# 부분 ID를 이용한 읽기전용 RFID태그 인증프로토콜

이 영 진[†] · 정 윤 수[†] · 서 동 일[††] · 이 상 호[†††]


## 요 약

오늘날 저가의 RFID 기술은 리더와 태그사이에 물리적인 접촉 없이 인식 가능한 기술로서 기업과 학술적 분야에서 많은 각광을 받고 있다. 그러나 태그의 정보가 전송과정에 무선특성에 따른 과도한 정보 노출과 사용자의 위치정보 추적과 같은 심각한 프라이버시 침해를 유발시킨다. 특히 읽기전용 태그에서의 보안문제는 단지 물리적 방법으로만 해결하고 있다. 이 논문에서는 간단한 XOR연산과 부분 ID를 이용하여 다양한 공격에 안전하며 읽기전용 태그에 적합한 저비용 인증 프로토콜을 제안한다. 제안 프로토콜은 재전송, 도청, 위장 공격에 안전하며 또한 위치 프라이버시가 보장된다.


**키워드 : 부분 ID, 저비용 RFID, 위치프라이버시, 인증**

# Authentication Protocol Of The Read Only RFID Tag Using Partial ID

Li Yong Zhen[†] · Jeong Yonn Su[†] · Seo Dong Il[††] · Lee Sang Ho[†††]


## ABSTRACT

Nowadays, low-cost radio frequency identification (RFID) technique, is recognizable without the physical contact between the reader and the tag, has been attracting more and more interests from both industry and academic institutes. however, it causes the serious privacy infringement such as excessive information exposure and user's location information tracking due to the wireless characteristics. The security problem of read only tag can be only solved by physical method. In this paper, we propose a low-cost authentication protocol which can be adopted for read-only RFID tag using XOR and Partial ID. The proposed protocol is secure against reply attacking, eavesdropping and spoofing attacking so that avoiding the location privacy exposure


**Key Words : Partial ID, Low-cost RFID, Location Privacy, Authentication**

## 1. 서 론

RFID란 무선인식 기술 즉 Micro-chip을 내장한 태그(Tag), 레이블(Label), 카드(Card) 등에 저장된 데이터를 무선 주파수를 이용하여 리더(Reader)에서 자동으로 인식하게 하는 기술을 말한다. 또한 칩의 저장능력과 인식능력이 향상되면서 이 무선인식 기술은 유비쿼터스 환경에서 필수적인 기술로 각광을 받고 있다. RFID 기술은 단순한 바코드의 대체 수준을 넘어서 통신, 물류, 국방, 소방, 금융, 의료, 환경, 교육, 정보가전, 도로, 건설 등 다양한 인간의 생활 전반에 활용되어 무한한 부가가치를 창출 가능하여, 향후 전 세계적인 산업구조, 시장구조의 변화뿐만 아니라 인간의 삶의 형태까지 변화시키게 될 유비쿼터스 컴퓨팅의 기반 기술로서 인식되고 있다[1, 2].

그러나 RFID 기술은 리더와 태그사이에 물리적인 접촉 없이 인식 가능하고 태그의 정보가 전송과정에 무선특성에 따른 과도한 정보 노출과 사용자의 위치정보 추적과 같은 심각한 프라이버시 침해를 유발시킨다. 이러한 우려들이 RFID의 상용화에 걸림돌이 되며, 성공적인 산업화를 위해서는 재반 프라이버시 문제를 해결해야 하는 것이 선결 과제로 되고 있다. 따라서 현재 태그에 저장된 정보를 보호하고 태그에 대한 위치추적 등과 같은 보안 문제를 해결을 위한 인증 프로토콜에 대한 연구가 활발히 진행되고 있다[3, 4, 5]. 그러나 지금까지 제안된 대부분의 인증 프로토콜은 읽기/쓰기가 가능한 태그들에만 적용 가능한 기법들이며 읽기 전용인 태그들에 대한 보안 기법은 거의 전무한 상태이다. 이는 읽기전용 태그를 비롯한 저가형 태그의 활용의 걸림돌로 되고 있다.

