(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
G09C 1/00

(45) 공고일자 2004년06월07일
(11) 등록번호 10-0434634
(24) 등록일자 2004년05월25일

(21) 출원번호 10-1999-0044736
(22) 출원일자 1999년10월15일

(65) 공개번호 10-2000-0029105
(43) 공개일자 2000년05월25일

(30) 우선권주장 특원평10-295829 1998년10월16일 일본(JP)
특원평11-092557 1999년03월31일 일본(JP)

(73) 특허권자 마츠시타 덴끼 산교 가부시키가이샤
일본 오오사카후 가도마시 오오아자 가도마 1006

(72) 발명자 하라다순지
일본국오오사카후오오사카시니시나리쿠다마데니시2-20-52

고즈카마사유키
미합중국캘리포니아아카디아코일애비뉴501

미나미마사타카
미합중국캘리포니아스코트로드1555버뱅크아파트103

다테바야시마코토
일본국효고켄다카라즈카시메후1-16-21

(74) 대리인 김영철

심사관 : 정재헌

# (54) 디지털 저작물인 콘텐트를 처리하는 저작물 보호시스템

요약

디지털 저작물인 디지털 콘텐트를 처리하는 본 발명의 저작물 보호시스템은 취득수단과, 제 1 콘텐트 복호수단과, 제 2 콘텐트 복호수단을 포함한다. 취득수단은 제 1 암호화가 행해지는 제 1 콘텐트와, 제 2 암호화가 행해지는 제 2 콘텐트를 포함한다. 제 2 암호화는 제 1 암호화보다 복호가 어렵다. 제 1 콘텐트 복호수단은 제 1 복호방법을 이용하여 취득된 데이터의 제 1 콘텐트를 복호한다. 제 2 콘텐트 복호수단은 제 1 복호방법보다 복잡한 제 2 복호방법을 사용하여 취득된 데이터의 제 2 콘텐트를 복호한다.

대표도

도 2

명세서

도면의 간단한 설명

도 1은 본 발명의 제 1 실시예에 의한 음악 콘텐트 재생/기록 시스템(1000)의 외관도
도 2는 본 발명의 제 1 실시예에 의한 음악 콘텐트 재생/기록 시스템(1000)의 기능 블록도
도 3은 메모리 카드 라이터(1200)의 하드웨어 구성도
도 4는 암호화된 C1 콘텐트(130)와 암호화된 C2 콘텐트를 생성하는 처리를 나타낸 데이터 흐름도
도 5는 암호화된 캡슐 고유키(110)와 암호화된 제어정보(120)를 생성하는 처리를 나타낸 데이터 흐름도
도 6은 음악 콘텐트 재생/기록 시스템(1000)에 의한 동작을 나타낸 흐름도
도 7은 메모리 카드에 오디오 데이터를 기록하기 위한 암호화 및 기록처리를 나타낸 흐름도
도 8은 본 발명의 제 2 실시예에 의한 음악 콘텐트 재생/기록 시스템(2000)의 기능 블록도
도 9는 인증 암호화부(2149, 2260)에 의한 인증 및 암호화 통신의 절차를 나 타낸 도면
도 10은 인증부(2224, 2310)에 의한 인증 및 암호화 통신의 절차를 나타낸 도면
도 11은 DES(Data Encryption Standard) 알고리즘에 따라 56비트 키를 사용하여 64비트 평문을 암호화하는 개념을 나타낸 도면

## 발명의 상세한 설명

### 발명의 목적

#### 발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 디지털 저작물의 저작권 보호를 기술적으로 실현하기 위한 시스템에 관한 것으로, 특히 디지털 저작물인 콘텐트를 재생 및 기록하는 저작권 보호기술에 관한 것이다.
최근 인터넷 관련 기술의 발전에 따라 인터넷을 통해 음악과 같은 콘텐트를 배포하고 이 배포된 콘텐트를 다운로드하는 사용자로부터 요금을 수취하는 것이 가능하게 되었다.
한편, 인터넷을 통해 퍼스널 컴퓨터에 다운로드된 디지털 저작물은 용이하게 복제될 수 있다. 인증되지 않은 복제를 방지하기 위해서는 예를들면, 암호화 기술이 사용된다.
판매용 콘텐트가 인터넷을 통해 공급될 때 낮은 품질의 콘텐트 샘플이 판매를 촉진시키기 위해 제공될 수 있다. 예컨대 사용자는 콘텐트의 공짜 샘플을 사용해 본 후 콘텐트 구입을 고려할 수 있다.
이 경우, 공급자는 가능한한 많은 사용자와 고객이 샘플을 이용해 보기를 원하기 때문에 이 샘플은 하드웨어로서 인터넷에 접속된 퍼스널 컴퓨터에 의해 재생될 수 있는 것이 바람직하다. 어떤 경우에는 공급자가 샘플의 배포를 통제하여 샘플의 일부만을 재생하도록 원할 수 있으므로 샘플의 콘텐트는 암호화되어야 할 것으로 생각된다.

#### 발명이 이루고자 하는 기술적 과제

그러나 만약 판매용 콘텐트와 샘플 콘텐트가 요구에 따라 동일한 암호화 시스템으로 암호화되어 인터넷을 통해 제공되면, 샘플의 내용에 따라 암호화 알고리즘의 분석과 같은 부정한 행위에 판매용의 콘텐트도 동일하게 공격당하게 된다. 종래의 고유키 알고리즘과 공통키 알고리즘을 결합시킨 하이브리드 암호기법을 사용하는 시스템이 미국 특허 5,343,527호에 개시되어 있다. 상기 시스템은 회복된 소프트웨어 구성요소가 최초의 발표자에 의해 재사용 라이브러리에 위치되어 있고 제 3자에 의해서는 변경되지 않는 것을 소프트웨어 재사용 라이브러리의 재사용자에게 보증하기 위해 사용되는 것으로 개시되어 있다. 하나의 알고리즘은 소프트웨어 자체를 암호화하고 복호하기 위해 사용되는 반면에, 다른 알고리즘은 상기 소프트웨어와 조합된 해시 다이제스트(hash digest)를 암호화하고 복호하기 위해 사용된다.
따라서 본 발명의 제 1 목적은 판매용 콘텐트와 시험용 콘텐트와 같이 중요도에 차이가 있는 2종류의 콘텐트가 조합되어 배포되는 경우 일반 퍼스널 컴퓨터에 의해 재생될 덜 중요한 콘텐트와 보다 중요한 콘텐트가 부정한 공격에 대해 강력하게 보호될 수 있도록 하는 저작물 보호 시스템을 제공하기 위한 것이다.
본 발명의 제 2 목적은 판매용 콘텐트를 보다 강력하게 보호하기 위해 콘텐트 등을 재생하기 위한 플레이어에 로드되는 기록매체에 콘텐트가 기록되도록 하고, 인터넷을 통해 콘텐트를 배포하는 암호화 알고리즘과 기록매체에 콘텐트를 기록하는 암호화 알고리즘 중의 하나가 다른 하나의 복호에 의해 영향을 받지 않도록 하는 저작물 보호 시스템을 제공하기 위한 것이다.
본 발명의 제 3 목적은 배포 및 기록을 위한 암호화 알고리즘이 서로의 부분을 공유하는 암호화 알고리즘을 사용함으로써 소프트웨어와 하드웨어에 의해 실현 되는 경우 원가절감을 도모할 수 있는 저작물 보호 시스템을 제공하기 위한 것이다.

### 발명의 구성 및 작용

본 발명은 제 1 암호화가 실행된 제 1 데이터와, 제 1 데이터의 콘텐트와 동일한 정보를 나타내지만 품질이 보다 낮은 콘텐트를 가지며, 제 1 암호화보다 풀기가 더 어려운 제 2 암호화가 실행된 제 2 데이터를 취득하는 취득수단(1110,

1130)과, 상기 제 1 데이터가 상기 취득수단에 의해 취득될 때 제 1 암호화에 대응하는 제 1 복호방법을 사용하여 제 1 데이터를 복호하는 제 1 데이터 복호수단(1140), 및 상기 제 2 데이터가 상기 취득수단에 의해 취득될 때 제 2 암호화에 대응하는 제 2 복호방법을 사용하여 제 2 데이터를 복호하는 제 2 데이터 복호수단(1211, 1212, 1213, 1215, 1216 및 1217)을 포함하여 멀티미디어 데이터를 보호하는 저작물 보호 시스템을 제공한다.

이러한 저작물 보호 시스템에 의해 제 1 및 제 2 콘텐트가 취득되면 상이한 2개의 중요도에 기인하여 상이한 정도의 암호화가 실행되는 각각의 콘텐트에 대하여, 제 1 및 제 2 콘텐트가 각각 별도로 복호된다. 결국 풀기 어려운 암호화에 의해 더 중요한 제 2 콘텐트를 부정행위로부터 강력하게 보호할 수 있다. 암호를 푸는 난도는 보다 복잡한 암호화 알고리즘을 사용함으로써 논리적으로 보증될 수 있으며, 예컨대 부정조작이 불가능한 하드웨어를 이용함으로써 이행 레벨에서 보증될 수 있다.

상이한 콘텐트를 복호하는 제 1 및 제 2 콘텐트 복호부를 실현하는 장치는 상이한 것일 수 있다. 예컨대 덜 중요한 콘텐트는 퍼스널 컴퓨터에 의해 복호 및 재생됨으로써 광범위하게 사용될 수 있고, 더 중요한 콘텐트는 특정목적의 장치에 의해 복호, 재생 및 기록됨으로써 부정행위에 대하여 강력하게 보호될 수 있다.

결국, 예를들면 시험용의 덜 중요한 콘텐트와 판매용의 더 중요한 콘텐트는 보안성을 갖는 네트웍과 기록매체를 통해 배포될 수 있다.

상기 저작물 보호 시스템에 있어서, 취득부와 제 1 콘텐트 복호부는 콘텐트를 복호하는 소프트웨어를 실행하는 퍼스널 컴퓨터에 의해 실현되고, 제 2 콘텐트 복호부는 부정조작이 불가능한 하드웨어와, 부정조작이 불가능한 소프트웨어를 실행하는 장치 중 어느 하나에 의해 실행되며, 제 1 콘텐트는 복호되고, 예를들면 범용 퍼스널 컴퓨터에 의해 재생될 수 있다. 한편 더 중요한 제 2 콘텐트는 복호되고 예컨대 부정행위에 대하여 강력하게 보호되는 특정목적의 하드웨어에 의해 재생 및 기록될 수 있다.

상기 저작물 보호 시스템에 있어서, 취득부는 외부 네트웍으로부터 데이터를 수신함으로써 데이터를 취득하며, 이 저작물 보호 시스템은 제 1 콘텐트 복호부에 의해 복호되는 제 1 콘텐트를 시각적 청각적으로 재생하기 위한 재생부와, 제 2 콘텐트 복호부에 의해 복호된 제 2 콘텐트에 대하여 제 2 암호화와 다른 제 3 암호화를 실행하기 위한 암호화부와, 암호화부에 의해 제 3 암호화가 실행되는 제 2 콘텐트의 적어도 일부를 기록매체에 기록하기 위한 기록부를 추가로 포함하며, 시험용의 덜 중요한 콘텐트와 판매용의 더 중요한 콘텐트가 보안성을 갖는 네트웍을 통해 배포될 수 있다. 예컨대 비디오, 음악, 정지화상 등의 디지털 저작물이 생성되는 경우 낮은 샘플링율로 표본화된 저품질의 음악 콘텐트와 비디오의 요약판과 같은 시험용의 콘텐트가 판매 촉진의 목적을 위해 보안성을 갖는 네트웍을 통해 광범위하게 배포될 수 있다. 한편 시험용 콘텐트는 퍼스널 컴퓨터에 의해 복호될 수 있으므로 일반 사용자가 광범위하게 콘텐트를 시험할 수 있으며 판매용 콘텐트는 특정목적의 하드웨어에 의해서만 메모리 카드와 같은 기록매체에 기록될 수 있으므로 높은 보안성이 보증되며 인증되지 않은 기록이 방지될 수 있다. 또한 메모리 카드와 같은 기록매체에 기록된 콘텐트는 암호화되므로 이 콘텐트가 훔쳐보여지는 것으로부터 보호될 수 있다.

게다가 제 2 콘텐트의 배포 및 기록에 대하여 상이한 암호화가 이용되므로 비록 하나의 암호화 알고리즘이 복호되더라도 그것에 의해 다른 하나가 영향을 받지는 않는다. 결국 상술한 제 2 목적이 실현된다.

상기 저작물 보호 시스템에 있어서, 암호화부와, 제 2 콘텐트 복호부와 암호화부 사이의 데이터 통신 채널은 부정조작이 불가능한 하드웨어와 부정조작이 불가능한 소프트웨어를 실행하는 장치 중의 하나에 의해 실현되므로, 기록매체에 기록하기 위한 표준에 따라 복호한 다음 판매용 제 2 콘텐트를 암호화하는 것이 필수적이다. 부정조작이 불가능한 하드웨어나 소프트웨어에 의해 복호로부터 암호화에 이르는 처리를 실행함으로써 복호후 제 2 콘텐트를 훔쳐보는 것이 방지되는 보안성을 확보할 수 있게 된다.

상기 저작물 보호 시스템에 있어서, 제 2 콘텐트 복호부에 의해 사용되는 암호화 알고리즘은 암호화부에 의해 암호화를 위해 사용되는 암호화 알고리즘과 부분 적으로 다르고, 암호화 알고리즘을 실현하는 소프트웨어나 하드웨어의 부분이 공유되므로 암호화 알고리즘을 개발하거나 실현하는데 드는 비용을 소프트웨어나 하드웨어의 부분이 공유되지 않는 경우에 비해 감축시킬 수 있다. 결국 상술한 제 3 목적이 실현된다.

본 발명의 저작물 보호 시스템은 소정의 인터페이스를 통해 퍼스널 컴퓨터에 접속하기 위한 PC 접속부와, 기록매체가 세트되는 기록매체 로딩부를 추가로 포함하며, 제 2 콘텐트 복호부, 암호화부, 기록부, PC 접속부 및 기록매체 로딩부는 하나의 하드웨어에 의해 실현되고, 제 2 콘텐트 복호부는 PC 접속부를 통해 취득부에 의해 취득된 데이터의 제 2 콘텐트를 취득하여 취득된 제 2 콘텐트를 복호하며, 기록부는 기록매체 로딩부에 세트된 기록매체에 제 2 콘텐트를 기록하고, 제 2 콘텐트의 복호로부터 기록에 이르는 처리는 하나의 특정 하드웨어에 의해 실현될 수 있으므로 비인증 기록에 대한 보안성이 보증된다.

상기 저작물 보호 시스템에 있어서, 취득부에 의해 취득되는 데이터는 취득된 데이터에 포함된 각 콘텐트에 대한 처리를 제어하며 암호화되어 있는 제어정보를 포함하며, 제 1 콘텐트 복호부와 제 2 콘텐트 복호부 중의 적어도 하나는 제어정보를 복호하기 위한 제어정보 복호부를 포함하고, 상기 저작물 보호 시스템에 있어서, 제 2 콘텐트 복호부는 제어정보 복호부를 포함하며, 제 2 콘텐트 복호부를 실현하는 퍼스널 컴퓨터는 제어정보를 복호하기 위한 소프트웨어를 실행하고, 부과금 정보와 복호조건에 관한 정보와 같은 각 콘텐트의 처리를 제어하기 위한 제어정보는 복호될 수 있으므로, 제어정보의 보안성이 보증될 수 있다.

상기 저작물 보호 시스템에 있어서, 제어정보는 제 2 콘텐트를 복호하기 위해 사용되는 키를 추가로 포함하고, 제어정보 복호부는 제 1 인증 암호화부를 포함하며, 제 2 콘텐트 복호부는 제 2 인증 암호화부를 추가로 포함하고, 제 1 인증 암호화부는 제 2 인증 암호화부의 인증을 실행하며, 제 2 인증 암호화부와 암호화 통신을 실행하고, 인증이 성공적으로 실행되었을 때 제어정보 복호부에 의해 복호된 제어정보의 키를 제 2 인증 암호화부에 송신하며, 제 2 인증 암호화부는 제 1 인증 암호화부의 인증을 실행하고, 제 1 인증 암호화부와 암호화 통신을 실행하며, 키를 취득하고, 제 2 콘텐트 복호부는 제 2 인증 암호화부가 취득한 키를 사용하여 제 2 콘텐트를 복호하며, 제 1 인증 암호화부는 인증이 성

