(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G11B 20/12 (2006.01)

(45) 공고일자 2007년01월04일
(11) 등록번호 10-0665440
(24) 등록일자 2006년12월28일

(21) 출원번호 10-2001-7013674
(22) 출원일자 2001년10월25일
심사청구일자 2005년04월26일
번역문 제출일자 2001년10월25일
(86) 국제출원번호 PCT/JP2000/002750
국제출원일자 2000년04월27일

(65) 공개번호 10-2002-0006714
(43) 공개일자 2002년01월24일

(87) 국제공개번호 WO 2000/67257
국제공개일자 2000년11월09일

(81) 지정국 국내특허 : 중국, 대한민국,

(30) 우선권주장
JP-P-1999-00122104 1999년04월28일 일본(JP)
JP-P-1999-00128197 1999년05월10일 일본(JP)
JP-P-1999-00299635 1999년10월21일 일본(JP)

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

(72) 발명자
나가이다카히로
일본국오사카후오사카시미야코지마쿠히가시노다쵸4-4-23메종히가시노다쵸301

이시하라히데시
일본국오사카후가타노시이쿠노1-10-120

다카기유지
일본국오사카후히라카타시데구치2-29-1-309

유미바다카시
일본국교토후우지시고와타니시우라58베르비니시우라606

쇼지마모루
일본국오사카후사카이시모주우메마치3-13-4-805

오시마미츠아키
일본국교토후교토시니시쿄쿠가츠라미나미다츠미쵸115-3

오하라순지
일본국오사카후히가시오사카시신조221-5

이토모토시
일본국오사카후오사카시조토쿠후루이치3-17-25-302

이시다다카시
일본국교토후야와타시하시모토이소쿠13-14

나카무라아츠시
일본국오사카후가도마시미도쵸25-3쇼코료

자하나다다시
일본국가나가와켄요코하마시미도리쿠가모이836-6다이5미네하이츠
202

나카타고헤이
일본국효고켄가와니시시마루노우치쵸13-15에미넨스마루노우치비305

(74) 대리인 최재철
권동용
서장찬
김기종

심사관 : 김용웅

전체 청구항 수 : 총 10 항

(54) 광 디스크, 광 디스크 기록 및 재생장치, 광 디스크 상의 데이터의 기록 및 재생 방법

(57) 요약

데이터를 기록하고 재생하는 데이터 기록 및 재생 영역(102)과, 광 디스크를 식별하는 디스크 식별 정보(107)를 기록하는 판독 전용 디스크 식별 정보 영역(104)을 포함하는, 데이터를 기록할 수 있는 기록 방식의 광 디스크가 제공된다. 광 디스크에서, 디스크 식별 정보(107)는 광 디스크에 형성된 반사막을 스트립(strip) 형상으로 제거함으로써 형성된다. 디스크 식별 정보(107)는 각각의 광 디스크에 대한 고유의 디스크 식별자를 포함하고, 또한, 데이터 기록 및 재생 영역은, 광 디스크를 식별하는 디스크 식별 정보를 포함하는 정보를 키로서 사용하여 암호화되는 암호화 데이터를 기록하는 영역을 포함한다.

대표도

도 1

특허청구의 범위

청구항 1.
삭제

청구항 2.
삭제

청구항 3.
삭제

청구항 4.
삭제

청구항 5.
삭제

청구항 6.
삭제

청구항 7.
삭제

청구항 8.
삭제

청구항 9.
삭제

청구항 10.
삭제

청구항 11.
삭제

청구항 12.
삭제

청구항 13.
삭제

청구항 14.
삭제

청구항 15.
삭제

청구항 16.
삭제

청구항 17.
삭제

청구항 18.
삭제

청구항 19.
삭제

청구항 20.
삭제

청구항 21.
삭제

청구항 22.
삭제

청구항 23.
삭제

청구항 24.
삭제

청구항 25.
삭제

청구항 26.
삭제

청구항 27.
삭제

청구항 28.
삭제

청구항 29.
삭제

청구항 30.
삭제

청구항 31.
삭제

청구항 32.
삭제

청구항 33.
삭제

청구항 34.
삭제

청구항 35.
삭제

청구항 36.
삭제

청구항 37.
삭제

청구항 38.
삭제

청구항 39.
삭제

청구항 40.
삭제

청구항 41.
삭제

청구항 42.
삭제

청구항 43.
삭제

청구항 44.
삭제

청구항 45.
삭제

청구항 46.
삭제

청구항 47.
삭제

청구항 48.
삭제

청구항 49.
삭제

청구항 50.
삭제

청구항 51.
삭제

청구항 52.
삭제

청구항 53.
삭제

청구항 54.
삭제

청구항 55.
삭제

청구항 56.
삭제

청구항 57.
삭제

청구항 58.
삭제

청구항 59.
삭제

청구항 60.
삭제

청구항 61.
삭제

청구항 62.
삭제

청구항 63.
삭제

청구항 64.
삭제

청구항 65.
삭제

청구항 66.
삭제

청구항 67.
삭제

청구항 68.
삭제

청구항 69.
삭제

청구항 70.
삭제

청구항 71.
삭제

청구항 72.
삭제

청구항 73.
삭제

청구항 74.
삭제

청구항 75.
삭제

청구항 76.
삭제

청구항 77.
삭제

청구항 78.

광 디스크에 있어서,

원주 방향을 따라서 스트라이프(stripe) 형태로 형성되어 있고, 낮은 반사 광량(光量)의 신호가 간헐적으로 취득되는 영역을 포함하는 제1영역과,

광 빔의 조사(照射)에 의해 사용자가 사용자 데이터를 기록할 수 있는 제2영역을 포함하고 있으며,

상기 제1영역은 상기 제2영역에 대하여 반경 방향으로 소정의 간격을 갖도록 상기 제2영역으로부터 떨어져서 형성되고,

상기 제1영역에 판독 전용 데이터로서 기록된 데이터는 상기 제1영역과 제2영역과의 사이에 위치한 영역에도 기록되는 것을 특징으로 하는 광 디스크.

청구항 79.

제78항에 있어서,

상기 제2영역의 내측에 형성된 인입 영역을 더 포함하고 있으며,

상기 인입 영역은 상기 제1영역의 최소한 일부를 포함하고 있는 것을 특징으로 하는 광 디스크.

청구항 80.

제78항 또는 제79항에 있어서,

상기 제2영역은 재기록할 수 있는 영역인 것을 특징으로 하는 광 디스크.

청구항 81.

제78항 또는 제79항에 있어서,

상기 제2영역은 추기형(追記形; write-once) 영역인 것을 특징으로 하는 광 디스크.

청구항 82.

제1영역과 제2영역을 포함하고 있는 광 디스크에서, 상기 제1영역은 원주 방향을 따라서 스트라이프 형태로 형성되고, 또한 상기 제1영역은 낮은 반사 광량의 신호가 간헐적으로 취득되는 영역을 포함하고 있으며, 상기 광 디스크에 사용하기 위한 광 디스크 기록장치에 있어서,

상기 제1영역은 상기 제2영역에 대하여 반경 방향으로 소정의 간격을 갖도록 상기 제2영역으로부터 떨어져서 형성되고,

상기 제1영역에 판독 전용 데이터로서 기록된 데이터는 상기 제1영역과 제2영역과의 사이에 위치한 영역에도 기록되고,

상기 광 디스크 기록장치는 상기 제2영역에 광 빔을 조사함으로써 사용자 데이터를 기록하는 기록 수단을 포함하는 것을 특징으로 하는 광 디스크 기록장치.

청구항 83.

제1영역과 제2영역을 포함하고 있는 광 디스크에서, 상기 제1영역은 원주 방향을 따라서 스트라이프 형태로 형성되고, 또한 상기 제1영역은 낮은 반사 광량의 신호가 간헐적으로 취득되는 영역을 포함하고 있으며, 상기 광 디스크에 사용하기 위한 광 디스크 기록 방법에 있어서,

상기 제1영역은 상기 제2영역에 대하여 반경 방향으로 소정의 간격을 갖도록 상기 제2영역으로부터 떨어져서 형성되고,

상기 제1영역에 판독 전용 데이터로서 기록된 데이터는 상기 제1영역과 제2영역과의 사이에 위치한 영역에도 기록되며,

상기 광 디스크 기록 방법은 상기 제2영역에 광 빔을 조사함으로써 사용자 데이터를 기록하는 단계를 포함하는 것을 특징으로 하는 광 디스크 기록 방법.

청구항 84.

제1영역과 제2영역을 포함하고 있는 광 디스크에서, 상기 제1영역은 원주 방향을 따라서 스트라이프 형태로 형성되고, 또한 상기 제1영역은 낮은 반사 광량의 신호가 간헐적으로 취득되는 영역을 포함하고 있으며, 상기 광 디스크에 사용하기 위한 광 디스크 재생장치에 있어서,

상기 제1영역은 상기 제2영역에 대하여 반경 방향으로 소정의 간격을 갖도록 상기 제2영역으로부터 떨어져서 형성되고,

상기 제1영역에 판독 전용 데이터로서 기록된 데이터는 상기 제1영역과 제2영역과의 사이에 위치한 영역에도 기록되며,

상기 광 디스크 재생장치는

상기 제1영역을 재생하는 제1재생 수단,

상기 제1영역과 제2영역과의 사이에 판독 전용 데이터로서 기록된 데이터를 재생하는 제2재생 수단, 및

상기 제2영역에 기록된 사용자 데이터를 재생하는 제3재생 수단을 포함하는 것을 특징으로 하는 광 디스크 재생장치.

청구항 85.

제1영역과 제2영역을 포함하고 있는 광 디스크에서, 상기 제1영역은 원주 방향을 따라서 스트라이프 형태로 형성되고, 또한 상기 제1영역은 낮은 반사 광량의 신호가 간헐적으로 취득되는 영역을 포함하고 있으며, 상기 광 디스크에 사용하기 위한 광 디스크 재생 방법에 있어서,

상기 제1영역은 상기 제2영역에 대하여 반경 방향으로 소정의 간격을 갖도록 상기 제2영역으로부터 떨어져서 형성되고,

상기 제1영역에 판독 전용 데이터로서 기록된 데이터는 상기 제1영역과 제2영역과의 사이에 위치한 영역에도 기록되며,

상기 광 디스크 재생 방법은,

상기 제1영역을 재생하는 단계,

상기 제1영역과 제2영역과의 사이에 판독 전용 데이터로서 기록된 데이터를 재생하는 단계, 및

상기 제2영역에 기록된 사용자 데이터를 재생하는 단계를 포함하는 것을 특징으로 하는 광 디스크 재생 방법.

청구항 86.

제78항 또는 제79항에 기재된 광 디스크에 정보를 기록하는 광 디스크 기록장치.

청구항 87.

제78항 또는 제79항에 기재된 광 디스크로부터 정보를 재생하는 광 디스크 재생장치.

명세서

기술분야

본 발명은 광 디스크, 광 디스크 기록 및 재생장치, 광 디스크 상의 데이터의 기록, 재생 및 삭제 방법과, 정보처리 시스템에 관한 것이다. 특히, 본 발명은 저작권으로써 보호된 영화의 영상 데이터 및 음악의 오디오 데이터를 포함하는 AV 데이터(오디오 및 비디오 데이터) 등의 데이터가 기록되어 있는 광 디스크로부터, 또 다른 기록 방식 등의 광 디스크 등 기타 기록 매체에, 불법적인 복사가 실행되는 것을 방지할 수 있는 광 디스크, 광 디스크 기록 및 재생장치, 광 디스크 상의 데이터의 기록, 재생 및 삭제 방법과, 정보처리 시스템에 관한 것이다.

배경기술

광 디스크는 랜덤 액세스(random access) 성능에 있어서 종래의 테이프 매체 보다 우수하고, 또한 레이저 광을 이용하여 비접촉 기록 및 재생을 할 수 있기 때문에 반복 사용으로 인한 열화(劣化)가 감소되는 이점을 갖는다. 또한, 광 디스크는, 디스크 제조자가 실행하는 마스터링(mastering)에 의해서 낮은 비용으로 대량 복제가 가능한 이점이 있고, 또한 고품질 디지털 오디오로서 CD(콤팩트 디스크)가 아날로그 기록하는 종래의 축음기 레코드 대신에 일반화되고 있다. 더욱이, 최근에는, 고품질 영상 데이터가 디지털 기록된 DVD(digital video disk 또는 digital versatile disk)가 상품화되어 있고, 광 디스크는 가까운 장래에 AV 데이터용 디지털 기록매체로서 더욱 발전될 것으로 예상된다.

한편, 음악 CD, CD-ROM, DVD-ROM 등, 디스크 제조자에 의해서 미리 홈이 파인(pre-pit) 형태로 데이터가 이미 기록된 판독 전용 광 디스크에 추가하여, CD-R, CD-RW, MO(magneto-optical;광자기), MD, DVD-RAM 등, 사용자가 가정에서 AV 데이터를 기록할 수 있는 기록 방식의 광 디스크가 최근에 개발되어서 널리 보급되었다.

또한, 텔레비전 방송에서, 종래의 아날로그 시스템 대신에 멀티 채널 또는 각종 서비스를 가능하게 하는 디지털 시스템이 도입되었고, 이러한 경향은 가까운 장래에 널리 보급될 것이다. 특히, 기록 방식의 광 디스크는, 디지털화된 방송 또는 통신을 통하여 전송되는 컨텐츠의 기록매체로서, 컨텐츠가 전송됨에 따라서 축적된 후에, 프로그램 선택을 실행하여, 선택된 컨텐츠를 청취하거나 또는 시청하는 시간 경과 이용을 주 목적으로 하는 AV 데이터의 기록에 이용될 것으로 예상된다.

종래부터, 컴퓨터에 주로 사용되었던 기록 방식의 광 디스크는 사용자 자신이 작성한 데이터를 저장하는 데에 사용되고, 또한 기록 방식의 광 디스크는 기록 방식의 광 디스크 간에 실행되는 복사를 방지하는 아무런 수단도 구비하고 있지 않다. 기록 방식의 광 디스크가 널리 이용되면, 보통의 사용자는 광 디스크의 기록 데이터를 기록 방식의 또 다른 광 디스크에 비합법적으로 그대로 복사하여, 이 AV 데이터의 저자 또는 작가에게 지불해야 하는 저작권 사용료를 지불하지 않고, 또한 기록 방식의 광 디스크가 디지털 방식으로 기록 가능하기 때문에 음질 및 화질의 열화없이 불법적인 복제품(複製品)을 취득할 수 있게 되어서, 이것이 우수한 컨텐츠의 보급을 방해하는 요인이 된다. 음악 등이 디지털 방식으로 기록되는 MD에 대하여, 기록 횟수를 제한하기 위하여 세대(世代; generation) 관리를 실행하는 수단이 도입되어서, 데이터와 함께 세대 관리 데이터가 광 디스크에 기록되고 세대 관리 데이터에 의해서 복사 횟수가 제한된다.

또한, CD-ROM 또는 DVD-ROM의 불법적인 복사를 방지하기 위하여, 예로서, 광 디스크의 요부(凹部; pit)에 바코드를 중첩해서 기록하기 위한 추가 기록 영역(write once area)인 버스트 커팅 영역(BCA; burst cutting area, 이하 BCA라고 함)을 형성하고, 광 디스크의 제조시에 BCA에 각각의 광 디스크에 대하여 서로 상이한 ID를 기록하는 방법이 국제 특허 공고 번호 WO97/14144호인 국제 특허 출원에 제안되었다. 이 방법에 의하면, 패스워드가 각각의 디스크 ID에 대하여 상이하므로, 하나의 패스워드는 하나의 디스크의 암호만을 해독할 수 있어서, 컨텐츠가 불법적으로 복사되더라도, 디스크 ID의 정보가 없으므로 컨텐츠는 해독될 수 없다.

도 39는 종래의 DVD-ROM의 사용자 데이터 영역의 구성, 및 사용자 데이터 영역의 데이터로부터 암호화된 컨텐츠를 해독하는 광 디스크 재생장치의 구성을 나타내는 블록도이다. DVD-ROM에서, 도 39에 나타낸 바와 같이, 디스크에 기록된 컨텐츠 데이터에 대하여 암호화가 실행된다.

도 39를 참조하면, DVD-ROM의 사용자 데이터 영역은 섹터 헤더 영역(3201), 주 데이터 영역(3202), 및 오류 검출 코드(3203)로써 구성된다. 이 경우에, 섹터 헤더 영역(3201)에는, 섹터의 위치를 나타내는 섹터 어드레스(3204), 주 데이터 영역(3202)에 기록된 데이터에 대한 저작권 제어 정보(예로서, 스크램블 플래그(flag), 복사 제어 정보 등)가 기록되는 저작권 제어 정보(3205), 및 주 데이터 영역(3202)에 기록된 데이터에 대하여 암호화가 실행되어 있는 경우에 암호를 해독하기 위한 암호 해독 키(key)(3206)가 기록된다. 또한, 주 데이터 영역(3202)에는, 저작권 보호를 필요로 하는 주로 AV 데이터 등이 암호화되어서 기록된다.

이러한 사용자 데이터 영역을 재생할 때에, 섹터 헤더 영역(3201)으로부터 암호화된 컨텐츠를 재생하는 데에 필요한 암호 해독 키(3206)를 우선 취득한다. 취득된 암호 해독 키(3206)는 키 암호 해독 장치(3207)에 입력되고, 키 암호 해독 장치는 소정의 디스크 키를 사용하여 입력된 암호 해독 키(3206)를 컨텐츠 암호 해독 키로 해독하여, 컨텐츠 암호 해독 키를 암호 해독 장치(3208)에 출력한다. 후속해서, 암호 해독 장치(3208)는, 주 데이터 영역(3202)에 대응하는, 섹터 헤더 영역(3201)에 저장된 저작권 제어 정보(3205)에 따라서, 해독된 컨텐츠 암호 해독 키를 사용하여 주 데이터 영역(3202)의 암호화된 컨텐츠를 해독하면, 재생 가능한 데이터인, 암호 해독된 컨텐츠를 취득할 수 있다.

도 39에 나타낸 구성에 의한 광 디스크에서, 개인용 컴퓨터 등의 구동장치로써 주 데이터 영역(3202)으로부터 판독을 실행할 수 있다. 그러나, 암호 해독 키(3206)가 기록된 영역을 정상적인 인증 기능을 구비한 광 디스크 재생장치로써만 판독할 수 있도록 광 디스크를 구성함으로써 불법적인 복제 또는 해적판의 제조를 방지할 수 있다.

그러나, 세대 관리 데이터를 이용하는, 불법적인 복사 방지 방법의 경우에, 복사에 따라서 세대 관리 데이터를 변경하지 않을 수 없다("1회 복사 가능"으로부터 "복사 불가능"으로의 변경). 또 한편으로는 광 디스크 상의 데이터를 세대 관리 데이터를 변경하지 않고 세대 관리 데이터와 함께 복사함으로써, 또는 컴퓨터 등으로써 세대 관리 데이터를 변경하여 광 디스크에 기록함으로써 불법적인 복사가 충분히 방지될 수 없는 문제가 있다. 또한, 컨텐츠와 함께 사전에 기록된 세대 관리 데이터에 따라서 복사 횟수가 제한되므로, 정상적인 저작권 사용료를 지불해도, "복사 불가능"으로 되어 있는 데이터는 또 다른 광 디스크로의 복사가 전혀 허용되지 않고, 사용자는 컨텐츠 제공자로부터의 컨텐츠 데이터의 공급을 대기해야 문제가 있다. 이 두 가지 문제는 컨텐츠 제공자가 사용자에 의해서 실행되는 기록 방식의 광 디스크에의 컨텐츠 복사를 충분히 관리할 수 없기 때문에 발생한다.

최근에, 개인용 컴퓨터는 성능이 더욱 향상되고 또한 네트워크에 접속되어서, 복수의 개인용 컴퓨터에 의해서 암호 해독이 고속으로 실행될 수 있다. 이러한 암호 해독에 대하여 암호의 강도(robustness)를 더욱 증대하기 위해서는, 암호에 사용되는 키의 길이의 확장이 필요하게 된다. 그러나, 종래에 제안된 바와 같이 섹터 헤더에 암호 해독 키를 기록하는 키 관리 방법에서는, 소정 길이의 크기(암호 해독 키 영역의 크기) 이하를 갖는 암호 해독 키 만이 기록되고, 또한 향후 암호의 강도를 증대할 목적으로 키 길이를 연장할 수 없는 문제가 있다.

본 발명의 첫째 목적은 컨텐츠 제공자가 관리할 수 없는 불법적인 디지털 복사를 방지할 수 있는, 광 디스크, 광 디스크 기록장치, 광 디스크 재생장치, 광 디스크 기록 및 재생장치, 광 디스크 상에의 데이터의 기록 및 재생 방법, 광 디스크에 데이터를 기록하는 방법, 광 디스크 상의 데이터의 재생 방법, 광 디스크 상의 데이터의 삭제 방법과, 정보처리 시스템을 제공하는 것이다.

또한, 본 발명의 둘째 목적은 저작권 보호를 필요로 하는 데이터를 암호 해독하는 데에 필요한 암호 해독 키의 신뢰성을 강화할 수 있는, 광 디스크, 광 디스크 기록장치, 광 디스크 재생장치, 광 디스크 기록 및 재생장치, 광 디스크 상에의 데이터의 기록 및 재생 방법, 광 디스크에 데이터를 기록하는 방법, 광 디스크 상의 데이터의 재생 방법, 광 디스크 상의 데이터의 삭제 방법과, 정보처리 시스템을 제공하는 것이다.

또한, 본 발명의 셋째 목적은 기록되는 컨텐츠의 저작권 보호 레벨에 따라서 암호의 강도 레벨을 설정할 수 있는, 광 디스크, 광 디스크 기록장치, 광 디스크 재생장치, 광 디스크 기록 및 재생장치, 광 디스크 상에의 데이터의 기록 및 재생 방법, 광 디스크에 데이터를 기록하는 방법, 광 디스크 상의 데이터의 재생 방법, 광 디스크 상의 데이터의 삭제 방법과, 정보처리 시스템을 제공하는 것이다.

발명의 상세한 설명

상기의 목적을 달성하기 위하여, 본 발명의 제1특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크는,

데이터를 기록하고 재생하는 데이터 기록 및 재생 영역과,

광 디스크를 식별하는 디스크 식별 정보를 기록하는 판독 전용 디스크 식별 정보 영역을 포함한다.

상기의 광 디스크에서, 디스크 식별 정보는 광 디스크에 형성된 반사막을 스트립(strip) 형상으로 제거함으로써 형성되는 것이 바람직하다.

또한, 상기의 광 디스크에서, 디스크 식별 정보는 각각의 광 디스크에 대한 고유의 디스크 식별자를 포함하는 것이 바람직하다.

또한, 상기의 광 디스크에서, 데이터 기록 및 재생 영역은, 광 디스크를 식별하는 디스크 식별 정보를 포함하는 정보를 키로서 사용하여 암호화되는 암호화 데이터를 기록하는 영역을 포함하는 것이 바람직하다.

또한, 상기의 광 디스크에서, 암호화된 데이터는 영상 데이터 및 음악 데이터 중 최소한 하나인 컨텐츠 데이터를 포함하는 것이 바람직하다.

또한, 상기의 광 디스크에서, 암호화된 데이터는 컨텐츠 데이터에 대하여 실행된 암호를 해독하는 디스크램블(descramble) 키를 포함하는 것이 바람직하다.

또한, 상기의 광 디스크에서, 암호화된 데이터는,

(a) 컨텐츠 데이터에 대하여 실행된 암호를 해독하는 디스크램블 키, 및

(b) 디스크램블 키의 오류를 검출하는 오류 검출 코드를 포함하는 것이 바람직하다.

본 발명의 또 다른 특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크로서,

광 디스크는, 데이터를 기록하고 재생하는 데이터 기록 및 재생 영역을 포함하고, 또한

데이터 기록 및 재생 영역은, 암호화된 영상 데이터 및 암호화된 음악 데이터 중 최소한 하나인 컨텐츠 데이터, 및 컨텐츠 데이터에 대하여 실행된 암호를 해독하는 디스크램블 키를 기록하는 영역을 포함하는 것을 특징으로 하는 광 디스크가 제공된다.

본 발명의 추가적인 특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크로서,

광 디스크를 식별하는 디스크 식별 정보를 기록하는 판독 전용 디스크 식별 정보 영역,

암호화된 영상 데이터 및 암호화된 음악 데이터 중 최소한 하나를 포함하는 컨텐츠 데이터를 기록하고 재생하는 데이터 기록 및 재생 영역, 및

컨텐츠 데이터를 재생할 때 사용되는 키 정보와, 디스크 식별 정보를 키로서 사용하여 암호화되는 디스크램블 키를 기록하는 키 관리 정보 영역을 포함하는 광 디스크가 제공된다.

본 발명의 또 다른 특징에 의하면,

(a) 데이터를 기록할 수 있는 기록 방식의 광 디스크의 데이터 기록 및 재생 영역에 데이터를 기록하는 기록 동작, 및

(b) 데이터 기록 및 재생 영역으로부터 데이터를 재생하는 재생 동작 중 최소한 하나를 제어하는 광 디스크 기록 및 재생장치로서,

광 디스크는, 광 디스크를 식별하는 디스크 식별 정보를 기록하는 디스크 식별 정보 영역을 포함하고, 또한

광 디스크 기록 및 재생장치는,

디스크 식별 정보 영역으로부터 디스크 식별 정보를 재생하는 재생 수단, 및

재생된 디스크 식별 정보에 따라서, 기록 동작과 재생 동작 중 최소한 하나를 실행할 것인가 아닌가를 판단하고, 또한 판단 결과에 따라서 기록 동작과 재생 동작 중 최소한 하나를 실행하도록 광 디스크 기록 및 재생장치를 제어하는 제어 수단을 포함하는 것을 특징으로 하는 광 디스크 기록 및 재생장치가 제공된다.

본 발명의 추가적인 특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크에 컨텐츠 데이터를 기록하는 광 디스크 기록장치로서,

광 디스크는, 광 디스크를 식별하는 디스크 식별 정보 영역을 기록하는 영역을 포함하고, 또한

광 디스크 기록장치는,

디스크 식별 정보 영역으로부터 디스크 식별 정보를 재생하는 재생 수단, 및

재생된 디스크 식별 정보를 키로서 사용하여, 최소한 부분적으로 암호화된 데이터를 광 디스크에 기록하는 기록 수단을 포함하는 것을 특징으로 하는 광 디스크 기록장치가 제공된다.

본 발명의 또 하나의 추가적인 특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크로부터 컨텐츠 데이터를 재생하는 광 디스크 재생장치로서,

광 디스크는, 광 디스크를 식별하는 디스크 식별 정보를 기록하는 디스크 식별 정보 영역을 포함하고, 또한

광 디스크 재생장치는,

디스크 식별 정보 영역으로부터 디스크 식별 정보를 재생하는 재생 수단, 및

광 디스크로부터 최소한 부분적으로 암호화된 데이터를 재생한 후에 재생된 디스크 식별 정보를 키로서 사용하여, 최소한 부분적으로 암호화된 데이터를 해독하는 암호 해독 수단을 포함하는 것을 특징으로 하는 광 디스크 재생장치가 제공된다.

본 발명의 또 다른 특징에 의하면,

(a) 데이터를 기록할 수 있는 기록 방식의 광 디스크의 데이터 기록 및 재생 영역에 데이터를 기록하는 기록 동작, 및

(b) 데이터 기록 및 재생 영역으로부터 데이터를 재생하는 재생 동작 중 최소한 하나를 제어하는 광 디스크 기록 및 재생 방법으로서,

광 디스크는, 광 디스크를 식별하는 디스크 식별 정보를 기록하는 디스크 식별 정보 영역을 포함하고, 또한

상기 방법은,

디스크 식별 정보 영역으로부터 디스크 식별 정보를 재생하는 단계, 및

재생된 디스크 식별 정보에 따라서 기록 동작과 재생 동작 중 최소한 하나를 실행할 것인가 아닌가를 판단하고, 또한 판단 결과에 따라서 기록 동작과 재생 동작 중 최소한 하나를 실행하도록 기록 동작 및 재생 동작을 제어하는 단계를 포함하는 것을 특징으로 하는 광 디스크 기록 및 재생 방법이 제공된다.

본 발명의 추가적인 특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크에 컨텐츠 데이터를 기록하는 광 디스크 기록 방법으로서,

광 디스크는, 광 디스크를 식별하는 디스크 식별 정보를 기록하는 디스크 식별 정보 영역을 포함하고, 또한

상기 방법은,

디스크 식별 정보 영역으로부터 디스크 식별 정보를 재생하는 단계, 및

재생된 디스크 식별 정보를 키로서 사용하여, 최소한 부분적으로 암호화된 데이터를 광 디스크에 기록하는 단계를 포함하는 것을 특징으로 하는 광 디스크 기록 방법이 제공된다.

본 발명의 또 하나의 추가적인 특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크로부터 컨텐츠 데이터를 재생하는 광 디스크 재생 방법으로서,

광 디스크는, 광 디스크를 식별하는 디스크 식별 정보를 기록하는 디스크 식별 정보 영역을 포함하고, 또한

상기 방법은,

디스크 식별 정보 영역으로부터 디스크 식별 정보를 재생하는 단계, 및

최소한 부분적으로 암호화된 데이터를 재생한 후에, 재생된 디스크 식별 정보를 키로서 사용하여, 최소한 부분적으로 암호화된 데이터를 해독하는 단계를 포함하는 것을 특징으로 하는 광 디스크 재생 방법이 제공된다.

본 발명의 또 다른 특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크로서,

제1디스크 정보를 기록하는 제1정보 영역과,

각각의 광 디스크를 식별하는 제2디스크 정보를 기록하는 제2정보 영역과,

사용자 데이터 영역에 광 빔을 조사(照射) 함으로써 정보 데이터를 기록하는 사용자 데이터 영역을 포함하는 광 디스크가 제공된다.

본 발명의 추가적인 특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크로서,

광 디스크는 복수의 섹터를 포함하는 섹터 구조를 구비하고,

각각의 섹터는 섹터 헤더 영역과, 암호화된 데이터를 기록하는 주 데이터 영역을 포함하고,

섹터 헤더 영역은 암호화된 데이터를 해독하는 데에 필요한 최소한 하나의 암호 해독 키를 기록하는 암호 해독 키 정보 영역을 포함하고, 또한

암호 해독 키 정보 영역의 크기는 각각의 암호 해독 키의 크기보다 작은 것을 특징으로 하는 광 디스크가 제공된다.

본 발명의 또 다른 추가적인 특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크로서,

광 디스크는 데이터를 기록하는 주 데이터 영역을 포함하고,

주 데이터 영역은 암호화하지 않은 상태로 데이터를 기록하는 비암호화 영역, 및 암호화한 상태로 데이터를 기록하는 암호화 영역을 포함하고,

비암호화 영역은 데이터를 해독하기 위한 암호 해독 키의 변환에 사용되는 암호 해독 키 변환 데이터를 포함하고, 또한

암호화 영역의 데이터는 암호 해독 키 변환 데이터를 사용하여 변환되는 암호 해독 키를 사용하여 암호화되는 것을 특징으로 하는 광 디스크가 제공된다.

본 발명의 또 다른 특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크에 데이터를 기록하는 광 디스크 기록 방법으로서,

광 디스크에 기록되어 있는 암호 해독 키 상태를 판독하고, 판독한 암호 해독 키 상태에 따라서 암호 해독 키용의 공백 영역이 있는가 없는가를 판단하는 단계와,

암호 해독 키용의 공백 영역이 있는 것으로 판단하면, 암호 해독 키 영역을 예약하고 암호 해독 키 영역에 암호 해독 키를 기록하는 단계와,

저작권 제어 정보 및 암호 해독 키 인덱스(index)를 파일(file) 단위 및 익스텐트(extent) 단위 중 최소한 하나의 단위로 배치하는 단계와,

암호 해독 키를 사용하여 데이터를 암호화하고, 암호화된 데이터를 파일 단위 및 익스텐트 단위 중 최소한 하나의 단위로 광 디스크에 기록하는 단계와,

광 디스크에 기록되는 데이터를 관리하는 광 디스크 파일 관리 정보를 광 디스크에 기록하는 단계를 포함하는 광 디스크 기록 방법이 제공된다.

본 발명의 추가적인 특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크로부터 데이터를 재생하는 광 디스크 재생 방법으로서,

재생될 데이터가 파일 단위 또는 익스텐트 단위로 기록되어 있는 데이터 기록 영역으로부터 암호 해독 키 인덱스를 재생하여 취득하는 단계,

취득한 암호 해독 키 인덱스에 대응하는 암호 해독 키를 재생하여 취득하는 단계, 및

암호화된, 파일 단위 또는 익스텐트 단위의 데이터를 암호 해독 키를 사용하여 재생하는 단계를 포함하는 광 디스크 재생 방법이 제공된다.

본 발명의 또 다른 추가적인 특징에 의하면, 데이터를 기록할 수 있는 기록 방식의 광 디스크로부터 데이터를 삭제하는 광 디스크 삭제 방법으로서,

삭제될 데이터가 파일 단위 또는 익스텐트 단위로 기록되어 있는 기록 영역으로부터 암호 해독 키 인덱스를 재생하여 취득하는 단계,

취득한 암호 해독 키 인덱스에 대응하고 또한 암호 해독 키의 기록 상태를 나타내는 암호 해독 키 상태를 갱신하고, 암호 해독 키를 해제하는 단계, 및

삭제될 데이터에 대응하는 파일 엔트리를 파일 관리 정보로부터 삭제함으로써, 광 디스크에 기록되는 데이터를 관리하는 파일 관리 정보를 갱신하는 단계를 포함하는 광 디스크 삭제 방법이 제공된다.

본 발명의 또 다른 특징에 의하면,

암호 키를 사용하여 데이터를 암호화하는 데이터 암호화 장치와,

데이터의 해독에 필요한 암호 해독 키를 기록 방식의 광 디스크에 기록하고, 또한 기록된 암호 해독 키를 재생하는 광 디스크 기록 및 재생장치와,

광 디스크 기록 및 재생장치와 데이터 암호화 장치에 접속된 제어 장치를 포함하는 정보 처리 시스템으로서,

광 디스크 기록 및 재생장치는,

암호 해독 키 테이블을 광 디스크에 기록하고, 또한 광 디스크로부터 암호 해독 키 테이블을 재생하는 제1기록 및 재생 수단,

암호 해독 키를 암호화하고, 암호화된 암호 해독 키를 송신하고, 암호화된 암호 해독 키를 제어 장치로부터 수신하고, 또한 암호화된 암호 해독 키를 해독하는 암호화 및 암호 해독 수단, 및

암호 해독 키의 기록 상태를 나타내는 암호 해독 키 상태 테이블을 광 디스크에 기록하고, 또한 광 디스크로부터 암호 해독 키 상태 테이블을 재생하는 제2기록 및 재생 수단을 포함하고,

데이터 암호화 장치는,

암호 해독 키를 암호화하고, 암호화된 암호 해독 키를 제어 장치에 송신하는 암호화 수단을 포함하고, 또한

제어 장치는,

데이터 암호화 장치의 암호화 수단으로부터 암호화된 암호 해독 키를 수신하는 수신 수단, 및

재생된 암호 해독 키 상태 테이블을 근거로 하여 암호 해독 키용의 공백 영역을 탐색하고, 수신한 암호화된 암호 해독 키를 탐색된 공백 영역에 할당하고, 또한 할당되어 암호화된 암호 해독 키를 광 디스크 기록 및 재생장치에 송신하는 할당 수단을 포함하고, 그리고,

광 디스크 기록 및 재생장치의 암호화 및 암호 해독 수단은 제어 장치의 할당 수단으로부터, 할당되어 암호화된 암호 해독 키를 수신하고, 수신한 암호화된 암호 해독 키를 해독하는 것을 특징으로 하는 정보 처리 시스템이 제공된다.

