RFID Tag 보안을 위한 인증 프로토콜에 관한 연구

정회원 정 용 훈*, 김 정 재**°, 전 문 석*

A Study on Authentication Protocol for Secure RFID Tag

Yong-Hoon Jung*, Jung-Jae Kim**°, Moon-Seog Jun* *Regular Members*

요 약

본 논문에서 제안하는 시스템은 기존의 RFID 시스템의 보안성을 높이기 위하여 2차원 배열 기법을 이용하여 안전성을 확보할 수 있게 되었다. 제안하는 시스템은 RFID Tag의 고유 ID 값인 UID값과 2차원 배열을 이용하여 태그와 리더간 인증을 하게 된다. 제안하는 시스템에서 암·복호화를 하기 위해서는 태그의 고유 ID값인 UID 값과 관리자가 정의한 캐릭터 셋을 이용한 암·복호화 과정에서의 안전성을 기존의 다른 시스템과의 비교를 통해 우수함을 입증한다.

Key Words : Authentication, RFID, Character set, Two dimension array, Key exchange

ABSTRACT

Firstly, this dissertation suggests the tag ID transfer method using two-dimensional arrangement. Secondly, provide better and stable security system compare to existing one by transferring tag; ID using established two-dimensional arrangement. Thirdly, provide operating module, which possible to descramble two-dimensional arrangement, with a character set when descrambling in a tag and a server. Lastly, suggest safe key transfer using a character set and two-dimensional arrangement.

In order to embody suggested system and assess, transferred two-dimensional arrangement several times to carry out the experiment. Confirmed that it is impossible for suggested system to decode key patterns compare to existing RFID systems.

Ⅰ. 서 론

오늘날 전 세계는 정보통신 및 교통수단의 발달로 공간적 이동과 정보 교환이 급속히 빨라졌을 뿐만 아니라 언제 어디서나 원하는 정보를 실시간으로 주고 받을 수 있는 유비쿼터스 환경으로 발전하고 있다. 이에 따라 유비쿼터스 컴퓨팅에 대한 RFID(Radio Frequency Identification) 시스템이 주목 받고 있다.

RFID 시스템은 무선 주파수를 이용한 자동 인식 기술로서 물리적 접촉 없이 태그가 부착된 개체의 정보를 읽거나 기록할 수 있는 시스템으로서 제품 및 자산 관리, 운송 환경 관리, 화물 및 컨테이너 추적, 차량 접근 및 제어, 전자 문서 관리, 신원 확인, 관광, 교통, 위치 정보는 물론 사람과 동물의 이동 경로 추적 등에까지 폭 넓게 사용되어지고 있다[1].

RFID 태그와 리더는 무선으로 통신하기 때문에 리더는 노출 되지 않은 형태로 숨겨져 있을 수 있으며, 리더가 설치된 곳을 통과할 때 그 물체의 위치 정보 확인, 저장, 축적될 수 있기 때문에 보안 위협과 개인 정보 침해라는 역기능도 동시에 가지고 있다[3].

기존의 정보시스템을 대상으로 한 정보보호를 위

* 숭실대학교 컴퓨터학과({s0178, mjun}@ssu.ac.kr), ** (주)리테일테크(argniss@nate.com) (° : 교신저자)
논문번호 : KICS2009-06-237, 접수일자 : 2009년 6월 3일, 최종논문접수일자 : 2009년 08월 21일

한 보안 기술이 제시되어 있으나, 이를 RFID 기술을 위하여 그대로 적용하는 데는 많은 문제점을 갖고 있다.

기존의 RFID 시스템에서 이러한 문제를 해결하기 위해 본 논문에서는 태그(Tag)와 리더(Reader)간 상호 인증을 위하여 2차원 배열(Array)과 XOR방법을 이용하여 불법적인 접근을 차단하는 RFID 시스템을 제안한다.

Ⅱ. 관련 연구

2.1 RFID 시스템

RFID는 마이크로칩을 내장한 태그(tag), 레이블, 카드 등에 저장된 데이터를 무선 주파수를 이용한 리더에서 자동 인식하는 기술이다. 이러한 RFID 시스템은 태그(Tag), 리더(Reader), 백엔드 서버(Back-end-Server) 3가지 구성 요소로 이루어진다.