이 논문에서는 부분 ID(PID: Partial ID)와 간단한 XOR 연산을 이용하여 읽기전용 태그들로 구성된 RFID 시스템에서도 적용 가능한 저비용 인증 프로토콜을 제안한다. 이 프로토콜은 기존 프로토콜에 비하여 태그의 계산량을 줄이고

† 준 회 원 : 충북대학교 전자계산학과 박사과정
†† 종신회원 : ETRI 정보보호연구단 선임연구원
††† 종신회원 : 충북대학교 전기전자컴퓨터공학부 교수
논문접수 : 2006년 2월 2일, 심사완료 : 2006년 8월 9일

또한 도청, 위장 및 프라이버시 침해와 같은 보안문제점을 해결하고 한다.

논문의 구성은 다음과 같다. 2장에서는 기존 인증프로토콜을 해쉬기반과 XOR기반으로 분류하여 분석한다. 3장에서는 부분 ID와 간단한 XOR연산을 이용한 저비용 인증 프로토콜을 제안하고 4장에서는 제안 프로토콜의 안전성과 효율성에 대하여 비교평가 한다. 마지막으로 5장에서 결론을 맺는다.

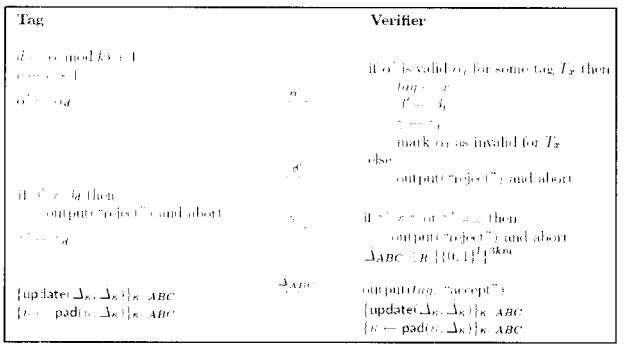
## 2. 관련연구

RFID 기술은 리더와 태그사이에서 무선으로 상호인증 및 정보교환이 이루어진다. 따라서 무선특성에 따른 정보 노출과 사용자의 위치정보 추적과 같은 심각한 프라이버시 침해를 유발시킨다. 현재까지 RFID 시스템에서 사용자의 프라이버시를 보호하기 위하여 여러 가지 기법들이 제안 되었다. 이런 기법들은 크게 태그 무효화(kill), Faraday Cage, Active Jamming 등 물리적 접근기법[7, 8]과 비트연산(XOR) 기반, 해쉬함수 기반, 재암호화 등 암호학적 접근기법[1-6,10.11]으로 분류된다. 물리적 방법들은 사용자 위치추적과 정보유출을 어느 정도 보호할 수는 있지만 차세대네트워크 환경에 적용하기에는 적합하지 않다. 해쉬함수 및 암호화 기법들은 사용자 위치 추적과 정보 유출을 막을 수 있지만 계산양이 많은 단점이 있다. 재암호화 위한 별도의 인프라가 필요하다는 단점이 있다.

저가의 RFID의 구현에 적합하며 보다 효율적인 태그 인증 방법은 XOR연산을 기반으로 한 Juels 기법[10]과 최은영이 제안한 기법[11]이 있다.

