情 報 保 護 學 會 誌
第22卷 第1號, 2012. 2

수동형 UHF RFID 보안기술 국제 표준화 동향

강 유 성*, 최 두 호*, 조 현 숙*

요 약

최근 들어, 자동화된 사물인식을 위한 대표적인 저가 경량의 전자 장치인 수동형 UHF RFID 태그의 확산을 위한 보안 기술 표준화 논의가 활발하게 전개되고 있다. 본 고에서는 수동형 UHF RFID 보안기술 표준화와 관련된 ISO/IEC JTC1 SC31의 표준문서와 EPCglobal 기술규격 관계를 정리하고, 특히 향후에 ISO/IEC JTC1 SC31 회의에서 논의될 것으로 보이는 주요 제안기술들을 분석한다. 분석 대상이 되는 주요 기술들은 유럽, 북미, 아시아 등 다양한 지역의 기업에서 제안된 기술들로서, 본 고에서는 제안기술의 주요 특징을 소개하며 향후 국제 표준화 전망을 요약하면서 결론을 맺는다.

Ⅰ. 서 론

기존의 바코드를 대신하는 저가의 비접촉식 정보매체로 고려되고 있는 RFID(Radio Frequency Identification) 기술은 지난 10여년 동안 인식률 향상과 가격 경쟁력 확보에 주력해 왔다. 특히 900 MHz UHF(Ultra High Frequency) 대역의 수동형 RFID 태그 기술은 EPCglobal의 UHF Class 1 Generation 2(이하 Gen2) 통신 규격이 ISO/IEC 18000-6 국제 표준의 에어 인터페이스 핵심기술로 수용되면서 국제 표준 기술의 전세계적 상용화에 한걸음 더 다가가게 되었다[1],[2].

그러나, 수동형 UHF RFID 기술의 광범위한 활용이 더딘 가장 큰 이유는 보안 문제라 해도 과언이 아닐 정도로 최근 들어 많은 기업들의 관심이 보안 문제 해결에 집중되고 있다. 그동안 수동형 UHF RFID 보안 문제 해결을 위한 많은 연구결과가 있었던 것도 사실이다. 국내에서는 ISO/IEC 국제 표준화 활동과 연계된 보안기술 연구가 2010년 8월 정보보호학회 논문지를 통해 발표되기도 하였다[3]. [3]에서 언급된 바와 같이 국내외 수많은 보안 전문가들이 수동형 RFID 시스템에 적합한 보안기법을 제안하고 검증해 왔으며, 향후에도 새로운 보안기법들이 발표될 가능성도 크다. 이러한 수많은 연구결과들이 빛을 발하기 위해서 최근에는 국제 표준 회의에서 다양한 제안기술들이 경쟁을 펼치기 시작했다. 수동형 UHF RFID 보안기술과 관련된 국제 표준화 기구로는 공식적인 국제표준화 그룹인 ISO/IEC JTC1 SC31과 산업체의 사실상 표준화 그룹인 EPCglobal UHFAI(UHF Air Interface) WG이 있다.

본 고에서는 위에서 언급한 두 개의 국제 표준화 그룹에서 다루고 있는 표준 문서와 기술규격의 관계를 설명하고, 특히 최근에 ISO/IEC JTC1 SC31 표준 그룹에 제안되고 있는 북미, 유럽, 아시아 국가들의 제안기술들을 분석한다. 또한 제안된 기술들의 분석에 기반하여 향후 표준화 전망을 예측한다. 본 고의 구성은 다음과 같다. 제 II장에서 국제 표준화 그룹 소개 및 관련 문서의 관계를 설명하고, 제 III장에서는 국제표준 기술이 지켜야 할 요구사항을 정리한다. 제 IV장에서 ISO/IEC JTC1 SC31 표준 회의에서 논의될 주요 제안기술들을 분석하고, 제 V장에서 향후 국제 표준화 전망을 요약하면서 결론을 맺는다.

