A RFID PROTOCOL FOR DETECTING THE EXISTENCE OF A SINGLE RFID TAG BY TWO RFID READERS

TAN AIK THENG

UNIVERSITI SAINS MALAYSIA

2012

A RFID PROTOCOL FOR DETECTING THE EXISTENCE OF A SINGLE RFID TAG BY TWO RFID READERS

by

TAN AIK THENG

Thesis submitted in fulfilment of the requirements
for the degree of
Master of Science

January 2012

ACKNOWLEDGMENT

First of all, I would like to thank Assoc Prof Rahmat Budiarto for giving me an opportunity to work on this research under his supervision. Besides that, I would like to thank Universiti Sains Malaysia for providing me financial support to publish proceeding and journal papers. Once again, I would like to thank my supervisor Assoc Prof Rahmat Budiarto who always provides me guidelines, encouragement, and valuable of comments on this thesis. Finally, I would like to thank those who render support to me especially my lovely mother and brother. I would like to dedicate this thesis to my late father who had passed away three years ago and hope that god will bless him forever.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

mod	Modulus
RFID	Radio Frequency Identification
ECC	Elliptic Curve Cryptography
MAC	Message Authentication Code
RSA	Rivest-Shamir-Adleman
ALU	Arithmetic Logic Unit
RAM	Read Access Memory
FDA	Food & Drug Administration
CMOS	Complementary Metal Oxide Semiconductor
EEPROM	Electrically Erasable Programmable Read Only Memory
FPGA	Field-Programmable Gate Array
ROM	Read Only Memory

LIST OF NOTATIONS

r, r_1, r_2	Random numbers
r_a, r_b , r_a', r_b', r_{1a}, r_{2b}	Hash values
P_{AB}	Proof that Tag A and B scan simultaneously
x_a, x_b, x_r	Secret keys sharing in between RFID tag and server
m_a, m_b, m_r, m_b', m_a', m_{1a}, m_{2b}, m_r	Message authentication code
P_1, P_2	Proof that RFID Reader 1 and 2 read the RFID tag simultaneously
n_{r1}, n_{r2}, n_{tA2}, n_{tB2}, n_{tA1}, n_{tB1}	Random numbers
C_A, C_B, C_A', C_B'	Cipher texts
n_1, n_2, n_3	Public keys

PROTOKOL RFID UNTUK PENGESANAN KEWUJUDAN SATU TAG RFID TUNGGAL DI ANTARA DUA PEMBACA RFID

ABSTRAK

Terdapat batasan bagi pembaca RFID untuk membaca ribuan data yang disediakan oleh tag RFID dalam sesaat. Oleh itu, konfigurasi pembaca RFID berbilang (multiple RFID reader) diperlukan untuk menangani senario ini. Dalam aplikasi sebenar sistem RFID, terdapat banyak konfigurasi untuk pembaca RFID dan tag RFID. Contohnya: tag RFID berbilang berkomunikasi dengan satu pembaca RFID atau sebaliknya, tag RFID berbilang berkomunikasi dengan pembaca RFID berbilang, dan pembaca RFID berbilang berkomunikasi dengan satu tag RFID tunggal (single RFID tag). Untuk memastikan protokol rangkaian sedia ada (yang dibangunkan oleh para penyelidik terdahulu bagi komunikasi dalam sistem RFID) boleh membantu dalam apa jua jenis tag RFID dan konfigurasi pembaca RFID, maka satu ujian khusus diperkenalkan dalam penyelidikan ini. Beberapa jenis pembaca RFID dan konfigurasi tag RFID digunakan bagi mengesahkan kemampuan setiap protokol sedia ada untuk mengesan kewujudan tag RFID tunggal dalam medan pembaca RFID berbilang. Berdasarkan analisis kami, terdapat dua jenis protokol rangkaian yang digunakan untuk membuktikan kewujudan tag RFID berbilang, iaitu tag bersandar dan tag bebas. Tag bersandar bergantung sesama sendiri untuk menjana kod rahsia dan kod pengesahan. Bagi tag bebas, adalah sebaliknya. Kedua-dua jenis protokol ini digunakan bagi mengesahkan kewujudan tag RFID dalam medan pembaca RFID berbilang, dalam usaha menentukan keupayaan pengesanan mereka dalam sistem RFID. Secara tipikal, tag RFID tunggal yang disahkan oleh konfigurasi pembaca RFID berbilang boleh digunakan

dalam infrastruktur RFID pelbagai tujuan. Di sini, tag RFID tunggal diperlukan oleh pelbagai pembaca bagi tujuan yang berbeza dan pengesahan komunikasi di antara pembaca RFID berbilang. Selain itu, kriptografi tak simetri seperti kriptografi keluk elips (eliliptic curve cryptography) digunakan bagi menggantikan kriptografi simetri. Hal ini bertujuan melaksanakan enkripsi data pada tag dan pembaca RFID dalam usaha menyediakan keselamatan perlindungan yang tinggi terhadap serangan, di samping mengekalkan aplikasi kunci rahsia pada tag dan pembaca RFID. Terdapat batasan dalam penyelidikan ini untuk menyelidik perkara ini dengan lebih mendalam selain membuktikan keupayaan protokol rangkaian mengesan kewujudan tag RFID tunggal dalam medan pembaca RFID berbilang, dan juga penambahbaikan keselamatan perlindungan. Sebagai kesimpulan, adalah penting untuk memastikan bahawa protokol rangkaian yang dibangunkan bagi komunkasi dalam sistem RFID boleh berfungsi dengan pembaca RFID dan konfigurasi tag RFID dalam usaha menyediakan suatu sistem yang boleh diharapkan dan selamat kepada pengguna.

