한국산학기술학회논문지
Vol. 10, No. 2, pp. 351-357, 2009

홈 네트워크에서 RFID를 이용한 디바이스 간 디지털 콘텐츠 이동에 관한 연구

김은환[1*], 정용훈[2], 전문석[3]

A Study on Convenient Move of Digital Contents Between Devices Using RFID in Home Network

Eun-Hwan Kim[1*], Yong-Hoon Jung[2] and Moon-Seog Jun[3]

요 약 홈 네트워크는 가정 내의 가전기기들이 모여 하나의 네트워크를 이루는 것으로 가전기기들의 발전함에 따라 확장되어 가고 있으며, 또한 디지털 콘텐츠의 수도 무수히 증가하고 있다. 그러나 콘텐츠 가전기기 사이에 사용 운영성 부족으로 디지털 콘텐츠의 지속적인 저작권 보호가 힘들 뿐 아니라, 가전기기 간에 콘텐츠 이동을 위해서는 DRM 서버로부터 라이선스를 재발급 받아야 한다. 홈 네트워크 안에서 디바이스 상호 인증을 통해 콘텐츠를 다른 디바이스로 자유롭게 이동 할 수 있는 프레임워크를 제안하며, DRM 서버의 라이선스 관리 부담을 줄이고 외부의 사용자가 홈 네트워크에 접근하더라도 디바이스 인증을 통해 콘텐츠 사용이 가능한 시스템을 제안한다.

Abstract Home network is a network composed of devices in home and is being expanded by evolving devices. Also, The number of digital contents in home network has been increasing steadily. But it is difficult to continually protect the rights of digital contents due to lack of interoperability among contents devices. Besides, a license has to be re-issued by DRM sever for contents transfer between devices. Thus, this paper proposes framework which can freely transfer and contents to another device through mutual device authentication and a system that can decrease overload of license management of the DRM sever and that enable device outside home network to use contents through user authentication.

Key Words : Home network, DRM, RFID, Device Authentication

1. 서론

인터넷의 확산과 컴퓨터 상호연결성의 증대로 디지털 자원에 대한 유통 환경이 급속히 변화함에 따라 온라인 음악, 동영상, e-Book 등 디지털콘텐츠의 유통이 활발해지면서 디지털콘텐츠 산업이 미래의 핵심 산업으로 각광을 받았으나 P2P 등의 무차별 공유 서비스로 인해 디지털콘텐츠 산업은 오랜 기간 동안 정체상태를 벗어나지 못하고 있다. 이러한 디지털콘텐츠의 불법복제 기승으로 인해 기존 오프라인 또는 아날로그 콘텐츠의 유통 구조를 장악하던 음반사 또는 영화제작사 등은 심한 타격을 받게 되었으며, 이들 콘텐츠 공급자들은 궁여지책으로 P2P 사이트에 대하여 불법복제 조장이라는 명목으로 소송을 제기하는 한편 인터넷을 통한 어떠한 형태의 디지털콘텐츠 유통 서비스도 강하게 반발하고 있다[1].

현재 DRM 벤더별 독자적인 기술규격 사용으로 디지털 콘텐츠 및 디지털 기기의 상호 호환성이 보장되고 있지 않으며, 지속적인 디지털 콘텐츠의 권리는 보장할 수 있지만 사용자가 콘텐츠를 사용하기 위해서는 많은 제한 및 불편함이 따른다. 미국의 InterTrust 사는 지속적인 저작권 보호를 위한 콘텐츠 분배 기술로 Superdistribution을 제안하였다.

Superdistribution은 사용자가 콘텐츠를 획득 하더라도 인증된 사용자만이 콘텐츠의 라이선스를 받아 사용할 수 있는 기술이다[2]. 이때 라이선스는 디바이스와 바인딩 되어 있으므로, 콘텐츠를 사용하기 위해서는 인증 받은

[1]숭실대학교 전산원(교수)
[2]숭실대학교 컴퓨터학과(박사과정)
[3]숭실대학교 컴퓨터학부(교수)
*교신저자: 김은환(ehkim@ssuci.ac.kr)
접수일 08년 12월 20일 수정일 09년 01월 26일 게재확정일 09년 02월 18일

디바이스 외에 다른 디바이스에서 콘텐츠를 사용할 수 없게 된다. 결국 사용자가 콘텐츠 제공자로부터 구입한 콘텐츠는 최초에 다운로드받은 디바이스 외에 자신이 소유하고 있는 다른 디바이로 콘텐츠를 이동하기 위해서는 DRM 서버로부터 다시 인증 받아야 하는 불편함이 생긴다[3][6].

