DVB-CSA3 스크램블 시스템의 설계 및 구현

*조용성, *정준영, *허남호, **임한재
*한국전자통신연구원, **엘컴텍
*yscho73@etri.re.kr

Design and Implementation of DVB-CSA3 Scramble System

*Cho, Yong Seong *Jung, Joon Young *Hur, Namho **Im, Han Jae
*ETRI, **Elcomtech

요 약

최근 UHD 방송서비스에 대한 관심이 고조됨에 따라 고품질 방송 콘텐츠 보호에 대한 요구가 증가하고 있다. 이에 따라, DVB, MPEG, ATSC 등 국제 표준단체에서는 기존 방식보다 보안 성능이 우수한 디지털 방송 보호 규격을 논의하고 있으며, 디즈니, 파라마운트, 소니 픽처스 등 세계 주요 콘텐츠 제작사들이 설립한 비영리 기관인 MovieLabs 에서도 고품질 콘텐츠 보호를 목적으로 AES-128 또는 그 이상의 강도를 갖는 콘텐츠 암호화 알고리즘을 필수적으로 사용하도록 규정하였다. 본 논문에서는 디지털 방송 보안을 위해 널리 사용되고 있는 DVB-CSA 및 AES-128 보다 보안성능이 우수한 것으로 알려진 방송 콘텐츠 암호화 규격인 DVB-CSA ver3 표준 규격 기반으로 설계 및 구현된 스크램블 시스템에 대해 소개한다.

1. 서론

케이블, 위성 등 디지털 유료방송 시스템에서는 서비스에 가입한 정당한 시청자들만 방송을 시청할 수 있도록 제한수신 시스템 기술을 적용하고 있다. 제한수신 시스템은 인증 받지 않은 수신기를 통한 불법 시청을 방지하기 위해 방송 콘텐츠를 특정한 키(key)로 암호화하여 전송하는 스크램블링 기술을 기반으로 하고 있으며, 전 세계적으로 DVB-CSA (Common Scrambling Algorithm) 규격이 가장 많이 이용 되고 있다[1].

DVB-CSA 규격은 유료방송 시스템에서 동일한 방송 서비스에 복수의 제한수신 시스템을 적용할 수 있도록 모든 제한수신 시스템이 공통으로 사용하도록 규정한 방송 콘텐츠 공통 암호화 규격이다. 1994 년 유럽의 표준화 기구인 ETSI 를 통해 처음 제정되었고, 2012 년 차세대 보안 및 콘텐츠 보호 기술을 지원할 수 있도록 데이터 보안과 안전성을 향상시킨 DVB-CSA3 규격으로 발전하였다.

이후, UHD 방송서비스에 대한 관심이 높아지면서 UHD 방송과 관련한 상업적 요구사항을 검토하는 DVB-CM-UHDTV 분과에서는 UHD 방송서비스를 위한 콘텐츠 보호 규격으로 AES-128 과 DVB-CSA3 규격의 보안성과 안정성을 비교한 결과, DVB-CSA3 가 AES-128 보다 보안성능이 훨씬 우수한 것으로 판단하였다.

본 논문에서는 현재 디지털 방송 콘텐츠의 보호를 위해 가장 많이 사용되고 있는 DVB-CSA, AES-128 규격보다 보안성능이 우수한 방송 콘텐츠 암호화 규격인 DVB-CSA3 표준 규격 기반으로 설계 및 구현된 스크램블 시스템에 대해 소개하고자 한다.

2. DVB-CSA3 알고리즘

DVB-CSA3 알고리즘의 기본 구조는 데이터 암호화와 암호화 키 생성의 두 가지 기능 블록으로 구분할 수 있다. 데이터 암호화 블록은 변형된 AES-128 블록 암호화기와 DVB 에서 새롭게 정의한 비공개 XRC(eXtended emulation Resistant Cipher) 블록 암호화기가 중첩되는 3 계층 형태의 기본 구조를 가지며, 128 비트 단위의 평문 데이터(plain text)를 128 비트 크기의 키로 암호화하여 암호 데이터(cipher text)를 생성한다. 암호화 키 생성 기능은 IDEA-NXT 블록 암호화기와 DVB 의 비공개 S-box 알고리즘이 결합된 구조로, 128 비트 크기의 제어단어(Control Word)로부터 데이터 암호화를 위한 각 계층의 키를 생성한다.

