(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0076606
(43) 공개일자 2009년07월13일

(51) Int. Cl.
G11B 20/10 (2006.01) *G06F 15/16* (2006.01)
(21) 출원번호 10-2008-0002651
(22) 출원일자 2008년01월09일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 매탄동 416
(72) 발명자
이대종
경기 수원시 영통구 매탄4동 매탄성일아파트 205-1212
정길수
경기 오산시 궐동 우남아파트 108-1601
(뒷면에 계속)
(74) 대리인
리앤목특허법인

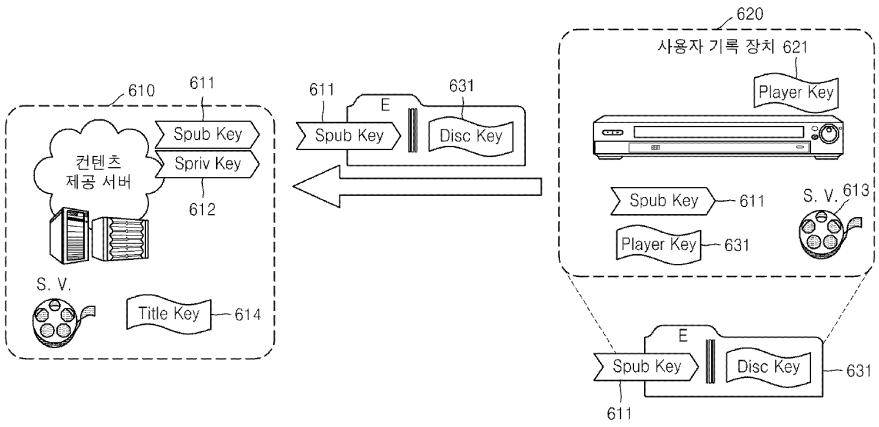
전체 청구항 수 : 총 12 항

(54) 컨텐츠 기록 방법, 타이틀 키 제공 방법, 컨텐츠 기록 장치및 컨텐츠 제공 서버

(57) 요 약

본 발명에 따라 권한없는 사용자에 의한 타이틀 키의 기록 및 복수의 디스크 기록을 방지할 수 있도록 하는 컨텐츠 기록 방법, 타이틀 키 제공 방법, 컨텐츠 기록 장치 및 컨텐츠 제공 서버가 개시된다. 본 발명에 따른, 네트워크로부터 다운로드한 컨텐츠를 기록하는 방법은, 기록 장치에서 컨텐츠를 기록할 디스크의 디스크 키로 암호화된 타이틀 키를 서버로부터 수신하는 단계와, 상기 수신된 디스크 키로 암호화된 타이틀 키와 상기 컨텐츠를 상기 디스크에 기록하는 단계를 포함하는 것이다.

대 표 도



(72) 발명자

강만석

경기 수원시 영통구 영통동 황골마을1단지아파트 134-1601

권준환

경기 수원시 영통구 영통동 황골마을1단지아파트 130-1301

유성열

경기 용인시 수지구 동천동 벽산아파트 102-1501

특허청구의 범위

청구항 1

네트워크로부터 다운로드한 컨텐츠를 기록하는 방법에 있어서,

기록 장치에서 컨텐츠를 기록할 디스크의 디스크 키로 암호화된 타이틀 키를 서버로부터 수신하는 단계와,

상기 수신된 디스크 키로 암호화된 타이틀 키와 상기 컨텐츠를 상기 디스크에 기록하는 단계를 포함하는 것을 특징으로 하는 컨텐츠 기록 방법.

청구항 2

제1항에 있어서,

상기 디스크 키로 암호화된 타이틀 키를 상기 서버로부터 수신하는 단계는,

상기 디스크 키를 상기 서버로 전송하는 단계를 포함하는 것을 특징으로 하는 컨텐츠 기록 방법.

청구항 3

제2항에 있어서,

상기 디스크 키를 상기 서버로 전송하는 단계는,

상기 서버로부터 상기 서버의 공개키를 수신하는 단계와,

상기 서버의 공개키를 이용하여 상기 디스크 키를 암호화하는 단계와,

상기 서버의 공개키를 이용하여 암호화된 상기 디스크 키를 상기 서버로 전송하는 단계를 포함하는 것을 특징으로 하는 컨텐츠 기록 방법.

청구항 4

네트워크로부터 다운로드한 컨텐츠를 기록하는 기록 장치에 타이틀 키를 제공하는 방법에 있어서,

상기 기록 장치에서 컨텐츠를 기록할 디스크의 디스크 키를 상기 기록 장치로부터 수신하는 단계와,

상기 수신된 디스크 키로 상기 타이틀 키를 암호화하는 단계와,

상기 디스크 키로 암호화된 상기 타이틀 키를 상기 기록 장치로 전송하는 단계를 포함하는 것을 특징으로 하는 타이틀 키 제공 방법.

청구항 5

제4항에 있어서,

상기 디스크 키를 상기 기록 장치로부터 수신하는 단계는,

상기 서버의 공개키를 상기 기록 장치로 전송하는 단계와,

상기 서버의 공개키를 이용하여 암호화된 상기 디스크 키를 상기 기록 장치로부터 수신하는 단계를 포함하는 것을 특징으로 하는 타이틀 키 제공 방법.

청구항 6

제4항에 있어서,

상기 수신된 디스크 키로 상기 타이틀 키를 암호화하는 단계는,

상기 서버의 공개키를 이용하여 암호화된 상기 디스크 키를 상기 서버의 개인키로 복호화하여 상기 디스크 키를 얻는 단계와,

상기 디스크 키를 이용하여 상기 컨텐츠를 암호화하는데 이용된 상기 타이틀 키를 암호화하는 단계를 포함하는

것을 특징으로 하는 타이틀 키 제공 방법.

청구항 7

네트워크로부터 다운로드한 컨텐츠를 기록하는 장치에 있어서,

다운로드한 컨텐츠를 디스크에 기록하는 기록부와,

상기 컨텐츠 및 상기 컨텐츠를 기록할 디스크의 디스크 키로 암호화된 타이틀 키를 컨텐츠 제공 서버로부터 수신하고, 상기 수신된 디스크 키로 암호화된 타이틀 키와 상기 컨텐츠를 상기 디스크에 기록하도록 상기 기록부를 제어하는 제어부를 포함하는 것을 특징으로 하는 컨텐츠 기록 장치.

청구항 8

제7항에 있어서,

상기 제어부는, 상기 디스크 키로 암호화된 타이틀 키를 상기 서버로부터 수신하기 위해 상기 디스크 키를 상기 서버로 전송하는 것을 특징으로 하는 컨텐츠 기록 장치.

청구항 9

제8항에 있어서,

데이터를 암호화/복호화하는 암호화/복호화부를 더 포함하고,

상기 제어부는, 상기 디스크 키를 상기 서버로 전송하기 위해, 상기 서버로부터 상기 서버의 공개키를 수신하여 상기 서버의 공개키를 이용하여 상기 디스크 키를 암호화하도록 상기 암호화/복호화부를 제어하고, 상기 서버의 공개키를 이용하여 암호화된 상기 디스크 키를 상기 서버로 전송하는 것을 특징으로 하는 컨텐츠 기록 장치.

청구항 10

네트워크로부터 다운로드한 컨텐츠를 기록하는 기록 장치에 타이틀 키를 제공하는 컨텐츠 제공 서버에 있어서,

데이터 암호화/복호화하는 암호화/복호화부와,

상기 기록 장치에서 컨텐츠를 기록할 디스크의 디스크 키를 상기 기록 장치로부터 수신하고, 상기 수신된 디스크 키로 상기 타이틀 키를 암호화하도록 상기 암호화/복호화부를 제어하고, 상기 디스크 키로 암호화된 상기 타이틀 키 및 상기 컨텐츠를 상기 기록 장치로 전송하는 제어부를 포함하는 것을 특징으로 하는 컨텐츠 제공 서버.

청구항 11

제10항에 있어서,

상기 제어부는,

상기 디스크 키를 상기 기록 장치로부터 수신하기 위해, 상기 서버의 공개키를 상기 기록 장치로 전송하고, 상기 서버의 공개키를 이용하여 암호화된 상기 디스크 키를 상기 기록 장치로부터 수신하는 것을 특징으로 하는 컨텐츠 제공 서버.

청구항 12

제10항에 있어서,

상기 제어부는, 상기 서버의 공개키를 이용하여 암호화된 상기 디스크 키를 상기 서버의 개인키로 복호화하여 상기 디스크 키를 얻고, 상기 디스크 키를 이용하여 상기 컨텐츠를 암호화하는데 이용된 상기 타이틀 키를 암호화하도록 상기 암호화/복호화부를 제어하는 것을 특징으로 하는 컨텐츠 제공 서버.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 권한없는 사용자에 의한 타이틀 키의 기록 및 복수의 디스크 기록을 방지할 수 있도록 하는 컨텐츠 기록 방법, 타이틀 키 제공 방법, 컨텐츠 기록 장치 및 컨텐츠 제공 서버에 관한 것이다.

배 경 기 술

<2> 최근 급속한 네트워크 인프라(Network Infra)의 발전으로 인터넷을 통한 동영상판매가 개시되고 있다. 또한 DVD 비디오 컨텐츠를 인터넷으로 다운로드하여 소비자 혹은 렌탈??에서 직접 비디오 디스크를 제조할 수 있게 하는 서비스가 일부 업체에서 시작될 예정이다. 이러한 서비스에 대해 직접 디스크를 구매하는 가격 대비 합리적인 가격이 책정된다면 소비자는 빠른 시간내에 저렴한 가격으로 고화질 비디오 컨텐츠를 가정에서 즐길 수 있게 된다.

<3> 즉, 컨텐츠 제공자(content provider)는 컨텐츠(content)를 더욱 쉽게 판매하기 위하여, 네트워크를 이용할 것이며, 사용자는 네트워크를 통하여 다양한 영화 컨텐츠를 쉽게 다운로드하는 것이 가능하다.

<4> 이와 같이, 네트워크를 통하여 다운받은 컨텐츠는 불법 복제 및 변조 가능성이 높아, 그에 대한 권익 보호의 필요성이 증대될 수 밖에 없다.

<5> 따라서, 불법 복제 및 변조를 방지하기 위한 DRM(Digital Right Management)기술의 일종으로서 CSS(Content Scrambling System) 등이 이용되고 있다. 즉, 컨텐츠 제공자는 컨텐츠를 사용자에게 배포하기 전, DRM 기술을 이용하여 해당 컨텐츠가 불법 복제 및 변조되지 않도록 하려고 한다. 따라서, DRM 기술을 적용하여 암호화된 컨텐츠를 기록매체에 기록 후 재생하기 위한 키(key)의 사용권한을 획득하는 것이 필요하고, 이러한 키를 얻기 위하여, 사용자와 컨텐츠 제공자간에 안전한 키 전송 방법이 필요해진다.

<6> DVD는 다른 매체와 달리 PC에서 직접 재생되기 때문에 하드디스크로 복제될 가능성이 많다. 따라서, 이와 같은 복사 방지를 위한 DRM으로 CSS (Content Scrambling System)을 도입하고 있다.

<7> CSS는 여러 개의 key값들을 이용하여 다단계의 암호해독(decryption) 과정을 통해 비디오 데이터를 재생할 수 있도록 하는데 이때 중요한 키는 다음과 같이 3가지로 이루어 진다.

