A Thesis for the Degree of Master

RFID-enabled Extensible Authentication Framework and Its Applications

Sungbae Ji

School of Engineering

Information and Communications University

2008

RFID-enabled Extensible Authentication Framework and Its Applications

RFID-enabled Extensible Authentication Framework and Its Applications

Advisor : Professor Kwangjo Kim

by

Sungbae Ji

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 20. 2007
Approved by

Professor Kwangjo Kim
Major Advisor

RFID-enabled Extensible Authentication Framework and Its Applications

Sungbae Ji

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 20. 2007

Approved:

Chairman of the Committee
Kwangjo Kim, Professor
School of Engineering

Committee Member
Young-Hee Lee, Professor
School of Engineering

Committee Member
Byoungcheon Lee, Assistant professor
Dept. of Information Security, Joongbu University

M.S. Sungbae Ji
20042055

RFID-enabled Extensible Authentication Framework and Its Applications

School of Engineering, 2008, 43p.
Major Advisor : Professor Kwangjo Kim.
Text in English

Abstract

Recently, various applications of RFID have been developed and researched while security issues RFID systems such as privacy infringement and the forgery of tags have being raised. Many types of authentication protocols were proposed in order to solve these security problems, but there is no universally adoptable authentication protocol. Therefore, it is difficult to combine heterogeneous RFID systems which have different security requirements and authentication protocols.

In this thesis, we propose a novel RFID authentication framework. Our proposed RFID-enabled Extensible Authentication Framework (REAF) enables us to integrate different RFID applications with various security requirements, RFID tags, and authentication protocols into a single RFID authentication system because it supports any authentication methods including vendor-specific methods. In the integrated RFID system using REAF, it is easy to manage or extend the system, and the owner of an RFID tag can change its authentication method as they want.

In order to use our proposed authentication framework, a specific authentication method is required. Therefore, we also present typical

examples of authentication methods using two different cryptographic primitives such as a hash function and a block cipher algorithm.

REAF-HF method is a REAF method using a hash function designed for logistical RFID applications which do not require to protect the IDs of tags. Any affordable hash functions for RFID tags can be used in our REAF-HF method. REAF-HF is simple but prevents replay attacks and tags spoofing. REAF solves the scalability problems of the previous hash-based authentication protocols and does not require the synchronization of DB.

Three kinds of REAF-BC methods provide different security properties for REAF. REAF-BC-TA authenticates tags with `Identity Type` and can be also useful for logistical RFID applications. REAF-BC-OA1 authenticates the owner of a tag, and REAF-BC-OA2 extends REAF-BC-OA1 into a mutual authentication. Because REAF-BC-OA1 and REAF-BC-OA2 can protect owner's privacy, they are suitable for consumer applications. Our REAF-BC methods are equal to or better than other previous RFID authentication protocols using block cipher in terms of its security properties and performance.

All these four REAF methods have a meaning in that they are designed for REAF. Each of our proposed REAF methods which aim for the different security requirements of RFID applications can be used in an integrated RFID system together. Because we can select an REAF method considering security requirements and levels of target applications, this feature can provide flexibility for RFID systems from the aspect of cost-security tradeoff.

Contents

List of Figures

List of Tables

List of Abbreviations

DB Database

EAP Extensible Authentication Protocol

EPC Electronic Product Code

GE Gate Equivalent

PIN Personal Identification Number

PRNG Pseudo Random Number Generator

REAF RFID-enabled Extensible Authentication Framework

RFID Radio Frequency Identification

XOR Exclusive OR

List of Notations

$\mathcal{T}$ An RFID tag

$\mathcal{R}$ An RFID reader

$\mathcal{M}$ A middleware for authentication

$\mathcal{O}$ The owner of an item to which $\mathcal{T}$ is attached

$\mathcal{A}$ An Adversary with RF communication capability

$\mathcal{D}$ A distributor

$\mathcal{S}$ A supplier or a manufacturer

$\mathcal{C}$ A customer of a RFID-tagged product

$A \rightarrow B : msg$ A message packet msg is transferred from entity A to entity B

$A \rightarrow B \rightarrow C : msg$ msg is relayed by B from A to C

$ID_{\mathcal{T}}$ Identity of $\mathcal{T}$

RND_A A random number generated by an entity A

$str_1 \oplus str_2$ Bitwise XOR value of two strings, str_1 and str_2

$str_1 \,||\, str_2$ Concatenation of str_1 and str_2

$\mathbf{Hash}(str)$ Hash value of str

$Secret$ A shared secret between $\mathcal{M}$ and $\mathcal{T}$

K_{AB} A shared key between A and B

$E_K(str)$ Block cipher encryption of str with K

$len(msg)$ The length of msg in bits

I. Introduction

Radio Frequency IDentification (RFID) technology has been widely used for tracking and inventorying systems in supply chains, check-out/in systems in libraries, electronic payment systems, and electronic passports. However there are sensitive issues that should be dealt with in order to make RFID systems secure.

Feldhofer *et al.*[4] described three security issues in RFID systems: privacy compromise, forgery of tags, and unauthorized access to tags. In addition to these issues, the problems of eavesdropping, tag spoofing, tag cloning, and replay attacks were pointed out in the other literatures [14, 21, 22]. These security and privacy risks in RFID systems are main barriers which restrict wider applications of RFID.

These security problems can be solved through proper authentication mechanisms. Recently, many authentication protocols are proposed such as hash-based authentication schemes PIN-based scheme [16], [14, 19, 20], and block-cipher-based scheme [4] to protect RFID systems, but there is no general-purpose authentication protocol that can be applied to many types of RFID systems. In fact, it is inevitable to have various authentication protocols because each application has its own security requirements. Moreover, each application requires different types of RFID tags because of their different characteristics. Therefore, it is hard to integrate RFID systems using different tags and authentication schemes into a single RFID authentication system.

1.1 Motivation and Objectives

(1) An Authentication Framework suitable for RFID Systems

Each RFID application must meet with its security requirements according to its own goal, and various types of RFID tags used for the applications also have their own security features (*e.g.* encryption algorithms, hash functions, and PINs) as well as its technical features (*e.g.* radio frequencies, computational resources, and data I/O rates). Because each system implements a suitable authentication protocol based on the capacity of tags and the security goal, there exist many authentication protocols. However, this diversity in RFID systems isolates each application and restricts the extension of RFID systems.

To solve this problem, we require an authentication framework to integrate different RFID applications with various authentication security requirements, tags, and protocols into a single RFID authentication system. EAP (Extensible Authentication Protocol) [17] seems to be a solution for this problem because of its extensibility and similar architectural model. However, there are a few limitations of applying EAP directly into RFID systems such as bulk-reading capabilities, traceability and privacy issues, and extremely low resources. These features make EAP inapplicable to RFID systems. Therefore, we will design a novel authentication framework suitable for RFID systems.

(2) Hash-based Authentication Method

According to Feldhofer *et al.* [27], the hardware implementations of hash functions show that they are not quite suitable for low-cost RFID tags. Nevertheless, many hash-based authentication schemes have been proposed for RFID tags. The representative hash-based schemes are hash-lock (HL) [14], randomized hash lock (RHL) [14], hash chain (HC)

[19], and hash-based ID variation (HIDV) scheme [20]. However, these schemes except HIDV are vulnerable to replay and tag spoofing attacks. RHL and HC are impractical for suppliers and distributors because of their scalability problem. HIDV scheme does not work with desynchronized DB caused by unreliable RF communication or attacks. To solve these problems, we will propose a hash-based authentication method for our proposed RFID authentication framework.

(3) Block-Cipher-based Authentication Methods

The first RFID authentication protocol using a block cipher was proposed by Feldhofer *et al.* [4, 6]. Their novel approach of an AES hardware implementation has achieved low power consumption and low die-size. Kaps *et al.* [8] also implemented AES encryption in CBC mode with the viable number of NAND gate equivalents. Feldhofer *et al.*'s recent work [5] suggested that AES-128 is more appropriate for RFID systems than any other hash functions. Usually, a low-cost RFID tag means a passive RFID tag less than 5 cents with roughly 500-5,000 gates [14]. Besides AES, light-weight block ciphers such as mCrypton [11], HIGHT [12], and PRESENT [13] are developed for resource-constraint devices. These implementations with less than 3,000 gates show that block ciphers are affordable for low-cost RFID tags.

Based on AES hardware implementation, following RFID authentication protocols using AES are proposed. Feldhofer [3] and Dominukus *et al.* [2] proposed a challenge-response authentication protocol conforming to ISO/IEC 18000-3 standard. Toiruul *et al.* [9] proposed a mutual authentication protocol with two shared random secrets. However, these protocols have some drawbacks. Protocol 5 in [2] requires one AES decryption which is not implemented in practice. When using different secret keys for different product classes, [2] have scalability problems to find a correct key. [9] requires three consecutive AES

encryptions at the tag side which might be incapable in passive tags. Traceability and desynchronization are also defects in [9].

In this thesis, we will propose three block-cipher-based authentication methods for our proposed RFID authentication framework. Our authentication methods will be designed for different security requirements and improve drawbacks in previous work.

