(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년01월13일
(11) 등록번호 10-0936458
(24) 등록일자 2010년01월05일

(51) Int. Cl.
H04N 5/913 (2006.01) *H04N 7/167* (2006.01)
H04N 7/16 (2006.01)
(21) 출원번호 10-2004-7013193
(22) 출원일자 2003년02월21일
심사청구일자 2008년02월20일
(85) 번역문제출일자 2004년08월24일
(65) 공개번호 10-2004-0088530
(43) 공개일자 2004년10월16일
(86) 국제출원번호 PCT/FR2003/000582
(87) 국제공개번호 WO 2003/073760
국제공개일자 2003년09월04일
(30) 우선권주장
02/02329 2002년02월25일 프랑스(FR)
(56) 선행기술조사문헌
WO0200056068 A1
EP0858184 A
WO0200062505 A1
전체 청구항 수 : 총 5 항

(73) 특허권자
톰슨 라이센싱
프랑스 에프-92100 블로뉴-빌랑꾸르 꿰 아 르 갤로 46
(72) 발명자
뒤랑, 알랭
프랑스 에프-3500 렌느 뤼 드 디낭 79
르리에브르, 씰벵
프랑스 에프-35000 렌느 뤼 드 베른 69
로랑, 크리스토프
프랑스 에프-35630 비뇨끄 뤼 데 프레쉬 3
(74) 대리인
백만기, 전경석, 주성민

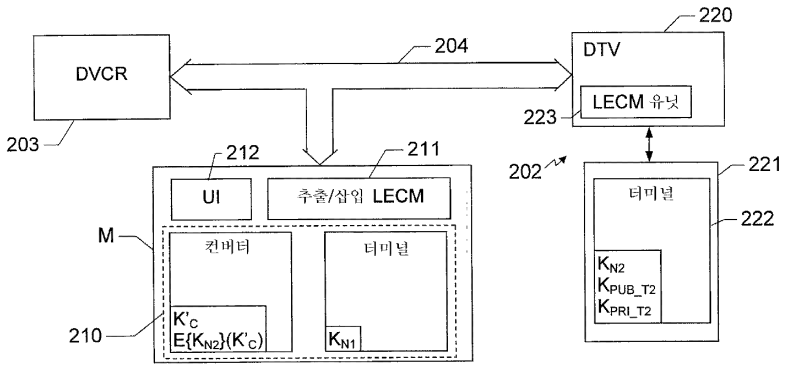
심사관 : 구대성

(54) 제1 도메인용으로 암호화한 데이터를 제2 도메인에 속한네트워크에서 처리하기 위한 디바이스 및 그 데이터를전송하는 방법

(57) 요 약

본 발명은, 제1 도메인에 특정된 인코딩 프로세스로부터 인코딩된 데이터를 수신하기 위하여 제2 도메인의 네트워크로의 접속을 위한 처리 디바이스에 관한 것으로서, 디코딩된 데이터를 얻기 위해 상기 제1 비밀 키를 이용하여 인코딩된 데이터를 디코딩하는 수단, 제2 도메인에 특정된 인코딩 프로세스에 따라 상기 디코딩된 데이터를 인코딩하는 수단을 포함하고, 상기 인코딩 수단에 의해 제공된 상기 인코딩된 데이터는 제2 도메인에 특정된 제2 비밀 키(K_{N2})를 이용하지 않고서는 디코딩될 수 없다. 본 발명은 또한 제1 도메인에 특정된 비밀 키를 이용하여 제2 도메인의 네트워크에서 인코딩된 데이터를 전송하는 방법과 관한 것이다.

대 표 도



특허청구의 범위

청구항 1

제1 도메인에 특정된 암호화 방법에 따라 암호화된 데이터(LECM1)를 수신하기 위하여 제2 도메인에 속하는 네트워크에 접속되도록 되어 있는 데이터 처리 디바이스로서,

- 상기 제1 도메인에 특정된 제1 비밀 키(K_{N1})를 내포하는 메모리;

- 해독된 데이터를 얻기 위해 상기 제1 비밀 키(K_{N1})를 이용하여 상기 암호화된 데이터(LECM1)를 해독하는 수단; 및

- 상기 제2 도메인에 특정된 암호화 방법에 따라 상기 해독된 데이터를 암호화하는 수단을 포함하고, 상기 암호화 수단에 의해 암호화된 데이터는 상기 제2 도메인에 특정된 제2 비밀 키(K_{N2})를 이용하여 해독 가능한, 데이터 처리 디바이스.

청구항 2

제1항에 있어서,

- 제1 대칭 키(K'_C)와, 상기 제2 도메인에 특정된 제2 비밀 키(K_{N2})를 이용한 상기 제1 대칭 키의 암호화($E\{K_{N2}\}(K'_C)$)를 내포하는 메모리-상기 암호화 수단은 상기 제1 대칭 키(K'_C)를 이용하여 해독된 데이터의 암호화를 수행함-와;

- 상기 암호화 수단에 의해 암호화된 데이터($E\{K'_C\}(CW)$) 및 상기 제2 도메인에 특정된 제2 비밀 키(K_{N2})를 이용한 상기 제1 대칭 키의 암호화($E\{K_{N2}\}(K'_C)$)를 상기 네트워크에서 방송하는 수단을 더 포함하는 것을 특징으로 하는 데이터 처리 디바이스.

청구항 3

청구항 3은(는) 설정등록료 납부시 포기되었습니다.

제1항에 있어서,

상기 제1 도메인에 특정된 제1 비밀 키(K_{N1})와 상기 제2 도메인에 특정된 제2 비밀 키(K_{N2})는 각각 대칭 키인 것을 특징으로 하는 데이터 처리 디바이스.

청구항 4

청구항 4은(는) 설정등록료 납부시 포기되었습니다.

제2항에 있어서,

- 단명 마스킹 키(ephemeral masking key)(R)를 발생하는 수단과;

- 마스킹된 데이터(MCW)를 형성하기 위해 상기 마스킹 키(R)를 이용하여 해독된 데이터를 마스킹하는 수단-상기 마스킹된 데이터는 상기 제1 대칭 키(K'_C)를 이용하여 상기 암호화 수단에 의해 암호화됨-과;

- 상기 방송 수단에 의해 방송된 데이터를 미리 수신한, 상기 네트워크에 접속된 프리젠테이션 디바이스에 의한 인증 동작에 응답하는 수단-상기 인증 동작에 대한 응답은 상기 단명 마스킹 키(R)를 포함함-을 더 포함하는 것을 특징으로 하는 데이터 처리 디바이스.

청구항 5

청구항 5은(는) 설정등록료 납부시 포기되었습니다.

제4항에 있어서,

단명 인증 키(K)-상기 단명 인증 키는 제1 대칭 키(K'_C)를 이용하여 상기 암호화 수단에 의해 상기 마스킹된 데이터(MCW)와 함께 암호화됨-를 발생하는 수단을 더 포함하며,

상기 인증 동작에 응답하는 수단은, 상기 인증 키, 및 상기 프리젠테이션 디바이스로부터 수신된 난수(R_i)의 함수로서 응답을 계산하는 것을 특징으로 하는 데이터 처리 디바이스.

청구항 6

청구항 6은(는) 설정등록료 납부시 포기되었습니다.

제2항에 있어서,

상기 디바이스에 의해 수신된 데이터(LECM1)는 "비공개(private) 복사 인증" 또는 "1회 복사만 인증" 유형의 복사 제어 정보를 내포하고,

상기 디바이스는 상기 복사 제어 정보를 "판독 전용" 유형의 다른 복사 제어 정보로 교체하는 수단을 포함하며,

상기 디바이스에 의한 데이터 방송은 상기 "판독 전용" 유형의 복사 제어 정보를 내포하는 것을 특징으로 하는 데이터 처리 디바이스.

청구항 7

제1 도메인에 특정된 제1 비밀 키(K_{N1})를 이용한 암호화 방법에 따라 암호화된 데이터(LECM1)를 제2 도메인에 속하는 네트워크에서 전송하는 방법으로서,

처리 디바이스에 대하여,

(a) 상기 네트워크에서 암호화된 데이터(LECM1)의 제1 방송(401)을 상기 네트워크에 접속되어 있는 제1 방송 디바이스(203, 503, 603)로부터 수신하는 단계와;

(b) 해독된 데이터를 얻기 위해 상기 처리 디바이스에 내포된 상기 제1 비밀 키(K_{N1})를 이용하여 상기 암호화된 데이터를 해독하는 단계와;

(c) 상기 처리 디바이스에 내포된 제1 대칭 키(K'_C)를 이용하여 상기 해독된 데이터를 암호화하는 단계와;

(d) 상기 제1 대칭 키를 이용하여 상기 단계 (c)에서 암호화된 데이터($E\{K'_C\}(CW)$), 및 상기 제2 도메인에 특정된 제2 비밀 키(K_{N2})를 이용한 상기 제1 대칭 키의 암호화($E\{K_{N2}\}(K'_C)$)-상기 암호화는 상기 제2 도메인의 디바이스에 의해 상기 처리 디바이스에 미리 전송됨-의 제2 방송(408)을 상기 네트워크에서 수행하는 단계를 포함하는 것을 특징으로 하는 데이터 전송 방법.

청구항 8

제7항에 있어서,

단계 (c)는, 상기 처리 디바이스에 대하여,

- 단명 마스킹 키(R)를 발생 및 저장하는 부단계(404)와;

- 마스킹된 데이터(MCW)를 형성하기 위해 상기 마스킹 키(R)를 이용하여 해독된 데이터를 마스킹하는 부단계(405)와;

- 상기 제1 대칭 키(K'_C)를 이용하여 상기 마스킹된 데이터를 암호화하는 부단계(406)를 포함하는 것을 특징으로 하는 데이터 전송 방법.

청구항 9

청구항 9은(는) 설정등록료 납부시 포기되었습니다.

제8항에 있어서,

단계 (c)는, 상기 처리 디바이스에 대하여,

- 단명 인증 키(K)를 발생 및 저장하는 부단계(404)와;

- 상기 단명 인증 키(K), 및 상기 마스킹된 데이터(MCW)를 상기 제1 대칭 키(K'_C)를 이용하여 암호화하는 부단계를 포함하고;

상기 데이터 전송 방법이, 단계 (d) 후에,

(f) 단계 (d)에서 방송 데이터를 미리 수신한, 상기 네트워크에 접속된 프리젠테이션 디바이스에 의한 인증 동작에 응답하는 단계(415)를 더 포함하며, 상기 인증 동작에 대한 응답은 상기 단명 마스킹 키(R)를 포함하는 것을 특징으로 하는 데이터 전송 방법.

청구항 10

청구항 10은(는) 설정등록료 납부시 포기되었습니다.

제9항에 있어서,

상기 인증 동작에 대한 응답은 상기 인증 키(K) 및 상기 프리젠테이션 디바이스로부터 수신된 난수(R_i)의 함수로서 계산(414)되는 것을 특징으로 하는 데이터 전송 방법.

청구항 11

청구항 11은(는) 설정등록료 납부시 포기되었습니다.

제7항에 있어서,

상기 제1 방송 중에 전송된 암호화 데이터는 "비공개 복사 인증" 또는 "1회 복사만 인증" 유형의 복사 제어 정보를 내포하고,

상기 데이터 전송 방법은, 상기 단계 (d) 전에, 상기 복사 제어 정보를 "판독 전용" 유형의 다른 복사 제어 정보로 교체하는 단계를 더 포함하는 것을 특징으로 하는 데이터 전송 방법.

