情報保護學會論文誌
第20卷 第4號, 2010. 8

UHF 수동형 RFID 시스템에 적합한 경량 고속의 보안 프로토콜 설계 및 구현*

강 유 성,[1†] 최 용 제[1], 최 두 호[1], 이 상 연[1], 이 형 섭[1]
[1]한국전자통신연구원

Design Implementation of Lightweight and High Speed Security Protocol Suitable for UHF Passive RFID Systems*

You Sung Kang,[1†] Yong Je Choi[1], Doo Ho Choi[1], Sang Yeoun Lee[1], Heyung Sup Lee[1]
[1]ETRI

요 약

제품의 아이디를 자동적으로 신속하게 인식하기 위한 기술로 주목받았던 수동형 RFID 태그가 직면한 문제는 가격, 인식률뿐만 아니라 최근에는 인증, 데이터 보호 및 제품추적 문제로 확대되고 있다. 대표적인 수동형 RFID 기술은 900 MHz UHF 대역의 국제표준인 ISO/IEC 18000-6 타입 C 기술이다. 이 국제표준은 보안 해결책을 제시하지 않았기 때문에 진품 확인, 태그의 저장정보 보호 및 추적 차단 서비스에 활용하기 어려운 단점이 있다. 본 논문에서는 인증, 데이터 보호 및 제품추적 문제 해결을 위한 ISO/IEC JTC 1/SC 31의 국제표준화 동향을 살펴보고, 국제표준에서 요구하는 암호 엔진을 사용하는 높은 수준의 보안성을 만족하는 UHF 대역의 수동형 RFID 보안 프로토콜을 제안하고 그에 대한 보안성을 분석한다. 또한 국제표준 문서에 적용될 수 있는 수준의 명령/응답 구조와 암복호화 방법을 제시함으로써 그 구현 가능성을 검증한다.

ABSTRACT

A passive RFID tag which received attention as a future technology for automatic and quick identification faces some difficulties about security problems such as tag authentication, reader authentication, data protection, and untraceability in addition to cost and reliable identification. A representative passive RFID technology is the ISO/IEC 18000-6 Type C which is an international standard for 900 MHz UHF-band. This standard has some difficulties in applying to the security services such as originality verification, tag's internal information protection, and untraceability, because it does not provide high-level security solution. In this paper, we summarize security requirements of ISO/IEC JTC 1/SC 31 international standardization group, propose security protocols suitable for the UHF-band passive RFID system using a crypto engine, and analyze its security strength. In addition, we verify that it is possible to implement a tag conforming with the proposed security protocols by presenting concrete command/response pairs and cryptographic method.

Keywords: RFID security, RFID security protocol, ISO/IEC 29167-6, RFID authentication.

* 접수일(2010년 4월 30일), 수정일(2010년 6월 4일), 게재확정일(2010년 8월 1일)
* 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업의 일환으로 수행하였음. [초경량 저전력 RFID 보안플랫폼 기술 개발]. 본 연구결과의 일부 내용은 국내표준 TTAK.KO-12.0091/R1에 공개되었음.
† 주저자, 교신저자, youskang@etri.re.kr

I. 서 론

제품의 아이디를 자동적으로 신속하게 인식하기 위한 대표적인 기술은 현재까지도 바코드가 담당하고 있다. 바코드를 대체하면서 기업과 사용자에게 보다 안전하고 효율적인 활용을 제공할 수 있는 기술은 저가의 수동형 RFID 기술이 대표적이다. 수십 cm 이내의 인식 거리를 가진 기존 13.56 MHz 대역의 HF 기술과 달리, ISO/IEC 18000-6 타입 C 표준은 인식 거리 수 m급의 900 MHz UHF 대역 수동형 RFID 기술을 정의하고 있으며 가장 상용화에 근접한 구현 제품이 등장해 있는 기술이다.[1]

UHF 수동형 RFID 기술의 저변 확대를 가로막는 장애물은 가격, 인식률과 더불어 태그/리더 인증, RFID 데이터 보호 및 제품 아이디 노출에 따른 제품 추적 문제가 대두되고 있다. 현재의 국제표준을 준수하는 UHF 수동형 RFID 태그는 수 m 이내의 리더의 요청에 대해 아무런 인증 절차 없이 자신의 아이디 정보를 평문으로 응답해야만 한다. 또한 제공되는 아이디 역시 표준화되어 있는 구조라서 어느 회사의 어느 제품인지를 쉽게 분석할 수 있다.[1-4] 동일한 값의 아이디 노출은 추적의 문제점도 안고 있다.

이러한 보안 문제점을 해결하기 위한 매우 다양한 연구결과들이 지난 5-6년 동안 전 세계적으로 쏟아져 나왔다. 대표적인 RFID 보안 전문가로 꼽히는 Ari Juels가 2006년 IEEE Journal on selected areas in communications에 초청논문으로 발표한 논문[5]에 따르면 저가 소형의 RFID 태그 사용에 있어 프라이버시와 인증 문제를 주요 보안 이슈로 언급했으며, 이를 극복하는 방안으로 태그 killing[6], 태그 sleeping과 같은 물리적 해결 기법, 아이디 relabeling[7], 암호학적 re-encryption[8]과 같은 정보 변경 기법, RFID 가디언[9], RFID Enhancer Proxy[10]과 같은 프록시 장치 활용 기법, 태그 안테나 절단[11]과 같은 통신 거리 제한 기법, 그리고 Blocker 태그[12]와 같은 고유의 통신 방식을 활용하는 틈새 기법 등이 제안되어 왔음을 비교적 잘 정리하고 있다. 물론 이 외에도 국내에서는 해쉬함수에 기반한 인증 프로토콜 제안[13], 블룸 필터를 이용한 RFID 인증 기법[14], 휴대형 리더 프라이버시 보호용 태그 검색 프로토콜 제안[15] 등 보안 이슈 해결을 위한 수많은 연구결과들이 발표되어 왔다.

그러나, 그동안 발표된 대부분의 연구결과에서 태그 내부에서의 실질적인 대칭키 암호 연산을 통한 보안 문제 해결로 접근하는 연구결과는 찾기 힘들다. 그 이유는 UHF 수동형 RFID 태그가 가지는 자원제약적 환경 때문인데, 특히 이미 ISO/IEC 18000-6 타입 C 국제표준이 정의하고 있는 태그의 응답시간(T1 time)이 최소 15.625 us ~ 최대 250 us로 제한되어 있어서 이러한 응답시간 내에 암호화 연산을 처리하기가 버겁기 때문이다. 대칭키 암호 연산을 사용하는 연구결과로 국내에서는 본 저자에 의해 2008년 12월에 TTA 잠정표준으로 제정된 TTAI.KO-12.0091[16]에서 AES 암호 알고리즘을 사용하는 보안 프로토콜이 제시된 바 있으며, 이 표준의 취약점을 분석하여 보안성을 개선시킨 연구결과가 2010년 상반기에 정보보호학회 논문지를 통해 발표되기도 하였다.[17] [17]에 의해 보안 취약점이 제기된 TTAI.KO-12.0091은 본 저자에 의해 2009년 12월에 보안성이 향상된 TTAK.KO-12.0091/R1으로 개정되었다.[18]

본 논문에서는 [18]의 내용을 바탕으로 최근 ISO/IEC JTC 1/SC 31 표준화 활동에서 나타나고 있는 암호 엔진을 사용하는 RFID 보안 기술 표준화 요구사항을 만족하는 UHF 대역의 수동형 RFID 보안 프로토콜을 제안하고 그에 대한 보안성을 분석한다. 또한 국제표준 문서에 적용될 수 있는 수준의 명령/응답 구조와 암복호화 방법을 제시함으로써 그 구현 가능성을 검증한다. 본 논문의 구성은 다음과 같다. 제 II장에서는 국제표준 요구사항을 보안 요구사항과 구현 요구사항에 따라 간략하게 설명하고, 제 III장에서 본 논문에서 제안하는 UHF 수동형 RFID 보안 기술을 상세히 설명한다. 제 IV장과 제 V장에서 제안된 보안 기술에 대한 보안성과 효율성을 분석하고, 제 VI장에서 본 논문의 결론을 맺는다.

II. 국제표준 요구사항

ISO/IEC JTC 1/SC 31 산하 WG7은 "Security for item management" 라는 이름의 작업그룹이며, 주파수 대역별로 구분된 RFID 표준 기술에 대한 보안 및 파일관리 방법을 표준화하는 것을 목표로 하고 있다. 2009년 6월에 공식 출범한 이 작업그룹에서는 ISO/IEC 29167-1 표준문서에서 RFID 보안 프레임워크 및 보안 서비스 등을 정의하고 있으며,[19] ISO/IEC 29167-6 표준문서에서 UHF 대역의 수동형 RFID 보안 기술 및 파일관리 기술의 표준화를 추진하고 있다.[20]