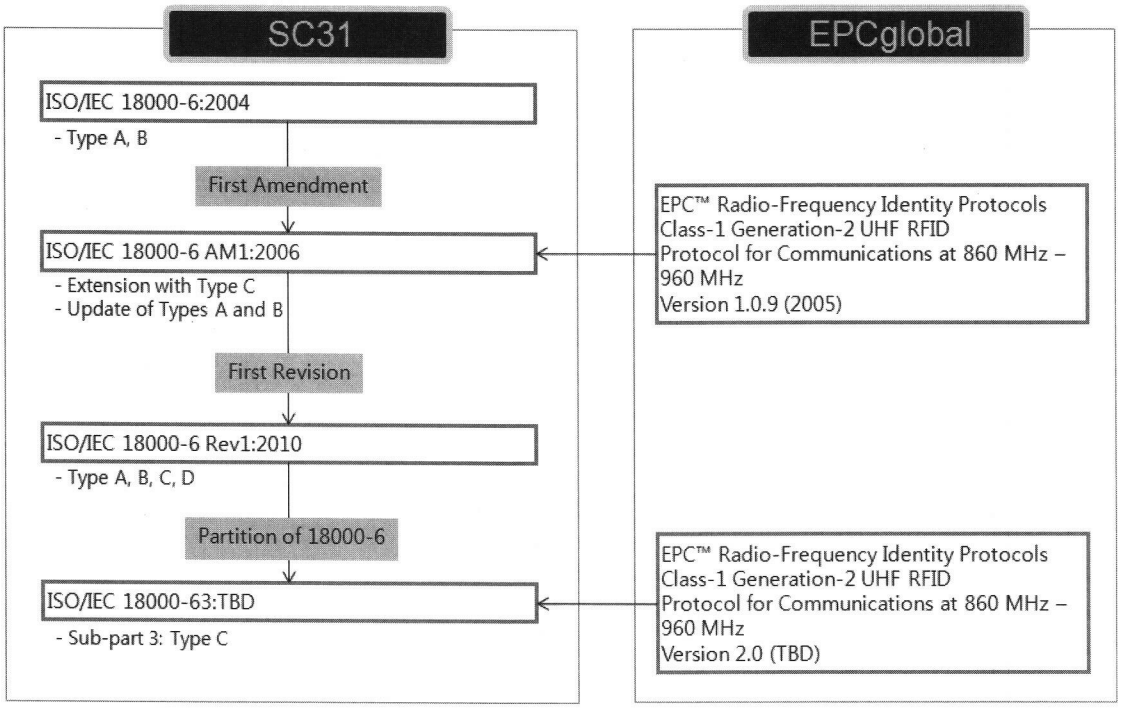
Ⅱ. 국제 표준화 그룹

2.1 ISO/IEC JTC1 SC31

ISO/IEC JTC1 SC31(이하 SC31)은 RFID 기술과 관련된 표준화를 담당하는 ISO/IEC JTC1 산하 분과위원회로서, "자동인식 및 데이터획득 기술(Auto Iden-

본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업의 일환으로 수행하였음. (초경량 저전력 RFID 보안 플랫폼 기술 개발).

* 한국전자통신연구원 사이버융합보안연구단 (youskang@etri.re.kr, dhchoi@etri.re.kr, hscho@etri.re.kr)



〔그림 1〕 ISO/IEC JTC1 SC31과 EPCglobal UHFAI WG의 표준 문서 관계도

tification and Data Capture Techniques)"의 표준화를 목표로 하고 있다. ISO/IEC JTC1에서 제정한 표준은 항상 ISO/IEC로 시작되는 문서번호를 갖는다. 즉, RFID 표준의 대표적인 문서인 RFID 에어 인터페이스 표준은 ISO/IEC 18000이며, 각 파트별로 ISO/IEC 18000-1 부터 ISO/IEC 18000-7까지의 규격번호를 갖는다. 그림 1은 수동형 UHF RFID 에어 인터페이스 기술에 대한 SC31 표준 문서와 EPCglobal 기술규격 사이의 관계도를 보인 것이다.

SC31 분과위원회 산하의 작업그룹(WG: Working Group)들 중 WG7이 보안서비스를 위한 RFID 태그와 리더의 에어 인터페이스 통신 규격을 만들고 있는 곳이다[4]. ISO/IEC JTC1 SC31 WG7(이하 WG7)은 "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 표준 문서에서 RFID 보안 프레임워크 및 보안 서비스 등을 정의하고 있으며, ISO/IEC 29167-10, 11, 12, 13, 14 등의 표준 문서에서 UHF 대역의 수동형 RFID 보안 기술 및 파일관리 기술의 표준화를 추진하고 있다. 회의는 비정기적으로 개최되며, 일반적으로 차기 2~3회까지의 회의 일정을 미리 계획해 놓는다. 계획된 일정이라 하더라도 논의사항이 긴급한 것이 아니라고 판단되면 취소되기도 한다. WG7 회의와 더불어 반드시 표준화 현황을 파악해야 할 곳이 WG4 SG3 표준화 그룹이다. 수동형 UHF RFID 보안기술 표준화 관점에서 두 그룹의 관계를 정리하면 다음과 같다.

