DOI: 10.3745/KIPSTC.2008.15-C.4.221

CAS기반 IPTV 보안 시스템

김 대 엽[†] · 주 학 수[††]

요 약

IPTV는 TPS (Triple Play Service)의 대표적인 서비스이다. TPS 서비스는 다양한 종류의 서비스를 하나의 묶음 서비스로 제공함으로써, 사용자는 저렴한 가격으로 다양한 서비스를 이용할 수 있다. 고품질의 디지털 콘텐츠를 안정적으로 공급하기 위해서는 콘텐츠 서비스의 유료화가 필수적으로 요구된다. 유료 콘텐츠 서비스를 위한 보안 기술은 서비스 특성에 따라 CAS(Conditional Access System)와 DRM(Digital Right Management)이 사용되고 있다. 현재 IPTV도 이와 같은 보안 기술을 접목하여 서비스를 운영하고 있거나 향후 운영할 것으로 예상된다. 본 논문에서는 IPTV 서비스에서 DRM 또는 CAS를 접목할 때 발생할 수 있는 보안 문제점을 암호키 운영과 관련하여 살펴보고, 이와 같은 서비스를 가능하게 하기 위한 방안을 제안한다.

키워드: IPTV, CAS, DRM

CAS-based Security System for IPTV

Kim DaeYoub[†] · Ju HakSoo[††]

ABSTRACT

IPTV is well known services of TPS (Triple play service). Since TPS supplies the bundle service, service providers can supply low-priced services for their subscribers. To supply high quality contents stably, it is an essential requirement to make payment for the services. According to the type of services, either CAS or DRM is used to protect the pay-contents service. Also IPTV uses or will use these security systems to protect the service. In this paper, we will describe security problems when a IPTV service provider chooses either CAS or DRM, and then propose a new security system to solve the problems.

Key Words: IPTV, CAS, DRM

1. 서 론

TPS (Triple Play Service)는 방송, 통신 그리고 데이터 서비스를 하나의 서비스로 구성하여 제공하는 융합 서비스로 IPTV는 TPS의 대표적인 예다. IPTV 서비스는 주문형 서비스(Video on Demand, VoD) 뿐만 아니라 방송 서비스를 인터넷 환경에서 제공할 수 있다는 장점 때문에 다양한 소비 계층의 욕구를 만족시킬 수 있을 것으로 기대되고 있다[1]. 그러나 이와 같은 서비스의 발전은 콘텐츠의 불법 복사 및 배포라는 새로운 문제에 직면했다. 그러므로 서비스 제공자(Service Provider, SP)가 고품질의 콘텐츠를 안정적으로 공급하기 위해서는 콘텐츠 사용 제어 및 요금 징수를 위한 보안 시스템이 반드시 필요하다. 콘텐츠 보호 및 사용 제어를 위하여, 디지털 위성 방송 같은 방송형 서비스에서는 제한수신시스템(Conditional Access System, CAS)이 사용되고 있고, VoD와 같은 주문형 서비스에서는 권한관리시스템(Digital Right Management, DRM)이 이용되고 있다[2][3].

그러나 방송 서비스 또는 주문형 서비스 중 한 가지 서비스만을 지원하던 기존의 서비스와는 달리, IPTV 서비스는 두 가지 서비스를 모두 제공하기 때문에 보안 시스템 구축에 있어 CAS 또는 DRM 하나만으로는 충분하지 않다. 이와 같은 연구는 2006년에 이미 발표되었다[4]. [4]에서는 실제 서비스 구현을 가정하고 DRM으로 기존의 CAS를 대치하는 방안, CAS 기반의 시스템에 추가로 DRM의 일부 기능을 구현하는 방안, 그리고 CAS와 유사한 방식으로 운영되는 DRM을 구현하는 방안을 제안하고, 제안된 방안들의 효과 및 문제점을 지적하고 있다. 특히 [4]에서는 수신기(Set-top box, STB) 개발 및 고속 통신 환경만 제공되면 기존의 DRM 시스템으로 CAS를 대치하는 방안이 IPTV에

† 종신회원 : 삼성전자 기술총괄 종합기술원 수석연구원
†† 종신회원 : 삼성전자 디지털미디어총괄 DM 연구소 책임연구원
논문접수 : 2007년 4월 4일
수 정 일 : 1차 2008년 1월 16일, 2차 2008년 3월 10일, 3차 : 2008년 4월 4일
심사완료 : 2008년 5월 7일

가장 적합한 방안이라고 결론 내리고 있다. 또한 CAS의 구조적인 문제로 인하여 VoD 및 PVR(Personal Video Recorder) 등의 기능에 직접적으로 대응하기 어렵다고 판단하고 있다.

