(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04N 7/167 (2006.01)

(45) 공고일자 2007년01월22일
(11) 등록번호 10-0672983
(24) 등록일자 2007년01월16일

(21) 출원번호	10-2000-7003623	(65) 공개번호	10-2001-0030925
(22) 출원일자	2000년04월03일	(43) 공개일자	2001년04월16일
심사청구일자	2003년08월26일		
번역문 제출일자	2000년04월03일		
(86) 국제출원번호	PCT/IB1998/001610	(87) 국제공개번호	WO 1999/18729
국제출원일자	1998년10월02일	국제공개일자	1999년04월15일

(81) 지정국 국내특허 : 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아 헤르체고비나, 바베이도스, 불가리아, 브라질, 벨라루스, 캐나다, 스위스, 중국, 쿠바, 체코, 독일, 덴마크, 에스토니아, 스페인, 핀란드, 영국, 그루지야, 헝가리, 이스라엘, 아이슬랜드, 일본, 케냐, 키르키즈스탐, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 리베이라, 레소토, 리투아니아, 룩셈부르크, 라트비아, 몰도바, 마다가스카르, 마케도니아공화국, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 슬로베니아, 슬로바키아, 타지키스탄, 투르크맨, 터어키, 트리니아드토바고, 우크라이나, 우간다, 미국, 우즈베키스탄, 베트남, 폴란드, 포르투칼, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 인도, 가나, 감비아, 짐바브웨, 세르비아 앤 몬테네그로,

AP ARIPO특허 : 케냐, 레소토, 말라위, 수단, 스와질랜드, 우간다, 가나, 감비아, 짐바브웨,

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르키즈스탐, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크맨,

EP 유럽특허 : 오스트리아, 벨기에, 스위스, 독일, 덴마크, 스페인, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴, 핀란드, 사이프러스,

OA OAPI특허 : 부르키나파소, 베닌, 중앙아프리카, 콩고, 코트디브와르, 카메룬, 가봉, 기니, 말리, 모리타니, 니제르, 세네갈, 차드, 토고,

(30) 우선권주장

97402322.8	1997년10월02일	유럽특허청(EPO)(EP)
98401388.8	1998년06월09일	유럽특허청(EPO)(EP)
98401389.6	1998년06월09일	유럽특허청(EPO)(EP)

(73) 특허권자
까날 + (쏘시에떼 아노님)
프랑스공화국 빠리 께 앙드레 씨뜨로엥 85/89

(72) 발명자
메일라드, 미쳴
프랑스, 에프 78120 람보우일렛, 애버뉴 듀 파크, 13

(74) 대리인
최홍순
조성욱
박세걸
특허법인세신

심사관 : 변형철

전체 청구항 수 : 총 4 항

(54) 암호화된 데이터 스트림 전송 방법 및 장치

(57) 요약

본 발명은 스크램블링된 데이터가 디코더(2020)로 전송되는 스크램블링된 데이터의 전송 및 수신 방법에 관한 것이며, 스크램블링된 데이터는 디코더(2020)에 삽입되는 보안 모듈 또는 스마트 카드(3020)로 보내져 디스크램블링되며, 스크램블링된 데이터 스트림은 스마트 카드(2020)로부터 암호화된 형태로 디코더(3020)로 다시 보내진다. 데이터 스트림의 암호화는 카드(2020)에서 실행되거나 또는 전송시에 제 2 암호화 단계로서 실행될 수도 있다. 데이터 스트림은 보안 모듈에서 디스크램블링된 시청각 데이터에 또는 전송물을 디스크램블링하도록 디코더에 의하여 연속적으로 사용되는 컨트롤 워드 데이터의 스트림에 상응한다.

대표도

도 4

특허청구의 범위

청구항 1.

디코더가 스크램블링된 데이터 스트림을 수신하여 상기 디코더에 삽입된 휴대형 보안 모듈로 보내고, 상기 휴대형 보안 모듈가 상기 스크램블링된 데이터 스트림을 디스크램블링하는, 스크램블링된 데이터 스트림 수신 방법으로서,

상기 데이터 스트림은 암호화된 형태로 상기 보안 모듈로부터 상기 디코더로 보내지고, 상기 디코더는 상기 암호화된 데이터 스트림을 복호화하여 사용하고, 상기 데이터 스트림은 제 1 암호화 키의 등가물을 사용하여 암호화를 위해 상기 디코더로 되돌아가기 전에 상기 제 1 암호화 키에 의하여 상기 보안 모듈에서 암호화되는 것을 특징으로 하는 스크램블링된 데이터 스트림 수신 방법.

청구항 2.

삭제

청구항 3.

삭제

청구항 4.

삭제

청구항 5.

삭제

청구항 6.

삭제

청구항 7.

삭제

청구항 8.
삭제

청구항 9.
삭제

청구항 10.
삭제

청구항 11.
삭제

청구항 12.
삭제

청구항 13.
삭제

청구항 14.
삭제

청구항 15.
삭제

청구항 16.
삭제

청구항 17.
삭제

청구항 18.
삭제

청구항 19.
삭제

청구항 20.
삭제

청구항 21.
삭제

청구항 22.

디코더 및 상기 디코더에 삽입된 휴대형 보안 모듈을 포함하는 디코더와 휴대형 보안 모듈 결합 장치로서,

상기 디코더는 스크램블링된 데이터 스트림을 수신하여 상기 휴대형 보안 모듈로 보내고, 상기 휴대형 보안 모듈은 상기 디코더로부터의 상기 스크램블링된 데이터 스트림을 디스크램블링하고 상기 디스크램블링된 데이터 스트림을 암호화하여 상기 디코더로 보내고, 상기 디코더는 상기 휴대형 보안 모듈로부터의 상기 암호화된 데이터 스트림을 복호화하여 사용하는 것을 특징으로 하는 디코더와 휴대형 보안 모듈 결합 장치.

청구항 23.

전송된 스크램블링된 데이터 스트림을 수신하여 휴대형 보안 모듈로 보내는 디코더로서,

상기 휴대형 보안 모듈에 의해 암호화된 데이터 스트림으로서 상기 스크램블링된 데이터 스트림을 상기 휴대형 보안 모듈로부터 수신하는 제1 수단; 및

상기 제1 수단에 의해 수신된 상기 암호화된 데이터 스트림을 복호화하여 사용하는 제2 수단을 포함하는 디코더.

청구항 24.

디코더와 상호 동작하는 휴대형 보안 모듈로서,

상기 디코더로부터 스크램블링된 데이터 스트림을 수신하여 디스크램블링하는 제1 수단; 및

상기 제1 수단으로부터의 상기 디스크램블링된 데이터 스트림을 암호화하고 상기 암호화된 데이터 스트림을 상기 디코더로 보내는 제2 수단을 포함하는 휴대형 보안 모듈.

명세서

기술분야

본 발명은 암호화되거나 또는 스크램블링(scrambled)된 전송, 예를 들어 스크램블링된 텔레비전 방송으로 사용하기 위한 방법 및 장치에 관한 것이다.

배경기술

암호화된 데이터의 전송은 유료 TV 시스템의 분야에서 널리 공지되어 있으며, 스크램블링된 시청각 정보는 통상 위성을 통하여 다수의 가입자들에게 방송되며, 각 가입자는 연속적인 시청을 위하여 전송된 프로그램을 디스크램블링(descramble)할 수 있는 디코더 또는 수신기/디코더를 소유한다.

전형적인 시스템에 있어서, 스크램블링된 데이터는 데이터를 디스크램블링하기 위한 컨트롤 워드와 함께 전송되며, 컨트롤 워드 자체는 소위 이용 키(exploitation key)에 의하여 암호화되어 암호화된 형태로 전송된다. 그런 다음, 스크램블링된 데이터 및 암호화된 컨트롤 워드는 디코더에 삽입된 스마트 카드에 저장된 이용 키의 등가물에 대한 억세스를 갖는 디코더에 의해 수신되어, 암호화된 컨트롤 워드를 복호하고 나서 전송된 데이터를 디스크램블링한다. 납입을 끝낸 가입자는 전송물 시청하기 위해 암호화된 컨트롤 워드를 복호하는데 필요한 이용키를 매달 ECM(권리부여 제어 메시지, Entitlement Control Message)에 수신한다.