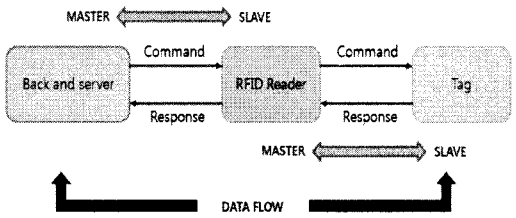


그림 1. RFID 시스템

2.1.1 태그(Tag)

태그(Tag)는 사람과 사물, 동물 등에 부착하여 그 사물에 대한 직접적 혹은 간접적인 식별 및 인식 정보를 송신하는 장치이다. 일반적으로 태그는 한 개의 IC 칩과 한 개의 안테나(antenna)로 구성되어 있다. 태그는 크게 능동형 태그(Active Tag)와 수동형 태그(Passive Tag)로 분류될 수 있다[4].

2.1.2 리더(reader)

RFID 리더는 태그의 정보를 읽어내기 위해 태그와 송수신하는 장치이며, 태그에서 수집된 정보를 미들웨어로 전송하는 기능을 한다. RFID 리더는 RF 아날로그부와 디지털 신호처리 제어부로 구성된다.

리더가 전체 RFID 시스템에서 하는 역할은 태그에게 정보 요청 신호를 보내고 태그로부터 받은 정보를 자체 서브시스템이나 외부 백엔드 서버 시스템을 이용하여 태그를 식별하는 것이다.

2.1.3 백엔드 서버(Back-end-Server)

백엔드 서버는 다수의 리더로부터 전송된 태그 정보에 대한 처리를 해주는 서버 시스템이다. 백엔드 서버에서는 태그와 관련된 정보를 데이터베이스화해서 관리하고 있으며 효율성을 위해서 여러 개의 서버로 분산 운영될 수도 있다. 백엔드 서버는 보안 측면에서 신뢰할 수 있는 시스템으로 간주된다[2].

2.2 RFID 인증 프로토콜

2.2.1 암호 기술과 인증

암호 기술에는 공개키 암호 알고리즘과 대칭키 암호 알고리즘, 해쉬 알고리즘을 이용한 방법이 있다.

비대칭키 암호 알고리즘(Asymmetric Key Algorithm)은 암/복호화하는데 서로 다른 2개의 키가 사용되는 알고리즘이다. 이와는 달리 대칭키 암호 알고리즘(Symmetric Key Algorithm)은 암/복호화 하는데 서로 같은 키가 사용되는 알고리즘이다.

해쉬 알고리즘(Hash Algorithm)은 임의의 비트열인 n 비트 서명문 M을 입력받아 해쉬함수 h를 통해 임의의 고정 비트열인 R 비트 해쉬값 H로 변환하는 알고리즘이다[8].

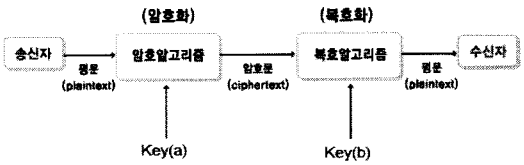


그림 2. 암호화 알고리즘

2.2.2 물리적 인증 프로토콜

기존에 제안된 RFID 시스템의 물리적 인증 기법은 다음과 같이 킬 명령어 기법(Kill command), 패러데이 케이지(Faraday cage) 기법, 액티브 재밍(Active Jamming) 기법, 블로커 태그(Broker-Tag) 기법 등이 있으며 여러 가지 문제점이 있다[5].

