(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년11월07일
(11) 등록번호 10-1081160
(24) 등록일자 2011년11월01일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04L 9/30* (2006.01)
H04L 9/08 (2006.01) *H04L 12/22* (2006.01)
(21) 출원번호 10-2011-7019418(분할)
(22) 출원일자(국제출원일자) 2004년03월05일
심사청구일자 2011년09월02일
(85) 번역문제출일자 2011년08월22일
(65) 공개번호 10-2011-0099067
(43) 공개일자 2011년09월05일
(62) 원출원 특허 10-2005-7016825
원출원일자(국제출원일자) 2004년03월05일
심사청구일자 2008년12월29일
(86) 국제출원번호 PCT/US2004/006767
(87) 국제공개번호 WO 2004/082147
국제공개일자 2004년09월23일
(30) 우선권주장
10/387,163 2003년03월11일 미국(US)
(56) 선행기술조사문헌
US6157719 A
전체 청구항 수 : 총 31 항

(73) 특허권자
소니 일렉트로닉스 인코포레이티드
미국, 뉴저지 07656, 파크 리지, 원 소니 드라이브
(72) 발명자
캔델로, 브랜트, 엘.
미국 92029-6502 캘리포니아주 에스콘디도 콰일 글렌 웨이 10124
(74) 대리인
주성민, 이중희, 백만기

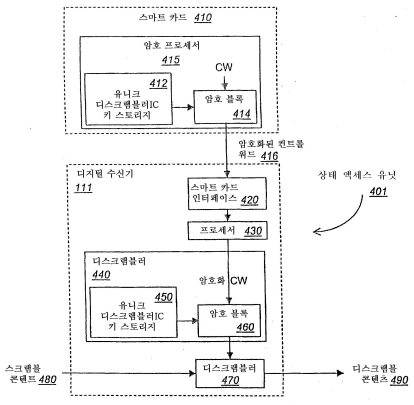
심사관 : 양종필

(54) 데이터 전송을 보호하기 위한 방법 및 장치

(57) 요 약

한 실시예에 따라, 프로그램 데이터를 스크램블 및 디스크램블하기 위한 방법은 제조자 식별자를 포함하는 메이팅 키 제너레이터 메시지의 수신을 포함한다. 메이팅 키 제너레이터 메시지는 제조자 식별자에 의해 식별된 제1 리모트 소스에 송신된다. 응답해서, 메이팅 키는 제1 리모트 소스로부터 수신된다. 그 후, 메이팅 키는 제2 리모트 소스에 제공되며, 그 후, 프로그램 데이터를 스크램블하는데 사용되는 서비스 키를 암호화하는데 사용된다.

대 표 도 - 도2



특허청구의 범위

청구항 1

보안 콘텐츠 전달 시스템에 있어서,

프로그램 데이터에 대한 요청을 개시하는 셋탑 박스 - 상기 셋탑 박스는 상기 셋탑 박스에 대한 고유 식별자를 포함함 -; 및

상기 셋탑 박스와 통신하는 상태 액세스(conditional access; CA) 제어 시스템을 포함하며,

상기 CA 제어 시스템은, 리모트 소스에 상기 고유 식별자 및 메이팅 키 제너레이터를 포함하는 정보를 송신하고, 응답으로, 상기 리모트 소스로부터 메이팅 키를 수신하며, 상기 메이팅 키는 상기 CA 제어 시스템으로부터 송신된 상기 고유 식별자 및 메이팅 키 제너레이터에 기초하며, 상기 메이팅 키는 상기 셋탑 박스에 송신되기 전에 상기 프로그램 데이터를 스크램블하는데 사용되는 컨트롤 워드를 암호화하는데 사용되는 것을 특징으로 하는 보안 콘텐츠 전달 시스템.

청구항 2

제1항에 있어서,

리모트 소스가 셋탑 박스 제조자와 각각 관련된 복수의 서버들인 것을 특징으로 하는 보안 콘텐츠 전달 시스템.

청구항 3

제2항에 있어서,

상기 CA 제어 시스템으로부터 송신된 정보는, 메이팅 키를 검색하기 위해 셋탑 박스 제조자와 관련된 복수의 서버들 중 하나를 식별하는 제조자 식별자를 포함하는 것을 특징으로 하는 보안 콘텐츠 전달 시스템.

청구항 4

제1항에 있어서,

상기 CA 제어 시스템으로부터 송신된 정보는, 메이팅 키의 길이가 1 패킷보다 긴 경우, 상기 메이팅 키를 형성하는 패킷들을 리오더하는데 사용되는 메이팅 키 시퀀스 번호를 포함하는 것을 특징으로 하는 보안 콘텐츠 전달 시스템.

청구항 5

제1항에 있어서,

상기 CA 제어 시스템으로부터 송신된 정보는, 프로그램 데이터 제공자를 식별하는 식별자를 포함하는데, 상기 제공자는 케이블 프로바이더, 위성 베이스 프로바이더, 지상 베이스 프로바이더 및 인터넷 서비스 프로바이더 중 하나인 것을 특징으로 하는 보안 콘텐츠 전달 시스템.

청구항 6

제1항에 있어서,

상기 CA 제어 시스템으로부터 송신된 정보는, 상기 CA 제어 시스템의 프로바이더를 나타내는 식별자를 포함하는 것을 특징으로 하는 보안 콘텐츠 전달 시스템.

청구항 7

제1항에 있어서,

리모트 소스가 CA 제어 시스템에 의해 액세스 가능한 복수의 데이터베이스를 포함하는 신뢰할만한 제삼국(trusted third party)인 것을 특징으로 하는 보안 콘텐츠 전달 시스템.

청구항 8

제1항에 있어서,

CA 제어 시스템이 메이팅 키를 수신한 후에 ECM(entitlement control message) 및 EMM(entitlement management message)을 생성해서 셋탑 박스에 제공하고, 상기 ECM은, ECM을 해독하는 적어도 하나의 글로벌 키와 키 식별자를 포함하고, 상기 키 식별자는 상기 글로벌 키가 부당하게 변경됐는지의 여부를 체크하는데 사용되기 위해 디지털로 부호화된(digitally signed) 값인 것을 특징으로 하는 보안 콘텐츠 전달 시스템.

청구항 9

제1항에 있어서,

상기 CA 제어 시스템이 메이팅 키를 수신한 후에 ECM(entitlement control message) 및 EMM(entitlement management message)을 생성해서 셋탑 박스에 제공하고, ECM이 암호화 포맷의 컨트롤 워드를 포함하고 EMM이 메이팅 키 제너레이터를 포함하는 것을 특징으로 하는 보안 콘텐츠 전달 시스템.

청구항 10

제9항에 있어서,

상기 셋탑 박스는 스마트 카드 및 디스크램블러 컴포넌트를 포함하는 것을 특징으로 하는 보안 콘텐츠 전달 시스템.

청구항 11

제10항에 있어서,

상기 셋탑 박스의 스마트 카드는 EMM을 수신하고, (i) EMM으로부터 메이팅 키 제너레이터를 상기 셋탑 박스의 디스크램블러 컴포넌트에 발송하며 (ii) ECM으로부터 복구된 암호화된 컨트롤 워드를 상기 셋탑 박스의 디스크램블러 컴포넌트에 발송하는 것을 특징으로 하는 보안 콘텐츠 전달 시스템.

청구항 12

제11항에 있어서,

상기 디스크램블러 컴포넌트가 메이팅 키와 동일한 키를 생성하기 위해 상기 디스크램블러 컴포넌트에 미리 저장된 유니크 키를 사용해서 상기 메이팅 키 제너레이터에 대한 암호화 오퍼레이션을 실행하는 제1 프로세스 블록을 포함하고, 메이팅 키와 동일한 상기 생성된 키는, 스크램블된 프로그램 데이터를 디스크램블링하는데 사용되는 컨트롤 워드를 생성하기 위해, 암호화된 컨트롤 워드를 해독하는데 사용되는 제2 프로세스 블록에 로드되는 것을 특징으로 하는 보안 콘텐츠 전달 시스템.

청구항 13

셋탑 박스의 제조자 식별자를 포함하는 메이팅 키 제너레이터 메시지를 수신하는 단계;

상기 제조자 식별자에 의해 식별된 제1 리모트 소스에 상기 메이팅 키 제너레이터 메시지 및 상기 셋탑 박스의 고유 식별자를 송신하는 단계;

상기 제1 리모트 소스로부터 메이팅 키를 수신하는 단계 - 상기 메이팅 키는 상기 송신된 고유 식별자 및 메이팅 키 제너레이터 메시지에 기초함 -; 및

상기 메이팅 키를 제2 리모트 소스에 제공하는 단계를 포함하며,

상기 메이팅 키는 그 후 프로그램 데이터를 스크램블하는데 사용되는 서비스 키를 암호화하는데 사용되는

것을 특징으로 하는 방법.

청구항 14

제13항에 있어서,

메이팅 키 제너레이터 메시지가 길이가 1 패킷보다 긴 메이팅 키를 형성하는 패킷들을 리오더(reorder)하는데

사용되는 메이팅 키 시퀀스 번호를 더 포함하는 것을 특징으로 하는 방법.

청구항 15

제13항에 있어서,

메이팅 키 제너레이터 메시지가 프로그램 데이터 제공자를 식별하는 식별자를 더 포함하는데, 상기 제공자는 케이블 프로바이더, 위성 베이스 프로바이더, 지상 베이스 프로바이더 및 인터넷 서비스 프로바이더 중 하나인 것을 특징으로 하는 방법.

청구항 16

제13항에 있어서,

메이팅 키를 제2 리모트 소스에 제공하는 단계가 셋탑 박스와 통신중인 CA 시스템에 메이팅 키를 제공하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 17

제16항에 있어서,

암호화 서비스 키 및 메이팅 키 제너레이터 메시지를 셋탑 박스의 디스크램블러 컴포넌트에 제공하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 18

제16항에 있어서,

상기 메이팅 키 제너레이터 메시지, 암호화된 서비스 키 및 암호화된 서비스 키와 관련된 서비스 층을 나타내는 값인 키 식별자를 포함하는 EMM을 생성하는 단계; 및

EMM을 셋탑 박스에 제공하는 단계

를 더 포함하는 것을 특징으로 하는 방법.

청구항 19

제16항에 있어서,

스크램블되지 않은 포맷의 전자 프로그램 가이드를 갖는 메타데이터를 CA 제어 시스템으로부터 셋탑 박스에 제공하는 단계 - 상기 메타데이터는 채널명, 프로그램 데이터 이름, 및 채널과 관련된 서비스 층을 나타내는 키 식별자를 각각 포함하는 복수의 태그 엔트리들을 포함함 - ; 및

메이팅 키 제너레이터 메시지를 CA 제어 시스템으로부터 셋탑 박스에 제공하는 단계를 더 포함하는

것을 특징으로 하는 방법.

청구항 20

제19항에 있어서,

상기 메타데이터가 메이팅 키 제너레이터 메시지를 더 포함하는 것을 특징으로 하는 방법.

청구항 21

상이한 콘텐츠 프로바이더와 각각 관련된 다수의 가입자 관리 시스템들과 통신하도록 적응된 메이팅 키 게이트웨이에 있어서,

프로그램 데이터 및 메이팅 키 제너레이터를 수신하도록 타겟팅된 셋탑 박스와 관련된 고유 식별자에 기초하여 제1 메이팅 키를 검색하는 수단; 및

다수의 가입자 관리 시스템들 중 제1 시스템에 상기 제1 메이팅 키를 송신하는 수단 - 상기 제1 메이팅 키는 상기 셋탑 박스에 제공된 적어도 하나의 서비스 키를 암호화하는데 사용됨 -

을 포함하는 것을 특징으로 하는 메이팅 키 게이트웨이.

청구항 22

제21항에 있어서,

상기 고유 식별자 및 상기 메이팅 키 제너레이터에 기초하여 제2 메이팅 키를 검색하는 수단; 및

상기 다수의 가입자 관리 시스템들 중 제2 시스템에 상기 제2 메이팅 키를 송신하는 수단을 더 포함하며,

상기 제2 메이팅 키를 검색하는 수단 및 상기 제2 메이팅 키를 송신하는 수단은, 상기 제1 메이팅 키를 검색하는 수단 및 상기 제1 메이팅 키를 송신하는 수단과 동시에 동작하는 것을 특징으로 하는 메이팅 키 게이트웨이.

청구항 23

제22항에 있어서,

적어도 두 개의 가입자 관리 시스템은 케이블 프로바이더, 위성 베이스 프로바이더, 지상 브로드캐스터(terrestrial broadcaster) 및 인터넷 서비스 프로바이더로 구성된 그룹에서 적어도 두 개를 포함하는 것을 특징으로 하는 메이팅 키 게이트웨이.

청구항 24

스크램블된 콘텐츠를 수신하고 스크램블된 콘텐츠를 디스크램블하도록 적응된 장치에 있어서,

(i) 암호화된 컨트롤 워드 및 (ii) 메이팅 키 제너레이터 메시지를 수신하도록 적응된 제거 가능 스마트 카드; 및

암호화된 컨트롤 워드 및 메이팅 키 제너레이터를 수신하고, 셋탑 박스에 로드된 스크램블된 콘텐츠를 디스크램블하는데 사용되는 컨트롤 워드를 복구하기 위해 암호화된 컨트롤 워드를 해독할 수 있는 키를 생성하도록 메이팅 키 제너레이터에 대한 암호 오퍼레이션을 실행하는 디스크램블러 컴포넌트

를 포함하는 것을 특징으로 하는 장치.

청구항 25

제24항에 있어서,

스마트 카드가 암호화된 컨트롤 워드를 포함하는 강화 컨트롤 메시지를 더 수신하고, 강화 컨트롤 메시지가 스크램블 콘텐츠가 송신된 특정 채널에 대한 액세스 기준을 포함하는 것을 특징으로 하는 장치.

청구항 26

제25항에 있어서,

디스크램블러 컴포넌트가 집적 회로인 것을 특징으로 하는 장치.

청구항 27

제26항에 있어서,

디스크램블러 컴포넌트에 의해 수신된 메이팅 키 제너레이터가 디스크램블러 컴포넌트 내에서 암호화된 컨트롤 워드를 전체적으로 복구하기 위해 강화 컨트롤 메시지를 해독하도록 적어도 하나의 키를 포함하는 것을 특징으로 하는 장치.

청구항 28

스크램블된 콘텐츠를 수신하도록 적응된 장치에 있어서,

네트워크 인터페이스; 및

네트워크 인터페이스를 통해 (i) 고유 식별자를 포함하는 메이팅 키 제너레이터 메시지, (ii) 적어도 하나의 암호화된 서비스 키 및 (iii) 암호화된 서비스 키와 관련된 서비스 층을 나타내는 대응 키 식별자를 수신하고, 스크램블된 콘텐츠를 디스크램블하는데 사용되는 서비스 키를 복구하기 위해 암호화된 서비스 키를 해독하기 위한

키를 생성하도록 메이팅 키 제너레이터에 암호 오퍼레이션을 실행하는 디스크램블러 컴포넌트

를 포함하는 것을 특징으로 하는 장치.

청구항 29

제28항에 있어서,

메이팅 키 제너레이터 메시지, 암호화된 서비스 키 및 대응 키 식별자가 싱글 EMM에 포함되는 것을 특징으로 하는 장치.

청구항 30

제28항에 있어서,

메이팅 키 제너레이터 메시지가 전자 프로그램 가이드와 관련된 메타데이터에 의해 제공되며, 동시에, 암호화된 서비스 키 및 대응 키 식별자가 EMM에 포함되는 것을 특징으로 하는 장치.

청구항 31

제28항에 있어서,

메이팅 키 제너레이터 메시지 및 대응 키 식별자가 모두 전자 프로그램 가이드와 관련된 메타데이터에 의해 제공되며, 동시에, 암호화된 서비스 키가 EMM에 포함되는 것을 특징으로 하는 장치.

명 세 서

기 술 분 야

[0001] 본 명세서는 1999년 3월 30일에 출원된 미국 가출원 번호 제60/126,805호를 근거로 한 2000년 2월 3일자 미국 특허 출원 번호 제09/497,393호의 일부계속 출원이다.

[0002] 본 발명의 실시예들은 디지털 장치와 관련된다. 특히, 본 발명의 한 실시예는 디지털 장치의 디지털 콘텐츠를 디스크램블링하기 위한 장치 및 방법에 관한 것이다.

배 경 기 술

[0003] 아날로그 통신 시스템은 디지털 통신 시스템에 빠르게 밀리고 있다. 디지털 텔레비전은 현재 국가적으로 이용될 수 있다고 예정된다. HDTV(High-definition television) 방송이 이미 주요 도시들에서 제한적으로 시작되었다. 유사하게, 인터넷 및 월드 와이드 웹의 폭발적인 성장으로 다른 콘텐츠뿐만 아니라 MP3-포맷 오디오 파일들과 같은 다운로드 가능한 오디오 비쥬얼 파일들의 증가에 따른 상관 성장이 야기된다.

[0004] 디지털 통신 시스템으로의 신속한 이동과 동시에, 디지털 기록 장치가 상당히 진보되어 왔다. DVD(digital versatile disk) 레코더, 디지털 VHS 비디오 카셋트 레코더(D-VHS VCR), CD-ROM 레코더(예를 들면, CD-R, CD-RW), MP3 기록 장치 및 하드 디스크 베이스 기록 유닛들은 단지 아날로그 통신 시스템에서 공지된 일반적인 강하(즉, 연속 카피들 간의 증가된 강하) 없이 고품질 레코딩 및 카피들을 야기할 수 있는 디지털 기록 장치들을 대표한다. 디지털 통신 시스템 및 디지털 기록 장치로의 이동 결합은 모션 픽처 및 음악 산업과 같은 콘텐츠 프로바이더와 관계된다. 콘텐츠 프로바이더는 저작권 보호 대상의 비허가 비제어 카피를 방지하기 희망한다.

[0005] 이에 응답해서, 지상 방송, 케이블 및 DBS(direct broadcast satellite) 회사 및 다운 로드 가능한 콘텐츠를 제공하는 인터넷 사이트들을 갖는 회사들이 보호 체계를 제시할 필요가 있다. CPTWG(Copy Protection Technical Working Group)의 인더스트리 커미티 서브그룹들인 DHSG(Data Hiding Sub Group) 및 DTDG(Data Transmission Discussion Group)의 5C 그룹에 의해 두가지 카피 보호 시스템들이 제안되었다(5C는 Sony, Hitachi, Toshiba, Matsushita 및 Intel의 대표자들을 포함함). CPTWG는 콘텐츠 프로바이더, 컴퓨터 및 컨수머 일렉트로닉 프라덕트 제조자들을 나타낸다.