### 2.1 Juels 기법

Juels가 제안한 기법은 단순 XOR 연산을 사용하여 저가의 RFID 시스템에서의 적용을 목적으로 제안되었다. (그림 1)에서와 같이 이 기법에서 태그는 리더로부터 이전 세션에서 받은 랜덤 값들과 현재 받은 랜덤 값들에 동일한 값을 가지고 있는지를 확인하여 상호인증을 한다. 구체적으로 보면 태그에는 $(\alpha_i, \beta_i, \gamma_i), 1 \leq i \leq k$로 구성된 비밀값 k를 저장한다. 데이터베이스에는 전체 태그들에 관 한 m개의 랜덤 값$\Delta_i = \{\delta^{(1)}(=(\Delta\alpha_i^{(1)}, \Delta\beta_i^{(1)}, \Delta\gamma_i^{(1)})), \cdots, \delta^{(m)}\}$ $.1 \leq i \leq k$로 테이블을 구성하여 저장한다. 인증과정은 우선 리더가 태그에 질의하면 태그는 $\alpha_d, d \equiv (c \bmod k) + 1$ (c는 초기값을 0인 카운터 수)를 리더에 전송한다. 리더는 $\alpha_d$를 데이터베이스에 전송하여 와 $\alpha_d$대응되는 $\beta_d$를 데이터베이스에서 받아 태그에 전송한다. 태그는 리더에서 받은 $\beta_d$와 자신이 저장하고 있던 $\beta_d$를 비교하여 리더를 인증하고 인가되면 태그는 다시 관련 $\gamma_d$를 리더를 통하여 데이터베이스에 전송하여 태그를 인증한다.



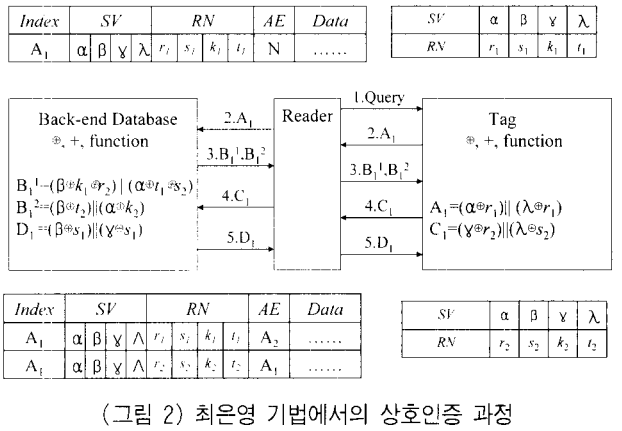

(그림 1) Juels기법에서의 RFID 태그 인증과정

### 2.2 Eunyoung기법

최은영이 제안한 기법은 (그림 2)에서와 같이 6개 단계로 나누어 태그와 리더가 상호인증을 실행한다.

① 리더는 태그에 질의를 보낸다.
② 태그는 비밀 값 α와 λ를 사용하여 A1를 계산하고 A1의 값을 리더를 통해 데이터베이스에 전송한다.
③ 데이터베이스에는 A1값을 이용하여 대응 태그 정보가 있는 위치를 찾는다. 그리고 네 개의 랜덤 값 $r_2$, $s_2$, $k_2$, $t_2$를 생성하고 $B_1^1$, $B_1^2$를 계산하고 $B_1^1$, $B_1^2$를 리더를 통해 태그에 전송한다.
④ 태그는 저장된 값 α, β, $k_1$, $t1$과 리더한테서 받은 $B_1^1$, $B_1^2$를 이용하여 $r_2$, $s_2$, $k_2$, $t_2$를 추출한다. 그다음 $r_2$, $s_2$를 이용하여 $C_1$을 계산하고 $C_1$을 리더를 통하여 데이터베이스에 전송한다.
⑤ 데이터베이스는 우선 전송받은 $C_1$과 저장된 값으로 계산한 $C_1$ 값이 동일한지 비교하여 태그를 인증한다. 다음은 다음번 태그인증을 위한 태그의 인텍스 값 $A_2$를 계산하여 저장하고, $D_1$ 계산하여 리더를 통하여 태그에 전송한다.
⑥ 태그는 리더로부터 전송받은 $D_1$과 저장된 값으로 계산한 $D_1$ 값이 동일한지 비교하여 리더를 인증한다.

