취약성 분석을 통한 경량 RFID 인증 프로토콜 고찰

곽민혜*, 김광조*

*한국정보통신대학교, 국제정보보호기술연구소

A Study on Lightweight Authentication Scheme for Low-Cost Tags through the Cryptanlaysis

Min-Hea Kwak*, Kwangjo Kim*

*International Research Center for information security(IRIS),

Information and Communications University (ICU)

요 약

저가형 태그가 대중화되면서 태그의 가용 저장공간과 연산능력을 고려하는 한편 외부 공격에 대응할 수 있는 경량 인증기법의 필요성이 증대되고 있다. 제안된 경량 인증 기법은 대부분 난수생성과 AND, OR같은 비트연산에 기반한 매우 효율적인 기법임은 틀림없지만 도청에 의한 태그 정보 누출 및 비동기화 오류등 능동적 공격뿐만 아니라 수동적 공격에도 취약하다. 본 논문에서는 기 제안된 RFID 인증프로토콜을 사용한 암호학적 기법 및 전자태그의 연산능력을 기준으로 중량, 단순, 경량과 초경량 인증 방식등 네가지로 분류하고 제시된 기법들의 장단점과 가능한 공격 기법을 통해 제안된 경량 인증기법을 한계점을 살펴보는 한편 보완 방향을 모색한다

I. 서론

무선 주파수를 이용하여 물리적 접촉없이 정보를 저장하거나 읽은 무선 인식기술인 RFID (Radio Frequency IDentification, 전자태그)는 반도체 기술의 발전과 인터넷의 등장으로 인하여 지난 10여년 동안 꾸준한 발전을 해왔으며 유통, 물류, 의료, 교육등 다양한 분야에 적용되고 있다. 그러나 RFID 시스템에서의 태그와 리더는 주파수 통신을 하기 때문에 태그의 정보가 노출되기 쉽고 이는 공격자의 기본정보로 활용되어 사생활 침해 및 보안 위협을 가할 수 있어 RFID 대중화의 걸림돌이 되고 있다. 기업 입장에서는, 산업 스파이가 취약한 전자태그의 정보의 불법적으로 수집, 위장 태그를 통해 잘못된 정보를 제공하고나 DoS 공격(Deinal of Service, 서비스 거부)를 시도할 우려가 있다. 개인 입장에서는, 대부분의 고객들은 자신의 정보가 외부에 노출되길 원치 않지만 전자태그가 부착된 상품을 구매하면서 태그의 위치를 추적당하거나 심지어 누가 특정 브랜드의 상품을 가지고 있는지 식별될 수 있는 위험성도 있다. 따라서 RFID 시스템에서 사생활 보호, 접근통제, 인증, 익명성, 데이터 복구등의 보안 요구사항을 만족하는 것은 필수적인 사항이다.

그러나 저가의 태그는 보통 5K~10K의 논리게이트와 250~3K의 보안 함수를 실행할 수 있는데 제한적인 연산능력과 저장공간의 한계로 인해 대칭키, 공개키같은 전통적 암호기법의 사용이 힘들다. 이러한 저가형 전자태그를 위한 자원의 소모가 적은 안전한 암호 기법과 최소한의 자원을 사용하면서도 안전한 인증 기법의 개발은 필수적이다.

지금까지 이러한 안전성 문제를 해결하기위하여 태그, 리더, 데이터베이스 서버간의 인증을 통한 정보제공에 대한 연구가 진행되고 있다[1][2][3][4].

본 논문에서는 현재까지 제안된 인증기법을 적용할 수 있는 전자태그의 연산능력과 저장공간에 따라 4가지로 분류하였다. 공개키 알고리즘과 일방향 해쉬함수가 적용가능한 중량 인증

방식, 난수 생성기와 일방향 함수를 사용한 단순 방식, 난수 생성기와 CRC(Cyclic Redundancy Code, 순환중복검사)같은 간단한 함수를 사용하는 경량 인증 방식, XOR, AND, OR같은 비트연산만 사용하는 초경량 인증방식으로 분류하고 있다.

