(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년02월12일
(11) 등록번호 10-1492669
(24) 등록일자 2015년02월05일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01)
(21) 출원번호 10-2010-7011591
(22) 출원일자(국제) 2008년11월25일
심사청구일자 2013년11월01일
(85) 번역문제출일자 2010년05월27일
(65) 공개번호 10-2010-0103474
(43) 공개일자 2010년09월27일
(86) 국제출원번호 PCT/EP2008/066108
(87) 국제공개번호 WO 2009/068511
국제공개일자 2009년06월04일
(30) 우선권주장
07121610.5 2007년11월27일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
US20040010467 A1
US7181624 B2
전체 청구항 수 : 총 14 항

(73) 특허권자
나그라비젼 에스에이
스위스, 체하-1033, 체슈아-주르-로잔, 루트 드 제네바 22
(72) 발명자
부르크카드, 앙투안
프랑스 에프-78180 몽티니 르 브르토뇌 루 루이스 앙투안 부갱빌 18
로비르, 세바스티앙
스위스 체하-1066 에빨랑쥐 르 그랜드-슈맹 122
(74) 대리인
김해중, 홍순우, 윤석운

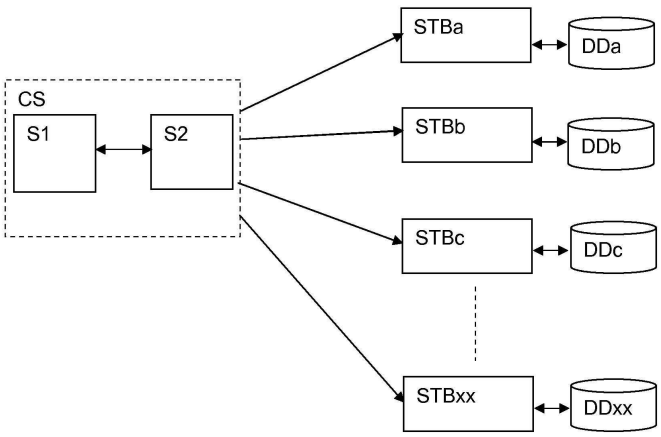
심사관 : 홍기완

(54) 발명의 명칭 **프로세싱 유닛에 의해 암호화된 콘텐츠 기록 및 복원 방법**

(57) 요 약

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작하는 방법으로, 상기 제1 프로세싱 유닛(STBa)과 제2 프로세싱 유닛(STBb)은 중심 서버(CS)에 의해 처리되는 고유키(Ka,Kb)를 구비한다. 프로세싱 유닛(STBa, STBb)은 콘텐츠에 관련된 파일에 의해 수반된 콘텐츠 키(CK)에 의해 암호화된 콘텐츠를 기록하려는 제거가능한 저장 메모리로의 접근성을 구비한다. 콘텐츠 키(CK)는 중심 서버(CS)에 의해 제공되는 두 개 이상의 상수(C1,C2)와 변수(R)의 제1 유닛(STBa)의 고유키(Ka)로부터 시작하여 순차적인 복호화를 통해 생성된다. 콘텐츠는 콘텐츠와 중심 서버(CS)에 의해 계산된 트랜스코딩 키(TK)를 수반한 파일에 저장된 상수(C1, C2)와 변수(R)를 이용함으로써 제2 프로세싱 유닛(STBb)의 고유키(Kb)로부터 시작하여 순차적인 복호화 과정을 통해 제2 프로세싱 유닛(STBb)에 의해 복원된다.

대 표 도 - 도1



특허청구의 범위

청구항 1

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는(operating) 방법으로서,

상기 제1 프로세싱 유닛(STBa) 및 제2 프로세싱 유닛(STBb)은 중심 서버(CS)에 의해 관리되는 각각의 고유키(Ka, Kb)를 구비하고 있고, 상기 제1 프로세싱 유닛(STBa) 및 제2 프로세싱 유닛(STBb)은 콘텐츠 키(CK)에 의해 암호화된(ciphered) 콘텐츠와 상기 콘텐츠와 관련된 데이터를 기록하도록 의도된 제거가능 저장 매체(removable stroage medium)에 액세스가능하고,

상기 콘텐츠 키(CK)는,

a) 제1 로컬키(KLa)를 획득하기 위해, 상기 제1 프로세싱 유닛(STBa)의 고유키를 이용해서 중심 서버(CS)에 의해 제공되는 제1 상수(C1)를 복호화(deciphering)하는 단계;

b) 중간키(KI)를 획득하기 위해, 제1 로컬키(KLa)를 이용해 중심 서버(CS)에 의해 제공되는 제2 상수(C2)를 복호화하는 단계;

c) 제1 프로세싱 유닛(STBa)에 의해 변수(R)를 획득하는 단계; 및

d) 변수(R)를 중간키(KI)로 복호화하여 얻어진 콘텐츠 키(CK)를 이용하여 콘텐츠를 암호화하고, 상기 제거가능 저장 매체 내에 암호화된 콘텐츠, 제1 상수(CI), 제2 상수(C2), 및 변수(R)를 저장하는 단계,

또는, d') 변수(R)와 동일한 콘텐츠 키(CK)를 사용하여 상기 콘텐츠를 암호화하고, 상기 제거가능 저장 매체 내에 암호화된 콘텐츠, 제1 상수(CI), 제2 상수(C2), 및 중간키(KI)로 암호화된 변수(R)를 저장하는 단계;

에 의해 생성되고,

상기 a) 내지 d) 또는 d') 단계에 따라 생성된, 콘텐츠 키(CK)로 암호화된 콘텐츠는 상기 제2 프로세싱 유닛(STBb)에 의해 복원되고,

상기 중심 서버(CS)는,

1) 중심 서버(CS)에서 제1 로컬키(KLa)를 획득하는 단계 - 상기 제1 로컬키(KLa)는 제1 프로세싱 유닛(STBa)의 고유키(Ka)에 의해 암호화되어 제1 상수(C1)가 획득됨 - ;

