# 수동형 RFID 태그 위조 방지를 위한 알고리즘

손 종 수 , 공 신 조 , 정 인 정
고려대학교 전산학과
{mis026, ggonga01, chung}@korea.ac.kr

# Algorithm for the passive RFID Tag Forgery Problem

Sohn Jong-Soo, Kong Sin Jo, In-Jeong Chung
Dept. of Computer Science, Korea University

요 약

본 논문은 RFID 시스템 상의 RFID Tag의 보안 취약점을 보완하는 방법을 제시한 논문으로서 임의로 취득한 RFID 태그의 데이터를 불법적으로 위조하는 것을 회피하는 알고리즘을 제시한다. 현재까지 제안된 RFID Tag의 보안 문제 해결방법들은 일정정도의 계산능력을 가진 칩을 내장해야만 구현기 가능하기 때문에 작은 메모리 용량을 갖는 수동형 RFID Tag를 사용하는 현업에서는 해당 알고리즘을 적용하는 것이 불가능했다. 본 논문에서 제시하는 방법은 기존 RFID Tag 보안문제 해결방법에서 제시한 해싱 함수를 사용하지만 해싱함수를 Tag에 내장하지 않고 해싱 키를 내장함으로서 현실적용이 가능하도록 하였다. 본 논문에서 제시한 방법을 통해 RFID Tag의 내용을 임의로 바꾸는 것을 회피할 수 있다.

## 1. 서론

유비쿼터스 컴퓨팅이란 '언제 어디서나 있다'[1]라는 라틴어에서 유래한 용어로서 컴퓨터를 이용한 서비스와 통신이 유선상의 네트워크 뿐 아니라 인간이 접할 수 있는 모든 곳에서 컴퓨팅이 가능한 환경을 일컫는 말이다. RFID(Radio Frequency IDentification) 시스템이란 흔히 보다 많은 데이터를 보관할 수 있는 무선인식 비접촉 바코드 시스템으로 알고 있지만 무선으로 대량의 태그를 자동으로 인식할 수 있다는 것과 더 많은 정보를 저장할 수 있다는 장점 때문에 유비쿼터스 컴퓨팅의 핵심 요소로 자리 잡고 있다. RFID 시스템은 라디오 주파수를 이용하여 고유한 ID를 가진 태그를 읽어 객체를 식별하는 것이다[3]. RFID 시스템은 크게 세가지 요소로 구성이 되는데 RFID 태그(Tag)의 ID를 읽어내는 RFID 리더(Reader)와 RFID 리더에 데이터를 전송하는 RFID 태그, 그리고 읽어들인 ID를 데이터와 매칭시키는 데이터베이스로 구성이 된다. 한편, RFID 태그는 능동형(Active) 태그와 수동형(Passive) 태그로 구분이 되는데 능동형 태그는 인식거리가 길고 큰 저장 공간을 갖지만 비용이 비싸며 수동형 태그는 인식거리가 상대적으로 짧고 저장 공간도 상대적으로 작지만 비용이 싸기 때문에 현업에서 광범위하게 사용되고 있다[3][11].

RFID 시스템을 도입했거나 도입하고 있는 기업의 경우 대부분 수동형 태그를 사용하고 있기 때문에 본 논문에서 제안하는 태그 위조 회피 방법은 수동형 RFID 태그를 사용하는 것으로 가정한다. RFID 태그와 리더간의 통신은 무선 주파수를 이용하기 때문에 같은 주파수 대역의 리더가 있다면 얼마든지 태그의 고유한 값이 외부에 노출될 수 있다. 이 때, RFID 태그의 보안 문제를 해결하기 위해 많은 연구가 진행되고 있으나 기존 연구들은 태그와 리더간의 통신 프로토콜을 제안하는 것으로 이 문제를 해결한다[10]. 통신 프로토콜을 사용하기 위해선 수동형 RFID 태그에 일정정도 이상의 계산 능력이 있어야 함을 의미하므로 현업에서 사용하기에는 무리가 있다. 따라서 본 논문에서는 특별히 태그가 계산을 하지 않고도 고유한

ID값을 노출시키지 않는 방법을 제안한다. 제안하는 방법은 RFID 태그에 ID를 삽입하지 않고 해당 ID를 해싱함수에 넣어 해싱 키를 만들어낸 후 그 해싱키를 RFID 태그에 삽입한다. 그리고 그와 동시에 만든 해싱키와 원래의 ID를 매칭시키는 해싱테이블을 데이터베이스에 생성하여 후에 리더가 RFID 태그를 읽었을 때 해싱테이블을 참조하여 본래의 ID를 찾는다. 이 방법을 사용하면 RFID 태그에 본래의 ID가 들어가지 않으므로 임의의 불법 침입자가 태그를 위조하여 비슷한 종류의 태그를 만들어내는 것을 회피할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문과 비슷한 취지의 관련 연구에 대해 기술한다. 3장에서는 본 논문에서 제안하는 방법에 대해 개념적으로 기술하며 4장에서는 제안하는 방법을 시뮬레이션을 통해 검증한다. 마지막으로 5장에서는 본 논문의 결론을 기술하며 향후 연구과제에 대하여 토의한다.