본 논문에서는 홈 디바이스들 간에 상호 인증을 통하여 자유롭게 콘텐츠 이동이 가능하도록 함으로써 콘텐츠 이동시 DRM 서버로부터 새롭게 사용자 인증과 License를 발급 받아야 하는 불편함을 제거하고. 오프라인에서도 지속적인 콘텐츠 저작권 보호가 가능한 시스템을 제안하였다.

2. 관련 연구

2.1 콘텐츠 보호 기술

디지털 콘텐츠는 비 손실 복제가 가능하며 디지털 정보 일부의 재사용이 가능하기 때문에 불법복제 및 불법 수정으로부터 저작자를 보호하기위한 안전한 디지털 저작권 보호 시스템의 개발이 필요하다. 그러므로 DRM 시스템에 대한 많은 연구와 솔루션 개발이 활발히 진행되고 있다.

콘텐츠의 기밀성과 무결성 확보를 위하여 암호기술을 중심으로 발전하여 왔으며 저작권에 대한 내용을 명시하기 위하여 XrML(eXtensible rights Markup Language)을 기반으로 표준화가 진전되고 있으며 식별자 부여를 위해서는 DOI(Digital Object Identifier)를 적극 활용해나가는 추세다. 최근 디지털 저작권 보호에 대한 관심이 커짐에 따라 DRM 솔루션을 제공하는 업체로는 세계시장의 50% 이상을 점유하고 있는 InterTrust사가 DRM 솔루션을 제공하고 있으며, Microsoft 사가 자사의 프로그램인 윈도우 미디어 플레이어에 DRM 기술을 적용한 솔루션을 제공하고 있다[4][5].

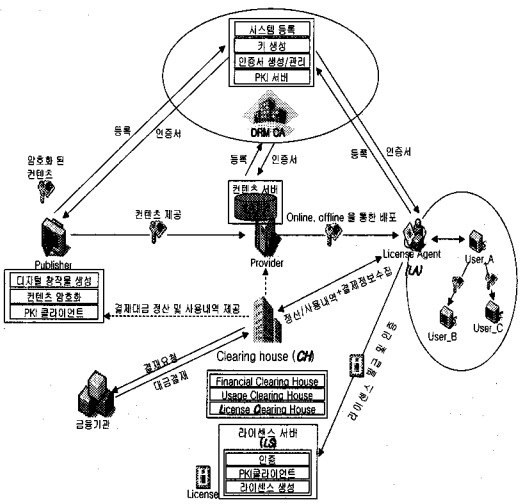
2.2 라이선스 구조

라이선스는 라이선스 일련 번호 sn, 라이선스 발행시간 date, 사용규칙 Usage rule, 라이선스 하드웨어 바인딩 정보인 KID = H(DID||LSID), 기타 필요한 정보를 포함한 Other_data를 포함한다. 여기서 DID는 사용자의 하드웨어 장치 ID를, LSID는 라이선스 서버의 ID를 의미한다. 무결성, 부인방지를 위해 이러한 파라미터들을 해쉬 함수 H로 처리하고 라이선스 서버의 개인키로 암호화 하여 서명을 한다[7].

License = {sn, KID, date, Usage rule, other_data, SigLS(H(sn, KID,date, Usage rule, other_data))}

2.3 DRM 시스템의 구성

DRM 시스템은 그림 1과 같이 출판업자와 콘텐츠 공급업자, 사용자, 그리고 클리어링 하우스(Clearing house) 등으로 구성되고 세부 기능은 다음과 같다[7].

