(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년03월07일
(11) 등록번호 10-1019321
(24) 등록일자 2011년02월24일

(51) Int. Cl.
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)
H04L 29/06 (2006.01) *G06F 17/00* (2006.01)
(21) 출원번호 10-2005-7012644
(22) 출원일자(국제출원일자) 2004년01월13일
심사청구일자 2008년12월09일
(85) 번역문제출일자 2005년07월06일
(65) 공개번호 10-2005-0091763
(43) 공개일자 2005년09월15일
(86) 국제출원번호 PCT/JP2004/000155
(87) 국제공개번호 WO 2004/064313
국제공개일자 2004년07월29일
(30) 우선권주장
JP-P-2003-00007349 2003년01월15일 일본(JP)
JP-P-2003-00101455 2003년04월04일 일본(JP)
(56) 선행기술조사문헌
EP01176754 A2*
WO2002060116 A2*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
파나소닉 주식회사
일본 오오사카후 가도마시 오오아자 가도마 1006 반치
(72) 발명자
나카노 도시히사
일본국 오오사카후 네야가와시 시메노 3-35-15
오모리 모토지
일본국 오오사카후 히라카타시 히가시타미야 1-7-30-103
(뒷면에 계속)
(74) 대리인
김영철

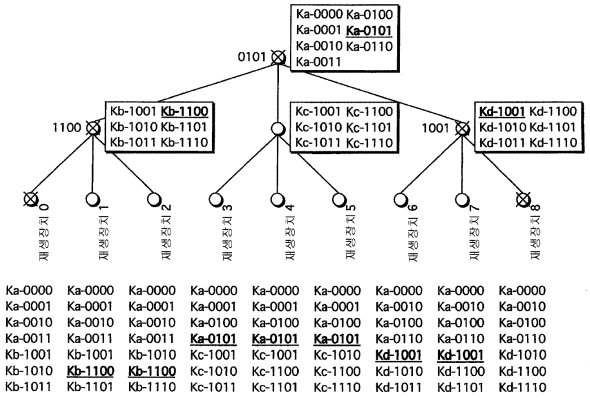
전체 청구항 수 : 총 25 항 심사관 : 정은선

(54) 콘텐츠 보호 시스템, 키 데이터 생성장치 및 단말장치

(57) 요 약

콘텐츠 보호 시스템은 장치 키들의 고유성을 체크하지 않고 불법 키 취득을 방지한다. 콘텐츠 보호 시스템은 키 데이터 생성장치와 사용자 단말을 포함한다. 키 데이터 생성장치는 콘텐츠를 이용하기 위한 제 1 키 데이터를 기설정된 변환 규칙에 근거하여 변환함으로써 제 2 키 데이터를 생성하고, 유효 단말이 보유한 장치 키를 이용하여 제 2 키 데이터를 암호화하며, 암호화된 키 데이터를 출력한다. 사용자 단말은 암호화된 키 데이터를 취득하고, 사용자 단말이 보유한 장치 키를 이용하여 암호화된 키 데이터를 해독함으로써 제 2 키 데이터를 생성하고, 상기 변환 규칙에 대응하는 재변환 규칙에 근거하여 제 2 키 데이터를 변환함으로써 제 1 키 데이터를 생성하고, 생성된 제 1 키 데이터를 이용하여 콘텐츠를 이용한다.

대 표 도



(72) 발명자

마츠자키 나츠메

일본국 오오사카후 미노시 아오신케 2-10-11

다테바야시 마코토

일본국 효고켄 다카라즈카시 메후 1-16-21

야마모토 나오키

일본국 오오사카후 네야가와시 간소즈카쵸 8-3

이시하라 히데시

일본국 오오사카후 가타노시 이쿠노 1-10-120

특허청구의 범위

청구항 1

정당한 단말장치만이 콘텐츠를 이용할 수 있는 저작물 보호시스템으로,

키 데이터 생성장치와 단말장치를 포함하며,

상기 키 데이터 생성장치는,

트리구조의 각 노드에 1 이상의 장치 키(device key)를 대응시켜서 각 단말장치가 갖는 장치 키를 규정하는 키 관리수단과,

규정되어 있는 장치 키에서 1 이상의 장치 키를 선택하는 선택수단과,

콘텐츠를 이용하기 위해서 이용하는 제 1 키 데이터를 상기 트리구조에서의 상기 선택한 장치 키에 대응하는 노드의 위치에 따라서 정해지는 정보인 변환정보를 이용해서 변환하여 제 2 키 데이터를 생성하는 변환수단과,

정당한 단말장치만이 보유하는 장치 키를 이용해서 상기 제 2 키 데이터를 암호화하여 암호화 키 데이터를 생성하는 암호화수단과,

상기 암호화 키 데이터를 출력하는 출력수단으로 구성되고,

상기 단말장치는,

암호화 키 데이터를 취득하는 취득수단과,

상기 암호화 키 데이터를 당해 단말장치가 보유하는 장치 키를 이용해서 복호하여 제 2 키 데이터를 생성하는 복호수단과,

상기 제 2 키 데이터를 상기 트리구조에서의 상기 장치 키에 대응하는 노드의 위치에 따라서 정해지는 정보인 변환정보를 이용해서 재변환하여 제 1 키 데이터를 생성하는 변환수단과,

상기 제 1 키 데이터를 이용해서 콘텐츠를 이용하는 콘텐츠 이용수단으로 구성되는 것을 특징으로 하는 저작물 보호시스템.

청구항 2

정당한 단말장치만이 콘텐츠를 이용할 수 있도록 키 데이터를 생성하는 키 데이터 생성장치로,

트리구조의 각 노드에 1 이상의 장치 키를 대응시켜서 각 단말장치가 갖는 장치 키를 규정하는 키 관리수단과,

규정되어 있는 장치 키에서 1 이상의 장치 키를 선택하는 선택수단과,

콘텐츠를 이용하기 위해서 이용하는 제 1 키 데이터를 선택한 상기 장치 키에 대응하는 노드의 상기 트리구조에서의 위치에 따라서 정해지는 정보인 변환정보를 이용해서 변환하여 제 2 키 데이터를 생성하는 변환수단과,

선택한 상기 장치 키를 이용해서 상기 제 2 키 데이터를 암호화하여 암호화 키 데이터를 생성하는 암호화수단과,

상기 암호화 키 데이터를 출력하는 출력수단을 포함하는 것을 특징으로 하는 키 데이터 생성장치.

청구항 3

청구항 2에 있어서,

상기 변환수단은 상기 장치 키에 대해서 변환정보를 생성하고, 생성한 정보와 상기 제 1 키 데이터로 역변환 가능한 연산을 실행하여 상기 제 2 키 데이터를 생성하며,

상기 출력수단은 상기 변환정보를 더 출력하는 하는 것을 특징으로 하는 키 데이터 생성장치.

청구항 4

청구항 3에 있어서,

상기 선택수단은 상기 트리구조에서 상기 정당한 단말장치만이 보유하는 장치 키 중 최상위층에 위치하는 노드에 대응되어 있는 1 이상의 장치 키를 선택하는 것을 특징으로 하는 키 데이터 생성장치.

청구항 5

청구항 4에 있어서,

상기 변환수단은 루트에서부터 선택한 상기 장치 키가 대응하고 있는 노드에 이르기까지의 경로를 구성하는 패스를 식별하는 ID 정보를 연결하여 상기 변환정보를 생성하는 것을 특징으로 하는 키 데이터 생성장치.

청구항 6

청구항 4에 있어서,

상기 변환수단은 상기 선택한 장치 키가 대응하는 노드의 위치를 상기 트리구조에서의 계층 및 동일 계층의 각 노드의 위치관계로 표현한 것을 상기 변환정보로서 생성하는 것을 특징으로 하는 키 데이터 생성장치.

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

청구항 2에 있어서,

상기 출력수단은 상기 암호화 키 데이터를 휴대형 기록매체에 기입하는 것을 특징으로 하는 키 데이터 생성장치.

청구항 14

청구항 2에 있어서,

상기 출력수단은 상기 암호화된 키 데이터를 통신매체를 이용하여 출력하는 것을 특징으로 하는 키 데이터 생성장치.

청구항 15

삭제

청구항 16

콘텐츠를 이용하는 단말장치로,

장치 키를 보유하는 콘텐츠 키 보유수단과,

트리구조를 이용하여 장치 키를 관리하고 있는 청구항 2에 기재된 키 데이터 생성장치로부터 상기 암호화 키 데이터를 취득하는 취득수단과,

상기 암호화 키 데이터를 상기 장치 키를 이용해서 복호하여 제 2 키 데이터를 생성하는 복호수단과,

상기 트리구조에서의 상기 장치 키에 대응하는 노드의 위치에 따라서 정해지는 정보인 변환정보를 보유하는 변환정보 보유수단과,

상기 제 2 키 데이터를 상기 변환정보를 이용해서 재변환하여 제 1 키 데이터를 생성하는 변환수단과,

상기 제 1 키 데이터를 이용해서 콘텐츠를 이용하는 콘텐츠 이용수단을 포함하는 것을 특징으로 하는 단말장치.

청구항 17

청구항 16에 있어서,

상기 장치 키 보유수단은 상기 장치 키를 포함하는 복수 개의 장치 키를 보유하고 있고,

상기 복수의 장치 키에서 상기 장치 키를 선택하는 선택수단을 구비하며,

상기 취득수단은 상기 키 데이터 생성장치에 의해 상기 장치 키에 대해서 생성한 변환정보와 상기 제 1 키 데이터로 역변환 가능한 연산을 실행하여 생성된 상기 제 2 키 데이터를 암호화하여 생성된 상기 암호화된 키 데이터를 취득하고,

상기 복호수단은 상기 선택된 장치 키를 이용하여 복호하며,

상기 변환수단은 상기 선택된 장치 키에 대한 변환정보를 생성하고, 상기 변환정보를 이용하여 상기 선택된 장치 키에 소정의 연산을 실행하여 상기 제 1 키 데이터를 생성하는 것을 특징으로 하는 단말장치.

청구항 18

청구항 17에 있어서,

상기 변환수단은 상기 암호화 키 데이터에 부수하는 헤더 정보로부터 상기 변환정보를 생성하는 것을 특징으로 하는 단말장치.

청구항 19

청구항 18에 있어서,

상기 헤더 정보는, 트리 구조를 이용하여 장치 키를 관리하고 있는 상기 키 데이터 생성장치가 상기 트리구조에서 상기 정당한 단말장치만이 보유하는 장치 키 중 최상위 층에 위치하는 노드에 대응되어 있는 1 이상의 장치 키를 선택하고, 선택한 상기 장치 키의 트리 구조에서의 위치정보에 의거하여 생성한, 상기 변환정보를 생성하기 위한 정보이며,

상기 변환정보 보유수단은 상기 트리구조에서의 당해 단말장치의 위치정보를 보유하고 있고,

상기 변환수단은 상기 헤더 정보와 상기 위치정보로부터 상기 변환정보를 생성하는 것을 특징으로 하는 단말장치.

청구항 20

삭제

청구항 21

삭제

청구항 22

청구항 16에 있어서,

상기 콘텐츠 이용수단은,

상기 제 1 키 데이터에 의거하여 상기 콘텐츠를 암호화하여 암호화 콘텐츠를 생성하는 암호화부와,

상기 암호화 콘텐츠를 출력하는 출력부를 구비하는 것을 특징으로 하는 단말장치.

청구항 23

청구항 16에 있어서,

상기 콘텐츠 이용수단은,

암호화된 콘텐츠를 취득하는 콘텐츠 취득수단과,

상기 제 1 키 데이터에 의거하여 상기 암호화 콘텐츠를 복호하여 콘텐츠를 생성하는 복호수단과,

상기 콘텐츠를 재생하는 재생수단을 더 구비하는 것을 특징으로 하는 단말장치.

청구항 24

콘텐츠의 암호화 및 복호에 이용하는 키 데이터를 기록하는 기록매체로,

트리구조의 각 노드에 1 이상의 장치 키를 대응시켜서 각 단말장치가 갖는 장치 키를 규정하는 키 관리수단과, 규정되어 있는 장치 키에서 1 이상의 장치 키를 선택하는 선택수단과, 콘텐츠를 이용하기 위해서 이용하는 제 1 키 데이터를 상기 트리구조에서의 선택한 장치 키에 대응하는 노드의 위치에 따라서 정해지는 정보인 변환정보를 이용해서 변환하여 제 2 키 데이터를 생성하는 변환수단과, 정당한 단말장치만이 보유하는 장치 키를 이용해서 상기 제 2 키 데이터를 암호화하여 암호화 키 데이터를 생성하는 암호화수단을 구비하는 키 데이터 생성장치에 의해 생성된 상기 암호화 키 데이터를 기록하는 것을 특징으로 하는 기록매체.

청구항 25

청구항 24에 있어서,

상기 제 1 키 데이터에 역변환 가능한 연산을 실행하여 상기 제 2 키 데이터를 생성할 때에 상기 연산에 이용하는 변환정보를 더 기록하는 것을 특징으로 하는 기록매체.

청구항 26

청구항 25에 있어서,

상기 정당한 단말장치만이 보유하는 장치 키 중 최상위층에 위치하는 노드에 대응되어 있는 1 이상의 장치 키의 트리구조에서의 위치정보에 의거하여 생성된 상기 변환정보를 기록하는 것을 특징으로 하는 기록매체.

청구항 27

삭제

청구항 28

정당한 단말장치만이 콘텐츠를 이용할 수 있도록 키 데이터를 생성하는 키 데이터 생성장치에서 이용되는 방법으로,

트리구조의 각 노드에 1 이상의 장치 키를 대응시켜서 각 단말장치가 갖는 장치 키를 규정하는 키 관리스텝과,

콘텐츠를 이용하기 위해서 이용되는 제 1 키 데이터를 선택한 장치 키에 대응하는 노드의 상기 트리구조에서의 위치에 따라서 정해지는 정보인 변환정보를 이용해서 변환하여 제 2 키 데이터를 생성하는 변환스텝과,

상기 선택한 장치 키를 이용하여 상기 제 2 키 데이터를 암호화하여 암호화 키 데이터를 생성하는 암호화스텝과,

상기 암호화 키 데이터를 출력하는 출력스텝을 포함하는 것을 특징으로 하는 키 데이터 생성장치에서 이용되는 방법.

청구항 29

삭제

청구항 30

정당한 단말장치만이 콘텐츠를 이용할 수 있도록 키 데이터를 생성하는 키 데이터 생성장치에 이용되는 프로그램을 기록하고 있는 컴퓨터 판독 가능한 기록매체로,

상기 프로그램은,

트리구조의 각 노드에 1 이상의 장치 키를 대응시켜서 각 단말장치가 갖는 장치 키를 규정하는 키 관리스텝과,

콘텐츠를 이용하기 위해서 이용되는 제 1 키 데이터를 선택한 장치 키에 대응하는 노드의 상기 트리구조에서의 위치에 따라서 정해지는 정보인 변환정보를 이용해서 변환하여 제 2 키 데이터를 생성하는 변환스텝과,

상기 선택한 장치 키를 이용하여 상기 제 2 키 데이터를 암호화하여 암호화 키 데이터를 생성하는 암호화스텝과,

상기 암호화 키 데이터를 출력하는 출력스텝을 포함하는 것을 특징으로 하는 컴퓨터 판독 가능한 기록매체.

청구항 31

청구항 1에 있어서,

상기 키 데이터 생성장치는,

상기 암호화 키 데이터의 생성에 이용된 장치 키의 상기 트리구조에서의 위치정보에 의거하여 생성된, 상기 변환정보를 생성하기 위한 정보인 헤더 정보를 생성하는 헤더 정보 생성수단을 구비하며,

상기 단말장치는,

복수의 장치 키를 보유하고 있는 장치 키 보유수단과,

상기 트리구조에서의 당해 단말장치의 위치정보를 보유하고 있는 변환정보 보유수단을 더 구비하고,

상기 취득수단은 상기 헤더 정보를 더 취득하고,

상기 변환수단은 상기 헤더 정보와 상기 위치정보로부터 상기 변환정보를 생성하고, 상기 제 2 키 데이터를 상기 생성한 변환정보를 이용하여 미리 정해진 변환규칙에 의거하여 변환함으로써 상기 제 1 키 데이터를 생성하는 것을 특징으로 하는 저작물 보호시스템.

청구항 32

청구항 2에 있어서,

상기 키 데이터 생성장치는,

상기 암호화 키 데이터의 생성에 이용된 장치 키의 상기 트리구조에서의 위치정보에 의거하여 생성된, 상기 변환정보를 생성하기 위한 정보인 헤더 정보를 생성하는 헤더 정보 생성수단을 더 구비하는 것을 특징으로 하는 키 데이터 생성장치.

