1 \| r_2)$

   if A_L *mathces*

   the tag is authenticated.

   The database sends A_R to the reader.

   Where, A_R is the right half of A.
5. The reader forwards the A_R to the tag

6. The tag compares the received A_R with the computed A_R. If they are equal then the reader is authenticated.

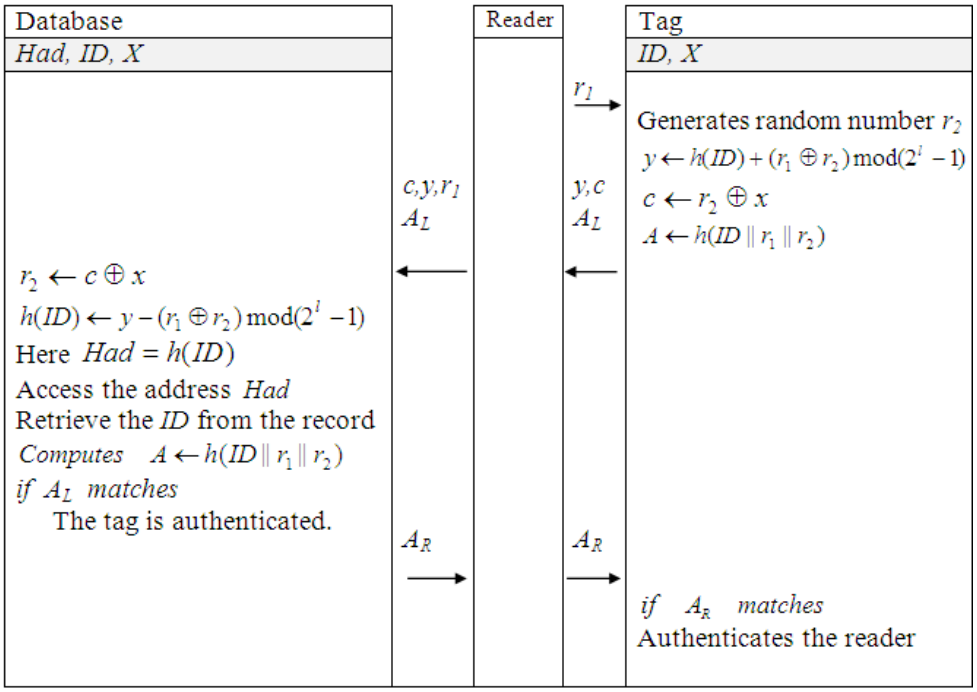

Figure 8-4: CPAP Protocol

8.2.5 Application and Evaluation

The e-passport security model using the cryptographic protection is shown in three layers in Figure 8-5. There are many sensitive information that a traveler may not want to expose to an unauthorized person. To protect information leakage and tracking of the passport holder's RFID chip or tag, information is only exposed to the authentic reader. The proposed authentication protocol prevents unauthorized readers from obtaining any information from the tags. The information from the passport is exposed in the air by encryption technique used in the proposed protocol. The reader can verify the encrypted data with the information stored in the database. The confidential code in the protocol is common for all the passports in same group. A confidential code (secret) number can be assigned for a country or a state as a group. An alternative way of using secret is to write the secret inside the e-passport together with the information such as passport number.

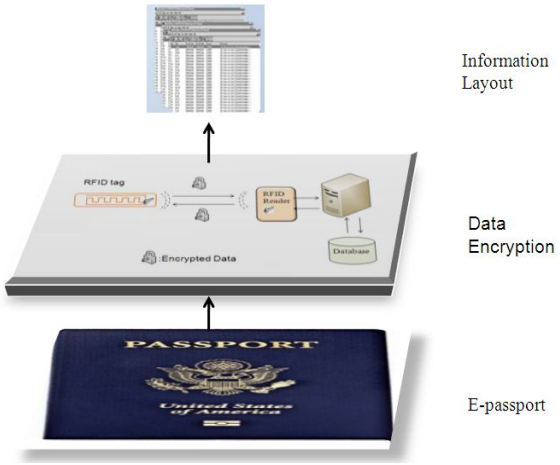

Figure 8-5: Security Implementation in e-passport

To evaluate the protocol it can be analyzed in two ways. Firstly is privacy and security analysis and secondly is efficiency analysis.

8.2.5.1 Privacy and Security Analysis

The privacy and security of the proposed protocol was analyzed against the threats discussed in RFID Privacy Problems in e-passport Section 8.2.

Clandestine scanning and tracking are not possible in the proposed protocol. An adversary must be authenticated to get any sensitive information from a tag. To authenticate an adversary they must know *ID*, *x* and r_2 to get any information from the tag. The combination of r_1 and r_2 makes the response *y* and *A* so unpredictable that an adversary can only guess the value or use brute-force technique with an advantage of at most $\frac{1}{2^l}$, which is negligible for a value like l=96.

Eavesdropping is also not possible by the adversary. Due to two random numbers in the tag side and the reader side the response is unpredictable. The adversary cannot extract any value from the response due to the one-way hash function.

Skimming and cloning are also not possible in this protocol. For each session the tag gives a new value of the response *y* that is totally indistinguishable and different from other sessions. Consequently, impersonation and replay attack is not possible in this system.

The cryptographic weakness is overcome by hash function and two random numbers. The one-way hash function with the random numbers always gives a result that cannot be produced and tracked by the adversary.

The summary of the privacy and security comparisons is given in Table 8-1.

Table 8-1 Privacy and Security Comparisons

Privacy Property	LCAP	CRAP	OHLCAP	Proposed CPAP
Information privacy	Y	Y	Y	Y
Tracking	N	Y	N	Y
Cloning/ Impersonation	A	Y	N	Y
Eaves dropping	Y	Y	Y	Y

Y: Provided A: provided under assumption N: Not Provided

8.2.5.2 Efficiency Analysis

The CPAP authentication protocol compares storage, communication and computation cost with the selected existing authentication protocols as shown in Table 8-2. It indicates that LCAP [Lee et al. 2005] as a reasonable performance however, it suffers from traceability problem and is also not ubiquitous. The CPAP protocol shows improved performance because it requires less tag side and database side storage and gives protection from all known attacks. The storage requirement for the tag and the database is small i.e. 2*l*, and 3*l* respectively, whereas OHLCAP Choi et al.[2005] requires 5*l* and 4*l* respectively. CRAP [Rhee et al. 2005] uses 1*l* storage for the tag but it needs $(\frac{N}{2}+1)$ hash operations which is unsuitable in practices because in ubiquitous environment the value of N is extremely high. It requires a large number of hash operations and therefore requires considerable computation time.

Table 8-2 Efficiency Analysis

Efficiency Criteria		**LCAP**	**CRAP**	**OHLCAP**	**CPAP**
Storage	Tag	1*l*	1*l*	5*l*	*2l*
	Reader	-	-	-	-
	Database	6*l*	1*l*	4*l*	2*l*
Computation	Tag	2*h*(+A)	3*h*(+A)	1*h*(+A)	*2h*(+A)
	Reader	-	-	-	-
	Database	2*h*+ε	$(\frac{N}{2}+1)h$	1*h*+ε	1h+ ε
Communication	Tag-to-Reader	1.5*l*	2*l*	2.5*l*	2.5*l*
	Reader-to-tag	0.5*l*	0.5*l*	0.5*l*	0.5*l*

A: Additional XOR and/or Add operations in tag ε: Small operation in back-end database

8.2.5.3 Simulation Experiment Result

To validate the proposed protocol CPAP and CRAP, simulation experiments have been conducted for comparison purposes. The objective of the simulation program was to check the anonymity of the response for one tag. The output of a hash function is the same for the same random number pair. The objective is to ensure unique response for different inputs of random number pair so that an adversary is unable to use any responses at later stage to access the tag or the reader. One response is compared with the subsequent responses for different random numbers. If it matches with any response it can be used by the adversary to attack the system by impersonation. The number of times a similar response is generated is given in Table 8-3. This number is represented by *m*. The experiment was conducted for 12, 16, 32 and 64 bits for secrets, random number and *ID*. We did not include the results for 12 bits since it is too short and result was very poor with many recurrences of the same response. The results shown in Table 8-3 indicated that for 64 bits there was no matching of the response and the responses were always unique. In this case the number of matching $m = 0$ in the Table. If the result is unique the adversary cannot use it for impersonation and replay attack. For 12, 16 bits there were some recurrences of the same response that means *m* is always > 0. For 32 bits the number of matching is $m >= 0$. It means sometimes the recurrences of the same response were found and sometimes the responses were unique. The matching of the response were due to two reasons, firstly it produced the same random number pairs. Secondly it produced the same responses for some other combination of random number pairs. If an adversary uses this response for these combinations of random numbers it may impersonate as a valid reader.

Table 8-3 Attacks and Success of an Adversary on one Tag in CPAP and CRAP

No. of Attempts	Attacker's Success					
	Data length (y=16 bits)		Data length (y=32 bits)		Data length (y=64 bits)	
	CPAP	CRAP	CPAP	CRAP	CPAP	CRAP
$4X10^{10}$	$m > 0$	$m > 0$	$m >= 0$	$m > 0$	$m = 0$	$m = 0$
$4X10^{12}$	$m > 0$	$m > 0$	$m >= 0$	$m > 0$	$m = 0$	$m = 0$

y: Tag response

This experiment indicated that with 64 bits the tag and the reader produced unique response for a tag *ID*.

The result was almost similar for 16 bits in the CPAP and the CRAP protocols since both the protocols produce the same responses many times. For 32 bits CRAP is always vulnerable by the recurrence of the same response but the proposed CPAP sometimes shows protected. The result was exactly same for 64 bits in the CPAP and the CRAP protocols since both the protocols shows no recurrence of the same response during the experiment. We did not perform any simulation experiments for the other protocols since it is already mentioned that logically and mathematically the LCAP and the OHLCAP are not protected against the identified privacy threats [Choi et al.2005, Ha et al. 2007]. CRAP is protected from all the threats but it requires a large number of hash operations in the database to search the tag. The CPAP and CRAP protocols successfully authenticate the tag and the reader without any privacy and security failure during the experiments undertaken for 64 bits.

However, the simulation experiment was done only for passive attacks. No active attack was applied to any of the protocols. It means we only tested the response to see if any recurrence of the same response was found. We did not manipulate the responses in the authentication process to attack the system using the same random number that an active adversary can do.

8.3 RFID in Health Care System: Privacy and Security Issues

Information technology and RFID has a tremendous potential in medical and healthcare service to improve patient safety and medical services. The use of RFID tags may cause privacy violation of users carrying an RFID tag. Due to the unique identification number of the RFID tag, this is subjected to different privacy and security threats such as information leakage of a tag, traceability of the consumer, denial of service attack, and impersonation of a tag etc. Through the tag the private data of a person can be tracked and the personal information can be captured which has implications on privacy regarding the Data Protection Act 1998 [Data 1998]. In the medical environment, the security and privacy problem will be crucial to RFID based medical application. The tracking of personal location or information of personal health and clinical history is sensitive for a patient. This section investigates different privacy and security problems in RFID systems used in hospital and proposes the implementation of the authentication protocol which has been developed to overcome those privacy and security problems. The proposed protocol requires less storage and computation than some RFID authentication protocols but offers larger ranges of security protection. Simulation experiment shows that the protocol is secure for larger entropy.

Healthcare is assumed to be the important potential area for RFID implementation [Ericson 2004]. Generally, the healthcare industry has been investing capital in Information Technology (IT) to reduce operating costs and improve patient safety. RFID is expected to become critical to healthcare organizations by achieving these two goals. Some hospitals and medical institutes are starting to conduct their own small-scale RFID testing projects. The application of RFID in healthcare is still in development stage. Healthcare organizations expect RFID technology can help save costs and improve patient safety. Many of them started with tracking and asset management of equipment. For automation RFID is being used in many hospitals [Wang et al. 2006].

8.3.1 RFID Privacy Problems in Medical Service

In the medical environment, the security and privacy problem will be crucial to RFID based medical application. In mobile RFID model, the user holds the RFID reader embedded in mobile phone. The user can use the reader to request information by capturing the tag attached to the patient. The reader then sends this information to the back-end database. The database subsequently returns the requested information to the reader and displays it to user. In an application where RFID technology

is being used to track an individual such as a patient in a hospital scenario this can be used to provide an enhanced secure and efficient environment. However, this can also be used for negative purpose to break the patient privacy [Lee and Kim 2007].

The privacy issue with tagged patient cards involves the risk of exposing the information, such as trace of personal location, information of personal health and clinical history. Through the tag the private data of a person can be tracked and the personal information can be captured which could be a violation of privacy under the Data Protection Act 1998. In the standard health level seven (HL7), the standard for customizing and detailed privacy mechanism has not yet been specified [Lee and Kim 2007]. Lee and Kim [2007] analyzed the privacy requirements for the ubiquitous service. It is not possible to solve the problems outlined with existing security technology, such as encryption and decryption. Using the security information acquired from the probing, the accessing application can access clinical information about an individual by querying the ubiquitous information server. In order to ensure privacy in this process, a mechanism of encryptions and decryptions of the outgoing data from tag and server has been proposed. However, these mechanisms may create limitations in the applicability of the ubiquitous service. In addition, if decryption of the information is successful, all information could be exposed. For this reason, Lee and Kim [2007] proposed a method that protects privacy in the ubiquitous system using a personal privacy policy in order to administer information more flexibly and securely as well as mitigate the problems discussed.

Many security threats are identified in RFID system in hospitals and some of these are similar to the threat types found in e-passport system [Jules et al. 2005]. Some threats in RFID systems in hospital are shown in the Figure 8-6.

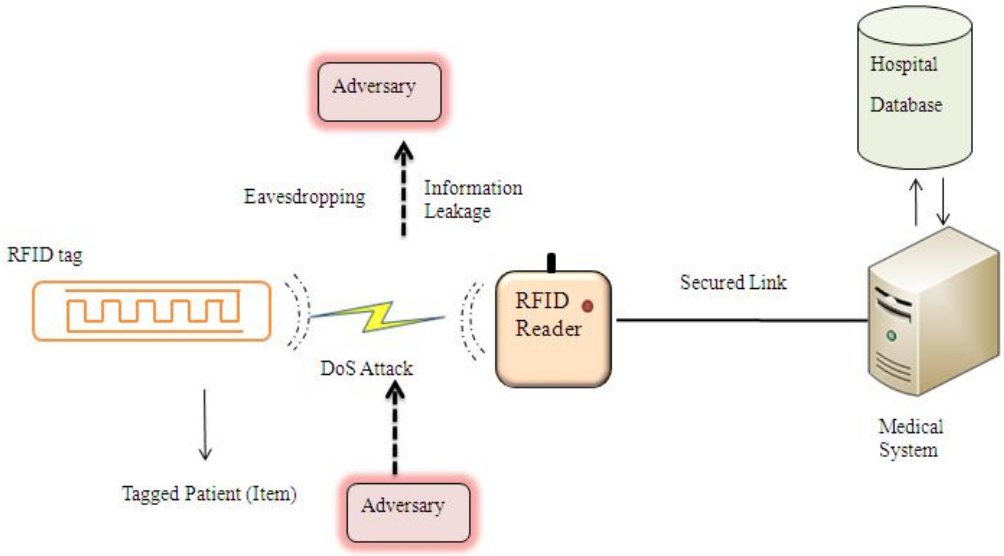

Figure 8-6: RFID Privacy and Security Problem in a Hospital

The identified threats are information leakage or clandestine scanning, clandestine tracking skimming and cloning, impersonation and replay attack and eavesdropping etc.

8.3.2 Related Works

Several types of RFID authentication protocols have been proposed. Different protocols are suitable for different purposes. Few of them are outlined in Section 8.2.3.4.

Lim and Kim proposed a privacy mechanism for RFID in healthcare system [Lee and Kim 2007]. They proposed a method that protects privacy in the ubiquitous system using a personal privacy policy in order to administer information more flexibly and securely as well as mitigating the privacy problems. In order to protect personal privacy of the patient, all of the treatment information should be controlled by privacy aware system. In addition, a unique RFID tag of the patient could also be used outside the hospital for emergency medical service or other hospital services.

8.3.3 Cryptographic Protection

In this section a new authentication protocol is adopted to ensure privacy and security of the RFID system effectively. This section analyses the privacy and security properties of the proposed protocol shows the results of the analysis and simulation experiment evaluation. This also proposes the implementation of the protocol in a hospital environment. This is a Novel Authentication Protocol for Hospital Systems (NAPHS) and is discussed as SUAP3 in Chapter 4. This is based on challenge-response method using the one-way hash function and the randomized hash function in the RFID systems.

The notations used in this protocol are as follows:

8.3.3.1 Notations

The notations used in this protocol are as follows:

h A one-way hash function, $h:\{0,1\}^* \rightarrow \{0,1\}^l$

l The length of an identifier

r_1 Random number in $\{0,1\}^l$

r_2 Random number in $\{0,1\}^l$

HID Hash Address of ID

ID Tag identifier

GID Group secret

$\oplus$ XOR operator

$\|$ Concatenation operator

$\leftarrow$ Assignment operator

Each tag and the database have a tag identifier *ID* and a group secret *GID*. The tag identifier *ID* represents the Patient ID.

8.3.3.2 NAPHS Operations

When a tag enters into the range of the reader, the reader can initiate the authentication protocol. The protocol is shown in Figure 8-7. The steps in the authentication protocol are as follows:

1. A reader selects a random number r_1 and sends a *Query* and r_1 to the tag.
2. After receiving the random number r_1 the tag will generate another random number r_2.
The tag computes

$$A \leftarrow GID \oplus r_2$$
$$B \leftarrow h(ID) \oplus (GID + r_1 \oplus r_2)$$
$$C \leftarrow h(ID \| GID \| r_1 \| r_2)$$

and sends the value of A,B,C_L to the reader.
3. The reader then sends r_1, A,B,C_L to the back-end database.
4. The back-end database then computes

$$r_2 \leftarrow GID \oplus A$$
$$HID_i \leftarrow A \oplus (GID + r_2 \oplus r_1) \quad \text{for all } GIDs$$
$$if \quad HID_i = HID$$
$$C \leftarrow h(ID \| GID \| r_1 \| r_2)$$

if C_L matched the *ID* is authenticated

5. The database sends C_R to the reader. The reader forwards C_R to the tag.
6. The tag verifies C_R

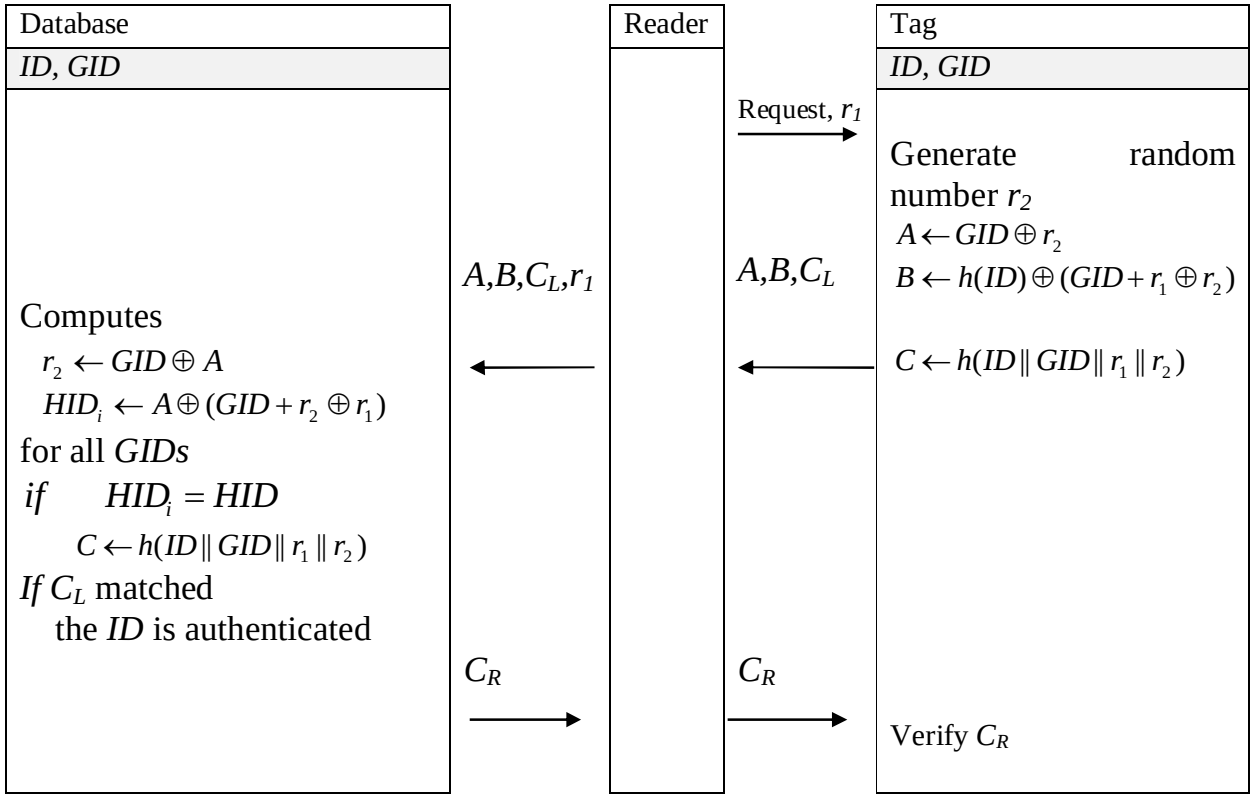

Figure 8-7: The NAPHS Protocol

8.3.4 Application and Evaluation

All the RFID tags and readers are equipped with the proposed RFID authentication protocols. There are several sensitive information that a patient or hospital authority may not want to expose to unauthorized person. The personal information of the patient, disease, diagnostics information, drugs usage and location are sensitive regarding a patient. All the patient, visitors, medicine, medical record, medical equipments use RFID tags supporting the proposed protocol. To protect information leakage, impersonation attack, tracking and cloning of an RFID tag the system should ensure that the information will be exposed only to the authentic reader. The proposed authentication protocol prevents unauthorized readers from getting any information from the tags as shown in Figure 8-8. The figure only shows the information of patient ID and its encryption in the RFID system and database. The authentication protocol authenticates the patient RFID tag and passes the encrypted ID to the encrypted database. The encrypted ID then passed to the patient ID database and can link the patient medical records. When any reader requests any patient information from the database it also authenticates the system with its patient ID and secret using the hash encryption. It then transmits the patient information encrypting with the hash function. The hash function uses the patient ID, any secret and random number to authenticate each other.