A RFID PROTOCOL FOR DETECTING THE EXISTENCE OF A SINGLE RFID TAG BY TWO RFID READERS

ABSTRACT

There is a limitation for a RFID reader to read thousands of data provided by RFID tags in a second. Hence, multiple RFID readers configuration is required to help resolving this scenario. In real world applications of RFID system, there will be a lot of configurations for RFID reader and RFID tag such as multiple RFID tag communicate with a RFID reader or vice versa, multiple RFID tag communicate with multiple RFID reader and multiple RFID readers communicate with a single RFID tag. In order to ensure that existing network protocols which developed by previous researchers for communication in RFID system can support in whatever types of RFID tag and RFID reader configuration, a reliability and specific test through these existing network protocols have been introduced in this research work. Several types of RFID reader and RFID tag configuration will be used for verifying each of existing network protocols ability for detecting a single RFID tag existence in multiple RFID readers field. Based on our analysis, it is discovered that there are two types of network protocol used for generating multiple RFID tag coexistence proof. They are named as tags dependent on each other's output network protocol and tags independent on each other's output network protocol which used to generate hash value and message authentication code. Via this research work, these two types of network protocol are applied for authenticating a single RFID tag existence in multiple RFID readers field in order to determine their ability to be used for authentication in RFID system. Typically, a single RFID tag authenticated by multiple RFID reader configuration can

be used in a multi-purpose RFID infrastructure where a single RFID tag is interrogated by various readers for different purposes and verification of race communication in between multiple RFID reader existence. Apart from that, an application of asymmetric cryptography such as elliptic curve cryptography to replace symmetric cryptography for performing data encryption on RFID tag and RFID reader helping to provide high security protecting to resist adversaries attack as well as maintaining small length of secret key application on RFID tag and RFID reader. There is a limitation for this research work to further enhance besides investigating on each of multiple RFID tag coexistence proof's network protocols ability for authenticating a single RFID tag existence in multiple RFID readers field as well as security improvement. As a conclusion, it is significant to ensure that network protocol developed for communication in RFID system can work in whatever types of RFID reader and RFID tag configurations in order to provide users a reliable and secure security monitoring system.

CHAPTER 1

INTRODUCTION

RFID (Radio-Frequency Identification) tags are small, inexpensive microchips capable of transmitting unique identifiers wirelessly over a short distance. Thanks to their ability in automating supply-chain logistics, RFID tags promise eventually to supplant the optical barcode as a means of identifying goods [12]. RFID system has been applied widely nowadays in many industries. It is important for manufacturers to ensure that each of RFID tags can function and support in different kinds of RFID reader configurations. RFID reader has limitation to read data sent by a group of RFID tags per second. Hence, it is necessary to apply more than one RFID reader to read data sent out by a group of RFID tags. It is common that a single RFID reader is unable to cover the entire region of interest [27]. Before each of RFID readers or RFID tags being applied in a complex network communication, manufacturers need to ensure that network protocol that has been designed for communication is able to handle on both scenarios which include a single RFID tag existence or multiple RFID tag coexistence authenticated by different kinds of RFID reader configurations. Yoking Proof [12] which developed by Ari Juels is a pioneer design used for proofing a group of RFID tags existence in a single RFID reader field. It is widely applied in pharmaceutical distribution and manufacturing fields. More detailed explanations are as follows:

- **Pharmaceutical distribution**: Suppose that there is a legal requirement for a certain medication to be dispensed together with a leaflet describing its side-effects. One RFID tag might be embedded in the container for the medication, while another is embedded in an accompanying leaflet. A yoking-proof would provide evidence that each container

of the medication was dispensed with a leaflet. It might be transmitted to, for example, the U.S. FDA, for verification, or stored by a pharmacist as evidence in case of dispute.

- **Manufacturing**: Suppose that a manufacturer of aircraft equipment wishes to certify that a certain part always leaves its factories with a safety cap attached. Given RFID tags in both the part and the cap, a yoking-proof can provide third-party verifiable evidence to support such certification [12].

There are many proposed works done for security improvement on Yoking Proof such as Grouping Proof [24], Modified Proof [22] and Proof Proposed by Thiti et al. [19]. However, there is a lack of research on existing network protocols which used to generate multiple RFID tag coexistence proof. In this chapter, we are going to review each existing network protocol ability for authenticating a single RFID tag existence in multiple RFID reader field. At first, let's go through some general steps of generating multiple RFID tag coexistence proof. The steps are as follows:

1. Server sends a random number to RFID reader.
2. RFID reader deploys the random number sent out by server to its surrounding RFID tags, and waits for RFID tags to generate hash value and message authentication code.
3. Once RFID reader receives hash values and message authentication codes generated by RFID tags, it will submit these parameters for verification.
4. RFID tags, RFID reader and server share same secret key for generating and verifying hash value and message authentication code.

As a short summary of this section, our point of view is network protocol developed for communication in RFID system should be compatible in whatever types of RFID reader and RFID

tag configurations in order to let users have a secure and safe security monitoring system in their daily applications.

1.1 Background Information

There are a lot of multiple RFID tag coexistence proofs which include Yoking Proof, Grouping Proof, Modified Proof, Ordinal Authentication Protocols for RFID Tags and The Proof Proposed by Thiti et al. have been introduced by previous researchers. All enhancements and improvements done previously were about the security for preventing adversary attacks. Until today, it is still a doubt whether these existing multiple RFID tag coexistence proof's network protocols could be applied in different kinds of RFID reader configurations for authenticating a single RFID tag existence. To date, there is no research work done for resketching these existing of network protocols under presence of multiple RFID readers field to determine their ability for authenticating a single RFID tag existence. The reason that these network protocols are proposed to test in multiple RFID readers field for authenticating a single RFID tag existence application because it covers one of configurations in our daily applications on RFID system. For example, various RFID readers query a RFID tag to retrieve information of interest for the person or object whose identification information is stored in the tag where such application of RFID system is known as multi-context RFID infrastructure [13]. The information of RFID tag could be retrieved by multiple RFID readers at the same time for verification purpose if multi-context RFID infrastructure is used. Another example is related to there is a possibility for a RFID tag mobiles in surrounding RFID readers field where we will normally see this application in supply chain management or manufacturing environments. Based on these two examples, it shows that there is a necessity of application on multiple RFID reader configuration to cover its interrogation region because each RFID reader has a limited interrogation region within which it can communicate with a tag [27]. Thus, this research work has been

carried out to ensure that existing of network protocols which used to generate multiple RFID tag coexistence proof could be applied in whatever of RFID reader configurations for authenticating a single or multiple RFID tag existence. Figure 1.1 and Figure 1.2 are the topologies used for authenticating data in different configurations of RFID reader and RFID tag.

