RFID의 프라이버시 보호 기법

김광조 · 양정규
한국정보통신대학교

요 약

무선 주파수 인식(RFID) 기술은 차세대 유비쿼터스 환경에서 중요한 기술적 위치를 차지할 것으로 예상되고 있으며, 다양한 분야에서 새로운 시장을 형성해 나갈 것으로 기대된다. 그러나 RFID 태그 내용의 노출 혹은 임의의 태그에 대한 위치 추적 가능성은 RFID의 실용화에 있어서 사용자의 프라이버시 위협이라는 심각한 문제를 야기할 수 있다. 따라서 본 고에서는 이러한 RFID 프라이버시 보호를 연구 동향들을 살펴보고 방식별 장단점을 비교한다.

Ⅰ. 서 론

무선 주파수 인식(Radio Frequency Identification, 이하 RFID)은 초소형 반도체에 식별정보를 넣고 무선주파수를 이용해 이 칩을 지닌 물체나 동물, 사람 등을 판독 · 추적 · 관리할 수 있는 기술로, 차세대 물류 · 유통뿐 아니라 전자 지불 · 보안 등 다양한 분야에서 새로운 시장을 형성할 것으로 기대되고 있다. RFID 기술은 2차 세계대전 당시 레이더에서 발산되는 신호로 적과 아군을 식별할 목적으로 연합군에 의해서 처음으로 사용된 것으로 알려져 있다. 아직까지는 RFID 칩의 높은 가격으로 인해 RFID 기술의 사용이 보편화되지 못하고 있지만, 칩 가격이 급속한 속도로 낮아지고 있어 현재의 추세라면 2, 3년 내에 RFID 기술의 사용이 전 산업분야로 확대되어 나갈 것으로 보인다.

그러나 RFID 태그의 사용에 있어서 프라이버시 보호에 대한 중요한 문제가 존재한다[15]. 이 문제는 RFID의 기본 특성(각 RFID 태그의 식별 정보가 쉽게 식별될 수 있다) 때문에 일어난다. RFID 태그는 모든 리더에게 자동적으로 응답한다. 다시 말하면, 태그의 소유자가 알지 못하는 사이에 태그는 그것의 정보를 전송하고, 이 성질이 프라이버시 침해 요소를 유발시킨다. 이러한 우려들이 공공의 관심사가 되기 시작하기 때문에, RFID의 성공적인 산업화를 위해서는 제시되는 프라이버시 문제들을 해결해야 하는 것이 우선 과제가 되고 있다.

본 고는 다음과 같이 구성되어 있다. Ⅱ장에서는 RFID 시스템 특성들에 관하여 살펴보고, Ⅲ장에서 RFID 관련 프라이버시 문제와 보안 요구사항에 관하여 살펴본다. Ⅳ장에서 RFID 관련 프라이버시 문제 해결하는 암호적인 기법을 조사하고, Ⅴ장에서는 각 기법의 장단점을 비교한 후, 끝으로 Ⅵ장에서 결론 및 향후 연구 방향을 제시한다.

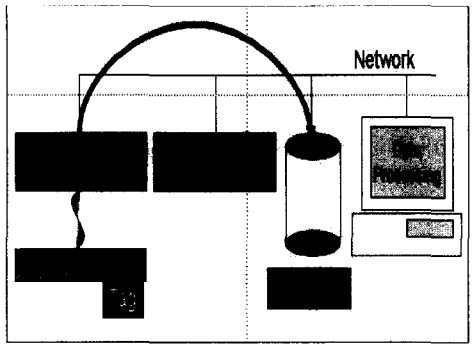
Ⅱ. RFID 시스템

2-1 RFID 시스템

RFID 시스템은 일반적으로 [그림 1]과 같이 무선 태그 T(Tag), 무선 리더기 R(Reader), 그리고 백-앤드 서버 B(back-end server)로 구성된 정보 추적 시스템이다[8],[11].

2-1-1 태그(Tag)

태그 T는 IC 칩과 안테나로 구성되어 있으며, 무선 신호에 대한 응답으로 자신의 정보를 RFID 리더에게 보낸다.