- WG4 SG3 : 각 주파수별 PHY/MAC 규격을 제정하면서 보안 프로토콜이 동작할 수 있는 Command/Response 포맷을 정의함. 즉, 프레임워크를 제공하는 표준임.(예를 들면, ISO/IEC 18000-63 표준 문서에서 Authenticate, SecureChannel 등의 신규 명령어 구조를 정의하고 있음.) WG4 SG3에서는 지난 2004년에 각 주파수 대역별로 태그와 리더의 통신을 위한 물리계층 특성과 데이터링크 계층 명령어 포맷을 규정하였음. 그리고, 각 주파수별 표준에 센서 기능과 배터리 지원 기능을 포함시킨 형태로 리비전 버전도 완료하였음. 현재는 보안기술과 파일관리 서비스를 지원하기 위해 리비전을 추구하고 있는 상황이며, 표 1은 WG4 SG3에서 작

〔표 1〕 ISO/IEC JTC1 SC31 WG4 SG3 표준 문서 요약

규격번호	Project	현단계	주도 국가 또는 기업
ISO/IEC 18001	Application requirement profiles	IS	미국 QED
ISO/IEC 18000-1	Reference architecture and definition of parameters to be standardized	REV1 IS	미국
ISO/IEC 18000-2	Parameters for air interface communications below 135 kHz	REV1 IS	유럽
ISO/IEC 18000-3	Parameters for air interface communications at 13,56 MHz	REV2 IS	네덜란드 NXP
ISO/IEC 18000-4	Parameters for air interface communications at 2.45 GHz	REV1 IS	오스트리아 CISC
ISO/IEC 18000-6	Parameters for air interface communications at 860 MHz to 960 MHz	REV1 IS REV2 WD	미국 임핀지, 오스트리아 CISC
ISO/IEC 18000-61	Parameters for air interface communications at 860 MHz to 960 MHz - Sub Part 1: Type A	WD	유럽
ISO/IEC 18000-62	Parameters for air interface communications at 860 MHz to 960 MHz - Sub Part 1: Type B	WD	유럽
ISO/IEC 18000-63	Parameters for air interface communications at 860 MHz to 960 MHz - Sub Part 1: Type C	WD	미국 임핀지, EPCglobal, 오스트리아 CISC
ISO/IEC 18000-64	Parameters for air interface communications at 860 MHz to 960 MHz - Sub Part 1: Type D	WD	영국, 남아공
ISO/IEC 18000-7	Parameters for air interface communications at 433 MHz	REV3 CD	미국 사비, 오스트리아 CISC
ISO/IEC 24710	Elementary tag license plate functionality for ISO/IEC 18000 air interface definitions	Withdrawn	영국

(약어설명)
IS (International Standard, 국제표준), REV1 (The first revision), REV2 (The second revision), WD (Working Draft, 작업초안), CD (Committee Draft, 위원회초안), Withdrawn (철회)

업 중인 표준문서 현황임.

- WG7 : WG4 SG3에서 개발한 표준 문서에 정의된 Command/Response 포맷을 활용하는 구체적인 보안 프로토콜, 암호 알고리즘, 키 관리 기법 등의 보안기술 표준 문서를 개발함.(예를 들면, ISO/IEC 29167-10 표준 문서에서 AES-128 암호 알고리즘을 사용하여 인증, 데이터 보호 등의 보안 서비스를 제공하는 보안기술을 정의함.) WG7에서는 WG4 SG3에서 정의된 RFID 에어 인터페이스와 호환되는 보안기술 정의를 목표로 하고 있으며, 표 2는 WG7의 표준 문서 현황임.

2.2 GS1 EPCglobal UHFAI WG

SC31 WG7이 국가대표단이 모여 공인된 국제표준을 제정하는 곳이라면, EPCglobal은 산업체 대표들이 상용제품에 탑재할 사실상 표준(De Facto Standard)을 제정하는 곳이다. 따라서 WG7과 EPCglobal은 서로 견제 및 협력을 해야 하는 상황이며, 멤버들 중 상당수는 겹치는 경우가 많다.