2.1 보안 요구사항

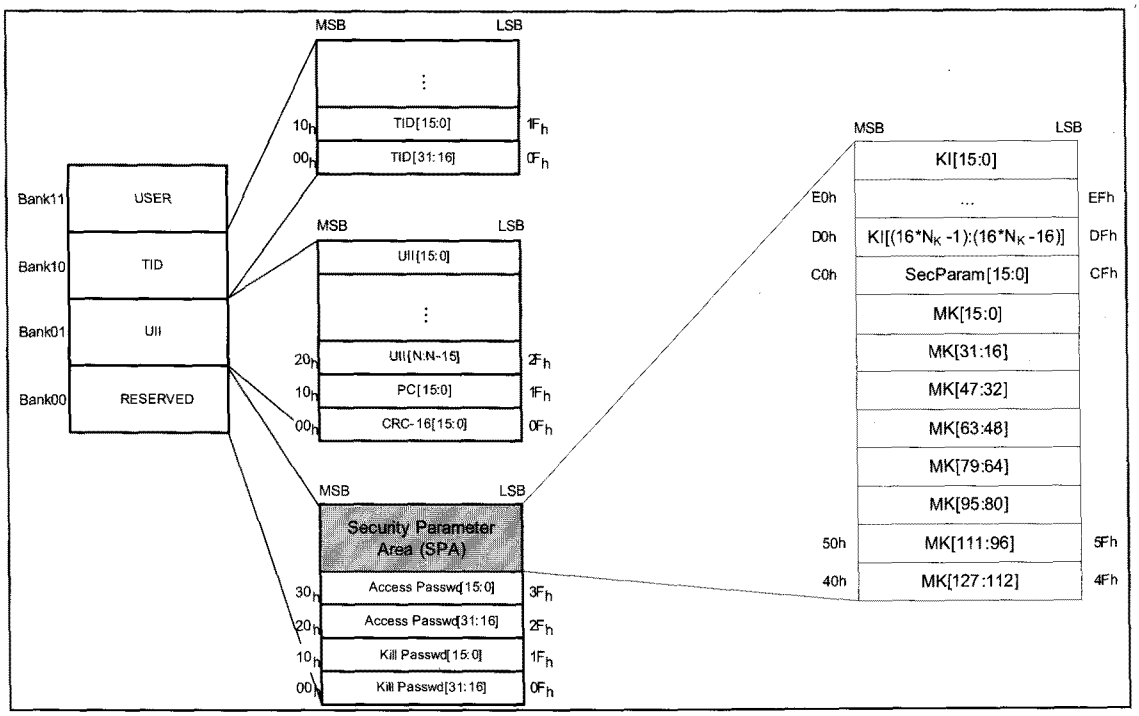
논의되고 있는 RFID 보안 프레임워크 표준문서인 [19]에서는 다음과 같은 암호학적 보안 서비스를 요구하고 있다. 암호학적 보안 서비스라 함은 태그 내부에서 암호 엔진을 구동하여 지원할 수 있는 보안 서비스를 의미한다.

- Untraceability (추적불가): 태그에 저장된 제품 아이디 정보를 통한 추적을 차단하는 서비스.
- Authenticity verification (진품 검증): 태그가 진품임을 인증하는 서비스.
- Secure communication (보안 통신): 태그와 리더 사이의 안전한 데이터 전송 서비스.
- Authentication (인증): 태그 또는 리더 또는 상호간에 고유 아이디를 인증하는 서비스.
- Access control (접근제어): 파일관리 기능 제공을 위해 필요한 태그 데이터 접근제어 서비스.

2.2 구현 요구사항

UHF 수동형 RFID 보안 서비스를 위해 수동형 RFID 태그에서 고려해야 할 구현 요구사항은 다음과 같다.

- 칩 면적: 칩 면적은 칩의 가격과 결부되어 있기 때문에 작게 구현할수록 이익이다. 수동형 RFID 칩 면적은 대략적으로 0.45 mm x 0.45 mm 즉, 202.5 um^2 면적을 가지는 것으로 평가되고 있다. 여기서 절반은 아날로그 파트가 활용해야 하므로 디지털 파트가 가질 수 있는 면적은 101.25 um^2 정도이다. 130 nm (5.2 nm^2/Gate) 또는 180 nm (12 nm^2 /Gate) 공정에 따라 차이는 있지만 디지털 파트에서 프로토콜 동작을 제외한 순수 암호 엔진 구현에 할당되는 칩 면적은 7,000 게이트 정도로 예상된다. 따라서 태그 칩 제작에서는 7,000 게이트 급의 암호 엔진 구현이 요구된다.
- 태그 응답시간: ISO/IEC 18000-6 타입 C 표준에 따르면, 인벤토리 과정에서 리더가 명령을 전송한 후 태그로부터 응답을 수신하기까지 걸리는 태그 응답시간은 최대 250 us이다. 따라서 태그는 이러한 제약조건을 고려한 동작 주파수 확보 및 암호 연산 구현이 요구된다.



[그림 1] 보안 파라미터 영역의 논리적 메모리 맵 구조

III. 제안하는 수동형 RFID 보안 기술

3.1 태그 메모리 맵 정보

ISO/IEC 18000-6 타입 C 태그는 [그림 1]의 왼편과 같은 메모리맵을 가지며, 본 논문에서 제안하는 수동형 RFID 보안 태그는 추가로 [그림 1]의 오른편과 같은 보안 파라미터 영역 (SPA: Security Parameter Area)의 정의가 필요하다.

SPA는 마스터 키 (MK: Master Key), 보안 파라미터 (SecParam: Security Parameter) 및 키 인덱스 (KI: Key Index)를 담으며, 기존의 ISO/IEC 18000-6 타입 C 명령에 의해서는 읽혀져서는 안 된다.

[그림 1]의 메모리 맵은 각 블록의 가로 크기가 1 워드 (즉, 16 비트) 사이즈를 가진다. 따라서 [그림 1]에서 보는 바와 같이 SecParam은 명시적으로 16 비트이고, KI는 SecParam의 특정 필드(Num of KI) 값에 따라 가변적인 크기를 가진다. 만일 KI가 1 워드의 길이를 가진다고 정의되면 16 비트의 KI[15:0] 하나만 존재한다. 그리고, MK는 총 128 비트(즉, 8 워드)이므로 하나의 블록이 아니라 8개의 블록에 위치한다. 즉, MK[15:0] 부터 MK[127:112] 까지를 연접한 값이 128 비트 마스터 키 하나를 구성한다. KI 역시 2 워드 이상의 길이를 가지게 될 경우에는 KI[15:0] 부터 마지막 KI 블록까지 연접한 값을 KI로 사용한다.

3.1.1 보안 파라미터와 키 인덱스

SecParam은 [표 1]과 같이 1 비트 SM (Security Mode), 1 비트 KS (Key Setting), 키 인덱스 블록의 개수를 지시하는 3 비트의 Num of KI, 사용되는 암호 알고리즘을 지시하는 4 비트의 CSI (Cryptographic Suite Identifier), 그리고 나머지는 RFU (Reserved for Future Use)로 구성되어 있다. 각 필드 별 의미는 다음과 같다.

- SM (Security Mode) : 태그가 보안 기능을 지원하는지 여부를 알려주는 지시자로서, 태그가 보안 기능을 지원하는 경우에 1로 셋팅되고, 그렇지 않은 경우에 0으로 셋팅된다. SecParam[0]에 위치하며 1 비트로 구성되어 있다.
- KS (Key Setting) : 태그에 마스터 키가 설정되어 있는지 여부를 알려주는 지시자로서, 마스터 키가 설정되어 있으면 1로 셋팅되고, 그렇지 않은 경우에 0으로 셋팅된다. SecParam[1]에 위치하며 1 비트로 구성되어 있다.
- Num of KI : 이 값은 워드 사이즈로 표현된 키 인덱스의 개수이다. [표 1]에서는 N_K 값이 약어로 사용된다. 디폴트는 1이며, 이는 1 워드에 해당하는 키 인덱스 값이 가능함을 의미한다. 즉, 이 경우에는 총 65,536 (= 2^16)개의 키 풀 (key pool)이 존재할 수 있음을 의미한다. 만약 값이 0 이라면 키 풀의 크기는 3 비트로 표현할 수 있는 최대값 즉 8 워드를 의미하여 이는 키 풀의 최대 크기가 2^128까지 가능함을 의미한다. 그리고 KI 메모리의 실제 값이 해당 키의 키 인덱스를 나타낸다.
- CSI (Cryptographic Suite Identifier) : 4 비트의 암호 알고리즘 지시자이다. 향후 확장성을 고려한 지시자이며, 디폴트는 1이고 이는 본 논문에서 제안하는 AES-OFB-like 모드를 사용함을 의미한다.
- RFU(Reserved for Future Use) : 7 비트의 예약 비트이다.
- KI (Key Index) : 본 논문에서 제안하는 수동형 RFID 보안 기술은 효율적인 키 관리를 위하여 키 풀 사용을 고려한다. KI 메모리에 있는 값은 키 풀에서의 키 인덱스를 지시한다. KI는 리더에 의해 태그에 설정되며 변경될 수 있다. Num of KI 필드의 값에 따라 가변적인 크기를 가진다.

[표 1] 보안 파라미터와 키 인덱스 구조

bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
KI(N_k-1)	Key index [15:0]															
...	...															
KI(0)	Key index [(16*N_k-1):(16*N_k-16)]															
SecParam	SM	KS	Num of KI [2:0] (N_k words)			CSI				RFU						

〔표 2〕 XPC 비트 할당

비트 위치	이름	값	의미
Bit $21A_h$	U-flag	0	최초 인벤토리 과정에서 진짜 UII를 평문으로 보냄.
		1	최초 인벤토리 과정에서 가짜 UII를 평문으로 보냄.
Bit $21B_h$	S-flag	0	보안 기능을 지원하지 않음.
		1	보안 기능을 지원함. (본 논문에서 제시하는 보안 기술 동작 가능)

3.1.2 마스터 키

마스터 키는 SPA에 위치한다. 사용되는 암호 알고리즘에 따라 다양한 길이의 마스터 키가 존재할 수 있지만 본 논문에서는 AES-128 알고리즘을 고려하여 128 비트 마스터 키로 한정한다. 마스터 키는 태그 외부로 전달되어서는 안 되며, 업데이트가 필요할 경우 반드시 리더 인증 이후에 업데이트 되어야 한다.

3.1.3 ISO/IEC 18000-6 타입 C와 연동

리더가 본 논문에서 제시하는 SPA의 인지 및 보안 프로토콜 동작을 수행하기에 앞서 태그가 이러한 기능을 지원하는지 여부를 알 수 있는 방법을 제공해야 한다. 이를 위해서는 기존의 ISO/IEC 18000-6 타입 C에서 정의된 XPC (eXtended Protocol Control)에 〔표 2〕와 같은 비트를 할당해 주어야 한다.