1.2 Our Contributions

In this thesis, we proposed a universal authentication framework suitable for RFID systems. When applying our RFID-enabled Extensible Authentication Framework (REAF) to RFID systems, a specific authentication method that a tag supports can be chosen in the negotiation process. As a result, many types of tags and authentication methods can be integrated into a single authentication system, and an owner of a tag can use an authentication method they want to use.

We also analyzed the existing RFID authentication protocols using hash functions and block ciphers and propose four new authentication methods with different security properties for REAF: REAF-HF, REAF-BC-TA, REAF-BC-OA1, and REAF-BC-OA2. REAF-HF and REAF-BC-TA authenticates tags with `Identity Type` and can be useful for supply chain management. REAF-BC-OA1 authenticates the owner of a tag, and REAF-BC-OA2 extends REAF-BC-OA1 into a mutual authentication. REAF-BC-OA1 and REAF-BC-OA2 can protect owner's privacy, and they are suitable for consumer applications.

Because all these REAF methods are performed over REAF, we can support RFID tags embedding various cryptographic primitives from each vendor. It is also possible to select an REAF method satisfying security requirements of a specific RFID application and provide flexible security level with various key sizes. Therefore, REAF and REAF

methods can be quite practically used in the real-world applications.

1.3 Organization

The rest of this thesis is organized as follows: Chapter 2 explains security and privacy issues, preliminary knowledge of the RFID technology, and related RFID authentication protocols. In Chapter 3, we describe why we need an authentication framework for RFID systems and propose RFID-enabled Authentication Framework based on its requirements and the limitations of EAP. In Chapter 4, we present RFID authentication methods designed for REAF using hash functions and block ciphers and analyze their security properties comparing other protocols. Finally, we summarize and conclude this thesis in Chapter 5.

II. Preliminaries

2.1 Security and Privacy Issues

Followings are security and privacy problems in RFID systems. These attacks can be exploited together to bypass the authentication or extract private information illegally.

- **Eavesdropping:** $\mathcal{A}$ can passively monitor and record a communication over RF channels between $\mathcal{T}$ and $\mathcal{R}$.
- **Replay Attack:** $\mathcal{A}$ can eavesdrop a message transmitted over an RF channel and retransmit it to $\mathcal{T}$ or $\mathcal{R}$.
- **Man-in-the-Middle Attack:** $\mathcal{A}$ can actively drop, relays or insert a message in an authentication phase between $\mathcal{T}$ and $\mathcal{R}$ as if $\mathcal{A}$ were legitimate $\mathcal{T}$ or $\mathcal{R}$.
- **Tag Tampering:** $\mathcal{A}$ can access $\mathcal{T}$ and change its content in the RF chip if $\mathcal{T}$ does not have proper tamper-resistant mechanism.
- **Tag Cloning:** $\mathcal{A}$ can physically make an identical copy of RF chip if $\mathcal{T}$ is not protected with Physical Unclonable Function (PUF).
- **Tag Spoofing:** $\mathcal{A}$ can pretend that $\mathcal{A}$ is a $\mathcal{T}$ with valid identity $ID_{\mathcal{T}}$ in its authentication phase between $\mathcal{A}$ and $\mathcal{R}$.
- **Unauthorized Access to Tags:** $\mathcal{A}$ accesses $\mathcal{T}$'s memory without authorization after bypassing authentication. As a result, $\mathcal{A}$ can reads from or writes to $\mathcal{T}$.

- **Desynchronization:** When $\mathcal{R}$ authenticates $\mathcal{T}$ using an authentication scheme whose identification information should be updated, $\mathcal{A}$ can desynchronize identification information between $\mathcal{T}$ and DB. As a result, $\mathcal{A}$ can make $\mathcal{T}$ unidentifiable.

- **ID Exposure:** When $\mathcal{R}$ authenticates $\mathcal{T}$, $ID_{\mathcal{T}}$ can be exposed to $\mathcal{A}$ by $\mathcal{A}$'s eavesdropping.

- **Traceability:** If a specific $\mathcal{T}$ is distinguishable from other tags by eavesdropping or active querying, $\mathcal{A}$ can trace $\mathcal{T}$, and $\mathcal{O}$'s privacy is violated.

2.2 RFID Application Requirements

Phillips *et al.* [15] categorized RFID systems into three applications as shown in Table 2.1. Logistical applications are the RFID applications used for inventorying and tracking products in supply chains. Because the products are required to be rather tracked and physically secured, strong authentication mechanisms in RFID systems are not necessarily required. Low-latency, high potential read rates and bulk-reading capabilities are much more important.

On the other hand, consumer applications need to protect consumers' privacy. When an unauthorized person or a device tries to access a smart card, an electronic passport, or a consumer's belongings, a certain level of authentication is required to protect privacy.

Vertical applications are somewhere between logistical applications and consumer applications and require specific security features according to their goals. For example, RFID-enabled banknotes [18] require limited access control to protect consumers' privacy and tracking capabilities to monitor illegal transactions as well.

Table 2.1: RFID Applications

Applications	Required	Not Required	Examples
Logistical	low-latency bulk-reading	little need for security mechanisms	inventorying & tracking supply chains
Consumer	privacy and security	bulk-reading	e-Passports consumers' belongings
Vertical	tailor security features to a specific business process		RFID-embedded bank notes and pocker chips

2.3 RFID Tag Classifications

Various RFID applications need various types of RFID tags. Based on the band of radio frequency and battery, RFID tags are categorized into followings:

- **Radio Frequency**
  - Low-frequency (LF): 125 - 134.2 kHz and 140 - 148.5 kHz
  - High-frequency (HF): 13.56 MHz
  - Ultra-high-frequency (UHF): 868 MHz-928 MHz
- **Battery**
  - Passive: Generally, passive tags are widely used in logistical applications because they are cheap and small
  - Active: Unlike passive tags, active tags require a power source and can have more computational resources.

EPCglobal Class-1 Generation-2 UHF tags (EPC Gen2 tags) [1] are passive identity tags designed to be used for supply chain and logistical

applications, and thus they are simple and cheap. They have a PRNG (pseudo random number generator), CRC (cyclic redundancy check) error detection, kill function (32-bit kill PIN), and password-protected access control (32-bit access PIN).

Smart cards and RFID-enabled passports are typical examples of RFID tags using ISO/IEC 14443 air interface. Because security features are not defined in the ISO/IEC standards, each vendor implements its own proprietary authentication and access protocol using cryptographic primitives such as DES, 3DES, AES, RSA, SHA-1, etc. Smart cards must be placed close to their readers for relatively lengthy periods to be read.

2.4 Hardware Implementation of Cryptographic Primitives

2.4.1 Hash Implementation

Hash functions are widely used building blocks for RFID authentication protocols. However, their hardware implementation result does not indicate suitability for low-cost RFID tags. Kaps *et al.* [8] implemented SHA-1 with 4,276 gate equivalents but they did not consider the message expansion RAM, which requires approximately 2,400 gates according to Feldhofer *et al.* [27]. In [27], Feldhofer *et al.* achieved the smallest SHA-256 ASIC implementation known so far. Their implementation which aim for low die-size and low power consumption have 10,868 gates and a mean power consumption of 15.87 µA at 100 kHz using a cheap 0.35 µm process technology with a supply voltage of 3.3 V. A hash calculation on a 512-bit block of data requires 1,128 clock cycles. They also provided the result of SHA-1 implementation and estimations of MD5 and MD4. Gate counts required for SHA-1, MD5, and MD4 are 8,120

GEs, 8,400 GEs, and 7,300 GEs respectively.

2.4.2 Block Cipher Implementation

AES Implementation for RFID

AES is a block cipher which can be used for strong authentication. Due to its simple design, the algorithm can be implemented on any platforms in hardware. Feldhofer *et al.* [4, 6] implemented encryption-only AES algorithm with 3400 gates as an 8-bit architecture in hardware. They achieved low power consumption and low die-size circuit enough to satisfy the restriction of passive RFID tags. This result shows that AES encryption algorithm can be used as a cryptographic primitive for RFID authentication protocols.

Kaps *et al.* [8] also presented hardware implementations of AES. Their AES design supports encryption in CBC mode and uses 20% more NAND gate equivalents than [6] while being almost twice as fast. From their result, AES is less efficient in energy consumption than SHA-1, still AES is suitable for ultra-low power applications with 17-byte or less payload size.

Unlike [8], Feldhofer *et al.* [5] states that RFID systems have minor relevance with energy consumption. Instead, they use three parameters as a metric for a fair comparison of different crypto implementation in hardware: mean power consumption, chip area (gate equivalents), and the number of clock cycles. They concluded AES-128 is more appropriate cryptographic primitive in RFID systems than other algorithms such as SHA-256, SHA-1, MD5, and ECC-192. [27] showed that the AES module requires only a third of the chip area and half of the mean power as compared with SHA-256. Even smaller hash functions like SHA-1, MD5 and MD4 are also less suitable for RFID tags than the AES.