청구항 12

제7항에 있어서,

-상기 처리 디바이스를 상기 제1 도메인에 속하는 네트워크에 접속시키는 단계와;

-상기 제1 도메인에 특정된 제1 비밀 키(K_{N1})를 상기 처리 디바이스에서 수신하는 단계로 이루어진 처리 디바이스 초기화 단계를 더 포함하고,

상기 제1 비밀 키는 상기 제1 도메인의 네트워크에 접속된 다른 디바이스에 의해 전송되는 것을 특징으로 하는 데이터 전송 방법.

청구항 13

청구항 13은(는) 설정등록료 납부시 포기되었습니다.

제12항에 있어서,

상기 초기화 단계는,

- 상기 처리 디바이스를 상기 제2 도메인에 속하는 네트워크에 접속시키는 단계를 더 포함하며;

상기 처리 디바이스에 대하여,

- 상기 제1 대칭 키(K'_C)를 발생하는 단계(100)와;

- 상기 제1 대칭 키(K'_C)를 상기 제2 도메인의 적어도 하나의 디바이스(202)에 보안 방식으로 전송하는 단계(104)와;

- 상기 제2 도메인에 특정된 제2 비밀 키를 이용한 상기 제1 대칭 키의 암호화($E\{K_{N2}\}(K'_C)$)를 상기 제2 도메인의 디바이스(202)로부터 수신하는 단계를 더 포함하는 것을 특징으로 하는 데이터 전송 방법.

명 세 서

기 술 분 야

<1> 본 발명은 특히 디지털 데이터가 디지털 도메스틱 네트워크(domestic network)와 같은 로컬 디지털 네트워크에서 유포될 때 그 디지털 데이터를 복사하는 것 및 그 데이터의 불법 액세스에 대한 보호 분야에 관한 것이다.

배 경 기 술

<2> 디지털 데이터의 불법 복사에 대한 보호와 관련하여, 디지털 콘텐츠를 정해진 도메인에서 사용하기 위해 복사할 수 있는 시스템이 공지되어 있다. 도메인은 예를 들면 하나의 동일한 도메스틱 네트워크에 속하는 한 세트의 설비를 의미하는 것으로 의도되고, 이러한 설비는 도메인에 특정된 비밀(secret), 예를 들면 암호화 키를 공유한다. 도메인에 속한 설비는 휴대형 설비일 수 있다. 특수 도메인의 멤버십은 그 특수한 도메인에 특정된 비밀을 아는 것에 의해 결정될 것이다.

<3> 그러한 도메인의 디지털 콘텐츠는 3가지로 분류될 수 있다.

<4> - "자유 복사"(free copy): 이 유형의 콘텐츠는 어느 도메인에서도 기록 또는 플레이(play)될 수 있어서, 이 유형의 콘텐츠를 판독하기 위해 도메인에 특정된 비밀을 알 필요가 없다;

<5> - "비공개 복사"(private copy): 이 유형의 콘텐츠는 그 콘텐츠를 다시 플레이할 수 있는 특수한 도메인에서만 복사할 수 있고; 이 콘텐츠는 다시 플레이할 수 있는 특수한 도메인의 비밀을 알고 있을 것을 요구하는 형태로 기록된다. 이 유형의 콘텐츠는 특수한 도메인에 속하지 않은 설비에서는 판독할 수 없다;

<6> - "판독 전용"(read only): 이 유형의 콘텐츠는 특수한 도메인에서 판독할 수만 있고 복사할 수 없다; 또는, 만일 콘텐츠의 복사가 이루어지면 그 콘텐츠는 그 후에 다시 플레이될 수 없다.

<7> 디지털 콘텐츠는 일반적으로 액세스 디바이스 또는 소스 디바이스를 통하여 도메인에 들어간다. 이 유형의 디바이스는 도메인 외부의 채널을 통하여 디지털 데이터를 검색하고, 그 디지털 데이터를, 예를 들면, 도메인의 다른 설비들을 접속하는 디지털 버스를 이용함으로써, 도메인의 다른 디바이스로 방송(broadcast)한다. 소스 디바이스는 특히 위성 안테나 또는 케이블 접속을 통해 디지털 도메스틱 네트워크의 외부로부터 비디오 프로그램을 수신하여 그 비디오 프로그램을 네트워크에서 방송하기 위한 디지털 디코더일 수 있다. 소스 디바이스는 또한 광디스크(이 경우에 디스크는 네트워크의 외부에서 생성된 데이터를 포함한다)에서 판독한 (오디오 및/또는 비디오) 데이터를 도메스틱 네트워크에서 방송하는 광디스크 드라이브일 수 있다.

<8> 도메인 내에서, 디지털 콘텐츠는 DVD("디지털 다기능 디스크") 레코더 또는 하드 디스크와 같은 디지털 기록 디바이스에 의해 기록될 수 있다.

<9> 마지막으로, 콘텐츠는 프리젠테이션 디바이스에 의해 도메인 사용자에게 제시된다. 이 디바이스들은 콘텐츠를 처리하고(특히 필요하다면 콘텐츠를 해독하고) 그 콘텐츠를 최종 사용자에게 제시하기 위해 도메인의 콘텐츠(특히 디지털 도메스틱 네트워크에서 유포되는 디지털 데이터)를 수신하기에 적합한 것이다. 이것은 특히 비디오 데이터를 보기 위해 사용하는 텔레비젼 수신기 또는 오디오 데이터를 듣기 위한 하이-파이(hi-fi) 설비를 포함한다.

<10> 소스 디바이스는 일반적으로 콘텐츠가 각각 "방송 콘텐츠"인지 또는 "광대역 콘텐츠"인지에 따라 "조건부 액세스" 모듈 또는 디지털 권리 관리 모듈(digital rights management module; "DRM")이라고 알려져 있는 모듈을 포함한다. 이 모듈들은 콘텐츠 공급자가 삽입한 콘텐츠의 보호를 관리한다.

<11> 예를 들어 유료 텔레비젼 프로그램을 생각하면, 콘텐츠 공급자, 즉 프로그램 방송자는 일반적으로 제어 워드라고 부르는 키를 이용하여 스크램블된 형태(즉, 암호화된 형태)로 디지털 프로그램을 공급하는데, 제어 워드 자체는 "ECM"("Entitlement Control Message")이라고 하는 메시지에서 암호화 형태로 데이터와 함께 전송된다. 콘텐츠 공급자는 또한 프로그램을 수신하기 위하여 요금을 지불한 가입자에게 제어 워드를 해독하기 위한 키, 및 특히 제어 워드를 해독하기 위한 알고리즘을 포함한 조건부 액세스 모듈을 제공한다(상기 키와 조건부 액세스 모듈은 바람직하게 스마트 카드에 포함된다). 콘텐츠 공급자는 또한 공급하는 콘텐츠의 사용 규칙, 즉 콘텐츠가 "자유 복사" 유형인지, "비공개 복사" 유형인지 또는 "판독 전용" 유형인지를 규정한다.

<12> SmartRight™(SmartRight는 톰슨 멀티미디어의 등록 상표임)의 명칭으로 알려진 복사에 대한 보호 시스템에서,

소스 디바이스는 수신된 콘텐츠를 그 콘텐츠의 사용 규칙에 따라 변환한다.

<13> 정해진 도메인의 소스 디바이스에서 수신한 콘텐츠가 "비공개 복사" 유형이면, 그 콘텐츠는 그 특수한 도메인에 속한 프리젠테이션 디바이스에 의해서만 해독될 수 있는 방식으로 변환된다(따라서 모두가 하나의 동일한 비밀을 공유한다). 톰슨 라이센싱 에스. 에이.(THOMSON Licensing S.A.)가 2001년 4월 25일에 출원한 통신 네트워크의 대칭 키 관리 방법에 관한 프랑스 특허 출원 제01 05568호에는, 통신 네트워크의 비밀 키를 알고 있는 프리젠테이션 디바이스만이 콘텐츠를 판독하기 위하여 콘텐츠를 해독할 수 있도록 상기 변환을 어떻게 실행하는지에 대하여 설명되어 있다.

<14> 이하의 설명에서, "비밀 키" 또는 "대칭 키"는, AES("Advanced Encryption Standard"의 머리글자임) 또는 "Rijndael"이라고 알려져 있고, 특히 "*Proceedings from the first Advanced Encryption Standard Candidate Conference, National Institute of Standards and Technology(NIST), August 1998, J. Daemen and V. Rijmen*"의 명칭의 문서에 설명되어 있는 알고리즘과 같은, 대칭 암호화 또는 해독 알고리즘에서 사용되는 암호화 키를 지칭하기 위해 사용된다.

<15> 소스 디바이스에서 수신한 콘텐츠가 "판독 전용" 유형이면, 이 콘텐츠는 네트워크 비밀 키를 알고 있는 네트워크의 프리젠테이션 디바이스에 의해서만 판독될 수 있도록 전술한 특허 출원에서 설명된 방법을 이용함으로써 상기 소스 디바이스에 의해 또한 변환된다. 또한, 톰슨 멀티미디어가 2000년 12월 7일에 출원한 프랑스 특허 출원 제00 15894호에 설명된 방법은 콘텐츠가 도메인에서 복사될 수 없도록, 또는 만일 복사되었으면 도메인의 프리젠테이션 디바이스에 의해 재생될 수 없도록 구현된다.

<16> 도메인에서 수신한 콘텐츠가 "자유 복사" 유형이면, 이 콘텐츠는 일반적으로 명문(clear)으로 되어 있고, 콘텐츠를 수신한 소스 디바이스에 의해 그 콘텐츠를 도메인에서 방송하기 위해 그 형태로 유지된다.

<17> 이 시스템 덕분에, 콘텐츠 공급자에게 관련 비용을 지불한 후에 콘텐츠를 수신한 사용자는, 그 콘텐츠의 비공개 복사본을 나중에 개인적인 용도로 사용하기 위하여 보관할 수 있다. 이 복사본은 상기 사용자의 도메인, 즉 콘텐츠를 처음에 수신한 도메인의 프리젠테이션 디바이스에 의해서만 판독될 수 있다.

<18> 그럼에도 불구하고, 제1 도메인에서 작성한 비공개 복사본을 제2 도메인의 프리젠테이션 디바이스에서 재생하는 것이 바람직한 경우가 있다. 특히, 사용자가 자신의 도메인에서 만든 영화의 복사본을 친구의 도메인에서 보고 싶어 하는 경우, 당연히 복사본 없이 친구의 도메인용으로 만들 수 있다.

<19> 이것은 사용자가 연합되거나 분리되는 경우에 또한 필요하다. 연합되는 경우에, 만일 각각의 사용자가 미리 그 자신의 도메인을 갖고 있으면, 2개의 도메인의 설비가 동일한 비밀을 공유하지 않기 때문에 2개의 도메인이 함께 연결될 수 없다. 이 경우에, 2명의 사용자가 2개의 다른 도메인을 관리하는 것을 원치 않으면, 제1 도메인에서 미리 기록된 콘텐츠는 제2 도메인에서 재생될 수 있어야 할 것이다. 마찬가지로, 하나의 도메인을 2개의 다른 도메인으로 분리할 필요가 있을 때(배우자가 떨어져 있거나 아이가 그 부모의 집에 남아있기 때문에), 공통 도메인에서 미리 기록된 콘텐츠는 2개의 새로운 도메인에서 재생가능할 필요가 있다.

<20> 본 발명은 상기 문제점들을 해결하기 위한 것이다.

