단계적 키 변환을 이용한 RFID 상호 인증 프로토콜

정회원 정 경 호*, 준회원 김 경 률*, 오 세 진*, 정회원 이 재 강*, 박 용 수*, 안 광 선*

A Mutual Authentication Protocol using Key Change Step by Step for RFID Systems

Kyung-Ho Chung* *Regular Member*, Kyoung-Youl Kim*, Se-Jin Oh* *Associate Members*,
Jae-Kang Lee, Yong-Soo Park*, Kwang-Seon Ahn* *Regular Members*

요 약

RFID(Radio-Frequency IDentification) 시스템은 개인 정보의 노출 및 위치 추적과 같은 보안상 문제점을 가지고 있다. 이러한 문제점을 해결하기 위해 해쉬함수와 같은 암호학적 접근방법들은 안전성을 증명하고 있지만 태그의 연산능력과 저장 공간의 한계로 인해 현실적으로 적용하기 어렵다. 최근의 경량 인증기법들은 단순 연산자만을 사용하여 높은 효율성을 보장하지만 안전성에 관한 주장이 충분하지 못하다. 본 논문에서는 안전한 RFID 인증을 위해서 대칭키 방식의 AES(Advanced Encryption Standard)를 이용하며 대칭키 방식에서의 고정된 키를 사용하던 문제를 단계적인 키 변환을 통해 해결한다. 프로토콜에서 태그와 서버의 동일한 대칭키는 태그, 리더, 백-엔드-서버에서 각각 생성된 난수를 이용하여 차례로 변환되며 태그와 리더의 출력 값을 항상 변경한다. 이와 같이 단계적으로 변환된 키를 이용할 경우 태그 정보의 노출 문제를 해결하며 도청, 재전송, 위치추적 및 스푸핑과 같은 공격에도 안전한 상호 인증이 이루어진다.

Key Words : RFID, AES, Authentication Protocol, Cryptograph, Key Change

ABSTRACT

The RFID system has the security problem of location tracking and user privacy. In order to solve this problem, the cryptographic access method using hash function is difficult to in real applications. Because there is a limit of computing and storage capacity of Tag, but the safety is proved. The lightweight authentication methods like HB and LMAP guarantee the high efficiency, but the safety is not enough to use. In this paper, we use the AES for RFID Authentication, and solve the problem of using fixed key with key change step by step. The symmetric keys of the tag and server are changed by the random number generated by tag, reader and server successively. This could prevent the key exposure. As a result, the output of the tag and reader always changes. These key changes could make it possible to prevent eavesdropping, replay attack, location tracking and spoofing.

Ⅰ. 서 론

RFID(Radio Frequency IDentification)는 무선 주파수와 자기장 변화를 이용하여 물리적 접촉 없이 아이템을 인식하거나 식별하는 시스템이다. RFID의 구성 요소는 아이템에 부착하는 식별 장비인 태그(Tag)와 태그를 인식하여 저장된 정보를 읽을 수 있는 리더(Reader)로 구성된다. 이와 같이 RFID는 태그와 리더를 사용하여 비접촉에 의해 대량의 사물을 동시에 인식할 수 있으므로 기존의 바코드에 비해 활용분야가 매우 넓다. 하지만 RFID 태그는 자신의 식별 정보를 무선 주파수를 사용하

* 경북대학교 컴퓨터공학과 임베디드 시스템 연구실 ({mccart, kimm2001, 170m3, 10004oke, timpark75, gsahn}@knu.ac.kr)
논문번호 : KICS2009-11-535, 접수일자 : 2009년 11월 1일, 최종논문접수일자 : 2010년 2월 8일

여 리더에 아무런 제약 없이 전송하기 때문에 도청을 통한 개인 정보 노출이나 위치 추적과 같은 여러 가지 문제점이 발생한다. 이러한 문제를 해결하기 위해서 안전한 암호 알고리즘 구현이 필요하며 제한된 하드웨어 자원에 대해 고려할 필요가 있다. 특히 수동형 RFID 태그는 리더로부터 전원을 공급받아야 동작하므로 자원 제약이 매우 심하다.

RFID 시스템에서 보안을 위한 기법은 크게 물리적 접근방법과 암호학적 접근방법으로 분류된다. 특히 프라이버시보호, 인증 및 데이터 보호를 위해서는 암호학적 접근방법이 필요하다. 암호학적 접근방법은 해쉬함수나 암호 알고리즘을 중심으로 RFID에 적용하기 위한 많은 연구가 이루어지고 있으며 안전성을 증명하고 있다. 하지만 하드웨어 자원 제약으로 인해 현실적으로 적용하기 어렵다. 이에 비해 자원 소비를 최소로 하는 경량 인증방식도 다양하게 연구되고 있지만 안전성 측면의 많은 문제들이 제시되고 있다. 최근에 Martin Feldhofer 등에 의해 태그에서 구현 가능한 저전력 AES(Advanced Encryption Standard) 기법이 제안 되어 RFID 시스템의 인증 및 암호 프로토콜로 사용가능함을 보이고 있다. 따라서 RFID에 적용 가능한 AES 대칭키 방식의 보안 연구가 필요하다. 하지만 기존의 연구들은 AES를 사용하는데 있어 서로 다른 태그가 고정된 같은 키를 사용하여 암호화하기 때문에 인증에 필요한 공격에 의한 태그와 리더값의 노출을 해결하고 있지 못하다.

본 논문에서는 RFID 시스템에 적용 가능한 대칭키 방식의 안전한 인증 프로토콜을 제안한다. 제안한 프로토콜은 난수와 XOR 연산을 적극 활용하여 태그와 리더를 안전하게 상호 인증하며 대칭키 방식에서 기존의 고정키를 사용하던 문제를 단계적인 키 변환을 통해 해결한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 RFID 시스템의 보안기법과 문제점에 대해서 기술하고 Ⅲ장에서는 제안된 인증 프로토콜에 대해서 기술한다. Ⅳ장에서는 공격 시나리오를 통해 안전성을 분석하고 마지막으로 Ⅴ장에서는 결론을 맺는다.

Ⅱ. RFID 시스템의 보안기법과 문제점

RFID 시스템은 태그와 리더간의 주파수 통신을 이용한 무선 통신 시스템이다. 따라서 RFID 보안기법에서 요구되는 조건은 태그와 리더 간의 암호화된 데이터 전송과 태그의 제한적인 연산 능력 및 메모리 공간의 최소 사용을 고려하여야 한다. 또한 태그와 리더의 상호 인증을 위한 안전한 프로토콜을 설계하여야 한다. 하지만 기존의 보안기법 가운데에는 이러한 조건을 모두 만족하는 방법이 존재하지 않았다. 본 장에서는 기존의 RFID 시스템의 보안기법들과 문제점을 살펴본다.

