ISSN(Print): 2287-5891

http://dx.doi.org/10.3745/KTCCS.2013.2.2.075

Key Generation and Management Scheme for Efficient Interoperability among Different Downloadable Conditional Access Systems

Hoonjung Lee† · Hasoo Eun† · Heekuck Oh††

ABSTRACT

CAS (Conditional Access System) is a content protection solution that restricts access to the system according to user's standing and only authorized users can access the content in a pay-TV system. DCAS (Downloadable Conditional Access System) can download CAS client which is a software implemented via network. In recent years, research and development has been carried out on DCAS to solve the problems of compatibility among heterogeneous devices and internetworking with other services. In this paper, we propose key generation and management scheme for efficient interoperability among different DCASs based on PBC (Pairing Based Cryptography).

Keywords : Downloadable Conditional Access System (DCAS), Interoperability, Key Management Scheme

서로 다른 DCAS 간 효율적 상호운용을 위한 키 생성 및 관리 기법

이 훈 정† · 은 하 수† · 오 희 국††

요 약

제한수신시스템(Conditional Access System, CAS)은 사용자의 조건에 따라 방송에 대한 접근을 제어하는 시스템으로 유료 TV 시스템에서 인가된 사용자만이 해당 프로그램에 접근할 수 있도록 하는 콘텐츠 보안 기술이다. 최근에는 기존의 하드웨어 기반 CAS가 가지는 이기종 기기 간 호환성, 다른 서비스와의 연동 등의 문제를 해결하고자 CAS의 클라이언트를 소프트웨어로 구현하여 네트워크를 통해 전송하는 다운로드가 가능한 제한수신시스템(Downloadable CAS, DCAS)에 대한 연구와 개발이 활발히 진행되고 있다. 본 논문에서는 서로 다른 DCAS 간 효율적인 상호운용이 가능한 PBC(Pairing Based Cryptography) 기반의 키 생성 및 관리 기법을 제안한다.

키워드 : 다운로드 가능 제한수신시스템, 상호운용성, 키 관리 기법

1. 서 론

CAS는 사용자의 조건에 따라 접근을 제한하는 시스템으로 인가된 사용자만이 해당 프로그램에 접근할 수 있도록 하는 콘텐츠 보안 기술이다[1]. 이러한 CAS는 현재 위성, 지상파, 케이블 방송의 유료 TV 시스템에 주로 사용되고 있다. CAS는 크게 2가지 기능을 수행한다. 첫 번째는 콘텐츠의 기밀성을 위해 콘텐츠를 암호화하는 기능이고, 두 번째는 암호화된 콘텐츠에 대한 접근을 위해 자격을 관리/제어하는 기능이다. 현재는 디지털 방송 수신기인 STB(Set-Top Box)에 내장된 소프트웨어와 스마트카드 또는 케이블 카드와 같은 하드웨어를 함께 사용하는 방식의 CAS를 주로 사용한다. 하지만 이러한 하드웨어 기반 CAS는 하나의 STB에 하나의 CAS만을 사용해야 하기 때문에 하나의 STB에서 동시에 여러 종류의 CAS를 사용하는 것이 불가능하다는 점과 CAS의 고장 시 CAS 모듈 전체 또는 STB 자체를 교체해야 하는데 따른 유지/보수비용의 증가 문제가 단점으로 지적되었다[2]. CAS의 상호운용과 유지/보수비용의 감소를 위한 STB와 CA(Conditional Access) 모듈의 분리에 대한 연구는 1990년대 초반부터 꾸준히 진행되어왔다. 유럽 중심의 디지털 방송 표준화 단체인 DVB(Digital Video Broadcasting)에서는 헤드 엔드에서 상호운용 개념을 도입한 Simulcript[3]와 STB에 내장되던 CA 모듈을 STB와 분리가 가능하도록 한 CI(Common

※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(NIPA-2012-H0301-12-4004).
※ 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2012-R1A2A2A01046986).
† 준 회 원 : 한양대학교 컴퓨터공학과 박사과정
†† 종신회원 : 한양대학교 컴퓨터공학과 교수
논문접수 : 2012년 7월 31일
수 정 일 : 1차 2012년 10월 23일
심사완료 : 2012년 11월 8일
* Corresponding Author : Heekuck Oh(hkoh@hanyang.ac.kr)

Interface)라 불리는 Multicript[4]를 제안하였다. Simulcrypt는 미국의 디지털 TV 표준인 ATSC(Advanced Television Systems Committee)의 CAS에도 채택되었다. 또한 미국의 케이블 방송 표준화 기구인 CableLabs는 OpenCable표준에 교체 가능한 하드웨어 장치인 케이블카드를 이용한 CAS를 제안하였다[5]. 그러나 이러한 방법들은 방송 시스템의 대역폭 증가와 STB의 연산량 부담 그리고 CAS 업체들의 비협조 등의 이유로 널리 사용되어 지지 못하였다. 또한 교체 가능한 하드웨어 기반의 CAS가 STB의 기기적 결함과 가격 상승을 야기한다는 단점도 지적되었다[2].

최근 통신 기술의 발달로 디지털 방송이 IP와 같은 양방향 통신망을 이용하는 것이 가능해지면서 CAS와 방송 업계에서는 하드웨어 기반 CAS의 한계 극복을 위한 방법으로 양방향 통신을 이용한 소프트웨어 다운로드 방식을 고려하고 있다. 2006년 CableLabs에서 CAS의 클라이언트를 소프트웨어로 구현하여 네트워크를 통해 다운로드가 가능한 DCAS를 처음으로 제안하였으며 그 이후 DCAS에 대한 연구와 개발이 활발히 진행되고 있다. DCAS의 보안 이슈는 크게 4가지로 나눌 수 있는데 첫째, DCAS 서버와 DCAS 호스트 간의 상호인증, 둘째, 네트워크를 통해 전송되는 DCAS 클라이언트의 보호, 셋째, DCAS 서버 내 구성요소 간의 보안 그리고 마지막으로 DCAS에 사용되는 키들의 생성과 관리이다. 현재까지 제안된 대부분의 DCAS 프로토콜은 CableLabs의 규격인 OpenCable DCAS를 기준으로 하고 있으며 DCAS 클라이언트의 안전한 다운로드와 구성요소 보안을 주로 다루고 있다.

