(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년11월24일
(11) 등록번호 10-0927968
(24) 등록일자 2009년11월16일

(51) Int. Cl.
H04N 7/16 (2006.01)
(21) 출원번호 10-2004-7002358
(22) 출원일자 2002년07월31일
심사청구일자 2007년07월31일
(85) 번역문제출일자 2004년02월17일
(65) 공개번호 10-2004-0027893
(43) 공개일자 2004년04월01일
(86) 국제출원번호 PCT/IB2002/003206
(87) 국제공개번호 WO 2003/017666
국제공개일자 2003년02월27일
(30) 우선권주장
09/932,069 2001년08월17일 미국(US)
(56) 선행기술조사문헌
EP0506435 A2
KR1019920702158 A
KR1020010043258 A
전체 청구항 수 : 총 12 항

(73) 특허권자
코닌클리케 필립스 일렉트로닉스 엔.브이.
네델란드왕국, 아인드호펜, 그로네보드스베그 1
(72) 발명자
프리맨마틴
네덜란드,아아인드호펜5656,홀스틀란6
루진
네덜란드,아아인드호펜5656,홀스틀란6
(74) 대리인
이범래, 장훈

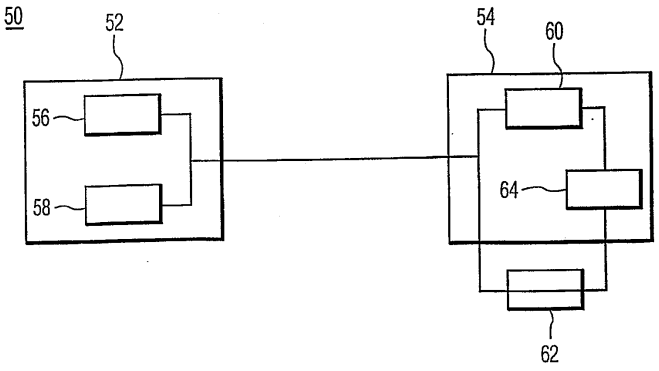
심사관 : 조남신

(54) 암호화된 전송들에 대한 하이브리드 조건부 액세스를 위한 시스템 및 방법

(57) 요 약

전송 스테이션에 의해 암호화된 전송들을 복호화하기 위한 시스템은 수신기를 포함하고, 상기 수신기는 수신기 내에 임베딩된 제 1 조건부 액세스 모듈, 및 상기 수신기로부터 제거가능한 제 2 조건부 액세스 모듈을 포함한다. 상기 제 1 조건부 액세스 모듈은 상기 전송 스테이션에 의해 전송된 제 1 신호를 복호화하고, 상기 제 2 조건부 액세스 모듈은 상기 전송 스테이션에 의해 전송된 제 2 신호를 복호화한다. 상기 제 1 및 제 2 신호들은 개별의 조건부 액세스 모듈들에 의해 암호화된다. 상기 전송 스테이션은 상기 수신기가 상기 전송을 복호화하도록 자격부여된 것을 전송 스테이션에 의해 검증시, 상기 전송을 상기 수신기가 복호화하도록 하기 위한 자격 코드를 상기 수신기에 제공한다.

대 표 도 - 도3



특허청구의 범위

청구항 1

적어도, 서비스 제공자(52)로부터의 비디오 콘텐트를 나타내며 전송들에 대한 액세스의 레벨을 제공하는 제 1 신호, 또는 서비스 제공자(52)로부터의 비디오 콘텐트를 나타내며 상기 전송들에 대한 부가적인 액세스 레벨을 제공하는 제 2 신호의 암호화된 전송들을 복호화하기 위한 시스템에 있어서,

상기 제 1 신호를 복호화하기 위한 임베딩된 조건부 액세스 모듈(60)을 갖는 수신기(54)와, 제거가능한 조건부 액세스 모듈(62)을 결합하기(engaging) 위한 인터페이스를 포함하고, 상기 제거가능한 모듈이 인에이블될 때, 상기 제거가능한 모듈은 상기 제 2 신호를 복호화하고 상기 임베딩된 모듈을 무시하도록 구성되는, 암호화된 전송들을 복호화하기 위한 시스템.

청구항 2

제 1 항에 있어서,

상기 제거가능한 모듈은 상기 인터페이스로 상기 제거가능한 모듈을 결합(engaging)함으로써 인에이블되는, 암호화된 전송들을 복호화하기 위한 시스템.

청구항 3

제 1 항에 있어서,

상기 제거가능한 모듈은 상기 시스템의 세팅을 변화시킴으로써 인에이블되는, 암호화된 전송들을 복호화하기 위한 시스템.

청구항 4

제 1 항에 있어서,

상기 모듈들의 각각의 모듈은 각각의 복호화 알고리즘을 사용하고, 상기 각각의 복호화 알고리즘들은 서로 다른, 암호화된 전송들을 복호화하기 위한 시스템.

청구항 5

제 1 항에 있어서,

상기 제거가능한 모듈이 권한부여되면, 상기 제 2 신호를 복호화할 수 있도록 하는 자격(entitlement)(130)을 스테이션(52)으로부터 수신하기 위해 인에이블된 상기 제거가능한 모듈에 대한 메시지를, 상기 시스템 외부의 상기 스테이션에 전송하기(125) 위한 전송기를 포함하는, 암호화된 전송들을 복호화하기 위한 시스템.

청구항 6

제 1 항에 있어서,

셋톱 박스에 수용되는, 암호화된 전송들을 복호화하기 위한 시스템.

청구항 7

제 1 항에 있어서,

상기 제 1 신호는 전체 비디오 신호 콘텐트 보다 작은 상기 비디오 콘텐트의 일부분을 나타내고, 상기 제 2 신호는 상기 전체 비디오 콘텐트를 나타내는, 암호화된 전송들을 복호화하기 위한 시스템.

청구항 8

적어도, 서비스 제공자(52)로부터의 비디오 콘텐트를 나타내며 전송들에 대한 액세스의 레벨을 제공하는 제 1 신호, 또는 서비스 제공자(52)로부터의 비디오 콘텐트를 나타내며 상기 전송들에 대한 부가적인 액세스 레벨을 제공하는 제 2 신호의 암호화된 전송들을 시스템이 복호화할 수 있게 하는 방법에 있어서,

상기 시스템은 상기 제 1 신호를 복호화하기 위한 임베딩된 조건부 액세스 모듈(60)을 갖는 수신기(54)와, 제거

가능한 조건부 액세스 모듈(62)을 결합하기(engaging) 위한 인터페이스를 포함하고, 상기 제거가능한 모듈은 상기 제 2 신호를 복호화하고 상기 임베딩된 모듈을 무시하도록 구성되는, 암호화된 전송들을 복호화할 수 있게 하는 방법.