본 논문에서는 현재까지 제안된 경량 인증 및 초경량 인증기법의 장단점을 분석하고 가능한 공격 기법을 통해 제안된 경량 인증기법을 한계점을 살펴보는 한편 보완 방향을 모색한다.

II. 본론

1.1 제안된 경량 인증기법

본 논문에서는 현재까지 제안된 RFID 인증기법을 네 가지로 분류하였다.

첫째, 중량 인증 방식은 해쉬함수, 암호화, 공개키 알고리즘등 전통적 암호기법을 사용하는 프로토콜로 [3,4,5]가 이와 같은 범주에 속한다.

둘째, 단순 인증 방식은 난수 생성기와 일방향 해쉬함수를 사용하는 프로토콜로 [6-14]와 같은 함수가 이에 속한다. 현재까지 제안된 저가 전자태그의 보안 요구사항과 프라이버시 보호를 위한 경량 인증 프로토콜은 대부분은 해쉬함수를 사용하는 기법들이다. 그러나 해쉬함수는 저가 태그의 하드웨어에 효율적으로 적용될 수 있지만 현재의 태그 능력에는 적합하지 않아 경량 인증 기법으로 분류하기 힘들다. EPC global 또한 Class-1 Gen-2 RFID는 MD5나 SHA-1같은 해쉬함수를 쓸 수 없다고 명시하고 있다. Chien[6]은 Weis등의[10-14] 취약점인 비밀키 누출 문제와 익명성 위반등의 문제를 연구하였고, Avoine등[15]은 Ohkubo[9]와 [8-10,13,14]등의 취약점을 밝혔다.

셋째, 경량 인증 방식은 EPC class-1 Gen-2가 PRNG(Pseudo-Random Number Generator, 의사난수생성기)와 CRC(Cyclic Redundancy Check, 순환 중복 검사)만 지원하기 때문에 해쉬함수를 사용하지 않고 난수생성과 CRC만 사용하는 프로토콜을 말한다. [16-18]등의 기법이 이에 속하며, [17]는 프라이버시 문제와 도청을 고려하지 않았고, Chien과 Chen[19]은 [16,18]의 DoS 공격, 재전송 공격, 위치추적, 위장등의 문제를 지적한바있다. HB 시리즈 프로토콜[20-25]은 Hopper와 Blum[22]이 LPN(Learning Parity with Noise) 문제에 기반하여 해쉬함수를 배제하고 가명을 사용한 기법이다. 초기 HB 프로토콜은 수동적 공격을 방어하는데 그쳤으나 [20,21,23-25]에서는 능동적 공격까지 고려하는 진보된 형태의 HB 시리즈 프로토콜이 등장하였다. 근본적으로 HB 시리즈는 태그 인증만을 고려하고 리더 인증, 위치 추적, 익명성 및 태그 식별 문제는 고려하지 않는 약점이 있다.

넷째, 초경량 인증 방식은 XOR, AND같은 간단한 비트연산만을 적용하는 부류이다. Peris-Lopez는[26-28]에서 XOR, AND, OR, 법2에 대한 덧셈같은 단순 연산만 하는 프로토콜을 제안하였는데 이는 300gate정도의 연산능력을 필요로 하는 매우 효율적인 기법이지만 비동기화 및 태그 완전 노출의 약점이 있다. EMAP, MMAP. LMAP등은 [18,19,26-28]에서 저강도의 인증 및 무결성만 보장하고 있다.