[0006] DTDG DTCP(Digital Transmission Copy Protection) 제안은 IEEE 1394 직렬 버스와 같은 디지털 전송 매체를 통해 접속된 디지털 장치들 간에 전송되는 카피-보호 디지털 콘텐츠를 보호하기 위한 것이다. 디바이스 베이스 제안은 컴플라이언트 디바이스의 컴포넌트들을 인코드하기 위해 대칭 키 암호 기술들을 사용한다. 이는 디바이스가 컴플라이언트인지를 결정하기 위해 디지털 콘텐츠의 전송 전에 임의의 디지털 디바이스의 인증을

고려한다. 디지털 콘텐츠는 전송 전에 인코드되어서, 콘텐츠의 비허가 카피가 무지한 포맷을 갖는 카피가 되게 한다.

[0007] 한가지 콘텐츠 인코드 방법이 DHSG에 의해 제안되었으며, 워터마킹 기술들을 근거로 한다. DHSG 제안의 메인 포커스가 특히 DVD 시스템에 적용되는 디지털 영화 및 비디오 콘텐츠의 카피 보호에 있었더라도, 디지털 방송 및 네트워크를 통해 전자적으로 분산된 임의의 디지털 콘텐츠의 카피 보호에 적용될 수 있을 것으로 기대된다. 사용자에게 비가시적인 워터마킹 기술들은 콘텐츠가 어떻게 인코드되었는지를 정확하게 식별하는 것을 매우 어렵게 해서, 콘텐츠를 손상하지 않고 워터마크를 제거하거나 변경하는 것을 매우 어렵게 하는 방식으로 입력 콘텐츠가 마크되게 한다. DHSG는 기술이 달성해야만 하는 검출 및 제어의 세가지 주요 케이스들: 재생, 기록 및 생성 카피 제어를 결정했다. 워터마킹 기술이 적어도 콘텐츠가 "copy never", "copy once", "copy free" 콘텐츠인지를 콘텐츠 프로바이더가 열거할 수 있게 해줄 것으로 예상된다. "copy never"는 콘텐츠 카피가 허용되지 않음을 나타내도록 디지털 콘텐츠를 마크하는데 사용되고, "copy free"는 콘텐츠가 자유롭게 카피될 수 있으며 추가 정보로 마크될 수 있음을 나타낸다. 이는 전혀 마크되지 않는 것과 상이하다. 마지막으로, "copy once"는 디지털 콘텐츠 카피가 오직 1회만 허용됨을 나타내는데 사용된다. 카피가 실행됨에 따라, 고유 "copy once" 콘텐츠 및 새롭게 카피된 콘텐츠는 "no more copy"로 다시 마크된다. 물론, 카피 관리 커맨드의 다른 타입들은 예를 들어, 특정 시간 기간, 존속 기간 또는 재생 횟수로 디지털 콘텐츠의 재생을 제한할 수도 있다.

[0008] 따라서, 셋탑 박스, 디지털 텔레비전, 디지털 오디오 플레이어 및 유사 디지털 디바이스와 같은 디지털 디바이스의 기능은 상태 액세스(CA)의 역사적 역할, 즉, 단지 실시간 뷰 및/또는 청취를 위한 CA-클리어 포맷으로 콘텐츠를 디스크램블링하는 것을 넘어서 확장되며, 디지털 콘텐츠의 기록 및 재생에 대한 제약 및 조건들을 포함한다. 예를 들어, 현재, 차후 디스크램블링을 위한 스크램블 콘텐츠의 카피 및 뷰 또는 청취는 적합한 서비스/콘텐츠 프로바이더 허가 또는 디지털 디바이스에 제공된 키에 따라 허용될 수도 있다.

[0009] 전형적인 유료-TV용 상태 액세스 시스템은 백 채널이 유효하지 않은 원웨이 방송 시스템으로부터 시작되었다. 셋탑 박스와 같은 상태 액세스 유닛에서 스마트 카드와 같은 암호 프로세서는 프로그램 액세스를 자동으로 승인하기 위해 일반적으로 정보 및 기능을 갖게 된다.

[0010] 예를 들어, 유료-TV 액세스 제어 애플리케이션을 갖는 스마트 카드는 통상 특정 서비스 권리를 승인하는 EMM(entitlement management message)를 수신한다. 통상, 서비스들 또는 그룹 키들은 동시에 전달되며, 셋탑 박스가 IPPV 프로그램들을 뷰하도록 허용되는 경우, 크레딧 및 비용 제한 정보가 송신될 수도 있다.

[0011] 프로그램으로 튜닝할 때, 스마트 카드는 쇼 액세스 승인을 위해 스마트 카드가 필요로 하는 권리가 무엇인지를 기술하는 ECM(Entitlement Control Message)을 수신한다. 해커들은 필요한 대금을 지불하지 않고 프로그램을 뷰하기 위해 EMM 및 ECM을 모두 조작하려고 할 수도 있다. EMM 및 ECM이 조작될 뿐만 아니라, 하드웨어가 조작되기도 한다. 이러한 소프트웨어 조작 및 하드웨어 조작으로 프로그램 프로바이더 허가 없이 스마트 카드가 스크램블된 프로그램을 해독하게 된다.

[0012] 일단 처리되면 스마트 카드의 기능을 변경하기는 어렵다. 스마트 카드에 새로운 코드를 다운로드하는 메카니즘은 프로그램을 훔치기 위해 스마트 카드에 침해 코드를 로드하는 동일한 메카니즘들을 사용하고자 할 수도 있는 해커들에 의해 침해되기 쉽다. 액세스 제어 시스템을 업그레이드하는 한가지 "안전한" 방법은 필드로부터 현존 스마트 카드들을 제거하고 새로운 스마트 카드들을 제공하는 것이다. 그러나, 이는 비용이 많이 들며 논리적으로 어려울 수 있다.

발명의 내용

해결하려는 과제

[0013] 데이터 전송을 보호하기 위한 방법 및 장치를 제공하고자 한다.

과제의 해결 수단

[0014] 한 실시예에 따라, 프로그램 데이터를 스크램블 및 디스크램블하기 위한 방법은 제조자 식별자를 포함하는 메이팅 키 제너레이터 메시지의 수신을 포함한다. 메이팅 키 제너레이터 메시지는 제조자 식별자에 의해 식별된 제1 리모트 소스에 송신된다. 응답해서, 메이팅 키는 제1 리모트 소스로부터 수신된다. 그 후, 메이팅 키는 제2 리모트 소스에 제공되며, 그 후, 프로그램 데이터를 스크램블하는데 사용되는 서비스 키를 암호화하는데 사용된다.

발명의 효과

[0015] 데이터 전송을 보호하기 위한 방법 및 장치를 제공한다.

도면의 간단한 설명

[0016] 본 발명의 실시예들은 첨부 도면들에서 제한이 아닌 일례로서 설명된 것으로, 도면들에서 유사한 참조 부호들은 유사한 소자들을 나타낸다.

도 1은 디지털 디바이스를 포함하는 엔터테인먼트 시스템의 일례의 실시예이다.

도 2는 스마트 카드에 따라 동작하도록 적응된 상태 액세스 유닛을 포함하는 보안 콘텐츠 전달 시스템의 제1 일례의 실시예이다.

도 3은 컨트롤 워드들을 도 2의 스마트 카드로부터 상태 액세스 유닛으로 안전하게 전달하기 위한 방법의 일례의 실시예이다.

도 4 및 도 5는 컨트롤 워드를 암호화 및 해독하기 위한 방법의 일례의 실시예들이다.

도 6은 도 2의 상태 액세스 유닛 내에서 구현된 디스크램블러 집적 회로의 일례의 실시예이다.

도 7은 네트워크 커넥션을 통해 헤드엔드 서버에 적응된 디코더를 포함하는 보안 콘텐츠 전달 시스템의 제2 일례의 실시예이다.

도 8은 도 7의 헤드엔드 서버에 대한 디코더 어댑터의 보다 상세한 도면이다.

도 9는 도 2의 상태 액세스 유닛 또는 도 7 또는 도 8의 디코더에 전달될 수도 있는 서비스들의 일례의 실시예이다.

도 10은 컨트롤 워드들 또는 서비스 키들을 요청 및 수신하기 위한 방법의 일례의 실시예이다.

도 11a는 보안 콘텐츠 전달 시스템의 제3 일례의 실시예이다.

도 11b는 보안 콘텐츠 전달 시스템을 통해 송신된 메이팅 키 제너레이터를 형성하는 데이터 구조의 일례의 실시예이다.

도 11c는 도 11a의 시스템의 셋탑 박스에 루팅된 EMM의 일례의 실시예이다.

도 12는 도 11a의 시스템의 셋탑 박스의 디코더 내에서 구현된 디스크램블러 IC의 제1 일례의 실시예이다.

도 13은 보안 콘텐츠 전달 시스템의 제4 일례의 실시예이다.

도 14a는 보안 콘텐츠 전달 시스템의 제5 일례의 실시예이다.

도 14b는 도 14a의 시스템의 셋탑 박스에 루팅된 EMM의 일례의 실시예이다.

도 15는 도 14a의 시스템의 셋탑 박스에 루팅된 EPG(electronic program guide)와 관련된 메타데이터의 일례의 실시예이다.

도 16은 도 14a의 셋탑 박스 내에서 구현된 디스크램블러 IC의 제1 일례의 실시예이다.

도 17은 보안 콘텐츠 전달 시스템의 제6 일례의 실시예의 일부이다.

도 18은 디지털 디바이스가 카피 보호 기능으로 적응된 보안 콘텐츠 전달 시스템의 제7 일례의 실시예의 일부의 일례의 실시예이다.

도 19는 도 18의 디지털 디바이스 내에서 구현된 디코더의 일례의 실시예이다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 발명의 다양한 실시예들은 데이터 전송을 보호하기 위한 장치, 시스템 및 방법에 관한 것이다. 한 실시예에서, 이러한 보호는 디지털 디바이스들의 하나 이상의 콘텐츠 프로바이더들로부터의 디지털 콘텐츠의 디스크램블링 또는 해독을 포함한다. "콘텐츠 프로바이더"의 일례들은 지상 방송, 케이블 오퍼레이터, DBS(direct broadcast satellite) 회사, 인터넷을 통해 다운로드하기 위한 콘텐츠를 제공하는 회사, 또는 임의의 유사 콘텐

츠 소스들을 포함하는데, 이들로만 제한되지는 않는다.

[0018] 이하의 설명에서, 본 발명의 특징들을 설명하기 위해 특정 용어가 사용된다. 예를 들어, 용어들 "컴포넌트", "블록" 또는 "로직"은 하나 이상의 기능들을 실행하도록 구성된 하드웨어 및/또는 소프트웨어를 나타낸다. 예를 들어, "하드웨어"의 일례들은 프로세서(예를 들어, 마이크로프로세서, 애플리케이션 지정 집적 회로, 디지털 신호 프로세서, 마이크로-컨트롤러 등)과 같은 집적 회로를 포함하지만, 이들로만 제한되지는 않는다. 물론, 하드웨어는 대안적으로 유한 상태 머신(finite state machine) 또는 조합 논리(combinatorial logic)로서 구현될 수 있다.

[0019] "소프트웨어"의 일례는 애플리케이션, 애플릿, 루틴 또는 심지어 일련의 명령들의 형태로 된 실행 가능 코드를 포함한다. 소프트웨어는 프로그램 가능 전자 회로와 같은 기계 판독 가능 매체, 휘발성 메모리(예를 들어, 랜덤 액세스 메모리 등)와 같은 반도체 메모리 디바이스 및/또는 비휘발성 메모리(예를 들어, 임의의 타입의 판독 전용 메모리 "ROM", 플래시 메모리), 플로피 디스켓, 광 디스크(예를 들어, 컴팩트 디스크 또는 디지털 비디오 디스크 "DVD"), 하드 드라이브 디스크, 테이프 등의 임의의 타입에 저장될 수도 있다.

[0020] 용어 "프로그램 데이터"는 일반적으로 보안 콘텐츠 전달 시스템을 통해 전송중인 임의의 타입의 정보를 나타낸다. 프로그램 데이터의 일례들은 시스템 정보, 하나 이상의 ECM 또는 EMM, 디지털 콘텐츠, 및/또는 다른 데이터를 포함하는데, 각각은 간략하게 후술될 것이다. "메시지"는 비트 스트림, 패킷 또는 연속 패킷들로서 송신된 비트 집합이다.

[0021] 도 1을 참조하면, 엔터테인먼트 시스템(100)의 일례의 실시예가 도시되어 있다. 엔터테인먼트 시스템(100)은 하나 이상의 콘텐츠 프로바이더로부터 프로그램 데이터를 포함하는 정보를 수신하기 위한 디지털 디바이스(110)를 포함한다. 프로그램 데이터는 예를 들어 디지털 비트 스트림으로서 전파될 수도 있다. 디지털 디바이스(110)는 셋탑 박스와 같은 임의의 수의 제품들 또는 텔레비전, 컴퓨터, 오디오 재생 장치(예를 들어, 디지털 라디오), 오디오 기록 장치(예를 들어, MP3 플레이어), 비디오 기록 장치(예를 들어, 캘리포니아주 앨비소의 TiVo Inc.의 TIVO® 레코더) 등에 통합된 하나 이상의 컴포넌트들로서 동작할 수도 있다.

[0022] 예를 들어, 디지털 디바이스(110)는 내장형 아키텍처, 분할 보안 아키텍처 또는 외부 보안 아키텍처에 따라 구성될 수도 있다. 내장형 아키텍처로서, 한 실시예에서, 디지털 디바이스(110)는 권리 관리 및 디스크램블링 오퍼레이션들을 모두 지원하는 고정형 내부 회로를 포함하는 셋탑 박스로서 구현된다.

[0023] 대안으로, 분할 보안 아키텍처 실시예에 따라, 디지털 디바이스(110)는 권리 관리를 처리하는 제거 가능 스마트 카드를 수신하도록 적응될 수도 있으며, 입력 프로그램 데이터의 디스크램블링은 내부 회로에 의해 제어된다.

[0024] 그러나, 외부 보안 실시예에 따라, 디지털 디바이스(110)는 대역외 채널을 통해 메시지들을 송신 및 수신함으로써 권리 관리 및 디스크램블링 오퍼레이션들을 모두 처리하는 PCMCIA 카드를 가진 "전개 시점(point-of-deployment)" 제품일 수도 있다.

[0025] 물론, 또 다른 대안 실시예로서, PCMCIA 카드가 디스크램블링 오퍼레이션을 처리하도록 구성될 수 있도록 외부 보안 타입이 분할될 수도 있지만, 권리 관리를 처리하기 위한 스마트 카드로 통신하도록 적응될 수도 있다. 본 발명의 원리 및 범위 내에 여전히 속하면서 디지털 디바이스(110)의 여타 실시예들이 구현될 수도 있다.

[0026] 디지털 디바이스(110)는 입력 정보를 처리하고, 프로그램 데이터를 추출하며, 인식 가능한 포맷(예를 들어, 뷰 가능 및/또는 청취 가능)으로 프로그램 데이터를 제공하는 수신기(111)를 포함한다. 상술된 바와 같이, 프로그램 데이터는 시스템 정보, 권리 제어 메시지, 권리 관리 메시지, 디지털 콘텐츠 및 다른 데이터 중 적어도 하나 이상을 포함할 수도 있다.

[0027] "시스템 정보"는 프로그램명, 방송 시간, 소스 및 검색 및 디코딩 방법을 포함할 수도 있으며, 프로그램 데이터가 재생, 재송신 및/또는 기록되는 방법 및 시간을 제어하는 정보를 가진 디지털 수신기 및 다른 장치들을 제공하는 카피 관리 커맨드들을 포함할 수도 있다. 카피 관리 커맨드들은 ECM과 함께 송신될 수도 있으며, 일반적으로 특정 채널 또는 서비스에 대한 액세스를 조정하는데 사용된다. "EMM"은 권리들(때때로 "특권"이라고도 함)을 디지털 수신기(111)에 전달하는데 사용될 수도 있다. 특정 권리들의 일례들은 액세스 권리, 액세스 파라미터, 및/또는 디스크램블링 키들을 포함할 수도 있는데, 이들로만 제한되지는 않는다. 디스크램블링 키는 일반적으로 승인된 권리를 근거로 스크램블 포맷으로부터 클리어 포맷으로 데이터를 복구하기 위해 디스크램블러 로직에 의해 요구되는 코드이다. 마지막으로, 프로그램 데이터 스트림의 "콘텐츠"는 이미지, 오디오, 비디오 또는 임의의 결합을 포함할 수도 있다. 콘텐츠는 스크램블 또는 클리어 포맷일 수도 있다.

[0028] 도시된 바와 같이, 셋탑 박스로서 구현될 때, 디지털 디바이스(110)는 전송 매체(120)를 통해 엔터테인먼트 시스템(100)의 다른 컴포넌트들에 결합될 수도 있다. 전송 매체(120)는 디지털 디바이스(110)와 엔터테인먼트 시스템(100)의 다른 컴포넌트들 간의 프로그램 데이터를 포함하는 제어 정보 및 데이터를 전송하도록 동작한다. 전송 매체(120)는 전선, 광섬유, 케이블, 무선 신호 회로에 의해 설정된 무선 링크 등을 포함할 수도 있는데, 이들로만 제한되지는 않는다.

[0029] 디지털 디바이스(110)에 대응하는 제품 타입에 따라, 엔터테인먼트 시스템(100)은 전송 매체(120)에 결합된 오디오 시스템(130)을 포함할 수도 있다. D-VHS VCR과 같은 디지털 VCR(140)은 전송 매체(120)를 통해 디지털 디바이스(110) 및 엔터테인먼트 시스템(100)의 다른 컴포넌트들에 결합될 수도 있다.

[0030] 하드 디스크 기록 유닛(150)은 전송 매체(120)를 통해 디지털 디바이스(110) 및 다른 컴포넌트들에 결합될 수도 있다. 디스플레이(160)는 고선명 텔레비전 디스플레이, 모니터, 또는 디지털 비디오 신호들을 처리할 수 있는 다른 장치를 포함할 수도 있다. 제어 유닛(170)은 전송 매체(120)에 결합될 수도 있다. 마지막으로, 엔터테인먼트 시스템(100)의 컴포넌트들 각각의 동작을 조정 및 제어하기 위해 제어 유닛(170)이 사용될 수도 있다.