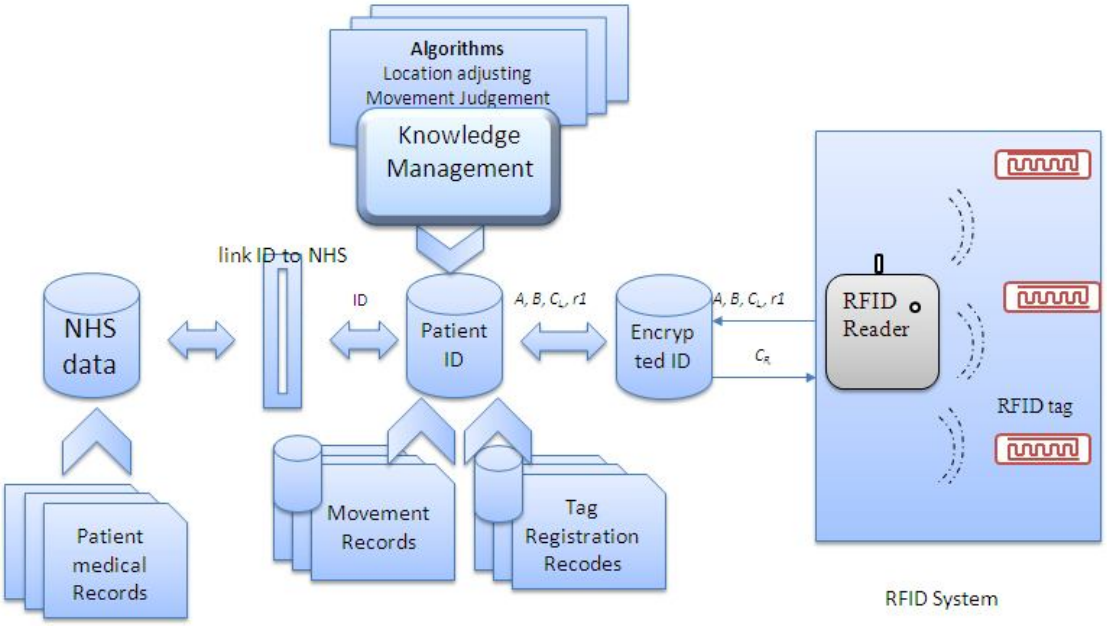

Figure 8-8: Information Encryption in Hospital

To evaluate the proposed protocol for privacy and security this was analyzed in two ways, firstly the privacy and security analysis and secondly the efficiency analysis.

8.3.4.1 Privacy and Security Analysis

The privacy and security of the proposed protocol is analyzed against the threats information leakage, location privacy, impersonation and replay attack, message interception and tracing.

- **Information Leakage or clandestine scanning:** To obtain any sensitive information from a tag this must be authenticated. To authenticate the system an adversary must know *ID, GID* and the hash function. The combination of r_1 and r_2 with *ID* and G*ID* makes the response *y* unpredictable.

- **Location Privacy:** The value of *C* cannot be linked with any particular tag. The protocol ensures location privacy by using new values of r_1, r_2 each time. The *ID* is also updated after every successful session.

- **Impersonation and Replay Attack:** Without the knowledge of the *ID*, the hash function and the secret *GID* an adversary is unable to impersonate. For each session the tag generates a new value of *C* which is totally indistinguishable and different from other session and subsequently the impersonation and replay attacks are not possible.

- **Message Interception:** The protocols use static identifier and secret. These do not face any update anomalies. If the adversary is able to prevent the last transmission to the tag from the reader it will not face any synchronization problem.

- **Traceability:** An adversary is unable to identify the tag from its response because each time it gives a different value which is non traceable from other responses. The adversary does not know the r_2, *ID,* secret *GID* and the hash value. This scheme is fully protected from the future forward and backward traceability.

The summary of the privacy and security properties is given in Table 8-4. The privacy and security properties of the proposed protocol are compared with three other schemes HIDV, LCAP, OHLCAP and EOHLCAP. The three schemes were chosen because all of these protocols involved

tag authentication and involve secret update process. The table shows that the proposed protocol provided protections from all the identified privacy and security threats. Some of the privacy and security properties are further tested by simulation program and outlined in Section 8.3.4.3.

Table 8-4 Privacy and Security Comparisons

Property	HIDV	LCAP	OHLCAP	EOHLCAP	Proposed
Information privacy	Y	Y	Y	Y	Y
Location Privacy	N	N	Y	Y	Y
Impersonation	N	A	N	Y	Y
Replay attack	N	Y	N	Y	Y
Message Interception	Y	Y	Y	Y	Y
Backward Traceability	N	Y	N	Y	Y
Forward Traceability	N	Y	N	Y	Y

Y: Protected A: provided under assumption N: Not Provided

8.3.4.2 Efficiency Analysis

Storage, communication and computation cost were considered for efficiency analysis. The efficiency of the proposed are also compared with three schemes HIDV, LCAP, OHLCAP and EOHLCAP as in privacy and security comparisons. Various existing authentication protocols were compared with the proposed authentication protocol. HIDV requires a larger storage and computations than other protocols and suffers from location privacy issues. It is also vulnerable to impersonation attack. LCAP appears to be better in performance however, it has location privacy problem [Choi et al.2005].

Table 8-5 Efficiency Analysis

Efficiency Criteria		**HIDV**	**LCAP**	**OHLCAP**	**EOHLCAP**	**Proposed NAPHS**
Storage	Tag	3*l*	1*l*	5*l*	3*l*	2*l*
	Reader	-	-	-	-	-
	Database	10*l*	6*l*	4*l*	3*l*	2*l*
Computation	Tag	3*h*	2*h*	1*h*(+A)	1*h*(+A)	2*h*(+*A*)
	Reader	-	-	-	-	-
	Database	3*h*+ ε	2*h*+ ε	1*h*+ε	$(\frac{m_i+1}{2})h+\varepsilon$	1*h*+ ε
Communication	Tag-to-Reader	3*l*	1.5*l*	2.5*l*	2.5*l*	2.5*l*
	Reader-to-tag	2*l*	0.5*l*	0.5*l*	0.5*l*	*0.5l*

A, ε: Small operation in tag, back-end database *f:* Function operation

The proposed protocol shows improved performance as shown in Table 8-5 because it requires less tag side and database side storage than the protocols OHLCAP and EOHLCAP and gives protection from the all identified attacks. The storage requirement for the tag and the database are 2l, and 3*l* respectively. The protocol requires less hash function in both the tag and the database. EOHLCAP gives protections from all the attacks but it needs $(m_i+1)/2$ hash operations which is costly because the value of m_i may be very high and many hash computations will make the protocol slower.

8.3.4.3 Simulation Experiment Result

To validate the proposed protocol, simulation experiments have been conducted. The objective is to ensure unique response for different inputs of random number pair so that an adversary is unable to use any responses at later stage to access the tag or the reader. The program checks to match a response *y* for different sets of random numbers. The number of times a similar response is generated is given in Table 8-6.

Table 8-6 Attacker's Success Table

Exp No	Number of Queries to the Tag	Attacker's Success for different data length	
		Data length	Number of Matches
1	10^{11}	16	1511114
2	10^{11}	16	1505568
3	10^{11}	16	1526852
4	10^{11}	32	0
5	10^{11}	32	42
6	10^{11}	32	0
7	10^{11}	32	40
8	10^{11}	32	0
9	10^{11}	32	0
10	10^{11}	64	0
11	10^{11}	64	0
12	10^{11}	64	0
13	10^{11}	64	0
14	10^{11}	64	0
15	10^{11}	64	0
16	10^{11}	64	0
17	10^{11}	64	0
18	10^{11}	64	0
19	10^{11}	64	0
20	10^{11}	64	0

The experiment was conducted for 16, 32 and 64 bits for secrets, random number and data. The results shown in Table 3 indicated that for 64 bits there no matching response and the results were always unique. For 16 and 32 bits there were some recurrences of the same response *y*. This was due to two reasons. Firstly it produces the same random number pairs. Secondly it produced similar responses for some other combination of random number pairs. This experiment indicated that during the experiment with 64 bits the tag and the reader produced unique response for a tag ID. The Table 8-7 shows the summary of the evaluation.

Table 8-7 Attacker's Success Table

Number of queries	Attacker's Success		
	Data length (16 bits)	Data length (32 bits)	Data length (64 bits)
	y	*y*	*y*
10^{11}	>=0	>=0	0

This experiment showed that the protocol is secure for 64 bits in 10^{11} attempts. For 16 and 32 bits there were some recurrences of the same response that can be used by an adversary.

The proposed scheme requires only one one-way hash function operation that makes it highly efficient. The storage requirement for the tag and database is also low in comparison to the other protocols. The comparison shows that the protocol is both secure and efficient than these protocols and it has many practical advantages like simplicity, privacy and security protection. The protocol is also implemented for the security of wireless database communication. The information is shared outside only with encryption proposed in the protocol. Simulation experiment indicated that for 16 bits data the RFID system is fully vulnerable to adversary attack.

8.4 An Airport Baggage Handling System using RFID Technology

In this section a new architecture is proposed for airport baggage handling using a combination of technologies such as RFID, the internet, networks, web and mobile communications. In this section the problems associated with handling baggage in airport are identified and a solution to overcome those problems is proposed using RFID technology. Some novel ideas to use popular technologies such as web, SMS and interactive television screens for baggage handling systems using RFID

technology are also proposed. The total baggage path is divided into several zones to track them correctly and to identify where baggage was lost or mishandled if possible.

8.4.1 Handling Baggage in Airport

Today, airlines are facing a number of challenges. The increasing number of air passengers and hence the increase in checked-in baggage is stressing the world's baggage handling systems. In this process many pieces of baggage are mishandled and lost. The cost of a mishandled bag is a major concern for the airlines, and the problem is growing day by day. In addition to the penalty incurred by the airlines for the mishandled bag, it is also a source of great inconvenience and dissatisfaction for the passenger.

RFID can enhance the automation of baggage handling and can significantly reduce the number of mishandled bags. In the recent years, many airports have initiated the implementation of RFID technology in the aviation industry replacing barcode for the automation of baggage handling and to reduce the mishandling of baggage. The growing number of air passengers and their baggage are creating a big challenge for the airline authorities. Major increases in the reported incidents of mishandled baggage give evidence of this challenge. Increased safety regulations in airports, growing passenger numbers and tight turn-around times are some of the main cause for baggage mishandling [AeroAssist 2008]. Passengers on U.S. airlines reported more than 4 million mishandled bags in the year 2006 [Reuters 2006]. In Europe, the Association of European Airlines (AEA) also reported that the incidence of mishandled baggage has increased by 1.2 million which is about 14.6 percent more than the previous year. The cost of a mishandled bag is also increasing rapidly. In 2006, approximately 34.3 million bags were mishandled globally, costing the airline industry $3.8B [Motorola 2007]. Giving the importance of missing baggage in airports, the Association of European Airlines (AEA) published a report [AeroAssist 2008] on 27 major airlines that reported baggage information to AEA. AEA identified the 7 or 8 most affected airlines each year as an "Above average" group in terms of missing bags per 1000 passengers as shown in Figure 8-9. Among them were Air France, Alitalia, British Airways, KLM, Lufthansa and TAP (Transportes Aéreos Portugueses) Air Portugal. The 'Above average' group has an average in itself that can be as high as 27% (in 2007) compared to the average of all AEA companies. Sometimes any one reason may cause poorer performance and can cause additional trouble to an airline. TAP airline is an example for this that shows very high rates of bags missing in 2007 due to the

extremely busy and exhausted Lisbon Airport. Due to these localized problems, airport baggage mishandling rates may differ significantly among the different airlines as can be seen in the Figure 8-9.

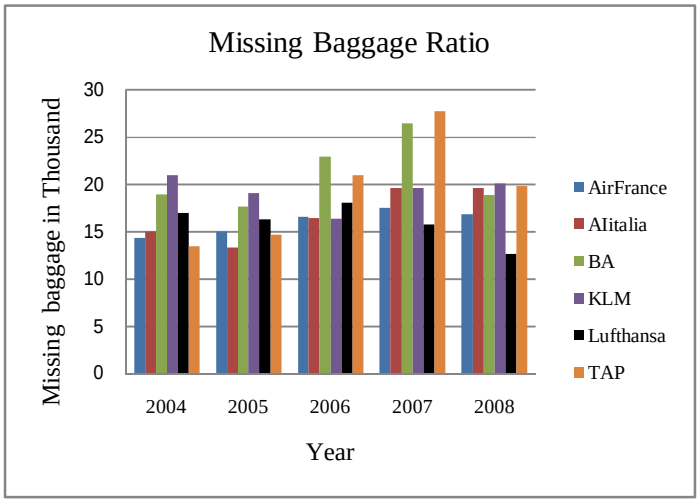

Figure 8-9: Missing Bags per 1000 Passengers: Airlines with Highest Rates

(Source AEA Consumer Reports, 2004-2009, Compiled by Authors)

According to the International Airport Transport Association (IATA) survey there are six key issues that are identified for baggage mishandling in air travel [Motorola 2007]. These are shown in Table 8-8.

Table 8-8 Six Key Issues Identified for Baggage Mishandling

Reasons for mishandling	Rate
Transfer bag: late arrival	30%
Transfer bag: delay in moving bag	18%
Missing baggage sortation message	11%
Error at check-in	10%
Poor barcode read rate	10%
Transfer passenger not checked in	10%
Other	11%

Source: IATA, RFID business case for baggage tagging, 2007

Most of the major causes can be reduced using RFID technology. The logical characteristics of baggage handling systems are well suited to RFID, which can help make the baggage handling process easier and efficient.

8.4.2 RFID in Business Domains

Passive tags are low-cost, have no on-board power and work in unused frequency ranges which are suitable for implementation in business enterprises and also in the aviation industry. RFID is widely used in many business areas [Zhang et al. 2008]. It has a significant benefit to supply chain management due to its low cost and flexibility. RFID has comparative advantages over other technologies such as barcodes, because it is, for example, contact-less, has multi-object recognition, does not require line-of-sight, and has long-distance reading capabilities. The demand for RFID is increasing day by day. In [Harrop 2006] the author points out that the RFID industry will increase by US $2.8 billion in 2006 to $26 in 2016. Large organizations like Wal-Mart, Procter and Gamble, and the United States Department of Defence are employing RFID tags for automated oversight of their supply chains [Jules 2005]. The UK retailer Marks and Spencer has also initiated the use of RFID tagging of individual items of apparel [Collins 2004]. The potential offered by RFID technology is that all existing physical objects can be managed by a virtual world created by a distributed database in a distributed networked RFID system.

8.4.3 Current Usage of RFID in Aviation for Baggage Control

A number of airports have started to use RFID on a trial basis to handle baggage [White paper by AeroAssist 2008]. Hong Kong International Airport is the first airport in the world to have implemented RFID baggage tagging which has been fully functional since 2005. Bag-tag read success rates were improved to 95% with estimated cost savings of US$ 3.8 million. Later, the read rate increased to more than 97%, much higher than the barcode rate [Hong Airport Press release 2008]. Beijing, Narita and six other Korean airports have also undertaken successful RFID trials. McCarran Airport in Los Angeles was the first airport in USA to adopt RFID tags in baggage handling. Amsterdam Schiphol Airport was the first airport in Europe to make a large scale attempt to introduce RFID baggage control in 2007.

IATA has published some results based on the trials that have been conducted between airports, airlines and manufacturers during the last few years [IATA 2007]. The main objective of the trials was to test the read rate success. The results are summarized in Table 8-9

Table 8-9 RFID Trial Read Rate

Trials	Date	Read-Rate
Kuala Lumpur Airport	2005-2006	100% (Gen 2) 98% (Gen 1)
Kansai-Hong Kong Airport	2005	95.4% 98.78%
Asiana- Korean Airport Corporation	2004-2005	97.00%
TSA World-wide Trial	2004-2005	~99%
Narita Airport	2004	-
British Airways at Heathrow T1	1999	96.40%

Compiled by author (see [IATA 2007])

The objective of the trial in Kuala Lumpur International Airport was to study the characteristics of UHF tags placed on the test baggage in various situations to identify when reading would become difficult, to study the recognition rate by placing the UHF tags on passenger's baggage in the actual airport environment, and to verify the effectiveness of the baggage tags during operations between airports and the effects on the UHF band by the airport facility materials. In this trial a large amount of RFID materials have been tested and performances analyzed in detail.

The objective of the trial in Kansai Airport- Hong Kong Airport was to carry out a basic performance validation in an operational environment different from Narita Airport and

- to verify the international interoperability of Japan's UHF-band airline baggage tag
- to confirm the data recognition at Kansai International Airport of the airport baggage tags that were attached in Hong Kong
- to verify the UHF band radio frequency characteristics
- to verify the electric intensity measurement inside the airport.

The trial by the Asiana-Korean Airport Corporation used six Korean airports. Tags for baggage were issued at check-in and were read at a number of points in the baggage process. RFID was used to track the baggage through security, reconciliation and finally to verify its arrival. When the baggage arrived in the claiming section, the passenger received a Short Message Service (SMS) about the location of the baggage. Passengers could also see the information on the Flight Information Display System (FIDS). The trial also focused many new processes. RFID systems enabled the creation of a link between the security screening station and the airline security database, allowing the passenger owning a piece of reported baggage to be identified and security staff notified. This baggage could then be manually searched after an x-ray. RFID was also used for the enhancement of the manual sortation process. RFID systems also gave the baggage loaders the right flight information for the baggage to be loaded. This was a successful trial with a read rate of 97%. The trial also showed the way in which RFID can be used to enhance processes and improve customer service.

The aim of the Transportation Security Administration's (TSA) world-wide trial was to demonstrate the interoperability of UHF RFID baggage tag systems between worldwide geographic regions having different UHF transmission regulations.

8.4.4 Baggage Handling Using RFID: A Proposed Architecture

RFID can help the baggage handling system in aviation in many ways. It can enhance the automation of baggage handling and can simplify the baggage handling system [Motorola 2007]. It can also identify the place and people correctly related to this baggage thus it can significantly reduce the number of mishandled bags. The flowchart of the baggage handling process is given below (Figure 8-10).