발명의 상세한 설명

<21> 본 발명은, 제1 양태에 따르면, 제1 도메인에 특정된 암호화 방법에 따라 암호화된 데이터를 수신하기 위하여 제2 도메인에 속하는 네트워크에 접속되도록 되어 있는 데이터 처리 디바이스에 관련이 있다. 이 디바이스는:

<22> - 제1 도메인에 특정된 제1 비밀 키를 내포하는 메모리;

<23> - 해독된 데이터를 얻기 위해 상기 제1 비밀 키를 이용하여 암호화된 데이터를 해독하는 수단;

<24> - 제2 도메인에 특정된 암호화 방법에 따라 해독된 데이터를 암호화하는 수단을 포함하고, 상기 암호화 수단에 의해 암호화된 데이터는 제2 도메인에 특정된 제2 비밀 키를 이용하여 해독될 수 있다.

<25> 본 발명의 특징에 따르면, 상기 데이터 처리 디바이스는,

<26> - 제1 대칭 키와 상기 제2 도메인에 특정된 제2 비밀 키를 이용한 제1 대칭 키의 암호화를 내포하는 메모리-상기 암호화 수단은 상기 제1 대칭 키를 이용하여 해독된 데이터의 암호화를 수행함-와;

<27> - 상기 암호화 수단에 의해 암호화된 데이터 및 상기 제1 대칭 키의 암호화를 상기 제2 도메인에 특정된 제2 비

밀 키를 이용하여 상기 네트워크에서 방송하는 수단을 더 포함한다.

<28> 따라서, 본 발명의 처리 디바이스는 제1 도메인에 특정된 비밀 키만을 내포한다. 제2 도메인용으로 데이터를 암호화하기 위해 제2 도메인에 특정된 비밀 키를 알 필요는 없다; 제2 도메인은 대칭 키를 이용하여 데이터를 암호화하고, 제2 도메인에 특정된 비밀 키를 이용한 제1 대칭 키의 암호화를 상기 암호화한 데이터에 부착한다. 따라서, 데이터는 제2 도메인에서 해독될 수 있다.

<29> 본 발명의 다른 특징에 따르면, 제1 도메인에 특정된 제1 비밀 키와 제2 도메인에 특정된 제2 비밀 키는 각각 대칭 키이다.

<30> 본 발명의 특수한 실시예에 따르면, 처리 디바이스는 단명(ephemeral)의 마스킹 키를 발생하는 수단과; 마스킹된 데이터를 형성하기 위해 마스킹 키를 이용하여 해독된 데이터를 마스킹하는 수단-상기 마스킹된 데이터는 상기 제1 대칭 키를 이용하여 상기 암호화 수단에 의해 암호화됨-과; 방송 수단에 의해 방송된 데이터를 미리 수신한, 상기 네트워크에 접속된 프리젠테이션 디바이스에 의한 인증 동작에 응답하는 수단-상기 인증 동작에 대한 응답은 단명 마스킹 키를 포함함-을 더 포함한다.

<31> 전술한 본 발명의 실시예의 변형예에 따르면, 처리 디바이스는 제1 대칭 키를 이용하여 상기 암호화 수단에 의해 마스킹된 데이터와 함께 암호화되는 단명 인증 키를 발생하는 수단을 더 포함하며, 상기 인증 동작에 응답하는 수단은, 인증 키, 및 상기 프리젠테이션 디바이스로부터 수신된 난수의 함수로서 응답을 계산한다.

<32> 본 발명의 다른 특징에 따르면, 상기 처리 디바이스에 의해 수신된 데이터는 "비공개(private) 복사 인증" 또는 "1회 복사만 인증" 유형의 복사 제어 정보를 내포하고; 상기 디바이스는 상기 복사 제어 정보를 "판독 전용" 유형의 다른 복사 제어 정보로 교체하는 수단을 포함하며; 상기 디바이스에 의한 데이터 방송은 상기 "판독 전용" 유형의 복사 제어 정보를 내포한다.

<33> 따라서, 제2 도메인의 네트워크에서의 데이터 방송은 제2 도메인에서 복사될 수 없다.

<34> 본 발명은, 제2 양태에 따르면, 제1 도메인에 특정된 제1 비밀 키를 이용한 암호화 방법에 따라 암호화된 데이터를 제2 도메인에 속하는 네트워크에서 전송하는 방법과 또한 관련이 있다. 이 방법은, 처리 디바이스에 대하여,

<35> (a) 상기 네트워크에서 암호화된 데이터의 제1 방송을 네트워크에 접속되어 있는 제1 방송 디바이스로부터 수신하는 단계와;

(b) 해독된 데이터를 얻기 위해 상기 처리 디바이스에 내포된 상기 제1 비밀 키를 이용하여 상기 암호화된 데이터를 해독하는 단계와;

<36> 삭제

<37> (c) 상기 처리 디바이스에 내포된 제1 대칭 키를 이용하여 상기 해독된 데이터를 암호화하는 단계와;

<38> (d) 상기 제1 대칭 키를 이용하여 상기 단계 (c)에서 암호화된 데이터 및 상기 제2 도메인에 특정된 제2 비밀 키를 이용한 상기 제1 대칭 키의 암호화-상기 암호화는 상기 제2 도메인의 디바이스에 의해 상기 처리 디바이스에 미리 전송됨-의 제2 방송을 네트워크에서 수행하는 단계를 포함한다.

<39> 본 발명의 특징에 따르면, 단계 (c)는, 상기 처리 디바이스에 대하여, 단명 마스킹 키를 발생 및 저장하는 부단계와; 마스킹된 데이터를 형성하기 위해 마스킹 키를 이용하여 해독된 데이터를 마스킹하는 부단계와; 상기 제1 대칭 키를 이용하여 상기 마스킹된 데이터를 암호화하는 부단계를 포함한다.

<40> 본 발명의 다른 특징에 따르면, 단계 (c)는, 상기 처리 디바이스에 대하여, 단명 인증 키를 발생 및 저장하는 부단계와; 상기 단명 인증 키, 및 상기 마스킹된 데이터를 상기 제1 대칭 키를 이용하여 암호화하는 부단계를 포함하고; 상기 데이터 전송 방법이, 단계 (d) 후에, 단계 (d)에서 방송 데이터를 미리 수신한, 상기 네트워크에 접속된 프리젠테이션 디바이스에 의한 인증 동작에 응답하는 단계를 더 포함하며, 상기 인증 동작에 대한 응답은 상기 단명 마스킹 키를 포함한다.

<41> 본 발명의 또다른 특징에 따르면, 상기 인증 동작에 대한 응답은 상기 인증 키 및 상기 프리젠테이션 디바이스로부터 수신된 난수의 함수로서 계산된다.

<42> 본 발명의 또다른 특징에 따르면, 상기 제1 방송 중에 전송된 암호화 데이터는 "비공개 복사 인증" 또는 "1회

복사만 인증" 유형의 복사 제어 정보를 내포하고, 상기 데이터 전송 방법이, 상기 단계 (d) 전에, 상기 복사 제어 정보를 "판독 전용" 유형의 다른 복사 제어 정보로 교체하는 단계를 더 포함한다.

<43> 본 발명의 특수한 양태에 따르면, 데이터 전송 방법은 상기 처리 디바이스를 상기 제1 도메인에 속하는 네트워크에 접속시키는 단계 및 상기 제1 도메인에 특정된 비밀 키를 상기 처리 디바이스에서 수신하는 단계로 이루어진 처리 디바이스 초기화 단계를 더 포함하고, 상기 비밀 키는 상기 제1 도메인의 네트워크에 접속된 다른 디바이스에 의해 전송된다.

<44> 본 발명의 다른 특수한 양태에 따르면, 상기 초기화 단계는, 상기 처리 디바이스를 상기 제2 도메인에 속하는 네트워크에 접속시키는 단계를 더 포함하며; 상기 처리 디바이스에 대하여, 상기 제1 대칭 키를 발생하는 단계; 상기 제1 대칭 키를 상기 제2 도메인의 적어도 하나의 디바이스에 보안 방식으로 전송하는 단계; 및 상기 제2 도메인에 특정된 제2 비밀 키를 이용한 상기 제1 대칭 키의 암호화를 상기 제2 도메인의 디바이스로부터 수신하는 단계를 더 포함한다.

실 시 예

<51> 먼저, 도 1과 관련하여, 디지털 콘텐츠의 비공개 복사본이 디지털 콘텐츠가 복사되는 도메스틱 네트워크에서만 나중의 사용을 위해 만들어질 수 있도록 복사 보호 시스템이 구현되는 도메스틱 네트워크의 일 예를 설명한다.

<52> 네트워크는 소스 디바이스(1), 프리젠테이션 디바이스(2) 및 기록 디바이스(3)를 포함하고, 이 디바이스들은, 예를 들면 표준 IEEE 1394에 따른 버스인 디지털 버스(4)에 의해 상호 접속되어 있다.

<53> 소스 디바이스(1)는 스마트 카드(11)가 비치된 스마트 카드 판독기를 구비한 디지털 디코더(10)를 포함한다. 이 디코더는 디지털 데이터, 특히 서비스 공급자에 의해 분배된 오디오/비디오 프로그램을 수신한다.

<54> 프리젠테이션 디바이스(2)는 스마트 카드(21)가 비치된 스마트 카드 판독기를 구비한 디지털 텔레비젼 수신기(DTV)(20)를 포함하고, 기록 디바이스(3)는 특히 디지털 비디오 카세트 레코더(DVCR)이다.

<55> 소스 디바이스(1)를 통해 네트워크에 진입하는 디지털 데이터는 일반적으로, 예를 들면 유료 텔레비젼 원리에 따라, 콘텐츠 공급자에 의해 스크램블된 데이터이다. 이 경우에, 데이터는 자격 관리 메시지(ECM)에 내포되어 있는 암호화 키(K_F)를 이용하여 암호화된 형태로 데이터 스트림에서 전송된 제어 워드(CW)를 이용하여 스크램블된다. 암호화 키(K_F)는 특히 스마트 카드에 저장된 데이터를 수신하기 위해 요금을 지불한 사용자에게 공급된다. 도 1의 예에서, 스마트 카드(11)는 암호화 키(K_F), 및 제어 워드(CW)를 해독할 수 있는 조건부 액세스(CA) 모듈(14)을 내포한다.

<56> 스크램블된 디지털 데이터를 수신한 소스 디바이스(1)는, 그 디지털 데이터를 도메스틱 네트워크에 특정된 보호 포맷으로 디지털 네트워크를 통해 방송하도록 자신을 포맷한다. 디코더(10)는 암호화 키(K_F)를 이용하여 암호화된 제어 워드를 내포한 ECM 메시지를, 수신된 데이터 스트림으로부터 추출하여 CA 모듈(14)로 전송하는 "ECM 유닛" 모듈(13)을 포함한다. CA 모듈은 제어 워드(CW)를 해독하여, 역시 스마트 카드(11)에 내포된 컨버터 모듈(12)에 전송한다.

<57> 컨버터 모듈(12)은 ECM 메시지에 내포된 정보를 로컬 도메스틱 네트워크에 특정된 비밀 키(K_{N1})를 이용하여 보호되는 LECM("Local Entitlement Control Message") 메시지로 변환하는 역할을 한다.

<58> 컨버터 모듈은 대칭 키(K_C)를 미리 랜덤하게 발생하고, 네트워크 비밀 키(K_{N1})를 이용하여 대칭 키(K_C)의 암호화를 요구하는 것으로 생각된다. 그러므로, 컨버터 모듈은 메모리 내에 대칭 키(K_C)를 내포하고, 대칭 키(K_C)는 네트워크 비밀 키(K_{N1})에 의해 암호화된다($E\{K_{N1}\}(K_C)$).