본 발명의 추가적인 특징에 의하면, 기록된 데이터를 재생하는 판독 전용 방식의 광 디스크로서,

데이터를 기록하는 데이터 재생 영역, 및

광 디스크를 식별하는 디스크 식별 정보를 기록하는 판독 전용 디스크 식별 정보 영역을 포함하는 광 디스크로서,

데이터 재생 영역은, 광 디스크를 식별하는 디스크 식별 정보를 포함하는 정보를 키로서 사용하여 암호화되는 데이터가 기록되는 영역을 포함하는 것을 특징으로 하는 판독 전용 방식의 광 디스크가 제공된다.

실시예

본 발명의 바람직한 실시예를 첨부 도면을 참조로 하여 이하에 설명한다.

(바람직한 제1실시예)

도 1은 본 발명에 의한 바람직한 제1실시예의 기록 방식 광 디스크(100)의 데이터 기록 영역을 설명하는 평면도를 나타낸다. 이 기록 방식 광 디스크(100)는 디지털 데이터를 기록할 수 있는 기록 매체이고, 추기형(追記形; write-once type)의 재기록 불능 광 디스크 및 재기록 가능 광 디스크를 포함한다.

도 1을 참조하면, 101은 광 디스크(100)에 대한 관리 정보를 기록하는 인입 영역을 나타내고, 102는 (a) 영화 등 영상 데이터(정지화상 및 애니메이션 화상을 포함하는)와 음악 등 음성 데이터 중 최소한 하나를 포함하는 AV 데이터 컨텐츠, 및 (b) 컴퓨터 소프트웨어 등, 저작권 보호를 필요로 하는 디지털 데이터를 기록하는 사용자 데이터 영역을 나타낸다. 103은 결함 관리 정보 등을 기록하는 인출 영역(lead-out area)을 나타낸다. 인입 영역(101)은 미리 홈이 파인 형태로 데이터가 기록되어 있는 판독 전용 영역(104), 및 재기록 가능 영역인, 가이드 홈을 구비한 기록 및 재생 영역(105)으로써 구성된다. 이 경우에, 판독 전용 영역(104)에는, 광 디스크(100)의 물리적 특성을 나타내는 제어 영역 등이 제조자에 의해서 미리 홈이 파인 형태로 기록된다. 인출 영역(103)과 재기록 가능 영역(105)에는, 광 디스크 기록장치에 의해서 실행되는 기록 테스트용 데이터, 광 디스크(100) 상의 결함을 관리하는 관리 정보가 광 디스크 기록장치에 의해서 기록된다. 또한, 컨텐츠가 기록된 광 디스크(103)가 완성된 후에, 인입 영역(101) 내의 판독 전용 영역(104)의 내주(內周) 측에는, 디스크 개별 정보로서 형성되는 BCA(106)가 이하의 공지된 방법으로써 광 디스크(100) 상에 일단 기록된다.

도 2A는 도 1에 나타낸 광 디스크(100)의 BCA(106)를 형성할 때의 장치 구성을 나타내는 블록도 및 단면도를 나타내고, 도 2B는 도 1에 나타낸 광 디스크(100)의 BCA(106)의 형성후의 광 디스크(100)의 단면도, 및 반사광의 강도를 수평 방향으로 나타내는 그래프를 나타낸다.

도 2A 및 2B를 참조하면, 양면 기록 방식의 광 디스크(100)의 예가 나와 있고, 광 디스크(100)는, 기록층(202), 반사층(203), 접착층(204), 반사층(205) 및 기록층(206)이 2개의 기판(201 및 207) 사이에 삽입되도록 구성된다.

도 2A에 나타낸 바와 같이, BCA가 광 디스크(100)에 기록될 때, 고출력 레이저 광원(211)으로부터 펄스 형태의 레이저 빔을 집속 렌즈(212)를 통하여, 예로서, 광 디스크(100)의 반사층(205)에 조사함으로써 반사층(205)의 일부를 제거하여 위상 부호화 변조후의 스트라이프(stripe) 형태의 데이터가 홈에 중첩되어 기록된다. 신호를 재생할 때에는, 도 2B에 나타낸 바와 같이, 반사층(205)이 제거된 부분으로부터의 적은 양의 반사광으로부터 발생하는 신호가 간헐적으로 재생된다. BCA 데이터는 재생 신호가 2진화된 후에 위상 부호화 복조를 통하여 재생된다. 이러한 기록 시스템으로써 형성되는 BCA는 각각의 광 디스크(100)에 대한 고유 정보인 디스크 식별자를 기록할 수 있고, 또한, BCA는 기록된 데이터를 왜곡할 수 없는 특징을 갖는다.

삭제

도 3은 도 1에 나타낸 BCA(106)의 기록 포맷을 나타내는 도면이다. 도 3에 나타낸 바와 같이, BCA(106)에는, 동기 코드(301), 오류 검출 코드(302), 오류 정정 코드(303) 등이 기록되어서 BCA 데이터(304)의 판독율을 향상시킨다. 복수의 BCA 데이터(304)를 연결함으로써, 디스크 식별 정보(305)가 구성된다. 디스크 식별 정보(305)에는, 사용자 데이터 영역에 기록할 수 있는 데이터의 타입과 사용자 데이터 영역으로부터 재생할 수 있는 데이터의 타입이 기록된다. BCA(106)의 데이터를 왜곡시키는 것은 불가능하므로, 광 디스크(100)를 제조할 때 기록되는 디스크 식별 정보로써, 사용자의 디스크 사용을 어느 정도까지 제한할 수 있다.

도 4는 도 1에 나타낸 사용자 데이터 영역(102) 내의 섹터 데이터(401)의 섹터 구조를 나타낸다. 도 4를 참조하면, 도 1에 나타낸 사용자 데이터 영역(102)은 소정량의 단위로써 액세스할 수 있는 섹터 구조를 가지며, 섹터 데이터(401)는 헤더(402), 주 데이터(403) 및 오류 검출 코드(404)로써 구성된다.

주 데이터(403)는 AV 데이터, 컴퓨터 데이터 등이 기록되는 영역이다. 헤더(402)에는, 데이터 ID(data identifier; 데이터 식별자)(405), ID 오류 검출 코드(406), 스크램블 제어 정보(407), 키 정보(408) 등이 기록된다. 데이터 ID(405)에는, 섹터를 식별하는 논리 어드레스 등이 기록되고, ID 오류 검출 코드(406)는 데이터 ID의 오류를 검출하기 위한 것이다. 스크램블 제어 정보(407)는 주 데이터가 스크램블되었는가 아닌가를 나타내는 플래그이고, 키 정보(408)에는, 주 데이터를 디스램블링하는 키에 관한 정보가 기록된다. 키에 관한 정보로서, 디스크램블 키 자체(바람직한 제1실시예의 바람직한 변형 실시예에서의) 또는 광 디스크(100)의 또 다른 영역에 기록된 디스크램블 키에 대한 포인터(pointer)인 키 인덱스(바람직한 제1실시예에서의)가 기록된다. 도 4의 예는 광 디스크(100)의 또 다른 영역인, 도 1에 나타낸 키 관리 정보 영역(107)에 기록된 디스크램블 키를 참조하기 위한 키 인덱스가 기록되어 있는 경우를 나타낸다.

도 5는 도 1에 나타낸 키 관리 정보 영역(107)의 구성을 나타낸다. 도 5를 참조하면, 키 관리 정보 영역(107)은 키 정보 영역(501), 컨텐츠 정보 영역(502) 및 키 인덱스 목록 영역(503)으로써 구성된다.

키 정보 영역(501)에는, 기록된 키 영역(504)의 수가 기록되고, 키 정보 영역(501)은, (a) 스크램블된 AV 데이터 등을 디스크램블하는 디스크램블 키를 기록하는 영역인 디스크램블 키 영역(505), 및 (b) 디스크램블 키 영역(505)에 기록된 디스크램블 키의 기록 상태(사용되지 않음, 영역 예약, 기록됨 등을 나타내는)를 기록하는 키 상태 영역(506)을 포함한다. 디스크램블 키 영역(505)에는, 복수의 디스크램블 키가 기록되고, 디스크램블 키 영역(505)에서의 저장된 위치를 나타내는 키 인덱스는 키 인덱스 목록 영역(503)에 기록된다. 상기 복수의 디스크램블 키는 이 키 인덱스로써 조회(照會)할 수 있다. 키 상태 영역(506)에는, 디스크램블 키의 기록 상태를 나타내는 상태 정보가 키 인덱스로써 조회할 수 있는 위치에 저장된다.

컨텐츠 정보 영역(502)에는, 광 디스크(100)에 기록된 컨텐츠 중에서 저작권 보호가 필요한 것이 등록되고, 상기 컨텐츠에 사용되는 키에 관한 정보가 등록된다. 컨텐츠 정보 영역(502)에는, 키 인덱스 목록 영역(503)에 등록된 컨텐츠의 수(507), 및 컨텐츠의 수에 대한 컨텐츠 정보(508)가 기록된다. 또한, 컨텐츠 정보(508)에는, 컨텐츠를 식별하는 컨텐츠 ID, 컨텐츠에 사용되는 디스크램블 키의 수, 및 사용된 키를 기록하는 키 인덱스 목록(509)에 대한 포인터가 기록된다. 키 인덱스 목록 영역(503)은 컨텐츠에 사용된 키에 대한 인덱스를 컨텐츠 단위의 형태로 기록하는 영역이다. 키 인덱스 목록 영역(503)에는, 컨텐츠에 사용된 디스크램블 키의 전체 기록 영역에 관한 키 인덱스가 기록된다.

이러한 방법으로 구성된 기록 방식의 광 디스크(100)로써, 재기록하기 어려운 디스크 식별 정보에, 지역 식별자, 데이터 범주(category) 식별자 및 디스크 식별자 등 디스크 사용에 대한 조건 또는 상태를 나타내는 정보를 제조시에 기록함으로써, 또한 광 디스크 및 재생장치에서 이러한 정보를 검출함으로써, 컨텐츠가 보유하는 저작권의 보호 레벨 또는 사용 레벨에 따라서 기록 동작과 재생 동작을 제어할 수 있다. 데이터가 재기록하기 어렵도록 기록되어서 사용자가 데이터를 변경할 수 없으므로, 저작권이 보호된 컨텐츠를 또 다른 광 디스크에 복사하는 경우에도, 사용자 데이터 영역을 복사하는 것은 가능하지만, 디스크 식별 정보는 복사할 수 없다. 따라서, 디스크 식별 정보를 사용하여 스크램블된 데이터를 광 디스크에 기록함으로써, 상이한 디스크 식별 정보를 갖는 광 디스크에서는 디스크램블될 수 없는 사용자 데이터 영역이 존재하므로 정확하게 재생하는 것을 방지할 수 있다.

도 15A는 바람직한 제1실시예에서 컨텐츠가 기록될 때 지역 식별자가 기록되는 경우에 동일한 지역 내에서 또한 상이한 지역에서 컨텐츠의 복사 또는 재생이 가능한가 아닌가를 나타내는 도면이고, 도 15B는 바람직한 제1실시예에서 광 디스크의 출하시에 지역 식별자가 이미 기록되어 있는 경우에 동일한 지역에서 또한 상이한 지역에서 컨텐츠의 복사 또는 재생이 가능한가 아닌가를 나타내는 도면이다.

예로서, 도 15A에 나타낸 바와 같이, 광 디스크의 출하시에 지역 식별 코드가 기록되어 있지 않고, 또한 컨텐츠가 기록될 때 컨텐츠를 이용할 수 있는 지역을 나타내는 지역 식별자가 기록 및 재생 영역에 기록되는 경우에, 또 다른 지역에서의 사용이 방지될 수 있다. 그러나, 컨텐츠는 또 다른 지역에서 사용되는 디스크(도 15A에 나타낸 지역 RC2용의)에 기록 가능하고, 또한 컨텐츠를 올바르게 재생할 수 있다. 컨텐츠의 디지털 복사가 가능한 기록 매체에는, 저작권 보유자의 이익을 보호하기 위하여 세금 부과 시스템이 마련되어서 광 디스크의 판매시에 부가된 요금을 수집한다. 그러나, 부가되는 요금은 국가에 따라서 상이하고, 또한 다른 국가에서 사용되는 기록 매체가 불법적으로 이용되는 경우에 저작권 보유자에게 적절한 이익을 배당할 수 없는 가능성이 남아 있다.

도 15B에 나타낸 바와 같이, 지역 식별자를 왜곡할 수 없는 방법으로 출하시에 미리 기록함으로써, 또 다른 지역에서 사용되는 광 디스크에의 컨텐츠의 복사 또는 재생을 방지할 수 있다. 상기의 방법에 유사한 방법으로, 디스크 식별 정보로서 데이터 범주 식별자를 기록한 경우에, 기록 데이터가 보유하는 범주 식별자들을 비교함으로써, 데이터를 기록할 수 있고 또

한 재생할 수 있는 디스크에의 컨텐츠의 복사 또는 재생을 제한할 수 있다. 디스크 식별 정보로서, 각각의 광 디스크에 대한 고유의 디스크 식별자를 기록한 경우에는, 기록된 데이터를 디스크 식별자로써 암호화함으로써, 기록된 데이터를 상기 광 디스크에 의해서만 이용 가능하게 할 수 있다.

본 바람직한 실시예에서, 디스크 식별 정보로써 스크램블된 데이터는 저작권 보호를 필요로 하는 AV 데이터 또는 컴퓨터 데이터이거나, 또는 스크램블된 AV 데이터 또는 컴퓨터 데이터를 디스크램블하는 디스크램블 키일 수도 있다.

도 13은 바람직한 제1실시예의 바람직한 변형 실시예에 의해서, 암호화된 디스크램블 키를 근거로 하여 디스크램블 키가 정상적인 디스크램블 키인가 아닌가를 판단하는 방법을 나타내는 블록도이다. 도 13에 나타낸 바와 같이, 디스크램블 키의 오류를 검출하는 오류 검출 코드를 디스크램블 키에 부가하여 취득한 데이터를 디스크 식별 정보를 사용하여 스크램블해서, 암호화된 디스크램블 키를 산출할 수 있도 있고, 이것을 광 디스크에 기록할 수도 있다. 광 디스크 재생장치에서, 암호화된 디스크램블 키는 디스크램블 키, 및 오류 검출 코드로 해독되어서, 해독된 오류 검출 코드의 패리티(parity) 검사에 따라서 오류를 검출함으로써 해독된 디스크램블 키가 정상적인 디스크램블 키인가 아닌가를 판단한다. 예로서, 상이한 디스크 식별 정보를 사용하여 디스크램블하는 경우에, 오류 디스크램블 키가 생성되고, 오류 검출 코드를 검사함으로써 정상적인 디스크램블 키가 아니라는 것을 판단하여 불법적인 복사를 검출할 수 있다.

디스크 식별 정보를 기록하는 또 다른 방법으로서, 복수 종류의 디스크 식별 정보를 갖는, 미리 홈이 파인 형태로 형성되는 스탬퍼(stamper)들을 구성함으로써, 또한 각각의 스탬퍼로부터 광 디스크를 형성함으로써, 상이한 스탬퍼로부터 형성된 각각의 광 디스크에 대하여 상이한 용도 제한이 부여될 수도 있다. 또한, 비밀 키를 사용하여 디스크 식별 정보를 스크램블함으로써, 또한 스크램블된 디스크 식별 정보를 광 디스크에 기록함으로써, 디스크 식별 정보에 기재된 저작권의 보호 레벨이 사용자에게 알려지지 않은 채로 유지되고, 결과적으로 저작권 보호가 더욱 강화된다.

디스크램블 키 자체를 도 4에 나타낸 키에 관한 정보로서 기록하는 경우(바람직한 제1실시예의 바람직한 변형 실시예에서)와, 디스크의 또 다른 영역에 기록된 디스크램블 키에 대한 포인터인, 키 인덱스를 기록하는 경우(바람직한 제1실시예에서)를 도 6A 및 6B를 참조로 하여 설명한다. 도 6A는 바람직한 제1실시예의 바람직한 변형 실시예에 의한, 도 1에 나타낸 섹터 데이터(401)에 디스크램블 키 및 AV 데이터를 기록하는 기록 방법을 나타내는 블록도이고, 도 6B는 바람직한 제1실시예에 의한, 도 1에 나타낸 섹터 데이터(401)에 디스크램블 키에 대한 키 인덱스 및 AV 데이터를 기록하는 기록 방법을 나타내는 블록도이다.

도 6A의 경우에는, 동일한 섹터 데이터(401)에, 주 데이터(403), 및 주 데이터(403)의 디스크램블링에 필요한 키 정보(408a)인 디스크램블 키가 기록된다. 따라서, AV 데이터를 기록할 때 디스크램블링에 필요한 디스크램블 키를 취득할 필요가 있다. 즉, AV 데이터를 기록할 때 키 자체의 취득 또는 구입이 필수적이거나 불가결하다.

다른 한편으로는, 도 6B의 경우에, 동일한 섹터 데이터(401)에는, 주 데이터(403), 및 주 데이터(403)의 디스크램블링에 필요한 정보를 기록하는 디스크램블 키 영역에 관한 키 정보(408)인 키 인덱스가 기록되고, 디스크램블 키는 키 인덱스가 나타내는 영역에 기록된다. AV 데이터를 기록할 때, 기록된 컨텐츠에 사용된 키들 중에서 어느 키가 디스크램블할 수 있는가를 나타내는 키 ID를 취득하고, 컨텐츠 정보에 포함된 키 인덱스 목록으로부터 키 ID에 대응하는 키 인덱스인, 키 정보(408)를 취득하여, 주 데이터(403)와 함께 기록한다. 디스크램블 키가 취득되면 디스크램블 키의 기록이 실행되어서 키 ID에 대응하는 키 인덱스가 나타내는 디스크램블 키 영역에 기록된다. 결과적으로, AV 데이터, 및 AV 데이터에 대응하는 디스크램블 키를 독립적으로 기록할 수 있다. 즉, AV 데이터의 기록 및 키의 취득 또는 구입은 독립적으로 실행될 수 있어서 AV 데이터를 기록할 때 키의 취득 또는 구입이 반드시 필요한 것은 아니다. 사용자는 컨텐츠를 기록하고 실제로 재생할 때 키를 취득하는 방법을 이용할 수 있게 된다.

도 14는 바람직한 제1실시예의 바람직한 변형 실시예에 의한, 디스크램블 영역 관리 테이블의 구성도를 나타낸다. 상기의 바람직한 실시예에서, 암호화된 컨텐츠와, 컨텐츠의 암호를 디스크램블하는 디스크램블 키를 상관시키기 위해서, 디스크램블 키를 조회하기 위한 키 인덱스를 동일한 섹터 데이터(401)에 기록하는 경우에 대하여 설명했지만, 암호화된 컨텐츠가 기록되는 섹터의 어드레스 범위와 디스크램블 키와의 사이의 대응 관계를 관리하는, 도 14에 나타낸 디스크램블 영역 관리 테이블을 사용할 수도 있다. 이 디스크램블 영역 관리 테이블은, 암호화된 컨텐츠가 시작 어드레스 및 종료 어드레스로써 기록되는 섹터의 어드레스 범위를 나타내고, 섹터의 데이터를 재생할 때, 디스크램블 키를 참조하여, 암호화된 컨텐츠를 디스크램블한다.

기록된 컨텐츠, 및 기록된 컨텐츠에 사용되는 디스크램블 키를 취득하기 위해서, 컨텐츠를 식별할 수 있게 하는 컨텐츠 ID를 이용한다. 도 5에 나타낸 바와 같이, 광 디스크에 기록된 컨텐츠 정보 영역(502) 내의 컨텐츠 관리 목록에 기록된 컨텐

츠 정보에는 컨텐츠 ID, 및 컨텐츠에 사용되는 디스크램블 키의 목록이 기록된다. 일편(一編)의 컨텐츠에 대해서 복수의 디스크램블 키를 사용할 수 있는 목록 구성을 구비함으로써, 컨텐츠의 일부 또는 소프트웨어의 일부를 판매할 수 있는 서비스가 가능하게 된다.

도 13을 참조로 하는 상기의 바람직한 변형 실시예에 있어서, 검사 합계(check sum) 또는 순환 중복 검사 코드(cyclic redundancy check code) 등 오류 검출 코드가 부가된 디스크램블 키를 디스크 식별 정보로써 스크램블한 데이터를 또 다른 디스크에 불법적으로 복사하는 경우, 상이한 디스크 식별 정보로써 디스크램블함으로써 오류로서 검출될 수 있다. 이러한 경우에, 광 디스크에 기록된 디스크 식별 정보에 의해서 스크램블되는 디스크램블 키를 취득하여, 상기 디스크램블 키를 취득된 디스크램블 키로써 대치함으로써 올바르게 재생될 수 있는 디스크를 작성할 수 있다.

도 1에 나타낸 키 관리 정보 영역(107)은 재기록 가능한 인입 영역(101)에 기록된다. 통상적으로, 사용자 데이터 영역(102)은 개인용 컴퓨터의 구동 장치로부터 액세스할 수 있는 사용자 영역, 및 광 디스크 상의 결함 섹터에 대한 여유 영역을 포함하고, 종래의 READ 명령 및 WRITE 명령으로써는, 사용자 영역만을 논리적인 연속 영역으로서 액세스할 수 있다. 키 관리 정보를 인입 영역(101)에 배치함으로써, 개인용 컴퓨터 등의 구동 장치로부터의 직접 액세스를 방지할 수 있어서 개인용 컴퓨터로부터, 스크램블된 AV 데이터 등을 디스크램블하는 키를 취득하는 것을 불가능하게 할 수 있다.

(바람직한 제2실시예)

도 7은 본 발명에 의한 바람직한 제2실시예의 광 디스크 기록 및 재생장치의 구성을 나타내는 블록도이다. 이 광 디스크 기록 및 재생장치는 바람직한 제1실시예에 의한 광 디스크(100)에, 저작권 보호를 필요로 하는 영상 데이터 또는 음악 데이터 등 AV 데이터의 컨텐츠를 기록하도록 구성되어 있다.

도 7을 참조하면, 701은 바람직한 제1실시예의 광 디스크를 나타내고, 702는 반도체 레이저 및 광 소자로써 구성되는 광 픽업인, 광 헤드를 나타내고, 703은 반도체 레이저의 동작을 제어하고 또한 재생 신호를 2진화하는 기록 및 재생 제어 회로를 나타낸다. 704는 기록되는 디지털 데이터를 디지털 변조하고 또한 2진화 재생 신호를 디지털 복조하는 변조 및 복조 회로를 나타내고, 705는 광 디스크(701) 상의 긁힘(scratch), 먼지 등에 의한 오류의 오류 검출과 정정 처리, 및 오류 검출과 정정 처리에 필요한 오류 정정 코드 생성 처리를 실행하는, 오류 검출 및 정정 회로를 나타낸다. 706은 오류 검출 및 정정 회로(705)의 동작 메모리 및 데이터 버퍼 메모리용으로 사용되는 버퍼 메모리인 RAM을 나타내고, 707은 스크램블되어 기록된 AV 데이터를 디스크램블하는 디스크램블 회로를 나타내며, 708은 압축되어 기록된 동영상 데이터 등을 확장하는 MPEG(Moving Picture Experts Group) 디코딩 회로를 나타낸다. 709는 확장된 영상 데이터를 D/A 변환하여 영상 신호 및 음성 신호를 생성하고 출력하는 출력 회로를 나타내고, 710은 광 디스크 기록 및 재생장치의 전체 동작을 제어하는 제어 CPU를 나타내며, 711은 컨텐츠에 배치된 암호를 디스크램블하는 디스크램블 키를 취득하는 통신 회로를 나타낸다. 712는 세트 톱(set-top) 박스 등 통신 단말 장치로부터 영상 데이터 및 음악 데이터 등 암호화된 컨텐츠의 디지털 데이터를 수신하는 데이터 수신 회로를 나타낸다.

상기와 같이 구성된 도 7의 광 디스크 기록 및 재생장치의 데이터 기록 동작을 설명한다. 세트 톱 박스 또는 MPEG 인코더 등 통신 단말 장치로부터 송신된 영상 데이터 또는 음악 데이터 등 암호화된 컨텐츠의 디지털 데이터는 데이터 수신 회로(712)에 의해서 수신된 후에 버퍼 메모리(706)에 일시적으로 저장된다. 오류 검출 및 정정 회로(705)는, 저장된 컨텐츠의 디지털 데이터에서, 광 디스크(701) 상의 긁힘 또는 먼지 등에 의한 오류의 검출과 정정 처리에 필요한 오류 검출 및 정정 코드를 생성하여 기록 데이터를 재구성한다. 오류 검출 및 정정 코드로서는, 널리 공지된 리드-솔로몬(Reed-Solomon) 코드 등의 코드가 사용된다. 이 경우에, 재구성된 기록 데이터는 컨텐츠 디지털 데이터와, 오류 검출 및 정정 코드를 포함한다. 변조 및 복조 회로(704)는 기록에 대하여 8/16 변조 시스템 등의 변조 시스템을 사용하여, 기록 데이터를 디지털 변조한다. 또한, 기록 및 재생 제어 회로(703)는 디지털 변조된 기록 데이터에 따라서, 광 헤드(702)로부터 출력되는 레이저 빔의 출력 강도를 변조하여 레이저가 광 디스크(701) 상에 조사되어서 기록 데이터가 광 디스크(701) 상에 기록되도록 한다.

도 8은 도 7에 나타낸 광 디스크 기록 및 재생장치의 제어 CPU(710)에 의해서 실행되는 AV 데이터의 기록 방법을 나타내는 흐름도이다.

도 8을 참조하면, 우선, 단계 S801에서, 광 디스크(701)로부터의 AV 데이터를 기록하기 전에 인입 영역(101)의 디스크 식별 정보를 재생하고, 이어서 단계 S802에서, 디스크 식별 정보에 기록되어 있는, 사용자 데이터 영역(102)에 기록 가능한 데이터의 방식 또는 분류로부터, 현재 기록되는 디지털 컨텐츠 데이터가 기록 가능한 것인가 아닌가를 판단한다. 단계 S802에서, YES인 경우에, 프로그램의 흐름은 단계 S803으로 진행하고, NO인 경우에는, 단계 S810에서 기록 동작이 정지되고, 이어서, AV 데이터의 기록 과정이 종료된다.

단계 S803에서, 인입 영역(101)의 키 관리 정보가 기록되어 있는 섹터의 데이터가 재생되고, S804에서, 재생된 키 관리 정보에, 컨텐츠를 기록하는 데에 필요한 키 정보용의 영역이 할당되었는가 아닌가를 판단한다. 단계 S804에서, NO인 경우에는, 키 관리 정보 영역(107)에, 키 정보를 기록하는 영역을 할당한 후에, 프로그램 흐름은 단계 S806으로 진행한다. 반면에, 단계 S804에서, YES인 경우에는, 프로그램 흐름은 단계 S806으로 직접 진행한다.

컨텐츠를 기록하는 경우에, 광 디스크 기록 및 재생장치의 제어 CPU(710)는, 통신 단말 장치로부터 데이터 수신 회로(712)를 통하여, 암호화된 컨텐츠의 기록 데이터, 및 암호를 디스크램블하는 디스크램블 키에 관한 정보를 수신한다. 이 경우에, 키에 관한 정보는 컨텐츠용으로 사용되는 키 자체, 또는 전체 컨텐츠에 사용되는 키 중에서 어느 키가 대응하는 가를 나타내는 키 ID이다. 키 ID를 수신한 경우에, 단계 S806에서, 수신된 키 ID는, 키 ID에 대응하는 디스크램블 키가 기록되는 영역을 나타내는 포인터인, 키 인덱스로 변환되고, 변환된 디스크램블 키는 디스크램블 키로써 암호 해독되는 컨텐츠 데이터가 기록되는 섹터의 헤더 영역에 배치된다. 이어서, 단계 S807에서, 제어 CPU(710)는 기록 및 재생 제어 회로(703), 변조 및 복조 회로(704)와 오류 검출 및 정정 회로(705)를 제어함으로써 이하의 기록 데이터 처리를 실행한다. 이 처리 과정에서, 기록할 필요가 있는 섹터 데이터에 오류 검출 및 정정을 위한 코드를 부가하고, 이어서, 이러한 코드가 부가된 섹터 데이터를 널리 공지된 8/16 변조 시스템 등의 변조 시스템을 사용하여 디지털 변조하고, 광 헤드(702)를 소정의 기록 위치에 위치하도록 제어하여, 레이저 빔의 강도를 디지털 변조된 기록 데이터에 따라서 변조한다. 이렇게 함으로써, 기록 데이터는 광 디스크(701)에 기록되고, 또한, S808에서, 컨텐츠의 기록이 완료되었는가 아닌가를 판단하고, NO의 경우에는, 프로그램 흐름은 단계 S806으로 복귀하여 상기의 과정을 반복한다. S808에서 YES의 경우에는, S809에서, 갱신된 키 관리 정보를 광 디스크(701) 상의 키 관리 정보 영역(107)에 기록하고, 이어서, AV 데이터의 기록 처리 과정을 종료한다.

도 9는 도 7에 나타낸 광 디스크 기록 및 재생장치의 제어 CPU(710)에 의해서 실행되는 키 관리 정보 영역의 할당 방법을 나타내는 흐름도이다. 이 방법은 컨텐츠 데이터를 기록하기 전에 디스크램블 키를 기록하는 영역을 할당하도록 구성된 것이다.

도 9를 참조하면, 단계 S901에서, 예로서, 전자 프로그램 가이드 등으로부터 기록된 컨텐츠의 키에 관한 정보(사용된 디스크램블 키의 수를 포함하는)를 취득하고, 이어서, 단계 S902에서, 광 디스크(701)에 기록된 키 관리 정보 영역(107) 내의 키 관리 정보를 재생한다. 이어서, 단계 S903에서, 키 상태 영역(506)으로부터 디스크램블 키 영역(505)의 공백 영역을 탐색하여, 기록하려고 하는 컨텐츠에 사용되는 디스크램블 키를 기록할 수 있는가 아닌가를 판단한다. 단계 S903에서 NO인 경우에는, 단계 S907에서, 기록 동작이 정지되고, 이어서, 할당 처리가 종료된다. 반면에, 단계 S903에서 YES인 경우에는, 기록하려고 하는 컨텐츠를 컨텐츠 정보 영역(502) 내의 컨텐츠 목록에 등록하고, 단계 S905에서, 디스크램블 키 영역(505)에 디스크램블 키를 기록하는 데에 필요한 영역을 예약하기 위하여 대응하는 키 상태 영역에 영역 예약 플래그를 설정함으로써 기록 영역이 할당된다. 또한, 단계 S906에서, 디스크램블 키를 기록하기 위해서 할당된 영역을 나타내는 키 인덱스를 키 목록으로서 작성하고, 이어서, 컨텐트 정보로서 설정된 포인터가 할당된 후에, 할당 처리 과정이 완료된다.

도 10은 도 7에 나타낸 광 디스크 기록 및 재생장치의 제어 CPU(710)에 의해서 실행되는, 디스크램블 키의 기록 방법을 나타내는 흐름도이다. 이 기록 방법은 키 관리 센터로부터 취득한 디스크램블 키를 광 디스크(701)에 기록하도록 구성된 것이다.

도 10을 참조하면, 우선, 단계 S1001에서, 광 디스크(701) 상의 인입 영역(101)의 디스크 식별 정보를 재생한 후에, 단계 S1002에서, 키 관리 센터로부터 디스크램블 키를 취득하기 위해서 디스크 식별 정보, 및 필요로 하는 컨텐츠를 디스크램블하는 데에 필요한 키를 식별하는 키 ID를 통신 회로(711)를 통하여 키 관리 센터에 송신한다. 키 관리 센터에서는, 소정의 키 ID로부터, 컨텐츠의 디스크램블링에 필요한 디스크램블 키를 선택하여, 디스크램블 키를 송신된 디스크 식별 정보 등, 정보를 사용하여 암호화된 다음, 회송한다.

단계 S1003에서, 키 관리 센터로부터 통신 회로(711)를 통하여 키 ID에 대응하는 디스크램블 키를 취득한 후에, 단계 S1004에서, 키 관리 정보 영역(107)의 데이터를 재생하여 재생된 키 관리 정보 영역(107) 내의 데이터 중 키 ID가 나타내는 키 인덱스 목록으로부터, 디스크램블 키를 기록하기 위한 영역을 나타내는 키 인덱스를 취득한다. 이어서, 단계 S1005에서, 상기에서 취득한 디스크램블 키를 키 인덱스가 나타내는 디스크램블 키 영역에 할당하고, 취득한 키를 나타내는 취득한 플래그를 대응하는 키 상태 영역(506)에 배치한다. 또한, 단계 S1006에서, 모든 키의 취득이 완료되었는가 아닌가를 판단하고, 이어서, NO의 경우에 단계 S1003으로 되돌려 보냄으로써 상기 과정을 반복한다. 반면에, 단계 S1006에서 YES의 경우에는 단계 S1007에서, 갱신된 키 관리 정보가 키 관리 정보 영역(107)에 기록되고, 이어서, 디스크램블 키 기록 처리 과정이 완료된다.

후속해서, 본 실시예의 광 디스크 기록 및 재생장치의 데이터 재생 동작을 도 7을 참조로 하여 설명한다. 광 디스크(701)에 기록된 디지털 데이터는 이하와 같이 재생된다. 광 헤드(702)로부터의 반도체 레이저의 레이저 빔을 광 디스크(701)에 조사하고, 이 때, 광 디스크(701) 상에서 반사되는 반사광은 광 헤드(702)를 통하여 기록 및 재생 제어 회로(703)에 입력된다. 기록 및 재생 제어 회로(703)는 입력된 반사광을 광전(光電) 변환한 후에 증폭 및 2진화 처리를 실행함으로써 재생된 2진화 신호를 생성하고 생성된 재생 2진화 신호를 변조 및 복조 회로(704)에 출력한다. 변조 및 복조 회로(704)는 기록의 경우에 널리 공지된 8/16 변조 시스템 등의 변조 시스템을 사용하여 디지털 변조된 신호를 디지털 신호로 디지털 복조하고, 이어서, 생성되는 디지털 신호를 오류 검출 및 정정 회로(705)에 출력한다. 후속해서, 오류 검출 및 정정 회로(705)는 동작 메모리로서 버퍼 메모리(706)를 사용하여 광 디스크(701) 상의 긁힘 또는 먼지에 의해서 발생되는 오류의 검출과 정정 처리를 실행한다. 이러한 오류 검출 및 정정 처리는, 예로서, 널리 공지된 리드-솔로몬(Reed-Solomon) 코드를 디코딩함으로써 실행된다.