본 논문에서는 DRM 또는 CAS를 IPTV에 구현 시, 콘텐츠를 암호화 할 때 사용되는 암호키의 특성 및 관리 방안을 중심으로 분석한 후, DRM 기반의 IPTV 보안 시스템의 문제점을 지적하고, CAS 기반의 IPTV 보안 시스템 구조를 새롭게 제안한다.

본 논문에서 제안하는 CAS 기반의 보안 시스템 구조는 방송 및 VoD 서비스를 지원할 뿐만 아니라, 방송 프로그램을 STB에 녹화하는 기능(PVR)을 지원하도록 설계했다.

2. IPTV 보안 시스템

2.1 IPTV의 보안 특성

IPTV는 방송 및 VoD 서비스를 동시에 지원하므로 보안 시스템은 이와 같은 두 종류의 이종 서비스를 모두 지원할 수 있어야 한다.

방송 서비스는 채널 단위의 서비스를 제공하므로 전방향 안전성(Forward Security)의 확보가 중요하다. 즉, 채널을 통해 방송되는 프로그램을 암호화한 키가 외부로 노출되어도, 노출 된 키를 이용하여 해당 채널을 통해 향후에 방송되는 프로그램을 불법적으로 계속 이용할 수 없도록 제어할 수 있어야 한다. CAS의 경우, 프로그램 암호키를 주기적으로 갱신하여 전방향 안전성을 확보한다.

VoD 서비스는 IPTV의 양방향 서비스의 특성을 이용하여 개인 단위 및 콘텐츠 단위로 서비스를 제공하기 때문에 전방향 안전성을 별도로 고려하지 않아도 된다. 즉, SP가 콘텐츠를 암호화할 때, 개인 및 콘텐츠 별로 서로 다른 암호키를 사용할 수 있기 때문에, 하나의 콘텐츠 암호키가 노출 되도, 노출된 키의 사용을 제어할 수 있다.

이러한 서비스 별 보안 특성은 프로그램 또는 콘텐츠 암호키 설계 및 관리 정책을 수립할 때 반드시 고려되어야 한다.

2.2 IPTV의 보안 시스템 특성

이 절에서는 CAS와 DRM의 구조를 설명하고, 두 보안 시스템의 차이를 살펴본다. (그림 1)은 일반적인 CAS 시스템의 구성 및 운영을 설명한다. 프로그램은 제어단어(Control Word, CW)로 암호화 된 후 가입자에게 전송된다. 일반적으로 CW는 채널 단위로 관리되며 주기적으로 갱신된다. CW의 암/복호화에는 SP와 사용자가 공유하고 있는 단말기 암호키(Device Key, DK)가 사용된다. 보안을 위하여 DK도 주기적으로 갱신된다. DK는 CAS마다 서로 다른 구조를 정의해서 사용하나 DK의 효율적인 운영을 위해 계층화된 키 구성이 일반적으로 사용된다[5].

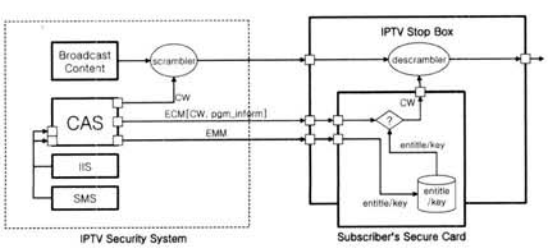
CW와 DK가 주기적으로 갱신되기 때문에 암호화된 프로그램을 시청하기 위해서 사용자는 갱신된 CW와 DK를 주기적으로 전송 받아야 한다. 또한, 프로그램을 시청하기 위해서는 해당 프로그램에 대한 시청 권한(Entitle)을 발급 받아야 한다. CW, DK 및 Entitle를 사용자에게 전송하기 위하여 CAS는 권한 제어 메시지(Entitlement Control Message, ECM)와 권한 관리 메시지(Entitlement Management Message, EMM)를 이용한다.

ECM은 DK로 암호화된 CW를 가입자에게 전달하기 위하여 사용된다. 또한, ECM은 프로그램 정보(예,프로그램 ID 등)와 접근조건(예, 시청 연령, 시청 지역-Black Out, 패키지 정보 등)을 함께 전달한다. 수신된 ECM은 사용자 스마트카드로 입력되어 처리된다. 스마트카드는 ECM의 접근조건과 스마트카드에 저장되어 있는 Entitle를 비교한 후, 해당 프로그램에 대한 권한을 갖고 있다고 판단되면 CW를 복호화해서 STB로 전달한다.