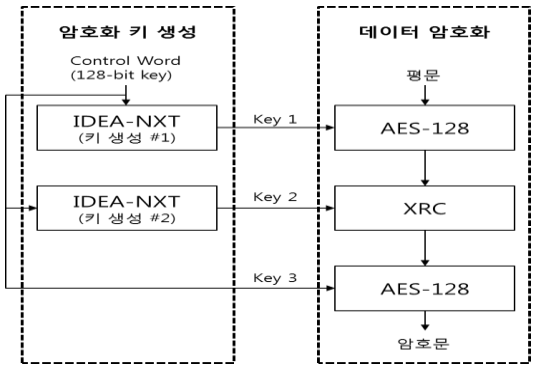

그림 1. DVB-CSA3 알고리즘의 기본 구조

디지털 방송시스템의 MPEG-2 TS 패킷을 앞서 설명한 알고리즘으로 암호화 하는 경우, 입력된 188 바이트의 MPEG-2 TS 패킷의 헤더를 제외한 184 바이트의 비디오 또는 오디오 페이로드를 16 바이트 크기의 블록으로 나누고, 각각의 블록을 128 비트의 키 값을 이용하여 암호화하는 방식으로 진행하게 된다.

3. 시스템 설계 및 구현

CSA3 스크램블러 코어는 188 바이트 크기의 MPEG-2 TS 패킷을 암호화하기 위해 그림 1 과 같은 암호화 블록 12 개를 연접시킨 구조를 가지며, 이전 블록의 암호문과 현재 블록의 평문을 XOR 한 값을 암호화하는 암호 블록 연쇄 모드(Cipher Block Chaining mode) 연산과 이전 블록의 평문과 암호문 그리고 현재 블록의 키 값을 XOR 하여 암호화 키로 사용하는 키 블록 연쇄 모드(Key Block Chaining Mode) 연산을 통해 패킷 단위로 MPEG-2 TS 가 암호화 될 수 있도록 설계되었다. 이와 같이 설계된 CSA3 스크램블러 코어는 Altera FPGA(Arria-II GX, EP2AGX260FF35I3)에 HDL 로 구현하였다.

디지털 방송시스템을 위한 DVB-CSA3 실시간 스크램블 시스템은 그림 2 와 같이 RF&ASI 입력 모듈, RF(QAM) 출력 모듈, DVB-CSA3 스크램블러 모듈을 포함하는 보드로 제작하였다. RF&ASI 입력 모듈을 통해 입력된 MPEG-2 TS 는 DVB-CSA3 스크램블러 모듈에서 암호화 된 후, RF 출력 모듈을 통해 출력된다.