2.1 보안기법

RFID 시스템의 보안기법은 크게 물리적 접근방법과 암호학적 접근방법으로 분류한다. RFID에 대한 물리적 공격은 탐사공격(Probe Attacks), 회로혼란(Circuit Disruption)등과 같이 물리적으로 태그를 조작하는 방식으로 리더의 태그 식별과정에서 불법적으로 태그를 복제하는 공격이 가능하다. 이러한 공격에 대해 Kill, Faraday Cage, Blocker Tag 등과 같은 물리적 접근방식이 있다[1]. 또한 RFID 표준을 개발 보급하는 국제민간기구인 EPCglobal은 저가형 태그 규격인 Gen-2(EPCglobal Generation 2)를 발표하여 Kill 및 Access 패스워드를 통해 태그 기능을 영구 정지 시키거나 태그의 특정 메모리 영역 쓰기기능을 제한하는 기법을 제공하고 있다[2]. 하지만 이미 A. Juels의 연구에서 Gen-2 규격이 태그와 리더 간의 상호 인증 기법의 부재로 인해 복제 및 도청, 중간자 공격에도 취약하다는 사실이 밝혀졌다[3].

암호학적 접근방법은 해쉬함수 및 암호 알고리즘을 통해 태그와 리더간의 메시지가 공격자에 의해 도청되는 문제를 해결한다. 해쉬함수 기법은 가변길이의 메시지로부터 고정 길이의 해쉬값을 계산하여 메시지가 전송되는 동안 의도되지 않은 변경이 발생하지 않도록 보장한다. 이러한 해쉬함수의 일방향성을 이용하여 메시지로부터 해쉬값을 계산하기는 쉬우나 해쉬값으로부터 메시지를 찾는 것은 불가능하다. S. Weis등은 고정된 키 값을 해쉬한 metaID 값을 사용하여 태그의 ID를 감추는 해쉬-락 기법[4]을 제안하였으나 태그의 추적과 재전송 공격에 취약한 문제점을 가지고 있다. 또한 태그의 응답을 랜덤화하여 위치 추적을 피하도록 설계한 랜덤화된 해쉬-락 기법을 제안하기도 하였다[4]. 그림 1은 랜덤화된 해쉬-락 기법을 나타낸다. M. Ohkubo등은 위치 추적에 안전한 방법으로 서로 다른 두 개의 해쉬함수를 이용한 해쉬체인 기법을 제안하였다[5]. 하지만 리더의 질의에 대해 항상 다른 응답을 하므로 공격자가 태그의 응답을 알고 있을 때 메시지를 재전송 하는 경우 정당한 태그로 위장할 수 있으므

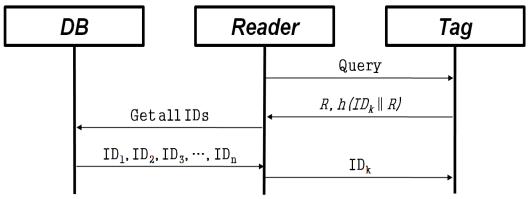

그림 1. Randomized-Hash Lock Protocol

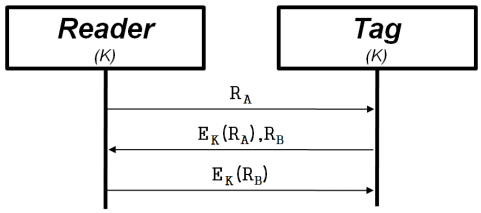

그림 2. Challenge-Response Protocol

로 재전송 공격과 스푸핑 공격에 취약할 수 있다.

이와 같이 해쉬함수 기법은 태그에 대한 다양한 공격에 안전성을 보장하지만 백-엔드-서버에서 모든 식별 정보에 대해서 해쉬연산과 비교연산을 하므로 서버 측에 부하가 많다. 또한 다수 태그의 경우 리더가 태그의 잠금 상태를 해제하는데 많은 시간이 소요되므로 실시간 인증에 적용하기는 어렵다. 무엇보다 20,000-25,000게이트 회로 이상의 하드웨어 기반이 필요하기 때문에 실제로 구현이 불가능하다.

2.2 저전력 AES 암호화 기법

RFID 시스템의 암호학적 접근방법으로 공개키나 대칭키를 이용하여 리더의 질의에 대해 태그가 항상 다른 값으로 응답하는 기법들이 있다. 이 기법들은 암호화를 통해서 태그 사용자의 위치 정보를 숨기며 암호 시스템을 기반으로 하기 때문에 다른 프로토콜보다 훨씬 안전하다. A. Juels와 R. Pappu는 ElGamal 공개키로 암호화하는 방법[6]을 제안하였으며 P. Golle등은 이를 확장한 재 암호화 기법[7]을 제안하였다. 하지만 공개키 기반의 암호화 기법들은 키 분배 문제를 해결하지만 암·복호화의 연산능력이 해쉬함수보다 높다. 이에 비해 대칭키 기반의 암호화 기법은 해쉬함수나 공개키 암호화 기법에 비해 메모리를 적게 소모하고 구현하기 쉬운 장점이 있다[8].

M. Feldhofer는 32bit 대칭키 암호 알고리즘인 AES를 저 전력이면서 효율적인 8bit AES로 설계하였다[9]. 이것은 3,595게이트와 100kHz에서 8.15μA의 전류 소비량을 가지며 하나의 S-Box만을 사용하는 저면적 구조로 되어 있다[10]. 또한 AES 암호화 연산에 1,000사이클 정도가 소요된다. 그림 2는 M. Feldhofer가 제안한 Challenge-Response 인증 프로토콜이다. 이 프로토콜은 태그와 리더간의 인증을 위해 ISO-18000과 호환을 이룰 수 있는 단순 양방향 인증 프로토콜이며 AES를 이용하여 RFID의 인증이 가능함을 보여준다. 하지만 이 프로토콜은 태그 및 리더가 둘만이 공유한 키를 가지고 상호 인증하는 방식으로 인증에 있어서 안전성이 보장 되지만 위치 추적과 같은 문제가 존재한다[11].

2.3 RFID 인증 프로토콜

인증은 특정 시스템이나 자원의 접근 허용 여부를 결정하는 문제로서, RFID 시스템에서 통신하는 상대에 대한 인증 절차가 없다면 공격자는 태그나 리더를 위조하여 공격 할 수 있다. 또한 태그나 리더 중 하나만 인증하는 단방향 인증인 경우에도 인증되지 않은 다른 하나에 대해서 위조하는 것이 가능하다면, 스푸핑 공격이나 재전송 공격이 가능하다. 안전한 인증 프로토콜은 태그, 리더, 백-엔드-서버간의 안전한 정보전달을 통해 상호 인증이 이루어져야 한다. 단방향 해쉬함수나 블록 암호화 기법을 이용하는 방식에서 백-엔드-서버의 역할은 태그와 리더가 수집한 정보를 저장 관리하므로 태그와 리더를 대신하여 복잡한 연산을 수행한다. 하지만 EPCglobal Gen2에서는 MD5나 SHA-1같은 해쉬함수를 쓸 수 없다고 명시하고 있다[2].