[0031] 디지털 프로그램의 콘텐츠는 스크램블 형태로 전송될 수도 있다. 한 실시예에서, 프로그램 데이터 파트로서, 액세스 요구 사항들이 스크램블 콘텐츠와 함께 디지털 디바이스(110)에 전송될 수도 있는데, 상기 디지털 디바이스(110)는 특히, 디지털 디바이스(110)가 셋탑 박스로서 동작할 때 상태 액세스 유닛으로서 작용하는 수신기(111)를 갖도록 구현된다. "상태 액세스 유닛(110)"으로 후술되는 상태 액세스 기능을 갖도록 구현된 디지털 디바이스(110)가 뷰 또는 청취 목적을 위해 스크램블 콘텐츠를 디스크램블하도록 허가받은지를 결정하는데 사용되는 제한 파라미터가 "액세스 요구 사항"이다. 예를 들어, 액세스 요구 사항은 콘텐츠를 인식(뷰 및/또는 청취)하는데 필요한 키이거나, 소정의 콘텐츠 프로바이더와 관련된 서비스 태그이거나, 심지어는 특정 디스크램블링 소프트웨어 코드일 수도 있다.

[0032] 스크램블 프로그램이 상태 액세스 유닛(110)에 의해 수신될 때, 프로그램에 대한 액세스 요구 사항들은 상태 액세스 유닛(110)이 실제로 가진 권리들과 비교된다. 한 실시예에서, 상태 액세스 유닛(110)이 클리어 형태로 스크램블 콘텐츠를 디스플레이하기 위해, 프로그램에 대한 액세스 요구 사항들이 상태 액세스 유닛(110)의 권리들과 비교된다. 권리들은 예를 들어, 상태 액세스 유닛(110)이 HBO(Home Box Office)와 같은 소정의 콘텐츠 프로바이더로부터 콘텐츠를 뷰/재생할 권리를 가짐을 나타낼 수도 있다. 권리들은 또한 콘텐츠를 디스크램블하는데 필요한 하나 이상의 키들을 포함할 수도 있다. 권리들은 또한 상태 액세스 유닛(110)이 콘텐츠를 디스크램블할 수 있는 시간 기간을 정의할 수도 있다.

[0033] 따라서, 한 실시예에서, 액세스 요구 사항들 및 권리들은 상태 액세스 유닛 또는 디코더가 특정 프로그램을 뷰하도록 허가받았는지를 결정하기 위해 액세스 제어 시스템의 파트를 형성한다. 텔레비전 방송, 구매 영화 등과 같은 오디오/비쥬얼 콘텐츠를 복구하는 메카니즘에 대한 설명이 후술될 것으로 예상된다. 그러나, 본 발명이 또한 시청 가능 콘텐츠(예를 들어, 디지털 뮤직 파일) 전용 디스크램블링에 적용될 수 있다고 예상된다.

[0034] 액세스 요구 사항 및 권리는 콘텐츠에 대한 다양한 지불 방법 및 다양한 스크램블 콘텐츠 액세스 승인 방법들을 소비자에게 제공할 수 있다. 이러한 선택 사항들은 PPP(pay per play), PPV(pay per view), IPPV(impulse pay per view), 타임 베이스 히스토리컬 PPT(pay per time), 카피 불가 영화 재구매, 퍼스널 스크램블링, 및 지역적 PPV를 포함할 수도 있다. "IPPV"는 셋탑 박스에 이전에 다운로드된 크레딧을 통해 PPV 영화들의 구매를 허용하는 기능이다. 구매 기록들이 저장되거나 지불 센터에 전화로 발송될 수도 있다. "타임 베이스 히스토리컬"은 예를 들어, 1997년 3월부터 12월까지와 같은 과거 시간 기간 동안 배달된 콘텐츠에 대한 액세스를 허용한다. 액세스 요구 사항들 및 권리들은 또한 스크램블 콘텐츠를 저장하는 상이한 옵션들을 소비자에게 제공할 수 있다.

[0035] 액세스 요구 사항들은 디지털 디바이스(110) 내에 배치되거나 PID(packet identifier)를 사용해서 전송 매체(120)를 통해 결합된 상태 액세스 유닛에 전달될 수도 있다. 각각의 PID는 소정의 서비스 또는 기능과 관련된 액세스 요구 사항들을 포함할 수도 있다. 상태 액세스 유닛에 전달된 콘텐츠는 다수의 PID들을 포함할 수도 있어서, 특정 수입 기능, 기술적 기능 또는 국부적으로 실행되는 다른 특별 기능들이 가능하다.

[0036] 콘텐츠를 수신하기 전에, 고객은 매체에 저장될 콘텐츠에 대한 액세스 승인을 위한 다수의 선택 사항들을 제공받을 수도 있다. 고객은 콘텐츠 액세스 및 뷰에 대한 권리를 구매하도록 요구받을 수도 있다. 따라서, 고객이 차후 검색 및 뷰를 위해 콘텐츠 기록을 희망하면, 고객이 구매한 액세스 요구 사항들이 콘텐츠와 함께 저장될 필요가 있다.

[0037] 또한, 도 18 및 도 19에 도시된 바와 같이, 디스크램블 콘텐츠(예를 들어, 트랜스포트 스트림)에 적용되는 카피 보호가 있을 수도 있다. 카피 보호 콘텐츠는 행선 인터페이스(예를 들어, NRSS-A, NRSS-B 또는 POD 모듈 인터페이스)와 소스를 상호 연결하는 인터페이스를 통해 다시 스크램블될 것이다. 소스 및 행선 인터페이스는 상기 콘텐츠를 다시 암호화하는데 사용되는 키와 일치할 필요가 있다. 이러한 카피 보호 키는 디지털 디바이스와 관련된 유니크 키로 암호화될 수 있다. 유니크 키는 EMM 또는 다른 방법, 예를 들어, 팩토리 로드 프로시져를 통해 수신될 수 있다.

[0038] 도 2에 도시된 바와 같이, 스마트 카드 인터페이스(420)와 함께 동작하도록 적응된 상태 액세스 유닛(401)을 포함하는 보안 콘텐츠 전달 시스템의 제1 일례의 실시예가 도시되어 있다. 본 실시예는 분할 보안 아키텍처 및 외부 보안 아키텍처와 일관된다. 분할 보안 아키텍처 구현에서, 디지털 디바이스(110)는 상태 액세스 유닛(401)(예를 들어, 도 1의 상태 액세스 유닛(110)과 동등함)으로서 동작하지만, 디지털 디바이스의 다른 타입 또는 셋탑 박스로서 구현된다. 외부 보안 아키텍처 구현에서, 상태 액세스 유닛(401)은 NRSS-B 상태 액세스 유닛이다.

[0039] 스마트 카드 인터페이스(420)가 디지털 수신기(111)에 내장될 수도 있지만, 디지털 수신기(111)는 예를 들어, 인터페이스(420)에 보완적인 카드 또는 디바이스(410)를 수신하기 위해 PCMCIA 카드 또는 USB(Universal Services Bus)와 같은 확장 슬롯을 가질 것으로 예상된다. 본 실시예에 있어서, 디지털 수신기(111)는 선택적 프로세서(430)와 디스크램블러 IC(440)를 포함한다.

[0040] 스마트 카드 인터페이스(420)는 스크램블 프로그램 콘텐츠를 디스크램블링하기 위한 하나 이상의 암호 컨트롤 워드를 포함하는 스마트 카드(410)를 수신한다. 스마트 카드(410)는 스마트 카드 인터페이스(420)에 컨트롤 워드(들)를 암호 형태로 전송할 수도 있다. 스마트 카드(410)와 스마트 카드 인터페이스(420) 간의 통신을 감시하는 인터로퍼에 의해 부적당하게 추출되는 것으로부터 하나 이상의 "CW"라고 하는 컨트롤 워드들을 보호하기 위해, 스마트 카드(410)는 CW를 암호화하기 위해 상태 액세스 유닛(401)에 유일한 암호 키를 사용할 수도 있다. 이는 상태 액세스 유닛(401)이 안전한 방식으로 CW를 해독할 수 있게 해주며 프로그램 콘텐츠를 디스크램블하기 위해 클리어 컨트롤 워드들을 사용할 수 있게 해준다.

[0041] 특히, 한 실시예에 따라, 예를 들어, ISO 7816 스마트 카드의 외부 암호 프로세서(415)는 콘텐츠를 디스크램블하는데 필요한 CW를 수신한다. 기억 소자(412)(예를 들어, 레지스터 또는 다른 휘발성 또는 비휘발성 메모리)는 CW를 암호화하기 위한 하나 이상의 키들로 미리 로드된다. 이러한 로딩은 스마트 카드(410) 제조 중에 실행되거나, 기억 소자(412)가 암호 프로세서(415)의 온칩 메모리일 때 암호 프로세서(415) 또는 기억 소자(412)의 제조 중에 실행되거나, 또는 스마트 카드 인터페이스(420)(도시되지 않음)을 통해 상태 액세스 유닛(401)을 통해 통신 경로를 통해 실행될 수도 있다. 스마트 카드(410)의 암호 블록(414)(예를 들어, 암호 프로세서(415)에 의해 실행되는 소프트웨어 또는 펌웨어, 전용 하드웨어 등)은 디스크램블러 IC(440)에 유일한 하나 이상의 키들로 CW를 암호화한다.

[0042] 본 실시예의 경우, 암호 CW가 해독 블록(460)(예를 들어, 상태 기계 또는 전용 회로)에 직접 송신될 수도 있지만, 스마트 카드(410)는 인터페이스(420)를 통해 프로세서(430)에 암호화 CW를 전달한다. 디스크램블러 IC(440)에 저장된 키들과 동일한 키들 또는 상기 키들로부터 유도된 키들을 사용하는 암호화가 아닌, CW에서 실행된 추가 혼잡 기술들을 방해하는 추가 오퍼레이션들을 실행하도록 구현될 수도 있다. CW가 디스크램블러 IC(440)에 의해 처리될 때까지 암호 포맷으로 유지됨을 주지하자. 따라서, 프로세서(430)와 디스크램블러 IC(440) 간의 통신은 안전하다.

[0043] 상태 액세스 유닛(401)의 디스크램블러 IC(440)는 기억 소자(450)에 기억된 하나 이상의 유니크 키들을 사용해서 CW를 해독할 것이다. 한 실시예에서, 기억 소자(450)는 상태 액세스 유닛(401)에 전송된 초기 프로그램 데이터를 통해 상태 액세스 유닛(401) 내에 구현된 후에 또는 제조자에서 로드된 하나 이상의 키 레지스터들을 포함한다.

[0044] 그 후 한 실시예에 따라, 해독 블록(460)은 디스크램블러 IC(440)에 위치한 디스크램블러 로직(470)의 ODD 및 EVEN 키 기억 소자들(도시되지 않음)에 교대로 해독된 CW를 기록한다. 디스크램블러 로직(470)은 그 후 정확한 시간에 입력 스크램블 콘텐츠(480)에 ODD/EVEN CW를 적용하고 디스크램블된 프로그램 콘텐츠(490)를 출력한다. 물론, 입력 스크램블 콘텐츠(480)의 디스크램블을 위해 ODD 및 EVEN 키 기억 소자들을 번갈아 로드하는 것이 사용될 수도 있다.

[0045] 따라서, CW가 암호 형태로 전송되기 때문에, 스마트 카드(410)로부터 상태 액세스 유닛(401)으로의 CW의 전송은

안전하다. CW가 안전하지 않은 프로세서(430)에 의해서 해독되지 않기 때문에, CW는 상태 액세스 유닛(401)에서 안전한 상태로 남게 된다. CW는 CW를 실제로 사용하는 디스크램블러 IC(440)에서만 해독되기 때문에, CW는 결코 클리어 형태로 공개되지 않으며, 해커에 의해 획득될 수 없다.

[0046] 또한, CW를 해독하는데 사용된 키는 디스크램블러 IC(440)의 하드웨어(예를 들어, 기억 소자(450))에 기억된다. 기억 소자(450)는 기억 소자(450)의 실리콘이 규명되지 않는 한 해킹될 수 없다. IC(440)의 기억 소자(450)에 기억된 키에 대한 시도가 이루어질 수도 있다. 그러나, 키가 충분히 크면, 공격 수단은 쓸모 없는 것으로 간주된다. 또한, CW가 관련 상태 액세스 유닛(401)에 유일한 키 또는 CW를 사용해서 스마트 카드(410)에 의해서 암호화되기 때문에, 키는 하나의 특정 상태 액세스 유닛(401)에 대해서만 유효할 수 있으며, CW를 해독하는 다른 유닛들에 의해서는 사용되지 않을 수도 있다. 따라서, 스마트 카드(410)로부터 상태 액세스 유닛(401)으로의 암호화된 컨트롤 워드(들)의 전송은 안전하며, 컨트롤 워드는 해커에 의해 침해되기 어렵다.

[0047] 디스크램블러 IC(440)는 컨트롤 워드의 안전한 프로세싱을 처리한다. 디스크램블러 IC(440)는 CPU, 펌웨어, 및 소프트웨어를 갖지 않는다. 복잡한 키 계층이 없다. 논프로세서 베이스 디스크램블러 IC(440)는 암호화 CW를 수신하고, 유니크 키를 상기 암호화 CW에 적용하며, 해독한다. 명령, 코드, 해싱 및 소프트웨어가 해독 블록(460)에 로드되지 않는다. 오직 단일 키 기능을 사용해서 디스크램블러 IC(440)의 하드 회로 또는 상태 기계에 의해 해독이 전체적으로 실행된다.

[0048] 일반적으로 "유니크 키"라고 하는 하나 이상의 유니크 키들은 제조 중에 기억 소자(450)에 프로그램될 수도 있다. 예를 들어, 한 실시예에서, 디스크램블러 IC(440)는 오직 한번 기록될 수 있는 비휘발성 유니크 키 기억 소자(450)를 갖는다. 셋탑 박스, 텔레비전, 또는 NRSS-B 모듈이 제조될 때, 기억 소자(450)가 프로그램된다. 본 실시예에서, 기억 소자(450)에 원래 로드되었던 유니크 키를 부적당하게 판독 또는 재기록하는 방법은 없다. 상태 액세스 유닛(401)의 일련 번호와 상태 액세스 유닛(401)의 디스크램블러 IC(440)에 로드된 유니크 키 간의 연관성이 기록될 수도 있다.

[0049] 상태 액세스 유닛(401)이 제조되고 스마트 카드(410)가 설치될 때, 스마트 카드(410)는 페어링시 상태 액세스 유닛(401)과 관련된 유니크 키를 수신할 수 있다. 그 때부터, 스마트 카드는 특정 호스트(예를 들어, 상태 액세스 유닛(401))에 "페어링"된다. 그 후, 스마트 카드(410)가 대체되거나 새로운 호스트로 이동되면, 스마트 카드(410)는 EMM을 통해 새로운 호스트와 관련된 유니크 키를 수신하도록 적응될 수도 있다. 물론, 대안으로서, 새롭게 프로그램된 유니크 키를 갖는 새로운 스마트 카드가 사용자에게 전달될 수도 있다.

[0050] 스마트 카드(410)로부터 상태 액세스 유닛으로 CW를 전송하기 위한 일례의 방법이 도 3에 도시되어 있다. 컨트롤 워드는 스마트 카드의 비휘발성 메모리에 기억된 키를 사용해서 스마트 카드(410)에서 암호화된다(블록(40)). 스마트 카드에 기억된 키는 디스크램블러 IC의 기억 소자에 기억된 키와 관련된다. 암호화된 컨트롤 워드는 스마트 카드로부터 수신된다(블록(41)).

[0051] 본 방법은 디스크램블러 IC의 프로그램 데이터를 포함하는 디지털 비트스트림을 수신하는 단계를 포함하는데, 프로그램 데이터는 시스템 정보 및 스크램블 디지털 콘텐츠를 포함한다(블록(42)). 암호화된 컨트롤 워드는 디스크램블러 IC의 기억 소자에 기억된 키를 사용해서 해독된다(블록(44)). 스크램블된 디지털 콘텐츠는 해독된 컨트롤 워드를 사용해서 디스크램블러 IC에서 디스크램블되고(블록(45)), 디스크램블된 디지털 콘텐츠가 출력된다(블록(46)).

[0052] 암호화 블록(414) 및 해독 블록(460)에 의해 실행되는 암호화 및 해독 기능들의 실시예들은 도 4, 도 5 및 도 6에 도시되어 있다. 상기 오퍼레이션들은 기억 소자들(412 및 450)에 기억된 유니크 키를 근거로 CW를 변환한다. DES, M6 또는 DVB 공통 스크램블링 알고리즘과 같은 암호화 알고리즘이 사용될 수도 있다. 도 4, 도 5 및 도 6에 도시된 실시예들에서는, 트리플 DES가 사용된다. 도 6에 도시된 바와 같이, 디스크램블러 IC(440)는 해독 블록(460)에서 CW를 해독하기 위해 트리플 DES를 사용한다. 해독 CW는 그 후 스크램블된 프로그램 콘텐츠(480)를 디스크램블하고 클리어 프로그램 콘텐츠(490)를 출력하기 위해 디스크램블러 로직(470)에 의해 사용된다.

[0053] 그러나, 컨트롤 워드(들)의 암호화 및 해독이 셋탑 박스에 국부적이기 때문에, 보다 견고한 암호화 전개시 단계적으로 실행할 수 있다. 예를 들어, 초기에 싱글 DES가 전개될 수도 있지만, 후에, 더블 또는 트리플 DES가 셋탑 박스들 및 스마트 카드들의 이미 처리된 페어링된 유닛들과 관련 없이 단계적으로 실행될 수 있다. 유니크 키의 키 길이는 유니크 키에 대한 해커들의 공격을 감소시키는 것을 돕기 위해 적어도 디스크램블된 CW만큼 클 수도 있다.

[0054] 도 2의 상태 액세스 유닛 구현의 다른 실시예에서, 스마트 카드는 도 7에 도시된 바와 같이 원웨이 또는 투웨이 네트워크(720)의 헤드엔드(710)에 의해 대체될 수도 있다. 헤드엔드(710)는 도 2의 로컬 암호 프로세서(415)의 액세스 권리들을 유지하는 대신, 디코더("디코더(701)"라고 함)로서 동작하는 디지털 디바이스에 대한 액세스 권리를 유지한다. 헤드엔드(710)는 디스크램블러 IC(740)에 기억된 유니크 키를 근거로 하나 이상의 서비스 키들(일반적으로 "서비스 키"라고 함)을 전달할 수 있다. 암호화 서비스 키는 하나의 채널로부터 다른 채널로의 전이를 용이하게 하기 위해 디코더(701)에 국부적으로 기억될 수도 있다. 서비스 키는 암호 형태로 기억되며, 필요할 때 디스크램블러 IC(740)에 로드된다. 서비스 키는 디스크램블러 IC(740)의 메모리(750)에 기억된 하나 이상의 유니크 키들을 사용해서 디스크램블러 IC(740)에서만 해독된다. 한 실시예에서, 서비스 키는 콘텐츠를 직접 디스크램블하기 위해 컨트롤 워드로서 사용된다. 다른 실시예에서, 서비스 키는 스크램블 콘텐츠와 함께 대역내에서 수신되어 디스크램블링을 위해 사용되는 하나 이상의 컨트롤 워드들을 해독하는데 사용된다.