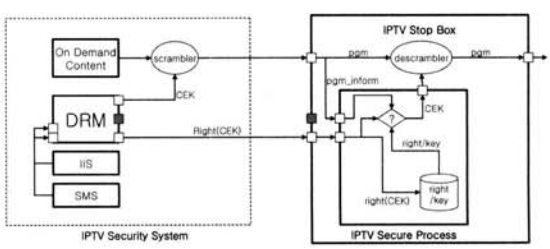
EMM은 갱신된 DK들과 사용자가 신청한 Entitle을 전송하기 위하여 사용한다. EMM의 구성 및 수신자의 특성에 따라 다양한 종류의 EMM이 사용된다.

(그림 2)는 DRM 시스템의 일반적인 구성과 운영을 설명한다. DRM 기반의 VoD 서비스는 콘텐츠 정보(pgm_inform)와 암호화된 콘텐츠로 구성된 패키지를 사용자에게 제공한다. pgm_inform은 콘텐츠 식별 정보(ID)와 콘텐츠 이용에 필요한 권한(Right)을 발급 받을 수 있는 정보센터(Clearinghouse)의 URL로 구성된다. Right는 사용자가 신청한 콘텐츠 사용 권한과 암호화된 CEK로 구성된다. DRM 사용자 모듈은 Right와 콘텐츠의 pgm_inform을 비교하여, 사용자의 Right가 해당 콘텐츠를 이용할 수 있는 정당한 권한을 포함하고 있는 경우에만 콘텐츠 이용을 허용한다.

(그림 1과 2)에서 볼 수 있는 것처럼 CAS와 DRM의 구성 및 운영 방법은 매우 유사하다. 두 시스템 모두 암호화된 상태로 콘텐츠를 제공하고, 특정 조건이 만족 될 때에만 콘텐츠의 이용을 허가한다. 특히, CAS의 CW은 DRM의 CEK와 유사하며, Entitle를 전송하는 EMM의 역할은 Right



(그림 1) CAS 구성 및 운영



(그림 2) DRM 구성 및 운영

의 역할과 비슷하다.

그러나 두 시스템 간의 명백한 차이점 또한 존재한다. CAS와 DRM의 가장 큰 차이점은 콘텐츠를 암호화 할 때 사용되는 암호키(CW, CEK)의 갱신 여부이다. (그림 1)에는 ECM을 통한 CW 갱신 과정이 포함되어 있으나, (그림 2)에는 이와 같은 과정이 생략 되 있다. 이와 같은 차이점은 앞서 설명한 것처럼 방송 서비스와 VoD 서비스의 특성 차이에 따른 전방향 안전성 확보 방법의 차이 때문에 발생한다.

3. DRM 기반 보안 시스템 분석

본 절에서는 DRM을 방송 서비스에 적용했을 때를 가정하여 그 적합성을 살펴본다. DRM을 방송 서비스에 적용할 때, Right의 발급 단위를 다음과 같이 나눠서 고려할 수 있다:

- 서비스 채널 단위 발급
- 서비스 채널에 편성된 개별 프로그램 단위 발급.

기본적으로 DRM은 콘텐츠 단위의 보안을 제공하기 때문에, 기존 DRM 시스템은 후자의 모델과 유사하다. 후자의 경우, 편성된 프로그램 단위로 Right를 발급하기 때문에, 프로그램 마다 서로 다른 CEK를 사용해서 암호화 할 수 있다. 이 경우, 전방향 안전성이 보장된다. 그러나 사용자가 채널 단위의 서비스를 이용하기 위해서는 해당 채널에 편성된 모든 프로그램의 Right를 발급 받아야 서비스를 이용할 수 있다. 또한, 프로그램 편성이 변경된 경우, 해당 채널에 가입한 모든 사용자에게 변경된 Right를 방송 시각 이전에 전송해야 한다.