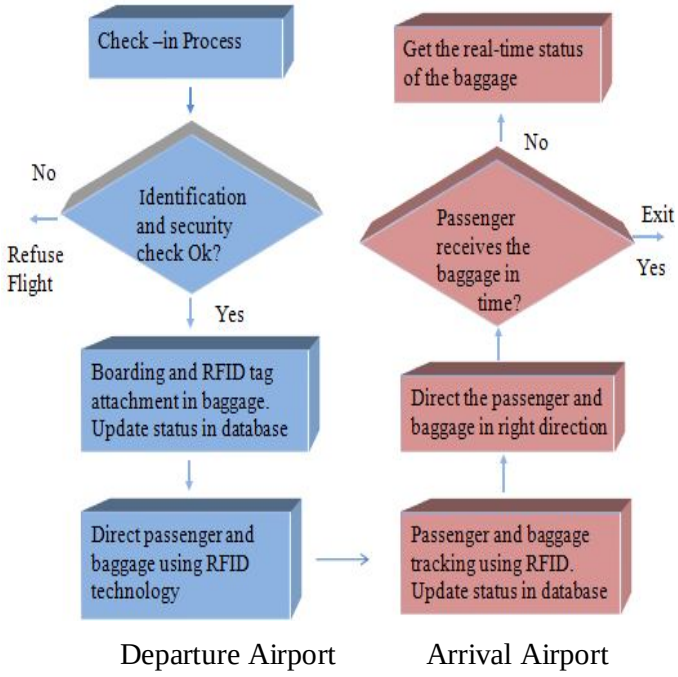

Figure 8-10: Logical Flow of Baggage in Airport

8.4.4.1 Making Zones for Identification

During air travel, baggage goes through various paths and places, and it is not possible to track the baggage at every point. For this reason various key points of the route are needed to identify. To identify the key points and track the baggage, the area passed by the baggage will be divided into several zones to determine its location, where it is kept or where it may be mishandled. The total area for the baggage can be classified into the following zones [Motorola 2007] at the departure airport as shown in Figure 8-11 and outlined as follows:

1. Check-in area
2. Conveyor
3. Distribution area
4. Trolley

Each zone will be implemented with an RFID system in such a way that any baggage passing through will be tracked correctly. The incoming, outgoing and duration of stay of the tags can be determined from the system. All the data will be recorded in the back-end database.

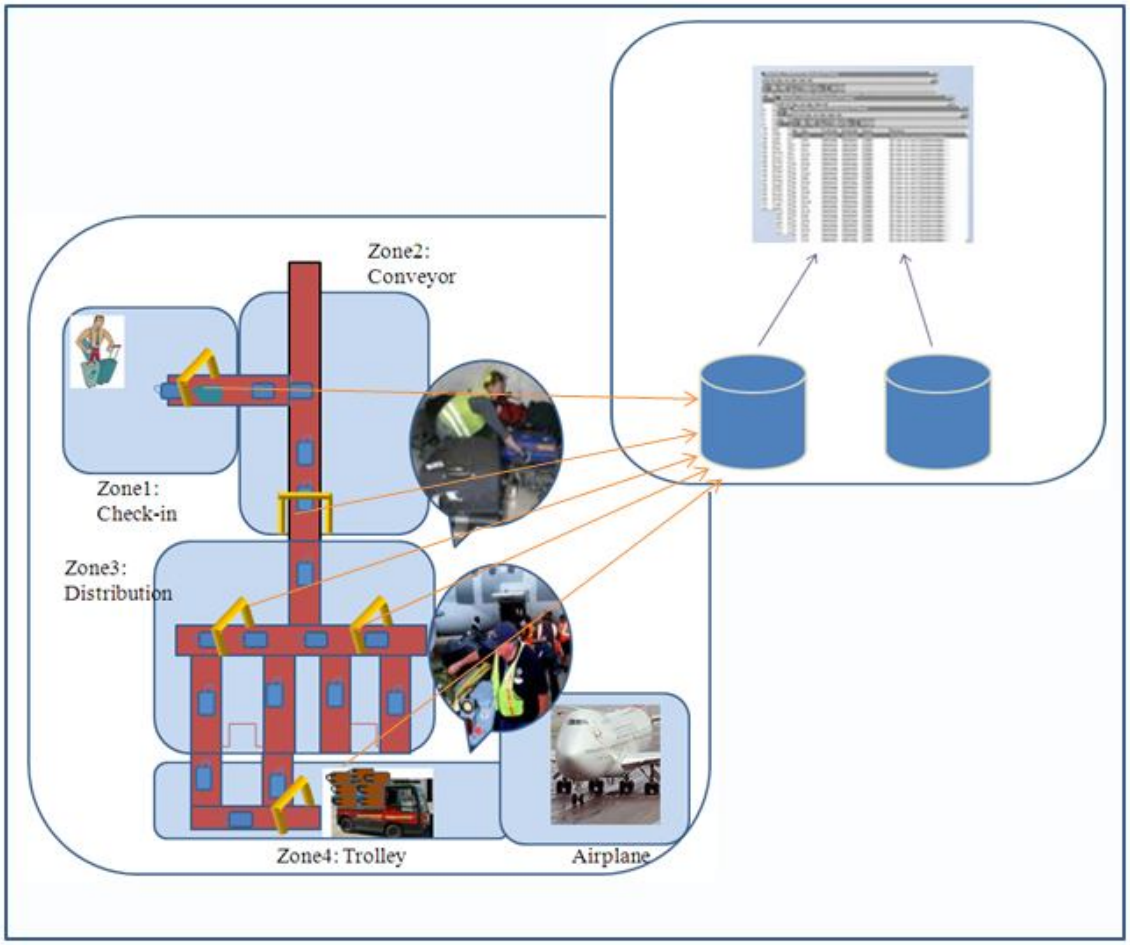

Figure 8-11: Baggage in Different Zones

Each member of staffs will carry an RFID tag in his batch and an identity card. Responsibility will be distributed between different zones and employees of each zone will be responsible for their respective zone. So, in each zone the staff will be identified by RFID tag. During duty time, staffs are required to keep their identity card with them and they should wear a uniform with an RFID batch. Staffs are allocated in each zone for different time schedules. In each zone there are RFID readers to scan the RFID tag of the baggage and the staff. The staff will also be responsible for handling and controlling the RFID readers. The total process can be described in several phases of zones:

- ***Check-in area:*** In the check-in areas, RFID printers enable the instant encoding of an RFID tag including required information such as flight information and any specific sortation directions. Before placing the bag on the conveyor an RFID reader captures the tag information and stores in the middleware database.

- ***Conveyor:*** As baggage moves to the conveyor belt an RFID reader can track the bag through the RFID tag and capture the available information from it, providing the information required to ensure delivery of the right bag to the right gate, right airline and right flight.
- ***Distribution area:*** Throughout the routing area, RFID readers capture the location of bags at key check points that help to identify the baggage and verify if it is moving in the right direction at real time to ensure timely and correct delivery to the airline.
- ***Trolley:*** Also, RFID readers can capture the information from the baggage to check that it is loaded onto the right trolley for delivery to the right plane. If any bag is mistakenly placed on the trolley it can easily be identified before it leaves, thus saving time.

The zones in the arrival airport are:

- ***Trolley:*** Baggage is loaded from the airplane and shifted to the right distribution area using the help of the RFID system. The arrival information will then be updated to the arrival airport database.
- ***Distribution area:*** In the distribution area the baggage will be sorted and distributed to the right conveyor using RFID system. Baggage loaders will be informed if any wrong placements of baggages are done.
- ***Conveyor:*** When the baggages are forwarded to conveyor it also takes the help of RFID system to move in a right direction. Databases will be automatically updated with the latest status.
- ***Reclaiming belt area:*** Passengers will receive an SMS to their mobile phones so that they are sure about their baggage arrival. Passengers can also search in the internet about their baggage with a password. If the baggage arrives correctly then systems will automatically send the SMS to the passenger's mobile informing them of the location of their baggage. Also, an email will be sent to the passenger with details of the baggage status. Airport authority will provide computers with internet and browsing facilities near the baggage receiving section. Passengers can also get information from the baggage query section of the information desk. The baggage query section can find information on the baggage from their database or online internet service and the scenario is shown in Figure 8-12.

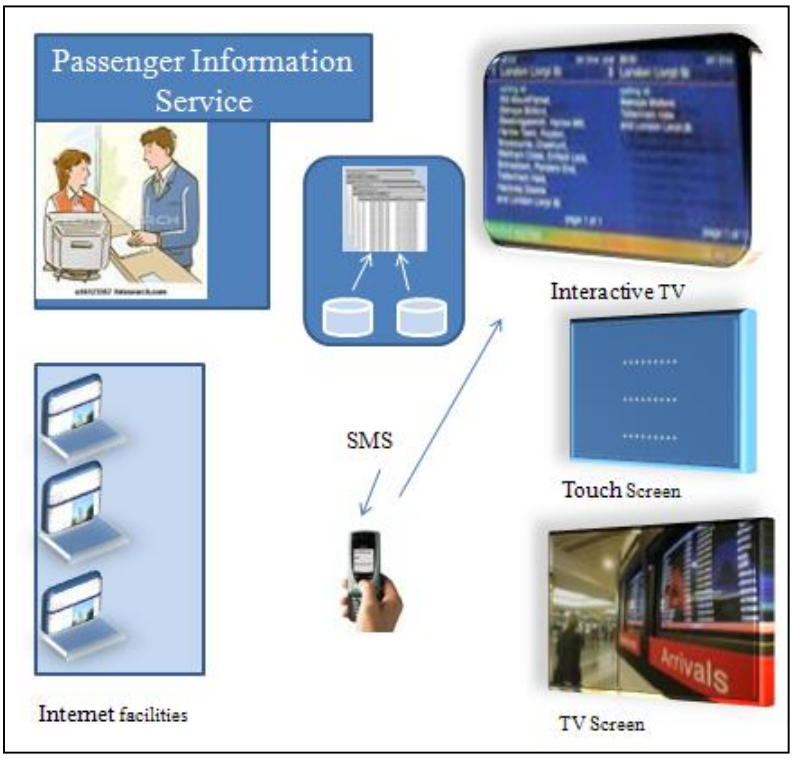

Figure 8-12: Passengers Receive Information in Various Ways

Utilization of RFID in Airport Baggage Handling IATA in [Das 2007] reported that the major reason why baggage is mislaid is due to the problem of reading barcodes properly on the baggage. RFID technology can offer a number of significant advantages over barcode solutions:

- Flexibility: Barcodes require line-of-sight contact with readers. In contrast, RFID tags are readable without line-of-sight contact and without precise positioning [Jules 2006].
- Ability: RFID can scan multiple bags simultaneously and distinguish from other items; it identifies the object as opposed to bar code, which is used for a single scan at a time.
- Reliability and accuracy: RFID is suitable for a fully automated system and can read reliably with up to 100% accuracy [Motorola 2007].

RFID technology can offer many opportunities in luggage handling in an airport terminal. Some typical scenarios and solutions using RFID technology are outlined as follows:

- **Real time tracking and management:** RFID can ensure real time information about the baggage. The current location of the tag is always available on the database. The passenger can get information on his baggage anytime and from anywhere. Using RFID, it is possible to identify exactly which baggage is in which container and in which place. Checking the baggage against the passenger 'aboard aircraft' status, and locating the container which

holds the passenger baggage is very important from the point of view of both security and operational efficiency [Celino and Walsh 2000].

- **Cross checking:** Cross checking is very easy and efficient using RFID technology. The movement of both the baggage and the passenger can be tracked. It can easily be checked if a passenger is on the board but the baggage is not and vice versa.

- **Digital imagery:** It is now possible by using an RFID tag attached to an identity card and air ticket to identify who is travelling. An X-Ray picture of the suitcase with RFID tag can identify what is being carried by different passengers (Figure 8-13).

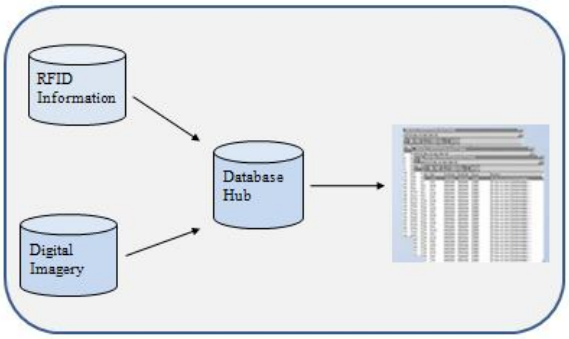

Figure 8-13: RFID Information with Digital Image.

- **Safety against new crimes:** In this era of RFID technology different types of crime are emerging, for example changing or killing the RFID tag information by RFID reader. Some adversaries can change the RFID tag of a bag in order to mislead the owner. This can be done without physical evidence using RFID reader from any covert place such as his pocket. In this case, a video camera cannot identify the adversary. RFID systems can trace this event if the tag seems absent due to unauthorised killing.

- **Identify who handled the baggage last:** Using RFID technology it is possible to identify the zone and the people group who handled the baggage last. From the database it is possible to identify approximately who was near the baggage in that location. This information can be used, with video cameras, to identify who mishandled or stole the baggage.

8.4.4.2 RFID Privacy and Security Protection

The baggage handling and passport system are similar and consequently the protocol has been outlined to avoid repetition. Some baggage may contain items that may be private and valuable and could be tracked by its RFID tag anywhere in the world. The owner of the baggage may not wish to expose the information to others and adversary could try to track the baggage. To protect the reading of the RFID serial number and tracking of the baggage data encryption protocol can be used. Appropriate RFID protocol can be chosen to protect the privacy and security of the RFID tag used in the baggage. Since the baggage moves many countries the RFID protocol should support ubiquitous computing environment. Due to this reason the proposed SUAP2 RFID authentication protocols may be suitable for the RFID system for the airport baggage handling. The SUAP2 protocol requires three fields in the tag side *ID*, *GID* and *x*. The ID is unique for all tags. *GID* may be used for the group and can be used to identify the Airline. The reader communicates with the tags using the data stored in the database. The conceptual framework is shown in Figure 8-14.

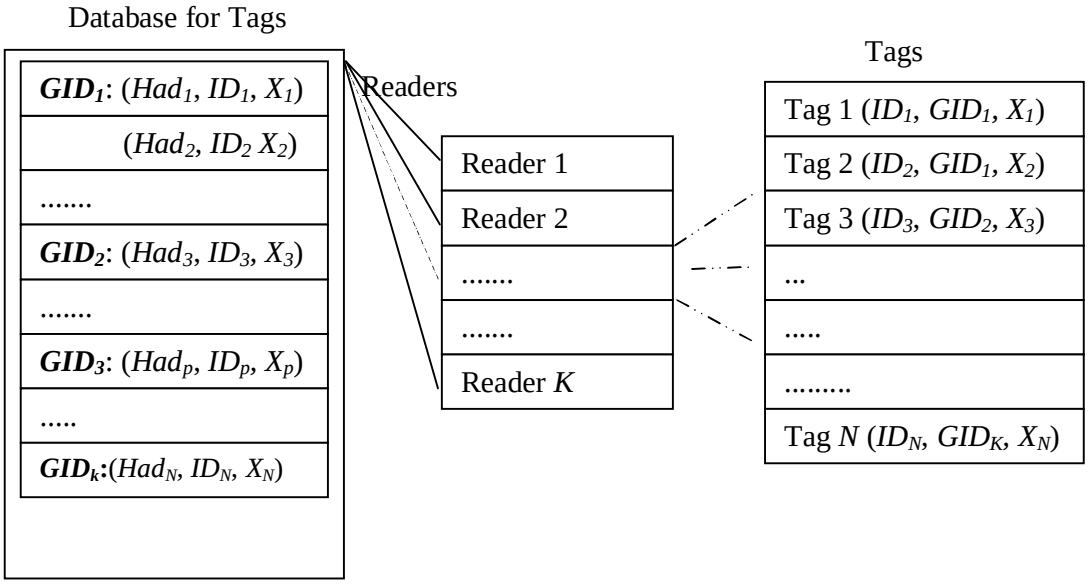

Figure 8-14: The Data Framework of the Baggage using SUAP2 Protocol

SUAP1, SUAP2 and SUAP3 protocols work in ubiquitous environment. However SUAP1 is suitable for small system (several thousands of tags) where the numbers of RFID tags are not too high and not distributed much. Hence SUAP1 is not suitable for baggage handling system. SUAP2 is suitable for this purpose. The protocol supports many groups that can be implemented for many countries or states. In this case *GID* will be used for country or state *ID*. The SUAP3 also support

many groups but for better security SUAP2 is preferred since it uses an extra secret value which will protect the baggage form all the identified threats effectively.

The GAPVI will not be suitable for the RFID system of baggage handling since this protocol is not designed for distributed system. It will not work properly in ubiquitous computing environment.

8.5 Conclusion

In this chapter privacy and security problems in the RFID systems are analyzed for e-passport and hospital. This chapter also analyzed the uses of RFID technology in baggage handling in airport and the possible privacy protection of the baggage in RFID technology.

In e-passport a protection scheme using an efficient and secure authentication protocol CPAP is proposed. CPAP is used to protect privacy for low-cost RFID system in pervasive computing environment. The proposed scheme requires only two one-way hash function operations that make it very efficient. The storage requirement for tag and the database is small. The comparison shows that the protocol described is both secure and efficient than other schemes. It also has practical advantages over them because it is simple and provides greater number of privacy and security protection. From simulation experiment it was found that for 12 and 16 bits data the RFID system is fully vulnerable to adversary attack. For 32 bits it also sometimes failed to give privacy protection. It was found to give good security and privacy for 64 bits. In our experiment data was always protected from privacy attack for 64 bits. So it is recommended for 64 or higher bits for proper security of the RFID systems. Most of the RFID standard support 96 bit EPC tag. Some standards support 128 bits for EPC memory. In that case our recommendation is for 96 or 128 bits of secret in RFID tag and reader.

The chapter also analyzed the privacy and security problems in RFID systems in a hospital environment. A proposed protection scheme NAPHS is proposed to protect privacy for low-cost RFID system in a hospital. The proposed scheme requires only one one-way hash function operation in database that makes it highly efficient. The storage requirement for the tag and database is also low in comparison to the other protocols. The comparison shows that the protocol is both secure and efficient than these protocols and it has many practical advantages like simplicity, privacy and security protection. Simulation experiment indicated that for 16 bits data the RFID

system is fully vulnerable to adversary attack. For 32 bits it also failed sometimes to ensure privacy protection. The results indicated appropriate security and privacy for 64 bits data and is suggested that 64 or higher bits is required for appropriate security of an RFID systems. Most RFID standards support 96 bit for EPC tag memory. Consequently it is recommendation that 96 or 128 bits data and secret would be fully secured in RFID tag and reader systems.

Finally RFID technology is considered in airports for baggage handling purposes. RFID can be used for sortation, identification, automation and location tracking. The read rate of RFID is much higher than the barcode read rate. RFID technology will reduce labour costs and strengthen automation. It can reduce the time for baggage sortation and distribution. The different activities required in the baggage handling process are very well suited for RFID technology. If RFID technology is implemented properly then passengers and airlines as well as airports will benefit. The passenger can get the information about their baggage's current location, expected arrival time etc. Moreover latest technologies like Internet web facilities, SMS, databases and interactive televisions can be used to identify and enhance the performance of the system to better handle the baggage in airport. Airlines can reduce their costs if they eliminate the charges for mishandling and mismanagement of baggage. It is possible to identify the employees responsible for handling baggage before it is lost or mishandled. Airports also enhance their efficiency and thus ensure better customer services. The trials in different airports also gave very positive results and opened up a window for the future. There are also some challenges in the implementation of RFID in airports. Many airports may not take this technology in the near future due to the initial investment and proper initiative needed. So, profit and benefits cannot be maximized until most of the airports use a common RFID-based network system. Most RFID technologies need to be integrated with existing systems like barcodes. Another challenge of RFID is the privacy and security of the tag, because the content of the tag is vulnerable to an adversary. To protect the baggage from tracking RFID authentication protocols are also proposed to implement in the RFID system.

Part of the substance of this chapter has been published or accepted in the following conferences.

1. Morshed, M.M., Atkins, A.S., Yu, H. 2011, E-passport: Privacy and Security Issues, International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2011), September 8-11, Benevento, Italy.

2. Morshed, M.M., Atkins A.S., Yu H, Ahmed, S.I., Akbar, M.M. 2010, 'A Novel Authentication Protocol using Varying Identifier for RFID System', IEEE 4th International Conference on Advanced Computing & Communication Technologies (ICACCT), India, pp.1-6.
3. Morshed M.M., Yu, H., Atkins, A.S., Ahmed, S.I., Akbar, M.M. 2010, 'A Two-Way RFID Authentication Protocol in Pervasive Computing' Proceedings of the 16th International Conference on Automation & Computing, University of Birmingham, Birmingham, UK, pp.164-169.
4. Morshed, M.M., Atkins, A.S., Yu, H., Ahmed, S.I., Akbar, M.M. 2010, "An Airport Baggage Handling System using RFID Technology-A Proposed Architecture", International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2010), Paro, Bhutan.