Eunyoung기법은 Juels 기법을 기반으로 제안하였으며 특징은 태그와 데이터베이스에서 전송하는 값들과 비밀 값들




(그림 2) 최은영 기법에서의 상호인증 과정

을 분리하여 처리하고 또한 단순 비트연산만 사용하여 기존 해쉬기반 기법이나 재암호 기법에 비하여 효율적이다. 하지만 태그에서의 추가적인 쓰기연산과 저장 공간이 필요하고 또한 데이터베이스에서 많은 계산량이 필요하다. 그리고 위의 두 가지 XOR기반 기법은 읽기/쓰기가 가능한 저가형 RFID 태그에 적합하지만 추가되는 저장공간의 필요로 읽기 전용 RFID 태그에는 적용할 수 없다.

## 3. 부분 ID 기반 인증프로토콜

이 장에서는 부분 ID를 사용하여 저가의 태크에 적합한 안전한 인증프로토콜을 제안한다. 랜덤하게 선택된 부분 ID를 사용하여 태그의 위치노출을 막고 공격자의 무차별한 도청에 따른 데이터분석 및 위장공격에도 안전하다. 이 논문에서는 RFID 시스템을 간단하게 태그(Tag), 리더(Reader) 및 백-엔드 DB(Back-end Database)로 구성하고 리더와 백-엔드 DB는 안전한 채널 상에서 통신이 이루어지고 태그와 리더간의 채널은 안전하지 않다고 가정한다.

### 3.1 보안 요구사항

1) 도청공격에 안전해야 한다. 공격자가 리더와 태그간의 통신을 도청 가능하더라도 태그에 저장된 비밀정보를 알아내는 것이 불가능해야 한다.
2) 재전송 공격에 안전해야 한다. 공격자가 이전 세션의 모든 통신내용을 도청을 통하여 알고 있다고 하더라도 현재 세션에 통신될 정보를 생성하는 것이 불가능해야 한다.
3) 위장공격에 안전해야 한다. 공격자가 태그나 리더로 위장하여 태그 혹은 리더의 비밀정보를 알아내는 것이다. 즉 리더로 위장 시 태그의 비밀정보를 알아내기 위한 공격을 할 수 있으며 태그로 위장하여 재전송 공격 등이 가능하다.
4) 위치트래킹공격에 안전해야 한다. 공격자가 태그와 리더사이에 주고받는 정보를 분석하여 동일한 태그에서 전송되는 정보의 패턴을 알아내어 태그의 위치정보 나아가서 태그소유자의 위치정보를 알아내는 공격을 말한다. 읽기전용인 태그에서 이 공격을 막을 방법은 아직까지는 물리적인 방법을 취하고 있다.

### 3.2 RFID 상호인증프로토콜

#### 3.2.1 초기화 단계

초기화 단계에서는 제안 프로토콜의 실행을 위한 준비단계로서 태그, 리더 및 데이터베이스에서의 연산과 초기화 값들을 설정한다.

① 모든 태그에는 각각 자신의 비밀정보 SID(secure ID)를 저장한다.
② 리더에는 의사난수를 생성할 수 있는 난수 생성기를 설치한다.
③ 그리고 데이터베이스에는 모든 태그의 비밀정보를 저장한다.
④ 그다음 리더와 태그의 상호인증에 사용될 부분 ID의 길이를 SID길이의 절반이상($\geq L/2$)인 값으로 설정한다.

#### 3.2.2 제안프로토콜의 실행과정

제안프로토콜은 (그림 3)에서 보는 바와 같이 11개 단계로 이루어진다.

① 리더가 난수를 생성하여 질의정보와 함께 태그에 전송한다.

$R \rightarrow T$: Query||R

② 태그가 자신의 SID에서 임의로 지정길이의 부분 ID(Partial ID)를 선정하고 리더에서 받은 난수 R과 XOR하여 R′를 계산한다.

