A Thesis for the Degree of Master

A Lightweight Authentication Protocol using Integer Arithmetic for low-cost RFID tags

Min-Hea Kwak

School of Engineering

Information and Communications University

2009

A Lightweight Authentication Protocol using Integer Arithmetic for low-cost RFID tags

A Lightweight Authentication Protocol using Integer Arithmetic for low-cost RFID tags

Advisor : Professor Kwangjo Kim

by

Min-Hea Kwak

School of Engineering
Information and Communications University

A thesis submitted to the faculty of Information and Communications University in partial fulfillment of the requirements for the degree of Master of Science in the School of Engineering

Daejeon, Korea
December 16, 2008
Approved by

Professor Kwangjo Kim
Major Advisor

A Lightweight Authentication Protocol using Integer Arithmetic for low-cost RFID tags

Min-Hea Kwak

We certify that this work has passed the scholastic standards required by the Information and Communications University as a thesis for the degree of Master

December 16, 2008

Approved:

Chairman of the Committee
Kwangjo Kim, Professor
School of Engineering

Committee Member
Young-Hee Lee, Assistant Professor
School of Engineering

Committee Member
Doo-Ho Choi, Ph.D
ETRI

M.S. Min-Hea Kwak
20072006

A Lightweight Authentication Protocol using Integer Arithmetic for low-cost RFID tags

School of Engineering, 2009, 39p.
Major Advisor : Professor Kwangjo Kim.
Text in English

Abstract

The cost of the tag is one of the important factors to their proliferation. Designing a secure and efficient light-weight authentication protocol is imperative for resisting against all feasible attacks. In general, the low-cost tag is difficult to implement the traditional public key cryptosystem since the tag's limited storage capacity(25-3K storage and 5-10K logic gates). Over the past years, several streams of research have emerged to resolve the RFID authentication security problem from different perspectives. Most of the previous light-weight RFID authentication protocols based on random number generator, Cyclic Redundancy Code(CRC) or bitwise operations (e.g., XOR, AND and OR)are vulnerable to both passive and active attacks [32, 31]. For instance, anyone can obtain the tag identity and secret key through the consecutive eavesdropping.[12]

In this paper, we propose a light-weight and secure authentication protocol that enhances Stephane *et al.*'s [24] protocol based on a random number generator and abstract of integer arithmetic (AIA), which generates secret key pool from the subset of the remainders and the carries of the integer multiplication.

We assume that the tag and the reader share the same secret K, AIA. Two parties then perform specific integer arithmetic to make message using their own K_i and AIA_i. Then, both parties convince that they share same secret key from exchanging their messages. We consider two different situation as the state of the authentication session, authentication terminates normally or not. Then, if the desynchronization between the tag and the reader occurs, the tag recovers the key, it was before.

Every tag is designed with a unique set of logic gates to perform the message computation so that our protocol strong to cloning attack as well as man-in-the-middle attack. Furthermore, Security properties such as man-in-the-middle attack, forgery attack, replay attack and de-synchronization, appear to be satisfied.

We compare our protocol with Stephane *et al.*'s scheme in terms of the storage, computation and communication requirements of both the reader and the tag. The most severe of the restrictions of the passive tag are the small number of logic gates(200-2000) which can be devoted to security functions, and the volatile memory available(32-128) to store intermediate calculations. Our protocol satisfies EPCglobal class-1 Gen-2 specification as well as security primitives. For the tags, $2(n+p)\log_2(b)+2$ bit for K_i,N_i, M_i and *flag*, and $(4b^2-b)\log_2(b!)$ bit of ROM to store AIA are needed. In addition, we reduce the computation and communication cost, $\frac{3}{2}(np)$ plus $(n+1)(p-1)+\frac{np}{2}$ and 4 times respectively. While requiring only 82 bit of RAM, 20 bit of ROM and 300-400 logic gates, our protocol can satisfy security requirements for RFID system. In conclusion, Our protocol may be scaled to provide a high level of security, using relatively little computational resources and be good alternative of the previous schemes based on bitwise operation.

Contents

List of Figures

List of Tables

List of Notations

$\mathcal{T}$ An RFID tag

$\mathcal{R}$ An RFID reader

$\mathcal{S}$ An Server

$\mathcal{A}$ An aversary

AIA Abstraction of Integer Arithmetic

I. Introduction

1.1 Motivation and Objectives

Radio Frequency Identification (RFID) refers to technologies and systems that use wireless radio signal to transmit data and uniquely identify objects. RFID transponder or tag consists of a chip and an antenna to identify and track the target object that is involved in RFID technology and system. The tag is classified into three types according to the ability of the power and the capacity : passive, semi-passive and active tags. The passive tag can only store 250-3K bit and 5K-10K logic gates which are used to implement security function. The system employing RFID tags used for various industries (*e.g.*, distribution, logistics, medical attendance and education service) instead of barcodes is emerging one of the most pervasive computing technologies.

Although the advantages of the RFID(*e.g.*, portable database, no line of sight, multiple tag read/write and traceability), RFID still has unsolved problems in security and privacy aspects. Since most existing RFID systems are not complete and leak information about the attached object, an adversary can trace the goods or customers silently. Some common types of attacks on RFID system include eavesdropping, replay attack, man-in-the-middle attack, denial of service (DoS), forgery (including skimming and cloning) and physical attack. Many researchers proposed the RFID authentication schemes to address these security issues.

As low-cost RFID becomes more and more popular, designing a secure and efficient light-weight authentication protocol is imperative for resist against all feasible attacks. Therefore, light-weight protocols only support simple operation such as a Pseudo Random Number Generator (PRNG), Cyclic Redundancy Code(CRC) checksum or bit-wise

operation(*e.g.*, XOR, AND and OR) are appeared. However, most of the previous light-weight RFID authentication protocols are vulnerable to active attacks; some researchers reported the weakness on previous light-weight and ultra light-weight schemes[31, 32].

1.2 Contributions

The novel contributions of this thesis are as follows :
· Technological trends on RFID :
We begin with a comprehensive survey of the state of the art concerning with RFID technology: RFID systems, standards related to RFID technology and a comprehensive study of the security requirements for RFID systems in Chapter 2; Then, we present security vulnerabilities in the previous light-weight protocols reported by other researchers as well as new ones in Chapter 3. Finally, we introduce the Abstraction Integer Arithmetic (AIA) concept proposed by Stephane *et al.* in Chapter 4.
· Lightweight cryptography for low-cost tags :
An important part of our research is that designing a lightweight cryptograhy to resist against passive and active attacks. We propose a more efficient and alternative light-weight and secure authentication protocol that improves Stephane *et al.*'s [12] protocol based on a random number generator and AIA, which generates secret key pool from the subset of the remainders and the carries of the integer multiplication.

1.3 Organization

This thesis is organized as follows:
In Chapter 2, RFID system is introduced. First, an overview of RFID system(components and technological trends) is given. Secondly, standards related to RFID technology are briefly described. Then, privacy

and security issues are described in detail with the kind of attacks that RFID systems can be pestered. In addition, performance evaluation factors are outlined. Chapter 3 presents an review of the previous light-weight solutions; the cryptanalysis of the recently proposed and improved lightweight and ultralightweight protocol. Chapter 4 introduces an algebraic structure which this term is usually denoted as AIA, and illustrate how to represent AIA as a short binary string. Chapter 5 introduces the our main proposal as a solution to the security issues discussed in Chapter 3. In Chapter 6, we evaluate our novel authentication protocol in terms of security and efficiency under the EPC Class-1 Gen-2 specification. Chapter 7 conclude with summary of our protocol was drawn in the previous chapters in the thesis.

II. RFID System

2.1 Overview of RFID system

At the moment, barcodes is one of the the most promising identification systems. However, recently, RFID systems substitutes for barcodes and magnetic cards. RFID system composed of RF readers or transceivers, RF tags or transponders and backend server. The reader broadcasts an wireless radio freqeuncy signal(wireless) to access resistant data stored in the tags. RFID gives several advantages over barcodes; the reader access the data on the multiple tags at the same time, and reads or writes automatically with no line of sight at a rate of a hundred times per second.