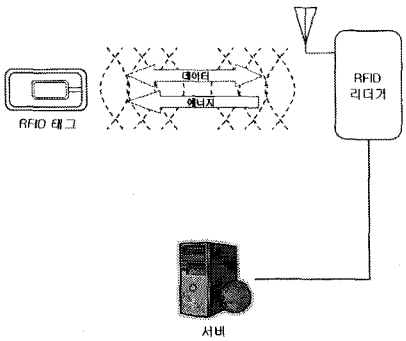


[그림 1] DRM 시스템의 구성

전체 DRM 시스템의 참여자들은 DRM CA로부터 공개키를 등록하고 인증서를 발급 받는다. 콘텐츠 출판업자는 콘텐츠 제공자에게 보호조건, 저작권, 사용조건, 인증정보, 사용 비용, 사용 추적 조건 등을 명시하고 분배 업자에게 전송한다. 콘텐츠 분배 업자는 출판업자가 제공한 보호조건에 맞도록 암호화 하여 암호화된 콘텐츠를 생성한다. 암호화된 콘텐츠는 콘텐츠를 이용하고자 하는 사용자에게 온라인 혹은 오프라인을 통하여 배포된다. 또한 분배 업자는 콘텐츠에 대한 가격, 결제 처리 방법 등을 정한 후 해당 정보를 데이터베이스에 저장하고 클리어링 하우스에 전송하여 사용자에 대한 결제 정보를 처리 할 수 있도록 한다. 사용자는 온라인이나 오프라인을 통해 다운로드 받은 콘텐츠는 암호화 되어 있기 때문에, 콘텐츠를 이용하기 위해서 라이선스 에이전트를 통해 클리어링 하우스로부터 라이선스를 발급받고 해당 라이선스를 클리어링 하우스를 통하여 인증한 후 결제 정보를 제공하면 라이선스 에이전트가 콘텐츠를 사용할 수 있도록 처리를 수행하게 된다.

2.4 RFID 시스템

RFID는 마이크로칩을 내장한 태그(tag), 레이블, 카드 등에 저장된 데이터를 무선 주파수를 이용한 리더에서 자동 인식하는 기술이다. 이러한 RFID 시스템은 태그(Tag), 리더(Reader), 백엔드 서버(Back-end-Server)등 3가지 구성 요소로 이루어진다.



[그림 2] RFID 시스템

2.4.1 태그(Tag)

태그(Tag)는 사람과 사물, 동물 등에 부착하여 그 사물에 대한 직접적 혹은 간접적인 식별 및 인식 정보를 송신하는 장치이다. 일반적으로 태그는 한 개의 IC 칩과 한 개의 안테나(antenna)로 구성되어 있다. 태그는 크게 능동형 태그(Active Tag)와 수동형 태그(Passive Tag)로 분류될 수 있다.

2.4.2 리더(reader)

RFID 리더는 태그의 정보를 읽어내기 위해 태그와 송수신하는 장치이며, 태그에서 수집된 정보를 미들웨어로 전송하는 기능을 한다. RFID 리더는 RF 아날로그부와 디지털 신호처리 제어부로 구성된다.

리더가 전체 RFID 시스템에서 하는 역할은 태그에게 정보 요청 신호를 보내고 태그로부터 받은 정보를 자체 서브시스템이나 외부 백엔드 서버 시스템을 이용하여 태그를 식별하는 것이다.

2.4.3 백엔드 서버(Back-end-Server)

백엔드 서버는 다수의 리더로부터 전송된 태그 정보에 대한 처리를 해주는 서버 시스템이다. 백엔드 서버에서는 태그와 관련된 정보를 데이터베이스화해서 관리하고 있으며 효율성을 위해서 여러 개의 서버로 분산 운영될 수도 있다. 백엔드 서버는 보안 측면에서 신뢰할 수 있는 시스템으로 간주된다[2].

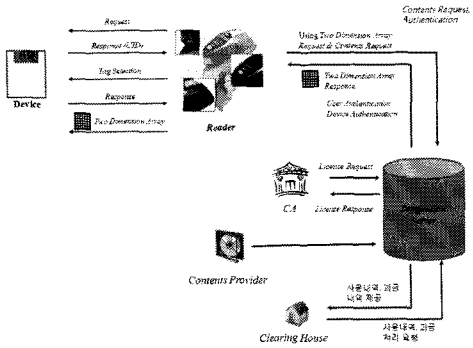
3. 제안하는 DRM 시스템

3.1 제안하는 시스템의 요구사항

제안하는 시스템은 모든 장치에 Tag가 삽입되어 있다고 가정한다. 또한 각각의 디바이스는 디바이스를 식별할 수 있는 고유한 ID(Identity)가 있으며, 디바이스 내부에는 키 유출에 대한 문제점을 위해 키셋을 포함하고 있다. 그리고 디바이스는 간단한 연산을 할 수 있는 연산 장치가 설치되어 있다.