오류 검출 및 정정 처리된 재생 데이터는 디스크램블 회로(707)에 출력되어서 디스크램블 처리가 실행된다. 디스크램블 회로(707)는 데이터 재생 전에 미리 재생된 키 관리 정보 영역(107)의 디스크램블 키를 사용하여, 재생 데이터에 대한 디스크램블 처리를 실행하고, 이어서, 이 데이터는 MPEG 디코딩 회로(708)에 출력된다. 후속해서, MPEG 디코딩 회로(708)는 압축된 동영상 데이터 및 음악 데이터 등을 확장하고, 확장된 데이터는 출력 회로(709)에 출력된다. 또한, 출력 회로(709)는 입력된 확장 데이터를 영상 신호 및 음성 신호로 D/A 변환하여, 생성되는 영상 신호 및 음성 신호를 텔레비전 세트, 오디오 장치 등 상위 레벨의 장치에 출력한다.

도 11은 도 7에 나타낸 광 디스크 기록 및 재생장치의 제어 CPU(710)에 의해서 실행되는 AV 데이터의 재생 방법을 나타내는 흐름도이다.

도 11을 참조하면, 우선, 단계 S1101에서, 광 디스크(701)로부터 AV 데이터를 기록하기 전에 인입 영역(101) 내의 디스크 식별 정보를 재생하고, 단계 S1102에서, 디스크 식별 정보에 기록된 재생 가능한 데이터의 타입으로부터, 현재 재생하려고 하는 컨텐츠가 재생 가능한가 아닌가를 판단한다. 단계 S1102에서 NO의 경우에, 단계 S1112에서 재생 동작이 정지되고, 이어서, AV 데이터의 재생 처리가 종료된다. 반면에, 단계 S1102에서 YES의 경우에, 인입 영역(101)의 키 관리 정보 영역(107) 내에, 키 관리 정보가 기록되어 있는 섹터의 데이터를 재생하고, 단계 S1104에서 컨텐츠의 재생에 필요한 키 정보가, 재생된 키 관리 정보에 기록되어 있는가 아닌가를 판단한다. 단계 S1104에서 YES의 경우에, 프로그램 흐름은 단계 S1106으로 직접 진행한다. 반면에, 단계 S1104에서 NO의 경우에, 단계 S1105에서, 키를 관리하는 키 관리 센터로부터 통신 회로(711)를 통하여 디스크램블 키를 취득하여, 광 디스크(701) 상의 키 관리 정보 영역(107)에 기록한 다음, 프로그램 흐름은 단계 S1106으로 진행한다.

이어서, 단계 S1106에서, 제어 CPU(710)는 광 헤드(702)를 광 디스크(701)의 사용자 데이터 영역으로 이동시키고, 기록 및 재생 제어 회로(703), 변조 및 복조 회로(704), 및 오류 검출 및 정정 회로(705)를 제어하여 AV 데이터를 재생한다. 이어서, 단계 S1107에서, 재생된 섹터의 헤더에 포함된 키 인덱스가 나타내는 디스크램블 키 영역(505)으로부터 섹터 데이터의 디스크램블링에 필요한 디스크램블 키를 취득하고, 후속해서, 단계 S1108에서, 디스크램블 키에 대한 스크램블된 정보를 디스크 식별 정보로써 디스크램블함으로써 디코딩한다. 또한, 단계 S1108에서, 디스크램블 키에 부가된 오류 검출 코드를 검사함으로써, 디스크램블 키에 오류가 있는가 없는가를 판단한다. 단계 S1108에서 YES의 경우에, 컨텐츠가 불법적으로 취득된 것(또는 컨텐츠가 불법적으로 복사된 것)으로 판단되고, 단계 S1112에서 재생 동작이 정지되며, 이어서 AV 데이터의 재생 처리 과정이 종료된다.

반면에, 단계 S1108에서 NO의 경우에, S1109에서, 컨텐츠 데이터를 디스크램블 키로써 디스크램블하고, 단계 S1110에서, 디스크램블된 AV 데이터를 MPEG 디코딩 회로(708)에 출력한다. 이어서, 제어 CPU(710)는 MPEG 디코딩 회로(708) 및 출력 회로(709)를 제어함으로써 소정의 MPEG 시스템을 사용하여, 디스크램블된 AV 데이터를 MPEG-확장하고, 이어서, MPEG-확장된 AV 데이터를 영상 신호 및 음성 신호로 D/A 변환하여, 텔레비전 세트, 오디오 장치 등 상위 레벨의 장치에 출력한다. 후속해서, 단계 S1111에서, 컨텐츠의 재생이 완료되었는가 아닌가를 판단하고, NO의 경우에 프로그램 흐름은 단계 S1106으로 복귀되어서 상기의 과정을 반복한다. 반면에, 단계 S1111에서 YES의 경우에, AV 데이터의 재생 처리 과정은 종료된다.

단계 S1109에서, 오류가 검출되는 경우에, 컨텐츠를 불법적으로 취득한 것으로 간주하거나, 예로서, 컨텐츠를 불법적으로 복사한 것으로 간주하여, 재생 동작을 정지한다. 그러나, 키 정보는 통신 회로(711)를 통하여, 키를 관리하는 키 관리 센터로부터 취득할 수도 있고 또한 아무런 키도 기록되어 있지 않은 경우에 동일한 방법으로 단계 S1105의 처리를 실행함으로써 광 디스크(701) 상의 키 관리 정보 영역(107)에 기록할 수도 있다. 이렇게 함으로써, 복사된 AV 데이터라도 합법적인 절차로 키를 취득함으로써 재생할 수 있게 된다.

도 12는 도 7에 나타낸 광 디스크 기록 및 재생장치의 제어 CPU(710)에 의해서 실행되는 디스크램블 키의 취득 방법을 나타내는 흐름도이다. 이 방법은 재생된 키 인덱스로부터 디스크램블 키를 재생하도록 구성된 것이고, 이 방법은 도 11에 나타낸 바와 같이 AV 데이터의 재생 처리 과정 전에 실행된다.

도 12를 참조하면, 우선, 단계 S1201에서, 재생된 섹터 영역의 데이터가 스크램블 제어 정보에 의해서 스크램블되어 있는가 아닌가를 판정하고, NO의 경우에, 프로그램 흐름은 단계 S1206으로 진행한다. 반면에, 단계 S1201에서 YES의 경우에, 단계 S1202에서, 상기의 섹터 영역에 동일한 섹터 영역에 기록된 키 정보를 재생함으로써 키 인덱스를 취득하고, 이어서, 단계 S1203에서, 디스크램블 키 영역(505)으로부터 상기의 키 인덱스가 나타내는 디스크램블 키를 취득하며, 후속해서, 단계 S1204에서, 취득된 디스크램블 키를 디스크 식별 정보를 사용하여 디스크램블하여, 오류 검출 코드를 검사함으로써 디스크램블 키에 오류가 있는가 없는가를 판단한다. 단계 S1204에서 YES의 경우에, 단계 S1205에서, 재생 동작을 정지하고, 디스크램블 키의 취득 처리 과정을 종료한다. 반면에, 단계 S1204에서 NO의 경우에, 프로그램 흐름은 단계 S1206으로 진행한다. 디스크 식별 정보로써 디스크램블 키를 디스크램블한 결과 재생된 섹터가 스크램블되어 있지 않거나 또는 아무런 오류도 존재하지 않는 것으로 판명되면, 단계 S1206에서, 재생 동작이 승인되어서, 재생된 섹터의 데이터가 출력되고, 이어서, 디스크램블 키의 취득 과정이 종료된다.

상기와 같이, 본 발명에 의한 바람직한 실시예의 광 디스크와, 광 디스크 기록 및 재생장치에 있어서, 기록 및 재생 동작은 디스크 제조 단계에서 작성된 판독 전용의 디스크 식별 정보를 사용하여 사용자에 의해서 제어될 수 있다. 또한, 상기의 디스크 식별 정보를 사용하여 데이터의 일부를 스크램블함으로써, 사용자 데이터 영역이 물리적으로 복사된 디스크 상의 데이터를 정상적으로 재생하는 것을 방지할 수 있다. 또한, 데이터 디스크램블링에 필요한 디스크램블 키를 데이터 영역과는 상이한 영역에 할당함으로써, 컨텐츠의 기록 및 디스크램블 키의 기록을 독립적으로 실행할 수 있다. 따라서, 컨텐츠를 기록하고 또한 필요하면, 디스크램블 키를 취득함으로써, 예로서, 컨텐츠 데이터를 재생할 때, 컨텐츠를 재생 가능한 상태로 유지할 수 있다. 이 때, 디스크램블 키를 디스크 식별 정보로써 스크램블함으로써, 물리적인 복사에 의한 불법적인 사용을 상기의 방법과 동일한 방법으로 방지할 수 있는 것은 명백하다. 이에 추가하여, 불법적으로 복사된 디스크는, 키 관리 센터로부터 광 디스크의 디스크 식별 정보로써 스크램블된 디스크램블 키를 공식적으로 취득함으로써, 또한 취득한 디스크램블 키를 광 디스크에 기록함으로써 정상적으로 재생될 수 있는 광 디스크가 될 수 있다.

상기에서 광 디스크 기록 및 재생장치에 입력된 이미 암호화된 컨텐츠 데이터를 설명하였지만, 광 디스크 기록 및 재생장치 내에 컨텐츠를 암호화하는 회로를 구성함으로써, 입력된 컨텐츠 데이터를 암호화하여 이 데이터를 광 디스크에 기록함으로써, 동일한 효과를 얻을 수 있다.

본 바람직한 실시예에서는, 암호화된 컨텐츠를 해독하는 데에 필요한 디스크램블 키만을 디스크 식별 정보를 사용하여 암호화함으로써, 상이한 디스크 식별 정보를 갖는 디스크들 간의 복사를 방지하지만, 컨텐츠 자체를 디스크 식별 정보를 사용하여 암호화함으로써 복사를 방지할 수 있다. 또한, 비밀 키를 사용하여 디스크 식별 정보를 암호화함으로써, 디스크에 기록된 컨텐츠의 불법적인 암호 해독을 더욱 어렵게 할 수 있다.

제1 및 제2실시예의 유리한 효과

본 발명에 의한 바람직한 실시예의 광 디스크는, 각각의 광 디스크에 대하여 기록 동작 및 재생 동작을 실행하는 디스크 식별 정보가 사용자 데이터 영역 내의 재기록 가능하지 않은 판독 전용 영역에 기록되므로, 상기 광 디스크는, 광 디스크 제조시에 기록된 정보를 사용하여 사용자에 의한 광 디스크에의 컨텐츠의 기록 동작 및 재생 동작을 제어할 수 있다.

본 발명에 의한 바람직한 실시예의 광 디스크는, 재기록할 수 없는 판독 전용의 디스크 식별 정보를 키로 하여 광 디스크의 사용자 데이터 영역에 암호화된 데이터를 기록함으로써 사용자에 의해서 사용자 데이터 영역 정보가, 상이한 기록 방식의 광 디스크에 복사되는 경우에도 디스크 식별 정보가 복사되는 것을 방지할 수 있으므로, 데이터의 올바른 디코딩 및 재생을 불가능하게 한다.

본 발명에 의한 바람직한 실시예의 광 디스크는 암호화된 데이터, 및 상이한 섹터 영역의 암호를 해독하는 디스크램블 키를 기록함으로써, (a) 영화, 음악 등 저작권 보호를 필요로 하는 데이터의 취득, 및 (b) 암호를 해독하는 디스크램블 키의 취득을 독립적으로 실행 가능하게 한다. 또한, 디스크 식별 정보를 키로 하여 디스크램블 키를 암호화하여 기록함으로써, 사용자에 의해서 사용자 데이터 영역 정보가 또 다른 기록 방식의 광 디스크에 복사되는 경우에도, 디스크 식별 정보는 복사될 수 없고, 데이터의 올바른 디코딩 및 재생이 불가능하게 되며, 복사되는 광 디스크에 대한 디스크 식별 정보를 키로 하여 암호화된 디스크램블 키를 취득하여 기록함으로써 데이터의 올바른 디코딩 및 재생이 가능하게 된다.

(바람직한 제3실시예)

이어서, 본 발명에 의한 바람직한 제3실시예의 암호화된 컨텐츠 기록 및 재생 방법을 도면을 참조로 하여 설명한다. 도 16은 본 발명에 의한 바람직한 제3실시예의 광 디스크(1101)의 데이터 기록 영역을 나타내는 평면도이다.

도 16을 참조하면, 1101은 디지털 데이터를 기록할 수 있고, 또한 재기록 가능 또는 재기록 불가능 광 디스크 등의 기록 방식의 광 디스크인 기록 매체를 나타내고, 1102는 디스크 정보가 미세한 요철(凹凸) 홈의 형태로 기록되는 제어 사용자 데이터 영역을 나타내고, 또한 1103은 광 디스크에 레이저 광 빔을 조사함으로써 사용자가 데이터를 기록하는 사용자 데이터 영역을 나타낸다. 1104는 디스크 ID가 기록되는 BCA를 나타낸다. BCA(1104)에는, YAG 레이저 등 펄스 레이저의 레이저 빔을 기록막 위에 부분적으로 조사함으로써, 제어 사용자 데이터 영역(1102)의 내주부의 미세한 요철 홈 위의 기록막이 트리밍(trimming)되어서, 복수의 트리밍 영역(1105)이 반경 방향으로 연장되는 형태로 형성됨에 따라서, 디스크램블된 식별 정보인 디스크 ID가 기록된다.

도 17은 바람직한 제3실시예에 의한 BCA 재생 회로(1401)에서의 재생 신호 (1201)와 재생 2진 신호(1207)의 신호 파형을 나타내는 파형도이고, 도 18은 바람직한 제3실시예에 의한 BCA 재생 회로(1401)의 구성을 나타내는 블록도이다. 도 17은 BCA(1104)의 데이터가 재생될 때의 재생 신호(1201)를 나타낸다. 도 18에서, 1301은 광 픽업을 나타내고, 1302는 전치 증폭기를 나타내고, 1303은 저역통과 필터(LPF)를 나타내고, 1304는 2진화 회로를 나타내며, 1305는 복조 회로를 나타낸다.

도 18을 참조하면, 광 픽업(1301)으로부터 출력된 레이저 빔이 광 디스크(1101)의 BCA(1104)를 조사하고, 반사광은 광 픽업(1301)에 의해서 광전 변환되고, 후속해서, 광전 변환된 전기 신호가 전치 증폭기(1302)에 의해서 증폭되어서 재생 신호(1201)가 취득된다. 이 경우에, 도 17에 나타낸 재생된 신호(1201)는 제어 사용자 데이터 영역(1102)의 요철 홈에 대응하는 레벨을 가지며, 이 재생된 신호(1201)에서, 1202, 1203 및 1204 각각은 펄스 레이저에 의한 트리밍 공정으로써 기록막이 제거될 때 신호가 요철 홈 형태로 탈락하는 트리밍 부분을 나타낸다. 이러한 트리밍 공정은 광 디스크의 제조자에 의해서 실행된다.

설명을 위해서 다시 도 18을 참조하면, 재생 신호(1201)는 저역통과 필터(1303)에 입력되고, 이어서 필터는 요철 홈에 의해서 형성된 피변조 신호를 제거한 후에, 생성된 신호를 2진화 회로(1304)에 출력한다. 2진화 회로(1304)에 입력된 재생 신호는 제어 사용자 데이터 영역(1102)의 신호를 2진화하는 정상 슬라이스(slice) 레벨(1205) 대신에 슬라이스 레벨(1205)보다 상당히 낮은 레벨인 슬라이스 레벨(1206)을 사용하여 2진화되어서 재생 2진화 신호(1207)가 취득된다. 2진화 회로(1304)로부터 출력된 재생 2진화 신호(1207)는 복조 회로(1305)에 의해서 복조되어서, 디스크 ID 신호(1306)가 취득된다.

상기한 바와 같이, 광 디스크를 식별하는 디스크 식별 정보를 부가함으로써, 광 디스크의 관리가 용이하게 실시될 수 있다. 또한, BCA(1104)를 요철 홈 형태로 기록함으로써, BCA(1104) 내의, 광 디스크를 식별하는 정보가 용이하게 왜곡되는 것을 방지할 수 있다. 추가로, 도 16에 나타낸 제어 사용자 데이터 영역(1102)과 BCA(1104)는 서로 인접하므로, 제어 사용자 데이터 영역(1102)의 데이터가 재생되면 BCA(1104)의 데이터가 연속적으로 재생될 수 있거나, 또는 BCA(1104)의 데이터가 재생되면 제어 사용자 데이터 영역(1102)의 데이터가 연속적으로 재생될 수 있으므로, 예로서, 광 디스크가 시동될 때 CPU가 광 디스크를 신속하게 식별하기 위한, BCA(1104)의 정보를 취득하고 또한 암호화된 컨텐츠를 기록하는 처리 과정을 앞당길 수 있게 된다.

바람직한 실시예의 BCA(1104)는 제어 사용자 데이터 영역(1102)의 내주부에 요철 홈 형태로 기록막을 트리밍하도록 형성되지만, 재기록 가능 디스크 또는 재기록 불가능 디스크 중 어느 하나인, 기록 방식의 광 디스크를 구성하는 기록막은 판독 전용 광 디스크 상에 형성된 반사막에 비하여 열에 의해서 쉽게 영향을 받는다. 사용자 데이터 영역(1102)의 내주부를 트리밍함으로써, 사용자 데이터 영역(1103)은 외주부를 트리밍하는 경우에 비하여 트리밍시에 방출되는 열로부터 보호된다. 또한, BCA(1104)를 제어 사용자 데이터 영역(1102)의 내주부에 형성하는 이유는 레이저 장치의 집속(集束) 서보(servo) 회로의 불안정성 때문에 레이저 빔의 스폿의 직경이 변화하는 경우에 여유를 고려해야 하기 때문이다.

트리밍 전에 BCA(1104)에 기록된 데이터를 제어 사용자 데이터 영역(1102)에 기록할 수도 있다. BCA(1104)에 기록된 데이터를 또한 제어 사용자 데이터 영역(1102)에 기록할 수도 있고, 이로 인하여 제어 사용자 데이터 영역(1102)의 상기 데이터가 트리밍으로부터 보호될 수 있다. 또한, BCA(1104)에 기록된 데이터가 BCA(1104)로부터 제어 사용자 데이터 영역(1102)에 연속적으로 또한 반복적으로 기록될 때, 제어 사용자 데이터 영역(1102)의 상기 데이터를 탐색함으로써 BCA(1104)의 위치를 예측할 수 있다.

이어서, 네트워크를 통하여 디스크 ID로써, 암호화된 컨텐츠를 상기의 BCA(1104)를 갖는 광 디스크(1101)에 기록하는 절차를 설명한다. 바람직한 제3 내지 제5실시예에서, 네트워크는, 예로서, 인터넷, 공공 전화 회선, 또는, 임대 회선 또는 회로 등 기타 통신 회선을 의미한다. 도 19는 바람직한 제3실시예에 의한 광 디스크 기록 및 재생 시스템의 구성을 나타내는 블록도이고, 상기의 BCA(1104)를 갖는 재기록 가능 디스크 또는 재기록 불가능 디스크 중 어느 하나인, 기록 방식의 광 디스크(1101)에 암호화된 컨텐츠를 기록하는 장치 구성을 나타낸다.

도 19를 참조하면, 광 디스크 기록 및 재생 시스템은 광 디스크 기록 및 재생장치(1410), 및 인터넷 등 네트워크(1405)를 통하여 서로 접속되는 암호부(1406)를 포함하여 구성된다. 광 디스크 기록 및 재생장치(1410)는 광 픽업(1301), BCA 재생 회로(1401), 인터넷(403), 기록 회로(1411), 데이터 재생부(1412) 및 암호 디코더(1413)를 포함한다. 또한, 암호부(1406)는 인터페이스(1404), 컨텐츠 메모리(1407) 및 암호 인코더(1408)를 포함한다.

우선, 광 픽업(1301)으로부터 출력된 레이저 빔은, 예로서, RAM 타입 광 디스크(1101)의 BCA(1104)를 조사하고, 이어서, 반사광이 광 픽업(1301)에 의해서 광전 변환된 후에, 광전 변환된 재생 신호가 BCA 재생 회로(1401)에 입력된다. BCA 재생 회로(1401)는 입력된 재생 신호에 따라서 BCA 내의 디스크 ID 신호(1402)를 재생하여, 재생된 디스크 ID 신호(1402)를 암호 디코더(1413)에 출력하고, 또한 동일한 디스크 ID 신호(1402)를 인터페이스(1403 및 1404) 및 네트워크(1405)를 통하여 암호부(1406)의 암호 인코더(1408)에 동시에 출력한다. 암호 인코더(1408)는 컨텐츠 데이터를 암호화하거나 또는 영상 및 음성 컨텐츠 데이터를 스크램블하고, 디스크 ID 신호(1402)가 컨텐츠 메모리(1407) 내의 컨텐츠 데이터가 기록되는 광 디스크(1101)에 대한 암호를 해독하는 암호 해독 키가 된다.

본 바람직한 실시예에서, 암호화 방법은, 디스크 ID 신호(1402)를 암호 키로서 사용하여 컨텐츠(1407)를 암호화하는 방법과 동일한 것을 의미한다. 또한, 본 바람직한 실시예에서, 암호화와 암호 해독은 자물쇠와 열쇠와의 사이의 관계로서 간주되어서, 자물쇠를 열쇠로써 잠그는 것은 암호화를 의미하고 자물쇠를 열쇠로써 여는 것은 암호 해독을 의미한다. 따라서, 암호화와 암호 해독은 실제의 연산이 서로 상이하지만, 암호화 키와 암호 해독 키는 서로 동일하다. 컨텐츠(1407)는 C로서 표시되고, 디스크 ID 신호(1402)는 BCAS로서 표시되고, 암호화된 컨텐츠(1409)는 C[BCAS]로서 표시되며, 암호화 처리에 대한 연산은 *로서 표시된다. 이어서, 이하의 식을 표시할 수 있다.

$$C * BCAS = C\ [BCAS] \quad (1)$$

암호부(1406)에 의해서 암호화된 컨텐츠(1409)는 인터페이스(1403 및 1404) 및 네트워크(1405)를 통해서 기록 및 재생 장치(1410)의 기록 회로(1411)에 송신된다. 기록 회로(1411)는 입력된 컨텐츠 데이터를 소정의 방법으로 디지털 변조하고, 디지털 변조된 데이터에 대응하여 광 픽업(1301)으로부터의 레이저 빔의 강도를 변조하여 레이저 빔을 광 디스크(1101)에 조사함으로써 컨텐츠 데이터를 광 디스크(1101)에 기록한다.

이어서, 광 디스크에 암호화되어 기록된 상기 컨텐츠를 재생할 때는, 광 픽업(1301)으로부터 출력되는 레이저 빔이 사용자 데이터 영역(1103)의 상기 암호화된 컨텐츠가 기록되어 있는 영역을 조사하고, 반사광이 광 픽업(1301)에 의해서 광전 변환된 후에, 광전 변환된 재생 신호가 데이터 재생부(1412)에 입력된다. 데이터 재생부(1412)는 입력된 재생 신호를 디지털 데이터로 A/D 변환하여, 디지털 데이터를 암호 디코더(1413)에 출력한다. 다른 한편으로는, 광 픽업(1301)으로부터의 레이저 빔이 광 디스크(1101)의 BCA(1104)에 조사되어, 반사광이 광 픽업(1301)에 의해서 광전 변환된 후에, 광전 변환된 재생 신호가 BCA 재생 회로(1401)에 입력된다. BCA 재생 회로(1401)는 입력된 재생 신호를 A/D 변환하여 디스크 ID 신호(1402)를 생성하고, 이어서, 디스크 ID 신호(1402)는 암호 디코더(1413)에 출력된다.

암호 디코더(1413)는 입력된 디스크 ID 신호(1402)를 암호화된 컨텐츠 데이터를 해독하는 키로서 사용한다. 이 때, 컨텐츠가 광 디스크(1101)에 합법적으로 기록될 때, 광 디스크(1101)에 기록된 암호화된 컨텐츠를 해독하는 키는 광 디스크(1101)의 디스크 ID 신호(1402)이고, 재생시에 BCA 재생 회로(1401)로부터 출력되는 디스크 ID 신호(1402)도 또한 광 디스크(1101)의 디스크 ID 신호(BCAS)이다. 따라서, 암호 해독되거나 또는 디스크램블된 컨텐츠가 출력 신호(1414)로서 암호 디코더(1413)로부터 출력된다. 디코딩 처리 연산을 #로써 표시하면, 이하의 식을 표시할 수 있다.

$$C\ [BCAS] \# BCAS = C \quad (2)$$

이 경우에, 컨텐츠 데이터가 영상 데이터일 때, MPEG 신호 등 영상 데이터는 확장되어서 영상 신호 데이터가 취득된다.

상기한 바와 같이, 본 바람직한 실시예의 암호화는 디스크 ID를 키로서 사용하며, 또한 하나의 광 디스크에 대응하여 하나의 디스크 ID만이 존재하므로, 동일한 암호화된 컨텐츠는 상기 광 디스크에만 기록될 수 있는 유리한 효과를 갖는다. 즉,

말하자면, 상기 컨텐츠(1407)를, 예로서, ID1의 디스크 ID를 갖는 합법적인 광 디스크로부터 ID2의 또 다른 디스크 ID를 갖는 또 다른 광 디스크에 복사하여 재생하려고 하는 경우, BCA 재생 회로(1401)로부터 디스크 ID 신호(1402)로서 ID2가 출력된다. 그러나, 암호화된 컨텐츠는 ID1인 디스크 ID 신호로써 암호화되어 있으므로, 암호화된 컨텐츠는 암호 디코더(1413)에 의해서 디코딩될 수 없다.

암호 인코더(1408)는 컨텐츠의 공급원에 배치되지 않고, 네트워크의 기록 및 재생장치측에 배치되어서, 암호 인코더가 장착된 IC 카드 등의 형태로 구성될 수도 있다. 또한, 상기의 광 디스크(1101)는 디스크 ID만을 사용하여 암호화되어 있으므로, BCA 재생 회로(1401)와 암호 디코더(1413)를 구비한 임의의 광 디스크 기록 및 재생장치로써 데이터를 재생할 수 있다.

(바람직한 제4실시예)

이어서, 본 발명에 의한 바람직한 제4실시예의 암호화된 컨텐츠 기록 방법을 도면을 참조로 하여 설명한다. 도 20은 본 발명에 의한 바람직한 제4실시예의 광 디스크 기록 및 재생 시스템의 구성을 나타내는 블록도이고, 이것은 BCA를 갖는 재기록 가능 광 디스크 또는 재기록 불가능 광 디스크 중 어느 하나인 기록 방식의 광 디스크에 암호화된 컨텐츠를 기록하는 장치 구성을 나타낸다. 바람직한 제4실시예의 설명에서, 바람직한 제3실시예에 공통인 구성 요소의 설명은 생략한다.

도 20을 참조하면, 바람직한 제4실시예에 의한 광 디스크 기록 및 재생 시스템은, CATV 회사의 장치(1501), 키 발행 센터 장치(1507), CATV 디코더(1506), 광 디스크 기록 및 재생장치(1514), 및 텔레비전 세트(1530)를 포함한다. 이 경우에, CATV 회사의 장치(1501)는 영화 소프트웨어 등 컨텐츠 데이터를 저장하는 컨텐츠 메모리(1502), 제1암호 키를 저장하는 제1암호 키 메모리(1503), 및 제1암호 인코더(1504)를 포함한다. 또한, 키 발행 센터 장치(1507)는 장치(1507)의 동작을 제어하는 제어부(1507a), 시간 제한 정보를 저장하는 시간 제한 정보 메모리(1510), 및 허가 제한 코드를 저장하는 기록 허가 코드 메모리(1511)를 포함한다. 또한, CATV 디코더(1506)는, CATV 디코더(1506)의 시스템 ID를 저장하는 시스템 ID 메모리(1508), 제1암호 디코더(1513), 제2암호 인코더(1516), 및 IC 카드(1522) 내에 구성된 회사 식별 신호 메모리(1523)를 포함한다. 또한, 광 디스크 기록 및 재생장치(1514)는 기록 회로(1518), 데이터 재생부(1519), BCA 재생 회로(1521), 제2암호 디코더(1520), 및 IC 카드(1524) 내에 구성된 회사 식별 신호 메모리(1526)를 포함한다.

우선, CATV 회사 장치(1501)의 제1암호 인코더(1504)는 제1암호 키 메모리(1503)에 저장된 제1암호 키를 사용하여, 컨텐츠 메모리(1502)에 저장된 영화 소프트웨어 등 컨텐츠 데이터를 암호화하고, 이에 따라서 제1암호화 컨텐츠(1505)를 생성한다. 이어서, 생성된 제1암호화 컨텐츠(1505)는 네트워크를 통하여 각각의 사용자의 CATV 디코더(1506)의 제1암호 디코더(1513)에 송신된다. 컨텐츠 메모리(1502)에 저장된 데이터를 C로서 표시하고, 제1암호 키(1503)를 FK로서 표시하고, 또한 제1암호화 컨텐츠(1505)를 C[FK]로서 표시하면, 이하의 식을 표시할 수 있다.

C * FK = C [FK] (3)

CATV 디코더(1506)는 네트워크를 통하여 키 발행 센터 장치(1507)에,

(a) 시스템 ID 메모리(1508)에 저장된 CATV 디코더(1506)용 시스템 ID, 및

(b) 오디오 타입 또는 RAM 타입의 광 디스크(1101)에 기록하려고 하는 상기 컨텐츠에 미리 부가되어 있는, 예로서, CATV 디코더(1506)의 키보드(도면에 나타내지 않음)를 사용하여 입력된 타이틀 코드(1509)를 송신한다. 이 경우에, 타이틀 코드(1509)는 TV 스크린에 따라서 선택하여 입력하거나, 또는 키보드를 사용하여 직접 입력하거나, 또는 원격 제어기 등으로부터 입력할 수도 있다. 따라서, 타이틀 코드(1509)는 사용자가 자기 자신의 방법으로 취득함으로써 취득되거나, 또는 제1암호화 컨텐츠(1505)와 함께 CATV 디코더(1506)에 입력될 수도 있다. 타이틀 코드(1509)는 프로그램 가이드 등의 형태로 제1암호화 컨텐츠(1505)의 시간과 상이한 시간에 미리 송신될 수도 있다.

CATV 디코더(1506)의 시스템 ID와 상기 컨텐츠의 타이틀 코드(1509)에 따라서, 키 발행 센터 장치(1507)의 제어부(1507a)는, 시간 제한 정보 메모리(1510)에 저장된 시간 제한 정보, 및 기록 허가 코드 메모리(1511)에 저장된 기록 허가 코드를 조회하여, 기록 허가 코드와 시간 제한 코드의 데이터에 대응하는 키(K)(1512)를 기록 허가 코드 및 시간 제한 코드와 함께, 네트워크를 통하여 CATV 디코더(1506)의 제1암호 디코더(1513)에 송신한다. 시간 제한 정보는 동일한 컨텐츠가 상이한 시간에 복수 회 전송되는 경우 중에서 동일한 컨텐츠를 구별할 수 있게 한다. 제1암호 해독 키를 FK로서 표시하고, CATV 디코더(1506)의 시스템 ID를 DID로서 표시하고, 시간 제한 정보를 TIME으로서 표시하고, 기록 허가 코드를 COPY로서 표시하고, 또한 컨텐츠의 타이틀 코드(1509)를 T로서 표시하면, 키(K)는 이하의 식으로 표시되는 관계를 만족시킨다.

FK = K * T * DID * TIME * COPY (4)

CATV 회사 장치(1501)가, 예로서, 방송 컨텐츠가 새로운 작품인가 또는 낡은 작품인가 아닌가를 판단하는 판단 결과에 따라서, 기록 허가 코드 메모리(1511)에 저장된 기록 허가 코드가 시청을 위해서만 허가할 것인가 또는 시청 및 기록 모두에 대하여 허가할 것인가를 결정한다.

CATV 디코더(1506)의 제1암호 디코더(1513)는, 제1암호 키(FK), 키(K)(1512), 상기 컨텐츠의 타이틀 코드(1509), 시스템 ID, 기록 허가 코드 및 시간 제한 정보가 상기 관계를 만족시키고, 또한 클록 회로(1527)로부터 출력된 현재 시간 정보가 시간 제한 정보의 조건을 만족시키면, 제1암호화 컨텐츠(1505)를 해독한다. 이 경우에, 상기 암호화 컨텐츠가 영상 신호일 때, 디스크램블된 영상 신호는 제1암호 디코더(1513)로부터 텔레비전 세트(1530)에 출력되고, 이어서, 사용자는 영상 신호의 영상을 보고 영상 신호에 대응하는 음성 신호를 청취할 수 있다. 이 경우에, 제1암호 디코더(1513)의 암호 해독 처리 과정은 이하의 식으로 표시된다.

C [FK] # (K*T*DID*TIME*COPY)

= C [FK] # FK

= C (5)

기록 허가 코드가 시청만을 승인할 때, 컨텐츠 데이터를 광 디스크(1101)에 기록할 수 없지만, 시청 및 기록 모두를 승인할 때는 컨텐츠 데이터를 광 디스크(1101)에 기록할 수 있다. 따라서, 이 방법을 이하와 같이 설명한다.

광 디스크 기록 및 재생장치(1514)의 BCA 재생 회로(1521)는 광 디스크(1101)의 BCA(1104)의 데이터를 재생하여 디스크 ID 신호(1515)를 취득하고, 디스크 ID 신호를 CATV 디코더(1506)의 제2암호 인코더(1516)에 출력한다. CATV 디코더(1506)의 제2암호 인코더(1516)는, 디스크 ID 신호(1515)를 제2암호 키로서 사용하여, 제1암호 디코더(1513)로부터 출력된 컨텐츠 데이터를 암호화하여 제2암호화 컨텐츠(1517)를 생성하고, 생성된 제2암호화 컨텐츠(1517)를 광 디스크 기록 및 재생장치(1514)의 기록 회로(1518)에 출력한다. 상기 제2암호 인코더(1516)의 암호화는 제1암호 디코더(1513)로부터 제1암호화 컨텐츠가 해독되어 출력되는 시간으로 제한되는 것을 염두에 두어야 한다. 제1암호 디코더(1513)로부터의 출력 신호인 컨텐츠를 C로 표시하고, 제2암호 키인 디스크 ID 신호(1515)를 BCAS로 표시하고, 또한 제2암호화 컨텐츠(1517)를 C[BCAS]로 표시하면, 이하의 식을 표시할 수 있다.