2) 중심 서버(CS)에서 제2 로컬키(KLb)를 획득하는 단계 - 상기 제2 로컬키(KLb)는 제2 프로세싱 유닛(STBb)의 고유키(Kb)에 의해 암호화될 때 제1 상수(C1)가 획득됨 - ;

3) 상기 제1 로컬키(KLa)에 의해 제2 상수(C2)를 복호화한 다음 복호화된 결과를 상기 제2 로컬키(KLb)에 의해 암호화함으로써 트랜스코딩 키(TK)를 계산하는 단계;

4) 상기 트랜스코딩 키(TK)를 상기 제2 프로세싱 유닛(STBb)으로 발송하는 단계;를 먼저 수행하고,

상기 제2 프로세싱 유닛(STBb)은,

A) 제2 로컬키(KLb)를 획득하기 위해, 상기 제2 프로세싱 유닛(STBb)의 고유키(Kb)에 의해, 제2 프로세싱 유닛(STBb)에 제공된 제1 상수(C1)를 복호화하는 단계;

B) 중간키(KI)를 획득하기 위해, 상기 제2 로컬키(KLb)를 이용해서 상기 트랜스코딩 키(TK)을 복호화하는 단계;

C) 콘텐츠 키(CK)를 획득하기 위해 상기 중간키(KI)를 이용해서 상기 변수(R)를 복호화하는 단계;

D) 상기 콘텐츠 키(CK)를 이용하여 상기 콘텐츠를 복호화하고 상기 제2 프로세싱 유닛(STBb)에 의해 상기 콘텐츠를 복원하는 단계;

를 수행하는 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 2

제1항에 있어서,

제1 및 제2 프로세싱 유닛(STBa, STBb)의 상기 고유키(Ka,Kb)는 상기 중심 서버(CS)에 저장되고, 상기 제1 로컬키(KLa)와 상기 제2 로컬키(KLb)는,

1') 제1 프로세싱 유닛(STBa)의 고유키(Ka)로 제1 상수(C1)를 복호화함으로써, 제1 로컬키(KLa)를 계산하는 단계; 및

2') 제2 프로세싱 유닛(STBb)의 고유키(Kb)로 제1 상수(C1)를 복호화함으로써, 제2 로컬키(KLb)를 계산 하는 단계를 통해 상기 중심 서버에 의해 획득되는 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 3

제1항에 있어서,

상기 변수(R)는 상기 제1 프로세싱 유닛(STBa)에 의해 생성된 난수인 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 4

제1항에 있어서,

상기 변수(R)는 상기 제1 프로세싱 유닛(STBa)에 저장된 리스트로부터 추출된 수인 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 5

제1항에 있어서,

상기 변수(R)는 상기 중심 서버(CS)에 의해 생성된 난수이며, 상기 제1 프로세싱 유닛(STBa)에 이용될 수 있는 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 6

제1항에 있어서,

상기 변수(R)는 상기 중심 서버(CS)에 저장된 리스트로부터 추출된 수이며, 상기 제1 프로세싱 유닛(STBa)에 이용될 수 있는 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 7

제1항에 있어서,

상기 변수(R)는 상기 제1 프로세싱 유닛(STBa)에 의한 각각의 콘텐츠 기록시에 상이한 값을 제시하는 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 8

제1항에 있어서,

b)와 c) 단계 사이에서, 파생된 중간키(KI')를 획득하기 위해 상기 중간키(KI)에 의해 하나 이상의 상수 또는 부가 변수를 복호화함으로써 하나 이상의 중간키(KI) 추가 유도하고, 단계 3)에서, 상기 트랜스코딩 키(TK)는 상기 제1 프로세싱 유닛(STBa)의 로컬키(KLa)를 사용하여 제2 콘텐츠(C2)로부터 하나 이상의 상수 또는 부가 변수를 복호화함으로써 계산되어 마지막 중간키(KI')를 획득하고 상기 마지막 중간키(KI')는 상기 제2 로컬키(KLb)에 의해 암호화되는 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 9

제1항에 있어서,

상기 제1 프로세싱 유닛(STBa)에 의해 콘텐츠가 기록되는 동안 단계 a), b), c), 및 d) 또는 d')에서 콘텐츠 키(CK)를 생성하는 동작과, 제2 프로세싱 유닛(STBb)에 의해 콘텐츠가 복원되는 동안 단계 A) 내지 C)에서 콘텐츠 키(CK)를 획득하는 동작은 상기 제1 프로세싱 유닛(STBa)과 상기 제2 프로세싱 유닛(STBb)의 각각의 칩셋에 의해 수행되는 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 10

제1항에 있어서,

암호화/복호화 동작은 대칭 키 알고리즘을 이용함으로써 수행되는 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 11

제1항에 있어서,

콘텐츠가 기록되는 동안, 상수(C1,C2)와 변수(R) 또는 상수(C1,C2)와 중간키(KI)를 사용하여 암호화된 변수(R)는 암호화된 콘텐츠를 수반한 파일(LCMa)에 저장되고, 중심 서버(CS)는 상기 트랜스코딩 키(TK)를 이동 파일(transfer file)(LClab)에 전송하고, 파일(LCMa, LClab)은 상기 콘텐츠를 복원하는 동안 상기 제2 프로세싱 유닛(STBb)에 이용될 수 있도록 구성되는 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 12

제11항에 있어서,

파일(LCMa)은 상기 제1 및 제2 프로세싱 유닛(STBa,STBb)과 관련된 보안 모듈의 키로 암호화되는 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 13

제1항에 있어서,

상기 제1 및 제2 프로세싱 유닛(STBa,STBb)은, 보안 모듈이 설치되며 상기 중심 서버에 의해 처리되는 유료 TV 디코더 또는 셋탑박스이고,