# 2. 관련 연구

기존 인식 시스템인 바코드를 대신할 RFID 시스템은 RFID 태그를 리더에 접촉하지 않고도[3] 여러 개의 태그 정보를 동시에 읽어 들일 수 있고 바코드보다도 대량의 정보를 입력할 수 있는 장점을 가지고 있다. 하지만 태그 내 정보를 라디오 전파를 이용하여 송수신하는 방식이여서 도청이 가능하고 태그 종류에 따라 여러 번 읽고 쓰기가 가능하기 때문에 정보의 유출 및 위변조등 보안상의 문제점을 수반하고 있다.[6]

본 장에서는 위의 문제점을 해결하고자 선행되었던 연구들을 살펴보고 비교 분석해 보기로 한다.

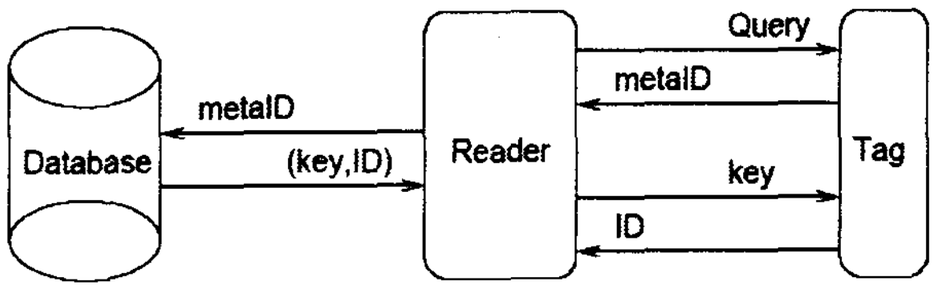
## 2.1 관련 연구

RFID 시스템 보안은 태그 정보 유출을 방지하여 자료의 비밀성, 무결성, 익명성을 보장 받기 위해 설계된다. 이를 위해서 많은 연구들이 진행 되어오고 있다[6].

### 2.1.1 Hash-Lock 기법

Hash-Lock 기법[5]은 단방향 함수인 해시 함수를 이용하여 태그 정보를 보안하는 기법으로 리더가 Meta ID로 키를 계산하여 각 태그에 대한 키 값을 갖게 되며 Meta ID는 각 태그에 저장한다. 리더에 의해서 태그의 Meta ID가 읽혀지게 되면 Meta ID와 관련된 키를 태그로 전송하며 태그 내에서 받은 키를 이용해 해시 값을 계산하고 Meta ID와 일치하는 경우에 한해서 실제 ID를 리더로 전송하게 된다.

하지만 Meta ID값이 고정되어 있기 때문에 의도적으로 특정 Meta ID만을 추적하여 정보의 위치를 알아챌 수 있는 단점이 있다.

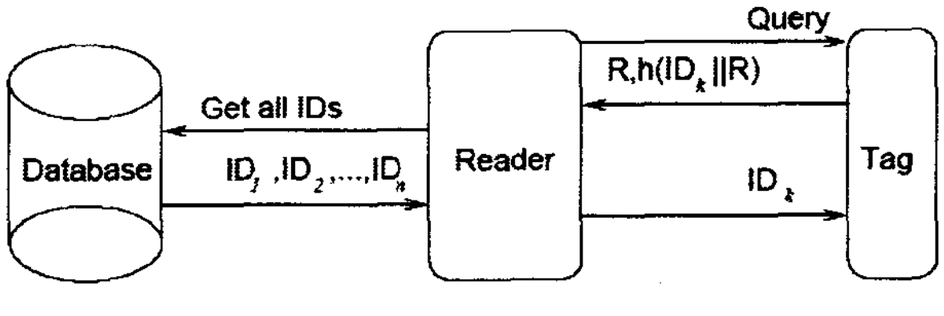



[그림 1] Hash-Lock 기법의 Unlocking 프로토콜

### 2.1.2 Randomized Hash-Lock 기법

기존 Hash-Lock 기법[7]에 난수 발생기에서 생성된 임의의 수 R을 이용하여 리더가 질의를 보낼 때마다 태그의 ID를 변경하는 기법이다. 태그는 해시함수에 의해 생성된 임의의 수 R과 ID를 통해 키를 만든다. R과 키를 데이터베이스에 저장하고, 저장된 모든 태그 ID와 각 태그의 임의의 수 R로 만든 키를 리더로 전송한다.