EPCglobal UHFAI WG은 EPCglobal에서 900 MHz UHF 대역의 수동형 RFID 태그의 에어 인터페이스 규격 정의를 담당하고 있는 작업그룹으로서 보안기술도 여기서 논의되고 있다. 이 작업그룹이 정의한 규격과 WG7에서 정의하는 국제표준이 서로 충돌되지 않아야 한다는 것이 양측의 암묵적인 동의이다. 대부분의 표준화 멤버들이 WG7과 더불어 EPCglobal 회의에 참석하게 된 배경도 이러한 이유 때문이다. 2011년에는 보안기술 및 파일관리 기술을 정의하고자 매주 텔레컨퍼런스와 두 달에 한번 대면회의를 개최하는 등 매우 활발한 활동을 펼쳤다. 그 결과 EPCglobal Gen2 Version 2.0 드래프트 문서가 거의 완성되어 가고 있다. 이 문서

〔표 2〕 ISO/IEC JTC1 SC31 WG7 표준 문서 요약

규격번호	Project	현단계	관련 기업
ISO/IEC 29167-1	Air Interface for security services and file management for RFID architecture	FDIS	네덜란드 NXP, 오스트리아 CISC
ISO/IEC 29167-3	Air Interface for security services and file management for RFID at 13.56 MHz	Withdrawn	네덜란드 NXP
ISO/IEC 29167-6	Air Interface for security services and file management for RFID at 860-960 MHz	Withdrawn	한국 ETRI
ISO/IEC 29167-10	Automatic identification and data capture techniques - Part 10: Air Interface for security services crypto suite AES128	WD	네덜란드 NXP, 벨기에 NXP
ISO/IEC 29167-11	Automatic identification and data capture techniques - Part 11: Air Interface for security services crypto suite Present	WD	네덜란드 NXP, 벨기에 NXP
ISO/IEC 29167-12	Automatic identification and data capture techniques - Part 12: Air Interface for security services crypto suite ECC	WD	네덜란드 NXP, 벨기에 NXP
ISO/IEC 29167-13(예정)	Automatic identification and data capture techniques - Part 13: Air Interface for security services crypto suite Grain-128A	NWIP	스위스 EM
ISO/IEC 29167-14(예정)	Automatic identification and data capture techniques - Part 14: Air Interface for security services crypto suite - AES OFB-like	NWIP	한국 ETRI

(약어설명)
FDIS(Final Draft International Standard, 최종초안 국제표준), WD(Working Draft, 작업초안), NWIP(New Work Item Proposal, 신규 작업 아이템 제안), Withdrawn(철회)

에는 구체적인 보안기술이 정의되는 것이 아니라 보안 기술을 담을 수 있는 프레임워크(즉, 보안 관련 명령어 포맷, 보안 관련 동작에 따른 상태 천이, 에러 코드 등)가 포함될 예정이다.

구체적인 보안기술, 즉 암호 알고리즘, 보안 프로토콜, 키 관리 메커니즘 정의는 WG7의 역할이며, WG7과 EPCglobal의 합의하에 WG7의 보안기술이 EPCglobal Gen2 Version 2.0 프레임워크를 준용하여 동작될 수 있도록 정의될 것이다. 물론, EPCglobal Gen2 Version 2.0 규격 자체도 WG4 SG3에서 ISO/ IEC 18000-63 국제표준으로 제정될 예정이다.

Ⅲ. 국제표준 요구사항

WG7에서 제정하고 있는 ISO/IEC 29167-1 문서에서는 ISO/IEC 29167 시리즈가 해결해야 할 보안 요구사항을 정의하고 있다[5]. 여기서는 참고문헌 [3]의 내용을 바탕으로 하여 ISO/IEC 29167-1 최신 문서에서 정의한 내용을 참조하여 보안 요구사항을 재구성하였다.

