(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
G06F 17/00
G06F 9/00

(11) 공개번호 10-2004-0104516
(43) 공개일자 2004년12월10일

(21) 출원번호 10-2004-7014515
(22) 출원일자 2004년09월15일
번역문 제출일자 2004년09월15일
(86) 국제출원번호 PCT/IB2003/000682
(87) 국제공개번호 WO 2003/079166
(86) 국제출원출원일자 2003년02월19일
(87) 국제공개일자 2003년09월25일

(30) 우선권주장 02076070.8 2002년03월18일 EP(EP)

(71) 출원인 코닌클리케 필립스 일렉트로닉스 엔.브이.
네델란드왕국, 아인드호펜, 그로네보드스베그 1

(72) 발명자 튈스핌,티.
네덜란드 5656 아아 아인트호벤, 프로페써 홀스틀란 6

스타링안토니우스에이.엠.
네덜란드 5656 아아 아인트호벤, 프로페써 홀스틀란 6

(74) 대리인 이화익

심사청구 : 없음

(54) 콘텐트에 대한 접근 통제 방법 및 시스템

요약

본 발명은, 키 록커 키(KLK)에 의해 암호화된 키 록커(5)에 저장된 콘텐트 키들(F1, F2)에 의해 암호화된 콘텐트에 대한 접근을 통제하는 방법 및 접근통제 시스템에 관한 것이다. 상기 콘텐트를 사용하여 장치(3)를 갱신할 필요가 없이, PC 응용 프로그램 또는 PC 응용 프로그램을 실행하는 컴퓨터(2)를 갱신하여 접근통제 시스템의 보안성을 복구하기 위해, 적어도 2개의 접근 키들(K1, K2)과 1개의 문자열(x)을 암호화부(1)에 의해 정의하는 단계와, 상기 접근 키들(K1, K2)을 사용하여 상기 암호화부(1)에 의해 상기 문자열(x)을 암호화하여 적어도 2개의 암호값들(h, E)을 얻는 단계와, 상기 암호값들(h, E)을 상기 콘텐트에 접근하도록 구성된 컴퓨터(2) 상에 저장하여 상기 컴퓨터(2)가 상기 키 록커 키(KLK)를 계산할 수 있도록 하는 단계와, 상기 접근 키들(K1, K2)을 상기 콘텐트에 접근하도록 구성된 장치(3) 상에 저장하고 상기 컴퓨터(2)로부터 또는 상기 암호화부(1)로부터 상기 장치(3)로 상기 암호값들(E) 중에서 적어도 1개를 전송함으로써, 상기 장치(3)가 상기 키 록커 키(KLK)를 계산할 수 있도록 하는 단계를 포함하는 방법이 제안된다.

대표도

도 1

색인어

콘텐트, 접근통제, 키 록커 키, 접근 키, 암호화, 문자열

명세서

본 발명은, 키 록커 키(key-locker key: KLK)에 의해 암호화된 키 록커에 저장된 콘텐트 키들에 의해 암호화된 콘텐트에 대한 접근을 통제하는 방법에 관한 것이다. 또한, 본 발명은, 대응하는 접근통제 시스템, 암호화부, 컴퓨터 및 이와 같은 접근통제 시스템에 사용되는 장치에 관한 것이다. 더구나, 본 발명은 컴퓨터 프로그램에 관한 것이다.