청구항 9

삭제

청구항 10

제 8 항에 있어서,

상기 제1 신호는 제 1 알고리즘을 사용하여 암호화되며, 상기 제 2 신호는 상기 제 1 알고리즘과는 다른 제 2 알고리즘을 사용하여 암호되는, 암호화된 전송들을 복호화할 수 있게 하는 방법.

청구항 11

제 8 항에 있어서,

상기 제 1 신호는 전체 비디오 콘텐트 보다 작은 상기 비디오 콘텐트의 일부분을 나타내며, 상기 제 2 신호는 상기 전체 비디오 콘텐트를 나타내는, 암호화된 전송들을 복호화할 수 있게 하는 방법.

청구항 12

제 8 항에 있어서,

상기 제거가능한 모듈이 권한부여되면, 상기 제 2 신호를 복호화할 수 있도록 하는 자격(entitlement)(130)을 스테이션(52)으로부터 수신하기 위해 인에이블된 상기 제거가능한 모듈에 대한 메시지를, 상기 시스템 외부의 상기 스테이션에 전송하는 단계(125)를 포함하는, 암호화된 전송들을 복호화할 수 있게 하는 방법.

청구항 13

제 12 항에 있어서,

상기 복호화할 수 있도록 하는 것은 상기 제 2 신호를 수신할 수 있게 하는 것을 포함하는, 암호화된 전송들을 복호화할 수 있게 하는 방법.

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

명 세 서

기 술 분 야

<1> 본 발명은 암호화된 전송들의 복호화에 관한 것이고, 특히 암호화된 전송들의 수신기들에 대해 하이브리드 조건부 액세스를 제공하기 위한 시스템, 디바이스, 및 방법에 관한 것이다.

배 경 기 술

<2> 케이블 텔레비전(CATV) 서비스 제공자들은 케이블을 통해 가입자들에게 신호를 전송한다. 그 신호는 신호의 주파수 범위 내에 분포된 다수의 채널들을 포함한다. CATV 서비스 제공자들은 비가입자들이 CATV 서비스 제공자의 신호를 이용하는 것을 방지하기 위해, 통상적으로 그 전송 신호들을 암호화한다. 가입자의 TV 또는 VCR이 신호를 이용하기 위해서는, 신호를 수신하고, 신호를 복호화하며, 채널을 선택하는 수단이 제공되어야 한다. 그 제

공된 수단은 통상적으로 셋톱 박스로 알려져 있는 디바이스이다. 그 셋톱 박스는 CATV 서비스 제공자에 의해 전송된 신호를 수신하기 위한 케이블에 접속된다. 셋톱 박스는 또한 디스플레이를 준비하는 신호를 제공하기 위해 가입자의 TV 또는 VCR에 접속된다. 셋톱 박스는 통상적으로 네비게이션(navigation) 기능 및 보안(security) 기능을 제공한다. 네비게이션 기능은 수신된 신호 내에서 채널들을 네비게이팅하여 선택하기 위한 것이다. 보안 기능은 수신된 신호를 복호화하기 위한 것이다. 그 셋톱 박스의 보안 기능은 CATV 서비스 제공자에 의해 제공된 서비스들에 대한 가입자 셋톱 박스의 자격(entitlements)을 결정하기 위한 조건부 액세스(CA) 시스템의 부분이다.

<3> FCC에 의해 요구되는 법에 따라, 네비게이션 기능은 보안 기능과 별도로 유지되어야 한다. 이는 통상적으로 셋톱 박스들 내에 임베딩된 별도의 영구 보안 기능, 또는 셋톱 박스와 인터페이싱하는 스마트 카드(smart card) 형태의 별도의 제거가능한 보안 기능 중 하나를 갖는 셋톱 박스들에 의해 달성된다.

<4> 임베딩된 보안 기능만을 갖는 셋톱 박스를 제공하는데는 단점들이 있다. 셋톱 박스 내의 보안 기능은 고정된다. 제어 액세스 시스템 내의 중요 특징들이 변화된 경우, 그 셋톱 박스 내의 보안 기능은 작동하지 않게(non-functional) 된다. 예를 들어, 케이블 서비스 제공자들은 주기적으로 사용되는 암호화 방법을 변화시킬 수 있고, 임의의 채널들에 대한 상이한 레벨의 자격을 가입자들에게 제공하거나 요구할 수 있다. 자격부여 또는 암호화 방법의 변화를 수용하기 위해, 다른 보안 기능을 갖는 새로운 셋톱 박스가 원래의 셋톱 박스를 대체하는 것이 요구된다. 더구나, 각각의 셋톱 박스는 CATV 서비스 제공자에 의해 특정된 것으로 주문 제작되어야 하며, 따라서 높은 제조 비용을 발생한다.

<5> 제거가능한 보안 기능을 셋톱 박스에 제공하는 것은 셋톱 박스를 대체할 필요없이 그 셋톱 박스의 보안 기능을 바꿀 수 있는 가능성을 제공한다. 더구나, 표준 셋톱 박스가 다양한 CATV 서비스 제공자들을 위해 사용될 수 있으며, 따라서 제조 비용을 낮춘다. 그러나, 보안 기능을 제공하는 제거가능한 모듈만을 셋톱 박스에 제공하는 것에 단점들이 있다. 제거가능한 모듈의 부재(absence) 또는 이탈(disengagement) 시에, 셋톱 박스는 네비게이팅 기능을 무시하고 수신된 전송들 중 어떤 것도 복호화할 수 없다. 제거가능한 모듈 없이, 셋톱 박스는 암호화되지 않은 콘텐트를 단지 보여줄 수 있을 뿐이다. 그러한 콘텐트는 대개 큰 가치가 없다.