청구항 33

청구항 16에 있어서,

상기 장치 키 보유수단은 상기 장치 키를 포함하는 복수의 장치 키를 보유하고 있고,

상기 변환정보 보유수단은 상기 트리구조에서의 당해 단말장치의 위치정보를 보유하고 있으며,

상기 복호수단은 상기 복수의 장치 키 중 하나인 상기 장치 키를 이용하여 상기 제 2 키 데이터를 생성하고,

상기 취득수단은 상기 암호화 키 데이터의 생성에 이용된 장치 키의 트리구조에서의 위치정보에 의거하여 생성된, 상기 변환정보를 생성하기 위한 정보인 헤더 정보를 더 취득하고,

상기 변환수단은 상기 헤더 정보와 상기 위치정보로부터 상기 변환정보를 생성하고, 상기 제 2 키 데이터를 상기 생성한 변환정보를 이용하여 미리 정해진 변환규칙에 의거하여 변환함으로써 상기 제 1 키 데이터를 생성하는 것을 특징으로 하는 단말장치.

청구항 34

청구항 24에 있어서,

상기 제 2 키 데이터는 상기 키 데이터 생성장치에 의해서 상기 제 1 키 데이터를 상기 장치 키에 대해서 생성한 변환정보를 이용하여 미리 정해진 변환규칙에 의거하여 변환한 데이터이며,

상기 기록매체는 상기 암호화 키 데이터의 생성에 이용된 장치 키의 상기 트리구조에서의 위치정보에 의거하여 생성된, 상기 변환정보를 생성하기 위한 정보인 헤더 정보를 더 기록하는 것을 특징으로 하는 기록매체.

청구항 35

콘텐츠를 이용하는 단말장치에서 이용되는 콘텐츠 이용방법으로,

상기 단말장치는 장치 키를 기억하고 있는 장치 키 보유수단과, 트리구조에서의 상기 장치 키에 대응하는 노드의 위치에 따라서 정해지는 정보인 변환정보를 보유하는 변환정보 보유수단을 구비하며,

상기 콘텐츠 이용방법은,

트리구조를 이용해서 장치 키를 관리하고 있는 청구항 2에 기재된 키 데이터 생성장치로부터 상기 암호화 키 데이터를 취득하는 취득스텝과,

상기 암호화 키 데이터를 상기 장치 키를 이용해서 복호하여 제 2 키 데이터를 생성하는 복호스텝과,

상기 제 2 키 데이터를 상기 변환정보를 이용해서 재변환하여 제 1 키 데이터를 생성하는 변환스텝과,

상기 제 1 키 데이터를 이용해서 콘텐츠를 이용하는 콘텐츠 이용스텝을 포함하는 것을 특징으로 하는 콘텐츠 이용방법.

청구항 36

콘텐츠를 이용하는 단말장치에서 이용되는 컴퓨터 프로그램을 기록한 컴퓨터 판독 가능한 기록매체로,

상기 단말장치는 장치 키를 기억하고 있는 장치 키 보유수단과, 트리구조에서의 상기 장치 키에 대응하는 노드의 위치에 따라서 정해지는 정보인 변환정보를 보유하는 변환정보 보유수단을 구비하며,

상기 컴퓨터 프로그램은,

트리구조를 이용해서 장치 키를 관리하고 있는 청구항 2에 기재된 키 데이터 생성장치로부터 상기 암호화 키 데이터를 취득하는 취득스텝과,

상기 암호화 키 데이터를 상기 장치 키를 이용해서 복호하여 제 2 키 데이터를 생성하는 복호스텝과,

상기 제 2 키 데이터를 상기 변환정보를 이용해서 재변환하여 제 1 키 데이터를 생성하는 변환스텝과,

상기 제 1 키 데이터를 이용해서 콘텐츠를 이용하는 콘텐츠 이용스텝을 포함하는 것을 특징으로 하는 컴퓨터 판독 가능한 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 광 디스크와 같은 대용량 기록매체에 영화와 같은 저작물인 콘텐츠의 디지털화된 데이터를 기록하고, 이 콘텐츠를 재생하기 위한 시스템에 관한 것이다.

배 경 기 술

[0002] 영화나 음악과 같은 저작물인 콘텐츠의 저작권을 보호하기 위하여, 재생장치에는 다수의 장치 키가 주어지며, 콘텐츠를 해독하는데 사용되고 콘텐츠를 재생하도록 허용되는 재생장치에 의해서만 얻을 수 있는 키 데이터와

함께 콘텐츠는 암호화된 상태로 기록매체에 기록된다. 이러한 종류의 키 데이터를 발생하기 위한 키를 관리하는 하나의 방법은 트리 구조를 이용하는 것이다.

[0003] 문헌 1은 트리 구조를 이용하는 키 관리 시스템에 관한 기술을 개시하는 바, 키 정보의 양이 상대적으로 적고 개별 키들은 폐지될 수 있다. 또한, 문헌 2는 문헌 1의 기술에 근거한 기술로, 재생장치가 미리 보유하는 장치 키의 개수의 증가를 억제하고 반면에 기록매체에 기록되는 키 정보의 양은 감소시키는 디지털 콘텐츠 보호 키 시스템에 관한 기술을 개시한다.

[0004] 다음은 문헌 1에 개시된 키 관리 방법의 개요이다.

[0005] 키 관리 조직은 트리 구조의 리프(leaf)가 재생장치와 일대일 대응하도록 장치 키를 관리한다. 각 재생장치는 루트로부터 재생장치에 대응하는 리프까지 통하는 도중에 위치한 노드에 대응하여 장치 키를 보유한다. 키 관리 조직은 모든 관리되는 장치 키 중에서 대부분의 재생장치에 의해 공유되는 장치 키인 장치 키 K를 이용하여 하나의 콘텐츠와 그 콘텐츠를 해독하는데 이용되는 매체 키 MK를 암호화한다. 이어, 키 관리 조직은 암호화된 매체 키 E(K, MK)를 기록매체에 기입한다. E(X, Y)는 데이터 Y를 키 데이터 X로 암호화하여 얻어지는 암호문을 의미하는 것에 유의하자.

[0006] 여기서, 재생장치가 내부적으로 분석되고 재생장치가 보유한 모든 장치 키가 노출된다면, 키 관리 조직은 노출된 키를 폐지하고, 나머지 장치 키들 중에서 대부분의 재생장치가 공유하는 장치 키를 선택하고, 매체 키 MK를 암호화하는데 선택된 장치 키를 이용한다.

[0007] 도 11에 도시된 바와 같이, 재생장치 0이 폐지된 경우, 장치 키 Kf, Kb 및 K1은 매체 키 MK를 암호화하는데 이용되며, 이에 따라 기록매체에 기입되는 암호문 E(Kf, MK), E(Kb, MK) 및 E(K1, MK)를 생성한다.

[0008] 따라서, 폐지된 재생장치 0은, 장치 키 Kf, Kb 및 K1 중 어느 것도 가지고 있지 않기 때문에 매체 키 MK를 얻을 수 없으며, 장치 키 Kf, Kb 및 K1 중 어느 것을 갖는 재생장치만이 매체 키 MK를 얻을 수 있다.

[0009] 여기서, 장치 키의 고유성이 분실되면, 예를 들어, 장치 키 Kf와 장치 K1 각각의 값이 동일하다면, 기록매체에 기록되는 암호문 E(Kf, MK)와 E(K1, MK)의 값은 동일할 것이다. 이것은 장치 키 Kf와 K1이 동일한 값을 갖는 것으로 공개적으로 알려지는 것을 의미한다.

[0010] 도 12에 도시된 바와 같이, 재생장치 7이 나중에 폐지되면, 키 관리 조직은 매체 키 MK를 장치 키 Kb, Kc, K1 및 K6을 사용하여 암호화하고, 4개의 암호문 E(Kb, MK), E(Kc, MK), E(K1, MK) 및 E(K6, MK)을 기록매체에 기록한다.

[0011] 여기서, 재생장치 7이 보유한 장치 키 Kf는 이미 노출되었고, Kf와 K1이 동일한 것으로 공개적으로 알려졌기 때문에 불법적인 당사자가 노출된 Kf를 이용하여 암호문 E(K1, MK)를 해독하여 불법적으로 매체 키 MK를 얻을 위험성이 있다. 이러한 불법적인 행위를 방지하기 위하여 암호문 E(K1, MK)가 기록매체에 기록되지 않는다면, 유효한 재생장치 1은 매체 키 MK를 얻을 수 없으며 부당하게 폐지되는 문제점이 발생한다.

[0012] 매체 키를 불법적으로 취득하는 것을 방지하고 폐지되지 않아야 하는 재생장치가 부당하게 폐지되는 것을 방지하는 방법의 일 예로 각 장치 키의 고유성을 보증하는 것이 있다. 구체적으로, 장치 키는 통상 난수 열을 생성하는 난수 생성기를 이용하여 생성되기 때문에, 한 가지 방법은, 장치 키가 생성될 때마다, 이 장치 키가 과거에 생성된 어떠한 장치 키와 일치하는지를 체크하는 것이다. 여기서, 난수 열은 일치하는 장치 키가 존재하면 파괴되고, 일치하는 장치 키가 존재하지 않으면 이용된다.

[0013] 그러나, 재생장치의 수가 수 십억인 대규모 시스템에서 각각 생성된 장치 키가 과거에 생성된 장치 키와 일치하는지를 체크하는 것은 시간 측면에서 막대하게 비용이 많이 든다. 문헌 2의 키 관리 방법이 이용되더라도, 장치 키를 체크하는데 걸리는 시간에 대해 같은 문제가 발생한다.

[0014] 문헌 1

[0015] 나카노, 오모리 및 다테바야시의 "Digital Content Hogo-you Kagi Kanri Houshiki(디지털 콘텐츠 보호를 위한 키 관리 시스템)", The 2001 Symposium on Cryptography and Information Security, SCIS2001, 5A-5, 2001. 1.

[0016] 문헌 2

[0017] 나카노, 오모리 및 다테바야시의 "Digital Content Hogo-you Kagi Kanri Houshiki - ki-kouzou pattern

Bunkatsu houshiki(디지털 콘텐츠 보호를 위한 키 관리 시스템 - 트리패턴 분리 방법), The 2002 Symposium on Cryptography and Information Security, SCIS2002, 10C-1, 2002. 1.

발명의 상세한 설명

[0018] 상기한 문제를 고려하여, 본 발명의 목적은 장치 키의 고유성을 체크하지 않고 매체 키의 불법적인 취득을 방지하고 폐지되지 않아야 할 재생장치의 부당한 폐지를 방지하는 저작물 보호시스템을 제공하는 것이다.

[0019] 상기한 목적을 달성하기 위하여, 본 발명은, 정당한 단말장치만이 콘텐츠를 이용할 수 있는 저작물 보호시스템으로, 키 데이터 생성장치와 단말장치를 포함하며, 상기 키 데이터 생성장치는, 트리구조의 각 노드에 1 이상의 장치 키(device key)를 대응시켜서 각 단말장치가 갖는 장치 키를 규정하는 키 관리수단과, 규정되어 있는 장치 키에서 1 이상의 장치 키를 선택하는 선택수단과, 콘텐츠를 이용하기 위해서 이용하는 제 1 키 데이터를 상기 트리구조에서의 상기 선택한 장치 키에 대응하는 노드의 위치에 따라서 정해지는 정보인 변환정보를 이용해서 변환하여 제 2 키 데이터를 생성하는 변환수단과, 정당한 단말장치만이 보유하는 장치 키를 이용해서 상기 제 2 키 데이터를 암호화하여 암호화 키 데이터를 생성하는 암호화수단과, 상기 암호화 키 데이터를 출력하는 출력수단으로 구성되고, 상기 단말장치는, 암호화 키 데이터를 취득하는 취득수단과, 상기 암호화 키 데이터를 당해 단말장치가 보유하는 장치 키를 이용해서 복호하여 제 2 키 데이터를 생성하는 복호수단과, 상기 제 2 키 데이터를 상기 트리구조에서의 상기 장치 키에 대응하는 노드의 위치에 따라서 정해지는 정보인 변환정보를 이용해서 재변환하여 제 1 키 데이터를 생성하는 변환수단과, 상기 제 1 키 데이터를 이용해서 콘텐츠를 이용하는 콘텐츠 이용수단으로 구성된다.

[0020] 상기한 구조에 의하면, 장치 키가 동일한 값을 갖더라도 암호화된 키 데이터는 반드시 동일한 값을 가질 필요는 없다. 또한, 암호화된 키 데이터를 이용하여 장치 키가 동일한 값을 갖는지를 결정할 수 없다. 그러므로, 제 1 키 데이터의 불법적인 취득은 방지될 수 있다. 따라서, 폐기되지 않아야 할 재생장치의 폐기가 방지된다.

실 시 예

[0033] 이하, 도면부호를 참조하여 본 발명의 실시예들을 설명한다.

[0034] 제 1 실시예

[0035] 1. 저작권 보호 시스템의 구조

[0036] 도 1과 6에 도시된 바와 같이, 저작권 보호 시스템은 키 데이터 생성장치(100), 다수의 재생장치(200a, 200b 등), 및 DVD(300)로 구성된다. 재생장치(200a, 200b 등)의 공통된 구조는 도 6의 재생장치(200)와 같이 도시된다.

[0037] 키 관리 조직이 보유한 키 데이터 생성장치(100)는 콘텐츠와 콘텐츠를 재생하는 키 데이터를 DVD(300)에 기록한다. 키 데이터는, 유효 재생장치만이 콘텐츠를 재생할 수 있도록 선택되며, 트리(tree) 구조로 관리된다.

[0038] 각각의 사용자가 보유한 재생장치(200a, 200b 등) 각각에는 키 데이터 생성장치(100)에 의해 미리 다수의 장치 키가 할당된다. 또한,, 재생장치(200a, 200b 등) 각각은 할당된 장치 키 중에서 적절한 장치 키를 선택하고, 선택된 장치 키를 이용하여 DVD(300)에 기록된 암호화된 콘텐츠를 해독하고 재생한다.

[0039] 다음은 각 구조에 대한 설명이다.

[0040] 1.1 키 데이터 생성장치(100)

[0041] 도 1에 도시된 바와 같이, 키 데이터 생성장치(100)는 장치 키 저장부(101), 장치 키 선택부(102), 변환부(103), 매체 키 암호화부(105), 콘텐츠 키 암호화부(106), 콘텐츠 암호화부(107), 입력부(108), 제어부(109), 및 구동부(110)로 구성된다.

[0042] 구체적으로, 키 데이터 생성장치(100)는 마이크로프로세서, ROM, RAM, 하드디스크 유닛, 표시유닛, 키보드, 마우스 등으로 구성되는 컴퓨터 시스템이다. 컴퓨터 프로그램은 RAM이나 하드디스크 유닛에 저장되고, 키 데이터 생성장치(100)는 컴퓨터 프로그램에 따라 동작하는 마이크로프로세서에 의해 그 기능을 달성한다.

[0043] (1) 입력부(108)와 구동부(110)

[0044] 입력부(108)는 외부 소스로부터 매체 키 MK, 콘텐츠 키 CK, 및 콘텐츠의 입력을 수신하고, 매체 키 MK를 변환부(103)와 콘텐츠 키 암호화부(106)에 출력하고, 콘텐츠 키 CK는 콘텐츠 키 암호화부(106)과 콘텐츠 암호화부

(107)에 출력하며, 콘텐츠는 콘텐츠 암호화부(107)에 출력한다.

[0045] 여기서, 매체 키는 DVD(300)에 고유한 정보이거나 DVD(300)에 고유한 정보로부터 생성된 키 데이터일 수 있다.

[0046] 구동부(110)는 제어부(109)의 제어하에 변환 정보, 암호화된 키 데이터, 및 암호화된 콘텐츠를 DVD(300)에 기입한다.

[0047] (2) 제어부(109)

[0048] 제어부(209)는 관리되는 장치 키들 중에서 대부분의 재생장치가 공통으로 보유하는 적어도 하나의 장치 키를 선택하도록 장치 키 선택부(102)를 제어한다.

[0049] 또한, 제어부(109)는 선택된 장치 키나 키들의 각각에 대해 변환 정보를 생성하도록 변환정보 생성부(104)를 제어한다.

[0050] 다음, 제어부(109)는 변환부(103)를 제어하여 변환정보 생성부(104)가 생성한 변환 정보의 각 부분을 이용하여 매체 키 MK를 각각 변환하도록 한다.