C * BCAS = C [BCAS] (6)

광 디스크 기록 및 재생장치(1514)의 기록 회로(1518)에 전송된 제2암호화 컨텐츠(1517)는, 예로서, 널리 공지된 8/16 변조 시스템을 기록 회로(1518)에 사용하여 변조되고, 이어서, 변조된 신호가 광 픽업(도면에 나타내지 않음)에 의해서 광 디스크(1101) 상의 사용자 데이터 영역(1103)에 기록된다. 광 디스크(1101)에 암호화되어 기록된 상기 컨텐츠를 재생할 때, 광 픽업으로부터 출력되는 레이저 빔이 상기 암호화된 컨텐츠가 기록되어 있는 광 디스크(1101)상의 영역을 조사하여, 반사광이 광 픽업에 입력된다. 상기 광 픽업이 입력된 반사광을 재생 전기 신호로 광전 변환한 후에, 광전 변환된 재생 신호는 데이터 재생부(1519)에 출력된다. 데이터 재생부(1519)는 입력된 재생 신호를 디지털 재생 신호로 A/D 변환하고, 이어서, 디지털 재생 신호는 제2암호 디코더(1520)에 출력된다.

다른 한편으로는, 광 픽업(1301)으로부터 출력된 레이저 빔은 광 디스크(1101)의 BCA(1104)에 조사되어, 반사광이 광 픽업에 입력된다. 상기 광 픽업은 입력된 반사광을 재생 전기 신호로 광전 변환하고, 이어서, 광전 변환된 재생 신호가 BCA 재생 회로(1521)에 출력된다. BCA 재생 회로(1521)는 입력된 재생 신호에 따라서 디스크 ID 신호(1515)를 생성하고, 이어서, 생성된 디스크 ID 신호는 제2암호 디코더(1520)에 출력된다. 디스크 ID 신호에 응답하여, 제2암호 디코더(1520)는 입력된 디스크 ID 신호(1515)를 키로서 사용하여, 데이터 재생부(1519)로부터의 재생된 암호화 컨텐츠를 해독한다. 이 때, 컨텐츠가 광 디스크(1101)에 합법적으로 기록되는 경우에, 광 디스크(1101)에 기록된 암호화된 컨텐츠를 해독하는 키는 광 디스크(1101)의 디스크 ID이고, BCA 재생 회로(1521)로부터 출력되는 디스크 ID 신호도 또한 광 디스크(1101)의 디스크 ID 신호(BCAS)이므로, 제2암호 디코더(1520)는 암호 해독 처리 과정을 정상적으로 실행할 수 있다. 따라서, 암호 해독되거나 또는 디스크램블된 컨텐츠 데이터가 출력 신호(1525)로서 제2암호 디코더(1520)로부터 출력된다. 이 경우에, 제2암호 디코더(1520)의 암호 해독 처리 과정을 이하의 식으로 표시할 수 있다. 데이터 컨텐츠가 영상 신호일 때, 제2암호 디코더(1520)는, 예로서, MPEG 신호를 확장하여, 원시 영상 신호를 재생하고, 이어서 영상 신호를 출력한다.

C [BCAS] # BCAS = C (7)

상기 광 디스크(1101)는 디스크 ID 신호(BCAS)(1515)만을 사용하여 암호화되어 있으므로, BCA 재생 회로(1521)와 제2암호 디코더(1520)를 포함하는 임의의 광 디스크 기록 및 재생장치로써 컨텐츠 데이터를 재생할 수 있다. 상기 실시예에서, 암호화 인코더(1504 및 1516)는 암호화를 실행하고, 암호 디코더(1513 및 1520)는 암호 해독을 실행하지만, 각각의 장치(1501, 1506 및 1514) 내의 제어부인 CPU에 의해서 실행되는 프로그램에 암호화 알고리즘 및 암호 해독 알고리즘용의 프로그램이 포함되어 있는 구성으로써 암호화 및 암호 해독이 실행될 수도 있다.

본 바람직한 실시예에서는, CATV 디코더(1506)의 제2암호 인코더(1516)가 제2암호 키로서 디스크 ID 신호(1515)를 사용하여 컨텐츠를 암호화하지만, 컨텐츠는 이하와 같이 암호화될 수도 있다. 예로서, 각각의 CATV 회사 장치(1501) 용으로 준비된 IC 카드(1522)를 CATV 디코더(1506)에 장착할 수도 있고, 또한 IC 카드(1522)의 회사 식별 신호 메모리(1523) 내에 기록된 회사 식별 신호와, BCA 재생 회로(1521)에 의해서 재생된 디스크 ID 신호(BCAS)를 조합하여, 제2암호 인코더(1516)에서 컨텐츠를 암호화하기 위한 제2암호 키로서 사용할 수도 있다. 제1암호 디코더(1513)로부터의 출력 신호인 컨텐츠를 C로 표시하고, 제1의 제2암호 키인 디스크 ID 신호(1515)를 BCAS로 표시하고, 제2의 제2암호 키인, 회사 식별 신호(1523)를 CK로 표시하고, 또한 제2암호화 컨텐츠(1517)를 C[BCAS, CK]로 표시한다. 이어서, 제2암호 인코더(1516)의 암호화 처리 과정은 이하의 식으로 표시된다.

C * BCAS * CK = [BCAS, CK] (8)

후속해서, 광 디스크(1101)에 암호화되어 기록된 컨텐츠를 재생할 때, 광 픽업으로부터 출력되는 레이저 빔은 상기 암호화된 컨텐츠가 기록되어 있는 광 디스크(1101)상의 영역을 조사하여, 반사광이 광 픽업에 입력된다. 광 픽업은 입력된 반사광을 재생 신호로 광전 변환하고, 이어서, 이 재생 신호는 데이터 재생부(1519)에 출력된다. 데이터 재생부(1519)는 입력된 재생 신호를 디지털 재생 신호로 A/D 변환하고, 이어서, 디지털 재생 신호는 제2암호 디코더(1520)에 출력된다. 다른 한편으로는, 광 픽업으로부터 출력된 레이저 빔은 광 디스크(1101)의 BCA(1104)에 조사되어, 반사광이 광 픽업에 입력된다. 광 픽업은 입력된 반사광을 재생 신호로 광전 변환하고, 재생 신호가 BCA 재생 회로(1521)에 출력된다. BCA 재생 회로(1521)는 입력된 재생 신호에 따라서 디스크 ID 신호(1515)를 재생하고, 이어서, 디스크 ID 신호(1515)는 제2암호 인코더(1516)와 제2암호 디코더(1520)에 출력된다.

또한, 광 디스크 기록 및 재생장치(1514)에 장착된 IC 카드(1524)의 회사 식별 신호 메모리(1526)에 저장된 회사 식별 신호는 제2암호 디코더(1520)에 입력된다. 회사 식별 신호는, IC 카드(1524)의 회사 식별 신호 메모리(1526) 내에 기록되어 있지 않을 수도 있고, 예로서, 광 디스크 기록 및 재생장치(1514)의 기록 프로그램의 설치시에, 회사 식별 신호를 광 디스크 기록 및 재생장치(1514)의 제어부의 CPU에 접속된 메모리(도면에 나타내지 않음)에 기록할 수도 있다. 또 다른 방법으로는, 회사 식별 신호를 광 디스크 기록 및 재생장치(1514)의 키보드(도면에 나타내지 않음)를 사용하여 입력할 수도 있다.

제2암호 디코더(1520)는 입력된 디스크 ID 신호(1515)와 회사 식별 신호를 암호 해독 키로서 사용하여, 암호화 컨텐츠를 해독한다. 이 때, CATV 디코더(1506)의 사용자가 CATV 회사 장치(1501)를 보유한 특정 CATV 회사와 공식적으로 계약하고, 또한 컨텐츠(1502)가 광 디스크(1101)에 합법적으로 기록되어 있는 경우에, 광 디스크(1101)에 암호화되어 기록된 암호화 컨텐츠에 대한 제1암호 해독 키는 바로 이 때 재생되는 광 디스크(1101)의 디스크 ID 신호(BCAS)이고, 또한 제2암호 해독 키는 계약한 CATV 회사로부터 공급된 IC 카드(1524)의 회사 식별 신호 메모리(1526)에 저장된 회사 식별 신호(CK)이다. 따라서, 디코딩되거나 또는 디스크램블된 컨텐츠 데이터의 출력 신호(1525)가 제2암호 디코더(1520)로부터 출력된다. 이 경우에, 제2암호 디코더(1520)의 암호 해독 처리 과정은 이하의 식으로 표시된다. 컨텐츠가 영상 신호일 때, 예로서, MPEG 신호는 제2암호 디코더(1520)에 의해서 확장되고, 이어서, 영상 신호인 출력 신호(1525)가 출력된다.

C [BCAS, CK] # (BCAS * CK) = C (9)

상기 광 디스크(1101)의 컨텐츠는 디스크 ID 신호(1515)와 회사 식별 신호를 사용하여 암호화되어 있으므로, 상기 컨텐츠를 공급하는 CATV 회사와 계약이 성립되면, BCA 재생 회로(1521)와 제2암호 디코더(1520)를 포함하는 임의의 광 디스크 기록 및 재생장치로써 재생을 실행할 수 있다. 반대로, 상기 CATV 회사와 계약이 성립되어 있지 않으면, 회사 식별 신호를 취득할 수 없고 컨텐츠를 재생할 수 없으며, 이로 인하여 계약 사용자와 비계약 사용자를 구별할 수 있게 된다.

또한, 본 바람직한 실시예에서는, 각각의 사용자가 광 디스크 기록 및 재생장치(1514)로부터 자신의 집에 위치한 CATV 디코더(1506)에 디스크 ID 신호를 전송하여 영상 데이터 등을 암호화하므로, CATV 장치(1501)는 각각의 사용자에게 개

별적으로 전달된 암호화된 컨텐츠를 변경할 필요가 없고, 따라서, 방송 시스템을 단순화할 수 있어서 동일한 컨텐츠를 낮은 비용으로 다수의 사용자에게 제공할 수 있다. 또한, 본 바람직한 실시예에 의하면, CATV 디코더(1506)를 보유한 각각의 사용자에 대하여 다만 하나의 RAM 타입 광 디스크에의 기록이 허용된다.

본 바람직한 실시예에서는, 케이블 텔레비전 시스템의 헤드 엔드(head end)로부터 컨텐츠가 전송되는 경우를 설명하였지만, 본 발명은 이 것에 한정되지 않고 무선파를 사용하는 방송에 적용될 수 있다.

(바람직한 제5실시예)

본 발명에 의한 바람직한 제5실시예의 암호화된 컨텐츠의 기록 및 재생 방법을 도면을 참조로 하여 설명한다. 도 21은 본 발명에 의한 바람직한 제5실시예의 광 디스크(1601)의 데이터 기록 영역을 나타내는 평면도이고, 도 22는 바람직한 제4실시예에 의한 광 디스크 기록 및 재생 시스템의 구성을 나타내는 블록도이다. 바람직한 제5실시예에서, 바람직한 제3실시예 및 제4실시예에 공통인 구성 요소의 설명은 이하의 설명에서 생략한다.

도 21을 참조하면, 1601은 재기록 가능 방식 또는 재기록 불가능 방식 광 디스크 중 어느 하나인 기록 방식의 광 디스크를 나타내고, 1602는 디스크 정보가 요철(凹凸) 홈의 형태로 기록되는 제어 사용자 데이터 영역을 나타내고, 1603은 사용자가 광 디스크에 레이저 광 빔을 조사함으로써 데이터를 기록하는 사용자 데이터 영역을 나타내고, 또한 1604는 디스크 ID가 기록되는 BCA를 나타낸다.

BCA(1604)에는, YAG 레이저 등 펄스 레이저를 사용하여, 제어 사용자 데이터 영역(1602)의 내주부의 요철 홈 위의 기록막을 부분적으로 트리밍함으로써, 복수의 트리밍 영역(1606)이 반경 방향으로 연장되는 형태로 형성된다. 트리밍은 디스크 제조자가 실행한다. 또한, BCA(1604)에 기록되는 데이터에 디스크 ID를 부가함으로써, 광 디스크의 관리가 용이하게 실시될 수 있다. 또한, 요철 홈에 BCA(1604)의 데이터를 기록함으로써, BCA(1604)에 기록되는, 광 디스크를 식별하는 정보가 쉽게 왜곡되는 것을 방지할 수 있다.

추가로, 제어 사용자 데이터 영역(1602)과 BCA(1604)를 서로 인접하게 배치함으로써, 제어 사용자 데이터 영역의 데이터가 재생되면 BCA(1604)의 데이터가 연속적으로 재생될 수 있거나, 또는 BCA(1604)의 데이터가 재생되면 제어 사용자 데이터 영역의 데이터가 연속적으로 재생될 수 있으므로, 예로서, 광 디스크가 시동될 때 CPU가 광 디스크를 신속하게 식별하기 위한, BCA(1604)의 정보를 취득하고 또한 암호화된 컨텐츠를 기록하는 처리 과정을 앞당길 수 있게 된다.

본 바람직한 실시예의 BCA(1604)는 제어 사용자 데이터 영역(1602)의 내주부에 요철 홈 형태로 기록막을 트리밍함으로써 형성되지만, 재기록 가능 방식의 광 디스크 또는 재기록 불가능 방식의 광 디스크 중 어느 하나인, 기록 방식의 광 디스크를 구성하는 기록막은 판독 전용 광 디스크 상에 형성된 기록막에 비하여 열에 의해서 쉽게 영향을 받는다. 제어 사용자 데이터 영역(1602)의 내주부를 트리밍함으로써, 사용자 데이터 영역(1603)의 기록 데이터는 외주부가 트리밍되는 경우에 비해서 트리밍시에 발생되는 열로부터 보호된다. BCA(1604)를 제어 사용자 데이터 영역(1602)의 내주측에 형성하는 이유는, 레이저 장치의 집속 서보 회로의 불안정성 때문에 레이저 빔의 빔 스폿의 직경이 변동할 때, 여유를 고려하기 때문이다.

트리밍 전에 BCA(1604)에 기록된 데이터는 제어 사용자 데이터 영역(1602)에 기록될 수도 있다. BCA(1604)에 기록된 데이터는 제어 사용자 데이터 영역(1602)에 기록될 수 있어서, 제어 사용자 데이터 영역(1602)의 상기 데이터가 트리밍시에 보호될 수 있다.

또한, 상기 데이터가 BCA(1604)로부터 제어 사용자 데이터 영역(1602)에 연속적으로 또한 반복적으로 기록되어 있는 경우에는, 제어 사용자 데이터 영역(1602)에서 상기 데이터를 탐색함으로써 BCA(1604)의 위치를 예측할 수 있다. 또한, 사용자 데이터 영역(1603)의 기록에 동일한 방법으로 광 빔을 조사함으로써 키 정보 기록 영역(1605)의 데이터가 기록된다.

본 바람직한 실시예의 방법에 유사한 방법으로, 제어 사용자 데이터 영역(1602)과 키 정보 기록 영역(1605)을 서로 인접하게 배치함으로써, 제어 사용자 데이터 영역(1602)의 데이터가 재생되면 키 정보 기록 영역(1605)의 데이터가 연속적으로 재생될 수 있거나, 또는 키 정보 기록 영역(1605)의 데이터가 재생되면 제어 사용자 데이터 영역(1602)의 데이터가 연속적으로 재생될 수 있으므로, 예로서, 광 디스크가 시동될 때 CPU가 광 디스크를 신속하게 식별하기 위한, BCA(1604)의 정보를 취득하고 또한 암호화된 컨텐츠를 재생하는 처리 과정을 앞당길 수 있게 된다.

도 22를 참조하면, 바람직한 제5실시예에 의한 광 디스크 기록 및 재생 시스템은, CATV 회사의 장치(1701), 키 발행 센터 장치(1707), CATV 디코더(1706), 광 디스크 기록 및 재생장치(1714), 및 텔레비전 세트(1730)를 포함한다. 이 경우에,

CATV 회사 장치(1701)는 영화 소프트웨어 등 컨텐츠를 저장하는 컨텐츠 메모리(1702), 제1암호 키를 저장하는 제1암호 키 메모리(1703), 및 제1암호 인코더(1704)를 포함한다. 또한, CATV 디코더(1706)는 시스템 ID 메모리(1708), 제1암호 디코더(1713), 현재의 시간 정보를 출력하는 클록 회로(1725)를 포함한다. 또한, 키 발행 센터 장치(1707)는 장치(1707)의 동작을 제어하는 제어부(1707a), 및 시간 제한 정보 메모리(1710)를 포함한다. 추가로, 광 디스크 기록 및 재생장치(1714)는 기록 회로(1717), 키 정보 기록 회로(1719), BCA 재생 회로(1720), 데이터 재생부(1721), 제2암호 디코더(1722), 및 키 정보 재생부(1723)를 포함한다.

우선, CATV 회사 장치(1701)의 제1암호 인코더(1704)는 제1암호 키(1703)를 사용하여, 컨텐츠 메모리(1702)에 저장된 영화 소프트웨어 등 컨텐츠 데이터를 암호화하여, 제1암호화 컨텐츠(1705)를 생성하고, 생성된 제1암호화 컨텐츠(1705)를 네트워크를 통하여 각각의 사용자의 CATV 디코더(1706)의 제1암호 디코더(1713)에 송신한다. 컨텐츠 메모리(1702)에 저장된 컨텐츠를 C로서 표시하고, 제1암호 키 메모리(1703)에 저장된 제1암호 키를 FK로서 표시하고, 또한 제1암호화 컨텐츠(1705)를 C[FK]로서 표시하면, 이하의 식을 표시할 수 있다.

C * FK = C [FK] (10)

CATV 디코더(1706)는 네트워크를 통하여 키 발행 센터 장치(1707)의 제어부(1707a)에, CATV 디코더(1706)의 시스템 ID 메모리(1708)에 저장된 시스템 ID, 및 사용자가 시청하기를 희망하고, 또한, 예로서, 키보드(도면에 나타내지 않음)를 사용하여 타이틀 코드(1709)가 입력되는, 상기 컨텐츠의 타이틀 코드(1709)를 송신한다. 상기 타이틀 코드(1709)는 텔레비전 세트(1730)의 스크린에서 선택하여 입력하거나, 또는 키보드를 사용하여 직접 입력하거나, 또는 원격 제어기 등으로부터 입력할 수도 있다. 따라서, 타이틀 코드는 사용자가 자기 자신의 방법으로 취득하거나, 또는 제1암호화 컨텐츠와 함께 CATV 디코더(1706)로부터 송신되거나, 또는 프로그램 가이드 등의 형태로 제1암호화 컨텐츠의 시간과 상이한 시간에 미리 송신될 수도 있다.

CATV 디코더(1706)의 시스템 ID와 상기 컨텐츠의 타이틀 코드에 따라서, 키 발행 센터 장치(1707)의 제어부(1707a)는, 시간 제한 정보 메모리(1710)에 저장된 해당 시간 제한 정보를 참조하여, 대응하는 키(K)(1712)를 생성하고, 이어서, 생성된 키(K)(1712)를 네트워크를 통하여 CATV 디코더(1706)의 제1암호 디코더(1713)에 송신한다. 시간 제한 정보는 동일한 컨텐츠가 상이한 시간에 복수 회 방송되는 경우를 구별할 수 있게 한다. 제1암호 키를 FK로서 표시하고, CATV 디코더(1706)의 시스템 ID를 DID로서 표시하고, 시간 제한 정보를 TIME으로서 표시하고, 또한 컨텐츠의 타이틀 코드를 T로서 표시하면, 키(K)(1712)는 이하의 식으로 표시되는 관계를 만족시킨다.

FK = K * T * DID * TIME (11)

제1암호 키(FK), 키 발행 센터 장치(1707)로부터 송신된 상기 키(K)(1712), 상기 컨텐츠의 타이틀 코드, 시스템 ID, 및 시간 제한 정보가 상기 관계를 만족시키고, 또한 시간 제한 정보가 클록 회로(1725)로부터 출력된 현재 시간 정보의 조건을 만족시키면, 제1암호 디코더(1713)는 제1암호화 컨텐츠(1705)를 해독한다. 이 경우에, 제1암호화 컨텐츠(1705)가 영상 신호일 때, 디스크램블된 영상 신호는 제1암호 디코더(1713)로부터 텔레비전 세트(1730)에 출력되어서, 사용자는 텔레비전 세트(1730)에서 컨텐츠를 시청할 수 있다. 이 경우에, 제1암호 디코더(1713)의 암호 해독 처리 과정은 이하와 같이 표시된다.

C [FK] # (K * T * DID * TIME)

= C [FK] # FK

= C (12)

후속해서, 광 디스크(1601)에 상기 컨텐츠를 기록하는 방법을 설명한다. 광 디스크(1601)에 컨텐츠를 기록할 때, CATV 디코더에 의해서 해독되지 않은 제1암호화 컨텐츠(1705)는 CATV 회사 장치(1701)의 제1암호 인코더(1704)로부터 광 디스크 기록 및 재생장치(1714)의 기록 회로(1717)에 송신된다. 기록 회로(1717)는 널리 공지된 8/16 변조 시스템을 사용하여, 수신된 제1암호화 컨텐츠(1705)를 디지털 변조하고, 변조된 디지털 데이터는 광 픽업(도면에 나타내지 않음)에 의해서 광 디스크(1601)에 기록된다. 따라서, 광 디스크(1601)에 암호화되어 기록된 상기 컨텐츠를 재생하기 위해서는, 제1암호화 컨텐츠(1705)를 해독할 필요가 있다.

광 디스크 기록 및 재생장치(1714)는, BCA 재생 회로(1720)에 의해서 재생된 광 디스크(1601)의 디스크 ID 신호(1715), 및 예로서, 키보드를 사용하여 입력되고 또한 사용자가 재생하기를 희망하는 상기 컨텐츠의 타이틀 코드(1716)를 네트워

크를 통하여 키 발행 센터 장치(1707)의 제어부(1707a)에 송신한다. 디스크 ID를 송신하는 타이밍에 대해서는, 키 발행 센터 장치(1707)에 액세스하였을 때 디스크 ID를 송신하거나, 또는 컨텐츠를 시청할 때 타이틀 코드와 함께 디스크 ID를 송신할 수도 있다.

디스크 ID 송신 방법으로서, 도 22에 나타낸 바와 같이, 광 디스크(1601)의 BCA(1604)를 재생함으로써 출력 신호를 BCA 재생 회로(1720)로부터 키 발행 센터 장치(1707)에 직접 송신하는 방법이 상기에 개시되어 있지만, 본 발명은 이 것에 한정되지 않고, 이하의 방법을 사용할 수도 있다. 예로서, 디스크를 시동할 때 키 발행 센터 장치(1707)에의 액세스 전에 BCA(1604)의 데이터를 재생하여, BCA(1604)의 데이터를 광 디스크 기록 및 재생장치(1714) 또는 CATV 디코더(1706)의 메모리(도면에 나타내지 않음)에 저장하고, 이어서, 상기 타이밍에 키 발행 센터 장치(1707)의 제어부(1707a)에 송신한다. 또한, 디스크 ID가 라벨(label) 등 어떤 형태로 시각적으로 인식될 수 있을 때, 디스크 ID를 입력하는 데에 키보드를 사용할 수도 있다. 라벨이 바코드일 때, 디스크 ID를 판독하는 데에 바코드 리더(reader)를 사용할 수도 있다.

키 발행 센터 장치(1707)의 제어부(1707a)는 광 디스크(1601)의 디스크 ID 신호(1715)와 컨텐츠의 타이틀 코드(1716)에 대응하는 키(DK)(1718)를 생성하고, 생성된 키(DK)(1718)를 광 디스크 기록 및 재생장치(1714)의 키 정보 기록 회로(1719)에 송신한다. 이 경우에, 제1암호 해독 키를 FK로서 표시하고, 광 디스크(1601)의 디스크 ID 신호(1715)를 BCAS로서 표시하고, 컨텐츠의 타이틀 코드(1716)를 T로서 표시하면, 키(DK)는 이하의 식의 관계를 만족시킨다.

FK = DK * BCAS * T (13)

광 디스크 기록 및 재생장치(1714)의 키 정보 기록 회로(1719)에 입력된 키(DK)는 널리 공지된 8/16 변조 시스템 등 변조 시스템을 사용하여 디지털 변조되고, 이어서, 변조된 디지털 데이터는 광 픽업(도면에 나타내지 않음)에 의해서 광 디스크(1601) 상의 키 정보 기록 영역(1605)에 기록된다. 키(DK)는 키 정보 기록 영역(1605)에 복수 회 기록될 수도 있다. 동일한 키를 복수 회 기록함으로써, 키 정보 기록 영역(1605)의 기록막이 열화(劣化)된 경우 또는 광 디스크(1601)가 긁혔을 때, 키(DK)가 보호되어서, 키(DK) 중 어느 하나의 데이터가 재생될 때에만 컨텐츠가 해독될 수 있다.

본 바람직한 실시예에서, 키 정보 기록 영역(1605)은 사용자 데이터 영역(1603)의 내주측에 구성되어 있지만, 이것은 사용자 데이터 영역(1603)의 외주측에 구성될 수도 있고, 또는 내주측 및 외주측 모두에 구성될 수도 있다. 키 정보 기록 영역(1605)을 외주측에 구성함으로써, 더 많은 키(DK)를 기록할 수 있게 된다. 또한, 복수의 키 정보 기록 영역을 분산해서 구성함으로써, 하나의 키 정보 기록 영역이 재생될 수 없는 경우에도 키(DK)는 기타의 키 정보 기록 영역에 의해서 보호될 수 있다.

다른 한편으로, 광 픽업으로부터 출력되는 레이저 빔은 상기 컨텐츠가 기록되어 있는 광 디스크(1601) 상의 영역을 조사하여, 반사광이 광 픽업에 입력된다. 광 픽업은 입력된 반사광을 재생 전기 신호로 광전 변환하고, 광전 변환된 재생 신호는 데이터 재생부(1721)에 출력된다. 이에 따라서, 데이터 재생부(1721)는 입력된 재생 신호를 암호화된 디지털 데이터로 A/D 변환하고, 이어서, 암호화된 디지털 데이터는 제2암호 디코더(1722)에 출력된다. 또한, 광 픽업으로부터 출력된 레이저 빔은 광 디스크(1601)의 BCA(1604)에 조사되고, 이어서, 반사광이 광 픽업에 입력된다. 광 픽업은 입력된 반사광을 재생 전기 신호로 광전 변환하고, 광전 변환된 재생 신호는 BCA 재생 회로(1720)에 출력된다. 이에 응답하여, BCA 재생 회로(1720)는 입력된 재생 신호에 따라서 디스크 ID 신호(1715)를 재생하고, 재생된 디스크 ID 신호는 암호 디코더(1722)에 출력된다. 또한, 광 픽업으로부터 출력된 레이저 빔은 광 디스크(1601)의 키 정보 기록 영역(1605)에 조사되어, 반사광이 광 픽업에 입력된다. 광 픽업은 입력된 반사광을 재생 전기 신호로 광전 변환하고, 재생 신호를 키 정보 재생부(1723)에 출력한다. 이에 따라서, 키 정보 재생부(1723)는 입력된 재생 신호에 따라서 키(DK) 데이터를 생성하고, 키(DK) 데이터는 제2암호 디코더(1722)에 출력된다.

키 발행 센터 장치(1707)에 액세스한 바로 직후에 컨텐츠를 재생하는 경우에, 키 정보 기록 회로(1719)는, 동일한 키(DK)를 키 정보 기록 영역(1605)에 기록하기 전에, 키(DK)를 제2암호 디코더(1722)에 직접 입력할 수도 있다. 이렇게 함으로써, 재생이 개시될 때까지의 시간을 단축할 수 있다. 암호 디코더(1722)는 입력된 디스크 ID 신호(1715), 키(DK), 및 상기 컨텐츠의 타이틀 코드(1716)를 포함하는 암호 해독 키를 사용하여, 암호화된 컨텐츠를 해독한다. 제2암호 디코더(1722)의 암호 해독 처리 과정은 이하의 식으로 표시된다. 컨텐츠가 영상 신호일 때, 예로서, MPEG 신호가 확장되어서 영상 신호인 출력 신호(1724)가 제2암호 디코더(1722)로부터 출력된다.

C [FK] # (DK * BCAS * T)

= C [FK] # FK

= C (14)

본 바람직한 실시예에서, 키 발행 센터 장치(1707)의 제어부(1707a)로부터 키 신호가 수신되어 사용자 요금이 부과될 때, 요금은 컨텐츠를 시청할 때 및 광 디스크(1601)에 기록된 컨텐츠를 처음 재생할 때 별도로 부과되고, 이로 인하여 컨텐츠 데이터를 광 디스크(1601)에 기록만 하는 경우에는 요금 부과를 제외한다. 따라서, 시청 및 광 디스크(1601)에의 기록 모두에 대하여 요금이 한 번 부과되는 경우에 비하여,

(a) 컨텐츠를 시청하기를 희망하지만, 컨텐츠 데이터를 광 디스크(1601)에 기록할 필요가 없는 사용자에 대하여, 또는

(b) 컨텐츠 데이터를 광 디스크(1601)에 기록하기를 희망하지만, 방송시에 컨텐츠를 시청할 필요가 없는 사용자에 대하여, 부과 요금을 낮출 수 있게 된다.

또한, 광 디스크(1601)에 기록하는 것만으로는 요금이 부과되지 않으므로, 사용자는 시청후에 다시 시청하기 위하여 광 디스크(1601)를 재생하는 키를 수신할 것인가 아닌가를 결정할 수 있다. 상기의 바람직한 실시예에서는, 네트워크를 통하여 키 발행 센터 장치(1707)의 제어부(1709a)로부터 키(DK)를 수신하는 방법을 사용하지만, 본 발명은 이것에 한정되지 않으며, 컨텐츠의 타이틀 및 디스크 ID 번호가 전화 등으로 구두로 전달될 수도 있고, 또한, 구두로 수신된 후에 키보드를 사용하여 입력할 수도 있다.

후속해서, 키 정보 기록 영역(1605)에 키(DK)가 기록되어 있는 광 디스크(1601)를, 키 발행 센터 장치(1707)로의 액세스가 완료된 후에, 재생하는 경우를 설명한다. 우선, 광 픽업으로부터 출력되는 레이저 빔은 상기 컨텐츠가 기록되어 있는 광 디스크(1601)의 영역을 조사하고, 이어서, 반사광은 광전 변환을 실행하는 광 픽업을 통하여 데이터 재생부(1712)에 입력된다. 이에 응답하여, 데이터 재생부(1712)는 암호화된 컨텐츠 데이터를 제2암호 디코더(1722)에 출력한다. 다른 한편으로는, 광 픽업으로부터 출력되는 레이저 빔은 광 디스크(1601)의 BCA(1604)에 조사되고, 반사광은 광전 변환을 실행하는 광 픽업을 통하여 BCA 재생 회로(1720)에 입력된다. 이에 응답하여, BCA 재생 회로(1720)는 입력된 재생 신호에 따라서 디스크 ID 신호(1715)를 생성하고, 이어서, 이 디스크 ID 신호(1715)는 제2암호 디코더(1722)에 출력된다.

또한, 광 픽업으로부터 출력된 레이저 빔은 광 디스크(1601)의 키 정보 기록 영역(1605)에 조사되고, 반사광은 광전 변환을 실행하는 광 픽업을 통하여 키 정보 재생부(1723)에 입력된다. 이에 따라서, 키 정보 재생부(1723)는 입력된 재생 신호에 따라서 키(DK) 데이터를 생성하고, 키(DK) 데이터는 제2암호 디코더(1722)에 출력된다. 제2암호 디코더(1722)는 입력된 디스크 ID 신호(1715), 키(DK), 및 상기 컨텐츠의 타이틀 코드(1716)를 포함하는 암호 해독 키를 사용하여, 데이터 재생부(1721)로부터 출력된 암호화된 컨텐츠를 해독한다. 제2암호 디코더(1722)의 디코딩 처리 과정은 이하의 식으로 표시된다. 컨텐츠가 영상 신호일 때, 예로서, MPEG 신호가 확장되고, 확장된 MPEG 신호인 영상 신호가 제2암호 디코더(1722)로부터 출력된다.

C [FK] # (DK * BCAS * T)

= C [FK] # FK

= C (15)

키 정보 기록 영역(1605)에 키(DK) 데이터를 한 번 기록함으로써, 상기 암호화된 컨텐츠는 키 발행 센터 장치(1707)로의 아무런 액세스없이 항상 재생될 수 있다. 또한, 암호 해독 처리 과정에 필요한 모든 암호 해독 키가 광 디스크(1601)에 기록되어 있으므로, 상기 광 디스크(1601)는, BCA 재생 회로(1720), 키 정보 재생부(1723) 및 제2암호 디코더(1722)를 포함하는 임의의 광 디스크 기록 및 재생장치에 의해서 재생될 수 있다.

또한, 상기 암호화된 컨텐츠를, 상이한 디스크 ID를 갖는 광 디스크(1601)에 복사한 후에 재생하려고 하는 경우에, 상기 광 디스크(1601)의 디스크 ID에 상이한 디스크 ID 신호가 BCA 재생 회로(1720)로부터 출력되므로, 암호화된 컨텐츠는 해독될 수 없고, 이로 인하여 컨텐츠가 복사된 후에 재생되는 것이 방지된다. 그러나, 이 경우에도, 컨텐츠의 타이틀 및 디스크 ID를 네트워크를 통하여 또는 구두로 키 발행 센터에 전달함으로써, 요금이 부과된 후에 암호 해독 키를 수신할 수도 있다. 이러한 방법으로, 암호화 컨텐츠가 또 다른 광 디스크(1601)에 복사되더라도, 어떠한 컨텐츠도 불법적으로 재생될 수 없고, 암호화 컨텐츠가 복사되어 있는 광 디스크를 재생할 때 요금이 항상 부과되어서, 컨텐츠에 대한 저작권이 보호된다.

도 23은 바람직한 제5실시예에 의한 ID 부가 테이블의 구성을 나타내는 테이블이고, 이 테이블은 상이한 시스템 ID 및 상이한 디스크 ID에 대하여, 재구성된 형태로 제1암호 디코더(1713)에 입력되는 키(K), 및 키 정보 기록 회로(1719)에 입력되는 키(DK)를 나타낸다.