T: $\{n|1 \leq n_R \leq L/2\}$, $PID \subset SID$, $R' = R \oplus PID$

③ 태그→는 계산한 R′과 타임스탬프 $T_1$ 를 리더한테 전송한다.

$T \rightarrow R$: $R'||T_1$

④ 리더가 위에서 생성했던 난수 R과 태그에서 받은 R′를 데이터베이스에 전송한다.

$R \rightarrow DB$: $R'||R$

⑤ 데이터베이스가 리더에게서 받은 R과 R′를 XOR하여 태그의 PID를 계산한다. 그리고 계산한 PID를 이용하여 이를 부분집합으로 하는 모든 태그의 SID를 찾고 이 찾은 각 SID에서 PID의 시작위치 정보를 수집한다.

DB: $PID = R' \oplus R$
Search
If $PID \subset SID_i$ Then
$SID_1, n_1; \ldots\ldots; SID_k, n_k$
compute $\overline{PID}_1, n_1; \ldots\ldots; \overline{PID}_k, n_k$

- 만일 검색한 결과 PID를 포함하는 SID가 하나라도 없다면 태그를 위장된 태그로 인정한다.

⑥ 수집된 시작위치와 PID여집합 정보들을 리더에게 전송한다.

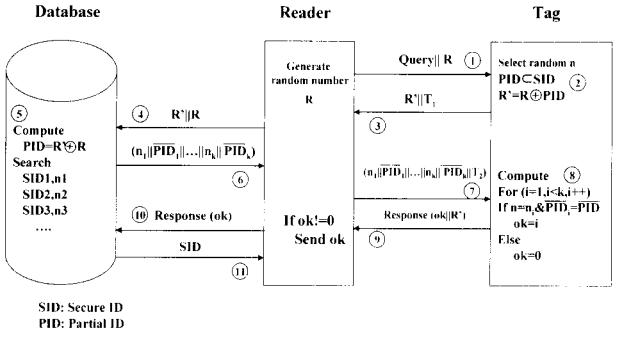
DB→R: response($n_1||\overline{PID}_1||n_2||\overline{PID}_2||\cdots\cdots||n_k||\overline{PID}_k||T_2$)

⑦ 리더는 데이터베이스에서 받은 정보에 타임스탬프 $T_2$를 추가하여 태그에 전송한다.

$R \rightarrow T$: response($n_1||\overline{PID}_1||n_2||\overline{PID}_2||\cdots\cdots||n_k||\overline{PID}_k||T_2$)

⑧ 태그는 데이터베이스에서 받은 PID의 시작위치정보에서 자신이 갖고 있는 PID 시작위치정보와 동일한 것을 찾는다.

T: For(i=1,i<k, i++)
If $n=n_i$ and $PID'_i=\overline{PID}$
ok=i
Else
ok=0




(그림 3) 제안 프로토콜

- 만일 찾은 결과 자신이 갖고 있는 PID 시작위치정보와 동일한 것이 없다면 우리는 리더가 위장된 것으로 인정한다.

⑨ 태그에서 자신이 갖고 있는 PID 시작위치와 동일한 시작위치를 찾았다면 위에서 받은 PID 순서번호 i값을 변수 ok에 저장, 그렇지 않으면 0을 변수 ok에 저장하여 응답 메시지로 리더에 전송한다.

T→R: response(ok||R')

⑩ 리더는 태그에서 받은 ok변수 값이 0이 아니면 ok값을 데이터베이스에 전송하고 만일 0을 받았다면 프로토콜을 종료한다.

R: if ok!=0 send ok to DB

else cancer

⑪ 데이터베이스는 태그에서 받은 순서번호에 근거하여 태그의 SID를 확정하고 관련 정보를 리더에게 제공한다.