RFID systems are become more valuable technology in various industries such as distribution, logistics, medical attendance, education service and manufacturing. Security and cost issues of RFID systems is major barrier to their proliferation. Nowday, most RFID tags are passive, however, typical passive tag can only store hundreds of bit which used to implement security functions, and may communicate within a few meters radius

However, traditional cryptosystems such as the Advanced Encryption standard(AES) needs between 20K and 30K gates. Taking into account power ability of the passive tags, nor system can be expected to perform the classical cryptography securely.

Despite all these limitations, the use of RFID technology is increasing steadily. Thus, we expect that RFID system will completely replace classical barcodes finally.

RFID system is currently used to various industries [37] :

· Wal-Mart applies RFID technology to their supply chains.
· Delta Airlines is testing to RFID tags for luggage control.
· The European Central Bank is planning to attach RFID tag into bank note.
· EZ-pass is accepted for contactless payment of tolls on the toll roads.
However, the use of RFID technology is confronted by certain organizations like Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) are strongly against that corporate uses RFID technology.

2.2 RFID standards

RFID system has no unitary standard. RFID standard generally involves the specification of the physical and the link layers, covering several aspects such as the communication protocols, air interface, anticollision mechanisms and security functions. Nonetheless, not every factor is well covered; some standardizations has a certain absence in protocols and application interfaces.
Many organizations are building standards around existing ones developed by the ISO/IEC, and then improve or modify them to meet the needs of their particular application or design.
The International Organization for Standardization (ISO) is the world's leading developer of international standards. ISO technical standards specify the requirements for processes, products, materials, service and systems. ISO also developed standards for managerial, organizational practices and conformity assessment.
The International Electrotechnical Commission (IEC) is a leading global organization that publishes and prepares international standards for all electric and related technologies. The IEC promotes international cooperation on electrotechnical standardization, such as the conformity

assessment to standards in the fields of electronics, electricity and related technologies such as RFID.
The EPCglobal is leading the development of industry-driven RFID standardization as a joint venture between the EAN International and the Uniform Code Council (UCC). EPCglobal is centered on establishing and supporting the Electronic Product Code (EPC) Network as the global specification and leading to the global worldwide standard (ISO) for automatic, immediate and accurate identification of goods in the supply chain. EPCglobal has become the major organization for the development of RFID specifications.

2.3 Requirements for RFID protocol

2.3.1 Privacy

We introduce following privacy issues should be addressed to guarantee the secure communication between $\mathcal{R}$ and $\mathcal{T}$. Threats on RFID system can be exploited to bypass the authentication or extract private information illegally. Typically, RFID systems use a unsecure radio channel between $\mathcal{R}$ and $\mathcal{T}$ so that their information about $\mathcal{T}$ and $\mathcal{R}$ (*e.g.*, identity or secret key) can be revealed, or $\mathcal{T}$ can be traced. We identify major privacy concerns.
· Information leakage : When $\mathcal{R}$ queries $\mathcal{T}$, $\mathcal{T}$ sends $\mathcal{T}$ identifier as answering to $\mathcal{R}$. Then, $\mathcal{R}$ can demand further details to $\mathcal{S}$ by sending $\mathcal{T}$'s identifier. If illegal $\mathcal{R}$ gets $\mathcal{T}$ identifier, then $\mathcal{A}$ may be able to identify the additional secret information of $\mathcal{T}$. For example, if the information associated with $\mathcal{T}$ attached to ID-card or a passport could be obtained by forgery $\mathcal{R}$, then personal information of $\mathcal{T}$ owner can be leaked out; it would be very serious. If RFID systems allow only authorized $\mathcal{R}$ is able to access the data associated to $\mathcal{T}$, they may protect against infor-

mation hijacking.
· Tag tracking : Each $\mathcal{T}$ has a unique and distinguishable identifier. If $\mathcal{T}$ replies identifier to $\mathcal{R}$, then the location of $\mathcal{T}$ could be traced by linkable $\mathcal{R}$. For instance, if the $\mathcal{T}$ reply their static identifier to $\mathcal{R}$, then the movement or social interaction with neighboring $\mathcal{T}$ can be monitored by third parties silently. Or, if $\mathcal{T}$ has a special identifier is distinguishable from other $\mathcal{T}$, $\mathcal{A}$ can trace $\mathcal{T}$ by active querying or consecutive eavesdropping; then $\mathcal{T}$ owner's privacy will be badly damaged. To avoid tracking problem, $\mathcal{T}$ identifier or messages should be anonymous.

2.3.2 Security

Security threats on RFID system can be classified into passive and active attacks. Passive attacks are feasible just by monitoring and manipulating communications between $\mathcal{R}$ and $\mathcal{T}$.
· Eavesdropping: $\mathcal{A}$ only observes and records communications between $\mathcal{T}$ and $\mathcal{R}$.
· Man-in-the-Middle Attack : If $\mathcal{A}$ plays as a legitimate $\mathcal{T}$ or $\mathcal{R}$, they can actively drop, insert or replay a message in communication and authentication between $\mathcal{T}$ and $\mathcal{R}$. This attack include impersonation and spoofing attacks.
· Tag Impersonation : If $\mathcal{A}$ impersonates $\mathcal{T}$ without secret information of $\mathcal{T}$, they could communicate with $\mathcal{R}$ as a valid $\mathcal{T}$ and then authenticate.
· Server Impersonation : If $\mathcal{A}$ knows the internal information of $\mathcal{T}$, then $\mathcal{A}$ could impersonate the valid $\mathcal{S}$ to $\mathcal{T}$. For example, if $\mathcal{A}$ impersonates $\mathcal{S}$, $\mathcal{A}$ could demand that $\mathcal{T}$ updates their shared information. Then, real $\mathcal{S}$ would be desynchronized and fail to no longer successful authentication. This attack could be a genuine threat.
· Tag Tampering : $\mathcal{A}$ accesses internal information of $\mathcal{T}$ without au-

thorization after bypassing authentication. If $\mathcal{T}$ does not have proper tmaper-resistant mechanism, $\mathcal{A}$ could access $\mathcal{T}$ and change the data in the $\mathcal{T}$. Ultimately, $\mathcal{A}$ can read from or writes to $\mathcal{T}$.

· Replay Attack: $\mathcal{A}$ can capture a message transmitted from previous sessions and retransmit it to $\mathcal{T}$ to perform a successful authentication.

· DoS attack : $\mathcal{A}$ disturbs the communication between $\mathcal{R}$ and $\mathcal{T}$ by intercepting or blocking messages transmitted. DoS attack could cause desynchronization between $\mathcal{S}$ and $\mathcal{T}$. For example, While $\mathcal{T}$ might update the shared key or identifier, $\mathcal{S}$ does not; they would no more be able to authenticate procedure each other due to their different data. These threats are feasible for $\mathcal{A}$ which has compromised a target $\mathcal{T}$. The memory of a low-cost $\mathcal{T}$ is not tamper-resistant, and hence $\mathcal{T}$'s internal data are liable to be exposed by physical attacks. Thus addressing such attacks is essential for the security of RFID schemes.

· Desynchronization : Typically, $\mathcal{R}$ and $\mathcal{T}$ update the their identificaiton information before the authentication terminates. If $\mathcal{A}$ can desynchronize the identification information between the $\mathcal{T}$ and $\mathcal{S}$, after all, $\mathcal{S}$ no longer make $\mathcal{T}$ identifiable.

· Backward Traceability : $\mathcal{A}$ extracts the identify of the target $\mathcal{T}$ interaction that occurred at previous authentication session using given all the current internal state of a target $\mathcal{T}$. That is, current internal state of $\mathcal{T}$ could help identify past interactions of $\mathcal{T}$ as a clue, then, $\mathcal{T}$ may allow $\mathcal{T}$ owner's past behavior are traced.