[0055] 서비스 키는 상술된 도 2, 도 4, 도 5 및 도 6의 실시예들에서 컨트롤 워드를 위해 사용된 알고리즘들 중 하나를 사용해서 암호화 및 해독될 수도 있다. 서비스 키 암호화 및 해독에 사용된 알고리즘은 프로그램 콘텐츠를 스크램블 및 디스크램블하는데 사용된 알고리즘과 상이할 수도 있다. 예를 들어, M6는 스마트 카드 또는 헤드엔드 키 서버의 소프트웨어에서 실행하는 것이 보다 쉬울 수도 있다. 또한, 각각의 서비스 키는 상이한 공중 소유권 주장 가능 암호화 알고리즘을 사용해서 암호화될 수도 있다. 상이한 소유권 주장 가능 알고리즘들은 클론 하드웨어를 무효로 만드는 임의의 침해로서 생각될 수도 있다.

[0056] 헤드엔드(710)는 EMM의 채널 또는 "서비스 층"을 기준으로 하나 이상의 서비스 키들을 전달할 수 있다. 서비스 키들은 암호화되어, 디코더(701)에 국부적으로 기억되며, 상이한 채널들에 튜닝할 때 필요한 경우 프로세서(730)에 의해 사용된다. 셋탑 박스들이 헤드엔드(710)에 비해 하이 볼륨으로 처리되기 때문에, 셋탑 박스로부터 스마트 카드(및 대응 암호 프로세서)를 제거함으로써, 네트워크의 유료-TV 시스템을 구현하는 비용을 상당히 감소시킬 수 있다.

[0057] 본 실시예가 원웨이 (논-IPPV) 방송 네트워크에서 동작하지만, 또한, IPPV 또는 VOD 구매 또는 임의의 다른 비예약 서비스와 같은 특정 서비스에 대한 키들이 요청되는 투웨이 상호 동작 네트워크들에서도 실행된다. 새로운 서비스에 대한 액세스 승인 기능이 로컬 제어 암호 프로세서 대신 헤드엔드(710)에서 실행되기 때문에, 리턴 채널(721)은 서비스 키(들)를 요청하는데 사용된다.

[0058] IPPV 프로그램들의 다수의 충동 구매들에 의해 야기되는 헤드엔드(710)에서의 오버로드 문제점들을 방지하기 위해, 프리 프리뷰 기간이 결정될 수 있으며 IPPV 프로그램들이 실제 뷰에 앞서서 매매될 수 있다. 본 실시예에서, 개별 쇼 또는 영화에 대한 서비스 키가 디코더(701)에 의해 요청되어 앞서서 전달될 수도 있다. 예를 들어, DOCSIS 모뎀 또는 대역외 송신기/수신기와 같은 리턴 채널(721)을 갖는 케이블 시스템과 같은 상호 작용 네트워크들은 PPK(Program Key) 메시지에 대한 요청을 디코더(701)로부터 헤드엔드(710)로 전달할 수 있다. 대안으로, 디코더(701)는 액세스된 각각의 프로그램에 대해 실시간에 서비스 키들을 요청할 수도 있다.

[0059] 네트워크 헤드엔드 서버(710)의 컨트롤러(도시되지 않음)는 PPK 메시지를 처리한다. PPK 메시지는 뷰될 채널을 식별하는데 필요한 정보 뿐만 아니라 디코더(701)의 어드레스를 포함할 수도 있다(상기 모두는 MPEG(Motion Picture Experts Group) 시스템으로부터 획득될 수도 있으며 프로그램 정보는 이미 안전하지 않은 프로세서에 의해 처리됐을 수도 있다). 요청은 예를 들어, IPPV 또는 VOD 요청들과 같이, 원하는 경우 서비스 침해 거부 중재 및 비거부에 대해 암호화될 수도 있다.

[0060] 메시지를 수신할 때, 헤드엔드(710)는 액세스 제어 리스트(디코더(701)의 각각의 권리를 열거함)의 엔트리들을 액세스하며 디코더가 특정 서비스 키를 수신하도록 허가받았는지를 검증한다. 허가받았으면, 헤드엔드 서버(710)는 서비스 키(디스크램블러 IC에 위치한 디코더(701)의 유니크 키를 사용해서 암호화됨)를 디코더(701)에 송신한다.

[0061] 도 8은 하나 이상의 서비스 키들의 요청 및 수신을 위해 헤드엔드 서버(710)에 적용되는 도 7의 디코더(701)의 보다 상세한 도면을 제공한다. 한 실시예에 따라, ECM(Entitlement Control Message) 또는 EPG(Electronic Program Guide)와 관련된 메타데이터와 같은 프로그램 데이터(800)는 콘텐츠 프로바이더에 의해 디코더(701)에 제공된다. 프로그램 데이터(800)는 희망 채널 또는 서비스("채널 또는 서비스 ID"라고 함)의 적어도 식별자를 전달하도록 적응된다. 프로그램 데이터(800)가 IPPV 또는 VOD 프로그램인 상황에서, 프로그램 데이터(800)는 PID(Program identifier)를 더 포함할 수도 있다. 이는 다른 어떤 ECM 프로세싱이 아니라, 적합한 암호화 키를 메모리로부터 식별하고, 상기 키를 사용해서 디스크램블러 IC(740)의 적합한 기억 소자(또는 레지스터)에 기록

하는 것이 필요하기 때문이다.

[0062] MPEG 디멀티플렉서(810)는 프로그램 데이터의 검출시 채널 또는 서비스 ID 를 추출하기 위해 메시지 프로세서로서 동작한다. 채널 또는 서비스 ID는 프로세서(730)에 루팅되며, 이와 결합해서 송신기/수신기 로직(820)은 도 7의 헤드엔드 서버(710)로의 루팅을 위해 채널(721)을 통해 서비스 키 (RSK) 메시지에 대한 요청을 생성한다.

[0063] 응답으로, 디코더(701) 허가시, 헤드엔드 서버(710)는 요청된 서비스 키(SK)를 암호화 포맷으로 송신기/수신기 로직(820)에 전송하며, 송신기/수신기 로직(820)은 SK를 프로세서(730)에 제공한다. 프로세서(730)는 메모리(735)에 SK를 저장할 수도 있으며, 실시간에 입력 스크램블 콘텐츠를 디스크램블링하기 위해 디스크램블러 IC(740)에 SK를 제공할 수도 있다. 예를 들어, SK를 국부적으로 저장하는 것이 바람직한 경우, 메모리(735)는 사용을 위한 선택적 컴포넌트이다. SK가 국부적으로 저장되지 않지만 필요한 경우 헤드엔드 서버(710)로부터 액세스되는 경우, 메모리(735)는 디코더(701)로부터 제거될 수도 있다.

[0064] 프로그램 데이터의 스크램블 콘텐츠를 수신할 때, 디스크램블러 IC(740)는 상기 콘텐츠를 디스크램블하며, 콘텐츠가 MPEG 포맷으로 압축되는 경우 MPEG 디코더(830)에 제공된다. MPEG 디코더(830)는 디지털 콘텐츠의 압축을 해제하고 압축 해제된 디지털 콘텐츠를 텔레비전 디스플레이를 위한 D/A 컨버터, DVI(Digital Video Interface) 링크 또는 네트워크 인터페이스(예를 들어, IEEE 1394 링크)에 루팅한다.

[0065] 도시된 바와 같이, 프로세서(730), 메모리(735), 디스크램블러 IC(740), MPEG 디멀티플렉터(810), 송신기/수신기 로직(820) 및 MPEG 디코더(830)는 버스 트레이스 또는 다른 통신 기법(예를 들어, 와이어, 광섬유 등)를 통해 상호 연결된 두개 이상의 집적 회로들에서 구현될 수도 있다. 대안으로, 상기 컴포넌트들은 단일 집적 회로에서 구현될 수도 있다.

[0066] 본 실시예에서, SK는 특정 시간 기간 동안 유효할 수도 있다. 디코더(701)는 메모리(735)에 SK를 저장할 수도 있는데, 디코더(701)는 서비스 키를 다시 요청할 필요 없이 SK가 여전히 유효한 경우 서비스 키에 다시 액세스할 수 있다. 본 실시예에서, SK는 메모리(735)에 암호화 형태(헤드엔드(710)로부터 네트워크를 통해 옴)로 저장된다.

[0067] SK는 프로그램 존속 기간 동안 유효할 수도 있으며, 선택된 시간 기간, 예를 들어, 6시간 동안 유효할 수도 있다. 보다 더 긴 시간 기간 동안 키를 사용해서 디코더(701)와 헤드엔드 서버 간의 트랜잭션의 총 회수를 감소시킬 수 있는데, 이는 키가 일단 디코더(701)의 메모리(735)에 저장되면, 쉽게 유용하기 때문이다. 현 서비스 키(예를 들어, SK)의 존속 기간에 따라, 다음 서비스 키(SK_{next})가 SK와 함께 전달될 수도 있다. 대안으로, 디코더(701)는 SK의 유효 시기(예를 들어, SK의 시간 존속 기간)의 끝을 검출한 후에 SK_{next}를 요청할 수도 있다. 한 실시예에서, 서비스 키는 사용자의 예약 기간의 존속 기간 동안 유효하다.

[0068] 서비스 키는 튜닝되는 채널에 적용될 수도 있도록 적합하게 식별돼야만 한다. 디코더(701)가 채널에 튜닝할 때, 적합한 암호화 서비스 키를 메모리(735)로부터 탐색하고 디스크램블러 IC(740)의 Odd/Even MPEG 키 레지스터에 기록한다. 도 2의 실시예에서처럼, 비밀 유니크 키 정보는 디코더(701)가 제조될 때 디스크램블러 IC(740)에 프로그램될 수도 있다.

[0069] 한 실시예에서, 서비스 키들은 56-비트, 112-비트 또는 168-비트 키들을 포함할 수도 있다. 표 1은 상이한 사이즈들의 키들에 대한 저장 요구 사항들을 보여준다.

표 1

[0070] 독립 서비스 키들을 저장하기 위한 바이트들의 수

독립 키들에 따른 채널들의 수	채널 ID (3 바이트)	16 바이트 트리플 DES 암호화 서비스 키	16 바이트 트리플 DES 암호화 서비스 키	총 바이트
		CURRENT	NEXT	
20	60	320	320	700
50	150	800	800	1750
100	300	1600	1600	3500
200	600	3200	3200	7000
400	1200	6400	6400	14000

[0071] 서비스들은 메뉴에 따라 판매되거나 팩키지로 판매될 수도 있다. 여러 층의 서비스들이 있을 수 있으며, 각각은 서비스 ID에 의해 식별된다. 예를 들어, 도 9에 도시된 바와 같이, 기본 층의 서비스들, 보다 많은 서비스들을 제공하는 중간 층, 및 상이한 프리미엄 서비스들을 제공하는 진보된 층들이 있을 수도 있다. 본 실시예에서, 각각의 층의 서비스들은 개별 키를 제공받을 수도 있다.

[0072] 표 1로부터, 고객이 20개의 상이한 타입들이 서비스 층들을 예약하고자 하면, 총 700 바이트들에 대해, ID 스토리지 60 바이트, 현재 유효 서비스 키들의 스토리지 320 바이트, 다음 시기에 유효한 서비스 키들의 스토리지 320 바이트가 요구된다.

[0073] 도 10은 서비스 키들을 요청 및 수신하기 위한 방법의 일례의 실시예를 도시한다. 프로그램 정보는 계속해서 헤드엔드로부터 디코더에 송신된다(블록들(1010 및 1015)). 그 후 뷰어는 시청할 채널을 선택한다(블록(1020)). 디코더는 헤드엔드로부터 서비스 키를 요청한다(블록(1025)). 헤드엔드는 디코더의 예약 상태를 체크한다(블록(1030)). 디코더가 예약되면, 헤드엔드는 디코더에 서비스 키를 제공한다(블록(1055)). 디코더가 예약되지 않으면, 뷰어는 디코더에 의해 예약할지를 질문받는다(블록(1035)). 뷰어는 예약하기로 결정한다(블록(1040)). 디코더는 헤드엔드에 구매에 대한 요청을 송신한다(블록(1045)). 헤드엔드는 디코더에 암호화된 서비스 키를 송신한다(블록(1050)).

[0074] 따라서, 도 7의 디코더(701)는 유니크 키를 갖는 디스크램블러 IC(440)를 포함한다. 서비스 키들은 유니크 키에 의해 암호화된 디코더(701)에 전달되어 디코더(701)에서 암호화 형태로 저장된다. 대안으로, 디코더(701)는 서비스 키들을 국부적으로 저장할 필요 없이 채널에 튜닝할 때마다 서비스 키를 요청할 수 있었다.

[0075] 예를 들어, 통상 도 2의 안전한 암호 프로세서에 의해 유지된 권리들은 도 7의 헤드엔드(710)의 키 서버와 같은 권한을 제어함으로써 유지된다. 디코더(701)의 프로세서(730)는 뷰잉 옵션을 뷰어에게 적합하게 디스플레이할 수 있도록 디스크램블을 허가받았음을 나타내는 메시지(예를 들어, ECM 또는 EMM)를 수신할 수도 있다. 그 후 프로세서(730)는 선택된 채널에 대한 서비스 키들을 요청할 수 있다.

[0076] 본 실시예에서, "안전한" 펌웨어 또는 소프트웨어가 내장되어 있지 않다. 상술된 하드웨어 해독 회로를 사용해서, 암호 기능을 실행하는 내장된 프로세서 코어 또는 펌웨어가 필요하지 않다. 이는 다수의 상태 액세스 애플리케이션들이 안전하지 않은 프로세서에 다운로드될 수도 있게 한다. 서비스 키는 암호화된 유닛 키이다. 이는 공중 비대칭 키이거나 안전한 대칭 키일 수도 있다.

[0077] 추가 장점들은 IC(740)에 하드와이어된 유니크 키들을 디스크램블러 IC(740)를 갖는 디코더(701)에 제공함으로써 암호 프로세서를 사용하지 않고 유료-TV 애플리케이션들을 포함한다. 디코더(701)는 네트워크 프로바이더로부터 서비스 키 또는 컨트롤 워드를 요청할 수 있다. 중요한 "보안" 기능이 디스크램블러 IC(740)에서 고립되기 때문에, 로컬 액세스 제어가 프로세서(730)에 의해 실행될 수 있다.

[0078] 이제 도 11a를 참조하면, 보안 콘텐츠 전달 시스템(1100)의 제3 일례의 실시예가 도시되어 있다. 보안 콘텐츠 전달 시스템(1100)은 가입자 관리 시스템(1110), 상태 액세스(CA) 제어 시스템(1120), 상이한 셋탑 박스 제조자들과 관련된 다수의 메이팅 키 서버들(1130_1-1130_N)($N \geq 2$) 및 스마트 카드(1150)를 수신하도록 적응된 셋탑 박스(1140)를 포함한다. 스마트 카드(1150)는 셋탑 박스(1140)의 유니크 키(1180)를 저장하도록 구성된 로컬 메모리(1170)를 포함하는 디스크램블러 IC(1160)와 통신한다.

[0079] 셋탑 박스(1140)의 사용자가 특정 프로그램 데이터를 수신하기 희망하면, 셋탑 박스(1140)는 요청된 프로그램 데이터와 관련된 권리들이 이미 저장되어 있는지를 결정한다. 권리들이 저장되어 있지 않으면, 사용자는 스크린 디스플레이로부터 통보받을 수 있으며 가입자 관리 시스템(1110)에게 요청(1111)을 제공하도록 프롬프트될 수도 있다. 도시된 바와 같이, 요청(1111)은 사용자에 의해 (i) 대역외 통신 경로(예를 들어, 인터넷을 통한 전자메일, 사용자에 의한 전화 호출 등)를 통해, 또는 (ii) 셋탑 박스(1140)와 통신하는 CA 제어 시스템(1120)으로의 대역내 통신 경로를 통해 제공될 수도 있다. 대안으로, 요청(1111)은 자동으로 송신될 수도 있으며, 실시간에 실제로 사용자를 허가하기 위해 정보 룩업을 실행하는 상태 액세스 제어 시스템(1120)에 루팅될 수도 있다.

[0080] 한 실시예의 경우, 요청(1111)은 요청된 콘텐츠의 식별자(예를 들어, 영숫자, 또는 수치 코드), 셋탑 박스의 일련 번호("STB 일련 번호"라고 함) 및/또는 스마트 카드(1150)의 식별자("스마트 카드 ID"라고 함)를 포함하는 메시지이다. 임의의 정보 프로세싱 시스템(예를 들어, 서버, 중계국 또는 서비스 프로바이더 또는 콘텐츠 프로바이더에 의해 제어되는 다른 장치)로서 구현되는, 가입자 관리 시스템(1110)은 요청(1111)을 처리하고 어떤 권리들이 셋탑 박스(1140)에 제공될 것인지를 결정한다. 도시되지 않았지만, 상태 액세스 제어 시스템(1120)이

셋탑 박스의 일련 번호들 또는 스마트 카드 ID들을 포함하는 데이터베이스의 룩업을 실행하도록 구성될 수 있어서, 가입자 관리 시스템(1110)에 대한 액세스를 제거할 수 있다고 예상된다.

[0081] STB 일련 번호 및 글로벌 키들(예를 들어, 대역내에서 콘텐츠와 함께 송신된 ECM들을 해독하는데 사용된 키들)을 포함할 수도 있는 허가 메시지(1112)를 가입자 관리 시스템(1110)으로부터 수신할 때, 상태 액세스 제어 시스템(1120)은 STB 일련 번호(1141) 및 메이팅 키 제너레이터(1121)를 메이팅 키 서버들(1130_1-1130_N)(일반적으로 "메이팅 키 서버(1130_i)"라고 함, $i \geq 1$) 중 적어도 하나에 루팅한다. 상태 액세스 제어 시스템(1120)은 다운로드된 스크램블 정보로부터 요청된 프로그램 데이터를 추출하는데 사용되는 메이팅 키(1122)의 전달을 조정하도록 중간물로서 동작한다. 상태 액세스 제어 시스템(1120)은 헤드엔드 서버, 방송국, 위성 업링크 등으로 구현될 수도 있다.

[0082] 상태 액세스 제어 시스템(1120)이 메이팅 키 제너레이터(1121) 및 STB 일련 번호(1141)를 메이팅 키 서버들(1130_1-1130_N)에 루팅하는 대신, 상기 정보가 메이팅 키들을 특징으로 하는 데이터베이스에 대한 액세스를 유지 및 제어하는 신뢰할만한 제3국(1135)에 송신될 수도 있다. 메이팅 키 제너레이터(1121) 및/또는 STB 일련 번호(1141)와 관련된 값들은 메이팅 키(1122)를 검색하는데 사용된다. "신뢰할만한 제3국"(1135)은 임의의 셋탑 박스 제조자 등으로부터 독립적으로 관리되는 회사, 정치적 엔티티를 포함할 수도 있는데, 이로만 제한되지는 않는다.