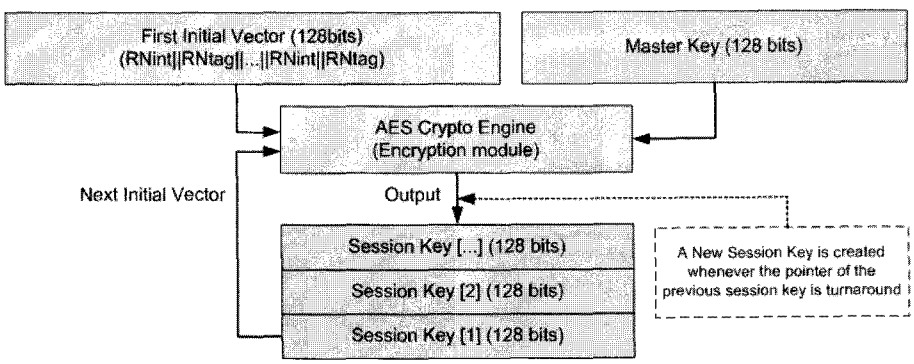
3.2 경량 고속 암복호화 방법

본 논문에서 제시하는 경량 고속 암복호화 방식은 암호 알고리즘은 AES-128을 사용하고, 활용에 있어 OFB (Output Feedback) 유사한 OFB-like 방법을 사용한다. 따라서 OFB-like 방법도 태그 내부에서는 암호화 모듈만으로 암복호화를 모두 수행할 수 있기 때문에 별도의 복호화 모듈을 추가로 구현하지 않아도 되는 장점을 가진다. 본 논문에서 필요로 하는 AES 암호 엔진의 경량 구현에 대해서는 이미 2008년도에 그 가능성을 보인 연구결과가 발표된 적이 있는데, 250 nm 공정에서 AES 암호 연산 및 레지스터 메모리와 인터페이스 블록까지 합쳐 대략 7,000 게이트 면적과 2 MHz 동작주파수에서 217 uW 소비전력이 소요됨을 시뮬레이션으로 증명하였다.[21]

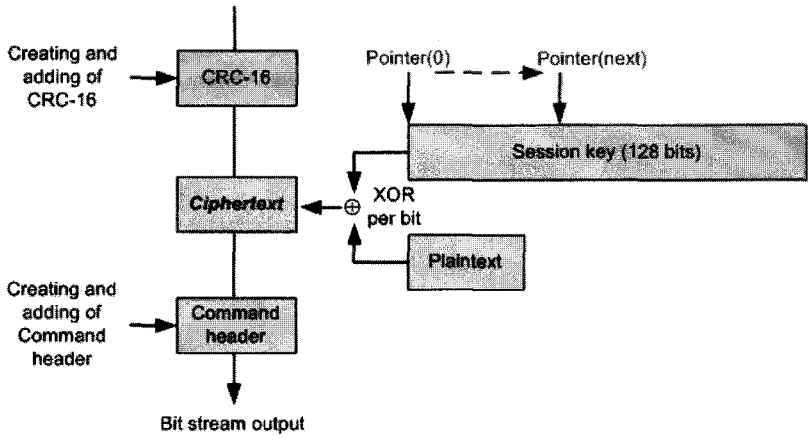
마스터 키는 보안 파라미터 영역 (SPA)에 저장된 128 비트 비밀키이며, 이로부터 세션 키를 생성하는 방법은 〔그림 2〕에 묘사되어 있다. 〔그림 3〕과 〔그림 4〕는 생성된 세션 키를 사용한 암호화 방법과 복호화 방법을 나타낸다. 〔그림 2〕, 〔그림 3〕, 〔그림 4〕는 본 저자에 의해 국내표준으로 제정된 참고문헌 〔18〕에도 제시되어 있으며, 본 논문에서도 그대로 사용된다.

3.2.1 세션 키 생성

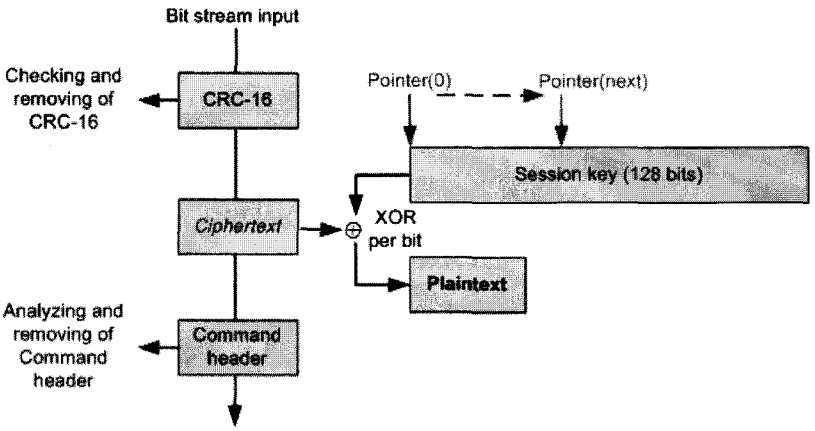
세션 키 생성에서 SPA에 저장된 MK는 마스터 키, 태그와 리더가 주고받은 랜덤넘버인 RNint (리더가 태그로 보낸 랜덤넘버)와 RNtag (태그가 리더로 보낸 랜덤넘버)의 확장된 128 비트는 최초 초기값 (IV: Initial Vector) 역할을 한다. 이 때 RNint와 RNtag는 태그에서의 랜덤넘버 생성의 편의를 위하여 각각 1 워드, 즉 16 비트의 동일한 크기를 가진다. 따



〔그림 2〕 세션 키 생성 방법



〔그림 3〕 암호화 방법



〔그림 4〕 복호화 방법

라서 128 비트의 초기값으로 입력되기 위해서 RNint와 RNtag를 연접한 후 동일한 비트를 반복시키는 방법으로 128 비트로 확장한다. 즉, 각각 16 비트 크기이므로 (RNint || RNtag)의 32 비트를 4번 반복한다. 그리고, MK와 IV를 입력받아 AES 암호화를 수행하여 128 비트 세션 키를 생성한다. 그 다음부터는 생성된 세션 키가 다시 키 생성 루틴에 활용된다. 데이터 암복호화에서는 생성된 세션 키가 스트림 암호화 방식처럼 사용된다. 이러한 구조로 설계한 이유는 수동형 RFID 태그의 연산 부담을 줄여 태그의 응답시간 요구사항을 충족시키기 위함이다.

3.2.2 데이터 암호화

생성된 세션 키를 이용한 데이터 암호화 동작은 평문 메시지와 세션 키의 XOR 연산으로 구성된다. 명령어 코드를 담은 헤더 부분과 CRC-16 부분은 암호화 연산에서 제외되면 페이로드 부분만 암호화 대상이 된다. 스트림 암호화 방식처럼 동작되므로 평문 메시지 길이에 따라 포인터를 이동하면서 암호화를 수행한다.

3.2.3 데이터 복호화

데이터 복호화는 암호화된 페이로드에 대해 XOR 연산을 수행하여 평문을 찾아내는 동작이다.

3.3 보안 프로토콜

본 논문에서 제안하는 보안 프로토콜은 상호 인증 및 데이터 보호 프로토콜과 태그 인증 프로토콜이다. 상호 인증 및 데이터 보호 프로토콜은 본 논문 2.1절에서 설명한 보안 요구사항을 모두 만족하며, 태그 인

증 프로토콜은 리더가 마스터 키가 없는 상황에서 태그 아이디와 진품 인증을 확인하는 서비스가 가능하다.

본 논문에서 제안하는 보안 프로토콜에서 사용되는 대표적인 약어는 다음과 같다.

- PC (Protocol Control): 태그의 현재 설정을 알려줌.
- XPC (eXtended Protocol Control): 확장된 PC로서, 보안기능 지원 여부를 알려줌.
- UII (Unique Item Identifier): 태그가 부착된 물품의 고유 아이디임.
- RNtag: 태그에서 생성한 랜덤넘버로서, 세션 키 생성에 사용됨.
- RNint: 리더에서 생성한 랜덤넘버로서, 세션 키 생성에 사용됨.
- CHtag: 태그에서 생성한 Challenge 랜덤넘버로서, 리더 인증에 사용됨.
- CHint: 리더에서 생성한 Challenge 랜덤넘버로서, 태그 인증에 사용됨.
- KI (Key Index): 태그에 저장된 키의 인덱스임.
- MK (Master Key): 태그에 저장된 마스터 키임.