도 23을 참조하면, T1, T2 및 T3은 상이한 컨텐츠에 대한 타이틀 코드를 나타내고, FK1, FK2 및 FK3은 각각 T1, T2 및 T3의 타이틀 코드를 갖는 암호화된 컨텐츠를 디코딩하는 암호 해독 키를 나타낸다. DID1, DID2 및 DID3은 상이한 CATV 디코더(1706)에 대한 시스템 ID를 나타내고, BCAS1, BCAS2 및 BCAS3은 상이한 광 디스크(1601)에 대한 디스크 ID를 나타낸다. 이 경우에, CATV 디코더(1706)에 입력되는 키(Kmn)는 이하의 식을 만족시키도록 결정된다.

$$FKn = Kmn * Tn * DID * TIMEn \quad (16)$$

또한, 광 디스크 기록 및 재생장치(1714)에 입력되는 키(DKmn)는 이하의 식을 만족시키도록 결정된다.

$$FKn = DKmn * BCAm * Tn \quad (17)$$

도 23에 나타낸 바와 같이, 상이한 컨텐츠의 경우뿐만 아니라 동일한 컨텐츠의 경우에도, 각각의 상이한 CATV 디코더(1706)에 대하여, 또한 각각의 상이한 광 디스크에 대하여, 또한 각각의 상이한 방송 시간에 대하여, 키 발행 센터 장치(1707)로부터 취득되는 키 정보는 서로 상이하도록 설정되어서, 이로 인하여 저작권을 상세하게 보호하게 된다. 동일한 방법으로, 동일한 컨텐츠에 경우에도 시스템 ID, 디스크 ID 및 시간 정보가 서로 상이하면 키 정보가 상이하므로, CATV 회사 장치(1701)는 각각의 사용자에 대하여 암호화 컨텐츠를 변경할 필요가 없고, 따라서, 하나의 컨텐츠에 대하여 하나의 암호화 컨텐츠를 준비하면 된다. 그러므로, 방송 시스템을 단순화할 수 있어서 컨텐츠를 낮은 비용으로 다수의 사용자에게 제공할 수 있다.

본 바람직한 실시예에서는, 케이블 텔레비전의 헤드 엔드로부터 컨텐츠를 방송하는 경우를 설명하였지만, 본 발명은 무선파를 사용하는 방송에 적용될 수 있다.

바람직한 제3실시예 내지 제5실시예의 유리한 효과

본 바람직한 실시예에 의한 광 디스크는 (a) 제1디스크 정보를 기록하는 제1정보 영역, (b) 개별 디스크를 식별하는 제2디스크 정보를 기록하는 제2정보 영역, 및 (c) 사용자 데이터 영역에 광 빔을 조사함으로써 정보 기록이 가능한 사용자 데이터 영역을 포함한다. 따라서, 종래 기술에 의한 광 디스크에 광 디스크를 식별하는 상기 정보를 부가함으로써, 광 디스크의 관리를 용이하게 실시할 수 있다. 이 경우에, 상기 제2정보 영역은 상기 제1정보 영역에 기록되는 것이 바람직하고, 또한 상기 제2정보 영역은 광 픽업으로써 상기 제1정보 영역을 재생함으로써 재생될 수 있다. 상기 제2정보 영역에는, 상기 제1정보 영역 내의 기록막을 부분적으로 제거하여 반경 방향으로 연장되는 형태를 갖는 복수의 트리밍 영역이 형성됨으로써 제2정보 데이터가 기록되고, 이로 인하여 상기 제2디스크 정보가 쉽게 왜곡되는 것을 방지할 수 있다.

본 바람직한 실시예의 암호화 컨텐츠를 기록하는 방법에 의하면, (a) 제1디스크 정보를 기록하는 제1정보 영역, (b) 개별 디스크를 식별하는 제2디스크 정보를 기록하는 제2정보 영역, 및 (c)사용자 데이터 영역에 광 빔을 조사함으로써 정보가 기록되는 사용자 데이터 영역을 포함하는 광 디스크의 사용자 데이터 영역에 컨텐츠 데이터를 기록하는 경우, 컨텐츠 데이터가 암호화되고 암호화된 데이터가 기록되어서, 컨텐츠 데이터는 최소한 상기 제2디스크 정보를 이용하는 연산 또는 계산에 의해서 암호 해독되어서 재생될 수 있다. 따라서, 하나의 특정 광 디스크에 유일하게 존재하는 광 디스크의 식별 정보를 사용하여 컨텐츠를 암호화함으로써, 컨텐츠의 불법적인 복사가 방지되어서 저작권을 보호할 수 있는 고유의 유리한 효과가 있다.

본 바람직한 실시예에 의한 광 디스크는 사용자 데이터 영역 내에 암호화되어 기록된 컨텐츠를 해독하는 키 정보를 기록하는 키 정보 기록 영역을 구비하고 있다. 따라서, 암호화되어 기록된 컨텐츠를 해독하는 키 정보를 필요로 하는 시스템에서, 키 정보 기록 영역에 키 정보를 한 번 기록한 후에 재생할 때마다 매번 키 정보를 입력할 필요가 없는 고유의 유리한 효과가 있다.

또한, 본 바람직한 실시예의 암호화 컨텐츠를 기록하는 방법에 의하면, (a) 제1디스크 정보를 기록하는 제1정보 영역, (b) 개별 디스크를 식별하는 제2디스크 정보를 기록하는 제2정보 영역, (c) 사용자 데이터 영역에 광 빔을 조사함으로써 정보가 기록되는 사용자 데이터 영역, 및 (d) 사용자 데이터 영역 내에 암호화되어 기록된 컨텐츠 데이터를 해독하기 위한 키 정보를 기록하는 키 정보 기록 영역을 포함하는 광 디스크의 사용자 데이터 영역에 컨텐츠를 기록하는 경우, 컨텐츠 데이

터가 암호화되고 암호화된 컨텐츠가 기록되어서, 컨텐츠 데이터는 최소한 상기 제2디스크 정보 및 상기 키 정보를 이용하는 연산에 의해서 암호 해독되고 재생될 수 있다. 따라서, 암호화 컨텐츠 데이터가 또 다른 광 디스크에 복사되더라도, 그 데이터는 불법적으로 재생될 수 없고, 암호화 컨텐츠 데이터가 복사되어 있는 광 디스크를 재생할 때마다 요금이 항상 부과되어서, 저작권이 보호된다.

이 경우에, 제1디스크 정보는 미세한 요철 홈의 형태로 형성하고, 또한 광 디스크를 식별하는 제2디스크 정보는 요철 홈에 기록하는 것이 바람직하다. 따라서, 제2디스크 정보가 왜곡되는 것을 용이하게 방지할 수 있다. 또한, 상기 제1디스크 정보와 제2디스크 정보는 서로 인접하게 형성하는 것이 바람직하다. 이 경우에, 상기 제1디스크 정보가 재생되면 제2디스크 정보가 연속적으로 재생될 수 있거나, 또는 제2디스크 정보가 재생되면 제1디스크 정보가 연속적으로 재생될 수 있으므로, 예로서, 광 디스크가 시동될 때 CPU가 디스크를 신속하게 식별하기 위한, 제2디스크 정보를 취득한 후에 암호화된 컨텐츠를 기록하는 처리 과정을 앞당길 수 있게 된다.

본 바람직한 실시예의 암호화된 데이터를 기록하는 방법에 의하면, 동일한 컨텐츠에 경우에도 각각의 상이한 시스템 ID, 각각의 디스크 ID 및 각각의 시간 정보에 대하여 키 정보가 상이하므로, CATV 회사 장치(1701)는 각각의 사용자에 대하여 암호화 컨텐츠를 변경할 필요가 없고, 이어서, CATV 회사 장치(1701)는 하나의 컨텐츠에 대하여 하나의 암호화 컨텐츠만을 준비하면 된다. 이로 인하여, 방송 시스템을 단순화할 수 있어서 컨텐츠를 낮은 비용으로 다수의 사용자에게 제공할 수 있다.

(바람직한 제3 및 제5실시예의 바람직한 변형 실시예)

도 16 및 도 21에 나타낸 바와 같이, 상기 바람직한 제3 및 제5실시예에서, 트리밍 영역(1105 및 1606)은 제어 사용자 데이터 영역(1102 및 1602) 내의 내주부에 위치한 BCA(1104 및 1604)에 각각 형성되지만, 본 발명은 이 것에 한정되지 않는다. 바람직한 제3 및 제5실시예의 바람직한 변형 실시예에 의한 광 디스크(1101a 및 1601a)의 데이터 기록 영역을 각각 설명하는 도 24 및 도 25에 나타내는 바와 같이, 트리밍 영역(1105a 및 1606a)은 제어 사용자 데이터 영역(1102 및 1602)으로부터 광 디스크의 내주측으로 돌출하도록 기록막을 트리밍함으로써 형성될 수도 있다. 말하자면, BCA(1104a 및 1604a)는 각각 제어 사용자 데이터 영역(1102 및 1602)에 포함되지 않지만, 제어 사용자 데이터 영역(1102 및 1602)의 내주측으로부터 제어 사용자 데이터 영역(1102 및 1602)의 내측으로 돌출하도록 형성되어서 배치된다. 이 바람직한 변형 실시예에서, BCA(1104a 및 1604a)를 이러한 방법으로 형성하는 이유는 레이저 장치의 집속 서보 회로의 불안정성 때문에 레이저 빔의 빔 스폿의 직경이 변동하는 경우, 여유를 고려하기 위한 것이다. 이 바람직한 변형 실시예에서, 사용자 데이터 영역(1103 및 1603)은 제어 사용자 데이터 영역(1102 및 1602)의 외측에 있으므로, 트리밍 영역(1105a 및 1606a)은 이 사용자 데이터 영역(1103 및 1603)에 기록된 데이터가 파괴되는 것을 보호하도록 배치되어 형성되어 있다.

(바람직한 제6실시예)

도 26은 본 발명의 바람직한 제6실시예에 의한, 광 디스크 내의 사용자 데이터 영역의 구성, 및 사용자 데이터 영역의 데이터로부터 암호화된 컨텐츠를 해독하는 광 디스크 재생장치의 구성을 나타내는 블록도이다. 본 바람직한 실시예에서, 광 디스크는, 예로서, DVD-RAM 등 기록 방식 광 디스크이다.

도 26에 나타낸 바와 같이, 사용자 데이터 영역(2150)은 섹터 헤더 영역(2101), 주 데이터 영역(2102), 및 오류 검출 코드(2103)를 포함한다. 섹터 헤더 영역(2101)에는, 섹터 위치를 나타내는 섹터 어드레스(2104), 및 주 데이터 영역(2102)에 기록된 데이터에 대한 저작권 제어 정보(스크램블 플래그, 복사 제어 정보 등을 포함하는)를 기록하는 저작권 제어 정보(2105)가 기록된다. 섹터 헤더 영역(2101)은 주 데이터 영역(2102)의 데이터에서 매입(埋入)되거나 또는 암호화된 암호 정보를 해독하는 암호 해독 키 영역(2106)을 포함한다. 또한, 주 데이터 영역(2102)은 암호화되지 않은 컨텐츠(2107)가 기록되는 영역, 및 암호화된 컨텐츠(2108)가 기록되는 영역으로 분할되고, 암호화되지 않은 컨텐츠(2107)는 MPEG에서의 동기 패턴 등 이후의 데이터에 대한 제어 정보 또는 모든 타입의 제어 정보를 포함한다. 또한, 암호화된 컨텐츠(2108)는 주로 암호화된 AV 데이터 등 저작권 보호를 필요로 하는 컨텐츠 데이터를 포함한다.

후속하는 주 데이터 영역(2102)을 재생하기 위한 암호 해독 키는 소정의 크기를 갖는 복수의 분할된 암호 해독 키(이하 분할된 암호 해독 키라고 함)로 분할되고, 이어서, 이 분할된 암호 해독 키는 암호 해독 키 영역(2106)에 등록된다. 예로서, 하나의 암호 해독 키 영역 4바이트에 대하여 암호 해독 키가 8바이트인 경우에, 8바이트의 암호 해독 키는 각각 4바이트인 2개의 분할된 암호 해독 키로 분할되고, 8바이트의 암호 해독 키를 각각 4바이트인 분할된 암호 해독 키로 분할한 후에 2개의 분할된 암호 해독 키가 2개의 논리적 연속 섹터의 암호 해독 키 영역(2106 및 2109)에 기록된다. 이러한 사용자 데이터 영역의 데이터를 재생할 때, 복수의 분할된 암호 해독 키는 복수의 논리적 연속 섹터(결함으로 인하여 이용 가능하지 않은 각각의 섹터는 제외된다)로부터 취득되고, 취득한 필요한 수의 분할된 암호 해독 키는 데이터 링크(link) 장치(2111)에

의해서 링크되거나 접속되어서 재생에 필요한 암호화된 암호 해독 키(8바이트)가 취득된다. 암호 해독 처리는, 암호화된 암호 해독 키(8바이트)를 취득할 수 있는 섹터의 주 데이터 영역(2102)에 기록된 데이터에 대하여, 각각의 단위의 컨텐츠의 저작권 제어 정보(2105)에 따라서, 암호 해독 장치(2114)에 의해서 실행된다.

또한, 암호화의 강도를 더욱 강화하기 위하여 암호 해독 키를 암호화할 수 있고, 또는 일정한 암호화 결과를 갖지 않도록 데이터 중의 정보인 암호 해독 키 변환 데이터를 키에 부가함으로써, 동일한 암호 키의 경우에도 상이한 암호화 결과를 제공할 수 있게 된다. 더욱 구체적으로는, 도 26에 나타낸 바와 같이, 데이터 링크 장치(2111)로부터 출력되는 암호화된 암호 해독 키는 키 암호 해독 장치(2112)에 입력되고, 이어서, 소정의 디스크 키를 사용하여, 키 암호 해독 장치(2112)는 입력되는 암호화된 암호 해독 키를 더미(dummy) 데이터인 패딩(padding) 데이터(1 바이트), 및 암호 해독 키(7 바이트)로 해독하고, 이어서, 패딩 데이터와 암호 해독 키가 키 변환기(2113)에 출력된다. 이 경우에, 디스크 키는 디스크 키 암호 해독 장치(도면에 나타내지 않음)로써, 예로서, 소정의 마스터 키인 비밀 키를 사용하여 광 디스크에 기록된 암호화된 디스크 키를 해독함으로써 취득된다. 또한, 키 변환기(2113)는 곱셈, 나눗셈, 또는 상기 키 암호 해독 장치(2112)로부터 출력되는 암호 해독 키를 사용하여 소정의 가중치 부여 계수를 이용하는 연산 등, 소정의 변환 연산을 통하여, 주 데이터 영역(2102)으로부터 판독된 암호 해독 키 변환 데이터의 데이터를 변환하고, 이어서, 컨텐츠 암호 해독 키(7 바이트)를 생성하여 암호 해독 장치(2114)에 출력한다. 후속해서, 암호 해독 장치(2114)는 상기 키 변환기(2113)로부터 출력되는 컨텐츠 암호 해독 키(7 바이트)를 사용하여 주 데이터 영역(2102)으로부터 판독된 컨텐츠 데이터를 암호 해독함으로써 해독된 컨텐츠 데이터를 생성하여 출력한다. 암호 해독 키 변환 데이터(2110)로서, 복사 세대 관리 정보 또는 아날로그 매크로 비전(macro-vision) 제어 플래그를 왜곡시키는 등 데이터의 불법적인 사용을 즉시 검출할 수 있는 데이터 등의 데이터를 이용하는 것이 바람직하다.

도 27은 바람직한 제6실시예에 의한 광 디스크의, 사용자 데이터 영역에서의 저작권 제어 정보 및 암호 해독 키의 배치, 및 주 데이터 영역에서의 암호화된 컨텐츠의 배치를 나타내는 블록도이다. 도 27에 나타낸 사용자 데이터 영역(2150)의 예에서, 암호 해독 키 영역은 4바이트의 분할된 암호 해독 키를 갖는 제1암호 해독 키 영역(2201), 및 4바이트의 분할된 암호 해독 키를 갖는 제2암호 해독 키 영역(2202)으로 분할되어 배치되어 있다. 따라서, 이 2개의 섹터에 기록되는 암호화된 컨텐츠의 크기에도 불구하고, 복수의 섹터(도 27에서 2개 섹터)가 이용된다. 이 경우에, 미사용 영역에는 보완 데이터로서 더미(dummy) 데이터가 기록된다. 도 27의 예에서, 하나의 섹터에 대해서만 암호화된 컨텐츠(2204)가 존재하는 경우에 하나의 섹터에 대한 보완 데이터(2203)가 기록된다.

도 28은, 바람직한 제6실시예에 의한 광 디스크에서, 하나의 오류 검출 단위가 복수의 섹터에 걸쳐서 배치되는 경우의 구성을 나타내는 블록도이다. 예로서, 광 디스크가 DVD인 경우에, 16섹터의 오류 정정 코드 단위 블록(이하 ECC(error correction code) 블록이라고 함)을 사용함으로써 오류 정정 능력을 향상시킨다. 따라서, 데이터 기록 또는 재생을 실행할 때, ECC 블록 단위를 사용하여 기록 처리를 실행하는 것이 필요하다. 암호 해독 키가 임의의 개수의 분할된 암호 해독 키로 분할되어 기록되는 경우에, 이러한 경우는 하나의 암호 해독 키가 복수의 오류 정정 블록에 기록되는 경우에 발생될 수도 있다. 상기의 암호 해독 키를 재생하는 경우에, 모든 복수의 분할된 암호 해독 키를 재생하는 것이 필요하므로, 암호화된 컨텐츠 데이터를 기록하는 섹터의 데이터뿐만 아니라 암호 해독 키가 기록되기 바로 전의 ECC 블록의 데이터도 재생하는 것이 또한 필요하다. 도 28의 예는, 암호 해독 키가 분할될 때 분할 개수가 ECC 블록의 섹터의 수의 약수(約數) 또는 인수(因數)로서 설정되는 것을 특징으로 한다. 이로 인하여, 복수의 분할된 암호 해독 키는 복수의 ECC 블록에 걸쳐서 배치되도록 기록될 수 없게 된다. 또한, 하나의 ECC 블록에 암호 해독 키로서, 하나의 방식의 암호 해독 키만이 사용되고, 또한 기록된 AV 데이터가 하나의 ECC 블록에 대하여 충분하지 않은 경우에, 보완 데이터 및 보완 섹터를 배치함으로써 재생시에 불필요한 섹터의 데이터가 광 디스크로부터 판독되는 것을 방지할 수 있다.

(바람직한 제7실시예)

도 29는 본 발명의 바람직한 제7실시예에 의한, 광 디스크내의 인입 영역(2401)과 사용자 데이터 영역(2402)의 구성, 및 인입 영역(2401)과 사용자 데이터 영역(2402)의 데이터로부터 암호화된 컨텐츠를 해독하는 광 디스크 재생장치의 구성을 나타내는 블록도이다.

도 29를 참조하면, 도 26의 바람직한 제6실시예의 방법에 동일한 방법으로, 인입 영역(2401)과 사용자 데이터 영역(2402) 각각은 섹터 헤더 영역(2101), 주 데이터 영역(2102) 및 오류 정정 코드(2103)를 갖는 섹터로 구성된다. 섹터 헤더 영역(2101)에는, 섹터 위치를 나타내는 섹터 어드레스(2104), 및 주 데이터 영역(2102)에 기록된 데이터에 대한 저작권 제어 정보(스크램블 플래그, 복사 제어 정보 등을 포함하는)를 기록하는 저작권 제어 정보(2105)가 기록되고, 또한, 섹터 헤더 영역(2101)은 주 데이터 영역(2102)의 데이터가 암호화되어 있는 경우에 해독하는 암호 해독 키를 조회하기 위한, 암호 해독 키의 기록 위치(즉, 주 데이터 영역(2102)내의 암호 해독 키 테이블(2404)에서의 저장 위치의 기록 위치)를 나타내는 키 인덱스를 기록하는 키 인덱스 영역(2403)을 또한 포함한다. 사용자 데이터 영역(2402)에 기록된 암호화된 컨

텐츠를 해독하는 암호 해독 키는, 테이블 형태로 재기록할 수 있는 인입 영역(2401)에 암호 해독 키 테이블(2401)의 형태로 기록된다. 인입 영역(2401)에 기록된 암호 해독 키는 키 인덱스 영역(2403)에 기록된 키 인덱스로써 조회한다. 도 26에 나타낸 바람직한 제6실시예의 방법에 동일한 방법으로, 상기에서 조회한 암호 해독 키는 키 암호 해독 장치(2112)에 의해서, 소정의 디스크 키를 사용하여, 패딩 데이터, 및 암호 해독 키(또는 타이틀 키)로 해독되고, 후속해서, 상기 해독된 암호 해독 키(또는 타이틀 키)는 키 변환기(2113)에 의해서 암호 해독 키 변환 데이터를 사용하여 컨텐츠 암호 해독 키로 변환된 다음, 변환된 컨텐츠 암호 해독 키가 암호 해독 장치(2114)에 출력된다. 암호 해독 장치(2114)는 컨텐츠 암호 해독 키를 사용하여 암호화 컨텐츠 데이터를 해독하고, 이어서, 해독된 컨텐츠 데이터를 생성하여 출력한다.

상기와 같이 구성된, 바람직한 제7실시예에 의한 광 디스크와, 광 디스크 재생장치에서, 섹터 헤더 영역(2101) 내의 키 인덱스 영역(2403)에 조회하기 위한 키 인덱스를 기록함으로써, 키 인덱스 영역(2403)의 크기와 관계없이 암호 해독 키 테이블(2404)의 암호 해독 키 크기를 할당할 수 있게 된다. 또한, 암호 해독 키 테이블(2404)의 크기를 할당한 후에, 키 인덱스 영역(2403)내의 키 인덱스가 나타내는 암호 해독 키 테이블(2404)로부터 복수의 암호 해독 키를 연속적으로 사용함으로써, 임의의 또는 자유스러운 크기의 암호 해독 키를 사용할 수 있다.

도 30A는 바람직한 제7실시예에 의한 광 디스크내의 인입 영역(2401)의 주 데이터 영역(2102)에 암호 해독 키의 초기치에 의한, 기록되지 않은 상태를 나타내는 경우의 데이터 구성을 나타내는 블록도이다. 도 30A를 참조하면, 광 디스크 등의 포맷팅시에 기록되는 암호 해독 키의 초기치로서, 기록되지 않은 상태의 데이터(2501)는 키로서 사용되지 않는 기지(旣知)의 고정치(예로서 모두 제로(zero) 등의 데이터)가 기록됨에 따라서, 암호 해독 키의 기록되지 않은 상태를 나타낸다.

도 30B는 바람직한 제7실시예에 의한 광 디스크내의 인입 영역(2401)의 주 데이터 영역(2102)에 암호 해독 키 상태 테이블로써, 기록된 상태를 나타내는 경우의 데이터 구성을 나타내는 블록도이다. 도 30B를 참조하면, 도 30A에 나타낸 암호 해독 키의 방법에 동일한 방법으로, 인덱스로써 조회할 수 있는 테이블 형태의 암호 해독 키 상태 테이블(2502)이 인입 영역(2401)에 배치되고, 암호 해독 키의 기록된 상태는 이하와 같이 기록 상태 데이터(2503)로서 기재된다.

(1) 0x00: 미사용

(2) 0x01: 영역 예약

(3) 0x03: 키가 기록됨

(4) 기타: 예비

이 경우에, 0x는 이하의 부호 또는 번호의 16진수 표시를 나타낸다.

도 31은 바람직한 제7실시예에 의한 광 디스크에서의 암호 해독 키의 배치를 나타내는 블록도이다. 도 31의 예에서, 디스크의 암호 해독 키 영역의 배치는 암호 해독 키의 신뢰성을 강화하도록 고안되어 있다. 통상적으로, 결함 관리는 사용자 데이터 영역(2602)에서 실행되므로, 기록 불량이 발생하는 경우에, 대체될 영역에 대한 대체 절차 등이 실행된다. 그러나, 인입 영역(2601)에서는, 상기한 바와 같은 결함 관리는 실행되지 않는다. 그러므로, 기록 불량, 판독 불량 등의 발생에 의해서, AV 데이터를 생성하는 데에 필요한 암호 해독 키가, 사용할 수 없는 상태로 변환될 수도 있고, 또한, 광 디스크 자체가 사용할 수 없는 상태로 변환되는 경우가 있을 수도 있다. 따라서, 전체의 복수의 암호 해독 키는 복수의 상이한 ECC 블록에 걸쳐서 기록할 필요가 있다. 복수의 암호 해독 키가 서로 인접한 영역에 기록되어 있는 경우에, 기록된 모든 복수의 암호 해독 키는 긁힘 또는 먼지로 인하여 판독되지 않을 수도 있다. 그러므로, 도 31에 나타낸 바와 같이, 광 디스크의 내주측 및 외주측 등 분리된 배치 위치에, 예로서, 인입 영역(2601)과 인출 영역(2603)에 기록하는 것이 바람직하다.

도 29의 바람직한 실시예에서, 암호 해독 키 영역은 인입 영역(2401 및 2601)에 배치된다. 이것은, 사용자 데이터 영역(2602)이 종래의 판독 명령 또는 기록 명령으로써 액세스할 수 있는 영역인 것을 고려하여, 개인용 컴퓨터 등의 구동 유닛으로부터 액세스할 때 안전을 강화하기 위한 것이다. 따라서, 이것들을 사용자 데이터 영역(2602)에 배치함으로써 동일한 유리한 효과를 얻을 수 있다.

(바람직한 제8실시예)

도 32는 본 발명에 의한 바람직한 제8실시예의 파일 관리 시스템에 의한 광 디스크의 데이터를 관리하는 데이터 구성을 나타내는 블록도이다. 도 32의 예에서, 파일 시스템의 구조에 따라서, 필요한 파일을 저장하는 섹터 어드레스를 관리한다.

국제 표준화 기구(International Standardization Organization)에 의한 ISO 13346에 규정된 파일 시스템의 구조에 있어서, 파일의 기록 위치는, 재기록 가능 방식의 광 디스크를 사용하기 위하여, 파일 엔트리(entry)라고 하는 정보를 사용하여 관리된다. 도 32에 나타낸 바와 같이, 예로서, 파일(1)(2703)의 기록 위치의 데이터는 파일 관리 정보 영역(2751) 내의 파일 엔트리(1)(2701)로서 저장되고, 파일(2)(2704)의 기록 위치의 데이터는 파일 엔트리(2)(2702)로서 저장된다. 각각의 파일은 광 디스크상에서 연속하도록 배치되는 복수의 섹터 영역을 관리하는 익스텐트(2705 및 2706)로 구성되어 있다. 바람직한 제7실시예에 나타낸 바와 같은 암호화된 컨텐츠는 파일 엔트리로서 표시된, 광 디스크 상의 주 데이터 영역(2102)에 기록되고, 암호 해독 키는 인입 영역(2601)내의 암호 해독 키 테이블(2707)에 기록된다. 암호화된 컨텐츠가 기록되는 사용자 데이터 영역(2602)내의 섹터 헤더 영역(2101)에는, 암호 해독에 필요한 암호 해독 키를 조회하기 위한, 기록 위치를 나타내는 포인터가 키 인덱스 영역(2708)에 기록된다. 본 바람직한 실시예에서, 암호 해독 키는 파일 단위, 익스텐트 단위를 사용하여 관리되고 기록되지만, 본 발명은 이 것에 한정되지 않는다. 암호 해독 키는 파일 단위 또는 익스텐트 단위 중 최소한 어느 하나를 사용하여 관리되고 기록될 수도 있다.

상기한 바와 같이 파일 관리 시스템으로써 관리되는 광 디스크에 있어서, 저작권 보호를 필요로 하는 컨텐츠의 기록 동작을 도 33을 참조로 하여 설명한다. 도 33은 바람직한 제8실시예에 의한 파일 관리 시스템에 의해서 실행되는, 저작권 보호를 필요로 하는 컨텐츠의 기록 방법을 나타낸다.

암호화된 컨텐츠를 기록하는 경우, 우선, 단계 S2801에서, 도 30B에 나타낸 암호 해독 키 상태 테이블(2502)을 판독하여 암호 해독 키 테이블(2707)의 공백 영역을 조사한다. 이어서, 단계 S2802에서, 암호 해독 키 테이블(2707)의 공백 영역이 있는가 없는가를 판단하고, NO의 경우에, 암호화된 컨텐츠에 대한 암호 해독 키가 기록될 수 없으므로 단계 S2807에서 기록 동작을 정지시킴으로써 컨텐츠의 기록 동작이 종료된다. 다른 한편으로는, 단계 S2802에서 YES의 경우에, 취득한 암호 해독 키(또는 타이틀 키)가 기록되고, 암호 해독 키가 취득될 수 없는 경우에는, 암호 해독 키 영역을 예약한다. 이어서, 단계 S2804에서, 기록된 컨텐츠의 저작권 제어 정보(암호화가 실행되었는가 아닌가에 대한 정보, 암호의 방식 또는 종류 등을 나타내는 정보를 포함하는), 및 키 인덱스 영역(2708)에 기록되는 키 인덱스가 설정되고, 이 후에, 단계 S2805에서 컨텐츠가 암호화된 다음, 암호화된 컨텐츠가 익스텐트 단위를 사용하여 파일 형태로 광 디스크에 기록된다. 이 경우에, 파일 단위를 이용하여 동일한 저작권 제어 정보 및 키 인덱스가 사용될 수도 있고, 또는 익스텐트 단위를 이용하여 변경될 수도 있다. 즉, 단계 S2804와 S2805에서, 처리되는 단위는 파일 단위 또는 익스텐트 단위 중 최소한 어느 하나이다. 최종적으로, 단계 S2806에서, 기록된 컨텐츠에 관한 정보에 따라서, 상기의 기록된 데이터를 관리하는 파일 관리 정보가 갱신된 후에, 컨텐츠의 기록 처리 과정이 종료된다.

도 34는 바람직한 제8실시예에 의한 파일 관리 시스템에 의해서 실행되는 컨텐츠의 재생 방법을 나타내는 흐름도이다. 도 34는 도 33에 나타낸 방법에 의해서 파일 형태로 기록된 컨텐츠를 광 디스크로부터 재생하는 방법을 나타낸다.

파일에 대한 재생 동작을 실행하는 경우, 파일 관리 정보 영역(2751)내의 파일 엔트리가 나타내는 영역에 대한 키 인덱스를 취득하여, 재생되는 파일에서 사용되는 암호 해독 키 테이블내의 영역을 탐색하거나 또는 인식한다. 더욱 구체적으로는, 단계 S2901에서, 파일 관리 정보(2751)로부터, 재생되는 파일의 파일 엔트리를 판독하여 재생함으로써 취득한 후에, 단계 S2902에서, 취득한 파일 엔트리가 나타내는 영역의 섹터 헤더 영역(2102)으로부터 키 인덱스 영역의 값을 판독하여, 재생한다. 익스텐트 단위를 이용하여 상이한 암호화 방법을 실행하는 경우에는, 각각의 익스텐트에 대한 섹터 헤더의 키 인덱스 영역을 판독한다. 이어서, 단계 S2903에서, 취득한 키 인덱스가 나타내는 암호 해독 키 테이블(2707)의 암호 해독 키 영역으로부터 암호 해독 키를 판독한 후, 재생하여 암호 해독 키를 취득한다. 또한, 단계 S2904에서, 파일 엔트리가 나타내는 영역으로부터 파일 내의 컨텐츠 데이터를 판독하여 재생하고, 이어서, 재생된 컨텐츠 데이터를 해독한다. 이 경우에, 컨텐츠 파일의 재생 및 암호 해독이 완료되면, 컨텐츠의 재생 처리 과정이 종료된다.

도 35는 바람직한 제8실시예에 의한 파일 관리 시스템에 의해서 실행되는, 컨텐츠의 삭제 방법을 나타내는 흐름도이고, 도 35는 도 33에 나타낸 방법에 의해서 기록된, 파일 형태의 컨텐츠 데이터의 삭제 동작을 나타낸다.

파일의 삭제 동작을 실행하는 경우, 파일 엔트리가 나타내는 영역에 대한 키 인덱스를 취득하여, 삭제되는 파일이 사용하는 암호 해독 키 테이블(2707)의 영역을 탐색하거나 또는 인식한다. 더욱 구체적으로는, 단계 S3001에서, 파일 관리 정보 영역(2751) 내의 파일 관리 정보로부터 삭제되는 파일의 파일 엔트리를 취득한 후에, 단계 S3002에서 파일 엔트리가 나타내는 영역의 섹터 헤더로부터 키 인덱스 영역의 값을 취득한다. 이 경우에, 익스텐트 단위를 사용하여 상이한 방법의 암호화 방법이 실행되면, 각각의 익스텐트에 대한 섹터 헤더의 키 인덱스 영역의 데이터를 판독한다. 이어서, 단계 S3003에서, 취득한 키 인덱스가 나타내는 암호 해독 키 테이블(2707)의 암호 해독 키 영역으로부터 암호 해독 키를 개방하거나 공개한 후에(여기서 암호 해독 키의 개방 또는 공개는 암호 해독 키를 테이블로부터 삭제하는 것을 의미한다), 단계 S3004에서, 삭제되는 파일의 기록 위치를 나타내는 파일 엔트리를 파일 관리 정보로부터 삭제하고, 이어서, 컨텐츠의 삭제 처리 과정

이 완료된다. 종래의 파일 시스템에서는 파일이 삭제될 때 파일 엔트리만이 삭제되지만, 암호화된 컨텐츠의 암호 해독 키와 기록 섹터가 별개의 영역에 기록되므로 또 다른 영역에 기록된 암호 해독 키는 삭제되지 않는다. 상기의 바람직한 실시예에서는, 파일 엔트리를 삭제하기 전에, 섹터 헤더 영역 내의 키 인덱스가 나타내는 암호 해독 키를 암호 해독 키 테이블(2707)로부터 삭제함으로써 광 디스크상에서의 암호 해독 키의 관리를 실행한다.

(바람직한 제9실시예)

도 36은 본 발명에 의한 바람직한 제9실시예의 광 디스크 시스템의 구성을 나타내는 블록도이고, 이 광 디스크 시스템은 광 디스크(3100)에 대한 저작권 보호를 필요로 하는 컨텐츠를 기록하고 재생하는 정보 처리 시스템이다. 상기 광 디스크 시스템은 인코딩 장치(3101), 광 디스크 장치(3102), 디코딩 장치(3103) 및 개인용 컴퓨터(3104)를 포함한다.

인코딩 장치(3101)는 컨텐츠 데이터를 저장하는 컨텐츠 메모리(3131), 상기 컨텐츠 데이터를 MPEG 포맷 형태로 인코딩하는 인코딩 회로(3132), 암호 키를 저장하는 암호 키 메모리(3133), 인코딩된 컨텐츠 데이터를 암호 키를 사용하여 암호화하고 또한 암호 해독 키를 생성하여 암호 해독 키 메모리(3111)에 저장하는 암호화 회로(3134), 암호 해독 키를 저장하는 암호 해독 키 메모리(3111), 암호 해독 키를 버스-암호화(bus-encrypting)하는 버스 암호화 회로(3112), 및 PCI (peripheral component interconnect bus) 버스(3151)를 통하여 개인용 컴퓨터(3104)의 인터페이스(3122)에 접속되는 인터페이스(3124)를 포함하고, 여기서 인터페이스(3124)는 암호화된 컨텐츠 데이터 및 암호 해독 키를 송신한다. 또한, 광 디스크 장치(3102)는 복수의 암호 해독 키를 저장하는 암호 해독 키 테이블 메모리(3113), 버스 암호화 및 암호 해독 회로(3114), 광 디스크(3100)에 데이터를 기록하고 또한 광 디스크(3100)로부터 데이터를 판독하고 재생하는 기록 및 재생 회로(3119), 및 SCSI(small computer interface system) 버스(3152)를 통하여 개인용 컴퓨터(3104)의 인터페이스(3121)에 접속되는 인터페이스(3120)를 포함하고, 여기서 인터페이스(3120)는 데이터 또는 신호의 송수신 및 신호 변환과 프로토콜 변환 등의 처리를 실행한다. SCSI 버스는 ATAPI 버스인 것이 바람직할 수도 있다. 이 경우에, 버스 암호화 및 버스 해독은 암호 키 또는 암호 해독 키를 암호화하고, 또한 상기 키들을 PCI 버스(3151) 또는 SCSI 버스(3152)를 통하여 송신 또는 수신하는 데에 사용하는, 암호화 처리 및 암호 해독 처리를 각각 의미한다.

