저가의 RFID에 관한 정보보호 기법 연구†

양정규*, 김광조*, 표철식**

*한국정보통신대학교, 국제정보보호기술연구소

**한국전자통신연구원,

A Study on Low-Cost RFID Schemes

Jeongkyu Yang*, Kwangjo Kim*, Cheol Sig Pyo**

*International Research Center for Information Security(IRIS),

Information and Communication Univ.(ICU), Korea

**Electronics and Telecommunications Research Institute, Korea

요 약

기존의 바코드를 대체할 차세대 인식 기술로 급부상하고 있는 무선 주파수 인식(이하 RFID) 기술은 사회 전반에 걸쳐 파급되는 효과가 매우 클 것으로 예상 된다. 하지만 핵심이 되는 태그 자체의 특성으로 인해서 사용자의 프라이버시 침해라는 역기능을 내포하고 있으며, 이는 향후 실용화에 있어서 심각한 문제점으로 대두될 전망이다. 본 논문에서는 저가의 RFID 태그의 보안침해 요인 및 제안된 정보보호 기법을 살펴보고 RFID 환경에서 안전한 정보보호 방안을 제시하기 위하여 어떠한 암호학적 기법들을 사용하였는지 이해하고자 한다. 또한, 이러한 기법들의 암호학적 특징들에 대한 차이점을 비교 분석한다.

I. 서론

RFID는 초소형 반도체에 식별정보를 넣고 무선주파수를 이용해 이 칩을 지닌 객체를 판독·추적·관리할 수 있는 기술을 말한다. 아직까지는 RFID 칩의 높은 가격으로 인해 RFID 기술의 사용이 보편화되지 못하고 있지만 칩 가격이 급속히 낮아지고 있어 빠른 시일 내에 RFID 기술의 사용이 전 산업분야로 확대되어 나갈 것으로 보인다.

그러나 RFID 태그의 사용에 있어서 프라이버시 침해라는 중요한 문제를 내재하고 있다[13]. 이 문제는 RFID 태그의 식별 정보가 쉽게 식별될 수 있다는 RFID 시스템의 기본 특성 때문에 일어난다. 즉, 태그의 소유자가 알지 못하는 사이에 태그의 정보가 전송됨으로써 프라이버시 침해 요소를 유발시킨다. 따라서 RFID의 향후 성공적인 산업화를 위해 이러한 프라이버시 문제들을 해결해야하는 것이 우선 과제가 되고 있다.

본 논문에서는 Ⅱ장에서 일반적인 RFID 시스템에 관한 소개와 저가의 RFID 관련 보안 문제 및 보안 요구사항에 관하여 살펴본다. Ⅲ장에서 RFID 관련 프라이버시 문제를 해결하기위한 암호적인 기법을 조사하고, Ⅳ장에서는 각 기법의 장단점을 비교한 후, 끝으로 Ⅴ장에서 결론 및 향후 연구 방향을 제시한다.

II. RFID 시스템 보안 문제 및 대책

1. RFID 시스템

일반적인 RFID 시스템은 태그 T(Tag), 리더 R(Reader), 그리고 백-앤드 서버 B(back-end server)로 구성 된다[6, 9].

T는 IC 칩과 안테나로 구성되어 있으며, 무선 신호에 대한 응답으로 자신의 정보를 R에 보낸다. R은 T에게 무선 주파수 신호를 보내고, T에 의하여 전송된 정보를 받으며, B에게 그 정보를 보낸다. B는 각각의 T에 대한 다양한 형태의 정보(예: 태그 식별정보, 리더 위치 등)를 저장·관리하는 안전한 서버이다. B는 인증된 리더를 통하여 T에 의하여 보내진 정보로부터 T의 식별정보를 결정한다.

2. 저가의 RFID 제한 사항

RFID 태그는 크게 자체 배터리를 내장하고 있는 능동형 태그(active tag)와 외부로부터 전원을 얻는 수동형 태그(passive tag)로 구분되어진다[9]. 본 논문에서는 향후 일반적인 형태의 RFID 태그가 될 수동형 태그에 관하여 논하고자 한다.