[그림 1] RFID 시스템의 구성도

2-1-2 리더(Reader)

리더 R은 태그 T에게 무선 주파수 신호를 보내고, T에 의하여 전송된 정보를 받으며, 백-앤드 서버 B에게 그 정보를 보낸다.

2-1-3 백-앤드 서버(Back-End Server)

서버 B는 각각의 태그 T에 대한 다양한 형태의 정보(예: 태그 식별 정보, 리더 위치 등)를 관리 저장하는 안전한 서버이다. 서버 B는 인증된 리더를 통하여 태그 T에 의하여 보내진 정보로부터 태그의 식별정보를 결정한다.

기타의 구성요소로써 네트워크 및 전사적 자원관리(ERP), 공급망 관리(SCM) 등의 관련 응용 프로그램 등을 들 수 있다.

2-2 RFID 시스템 특성

RFID 태그는 크게 능동형 태그(active tag)와 수동형 태그(passive tag)로 구분되어진다. 능동형 태그는 자체 배터리를 내장하고 있어 자체적으로 신호를 발생시킬 수 있다. 자체 배터리를 가지지 않는 수동형 태그는 전원을 외부로부터 얻는다. 비용이 저렴하기 때문에 수동형 태그가 가장 일반적인 형태의 RFID 태그가 될 것이고, 그러한 이유로 본 고에서는 수동형 태그에 관하여 논의하고자 한다.

일반적으로, 시장성을 고려해볼 때 수동형 태그의 가격이 5센트 이하가 될 것으로 예상되어진다. 5센트 태그를 위해서는, IC 가격이 2센트를 초과하지 않아야 한다[13]. 이러한 조건들이 태그내의 게이트 수를 7.5~15 kgate로 제한하고 있다. 실제로 보안을 위한 게이트의 수는 2.5~5 kgate를 넘지 않아야 한다[12]. 이러한 이유로, RFID 관련 보안문제 해결방안으로 일반적으로 상용화 되고 있는 암호 알고리즘의 사용은 어려울 것으로 판단되고 있다[2].

RFID 태그와 리더기와의 통신에 있어서는 무선통신 기반이기 때문에, 도청이 용이할 것으로 간주되며, 리더기와 백-앤드 서버는 기존의 안전한 채널에서 통신이 이루어진다고 가정한다.

Ⅲ. RFID와 관계된 프라이버시 문제

본 절에서는 RFID의 실용적인 적용에 있어서 대두되는 프라이버시 관련 문제점을 조명해 보고 이를 통해 RFID에서 요구되는 보안 목표를 기술하며, 프라이버시 보호 해결을 위하여 진행된 연구 동향들을 소개하고자 한다.

3-1 RFID 보안 문제

RFID 통신은 비접촉(Contactless) 방식을 취하기 때문에 태그의 소유자가 알지 못하는 사이에 개인의 프라이버시에 해당하는 정보가 원격으로 취득될 수 있는 등의 프라이버시 침해 요소들이 많다. 이에 프라이버시 침해 요소를 최소화하기 위한 방안이 모색중에 있다.

RFID 보안 문제는 크게 두 가지로 구분지어 생각해볼 수 있다. 첫째는 태그 내 데이터의 누출이고[9], 두 번째는 임의의 태그 ID를 추적함으로서 일어날 수 있는 불법추적행위이다[17].

3-1-1 사용자 소지품에 대한 정보의 유출

일상생활에서, 대게 우리들은 다양한 물건을 지니고 다닌다. 그러한 물건들 중 일부는 개인적인 물건들일 것이고, 누군가가 그 물건이 무엇인지 아는 것을 원치 않는 경우들이 종종 있다. 예를 들면, 자신이 얼마의 돈을 가지고 있는지, 어떤 값비싼 물건들을 지니고 있는지, 어떠한 약을 혹은 어떠한 책들을 가지고 있는지를 타인이 아는 것을 원치 않는 경우들이 종종 발생하곤 한다. 만약 그러한 물건들에 태그가 부착되어 있는 경우, 소유자의 허락없이 태그의 내용 정보들이 타인에게 유출될 위험을 가지고 있다.

3-1-2 개인 위치 추적

상품에 태그를 이식할 경우 태그의 내용이 안전하더라도 단지 그 태그의 응답 메시지를 통해 각 개체의 위치를 파악할 수 있다. 이러한 문제는 특히 특정 태그가 오랜 기간동안 추적 당할 수 있을 때 더욱 심각한 문제를 야기시킬 수 있다.