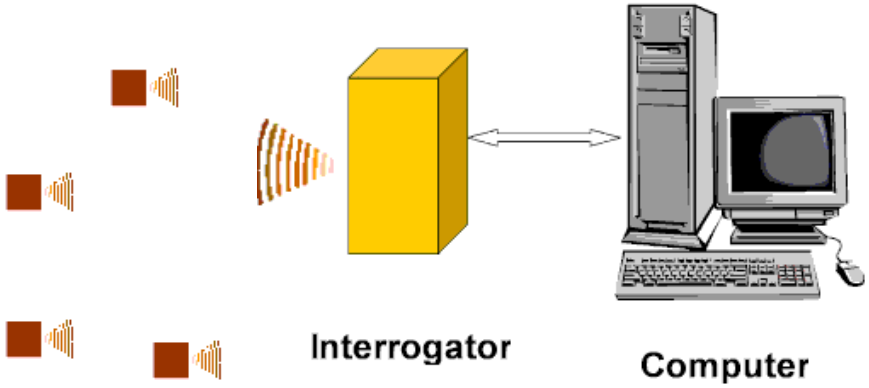

Figure 1.1: Topology for authenticating multiple RFID tags existence

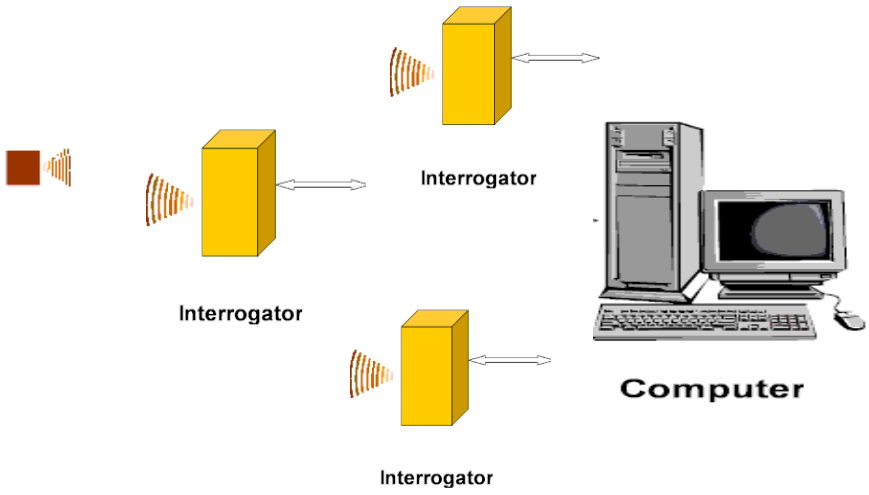

Figure 1.2: Topology for authenticating a single RFID tag existence

1.2 Problem Statement

Based on our finding, there are two types of network protocol applied for generating multiple RFID tag coexistence proof. The types of network protocol are named as follows:

- Tags dependent on each other's output network protocol - The protocol used to transfer outputs generated by a RFID tag to other RFID tag via RFID reader as inputs for generating message authentication code and hash value.
- Tags independent on each other's output network protocol - The protocol is restricted for communication among RFID tag and RFID reader. It can only be used for communication between RFID reader and RFID tag. All outputs generated by each RFID tag will be directly submitted to RFID reader without sending it to other RFID tags.

Most of multiple RFID tag coexistence proofs apply tags dependent on each other's output network protocol for generating its proof, but unfortunately a problem occurs when tags dependent on each other's output network protocol is applied in multiple RFID readers field for authenticating a single RFID tag existence. A single RFID tag existence in multiple RFID readers field is unable to be detected by multiple RFID readers when tags dependent on each other's output network protocol is used for communication in this configuration. Based on our analysis, tags dependent on each other's output network protocol requires at least a pair of RFID tag existence in multiple RFID readers field in order to enable RFID readers detecting both RFID tags existence. With current existing of network protocols developed by previous researchers which used for generating multiple RFID tag coexistence proof such as Yoking Proof, Grouping Proof, Modified Proof by S. Piramuthu and Ordinal Authentication Protocols for RFID Tags, a single RFID tag is unable detected by RFID readers when a tag is located within multiple RFID readers field. However, network protocol which developed by Thiti et al.

is the only one that can be used in multiple RFID readers field for detecting a single RFID tag existence. Even though, Thiti et al. has resolved network protocol issue that causes a flaw on authentication in RFID system, there is a security issue needed to be improved during authentication between RFID tag and RFID reader. In order to resolve the security issue, a solution has been proposed via this research work by introducing application of asymmetric cryptography such as elliptic curve cryptography to replace symmetric cryptography which has been applied in existing of multiple RFID tag coexistence proofs for performing data encryption and verification. The purpose of asymmetric cryptography is proposed to replace symmetric cryptography used for generating multiple RFID tag coexistence proof due to asymmetric cryptography's ability to prevent secret key being eavesdropped during authentication is on going between sender and receiver, and indirectly server does not need to manage a large quantity of secret keys if a public key is used by a group of RFID tags. It helps to save time during key management process. As a summary, elliptic curve cryptography is identified suitable to replace symmetric cryptography for performing data encryption in RFID system because its private key remains private and the size of the secret key being used is small. Besides that, it helps to prevent replay attack occurs during authentication data process happening between RFID reader and RFID tag because adversary does not know secret key stored on each sender.

1.3 Research Motivation

It is important to ensure that a single RFID tag existence and multiple RFID tag coexistence are able to be detected by different kinds of RFID reader configurations by using the same network protocol. In our daily applications of RFID system, there might be a configuration of a single RFID tag being authenticated in multiple RFID readers field. Typically, such configuration can be seen when a single RFID tag information is interrogated by various readers for different purposes, in supply chain and manufacturing environment. Thus, it becomes a motivation of

this study to come out with a completed research work to ensure that network protocols have been developed by previous researchers for authenticating multiple RFID tags coexistence in a single RFID reader field are able as well applied for authenticating a single RFID tag existence in multiple RFID readers field.