시스템의 보안성을 향상시키기 위해, 컨트롤 워드는 통상 매 10초마다 또는 그렇게 변화된다. 이러한 것은 컨트롤 워드가 대중적으로 공지될 수도 있는 경우에 컨트롤 워드를 정적 또는 느리게 변화시키는 상황을 피하게 한다. 이러한 상황에서, 부정한 사용자가 전송물을 디스크램블링하기 위해 부정한 사용자의 디코더 상의 디스크램블링 유닛에 공지된 컨트롤 워드를 공급하는 것이 비교적 간단하게 된다.

이러한 보안상의 한계에도 불구하고, 예를 들어 방송 필름이 공지되는 동안 컨트롤 워드의 스트림이 전송되는 문제가 최근에 발생하였다. 이러한 정보는 비디오 레코더에 스틸-스크램블링된 필름을 기록하였던 어떠한 승인되지 않은 사용자에 의하여 사용될 수도 있다. 컨트롤 워드의 스트림이 디코더로 공급되는 것과 동시에 필름이 재생되면, 필름의 시각화가 가능하게 된다. 사용자가 컨트롤 워드와 필름을 동기화하면, 특히 디스크램블러를 만드는데 필요한 하드웨어 요소들이 용이하게 얻어지기 때문에 이러한 사기를 실행하는데 큰 기술적인 문제는 없다.

이러한 문제는 인터넷의 증대로 악화되었으며, 현재 주어진 전송동안 발산되는 컨트롤 워드의 스트림을 공표하는 특정 수의 인터넷 사이트들을 찾는 것은 드문 것이 아니다.

본 발명의 목적은 상기된 바와 같은 공격에 대항할 수 있는 안전한 디코더 구성을 제공하도록 스크램블링된 전송물들을 위한 공지된 종래 기술과 연관된 문제들을 문제들을 극복하는데 있다.

본 발명에 의하면, 스크램블링된 데이터 스트림이 디코더로 전송되고, 그런 다음 디코더에 삽입된 휴대형 보안 모듈로 전송되어, 휴대형 보안 모듈에 의하여 디스크램블링되며, 데이터 스트림이 보안 모듈로부터 암호화된 형태로 디코더로 보내져, 디코더에 의하여 복호되어 연속적으로 사용되는 것을 특징으로 하는 스크램블링된 데이터 스트림의 전송 및 수신 방법이 제공된다.

상기된 바와 같은 종래의 시스템에서, 컨트롤 워드는 이용 키에 의하여 암호화되어, 전송물을 디스크램블링하기 위하여 복호된 형태로 디코더에 있는 컨트롤 유닛으로 전송되기 전에 디코더로부터 복호용 스마트 카드로 전송된다. 스마트 카드와 디코더 사이의 접속을 결정하고 이러한 접속을 따라서 통과하는 컨트롤 워드 정보를 기록하는 것이 비교적 용이하기 때문에, 이러한 기술에서의 약점은 스마트 카드와 디코더 유닛 사이에서“보통문으로(in clear)”컨트롤 워드가 전송되는 것에 있다.

이러한 약점을 확인하고, 데이터가 암호화된 형태로 디코더로 되돌아가기 전에 휴대형 보안 모듈에 의하여 디스크램블링되는 해결 수단을 가지는 것에 의하여, 본 발명은 이러한 기술로 문제점들을 해결한다.

발명의 상세한 설명

본 발명의 제 1 형태의 실현에 의하면, 데이터 스트림은 제 1 암호화 키의 등가물을 사용하여 복호하기 위한 디코더로 되돌아가기 전에 제 1 키에 의해 보안 모듈에서 암호화된다. 그러나, 아래에 기술되는 바와 같이, 데이터가 보안 모듈로부터 디코더로 암호화된 형태로 전송되지만 암호화는 전송 레벨에서 발생하는, 본 발명의 다른 실현이 가능하다.

상기 실현의 하나의 실시예에서, 데이터 스트림은 디코더 식별값에 따라서 변하는 제 1 암호화 키에 의하여 보안 모듈에서 암호화되고, 디코더는 키의 등가물 및 데이터를 암호화하는데 필요한 값을 가진다. 예를 들어, 디코더 식별값은 디코더의 시리얼 또는 배치(batch) 번호에 일치할 수 있다.

디코더 식별값은 보안 모듈 및 송신기로서 알려진 개별화 키(personalized key)에 의하여 암호화될 수도 있으며, 디코더 식별값은 보안 모듈로 전송하는 디코더로 암호화된 형태로 전송된다. 보안 모듈 내에서 개별화 키에 의하여 암호화되면, 디코더 식별값 및 제 1 암호화 키는 보안 모듈에 의하여 암호화된 데이터 스트림을 생성하는데 사용될 수 있다.

보안 모듈로의 디코더 식별값의 전송은 디코더로부터 보안 모듈로 보내지는 신호를 반드시 수반하게 된다. 알 수 있는 바와 같이, 이러한 채널들을 가로지르는 메시지의 전송은 모니터링하는 것이 비교적 용이하고, 그러므로 판독할 수 없는 형태로 식별값을 보안 모듈로 전송하는 것이 바람직하다.

이러한 형태의 개별화 키들은 EMMs 또는 권리부여 관리 메시지(Entitlement Management Messages)에 관련하여 공지되었으며, 이는 필요한 개별화 키를 가지는 선택된 가입자 또는 가입자 그룹에 그 달의 ECM을 복호하기 위한 관리 키를 암호화된 형태로 매달 전송하여, EMM을 복호한다.

또 다른 해결 수단에서, 디코더 식별값은 보안 모듈로 공지된 개별화 키에 의하여 암호화될 수도 있으며, 암호화된 디코더 식별값은 디코더에 보안 모듈을 삽입하는 제조시에 보안 모듈로 전송하기 위한 디코더에 저장된다.

확정된 디코더 식별값의 사용에 대한 대안으로서, 제 1 암호화 키는 디코더에 의해 발생되어 보안 모듈로 전송되는 난수 또는 유사 난수에 좌우될 수도 있다.

바람직하게, 디코더와 보안 모듈 사이의 암호화되지 않은 데이터의 전송에 관련된 문제의 관점에서, 난수는 디코더와 보안 모듈 사이에서 또는 그 역으로 전송되기 전에 제 2 암호화 키에 의하여 암호화된다.

하나의 실시예에 있어서, 난수는 디코더에서 발생되어 제 2 암호화 키에 의하여 암호화되고, 보안 모듈에 저장된 이 제 2 키의 등가물에 의하여 복호하기 위한 보안 모듈로 전송된다.

대안적인 실시예에 있어서, 보안 모듈 및 디코더의 동작은 간단하게 역전되어서, 난수는 보안 모듈에서 발생되어 제 2 키에 의하여 암호화되고, 디코더에 저장된 제 2 키의 등가물에 의하여 복호하기 위한 디코더로 전송된다.

상기에서 주어진 예들에서, 제 1 및 제 2 암호화 키, 개별화 보안 모듈 키 등은 DES, RC2 등과 같이 공지된 대칭 암호화 알고리즘에 따라서 모두 생성될 수도 있다. 그러나, 디코더가 난수 발생을 책임지는 바람직한 실시예에서, 난수를 암호화하는데 사용되는 제 2 키는 공개키에 해당되고, 보안 모듈은 난수 값을 복호화하는데 필요한 등가의 개인키가 구비된다.

스마트 카드와 같은 휴대형 보안 모듈과 비교되는 바와 같이, 제 1 및 제 2 암호화 키를 저장하는데 사용되는 디코더에 있는 하드웨어 부품(전형적으로 ROMs)은 부착된 접점 등의 수단에 의하여 격리하여 모니터링하는 것이 비교적 용이하다.

그러므로, 전용된 부정 사용자는 보안 모듈 및 디코더 사이의 통신을 모니터링함으로써 제 1 및 제 2 키들과, 난수의 암호화된 값을 얻을 수도 있다. 대칭 알고리즘이 제 2 키를 위해 사용되면, 난수는 공개된 디코더 제 2 키로 복호되어, 컨트롤 워드를 복호하기 위해 공개된 제 1 키로 공급될 수도 있다.