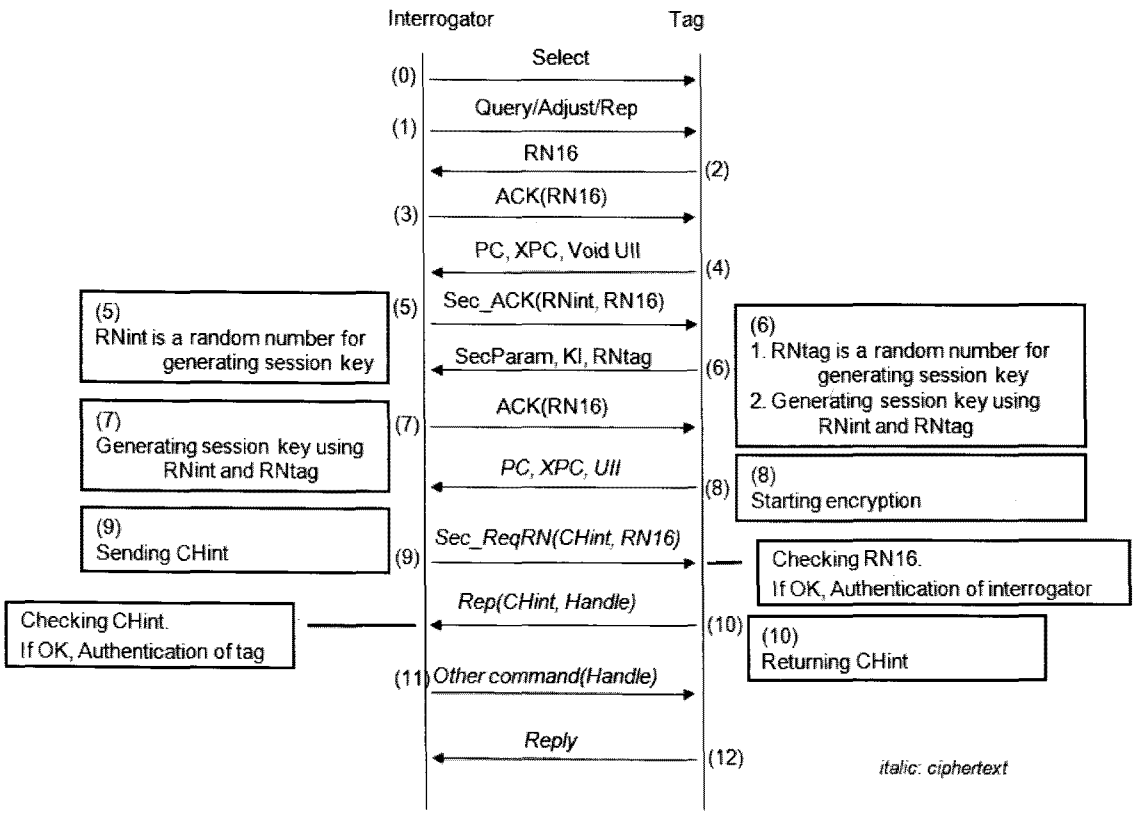
3.3.1 상호 인증 및 데이터 보호 프로토콜

상호 인증 및 데이터 보호 프로토콜 절차는 [그림 5]와 같다. 이 프로토콜(이하 프로토콜1 이라 칭함)의 목적 및 전제조건은 다음과 같다.

(1) UII는 일반적으로 아이디 체계에 관한 국제표준 또는 특정 형식을 가지고 있으므로, UII 노출 시 제조사, 물품 유형 등이 예측될 수 있다. 따라서 UII 노출을 방지해야 할 필요성이 있는 곳에서는 UII를 감추어야 하는데, 프로토콜1의 가장 큰 목적이 임의의 리더로부터 UII를 감추는 것이다.

(2) 태그와 리더는 마스터 키를 서로 알고 있다고 가정한다. 이는 키 인덱스와 관련된 정확한 키 값을 리더가 알 수 있음을 의미한다.

(3) 리더는 각 UII에 대해 해당 UII와 관련된 마



[그림 5] 상호 인증 및 데이터 보호 프로토콜

스터 키 및 키 인덱스를 데이터베이스화하여 관리하고 있다고 가정한다.

(4) 프로토콜1이 사용될 것으로 예상되는 환경은 태그가 부착된 물품이 특정 개인 또는 기업에 소유되는 상황으로써, 해당 개인 또는 기업의 리더는 태그의 데이터뿐만 아니라 UII도 감추고 싶어하는 환경을 가정한다.

태그는 가장 먼저 리더로부터 Wake-up 신호를 받아서 깨어나게 된다. 깨어난 태그는 다음과 같은 절차에 따라 상호 인증 및 데이터 보호 프로토콜을 수행한다.

- 단계 (0) ~ 단계(3): 기존의 ISO/IEC 18000-6 타입 C 표준의 동작과 동일하다. 단계(3)의 ACK 명령은 태그에게 UII (Unique Item Identifier)를 요청하는 명령이다. 세분화하여 설명하면, (0) Select로 태그 그룹을 선택하고, (1) 리더가 태그에게 쿼리 메시지를 전송한다. Query, Query_Adjust, Query_Rep 등은 ISO/IEC 18000-6 타입 C에 정의되어 있는 명령이다. 쿼리 메시지를 받은 태그는 (2) 랜덤넘버(RN16)를 회신한다. RN16를 받은 리더는 (3) ACK 메시지를 전송한다.
- 단계 (4): 본 프로토콜을 따르는 태그는 ACK 명령에 대한 응답으로 PC (Protocol Control), XPC (eXtended Protocol Control), 그리고 Void UII를 회신한다. 여기서 Void UII는 진짜 UII와 길이가 동일한 모두 0, 모두 1, 또는 랜덤한 값으로 구성된 UII를 의미한다.
- 단계 (5): 리더는 세션 키 생성에 사용되는 리더 측 랜덤넘버(RNint)를 태그에게 전달함과 동시에 태그의 SecParam, KI 및 세션 키 생성에 사용되는 태그 측 랜덤넘버(RNtag)를 요청하기 위하여 Sec_ACK 명령을 전송한다.
- 단계 (6): 태그는 내부적으로 RNtag를 생성하고, 생성된 RNtag와 수신된 RNint를 사용하여 세션 키를 생성한다. 그리고, Sec_ACK에 대한 응답으로 SecParam, KI, RNtag를 회신한다.
- 단계 (7): 리더는 내부적으로 RNint와 RNtag를 사용하여 세션 키를 생성한다. 그리고, UII를 요청하기 위하여 ACK 명령을 전송한다.
- 단계 (8): 단계(8) 이후부터는 전송 메시지의 페이로드는 암호화되어 전송된다. 태그는 PC, XPC, UII를 현재의 세션 키로 암호화하여 회신한다.
- 단계 (9): 리더는 PC, XPC, UII를 복원한 후, 세션 키 생성에 사용된 KI 및 MK가 현 단계에서 복원한 UII와 연관성이 있는지 자신의 데이터베이스를 참조하여 검증한다. 만일, 복원된 UII와 관련이 없는 KI 및 MK가 사용되었다면 인증 실패로 처리한다. 그리고 리더는 상호 인증을 위하여 Challenge에 해당하는 16 비트 랜덤넘버(CHint)를 포함한 Sec_ReqRN 명령을 전송한다. 이 때 RN16도 암호화하여 전송하는데, 태그에서 RN16을 복호화하여 확인이 되면 태그는 리더 인증을 성공한 것으로 본다.
- 단계 (10): 태그는 CHint를 복호화한 후 이를 다시 암호화하고, 이 값과 새로운 16 비트 랜덤넘버(Handle)를 회신한다. CHint를 복호화한 후에 다시 암호화하더라도 동일한 암호문 형태를 가지지 않는다. 이는 본 논문에서 제안하는 암호화 방식에서 메시지 암호화는 스트림 암호화 방식처럼 동작하도록 구성하였기 때문이다. 리더에서는 태그가 암호화하여 보낸 CHint를 복호화하여 확인이 되면 태그 인증을 성공한 것으로 본다.

여기까지 정상적으로 진행되었다면 이는 태그와 리더의 상호 인증이 완료된 것이다. 이 후의 단계 (11)과 단계 (12)의 명령/응답은 태그의 사용자 메모리 영역을 읽고 쓰기 위한 명령이 될 수 있으며, 주고받는 데이터가 암호화되어 전송되기 때문에 데이터 보호가 가능한 상황이다.

3.3.2 태그 인증 프로토콜

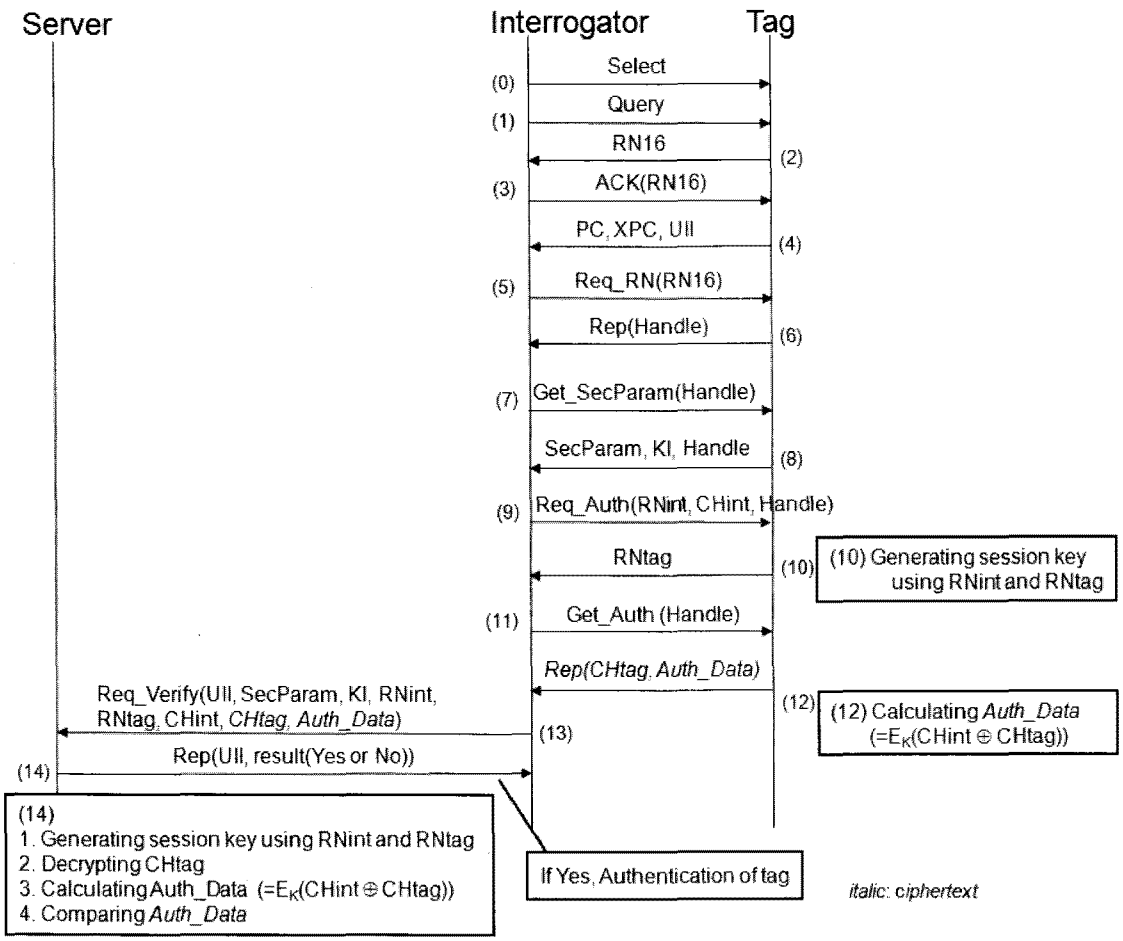
태그 인증 프로토콜 절차는 [그림 6]과 같다. 이 프로토콜(이하 프로토콜2라 칭함)의 목적 및 전제조건은 다음과 같다.