<59> 이하의 설명에서, 기호 E{K}(M)은 항상 데이터 M의 키 K에 의한 암호화를 나타내기 위해 사용된다.

<60> 전술한 프랑스 특허 출원 제01 05568호에는 컨버터 모듈이 네트워크 비밀 키(K_{N1})을 이용하여 대칭 키(K_C)를 얻는 방법이 상세히 설명되어 있고, 암호화는 프리젠테이션 디바이스에서 수행된다. 구체적으로, 도 1에서 부호 '2'로 표시한 것과 같은 네트워크의 프리젠테이션 디바이스는 네트워크 비밀 키(K_{N1})를 가진 유일한 디바이스이다. 네트워크 비밀 키(K_{N1})는, 특히 네트워크 키(K_{N1})에 의한 암호화 및 해독 동작을 수행하는 단말기 모듈(22)과 함께 스마트 카드에 내포된다.

<61> 시스템은 다음과 같이 동작한다. 디지털 데이터가 디코더(10)에서 수신될 때, "ECM 유닛" 모듈(13)은 콘텐츠 공급자에게 특정된 키(K_F)를 이용하여 암호화된 제어 워드(CW)를 내포하는 ECM 메시지를 추출하여 CA 모듈(14)에 공급한다. CA 모듈(14)은 제어 워드(CW)를 해독하여 컨버터 모듈(12)에 전송한다. 또한, ECM 메시지는 콘텐츠가 네트워크에서 자유롭게 복사될 수 있는지 없는지 또는 네트워크에서 보기(또는 듣기 등) 전용인지 여부를 나타내는, 전송된 콘텐츠의 복사의 제어에 관한 정보를 내포할 수 있다. 이 정보는 또한 컨버터 모듈에 전송된다.

<62> 그 다음에, 컨버터 모듈은 이들 데이터에 기초하여 LECM 메시지를 구성한다. 이 메시지는 바람직하게 다음의 요소들을 포함한다:

<63> - 콘텐츠의 복사의 제어에 관한 정보, 다시 말해서 콘텐츠가 "자유 복사" 유형인지, "비공개 복사" 유형인지 또는 "판독 전용" 유형인지를 나타내는 정보를 특히 내포하는 명문의 부분 A. 이 정보는 가끔 VCI("보기 제어 정보")로 표시된다. 명문의 부분은 네트워크 키에 의해 암호화된 대칭 키(K_C)를 또한 내포한다($E\{K_{N1}\}(K_C)$).

<64> - 대칭 키(K_C)로 암호화되고, 본질적으로 해독된 제어 워드(CW)를 내포하는 부분 B; 이 부분은 $E\{K_C\}(CW)$로서 요약될 수 있다.

<65> - 부분 B의 암호화 전에 부분 A와 부분 B 모두에 적용된 해시 함수(hash function)의 결과에 의해 형성된 무결성 필드(integrity field). 이 무결성 필드는 LECM 메시지의 유효성을 증명하기 위해서 및 LECM 메시지가 불법적으로 변형되지 않았음을 보장하기 위하여 유리하게 사용된다.

<66> 그 다음에, LECM 메시지는 ECM 유닛에 전송되고, ECM 유닛은 LECM 메시지를 ECM 메시지의 위치에서 데이터 스트림에 삽입한다. 수신된 콘텐츠가 전술한 바와 같이 이미 스크램블된 형태가 아니고, 어떠한 ECM 메시지도 내포하고 있지 않으면, 컨버터 모듈(12)은, 이 경우에, 네트워크(4)를 통하여 방송되는 데이터 스트림이 LECM 메시지 및 스크램블 데이터를 내포하는 도 1에 표시된 패킷(40)과 같은 데이터 패킷 형태로 항상 유지되도록 데이터를 이 형태로 두는 역할을 한다.

<67> 이 패킷의 콘텐츠는 다음과 같이 요약될 수 있다:

<68> LECM | E{CW}(<데이터>); 또는

<69> $E\{K_{N1}\}(K_C)$ | VCI | $E\{K_C\}(CW)$ | 무결성 필드 | E{CW}(<데이터>)

<70> 여기에서, " | "는 연결 연산자를 나타낸다.

<71> 이 데이터 패킷들이 디지털 텔레비젼 수신기(20)에서 수신될 때, 데이터 패킷들은 "LECM 유닛" 모듈(23)에 전송되고, 모듈(23)은 데이터 패킷으로부터 LECM 메시지를 추출하여 그 메시지를 단말기 모듈(22)에 전송한다. 단말기 모듈(22)은 먼저 비밀 키(K_{N1})를 이용하여 $E\{K_{N1}\}(K_C)$를 해독하고 대칭 키(K_C)를 얻는다. 그 다음에, 대칭 키(K_C)를 이용하여 $E\{K_C\}(CW)$를 해독하여 제어 워드(CW)를 얻고, 이 제어 워드는 "LECM 유닛" 모듈(23)에 전송된다. 그 다음에, "LECM 유닛" 모듈(23)은 제어 워드를 이용하여 데이터 E{CW}(<데이터>)를 디스크램블할 수 있다. 그 다음에, 스크램블되지 않은 데이터가 사용자에게 제공된다. 비디오 데이터의 경우에, 데이터는 텔레비젼 수신기(20)에서 볼 수 있다.

<72> 패킷(40)을 내포하는 데이터 스트림이 나중에 재생하기 위해 디지털 비디오 카세트 레코더(3)에 의해 기록되면, 데이터가 제공되는 프리젠테이션 디바이스가 데이터가 기록된 도메인의 비밀 키(K_{N1})를 내포하고 있지 않는 한, 재생이 불가능하다. 이하, 이 도메인은 N1이라고 부른다.

<73> 도 1의 예에서, 도메인은 디지털 도메스틱 네트워크, 도메스틱 네트워크에 접속된 모든 설비 및 도메스틱 네트워크에 접속될 수 있고 도메스틱 네트워크를 소유하는 가족들에게 속하는 휴대형 프리젠테이션 설비(도시 생략)라고 이해하였던 점을 기억하자. 휴대형 프리젠테이션 설비(예를 들면, 압축 음악 파일 판독기)는 이들이 비밀 키(K_{N1})를 내포하고 있을 때 도메인(N1)의 일부를 형성하는 것으로 생각된다. 도메인(N1)의 비밀 키가 도메인에 "진입"(enter)하는 새로운 프리젠테이션 디바이스(예를 들면, 가족 중의 한 사람이 새로운 설비를 구입하였을 때)에 어떻게 전송되는가에 대한 설명은 전술한 프랑스 특허 출원 제01 05568호를 참조한다.

<74> 이제, "비공개 복사" 유형의 콘텐츠(예를 들면, 영화)를 자신의 도메인(N1)에서 녹화한 사용자가 N2라고 부르는 다른 도메인에 속하는 텔레비젼 수신기에서 볼 수 있기를 원한다고 가정하자.

<75> 이 경우에, 사용자는 예를 들면 영화를 내포하는 카세트를 도메인 N2의 디지털 비디오 카세트 레코더에 삽입한다. 이 비디오 카세트 레코더는 도메인 N2의 도메스틱 네트워크를 통해 영화를 방송하여 그 영화를 도메인 N2의 텔레비젼 수신기에서 볼 수 있게 한다. 그러나, 도메인 N2의 텔레비젼 수신기는 도메인 N1의 비밀 키(K_{N1})를 모르기 때문에, LECM 메시지의 콘텐츠를 해독할 수 없고, 따라서, 사용자에게 영화를 제공하기 위해 데이터를 디스크램블할 수 없을 것이다.

<76> 본 발명의 원리에 따르면, 도메인 N1에서 "비공개 복사"로서 기록된 콘텐츠를 도메인 N2에서 볼 수 있게 하기 위하여, 콘텐츠가 도메인 N2의 "판독 전용" 유형의 콘텐츠로 변환될 것이다.

<77> 이하에서는 이 변환을 수행하는 몇가지 실시예를 설명한다.

<78> 먼저, 각종 실시예에서 사용되는 일반적인 원리를 설명한다.

<79> 이를 위해, 변환을 실행하기 위하여 우리가 M이라고 부르는 디바이스가 필요하다. 이 디바이스는 도메인 N1의 비밀, 즉 키 K_{N1}을 내포해야 하고, 변환을 행할 수 있기 전에 도메인 N2에 설치되어야 한다. M은 도메인 N2의 콘텐츠를 변환할 수 있게 하기 위하여 도메인 N2의 프리젠테이션 디바이스의 단말기 모듈과 등가인 단말기 모듈 및 도메인 N2의 소스 디바이스의 컨버터 모듈과 등가인 컨버터 모듈을 포함해야 한다.

<80> 이 디바이스(M)는, 도메인 N2의 도메스틱 네트워크에 연결되면, 먼저 대칭 키(K'_C)를 발생해야 하고, 그 대칭 키를 $E\{K_{N2}\}(K'_C)$를 얻기 위해 도메인 N2의 비밀 키(K_{N2})를 이용하여 암호화해야 한다. 다음에, 도메인 N2의 디지털 비디오 카세트 레코더에서 방송 콘텐츠를 수신할 때, VCI가 "비공개 복사" 코드를 내포하는 $E\{K_{N1}\}(K_C)$ | VCI | $E\{K_C\}$(CW) | 무결성 필드를 내포하는 메시지 LECM1을 VCI가 "판독 전용" 코드를 내포하는 $E\{K_{N2}\}(K'_C)$ | VCI | $E\{K'_C\}$(CW) | 무결성 필드를 내포하는 메시지 LECM2로 교체하고, 그에 따라 비밀 키 K_{N2}를 내포하는 도메인 N2의 텔레비젼 수신기에 의해 해독 가능하게 된 콘텐츠를 방송한다.

<81> 도 2에는 본 발명의 제1 실시예가 구현되는 도메인 N2의 디지털 도메스틱 네트워크를 도식적으로 나타내고 있다. 우리는 본 발명의 이해에 필요한 요소들만을 도시하였다.

<82> 이 네트워크에서, 디지털 버스(204)는 디지털 비디오 카세트 레코더(203), 프리젠테이션 디바이스(202) 및 도메인 N1에서 생성된 디바이스(M)를 상호 접속한다. 디지털 버스(204)는 바람직하게 표준 IEEE 1394에 따른 버스이다. 프리젠테이션 디바이스(202)는 "LECM 유닛" 모듈(223)을 내포하는 디지털 텔레비젼 수신기(DTV)(220) 및 단말기 모듈(222)을 내포하는 스마트 카드(221)를 포함한다. 스마트 카드(221)에는 도메인 N2의 비밀 키(K_{N2})가 저장된다.

<83> 디바이스 M은, 예를 들면, 설비 M의 보안 프로세서에 구축된 모듈, 또는 설비 M에 삽입되는 스마트 카드에 내포된 제거가능 모듈일 수 있는 단말기/컨버터 모듈(210)을 포함한 휴대형 설비이다. 단말기/컨버터 모듈(210)은 도 1과 관련하여 설명한 것과 같은 컨버터 및 단말기 모듈의 기능들을 구현한다. 디바이스 M은 또한 "추출/삽입 LECM" 모듈(211)을 내포하고, 이 모듈의 동작에 대해서는 나중에 설명한다.

<84> 디바이스 M은 또한 디바이스 M이 위치한 도메인에 따라 디바이스 M을 사용자가 프리젠테이션 디바이스로서 또는 소스 디바이스로서 구성할 수 있게 하는 사용자 인터페이스(UI)(212)를 포함한다.