3-2 보안 요구 사항

위에서 살펴본 RFID 보안 문제들을 해결하기 위하여 RFID는 RF 태그와 보유자 및 리더 등 구성 환경에 대해 다음과 같은 사항을 고려해 보안 목표를 설정해 볼 수 있다[11].

- 태그는 태그 소유자의 프라이버시를 손상 또는 위협하지 말아야만 한다.
- 정보는 인증이 되지 않은 리더로 유출이 되서는 안 되며, 태그와 그 소유자 사이에 긴 기간 동안의 추적(long-term tracking)이 불가능해야만 한다.
- 추적을 막기 위해서 소유자는 그들이 보유한 태그를 감지하거나 사용불가로 만들 수 있어야만 한다.
- 공개적으로 사용 가능한 태그의 결과는 랜덤화 되거나 태그와 소유자 사이의 장기간 관련성(long-term association)을 회피하기 위해 쉽게 수정이 가능해야만 한다.
- 비공개적인 태그의 내용은 접근제한기법(access control)에 의해 질의 채널(interrogation channel)이 안전하지 않다고 예상된다면 암호화되어야 한다.
- 태그와 리더는 모두 상호 신뢰해야만 한다.
- 태그와 리더 어느 쪽이든 스푸핑(spoofing)이 어려워야 한다.
- 접근제한 기법의 제공 이외에도 태그와 리더 사이에는 상호인증(mutual authentication)이 신뢰의 척도로서 제공된다[6].
- 전원의 중단이 프로토콜을 손상시키거나 가로채기공격(hijack) 시도에 대한 대책을 강구하여야 한다.
- 태그와 리더 모두 재생공격(replay attack) 및 공격자 중간 공격(man-in-the-middle attack)에 저항력이 있어야만 한다.

Ⅳ. RFID 보안문제 해결을 위한 연구동향

RFID 시스템에서 사용자 프라이버시의 보호를 위한 많은 연구들이 진행되어오고 있다. 이 절에서는 현재 진행되어왔던 연구 결과들을 살펴보기로 한다.

4-1 방식 A : Kill 명령어의 접근법

MIT의 Auto-ID 센터에 의하여 알려진 Kill 명령어 접근법에서는, 각 태그가 8비트의 고유한 패스워드를 갖고 있으며, 자신의 패스워드를 받을 경우 태그는 그 자신을 소거한다[5]. 그러나 이 방법은 시작 전 신중한 결정이 필요한 점, Kill 명령이 제대로 완료되었는지 확인하기 어렵다는 점, 응용 방법이 제한된다는 점 등의 문제들을 가지고 있다. 또한 패스워

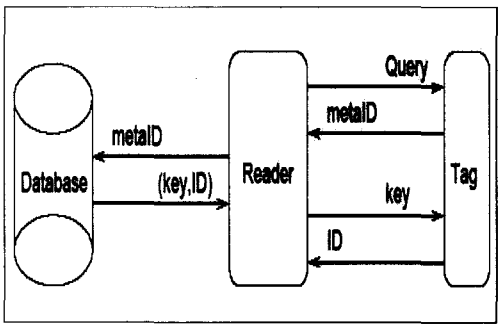
드가 8비트이므로, 공격자가 2^8 계산 안에 정확한 패스워드를 결정할 수 있다는 결점을 가지고 있다.