Juels은 [29]에서 저가형 태그에 적합한 질의-응답형 경량 보안 모델을 제시했는데 해쉬함수 및 전통적 암호 기법들을 배제한 가명(pseudonym)을 사용하는 기법이다. 태그는 임의의 식별자나 가명의 짧은 목록을 저장하고, 태그가 질의를 받으면 목록의 다음 가명을 전송하는 방식을 취하는데, 불분명한 카운터 증가를 사용하는 대신에 사전에 정해진 d개의 출력값 $f_{k_i}[z], f_{k_i}[z+1], \ldots, f_{k_i}[z+d-1]$의 수열을 반복해서 전송한다. 리더와의 상호인증이 성공적일 경우, 태그는 d개의 출력값 중 다음 값으로 넘어간다. 리더가 모든 태그를 인증하기 위해서는 $O(dn)$개의 동적 검색 테이블을 유지해야 한다. 리더와의 상호인증이 성공적일 경우, 태그는 짧은 가명 목록을 저장하고 리더의 질의에 대한 응답으로 리스트의 난수를 전송한다. 원칙적으로 동일한 태그에 두 개 이상의 다른 식별자가 있을 때 정당한 리더만이 통신을 할 수 있다. 물론 공격자는 보안 프로토콜을 무력화 시키고 모든 태그 정보를 획득하기 위해 수

차례 질의를 할 수 있다. 이러한 공격을 막기 위해 몇 가지 대응책을 제시하고 있는데 첫째, 태그는 사전에 규정된 비율로 태그의 식별자를 발급한다. 둘째, 가명는 검증된 리더에 의해서만 생성할 수 있다. 태그측에서는 XOR와 AND 연산외에는 암호학적 연산을 수행하지 않도록 규정하고 있음에도 불구하고 제안된 프로토콜은 연산량이 요구되는 네 개의 메시지 생성과 비밀키 업데이트를 필요로 하는데 이는 비현실적이다. 일정 횟수의 인증 세션 후, 난수 리스트는 대역외 채널을 통해 업데이트되거나 재사용되어야 하는데 이것의 현실적 가능성도 문제이다.

Juels[30]은 [29]의 보완된 형태로 정상적인 태그를 복제해 위장하는 공격을 방지하기 위해 제안하였다. EPC class-1 Gen-2 태그의 읽기 방지 32bit Kill 명령어가 태그인증 프로토콜에 사용된다. 이 프로토콜은 태그의 EPC는 검색되더라도 kill 명령어의 보안은 유지된다는 사실에 기반한다. 그러나 만약 Kill 명령어가 DB에 저장된 진짜 암호를 맞춘다면, 복제 태그는 태그 정지 없이도 테스트에 의해서 발견될 수 있다. 또한 제안된 프로토콜은 도청 및 사생활 침해를 고려하지지 않아서 비밀정보 누출에 대응할 수 없다.

Karthikeyan와 Nesterenko[31]는 XOR연산과 행열연산에 기반한 프로토콜로 Gen-2 태그를 위한 효율적인 태그 식별 및 리더 인증기법이다. 초기 두 개의 크기 $p\times p$인 정방행열 M_1과 M_2^{-1}은 각 태그에 저장되고, 태그와 리더는 크기 $q=rp$의 벡터인 키 $K=[K_1,K_2,...,K_r]$, $p\ni\{i=1,2,...,r\}$를 저장한다. $X=KM$는 크기 q의 벡터의 행렬 K와 $p\times p$의 행열 M의 행열곱의 결과이다. 태그는 $X=KM_1$을 계산하여 리더측에 X를 되돌려준다. 리더는 다시 서버측으로 재전송해 서버측의 DB에서 검색을 하고, 만약 DB에서 검색이 되면 정당한 태그로 식별되어 서버는 태그를 인증하기 위한 연산과 키 업데이트를 수행한다. 그러나 키 업데이트 과정에서 태그가 수신한 값 Z를 인증하지 않은 상태에서 공격자가 전송된 Z값을 예전 Z' 또는 Z^*로 바꾼다면 정당한 값 Y와 변조된 값 Z^*를 수신함으로써 태그는 Y를 정상적으로 인증하게 되고 키는 $K^*=M_1Z^*$로 업데이트하게 된다. 그러나 키가 잘못 업데이트 되었기 때문에 정당한 리더와 태그는 더 이상의 인증과정을 수행할 수 없고 DoS 공격에 노출되게 된다. 위의 공격 형태에서 만약 공격자가 Z를 예전 Z'로 바꾼다면 태그를 속이기 위해 다음번 세션에서 또 다른 예전 값 Y'를 재전송하여 잘못된 요청을 수락하고 태그에 접근을 허락할 수 있다. 심지어는 수차례의 세션의 도청을 통해 전송된 데이터를 저장하여 위와 같은 공격을 수차례 실시할 수 도 있다. 이는 태그의 위치 추적뿐만 아니라 익명성까지도 손상이 될 것이다.