RFID 시스템의 인증방식은 태그의 연산능력과 저장 공간에 따라 크게 두 가지로 분류할 수 있다. 암호학적 알고리즘을 적용할 경우 중량 인증방식이라 보며 난수 생성기와 간단한 함수를 사용하는 경우는 경량 인증방식이라고 할 수 있다. 특히 XOR, AND, OR같은 논리 비트연산만 사용하는 경우는 초경량 인증방식으로 분류한다. 최근에는 난수 생성기와 XOR과 같은 단순 연산자를 이용한 경량 인증방식의 연구가 진행되고 있다. 경량 인증방식의 경우 자원의 소비를 최소화 하는 방법으로 저가의 RFID 태그에 적용 가능한 방식이다. 이들 방식의 대표적인 것으로 그림 3과 같이 Hopper-Blum의 HB 프로토콜[12],[13]과 Peris-Lopez의 LMAP(A Real Light-weight Mutual Authentication Protocol)[14], M^{2}AP(A Minimalist Mutual Authentication Protocol)[15], EMAP(An Efficient Mutual Authentication Protocol)[16] 등이 있다. 하지만 경량 인증방식들은 효율성과 안전성 주장이 충분하지 못한 단점이 있다. HB 프로

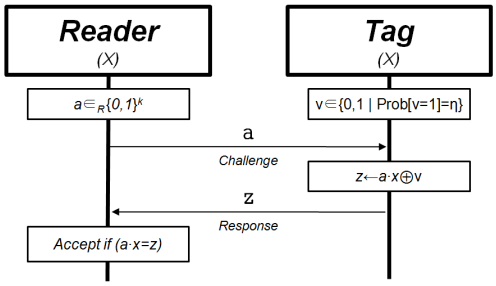

그림 3. HB Protocol

토콜의 경우 안전성 증명은 제시되어 있으나 태그 인증만을 고려하고 리더 인증, 위치 추적, 익명성 및 태그 식별 문제는 고려하지 않는 등의 효율성이 떨어지는 단점을 가지고 있으며 Periz-Lopez의 프로토콜들은 효율적인 방식이지만 비동기화 및 태그 완전 노출의 약점이 있다[17],[18].

2.4 AES와 안전한 인증방식

RFID 시스템에서 태그와 리더간의 통신을 도청하여 다른 공격에 활용할 수도 있으며 악의적인 리더에 의한 태그의 응답을 미리 예측할 수도 있다. 예측된 정보는 태그의 위치 변화를 감지하여 이동경로를 파악할 수도 있다. 이와 같이 RFID 시스템에서의 보안 요구사항은 도청공격에 안전해야 하며 공격자가 이전 세션의 모든 통신 내용이 도청을 통해 알 수 있다 하더라도 현재 세션에 통신될 정보 생성이 어려워야 한다. 위치 추적의 경우 메시지가 암호화되어 있더라도 같은 비트패턴의 태그가 이동하는 것을 알 수 있기 때문에 안전한 인증 프로토콜 설계는 매우 중요하다.

태그와 리더 간에 전송되는 메시지를 보호하기 위해 난수 생성기를 활용하는 방법이 있다. 난수 생성기를 이용하면 태그의 출력을 구별하지 못하게 하므로 출력 값과 태그의 ID를 연결시킬 수 없다. 또한 공격자가 태그에 저장된 비밀 데이터를 얻을 수 있더라도 이 정보를 이용하여 현재의 출력 값을 통해 이전 출력 값을 예상할 수 없다. S. Kinoshita는 익명-ID 방식을 통해 태그의 익명-ID를 암호화거나 ID와 연관된 난수를 사용하여 위치 추적의 문제를 해결하였다[19]. D. Molnar는 태그에 대한 프라이버시 보호를 위해 난수를 이용한 상호 인증 기법을 제안하였다[20]. EPCglobal Gen-2에도 PRNG (Pseudo Random Number Generator)를 이용한 난수생성을 지원하고 있다[2].

암호학적 접근방식에서 살펴볼 때 해쉬함수와 같은 기법들은 RFID 시스템의 많은 보안 요구사항에 적절히 대처하고 있지만 현재의 하드웨어 자원에서는 현실적으로 적용하는데 문제가 있다. 경량 인증방식도 안전성에 대한 충분한 검증이 필요한 실정이다. 따라서 RFID 시스템의 안전한 인증을 위해서는 최소한의 암호학적 기법이 요구되는데 2.2절에서 기술한 바와 같이 저전력 AES를 이용한 프로토콜 설계가 현실적이라고 할 수 있으며 RFID에 적용 가능한 연구가 계속 진행되고 있다[21]. 하지만 AES와 같은 대칭키 알고리즘을 사용할 경우 키 관리와 같은 문제가 여전히 존재한다.

RFID 시스템에서 대칭키 방식을 적용할 경우 리더와 태그간의 키를 공유해야 하며 각 태그마다 유일한 키를 관리하기 위한 기법에 대한 연구가 필요하다. 그림 4의 B. Toiruul의 상호 인증 프로토콜에서는 위치 추적을 방지하기 위해 두 개의 키 값을 일정한 방식으로 갱신하여 서버와 태그에 동일하게 저장하고 다음 인증에 사용한다[22]. 이것은 여러 개의 태그를 사용할 때 각각 태그마다 고정된 서로 다른 키를 사용하며, 태그를 식별하는 문제와 태그마다 같은 키 값으로 암호화하는 잠재적인 문제가 있다. 이남기 등의 논문에서는 서버와 태그사이의 사전에 공유된 키 값을 이용하여 서버와 태그의 인증에 사용하고 서버에서 생성한 난수를 이용하여 동일하게 키 값을 갱신 한다[23]. 하지만 첫 단계에서 리더난수가 노출되어 다음 단계의 도청을 통해 키 값을 유추해 낼 수 있으며 키가 노출 시에 태그의 식별정보도 노출되는 문제점을 가지고 있다. M. Feldhofer의 Challenge-Response 프로토콜에서는 고정된 두 개의 키 값으로 인증을 수행하고 있으며 물리적 공격이나 프로토콜상의 여러 단계의 도청을 통해 키 값의 유추가 가능하다[11]. 경량 인증방식에서도 암호화 과정을 거치지 않기 때문에 키 노출 문제가 여전히 나타나고 있다[17].

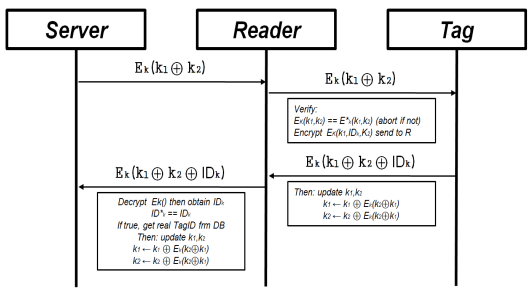

그림 4. B. Toiruul의 Mutual-Authentication Protocol

해쉬-락의 경우 태그에 해쉬함수의 구현만을 요구하고, 백-엔드-서버에 키 관리를 요구하지만 고정된 키를 해쉬한 값을 사용하기 때문에 보안의 여러 문제를 가지고 있다. 키 값이 고정되어 있다는 의미는 키 값이 노출될 때 태그의 식별정보도 노출될 수 있는 중요한 문제가 있으며 위치 추적의 문제도 방지 하지 못한다. 따라서 태그와 리더의 출력 값들은 고정된 값이 아니라 항상 변해야 하며 이를 위해 난수를 이용하여 식별 정보를 찾아내는 방법을 사용하기도 한다. 해쉬체인 기법의 경우 새로운 정보들을 태그에 저장하고, 리더에게 보내는 출력 값을 항상 변하게 하여 보안 문제를 해결한다.