공적으로 실행되었을 때 제 2 콘텐트를 복호하는 키를 제 2 인증 암호화부에 송신한다. 결국 키는 보안성을 갖고 송신될 수 있고, 제어정보가 복호되는 부분으로부터 제 2 콘텐트가 복호되는 부분으로 제 2 콘텐트의 비인증 복사가 실행되는 것이 방지될 수 있다.
상기 저작물 보호 시스템에 있어서, 제 1 콘텐트는 시험용 음악 콘텐트이고, 제 2 콘텐트는 판매용 음악 콘텐트로서 제 1 콘텐트보다 높은 음질을 가지며, 시험 및 판매용의 음악 콘텐트는 보안성을 갖는 네트웍 상에서 배포될 수 있다. 상기 저작물 보호 시스템은 제 1 콘텐트 복호부에 의해 복호된 제 1 콘텐트를 재생하기 위한 재생부를 추가로 포함하고, 사용자는 다운로드된 시험용 음악 콘텐트를 들을 수 있다.
상기 저작물 보호 시스템에 있어서, 암호화부는 미리 마스터키를 저장하기 위한 마스터키 저장부와, 디스크키를 생성하기 위한 디스크키 생성부와, 상기 마스 터키를 사용하여 디스크키 생성부에 의해 생성된 디스크키를 암호화하기 위한 디스크키 암호화부와, 타이틀키를 생성하기 위한 타이틀키 생성부와, 상기 디스크키를 사용하여 타이틀키 생성부에 의해 생성된 타이틀키를 암호화하기 위한 타이틀키 암호화부와, 상기 타이틀키를 사용하여 제 2 콘텐트 복호부에 의해 복호된 제 2 콘텐트의 적어도 일부를 암호화하기 위한 콘텐트 암호화부를 포함하며, 상기 기록부는 디스크키 암호화부에 의해 암호화된 디스크키와 타이틀키 암호화부에 의해 암호화된 타이틀키와, 콘텐트 암호화부에 의해 암호화된 제 2 콘텐트를 기록매체에 기록하고, 하나의 콘텐트에 디스크키와 타이틀키를 사용하여 2단의 암호화를 실행하므로 마스터키를 갖는 장치에 의해서만 콘텐트가 복호된다. 결국 기록매체에 기록되는 콘텐트는 고도로 보호되고 일반 사용자에 의한 비인증 복사가 방지될 수 있다.
또 콘텐트의 보안은 사용자에 의해 접근할 수 없는 기록매체 상의 영역에 디스크키와 타이틀키를 기록함으로써 개선될 수 있다. 기록매체가 DVD(디지털 비디오 디스크)이면 저작물 보호 시스템은 DVD 재생장치에 구비될 수 있다.
저작물 보호 시스템에 있어서, 기록매체에 고유한 고유정보는 미리 기록매체에 기록되고, 디스크키 생성부는 기록매체 상의 고유정보에 따라 디스크키를 생성하며, 또 저작물 보호 시스템에 있어서, 마스터키를 사용하여 암호화된 기록매체에 고유한 고유 디스크키는 미리 기록매체에 기록되고 암호화부는 미리 마스터키를 저장하기 위한 마스터키 저장부와, 마스터키를 사용하여 기록매체상에 고유 디스크키를 복호함으로써 디스크키를 생성하기 위한 디스크키 생성부와, 타이틀키를 생성하기 위한 타이틀키 생성부와, 디스크키를 사용하여 타이틀키 생성부에 의해 생성된 타이틀키를 암호화하기 위한 타이틀키 암호화부와, 타이틀키를 사용하여 제 2 콘텐트 복호부에 의해 복호된 제 2 콘텐트의 적어도 일부를 암호화하기 위한 콘텐트 암호화부를 포함하며, 상기 기록부는 타이틀키 암호화부에 의해 암호화된 타이틀키와 콘텐트 암호화부에 의해 암호화된 제 2 콘텐트를 기록매체에 기록하며, 상이한 기록매체에 대하여 상이한 암호화가 실행된다. 결국 암호화의 보안성이 향상된다. 한편 디스크키와 기록매체상의 고유정보를 참조함으로써 기록이 올바르게 실행되는지를 검사할 수 있게된다. 결국 기록이 정확할 때에만 재생이 실행될 수 있다.
상기 저작물 보호 시스템에 있어서, 타이틀 생성부는 제 2 콘텐트 복호부에 의해 복호된 제 2 콘텐트의 일부분인 정보에 따라 타이틀키를 생성하고, 상이한 암호화가 상이한 콘텐트에 대하여 실행된다. 결국 암호화의 보안성이 향상된다.
상기 저작물 보호 시스템에 있어서, 기록매체는 인증정보를 송신하기 위한 기록장치 인증부를 포함하며, 기록부는 기록장치 인증부로부터 송신된 인증정보에 따라 기록매체의 정확성을 판정하여 기록매체가 정확할 경우에만 제 3 암호화가 실행되는 제 2 콘텐트의 적어도 일부가 기록매체에 기록되는 기록을 실행하므로, 콘텐트를 훔쳐보는 비인증 기록을 방지할 수 있다.
저작물 보호 시스템에 있어서, 취득부에 의해 취득된 데이터는 취득된 데이터가 제 1 콘텐트를 포함하는 경우 제 1 콘텐트의 복호에 관한 부과금 정보인 제 1 콘텐트 부과금 정보를 포함하고, 취득된 데이터가 제 2 콘텐트를 포함하는 경우 제 2 콘텐트의 복호에 관한 부과금 정보인 제 2 콘텐트 부과금 정보를 포함하며, 제 1 콘텐트 복호부는 제 1 콘텐트가 복호될 때 제 1 콘텐트 부과금 정보에 따라 부과금 처리를 실행하며, 제 2 콘텐트 복호부는 제 2 콘텐트가 복호될 때 제 2 콘텐트 부과금 정보에 따라 부과금 처리를 실행하므로 콘텐트의 복호에 대하여 요금을 청구할 수 있다. 결국 콘텐트를 용이하게 판매할 수 있다. 보다 구체적으로는 복호에 대해 요금청구를 함으로써 사용자에게 콘텐트의 소유권이 주어지는 판매 시스템이 실현될 수 있다.
저작물 보호 시스템에 있어서, 제 1 암호화는 제 1 키를 이용하여 실행되며, 제 2 암호화는 제 1 키보다 데이터 크기가 큰 제 2 키를 사용하여 실행되고, 취득부에 의해 취득된 데이터는 제 1 및 제 2 키를 가지며 취득될 데이터에 포함된 각 콘텐트에 관한 처리를 제어하는 제어정보를 추가로 포함하고, 제 1 콘텐트 복호부는 제 1 키를 이용하여 제 1 콘텐트를 복호하며, 제 2 콘텐트 복호부는 제 2 키를 이용하여 제 2 콘텐트를 복호하고, 키는 콘텐트를 복호하는 장치에 고정되게 포함되지 않는다. 결국 상이한 키를 이용하여 상이한 콘텐트가 복호될 수 있다. 키의 위치는 일반 사용자에 의해 알려져 있지 않으나 키는 사용자에 의해 인식되지 않는다.
상기 저작물 보호 시스템에 있어서, 제어정보는 제 3 키와 시스템 공통키로부터 유도된 제어키를 사용하여 암호화되고, 취득부에 의해 취득된 데이터에 포함되고, 제 3 키는 제 4 키를 이용하여 암호화되고 취득된 데이터에 포함되며, 제 1 콘텐트 복호부는 미리 제 4 키에 대응하는 제 5 키와 시스템 공통키를 저장하고, 제 5 키를 이용하여 제 3 키를 복호하며, 복호된 제 3 키와 시스템 공통키로부터 제어키를 유도하고, 제어키를 이용하여 제어정보를 복호하기 위한 제 1 제어정보 복호부를 포함하며, 제 2 콘텐트 복호부는 미리 제 4 키에 대응하는 제 5 키와 시스템 공통키를 저장하고, 제 5 키를 이용하여 제 3 키를 복호하며, 복호된 제 3 키와 시스템 공통키로부터 제어키를 유도하고, 제어키를 이용하여 제어정보를 복호하기 위한 제 1 제어정보 복호부를 포함하며, 콘텐트를 복호하기 위한 키를 포함하는 제어정보는 암호화된다. 따라서, 보안성이 더욱 고도로 보호된다. 한편 복호조건과 콘텐트의 부과금 정보가 제어정보에 포함되면 이들 정보 또한 부정조작과 같은 부정행위에 대해 고도로 보호될 수 있다. 제 4 및 제 5 키가 비밀키와 비밀키에 대응하는 공개키인 것으로 가정하면 예를들어 비밀키에 종속하는 암호화가 제어정보에 대해 실행된다. 결국 콘텐트를 복호하기 위한 장치에 저장된 공개키가 복호되더라도 타원 암호시스템이 사용되면 비밀키는 알려지지 않는다. 결국 제어정보는 고도로 보호된다.

상술한 목적 및 기타의 목적과 본 발명의 특징 및 이점은 첨부도면과 관련한 다음의 상세한 설명을 통해 보다 분명해질 것이다.
이하, 본 발명의 실시예를 도 1 도 18의 첨부도면을 참조하여 상세히 설명하기로 한다.
(제 1 실시예)
본 발명의 제 1 실시예에 의한 음악 콘텐트 재생/기록 시스템에 대하여 첨부도면을 참조하여 설명하기로 한다.
(구성)
도 1은 본 발명의 제 1 실시예에 의한 음악 콘텐트 재생/기록 시스템(1000) 의 외관도이다.
음악 콘텐트 재생/기록 시스템(1000)은 통신회선(1001)을 통해 수신된 음악 콘텐트가 퍼스널 컴퓨터(1100)를 사용하여 재생되고 음악 콘텐트가 메모리 카드(1300)에 기록되는 시스템이다. 메모리 카드(1300)는 두께가 수mm, 길이와 폭이 2cm인 반도체 메모리이다. 메모리 카드(1300)는 저장용량 64메가바이트이며, 내장 제어회로를 갖는다. 사용자는 메모리 카드(1300)를 메모리 카드 재생장치에 삽입하여 메모리 카드(1300)에 기록된 음악 콘텐트를 메모리 카드 재생장치에 의해 판독 및 재생되게 하고 헤드폰 등을 통해 재생되는 음악을 즐길 수 있다.
도 1에 도시된 바와 같이 음악 콘텐트 재생/기록 시스템(1000)은 디스플레이(1191)와 키보드(1192)를 구비하는 퍼스널 컴퓨터(1100)와, 퍼스널 컴퓨터(1100)에 삽입되는 메모리 카드 라이터(writer)(1200)를 포함한다.
퍼스널 컴퓨터(1100)는 CPU, 메모리, 하드디스크 등을 포함하며, 사용자의 명령에 따라 음악 콘텐트를 재생하는 프로그램을 실행한다. 퍼스널 컴퓨터(1100)는 스피커(1193)와 통신회선(1001)에 접속되며 소위 PC 카드 슬롯이라 하는 메모리 카드 라이터 삽입슬롯(1195)을 구비한다.
메모리 카드 라이터(1200)는 PC 카드라 불리며, 메모리 카드(1300)를 삽입하기 위한 메모리 카드 삽입슬롯(1299)을 구비한다.
도 2는 본 발명의 제 1 실시예에 의한 음악 콘텐트 재생/기록 시스템(1000)의 기능블록도이다.
음악 콘텐트 재생/기록 시스템(1000)은 기능적으로 수신부(1110), 제어부(1120), 캡슐 저장부(1130), 제 1 콘텐트 처리부(1140), 재생부(1150) 및 메모리 카드 라이터(1200)를 포함한다. 음악 콘텐트 재생/기록 시스템(1000) 외에도 도 2에는 메모리 카드 라이터(1200)에 삽입되는 메모리 카드(1300)와, 수신부(1110)가 통신회선(1001)으로부터 수신하여 캡슐 저장부(1130)에 저장하는 캡슐(100)이 도시되어 있다. 여기에서 캡슐(100)은 통신회선(1001)으로부터 음악 콘텐트 재생/기록 시스템(1000)으로 입력되는 데이터이며, 음악 콘텐트에 대한 암호화된 음악 콘텐트와 암호화된 제어정보를 포함한다. 이 캡슐(100)에 대한 상세한 설명은 후술하기로 한다.
수신부(1110), 제어부(1120), 제 1 콘텐트 처리부(1140) 및 재생부(1150)는 퍼스널 컴퓨터(1100)의 메모리 내의 음악 콘텐트를 재생하기 위한 프로그램이 CPU에 의해 실행될 때 실현되는 기능을 갖는다. 캡슐 저장부(1130)는 퍼스널 컴퓨터(1100)의 하드디스크 또는 메모리 중의 한 영역이다.
음악 콘텐트를 재생하기 위한 프로그램은 사용자가 수신될 음악 콘텐트를 선택하여 사용자 명령을 재생하거나 선택된 음악 콘텐트를 기록하게 하기 위한 프로그램이다. 제어부(1120)는 키보드(1192)의 사용자 조작을 수신하여 사용자 조작에 따라 음악 콘텐트를 수신, 재생 및 기록하는 것을 명령하기 위한 기능을 갖는다.
음악 콘텐트를 수신하도록 명령을 수신하면 수신부(1110)는 캡슐, 즉 통신회선(1001)으로부터 암호화된 음악 콘텐트를 포함하는 데이터를 수신하고, 캡슐 저장부(1130)에 그 캡슐을 저장하며, 캡슐이 저장된 위치를 제어부(1120)에 알려준다. 캡슐은 예컨대 인터넷을 통해 음악 콘텐트 공급자 등으로부터 배포된다. 여기에서 는 설명의 편의를 위해 캡슐(100)이 도 2에 도시된 바와 같은 수신부(1110)에 의해 캡슐 저장부(1130)에 저장되는 것으로 가정한다.
캡슐(100)이 저장된 위치에 관한 정보와 음악 콘텐트를 재생하기 위한 명령을 제어부(1120)로부터 수신하면 제 1 콘텐트 처리부(1140)는 암호화된 C1 콘텐트(130)를 복호하는 처리를 실행하여 암호화된 C1 콘텐트(130)를 재생부(1150)에 출력한다.
16KHz의 샘플링율로 샘플링된 낮은 품질의 샘플용 음악 콘텐트와 64KHz의 샘플링율로 샘플링된 보다 높은 품질의 판매용 음악 콘텐트의 2종류의 음악 콘텐트가 있다. 본 명세서에서 샘플용 음악 콘텐트를 'C1 콘텐트'라 하고, 판매용 음악 콘텐트를 'C2 콘텐트'라 한다. 암호화된 C1 콘텐트(130)는 암호화가 완료된 C1 콘텐트이며, 암호화된 C2 콘텐트(140)는 암호화가 완료된 C2 콘텐트이다. 제 1 콘텐트 처리부(1140)의 상세한 설명에 대해서는 캡슐(100)의 콘텐트의 설명과 함께 후술하기로 한다.
재생부(1150)는 제 1 콘텐트 처리부(1140)로부터 전송된 C1 콘텐트를 재생하여 스피커(1193)로 소리를 듣게 하는 기능을 갖는다. 또한 재생부(1150)는 음악 콘텐트가 MPEG(Moving Picture Experts Group) 오디오 표준에 따라 압축되기 때문에 음악 콘텐트를 신장시킨다.
메모리 카드 라이터(1200)는 도 3에 도시된 하드웨어 구성을 갖는 PC카드이다. 메모리 카드 라이터(1200)는 캡슐(100) 내의 암호화된 C2 콘텐트(140)를 복호하고, 이 복호된 C2 콘텐트를 다른 암호문으로 암호화하여 캡슐(100)이 기록된 위 치에 이 정보를 기록하라는 명령을 제어부(1120)로부터 수신하게 되면 새롭게 암호화된 C2 콘텐트를 메모리 카드(1300)에 기록하는 기능을 갖는다.
도 3은 메모리 카드 라이터(1200)의 하드웨어 구성도이다.
도 3에 도시된 바와 같이, 메모리 카드 라이터(1200)는 CPU(1201), ROM(1202), RAM(1203), PC 인터페이스(1204), 메모리 카드 인터페이스(1205) 및 제 2 콘텐트 처리부(1210), 즉 하드웨어로서 복수의 터미널을 갖는 LSI를 포함한다. 메모리 카드 라이터(1200)에서 모든 구성요소는 버스에 의해 접속된다. 메모리 카드 라이터(1200)는 PCMCIA(Personal Computer Memory Card International Association)에 따라 PC 인터페이스(1204)를 통해 퍼스널 컴퓨터(1100)와 데이터 통신을 하며, 메모리 카드 인터페이스(1205)를 통해 메모리 카드(1300)와 데이터 통신을 한다.
여기에서 CPU(1201)는 ROM(1202)에 기록된 프로그램을 실행하고 작업영역으로서 RAM(1203)을 사용하는 메모리 카드 라이터(1200)를 제어하기 위한 구성요소이다. 제 2 콘텐트 처리부(1210)는 전류공급을 위해 리드로 감싼 부정

조작이 불가능한 LSI 패키지이다. '부정조작이 불가능'하다는 것은 비인증 액세스에 대한 보호를 의미한다. 제 2 콘텐트 처리부(1210)는 하나의 실리콘 보드, 즉 단일칩 집적회로에 형성된다. 또한 제 2 콘텐트 처리부(1210)의 내부 데이터를 전기적 물리적으로 조사하는 것은 불가능하다. 보다 구체적으로 제 2 콘텐트 처리부(1210)에서 LSI 패키지의 내부 데이터는 EEPROM에 유지되고 LSI 패키지가 개방될 때 리드가 절단된다. 이러한 조건하에서 LSI 패키지가 개방되면 LSI 패키지에 대한 전류공급이 차단되어 캐패시터에 저장된 전하로 된 내부 데이터가 소멸한다.

메모리 카드 라이터(1200)는 도 2에 도시된 바와 같이 제 2 콘텐트 처리부(1210), 메모리 카드 ID 취득부(1230), 기록부(1240)를 기능적으로 포함한다. 제 2 콘텐트 처리부(1210)는 암호화된 C2 콘텐트(140)를 복호하고 오디오 데이터를 기록하기 위해 복호된 암호화 C2 콘텐트(140)를 새롭게 암호화한다. 메모리 카드 ID 취득부(1230)는 메모리 카드(1300)의 메모리 카드 ID를 메모리 카드(1300)로부터 취득한다. 기록부(1240)는 암호화된 오디오 데이터를 메모리 카드(1300)에 기록한다. 제 2 콘텐트 처리부(1210)는 메모리 카드(1300)의 정확도의 인증을 실행하기 위한 인증부(1224)를 포함한다. 제 2 콘텐트 처리부(1210)에 의한 동작의 상세한 설명에 대해서는 후술하기로 한다.

(데이터 구조 및 관련처리)

이하, 캡슐(100)의 콘텐트에 대해 설명하기로 한다. 캡슐(100)은 저작권 보호를 위한 중립적 기구, 예컨대 저작권 보호센터에 의해 만들어진 데이터이다. 저작권 보호센터는 음악 콘텐트 공급자 등으로부터 음악 콘텐트와 음악 콘텐트에 관한 제어정보를 수신하고 그 음악 콘텐트와 제어정보를 암호화하여 캡슐(100)을 생성한다.

음악 콘텐트 재생/기록 시스템(1000)에 입력되는 캡슐(100)은 160비트의 암호화된 캡슐 고유키(110)와, 고정길이의 암호화된 제어정보(120)와, 데이터 길이가 도 2에 도시된 바와 같은 콘텐트에 따라 변할 수 있는 암호화된 C1, C2 콘텐트(130, 140)로 구성된다.

도 4는 암호화된 C1 콘텐트(130)와 암호화된 C2 콘텐트(140)를 생성하는 처리를 나타낸 흐름도이다.

도 4에 도시된 바와 같이 암호화된 C1 콘텐트(130)는 평문인 C1 콘텐트(30)를 C1 키(21)로 암호화함으로써 생성되는 데이터이다. 이 경우, C1 키(21)는 64비트 키데이터이고 블록 암호 시스템이며, 예를들어 DES(Data Encryption Standard) 알고리즘이 사용된다.

한편, 암호화된 C2 콘텐트(140)는 평문인 C2 콘텐트(40)를 C2키(25)로 암호화함으로써 생성되는 데이터이다. 이 경우, C2 키(25)는 128비트의 키데이터이고 블록 암호 시스템이며, 예를들어 DES 알고리즘에 따르는 알고리즘이 사용된다. C1 콘텐트(30)와 C2 콘텐트(40)의 각각은 MPEG 오디오 표준에 따라 압축된다.

도 5는 암호화된 캡슐 고유키(110)와 암호화된 제어정보(120)를 생성하기 위한 처리를 나타내는 데이터 흐름도이다.