이와 같은 서비스를 위해 필요한 계산량 및 전송량을 고려해 보자. 성능 분석을 위한 인자는 다음과 같다:

- N_c: 전체 서비스 채널 수
- N_p: 채널 당 편성 프로그램 수
- t: 프로그램 당 방영 시간
- N_s: 가입자 수
- N_{sc}: 가입자가 가입한 채널 수
- t_p: Right 전송 주기
- t_d: Right 전송 기간

모든 시간 인자들의 단위를 분이라 할 때, SP는 N_c개의 채널에서 현재 방송 중인 프로그램의 Right를 가입자에게 전송하기 위해서 t분마다 $N_{sc} \times N_s$개의 Right를 생성하여 t_p분마다 한번씩 전송해야 한다. 방송 서비스에서는 일반적으로 동기를 맞추기 위하여 Even/Odd 메시지를 함께 전송한다. 이 경우 $t_d = 2t$가 된다. 그러므로 SP는 분당 평균 $\frac{2 \times N_{sc} \times N_s}{t_p}$개의 Right를 전송해야 한다. 예를 들어 100개의 채널을 보유한 SP가 100만의 가입자에게 서비스를 제공한다고 가정하자. 가입자는 평균 60개의 채널에 가입해서 이용하고, Right의 전송 주기는 3분이라 하면, SP는 분당 40,000,000개의 Right를 전송해야 한다. 이와 같은 많은 수의 Right를 전송하는 것은 네트워크 부하의 원인이 될 수 있다. 그러므로 Right를 방송 프로그램 단위로 발급하는 것은 부적합하다.

동일한 환경 아래에서 서비스 채널 단위로 Right를 발급하면, 전체 가입자에게 N_{sc}개씩 Right가 발급된 후에는, 신청한 서비스가 변경된 가입자에게만 N_{sc}개의 Right를 전송하면 된다. 즉, 서비스 변경 신청을 하거나 서비스 기간이 만료되어 Right를 재발급 받아야 되는 가입자의 수가 전체 가입자의 c%라고 하면, $N_{sc} \times N_s$개의 Right가 한번 발급된 후 주기적으로 발급되는 Right의 수는 다음과 같다:

$$\frac{2 \times N_{sc} \times N_s}{t_p} \times \frac{c}{100}.$$

앞의 예와 동일한 가정 아래에서 $c = 10$이고 t_d는 24시간 이라 가정하면 3분 주기로 분당 4,000,000개의 Right를 전송하면 된다. 실제 서비스의 경우 변경 비율이 매우 낮다. 또한 만약 채널을 그룹화 하여 서비스를 한다면, 이 전송량은 더욱 감소될 수 있다.

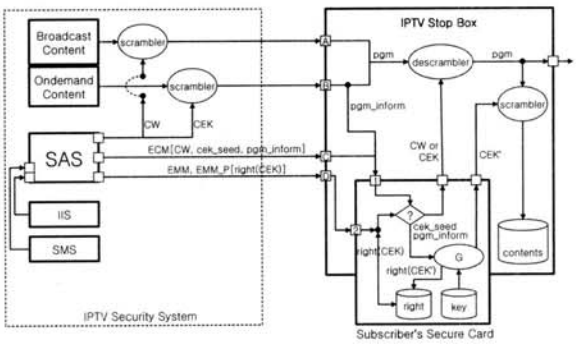
그러나 DRM을 이용하여 서비스 채널 단위로 Right를 발급하는 경우에는 전방향 안전성을 고려하여 프로그램 암호키를 갱신해야 한다. 그러나 (그림 2)에서처럼, 기존 DRM은 CEK 갱신을 고려하지 않는다. 그러므로 서비스 채널 단위로 Right를 발급하고 CEK를 주기적으로 갱신하기 위해서는 별도의 키 갱신 채널을 추가해야 된다. 이 경우, DRM 구성은 (그림 1)의 CAS 구성과 실제로 같게 된다.

그러므로 CAS를 이용하여 VoD를 효과적으로 지원할 수 있다면, DRM 기반의 IPTV 보안 시스템 보다 CAS 기반의 시스템이 더 효과적일 수 있다.

4. CAS 기반 보안 시스템 제안

본 절에서는 CAS 기반으로 VoD 서비스와 녹화 서비스를 제공할 수 있는 방안을 제안한다. 제안하는 방식은 기존의 CAS 구성에 변화 없이 EMM과 ECM의 내용만을 수정하여 VoD 및 녹화 서비스를 지원할 수 있도록 했다. 특히, 녹화 서비스는 정당한 Entitle을 갖고 있는 사용자만이 녹화 서비스를 이용할 수 있도록 설계되었다. 가입자가 프로그램을 STB에 녹화한 후 일정 기간 동안 이용할 수 있으며, SP가 녹화를 허용한 프로그램만 녹화할 수 있다.