제거가능 저장 매체로 액세스가능한 제1 및 제2 프로세싱 유닛들(STBa,STBb)은, 콘텐츠를 기록한 것과 상이한 프로세싱 유닛 또는 동일한 프로세싱 유닛에 의해 복원하고자 하는 암호화된 콘텐츠를 기록할 수 있는 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

청구항 14

제1항에 있어서,

상기 제1 및 제2 프로세싱 유닛(STBa,STBb)은 내부 또는 외부 보안 모듈이 설치되고 중심 서버에 의해 관리되는 PC이고,

제거가능 저장 매체로 액세스가능한 제1 및 제2 프로세싱 유닛들(STBa,STBb)은 콘텐츠를 기록한 것과 상이한 프로세싱 유닛 또는 동일한 프로세싱 유닛에 의해 복원하고자 하는 암호화된 콘텐츠를 기록할 수 있는 것을 특징으로 하는

제1 프로세싱 유닛(STBa)에 의해 기록된 콘텐츠를 제2 프로세싱 유닛(STBb)에 의해 동작시키는 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 오디오/비디오 콘텐츠의 암호화된 디지털 데이터의 프로세싱 유닛 분야에 관한 것이다. 이들 유닛은 예를 들어 PC, 모바일 장비 또는 디지털 유료 TV 디코더와 같은 서로 상이한 멀티미디어 장비에 적용된다. 유닛은 일반적으로 나중에 복원할 목적인 콘텐츠를 기록하기 위한 하드 디스크, 광학 디스크, 카드, 모듈 또는 임의의 다른 종류의 대용량 메모리 같은 제거할 수 있는 저장 메모리나 외부 저장 메모리와 관련 있다.

배 경 기 술

[0002] 콘텐츠의 무제한 기록과 복원은 저작권에 의해 일반적으로 보호되는 콘텐츠가 남용될 가능성을 드러낸다. 복원 콘텐츠를 위한 많은 보호 수단과 제어 수단은 다음의 실시예에 도시된 바와 같이 발전 된다.

[0003] EP1169856B1호는 암호화된 콘텐츠에 접속하는 방법을 개시한다. 암호화된 콘텐츠는 콘텐츠의 복호화를 위해 요구된 키의 재암호화에 의해 로컬 네트워크에서 보호된다. 제1 유닛은 암호화된 데이터 콘텐츠를 수신하고 저장하며, 제1 유닛에 한정된 키를 사용하여 데이터의 복호키를 암호화한다. 데이터와 암호화된 키는 복호화를 위해 네트워크에 속한 제2 유닛에 전송된다. 실시예에 따르면, 제1 유닛에 관련된 키는 공개키(public key)이고, 상응하는 개인키(private key)는 제2 유닛에 위치된다.

[0004] US7181624호는 전송 스트림(transport stream)에서 디지털 데이터 방송의 기록 장치와 재생 장치를 개시한다. 이 장치는 전송 스트림에 포함된 각각의 데이터 패킷에 도착시간을 나타내는 일시적 데이터를 첨부한다. 블록키(block key)는 패킷의 일시적 데이터 도착시간이 각각 수반된 다수의 전송 패킷을 포함하는 데이터 블록을 암호화하기 위해 생성된다. 블록키(block key)는 일시적 데이터 도착시간을 포함하는 데이터 블록 고유의 부가적 정보를 포함하는 핵심 블록(root block)에서 생성되며 각각의 데이터 블록을 암호화한다. 따라서 디지털 데이터는 장치의 메모리에 저장된다. 데이터의 재생은 기록 동안 암호화하는 것에 반하는 복호화 과정에 따라 수행된

다.

[0005] US2004010467호는 모바일 장비의 메모리 카드를 개시한다. 모바일 장비는 암호화된 데이터 콘텐츠를 저장하기 위한 메모리 존(zone), 분배 시스템에 의해 전송된 허가(license) 데이터를 저장하기 위한 존(zone), 및 분배 시스템 공통의 공개키에 의해 증명된 인증 데이터를 저장하기 위한 복수의 존(zone)을 포함한다. 모바일 장비에서 발생된 분배 요청에 응답하여, 허가 서버는 메모리 카드의 진위를 확인하고 암호화된 콘텐츠 및 상응하는 라이센스를 모바일 장비에 분배한다. 제1 모바일 장비에 의해 받은 암호화된 콘텐츠는 상응하는 라이센스가 확보될 경우에만 콘텐츠를 잘 활용할 수 있는 제2 모바일 장비로 이동될 수 있다. 따라서 제2 장비는 메모리 카드의 적합성을 확인할 분배 시스템에서 콘텐츠의 복호키를 포함한 라이센스를 얻어야만 할 것이다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 목적은 하나의 프로세싱 유닛에서 또 다른 프로세싱 유닛으로 이동될 수 있는 저장 메모리에 기록된 콘텐츠의 과도한 복제에 대한 보호를 향상시키는데 있다.

[0007]

과제의 해결 수단

[0008] 본 발명의 목적은 제1 프로세싱 유닛에 의해 기록되는 콘텐츠를 제2 프로세싱 유닛에 의해 동작하는 방법으로 달성된다. 상기 제1 프로세싱 유닛과 제2 프로세싱 유닛은 중심 서버에 의해 관리되는, 각각의 고유키(Ka,Kb)를 구비한다. 프로세싱 유닛은 콘텐츠에 관련된 데이터 및 콘텐츠 키에 의해 암호화된 콘텐츠를 기록할 목적인 제거할 수 있는 저장 메모리에 접근할 수 있다. 콘텐츠 키는 다음 a) 내지 d) 또는 d')의 단계에 따라 생성되는 것이다.