도 5에 도시된 바와 같이, 암호화된 제어정보(120)는 트랜스포트키(1144)로 제어정보(20)를 암호화함으로써 생성되는 데이터이다. 여기에서 제어정보(20)는 도 4에 도시된 C1 콘텐트(30)와 C2 콘텐트(40)에 관한 정보이다. 제어정보(20)는 C1키(21), C1 어드레스(22), C1 복호조건 정보(23), C1 부과금 정보(24), C2 키(25), C2 어드레스(26), C2 복호조건 정보(27) 및 C2 부과금 정보(28)에 관한 정보이다. 한편, 암호화(3)에서는 블록 암호 시스템, 예컨대 DES 알고리즘에 따른 알고리즘이 사용된다.

여기에서 C1 어드레스(22)와 C2 어드레스(26)는 각각 암호화된 C1 콘텐트(130)의 상대 어드레스와 암호화된 C2 콘텐트(140)의 상대 어드레스이다. C1 복호조건 정보(23)와 C2 복호조건 정보(27)는 각각 C1 콘텐트(30) 및 C2 콘텐트(40)를 복호하는 조건, 예컨대 C1 콘텐트(30)와 C2 콘텐트(40)를 복호하도록 허용되는 날짜를 나타내는 정보이다. 한편 C1 부과금 정보(24)와 C2 부과금 정보(28)는 C1 콘텐트(30)와 C2 콘텐트(40)가 복호될 때 부과되는 요금, 즉 음악 콘텐트의 시험과 구매를 위한 요금에 관한 정보이다.

트랜스포트키(1144)는 저작권 보호센터가 자유롭게 결정한 160비트 키데이터이다.

한편, 암호화된 캡슐 고유키(110)는 캡슐 고유키(10)를 암호화함으로써 생성되는 데이터이며, 도 5에 도시된 바와 같은 타원 암호 시스템의 알고리즘에 따라 타원 비밀키(5)를 사용하여 트랜스포트키(1144)의 배타적 OR 논리합에 의해 취득된다. 여기에서 S1 키(1142)는 음악 콘텐트 재생/기록 시스템(1000)의 제 1 콘텐트 처리부(1140)에 저장된 S1 키와 동일한 값을 갖는 160비트 공통키이다. 타원 비밀키(5)는 K1 키(1141)와 쌍을 이루는 160비트 비밀키이며, 제 1 콘텐트 처리부(1140)에 저장된 공개키이다. 타원키에 대한 상세한 설명은 '암호화 이론의 기초'(Douglas R. Stinson, Kyoritsu Shuppan Co., Ltd.)에 기재되어 있다.

제 1 콘텐트 처리부(1140) 및 제 2 콘텐트 처리부(1210)에 의한 동작의 상세한 설명은 전술한 바와 같이 생성된 캡슐(100)의 콘텐트에 관한 프로세스를 처리하는 것으로 설명하기로 한다.

먼저 제 1 콘텐트 처리부(1140)에 의한 동작을 설명하기로 한다.

제 1 콘텐트 처리부(1140)는 K1 키(1141)와 S1 키(1142)를 저장한다. 제 1 콘텐트 처리부(1140)는 그 구성요소로서 캡슐 고유키 복호부(1143), 제어정보 복호부(1145), C1 콘텐트 복호 제어부(1146) 및 C1 콘텐트 복호부(1147)를 포함한다.

캡슐 고유키 복호부(1143)는 K1 키(1141)를 사용하여 캡슐(100)내의 암호화된 캡슐 고유키(110)를 복호하여 복호된 암호화 캡슐 고유키(110)를 출력한다. 제어정보 복호부(1145)는 트랜스포트키(1144)를 사용하여 캡슐(100) 내의 암호화된 제어정보(120)를 복호하는데, 이것은 출력 복호된 암호화 캡슐 고유키(110)와 공개키인 S1 키(1142)의 배타적 논리합의 결과이다.

C1 콘텐트 복호 제어부(1146)는 C1 콘텐트가 제어정보(20) 내의 C1 복호조건 정보(23)를 참고하여 복호될 수 있는지를 판단하는데, 이것은 복호된 암호화 제어이다. 그 결과 C1 콘텐트가 복호될 수 있는 것으로 판단되면 C1 콘텐트 복호 제어부(1146)는 C1 부과금 정보(24)를 참고하여 부과금 처리를 실행하여, C1 콘텐트 복호부(1147)에 복호명령을 보낸다. 여기에서 부과금 처리는 사용자에게 시험 부과금을 지불하도록 지시하는 통신회선(1001)을 통해 정보를 전송하기 위한 것이다. 시험 부과금이 공짜라면 정보는 전송되지 않는다.

C1 콘텐트 복호부(1147)는 제어정보(20) 내의 C1 어드레스(22)를 참조하여 암호화된 C1 콘텐트(130)의 위치를 특정하고, 제어정보(20)내의 C1 키(21)를 이용하여 암호화된 C1 콘텐트(130)를 복호하며, C1 콘텐트(30)를 재생부(150)에 출력한다. 복호 알고리즘은 블록 암호 시스템에서 도 4에 도시된 암호화(1)에 대응하는 알고리즘이다.
다음으로, 제 2 콘텐트 처리부(1210)에 의한 동작을 설명하기로 한다. 제 2 콘텐트 처리부(1210)에 의한 동작은 C2 콘텐트(40)의 복호와 메모리 카드(1300)에 기록을 위한 복호된 C2 콘텐트(40)의 재암호화로 크게 나뉘나, C2 콘텐트(40)의 복호는 상술한 제 1 콘텐트 처리부(1140)에 의한 동작과 유사하다.
제 2 콘텐트 처리부(1210)는 K2 키(1211)와 C2 콘텐트(40)의 복호를 위한 S2 키(1212)를 저장한다. 제 2 콘텐트 처리부(1210)는 그 구성요소로서 캡슐 고유키 복호부(1213), 제어정보 복호부(1215), C2 콘텐트 복호 처리부(1216) 및 C2 콘텐트 복호부(1217)를 포함한다. 제 2 콘텐트 처리부(1210)는 재암호화와 메모리 카드(1300)에 기록을 위한 복수의 마스터키(1219)를 추가로 저장한다. 제 2 콘텐트 처리부(1210)는 그 구성요소로서 디스크키 생성부(1218), 디스크키 암호화부(1220), 타이틀키 생성부(1221), 타이틀키 암호화부(1222), 오디오 데이터 암호화부(1223) 및 인증부(1224)를 포함한다. 여기에서 각 마스터키는 상이한 제조자의 메모리 카드 재생장치에 유지된 키데이터와 동일한 값을 갖는 키데이터이다. 마스터키의 각각은 상이한 콘텐트를 갖는 키데이터이다. 복수의 제조자에 대한 마스터키는 제 2 콘텐트 처리부(1210)에 저장되므로 메모리 카드(1300)는 복수의 제조자에 의해 메모리 카드 재생장치에서 재생될 수 있다.
캡슐 고유키 복호부(1213)는 공개키인 K2 키(1211)를 사용하여 캡슐(100)내의 암호화된 캡슐 고유키(110)를 복호하고, 복호된 암호화 캡슐 고유키(110)를 출력한다. 제어정보 복호부(1215)는 출력 복호된 암호화 캡슐 고유키(110)와 S2 키(1212)의 배타적 논리합의 결과인 트랜스포트키(1214)를 사용하여 캡슐(100) 내 의 암호화된 제어정보(120)를 복호한다. 여기에서 트랜스포트키(1214)는 상술한 제 1 콘텐트 처리부(1140)에서 취득된 트랜스포트키(1144)와 동일한 값을 갖는다. K2 키(1211)와 S2 키(1212)는 비록 도 5에 도시된 타원 비밀키(5)와 S1키(1142)가 공개키인 K2 키(1211)와 S2 키(1212)에 각각 대응하는 타원 비밀키로 대체된다 하더라도 도 5에 도시된 바와 같은 트랜스포트키(1144)에 따라 암호화된 캡슐 고유키(110)를 생성시킬 수 있는 키데이터이다.
C2 콘텐트 복호 제어부(1216)는 암호화된 C2 콘텐트(140)가 제어정보 복호부(1215)에 의해 복호된 암호화된 제어정보인 제어정보(20) 내의 C2 복호조건 정보(27)를 참조하여 복호될 수 있는지를 판정한다. 판정결과 암호화된 C2 콘텐트(140)가 복호될 수 있는 것으로 판정되면 C2 콘텐트 복호 제어부(1216)는 C2 부과금 정보(28)를 참조하여 부과금 처리를 실행하고, 복호명령을 C2 콘텐트 복호부(1217)에 보낸다. 여기에서 C2 콘텐트 복호 제어부(1216)에 의한 부과금 처리는 C1 콘텐트 복호 제어부(1146)에 의한 부과금 처리와 동일하다. 즉, 사용자로 하여금 음악 공급 회사 등에 구매를 위한 요금을 사용자가 미리 열어 놓은 은행구좌로부터 지불하도록 지시하는 통신회선(1001)을 통해 정보를 전송할 수 있다. 이 정보는 퍼스널 컴퓨터(1100)의 제어부(1120)로부터 메모리 카드 라이터(1200)내의 PC 인터페이스(1204)를 통해 통신회선(1001)에 전송된다. C2 콘텐트 복호 제어부(1216)는 카운터 값을 저장하고 C2 콘텐트(40)가 복호될 때마다 1씩 카운터 값을 증가시킨다. 결국, 카운터 값과 판매용 요금을 곱한 값이 구해지므로 1일의 총부과금을 지불하도록 하는 명령이 야간에 통신회선(1001)을 통해 전송될 수 있 다.
C2 콘텐트 복호부(1217)는 제어정보(20)의 C2 어드레스(26)를 참조하여 암호화된 C2 콘텐트(40)의 위치를 특정하고, C2 키(25)를 사용하여 암호화된 C2 콘텐트(140)를 복호하며, C2 콘텐트(40)를 오디오 데이터 암호화부(1223)로 송신한다. 암호화 알고리즘은 블록 암호 시스템에서 도 4에 도시된 암호화(2)에 대응하는 알고리즘이다.
한편, 인증부(1224)는 메모리 카드(1300) 내의 인증부(1301)와 서로 인증을 실행하는 기능을 갖는다. 인증부(1301)는 메모리 카드(1300)에 데이터를 기록하는 장치의 정확도를 인증하지만 인증부(1224)는 인증부(1301)로부터 인증정보를 수신하여 수신된 인증정보에 따라 메모리 카드(1300)의 정확도를 판정하기 위해 인증부(1301)로부터 인증정보를 수신한다. 보다 구체적으로 예컨대 메모리 카드 라이터(1200) 내의 인증부(1224)는 메모리 카드(1300) 내의 인증부(1301)에 난수를 송신하고, 인증부(1301)는 비밀 암호화 알고리즘에 따라 난수를 암호화하고 암호화된 난수를 인증부(1224)로 복귀시킨다. 복호 알고리즘에 따라 수신된 암호화 난수의 복호결과가 원래의 난수값과 동일하면 인증부(1301)가 갖는 암호화 알고리즘은 인증부(1224)가 갖는 복호 알고리즘과 대응한다. 결국 인증이 성공적으로 실행된 것으로 판정된다. 인증은 후술하는 방식으로 실행될 수 있다. 메모리 카드 라이터(1200)와 메모리 카드(1300)는 인증키와 인증방법을 공유하며, 메모리 카드 라이터(1200)와 메모리 카드(1300)는 인증키를 사용하여 챌린지 응답 절차에 따라 서로의 인증을 실행한다.
인증이 성공적으로 실행되면, 즉 메모리 카드(1300)가 정확한 것으로 판정되면 인증부(1224)는 ID의 취득을 허용하고 메모리 카드 ID 취득부(1230)와 기록부(1240)에 각각 기록을 허용하는 명령을 보낸다. ID 취득의 허용을 수신하면 메모리 카드 ID 취득부(1230)는 메모리 카드(1300)로부터 고유정보인 메모리 카드 ID를 취득하여 취득된 메모리 카드 ID를 디스크키 생성부(1218)에 보낸다. 기록의 허용이 수신되면 기록부(1240)는 디스크키 암호화부(1220)와, 타이틀키 암호화부(1222)와 오디오 데이터 암호화부(1223)로부터 출력된 데이터를 메모리 카드(1300)에 기록한다.
디스크키 생성부(1218)는 메모리 카드 ID 취득부(1230)로부터 구한 메모리 카드 ID 상의 정보를 포함하는 64비트 디스크키를 생성한다. 여기에서 디스크키는 기록매체인 모든 종류의 메모리 카드에 공통인 키데이터이다.
디스크키 암호화부(1220)는 디스크키 암호화부(1220)에 미리 저장된 복수의 마스터키(1219) 중 하나를 사용하여 디스크키 생성부(1218)에 의해 생성된 디스크키를 암호화한다. 디스크키 암호화부(1220)는 다른 마스터키(1219)를 사용하여 동일한 디스크키를 계속 암호화하여 마스터키(1219)의 것과 동일한 수의 암호화 디스크키를 생성하고, 생성된 암호화 디스크키를 메모리 카드 라이터(1200) 내의 기록부(1240)에 출력한다.
타이틀키 생성부(1221)는 적당한 64비트 타이틀키를 생성하여 생성된 타이틀키를 타이틀키 암호화부(1222)에 보낸다. 여기에서 타이틀키는 각각의 음악 콘텐트에 대해 설정될 수 있는 키데이터를 나타낸다.

타이틀키 암호화부(1222)는 디스크키 생성부(1218)에 의해 생성된 디스크키를 사용하여 타이틀키 생성부(1221)에 의해 생성된 타이틀키를 암호화하고, 암호화된 타이틀키를 기록부(1240)에 출력한다. 한편 오디오 데이터 암호화부(1223)는 타이틀키 생성부(1221)에 의해 생성된 타이틀키를 사용하여 C2 콘텐트 복호부(1217)로부터 출력된 C2 콘텐트로부터 출력된 C2 콘텐트를 재암호화하고, 재암호화된 C2 콘텐트(40)를 기록부(1240)에 출력한다.
디스크키 암호화부(1220), 타이틀키 암호화부(1222) 및 오디오 데이터 암호화부(1223)에 의해 사용된 암호화 알고리즘은 블록 암호 시스템의 DES 알고리즘이다.
기록부(1240)는 메모리 카드(1300)의 사용자 접근가능한 영역에 오디오 데이터 암호화부(1223)로부터 전송되는 오디오 데이터를 기록하고, 사용자에 의해 접근할 수 없는 메모리 카드(1300)의 시스템 영역에 암호화된 디스크키와 타이틀키를 기록한다. 한편, 메모리 카드(1300)가 삽입될 수 있는 메모리 카드 재생장치는 마스터키를 유지하기로 되어 있고, 암호화된 디스크키와 타이틀키를 사용하여 역순으로 전술한 암호화 처리를 실행하며, 메모리 카드(1300)의 인증이 성공적으로 실행될 때 오디오 데이터를 복호함으로써 음악을 재생하도록 하는 기능을 갖는다.
(동작)
이하, 그 구조에 대해서는 이미 설명된 음악 콘텐트 재생/기록 시스템(1000)에 의한 동작에 대하여 설명하기로 한다.
도 6은 음악 콘텐트 재생/기록 시스템(1000)에 의한 동작을 설명한다.
도 6에 도시된 바와 같이, 음악 콘텐트 재생/기록 시스템(1000)의 수신부(1110)는 사용자 명령에 응답하여 인터넷을 통해 음악 콘텐트 제공자의 서버로부터 음악 콘텐트를 포함하는 캡슐(100)을 수신하여 수신된 캡슐(100)을 캡슐 저장부(1130)에 저장한다(단계 S301).
그리고 캡슐(100)이 캡슐 저장부(1130)에 저장되면 제어부(1120)는 음악 콘텐트의 시험, 구매 및 처리의 종료 중의 하나를 사용자가 선택할 수 있도록 디스플레이(1191) 상에 그래픽 사용자 인터페이스 스크린을 디스플레이한다.
그 다음에, 사용자가 시험을 선택하였음을 검출하면(단계 S302) 제어부(1120)는 C1 콘텐트(30)를 재생하도록 제 1 콘텐트 처리부(1140)에 명령하여 C1 콘텐트(30)를 재생한다. 재생명령을 수신하면 제 1 콘텐트 처리부(1140)는 캡슐 고유키 복호부(1143)의 복호에 의해 캡슐 고유키(10)를 취득하고, 제어정보 복호부(1145)의 복호에 의해 제어정보를 취득한다(단계 S303).
제어정보 복호부(1145)의 제어정보(20)를 취득한 후, C1 콘텐트 복호 제어부(1146)는 C1 복호조건 정보(23)를 참조한다. 예컨대 C1 복호조건이 만족되면, 즉 시험을 위해 설정된 날짜 범위내이면 복호의 수는 미리 결정된 회수 보다 크지 않고, C1 콘텐트 복호 제어부(1146)는 부과금 처리를 실행하고(단계 S305), C1 콘텐트 복호부(1147)가 복호에 의해 C1 콘텐트(30)를 취득하도록 하며(단계 S306), 재생부(1150)로 하여금 C1 콘텐트(30)를 재생하도록 하여 스피커(1193)에 소리를 출력하도록 한다(단계 S307). 한편 C1 복호조건이 만족되지 않으면, 예컨대 시험을 위한 날짜가 지나면(단계 S304), 단계 S305에서 단계 S307의 동작이 실행되 지 않는다.
한편, 사용자가 구입을 선택하면, 즉 사용자가 메모리 카드(1300)에 기록된 음악 콘텐트를 요청한 것으로 검출하면(단계 S308), 제어부(1120)는 C2 콘텐트(40)를 재생하도록 메모리 카드 라이터(1200)의 제 2 콘텐트 처리부(1210)에 명령한다. 재생명령을 수신하면 제 2 콘텐트 처리부(1210)는 캡슐 고유키 복호부(1213)의 복호에 의해 캡슐 고유키(10)를 취득하고, 제어정보 복호부(1215)의 복호에 의해 제어정보(20)를 취득한다(단계 S309). 제어정보 복호부(1215)의 제어정보(20)를 취득한 후, C2 콘텐트 복호 제어부(1216)는 C2 복호조건 정보(27)를 참조한다. 예를들어 C2 복호조건이 만족되면, 예컨대 그것이 구매를 위해 설정된 날짜의 범위 내에 있으면(단계 S310), C2 콘텐트 복호 제어부(1216)는 부과금 처리를 실행하고(단계 S311), C2 콘텐트 복호부(1217)로 하여금 복호에 의해 C2 콘텐트(40)를 취득하게 하고(단계 S312) 재암호화 및 기록을 위한 처리를 하게 한다(단계 S313). 반면 C2 복호조건이 만족되지 않으면, 예컨대 구매를 위한 날짜 뒤이면(단계 S310), 단계 S311에서 단계 S313의 처리가 실행되지 않는다.
한편, 제어부(1120)가 사용자에 의해 처리의 종료가 선택되었음을 검출하면(단계 S314), 시험과 구매에 대한 모든 처리가 완료된다. 반면 사용자가 처리의 종료를 선택하지 않으면 처리는 단계 S302로 복귀한다. 결국 사용자는 시험 및 구매를 여러 번 선택할 수 있다.
도 7은 메모리 카드(1300)에 오디오 데이터를 기록하기 위한 암호화와 기록처리를 나타낸 흐름도이다.
도 7에 도시된 바와 같이, 인증부(1224)는 메모리 카드(1300)의 인증을 실행한다(단계 S401). 반면 인증이 성공적으로 실행되지 않으면 암호화 및 기록이 실행되지 않으며, 인증이 성공적으로 실행되면(단계 S402), 후술하는 바와 같은 처리가 실행된다.
메모리 카드 ID 취득부(1230)는 메모리 카드(1300)로부터 메모리 카드 ID를 취득하여 취득된 메모리 카드 ID를 디스크키 생성부(1218)에 보낸다(단계 S403). 디스크키 생성부(1218)는 주어진 메모리 카드 ID에 따라 디스크키를 생성한다.(단계 S404).
디스크키 암호화부(1220)는 복수의 마스터키(1219) 각각을 사용하여 생성된 디스크키를 암호화하고(단계 S405), 복수의 암호화된 디스크키를 기록부(1240)를 통해 메모리 카드(1300)에 기록한다.
암호화된 디스크키를 기록한 후(단계 S406), 타이틀키 생성부(1221)는 타이틀키를 생성하고, 디스크키를 사용하여 생성된 타이틀키를 암호화하여(단계 S407) 기록부(1240)를 통해 메모리 카드(1300)에 암호화된 타이틀키를 기록한다(단계 S408). 오디오 데이터 암호화부(1223)가 C2 콘텐트 복호부(1217)의 복호에 의해 취득된 C2 콘텐트(40)를 재암호화하고 재암호화된 C2 콘텐트(40)를 기록부(1240)를 통해 메모리카드(1300)에 기록한다(단계 S409).
상술한 바와 같이, 음악 콘텐트 재생/기록 시스템(1000)은 음악 콘텐트를 재생하고 사용자의 요청에 따라 음악 콘텐트를 메모리 카드에 기록한다.
(제 2 실시예)
본 발명에 따르는 저작물 보호 시스템의 제 2 실시예인 음악 콘텐트 재생/기록 시스템(2000)에 대해 도면을 참조하여 설명하기로 한다.