<8> 디스크 키(Disc Key) : 암호화(encryption)된 타이틀 키(Title Key)값들을 해독하기 위하여 사용되는 암호화된 값으로서, 디스크 내부에 존재하며, 디스크 당 하나의 고유한 값을 가진다.

<9> 타이틀 키(Title Key) : 하나의 비디오 타이틀 셋 VTS (Video Title Set)에 하나의 타이틀 키가 부여되며, 이를 이용하여 VTS에 포함된 비디오 데이터 전체 혹은 일부에 적용된 암호화를 해독하기 위하여 사용되는 암호화된 값이다. 타이틀 키 값들은 각 타이틀의 헤더 섹션에 저장되어 있다.

<10> 플레이어 키(Player Key) : 모든 소비자용 DVD 재생장치 및 PC용 재생 소프트웨어에 할당되어 지는 고유한 키값으로 디스크 키를 해독하기 위하여 사용되는 값이다.

<11> CSS 암호화 된 DVD의 재생은 도 1에서와 같이 이루어진다.

<12> DVD(100)는 암호화된 디스크 키, 암호화된 타이틀 키들, 그리고 암호화된(스크램블된) 비디오 데이터를 포함한다. 재생 장치(110)는 재생 장치 내부에 저장된 플레이어 키(120)를 이용하여 암호화된 디스크 키를 해독(130)하여 디스크 키(140)를 얻고, 디스크 키(140)를 이용하여 암호화된 타이틀 키를 해독(150)하여 타이틀 키(160)를 얻는다. 그리고 타이틀 키(160)를 이용하여 암호화된 비디오 데이터를 디스크램블(170)하여 비디오 데이터를 얻어 재생한다.

<13> CSS Managed Recording(CSS 관리 기록)은 네트워크를 통해 컨텐츠를 다운로드 받아서 빈 DVD 디스크에 상업용 DVD 타이틀과 동일한 컨텐츠 보호 시스템(CSS : Content Scrambling System)을 적용하여 기록할 수 있는 기술을 말한다.

<14> 도 2는 CSS Managed Recording(CSS 관리 기록)의 개념을 설명하기 위한 참고도이다.

<15> 도 2를 참조하면, 컨텐츠 제공자(210)는 타이틀 키(230)와, 타이틀 키에 의해 CSS 암호화된 비디오 데이터(220)를 사용자(240)에게 제공한다. 사용자(240)에 의해 기록장치(250)는 타이틀 키(230)를 이용하여 디스크(270)에 암호화된 비디오 데이터(220)를 기록하며, 이때 디스크 키로 암호화된 타이틀 키(280)이 또한 디스크(270)에 기록된다. 플레이어 키로 암호화된 디스크 키(290)는 디스크에 원래 저장되어 있는 값이다.

<16> 본 발명에서 사용되는 암호화 복호화 표현을 도 3을 참조하여 간단히 설명한다.

<17> 도 3의 (a)는 A 키를 이용하여 메시지를 암호화하는 것을 의미하며, E[A 키, 메시지]로 표시할 수도 있다. 도 3의 (b)는 A 키를 이용하여 암호화된 메시지를 A 키를 이용하여 복호화하는 것을 의미하며, D[A 키, E[A 키, 메시지]로 표시할 수도 있다. 그 결과는 메시지가 된다.

<18> 이제, 도 4를 참조하여 종래 기술에 따른 CSS Managed Recording(CSS 관리 기록)의 동작을 설명한다.

<19> 도 4a를 참조하면, 컨텐츠 제공자(210)는 타이틀 키(230)와, 타이틀 키로 암호화된 컨텐츠(220)를 가지고 있다. 사용자가 가지고 있는 기록 장치(250) 내부에는 플레이어 키(260)가 내장되어 있으며, 또한 사용자 공개키(CEpub Key)(410)와 사용자 개인키(CEpriv Key)(420)는 사용자가 타이틀 키를 안전하게 전송 및 복호화하기 위하여 사용하는 공개키 셋이다. 사용자 공개키(CEpub Key)(410)와 사용자 개인키(CEpriv Key)(420)는 공개 키 암호화(Public-Key cryptography) 방식으로 생성된 키 셋이며, 동종의 디바이스 즉 동일한 모델의 기록 장치에는 동일한 키 셋을 구비한다. 공개 키 암호화(Public-Key cryptography) 방식을 좀더 설명하면, 공개키와 개인키로 이루어진 한쌍의 키를 통해 암호화하는 방식으로서, 한쌍의 키중 어느 것으로도 암호화가 가능하며 복호화하기 위해서는 다른 키를 이용한다. 일반적으로 공개키는 광범위하게 사용되어 모든 사용자가 사용할 수 있으나, 개인 키의 경우는 소유자 본인만 사용할 수 있게 된다.

<20> 도 4b를 참조하면, 사용자는 컨텐츠 제공자(210)로부터 암호화된 비디오를 기록후 재생하기 위해 필요한 타이틀 키를 안전하게 얻기 위하여 해당 타이틀 키를 암호화할 사용자 공개키(410)를 컨텐츠 제공자(210)로 전송한다.

<21> 도 4c를 참조하면, 컨텐츠 제공자(210)는 사용자로부터 수신한 사용자 공개키(410)를 이용하여 타이틀 키(230)를 암호화하여, 사용자 공개키로 암호화된 타이틀 키(430)를, 타이틀 키(230)로 암호화된 컨텐츠(220)와 함께 사용자 기록 장치(250)로 전송한다.

<22> 도 4d를 참조하면, 사용자 기록 장치(250)는 사용자 공개키로 암호화된 타이틀 키(430)를 사용자 개인키(420)로 복호화하여 타이틀 키(230)를 추출한다.

<23> 도 4e를 참조하면, 사용자 기록 장치(250)는 기록용 디스크(270)로부터, 플레이어 키로 암호화된 디스크 키(290)를 추출하고, 기록 장치(250)에 내장된 플레이어 키(260)를 이용하여, 플레이어 키로 암호화된 디스크 키(290)를 복호화하여 디스크 키(440)를 얻는다.

<24> 도 4f를 참조하면, 사용자 기록 장치(250)는 이와 같이 얻은 디스크 키(440)를 이용하여, 컨텐츠 제공 서버(210)로부터 수신한 타이틀 키(230)를 암호화하여, 디스크 키로 암호화된 타이틀 키(450)를 생성한다.

<25> 도 4g를 참조하면, 사용자 기록 장치(250)는 컨텐츠 제공 서버(210)로부터 다운로드받은 CSS 암호화된 컨텐츠(220)와, 디스크 키로 암호화된 타이틀 키(450)를 기록용 디스크(270)에 기록한다.

<26> 이제 도 5를 참조하여, 위와 같은 종래의 CSS Managed Recording(CSS 관리 기록)의 동작에서 발생할 수 있는 문제점을 설명한다.

<27> 도 5a를 참조하면, 동일한 모델에 따른 기록 장치(250)는 동일한 공개키(410) 개인키(420) 쌍을 가지고 있다. 그리고 사용자 A와 사용자 B 모두 컨텐츠 제공 서버(210)로부터 CSS 암호화된 컨텐츠를 다운로드받을 수 있다.

<28> 도 5b를 참조하면, 정당한 사용자 A는 다운로드한 컨텐츠를 기록용 디스크에 기록하기 위해 타이틀 키의 구매를 실시하려고 하며, 이를 위해 해당 타이틀 키를 암호화하기 위한 기록 장치의 공개키(410)를 컨텐츠 제공 서버(210)로 전송한다. 그러면, 컨텐츠 제공 서버(210)는 수신한 기록 장치의 공개키(410)로 타이틀 키를 암호화한다.

<29> 도 5c를 참조하면, 컨텐츠 제공 서버는 기록 장치의 공개키로 암호화된 타이틀 키(430)를 사용자 A의 기록 장치(250)로 전송하는데, 이때 권한이 없는 사용자 B에 의해 이러한 타이틀 키(430)이 가로채질(intercept) 수 있다.

<30> 도 5d를 참조하면, 기록 장치의 공개키로 암호화된 타이틀 키(430)를 가로챈 사용자 B는 사용자 A와 동일한 기록 장치에 의해 동일한 키 셋을 보유하고 있으므로, 기록 장치(250)의 개인 키(420)를 이용하여 공개키로 암호화된 타이틀 키(430)를 복호화하여 타이틀 키(230)를 추출할 수 있다. 그리고, 사용자 B는 이러한 추출된 타이틀 키(230)를 디스크 키(440)로 암호화하여, 디스크 키로 암호화된 타이틀 키(450)를 생성할 수 있으므로, 사용자 B는 타이틀 키를 구매하지 않고도 기록용 디스크에 컨텐츠를 기록가능하게 된다.

<31> 또한, 도 5e를 참조하면, 새로운 디스크(510)로부터 디스크 키(530)를 추출하여, 이 디스크 키(530)를 이용하여 타이틀 키를 암호화할 수 있으므로, 또다시 새로운 디스크(510)에 컨텐츠를 기록하는 것이 가능하다. 즉, 사용자 B는 복호화된 타이틀 키를 저장하고 있으므로, 새로운 기록용 디스크를 이용하여 매 디스크 마다 디스크 키를 추출하고, 그 추출된 디스크 키를 이용하여 타이틀 키를 암호화할 수 있으므로, 컨텐츠의 멀티플 디스크 레코딩(multiple disc recording)이 가능하게 된다.

발명의 내용

해결 하고자하는 과제

<32> 본 발명은 상기와 같은 문제점을 해결하여 권한없는 사용자에 의한 타이틀 키의 기록 및 복수의 디스크 기록을 방지할 수 있도록 하는 컨텐츠 기록 방법, 타이틀 키 제공 방법, 컨텐츠 기록 장치 및 컨텐츠 제공 서버를 제공하는 것을 목적으로 한다.

과제 해결수단

<33> 상기와 같은 과제를 해결하기 위한 본 발명의 하나의 특징은, 네트워크로부터 다운로드한 컨텐츠를 기록하는 방법에 있어서, 기록 장치에서 컨텐츠를 기록할 디스크의 디스크 키로 암호화된 타이틀 키를 서버로부터 수신하는 단계와, 상기 수신된 디스크 키로 암호화된 타이틀 키와 상기 컨텐츠를 상기 디스크에 기록하는 단계를 포함하는 것이다.

<34> 상기 디스크 키로 암호화된 타이틀 키를 상기 서버로부터 수신하는 단계는, 상기 디스크 키를 상기 서버로 전송하는 단계를 포함하는 것이 바람직하다.

<35> 상기 디스크 키를 상기 서버로 전송하는 단계는, 상기 서버로부터 상기 서버의 공개키를 수신하는 단계와, 상기 서버의 공개키를 이용하여 상기 디스크 키를 암호화하는 단계와, 상기 서버의 공개키를 이용하여 암호화된 상기 디스크 키를 상기 서버로 전송하는 단계를 포함하는 것이 바람직하다.

<36> 본 발명의 다른 특징은, 네트워크로부터 다운로드한 컨텐츠를 기록하는 기록 장치에 타이틀 키를 제공하는 방법에 있어서, 상기 기록 장치에서 컨텐츠를 기록할 디스크의 디스크 키를 상기 기록 장치로부터 수신하는 단계와, 상기 수신된 디스크 키로 상기 타이틀 키를 암호화하는 단계와, 상기 디스크 키로 암호화된 상기 타이틀 키를 상기 기록 장치로 전송하는 단계를 포함하는 것이다.