키의 노출 문제는 PUF(Physically Unclonable Function)를 이용하여 해결할 수 있다. PUF는 동일한 회로라 하더라도 회로를 구현하는 공정 상황에 따라 Wire Delay 및 Gate Delay가 미세하게 다르다는 점을 이용한 회로이다. 최근에 물리적 공격에 의한 키 추출을 방지하기 위해 PUF를 활용한 연구가 많이 진행되고 있다[24],[25].

Ⅲ. 제안 인증 프로토콜

본 장에서는 RFID시스템의 다양한 공격에도 안전한 인증 프로토콜을 제안한다. 이것은 저전력 AES를 이용한 암호학적 기법을 적용한다. 또한 태그와 리더의 출력값을 항상 변하게 하기 위해 난수와 XOR 연산만을 사용하고 단계적으로 키가 변하면서 태그와 리더간의 상호 인증을 수행한다. 제안 프로토콜은 시스템의 초기화 단계와 상호 인증 단계, 정보획득 단계로 구성한다.

3.1 초기화 단계

제안하는 RFID 시스템의 구성은 태그, 리더, 백-엔드-서버로 구성되며 태그는 리더로부터 전원을 공급 받아 동작하면서 인증절차를 수행한다. 태그와 리더 사이의 통신 채널은 무선 주파수를 사용하므로 안전하지 않은 채널이며 백-엔드-서버와 리더간의 통신 채널은 안전하다고 가정한다. 또한 태그와 백-엔드-서버는 AES 암호화 및 복호화 연산을 수행할 수 있으며 태그와 리더, 백-엔드-서버는 각각 난수 생성기를 가지고 인증을 위한 난수를 생성한다. 표 1은 제안한 프로토콜에 사용되는 표기법을 나타내며 초기화 단계는 제안 프로토콜의 실행을 위한 준비단계로서 다음과 같다.

표 1. 표기법

표기법	내용
ID	태그의 고유 식별자
M	난수 정보의 Mask Bit
R_{tag}	태그에서 생성된 원본 난수
R'_{tag}	암호화되는 태그 난수
R_{reader}	리더에서 생성된 원본 난수
R'_{reader}	암호화되는 리더 난수
R_{server}	서버에서 생성된 원본 난수
R'_{server}	암호화되는 서버 난수
$PRNG$	난수 생성기
K_0	초기 대칭키
K_1, K_2, K_3	1차, 2차, 3차 변환키
$\oplus$	exclusive-OR 연산자
$\|$	연접(concatenation) 연산자
$E()$	블록 암호문

1) 모든 태그에는 각각 자신의 비밀정보 ID를 저장한다.
2) 백-엔드-서버에는 모든 태그의 비밀정보를 저장한다.
3) 태그와 백-엔드-서버는 사전에 동일한 초기 대칭키(K_0)를 가지고 있다.
4) 태그와 리더는 생성된 난수를 마스크하기 위한 마스크 비트(M)를 가지고 있다.

3.2 프로토콜 전체구성

본 논문에서 제안한 프로토콜은 태그와 리더간의 안전한 상호 인증을 목적으로 하며 저전력 AES 암호학적 기법과 난수와 XOR 연산만을 사용하여 설계한다. 기존의 인증 프로토콜들은 고정된 키 값을 이용하여 암호화하였고 이것은 키 값이 노출될 수 있는 문제점을 가지고 있다. 따라서 키 변환을 통해 태그와 리더의 출력 값을 항상 변환하여 다양한 공격에 안전하도록 설계한다. 이를 위해 태그와 서버가 가지고 있는 동일한 대칭키를 태그, 리더, 서버에서 생성된 난수를 이용하여 차례로 변환하면서 변환된 키로 태그와 리더를 상호 인증한다. 키 변환은 총 세 차례 이루어지며 태그에서 변환된 키에 의해 태그가 인증되며 서버에서 변환된 키에 의해 리더가 인증된다. 그림 5는 본 논문에서 제안한 RFID 상호 인증 프로토콜의 전체구성을 나타낸다.

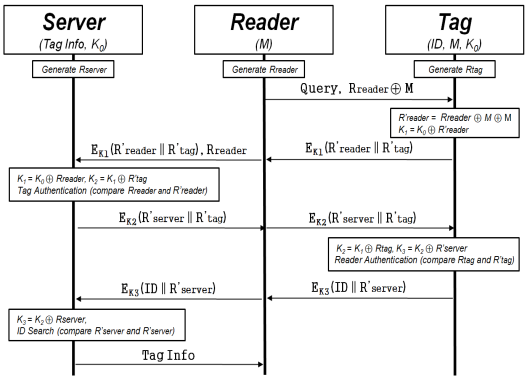

그림 5. 제안 프로토콜의 전체구성

3.3 태그 인증 과정

상호 인증 과정은 태그의 정보를 얻기 위해 리더가 태그에게 질의를 보내면서 시작한다. 그림 6은 첫 번째 키 변환을 통해 백-엔드-서버가 태그를 인증하는 과정이다. 리더는 태그에게 질의를 요청하기 전에 리더의 난수 생성기 $PRNG(Reader)$를 이용하여 리더 난수 R_{reader}를 생성한다. R_{reader}는 나중에 태그를 인증하는 중요한 데이터로 사용되며 마스크 연산을 통해 태그에 전달한다. 마스크 연산에 사용되는 M은 리더와 태그가 가지고 있는 공유 값으로 R_{reader}값을 안전하게 보내기 위해서 필요하며 Step 1의 데이터 전송을 위해서만 사용한다. MOR (Mask of Random)은 리더에서 태그로 전달되는 Step 1의 PDU(Protocol Data Unit) 프레임 필드이며 프로토콜 설계를 위해 재설계한 것이다.

태그는 자신의 난수 생성기 $PRNG(Tag)$를 이용하여 태그 난수 R_{tag}를 생성하고 이 값은 나중에 리더를 인증하는 용도로 사용한다. 또한 태그는 리더에서 전송된 프레임으로부터 MOR를 읽어와 태그에 저장된 M을 이용하여 리더 난수 R'_{reader}를 얻을 수 있다. 이때 R'_{reader}는 태그에 저장된 초기 대칭키 K_0와의 연산을 통해 1차 변환키가 생성되며 이 값이 K_1이다. K_1은 리더 난수와 태그 난수를 암호화하는데 사용하며 태그난수 R'_{tag}는 나중에 리더를 인증하는데 사용된다. 암호화된 메시지는 Step 2에서와 같이 리더로 응답 프레임에 포함되어 전송되고 이 메시지는 리더가 가지고 있는 원본 리더난수 R_{reader}와 같이 서버로 다시 전송된다. 태그 인증은 리더가 아닌 서버를 통해서 이루어진다. 서버는 리더로부터 전달된 원본 리더난수 R_{reader}를 이용하여 K_1을 얻을 수 있으며 이 값을 이용하여 전달된 메시지를 복호화 할 수 있다. 서버는 리더로부터 전송된 R_{reader}와 태그로부터 전달된 R'_{reader}와의 비교를 통해 태그 인증을 수행한다. 그림 7은 태그 인증에 대한 각 스텝의 동작 코드이다.