In order to prove that tags dependent on each other's output network protocol causes a flaw when it is applied in multiple RFID readers field for authenticating a single RFID tag existence, some figures have been drawn to show their disability behaviour. With application of asymmetric cryptography, verifier needs to go through some difficult processes of solving factorize or complexity equations before it can view the actual data enlightening us on how to improve security performance during process of authentication data in RFID system. These two scenarios discussed above have motivated this study to provide a solution for solving security issues

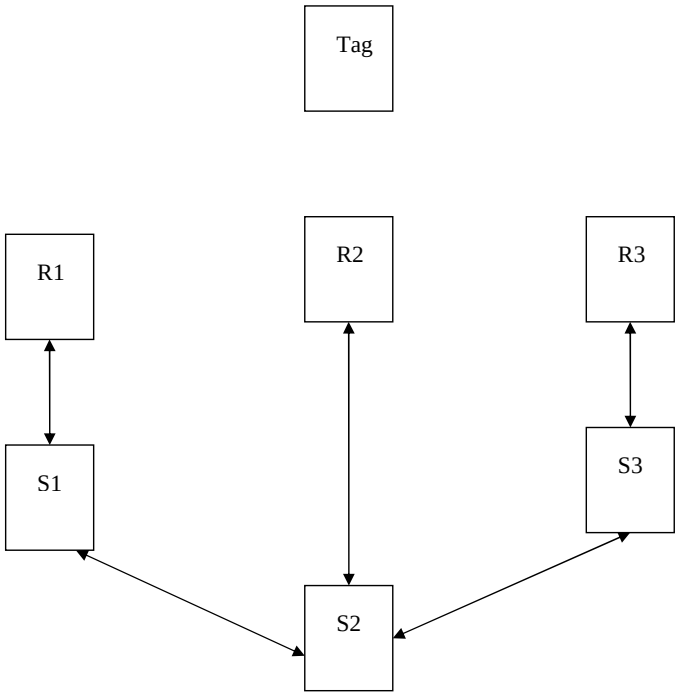

Figure 1.3: Topology of multi-propose RFID infrastructure

which occur on existing proofs and making a decision on type of network protocol being used for authentication in RFID system. Based on article [13], it stated that there is a possibility for

a single RFID tag being authenticated by various RFID readers for different purposes whereby the authentication process occurs at the same time or vice-versa. Hence, it is important to make sure that existing network protocols which are used to authenticate multiple RFID tag existence in a single RFID reader field can be used to authenticate a single RFID tag existence in multiple RFID reader field. In figure 1.3, it shows an example of topology for multi-propose RFID infrastructure which is used to authenticate information stored in a RFID tag by multiple RFID reader. RFID readers **R1**,**R2**,**R3** are used to read information stored in a RFID tag simultaneously while server **S1**,**S2** and **S2** are databases used to verify each information submitted by RFID readers **R1**,**R2**,**R3**. The configuration of RFID system in such manner is useful on application of issuing a visa to a citizen. When an individual wants to apply a visa from visa department, he or she just needs to stand in front of counter of application visa,counter of police department and counter of bank department by holding RFID tag to let RFID reader on each department checks the information contained in a RFID tag. The purpose of scanning information which contained in a RFID tag simultaneously by multiple RFID reader as mentioned on above scenario is to track a record on an individual before visa department proceed with issuing a visa to an individual. If an individual has a criminal record or bad financial record from police department or bank department, server from police department or bank department will directly send a record to server which is used on visa department. Thus, visa department

Table 1.1: Representative of each device in figure 1.3

Device	Department
RFID reader **R1**	Police
RFID reader **R2**	Visa
RFID reader **R3**	Bank
Server **S1**	Police
Server **S2**	Visa
Server **S3**	Bank

will not approve a visa applied by particular individual if there is any bad records provided by server from police department or bank department. With multiple RFID readers authenticating

information stored in a RFID tag, it facilitates visa department to track a record on an individual and expedites a process of approving a visa to a citizen.

1.4 Objectives of Research

The objectives of this research work are stated as follows:

- To unify network protocol used for authentication data in RFID system .
- To propose application of asymmetric cryptography such as elliptic curve cryptography for performing encryption and decryption data on RFID tag used for authentication.
- To compare security performance on applications of symmetric cryptography and asymmetric cryptography for authenticating data in RFID system.
- To describe on existing network protocols' characteristics which are used for generating multiple RFID tag coexistence proof.

1.5 Scope and Limitation

The research scope of this study is mainly focusing on network protocols which are used for generating multiple RFID tag coexistence proof. Two types of network protocol have been identified from this study being used for generating multiple RFID tag coexistence proof. Hence, these network protocols are tested for authenticating a single RFID tag existence in multiple RFID readers field in order to ensure that these two types of network protocol can be used in different kinds of RFID reader and RFID tag configurations for authenticating data purpose. Besides that, an application of asymmetric cryptography for performing encryption data on RFID tag requires a study and understanding on algorithms of asymmetric cryptography before it can be used on our proposed scheme. As a short summary, the scope of study for this

research work includes understanding of elliptic curve cryptography algorithm, understanding on each characteristic of existing network protocols which is used to generate multiple RFID tag coexistence proof and possibility of attacks encountered by RFID tag, RFID reader and server during data transmission over the air. However, this research work has its own limitation to perform development and enhancement. But, it is important to reveal the existing network protocols' ability in performing authentication in RFID system. This study is beneficial to those who are interested in designing of network protocol for communication and application of asymmetric cryptography for verification data in RFID system.

1.6 Organization of Thesis

The remainder of chapters are organized as follows:**Chapter 2**: Theoretical background and literature review on existing proofs,**Chapter 3**: Analysis and proposed scheme,**Chapter 4**: Discussion of security analysis and **Chapter 5**: Conclusion and future research.

CHAPTER 2

THEORETICAL BACKGROUND AND LITERATURE REVIEW FOR EXISTING PROOFS

Many types of development have been proposed by researchers for generating multiple RFID tag coexistence proof such as Yoking Proof [12], Grouping Proof [24], Modified Proof by S. Piramuthu [22], Ordinal Authentication Protocols for RFID Tags [16] and The Proof Proposed By Thiti et al [19]. In this chapter, we are going to review each of network protocols which has been developed for generating multiple RFID tag coexistence proof and theoretical background of these existing proofs. Before we are going to review each of the proofs, let's review RFID tag features at a glimpse.