이 논문에서는 DCAS 간 상호운용에 대해 다룬다. 하나의 STB에 다운로드 된 다수개의 CAS들의 효율적 상호운용을 위한 고려 사항을 분석하고 이를 만족하는 키 생성 방법과 생성된 키의 관리 기법을 제안한다. 이어지는 논문의 구성은 다음과 같다. 2장에서는 DCAS와 DCAS의 보안 이슈 그리고 관련연구에 대해 살펴보고 3장에서는 제안하는 기법에 대해 자세히 설명한다. 4장에서는 제안하는 기법의 안전성과 효율성에 대해 분석하고 마지막 5장에서는 결론을 맺는다.

2. 연구 배경

이 장에서는 연구의 배경인 DCAS와 DCAS에 대한 선행연구에 대해 살펴본다. 이 논문에서 다루는 DCAS는 OpenCable 기반 DCAS를 기준으로 한다.

2.1 DCAS

1) DCAS 구성 요소와 동작 과정

DCAS는 Downloadable conditional access system의 약자로 현재 디지털 방송에서 주로 사용되는 콘텐츠 보호 방법인 CAS에 네트워크를 통한 다운로드 개념을 더한 것이다. DCAS의 핵심은 기존의 하드웨어 기반 CAS의 구성요소 중에서 클라이언트 부분을 소프트웨어로 구현하여 이를 네트워크를 통해 전송하는 것이다. Fig. 1은 OpenCable 기반 DCAS의 구조도이다. DCAS는 DCAS 서버, 백 오피스, 헤드 엔드, DCAS 호스트 그리고 신뢰기관으로 구성된다. DCAS 서버는 AP(Authentication Proxy), LKS(Logical Key Server), PS(Provisioning System), IPS(Integrated Personalization Server)로 구성되는데 이는 DCAS 호스트와의 통신과 CAS 클라이언트의 다운로드를 담당한다. 백 오피스는 가입자의 자격관리와 과금을 담당하고, 헤드 엔드는 오디오, 비디오 그리고 데이터를 멀티플렉싱하여 TS(Transport Stream)를 생성하는 일을 담당한다. DCAS 호스트는 TP(Transport Processor), SM(Secure Micro)으로 이루어져 있다. SM은 CAS 클라이언트의 다운로드와 적재를 담당하는 부분이고 TP는 TS의 수신과 암호화된 콘텐츠의 복호화를 수행하는 부분이다.

DCAS는 신뢰기관의 식별 정보 발급, DCAS 클라이언트 다운로드 준비, DCAS 클라이언트 전송, 다운로드된 DCAS 클라이언트 적재, 자격관리/제어 메시지(Entitlement Management/Control Message, EMM/ECM) 전송, 제어 단어(Control Word, CW) 획득 및 암호화된 콘텐츠 복호화의 6단계를 거쳐 동작한다. 각 단계에서 수행되는 자세한 동작은 다음과 같다.

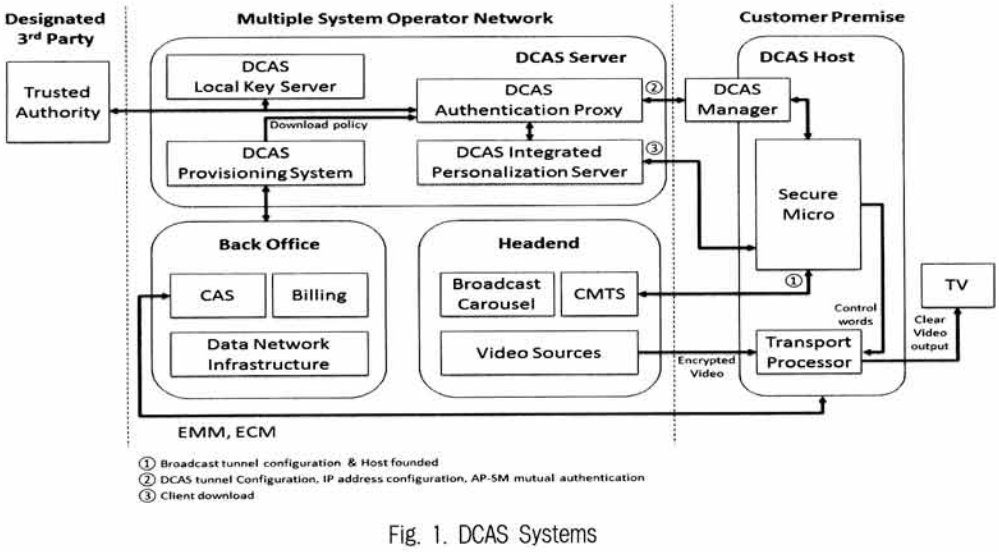


Fig. 1. DCAS Systems

① 신뢰기관의 식별 정보 발급: 신뢰기관은 DCAS 호스트에 존재하는 SM과 TP의 식별정보를 발급한다. 이 식별정보는 DCAS 서버가 DCAS 호스트를 인증할 때 사용된다.
② DCAS 클라이언트 다운로드 준비: CAS 클라이언트의 안전한 다운로드를 위해 DCAS 서버의 AP와 DCAS 호스트의 SM 간의 안전한 통신채널을 생성한다.
③ DCAS 클라이언트 전송: ②에서 생성된 채널을 통해 DCAS 서버는 DCAS 호스트에게 소프트웨어 형태의 CAS 클라이언트를 전송한다.
④ 다운로드된 DCAS 클라이언트 적재: DCAS 호스트는 ③에서 전달받은 CAS 클라이언트를 사용 가능한 형태로 시스템에 적재한다.
⑤ EMM/ECM 전송: 암호화된 콘텐츠의 복호화에 필요한 자격관리/제어 메시지들을 DCAS 호스트에게 전송한다.
⑥ CW 획득 및 암호화된 콘텐츠 복호화: ④에서 적재된 CAS 클라이언트는 ⑤에서 전송 받은 ECM/EMM을 이용해 CW를 획득하고 CW를 이용해 암호화된 콘텐츠를 복호화한다.