<6> 발명의 명칭이 Video Signal Decoder System인, EP 공개번호 0 585 833 A1호는 비디오 신호들을 디코딩하기 위한 셋톱 박스를 개시하고 있고, 그 박스는 두 개의 보안 기능 모듈들: 임베딩된 보안 기능 모듈, 및 그 박스와 인터페이싱하는 교환가능한 스마트 카드 보안 기능 모듈을 포함한다. 그러나, 개시된 박스는 많은 단점들을 갖는다. 신호를 수신하자마자, 복호화는 보안 기능 모듈들 중 하나에 의해 수행된다. 보안 기능 모듈은 시행착오(trial and error) 방법을 통해 그 박스에 의해 선택된다. 임베딩된 보안 기능 모듈은 선택을 위해 먼저 테스트되고, 스마트 카드가 두번째로 테스트된다. 임베딩된 보안 기능 또는 스마트 카드 보안 기능 중 선택된 하나의 보안 기능 모듈은 어느 것이 수신된 신호의 암호화 알고리즘에 대응하는 복호화 알고리즘을 갖는지에 의존한다. 따라서, 복호화를 수행하기 위한 하나의 보안 기능 모듈의 선택은 그 박스에 의해 수신된 신호에 따라서 행해지고, 다른 보안 기능 모듈은 디스에이블(disable)된다. 따라서 그 박스는 디폴트 보안 기능 모듈을 제공하지 않는다. 그 박스는 수신된 전송에 대한 상이한 액세스 레벨들을 허용하지 않는다.

<7> U.S. 특허번호 5,742,680호는 수신된 신호의 복호화를 제공하기 위한 셋톱 박스를 개시하며, 그 신호는 복수의 전송기들로부터 선택된 전송기에 의해 전송되고, 복호화는 복수의 스마트 카드 보안 기능 모듈들 중 대응하는 스마트 카드에 의해 수행된다. 그 박스는 임베딩된 보안 기능 모듈을 포함하지 않는다. 선택된 신호를 위한 대응하는 스마트 카드가 없다면, 그 셋톱 박스는 복호화를 수행할 수 없다.

<8> 앞서 언급한 참조들에서, 스마트 카드의 소유자는 호환성 있는 셋톱 박스에 그 스마트 카드를 사용할 수 있다. 그러나, 전송된 신호들의 제공자들은 종종 가입자에 속하는 셋톱 박스에 대해 그들 신호들의 복호화를 제한하는 것이 제공자들에게 이점임을 발견한다. 더욱이, 앞서 언급된 참조들은 그 전송된 신호들을 복호화하기 위해 자격을 점검하는 것을 제공하지 않는다. 또한 참조들은 더 이상 자격부여되지 않는 보안 기능 모듈들을 디스에이블하지도 않는다. 자격이 부여되지 않은(non-entitled) 복호화를 방지하기 위해, 신호 전송들의 제공자들은 전송된 신호들의 암호화 알고리즘을 바꾸어야 한다. 이는 모든 자격부여된 고객들에게 새로운 스마트 카드들의 배분을 필요로 할 것이다.

<9> EP 공개번호 0 570 785 A1호는 규정된 지리학적 위치에서 스마트 카드를 사용하여 전송된 신호들의 복호화를 허용하기 위한 방법을 개시한다. 그러나, 이를 달성하기 위해, 상기 방법은 적어도 두 개의 별개의 프로세서들에 의해 수신되는 적어도 두 개의 데이터 채널들의 전송을 필요로 한다.

발명의 상세한 설명

<10> 본 발명의 목적은 전송 스테이션으로부터 암호화된 전송들을 수신하고 복호화하기 위한 수신기를 제공하는 것이며, 그 수신기는 디폴트 임베딩된 보안 기능 모듈 및 그 전송들에 대한 부가적인 액세스 레벨을 제공하기 위한 제거가능한 보안 기능 모듈을 가지며, 디폴트 모드는 제거가능한 보안 기능 모듈의 가용성에 무관하게 동작한다.

<11> 본 발명의 다른 목적은 수신기에 의해 전송 시스템으로부터의 암호화된 전송들로의 액세스를 제공하기 위한 시스템 및 방법을 제공하는 것이며, 그 수신기는 디폴트 레벨을 포함하여 전송들에 대한 다양한 액세스 레벨들이 허용된다.

<12> 본 발명의 다른 목적은 전송들에 대한 사용자 및 수신기 중 하나의 자격들(entitlements)에 따라서, 수신기에 의해 전송 시스템으로부터의 암호화된 전송들로의 액세스를 제공하기 위한 시스템 및 방법을 제공하는 것이다.

<13> 본 발명의 다른 목적은 최상의 서비스를 제공하면서 제조 및 분배에 효율적인, 보안 기능 모듈들 및 수신기를 제공하기 위한 시스템 및 방법을 제공하는 것이 다.

<14> 상기 목적들을 달성하기 위해, 본 발명에 따른 전송 스테이션으로부터 암호화된 전송들을 수신하고 복호화하기 위한 시스템은, 전송들을 수신하며, 선택가능한 제 1 및 제 2 보안 기능 모듈들 및 초기화 모듈을 갖는 수신기를 포함한다. 제 1 보안 기능 모듈은 수신기 내에 임베딩되며, 전송의 제 1 신호가 복호화되는 디폴트 복호화 모드를 제공한다. 제 2 보안 기능 모듈은 수신기로부터 제거가능하고 제 2 전송 신호를 복호화한다. 보안 기능 모듈 선택시, 초기화 모듈이 선택된 보안 기능 모듈로 수신된 신호를 복호화하고 그 선택을 전송 스테이션에게 알리기 위해 수신기를 초기화한다. 시스템은 제 1 및 제 2 신호들을 암호화하는 전송 스테이션의 헤드-엔드(head-end)에 있는 별개의 보안 기능 모듈들을 더 포함한다. 그 전송 스테이션은 제 1 또는 제 2 신호들을 수신하는 수신기의 자격들을 검증하고, 수신기의 선택된 보안 기능 모듈이 대응하는 신호를 복호화하는 것을 허용하는 자격 코드를 수신기에게 제공한다.

<15> 본 발명은 또한 전송 스테이션으로부터 수신기로 전송된 암호화된 전송들을 복호화하기 위한 방법을 개시하고, 이는 상기 전송 스테이션에 의한 전송을 전송하는 단계; 상기 전송의 제 1 신호를 수신하는 단계; 상기 수신기 내에 임베딩된 제 1 보안 기능 모듈에 의해 제 1 신호를 복호화하는 단계; 상기 수신기에 인터페이싱된 제 2 조건부 액세스 모듈을 인에이블하는 단계; 상기 제 1 보안 기능 모듈에 의한 상기 제 1 신호의 복호화를 중지하는 단계; 상기 수신기에서 상기 전송의 제 2 신호를 수신하는 단계; 및 상기 제 2 조건부 액세스 모듈에 의해 상기 제 2 신호를 복호화하는 단계를 포함한다.