[0051] 또한, 제어부(109)는 매체 키 암호화부(105)를 제어하여 선택된 각 장치 키를 이용하여 변환된 매체 키 MK를 암호화하도록 한다. 제어부(109)는 또한 콘텐츠 키 암호화부(106)를 제어하여 수신한 콘텐츠를 매체 키를 이용하여 암호화하도록 하고, 콘텐츠 암호화부(107)를 제어하여 콘텐츠를 암호화하도록 한다.

[0052] 제어부(109)는 각각의 암호화된 키 데이터, 변환 정보 및 암호화된 콘텐츠를 구동부(110)를 통하여 DVD(300)에 기록되도록 한다.

[0053] (3) 장치 키 저장부(101)

[0054] 장치 키 저장부(101)는 저작권 보호 시스템에 속하는 재생장치에 주어지는 모든 장치 키들을 저장한다.

[0055] 장치 키 저장부(101)에 의해 저장되는 장치 키들은 도 2에 도시된 키 관리 방법의 트리 구조를 이용하여 생성되고 재생장치에 할당된다.

[0056] 여기서, 이 실시예에서 트리 구조가 3개의 레이어를 갖는 3중 트리인 것으로 설명되었지만, 더 많은 레이어를 가질 수 있다. 트리 구조 관리방법은 문헌 2에 상세하게 설명되어 있다.

[0057] 다음에서 트리 구조를 간단하게 설명한다.

[0058] 트리 구조는 노드와 경로로 구성된다. 트리의 각 "조인트(joint)"가 노드(node)라 불리며, 노드는 경로(path)에 의해 연결된다. 트리 구조에서 노드들이 위치하는 각 레벨은 레이어(layer)라 불린다. 특정 노드 위에 있고 하나의 경로에 의해 그 노드에 연결되는 노드는 부모 노드(parent node)라 하고, 부모 노드 아래에 있고 여러 경로에 의해 부모 노드에 연결되는 노드를 자식 노드(child node)라 한다.

[0059] 또한, 가장 높은 레이어의 노드를 루트(root)라 하고, 가장 낮은 레이어의 노드를 리프(leaf)라 한다. 재생장치는 리프에 일 대 일로 할당된다. 도 2에서, 재생장치에는 번호 0 내지 8이 각각 할당된다.

[0060] 또한, 각 노드에는 노드 ID가 할당된다. 노드 ID는 루트로부터 특정 노드까지 경로 번호의 연결이다. 경로 번호 00, 01 및 10은 좌에서 우로 설명한 순서로 경로에 할당된다. 예를 들어, 재생장치 6이 할당된 리프의 노드 ID는 "1000"이다.

[0061] 다음은 저작권 보호 시스템에서 장치 키가 어떻게 할당되는지를 설명한다.

[0062] <루트>

[0063] 다수의 장치 키가 루트에 할당된다. 도 2에서, 이 장치 키들은 식별정보 Ka-0000, Ka-0001, Ka-0010, Ka-0011, Ka-0100, Ka-0101, 및 Ka-0110으로 표현된다. 식별정보에서 "Ka-"는 장치 키가 루트에 할당된 것을 나타낸다. "Ka-" 이후의 4비트는 NRP(Node Revocation Pattern)로, NRP의 최상위 비트는 노드가 리프와 관련하여 부모 노드인지를 식별한다. 노드가 부모 노드일 때, 최상위 비트는 "1"이고, 그외 다른 노드에서는 "0"이다.

[0064] NRP의 3개의 하위 비트는 폐기정보를 표현한다. 폐기정보는, 루트의 자식 노드 각각에 대해, 폐기 장치 키나 키들이 자식 노드에 할당된 장치 키에 존재하는지를 나타낸다. 여기서, "1"은 폐기 장치 키나 키들을 갖는 자식 노드를 나타내고, "0"은 폐기 장치 키나 키들을 갖지 않는 자식 노드를 나타낸다. 폐기정보는 트리 구조의 좌에서 우 순서로 연결되는 각 자식 노드에 대한 정보로 구성된다.

[0065] 여기서, "폐기(revoke)"는 재생장치가 분석되고 장치 키가 노출되는 것과 같은 이유로 재생장치와 장치 키를 무효화하는 것을 의미한다. 이와 같이 폐기 장치 키에 대응하는 노드는 폐기된다. 이러한 노드를 폐기 노드라 한다.

[0066] Ka-0000은 트리 구조에 속하는 모든 재생장치가 보유하는 키이며, 이는 트리 구조내 어떠한 재생장치도 폐기되지 않은 초기 상태에서 이용되는 장치 키이다.

[0067] 다른 장치 키들은, 폐기 장치 키가 자식 노드에 존재할 때, 매체 키를 암호화하는데 이용된다.

[0068] 예를 들어, 폐기 재생장치가 루트의 가장 좌측 자식 노드 아래에 존재할 때, 그리고 다른 자식 노드에는 폐기 재생장치가 존재하지 않을 때, Ka-0100에 의해 식별되는 폐기정보 "100"을 갖는 장치 키가 이용된다. 이와 같이, 장치 키는 각각 대응하는 폐기정보에 할당되고, 트리 구조내 폐기 재생장치의 위치에 따라서, 연속하여 사용되는 폐기정보 부분에 의해 식별되는 장치 키 중에서 선택이 이루어진다.

[0069] 또한, 폐기정보 "111"을 갖는 장치 키는 할당되지 않는다. 이는 최하위 레이어에 할당된 장치 키는 모든 자식 노드가 폐기 재생장치를 가질 때 이용되기 때문이다.

[0070] <노드>

[0071] 6개의 장치 키 Kb-1001, Kb-1010, Kb-1011, Kb-1100, Kb-1101, 및 Kb-1110은 레이어 1의 가장 좌측 노드에 할당된다. 여기서, "Kb"는 레이어 1의 가장 좌측 노드에 할당된 장치 키를 나타낸다. 루트의 장치 키와 같은 방법으로, 각 장치 키는 자식 노드에 대한 폐기정보에 의해 식별된다. 또한, 폐기정보 "000"을 갖는 장치 키는 할당되지 않는다. 이는 특정 노드 아래의 노드에 대해 폐기 재생장치가 존재하지 않을 때 특정 노드 위의 노드인 루트에 할당된 장치 키가 이용되기 때문이다. 또한, 폐기정보 "111"을 갖는 장치 키도 할당되지 않는다. 이는 자식 노드인 3개의 리프에 대응하는 모든 재생장치가 폐기될 때 그 노드에 할당된 장치 키들은 이용되지 않기 때문이다.

[0072] <리프>

[0073] 각 리프에는 재생장치가 할당된다. 여기서, 재생장치는 번호 0 내지 8로 식별된다.

[0074] 레이어 2의 가장 좌측의 리프에는 장치 키 Ka-0000, Ka-0001, Ka-0010, Ka-0011, Kb-1001, Kb-1010, 및 Kb-1011가 할당된다.

[0075] 재생장치 0이 폐기될 때를 위한 폐기 형태에 대응하는 장치 키를 제외하고, 루트로부터 리프까지의 경로상의 노드에 할당되는 모든 장치 키가 리프에 할당된다. 환언하면, 장치 키 Ka-0100, Ka-0101, Ka-0110, Kb-1100, Kb-1101, 및 Kb-1110은 재생장치 0에 할당되지 않으며, 이는 이들이, 루트와 레이어 1의 가장 좌측 노드에 할당된 장치 키 중에서, 재생장치 0이 폐기될 때 이용되는 장치 키이기 때문이다.

[0076] 다른 리프에도 같은 방법으로 장치 키들이 할당된다.

[0077] (4) 장치 키 선택부(102)

[0078] 장치 키 선택부(102)는 폐기 재생장치가 콘텐츠를 이용할 수 없도록 장치 키를 선택하고, 선택된 장치 키를 매체 키 암호화부(105)에 출력한다.

[0079] 초기상태에서, 장치 키 선택부(102)는 Ka-0000을 선택하고, 이 선택된 장치 키를 매체 키 암호화부(105)에 출력한다.

[0080] 하나 이상의 폐기 재생장치가 존재할 때 장치 키를 선택하는 방법은 도 3을 이용하여 설명된다.

[0081] 재생장치 0과 8이 폐기된 경우, 루트로부터 재생장치 0과 8에 대응하는 각 리프까지의 경로상의 모든 노드는 폐기된다. 각 폐기노드는 도 3에서 크로스(×)로 표시된다. 하나 이상의 재생장치가 폐기될 때, 이용되고 있던 장치 키는 더 이상 이용될 수 없다. 환언하면, 초기상태에서 이용되고 있던 Ka-0000은 이용될 수 없다.

[0082] 다음, 장치 키 선택부(102)는, 각 폐기노드에 대해, 노드의 폐기 형태에 대응하는 장치 키를 선택한다. 루트의 경우, 장치 키 선택부(102)는, 좌측과 우측의 자식 노드가 폐기되기 때문에, 그것의 폐기정보가 "101"인 장치 키 Ka-0101을 선택한다.

[0083] 레이어 1의 가장 좌측 노드의 경우, 장치 키 선택부(102)는, 가장 좌측의 자식 노드가 폐기되기 때문에, 그것의 폐기정보가 "100"인 장치 키 Kb-1100를 선택한다. 레이어 1의 중앙은 폐기 자식 노드를 갖지 않으므로 위의 레

이어에 할당된 장치 키, 이 경우 루트에 할당된 Ka-0101이 이용된다. 또한, 장치 키 선택부(102)는, 가장 우측의 자식 노드가 폐기되기 때문에, 레이어 1의 가장 우측의 자식 노드에 대해 그것의 폐기정보가 "001"인 장치 키 Kd-1001을 선택한다.

[0084] (5) 변환정보 생성부(104)

[0085] 변환정보 생성부(104)는 장치 키 선택부(102)에 의해 선택된 장치 키 각각에 대해 변환정보를 생성한다.

[0086] NRP 정보는 루트로부터 선택된 장치 키가 할당되는 노드까지 NRP를 연결함으로써 생성된다.

[0087] 도 3에 도시된 바와 같이, 재생장치 0과 8이 폐기될 때, 변환정보 생성부(104)는 장치 키 선택부(102)가 선택한 장치 키 Ka-0101, Kb-1100, 및 Kd-1001에 대한 변환정보를 생성한다.

[0088] 먼저, 변환정보 생성부(104)는 재생장치 3 내지 5가 공유하는 장치 키 Ka-0101에 대한 변환정보를 생성한다. 여기서, 루트로부터 장치 키 Ka-0101이 할당되는 노드까지를 통하여 이 노드들에 대한 유일한 NRP가 "101"이기 때문에, 변환정보 생성부(104)는 "101"을 변환정보로 변환부(103)에 출력한다.

[0089] 이어, 변환정보 생성부(104)는 재생장치 1과 2가 공유하는 장치 키 Kb-1100에 대한 변환정보를 생성한다. 루트로부터 장치 키 Kb-1100이 할당된 노드까지를 통하여 노드들에 대한 NRP가 "101"과 "100"이기 때문에, 변환정보 생성부(104)는 이 NRP를 연결하여 변환정보 "101100"을 생성하고, 생성된 변환정보를 변환부(103)에 출력한다.

[0090] 다음, 변환정보 생성부(104)는 재생장치 6과 7이 공유하는 장치 키 Kb-1001에 대한 변환정보를 생성한다. 루트로부터 장치 키 Kb-1001이 할당된 노드까지를 통하여 노드들에 대한 NRP가 "101"과 "001"이기 때문에, 변환정보 생성부(104)는 이 NRP를 연결하여 변환정보 "101001"을 생성하고, 생성된 변환정보를 변환부(103)에 출력한다.

[0091] 또한, 변환정보 생성부(104)는 변환정보를 생성하는데 사용된 NRP를 구동부(110)를 통하여 DVD(300)의 변환정보 기록영역(301)에 기입하도록 한다. 여기서, NRP는 그들이 할당된 레이어의 높이순으로 기입된다.

[0092] 암호화된 매체 키나 암호화된 콘텐츠 키에 첨부된 헤더 정보가 변환정보로 이용되는 경우, 변환정보를 기록하는 것은 불필요하다는 것에 유의하라. 또한, 재생장치가 변환정보를 생성할 수 있는 구조를 갖는다면 변환정보를 기록할 필요가 없다.

[0093] (6) 변환부(103)

[0094] 변환부(103)는 입력부(108)를 통하여 외부 소스로부터 매체 키를 수신하고, 변환정보 생성부(104)로부터 변환정보를 수신한다. 변환부(103)는 각 변환정보 부분을 이용하여 매체 키에 각각 XOR 연산을 적용하여 매체 키를 변환한다.

[0095] 구체적으로, 도 4A에 도시된 바와 같이, 변환부(103)는 먼저 장치 키 Ka-0101에 대응하는 변환정보 "0101"을 이용하여 매체 키 MK를 변환함으로써 변환 매체 키 MK'를 생성한다. 다음, 도 4B에 도시된 바와 같이, 변환부(103)는 장치 키 Kb-1100에 대응하는 변환정보 "01011100"를 이용하여 매체 키 MK를 변환함으로써 변환 매체 키 MK''를 생성한다. 또한, 변환부(103)는 장치 키 Kd-1001에 대응하는 변환정보 "01011001"를 이용하여 매체 키 MK를 변환함으로써 변환 매체 키 MK'''를 생성한다.

[0096] 변환부(103)는 생성된 변환 매체 키 MK', MK'', 및 MK'''를 매체 키 암호화부(1050에 출력한다.

[0097] (7) 매체 키 암호화부(105)

[0098] 매체 키 암호화부(105)는 장치 키 선택부(102)로부터 장치 키를 수신하고, 변환부(103)로부터 변환 매체 키를 수신한다. 매체 키 암호화부(105)는 각 변환 매체 키를 수신한 각 장치 키로 암호화한다.

[0099] 구체적으로, 도 4A에 도시된 바와 같이, 매체 키 암호화부(105)는 먼저 장치 키 Ka-0101을 이용하여 변환 매체 키 MK'에 암호화 알고리즘 E1을 적용하여 암호화 키 E(Ka-0101, MK')를 생성한다. 여기서, 암호화 알고리즘 E1은, 예를 들어, AES(Advanced Encryption Standard)이다. AES는 통상적으로 알려져 있기 때문에 이에 대한 설명은 생략한다. E(X, Y)는 데이터 Y를 키 데이터 X로 암호화하여 얻어지는 암호문을 의미하는 것에 유의하라.

[0100] 같은 방법으로, 도 4B에 도시된 바와 같이, 매체 키 암호화부(105)는 장치 키 Kb-1100을 이용하여 변환 매체 키 MK''에 암호화 알고리즘 E1을 적용하여 암호화 키 E(Kb-1100, MK'')를 생성한다. 다음, 도 4C에 도시된 바와 같이, 매체 키 암호화부(105)는 장치 키 Kd-1001을 이용하여 변환 매체 키 MK'''에 암호화 알고리즘 E1을 적용하여 암호화 키 E(Kd-1001, MK''')를 생성한다.

[0101] 또한, 매체 키 암호화부(105)는 생성된 암호화된 매체 키 E(Ka-0101, MK'), E(Kb-1100, MK'') 및 E(Kd-1001, MK''')를 구동부(110)를 통하여 DVD(300)의 매체 키 데이터 기록영역(302)에 기입한다.

[0102] (8) 콘텐츠 키 암호화부(106)

[0103] 콘텐츠 키 암호화부(106)는 입력부(108)를 통하여 콘텐츠 키 CK와 매체 키 MK를 수신한다. 콘텐츠 키 암호화부(106)는 수신한 매체 키 MK를 이용하여 콘텐츠 CK에 암호화 알고리즘 E1을 적용하여 콘텐츠 키 CK를 암호화함으로써 암호화된 콘텐츠 키 E(MK, CK)를 생성한다. 이어 콘텐츠 키 암호화부(106)는 생성된 암호화된 콘텐츠 키 E(MK, CK)를 구동부(110)를 통하여 콘텐츠 키 데이터 기록영역(303)에 기입한다.

[0104] (9) 콘텐츠 암호화부(107)

[0105] 콘텐츠 암호화부(107)는 입력부(108)를 통하여 외부 소스로부터 콘텐츠와 콘텐츠 키 CK를 수신한다. 콘텐츠 암호화부(107)는 수신한 콘텐츠 키 CK를 이용하여 콘텐츠에 암호화 알고리즘 E1을 적용하여 콘텐츠를 암호화함으로써 암호화된 콘텐츠 E(CK, 콘텐츠)를 생성한다. 콘텐츠 암호화부(107)는 생성된 암호화 콘텐츠 E(CK, 콘텐츠)를 구동부(110)를 통하여 DVD(300)의 콘텐츠 기록영역(304)에 기입한다.