따라서 기존의 Hash-Lock 기법의 문제점인 Meta ID를 추적하여 정보를 빼내는 문제는 해결할 수 있으나, 해시 함수와 난수 발생기를 동시에 태그에 구현해야 하므로 구현이 어렵고, 특정 태그의 정보를 검색할 때 모든 태그 정보와 R에 대한 키를 검사하는 부담이 있다.



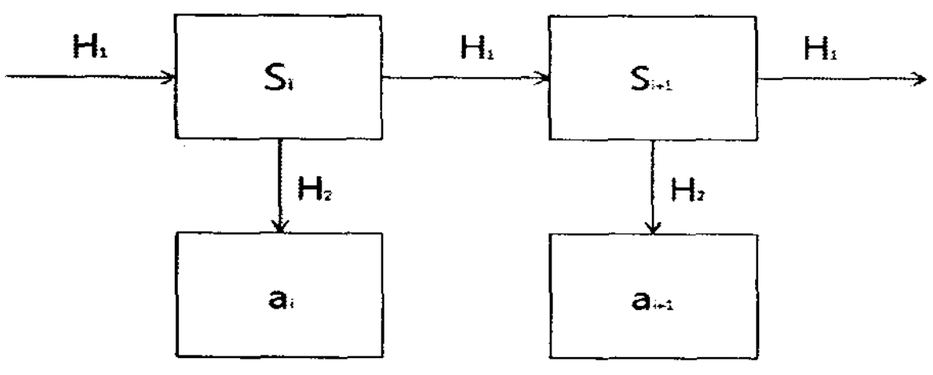

[그림 2] Randomized Hash-Lock 기법의 Unlocking 프로토콜

### 2.1.3 Hash Chain 기법

해시 체인 기법[2]은 서로 다른 두 개의 hash 함수 $H_1$과 $H_2$를 이용한다. 초기 키인 $S_1$을 $H_1$을 이용해

생성하고 매회 통신에서 $H_1$을 통해 비밀값을 $S_{n+1}$으로 갱신한다. 함수 $H_2$는 매회 통신마다 갱신된 키를 다시 한번 해싱하여 태그의 ID와 함께 데이터베이스에 저장해 태그 정보를 보호한다. 이를 통해 리더는 같은 태그에 대해서 매회 요청마다 다른 응답을 받게 되어 태그의 정보를 추적하는 문제를 해결했다.

하지만 서로 다른 두 개의 해시 함수를 구현해야 하는 문제와 데이터베이스 내의 태그 정보를 검색할 때 드는 계산량이 많아진다.




[그림 3] Hash Chain 기법

#### 2.1.4 재 암호화 기법

재 암호화 기법[8][9]은 공개키를 이용하여 암호화된 정보를 태그에 넣고 일정 주기를 두어 기존에 저장된 태그 정보를 암호화하여 변경시켜주는 기법이다. 태그 내에서 공개키를 이용한 암호화 연산이 어려우므로 별도의 공개키를 태그의 외부에 두고 연산을 처리한다.

#### 2.1.5 Kill 명령어 기법

Kill 명령어 기법[4]은 각 태그에 일정 비트의 고유 kill code를 저장하여 kill code를 태그에 전송하게 되면 태그를 영구적으로 비 활성화시켜 정보의 유출을 원천적으로 차단하는 방법이다. 하지만 Kill 명령으로 비 활성화된 태그는 재사용이 불가능하다는 단점이 있다[2].

## 3. RFID 태그의 위조 회피 방법

### 3.1 RFID 태그의 위조 회피 방법

기존의 RFID 태그 보안 문제 해결을 위한 연구들은 RFID 시스템의 현실적인 문제들을 고려하지 않고 보안 프로토콜 등을 제안하고 있다. 보편적으로 많이 쓰이는 RFID 태그는 어떤 계산능력도 갖지 못하는 것이 현실이므로 이를 고려한 방안이 필요하다.