대조적으로, 공개키/개인키 구조의 사용을 통해, 디코더에 의해 소유되는 제 2 공개키의 소유는 부정 사용자가 암호화된 난수를 복호하지 못하게 할 수 있다. 난수가 발생되어 디코더의 RAM에 저장되어, 어떠한 경우에 규정 원리에서 변화할 수 있기 때문에, 직접 난수를 얻는 것이 항상 가능한 한편, 이러한 것은 키들을 얻어 전송된 암호화된 값을 픽업하는 것과 비교하여 보다 어려운 것이다.

바람직하게, 제 2 개인 키는 보안 모듈에만 있는 것이다. 이 실시예는 보안 모듈과 디코더 사이에서 전송된 데이터 스트림이 어떠한 경우에도 그 기간동안 발생된 난수에 좌우되는 것을 알 수 있을지라도 시스템 보안을 증가시킨다.

상기된 바와 같이, 제 2 암호화 키에 관련하여 공개/개인키 구조의 사용은 개인키가 보안 모듈에 저장되고, 공개키가 디코더에 저장되는 경우에 특히 유익하다. 그러나, 대안적인 실시예에 있어서, 상황이 역전되어서 개인키가 디코더에 의해 소유되며, 공개키가 보안 모듈에서 유지된다.

바람직하게, 제 2 디코더 키는 디코더로 전송되기 전에 제 3 키에 의하여 암호화되고, 디코더는 제 2 디코더 키를 복호화하여 확인하기 위해 대응하는 제 3 키를 소유한다.

특히 바람직한 실시예에서, 제 2 디코더 키를 복호화하는데 사용된 제 3 키는 개인키이며, 디코더는 전송된 제 2 키를 암호화하여 확인하기 위해 등가의 공개키를 소유한다.

제 1 형태의 실현의 상기 모든 실시예에서, 데이터 스트림은 디코더로 보내지기 전에 보안 모듈에 의해 소유되는 제 1 암호화 키에 의하여 다시 암호화된다.

상기된 바와 같이, 대안적인 형태의 실현에서, 보안 모듈과 디코더 사이에서 전송된 암호화된 데이터 스트림은 보안 모듈의 상향스트림에 준비된다. 이러한 실현에서, 데이터 스트림은 제 1 암호화 키에 의해 전송 지점에서 암호화되고, 이 키의 등가물에 의하여 디코더에서 복호화된다.

바람직한 실시예에서, 데이터 스트림은 송신기 및 디코더로 알려진 변수에 따라서 제 1 암호화 키에 의해 전송 지점에서 암호화되고, 이 키 및 변수의 등가물에 의하여 디코더에서 복호화된다.

예를 들어, 데이터 스트림은 전송의 실시간 및/또는 날짜에 따라 제 1 암호화 키에 의해 전송 지점에서 암호화될 수도 있다. 이러한 경우에, 암호화된 데이터 스트림은 단지 방송의 전송 시간에서의 함수이며, 디코더의 복호키(또는 변수에 관련된 것이라 할 수 있는)가 변화되었기 때문에, 방송이 기록된 후에 디코더의 디스크램블러로 공급될 수 없다.

예측할 수 있는 바와 같이, 이러한 실현이 상기된 제 1 실현의 실시예들보다 덜 안전한 한편, 존재하는 보안 모듈의 하드웨어에 대한 변화가 필요없다는 이점을 가진다. 더욱이, 본 발명을 이행하는데 필요한 디코더 및 송신기의 변경은 디코더인 경우에, 예를 들어 전송된 데이터를 다운로드하는 것에 의하여 소프트웨어에서 이행될 수 있다.

이러한 제 2 형태의 실현에서, 암호화된 데이터 스트림은 전송 지점에서 이용 키에 의하여 더욱 암호화되고, 보안 모듈에 있는 등가의 이용 키에 의하여 복호화되어, 제 1 암호화된 형태로 디코더에 보내질 수 있다.

상기의 모든 실시예에서 기술된 바와 같이, 보안 모듈과 디코더 사이에서 암호화된 형태로 보내진 데이터 스트림은 시청각 데이터를 포함할 수도 있다. 이러한 실시예에서, 데이터 스트림의 복호 후에, 디코더는 시청각 데이터를 간단하게 디스플레이하게 된다.

그러나, 대안적인 실시예에서, 보안 모듈과 디코더 사이에서 암호화된 형태로 보내진 데이터 스트림은 컨트롤 워드 스트림을 포함할 수도 있으며, 복호화된 컨트롤 워드 스트림은 그 후에 관련된 스크램블링된 시청각 데이터를 디스크램블링하도록 디코더에서 사용된다.

이 실시예에서, 상기된 바와 같은 컨트롤 워드 스트림의 "스크램블링" 및 "디스크램블링"은 종래의 시스템에서와 같이 이용 키를 사용한 ECM 메시지들의 암호화 및 복호화에 해당된다.

시스템의 보안성을 증가시키기 위하여, 상기된 실시예들의 어느 하나 또는 모두는 서로 조합하여 이행될 수도 있다.

본 발명은 특히 텔레비전 방송의 전송에 적용할 수 있다. 본 발명은 또한 상기된 바와 같은 전송 방법에 적합한 디코더 및 보안 모듈로 확장한다.

"휴대형 보안 모듈"이라는 용어는 마이크로프로세서 및/또는 메모리 저장부를 가지는 종래의 칩에 근거된 휴대형 카드 형태의 디바이스를 의미하도록 사용된다. 이러한 것은 스마트 카드, PCMCIA 카드, SIM 카드 등을 포함한다. 종종 TV 디코더 시스템들에서 사용되는 것과 같은 키 형상 디바이스와 같은 대안적인 물리적 형태를 가지는 칩 디바이스가 이러한 용어에 포함된다.

"스크램블링된", "암호화된", "컨트롤 워드"및 "키"라는 용어들은 말의 명료성의 목적을 위하여 다수의 방식으로 여기에서 사용된다. 그러나, "스크램블링된 데이터"와 "암호화된 데이터"또는 "컨트롤 워드"와 "키" 사이에서 근본적인 구별이 만들어지지 않는다는 것을 알 수 있을 것이다.

유사하게, 설명은 "수신기/디코더"와 "디코더"로 언급하였지만, 다른 기능을 통합하는 물리적으로 별개인 디코더 유닛, 텔레비전, 기록 장치 등과 같은 다른 장치와 통합되는 디코더 유닛과 비교하여 기능하는 디코더 유닛에 대해 디코더와 통합되는 수신기를 가지는 실시예에 본 발명이 적용할 수 있다는 것을 알 수 있을 것이다.

실시예

디지털 텔레비전 시스템

본 발명에 적합한 디지털 텔레비전 방송 및 수신 시스템(1000)의 전체 구성이 도 1에 도시되어 있다. 시스템은 압축된 디지털 신호를 전송하도록 공지된 MPEG-2 압축 시스템을 사용하는 통상적인 종래 평범한 디지털 텔레비전 시스템(2000)을 포함한다. 보다 상세하게, 방송 센터에 있는 MPEG-2 압축기(2002)는 디지털 신호 스트림(전형적으로 화상 신호 스트림)을 수신한다. 멀티플렉서(2004)는 다수의 추가 입력 신호들을 수신하고 하나 이상의 이송 스트림으로 조합하여 압축된 디지털 신호를 링크(2010)를 통해 방송 센터의 송신기(2008)로 전송하며, 여기서 물론 링크(2010)는 원격 통신 링크를 포함하는 다양한 형태를 취할 수 있다. 송신기(2008)는 업링크(2012)를 경유하여 전자기 신호들을 트랜스폰더(2014)로 전송하고, 전자기 신호들은 관념상의 다운 링크(2016)를 경유하여 통상 단말 사용자가 소유하거나 대여한 접시 안테나의 형태로 하는 지상 수신기(2018)로 보내져 방송된다. 지상 수신기(2018)에 수신된 신호들은 단말 사용자가 소유하거나 대여하였으며 단말 사용자의 텔레비전(2022)에 접속된 수신기/디코더(2020)로 전송된다. 수신기/디코더(2020)는 압축된 MPEG-2 신호를 텔레비전 세트(2022)를 위한 텔레비전 신호로 복호한다.

