情報保護學會論文誌
第15卷 第5號, 2005. 10

저가형 RFID 시스템을 위한 효율적인 인증 프로토콜*

최 은 영,[1†] 최 동 희,[2] 임 종 인,[1‡] 이 동 훈[1]
[1]고려대학교 정보보호 대학원, [2]LG 전자

Efficient authenticate protocol for very Low-Cost RFID*

Eun Young Choi,[1†] Dong Hee Choi,[2] Jong In Lim,[1‡] Dong Hoon Lee[1]
[1]Graduate School of Information Security, Korea University, [2]LG Electronics Inc

요 약

무선 주파수 인식 (RFID: Radio Frequency Identification) 시스템은 유비쿼터스 컴퓨팅 환경에서 중요한 기술로 주목받고 있으나 RFID 시스템이 가지고 있는 특성으로 인하여 시스템의 보안과 프라이버시 침해가 대두되면서 이를 해결하기 위해 많은 프로토콜들이 제안되었다. 최근, Juels은 저가형의 RFID 태그를 위한 최소한의 암호화 기법을 사용하는 안전한 프로토콜을 제안하였다.[3] 그러나 제안된 프로토콜의 안전성은 공격자가 미리 정해진 세션만을 도청할 수 있다는 가정에 기반하고 있다. 본 논문에서는 저가의 RFID 태그를 위한 프라이버시를 보호하는 안전하고 효율적인 기법을 제안한다. 제안하는 프로토콜은 해쉬, 암호화 알고리즘과 같은 암호화 기법을 사용하지 않으며 단지 단순한 비트 연산을 사용하며, 리더와 태그 사이의 모든 통신을 도청할 수 있는 공격자에 대해 안전하며, Juels가 제안한 기법보다 적은 연산량과 데이터를 요구하기 때문에 더 효율적이다.

ABSTRACT

A RFID (Radio Frequency Identificaion) system receives attention as the technology which can realize the ubiquitous computing environment. However, the feature of the RFID tags may bring about new threats to the security and privacy of individuals. Recently, Juels proposed the minimalist cryptography for very low-cost RFID tags[3], which is secure, but only under the impractical assumption such that an adversary is allowed to eavesdrop only the pre-defined number of sessions. In this paper, we propose a scheme to protect privacy for very low-cost RFID systems. The proposed protocol uses only bit-wise operations without any costly cryptographic function such as hashing, encryption, which is secure which is secure against an adversary who is allowed to eavesdrop transmitted message in every session any impractical assumption. The proposed scheme also is more efficient since our scheme requires less datas as well as few number of computations than Juels's scheme.

Keywords : *Low-cost RFID, Privacy, Ubiquitous, Mutual authentication.*

Ⅰ. 서 론

RFID(Radio Frequency Identification) 시스템은 무선 주파수를 이용하여 물리적인 접촉 없이 개체에 대한 정보를 읽거나 기록하는 자동인식 기술 시스템이다. RFID 시스템은 물류 및 유통 분야에

접수일 : 2005년 5월 19일 ; 채택일 : 2005년 8월 16일
* 본 연구는 정보통신부 및 정보 통신 연구진흥원의 대학 IT연구센터 육성·지원으로 수행되었습니다.
† 주저자, bluecey@cist.korea.ac.kr
‡ 교신저자, jilim@korea.ac.kr

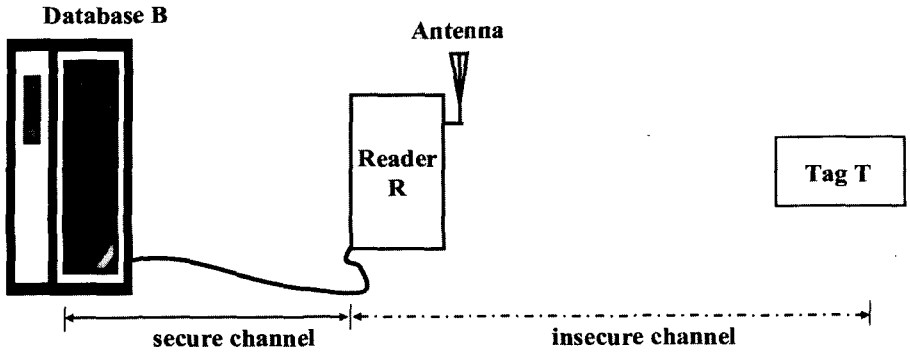


그림 1. RFID 시스템 구성

서 사용되던 바코드에 비해서 저장 능력이 뛰어나고 비접촉식 이라는 이점을 가진다는 점에서 바코드를 대체할 자동 인식 시스템으로 주목 받으면서 많은 연구가 이루어지고 있다. 최근 RFID 시스템은 교통요금 지불 시스템, 가축관리, 의료 분야 등에서도 일부 활용되고 있다.

그러나 RFID 시스템의 물리적인 접촉 없이도 인식이 가능하다는 특징은 시스템의 안전성과 개인의 정보 노출, 위치 추적 등의 프라이버시 측면에서 여러 가지 문제들을 발생 시킨다. 예를 들어, RFID 태그의 정보가 리더에 전송될 때, 태그와 리더의 통신에 제 삼자의 도청이 가능하게 된다. 공격자는 도청한 정보를 사용하여 사용자의 위치를 추적할 수 있으며, 이것은 사용자의 프라이버시 침해를 야기시킨다. RFID 시스템의 프라이버시 침해 문제를 해결하기 위해 영구적으로 태그를 무력화 시키는 물리적인 기법과 해쉬 함수, 암호학적 알고리즘 또는 단순한 연산자를 사용하는 다양한 기법들이 제안되었다.[1-11,15,16]

본 논문에서는 기존에 제안된 저가형의 RFID 시스템을 위한 기법들 보다 효율적인 상호 인증 기법을 제안한다. 제안하는 기법은 리더와 태그 모두 단순한 비트 연산만을 사용하며, 태그에 적은 연산량과 적은 양의 데이터 저장을 요구하기 때문에 저가의 태그에 적합하며, 태그와 리더 사이의 모든 통신이 도청 가능한 공격자에 대해서 안전하다.

본 논문의 구성은 다음과 같다. 2장에서는 RFID 시스템의 구성과 RFID 시스템의 문제점에 대해서 언급하고 3장에서는 RFID 시스템에서 가능한 공격에 대해 언급하고, 기존에 제안된 기법들에 대해 분석하고, 안전한 RFID 시스템 설계 시 고려사항에 대해 설명한다. 4장에서는 제안하는 프로토콜에 대해서 기술하고 5장에서는 제안하는 기법의 안전성과 효율성을 분석한다. 마지막으로 6장에서는 결론을 맺는다.

II. RFID 시스템의 문제점

2.1 RFID 시스템 구성

RFID 시스템은 세 가지 요소, 태그(트랜스폰더), 리더(트랜시버), 데이터베이스로 구성되며, 각각의 기능은 다음과 같다. 그림 1은 RFID 시스템의 구성을 나타낸 것이다.