[0083] STB 일련 번호(1141) 및 메이팅 키 제너레이터(1121)를 전송하기 전에, 상태 액세스 제어 시스템(1120)은 상태 액세스 제어 시스템(1120)과 메이팅 키 서버(1130_1) 간의 세션 키를 설정하기 위해, 서버(1130_1)와 같은 선택된 메이팅 키 서버로 인증 기법을 실행할 수도 있다. 물론, 인증 기법은 메이팅 키 서버(1130_1) 대신에 구현되는 경우 신뢰할만한 제3국으로 실행된다. 세션 키는 안전한 링크를 제공하기 위해 국들 간에 교환되는 정보를 암호화하는데 사용될 수 있다. 다양한 타입들의 인증 기법들의 일례들은 디지털 증명서, 디지털 서명, 해시값 등의 교환을 포함한다.

[0084] 도 11b에 도시된 바와 같이, 메이팅 키 제너레이터(1121)는 셋탑 박스 제조자 식별자(STB 제조자 ID)(1123), 서비스 프로바이더 ID(1124), 상태 액세스 프로바이더 ID(1125) 및 메이팅 키 시퀀스 번호(1126) 중 하나 이상을 포함하는 메시지이다. 본 실시예의 경우, "STB 제조자 ID(1123)"는 셋탑 박스(1140)의 제조자를 식별하는 선정된 값이다. 물론, STB 제조자 ID(1123)는 STB 일련 번호(1141)의 특정 배열에 따라 선택적이라고 예상된다. "서비스 프로바이더 ID(1124)"는 선택된 분포 메카니즘 뿐만 아니라 통신 시스템 프로바이더를 식별하는 값(예를 들어, 16비트들과 같은 1 이상의 비트들)이다. 예를 들어, 서비스 프로바이더 ID(1124)는 어떤 케이블, 위성, 지상 또는 인터넷 회사가 해당 회사의 특정 헤드엔드 서버 및/또는 요청된 프로그램 데이터를 지원중인지를 식별할 수도 있다. "상태 액세스 프로바이더 ID(1125)"는 상태 액세스 제어 시스템(1120)의 프로바이더를 나타낸다. "메이팅 키 시퀀스 번호(1126)"는 메이팅 키(1122)의 길이가 1 패킷 보다 많은 경우 정보의 패킷 리오더에 사용되고, 특정 시스템에서는, 메이팅 키 제너레이터(1121)의 만기를 나타내는데 사용될 수도 있다.

[0085] 도 11a를 참조하면, STB 일련 번호(1141)는 액세스하고자 하는 메이팅 키 서버(1130_1), ..., 메이팅 키 서버(1130_N)(또는 신뢰할만한 제3국(1135)의 데이터베이스)를 식별하기 위해 각각의 STB 제조자 ID(1123)에 대해 유일한 부분을 가질 수도 있다. 대안으로, STB 일련 번호(1141)는 셋탑 박스(1140)의 제조자를 식별하기 위한 코드 필드 뿐만 아니라 셋탑 박스(1140)의 일련 번호를 포함하도록 확장될 수도 있다. 물론, 비트들의 수는 설계시 선택 사항이다.

[0086] 메이팅 키 제너레이터(1121) 및 STB 일련 번호(1141)를 수신할 때, 적합한 메이팅 키 서버(예를 들어, 서버(1130_i)라고 함, $i \geq 1$)가 메이팅 키(1122)를 리턴한다. 본 실시예에서, 메이팅 키(1122)는 셋탑 박스(1140)에 송신중인 스크램블 콘텐츠를 디스크램블하는데 필요한 컨트롤 워드를 암호화하는데 사용된다. 특히, 메이팅 키 서버(1130_i)는 서버(1130_i)에 미리 저장된 유니크 키(1180)의 동일한 카피인 키에 액세스해서, 액세스된 키를 사용해서 메이팅 키 제너레이터(1121)를 암호화한다. 따라서, 메이팅 키(1122)와 동일한 키가 생성된다. 대안으로, 전체 메시지(1121)가 암호화되는 대신에 결과가 암호화되거나 메시지(1121)의 일분가 암호화되는 원웨이 해시 오퍼레이션을 메이팅 키 제너레이터(1121)가 시행할 수도 있다고 예상된다.

[0087] 메이팅 키(1122)를 수신할 때, 상태 액세스 제어 시스템(1120)은 스마트 카드(1140)에 송신되는 하나 이상의 ECM들(1142)과 함께 권리 관리 메시지(EMM)(1148)를 생성한다. EMM(1148)의 한 실시예는 도 11c에 도시되어

있다.

[0088] 도 11c에 도시된 바와 같이, EMM(1148)은 스마트 카드 ID(1143), 길이 필드(1144), 메이팅 키 제너레이터(1121), "M"개의(M≥1) 키 식별자들(1145_1-1145_M) 및 키 식별자들(1145_1-1145_M)과 관련된 글로벌 키들(1146_1-1146_M) 중 적어도 두개를 포함한다. 물론, 다른 권리들(1147)이 EMM(1148)에 포함될 수도 있다. 또한, 메이팅 키 제너레이터(1121)가 EMM(1148)으로부터 배제되어 개별적으로 송신되며 EMM(1148)과 일반적으로 동시발생할 수도 있다고 예상된다.

[0089] 스마트 카드 ID(1143)는 특정 셋탑 박스 및 셋탑 박스의 제조자를 나타내는데 사용되는 비트 값이다. "EMM 길이 필드"(1144)는 EMM(1148)의 길이를 나타내는데 사용되는 비트 값이다. 도시된 바와 같이, 메이팅 키 제너레이터(1121)는 도 11b의 위에서 4번째 파라미터들을 포함하는 비트값이다. 각각의 "키 식별자"(1145_1-1145_M)는 글로벌 키들(1146_1-1146_M)이 부정하게 변경되었는지를 체크하는데 사용되기 위해 부호화된 16-비트 권리 태그 값이다. 글로벌 키들(1146_1-1146_M)은 액세스 표준 요구 사항들 및 적어도 하나의 컨트롤 워드를 암호화 포맷으로 전달하는데 사용되는 ECM(1142)들을 해독하는데 사용된다. 상기 값들/필드들의 사이즈(비트)는 변할 수 있다.

[0090] 스마트 카드(1150)는 EMM(1148)을 수신하고 도 12에 도시된 바와 같이 셋탑 박스(1140)의 디스크램블러 IC(1160)에 ECM(1142)으로부터 복구된 암호화된 컨트롤 워드(1151) 및 메이팅 키 제너레이터(1121)를 발송한다.

[0091] 도 12는 도 11a의 시스템의 셋탑 박스(1140) 내에서 구현된 디스크램블러 IC(1160)의 제1 일례의 실시예이다. 스마트 카드(1150)로부터 메이팅 키 제너레이터(1121) 및 암호화된 컨트롤 워드(1151)를 수신할 때, 디스크램블러 IC(1160)는 디스크램블러 IC(1160)에 미리 저장된 유니크 키(1162)를 사용해서 메이팅 키 제너레이터(1121)에 대한 암호화 오퍼레이션을 실행하는 제1 프로세스 블록(1161)을 포함한다. 암호화 오퍼레이션은 DES, AES, IDEA, 3DES 등과 같은 대칭 키 암호 기능들에 따를 수도 있다. "DES" 오퍼레이션들은 설명을 위해 도시된다.

[0092] 메이팅 키 제너레이터(1121)에 대한 암호화 오퍼레이션은 메이팅 키(1122)와 동일한 키(1163)를 생성하며, 상기 키는 컨트롤 워드(1165)를 생성하기 위해 암호화된 컨트롤 워드(1151)를 해독하는데 사용되며 제2 프로세스 블록(1164)으로 로드된다. 컨트롤 워드(1165)는 셋탑 박스(1140)에 또한 특히 디스크램블러 IC(1160)에 로드된 스크램블 콘텐츠(1166)를 디스크램블하는데 사용된다. 디스크램블링은 스크램블 콘텐츠(1166)에 대한 3DES 오퍼레이션 실행을 포함할 수도 있다. 결과는 클리어 포맷의 콘텐츠이며, 디스크램블러 IC(1160)로부터 송신되어서 도 8에 도시된 MPEG 디코더로 로드되거나, D/A 컨버터, DVI 인터페이스 또는 IEEE 1394 인터페이스에 선택적으로 로드될 수도 있다.

[0093] 프로세스 블록들(1161 및 1164)이 메이팅 키(1122)가 공식화되는 방법에 따라 해독 및 암호화를 각각 지원하도록 변경될 수도 있다고 예상된다.

[0094] 이제 도 13을 참조하면, 보안 콘텐츠 전달 시스템(1200)의 제4 일례의 실시예가 도시되어 있다. 보안 콘텐츠 전달 시스템(1200)은 가입자 관리 시스템(1110), 상태 액세스(CA) 제어 시스템(1120), 메이팅 키 게이트웨이(1210), 메이팅 키 서버들(1130_1-1130_N) 및 셋탑 박스(1140)를 포함한다. 도 11a에 도시된 바와 같이 선택된 메이팅 키 서버들(1130_i) 중 하나에 상태 액세스 제어 시스템(1120)으로부터 메이팅 키 제너레이터(1121) 및 STB 일련 번호(1141)를 송신하는 대신, 상기 정보는 메이팅 키 게이트웨이(1210)에 루팅될 수도 있다. 메이팅 키 게이트웨이(1210)는 메이팅 키 제너레이터(1121)로부터 STB 제조자 ID에 액세스하고 메이팅 키 제너레이터(1121) 및 STB 일련 번호(1141)를 선택된 메이팅 키 서버(1130_i)에 적합하게 루팅한다. 이는 메이팅 키(1122)를 복구하는 상태 액세스 제어 시스템(1120) 또는 서버들(1130_1-1130_N)에 의한 프로세싱 시간을 감소시킨다.

[0095] 대안으로, 메이팅 키 게이트웨이(1210)가 메이팅 키 제너레이터(1121) 및 STB 일련 번호(1141)를 선택된 메이팅 키 서버(1130_i)에 루팅하는 대신, 상기 정보는 메이팅 키 검색을 위해 데이터베이스에 액세스하는 신뢰할만한 제3국(1135)에 루팅될 수도 있다고 예상된다. 메이팅 키는 메이팅 키 제너레이터(1121) 및/또는 STB 일련 번호(1141)와 관련된 값들을 근거로 한다. 각각의 데이터베이스는 메이팅 키 제너레이터(1121) 및/또는 STB 일련 번호(1141) 내에 관련된 값들이 메이팅 키(1122)가 액되는 타겟 데이터베이스를 식별하는데 사용될 수 있는 값들의 범위를 할당받을 수도 있다.

[0096] 도 14a는 보안 콘텐츠 전달 시스템(1300)의 제5 일례의 실시예이다. 보안 콘텐츠 전달 시스템(1300)은 가입자 관리 시스템(1310), 상태 액세스 제어 시스템(1320), 상이한 셋탑 박스 제조자들과 관련된 다수의 메이팅 키 서

버들(1330_1-1330_N), 셋탑 박스(1340), 메이팅 키 게이트웨이(1350)(게이트웨이(1213)와 유사함), 및 네트워크 인터페이스(1355)(예를 들어, DOCSIS CMTS)를 포함한다. 셋탑 박스(1340)는 셋탑 박스(1340)의 유니크 키(1380)를 저장하도록 구성된 로컬 메모리(1370)를 포함하는 디스크램블러 IC(1360)를 포함한다.

[0097] 스크램블되지 않은 포맷의 EPG 및 스크램블 포맷의 디지털 콘텐츠(1348)를 갖는 EPG(electronic program guide) 메타데이터를 수신했다. 한 실시예에서, EPG 메타데이터(1400)는 상태 액세스 제어 시스템(1320)에 의해 대역외로 제공된다. 도 15에 도시된 바와 같이, EPG 메타데이터(1400)의 한 실시예는 콘텐츠 프로바이더에 의해 제공된 상이한 타입들의 콘텐츠에 대한 다수의 태그 엔트리들(1410_1-1410_S)(S≥1)을 포함한다. 각각의 태그 엔트리(1410_j)는 적어도 하나의 채널명(1420), 콘텐츠명(1430), 및 채널과 관련된 서비스 층을 나타내는 키 식별자(1440)를 포함한다. 또한, 각각의 태그 엔트리(1410_j)는 프로그램 식별자(PID)(1450) 및 메이팅 키 제너레이터(MKG)(1121)를 더 포함한다.

[0098] 도 14a를 다시 참조하면, 셋탑 박스(1340)의 사용자가 특정 타입의 콘텐츠(예를 들어, PPV 영화, 방송 채널 등)을 수신하기 희망하면, 셋탑 박스(1340)는 요청된 콘텐츠와 관련된 권리들이 이미 저장되어 있는지를 결정한다. 권리들이 저장되어 있지 않으면, 사용자가 (1) 스크린 디스플레이 또는 오디오 재생을 통해 직접 통보받고 요청(1311)을 가입자 관리 시스템(1310)(또는 상태 액세스 제어 시스템(1320))에 제공하도록 프롬프트될 수 있으며, 또는 (2) 요청(1111)이 자동으로 송신될 수도 있다. 요청(1311)은 대역외로(예를 들어, 전화 호출 또는 인터넷을 통한 이메일) 또는 대역내로(상태 액세스 제어 시스템(1320)을 통한 가입자 관리 시스템(1310)으로의 전송을 위해 리모트에서 정렬 버튼을 누름) 제공될 수도 있다.

[0099] 요청(1311)은 셋탑 박스의 일련 번호("STB 일련 번호"라고 함) 및 요청된 콘텐츠의 식별자(예를 들어, 영숫자 또는 수치 코드)를 포함하는 메시지일 수도 있다. 가입자 관리 시스템(1310)은 요청(1311)을 처리하고 어떤 권리들이 셋탑 박스(1340)에 제공될 지를 결정한다.

[0100] STB 일련 번호(1341) 및 권리들을 포함하는 허가 메시지(1312)를 가입자 관리 시스템(1310)으로부터 수신할 때(또는 상태 액세스 제어 시스템(1320)에서 STB 일련 번호(1341)를 룩업할 때), 상태 액세스 제어 시스템(1320)은 STB 일련 번호(1341) 및 메이팅 키 제너레이터(1321)를 메이팅 키 게이트웨이(1350)에 루팅한다. 메이팅 키 게이트웨이(1350)는 다운로드된 스크램블 정보로부터 요청된 콘텐츠를 추출하는데 사용되는 메이팅 키(1322)의 전달을 조정하도록 중간물로서 동작한다. 상술된 바와 같이, 상태 액세스 제어 시스템(1320)은 헤드엔드 서버, 방송국, 위성 업링크 등으로 구현될 수도 있다.

[0101] STB 일련 번호(1341) 및 메이팅 키 제너레이터(1321), 상기 도 11a 내지 도 11c에 도시된 상기 메시지들의 요소들을 전송하기 전에, 상태 액세스 제어 시스템(1320)은 안전한 통신을 가능케 하는 세션 키를 설정하기 위해 메이팅 키 게이트웨이(1350)로 인증 기법을 실행할 수도 있다.

[0102] 메이팅 키(1322)를 수신할 때, 상태 액세스 제어 시스템(1320)은 하나 이상의 EMM(1342)들을 생성한다. EMM(1342)의 한 실시예는 도 14b에 도시되어 있다.

[0103] 도 14b에 도시된 바와 같이, EMM(1342)은 STB 일련 번호(1341), EMM 길이 필드(1343), 메이팅 키 제너레이터(1321), "M"개의(M≥1) 키 식별자들(1344_1-1344_M) 및 키 식별자들(1344_1-1344_M)과 각각 관련된 암호화 서비스 키들(1345_1-1345_M) 중 적어도 두개를 포함한다. 물론, 상기 값들의 사이즈(비트)는 변할 수 있으며, 식별자들 또는 서비스 키들이 아닌 다른 타입들의 권리들(1346)이 EMM(1342)에 포함될 수도 있다. 또한, 메이팅 키 제너레이터(1321)가 EMM(1342)으로부터 배제되어 개별적으로 송신되며 EMM(1342)과 일반적으로 동시발생할 수도 있다고 예상된다. 물론, 상기 값들/필드들의 사이즈(비트)는 변할 수 있다.

[0104] STB 일련 번호(1341)는 특정 셋탑 박스 및 셋탑 박스의 제조자를 나타내는데 사용되는 비트 값이다. "EMM 길이 필드"(1343)는 EMM(1342)의 길이를 나타내는데 사용되는 비트값이다. 도시된 바와 같이, 메이팅 키 제너레이터(1321)는 도 11b의 위에서 4번째 파라미터들을 포함하는 비트값이다. 각각의 "키 식별자"(1344_1-1344_M)는 대응 암호화 서비스 키들(1345_1-1345_M)과 각각 관련된 서비스 층을 나타내는 16-비트 값이다. 암호화 서비스 키들(1345_1-1345_M)은 도 16에 도시된 바와 같이 메이팅 키(1322)와 동일한 디스크램블러 IC(1360) 내에 생성된 키에 의해 해독된다.

[0105] 도 16은 도 14a의 셋탑 박스(1340) 내에서 구현된 디스크램블러 IC(1360)의 제1 일례의 실시예이다. EMM(134

2)에 포함된 암호화 서비스 키들(1345_j)($1 \leq j \leq m$) 및 메이팅 키 제너레이터(1321)를 수신할 때, 디스크램블러 IC(1360)는 디스크램블러 IC(1360)에 미리 저장된 유니크 키(1362)를 사용해서 메이팅 키 제너레이터(1321)에 대한 암호화 오퍼레이션을 실행하는 제1 프로세스 블록(1361)을 포함한다. 암호화 오퍼레이션은 DES, AES, IDEA, 3DES 등과 같은 대칭 키 암호 기능들에 따를 수도 있다. 물론, 블록(1361)은 암호화 기능 대신 해싱 기능을 실행하도록 변경될 수도 있다고 예상된다.

[0106] 메이팅 키 제너레이터(1321)에 대한 암호화 오퍼레이션은 메이팅 키(1322)와 동일한 키(1363)를 생성하며, 상기 키는 셋탑 박스(1340) 및 특히 디스크램블러 IC(1360)에서 로드된 스크램블 콘텐츠(1365)를 디스크램블하는데 사용된 서비스 키를 복구하기 위해 암호화 서비스 키(1345_j)를 해독하는데 사용되며 제2 프로세스 블록(1364)으로 로드된다. 디스크램블링은 스크램블 콘텐츠에 대한 3DES 오퍼레이션 실행을 포함할 수도 있다. 결과는 클리어 포맷의 콘텐츠이며, 디스크램블러 IC(1360)로부터 송신되어서 도 8에 도시된 MPEG 디코더로 로드되거나, D/A 컨버터, DVI 인터페이스 또는 IEEE 1394 인터페이스에 선택적으로 로드될 수도 있다.