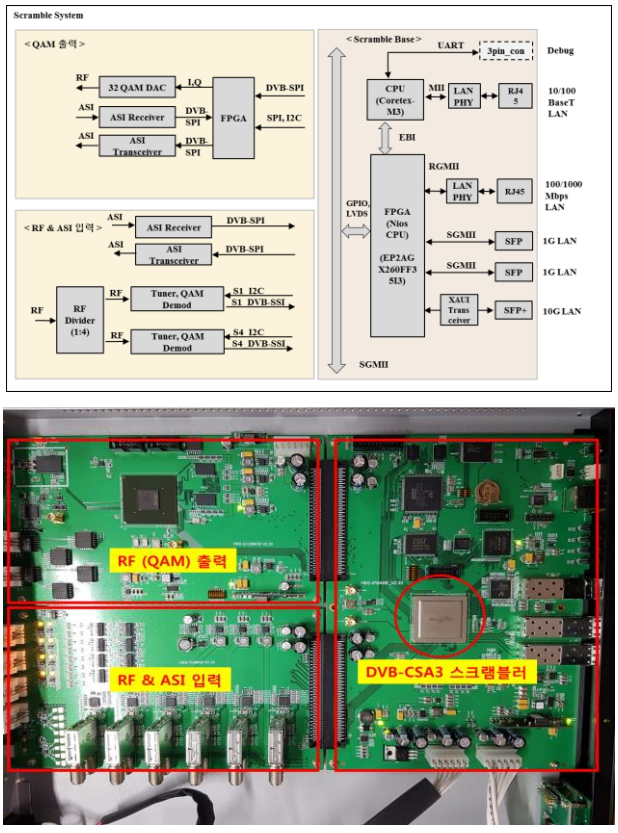

그림 2. DVB-CSA3 스크램블 시스템 구성도 및 보드 형상

구현된 스크램블 시스템의 기능 및 성능은 CSA3 표준 문서의 테스트 벡터를 이용하였다. 184 바이트 크기의 평문 데이터에 4 바이트 헤더를 붙여 실제 MPEG-2 TS 와 동일한 크기의 패킷을 생성하고, 이를 FGPA 에 구현된 스크램블러에서 암호화 한 후, 그 결과를 표준 문서의 암호화 값과 비교하여 구현된 스크램블 시스템이 규격과 동일하게 동작하는지 여부를 검증하였다. 또한, MPEG-2 TS 패킷 입력 시간과 스크램블 처리 후 패킷 출력 시간을 측정하여 구현한 알고리즘의 처리 지연시간을 검증하였다.

그림 3 은 구현된 DVB-CSA3 스크램블 시스템의 성능 시험 결과를 예시한 것이다.

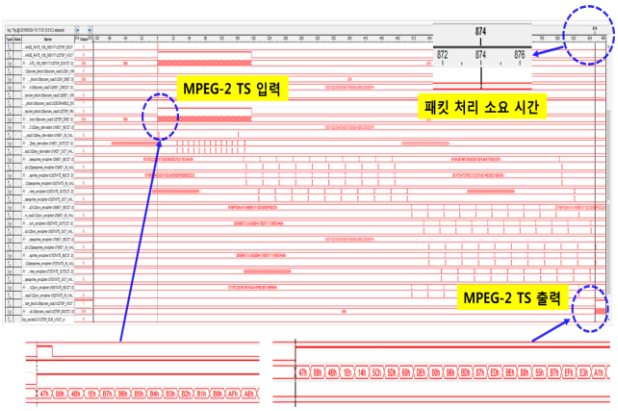

그림 3. DVB-CSA3 스크램블 시스템의 성능 검증

구현된 스크램블 시스템에서 입력 받은 MPEG-2 TS 패킷을 암호화한 후, 출력될 때까지 총 874 클럭이 소요되었다. 40.50MHz 속도의 클럭을 기준으로 MPEG-2 TS 패킷 한 개를 처리하는데 약 21.579us (24.69ns x 874 clock) 정도의 시간이 소요되므로, 초당 최대 70Mbps 정도의 MPEG-2 TS 를 실시간으로 암호화 할 수 있다.

4. 결론

본 논문에서는 DVB-CSA3 표준을 기반으로 설계 및 구현된 스크램블 시스템을 소개하였다. 또한, 구현된 시스템의 성능 검증을 통해 실시간 스크램블 시스템으로 활용할 수 있음을 확인하였다.

향후 시스템 구조 수정 및 최적화를 통해 시스템에서 처리할 수 있는 최대 데이터량을 더욱 늘릴 수 있도록 노력할 예정이다.

감사의 글

본 연구는 미래창조과학부 및 정보통신기술연구진흥센터의 정보통신 · 방송 기술개발사업의 일환으로 수행하였음. [B0484-15-1013, 고품질 UHD 방송 서비스를 위한 스크램블 시스템 개발]

참고문헌

[1] Ralf-Philipp Weinmann, Kai Wirt, “Analysis of the DVB common scrambling algorithm”, Communications and Multimedia Security, vol. 175, pp. 195-207