<37> 상기 디스크 키를 상기 기록 장치로부터 수신하는 단계는, 상기 서버의 공개키를 상기 기록 장치로 전송하는 단계와, 상기 서버의 공개키를 이용하여 암호화된 상기 디스크 키를 상기 기록 장치로부터 수신하는 단계를 포함하는 것이 바람직하다.

<38> 상기 수신된 디스크 키로 상기 타이틀 키를 암호화하는 단계는, 상기 서버의 공개키를 이용하여 암호화된 상기 디스크 키를 상기 서버의 개인키로 복호화하여 상기 디스크 키를 얻는 단계와, 상기 디스크 키를 이용하여 상기 컨텐츠를 암호화하는데 이용된 상기 타이틀 키를 암호화하는 단계를 포함하는 것이 바람직하다.

<39> 본 발명의 또 다른 특징은, 네트워크로부터 다운로드한 컨텐츠를 기록하는 장치에 있어서, 다운로드한 컨텐츠를 디스크에 기록하는 기록부와, 상기 컨텐츠 및 상기 컨텐츠를 기록할 디스크의 디스크 키로 암호화된 타이틀 키를 컨텐츠 제공 서버로부터 수신하고, 상기 수신된 디스크 키로 암호화된 타이틀 키와 상기 컨텐츠를 상기 디스크에 기록하도록 상기 기록부를 제어하는 제어부를 포함하는 것이다.

<40> 본 발명의 또 다른 특징은, 네트워크로부터 다운로드한 컨텐츠를 기록하는 기록 장치에 타이틀 키를 제공하는 컨텐츠 제공 서버에 있어서, 데이터 암호화/복호화하는 암호화/복호화부와, 상기 기록 장치에서 컨텐츠를 기록할 디스크의 디스크 키를 상기 기록 장치로부터 수신하고, 상기 수신된 디스크 키로 상기 타이틀 키를 암호화하도록 상기 암호화/복호화부를 제어하고, 상기 디스크 키로 암호화된 상기 타이틀 키 및 상기 컨텐츠를 상기 기록 장치로 전송하는 제어부를 포함하는 것이다.

효 과

<41> 이상과 같은 본 발명에 따르면, 권한없는 사용자에 의한 타이틀 키의 기록 및 복수의 디스크 기록을 방지할 수 있다.

발명의 실시를 위한 구체적인 내용

<42> 이제, 첨부된 도면들을 참조하여 본 발명을 상세히 설명한다.

<43> 위와 같은 문제점을 해결하기 위해 본 발명은, 다운로드받을 권한이 없는 사용자에 의하여 암호화된 타이틀 키가 가로채지더라도, 암호화된 타이틀 키를 복호화할 수 없도록, 다운로드받을 권한이 있는 사용자로부터 획득한 디스크 키에 의해 암호화된 타이틀 키를 컨텐츠 제공 서버로부터 수신하도록 하며, 다운로드받을 권한이 있는 사용자만 보유하고 있는 디스크 키를 컨텐츠 제공 서버에 안전하게 전송하기 위해 컨텐츠 제공 서버가 생성한 공개키와 개인 키를 이용한다.

<44> 도 6은 본 발명에 따라 컨텐츠 제공 서버와 사용자 기록 장치간에 데이터 송수신 과정을 설명하기 위한 참고도이다.

<45> 도 6a를 참조하면, 컨텐츠 제공 서버(610)는 공개키(611)와 개인키(612)를 가지고 있고, 또한 타이틀 키(614), 타이틀 키(614)로 암호화된 컨텐츠(613)를 가지고 있다. 사용자 기록 장치(620)는 플레이어 키(621)를 내장하고 있으며, 사용자 기록 장치(620)에서 컨텐츠를 기록할 디스크(630)에는 플레이어 키(621)로 암호화된 디스크 키(631)가 저장되어 있다.

<46> 먼저, 사용자 기록장치(620)는 컨텐츠 제공 서버(610)로부터 타이틀 키(614)로 암호화된 CSS 암호화된 컨텐츠(613)와, 서버의 공개키(611)를 다운로드받는다. 물론 암호화된 컨텐츠(613)와 서버의 공개키(611)는 반드시 같이 전송되어야 하는 것은 아니며, 별도로 전송될 수도 있다.

<47> 도 6b를 참조하면, 사용자 기록 장치(620)는 디스크(630)로부터 플레이어 키로 암호화된 디스크 키를 추출하고, 기록 장치(620)의 플레이어 키(621)를 이용하여 플레이어 키(621)로 암호화된 디스크 키를 복호화하여 디스크 키(631)를 얻는다.

<48> 도 6c를 참조하면, 사용자 기록 장치(620)는 컨텐츠 제공 서버(610)로부터 수신한 서버 공개키(611)를 이용하여 디스크 키(631)를 암호화하고, 암호화된 디스크 키를 컨텐츠 제공 서버(610)로 전송한다.

<49> 도 6d를 참조하면, 컨텐츠 제공 서버(610)는 서버 개인키(612)를 이용하여, 서버 공개키(611)로 암호화된 디스크 키(631)를 복호화함으로써, 디스크 키를 얻는다. 그리고나서, 디스크 키(631)를 이용하여, 컨텐츠를 암호화했던 타이틀 키(614)를 암호화한다.

<50> 도 6e를 참조하면, 컨텐츠 제공 서버(610)는 디스크 키(631)로 암호화된 타이틀 키(614)를 사용자 기록 장치(620)로 전송한다.

<51> 도 6f를 참조하면, 사용자 기록 장치(620)는 다운로드받은 CSS 암호화된 컨텐츠(613)와, 디스크 키(631)로 암호화된 타이틀 키(614)를 기록용 디스크(630)에 기록한다.

<52> 이상 설명한 바와 같은 본 발명에 따른 방법에 의하면, 다운로드 권한이 없는 사용자 B에 의하여 타이틀 키의 가로챔(interception)이 일어나는 경우, 사용자 B에 의한 데이터 기록을 방지할 수 있다.

<53> 도 7을 참조하면, 권한이 없는 사용자 B는 컨텐츠 제공 서버(610)로부터 정당한 사용자의 기록 장치(620)로 전송되는, 디스크 키(631)로 암호화된 타이틀 키(614)를 가로채더라도, 디스크 키(631)로 암호화된 타이틀 키(614)를 복호화할 디스크 키를 가지고 있지 못하기 때문에, 디스크 키(631)로 암호화된 타이틀 키(614)를 복호화할 수 없다. 즉, 디스크 키는 각 디스크 마다 고유한 값이기 때문에 사용자 B는 자신이 가지고 있는 디스크의 디스크 키를 이용하여, 암호화된 타이틀 키(614)를 복호화할 수 없다.

<54> 만약 사용자 B가 사용자 A의 디스크 키를 얻기 위해 도 6c에서 전송되는 서버 공개키(611)로 암호화된 디스크 키(631)를 가로챈다고 하더라도, 이러한 서버 공개키(611)로 암호화된 디스크 키(631)를 복호화하는 것 또한 불가능하다. 즉, 서버 공개키(611)로 암호화된 디스크 키(631)는 서버 개인키를 이용하여 복호화하여야 하는데 사용자 B는 서버 개인키를 가질 수 없기 때문이다.

<55> 도 8은 본 발명에 따른 컨텐츠 제공 서버(810)와 기록 장치(830)의 블록도이다.

<56> 도 8을 참조하면, 본 발명에 따른 컨텐츠 제공 서버(810)는 사용자 기록 장치(830)에 암호화된 컨텐츠와 컨텐츠의 암호화에 이용된 타이틀 키를 제공하는 컴퓨터이다. 컨텐츠 제공 서버(810)는 암호화된 컨텐츠와 컨텐츠의 암호화에 이용된 타이틀 키를 제공하는 기능을 할 수 있다면, 어떠한 형태의 컴퓨터라도 이용될 수 있다. 또한, 컨텐츠 제공 서버(810)는 두개 이상의 컴퓨터로 구현될 수 있으며, 따라서, 암호화된 컨텐츠를 제공하는 컴퓨터

와 컨텐츠의 암호화에 이용된 타이틀 키를 제공하는 컴퓨터는 분리될 수 있다.

<57> 본 발명에 따른 사용자 기록 장치(830)는 기록용 디스크(840)에 암호화된 컨텐츠와 컨텐츠의 암호화에 이용된 타이틀 키를 기록하는 장치로서, 기록용 디스크(840)에 암호화된 컨텐츠와 컨텐츠의 암호화에 이용된 타이틀 키를 기록하는 기능을 할 수 있다면 어떠한 형태의 기록 장치라도 이용될 수 있다.

<58> 컨텐츠 제공 서버(810)와 사용자 기록 장치(830)는 통신망(820)을 통해서 연결된다. 즉, 컨텐츠 제공 서버(810)와 사용자 기록 장치(830)는 통신망(820)을 통해서 암호화된 컨텐츠 및 컨텐츠의 암호화에 이용된 타이틀 키를 안전하게 전달하도록 송수신되는 그 밖의 키들을 송수신한다.

<59> 컨텐츠 제공 서버(810)는 통신부(811), 암호화/복호화부(812), 제어부(813)를 포함한다.

<60> 통신부(811)는 암호화된 컨텐츠와, 컨텐츠의 암호화에 이용된 타이틀 키 및 그 밖의 키들을 통신망(820)을 통해서 기록 장치(830)로 전송하고 또한, 기록 장치(830)로부터 보내진 소정의 키들을 수신한다. 좀더 구체적으로, 통신부(811)는 암호화된 컨텐츠(613), 서버 공개키(611), 디스크 키로 암호화된 타이틀 키를 기록 장치(620)로 전송하고, 기록 장치(620)로부터 서버 공개키로 암호화된 디스크 키를 수신한다.

<61> 암호화/복호화부(812)는 컨텐츠 및 소정의 키들을 암호화하거나 복호화한다. 암호화/복호화부(812)는 기록 장치(820)로부터 서버 공개키로 암호화된 디스크 키를 수신하면, 서버 공개키로 암호화된 디스크 키를 서버 개인키로 복호화하여 디스크 키를 얻고, 디스크 키를 이용하여 타이틀 키를 암호화한다.

<62> 제어부(813)는 본 발명에 따른 방법에 의해 암호화된 컨텐츠 및 타이틀 키를 기록 장치(830)로 전달하는 기능을 수행하기 위한 제어를 하며, 또한, 통신부(811) 및 암호화/복호화부(812)를 제어한다.

<63> 또한 도면에는 도시되지 않았지만, 컨텐츠 제공 서버(810)는 암호화된 컨텐츠, 타이틀 키, 서버 공개키 및 개인키를 저장하는 저장부로서 메모리나 하드디스크 등을 더 포함할 수 있다.

<64> 사용자 기록 장치(830)는 통신부(821), 암호화/복호화부(822), 기록부(823), 제어부(824)를 포함한다.

<65> 통신부(821)는 암호화된 컨텐츠와, 컨텐츠의 암호화에 이용된 타이틀 키 및 그 밖의 키들을 통신망(820)을 통해서 기록 장치(830)로부터 수신하고 또한, 컨텐츠 제공 서버(810)로 보낼 소정의 키들을 전송한다. 좀더 구체적으로, 통신부(821)는 컨텐츠 제공 서버(810)로부터 서버 공개키(611), 암호화된 컨텐츠(613), 디스크 키로 암호화된 타이틀 키를 수신하며, 컨텐츠 제공 서버(810)로 서버 공개키로 암호화된 디스크 키를 전송한다.