[0107] 이제 도 17을 참조하면, 보안 콘텐츠 전달 시스템(1500)의 제6 일례의 실시예가 도시되어 있다. 도 14a의 가입자 관리 시스템(1310) 및 상태 액세스 제어 시스템(1320) 대신, 메이팅 키 게이트웨이(1350)는 상이한 콘텐츠 프로바이더와 각각 관련된 다수의 가입자 관리 시스템(SMS)(1510_1-1510_K)($K \geq 1$)과 통신하도록 적응될 수도 있다. 상기 가입자 관리 시스템들(1510_1-1510_K) 각각은 메이팅 키 제너레이터들 및 STB 일련 번호들(1520_1-1520_K)을 메이팅 키 게이트웨이(1350)에 제공하고, 대응 메이팅 키들(1530_1-1530_K)을 수신한다. 상기 메이팅 키들(1530_1-1530_K)은 하나 이상의 타겟 셋탑 박스들(도시되지 않음)에 제공된 서비스 키들을 암호화하는데 사용된다. 대안으로, 신뢰할만한 제3국(1135)은 도 11a, 도 13 및 도 14에 도시된 바와 같이 사용될 수도 있다.

[0108] 예를 들어, 본 실시예의 경우, 가입자 관리 시스템들(1510_1 및 1510_2)은 지상 브로드캐스터로서, 각각 메이팅 키 제너레이터들 및 STB 일련 번호들(1520_1, 1520_2)을 메이팅 키 게이트웨이(1350)에 제공하고, 대응 메이팅 키들(1530_1, 1530_2)을 수신한다. 오퍼레이션이 유사한 가입자 관리 시스템들(1510_3 및 1510_4)은 케이블 오퍼레이터들이며, 가입자 관리 시스템(1510_5)은 DBS 회사이고, 가입자 관리 시스템들(1510_{K-1} 및 1510_K)은 인터넷 콘텐츠 소스들이다.

[0109] 도 18을 참조하면, 보안 콘텐츠 전달 시스템(1600)의 제7 일례의 실시예의 일부가 도시되어 있다. 시스템(1600)의 셋탑 박스(1610)는 제1 소스로부터 스크램블 또는 암호화 콘텐츠(1620)를 수신하고 제2 소스로부터 EMM(1640)을 수신한다. 제2 소스는 스마트 카드 또는 상태 액세스 제어 시스템일 수도 있다.

[0110] 본 발명의 실시예에 따라, EMM(1640)은 사용자 키 제너레이터(1642) 및 암호화 사용자 키(1641)를 포함한다. 도 18 및 도 19에 도시된 바와 같이, 암호화 사용자 키(1641)는 유니크 키(1631) 또는 그로부터 유도된 키에 의해 해독될 때 디스크램블러 IC(1630)의 특정 값을 생성하도록 계산되는 값이다. 상기 키(1641)는 공유되기 위한 특정 값이다. 지불 및 CA 디스크램블링 후에, 콘텐츠는 사용자 키(1633)를 근거로 하는 카피 보호 키(1635)를 사용해서 다시 스크램블될 수 있다. 카피 보호 키(1635)는 해독을 위해, 다른 셋탑 박스(1670), 포터블 컴퓨터(예를 들어, PDA)(1671), 또는 심지어 포터블 쥬크박스(1672)와 같은 다른 디바이스들과 공유된다.

[0111] 도 19에 더 도시된 바와 같이, 디스크램블러 IC(1630)의 실시예는 제2 소스로부터 암호화 사용자 키(E_{key})(1641), 사용자 키 제너레이터(UKG)(1642) 및 암호화 컨트롤 워드(1643)를 수신한다. 디스크램블러 IC(1630)는 DES, AES, IDEA, 3DES 등과 같은 대칭 키 암호 기능들에 따라 유니크 키(1631)로 E_{key}(1641)를 해독하는 제1 프로세스 블록(1632)을 포함한다.

[0112] E_{key}(1641)에 대한 해독 오퍼레이션은 사용자 키(1633)를 복구하며, 상기 키는 제2 프로세스 블록(1643)에 로드되어, 카피 보호 키(1635)를 생성하기 위해 UKG(1642)를 암호화하는데 사용된다. 암호화 컨트롤 워드(1643)는 셋탑 박스(1670)에 로드된 특히 디스크램블러 IC(1630)에 로드된 암호화 콘텐츠(1620)를 디스크램블링 및/또는 해독하기 위해 클리어 포맷으로 컨트롤 워드를 복구하기 위해 유니크 키(1631)(또는 유도된 키)를 사용해서 해독된다. 디스크램블링 및/또는 해독은 3DES 오퍼레이션 실행을 포함할 수도 있다.

[0113] 결과로서, 콘텐츠는 임시적으로 클리어 포맷이지만, 행선 디지털 디바이스들 중 임의의 디바이스 또는 전부와 관련된 카피 보호 키(1635)로 디스크램블된 콘텐츠를 해독하는 로우-레벨 암호화 로직(1660)으로 루팅된다. 따라서, 콘텐츠는 다음 전송 중에 안전하다.

[0114] 상술된 설명에서, 본 발명은 특정 일례의 실시예들을 참조해서 기술된다. 그러나, 첨부된 청구항들에 기재된 본 발명의 보다 넓은 범위 및 원리에서 벗어나지 않으면서 다양한 변경 및 변화가 달성될 수도 있음이 명백하다. 명세서 및 도면은 제한의 의미가 아니며 설명을 위한 것이다.

부호의 설명

[0115] 111: 디지털 수신기

401: 상태 액세스 유닛

410: 스마트 카드

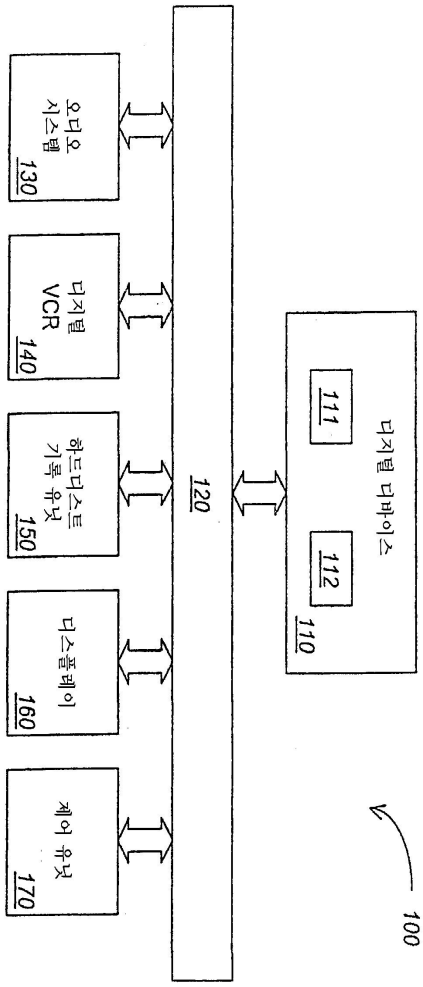
416: 암호화된 컨트롤 워드

480: 스크램블 콘텐츠

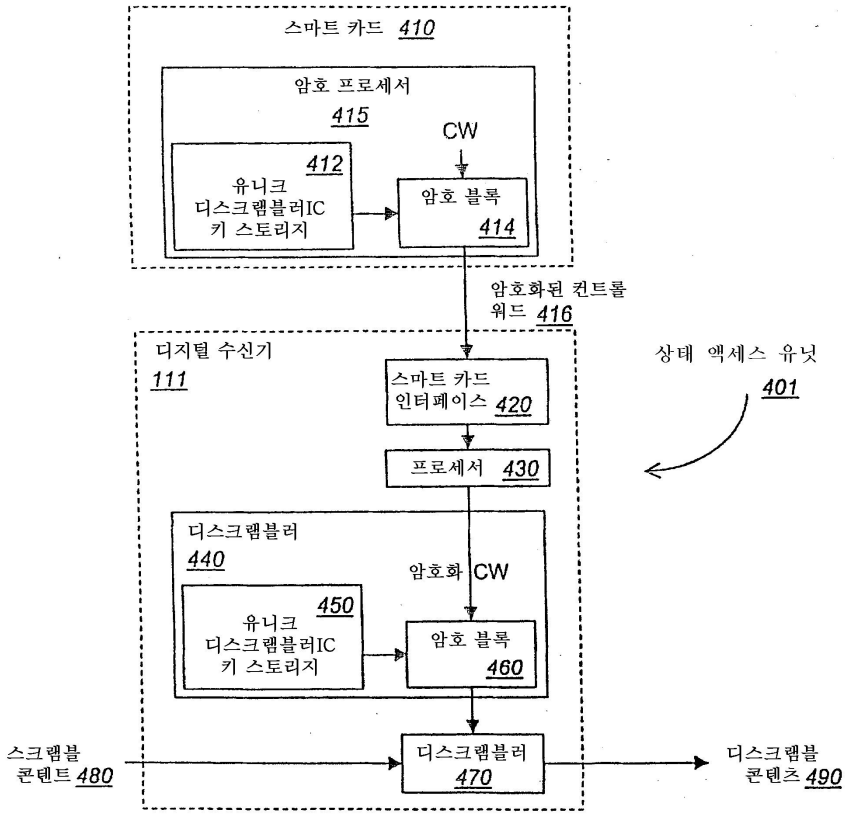
490: 디스크램블 콘텐츠

도면

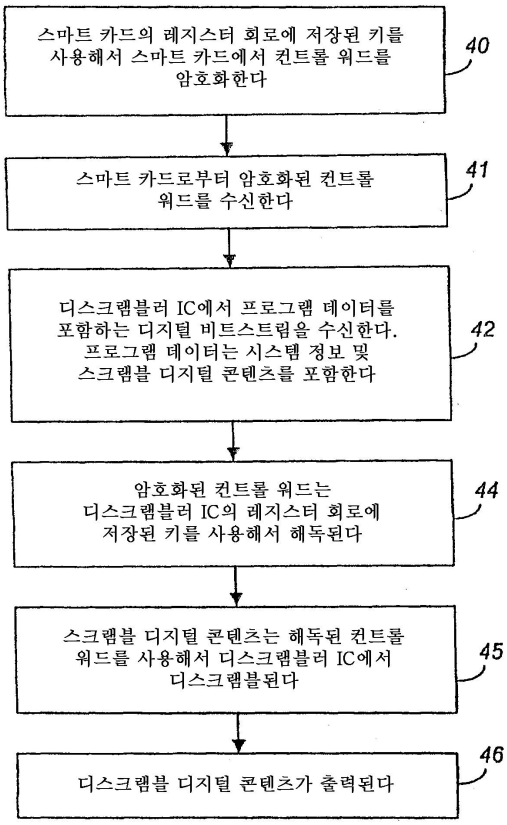
도면1



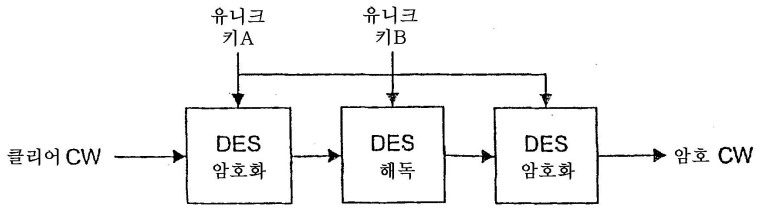
도면2


스마트 카드 410
암호 프로세서
415
CW
412
유니크
디스크램블러IC
키 스토리지
암호 블록
414
암호화된 컨트롤
워드 416
디지털 수신기
111
스마트 카드
인터페이스 420
상태 액세스 유닛
401
프로세서 430
디스크램블러
440
암호화 CW
450
유니크
디스크램블러IC
키 스토리지
암호 블록
460
스크램블
콘텐트 480
디스크램블러
470
디스크램블
콘텐츠 490

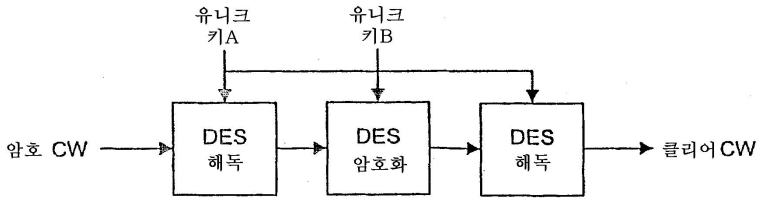
도면3


스마트 카드의 레지스터 회로에 저장된 키를 사용해서 스마트 카드에서 컨트롤 워드를 암호화한다
40
스마트 카드로부터 암호화된 컨트롤 워드를 수신한다
41
디스크램블러 IC에서 프로그램 데이터를 포함하는 디지털 비트스트림을 수신한다. 프로그램 데이터는 시스템 정보 및 스크램블 디지털 콘텐츠를 포함한다
42
암호화된 컨트롤 워드는 디스크램블러 IC의 레지스터 회로에 저장된 키를 사용해서 해독된다
44
스크램블 디지털 콘텐츠는 해독된 컨트롤 워드를 사용해서 디스크램블러 IC에서 디스크램블된다
45
디스크램블 디지털 콘텐츠가 출력된다
46

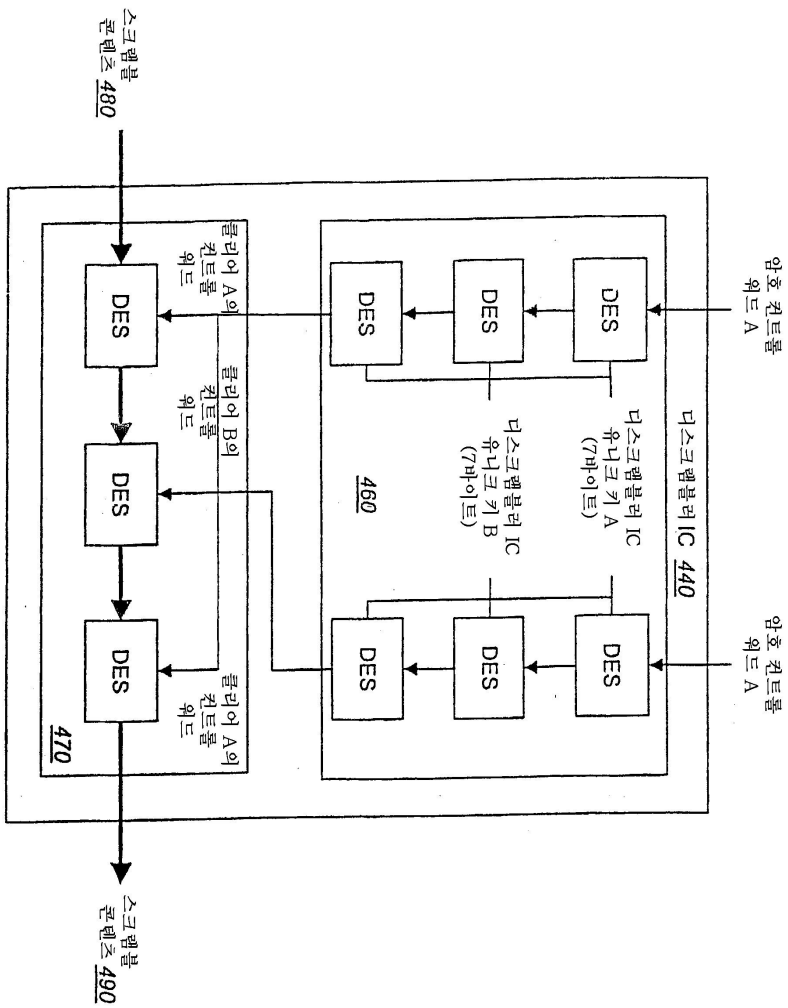
도면4


유니크 키A
유니크 키B
클리어 CW
DES 암호화
DES 해독
DES 암호화
암호 CW

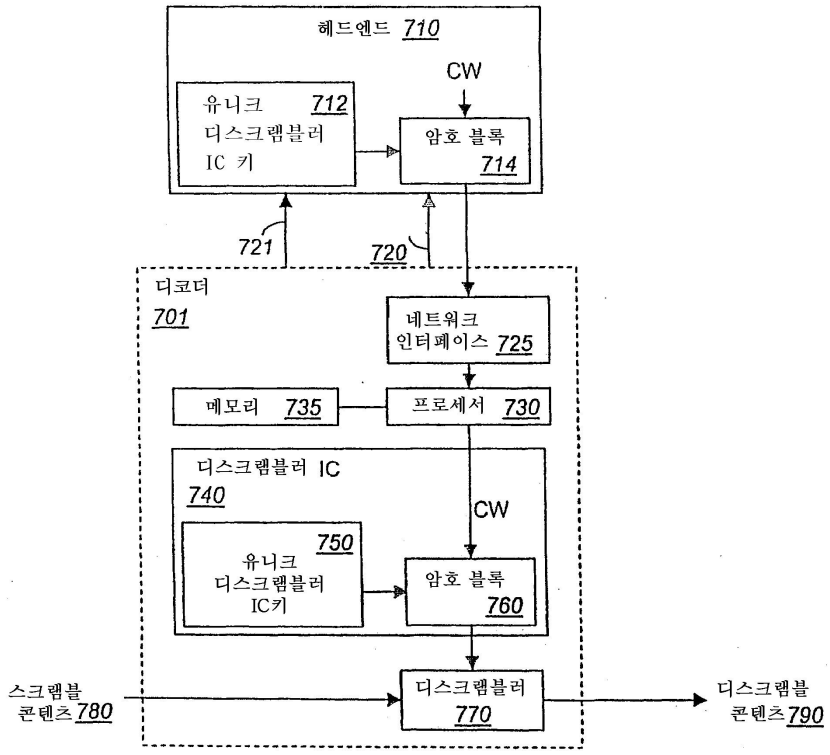
도면5


유니크 키A
유니크 키B
암호 CW
DES 해독
DES 암호화
DES 해독
클리어 CW

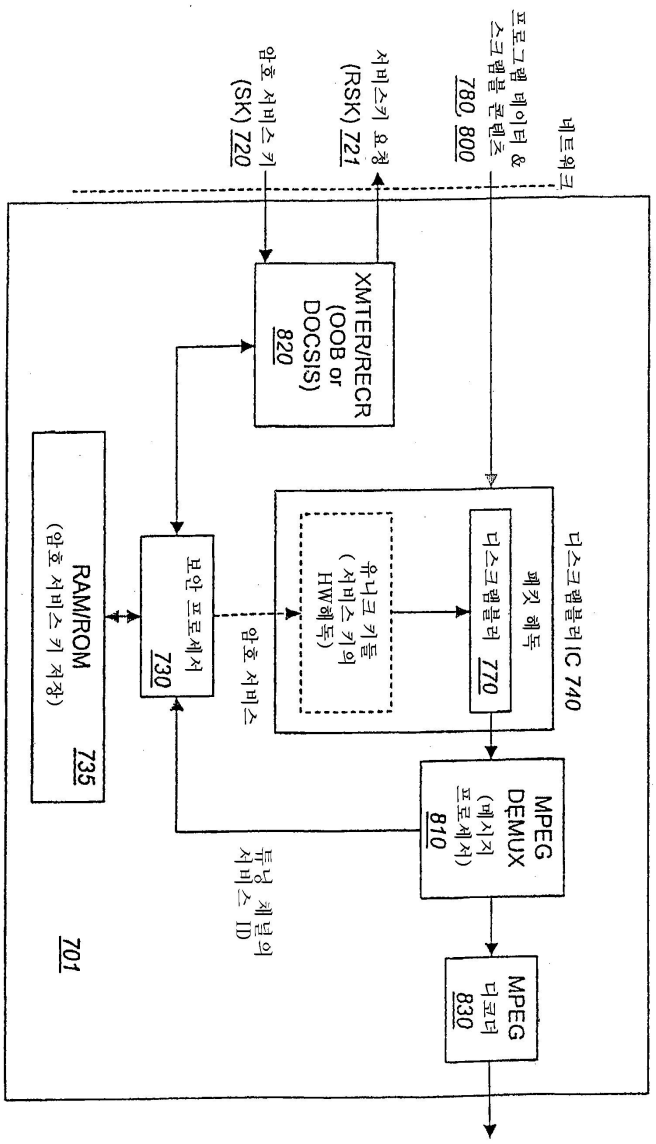
도면6


스크램블 콘텐츠 480
DES
DES
DES
470
클리어 A의 컨트롤 워드
클리어 B의 컨트롤 워드
클리어 A의 컨트롤 워드
460
DES
DES
DES
DES
DES
DES
디스크램블러 IC 440
디스크램블러 IC 유니크 키 A (7바이트)
디스크램블러 IC 유니크 키 B (7바이트)
암호 컨트롤 워드 A
암호 컨트롤 워드 A
스크램블 콘텐츠 490