[0106] 1.2 DVD(300)

[0107] DVD(300)는, 도 5에 도시된 바와 같이, 변환정보 기록영역(301), 매체 키 기록영역(302), 콘텐츠 키 데이터 기록영역(303), 및 콘텐츠 기록영역(304)을 포함한다.

[0108] 변환정보 기록영역(301)은 변환정보를 생성하는데 이용되는 NRP가 기입되는 영역이다. NRP는 그들이 할당된 레이어의 높이순으로 기입된다.

[0109] 매체 키 데이터 기록영역(302)은 암호화된 매체 키를 기록하는 영역이다. 암호화된 매체 키는 트리 구조의 최상위 레이어에 할당된 장치 키를 이용하여 암호화된 매체 키로부터 순서대로 기입된다.

[0110] 콘텐츠 키 데이터 기록영역(303)은 암호화된 콘텐츠 키를 기록하는 영역이다.

[0111] 콘텐츠 기록영역(304)은 암호화된 콘텐츠를 기록하는 영역이다.

[0112] 1.3 재생장치(200)

[0113] 재생장치(200)는 재생장치(200a, 200b 등)에 공통인 구조를 나타내며, 트리 구조의 재생장치 0 내지 8의 임의의 것에 대응한다.

[0114] 도 6에 도시된 바와 같이, 재생장치(200)는 장치 키 선택부(201), 장치 키 저장부(202), 매체 키 해독부(203), 변환부(204), 콘텐츠 키 해독부(205), 콘텐츠 해독부(206), 구동부(207), 재생부(208), 제어부(209), 및 입력부(210)로 구성된다. 모니터(220)와 스피커(221)는 재생부(208)에 연결된다.

[0115] 키 데이터 생성부(100)와 유사하게, 재생장치(200)는, 구체적으로, 마이크로프로세서j, ROM, RAM, 하드디스크 유닛, 표시유닛 등으로 구성된다. 재생장치(200)는 RAM이나 하드디스크에 저장된 컴퓨터 프로그램에 따라 동작하는 마이크로프로세서에 의해 그 기능을 달성한다.

[0116] (1) 구동부(207)와 입력부(210)

[0117] 입력부(210)는 외부 소스로부터 입력을 수신하고, 제어부(209)에 수신한 입력정보를 출력한다.

[0118] 구동부(207)는 제어부(209)의 제어하에 DVD(300)를 판독한다.

[0119] 먼저, 제어부(209)의 제어하에, 구동부(207)는 변환정보 기록영역(301)으로부터 변환정보를 판독하고, 판독한 변환정보를 장치 키 선택부(201)에 출력한다.

[0120] 다음, 구동부(207)는 매체 키 데이터 기록영역(203)으로부터 암호화된 매체 키를 판독하고, 판독한 암호화된 매체 키를 매체 키 해독부(203)에 출력한다.

[0121] 또한, 구동부(207)는 콘텐츠 키 기록영역(303)으로부터 암호화된 콘텐츠 키 E(MK, CK)를 판독하고, 판독한 암호화된 콘텐츠 키 E(MK, CK)를 콘텐츠 키 해독부(205)에 출력한다.

[0122] 구동부(207)는 또한 암호화된 콘텐츠 E(CK, 콘텐츠)를 콘텐츠 기록영역(304)으로부터 판독하고, 판독한 암호화된 콘텐츠 E(CK, 콘텐츠)를 콘텐츠 해독부(206)에 출력한다.

[0123] (2) 재생부(208)

[0124] 제어부(209)의 제어하에, 재생부(208)는 콘텐츠 해독부(206)로부터 수신한 콘텐츠에서 비디오 신호와 오디오 신호를 생성하고, 생성된 비디오 신호와 오디오 신호를 모니터(220)와 스피커(221)에 각각 출력한다.

[0125] (3) 제어부(209)

[0126] 입력부(210)로부터 DVD(300)에 기록한 콘텐츠의 재생을 지시하는 명령 정보를 수신한 경우, 제어부(209)는 구동부(207)를 제어하여 DVD(300)로부터 다양한 종류의 정보를 판독한다.

[0127] 먼저, 제어부(209)는 장치 키 선택부(201)를 제어하여 장치 키를 선택하고, 암호화된 매체 키의 기록위치를 특정하고, 변환정보를 생성한다.

[0128] 다음, 제어부(209)는 매체 키 해독부(203)를 제어하여 암호화된 매체 키를 해독함으로써 변환 매체 키를 생성하고, 변환부(204)가 변환 매체 키를 다시 변환하게 하여 매체 키를 생성한다.

[0129] 또한, 제어부(209)는 매체 키를 이용하여 콘텐츠 키 해독부(205)를 제어하여 판독한 암호화된 콘텐츠 키를 해독함으로써 콘텐츠 키를 생성한다. 제어부(219)는 콘텐츠 해독부(206)로 하여금 생성된 콘텐츠 키를 이용하여 판독한 암호화된 콘텐츠를 해독하게 함으로써 콘텐츠를 생성하고, 재생부(208)를 제어하여 콘텐츠를 재생하도록 한다.

[0130] (4) 장치 키 저장부(202)

[0131] 장치 키 저장부(202)는 관리자에 의해 재생장치(200)에 할당된 다수의 장치 키를 저장한다. 할당된 장치 키들은 재생장치 0 내지 8 각각의 아래에 도시된 식별자에 의해 도 2에 표시된다. 예를 들어, 재생장치 6은 식별정보 Ka-0000, Ka-0010, Ka-0100, Ka-0110, Kd-1001, Kd-1010, 및 Kd-1011에 의해 표시되는 장치 키를 갖는다.

[0132] 또한, 장치 키 저장부(202)는 재생장치가 대응되는 루트의 트리 구조내 위치를 나타내는 ID 정보를 저장한다.

[0133] (5) 장치 키 선택부(201)

[0134] 장치 키 선택부(201)는 장치 키를 선택하고, 선택된 장치 키를 매체 키 해독부(203)로 출력한다. 장치 키를 선택하는데 사용하는 방법의 일 예는 각 장치 키에 미리 식별자가 부여되고, 키 데이터 생성장치는 선택된 장치 키의 식별자를 DVD에 기록하고, 재생장치는 DVD에 기록된 식별자에 의해 지시되는 장치 키를 선택하는 것이다. 이러한 장치 키 선택방법은 잘 알려져 있으므로 상세한 설명은 생략한다.

[0135] 장치 키 선택부(201)는 선택된 장치 키에 대응하는 암호화된 매체 키의 기록위치를 특정하고, 변환정보를 생성하며, 기록 위치를 매체 키 해독부(203)에 출력하고 변환정보를 변환부(204)에 출력한다. 여기서, 기록위치 지정과 변환정보 생성을 위한 처리는 후술한다.

[0136] (6) 매체 키 해독부(203)

[0137] 매체 키 해독부(203)는 장치 키 선택부(201)로부터 장치 키와 암호화된 매체 키 기록위치를 수신하고, 수신한 기록위치에 의해 지시되는 영역에 기록된 암호화된 매체 키를 구동부(207)를 통하여 DVD(300)로부터 판독한다.

[0138] 매체 키 해독부(203)는 장치 키를 이용하여 암호화된 매체 키에 해독 알고리즘 D1을 적용함으로써 변환 매체 키를 생성한다. 여기서, 해독 알고리즘 D1은 암호화 알고리즘 E1과 반대의 처리를 수행한다. 매체 키 해독부(203)는 생성된 변환 매체 키를 변환부(204)에 출력한다.

[0139] 도 7A에 도시된 바와 같이, 선택한 장치 키가 Ka-0101의 구체적인 예를 들면, 매체 키 해독부(203)는 암호화된 매체 키 E(Ka-0101, MK')를 선택한 장치 키 Ka-0101을 이용하여 해독함으로써 변환 매체 키 MK'를 생성한다. 도 7B에 도시된 바와 같이, 선택한 장치 키가 Kb-1100인 경우, 매체 키 해독부(203)는 암호화된 매체 키 E(Kb-1100, MK'')를 선택한 장치 키 Kb-1100을 이용하여 해독함으로써 변환 매체 키 MK''를 생성한다. 선택한 장치 키가 Kd-1001인 경우, 매체 키 해독부(203)는 암호화된 매체 키 E(Kd-1001, MK''')를 선택한 장치 키 Kd-1001을 이용하여 해독함으로써, 도 7C에 도시된 바와 같이, 변환 매체 키 MK'''를 생성한다.

[0140] 매체 키 해독부(203)는 생성된 변환 매체 키 MK', MK'', MK'''를 변환부(204)에 출력한다.

[0141] (7) 변환부(204)

[0142] 변환부(204)는 매체 키 해독부(203)로부터 변환 매체 키를 수신하고, 장치 키 수신부(201)로부터 변환정보를 수

신한다.

[0143] 변환부(204)는 수신한 변환 매체 키에 장치 키 선택부(201)에 의해 생성된 변환정보로 XOR 연산을 수행함으로써 매체 키를 생성한다.

[0144] 도 7A에 도시된 바와 같이, 선택한 장치 키가 Ka-0101의 구체적인 예를 들면, 변환부(204)는 변환 매체 키 MK'를 장치 키 Ka-0101에 대응하는 변환정보 "0101"을 이용하여 해독함으로써 매체 키 MK를 생성한다. 도 7B에 도시된 바와 같이, 선택한 장치 키가 Kb-1100인 경우, 변환부(204)는 변환 매체 키 MK''를 대응하는 변환정보 "01011100"을 이용하여 해독함으로써 매체 키 MK를 생성한다. 선택한 장치 키가 Kd-1001인 경우, 변환부(204)는 변환 매체 키 MK'''를 대응하는 변환정보 "01011001"을 이용하여 해독함으로써, 도 7C에 도시된 바와 같이, 매체 키 MK를 생성한다.

[0145] 변환부(204)는 생성된 매체 키 MK를 콘텐츠 키 해독부(205)에 출력한다.

[0146] (8) 콘텐츠 키 해독부(205)

[0147] 콘텐츠 키 해독부(205)는 구동부(207)로부터 암호화된 콘텐츠 키를 수신하고, 변환부(204)로부터 매체 키를 수신한다. 콘텐츠 키 해독부(205)는 수신한 매체 키를 이용하여 암호화된 콘텐츠 키에 해독 알고리즘 D1을 적용함으로써 콘텐츠 키를 생성하고, 생성한 콘텐츠 키를 콘텐츠 해독부(206)에 출력한다.

[0148] (9) 콘텐츠 해독부(206)

[0149] 콘텐츠 해독부(206)는 구동부(207)로부터 암호화된 콘텐츠를 수신하고, 콘텐츠 키 해독부(205)로부터 콘텐츠 키를 수신한다. 콘텐츠 해독부(206)는 수신한 콘텐츠 키를 이용하여 암호화된 콘텐츠에 해독 알고리즘 D1을 적용함으로써 콘텐츠를 생성하고, 생성한 콘텐츠를 재생부(208)에 출력한다.

[0150] 2. 저작권 보호 시스템의 동작

[0151] 2.1 키 데이터 생성장치(100)에 의한 동작

[0152] 다음은 도 8을 이용하여 키 데이터 생성장치의 동작을 설명한다.

[0153] 장치 키 선택부(102)는 폐기된 적이 없는 대부분의 재생장치가 공유하는 하나 이상의 장치 키를 선택하고(단계 S401), 선택한 장치 키를 매체 키 암호화부(105)와 변환정보 생성부(104)에 출력한다.

[0154] 다음, 변환정보 생성부(104), 변환부(103), 및 매체 키 암호화부(105)는 선택한 장치 키 각각에 대해 다음의 처리를 반복한다. 도 8에서, "A"는 선택한 장치 키의 개수를 나타낸다.

[0155] 변환정보 생성부(104)는 변환정보를 생성하고(단계 S403), 변환정보를 변환부(103)에 출력한다. 변환부(103)는 입력부(108)를 통하여 취득한 매체 키를 변환함으로써 변환 매체 키를 생성하며(단계 S404), 생성한 변환 매체 키를 매체 키 암호화부(105)로 출력한다. 매체 키 암호화부(105)는 선택한 장치 키와 변환 매체 키를 취득하고, 취득한 장치 키를 이용하여 변환 매체 키를 암호화함으로써 암호화된 매체 키를 생성한다(단계 S405).

[0156] 단계 S403 내지 S405의 처리는 모든 선택된 장치 키에 대해 수행되었기 때문에, 생성한 변환정보와 암호화된 매체 키는 구동부(110)를 통하여 DVD(300)에 기입된다(단계 S406).

[0157] 다음, 콘텐츠 키 암호화부(106)는 미변환 매체 키(변환 전의 매체 키)를 이용하여 콘텐츠 키를 암호화함으로써 암호화된 콘텐츠 키를 생성하고, 생성한 암호화된 콘텐츠 키를 구동부(110)를 통하여 DVD(300)에 기입한다(단계 S407).

[0158] 2.2 재생장치에 의한 동작

[0159] 다음은 도 9를 이용하여 DVD(300)에 기록된 콘텐츠를 재생하기 위한 재생장치(200)의 동작을 설명한다.

[0160] 장치 키 선택부(201)는 구동부(207)를 통하여 판독된 변환정보에 근거하여 장치 키를 선택하고, 암호화된 매체 키 기록위치 지정과 변환정보 생성을 수행한다(단계 S411). 장치 키 선택부(201)는 선택한 장치 키와 기록위치를 매체 키 해독부(203)에 출력하고, 변환정보를 변환부(204)에 출력한다.

[0161] 매체 키 해독부(203)는 기록위치에 따라 구동부(207)를 통하여 DVD(300)로부터 암호화된 매체 키를 판독하고, 장치 키 선택부(201)로부터 수신한 장치 키를 이용하여 암호화된 매체 키를 해독함으로써 변환 매체 키를 취득한다(단계 S412). 이어, 매체 키 해독부(203)는 변환 매체 키를 변환부(204)에 출력한다.

[0162] 변환부(204)는 장치 키 선택부(201)로부터 수신한 변환정보를 이용하여 변환 매체 키에 XOR 연산을 수행하고(단계 S413), 결과의 매체 키를 콘텐츠 해독부(205)에 출력한다.

[0163] 콘텐츠 해독부(206)는 구동부(207)를 통하여 DVD(300)로부터 판독한 암호화된 콘텐츠 키를 매체 키를 이용하여 해독함으로써 콘텐츠 키를 취득하고(단계 S414), 콘텐츠 키를 콘텐츠 해독부(206)에 출력한다.

[0164] 콘텐츠 해독부(206)는 구동부(207)를 통하여 DVD(300)로부터 취득한 암호화된 콘텐츠를 콘텐츠 키 해독부(205)로부터 수신한 콘텐츠 키를 이용하여 해독함으로써 콘텐츠를 취득하고(단계 S415), 콘텐츠를 재생부(208)로 출력한다.

[0165] 재생부(208)는 수신한 콘텐츠를 재생하고 이를 모니터(220)와 스피커(221)에 출력한다(단계 S416).

[0166] 2.3 암호화된 매체 키 특정과 변환정보 생성

[0167] (1) 다음은 도 10을 이용하여 단계 S411에서의 암호화된 매체 키 특정과 변환정보 생성을 설명한다.

[0168] 장치 키 선택부(201)는 변환정보 기록영역(301)에 기록된 NRP를 순서대로 체크한다. 장치 키 선택부(201)는 체크되는 NRP의 위치를 나타내는 변수 Y, 암호화된 매체 키의 기록위치를 나타내는 변수 X, 재생장치와 관련하여 NRP의 위치를 나타내는 변수 A, 특정 레이어의 NRP의 번호를 나타내는 변수 W, 및 트리 구조의 레이어 번호를 나타내는 변수 D를 갖는다. 여기서, 재생장치(200)와 관련된 NRP는 트리 구조에서 사용자 장치가 할당되는 리프로부터 루트까지의 경로상의 노드들의 NRP이다.

[0169] 장치 키 선택부(201)는 레이어 i=0 내지 i=D-1 동안 다음의 과정에 따라 분석을 한다.

[0170] 장치 키 선택부(201)는 다음을 초기값으로 설정한다: 변수 A=0, 변수 W1, 변수 i=0, 변수 Y=0 그리고 X=0이다(단계 S421).