---

† 본 논문 내용의 일부는 한국전자파학회 학회지 5월호 게재 되었음

실용화를 위해 RFID 태그의 가격은 5센트 미만으로 떨어져야만 하는데, 5센트 태그를 위해서는 IC 가격이 2센트를 초과하지 않아야한다[11]. 이러한 요인들은 태그내의 게이트 수를 7.5~15KGate로 제한하고 있으며, 실제로 보안을 위한 게이트의 수는 2.5~5KGate를 넘지 않아야한다[10]. 따라서 RFID 관련 보안문제의 해결방안으로 기존의 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.

3. 보안 문제

RFID 보안 문제는 크게 두 가지로 구분지어 생각해볼 수 있다. 첫째는 태그 내 데이터의 누출이고[7], 두 번째는 임의의 태그 ID를 추적함으로서 일어날 수 있는 불법추적행위이다[8].

예상되는 공격 방법으로 서비스거부 공격(Denial of service attack), 에러유발(fault induction), 전원중단(power interruption), 무선사보타지(wireless sabotage) 등이 있다[11]. 이러한 공격은 공격자들이 RF 신호 채널을 방해하거나 다른 방법으로 태그를 사용할 수 없게 할 수 있다.

다른 유형의 공격으로 공격자의 태그 스프핑 공격(Tag Spoofing)이 있을 수 있다. 즉, 상품의 태그 정보를 이용하여 유인태그를 만들고, 이런 유인태그를 실제제품과 바꾸는 등의 공격이 발생할 수 있다. 비슷한 유형의 공격으로 재생공격(replay attack) 및 공격자 중간 공격(man-in-the-middle attack) 등이 있다[11].

4. 보안 요구 사항

현재 제시되고 있는 보안요구사항들로 다음과 같은 항목들을 고려해 볼 수 있다[8,11].

- 기밀성(Confidentiality)

RFID 태그는 소유자의 개인정보 처리에 절대 관여하지 말아야만 한다. 태그에 저장된 정보는 비인가된 리더기나 태그와 소유자와의 관계를 추적할 수 있는 데이터의 수집이 이루어지지 않아야 한다.

- 익명성(Anonymity)

RFID 태그가 암호화되는 경우에도 태그의 고유한 식별정보는 존재한다. 태그의 식별정보를 통해 공격자가 태그를 식별할 수 있는 것이 가능하다. 따라서 태그의 식별정보에 대한 익명성을 보호하는 것이 중요하다.

- 무결성(Integrity)

재 기록이 가능한 태그의 경우, 태그 내부의 기록 자체에 대한 위변조의 위협이 존재한다. 따라서 태그의 정보에 대한 무결성을 확인할 수 있어야 한다.

III. 저가의 RFID 보안 기법

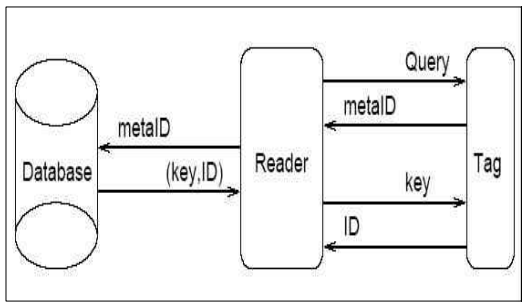
이 절에서는 저가의 RFID 시스템에서 시스템 요구 사항을 만족시키기고 사용자 프라이버시 보호를 위해 제안된 연구 결과들을 집중 조명해 본다.

1. Kill 명령어의 접근법[기법 A]

MIT의 Auto-ID 센터에서 제시한 Kill 명령어 접근법에서는, 각 태그가 8비트의 고유한 패스워드를 갖고 있으며, 자신의 패스워드를 받을 경우 태그는 스스로 기능을 정지시킨다[5]. 그러나 이 방법은 Kill 명령이 제대로 완료되었는지 확인하기 어렵다는 점, 응용 방법이 제한된다는 점 등의 문제들을 가지고 있다. 또한 패스워드가 8비트이므로, 공격자가 2^8의 계산 안에 정확한 패스워드를 결정할 수 있다는 결점을 가지고 있다.