Other Block Cipher Implementation for RFID

After AES hardware implementation, other block cipher algorithms suitable for RFID authentication were designed and implemented in hardware. mCrypton [11] is a 64-bit block cipher with three key lengths of 64, 96, and 128 bits. Its design is based on a 128-bit block cipher, Crypton, which was a candidate for AES. mCrypton is simply redesigned for low-cost RFID tags and sensors. mCrypton implementation in hardware requires about 3500 to 4100 gates for both encryption and decryption, and about 2400 to 3000 gates for encryption only.

HIGHT [12] is another block cipher designed for resource-constrained devices. It is a variant of generalized Feistel network with 32-round iterative structure, 64-bit block length, and 128-bit key length. HIGHT encryption implementation requires 3048 gates and implementation for both encryption and decryption does not require much more gates than the encryption-only circuit.

PRESENT [13] is a ultra-lightweight block cipher designed by Bogdanov *et al.* It has 64-bit block length and 80 or 128-bit keys. Its implementation requires 1570 gates and a simulated power consumption of 5µW to encrypt one block of plaintext with an 80-bit key. In its power-optimized implementation, they achieved a power consumption of only 3.3µW with additional 53 gates. Also, PRESENT with 128-bit key requires 1886 gates, which is much less than other block ciphers.

2.5 RFID Authentication Schemes

2.5.1 PIN-based Schemes

An EPC Gen2 tag has two 32-bit PINs. Many EPC-compliant authentication protocols utilize these PINS for the password-protected access control. Juel [16] proposed authentication protocols to strengthen EPC

tags against cloning. The EnhancedTagAuth protocol is a mutual authentication protocol between a tag and a reader. The tag authenticates the reader using the access PIN and the reader authenticates the tag using the kill PIN. Unlike the EnhancedTagAuth protocol, the BasicTagAuth+ protocol is a three-party protocol. Its one-way authentication using the kill PIN is performed between tags and a verifier while limiting intervention from readers. In these authentication methods, adversaries can eavesdrop a session and figure out the PINs. Replay and spoofing attacks are also possible. However, these authentication protocols have a meaning in that it was designed for the purpose of securing EPC tags.

2.5.2 Hash-based Schemes

Due to their simplicity, many hash-based authentication schemes have been proposed for RFID tags. Hash-lock (HL) scheme [14] reveals keys in plaintexts and cannot protect location privacy because a tag is authenticated using a fixed metaID. In randomized hash lock (RHL) [14], a tag responds with randomized ID value but it is still vulnerable to replay and spoofing attacks. This scheme is not scalable because a reader performs brute-force search to find a match of the randomized hash value. Hash chain (HC) [19] is designed to provide user privacy based on indistinguishability and forward secrecy, but its scalability problem is even worse than RHL. The back-end database requires a series of hash computations, and tag should have two different hash functions. Hash-based ID variation (HIDV) scheme [20] renews the ID of tag on every successful session. Although this property makes it secure against replay attack and spoofing attack, the DB desynchronization from unreliable RF communication or attacks can cause problems. Also, attackers can trace a tag by selectively dropping the reader's request in the middle.

2.5.3 Block Cipher based Schemes

RFID Authentication Protocols using AES

Based on the feasibility of AES for RFID tags, RFID authentication protocols using AES are proposed. Feldhofer [3] proposed a simple two-way challenge-response authentication protocol extending the packet and packet formats of ISO/IEC 18000-3 standard which defines procedural communication mechanisms at 13.5 MHz. In this protocol, application protocol data units (APDUs) include a unique identifier (UID) which is retrieved from the tag by the inventory request before the authentication phase. The reader indicates a UID of a tag to answer, and the tag also sends back its UID to be identified. Indicating a UID ensures which key to use for encryption, but the identity of the tag is exposed. Therefore, this protocol should be limited to only well-known trusted RFID readers in closed environments.

Dominukus *et al.* [2] also proposed authentication protocols using AES-128. Their five authentication protocols are designed based on ISO/IEC 18000-3 standard thus starts with an inventory request and end with a stay quiet request. Therefore, this protocol could be non-conforming to other RFID air interfaces. Moreover, all these protocols assume one global key because the reader cannot know which key to use when assuming one key per tag in Protocol 2, 3, 4, and 5. As a result, a tag can spoof its ID.

Toiruul *et al.* [9] proposed a mutual authentication protocol using encryption-only AES on tags. In this protocol, two shared random secrets (k_1 and k_2) between each tag and the back-end server are updated in every session. The authors claim that the freshness of these two values protects tags from being eavesdropped and tracked. However, this protocol cannot work without the synchronization of k_1 and k_2 between each tag and database. Moreover, the exposure of unique IDs in

the inventory response is contradictory to the security analysis of this protocol. This protocol also has the overhead of three AES encryption operations at the tag side using power induced from only one incoming RF signal.

III. RFID-enabled Extensible Authentication Framework

Each RFID application must meet with its security requirements according to its own goal, and various types of RFID tags used for the applications also have their own security features (*e.g.* encryption algorithms, hash functions, and PINs) as well as their technical features (*e.g.* radio frequencies, computational resources, and data I/O rates). Because each system implements a suitable authentication protocol based on the capacity of tags and the security goal, there exist many authentication protocols. However, this diversity in RFID systems isolates each application and restricts the extension of RFID systems. Therefore, we require an authentication framework to integrate different RFID applications with various security requirements, tags, and protocols into a single RFID authentication system. With an integrated RFID system using an authentication framework, it is easy to manage or extend the system, and the owner of an RFID tag can change its authentication method as they want. In this chapter, we define our RFID system architecture and design RFID-enabled Extensible Authentication Framework (REAF).

3.1 RFID System Architecture

An RFID system architecture consists of RFID tags, RFID readers, and a backend authentication server with DB. In this thesis, we use a term "a middleware" instead of a backend server because it connects RFID tags to RFID applications (e.g. EPC networks) in the middle layer. Usually, RFID authentication is done between a middleware and tags.

An RFID reader relays messages between tags and a middleware and does not necessarily concern credentials used in authentication methods and policy decision. The followings are our basic assumption and requirements for our REAF architecture in this thesis.

3.1.1 Assumptions

- **Pre-established secure channel**. A middleware authenticates RFID readers beforehand and establishes a secure channel with each reader via pre-shared key or current well-known security mechanism such as SSL/TLS. If a wired reader is attached to a host computer, the host computer is authenticated instead of the reader. In case of wireless/mobile readers (e.g. PDA), they can be authenticated after connected to WLAN securely using EAP method and WPA2.

- **Reliable transport of low layer**. The underlying air interface protocol covers unreliable transport more than an expected level so that it guarantees a high probability of successful detection. Class 1 Generation 2 UHF Air Interface Protocol Standard provides higher reliability in radio communications and collision avoidance than previous RFID air interface.

- **Random anti-collision identifier**. We also assume that any anti-collision mechanism can be used for RFID air interface as long as they use random IDs instead of UIDs to protect tags from being tracked, such as "Q" protocol in EPC Gen2 specification [1].

3.1.2 Requirements

- **Multiple instances in the tags**. Tags can store the instances of authentication protocols and distinguish them. In order to sup-

port multiple readers, each of multiple states is maintained in the memory of tags until the authentication processes is finished. Because the lack of memory, instances are stored in the memory circularly (*e.g.* round robin queuing).

- **Timer-driven authentication in the middleware**. A middleware maintains each instance from each valid response on a timer-driven basis because multiple tags can respond to a request message. The terminated instances are discarded.

- **Pass-through behavior**. RFID readers act as "pass-through agents" without authentication method layer functionalities so that they are compatible with multiple authentication methods.

- **Mutual authentication support**. Authentication framework should support mutual authentication as well in order to prevent the accesses from unauthorized readers.

- **Authentication method negotiation**.To support multiple authentication methods, negotiation should be provided in the framework.

- **Logging supports**. A middleware stores event logs such as authentication failures and ownership transfer so that it can detect attacks or manage the system effectively.

3.2 EAP and Its Limitation in RFID Systems

The RFID system architecture is very similar to the WLAN architecture. First, they are using RF signal to communicate between RFID tags and readers; and between access points (APs) and supplicants.

Moreover, readers and APs are the interfaces of the RFID applications and Internet services respectively. Mutual authentications in WLANs are performed between an authentication server (e.g. RADIUS server) and supplicants not between APs and supplicants because of rogue AP problems. In the same manner, authentications can be done between a middleware and tags, and readers act as "pass-through agents" so that RFID readers do not need to concern credentials used in authentication methods and policy decision. This similarity makes us think Extensible Authentication Protocol (EAP) [17] to be probably adoptable to RFID systems.

EAP is usually used in wireless LANs but not limited to wireless LANs. It is, in fact, a universal authentication framework which can be used any network environment. It supports multiple authentication methods including vendor-specific methods. There are more than 40 authentication methods defined in RFCs. Each method takes different approaches to authenticate EAP peer only or both EAP peer and authenticator in mutual. EAP-MD5, LEAP, EAP-TLS, EAP-TTLS, PEAP are widely used in WLANs and they have different performances and security features using various cryptographic primitives. Through the EAP negotiation, a peer and an authenticator can choose an authentication method they want.