- 태그 (Tag) 또는 트랜스폰더 (Transponder) : 태그는 RFID 시스템에서 리더의 질의에 대하여 사물, 사람 등의 식별 정보를 무선 통신을 사용하여 전송하며, 태그의 구성은 무선 통신을 위한 안테나와 연산을 수행하고 정보를 저장하는 마이크로 칩으로 이루어져있다. 태그는 전력을 공급받는 방법에 따라 능동형 태그 (active tag)와 수동형 태그 (passive tag)로 분류된다.
  - 능동형 태그 (active tag) : 능동형 태그는 자체 내장된 배터리를 통해서 전력을 공급한다. 자체 내장된 배터리를 사용하기 때문에 원거리 정보 전송이 가능하다. 하지만 자체 내장 배터리가 내장되어 있어서 태그의 가격이 비싸며, 태그의 수명도 배터리에 종속적이라는 단점을 갖는다. 능동형 태그는 토목·건축분야, 의료분야 등에 사용된다.
  - 수동형 태그 (passive tag) : 수동형 태그는 리더로부터 수신한 전자기파로부터 유도한

전류를 전원으로 사용한다. 태그의 전송 전력이 리더에 비해 낮기 때문에 근거리 통신이 가능하다. 수동형 태그는 배터리를 내장하고 있지 않기 때문에 능동형 태그 보다 가격이 싸며, 태그의 수명이 반영구적이다. 수동형 태그는 물류관리, 전자 상거래, 교통 분야, 전자물체감시(EAS) 시스템 분야 등에 사용된다.

- 리더 (Reader) 또는 트랜시버 (Transceiver) : 리더는 태그가 전송하는 데이터를 수신하여 태그를 인식하거나 태그에 새로운 정보를 다시 쓰는 역할을 수행하는 장치이다. 리더가 태그에 무선 통신을 사용하여 태그에 정보를 요청하고 받은 정보를 데이터베이스에 전송한다.
- 데이터베이스 (Database) : 데이터베이스는 태그에 관련된 정보를 저장하고 관리하는 역할을 한다. 데이터베이스는 정당한 리더로부터 전송된 임의의 태그의 정보를 통해서 개체를 식별하고 수집된 정보의 진위를 판별하는 기능을 수행한다. 데이터베이스는 연산 능력이 낮은 리더나 태그를 대신하여 연산을 수행하기도 한다.

본 논문에서 다루는 저가형 RFID 시스템은 다음의 가정 하에서 동작한다.

- 태그는 리더로부터 전원을 공급하는 수동형 태그이다. 이 수동형 태그는 리더와 수 미터에서 통신이 가능하며 수 백개의 비트를 저장할 수 있다.
- 태그와 리더 사이의 통신 채널은 공격자의 공격에 안전하지 않다고 가정한다. 이 영역에서는 공격자가 시스템에 공격을 가할 수 있다.
- 리더와 데이터베이스 사이의 통신 채널은 공격자의 공격에 안전하다고 가정한다.

2.2 RFID 시스템의 문제점

RFID 시스템의 특성상 리더와 태그는 비 접촉의 무선 통신을 사용하여 데이터를 주고받는다. 태그는 주위의 리더의 신호에 반응하여 자신의 고유정보를 리더로 전송한다. 즉, 태그는 주위 리더가 정당한 리더인지에 대한 확인 없이 자신의 고유 정보를 리더로 전송한다. 이러한 RFID 동작 원리는 리더 주변의 제 삼자가 손쉽게 사용자의 구매 이력이나 위치 정보를 얻을 수 있으므로 사용자의 프라이버시 침해 문제를 발생시킨다. RFID 시스템에서는 사용자 프라이버시 침해에 관련해서 다음의 두 가지 문제점이 언급된다.[7]

(1) 사용자의 개인정보 노출 문제점 : RFID 시스템이 널리 사용됨에 따라 사람들은 개체에 태그가 내장된 다양한 물건들을 지니게 될 것이다. RFID 시스템은 주위의 리더의 질의에 무분별하게 태그 고유의 정보를 전송하기 때문에 물건에 내장된 태그는 사용자가 다른 사람에게 알리고 싶지 않은 정보, 예를 들면, 고가의 물건의 소유, 특정 병력에 관한 약품 소지 등에 대한 정보를 제 삼자에게 제공할 수 있다. 그래서 사용자에 대한 다양한 정보가 사용자의 동의 없이 누출될 수 있다.

(2) 사용자의 위치 추적 문제점 : 사용자가 태그가 내장된 물건을 구매할 때, 공격자는 사용자와 태그의 고유 정보에 연관성을 줄 수 있다. 더구나 사용자는 태그가 내장된 물건을 지니고 다니기 때문에 공격자는 태그 고유 정보를 이용하여 사용자의 이동 경로를 추적할 수 있다.

Ⅲ. 안전한 RFID 시스템 설계 고려사항

RFID 시스템은 리더와 태그 간에 무선 통신을 사용하며 태그의 고유 정보에 대한 무분별하게 전송하는 동작 원리로 인해서 여러 위협에 노출되기 쉽다. 이러한 취약점들은 공격자가 기존의 다른 시스템에서 보다 적은 노력으로 원하는 정보를 얻을 수 있게 한다. 본 장에서는 태그의 비밀 정보를 얻기 위해서 RFID 시스템에 공격자가 행할 수 있는 공격 방법들에 대해서 알아보고 기존에 제안된 프라이버시 보호 기법들의 안전성에 대해 분석해 본다. 그 후, 이러한 공격에 안전한 RFID 시스템을 설계함에 있어 고려해야 할 사항들에 대해서 알아본다.

3.1 RFID 시스템의 공격 방법

일반적으로, 공격자는 능동적인 공격자와 수동적인 공격자로 나뉜다. 수동적인 공격자는 리더와 태그 사이에 전송되는 메시지에 대해 도청만이 가능하며, 능동적인 공격자는 리더와 태그간의 통신을 도

청 가능할 뿐만 아니라 두 개체 사이에 전송되는 메시지를 변형하여 메시지를 전송하는 것과 같은 다양한 공격을 할 수 있다. RFID 시스템에 공격자가 행할 수 있는 공격의 방법은 다음과 같다.

(1) 도청 : 수동적인 공격자는 리더와 태그 사이에 전송되는 메시지를 도청할 수 있다. 공격자는 도청을 통해서 쉽게 사용자의 비밀 정보를 얻거나, 도청된 메시지를 활용하여 이후 설명되는 여러 가지 공격방법을 적용하여 사용자의 위치 정보를 얻을 수도 있다. RFID 시스템은 무선 통신을 사용하기 때문에 공격자가 통신을 도청하는 것을 막는 것은 불가피하다. 그러므로 도청이 불가능하게 하는 것이 목적이기 보다는 도청하는 것만으로는 사용자의 비밀 정보를 얻을 수 없으며, 도청된 정보를 통해 다른 공격에 활용 가능한 어떠한 정보도 얻을 수 없도록 하여야 한다.

(2) 위조 : 이 공격은 능동적인 공격자에 의해 이루어지며 공격자는 정당하지 않은 개체를 정당한 것처럼 속여 인증과정을 통과하는 방법이다. 이러한 위조 공격은 두 가지 유형으로 나눌 수 있다.

- 재전송 공격 (Replay Attack) : 공격자는 리더와 특정 태그 사이에 전송되는 데이터를 도청하고 도청한 메시지를 저장한다. 리더와 특정 태그 사이의 통신이 정상적으로 종료된 이후에 공격자는 임의의 태그를 특정 태그로 가장하기 위해 저장한 메시지를 사용한다.