2. 해쉬-락 프로토콜[기법 B]

2003년 S. Weis등에 의하여 제안된 이 기법에서는 단지 한번의 해쉬 함수만을 사용하기 때문에 저가로 구현될 수 있다[12]. 이 기법에서 리더는 각각의 태그에 대한 키 k를 가지고 있고, 각각의 태그는 키에 대한 해쉬 값 $metaID = h(k)$를 갖는다. <그림 2>에서처럼 태그가 리더로부터 접근 요청을 받으면 응답으로 $metaID$ 값을 보낸다. 리더는 태그로부터

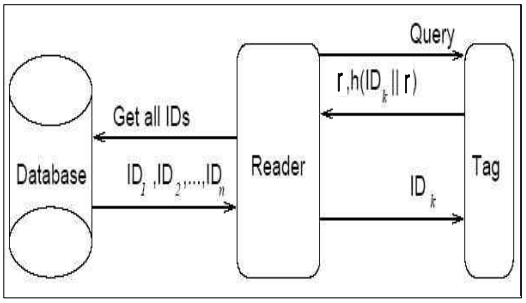


<그림 2> 해쉬-락 기법

받은 $metaID$ 와 관계된 키 k를 태그에게 보낸다. 이때, 태그는 리더로부터 받은 키에 대한 해쉬 값을 계산하고 그 값이 자신이 가지고 있는 $metaID$ 값과 같은지를 판단 한다. 두 값이 일치할 경우에만, 태그는 그 자신의 ID를 리더에게 보낸다. 비록 이 기법은 저가로 구현될 수 있는 장점을 가지고 있지만, $metaID$ 값이 항상 일정하기 때문에, 공격자가 임의의 태그를 추적할 수 있는 단점을 가지고 있다.

3. 확장된 해쉬-락 프로토콜[기법 C]

이 방법은 위에 설명한 해쉬-락 기법의 확장이다[12]. 태그는 해쉬 함수와 의사난수 생성기를 갖는다. <그림 3>에서처럼 각 태그는 해쉬 함수에서 생성된 의사 난수와 자신의 ID를 입력 값으로 하여 $c = hash(ID \| r)$을 계산한다. 태그는 c와 r을 리더에 전달한다. 리더는 이 값을 백-앤드 서버에게 전달



<그림 3> 해쉬-락 기법의 확장

한다. 서버는 자신이 저장하고 있는 모든 태그의 식별정보 ID_t와 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 태그 내에 저가의 해쉬 함수와 의사-난수 생성기의 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. XOR 기반 일회용패드 기법[기법 D]

이 기법은 단지 XOR 연산만을 요구하며, 매우 저렴한 비용을 요구한다[1]. 리더(실제로 백-앤드 서버) B와 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 필요가 있다. 이런 문제가 구현 및 효율성에 어려움으로 남아 있다.

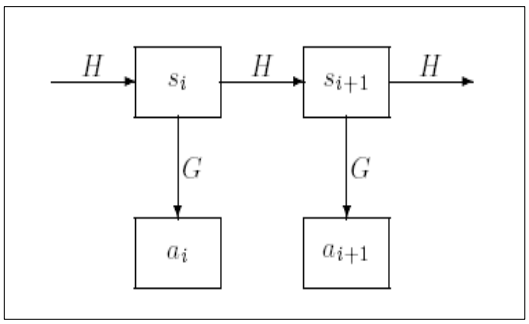
5. 외부 재 암호화 기법[기법 E]

외부 재 암호화(External re-encryption scheme) 기법 에서는 공개키 암호를 사용한다[3]. 태그 데이터는 외부 유닛으로부터 전달된 데이터를 사용자가 사용을 요청할 때 재 기록 된다. 이 외부 유닛은 공개키 암호화가 많은 연산 량을 요구하기 때문에 태그만으로는 연산 처리가 어려우며, 이 작업은 대체로 리더에 의해 수행된다. 태그의 결과 값은 각각 재 기록 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.