2.1 Types of RFID tag

Nowadays, there are three main types of RFID tag available in market. The types are as follows:

- Passive RFID tag - Passive RFID tags have no internal power supply. However, a small electric current is created in the antenna when an incoming signal reaches it. This current provides enough power to briefly activate the tag, usually just long enough to relay simple information, such as an ID number or product name. Because passive RFID tags do not contain a power supply, they can be very small in size, sometimes thinner than a piece of paper. These tags can be activated from a distance of ten millimeters to over 6 meters away.

- Active RFID tag - Active RFID tags do contain an internal power source, which allows

for a longer read-range and for a bigger memory on the tag itself. The power source also makes it possible to store information sent by the transceiver. Active RFID tags are larger than passive tags, usually slightly bigger than a coin. They can be read from many meters away, and generally have a battery life of about ten years. Advantages of active tags include accuracy, reliability, and superior performance in adverse environments, such as damp or metallic.

- Semi-Passive RFID tag - The tag uses an internal power source to monitor environmental conditions, but it needs RF signal from RFID reader to power it up. Typically, an external power source is used to extend tag's signal strength and monitoring environmental condition such as temperature and shock. The rest of characteristics are similar with passive RFID tag.

Radio frequency which is used for communication in between RFID tag and RFID reader can be divided into four categories such as:

1. **Low frequency tags 125 or 134.2** kHz
2. **High frequency tags 13.56** MHz
3. **UHF 868 to 956** MHz
4. **Microwave tags 2.45** GHz

2.1.1 RFID Applications

There are wide applications of RFID system in different kinds of field. The examples are as follows:

- **Medical**: Tags are placed on prescription pill bottles for the visually impaired. A spe-

cial reader provides audible information on the name, instructions and warnings of the prescription.

- **Animal Identification**: Low frequency tags are implanted in animals, wild or domestic, which can be read to provide information such as gender, name, diseases etc. These tags also allow lost pets to be returned to their owners.

- **Tracking**: High frequency RFID tags are used to track library books, baggage, ID tags, warehouse inventory and even credit cards. American Express has a new service called Express Pay, featured on the American Express Blue credit card, which utilizes RFID technology.

- **Geology/Vulcanology**: RFID transceivers relay seismic information to specialized readers, greatly simplifying the collection of data.

- **Automotive**: Michelin has spearheaded a program to embed RFID tags in their tires. This will help track down problems should a recall have to be utilized. In addition, some Toyota and Lexus models feature a Smart Key option, which uses an active RFID tag to allow the driver to unlock doors and roll down windows without having to take the key out of their pocket.

2.1.2 Classes of RFID Tag

There are six classes of RFID tag available in market nowadays. The classes of RFID tag can be classified as Class 0,Class 1,Class 2,Class 3,Class 4 and Class 5. Each class has its own specific read and write capability. The descriptions on each type of classes are as follows:

- **Class 0** - Only can be used to be preprogrammed on passive tag and read only. Used in UHF band.

- **Class 1** - The tag can only be used to write once and read for many times. Used in UHF and HF band.
- **Class 2** - Passive RFID tag that can be used to read and write for many times.
- **Class 3** - The tag can be read and written on board sensor used to record parameters such as temperature,pressure, and motion. It can either be semipassive or active RFID tag.
- **Class 4** - Read and write active RFID tag with integrated transmitter. It can be used to communicate with other RFID tag and RFID reader.
- **Class 5** - It is similar to class 4 RFID tag, but it has additional function which is used to power up other RFID tag and RFID reader.

2.1.3 Using Elliptic Curves on RFID Tags

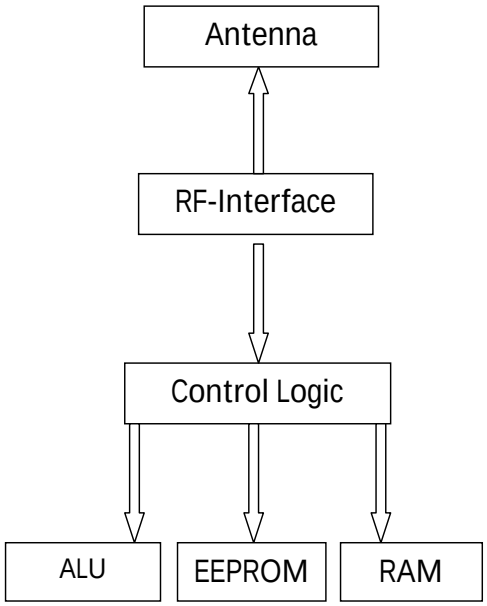

Figure 2.1: RFID Tag Architecture

Based on article [1], Siemens AG, Coporate Technology has introduced a RFID tag which uses Elliptic Curve cryptography for encrypting and decrypting data as shown in Figure 2.1. The architecture of RFID tag comprises control logic, read access memory (RAM), electri-

cally erasable programmable read only memory (EEPROM),arithmetic logic unit (ALU) and antenna. There is a simulation on gate count of the elliptic curve unit done by [1] in their research work, whereby they have implemented elliptic curve hardware in VHDL on Xilinx Spartan 3 FPGA. As a result of simulation, the synthesis tool had counted 18121 gates computed in different components on RFID tag. Nowadays, it is possible to use RFID tag which applies elliptic curve cryptography for performing encryption and decryption data to generate multiple RFID coexistence proof since Siemens has already invented it. Table 2.1 has shown that number of logic gates required in [1]'s design on RFID tag. According to [1]'s report, the tag requires only $64ms$ to perform scalar multiplication with a 163 scalar bits when a clock of $5MHz$ and an elliptic curve over the field GF(2^{163}) are used. Table 2.2 shows each component functionality on architecture of RFID tag designed by [1].