Weis[32]는 저비용 RFID 시스템에서 사용할 수 있는 Hopper와 Blum의 연구에 기반한 human-컴퓨터 인증 프로토콜의 개념을 소개했다. 이 기법은 Weis와 Juels에 의해 확장되어 HB+[23]라는 경량 대칭키 인증 프로토콜로 발전되었다. 두 프로토콜 HB와 HB+의 안정성은 통계적인 LPN(Learnign Parity with Nosie)문제에 기반한다. HB+를 구현하기 위해서는 비트단위 AND와 XOR연산과 난수 "noise bit"이 필요하다. HB+에 대한 능동적 공격에 대한 보안 취약점을 보완한 HB++[24], HB*등이 제안되었다. 그러나 현재 LPN 문제의 어려움은 미해결 문제로 남아있다. 또한 태그 인증과정만 있고 리더의 인증은 고려하지 않아 위치추적, 익명성, 태그 ID의 보안 문제도 해결해야할 과제이다.

경량 프로토콜의 진보된 형태로 Peris-lopez는 EMAP[33]를 제안하였는데, XOR, AND OR 등의 단순한 비트연산만으로 구성되어 있고 480비트의 EEPROM(Electrically Erasable Programmable Read-Only Memory, 비휘발성 메모리)과 96비트의 ROM(Read Only Memory, 읽기전용 메모리)만 요구하는 매우 효율적인 상호 인증 프로토콜이다. 대부분의 저가태그는 수동형이기 때문에 연산이 많이 필요한 곱셈연산이나 해쉬 함수는 사용하지 않고 난수 생성 조차 리더측에서 수행한다. 태그의 *IDS*

*(I*ndex-pseudonym)는 태그의 모든 정보가 저장되는 테이블의 색인으로서 사용되고 키는 각각 네 부분의 96*bit* 서브키로 이루어져 있으며 *IDS*와 키는 상호 인증 성공 후에 업데이트 된다. EMAP는 상호인증의 형태를 취하고 있지만 리더가 수신한 메시지 $D|E$에 대한 검증절차 없어 성공적으로 수신 되었거나 검증 되었는지 알 수 없고, 수신이 실패했을 경우 *IDS*와 키의 업데이트 또한 비동기화될 우려가 있다. EMAP는 전자태그가 특정 리더에 구속되지 않는다고 가정을 하고 있는데, 즉 프로토콜의 실행상태를 기억하지 않기 때문에 어떤 태그와도 불완전한 프로토콜을 수차례 반복적으로 수행할 수 있게 된다. 하지만 이러한 태그의 비구속성 때문에 태그의 비밀정보가 완전히 노출될 우려가 있다.