<85> 용어 "버진"(virgin), "원조"(originator) 및 "스테릴"(sterile)은 앞에서 언급한 프랑스 특허 출원 제0105568호에 정의되어 있으며, 각각 다음과 같은 프리젠테이션 디바이스(또는 더 정확하게는 프리젠테이션 디바이스의 단말기 모듈)을 지칭한다.

<86> - 어떤 도메인에도 접속되지 않으며 도메인 비밀 키를 내포하고 있지 않은 디바이스("버진" 디바이스);

<87> - 도메인의 비밀 키를 구비하고, 그 비밀 키를 도메인에 접속될 새로운 버진 프리젠테이션 디바이스에 전송할 수 있는 디바이스("원조" 디바이스); 및

<88> - 도메인의 비밀 키를 구비하지만 그 비밀 키를 다른 디바이스에 전송할 수 없는 디바이스("스테릴" 디바이스).

<89> 상기 특허 출원에는 또한 다른 디바이스들 간에 비밀 키의 전송을 보장하기 위한 메카니즘이 설명되어 있다.

<90> 그 다음에, 디바이스 M은 사용자가 도메인 N1에서 "비공개 복사"로서 기록된 콘텐츠를 보기 원하는 도메인 N2에 접속될 수 있다. 이러한 경우, 디바이스 M은 도메인 N2의 네트워크에 소스 디바이스로서 접속된다.

<91> 도 3은 디바이스 M이 도메인 N2의 네트워크에 접속된 후에 구현되는 단계들을 도시한다.

<92> 제1 단계(100)에서, 대칭 키(K'_C)가 디바이스 M의 컨버터 모듈에 의해 랜덤하게 발생되어 그 디바이스에 의해 저장된다. 이하에서, 우리는, 단말기/컨버터 모듈(210)이 관습적으로 컨버터 모듈에 의해 구현되는 기능을 구현하는지 또는 단말기 모듈에 의해 구현되는 기능을 구현하는지에 따라, 때로는 디바이스 M의 컨버터 모듈을 말하기도 하고, 때로는 단말기 모듈을 말하기도 할 것이다.

<93> 다음 단계(101)에서, 디바이스 M은 네트워크의 프리젠테이션 디바이스의 공개 키를 수신하기 위해 도메인 N2의 네트워크를 통해 요구 메시지를 방송한다. 각각의 프리젠테이션 디바이스는, 실제로는, 단말기 모듈을 내포한 스마트 카드에 저장된 비대칭 키 쌍을 구비한다. 예를 들면, 도 2의 프리젠테이션 디바이스(202)는 공개 키(K_{PUB_T2})와 비공개 키(K_{PRI_T2})를 갖고 있다. 이 키들은 비대칭 암호화 알고리즘(예컨대, 창시자인 Rivest, Shamir 및 Adleman의 이름을 따서 이름지은 RSA 알고리즘)을 이용하여 암호화 또는 해독 동작을 실행하기 위해 본질적으로 알려진 방식으로 사용된다.

<94> 도메인 N2의 임의의 프리젠테이션 디바이스는 이 요구(101)에 응답할 수 있다. 이하에서는 프리젠테이션 디바이스(202)가 단계 102에서 디바이스 M에 그 공개 키(K_{PUB_T2})를 보냄으로써 상기 요구에 응답하는 것으로 가정한다.

<95> 그 다음에, 디바이스 M의 컨버터 모듈은 수신된 공개 키(K_{PUB_T2})를 이용하여 대칭 키(K'_C)의 암호화를 실행하고(단계 103), 그 다음에, 상기 암호화의 결과($E\{K_{PUB\_T2}\}(K'_C)$)를 프리젠테이션 디바이스(202)에 보낸다(단계 104). 프리젠테이션 디바이스(202)는 수신된 상기 결과를 비공개 키(K_{PRI_T2})를 이용하여 해독하여 K'_C를 얻는다(단계 105). 프리젠테이션 디바이스(202)는 그 다음에 도메인 N2의 비밀 키(K_{N2})로 K'_C를 암호화하여 $E\{K_{N2}\}(K'_C)$를 얻고, 그 결과를 단계 107에서 디바이스 M에 보낸다. 디바이스 M은 다음 단계 108에서 상기 결과 $E\{K_{N2}\}(K'_C)$를 저장한다.

<96> 이제, 디바이스 M은 도메인 N1으로부터 "비공개 복사" 유형의 콘텐츠를 수신하여 그 콘텐츠를 도메인 N2용의 "판독 전용" 유형의 콘텐츠로 변환할 준비가 되었다.

<97> 이제, 도 4를 참조하여 상기 변환을 수행하는 방법을 설명한다.

<98> 도 4(첨부 도면에서는 2개의 도면(도 4a, 도 4b)으로 분리되어 있다)는 디지털 비디오 카세트 레코더(DVCR)(203), 디바이스 M 및 프리젠테이션 디바이스(202)에 의해 수행되는 처리, 및 도메인 N1으로부터 생성된 새로운 콘텐츠를 도메인 N2의 디지털 도메스틱 네트워크에서 방송할 때 상기 디바이스들 사이의 교환을 설명하기 위하여 시간축을 나타내는 3개의 하향 수직축(t)을 사용한다.

<99> 먼저, 사용자는 예를 들면 도메인 N1에서 녹화한 비디오 프로그램을 내포한 비디오 카세트를 도메인 N2의 디지털 비디오 카세트 레코더(203)에 삽입한다. 이 때, 비디오 카세트 레코더는 카세트에 녹화된 데이터를 도메인 N2의 네트워크를 통하여 디바이스 M을 향해 방송한다. 이 방송은 사용자에 의해 미리 규정되거나 선택된 네트워크의 특수한 채널을 이용하여 수행된다. 디바이스 M은 방송 데이터를 수신하기 위해 동일한 채널로 설정된다.

<100> 도 4의 단계 401에서 방송되는 데이터는 다음과 같은 데이터 패킷을 내포하고 있다:

<101> LECM1 | E{CW}(<데이터>), 즉,

<102> $E\{K_{N1}\}(K_C)$ | CP | $E\{K_C\}$(CW) | 무결성 필드 | E{CW}(<데이터>). 여기에서, "CP"는 "VCI" 정보의 "비공개 복사" 코드에 대응한다.

<103> 상기 데이터 패킷들이 디바이스 M에서 수신된 때, "추출/삽입 LECM" 모듈(211)이 상기 데이터 패킷으로부터 메시지 LECM1을 추출하여 그 메시지를 디바이스 M의 단말기 모듈로 전송한다. 디바이스 M은 먼저 단계 402에서 $E\{K_{N1}\}(K_C)$를 비밀 키(K_{N1})로 해독하여 키 K_C를 얻는다. 그 다음에, 디바이스 M은 $E\{K_C\}$(CW)를 이전 단계에서 얻은 키 K_C로 해독하여 제어 워드(CW)를 얻고(단계 403), 이 제어 워드는 컨버터 모듈로 전송된다.

<104> 다음에, 상기 콘텐츠는 디바이스 M의 컨버터 모듈에 의해 도메인 N2 용의 "판독 전용" 유형의 콘텐츠로 변환되어야 한다. 그러므로, 다음 단계들은 디바이스 M의 컨버터 모듈에 의해 수행된다:

<105> 단계 404에서, 컨버터 모듈은 2개의 난수(R, K)를 발생한다. 이 난수들은 바람직하게 그 자체로서 공지되어 있는 의사 난수 발생기에 의해 발생된다. 난수 R은 제어 워드에 대한 단명 마스킹 키로서 사용되고 이 명세서에서 사실상 "마스킹 키"라고 부를 것이다. 난수 K 자체는 이 명세서에서 더 큰 편리성을 위해 사실상 "인증 키"라고 부르는 단명 인증 키를 구성한다.

<106> 마스킹 키(R)와 인증 키(K)는 방송 콘텐츠의 제1 데이터 패킷이 디바이스 M에서 수신될 때 발생된다. 마스킹 키(R)와 인증 키(K)는 또한 단계 404에서 디바이스 M의 보안 메모리 구역에 임시 저장되고, 나중에 설명하는 바와 같이, 콘텐츠가 도메인 N2의 프리젠테이션 디바이스로 완전히 전송된 때에 소거될 것이다. 단계 404는 그러므로 컨버터 모듈에서 메시지 LECM1을 수신할 때마다 구현되지 않는다. 반면에, 그 후속 단계들은 수신된 각각의 새로운 메시지 LECM1에 대하여 구현된다.

<107> 단계 405에서, 디바이스 M의 컨버터 모듈은 단계 403에서 얻은 평문(plaintext) 제어 워드 및 마스킹 키(R)의 함수로서 마스크 제어 워드(MCW)를 계산한다. 바람직하게는, 하기의 동작이 수행된다:

<108> MCW = CW ⊕ R; 여기에서 ⊕는 "배타적 OR" 연산("XOR")을 나타낸다.

<109> 다음에, 단계 406에서, 컨버터 모듈은 대칭 키(K'_C)를 이용하여 마스크 제어 워드(MCW)와 인증 키(K)를 암호화하고, 그 다음에, 단계 407에서, 하기의 내용을 내포한 메시지 LECM2를 구성한다:

<110> $E\{K_{N2}\}(K'_C) | LS | E\{K'_C\}(MCW | K) |$ 무결성 필드, 여기에서 "LS"는 "VCI" 정보에 대한 "판독 전용" 코드에 대응하고, 무결성 필드는 다음과 같이 계산된다:

<111> 해시 $(E\{K_{N2}\}(K'_C) | LS | MCW | K)$

<112> 여기에서 "해시 (x)"는 해시 함수, 즉, 입력 데이터 세트 "x"를 고정 크기, 또는 가끔은 입력 데이터 크기보다 더 작은 데이터 세트 "y"로 변환하고 입력 데이터를 대표하는 수학적 함수를 나타낸다; 이 함수는 또한 일방 함수(one way function), 즉, y=해시(x)와 같이, "y"를 알 때 "x"를 다시 찾을 수 없는 함수이다. 바람직하게는, "*Secure Hash Standard, FIPS PUB 180-1, National Institute of Standard Technology, 1995*"의 문서에 설명된 SHA-1 함수가 사용된다.

<113> 일단 디바이스 M의 컨버터 모듈에 의해 메시지 LECM2가 구성되었으면, 상기 메시지 LECM2는 "추출/삽입 LECM" 모듈(211)에 전송되고, "추출/삽입 LECM" 모듈(211)은 상기 메시지 LECM2를 초기의 메시지 LECM1 대신에 데이터 패킷에 삽입한다.

<114> 단계 408에서, 메시지 LECM2에 의해 변형된 데이터 패킷은 디지털 비디오 카세트 레코더의 종래의 방송 채널을 이용하여 도메인 N2의 네트워크의 버스(204)를 통하여 보내진다. 따라서, 도메인 N2의 프리젠테이션 디바이스는 마치 디지털 비디오 카세트 레코더(203)에 의해 직접 방송되는 것처럼 콘텐츠에 액세스할 수 있다.

<115> 사용되는 방송 채널은 IEEE 1394 버스의 등시 채널(isochronous channel) 중의 하나이고, 이 채널은 MPEG 2 표준(ISO/IEC 13818-1)에 따라 압축된 데이터를 관습적으로 운송한다.

<116> 사용자가 도메인 N2의 프리젠테이션 디바이스(202), 즉, 다시 말해서 텔레비젼 수신기(220)에서 콘텐츠를 보기를 원한다고 가정하자. 따라서, 단계 408에서 보내진 데이터 패킷들은 디지털 텔레비젼 수신기(220)에서 수신되고, "LECM 유닛" 모듈(223)은 메시지 LECM2를 추출하며, 상기 메시지 LECM2를 처리를 위해 단말기 모듈(222)에 전송한다.