2) DCAS 보안 이슈

하드웨어 기반 CAS에서는 CAS 클라이언트가 적재된 STB를 사용하였다. 이 시기에는 역공학을 제외하고는 CAS 클리이언트의 안전성을 위협하는 요소가 거의 존재하지 않았다. 그러나 CAS 클라이언트를 네트워크를 통해 다운로드하는 DCAS의 경우 CAS 클라이언트의 안전성을 위협하는 요소가 많다. 안전한 DCAS를 위해 고려해야하는 보안 이슈들은 다음과 같다.

■ DCAS 서버와 DCAS 호스트 간의 상호인증: OpenCable 기반 DCAS의 규격에는 서버와 호스트가 오프라인 방식 등으로 사전에 공유된 비밀키를 이용해 상호인증을 수행한다고 명시되어 있지만 이에 대한 구체적인 방법에 대한 정의는 없다. 서버와 호스트 간의 상호인증 과정이 존재하지 않는다는 것은 위장 공격이나 중간자 공격 등 상호인증을 수행하지 않았을 때 발생 가능한 모든 문제가 존재함을 의미한다. 그러므로 안전한 DCAS를 위해서는 서버와 호스트 간의 상호인증은 반드시 필요하다.
■ DCAS 클리이언트의 보호: OpenCable 기반 DCAS의 규격에는 다운로드되는 CAS 클라이언트의 무결성 검증과 전자서명을 이용하여 클라이언트의 신뢰성을 보장하도록 하고 있다. 하지만 무결성과 서명을 통한 출처의 확인 외에 클라이언트의 기밀성이 보장되어야 한다. CAS는 콘텐츠를 보호하기 위한 기법인데 CAS 클라이언트의 기밀성은 CAS 자체의 안전성에 큰 영향을 미치기 때문에 클라이언트의 보호는 반드시 필요하다.
■ DCAS 서버 내 구성 요소 간 보안: DCAS 서버 내 구성요소인 LKS에는 DCAS에서 사용되는 키 들이 저장되어 있고 PS에는 다운로드 일정, 방법 등이 저장되어 있다. 이런 LKS와 PS는 AP가 CAS 클라이언트를 다운로드할 때 정보를 교환한다, 정보를 교환하는 과정을 보호하지 않을 경우 중요한 데이터가 노출될 수 있다, 그러므로 DCAS 서버 내 구성 요소 간 통신 채널을 보호하는 것이 반드시 필요하다.
■ DCAS에서 사용되는 키 들의 생성과 관리: DCAS에서는 서버와 DCAS 호스트 간 상호인증에 사용되는 키, 클라이언트를 암호화하기 위한 키, 전자서명에 사용되는 키 그리고 자격관리/제어를 위한 키와 콘텐츠를 암호화하는 키 등과 같이 많은 키 들이 사용된다. DCAS의 안전하고 효율적인 운용을 위해서 이러한 키 들의 생성과 관리는 매우 중요한 요소이다.

2.2 선행 연구

CAS 클라이언트 부분을 소프트웨어로 구현하여 네트워크를 통해 다운로드 하는 개념은 F. Kamperman 등에 의해 처음 소개되었다[6]. 그 후 OpenCable DCAS의 표준이 제안되면서 DCAS에 대한 연구가 활발히 진행되었다. DACS에 대한 연구는 DCAS 구성요소 간 보안에 대한 연구와 DCAS 서버와 DCAS 호스트의 구현에 관한 연구 그리고 DCAS 간 상호운용에 관한 연구들이 진행되었다.

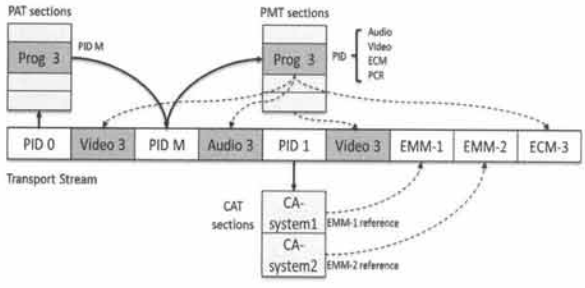
DCAS 구성 요소 간 보안에 관한 연구들 중에는 사전 공유키 방식을 이용한 서버와 호스트 간의 상호인증 기법에 관한 연구가 활발하게 진행되었다. Y. Jeong 등은 전용 칩과 사전 공유키 기반의 DCAS 서버와 DCAS 호스트 간의 상호인증과 CAS 클라이언트 보호기법을 제안하였는데 이후에 H. Jeong 등은 Y. Jeong 등의 기법이 위장 공격에 취약함을 보이고 이를 보완한 기법을 제안하였다[7,8]. 이들의 제안 외에도 DCAS 서버와 호스트의 상호인증과 서버 내 구성요소 간 보안에 관한 다양한 기법들이 제안되었다[9-11]. Koo 등은 DCAS 호스트 내의 SM과 TP 사이에 전송되는 CW를 보호하는 기법을 제안하였다[12]. DCAS 서버와 호스트의 구현에 관한 연구는 안전성 보다는 효율적인 시스템의 구조와 설계에 관한 연구들이 주로 진행되었다[13-15]. Moon 등은 하나의 STB에 다수개의 CAS들의 다운로드 되고 이 CAS간의 상호운용을 위한 시스템의 구조를 제안하였다[16].

3. 제안하는 기법

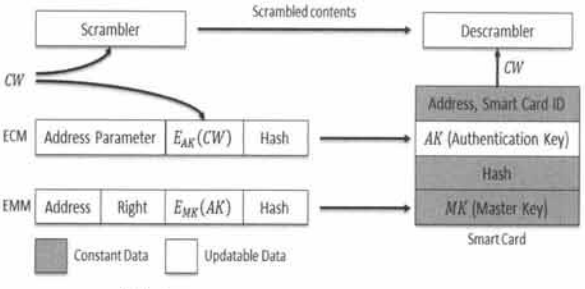
이 장에서는 CAS의 자격관리/제어 방법과 상호운용의 관계에 대해 살펴보고 DCAS 간 상호운용을 위한 키 생성과 관리 방법에 대해 자세히 설명한다.