4-2 방식 B : 해쉬-락 기법

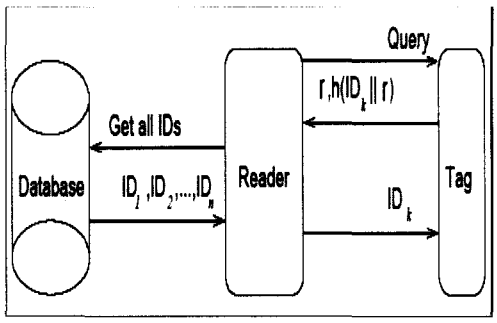
2003년 S. Weis 등에 의하여 제안된 이 기법에서는 단지 한번의 해쉬 함수만을 사용하기 때문에 저가로 구현될 수 있다[14]. 이 기법에서 리더는 각각의 태그에 대한 키 K를 가지고 있고, 각각의 태그는 키에 대한 해쉬 값 *meta*ID=$H(k)$를 갖는다. [그림 2]에서처럼 태그가 리더로부터 접근 요청을 받으면 응답으로 *meta*ID 값을 보낸다. 리더는 태그로부터 받은 *meta*ID와 관계된 키 K를 태그에게 보낸다. 이 때, 태그는 리더로부터 받은 키에 대한 해쉬 값을 계산하고 그 값이 자신이 가지고 있는 *meta*ID 값과 같은지를 판단한다. 두 값이 일치할 경우에만, 태그는 그 자신의 ID를 리더에게 보낸다. 비록 이 기법은 저가로 구현될 수 있는 장점을 가지고 있지만, *meta*ID 값이 항상 일정하기 때문에, 공격자가 임의의 태그를 추적할 수 있는 단점을 가지고 있다.

4-3 방식 C : 해쉬-락 기법의 확장

이 방법[14]는 위에 설명한 해쉬-락 기법의 확장이다. 태그가 해쉬 함수와 의사난수 생성기를 갖는다. [그림 3]에서처럼 각 태그는 해쉬 함수에서 생성



[그림 2] 해쉬-락 기법



[그림 3] 해쉬-락 기법의 확장

된 의사 난수와 자신의 ID를 입력 값으로 하여 c=*hash*(*ID* ‖ r)을 계산한다. 태그는 c와 r을 리더에 전달한다. 리더는 이 값을 백-앤드 서버에게 전달한다. 서버는 자신이 저장하고 있는 모든 태그의 식별정보 ID_i와 r로부터 c에 대응하는 유일한 식별정보를 찾은 후, 그 값을 리더에 전달한다.

이 기법에서는 태그의 결과 값이 매번 바뀌기 때문에 위치 추적을 막을 수 있으며 재생 공격에 강하다. 그러나 저가의 해쉬 함수와 동시에 의사-난수생성기의 구현이 어려운 장벽이다. 더욱이 이 기법에서 백-앤드 서버는 특정 태그의 식별정보를 찾기 위하여 매번 모든 태그의 식별정보와 의사 난수에 대한 해쉬 값을 계산해야하는 단점을 가지고 있다.

4-4 방식 D : XOR 기반 일회용 패드 기법

이 기법[1]은 단지 XOR 연산만을 요구하며, 정말로 저렴한 비용을 요구한다. 리더(실제로 백-앤드 서버 B)와 태그는 무작위 키에 대한 공통 목록을 갖고 있으며, 여러 번의 연결로 상대방이 동일 목록의 키를 가지고 있음을 확인한다. 이 단계 후 태그는 ID를 전달한다.

그러나 이 기법은 리더와 태그 사이의 인증을 위하여 너무 많은 통신을 필요로 한다. 게다가 안전성을 위해 공통 목록이 완전히 새롭게 재 기록될 필요

가 있다. 이런 문제가 구현 및 효율성에 어려움으로 남아 있다.

4-5 방식 E : 외부 재 암호화 기법

외부 재 암호화(External re-encryption scheme)[3]에서는 공개키 암호를 사용한다. 태그 데이터는 외부 유닛으로부터 전달된 데이터를 사용자가 사용 요청할 때 재 기록된다. 이 외부 유닛은 공개키 암호화가 많은 연산량을 요구하기 때문에, 태그만으로는 연산처리가 어려우며, 이 작업은 대체로 리더에 의해 수행된다. 태그의 결과 값은 각각 재기록 주기 안에서 무작위로 보이므로, 태그의 결과 값을 도청하는 공격자는 긴 시간 주기 동안 태그를 추적할 수 없다.

그러나 이 기법은 암호화된 ID는 일정하기 때문에 각 태그의 데이터는 반드시 자주 재 기록되어야 하는 어려움이 있다. 사용자의 행위를 통한 이런 작업은 다소 비현실적인 것으로 판단되고 있다.