[0171] 장치 키 선택부(201)는 변수 i와 변수 D를 비교하고, 변수 i가 변수 D보다 더 크면(단계 S422), 재생장치가 폐기되었기 때문에 처리를 종료한다.

[0172] 변수 i가 변수 D와 같거나 작은 경우(단계 S422), 장치 키 선택부(201)는 변환정보 기록영역(301)에 기록된 Y번째 NRP의 최하위 3비트가 "111"인지를 판정한다(단계 S423). 3비트가 "111"이면, 장치 키 선택부(201)는 Y=Y+1을 계산하고(단계 S426), 단계 S423의 처리로 복귀한다.

[0173] 3비트가 "111"이 아닌 경우, 장치 키 선택부(201)는 변수 Y의 값과 변수 A의 값이 동일한지를 판정한다(단계 S424). 값들이 다른 경우, 장치 선택부(201)는 X=X+1을 계산하고(단계 S425), Y=Y+1을 계산하고(단계 S426), 단계 S423의 처리로 복귀한다.

[0174] 변수 Y의 값과 변수 A의 값이 동일한 경우, 장치 키 선택부(201)는 레이어 i의 Y번째 NRP를 저장한다(단계 S427).

[0175] 다음, 장치 키 선택부(201)는, Y번째 NRP를 구성하는 4개 비트 중, 최상위 2i번째 비트와 2i-1번째 비트의 값에 대응하는 비트 위치의 값 B가 "0" 또는 '1"인지를 판정한다(단계 S428). 여기서, 대응하는 비트 위치는, 최상위 2i번째 비트와 2i-1번째 비트의 값이 "00"인 경우, Y번째 NRP의 가장 좌측 비트이고, "01"의 경우, Y번째 NRP의 중간 비트이고, "10"인 경우, Y번째 NRP의 가장 우측 비트이다. 도 2에 도시된 바와 같이, 트리 구조에서 좌측 경로에 "00"이 할당되고, 중간 경로에 "01"이 할당되고, 우측 경로에 "10"이 할당되는 규칙에 근거하여 ID 정보가 작성되므로, 루트로부터 재생장치에 대응하는 리프까지의 경로를 보여준다.

[0176] 값 B가 "1"인 경우(단계 S428), 장치 키 선택부(201)는 레이어 i의 W NRP의 "1들"의 개수를 카운트한다. 그러나, 장치 키 선택부(201)는 그것의 최상위 비트가 "1"인 NRP의 "1들"은 카운트하지 않는다. 장치 키 선택부(201)는 카운트한 값을 변수 W에 할당한다. 이와 같이 취득한 변수 W는 다음 레이어 i+1의 NRP의 번호를 나타낸다(단계 S429).

[0177] 다음, 장치 키 선택부(201)는 첫 번째 NRP로부터 대응하는 비트 위치의 NRP까지 NRP의 "1들"의 개수를 카운트한다. 그러나, 장치 키 선택부(201)는 그것의 최상위 비트가 "1"인 NRP의 "1들"은 카운트하지 않는다. 장치 키 선택부(201)는 카운트한 값을 변수 A에 할당한다. 여기서, 장치 키 선택부(201)는 대응하는 비트 위치의 값은 카운트하지 않는다. 이러한 방법으로 취득한 변수 A는 재생장치(200)에 관련한 NRP의 위치를 나타낸다(단계 S430).

[0178] 다음, 장치 키 선택부(201)는 X=X+1을 계산하고(단계 S431), Y=0을 계산하고(단계 S432), i=i+1을 계산하고(단

계 S433), 단계 S422의 처리로 복귀한다.

[0179] 단계 S428에서 값 B=0인 경우, 장치 키 선택부(201)는 변수 X의 값을 암호화된 매체 키의 기록위치로 매체 키 해독부(203)에 출력하고, 생성된 변환정보를 변환부(204)에 출력하고(단계 S434), 처리를 종료한다.

[0180] (2) 다음은 도 2의 재생장치 6의 경우를 예로 이용하여 암호화된 매체 키의 선택과 변환정보 생성을 위한 구체적인 처리를 설명한다.

[0181] 재생장치 6은 장치 키로 미리 Ka-0000, Ka-0010, Ka-0100, Ka-0110, Kd-1010, Kd-1011을 보유하고, ID 정보로 "1000"을 보유한다.

[0182] a) 장치 키 선택부(201)는 변환정보 기록영역(301)에 기록된 0번째 NRP "0101"의 최하위 3비트가 "111"인지를 판정한다(단계 S423).

[0183] b) 최하위 3비트가 "111"이 아니기 때문에, 장치 키 선택부(201)는 변수 Y와 변수 A의 값을 비교하고(단계 S424), 이 값들이 동일하기 때문에 레이어 0의 0번째 NRP의 값 "0101"을 저장한다.

[0184] c) ID 정보의 톱 2비트의 값이 "10"이기 때문에, 장치 키 선택부(201)는 0번째 NRP의 최하위 3비트의 가장 우측 비트를 체크한다(단계 S428). 가장 우측 비트는 "1"이기 때문에, 장치 키 선택부(201)는 단계 S429의 처리로 진행한다.

[0185] d) 장치 키 선택부(201)는 레이어 0의 한 NRP "0101"의 최하위 3비트의 "1들"의 개수를 카운트한다. 카운트한 값이 "2"이므로, 두 개의 NRP가 다음 레이어 1에 존재하는 것을 알게 된다.

[0186] e) 다음, 장치 키 선택부(201)는 대응하는 비트 위치까지 NRP의 "0101"의 최하위 3비트의 "1들"의 개수를 카운트한다. 여기서, 장치 키 선택부(201)는 대응 비트 위치의 값은 카운트하지 않는다. 카운트한 값이 "1"이기 때문에, 다음 레이어 1의 대응 NRP의 위치 A는 위치 1인 것을 알게 된다.

[0187] f) 장치 키 선택부(201)는 X=X+1, Y=0, i=i+1을 계산한다(단계 S431 내지 S433). 그 결과, 변수 X의 값은 "1"이 된다.

[0188] g) 장치 키 선택부(201)는 변환정보 기록영역(301)에 기록된 레이어 1의 0번째 NRP "1100"의 최하위 3비트가 "111"인지를 판정하고(단계 S423), 최하위 3비트가 "111"이 아니기 때문에 변수 Y와 변수 A의 값을 비교한다(단계 S424).

[0189] h) 변수 Y와 변수 A의 값이 다르기 때문에, 장치 키 선택부(201)는 X=X+1을 계산한다(단계 S425). 그 결과, X의 값은 "2"가 된다. 또한, 장치 키 선택부(201)는 Y=Y+1을 계산한다(단계 S426). 그 결과, Y의 값은 "2"가 된다.

[0190] i) 장치 키 선택부(201)는 레이어 1의 첫 번째 NRP "1001"의 최하위 3비트가 "111"인지를 판정하고(단계 S423), 최하위 3비트가 "111"이 아니기 때문에 변수 Y와 변수 A의 값을 비교한다(단계 S424).

[0191] j) 변수 Y와 변수 A의 값이 동일하기 때문에, 장치 키 선택부(201)는 레이어 1의 위치 1의 NRP "1001"과 이미 저장된 NRP "0101"을 연결하고, 그 결과 연결된 값을 저장한다(단계 S427).

[0192] k) ID 정보의 3 및 4번째 톱 비트의 값이 "00"이기 때문에, 장치 키 선택부(201)는 위치 1의 NRP의 최하위 3비트의 가장 좌측 비트를 체크한다(단계 S428). 가장 좌측 비트가 "0"이므로 분석은 종료된다.

[0193] l) 장치 키 선택부(201)는 변수 X의 값 "2"를 기록위치로 매체 키 해독부(203)로 출력하고, "01011001"을 변환정보로 변환부(204)에 출력한다(단계 S434).

[0194] 상기한 처리는 재생장치 6의 기록위치 2로부터 암호화된 매체 키 E(Kd-1001, MK)가 구체화되는 결과를 가져오고, 변환정보 "01011001"이 생성되는 결과를 가져온다.

[0195] 3. 변형

[0196] 본 발명은 바람직한 실시예에 근거하여 설명되었지만, 본 발명은 여기에 한정되지 않는다. 다음과 같은 경우도 본 발명에 포함된다.

[0197] (1) 이용된 암호화 방법은 AES에 한정되지 않으며, 다른 암호화 방법이 이용될 수 있다.

[0198] (2) 바람직한 실시예에서 외부 소스로부터 매체 키와 콘텐츠 키가 입력되지만, 대신 이들은 키 데이터 생성장치에 저장될 수 있다. 선택적으로, 매체 키와 콘텐츠 키는 키 데이터 생성장치가 이용될 때마다 생성될 수 있다.

[0199] (3) 바람직한 실시예에서는 2개의 암호화 레이어가 이용된다. 즉, 콘텐츠는 콘텐츠 키를 이용하여 암호화되고 콘텐츠 키는 매체 키를 이용하여 암호화된다. 그러나, 콘텐츠가 매체 키로 암호화되는 하나의 암호화 레이어를 사용하는 것 또는 추가의 키나 키들을 제공하여 암호화 레이어의 수를 증가시키는 것이 가능하다. 암호화 레이어의 수가 증가하면, 암호화된 키들 중 하나가 변환되는 것은 충분하다.

[0200] (4) 변환정보는 바람직한 실시예에서 설명한 바와 같이 NRP인 것에 한정되지 않는다. 변환정보는 장치 키가 할당되는 노드와 다른 노드의 위치 사이의 트리 구조내 관계를 나타내도록 그리고 경로 수, 노드 위치정보, NRP 등에 대해 기설정된 규칙을 따르도록 생성되는 어떠한 정보일 수 있다. 변환정보의 예로는 이하 (a) 내지 (f)에서 설명된다.

[0201] (a) 변환정보 생성부(104)는 선택된 장치 키에 할당된 노드의 노드 ID를 검색하고, NRP도 검색한다. 이들은 연결되어 변환정보를 생성한다. 다음은 구체적인 예이다.

[0202] 재생장치 0, 1 및 8이 도 3에서와 같이 폐기되는 경우, 장치 키 선택부(102)는 장치 키 Ka-0101, Kb-1100, 및 Kd-1001을 선택한다.

[0203] 변환정보 생성부(104)는 먼저 장치 키 Ka-0101에 대한 변환정보를 생성한다. 여기서, 장치 키 Ka-0101이 할당된 노드는 루트이고, 노드 ID가 존재하지 않으므로 NRP인 "0101"이 변환정보이다.

[0204] 다음, 변환정보 생성부(104)는 장치 키 Kb-1100에 대한 변환정보를 생성한다. 여기서, 장치 키 Kb-1100이 할당된 노드의 노드 ID는 "00"이고 NRP는 "1100"이며, 이들은 연결되어 변환정보 "001100"을 생성한다.

[0205] 이어, 변환정보 생성부(104)는 장치 키 Kd-1001에 대한 변환정보를 생성한다. 여기서, 장치 키 Kd-1001이 할당된 노드의 노드 ID는 "10"이고 NRP는 "1001"이며, 이들은 연결되어 변환정보 "101001"을 생성한다.

[0206] 또한, 노드 ID와 NRP를 연결하는 이외에 노드 ID만 변환정보로 이용할 수 있다. 이 경우, 변환정보가 장치 키 Ka-0101에 대해서는 존재하지 않으므로, 장치 키 Ka-0101은 변환되지 않고 암호화될 수 있거나, 또는 루트에 대해 미리 설정된 변환정보를 이용하여 변환될 수 있다. 여기서, 이 변환정보를 위해 이용된 값은 다른 변환정보와 다르다.

[0207] (b) 트리 구조의 각 노드에는, 도 3에 도시된 바와 같이, 루트에서 시작하여 위에서 아래로 그리고 좌에서 우로 순서대로 식별번호가 부여되고, 식별번호는 변환정보로 이용된다.

[0208] 다시 말해, 재생장치 0, 1, 및 8이 도 3에 도시된 바와 같이 폐기될 때, Ka-0101의 변환정보는 "0"이고, Kb-1100의 변환정보는 "01"이고, Kd-1001의 변환정보는 "11"이다.

[0209] (c) 트리 구조의 각 레이어는 도 2에 도시된 바와 같이 레이어 번호가 부여되고, 동일한 레이어의 노드는 좌에서 우로 순서대로 상대 노드번호가 부여된다. 노드 위치정보는 레이어 번호와 상대 노드번호에 근거하여 생성되며, 이 생성된 위치정보는 변환정보로 이용된다.

[0210] (d) 루트로부터 선택한 장치 키가 할당되는 노드까지의 모든 노드의 NRP는 최상위 레이어로부터 최하위 레이어까지 그리고 각 레이어내 좌에서 우로 검색되고, 변환정보를 생성하도록 연결된다. 필요하다면, 이 생성된 변환정보는 압축되고 임의 길이의 열로 변환될 수 있고, 이 열은 변환정보로 이용될 수 있다.

[0211] (e) 노드는 루트로부터 시작하여 최상위 레이어로부터 최하위 레이어까지 검색되고, "1들"(또는 "0들")의 개수는 장치 키가 대응되는 노드까지 카운트된다. 카운트된 값은 변환정보로 이용된다.

[0212] 여기서, 카운트된 값은 이진수로 변환될 수 있으며, 이진 데이터는 NRP와 연결되어 변환정보를 생성한다. 여기에 이용된 NRP는 루트로부터 장치 키가 할당된 노드까지의 NRP이거나, 상기한 규칙에 근거하여 검색된 모든 NRP일 수 있다. 선택적으로, 이진 데이터는 마지막으로 검색된 단 하나의 NRP에 연결될 수 있다. 다른 대안으로 이진 데이터를 사용된 장치 키의 식별자와 연결하는 것이다.

[0213] (f) 루트로부터 장치 키가 대응되는 노드까지의 모든 NRP는 검색되고 십진수로 변환되며, 그 전체가 변환정보로 이용된다. 선택적으로, NRP는 이진수로 XOR 연산을 할 수 있고, 그 결과는 변환정보로 이용될 수 있다.

[0214] (5) 바람직한 실시예에서, NRP의 최상위 비트는 노드가 리프보다 하나 더 높은 레이어에 있는지를 나타내지만, 이 비트는 다른 정보를 전달하는데 이용될 수 있다. 예를 들어, 최상위 비트는 어떠한 유효 장치가 노드의 자손에 존재하는지를 나타내는데 이용될 수 있다. 선택적으로, NRP의 4비트 중 2 또는 3번째 하위 비트만을 이용하는 것도 가능하다. 마찬가지로, 경로 번호가 반드시 2비트일 필요는 없다. NRP에 대해서와 같이, 경로 번호는

거기에 첨부되는 다른 정보를 가질 수 있다. 또한, 경로 번호의 모든 비트 또는 일부 비트 중 어느 하나를 이용할 수 있다.

[0215] (6) 바람직한 실시예에서, 상기한 검색은 최상위에서 최하위로 그리고 좌에서 우의 순서로 수행되는 것에 한정되지 않는다. 기설정된 규칙에 근거하여 어떠한 방법도 가능하다. 예를 들어, 트리 구조에서 좌측방향으로 또는 깊이 우선으로 검색이 수행될 수 있다.

[0216] (7) 바람직한 실시예에서, 변환정보와 매체 키가 수행하는 연산은 상기한 XOR 연산에 한정되지 않는다. 예를 들어, 산수의 4칙연산의 어느 것도 이용될 수 있다.

[0217] (8) 매체 키 데이터에 패리티 비트를 포함하는 형태의 경우, 매체 키와 변환정보를 연산하는 대신에 변환정보는 매체 키의 패리티 비트에 임베드될 수 있다.

[0218] 예를 들어, DES 암호화가 이용되는 경우, 64비트 매체 키 중 8비트는 패리티 비트이고, 키 데이터 생성장치(100)는 이 8비트에 임베드된 변환정보를 갖는 매체 키를 변환한다.

[0219] 재생장치(200)가 반드시 변환정보를 생성할 필요는 없다. 대신에, 재생장치(200)는 DVD(300)로부터 암호화된 매체 키를 판독하고, 매체 키로부터 8 패리티 비트를 삭제하며, 56비트의 유효 키 데이터를 매체 키로 이용할 수 있다.

[0220] 또한, 매체 키는, 매체 키가 장치 키로 암호화될 때마다, 서로 다른 난수를 패리티 비트로 임베드함으로써 변환될 수 있다. 이 경우에도, 재생장치(200)는 체크없이 패리티 비트를 삭제하고, 56비트의 유효 키 데이터를 매체 키로 이용한다.