3.1 CAS의 자격관리/제어와 상호운용

CAS의 자격관리/제어 방법을 살펴보면 다음과 같다. 방송을 전송하는 CAS 서버에서는 CW를 생성하고 CW를 이용해 방송 콘텐츠를 스크램블링하여 전송한다. 이때 생성된 CW는 인증 키(Authorization Key, AK)로 암호화 되어 ECM을 통해 전송되고, AK는 각 사용자의 스마트카드에 저장되어 있는 마스터 키(Master Key, MK)로 암호화 되어 EMM을 통해 전송된다. 방송을 수신하는 STB에서는 송신



(a) MPEG-TS



(b) CW obtainments process of CAS

Fig. 2. Entitlement control of CAS

측과 반대 과정을 수행하게 되는데 EMM을 통해 전송되는 MK로 암호화된 AK를 복호화한 후 ECM을 통해 전송되는 AK로 암호화 되어있는 암호화된 CW를 복호화하여 STB의 디스램블러에게 전달한다. STB의 디스크램블러는 전달받은 CW를 이용하여 스크램블링 되어 있는 콘텐츠를 디스크램블링할 수 있게 된다. Fig. 2의 (a)는 자격제어/관리에 사용되는 EMM, ECM, CAT(Conditional Access Table) 등이 존재하는 MPEG-TS의 구성도이며 프로그램 3을 시청하기 위해 필요한 자격관리/제어메시지를 찾는 과정을 나타낸다. Fig. 2의 (b)는 EMM/ECM을 이용해 CW를 획득하는 과정을 보여준다. EMM/ECM을 통해 CW를 획득하는 과정이 CAS 클라이언트에서 수행하는 일이다. 하드웨어 기반 CAS의 경우 어떠한 CAS가 사용될지 알고 있으며 CAS 업체에서 발행한 MK가 저장되어 있는 스마트카드가 방송 수신자의 STB에 장착되어 있기 때문에 MK로 암호화 되어있는 AK를 쉽게 복호화 할 수 있다. 어떠한 CAS가 사용되는지는 CAT내의 CAS ID를 통해 알 수 있다.

CAS간 상호운용이 어려운 이유는 사용자의 MK와 EMM/ECM의 형태와 처리 과정이 각 CAS업체마다 다르기 때문이다. 방송 수신자들은 하나의 STB를 이용해 다수의 방송을 시청하길 원한다. 이런 환경에서 현재의 디지털 방송처럼 한 방송 사업자가 하나의 CAS를 선택해서 송신하는 모든 방송을 하나의 CAS로 암호화하는 경우 수신자들의 STB에는 하나의 CAS만이 탑재되어 있어도 모든 방송을 시청하는 것이 가능하며 CAS간 상호운용을 고려할 필요가 없을 것이다. 하지만 현재의 지상파 방송처럼 다수의 방송 사업자 존재하는 경우 각 방송 사업자들이 서로 다른 CAS를 선택해서 각각의 방송이 서로 다른 CAS로 암호화하는 경우 수신자들의 STB에는 방송 사업자들이 선택한 CAS가 모두 탑재 되어있어야만 모든 방송의 시청이 가능하며 이 경우에는 CAS간 상호운용을 반드시 고려해야 한다.

현재까지 제안된 대부분의 DCAS에 관한 연구는 DCAS 서버로부터 DCAS 호스트까지 CAS 클라이언트를 안전하게 전달하는 방법에 대한 것이다. 대부분의 연구에서 자격관리/제어 방법은 기존 하드웨어 기반 CAS의 자격관리/제어 방법을 그대로 사용하고 있다. 그 외에는 DCAS 서버와 DCAS 호스트 간 상호인증을 위해 생성되는 키를 이용해 MK 역할을 하는 비밀키를 생성하는 방법이 제안되었다.

기존에 제안된 대부분의 DCAS 관련 연구들은 DCAS 간 상호운용을 고려하고 있지 않다. DCAS간 효율적 상호운용이 가능하기 위해서는 다음 2가지 사항을 고려해야한다.

■ CAS 수 증가에 따른 MK 수의 증가

CAS 업체마다 사용하는 MK가 모두 다르기 때문에 사용하고자 하는 CAS 수만큼의 MK를 가지고 있어야 하는 MK 수의 증가와 관리 문제이다. 기존의 하드웨어 기반 CAS를 그대로 따를 경우 스마트카드처럼 사용자의 MK가 저장되어 있는 매체가 필요하다. 수신자 측의 STB에서 채널을 변경하는 경우 현재 시청하고 있던 채널과 변경을 원하는 채널이 서로 다른 CAS를 사용한다면 CAS 클라이언트를 새로 다운로드 하게 될 것이고 이때 다운로드된 CAS에 적합한 EMM/ECM 복호화에 필요한 MK가 있어야 하기 때문이다. 이는 사용하게 될 CAS의 종류도 미리 알아야 하고 사용하게 될 CAS에 적합한 MK도 가지고 있어야 함을 의미한다. 서로 다른 CAS를 사용하는 여러 방송의 시청을 원할 경우 위와 같은 상황은 매우 비효율적이고 비현실적이라 할 수 있다.

■ CAS 간 이동시 발생하는 지연시간

MK를 호스트 내에 저장하지 않고 DCAS 서버와 DCAS 호스트 간 상호인증에 사용되는 키들을 이용하여 생성하는 경우 발생하는 지연시간 문제이다. DCAS 서버와 DCAS 호스트간의 상호인증에 사용되는 키를 이용하는 경우 CAS 클라이언트의 변경 때 마다 상호인증을 하고 그 후에 MK를 생성해야한다. 이런 경우 많은 시간이 소요되기 때문에 이는 실시간 방송 환경에는 적합하지 않다.

서로 다른 CAS 간 효율적인 상호운용을 위해서는 현재 사용하고 있는 CAS와 다른 CAS를 다운로드 하더라도 EMM/ECM 획득이 용이한 MK 생성과 관리 방법이 필요하다.