(구성)
음악 콘텐트 재생/기록 시스템(2000)은 통신회선을 통해 수신된 음악 콘텐트가 퍼스널 컴퓨터를 사용하여 재생되고 메모리 카드에 기록되는 시스템이다. 음악 콘텐트 재생/기록 시스템(2000)의 외관도는 도 1 에 도시된 제 1 실시예에 따르는 음악 콘텐트 재생/기록 시스템(1000)의 외관도와 동일하다.
도 8은 본 발명의 제 2 실시예에 따르는 음악 콘텐트 재생/기록 시스템(2000)의 기능블록도이다.
도 8에 도시된 바와 같이, 음악 콘텐트 재생/기록 시스템(2000)은 퍼스널 컴퓨터(2100)와 메모리 카드 라이터(2200)를 포함한다. 음악 콘텐트 재생/기록 시스템(2000)은 암호화된 캡슐(200)이 수신된 시스템이며, 캡슐(200)에 포함된 음악 콘텐트는 퍼스널 컴퓨터(2100)에 의해 재생되고, 음악 콘텐트 및 관련 제어정보는 메모리 카드 라이터(2200)에 삽입되는 메모리 카드(2300)에 기록된다.
도 8에서, 도 2와 동일한 구성요소에 대해서는 동일한 참조부호를 부여하여 그에 대한 설명은 생략한다.
여기에서, 캡슐(200)은 C1키(21)와 C2키(25)를 포함하는 암호화된 제어정보(120)와, 암호화된 C1 콘텐트(130)와, 암호화된 C2 콘텐트(140)로 구성된다. 캡슐(200)에 대한 상세한 설명은 후술하기로 한다.
퍼스널 컴퓨터(2100)는 수신부(1110), 제어부(1120), 캡슐 저장부(1130), 제 1 콘텐트 처리부(2140) 및 재생부(1150)를 포함한다. 퍼스널 컴퓨터(2100)에서 수신부(1110)에 의해 캡슐 저장부(1130)에 저장된 암호화된 C1 콘텐트(130)는 제 1 콘텐트 처리부(2140)에 의해 복호되고 재생부(1150)에 의해 재생된다.
한편 메모리 카드(2300)가 삽입되고 퍼스널 컴퓨터(2100)에 접속된 PC 카드는 부정조작이 불가능한 하드웨어로 구성된 제 2 콘텐트 처리부(2210)를 포함한다.
여기에서, 메모리 카드(2300)는 인증부(2310)를 포함한다. 메모리 카드(2300)에는 재기록 가능하지 않은 영역에 미리 64비트 메모리 카드 ID(2320)가 저장되고 기록가능한 영역에는 MC 암호화된 제어정보(2330)와 MC 암호화된 C2 콘텐트(2340)가 기록된다. MC 암호화된 C2 콘텐트(2340)는 기록을 위해 암호화된 C2 콘텐트이다. 반면 MC 암호화된 제어정보(2330)는 MC 암호화된 C2 콘텐트(2340)를 복호하기 위한 키인 C2'키(2331)를 포함한다. MC 암호화된 제어정보(2330)는 예컨대 C2 콘텐트를 제어하기 위해 사용되는 암호화된 MC 제어정보이다.
제 1 콘텐트 처리부(2140)와 제 2 콘텐트 처리부(2210)의 상세한 설명에 대해서는 후술하기로 한다.
(데이터 구조 및 관련처리)
이하, 캡슐(200)에 대해 설명하기로 한다.
캡슐(200)은 캡슐(100)의 경우와 마찬가지로 저작권 보호센터에 의해 만들어진 데이터이다. 캡슐(200)은 암호화된 캡슐 고유키(110)가 제거된 점을 제외하면 제 1 실시예의 캡슐(100)과 동일한 구조를 갖는다. C1 키(21) 및 C2 키(25)의 데이터 크기와 캡슐(200) 내의 암호화된 제어정보(120)의 암호화 알고리즘은 제 1 실시 예의 것들과는 다르다.
암호화된 제어정보(120)는 C1 키(21)와 C2 키(25) 외에도 도 8에는 나타나 있지 않은 각 콘텐트와 부과금 정보의 복호조건을 나타내는 정보를 포함한다. 즉, 암호화된 제어정보(120)는 도 5를 이용하여 제 1 실시예에 설명된 제어정보(20)를 암호화함으로써 생성되는 데이터이다. 여기에서 재생회수 및 복사회수의 제한에 관한 정보와 메모리 카드에 기록된 C2 콘텐트의 부과금 정보(본 명세서에서는 '제어 사용정보'라 함)가 제 2 실시예의 제어정보(20)에 포함되는 것으로 가정한다.
암호화된 제어정보(120)는 타원곡선 암호 시스템의 알고리즘에 따라 암호화됨으로써 생성된다.
암호화된 C1 콘텐트(130)는 C1 키(21)를 사용하여 평문인 C1 콘텐트(30)를 암호화함으로써 생성되는 데이터이며(도 4 참조), 데이터 길이는 콘텐트에 따라 변경될 수 있다. C1 키(21)는 40비트 키데이터이며, C1 키(21)를 사용하는 암호화는 블록 암호 시스템에서 실행된다. 예컨대, DES 알고리즘이 사용된다.
암호화된 C2 콘텐트(140)는 C2 키(25)를 사용하여 평문인 C2 콘텐트(40)를 암호화함으로써 생성되는 데이터이며(도 4 참조), 데이터 길이는 콘텐트에 따라 변경될 수 있다. C2 키(25)는 56비트 키데이터이며, C2 키(25)를 사용하는 암호화는 블록 암호 시스템에서 실행된다. 예컨대, DES 알고리즘이 사용된다.
C1 콘텐트(30)와 C2 콘텐트(40)는 예컨대 MPEG 오디오 표준을 따라 압축된다.
이하, 상술한 캡슐(200)의 콘텐트에 관한 처리를 실행하는 제 1 콘텐트 처리 부(2140)와 제 2 콘텐트 처리부(2210)에 대해 설명하기로 한다.
제 1 콘텐트 처리부(2140)는 제어정보 복호부(2145), C1 콘텐트 복호부(1147) 및 인증 암호화부(2149)를 포함한다.
여기에서 제어정보 복호부(2145)는 타원곡선 암호 시스템의 알고리즘에 따라 암호화된 제어정보(120)를 복호함으로써 제어정보(20)를 취득하고, 제어정보(20)의 C1키(21)를 C1 콘텐트 복호부(1147)에 공급하며, C2 키(25)와 제어 사용정보를 인증 암호화부(2149)에 공급한다.
제어정보 복호부(2145)는 C1 콘텐트 복호 처리부(1146)의 기능을 포함한다. 제어정보 복호부(2145)는 C1 콘텐트(30)가 제어정보(20)내의 C1 복호조건 정보(23)를 참조하여 복호될 수 있는지의 여부를 판정한다. 그 결과 C1 콘텐트(30)가 복호될 수 있다고 판정되면 제어정보 복호부(2145)는 C1 부과금 정보(24)를 참조하여 부과금 처리를 실행하고, C1 키(21)를 C1 콘텐트 복호부(1147)에 공급하며, C1 콘텐트 복호부(1147)에 복호명령을 보낸다. 제어정보 복호부(2145)는 C2 콘텐트 복호 제어부(1216)의 기능을 포함한다. 제어정보 복호부(2145)는 C2 콘텐트(40)가 제어정보(20)의 C2 복호조건 정보(27)를 참조하여 복호될 수 있는지의 여부를 판정한다. 그 결과 C2 콘텐트(40)가 복호될 수 있다고 판정되면 제어정보 복호부(2145)는 C2 부과금 정보(28)를 참조하여 부과금 처리를 실행하고, C2 키(25)와 제어정보(20)의 제어 사용정보를 인증 암호화부(2149)에 공급한다. 부과금 처리는 제 1 실시예의 것과 동일하므로 그에 대한 상세한 설명은 생략한다. C1 콘텐트 복호부(1147)는 제어정보(20)의 C1 키(21)를 사용하여 암호화된 C1 콘텐트(130)를 복 호하고, 복호된 암호화 C1 콘텐트(130)를 재생부(1150)에 출력한다. 복호에 사용된 복호 알고리즘은 C1 콘텐트의 암호화에 사용되는 알고리즘에 대응하는 블록 암호 시스템의 알고리즘이다.

인증 암호화부(2149)는 제 2 콘텐트 처리부(2210)의 인증 암호화부(2260)와 데이터를 교환함으로써 메모리 카드 라이터(2200)의 인증을 실행하며, 제어정보 복호부(2145)로부터 공급되는 제어 사용정보와 C2 키(25)를 암호화하여 암호화된 C2 키(25)와 제어 사용정보를 인증 암호화부(2260)로 송신한다.
한편, 제 2 콘텐트 처리부(2210)는 인증 암호화부(2260), C2 콘텐트 복호부(1217), 인증부(2224), MC 제어정보 암호화부(2270) 및 MC 콘텐트 암호화부(2280)를 포함한다.
여기에서 인증 암호화부(2260)는 인증 암호화부(2149)와 데이터를 교환함으로써 퍼스널 컴퓨터(2100)의 인증을 실행하며, 암호화된 C2 키(25)와 인증 암호화부(2149)로부터 송신된 제어 사용정보를 수신하고, 암호화된 C2키(25)와 제어 사용정보를 복호한다.
C2콘텐트 복호부(1217)는 인증 암호화부(2260)로부터 C2키(25)를 취득하고, C2키(25)를 사용하여 C2 콘텐트(40)의 암호화에 대응하는 블록 암호 시스템의 알고리즘에 따라 암호화된 C2 콘텐트(140)를 복호한다.
인증부(2224)는 메모리 카드(2300)의 인증부(2310)와 데이터를 교환함으로써 메모리 카드(2300)의 인증을 실행하며, 인증부(2310)로부터 송신된 메모리 카드 ID(2320)를 수신한다.
MC 제어정보 암호화부(2270)는 인증 암호화부(2260)로부터 제어 사용정보를 수신하고, 제어 사용정보와 C2' 키(2331)로 구성된 MC 제어정보를 암호화하여 MC 암호화 제어정보(2330)를 메모리 카드(2300)에 기록한다.
MC 콘텐트 암호화부(2280)는 기록을 위해 복호된 C2 콘텐트(40)를 암호화하여 메모리 카드(2300)에 MC 암호화된 C2 콘텐트(2340)를 기록한다.
MC 제어정보 암호화부(2270)와 MC 콘텐트 암호화부(2280)에 의해 메모리 카드(2300)에 기록하는 것에 대한 상세한 설명은 후술하기로 한다.
이하, 인증처리와 인증 암호화부(2149) 및 인증 암호화부(2260)에 의해 실행되는 암호화 통신 처리에 대해 설명하기로 한다.
인증 암호화부(2149)와 인증 암호화부(2260)는 인증 시스템으로서 예를들면 JIS(일본 산업표준)에 의한 JISX5056-2, '보안기술-엔티티 인증 메커니즘-제 4 섹션 암호화 검사기능을 이용하는 인증 메커니즘(Security Technology-Entity Authentification Mechanism-Authentification Mechanism using the forth Section Encryption Check Function)'을 사용한다.
보다 구체적으로 정확한 인증 암호화부는 동일한 공통키 시스템에서 암호화 알고리즘 E를 사용하므로, 대응하는 인증 암호화부의 인증은 인증 암호화부가 동일한 암호화 알고리즘 E를 사용하는지의 여부를 검사함으로써 실행된다. DES 알고리즘은 암호화 알고리즘 E로서 사용된다.
인증 암호화부(2149, 2260)에 의한 인증 및 암호화 통신의 절차에 대해 도 9를 참조로 설명하기로 한다. 인증 암호화부(2149)는 알고리즘 E를 사용하며, 인증 암호화부(2260)는 인증이 상호 실행되기 전의 처리를 설명하는 알고리즘 E'를 사용한다.
도 9는 인증과 인증 암호화부(2149, 2260)에 의한 암호화 통신의 절차를 나타낸다.
퍼스널 컴퓨터(2100)의 인증 암호화부(2149)는 난수 R1을 생성하고, 암호화 알고리즘 E에 따라 난수 R1을 변환함으로써 값 E(R1)을 생성하며, 난수 R1을 메모리 카드 라이터(2200)의 인증 암호화부(2260)로 송신한다(단계 S3001).
난수 R1을 수신하면 메모리 카드 라이터(2200)의 인증 암호화부(2260)는 암호화 알고리즘 E'에 따라 난수 R1을 변환함으로써 값 E'(R1)을 생성하고 값 E'(R1)을 퍼스널 컴퓨터(2100)의 인증 암호화부(2149)에 송신한다(단계 S3002).
값 E'(R1)을 수신하면 퍼스널 컴퓨터(2100)의 인증 암호화부(2149)는 수신된 값 E'(R1)이 인증 암호화부(2149)에 의해 생성된 값 E(R1)과 일치하는지의 여부를 검증하고, 값 E'(R1)이 값 E(R1)과 일치할 때 메모리 카드 라이터(2200)가 정확한지를 판정한다(단계 S3003).
마찬가지로 메모리 카드 라이터(2200)의 인증 암호화부(2260)는 난수 R2를 생성하고 암호화 알고리즘 E'에 따라 난수 R2를 변환함으로써 값 E'(R2)를 생성하며, 난수 R2를 퍼스널 컴퓨터(2100)의 인증 암호화부(2149)로 송신한다(단계 S3004).
난수 R2를 수신하면 퍼스널 컴퓨터(2100)의 인증 암호화부(2149)는 암호화 알고리즘 E에 따라 수신된 난수 R2를 변환함으로써 값 E(R2)를 생성하고 생성된 값 E(R2)를 메모리 카드 라이터(2200)의 인증 암호화부(2260)에 송신한다(단계 S3005).
값 E(R2)를 수신하면 메모리 카드 라이터(2200)의 인증 암호화부(2260)는 수신된 값 E(R2)가 인증 암호화부(2260)에 의해 생성된 값 E'(R2)와 일치하는지의 여부를 검증하고, 값 E(R2)가 값 E'(R2)와 일치할 때 퍼스널 컴퓨터(2100)가 정확한지를 판정한다(단계 S3006).
인증이 상술한 바와 같이 상호 실행되면, 즉 암호화 알고리즘 E와 E'가 동일한 알고리즘이고 인증 암호화부(2149, 2260)에 의해 사용된 키가 동일한 키이면 각 인증 암호화부(2149, 2260)는 값 E(R1) 및 E(R2)의 배타적 논리합 입력의 결과인 비트열 K를 암호화 알고리즘 E로 생성한다.
비트 스트링 K를 생성한 후, 퍼스널 컴퓨터(2100)의 인증 암호화부(2149)는 암호화 알고리즘 E에 따라 키로서 비트열을 사용하여 제어정보 복호부(2145)에 의해 복호의 결과인 제어 사용정보와 C2 키(25)를 암호화하여 암호화된 C2 키(25)와 제어 사용정보를 메모리 카드 라이터(2200)의 인증 암호화부(2260)에 송신한다(단계 S3007).
암호화된 C2키(25)와 제어 사용정보를 수신하면 메모리 카드 라이터(2200)의 인증 암호화부(2260)는 암호화된 C2 키(25)와 제어 사용정보를 복호한다(단계 S3008).
인증 암호화부(2149 또는 2260)가 단계 S3003 또는 S3006에서 정확하지 않은 것으로 판정되면 다음 처리는 실행되지 않는다.