1) 킬 명령어(Kill command) 기법

Auto-ID 센터가 제안한 방법으로 킬 명령어를 전송해 사용자에게 태그가 주어지기 전에 태그의 기능을 정지시키는 기법이다. 킬 패스워드(Kill password)는 32bit의 패스워드이며, 모든 패스워드가 0이면 동작하지 않는다. 또한 프로그램으로 입력시에 킬 패스워드의 값은 백엔드 서버가 미리 알고

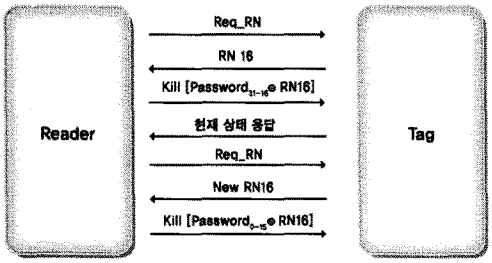


그림 3. Kill 명령어 동작과정

있으며, 태그에서는 RN(Random Number : 난수 재생기)가 포함이 되어 있다. Kill 명령어를 수행시켜 태그의 동작을 정지시키기 위해서는 리더는 태그에게 2번의 Kill 명령어를 성공적으로 수행해야만 동작을 멈출 수가 있다. 이 동작과정은 다음 그림 3과 같다[11].

2) 패러데이 케이지(Faraday cage) 기법

라디오 신호가 투과되지 않도록 하는 금속 혹은 망으로 만들어진 컨테이너(Faraday cage)를 이용하는 방법으로 사용자의 프라이버시를 보호해주는 부분적인 해결책이라 할 수 있다[6].

3) 액티브 재밍(Active Jamming)

근처에 있는 RFID 리더의 기능을 막거나 혹은 방해할 수 있는 라디오 신호를 브로드캐스트 하는 디바이스를 이용하는 것이다. 이 디바이스가 라디오 신호에 대한 전파 방해를 수행함으로써 태그가 노출되는 정보를 보호할 수 있으나, 이러한 접근법은 근처에 있는 모든 RFID 리더가 작동되지 않도록 방해할 수 있기 때문에 매우 강력한 해결책이라 할 수 있다[7].

2.2.3 암호학적 인증 프로토콜

현재 RFID 시스템에서는 암호학적인 방법을 이용한 인증기법을 주로 연구하고 있으며, 현재까지 해쉬락 기법, 확장된 해쉬락 기법, 해쉬체인 기법, 해쉬 기반 ID 변형 기법, 개선된 해쉬 기반 ID 변형 기법, 외부 재암호화 기법, Challenge-Response 기반 안전한 RFID 인증 기법 등이 제안되었다.

1) 해쉬락 기법

2003년 MIT 대학의 S. Weis등에 의하여 제안된 이 기법은 태그가 적합한 값이 들어올 때 까지 ID를 표시하는 것을 거절하는 방법이다. 이는 단지 한

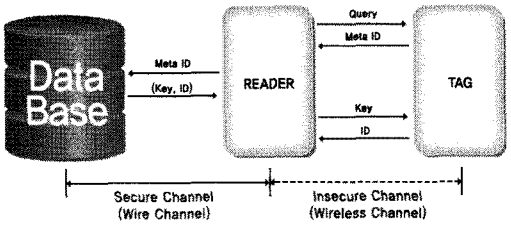


그림 4. 해쉬락 기법

번의 해쉬 함수(Hash Function)만을 사용하기 때문에 저가로 구현될 수 있다[10].

2) 확장된 해쉬락 기법

위에 설명한 해쉬-락 기법의 확장된 기법으로 위치 추적 문제를 해결한 방법이며, 태그는 해쉬 함수와 의사난수 생성기(Random Number Generator)를 갖는다는 것을 가정한다[9].

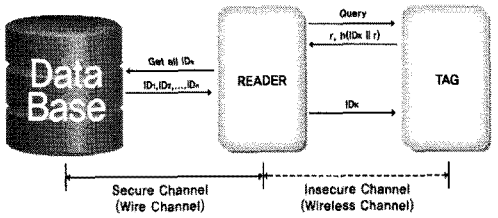


그림 5. 확장된 해쉬락 기법

3) 개선된 해쉬기반 ID 변형 기법

이 기법은 앞의 해쉬기반 ID 변형 기법의 문제점인 스푸핑에 대한 취약점을 보완하고, 태그의 해쉬 횟수를 줄인 방법이다[5].