3.2 DCAS간 상호운용을 위한 키 생성과 관리 기법

본 장에서는 DCAS간 효율적인 상호운용을 위한 MK, EMM/ECM의 생성과 관리 방법을 제안한다.

제안하는 기법에서는 MK 수의 증가와 관리 문제를 해결하기 위해 신뢰기관, DCAS 서버, DCAS 호스트 간의 키 동의를 사용하였으며 CAS 간 이동시 발생하는 지연시간 문제는 DCAS 서버와 DCAS 호스트간의 상호인증에 사용되는 키와 자격제어/관리에 사용되는 키의 분리를 통해 해결하였다. 상호인증에 사용되는 키와 자격제어/관리에 사용되는 키를

분리 하였으므로 DCAS 서버와 DCAS 호스트, DCAS 호스트 내 개체들 간의 상호인증은 기존에 제안된 방법들을 따른다고 가정하고 MK, EMM/ECM의 생성에 대해서만 다룬다.

1) 수학적 배경 및 시스템 구성

제안하는 키 생성 기법은 현재 널리 사용되고 있는 pairing 기반 암호기법(Pairing Based Cryptography, PBC)을 기반으로 한다. 제안하는 기법에서 사용되는 PBC의 기본 개념인 bilinear pairing은 다음과 같다.

이 논문에서는 앞으로 다음과 같은 표기법을 사용한다. 1) q는 매우 큰 소수이다. 2) G_1과 G_2는 같은 위수 q를 갖는 군으로 G_1은 타원곡선위의 덧셈군, G_2는 유한체위의 곱셈군이다. 3) P, Q, R은 G_1의 임의의 원소들이다. 4) a, b, c는 Z_q^*의 임의의 원소들이다.

정의 1. Bilinear pairing. 다음과 같은 조건들을 만족하는 함수 $e: G_1 \times G_1 \rightarrow G_2$를 admissible bilinear pairing이라 한다.

■ Bilinear: 임의의 $P, Q, R \in G_1$에 대해 다음이 성립해야 한다.
- $e(P+Q, R) = e(P, R) \cdot e(Q, R)$
- $e(P, Q+R) = e(P, Q) \cdot e(P, R)$

■ Non-Degenerate: G_1의 모든 쌍 P, Q에 대해 $e(P, Q)$는 G_2의 항등원이 아니어야 한다.

■ Computable: 임의의 $P, Q \in G_1$에 대하여 $e(P, Q)$를 계산할 수 있는 효율적인 알고리즘이 존재해야 한다.

Bilinear 특성에 의해 다음 특성을 추가적으로 유도할 수 있다.

$$e(aP, bQ) = e(P, bQ)^a = e(aP, Q)^b = e(P, Q)^{ab} = e(abP, Q) = e(P, abQ)$$

제안하는 기법을 위한 DCAS 시스템은 비밀키 발급을 담당하는 신뢰기관과 CAS 클라이언트를 다운로드 받는 DCAS 호스트 그리고 CAS 클라이언트를 송신하는 DCAS 서버로 구성된다. 이때 DCAS 서버는 다수 존재하며 방송사업자의 시스템 내에 존재한다. Table 1은 제안하는 시스템에서 사용하는 표기법이다.

Table 1. Notations used in proposed method

Notation	Description
P	Random generator of G_1
u	Secret key of DCAS host, Random element of G_1
t	Secret key of trusted authority, Random element of G_1
s_n	Secret key of n-th broadcasting industry, Random element of G_1
KDF_n	Key derivation function of n-th broadcasting industry

2) 제안하는 기법

제안하는 기법은 키 생성 및 관리와 MK 저장 및 콘텐츠 재생의 2단계로 구성된다. Fig. 3은 제안하는 하는 기법의 시스템 구성과 키 생성 및 관리 방법을 보여준다.

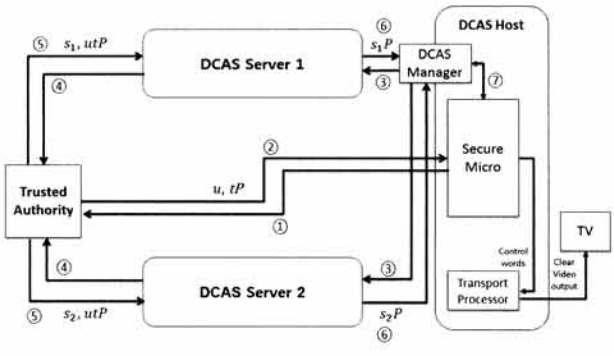


Fig. 3. Proposed key creation and management method

■ 키 생성 및 관리 단계

키 생성 및 관리는 호스트 비밀키 요청, 호스트 비밀키 발급, 방송 서비스 요청, 호스트 확인 및 사업자 비밀키 요청, 사업자 비밀키 발급, 사업자 비밀키 발급, MK 생성의 순서로 진행된다. 각각의 과정에서 수행되는 내용은 다음과 같다.

① 호스트 비밀키 요청: DCAS 호스트는 신뢰기관에게 자신이 사용할 비밀키와 신뢰기관의 비밀키를 요청한다.

② 호스트 비밀키 발급: DCAS 호스트의 요청을 받은 신뢰기관은 DCAS 호스트의 비밀키 u와 신뢰기관의 비밀키 t를 발급한다. 이때, 신뢰기관은 자신의 비밀키 노출을 막기 위해 tP형태로 전달한다. 신뢰기관은 DCAS호스트에게 안전한 비밀키를 전달을 위해 오프라인을 이용해 발급하거나 SSL/TLS등과 같은 안전한 통신채널을 사용한다.

③ 방송 서비스 요청: DCAS 호스트는 DCAS 매니저를 통해 방송 사업자1과 방송 사업자2에게 서비스 사용 요청을 한다.

④ 호스트 확인 및 사업자 비밀키 요청: 서비스 요청을 받은 방송 사업자1과 2는 신뢰기관에게 DCAS 호스트의 정보 확인과 비밀키를 요청한다.

⑤ 사업자 비밀키 발급: 방송 사업자들의 요청을 받은 신뢰기관은 각 방송 사업자의 DCAS 서버를 위한 비밀키 s_1, s_2과 신뢰기관과 사용자의 정보가 포함되어 있는 비밀키 utP를 각각 발급한다. 신뢰기관으로부터 발급받은 비밀키를 이용해 MK로 사용할 $e(utP, P)^{s_n} = e(P, P)^{uts_n}$을 계산한다.

⑥ 사업자 비밀키 전송: 각 방송 사업자들은 DCAS 호스트의 DCAS 매니저에게 신뢰기관으로부터 발급받은 비밀키

s_n에 P를 곱한 s_nP를 전달한다.

⑦ MK 생성: DCAS 호스트에서는 DCAS 매니저를 통해 전달받은 s_nP와 신뢰기관으로 전달받은 tP 그리고 호스트의 비밀키 u를 이용해 MK로 사용할 $e(s_nP, tP)^u = e(P,P)^{s_n tu}$를 계산한다.

DCAS 서버와 DCAS 호스트가 ⑤번과 ⑦번을 통해 각각 계산하는 MK가 동일함은 다음을 통해 확인할 수 있다.

$$e(utP,P)^{s_n} = e(s_nP, tP)^u = e(P,P)^{s_n tu}$$

■ MK 저장 및 콘텐츠 재생

MK는 AK를 암호화하는데 사용되는 키로 서로 다른 CAS는 서로 다른 형태의 MK를 사용할 것이다. 따라서 SM에 저장되는 MK의 형태는 $e(P,P)^{s_n tu}$형태가 아닌 각 DCAS 시스템이 사용하는 MK의 형태가 되어야한다. 예를 들어 DCAS 시스템 1의 경우 AK 암호화에 AES-256을 사용할 경우 MK는 256비트여야 하고, DCAS 시스템 2의 경우 AK 암호화에 AES-128을 사용할 경우 MK는 128비트이어야 한다. 각 DCAS 시스템에 적합한 MK 형태로 변경하기 위해서 키 유도 함수를 사용한다. SM에는 다음과 같은 형태의 MK들이 저장된다.

$$KDF_1(e(P,P)^{s_1 tu}, SN_1) = MK_1$$
$$KDF_2(e(P,P)^{s_2 tu}, SN_2) = MK_2$$
$$\vdots$$
$$KDF_n(e(P,P)^{s_n tu}, SN_n) = MK_n$$

DCAS 서버는 DCAS 호스트가 다운로드 할 DCAS 클라이언트에 키 유도함수를 포함하여 전달한다. 이를 통해 DCAS 서버와 DCAS 호스트는 키 유도 함수를 공유할 수 있다. 키 유도 함수 KDF는 $e(P,P)^{s_n tu}$와 클라이언트가 다운로드 될 때 전달하는 임의의 일련번호를 입력받아 일정한 크기의 비트를 출력하는 암호학적 일방향 해쉬함수이다. DCAS 클라이언트가 다운 된 후에는 DCAS 클라이언트가 실행 될 때 DCAS 서버로부터 새로운 일련번호를 수신하고 이를 이용해 새로운 MK를 생성한다.

DCAS 호스트는 위와 같이 생성된 MK를 SM에 저장하여 놓고 MPEG-TS의 CAT에 포함되어 있는 CAS ID를 통해 현재 사용되는 CAS의 종류와 그에 대응되는 MK를 사용하여 AK를 복호화할 수 있게 되고 복호화 된 AK를 이용해 CW를 복호화하여 콘텐츠를 시청할 수 있게 된다.

4. 제안 기법에 대한 분석

이 장에서는 제안하는 기법의 효율성과 안전성에 대해 분석한다. 효율성은 DCAS 호스트 내에서 서로 다른 CAS 간 이동 시 필요한 연산을 기존에 제안된 DCAS 기법들과 비교하였으며 안전성은 제안하는 기법이 키 확립 기법의 보안 요구사항을 만족하는지에 대해 분석한다.

4.1 효율성 분석

하나의 DCAS 호스트에 여러 종류의 CAS가 다운로드 될 경우 채널 전환과 같은 CAS간 이동이 필요할 경우 하드웨어 기반 CAS를 그대로 사용하는 경우 스마트카드나 케이블카드 등 MK 저장매체의 교체가 필요하게 될 것이다. Moon 등은 다수개의 CAS를 다운로드 하여 DCAS 호스트 내에 저장하여 놓고 필요한 CAS를 선택하여 사용하는 방법을 제안하였으나 MK는 기존 하드웨어 기반 CAS의 방법을 그대로 사용하였다[16]. 하드웨어 기반 CAS를 그대로 사용하지 않고 DCAS 서버와 DCAS 호스트 간 상호인증에 사용되는 키를 사용하는 방법인 강성구 등이 제안한 기법[9]과 최현우 등이 제안한 기법[10]의 경우 CAS의 변경 시 DCAS 서버와 DCAS 호스트 간의 상호인증 절차를 매번 거침에 따른 지연 시간을 야기할 것이다. 이러한 방법은 실시간 방송 환경에는 적합하지 못하다.

제안하는 기법은 이러한 문제를 해결하기 위해 신뢰기관, DCAS 서버, DCAS 호스트 간의 3자간 키 동의 통해 생성된 MK를 DCAS 호스트의 SM에 저장하는 방법을 사용하였다. 이를 통해 MK저장 매체의 교체가 불필요하며 한번 생성한 MK를 지속적으로 사용함으로써 빠른 CAS 간 전환이 가능하다는 장점을 가진다.

제안하는 기법에서는 신뢰기관, DCAS 서버, DCAS 호스트 3개체 간 동일한 키를 공유하기 하기 위해 3자간 키 동의 기법을 사용하였다. 키 동의를 하려는 A, B, C 세 개체가 있고 각각의 비밀키를 a, b, c라고 했을 때, 곱셈순환군을 이용하여 Diffie-Hellman 키 동의를 할 경우 g^{abc}의 형태로 키를 만들기 위해서는 2 라운드 이상의 통신이 필요하다. 개체 A를 예로 들면, A는 B, C와 각각 키 동의를 하고 B 또는 C로부터 B, C 간 동의 된 값 g^{bc}를 전달받아야 g^{abc} 형태의 키를 생성할 수 있게 된다. 하지만 pairing을 이용할 경우 A는 B, C로부터 bP와 cP를 전달 받아 pairing 연산의 bilinear 특성을 이용하여 $e(bP,cP)^a = e(P,P)^{abc}$의 형태의 키를 1 라운드 만에 쉽게 생성하는 것이 가능하다.

제안하는 기법에서 사용한 pairing 연산은 많은 컴퓨팅 능력을 요구하는 연산으로 알려져 있지만 현재 상용화 되어 있는 TV, PC 심지어 휴대폰에서도 pairing 연산을 무리 없이 수행할 수 있음이 연구를 통해 보여 지고 있다[18].

4.2 안전성 분석

제안하는 기법은 pairing 기반의 3자간 키 동의 기법을 응용한 키 확립 기법이다. 키 동의 기법은 프로토콜에 참여하는 모든 개체들이 키 생성에 참여하는 것이다. 제안하는 기법은 모든 참여자가 키 생성에 참여하지 않고 신뢰기관에 키 동의에 필요한 비밀값을 다른 개체에게 전달해 주는 방

법을 사용하고 있기 때문에 프로토콜에 참여하는 참여자들 중 하나가 비밀통신에 사용할 키를 생성해 다른 사용자들에게 안전하게 전달하는 키 전송 프로토콜과 유사하다. 제안하는 기법의 안전성 분석을 위해 키 확립 프로토콜의 보안 요구사항들을 만족하는지를 분석한다. 대부분의 PBC 기반 암호기법들은 다음 3가지 어려움에 기반하고 있다.

- G_1에서의 Discrete Logarithm Problem (DLP): G_1의 원소 P와 aP가 주어졌을 때, $a(\in Z_q)$를 계산하는 문제를 말한다.
- G_1에서의 Computational Diffie-Hellman Problem (CDHP): G_1의 원소 P, aP, bP가 주어졌을 때, $abP(\in G_1)$를 계산하는 문제를 말한다.
- G_1과 G_2에서의 Bilinear Diffie-Hellman Problem (BDHP): G_1의 원소 P, aP, bP, cP 가 주어졌을 때, $e(P,P)^{abc}(\in G_2)$를 계산하는 문제를 말한다.

현재까지 DLP, CDHP, BDHP를 다항시간 내에 계산하는 것은 계산적으로 어렵다고 알려져 있다[17]. 이 논문에서 제안하는 프로토콜의 안전성은 위의 문제들을 다항시간 내에 계산하는 것이 어렵다는 가정에 기반하고 있다.

- 키 최근성: 생성된 비밀키의 최근성을 보장해야 한다. 현재 사용되고 있는 키가 현재 세션에서 생성되었음을 확인할 수 있어야 한다. 또한 이는 이전에 생성된 키의 재사용이 불가능해야 함을 의미한다. 제안하는 기법에서는 3.2.2절의 ⑤번과 ⑦번을 통해 확립된 공유키를 그대로 사용하지 않고 DCAS 클라이언트에 포함되어 있는 키 유도 함수와 임의의 번호를 이용해 실제 사용될 MK를 생성한다. DCAS 클라이언트 사용을 하나의 세션으로 가정하면 매 세션마다 사용할 키 유도 함수의 압력 값 중 하나인 임의의 일련번호는 변경되므로 제안하는 기법은 키 최근성을 만족한다.
- 키 기밀성: 생성된 비밀키의 기밀성을 보장해야 한다. 키 사용이 허가된 개체 이외에는 키를 계산하는 것이 불가능해야 한다. 제안하는 기법에서 생성하는 비밀키 즉 키 유도함수의 입력이 되는 값은 $e(utP,P)^{s_n}=e(s_nP,tP)^u=e(P,P)^{s_ntu}$의 형태이다. 제안하는 시스템에서 DCAS 서버와 신뢰기관, DCAS 호스트 내의 SM과 신뢰기관과의 통신채널은 오프라인 또는 안전한 통신채널을 사용함을 가정한다. 공개된 채널을 통해 전송되는 값은 DCAS 서버가 DCAS 호스트에게 전송하는 s_nP 값이다. s_nP가 노출된다 하더라도 공유되는 비밀키 $(P,P)^{s_ntu}$를 계산하는데 필요한 값을 얻는 것은 DLP 이기 때문에 계산적으로 어렵다. 또한 $(P,P)^{s_ntu}$를 이용해 실제 사용되는 MK를 생성하기 위해서는 DCAS 서버가 DCAS 호스트에게 전송하는 키 유도함수와 일련번호가 필요하다. DCAS 서버로부터 키 유도함수와 일련번호가 포함되어 있는 CAS 클라이언트를 전송받기 위해서는 상호인증 과정을 거쳐야하기 때문에 키 유도 함수와 일련번호를 획득하는 것 역시 불가능하기 때문에 제안하는 기법은 키 기밀성을 만족한다.
- 키 인증: 생성된 비밀키를 사용하는 개체들이 서로 동일한 키를 가지고 있는지를 보장해야 한다. 키 확인 과정을 통해 동일한 키를 소유하고 있는지 확인하는 것이 가능해야 한다. 제안하는 기법은 명시적 인증이 아닌 묵시적 인증을 통해 키 인증 기능을 제공한다. 제안하는 기법을 통해 생성된 MK는 AK를 암호화하는데 사용된다. MK로 암호화된 AK는 EMM을 통해 DCAS 호스트에 전달되고 DCAS 호스트는 DCAS 서버와 공유하고 있는 MK를 이용해 AK를 복호화하고 ECM을 통해 전달 받은 AK로 암호화되어 있는 CW를 복호화하여 방송을 시청하는 것이 가능하다. 방송시청이 가능하면 동일한 키를 가지고 있는 것이고, 방송시청이 불가능 하다면 동일한 키를 가지고 있지 않은 것이 되는 묵시적 인증을 제공한다.