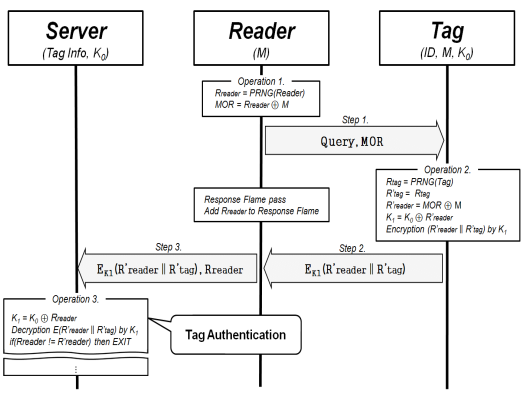

그림 6. 태그 인증 과정

```
Operation 1.
Reader : R_reader = PRNG(Reader)
         MOR = R_reader ⊕ M
Step 1.  Reader ⇒ Tag : Query, MOR

Operation 2.
Tag :    R_tag = PRNG(Tag)
         R'_tag = R_tag
         R'_reader = MOR ⊕ M
         K1 = K0 ⊕ R'_reader
         Encryption (R'_reader ‖ R'_tag) by K1
Step 2.  tag ⇒ Reader : E_K1(R'_reader ‖ R'_tag)
Step 3.  Reader ⇒ Server : E_K1(R'_reader ‖ R'_tag), R_reader

Operation 3.
Server : K1 = K0 ⊕ R_reader
         Decryption E_K1(R'_reader ‖ R'_tag) by K1
         if(R_reader != R'_reader) then Exit
```

그림 7. 태그 인증 동작 코드

3.4 리더 인증 과정

리더의 인증은 태그에서 태그 난수의 비교를 통해 인증을 수행한다. 이때 태그 난수는 2차 변환키로 암호화된 메시지로 전달되며 그림 8은 태그에서 리더를 인증하는 과정을 나타낸다.

서버는 태그로부터 전달된 태그 난수 R'_{tag}를 통해 태그로 전달할 메시지를 암호화하기 위한 2차 변환키 K_2를 생성한다. 이때 K_2는 이전에 생성된 K_1을 통해서 만들어지고 나중에 태그의 ID를 전달

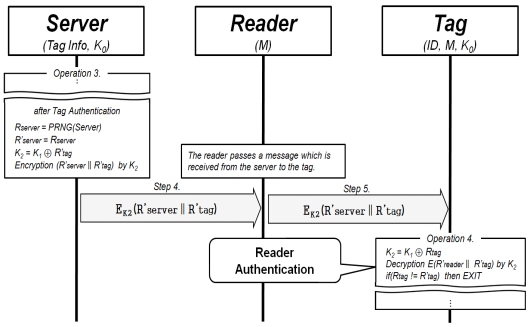

그림 8. 리더 인증 단계

받기 위해 필요한 서버 난수 R'_{server}와 R'_{tag}를 같이 암호화하여 태그로 전달한다. 태그로 메시지를 전달하는 과정에서 리더는 이 메시지를 그대로 태그로 다시 전달하게 되고 태그는 이 메시지로부터 자신이 이전에 보낸 태그 난수 R'_{tag}를 얻게 되어 리더 인증을 수행 할 수 있다. 태그는 이미 자신이 가지고 있는 K_1과 R_{tag}를 이용하여 K_2를 추출할 수 있으며 이 키를 이용하여 전달받은 암호 메시지를 복호화 할 수 있다. 리더의 인증은 태그에 이미 저장되어 있는 R_{tag}와 서버로부터 전달받은 R'_{tag}의 비교를 통해 이루어진다. 그림 9는 리더 인증에 대한 각 스텝의 동작 코드이다.

```
Operation 3.
Server : Rserver = PRNG(Server)
         R'server = Rserver
         K2 = K1 ⊕ R'tag
         Encryption (R'server ‖ R'tag) by K2
Step 4.  Server ⇒ Reader : EK2(R'server ‖ R'tag)
Step 5.  Reader ⇒ Tag : EK2(R'server ‖ R'tag)

Operation 4.
Tag :    K2 = K1 ⊕ Rtag
         Decryption EK2(R'server ‖ R'tag) by K2
         if(Rtag != R'tag) then Exit
```

그림 9. 리더 인증 동작 코드

3.5 태그의 정보 획득 과정

태그와 리더의 상호 인증이 정상으로 수행될 경우 태그는 리더에게 자신의 식별자 *ID*를 전달할 수 있다. 이 정보는 3차 키 변환을 통해 생성된 키로 암호화된 메시지에 포함된다. 그림 10은 태그의 *ID* 정보를 서버에 전달하여 리더가 얻게 되는 과정을 나타낸다. 태그와 리더의 상호 인증 후에는 태그의 *ID*를 리더가 획득 할 수 있다. 태그는 2차 변환키

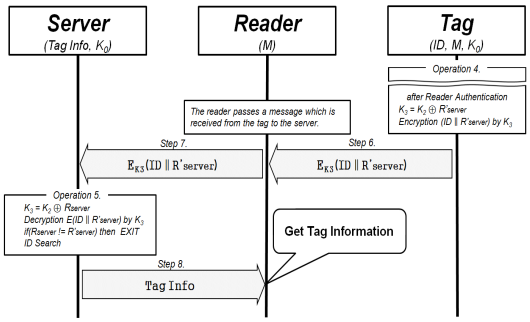

그림 10. 태그의 정보 획득 과정

K_2와 서버로부터 전달 받은 서버 난수 R'_{server}를 이용하여 3차 변환키 K_3를 생성한다. 태그는 자신의 식별자 *ID*와 R'_{server}를 K_3에 의해 암호화한 후 메시지를 서버로 전달한다. 이때 서버 난수는 서버가 정당한 태그인지를 재확인하는 용도로 사용된다. 서버에서는 태그로부터 전달된 메시지를 복호화하기 위해 이전의 K_2와 자신의 서버 난수 R_{server}를 가지고 K_3를 추출한 다음, 서버에 이미 저장되어 있는 R_{server}와 태그로부터 전달받은 R'_{server}의 비교를 통해 *ID*를 획득하여 정보를 검색 할 수 있다. 검색된 정보는 리더로 전송되어 태그와 리더간의 한 세션은 종료 된다. 그림 11은 태그 정보를 획득하는 과정에 대한 각 스텝의 동작 코드이다.

```
Operation 4.
Tag :    K3 = K2 ⊕ R'server
         Encryption (ID ‖ R'server) by K3
Step 6.  Tag ⇒ Reader : EK3(ID ‖ R'server)
Step 7.  Reader ⇒ Server : EK3(ID ‖ R'server)

Operation 5.
Server : K3 = K2 ⊕ Rserver
         Decryption EK3(ID ‖ R'server) by K3
         if(Rserver != R'server) then Exit
Step 8.  Server ⇒ Reader : Tag Info
```