[0009] a) 제1 로컬키(local key)를 획득하기 위하여, 중심 서버에서 제공된 제1 상수를 제1 프로세싱 유닛의 고유키에 의해 복호화하는 단계,

[0010] b) 중간키(intermediate key)를 획득하기 위하여, 제1 로컬키를 구비한 중심 서버에 의해 제공된 제2 상수를 복호화하는 단계,

[0011] c) 제1 프로세싱 유닛에 의한 변수를 획득하는 단계와,

[0012] d) 중간키로 변수를 복호화함으로써 획득한 콘텐츠 키를 구비한 콘텐츠를 암호화하고, 암호화된 콘텐츠, 제1 상수, 제2 상수 및 변수를 저장 메모리에 저장하는 단계, 또는

[0013] d') 변수와 동일한 콘텐츠 키를 구비하는 콘텐츠의 암호화하고, 암호화된 콘텐츠, 제1 상수, 제2 상수 및 중간키를 사용하여 암호화된 변수를 저장 메모리에 저장하는 단계.

[0014] 이 방법은 a),b),c),d) 단계 또는 a),b),c),d') 단계를 따라 생성된 콘텐츠 키를 구비한 암호화된 콘텐츠가 제2 프로세싱 유닛에 의해 복원되는 것을 특징으로 한다. 다음 단계는 중심 서버에 의해 미리 수행되는 단계이다.

[0015] 1. 중심 서버에 의해 제1 로컬키를 획득하는 단계로, 제1 로컬키는 제1 프로세싱 유닛 고유키에 의해 암호화할 때 제1 상수를 획득하는, 제1 로컬키 획득 단계,

[0016] 2. 중심 서버에 의해 제2 로컬키를 획득하는 단계로, 제2 로컬키는 제2 프로세싱 유닛 고유키에 의해 암호화할 때 제1 상수를 획득하는 제2 로컬키 획득 단계,

[0017] 3. 제1 로컬키에 의해 제2 상수를 복호화한 다음, 그 결과를 제2 로컬키에 의해 암호화함으로써 트랜스코딩 키를 계산하는 단계,

[0018] 4. 제2 프로세싱 유닛으로 트랜스코딩 키를 발송하는 단계.

[0019] 다음 단계는 제2 프로세싱 유닛에 의해 수행된다.

[0020] A. 제2 프로세싱 유닛 고유키에 의해, 제2 로컬키를 획득하기 위해 제공되는 제1 상수를 복호화하는 단계,

[0021] B. 중간키를 획득하기 위해, 제2 로컬키를 구비한 트랜스코딩 키를 복호화하는 단계,

[0022] C. 콘텐츠 키를 획득하기 위해 중간키에 의해 변수를 복호화하는 단계,

[0023] D. 콘텐츠 키를 구비한 콘텐츠를 복호화하며, 제2 프로세싱 유닛에 의해 콘텐츠를 복원하는 단계.

[0024] 이 방법은 프로세싱 유닛의 고유키를 중심 서버 또는 제거할 수 있는 메모리의 저장 장치로 전송하여 프로세싱 유닛 고유키를 드러내지 않는 중요한 장점을 제공한다. 콘텐츠를 암호화 및 복호화하는 동안 이용된 상수 및 변수인 키는 유닛 고유키로부터 얻어지며, 이들 키의 지식은 고유키의 검색을 허락하지 않는다. 콘텐츠의 기록과 복원 과정 동안, 관련된 유닛과 중심 서버에 의해 알려진 유닛은 암호화/복호화 동작을 위해 콘텐츠와 연관된 데이터를 이용할 수 있다.

[0025] 제1 유닛에 의한 콘텐츠 기록 동안 콘텐츠키를 생성하는 a),b),c),d) 또는 d') 단계의 동작과 제2 유닛에 의한 콘텐츠 복원 동안 콘텐츠키를 획득하기 위한 A 내지 C 단계의 동작은 제1 유닛과 제2 유닛 각각의 칩셋(chipset)에 의해 바람직하게 수행된다. 칩셋은 유닛의 상이한 요소 사이에 데이터 교환 처리를 프로세서에 허용하는 전자전 회로망 셋트이다. 유닛의 칩셋 레벨에서 이들 동작의 실행은 프로세서에 의해 이용되는 유닛 고유키를 발견하기 위해 교환된 신호의 분석으로 구성된 모든 실질적인 공격을 막는 것이 목표이다. 따라서 고유키, 로컬키 및 중간키는 칩셋 외부에 접근할 수 없다. 또한 암호화/복호화 모듈은 동일한 칩셋에 배치되어 콘텐츠 키 역시 외부로부터 접근할 수 없을 것이다.

[0026] 콘텐츠를 기록하는 동안의 복호화 동작 단계 a), b) 및 d)의 트랜스코딩을 계산하는 동안의 복호화/암호화, 그리고 콘텐츠를 복원하는 동안의 단계 A,B 및 C의 복호키는 암호화 동작에 의해 각각의 암호화/복호화 동작으로 대체될 수 있다고 알려져야 한다.

발명의 효과

[0027] 본 발명을 따르는 프로세싱 유닛에 대해 암호화된 콘텐츠를 기록하고 복원하는 방법은 저장 메모리에 기록된 콘텐츠의 과도한 복제에 대한 보호를 향상시킬 수 있다.

도면의 간단한 설명

[0028] 본 발명은 제한적이지 않은 실시예로 주어진 그림과 관련한 상세한 설명을 통해 더 잘 이해될 것이다.

도 1은 중심 서버에 의해 관리되는 제거할 수 있는 콘텐츠 저장 메모리가 설치된 복수의 프로세싱 유닛을 도시한 도면이다.

도 2는 프로세싱 유닛에 의한 콘텐츠의 기록 과정을 도시한 도면으로, 콘텐츠는 콘텐츠 키에 의해 암호화되며 프로세싱 유닛의 고유키로부터 얻어지며, 또한 콘텐츠는 중심 서버에 의해 제공되는 두개의 상수 및 국부적으로 생성된 변수로부터 생성된다.

도 3은 중심 서버에 의해 수행되는 트랜스코딩 키(transcoding key)의 생성을 도시한 도면이다.