3.1 보안 요구사항

WG7에서 논의를 끝마친 RFID 보안 프레임워크 표준 문서인 [5]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): 태그 아이디의 전부 또는 일부를 감출 수 있는 보안 서비스.
- Certify authenticity(진품 검증): 하나 또는 다수의 에어 인터페이스 명령어를 이용하여 태그가 진품임을 인증하는 증명을 제공할 수 있는 서비스.
- Secure access to tag data and functions(태그 데이터와 기능에 대한 안전한 접근) : 태그 데이터 접근 제어와 기능 설정 접근 제어를 제공하며, 또한 전송 데이터가 안전하게 통신할 수 있는 서비스

- Key management(키 관리) : 보안 키가 안전하게 전달되거나 또는 안전하게 저장되어 관리되는 서비스

3.2 구현 요구사항

수동형 UHF 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 UHF RFID 칩 면적은 대략적으로 0.45 mm x 0.45 mm 즉, 202.5 μm^2 면적을 가지는 것으로 평가되고 있다. 여기서 절반은 아날로그 파트가 활용해야 하므로 디지털 파트가 가질 수 있는 면적은 101.25 μm^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 μs이다. 따라서 태그는 이러한 제약조건을 고려한 동작 주파수 확보 및 암호 연산 구현이 요구된다.

Ⅳ. 주요 제안기술

2012년 1월 현재 WG7은 8차에 걸친 공식 회의를 통해 RFID 보안 서비스 제공에 필요한 요구사항을 만족하는 표준 기술을 정의하고자 노력하고 있다. 표 3은 지난 2009년부터 2011년까지 개최된 WG7 회의에 대하여 간략하게 정리한 것이다.

WG7의 최초 계획은 ISO/IEC 18000 시리즈처럼 주파수 대역별 에어 인터페이스와 관련한 보안기술을 제정하는 것이었다. 그에 따라 13.56 MHz 보안기술은 ISO/IEC 29167-3, 그리고 900 MHz 보안기술은 ISO/IEC 29167-6에서 정의하고자 하였다. 그러나, 900 MHz UHF RFID 보안 서비스를 위한 후보기술들이 너무 많이 제안되었고 공통의 합의점을 찾지 못하여 하나의 표준 문서에서 모두 수용하기 어렵게 되자, 결국 WG7은 ISO/IEC 29167-6을 철회하고 후보기술들을 각각 별도의 표준으로 제안하도록 권고하였다. 그리고 새롭게 제안될 표준들은 신규제안 투표를 통과한 순서대로 표준문서 번호를 ISO/IEC 29167-10부터 부여하기로 합의하였다. 본 고가 작성된 시점인 2012년 1월 현재는 오스트리아에서 제안한 3개의 기술이 ISO/IEC 29167-10, 11, 12의 표준번호를 부여받고 WD(Working Draft, 작업초안) 작성 단계에 와 있다. 그리고, 스위스에서 제안한 NP(New Proposal, 신규제안서)와 한국에서 제안한 NP가 각각 NP 투표 진행 중에 있다.

본 장에서는 이미 표준번호를 부여받은 3개의 오스트리아 제안기술, 공식 제안되어 투표가 진행 중인 스위스 제안기술과 한국 제안기술, 그리고 그동안 WG7 표준회의에서 논의되었던 또 다른 5개의 후보기술 등 총 10개의 기술에 대하여 간략하게 요약한다.

4.1 ISO/IEC 29167-10(AES-128)

3건의 오스트리아 제안기술들은 실질적으로는 모두

〔표 3〕 ISO/IEC JTC1 SC31 WG7 회의 요약

순번	회의 차수	일시	장소	핵심 내용
1	준비회의	2009년 6월	호주 시드니	ISO/IEC 29167 표준화 시작
2	제 1차	2009년 8월	영국 런던	13.56 MHz 대역과 900 MHz 대역 표준화 분리
3	제 2차	2010년 3월	한국 제주	한국 ETRI의 ISO/IEC 29167-6 에디터 진출
4	제 3차	2010년 5월	중국 베이징	임핀지, NXP, ETRI 등 주요 세력 경쟁
5	제 4차	2010년 9월	프랑스 툴루즈	WG7과 EPCglobal 밀접한 협력 합의
6	제 5차	2010년 11월	미국 페어팩스	보안 프레임워크, 보안 아키텍처 논의
7	제 6차	2011년 2월	미국 사라소타	ISO/IEC 29167-3, 29167-6 철회 여부 논의
8	제 7차	2011년 8월	영국 런던	ISO/IEC 29167-3, 29167-6 철회 결정
9	제 8차	2011년 11월	미국 페어팩스	새롭게 제안된 10개의 후보기술 발표
10	제 9차	2012년 2월	텔레컨퍼런스 (예정)	공식투표를 통과한 5개 후보기술 논의 (예정)

NXP 기업의 기술이다. 어떠한 연유에서 오스트리아 대표단이 공식 제안자 역할을 하고 있는지는 공개되지 않았지만, WG7 표준회의에서는 ISO/IEC 29167-10, 11, 12에 대해서 네덜란드 NXP 소속의 참석자가 기술 발표 및 표준화 추진 의사를 보였다.