· Forward Traceability : This attack is similar backward traceability defined above; difference between backward and forward traceability is that threat to past and future anonymity. $\mathcal{A}$ extracts the identify of the target $\mathcal{T}$ interaction that will occur at next authentication session using given all the current internal state of a target $\mathcal{T}$. This attack related to ownership of $\mathcal{T}$; if an authentication protocol does not guarantee forward and backward untraceability, the ownership of $\mathcal{T}$ is transferred

and $\mathcal{A}$ might be able to access communications between the new and old owner and $\mathcal{T}$.
· Cloning attack: If $\mathcal{T}$ is not protected with Physical Unclonable Function (PUF), $\mathcal{A}$ can physically clone an identical copy of RF chip on $\mathcal{T}$.
· ID Exposure: When $\mathcal{R}$ queries to $\mathcal{T}$ or eavesdrops communication between $\mathcal{R}$ and $\mathcal{T}$, $\mathcal{A}$ can expose the identity of $\mathcal{T}$.
· Physical attack: Typically, $\mathcal{T}$ can be faked physically in laboratory. For example, attacks such as probe attack, circuit disruption, shaped charge appeared. However, RFID system barely prepare no countermeasure.

2.3.3 Performance

General passive tag cannot use high computational cryptographic function for privacy and security since ability (storage capacity and processing power)of the low-cost $\mathcal{T}$ are limited.
· Computation : Computation cost of $\mathcal{T}$ should be minimized; $\mathcal{T}$ has very limited power resources to compute messages.
· Capacity : $\mathcal{T}$ should store a minimum volume of data; $\mathcal{T}$ has a very limited size of $\mathcal{T}$ memory.
· Communication : $\mathcal{R}$ and $\mathcal{T}$ consider communication traffic; $\mathcal{T}$'s transmission data per second is restricted by available bandwidth of $\mathcal{T}$.
· Scalability: RFID system communicates multiple $\mathcal{T}$ over the same radio channel. Therefore, the amount of work in $\mathcal{S}$ can be increasing as the number of $\mathcal{T}$ should be handling. When $\mathcal{T}$ population is large, $\mathcal{S}$ is difficult to performs an exhaustive search which identify individual $\mathcal{T}$.

III. Related Work

3.1 Introduction

We can classify previous RFID authentication protocols into four types: Full-fledged, Simple, Light-weight and Ultra light-weight.

The protocols [1, 2] belonging to the full-fledged class support classical cryptography like hash function, modular arithmetic(RSA and DSS), elliptic curves and even public key algorithms on the tags. Juel *et al.*[1] raised concerns as to whether data on the chip embedded in an e-passport could be collected by means of "skimming" or "eavesdropping".

The tags in the protocols of the simple class should support hash and pseudo random number functions but not traditional cryptographic function such as public key cryptography. Examples are like [4, 5], where Molnar and Wagner [4] proposed a tree based scheme in which a tag contains not one symmetric key, but multiple keys in a hierarchical structure defined by the tree S. The basic idea in [5] is to modify the identifier each time so that the tag is recognized by authorized parties only. Avoine *et al.* [15] reported the replay attack and the unscalability of Ohkubo *et al.*'s scheme [5].

The third class called light-weight refers to those protocols [4, 5] that do not require hashing function on the tags. Some researchers present the hash based protocol [13, 14] as the light-weight protocol, but current cryptographic hash functions is difficult to implemented on the passive tag. The EPCglobal also announced Class-1 Gen-2 RFID tag only [25] supports Cyclic Redundancy Code (CRC)checksum and PRNG but not hash function. Juels [16] proposed a challenge-response protocol using short pseudonym list in the tags. Chien and Chen [18] reported the

DOS attack, replay attack, tracking attack and spoofing tag problem on the scheme [17], which based on simple XOR and matrix operations, where matrices M1 and M2 are stored on each tag and the reader as the shared secret key, designed an efficient tag identification and the reader authentication scheme for GEN-2 RFID. The HB-series [19, 21, 22] can also be classified into this class, since they demand the support of random number generator but not hash function on the tags. Hopper and Blum [19] first introduced the Human-Computer protocol based on the Learning Parity with Noise (LPN) problem. Later, the HB protocol was attacked and improved by its sister works [21, 22]. Actually, the HB-series only considered the authentication on the tag side but not the reader. These protocols considered as uncompleted solutions. HB series ignored the security issues on the readers which lead the anonymity and tracking problem on the tags.

Currently, Peris-Lopez *et al.* proposed a series of ultra-lightweight authentication protocols [9, 10, 11] where the tags involve only simple bit-wise operations like XOR, AND, OR and addition mod 2^m. These schemes are very efficient that only require about 300-400 gates. Unfortunately, some researchers[31, 32] reported the desynchronization attack and the full-disclosure attack on these protocols and sister works. The previous ultra light-weight schemes [9, 10, 11, 12] only provide weak authentication and integrity protection, which make them vulnerable to both passive and active attacks. Most of the light-weight and the ultra lightweight protocols based on PRNG, CRC or bitwise operations are obivously efficient but has fundamental security flaws that an adversary can reveal the tag's identity and even the security key throught consecutive eavesdropping.

3.2 Light-weight Authentications

3.2.1 List of Pseudonyms

Juels[7] proposed a solution based on the use of pseudonyms, without hash functions at all. The tag stores a short list of random identifiers or pseudonyms $(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k)$. When the tag is queried, it emits the next pseudonym in the list. An adversary can, however, collect all pseudonyms on the list by querying the tag multiple times. Then the attacker could impersonate the valid tag. This is a kind of cloning attack for standard tags with static identifiers.

To prevent such an attack, some solutions were proposed later: The tags could release their name only at a certain prescribed rate, or pseudonyms could be refreshed only by authorized the readers. Juels proposed a lightweight mutual authentication protocol based on the release of keys shared between both parties. The verifier authenticates to the tag by releasing a key β_i, which is unique to a pseudonym α_i. Once the verifier has authenticated to the tag, the tag authenticates itself to the reader by releasing an authentication key i. Like β_i, this authentication key i is unique to a pseudonym α_i. After mutual authentication, key (β_i, i) and pseudonym (α_i) updating is accomplished. The reader transmits one-time padding data that the tag uses in the updating stage. Although encryption is not explicitly involved by means of one-time pads, it is equivalent to encryption. Pads can be considered keys used to "encrypt" and thereby update the α_i, β_i and i values. Indeed, each tag stores a series of pads. The stored pads are updated with new material on each authentication. This new pad material is sent in clear on the channel, but the updating procedure ensures that it will be used only after a certain number, m, of updates. This number should be chosen such that an adversary cannot observe m consecutive authentications.

As it has been shown, Juels's protocol requires the use of non cryptographic primitive. However, it involves the exchange of four messages and needs key updating, which may be costly and difficult to perform securely. Moreover, the assumption that an attacker can not observe m consecutive authentications does not hold in many real scenarios.

3.2.2 Human Protocol

In [27], Weis introduced the concept of human-computer authentication protocols, adapted to low-cost RFID tags. The security of the proposed protocol is rooted in the Learning Parity with Noise Problem, whose hardness over random instances still remains an open question. Suppose that the reader and the tag share a k-bit secret x, and the tag would like to authenticate itself to the reader. The reader selects a random challenge a $\in (0,1)^k$ and sends it to the tag. The tag responds to the reader challenge by computing the binary inner-product $a \cdot x$ and injecting noise into the result. The tag intentionally sends the wrong response with probability $\eta \in (0,\ 1/2\ )$. This interaction must be repeated q rounds and the reader will authenticate the tag's identity if fewer than $q\eta$ of its responses are incorrect. The above protocol is resistant to passive attacks, but not to active attacks.
Juels and Weis proposed new version of its protocols (HB and HB+) to offer protection against active attacks [21]. The main differences with respect to the HB protocol are the following: They introduce another k-bit secret key, y, shared between the reader and the tag. The tag and not the reader initiates the protocol, transmitting a k-bit blinding vector. Finally, z is computed as the scalar product of the newly introduced secret key, y, and the blinding vector transmitted by the tag, xored with the z in HB. Although Juels *et al.* claimed that HB+ is resistant to active attacks, Gilbert *et al.* showed how a man-in-the-middle

attack can be accomplished [28].

In order to avoid Gilbert *et al.*'s attack on HB+, Bringer *et al.*[8] proposed two protocols (HB++[first attempt] and HB++ that protect against such man-in-the-middle attacks). However, these protocols are vulnerable to attacks from an adversary that pretends to be a genuine reader.

Piramuthu [30] proposed a new protocol inspired by the HB++ protocol. The main changes introduced are as follows: When an adversary pretends to be a valid reader, z and the related vectors (x, y) and ν were omitted. Additionally, the protocol is kept more lightweight. In order to prevent the use of the same ρ until protocol completion, updating of ρ is accomplished every time z is computed.