조건부 억세스 시스템(3000)은 멀티플렉서(2004) 및 수신기/디코더(2020)에 접속되며, 부분적으로 방송 센터에 그리고 부분적으로 디코더에 위치된다. 조건부 억세스 시스템(3000)은 단말 사용자가 하나 이상의 방송 공급자로부터의 디지털 텔레비전 방송에 억세스할 수 있게 된다. 상업적 제공(즉, 방송 공급자에 의해 판매된 하나 또는 수 개의 텔레비전 프로그램들)에 관계하는 메시지를 복호화할 수 있는 스마트 카드는 수신기/디코더(2020)에 삽입될 수 있다. 디코더(2020) 및 스마트 카드를 사용하여 단말 사용자는 예약 모드 또는 유료 시청 모드로 이벤트를 구매할 수도 있다.

또한, 멀티플렉서(2004) 및 수신기/디코더(2020)에 접속되고 부분적으로 방송 센터에 그리고 부분적으로 디코더에 위치되는 쌍방향 시스템(4000)은 단말 사용자가 모뎀 백 채널(modemmed back channel; 4002)을 경유하여 다양한 애플리케이션과 상호 작용하도록 할 수 있다.

조건부 억세스 시스템

도 2를 참조하여, 조건부 억세스 시스템(3000)은 가입자 승인 시스템(3002, SAS, Subscriber Authorization System)을 포함한다. SAS(3002)는 각각의 TCP-IP 링크(3006, 비록 다른 형태의 링크들이 대안적으로 사용될지라도)에 의하여 하나 이상의 가입자 관리 시스템(3004, SMS, Subscriber Management System, 하나의 SMS는 각 방송 공급자를 위한 것이다)에 연결된다. 대안적으로, 하나의 SMS는 2개의 방송 공급자들 사이에서 공유되거나 하나의 공급자가 2개의 SMS를 사용할 수 있다.

"머더(mother)"스마트 카드(3010)를 이용하여 암호 기입 유닛(3008)의 형태로 하는 제 1 암호화 유닛은 링크(3012)에 의하여 SAS에 연결된다. 머더 스마트 카드(3016)를 이용하여 암호 기입 유닛(ciphering unit; 3014)의 형태로 하는 제 2 암호화 유닛은 링크(3018)에 의하여 멀티플렉서(2004)에 연결된다. 수신기/디코더(2020)는 "도터(daughter)"스마트 카드(3020)를 수용한다. 이것은 모뎀 백 채널(4002)을 경유하여 통신 서버(3022)에 의하여 SAS(3002)에 직접 연결된다. SAS는 요청에 의해 그 중에서 도터 스마트 카드에 대한 예약 권리를 보낸다.

스마트 카드들은 하나 이상의 상업적 오퍼레이터들의 비밀 번호를 수용한다. "머더"스마트 카드는 상이한 종류의 메시지를 암호화하고, "도터"스마트 가트는 이것들이 그렇게 하는 권리를 가지면 메시지를 복호화한다.

제 1 및 제 2 암호 기입 유닛(3008,3014)들은 랙, 20개의 전자 카드들 및 각 전자 카드에 대한 스마트 카드(3010,3016)까지 EEPROM에 저장된 소프트웨어를 가지는 전자 VME 카드를 포함하며, 스마트 카드(3016)는 ECM을 암호화하기 위한 것이며 스마트 카드(3010)는 EMM을 암호화하기 위한 것이다.

멀티플렉서 및 스크램블러

도 1 및 도 2를 참조하여, 방송 센터에서, 디지털 화상 신호는 먼저 MPEG-2 압축기(2002)를 사용하여(또는 감소된 비트율로) 먼저 압축된다. 이 압축된 신호는 다른 압축 데이터와 같은 다른 데이터와 멀티플렉싱되기 위하여 링크(2006)를 경유하여 멀티플렉서 및 스크램블러(2004)로 전송된다.

스크램블러는 스크램블링 처리에 사용되며 멀티플렉서(2004)에 있는 MPEG-2 스트림에 포함되는 컨트롤 워드(CW)를 발생시킨다. 컨트롤 워드(CW)는 초기에 발생되며, 단말 사용자의 통합된 수신기/디코더(2020)가 프로그램을 디스크램블링할 수 있게 한다. 프로그램이 어떻게 상업화되는지를 지시하는 접근 기준이 또한 MPEG-2 스트림에 더해진다. 프로그램은 다수의 "가입"모드들중 하나 및/또는 다수의 "유료 시청(PPV, Pay Per View))"모드들 또는 이벤트들중 하나로 상업화될 수 있다. 가입 모드에서, 단말 사용자는 하나 이상의 상업적 제공"부케(bouquests)"에 가입하며, 그러므로 이러한 부케들 내에 있는 모든 채널을 시청할 권리를 취한다. 바람직한 실시예에서, 960개까지의 상업적 제공들이 한 부케의 채널들로부터 선택될 수도 있다. 유료 시청 모드에서, 단말 사용자는 그가 원하는 것과 같은 이벤트들을 구매하는 능력을 구비한다. 이러한 것은 미리 이벤트를 예약하거나 이것이 방송되자 마자이벤트를 구매하는 것("충동 모드")에 의하여 달성될 수 있다.

컨트롤 워드(CW) 및 접근 기준 모두는 권리부여 제어 메시지(ECM, Entitlement Control Message)를 만들도록 사용되고; 이러한 것은 하나의 스크램블링된 프로그램과 관련하여 보내진 메시지이다. 메시지는 컨트롤 워드(프로그램의 디스크램블링을 위하여 허용하는) 및 방송 프로그램의 접근 기준을 포함한다. 접근 기준 및 컨트롤 워드들은 링크(3018)를 경유하여 제 2 암호화 유닛(3014)으로 전송된다. 이러한 유닛에서, ECM이 발생되고 이용 키(Cex)로 암호화되어, 멀티플렉서 및 스크램블러(2004)로 전송된다.

프로그램 전송

멀티플렉서(2004)는 SAS(3002)로부터 암호화된 EMM, 제 2 암호화 유닛(3014)으로부터 암호화된 ECM, 및 압축기(2002)로부터 압축된 프로그램들을 포함하는 전자 신호들을 수신한다. 멀티플렉서(2004)는 프로그램들을 스크램블링하

고 스크램블링된 프로그램, 암호화된 EMM(존재하면), 암호화된 ECM을 전자 신호로서 링크(2010)를 경유하여 방송 센터의 송신기(2008)로 전송한다. 송신기(2008)는 업링크(2012)를 경유하여 트랜스폰더(2014)를 향하여 전자기 신호들을 전송한다.

프로그램 수신

트랜스폰더(2014)는 송신기(2008)에 의하여 전송된 전자기 신호들을 수신하고 처리하여, 다운링크(2016)를 경유하여 단말 사용자가 소유하거나 대여한 형태로 하는 지상 수신기(2018)로 신호를 전송한다. 수신기(2018)에 수신된 신호들은 단말 사용자가 소유하거나 대여하였으며 단말 사용자의 텔레비전 세트(2022)에 연결된 통합 수신기/디코더(2020)로 전송된다. 수신기/디코더(2020)는 암호화된 EMM 및 암호화된 ECM으로 스크램블링된 프로그램들을 얻도록 신호들을 디멀티플렉싱한다.

프로그램이 스크램블링되지 않으면, 수신기/디코더(2020)는 데이터를 압축해제하여, 신호들을 텔레비전 세트(2022)로 전송을 위한 화상 신호로 변형시킨다.

프로그램이 스크램블링되면, 수신기/디코더(2020)는 MPEG-2 스트림으로부터 대응하는 ECM을 추출하여 ECM을 단말 사용자의 "도터"스마트 카드(3020)로 보낸다. 이것은 수신기/디코더(2020)에 있는 하우징에 배열한다. 도터 스마트 카드(3020)는 단말 사용자가 ECM을 암호화하여 프로그램에 접근하는 권리를 가지는지를 제어한다. 그러하지 않으면, 프로그램이 디스크램블링될 수 없는 것을 지시하도록, 네거티브 상태가 수신기/디코더(2020)로 보내진다. 단말 사용자가 그러한 권리를 가지면, ECM가 복호화되어 컨트롤 워드가 추출된다. 디코더(2020)는 이러한 컨트롤 워드를 사용하여 프로그램을 디스크램블링할 수 있다. MPEG-2 스트림이 압축해제되어 텔레비전(2022)에 대한 화상 신호 전진 전송(video signal onward transmission)으로 전환된다.