인터넷이 디지털 음악을 배포하기 위한 가장 중요한 수단들 중에서 한가지가 되고 있다고 널리 생각되고 있다. 크게 감소된 배포 비용과 훨씬 더 많은 목록의 입수가능성과 같은 수많은 이점에도 불구하고, 여전히 해결해야 하는 다수의 문제점이 잔존하고 있다. 복제방지의 결여는, 주요한 레코드 회사들이 이 영역에 들어오기 것을 막는 주된 이슈이다. 보호를 받는 음악을 다운로드하는 특수한 (가입 기반의) 서비스를 개시하는 것이 시도되고 있다. MP3 파일들과 같은 암호화된 파일들을 다운로드하고, 이 파일들을 일반적인 PC 기반의 CD 또는 DVD 레코더를 사용하여 CD-R 디스크 등의 기록형 정보매체에 저장하는 위해 특수한 PC 응용 프로그램이 배포된다. 이 암호화된 파일들은 PC 상에서 뿐만 아니라, 일반적이거나 약간 변형된 장치들, 예를 들면 휴대용 MP3-CD 플레이어 상에서 재생될 수 있다. 암호화된 파일 들의 키들은, 이와 같은 목적을 위해 마련된 디스크 상의 영역인 소위 키 록커에 저장된다. 키 록커 그 자체는 키, 즉 전체 시스템과 관련된 비밀값과, 일반적으로는, 고유 디스크 식별자로부터 유도되는 소위 키 록커 키를 사용하여 암호화된다. 이때, 이와 같은 사용을 위해 변형된 모든 장치 상에서 디스크가 재생될 수 있도록 보장하기 위해, 전역적인 비밀값의 사용이 필요하다는 점에 주목하기 바란다.

전술한 PC 응용 프로그램이 암호화된 파일들을 재생할 수 있으므로, 이 응용 프로그램이 키 록커 키에 접근한다. 따라서, 전역적인 비밀값에도 접근한다. PC 소프트웨어가 비교적 쉽게 해킹된다는 것이 잘 알려져 있으므로, 보안 관점에서, 이것은 약점이 된다. 따라서, 단기간에 전역적인 비밀값이 노출될 것으로 예상된다. 보안성 침해를 복구하기 위해 PC 응용 프로그램을 갱신된 프로그램으로 교체하는 것은 비교적 용이하다. 그러나, 휴대용 MP3-CD 플레이어 등의 하드웨어 장치를 교체하는 것은 불가능하다.

결국, 본 발명의 목적은, 장치의 하드웨어를 변경할 필요가 없이 PC 응용 프로그램을 교체함으로써, 보안성 침해로부터 복구할 수 있도록 하는 방법을 제공함에 있다. 본 발명의 또 다른 목적은, 이와 같은 시스템에 사용되는 접근통제 시스템 및 방법과, 컴퓨터 프로그램을 제공함에 있다.

상기한 목적은, 청구항 1에 기재된 것과 같은 콘텐트에 대한 접근통제방법에 의해 달성되는데, 상기 방법은,

- 암호화부에 의해 적어도 2개의 접근 키와 1개의 문자열을 정의하는 단계와,

- 상기 접근 키들을 사용하여 상기 암호화부에 의해 상기 문자열을 암호화하여 적 어도 2개의 암호값들을 얻는 단계와,

- 상기 콘텐트를 접근하도록 구성된 컴퓨터 상에 상기 암호값들을 저장하여, 상기 컴퓨터가 상기 키 록커 키를 계산할 수 있도록 하는 단계와,

- 상기 콘텐트를 접근하도록 구성된 장치 상에 상기 접근 키들을 저장하고, 상기 컴퓨터 또는 상기 암호화부로부터 상기 장치로 상기 암호값들 중에서 적어도 1개를 전송하여, 상기 장치가 상기 키 록커 키를 계산할 수 있도록 하는 단계를 포함한다.

본 발명은, 장치가 컴퓨터와 다른 비밀값들을 사용해야 한다는 착상에 근거를 두고 있다. 컴퓨터를 해킹하는 것은 비교적 용이하기 때문에, 컴퓨터가 해킹될 때, 장치에 의해 사용된 키들을 분실하거나 노출되는 것을 방지해야 한다. 이것은, 본 발명에 따르면, 암호화부, 예를 들면, 장치들의 제조사, 서비스 제공자 또는 콘텐트 제공자 등의 신뢰된 제 3 자에 의해 정의된 문자열의 암호값들을 발생하고, 마찬가지로 상기 암호화부에 의해 정의된 접근 키들을 사용하며, 상기 암호값들만을 컴퓨터에 제공하고, 상기 접근 키들과 상기 문자열은 제공하지 않음으로써, 피할 수 있다. 이들 접근 키들은, 모든 기능들이 보통 장치의 하드웨어에 내장되므로 쉽게 해킹이 불가능한 장치에만 제공된다. 접근 키들, 문자열과, 암호값들을 생성하기 위한 암호화 함수들은, 문자열이 알려진 경우에는 키 록커 키를 계산하는 것이 용이하지만, 문자열이 알려지 있지 않은 경우에는, 암호값들을 알고 있더라도, 접근 키들을 계산하는 것이 곤란하거나 거의 불가능하도록 선택된다.