일반적인 시스템에서는 RFID 태그에 아무런 조작 없이 ID를 입력한다. 이 때 RFID 태그에 쓰여지는 데이터는 [001, 002, 003, 004] 와 같이 순차적으로 각 태그마다 쓰여지기 때문에 침입자들은 [005, 006, 007, 008] 등과 같이 태그 ID 부여 정책을 쉽게 파악할 수 있다. 기존에 제안된 RFID 태그 보안 방법들은 모두 RFID 태그에 일정정도 이상의 계산 능력이 있다는 가정 하에 알고리즘을 작성하고 8bit 이상의 칩을 삽입한 태그를 사용하여 실험한 예제들이었다. 따라서 광범위하게 사용되고 있는 일반적인 저가·수동형 RFID 태그를 사용하는 경우에는 어떤 대안도 제시하지 못하고 있다. 가장 많이 제안된 RFID 태그 보안 방법은 해시 함수를 RFID 태그에 내장하는 방법인데 이 방법 역시 RFID 태그가 계산능력이 있다는 가정하게 고안된 것이므로 현실적으로 현업에 적용하는데 무리가 있다. 따라서 우리는 해시 함수를 적용하는 방법을 변칙적으로 적용하여 RFID 태그에 해싱 테이블 주소를 넣고 리더에 해시 함수를 내장하여 현실적인 면을 고려한 RFID 태그 보안 방법을 고안하였다.

본 논문에서 제시하는 방법은 RFID 태그에 해싱함수로 만든 주소 값을 삽입하고 리더가 해당 태그의 주소를 읽어오면 데이터베이스가 해당 태그의 ID를 리더로 전송하여 태그를 인식하는 방법으로서 도청자나 고의적 태그 위변조자가 쉽게 태그의 내용을 파악하지 못하게 한다. RFID 태그에 비 연속적이고 무작위의 데이터가 삽입되면 데이터베이스를 직접 참조하지 않고선 해당 태그의 내용이 무엇인지 파악하기가 사실상 불가능해진다.

우리가 제안하는 RFID 태그의 위조 회피 방법은 다음과 같은 순서로 작동된다.

**태그에 ID를 입력하는 경우**

① 사용자가 RFID 태그에 ID입력 명령

② RFID 리더는 해당 태그의 ID를 해싱 함수에 넣고 주소를 계산

③ 계산된 주소와 ID는 데이터베이스에 저장

④ 태그에 해싱 테이블의 주소 입력

**태그를 읽는 경우**

① 사용자가 리더를 이용해 태그 읽기 명령

② 리더는 태그에서 해싱 테이블 주소를 가져옴

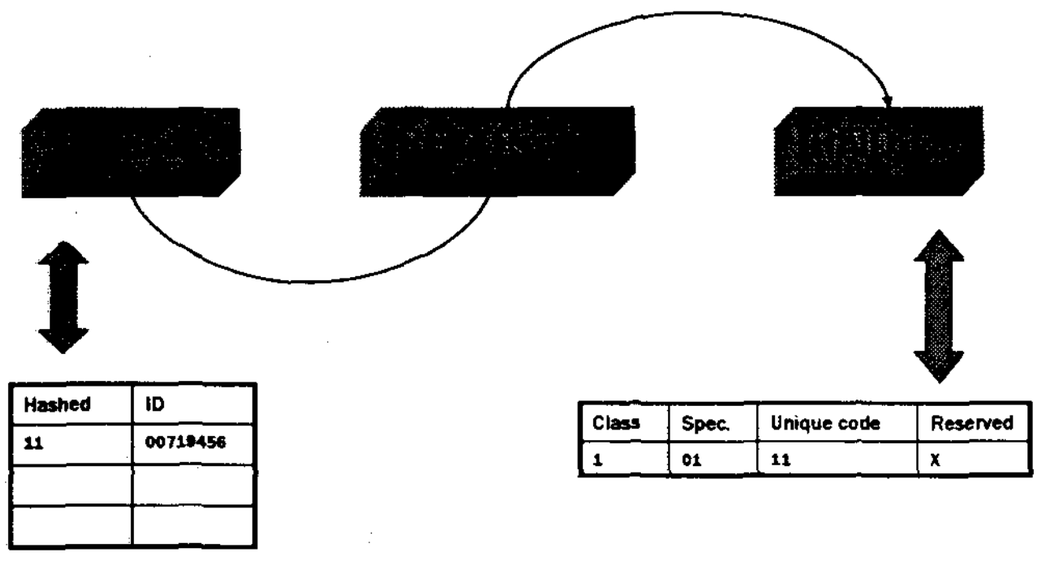
③ 리더는 가져온 해싱 테이블 주소를 참조해서 데이터베이스에서 해당 태그의 ID를 읽음

④ 사용자에게 읽은 태그의 ID를 출력

### 3.2 시스템 구조

본 논문에서 제시하는 방법은 RFID 리더가 전파를 보내면 가진 데이터를 리더에 전송하는 역할을 하는 RFID 태그의 현실적인 면을 고려하였다.