가입자 관리 시스템(SMS)

가입자 관리 시스템(3004, SMS)은 다른 것들 중에서 단말 사용자의 파일, 상업적 제공(운임표 및 선전용 팜플렛과 같은), 예약, PPV 명세서, 및 단말 사용자의 소비 및 승인 모두를 관리하는 데이터 베이스(3024)를 포함한다. SMS는 물리적으로 SAS로부터 떨어져 있을 수도 있다.

각 SMS(3004)는 단말 사용자에게 전송되는 권리부여 관리 메시지(EMM)에 대한 변경 또는 생성을 할 수 있도록 각 링크(3006)를 경유하여 SAS(3002)로 메시지를 전송한다.

SMS(3004)는 또한 EMM의 변경 또는 생성을 하지 않으며 단지 단말 사용자의 상태에서의 변화(제품을 주문할 때 단말 사용자에 부여되는 승인 또는 단말 사용자에게 청구되는 금액에 관한)를 부과하는 SAS(3002)로 메시지를 전송한다.

권리부여 관리 메시지 및 권리부여 제어 메시지

ECM, 즉 권리부여 제어 메시지들은 전송된 프로그램의 데이터 스트림에 삽입되는 암호화된 메시지들이며, 이는 프로그램을 디스크램블링하는데 필요한 컨트롤 워드를 포함한다. 주어진 수신기/디코더의 승인은 EMM 또는 권리부여 관리 메시지에 의하여 제어되고 덜 빈번한 근거상에 전송되며, 이는 ECM을 복호화하는데 필요한 이용 키를 구비하는 승인된 수신기/디코더를 공급한다.

EMM은 개개의 단말 사용자(가입자) 또는 일정 그룹의 단말 사용자들에게 제공되는 메시지이다. 하나의 그룹은 주어진 수의 단말 사용자들을 포함한다. 하나의 그룹으로서 이러한 조직은 대역폭을 최적화하는 것을 목적으로 하고; 즉, 하나의 그룹에 대한 억세스는 다수의 단말 사용자들의 도달을 허용할 수 있다.

다양한 특정 형태의 EMM이 사용될 수도 있다. 개개의 EMM들은 개개의 가입자들에게 제공되며, 전형적으로 유료 시청 서비스의 준비에 사용된다. 소위 "그룹"가입자 EMM들은 256인의 개개의 사용자들의 그룹에 제공되며, 전형적으로 일부 예약 서비스의 관리에 사용된다. 이러한 EMM은 그룹 식별자 및 가입자의 그룹 비트맵을 가진다.

보안상의 이유 때문에, 암호화된 ECM에 끼워지는 컨트롤 워드(CW)는 평균 매 10초 또는 그 정도로 변화한다. 대조적으로, ECM을 복호화하도록 수신기에 의해 사용되는 이용 키(Cex)는 EMM의 수단에 의하여 매달 변화된다. 이용 키(Cex)는

스마트 카드에 기록된 가입자 또는 그룹 가입자들의 신분에 대응하는 특정인에 대한 키를 사용하여 암호화된다. 가입자가 업데이트된 이용 키(Cex)를 수신하도록 선택된 사람들중 하나이면, 카드는 특정 월의 이용 키(Cex)를 얻도록 이 개별화 키를 사용하여 메시지를 복호화하게 된다.

EMM 및 ECM의 동작은 당업자에게 널리 공지된 것이며, 여기에서 보다 상세하게 설명되지 않는다.

스마트 카드에 의한 데이터 스트림의 암호화

도 3 및 도 4를 참조하여, 본 발명의 제 1 실현의 다수의 실시예들이 기술된다. 도 3에 도시된 바와 같이, 스크램블링된 시청각 데이터 스트림은 수신기/디코더(2020)에 의해 수신되고, 복호화된 컨트롤 워드(CW)를 발생시켜 전송물을 디스크램블링하기 위해 카드에 의해 소유된 이용 키(Cex)를 사용하여 3030에서 디스크램블링되는 휴대형 보안 모듈로 보내진다. 알 수 있는 바와 같이, 본 발명에서, 전송물의 디스크램블링은 휴대형 보안 모듈에서 완전하게 실행되며, 이것은 스마트 카드, PCMCIA 카드 등을 포함한다.

디코더로 다시 보내지기 전에, 데이터 스트림은 3031에서 제 1 암호화 키(Kf)에 따라서 다시 암호화된다. 제 1 암호화 키(Kf)의 동작은 디코더의 확인, 예를 들어 디코더의 시리얼 넘버와 연관된 디코더 확인값(N)에 좌우된다. 이 값(N)은 암호화된 EMM의 수단에 의하여 카드로 전송되고 수신기/디코더 시스템의 초기화 스테이션으로 전송되어 지점(3032)에서 복호화하기 위해 디코더(2020)에 의해 카드(3020)로 보내진다.

모든 EMM에 대한 것으로서, 확인값(N)을 포함하는 EMM은 카드에 의해 소유되며 메시지의 송신기에 의하여 공개된 키에 대응하는 개별화 키에 의하여 암호화되며, 이것은 그 카드 또는 카드 그룹이 암호화된 EMM을 복호화할 수 있게 한다.

대안적인 실시예에서, 초기화하는 EMM은 디코더의 메모리에 미리 저장되어 카드의 첫 번째 삽입시에 카드에 보내지거나, 또는 각 시간마다 디코더는 켜지게 된다. 후자의 경우에, 카드는 단지 이를 수신하는 처음에만 초기화 EMM을 수용하도록 프로그램된다. 다시, 전송된 EMM에 대한 것으로서, 카드와 관련된 개별화 키는 전송된 값을 암호화하고 복호화하도록 사용된다.

디코더(2020)를 참조하여, 이것은 또한 키(Kf), 확인 또는 시리얼 번호(N)가 구비된다. 키(Kf)와 번호(N)는 예를 들어 디코더의 ROM에 저장될 수도 있다. 키(Kf)와 확인값(N)을 사용하여, 디코더는 디스크램블링된 데이터 스트림을 복호화한다. 실제로, 확인값은 고정될 필요가 없으며, 이것이 필요하다고 판정되면 간단하게 카드 내에 저장된 확인값(N)을 재프로그램할 수 있다.

이 실시예에서, 키(Kf)는 주어진 값에 의하여 다양화될 수 있는 키를 생성하기 위하여 어떠한 공지된 대칭키 알고리즘을 사용하여 간단하게 생성될 수 있다(상기 예에서의 확인값(N)과 같이). 공개/개인키 페어링(pairing) 또한 생각할 수 있으며, 공개키는 디코더와 관련되며, 개인키는 스마트 카드와 관련된다. 종래의 시스템에서와 같이, 이용 키 및 개별화 키는 대칭형 알고리즘에 의해 생성될 수도 있다.

알 수 있는 바와 같이, 데이터 스트림은 단지 암호화 및 스크램블링된 형태로 카드와 디코더 사이에서 전송되어, 본원의 서두에 기술된 부정한 형태의 위험을 감소시킨다. 더욱이, 이 실시예에서, 카드와 디코더 사이의 모든 통신은 실제로 암호화되어 시스템의 보안성을 증가시킨다.

상기 실시예에서, 3030에서 복호화되어 3031에서 다시 암호화된 데이터 스트림은 시청각 데이터에 상응한다. 대안적인 실시예에서, 데이터 스트림은 컨트롤 워드 데이터의 스트림에 상응하고, ECM의 복호화는 3031에서 다시 암호화된 컨트롤 워드 스트림을 생성하도록 3030에서 수행되어 디코더로 전송된다. 디코더에 의해 복호화된 컨트롤 워드 스트림은 그런 다음 컨트롤 워드 스트림과 관련되어 스크램블링되어 전송된 시청각 데이터를 디스크램블링하도록 디코더에 의해 사용된다.

이러한 실시예의 이점은 시청각 데이터의 흐름을 처리하고 디스크램블링에 대한 전기 회로가 보안 모듈에서보다는 오히려 디코더 내에서 구체화되며, 이것은 단지 컨트롤 워드 스트림의 복호화 및 재 암호화를 취급한다.

도 3의 시스템의 하나의 결점은 비록 사소한 것은 아니지만 디코더의 ROM으로부터 키(Kf)와 확인값(N)의 추출이 너무 어려움없이 수행될 수도 있다는 것이다. 도 4의 실시예는 이러한 어려움을 극복한다.