Chapter 9 Conclusion and Future Work

9.1 Introduction

In this chapter the overall conclusions are made from the work carried out in this thesis. It outlines the summaries of the findings. It also suggests directions of future work.

This thesis focuses on the privacy and security threats of RFID systems in many applications. The RFID tag contains unique identifier that can be easily tracked. The RFID systems exert its data to the air that are vulnerable to the adversary. The thesis also investigates various existing RFID privacy and security protocols and also identifies various problems in the existing RFID authentication protocols. This aim of the research work is to overcome the identified privacy and security problems and offers various RFID authentication protocols.

9.2 Revisiting the Objectives

The primary objective of the research was to develop authentication protocols to ensure privacy and security of the RFID systems that would be suitable for different applications for example, healthcare systems, e-passport, baggage handling in airports and supply chain operations. This research outlined the specific objectives in Section 1.2 and are re-examined as follows:

> *"To identify the challenges through literature review with the relevant fields of RFID systems, application, privacy and security problems and the basic cryptographic techniques that can be used in low-cost RFID systems."*

Chapter 2 gives a review of RFID systems and also discusses the components of RFID systems including the readers, tags and backend database. This chapter also discusses the classification of RFID tags. It outlined RFID standards and the details of different types of EPC classes. This chapter discusses some application and advantages of RFID systems compared to bar code etc. It identified many advantages of RFID tags over the optical barcode. Barcodes require line-of-sight contact with readers. In contrast, RFID tags are readable without line-of-sight contact and without precise

positioning. RFID readers can scan tags at rates of hundreds per second. A barcode indicates the type of object on which it is used. An RFID tag emits a unique serial number that distinguishes among many millions of identically manufactured objects. However in RFID systems there are issues regarding privacy and security. The information in these systems is vulnerable to various attacks. This chapter also presented these types of attacks and indicated the security requirements of RFID systems. This chapter further discusses general cryptographic techniques that are used in network communication and information systems security. Modern cryptographic techniques are divided into two main classes, symmetric and asymmetric techniques. Some cryptographic data integrity algorithms such as cryptographic hash functions, message authentication codes and digital signatures are also discussed for data security.

"To investigate the existing protocols for privacy and security of RFID system."

Chapter 3 has reviewed a number of existing security approach and authentication protocols for RFID systems. It classified the authentication protocols according to their implementation. Advantages and disadvantages of the protocols are also outlined for each protocol. The protocols are classified based on hash-based varying identifier, static identifier and light-weight encryption based protocols for RFID systems. The protocols with hash-based varying identifiers ensure privacy and security of the information by updating it after every authentication session so that the response is unpredictable. In this case the adversary cannot use any response in future to authenticate the system since the identifier and the secret value are no longer similar. However it requires synchronization in the tag side and the database side which involves computational and storage overhead. This approach is not suitable in the ubiquitous computing environment since the synchronization of the updated values is difficult to ensure in the distributed environment. The protocols with static identifiers are suitable for ubiquitous computing environment but it requires more storage. Finally the light-weight encryption protocols require less complex operations than hash-based protocols since hash functions are complex and computation intensive.

The privacy, security and efficiency problems in different existing protocols are also identified in this chapter. It is a challenge to ensure all the identified privacy and security threats effectively and efficiently. The concepts of the existing protocols are used as the foundation for the proposed protocols. The proposed protocols identified the various techniques in the existing protocols that can be combined and used to overcome the privacy and security problems in RFID systems.

"To develop new protocols for RFID privacy and security to improve efficiency and reliability."

"To develop simulation software and carry out experiment using the simulation software based on the developed protocols."

"To evaluate the performance of the developed protocols and algorithms against other privacy and security protocols in terms of potential benefits and effects to justify the adoption of proposed work. "

Chapter 4 proposed four hash-based ubiquitous authentication protocols for the privacy and security of the RFID systems. The protocols are SUAP1, SUAP2, SUAP3 and EMAP.

SUAP1, SUAP2 and SUAP3 uses group-based approach using hash function, random numbers to protect the privacy for the low-cost RFID system. The privacy and security problem of OHLCAP is overcome in these protocols. SUAP1 is suitable for the organization having small number of tags. SUAP2 and SUAP3 are for medium and large organizations having several departments. All the proposed schemes require only two one-way hash function operations that make them very efficient. The tag search time in the database is reduced by using the hash value as the address of the corresponding tag. The proposed protocol is compared with four other protocols LCAP, CRAP, OHLCAP and EOHLCAP. LCAP updates the identifier after each authentication process and hence it is not suitable for ubiquitous computing. The protocol also has location privacy problem until authentication process is successful. The CRAP and the OHLCAP work in ubiquitous computing environment however, CRAP requires a large number of hash computations and the OPHLCAP has privacy and security problems. The proposed protocol eliminates the privacy, security and efficiency problems in these protocols. The EOHLCAP also overcomes the problem in OHLCAP and protects the RFID system from most of the attacks however it requires many complex hash operations in the database side. In the proposed protocols the number of hash operations has been reduced on the database side and ensure both privacy and security protections from the identified threats. The storage requirements in SUAP1 and SUAP3 are also less than the other protocols. The privacy and security comparison shows that the proposed protocols are both secure and efficient than LCAP, CRAP, OHLCAP and EOHLCAP schemes since the protocols are protected from all the identified privacy and security threats like information leakage, location privacy, impersonation

and replay attack, message interception and tracing with lower storages, computations and communication costs.

The protocol EMAP in Chapter 4 is proposed using individual secret for each tag to protect privacy for low-cost RFID systems. It also uses static identifier so that it can work in a ubiquitous computing system. The proposed EMAP requires two one-way hash functions. The storage requirements for the tag and database are also low. Due to the two random numbers, one generated in the reader and the other generated in the tag, a tracing attack and impersonation attack become impossible. It has practical advantages over other protocols because it is simple and provides a larger range of privacy and security protections. The proposed protocol is robust to the identified threats, such as information leakage, an impersonation attack, replay attack, DoS attack and location tracing problem.

Chapter 5 presented a new efficient and secure authentication protocol ESAP to protect privacy for low-cost RFID systems. The protocol uses a static identifier to provide effective privacy and security in a ubiquitous environment using hash functions, a timestamp and a random number. The strength of this protocol is the use of a monotonically increasing timestamp and a random number effectively to make the response more unidentifiable. This protocol stores the current timestamp after each successful authentication. This protocol uses the search index *IDX* to search the tag records in the database. It reduces the tag search time substantially in the database. The simulation experiment also proved that, the responses during the experiment were unique for both the 64 and 96 bits long secret and data length. It is also secured from an adversary from all the identified attacks such as information leakage, location privacy, impersonation and replay attack, message interception and tracing. Specific privacy and security protections from an adversary appropriate to simulation experiment were tested and found to be satisfactory. The privacy and security protections were also analyzed and the analysis verified that this protocol is protected from the identified threats. The proposed scheme requires only two one-way hash functions making it highly efficient. The storage requirements for the tag and database are also cost efficient. The comparison outlined in the analysis and experiment result shows that the proposed protocol is secure and efficient in compared to the other protocols. It has practical advantages over these protocols because it is simple and provides a larger range of privacy and security protections. This protocol will be suitable in the RFID systems of healthcare industry, supply chain management etc.

Chapter 6 proposed a new efficient and secure authentication protocol GAPVI to protect privacy for low-cost RFID systems using a varying identifier to provide effective privacy and security with recovery of the identifier to maintain synchronization. It is secured from an adversary by maintaining location privacy. It also protects the systems from an adversary for both privacy and security attacks as it was tested in the simulation experiment and analysis. The proposed scheme requires two one-way hash functions making it highly efficient. The storage requirement for the tag and database is also cost efficient. The comparison outlined in the analysis of the protocol is both secure and efficient compared to the other protocols outlined. It has practical advantages over these protocols because it is simple and provides a larger range of privacy and security protections.

Chapter 7 proposed a new efficient and secure authentication protocol EHB-MP using light-weight encryption technique to protect privacy for low-cost RFID system in pervasive computing environment. The proposed protocol derived from HB+ and HB-MP protocols by removing the existing privacy and security problems. The proposed scheme requires only lightweight cryptography which is more suitable than hash function for low-cost RFID tag. The storage requirements for tag and the reader are also very low. The comparison shows that the protocol described here is both secure and efficient than HB+ and HB-MP protocols. A mathematical proof is given to show that the proposed EHB-MP protocol is fully protected from the man-in-the-middle attack.

> *"To propose architectures for the implementation of the developed protocols in real life applications like healthcare systems and e-passport."*

The Chapter 8 investigated the privacy and security problems in e-passport and also outlined the present privacy and security measure for the RFID data in it. A protection scheme using a secure authentication protocol CPAP is proposed to ensure the privacy and security of the RFID data more efficiently. CPAP is used to protect privacy for low-cost RFID system in pervasive computing environment. The proposed scheme requires only two one-way hash function operations that make it highly efficient. The storage requirement for tag and the database is relatively small. The proposed protocol is compared with three other protocols LCAP, CRAP and OHLCAP. The privacy, security and efficiency comparison shows that the protocol described is both secure and efficient than these schemes. The protocol is also secured form the identified privacy and security threats. It also has practical advantages over them because it is simple and it provides greater

number of privacy and security protection with low storage, computation and communications costs.

The Chapter also analyzed the privacy and security problems in RFID systems in a hospital environment. A proposed protection scheme NAPHS is proposed to protect privacy for low-cost RFID system in a hospital. The proposed scheme requires only one one-way hash function operation that makes it highly efficient. The storage requirement for the tag and database is also low in comparison to the other protocols. The comparison shows that the protocol is both secure and efficient than these protocols and it has many practical advantages like simplicity, privacy and security protection.

This Chapter further investigates the scope of RFID technology in airports for baggage handling purposes. RFID can be used for sortation, identification, automation and location tracking. RFID technology will reduce labour costs and strengthen automation. It can reduce the time for baggage sortation and distribution. The different activities required in the baggage handling process are very well suited for RFID technology. If RFID technology is implemented properly then passengers and airlines as well as airports will benefit. The passenger can get the information about their baggage's current location, expected arrival time etc. Latest technologies like Internet web facilities, SMS, databases and interactive televisions can be used to identify and enhance the performance of the system to better handle the baggage in airport. Airlines can reduce their costs if they eliminate the charges for mishandling and mismanagement of baggage. It is possible to identify the employees responsible for handling baggage before it is lost or mishandled. Airports also enhance their efficiency and thus ensure better customer services. The trials in different airports also gave very positive results and opened up a window for the future. There are also some challenges in the implementation of RFID in airports. Many airports may not invest to this technology in the near future due to the initial investment and proper initiative needed. Therefore, profit and benefits cannot be maximized until most of the airports use a common RFID-based network system. Most RFID technologies system need to be integrated with existing systems like barcodes because in some cases an organisation may not have invested in RFID systems . Another challenge of RFID is the privacy and security of the tag, because the content of the tag is vulnerable to an adversary. To protect the baggage from tracking RFID authentication protocols are also proposed to implement in the RFID system.

9.3 Summary of Contributions of this Research

The contributions of this research are categorized as two ways. Firstly is the major contribution in the development of seven new protocols. This includes improvements in the privacy and security of the RFID systems with lower storage, computation and communication costs. Secondly the other contribution includes the common requirements for any privacy and security protection research work. These are the privacy and security identification in RFID applications, reviews of the existing research work to protect the RFID systems from various threats, the challenge and problems in the existing authentication protocols, and the performance comparisons with the proposed protocols and other well known protocols. The contributions of this research are given as follows:

9.3.1 Major Contributions

The major Contributions of this research are as follows:

- The thesis proposes 7 new RFID authentication protocols for RFID systems. The protocols are SUAP1, SUAP2, SUAP3, EMAP, ESAP, GAPVI, EHB-MP respectively. It identifies that different protocols are suitable for different situations. Different protocols also have different advantages and disadvantages. All the proposed protocols protect the RFID systems from all the identified privacy and security threats: information leakage, location privacy, impersonation attack, man-in-the-middle attack, replay attack, DoS attack, forward privacy and backward privacy.
- Features of SUAP1, SUAP2 and SUAP3
  - Group based protocols
  - SUAP1, SUAP2, SUAP3 use hash function and hash address to ensure the privacy and security in ubiquitous computing environment. Two random numbers in hash function ensures the better privacy and security of the transmitted message.
  - No message or hash address transmitted in plaintext.
  - Hash address reduces the searching time of the RFID tag in the database.
  - SUAP1 is suitable for small system and SUAP2 and SUAP3 are suitable for true ubiquitous large RFID systems. These are actually suitable for a system where the tags may be divided into different groups.

- All these protocols protect the identified privacy and security of the RFID systems with storage and computation cost suitable for low-cost tags.

- Features of EMAP
  - EMAP uses individual tag secret instead of group secret to ensure privacy and security efficiently.
  - No message transmitted in plaintext.
  - Suitable for ubiquitous computing environment where the number of tags are not too high.
  - The protocol protect the identified privacy and security of the RFID systems with storage and computation cost suitable for low-cost tags.

- Features of ESAP
  - ESAP is also efficient authentication protocols that efficiently protect the privacy and security of the RFID systems.
  - It uses a monotonically increasing timestamp and a random number to ensure the privacy and security efficiently.
  - No message transmitted in plaintext.
  - ESAP is suitable for ubiquitous computing environment where the number of tags are not too high.
  - The protocol protect the identified privacy and security of the RFID systems with storage and computation cost suitable for low-cost tags.

- Features of GAPVI
  - GAPVI is an efficient authentication protocol using varying identifier and hash address.
  - Reduces hash computations
  - Not suitable for ubiquitous computing environment.
  - No message transmitted in plaintext.
  - The protocol protects the identified privacy and security of the RFID systems with storage and computation cost suitable for low-cost tags.

    .

- Features of EHB-MP
  - EHB-MP uses xor-based light-weight encryption method to ensure privacy and security.
  - It removes the privacy problem of previous xor-based light-weight authentication protocols. It shows that it is protected from the man-in-the-middle attack which is a big challenge in the RFID authentication protocol in light-weight encryption technology.
  - Requires low storages
  - Suitable for ubiquitous computing environment.
  - No message transmitted in plaintext.
  - The protocol protects the identified privacy and security of the RFID systems with less storage and computation cost.

This research conducted some simulation experiments for the proposed and some existing well known RFID authentication protocols. The experiments mainly test if the response can be reused to break the privacy and security of the RFID systems. For this purpose it checks if any response for a tag is recurred in a specified number of attempts. If the same response is generated it can be used to break the privacy and security of the RFID systems. The key achievement of this research is that the proposed RFID authentication protocols protect the system from all the identified privacy and security threats. This research also has investigated the implementation of the proposed RFID authentication protocols in some applications. It proposed proper privacy and security of RFID systems for e-passport, healthcare system and baggage handling system in airport. It is observed that each RFID application has its own specific requirements. For example e-passport and baggage handling in airport require distributed system where the RFID protocol should support ubiquitous computing environment. However in some cases such as a hospital may use an RFID system which may be implemented in a computing environment that is not much distributed compared to passport systems where the individual my travel globally to many countries.

9.3.2 Other Contributions

The other achievements of this research are summarized as follows:

- It identifies the privacy and security requirements in RFID systems. It identifies privacy and security requirements for both the tag and database. The tag privacy covers both the

information and location privacy. Two types of security attacks are covered- the weak attacks and strong attacks. Tag impersonation, cloning, replay attack, man-in-the-middle attack and DoS attack are identified as weak attacks. On the other hand backward traceability, forward traceability and server impersonation attack are identified as strong attack.

- It also identifies the performance requirements for RFID protocols. The performance requirements are identified as storage costs, computation costs, communication costs and scalability.
- This research reviewed varieties of existing RFID authentication protocols. It includes a number of hash-based and xor-based lightweight authentication protocols. It also identifies the privacy and security problems in the existing RFID authentication protocols.
- It also compared the privacy and security properties with related existing RFID protocols.

9.4 Limitations and Future Work

One limitation of this thesis is that it only considers hash based encryption and lightweight encryption to ensure the privacy and security of the RFID systems. It did not consider other encryptions like AES and DES which is beyond the scope of this thesis. Another limitation of this thesis is that it did not perform any experiment for lightweight protocols EHB-MP to test how many times a reader wrongly authenticate a tag or how many times it does not authenticate a valid tag because of time constraints.

The privacy and security concern in RFID systems is new and emerging as an important issue in wireless technology.

This research identifies various existing privacy and security problems with RFID systems which still in its ‘infancy stage’. In future more privacy and security threats may be identified in different sections of the RFID systems and consequently privacy and security threats will inevitably be an important research issue.

This research basically proposes two ways to design the protocols for RFID privacy and security: 1. hash function based authentication protocols and 2. xor based light-weight authentication protocols. In future other cryptographic methods can be investigated to develop lightweight authentication

protocols. Also the tag capacity will also be increased in future. More computation and storage intensive protocols also may be considered for future work.

This thesis uses the symmetric cryptography to develop the privacy and security protocols. In future asymmetric cryptography may be considered to develop new RFID privacy and security protocols. The asymmetric cryptography requires more storages and it is more complex computational intensive. At present the low-cost tag is not suitable to use asymmetric cryptography due to its storages and processing limitations.

The proposed protocols can be implemented in the real scenario of e-passport, healthcare systems and in baggage handling system in airport in future. The real performance of the systems can be verified with the research results.

An important research problem is that though it is possible to design a ubiquitous design for the privacy and security of the RFID systems but it is really difficult to manage it in a true distributed computing environment. The first problem is that it requires a large common database to store the information of the tags. In this case some RFID readers may need to communicate a long distance for the data stored in the database. Another alternative is to replicate all the RFID tag information in many databases in many places. This requires large storages space for a billion numbers of tags. To reduce the replication the scope of the RFID tags can be defined for some specific places and databases. The information of the relevant RFID tags will only be stored in the associated databases. That means a group of databases and systems can only handle the RFID tags at any instance. One of the database servers will act as an owner of the tags in this group. This server will be called Administrative Centre (AC). The ownership means only the one trusted database server AC will have the authority to manage and control all the information of the RFID tags under this system [Song 2008]. It also manages the privacy and security policies for the associated tags. It can delegate access to the tags to the other database systems and readers. Other database systems and readers can only authenticate the tags using secret and tag information but cannot control or even update the secret values of the tags. The AC can directly communicate with the readers or it can communicate with the other databases. Figure 9-1 shows a basic architecture of an ownership model for an Administrative Centre (AC) with other databases and readers.