<117> 도 2에서, 우리는 도메인 N2에서 단일 프리젠테이션 디바이스만을 나타내었지만, 복수의 프리젠테이션 디바이스를 설치하는 것도 전적으로 가능하다. 이 경우, 도 3에서 도시한 바와 같이, 네트워크의 비밀 키(K_{N2})로 대칭 키(K'_C)의 암호화를 수행하고, 도 4에 도시한 바와 같이 디바이스 M에 의해 데이터 패킷 방송을 수신하는 동일한 프리젠테이션 디바이스일 필요는 없다.

<118> 후속 단계들은 프리젠테이션 디바이스(202)의 단말기 모듈(222)에서 구현된다.

<119> 시작을 위해, 단계 409에서, 단말기 모듈은 메시지 LECM2의 콘텐츠를 해독한다. 먼저, 단말기 모듈은 키 K_{N2}로 $E\{K_{N2}\}(K'_C)$를 해독하여 키 K'_C를 얻고, 이 키 K'_C로 $E\{K'_C\}(MCW | K)$를 해독하여 $MCW | K$를 얻는다.

<120> 다음에, 단계 410에서, 상기 해독된 데이터에 기초하여 해시 $(E\{K_{N2}\}(K'_C) | LS | MCW | K)$를 계산하고 그 결과를

메시지 LECM2의 무결성 필드와 비교함으로써, 메시지 LECM2의 무결성에 대한 체크가 수행된다.

<121> 만일 상기 2개가 동일하면, 메시지 LECM2는 유효한 것으로 간주되어 방법이 계속되고, 그렇지 않으면 방법이 중단된다. 방법이 중단된 경우에, 사용자에게 경고 메시지를 표시하기 위한 설비가 구성될 수 있다.

<122> 메시지 LECM2가 유효일 때, 단말기 모듈은 다음에 단계 411에서 VCI 필드 = "LS"를 판독함으로써, 이것이 "판독 전용" 유형의 콘텐츠인 것을 검출한다.

<123> 다음 단계 412에서, 네트워크를 통해 데이터 패킷을 보낸 디바이스 M을 인증함으로써, 단말기 모듈(222)은 난수(R_i)를 발생하고, 그 다음에 프리젠테이션 디바이스(202)는 커맨드 메시지가 관습적으로 이동하는 버스(204)의 비동기 채널을 이용하여 상기 난수(R_i)를 디바이스 M에 전송한다(단계 413)(버스(204)의 비동기 채널에 의한 전송은 도 4에서 점선으로 표시되어 있다).

<124> 단계 414에서, 디바이스 M이 난수(R_i)를 수신하면, 디바이스 M은 하기의 계산을 수행한다(컨버터 모듈에 의해 수행한다):

<125> $Hi = MAC_K(R_i)$

<126> 여기에서 "$MAC_K(x)$"는 키 K를 이용한 메시지 x의 "메시지 인증 코드"를 나타낸다. "MACs"에 관한 추가적인 상세에 대하여, "*Handbook of applied cryptography, Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, 1997, page 325*"의 문헌을 참조할 수 있다.

<127> 특히 인터넷 어드레스 *http://www.ietf.org/rfc/rfc2104.txt*에서 입수가능한 공보 "*Keyed-Hashing for Message Authentication, RFC 2104, Krawczyk, Bellare and Canneti, 1997*"에 설명되어 있는 HMAC-SHA-1 함수가 H_i를 계산하기 위해 바람직하게 이용될 것이다.

<128> 다음 단계 415에서, 디바이스 M은 $H_i=MAC_K(R_i)$ 계산의 결과 및 마스킹 키(R)를 버스(204)의 비동기 채널을 통하여 프리젠테이션 디바이스(202)에 보낸다.

<129> 그 다음에, 단말기 모듈(222)은, 단계 416에서, 단계 412에서 발생한 난수(Ri) 및 단계 409에서 메시지 LECM2를 해독함으로써 얻어진 인증 키(K)를 이용하여 $H'_i=MAC_K(R_i)$를 계산함으로써 수신된 수 H_i의 유효성을 체크한다.

<130> 만일 H'i가 디바이스 M으로부터 수신한 수 Hi와 다르면, 방법이 중단된다. 예를 들면, 콘텐츠를 볼 수(또는 청취할 수) 없다는 것을 사용자에게 경고하기 위해 사용자에게 주의를 주기 위한 메시지가 표시된다.

<131> 반면에, $H'_i=H_i$이면, 디바이스 M이 인증된다. 이 경우에, 단말기 모듈(222)은 수신된 마스킹 키(R)를 이용하여 하기의 연산을 수행함으로써 MCW로부터 제어 워드(CW)를 검색한다(단계 417):

<132> $MCW \oplus R = CW \oplus R \oplus R = CW$

<133> 다음에, 해독된 제어 워드(CW)는 "LECM 유닛" 모듈(223)에 전송될 수 있고, "LECM 유닛" 모듈(223)은 단계 408에서 수신된 패킷의 데이터를 제어 워드(CW)로 디스크램블하여(단계 418) 그 데이터가 사용자에게 제시될 수 있다.

<134> 단계 409, 410, 417 및 418은 디바이스 M으로부터 프리젠테이션 디바이스(202)로 전송된 콘텐츠를 형성하는 각각의 데이터 패킷에 대하여 반복된다. 그 다음에, 다음 단계 419에서, 프리젠테이션 디바이스(202)는 상기 계산을 수행하기 위하여 임시로 저장되었던 마스킹 키(R) 및 인증 키(K)를 자신의 메모리로부터 소거한다.

<135> 콘텐츠를 형성하는 모든 데이터 패킷이 디바이스 M으로부터 프리젠테이션 디바이스(202)로 일단 전송되었으면, 마스킹 키(R)와 인증 키(K)가 단계 420에서 디바이스 M의 메모리로부터 즉시 소거되어, 디바이스 M이 콘텐츠의 가능한 재생을 위하여 도메인 N2의 프리젠테이션 디바이스로 다시 상기 데이터를 전송하는 것이 더 이상 불가능하게 한다. 따라서, 비록 사용자가 단계 408에서 네트워크를 통해 방송된 데이터 패킷을 기록하였다 하더라도, 마스킹 키(R)와 인증 키(K)가 디바이스 M의 메모리 및 프리젠테이션 디바이스(202)의 메모리로부터 소거되었기 때문에, 사용자는 그 데이터를 재생할 수 없게 될 것이다.

<136> 도 5는 도메인 N1에서 "비공개 복사"로서 기록된 콘텐츠를 도메인 N2 용의 "판독 전용" 유형의 콘텐츠로 변환할 수 있는 본 발명의 제2 실시예를 도시한다.

<137> 도 5에서는 디지털 비디오 카세트 레코더(503), 제1 프리젠테이션 디바이스(502) 및 제2 프리젠테이션 디바이스(505)가 접속된 디지털 버스(504)를 포함하는 도메인 N2의 디지털 도메스틱 네트워크를 도식적으로 표시하였다

<138> 제1 프리젠테이션 디바이스(502)는 "LECM 유닛" 모듈(523)을 내포한 텔레비젼 수신기(DTV1)(520) 및 단말기 모듈(522)을 내포한 스마트 카드(521)를 포함한다.

<139> 이 실시예에서, 도메인 N2 용의 콘텐츠의 변환을 수행하는 디바이스 M은, 내부에 통상적으로 위치된 제2 프리젠테이션 디바이스(505)의 단말기 모듈을 내포하는 스마트 카드 대신에, 제2 프리젠테이션 디바이스(505)로 삽입되는 단말기 모듈(512) 및 컨버터 모듈(514)을 내포하는 스마트 카드(511)(이하, "단말기/컨버터" 카드라고 부른다)에 의해 구현된다(즉, 다시 말해서, 도메인 N1에서 기록된 콘텐츠를 도메인 N2에서 판독할 필요가 없다). 프리젠테이션 디바이스(505)는 "LECM 유닛" 모듈(513) 및 우리가 M'라고 부르고 LECM 메시지를 데이터 패킷에 삽입하는 것 및 데이터 패킷을 네트워크를 통하여 방송하는 것이 가능한 추가의 모듈을 내포하는 디지털 텔레비젼 수신기(DTV2)(510)를 또한 포함한다. 이 기능들은 사실상 종래의 프리젠테이션 디바이스에서 구현되지 않았다.

<140> 이 실시예의 동작 방법은 도 2 및 도 4와 관련하여 설명한 방법과 유사하다.

<141> 먼저, 단말기/컨버터 카드(511)는 비밀 키(K_{N1})를 수신하기 위해 도메인 N1에서 초기화되어야 한다. 상기 카드(511)는, 예를 들면, "버진" 단말기 모듈의 모습으로 프리젠테이션 디바이스의 종래의 단말기 모듈(이하, "단말기 카드"라고 부른다)을 내포하는 카드 대신에 삽입되어, 도메인 N1의 네트워크의 "원조" 단말기 모듈로부터 비밀 키(K_{N1})를 수신하고, 그 다음에 "스테릴"로 된다.

<142> 그 다음에, 단말기/컨버터 카드(511)는 특히 상기 모듈 M'를 포함하는 프리젠테이션 디바이스(505)의 단말기 카드 대신에 삽입되어 도메인 N2까지 접속될 수 있다. 이것은 프리젠테이션 디바이스(505)가 (텔레비젼 수신기(510)에 통상적으로 삽입되어 있는 단말기 카드에 내포된) 도메인 N2의 비밀 키(K_{N2})를 더 이상 갖고 있지 않기 때문에 프리젠테이션 디바이스(505)의 로크아웃 상황을 발생하지 않게 하는 특수한 카드라는 것을, 텔레비젼 수신기(510)의 사용자 인터페이스에 의해 사용자에게 표시하기 위한 설비가 만들어질 수 있다.

<143> 다음에, 컨버터 모듈(514)이 대칭 키(K'_C)를 발생하고, 이 대칭 키는 도메인 N2의 프리젠테이션 디바이스, 예를 들면, 디바이스 502에 의해 해독되어 도 3에 도시된 것과 동일한 단계들을 구현함으로써 $E\{K_{N2}\}(K'_C)$를 얻는다.

<144> 그 다음에, 도메인 N1에서 기록된 콘텐츠는 디지털 비디오 카세트 레코더(503)로부터 프리젠테이션 디바이스(505)로 방송될 수 있고, 이어서, 프리젠테이션 디바이스(505)가 디바이스 M을 교체하고 프리젠테이션 디바이스(502)가 프리젠테이션 디바이스(202)를 교체하여, 도 4에 도시된 방법과 동일한 방식으로 방법이 수행된다.

<145> 도 6은 도메인 N1에서 "비공개 복사"로서 기록된 콘텐츠를 도메인 N2 용의 "판독 전용" 유형의 콘텐츠로 변환할 수 있는 본 발명의 제3 실시예를 도시한다.

<146> 도 6에서는 디지털 비디오 카세트 레코더(603), 소스 디바이스(601) 및 프리젠테이션 디바이스(602)가 접속된 디지털 버스(604)를 포함하는 도메인 N2의 디지털 도메스틱 네트워크를 도식적으로 표시하였다.

<147> 프리젠테이션 디바이스(602)는 "LECM 유닛" 모듈(623)을 내포한 텔레비젼 수신기(DTV)(620) 및 단말기 모듈(622)을 내포한 스마트 카드(621)를 포함한다.