상기 절차에 따라 C2키(25)와 제어 사용정보는 퍼스널 컴퓨터(2100)로부터 메모리 카드 라이터(2200)로 확실하게 송신된다.
여기에서 인증부(2224)와 인증부(2310)에 의해 실행되는 인증처리와 통신처리에 대해 설명하기로 한다.
인증부(2224)와 인증부(2310)는 인증 시스템으로서 예를들면 JIS(일본 산업표준)에 의한 JISX5056-2, '보안기술-엔티티 인증 메커니즘-제 4 섹션 암호화 검사기능을 이용하는 인증 메커니즘(Security Technology-Entity Authentification Mechanism-Authentification Mechanism using the forth Section Encryption Check Function)'을 사용한다.
보다 구체적으로 정확한 인증 암호화부는 동일한 공통키 시스템에서 암호화 알고리즘 F를 사용하므로, 대응하는 인증부의 인증은 인증부가 동일한 암호화 알고리즘 F를 사용하는지의 여부를 검사함으로써 실행된다. DES 알고리즘이 암호화 알고리즘 F로서 사용된다.
인증부(2224, 2310)에 의한 인증 및 통신의 절차에 대해 도 10을 참조로 설명하기로 한다. 인증부(2310)는 알고리즘 F를 사용하며, 인증부(2224)는 인증이 상호 실행되기 전의 처리를 기술한 알고리즘 F'를 사용한다.
도 10은 인증부(2224, 2310)에 의한 통신과 인증의 절차를 나타낸다.
메모리 카드(2300)의 인증부(2310)는 난수 R3을 생성하고, 암호화 알고리즘 F에 따라 난수 R3을 변환함으로써 값 F(R3)을 생성하며, 난수 R3을 메모리 카드 라이터(2200)의 인증부(2224)로 송신한다(단계 S3501).
난수 R3을 수신하면 메모리 카드 라이터(2200)의 인증부(2224)는 암호화 알고리즘 F'에 따라 난수 R3을 변환함으로써 값 F'(R3)을 생성하고 값 F'(R3)을 메모리 카드(2300)의 인증부(2300)에 송신한다(단계 S3502).
값 F'(R3)을 수신하면 메모리 카드(2300)의 인증 암호화부(2310)는 수신된 값 F'(R3)이 인증부(2310)에 의해 생성된 값 F(R3)과 일치하는지의 여부를 검증하고, 값 F'(R3)이 값 F(R3)과 일치할 때 메모리 카드 라이터(2200)가 정확한 것으로 판정한다(단계 S3503).
마찬가지로 메모리 카드 라이터(2200)의 인증부(2224)는 난수 R4를 생성하고 암호화 알고리즘 F'에 따라 난수 R4를 변환함으로써 값 F'(R4)를 생성하며, 난수 R4를 메모리 카드(230)의 인증부(2310)로 송신한다(단계 S3504).
난수 R4를 수신하면 메모리 카드(2300)의 인증부(2310)는 암호화 알고리즘 F에 따라 수신된 난수 R4를 변환함으로써 값 F(R4)를 생성하고 생성된 값 F(R4)를 메모리 카드 라이터(2200)의 인증부(2224)에 송신한다(단계 S3505).
값 F(R4)를 수신하면 메모리 카드 라이터(2200)의 인증부(2224)는 수신된 값 F(R4)가 인증부(2224)에 의해 생성된 값 F'(R4)와 일치하는지의 여부를 검증하고, 값 F(R4)가 값 F'(R4)와 일치할 때 메모리 카드(2300)가 정확한 것으로 판정한다(단계 S3506).
인증부(2224 또는 2310)가 단계 S3503 또는 S3506에서 정확하지 않으면 다음 처리는 실행되지 않는다.
인증이 상술한 바와 같이 인증부(2224, 2310)에 의해 상호 실행되면, 즉 암 호화 알고리즘 F와 F'가 동일한 알고리즘이고 인증부(2224, 2310)에 의해 사용된 키가 동일한 키이면 인증부(2310)는 메모리 카드 ID(2320)를 인증부(2224)에 송신하고(단계 S3507), 인증부(2224)는 메모리 카드 ID(2320)를 수신한다(단계 S3508).
인증이 상호 실행되고 인증부(2224)가 메모리 카드 ID(2320)를 수신한 후, MC 제어정보는 MC 제어정보 암호화부(2270)에 의해 암호화되고, 암호화된 C2 콘텐트(140)는 C2 콘텐트 복호부(1217)에 의해 복호되며, 복호된 C2 콘텐트(40)는 제 2 콘텐트 처리부(2210)의 MC 콘텐트 암호화부(2280)에 의해 재암호화된다.
이하, MC 제어정보 암호화부(2270)와 MC 콘텐트 암호화부(2280)에 의해 메모리 카드(2300)에 데이터를 기록하는 절차에 대해 설명하기로 한다.
인증부(2224, 2310)의 상호인증이 성공적으로 실행되면 메모리 카드 ID(2320)를 수신한 인증부(2224)는 메모리 카드 ID(2320)의 입력결과로서 암호화 알고리즘 G로 56비트 메모리 카드 고유키를 생성한다. 암호화 알고리즘 G는 비밀값이 키인 DES 알고리즘이다.
그리고, 인증부(2224)는 56비트 난수를 생성하며, 생성된 난수와 메모리 카드 고유키의 배타적 논리합의 결과인 56비트 C2'키를 생성한다.
인증부(2224)에 의해 메모리 카드 고유키와 C2'키가 생성된 후, MC 콘텐트 암호화부(2280)는 C2 콘텐트 복호부(1217)의 복호에 의해 취득된 C2'키를 사용하여 C2 콘텐트를 재암호화하며, 재암호화된 C2 콘텐트를 메모리 카드(2300)에 기록한다. 결국 MC 암호화된 C2 콘텐트(2340)는 메모리 카드(2300)에 기록된다.
한편, 인증부(2224)에 의해 메모리 카드 고유키와 C2'키가 생성된 후, MC 제 어정보 암호화부(2270)는 C2'키와 제어 사용정보로 구성되며, 키로서 메모리 카드 고유키를 사용하여 인증 암호화부(2260)의 복호에 의해 취득된 MC 제어정보를 암호화한다. MC 제어정보 암호화부(2270)는 메모리 카드(2300)에 암호화된 MC 제어정보를 기록한다. 결국 MC 암호화 제어정보(2330)는 메모리 카드에 기록된다. DES 알고리즘에 따르지만 부분적으로 DES 알고리즘과 다른 암호화 알고리즘이 MC 콘텐트 암호화부(2280)와 MC 제어정보 암호화부(2270)에서의 암호화를 위해 사용된다.
도 11은 DES 알고리즘에 따라 56비트 키를 사용하여 64비트 평문을 암호화하는 개념을 나타낸다. 암호화는 평문에 대한 함수를 16회 사용하여 계산을 반복함으로써 실행된다. 도 11은 제 1 계산 및 제 2 계산을 나타낸다. 도 11에서 부호 '+'는 배타적 논리합 연산을 나타낸다.
보다 구체적으로는, DES 알고리즘에서는 도 10에 도시된 바와 같이 평문의 하위 32비트와 키로부터 유도된 중간키는 함수 'f'의 입력이 되며, 함수 'f'로부터의 출력인 32비트열과 평문의 상위 32비트의 배타적 논리합은 제 1 계산의 하위 32비트가 되고, 평문의 하위 32비트는 제 1 계산에서 상위 32 비트가 된다. 평문은 이 절차를 16회 반복하여 암호화된다.
여기에서 32비트 데이터를 출력하는 함수 'f'는 소정의 순서로 8개의 함수 g1, g2, g3, …, g8의 출력결과를 조합하여 조합된 결과를 출력하는 함수이다. 함수 'f'는 'f=(g1, g2, g3, …g8)'로 표시된다.
한편, 함수 'f'' (f'=(g1, g2, g3, …g8))는 예를들면 함수 g1만을 다른 함수 g1'로 대체함으로써 생성될 수 있다.

결국 MC 콘텐트 암호화부(2280)와 MC 제어정보 암호화부(2270)에 의해 사용되는 암호화 알고리즘은 C2 콘텐트 복호부(1217)에 의해 사용된 DES 알고리즘이 도 11에 도시된 것이면 함수 'f'가 함수 'f''로 대체되는 도 11의 알고리즘일 수 있다.
상술한 바와 같이 C2 콘텐트 복호부(1217)에 의해 사용된 암호화 알고리즘이 부분적으로 MC 콘텐트 암호화부(2280)에 의해 사용된 것과 다르므로 이들 암호화 알고리즘이 소프트웨어 또는 하드웨어에 의해 실현될 때 이들 알고리즘의 부분은 어느 정도 공유될 수 있다. 결국 암호화 알고리즘의 개발 및 실현을 위한 비용은 전체적으로 상이한 암호화 알고리즘을 사용하는 것에 비해 절감될 수 있다.
(보충설명)
본 발명에 따르는 저작물 보호 시스템은 제 1 및 제 2 실시예의 음악 콘텐트 재생/기록 시스템을 참조하여 설명되어 있으나 본 발명은 이들 실시예에 한정되는 것은 아니다.
(1) 상기 실시예에서는 C2 콘텐트를 암호화하고 암호화된 C2 콘텐트를 메모리 카드에 기록하는 메모리 카드 라이터가 PC카드로 되어 있지만 메모리 카드 라이터가 PC카드에 국한되는 것은 아니다. 메모리 카드 라이터는 예를들면 USB(Universal Serial Bus)에 의해 퍼스널 컴퓨터에 접속될 수 있는 장치일 수 있다.
한편, 제 1 실시예의 수신부(1110), 제어부(1120), 캡슐 저장부(1130), 제 1 콘텐트 처리부(1140) 및 재생부(1150)는 퍼스널 컴퓨터(1100)에 의해 실현되는 것 으로 가정하고, 제 2 실시예의 수신부(1110), 제어부(1120), 캡슐 저장부(1130), 제 1 콘텐트 처리부(2140) 및 재생부(1150)는 퍼스널 컴퓨터(2100)에 의해 실현되는 것으로 가정하였다. 그러나 퍼스널 컴퓨터(1100, 2100)는 메모리와 CPU를 포함하며 프로그램 실행 제어기능을 갖는 전기기구일 수 있다. 예컨대 인터넷에 접속되는 기능을 갖는 TV 세트일 수 있다.
또한 제 1 실시예에서 제 2 콘텐트 처리부(1210)는 전류공급을 위한 리드로 감싼 부정조작이 불가능한 LSI 패키지인 것으로 가정하였으나 제 2 콘텐트 처리부(1210)는 부정조작이 불가능하여야 하지만 반드시 리드로 감쌀 필요는 없다.
또한 제 1 실시예의 제 2 콘텐트 처리부(1210)와 제 2 실시예의 제 2 콘텐트 처리부(2210)는 예컨대 보호될 데이터를 처리하는 처리 프로그램과 불필요한 프로그램을 조합함으로써 용이하게 판독될 수 없도록 설계된 부정조작이 불가능한 소프트웨어를 실행하거나 소프트웨어와 같은 보호될 데이터에 액세스하는 것을 제한하는 퍼스널 컴퓨터와 같은 구성요소일 수 있다. 제어정보 복호부(2145)와 인증 암호화부(2149)는 제 2 콘텐트 처리부(2210)에 포함될 수 있다.
(2) 제 1 실시예에서는 메모리 카드 라이터(1200)의 C2 콘텐트 복호부(1217)의 복호에 의해 취득되는 오디오 데이터인 C2 콘텐트가 메모리 카드에 기록을 위해 재암호화되는 것으로 가정하였으나 오디오 데이터가 직접 재생될 수도 있다. 이 경우, 스피커가 메모리 카드 라이터(1200)에 접속되면 음악 콘텐트가 스피커로부터 나온다.
(3) 제 1 실시예와 제 2 실시예에서는 하나의 캡슐이 하나의 암호화된 C1 콘 텐트와 하나의 암호화된 C2 콘텐트를 포함하지만 하나의 캡슐이 암호화된 C1 콘텐트와 암호화된 C2 콘텐트 중의 하나와 복수의 암호화된 C1 콘텐트와 암호화된 C2 콘텐트를 포함할 수 있다. 또한 각 캡슐은 C1 콘텐트와 암호화된 C2 콘텐트를 별도로 포함할 수 있다.
캡슐은 캡슐이 C1 콘텐트를 포함할 때에만 C1 콘텐트에 관한 부과금 정보와 같은 정보를 포함할 필요가 있으며, 캡슐이 C2 콘텐트를 포함할 때에만 C2 콘텐트에 관한 부과금 정보와 같은 정보를 포함할 필요가 있다.
(4) 상기 실시예에서는 키데이터의 길이에 대해 설명되어 있다. 예컨대 C1 키와 C2 키의 길이는 제 1 실시예에서는 64비트와 128비트로 기재되어 있으나, C1키, C2키 및 C2'키의 길이는 제 2 실시예에서는 40비트, 56비트, 56비트로 기재되어 잇다. 그러나 키데이터의 길이는 이들 값에 국한되는 것은 아니다. K1키, K2키, S1키, S2키 및 트랜스포트키는 상이한 길이를 가질 수 있다.
암호화된 캡슐 고유키(110)는 K1키에 의해 복호된 키와 K2키에 의해 복호된 키의 조합일 수 있다. 한편 트랜스포트키의 계산을 위한 배타적 논리합은 모든 비트에 대해 실행될 수는 없으나 소정수의 비트에 대해 실행될 수 있다.
또 C1 및 C2 콘텐트 복호부에 의해 사용된 복호 알고리즘은 통신회선을 통해 다운로드되는 알고리즘일 수 있다. 이 경우에 복호 알고리즘은 서명정보의 정확도가 인식되는 경우에만 다운로드될 수 있다. C2 콘텐트에 대한 복호 알고리즘은 이 경우 CPU(1201)에 의해 메모리 카드 라이터(1200)의 ROM(1202)에 포함된 전송을 위한 프로그램의 실행에 의해 퍼스널 컴퓨터(1100)로부터 PC 인터페이스(1204)를 통 해 제 2 콘텐트 처리부(1210)에 기록된다.
C1 및 C2 콘텐트 복호부에 의해 사용된 복호 알고리즘의 경우에서처럼 디스크키 암호화부(1220), 타이틀키 암호화부(1222) 및 오디오 데이터 암호화부(1223)에 의해 사용된 암호화 알고리즘은 다운로드될 수 있으며 서명정보의 정확도는 알고리즘이 다운로드될 때 인식된다.
이하 서명정보의 정확도의 인식예에 대해 설명하기로 한다. 복호 알고리즘 및 서명정보는 저작권을 보호하기 위한 중립기구에서 전송되는 것으로 가정한다. 서명정보는 비밀키를 이용하여 암호화되며, 비밀키에 대응하는 공개키는 미리 ROM(1202)에 저장되고, 서명정보는 서명정보를 인식할 수 있도록 상술한 프로그램을 실행함으로써 공개키를 사용하여 복호된다.
한편, 비록 C1 및 C2키가 제 1 및 제 2 실시예의 제어정보에 포함되더라도 C1 및 C2키는 C1 및 C2 콘텐트 복호부에 각각 저장된 키데이터일 수 있다.
(5) 제 1 및 제 2 실시예의 C1 및 C2 콘텐트에 대한 암호화 알고리즘은 DES 알고리즘으로 국한되는 것은 아니다. 인증 암호화부(2149)와 인증 암호화부(2260) 사이 및 인증부(2224)와 인증부(2310) 사이에서 실행되는 인증의 절차는 상술한 절차에 국한되는 것은 아니다. 한편 DES 알고리즘이 제 2 실시예의 암호화 알고리즘 E, F, G로서 사용되더라도 DES 알고리즘을 제외한 다른 알고리즘이 사용될 수도 있다.
암호화 알고리즘 E와 C2 콘텐트 복호부(1217)에 의해 사용되는 암호화 알고리즘은 동일한 DES 알고리즘일 수 있으며, 암호화 알고리즘 F 및 G와 MC 제어정보 암호화부(2270)에 의해 사용되는 암호화 알고리즘은 부분적으로 DES

알고리즘과 다른 모두 동일한 알고리즘이다. 더욱이 이들 각 암호화 알고리즘은 부분적으로 서로 다른 알고리즘일 수 있다. 즉 비록 알고리즘이 DES 알고리즘이 아니더라도 알고리즘의 부분이 어느 정도 공유되는 한 제조비용을 절감할 수 있다.

(6) 캡슐은 제 1 및 제 2 실시예에서는 통신회선을 통해 전송되나 그 경우로 국한되는 것은 아니다. 예컨대 캡슐은 광디스크와 같은 기록매체에 기록될 수 있다. 이 경우에 수신부(1110)는 기록매체로부터 캡슐을 판독하여 캡슐 저장부(1130)에 캡슐을 저장하는 것이 필요할 뿐이다.

(7) 타이틀키 생성부(1221)는 제 1 실시예에서는 적절한 방식으로 타이틀키를 생성하지만 그것에 국한되는 것은 아니다. 예컨대 타이틀키 생성부(1221)는 C2콘텐트 복호부(1217)가 출력을 갖고 음악 타이틀과 같은 데이터에 따라 타이틀키를 생성하는 C2 콘텐트를 참조하거나 또는 제어정보 복호부(1215)에 의한 복호의 결과인 제어정보의 C2키를 참조하여 C2키에 따라 타이틀키를 생성할 수 있다.

또한 타이틀키 생성부(1221)는 메모리 카드 라이터(1200)에 고유한 값에 따라 타이틀키를 생성할 수 있다.

(8) 디스크키 생성부(1218)는 제 1 실시예의 메모리 카드 ID에 따라 디스크키를 생성하지만 디스크 생성부(1218)는 메모리 카드 ID와 독립적인 디스크키를 생성할 수 있다. 디스크키는 후술하는 방식으로 생성될 수 있다. 매체에 고유한 마스터키에 의해 암호화된 고유 디스크키는 메모리 카드에 기록되는 것으로 가정되며, 디스크키 생성부(1218)는 마스터키를 사용하여 고유 디스크키를 복호함으로써 디스 크키를 생성한다. 이 경우에 디스크 암호화부(1220)는 제 2 콘텐트 처리부(1210)에 포함될 필요가 없으며, 타이틀키와 암호화된 오디오 데이터는 메모리 카드에 기록될 필요가 있다.

(9) 오디오 데이터 암호화부(1223)는 C2 콘텐트, 즉 제 1 실시예의 오디오 데이터를 암호화하지만 오디오 데이터 암호화부(1223)는 C2 콘텐트의 부분을 암호화하여 C2콘텐트를 출력할 수 있다.

(10) 복수의 마스터키는 제 1 실시예에서는 미리 제 2 콘텐트 처리부(1210)에 저장되어 있으나 하나의 마스터키가 저장될 수 있다.

또한 제 2 콘텐트 처리부(1210)는 통신회선과 퍼스널 컴퓨터를 통해 외부 네트웍으로부터 마스터키를 다운로드할 수 있으며, 다운로드된 마스터키를 저장한다. 제 2 콘텐트 처리부(1210)는 특정 마스터키를 제거하는 기능을 가질 수 있다. 더욱이 제 2 콘텐트 처리부(1210)는 마스터키의 정확도가 서명정보로 인식될 수 있을 경우에만 마스터키를 다운로드할 수 있다. 마스터키는 이 경우에 CPU(1202)에 의해 메모리 카드 라이터(1200)의 ROM(1202)에 포함된 전송용 프로그램의 실행에 의해 퍼스널 컴퓨터(1100)로부터 PC 인터페이스를 거쳐 제 2 콘텐트 처리부(1210)에 기록된다. 여기에서 서명정보는 상술한 복호 알고리즘의 경우와 동일한 방식으로 인식된다.