Table 2.1: Gate count of the elliptic curve unit [1]

Component	Gate equivalent
Arithmetic Unit	4548
Memory	11205
Control Logic	2368

Table 2.2: Function of each component on RFID tag designed by [1]

Component	Function
Arithmetic Unit	computes additions and multiplications in the finite field over which the elliptic curve is defined
Control Logic	implements the scalar multiplication of points on the elliptic curve and the cryptographic protocol of the application
Memory	contains volatile intermediate results of the point arithmetic and non-volatile system parameters and keys

2.2 Theoretical Background for Generating Multiple RFID Tag Coexistence Proof

Basically, the process of generating multiple RFID tag coexistence proof involves a server, RFID reader and a group of RFID tags. The main function of server or verifier is to generate a random number or timestamp to a group of RFID tags and verify hash value and message authentication code submitted by RFID reader. Meanwhile, RFID reader is used as a medium to transmit random number or timestamp received from server to a group of RFID tags. Besides that, RFID reader is applied to read hash value and message authentication code generated by each of RFID tags. Once RFID reader has read all hash values and message authentication code values generated by its surrounding RFID tags, it will submit collected parameters to server for verification. Each of RFID tags applies random number or timestamp generated by server as one of the inputs to generate hash value and message authentication code value. There are two main theoretical cryptography applications involved for generating multiple RFID tag coexistence proof which include hash function and message authentication code. Hash function is applied for converting large bits of random number sent out by server to a fixed size of hash value. If adversary tries to change or modify the data during its transmission in the air, it would cause the hash value to change. Hence, server or verifier is able to detect the hash value's status when it has been tempered or modified by an adversary. On the other hand, message authentication code is used to authenticate the message that has been compressed to fixed size of data. Once a large bits of random number being sent out by server, RFID reader and RFID tag will apply hash function to compress that particular block of random number becoming a fixed size of data or known as hash value. Next, the hash value will be computed into MAC function for generating a short piece of information which is known as MAC value and it will be sent for authentication.

2.3 Cryptography Hash Function

A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, cryptographic hash value, such that an accidental or intentional change to the data will change the hash value [5]. The data to be encoded is often called the "message", and the hash value is called message digest or simply digest [5].

The ideal cryptographic hash function has four main properties:

- it is easy to compute the hash value for any given message
- it is infeasible to find a message that has a given hash
- it is infeasible to modify a message without changing its hash
- it is infeasible to find two different messages with the same hash

Existing multiple RFID tag coexistence proofs apply hash function to generate hash value with a random number sent out by server as an input. Each of RFID tags applies different secret key for encrypting the plain text. The purpose of hash function being used in multiple RFID tag coexistence proof is to fix of random number size and prevent actual data reveal by adversary [21]. Previous researchers have chosen hash function for encrypting data because it is able to withstand all known types of cryptanalytic attack. A strong cryptographic hash function must constitute at least three minimum properties:

- **Preimage resistance**: Given a hash h it should be hard to find any message m such that h = hash (m). This concept is related to that of one way function. Functions that lack this property are vulnerable to preimage attacks [5].
- **Second preimage resistance**: Given an input m_1, it should be hard to find another input,

m_2 (not equal to m_1) such that hash (m_1) = hash (m_2). This property is sometimes referred to as weak collision resistance. Functions that lack this property are vulnerable to second preimage attacks [5].

- **Collision resistance**: It should be hard to find two different messages m_1 and m_2 such that hash (m_1) = hash (m_2). Such a pair is called a (cryptographic) hash collision, and this property is sometimes referred to as strong collision resistance. It requires a hash value at least twice as long as what is required for preimage-resistance, otherwise collisions may be found by a birthday attack [5].

2.4 Message Authentication Code (MAC)

In cryptography, a message authentication code is a short piece of information used to authenticate a message [23]. A MAC algorithm, sometimes it is being called a keyed (cryptography) hash function, accepted as input a secret key and an arbitrary length message to be authenticated, and output a MAC (sometimes known as a tag)[23]. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes on message content. MAC value is generated and verified by using same secret key [26]. Hence, sender and receiver must agree on the same secret key before they can initiate a communication [26]. Existing multiple RFID tag coexistence proofs apply message authentication code MAC as a short piece of information for verifying hash value. The server shares the same secret key with authorized RFID tags and applies it for regenerating and verifying hash value and MAC value received from RFID tags. Figure 2.2 shows that how MAC value is generated and authenticated by server. Besides that, it also shows that sender and receiver possess the same secret key for encrypting and decrypting data. Once the process of key agreement in between sender and receiver is successful,sender starts to compute a message into MAC function for generating MAC value with application of a secret key. Af-

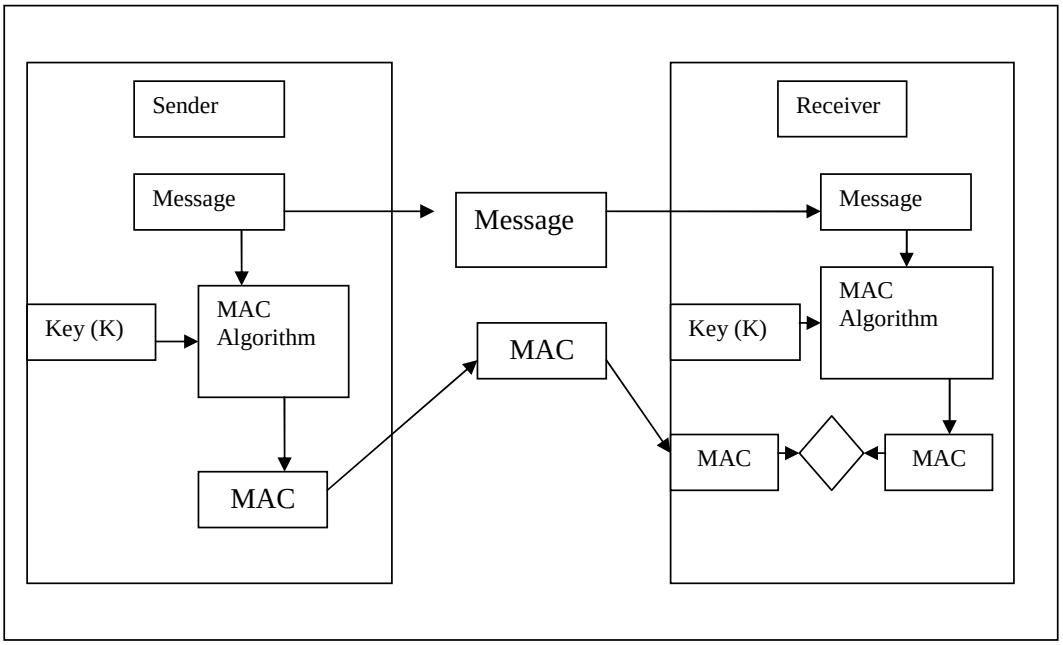

Figure 2.2: Example of how MAC value is generated and authenticated

ter MAC value is generated, sender will forward the MAC value to receiver. When receiver receives the message and MAC value generated by sender, it will apply MAC function, received message and its secret key to regenerate that particular MAC value again before making a comparison to determine its validity.