<66> 암호화/복호화부(822)는 소정의 키들을 암호화하거나 복호화한다. 즉, 암호화/복호화부(822)는 디스크에 저장된 암호화된 디스크 키를 독출하여 기록 장치의 플레이어 키로 암호화된 디스크 키를 복호화하여 디스크 키를 얻는다. 그리고, 얻어진 디스크 키를 서버 공개키로 암호화한다.

<67> 기록부(823)는 컨텐츠 제공 서버(810)로부터 수신한 암호화된 컨텐츠 및 디스크 키로 암호화된 타이틀 키를 기록용 디스크(840)에 기록한다.

<68> 제어부(824)는 본 발명에 따른 방법에 의해 암호화된 컨텐츠 및 타이틀 키를 컨텐츠 제공 서버(810)로부터 수신하여 이를 디스크(840)에 기록하는 기능을 수행하기 위한 제어를 하며, 또한, 통신부(821), 암호화/복호화부(822) 및 기록부(823)를 제어한다. 또한 기록 장치(830)는 플레이어 키를 내장하고 있다.

<69> 도 9는 본 발명에 따라 기록 장치에서의 암호화된 컨텐츠를 기록하는 방법의 흐름도이다.

<70> 도 9를 참조하면, 기록 장치에서 컨텐츠를 기록할 디스크의 디스크 키로 암호화된 타이틀 키를 컨텐츠 제공 서버로부터 수신한다(910). 컨텐츠 제공 서버로부터, 디스크 키로 암호화된 타이틀 키를 제공받기 위해 기록장치는 기록 장치에서 컨텐츠를 기록할 디스크의 디스크 키를 컨텐츠 제공 서버로 전송할 수 있다. 또한, 컨텐츠 제공 서버로 보내는 디스크 키는 서버의 공개키를 이용하여 암호화될 수 있다.

<71> 수신된 디스크 키로 암호화된 타이틀 키와 컨텐츠를 디스크에 기록한다(920).

<72> 도 10은 본 발명에 따라 컨텐츠 제공 서버에서 타이틀 키를 기록 장치로 제공하는 방법의 흐름도이다.

<73> 도 10을 참조하면, 기록 장치에서 컨텐츠를 기록할 디스크의 디스크 키를 기록 장치로부터 수신한다(1010). 안전한 송수신을 위해 기록 장치로부터 수신하는 디스크 키는 서버의 공개키를 이용하여 암호화될 수 있으며, 이를 위해 컨텐츠 제공 서버는 기록 장치로 서버의 공개키를 전송할 수 있다.

<74> 수신된 디스크 키로 타이틀 키를 암호화한다(1020). 수신된 디스크 키가 서버의 공개키로 암호화되어 있다면

컨텐츠 제공 서버는 서버의 개인키를 이용하여 서버의 공개키로 암호화된 디스크 키를 복호화하여 디스크 키를 얻고, 이 얻어진 디스크 키를 이용하여 컨텐츠의 암호화에 이용된 타이틀 키를 암호화한다.

<75> 디스크 키로 암호화된 타이틀 키를 기록 장치로 전송한다(1030).

<76> 이상 설명한 바와 같은 컨텐츠 기록 방법 및 타이틀 키 제공 방법은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고, 상기 기록 재생 방법을 구현하기 위한 기능적인(function) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술분야의 프로그래머들에 의해 용이하게 추론될 수 있다.

<77> 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면의 간단한 설명

<78> 도 1은 CSS 암호화 된 DVD의 재생을 설명하기 위한 참고도,

<79> 도 2는 CSS Managed Recording(CSS 관리 기록)의 개념을 설명하기 위한 참고도,

<80> 도 3은 본 발명에서 사용되는 암호화 복호화 표현을 설명하기 위한 참고도,

<81> 도 4는 종래 기술에 따른 CSS Managed Recording(CSS 관리 기록)의 동작을 설명하기 위한 참고도,

<82> 도 5는 종래의 CSS Managed Recording(CSS 관리 기록)의 동작에서 발생할 수 있는 문제점을 설명하기 위한 참고도,

<83> 도 6은 본 발명에 따라 컨텐츠 제공 서버와 사용자 기록 장치간에 데이터 송수신 과정을 설명하기 위한 참고도,

<84> 도 7은 본 발명에 따른 데이터 송수신 과정에서 권한없는 사용자의 가로챔이 발생한 경우의 잇점을 설명하기 위한 참고도,

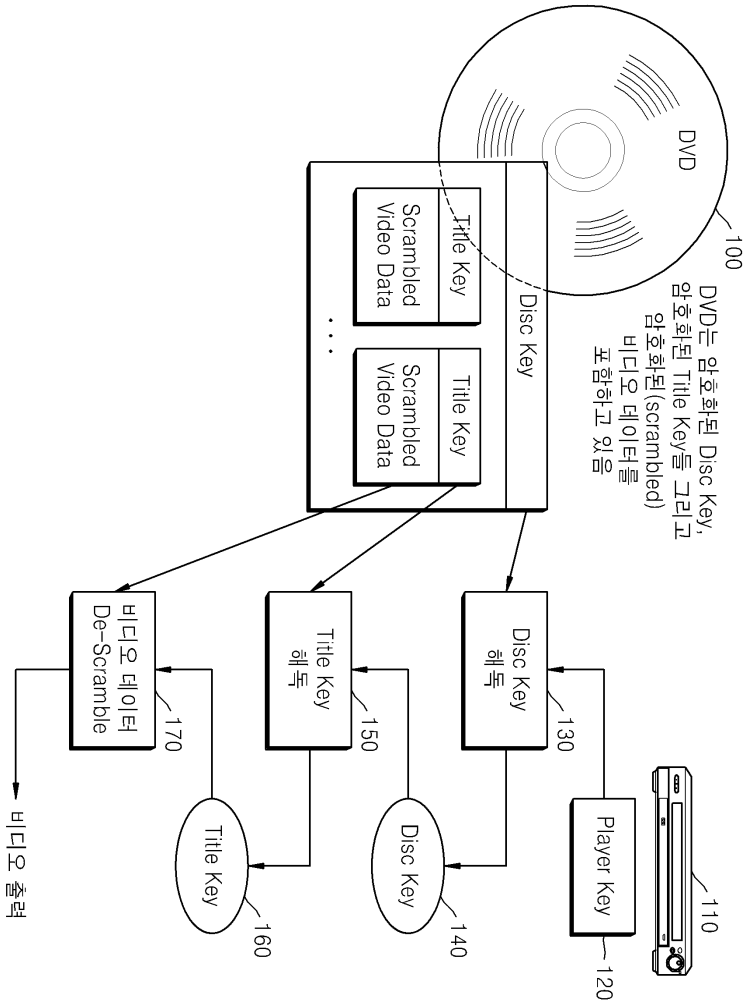
<85> 도 8은 본 발명에 따른 컨텐츠 제공 서버(810)와 기록 장치(830)의 블록도,

<86> 도 9는 본 발명에 따라 기록 장치에서의 암호화된 컨텐츠를 기록하는 방법의 흐름도,

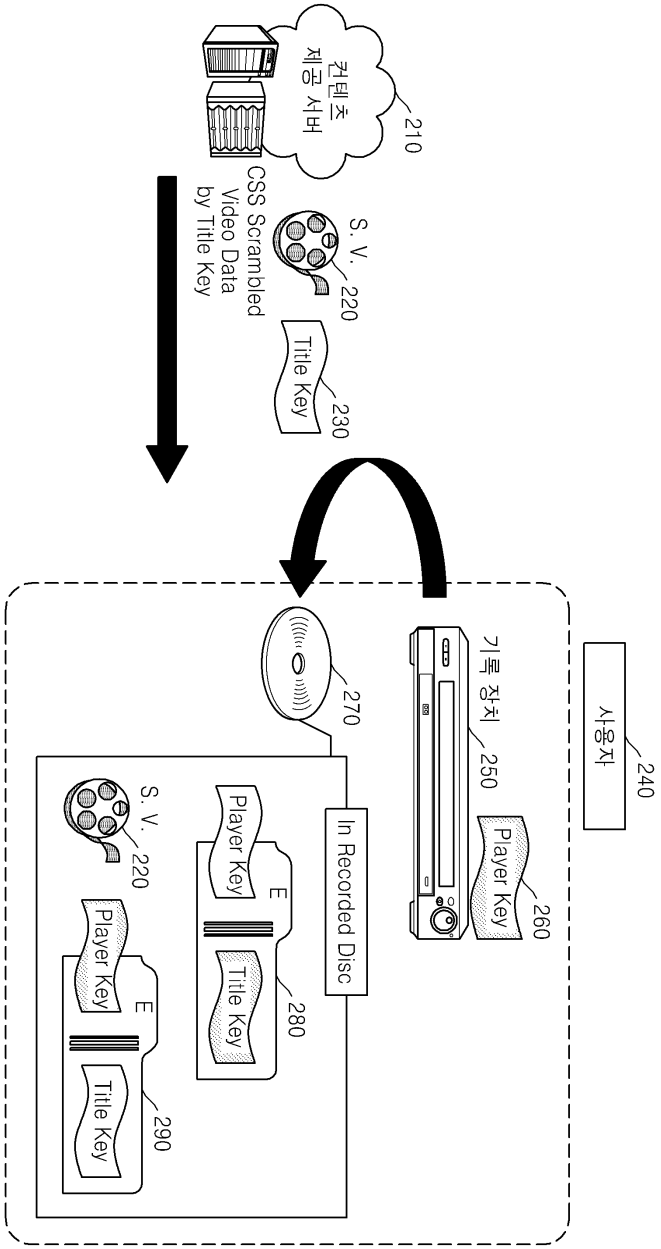
<87> 도 10은 본 발명에 따라 컨텐츠 제공 서버에서 타이틀 키를 기록 장치로 제공하는 방법의 흐름도.