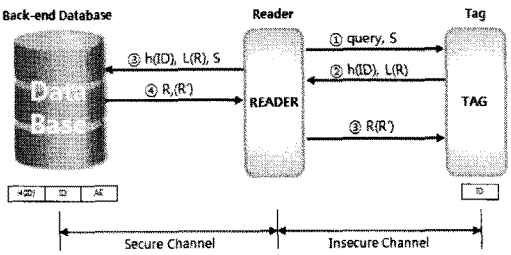


그림 6. 개선된 해쉬기반 ID 변형 기법

Ⅲ. 제안 시스템 구조

3.1 2차원 배열을 이용한 인증 기법

본 논문에서 제안하는 RFID Tag 인증 기법은

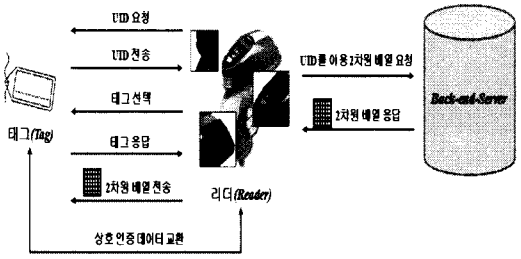


그림 7. 전체 시스템 구조

기존에 제안된 RFID 시스템의 인증에 이용되었던 물리적 인증 기법과 암호학적 인증 프로토콜 방법을 사용해 정보 보호를 하는 방법 대신, 2차원 배열(Array)과 XOR 기법을 이용하여 복잡한 암호화 방법이 없는 인증 기법으로 제안하는 시스템의 전체 구조는 그림 7과 같다.

리더가 태그에게 UID 값을 요청하면 태그는 리더에게 UID 값을 전송한다. 리더는 태그로부터 전송 받은 UID 값을 백엔드 서버(back-end-server)로 전송하고 2차원 배열 생성을 요청한다. 백엔드 서버는 태그의 UID 값에 해당하는 문자셋(Character set)을 이용하여 2차원 배열을 생성하여 리더에게 전송한다. 리더는 서버로부터 전송받은 2차원 배열을 태그에게 전송하고, 태그는 리더로부터 전송받은 2차원 배열을 복호화 하고 자신이 보낸 태그 아이디(TagID)값과 동일한지 검사한다. 만일 동일할 경우 태그는 2차원 배열을 생성하여 리더로 전송하고 리더는 백엔드 서버로 전송한다. 이렇게 전송된 2차원 배열은 서버에서 복호화 하여 태그 아이디 값과 동일한지 비교하고 동일한 경우 상호 인증이 이루어진다.

3.2 2차원 배열 기법 설계

RFID 시스템에서 태그에 대한 문자셋은 태그와 서버 모두가 가지고 있다. 여기서 문자셋 셋이란 아스키코드와 같이 일련의 문자를 비트로 환산하기 위해 미리 정의해 놓은 코드표이며, 알파벳 A~Z 26글자, a~z 26글자, 숫자 0~9 10글자, UnderLine과 (.)닷 2글자 모두 합쳐 64개의 글자가 서로 다른 조합으로 1개씩 나열되어 있는 순서이다. 각각의 리더, RFID Tag마다 서로 다른 문자셋이 정의되어 있으며, 이 값은 나중에 중간 공격자로부터 공격이 들어오더라도 문자셋 값을 알지 못하기 때문에 안전히 통신을 할 수 있게 하는 값이다.

예를 들어 1번 Tag는 "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz01234 56789_."으로 구성되어 있으며, 2번 Tag는 "._9876 543210zyxwvutsrqponmlkjihgfedcbaZYXWVUTSR QPONMLKJIHGFEDCBA"으로 구성될 수 있다. 즉 1번 Tag는 A 글자는 1번째 글자이며 2진수로 000000으로 표현할 수 있으며, B 글자 → 000001, C 글자 → 000010, UnderLine(_) → 111110, 닷(.) → 111111로 나타낼 수 있다.

단 문자셋의 순서만 다르게 해주면 전체 사용가능한 가지의 수는 64!이며 1.26886932185884164 10343338933516e+89 가지 수가 된다. 태그에 적용할 수 있는 가지의 수는 거의 무한대에 가까운 수가 나온다.

3.2.1 2차원 배열 생성

백엔드 서버에서는 그림 8과 같이 2차원 배열을 생성하며 다음은 가로 세로가 각각 6바이트(byte)씩 생성된 2차원 배열을 가지고 설명한다.