4-6 방식 F : 해쉬 체인 기반 기법

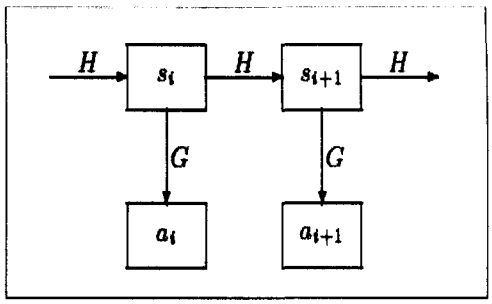
가장 최근에 M. Ohkubo 등은 RFID 시스템에 적용 가능한 전 방향 안전성(forward secure)을 제공하는 해쉬 체인 기법을 소개하였다[17]. 이 기법에서 초기상태의 태그는 초기 비밀 값 S_1을 가지고 있다 가정한다. 프로토콜의 주요 아이디어 [그림 4]와 같이 태그의 이전 응답 메시지와 이후 응답 메시지 간에 관계를 공격자로 하여금 추측할 수없게 하는 것이다. 요약하면 i-번째 통신에서, 태그는 다음을 수행한다.

(1) 리더의 요청신호의 응답으로 $a_i=G(s_i)$ 값을 리더에게 보낸다.

(2) 이전의 자신의 비밀 값 s_i를 $s_{i+1}=H(s_i)$로 갱신한다.

이 때, 함수 G와 H는 해쉬 함수이다.

전체적인 RFID 시스템 프로토콜은 다음과 같다.



[그림 4] 해쉬 체인 기반 기법

구조 : m을 태그의 수라 하고, 각각의 태그를 $T_t(t=1, \cdots, m)$이라 하자. 서버 **B**는 다음을 수행한다.

(1) 각각의 태그 T_t에 대한 랜덤 비밀 값 $s_{t,1}$을 발생시킨다.

(2) 태그 T_t의 메모리에 초기 비밀 값 $s_{t,1}$을 저장한다.

(3) 데이터베이스에 태그 T_t에 대한 식별정보 $ID_t=(id_t, s_{t,1})$를 저장한다.

태그 : i-번째 통신에서 태그 T_t는 다음을 수행 한다.

(1) 리더의 요청신호에 대한 응답으로 $a_{t,i}=G(s_{t,i})$ 값을 리더에게 보낸다.

(2) 이전의 자신의 비밀 값 $S_{t,i}$를 $S_{t,i+1}=H(s_{t,i})$로 갱신한다.

리더 : i-번째 통신에서 리더 **R**은 다음을 수행한다.

(1) 태그 T_t로부터 $a_{t,i}$값을 받는다.

(2) 안전한 채널을 통하여 백-앤드 서버 **B**에게 $a_{t,i}$값을 보낸다.

(3) 안전한 채널을 통하여 백-앤드 서버 **B**로부터 태그 T_t의 식별정보 id_t값을 받는다.

백-앤드 서버 : 백-앤드 서버 **B**는 모든 태그의 식

별정보 값 $ID_i=(id_i, s_{i,1})$을 관리한다. 서버 **B**는

(1) 안전한 채널을 통하여 리더 **R**로부터 $a_{t,i}$ 값을 전달 받는다.

(2) 데이터베이스에 저장되어 있는 모든 $s_{i,1}(t=1, \cdots, m)$와 모든 $i(1\le i\le n)$에 대하여 $a_{t,i}=G(H^{i-1}(s_{i,1}))$를 체크함으로서 $a_{t,i}$에 대응하는 id_i 값을 찾는다. (여기서 n은 해쉬 체인의 최대 길이를 의미한다.)

(3) 안전한 채널을 통하여 리더 **R**에게 id_i 값을 보낸다.

이 기법은 리더의 요청에 대한 태그의 응답 값이 매번 다르기 때문에 추적 문제를 해결할 수 있다고 주장되어진다[17]. 한편, 태그의 i-번째 비밀 값이 노출되었다 하더라도 i-번째 이전의 정보들이 보호될 수 있다는 의미에서 전 방향 안전성(forward secrecy)을 제공하는 것으로 알려져 있다. 그러나 이 기법은 백-앤드 서버 **B**가 많은 계산량을 감수해야만 하는 단점을 가지고 있으며 태그 내에 두 개의 서로 다른 해쉬 함수를 구현하여야 하는 것도 부담이다.