(1) 프로토콜2에서는 리더의 인벤토리 과정은 기존 ISO/IEC 18000-6 타입 C와 동일하다. 즉 모든 리더에게 태그는 자신의 UII를 평문으로 전달한다.

(2) 마스터 키는 태그 내부에 저장되어 있으며, 리더는 마스터 키를 알지 못한다고 가정한다. 마스터 키의 사용은 오직 태그가 자신을 인증시키는 데만 사용한다.

(3) 인증서버가 별도로 존재한다고 가정하며, 인증서버는 태그의 마스터 키를 알 수 있다고 가정한다.

(4) 인증서버는 각 UII에 대해 해당 UII와 관련된 마스터 키 및 키 인덱스를 데이터베이스화하여 관리하



〔그림 6〕 태그 인증 프로토콜

고 있다고 가정한다.

(5) 프로토콜2가 사용될 것으로 예상되는 대표적인 장소는 정육점과 같은 상점이다. 이러한 환경에서는 상점의 리더는 인증서버와는 서로 안전한 통신이 된다고 가정한다. 그러나 상점의 리더가 태그(정육점의 경우는 쇠고기 포장에 부착된 태그)의 마스터 키를 알게 된다면 이를 악용할 수 있는 여지가 있기 때문에 원천적으로 이를 막기 위해서는 상점의 리더가 마스터 키를 몰라야 한다. 그렇지만 소비자는 해당 태그가 정상적인 태그인지는 확인해야 하므로 상점의 리더 또는 소비자의 휴대 리더를 통해 태그를 인증해야 한다. 즉, 프로토콜2의 가장 큰 목적은 임의의 리더가 인증서버로부터 태그의 인증여부를 확인 받을 수 있도록 하는 것이다.

태그와 리더, 그리고 인증서버는 다음과 같은 절차에 따라 태그 인증 프로토콜을 수행한다.

- 단계 (0) ~ 단계(6): 기존의 ISO/IEC 18000-6 타입 C 표준의 인벤토리 동작과 동일하다. 세분화하여 설명하면, (0) Select로 태그 그룹을 선택하고, (1) 리더가 태그에게 쿼리 메시지를 전송한다. Query, Query_Adjust, Query_Rep 등은 ISO/IEC 18000-6 타입 C에 정의되어 있는 명령이다. 쿼리 메시지를 받은 태그는 (2) 랜덤넘버를 회신한다. 리더는 (3) ACK 명령을 전송하고, 태그에 이에 대한 응답으로써 PC, XPC 및 UII를 평문으로 전달한다. 그리고, 리더는 (5) Req_RN 명령을 보내며, 이에 대한 응답으로 태그는 (6) Handle을 응답한다. 이 후부터는 Handle을 보낸 태그와 peer-to-peer 통신이 시작된다.
- 단계 (7): 본 프로토콜을 따른 리더는 태그의 SecParam을 얻기 위하여 Get_SecParam 명

령을 전송한다. 이 때, 리더는 마스터 키가 없으므로 세션 키를 생성할 수 없어서 모든 명령을 평문으로 전송한다.

- 단계 (8): 태그는 Get_SecParam 명령에 대한 응답으로 SecParam과 KI를 회신한다.
- 단계 (9): 리더는 태그 인증을 위한 인증 데이터를 요청하기 위하여 Req_Auth 명령을 전송한다. Req_Auth 명령은 세션 키 생성에 사용되는 리더의 RNint, Challenge에 해당하는 CHint를 포함하며, 이들은 평문으로 전송된다.
- 단계 (10): 태그는 내부적으로 세션 키 생성에 사용되는 태그의 RNtag를 생성하고, 수신된 RNint와 RNtag를 사용하여 세션 키를 생성한다. 태그는 RNtag를 평문으로 리더에게 응답한다.
- 단계 (11): 리더는 태그 인증을 위한 인증 데이터를 가져오기 위하여 Get_Auth 명령을 전송한다.
- 단계 (12): 태그는 태그 인증에 사용되는 랜덤넘버(CHtag) 및 Auth_Data를 회신한다. 페이로드에 해당하는 CHtag와 Auth_Data는 암호화된 값이다. Auth_Data는 CHint와 CHtag를 XOR 한 후 이 값을 암호화한 것이다.
- 단계 (13): Auth_data까지 수신한 리더는 이제 태그와의 통신을 끝내고 인증서버와의 통신을 통해 태그가 보내온 값들을 검증한다. 즉, 리더는 인증서버에게 Req_Verify 메시지를 보내는데, 파라미터로는 태그의 UII, SecParam, KI, RNint, RNtag, CHint, 그리고 단계(12)에서 받은 암호화된 CHtag와 Auth_Data를 모두 포함하여 전송한다. 이 때, 리더와 인증서버 사이의 통신은 안전한 채널을 통해 수행된다고 가정한다.
- 단계 (14): 인증서버는 해당 UII와 관련된 마스터 키를 검색하여 찾고, RNint와 RNtag 및 마스터 키로부터 세션 키를 유도한다. 인증서버가 자신의 데이터베이스에서 찾은 키 인덱스와 수신된 키 인덱스가 일치하지 않는다면 곧바로 인증 실패로 처리한다. 일치하면 먼저 CHtag를 복호화하여 구하고, CHint와 CHtag를 XOR하고 세션 키를 사용하여 이를 암호화하여 Auth_Data를 구한다. 인증서버가 자체적으로 구한 Auth_Data 값과 리더로부터 수신한 Auth_Data 값을 비교하여 동일하면 인증 성공, 동일하지 않으면 인증 실패로 판단하여 그 결과를 리더에게 회신한다.

3.4 명령/응답 구조

본 논문에서 제시하는 보안 프로토콜을 수행하기 위해서는 태그와 리더 사이에서 주고받을 다음과 같은 명령/응답 메시지가 필요하다.

- Sec_ACK 명령과 응답 메시지
- Sec_ReqRN 명령과 응답 메시지
- Get_SecParam 명령과 응답 메시지
- Req_Auth 명령과 응답 메시지
- Get_Auth 명령과 응답 메시지

그리고 아래 메시지는 리더와 인증서버 사이에서 주고받는 명령/응답 메시지이다.

- Req_Verify 명령과 응답 메시지

3.4.1 Sec_ACK

Sec_ACK 명령은 세션 키 생성에 사용되는 리더의 RNint를 전달하는 역할을 수행하는 명령으로 그 구

Sec_ACK Command

	Command	RNint	RN16	CRC-16
# of bits	16	16	16	16
description	command code	random number	handle	

Sec_ACK Reply

	SecParam	KI	RNtag	RN16	CRC-16
# of bits	16	16 * (Num of KI)	16	16	16
description	security parameter	key index	random number	handle	

〔그림 7〕 Sec_ACK 명령/응답 메시지

Sec_ReqRN Command

	Command	CHint	RN16	CRC-16
# of bits	16	16	16	16
description	command code	random number	handle	

Sec_ReqRN reply

	Response	RN16	CRC-16
# of bits	16	16	16
description	CHint	handle	

: Plain Data
: Encrypted Data

〔그림 8〕 Sec_ReqRN 명령/응답 메시지

Get_SecParam Command

	Command	RN16	CRC-16
# of bits	16	16	16
description	command code	handle	

Get_SecParam Reply

	Header	SecParam	KI	RN16	CRC-16
# of bits	1	16	16 * (Num of KI)	16	16
description	0(success) or 1(failure)	security parameter	key index	handle	

〔그림 9〕 Get_SecParam 명령/응답 메시지

성은 〔그림 7〕과 같다. 태그는 Sec_ACK 명령에 대한 응답으로 SecParam, KI, 그리고 RNtag를 회신한다. 여기서 KI는 SecParam의 Num of KI 필드의 값에 따라 가변적인 길이로 응답되는데, 그 길이는 (16 * Num of KI) 비트가 된다. 본 명령과 응답은 세션 키 생성에 사용되는 RNint와 RNtag를 교환하는 역할과 태그가 AES 암호 모듈을 구동시킬 수 있는 시간을 벌기 위한 역할을 하며, 평문으로 전달된다.

3.4.2 Sec_ReqRN

Sec_ReqRN 명령은 ISO/IEC 18000-6 Type C 표준의 Req_RN 명령처럼 태그의 state를 Open state로 천이시킨다. Sec_ReqRN 명령과 응답은 태그와 리더의 상호 인증을 위한 Challenge/Response를 주고받는 동작이며, 그 구성은 〔그림 8〕과 같다. 명령과 응답의 페이로드 부분은 모두 암호화 되어 전달된다. Sec_ReqRN 명령에서 Challenge에 해당하는 CHint 값은 리더가 랜덤하게 생성한 Nonce 이며 16 비트의 길이를 가진다. 태그 응답의 Response 값은 리더로부터 전달받은 CHint를 태그가 암호화한 값이다. 응답을 받은 리더는 응답을 복호화한 후, 자신의 CHint 값이 Response 값으로 돌아온 것을 확인하여 태그를 인증한다. 또한 태그는 수신된 명령에서 리더가 올바른 RN16의 암호문을 전송한 것을 확인하여 리더를 인증한다. 본 Challenge/Response를 통해 Replay 공격 방지와 상호 인증을 달성할 수 있다. 여기서, 명령어 타입과 CRC(Cyclic redundancy Check)-16 값은 암호화 되지 않는다.