도 4는 제1 프로세싱 유닛에 의해 기록되고 암호화된 콘텐츠를 제2 프로세싱 유닛에 의해 복원되는 과정을 도시한 도면으로, 여기서, 콘텐츠 키는 기록하는 동안 사용되는 상수 및 변수로부터, 중심 서버에 의해 생성된 트랜스코딩 키(transcoding key)로부터 복호화된다.

발명을 실시하기 위한 구체적인 내용

[0029] 본 발명의 방법은 유료 TV 프로그램의 디코더(셋탑박스(set top box))와 같은 오디오/비디오 콘텐츠 유닛 프로세싱에 예를 들어 적용된다. 이들 유닛의 각각 하나는 보안 모듈에 일반적으로 연관된다. 보안 모듈은 다양한 암호화/복호화 키를 포함한 훼손-방지(tamper-proof)장치, 네트워크 사용자를 식별하기 위해 이용된 데이터및 방송 오디오/비디오 콘텐츠의 수신을 위해 획득된 사용자의 권리를 정의하는 데이터로 잘 알려져 있다. 보안 모듈은 판독기(reader)에 삽입된 제거 가능한 스마트 카드, 마더보드에 결합된 집적회로, 거의 모든 모바일 장비 또는 소프트 모듈 및/또는 칩셋 내에 캡슐화된 자료인 SIM(Subscriber Identity Module) 타입 카드와 같은 상이한 형태를 구비할 수 있다.

[0030] 도 1의 다이어그램은 제거할 수 있는 하드 디스크 및/또는 광학 디스크, 플래쉬 타입의 비휘발성 메모리 또는

프로그램 콘텐츠의 기록과 그 후의 복원이 허용되는 그 이외의 것들과 같은 외부 저장 미디어를 바람직하게 갖춘 중심 서버(헤드 엔드)에 의해 관리되는 유닛을 도시한다. 저장 미디어의 호환성 때문에, 주어진 유닛에 의해 등록된 콘텐츠는 동일한 서버에 의해 관리되는 또 다른 유닛을 통해 재생될 수 있다. 물론, 유닛에 의해 등록된 콘텐츠는 동일한 유닛에 의해 복원될 수 있다. 콘텐츠 동작 기록과 복원은 콘텐츠의 암호화/복호화에 필요한 파라미터와 키를 제공하는 중심 서버에 의해 제어된다.

[0031] 또한 프로세싱 유닛은 내부 또는 외부 보안 모듈을 갖춘 모바일 또는 고정된 PC로 구성될 수 있다. 예를 들어, 외부 보안 모듈은 판독기에 삽입된 스마트 카드 형태이거나 USB 시리얼 인터페이스 또는 컴퓨터에 이용할 수 있는 일부 다른 인터페이스를 수단으로 컴퓨터에 연결된 전자 키(동글)의 형태이다. 유닛 또는 유닛들은 중심 서버에 의해 관리되고, 또한 하드 디스크 및/또는 광학 디스크, 플래쉬 타입 또는 다른 형태의 비휘발성 메모리와 같은 제거할 수 있는 저장 미디어로의 접근성을 가지며, 동일한 유닛이나 기록된 콘텐츠를 구비한 것과 상이한 유닛에 의해 복원될 예정인 암호화된 콘텐츠를 기록 할 수 있다.

[0032] 예시적인 구성에 따르면, 중심 서버는 제1 서버(S1)를 포함한다. 제1 서버에서는 유닛(STBa,STBb,… STBxx)의 고유키(Ka,Kb,…Kxx)가 생성된 후 저장되며, 제2 서버(S2)는 키 계산에 이용되고 유닛에 의해 기록된 콘텐츠의 복호화를 위해 필요한 키 파일을 제공한다. 중심 서버(CS)에 설치된 유닛의 제1 연결 동안, 제1 서버(S1)는 고유키를 유닛에 제공하며, 유닛은 단 한번만 기록 가능한 특정 메모리에 고유키를 저장한다. 제2 서버(S2)는 유닛의 고유키를 저장하지 않지만, 키는 유닛의 고유키로부터 파생된다.

[0033] 프로세싱 유닛의 메모리에 기록된 콘텐츠는 두 개의 상수 C1과 C2로 표시된 중심 서버(CS)에 의해 제공된 두 개 파라미터의 연속적인 복호화 결과와 프로세싱 유닛에 의해 국부적으로 생성된 변수(R)의 결과인 콘텐츠 키(CK)에 의해 암호화된다. 도 2의 다이어그램은 콘텐츠(Ct)의 암호일 수 있는 키(CK)를 획득하기 위해 수행되는 상이한 복호화 단계를 도시한다.

[0034] 제1 단계에서, 상수(C1)는 로컬키(KLa)를 획득하기 위해 프로세싱 유닛(STBa)의 특정한 고유키(Ka)에 의해 복호화된다. 고유하고 변함없는 키(Ka)는 유닛 칩셋의 읽기 전용 메모리에 저장되고 유닛 칩셋의 외부에서 접근할 수 없다. 복호화는 T^{-1}로 표시된 블록과 T로 표시된 블록에 의한 암호화에 의해 도 2, 도 3 및 도 4에 제시된다. 암호화/복호화는 DES 타입(Data Encryption Standard), TDES(Triple DES), IDEA(International Data Encryption Algorithm), AES(Advanced Encryption System) 등의 대칭 키 알고리즘을 이용함으로써 바람직하게 수행된다.

[0035] 실시예에 따르면, 각각의 유닛은 한 쌍의 비대칭 키를 포함한다. 공개키는 제1 상수(C1)와 유닛 칩셋에 저장된 상응하는 개인키를 복호화하기 위해 이용된다. 또한 공개키는 하단의 실시예(1)와 관련하여 중심 서버로 잘 알려져 있다.