  우선, 공격자는 특정 태그와 리더 사이의 통신을 도청하고 도청한 데이터를 임의의 태그에 도청한 데이터를 저장한다. 리더로부터 질의를 받았을 때 임의의 태그는 저장된 메시지를 전송한다. 리더는 전송된 메시지를 통해서 자신과 통신하는 태그를 이 메시지를 생성한 태그로 인식 가능하다. 즉, 공격자는 임의의 태그를 특정 태그로 위조가능하다.
- 스푸핑 공격 (Spoofing Attack) : 이 공격을 위해서 우선, 공격자는 리더로 가장하여 특정 태그, 위조하고자 하는 태그로부터 전송되는 데이터를 받는다. 공격자는 데이터를 받고 리더와 태그 사이의 정상적으로 통신이 종료되기 전에 그 세션을 종료한다. 공격자는 그 태그로부터 전송받은 데이터를 사용하여 리더를 속여 특정 태그인척 할 수 있다. 예로 들면, 상점에서 태그가 내장된 싼 가격의 상품에 공격자는 리더로 위장하여 인증 받을 수 있는 정보를 얻고 정상적인 인증과정을 위한 과정이 완료되기 전에 통신을 종료한다. 그 이후에 공격자는 고가의 상품을 구매하는 과정에서 싼 가격의 상품에서 얻은 데이터를 사용하여 고가의 상품을 싼 가격의 상품으로 인증 받고 구매할 수 있다.

(3) 메시지 차단 (message interception) : 이 공격은 서비스 거부 공격의 유형의 것으로, 공격자가 고의로 리더와 태그 사이에 전송되는 데이터를 가로챌 수 있다 (때로는 시스템의 문제로 인해서 발생하기도 한다). 이러한 공격은 인증 세션의 비정상적인 종료뿐만 아니라 메시지 유실로 인해 리더와 태그 사이의 동기가 어긋나게 되어 정당한 태그가 더 이상 사용될 수 없는 경우가 발생된다.

3.2 기존에 제안된 프라이버시 보호 기법 분석

사용자의 프라이버시를 보호하기 위해 제안된 기존의 기법 중 가장 단순한 방법은 킬(kill) 명령어 기법이다.[1] 킬 명령어 기법은 Auto-ID 센터에 의해 제안된 기법이며, 사용자의 프라이버시를 보호하기 위해서 물건이 계산대에서 리더에 읽혀질 때, 리더가 태그가 더 이상 동작하지 못하도록 킬 명령어를 전송하는 것이다. 그러나 이 방법은 홈 네트워크와 같은 유비쿼터스 환경에 적용되어야 하는 RFID 태그를 단순히 무력화 시킨다는 점에서 프라이버시를 보호하기 위한 적당한 해결책이라고 할 수 없다. 이러한 킬 명령어 기법과 유사한 물리적인 기법으로는 Faraday Cage 와 active jamming 기법이 있으나 사용자의 프라이버시를 보호하기에는 적합하지 않다.[6] 그 이후, RFID 시스템에서 정당한 리더와 데이터베이스는 태그를 이용하여 사용자와 유용한 서비스가 가능하며, 정당하지 않은 개체들은 태그에 대한 어떤 정보도 얻지 못하도록 하여 사용자의 프라이버시를 보호하는 기법들이 제안되었다.[2-5,7-11,15,16]

기존에 제안된 방법들은 해쉬 함수, 암호화 알고리즘과 같은 암호학적 방법들을 사용하는 기법들[2,4,7-11,15,16]과 XOR 함수를 사용하는 기법[3]이 있다.

표 1. 해쉬 함수/재 암호화 기법 ○ : 안전, × : 불안전

기반	기법		위치 추적	위조		메시지 차단	태그 해쉬연산 (재 암호화) 횟수
				스푸핑	재전송		
해쉬 기반	[16]	기법 1	가능	×	×	○	1
		기법 2	불가능	×	×	○	1
	[11]		불가능	×	○	○	2
	[2,15]		불가능	×	○	○	2
	[8]		불가능	×	○	○	3
	[9]		불가능	○	○	○	2
	[10]		불가능	○	○	○	3
재 암호화	[4]		가능	-	-	○	0
	[7]		가능	×	○	○	1

(1) 해쉬 함수 기반 기법 : 해쉬 함수를 사용하는 기법으로 대표적인 것이 해쉬 락 (hash lock) 기법이다.[16] 이 기법은 해쉬 함수를 사용한다는 점에서 저가의 태그에 적용될 수 있다. 그러나 리더와 태그 사이의 통신에서 고정된 해쉬 아이디 (meta ID=hash(key))를 사용한다는 점에서 공격자가 태그의 위치를 추적할 수 있으며 이로 인해 사용자의 프라이버시도 침해된다. 이러한 문제점을 해결하기 위해, Weis은 태그가 의사 난수 생성기(pseudo random generator)를 사용하여 리더의 질의에 대해서 태그가 항상 랜덤한 값을 응답할 수 있도록 하는 기법을 제안하였다.[16] 그러나 [16]의 논문에 제안된 기법들은 공격자의 재전송, 스푸핑 공격에 안전하지 않다. 그 이외에도 해쉬 함수 기반의 기법이 제안되었으며 다음과 같다.

Ohkubo은 두개의 해쉬 체인을 사용하여 사용자의 프라이버시를 보호하는 기법을 제안하였다.[11] 그러나 이 기법은 데이터베이스가 리더의 질의에 대한 태그의 응답이 정당한 것인지를 확인하기 위해서 계산하여야 하는 해쉬 값이 태그의 수에 비례한다는 문제점을 갖는다. 그 이후, 이 기법의 효율성을 향상시키기 위한 여러 가지 기법들이 제안되었다.[2,15] 또한 Henrici은 일방향 해쉬 함수를 사용하여 추적될 수 있는 태그의 ID를 변화 시키는 기법을 제안하였으나 공격자의 스푸핑 공격에 취약하다는 문제점을 가지고 있다.[8] 최근에는 해쉬 기반의 스푸핑 공격에도 안전한 기법이 이수미 등에 의해서 제안되었으며[9], 다양한 서비스 제공이 가능한 분산 환경에 적합한 해쉬 기반의 기법도 제안되었으나 이 기법도 데이터베이스가 데이터베이스에 저장된 태그의 수에 의존하여 계산하여야 한다는 점에서 시스템 적용에 문제점을 갖는다.[10]

(2) 재 암호화 기반 기법 : 해쉬 함수 이외의 암호학적 함수를 사용하는 방법으로는 재 암호화 기법이 있다.[4,7] Juels는 유로 화폐에 태그를 삽입하여 사용자의 프라이버시를 보호하는 기법을 제안하였다.[4] 이 기법은 특정 리더만이 태그 정보의 정확성을 확인 할 수 있다는 가정 하에서 안전성이 보장된다. Saito는 태그가 매 세션마다 리더로부터 받은 one-time 랜덤 값들을 사용하여 태그의 비밀 정보를 재 암호화하여 전송함으로써 사용자의 프라이버시를 보호하는 기법을 제안하였다.[7] 그러나 이 두 기법 모두 재 암호화 방법으로 공개키 암호화 알고리즘을 사용하므로 태그의 제한된 계산 능력으로 인해서 외부의 제 삼자에 의해 이러한 동작이 수행되어야 한다. 이점은 재 암호화 기법을 사용하기 위해 외부 인프라를 형성하여야 한다는 단점을 가진다. 또한 일정 기간 동안 태그의 재 암호화가 수행되지 않는다면 고정된 암호화 값으로 인해 위치 추적이 가능 할 수도 있다. 표 1에서 해쉬 함수와 재 암호화 기반 기법들에 대한 안전성에 대해 간략히 제시한다.