<148> 이 실시예에서, 도메인 N2 용의 콘텐츠의 변환을 수행하는 디바이스 M은, 내부에 통상적으로 위치된 소스 디바이스의 컨버터 모듈을 내포하는 스마트 카드 대신에, 소스 디바이스(601)에 삽입되는 단말기 모듈(612) 및 컨버터 모듈(614)을 내포하는 스마트 카드(611)(이하, "단말기/컨버터" 카드라고 부른다)에 의해 구현된다. 소스 디바이스(601)는 "ECM 유닛" 모듈(613) 및 우리가 M"라고 부르고 LECM 메시지를 수신된 데이터 패킷으로부터 추출할 수 있는 추가의 모듈을 내포하는 디지털 디코더(610)를 또한 포함한다. 이 기능은 사실상 종래의 소스 디바이스에서 구현되지 않았다.

<149> 이 실시예의 동작 방법은 앞에서 설명한 2개의 실시예의 방법과 유사하다.

<150> 먼저, 단말기/컨버터 카드(611)는 비밀 키(K_{N1})를 수신하기 위해 도메인 N1에서 초기화되어야 한다. 이것은 앞에서 설명한 제2 실시예에서와 동일한 방식으로 수행된다.

<151> 그 다음에, 단말기/컨버터 카드(611)는 상기 모듈 M"를 포함하는 특수한 소스 디바이스(601)에 컨버터 카드 대

신 삽입됨으로써 도메인 N2에 접속될 수 있다. 이 카드는 조건부 액세스 모듈(도 1의 모듈 CA(14) 등) 또는 디지털 권리 관리 모듈(DRM 모듈) 대신에 단말기 모듈(612)을 갖고 있기 때문에 소스 디바이스에 의해 "특수한" 컨버터 카드로서 인식된다. 그러나, 그 동작 방법은 전적으로 종래의 컨버터 카드의 동작 방법과 유사하다.

<152> 컨버터 모듈(614)이 대칭 키(K'_C)를 발생하고, 이 대칭 키는 도메인 N2의 프리젠테이션 디바이스, 예를 들면, 디바이스 602에 의해 해독되어 도 3에 도시된 것과 동일한 단계들을 구현함으로써 $E\{K_{N2}\}(K'_C)$를 얻는다.

<153> 그 다음에, 도메인 N1에서 기록된 콘텐츠는 디지털 비디오 카세트 레코더(603)로부터 소스 디바이스(601)로 방송된다. 메시지 LECM1은 단말기 모듈(612)에 전송되기 전에 모듈 M"에 의해 수신된 데이터 패킷으로부터 추출되고, 단말기 모듈(612)은 제어 워드(CW)를 해독하여 컨버터 모듈(614)에 전송한다.

<154> 이어서, 도 4에 도시된 방법(단계 404 내지 420)과 동일한 방식으로 방법이 수행되어 소스 디바이스(601)가 도 4의 디바이스 M을 교체하고 프리젠테이션 디바이스(602)가 도 4의 프리젠테이션 디바이스(202)를 교체한다.

<155> 본 발명은 전술한 예시적인 실시예들에 제한되지 않는다. 특히, 본 발명은 네트워크가 속하는 도메인에 특정된 비대칭 키 쌍을 이용하여 데이터(특히 LECM 메시지)가 보호되고, 네트워크의 공개키가 데이터를 암호화하기 위해 소스 디바이스에 내포되며, 비공개 키가 데이터를 해독하기 위해 프리젠테이션 디바이스에 내포되는 디지털 도메스틱 네트워크에 동일하게 적용된다. 이 경우에, 디바이스 M 또는 단말기/컨버터 카드는, 초기화 단계 후에, 제1 도메인용으로 암호화된 데이터를 제2 도메인의 프리젠테이션 디바이스에 의해 해독될 수 있는 데이터로 변환할 수 있도록 제1 도메인의 비공개 키와 제2 도메인의 공개 키를 내포하여야 한다.

도면의 간단한 설명

<45> 본 발명의 다른 특징 및 장점들은 첨부 도면을 참조하여 설명하는 특수한 비제한적 실시예의 설명을 통하여 명백하게 될 것이다. 첨부 도면에 있어서:

<46> 도 1은 제1 도메인에 속하는 디바이스를 상호 접속하는 디지털 도메스틱 네트워크의 블록도이다.

<47> 도 2는 본 발명의 제1 실시예를 설명하는, 제2 도메인에 속하는 디바이스를 포함한 도메스틱 네트워크의 블록도이다.

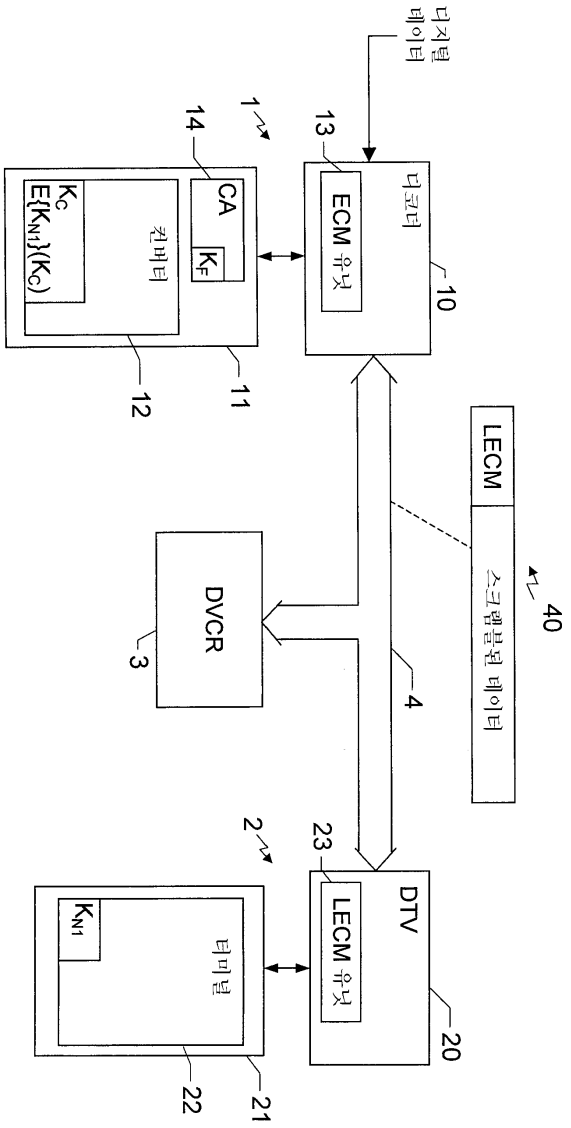
<48> 도 3은 본 발명의 제1 실시예에 따라, 도 2의 도메스틱 네트워크의 2개의 디바이스 사이에서 키의 교환을 설명하기 위한 타이밍도이다.

<49> 도 4a 및 도 4b는 제1 도메인에서 기록된 콘텐츠를 제2 도메인에서 (복사하지 않고) 판독하기 위해 사용할 수 있는 도 2의 도메스틱 네트워크의 디바이스들 사이에서 데이터의 교환을 설명하기 위한 타이밍도이다.

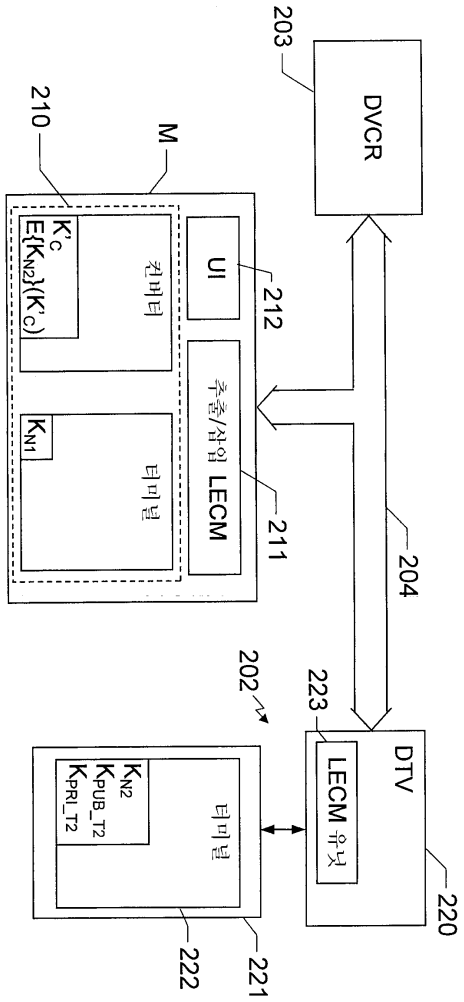
<50> 도 5와 도 6은 본 발명의 제2 실시예 및 제3 실시예를 설명하기 위한 도메스틱 네트워크의 블록도이다.

도면

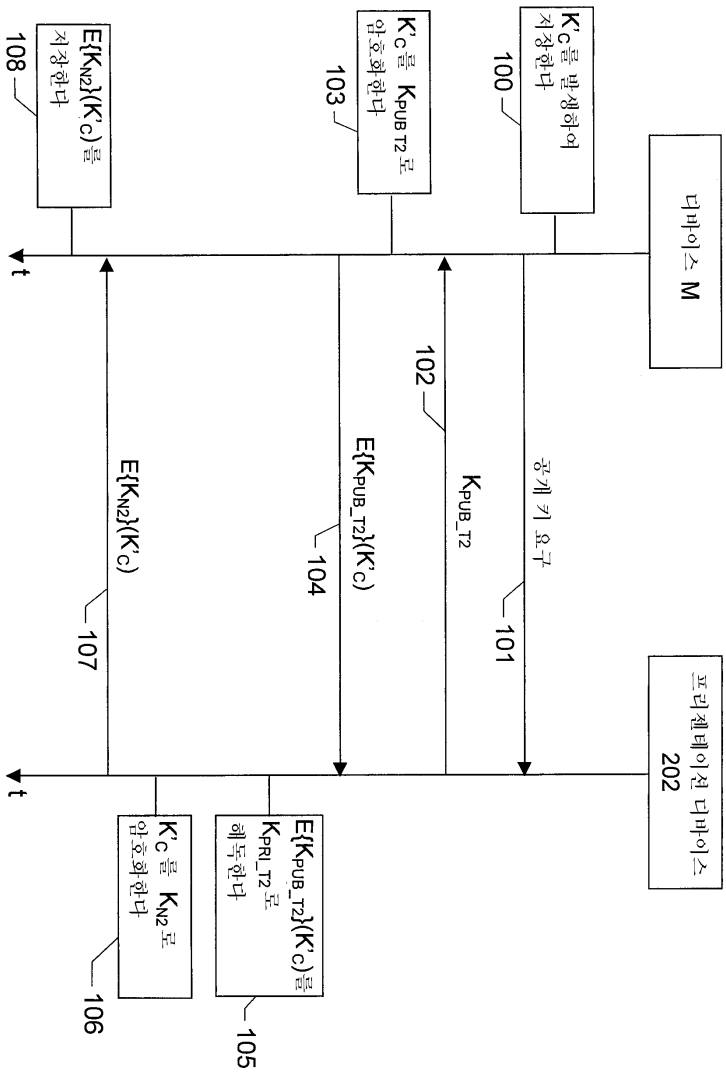
도면1


디지털 데이터
1
13
14
ECM 유닛
디코더
10
CA
K_F
K_C
$E\{K_{N1}\}(K_C)$
컨버터
12
11
LECM
스크램블된 데이터
40
DVCR
3
4
2
23
LECM 유닛
DTV
20
K_{N1}
터미널
22
21