<16> 본 발명은 또한 일반적으로 적어도 제 1 신호 및 제 2 신호의 암호화된 전송들을 복호화하기 위한 시스템을 제공한다. 상기 시스템은 적어도 제 1 신호 및 제 2 신호의 전송들을 수신하기 위한 수신기를 포함한다. 상기 수신기는 제 1 전송된 신호를 복호화하기 위한 제 1 임베딩된 조건부 액세스 모듈 및 제 2 전송된 신호를 복호화하기 위한 제 2 제거가능한 조건부 액세스 모듈을 갖는다. 제 2 조건부 액세스 모듈을 인에이블하는 것은 제 2 조건부 액세스 모듈이 제 1 조건부 모듈을 무시하게 된다.

<17> 본 발명은 또한 일반적으로 수신기로의 암호화된 전송들을 전송하기 위한 전송 스테이션을 포함한다. 상기 전송 스테이션은 제 1 신호를 암호화하기 위한 제 1 조건부 액세스 모듈 및 제 2 신호를 암호화하기 위한 제 2 조건부 액세스 모듈을 갖는 적어도 하나의 헤드-엔드를 포함한다. 상기 헤드-엔드는 수신기가 제 2 신호를 복호화할 권리를 갖는지 여부를 결정하기 위한 자격 모듈(entitlement module)을 더 포함한다. 그 자격 모듈에 의한 포지티브 결정시, 상기 전송 스테이션은 수신기가 제 2 신호를 복호화하도록 허용하는 수신기에게 자격 코드를 전송한다.

<18> 그러므로, 수신기가 전송 스테이션에 의해 전송되는 전송을 수신하고 복호화하는 시스템에 대한 필요성이 존재하며, 그 수신기는 임베딩된 보안 기능 모듈 및 제거가능한 보안 기능 모듈 둘 모두를 갖는다. 디폴트 모드를 제공하기 위해 임베딩된 보안 기능 모듈의 필요성이 존재하므로, 전송 스테이션으로부터의 전송들은 제거가능한 보안 기능 모듈의 가용성에 무관하게 디폴트 레벨로 복호화될 수 있다. 전송들에 대한 다양한 액세스 레벨들을 제공할 필요성이 존재한다. 자격들을 갖지 않는 사용자들이, 기존의 보안 기능 모듈들의 영구적인 무력화를 요구하지 않으면서, 제한된 전송들을 보는 것을 방지하기 위한 필요성이 존재한다.

<19> 본 발명의 상기 및 다른 목적들, 특징들 및 이점들이 첨부된 도면들과 관련하여 취해지는 예시적인 실시예의 다음의 상세한 설명의 관점에서 분명해질 것이다.

실 시 예

<25> 이제, 도면들로 돌아가서, 같은 참조 번호들은 몇 가지 시점들을 통해 유사하거나 동일한 요소들을 식별하며, 전송 스테이션에 의해 전송된 암호화 전송들의 복호화에 대해 종래 기술의 시스템은 도 1에 도시된다.

<26> 도 1을 참조하면, (10)으로 도시된 종래 기술의 시스템은 신호를 수신기(14)로 전송하는 헤드 엔드(head-end)(12)를 갖는 전송 스테이션을 포함한다. 상기 전송 스테이션은 통상적으로 케이블 텔레비전(CATV) 서비스 제공자이다. 상기 수신기(14)는 통상적으로 셋톱 박스이다. 셋톱 박스와 전송 시스템 사이에서 전송은 케이블을 통해 전송된다. 일단 전송들이 수신되어 복호화되면, 셋톱 박스는 그 전송들을 시청하기 위한 TV 또는 VCR과 통신한다. 조건부 액세스(CA) 시스템으로 알려져 있는 보안 시스템이 자격들을 갖지 않는 수신기에 의해 액세스되는 것으로부터 전송의 보안을 위해 제공된다. 도 1에 도시된 시스템의 CA 시스템은 CA 모듈(16) 및 CA 모듈(18)로 구성된다. CA 모듈(16)은 전송 스테이션의 헤드-엔드에 위치된다. CA(16)는 전송을 위해 그 신호의 콘텐츠를 암호화하는 반면, CA(18)는 시청을 위해 그 수신된 신호를 복호화한다. CA(18)는 영구적인 구성요소로서 셋톱 박스 내에 임베딩된다.

<27> 다른 종래 기술은 도 2에 도시된다. 도시된 종래 기술의 시스템(20)은 헤드-엔드(22) 및 셋톱 박스(24)를 포함한다. CA 모듈(26)은 헤드-엔드(22)에 위치되고, CA 모듈(28)은 셋톱 박스(24)에 위치된다. CA 모듈(28)은 제거가능한 스마트 카드이다. CA 모듈(28)은 다른 스마트 카드로 교환될 수 있다.

<28> 도 3을 참조하면, 본 발명의 시스템의 일 실시예가 도시된다. 본 발명의 시스템(50)은 헤드-엔드(52)를 갖는 전송 스테이션 및 셋톱 박스(54)을 제공한다. 셋톱 박스(54)는 위성 접시형 안테나(satellite dish antenna)에 의해 수신된 방송 전파(airwaves)와 같은 무선 수단을 통해 또는 케이블들을 통해 전송 스테이션(52)으로부터의 전송을 수신한다. 전송 스테이션(52)은 두 개의 신호들을 전송한다. 제 1 CA 모듈(56)은 제 1 신호를 암호화한다. 제 2 CA 모듈(58)은 제 2 신호를 암호화한다.

<29> 셋톱 박스는 전송 스테이션에 의해 전송된 신호들을 복호화하기 위해 임베딩된 CA 모듈(60) 및 제거가능한 CA 모듈(62)을 포함하는 하이브리드 조건부 액세스 아키텍처를 제공한다. 셋톱 박스에는 CA 모듈(62)을 결합(engaging)하고 CA 모듈을 셋톱 박스와 인터페이싱하기 위한 표준 인터페이스가 제공된다.

<30> 동작시, 초기에, 셋톱 박스는 CA 모듈(56)에 의해 암호화된 전송 스테이션으로부터 신호들을 수신하고, 임베딩된 CA 모듈(60)을 통해 제 1 암호화된 신호를 복호화한다. CA 모듈(60)은, 심지어 제거가능한 모듈이 인에이블되지 않거나 사용가능하기 않은 경우에도, 전송 스테이션으로부터의 전송을 복호화하기 위한 디폴트 조건부 액세스 능력을 제공한다.