(3) XOR 기반 기법 : 최근, Juels은 최저가의 태그를 위한 프라이버시 보호 기법을 제안하였다.[3] 이 기법은 단지 XOR (exclusiveor)

연산을 사용하기 때문에 최저가의 RFID 시스템에 적용 가능하다. 이 기법에서 태그는 리더로부터 세션마다 다음 세션에 사용할 랜덤 값들을 받으며, 동일한 랜덤 값들을 가지고 있는지에 대한 확인 과정을 통해 상호 인증을 한다. 이와 같이 매 세션마다 랜덤한 값을 사용하여 태그에서 리더로 정송하는 값을 변경하기 때문에 공격자에 의한 태그의 위치 추적이 불가능하다. 그러나 제안된 기법은 공격자가 정해진 세션 (2m 개 이하)만을 도청할 수 있다는 가정 하에서 안전성이 보장된다. 만약 공격자가 가정 이상의 세션을 도청 하게 된다면 도청한 값들을 사용하여 태그의 비밀 정보를 알아 낼 수 있다. 이 기법에 대해 구체적인 값에 대해 간략히 설명하도록 하겠다.

Juels 기법에서 태그는 비밀 값 k개를 저장한다. 비밀 값은 $(\alpha_i,\beta_i,\gamma_i), 1 \le i \le k$로 구성되어 있다. 태그와 데이터베이스가 저장하고 있는 랜덤 값 테이블은 m개의 $\triangle_i = \{\delta_i^{(1)}(=(\triangle\alpha_i^{(1)}, \triangle\beta_i^{(1)}, \triangle\gamma_i^{(1)})), ..., \delta_i^{(m)}\}$, $1 \le i \le k$로 구성되어 있다. 태그는 리더의 질의에 α_d, $d \leftarrow (c \bmod k)+1$ (c: 카운터, 처음에 0으로 초기화 되어 있는 값) 에 대응되는 값을 리더에 전송하고 리더는 데이터베이스에 전송하며 데이터베이스는 받은 값과 관련된 β_d를 리더에 전송한다. 리더는 β_d을 태그에 전송하고 γ_d을 받고 데이터베이스에 전송한다. 데이터베이스는 받은 값을 데이터베이스 테이블에서 확인한 후 리더가 태그에 전송할 새로운 랜덤 값 테이블을 생성하여 전송하며 새로 생성된 랜덤 값 테이블은 $\widetilde{\triangle_i} = \{\tilde{\delta}_i^{(1)}(=(\triangle\tilde{\alpha}_i^{(1)}, \triangle\tilde{\beta}_i^{(1)}, \triangle\tilde{\gamma}_i^{(1)})), ..., \tilde{\delta}_i^{(m)}\}, 1 \le i \le k$로 구성된다. 이 랜덤 값 테이블을 받아서 태그는 기존의 랜덤 값 테이블 갱신에 필요한 값을 생성한다. 우선, 기존의 $\triangle_i = \{\delta_i^{(1)}, ..., \delta_i^{(m)}\}, 1 \le i \le k$ 값의 원소에 $\delta_i^{(j)} = \delta_i^{(j+1)}$, $1 \le j \le m-1$을 적용하고, 마지막 값은 $\delta_i^{(m)} = 0^{3\ell}$로 갱신한다. 리더로부터 받은 $\widetilde{\triangle_i} = \{\tilde{\delta}_i^{(1)}(=(\triangle\tilde{\alpha}_i^{(1)}, \triangle\tilde{\beta}_i^{(1)}, \triangle\tilde{\gamma}_i^{(1)})), ..., \tilde{\delta}_i^{(m)}\}$과 위의 과정에서 생성한 $\triangle_i = \{\delta_i^{(1)}, ..., \delta_i^{(m)}\}, 1 \le i \le k$을 XOR한다. 즉 $\delta_i^{(j)} = \delta_i^{(j)} \oplus \tilde{\delta}_i^{(j)}, 1 \le i \le k, 1 \le j \le m$을 생성한다. 태그는 다음 세션에 이전 세션의 비밀 값 $(\alpha_i,\beta_i,\gamma_i)$에 $\delta_i^{(1)}$을 XOR하여 새로운 랜덤 값 테이블을 생성한다. 이 랜덤 값 테이블의 값은 다음 세션에 사용된다.

3.3 안전한 RFID 시스템 요구사항

RFID 시스템에서의 여러 가지 위협으로부터 사용자 프라이버시를 보호하기 위해 3.1절에서 언급한 공격에 안전한 RFID 시스템을 설계하여야 한다. 결과적으로, RFID 시스템은 다음의 요구사항들을 만족하여야 한다.

- 구별 불가능성 : 태그의 출력 값은 랜덤 값과 구별 불가능해야 하며, 태그의 ID와 연결되지 않아야 한다. 만약 공격자가 특정 태그의 출력 값을 랜덤 값과 구별 가능하거나 태그들이 출력한 값들에서 특정한 태그의 값들을 찾아 낼 수 있다면, 공격자는 특정 태그를 구별 가능하고 추적 가능하다.

RFID 시스템에서는 통신하는 상대(리더 나 태그)에 대한 인증 절차 없이 통신이 이루어지기 때문에 공격자는 리더나 태그에 대해 위조할 수 있다. 그래서 RFID 시스템은 리더와 태그 사이의 통신에서 상호 인증하는 과정이 필요하다.

- 상호 인증 : 상호 인증이란 태그 (또는 리더)가 자신과 통신하는 리더 (또는 태그)가 정당한 개체라고 확신하는 것이다.

(1) 리더의 태그 인증 : 리더는 자신과 통신하는 태그가 정당한 태그라는 것을 확신할 수 있어야만 한다. 만약 리더가 태그의 정당성을 인증하는 과정을 수행하지 않는다면, 공격자는 RFID 시스템에 위조 공격 (재전송, 스푸핑)을 행할 수 있다.

- 재전송 공격의 경우, 공격자는 리더와 특정 태그 사이의 통신을 도청하여 저장한다. 그 이후 공격자는 리더의 질의에 대해 특정 태그로 임의의 태그를 위장하기 위해서 저장했던 메시지를 전송한다. 만약 리더가 태그를 인증하는 과정을 수행한다면, 공격자는 특정 태그로 위장할 수 없을 것이다.

- 스푸핑 공격의 경우, 공격자는 리더로 위장하여 특정 태그의 정보를 얻는다. 이 과정은 재전송 공격과 달리 태그와 리더 사이의 하나의 세션이 완료되기 전에 필요한 정보를 태그로부터 얻고 그 세션을 종료한다. 그 이후 공격자는 특정 태그를 임의의 태그로 위장 할 수 있다.

(2) 태그의 리더 인증 : 태그는 자신과 통신하는 리더가 정당한 태그라는 것을 확실 할 수 있어야만 한다. 만약 태그가 리더의 정당성을 인증하는 과정을 수행하지 않는다면, 공격자는 RFID 시스템에서의 리더로 위장할 수 있으며 특정 태그에 질의를 통해서 태그의 정보를 얻을 수 있다. 이러한 문제점은 공격자가 자신과 통신하는 태그가 정당한지를 확인하지 않고 비밀 정보를 전송하는 것에서 발생하는 사용자의 프라이버시 침해 문제를 야기 시킨다.