DB→R: send SID

## 4. 안전성 및 성능평가

이 장에서는 제안프로토콜에 대하여 기존 대표적인 프로토콜들과 비교하여 제안 프로토콜의 다양한 보안기능과 태그의 효율성을 분석하였다. 분석에서 저가의 RFID 시스템을 구현함에 있어서 효율성은 주로 제한된 자원 특성을 갖는 태그에 대하여 분석을 하며 백-엔드 DB는 계산능력이 강한 호스트로서 저비용 RFID시스템의 전체적인 효율성에 큰 영향을 미치지 않는다고 가정한다.

### 4.1 안전성

1) 재전송 공격에 대한 안전성 : 공격자는 리더로 위장한 재전송 공격과 태그로 위장한 재전송 공격 두 가지 경우가 있다. 리더로 위장한 경우 공격자는 리더에서 태그로 전송되는 메시지를 도청하여 재전송하는 경우인데 제안 프로토콜에서는 타임스탬프 $T_1$, $T_2$의 유효시간을 설정하여 재전송 공격을 막는다.

2) 전송메시지의 기밀성 보장 : 대부분 경우에 전송메시지의 기밀성을 보장하기 위하여 대칭키 암호기법을 이용한다. 하지만 RFID 태그의 저장공간과 연산능력의 제약으로 이런 암호화 기법을 사용하기에는 너무 많은 비용이 든다. 제안프로토콜에서는 난수와의 비트연산을 통하여 전송메시지(PID)를 은닉시켜 전송하여 인증과정에 주고받는 메시지들의 기밀성을 보장한다. 즉, 난수와 PID정보를 알고 있어야만 전송되는 태그의 일부분 ID를 계산해낼 수 있다. 따라서 PID가 노출된다 해도 태그의 전반 SID를 계산이 $1/2^{(L_{SID}-L_{PID})}$(여기서 $L_{SID}$는 SID의 길이, $L_{PID}$는 PID의 길이) 확률적 안전성을 보여 메시지 도청공격에 안전하다.

3) 위치 추적에 대한 안전성 : 태그와 리더간에 주고받는 메시지가 모든 인증 단계에서 매번 서로 다른 메시지가 전달된다. 또한 임의로 선택된 PID를 전송하므로 매번 서로 다른 정보를 교환하기에 기존 불변메시지를 통한 태그의 위치 추적은 불가능하다. 하지만 태그의 SID를 알고 있을 경우 매번 서로 다른 메시지가 전송된다 해도 태그의 위치를 추정할 수 있다. 이것은 특수 목적(법적수사)의 태그추적은 관리자의 권한위임을 통하여 가능함을 제시한다.

4) 사용자 프라이버시 보호: 사용자 프라이버시는 주로 태그의 소유자의 위치정보나 태그정보 누출을 말한다. 위에서 설명한바와 같이 제안 프로토콜에서는 동일한 리더기가 동일한 태그에 대한 인증이라 해도 난수를 기반으로 정보은닉과 부분 ID를 이용하여 매번 서로 다른 인증메시지를 전송함으로 태그의 위치노출과 태그정보유출을 막을 수 있어 사용자 프라이버시가 보장된다.

<표 1>은 기존 인증기법과 비교분석한 결과이다. 분석결과를 보면 제안 프로토콜은 안전성 기능이 기존기법에 기능에 비하여 확장되었음을 알 수 있다.

제안 프로토콜은 다양한 보안 기능을 제공하지만 기존 해쉬기반 기법이나 암호기법에 비하여 보안 강인성이 떨어진다는 문제점이 있다. 그러나 기존 일반 상품관리와 같이 저가의 RFID 태그를 필요로 하는 시스템에서 활용하고 있는 물리적 보안방법보다는 신뢰성이 높고 재사용이 가능하며 또한 구매 후 상품관리도 가능하다는 장점이 있다.