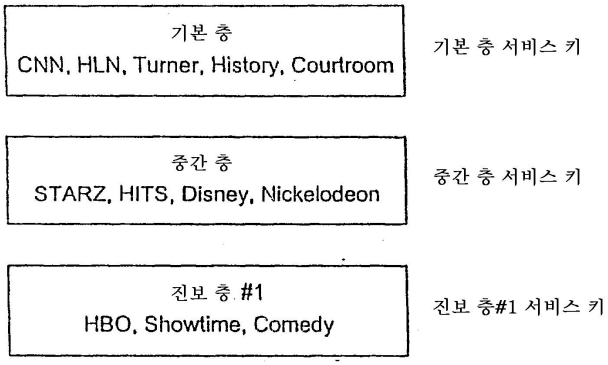
도면7


헤드엔드 710
CW
유니크 712
디스크램블러
IC 키
암호 블록
714
721
720
디코더
701
네트워크
인터페이스 725
메모리 735
프로세서 730
디스크램블러 IC
740
CW
750
유니크
디스크램블러
IC키
암호 블록
760
스크램블
콘텐츠 780
디스크램블러
770
디스크램블
콘텐츠 790

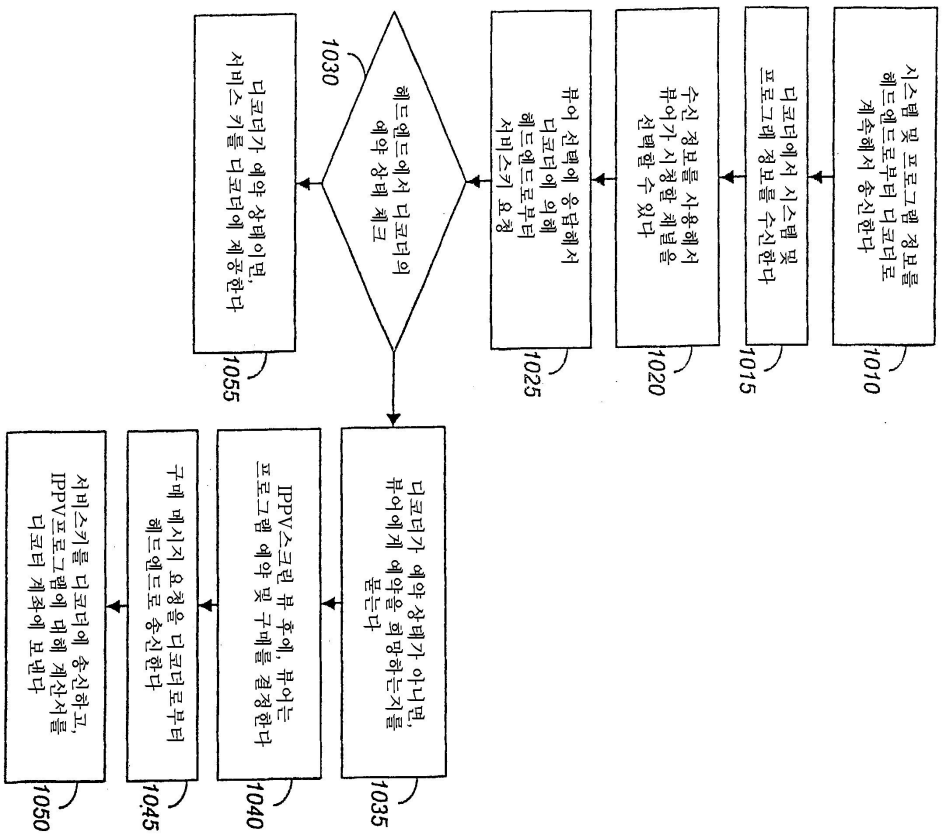
도면8


네트워크
프로그램 데이터 & 스크램블 콘텐츠 780, 800
서비스키 요청 (RSK) 721
암호 서비스 키 (SK) 720
XMTER/RECR (OOB or DOCSIS) 820
디스크램블러 IC 740
패킷 해독
디스크램블러 770
유니크 키들 (서비스 키의 HW해독)
보안 프로세서 730
암호 서비스
RAM/ROM (암호 서비스 키 저장) 735
MPEG DEMUX (메시지 프로세서) 810
튜닝 채널의 서비스 ID
MPEG 디코더 830
701

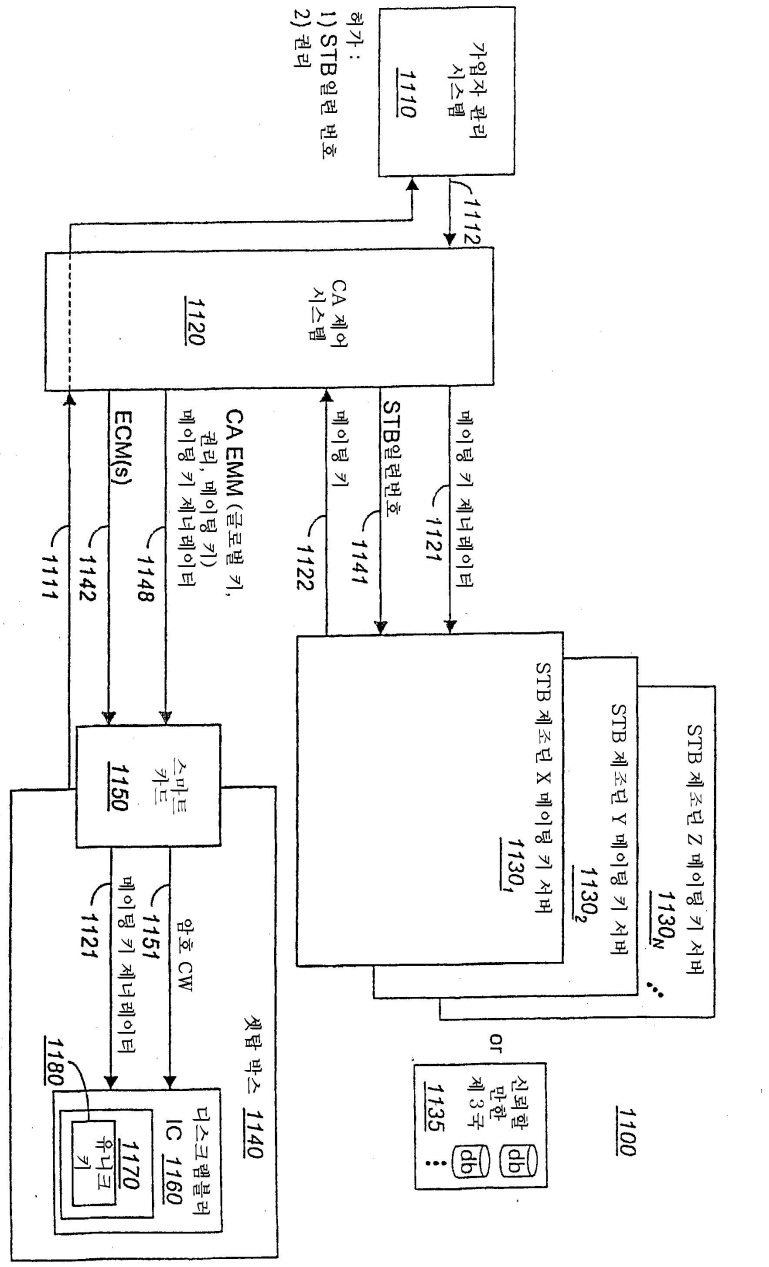
도면9


기본 층
CNN, HLN, Turner, History, Courtroom
기본 층 서비스 키
중간 층
STARZ, HITS, Disney, Nickelodeon
중간 층 서비스 키
진보 층 #1
HBO, Showtime, Comedy
진보 층#1 서비스 키

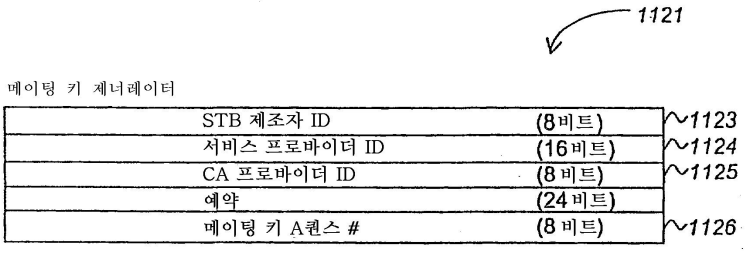
도면10


시스템 및 프로그램 정보를
헤드엔드로부터 디코더로
계속해서 송신한다
1010
디코더에서 시스템 및
프로그램 정보를 수신한다
1015
수신 정보를 사용해서
뷰어가 시청할 채널을
선택할 수 있다
1020
뷰어 선택에 응답해서
디코더에 의해
헤드엔드로부터
서비스키 요청
1025
헤드엔드에서 디코더의
예약 상태 체크
1030
디코더가 예약 상태이면,
서비스 키를 디코더에 제공한다
1055
디코더가 예약 상태가 아니면,
뷰어에게 예약을 희망하는지를
묻는다
1035
IPPV스크린 뷰 후에, 뷰어는
프로그램 예약 및 구매를 결정한다
1040
구매 메시지 요청을 디코더로부터
헤드엔드로 송신한다
1045
서비스키를 디코더에 송신하고,
IPPV프로그램에 대해 계산서를
디코더 계좌에 보낸다
1050

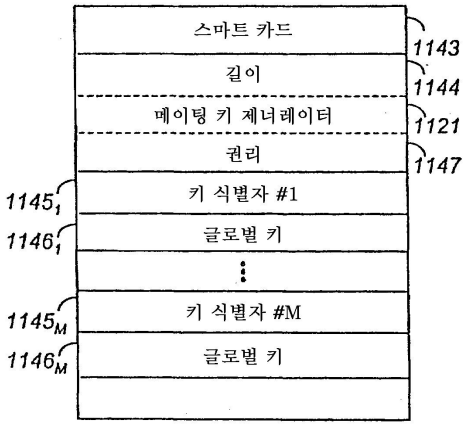
도면11a


가입자 관리 시스템
1110
허가 :
1) STB일련 번호
2) 권리
1112
CA 제어 시스템
1120
CA EMM (글로벌 키, 권리, 메이팅 키)
메이팅 키 제너레이터
ECM(s)
메이팅 키
STB일련번호
메이팅 키 제너레이터
1111
1142
1148
1122
1141
1121
STB 제조딘 X 메이팅 키 서버
1130₁
STB 제조딘 Y 메이팅 키 서버
1130₂
STB 제조딘 Z 메이팅 키 서버
1130N
or
신뢰할 만한 제 3 국
1135
db
1100
스마트 카드
1150
셋탑 박스 1140
메이팅 키 제너레이터
암호 CW
1121
1151
1180
디스크램블러 IC 1160
유니크 키
1170

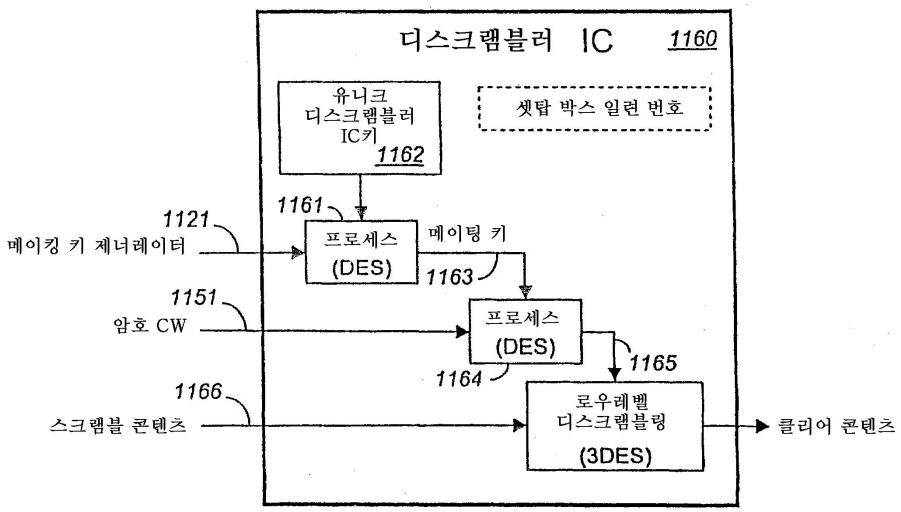
도면11b


1121
메이팅 키 제너레이터
STB 제조자 ID (8비트) 1123
서비스 프로바이더 ID (16비트) 1124
CA 프로바이더 ID (8비트) 1125
예약 (24비트)
메이팅 키 A퀀스 # (8 비트) 1126

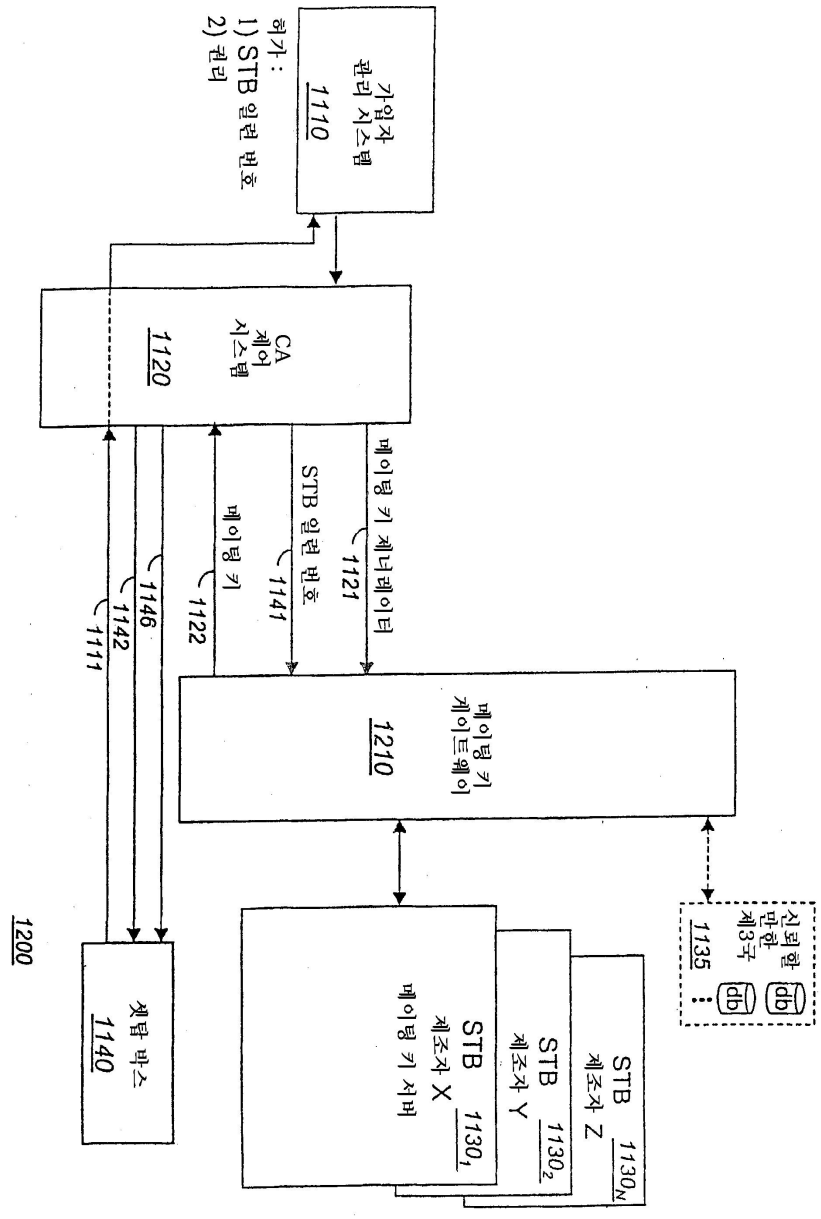
도면11c


스마트 카드
1143
길이
1144
메이팅 키 제너레이터
1121
권리
1147
1145₁
키 식별자 #1
1146₁
글로벌 키
1145M
키 식별자 #M
1146M
글로벌 키