[0036] 제1 단계에서 구해진 로컬키(KLa)는 중간키(KI)를 획득하기 위해 제2 상수(C2)를 복호화하도록 이용된다. 중간키(KI)는 변수(R)를 복호화하고 콘텐츠 키(CK) 획득하기 위한 마지막 단계에 이용된다. 변수(R)의 이용 때문에, 콘텐츠 키(CK)는 각각의 콘텐츠 기록에 대해 다를 것이며 콘텐츠 키는 이전 기록 동안 획득한 키로부터 추정될 수 없다. 또한, 콘텐츠 키(CK)는 유닛(STBa)의 고유키(Ka)에 의존하거나 유닛(STBa)의 고유키(Ka)에서 파생된다. 그 이유는 콘텐츠 키(CK)가 상기 고유키(Ka)를 사용하여 수행된 초기 파라미터(C1)의 복호화 결과인 키에 의해 그 후의 파라미터(C2,R)의 복호화가 순차적으로 진행된 결과이기 때문이다.

[0037] 콘텐츠는 키(CK)로 암호화된 형태와 상수 C1, C2 및 변수(R)를 포함하는 파일(LCMa) 정보가 동반된 형태로 저장 유닛(DDa)에 저장된다. 이 파일(LCMa)은 유닛(STBa)에 관련된 보안 모듈로부터 발행된 키에 의해 암호화될 수 있다.

[0038] 선택에 따라, 콘텐츠의 복원 변수를 결정하기 위해 콘텐츠 키(CK)는 변수(R)와 동등하며 파일(LCMa)은 중간키(KI)로 암호화된 변수(R)를 포함하고, 중간키(KI)가 필요해진다.

[0039] 상기 개시된 방법의 단계 d)는 콘텐츠 키(CK)와 동등한 변수(R)에 의해 콘텐츠 암호화하고, 암호화된 콘텐츠, 상수 C1, C2 및 저장 메모리에 중간키(KI)로 암호화된 변수(R)의 저장하는 단계 d')로 대체된다.

[0040] 다른 실시예에 따르면, 상수 복호화와 부가 변수의 하나 이상 추가 단계는 단계 b)와 콘텐츠 키(CK) 생성과정인 단계 c) 사이에 삽입될 수 있다. 따라서, 획득한 마지막 중간키(KI')는 제2 콘텐츠(C2)의 복호화로부터 발행되는 제1 키(KI)에서 파생된 것으로 정의된다. 모든 부가 상수와 부가 변수는 콘텐츠 복원에 이용될 파일(LCMa) 내에 저장된다.

[0041] 변수(R)는 프로세싱 유닛에 의해 생성된 난수(random number)의 형태가 바람직하다. 또한 변수는 메모리에 저장된 리스트로부터 유닛에 의해 추출된 수 형태로 나타난다.

[0042] 또 다른 실시예에 따르면, 변수(R)는 중심 서버(CS)에 저장되고 프로세싱 유닛(STBa)에 제공된 리스트로부터 생성되거나 추출될 수 있다.

[0043] 두 가지의 실시예에서, 변수(R)의 상이한 값은 유닛에 의한 콘텐츠 각각의 기록에서 제공된다. 변수는 임의로 생성되거나 리스트로부터 발생된다.

[0044] 암호화된 콘텐츠가 콘텐츠를 기록한 동일한 유닛(STBa)에 의해 복원될 때, 콘텐츠 키(CK)의 판단 과정은 요구된 파라미터(C1, C2, R)를 포함한 파일(LCMa) 때문에 기록하는 동안 시행된 것과 동일하다. 사실, 유닛의 고유키(Ka)를 구비하는 상수(C1=[KLa]Ka)의 복호화는 상수(C2=[KI]KLa)를 복호화하기 위해 이용되는 로컬키(KLa)를 생성하며, 또한 콘텐츠 키(CK)를 생성하기 위한 변수(R=[CK]KI)를 복호화하도록 하는 중간키(KI)를 생성한다.

[0045] 하나 이상의 부가 상수 또는 부가 변수가 기록 과정 동안 이용되는 실시예에서, 유닛(STBa)의 고유키(Ka)를 구비하는 제1 상수(C1)로부터 이들 상수 또는 변수의 연이은 복호화는 마지막 중간키(KI')를 생성한다. 마지막 중간키(KI')는 콘텐츠 키(CK)를 획득하기 위해 변수(R)를 복호화하거나 변수들을 연속적으로 복호화하기 위해 이용될 것이다.

[0046] 암호화된 콘텐츠가 콘텐츠를 기록한 유닛과 상이한 유닛(STBa)에 의해 복원될 때, 콘텐츠 키를 결정한 유닛의 고유키에 콘텐츠 키(CK)가 의존하기 때문에 콘텐츠 키(CK) 결정 과정은 더 복잡해진다. 도 4의 예에서, 콘텐츠는 제1 프로세싱 유닛(STBa)에 의해 기록된 다음에 제1 유닛(STBa)과 동일한 서버(CS)에 의해 관리되는 제2 유닛(STBb)으로 전달된다.

[0047] 제2 유닛(STBb)에 의한 복원 과정은 트랜스코딩 키(TK)의 중심 서버(CS)에 의한 생성을 요구한다. 트랜스코딩 키(TK)는 암호화된 콘텐츠가 다뤄지는 제2 유닛(STBb)에 전송될 것이다. 두 개의 실시예가 고려될 수 있다.

[0048] 1) 유닛의 고유키(Ka, Kb, …Kxx)는 중심 서버(CS)에 의해 알려져 있거나 각각 제2 서버(S2)에 의해 알려져 있다.

[0049] 제1 실시예에 따르면, 중심 서버는 제1 유닛(STBa)의 고유키(Ka)를 사용하여 제1 상수(C1)를 복호화함으로써 제1 유닛(STBa)으로부터 로컬키(KLa)를 계산한다.

[0050] 그 다음에 중심 서버는 제2 유닛(STBb)의 고유키(Kb)를 사용하여 동일한 상수(C1)를 복호화함으로써 제2 유닛(STBb)으로부터 로컬키(KLb)를 계산한다.