[0221] (9) 패리티 비트가 (5)에 설명한 바와 같이 포함된 경우, 변환정보 또는 난수는 일부 패리티 비트에 임베드될 수 있고, 잔여 패리티 비트는 정보를 전달하는데 이용될 수 있다.

[0222] 예를 들어, 8 패리티 비트가 있다면, 난수는 7비트에 임베드될 수 있고, 나머지 1비트는 정보를 전달하는데 이용될 수 있다. 비트가 정보를 전달하는데 이용되는 방법의 일 예는 비트를, 예를 들어, 폐기된 키의 식별자 리스트가 키 데이터가 기록된 기록매체에 존재하는지를 나타내는 플래그로 이용하는 것이다. 여기서, 정보를 전달하는데 이용되는 비트는 특정 기록매체에 대해 고정값을 갖지만, 난수가 나머지 7 패리티 비트에 임베드되기 때문에 변환 매체 키는 각 장치 키에 대해 다르다.

[0223] (10) 바람직한 실시예에서, 키 데이터 생성장치(100)는 키 데이터를 생성하고, 콘텐츠를 암호화하고, 기 데이터와 암호화된 콘텐츠를 기록매체에 기입한다. 그러나, 이러한 모든 동작이 키 데이터 생성장치(100)에 의해 수행될 필요는 없다. 다시 말해, 각각 키 데이터를 생성하고, 키 데이터를 기록하며, 콘텐츠를 기록하는 다른 장치들을 가질 수 있다.

[0224] 또한, 키 데이터 생성장치(100)는 재생장치의 장치 키에 더하여 기록장치의 장치 키를 관리할 수 있다.

[0225] 이 경우, 기록장치는 트리 구조의 리프에 할당된 장치 키들을 보유한다. 기 데이터 생성장치(100)는 실시예에서 설명한 처리를 수행하고, 변환정보와 매체 키 데이터를 생성하고, 이를 DVD에 기록한다.

[0226] 콘텐츠를 암호화하기 위한 콘텐츠 키를 암호화할 때, 기록장치는 재생장치(200)와 동일한 처리를 수행하며, 보유한 장치 키 중에서 적절한 장치 키를 선택하고 취득한다. 기록장치는 취득한 매체 키를 이용하여 콘텐츠 키를 암호화하고, 암호화된 콘텐츠 키와 암호화된 콘텐츠를 DVD에 기입한다.

[0227] 또한, 기록장치는 콘텐츠 키로 키 데이터 생성장치(100)에 의해 기록된 키 데이터를 이용할 수 있다.

[0228] (11) 키 데이터는 DVD에 기록되는 것에 한정되지 않는다. CD, MD, MO 또는 BD(Blu-ray Disc)와 같이, 휴대할 수 있고 키 데이터 생성장치(100)와 재생장치(200) 모두에 장착할 수 있는 어떠한 기록매체도 이용될 수 있다. 또한, 키 데이터와 콘텐츠는 인터넷 등을 통한 통신에 의해 키 데이터 생성장치(100)로부터 재생장치로 전송될 수 있다.

[0229] (12) 본 발명은 상기에서 보여준 방법일 수 있다. 또한, 이 방법은 컴퓨터에 의해 구현되는 컴퓨터 프로그램일 수 있고, 컴퓨터 프로그램의 디지털 신호일 수 있다.

[0230] 또한, 본 발명은 플렉시블 디스크, 하드디스크, CD-ROM(compact disk-read only memory), DVD-ROM(digital versatile disk-read only memory), DVD-RAM(digital versatile disk-random access memory), BD(BluRay Disc) 또는 반도체 메모리와 같이 컴퓨터 프로그램이나 디지털 신호를 저장하는 컴퓨터-판독가능한 기록매체일

수 있다. 또한, 본 발명은 상기한 기록매체 장치 중 어느 것에 기록된 컴퓨터 프로그램이나 디지털 신호일 수 있다.

[0231] 또한, 본 발명은 전자통신, 유무선 통신선 또는 인터넷으로 대표되는 네트워크 상에서 전송되는 컴퓨터 프로그램이나 디지털 신호일 수 있다.

[0232] 또한, 본 발명은 컴퓨터 프로그램에 따라 동작하는 마이크로프로세서와 컴퓨터 프로그램을 저장하는 메모리를 포함하는 컴퓨터 시스템일 수 있다.

[0233] 또한, 프로그램이나 디지털 신호를 기록매체 장치에 전송함으로써, 또는 프로그램이나 디지털 신호를 네트워크 등을 통하여 전송함으로써, 프로그램이나 디지털 신호는 다른 독립된 컴퓨터 시스템에 의해 실행될 수 있다.

[0234] (13) 본 발명은 상기한 실시예와 변형의 어떠한 조합일 수 있다.

[0235] 4, 결론

[0236] 상기한 바와 같이, 본 발명은 콘텐츠를 유효 단말장치에 의해서만 이용할 수 있는 저작물 보호시스템으로서, 키 데이터 생성장치와 단말장치를 포함하며, 상기 키 데이터 생성장치는, 상기 콘텐츠를 이용하는데 사용되는 제 1 키 데이터를 기설정된 변환 규칙에 근거하여 변환함으로써 제 2 키 데이터를 생성하는 변환부; 상기 유효 단말장치가 보유한 장치 키를 이용하여 상기 제 2 키 데이터를 암호화함으로써 암호화된 키 데이터를 생성하는 암호화부; 및 상기 암호화된 키 데이터를 출력하는 출력부를 포함하고, 상기 단말장치는, 상기 암호화된 키 데이터를 취득하는 취득부; 상기 단말장치가 보유하는 장치 키를 이용하여 상기 암호화된 키 데이터를 해독함으로써 제 2 키 데이터를 생성하는 해독부; 상기 제 2 키 데이터를 기설정된 변환 규칙에 근거하여 변환함으로써 제 1 키 데이터를 취득하는 변환부; 및 상기 제 1 키 데이터에 근거하여 상기 콘텐츠를 이용하는 콘텐츠 이용부를 포함한다.

[0237] 또한, 본 발명은 콘텐츠가 유효 단말장치에 의해서만 이용될 수 있도록 키 데이터를 생성하는 키 데이터 생성장치로서, 상기 콘텐츠를 이용하는데 사용되는 제 1 키 데이터를 기설정된 변환 규칙에 근거하여 변환함으로써 제 2 키 데이터를 생성하는 변환부; 유효 단말장치가 보유한 장치 키를 이용하여 상기 제 2 키 데이터를 암호화함으로써 암호화된 키 데이터를 생성하는 암호화부; 및 상기 암호화된 키 데이터를 출력하는 출력부를 포함한다.

[0238] 또한, 본 발명은 콘텐츠를 이용하는 단말장치로서, 기설정된 변환 규칙에 근거하여 콘텐츠를 이용하는데 사용되는 제 1 키 데이터를 변환하여 제 2 키 데이터를 생성하고 상기 제 2 키 데이터를 장치 키를 이용하여 암호화하는 키 데이터 생성장치에 의해 생성되었던 암호화된 키 데이터를 취득하는 취득부; 상기 단말장치가 보유한 장치 키를 이용하여 상기 암호화된 키 데이터를 해독함으로써 제 2 키 데이터를 취득하는 해독부; 기설정된 변환 규칙에 근거하여 상기 제 2 키 데이터를 변환함으로써 제 1 키 데이터를 취득하는 변환부; 및 상기 제 1 키 데이터에 근거하여 상기 콘텐츠를 이용하는 콘텐츠 이용부를 포함한다.

[0239] 상기한 구조에 따르면, 장치 키가 동일한 값을 갖더라도 암호화된 키 데이터는 반드시 동일한 값을 가질 필요는 없다. 또한, 암호화된 키 데이터를 이용하여 장치 키가 동일한 값을 갖는지를 결정할 수 없다. 그러므로, 제 1 키 데이터의 불법적인 취득은 방지될 수 있다. 따라서, 폐기되지 않아야 할 재생장치의 폐기가 방지된다.

[0240] 여기서, 키 데이터 생성장치에서, 변환부는 장치 키에 대한 변환정보를 생성하고 생성된 정보와 제 1 키 데이터에 대해 가역 연산을 수행함으로써 제 2 키 데이터를 생성하며, 출력부는 변환정보를 추가로 출력할 수 있다.

[0241] 또한, 단말장치는, 다수의 장치 키를 보유하는 보유부; 및 장치 키 중 하나를 선택하는 선택부를 추가로 포함하고, 취득부는 제 1 키 데이터와 장치 키에 대해 생성된 상기 변환정보에 대해 가역 연산을 수행함으로써 제 2 키 데이터를 취득하고 제 2 키 데이터를 암호화하는 키 데이터 생성장치에 의해 생성되었던 암호화된 키 데이터를 취득하는 취득하고, 해독부는 선택된 장치 키를 사용하여 해독하며, 변환부는 선택된 장치 키에 대한 변환정보를 생성하고, 변환정보를 이용하여 선택된 장치 키에 기설정된 연산을 적용함으로써 제 1 키 데이터를 생성한다.

[0242] 상기한 구조에 의하면, 키 데이터 생성장치는 선택된 장치 키에 대해 생성된 변환정보를 이용하여 제 1 키 데이터에 가역 연산을 적용함으로써 제 2 키 데이터를 생성한다. 장치 키를 보유한 단말장치만이 제 1 키 데이터를 생성하기 위하여 제 2 키 데이터를 다시 변환할 수 있다.

[0243] 여기서, 키 데이터 생성장치는 단말장치들이 보유한 장치 키들을, 상기 단말장치들 사이에 공유되는 상기 장치

키들 간의 관계를 정의하는 트리 구조의 노드들과 대응시키는 키 관리부; 및 유효 단말장치들이 보유한 장치 키들 중, 상기 트리 구조의 최상위 위치의 노드에 대응되는 하나 이상의 장치들을 선택하는 선택부를 추가로 포함하며, 상기 변환부는 상기 하나 이상의 선택된 장치 키들 각각의 상기 트리 구조의 위치정보에 근거하여 상기 변환정보를 생성하고, 상기 암호화부는 상기 하나 이상의 선택된 장치 키들의 각각을 이용하여 상기 제 2 키 데이터를 각각 암호화한다.

[0244] 또한, 단말장치에서, 상기 변환부는 상기 암호화된 키 데이터에 첨부된 헤더 정보로부터 상기 변환정보를 생성할 수 있다.

[0245] 또한, 단말장치에서, 헤더 정보는 상기 변환정보를 생성하는데 이용되고, 트리 구조를 이용하여 장치 키들을 관리하는 상기 키 데이터 생성장치에 의해 생성되되, 유효 단말장치가 보유한 장치 키들 중 상기 트리 구조의 최상위 위치의 노드에 대응되는 하나 이상의 장치 키를 선택하고, 상기 하나 이상의 선택된 장치 키들 각각의 상기 트리 구조내 위치정보에 근거하여 상기 헤더 정보를 생성하며, 상기 보유부는 상기 단말장치의 위치정보를 보유하고, 상기 변환부는 상기 헤더 정보와 상기 보유한 위치정보를 이용하여 상기 변환정보를 생성할 수 있다.

[0246] 상기한 구조에 따르면, 키 데이터 생성장치는 트리 구조내 선택된 장치 키의 위치에 근거하여 생성된 변환정보를 이용하여 제 1 키 데이터를 변환한다. 그러므로, 장치 키가 동일한 값을 갖더라도, 트리 구조내 다른 위치의 장치 키는 제 2 키 데이터를 올바르게 다시 변환하는데 이용될 수 없다. 따라서, 제 1 키 데이터의 불법 취득이 방지될 수 있다.

[0247] 여기서, 키 데이터 생성장치는 단말장치들이 보유한 장치 키들을 상기 단말장치들 사이에 공유되는 상기 장치 키들 간의 관계를 정의하는 트리 구조의 노드들과 대응시키고 상기 장치 키들 각각이 폐기되는지를 정의하는 키 관리부; 및 유효 단말장치들이 보유한 장치 키들 중, 상기 트리 구조의 최상위 위치의 노드에 대응되는 하나 이상의 장치들을 선택하는 선택부를 추가로 포함하며, 상기 변환부는 상기 선택된 장치 키가 대응되는 상기 노드에 따라 정의되는 폐기 정보와 다른 노드의 폐기 상태에 근거하여 상기 하나 이상의 선택된 장치 키들 각각에 대한 변환정보를 생성할 수 있다.

[0248] 또한, 단말장치에서, 헤더 정보는 상기 변환정보를 생성하기 위한 것으로, 상기 헤더 정보는, 단말장치가 보유한 장치 키를 상기 단말장치 간에 공유되는 상기 장치 키 사이의 관계를 정의하고 상기 장치 키 각각이 폐기되는지를 정의하는 트리 구조의 노드와 대응시키고, 유효 단말장치가 보유한 장치 키들 중 상기 트리 구조의 최상위 위치의 노드에 대응되는 적어도 하나 이상의 장치 키를 선택하며, 상기 헤더 정보를 상기 선택된 장치 키가 대응되는 노드에 근거하여 정의되는 폐기 정보와 다른 노드들의 폐기 상태를 기초로 함으로써 생성되었고, 상기 보유부는 단말장치의 장치 키를 관리하기 위한 트리 구조내 상기 단말장치의 위치정보를 상기 키 데이터 생성장치에 보유하며, 상기 변환부는 상기 헤더 정보와 상기 보유한 위치정보를 이용하여 상기 변환정보를 생성할 수 있다.

[0249] 상기한 구조에 따르면, 변환정보는 폐기 장치 키의 트리 구조내 위치관계에 따라 생성되므로, 트리 구조에서 다른 위치를 갖는 장치 키는 제 2 키 데이터를 올바르게 다시 변환하는데 이용될 수 없다. 따라서, 제 1 키 데이터의 불법 취득이 방지될 수 있다.

[0250] 여기서, 키 데이터 생성장치에서, 변환부는, 각각이 루트로부터 상기 선택된 장치 키가 상기 트리 구조에서 대응되는 상기 노드까지의 노정의 경로를 식별하는 ID 정보 부분을 연결함으로써 상기 하나 이상의 선택된 장치 키들 각각에 대한 상기 변환정보를 생성할 수 있다.

[0251] 또한, 변환부는, 상기 하나 이상의 선택된 장치 키들 각각에 대한 상기 변환정보로서, 상기 선택된 장치 키에 대응되는 노드의 위치를 나타내는 데이터를 생성하고, 상기 위치는 상기 트리 구조의 레이어들 사이 및 동일한 레이어의 노드들 사이의 위치 관계를 고려하여 표시될 수 있다.

[0252] 또한, 변환부는, 각각이 루트로부터 상기 선택된 장치 키가 대응되는 상기 노드까지의 노정에 위치하는 노드에 관련되는 폐기 정보 부분을 연결함으로써 상기 변환정보를 생성할 수 있다.

[0253] 또한, 변환부는, 기설정된 순서로 배열된 노드들에 대응되는 폐기 정보 중에서, 폐기 정보의 제 1 부분을 상기 선택된 장치 키에 대응하는 상기 노드의 폐기 정보의 한 부분에 연결함으로써 상기 변환정보를 생성할 수 있다.

[0254] 상기한 구조에 따르면, 트리 구조내 장치 키의 위치에 따라 다양한 형태가 존재하므로, 트리 구조내 유효 장치 키의 위치정보를 갖지 못하는 단말장치는 변환정보를 생성할 수 없고, 따라서 제 1 키 데이터를 취득할 수 없다.

[0255] 여기서, 키 데이터 생성장치에서, 변환부는 상기 장치 키에 대한 변환정보를 생성하고 상기 제 1 키 데이터의 잉여(redundant) 부분의 적어도 일부에 상기 변환정보를 임베드함으로써 상기 제 2 키 데이터를 생성할 수 있다.

[0256] 또한, 키 데이터 생성장치에서, 변환부는 상기 장치 키에 대해 난수를 생성하고, 상기 제 1 키 데이터의 잉여 부분의 적어도 일부에 상기 생성된 난수를 임베드함으로써 상기 제 2 키 데이터를 생성할 수 있다.

[0257] 또한, 단말장치에서, 제 2 키 데이터는 상기 장치 키에 의해 생성된 변환정보를 상기 제 1 키 데이터의 잉여 부분의 적어도 일부에 임베드함으로써 상기 키 데이터 생성장치에 의해 생성될 수 있다.