또한, 개인용 컴퓨터(3104)는 개인용 컴퓨터(3104)의 동작을 제어하는 제어부(3130), 복수의 버스 암호화 암호 해독 키를 저장하는 버스 암호화 암호 해독 키 테이블 메모리(3115), 상기 복수의 버스 암호화 암호 해독 키에 대응하는 복수의 암호 해독 키 상태(복수의 암호 해독 키 상태의 기록 상태 또는 조건을 나타내는, 더욱 구체적으로는, 사용안함 또는 미사용, 영역 예약, 키가 기록됨, 예약 등을 나타내는)의 데이터를 저장하는 암호 해독 키 상태 테이블 메모리(3116), SCSI 버스(3152)를 통하여 인터페이스(3120) 또는 광 디스크 장치(3102)에 접속되어서, 데이터와 신호의 송수신 및 신호 변환과 프로토콜 변환 등의 처리를 실행하는 인터페이스(3121), 및 PCI 버스(3151)를 통하여 디코딩 장치(3103)의 인터페이스(3123)와 인코딩 장치(3101)의 인터페이스(3124)에 접속되어서, 데이터 또는 신호의 송수신 및 신호 변환과 프로토콜 변환 등의 처리를 실행하는 인터페이스(3122)를 포함한다. 또한, 디코딩 장치(3103)는 개인용 컴퓨터(3104)의 인터페이스(3122)에 접속되어서 데이터 또는 신호의 송수신 및 신호 변환과 프로토콜 변환 등의 처리를 실행하는 인터페이스(3123), 인터페이스(3123)에 의해서 수신된 암호화 암호 해독 키를 버스-암호 해독 또는 버스-디코딩하는 버스 암호 해독 회로(3117), 암호 해독 키를 저장하는 암호 해독 키 메모리(3118), 및 인터페이스(3123)에 의해서 수신된 암호화된 컨텐츠 데이터를 암호 해독 키 메모리(3118)의 암호 해독 키를 사용하여 암호 해독하거나 또는 디코딩하고, 또한 MPEG 포맷의 디코딩 처리를 실행함으로써 영상 신호 또는 음성 신호를 생성하는 암호 해독 회로(3141)를 포함하고, 여기서 생성된 영상 신호 및 음성 신호는 디스플레이 장치(3105)에 출력된다.

이 광 디스크 시스템의 인코딩 장치(3101)에서, 인코딩 회로(3132)는 컨텐츠 메모리(3131)에 저장되거나 또는 입력된 MPEG 포맷 형태의 AV 데이터 등 컨텐츠 데이터를 인코딩하고, 암호화 회로(3134)는 개인용 컴퓨터(3104)를 통한 컨텐츠의 불법적인 사용을 방지하기 위해서 생성되는, 암호화 키 메모리(3133) 내의 암호 키를 사용하여 상기 인코딩된 컨텐츠 데이터를 암호화한 후, 인터페이스(3124) 및 개인용 컴퓨터(3104)를 통하여 인코딩된 컨텐츠 데이터를 광 디스크 장치(3102)에 송신한다. 이 경우에, 암호화된 컨텐츠 데이터는 인코딩 장치(3101)의 인터페이스(3124)로부터 PCI 버스(3151), 개인용 컴퓨터(3104)의 인터페이스(3122)와 인터페이스(3121), 및 광 디스크 장치(3102)의 인터페이스(3120)를 통하여 기록 및 재생 회로(3119)에 송신된다. 이어서, 암호화된 컨텐츠 데이터는 광 디스크 장치(3102)의 기록 및 재생 회로(3119)에 의해서 광 디스크(3100)에 기록된다. 또한, 광 디스크 장치(3102)의 기록 및 재생 회로(3119)는 광 디스크(3100)에 기록된 암호화된 컨텐츠 데이터를 재생하고, 이어서, 재생된 암호화된 컨텐츠 데이터를 인터페이스(3120), 개인용 컴퓨터(3104)의 인터페이스(3121)와 인터페이스(3122), 및 디코딩 장치(3103)의 인터페이스(3123)를 통하여 암호 해독 회로(3141)에 송신한다. 디코딩 장치(3103)의 암호 해독 회로(3141)는 암호화된 컨텐츠 데이터에 대한 암호를 해독하고, MPEG 포맷의 디코딩 처리를 실행한 후에, 디코딩된 컨텐츠의 영상 신호 또는 음성 신호를 디스플레이 장치(3105) 및 스피커 장치(도면에 나타내지 않음)에 출력한다.

인코딩 장치(3101)의 암호화 회로(3134)는 암호 키 메모리(3133) 내의 암호 키를 사용하여, MPEG 포맷 형태로 인코딩된 컨텐츠 데이터에 대한 암호화를 실행하고, 또한 동시에 재생시에 필요한 암호 해독 키를 생성하여 암호 해독 키 메모리(3111)에 저장한다. 인코딩된 컨텐츠 데이터 및 암호 해독 키를 광 디스크(3100)에 기록할 필요가 있지만, 암호 해독 키가 개인용 컴퓨터(3104) 상에서 평문(平文)(암호화되지 않은)으로서 취급되는 경우에는, 광 디스크(3100)로부터 암호 해독 키를 판독함으로써, 암호화된 컨텐츠 데이터의 디코딩이 용이하게 될 수도 있는 가능성이 있다. 이러한 것을 피하기 위해서, 인코딩 장치(3101)와 광 디스크 장치(3102)와의 사이에 상호 인증을 실시하고 상호 공유하는 버스 키를 사용하여 버스 암호화를 실행한다.

즉, 더욱 구체적으로는, 인코딩 장치(3101)의 암호 해독 키 메모리(3111)에 저장된 암호 해독 키는 버스 암호화 회로(3112)에 의해서 암호화되고, 이어서, 암호화된 암호 해독 키는 인터페이스(3124), PCI 버스(3151), 및 인터페이스(3122)를 통하여 개인용 컴퓨터(3104)의 버스 암호화 암호 해독 키 테이블 메모리(3115)에 저장된다. 다른 한편으로는, 광 디스크 장치(3102)의 버스 암호화 및 암호 해독 회로(3114)에서, 기록 및 재생 회로(3119)에 의해서 광 디스크(3100)로부터 재생되는 암호화된 암호 해독 키의 디코딩이 실행되고, 이 후에, 암호 해독되거나 디코딩된 암호 해독 키가 암호 해독 키 테이블 메모리(3113)에 저장된다. 또한, 버스 암호화 및 암호 해독 회로(3114)는, 예로서, 버스 암호화 암호 해독 키 테이블 메모리(3115)로부터 인터페이스(3121), SCSI 버스(3152) 및 인터페이스(3120)를 통하여, 갱신된 버스-암호화 암호 해독 키를 수신하여 버스-암호 해독하고, 버스-암호 해독된 암호 해독 키를 암호 해독 키 테이블 메모리(3113)에 저장한다. 이어서, 버스-암호 해독된 암호 해독 키는 기록 및 재생 회로(3119)에 의해서 광 디스크(3100)에 기록된다.

암호 해독 키 상태 테이블이 기록 및 재생 회로(3119)에 의해서 광 디스크(3100)로부터 재생된 후에, 암호 해독 키 상태 테이블은 인터페이스(3120), SCSI 버스(3152) 및 인터페이스(3121)를 통하여 암호 해독 키 상태 테이블 메모리(3116)에 전송되어 저장된다. 또한, 개인용 컴퓨터에 의해서 갱신된 암호 해독 키 상태 테이블은 암호 해독 키 상태 테이블 메모리(3116)로부터 판독된 다음에, 인터페이스(3121), SCSI 버스(3152) 및 인터페이스(3120)를 통하여 기록 및 재생 회로(3119)에 전송된다. 이어서, 기록 및 재생 회로(3119)는 수신한 암호 해독 키 상태 테이블을 광 디스크(3100)에 기록한다. 따라서, 버스 암호화 암호 해독 키 테이블 메모리(3115)와 암호 해독 키 상태 테이블 메모리(3116)를 사용함으로써, 중앙에 위치한 개인용 컴퓨터(3104)에서는, 암호화된 암호 해독 키만을 취급하고, 이로 인하여 안전성이 더욱 확보된다.

동일한 방법으로 광 디스크 장치(3102)와 디코딩 장치(3103)와의 사이에서의 암호 해독 키의 버스-암호화를 실시하면 안전성이 더욱 확보된다. 즉, 디코딩 장치(3103)의 버스 암호 해독 회로(3117)는 인터페이스(3123)를 통하여 개인용 컴퓨터(3104)로부터 수신한 암호화된 암호 해독 키를 버스-암호 해독하거나 또는 버스-디코딩하여, 버스-암호 해독된 암호 해독 키를 암호 해독 키 메모리(3118)에 저장한다. 암호 해독 회로(3141)는 암호 해독 키 메모리(3118)에 저장된 암호 해독 키를 사용하여, 암호화된 컨텐츠 데이터를 해독한다.

상기의 바람직한 제7실시예에 나타낸 바와 같이, 광 디스크(3100) 상의 암호화된 컨텐츠 데이터를 암호 해독하는 암호 해독 키가 테이블 형태로 기록되어 있는 경우에, 광 디스크 장치(3102)에 의해서 재생되는 암호 해독 키 테이블은 버스 암호화 및 암호 해독 회로(3114)에 의해서 버스-암호화되고, 이어서, 버스-암호화된 암호 해독 키 테이블의 데이터는 인터페이스(3120)를 통하여 개인용 컴퓨터(3104)의 버스-암호화된 암호 해독 키 테이블 메모리(3115)에 전송되어서, 그 곳에 저장된다. 컨텐츠 데이터를 기록하는 경우, 개인용 컴퓨터(3104)는 평문 형태로 광 디스크(3100)에 기록된 암호 해독 키 상태 테이블로부터 암호 해독 키 테이블의 공백 영역을 검색함으로써 탐색하고, 이어서, 인코딩 장치(3101)로부터 전송된 버스-암호화된 암호 해독 키를 탐색된 공백 영역에 할당한다. 이 경우에, 버스 암호로서, 암호 해독 키 단위로써 완결되는 암호(예로서, 암호 해독 키 길이의 단위로써 암호화하는 블록 암호)이면, 암호 해독 키 블록에의 암호 해독 키의 할당시에 암호 해독 키를 해독할 필요가 없고 또한 재암호화할 필요가 없다.

광 디스크(3100), 광 디스크 장치(3102) 및 개인용 컴퓨터(3104) 사이에서 전송되고 저장되는 암호 해독 키 테이블 및 암호 해독 키 상태 테이블은 각각 블록 데이터의 일부이므로, 이것들은 블록 데이터라고 할 수 있다.

컨텐츠를 재생하는 경우에, 광 디스크 장치(3102)로부터 재생되는 암호 해독 키 블록으로부터 재생하려고 하는 컨텐츠의 암호 해독에 필요한 암호 해독 키만이 버스 암호화된 암호 해독 키 테이블 메모리(3115)로부터 검색되어 취출되고, 취출된 암호 해독 키는 개인용 컴퓨터(3104)의 버스 암호 해독 회로(3117)와, 디코딩 장치(3103)를 통하여 암호 해독 키 메모리(3118)에 전송되어 저장된다. 후속해서, 암호 해독 회로(3141)는 광 디스크 장치(3102)의 기록 및 재생 회로(3119)에 의해서 광 디스크(3100)로부터 재생된 암호화된 AV 데이터를 개인용 컴퓨터(3104) 및 인터페이스(3123)를 통하여 수신하고, 이어서, 수신한 암호화된 AV 데이터는 암호 해독 키 메모리(3118) 내의 암호 해독 키를 사용하여 암호 해독되어서, 해독된 데이터가 영상 신호 및 음성 신호로서 출력된다. 이 경우에, 상기의 경우의 방법에 유사한 방법으로, 컨텐츠를 기록할 때, 버스 암호로서, 암호 해독 키 단위로써 완결되는 암호(예로서, 암호 해독 키 길이의 단위로써의 블록 암호)이면, 암호

해독 키 블록으로부터 암호 해독 키를 취출할 때 암호 해독 키를 해독할 필요가 없고 또한 재암호화할 필요가 없다. 또한, 암호 해독 키의 크기를 확장하는 경우, 광 디스크 장치(3102)의 구성을 아무 것도 변경하지 않고, 복수의 암호 해독 키를 할당하는 등의 암호 해독 키 영역의 확장을 개인용 컴퓨터(3104) 상에서 용이하게 또한 안전하게 실행할 수 있다.

(바람직한 제10실시예)

도 37은 본 발명의 바람직한 제10실시예에 의한, 광 디스크 상의 사용자 데이터 영역의 구성, 컨텐츠를 암호화하여 암호화된 컨텐츠를 사용자 데이터 영역에 기록하는 광 디스크 기록장치의 구성, 및 사용자 데이터 영역의 데이터로부터 암호화된 컨텐츠를 해독하는 광 디스크 재생장치의 구성을 나타내는 블록도이다. 본 바람직한 제10실시예는 바람직한 제6실시예의 구성에 광 디스크 기록장치의 구성이 추가되는 것을 특징으로 하고, 이에 대한 구성을 상세하게 설명한다.

광 디스크 기록장치에서, 일정한 암호화 결과를 갖지 않도록 암호의 강도를 강화하기 위하여, 곱셈, 나눗셈, 또는 컨텐츠 내의 정보인 암호 해독 키 변환 데이터를 이용하여 키 변환기(2119)로써 소정의 가중치 부여 계수에 의한 연산(계산) 등, 입력된 암호 키에 대한 소정의 키 변환을 실행함으로써, 컨텐츠 암호 해독 키를 취득한 후에, 컨텐츠 암호 해독 키를 사용하여 컨텐츠 데이터를 암호화한다.

즉, 컨텐츠를 기록할 때, 컨텐츠 데이터, 및 컨텐츠 데이터를 암호화하는 암호 키를 광 디스크 기록장치에 입력한다. 이 경우에, 컨텐츠 데이터는 키 변환기(2119) 및 암호화 장치(2120)에 입력되고, 암호 키는 키 암호화 장치(2118) 및 키 변환기(2119)에 입력된다. 키 변환기(2119)는, 각각 컨텐츠 내의 정보의 일부인, 제1 및 제2암호 해독 키 변환 데이터(2115 및 2116)를 사용하여, 상기 입력 암호 키에 대한 소정의 키 변환 연산 또는 계산을 실행하고, 이어서, 컨텐츠 암호 해독 키를 생성하여 암호화 장치(2120)에 출력한다. 후속해서, 암호화 장치(2120)는 상기 컨텐츠 암호 해독 키를 사용하여 상기 입력된 컨텐츠를 암호화한 다음, 암호화된 컨텐츠를 광 디스크의 사용자 데이터 영역(2150) 내의 AV 데이터 기록 섹터(2152)에 기록한다.

이 경우에, 광 디스크 재생장치에서 사용되는 암호 해독 키 변환 데이터로서, AV 데이터 내의 정보이고 또한 통상적으로 섹터 단위가 상이한 제2암호 해독 키 변환 데이터(2116), 제어 정보가 기록되는 섹터에 포함된 복사 세대 관리 정보, 및 아날로그 매크로-비전 제어 플래그를 포함하는 복사 제어 정보인 제1암호 해독 키 변환 데이터(2115)를 사용한다. 전자의 제2암호 해독 키 변환 데이터(2116)를 사용함으로써, 제2암호 해독 키 변환 데이터의 컨텐츠에 따라서 키 변환기(2113)로써 각각의 섹터에 대한 컨텐츠 데이터를 암호화하는 컨텐츠 암호 해독 키를 복구할 수 있게 된다. 또한, 후자의 제1암호 해독 키 변환 데이터는 왜곡시에 불법적인 사용을 용이하게 검출할 수 있게 하기 위한 데이터이므로, 제1암호 해독 키 변환 데이터가 왜곡된 경우 컨텐츠 데이터가 암호 해독되는 것을 용이하게 방지할 수 있는 유리한 효과를 얻을 수 있다. 더욱 구체적으로는, 제1암호 해독 키 변환 데이터로서, AV 데이터의 재생 제어에 사용되는 재생 제어 정보를 기록하기 위한 재생 제어 기록 섹터 내의 데이터를 사용하여, 소정의 변환 연산을 실행함으로써, 암호 키를 암호 해독 키로 변환하고, 변환된 암호 해독 키를 암호화 장치(2120)에서 컨텐츠 암호 해독 키로서 사용한다. 또한, 재생 제어 기록 섹터 내의 데이터인 제1암호 해독 키 변환 데이터와, 암호화된 컨텐츠를 기록하는 섹터 내의 암호화되지 않은 컨텐츠의 일부인 제2암호 해독 키 변환 데이터를 포함하는 2개의 암호 해독 키 변환 데이터를 사용하여 암호 키에 대하여 소정의 변환 연산 또는 계산을 실행함으로써, 암호화 장치(2120)에서 컨텐츠 암호 해독 키로서 사용될 수도 있는 또 다른 컨텐츠 암호 해독 키가 산출된다.

한편, 키 암호화 장치(2118)는 광 디스크 재생장치의 방법에 동일한 방법으로 입력된 디스크 키를 사용하여 상기 입력된 암호 키를 암호화하여, 암호화된 암호 해독 키를 생성한다. 상기 암호화된 암호 해독 키의 크기에 비하여, 섹터 헤더 영역 내의 각각의 암호 해독 키 영역(2106 및 2109)은 작으므로, 데이터 분할기(2121)가 암호화된 암호 해독 키를 복수의 분할된 암호 해독 키로 분할한 후에, 각각의 분할된 암호 해독 키를 상이한 암호 해독 키 영역(2106 및 2109)에 기록한다. 도 37의 예에서, 암호화된 암호 해독 키는 2개의 암호화되어 분할된 암호 해독 키로 분할되고, 이것들은, 이어서, 2개의 연속 섹터인 암호 해독 키 영역(2106 및 2109)에 기록된다. 이 경우에, 암호 키의 암호 해독 키는 키 암호화 장치(2118)에 의해서 암호화되어 있으므로, 암호 키에 대한 암호의 보안 강도가 강화될 수 있다.

컨텐츠를 재생하는 경우, 키 변환기(2113)는, 상기 제1암호 해독 키 변환 데이터(2115)와 제2암호 해독 키 변환 데이터(2116)의 정보를 사용하여, 키 암호 해독 장치(2112)로부터의 암호 해독 키에 대하여 소정의 키 변환 연산 또는 계산을 실행하여 컨텐츠 암호 해독 키를 생성하고, 이어서 이 컨텐츠 암호 해독 키는 암호 해독 장치(2114)에 출력된다. 또한, 암호 해독 장치(2114)는 상기 컨텐츠 암호 해독 키를 사용하여, 암호화된 컨텐츠 데이터를 해독하여 암호 해독된 컨텐츠를 취득한다. 이 경우에, 키 변환기(2113)는 제1암호 해독 키 변환 데이터(2115)의 정보만을 사용하여, 키 암호 해독 장치(2112)로부터의 암호 해독 키에 대하여 소정의 키 변환 연산 또는 계산을 실행할 수도 있다.

(바람직한 제11실시예)

도 38은 본 발명에 의한 바람직한 제11실시예에 의한, 광 디스크 상의 사용자 데이터 영역의 구성, 컨텐츠를 암호화하여 암호화된 컨텐츠를 사용자 데이터 영역에 기록하는 광 디스크 기록장치의 구성, 및 사용자 데이터 영역의 데이터로부터의 암호화된 컨텐츠를 해독하는 광 디스크 재생장치의 구성을 나타내는 블록도이다. 본 바람직한 제11실시예는 바람직한 제7실시예의 구성에 광 디스크 기록장치의 구성이 추가되는 것을 특징으로 하고, 이에 대한 구성을 상세하게 설명한다.

도 38을 참조하면, 광 디스크 기록장치는 도 37에 나타낸 바람직한 제10실시예의 방법에 동일한 방법으로 소정의 디스크 키를 사용하여 암호 키를 암호화하는 키 암호화 장치(2118), 컨텐츠내의 제1 및 제2암호 해독 키 변환 데이터(2115 및 2116)를 사용하여 암호 키에 대한 소정의 키 변환 연산을 통하여 컨텐츠 암호 해독 키를 연산 또는 계산하는 키 변환기(2119), 및 상기의 컨텐츠 암호 해독 키를 사용하여 컨텐츠를 암호화하는 암호화 장치(2120)를 포함한다. 이 경우에, 키 암호화 장치(2118)로부터 출력되는 암호 해독 키는 인입 영역(2401) 내의 주 데이터 영역(2102)에 기록된다. 한편, 광 디스크 재생장치는 도 29에 나타낸 바람직한 제7실시예의 방법에 동일한 방법으로 키 암호 해독 장치(2112), 키 변환기(2113), 및 암호 해독 장치(2114)를 포함한다. 이 경우에, 인입 영역(2401) 내의 주 데이터 영역(2102)에 기록된 암호 해독 키는 판독되어서 키 암호 해독 장치(2112)에 입력되고, 이어서, 키 암호 해독 장치는 소정의 디스크 키를 사용하여 암호 해독 키를 해독하여 해독된 암호 해독 키를 키 변환기(2113)에 출력한다. 또한 키 변환기(2113)는 제1 및 제2암호 해독 키 변환 데이터(2115 및 2116)를 사용하여 키 암호 해독 장치(2112)로부터의 암호 해독 키에 대한 소정의 키 변환 연산 또는 계산을 실행하여 컨텐츠 암호 해독 키를 산출하고, 이어서 이 컨텐츠 암호 해독 키는 암호 해독 장치(2114)에 출력된다.

바람직한 제6 내지 제9실시예의 유리한 효과

상기한 바와 같이, 본 바람직한 실시예에 의한 기록 방식의 광 디스크는 암호 해독 키를, 섹터 헤더 영역에 배치되는 소정 크기를 갖는 암호 해독 키 영역의 암호 해독 키들로 분할하여 기록하거나, 또는 가변 길이를 갖는 암호 해독 키를, 섹터 헤더 영역에 배치되는 키 인덱스 영역이 나타내는 암호 해독 키 영역에 기록하고, 이어서, 섹터 헤더 영역에서 규정된 크기의 암호 해독 키 영역에 관계없이 임의의 또는 자유로운 길이의 암호 해독 키를 사용할 수 있는 기록 방식의 광 디스크가 제공될 수 있다. 그러므로, 기록된 컨텐츠에 대한 저작권 보호 레벨에 따라서, 임의의 키 길이를 사용하는 암호화를 사용할 수 있게 된다.

(바람직한 변형 실시예)

상기의 바람직한 실시예에서, 상기 디스크 식별 정보는 재기록 불가능한 미리 파인 홈으로써 구성하는 것이 바람직하고, 상기 디스크 식별 정보는 광 디스크가 사용되는 지역을 나타내는 지역 식별자를 갖는 것이 바람직하다. 또한, 상기 디스크 식별 정보는 광 디스크에 기록 가능하고 재생 가능한 컨텐츠의 방식, 분류 또는 종류를 나타내는 데이터 범주 식별자를 갖는 것이 바람직하다. 또한, 상기 디스크 식별 정보는, 비밀 키를 사용하여 암호화되어서, 제조시에 디스크 식별 정보 영역에 기록하는 것이 바람직하다. 또한, 상기 디스크 식별 정보는, 데이터 기록 및 재생 영역에 기록할 수 있는 데이터의 방식, 분류 또는 종류, 또는 데이터 기록 및 재생 영역으로부터 재생할 수 있는 데이터의 방식, 분류 또는 종류를 나타내는 데이터를 포함하는 것이 바람직하다.

상기 바람직한 실시예에서, 상기 광 디스크는 컨텐츠 데이터, 및 디스크램블 키와의 대응 관계를 관리하는 디스크램블 영역 관리 테이블용의 섹터 영역을 갖는 것이 바람직하다. 키 관리 정보 영역은, 키로서 디스크 식별 정보를 사용하여 암호화된 디스크램블 키를 기록하는 디스크램블 키 영역, 디스크램블 키의 기록 상태를 나타내는 디스크램블 키 상태 영역을 갖는 키 정보 영역, 디스크에 기록된 컨텐츠의 재생시에 사용되는 키 정보를 기록하는 컨텐츠 정보 영역, 및 컨텐츠의 재생에 필요한 디스크램블 키를 조회하는 포인터를 기록하는 키 인덱스 영역을 포함하는 것이 바람직하다. 또한, 컨텐츠를 기록하는 섹터에는, 상기 컨텐츠 데이터, 및 디스크램블 키를 기록하는 영역을 나타내는 포인터를 기록하는 것이 바람직하다.

상기 바람직한 실시예에서, 광 디스크 기록 및 재생장치의 디스크 식별 정보의 재생 회로는, 비밀 키를 사용하여 암호화된 디스크 식별 정보를 암호 해독하는 회로를 포함하는 것이 바람직하다. 또한, 광 디스크 기록 및 재생장치에서, 디스크 식별 정보를 키로 하여 암호화된 데이터는 영상 데이터 및 음악 데이터 등 컨텐츠 데이터인 것이 바람직하다. 또한, 디스크 식별 정보는 데이터 기록 및 재생 영역에 기록 가능한 데이터의 방식, 분류 또는 종류를 나타내고, 디스크 식별 정보 재생 회로는 상기 데이터의 방식, 분류 또는 종류에 의해서 데이터가 기록 가능한 컨텐츠인가 아닌가를 판단하는 것이 바람직하다. 또한, 디스크 식별 정보를 키로서 사용하여 암호 해독된 데이터는 영상 데이터 또는 음악 데이터 등 컨텐츠 데이터인 것이

바람직하다. 또한, 디스크 식별 정보는 데이터 기록 및 재생 영역으로부터 재생 가능한 데이터의 방식, 분류 또는 종류를 나타내고, 재생 회로는 상기 데이터의 방식, 분류 또는 종류에 따라서 데이터가 재생 가능한 컨텐츠인가 아닌가를 판단하는 것이 바람직하다.

상기 바람직한 실시예에서, 컨텐츠 기록 회로는 암호화된 영상 데이터와 음악 데이터 등 컨텐츠 데이터, 및 상기 컨텐츠 데이터의 암호를 디코딩 또는 해독하는 디스크램블 키를 동일한 섹터에 기록하는 것이 바람직하다. 또한, 컨텐츠 재생 회로는 암호화된 영상 데이터와 음악 데이터 등 컨텐츠 데이터, 및 상기 컨텐츠 데이터의 암호를 디코딩 또는 해독하는 디스크램블 키를 동일한 섹터로부터 재생하는 것이 바람직하다.

상기 바람직한 실시예에서, 키 영역을 할당하는 회로 또는 방법은 디스크램블 키의 기록된 상태를 나타내는 디스크램블 키 상태 영역에 예약 영역에 대한 플래그를 배치하여, 컨텐츠 데이터 재생시에 사용되는 키에 관한 정보를 기록하고, 또한 컨텐츠 데이터에 대하여 할당된 디스크램블 키의 기록 영역을 나타내는 키 인덱스를 기록하는 것이 바람직하다. 또한, 디스크램블 키를 배치하는 회로 또는 방법은 컨텐츠 정보 영역으로부터 컨텐츠에 사용된 디스크램블 키 영역의 키 인덱스를 재생하여, 기록된 디스크램블 키에 대응하는 키 인덱스에 표시된 디스크램블 키 영역에 디스크램블 키를 배치하고, 또한 기록된 디스크램블 키에 대응하는 키 인덱스에 표시된 디스크램블 키 상태 영역에, 기록되는 정보의 플래그를 배치하는 것이 바람직하다.

상기 바람직한 실시예에서, 광 디스크 재생장치는 디스크 식별 정보를 재생하고, 컨텐츠가 재생 가능한가 아닌가를 탐색하고, 키 관리 정보를 재생하고, 영상 데이터 또는 음악 데이터 등의 컨텐츠 데이터가 기록된 섹터를 재생하고, 또한 재생된 섹터로부터 디스크램블 키를 취득하는 것이 바람직하다. 또한, 재생된 컨텐츠 데이터를 디스크램블 키로써 디스크램블하여, 디스크램블된 데이터를 출력하는 것이 바람직하다.

상기 바람직한 실시예에서, 제1디스크 정보를 기록하는 제1정보 영역, 개별적인 디스크를 식별하는 제2디스크 정보를 기록하는 제2정보 영역, 및 광 빔을 조사함으로써 정보를 기록하는 사용자 데이터 영역을 갖는 광 디스크의 사용자 데이터 영역에 컨텐츠를 기록하는 경우, 컨텐츠 데이터 기록 방법은, 최소한 상기 제2디스크 정보를 사용하여 연산 또는 계산함으로써 디코딩하고 재생할 수 있도록 암호화된 컨텐츠를 기록하는 것이 바람직하다.

상기 바람직한 실시예에서, 제1디스크 정보를 기록하는 제1정보 영역, 개별적인 디스크를 식별하는 제2디스크 정보를 기록하는 제2정보 영역, 광 빔을 조사함으로써 정보를 기록하는 사용자 데이터 영역, 및 사용자 데이터 영역에 암호화되어 기록된 컨텐츠를 디코딩하거나 또는 암호 해독하기 위한 키 정보를 기록하는 키 정보 기록 영역을 갖는 광 디스크의 상기 사용자 데이터 영역에 컨텐츠를 기록하는 경우, 컨텐츠 데이터 기록 방법은, 최소한 제2디스크 정보 및 키 정보를 사용하여 연산 또는 계산함으로써 디코딩되고 재생될 수 있도록 정보를 암호화하여 기록하는 것이 바람직하다.

상기 바람직한 실시예에서, 복수의 연속 섹터에, 바람직하게는 AV 데이터를 포함하는 데이터 크기가 (주 데이터 크기) × (분할된 암호 해독 키의 수) 이하인 주 데이터 영역에, 복수의 분할된 암호 해독 키를 기록하는 암호 해독 키 영역을 갖는 광 디스크의 섹터에 더미 데이터가 기록된다. 또한, ECC 블록에는, 복수의 연속 섹터로 분할된 암호 해독 키를 기록하는 암호 해독 키 영역을 갖는 섹터가 (ECC 블록 단위)/(분할된 암호 해독 키의 수)에 해당하는 횟수만큼 기록되고, AV 데이터를 포함하는 데이터 크기가 (주 데이터 크기) ×(ECC 블록 단위) 이하인 주 데이터 영역에 더미 데이터가 기록된다.

상기 바람직한 실시예에서, AV 데이터를 포함하는 데이터에 대하여 실행된 암호를 해독하는 암호 해독 키를, 소정의 크기를 갖는 복수의 분할된 암호 해독 키로 분할하여, 복수의 분할된 암호 해독 키를, 암호 해독 키 테이블이 연속되는 복수의 암호 해독 키 영역에 기록하는 것이 바람직하다. 또한, 상기 암호 해독 키 테이블은 재기록 가능한 인입 영역 내의 주 데이터 영역에 기록하는 것이 바람직하다. 추가로, 암호 해독 키 테이블의 각각의 암호 해독 키 영역에는 암호 해독 키 테이블의 기록 상태를 나타내는 정보를 고정치로서 기록하는 것이 바람직하다. 또한, 암호 해독 키 테이블은 광 디스크의 내주 및 외주에 배치된 상기 상이한 ECC 블록에 복수 회 기록된다.

상기 바람직한 실시예에서, 데이터 암호화 장치의 인코딩 장치(3101), 및 광 디스크 기록 및 재생장치의 광 디스크 장치(3102)는 상호 인증 시스템의 버스 키를 공유하는 것이 바람직하다. 또한, 데이터 디코딩 장치의 디코딩 장치(3103), 및 광 디스크 기록 및 재생장치의 광 디스크 장치(3102)는 상호 인증 시스템의 버스 키를 공유하는 것이 바람직하다.

상기 바람직한 실시예에서, 데이터를 기록할 수 있고, 또한 RAM 타입을 포함하는 추기형의 또는 재기록 가능 방식 광 디스크, 또는 재기록 불가능 디스크 중 어느 하나인, 기록 방식의 광 디스크를 설명하였지만, 본 발명은 이것에 한정되지 않는다. 본 발명은, 이전에 기록된 데이터를 판독하고 재생할 수 있지만 데이터를 새로이 기록할 수 없는 판독 전용 방식의 광 디스크에 적용될 수 있다. 판독 전용 방식 광 디스크의 경우에, 데이터 기록 및 재생 영역은 데이터를 판독하고 재생하

는 데이터 재생 영역으로써 대체될 수 있고, 또한 컨텐츠 데이터 또는 기타의 여러가지 제어 정보 데이터는 제조시에 사전에 기록된다. 이 경우에, 기록 방식의 광 디스크는 CD-R, CD-RW, MO, MD, DVD-RAM 등을 포함한다. 판독 전용 방식의 광 디스크는 음악 CD, CD-ROM, DVD-ROM 등을 포함한다.

산업상 이용 가능성

상기에서 상세하게 설명한 바와 같이, 본 발명의 광 디스크에 의하면, 각각의 광 디스크에 대하여 기록 동작 및 재생 동작을 실행하는 데에 사용하는 디스크 식별 정보가 재기록 불가능한 판독 전용 영역에 기록되고, 광 디스크에의 또는 광 디스크로부터의 컨텐츠의 기록 동작 및 재생 동작은, 광 디스크의 제조시에 기록된 정보를 사용하여, 사용자에 의해서 제어될 수 있다.

또한, 본 발명의 광 디스크에 의하면, 재기록할 수 없는 판독 전용 디스크 식별 정보를 키로서 사용하여 암호화된 데이터가 광 디스크의 사용자 데이터 영역에 기록되어 있으므로, 사용자 데이터 영역이 사용자에 의해서 기록 방식의 또 다른 광 디스크에 복사되는 경우에도, 디스크 식별 정보는 복사될 수 없어서, 데이터의 올바른 암호 해독 및 재생이 불가능하게 된다.