〈표 1〉 기존 인증프로토콜과의 안전성 기능비교

| 기법 | 위치추적 | 도청 | 재전송 | 기밀성 | 해쉬계산량 |
|---|---|---|---|---|---|
| 해쉬락[1] | 가능 | × | × | ○ | **해쉬** 1회 |
| 랜덤해쉬락[2] | 불가능 | × | × | ○ | **해쉬** 1회 |
| 해쉬체인[6] | 불가능 | × | ○ | ○ | **해쉬** 2회 |
| 재암호화[8,9] | 가능 | × | ○ | ○ | **암호** 1회 |
| XOR기반[10,11] | 불가능 | ○ | ○ | ○ | 비트연산 |
| 제안 기법 | 불가능 | ○ | ○ | ○ | 비트연산 |

### 4.2 효율성

RFID 시스템에서는 전력소비, 처리시간, 저장 공간 및 게이트(gate)수 등이 비용계산의 주요변수로 작용한다. 따라서 저비용 RFID 시스템의 구현에 있어서 위의 4가지요소를 줄

〈표 2〉 기존 프로토콜과의 효율성 비교분석

| | | | Juels[10] | Eunyoung[11] | 제안기법 |
|---|---|---|---|---|---|
| 연산량 | 태그 | | (3k~4k)XOR | 8(XOR)+4(+) | (1~k')XOR |
| | 리더 | | 0 | 0 | 1개 난수생성 |
| | DB | 검색 | k*n | n/2 | n/2~n |
| | | 랜덤 값 | 3k개 | 4개 | 0 |
| 다음 세션을 위한 추가정보 | | | 필요 | 필요 | 불필요 |
| 태그의 쓰기연산 | | | 필요 | 필요 | 불필요 |
| 리더와 정보교환회수 | | | 4 | 3 | 4 |
| n: 태그 수, k: 랜덤 값 개수, k': DB에서 찾을 수 있는 PID수 | | | | | |

이는 것이 매우 중요하다. 기존에 제안된 기법에서는 주로 해쉬함수와 암호화 기법을 사용하여 구현하는데 20000~30000gate 비용이 든다. 그 외 최근에 제안한 비트연산을 이용한 Juels기법과 Eunyoung 기법은 500~5000gate의 비용이 들어 해쉬함수나 암호화기법을 보다는 효율적이다. 그러나 이 두 가지 기법 역시 EPC 표준의 Class 1에 속하는 읽기전용 태그에는 적용할 수 없다. <표 2>는 기존 Juels기법과 Eunyoung 기법 및 제안프로토콜들의 태그에서의 비용을 비교분석한 결과이다.

<표 2> Juels 기법에서는 $3km$(여기서 $k$는 각 세션에 사용되는 랜덤 값 개수, $m$는 태그에 저장된 $k$개 랜덤 값을 한 조로한 비밀 값 개수,$l$:태그의 비트 수)번의 XOR연산을 수행하고 Eunyoung 기법에서는 8번의 XOR연산과 4번의 덧셈을 수행하며 제안프로토콜에서는 3번의 XOR만 수행한다. 따라서 Juels 기법과 Eunyoung 기법에 비하여 태그의 연산량이 절반이 줄었으며 또한 쓰기연산과 추가적 저장 공간 필요로 하지 않으므로 저비용 읽기전용 RFID 태그의 활용에 적합하다. 기존 읽기전용으로 태그를 이용한 RFID시스템의 정보보호는 단지 물리적 접근으로만 가능한 것을 제안프로토콜에서는 소프트웨어적 방법으로 해결하였음은 기존 기법보다 우월하다는 것을 입증할 수 있다.

## 5. 결 론

최근 들어 RFID 기술이 기존 바코드 기술에 비해 인식속도가 빠르고, 저장 공간이 크며 무선인식 등 장점을 갖고 있어 사회의 각 분야에 활용되고 있다. 그러나 기존 RFID 시스템은 비용문제, 무선환경의 보안 취약성 및 프라이버시 침해와 같은 새로운 보안문제점이 발생하고 있다. 특히 읽기전용 태그를 이용하는 RFID 시스템에서는 물리적 방법으로만 정보보호문제를 해결하고 있다.