도면

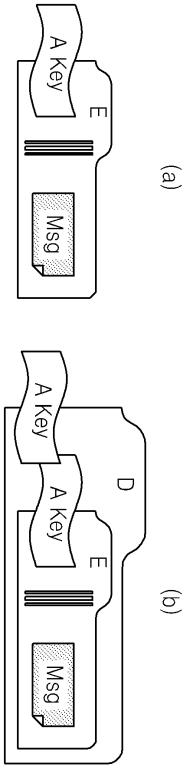
도면1


DVD
100
DVD는 암호화된 Disc Key,
암호화된 Title Key들 그리고
암호화된(scrambled)
비디오 데이터를
포함하고 있음
Disc Key
Title Key
Scrambled
Video Data
Title Key
Scrambled
Video Data
...
Disc Key
해독
130
Title Key
해독
150
비디오 데이터
De-Scramble
170
Player Key
120
Disc Key
140
Title Key
160
110
비디오 출력

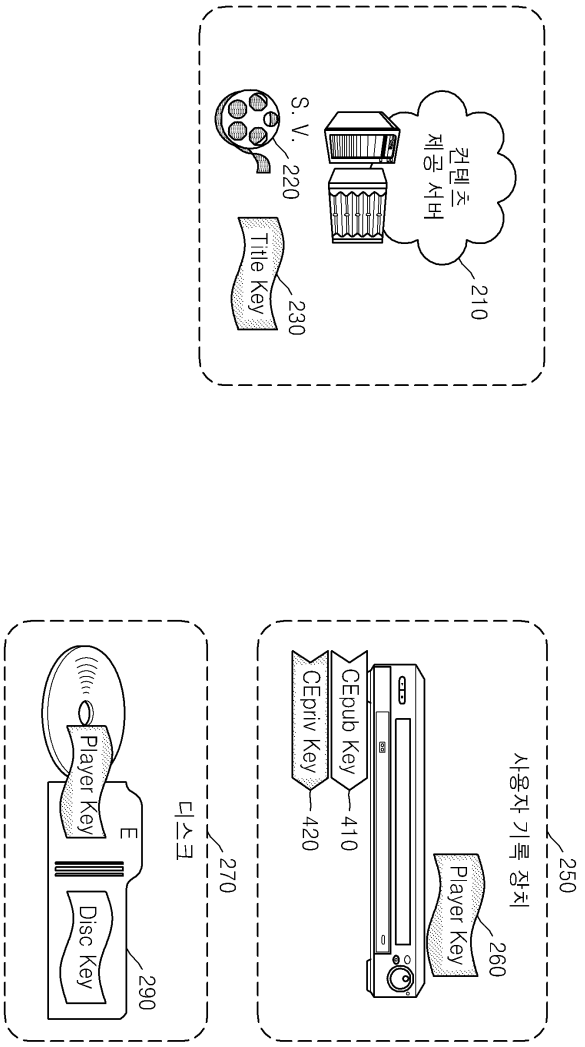
도면2


컨텐츠 제공 서버
210
CSS Scrambled Video Data by Title Key
S. V.
220
Title Key
230
사용자
240
기록 장치
250
Player Key
260
270
In Recorded Disc
S. V.
220
Player Key
E
Title Key
280
Player Key
E
Title Key
290

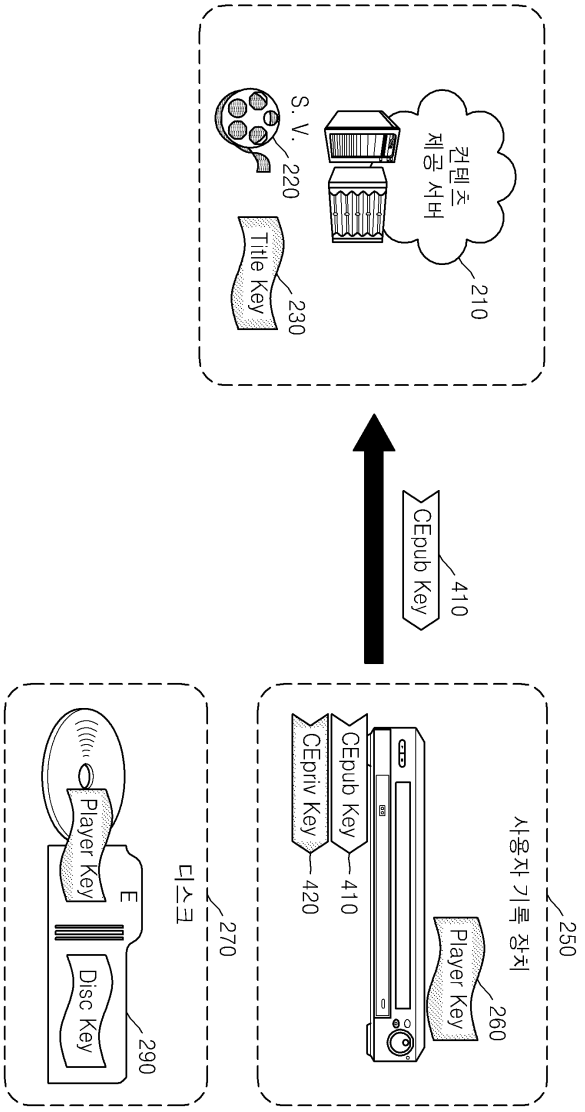
도면3



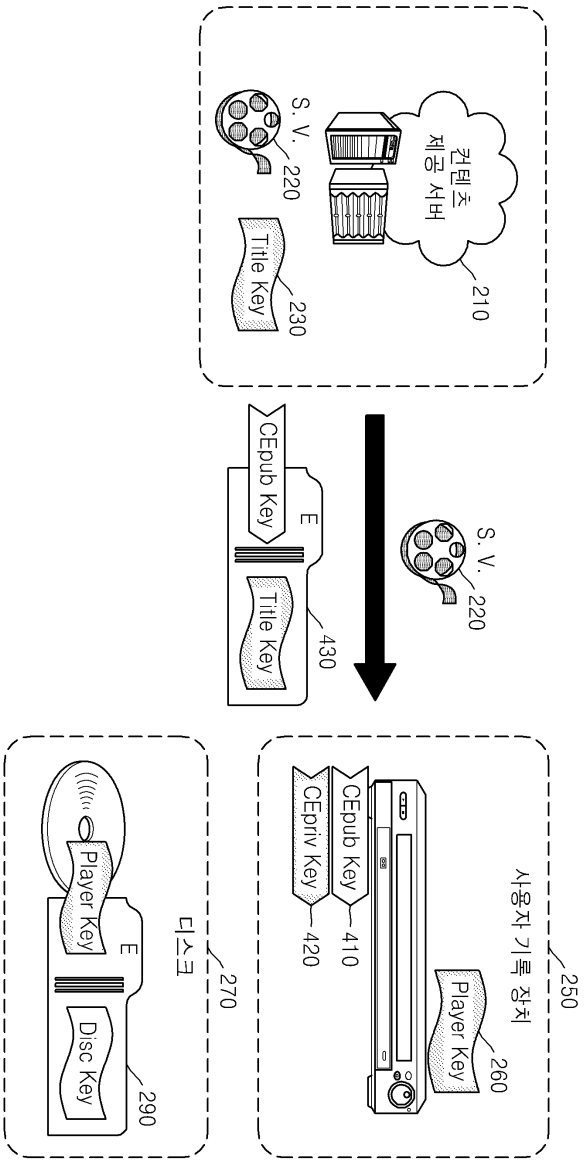
도면4a


컨텐츠
제공 서버
210
S. V.
220
Title Key
230
사용자 기록 장치
250
CEpub Key
410
CEpriv Key
420
Player Key
260
디스크
270
Player Key
Disc Key
290

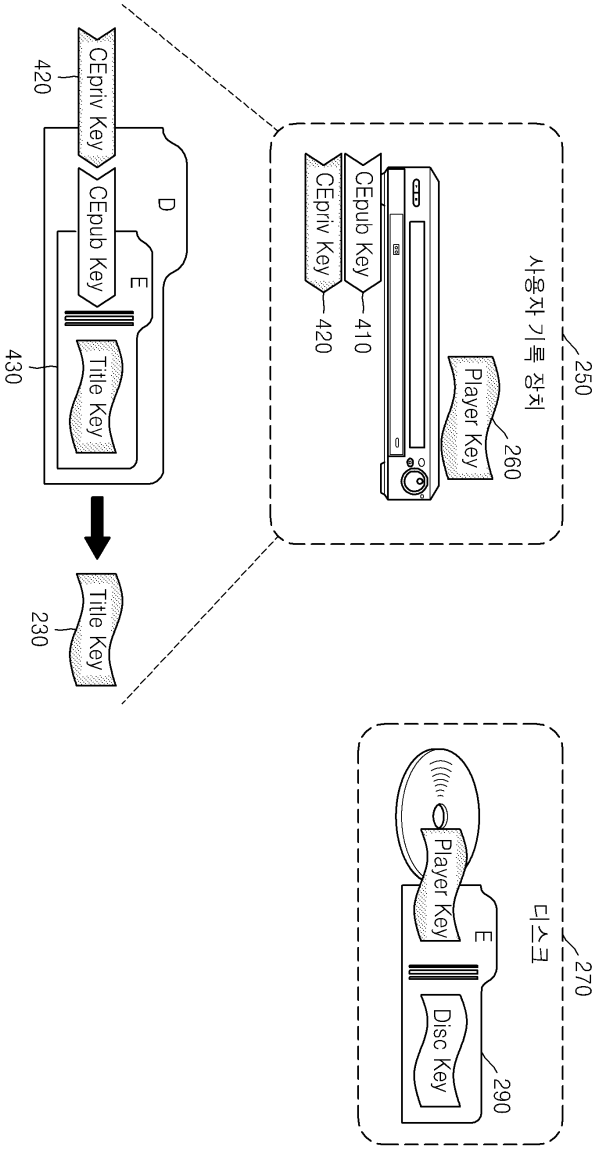
도면4b


컨텐츠
제공 서버
210
S. V.
220
Title Key
230
CEpub Key
410
사용자 기록 장치
250
CEpriv Key
CEpub Key
410
420
Player Key
260
디스크
270
Player Key
Disc Key
290

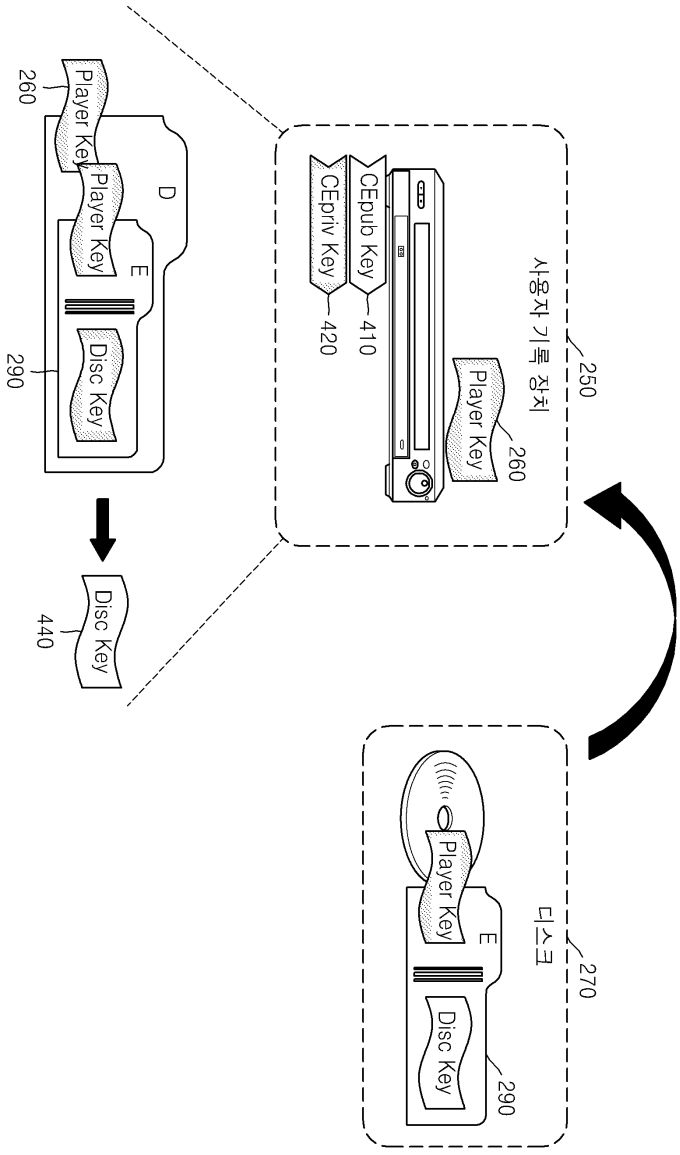
도면4c


컨텐츠
제공 서버
210
S. V.
220
Title Key
230
CEpub Key
E
Title Key
430
S. V.
220
사용자 기록 장치
250
CEpriv Key
420
CEpub Key
410
Player Key
260
디스크
270
Player Key
E
Disc Key
290