제안하는 방법은 [그림4]와 같은 구조를 가지고 있다. 여기서 데이터베이스는 해싱테이블의 역할을 담당하며 RFID 리더는 해싱 함수의 역할을, RFID 태그에 입력될 해싱된 ID는 주소(Address)의 역할을 담당한다.




[그림 4] RFID 제안하는 시스템의 구조

### 3.3 각 구성 요소의 역할

**RFID 리더**

RFID 리더는 RFID 태그에 ID를 읽고 쓰는 역할을 한다. 이 때 RFID 리더는 해싱 함수를 내장하고 있으며 RFID 태그에 ID를 입력할 때 해당 ID를 해싱 함수에 넣어 주소를 생성하며 생성된 주소를 RFID 태그에 입력한다. 그리고 그와 동시에 데이터베이스의 해싱 키와 ID를 매칭시키는 해싱 테이블에 주소와 주소에 해당하는 ID를 입력한다.

**RFID 태그**

위 RFID 리더에서 생성된 주소는 RFID 태그에 입력된다. 후에 RFID 리더에서 읽기를 시도하면 RFID 태그는 해싱된 ID의 주소를 반환한다.

**데이터베이스**

RFID 리더가 주소를 생성할 때 해싱 테이블에 레코드를 저장한다. RFID 리더가 태그를 읽어 주소를 데이터베이스에 전송하면 데이터베이스는 전송받은 주소에 해당하는 ID를 RFID 리더에 전송한다.

### 3.4 예제

RFID 태그는 EPC Global의 96bit Class 1 Gen 2를 사용하였다. 태그의 비트를 실험에 맞게 Classification code, Specification code, Unique code, Unique code 이렇게 4개의 뱅크로 구성하였다. Classification code는 주로 해당 태그의 대분류를 표시하며 Specification code는 중분류, Unique code는 해당 태그의 ID를 표시한다. 여기서 우리는 가장 많은 데이터를 수용할 수 있는 Uniqe code의 ID만을 고려하도록 한다.

RFID 태그에 입력하기를 원하는 ID가 “00719456”이라고 가정하면 RFID 리더는 “00719456”을 해싱 함수에 넣어 주소를 생성한다. 여기서 사용하는 해싱 함수는 간단히 예제를 보이기 위해 보편적으로 사용되는 경계폴링 방법을 사용한다. 경계폴링 방법을 사용하여 “00719456”을 해싱하면 “11”이라는 주소가 생성된다. RFID 리더는 여기서 생성된 주소 “11”을 RFID 태그에 입력한다. 그리고 동시에 주소 ”11“과 주소 ”11“에 해당하는 ID(00719456)를 데이터베이스의 해싱 테이블에 삽입한다.

RFID 태그에 RFID 리더가 전파를 보내 태그의 데이터를 읽어오면 태그는 “11”을 반환한다. 이 때, RFID 리더는 “11”이라는 주소를 데이터베이스로 전송하여 해싱테이블 안의 주소 “11”이 가르키는 레코드를 찾아 그 결과값을 다시 RFID 리더로 전송한다.

## 4. 구현 및 실험

### 4.1 실험 개요

본 논문에서 제시하고 있는 RFID 태그의 위변조 회피에 대한 실험은 RFID 리더와 수동형 RFID 태그, 데이터베이스를 이용하여 실시되었다. 사용한 RFID 리더와 태그는 900MHz 대역의 주파수를 사용하며 태그에 대한 읽기와 쓰기가 모두 가능하다. 사용한 해시 함수는 MD5이다. MD5 알고리즘은 입력 데이터 (길이에 상관없는 하나의 메시지)로부터 128 비트 메시지 축약을 만듦으로써 데이터 무결성을 검증하는데 사용되는 알고리즘으로써 해싱 테이블 주소의 충돌이 적고 충분한 주소를 생성할 수 있으므로 사용하였다.

실험을 하기에 앞서 본 실험의 취지에 맞게끔 다음과 같은 가정을 설정했다.

### a. 태그의 물리적 복사

본 실험에서는 태그의 계산능력이 전무 하다는 현실적인 문제를 파악하고 개선하고자 하는데 있다. 따라서 태그의 정보는 물리적 복사가 불가능하다는 가정을 세워 실험의 취지를 높이도록 했다.