(그림 3)은 이와 같은 방송 및 VoD 서비스를 위한 CAS 기반의 보안 시스템 구성 및 운영 방법을 설명한다. 방송 서비스는 기존의 CAS의 운영 방식을 그대로 적용하면 되기 때문에 VoD 및 녹화 서비스를 지원하기 위한 메시지 구조 및 운영 방안만을 설명한다.



(그림 3) CAS 기반 IPTV 보안 시스템 구성 및 운영

제안하는 시스템은 VoD 서비스를 지원하기 위해 정보센터를 통해서 발급되던 Right 정보를 특정 사용자에게 전송되는 EMM을 이용하여 전송한다. VoD 서비스를 위한 EMM의 구조는 <표 1>과 같다. EMM_id는 EMM의 종류를 표시하며, EMM_length는 메시지의 길이를 나타낸다. subscriber_id는 Right를 신청한 가입자의 ID이며, right는 시청권한을 의미한다. 시청권한은 서비스의 종류에 따라 다양한 방식으로 구성될 수 있다. dk_index는 CEK의 암호에 사용된 DK 식별자이며, 암호화된 CEK는 encrypted_CEK를 통해 전송된다.

EMM을 수신한 STB는 가입자 스마트카드에 EMM을 전달한다. 스마트카드는 EMM의 Right()를 저장/관리한다. 콘텐츠 이용 방법은 DRM의 운영과 동일한 방법으로 이용 할 수 있다.

녹화 서비스를 위한 ECM의 구성은 <표 2>와 같다. ECM_id는 ECM의 종류를 나타낸다. ECM_id의 MSB는 프로그램 녹화 허용 여부를 나타내는 지정비트(Flag bit)로 사용한다. ECM_id의 MSB를 제외한 7비트는 해당 ECM에 대

〈표 1〉 EMM 패킷 구성

Syntax	bits
EMM_packet() {	
EMM_id	8
EMM_length	8
Right()	RL+76
for(i=0;i<PL;i++) padding_data	PL
MAC_key_index	4
MAC }	64
Right() {	
subscriber_id	4
right()	RL
dk_index	8
encrypted_CEK }	64
right(){ for(i=0;i<RL;i++) right_data}	RL

〈표 2〉 ECM 패킷 구성

Syntax	bits
ECM_packet() {	
ECM_id	8
ECM_length	8
pgm_inform()	AL+20
dk_index	4
encrypted_CW	128
if((ECM_id & 0x10)) record()	96
for(i=0;i<PL;i++) padding_data	PL
MAC_key_index	4
MAC }	64
pgm_inform() {	
pgm_inform_length	8
pgm_id	8
parent_rate	4
access_condtion() }	AL
access_condition(){	
for(i=0;i<AL;i++) ac_data }	AL
record(){	
duration	32
CEK_seed }	64

응되는 채널 정보를 나타낸다. pgm_inform은 채널을 통하여 전송되는 프로그램 정보를 포함한다. 특히, 해당 프로그램의 이용 조건은 access_condition에 명시되어 있다. record는 녹화된 프로그램을 이용할 수 있는 기간 정보인 duration과 CEK 생성에 필요한 CEK_seed로 구성된다.

녹화를 위해서는 CW를 우선 복호화 해야 되기 때문에, 사용자는 프로그램에 대한 Entitle을 갖고 있어야 한다. 사용자가 녹화를 시작하면, STB는 스마트카드에 Right 생성 및 CEK를 요청하고, 스마트카드는 다음과 같은 과정을 수행한다:

- ECM_id를 분석하여 해당 프로그램이 녹화가 가능한 프로그램인지를 확인한다.
- pgm_id, parent_rate, duration 및 사용자 ID(subscriber_id)를 근거로 가입자 Right를 구성 한다.
- DK 중 사용자에게만 할당된 키(PK)로 CEK_seed를 암호화해서 CEK를 생성 한다: CEK= E_{PK}(CEK_seed).
- 생성된 Right와 CEK를 스마트카드에 저장한 후,

pgm_id, subscriber_id 및 CEK를 STB에 전송한다.

STB는 스마트카드로부터 출력된 CEK를 이용하여 녹화 프로그램을 암호화 한 후, {pgm_id, subscriber_id}와 함께 암호화된 콘텐츠를 패키징 하여 저장한다. 사용자마다 서로 다른 PK를 사용하기 때문에 동일한 프로그램이라도 서로 다른 CEK로 암호화 된다. 그러므로 녹화된 프로그램이 외부로 유출되더라도, 다른 가입자 스마트카드로 해당 프로그램을 이용할 수 없다. 사용자가 녹화된 프로그램을 이용할 때에는 앞서 설명한 VoD 서비스 이용 방식과 동일한 방식으로 이용할 수 있다.