그림 11. 태그 정보 획득 동작 코드

3.6 제안 프로토콜에 대한 PDU 설계

제안한 프로토콜의 각 스텝에 따른 전송 프레임은 EPCglobal의 표준 PDU(Protocol Data Unit)를 바탕으로 재설계 하였다. 프레임은 크게 요청 프레임, 응답 프레임으로 구성되며 질의와 응답이 끝나면 접근 명령을 수행을 위해 다수의 태그를 선택하는 Select 명령이 이루어진다. 그림 12는 제안한 프

SOF	Flags	inventory	Optical AFI	Mask Length	Mask Value	MOR (Mask of Random)	CRC	EOF

(a) Step 1`s Modified Inventory Request Flame Format

SOF	Flags	DSFID	UID (Unique Item Identifier)	CRC	EOF

(b) Step 2 & 6`s Modified Response Flame Format

SOF	Flags	Select	UID (Unique Item Identifier)	CRC	EOF

(c) Step 5`s Modified Request Flame Format

그림 12. 제안한 프로토콜의 수정된 프레임 포맷

로토콜의 각 스텝에 따른 요청 및 응답 프레임의 포맷을 나타내며 표 2는 프레임의 각 필드 내용을 나타내고 있다. 그림 12(a)에서 MOR은 마스크화된 리더난수 필드이며 inventory는 질의 요청에 관한 필드를 나타낸다. 그림 12(b)는 요청 프레임에 대한 응답 프레임의 포맷이며 암호화된 메시지는 UID 필드를 통해 전달된다. 그림 12(c)는 질의에 대한 응답이 이루어진 후 리더가 태그에게 보내는 Select 명령에 대한 프레임 포맷이다.

표 2. 수정된 프레임의 각 필드 의미

필드	설명
SOF(Start of Field)	프레임의 시작
Flags	데이터의 전송타입, 태그의 접근 방식, 데이터 rate등의 정보 등
Inventory	Query에 관한 필드 (Query, QueryAdj, QueryRep, ACK, NAK)
Select	접근 명령의 수행을 위해 대수의 태그를 선택하는 절차
DSFID	UII(Unique Item Identifier) 데이터 구조 및 Object ID 저장 방식 기록
Optional AFI	응용분야를 구별하는 식별자
Mask Length	한 세션에서 특정 태그를 구별하기 위한 마스크 값
Mask Value	한 세션에서 특정 태그를 구별하기 위한 마스크 길이
MOR(Mask of Random)	리더 난수를 숨기기 위한 마스크 값
UID(Unique Identifier)	태그나 리더에게 전하고자하는 식별정보
CRC	에러 체크
EOF(End of Field)	프레임의 끝

Ⅳ. 제안 프로토콜의 안전성 분석

본 장에서는 제안 프로토콜에서 가능한 공격 유형을 두 가지 시나리오로 제시하고 이를 통해 안전성을 분석한다. 또한 기존의 인증 프로토콜과 제안 프로토콜과의 비교를 통해 안전성을 검증한다.

4.1 공격 방법

RFID 시스템의 공격은 도청(Eavesdropping)을 비롯하여 재전송 공격(Relay Attack), 위치 추적(Location Tracking) 및 스푸핑(Spoofing) 등이 있다. 공격자는 태그에서 리더로 전송되는 무선정보를 쉽게 도청 할 수 있는 수동적 공격이 가능하다. 만약 통신의 내용이 도청 가능하더라도 공격자에게는 의미 없는 값이 되어야하며 이로부터 관련된 정보를 알아 낼 수 없어야한다. 만약 도청에 의한 공격이 가능하다면 공격자는 도청된 메시지를 저장하고 있다가 그 메시지를 재전송하여 공격을 시도할 수 있다. 이것은 공격자가 정상 태그인척 위장하여 리더를 속이게 되며 정당한 태그로 인증 받을 수 있다. 위치 추적의 경우 공격자가 도청을 통해 얻은 트래픽을 분석하여 태그의 위치를 추적하는 것이다. 위치 추적은 태그의 출력 값이 일정한 경우에 공격을 당할 수 있으며 태그와 리더간의 메시지가 암호화 되어 있다 하더라도 같은 패턴의 태그가 이동하는 것을 알 수 있으면 태그의 움직임을 알 수 있다. 스푸핑은 공격자가 태그나 리더를 불법적으로 위장하여 인증을 수행 하는 것을 말한다. 공격자는 마치 정당한 리더인 것처럼 가장하여 태그로부터 고유정보를 얻어 낼 수 있거나 정당한 리더의 요청에 마치 자신이 정상 태그인 것처럼 속여서 거짓 정보로 응답하여 공격 할 수 있다. 따라서 태그와 리더는 서로가 정당한 개체로 인증되어야 한다.

4.2 공격 시나리오에 따른 안전성 분석

본 절에서는 제안한 프로토콜에 대해 두 가지 공격 시나리오를 제시한다. 두 가지 시나리오는 공격자가 위장 태그를 이용하여 공격하며 태그와 리더의 인증이 실패함을 보여준다. 그림 13은 공격자가 초기 Step 1의 메시지를 도청하여 마스크 비트 값 M과 리더 난수 R'_{reader}를 알고 있다는 가정 하에 위장 태그가 태그 인증을 수행하려는 시나리오이다. 시나리오 1에서 위장 태그는 정상 태그와 마찬가지로 태그 난수 R_{tag}를 생성한 후 1차 키 변환을 통해 암호화된 메시지를 Step2, 3과 같이 서버로 전송한다. 하지만 위장 태그의 1차 변환키 값은 K_0를 모른 상태에서 생성되었기 때문에 실제 서버로 전송된 암호 메시지는 서버의 K_1으로 복호화 할 수 없다. 따라서 서버는 R'_{reader}를 알 수 없으므로 태

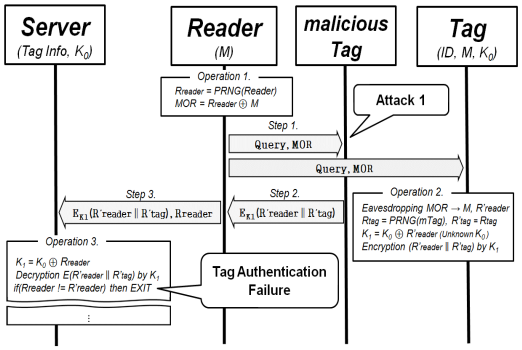

그림 13. 위장 태그를 통한 공격 시나리오 1

그의 인증은 실패하게 된다. 만약 태그내의 K_0가 노출된다면 전체 프로토콜의 위험이 클 수도 있다. 하지만 K_0는 제안한 전체 프로토콜에서 통신에 사용되는 데이터가 아니기 때문에 외부로 노출될 가능성이 적다. 또한 하드웨어적인 불법 복제로 인한 보안 문제는 PUF(Physically Unclonable Function)와 같은 기술로 해결이 가능하므로 본 논문에서는 배제한다.