From this point of view, Dantu et al. [25] examined and evaluated existing EAP methods for RFID systems. However, they overlooked the main difference between WLANs and RFID systems. In WLAN, EAP methods are used in the IEEE 802.1X phase not only for authentication but also for generation of key materials. Using a key derived from IEEE 802.11i 4-way handshake, data can be encrypted. Unlike continuous data exchange in WLANs, passive RFID tags respond only when a reader requests in the authentication process. That means RFID systems do not need a key or key material for further continuous data

exchange. Moreover, there are some features they did not consider seriously when applying EAP to RFID systems. In the following items, we point out limitations of applying EAP into RFID systems.

Limitation

- **Bulk-reading capability**. In EAP, an authentication is performed with an EAP peer one-to-one, and each entity proceeds to the next authentication step synchronously, so-called "lock-step protocol." Unlike EAP, some RFID applications need bulk-reading capability. When a request is fired, a middleware should expect 0 or more responses from tags and keep authentication state per tag with timer.

- **Traceability and privacy issues**. An `Identity` (`Type 1`) exchange sent in cleartext is optional in EAP, but it is "recommended to be used primarily." On the other hand, in RFID systems, it is better to design a method-specific identity exchange not to expose the identity of tag, especially in consumer application. Because obtaining the identity of a tag is the only goal in RFID application, `Identity Type` should be used in the authentication method carefully.

- **Extremely low resources**. Passive RFID tags have extremely low power because they induce current from incoming RF signals. Because outgoing RF communication consumes the large portion of available power, the shorter packet length is more suitable for RFID applications. EAP is designed to provide 1020 octets of MTU (Maximum Transmission Unit) and fragmentation. However, the MTU size for RFID systems should be relatively small, and RFID cannot consider fragmentation.

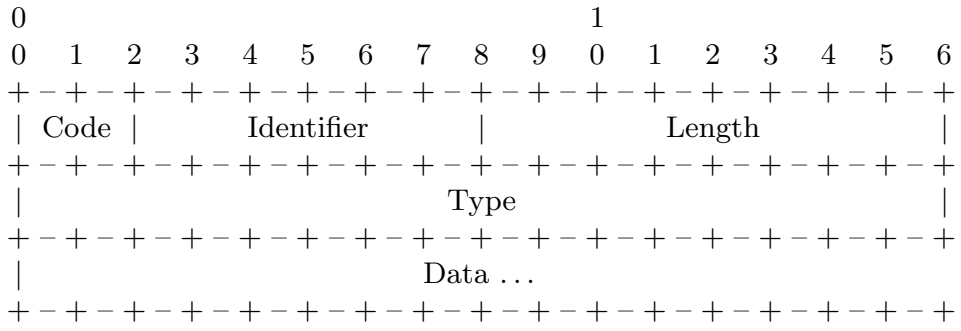

Figure 3.1: REAF Message Packet Format

3.3 Design of REAF based on EAP

The authentication process always starts from RFID reader's `Initiation` so as to be applied to passive RFID tags. A passive tag receives `Request` from the middleware, induces current needed to operate itself, and sends `Response` to the middleware via the reader. Except for the `Initiation` message, readers act as pass-through agents.

3.3.1 REAF Packet Format

As shown in Figure 3.1, the message packet format of proposed authentication framework is designed based on EAP. However, some fields are changed, and almost all the fields are shortened after considering the feature of RFID technology and the applicability of EAP to RFID applications.

The 2-bit `Code` field is assigned as shown in Table 3.1. The `Initiation` is sent only by a reader in order to initiate an REAF method. The `Initiation` does not have the `Type` and `Data` field. `Success` and `Failure` in EPC are combined into `Notification` and divided in the `Type` field. When a tag receives `Notification`, it can release the authentication instance in its memory.

Table 3.1: `Code` Field

0	`Initiation`
1	`Request`
2	`Response`
3	`Notification`

The `Identifier` field is the same as the EAP Identifier field except the length. Because this field has no cryptographic meaning, 6-bit long Identifier is enough to match Response packets with Request packets.

The `Length` field is the packet length in octets. This means the length of packet cannot exceed 255 bytes, which is long enough to be used for RFID applications.

Table 3.2: `Type` Field

0	`Identity` (Null authentication)
1	`Nak` (Response only)
2	`Success` (Notification only)
3	`Failure` (Notification only)
4 – 127	`Standard Types`
128 – 65535	`Vendor-specific Types`

An 16-bit `Type` field value (Table 3.2) is selected among 65536 values corresponding to the `Code` field. `Identity` is used for null authentication, which requests the Identity of tags but not authenticates them or which can be used with another authentication method. `Nak` is a type for authentication negotiation when a received `Type` of `Request` is not supported by a tag. `Success` or `Failure` notify whether a performed

authentication is done successfully or not. Other than these types, 124 defined standard authentication types and 65408 vendor-specific types can be supported. Whenever a vendor-specific type is used, the first 12 bits of `Type` indicate a globally unique `Vendor-ID` to specify which vendor's tag is used. This `Vendor-ID` can be supported upto 4088 vendors and each vendor can allocate 16 authentication methods to the last 4 bits of `Type` field.

Table 3.3: `Data` Field determined by `Type-Code`

`Type-Code`	`Data`
`Identity-Request`	0 octet
`Identity-Response`	ID (*e.g.* 12 octets for EPC)
`Nak-Response`	A set of `Type`s
	0 or $2t$ octets, where t = # of `Type`s
`Success-Notification`	optional commands to access a tag's memory
	(0 or more octets)
`Failure-Notification`	0 octet
`Type(4-255)-Request`	0 or more octets depending on the `Type`
`Type(4-255)-Response`	0 or more octets depending on the `Type`

The `Data` field is 0 or more octets depending on the `Code` and `Type` field. The `Data` field corresponding to each `Type-Code` case is shown in Table 3.3. The `Data` field of `Nak-Response` message is filled with authentication types that a tag wants to use. When there is no desired authentication types, `Nak-Response` will have 0 octet for the `Data` field. `Success-Notification` can include optional commands to access a tag's memory (*e.g.* to update a shared secret or a key, or to obtain additional information about the product).

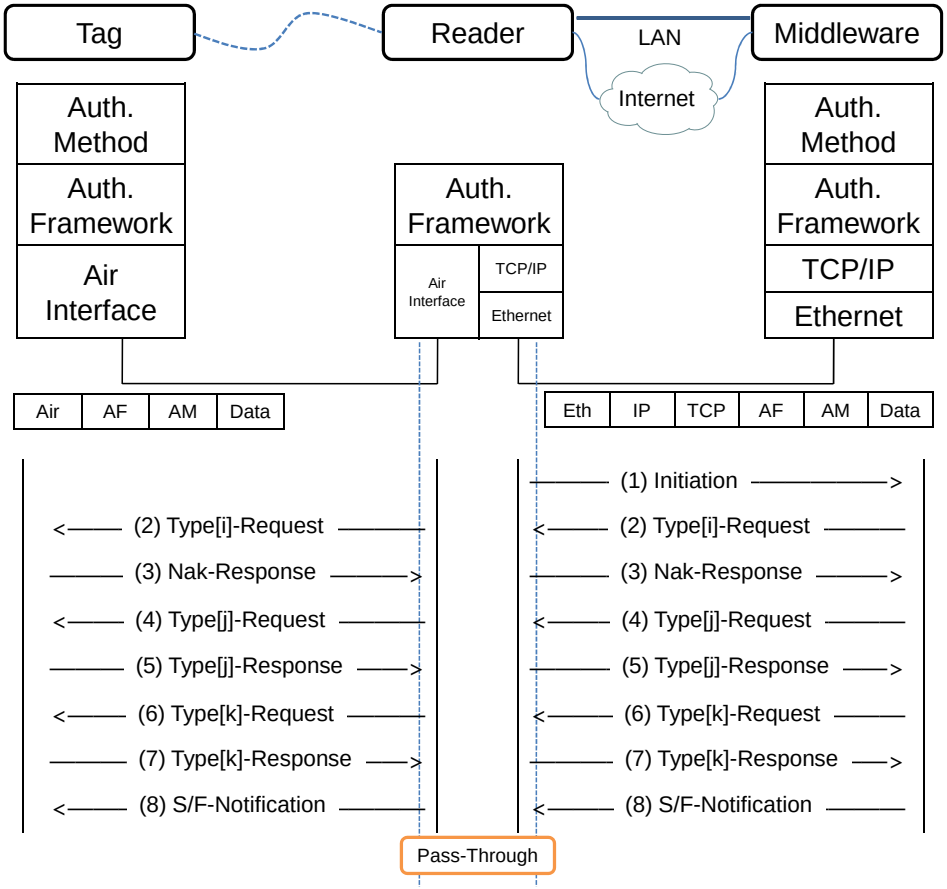

Figure 3.2: REAF and Authentication Flow

3.3.2 Authentication Flow

Figure 3.2 shows an RFID system. A tag and a middleware have three layers: authentication method (AM) layer, authentication framework (AF) layer, and underlying network layers. On the other hand, a reader has only two layers and bridges underlying network layers. Each layer encapsulates upper-layer data by adding header or footer. In our framework, AF header is `(Code, Identifier, Length)`, and AM header is `(Type)`.