[0051] 트랜스코딩 키(TK)는 제2 로컬키(KLb)를 사용하여 암호화될 중간키(KI)를 획득하기 위해 제1 로컬키(KLa)를 사용하여 제2 상수(C2=[KI]KLa)를 복호화함으로써 계산된다. 따라서, 획득한 트랜스코딩 키(TK=[KI]KLb)는 파일(LC1ab) 전송시에 제2 유닛(STBb)으로 전송된다.

[0052] 2) 유닛의 고유키(Ka, Kb, …Kxx)는 중심 서버(CS)에 의해 알려져 있지 않거나 더 정확히 말하면 보통 말하는 제2 서버(S2)에 의해 알려져 있지 않지만, 고유키의 파생된 로컬키(KLa, KLb,…KLxx)는 상수(C1, C2)처럼 제2 서버(S2)에 저장된다.

[0053] 도 3에 개시된 제2 실시예에 따르면, 제1 프로세싱 유닛(STBa)의 로컬키(KLa)와 제2 프로세싱 유닛(STBb)의 로컬키(KLb) 각각의 처리를 시도하는 중심 서버는 제1 로컬키(KLa)에 의해 제2 상수(C2=KI[KLa])를 복호함으로써 제일 먼저 중간키(KI)를 계산한다. 그 다음은 제2 로컬키(KLb)를 사용하여 중간키(KI)를 암호화 함으로써 트랜스코딩 키(TK=[KI]KLb)를 계산한다. 트랜스코딩 키(TK=[KI]KLb)는 파일(LC1ab)에 의한 제1 실시예처럼 제2 유닛(STBb)으로 전송된다.

[0054] 암호화된 콘텐츠를 수반하고 상수(C1), 및 변수(R)를 포함한 파일(LCMa) 때문에, 제2 유닛(SRBb)은 상응하는 로컬키(KLb)를 획득하기 위해 고유키(Kb)를 사용하여 제1 상수(C1)를 복호화한다. 파일(LC1ab)이 트랜스코딩 키(TK=[KI]KLb)를 제공하면 트랜스코딩 키(TK=[KI]KLb)는 이전에 획득한 로컬키(KLb)를 사용하여 복호화한다. 그 결과, 중간키(KI)를 구한다. 제2 유닛(STBb)이 콘텐츠를 복호화하고 이를 명백히 실행하는 것을 허용하는 콘텐츠 키(CK)를 획득하기 위해, 변수(R=[CK]KI)를 복호화하는데 필요한 변수 복호화는 중간키(KI)를 구한다.

[0055] 이 방법의 장점은 두 가지의 실시예에서 프로세싱 유닛에 한정된 고유키가 동일한 중심 서버에 의존하는 일부 유닛에 기록되거나 복원되는 동안 전송되지 않는다는 것이다. 또한 고유키는 암호화된 콘텐츠 데이터를 수반한

파일에 저장되지 않는다.

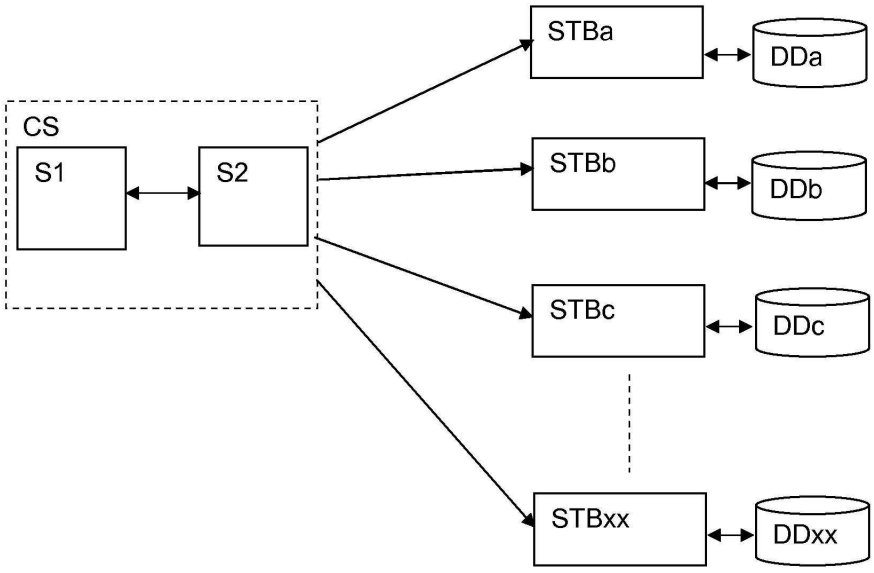
[0056] 제2 실시예는 더 높은 보안 레벨을 제공하기 때문에 더 바람직할 수 있다. 각각의 프로세싱 유닛(STBa, STBb)에 한정된 고유키(Ka, Kb)는 각각의 유닛(STBa, STBb)의 각각의 칩셋에서처럼 본래 형태로 제2 서버(S2)에 저장되지 않는다는 사실 때문에 더 높은 보안 레벨이 제공된다. 하지만, 서버는 각각의 유닛의 로컬키(KLa, KLb)를 저장한다. 로컬키(KLa, KLb)는 제1 상수(C1)를 획득하는 프로세싱 유닛(STBa, STBb)에 상응하는 특정한 키(Ka, Kb)에 의해 암호화된다. 도 2와 도 4에 도시된 예에서, 상수(C1)는 [KLa]Ka와 [KLb]Kb와 동등하다.

[0057] 또한 제2 유닛(STBb)에 의한 콘텐츠 키의 복원 동안 콘텐츠 키(CK) 계산을 위한 동작은 제2 유닛의 칩셋에 의해 수행된다.