ISO/IEC 29167-10은 AES-128 알고리즘을 사용하고 있으며, 인증(태그 인증, 리더 인증, 상호 인증) 및 데이터 보호 기능을 제공한다. 보안 프로토콜 측면에서는 운영모드(mode of operation)를 다양하게 적용하여 데이터 보호 및 메시지 인증 서비스를 제공할 수 있도록 설계되었다[6]. NXP의 IC 카드 기반 보안 솔루션을 바탕으로 한 제안으로 판단되며, 향후 표준화 과정에서 수동형 RFID 태그에서 실제로 CBC-MAC(Cipher Block Chaining - Message Authentication Code)처럼 연산 부담이 큰 운영모드 구현 가능성에 대한 논란이 있을 것으로 예상된다.

4.2 ISO/IEC 29167-11(PRESENT-80)

ISO/IEC 29167-11 역시 NXP 제안기술이며, 사용되는 알고리즘은 PRESENT이다. NXP에서는 AES 알고리즘 이외에 수동형 RFID 태그에 적합한 경량의 보안 알고리즘으로서 PRESENT를 선택한 것으로 판단된다. 사용되는 키 길이는 80 비트를 제안하고 있으며, 기능적으로는 ISO/IEC 29167-10과 동일하다.

4.3 ISO/IEC 29167-12(ECC)

ISO/IEC 29167-12 역시 NXP 제안기술이며, 사용되는 알고리즘은 비대칭키 알고리즘인 ECC(Elliptic Curve Cryptography)이다. 키 관리 효율성을 고려한 것으로 보이며, 오직 태그 인증 기능만을 제공한다. 비대칭키 기반의 제안기술 역시 향후 표준화 과정에서 수동형 RFID 태그에 구현 가능할지에 대한 논란이 있을 것으로 예상된다.

4.4 ISO/IEC 29167-13(Grain-128A)

현재 투표가 진행 중인 스위스 제안기술은 투표 성공 시 ISO/IEC 29167-13이 될 것이다. 이 기술은 EM 기업의 제안기술이며, 사용되는 알고리즘은 Grain-128A이다. Grain-128A는 Grain-128을 향상시킨 스트림 암호이며, 기능적으로는 태그와 리더의 상호 인증을 필수 구현 기능으로 정의하고 있다. 태그 인증, 리더 인증 및 데이터 보호 기능은 선택 구현사항으로 정의하고 있다[7].

4.5 ISO/IEC 29167-14(AES-OFB like)

한국 제안기술 역시 2012년 1월 현재 투표가 진행 중이며, 투표 성공 시 ISO/IEC 29167-14가 될 것이다. 이 기술은 ETRI에서 제안한 기술로서, 사용되는 알고리즘은 AES-128이다. 한국 제안기술은 기존의 ISO/IEC 29167-6 WD의 Proposal A로써 표준화가 진행되던 내용이다.

수동형 UHF RFID 태그의 응답시간 조건을 만족하면서 인증(태그 인증, 리더 인증, 상호 인증), 보안 채널 생성 및 효율적인 키 관리 기능을 제공하고 있다[8]. 주요 특징으로는 OFB(Output Feedback) 모드를 변형하여 데이터 암복호화를 효율적으로 수행하도록 구성하였으며, 암호화 모듈만으로 암호화 및 복호화를 수행할 수 있어서 칩 구현 면적을 줄일 수 있는 장점을 가지고 있다. 국제 표준화 추진 과정에서 EPCglobal 기술규격과의 호환을 위하여 메시지 포맷 내부에서 작은 변화들이 있긴 하지만, 기본적인 뼈대는 참고문헌 [3]의 내용을 기반으로 하고 있다.