3.4.3 Get_SecParam

Get_SecParam 명령은 태그의 보안 파라미터를 얻을 때 사용하는 명령으로 그 구성은 〔그림 9〕와 같다. Get_SecParam 명령을 수신한 태그는 자신의 SecParam과 KI를 회신한다. 본 명령과 응답은 일

Req_Auth Command

	Command	RNint	CHint	RN16	CRC-16
# of bits	16	16	16	16	16
description	command code	random number	random number	handle	

Req_Auth reply

	RNtag	Handle	CRC-16
# of bits	16	16	16
description	random number	handle	

〔그림 10〕 Req_Auth 명령/응답 메시지

Get_Auth Command

	Command	Handle	CRC-16
# of bits	16	16	16
description	command code	handle	

: Plain Data
: *Encrypted Data*

Get_Auth reply

	CHtag	*Auth_Data*	Handle	CRC-16
# of bits	*16*	*16*	16	16
description	*random number*	*CHint @ CHtag*	handle	

〔그림 11〕 Get_Auth 명령/응답 메시지

단 리더에게 자신의 보안 파라미터를 전달하는 역할을 하기 때문에 평문으로 전달된다.

3.4.4 Req_Auth

Req_Auth 명령은 태그 인증을 위한 인증 데이터를 요청하기 위하여 사용되는 명령으로 그 구성은 〔그림 10〕과 같다. 리더가 보내는 명령은 세션 키 생성에 사용되는 리더의 RNint, Challenge에 해당하는 CHint를 포함하며, 이들은 평문으로 전송된다. 값은 리더가 랜덤하게 생성한 Nonce 이며 16 비트의 길이를 가진다. 태그에서는 세션 키 생성을 위한 태그의 RNtag를 생성하여 응답하며, 내부적으로 RNint와 RNtag를 사용하여 세션 키를 생성한다. 그리고 Get_Auth 명령을 기다린다.

3.4.5 Get_Auth

Get_Auth 명령은 태그 인증을 위한 인증 데이터를 가져오기 위하여 사용되는 명령으로 그 구성은 〔그림 11〕과 같다. 인증 데이터를 요청하는 Req_Auth 명령과 인증 데이터를 가져오는 Get_Auth 명령을 구분하여 사용하는 이유는 태그에서 RNint와 RNtag로부터 세션 키를 생성하는 시간을 벌기 위함이다. 즉, 태그가 리더로부터 RNint를 수신하고 RNtag를 생성 후 이로부터 세션 키 생성하여 암호화된 데이터를 만들어서 응답하게 되면 수동형 RFID 태그의 제한적인 연산 능력 때문에 ISO/IEC 18000-6 타입 C 표준의 태그 응답시간을 만족하기 어렵게 된다. 따라서, 인증 데이터 요청 후 다시 인증 데이터를 가져오는 명령으로 두번의 실행으로 동작하도록 설계하는 것이 대안이 될 수 있다. 리더가 보내는 명령은 handle 만을 포함하며, 평문으로 전송된다. 태그는 Challenge에 해당하는 CHtag와 인증 데이터인 Auth_Data를 암호화하여 회신한다. 즉, 3.3.2절의 태그 인증 프로토콜에서는 리더가 마스터 키를 가지고 있지 않기 때문에 리더의 명령은 암호화될 수 없지만 태그는 자신의 마스터 키를 사용하여 세

Req_Verify Command

	Target	SecParam	KI	RNint	RNtag	CHint	CHtag	Auth_Data
# of bits	-	16	16 * (Num of KI)	16	16	16	16	16
description	UII	security parameter	key index	random number of interrogator	random number of tag	challenge number of interrogator	challenge number of tag	authentication data

Req_Verify reply

	Header	Target
# of bits	1	-
description	0(success) or 1(failure)	UII

〔그림 12〕 Req_Veryfi 명령/응답 메시지

션 키 생성과 암호화 동작을 수행할 수 있다. 태그가 보낸 암호화된 CHtag와 Auth_Data는 인증서버로 전달된 후 인증서버에서 복호화된다. Auth_Data는 CHint와 CHtag를 XOR 한 후 이 값을 암호화한 것이다. CHint 값은 리더가 랜덤하게 생성한 Nonce 이고 CHtag 값은 태그가 랜덤하게 생성한 Nonce 인데, 각각 16 비트의 길이를 가진다. 따라서 Auth_Data 역시 CHint와 CHtag 길이와 동일한 16 비트의 길이를 가진다.

3.4.6 Req_Verify

Req_Verify 명령은 인증서버에게 태그의 정당성을 검증해달라고 요청하기 위하여 리더가 인증서버에게 보내는 명령으로 그 구성은 〔그림 12〕와 같다. 리더는 태그로부터 수신한 정보인 SecParam, KI, RNtag, CHtag, Auth_Data와 리더 자신이 생성한 RNint, CHint 등을 해당 태그의 UII와 함께 인증서버로 전달한다. 인증서버는 관련 정보를 참조하여 인증 성공여부를 리더에게 회신한다.

IV. 보안성 분석

4.1 상호 인증 및 데이터 보호 프로토콜의 보안성 분석

본 논문 3.3.1절의 프로토콜1의 절차에 따른 보안성 분석은 다음과 같다.

- 단계 (0) ~ 단계(3): 기존 18000-6 타입 C 인벤토리 과정의 일부로서 보안 이슈와는 관련이 없다.
- 단계 (4): 기존의 18000-6 타입 C 태그는 이 단계에서 PC, XPC 및 UII를 평문으로 응답하지만, 본 프로토콜1에서는 UII 진짜 값 대신 Void UII를 응답한다. 이는 보안 기능을 가진 리더가 아닌 기존 리더와의 호환성을 위한 것으로서, 기존 리더는 Void UII를 실제 UII로 인식하기 때문에 본 프로토콜1을 따르는 태그는 기존 리더에게는 진짜 UII를 노출시키지 않는 효과를 얻을 수 있다.
- 단계 (5): 본 프로토콜 1을 위해서 정의한 리더의 명령이며, RNint 전달의 기능 및 SecParam, KI, RNtag를 요청하는 기능을 가진다.
- 단계 (6): 태그는 이 단계에서 세션 키를 유도하고 대기한다. 리더가 바뀌거나 통신이 끊어졌다가 다시 연결되는 등 매 세션마다 이 단계에서 태그의 새로운 랜덤넘버(RNtag) 및 리더의 새로운 랜덤넘버(RNint)를 사용하여 세션 키를 생성하기 때문에 키 신선도(freshness) 조건이 만족된다.
- 단계 (7): 리더는 이 단계에서 세션 키를 유도하고 대기한다. 단계 (6)과 동일한 이유로 리더에서도 키 신선도 조건이 만족된다.
- 단계 (8): 여기서부터는 데이터들이 암호화되어 통신된다. 즉, 이 단계에서 태그가 진짜 UII를 전달하며, 그 값은 암호화되어 전달된다. 따라서, 리더가 정확한 마스터 키를 가지고 세션 키를 유도했을 경우에만 해당 UII를 복원할 수 있다.
- 단계 (9): 공격자가 고의적 또는 우연히 하나의 태그에 대한 마스터 키와 키 인덱스를 획득하게 되면 임의의 UII로 인증을 시도할 수 있는데, 리더에서 UII와 관련된 마스터 키 및 키 인덱스를 유지하기 때문에 임의의 UII 인증 시도를 차단할

수 있다. 그리고 이 단계에서는 리더는 2가지 효과를 가질 수 있는데, 첫째는 Handle로 사용하던 RN16을 암호화하여 태그에게 전달함으로써 태그가 이를 복호화하여 RN16을 확인하도록 하여 리더 자신을 인증시키는 것이고, 둘째는 태그를 인증하기 위하여 태그에게 Challenge 랜덤 넘버를 전달하고 태그로부터 암호화된 Challenge가 제대로 오기를 기다리는 것이다.

- 단계 (10): 리더는 태그로부터 암호화되어 전달되어 온 CHint를 복호화하여 확인함으로써 태그 인증을 수행한다.

위와 같은 분석을 통해 다음과 같은 보안 서비스 제공이 가능함을 확인할 수 있다.

(1) 상호 인증: 리더는 태그가 생성한 RN16을 암호화하여 회신하고, 태그는 리더가 생성한 CHint를 암호화하여 회신하기 때문에 각각 이를 복호화하여 확인할 수 있다면, 상대가 정확한 세션 키를 사용하고 있다고 볼 수 있다. 이는 정확한 마스터 키로부터 세션 키를 유도한 것이므로 서로 마스터 키를 공유한 정당한 태그와 리더라고 인증할 수 있다.

(2) 데이터 기밀성: 중요 정보로 취급할 수 있는 UII를 암호화하여 전달하며, 이후에 사용자 메모리 영역의 데이터 읽기와 쓰기 등의 명령/응답은 암호화 통신이 수행된다.

(3) 스푸핑 공격 탐지: 프로토콜1의 절차 중 단계 (5)와 단계 (6)는 매 세션마다 다르게 생성되는 RNint와 RNtag를 주고 받는 절차이다. RNint와 RNtag는 세션 키 생성에 사용되는 IV 역할을 하기 때문에 매 세션마다 다르게 사용된다는 것은 세션 키의 신선도를 보장할 수 있음을 의미한다. 이는 악의적인 도청자의 재생 공격에 의한 스푸핑 공격을 탐지해 낼 수 있는 특성을 가진다.