이에 따르면, 문자열이 트랩도어(trapdoor)의 역할을 한다. 컴퓨터가 망가지 기는 했지만 장치의 접근 키들을 여전히 알지 못하는 경우에는, 컴퓨터 상에서 실행되는 PC 응용 프로그램을 교체하거나, 이와 다르게 선택된 문자열을 사용하여 생성된 새로운 암호값들을 컴퓨터에 제공함으로써, 접근통제 시스템의 갱신이 가능하다. 이에 따르면, 새로운 키들을 사용하여 장치를 갱신할 필요는 없으며, 컴퓨터를 통해 실행될 수 있는 상기 암호값들 중에서 한 개를 장치에 제공하는 것만이 필요하다.

이때, 암호화라는 용어는, 개인 및 공개 키 쌍들 또는 (공모 방지(collusion-resistant) 일방향 해시함수의 사용과 같은 모든 형태의 암호화를 포함한다는 점에 주목하기 바란다.

본 발명의 바람직한 실시예들은 종속항들에 기재되어 있다. 바람직하게는, 청구항 1에 기재된 방법을 구현하기 위해, 암호화부, 컴퓨터와 장치를 구비한 접근통제 시스템은 청구항 9에 기재되어 있다. 또한, 본 발명은, 청구항 10 내지 12에 기재된 것과 같이 이와 같은 접근통제 시스템에 사용되는 암호화부, 컴퓨터 및 장치에 관한 것이다. 청구항 9에 기재된 것과 같은 접근통제 시스템의 1개 이상의 구성요소 상에서 컴퓨터 프로그램이 실행될 때, 컴퓨터가 청구항 1에 기재된 것과 같은 방법의 단계들을 수행하도록 하는 컴퓨터 프로그램 코드수단을 포함하는 본 발명에 따른 컴퓨터 프로그램은 청구항 13에 기재되어 있다.

바람직한 일 실시예에 따르면, 콘텐트 및 키 록커가 정보매체, 특히 CD 또는 DVD 등의 광 디스크 상에 저장되고, 키 록커 키는 상기한 정보매체의 고유 매체 식별자와 상기 암호값들 중에서 1개에서 유도된다. 바람직하게는, 키 록커 키를 계산 하기 위해 사용되는 암호값은 장치 상에 설치되거나 장치로 주어지지 않으며, 상기 암호값은 적어도 2개의 접근 키들과 기타 암호값들을 사용하여 장치에 의해 생성된다.

더구나, 전술한 실시예들에 근거하여, 상기 정보매체에 접근할 때, 매체 식별자가 상기 컴퓨터에 의해 정보매체로부터 판독되고, 이 매체 식별자에 접근할 때, 매체 식별자가 컴퓨터로부터 장치로 전송되거나 장치에 의해 정보매체로부터 판독되는 것이 바람직하다. 이에 따르면, 장치는 정보매체에 직접 접근, 예를 들면 인터넷으로부터 다운로드된 콘텐트가 저장된 디스크를 재생하거나, 컴퓨터만이 정보매체에 접근하고, 고유 매체 식별자를 판독하여, 매체 식별자와 필요한 암호값과 함께 콘텐트를 장치로 전송하여, 이 장치가 콘텐트에 접근하기 위한 콘텐트 키를 얻는데 필요한 키 록커 키를 재구성한 후에, 추후에 어느 때나 콘텐트를 재생하는 것이 가능하다.