4.6 미국 제안기술 A(HB2-128)

아직 공식적으로 투표가 진행되지는 않았지만 WG7 회의에서 발표되었던 후보 기술 중 하나는 미국 Revere Security 기업이 제안한 Hummingbird 알고리즘에 기반한 HB2-128이다[9]. HB2-128 알고리즘은 128비트 키 길이를 사용하는 대칭키 블록 암호이며, 수동형 RFID 태그에 적합하도록 경량 구현이 가능하다는 장점이 있다. 기능적으로는 AES-128 암호가 제공할 수 있는 모든 기능을 대체할 수 있지만, 미국 Revere Security에서 독자적으로 개발한 암호로서 향후 표준화 과정에서 IPR 이슈가 크게 부각될 것으로 예상되는 제안기술이다.

4.7 미국 제안기술 B(AE)

제 8차 WG7 회의에서 미국 SecureRF는 수동형 RFID 태그에 적합한 암호 알고리즘으로 AE™(Algebraic Eraser™)를 발표하였다. 미국 SecureRF는 제안된 AE가 RSA와 ECC 보다 효율적인 공개키 기반 구조

를 구성할 수 있으며, 더 적은 면적으로 구현 가능한 장점이 있다고 강조하였다. 미국 Revere Security의 Hummingbird 경우와 마찬가지로 AE는 미국 SecureRF의 독자 개발 기술로서 향후 IPR 이슈가 큰 문제가 될 것으로 예상된다.

4.8 브라질 제안기술(AES-CTR)

브라질의 VBC(Wernher von Braun Center for Advanced Research)에서는 AES-CTR(Counter) 모드를 수동형 RFID 태그에 적용할 수 있다고 주장하였다[10]. 이는 다양한 운영모드 중 하나인 AES-CTR 역시 후보가 될 수 있다는 주장이다. AES-CTR 모드는 AES-OFB 모드처럼 암호화 모듈만으로 암호화와 복호화를 수행할 수 있는 특징을 가지고 있다.

4.9 중국 제안기술 A(ECC)

아시아권에서 제안된 기술로는 한국 이외에 중국에서 제안한 2개의 기술이 있다. 그 중 하나가 ECC 알고리즘을 사용하는 기술이다. ECC 알고리즘을 이용하여 상호 인증 및 세션 키 교환을 수행하는 프로토콜을 제안하고 있다[11]. 중국의 ECC 제안기술은 ISO/IEC 29167-12와 마찬가지로 구현 가능성 및 효율성 측면에서 많은 검토가 필요할 것으로 보인다.

4.10 중국 제안기술 B(XOR)

중국의 또 다른 제안은 매우 간단한 XOR 활용 프로토콜이다[12]. 이는 한국 제안기술인 AES-OFB like 모드를 변형한 것인데, 한국 제안기술은 RFID 태그에서 AES 암호화 모듈을 구동시켜 세션 키를 설립하여 인증 프로토콜에 사용하는 반면, 중국 XOR 제안기술은 별도의 세션 키 설립 없이 마스터 키를 사용하여 인증용 challenge를 직접 XOR하는 방법을 채택하고 있다. 따라서 당연히 보안상 취약점이 존재하지만, 제안 기업인 IWNCOMM에서는 매우 간단하게 사용할 수 있음을 강조하면서 후보기술이 될 수 있다고 주장하고 있다.

V. 결 론

본 고에서는 2012년 1월 현재 활발하게 국제 표준화가 진행 중인 WG7의 수동형 RFID 보안기술 표준화 관련 제안기술들에 대하여 간략하게 정리하였다.

EPCglobal은 사실상 산업체 표준인 Gen2 Version 2.0 기술규격을 정의하고 있으며, 이 기술규격은 향후에 WG4 SG3를 통해 ISO/IEC 18000-63으로 승인될 전망이다. 이에 따라 RFID 보안기술을 논의하는 WG7에서는 Gen2 Version 2.0의 표준화와 밀접하게 협력하고 있으며, 이 기술규격에 호환되는 보안기술을 표준화하고자 노력하고 있다.