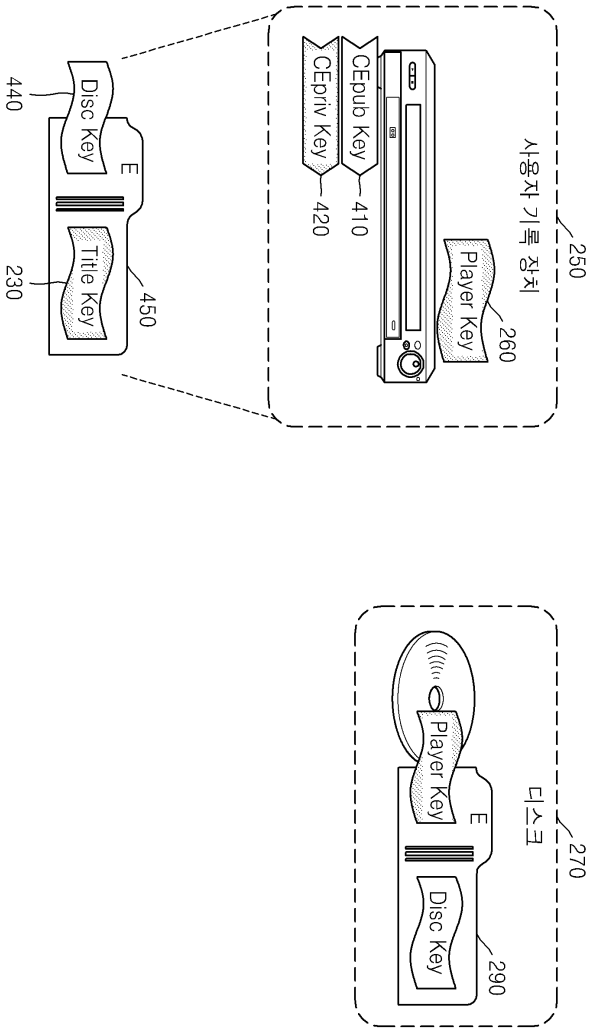
도면4d


CEpriv Key
420
CEpub Key
D
E
Title Key
430
Title Key
230
사용자 기록 장치
250
CEpriv Key
420
CEpub Key
410
Player Key
260
디스크
270
Player Key
E
Disc Key
290

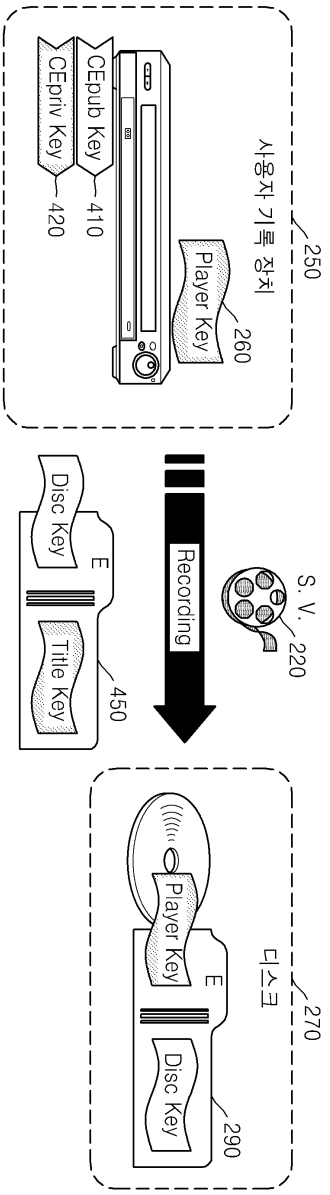
도면4e


사용자 기록 장치
250
CEpub Key
410
CEpriv Key
420
Player Key
260
D
Player Key
260
Player Key
E
Disc Key
290
Disc Key
440
디스크
270
Player Key
E
Disc Key
290

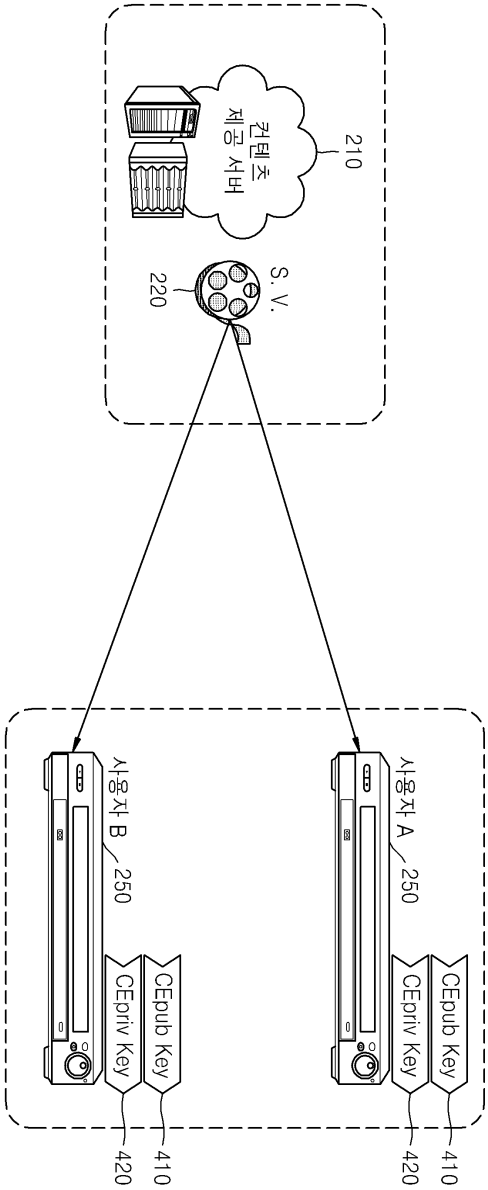
도면4f


사용자 기록 장치
250
CEpriv Key
420
CEpub Key
410
Player Key
260
Disc Key
440
E
Title Key
230
450
디스크
270
Player Key
E
Disc Key
290

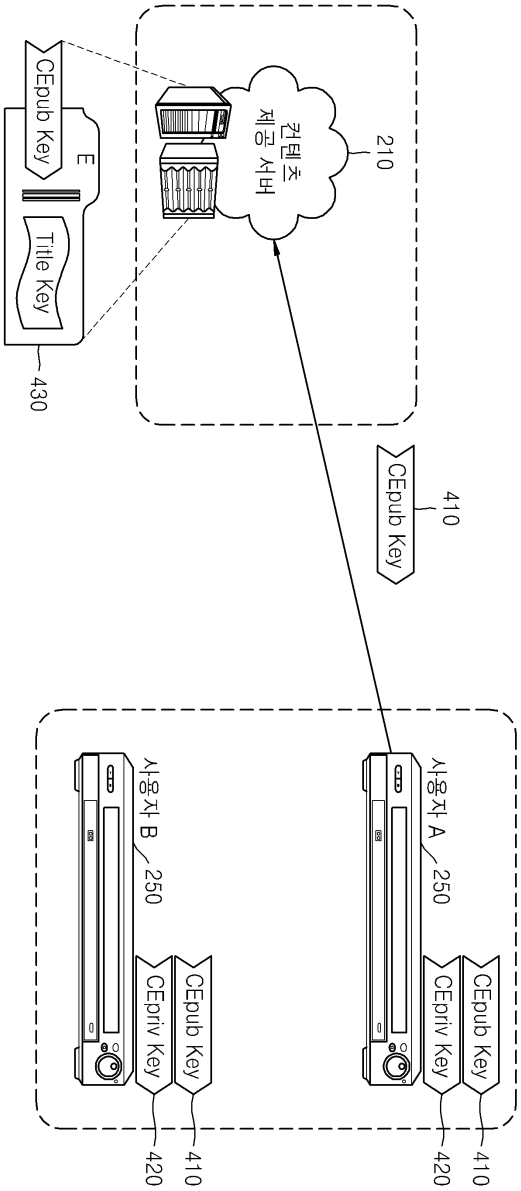
도면4g


사용자 기록 장치
250
CEpub Key
410
CEpriv Key
420
Player Key
260
Recording
S. V.
220
Disc Key
E
Title Key
450
디스크
270
Player Key
E
Disc Key
290

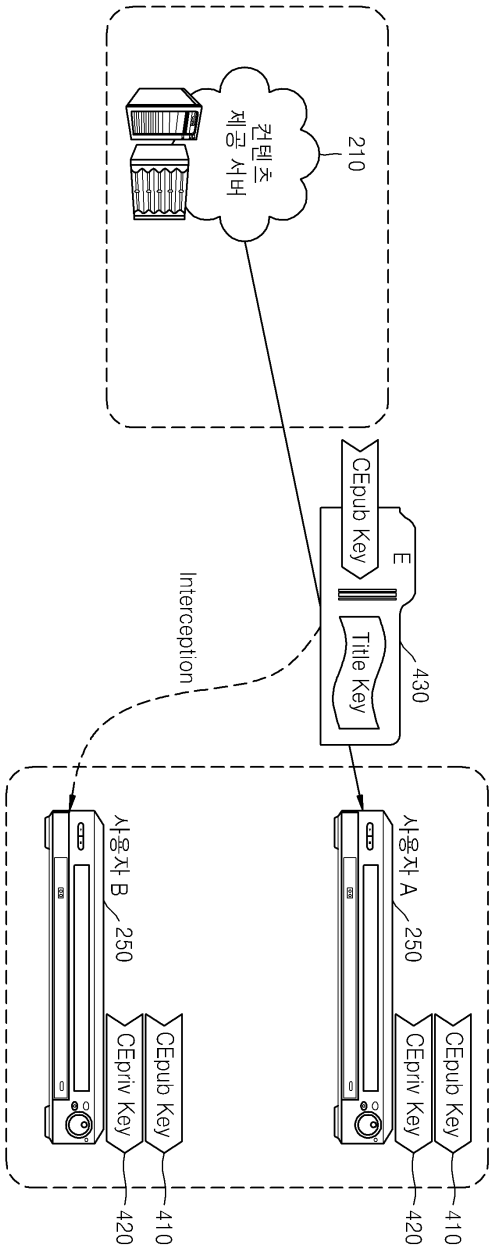
도면5a


컨텐츠
제공서버
210
S. V.
220
사용자 B
250
CEpriv Key
CEpub Key
420
410
사용자 A
250
CEpriv Key
CEpub Key
420
410