(4) 제품정보 노출 방지: 일반적인 태그는 고유의 아이디로서 태그 자체적인 아이디(TID) 및 부착되는 물품과 관련된 유일 아이디(UII)를 가진다. 만일 특정 개인 또는 기업이 UII를 사용할 때, 임의의 리더가 손쉽게 UII 를 읽음으로써 UII 포맷 규칙에 따라 제품정보를 파악할 수 있다. 그러나, 프로토콜1은 세션 키를 생성할 수 있는 정상적인 리더를 제외한 임의의 리더에 대해서는 실제 UII를 감추기 때문에 제품정보 노출을 막을 수 있다. 이러한 특징은 사용자 프라이버시 보호와도 일맥상통하다고 볼 수 있다.

4.2 태그 인증 프로토콜의 보안성 분석

본 논문 3.3.2절의 프로토콜2의 절차에 따른 보안성 분석은 다음과 같다.

- 단계 (0) ~ 단계(6): 기존 ISO/IEC 18000-6 타입 C 인벤토리 과정과 동일하다. UII는 노출되며 본 프로토콜2는 UII 노출에 따른 프라이버시 문제는 해결대상이 아닌 것으로 본다.
- 단계 (7): 본 프로토콜 1을 위해서 정의한 리더의 명령이며, SecParam과 KI를 요청하는 기능을 가진다.
- 단계 (8): 태그의 응답이며, 평문 전송이다.
- 단계 (9): 이 단계에서 리더는 세션 키 생성에 사용되는 RNint와 Challenge에 해당하는 CHint를 평문으로 전송한다.
- 단계 (10): 태그는 이 단계에서 세션 키를 유도하고 대기한다. 이 단계에서는 매 세션마다 새로운 태그의 RNtag 및 리더의 RNint를 사용하여 세션 키를 생성하기 때문에 키 신선도 조건이 만족된다. Req_Auth에 대한 응답으로 곧바로 암호화된 Auth_Data를 보내지 못하고 RNtag만을 보내면서 Get_Auth를 다시 기다리는 이유는 그 사이에 AES 암호 엔진을 사용하여 세션 키를 생성하는 시간을 벌기 위함이다.
- 단계 (11): 암호화된 Auth_Data를 얻기 위한 리더의 명령이다.
- 단계 (12): 태그는 인증용 데이터로서 리더로부터 수신한 CHint와 태그 자신이 생성한 CHtag를 XOR 한 값을 사용한다. 그리고, 태그는 CHtag와 인증용 데이터를 암호화하여 전달한다.
- 단계 (13): 리더는 마스터 키가 없기 때문에 태그와의 통신을 통해 얻은 정보를 인증서버로 그대로 전달해야 한다. 리더와 인증서버와의 통신은 일종의 웹서버 접속으로 볼 수 있다. 따라서 리더는 상점의 리더 또는 소비자의 휴대 리더(예를 들면, 휴대폰에 장착된 리더)가 될 수 있다.
- 단계 (14): 인증서버는 주어진 정보에 기반하여 결과만을 회신한다. 공격자가 고의적 또는 우연히 하나의 태그에 대한 마스터 키와 키 인덱스를 획득하게 되면 임의의 UII로 인증을 시도할 수 있는데, 인증서버에서 UII와 관련된 마스터 키 및 키 인덱스를 유지하기 때문에 임의의 UII 인증 시도를 차단할 수 있다.

위와 같은 분석을 통해 다음과 같은 보안 서비스 제공이 가능함을 확인할 수 있다.

(1) 태그 인증: 프로토콜2는 모든 리더에게 UII를 평문으로 제공한다. 즉, 리더 인증을 요구하지는 않는 응용에서 사용 가능하다. 그러나 태그 인증은 중요하게 고려하고 있다. 태그는 리더가 생성하여 전달해 준 CHint를 포함하여 인증용 데이터를 생성한 후 이를 암호화하여 회신하기 때문에 인증서버에서 확인한 값이 정확한 값이라면 태그는 정확한 세션 키를 사용하고 있다고 볼 수 있다. 이는 정확한 마스터 키로부터 세션 키를 유도한 것이므로 태그가 가진 마스터 키는 인증서버가 가진 마스터 키와 동일하다고 보고 정당한 태그라고 인증할 수 있다.

(2) 스푸핑 공격 탐지: 프로토콜2의 절차 중 단계 (9)와 단계 (10)에서 매 세션마다 다르게 생성되는 RNint와 RNtag를 주고 받을 수 있다. RNint와 RNtag는 세션 키 생성에 사용되는 IV 역할을 하기 때문에 매 세션마다 다르게 사용된다는 것은 세션 키의 신선도를 보장할 수 있음을 의미한다. 이는 악의적인 도청자의 재생 공격에 의한 스푸핑 공격을 탐지해 낼 수 있는 특성을 가진다. 본 프로토콜2에서는 UII 자체를 공개하고 있으며 리더가 마스터 키를 가지고 있지 않기 때문에 제품정보 노출 방지(사용자 프라이버시 보호 측면)와 데이터 암/복호화(데이터 기밀성 측면) 보안 서비스는 제공하지 못한다. 즉 프로토콜2의 주요 관심대상은 태그 인증일 뿐이다.

4.3 알려진 취약점

본 논문에서 제안하는 보안 프로토콜의 알려진 취약점은 다음과 같다.

첫째, 3.3.1절 상호 인증 및 데이터 보호 프로토콜에서는 세션 키 비트 스트림의 일부가 노출될 수 있다. 단계(8)의 PC, XPC와 단계(9)의 RN16은 암호화하여 전송하게 되는데, 이 데이터들은 이전 단계에서 평문으로 전송되고 있기 때문에 단계(8)과 단계(9)의 암호화된 PC, XPC, RN16과 평문 PC, XPC, RN16이 도청될 경우, 프로토콜1의 암복호화 방법이 세션 키와 평문 메시지의 XOR 이므로 알려진 평문과 암호문 2개의 데이터를 그대로 XOR하면 세션 키 비트 스트림 중 일부가 노출될 수 있다. 그러나 이후에 암호화되는 데이터는 이미 사용된 키에서 이동된 곳의 키 비트가 사용되기 때문에 노출된 일부 키 비트로 인한 추가적인 데이터 노출의 위험은 없다. 본 논문에서는 RN16 암호화 및 복호화 동작을 리더 인증 수단으로 사용하고 있으며, 또한 태그에서 세션 키가 설립된 이후에는 모든 응답의 페이로드는 암호화시켜 응답하는 구현의 효율성을 고려하여 프로토콜1을 설계하였다.

둘째, 3.3.1절과 3.3.2절의 프로토콜에서, 랜덤넘버 및 Challenge로 사용되는 데이터의 크기가 전사 공격(brute force attack)에 대한 안전성을 제공한다. 따라서 각각의 랜덤넘버 길이가 16 비트이므로 2^16의 안전성이라고 볼 수 있다. 랜덤넘버의 길이를 16 비트로 고려한 이유는 기존 ISO/IEC 18000-6 타입 C 표준에서 태그의 랜덤넘버가 주로 16비트였기 때문에 이에 맞는 길이를 고려했기 때문이다. 만일 태그에서 더욱 확장된 랜덤넘버를 신속하게 생성하고 처리할 수 있다면 전사 공격에 대한 안전성도 확장된다.

셋째, 공격자가 고의적 또는 우연히 하나의 태그에 대한 마스터 키와 키 인덱스를 획득하여 정상적인 리더를 상대로 임의의 UII를 사용하여 태그 인증을 시도하는 경우, 만일 태그 인증을 수행하는 리더 또는 인증서버에서 태그의 UII와 관련된 마스터 키 및 키 인덱스를 데이터베이스화하여 관리하지 않는다면 임의의 UII에 대한 태그 인증이 성공할 수 있을 것이다. 그러나 본 논문의 프로토콜1과 프로토콜2의 예상 활용환경을 고려하면 다음과 같은 상황이 된다. 프로토콜1의 경우, 프로토콜1의 가장 큰 목적은 UII 자체도 감추는 것이다. 이는 보안 서비스 측면에서 사용자 프라이버시 보호와 제품정보 노출 방지 효과를 가져올 수 있다. 특히 개인화된 제품인 경우는 키 관리가 전적으로 개인 리더(예를 들면, 휴대폰)에서 처리된다. 만약 공격자가 내 소유의 물품을 취득하여 하나의 키와 그에 해당하는 키 인덱스를 알아낸다고 가정하면 그 공격자가 얻을 수 있는 효과는 임의의 UII로 인증을 받을 수 있는 것이다. 하지만 공격자의 인증 성공은 본 논문의 프로토콜1이 추구하는 사용자 프라이버시 보호와 제품정보 노출 방지에는 영향을 주지는 않는다. 또한, 리더에서 세션 키 생성에 사용된 마스터 키 및 키 인덱스가 수신된 UII와 연관성이 있는지 자신의 데이터베이스를 참조하여 검증하게 되면 이러한 태그 인증 시도에 대해 오류로 처리할 수 있다. 프로토콜2의 경우, 프로토콜2도 UII와 마스터 키가 서로 연관되어 있는 환경을 고려한다. 즉 인증서버는 UII를 수신하여 그 UII와 관련된 마스터 키와 키 인덱스를 데이터베이스로 관리하고 있는 것이다. 따라서 임

의의 UII가 공격자에게 노출된 마스터 키 및 키 인덱스와 연결이 되지 않는다면 인증서버에서 이를 확인하여 오류로 처리할 수 있다.

V. 효율성 및 구현 가능성 분석

UHF 수동형 RFID 보안 기술의 구현은 본 논문 2.2절에서 설명한 구현 요구사항을 만족하면서 효율성도 극대화 시켜야 한다. 본 논문의 실험에서는 본 저자들이 설계한 AES 암호 모듈을 사용하여 구현 요구사항을 만족시켰으며, AES-OFB-like 모드로 보안 프로토콜을 구현하여 효율성을 극대화 시켰다. 다음의 [표 3]은 본 논문의 실험조건 및 결과를 정리한 것이다.