이 논문에서는 간단한 XOR연산과 부분 ID를 이용하여 다양한 공격에 안전하며 읽기전용태그에도 적용 가능한 저비용 상호인증 프로토콜을 제안하였다. 이 인증프로토콜은 기존 프로토콜에 비하여 자원소비의 최소화 하였고 또한 도청, 위장 및 프라이버시 침해와 같은 문제점을 해결하였음을 기존 기법과의 비교분석을 통하여 입증 하였다. 향후 제안 기법에서의 부분 ID 충돌문제 및 데이터베이스에서의 검색에서 효율성 문제를 위한 연구가 필요하다.

## 참 고 문 헌


[1] S. A. Weis, "Radio-frequency identification security and privacy," Master's thesis, M.I.T. 2003.

[2] S. A. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," In First International Conference on Security in Pervasive Computing 2003, LNCS 2802, pp. 201-212, Springer-Verlag.

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

[4] D. Molnar, A. Soppera, and D. Wagner. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In B. Preneel and S. Tavares, editors, Selected Areas in Cryptography-SAC 2005, Lecture Notes in Computer Science. Springer Verlag, 2005.

[5] D. Henrici, P. Muller, "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 Workshops. PERCOMW '04, pp.149-153, IEEE, 2004.

[6] M. Ohkubo, K. Suzuki, and S. Kinoshita (2003), "A Cryptographic Approach to "Privacy-Friendly" tag," RFID Privacy Workshop

[7] Junko Yoshida, "RFID Backlash Prompts 'Kill' Feature," EETimes. April 28, 2003.

[8] 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.

[9] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal reencryption for mixnets. In T. Okamoto, editor, The Cryptographers' Track at the RSA Conference-CT-RSA, volume 2964 of Lecture Notes in Computer Science, pages 163-178. Springer-Verlag, 2004.

[10] A. Juels, "Minimalist cryptography for low-cost RFID tags," In 4th Intel. Conf. on Security in Communication Networks-SCN 2004 vol. 3352 LNCS. pp.149-164.

[11] 최은영, 최동희, 임종인, 이동훈 "저가형 RFID시스템을 위한 효율적인 인증 프로토콜" 한국정보보호학회 논문지 제15권 제5호 pp.59-72, 2005. 10.

## 이 영 진

e-mail : lyz2003@netsec.cbnu.ac.kr
1994년 6월 중국 연변대학교 물리학과 (이학사)
1997년 6월 중국 연변대학교 물리학과 (이학석사)
2003년 3월~현재 충북대학교 대학원 전자계산학과 박사과정
관심분야 : 암호이론, 유비쿼터스 보안, 프라이버시 보호

## 서 동 일

e-mail : bluesea@etri.re.kr
1989년 2월 경북대학교 전자공학과 (공학사)
1994년 2월 포항공과대학교 정보통신공학과졸업(공학석사)
2004년 8월 충북대학교 전자계산학과 (이학박사)
1994년~현재 ETRI 정보보호연구단 선임연구원
관심분야 : 인터넷 정보보호, 컴퓨터 통신, 네트워크관리

## 정 윤 수

e-mail : bukmunro@netsec.cbnu.ac.kr
1998년 2월 청주대학교 전자계산학과 (이학사)
2000년 2월 충북대학교 대학원 전자계산학과(이학석사)
2003년 3월~현재 충북대학교 대학원 전자계산학과 박사과정
관심분야 : 암호이론, 정보보호, Network Security, 이동통신보안, 전자상거래보안

## 이 상 호

e-mail : shlee@chungbuk.ac.kr
1976년 숭실대학교 전자계산학과 (공학사)
1981년 숭실대학교 전자계산학과 (공학석사)
1989년 숭실대학교 전자계산학과 (공학박사)
1976년 1월~1979년 5월 한국전력 전자계산소
1981년 6월~현재 충북대학교 전기전자컴퓨터공학부 교수
관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture