디지털 방송 콘텐츠의 안전한 저장을 위한 Set Top Box와 비대칭 암호 시스템의 결합

이혜주* · 최형기** · 홍진우*

*한국전자통신연구원 전파방송연구소 방송미디어부

**한국정보통신대학원대학교 암호와 정보보안 연구실

Combination of Set Top Box and Asymmetric Cryptosystem for Secure Storage of Digital Broadcasting Contents

Hye Joo Lee* · Hyung Ki Choi** · Jin Woo Hong*

*Broadcasting Media Department, Radio & Broadcasting Laboratory, Electronics and Telecommunications Research Institute

**Cryptology & Information Security Laboratory, Information and Communication University,

Email:hyejoo@etri.re.kr, hkchoi@icu.ac.kr, jwhong@etri.re.kr

요 약

디지털 방송 콘텐츠 시청자에게 콘텐츠의 저장(녹화)을 허용함과 동시에 저작권 침해를 방지하기 위해 저장되는 콘텐츠에 대한 보호 기법이 필요하다. 보호 기법의 한 방법으로 콘텐츠를 암호화하여 저장할 수 있다. 본 논문에서는 Set Top Box에서 암호화를 수행할 수 있도록 방송 서버가 암호화 키를 MPEG-2 TS(transport stream) 스트림에 다중화하고 Set Top Box는 수신된 TS로부터 암호화 키를 역다중화하여 콘텐츠를 암호화하는 방법을 제안한다. 제안 방법은 MPEG-2 TS로 구성된 파일에 대해 PMT를 수정하여 암호화 키에 대한 정보와 이에 관련된 암호화 키를 다중화하고, 암호화 키를 추출하여 암호화를 수행한다.

ABSTRACT

It requires protection technologies to permit consumer to store a digital broadcasting content and at the same time to protect the intellectual property from illegal action. There is content encryption as one of protection technologies. In this paper, we proposed a protection scheme for digital broadcasting content that broadcasting server multiplexes the encryption key into MPEG-2 TS(transport stream) to be able to encrypt received TS at set top box. The proposed method is to modify PMT(program map table) for the information related encryption key and to multiplex key as TS packets. After then the encryption key is extracted from TS stream which is encrypted in set top box.

키워드

디지털 방송 콘텐츠 보호, 암호화, MPEG-2 TS, 다중화, 2차배포(superdistribution)

I. 서 론

디지털 방송 콘텐츠를 Set Top Box의 하드 디스크나 개인용 비디오 녹화기(personal video recorder, PVR) 등에 저장하는 경우, 발생할 수 있는 위협은 소비자의 2차 배포(superdistribution)에 의한 저작권 침해이다. 이와 같이 소비자에게 디지털 방송 콘텐츠의 저장을 허용하면서 저작권 침해를 방지하기 위해서 콘텐츠 보호 기법이 필요하다. 일반적으로 콘텐츠 보호를 위한 기법으로 DES와 같은 암호화 기법을 적용하는데, 이 경우에는 서버가 콘텐츠를 암호화하여 클라이언트 측에 전송하고, 클라이언트는 복호화 키를 서버로부터 정당하게 획득하여야만 암호화된 콘텐츠를 이용할 수 있게 된다.

그러나, 방송 환경에서 방송되는 콘텐츠는 접

근이 허가된 시청자가 일단 시청 가능해야 하기 때문에 위와 같은 시나리오는 방송 환경에는 적합하지 않다. 따라서 방송 서버는 디지털 방송 콘텐츠의 전송과 함께 암호화 키를 전송하고 Set Top Box는 시청자가 프로그램을 시청함과 동시에 저장을 요구하는 경우 암호화 키를 이용하여 수신된 방송 프로그램을 암호화하여 저장하도록 하는 방법이 고려될 수 있다.

본 논문에서는 위와 같은 경우를 고려하여 방송 서버가 MPEG-2 TS(transport stream)에 암호화 키를 다중화하고 Set Top Box에서 암호화 키를 역다중화하여 암호화를 수행하는 시나리오를 가정한다. 이에 암호화 키를 다중화하기 위한 MPEG-2 TS 상의 신택스 구조를 정의하고 Set Top Box에서의 처리를 제안한다. 본 논문은 다음과 같이 구성된다. 먼저, 2장에서는 디지털 방송 콘텐츠를 보호하기 위한 기존의 방법들을 기술하고 3장에서는 MPEG-2 TS 패킷 구조와 암호화 키를 다중화하기 위한 신택스 구조 및 Set Top Box에서의 처리 과정을 기술한다. 그리고 4장에서는 소프트웨어적으로 암호화 키를 다중화하고 암호화를 수행한 결과를 나타내고, 마지막으로 결론으로 5장에서는 향후의 과제를 기술한다.

II. 디지털 방송 콘텐츠 보호 방법

2.1 제한 수신 시스템

제한 수신 시스템(conditional access system)[1]은 케이블방송이나 위성 방송과 같은 채널에 대한 접근이 허가된 특정 가입자만이 프로그램을 시청할 수 있도록 하기 위한 시스템으로 자격 제어 기능 및 자격 관리 기능, 그리고 스크램블링(scrambling) 및 디스크램블링(descrambling) 기능이 요구된다. 스크램블링은 전송되는 방송 스트림을 DES와 같은 암호화 방법을 이용하여 TS의 헤더부분을 제외한 유료부하를 암호화하는 기법으로, 스크램블링을 수행할 때 제어단어(control word, CW)를 이용한다. 자격제어기능은 CW를 인증키(authorization key, AK)로 암호화하여 ECM(entitlement control message)로 전송하는 것으로, 이 ECM으로부터 CW를 복호하여 스크램블링된 전송 스트림을 디스크램블링 할 수 있게 된다. 여기서, AK는 다시 분배 키(distribution key, DK)로 암호화하여 EMM(entitlement management message)에 포함시키게 된다. 그림 1은 이와 같은 과정을 나타낸 CAS의 블록도를 의미한다.

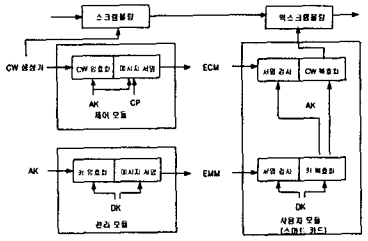

그림 1. CAS의 블록도

2.2 MPEG-2 IPMP

MPEG-2 IPMP[2]는 MPEG-2의 IPMP(intellectual property management & protection)에 관한 표준화 작업으로 IPMP 시스템은 콘텐츠를 소비할 수 있는 플랫폼인 단말과 콘텐츠의 관리와 보호를 위한 툴(tool), 툴과 단말(terminal) 사이의 정보 교환을 지원하는 인터페이스로 구성된다.

MPEG-2 IPMP는 콘텐츠의 관리와 보호를 위한 방법으로 툴(tool)의 개념을 이용한다. 툴이란 인증, 복호화, 워터마킹 등과 같은 IPMP 기능을 수행하는 하나 이상의 모듈로써, 유일한 식별자(identifier)인 Tool_ID로 식별되어진다. 단말은 이러한 툴을 수행함으로써 콘텐츠 관리와 보호를 수행하게 된다. 그림2는 MPEG-2 IPMP 구조를 나타내며, 툴에 대한 정보, 컨텐츠를 처리하기 위해 요구되는 IPMP 정보들이 MPEG-2 TS 혹은 PS(program stream)에 포함되어 진다.

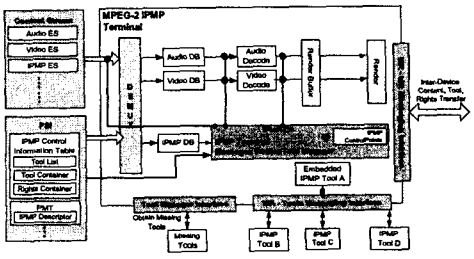

그림 2. MPEG-2 IPMP 구조

이외에도 디지털 방송 콘텐츠 서비스를 위한 규격을 제정하기 위한 표준화활동으로 TV Anytime Forum 등이 있다.

III. 디지털 방송 전송 스트림의 저장을 위한 암호화 키 다중화 방법 및 암호화

콘텐츠를 보호하기 위한 암호화 방법[3]은 대칭키 기반 암호 시스템(symmetric cryptosystem)과 비대칭키 기반 암호 시스템(asymmetric cryptosystem)으로 나눌 수 있다. 대칭키 기반 암호 시스템은 암호화 키와 복호화 키가 동일한 것을 의

미하는 것으로 DES와 같은 암호 알고리즘을 이용한다. 반대로 비대칭키 기반 암호 시스템은 암호화 키와 복호화 키가 다른 것으로 RSA와 같은 암호 알고리즘을 이용하게 된다. 대칭키 기반의 암호 시스템을 이용하는 경우, 복잡한 과정을 거쳐 Set Top Box로 전송하여야 한다. 그러나, 암호화 키를 비대칭키의 공개키(public key)를 이용하는 경우 복잡한 키 전송 과정이 필요하지 않는다.

MPEG-2 전송 스트림은 그림3과 같이 4바이트의 헤더와 유료부하(payload)를 갖는 188바이트의 TS 패킷으로 구성된다[4].

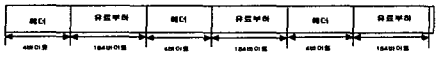

그림 3. MPEG-2 전송 스트림

TS 패킷의 헤더에는 13비트로 구성된 PID(packet identifier)라고 하는 유료부하의 데이터 타입을 지시하는 필드가 있다. TS 패킷의 종류에는 일정한 간격으로 반복되어 존재하는 PSI(program specification information) 정보가 있으며, 이것은 표1과 같이 4개의 테이블로 분류된다.

표 1. PSI 정보

테이블	의미
PAT	Program Association Table로써, 현재 전송되고 있는 프로그램 번호 및 PMT의 PID
PMT	Program Map Table로써, 한 프로그램에 포함되어 있는 ES(elementary stream)에 대한 내용 및 PID
NIT	Network Information Table로써 전송에 관련된 파라메터를 나타내는 값
CAT	Conditional Access Table로써, 접근 제어에 대한 관련 정보를 포함

PAT와 PMT를 좀 더 구체적으로 기술하면, PAT는 TS 패킷 헤더의 PID 값을 '0'으로 MPEG 규격으로 정의하고 있다. 따라서 PAT 이외는 PID로 '0'의 값을 가질 수 없다. PMT는 PAT에서 지정한 PMT_PID를 PID로 갖는 TS 패킷으로 ES에 대한 정보와 오디오 및 비디오 스트림이 포함된 ES PID를 가지고 있다. 따라서, MPEG 시스템 디코더는 먼저 PAT로부터 PMT_PID를 알아 낸 다음, PMT_PID를 PID로 갖는 TS 패킷으로부터 ES PID를 알아내어 각각의 오디오 및 비디오 ES를 디코딩할 수 있게 된다.

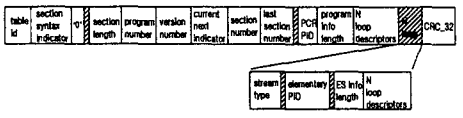

그림 4. program map section 구조

단말인 SetTop Box에서 암호화를 수행하기 위하여 암호화 키를 TS 전송 스트림에 다중화하는 방법으로 PMT의 기술자(descriptor)를 이용 가능하다. 그림4는 PMT의 신택스(syntax)를 나타내는데, 'N loop descriptor'으로 기술된 2개의 기술자 중에서 첫 번째 기술자는 전체 프로그램에 적용되는 정보가 기술되는 반면에, 두 번째의 기술자는 프로그램을 구성하는 ES 각각에 적용되는 정보가 기술되어진다. 따라서, 암호화를 전체 프로그램에 기술하는지, 혹은 어느 특정 ES에 적용하는 가에 따라 암호화 키에 대한 기술자의 위치가 달라질 수 있다.

암호화 키를 다중화하기 위한 PMT 내에 기술되는 기술자의 신택스는 표2와 같이 간단하게 구성하고, 이것을 ENCKEY descriptor라고 한다.

표 2. ENCKEY descriptor

Syntax	Num. of bit

ENCKEY_descriptor() {
tag
reserved
KEY_PID
}
	
	8bit
	3bit
	13bit

tag는 암호화 키 기술자를 지시하는 필드이며, KEY_PID는 암호화 키를 포함한 TS 패킷의 PID를 설정한다. 이와 같이 PMT 내의 ENCKEY descriptor에 의해 기술된 KEY_PID를 PID로 갖는 TS 패킷을 생성하고, TS 패킷의 유료부하에 암호화 키를 포함시킨다.

암호화 키를 포함한 TS 패킷의 신택스는 그림5와 같은 private section 구조를 이용하여 기술하게 된다.

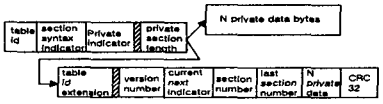

그림 5. private section 구조

private section의 구조를 살펴보면, section_syntax_indicator의 값이 '0'일 경우 private_section_length의 이후에 바로 private data가 나타나지만, 그렇지 않은 경우에는 table_id_extension 이후의 값들이 기술된 후에 private data가 나타나게 된다. private data가 하나 이상의 section에 포함될 경우에 이러한 형태로 기술된다.

위와 같이 암호화 키를 TS 스트림에 다중화하고 전송하게 되면 단말인 SetTop Box는 그림6과 같은 과정으로 암호화를 수행하게 된다. 먼저, 수신된 전송 스트림의 TS 패킷에 대하여, PAT로부터 PMT_PID를 검출하고, PMT_PID를 PID로 갖는 PMT로부터 ENCKEY descriptor를 파싱하여 KEY_PID를 알아내게 되고, 이 KEY_PID를 PID

로 갖는 TS 패킷으로부터 암호화 키를 역다중화하고 이 키를 이용하여 암호화를 수행하게 된다.

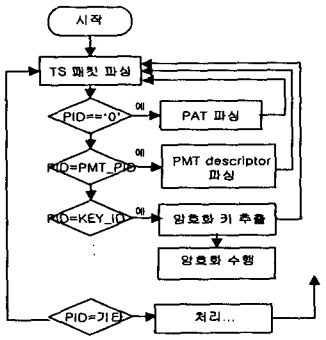

그림 6. Set Top Box에서의 처리

IV. 실험 및 결과

TS 스트림에 암호화 키를 다중화하여 TS를 암호화하는 제안 방법에 대하여, 다음과 같이 소프트웨어적으로 실험하였다. 먼저 이미 만들어진 TS 스트림에 PMT를 검색하여 원래의 PMT descriptor에 ENCKEY descriptor를 삽입하고, 암호화 키를 포함한 TS 패킷을 TS 스트림에 삽입하였다. 암호를 수행하기 위한 암호 라이브러리는 Peter Gutmann의 cryptlib v3.2 beta2[5]를 이용하였으며, 암호 알고리즘은 비대칭 키 암호 알고리즘RSA에 대하여 1024 비트의 키, 암호화 모드는 CBC(chiper block chaning)을 이용하였다.

그림7은 ENCKEY_descriptor와 암호화 키가 다중화된 TS 스트림을 나타내고 있다.

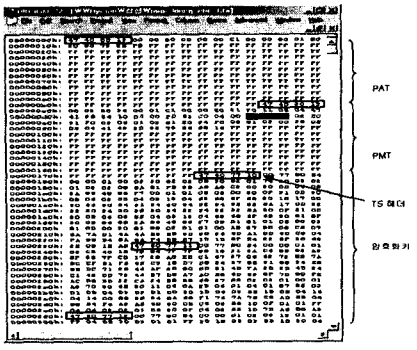

그림 7. 다중화된 TS 스트림

그림에서 짙은 음영으로 표시된 부분이 PMT 내의 ENCKEY descriptor로 암호화 키의 PID 값이 0x077으로 설정하였음을 나타내고 있다. 따라서, 암호화 키가 포함된 TS의 PID 값이 0x077으로 설정되어 있음을 알 수 있다.

TS의 암호화는 TS 내 헤더 부분과 NULL 패킷, PSI 패킷 등을 제외한 다른 TS 패킷의 유료부하 부분만을 암호화하였다. 표3는 암호화를 수행한 실험 결과를 나타내고 있다.

표 3. 다중화 및 암호화 결과

	값
원 TS 파일 크기	210,941KB
다중화 후 파일크기	214,237KB
암호화 후 파일크기	214,238KB
암호화된 TS 갯수	348,163
암호화 시간	58 초

표3의 결과에서, PMT와 암호화키가 포함된 TS 패킷의 반복 삽입에 의해 다중화 후의 파일크기가 증가된다. 그림 8-9는 MPEG-2 TS를 암호화된 상태의 스트림과 복호화된 상태의 MPEG-2 TS를 나타내고 있다. 암호화된 TS를 복호화하기 위해서는 RSA 공개키와 쌍인 개인키(private key)를 이용해야 한다.

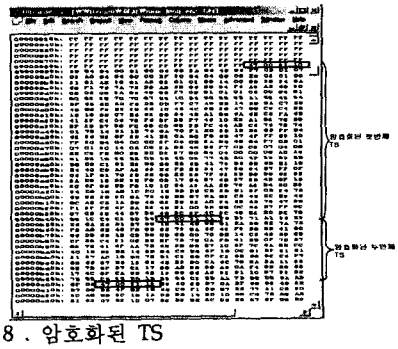

그림 8 . 암호화된 TS

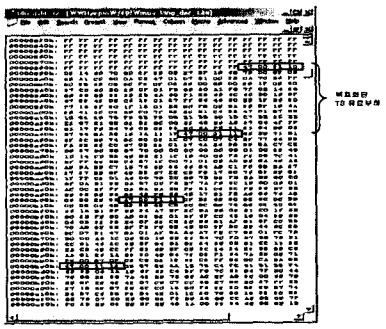

그림 9. 복호화된 TS

암호화된 TS를 복호화하기 위해서는 정당한 방법으로 복호화 키를 서버에 요청하여 획득하여야 한다. 이를 위해서는 복호화 키인 개인키는 DRM(digital rights management) 기법에서 이용

하는 라이센스 기법을 이용하여 복호화 키를 단말에 전달하는 것이 가능하다.

V. 결 론

본 논문에서는 디지털 방송 콘텐츠를 저장 매체에 저장하기 위한 보호기법으로 MPEG-2 TS에 암호화 키를 다중화하여 단말에서 암호화를 수행하는 방법을 제안하였다. 제안 방식에 의하면 디지털 방송 콘텐츠의 시청과 동시에 암호화를 수행할 수 있도록 하여 소비자의 2차 배포를 허용할 수 있다. 단, 복호화 키를 전송하는 과정은 본 논문에서 다루지 않았으며 이것은 향후의 과제가 될 것이다.

참고문헌

[1] 디지털 방송 RMP 기반 기술 연구에 관한 보고서, 한국전자통신연구소, 2002
[2] 강주성 외, 현대암호학, 경문사, 2000
[3] 유시룡 외, MPEG 시스템, 대영사, 1997
[4] ISO/IEC FCD 13818-11, 2003
[5] P.Gutmann, cryptlib Security Toolkit, http://www.cs.auckland.ac.ns/~pgut001/cryptlib, 2002