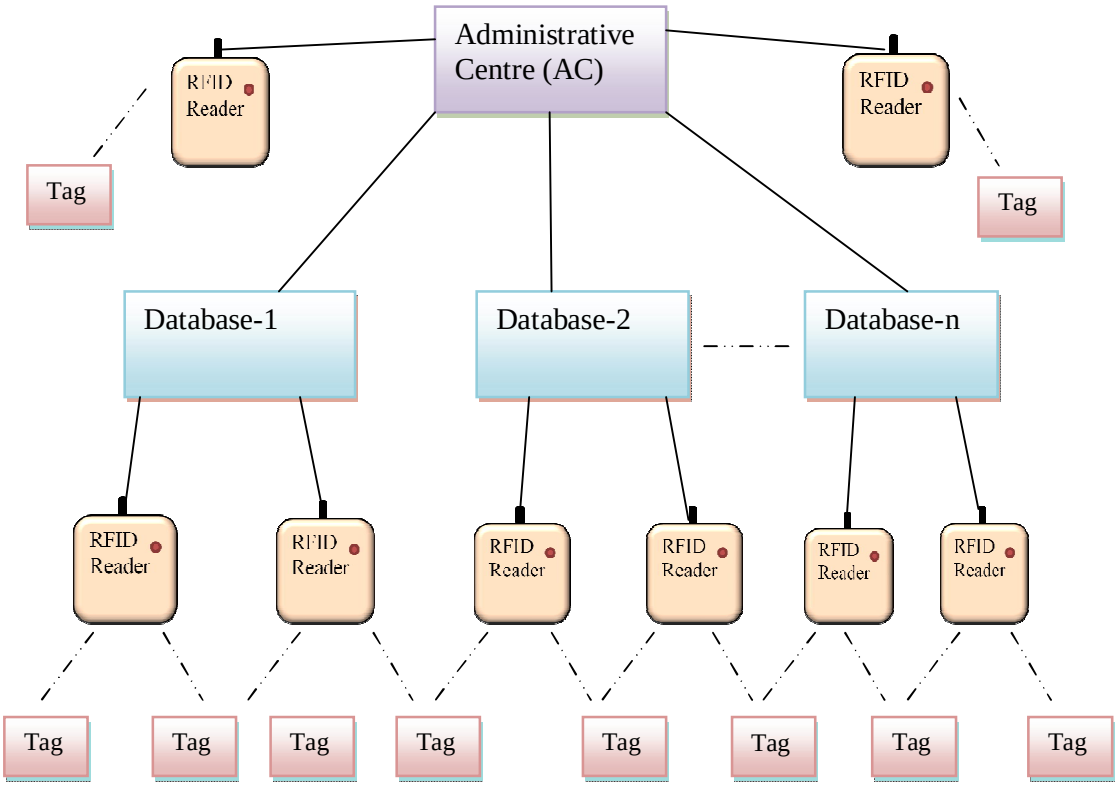

Figure 9-1: Ownership Architecture of an Administrative Centre

There may be several Administrative Centres say AC_1, AC_2 ... AC_n etc. If these tags require travelling further from this system of one Administrative Centre to the range of the other Administrative Centre then the ownership of these tags can be transferred to that centre with the permission of the present owner Administrative Centre. For example if it moves from AC_1 to AC_2 then the ownership will be transferred to AC_2. In that case only the AC_2 can control the tag and the AC_1 can no more manage or control the tag. In ideal case it cannot even authenticate the tag anymore. To be able to authenticate the tag the AC_2 may delegate access permission to AC_1. The advantage of this design is that it does not require storing the information of all the tags in many databases. It will reduce the storage requirements for redundant information. It will also reduce the administrative overhead to manage the large number of tags. The ownership transfer scenario is shown in Figure 9-2.

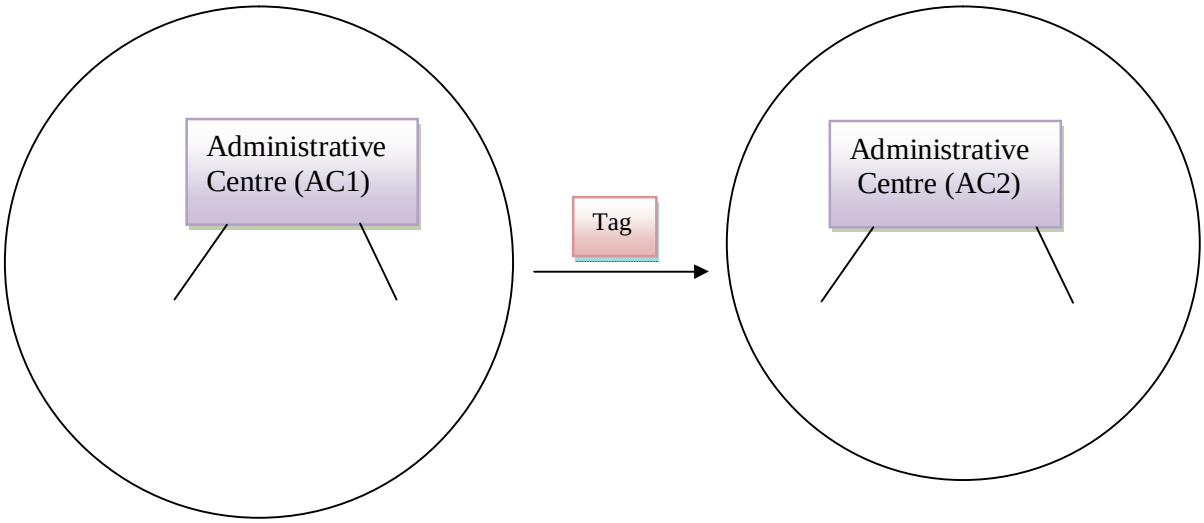

Figure 9-2: Ownership Transfer of the Tag

Few researchers worked in the field of ownership transfer but it is still in initial stage. There is a complex relationship of different counterparts along the supply chains: tag holders, subcontractors, service providers, etc. with different requirements and interests. Therefore the ownership delegation may be an important research area near future [Molnar et al 2005, Song 2008, Henrici and Muller 2008]. Neural network may be a promising model to enhance the performance for the ownership transfer architecture. This is an interconnected group of natural or artificial neurons that uses a computational model for information processing based on a connectionistic approach to computation. Neural network can be a useful model to search and classify the large number of tags that are distributed worldwide.

Another very important research area for privacy and security of the RFID systems is the Internet of Things (IoT). The Internet of Things refers to uniquely identifiable objects and their virtual representations in an Internet-like structure. The very primary definition of IoT comes from the things oriented perception such as sensors with unique IDs or RFID tags and the term "Internet of Things" attributed to renowned networks of academic research laboratories [Auto-Id Labs]. Their key focus has been to support the proliferation of RFID tags using the standard EPC. For the full deployment of IoT it requires the central focus on the things' intelligence. Smart things or objects are able to interact and communicate among them and with the environment by exchanging data and information and can react autonomously with physical world, trigger action, create service

without human interaction and has context awareness capability [Atzori et al. 2010]. In the IoT platform numerous services should be available to interact with smart things through standard interfaces that will provide link via internet, to retrieve inform changes of state. IoT should be built in such a way that it should easy to use and secure for the user. In the IoT smart things could be connected to the Internet superhighway to communicate with other objects which may create the privacy and security problems for the users. The IoT is vulnerable because of various reasons such as [Atzori et al. 2010]:

- Due to the pervasiveness of the IoT applications the privacy and security threats are also pervasive.
- In most of the cases the components of the IoT are kept unattended which are easy to attack by the attacker.
- The components of IoT mostly use wireless technology such as RFID tags, sensors which make information leakage and spoofing very easy.
- Most of the RFID components like passive RFID tags and sensors have low storage, computation and communication capabilities and do not support traditional complex privacy and security schemes.

It is a major challenge to ensure privacy and security in IoT applications as the authentication and data integrity are difficult to achieve. This requires appropriate authentication infrastructures and servers that might require authentication from the remote place. These approaches are not feasible for IoT application as the passive RFID tags cannot transmit too many messages with the servers.

References

Ahamed, S.I., Rahman, F., Hoque, E., Kawsar, F., and Nakajima, T. 2008, *S3PR: Secure serverless search protocols for RFID.* In Proceedings of the International Conference on Information Security and Assurance (ISA 08), IEEE, IEEE Computer Society Press. New York, USA. pp. 187-192.

AeroAssist 2008. RFID in Aviation: airport luggage control. Available: www.AeroAssist.pt. [Accessed 8th April 2011]

Aissi, S., Dabbous, N. and Prasad, A.R. 2006, Security for Mobile Networks and Platforms. Universal Personal Communications. Artech House, Norwood, MA, USA.

Atzori L., Iera Antonio and Morabito Giacomo 2010, The Internet of Things: A Survey, Computer Networks 54, Elsevier, pp. 2787-2805.

Atkins, A.S., Zhang, L., Yu, H., and Miao, W. 2009, 'Application of Intelligent Systems Using Knowledge Hub and RFID Technology in Healthcare Waste Management in UK and China', International Conference in e-Business, pp. 44-49 July, Milan, Italy ISBN 978-989-674-006-1.

Atkins, A.S., Zhang, L. and Yu, H. 2010, 'Application of RFID and Mobile technology in Tracking of Equipment for Maintenance in the Mining Industry' 2010 Underground Coal Operators' Conference, The Australasian Institute of Mining and Metallurgy, pp. 350-358 ISBN 978-1-921522-16-1.

Auto-Id Labs, Available: <http://www.autoidlabs.org/> [Accessed 4th March 2010]

Avoine, G 2005, Cryptography in Radio Frequency Identi_cation and Fair Exchange Protocols. PhD thesis, Ecole Polytechnique Federale de Lausanne (EPFL), Lausanne, Switzerland.

Avoine, G. and Oechslin, P. 2005, *RFID Traceability: A Multilayer Problem*, Financial Cryptography.

Avoine, G. , Dysli, E. and Oechslin, P 2005. Reducing time complexity in RFID systems. In B. Preneel and S. Tavares, editors, Selected Areas in Cryptography -- SAC 2005, volume 3897 of Lecture Notes in Computer Science, Kingston, Canada. Springer-Verlag, pp. 291-306.

Banks, J., Hanny D., Pachano M.A. and Thompson L.G. 2007, RFID Applied, John Wily & Sons, Inc., Hoboken, New Jersey, ISBN-10: 0471793655.

Bar-El, H 2002, Introduction to side channel attacks. White paper, Discretix Technologies Ltd. Avalilable: http://www.hbarel.com/publications/ Introduction_To_Side_Channel_Attacks.pdf. [Accessed 15th October 2010]

Bing, B. 2002, *Broadband Wireless Access*. Kluwer Academic Publishers, ISBN: 0-7923-7955-1.

Bringer, J., Chabanne, H. and Dottax, E. 2006, HB++: a lightweight authentication protocol secure against some attacks, in: IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in pervasive and Ubiquitous Computing – SecPerU.

Cai. S., Li, Y., Li, T. and Deng, R.H. 2009, Attacks and Improvements to an RFID Mutual Authentication Protocol and its Extensions, *WiSec'09,* Zurich, Switzerland, March 16–18.

Cerino, A. and Walsh, W.P. 2000, Research and Application of Radio Frequency Identification (RFID) Technology to Enhance Aviation Security, presented at the IEEE 2000 National Aerospace and Electronics Conference, Dayton, OH, October 10-12, pp. 127-135.

Chien, H. and Chen, C. 2007, Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards. Computer Standards & Interfaces, 29(2): pp. 254–259.

Choi E.Y., Lee S.M. and Lee D.H. 2005, "Efficient RFID Authentication Protocol for Ubiquitous Computing Environment," Embedded and Ubiquitous Computing, vol.3832, pp..945-954.

Collins, J. 2004, Marks and Spencer expands RFID retail trial. *RFID Journal*, 10 February 2004. Available: http://www.rfidjournal.com/article/articleview/791/1/1/. [Accessed 8th March 2010]

Coron, J., Naccache, D. and Stern, J. 1999, On the security of RSA padding. In *CRYPTO 99*.

Cresswell, J.W. 2003, Research Design: Qualitative, Quantitative and mixed Methods Approaches, (2nd Ed.). Thousand Oakes, CA: Sage Publications.

Das, R. 2007. The Myth and Reality of Baggage Tagging. [Online]. Available: http://www.idtechex.com/products/en/articles/00000534.asp. [Accessed 6th February 2010]

Dimitriou, T. 2005, A lightweight RFID protocol to protect against traceability and cloning attacks. In Conference on Security and Privacy for Emerging Areas in Communication Networks — SecureComm, Athens, Greece, September. IEEE, pp. 59–66.

Duc, D.N., Park, J., Lee, H. and Kim, K. 2006, Enhancing security of EPCglobal gen-2 RFID tag against traceability and cloning. In Symposium on Cryptography and Information Security — SCIS 2006, Hiroshima, Japan, January. The Institute of Electronics, Information and Communication Engineers.

EPCglobal Web site, 2005. Available: http://www.EPCglobalinc.org. [Accessed 10th September 2010]

Ericson, J. 2004, RFID for Hospital Care, in Line 56, the E-Business Executive Daily. July 23.

Fishkin, K.P., Wang, M, and Borriello, G 2003. A ubiquitous system for medication monitoring. In *Pervasive 2004*, 2004. Available as 'A Flexible, Low-Overhead Ubiquitous System for Medication Monitoring,Intel Research Seattle Technical Memo IRS-TR-03-011, 25 October.

Fishkin, K.and Lundell, J. 2005. RFID in healthcare. In S. Garfinkel and B. Rosenberg, editors, *RFID: Applications, Security, and Privacy*, Addison-Wesley, pp. 211–228..

Garfinkel, S., Jules, A. and Pappu, R. 2005, RFID privacy: an overview of problems and proposed solutions. IEEE Security and Privacy. 3(3): 34-43, May/June.

Garg, V.K. 2000, IS-95 CDMA and cdma2000, Prentice Hall.

Gilbert, H., Robshaw, M. and Sibert, H. 2005, An active attack against HB+ – a provably secure lightweight authentication protocol. Manuscript, July.

Gilbert, H., Robshaw, M., and Seurin, Y. 2008, "HB#: Increasing the security and efficiency of HB ," in *Proc. EUROCRYPT (Lecture Notes in Computer Science)*, N. P. Smart, Ed. Berlin, Germany: Springer-Verlag, vol. 4965, pp. 361-378.

Giusto, D., Iera, A. Morabito, G. and Atzori, L. 2010, The Internet of Things, Springer, ISBN: 978-1-4419-1673-0.

Glover, B. & Bhatt, H. 2006, RFID Essentials. O'Reilly, Gravenstein Highway North, Sebastopol, CA, USA, pp. 54-169.

Goldreich, O. and Levin, L.A. 1989, Hard-core Predicates for Any One-Way Function, 21st ACM Symposium on Theory of Computation, pp. 25-32.

Günther, O. and Spiekermann, S. 2005, 'RFID and the perception of control: The consumer's view', Communications of the ACM, Vol. 48, No. 9, pp.73-76.

Ha, J., Moon, S., Nieto, J.M.G. and Boyd, C. 2007, "Security Analysis and Enhancement of One-Way Hash Based Low- Cost Authentication Protocol", Emerging Technologies in Knowledge Discovery and Data Mining, vol.4819, pp. 574-583.

Harrop, P. 2006, RFID in the Air Industry and Land Transport. August. Available: http://www.idtechex.com/products/en/articles/00000486.asp. [Accessed 12th September 2010]

Henrici, D. and Muller, P. 2004, Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In R. Sandhu and R. Thomas, editors, International Workshop on Pervasive Computing and Communication Security — PerSec 2004, pages 149–153, Orlando, Florida, USA, March. IEEE Computer Society.

Henrici, D. and Muller, P. 2008, Providing Security and Privacy in RFID Systems Using Triggered Hash Chains, Sixth Annual IEEE International Conference on Pervasive Computing and Communications, IEEE Computer Society, pp. 50–59.

Hitachi unveils smallest RFID chip 2003, *RFID Journal*, 14 March 2003. Available: http://www.rfidjournal.com/article/articleview/337/1/1/. [Accessed 15th October 2010]

Hong Airport Press release 2008, HKIA Boosts Baggage Handling Efficiency with RFID Technology, Available: http://www.hongkongairport.com/eng/media/press-releases/pr_914.html. [Accessed 2nd May 2010]

Hopper, N.J. and Blum, M. 2001, Secure human identification protocols, Advances in Cryptology – ASYACRYPT'2001, Lecture Notes in Computer Science, vol. 2248, Springer, pp. 52–66.

Hoque, M.E., Rahman, F. and Ahamed, S.I. 2009, "Supporting Recovery, Privacy and Security in RFID Systems Using A Robust Authentication Protocol," Proceedings of the 2009 ACM symposium on Applied Computing, *SAC'09*, Honlulu, Hawaii,USA. pp.1062-1066.

IATA 2007, "RFID Business case for baggage tagging", IATA Simplifying the Business.

ICAO 2004a, Document 9303, machine readable travel documents, October.

ICAO 2004b, PKI for machine readable travel documents offering ICC read-only access, version 1.1, October 2004.

International Civil Aviation Organization (ICAO) 2005. Document 9303, machine readable travel documents (MRTD), part I: Machine readable passports.

ISO 1999. ISO/IEC 9797-1 algorithm 3. Available: http://webstore.iec.ch/preview/info_isoiec9797-1%7Bed2.0%7Den.pdf. Accessed 12th October 2010]

Jacobs, B 2005. Biometry in passports. Available: http://www.sos.cs.ru.nl/research/society/passport/index.html. [Accessed 7th January 2011]

Juels, A., Rivest, R.L. and Szudlo, M. 2003, *The Blocker Tag: Selective Blocking of RFID tags for Consumer Privacy*. In the 8th ACM Conference on Computer and Communications Security, pp. 103-111. ACM Press.

Juels, A. 2004, Minimalist Cryptography for Low-Cost RFID Tags. In C. Blundo and S. Cimato, editors, International Conference on Security in Communication Networks --SCN 2004, volume 3352 of Lecture Notes in Computer Science, Amalfi, Italia, September. Springer-Verlag, pp. 149-164.

Jules, A. 2005 RFID Privacy: A Technical Primer for the Non-Technical Reader Draft: 23 February.

Juels, A., Molnar, D. and Wagner, D. 2005. Security and privacy issues in e-passports. In D. Gollman, G. Li, and G. Tsudik, editors, *IEEE/CreateNet SecureComm*. IEEE. Available: http://www.cs.berkeley.edu/ dmolnar/papers/papers.html. [Accessed 4th April 208]

Juels, A. and Weis, S. 2005, *Authenticating Pervasive Devices with Human Protocols*, Proceedings of CRYPTO'05, Victor Shoup (Ed.), Springer-Verlag, LNCS 3261, pp. 293–308.

Jules, A. 2006, RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communication, 24(2), February.

Karthikeyan, S. and Nesterenko, N. 2005. RFID security without extensive cryptography. In Workshop on Security of Ad Hoc and Sensor Networks — SASN '05, , Alexandria, Virginia, USA, November, ACM Press, pp. 63–67.

Katz, J. and Shin, J.S. 2005, Parallel and concurrent security of the HB and HB+ protocols, Cryptology ePrint archive, Report 2005/461. Available: http://eprint.iacr.org. [Accessed 9th January 2011]

Kumar, R. 2005, Research methodology; a step-by-step guide for beginners, 2nd ed, London: SAGE.

Laurie, A. 2007. Practical attacks against RFID. Network Security, 2007(9):4-7, September.

Lee, S.M., Hwang, Y.J., Lee, D.H. and Lim, J.I. 2005. *Efficient Authentication for Low-Cost RFID systems.* ICCSA05, vol. 3480 LNCS, Springer-Verlag, pp.619-629.

Lee, B. and Kim, H. 2007, Ubiquitous RFID based Medical Application and the Security Architecture in Smart Hospitals, International Conference on Convergence Information Technology IEEE Computer Society, pp. 2359-2362

Leng, X., Mayes, K.and Markantonakis, K. 2008, HB-MP+ Protocol: An Improvement on the HB-MP Protocol, IEEE International Conference on RFID, April.

Lim, C. and Kwon, T. 2006, Strong and robust RFID authentication enabling perfect ownership transfer. In P. Ning, S. Qing, and N. Li, editors, Conference on Information and Communications Security — ICICS '06, volume 4307 of Lecture Notes in Computer Science, Raleigh, North Carolina, USA, December, Springer-Verlag, pp. 1–20.

Menezes, A.J., Oorshot, P.C. and Vanstone, S.A. 1996, *Handbook of Applied Cryptography*, chapter 1.9. CRC Press.

Metcalfe, R.M. and Boggs, D.R. 1976, Ethernet: Distributed Packet Switching for Local Computer Networks. *Communications of the ACM*, 19(5):395–404, July.

Mitchell, C.J. 2003, Cryptography for mobile security. In C. J. Mitchell, editor, Security for Mobility, IET Telecommunications, chapter 1. The Institution of Engineering and Technology, December, pp. 3-10.

Molnar, D. and Wagner, D. 2004. Privacy and security in library RFID: Issues, practices, and architectures. In B. Pfitzmann and P. Liu, editors, Conference on Computer and Communications Security — ACM CCS , Washington, DC, USA, October, ACM Press, pp. 210–219

Molnar, D., Soppera, A. and Wagner, D. 2005. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In B. Preneel and S. Tavares, editors, Selected Areas in Cryptography -- SAC 2005, volume 3897 of Lecture Notes in Computer Science, Kingston, Canada, August, Springer-Verlag, pp. 276-290,.

Moore, N. 2006, How to do research: a practical guide to designing and managing research projects, 3rd Ed, London: Facet.

Morshed, M.M., Yu, H., Atkins, A., Ahamed, S.I. and Akbar, M.M. 2010, A Two-Way RFID Authentication Protocol in Pervasive Computing , The proceedings of 16th International Conference on Automation and Computing (ICAC'10), Birmingham University, UK, pp. 164-169.

Motorola 2007, INDUSTRY BRIEF: Baggage Tracking RFID Solutions. Available: motorola.com. [Accessed 13th February 2010]

Munilla, J. and Peinado, A. 2007, HB-MP: A further step in the HB-family of lightweight authentication protocols, Computer Netwroks 51 (2007), pp.2262-2267.