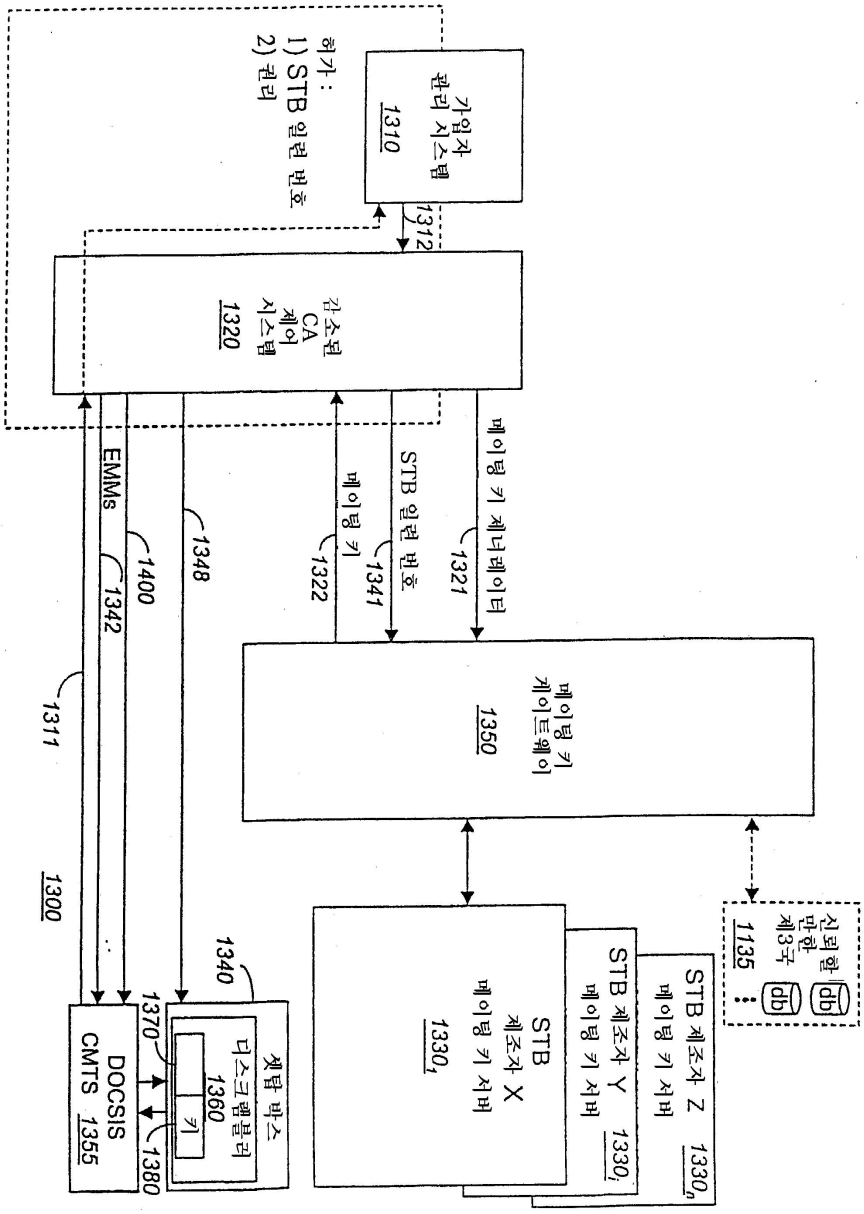
도면12


디스크램블러 IC
1160
유니크 디스크램블러 IC키
1162
셋탑 박스 일련 번호
1161
1121
메이킹 키 제너레이터
프로세스 (DES)
메이팅 키
1163
1151
암호 CW
프로세스 (DES)
1165
1164
1166
스크램블 콘텐츠
로우레벨 디스크램블링 (3DES)
클리어 콘텐츠

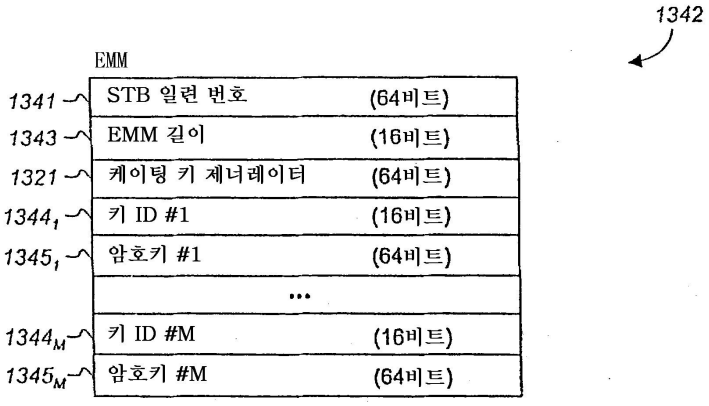
도면13


가입자 관리 시스템 1110
허가 :
1) STB 일련 번호
2) 권리
CA 제어 시스템 1120
메이텡 키 제너레이터 1121
STB 일련 번호 1141
메이텡 키 1122
1111
1142
1146
메이텡 키 게이트웨이 1210
신뢰할 만한 제3국 1135
STB 제조자 X 1130$_1$
메이텡 키 처버
STB 제조자 Y 1130$_2$
STB 제조자 Z 1130$_N$
셋탑 박스 1140
1200

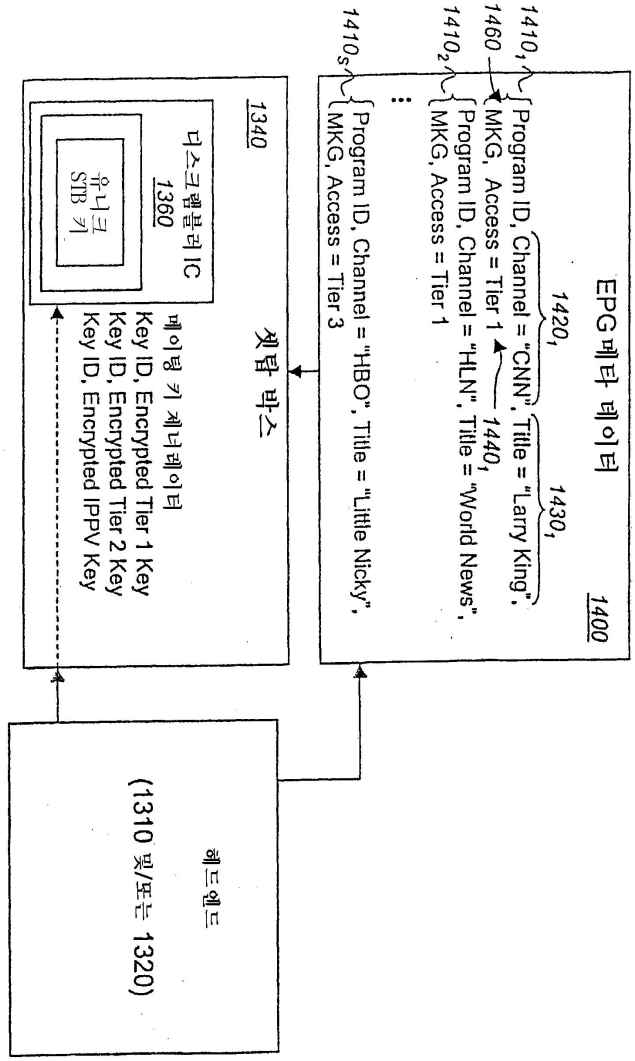
도면14a


허가 :
1) STB 일련 번호
2) 권리
가입자 관리 시스템 1310
1312
감소된 CA 제어 시스템 1320
메이팅 키 제너레이터
STB 일련 번호
메이팅 키
1321
1341
1322
EMMs
1400
1342
1348
1311
1300
메이팅 키 게이트웨이 1350
신뢰할 만한 제3국 1135
db
db
STB 제조자 Z 메이팅 키 서버 1330n
STB 제조자 Y 메이팅 키 서버 1330i
STB 제조자 X 메이팅 키 서버 1330i
1340
셋탑 박스
디스크램블러 1360
키
1370
1380
DOCSIS CMTS 1355

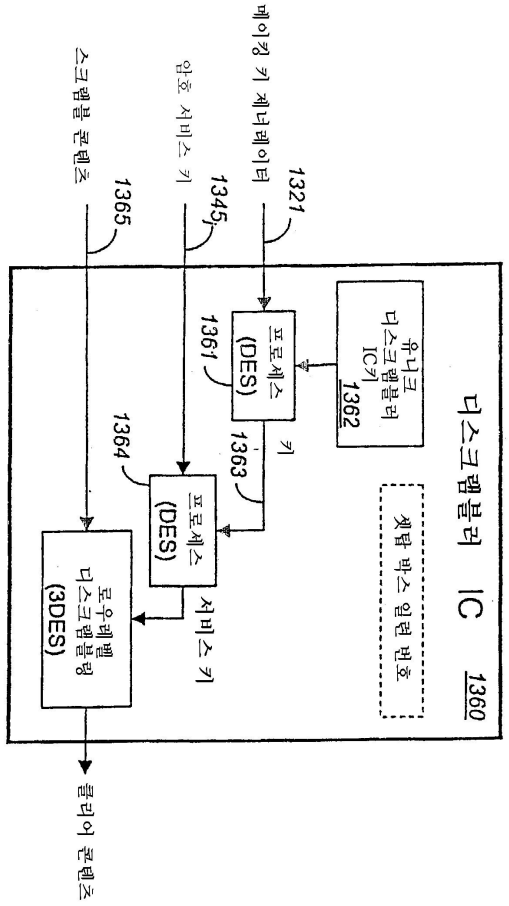
도면14b


1342
EMM
1341 STB 일련 번호 (64비트)
1343 EMM 길이 (16비트)
1321 케이팅 키 제너레이터 (64비트)
1344$_1$ 키 ID #1 (16비트)
1345$_1$ 암호키 #1 (64비트)
...
1344$_M$ 키 ID #M (16비트)
1345$_M$ 암호키 #M (64비트)

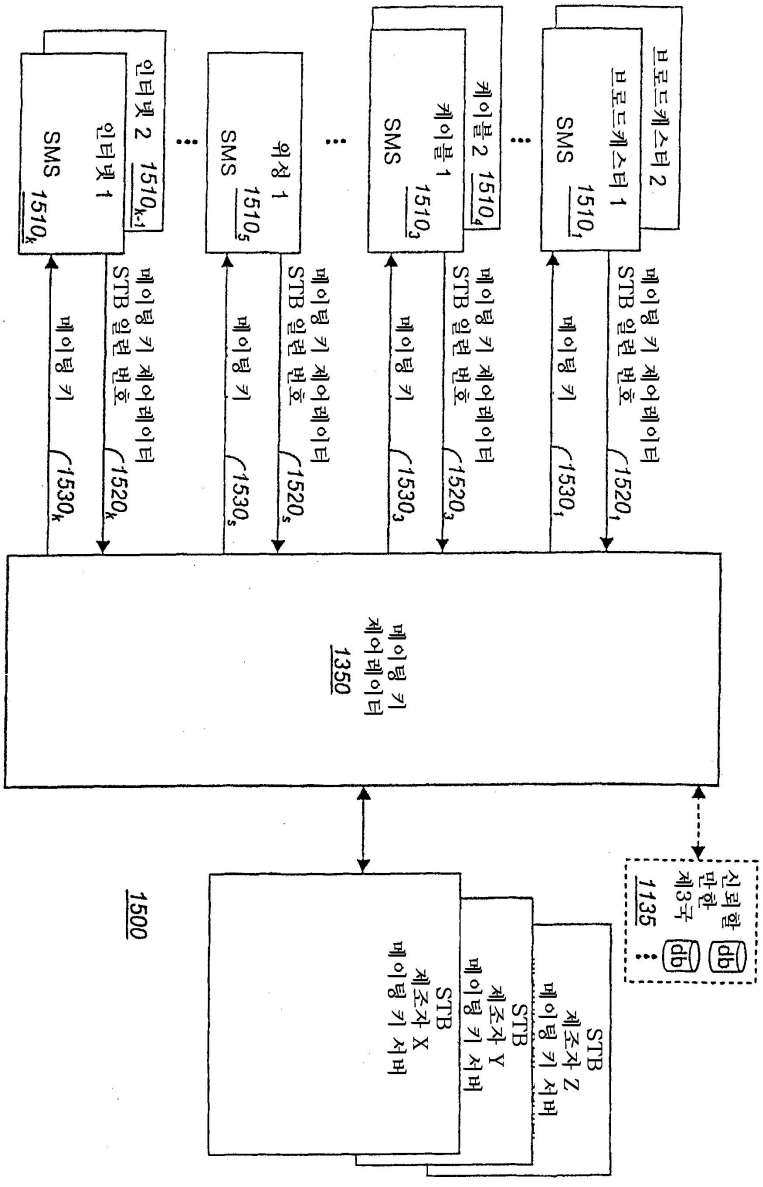
도면15


EPG 메타 데이터 1400
1410$_1$ Program ID, Channel = "CNN", Title = "Larry King",
1420$_1$ 1430$_1$
1460 MKG, Access = Tier 1
1440$_1$
1410$_2$ Program ID, Channel = "HLN", Title = "World News",
MKG, Access = Tier 1
...
1410$_S$ Program ID, Channel = "HBO", Title = "Little Nicky",
MKG, Access = Tier 3
셋탑 박스 1340
디스크램블러 IC 1360
유니크 STB 키
메이팅 키 제너레이터
Key ID, Encrypted Tier 1 Key
Key ID, Encrypted Tier 2 Key
Key ID, Encrypted IPPV Key
헤드엔드 (1310 및/또는 1320)

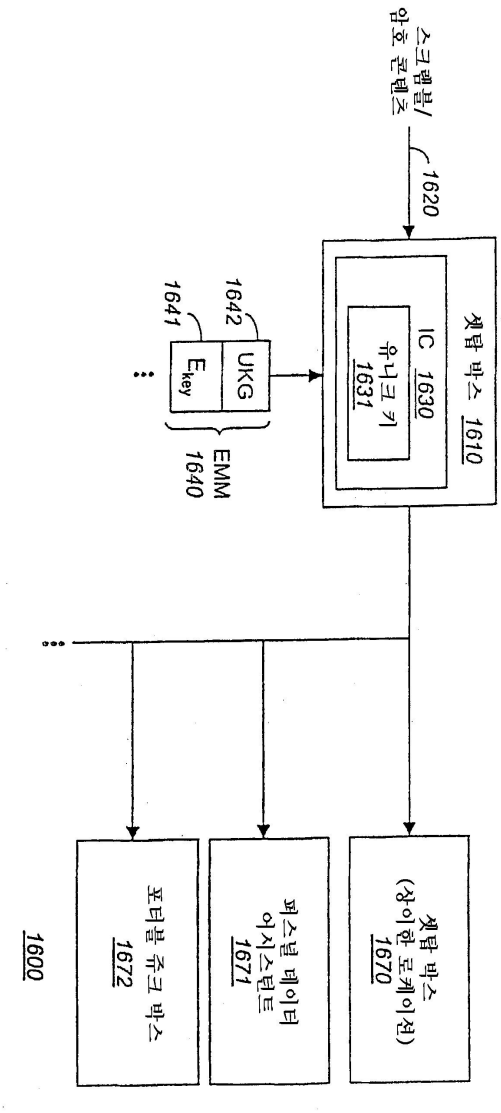
도면16


메이킹 키 제너레이터
1321
암호 서비스 키
1345
스크램블 콘텐츠
1365
디스크램블러 IC 1360
유니크 디스크램블러 IC키 1362
프로세스 (DES)
1361
키
1363
셋탑 박스 입력 번호
1364
프로세스 (DES)
서비스 키
로우레벨 디스크램블링 (3DES)
클리어 콘텐츠

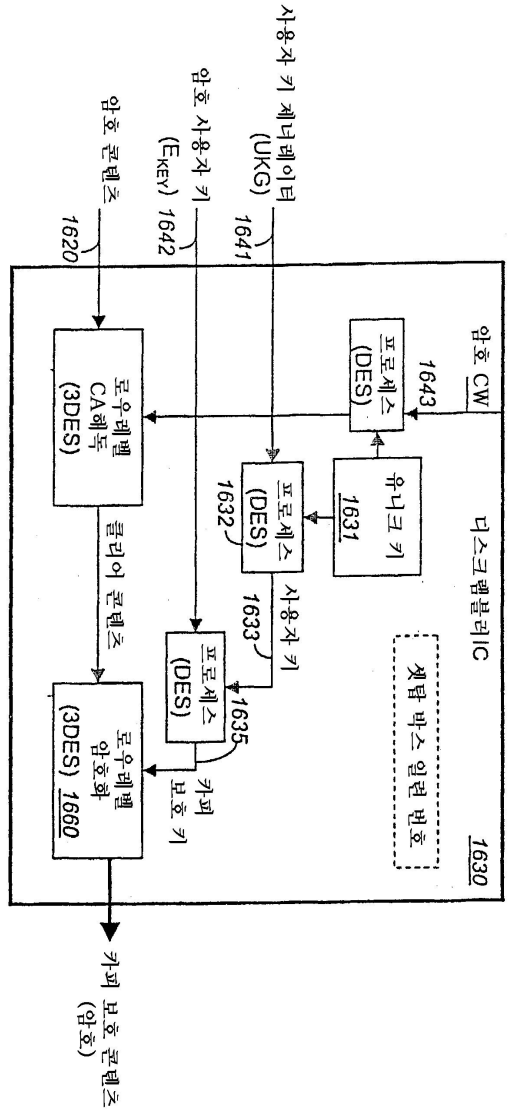
도면17


브로드캐스터 2
브로드캐스터 1
SMS 1510$_1$
케이블 2 1510$_4$
케이블 1
SMS 1510$_3$
위성 1
SMS 1510$_5$
인터넷 2 1510$_{k-1}$
인터넷 1
SMS 1510$_k$
메이텅 키 제어레이터
STB 일련 번호
1520$_1$
메이텅 키
1530$_1$
메이텅 키 제어레이터
STB 일련 번호
1520$_3$
메이텅 키
1530$_3$
메이텅 키 제어레이터
STB 일련 번호
1520$_5$
메이텅 키
1530$_5$
메이텅 키 제어레이터
STB 일련 번호
1520$_k$
메이텅 키
1530$_k$
메이텅 키
제어레이터
1350
신뢰할 만한 제3국
1135
STB
제조자 Z
메이텅 키 서버
STB
제조자 Y
메이텅 키 서버
STB
제조자 X
메이텅 키 서버
1500

도면18


스크램블/
암호 콘텐츠
1620
셋탑 박스 1610
IC 1630
유니크 키
1631
1642
1641
UKG
E_{key}
EMM
1640
셋탑 박스
(상이한 로케이션)
1670
퍼스널 데이터
어시스턴트
1671
포터블 쥬크 박스
1672
1600

도면19


사용자 키 제너레이터
(UKG)
1641
암호 사용자 키
(EKEY) 1642
암호 콘텐츠
1620
암호 CW
1643
프로세스
(DES)
유니크 키
1631
프로세스
(DES)
1632
사용자 키
1633
셋탑 박스 일련 번호
디스크램블러IC
1630
로우레벨
CA해독
(3DES)
클리어 콘텐츠
프로세스
(DES)
1635
카피
보호 키
로우레벨
암호화
(3DES) 1660
카피 보호 콘텐츠
(암호)