<31> CA 모듈(62)을 인에이블할 시, 재초기화 유닛(reinitialize unit)(64)은 CA 모듈(62)이 수신된 전송을 복호화하는 것을 허용하기 위해 셋톱 박스를 재초기화함으로써 셋톱 박스를 리셋하고, 전송 스테이션(52)에 변경 신호 메시지를 전송할 것을 셋톱 박스(54)에 명령하고, CA 모듈(60)에 의한 제 1 신호의 복호화를 중단한다. 변경 신호 메시지는 셋톱 박스(54)가 제 2 신호를 복호화할 준비가 되었음을 전송 스테이션에 알린다.

<32> 변경 신호 메시지를 수신할 시, 전송 스테이션(52)의 헤드-엔드는 셋톱 박스가 제 2 신호를 수신할 자격이 있는지의 여부를 결정한다. 상기 결정은 셋톱 박스의 소유자들이 데이터베이스 내에 기록된 것과 같은 전송 스테이션에 의해 제공된 서비스에 대해 가입 요금을 지불했는지의 여부와 같은 전송 스테이션의 관리자들에 의해 설정된 기준들에 따라서 행해진다.

<33> 긍정적인 결정(positive determination)시, 헤드-엔드는 자격 코드(entitlement code)를 전송하고, 이는 셋톱 박스가 제 2신호를 복호화할 수 있게 할 것이다. 셋톱 박스(54)가 자격 코드를 갖는 제 2 신호를 수신할 시, CA 모듈(62)은 제 2 신호를 복호화하도록 진행한다.

<34> 바람직한 실시예의 셋톱 박스에서, 제거가능한 CA 모듈(62)은 효율적인 제조 및 분배를 위해 제공하는 표준 모듈이다. 이는 업그레이드들, 보안 변경들 및 새로운 제품들을 처리하기에 유리하다. 도 4 및 도 5는 각각 본 발명의 일 실시예의 셋톱 박스 및 전송 스테이션에 의해 수행된 단계들을 기술하는 예시적인 흐름도들이다. 변경들이 선호(preference), 설계 선택(design choice) 등에 따라 구현될 수 있다.

<35> 도 4를 참조하면, 셋톱 박스에 의해 수행되는 단계들은 이제 기재될 것이다. 단계 98에서, 전송들을 수신하기 위해 셋톱 박스(54)를 활성화할 시, 셋톱 박스(54)는 셋톱 박스(54)의 CA 모듈(60)이 제 1 신호를 복호화할 준비가 되었음을 전송 스테이션에 알리기 위해 전송 스테이션에 메시지를 보낸다.

<36> 단계 100에서, 셋톱 박스는 전송들을 수신한다. 바람직한 실시예에서, 제 1 신호는 제 1 신호에 대한 자격 코드와 함께 수신된다. 제 1 신호 자격 코드는 셋톱 박스가 제 1 신호를 수신하도록 허용한다. 다른 실시예에서, 자격 코드는 셋톱 박스가 신호를 복호화하도록 허용하는 키 데이터(key data)를 제공한다. 또 다른 실시예에서, 자격 코드는 상기 기능 둘 모두를 허용한다.

<37> 결정 단계 102에서, 제 1 신호 자격 코드가 수신되었는지의 여부가 결정된다. 수신되지 않았다면, 제 1 신호는 복호화될 수 없으며, 제어는 셋톱 박스의 사용자에게 그가 임의의 신호들을 시청할 자격이 부여되지 않았으며 액세스가 거부되었음을 알리기 위해 단계 103으로 진행한다. 이어서 프로세스는 단계 98로 귀환한다.

<38> 제 1 신호 자격 코드가 수신되었다는 결정시, 프로세스는 단계 105로 이동한다. 단계 105에서, 제 1 신호는 CA 모듈(60)에 의해 복호화된다. 결정 단계(110)에서, 셋톱 박스는 CA 모듈(62)이 인에이블되었는지에 대한 여부를 결정한다. 동작시, CA 모듈(62)은 일단 삽입되면, 제거가능한 모듈을 삽입하거나 또는 스위치를 활성화하는 것과 같은 여러가지 방법들로 인에이블될 수 있다. CA 모듈(62)이 인에이블되지 않을 경우, 셋톱 박스는 제 1 신호를 수신하고 복호화하는 것을 계속하며, 프로세스는 단계 110으로 귀환한다. CA 모듈(62)가 활성화되었다면, 프로세스는 단계 115로 이동한다.

<39> 단계 115에서, 셋톱 박스는 리셋된다. CA 모듈(62)이 수신된 신호를 복호화하도록 허용하기 위해 초기화 루틴(initialization routine)이 수행된다. 단계 120에서, CA 모듈(60)에 의한 제 1 신호의 복호화가 중단된다. 단계 125에서, 셋톱 박스는 CA 모듈(62)이 선택되었으며 제 2 신호를 복호화할 준비가 되었음을 전송 스테이션에 알리기 위해 전송 스테이션에게 변경 신호 메시지를 전송한다. 단계들 115 내지 125의 수행 순서는 설계 선택에 따라 재구성될 수 있다.

<40> 단계 130에서, 셋톱 박스는, 권한이 부여된 경우, 전송 스테이션으로부터 제 2 신호에 대한 자격 코드를 수신한다. 결정 단계 132에서, 제 2 신호에 대한 제 2 신호 자격 코드가 수신되었는지의 여부가 결정된다. 수신되지 않았다면, 제 2 신호는 복호화될 수 없으며, 프로세스는 제 1 신호를 복호화하기 위해 셋톱 박스를 재초기화하고, 셋톱 박스가 제 1 신호를 복호화할 준비가 되었음을 전송 스테이션에 알리기 위한 단계 133으로 진행한다.

<41> 제 2 신호 자격 코드가 단계 132에서 수신되었다는 결정시에, 프로세스는 단계 135로 이동한다. 단계 135에서, CA 모듈(62)은 제 2 신호를 복호화한다. 단계 140에서, CA 모듈(62)이 여전히 인에이블 상태인지의 여부에 관해 결정이 이루어진다. 제 2 신호의 복호화는 CA 모듈(62)이 디스에이블될 때까지 계속된다. CA 모듈(62)의 디스에이블 시에, 셋톱 박스는 제 2 신호를 복호화하는 것을 중단하며, 프로세스는 제 1 신호를 수신하여 복호화하기 위해 재초기화를 위한 단계 133으로 진행한다.

<42> 다음으로, 도 5를 참조하면, 전송 스테이션에 의해 수행되는 단계들이 이제 기재될 것이다. 암호화된 제 1 및 제 2 신호들을 계속적으로 전송하는 동안, 전송 스테이션은 단계 210에서 CA 모듈(60)이 제 1 신호를 복호화할 준비가 되었다는 메시지의 수신을 위해 대기한다.