2차원 배열의 모든 셀들은 마지막 행을 제외한 총 64 가지의 문자셋을 이용하여 랜덤하게 패딩(padding) 된다. 다음 마지막 행에 입력되는 값은 나중에 원래 암호화가 될 키를 연산하기 위해 남겨둔다.

그림 9는 난수값을 이용하여 마지막 행을 제외한 나머지를 64가지의 문자를 이용하여 패딩한 결과이다.

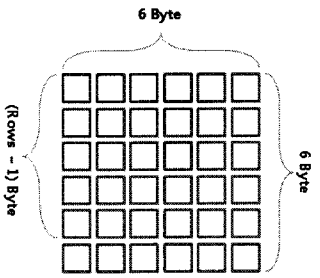


그림 8. 2차원 배열

A	E	d	B	r	8
8	C	8	6	B	6
h	4	6	E	h	r
L	r	B	C	4	E
6	d	r	L	C	E
A_0	A_1	A_2	A_3	A_4	A_5

그림 9. 난수값으로 패딩된 2차원 배열

3.2.2 2차원 배열의 마지막 행 생성 방법

마지막 행에 패딩되는 값은 각 열을 XOR한 값과 각각의 마지막 행에 해당하는 A0값을 XOR한 값이 태그 아이디(tagID) 값이 된다. 태그 아이디(tagID)값을 "dCrr4h" 이라 가정하고 마지막 행의 자세한 생성 방법은 그림 10과 같다.

연산으로 A_0 이전의 값과 A_0값을 XOR하면 그림 10과 같이 d(keyID)값이 나오고, A_0의 값을 구한다. 태그 아이 값을 얻는 방법은 식 1과 같다.

$$A \oplus 8 \oplus h \oplus L \oplus 6 \oplus A_0 = d(keyID) \qquad (1)$$

각 열의 값을 XOR 하여 태그 아이디 값을 구하기 위해서는 문자셋을 필요로 하며, 문자셋은 그림 11과 같다. 태그와 백엔드 서버에서는 동일한 문자셋을 가지고 있다. 이는 전체 문자셋이 64가지 글자이며, 각 글자당 6Bit씩 할당하여 전체 문자셋을 표현할 수 있다.

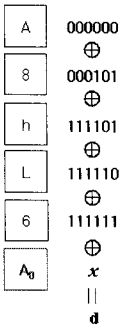


그림 10. 마지막 행값 생성 방법

000000	A
000001	B
000010	C
000011	d
000100	E
000101	8
000110	r
000111	4
...	...
111000	x
111001	Z
111010	s
111101	h
111110	L
111111	6

그림 11. 문자셋(Character set)

이 문자셋은 각 태그마다 다른 순서를 가지고 있으며, 서버는 모든 태그마다의 문자셋을 가지고 있으며, 각각의 태그들은 자신만의 문자셋만을 알고 있다. 즉 위의 예제에서는 "A" 의 값이 "000000" 이지만 다른 태그는 문자셋이 서로 틀린 조합을 가지고 있으므로 "000000" 값은 64가지 중 다르게 표현 될 수도 있다.

3.2.3 완성된 2차원 배열

A0~A6 까지의 값을 구하여 패딩한 후 완성된 2차원 배열은 다음 그림 12와 같다.

완성된 2차원 배열은 태그와 서버가 요청시 마다 새롭게 생성되어 전송된다. 전체 시스템은 그림 13과 같다.

다음은 태그와 백엔드 서버 각각이 가지고 있는 모듈에 대한 설명이다.