Ohkubo, M., Suzki, K., and Kinoshita, S. 2003, Cryptographic approach to "privacy-friendly" tags. In RFID Privacy Workshop, MIT, MA, USA, November. http://www.rfidprivacy.us/2003/agenda.php.

Ouafi, K. and Phan, and R.C.W. 2008, Traceable Privacy of Recent Provably-Secure RFID Protocols. In S.M. Bellovin, R. Gennaro, A. Keromytis, and M. Yung, editors, 6th International Conference on Applied Cryptography and Network Security | ACNS 2008, volume 5037 of Lecture Notes in Computer Science, New York City, New York, USA, June. Springer-Verlag, pp. 479-489,

Pattinson, N. 2004. Securing and enhancing the privacy of the e-passport with contactless electronic chips. Contact: pattinson@axalto.com.

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

Piramuthu,S. 2006, HB and related lightweight authentication protocols for secure RFID tag/reader authentication, in: CollECTeR Europe Conference, Basel, Switzerland, 9–10 June.

Prabhu, B.S., Su, X., Ramamurthy, H., Chu, C. and Gadh, R. 2005, WinRFID – A Middleware for the enablement of Radio Frequency Identification (RFID) based Applications *UCLA - Wireless Internet for the Mobile Enterprise Consortium (WINMEC)420 Westwood Pl., Los Angeles CA 90095*.

Reuters 2007, Edition: UK. Available: http://uk.reuters.com/article/idUKN0741544820070207 [Accessed 11th May 2010]

Rhee K., Kwak, J., Kim, S. and Won D. 2005. *Challenge-Response Based RFID Authentication Protocol for Distributed Database Environmnet.*, SPC 2005, LNCS 3450, pp. 70-84.

Roberti, M. 2004. RFID Upgrade Gets Goods to Iraq. *RFID Journal*, 23 July. Available: http://www.rfidjournal.com/article/articleview/1061/1/1/. [Accessed 22th April 2010]

Saad, M.K. and Ahmed, S.V. 2007, Vulnerabilities of RFID Systems in Infant Abduction Protection and Patient Wander Prevention. **i**nroads – The SIGCSE Bulletin, Volume 39, Number 2, June, pp.160-185.

Sarma, S.E., Weis, S.A., and Engels, D.W. 2002a, Radio-frequency identification systems. In Burton S. Kaliski Jr., C¸etin Kaya Ko¸c, and Christof Paar, editors, *CHES '02*, Springer-Verlag, LNCS no. 2523, pages 454–469.

Sarma, S.E., Weis, S.A., and Engels, D.W. 2002b, RFID systems, security and privacy implications. Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT.

Sarma, S., Weis, S., and Engels, D. Radio-frequency identification: Security risks and challenges. *CryptoBytes*, 6(1).

Saunders,M., Lewis, P.,and Thornill, A. 2007, Research Methods for Business Students, fifth edition, London, Financial Times-Prentice Hall.

Schouten, B., and Jacobs, B. 2009, "Biometrics and Their Use in e- Passports", Image and Vision Computing, pp. 205-312.

Shim, R. 2003, Benetton to track clothing with ID chips. *CNET*, 11 March 2003. Available: http://news.com.com/2100-1019-992131.html. [Accessed 21th November 2010]

Singel, R. 2005. No encryption for e-passports. *Wired News*, 24 February. Avalibale: http://www.wired.com/news/privacy/0,1848,66686,00.html?tw=wn_tophead_1. [Accessed 2nd February 2011]

Song, B. and Mitchell, CJ. 2008, RFID authentication protocol for low-cost tags. In *WISEC*, pp. 140-147.

Song, B. 2008. RFID Tag Ownership Transfer. In *4thWorkshop on RFID Security (RFIDsec 08)*, Budaperst, Hungary, July.

Stallings, W. 2011, Cryptography and Network Security: Principles and Practice, Fifth Edition, Pearson Education, Inc., Prentice Hall, New York.

Stapleton-Gray, R. 2003. Would Macy's scan Gimbels? competitive intelligence and RFID. Available: www.stapleton-gray.com. [Accessed 6th June 2010]

Stinson, D. 2002, Cryptography: Theory and Practice. CRC Press, Boca Raton, Florida, second edition.

Tan, C.C., Sheng, B., and Li, Q. 2008, Secure Serverless Search and Authentication Protocols for RFID, *IEEE Transactions on Wireless Communications*, Vol. 7, NO. 4, pp.1400-1407.

Thornton, F., Haines, B., Das, A.M., Bhargava, H., Campbell, A. and Kleinschmidt, J. 2006. RFID Security. Syngress, Massachusetts, USA.

Trochim, W. 2001, Research Methods Knowledge Base, Atomic Dog 2nd edition. ISBN-10: 1592602916

Tsudik, G. 2006, YA-TRAP: Yet another trivial RFID authentication protocol. In Fourth IEEE Annual Conference on Pervasive Computing and Communications -- PerCom, Pisa, Italy, March. IEEE Computer Society, pp. 640-643,.

Tsudik, G. 2007, A family of dunces: Trivial RFID identification and authentication protocols. In N. Borisov and P. Golle, editors, Privacy Enhancing Technologies, 7th International Symposium -- PET 2007, volume 4776 of Lecture Notes in Computer Science, Ottawa, Canada, June. Springer-Verlag, Berlin, pp. 45-61.

U. S. Department 2004, Abstract of the concept of operations for integration of contactless chip in the US passport. Available: http://www.statewatch.org/news/2004/jul/us-biometric-passport-original.pdf. [Accessed 27th October 2010]

Wang, S., Chenb, W., Onga, C. , Liuc, L., and Chuangb, Y. 2006, "RFID Application in Hospitals: A Case Study on a Demonstration RFID Project in a Taiwan Hospital", HICSS2006, Vol. 8, 04-07.

Want, R. 2005,"An Introduction to RFID Technology," IEEE Pervasive Computing, vol. 5, pp. 25 – 33.

Weis, S.A., Sarma, S.E., Rivest, R.L. and Engels, D.W. 2004, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Security in Pervasive Computing, volume 2802 of Lecture Notes in Computer Science, pp. 201–212.

Weste, N. and Harris, D. 2005, CMOS VLSI Design, Addison & Wesley.

Yin, R.K. 2003, Case study research: Design and Method(3rd edn). London; Sage.

Yoon, B., Sung, MY., Yeon, S., Oh, H.S., Kwon, Y., Kim, C., Kim, K. 2009, HB-MP++ Protocol: An Ultra Light-weight Authentication Protocol for RFID System, IEEE International Conference on RFID, pp.186-191.

Zhang, T., Ouyang, Y. and He,Y. 2008, Traceable Air Baggage Handling System Based on RFID Tags in the Airport, Journal of Theoretical and Applied Electronic Commerce

Research, ISSN 0718–1876 Electronic Version vol 3 / issue 1 / April 2008 / 106-115 © Universidad de Talca – Chile.

Zhi-Wei, J., Xiao-yan S., Lee, H. and Tao, Z. 2009, A Revised One-way Hash based Low-cost Authentication Protocol In RFID System, Wireless Communications, Networking and Mobile Computing. WiCom '09. 5th International Conference, pp. 1- 4.

Appendix A: Existing Authentication Protocols

1. Song & Mitchell (SM) mutual authentication protocol

SM mutual authentication protocol is claimed to provide the most security properties (Song & Mitchell 2008). The protocol is designed for the tags that can generate random strings and perform a hash function and a keyed hash function.

Notation

The following notations are used in the protocol description.

h	A hash function, h: $\{0, 1\}^l \rightarrow \{0, 1\}^l$
f_k	A keyed hash function, f_k: $\{0, 1\}^l \times \{0, 1\}^l \rightarrow \{0, 1\}^l$
N	The number of tags
l	The bit-length of a tag identifier
T_i	The i-th tag
D_i	The detailed information associated with tag T_i
u_i	A string of l bits assigned to T_i
t_i	T_i's identifier of l bits, which equals $h(u_i)$
x_{new}	The new (refreshed) value of x
x_{old}	The most recent value of x
r	A random string of l bits
ϵ	Error message
$\oplus$	XOR operator
$\|$	Concatenation operator
$\leftarrow$	Substitution operator
x >> k	Right circular shift operator, which rotates all bits of x to the right by k bits, as if the left and right ends of x were joined.
x << k	Left circular shift operator, which rotates all bits of x to the left by k bits, as if the left and right ends of x were joined.
$\in_R$	The random choice operator, which randomly selects an element from a finite set using a uniform probability distribution

Protocol

The protocol is described in two parts- initialization and authentication process. The protocol is summarized in Figure A-1

Initialization

The following steps are performed by the tag manufacturer prior to using the protocol.

- The tag manufacturer assigns a string u_i of l bits to each tag T_i, computes $t_i = h(u_i)$, and stores t_i in the tag, where l should be large enough so that an exhaustive search to find the l-bit values t_i and u_i is computationally infeasible.
- The tag manufacturer stores the entries $[(u_i, t_i)_{new}, (u_i, t_i)_{old}, D_i]$ for every tag that it manages. The first pair is for the newly assigned values of u_i and t_i, the second pair is for the previously assigned values, and D_i is for the tag information. Initially $(u_i, t_i)_{new}$ is assigned the initial values of u_i and ti, and $(u_i, t_i)_{old}$ is set to null.

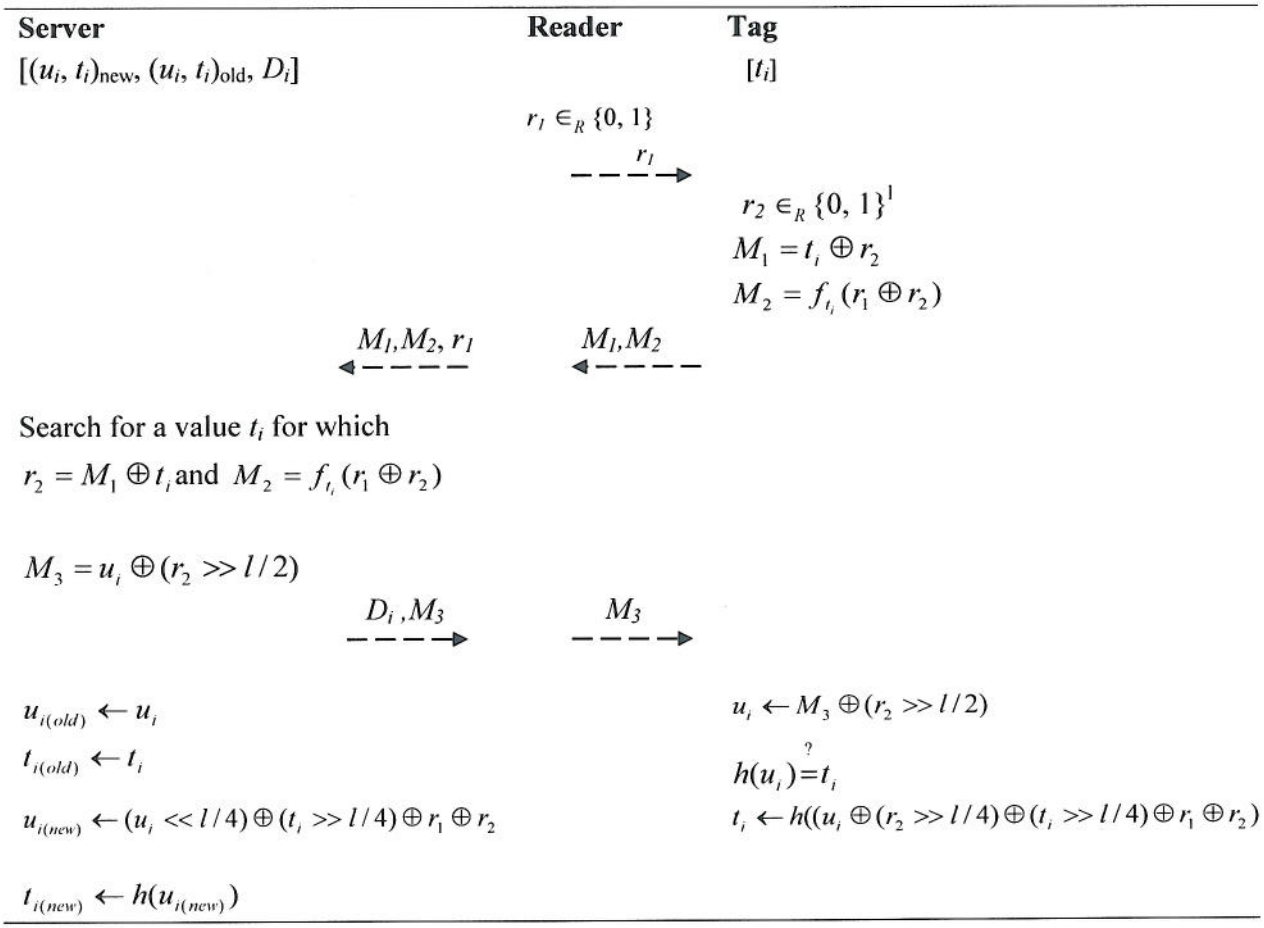

Figure A-1: SM Mutual Authentication Process

Authentication Process

1. Reader: A reader generates a random bit-string $r_1 \in_R \{0, 1\}^l$ and sends it to T_i.

2. Tag: The tag Ti generates a random bit-string $r_2 \in_R \{0, 1\}^l$ as a temporary secret for the session, and computes $M_1 = t_i \oplus r_2$ and $M_2 = f_{t_i}(r_1 \oplus r_2)$. Ti then sends M_1 and M_2 to the reader.

3. Reader: The reader transmits M_1, M_2 and r_1 to the server.

4. Server:

(a) The server searches its database using M_1, M_2 and r_1 as follows.

i. It chooses t_i from amongst the values $t_{i(new)}$ or $t_{i(old)}$ stored in the database.

ii. It puts $r_2 = M_1 \oplus t_i$ and computes $M_2' = f_{t_i}(r_1 \oplus r_2)$.

iii. If $M_2' = M_2$, then it has identified and authenticated Ti. It then goes to step (c). Otherwise, it returns to step i.

(b) If no match is found, the server sends ϵ to the reader and stops the session.

(c) The server computes $M_3 = u_i \oplus (r_2 >> l/2)$ and sends it with D_i to the reader.

(d) The server updates $u_{i(old)}$ and $t_{i(old)}$ for the tag T_i to u_i and t_i respectively, and sets $u_{i(new)} \leftarrow (u_i << l/4) \oplus (t_i >> l/4) \oplus r_1 \oplus r_2$ and $t_{i(new)} \leftarrow h(u_{i(new)})$.

5. Reader: The reader forwards M_3 to T_i.

6. Tag: T_i computes $u_i \leftarrow M_3 \oplus (r_2 >> l/2)$ and checks that $h(u_i) = t_i$. If the check succeeds, the tag has authenticated the server, and sets $t_i \leftarrow h((u_i \oplus (r_2 >> l/4) \oplus (t_i >> l/4) \oplus r_1 \oplus r_2)$. If the check fails, the tag keeps the current value of t_i unchanged.

This protocol is claimed to design to have the most security properties in the literature (song 2008). However, Cai et al. (2009) discovered that the mutual authentication protocol is vulnerable to both tag impersonation attack and reader impersonation attack. This enables an adversary to impersonate any legitimate reader or tag.

2. The Duc-Park-Lee-Kim (DPLK) Protocol

Duc et al. (2006) proposed an authentication protocol DPLK for EPCglobal Class-1 Gen-2 RFID tags. The researchers present a synchronization-based communication protocol for RFID devices. They focus on the EPCGlobal Class-1 Gen-2 RFID tag which supports only simple cryptographic

primitives like Pseudo-random Number Generator (PRNG) and Cyclic Redundancy Code (CRC). Figure A-2 summarizes the DPLK protocol.

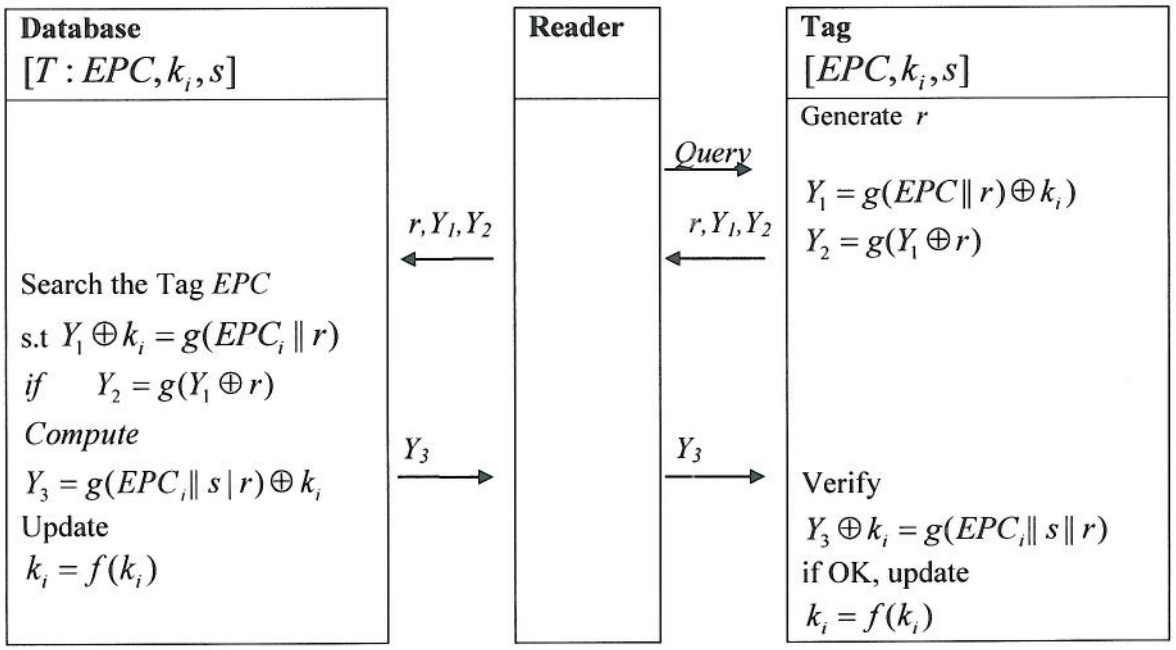

Figure A-2: The DPLK protocol

A tag has an Electronic Product Code EPC, a session key k_i and a long-term secret s. A server stores the values of EPC, k_i and s for each tag. f and g are used respectively to denote the pseudo-random number generator and cyclic redundancy code used by the scheme. When a reader queries to a tag, the tag generates a random number r and responds with $Y_1 = g(EPC \| r) \oplus k_i)$ and $Y_2 = g(Y_1 \oplus r)$. The reader then sent these to the server. The server then performs an exhaustive search to find a stored EPC for which $Y_1 \oplus k_i = g(EPC_i \| r)$. If the server finds a matching value, it sends $Y_3 \oplus k_i = g(EPC_i \| s \| r)$ to the tag. If the authentication process ends successfully, the copies of the session key k_i of the tag and the server are updated using the function f. The security of the scheme can be improved by employing cryptographic hash functions instead of g and f.

The scheme cannot prevent replay attacks before the next successful authentication, because Y_1 and Y_2 can be reused by an attacker to impersonate the tag. Another problem of this scheme is that, a

DoS attack could permanently desynchronise a server and a tag (Chien & Chen 2007). The scheme also does not provide backward untraceability because EPC and s are fixed (Chien & Chen 2007).

3. The Lim-Kwon (LK) Protocol

Lim and Kim (2006) proposed a challenge-response based protocol employing pseudo-random functions. The proposed protocol starts with the simple hash-chain (OSK) protocol and augments it with mutual authentication and further protection capability in view of forward untraceability, thus making the resulting protocol immune against both the forward and the backward tracking attacks. The basic idea to enhance the protocol with forward untraceability is to refresh the tag secret simultaneously within both the tag and the central database, whenever the authentication is completed successfully, using the authentic random numbers exchanged during the protocol execution. The LK scheme uses a forward key chain for tag secret evolution and a backward key chain used in reverse order for server validation.

This scheme makes use of three pseudo-random functions *f*, *g* and *h*, all of which may be constructed from a single lightweight block cipher. The function *f*, *g*, *h* can be described in the following ways:

$f:\{0,1\}^l \times \{0,1\}^{2l_1} \rightarrow \{0,1\}^{2l_1}$: A pseudorandom function to generate authenticators.