<43> 단계 210에서 메시지의 수신시, 프로세스는 결정 단계 215로 이동한다. 단계 215에서, 전송 스테이션은 셋톱 박스가 제 1 신호를 복호화할 자격이 부여되었는지의 여부를 결정한다. 부여되지 않았다면, 프로세스는 단계 210으로 귀환한다. 설계 선택에 따라서, 루틴이 다양한 단계들을 이용하여 대안으로 수행될 수 있다. 예를 들어, 루틴은 프로세스가 단계 210으로 귀환한 후, 사용자에게 그가 전송들의 콘텐츠를 시청할 자격이 부여되지 않았음을 알리기 위해 셋톱 박스에 메시지를 보낼 수 있다. 또한, 단계들 210 및 215는 하나의 단계로 통합될 수 있으며, 현재 자격들을 갖는 셋톱 박스들로부터 수신된 메시지들만이 인식된다. 만일, 단계 215에서, 셋톱 박스가 제 1 신호를 복호화할 자격이 부여되었음이 확인되면, 프로세스는 단계 225로 진행한다.

<44> 단계 225에서, 제 1 신호 자격 코드가 셋톱 박스로 전송된다. 제 1 신호 자격 코드는 셋톱 박스가 제 1 신호를 복호화하도록 허용한다. 일 실시예에서, 제 1 신호 자격 코드는 셋톱 박스가 제 1 신호를 수신하도록 허용하기 위해 제 1 신호의 전송에 대한 프리픽스(prefix)로서 부착된 셋톱 박스에 대응하는 어드레스이다. 다른 실시예에서, 제 1 신호 자격 코드는 키를 포함하고, 이는 CA 모듈(60)이 CA 모듈(56)에 의해 사용된 암호화 알고리즘에 대응하는 복호화 알고리즘을 사용하도록 허용한다. 또 다른 실시예에서, 제 1 신호는 자격의 검증을 요구하지 않으면서, 전송 스테이션과 통신하는 임의의 셋톱 박스에 의해 수신되어 복호화될 수 있다.

<45> 단계 230은 대기 단계이며, 전송 스테이션은 CA 모듈(60)이 제 1 신호를 더 이상 복호화하지 않을 것이라는 것과, CA 모듈(62)이 제 2 신호를 복호화할 준비가 되었음을 설명하는 셋톱 박스로부터의 변경 신호 메시지의 수신을 대기한다. 변경 신호 메시지의 수신시, 프로세스는 단계 235로 진행한다. 결정 단계 235에서, 전송 스테이션은 셋톱 박스가 제 2 신호를 복호화할 자격이 부여되었음을 검증한다. 검증시에, 프로세스는 단계 240으로 진

행한다.

<46> 단계 240에서, 전송 스테이션은 셋톱 박스로 제 2 신호 자격 코드를 전송한다. 제 2 신호 자격 코드는 셋톱 박스가 제 2 신호를 복호화하도록 허용한다. 제 2 신호 자격 코드는 제 1 신호 자격 코드와 유사한 방식으로 기능한다.

<47> 셋톱 박스가 제 2 신호의 복호화에 자격부여 되어 있지 않음이 결정되었다면, 프로세스는 단계 225로 귀환한다. 대안으로, 루틴이 설계 선택에 따라서 수행될 수 있다. 예를 들어, 루틴은 사용자에게 그들이 제 2 신호의 콘텐츠를 시청하도록 자격부여되지 않았음을 알리기 위해 셋톱 박스에 메시지를 전송하기 위한 단계를 가질 수 있으며, 이어서 프로세스는 셋톱 박스가 시청을 위한 제 1 신호를 복호화하도록 허용하기 위한 단계 225로 귀환될 수 있다.

<48> 도 4 및 도 5에 도시된 실시예에서, 셋톱 박스는 제 2 신호를 수신하여 복호화하도록 허용되기 이전에 제 1 신호를 수신하여 복호화하는 것이 바람직하다. 다른 실시예에서, 시스템 및 방법은 셋톱 박스의 사용자가 제 2의 복호화를 위한 CA 모듈(60) 또는 제 2 신호의 복호화를 위한 CA 모듈(62) 둘 중 하나를 초기에 선택하도록 허용하기 위해 변경될 수 있다. 하나의 가능한 변경에서, 전송 스테이션은 CA 모듈(62)이 제 2 신호를 복호화하도록 허용하기 전에 전송 스테이션으로부터의 전송들을 복호화하는 셋톱 박스의 자격을 검증한다. 이는 불입한(paid-up) 가입자들에 속하는 셋톱 박스들과 함께 사용하는 제거가능한 CA 모듈(62)의 사용을 제한한다. 다른 변경에서, 자격들은 CA 모듈들(60, 62) 각각에 대해 개별적으로 검증되므로, 제거가능한 CA 모듈(62)은 셋톱 박스와 연관된 자격들과 무관하게 임의의 호환가능한 셋톱 박스에서 사용될 수 있다.

<49> 다른 실시예에서, CA 모듈(60)은 기본적인 액세스 레벨을 제공하고, CA 모듈(62)은 부가적인 액세스 레벨들을 제공하지만 기본적인 액세스 레벨을 제공하지는 않는다. CA 모듈(62)이 인에이블된 경우, CA 모듈들(60, 62)은 전체 범위의 액세스 레벨들을 함께 제공한다. 예를 들어, 전송 스트림(transport stream)이 비디오 스트림 및 두 개의 오디오 스트림들을 포함하는 전송이 제공된다. 하나의 오디오 스트림은 영어이고, 다른 오디오 스트림은 스페인어이다. CA 모듈(60)은 영어 오디오 스트림만을 복호화하는 반면, CA 모듈(62)은 스페인어 오디오 스트림만을 복호화할 수 있다. CA 모듈(62)을 수신기로 삽입하기에 전에, 시청자들은 단지 시청자들에게 디폴트 액세스를 제공하는 영어 언어만을 들을 수 있다. CA 모듈(62)을 수신기로 삽입할 시, 시청자들은 그 시청자들에게 프리미엄 액세스(premium access)를 제공하는 둘 모두의 언어로부터 선택할 수 있다.