3.1절에서 설명했듯이 RFID 시스템에서 공격자는 리더와 태그 사이의 통신에서 고의로 메시지를 차단할 수 있으며, 이로 인해서 정당한 태그가 더 이상 동작하지 못하게 될 수도 있다. 그러므로 공격자의 메시지 차단 공격에 대해서 RFID 시스템은 다음과 같은 조건을 만족해야 한다.

- 메시지 차단 : 만약 공격자가 고의로 메시지 차단이 발생한 경우, 데이터베이스는 메시지 차단(유실)이 발생하였다는 것을 감지 할 수 있어야 한다. 만약 태그가 리더로부터 메시지를 받고 그 메시지를 다음 세션에 리더와의 통신에 사용한다면, 태그와 데이터베이스 사이의 인증을 위한 메시지에 대한 동기화를 유지하는 것이 중요하다. 그러므로 공격자의 메시지 차단으로 이전 세션의 인증 메시지를 사용하여 태그와 통신하는 경우 데이터베이스는 정당한 태그가 정상적으로 동작할 수 있도록 인증에 필요한 데이터를 복원할 수 있어야 한다. 이 요구사항은 태그와 데이터베이스 사이에 데이터 동기화가 필요 없는 환경에서는 고려되지 않을 수도 있다.

Ⅳ. 제안 프로토콜

본 장에서는 최저가의 태그에 적합한 효율적이고 안전한 상호 인증 프로토콜을 제안한다. 제안 프로토콜은 단순한 비트 연산만을 사용하기 때문에 효율적이며, 공격자가 리더와 태그 사이의 통신을 모두 도청 가능하다는 가정에서도 안전하다. 제안 프로토콜은 시스템 초기화 단계와 상호 인증 단계로 구성된다.

표 2. 표기법

연산자	표기법
비트 덧셈	+
비트 XOR (exclusive-or)	⊕
메시지 m과 w의 연접	m‖w
m의 i번째 세션 메시지	mi

우선, 제안 프로토콜을 설명하기 전에 제안 프로토콜에 사용되는 표시법에 대해 알아보도록 한다. 프로토콜에 사용되는 표기법은 표 2에서 설명된 것과 같다. 설명된 표시법을 바탕으로 하여 제안 프로토콜에 대해서 알아보도록 한다.(본 장에서의 프로토콜의 설명은 첫 번째 세션을 설명하고 있으며 그 이후의 세션은 동일 방법으로 확장하여 적용하면 된다.)

4.1 초기화 단계

초기화 단계에서는 태그와 데이터베이스는 비밀 정보와 태그의 ID를 저장한다. 태그 제조자는 다음과 같은 초기화 단계를 수행한다.

(1) 태그 제조자는 ℓ 비트의 네 개의 비밀 값 α, β, γ, λ를 생성하고 96 비트의 태그 ID를 선택한다. (Juels의 기법에서는 ℓ 비트를 80 비트 정도로 제시하고 있으며[3] Auto-ID 센터에 의한 EPC (Electronic Product Code)의 표준은 태그 ID 의 길이를 64, 96, 256 비트의 상품 체계에 기반하고 있다[5])

(2) 태그 제조자는 ℓ 비트의 네 개의 랜덤 값 r_1, s_1, k_1, t_1를 선택한다.

- 제안 기법에서 사용된 파라미터의 의미는 다음과 같다.
  - r, s는 태그와 리더간의 상호 인증을 위해서 사용되며 이 과정에서 기존에 사용된 α, β를 사용하는 경우 공격자가 태그와 리더의 통신을 도청함으로써 태그의 비밀 값 α, β을 알 수 있기 때문에 γ, λ

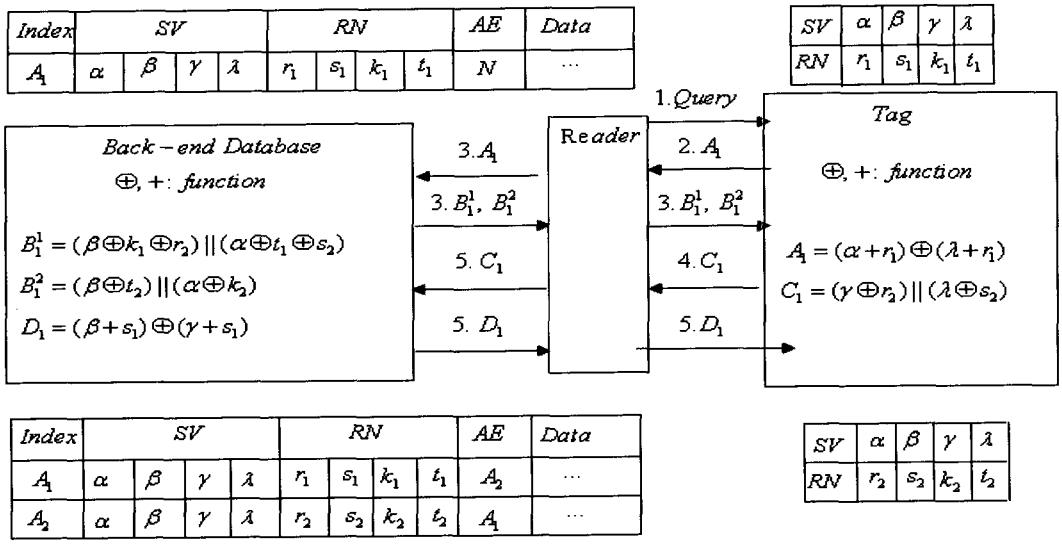


그림 2. 제안 프로토콜

값이 필요하다.

- k, t의 랜덤 값은 α, β 값과 같이 사용되어 다음 세션에 사용될 r, s, k, t랜덤 값에 대한 정보를 비밀 값을 알고 있는 정당한 태그만이 알 수 있도록 하는데 필요하다. 만약 상호 인증을 위해 사용된 r, s만 사용될 경우 비밀 값을 모르는 공격자도 태그인척 할 수 있기 때문에 네 개의 랜덤 값이 필요하다.

(3) 태그 제조자는 선택한 4개의 랜덤 값, 비밀 값, 태그의 ID를 데이터베이스의 첫 번째 행에 저장하고, 태그에도 동일하게 저장한다. 데이터베이스의 AE-필드는 Null 값으로 초기화 된다. 데이터베이스의 데이터 필드는 각각의 태그와 관련된 태그 ID, 태그 위치 정도 등 다양한 정보들을 포함한다.

데이터베이스에서 사용될 AE-필드는 처음 Hernici에 의해서 제시되었으며[8], 현재 세션에서 데이터 유실이 발생하였을 때 데이터베이스에서 태그의 이전 데이터를 찾기 위해 사용된다. AE-필드가 데이터 유실 복구의 성질을 제공하기 위해서 데이터베이스는 다음과 같이 동작한다. 데이터베이스는 하나의 세션이 끝난 후에는 항상 두개의 행이 생성된다. 첫 번째 행에는 다음 세션에 사용될 값을 저장하고 두 번째 행에는 이전 세션에 사용된 값을 저장한다. 만약 공격자가 태그로 전송되는 데이터를 가로챈다면, 태그는 현재의 세션에서 새로운 값을 받지 못하여 다음 세션에서 이전 세션에서 리더에 전송했던 것과 동일한 값을 전송하게 된다. 이 과정에서 데이터베이스는 AE-필드를 참조하여 데이터베이스에서 사용된 태그의 값들을 찾을 수 있다.