$g:\{0,1\}^l \rightarrow \{0,1\}^l$: A pseudorandom function to build the forward key chain used to evolve tag

$h:\{0,1\}^{2l_1} \rightarrow \{0,1\}^{2l_1}$: A pseudorandom function to build the backward key chain used to authenticate the server.

Here, l is the bit-length of a tag secret, and l_1 is the bit-length of random challenges and responses. A server stores two sets of data for each tag, namely the current data set and the most recent old data set. The current data set contains the following tag data: a random secret s_i, m identifiers $t_i^j = ext(g^j(s_i), l_2)$ for $0 \le j \le m-1$, a random number u_i for a backward key chain, the length n_i of the backward key chain, and two secrets for server validation $w_{i,S} = h(u_i)^{n_i}$ and $w_{i,T} = h(w_{i,S})$, where m is the maximum number of allowable authentication failures between two valid sessions, $ext(x,l)$ denotes a simple extract function returning l bits out of x, g^j denotes j iterations of the function g, and l_2 is the bit-length of a tag secret sent by the tag to help the back-end server to identify it. Figure A-3 summarizes the LK protocol.

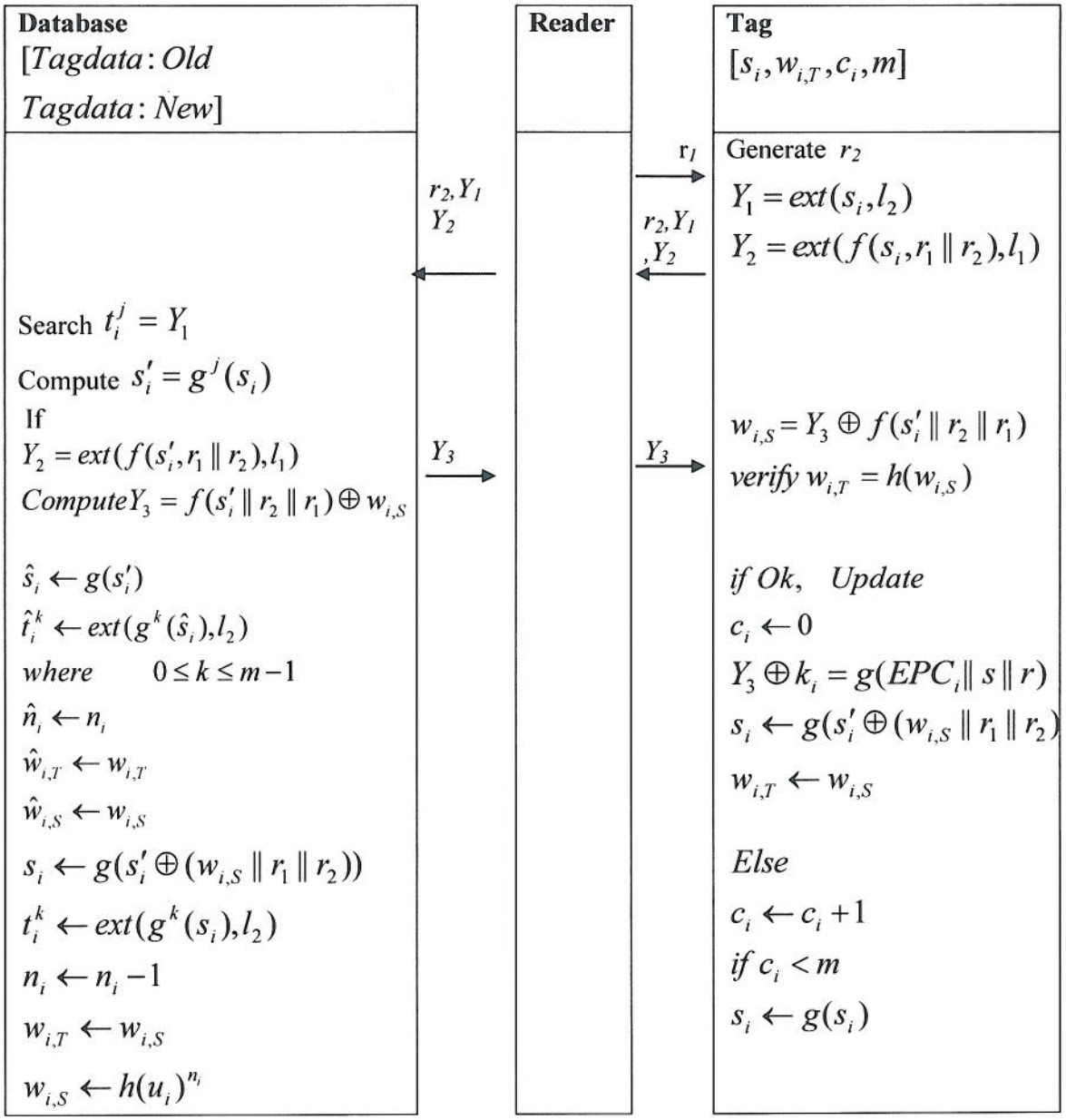

Figure A-3: The LK protocol

The tag stores the tag secret s_i, the server validator $w_{i,T}$, a failure counter c_i and the maximum number of the counter m, where c_i is initialised to 0.

The LK protocol refreshes the tag secret s_i within both the tag and the server whenever the authentication process completes successfully, using exchanged random numbers r_1 and r_2 and a

secret for server validation $w_{i,S}$, i.e. $s_i = g(s_i \oplus (w_{i,S} \| r_1 \| r_2))$. If an authentication session fails, only the tag updates its stored tag secret s_i to $g(s_i)$. The protocol is summarized in Figure.

For tag ownership transfer, the server of the new owner of a tag securely communicates with the server of the current owner, and receives all the relevant information for the tag. The new owner's server then communicates with the tag outside the reading range of the previous owner's server. As a result, the tag refreshes its secrets using random values shared only with the new server, and so no other party can communicate with the tag from this point onwards. The protocol provides forward untraceability from the moment that an adversary misses just one successful authentication session after it has compromised the tag secret. The use of the backward hash key chain makes it difficult to impersonate a server to tags. Storing the most recent old data set protects against the desynchronisation problem arising from DoS attacks. The server can identify a tag in O(1) work.

However, the server must perform O(m) operations for tag authentication, and must perform a significant number of pseudo-random function computations to update the tag secrets after a successful tag authentication. In addition, the server must store two key chains for each tag (Lim & Kim 2006). Also, an attacker can perform rapid-fire interrogation of a tag to increment its counter c_i to the maximum possible value.

As a result, the tag secret s_i will remain static and will give the same response Y_1 to every query until a valid session is performed, thereby allowing tag tracking (Lim & Kim 2006). Moreover, an attack introduced in (Quafi & Phan 2008) allows an adversary to trace a tag without compromising the tag.

4. The Chien-Chen (CC) Protocol

Chien and Chen (2007) proposed an RFID mutual authentication protocol based on the EPCglobal Class-1 Gen-2 RFID standard. The protocol uses simple cryptographic primitives such as a pseudo-random number generator and a cyclic redundancy code.

The server stores five fields for each tag. They are

An Electronic Product Code EPC

The new authentication key k_i

The new access key s_i

The most recent old authentication key $\hat{k}_i$

The most recent old access key $\hat{s}_i$.

A tag stores three values, namely *EPC*, k_i, and s_i. The values of k_i and s_i are updated after each successful authentication to give backward untraceability. f and g are used respectively to denote the pseudorandom number generator and cyclic redundancy code used by the scheme. Figure A-4 summarizes the CC protocol.

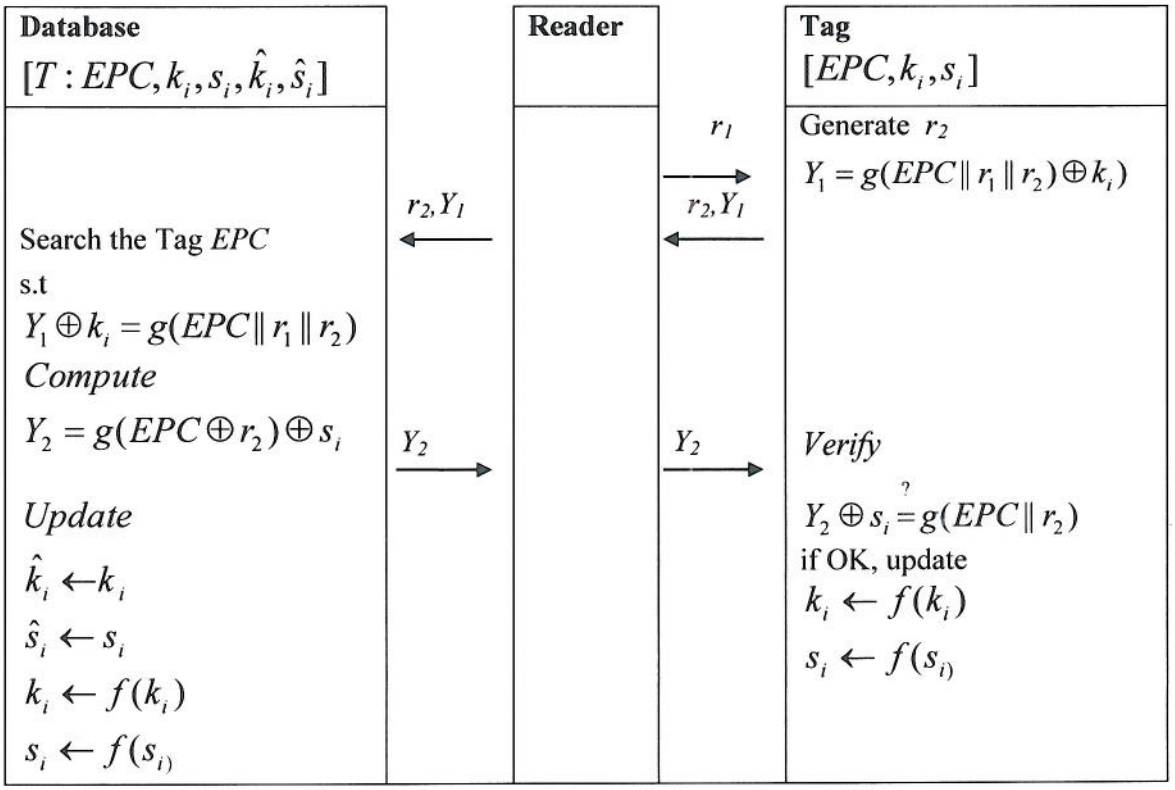

Figure A-4: The CC protocol

The reader queries a tag by sending it a random number r_1. The tag generates another random number r_2, computes $Y_1 = g(EPC \| r_1 \| r_2) \oplus k_i)$ and sends r_2 and Y_1 back to the reader. The reader then sent all these things to the server. The server performs an exhaustive search to find an *EPC* for which $Y_1 \oplus k_i = g(EPC \| r_1 \| r_2)$. If an EPC is matched, the server computes $Y_2 = g(EPC \oplus r_2) \oplus s_i$ and sends it to the reader and then the reader sends it to the tag. The server

then updates k_i and s_i to $f(k_i)$ and $f(s_i)$, respectively. The tag verifies the received value of Y_2. If the verification is successful, the tag also updates its keys k_i and s_i.

As because the *EPC* is static, the protocol still permits a degree of backward traceability. If a strong attacker has compromised a tag and intercepted the values of r_1 and Y_1 sent in the immediately previous session the attacker can check that $f(Y_1 \oplus g(EPC \| r_1 \| r_2))$ equals the compromised key k_i, and can thus determine the previous key $\hat{k}_i$. In the same way, if a strong attacker has intercepted r_2 and Y_2 in the immediately previous session, it can compute $\hat{s}_i$ by checking whether $f(Y_2 \oplus g(EPC \oplus r_2))$ equals s_i. Moreover, the CC scheme permits location tracking, tag impersonation, server impersonation, and backward traceability, because of the linear properties of a cyclic redundancy code (CRC) that is used as a checksum algorithm (Peris-Lopez et al. 2009). In addition, the use of a short length (16-bit) CRC allows desynchronisation by DoS attacks and does not guarantee unequivocal tag identification (Peris-Lopez et al. 2009).

5. The Tsudik Protocols

Tsudik (2006) described an RFID identification protocol that provides a basic level of tag identification using time-stamps. It will be referred to as T1. This is a famous authentication protocol that places little burden on the back-end server and uses monotonically increasing timestamp which makes it secure against tracking but unsecure against DoS attack. Tsudik (2007) proposed two further schemes referred to as the T2 and T3 schemes that also provide tag authentication. The schemes use monotonically increasing time-stamps for tracking-resistant tag authentication, and employ a keyed hash function *f*.

In these three schemes, a tag stores k_i, t_0, and t_{max}, where k_i is a tag-specific secret, t_0 is initially a time-stamp assigned to the tag at the time of manufacture, and t_{max} is the highest possible time-stamp. The value k_i serves as both a tag identifier and a cryptographic key. Neither t_0 nor t_{max} need to be unique to a tag. A tag must also possess a uniquely seeded pseudo-random number generator.

In T1, a server maintains a periodically updated hash table in which each row contains ID_i, k_i, and $f_{k_i}(t_0')$ for a tag, where t_0' is the time-stamp for the server. The server first sends t_0' to a tag. If $t_0' \leq t_0$ or $t_0' > t_{max}$, the tag generates and returns a pseudo-random number r. Otherwise, the tag

updates its time stamp t_0 to t_0', and replies with $Y_1 = f_{k_i}(t_0)$. The server can identify the tag by finding Y_1 in its look-up table and sends an acknowledgement message ACK to the reader and then the reader to the tag. Figure A-5 summarizes the T1 protocol.

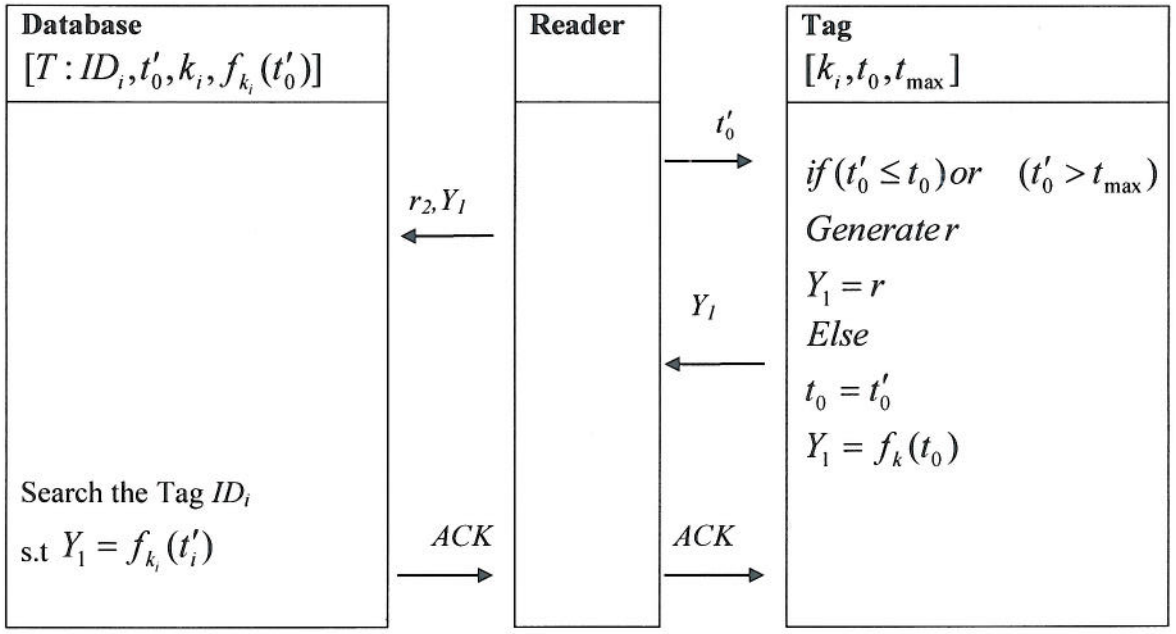

Figure A-5: The Tsudik T_1 Protocol

The T1 scheme only needs O(1) operations to identify a tag, because a hash table is used for all look-ups. However, the scheme merely identifies a tag and does not provide tag authentication. Additionally, the scheme is susceptible to a trivial DoS attack in which an attacker incapacitates a tag by sending it an inaccurate future time-stamp value (Tsudik 2007). Moreover, the scheme makes the assumption that a given tag is never identified more than once within the same time interval (Tsudik 2007).

To overcome the problem of the scheme T1 the T2 scheme introduce tag authentication using a challenge-response method. In this scheme a tag receives a query consisting of a time-stamp t_0' and a random number r_1, it checks that t_0' is a valid time-stamp. If the validation is successful, the tag updates t_0 to t_0', and computes $Y_1 = f_k(t_0)$. Otherwise, the tag generates a pseudo-random number r_2 instead of computing Y_1. The tag then generates a pseudo-random number r_3, computes $Y_2 = f_{k_i}(r_3 \parallel r_1)$ and responds to the server with r_3, Y_1 and $Y2$. The server identifies the tag by

finding Y_1 in its look-up table for the time-stamp t_0', and authenticates the tag by checking that $Y_2 = f_{k_i}(r_3 \parallel r_1)$. Figure A-6 summarizes the T2 protocol.

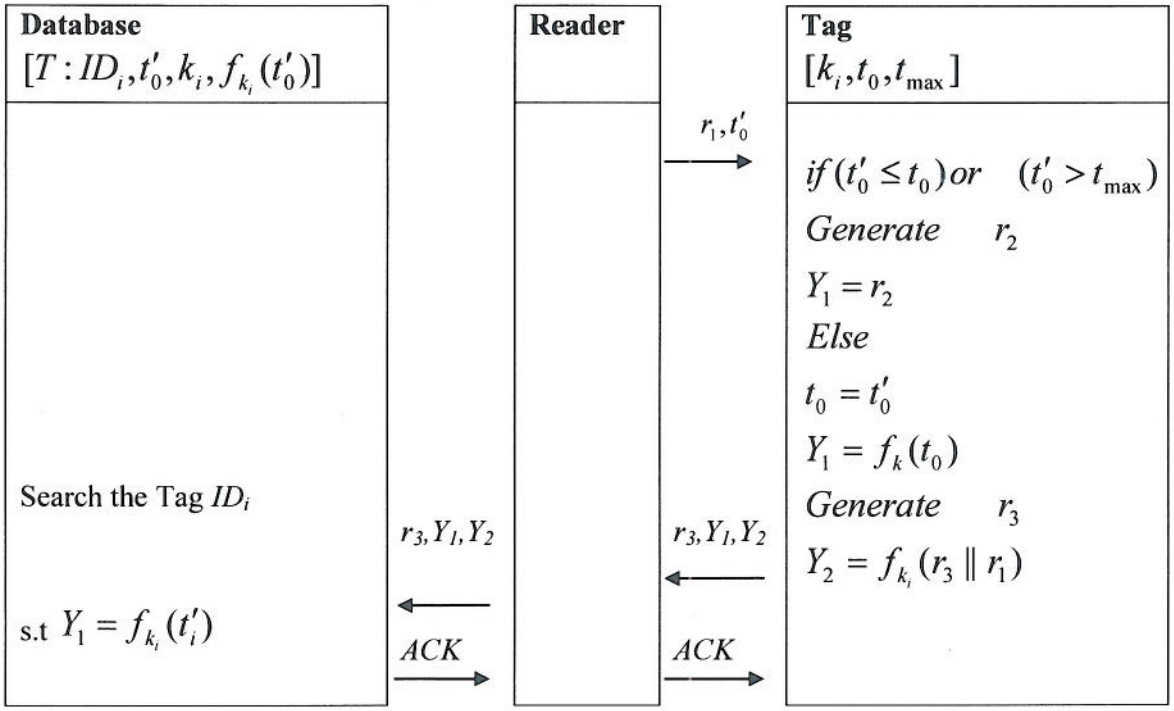

Figure A-6: The Tsudik T2 protocol

This scheme also takes constant time to identify and authenticate a tag because of its use of a look-up table. However, if a tag has been previously desynchronised by an attacker, it requires the server to perform O(n) operations to authenticate the tag. The T2 scheme is also susceptible to DoS attacks, like the T1 scheme (Tsudik 2007).

The DoS vulnerability of the T1 and T2 schemes is overcome in T3 scheme by using a hash-chain to generate a so-called epoch token, which allows a tag to ascertain that a time-stamp is not too far into the future. Figure A-7 summarizes the T3 protocol.