4-7 방식 G : 해쉬 체인 기반의 확장

앞서 설명한 해쉬 체인 기법에서 서버 **B**의 계산 로드를 줄이기 위하여 제안된 기법이다[17]. 이 기법에서 태그 T_i는 리더의 요청 응답 값으로 $a_{t,i}$값 대신에 카운트 정보를 포함한 값 $(a_{t,i}, i)$을 보낸다. 이 경우, 서버 **B**는 카운트 정보 i만을 체크하면 된다. 더불어서, 서버 **B**는 태그에게서 받은 이전 정보 $s_{t,i-1}$를 저장할 수 있다. 이 경우, 서버 **B**의 해쉬 함수 계산 과정을 줄일 수 있다. 끝으로, 향상된 기법에서는 하나의 해쉬 함수를 이용하여 두 개의 해쉬를 사용하는 효과를 제공함으로서 구현의 비용을 줄이고 있다. 비록 이 기법이 이전의 해쉬 체인 기법에 비하여 효율적이기는 하지만, 초경량(lightweight) 해쉬 함수의 구현에 대한 연구와 보다 세심한 안전성, 효율성에 대한 검토가 필요하다.

4-8 방식 H : 블러커 태그 방법

Kill 명령을 이용한 방식 A는 태그의 정보유출을 원천적으로 방지함으로써 사용자의 프라이버시를 확실히 보장할 수 있다. 하지만 유용한 태그의 정보를 이후에 재이용하고자 하는 현실적인 문제에 있어서 문제점을 안고 있다. 또한 위에서 나열한 여러 방법이 현 시점에 있어 저가의 RFID 태그의 응용에 적용 가능한가의 의문을 안고 있다. 이런 점에서 현시점의 RFID 기술을 적용하면서 보다 현실적으로 사용자의 프라이버시를 보호할 수 있는 방안으로서 사용자 프라이버시가 보장되어야 할 시점부터 별도의 태그를 이용하여 공중파로 노출되는 태그 정보의 노출을 막아보고자 하는 방안이 [4]에서 제안되고 있다.

이 방안에서는 블러커 태그(Blocker Tag)라는 별도의 태그를 보호하고자 하는 태그에 용도별로 별도로 부착하는 형태이다. 이때 블러커 태그는 보호하고자 하는 태그의 정보를 알아내고자 하는 공격자의 요청에 대해 실제 태그와 같은 정보로 응답하되, 특정 태그 정보가 아닌 전체 태그 정보를 전달하는 형태로 공격자가 특정태그 정보를 찾지 못하게 하는 방법이다.

이 방법은 기본적으로 [13]에서 제시된 RFID 태그의 응답에 대한 충돌 회피 기법으로 제안된 이진 트리를 이용한 2진 트리 프로토콜을 이용하고 있다. 이 방법의 유용한 또 다른 점은 블러커 태그 방안이 임의의 공격에 대응해 보호받을 태그의 범위를 이진 트리의 특정 영역으로 세분화 하는 방안을 제시하고 있다는 점이다. 이렇게 함으로써 보호영역 자체를 다중 프라이버시 영역(Multiple Privacy Zone)으로 나눠 2진 트리의 탐색에 효율을 기할 수 있다. 더불어

관리하고자 하는 제품에 대해 태그의 영역정책(Zone Policy)을 적용해 다양한 보호정책을 펼 수 있도록 할 수 있다.

블러커 태그를 이용한 방안은 현재 RFID 태그에 바로 적용할 수 있다는 실용적인 측면과 향후 유비쿼터스 환경에서 RFID 태그로부터의 정보를 재활용할 수 있다는 측면에서 의미를 부여할 수 있다.

V. 방식별 비교

여기서는 지금까지 제시한 방식별에 대한 암호학적 특성과 장단점을 〈표 1〉과 같이 비교 분석한다.