3.2 제안하는 시스템 모델

본 논문에서 제안하는 시스템은 기존 시스템에서 인증에 이용되었던 물리적 인증 기법과 암호학적 인증 프로토콜 방법을 사용해 정보 보호를 하는 방법 대신, 2차원 배열(Array)과 XOR 기법을 이용하여 복잡한 암호화 방법이 없는 인증 기법이다. 그림 3은 제안하는 시스템의 전체 구조 이다.



[그림 3] 제안하는 시스템

사용자가 콘텐츠를 요청하게 되면 먼저 RFID 시스템을 통하여 장치 인증을 거치게 되며, 인증을 마친 후 리더는 통합서버(Integration Server)로부터 콘텐츠를 요청하게 된다. 통합서버에서는 콘텐츠의 사용 내역 및 라이센스를 확인 후 콘텐츠를 인증된 디바이스에게 제공한다.

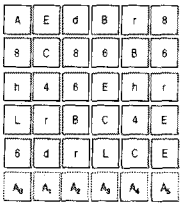
3.3 제안한 시스템의 동작과정

3.3.1 2차원 배열 생성

통합 서버는 2차원 배열을 생성하며 배열에 사용되는 키는 N*M 바이트(byte)로 각 셀당 64 가지의 문자를 이용하여 생성한다.

2차원 배열 생성 방법은 마지막 행을 제외한 나머지는 A~Z, a~z, 0~9 "+", "-" 총 64 가지의 문자를 이용하여 랜덤하게 패딩(padding) 된다. 마지막 행에 입력되는 값

은 각각의 열을 XOR 연산한 결과 값으로 패딩 된다.

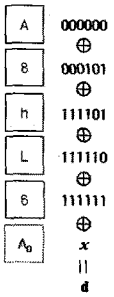


[그림 4] 난수값으로 패딩된 2차원 배열

그림 4는 난수값을 이용하여 마지막 행을 제외한 나머지를 64가지의 문자를 이용하여 패딩한 결과이다. 이렇게 패딩된 값을 XOR 하여 마지막 행에 들어갈 값을 구한다.

3.3.2 2차원 배열의 마지막 행 생성 방법

마지막 행에 패딩되는 값은 각 열을 XOR한 값과 각각의 마지막 행에 해당하는 A0값을 XOR한 값이 태그 아이디(tagID) 값이 된다. 태그 아이디(tagID)값을 "dCrr4h"이라 가정하고 마지막 행의 자세한 생성 방법은 그림 5와 같다.



[그림 5] 마지막 행값 생성 방법

연산으로 A_0 이전의 값과 A_0값을 XOR하면 그림 5와 같이 d(tagID)값이 나오고, A_0의 값을 구한다. 태그 아이 값을 얻는 방법은 식 1과 같다.

$$A \oplus 8 \oplus h \oplus L \oplus 6 \oplus A_0 = 'd'(tagID) \qquad \text{(식 1)}$$

각 열의 값을 XOR 하여 태그 아이디 값을 구하기 위해서는 키셋(keyset)을 필요로 하며, 키셋은 그림 6과 같다. 태그와 통합서버에서는 동일한 키셋을 가지고 있다.

000000	A
000001	B
000010	C
000011	d
000100	E
000101	8
000110	r
000111	4
...	...
111000	x
111001	Z
111010	a
111101	h
111110	L
111111	6

[그림 6] 키셋(keyset)

키셋의 값은 A~Z, a~z, 0~9 "+", "-" 총 64가지의 문자를 이용하여 랜덤하게 생성된다. 예를 들어 "A" 의 값은 "000000" 이 되지만 각 사용자 마다 서로 다른 키셋이 존재하기 때문에 결과 값이 틀려진다.