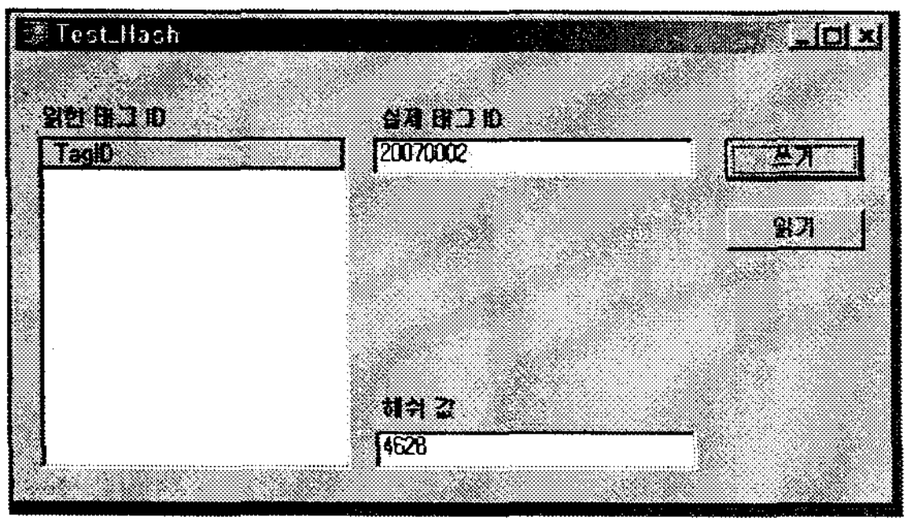
### b. 공격의 범위

본 실험에서 사용하는 리더는 신뢰성이 증명되었으며, 공격의 범위는 태그의 실제 코드에 대한 순차적 정보를 알아내어 위조함으로써 정보를 도용하고자 하는데 있다.

### c. 태그 ID의 연속성

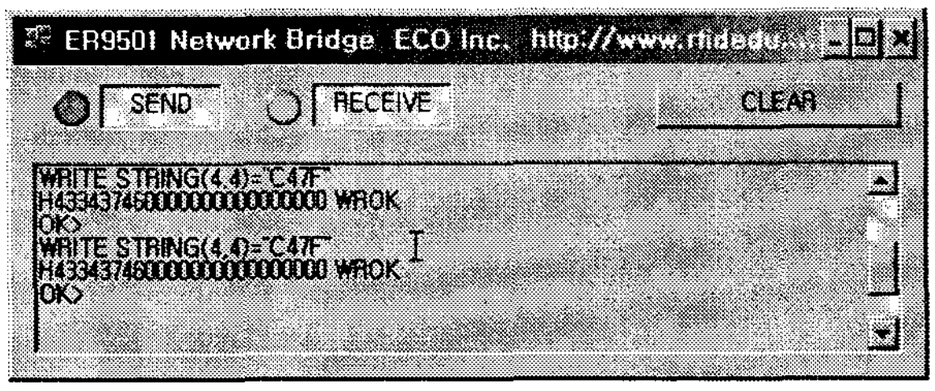
일반적으로 RFID 태그에 입력되는 데이터는 연속성을 갖는다. 이에 본 실험에 사용한 태그의 실제 ID는 연속적인 8자리의 숫자(2007000x)를 사용했다.

## 4.2 실험 진행




[그림 2] RFID 제어 응용프로그램

RFID 태그에는 계산 능력이 없으므로 해시 함수를 RFID 태그의 외부에 두어야 한다. 본 실험에서는 리더와 통신하는 태그 제어 응용프로그램을 작성하였고 이 응용프로그램은 실제 ID를 이용한 해시 값을 생성한다. 응용프로그램은 [그림 2]와 같다. 본 응용프로그램은 리더를 통해 태그에 데이터를 읽고 쓰기가 모두 가능하다. '실제 태그 ID 부분'에 실제 ID 값을 입력하고 '쓰기' 버튼을 누르면 '해시 값'에 실제 ID이용하여 생성된 해싱 테이블 주소값이 작성되고 리더를 통해 태그에 기록한다. 기록되는 내용은 다음과 같다.




[그림 3] RFID 브릿지 소프트웨어

리더에 설치된 RFID 브릿지 소프트웨어를 이용하여 태그에 정상적으로 정보가 기록되었는지를 알아보았다. [그림 3]은 실험을 통해 태그에 정보가 기록되는 것을 보이고 있다.