6. 해쉬체인 기반 기법[기법 F]

가장 최근에 M. Ohkubo 등은 RFID 시스템에 적용 가능한 전방향 안전성(forward secure)을 제공하는 해쉬 체인 기법을 소개하였다[8]. 이 기법에서 초기상태의 태그는 초기 비밀 값 s_1을 가지고 있다고 가정한다. 프로토콜의 주요 아이디어는 <그림 4>와 같이 태그의 이전 응답 메시지와 이후 응답 메시지 간에 관계를 공격자로 하여금 추측할 수없게 하는 것이다. i-번째 통신에서, 태그는 리더의 요청신호에 대한 응답으로 $a_i = G(s_i)$값을 리더에게 보내고 이전의 자신의 비밀 값 s_i를 $s_{i+1} = H(s_i)$로 갱신한다.



<그림 4> 해쉬 체인 기반 기법

이때, 함수 G와 H는 해쉬 함수이다.

전체적인 RFID 시스템 프로토콜은 다음과 같다.

▪ 구조 : m을 태그의 수라하고, 각각의 태그를 T_t $(t=1, \cdots, m)$이라 하자. 서버 B는 각각의 태그 T_t에 대한 랜덤 비밀 값 $s_{t,1}$을 발생시키고 태그 T_t의 메모리에 초기 비밀 값 $s_{t,1}$을 저장한 후 데이터베이스에 태그 T_t에 대한 식별정보 $ID_t = (id_t, s_{t,1})$를 저장한다.

▪ 태그 : i-번째 통신에서 태그 T_t는 리더의 요청신호에 대한 응답으로 $a_{t,i} = G(s_{t,i})$ 값을 리더에게 보내고 이전의 자신의 비밀 값 $s_{t,i}$를 $s_{t,i+1} = H(s_{t,i})$로 갱신한다.

▪ 리더 : i-번째 통신에서 리더 R은 태그 T_t로부터 $a_{t,i}$값을 받은 후 안전한 채널을 통하여 백-앤드 서버 B에게 $a_{t,i}$값을 보내고 안전한 채널을 통하여 백-앤드 서버 B로부터 태그 T_t의 식별정보 id_t값을 받는다.

▪ 백-앤드 서버 : 백-앤드 서버 B는 모든 태그의 식별정보 값 $ID_t = (id_t, s_{t,1})$을 관리한다. 서버 B는 안전한 채널을 통하여 리더 R로부터 $a_{t,i}$값을 전달 받는다. B는 데이터베이스에 저장되어있는 모든 $s_{t,1}$ $(t = 1, \cdots, m)$와 모든 i $(1 \le i \le n)$에

대하여 $a_{t,i} = G(H^{i-1}(s_{t,1}))$를 체크함으로서 $a_{t,i}$에 대응하는 id_t값을 찾은 후 안전한 채널을 통하여 리더 R에게 id_t값을 보낸다.

이 기법은 리더의 요청에 대한 태그의 응답 값이 매번 다르기 때문에 추적 문제를 해결할 수 있다고 주장 되어진다[8]. 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 B가 많은 계산량을 감수해야만 하는 단점을 가지고 있으며 태그 내에 두개의 서로 다른 해쉬 함수를 구현해야 하는 것도 부담이다.

7. 블러커 태그 방법[기법 G]

이 방안에서는 블러커 태그(Blocker Tag)라는 별도의 태그를 보호하고자 하는 태그에 용도별로 부착하는 형태이다[4]. 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 [11]에서 제시된 RFID 태그의 응답에 대한 충돌 회피 기법으로 제안된 이진트리를 이용한 2진 트리 프로토콜을 이용하고 있다. 이 방법의 또 다른 장점은 블러커 태그 방안이 임의의 공격에 대응해 보호받을 태그의 범위를 이진트리의 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 한다.