4.2 상호 인증 단계

이 과정에서는 태그와 리더는 다음의 과정을 통해서 서로를 인증한다. 그림 2에서 제안 프로토콜의 동작 과정을 나타내고 있다.

단계 1. (리더 → 태그) 리더는 태그에 질의를 보낸다.

단계 2. (태그 → 리더) 태그는 리더의 질의에 응답하기 위해 다음의 과정을 수행한다.

(1) 태그는 비밀 값 α와 λ를 사용하여 ℓ 비트의 $A_1 = (\alpha + r_1) \oplus (\lambda + r_1)$을 생성한다. 만약 $(\alpha + r_1)$또는 $(\lambda + r_1)$값이 ℓ 비트 이상일 경우, 발생한 캐리는 버린다.

(2) 태그는 리더의 질의에 대한 응답으로 A_1을 전송한다.

단계 3. (리더 → 태그) 리더는 태그로부터 A_1을 받았을 때 다음의 과정을 수행한다.

(1) 리더는 데이터베이스에 A_1을 전송한다.

(2) 데이터베이스는 A_1을 사용하여 데이터베이스에서의 위치를 찾는다. 데이터베이스는

네 개의 랜덤 값 r_2, s_2, k_2, t_2을 생성하고, 2ℓ 비트의 $B_1^1 = (\beta \oplus k_1 \oplus r_2) \| (\alpha \oplus t_1 \oplus s_2)$와 $B_1^2 = (\beta \oplus t_2) \| (\alpha \oplus k_2)$를 생성하여 리더에게 B_1^1, B_1^2을 전송한다.

(3) 리더는 태그에 B_1^1, B_1^2을 전송한다.

단계 4. (태그 → 리더) 리더는 B_1^1, B_1^2을 받고 다음의 과정을 수행한다.

(1) 태그는 저장된 값 β, α, k_1, t_1을 사용하여 B_1^1에서 다음 세션에 사용할 r_2, s_2을 추출해 내고, α, β를 사용하여 B_1^2에서 다음 세션에 사용할 k_2, t_2을 추출해 낸다.

(2) 태그는 추출한 값 r_2, s_2을 사용하여 2ℓ 비트의 $C_1 = (\gamma \oplus r_2) \| (\lambda \oplus s_2)$을 생성하여 리더에 전송한다.

단계 5. (리더 → 태그 : 태그 인증) 리더는 태그로부터 C_1받고 다음이 과정을 수행하여 태그를 인증한다.

(1) 리더는 데이터베이스에 C_1값을 전송한다.

(2) 데이터베이스는 리더로부터 받은 C_1값이 데이터베이스 값으로 생성한 $(\gamma \oplus r_2) \| (\lambda \oplus s_2)$과 동일한지를 확인하는 것으로 태그를 인증한다.

- 만약 두 값이 동일하지 않다면, 데이터베이스는 리더에게 "프로토콜 중단" 메시지를 전송하고 프로토콜을 중단한다.
- 그렇지 않다면, 데이터베이스는 데이터베이스의 두 번째 행에 첫 번째 행의 비밀값과 새로 생성한 랜덤 값 r_2, s_2, k_2, t_2값을 저장한다.

(3) 데이터베이스는 $A_2 = (\alpha + r_2) \oplus (\lambda + r_2)$을 생성하여 두 번째 행의 인덱스로 사용한다 (만약$(\alpha + r_2)$나 $(\lambda + r_2)$의 값이 ℓ 비트 이상이면, 발생한 캐리는 버린다). AE-필드의 첫 번째 행은 A_2로 채워지고 두 번째 행은 A_1으로 채워짐으로서 서로 참조하도록 구성한다.

(4) 데이터베이스는 $D_1 = (\beta + s_1) \oplus (\gamma + s_1)$을 생성하여 리더에게 전송한다 (만약$(\alpha + r_2)$나 $(\lambda + r_2)$의 값이 ℓ 비트 이상이면 발생한 캐리는 버린다). 리더는 전송 받은 D_1을 태그에 전송한다.

단계 6 .(리더 인증) 태그는 리더로부터 받은 D_1 값과 자신이 생성한 $(\beta + s_1) \oplus (\gamma + s_1)$값이 동일한지를 확인하는 것으로 리더를 인증한다. 만약 두 값이 동일하면, 태그는 저장된 랜덤 값 r_1, s_1, k_1, t_1을 r_2, s_2, k_2, t_2으로 대체한다.

V. 제안 기법의 안전성과 효율성

본 절에서는 제안 프로토콜에 대한 효율성과 안전성에 대해 논의하고자 한다.

5.1 안전성

제안된 기법은 안전한 RFID 시스템 설계 요구조건을 고려하여 분석한다. 본 논문에서 제안하는 프로토콜은 상호 인증, 메시지 차단과 구별 불가능의 요구조건을 만족한다.

- 상호 인증 : 제안 프로토콜은 상호 인증을 제공한다. 만약 리더와 태그가 제안 프로토콜을 수행하면, 그들은 서로를 정당한 개체로 인증해야만 한다. 제안 프로토콜에서 태그와 리더 사이에 전송되는 메시지는 XOR 연산과 (또는) 덧셈 연산을 사용하기 때문에 전송된 메시지에 사용된 랜덤 값을 아는 공격자만이 전송되는 메시지에서 비밀 값을 추출해 낼 수 있다. 그러나 랜덤 값은 데이터베이스에서 생성한 값이기 때문에 공격자가 랜덤 값을 얻기 위해 태그의 비밀 값들에 대해서 알고 있어야만 한다. 이것은 정당한 개체 (태그, 리더) 만이 제안 프로토콜을 통해 서로를 인증할 수 있는 메시지를 생성할 수 있다. 더욱이, 태그에 저장된 랜덤 값들은 데이터베이스에서 생성하여 전송한 랜덤 값으로 대체된다. 그러므로 제안 프로토콜은 위장 공격인 재전송과 스푸핑 공격에 안전하다.

  (1) 리더의 태그 인증 : 만약 태그가 정당하지 않다면, 그 태그는 단계 2, 4의 메시지를 생성할 수 없다. 단계 2, 4의 메시지는 비밀 값과 랜덤 값으로 구성된다. 제안 프로토콜에서는 공격자가 도청을 통해서 랜덤 값과 비밀 값에 대한 정보를 얻을 수 없다. 그래서 정당하지 않은 태그가 리더의 태그

인증 과정을 통과하기 위해 단계 2, 4에 적합한 메시지로 $\{0,1\}^{\ell}$, $\{0,1\}^{2\ell}$에서 ℓ 비트, 2ℓ 비트의 랜덤한 값들을 선택해야만 한다. 이 과정에서 공격자의 정당하지 않은 태그가 정당한 개체로 인증될 수 있는 확률은 최대 $1/(2^{2\ell})$이다. 이 확률은 아주 작은 값이다. 그러므로 정당하지 않은 태그가 리더의 태그 인증 과정인 단계 5를 통과할 수 있는 데이터를 생성하는 것이 불가능하다. 이러한 이유에서 제안 프로토콜은 위장 공격인 재전송과 스푸핑 공격에 안전하다. 공격자가 스푸핑 공격을 행할 경우, 공격자는 리더로 가정하여 태그로부터 A의 정보를 얻을 지라도 단계 4 의 값을 생성 할 수 없기 때문에 스푸핑 공격에 성공 할 수 없다. 또한, 재전송의 공격의 경우, 공격자가 이전 세션에서 도청한 값 A을 사용하여 리더에 전송 할 지라도 세션마다 새로운 랜덤 값을 생성하여 태그에 전송하기 때문에 이전에 도청한 C 값으로 리더의 인증 과정 단계 5를 통과 할 수 없다.