본 발명의 또 다른 국면에서는, 콘텐트가 서로 다른 콘텐트 키들에 의해 각각 암호화되는 MP3 파일들 등의 데이터 파일들을 포함하고, 상기 콘텐트 키들은 상기 키 록커에 저장된다. 더구나, 상기 데이터 파일들은 암호값과 함께 컴퓨터로부터 장치로 전송된다. 이때, '콘텐트'는 오디오 파일을 의미할 뿐만 아니라, 모든 자치 상에서 재생되거나 사용될 수 있는 화상, 비디오 및 소프트웨어 데이터 등의 모든 다른 종류의 데이터를 포함할 수도 있다는 점에 주목하기 바란다. 마찬가지로, 용어 '장치'는 휴대용 MP3-CD 플레이어 등의 오디오 재생장치에 한정되지 않으며, 비디오 카메라, 카메라, 핸드헬드 컴퓨터 또는 휴대용 게임장치 등의 임의의 종류의 데이터를 재생하거나 사용하는 모든 다른 장치도 포함할 수도 있다.

바람직하게는, 키 록커 키는 접근 키들과 수신된 암호값들을 사용하여 장치에 의해 계산된다. 첫 번째 단계에서, 암호화부에 의해 정의된 문자열이 수신된 암호값과, 바람직하게는, 상기 접근 키들 중에서 1개를 사용하여 재구성된다. 두 번째 단계에서는, 제 2 접근 키를 사용하여 재구성된 문자열이 암호화되어, 키 록커 키를 계산하는데 필요한 다른 암호값을 얻는다. 따라서, 장치가 컴퓨터로 주어진 모든 암호값들을 수신하는 것이 불필요하며, 상기 암호값들 중에서 1개면 충분하다.

본 발명의 또 다른 실시예에 따르면, 암호화부는, 제 1 가변 문자열과 제 2 고정 문자열을 정의하며, 이 제 2 고정 문자열은 마찬가지로 장치 상에 저장된다. 그후, 적어도 2개의 암호값들 중에서 1개는 제 1 문자열만을 암호화하여 얻어지는 한편, 두 번째 암호값은 상기 제 1 및 제 2 문자열의 조합, 예를 들면 상기 2개의 문자열의 모듈로-2-가산의 결과값을 암호화하여 얻어진다. 암호값들을 컴퓨터의 해킹에 의해 잃어버리더라도, 접근 키들과 제 1 가변 문자열에 대한 정보를 거의 잃어버리지 않으므로, 이와 같은 구성은 전체 접근통제 시스템의 보안성을 더욱 더 향상시킨다. 따라서, 추가적인 제 2 문자열의 사용은, 그들 마음대로 더욱 더 많은 암호문을 갖는 해커들에 대해 접근통제 시스템을 더욱 더 안전하게 만든다. 접근통제 시스템의 보안성을 더욱 더 향상시키기 위해, 또 다른 실시예에 있어서는, 제 2 문자열이 제 1 가변 문자열 부분과 제 2 고정 문자열 부분을 포함한다. 본 실시예에서는, 제 1 문자열 부분이 암호화부로부터 직접 또는 컴퓨터를 통해 장치로 전송 되는 반면, 제 2 문자열 부분은 접근 키들과 함께 처음부터 장치 상에 저장된다. 따라서, 갱신시에, 암호화부는 새로운 제 1 문자열과 제 2 문자열의 새로운 제 1 문자열 부분만을 선택한다. 이와 같은 구성은 새로운 제 2 문자열과, 이에 따라 새로운 암호화 키들을 제공한다. 컴퓨터 또는 이 컴퓨터 상에서 실행되는 응용 프로그램이 갱신될 때마다, 제 2 문자열도 갱신될 수 잇다는 사실은, 평문에 더욱 더 많은 무작위성을 도입하므로, 암호값들로부터 더 적은 정보를 얻을 수 있다.

전술한 것과 같이, 컴퓨터 상에 저장된 암호값들이 부당하게 변조될 때에는, 이 암호값들을 갱신하는 것이 바람직하다. 이와 달리 또는 이에 덧붙여, 이들 암호값들은 접근통제 시스템의 보안성을 향상시키기 위해 정기적으로 갱신될 수도 있다.