MMAP[34]와 LMAP[35]는 거의 유사한 형태의 프로토콜로 MMAP는 LMAP프로토콜에서 응답 메시지 *E*를 추가하였다. 각 태그는 단일한 *ID*와 *IDS*, 비밀키*(K1,K2,K3,K4)*를 가지고 있고 *XOR, OR, AND*의 단순연산만 수행한다. 상호 인증 성공 후에는 *IDS*와 비밀키의 업데이트 과정을 거친다. MMAP의 비트연산에서 모든 비트는 주어진 비트의 왼쪽에 있는 비트에게만 영향을 끼치는데, 각 비트는 동일하거나 큰 색인의 비트에 의존하게 되는것이다. 즉, MMAP가 비트연산과 법 2에 대한 덧셈연산만 수행하는데, 최하위 비트는 다른 비트에 영향을 받지 않고 최하위 비트만 고려했을때 XOR연산은 법 2에 대한 덧셈은 동일한 결과값을 산출한다. 메시지 *B*와 *D*에서 OR과 AND 비트연산에서 공격자는 *IDS*를 재설정할 수 있어 난수 n_1과 n_2의 모든 정보를 쉽게 획득할 수 있다. 우측의 모든 비트를 획득한다면 법 2에 대한 덧셈을 알아내는 것은 어려운 일이 아니다. 따라서 공격자는 몇 번의 연속적인 도청을 통해 태그 *ID*나 비밀키를 획득하고, 더 많은 횟수의 도청을 하면 결국 모든 정보가 누출되고 정당한 태그 또는 리더로의 위장이 가능하다. 또한 LMAP와 MMAP의 태그와 리더간 상호인증은 키와 *IDS*의 동기화후에 이루어져야 하는데, 공격자가 태그의 응답 메시지 *D*를 가로채면 동기화는 쉽게 무너진다.

SASI[36] 또한 비트연산(XOR, OR AND)과 위치교환 함수에 기반한 초경량 인증 프로토콜이다. 태그의 식별자(ID)와 두 개의 키(k_1,k_2)가 태그와 서버에 저장되어 있고 비트연산에 의한 메시지를 생성해 전송하고 검증하는 방식이다. 공격자는 리더의 응답 메시지 *D*를 강제적으로 중단시켜 서버측의 DB업데이트를 방해하는 공격으로 비동기화 오류가 발생시킬 수 있다. 또한 공격자가 메시지 *D*를 탈취해 재전송할 경우 태그의 *IDS*를 획득할 뿐만 아니라 변조 메시지로 인증하게 된다.

1.3 취약점 분석 및 비교

표[1]은 1.2에서 언급한 경량인증 프로토콜의 보완요구사항 비교한 결과이다.

[표 1] 보안성 비교

제안기법	도청	재전송 공격	위치 추적	비동기	DoS	익명성	복제	위장
Juels[29]	X	X	X	·	X	X	·	X
Juels[30]	X	X	X	·	X	O	X	X
Karthikeyan[31]	X	X	X	·	X	X	X	X
HB[22]	X	X	X	·	X	X	O	O
HB+,HB++[23]	X	X	X	·	X	X	O	O
EMAP[33]	X	X	X	X	X	X	X	X
M^{2}AP[[34]	X	X	X	X	X	X	·	·
LMAP[35]	X	X	X	X	X	X	·	·
SASI[36]	X	X	X	X	X	X	·	·

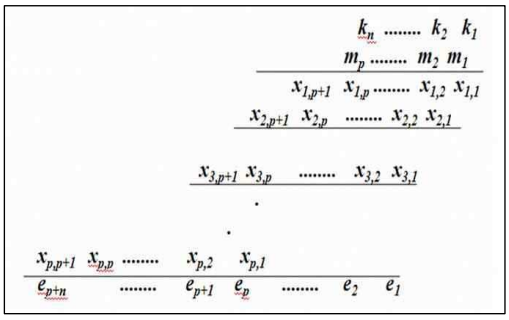
※ X: 취약 , O:안전

1.1 에서 언급한 경량 및 초경량 인증프로토콜은 공통적으로 저가 수동형 태그를 고려하여 설계되었기 때문에 EPC global의 태그 저장공간 및 연산능력등의 요구조건을 만족하는 효율적인 기법들이다. 하지만 EMAP, M^{2}AP류의 초경량 인증기법은 이미[37,38]등에서 전송 메시지의 탈취 및 재전송 공격, 비동기화와 태그 정보 누출등의 공격위협에 노출되었고 보완된 형태의 [36],[39] 또한 이러한 위협에 취약성이 드러났다. [31],[32]등의 경량 인증프로토콜에서도 연속된 도청에 의한 위치추적과 비밀키가 노출되는 약점이 드러났다. 비트연산방식에 기반한 경량 및 초경량 인증 프로토콜은 메시지 생성