Kill 명령어에 의한 접근법은 방식 자체의 간단함으로 현실성이 높지만 패스워드의 길이가 짧다는 점, Kill 명령어가 제대로 완료되었는지에 대한 확인이 어렵다는 점 및 응용 방법이 제한된다는 점 등의 보완 여지가 많다. 해쉬-락 기법은 가장 저렴한 구현을 요구하여 RFID 태그에 적용 가능하지만, 사용자 추적이 가능하다는 매우 취약한 결점을 가지고 있다. 비록 확장된 해쉬-락 기법이 사용자 추적 공격을 피할 수는 있지만, 인증 확인시 백-앤드 서버가 모든 사용자의 식별정보를 계산해야만 하는 계산적 부담을 가진다. 또한, 태그 내에 난수 발생기를 구현해야 한다는 결점도 가지고 있다. XOR 기반의 일회용 패드기법과 외부 재 암호화 기법들은 각각 태그와 리더간의 인증을 위하여 너무 많은 통신이 이루어져야 한다는 결점과 외부 유닛을 가져야 한다는 결점때문에 비현실적이다. 해쉬 체인 기법은 기본적인 RFID 시스템의 보안 요구사항들을 만족하는 것으로 주장되고 있으나, 그에 대한 검증이 아직 이루어지지 않

〈표 1〉 보안 방식별 비교 분석

보안방식	보안요구도의 충족도			태그 연산	장점	단점
	태그 보호	트래킹 보호	전방위 안전성			
방식 A	△	○	△	×	구현 용이	짧은 패스워드에 대한 공격의 위험성 존재 명령의 완료
방식 B	○	×	×	해쉬	구현 용이	추적 가능 태그의 위조 가능
방식 C	○	○	×	해쉬, 난수 발생	보안요구사항 만족	난수 발생기의 구현 필요, 백-앤드 서버의 계산 로드
방식 D	○	○	×	XOR	가장 적은 계산량	인증을 위하여 너무 많은 통신을 필요, 공통 목록의 재 기록 필요
방식 E	○	○	○	×	이론적으로 가장 안전	외부 유닛 필요, 비현실적
방식 F	○	○	○	해쉬	저가의 연산으로 보안 요구사항 만족	안전성 검증 미비, 저가의 해쉬함수 구현 연구 필요
방식 H	○	○	○	×	추가 구현이 불필요	별도 태그의 부착을 필요로 함

(기준: ○-만족, △-일부 만족, ×-만족 않음)

았으며, 저가의 해쉬 함수의 구현방안이 해결되어야 할 연구과제로 남아 있다. 마지막으로 블러커 태그를 이용하는 방법은 서비스 거부공격(Denial-of-service)이 거론되어지고 있으나 큰 위협으로 평가되고 있지 않으며, 방식 자체가 매우 간단하여 추가 구현이 필요치 않다는 점에서 기존의 응용분야에의 적용에 현실성이 있는 방식으로 고려된다.

Ⅵ. 결 론

RFID 관련 프라이버시 보호에 대한 핵심 연구 주제 중 하나는 낮은 비용으로 암호화 프로세스가 가능한 RFID를 개발하고 구현하는 것이다. 여기에는 해쉬 함수, 난수 생성기 그리고 대칭키 암호, 비대칭키 암호(공개키 암호) 등의 경량화 연구가 포함된다.

낮은 비용의 하드웨어 구현은 반드시 회로 부분을 최소화 하여 비용을 낮추고, 공격자가 전력의 소비 시간을 예측할 수 없이 전력 소비가 이루어져야 한다. 고가의 RFID 디바이스에서는 이미 대칭키 암호가 적용되거나 NTRU 같은 공개키 암호 알고리즘이 쓰이고 있다. 하지만 이러한 기법들이 저가의 RFID에도 적용될 수 있어야만 한다. 즉, 수동형 RFID 태그에 적용 가능하여야만 시장성이 있다고 볼 수 있다.

현재 RFID의 보안 요구 사항으로 태그 정보의 보호, 임의의 태그에 대한 추적 방지 등이 제시되고 있다. 가장 최근에 연구되고 있는 프라이버시 보호를 위한 해쉬 체인 기법 등의 연구는 RFID의 보안 요구사항을 어느 정도 만족하고 있다. 그러나 연산량의 줄이는 방법, 초경량 해쉬 함수의 구현 문제 사항들이 더욱 연구되어야만 한다. 또한, 재 기록이 가능한 태그(rewritable tag)에 대한 무결성 보장 등도 연구 주제로 진행되고 있다.

아직까지는 표준화된 RFID의 보안 요구 사항에 대한 정의 및 정형화된 기법은 존재하지 않고 있다. 따라서 보안에 대한 기술적 접근과 더불어 RFID 보안 연구에 있어 표준화 작업도 다각적으로 전개될 전망이다.