The reader initiates a authentication session and drops or relays

packets between the tag and the middleware after checking the validity of AF header. For example, `Request` or `Notification` from the tag and `Response` from the middleware is invalid `Code` field. If the reader receives `Identifier` value that the reader has not initiated, the packet is should be discarded. Because the readers do not concern the `Type` and `Data`field, they are compatible with various authentication methods in REAF. A typical authentication flow of our proposed framework is as follows.

(1) $\mathcal{R}$ initiates an authentication by sending `Initiation` message to $\mathcal{M}$. `Identifier` value is incremented from the previous value.

(2) $\mathcal{M}$ starts the default authentication method, `Type`[i] where $i \in \{0, 4 : 255\}$. ($a : b = \{a, a + 1, \ldots, b\}$ where $a < b$)

(3) If the default authentication method, `Type`[i] is satisfied with $\mathcal{T}$, go to Step (5a) and assume $j = i$. Otherwise, $\mathcal{T}$ sends `Nak` = `Type`[1]. The `Data` field of `Nak` will be filled with authentication type set, $TypeSet$ where `Type`[1], `Type`[2], `Type`[3], `Type`[i] $\notin TypeSet$.

(4) $\mathcal{M}$ selects an element `Type`[j] $\in TypeSet$ and re-initiate authentication process. `Identifier` value is not incremented. Go to Step (5b).

(5a) $\mathcal{T}$ operates the `Type`[j] authentication method and responds with `Type`[j]-`Response`. `Type`[j] can be more than one round trip.

(5b) If $\mathcal{T}$ receives (4) with the same `Identifier` after sending (3), it responds to (4) with `Type`[j]-`Response`. Depending on the `Type`[j], (4)-(5) can be more than one round trip.

(6) (6)-(7) is not necessarily required, but another authentication type can be jointly used in this framework. Usually, in this case, `Type`[0]

= `Identity` is jointly used. $\mathcal{M}$ sends `Type`[k]-`Request` where $k \in \{0, 4 : 255\}, k \neq i$, and $k \neq j$. If $\mathcal{M}$ has received `Nak` message, $k \in TypeSet$ and $k \neq j$.

(7) $\mathcal{T}$ sends corresponding `Type`[k]-`Response` to (6). Depending on the `Type`[k], (6)-(7) is more than one round trip.

(8) If authentication fails in the middle of authentication, $\mathcal{M}$ sends `Failure-Notification` immediately. If authentication ends successfully, $\mathcal{M}$ sends `Success-Notification`.

In a session, if $\mathcal{T}$ receives `Type`[l]-`Request` with the same `identifier` before finishing `Type`[j] or Type[k] authentication, $\mathcal{T}$ drops the received `Type`[l]-`Request`, where $l \neq j$ and $l \neq k$.

Beacuse REAF supports bulk-reading using `identifier` and the timer, it is suitable for RFID applications. Also, REAF packet format is designed as compact as possible to support resource-constraint RFID tags. As a result, REAF can support multiple authentication methods only with 4-byte overhead.

IV. REAF Methods and Applications

In order to use our proposed authentication framework, specific REAF methods are required. Existing 3-party protocols can be transformed to REAF-conforming methods with our packet format as long as readers act as pass-through agents in the protocols. In this chapter we present typical authentication methods as examples, using two different cryptographic primitives such as a hash function and a block cipher algorithm. Although our methods are designed for REAF, they can be independently adoptable to RFID applications regardless of the adoption of REAF.

Our REAF methods can be used in the heterogeneous RFID applications. For example, we can authenticate daily necessaries with a REAF-HF or a REAF-BC-TA method while expensive valuables are authenticated with a REAF-BC-OA1 or a REAF-BC-OA2 method.

4.1 REAF-HF

In this section, we propose a REAF method using a hash function, where HF $\in$ {MD4, MD5, SHA-1, SHA-256, $\cdots$}. Any affordable hash functions for RFID tags can be used as REAF-HF methods. For example, REAF-SHA1 means an authentication method using SHA-1 which conforms to REAF specification.

4.1.1 Protocol

The REAF-HF authentication method is designed based on EAP-MD5. It needs a pre-distributed shared secret (*e.g.* a password). Figure 4.1 shows REAF-HF authentication method flow, where $len(ID_{\mathcal{T}}) = 96$

bits, $len(Secret) = 128$ bits, and $len(RND_{\mathcal{M}}) = 32$ bits. A middleware successfully authenticate tags when the received hashed value is equal to the value calculated by the middleware itself.

$\mathcal{R} \rightarrow \mathcal{M}$	: `Initiation`	
$\mathcal{T} \leftarrow \mathcal{R} \leftarrow \mathcal{M}$	: `Identity-Request`	
$\mathcal{T} \rightarrow \mathcal{R} \rightarrow \mathcal{M}$	: `Identity-Response`	$ID_{\mathcal{T}}$
$\mathcal{T} \leftarrow \mathcal{R} \leftarrow \mathcal{M}$	: `HF-Request`	$RND_{\mathcal{M}}$
$\mathcal{T} \rightarrow \mathcal{R} \rightarrow \mathcal{M}$	: `HF-Response`	$\text{Hash}(ID_{\mathcal{T}}\|\|Secret\|\|RND_{\mathcal{M}})$
$\mathcal{T} \leftarrow \mathcal{R} \leftarrow \mathcal{M}$	: `Notification`	

Figure 4.1: REAF-HF Authentication Method

4.1.2 Analysis

In this subsection, we analyze the security of REAF-HF comparing with other hash-based authentication schemes. Table 4.1 shows the summarized result of comparison. In REAF-HF, the authentication phase is performed after a tag sends its ID in plaintext. Because of this ID exposure, tags are traceable. Still, this is secure against eavesdropping, replay, and spoofing attack due to hashed value of $Secret$ and $RND_{\mathcal{M}}$ and thus applicable to supply chains.

REAF-HF is as simple as HL [14] but prevents replay attacks and tags spoofing. RHL [14] and HC [19] are only feasible for owners of a relatively small number of tags because of the scalability problem. Moreover, they are still vulnerable to replay and spoofing attacks. HIDV [20] provides ID anonymity, but this scheme does not work if the DB is desynchronized. It also requires two more hash operations on the tag than REAF-HF. If the RFID application does not require to protect the ID of tags, REAF-HF can be a reasonable authentication method.

Table 4.1: Comparison with other Hash-based Authentication Schemes

Security Requirements	HL [14]	RHL [14]	HC [19]	HIDV [20]	REAF-HF
ID anonymity	X	△	O	O	X
Untraceability	X	△	O	X	X
Replay attack	X	X	X	O	O
Tag spoofing	X	X	X	O	O
Retrieval from DB	$O(1)$	$O(n)$	$O(n)$	$O(1)$	$O(1)$
Hash operations on $\mathcal{M}$	0	$O(n)$	$O(mn)$	4	1
Hash operations on $\mathcal{T}$	1	1	2	3	1
Synchronization	-	-	-	X	-

O The protocol satisfies the security requirement or it is secure against the attack.
X The protocol does not satisfy the security requirement or it is vulnerable to the attack.
△ The protocol partially satisfies the security requirement.
– The protocol does not require the requirement.
n The number of DB entries
m The number of previous transactions

4.2 REAF-BC

In this section, we propose three REAF methods using a block cipher, where BC ∈ {DES, AES, mCrypton, HIGHT, PRESENT, TEA, $\cdots$}. Any affordable block ciphers for RFID tags can be used as REAF-BC methods. For example, a REAF-AES method means an authentication method using AES which conforms to REAF specification.

4.2.1 Protocols

REAF-BC-TA: Tag Authentication with Identity Type

A unilateral tag authentication with `Identity Type` is shown in Figure 4.2. REAF-BC-TA assumes that $K_{\mathcal{TM}}$ is established securely before

authentication is placed. This authentication is initiated by `Identity-Request` from $\mathcal{M}$ to get $ID_{\mathcal{T}}$. After receiving `Identity-Response`, $\mathcal{M}$ can retrieve corresponding $K_{\mathcal{TM}}$ from its database. Using $K_{\mathcal{TM}}$, $\mathcal{T}$ encrypts $ID_{\mathcal{T}}||RND_{\mathcal{M}}$, and $\mathcal{M}$ authenticates $\mathcal{T}$ by decrypting the encrypted block of `BC-TA-Response`. If $\mathcal{M}$ succeeds in authentication, $\mathcal{M}$ sends `Success-Notification`, otherwise sends `Failure-Notification`. In case of REAF-AES with EPC tags whose ID length is 96 bits, only one-block encryption is required in this authentication, where $RND_{\mathcal{M}} \in {}_{R}\{0,1\}^{32}$. Note that REAF-BC-TA requires only one encryption at the tag side which is affordable for low-cost RFID tags.

$\mathcal{R} \rightarrow \mathcal{M}$	: `Initiation`	
$\mathcal{T} \leftarrow \mathcal{R} \leftarrow \mathcal{M}$	: `Identity-Request`	
$\mathcal{T} \rightarrow \mathcal{R} \rightarrow \mathcal{M}$	: `Identity-Response`	$ID_{\mathcal{T}}$
$\mathcal{T} \leftarrow \mathcal{R} \leftarrow \mathcal{M}$	: `BC-TA-Request`	$RND_{\mathcal{M}}$
$\mathcal{T} \rightarrow \mathcal{R} \rightarrow \mathcal{M}$	: `BC-TA-Response`	$E_{K_{\mathcal{TM}}}(ID_{\mathcal{T}}\|\|RND_{\mathcal{M}})$
$\mathcal{T} \leftarrow \mathcal{R} \leftarrow \mathcal{M}$	: `Notification`	

Figure 4.2: REAF-BC-TA Authentication Method

REAF-BC-OA1: Tag Owner Authentication

Another unilateral authentication method, REAF-BC-OA1 authenticates $\mathcal{O}$, not $\mathcal{T}$. $\mathcal{M}$ preshares a key, $K_{\mathcal{OM}}$ with the owner of tag, $\mathcal{O}$. Therefore this method can be useful when the only owner of tags can access tags and reject others' requests. Usually, $\mathcal{O}$ has their own RFID system or has an access right to other RFID systems.

Figure 4.3 shows the authentication steps of REAF-BC-OA1. Authentication is initiated by `BC-OA1-Request` with $RND_{\mathcal{M}}$. Then $\mathcal{T}$ calculates $E_{K_{\mathcal{OM}}}(ID_{\mathcal{T}}||(RND_{\mathcal{M}} \oplus RND_{\mathcal{T}}))$ and sends it with $RND_{\mathcal{T}}$.

On receiving `BC-OA1-Response`, $\mathcal{M}$ decrypts $ID_{\mathcal{T}}$ and verify whether the last 32-bit of the decrypted block is $RND_{\mathcal{R}} \oplus RND_{\mathcal{T}}$.

$\mathcal{R} \rightarrow \mathcal{M}$	: `Initiation`	
$\mathcal{T} \leftarrow \mathcal{R} \leftarrow \mathcal{M}$	: `BC-OA1-Request`	$RND_{\mathcal{M}}$
$\mathcal{T} \rightarrow \mathcal{R} \rightarrow \mathcal{M}$	: `BC-OA1-Response`	$E_{K_{\mathcal{OM}}}(ID_{\mathcal{T}}\|\|(RND_{\mathcal{M}} \oplus RND_{\mathcal{T}}))\|\|RND_{\mathcal{T}}$
$\mathcal{T} \leftarrow \mathcal{R} \leftarrow \mathcal{M}$	: `Notification`	

Figure 4.3: REAF-BC-OA1 Authentication Method

REAF-BC-OA2: Mutual Authentication

REAF-BC-OA2 is a mutual authentication method extending REAF-BC-OA1. REAF-BC-OA2 assumes that $\mathcal{T}$ can get enough power to operate two block cipher encryptions in the process of verifying the fourth REAF message and constructing the fifth message in Figure 4.4. $\mathcal{T}$ sends its $ID_{\mathcal{T}}$ in encrypted form only after a successful 3-round authentication between $\mathcal{T}$ and $\mathcal{M}$. If $\mathcal{M}$ receives the invalid `BC-OA2-Response`, $\mathcal{M}$ stops the authentication and sends `Failure-Notification` immediately.

$\mathcal{R} \rightarrow \mathcal{M}$	: `Initiation`	
$\mathcal{T} \leftarrow \mathcal{R} \leftarrow \mathcal{M}$	: `BC-OA2-Request`	$RND_{\mathcal{M}}$
$\mathcal{T} \rightarrow \mathcal{R} \rightarrow \mathcal{M}$	: `BC-OA2-Response`	$E_{K_{\mathcal{OM}}}(RND_{\mathcal{M}}\|\|RND_{\mathcal{T}})$
$\mathcal{T} \leftarrow \mathcal{R} \leftarrow \mathcal{M}$	: `BC-OA2-Request`	$E_{K_{\mathcal{OM}}}(RND_{\mathcal{T}}\|\|RND_{\mathcal{M}})$
$\mathcal{T} \rightarrow \mathcal{R} \rightarrow \mathcal{M}$	: `BC-OA2-Response`	$E_{K_{\mathcal{OM}}}(ID_{\mathcal{T}}\|\|RND_{\mathcal{T}})$
$\mathcal{T} \leftarrow \mathcal{R} \leftarrow \mathcal{M}$	: `Notification`	

Figure 4.4: REAF-BC-OA2 Authentication Method

4.2.2 Analysis

Security Properties of REAF-BC Methods

Table 4.2 summarizes the security properties of three authentication methods. In REAF-BC-TA, the authentication phase is performed after $\mathcal{T}$ sends its ID, $ID_{\mathcal{T}}$ in plaintext. Because of this ID exposure, tags are traceable. Still, this is secure against replay and spoofing attack due to the secret key, $K_{\mathcal{TM}}$ and the freshness of $RND_{\mathcal{M}}$. Therefore it is applicable to supply chains.

Unlike REAF-BC-TA, REAF-BC-OA1 authenticates $\mathcal{O}$, not $\mathcal{T}$. Due to this property, it is possible for $\mathcal{O}$ to spoof $ID_{\mathcal{T}}$. Nevertheless, this method can be used if there is no benefit for the owner from deceiving the IDs of tags. In this method, $ID_{\mathcal{T}}$ is protected from eavesdropping, and $RND_{\mathcal{T}}$ makes $\mathcal{T}$ untraceable even with fixed $RND_{\mathcal{M}}$. Because REAF-BC-OA1 provides ID hiding and untraceability, it is suitable to consumer applications.

In REAF-BC-OA2, $\mathcal{T}$ sends its $ID_{\mathcal{T}}$ in encrypted form only when $\mathcal{T}$ and $\mathcal{M}$ authenticate each other successfully. Therefore, it can be used in more secure applications. $RND_{\mathcal{T}}$ in the fifth message ensures untraceability.

In case of REAF-AES with EPC tags and $RND \in_R \{0,1\}^{32}$, all these methods are utilizing one-block encryption of AES at the tag side. For further access to a tag, it is better to have block cipher decryption on tags. OFB (Output FeedBack), CFB (Cipher FeedBack), and CTR (Counter) modes use the same encryption of block cipher when decrypting. Thus, tags can decrypt messages if one of these three modes of operations is implemented in the tags. In fact, they are identical when the plaintext size is equal to or less than one block.

Table 4.2: Security Properties of REAF-BC Methods

Security Requirements	TA	OA1	OA2
ID anonymity	X	O	O
Untraceability	X	O	O
Integrity protection	O	O	O
Tag authentication	O	X	X
Owner authentication	X	O	O
Middleware authentication	X	X	O
Secure against Replay attack	O	O	O
Secure against Tag Spoofing	O	X	X

O The protocol satisfies the security requirement.
X The protocol does not satisfy the security requirement.

Comparison with Other RFID Authentication Protocols using AES

Table 4.3 shows comparison between REAF-BC methods and other RFID authentication protocols using a block cipher. Because AES is one of representative block ciphers currently used for RFID authentication protocols, we consider only authentication protocols using AES presented in Related Work. We omit [3] from comparison because it is similar to Protocol 1 in [2].

Protocol 1, 2, 3, and 4 in [2] need one or two AES encryption operations on $\mathcal{T}$ for unilateral or mutual authentication respectively. Protocol 5 requires one AES decryption which is not implemented in practice. When different secret keys for different product classes are used instead of a global key, $\mathcal{M}$ needs $O(n)$ operations to find a correct key if additional bytes are not provided, where n is the number of product classes.

In [9], an initial inventory request is needed for anti-collision. But

Table 4.3: Comparison with other AES Authentication Protocols

	[2]	[9]	REAF-AES
AES Operations on $\mathcal{T}$	E 2E E+D	3E	E 2E
Retrieval from $\mathcal{M}$'s DB	$O(1)$ $O(n)$	$O(1)$	$O(1)$
Synchronization	-	X	-
REAF method	X	X	O

O	The protocol satisfies the property.	E	AES encryption
X	The protocol does not satisfy the property.	D	AES decryption
–	The protocol does not require the property.	n	The number of DB entries

due to the unique IDs in the inventory response, [9] cannot provide tag anonymity and untraceability as they claim. Moreover, this protocol requires three consecutive AES encryptions at the tag side, which might be incapable in passive tags. Desynchronization is another problem of [9].

Similarly to [2], REAF-AES methods require one or two AES encryptions on $\mathcal{T}$ and O(1) operations on $\mathcal{M}$. Our proposed authentication methods have a meaning in that they are designed for REAF, which can flexibly integrate heterogeneous RFID applications. Not only these three REAF-AES methods but also other authentication methods designed for REAF can be used in a single RFID system together. This property can provide flexibility for RFID systems in terms of cost-security tradeoffs.

4.3 Applications

In this section, we describe how REAF methods can be used to practical applications. Assume that a distributor $\mathcal{D}$ ordered an RFID-tagged product which can support REAF-BC authentication methods. When $\mathcal{D}$ takes over the product from a supplier $\mathcal{S}$, $\mathcal{S}$ authenticates the item from $\mathcal{S}$'s middleware using REAF-BC-TA with $K_{\mathcal{TS}}$, where $K_{\mathcal{TS}}$ is a shared key between $\mathcal{T}$ (the tag on the item) and $\mathcal{S}$'s middleware. In the process of authentication, $\mathcal{D}$ populates its middleware DB (e.g. EPCIS Repository [10]) with [$ID_{\mathcal{T}}$, $K_{\mathcal{TD}}$, OtherProductRelatedInfo], where $K_{\mathcal{TD}}$ is a new shared key between $\mathcal{T}$ and $\mathcal{D}$'s middleware. Then $\mathcal{S}$ safely transfers $\mathcal{T}$'s ownership to $\mathcal{D}$ updating the key in $\mathcal{T}$ from $K_{\mathcal{TS}}$ to $K_{\mathcal{TD}}$ after `Success-Notification`.

When a customer $\mathcal{C}$ checks out the item to buy, $\mathcal{D}$ authenticates the item from $\mathcal{D}$'s middleware using REAF-BC-TA with $K_{\mathcal{TD}}$. After payment, $\mathcal{D}$ disables $\mathcal{T}$ for REAF-BC-TA and transfers $\mathcal{T}$'s ownership to $\mathcal{C}$ updating the key in $\mathcal{T}$ from $K_{\mathcal{TD}}$ to $K_{\mathcal{CH}}$, where $K_{\mathcal{CH}}$ is a shared key between $\mathcal{C}$ and a middleware in $\mathcal{C}$'s home network RFID system. Then $\mathcal{D}$ can move the item entry in the DB to other tables for inventory control or sales record.

Now, $\mathcal{C}$ brings the item to $\mathcal{C}$'s home. On the way to $\mathcal{C}$'s home, adversaries cannot know what $\mathcal{C}$ bought by scanning, because REAF-BC-TA is disabled. $\mathcal{C}$ can identify the item using REAF-BC-OA1 or REAF-BC-OA2 in $\mathcal{C}$'s home with any readers connected to $\mathcal{C}$'s home network middleware and get useful information about the item from $\mathcal{S}$'s DB if $\mathcal{C}$ has the access right to $\mathcal{S}$'s DB (e.g. through EPCIS Query Interface and EPCIS Accessing Application [10]). Or $\mathcal{C}$ can register $K_{\mathcal{CH}}$ to $\mathcal{S}$'s DB and directly authenticates $\mathcal{T}$ to access $\mathcal{S}$'s DB anywhere with a mobile RFID reader.

In this example, many REAF-BC methods can be used in an RFID

system. REAF can support any REAF-BC methods using different block ciphers (*e.g.* REAF-AES, REAF-mCrypton, REAF-HIGHT, and etc.). $\mathcal{S}$ does not have to fix its authentication method. $\mathcal{S}$ can select an REAF-BC method considering security requirements and levels of target applications. Not only REAF-BC but also REAF-HF methods are applicable under our propose authentication framework. Our REAF integrates heterogeneous RFID systems using different authentication methods into a single RFID system.

V. Conclusion

In this thesis, we propose a novel authentication framework suitable for RFID systems. With our proposed REAF, various types of tags and authentication methods will be integrated into a single authentication system so that it can be easy to manage or extend the RFID system. Moreover, the owner of a tag can make the tag to use a specific authentication method appropriate for their application after ownership is transferred.

We also analyze the existing RFID authentication protocols and propose new authentication methods for REAF using two different cryptographic primitives such as a hash function and a block cipher algorithm. REAF-HF method designed for logistical RFID applications is simple but prevents replay attacks and tags spoofing. It also solves the scalability problems of previous hash-based authentication protocols and does not require the synchronization of DB. Three kinds of REAF-BC methods provide different security properties for REAF. REAF-BC-TA authenticates tags with `Identity Type` and can be also useful for logistical RFID applications. Because REAF-BC-OA1 and REAF-BC-OA2 can protect owner's privacy, they are suitable for consumer applications.

Finally, we describe how REAF methods can be used to practical applications. Each of our REAF methods has different security properties and is flexibly applicable to logistical or consumer applications in REAF. We can select an REAF method considering security requirements and levels of target applications without considering interoperability. Consequently, we can expect that RFID systems using REAF will provide much better integrated services and improve the quality of our life.

For the further research, we will demonstrate our proposed authentication framework through an implementation and verify its wide appli-

cability. We also need to clarify optional commands with `Success-Notification` and research ownership transfer in REAF.

RFID 시스템을 위한 확장가능 인증 프레임워크와 응용

지성배

최근 다양한 RFID 응용이 개발되고 연구되고 있는 반면에 개인적 자유의 침해, 태그의 위변조와 같은 보안 문제들이 제기되고 있다. 많은 종류의 인증 프로토콜이 이러한 보안 문제들을 해결하기 위해 제안되었지만 다양한 RFID 응용에 적용할 수 있는 범용의 인증 프로토콜이 없기 때문에 서로 다른 보안 요구사항과 인증 프로토콜을 가진 이종의 RFID 시스템 통합하는 것이 어렵다.

본 논문은 새로운 RFID 인증 프레임워크를 제안한다. 제안된 RFID 시스템을 위한 확장가능 인증 프레임워크 (REAF: RFID-enabled Extensible Authentication Framework)는 업체 고유의 인증 방식을 포함한 어떠한 인증 방식이라도 지원하므로, 다양한 보안 요구사항과 다양한 종류의 태그와 인증 프로토콜을 가진 서로 다른 RFID 응용들을 하나의 RFID 인증 시스템으로 통합 가능하게 한다. REAF를 사용하여 RFID 시스템을 통합하면, 시스템을 관리하고 확장하기 쉽고 RFID 태그의 소유자가 원하는 인증 방식을 선택하여 사용할 수 있다.

제안된 인증 프레임워크를 사용하기 위해서는 특정 인증 방식이 필요하다. 그러므로 본 논문은 두 가지 다른 암호학적 프리미티브 즉, 해쉬 함수와 블록 암호화 알고리즘을 사용한 전형적인 인증 방식을 예제로 제시한다.

REAF-HF 방식은 태그의 ID를 보호할 필요가 없는 물류 RFID 응용을 위해 설계한 REAF 인증 방식으로서 RFID 태그에 적용 가능한 어떠한 해쉬 함수라도 사용될 수 있다. REAF-HF는 인증 절차가 간단하지만 재전송 공격과 태그의 스푸핑을 막을 수 있고 DB의 동기화가 필요하지 않다는 장점을 가진다.

REAF를 위한 세 가지 종류의 REAF-BC 인증 방식은 보안상 서로 다른 특징을 제공한다. REAF-BC-TA는 REAF-HF와 마찬가지로 `Identity Type` 요청/응답과 함께 태그를 인증하므로 물류 RFID 응용에 유용하게 쓰일 수 있다. REAF-BC-OA1은 태그의 소유자를 인증하고, REAF-BC-OA2는 이를 상호 인증으로 확장한다. REAF-BC-OA1와 REAF-BC-OA2는 태그 소유자의 사생활을 보호할 수 있으므로 소비자를 위한 RFID 응용에 적합하다. 제안한 REAF-BC 인증 방식들은 기존에 제안된 블록 암호화를 이용한 RFID 인증 프로토콜 이상의 보안과 성능을 보인다.

제안한 모두 네 가지 REAF 인증 방식들은 REAF를 위해 설계되었다는 점에서 의의를 가진다. 서로 다른 보안 요구사항의 충족을 목표로 설계된 각각의 REAF 인증 방식은 통합된 RFID 시스템에서 함께 사용될 수 있다. 또한 보안 요구사항과 보안 수준을 고려하여 REAF 인증 방식을 선택할 수 있으므로, 비용과 보안이 상충적이라는 점에서 유연한 RFID 시스템을 구축 가능하게 한다.

References

1. EPCglobal Inc, EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.0.9, Jan 2005.

2. Sandra Dominikus, Elisabeth Oswald, and Martin Feldhofer, Symmetric Authentication for RFID Systems in Practice, Handout of the *Ecrypt Workshop on RFID and Lightweight Crypto*, Jul, 2005.

3. Martin Feldhofer, An Authentication Protocol in a Security Layer for RFID Smart Tags, *The 12th IEEE Mediterranean Electrotechnical Conference - MELECON 2004*, vol. 2, pp. 759-762, May 2004.

4. Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, Strong Authentication for RFID Systems Using the AES Algorithm, *Workshop on Cryptographic Hardware and Embedded Systems - CHES 2004*, LNCS 3156, pp. 357-370, Aug 2004.

5. Martin Feldhofer and Johannes Wolkerstorfer, Strong Crypto for RFID Tags - A Comparison of Low-Power Hardware Implementations, *The IEEE International Symposium on Circuits and Systems*, pp. 1839-1842, 2007.

6. Martin Feldhofer, Johannes Wolkerstorfer and Vincent Rijmen, AES implementation on a grain of sand, *IEE Proceedings on Information Security*, vol. 152, pp. 13-20, Oct 2005.

7. Sungbae Ji, Hyunrok Lee, Sungjune Yoon, and Kwangjo Kim, An Authentication Framework for Integrating RFID Systems, Auto-ID Labs White Paper WP-SWET-025, Oct 2007.