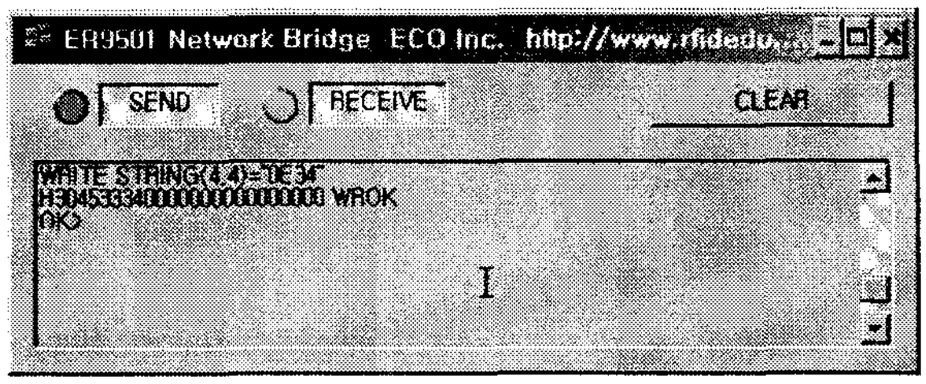
## 4.3 실험 결과

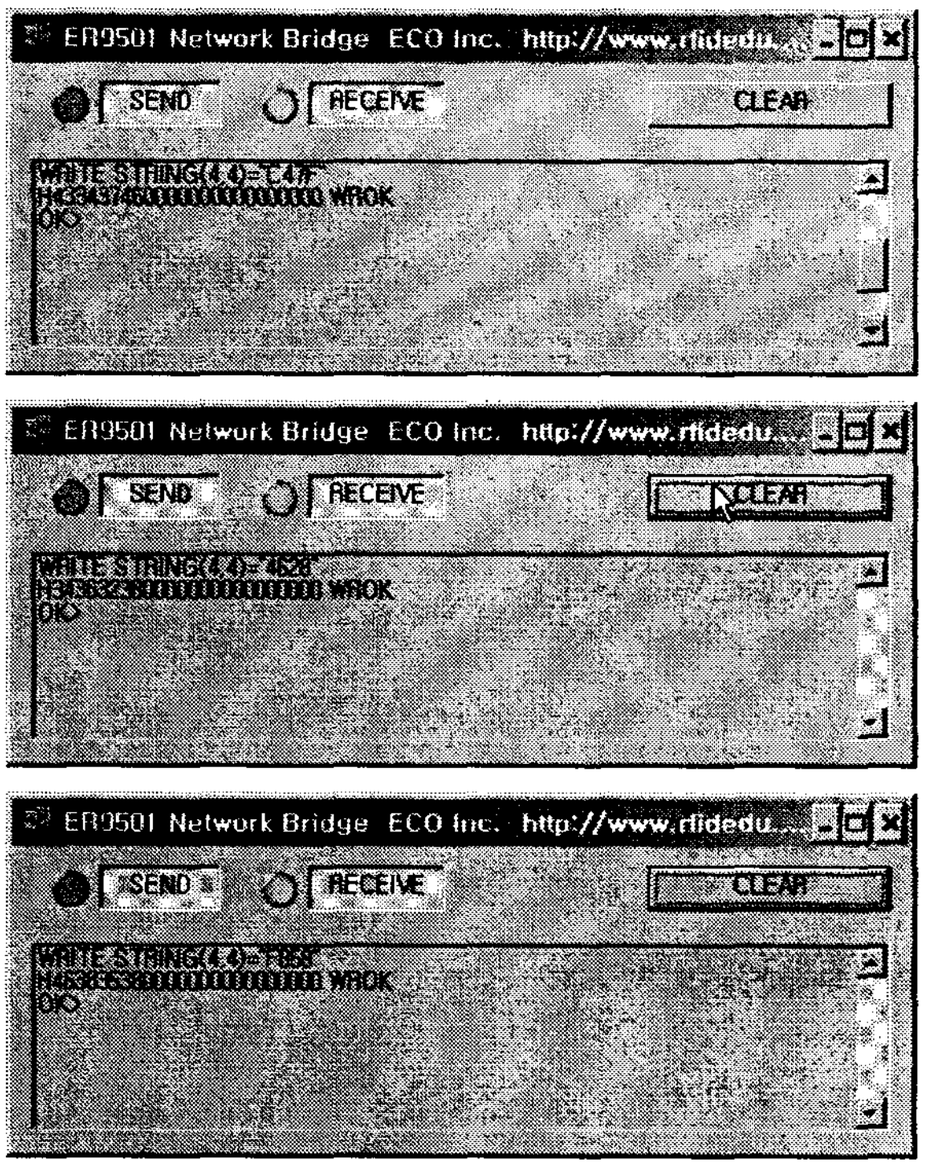
상기의 설정을 바탕으로 200개의 태그를 대상으로 실험한 결과 실제 태그 ID에 대한 해싱 테이블 주소 값은 모두 비연속성을 띄며 태그에 정상적으로 기록이 되었다. 또한 기록된 태그를 읽어 데이터베이스에 저장된 해시 값과 비교한 결과 등록되지 않거나 비정상적인 태그 ID를 식별해 내어 태그의 위조 회피를 구현할 수 있었다.