또한, 본 발명의 광 디스크에 의하면, 암호화된 데이터, 및 암호를 해독하기 위한 디스크램블 키는 서로 상이한 섹터 영역에 기록되어서, 저작권 보호를 필요로 하는 영화 및 음악 등 데이터, 및 암호를 디스크램블하는 디스크램블 키를 독립적으로 취득할 수 있게 된다. 더욱이, 디스크 식별 정보를 키로서 사용하여 디스크램블 키를 암호화하여 기록함으로써, 디스크 식별 정보는 복사될 수 없고, 이로 인하여 사용자에 의해서 사용자 데이터 영역이 기록 방식의 또 다른 광 디스크에 복사되더라도 데이터를 올바르게 기록하고 재생할 수 없게 된다. 데이터가 복사되어 있는 광 디스크의 디스크 식별 정보를 키로서 사용하여 암호화된 디스크램블 키를 취득하여 기록함으로써, 데이터를 올바르게 기록하고 재생할 수 있게 된다.

또한, 본 발명에 의한 광 디스크는 제1디스크 정보를 기록하는 제1정보 영역, 개별적인 디스크를 식별하는 제2디스크 정보를 기록하는 제2정보 영역, 및 광 빔을 조사함으로써 정보를 기록하는 사용자 데이터 영역을 포함한다. 따라서, 종래 기술에 의한 광 디스크에, 상기 광 디스크를 식별하는 정보를 부가함으로써, 광 디스크의 관리가 용이하게 실행될 수 있다. 이 경우에, 상기 제2정보 영역은 상기 제1정보 영역에 기록되는 것이 바람직하고, 제2정보 영역의 데이터는 광 픽업으로써 상기 제1정보 영역을 재생함으로써 재생될 수 있다. 또한, 상기 제2정보 영역은 상기 제1정보 영역의 기록막을 부분적으로 제거함으로써 기록되어서, 반경 방향으로 연장되는 형상을 갖는 복수의 트리밍 영역이 형성되고, 이에 따라서, 상기 제2디스크 정보의 용이한 왜곡이 방지될 수 있다.

또한, 본 발명의 광 디스크에 의하면, 암호 해독 키가 복수의 암호 해독 키로 분할되어서, 섹터 헤더 영역에 배치되는 각각 소정 크기를 갖는 암호 해독 키 영역에 할당되거나, 또는 암호 해독 키가, 섹터 헤더 영역에 배치되는 키 인덱스 영역이 나타내는 암호 해독 키 영역에 기록된다. 이로 인하여, 섹터 헤더 영역내에 규정된 크기를 갖는 암호 해독 키 영역에 관계없이, 임의의 또는 자유로운 길이의 암호 해독 키를 사용할 수 있는 기록 방식의 광 디스크가 제공될 수 있다. 그러므로, 기록된 컨텐츠에 대한 저작권 보호 레벨에 따라서, 임의의 키 길이를 사용하는 암호를 사용할 수 있게 된다.

본 발명은 첨부 도면을 참조로 하여 바람직한 실시예로써 충분히 설명하였지만, 당업자에게는 각종 변경 및 변형이 있을 수 있다는 것을 유념해야 한다. 이러한 변경 및 변형은 첨부된 청구 범위로부터 벗어나지 않는 한 청구 범위에 의해서 정의된 바와 같이 본 발명의 범위내에 포함되는 것으로 이해하여야 한다.

도면의 간단한 설명

본 발명의 이러한 목적 및 기타의 목적과 특징은 첨부 도면을 참조로 하는 바람직한 실시예에 의한 이하의 설명으로부터 명백하게 되고, 또한 도면에 걸쳐서 유사한 부분은 동일한 참조 번호로써 표시되어 있다.

도 1은 본 발명에 의한 바람직한 제1실시예의 기록 방식 광 디스크(100)의 데이터 기록 영역을 나타내는 평면도.

도 2A는 도 1에 나타낸 광 디스크(100)의 BCA(106)를 형성하는 장치 구성을 나타내는 블록도 및 단면도.

도 2B는 도 1에 나타낸 광 디스크(100)의 BCA(106)의 형성후의 광 디스크(100)의 단면도, 및 반사광의 강도를 수평 방향으로 나타내는 그래프.

도 3은 도 1에 나타낸 BCA(106)의 기록 포맷을 나타내는 도면.

도 4는 도 1에 나타낸 사용자 데이터 영역(102) 내의 섹터 데이터(401)의 섹터 구조를 나타내는 도면.

도 5는 도 1에 나타낸 키 관리 정보 영역(107)의 구성을 나타내는 도면.

도 6A는 바람직한 제1실시예의 바람직한 변형 실시예에 의한, 도 1에 나타낸 섹터 데이터(401)에 디스크램블 키 및 AV 데이터를 기록하는 기록 방법을 나타내는 블록도.

도 6B는 바람직한 제1실시예에 의한, 도 1에 나타낸 섹터 데이터(401)에 디스크램블 키에 대한 키 인덱스 및 AV 데이터를 기록하는 기록 방법을 나타내는 블록도.

도 7은 본 발명에 의한 바람직한 제2실시예의 광 디스크 기록 및 재생장치의 구성을 나타내는 블록도.

도 8은 도 7에 나타낸 광 디스크 기록 및 재생장치의 제어 CPU(710)에 의해서 실행되는 AV 데이터의 기록 방법을 나타내는 흐름도.

도 9는 도 7에 나타낸 광 디스크 기록 및 재생장치의 제어 CPU(710)에 의해서 실행되는 키 관리 정보 영역의 할당 방법을 나타내는 흐름도.

도 10은 도 7에 나타낸 광 디스크 기록 및 재생장치의 제어 CPU(710)에 의해서 실행되는, 디스크램블 키의 기록 방법을 나타내는 흐름도.

도 11은 도 7에 나타낸 광 디스크 기록 및 재생장치의 제어 CPU(710)에 의해서 실행되는, AV 데이터의 재생 방법을 나타내는 흐름도.

도 12는 도 7에 나타낸 광 디스크 기록 및 재생장치의 제어 CPU(710)에 의해서 실행되는 디스크램블 키의 취득 방법을 나타내는 흐름도.

도 13은 바람직한 제1실시예의 바람직한 변형 실시예에 의해서, 암호화된 디스크램블 키를 근거로 하여 디스크램블 키가 정상적인가 아닌가를 판단하는 방법을 나타내는 블록도.

도 14는 바람직한 제1실시예의 바람직한 변형 실시예에 의한, 디스크램블 영역 관리 테이블의 구성을 나타내는 도면.

도 15A는 바람직한 제1실시예에서 컨텐츠가 기록될 때 지역 식별자가 기록되는 경우에 동일한 지역 내에서 또는 상이한 지역에서 컨텐츠의 복사 또는 재생이 가능한가 아닌가를 나타내는 도면.

도 15B는 바람직한 제1실시예에서 광 디스크가 운송될 때 지역 식별자가 이미 기록되어 있는 경우에 동일한 지역 내에서 또는 상이한 지역에서 컨텐츠의 복사 또는 재생이 가능한가 아닌가를 나타내는 도면.

도 16은 본 발명에 의한 바람직한 제3실시예의 광 디스크(1101)의 데이터 기록 영역을 나타내는 평면도.

도 17은 바람직한 제3실시예에 의한 BCA 재생 회로(1401)에서의 재생 신호 (1201)와 재생 2진 신호(1207)의 신호 파형을 나타내는 파형도.

도 18은 바람직한 제3실시예에 의한 BCA 재생 회로(1401)의 구성을 나타내는 블록도.

도 19는 바람직한 제3실시예에 의한 광 디스크 기록 및 재생 시스템의 구성을 나타내는 블록도.

도 20은 본 발명에 의한 바람직한 제4실시예의 광 디스크 기록 및 재생 시스템의 구성을 나타내는 블록도.

도 21은 본 발명에 의한 바람직한 제5실시예의 광 디스크(1601)의 데이터 기록 영역을 나타내는 평면도.

도 22는 바람직한 제5실시예에 의한 광 디스크 기록 및 재생 시스템의 구성을 나타내는 블록도.

도 23은 바람직한 제5실시예에 의한 ID 부가 테이블의 구성을 나타내는 테이블.

도 24는 바람직한 제3실시예의 바람직한 변형 실시예에 의한 광 디스크(1101a)의 데이터 기록 영역을 나타내는 평면도.

도 25는 바람직한 제5실시예의 바람직한 변형 실시예에 의한 광 디스크(1601a)의 데이터 기록 영역을 나타내는 평면도.

도 26은 본 발명의 바람직한 제6실시예에 의한, 광 디스크 상에서의 사용자 데이터 영역의 구성, 및 사용자 데이터 영역의 데이터로부터 암호화된 컨텐츠를 해독하는 광 디스크 재생장치의 구성을 나타내는 블록도.

도 27은 바람직한 제6실시예에 의한 광 디스크에서, 사용자 데이터 영역내로의 저작권 제어 정보 및 암호 해독 키의 배치, 및 주 데이터 영역내로의 암호화된 컨텐츠의 배치를 나타내는 블록도.

도 28은 바람직한 제6실시예에 의한 광 디스크에서, 복수의 섹터에 대하여 하나의 오류 검출 단위가 사용되는 경우의 배치를 나타내는 블록도.

도 29는 본 발명에 의한 바람직한 제7실시예의 광 디스크내의 인입 영역(lead-in area)(2401)과 사용자 데이터 영역(2402)의 구성, 및 인입 영역(2401)과 사용자 데이터 영역(2402)에 저장된 데이터로부터 암호화된 컨텐츠를 해독하는 광 디스크 재생장치의 구성을 나타내는 블록도.

도 30A는 바람직한 제7실시예에 의한 광 디스크내의 인입 영역의 주 데이터 영역에서의 암호 해독 키의 초기치에 의한 기록되지 않은 상태를 나타내는 경우의 데이터 구성을 나타내는 블록도.

도 30B는 바람직한 제7실시예에 의한 광 디스크내의 인입 영역의 주 데이터 영역에서의 암호 해독 키 상태 테이블에 의한 기록된 상태를 나타내는 경우의 데이터 구성을 나타내는 블록도.

도 31은 바람직한 제7실시예에 의한 광 디스크에서의 암호 해독 키의 배치를 나타내는 블록도.

도 32는 본 발명에 의한 바람직한 제8실시예의 파일 관리 시스템에 의한 광 디스크의 데이터를 관리하는 데이터 구성을 나타내는 블록도.

도 33은 바람직한 제8실시예에 의한 파일 관리 시스템에 의해서 실행되는 저작권 보호를 필요로 하는 컨텐츠의 기록 방법을 나타내는 흐름도.

도 34는 바람직한 제8실시예에 의한 파일 관리 시스템에 의해서 실행되는 컨텐츠의 재생 방법을 나타내는 흐름도.

도 35는 바람직한 제8실시예에 의한 파일 관리 시스템에 의해서 실행되는 컨텐츠의 삭제 방법을 나타내는 흐름도.

도 36은 본 발명에 의한 바람직한 제9실시예의 광 디스크 시스템의 구성을 나타내는 블록도.

도 37은 본 발명에 의한 바람직한 제10실시예의 광 디스크 내의 사용자 데이터 영역의 구성, 컨텐츠를 암호화하여 사용자 데이터 영역에 기록하는 광 디스크 기록장치의 구성, 및 사용자 데이터 영역에 저장된 데이터로부터의 암호화된 컨텐츠를 해독하는 광 디스크 재생장치의 구성을 나타내는 블록도.

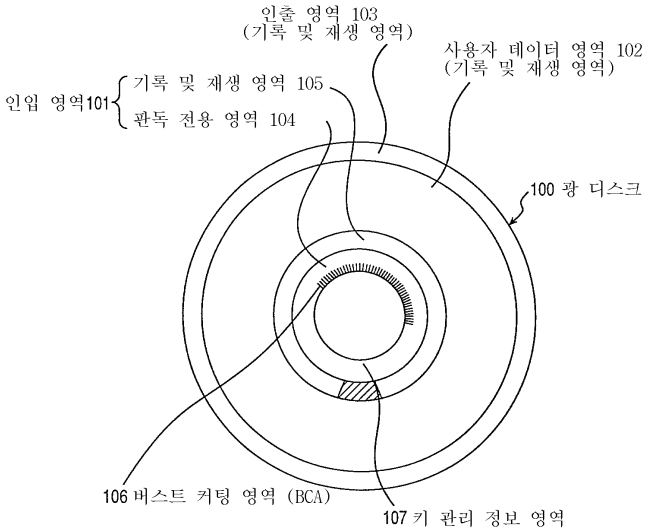
도 38은 본 발명에 의한 바람직한 제11실시예의 광 디스크 내의 사용자 데이터 영역의 구성, 컨텐츠를 암호화하여 사용자 데이터 영역에 기록하는 광 디스크 기록장치의 구성, 및 사용자 데이터 영역의 데이터로부터의 암호화된 컨텐츠를 해독하는 광 디스크 재생장치의 구성을 나타내는 블록도.

도 39는 종래 기술에 의한, DVD-ROM의 사용자 데이터 영역의 구성, 및 사용자 데이터 영역의 데이터로부터의 암호화된 컨텐츠를 해독하는 광 디스크 재생장치의 구성을 나타내는 블록도.

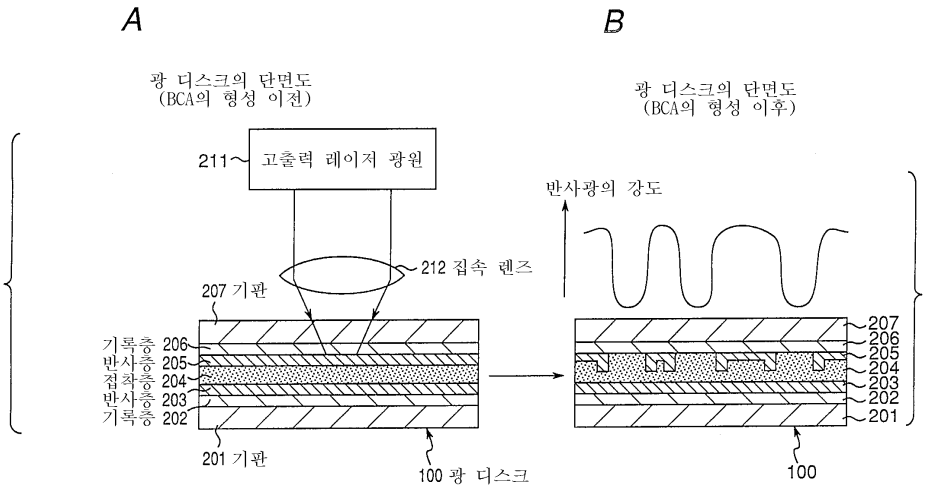
도면

도면1

바람직한 제1실시예

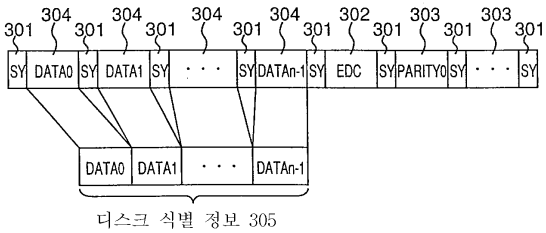


도면2



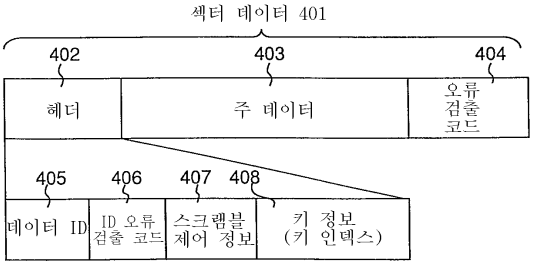
도면3

BCA 106의 기록 포맷

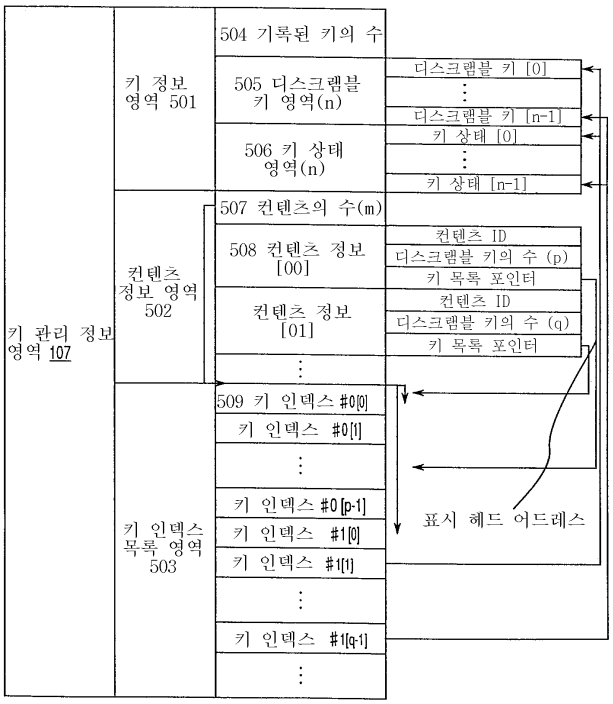


도면4

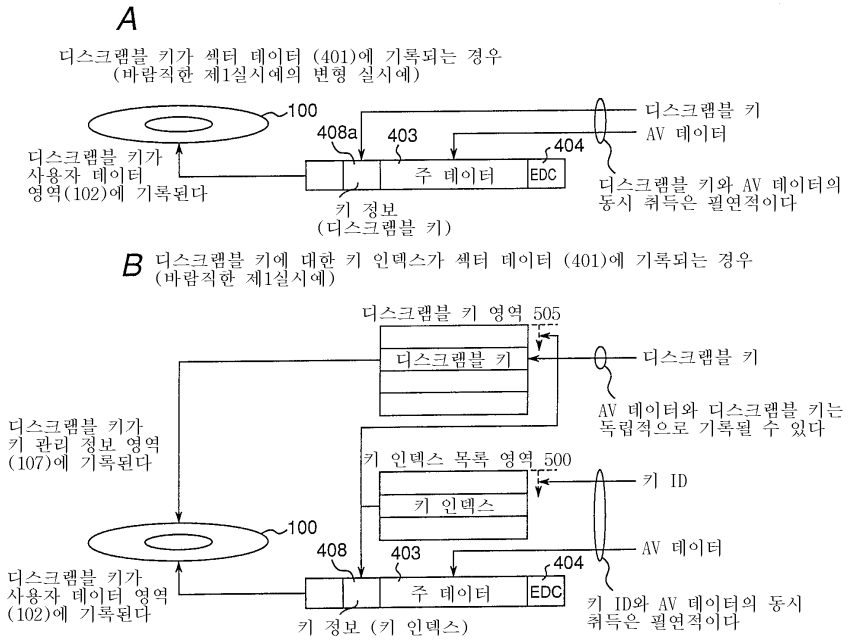
사용자 데이터 영역 102 내의 섹터 데이터 401의 섹터 구조



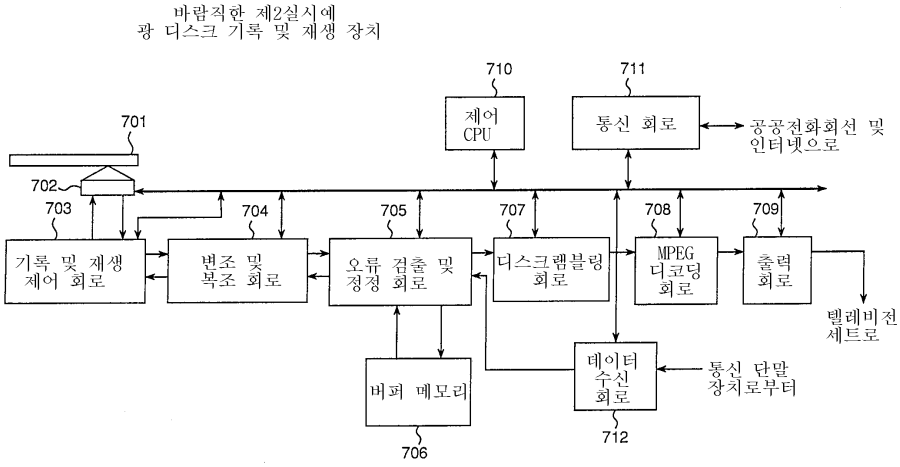
도면5



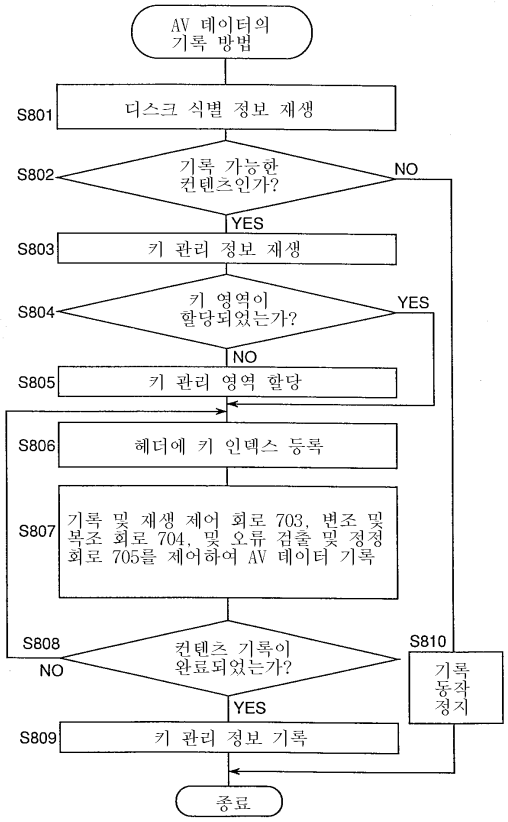
도면6


A
디스크램블 키가 섹터 데이터 (401)에 기록되는 경우
(바람직한 제1실시예의 변형 실시예)
100
408a
403
404
주 데이터
EDC
디스크램블 키
AV 데이터
디스크램블 키가
사용자 데이터
영역(102)에 기록된다
디스크램블 키와 AV 데이터의
동시 취득은 필연적이다
키 정보
(디스크램블 키)
B 디스크램블 키에 대한 키 인덱스가 섹터 데이터 (401)에 기록되는 경우
(바람직한 제1실시예)
디스크램블 키 영역 505
디스크램블 키
디스크램블 키
AV 데이터와 디스크램블 키는
독립적으로 기록될 수 있다
디스크램블 키가
키 관리 정보 영역
(107)에 기록된다
키 인덱스 목록 영역 500
키 인덱스
키 ID
AV 데이터
100
408
403
404
주 데이터
EDC
디스크램블 키가
사용자 데이터 영역
(102)에 기록된다
키 정보 (키 인덱스)
키 ID와 AV 데이터의 동시
취득은 필연적이다

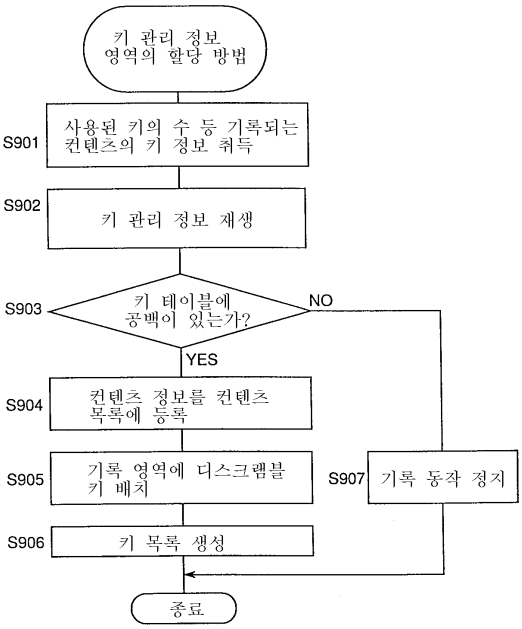
도면7


바람직한 제2실시예
광 디스크 기록 및 재생 장치
710
711
제어
CPU
통신 회로
공공전화회선 및
인터넷으로
701
702
703
704
705
707
708
709
기록 및 재생
제어 회로
변조 및
복조 회로
오류 검출 및
정정 회로
디스크램블링
회로
MPEG
디코딩
회로
출력
회로
텔레비전
세트로
버퍼 메모리
706
데이터
수신
회로
712
통신 단말
장치로부터

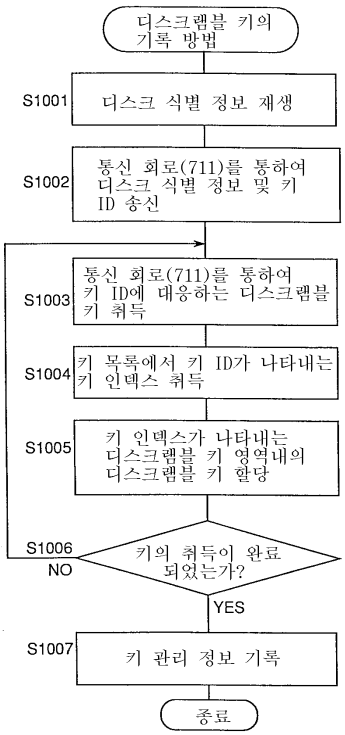
도면8


AV 데이터의 기록 방법
S801
디스크 식별 정보 재생
S802
기록 가능한 컨텐츠인가?
NO
YES
S803
키 관리 정보 재생
S804
키 영역이 할당되었는가?
YES
NO
S805
키 관리 영역 할당
S806
헤더에 키 인덱스 등록
S807
기록 및 재생 제어 회로 703, 변조 및 복조 회로 704, 및 오류 검출 및 정정 회로 705를 제어하여 AV 데이터 기록
S808
컨텐츠 기록이 완료되었는가?
NO
YES
S810
기록 동작 정지
S809
키 관리 정보 기록
종료

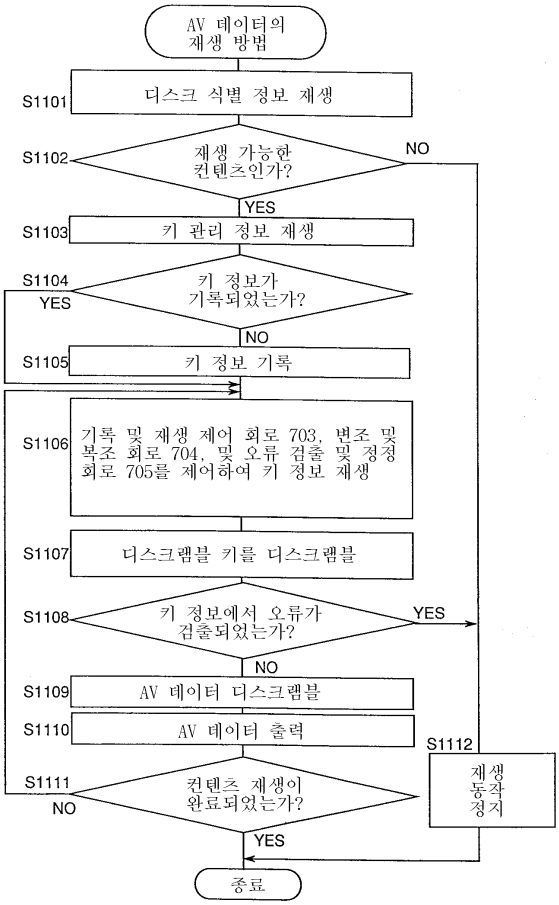
도면9


키 관리 정보 영역의 할당 방법
S901
사용된 키의 수 등 기록되는 컨텐츠의 키 정보 취득
S902
키 관리 정보 재생
S903
키 테이블에 공백이 있는가?
NO
YES
S904
컨텐츠 정보를 컨텐츠 목록에 등록
S905
기록 영역에 디스크램블 키 배치
S906
키 목록 생성
S907
기록 동작 정지
종료

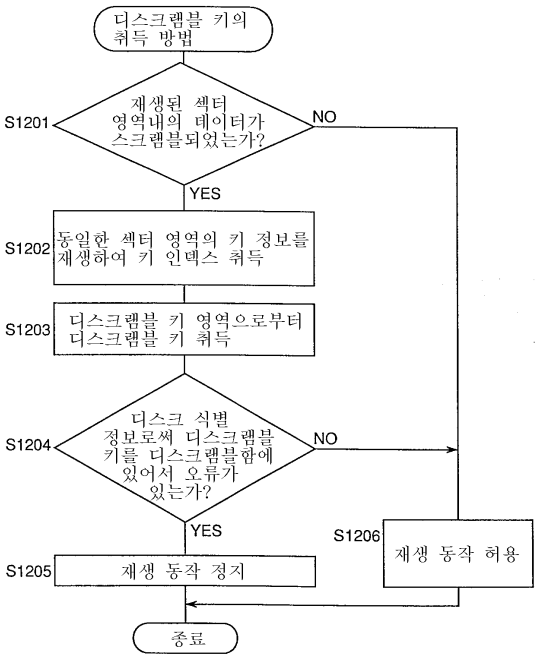
도면10


디스크램블 키의 기록 방법
S1001
디스크 식별 정보 재생
S1002
통신 회로(711)를 통하여 디스크 식별 정보 및 키 ID 송신
S1003
통신 회로(711)를 통하여 키 ID에 대응하는 디스크램블 키 취득
S1004
키 목록에서 키 ID가 나타내는 키 인덱스 취득
S1005
키 인덱스가 나타내는 디스크램블 키 영역내의 디스크램블 키 할당
S1006
키의 취득이 완료 되었는가?
NO
YES
S1007
키 관리 정보 기록
종료

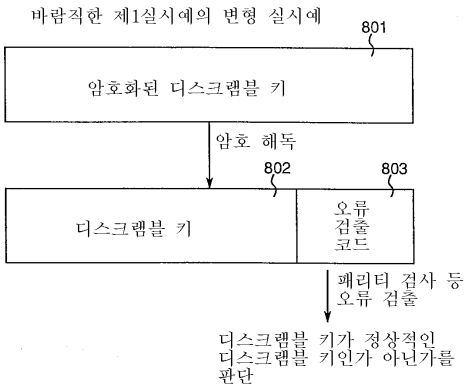
도면11


AV 데이터의 재생 방법
S1101
디스크 식별 정보 재생
S1102
재생 가능한 컨텐츠인가?
NO
YES
S1103
키 관리 정보 재생
S1104
키 정보가 기록되었는가?
YES
NO
S1105
키 정보 기록
S1106
기록 및 재생 제어 회로 703, 변조 및 복조 회로 704, 및 오류 검출 및 정정 회로 705를 제어하여 키 정보 재생
S1107
디스크램블 키를 디스크램블
S1108
키 정보에서 오류가 검출되었는가?
YES
NO
S1109
AV 데이터 디스크램블
S1110
AV 데이터 출력
S1111
컨텐츠 재생이 완료되었는가?
NO
YES
S1112
재생 동작 정지
종료

도면12



도면13



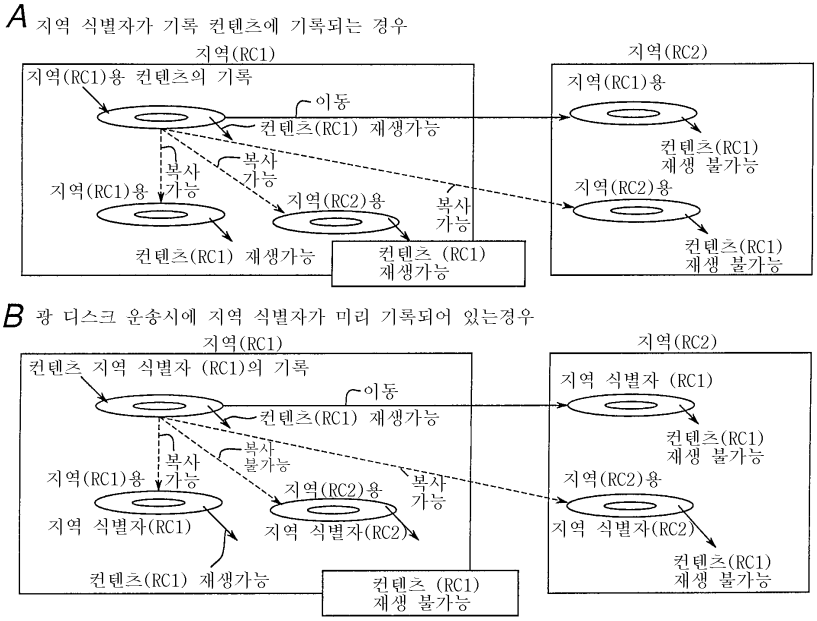
도면14

바람직한 제1실시예의 변형 실시예

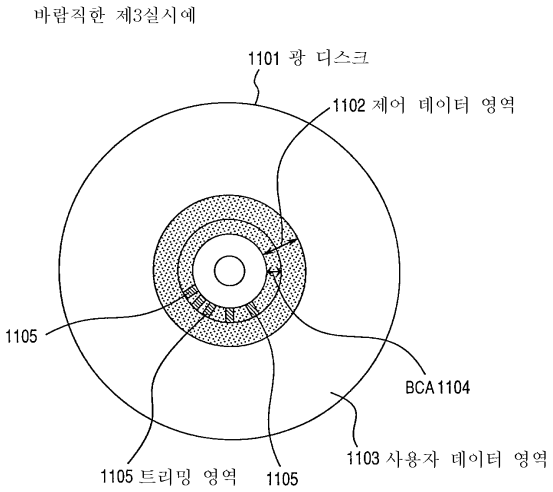
디스크램블 영역 관리 테이블

1	시작 어드레스 1	종료 어드레스 1	디스크램블 키 1
2	시작 어드레스 2	종료 어드레스 2	디스크램블 키 2
⋮	⋮	⋮	⋮
n	시작 어드레스 n	종료 어드레스 n	디스크램블 키 n