이하, 다음의 첨부도면을 참조하여 본 발명을 더욱 더 상세히 설명한다:

도 1은 본 발명에 따른 접근통제 시스템의 제 1 실시예의 블록도이고,

도 2는 본 발명에 따른 접근통제 시스템의 제 2 실시예의 블록도이며,

도 3은 본 발명에 따른 접근통제 시스템의 제 3 실시예의 블록도이다.

도 1에 도시된 본 발명에 따른 접근통제 시스템은, 신뢰된 제 3자(trusted third party: TTP) 등의 암호화부(1)와, 퍼스널컴퓨터(PC) 등의 컴퓨터(2)와, 휴대용 CD 플레이어, MP3-CD 플레이어, 예를 들면 필립스 eXpanium의 변형된 버전, 또는 DVD 플레이어 등의 장치(3)와, 그 위의 특정한 영역에 또는 특정한 방식으로 키 록커(5)가 저장되는 CD 또는 DVD 등의 기록형 또는 재기록형 디스크, 반도체 플래시 카드 또는 착탈가능한 하드디스크 등의 정보매체(4)를 구비한다. 정보매체(4)는, 고유 식별자와, 만일 존재한다면, 컴퓨터(2)로 주어질 다른 데이터를 더 포함한다. 이와 같은 데이터의 전체 집합을 부호 A로 표시한다. 정보매체(4)는, 바람직하게는, 컴퓨터(2)에 의해 예를 들면 인터넷을 거쳐 서버로부터 다운로드된 오디오, 비디오 또는 소프트웨어 데이터 등의 모든 종류의 데이터를 그 위에 저장할 수 있도록 기록형 또는 재기록형의 형태를 갖는 것이 바람직하다.

암호화부(1)는 문자열 $x \in Z_2^m$ 과 2개의 접근 키들 $K_1, K_2 \in Z_2^k$ 를 무작위로 선택한다. 이때, 컴퓨터(1)와 이 컴퓨터 상에서 실행되는 PC 응용 프로그램은 다음과 같은 데이터, 즉 $l \leq m$일 때 비밀 암호값 $h_{K1}(x) \in Z_2^l$ 과, 바람직하게는 비밀 암호값 $E_{K2}(x) \in Z_2^m$ 을 가질 수 있다. 함수 h는 일방향 함수 또는 암호 함수 E일 수 있는데, 즉 이들은 서로 다른 것이 바람직하다. 암호값들 $h_{K1}(x)$와 $E_{K2}(x)$는 암호화부(1)에 의해 생성되고 컴퓨터(2)로 전송되어 컴퓨터에 저장된다.

이 대신에, 장치(3)는 암호값들 $h_{K1}(x)$ 및 $E_{K2}(x)$를 수신하지 않고, 암호값들 $h_{K1}(x)$, $E_{K2}(x)$를 생성하는데 사용된 키들 K_1 및 K_2 를 수신하는데, 즉 접근 키들 K_1, K_2 는 암호값들 $h_{K1}(x)$ 및 $E_{K2}(x)$를 생성하는 정의된 문자열 x를 암호화하는데 사용된 암호함수들 h_{K1} 및 E_{K2} 의 키들이다.

키 록커 키 KLK는 컴퓨터에 의해 $KLK=f(A, h_{K1}(x))$로서 계산된다. 함수 f는, 데이터 A, KLK 및 f 그 자체를 알고 있더라도, 암호값 $h_{K1}(x)$를 여전히 유도하기가 곤란하도록 선택된다. 따라서, f에 대해 일방향 또는 암호 함수를 선택하는 것을 추천한다.