도시된 바와 같이, 난수 또는 유사 난수(RN)는 3040에서 디코더 내에서 생성되어 RSA와 같은 적절한 공개/개인키의 공개키(Kpub)에 의하여 3041에서 연속적인 암호화를 위해 보내진다. 대응하는 개인키(Kpri)는 스마트 카드에 의해 소유된다. 암호화된 난수(p(RN))는 그럼 다음 암호화된 난수 값(p(RN))을 3042에서 복호화하도록 개인키(Kpri)를 사용하는 스마트 카드로 보내진다.

이전의 실시예에서의 확인값(N)으로서, 값(RN)은 암호화되고 카드로부터 디코더로 보내지는 데이터 스트림을 얻도록 디스크램블링된 데이터 스트림의 대칭키(Kf)에 의한 암호화로 3031에서 사용된다. 디코더로부터 스마트 카드로의 원래의 디스크램블링된 데이터 스트림의 통신은 디코더로부터 도면을 간단하게 하기 위하여 여기에서 생략되었다.

디코더의 한 측부에서, 암호화된 값의 데이터 스트림은 대칭키(Kf)와 난수 값(RN)을 사용하여 3033에서 복호화된다. 이전의 실시예의 확인값(N)과는 달리, 난수 값(RN)은 디코더의 RAM에 저장되어 빈번하게 변화하는 값이며 비교적 확인하는데 어려울 수 있다. 공개키(Kpub) 및 대칭키 값은 장치에서 보다 영구적인 형태로 저장되며 덜 안전하다. 그러나, 승인되지 않은 사용자가 이러한 키 및 암호화된 값(p(RN))들을 얻도록 관리하는 경우조차도, 개인, 공개키 알고리즘의 특성 때문에 이러한 정보로부터 데이터 스트림을 복호화하는데 필요한 RN값을 생성하는 것이 가능하지 않으며, 컨트롤 워드의 보안성은 손상되지 않는다.

동일한 공개/개인키 쌍이 일련의 디코더 및 카드들을 위하여 사용될 수 있다. 그러나, 보안성의 레벨은 스마트 카드와 관련된 독특한 공개/개인키 쌍의 사용으로 증가될 수 있다.

도시된 바와 같이, Kpub 및 Kpri의 값들은 3050에서 도시된 시스템 오퍼레이터에 의하여 생성되어 스마트 카드(3020)에 삽입된다. 그런 다음, Kpub의 값은 디코더에서 스마트 카드의 삽입 순간에 디코더로 전송된다. 개인키(Kpri)가 난수 값(RN)을 암호화하도록 사용되기 때문에, 디코더가 이 키의 기원을 입증하도록, 즉 부정한 사용자에 속하는 공개키의 수신에 응답하여 디코더가 정보를 전송하는 것을 방지하는데 사용되는 것은 중요하다.

이러한 목적을 위하여, 공개키(Kpub)는 3051에서 도시되고 오퍼레이터에 대해 독특한 개인키(KeyG)에 의하여 암호화되고, 그런 다음 Kpub를 수용하는 인증서가 3052에서 스마트 카드(3020)로 전송되어 저장된다. 디코더에서 카드의 삽입순간에, 3054에 저장된 등가의 공개키(KeyG)를 사용하여 디코더에 의해 복호화되어 인증된다. 그러므로, 얻어진 Kpub의 값은 연속적인 암호화 단계들을 위하여 사용되게 된다.

3030에서 암호화되고 3031에서 재 암호화되는 데이터 스트림이 시청각 데이터에 관계하여 기술되었지만, 이것은 컨트롤 워드 데이터의 스트림에 동일하게 일치한다. 상기 실시예서와 같이, 컨트롤 워드를 포함하는 ECM이 3030에서 복호화되고 디코더로 전송을 위하여 3031에서 다시 암호화된다. 3033에서 얻어진 복호화된 컨트롤 워드 데이터는 그런 다음 관련된 시청각 데이터 스트림을 디스크램블링하기 위해 디코더에 의해 사용된다.

송신기에서의 데이터 스트림의 암호화

상기 실시예들은 카드로부터 디코더로 전송된 데이터 스트림의 암호화가 스마트 카드 자체에서 실행되는 본 발명의 제 1 형태의 실현에 관한 것이다. 다음의 실시예에서, 대안적인 실현은 암호화가 송신기에서 추가의 상향스트림을 실행하는 도 5를 참조하여 기술된다. 명백하게 되는 바와 같이, 이것은 데이터 스트림의 종래의 암호화 또는 스크램블링에 추가되는 것이다.

도 5는 송신기(2008), 스마트 카드(3020) 및 디코더(2020) 사이에서 본 실시예에서의 정보 흐름을 나타낸다. 명백한 것으로서, 이 도면은 설명을 단순화하기 위하여 송신기와 스마트 카드 사이에서 직접 전송되는 정보를 도시하였지만, 스마트 카드에 의해 수신된 어떠한 신호들도 수신기/디코더 유닛을 경유하여 수신되어 카드로 전송될 것이다. 유사하게, 송신기가 이 경우에 하나의 기능적 블록으로 나타났지만, 전송된 메시지의 암호화는 도 1 및 도 2에 관계하여 기술된 바와 같은 시스템의 별개의 요소들에 의하여 실시될 수도 있다.

이 실시예에서, 시청각 데이터 스트림은 암호 키(Kt)에 의하여 암호화되고, 이것의 추출값은 전송물의 실시간 및/또는 날짜와 같은 시스템의 모든 요소로 공지된 포괄적 변수(t)에 좌우된다. 암호화된 데이터(f(DATA)는 그럼 다음 종래의 시스템에서와 같이 컨트롤 워드와, 디코더(2020) 내에서 보안 모듈(3020)로 전송되어 통신되는 결과적인 암호화되어 스크램블링되는 데이터에 의하여 3051에서 스크램블링된다. 스크램블링된 데이터는 보안 모듈에 의하여 3020에서 디스크램블링된다.

존재하는 시스템과는 달리, 데이터는 여전이 암호화된 형태(f(DATA)로 있게 되며, 이 형태로 지점(3052)에서 복호화를 위해 디코더(2020)로 보내진다. 디코더(2020)는 또한 키(Kt)의 등가물을 가지며, 시간 및/또는 날짜와 같은 포괄적으로 이용가능한 정보가 사용되면, 값(t)를 소유하게 된다. 데이터는 그런 다음 디코더에 의해 복호화되어 처리된다.

변화하는 포괄적인 변수를 사용하여, 전송 순간에 사용할 수 있는 제어 스트림이 미래의 시간/날짜에 디코더에 의해 사용될 수 없기 때문에, 시스템은 카드/디코더 통신을 모니터링하는 것에 의하여 얻어진 암호화된 제어 스트림(f, CW)의 어떠한 기록도 미래에 승인되지 않은 사용자에 의하여 사용될 수 있는 문제를 제거한다. 대조적으로, 포괄적인 변수가 송신기/디코더 사이에서 이러한 변수의 전송을 명시하지 않는 수단을 선택한다는 사실이 필요하다.

상기된 실시예에서, 보안 모듈(3020)은 첫 번째의 디스크램블링 단계에 필요한 컨트롤 워드 데이터를 얻도록 ECM 데이터(도시되지 않음)를 암호화하는 이용 키를 사용하여, 암호화되고 스크램블링된 폭 넓은 데이터를 실행한다.

대안적인 실시예에서, 도 5에 도시된 단계들은 이용 키(Cex)를 이용하여 한 번 암호화된 워드 데이터를 3051에서 암호화하고, 등가의 이용 키를 사용하여 카드(3020)에서 첫 번째 복호화를 실행한 후에, 명확한 형태로 컨트롤 워드 데이터를 얻도록 값(t)을 사용하여 3052에서 두 번째 복호화를 실행함으로써 컨트롤 워드 데이터 자체에서 실행될 수도 있다. 이것은 그런 다음 디코더에 의해 수신된 관련 스크램블링된 시청각 데이터를 디스크램블링하도록 사용될 수도 있다.

이전의 실시예들보다 덜 안전하지만, 이러한 형태의 시스템은 새로운 스마트 카드를 생성하는 어떠한 필요성없이 존재하는 시스템에서 간단하게 이행되며 디코더 및 송신기 유닛에 필요한 변경이 재프로그래밍에 의해 유도될 수도 있다는 이점을 가진다.

알 수 있는 바와 같이, 도 3 내지 도 5를 참조하여 기술된 모드 실시예들은 필요하다면 보안 레벨을 증가시키도록 별개로 또는 어떤 조합으로 이행될 수도 있다.