A	E	d	B	r	8
8	C	8	6	B	6
h	4	6	E	h	r
L	r	B	C	4	E
6	d	r	L	C	E
s	r	x	A	x	B

그림 12. 완성된 2차원 배열

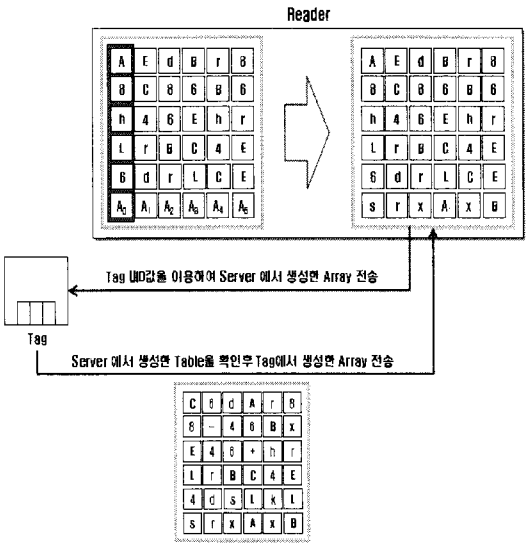


그림 13. 전체 시스템 흐름도

1) 태그 연산 모듈

리더가 태그 아이디 값 요청시 2차원 배열을 이용하여 암호화하는 역할과 서버로부터 전송받은 2차원 배열을 복호화 하는 기능을 한다.

2) 태그 인증 모듈

연산 모듈을 통해 복호화된 2차원 배열의 값이 태그 아이디 값과 동일한지를 비교하여 인증을 하며, 인증된 리더인지 아닌지 판별하는 기능을 한다.

3) 서버측 연산 모듈

태그로부터 전송받은 UID 값을 이용하여 2차원 배열을 생성하고 태그로 보내고, 태그로부터 전송받은 2차원 배열을 복호화 하는 기능을 한다.

4) 서버측 인증 모듈

태그 인증 모듈과 같이 연산 모듈을 통해 복호화된 2차원 배열의 값이 태그 아이디 값과 동일한지를 비교하여 인증을 하며, 인증된 태그와 통신을 허가 한다.

Ⅳ. 안전성에 대한 평가

4.1 스푸핑 공격에 대한 안전성

기존 시스템 해쉬-락 기법과 해쉬 기반 ID 변형 기법은 스푸핑 공격에 취약하지만 제안하는 시스템은 스푸핑 공격에 안전하다.

제안하는 시스템에서는 공격자가 정당한 리더로 위장해도 태그의 UID값에 해당하는 문자셋과 태그 아이디를 모르고 있으므로 2차원 배열을 태그에서 복호화 한다 하더라도 인증 거부를 한다. 또한 위장된 태그에는 올바른 UID값을 알 수 있지만, UID값에 해당하는 문자셋을 알 수 없으므로 획득한 2차원 배열로는 스푸핑 공격이 불가능하다.

4.2 재전송 공격에 대한 안전성

기존 시스템 해쉬락 기법은 재전송 공격에 취약하지만, 해쉬 기반 ID 변형 기법은 재전송 공격에 안전하다.

제안하는 시스템에서는 정당한 리더가 쿼리와 함께 전송하는 2차원 배열에 대하여 태그가 리더에 응답으로 2차원 배열을 요청시마다 재생성하여 전송한다. 정당한 리더는 문자셋을 이용하여 2차원 배열을 복화화 하지만 자신이 보낸 태그 아이디와 다른 값이 나오므로 정당한 리더는 태그에 대한 인증을 거부한다.

4.3 제안하는 RFID 인증 프로토콜

제안하는 RFID 인증 프로토콜 기법은 공격에 대한 안전성은 태그가 리더로부터 수신한 2차원 배열을 이용하여 요청마다 다른 2차원 배열로 응답을 하기 때문에 스푸핑 공격, 재전송 공격, 트래픽 분석 공격과 위치 트래킹 공격에 안전하게 나타났다. 표 1은 공격에 대한 안전성을 비교분석한 결과이다.

제안하는 RFID 시스템에서 상호인증을 위해서는 UID, 태그 아이디, 문자셋을 가지고 있어야만 암/복호화 가능하다.

표 1. 공격에 대한 안전성 비교

프로토콜 / 공격형태	해쉬-락 기법	해쉬 기반 ID 변형 기법	개선된 해쉬 기반 ID 변형 기법	제안하는 RFID 인증 프로토콜
스푸핑 공격	취약	취약	취약	안전
재전송 공격	취약	안전	안전	안전
트래픽 분석 공격	취약	안전	안전	안전
위치 트래킹 공격	취약	취약	보통	안전

Ⅴ. 결 론

본 논문에서는 제안하는 RFID 시스템에서 제안하는 RFID 인증 프로토콜은 백엔드 서버에 등록된 태그의 UID, 태그 아이디(TagID), 문자셋(Character set)의 정보를 가지고 있다. 이러한 정보를 이용하여 상호 인증을 수행함으로써 인증되지 않은 태그 또는 리더에게 개인정보가 유출되지 않도록 보안성을 강화 하였다.