(2) 태그의 리더 인증 : 만약 리더가 정당하지 않다면, 그 리더는 단계 3, 5의 메시지를 생성 할 수 없다. 단계 3, 5의 메시지도 비밀 값과 랜덤 값으로 구성된다. 제안 프로토콜에서 공격자는 단계 3, 4의 메시지를 생성하는데 사용될 랜덤 값과 비밀 값을 얻을 수 없다. 이 과정에서 공격자의 정당하지 않은 리더가 정당한 개체로 인증 될 확률은 '리더의 태그 인증' 과정에서와 같은 성공 확률을 갖는다. 이 확률은 아주 작은 값이다. 그러므로 정당하지 않은 리더는 결코 단계 6의 과정을 통과 할 수 없다. 그 후, 태그는 더 이상 확인 과정에 실패한 리더와 통신을 멈추고 기존의 랜덤 값을 전송받은 랜덤 값으로 대체하지 않는다.

이와 같이 단지 정당한 리더와 태그들만이 제안하는 프로토콜을 만족하는 정당한 메시지를 생성할 수 있다.

제안하는 프로토콜에서 태그는 리더가 전송하는 새로운 랜덤 값을 받아서 다음 세션에 사용한다. 이러한 기법을 사용하는 RFID 시스템에서는 태그와 데이터베이스 사이의 인증을 위해 필요한 메시지에 대한 동기화 유지가 필요하다.

- 메시지 차단 : 제안하는 프로토콜에서 태그는 리더가 전송하는 새로운 랜덤 값을 받는다. 이 과정에서 메시지 차단의 공격이 발생할 수 있다. 만약 공격자가 리더와 태그 사이에 전송되는 메시지를 가로챈다면 태그는 다음에 리더와 통신하는 과정에서 변경되지 않은 값을 사용하여 응답할 것이다. 제안하는 프로토콜은 상호 인증을 제공하면서 메시지 차단 공격을 감지하고 데이터를 복구하는 기능을 제공한다. 예를 들면, 공격자가 제안하는 프로토콜의 첫 번째 세션의 마지막 단계에 전송되는 메시지 D_1을 가로챈다면, 태그는 현재 세션에서 사용된 랜덤 값들을 다음 세션에도 사용하게 된다. 그러나 데이터베이스는 D_1값을 생성해서 전송하면서 그 태그가 다음 세션에 사용할 인덱스 A_2를 생성하게 된다. 즉, 데이터베이스와 태그 사이의 동기가 어긋나게 된다. 그 후 리더의 질의를 받은 태그는 A_1의 값을 전송하게 된다. 데이터베이스는 값 A_1을 이용하여 태그와 관련된 값이 저장된 데이터베이스의 위치를 찾아낼 수 있다.

게다가 제안하는 프로토콜에서 태그는 매 세션마다 새로운 랜덤 값들을 사용하기 때문에 태그 출력 값들에 대한 구별 불가능의 요구조건을 만족한다.

- 구별 불가능 : 제안하는 프로토콜에서 랜덤 값 r, s, k, t은 매 세션마다 리더로부터 새로운 값을 받아 연속적으로 변경된다. 세션마다 새로운 랜덤 값으로 대체되기 때문에 공격자는 랜덤 값과 특정 태그의 출력 값들을 구별할 수 없다. 그래서 공격자는 특정 태그에 대한 어떤 정보도 얻을 수 없으며 특정 태그의 이동 경로를 추적할 수 없다. 이것은 누구도 그 특정 태그를 소유한 사용자의 위치 정보를 알 수 없다는 것을 의미한다.

5.2 효율성

논문[1, 4, 16]에 제안된 기법들은 해쉬 함수와 암호화 알고리즘과 같은 암호학적 함수를 사용한다. 그러나 AES와 같은 대칭 암호화 알고리즘을 구현하는데 20,000에서 30,000개의 게이트 (gate)가

표 3. 제안 기법의 효율성과 안전성 비교

	Juels의 기법	제안 기법
태그 사용 연산자	비트 XOR 연산	비트 XOR 연산, 덧셈 연산
다음 세션을 위해 태그가 리더로부터 받는 랜덤 값	$\ell \cdot (3km)$	$2\ell \cdot (2)$
태그 연산 횟수	$3km$(XOR)	8(XOR) + 4(덧셈)
태그 저장 데이터양	$\ell \cdot (3km+3k)$	$\ell \cdot 8$
안전성	정해진 세션만 도청 가능한 공격자에 안전	모든 세션 도청 가능한 공격자에 안전

필요하며 SHA-1과 같은 해쉬 함수를 구현하는데도 많은 비용이 요구된다.[1,16]

저가의 RFID 시스템은 전력 소비, 연산 처리 시간, 저장, 게이트(gate) 수와 같은 부분에서 많은 제약을 갖는다. MIT의 Auto-ID 센터는 5센트의 저가의 태그의 설계에 대해서 언급하였다.[12] 이러한 저가의 태그는 대략 500-5,000 게이트 정도로 구현될 수 있다. 그래서 이전에 제안된 인증 프로토콜은 최저가의 RFID 시스템에는 적용할 수 없다. 저가의 태그에 제안한 프로토콜에서 사용된 단순한 XOR, 덧셈 연산을 구현하는 것이 가능하기 때문에 제안된 기법은 저가의 RFID 시스템에 가장 적합하다.

이전에 제안된 기법에서 가장 저가의 RFID 시스템에 적용 가능한 기법은 Juels의 기법이다.[3] 이 기법은 세션의 마지막 단계에서 다음 세션에 사용될 ℓ 비트 랜덤값 $(3k) \cdot m$(m는 태그의 비밀 값의 개수이며 공격자의 세션 도청 가능횟수와 관련된 값, $3k$는 태그에 저장된 비밀 값의 개수)를 전송받는다. 태그는 전송 받은 랜덤 값을 사용하여 기존의 값들을 변경한다. 만약 Jules의 기법에서 시스템의 안전성을 강화하기 위해 m값을 크게 가정한다면, 매 세션을 도청하는 공격자에 안전한 시스템만큼의 안전성을 가질 수도 있다. 그러나 m값이 커지게 되면 마지막 세션에 태그가 받아서 처리하여야 하는 랜덤 값의 양이 그만큼 증가하게 되서 비효율적이다. 제안하는 기법은 단지 2ℓ 비트 두개의 메시지를 리더로부터 받고 4개의 랜덤 값을 다음 세션의 전송 값을 변경하는데 사용한다. 그러므로 제안하는 기법이 더 효율적이다. 그리고 Juels의 기법은 다음 세션을 위해 전송받은 $3km$에 XOR 연산을 수행하여야 하며 이 기법의 안전성은 공격자의 공격 능력에 따라 달라진다. 만약 공격자가 연속적으로 5세션 이상을 도청 할 수 없다면 $k \geq 5, m \geq 2$정도면 안전 할 것이다. 그러나 제안 기법은 공격자의 공격능력에 의존하지 않으며 8번의 XOR 연산과 4번의 덧셈을 수행해야 하며, 기존 Juels의 기법은 상호 인증을 위해서 태그에 ℓ 비트 $(3km + 3k)$개의 데이터를 저장하여야 하는 반면 제안 기법은 표 3에서 볼 수 있듯이 ℓ 비트 8개의 데이터를 저장해야 한다는 점에서 저가형의 태그에 더 적합하다.