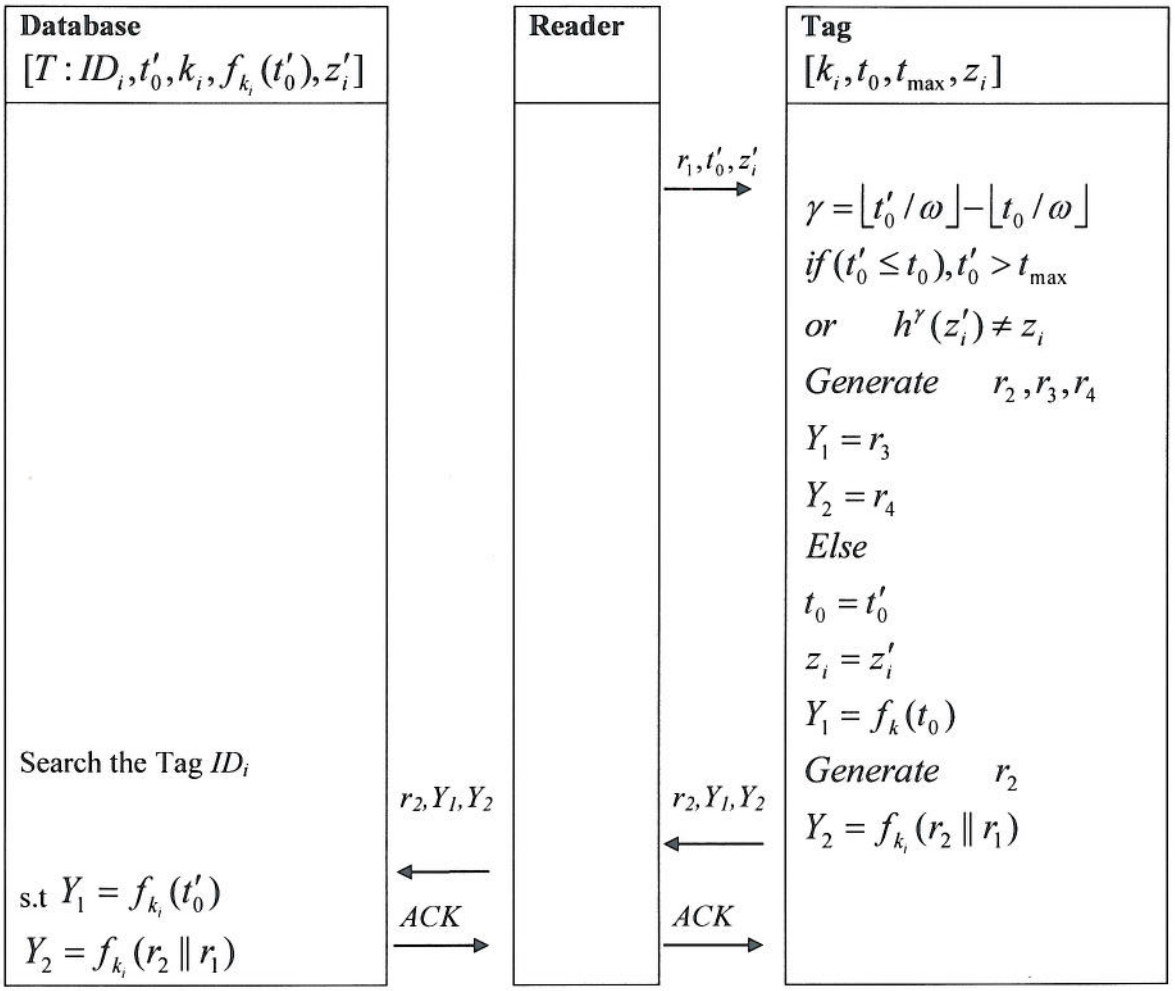

Figure A-7: The Tsudik T3 protocol

A server generates a hash chain of length v by starting with an initial value (say, X) and repeatedly hashing it v times to produce a root $h^v(X)$, where $v = \lfloor t_{max} / \omega \rfloor$ and ω is the epoch duration, (e.g. one day). Each tag initially stores an epoch token z_i as a root of the hash chain, $h^v(X)$.

A server generates a random number r_1 and sends t_0', r_1 and its epoch token z_i' to a tag. The tag checks the received values of t_0' and z_i' by verifying that $t_0' \geq t_0$ and $t_0' < t_{max}$ and that $z_i' = h^{\gamma}(z_i')$, where $\gamma = \lfloor t_0' / \omega \rfloor - \lfloor t_0 / \omega \rfloor$. If the validations are successful, the tag updates t_0 and z_i to t_0' and z_i', respectively. The tag then computes $Y_1 = f_{k_i}(t_0)$, generates r_2, computes $Y_2 = f_{k_i}(r_1 \| r_2)$, and sends Y_1, Y_2, and r_2 as its reply. Otherwise, the tag generates pseudo-

random numbers r_2, r_3 and r_4, and sends them instead. The server identifies the tag by finding Y_1 in its look-up table for the time-stamp t_0', and authenticates the tag by checking that $Y_2 = f_{k_i}(r_2 \| r_1)$. Figure summarises the T_3 protocol.

The server only needs to perform $O(1)$ operations to identify and authenticate a tag, if the tag reply is valid. If not, the server takes O(n) time to authenticate a tag. For T_3, DoS attacks still remain a threat, because an adversary can incapacitate a tag for the epoch duration ω, if it queries the tag with the current epoch token and the maximum possible t_0' within the current epoch (Tsudik 2007). In addition, for both T_2 and T_3, the adversary can potentially distinguish between synchronised and desynchronised tags by timing the server responses, because a synchronised tag only requires a server to perform a quick table look-up, whereas a desynchronised tag requires it to perform an exhaustive search. Moreover, all three of the Tsudik schemes have backward traceability, because of their use of a fixed key k_i (Tsudik 2007).

6. The Molnar-Soppera-Wagner (MSW) Protocol

Molnar et al. (2005) proposed an RFID pseudonym protocol that employs pseudo-random number functions. They claim that, the scheme provides two new features not seen in prior RFID protocols, namely time-limited delegation and ownership transfer. The protocol is based around a tree of secrets of depth $d = d_1+d_2$ like the MW scheme. Each node in the tree has its own k-bit secret key. The first d_1 levels of the tree contain node secrets that are chosen uniformly and independently at random by the Trusted Center during system initialization. Each node at depth d1 corresponds to a unique tag. When a tag is enrolled into the system, it receives all keys on the path from its node to the root. Thus, each tag needs the capacity to store d_1 secrets. The next d_2 levels of the tree contain secrets that are derived using a pseudo-random generator G.

When a reader queries a tag, the tag generates a random number r, computes the key values $k_{(d_1+j)} = G_b(k_{(d_1+(j-1))})$, where j = 1, 2, · · · · , d_2 and $b \in \{0,1\}$, and responds with a pseudonym $Y_1 = (F_{k_1}(r), F_{k_2}(r),..., F_{k_d}(r))$, where F is a pseudo-random number function and k_j (j = 1,2,· · · · ·, d) represent the secrets along the path in the tree of secrets from the root to the tag's current leaf. The tag then increments the counter c_i. Figure A-8 summarizes the MSW protocol.

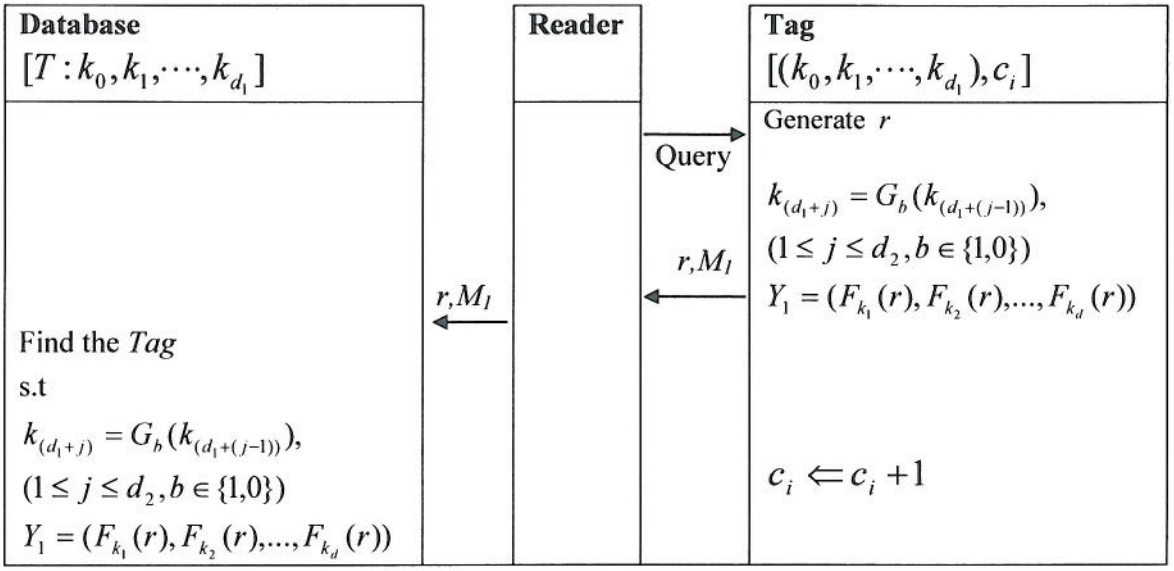

Figure A-8: MSW Protocol

The scheme uses tree to store the tag information. So the tag identification complexity is O(log$n$) which is much lower than O(n). Moreover, it allows for time-limited delegation. However, the ownership transfer procedure of this scheme is rather restrictive, in the sense that the old and new owners must trust the same Trusted Centre (TC), and the TC's database controls all the secret tag information. A reader that has received partial information from the TC can read the tag only a limited number of times without on-line connectivity to the TC. The problem in this scheme is that, it only provides tag identification, not mutual authentication. It also allows replay attacks. The tree-based secrets approach requires that each tag stores the $\lceil \log n \rceil$ secrets corresponding to the path from the root to the tag and performs a number of pseudo-random number function computations to generate its pseudonym. In addition, if a tag secret is compromised, then the attacker can compute the secrets for every descendent in the sub-tree rooted at that tag node.

7. HB-MP$^+$ Protocol

Leng et al.(2008) propose an enhanced version of the HB-MP authentication protocol, called the HB-MP$^+$ protocol. The HB-MP$^+$ protocol overcomes the man-in-the-middle attack to which the basic HB-MP protocol is vulnerable. Protection against the man-in-the-middle attack as proposed by Gilbert et al. (2005) has been considered in the HB-MP protocol. The rotation of xm is used to protect from the attack. However, this rotation has its own weakness. In the HB-MP protocol, for

every new session, *xm* needs to be identical in the *i*th round. It is not mentioned clearly about when to start and end an authentication session. It is assumed that when the tag enters the range and starts to communicate with the reader, an authentication session begins and when the *q*-round is finished or the tag leaves from the range of the reader, the session ends. Since $x = Rotate(x, yi)$, *xm* in the first round of all the authentication sessions should be the same. The attacker can initiate repetitive authentication sessions, initially restricted to the first round. The techniques used in last section can then be exploited to reveal the tag's first round *xm*. If the attacker observes the *i*th round, he is able to reveal the *xm* used in the *i*th round.

The protocol has to use the same *xm* between authentication sessions to avoid the synchronisation problem. The value of x is fixed. If the value of x is changed after every authentication session on both the reader and tag side, a new reader will not be able to verify the updated tag and cannot verify new tag. It is possible only if all the readers and tags are updated at the same time after every authentication session, which is expensive and technically difficult. Even if the synchronization problem is removed and the value of x is updated in every authentication session there is still a way to conduct the man-in-the-middle attack. The length of x and y is k. If in an authentication session, the protocol runs k rounds, the x will be rotated p bits, here p is the number of '1' in y, so if the attacker runs the protocol for k times, namely k^2 rounds, the x will be rotated $p \cdot k$ times and it is rotated back to its initial value. So a repeat of *xm* happens again. Since the proposed x is 512 bits, 262144 rounds will definitely generate a repeated *xm* which is an affordable attack.

To overcome the weakness resulting from the predictable repetition of xm, Leng et al.(2008) use some additional random bits generated by the reader to randomize the rotation. The objective of HB-MP+ is to use a random secret in each round, namely a round key x_s.

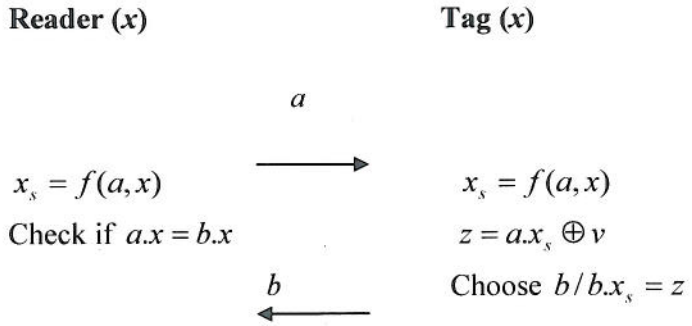

Figure A-9: A single round of HB-MP$^+$ protocol

The HB-MP+ protocol is shown in Figure A-9 and the steps are given as follows:

1. The reader picks at random a m-bit binary vector a and sends it to the tag.
2. The reader and tag computes the round key $x_s = f(a,x)$. $f(.)$ is a one-way function.
3. The tag computes z as follows $z = a.x_s \oplus v$ and looks for a m-bit binary vector b such that $b.x_s = z$
4. The tag sends b to the reader
5. The reader computes the $x_s = f(a, x)$, using the secret x and random number a
6. The reader checks if $a.x_s = b.x_s$

The round key x_s is obtained by a random number a and the shared secret x. There is no need for another secret y and because the x is not changed. There is no problem of synchronization between tag and reader. Since the rotation is a linear operation, the output of $f(.)$ should be less predictable. Using the bit operations, it is easy to implement a low-cost non-linear function $f(.)$. As $f(.)$ does not necessarily use rotation, the bits of x are not mentioned.

8. HB-MP^{++} Protocol

The nonlinear one-way function used in HB-MP+ is abstract. So it is not possible to prove the validity of the protocol for RFID systems. Also, as the tag's response has the same number of bits, the protocol is still vulnerable to traceability (Weste & Harris 2005, Garg, 2000). The HB-MP++ uses the LSFR that has two consecutive two-stage memory or storage stage and feedback logic (Weste & Harris 2005, Garg, 2000). Pseudorandom Noise (PN) sequences are generated by combining the outputs of feedback shift registers. PN sequences are shifted through the shift register in response to clock pulses. The initial contents of the stages and feedback logic determine the successive contents of the stages. A feedback shift register and its output are linear when the feedback logic consists of entirely of modulo-2 adders. Figure A-10 shows n-stage LSFR. The main reason why the LSFR is used in this protocol is that the output of LSFR (PN sequences) has a "run property". With the "run property", it is possible to provide a more efficient resistance against the man-in-the-middle attacks by adding more randomness. A "run" is the sequence of a single type of binary digits. The length of the "run" is the number of same digits in the PN sequences. The length of the run will be used in the function of Rotation and Truncation.

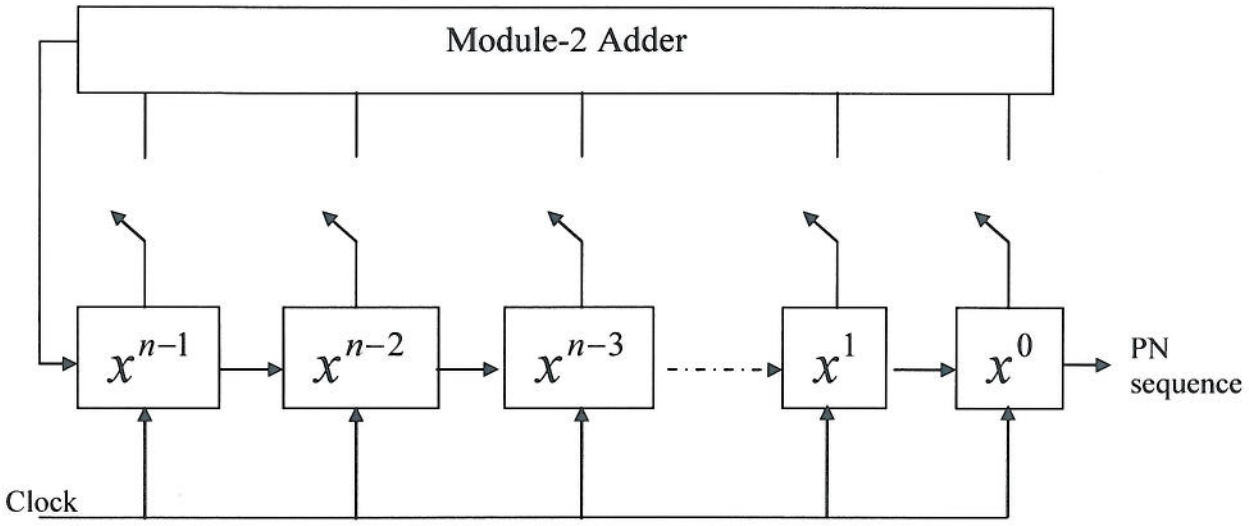

Figure A-10: N-stage Linear Feedback Shift Register

The main idea of HB-MP++ protocol is to implement the concrete and ultra light-weight functions in order to rotate the secret key x in each round. These functions ensures unpredictable randomness to overcome the weakness of HB-MP^{+}. The notations used in HBMP++ are as follows:

k length of the secret key shared by reader and tag

x k-bit secret key shared by reader and tag

x' denotes *Rotate*(x, r_n)

x_s denotes *Truncate*(x', r_n)

a random k-bit binary vector

a' denotes $a \oplus x$

a_s denotes *Truncate*(a', r_n)

r_n number of run of PN sequence

Rotate(p,u) bitwise left rotate operator. The operand p is rotated u position

Truncate(p,u) truncate operator. The operand p is truncated u-LSB bits.

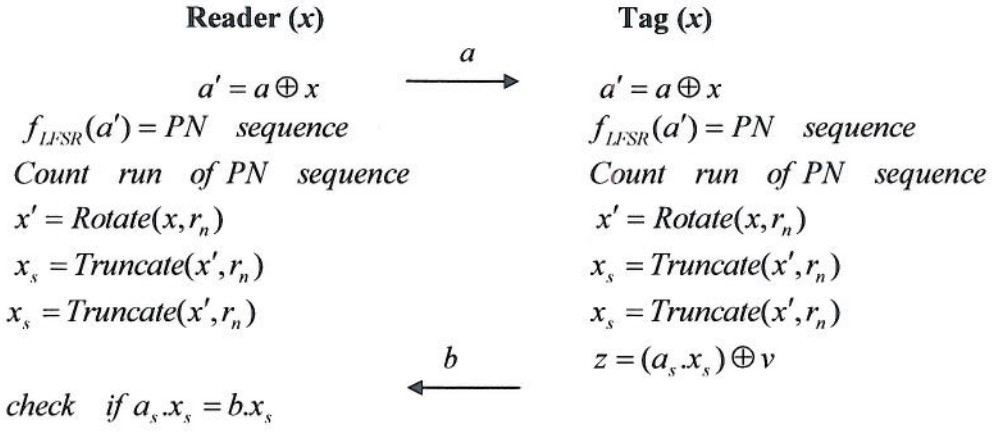

Figure A-11: One Round of HB-MP^{++} Protocol

The protocol HB-MP++ is also composed of q rounds, shown in Figure A-11, and can be described as follows:

1. The reader generates a k-bit binary vector a and sends it to the tag
2. The tag and reader compute $a' = a \oplus x$
3. The tag and reader generate PN sequence from LFSR using a' as initial value
4. The tag and reader calculate the length of "run" of the PN sequence
5. The tag and reader compute x = $Rotate(x, r_n)$ and $x_s = Truncate(x, r_n)$ and $a_s = Truncate(a', r_n)$
6. The tag computes z as follows: $z = a_s . x_s \oplus v$ and looks for a random-bit($<k$) binary vector b such that $z = b . x_s$
7. The tag sends b to the reader
8. The reader checks if $a_s . x_s = b \oplus x_s$

The strength of this protocol is that the XOR function can enhance the unpredictability of a in step 2. If the adversary eavesdrops a illegally, he cannot get the value a' as the secret key x is unknown. The value of a' is used for the initial value of the LFSR and generate a PN noise sequence. The secret key x is rotated r_n position left to give randomness. The r_n is also used in Truncate function. As the value of r_n varies in each stage the bit number of a_s is supposed to vary. The bit number's change of the tag's response b makes the protocol resistant to traceability.