그림 14는 위장 태그가 Step 2의 메시지를 도청하고 있다가 그대로 리더에게 전달하여 인증을 수행하는 시나리오이다. 시나리오 2의 경우 위장 태그는 정상 태그에서 리더로 응답하는 메시지를 도청하여 위장 태그가 정상 태그인척 리더에게 같은 메시지를 보내는 경우이다. 이 메시지는 Step 3을 통해 서버로 전달되며 정상적으로 복호화 되어 태그 인증이 이루어진다. 이후에 Step 4, 5를 통해 K_2로 암호화된 메시지가 위장 태그로 전달되지만 위장 태그는 이전의 K_1을 알 수 없기 때문이 메시지를 복호화 할 수 없다. 따라서 시나리오 2는 태그 인증은 가능하지만 리더 인증은 실패하여 상호 인증이 불가능하다.

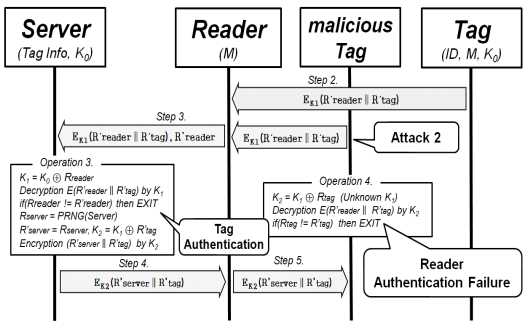

그림 14. 위장 태그를 통한 공격 시나리오 2

4.3 기존 프로토콜과의 안전성 비교 분석

본 절에서는 앞 장에서 기술한 기존 프로토콜과 제안 프로토콜의 안전성을 비교 분석한다. 비교 대상의 프로토콜은 해쉬 계열의 해쉬-락, 랜덤화된 해쉬-락, 해쉬-체인, Feldhofer's Challenge-Response, Toiruul's 프로토콜을 대상으로 한다. 표 3은 이들 프로토콜과 제안한 프로토콜을 중간자 공격, 재전송 공격, 위치 추적, 키 노출, 키 분배, 상호 인증의 6가지 측면에서 안전성을 비교한 내용이다.

①은 metaID가 항상 일정하므로 위치 추적이 가능하며, 공격자가 태그의 metaID를 도청하여 정당한 리더에게 재전송하는 경우 리더는 정당한 키를 공격자에게 보내게 되는 위험이 있다. 또한 ②의 경우도 리더에서 계산량이 많아진다는 부담이 있으며 메시지를 재전송하는 공격과 정당한 태그로 가장할 수 있는 스푸핑 공격이 가능하다. ④는 단방향 인증 프로토콜이므로 스푸핑이나 중간자 공격에 취약한 문제점이 있다. 또한 리더 난수가 노출되어 공격자는 도청된 정보를 바탕으로 키 값을 쉽게 알아낼 수 있다. ⑤의 경우 갱신된 비밀키를 다음 인증에 사용하지만 각 태그마다 다른 키를 사용할 경우 서버의 계산량이 증가하여 태그를 식별하는데 문제가 있으며 태그와 리더의 비밀키를 일정한 방식으로 갱신함으로서 위치 추적에 노출 될 수 있다.

제안 프로토콜의 경우 태그, 리더, 서버의 난수들은 매 세션마다 서로 다른 키 값으로 암호화하며 태그와 리더 사이의 주고받는 메시지가 모든 인증 단계에서 매번 서로 다른 메시지가 전달된다. 이것은 난수와 변환된 키 값을 사용하기 때문에 매 세션마다 응답 값이 변경된다는 것을 의미하므로 태그와 리더 사이의 응답값은 항상 변하게 되어 위치

표 3. 기존 프로토콜과 제안 프로토콜의 안전성 비교

○ : Satisfied △ : Partially Satisfied × : Not Satisfied

프로토콜 평가유형	① Hash Lock	② Randomized Hash-Lock	③ Hash Chain	④ Feldhofer's Protocol	⑤ Toiruul's Protocol	⑥ Proposed Protocol
중간자 공격	△	△	×	×	○	○
재전송 공격	×	△	×	△	○	○
위치 추적	×	×	○	×	×	○
키 노출	×	×	△	×	△	○
키 분배	·	·	·	×	×	○
상호 인증	△	△	△	△	○	○

추적에 안전하다. 또한 공격자가 도청을 하였다 하더라도 의미 없는 정보가 될 수 있으며 도청한 정보를 가지고 이전키를 찾아 낼 수 없어서 공격에 활용될 수 없다. 그리고 공격자가 메시지를 그대로 전송할 경우 정상적인 리더와 태그 입장에서는 이전 값을 보내게 되어 인증 과정을 통과 할 수 없다. 공격자가 키 값을 얻기 위해서는 태그의 초기 키 값과 난수를 알고 있어야 하는데 태그의 초기 키 값은 메시지 전송과정에서 드러나지 않는다. 따라서 하드웨어적인 불법복제 방지가 보장 된다면 안전하다고 할 수 있다[25].

V. 결 론

RFID 시스템은 무선을 이용한 자동인식 기술로 주목받고 있지만 개인의 위치추적이나 사용자 프라이버시와 같은 정보 유출의 위험성을 가지고 있다. RFID의 보안 연구과 관련하여 기존의 암호학적 접근방법은 하드웨어 자원 한계를 극복하고 있지 못하며 경량 인증방식 또한 안전성 문제를 완전히 해결하고 있지 못하다. M. Feldhofer등은 태그에서 구현 가능한 저전력 AES기법을 제안하였다. 이것은 RFID 시스템의 인증 프로토콜로 사용가능함을 보이고 있다. 하지만 기존의 연구들은 저전력 AES를 사용하는데 있어 서로 다른 태그가 키 값을 고정된 상태로 사용하기 때문에 태그와 리더사이의 응답 값의 노출을 해결하고 있지 못하다.

본 논문에서는 RFID 시스템에 적용 가능한 저전력 AES를 이용하여 안전한 인증 프로토콜을 설계하였다. 제안 프로토콜은 태그와 리더간의 교환되는 메시지를 보호하기 위해 난수와 XOR 연산을 적극 활용하였으며 대칭키 기반의 RFID 인증 프로토콜에서 항상 고정키를 사용하여 키 값이 노출되는 문제를 단계적인 키 변환을 통해 해결하였다. 단계적인 키 변환은 태그와 서버의 고정된 키와 태그, 리더, 서버에서 생성된 난수를 이용하여 세 번의 키 변환이 이루어지며 변환된 키로 매 단계마다 난수를 암호화하여 서버에서 태그를 인증하고 태그에서 리더를 인증한다. 안전성 분석은 위장 태그를 이용한 공격 시나리오를 통해 안전함을 증명하였다. 또한 변환된 키를 이용하여 난수를 암호화하였기 때문에 태그의 응답은 가변적이므로 기존의 다른 프로토콜에 비해 재전송, 도청, 위치추적 및 스푸핑과 같은 공격에도 안전하다.

참 고 문 헌

〔1〕 A. Juels, R. Rivest, and M. Szydlo, “The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy,” *8th ACM Conference on Computer and Communications Security*, pp. 103-111, Oct 2003.

〔2〕 EPCglobal Inc, “EPC RFID Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz - 960MHz,” Oct, 2008.