Recently, Munilla and Peinado proposed HB-MP inspired by HB [22]. Munilla *et al.* acknowledge that the HB-MP was vulnerable to a simple man-in-the-middle attack, just like the initial HB+ protocol. To avoid this weakness, a new protocol named HB-MP$\prime$ was worked out. Suppose that the reader and the tag share a k-bit secret x, and the tag would like to authenticate itself to the reader. The reader selects a random k-bit binary vector a and sends it to the tag. The tag computes the binary innerproduct $a \cdot x$ and injects noise into this result. Then, the tag looks for a k-bit binary vector b such that $b \cdot x = z$. The tag sends back b to the reader. The reader checks the equality of $b \cdot x$ and $a \cdot x$. If it is correct, the tag is authenticated. This protocol differs slightly from the protocols based on the LPN problem. However, [22] maintains that the problem of finding x, knowing the vectors a and b, is at least as difficult as solving the LPN problem. In 2008, Leng *et al.* exposed a man-in-the-middle attack against HB-MP and proposed an enhanced version of the aforemention protocol, called the HB-MP+ protocol [29].

3.2.3 CC07

Chien and Chen proposed a mutual authentication protocol, which is compatible with EPCglobal Class 1 Generation 2 standards [18]. Their scheme only supports lightweight operations, such as PRNG, XOR function, and CRC checksum function. Each tag maintains a unique identification EPC_x and the secret key values K_{x_i},P_{x_i} with server during each authentication session i. In addition, Server maintains two record of each shared secret key value $(K_{new}, K_{old}, P_{new}, P_{old})$ for each entry to resist DoS attack. Two parties generate the messages using CRC function with the tag's identification and random number, then exchange them between the tag and the server to prevent replay attack. Both the authentication key and the access key are updated after a successful session in order to give backward untraceability.

We identified several weaknesses of their scheme. For the efficiency aspects, their scheme generate heavy computation load on finding the matching data entry at server due to server have to xoring message M_1 and the shared symmetric key (K_{new}, K_{old}) of each entry in back-end database. For security aspect, before server updates the shared symmetric key, the attacker can easily perform replay attack to server with iteratively issuing the eavesdropped legitimate authentication request (M_1, N_1, N_2). In addition, the anonymity property also cannot be guaranteed in their scheme. Before the tag updates the shared secret key, if the attacker sequentially sends two queries to the tag in a reasonable time, the tag will response two values M_1 and $M-2$ back to attacker. After xoring M_1 and M_2,the shared secret key K_{x_i} will be eliminated. According to the known N_1, N_2, N_3 and N_4, the attacker can easily trace the tag without being noticed. Finally, their scheme cannot provide forward security either. For each session, attacker first issues a query to the tag to get M_1 and sends M_1 to server for obtain-

ing M_2. Then, attacker stores these two values M_1 and M_2 without transmitting M_2 to the tag. Next, attacker eavesdrops the transmitted message M_3 and M_4 between the tag and other legitimate readers. With these four transmitted M_1, M_2, M_3 and M_4 of each session, once the tag is compromised (the attacker would get the current secret information such as the EPC_x), the transmitted message M_3 and M_4 can be derived with known EPC_x, N_1, N_2, N_3 and N_4. Hence, the forward security also cannot be guaranteed.

3.3 Ultra Light-weight Authentications

3.3.1 EMAP, MMAP, LMAP

In 2006, Peris *et al.* proposed a series of ultralightweight mutual authentication protocols: M2AP[11], EMAP[9], LMAP[10]. These protocols involve only simple bit-wise operation and pseudonyms to guarantee tag anonymity. Specifically, an index-pseudonym is used by an authorized reader to retrieve the information associated with a tag. Additionally, a key, divided in several subkeys, is shared between the legitimate tags and readers. Both readers and the tags use these subkeys to construct the messages exchanged in the mutual authentication phase.

In line with their real processing capabilities, the tags only support on-board simple operations. Indeed, these protocols are based on bitwise XOR ($\oplus$), bitwise OR ($\vee$), bitwise AND ($\wedge$) and addition mod 2^m. By contrast, only the readers need to generate pseudorandom numbers; the tags only used them for creating fresh messages to the protocol.

In the UMAP family of protocols, the proposed scheme consists of three stages. First, the tag is identified by means of the index-pseudonym. Secondly, the reader and the tag are mutually authenticated. This phase is also used to transmit the static tag identifier securely. Finally, the

indexpseudonym and keys are updated. Since the publication of the UMAP family of protocols, their security has been analyzed in depth by the research community. In [31, 32], the desynchronization and the full disclosure attacks are presented. These require an active attacker and several incomplete executions of the protocol to disclose the secret information on the tag based on the same attack model. Later, Chien *et al.* proposed a far more efficient full-disclosure attack [34]. Additionally, Barasz *et al.* showed how a passive attacker (an attack model that may be, in certain scenarios, much more realistic) can find out the static identifier and particular secrets shared by the reader and the tag after eavesdropping on a few consecutive protocol rounds [35, 36].

In our opinion, ultra light-weight RFID tags have to be resistant to passive attacks but not necessarily to active attacks, because of their severe restrictions such as storage, circuitry and power consumption. Ultra light-weight protocols based on bitwise operations have fundamental security flaws are as follows. The ultra light-weight protocols of protocols is based on the composition of simple operations like bitwise AND, XOR, OR and sum mod 2^m. Because all of these are triangular functions, the information does not propagate well from left to right. In other words, the bit in position i in the output only depends on bits j = 0,..., i of the input words.

·The use of the bitwise AND or OR operations to build public submessages is a weakness common to all these protocols. When a bitwise AND and OR operations is computed even over random inputs, the probability of obtaining a one (or zero) is $\frac{3}{4}$. In other words, the result is strongly biased. This poor characteristic is the basis of all the passive attacks proposed so far.

3.3.2 SASI

Chien proposed a very interesting ultralightweight authentication protocol providing Strong Authentication and Strong Integrity (SASI) for very low-cost RFID tags [12]. We briefly describe the procedure of the protocol. An index-pseudonym (IDS), the tag's private identification (ID), and two keys (k1,k2) are stored both on the tag and in the back-end database. Simple bitwise XOR ($\oplus$), bitwise AND ($\wedge$), bitwise OR ($\vee$), addition 2^m and left rotate (Rot(x,y)) are required on the tag. Additionally, random number generation (i.e. n_1 and n_2) is required on the reader.

The protocol is divided into three states: tag identification, mutual authentication and updating phase. In the identification phase, the reader sends a "hello" message to the tag, and the tag answers with its IDS. The reader then finds the information associated with the tag (k_1, k_2 and IDS) in the database, and the protocol continues to the mutual authentication phase. After the reader and the tag authenticate each other, the index-pseudonym and keys are subsequently updated. Hernandez-Castro *et al.* recently showed that the protocol was not carefully designed [33]. Indeed, a passive attacker can obtain the secret static identifier of the tag (ID) after observing several consecutive authentication sessions.

We identify the some weaknesses of the protocol. The second component of the IDS updating equation is dependent on the bitwise XOR between n2 and K_1^*. This gives rise to poor statistical properties as K_1^* is also function of n_2. The key updating equation has a kind of distributive operation that might be employed to attack the protocol, for example: $K_1^* = \text{Rot}(k_1 \oplus n_2, k_1) = Rot(k_1, k_1) \oplus Rot(n_2, k_1)$ Bitwise OR and AND operations should be used with extreme care. These operations result in a strongly biased output. For example, the nonce

n_2 can be approximated with very good precision by simply computing $n_2 \simeq B - 1$. These operations might therefore be only employed in the inner parts of the protocol but should be avoided in the generation of public submessages B and D. In fact, all the exchanged messages should resemble random values as far as possible.

IV. AIA

4.1 Abstraction of Integer Arithmetic

Stephane *et al.*[24] introduces a light-weight authentication protocol based on AIA concept. The specific multiplication of two integers can actually be viewed as a complex binary operation on strings of digits involving multiple iterations of two interlocking binary operations $(\otimes, \oplus)$ which acts on pairs of digits. If we consider the product of an n digit integer K and a p digit integer M in some unspecified base b. The result is labeled $E = e_{p+n}...e_2e_1$. Figure 4.1 shows detailed description of the integer multiplication.