3.3.3 디바이스 인증

사용자는 최초에, 자신이 소유하고 있는 디바이스를 RFID 시스템을 이용하여 장치를 인증하게 된다. 인증하는 방법은 디바이스에 내장되어 있는 태그를 이용하게 된다.

먼저 리더는 디바이스 내에 있는 태그에게 UID값을 요청한다. 디바이스 내에 태그는 리더에게 자신이 가진 UID 값을 전송하게 된다. 리더는 태그의 UID값을 통합서버(Integration Server)에게 전송하고 이를 이용한 2차원 배열을 요청한다.

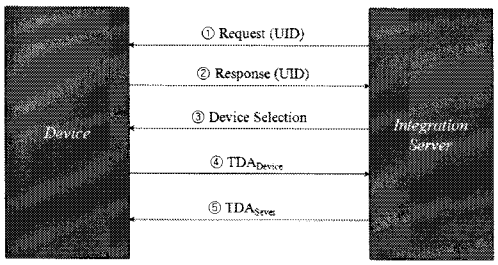
통합서버는 리더로부터 전송받은 UID값과 키셋(Keyset)을 이용하여 2차원 배열을 생성하고 생성된 2차원 배열을 리더에게 전송한다.

리더는 통합서버로부터 전송받은 2차원 배열을 디바이스에게 보내고, 디바이스는 전송받은 2차원 배열을 자신이 가진 키셋을 이용하여 자신이 보낸 UID값과 비교하여 상호 인증을 하게 된다.

3.3.4 디바이스 등록

최초 사용자가 디바이스를 통합서버에 등록하고자 할 때 아래의 그림 7과 같은 진행과정을 거친다.

• 용어 정리
- UID : Device UID
- TDA(Two Dimension Array) : 키셋을 이용하여 생성된 2차원 배열



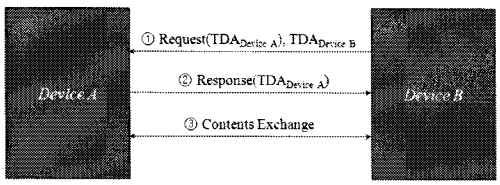
[그림 7] 디바이스 등록 프로토콜

① 통합서버는 리더를 통하여 디바이스에게 UID값을 요청한다.
② 디바이스는 리더를 통하여 통합서버에 UID값을 전송한다.
③ 통합서버는 여러 디바이스 중에서 UID값에 해당하는 디바이스를 선택한다.
④ 디바이스는 자신의 UID값을 이용하여 생성된 2차원 배열(TDA)을 전송한다.
⑤ 통합서버는 태그로부터 전송받은 UID값과 키셋을 이용하여 2차원 배열(TDA)을 디바이스로 보내고 디바이스에서는 이를 복호화하여 자신의 ID와 동일하면 인증 성공을 하게 된다.

디바이스의 모든 등록 과정을 마치게 되면 통합서버에는 각 장치에 해당하는 UID값과 TDA 값을 저장하게 된다.

3.3.5 디바이스 상호 인증

콘텐츠를 다운로드 받은 Device는, 다른 디바이스가 콘텐츠를 요구할 경우, 상호 인증 과정을 거쳐 디바이스에게 콘텐츠를 주어야 한다. 아래의 그림 8은 Device B가 Device A에게 콘텐츠를 요구하는 경우이다.



[그림 8] 디바이스 상호 인증 프로토콜

① Device B는 Device A에게 콘텐츠를 요청 메시지와 자신의 2차원 배열(TDA)을 보낸다.
② Device A는 Device B에게 받은 2차원 배열(TDA)을 키셋을 이용하여 복호화하고, 복호화된 UID값을 비교하여 인증을 하게 된다. 인증이 완료되면 자신의 2차원 배열(TDA)로 응답한다.
③ Device B는 키셋을 이용하여 Device A로부터 전송받은 2차원 배열(TDA)을 복호화하고 이를 비교한다. 검증이 완료되면 콘텐츠를 교환한다.

3.3.6 콘텐츠 이동

콘텐츠가 디바이스 사이를 옮겨갈 때마다, 콘텐츠는 TDA에 맞게 암호화 된다. 그러나 Passive 디바이스는 제한된 처리능력으로 인해 암호화를 할 수 없다. 그러므로 Active 태그를 이용한 디바이스를 사용한다.