Ⅵ. 결 론

RFID 시스템은 원거리 통신으로 사물을 인식한다는 점에서 물류, 유통, 재고 관리에 유용한 도구가 될 것이다. 그러나 RFID 시스템은 동작 원리의 특성상 사용자의 프라이버시를 침해를 야기 시킨다. 또한, RFID 시스템에서는 리더와 태그 간에 무선 통신을 사용하여 통신하기 때문에 공격자로 인한 도청, 스푸핑 공격, 재전송 공격, 메시지 차단과 같은 공격에 취약하다. 이와 같은 RFID의 문제점을 해결하기 위해서 해쉬 함수, 암호화 알고리즘, 암호학적 함수가 아닌 단순한 연산에 기반하는 여러 가지 프라이버시 보호 기법들이 제안되었다. 본 논문에서는 암호학적 함수를 사용하지 않는 단순한 비트 연산을 사용하는 저가의 RFID 시스템에 적합한 안전하고 효율적인 프로토콜을 제안한다. 제안한 프로토콜은 안전한 RFID 시스템의 설계 요구 조건을 만족할 뿐만 아니라 리더와 태그 사이의 모든 통신을 도청 할 수 있는 공격자로부터 안전하다.

지금까지 저가형의 RFID 시스템의 프라이버시를 보호하기 위해 제안된 기법들은 대부분 하나의 데이터베이스를 통해서 상호 인증 절차를 수행하는 RFID 시스템이다. 하지만 유비쿼터스 환경에서는 '언제 어디서나' 인가된 리더는 태그의 정보를 얻을 수 있어야 하기 때문에 하나의 고정된 데이터베이스와의 통신을 통해서만 상호인증이 가능한 기존의 RFID 시스템은 적합하지 않다. 그러므로 유비쿼터스 환경에 적합한 저가형의 RFID 시스템에서의 프라이버시 보호 기법에 대한 연구가 필요하다.

참 고 문 헌

[1] Auto-ID Center, "860Mhz-960MHz Class I Radio Frequency Identification Tag Radio Frequency and Logical communication Interface Specification Proposed Recommendation Version 1.0.0. Technical Report MIT-AUTOID-TR-007", *AutoID Center, MIT*, 2002.

[2] G. Avoine and Ph. Ocehslin, "A Scalable and Provably Secure Hash-Based RFID Protocol", *The 2nd IEEE International Workshop on Pervasive Computing and Communication Security -PerSec 2005, IEEE Computer Society Press*, Kauai Island, Hawaii, USA, 3, 2005

[3] A. Juels. "Minimalist cryptography for Low-Cost RFID Tags", *In The Fourth Internationl Conferecne on Security in Communication Networks-SCN 2004*, vol. 3352 LNCS, pp. 149-164, Springer-Verlag. 2004.

[4] A. Juels and R. Pappu. "Squealing euros : Privacy protection in RFID-enabled banknotes", *In proceedings of Financial Cryptography-FC'03*, vol. 2742 LNCS, pp.103-121, Springer-Verlag, 2003.

[5] EPCglobal. "EPCTM Tag Data Standards Version 1.1 Rev.1.24 Standard Specification 01", 04, 2004.

[6] A. Juels, R. L. Rivest and M. Szudlo. "The Blocker Tag: Selective Blocking of RFID tags for Consumer Privacy". *In the 8th ACM Conference on Computer and Communications Security*, pp. 103-111, ACM Press. 2003.

[7] S. Junichiro, R. Jae-Cheol and S. Kouichi, "Enhancing privacy of Universal Re-encryption scheme for RFID Tags", *EUC 2004*, Vol. 3207 LNCS, pp.879-890, Springer-Verlag, 12, 2004

[8] D. Henrici and Paul Muller. "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers". *PerSec'04 at IEEE PerCom*. pp. 149-153, 2004.

[9] L. Su Mi, H. Young Ju, L. Dong Hoon and L. Jong In. Efficient uthentication for Low-Cost RFID systems. *ICCSA05*, vol. 3480 LNCS, pp.619~629, May 2005.

[10] Keunwoo Rhee, Jin Kwak, Seungjoo Kim and Dongho Won, "Challenge-Response based secure RFID Authentication Protocol for Distributed Database Environment", SPC2005, Vol. 3450 LNCS, pp.70-84, Springer-Verlag, 4, 2005.

[11] M. Ohkubo, K. Suxuki and S. Kinoshita. "Efficient Hash-Chain Based RFID Privacy Protection Scheme", Ubcomp2004 workshop.

[12] S. E. Sarma. "Towards the five-cent tag. Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center", 2001. Abailable from http://www.autoidcenter. org.

[13] S. E. Sarma, S. A. Weis and D. W. Engels. "Radio-frequency identification systems". *CHES'02*, vol.2523 LNCS, pp.454-469, Springer-Verlag, 2002.

[14] S. E. Sarma, S. A. Weis and D. W. Engels. "RFID systems, security and privacy implications. Technical Report MIT-AUTOID-WH-014", *AutoID Center, MIT*, 2002.

[15] 유성호, 김기현, 황용호, 이필중, "상태 기반 RFID 인증 기법 프로토콜", 정보보호학회논문지, 제 4권, 6호, 12, 2004

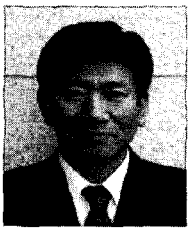
[16] S. A. Weis, S. E. Sarma, S. A. Weis and D. W. Engels. "Security and privacy Aspects of Low-Cost Radio Frequency Identification Systems". *First International Conference on Security in Pervasive Computing*, 2003. http://theory.lcs.mit.edu/sweis/spc-rfid.pdf.

〈著者紹介〉

최 은 영 (Choi, Eun Young) 학생회원
2001년 8월: 고려대학교 수학과 학사
2003년 8월: 고려대학교 정보보호대학원 공학석사
2004년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 암호 이론, 정보보호 이론, RFID 정보보호 기술, 유비쿼터스

최 동 희 (Choi, Dong Hee)
2002년 2월: 고려대학교 전산학과 학사
2004년 8월: 고려대학교 정보보호대학원 공학석사
2004년 8월~현재: LG 전자 이동 통신 기술 연구소
〈관심분야〉 모바일 통신 보안, 정보보호 이론

임 종 인 (Lim, Jong In)
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월:고려대학교 수학과 박사
1986년 9월~2001년 1월: 고려대학교 자연과학대학정교수
2001년 2월~현재: 고려대학교 정보보호대학원 원장, 고려대학교 정보보호기술연구센터 센터장
〈관심분야〉 암호 이론, 암호 정책, PET 기술



이 동 훈 (Lee, Dong Hoon) 종신회원
1983년 8월: 고려대학교 경제학사
1987년 12월: Oklahoma University 전산학 석사
1992년 5월: Oklahoma University 전산학 박사
1992년 8월: 단국대학교 전자계산학과 전임강사
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 3월~2002년 2월: 고려대학교 정보보호대학원 부교수
2002년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술