및 인증을 위한 검증과정에서 비트연산에 의해 메시지를 생성하는데 이는 연속적인 도청에 의해 식별자 및 키 노출이 불가피하고, 획득한 기본정보는 태그정보의 완전노출 및 태그 복제, 위장등의 공격으로 쓰이는 등 태생적 한계점을 지니고 있다.

1.3 정수연산방식

본 논문에서는 비트연산방식의 대안으로 두 이진 수열의 내부연산을 통한 정수 연산방식을 제시하고 이를 전자태그와 리더간의 인증기법에 적용하고자 한다.



[그림 1] 정수열 내부연산

일반적인 두 정수열의 내부연산 알고리즘은 그림 1의 두 정수열 $k_n \cdots\cdots k_2 k_1$과 $m_n \cdots\cdots m_2 m_1$의 연산결과인 $e_{p+n+1} e_{p+n} \cdots\cdots e_2 e_1$로 표현된다. 10진수 3과 7의 연산을 가정하면, 이진 곱셈 연산자 ⊗:(3,7)→(2,1)로, 이진 덧셈 연산자 ⊕:(3,7)→(1.0)로 표기할 수 있다. 위의 이진 연산을 올림수와 나머지의 쌍으로 표기하면 ⊗:(3,7)→((3⊗7)c,(3⊗7)r)로 표기할 수 있고, 정수열 $k_n \cdots\cdots k_2 k_1$ 과 m_i의 연산결과인 $x_{i,n+1} x_{i,n} \cdots\cdots x_{i,2} x_{i,1}$은 아래와 같이 표기한다.

$x_{i,1} = (k_1 \otimes m_i)_r$

$x_{i,2} = ((k_2 \otimes m_i)_r \oplus (k_1 \otimes m_i)_c)_r$

$x_{i,3} = ((k_3 \otimes m_i)_r \oplus ((k_2 \otimes m_i)_c \oplus ((k_1 \otimes m_i)_r \oplus (k_1 \otimes m_i)_c)_c)_r$

최종 연산결과인 $e_{p+n+1} e_{p+n} \cdots\cdots e_2 e_1$은 중간 연산결과인$x_{i,j}$ 수직 열의 합이다.

Stephane등은 위의 일반적 곱셈연산 알고리즘을 바탕으로 새로운 정수열 연산방식인 Abstraction of Integer Arithmetic(AIA)를 제안하고 아래와 같이 정의하였다.

정의1 (Abstraction of Integer Arithmetic)

임의의 기수 b의 $4b^2$자리수 수열 s는 곱셈, 덧셈의 올림수와 나머지를 고려한 곱셈 알고리즘을 이용하여 기수 b의 수열 전체 집합 B에 대하여 이진연산 $\times_s$을 정의한다.

이진 덧셈 및 곱셈 연산에서 올림수와 나머지 집합은 표 또는 수열로 표현할 수 있는데 표 2는 기수 3일때의 AIA 샘플이다. AIA는 하드웨어 형태도 태그와 리더에 저장되어 상호인증과정에서 메시지 교환 및 업데이트시 적용한다. AIA는 각 태그별 하드웨어형태로 구현되기 때문에 태그복제 및 키 탈취가 어려운 장점이 있어 저가태그에 효율적으로 적용가능하다.