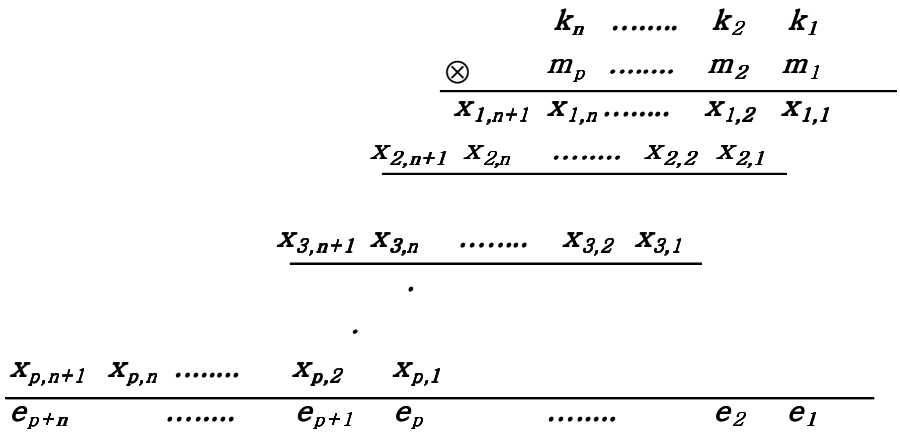

Figure 4.1: Regular Integer multiplication algorithm

In the above product in figure 4.1, each number $x_{i,p+1}x_{i,p}...x_{i,2}x_{i,1}$ is the intermediate product of the string $k_n...k_2k_1$ and the digit m_i. If we consider the product of two single digit integers, 3 and 7 in a base 10, then the product can be viewed as a binary operation that

the set of ordered pairs of digits. In case of $\otimes : (3,7) \rightarrow (2,1)$, in case of $\oplus : (3,7) \rightarrow (1,0)$. If we label the coordinates of the output as the carry and remainder of the operation, then we can write $\otimes : (3,7) \rightarrow ((3 \otimes 7)_c, (3 \otimes 7)_r)$. We can then uses the regular steps commonly accepted for multiplying two integers 'by hand' to write each digit in the product of the string $k_n...k_2k_1$ and the digit m_i as a composition of these two operation. For example,

$x_{i,1} = (k_1 \otimes m_i)_r$,

$x_{i,2} = ((k_2 \otimes m_i)_r \oplus (k_2 \otimes m_i)_c)_r$,

$x_{i,3} = ((k_3 \otimes m_i)_r \oplus ((k_2 \otimes m_i)_c \oplus ((k_2 \otimes m_i)r \oplus (k_1 \otimes m_i)_c)_c)_r)_r$.

We can then sum vertical columns of digits to derive a formula for each e_i. We elucidate a number of interesting properties of integer multiplication :

1. Both digit-wise addition, $\oplus$ and digit-wise multiplication, $\otimes$ are binary operations that map each pair of digits (with respect to a given base b) to another pair of digits, namely the remainder and carry.

2. The algorithm for multiplication of integers works independent of the choices of output for the operations $\oplus$ and $\otimes$. That is, for each of $\oplus$ and $\otimes$, if we change the output (carries and remainders) associated with one or more ordered pairs of digits, then the integer multiplication algorithm will still work but will produce different output strings.

3. Changing the outputs of $\oplus$ and $\otimes$ can alter the algebraic properties of the resulting string-wise multiplication.

Since given algorithm for basic arithmetic is common knowledge, in order to define a new string-wise multiplication, AIA would be list as a table format or an ordered string the remainders and carries associated with each ordered pair of digits for the $\oplus$ and $\otimes$ operations. Table 4.1 and the subsequent derived string, 000102010210021011000000000102000211, give the remainders and carries for actual addition and multiplication in base 3. we can define tables for $\oplus$ and $\otimes$, and thus generate a new

string-wise multiplication.

Add. Base 3 $\oplus$				Add. Base 3 $\otimes$			
a	b	carry	remainder	a	b	carry	remainder
0	0	0	0	0	0	0	0
0	1	0	1	0	1	0	0
0	2	0	2	0	2	0	0
1	0	0	1	1	0	0	0
1	1	0	2	1	1	0	1
1	2	1	0	1	2	0	2
2	0	0	2	2	0	0	0
2	1	1	0	2	1	0	2
2	2	1	1	2	2	1	1
Derived String			000102010210021011000000000102000211				

Table 4.1: Base 3 Arithmetic

Stephane *et al.* defines AIA as follows:

Abstraction of Integer Arithmetic

Let B be the set of all base-b strings of finite length. Then any base-b string, s, of length $4b^2$ defines a binary operation, $\times_s$ on B using the algorithm for regular integer multiplication but with the remainders and carries of digit-wise multiplication and addition taken from s as detailed above. We call the pair $(b,\times_s)$ an abstraction of integer arithmetic, or *AIA* for short.

V. Our Protocols

5.1 Assumption and Notation

The following assumptions are made:
· The authentication will occur between a reader and a tag.
· The communication channel between the server and the reader assumed to be secure, but that between the reader and the tag is unsecure.
· The reader will store many secret keys, each corresponding to a different RFID tag, and has infinite power.
· The tag will have a single secret key,K, in memory. The rest of the secret key, AIA, will be implemented as hardware, in the form of logic gates on the tag.
· The tag support a random number generator and can perform simple calculations provided the maximum allowable gate count to perform these calculations is not exceeded.
Notations for the protocol are summarized as follow:

5.2 Description

We begin by sharing the same secret key (K, AIA) described above, and the reader and the tag participate in an message computation algorithm in Table 5.2 to generate a message that will be exchanged between two parties. Main idea of our protocol is that reducing the computation and communication costs by message computation algorithm.
Our protocol consist of two part; tag identification and mutual authentication and key updating phase.

Table 5.1: Notation

Item	Description
K	Secret key, $K = \{K_1, K_2, ..., K_n\}$
N_i	Random base, $N_i = \{m_p m_{p-1} ... m_2 m_1\}$
K_{mi}	$K \times_{AIA} m_i = \{t_{n+1} t_n ... t_2 t_1\}$
M_i	$K \times_{AIA} N_i = \{e_{n+p} ... e_n ... e_2\}$
AIA	$AIA = \{AIA_1, AIA_2, ..., AIA_n\}$
X	Register
X_i	i^{th} right-most digit of X
X'	Left-most *n-1* digits of X
M_{i-R}	Right half of M_i, $\{e_{(p+n)/2} ... e_2 e_1\}$
M_{i-L}	Left half of M_i, $\{e_{p+n} ... e_{1+(p+n)/2}\}$
flag	Session state,(normal:0, abnormal:1)

Tag identification :

The reader requests to the tag, which first responds with its AIA_i and a random base string N_1. The reader perform exhaustive searching the database on the server. If the server could find a matched AIA_i in the database, it move on the next step,the mutual authentication phase.; otherwise, the reader request again.

Mutual authentication and Key updating:

In mutual authentication and key updating phase, the reader and the tag exchange message computed by AIA algorithm and then update their secret key. We consider two cases as the state of the authentication session, authentication terminates normally or not.

When the authentication terminates normally, neach process looks like Figure 5.1:

1. The reader sends M_1, a new random base N_2 and *flag* after computing a message M_1 using AIA_i and the random base N_1 received from the tag.

Table 5.2: Message Computation

Input	$K = k_n k_{n-1} ... k_2 k_1, N_i = m_p m_{p-1} ... m_2 m_1$
Output	$M_i = K \times_{AIA} N_i$
Step 1	For i=1 to p
Step 2	$t_1 \leftarrow (k_1 \otimes N_i)_r, carry \leftarrow (k_1 \otimes N_i)_c$
Step 3	For j=2 to n
Step 3a	$t_j \leftarrow ((k_j \otimes N_i)_r \oplus carry)_r$
Step 3b	$carry \leftarrow ((k_j \otimes N_i)_c \oplus ((k_j \otimes i)_r \oplus carry)_c)_r$
End For	
Step 4	$t_{n+1} \leftarrow carry$
Step 5	Output $K_{Ni} = t_{n+1} t_n ... t_2 t_1$
Step 6	$X \leftarrow (K_{m1})'$
Step 6a	$e_i \leftarrow (X +_{AIA} K_{mi})_1, X \leftarrow (X +_{AIA} K_{mi})'$
End For	
Step 7	$M_i = e_{n+p} ... e_n ... e_2$, stop

2. The tag performs the same addition as the reader to verify the reader's message. If it does not, the reader fails to authenticate. If it does the tag calculates the next message, M_{2-R}, by randomly choosing N_3.