특히, 태그 내부에 해싱 함수를 내장시키지 않고, RFID 리더 측에서 생성된 값을 이용함으로써 수동형 태그의 보안 문제를 해결하였다.

| 실제 태그 ID | 해싱 테이블 주소(Hex) |
|---|---|
| 20070001 | 30453334 |
| 20070002 | 34363238 |
| 20070003 | 43343746 |
| 20070004 | 46383538 |

[표 1] 실제 태그 ID 및 생성된 주소값






[그림 4] 비연속적 태그 데이터 기록

## 5. 결론 및 향후 과제

유비쿼터스 컴퓨팅 환경에서는 RFID 기술이 현실 세계에서의 여러 가지 사물을 식별하는 주요한 방법으로 사용될 것이다. 그리고 재고관리, 자산관리, 물류 등 기업에서 많은 인적, 시간적 낭비를 내던 업무 분야에 적용되어 큰 효용을 낼 것으로 기대되고 있다.

그러나 라디오 주파를 사용하는 시스템의 특성상 인증되지 않은 사람에게 태그의 내용을 그대로 드러내게 될 위험이 크게 존재한다. 그리고 태그의 내용을 임의로 위조하여 시스템에 큰 혼란을 줄 위험요소가 충분하다.

위와 같은 문제를 해결하기 위하여 RFID 인증 프로토콜 및 프라이버시 해결 방안 등 많은 연구가 있어왔지만 컴퓨팅 능력을 갖지 못한 RFID 태그의 특성을 반영하지 못하여 실질적으로 사용가능한 대안을 제시하고 있지 못한 실정이다.

본 논문에서는 일반적으로 연구되고 있는 RFID 태그에 해싱 함수를 내장하는 방법에서 벗어나 해싱함수를 RFID 리더 측에서 사용하며 RFID 태그에는 해싱 테이블의 레코드를 참조하는 주소를 넣는 방법을 사용하였다. 이 방법을 사용하면 RFID 태그에 들어가는 데이터를 완벽하게 감출 수는 없지만 비 연속적인 데이터를 삽입함으로서 침입자가 RFID 태그의 ID정책을 엿볼 수 없도록 할 수 있다. 이를 통해 임의의 RFID 태그 위조를 방지할 수 있으며 침입자가 RFID 태그를 위조하여 본 시스템에 투입하였더라도 해싱테이블에서 주소로 매칭될 확률이 극히 적어지기 때문에 안정적인 시스템 운영이 가능하다. 또한 본 논문에서 제시한 방법은 다른 선행연구에서 보여진 바와 달리 RFID 태그의 현실적인 면 - 컴퓨팅 능력이 없고 저장 공간이 크지 않음 - 을 고려하였으므로 당장 현실 적용가능하다는 장점을 가지고 있다.

앞으로 제시한 방법에 가장 적합한 해싱 함수를 찾아 각 해싱 함수별로 성능을 검증하는 작업이 필요하며 데이터베이스에 들어가는 해싱 테이블이 시스템 전체에 미치는 영향을 조사, 실험할 필요가 있다.

## 참 고 문 헌

[1] Weiser, M., "The computer for the 21st century", 1991, Scientific American 265, pp.94-95, 98-102

[2] S. Weis et al., "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems", Security and Pervasive Computing 2003, LNCS 2802, pp.201-212.

[3] K. Finkenzeller(1999), RFID Handbook, John Wiley and Sons

[4] A. Juels and R. Pappu(2003), "Squealing Euros : Privacy protection in RFID-enabled banknotes", Financial Cryptography'03, LNCS 2742, pp. 103-121, Springer-Verlag

[5] A. Juels, R. L. Rivest and M. Szydlo(2003),"The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy", 10th ACM Conference on Computer and Communications Security, CCS 2003, pp. 103-111

[6]Giorgi. HASH Based Authentication in RFID. Moniava Seminar Information Security Technology: 2IF03

[7]A Juels. ""RFID security and privacy: a research survey"". Selected Areas in Communications, IEEE Journal on, 2006. pages: 381- 394.

[8]L. Lamport, Password Authentication with

Insecure Communication, Communications of the ACM 24.11, 1981

[9]P. Golle et al., Universal Re-encryption for Mixnets, CT-RSA 2004, LNCS 2964, pp.163-178.

[10]A. Perrig et al., "SPINS : Security Protocols for Sensor Networks," Wireless Nets, Sep. 2002, pp.521-534.

[11]이재우, 신하용, "RFID 기술 개요 및 현황 ," 한국과학기술원 산업공학과 VMS Lab. Technical Report: VMS-2004-03