마찬가지로 외부 네트웍으로부터 특정 마스터키를 제거하라는 명령을 받으면 특정 마스터키는 서명정보의 정확도가 인식될 때만 제거될 수 있다.

(11) 제 1 실시예에서는 메모리 카드의 인증이 실행되고(단계 S401), 인증이 성공적으로 수행되지 않았을 때에는 오디오 데이터가 암호화되지 않고 기록된다(단계 S402). 인증실패의 경우에는 메모리 카드에의 기록만이 금지되어야만 한다. 결국 오디오 데이터는 어느 경우에도 암호화될 수 있으며, 암호화의 결과인 데이터는 예컨대 인증실패에 대해서만 제 2 콘텐트 처리부(1210)로부터 출력되지 않게 할 수 있다.

(12) 제 1 실시예에서 메모리 카드에 암호화된 데이터를 기록하는 절차(단계 S406, S408, S409)는 이 순서로 국한되는 것은 아니다. 기록절차는 임의의 순서로 실행될 수도 있다.

한편 복수 콘텐트의 데이터는 동일한 메모리 카드에 기록될 수 있다. 이 경우에 타이틀키 생성부(1221)는 콘텐트의 수에 대응하는 수의 타이틀키를 생성하며, 타이틀키 암호화부(1222)는 콘텐트의 수에 대응하는 수의 암호화된 타이틀키를 출력하고, 오디오 데이터 암호화부(1223)는 콘텐트의 수에 대응하는 수의 암호화된 데이터를 출력한다.

(13) 캡슐은 제 1 실시예의 저작권 보호센터에 의해 생성되나 캡슐은 예컨대 콘텐트 공급자 및 다른 공급자에 의해 생성될 수 있다. 이 경우에 콘텐트 공급자나 다른 공급자는 공개키를 사용하여 캡슐 고유키를 암호화하고 재생장치는 보안성을 높이기 위해 공개키에 대응하는 비밀키를 사용하여 암호화된 캡슐 고유키를 복호할 수 있다.

(14) 제 1 실시예에서 부과금 처리시 지불명령 정보가 송신되지만 이 정보의 전송에 국한되는 것은 아니다. 예컨대 복호의 수는 부과금 정보에 포함될 수 있고 부과금 정보는 암호화되어 요금 부과기관에 전송될 수 있다.

이 경우에 부과금 정보는 콘텐트로 고려될 수 있고 캡슐과 동일한 포맷으로 암호화되어 전송된다. 이러한 목적을 위해 캡슐을 생성하는 암호화부는 제 1 콘텐트 처리부(1140)와 제 2 콘텐트 처리부(1210)에 포함될 수 있다. 이들 암호화부의 암호화는 도 4 및 도 5에 도시된 캡슐의 생성과 동일한 절차를 따라 실행될 필요가 있다.

기록부(1240)는 메모리 카드와 같은 기록매체에 콘텐트를 기록할 때 복호조건정보와 부과금 정보를 기록할 수 있다. 이 경우, 복호조건 정보와 부과금 정보 또한 더욱 엄격한 조건으로 기록될 수 있다. 그렇게 함으로써 기록매체에 기록한 후 콘텐트의 재생을 제어하고 요금을 부과할 수 있다.

또한 비록 제 2 실시예에서 설명된 제어정보가 제어정보(20)에 포함되어 있지 않지만 MC 제어정보 암호화부(2270)는 부과금 정보를 포함하는 MC 제어정보와, 미리 저장된 정보를 사용하여 MC 암호화된 C2 콘텐트(2340)의 복호조건과 재생 및 복사제어에 관한 정보를 계산할 수 있으며, 계산된 정보를 암호화하여 암호화된 정보를 MC 암호화 제어정보(2330)로서 메모리 카드(2300)에 기록할 수 있다.

(15) 비트열 K는 제 2 실시예에서 값 E(R1) 및 E(R2)의 배타적 논리합 연산에 의해 취득되나 비트열의 취득이 이 실시예에 국한되는 것은 아니다. 인증 암호화부(2149, 2260) 만이 비트열 K를 공통으로 취득하거나 유도하지 않으면 안된다.

또한 C2'키는 메모리 카드 고유키와 난수의 배타적 논리합에 의해 실행될 수 없다.

비록 본 발명이 첨부도면을 참조로 한 실시예에 의해 충분히 설명되고 있으나 당업자라면 이들로부터 다양한 변경과 수정을 가하여 실시할 수 있음이 명백하다. 따라서 이러한 변경과 수정이 본 발명의 사상으로부터 벗어나지 않는 것

이라면 이들은 본 발명에 포함되는 것으로 간주되어야만 한다.

## 발명의 효과

상술한 바와 같이 본 발명의 저작물 보호 시스템에 의해 제 1 및 제 2 콘텐트가 취득되면 상이한 2개의 중요도에 기인하여 상이한 정도의 암호화가 실행되는 각각의 콘텐트에 대하여, 제 1 및 제 2 콘텐트가 각각 별도로 복호되므로 풀기 어려운 암호화에 의해 더 중요한 제 2 콘텐트를 부정행위로부터 강력하게 보호할 수 있다.
게다가 제 2 콘텐트의 배포 및 기록에 대하여 상이한 암호화가 이용되므로 비록 하나의 암호화 알고리즘이 복호되더라도 그것에 의해 다른 하나가 영향을 받지는 않는다.
또 제 2 콘텐트 복호부에 의해 사용되는 암호화 알고리즘은 암호화부에 의해 암호화를 위해 사용되는 암호화 알고리즘과 부분적으로 다르고, 암호화 알고리즘을 실현하는 소프트웨어나 하드웨어의 부분이 공유되므로 암호화 알고리즘을 개발하거나 실현하는데 드는 비용을 소프트웨어나 하드웨어의 부분이 공유되지 않는 경우에 비해 감축시킬 수 있다

## (57) 청구의 범위

### 청구항 1.
멀티미디어 데이터를 보호하는 저작물 보호 시스템에 있어서,
제 1 암호화가 실행된 제 1 데이터와, 제 1 데이터의 콘텐트와 동일한 정보를 나타내지만 품질이 보다 낮은 콘텐트를 가지며, 제 1 암호화보다 풀기가 더 어려운 제 2 암호화가 실행된 제 2 데이터를 취득하는 취득수단(1110, 1130)과,
상기 제 1 데이터가 상기 취득수단에 의해 취득될 때 제 1 암호화에 대응하는 제 1 복호방법을 사용하여 제 1 데이터를 복호하는 제 1 데이터 복호수단(1140), 및
상기 제 2 데이터가 상기 취득수단에 의해 취득될 때 제 2 암호화에 대응하는 제 2 복호방법을 사용하여 제 2 데이터를 복호하는 제 2 데이터 복호수단(1211, 1212, 1213, 1215, 1216 및 1217)을 포함하는 것을 특징으로 하는 저작물 보호 시스템.

### 청구항 2.
제 1 항에 있어서,
상기 취득수단과 제 1 데이터 복호수단은 데이터를 복호하는 소프트웨어를 실행하는 퍼스널 컴퓨터에 의해 실현되고,
제 2 데이터 복호수단은 부정조작이 불가능한 하드웨어와, 부정조작이 불가능한 소프트웨어를 실행하는 장치 중 하나에 의해 실현되는 것을 특징으로 하는 저작물 보호 시스템.

### 청구항 3.
제 2 항에 있어서,
상기 취득수단은 외부 네트웍으로부터 데이터를 수신함으로써 데이터를 취득하며,
상기 저작물 보호 시스템은,
제 1 콘텐트 복호수단에 의해 복호된 제 1 데이터의 콘텐트를 시청각적으로 재생하는 재생수단과,
제 2 데이터 복호수단에 의해 복호된 제 2 데이터에 대하여 제 2 암호화와 다른 제 3 암호화를 실행하는 암호화수단과,
상기 암호화수단에 의해 제 3 암호화가 실행된 제 2 데이터의 콘텐트의 적어도 일부를 기록매체에 기록하는 기록수단을 추가로 포함하는 것을 특징으로 하는 저작물 보호 시스템.

### 청구항 4.
제 3 항에 있어서,
상기 암호화수단과, 상기 제 2 데이터 복호수단과 상기 암호화수단 사이의 데이터 통신 채널은 부정조작이 불가능한 하드웨어와 부정조작이 불가능한 소프트웨어를 실행하는 장치 중의 하나에 의해 실현되는 것을 특징으로 하는 저작물 보호 시스템.

### 청구항 5.
제 3 항에 있어서,
상기 제 2 데이터 복호수단에 의해 사용되는 암호화 알고리즘은 상기 암호화수단에 의한 암호화에 사용되는 암호화 알고리즘과 부분적으로 다른 것을 특징으로 하는 저작물 보호 시스템.

### 청구항 6.
제 3 항에 있어서,
소정의 인터페이스를 통해 퍼스널 컴퓨터에 접속하는 PC 접속수단과,
기록매체가 세트되는 기록매체 로딩수단을 추가로 포함하며,
상기 제 2 데이터 복호수단과, 상기 암호화수단과, 상기 기록수단과, 상기 PC 접속수단과, 상기 기록매체 로딩수단은 하나의 하드웨어에 의해 실현되고,
상기 제 2 데이터 복호수단은 상기 PC 접속수단을 통해 상기 취득수단에 의해 취득된 데이터의 제 2 데이터의 콘텐트를 취득하여 취득된 제 2 콘텐트를 복호하며,
상기 기록수단은 상기 기록매체 로딩수단에 세트된 상기 기록매체에 제 2 데이터의 콘텐트를 기록하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 7.**
제 2 항에 있어서,
상기 취득수단에 의해 취득되는 데이터는 취득된 데이터에 포함된 각 콘텐트에 대한 처리를 제어하는 암호화되어 있는 제어정보를 포함하며,
상기 제 1 데이터 복호수단과 상기 제 2 데이터 복호수단 중의 적어도 하나는 상기 제어정보를 복호하는 제어정보 복호부를 포함하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 8.**
제 7 항에 있어서,
상기 제 2 데이터 복호수단은 상기 제어정보 복호부를 포함하며,
상기 제 2 데이터 복호수단을 실현하는 퍼스널 컴퓨터는 제어정보를 복호하는 소프트웨어를 추가로 실행하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 9.**
제 8 항에 있어서,
상기 제어정보는 제 2 데이터를 복호하기 위해 사용되는 키를 포함하고,
상기 제어정보 복호부는 제 1 인증 암호화부를 추가로 포함하며,
상기 제 2 데이터 복호수단은 제 2 인증 암호화부를 추가로 포함하고,
상기 제 1 인증 암호화부는 상기 제 2 인증 암호화부의 인증을 실행하며, 상기 제 2 인증 암호화부와 암호화 통신을 실행하고, 인증이 성공적으로 실행되었을 때 상기 제어정보 복호부에 의해 복호된 제어정보의 키를 제 2 인증 암호화부에 송신하며,
상기 제 2 인증 암호화부는 제 1 인증 암호화부의 인증을 실행하고, 제 1 인증 암호화부와 암호화 통신을 실행하며, 키를 취득하고,
상기 제 2 데이터 복호수단은 상기 제 2 인증 암호화부가 취득한 키를 사용하여 제 2 데이터를 복호하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 10.**
제 1 항에 있어서,
상기 취득수단과 제 1 데이터 복호수단은 데이터를 복호하는 소프트웨어를 실행하는 장치에 의해 실현되고,
상기 제 2 데이터 복호수단은 부정조작이 불가능한 하드웨어와, 부정조작이 불가능한 소프트웨어를 실행하는 장치 중 하나에 의해 실현되는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 11.**
제 10 항에 있어서,
상기 취득수단은 외부 네트웍으로부터 데이터를 수신함으로써 데이터를 취득고,
상기 제 1 데이터의 콘텐트와 제 2 데이터의 콘텐트는 상이한 스타일의 디지털 데이터로 표현된 동일한 저작물인 것을 특징으로 하는 저작물 보호 시스템.

**청구항 12.**
제 11 항에 있어서,
상기 제 2 데이터 복호수단에 의해 복호된 제 2 데이터에 대하여 제 2 암호화와 다른 제 3 암호화를 실행하는 암호화수단과,
상기 암호화수단에 의해 제 3 암호화가 실행된 제 2 데이터의 콘텐트의 적어도 일부를 기록매체에 기록하는 기록수단을 추가로 포함하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 13.**
제 12 항에 있어서,
상기 암호화수단과, 상기 제 2 데이터 복호수단과 상기 암호화수단 사이의 데이터 통신 채널은 부정조작이 불가능한 하드웨어와 부정조작이 불가능한 소프트웨어를 실행하는 장치 중의 하나에 의해 실현되는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 14.**
제 12 항에 있어서,
상기 제 1 데이터의 콘텐츠는 시험용 음악 콘텐트이고,
상기 제 2 데이터의 콘텐트는 판매용 음악 콘텐트로서 제 1 데이터의 콘텐트보다 높은 음질을 갖는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 15.**
제 14 항에 있어서,
상기 제 1 데이터 복호수단에 의해 복호된 제 1 데이터의 콘텐트를 재생하는 재생수단을 추가로 포함하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 16.**
제 12 항에 있어서,
상기 제 2 데이터 복호수단에 의해 사용되는 암호화 알고리즘은 상기 암호화 수단에 의한 암호화에 사용되는 암호화 알고리즘과 부분적으로 다른 것을 특징으로 하는 저작물 보호 시스템.

**청구항 17.**

제 12 항에 있어서,
상기 암호화수단은,
미리 마스터키를 저장하는 마스터키 저장부와,
디스크키를 생성하는 디스크키 생성부와,
상기 마스터키를 사용하여 상기 디스크키 생성부에 의해 생성된 디스크키를 암호화하는 디스크키 암호화부와,
타이틀키를 생성하는 타이틀키 생성부와,
상기 디스크키를 사용하여 상기 타이틀키 생성부에 의해 생성된 타이틀키를 암호화하는 타이틀키 암호화부와,
상기 타이틀키를 사용하여 상기 제 2 데이터 복호수단에 의해 복호된 제 2 데이터의 적어도 일부를 암호화하는 데이터 암호화부를 포함하며,
상기 기록수단은 상기 디스크키 암호화부에 의해 암호화된 디스크키와, 상기 타이틀키 암호화부에 의해 암호화된 타이틀키와, 상기 데이터 암호화부에 의해 암호화된 제 2 데이터를 기록매체에 기록하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 18.**

제 17 항에 있어서,
상기 기록매체에 고유한 고유정보는 미리 기록매체에 기록되고,
상기 디스크키 생성부는 기록매체 상의 고유정보에 따라 디스크키를 생성하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 19.**

제 17 항에 있어서,
상기 타이틀키 생성부는 상기 제 2 데이터 복호수단에 의해 복호된 제 2 데이터의 일부분인 정보에 따라 상기 타이틀키를 생성하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 20.**

제 12 항에 있어서,
마스터키를 사용하여 암호화된 상기 기록매체에 고유한 고유 디스크키는 미리 상기 기록매체에 기록되고,
상기 암호화수단은
상기 마스터키를 미리 저장하는 마스터키 저장부와,
상기 마스터키를 사용하여 상기 기록매체에 상기 고유 디스크키를 복호함으로써 디스크키를 생성하는 디스크키 생성부와,
타이틀키를 생성하는 타이틀키 생성부와,
상기 디스크키를 사용하여 상기 타이틀키 생성부에 의해 생성된 타이틀키를 암호화하는 타이틀키 암호화부와,
상기 타이틀키를 사용하여 제 2 데이터 복호수단에 의해 복호된 제 2 데이터의 적어도 일부를 암호화하는 데이터 암호화부를 포함하며,
상기 기록수단은 상기 타이틀키 암호화부에 의해 암호화된 타이틀키와 상기 데이터 암호화부에 의해 암호화된 제 2 데이터를 상기 기록매체에 기록하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 21.**

제 12 항에 있어서,
상기 기록매체는 인증정보를 송신하는 기록장치 인증부를 포함하며,
상기 기록수단은 상기 기록장치 인증부로부터 송신된 인증정보에 따라 상기 기록매체의 정확성을 판정하여 기록매체가 정확할 때에만 제 3 암호화가 실행된 제 2 데이터의 적어도 일부가 상기 기록매체에 기록되는 기록을 실행하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 22.**

제 10 항에 있어서,
상기 제 2 데이터 복호수단에 의해 복호된 제 2 데이터에 대하여 제 2 암호화와 다른 제 3 암호화를 실행하는 암호화수단과,
상기 암호화수단에 의해 제 3 암호화가 실행된 제 2 데이터의 적어도 일부를 기록매체에 기록하는 기록수단을 추가로 포함하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 23.**

제 22 항에 있어서,
상기 제 2 데이터 복호수단에 의해 사용되는 암호화 알고리즘은 상기 암호화 수단에 의한 암호화에 사용되는 암호화 알고리즘과 부분적으로 다른 것을 특징으로 하는 저작물 보호 시스템.

**청구항 24.**

제 10 항에 있어서,
상기 취득수단에 의해 취득되는 데이터는 취득되는 데이터가 제 1 데이터의 콘텐트를 포함할 때 제 1 데이터의 복호에 관한 부과금 정보인 제 1 데이터 부과금 정보를 포함하고, 취득되는 데이터가 제 2 데이터의 콘텐트를 포함할 때 제 2 데이터의 복호에 관한 부과금 정보인 제 2 데이터 부과금 정보를 포함하며,
상기 제 1 데이터 복호수단은 제 1 데이터가 복호될 때 제 1 데이터 부과금 정보에 따라 부과금 처리를 실행하며,
상기 제 2 데이터 복호수단은 제 2 데이터가 복호될 때 제 2 데이터 부과금 정보에 따라 부과금 처리를 실행하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 25.**
제 1 항에 있어서,
상기 제 1 암호화는 제 1 키를 사용하여 실행되며,
상기 제 2 암호화는 제 1 키보다 데이터 크기가 큰 제 2 키를 사용하여 실행되고,
상기 취득수단에 의해 취득되는 데이터는 제 1 및 제 2 키를 가지며 취득되는 데이터에 포함된 각 콘텐트에 관한 처리를 제어하는 제어정보를 추가로 포함하고,
상기 제 1 데이터 복호수단은 제 1 키를 사용하여 제 1 데이터를 복호하며,
상기 제 2 데이터 복호수단은 제 2 키를 사용하여 제 2 데이터를 복호하는 것을 특징으로 하는 저작물 보호 시스템.