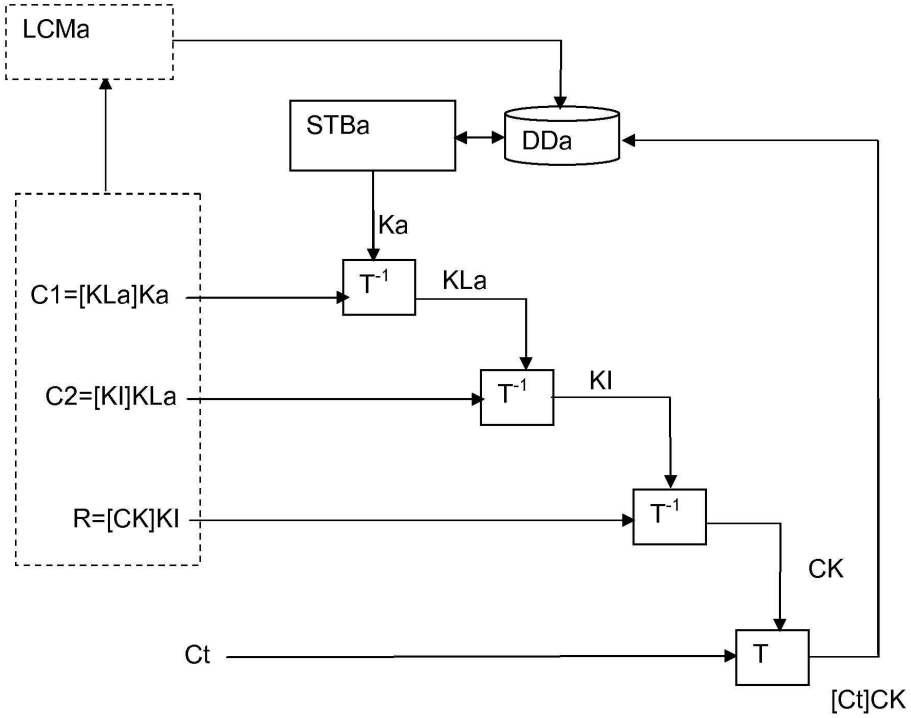
[0058] 하나 이상의 부가 항수 또는 변수가 기록되는 과정에서 이용되는 실시예에서, 트랜스코딩 키(TK)는 유닛(STBa)의 로컬키(KLa)를 사용하여 제2 상수(C2)로부터 이들 상수 또는 변수를 연속적으로 복호화함으로써 계산되어 제2 유닛(STBb)의 로컬키(KLb)를 사용하여 암호화될 마지막 중간키(KI')를 획득한다.

도면

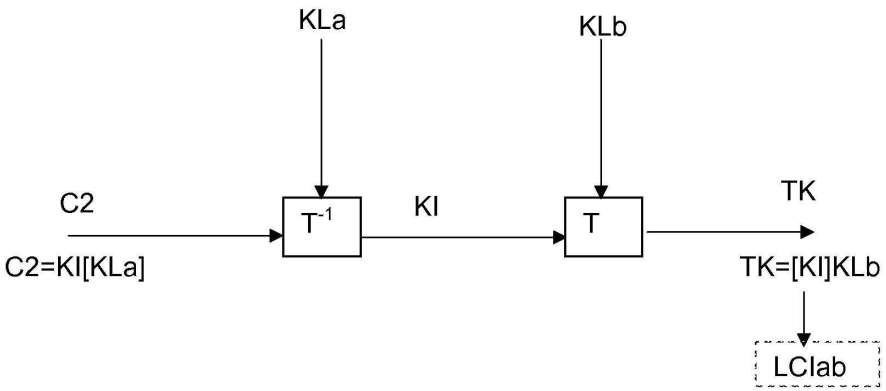
도면1



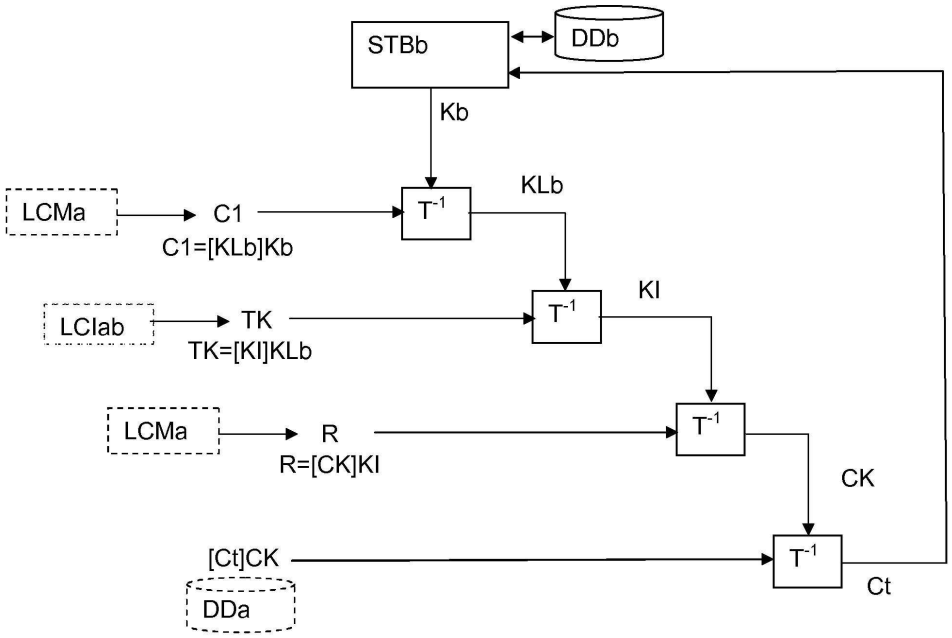
도면2


LCMa
STBa
DDa
Ka
C1=[KLa]Ka
T-1
KLa
C2=[KI]KLa
T-1
KI
R=[CK]KI
T-1
CK
Ct
T
[Ct]CK

도면3


KLa
KLb
C2
T-1
KI
T
TK
C2=KI[KLa]
TK=[KI]KLb
LCIab

도면4


STBb
DDb
Kb
LCMa
C1
C1=[KLb]Kb
T-1
KLb
LCIab
TK
TK=[KI]KLb
KI
LCMa
R
R=[CK]KI
CK
[Ct]CK
DDa
Ct