도면의 간단한 설명

본 발명의 다수의 실시예들이 첨부된 도면을 참조하여 단지 예의 방식으로 기술된다.

도 1은 본 발명에 의해 적합할 수도 있는 공지된 디지털 텔레비전 시스템의 전체적인 구조를 도시한 도면;

도 2는 도 1의 텔레비전 시스템의 조건부 억세스 시스템을 도시한 도면;

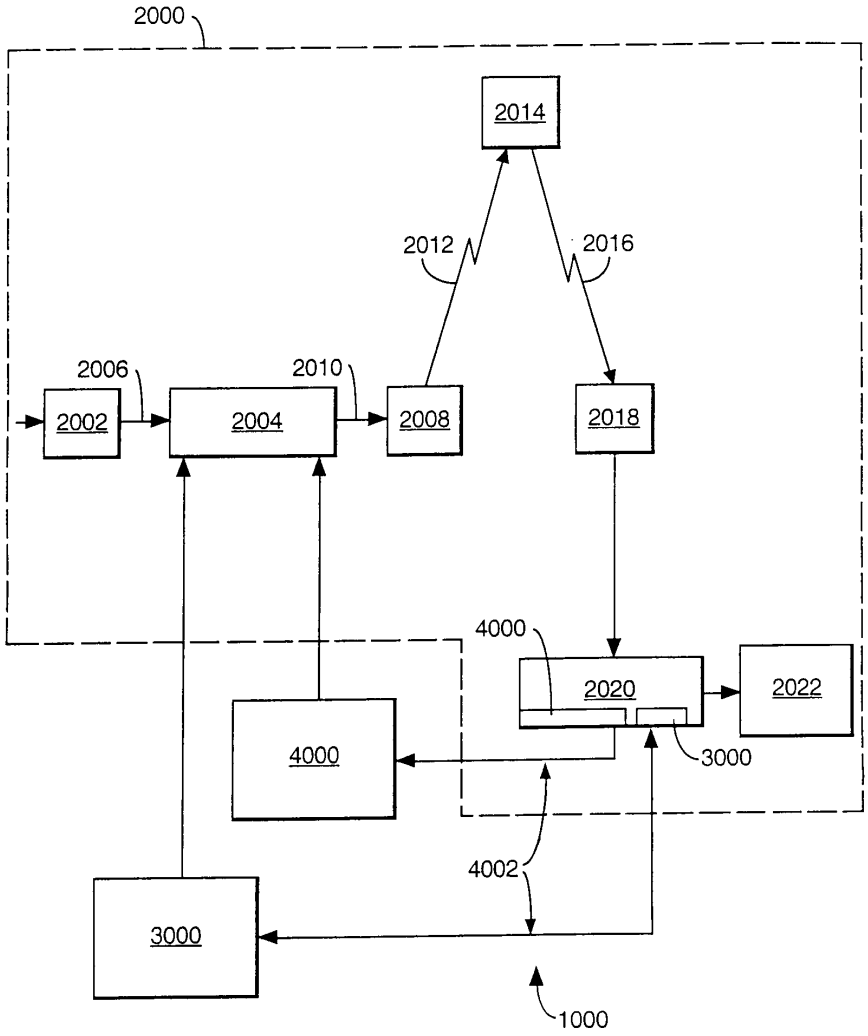
도 3은 본 발명의 제 1 실시예를 도시한 도면;

도 4는 본 발명의 제 2 실시예를 도시한 도면; 및

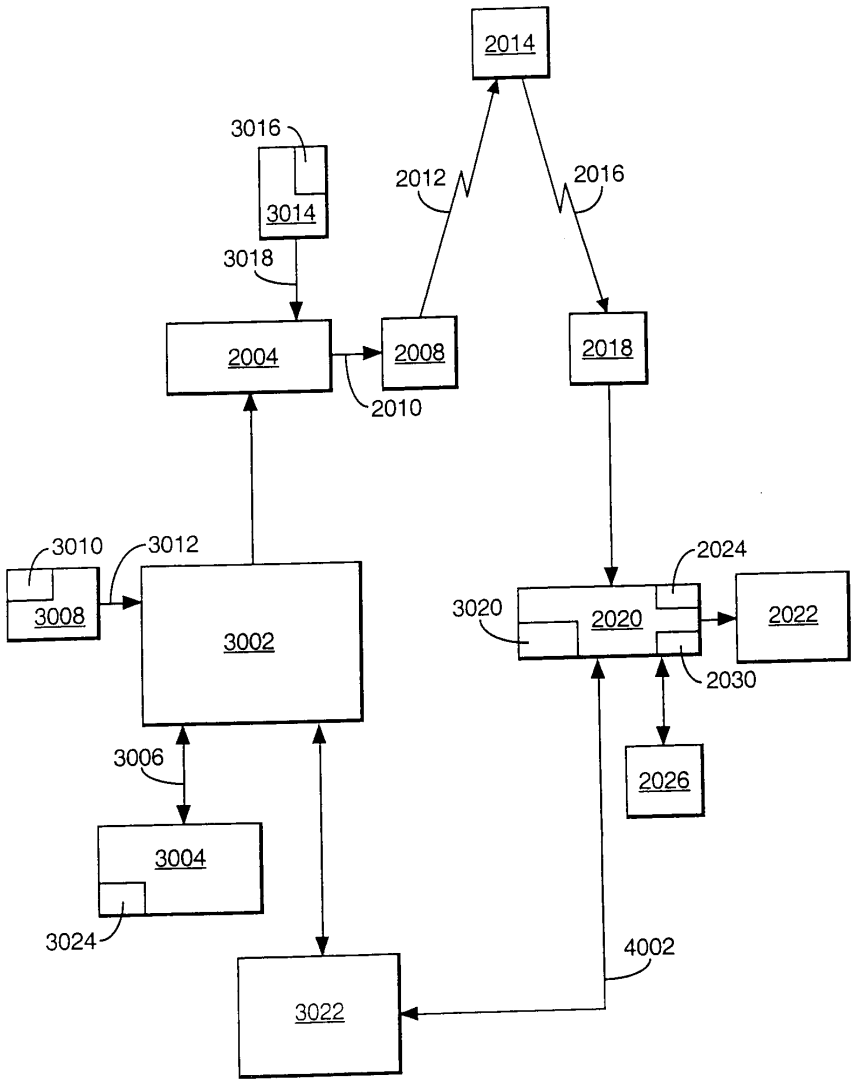
도 5는 본 발명의 제 3 실시예를 도시한 도면이다.

도면

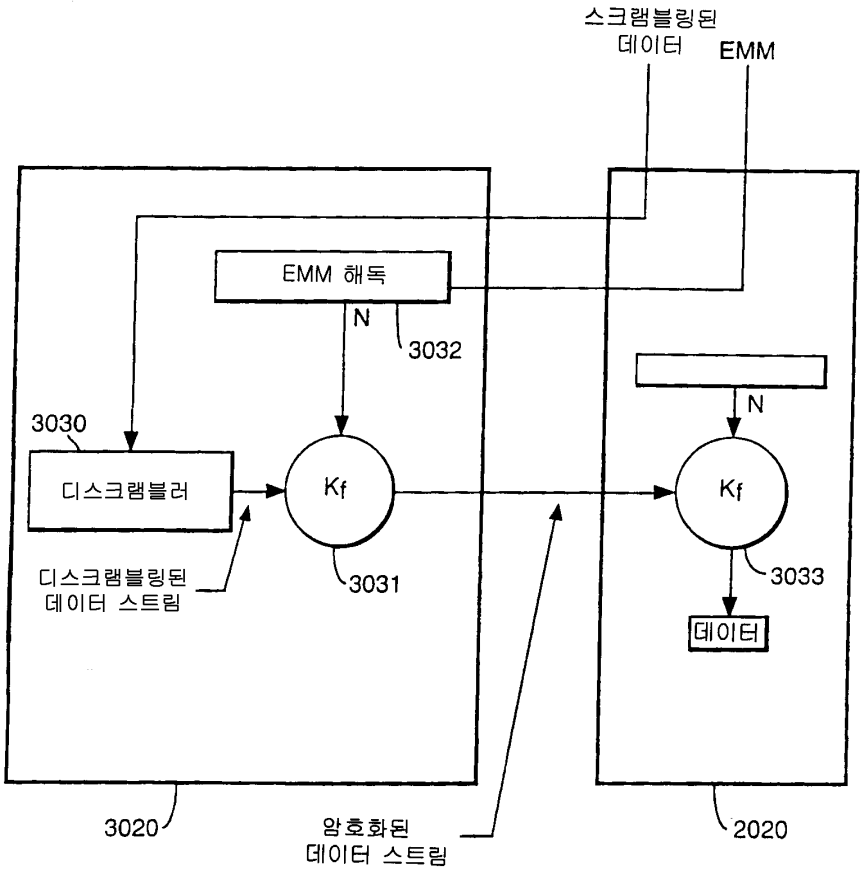
도면1


2000
2014
2012
2016
2006
2010
2002
2004
2008
2018
4000
2020
2022
4000
3000
4002
3000
1000