[표 1] 콘텐츠의 이동 방향 및 암호화 여부

콘텐츠 이동방향	암호화 여부	이동 여부
Active → Active	○	○
Active → Passive	○	○
Passive → Active	×	○
Passive → Passive	×	○

3.3.7 디바이스의 추가 및 삭제

디바이스가 추가 되었을 경우 새로운 디바이스는 등록 프로토콜을 통해 통합서버에 등록을 한다. 그러나 통합서버에 등록된 디바이스들에게 새로운 디바이스가 추가 되었다는 사실을 통보해야 한다.

디바이스가 다른 통합서버로 이동하거나 물리적인 손상, 도난, 해킹을 당했을 경우 통합서버에서 제거 해야 한다. 이때 이 디바이스가 더 이상 통합서버에서 사용할 수 없다는 것을 다른 장치들에게도 통보해야만 한다.

사용자가 통합서버로부터 새로운 콘텐츠를 다운 받을 경우 콘텐츠 안에는 통합서버에서 사용 가능한 디바이스 목록이 포함되어 있어야 한다.

통합서버에서는 항상 사용 가능한 Device 목록을 최신의 것으로 유지하여, 콘텐츠의 불법적인 유출을 막아야 한다.

4. 실험평가

4.1 안전성에 대한 평가

4.1.1 스푸핑 공격에 대한 안전성

기존 시스템 해쉬-락 기법과 해쉬 기반 ID 변형 기법은 스푸핑 공격에 취약하지만 제안하는 시스템은 스푸핑 공격에 안전하다.

제안하는 시스템에서는 공격자가 정당한 리더로 위장

해도 태그의 UID값에 해당하는 키셋과 태그 아이디를 모르고 있으므로 2차원 배열을 태그에서 복호화 한다 하더라도 인증 거부를 한다. 또한 위장된 태그에는 올바른 UID값을 알 수 있지만, UID값에 해당하는 키셋을 알 수 없으므로 획득한 2차원 배열로는 스푸핑 공격이 불가능하다.

4.1.2 재전송 공격에 대한 안전성

기존 시스템 해쉬-락 기법은 재전송 공격에 취약하지만, 해쉬 기반 ID 변형 기법은 재전송 공격에 안전하다.

제안하는 시스템에서는 정당한 리더가 쿼리와 함께 전송하는 2차원 배열에 대하여 태그가 리더에 응답으로 2차원 배열을 재생성하여 전송한다. 정당한 리더는 키셋을 이용하여 2차원 배열을 복호화 하지만 자신이 보낸 태그 아이디와 다른 값이 나오므로 정당한 리더는 태그에 대한 인증을 거부한다.

4.2 제안하는 시스템

제안하는 시스템은 공격에 대한 안전성은 태그가 리더로부터 수신한 2차원 배열을 이용하여 요청마다 다른 2차원 배열로 응답을 하기 때문에 스푸핑 공격, 재전송 공격, 트래픽 분석 공격과 위치 트래킹 공격에 안전하게 나타났다. 표 2는 공격에 대한 안전성을 비교분석한 결과이다.

[표 2] 공격에 대한 안전성 비교

프로토콜 / 공격형태	해쉬-락 기법	해쉬 기반 ID 변형 기법	개선된 해쉬기반 ID 변형 기법	제안 시스템
스푸핑 공격	취약	취약	취약	안전
재전송 공격	취약	안전	안전	안전
트래픽 분석 공격	취약	안전	안전	안전
위치 트래킹 공격	취약	취약	보통	안전

제안하는 시스템에서 각 디바이스 상호인증을 위해서는 UID, 태그 아이디, 키셋을 가지고 있어야만 가능하며, 이중 태그 아이디와 키셋을 필수적으로 가지고 있어야만 2차원 배열을 복호화하고 이를 통하여 상호인증을 할 수 있다.

5. 결 론

본 논문에서 제안하는 시스템에서 각 디바이스 인증에 필요한 정보는 백엔드 서버에서 태그의 UID, 태그 아이디(TagID), 키셋(KeySet)의 정보가 등록 관리 된다. 이러한 정보를 이용하여 디바이스간 상호 인증을 수행함으로써 인증되지 않은 디바이스 또는 리더에게 콘텐츠가 유출되지 않도록 보안성을 강화 하였다.