유럽의 NXP와 한국의 ETRI가 비교적 신속하게 대응하고 있으며, 미국 기업들은 독자적인 기술을 앞세워 표준화를 추진하고 있다. 이미 제안 되었거나 앞으로 제안될 10여건의 후보기술들은 각각의 표준번호를 부여받아 국제 표준 문서로 등록될 가능성이 높다. 하지만 실제 생산 기업 또는 서비스 기업에서 Gen2 Version 2.0 기술규격을 준용하는 수동형 UHF RFID 태그를 제작할 때 포함될 보안기술은 결국 구현 가능성, 성능 및 가격 경쟁력 등에서 앞서는 기술이 선택될 것으로 판단된다.

수동형 UHF RFID 서비스의 본격적인 활성화를 위한 보안기술 표준화는 앞으로 급물살을 탈 것으로 보이며, 그 후보 또한 10여개 기술에 달할 것으로 보인다. 수동형 UHF RFID 보안기술이 향후 서비스 활성화에 기여할 파급력을 고려할 때, 본 고의 내용이 독자들에게 보안기술 표준화에 대한 현 상황의 이해에 도움이 되기를 기대한다.

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," 2006.

[2] EPCglobal, "EPC™ Radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz - 960 MHz version 1.0.9", 2004.

[3] 강유성, 최용제, 최두호, 이상연, 이형섭, "UHF 수동형 RFID 시스템에 적합한 경량 고속의 보안 프로토콜 설계 및 구현", *정보보호학회논문지*, 20(4), pp. 117-134, August 2010.

[4] 강유성, 최두호, 김정녀, 조현숙, "RFID 정보보안 서비스를 위한 통신규격 표준화 동향", *한국정보기술학회지*, 8(1), pp. 43-49, November 2012.

[5] ISO/IEC, "ISO/IEC FDIS 29167-1 Information technology - Radio-Frequency Identification for item management - Part 1: Air interface for security services and file management for RFID - architecture," August 2011.

[6] NXP Semiconductors & Wernher von Braun Center for Advanced Research, "Joint NXP/VBC AES-Crypto-Suite Proposal, Version 2.2", WG7_201108_195, July 25, 2011.

[7] EM Microelectronic - Marin S.A, "Grain-128A Cryptographic Suite Proposal, Version 4.0", WG7_201110_210, September 30, 2011.

[8] ETRI, "Information technology - Automatic identification and data capture techniques - Part xx: Air Interface for security services crypto suite - AES OFB-like", WG7_201110_218, October 1, 2011.

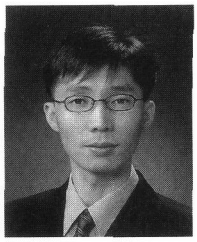
[9] Revere Security, "HB2-128 Crypto-Suite Proposal", WG7_201110_208, September 16, 2011.

[10] Wernher von Braun Center for Advanced Research, "AES-CTR Proposal: Add AES-CTR mode as Supported Crypto-Suite to ISO 29167-6", WG7_201110_212, November 17, 2010.

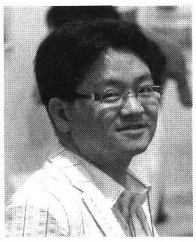
[11] IWNCOMM, "The Draft Specification of ECC Crypto Suite", WG7_201110_214, October 1, 2011.

[12] IWNCOMM, "The Draft Specification of XOR Crypto Suite", WG7_201110_215, October 1, 2011.

〈著者紹介〉



강 유 성 (Yousung Kang)
정회원
1997년 2월 : 전남대학교 전자공학과 졸업
1999년 8월 : 전남대학교 전자공학과 석사
2005년 3월~현재 : KAIST 전기 및 전자공학과 박사과정
1999년 11월~현재 : 한국전자통신연구원 선임연구원
<관심분야> RFID/USN보안, 부채널 분석, 보안 프로토콜



최 두 호 (Dooho Choi)
정회원
1994년 2월 : 성균관대학교 수학과 졸업
1996년 2월 : KAIST 수학과 석사
2002년 2월 : KAIST 수학과 박사
2002년 1월~현재 : 한국전자통신연구원 팀장/선임연구원
<관심분야> 암호학, 부채널 분석, RFID/USN보안

조 현 숙 (Hyun Sook Cho)
정회원
1979년 2월 : 전남대학교 수학교육과 졸업
1989년 2월 : 충북대학교 컴퓨터과학과 석사
2001년 2월 : 충북대학교 컴퓨터과학과 박사
1982년 ~현재 : 한국전자통신연구원 단장/책임연구원
<관심분야> 암호학, 보안 프로토콜, 네트워크 보안