3. Then, the tag updates the current secret key as $K_{i-old} = K_i$ and $K_{i-new} = K_i +_{AIA} IDS_i$, transmitting $(M_{2-R}||N_3)$ and *flag* to the reader.

4. After reader authentication, the reader verifies the message M_{2-R} to convince that the tag received the message M_1 correctly. Finally, the reader updates the secret key as $K_i = K_i +_{AIA} IDS_i$.

When the authentication terminates abnormally, each process looks like Figure 5.2:

If the last message $(M_{2-R}||N_3)$ in session 9 is interrupted by network disconnection or the adversary, key updating can lead to desynchronization in DB between the tag and the reader, the tag updates the secret

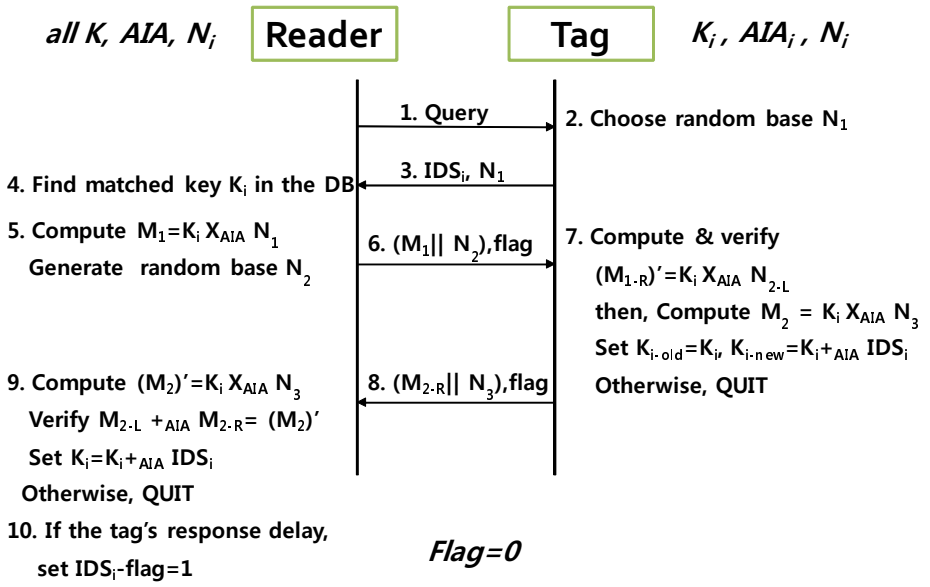

Figure 5.1: Mutual Authentication I

key but not the reader. We consider the abnormal situation as follows:
1. The reader initiates the *flag* as 1.
2. The reader sends M_1, a new random base N_2 and *flag* after computing a message M_1 using AIA_i and the random base N_1.
3. When the *flag* is 1, the tag performs different additions using old key and new key to reset the secret key K_i. The tag checks whether received message M_1 corresponds with M_{1-old} or M_{1-new}.
4. The tag initiates the next step by randomly choosing N_3, calculating right half message M_{2-R}. Then, the tag updates the current secret key as $K_{i-old} = K_i$ and $K_{i-new} = K_i +_{AIA} IDS_i$, transmitting message $(M_{2-R}||N_3)$ and *flag* to the reader.
5. After reader authentication, the reader combines the received message M_{2-R} and their computing message M_{2-L} to verify that the tag received the message M_1 correctly and they are sharing same secret K_i and AIA. Finally, the reader updates the secret key as $K_i = K_i +_{AIA} IDS_i$.

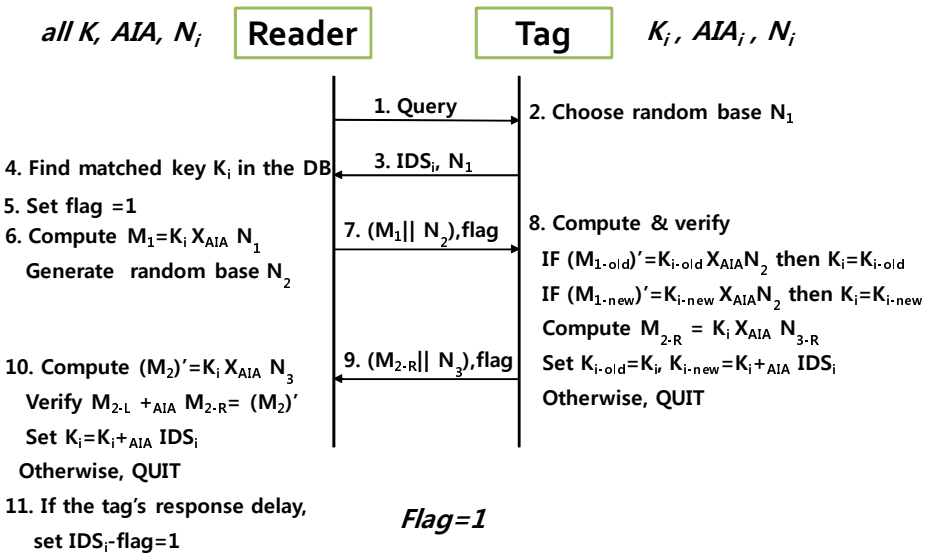

Figure 5.2: Mutual Authentication II

VI. Security and Performance Analysis

6.1 Security Analysis

The each tag is designed with a unique set of logic gates to perform the authentication. In this instance the attacker does not know any portion of (K, AIA, N). Brute force would then require uncovering all K_i and N_i as well as the table values for each of AIA_i. Given this amounts to b^{nb} guesses for K_i, $3b^p$ guesses for N_1, N_2, N_3 and $((4b^2(b!)^b)^n$ guesses for all AIA for a total of $b^{nb} + ((4b^2(b!)^b)^n + 3b^p$. We believe that this hard problem is as difficult as uncovering (K, AIA, N). In so doing the following security properties appear to be satisfied.

· Man-in-the-middle attack prevention : Even if the adversary sends flipped message $(M_i'||N_i')$, both parties should verify the messages with their unique AIA_i so that each round of the protocol prevents a man in the middle attack.

· Resistance to Cloning Attacks : Even if the secret string AIA is lifted from the tag, an attacker wishing to clone the tag would need to read the logic gate configuration on the tag and produce new tags with this same logic gate configuration in order to imitate the original tag.

· Forward Security : As the secret string K is stored in memory, periodically, once authentication is successful the tag's secret string could be updated.

· Replay attack prevention : Storing all messages from communication between the tag and the reader, and replaying them to the appropriate device will not work because both parties newly generate the message M_i' with their AIA_i.

· Synchronization: Setting up the session state, $flag$, to 0 or 1 as the

condition of the authentication session. When the authentication overs abnormally, the tag resets the secret key, as K was before.
The comparisons with the other light-weight schemes are summarized in Table 6.1 .