2.5 Symmetric Cryptography

The general idea on how symmetric cryptography works is sender and receiver each has the same secret key for authentication before it is used for performing encryption data. All existing of multiple RFID tag coexistence proofs are applied hash function to generate fixed size of data, while applying MAC function for generating a short piece of information with hash value as one of the inputs. When symmetric cryptography is used for generating multiple RFID tag coexistence proof, server possess all secret keys (x_a,x_b,x_c,x_d) which belonged to authorized RFID tags. The purpose of symmetric cryptography being applied for generating multiple RFID tag coexistence proof is to ensure that only authorized RFID tag can generate a similar MAC value and hash value with server [26]. With the application of symmetric cryptography, server will

be able to detect data which submitted by unauthorized RFID tag [10]. But there is a disadvantage when applying symmetric cryptography for performing encryption and verification data because the secret key is easily eavesdropped by an adversary during secret key agreement process in between sender and receiver. Thus, asymmetric cryptography has been proposed to replace symmetric cryptography via this research work for resolving security issues that exist on existing multiple RFID tag coexistence proof. Anyhow, there is one advantage of using symmetric cryptography whereby it only requires small length of secret key to store in RFID tag which makes the process of encryption faster compared with application of asymmetric cryptography.

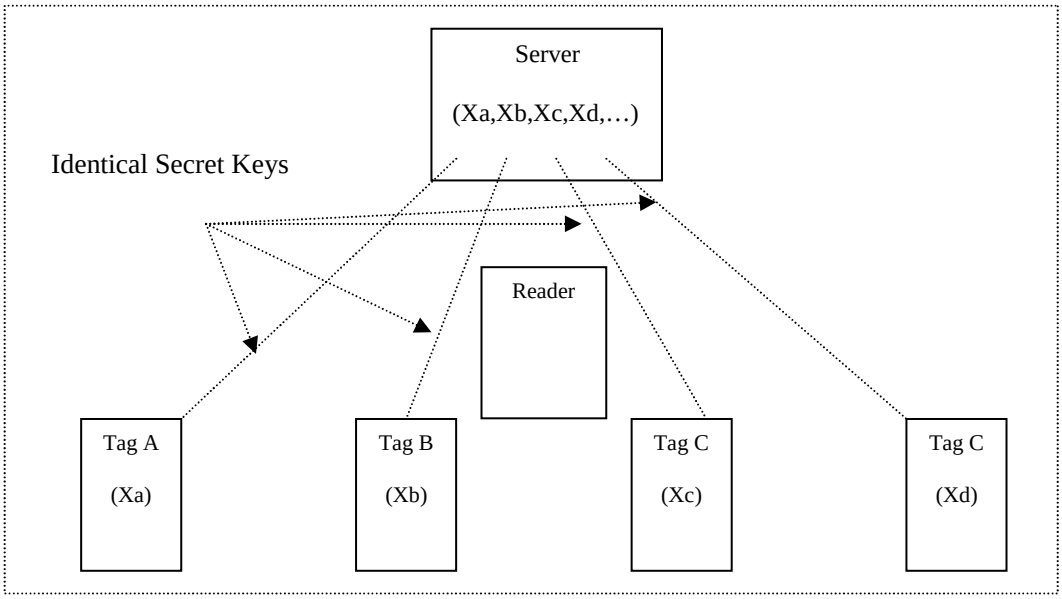

Figure 2.3: Symmetric cryptography

2.6 Asymmetric Cryptography

Figure 2.4 shows a brief idea on how asymmetric cryptography can be applied for performing encryption and decryption data on RFID tag and RFID reader, and the way on how it works. Each of RFID tags (A, B, C, D) applies public key (E) for encrypting random number

or timestamp sent by server, while server applying its private key (P_s) for decrypting cipher texts generated by RFID tags. Besides that,server applies all public keys which submitted by RFID tags (E_A,E_B,E_C,E_D) for verifying each of RFID tag's digital signatures. Even though symmetric cryptography consumes less computing power, in terms of security performance, asymmetric cryptography is more reliable because an adversary cannot directly apply public key that it receives from server to construct a cipher text and submitted for verification. Hence, it is very hard for an adversary to forge the data or act as an authorized verifier because only sender knows its own private key, and it is impossible for any other devices to forge the private key from sender [8]. There are few types of asymmetric cryptography methods that have been introduced to date such as RSA cryptosystem, Rabin cryptosystem, ElGamal cryptosystem and Eliptic Curve cryptosystem. RSA algorithm is based on difficulty to factor a large integer composed of two or more large prime numbers, while Rabin crytosystem deals with quadratic congruence whereby decryption of the message is infeasible if two private keys are unknown. ElGamal cryptography is based on difficulty to solve discrete algorithm while elliptic curve cryptography is based on difficulty of solving elliptic curve logarithm problem [27]. Basically, RSA and Rabin cryptosystem require at least 1024 bits of secret key to achieve same security level with symmetric cryptography which uses only 80 bits of secret key. On the other hand, Elliptic Curve cryptography requires only 160 bits of secret key to achieve same security level with RSA, Rabin cryptosystem and symmetric cryptography. Based on Table 2.3, we can

Table 2.3: Key sizes in bits for equivalent levels [20]