제안하는 시스템에서는 리더와 디바이스 내에 탑재된 태그가 2차원 배열을 요청할 때마다 새롭게 생성하여 전송하기 때문에 기존 시스템보다 공격에 강한 특징을 가지고 있으며, 2차원 배열은 별다른 암호화를 사용하지 않기 때문에 키셋만 가지고 있다면 복호화 과정까지 전부 자동으로 진행되기 때문에 속도가 빠르다는 장점을 가진다. 또한 키셋을 가지고 있지 않다면 2차원 배열을 복호화 할 수 없으며 키셋을 이루고 있는 값들은 랜덤하게 바뀌므로 태그 아이디를 유추할 수 없다.

향후 연구과제로는 Passive 디바이스의 제한된 처리능력으로 암호화를 할 수 없으며 콘텐츠의 이동도 제한되는 문제점을 해결하기위해 연구할 계획이다.

참고문헌

[1] 정용훈, "멀티미디어 콘텐츠 보호를 위한 인증 프로토콜에 관한 연구" 숭실대학교 석사학위논문, 2006.

[2] 김정재, "멀티미디어 데이터 보호를 위한 대칭키 암호화 시스템에 관한 연구" 숭실대학교 박사학위논문, 2005.

[3] 한성동, "RFID Tag 보안을 위한 인증 프로토콜에 관한 연구" 숭실대학교 정보과학대학원 석사학위논문, 2007.

[4] Bogdan C. Popescu, Bruno Crispo, Frank L.A.J. Kamperman, Andrew S. Tanenbaum "A DRM Security Architecture for Home Networks" Proc. 4th ACM Workshop on DRM, pp. 1-10, 2004.

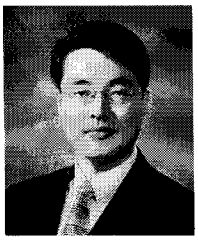
[5] G. Avoine. Privacy issues in RFID banknote protection schemes. Smart Card Research and Advanced Application - CARDIS, pp. 33-48, Kluwer, 2004.

[6] Natali. Helberger, Nicole, Dufft, Margreet Groenenboom, Kristóf Kerényi, Carsten, Orwat, Ulrich Riehm, "Digital rights management and consumer acceptability" A multi-disciplinary discussion of consumer concerns and expectations, State-of-the-art report, Amsterdam, pp.104 et seq...,

2004.

[7] Iwata. T, Abe. T, Ueda. K, Sunaga. H, "A DRM system suitable for P2P content delivery and the study on its implementation", Proceeding of the 9th Asia-Pacific Conference on Communications (APCC 2003), Vol. 2, pp. 806-811, 2003.

김 은 환(Eun-Hwan Kim) **[정회원]**



- 1930년 2월 : 숭실대학교 전자계산학과(공학사)
- 1997년 8월 : 숭실대학교 대학원 컴퓨터학과(공학석사)
- 2003년 2월 : 숭실대학교 대학원 컴퓨터학과(공학박사)
- 1990년 3월 ~ 1995년 8월 : 국방과학연구소 연구원
- 1997년 9월~현재 : 숭실대학교 전산원 인터넷 정보통신학과 교수

<관심분야>
멀티미디어 통신, 네트워크 보안, 홈 네트워크, 유비쿼터스

정 용 훈(Yong-Hoon Jung) **[정회원]**

- 2004년 2월 : 숭실대학교 전자계산원 멀티미디어학과(공학사)
- 2006년 8월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2006년 9월 ~ 현재 : 숭실대학교 컴퓨터학과(박사과정)

<관심분야>
멀티미디어 보안, DRM, RFID 응용,

전 문 석(Moon-Seog Jun) **[정회원]**

- 1980년 2월 : 숭실대학교 전자계산학과(공학사)
- 1986년 2월 : University of Maryland 전산학과(공학석사)
- 1989년 2월 : University of Maryland 전산학과(공학박사)
- 1991년 3월 ~ 현재 : 숭실대학교 컴퓨터학부 교수

<관심분야>
네트워크 보안, 컴퓨터 알고리즘, 병렬처리, 암호학, 유비쿼터스