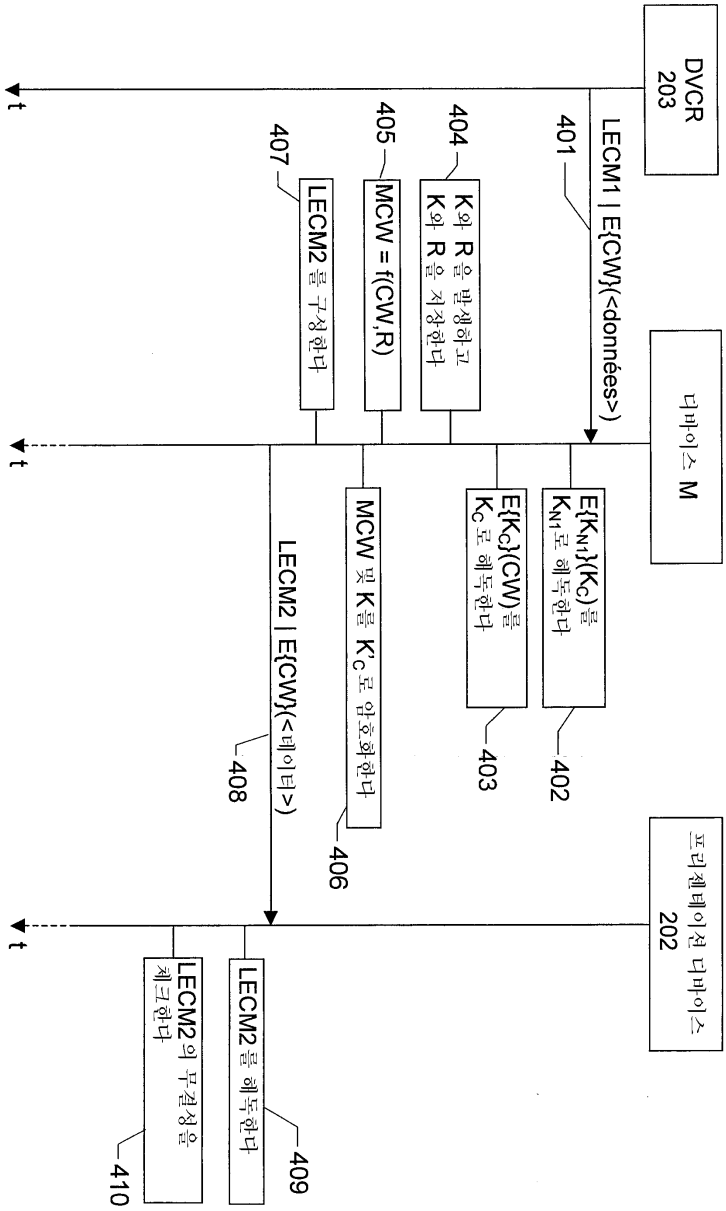
도면2


203
DVCR
210
M
K'c
E{KN2}(K'c)
컨버터
UI
212
추출/삽입 LECM
211
KN1
터미널
204
202
223
DTV
LECM 유닛
220
KN2
KPUB_T2
KPRI_T2
터미널
222
221

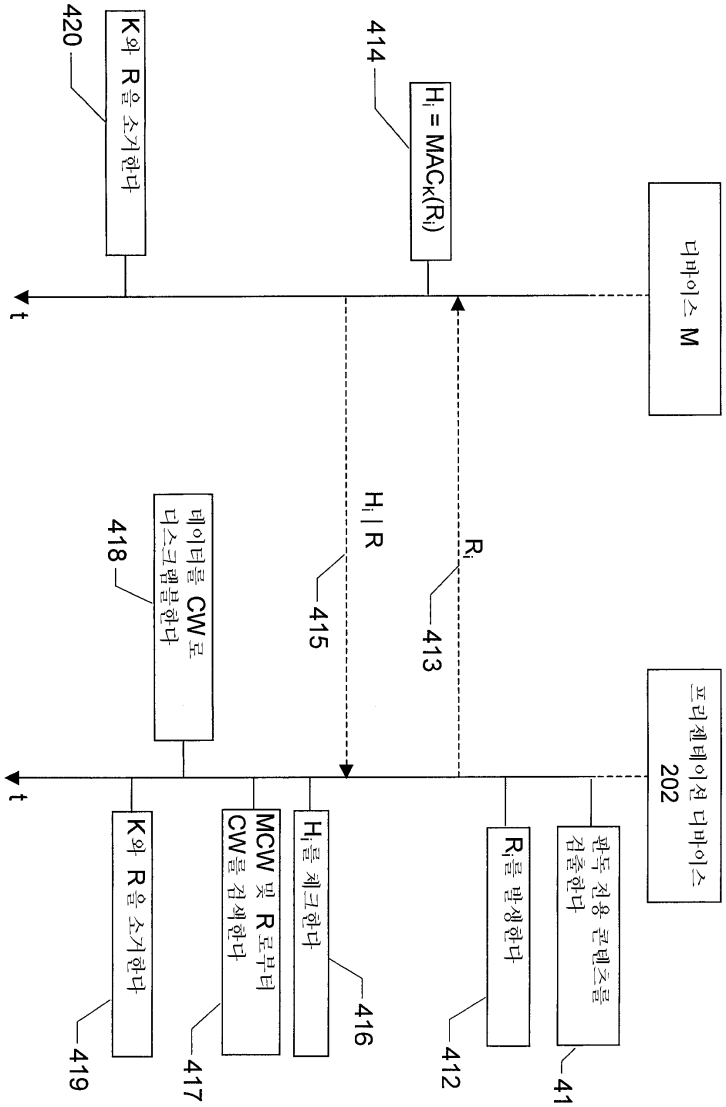
도면3


디바이스 M
프리젠테이션 디바이스 202
K'C를 발생하여 저장한다
100
공개 키 요구
101
KPUB_T2
102
K'C를 KPUB T2로 암호화한다
103
E{KPUB_T2}(K'C)
104
E{KPUB_T2}(K'C)를 KPRI_T2로 해독한다
105
K'C를 KN2로 암호화한다
106
E{KN2}(K'C)
107
E{KN2}(K'C)를 저장한다
108
t
t

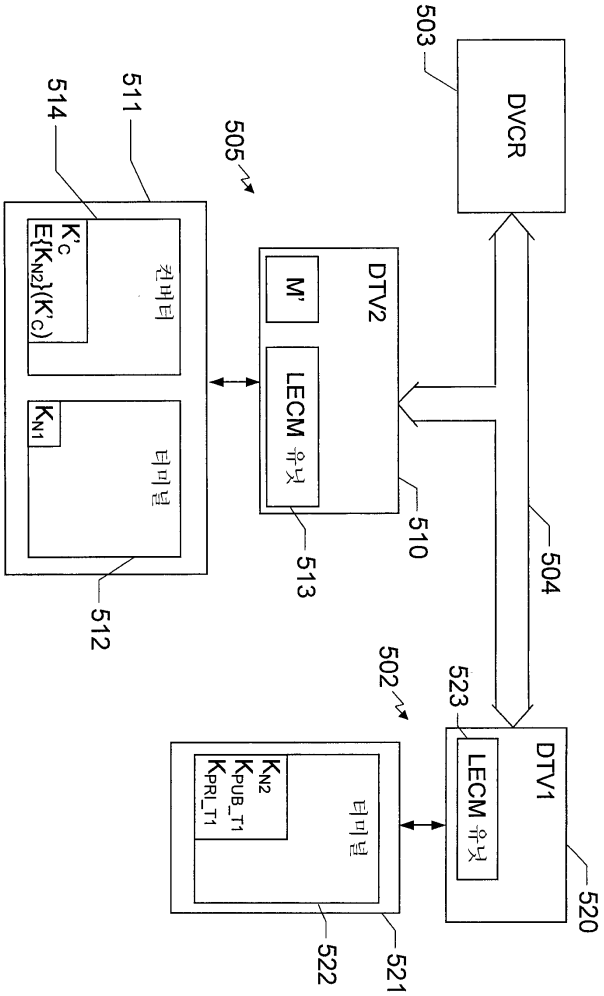
도면4a


DVCR
203
LECM1 | E{CW}(<données>)
401
디바이스 M
K와 R을 발생하고
K와 R을 저장한다
404
MCW = f(CW,R)
405
LECM2를 구성한다
407
E{KN1}(KC)를
KN1로 해독한다
402
E{KC}(CW)를
KC로 해독한다
403
MCW 및 K를 K'C로 암호화한다
406
LECM2 | E{CW}(<데이터>)
408
프리젠테이션 디바이스
202
LECM2를 해독한다
409
LECM2의 무결성을
체크한다
410
t
t
t

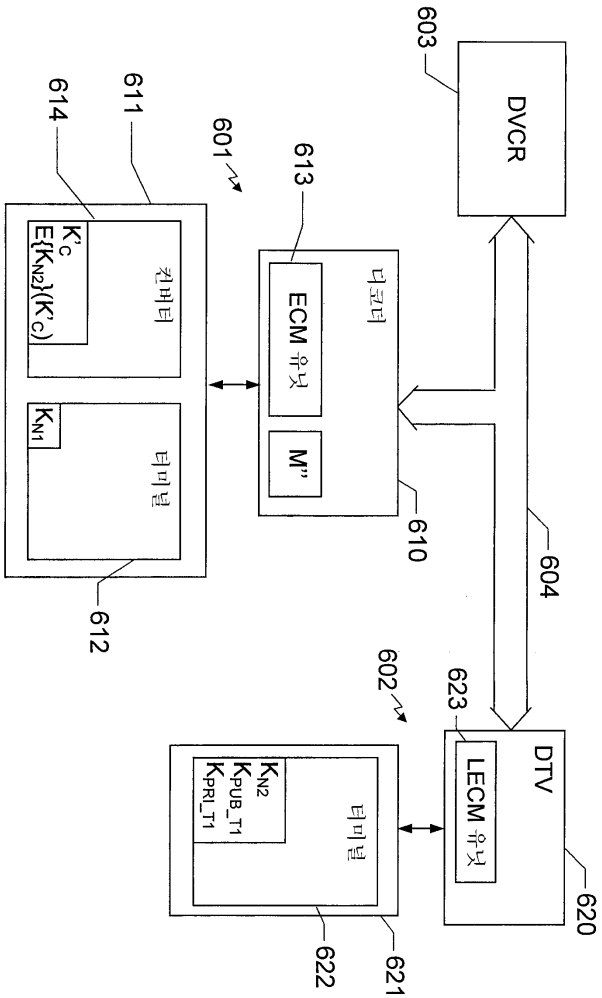
도면4b


디바이스 M
프리젠테이션 디바이스 202
414
$H_i = MAC_K(R_i)$
420
K와 R을 소거한다
R_i
413
$H_i \mid R$
415
412
R_i를 발생한다
411
펌웨어 전용 콘텐츠를 검출한다
418
데이터를 CW로 디스크램블한다
416
H_i를 체크한다
417
MCW 및 R 모듈러 CW를 검색한다
419
K와 R을 소거한다
t
t

도면5


503
DVCR
504
505
511
514
K'C
E{KN2}(K'C)
컨버터
KN1
터미널
512
DTV2
M'
LECM 유닛
510
513
502
523
LECM 유닛
DTV1
520
KN2
KPUB_T1
KPRL_T1
터미널
521
522

도면6


603
DVCR
611
614
601
613
컨버터
K'_C
$E(K_{N2})(K'_C)$
K_{N1}
터미널
ECM 유닛
M''
디코더
610
604
612
602
623
DTV
LECM 유닛
620
K_{N2}
K_{PUB_T1}
K_{PRI_T1}
터미널
622
621