IV. 보안 기법의 비교 분석

본 절에서는 지금까지 제시한 각 방식별 암호학적 특성과 장단점을 [표 1] 과 같이 비교 분석한다.

Kill 명령어에 의한 접근법은 방식 자체가 간단하기 때문에 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 RFID태그에 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 이루어져야한다는 결점과 외부 유닛을 가져야한다는 결점 때문에 비현실적이다. 해쉬 체인 기법은 기본적인 RFID시스템의 보안 요구사항들을 만족하는 것으로 주장 되고 있으나, 그에 대한 검증이 아직 이루어지지 않았으며, 저가의 해쉬 함수의 구현방안이 해결되어야할 연구과제로 남아있다. 마지막으로 블러커 태그를 방법은 서비스거부공격(Denial-of-service)의 위협이 거론 되어지고 있으나 큰 위협으로 평가되고 있지 않으며, 방식 자체가 매우 간단하여 추가 구현이 필요치 않다는 점에서 기존의 응용분야의 적용에 현실성이 있는 방식으로 고려된다.

V. 결론

RFID의 정보보호에 대한 핵심 연구 주제 중 하나는 낮은 비용으로 암호화 프로세스가 가능한 RFID를 개발하고 구현하는 것이다. 여기에는 해쉬 함수,

[표 1] 보안 기법별 비교 분석

(기준 : ○-만족 , △-일부만족, ×-만족않음)

보안방식	보안요구도의 충족도			태그 연산	장점	단점
	태그 보호	트래킹 보호	전방위 안전성			
기법 A	△	○	△	×	구현용이	짧은 패스워드에 대한 공격의 위험성 존재 명령의 완료 검증 문제
기법 B	○	×	×	해쉬	구현용이	추적가능 태그의 위조가능
기법 C	○	○	×	해쉬, 난수발생	보안요구사항 만족	난수발생기의 구현 필요, 백-앤드 서버의 계산 로드
기법 D	○	○	×	XOR	가장 적은 계산량 요구	인증을 위하여 너무 많은 통신을 필요, 공통 목록의 재 기록 필요
기법 E	○	○	○	×	이론적으로 가장 안전	외부 유닛 필요, 비현실적
기법 F	○	○	○	해쉬	저가의 연산으로 보안 요구사항 만족	안전성 검증 미비, 저가의 해쉬함수 구현연구 필요
기법 G	○	○	○	×	추가 구현이 불필요	별도 태그의 부착을 필요로 함

난수 생성기 그리고 대칭키 암호, 비대칭키 암호(공개키 암호) 등의 경량화 연구가 포함된다.

낮은 비용의 하드웨어 구현을 위해 반드시 회로 부분을 최소화하여 비용을 낮추고, 공격자가 전력의 소비 시간을 예측할 수 없게 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 연산 량을 줄이는 방법, 초경량 해쉬 함수의 구현 문제들이 더욱 연구되어야만 한다. 또한, 재 기록이 가능한 태그(rewritable tag)에 대한 무결성 보장 등도 연구 주제로 진행되고 있다. 나아가 향후 USN(Ubiquitous Sensor Network) 환경에서 RFID의 다양한 활용에 따라서 발생할 보안 문제에 대한 선행 연구도 활발히 시도되고 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.

[참고문헌]

[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, 200

[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, "860MHz-960MHz 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] K. Romer, T. Schoch, F. Mattern, and T. Dubendorfer, "Smart Identification Frameworks for Ubiquitous Computing Applications"

[7] R.L. Rivest, "Approaches to RFID Privacy", RSA Japan Conference 2003

[8] 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, 2003 Oct. (in Japanese)

[9] S. Sarma, S. Weis, and D. Engels, "RFID Systems, Security & Privacy Implications", Auto-ID Center

[10] S. Sarma, S. Weis, and D. Engels, "Radio-Frequency Identification: Security Risks and Challenges" , CryptoBytes, 2003

[11] S. Weis, "Security and Privacy in Radio-Frequency Identification Devices", Master's thesis, MIT. 2003

[12] 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

[13] 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