본 논문에서 제안하는 수동형 RFID 보안 기술의 주요 특징은 AES-OFB-like 모드의 사용이다. 본 논문의 수동형 RFID 보안 기술에 따르면, 태그는 AES 복호 모듈을 별도로 가질 필요 없이 AES 암호 모듈만 구현하면 된다. 또한 태그와 리더 사이의 세션 키 생성 시 AES 암호 연산을 수행하고, 실제 태그의 응답 시 데이터 암호화는 세션 키와 응답 데이터의 XOR이므로 태그의 최대 응답 제한시간인 250 us 내에 암호화된 데이터를 응답할 수 있다. [표 3]의 실험결과에서 확인할 수 있듯이 128 비트 데이터의 암호화 응답은 114 us 이므로 ISO/IEC 18000-6 타입 C 국제표준을 준수하는 태그의 UII를 충분히 전달할 수 있다. 즉, 본 논문의 암복호화 방법은 기존의 해쉬 기반의 UHF 수동형 RFID 인증 기법 또는 13.56 MHz HF 대역용으로 제안된 AES-CBC 모드 활용 기법에 비해 UHF 수동형 RFID 시스템에 적합하도록 효율성과 구현 가능성을 향상시킨 방법이다.

[표 3] 보안 프로토콜 실험 조건 및 결과

항목		내용
실험 조건	AES 암호 모듈 하드웨어 면적	7,029 gates[21]
	소비전력	217 uW (@ 2 MHz 동작)
	태그 동작 주파수	1.92 MHz
	태그-리더 동작 모드	160 kHz/640 kHz
실험 결과	128 비트 암호화 응답 시간	114 us

VI. 결 론

본 논문에서는 국제표준에서의 보안 요구사항에 비추어, AES 암호 엔진을 사용하는 UHF 수동형 RFID 시스템에 적합한 보안 프로토콜을 제시하였다. 그리고 이에 적합한 암복호화 방법 및 구체적인 명령/응답 메시지를 정의함으로써 그 구현 가능성을 검증하였다. 또한 본 논문이 제시한 보안 프로토콜과 암복호화 방법이 국제표준에서 논의되고 있는 보안 요구사항인 추적불가(untraceability), 진품 검증(authenticity verification), 보안 통신(secure communication), 인증(authentication) 및 접근제어(access control) 기능을 제공할 수 있는 토대가 될 수 있음을 보였다.

ISO/IEC 18000-6 타입 C 규격으로 대표되는 UHF 수동형 RFID 기술은 암호 엔진을 통합시킨 태그의 활용을 예상하면서 국제표준화가 진행되고 있다. 그 과정에서 가장 먼저 고려되고 있는 사항이 호환성을 보장하는 구현 가능성인데, 본 논문에서 제시하는 UHF 수동형 RFID 보안 기술은 AES 암호 모듈을 7,000 게이트 급으로 구현하고 이를 OFB-like 모드에 적용하여 128 비트 데이터 암호 연산을 114 us 이내에 처리함으로써 그 구현 가능성을 검증하였다.

본 논문은 기존의 ISO/IEC 18000-6 타입 C 규격과의 호환성을 보장하면서 AES 암호 엔진을 활용한 보안 서비스 제공이 가능함을 보임으로써 기술발전 방향 및 국제표준화 추진 방향을 주도하는 역할을 할 것으로 기대된다.

참고문헌

[1] ISO/IEC, "ISO/IEC 18000 Information technology - Radio-Frequency Identification for item management - Part 6: Parameters for air interface communications at 860 MHz to 960 MHz Amendment 1," Jun. 2006.

[2] ISO/IEC, "ISO/IEC 15961 Information technology - Radio-Frequency Identification for item management - Data protocol: application interface," Oct. 2004.

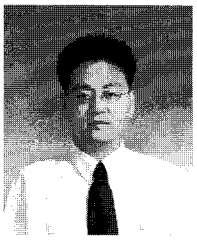
[3] ISO/IEC, "ISO/IEC 15962 Information technology - Radio-Frequency Identification for item management - Data

protocol: data encoding rules and logical memory functions," Oct. 2004.
[4] ISO/IEC, "ISO/IEC 15963 Information technology - Radio-Frequency Identification for item management - Unique identification for RF tags," Sep. 2004.
[5] A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381-394, Feb. 2006.
[6] EPCglobal, "EPCTM Radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz - 960 MHz version 1.0.9", Jan. 2005.
[7] N. Good, J. Han, E. Miles, D. Molnar, D. Mulligan, L. Quilter, J. Urban, and D. Wagner, "Radio frequency identification and privacy with information goods," Proceedings of Workshop on Privacy in the Electronic Society, pp. 41-42, Apr. 2004.
[8] A. Juels and R. Pappu, "Squealing euros: privacy protection in RFID-enabled banknotes," Proc. of the Financial Cryptography, LNCS 2742, pp. 103-121, 2003.
[9] M. Rieback, B. Crispo, and A. Tanenbaum, "RFID Guardian: A battery-powered mobile device for RFID privacy management," Proc. of the Australasian Conference on Information Security and Privacy, LNCS 3574, pp. 184-194, 2005.
[10] A. Juels, P. Syverson, and D. Bailey, "High-power proxies for enhancing RFID privacy and utility," Proc. of the Privacy Enhancing Technologies, LNCS 3856, pp. 210-226, 2006.
[11] G. Karjoth and P. Moskowitz, "Disabling RFID tags with visible confirmation: Clipped tags are silenced," Proceedings of Workshop on Privacy in the Electronic Society, pp. 27-30, 2005.
[12] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy," Proceedings of 8th ACM Conference on Computer and Communication Security, pp. 103-111, 2003.
[13] 하재철, 백이루, 김환구, 박제훈, 문상재, "해쉬함수에 기반한 경량화된 RFID 인증 프로토콜," 한국정보보호학회논문지, 19(3), pp. 61-72, 2009년 6월.
[14] 김진호, 서재우, 이필중, "저비용 RFID 시스템에 적합한 효율적인 인증 방법," 한국정보보호학회논문지, 18(2), pp. 117-128, 2008년 4월.
[15] 천지영, 황정연, 이동훈, "이동형 리더 소지자의 프라이버시를 보호하는 RFID 태그 검색 프로토콜," 한국정보보호학회논문지, 19(5), pp. 59-69, 2009년 10월.
[16] 정보통신단체표준(잠정표준) TTAI.KO-12.0091, "수동형 RFID 보안태그와 리더의 인증 및 데이터 보호 프로토콜," 2008년 12월.
[17] 양연형, 김선영, 이필중, "개선된 수동형 RFID 보안태그와 리더의 인증 및 데이터 보호 프로토콜," 정보보호학회논문지, 20(1), pp. 85-93, 2010년 2월.
[18] 정보통신단체표준 TTAK.KO-12.0091/R1, "수동형 RFID 보안태그와 리더의 인증 및 데이터 보호 프로토콜," 2009년 12월.
[19] ISO/IEC, "ISO/IEC WD 29167 Information technology - Radio-Frequency Identification for item management - Part 1: Air interface for security services and file management for RFID - architecture," Jun. 2010.
[20] ISO/IEC, "ISO/IEC WD 29167 Information technology - Radio-Frequency Identification for item management - Part 6: Air interface for security services and file management for RFID at 860 - 960 MHz," Jun. 2010.
[21] 최용제, 최두호, 이상연, 정교일, "수동형 RFID를 위한 보안 기술 구현," 한국통신학회 하계종합학술발표회, pp. 96-99, 2008년 7월.

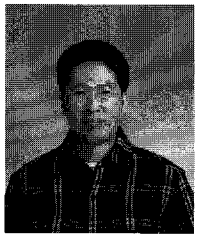
〈著者紹介〉

강 유 성 (You Sung Kang) 정회원
1997년 2월: 전남대학교 전자공학과 졸업
1999년 8월: 전남대학교 전자공학과 석사
1999년 11월~현재: 한국전자통신연구원 선임연구원
2005년 3월~현재: KAIST 전기및전자공학과 박사과정
〈관심분야〉 RFID/USN 보안, 부채널 분석, 보안 프로토콜

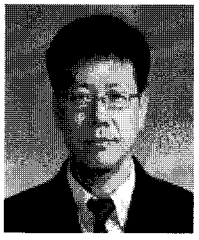
최 용 제 (Yong Je Choi) 정회원
1996년 8월: 전남대학교 전자공학과 졸업
1999년 2월: 전남대학교 전자공학과 석사
1999년 2월~8월: 전남대학교 전자통신연구소 인턴연구원
1999년 8월~현재: 한국전자통신연구원 선임연구원
〈관심분야〉 보안 프로세서 설계, 부채널 분석 시스템, RFID/USN 보안



최 두 호 (Doo Ho Choi) 정회원
1994년 2월: 성균관대학교 수학과 졸업
1996년 2월: KAIST 수학과 석사
2002년 2월: KAIST 수학과 박사
2002년 1월~현재: 한국전자통신연구원 선임연구원
〈관심분야〉 암호학, 부채널 분석, RFID/USN 보안



이 상 연 (Sang Yeoun Lee) 정회원
1996년 2월: 강원대학교 전자공학과 졸업
1998년 2월: 강원대학교 전자공학과 석사
2000년 10월~현재: 한국전자통신연구원 선임연구원
〈관심분야〉 RFID 보안태그, 전광통합망 기술



이 형 섭 (Heyung Sub Lee) 정회원
1985년 2월: 충남대학교 전자공학과 졸업
1994년 8월: 충남대학교 전자공학과 석사
2002년 8월: 충남대학교 전자공학과 박사
1990년 9월~현재: 한국전자통신연구원 팀장/책임연구원
1994년 8월: 정보통신 기술사
〈관심분야〉 RFID시스템, RFID/USN 보안, 통신망 프로토콜, 디지털 모뎀 설계