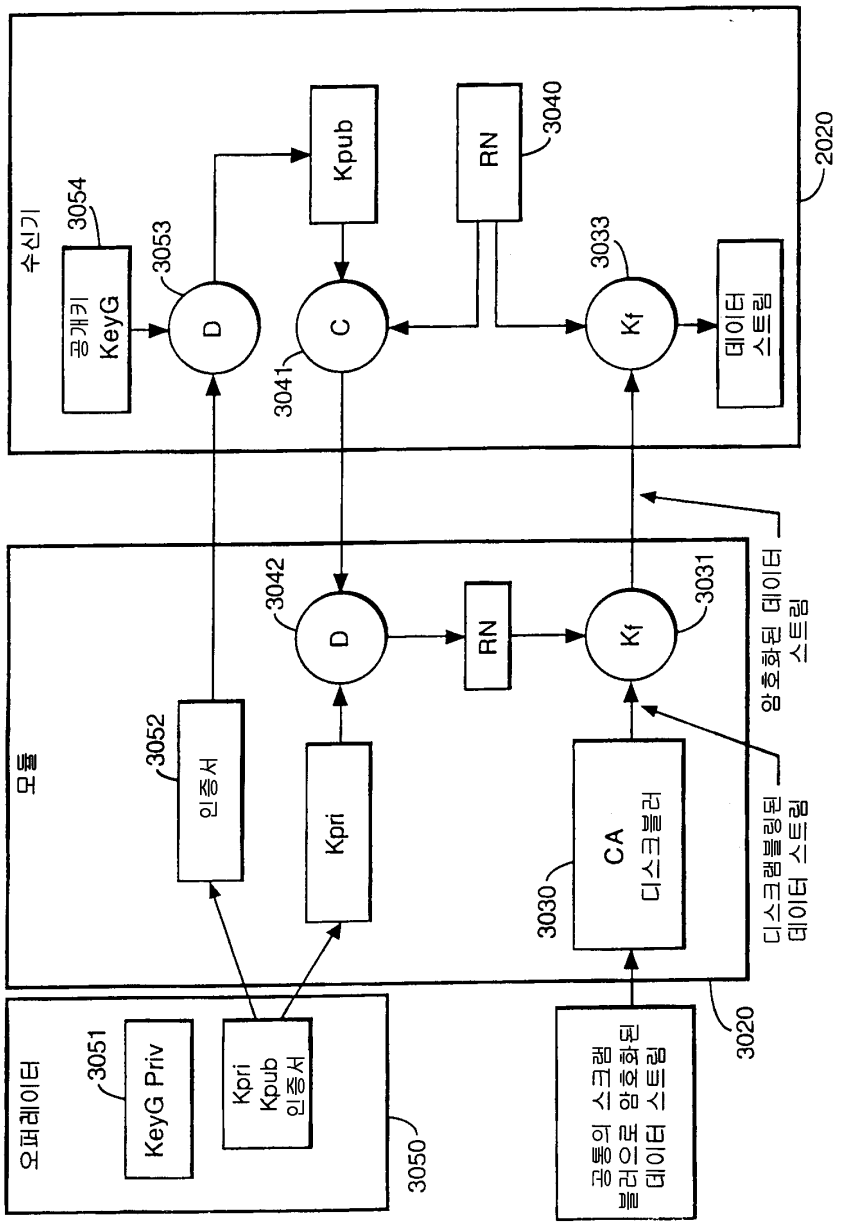
도면2


2014
3016
3014
2012
2016
3018
2004
2008
2018
2010
3010
3012
3008
3002
2024
3020
2020
2022
2030
3006
2026
3004
3024
4002
3022

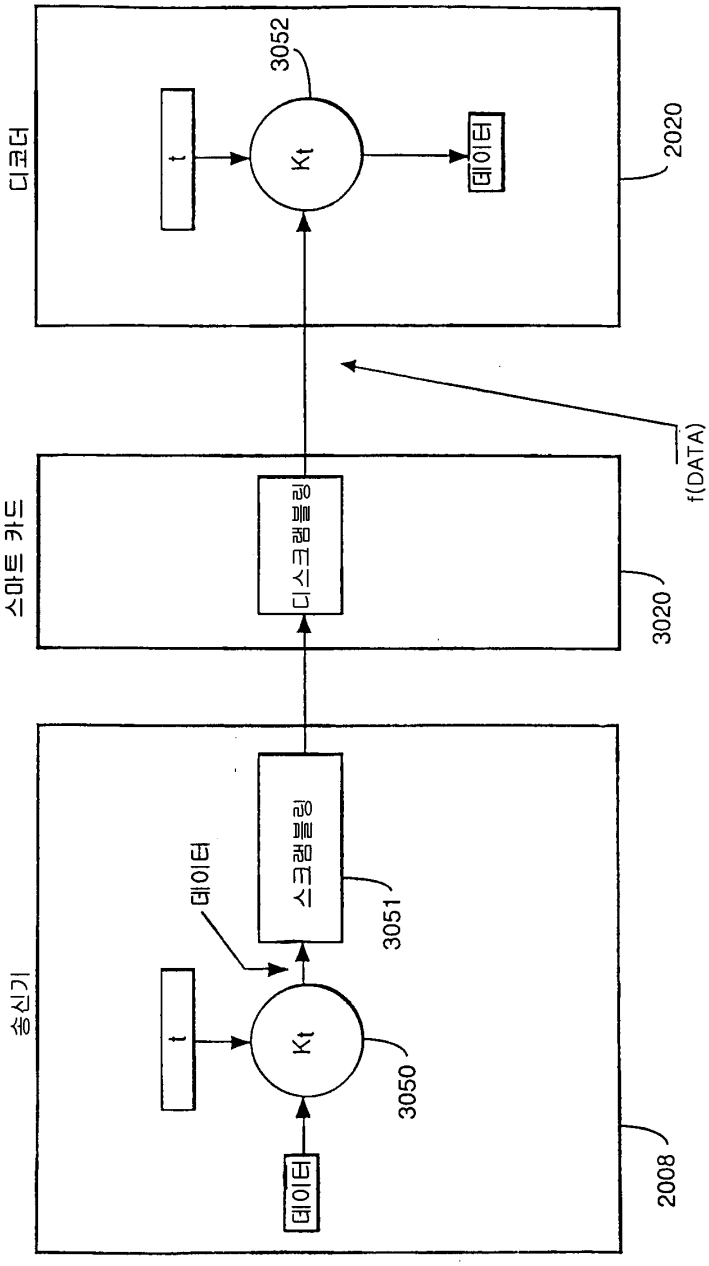
도면3


스크램블링된
데이터
EMM
EMM 해독
N
3032
3030
디스크램블러
Kf
디스크램블링된
데이터 스트림
3031
N
Kf
3033
데이터
3020
암호화된
데이터 스트림
2020

도면4


수신기
3054
공개키 KeyG
3053
D
Kpub
RN
3040
C
3041
Kf
3033
데이터 스트림
2020
모듈
3042
D
RN
Kf
3031
3052
인증서
Kpri
3030
CA 디스크블러
암호화된 데이터 스트림
디스크램블링된 데이터 스트림
오퍼레이터
3051
KeyG Priv
Kpri Kpub 인증서
3050
공통의 스크램블러 암호화된 데이터 스트림
3020

도면5


디코더
t
Kt
3052
데이터
2020
f(DATA)
스마트 카드
디스크램블링
3020
송신기
데이터
t
Kt
3050
스크램블링
3051
데이터
2008