Table 6.1: Security Comparisons

Item	CC07[18]	HBMP07[22]	KN05[17]	SA07[24]	Our Protocol
Privacy	O	O	O	O	O
Anonymity	O	O	X	O	O
Resist to replay attack	O	X	X	O	O
Resistance to man in the middle attack	O	X	X	X	O
Resistance to Cloning	X	X	X	X	O
Synchronization	X	X	X	X	O

O : Provided , X : Not provided

6.2 Performance Analysis

We compare our protocol with stephane *et al.*' scheme in terms of the storage, computation and communication requirements of both the reader and the tag.
Table 6.3 gives the comparisons of the storage on the reader and the tag in each protocols. The most severe restrictions of the passive tag are the small number of logic gates(200-2000) which can be devoted to security algorithms, and the volatile memory available(32-128 bit) to store intermediate calculations. The implementation of the standard private key cryptosystem, AES (Advanced Encryption Standard), currently requires approximately 4000 logic gates. EPC Class-1 Gen-2 sample tag allows only 128-512 bit of ROM, 32-128 bit of RAM and 1000-10000

Table 6.2: Storage Capacity Comparisons

Approach		RAM	ROM
Stephane [24]	Tag	$(n+1)\log_2(b)$	$b(n+1)\log_2(b)+2$
	Reader	$n((4b^2-b)b\log_2(b!))$	$b(n+1)\log_2(b)+2$
Our protocol	Tag	$2(n+p)\log_2(b)+2$	$(4b^2-b)\log_2(b!)$
	Reader	$(4b^2-b)\log_2(b!)$	$N(4b^2-b)\log_2(b!)$

n : the bit-length of secret key K_i,

N : the number of tags

b : random base

p : the bit-length of a random base string N_i

gates.

Our protocol requires $2(n+p)\log_2(b)+2$ bit for K_i,N_i, M_i and *flag*, and $(4b^2-b)\log_2(b!)$ bit of ROM to store AIA for the tag where each K_i is n digits long, N_i is p digits long and random base is b. The reader is required to store the tag's all AIA_i consisting of $4b^2-b$ additive carry bit and the $b!$ possible permutations so that the reader side needs $N(4b^2-b)\log_2(b!)$ bit and $N(2(n+p)\log_2(b)+2)$ bit, AIA and K, N respectively. For example if we choose $b=4$, $n=10$, $p=10$ the tag will require 20 bit of ROM, 82 bit of RAM, and 300-400 logic to store (AIA, K, N_i). Our protocol seems efficient enough to satisfy the EPC Class-1 Gen-2 specification.

We take into account the AIA algorithm that involves bit-wise multiplication and addition in each authentication session in order to compare the computation cost of the protocols. Table 6.3 shows our protocol needs only $\frac{3}{2}(np)$ times of bit-wise multiplication and $(n+1)(p-1)+\frac{np}{2}$ times of bit-wise addition; we reduce the computation cost Stephane *et al.*'s one[24].

Moreover, while Stephane *et al.*'s protocol repeats at least 40 times of

Table 6.3: Computation & Communication Comparisons

Approach		$\oplus$	$\otimes$	Communication
Stephane [24]	Tag	$(n+1)r$	nr	*2r*
	Reader	$(n+1)r$	nr	
Our protocol	Tag	$(n+1)(p-1)+\frac{np}{2}$	$\frac{3}{2}(np)$	3
	Reader	$2(n+1)(p-1)$	$2np$	

r : the number of authentication session round

n : the bit-length of secret key K_i

b : random base

p : the bit-length of a random base string N_i

authentication round to guarantee reasonable security, our protocol only need 3 times of authentication session. Stephane *et al.*'s protocol exchanges one bit message each other so that the adversary can guess the messages transmitted. Therefore, their protocol is forced to repeat the authentication session. Thus, our protocol has practical performance advantages over the Stephane *et al.*'s scheme, while also providing the privacy and security properties.

VII. Conclusion

In this thesis, we have reviewed the security flaws of the previous light-weight protocol based on bitwise operations or CRC reported by other researchers as well as new ones. We show that most of the previous light-weight RFID authentication protocols based on random number generator, Cyclic Redundancy Code(CRC) or bitwise operations (*e.g.*, XOR, AND and OR)are vulnerable to both passive and active attacks [32, 31]. For instance, anyone can obtain the tag identity and secret key through the consecutive eavesdropping.[12] Then, we introduce the Abstraction Integer Arithmetic(AIA), key pool with a unique subset of the remainders and carries of the integer for each tag, proposed by Stephane *et al.*[24]. We enhance efficiency as well as security of Stephane *et al.*'s protocol. While requiring only 82 bit of RAM, 20 bit of ROM and 300-400 logic gates, our protocol can satisfy security requirements(*e.g.*, synchronization, protection to replay, cloning and impersonation)for RFID system. Our protocol may be scaled to provide a high level of security, using relatively little computational resources and be an alternative of the previous schemes based on bitwise operation.

정수연산방식을 적용한 경량 RFID 인증 프로토콜 연구

곽민혜

무선 주파수를 이용하여 물리적 접촉 없이 정보를 저장하거나 읽은 무선 인식기술인 RFID (Radio Frequency IDentification, 전자태그)는 반도체 기술의 발전과 인터넷의 등장으로 인하여 지난 10여년 동안 꾸준한 발전을 해왔으며 유통, 물류, 의료, 교육등 다양한 분야에 적용되고 있다. 그러나 RFID 시스템에서의 태그와 리더는 주파수 통신을 하기 때문에 태그의 정보가 노출되기 쉽고 이는 공격자의 기본정보로 활용되어 사생활 침해 및 보안 위협을 가할 수 있어 RFID 대중화의 걸림돌이 되고 있다. 기업입장에서는, 산업 스파이가 취약한 전자태그의 정보의 불법적으로 수집, 위장 태그를 통해 잘못된 정보를 제공하고나 DoS 공격(Deinal of Service, 서비스 거부)를 시도할 우려가 있다. 따라서 RFID 시스템에서 사생활 보호, 접근 통제, 인증, 익명성, 데이터 복구등의 보안 요구사항을 만족하는 것은 필수적인 사항이다.

이러한 안전성 문제를 해결하기 위하여 태그, 리더, 데이터베이스 서버간의 인증을 통한 정보제공에 대한 인증기법에 대한 연구가 진행되었다. 그러나 저가의 태그는 보통 5K∼10K의 논리 게이트와 250∼3K의 보안 함수를 실행할 수 있는데 제한적인 연산능력과 저장공간의 한계로 인해 대칭키, 공개키같은 전통적 암호기법 적용에 어려움있다. 기존의 경량 인증기법은 대부분 난수 생성기와 XOR, AND, OR 같은 비트연산기반으로 연속적인 도청에 의한 태그 식별 및 비밀키 노출, 재전송 공격등에 취약한 단점이 있다.

본 논문에서 정수연산방식(AIA, Abstraction of Integer Arithmetic), 두 정수열 곱셈 알고리즘의 올림수와 내림수에 대응하는 집합을 AIA로

정의하고, 리더와 태그측에서 각각 AIA 연산을 통해 메시지를 생성하고 교환을 통해 상대방이 동일한 비밀키와 AIA를 가지고 있다고 신뢰하고 인증하는 방식이다. 정수연산방식에 기반한 인증 프로토콜은 최소 82 비트의 휘발성 메모리, 20 비트 저장공간, 300-400 논리 게이트를 필요로 하는 만큼 EPC의 규격 요건을 만족하는 효율적인 기법이며, 또한 상호인증방식을 통해 중간자 공격과 재전송공격을 차단하고 각 태그의 비밀키인 AIA가 하드웨워 논리 게이트 형태로 구현되어 복제 및 위장공격의 위험으로부터 안전성을 보장하는한다. 정수연산방식에 기반한 경량 인증 프로토콜은 RFID의 대중화의 가장 큰 걸림돌인 사생활 침해 및 외부 공격등의 안전성 문제를 해결하고 유통, 물류, 의료등 산업분야 뿐만아니라 군 무선정찰 시스템등 높은 보안성을 요구하는 분야에서도 효율적으로 사용되리라 기대한다.

References

1. A. Juels, D. Molnar, and D. Wagner, "Security and privacy issues in e-passports," IEEE/Create Net Secure Commun., 2005.

2. S. Kinoshita, M. Ohkubo, F. Hoshino, G. Morohashi, O. Shionoiri, and A.Kanai, "Privacy Enhanced Active RFID tag," International Workshop on Exploiting Context Histories in Smart Environments, May 2005.

3. S. S. Kumar and C. Paar,"Are standards comliant Elliptic Curve Cryptosystems feasible on RFID?," in Proceedings of Workshop on RFID Security, Austria, July 2006.

4. D. Molnar and D. Wagner,"Privacy and security in library RFID: Issues, practices and architectures," Conference on Computer and Communications Security-CCS'04, pp. 210..219, 2004.