⊕, 덧셈, 기수3

a	b	올림수	나머지
0	0	0	0
0	1	0	1
0	2	0	2
1	0	0	1
1	1	0	2
1	2	1	0
2	0	0	2
2	1	1	0
2	2	1	1

⊗, 곱셈, 기수3

a	b	올림수	나머지
0	0	0	0
0	1	0	0
0	2	0	0
1	0	0	0
1	1	0	1
1	2	0	2
2	0	0	0
2	1	0	2
2	2	1	1

[그림 2] 기수 3일때 AIA 샘플

III. 결론 및 향후계획

본 논문에서는 기 제안된 RFID 인증프로토콜을 사용한 암호학적 기법 및 전자태그의 연산능력을 기준으로 중량, 단순, 경량과 초경량 인증 방식등 네가지로 분류하고 제시된 기법들의 장단점과 가능한 공격을 소개하였다. 대부분의 경량형 인증 프로토콜의 기반은 비트연산방식은 수차례의 도청을 거치면 태그의 식별자 및 비밀키등이 노출되는 치명적 단점을 가지고 있다. 따라서 비트연산방식을 대체하면서 저가 태그의 연산능력을 고려한 효율적인 인증 프로토콜에 대한 연구가 절실한데 정수연산방식(AIA)은 하나의 대안이 될 것으로 기대한다.

[참고문헌]

[1] EPC global http://www.epcglobalinc.org

[2] ISO국제표준기구 http://www.iso.org

[3] A. Juels, D. Molner, and D. Wagner, "Security and Privacy Issues in E-passports", *RSA laboratoreis, and UC-Berkeley*

[4] A. Juels and S. A. Weis, "Authenticating pervasive devices with human protocols", in *Advances in Cryptogloy-Crypto '05*, LNCS 3126, pp.293-308, springer, 2005

[5] S. S. Kumar and C. Paar, "Are standards compliant Elliptic Curve Cryptosystems Feasible on RFID?", in P*roceedings of Workshop on RFID security*, Austria, July 2006

[6] H. Y. Chien,"Secure Access Control Schemes for RFID systems with Anonymity", in *Proceedings of 2006 national Workshop on Future Mobile and Ubiquitous Information Technologies (FMUIT'06)*, May, Japan.

[7] A. D. Henrici and P. Mauller, "Hash based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", i*n the Proceedings of PerSec'04 at IEEE PerCom*, pp.149-153, 2004.

[8] D. Molnar and D. Wagner, "Privacy and security in library RFID:Issues, practices, and architectures", in C*onference on Computer and Communications Security* -CCS'04, pp. 210 AN219, 2004.

[9] M. Ohkubo, K. Suzki and S. Kinoshita, "Cryptographic Approach to 'Privacy-Triendly' Tags", i*n RFID Privacy Workshop, 2003.*

[10] K. Rhee, J. Kwak, S. Kim, and D.Won, "Challenge-response based RFID authentication protocl for distributed database environment", in *International Conference on Security in Pervasive Computing - SPC 2005*, pp. 70 NE84, 2005.

[11] S. A. Weis, "Security and Privacy in Radio-Frenquency Identification Devices", *Masters Thesis MIT, 2003.*

[12] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspect of Low-Cost Radio Frequency Identification Systems", i*n the Proceedings of the First Security in Pervasive Computing*, LNCS2802, pp.201-212, Springer, 2003.

[13] J. Yang, J. Park, H. Lee, K. Ren, and K. Kim,"Mutual authentication protocol for low-cost RFID", *Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, 2005.*

[14] J. Yang, K. Ren and K. Kim, "Security and Privacy on authentication protocol for low-cost radio", in *The 2005 Symposium on Cryptography and Information Security, 2005.*

[15] G. Avoine, E. Dysli, and P. Oechslin, "Reducing time complexity in RFID systems," in *The 12th Annual Workshop on Selected Areas in Cryptography(SAC),* 2005.

[16] D. N. Duc, J. Park, H. Lee and K. Kim, "Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning", in *The 2006 Symposium onCryptography and Information Security, 2006*

[17] A. Juels, "Strengthening EPC Tag against Cloning", in *ACM Workshop on Wireless Security (WiSe), pp.67-76. 2005.*

[18] S. Karthikeyan, and M. Nesterenko,"RFID security without extensive cryptography", in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pp. 63-67, 2005.