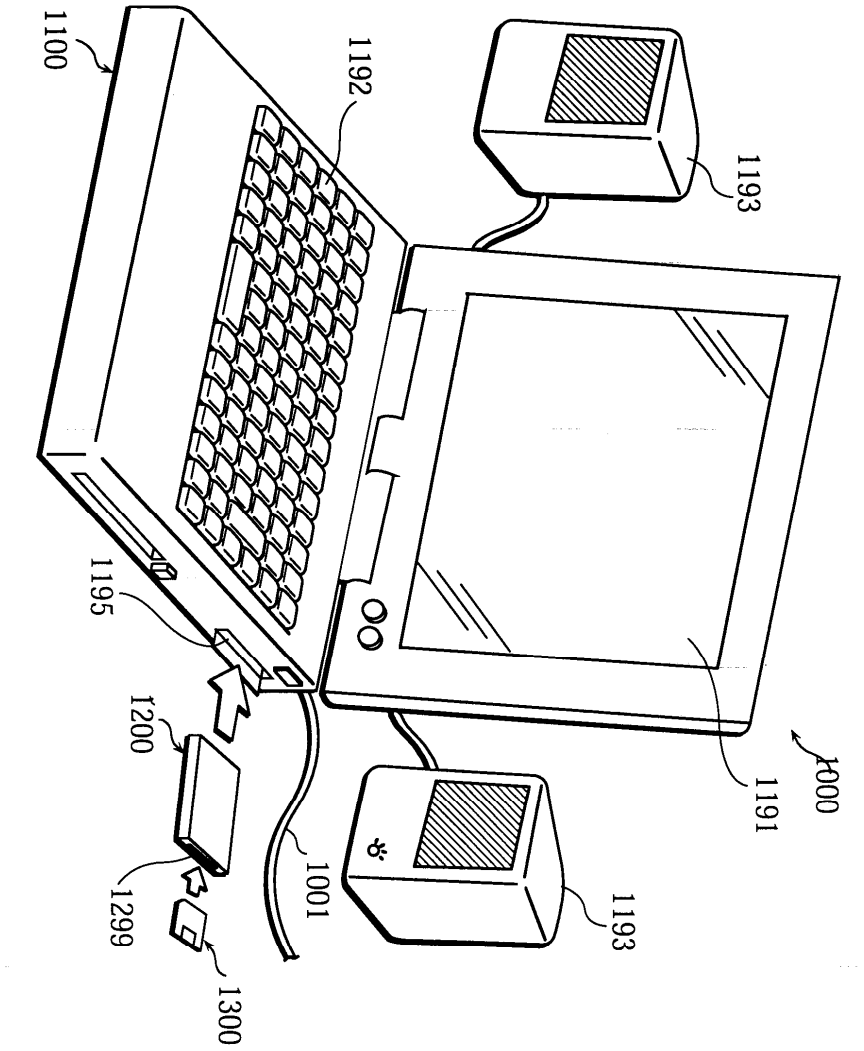
**청구항 26.**
제 25 항에 있어서,
상기 제어정보는 제 3 키와 시스템 공통키로부터 유도된 제어키를 사용하여 암호화되고, 상기 취득수단에 의해 취득되는 데이터에 포함되며,
상기 제 3 키는 제 4 키를 사용하여 암호화되고 취득되는 데이터에 포함되고,
상기 제 1 데이터 복호수단은 제 4 키에 대응하는 제 5 키와 시스템 공통키를 미리 저장하고, 제 5 키를 사용하여 제 3 키를 복호하며, 상기 복호된 제 3 키와 시스템 공통키로부터 제어키를 유도하고, 상기 제어키를 사용하여 제어정보를 복호하는 제 1 제어정보 복호부를 포함하며,
상기 제 2 데이터 복호수단은 제 4 키에 대응하는 제 5 키와 시스템 공통키를 미리 저장하고, 제 5 키를 사용하여 제 3 키를 복호하며, 상기 복호된 제 3 키와 시스템 공통키로부터 제어키를 유도하고, 상기 제어키를 사용하여 제어정보를 복호하는 제 2 제어정보 복호부를 포함하는 것을 특징으로 하는 저작물 보호 시스템.

**청구항 27.**
제 1항에 있어서,
상기 제 2 데이터는 판매용 음악 콘텐트이고,
제 1 데이터는 보다 낮은 품질의 판매용 음악 콘텐트의 오디오를 나타내는 시험용 음악 콘텐트이며,
상기 취득수단은 제 1 데이터 및 제 2 데이터가 조합된 데이터를 외부의 네트웍으로부터 취득하고,
상기 저작물 보호 시스템은
상기 제 1 데이터 취득수단에 의해 복호된 제 1 데이터의 음악을 재생하는 재생수단(1150)과,
상기 제 2 데이터 복호수단에 의해 복호된 제 2 데이터에 대하여 제 2 암호화와 다른 제 3 암호화를 실행하는 암호화수단(1218, 1219, 1220, 1221, 1222 및 1223)과,
상기 암호화수단에 의해 제 3 암호화가 실행된 제 2 데이터의 적어도 일부분을 기록매체에 기록하는 기록수단(1240)을 추가로 포함하며,
상기 취득수단과 제 1 데이터 복호수단은 콘텐트를 복호하는 소프트웨어를 실행하는 퍼스널 컴퓨터에 의해 실현되고,
상기 제 2 데이터 복호수단과, 상기 암호화수단과, 상기 제 2 데이터 복호수단과 상기 암호화수단 사이의 데이터 통신 채널은 부정조작이 불가능한 하드웨어와 부정조작이 불가능한 소프트웨어를 실행하는 장치중의 하나에 의해 실현되는 것을 특징으로 하는 저작물 보호 시스템.

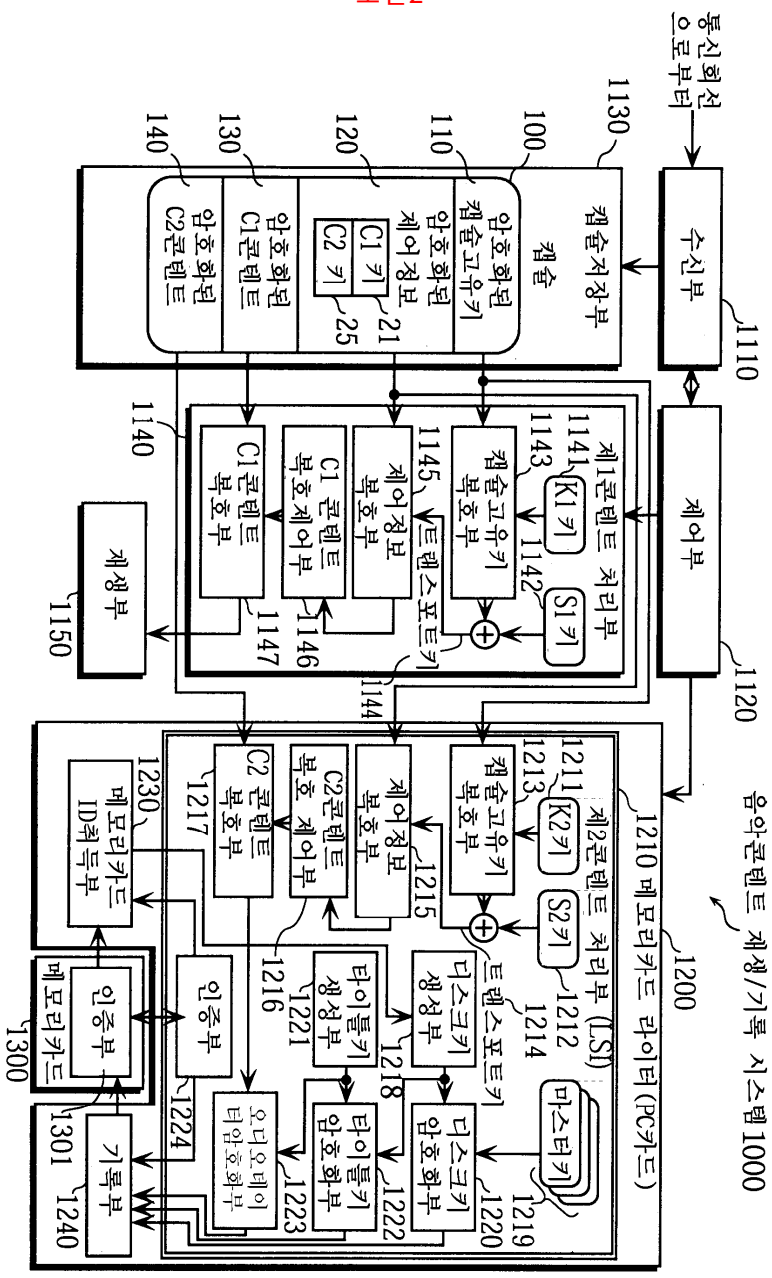
**청구항 28.**
제 27 항에 있어서,
상기 제 2 데이터 복호수단에 의해 사용되는 암호화 알고리즘은 상기 암호화 수단에 의한 암호화에 사용되는 암호화 알고리즘과 부분적으로 다른 것을 특징으로 하는 저작물 보호 시스템.

도면

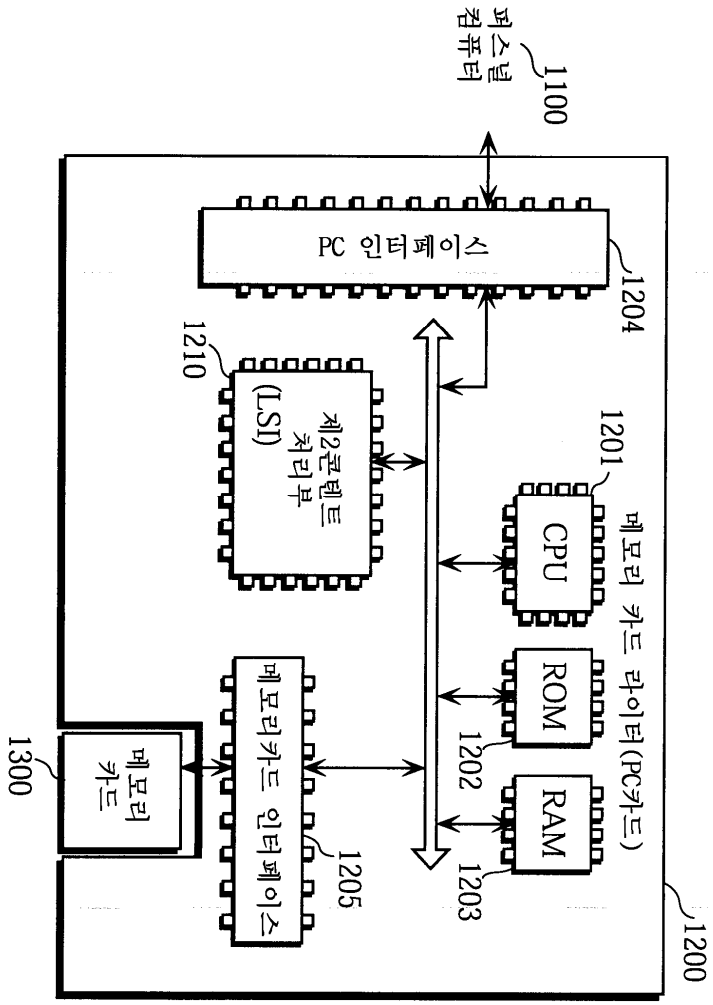
도면1



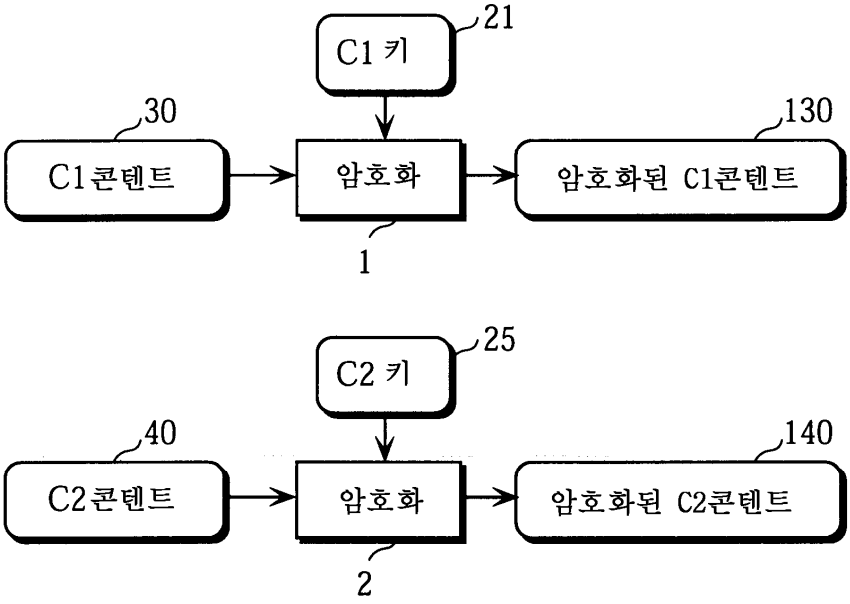
도면2


통신회선으로부터
수신부
1110
제어부
1120
음악콘텐트 재생/기록 시스템 1000
캡슐저장부
캡슐
1130
100
암호화된 캡슐고유키
암호화된 제어정보
C1 키
C2 키
21
25
110
120
암호화된 C1콘텐트
130
암호화된 C2콘텐트
140
제1콘텐트 처리부
1140
K1키
1141
1143
캡슐고유키 복호부
1142
S1키
제어정보 복호부
1145
트렌스포트키
C1 콘텐트 복호부
C1 콘텐트 복호제어부
1146
1147
재생부
1150
1144
제2콘텐트 처리부 (LSI)
1210
메모리카드 라이터 (PC카드)
1200
K2키
1211
1213
캡슐고유키 복호부
S2키
1212
1214
트렌스포트키
마스터키
1219
디스크키 생성부
디스크키 암호화부
1220
타이틀키 생성부
1221
타이틀키 암호화부
1222
오디오데이터 암호화부
1223
1218
C2 콘텐트 복호부
1217
C2콘텐트 복호 제어부
1216
제어정보 복호부
1215
메모리카드 ID취득부
1230
인증부
1224
메모리카드
1300
인증부
기록부
1301
1240

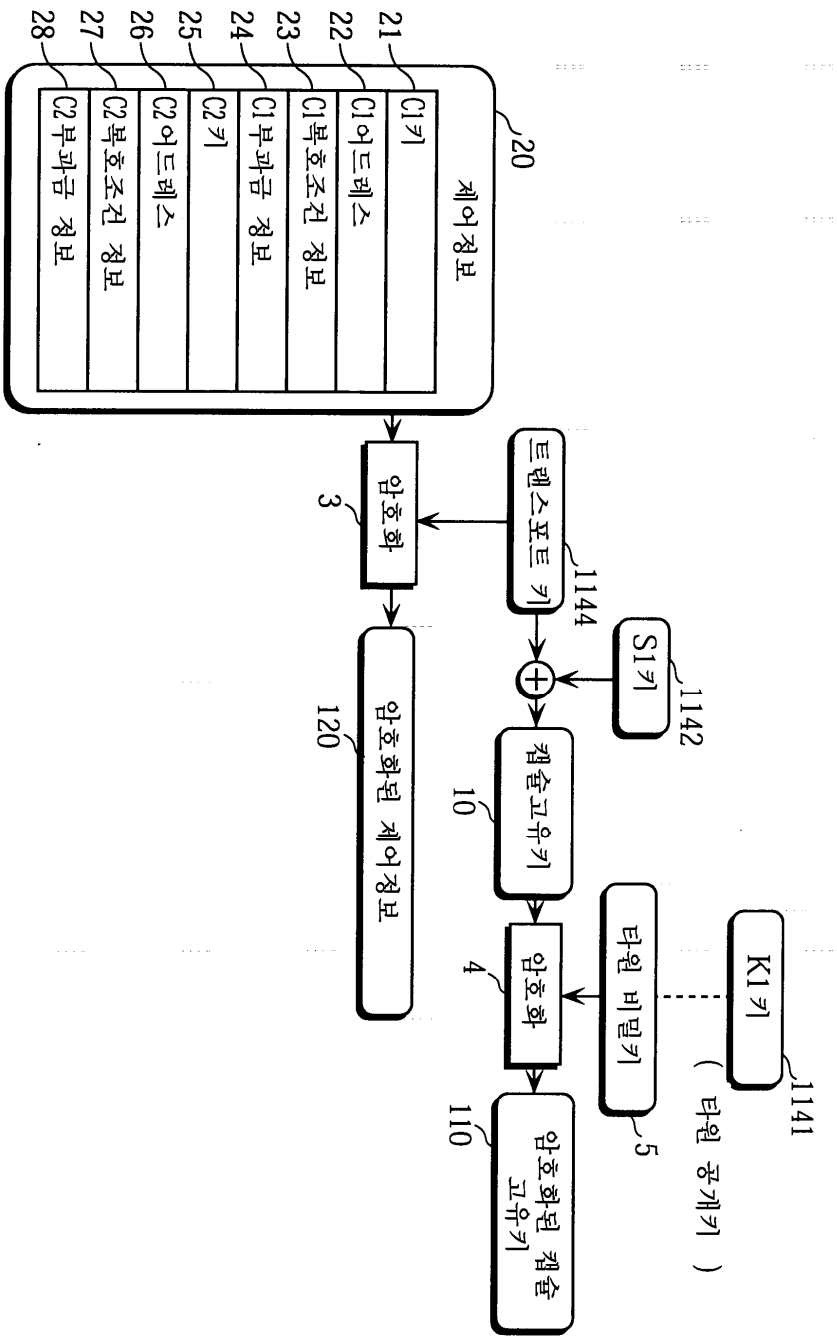
도면3


퍼스널 컴퓨터
1100
PC 인터페이스
1204
1210
제2콘텐트 처리부 (LSI)
1201
CPU
메모리 카드 라이터(PC카드)
ROM
RAM
1202
1203
메모리카드 인터페이스
1205
메모리 카드
1300
1200