8. Jens-Peter Kaps and Berk Sunar, Energy Comparison of AES and SHA-1 for Ubiquitous Computing, *Embedded and Ubiquitous Computing (EUC-06) Workshop Proceedings*, LNCS 4097, pp. 372-381, Aug 2006.

9. Batbold Toiruul and KyungOh Lee, An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems, International Journal of Computer Science and Network Security, vol. 6, pp. 156-162, Sep 2006.

10. Ken Traub, Greg Allgair, Henri Barthel, Leo Burstein, John Garrett, Bernie Hogan, Bryan Rodrigues, Sanjay Sarma, Johannes Schmidt, Chuck Schramek, Roger Stewart, and KK Suen, The EPCglobal Architecture Framework, EPCglobal Inc, Jul 2005.

11. Chae Hoon Lim and Tymur Korkishko, mCrypton - A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors, *WISA 2005*, LNCS 3786, pp. 243-258, 2006.

12. Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bonseok Koo, Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek Chee, HIGHT: A New Block Cipher Suitable for Low-Resource Device, *CHES 2006*, LNCS 4249, pp. 46-59, 2006.

13. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe, HIGHT: PRESENT: An Ultra-Lightweight Block Cipher, *CHES 2007*, LNCS 4727, pp. 450-466, 2007.

14. Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels, Security and Privacy Aspects of Low-Cost Radio Fre-

quency Identification Systems, *Security in Pervasive Computing - SPC 2003*, LNCS 2802, pp. 201-212, 2004.

15. Ted Phillips, Tom Karygiannis, and Rick Kuhn, Security Standards for the RFID Market, Security & Privacy Magazine, IEEE, vol. 3, no. 6, pp. 85-89, Nov-Dec. 2005.

16. Ari Juels, Strengthening EPC Tags Against Cloning, *ACM Workshop on Wireless Security (WiSe)*, pp.67-76. 2005.

17. Bernard Aboba, Larry J. Blunk, John R. Vollbrecht, James Carlson, and Henrik Levkowetz, Extensible Authentication Protocol (EAP), RFC 3748, IETF, 2004.

18. Ari Juels and Ravikanth Pappu, Squealing Euros: Privacy Protection in RFID-Enabled Banknotes, LNCS 2742, pp. 103-121, 2003.

19. Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita, Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID, *Proceedings of the SCIS 2004*, pp.719-724, 2004.

20. Dirk Henrici and Paul Müller, Hash-Based Enhancement of Location Privacy For Radio-Frequency Identification Devices Using Varying Identifiers, *PerSec*, 2004.

21. Sanjay Sarma, Stephen Weis, and Daniel Engels, Radio-Frequency Identification: Security Risks and Challenges, Cryptobytes, RSA Laboratories, 2003.

22. István Vajda and Levente Buttyán, Lightweight Authentication Protocols for Low-cost RFID tags, *Workshop on Security in Ubiquitous Computing*, 2003.

23. ISO/IEC 14443-2, Identification cards - Contactless integrated circuit(s) cards - Proximity cards (PICCS) - Part 2: Radio frequency power and signal interface, 2001.

24. ISO/IEC 15693-2, Identification cards - Contactless integrated circuit(s) cards - Vicinity cards (VICCs) - Part 2: Air interface and initialisation, 2000.

25. Ram Dantu, Gabriel Clothier, and Anuj Atri, EAP Methods for Wireless Networks, Computer Standards & Interfaces 29, pp. 289-301, 2007.

26. Dario Carluccio, Kerstin Lemke-Rust, Christof Paar, and Ahmad-Reza Sadeghi, E-Passport: The Global Traceability or How to Feel Like an UPS Package, *WISA 2006*, LNCS 4298, pp. 391-404, 2007.

27. Martin Feldhofer and Christian Rechberger, A Case against Currently Used Hash Functions in RFID Protocols, *OTM Workshops 2006*, LNCS 4277, pp. 372-381, 2006.

Acknowledgement

This thesis is the result of two-year work in ICU. During my graduate study, I have been accompanied and supported by many people. This thesis could not have been written without their advices and encouragement. Now, I am happy to have the opportunity to express my gratitude for all of them.

First of all, I would like to express my deep and sincere gratitude to my advisor, Prof. Kwangjo Kim, for his constant direction and support during my research. His encouraging and kind guidance have provided a good basis for the present thesis. Special thanks also go to Prof. Young-Hee Lee and Prof. Byoungcheon Lee for their generosity as advisory committee members.

Furthermore, I would like to thank all my lab buddies at the Cryptography & Information Security Laboratory: Liem, Divyan, Hyunrok, Duc, Zeen, Kyusuk, Jangseong, Sungjune, Minhea, Hanyoung, Hyeran, and Hyewon. They have inspired me in research and life through our long hours in the lab. I also thank an old boy, Youngjoon for advice on my research and a new boy, Imsung for his kindness.

사랑하는 우리 가족에게도 항상 믿어줘서 고맙다는 말을 전합니다. 부족한 아들에게 언제나 관심과 믿음을 주신 부모님. 대전에 나와 살면서 전화도 자주 드리지 못해서 미안해요. 졸업 후에는 부모님께 넘치게 받은 사랑 돌려 드릴게요. 지금 혼자 캐나다에서 외로워하고 있을 누나. 오히려 내 안부를 묻고 응원을 해줘서 고마워. 곧 돌아올 테니 힘내. 석사 선배 우리 형. 내가 2년 전 형이 걸었던 그 힘든

길을 걷고 보니 너무 존경스러워. 지금 준비하고 있는 새로운 도전이 성공하길 바래. 우리 가족 모두 사랑합니다! 고맙습니다!

Last but not least, I would like to thank all people who have helped and inspired me during my graduate study. I will always remember invaluable two years with our great C&IS lab members at ICU. You complete me.

Curriculum Vitae

Name : Sungbae Ji

Date of Birth : October. 1. 1980

Sex : Male

Nationality : Korean

Education

1999.03–2004.02	Computer Engineering Ajou University (B.E.)
2006.02–2008.02	Cryptography and Information Security, Engineering Information and Communications University (M.S.)

Career

2006.04–2006.11	Graduate Research Assistant Research on the Key Predistribution Scheme for Wireless Sensor Networks National Security Research Institute (NSRI)
2006.05–2006.11	Graduate Research Assistant A Research on Key Recovery Technique for VoIP Korea Information Security Agency (KISA)

2006.08–2006.12	Graduate Research Assistant Research on Security Technology in Ubiquitous-Web Platform KT Future Technology Lab
2006.07–2007.06	Graduate Research Assistant A Study on the ID-Based Encryption (IBE) and Its Application in 4G. Network Samsung-ICU Research Center
2006.12–2007.12	Graduate Research Assistant Research and Development of Next Generation DRM SK Telecom
2007.03–2007.12	Graduate Research Assistant Development of Cyber Security Policy Standard for Digital I&C System Korea Institute of Nuclear Safety (KINS)
2007.03–2007.12	Graduate Research Assistant Development of Sensor Tag and Sensor Node Technologies for RFID/USN Ministry of Information and Communication (MIC) Institute for Information Technology Advancement (IITA)
2007.06–2007.08	Internship Research A Study on Security Application using Window Filter Driver MarkAny Inc.

Publications

(1) 2007.02 지성배, 이현록, 김광조, "대학 무선 랜에 적용되는 새로운 확장 가능 인증 프로토콜," 2007년도 한국정보보호학회 영남지부 학술발표회논문집, 2007.2.23, 대구한의대, 대구.

(2) 2007.08 Sungjune Yoon, Hyunrok Lee, Sungbae Ji and Kwangjo Kim, "A User Authentication Scheme with Privacy Protection for Wireless Sensor Networks," *The 2nd Joint Workshop on Information Security*, 6-7 Aug 2007, Tokyo, Japan.

(3) 2007.10 Sungbae Ji, Hyunrok Lee, Sungjune Yoon, and Kwangjo Kim, "An Authentication Framework for Integrating RFID Systems," 10 Oct 2007, Auto-ID Labs Whitepaper.

(4) 2007.10 지성배, 이현록, 윤성준, 김광조, "전자태그 시스템을 위한 인증 프레임워크의 요구 사항," 2007년도 한국정보보호학회 충청지부 학술발표회논문집, 2007.10.12, 한국기술교육대학교, 천안.

(5) 2007.12 지성배, 김광조, "ICAO 규격 전자여권의 보안 문제 조사 분석," 2007년 한국정보보호학회 동계학술대회논문집, 2007.12.1, 상명대학교, 서울.

(6) 2007.12 한규석, 지성배, 김광조, "ID 기반 암호 기술을 이용한 VoIP 보안 서비스 설계 및 구현," 2007년 한국정보보호학회 동계학술대회논문집, 2007.12.1, 상명대학교, 서울.

(7) 2008.01 Sungbae Ji, Zeen Kim, Kwangjo Kim "Design of an RFID-embedded e-ID System for Privacy Protection," To appear in the Proc. of *The 2008 Symposium on Cryptography and Information Security*, 22-25 Jan 2008, Miyazaki, Japan.