[0258] 상기한 구조에 따르면, 잉여 비트가 제 1 키 데이터에 포함될 때, 각 변환에 대해 다른 변환정보나 값으로 임베드됨으로써 동일한 값의 장치 키로 암호화된 제 1 키 데이터를 찾기 어렵게 한다. 따라서, 키 데이터의 정확한 위치를 지정할 수 있는 단말장치만이 제 1 키 데이터를 취득할 수 있다.

[0259] 여기서, 키 데이터 생성장치에서, 변환부는 상기 난수가 임베드되지 않은 상기 잉여 부분의 잔여 부분을 다른 정보를 전달하는데 사용할 수 있다.

[0260] 상기한 구조에 의하면, 난수가 잉여 비트의 일부에 임베드되고, 잔여 잉여 비트는 정보를 전달하는데 이용된다. 따라서, 다른 정보가 전달될 수 있는 반면, 제 1 키 데이터의 불법 취득이 방지될 수 있다.

산업상 이용 가능성

[0261] 본 발명은 트리 구조를 이용하는 키 관리 방법에 이용될 수 있고, 특히 불법적인 키 데이터의 취득을 방지하는데 적절하다.

도면의 간단한 설명

[0021] 도 1은 키 데이터 생성장치(100)와 기록매체(300)의 구조를 보여주는 블록 다이어그램이다.

[0022] 도 2는 키 데이터 생성장치(100)에서 장치 키 사이의 상호관계를 표현한 크리 구조를 보여준다.

[0023] 도 3은 폐지될 장치 키가 존재하는 경우에 장치 키 간의 상관관계를 보여준다.

[0024] 도 4는 매체 키 변환과 암호화 처리의 내용을 보여준다.

[0025] 도 5는 DVD(300)의 기록영역의 구조를 보여준다.

[0026] 도 6은 DVD(300)와 재생장치(200)의 구조를 보여주는 다이어그램이다.

[0027] 도 7은 암호화된 매체 키 해독과 역변환 처리의 내용을 보여준다.

[0028] 도 8은 키 데이터 생성장치(100)의 키 데이터 생성 처리를 보여주는 플로차트이다.

[0029] 도 9는 재생장치(200)의 동작을 보여주는 플로차트이다.

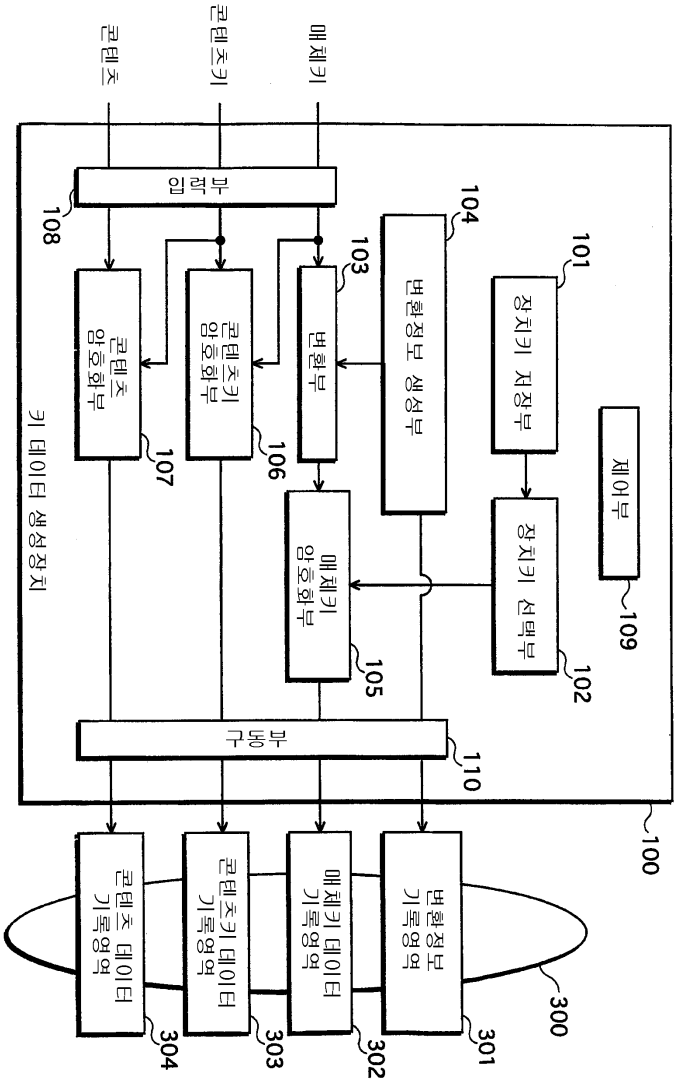
[0030] 도 10은 재생장치(200)의 기록위치 지정과 변환정보 생성 동작을 보여주는 플로차트이다.

[0031] 도 11은 트리 구조를 이용한 키 관리 방법의 일 예를 보여준다.

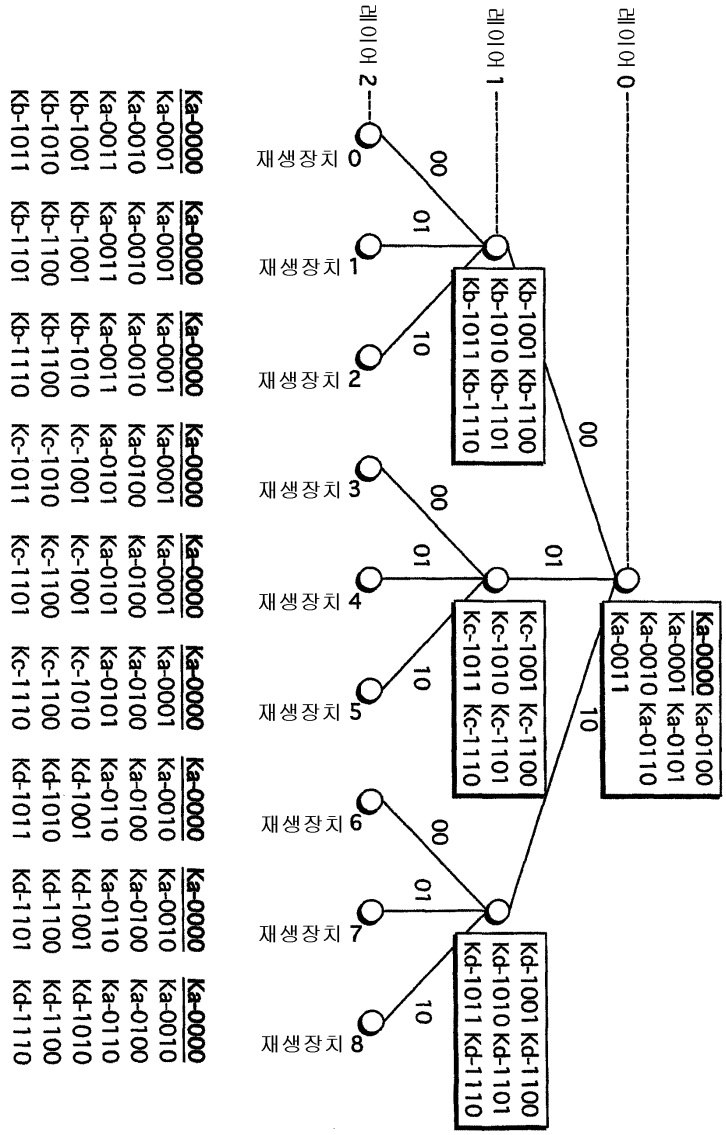
[0032] 도 12는 트리 구조를 이용한 키 관리 방법의 일 예를 보여준다.

도면

도면1

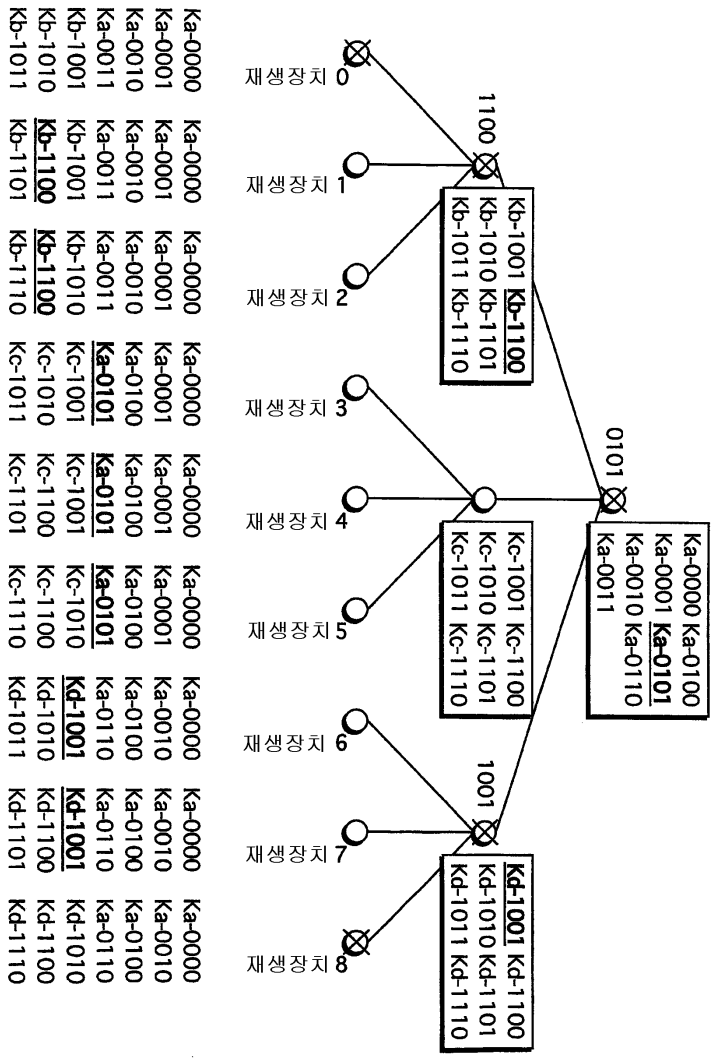

콘텐츠
콘텐츠키
매체키
입력부
108
콘텐츠 암호화부
107
콘텐츠키 암호화부
106
변환부
103
변환정보 생성부
104
정지키 저장부
101
제어부
109
정지키 선택부
102
매체키 암호화부
105
구성부
110
키 데이터 생성장치
100
콘텐츠 데이터 기록영역
304
콘텐츠키 데이터 기록영역
303
매체키 데이터 기록영역
302
변환정보 기록영역
301
300

도면2

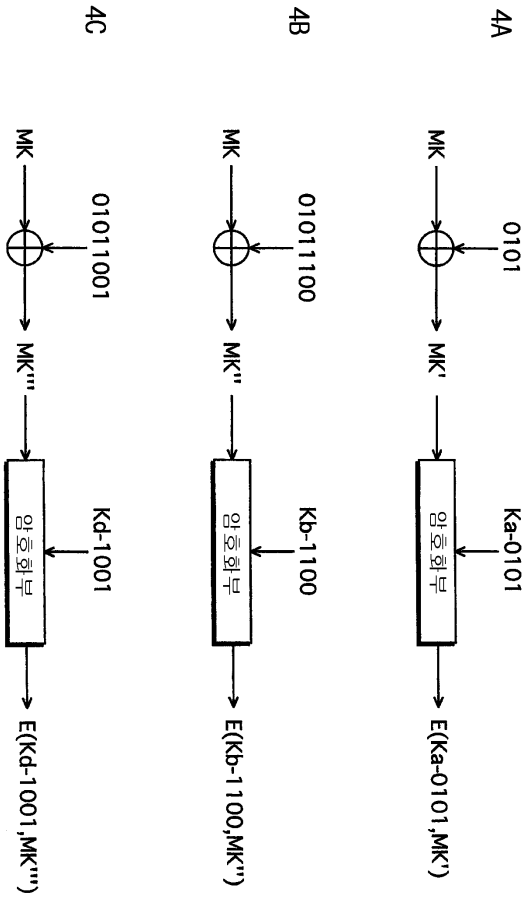


Ka-0000	**Ka-0000**	**Ka-0000**	**Ka-0000**	**Ka-0000**	**Ka-0000**	**Ka-0000**	**Ka-0000**	**Ka-0000**
Ka-0001	Ka-0001	Ka-0001	Ka-0001	Ka-0001	Ka-0001	Ka-0010	Ka-0010	Ka-0010
Ka-0010	Ka-0010	Ka-0010	Ka-0100	Ka-0100	Ka-0100	Ka-0100	Ka-0100	Ka-0100
Ka-0011	Ka-0011	Ka-0011	Ka-0101	Ka-0101	Ka-0101	Ka-0110	Ka-0110	Ka-0110
Kb-1001	Kb-1001	Kb-1010	Kc-1001	Kc-1001	Kc-1010	Kd-1001	Kd-1001	Kd-1010
Kb-1010	Kb-1100	Kb-1100	Kc-1010	Kc-1100	Kc-1100	Kd-1010	Kd-1100	Kd-1100
Kb-1011	Kb-1101	Kb-1110	Kc-1011	Kc-1101	Kc-1110	Kd-1011	Kd-1101	Kd-1110

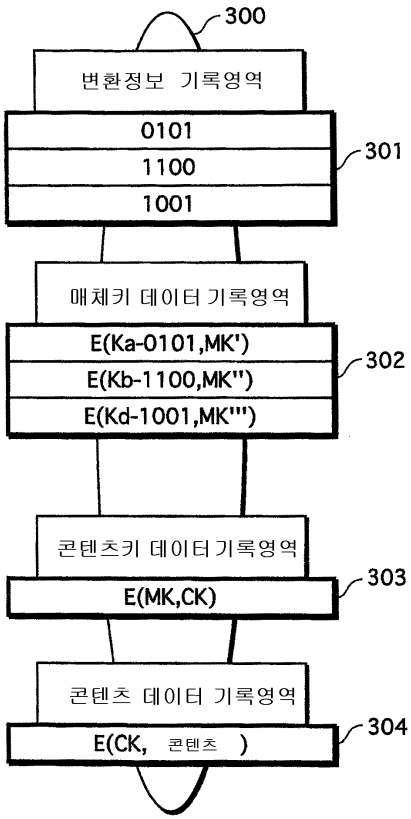
도면3


재생장치 0
재생장치 1
재생장치 2
재생장치 3
재생장치 4
재생장치 5
재생장치 6
재생장치 7
재생장치 8
1100
0101
1001
Kb-1001 Kb-1100 Kb-1010 Kb-1101 Kb-1011 Kb-1110
Kc-1001 Kc-1100 Kc-1010 Kc-1101 Kc-1011 Kc-1110
Kd-1001 Kd-1100 Kd-1010 Kd-1101 Kd-1011 Kd-1110
Ka-0000 Ka-0100 Ka-0001 Ka-0101 Ka-0010 Ka-0110 Ka-0011
Ka-0000 Ka-0000 Ka-0000 Ka-0000 Ka-0000 Ka-0000 Ka-0000 Ka-0000
Ka-0001 Ka-0001 Ka-0001 Ka-0001 Ka-0001 Ka-0001 Ka-0001 Ka-0001
Ka-0010 Ka-0010 Ka-0010 Ka-0100 Ka-0100 Ka-0100 Ka-0100 Ka-0010
Ka-0011 Ka-0011 Ka-0010 Ka-0101 Ka-0101 Ka-0101 Ka-0110 Ka-0100
Kb-1001 Kb-1001 Kb-1010 Kc-1001 Kc-1001 Kc-1010 Kd-1001 Ka-0110
Kb-1010 Kb-1100 Kb-1100 Kc-1010 Kc-1100 Kc-1100 Kd-1010 Kd-1001
Kb-1011 Kb-1101 Kb-1110 Kc-1011 Kc-1101 Kc-1110 Kd-1011 Kd-1101
Kd-1100 Kd-1010
Kd-1100 Kd-1110