참 고 문 헌

[1] A. Juels, "Privacy and authentication in low-cost RFID tags", In submission, Available at http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/

[2] A. Juels, "Minimalist cryptography for low-cost RFID tags", Available at http://www. rsasecurity.com/rsalabs/staff/bios/ajuels/publications/index.html

[3] A. Juels, R. Pappu, "Squealing euros: privacy protection in RFID-enabled banknotes", *In Proceedings of Financial Cryptography FC'03*, 2003.

[4] A. Juels, R. L. Rivest and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy", *In Proceedings of 10th ACM Conference on Computer and Communications Security(CCS 2003)*, Oct. 2003.

[5] Auto-ID Center, "860 MHz~960 MHz class I radio frequency identification tag radio frequency & logical communication interface specification proposed recommendation version 1.0.0", *Technical Report MIT-AUTOID-TR-007*, Nov. 2002.

[6] I. Vajda, L. Buttyan, "Lightweight Authentication Protocols for Low-Cost RFID Tags", *UbiComp 2003.*

[7] K. Finkenzeller, *RFID Handbook*, John Wiley & Sons, 1999.

[8] K. Romer, T. Schoch, F. Mattern and T. Dubendorfer, "Smart identification frameworks for ubiquitous computing applications".

[9] R. L. Rivest, "Approaches to RFID privacy", *RSA Japan Conference, 2003.*

[10] S. Kinoshita, F. Hoshino, T. Komuko, A. Fujimura and M. Ohkubo, "Nonidentifiable anonymous-ID scheme for RFID privacy protection", *Proc. of CSS 2003*, pp. 497-502, IPSJ, (in Japanese), Oct. 2003.

[11] S. Sarma, S. Weis and D. Engels, "RFID systems, security & privacy implications", Auto-ID Center.

[12] S. Sarma, S. Weis, and D. Engels, "Radio-frequency identification: security risks and challenges", *CryptoBytes*, 2003.

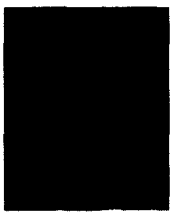
[13] S. Weis, "Security and privacy in radio-frequency identification devices", *Master's thesis*, MIT. 2003.

[14] S. Weis, S. Sarma, R. Rivest and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", *In Proceedings of the 1st Security in Pervasive Computing*, 2003.

[15] T. Scharfeld, "An analysis of the fundamental constraints on low cost passive radio-frequency identification system design", *Master's Thesis*, Dept. of Mechanical Engineering, MIT, Cambridge, 2001.

≡ 필자소개 ≡

김 광 조



1980년: 연세대학교 전자공학과 (공학사)
1983년: 연세대학교 대학원 전자공학과 (공학석사) (M/W 전공)
1991년: 일본 요꼬하마 국립대 대학원 전자정보공학 (공학박사) (암호학 및 정보보호 전공)
1979년 12월~1997년 12월: 한국전자통신연구원 부호1실장/책임연구원
1995년 1월~1997년 5월: 한국정보통신기술표준협회 일반보안 기술 실무 작업반 의장
1996년 3월~1997년 8월: 충남대학교 컴퓨터과학과 겸임교수
1999년 12월~2000년 2월: 요꼬하마 국립대 및 동경대 방문교수
1998년 1월~현재: 한국정보통신대학교(ICU) 공학부 교수
1999년 1월~현재: 세계암호학회 이사
2001년 3월~현재: 국제정보보호기술연구소(IRIS) 소장
2003년 1월~현재: IT 영재교육연구원 소장
[주 관심분야] 암호와 정보보호 이론 및 응용

양 정 규

1999년: 한남대학교 컴퓨터공학 (공학사)
2003년 2월~현재: 한국정보통신대학교(ICU) 정보보호 (공학석사)
2003년 3월~2004년 2월: 국제정보보호연구소 운영지원사업연구원
2004년 2월~현재: NITZ Co. 유비쿼터스 시스템보안 사업 연구원
1999년 2월~현재: 한국조폐공사 경영정보팀
2004년 4월~현재: ETRI 링크레이어 보안 사업 연구원