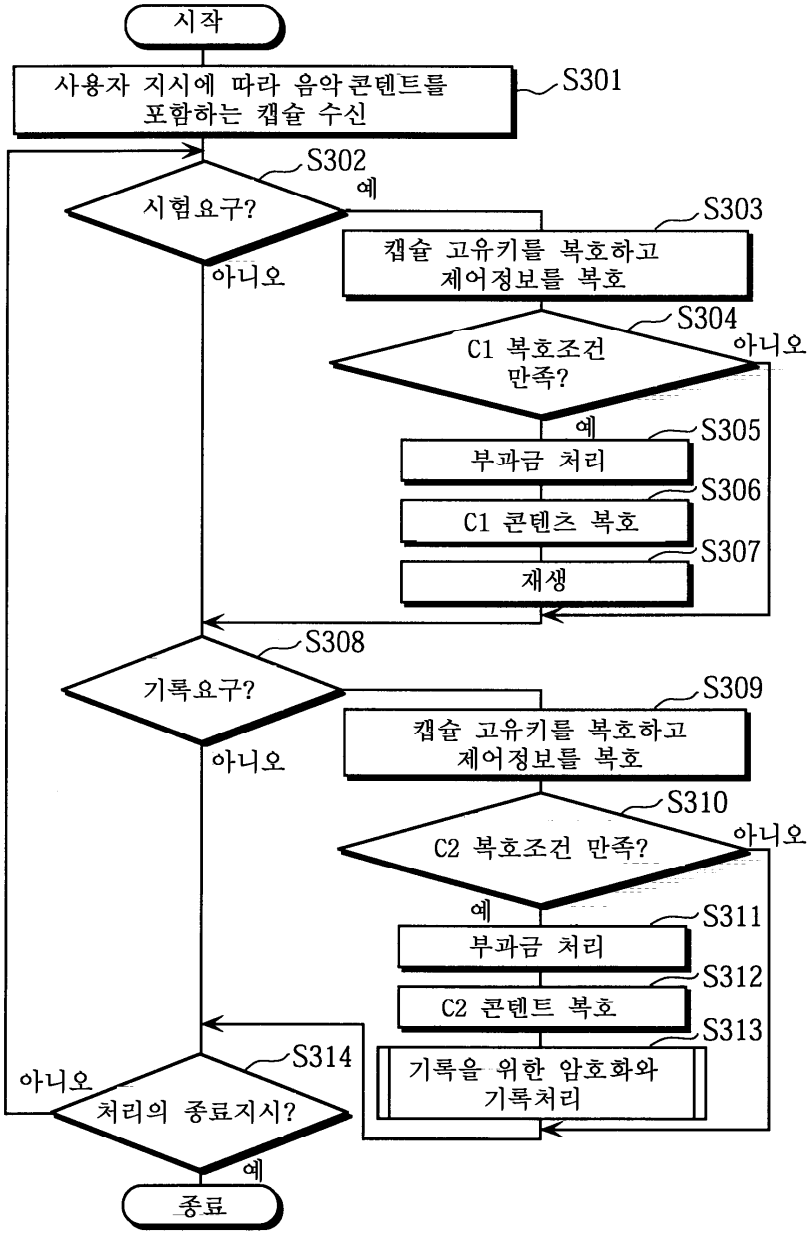
도면4


C1 키
21
30
C1콘텐트
암호화
130
암호화된 C1콘텐트
1
C2 키
25
40
C2콘텐트
암호화
140
암호화된 C2콘텐트
2

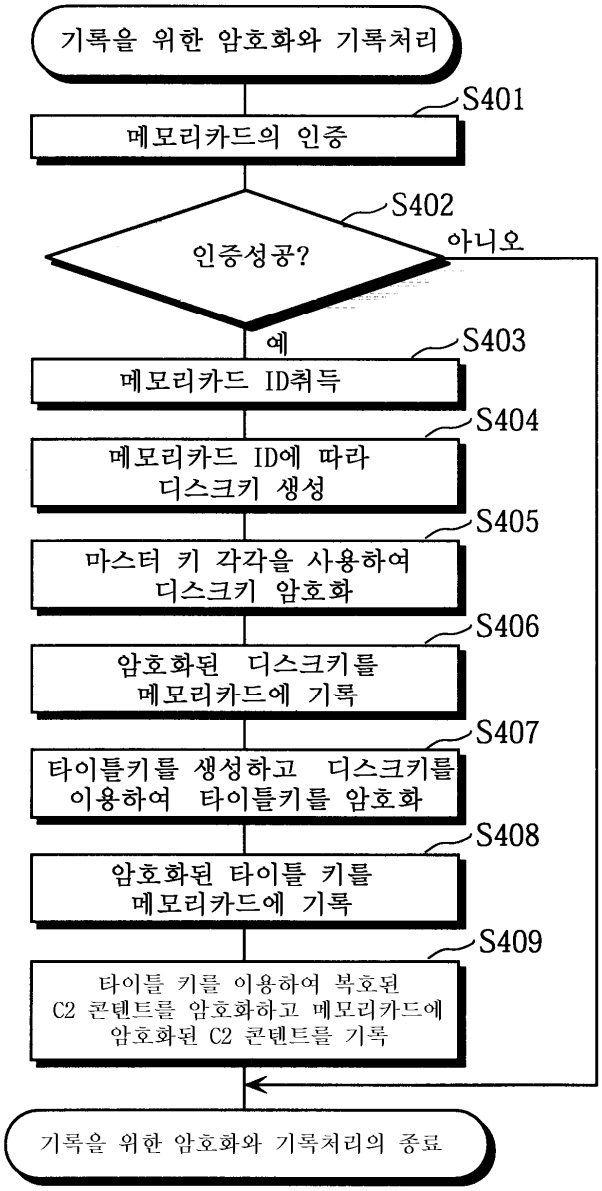
도면5


제어정보
20
C1키
C1어드레스
C1복호조건 정보
C1부과금 정보
C2키
C2어드레스
C2복호조건 정보
C2부과금 정보
21
22
23
24
25
26
27
28
암호화
3
트랜스포트 키
1144
S1키
1142
캡슐고유키
10
암호화
4
타원 비밀키
5
K1키
1141
( 타원 공개키 )
암호화된 캡슐 고유키
110
암호화된 제어정보
120

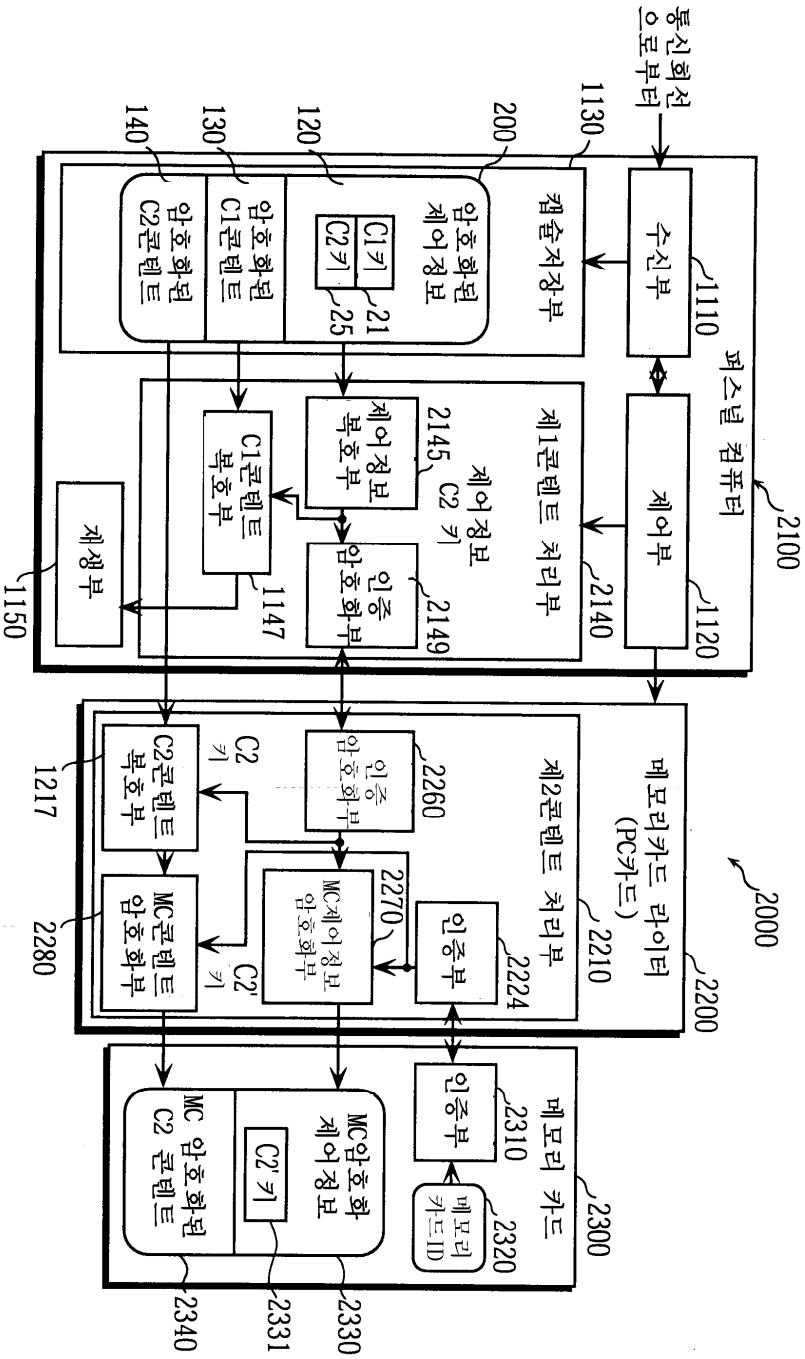
도면6


시작
사용자 지시에 따라 음악 콘텐트를 포함하는 캡슐 수신
S301
S302
시험요구?
예
아니오
S303
캡슐 고유키를 복호하고 제어정보를 복호
S304
C1 복호조건 만족?
아니오
예
S305
부과금 처리
S306
C1 콘텐츠 복호
S307
재생
S308
기록요구?
아니오
S309
캡슐 고유키를 복호하고 제어정보를 복호
S310
C2 복호조건 만족?
아니오
예
S311
부과금 처리
S312
C2 콘텐트 복호
S313
기록을 위한 암호화와 기록처리
S314
아니오
처리의 종료지시?
예
종료

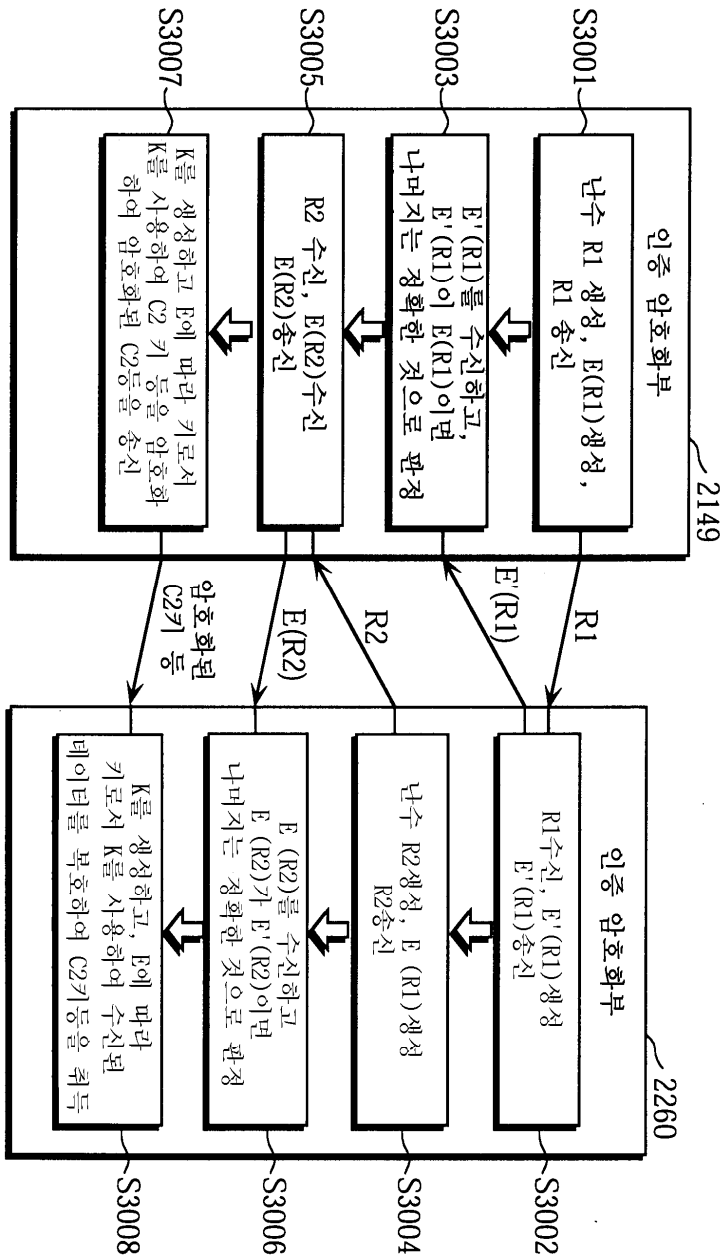
도면7


기록을 위한 암호화와 기록처리
S401
메모리카드의 인증
S402
인증성공?
아니오
예
S403
메모리카드 ID취득
S404
메모리카드 ID에 따라
디스크키 생성
S405
마스터 키 각각을 사용하여
디스크키 암호화
S406
암호화된 디스크키를
메모리카드에 기록
S407
타이틀키를 생성하고 디스크키를
이용하여 타이틀키를 암호화
S408
암호화된 타이틀 키를
메모리카드에 기록
S409
타이틀 키를 이용하여 복호된
C2 콘텐트를 암호화하고 메모리카드에
암호화된 C2 콘텐트를 기록
기록을 위한 암호화와 기록처리의 종료

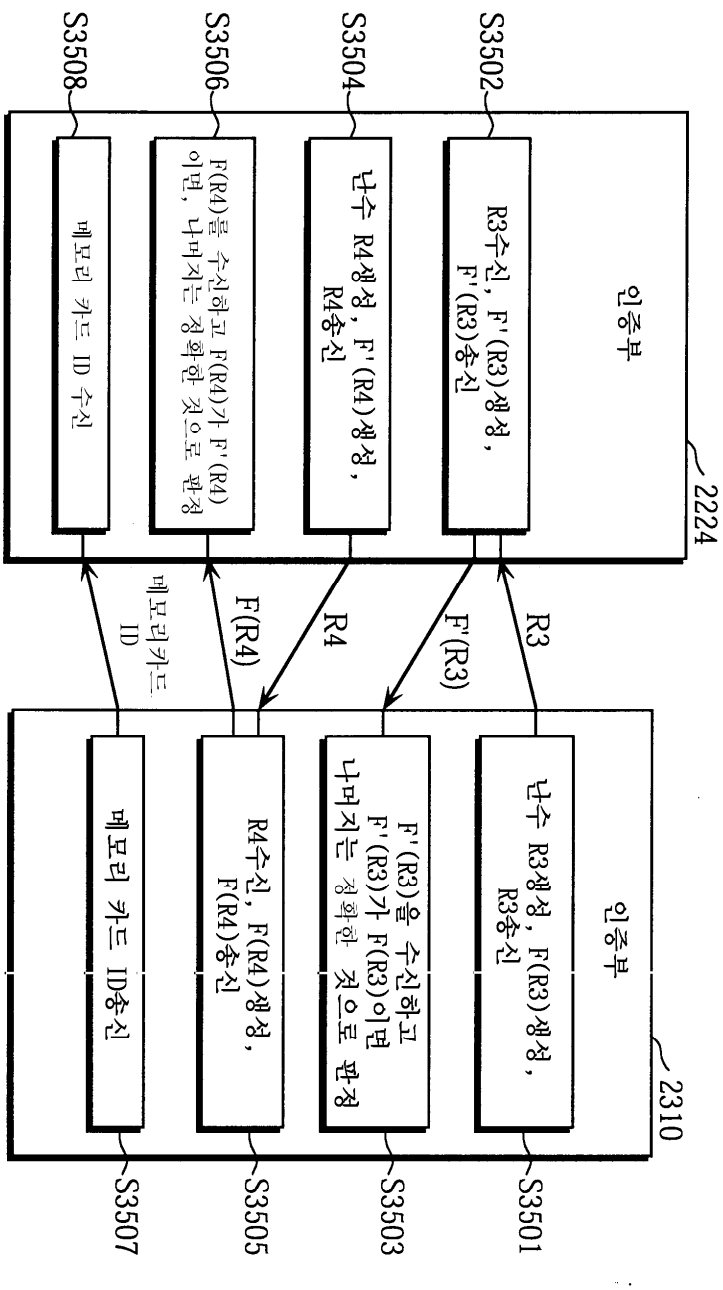
도면8


통신회선으로부터
1130
수신부
1110
퍼스널 컴퓨터
2100
캡슐저장부
200
암호화된 제어정보
C1키
C2키
21
25
120
암호화된 C1콘텐트
130
암호화된 C2콘텐트
140
제1콘텐트 처리부
2140
제어부
1120
제어정보 복호부
2145
C2 키
C1콘텐트 복호부
1147
인증 암호화부
2149
재생부
1150
메모리카드 라이터 (PC카드)
2000
제2콘텐트 처리부
2210
2200
인증 암호화부
2260
C2 키
C2콘텐트 복호부
1217
2270
MC제어정보 암호화부
C2' 키
인증부
2224
MC콘텐트 암호화부
2280
메모리 카드
2300
인증부
2310
메모리 카드ID
2320
MC암호화 제어정보
C2' 키
2331
2330
MC 암호화된 C2 콘텐트
2340

도면9


S3001
S3003
S3005
S3007
인증 암호화부
난수 R1 생성, E(R1)생성,
R1 송신
E'(R1)를 수신하고,
E'(R1)이 E(R1)이면
나머지는 정확한 것으로 판정
R2 수신, E(R2)수신
E(R2)송신
K를 생성하고 E에 따라 키로서
K를 사용하여 C2 키 등을 암호화
하여 암호화된 C2등을 송신
2149
R1
E'(R1)
R2
E(R2)
암호 화된
C2키 등
인증 암호화부
R1수신, E'(R1)생성
E'(R1)송신
난수 R2생성, E (R1)생성
R2송신
E (R2)를 수신하고
E (R2)가 E'(R2)이면
나머지는 정확한 것으로 판정
K를 생성하고, E에 따라
키로서 K를 사용하여 수신된
데이터를 복호하여 C2키등을 취득
2260
S3002
S3004
S3006
S3008

도면10


인증부
2224
R3수신, F'(R3)생성,
F'(R3)송신
난수 R4생성, F''(R4)생성,
R4송신
F(R4)를 수신하고 F(R4)가 F'(R4)
이면, 나머지는 정확한 것으로 판정
메모리 카드 ID 수신
S3502
S3504
S3506
S3508
R3
F'(R3)
R4
F(R4)
메모리카드
ID
인증부
2310
난수 R3생성, F(R3)생성,
R3송신
F''(R3)을 수신하고
F''(R3)가 F(R3)이면
나머지는 정확한 것으로 판정
R4수신, F(R4)생성,
F(R4)송신
메모리 카드 ID송신
S3501
S3503
S3505
S3507

도면11