[19] H.-Y. Chien, and C.-H. Chen, "Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards", in *Computers Standards & Interfaces* 29(2), pp 254-259, 2007.

[20] J. Bringer, H. Chabanne, and E. Dottax, "HB++: A Lightweight Authentication Protocol Secure against Some Attacks", in *Proc. IEEE Int' Conf. Pervasive Service, Workshop Security, Privacy and Trust in Pervasive and Ubiquitous Computing,* 2006.

[21] H. Gilbert, M. Robshaw, and H. Sibert, "n Active Attack against HB+-A Provably Secure Lightweight Authentication Protocol", in *Cryptology ePrint Archive*, Report 2005/237, 2005.

[22] N. J. Hopper and M. Blum, "Secure Human Identification Protocols," in *Proc. Seventh Int' Conf. Theory and Application of Cryptology and Information Security*, pp. 52-66, 2001.

[23] A. Juels and S.A. Weis, "Authenticating Pervasive Devices with Human Protocols," in *Proc. 25th Ann. Int' Cryptology Conf. (CRYPTO '05)*, pp. 293-308, 2005.

[24] J. Munilla and A. Peinado, "HB-MP: A further step in the HB-family of lightweight authentication protocols", *Computer Networks*, 51(9):2262 - -2267, June 2007.

[25] S. Piramuthu, "HB and Related lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication", in *Proceeding. CollECTeR Europe Conference*, June 2006.

[26] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A.Ribagorda, "LMAP: A Real Lightweight Mutual Authentication Protocol for Low-Cost RFID Tags," *Proc. Second Workshop RFID Security*, July 2006.

[27] P. Peris-Lopez, J. C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags", *Proc. OTM Federated Conf. and Workshop: IS Workshop*, Nov. 2006.

[28] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "M2AP: A Minimalist mutual-Authentication Protocol for Low-Cost RFID Tags", *Proc. Int' Conf. Ubiquitous Intelligence and Computing (UIC '06)*, pp. 912-923 2006.

[29] A. Juels, ""Minimalist cryptography for low-cost RFID tags,"" in *Proc.4th Int. Conf. Security Commun. Netw.*, C. Blundo and S. Cimato, Eds. New York: Springer-Verlag, 2004, vol. 3352, Lecture Notes in Computer Science, pp. 149 - -164.

[30] A. Juels, "Strengthening EPC Tag against Cloning", in *Proc. ACM Workshop Wireless Security (WiSe '05)*, pp. 67-76, 2005.

[31] S. Karthikeyan and M. Nesterenko, "RFID security without extensive cryptography", in *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks* (2005), pp. 63 - 67.

[32] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels. "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", In *security in Pervasive Comp.*, volume 2802 of LNCS, pasges 201-212, 2004

[33] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags,"" Proc. OTM Federated Conf. and Workshop: IS Workshop,Nov. 2006.

[34] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A.

Ribagorda, "LMAP: A Real Lightweight Mutual Authentication Protocol for Low-Cost RFID Tags", in *Proc. Second Workshop RFID Security*, July 2006.

[35] P. Peris-Lopez, J. C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "M2AP: A Minimalist Autual -Authentication Protocol for Low-Cost RFID Tags", in *Proc. Int'l Conf. Ubiquitous Intelligence and Computing* (UIC'06), pp. 912-923 2006.

[36] H.-Y. Chien. "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity". *IEEE Transactions on Dependable and Secure Computing* 4(4):337 - -340. Oct.-Dec. 2007.

[37] T. Li and R.H. Deng, "Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol", in P*roc. Second International Conference, Availability, Reliability, and Security (AReS '*07), 2007.

[38] T. Li and G. Wang, "Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols", in *Proc. 22nd IFIP TC-11 International Information Security Conference*, May 2007.