5. M. Ohkubo, K. Suzki and S. Kinoshita,"Cryptographic Approach to 'privacy-Friendly' Tags,"in RFID Privacy Workshop, 2003.

6. K. Rhee, J. Kwak, S. Kim, and D. Won,"Challenge-response based RFID authentication protocol for distributed database environment," International Conference on Security in Pervasive Computing SPC 2005, pp.70-84, 2005.

7. A. Juels. "Minimalist cryptography for low-cost RFID tags," In C. Blundo and S. Cimato, editors, Security in Communication Networks (SCN 04), pages 149.164. Springer-Verlag, 2004. LNCS no. 3352.

8. J. Bringer, H. Chabanne and E.Dottax,"HB++Protocol Secure against Some Attacks," IEEE International Conference on Pervasive Service, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing -SecPerU, 2006.

9. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags," Proc. OTM Federated Conf. and Workshop: IS Workshop,Nov. 2006.

10. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A.Ribagorda,"LMAP: A Real Lightweight Mutual Authentication Protocol Low-cost RFID tags," in: Proc. of 2ndWorkshop on RFID Security, July 2006.

11. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A.Ribagorda, "M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tagsin,"in: Proc. of International Conference on Ubiquitous Intelligence and Computing UIC'06, LNCS 4159, pp. 912-923, Springer, 2006.

12. H.Y. Chien. "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity," IEEE Transactions on Dependable and Secure Computing 4(4):337-340. Oct.-Dec. 2007.

13. E.Y. Choi, S.M. Lee, and D.H. Lee. Efficient RFID authentication protocol for ubiquitous computing environment. In Proc. of SECUBIQ'05, LNCS, 2005.

14. I. Vajda and L. Buttyan, "Lightweight authentication protocols for low-cost RFID tags," in Proc. 2nd Workshop on Security in Ubiquitous Comput., 2003.

15. G. Avoine, E. Dysli, and P. Oechslin, "Reducing time complexity in RFID systems," in Proc. Sel. Areas Cryptography, B. Preneel and S.Tavares, Eds. New York: Springer-Verlag, 2005, Lecture Notes in Computer Science, to be published.

16. A. Juels, "Strengthening EPC Tag against Cloning," in ACM Workshop on Wireless Security (WiSe), pp.67-76. 2005.

17. S. Karthikeyan and M. Nesterenko,"RFID security without extensive cryptography," in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pp. 63-67, 2005

18. H.Y. Chien and C.H. Chen, "Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards," in Computers Standards and Interfaces 29(2), pp 254-259, 2007.

19. N. J. Hopper and M. Blum, "Secure Human Identification Protocols," in Proc. Seventh Int' Conf. Theory and Application of Cryptology and Information Security, pp. 52-66, 2001.

20. H. Gilbert, M. Robshaw and H. Sibert, "Active Attack against HB+ -A Provably Secure Lightweight Authentication Protocol", in Cryptology ePrint Archive, Report 2005/237, 2005.

21. A. Juels and S.A. Weis, "Authenticating Pervasive Devices with Human Protocols," in Proc. 25th Ann. Int' Cryptology Conf. (CRYPTO'05), pp. 293-308, 2005.

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

23. M. H. Kwak and K. J. Kim, "A Study on Lightweight RFID Authentication Protocol using Integer Arithmetic," Conference on Information Security and Cryptology (CISC'08),pp.157-161, 2008

24. L. Stephane and T. L. Adrian ,"Clone resistant mutual authentication for low-cost RFID technology," IACR Eprint, 2007.

25. EPCglobal, http://www.epcglobalinc.org/.

26. I. Vajda and L. Buttyan ,"Lightweight authentication protocols for low-cost RFID tags," In Proc. of UBICOMP'03, 2003.

27. S. Weis ,"Security parallels between people and pervasive devices," In Proc. of PERSEC'05, pages 105.109. IEEE Computer Society, 2005

28. H. Gilbert, M. Robshaw, and H. Sibert," An active attack against HB+ - A provably secure lightweight authentication protocol," Manuscript,2005.

29. X. Leng, K. Mayes, and K," Markantonakis. HB-MP+ protocol: An improvement on the HB-MP protocol," IEEE International Conference on RFID, pages 118.124, 2008.

30. Selwyn Piramuthu,"HB and related lightweight authentication protocols for secure RFID tag/reader authentication," In Proc. of CollECTeR'06, 2006.

31. T. Li and R. H. Deng,"Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol," The Second International Conference on Availability, Reliability and Security (AReS 2007), Vienna, 2007.

32. T. Li and G. Wang,"Security Analysis of Two Bultra-lightweight RFID Authentication Protocols," IFIP SEC 2007, May 2007

33. J. C. Hernandez-Castro, J. M. E. Tapiador, P. Peris-Lopez and J.-J. Quisquater,"Cryptanalysis of the SASI Ultralightweight RFID Authentication Protocol,"IEEE Transactions on Dependable and Secure Computing, April 2008.

34. H.-Y. Chien and C.-W. Huang," Security of ultra-lightweight RFID authentication protocols and its improvements," SIGOPS Oper. Syst. Rev., 41(4):83.86, 2007.

35. M. Barasz, B. Boros, P. Ligeti, K. Loja, and D. Nagy,"Breaking LMAP," Hand. of RFIDSec'07, 2007.

36. M. Barasz, B. Boros, P. Ligeti, K. Loja, and D. Nagy," Passive attack against the M2AP mutual authentication protocol for RFID tags," Proc. of First International EURASIP Workshop on RFID Technology, 2007.

37. F. Thornton, B Haines, A.M. Das, H. Bhargava, A. Campbell and J. Kleinschmidt," RFID Security Barasz," Syngress Publishing, 2006

Acknowledgement

It is a pleasure to thank the many people who made this thesis possible. First of all, I would like to express my sincere gratitude to Prof. Kwangjo Kim, my academic advisor, for his constant direction and support. Without his guidance, I could never have carried out my research in ICU. Special thanks are also due to Prof. Lee and Ph.D. Choi for their generosity and agreeing to serve as advisory committee members. I would also like to thank all members of Cryptology and Information Security Laboratory: Hyunrok Lee, Zeen Kim, Kyusuk Han, Jangseong Kim, Dang Nguyen Duc, Konidala Munirathnam Divyan, Hanyoung Noh, Hyewon Park, Hyeran Mun, Sungmok Shin, Myunghan Yoo and Imsung Choi for giving me lots of interests and good advices during the course of my study. I also thank Hyunkyung Park for helpful support as a staff member. I also appreciate to the graduates: Sungbae ji, Sungjun Yoon for their everlasting guidance in life and study of ICU.

Most of all, I would like to express my loving thanks to my mother, Kyungsuk Yang, my husband, Jinyoo Kim, and my son, Yoomin Kim, for their endless concerns and devotional affection. Without their prayers, faiths, and supports to me, I could never complete my study and have a good time in ICU. To them I dedicate this thesis. Finally, I'll never forget the time in ICU.

Curriculum Vitae

Name : Min-Hea Kwak

Date of Birth : September 28, 1976

Sex : Female

Nationality : Korean

Education

1995.3–1999.2 Computer Science
Korea University (B.S.)

Career

2001.3–2006.12 Chief of the Computer department
Project Title
Korea Army

Publications

(1) 2008.6 곽민혜,김광조, 정수연산방식을 적용한 저가 전자태그의 경량 인증기법 연구,summitted to *CISC'08 Summer* Korea

(2) 2008.10 김장성,권미영,김이형,곽민혜,한규석,김광조,"감시정찰 센서네트워크 및 주요 시설물 관리에서의 키관리 기법 비교", 2008 한국정보보학회 충청지부 학술발표회 논문집, pp.75-83, 2008.10.17, 배재대학교,대전, 2008

(3) 2008.12 곽민혜,김광조, 취약성 분석을 통한 경량 RFID 인증 프로토콜 고찰,summitted to *CISC'08 Winter* Korea

(4) 2009.1 Min-Hea Kwak, Jangsung Kim, Kwangjo Kim, Advanced Light-weight RFID Authentication Protocol using Integer Arithmetic, summitted to *SCIS'09* Korea

Participated Projects

2008.3–2009.2 RFID/USN용 센서태그 및 센서노트 기술 개발.