5. CAS 기반 보안 시스템의 특징

본 논문에서는 제안하는 CAS 기반의 IPTV 보안 시스템은 기존 CAS에서 사용하는 EMM과 ECM을 이용하여 VoD와 녹화 서비스를 모두 지원하기 때문에 [4]에서 제안된 모델인 CAS 적응형 DRM 모델처럼 CAS와 DRM을 모두 갖출 필요가 없다. 또한, 제안된 EMM 내용 및 운영 방법은 기존 DRM Right의 내용 및 운영 방법과 동일한 형태를 갖추고 있기 때문에 [4]에서 제기한 ECM/EMM의 사용에 따른 구조적 결함 가능성을 배제시킬 수 있다. 뿐만 아니라, ECM/EMM을 이용하여 녹화 서비스를 지원하고, 특히 동일한 프로그램을 녹화하더라도 사용자마다 서로 다른 CEK를 이용하여 암호화하기 때문에 녹화된 콘텐츠가 외부로 유출되더라도 이용을 제어할 수 있도록 안전하게 설계 되었다.

6. 결 론

IPTV를 위한 보안 시스템으로 CAS와 DRM이 제안되고 있다. 그러나 CAS와 DRM은 각각의 서비스 모델을 다르게 가정하고 설계되었기 때문에 두 시스템 중 하나로 방송 및 VoD 서비스를 동시에 지원하기에는 부족한 부분이 있다.

본 논문에서는 기존에 DRM을 이용한 IPTV 보안 시스템을 살펴보고 문제점을 분석했다. 또한 CAS 기반의 IPTV 보안 시스템 구성 및 운영 방안을 제안하고, 이를 바탕으로 EMM과 ECM의 구성을 함께 제안하였다. CAS의 구조적인 문제로 인하여 VoD와 PVR 등의 기능에 직접적으로 대응하기 어렵다는 그 동안의 주장과 달리, 제안된 시스템은 방송 및 VoD 서비스, 그리고 녹화 서비스까지 지원할 수 있는 시스템으로 CAS의 기본적인 모델을 최대한 수용하여 향후 실제 서비스 적용 시 시스템 변경을 최소화 할 수 있도록 설계 되었다.

현재 제안된 모델의 녹화서비스는 녹화된 프로그램의 이용을 최초 녹화된 STB로 한정시키고 있으나, 현재 Trust Domain과 같은 개념을 도입하여 이용 영역을 홈 도메인과 같은 한정된 영역으로 확대시키는 방안에 대한 추가적인 연구가 앞으로 필요할 것으로 예상된다.

참 고 문 헌

[1] 현대원, "퍼스널미디어: 디지털 경제의 승부처", 디지털미디어리서치, 2004.

[2] EBU Project Group B/CA, "Functional model of a conditional access system," EBU Technical Review Winter 1995.

[3] 주학수, 김대엽, 장기식, 김승주, "디지털 저작권 관리 시스템(DRM)의 개발현황", 한국정보보호학회지, 제13권 2호, pp.81-91, 2003.

[4] 우제학, 노창현, 이완복, "IPTV 콘텐츠 보호 기술의 비교 - CAS와 DRM 중심으로", 한국콘텐츠학회논문지 Vol.6, No.8, pp.157-164, 2006.

[5] Fu-Kuan Tu, Chi-Sung Haih, Hsu-Hung Tung, "On Key Distribution Management For Conditional Access System on Pay-TV System," IEEE Transactions on Consumer Electronics, Vol.45, No.1, February 1999.

김 대 엽

e-mail : daeyoub69@paran.com

1997년 고려대학교 대학원 수학과 (이학석사)

2000년 고려대학교 대학원 수학과 (이학박사)

1997년~1999년 (주)텔리맨 위성통신연구소 책임연구원

2000년~2001년 (주)시큐아이닷컴 정보보호연구소 책임연구원

2002년~현 재 삼성전자 기술총괄 종합기술원 수석연구원

관심분야 : CAS, DRM, 스마트카드 보안, 보안 프로토콜

주 학 수

e-mail : haksoo.ju@samsung.com

1999년 고려대학교 대학원 수학과 (이학석사)

2005년 고려대학교 대학원 수학과 (이학박사)

2001년~2005년 한국정보보호진흥원 연구원

2006년~현 재 삼성전자 DM연구소 책임연구원

관심분야 : DRM, 보안 프로토콜