5. 결론 및 향후과제

하드웨어 기반 CAS가 가지는 여러 문제점들을 해결하기 위해 DCAS가 등장하였으며 현재까지 활발한 연구가 진행되었다. 하지만 DCAS에 대한 연구는 DCAS 서버와 DCAS 호스트 간의 상호인증과 DCAS 클라이언트의 안전한 전송 등에 관한 연구가 대부분이었다. 본 논문에서는 이러한 DCAS를 사용함에 있어 하나의 DCAS 호스트에서 서로 다른 DCAS 간 상호운용 시 이를 효율적으로 사용가능하도록 한 키 생성과 관리기법을 제안하였다, 제안하는 기법은 PBC기반의 키 동의 기법을 응용하여 신뢰기관, DCAS 서버, DCAS 호스트 3자간 공유키 확립을 쉽게 하였으며 DCAS 서버와 DCAS 호스트 간의 상호인증에 사용되는 키와 자격제어/관리에 사용되는 키의 분리를 통하여 효율적인 CAS 간 상호운용을 가능하게 하였다.

향후에는 구현 및 시뮬레이션을 통해 DCAS 간 상호운용 시 기존 기법들과의 제안하는 기법을 정량적으로 비교하는 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] EBU Project Group B/CA, "Functional model of a conditional access system," EBU Technical Review, pp.64-77, 1995.

[2] J.Y. Moon, B.J. Oh, and E.H. Park, "Trends on Technologies for Interoperability of Various Conditional Access Systems," ETRI Electronics and Telecommunications Trends, Vol.21, No.5, pp.21-29, 2006.

[3] ETSI TS 103 197 v1.4.1, Digital Video Broadcasting(DVB) Head-end implementation of DVB Simulcrypt, 2004.

[4] Common Interface Specification for Conditional Access and Other Digital Video Broadcasting Applications, EN50221, 1997.

[5] Cable Television Labortories, Inc., "OpenCable DCAS System Overview Technical Report," OC-TR-DCAS-D01-060 206, 2006.

[6] F. Kamperman and B. Rijnsoever, "Conditional Access System Interoperability Through Software Downloading," IEEE Transaction on Consumer Electronics, Vol.47, No.1, pp.47-54, 2001.

[7] Y. Jeong, S. Kim, H. Kim, H. Koo and E. Kwon, "A Novel Protocol for Downloadable CAS," IEEE Transaction on Consumer Electronics, Vol.54, No.3, pp.1236-1243, art. No.65, 2008.

[8] H. Jeong, S. Kim and D. Won, "On the Security of an Novel Protocol for Downloadable CAS," International Conference on Ubiquitous Information Management and Communication (ICUIMC), art. No.65, 2012.

[9] S. Kang,, J. Park, E. Paik, C. Park, and J. Ryou, "Technique and Implementation of Secure Downloadable Conditional Access System," Journal of The Korea Institute of Information Security & Cryptology (KIISC), Vol.19, No.6, pp.161-174. 2009.

[10] H. Choi, D. Yeo, J. Jang, and H. Youm, "Proposal of a Mutual Authentication and Key Management scheme based on SRP protocol," Journal of The Korea Institute of Information Security & Cryptology (KIISC), Vol.20, No.3, pp.53-65, 2010.

[11] D. Cho, B. Koh, and S. Yeo, "Secure D-CAS System for Digital Contetns Downloading Service," The Journal of Supercomputing, pp.1-15, 2011.

[12] H. Koo, O. Kwon, and S. Lee, "Key Establishment and Pairing Management Protocol for Downloadable Conditional Access System Host Devices," ETRI Journal, Vol.32, No.2, pp.204-213, 2010.

[13] S. Kim, Y. Jeong, O. Kwon, and J. Chung, "Method for Efficient CA Software Provisioning in Downloadable Conditional Access System," IEEE International Symposium on Comsumer Electronics (ISCE), pp.335-338, 2011.

[14] Y. Jeong, S. Kim, O. Kwon, C. Ahn and J. Hong, "Design and Implementation of Headend Servers for Downloadable CAS," IEEE International Conference on Comsumer Electronics (ICCE), pp.727-728, 2011.

[15] W. You, J. Lee, Y. Cho, O. Kwon, and S. Lee, "Design and Implementation of DCAS User Terminal," IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, (BMSB), pp.1-5, 2011.

[16] J. Moon, J. Kim, J. Park, and E. Paik, "Achieving Interoperability in Conditional Access Systems through the Dynamic Download and Execution of Cryptographic Software for the IPTV System," International Conference on Convergence and Hybrid Information Technology (ICCHIT), pp.380-385, 2008.

[17] D. Boneh and M. Franklin, "Identity-based Encryption from the Weil Pairing," Advances in Cryptology, Crypto '01, LNCS Vol.2139, pp.213-229, 2001.

[18] W. Shin, K. Fukushima, S. Kiyomoto, and Y. Miyake, "AMY: Use your cell phone to create a protected personal network over devices," IEEE Transactions on Consumer Electronics, Vol.57, No.1, pp.99-104, 2011.

이 훈 정

e-mail : hjlee@infosec.hanyang.ac.kr
2003년 단국대학교 전자컴퓨터학부(학사)
2005년 한양대학교 컴퓨터공학과(석사)
2005년~2009년 (주)한단정보통신 전임연구원
2009년~현 재 한양대학교 컴퓨터공학과 박사과정
관심분야 : 암호기술 응용, 키 관리

은 하 수

e-mail : hseun@infosec.hanyang.ac.kr
2010년 한양대학교 컴퓨터공학과(학사)
2012년 한양대학교 컴퓨터공학과(석사)
2012년~현 재 한양대학교 컴퓨터공학과 박사과정
관심분야 : 암호기술 응용, 암호학

오 희 국

e-mail : hkoh@hanyang.ac.kr
1983년 한양대학교 전자공학과(학사)
1989년 아이오와주립대학교 전자계산학과 (석사)
1992년 아이오와주립대학교 전자계산학과 (박사)
1993년~1994년 한국전자통신연구원 선임연구원
1995년~현 재 한양대학교 컴퓨터공학과 교수
관심분야 : 암호프로토콜, 네트워크 보안