<50> 앞서 제안된 바와 같이, 실시예들이 "제 1 신호" 및 "제 2 신호"를 사용하지만, 이들은 다수의 신호들을 각각 포함하는 제 1 및 제 2 패키지들을 나타낼 수 있다. 예를 들어, 신호들의 제 1 패키지는 기본적인 케이블 채널들에 대응할 수 있고, 신호들의 제 2 패키지는 프리미엄 케이블 채널들의 패키지에 대응할 수 있다. 케이블 제공자는 다수의 상이한 제 2 또는 프리미엄 패키지들을 이용할 수 있도록 할 수 있다. 각각의 그러한 패키지는 그 패키지에 대한 신호들을 복호화하는 특정의 제거가능한 CA 모듈을 가질 것이다.

<51> 또한, 수신기는 다수의 제거가능한 CA 모듈들을 수신하기 위한 하나 이상의 포트를 가질 수 있다. 각각의 그러한 제거가능한 모듈은 앞서 기재된 바와 같이 별개의 "제 2 신호", 다시 말해 제 3, 제 4 등의 신호들을 수신할 수 있다. 각각의 그러한 제거가능한 모듈은 구별되는 복호화 알고리즘을 가질 수 있고, 복호화 권한부여는 앞서 기재된 전송 스테이션과 신호 교환 및 처리와 유사할 수 있다. 또한, 임베딩된 CA 모듈과 다수의 제거가능한 CA 모듈들 중 하나를 인에이블하고 나머지는 디스에이블하는 우선순위 구성이 될 수 있다. 예를 들면, 제거가능한 CA 모듈들을 위한 수신기에서 포트들은 케이블 패키지를 위한 제거가능한 모듈이 그에 플러그인 될 수 있도록 구성될 수 있다. 다수의 모듈들이 플러그인되면, 전송 스테이션에 의해 권한을 부여받은 가장 높은 레벨의 프리미엄 채널은 인에이블되는 반면, 모든 다른 것들이 디스에이블된다.

<52> 자격 권리들의 결정은 전송 스테이션의 관리에 의해 소망되는 바와 같이 신호들 중 하나를 복호화하기 위한 권리들에 대하여 생략되는 것으로 고려된다.

<53> 도 4 및 도 5에 도시된 자격 권리들의 결정은 단지 예시적인 것이고, 다른 방법이 전송 스테이션의 관리의 목적들에 따라서 구현될 수 있다.

<54> CA 모듈(62)이 복수의 제거가능한 모듈들을 포함할 수 있으며, 각각의 제거가능한 모듈은 전송 스테이션에 상이한 액세스 레벨을 제공하며, CA 모듈(60)은 여전히 디폴트 모드를 제공하면서 제거가능하고 교환가능한(interchangeable) 것으로 고려된다.

<55> 전송 스테이션이 하나의 신호를 전송할 것으로 또한 고려되며, 그 임베딩되고 제거가능한 CA 모듈들은 동일한 신호에 상이한 액세스 레벨들을 제공한다. 그러므로, 예를 들어, 시스템은 적어도 하나의 신호의 암호화된 전송

들을 복호화하기 위한 것일 수 있다. 시스템은 적어도 하나의 신호의 전송들을 수신하기 위한 수신기를 포함할 수 있다. 수신기는 수신된 전송들을 복호화하기 위해 제 1 임베딩된 조건부 액세스 모듈 및 제 2 제거가능한 조건부 액세스 모듈을 갖는다. 제 2 조건부 액세스 모듈을 인에이블하는 것은 제 2 조건부 액세스 모듈이 제 1 조건부 액세스 모듈을 무시하도록 한다. 제 1 임베딩된 조건부 액세스 모듈 및 제 2 제거가능한 조건부 액세스 모듈은 상이한 복호화 알고리즘들을 가질 수 있다. 단일 신호가 수신될 때, 제 1 조건부 액세스 모듈이 (프리미엄 방송의 "프리뷰(preview)"와 같은) 신호의 단지 임의의 양상들(aspects)을 복호화할 수 있는 반면, 제 2 제거가능한 조건부 액세스 모듈의 복호화 알고리즘은 전체 신호를 복호화할 수 있으며, 따라서 프리미엄 방송 그 자체의 시청을 허용한다. 따라서, 제 2 제거가능한 조건부 액세스 모듈이 인에이블되는 경우, 시청자는 프리미엄 방송을 시청할 것이다.

<56> 전송 스테이션이 둘 이상의 신호들을 전송하고, 셋톱 박스는 하나 이상의 전송 스테이션으로부터의 전송들을 수신하는 것이 또한 고려된다.

<57> 전송 스테이션은 임의의 사용가능한 매체를 통해 신호들을 전송하고, 그 신호는 암호화가 바라는 임의의 신호 형태가 될 수 있으로 고려된다.

<58> 본 발명이 바람직한 실시예들을 참조하여 상세하게 기재되었을지라도, 그들은 단지 예시적인 응용들을 나타낸다. 그러므로, 많은 변경들이 첨부 청구항들에 의해 정의된 바와 같이 본 발명의 범위 및 정신에서 벗어나지 않고 본 기술 분야의 숙련자에 의해 행해질 수 있다.

도면의 간단한 설명

<20> 도 1은 CATV 서비스 제공자의 전송 스테이션에 의해 전송되는 암호화된 신호의 수신기에 의한 복호화를 위한 종래 기술의 시스템의 블록도.

<21> 도 2는 CATV 서비스 제공자의 전송 스테이션에 의해 전송된 암호화된 신호의 수신기에 의한 복호화를 위한 시스템의 블록도.

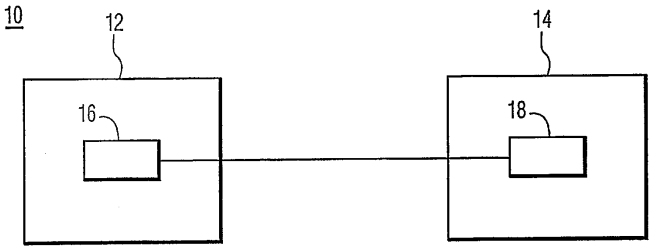
<22> 도 3은 본 발명에 따른 전송 스테이션에 의해 전송되는 암호화된 신호의 수신기에 의한 복호화를 위한 시스템의 블록도.

<23> 도 4는 본 발명에 따른 복호화된 전송들의 수신기에 의해 수행된 단계들을 설명하는 예시적인 플로우차트.