Symmetric Key Size	Security (bits)				
	80	112	128	192	256
RSA	1024	2048	3072	8192	15360
ECC	160	224	256	384	512

conclude that elliptic curve cryptography is suitable to use for authentication event in multiple RFID tag coexistence scenario because it only requires 160 bits of secret key to perform en-

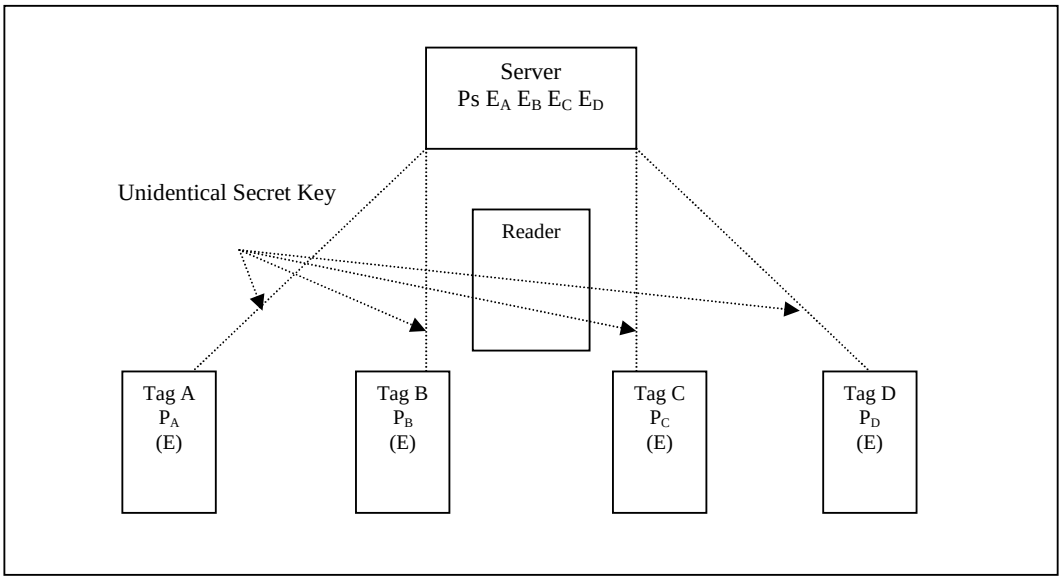

Figure 2.4: Asymmetric cryptography

cryption and decryption data on RFID tag and RFID reader. Nowadays, Siemens Technology has manufactured RFID tag which uses asymmetric cryptography to operate. Hence, it is possible to apply asymmetric cryptography in performing authentication in RFID system provided that the users are willing to pay more. In order to prove that there is a possibility to implement elliptic curve cryptography on passive RFID tag, a table of synthesis result and performance prepared by [17] is shown below. Based on information provided in table 2.4, if elliptic curve

Table 2.4: Synthesis result and performance [17]

PKC	Area(gates)	Freq(KHz)	Perf(msec)	Power(μW)
ECC GF(2^{163})	12506	1,130	244.08	36.63
	14064	590	245.49	21.55
	14729	411	246.19	15.75
	15356	323	243.17	12.08

cryptography is implemented on RFID tag by using CMOS 0.13 μm technology, there will be less logic gates are required for running the operations of general modular operation and point multiplication compared with the work proposed by [1]. The research work done by [17] has helped to reduce the number of logic gates applied for operating elliptic curve cryptography. The specifications of RFID tag and RFID reader being used for this research work are as

follows:

- Number of Logic Gates - 12506
- Operating Frequency - 1,130 KHz
- Power consumption - 36.63 μw
- Class 2 of RFID tag

The reason that we select CMOS 0.13 μm technology proposed by [17] for operating elliptic curve cryptography is because less of logic gates are required and it is suitable to apply on low cost RFID tag which operates in low frequency. Besides that, Class 2 of RFID tag being used is to allow user to program and erase the information of secret key when there is a need to change the secret key stored in RFID tag.

2.6.1 Diffie-Hellman key exchange for elliptic curves cryptography

In application of asymmetric cryptography, prior sender and receiver can use each other's public key to perform encryption and decryption data, there will be a key agreement process needed to go through by sender and receiver. Below are small examples on the process of how key agreement for elliptic curve is achieved between sender and receiver. This example is picked up from [6].

- Alice and Bob agree on an elliptic curve E over a finite field F_q so the discrete logarithm problem is hard in E(F_q).
- They also agree on a point $P \in$ E(F_q) such that the subgroup generated by P has large order (usually prime).
- Alice chooses secret integer, a, computes $P_a = a$P and sends P_a to Bob.

- Bob chooses secret integer, b, computes $P_b = b\mathrm{P}$ and sends P_b to Alice.
- Alice computes a$P_b = ab\mathrm{P}$. Bob computes $bP_a = ab\mathrm{P}$.
- Alice and Bob agree on a method to extract a key from $ab\mathrm{P}$.
- In order to break the encryption, eavesdropper needs to know secret keys (a,b) which belonged to Alice and Bob. Therefore, eavesdropper needs to solve Diffie-Hellman problem for elliptic curves.

2.6.2 Theory of Elliptic Curve Cryptography

Basically, authentication event in RFID system requires secure and privacy channel to avoid adversary attack. But, with an application of symmetric cryptography it doesn't achieve the security level that asymmetric cryptography can perform. Hence, we have proposed application of asymmetric cryptography to generate cipher text in multiple RFID tag coexistence proof instead of using symmetric cryptography. Anyhow, in view of RFID tag has limitation of capacity to store a data, a proper review on which type of asymmetric cryptography is suitable to be used on RFID tag is one of the necessities to ensure that number of logic gates implemented on RFID tag are comparable with number of secret key bits being used. Among the four types of asymmetric cryptography,elliptic curve cryptography is identified as the most suitable to be used as algorithm for encryption and decryption data on wireless communication devices due to it applies smaller amounts length of secret key compared to others asymmetric cryptography. Some descriptions of elliptic curve algorithm are as follows:

- Elliptic curve cryptography involves elliptic curves over a finite field. There are two types of field such as prime fields GF(p) and binary finite fields GF(2^m).