제안하는 RFID 인증 프로토콜은 리더와 태그가 2차원 배열을 요청할 때마다 새롭게 생성하여 전송하기 때문에 기존 시스템보다 공격에 강한 특징을 가지고 있으며, 2차원 배열은 별다른 암호화를 사용하지 않기 때문에 문자셋만 가지고 있다면 복호화 과정까지 전부 자동으로 진행되기 때문에 속도가 빠르다는 장점을 가진다. 또한 문자셋을 가지고 있

지 않다면 2차원 배열을 복호화할 수 없으며 문자셋을 이루고 있는 값들은 랜덤하게 바뀌므로 태그 아이디를 유추할 수 없다.

참 고 문 헌

[1] 정용훈, "멀티미디어 콘텐츠 보호를 위한 인증 프로토콜에 관한 연구", 숭실대학교 석사학위논문, 2006.

[2] 이근우, 오동규, 곽 진, 오수현, 김승주, 원동호, "분산 데이터베이스 환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜", 한국정보처리학회 논문지 C, 제12권-C권, 제3호, pp.309-316, 2006. 6

[3] 강전일, 박주성, 양대헌, "RFID 시스템에서의 프라이버시 보호기술", 한국정보처리학회지, 제12권, 제6호, pp.28-36, 2004. 12.

[4] Auto-ID Center, "860MHz-960MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical communication Interface Specification Proposed Recommendation Version 1.0.0", Technical Report MIT-AUTOID-TR-007, NOV, 2002

[5] Henrich, D. and Műller, P., "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshop (PERCOMW'04), pp. 149-153, IEEE, 2004.

[6] M. Ohkubo, K. Suzuki, and S. Kinosita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID", Proceedings of the SCIS 2004, pp.719-724, 2004.

[7] Weis, S. et al., "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security Pervasive Computing, 2003 LNCS 2802, pp.201-212, Springer-Verlag Heidelberg. 2004.

[8] Ronald L. Rivest The MD5 Message-Digest Algorithm IETF RFC 1321 April 1992.

[9] S. A. Weis, S. e. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security in Pervasive Computing 2003, LNCS 2802, pp. 201-212, Springer-Verlag Heidelberg, 2004.

[10] S. A. Weis, "Security an Privacy in Radio-Frequency Identification Devices " MS Thesis. MIT. May, 2003.

[11] Understanding the EPC Gen 2 Protocol, RFID Journal Special Report, 2005.

정 용 훈 (Yong-hoon Jung) 정회원

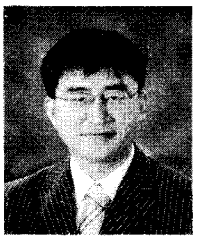
2004년 2월 숭실대학교 전자계산원 공학사

2004년 9월 숭실대학교 대학원 컴퓨터학과 공학석사

2006년 9월~현재 숭실대학교 컴퓨터학과 박사과정

<관심분야> RFID, DRM, Network security, 인증시스템

김 정 재 (Jung-jae Kim) 정회원



1999년 2월 영동대학교 컴퓨터공학과 공학사

2001년 2월 숭실대학교 대학원 컴퓨터학과 공학석사

2005년 8월 숭실대학교 대학원 컴퓨터학과 공학박사

2006년 7월~현재 리테일테크 수석연구원

<관심분야> RFID, DRM, Network security, 멀티미디어보안

전 문 석 (Moon-seog Jun) 정회원

1989년 2월 University of Maryland Computer Science 공학박사

1989년~1991년 New Mexico State University Physical Science Lab 책임 연구원

1991년~현재 숭실대학교 정교수

<관심분야> 전자상거래 보안, 인터넷 보안, 멀티미디어 보안, 인증 시스템