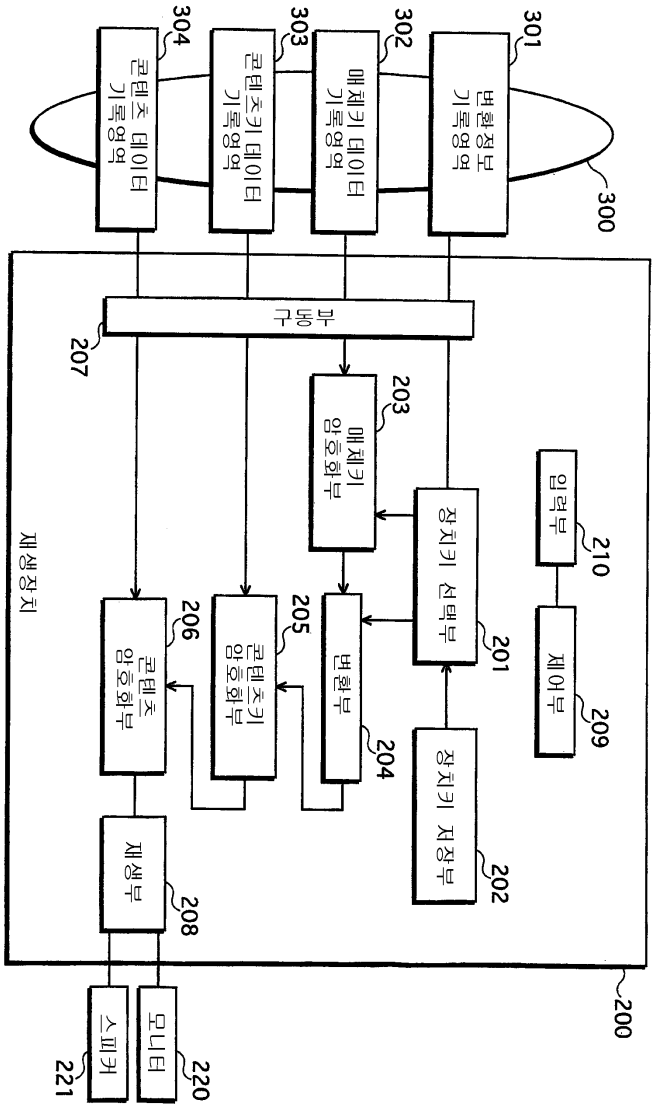
도면4


4A
MK
0101
MK'
암호화부
Ka-0101
E(Ka-0101,MK')
4B
MK
01011100
MK''
암호화부
Kb-1100
E(Kb-1100,MK'')
4C
MK
01011001
MK'''
암호화부
Kd-1001
E(Kd-1001,MK''')

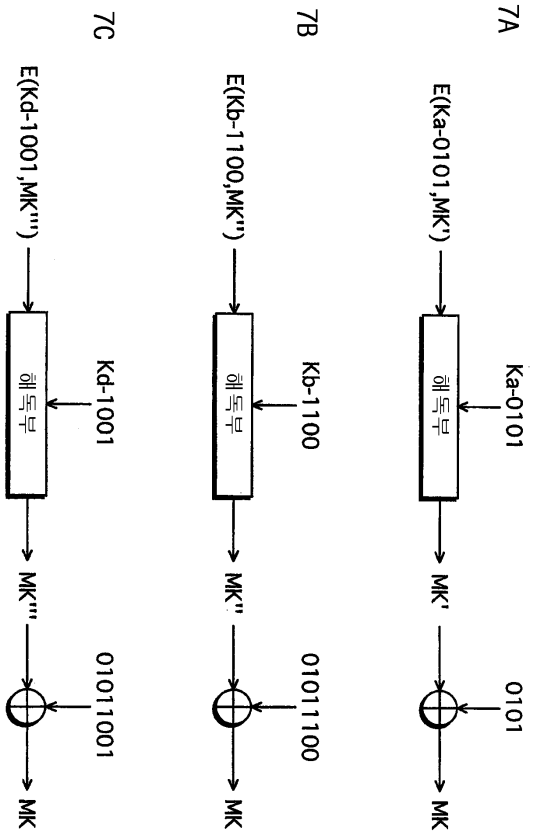
도면5


300
변환정보 기록영역
0101
1100
1001
301
매체키 데이터 기록영역
E(Ka-0101,MK')
E(Kb-1100,MK'')
E(Kd-1001,MK''')
302
콘텐츠키 데이터기록영역
E(MK,CK)
303
콘텐츠 데이터 기록영역
E(CK, 콘텐츠)
304

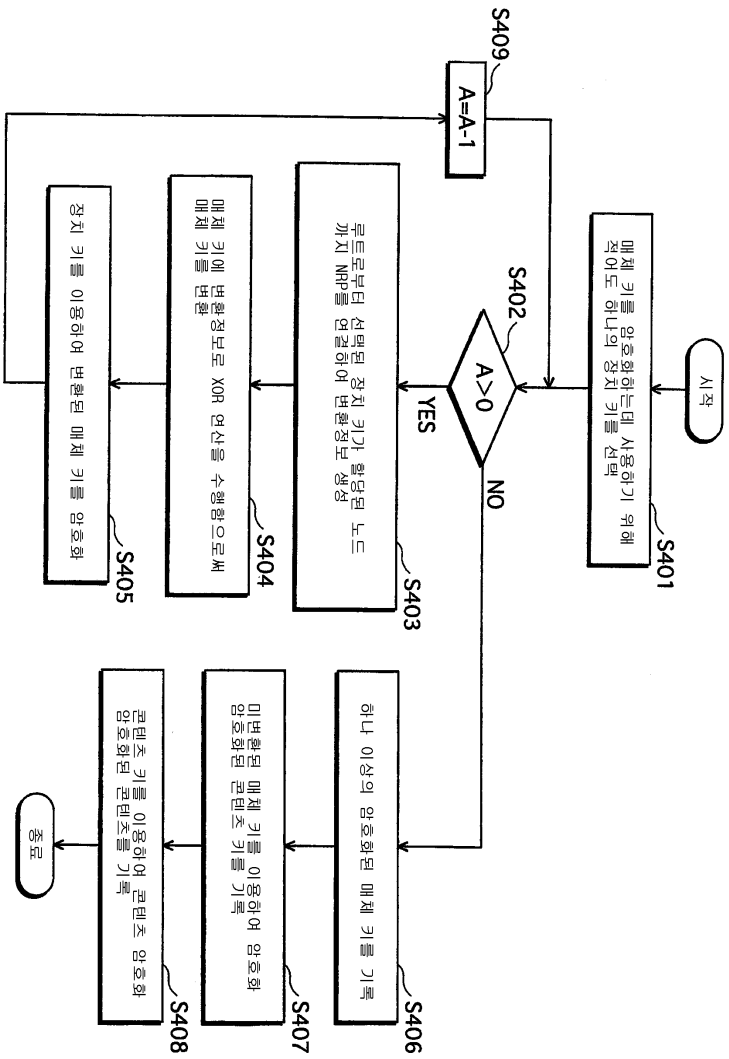
도면6


300
301
변환정보 기록영역
302
매체키 데이터 기록영역
303
콘텐츠키 데이터 기록영역
304
콘텐츠 데이터 기록영역
207
구성부
203
매체키 암호화부
장치키 선택부
201
입력부
210
제어부
209
장치키 저장부
202
변환부
204
205
콘텐츠키 암호화부
206
콘텐츠 암호화부
재생부
208
재생장치
200
스피커
221
모니터
220

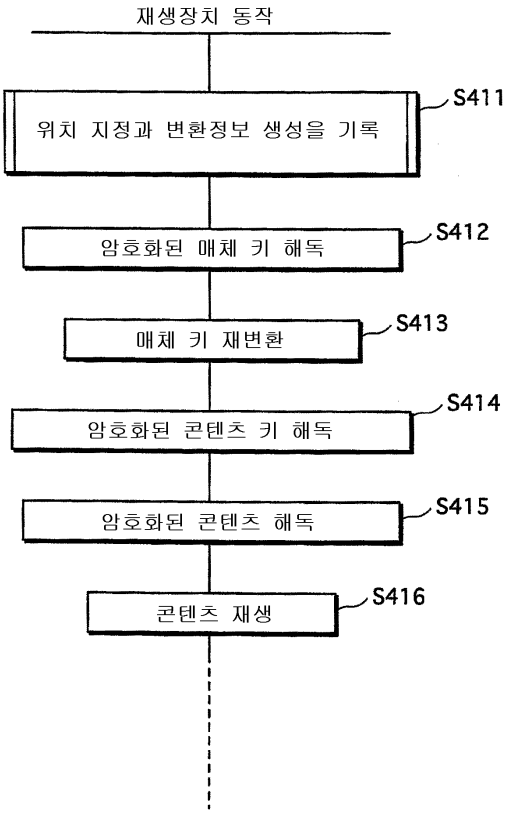
도면7


7A
E(Ka-0101,MK')
해독부
Ka-0101
MK'
0101
MK
7B
E(Kb-1100,MK'')
해독부
Kb-1100
MK''
01011100
MK
7C
E(Kd-1001,MK''')
해독부
Kd-1001
MK'''
01011001
MK

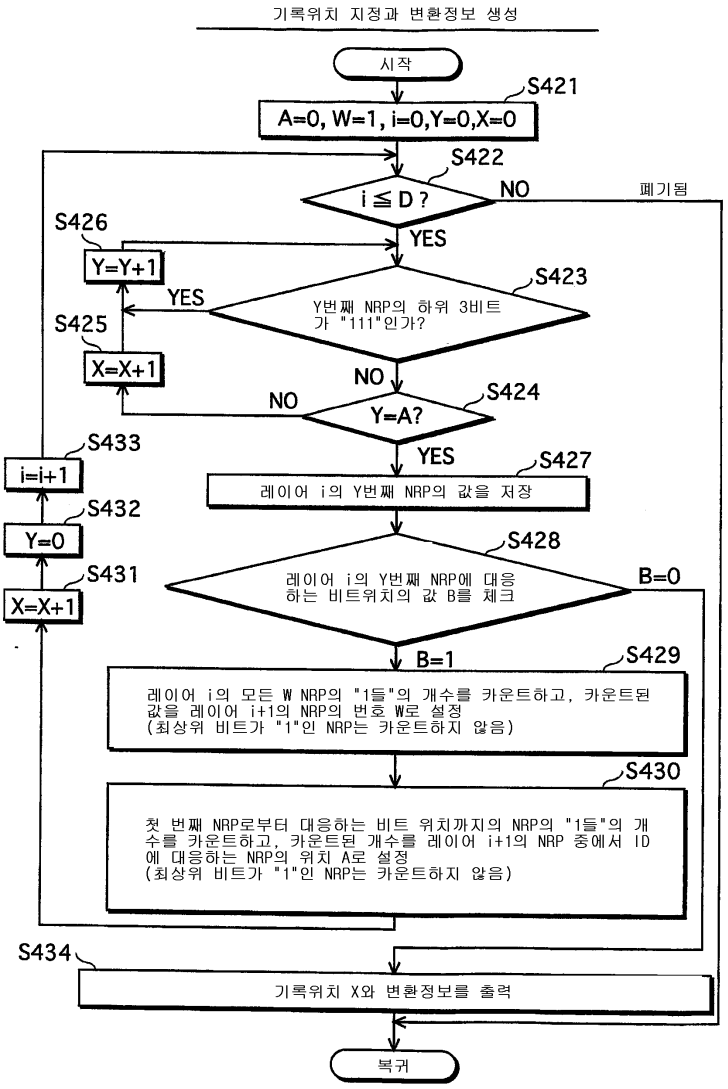
도면8


시작
S401
매체 키를 암호화하는데 사용하기 위해 적어도 하나의 정지 키를 선택
S402
A>0
YES
NO
S403
루트쿠브텀 선택된 정지 키가 할당된 노드까지 NRP를 연결하여 변환정보 생성
S404
매체 키에 변환정보로 XOR 연산을 수행함으로써 매체 키를 변환
S405
정지 키를 이용하여 변환된 매체 키를 암호화
S409
A=A-1
S406
하나 이상의 암호화된 매체 키를 기록
S407
미변환된 매체 키를 이용하여 암호화 콘텐츠 키를 기록
S408
콘텐츠 키를 이용하여 콘텐츠를 암호화 암호화된 콘텐츠를 기록
종료

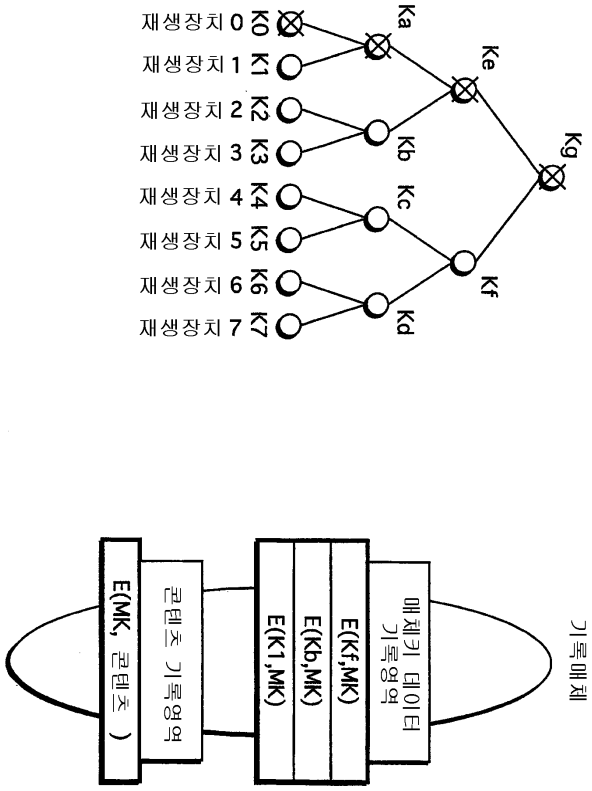
도면9


재생장치 동작
위치 지정과 변환정보 생성을 기록
S411
암호화된 매체 키 해독
S412
매체 키 재변환
S413
암호화된 콘텐츠 키 해독
S414
암호화된 콘텐츠 해독
S415
콘텐츠 재생
S416

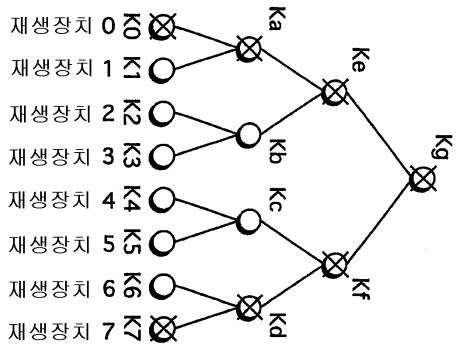
도면10

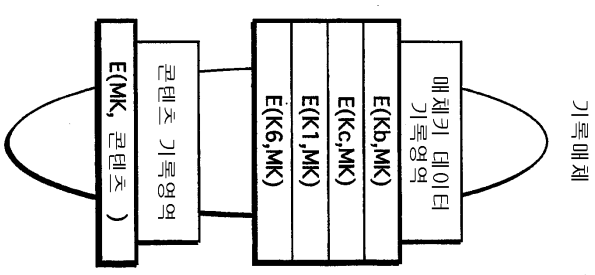

기록위치 지정과 변환정보 생성
시작
S421
A=0, W=1, i=0,Y=0,X=0
S422
i ≦ D ?
NO
폐기됨
YES
S426
Y=Y+1
S423
YES
Y번째 NRP의 하위 3비트 가 "111"인가?
S425
X=X+1
NO
NO
S424
Y=A?
YES
S427
레이어 i의 Y번째 NRP의 값을 저장
S428
레이어 i의 Y번째 NRP에 대응 하는 비트위치의 값 B를 체크
B=0
B=1
S429
레이어 i의 모든 W NRP의 "1들"의 개수를 카운트하고, 카운트된 값을 레이어 i+1의 NRP의 번호 W로 설정 (최상위 비트가 "1"인 NRP는 카운트하지 않음)
S430
첫 번째 NRP로부터 대응하는 비트 위치까지의 NRP의 "1들"의 개수를 카운트하고, 카운트된 개수를 레이어 i+1의 NRP 중에서 ID에 대응하는 NRP의 위치 A로 설정 (최상위 비트가 "1"인 NRP는 카운트하지 않음)
S433
i=i+1
S432
Y=0
S431
X=X+1
S434
기록위치 X와 변환정보를 출력
복귀

도면11


재생장치 0 K0
재생장치 1 K1
재생장치 2 K2
재생장치 3 K3
재생장치 4 K4
재생장치 5 K5
재생장치 6 K6
재생장치 7 K7
Ka
Kb
Kc
Kd
Ke
Kf
Kg
매체키 데이터 기록영역
E(Kf,MK)
E(Kb,MK)
E(K1,MK)
콘텐츠 기록영역
E(MK, 콘텐츠)
기록매체

도면12


재생장치 0
재생장치 1
재생장치 2
재생장치 3
재생장치 4
재생장치 5
재생장치 6
재생장치 7
K0
K1
K2
K3
K4
K5
K6
K7
Ka
Kb
Kc
Kd
Ke
Kf
Kg


E(MK, 콘텐츠)
콘텐츠 기록영역
E(K6,MK)
E(K1,MK)
E(Kc,MK)
E(Kb,MK)
매체키 데이터 기록영역
기록매체