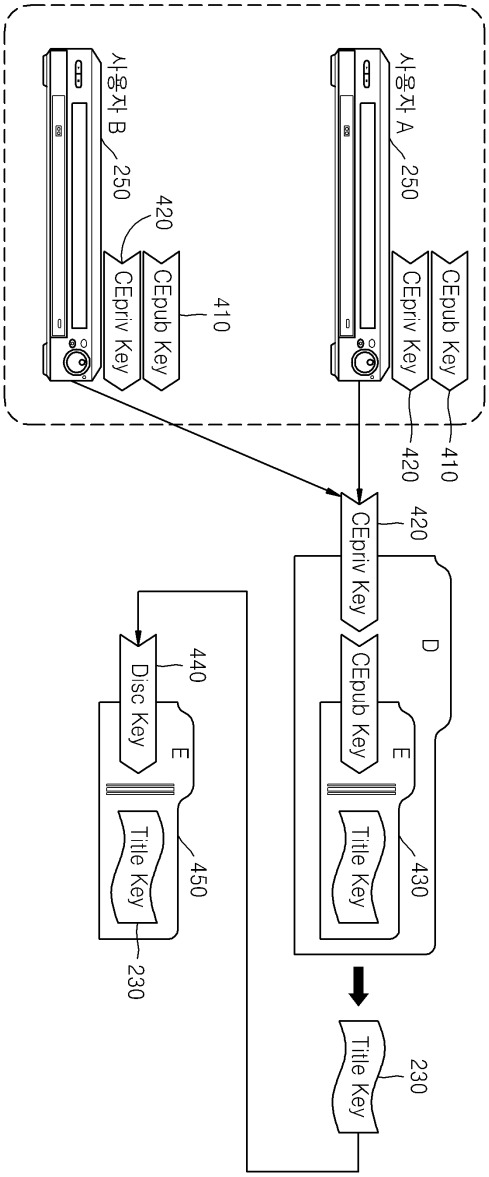
도면5b


CEpub Key
E
Title Key
430
컨텐츠
제공 서버
210
CEpub Key
410
사용자 B
250
CEpriv Key
CEpub Key
420
410
사용자 A
250
CEpriv Key
CEpub Key
420
410

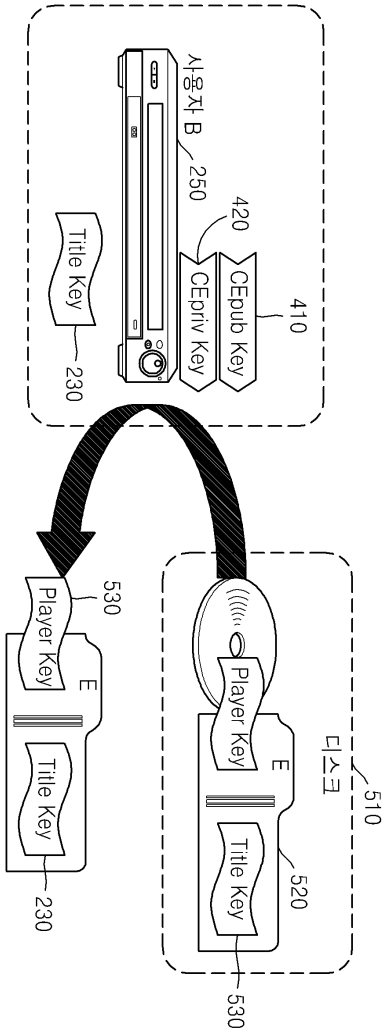
도면5c


컨텐츠 제공 서버
210
CEpub Key
E
Title Key
430
Interception
사용자 B
250
CEpriv Key
CEpub Key
420
410
사용자 A
250
CEpriv Key
CEpub Key
420
410

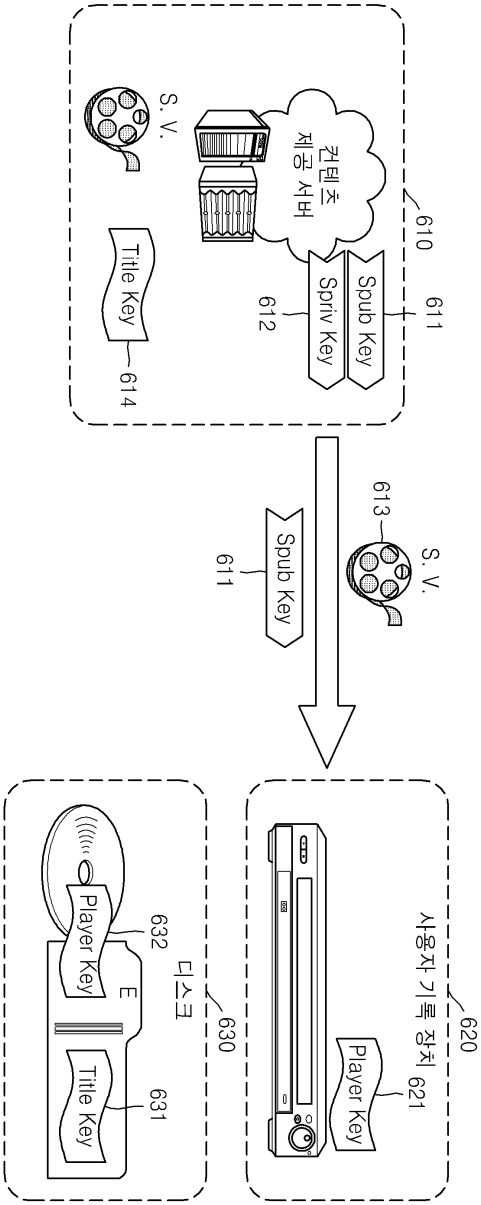
도면5d


사용자 A
250
CEpriv Key
CEpub Key
420
410
사용자 B
250
420
CEpriv Key
CEpub Key
410
CEpriv Key
420
D
CEpub Key
E
Title Key
430
Disc Key
440
E
Title Key
450
230
Title Key
230

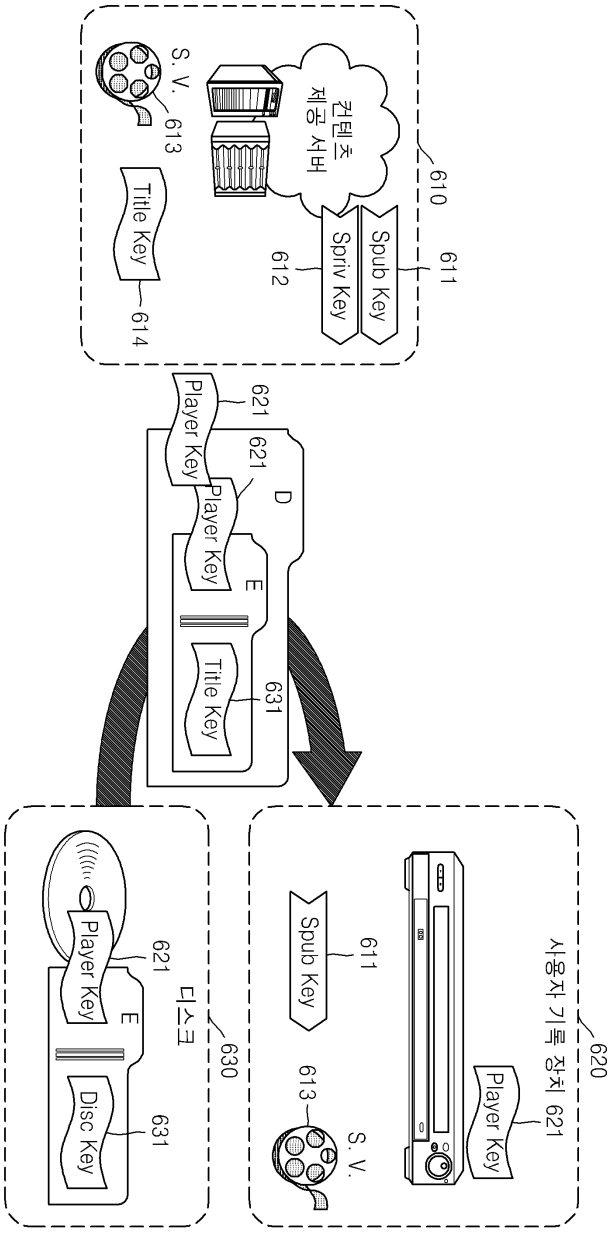
도면5e


사용자 B
250
420
CEpub Key
CEpriv Key
410
Title Key
230
530
Player Key
E
Title Key
230
Player Key
E
디스크
510
Title Key
520
530

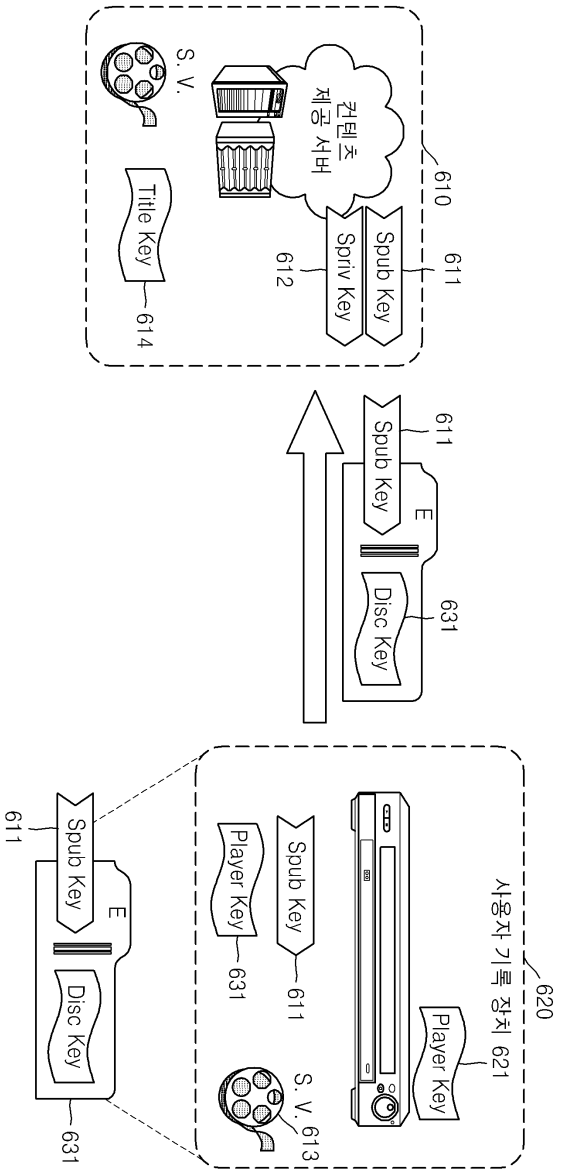
도면6a


컨텐츠
제공 서버
610
S. V.
Title Key
614
Spriv Key
612
Spub Key
611
Spub Key
611
613
S. V.
사용자 기록 장치
620
Player Key
621
디스크
630
Player Key
632
E
Title Key
631

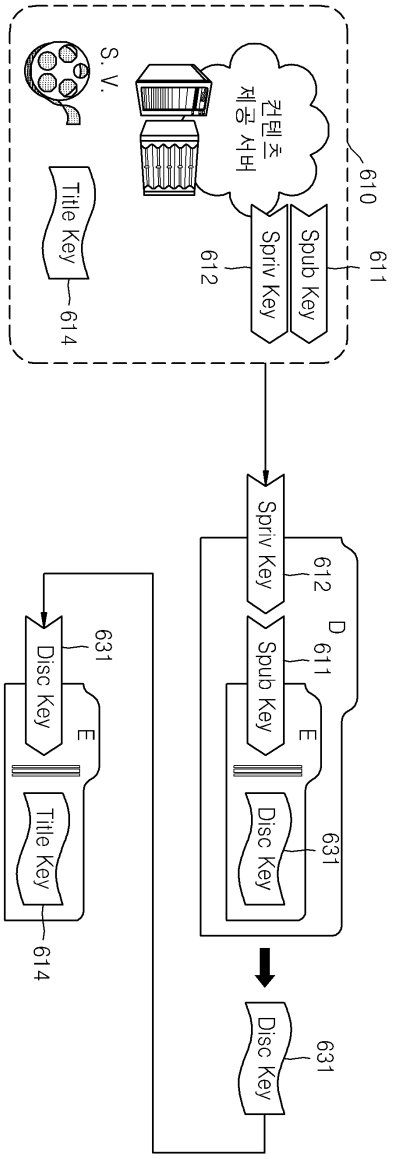
도면6b


컨텐츠
제공 서버
610
Spub Key
611
Spriv Key
612
S. V.
613
Title Key
614
Player Key
621
D
E
Title Key
631
사용자 기록 장치 621
Player Key
Spub Key
611
S. V.
613
620
디스크
630
Player Key
621
E
Disc Key
631