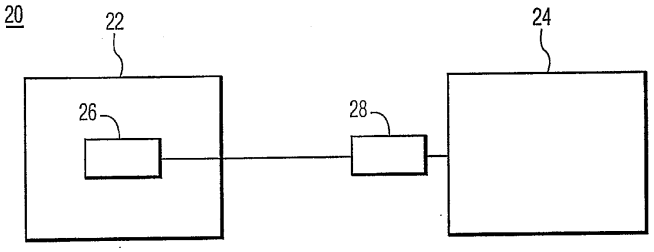
<24> 도 5는 본 발명에 따른 암호화된 전송들의 전송기에 의해 수행된 단계들을 설명하는 예시적인 플로우차트.

도면

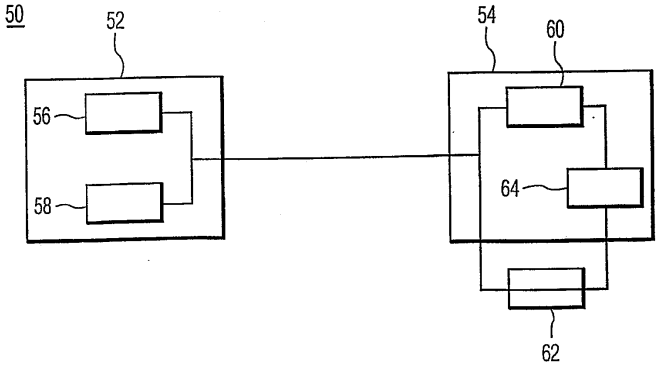
도면1



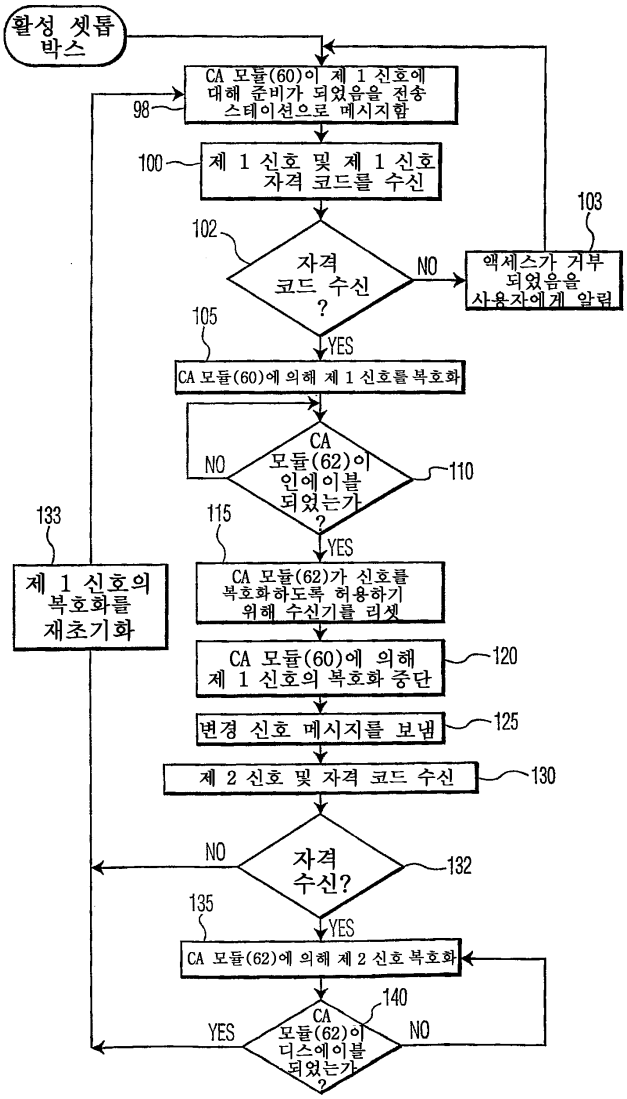
도면2



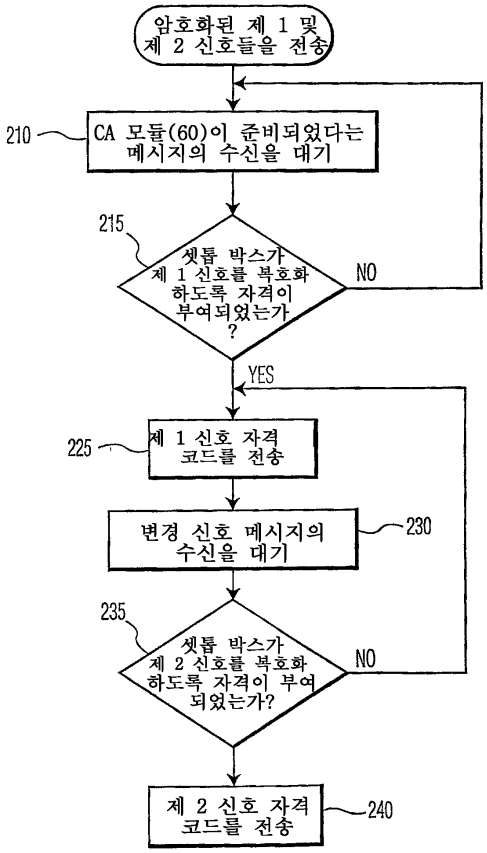
도면3



도면4


활성 셋톱 박스
CA 모듈(60)이 제 1 신호에 대해 준비가 되었음을 전송 스테이션으로 메시지함
98
제 1 신호 및 제 1 신호 자격 코드를 수신
100
자격 코드 수신 ?
102
NO
액세스가 거부 되었음을 사용자에게 알림
103
YES
CA 모듈(60)에 의해 제 1 신호를 복호화
105
CA 모듈(62)이 인에이블 되었는가 ?
110
NO
YES
CA 모듈(62)가 신호를 복호화하도록 허용하기 위해 수신기를 리셋
115
CA 모듈(60)에 의해 제 1 신호의 복호화 중단
120
변경 신호 메시지를 보냄
125
제 2 신호 및 자격 코드 수신
130
자격 수신?
132
NO
YES
135
CA 모듈(62)에 의해 제 2 신호 복호화
CA 모듈(62)이 디스에이블 되었는가 ?
140
YES
NO
제 1 신호의 복호화를 재초기화
133

도면5


암호화된 제 1 및 제 2 신호들을 전송
210
CA 모듈(60)이 준비되었다는 메시지의 수신을 대기
215
셋톱 박스가 제 1 신호를 복호화 하도록 자격이 부여되었는가 ?
NO
YES
225
제 1 신호 자격 코드를 전송
변경 신호 메시지의 수신을 대기
230
235
셋톱 박스가 제 2 신호를 복호화 하도록 자격이 부여 되었는가?
NO
제 2 신호 자격 코드를 전송
240