〔3〕 A. Juels, “Strengthening EPC Tags Against Cloning,” *ACM Workshop on Wireless Security*, pp.67-76, 2005.

〔4〕 S. Weis, S. Sarma, R. Rivest, and D. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems,” *In Security in Pervasive Computing*, LNCS 2802, pp.201-212, 2005.

〔5〕 M. Ohkubo, K. Suzuki, and S. Kinoshita, “A Cryptographic Approach to “Privacy-Friendly” tag,” *RFID Privacy Workshop*, 2003.

〔6〕 A. Juels, R. Pappu, “Squealing Euros : Privacy protection in RFID-enabled banknotes,” *Financial cryptography International conference*, LNCS 2742, pp.103-123, 2003.

〔7〕 P. Golle, M. Jakobsson, A. Juels, and P. Syverson, “Universal Re-encryption for mixnets,” *RSA Conference Cryptographers Track ’04*, LNCS 2964, pp.163-178, 2003.

〔8〕 M. Feldhofer, C. Rechberger, “A Case Against Currently Used Hash Functions in RFID Protocols,” *On the Move to Meaningful Internet Systems*, LNCS 4277, pp.372-381, 2006.

〔9〕 M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, “Strong Authentication for RFID Systems Using the AES Algorithm,” *Cryptographic Hardware and Embedded Systems*, LNCS 3156, pp.85-140, 2004.

〔10〕 M. Jung, H. Fiedler and R. Lerch, “8-bit microcontroller system with area efficient AES coprocessor for transponder applications,” *Ecrypt Workshop on RFID and Lightweight Crypto 2005*, pp.32-43, 2005.

〔11〕 M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, “AES implementation on a grain of sand,” *IEEE*

Proceedings Information Security, 152(4), pp. 13-20, Nov 2005.

〔12〕 N. Hopper, M. Blum, "Secure Human Identification Protocols," *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security*, LNCS 2248, pp.52-66, 2001.

〔13〕 A. Juels, S, Weis, "Authenticating Pervasive Devices with Human Protocols," *Advances in Cryptology (CRYPTO 2005)*, LNCS 3621, pp. 293-308, 2005.

〔14〕 P. Peris-Lopez, J. Hermandez-Castro, J. Estevez-Tapaidor, and A. Ribagorda, "LMAP: A Real Leightweight Mutual Authentication Protocol for Low-cost RFID tags," *Workshop on RFID security*, pp.137-148, July 2006.

〔15〕 P. Peris-Lopez, J. Hermandez-Castro, J. Estevez-Tapaidor, and A. Ribagorda, "M2AP: A Minmalist Mutual-Authentication Protocol for Low-cost RFID tags," *Proceedings of UIC*, LNCS 4159, pp.912-923, 2006.

〔16〕 P. Peris-Lopez, J. Hermandez-Castro, J. Estevez-Tapaidor, and A. Ribagorda, "EMAP: An Efficient Mutual-Authentication Protocol for Low-Cost RFID Tags," *Proceedings of On the Move to Meaningful Internet Systems 2006*, pp. 352-261, 2006.

〔17〕 권대성, 이주영, 구본욱, "경량 RFID 상호 인증 프로토콜 LMAP, M2AP, EMAP에 대한 향상된 취약성 분석", *정보보안학회논문지*, 17(4), pp. 103-113, Aug 2007.

〔18〕 T. Li, R. Deng, "Vulnerability Analysis of EMAP," *Proceedings of the The Second International Conference on Availability Reliability and Security*, pp.238-245, 2007.

〔19〕 S. Kinoshita, M. Ohkubo, F. Hoshino, G. Morohashi, O. Shionoiri, and A. Kanai, "Privacy Enhanced Active RFID Tag," *1st International Workshop on Exploiting Context Histories in Smart Environments*, 2005.

〔20〕 D. Molnar, D. Wagner, "Privacy and Security in Library RFID Issues, Practices, and Architectures," *Proceedings of the 11th ACM conference on Computer and communications security*, pp.210-219, Oct 2004.

〔21〕 CHES2009, "Workshop on Cryptographic Hardware and Embedded Systems," http://www.chesworkshop.org, 2009.

〔22〕 B. Toiruul, K. Lee, "An Advanced Mutual Authentication Algorithm Using AES for RFID Systems," *International Journal of Computer Science and Network Security*, 6(9B), pp. 156-162, Sep 2006.

〔23〕 이남기, 장태민, 전병찬, 전진오, 유수봉, 강민섭, "AES 암호 프로세서를 이용한 강인한 RFID 인증 프로토콜 설계", *한국정보처리학회 2008 추계 학술발표대회*, 15(2), pp.1473-1476, Nov 2008.

〔24〕 G. E. Suh, S. Devadas, "Physical unclonable functions for device authentication and secret key generation," *Proceedings of the 44th annual Design Automation Conference*, pp.9-14, 2007.

〔25〕 박용수, 신주석, 최명실, 정경호, 안광선, "해쉬된 태그ID와 대칭키 기반의 RFID 인증프로토콜", *한국정보처리학회논문지*, 16(C), 6호, pp.669-680, Dec 2009.

정 경 호 (Kyung-ho Chung) 정회원

2002년 2월 대구대학교 컴퓨터정보공학부 졸업
2002년 8월 경북대학교 컴퓨터공학과 석사
2005년 2월 경북대학교 컴퓨터공학과 박사수료
2005년 3월~현재 경운대학교 컴퓨터공학과 전임강사
<관심분야> 임베디드 라눅스 시스템, 시스템 프로그래밍, RFID, 정보보호

김 경 률 (Kyoung-youl Kim) 준회원

2008년 2월 영동대학교 임베디드 소프트웨어학과 졸업
2010년 2월 경북대학교 컴퓨터공학과 석사
<관심분야> RFID, 정보보호, 임베디드 시스템

오 세 진 (Se-jin Oh) 준회원

2009년 2월 경운대학교 컴퓨터공학과 졸업
2009년 3월~현재 경북대학교 컴퓨터공학과 석사과정
<관심분야> RFID, 정보보호, 임베디드 시스템

이 재 강 (Jae-kang Lee) 정회원

2002년 2월 가야대학교 컴퓨터공학과 졸업
2005년 8월 경북대학교 컴퓨터공학과 석사
2009년 3월~현재 경북대학교 컴퓨터공학과 박사과정
<관심분야> 임베디드 시스템, RFID, 정보보호

박 용 수 (Yong-soo Park) 정회원

1979년 2월 경북대학교 전자공학과 졸업
1981년 2월 경북대학교 전자공학과 석사
1981년 2월 대구가톨릭대학교 전산통계학과 박사
2007년 3월~현재 경북대학교 BK21 Post-Doc
<관심분야> 임베디드시스템 설계, RFID, 정보보호

안 광 선 (Kwang-seon Ahn) 정회원

1972년 2월 연세대학교 전기공학과 졸업
1975년 2월 연세대학교 전자공학과 석사
1980년 2월 연세대학교 전자공학과 박사
1977년 3월~현재 경북대학교 컴퓨터공학과 교수
<관심분야> 임베디드 시스템 설계, RFID