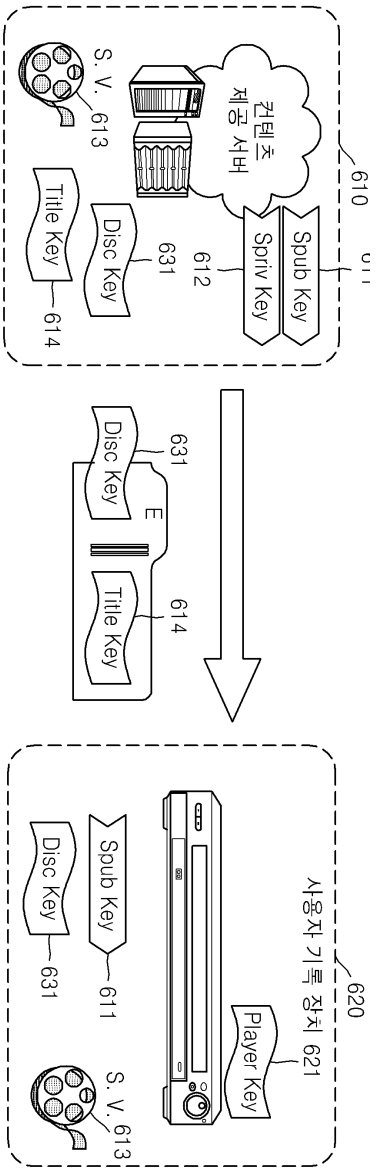
도면6c


컨텐츠 제공 서버
610
Spub Key
611
Spriv Key
612
S. V.
Title Key
614
Spub Key
611
E
Disc Key
631
사용자 기록 장치 621
620
Player Key
Spub Key
611
Player Key
631
S. V.
613
Spub Key
611
E
Disc Key
631

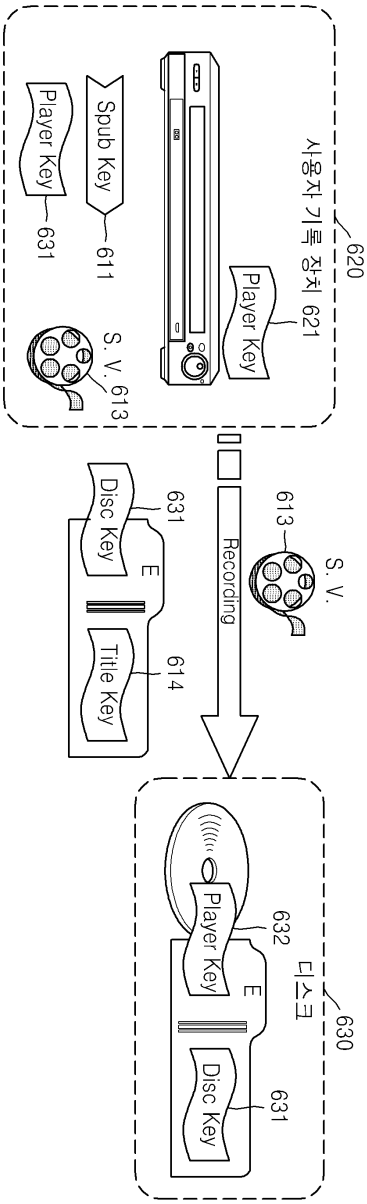
도면6d


S. V.
Title Key
614
컨텐츠 제공 서버
610
Spriv Key
612
Spub Key
611
Spriv Key
612
D
Spub Key
611
E
Disc Key
631
Disc Key
631
631
Disc Key
E
Title Key
614

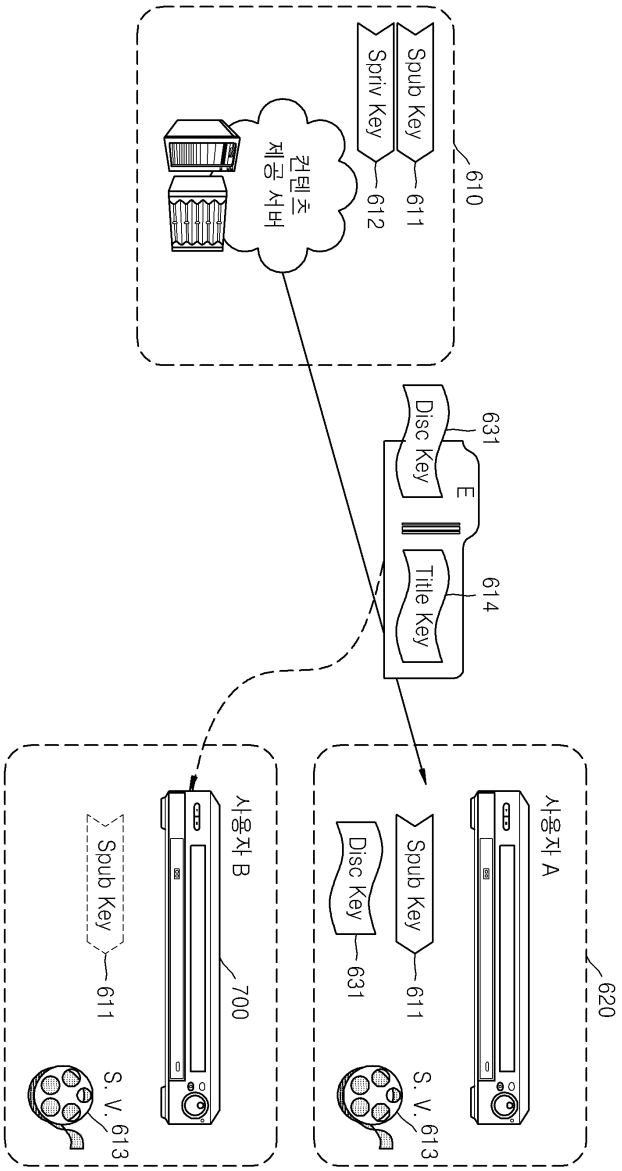
도면6e


610
컨텐츠
제공 서버
Spub Key
Spriv Key
612
Disc Key
631
Title Key
614
S. V.
613
E
620
사용자 기록 장치 621
Player Key
Sub Key
611
Disc Key
631
S. V.
613

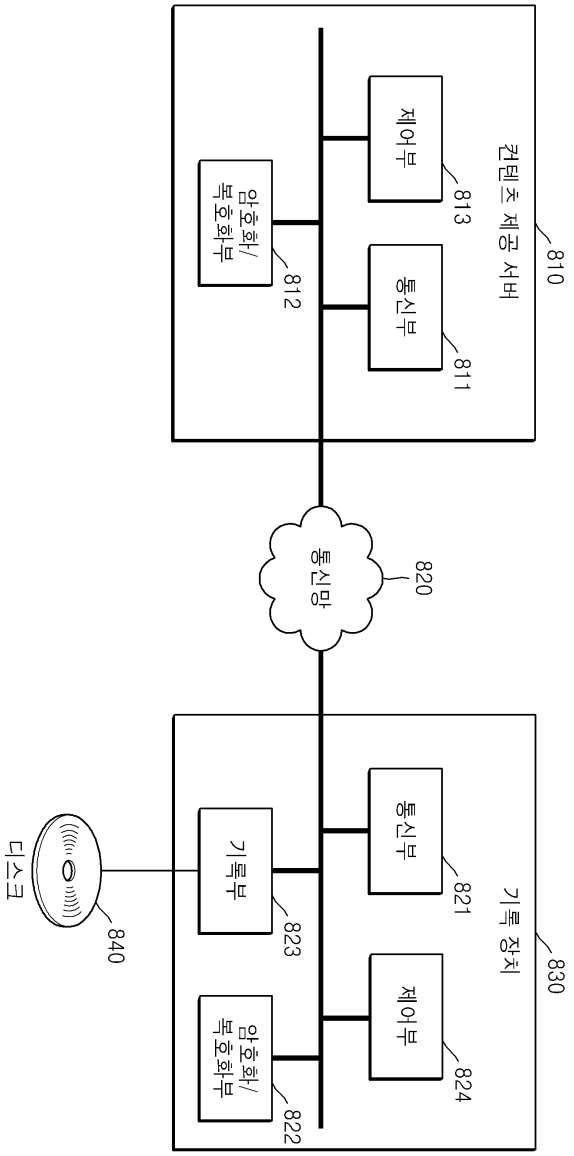
도면6f


사용자 기록 장치 621
620
Player Key
Spub Key
611
Player Key
631
S. V. 613
Recording
S. V.
613
Disc Key
631
E
Title Key
614
디스크
630
Player Key
632
E
Disc Key
631

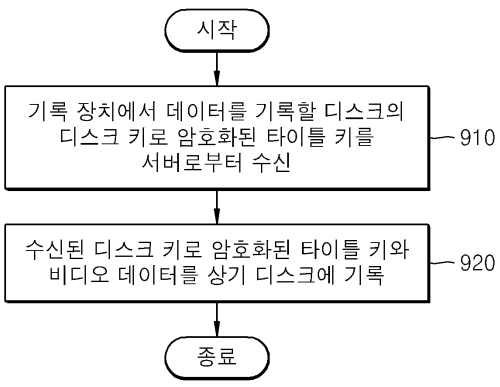
도면7


Spub Key
Spriv Key
611
612
610
컨텐츠 제공 서버
Disc Key
631
E
Title Key
614
사용자 A
Spub Key
Disc Key
631
611
S. V. 613
620
사용자 B
Spub Key
611
700
S. V. 613

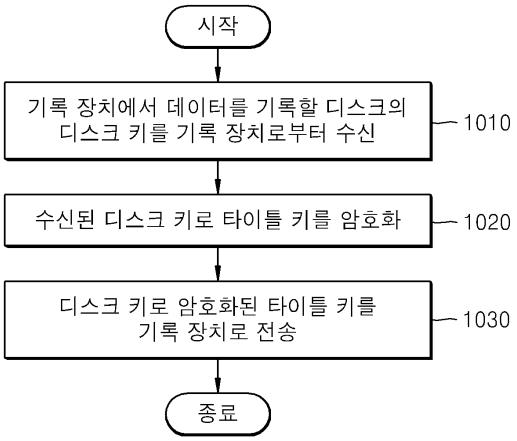
도면8


컨텐츠 제공 서버
810
제어부
813
암호화/복호화부
812
통신부
811
통신망
820
기록 장치
830
통신부
821
기록부
823
제어부
824
암호화/복호화부
822
디스크
840

도면9


시작
기록 장치에서 데이터를 기록할 디스크의 디스크 키로 암호화된 타이틀 키를 서버로부터 수신
910
수신된 디스크 키로 암호화된 타이틀 키와 비디오 데이터를 상기 디스크에 기록
920
종료

도면10


시작
기록 장치에서 데이터를 기록할 디스크의 디스크 키를 기록 장치로부터 수신
1010
수신된 디스크 키로 타이틀 키를 암호화
1020
디스크 키로 암호화된 타이틀 키를 기록 장치로 전송
1030
종료