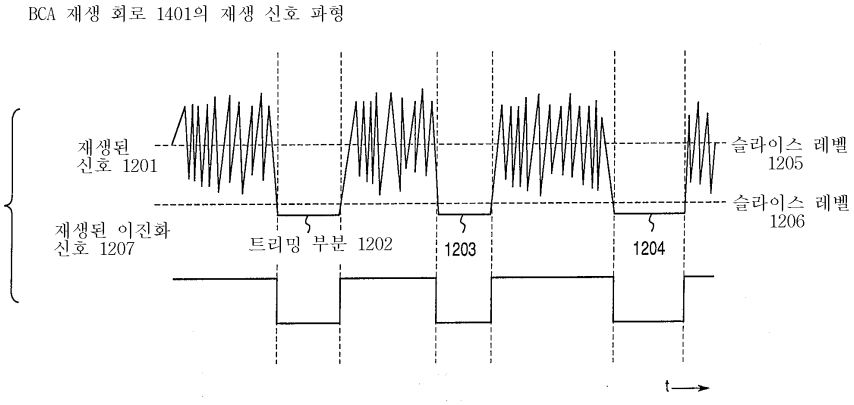
도면15



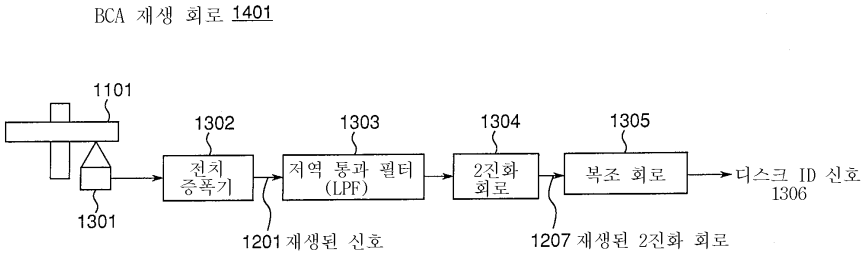
도면16



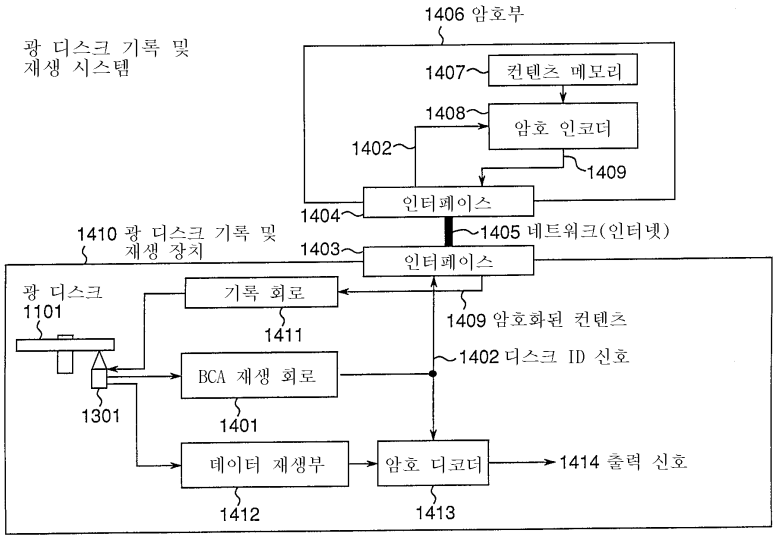
도면17



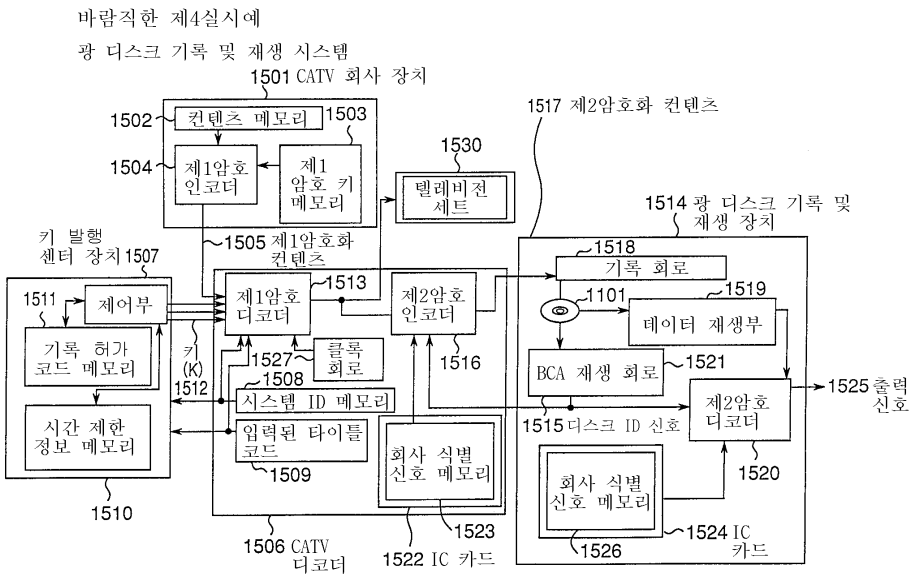
도면18



도면19

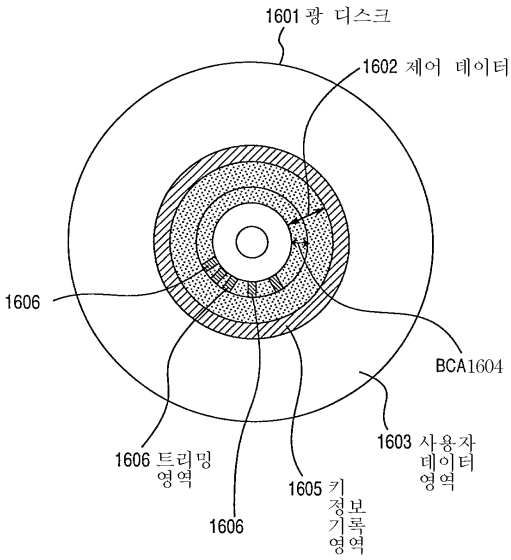


도면20



도면21

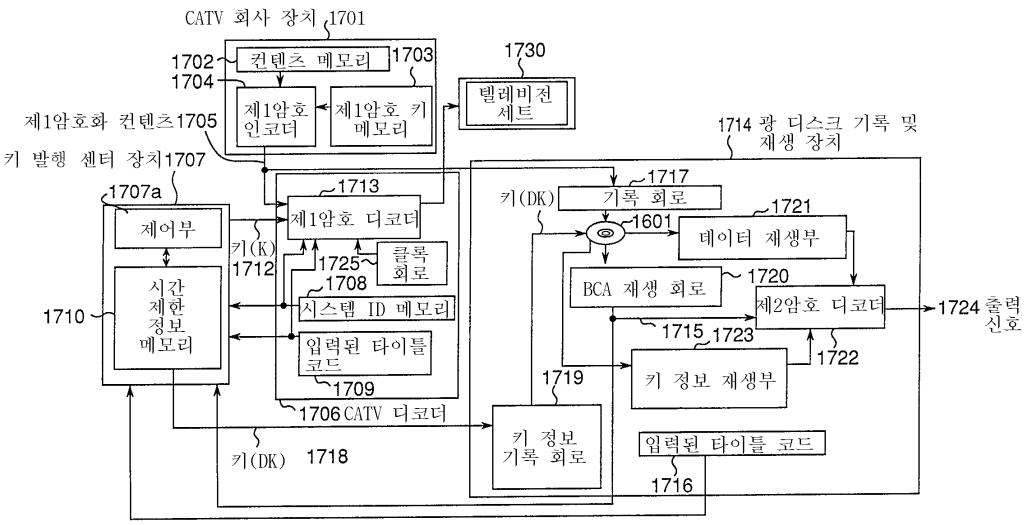
바람직한 제5실시예



도면22

바람직한 제5실시예

광 디스크 기록 및 재생 시스템



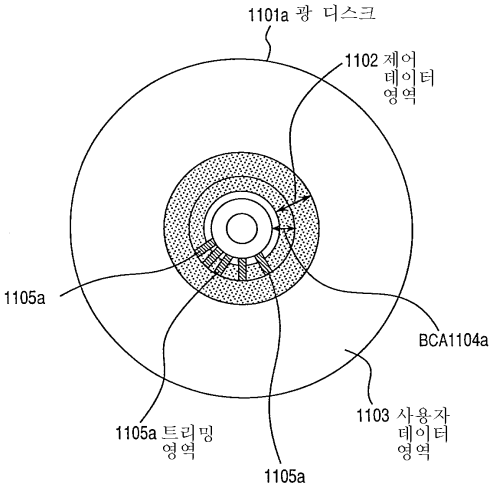
도면23

ID 부가 테이블

타이틀 코드 T		T1	T2	T3
제1암호 해독 키 FK		FK1	FK2	FK3
시간 제한 정보 TIME		TIME1	TIME2	TIME3
시스템 ID	DID1	K11	K12	K13
	DID2	K21	K22	K23
	DID3	K23	K32	K33
디스크 ID	BCAS1	DK11	DK12	DK13
	BCAS2	DK21	DK22	DK23
	BCAS3	DK31	DK32	DK33

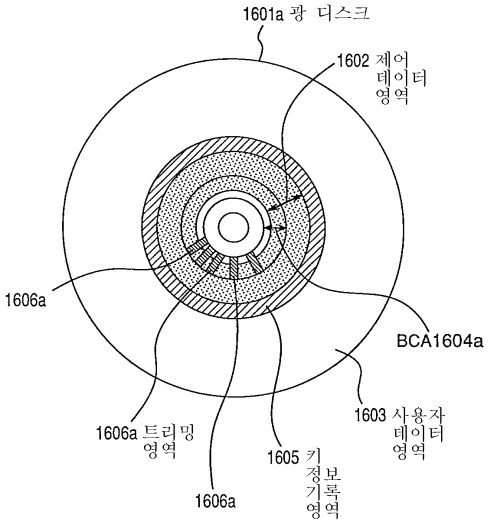
도면24

바람직한 제3실시예 변형 실시예

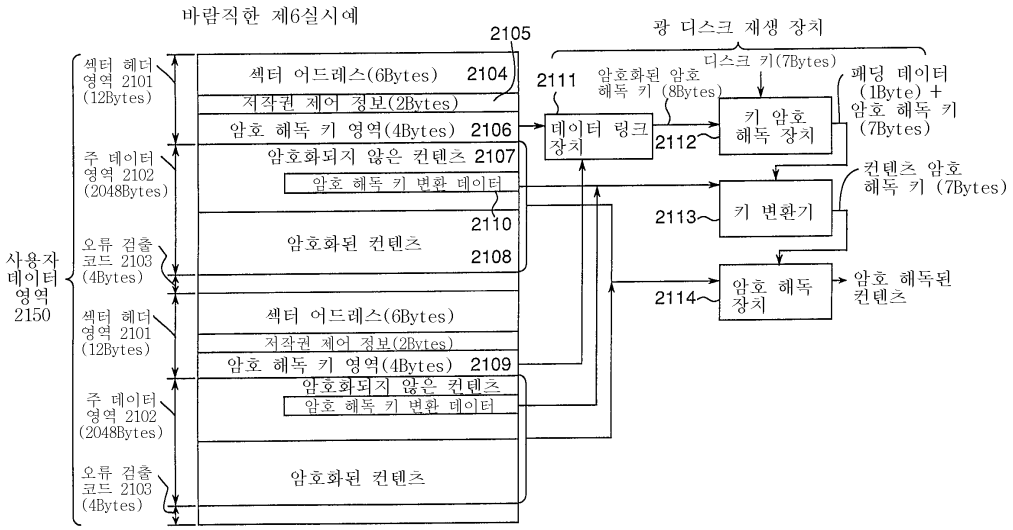


도면25

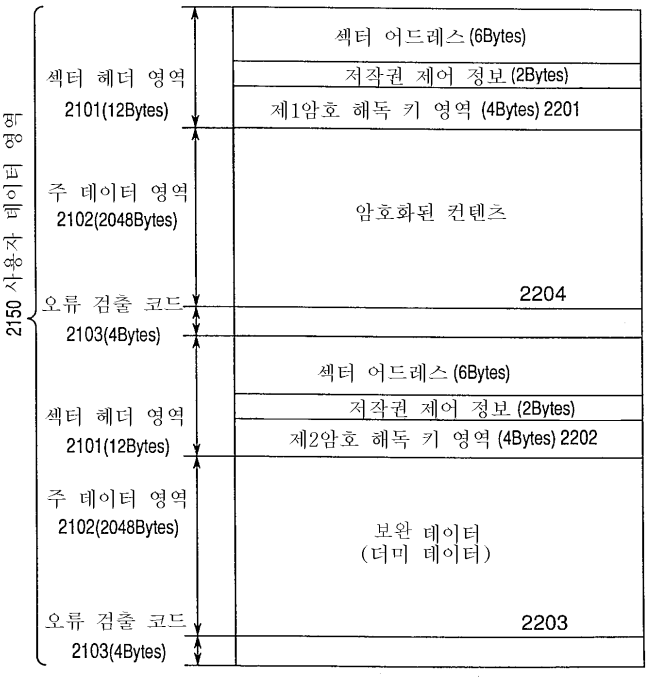
바람직한 제5실시예의 변형 실시예



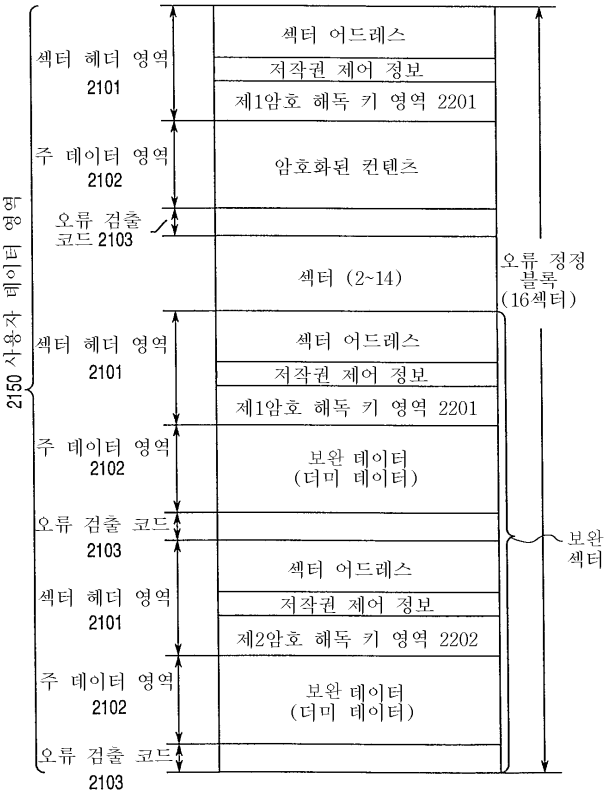
도면26


바람직한 제6실시예
광 디스크 제생 장치
2105
섹터 헤더 영역 2101 (12Bytes)
섹터 어드레스(6Bytes) 2104
저작권 제어 정보(2Bytes)
암호 해독 키 영역(4Bytes) 2106
주 데이터 영역 2102 (2048Bytes)
암호화되지 않은 컨텐츠 2107
암호 해독 키 변환 데이터
2110
암호화된 컨텐츠
2108
오류 검출 코드 2103 (4Bytes)
사용자 데이터 영역 2150
섹터 헤더 영역 2101 (12Bytes)
섹터 어드레스(6Bytes)
저작권 제어 정보(2Bytes)
암호 해독 키 영역(4Bytes) 2109
주 데이터 영역 2102 (2048Bytes)
암호화되지 않은 컨텐츠
암호 해독 키 변환 데이터
암호화된 컨텐츠
오류 검출 코드 2103 (4Bytes)
디스크 키(7Bytes)
2111
암호화된 암호 해독 키 (8Bytes)
데이터 링크 장치
2112
키 암호 해독 장치
패딩 데이터 (1Byte) + 암호 해독 키 (7Bytes)
컨텐츠 암호 해독 키 (7Bytes)
2113
키 변환기
2114
암호 해독 장치
암호 해독된 컨텐츠

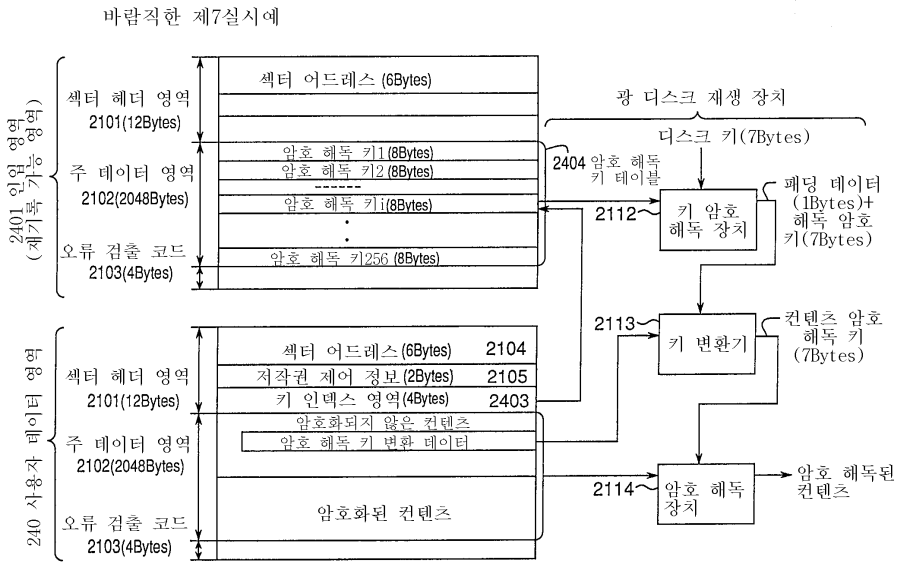
도면27


2150 사용자 데이터 영역
섹터 헤더 영역 2101(12Bytes)
섹터 어드레스 (6Bytes)
저작권 제어 정보 (2Bytes)
제1암호 해독 키 영역 (4Bytes) 2201
주 데이터 영역 2102(2048Bytes)
암호화된 컨텐츠
2204
오류 검출 코드 2103(4Bytes)
섹터 헤더 영역 2101(12Bytes)
섹터 어드레스 (6Bytes)
저작권 제어 정보 (2Bytes)
제2암호 해독 키 영역 (4Bytes) 2202
주 데이터 영역 2102(2048Bytes)
보완 데이터 (더미 데이터)
2203
오류 검출 코드 2103(4Bytes)

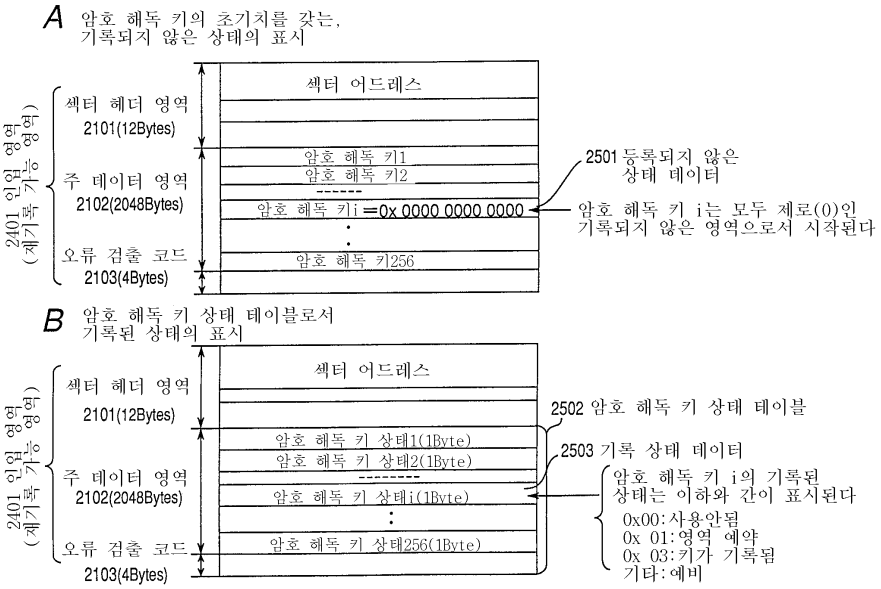
도면28


2150 사용자 데이터 영역
섹터 헤더 영역
2101
주 데이터 영역
2102
오류 검출 코드 2103
섹터 어드레스
저작권 제어 정보
제1암호 해독 키 영역 2201
암호화된 컨텐츠
섹터 (2~14)
오류 정정 블록 (16섹터)
보완 섹터
보완 데이터 (더미 데이터)
제2암호 해독 키 영역 2202

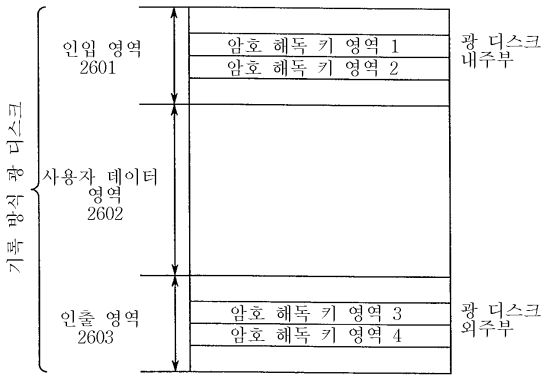
도면29


바람직한 제7실시예
2401 인덱 영역 (제거록 가능 영역)
240 사용자 데이터 영역
섹터 헤더 영역 2101(12Bytes)
주 데이터 영역 2102(2048Bytes)
오류 검출 코드 2103(4Bytes)
섹터 어드레스 (6Bytes)
암호 해독 키1 (8Bytes)
암호 해독 키2 (8Bytes)
암호 해독 키i (8Bytes)
암호 해독 키256 (8Bytes)
광 디스크 재생 장치
디스크 키(7Bytes)
2404 암호 해독 키 테이블
2112
키 암호 해독 장치
패딩 데이터 (1Bytes)+ 해독 암호 키(7Bytes)
2113
키 변환기
컨텐츠 암호 해독 키 (7Bytes)
섹터 어드레스 (6Bytes) 2104
저작권 제어 정보 (2Bytes) 2105
키 인덱스 영역 (4Bytes) 2403
암호화되지 않은 컨텐츠
암호 해독 키 변환 데이터
암호화된 컨텐츠
2114
암호 해독 장치
암호 해독된 컨텐츠

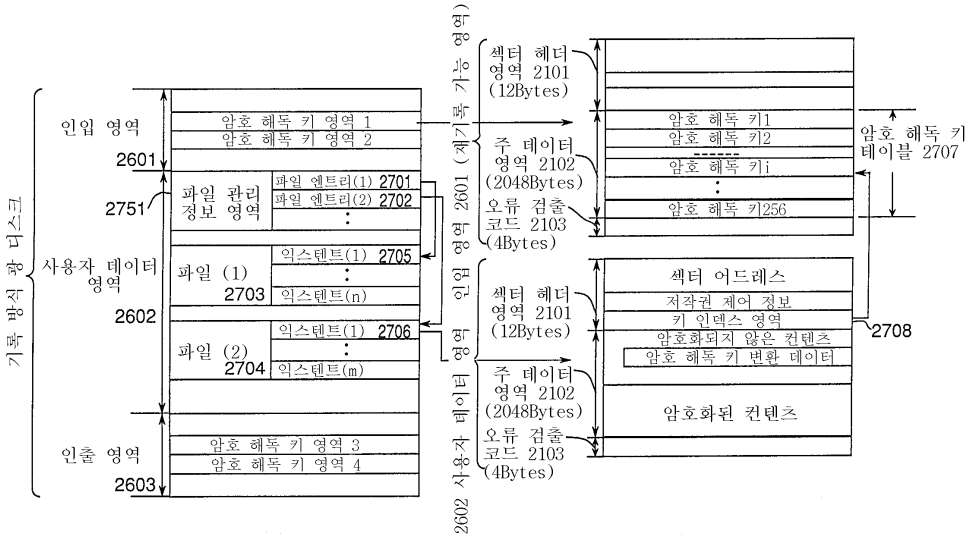
도면30



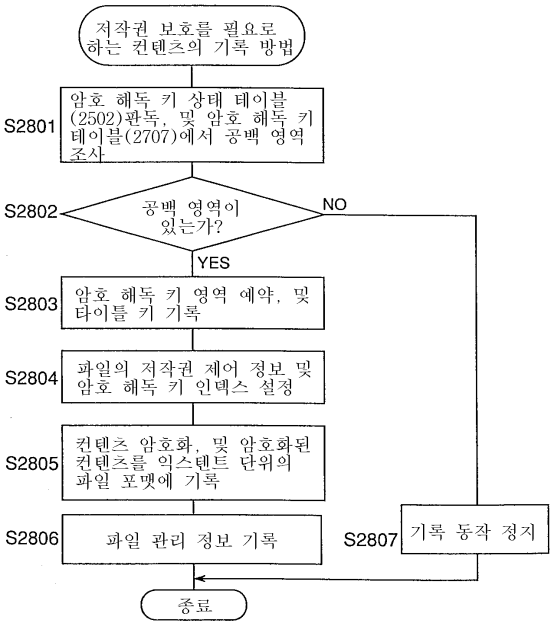
도면31



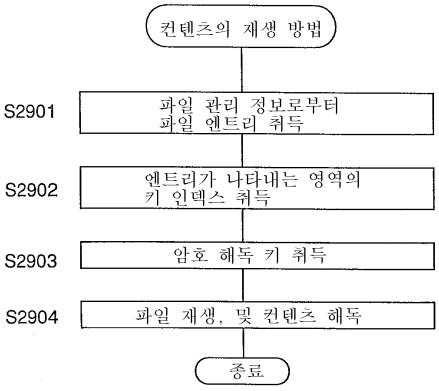
도면32



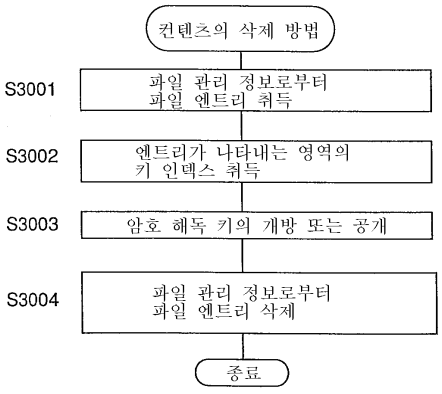
도면33



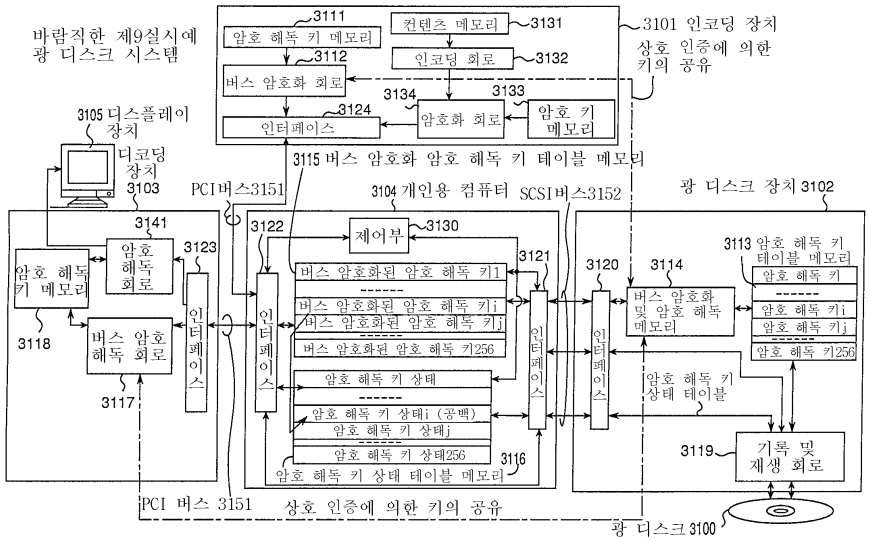
도면34



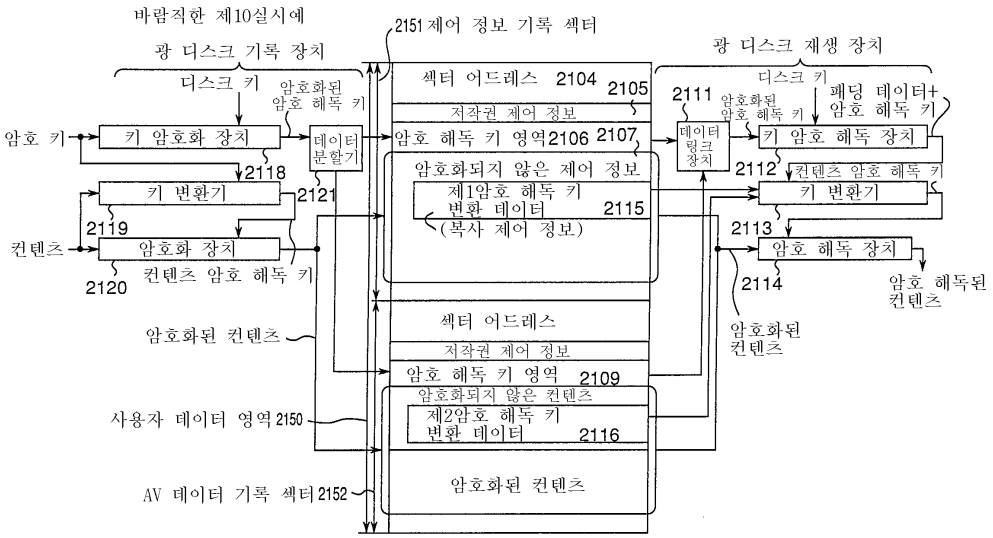
도면35



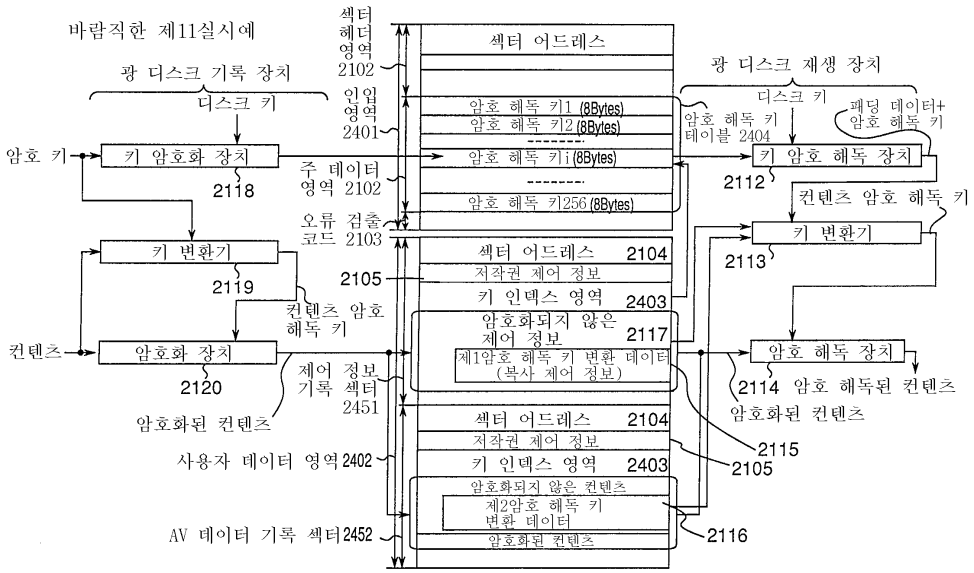
도면36


바람직한 제9실시예
광 디스크 시스템
3111
암호 해독 키 메모리
컨텐츠 메모리
3131
3101 인코딩 장치
상호 인증에 의한
키의 공유
3112
버스 암호화 회로
인코딩 회로
3132
3134
3133
3124
인터페이스
암호화 회로
암호 키
메모리
3105 디스플레이
장치
디코딩
장치
3103
3115 버스 암호화 암호 해독 키 테이블 메모리
PCI버스3151
3104 개인용 컴퓨터
SCSI버스3152
광 디스크 장치 3102
3141
3122
제어부
3130
3123
3121
3120
3114
3113 암호 해독 키
테이블 메모리
암호 해독
키 메모리
암호
해독
회로
버스 암호화된 암호 해독 키1
버스 암호화된 암호 해독 키i
버스 암호화된 암호 해독 키j
버스 암호화된 암호 해독 키256
버스 암호화
및 암호 해독
메모리
암호 해독 키
암호 해독 키i
암호 해독 키j
암호 해독 키256
3118
버스 암호
해독 회로
인터
페이스
암호 해독 키 상태
암호 해독 키 상태i (공백)
암호 해독 키 상태j
암호 해독 키 상태256
암호 해독 키 상태 테이블 메모리
3116
암호 해독 키
상태 테이블
3119
기록 및
재생 회로
3117
PCI 버스 3151
상호 인증에 의한 키의 공유
광 디스크 3100

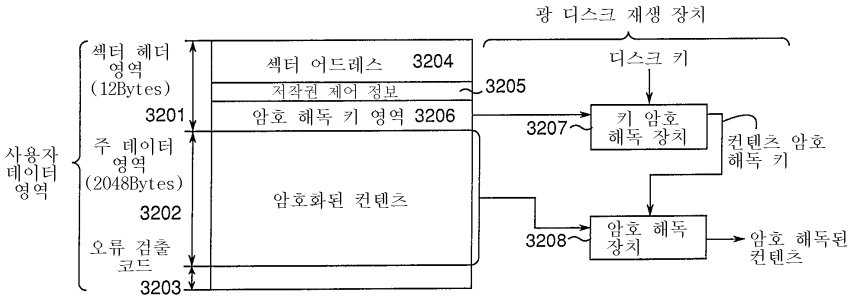
도면37


바람직한 제10실시예
광 디스크 기록 장치
2151 제어 정보 기록 섹터
광 디스크 재생 장치
디스크 키
암호화된
암호 해독 키
섹터 어드레스 2104
2105
디스크 키
2111
암호화된
암호 해독 키
패딩 데이터+
암호 해독 키
저작권 제어 정보
암호 키
키 암호화 장치
데이터
분할기
암호 해독 키 영역2106
2107
데이터
링크
장치
키 암호 해독 장치
2118
암호화되지 않은 제어 정보
2112
컨텐츠 암호 해독 키
키 변환기
2121
제1암호 해독 키
변환 데이터
2115
(복사 제어 정보)
키 변환기
2119
2113
컨텐츠
암호화 장치
암호 해독 장치
2120
컨텐츠 암호 해독 키
2114
암호 해독된
컨텐츠
섹터 어드레스
암호화된 컨텐츠
저작권 제어 정보
암호화된
컨텐츠
암호 해독 키 영역 2109
암호화되지 않은 컨텐츠
사용자 데이터 영역 2150
제2암호 해독 키
변환 데이터
2116
암호화된 컨텐츠
AV 데이터 기록 섹터 2152

도면38


바람직한 제11실시예
광 디스크 기록 장치
디스크 키
암호 키
키 암호화 장치
2118
키 변환기
2119
암호화 장치
2120
컨텐츠
암호화된 컨텐츠
사용자 데이터 영역 2402
AV 데이터 기록 섹터 2452
섹터 헤더 영역 2102
인입 영역 2401
주 데이터 영역 2102
오류 검출 코드 2103
컨텐츠 암호 해독 키
제어 정보 기록 섹터 2451
섹터 어드레스
암호 해독 키1 (8Bytes)
암호 해독 키2 (8Bytes)
암호 해독 키i (8Bytes)
암호 해독 키256 (8Bytes)
섹터 어드레스 2104
저작권 제어 정보
2105
키 인덱스 영역 2403
암호화되지 않은 제어 정보 2117
제1암호 해독 키 변환 데이터 (복사 제어 정보)
섹터 어드레스 2104
저작권 제어 정보
키 인덱스 영역 2403
암호화되지 않은 컨텐츠
제2암호 해독 키 변환 데이터
암호화된 컨텐츠
2115
2105
2116
광 디스크 재생 장치
디스크 키
암호 해독 키 테이블 2404
패딩 데이터+암호 해독 키
키 암호 해독 장치
2112
컨텐츠 암호 해독 키
키 변환기
2113
암호 해독 장치
2114
암호 해독된 컨텐츠
암호화된 컨텐츠

도면39


종래 기술
광 디스크 재생 장치
디스크 키
섹터 헤더 영역 (12Bytes)
3201
주 데이터 영역 (2048Bytes)
3202
오류 검출 코드
3203
사용자 데이터 영역
섹터 어드레스 3204
3205
저작권 제어 정보
암호 해독 키 영역 3206
3207
키 암호 해독 장치
컨텐츠 암호 해독 키
암호화된 컨텐츠
3208
암호 해독 장치
암호 해독된 컨텐츠