인터넷에서 데이터를 다운로드한 후에, 이 데이터는 디스크(4)에 저장되거나, 및/또는 예를 들어 디스크(4)에 의해, 임의의 위치에서 사용하기 위해 장치(3)로 전송되는데, 예를 들어 음악을 포함하는 MP3 파일들이 휴대용 MP3 플레이어 상에 저장될 수 있다. 상기한 파일들에 접근하기 위해서는, 장치(3)가 먼저 키 록커에 접근하여, 이들 파일들을 복호화하기 위해 콘텐트 키들 F_1, F_2 등을 얻을 필요가 있다. 키 록커(5)에 접근하기 위해서는, 다음과 같이 장치에 의해 계산될 수 있는 키 록커 키 KLK가 필요하다: $KLK=f(A, h_{K1}(D_{K2}(E_{K2}(x))))$. 이때, D_{K2} 는 암호 함수 E_{K2} 에 대응하는 복호 함수이다. 암호값 $E_{K2}(x)$를 복호화하여, 문자열 x가 얻어지게 되며, 이 문자열에 대해 암호 함수 h_{K1} 이 적용된다. 함수 f는 컴퓨터(2)에 의해 적용된 함수 f와 동일하다. 필요한 데이터 집합 A는 디스크(4)에서 직접 수신되거나, 바람직하게는, 컴퓨터(2)를 통해 수신되며, 이 컴퓨터로부터 바람직하게는 변환 채널을 통해 암호값 $E_{K2}(x)$가 더 수신된다. 그러나, 암호값 $E_{K2}(x)$는 접근 키들 K_1, K_2 와 함께 암호화부(1)에서 직접 수신될 수도 있다.

따라서, 문자열 x는 트랩도어의 역할을 한다. x를 무작위로 선택하는 것이 용이하다. x를 알고 있으면, 키 록커 키 KLK를 계산하는 것이 용이하지만, x를 알지 못하는 경우에는, 암호값들 $h_{K1}(x)$와 $E_{K2}(x)$를 알고 있더라도, 키 K_1 을 계산하는 것이 실시불가능할 정도로 곤란하다. 컴퓨터(2) 또는 이 컴퓨터 상의 PC 응용 프로그램이 깨졌지만 비밀 키들 K_1, K_2 를 여전히 모르는 경우에는, 접근통제 시스템에 기반을 둔 PC 응용 프로그램을 이와 다르게 선택된 데이터 x로 교체하거나 컴퓨터(2)에 새로운 문자열 x를 제공함으로써 접근통제 시스템이 쉽게 갱신될 수 있는데, 즉 암호화부(1)는 새로운 문자열 x를 선택하고, 암호값들 $h_{K1}(x)$, $E_{K2}(x)$를 계산하여, 이들 값을 컴퓨터(2)로 제공한다. 따라서, 새로운 데이터를 암호화부(1)에서 장치(3)로 제공할 필요가 없으며, 장치(3)가 컴퓨터(2)로부터 새로운 암호값 $E_{K2}(x)$를 수신하면 된다.

암호값 $E_{K2}(x)$가 알려지더라도, 예를 들면 컴퓨터(2)로부터 장치(3)를 향해 전송하는 동안 이 암호값이 가로채어진 경우에도, 접근 키 K_2 에 대한 어떠한 정보도 누설되지 않는다는 것을 알 수 있다. 더구나, 컴퓨터(2)가 파괴되어 암호값들 $h_{K1}(x)$와 $E_{K2}(x)$가 알려지더라도, (정보이론 관점에서) 접근 키들 K_1, K_2 에 대한 절반만이 누설된다는 것을 알 수 있다.

도 2는 본 발명에 따른 접근통제 시스템의 개량된 실시예에 대한 블록도이다. 이 시스템은 도 1에 도시된 시스템과 동일한 구성요소들을 구비한다. 차이점 은, 암호화부(1)도 무작위로 고정 문자열 $c \in Z_2^m$ 을 선택한다는 사실이다. 따라서, 컴퓨터(2)는 다음과 같은 암호값 $h_{K1}(x)$와 $E_{K2}(x \oplus c)$를 포함한다. 그후, 장치는 이와 같은 고정 문자열을 1개의 추가적인 비밀값으로 얻는다. 마찬가지로, 컴퓨터(2)는 도 1을 참조하여 전술한 것과 같이 키 록커 키 KLK를 계산한다. 그러나, 장치(3)는 이와 다르게 다음과 같은 관계에 따라 키 록커 키 KLK를 계산한다: $KLK=f(A, h_{K1}(D_{K2}(E_{K2}(x \oplus c)) \oplus))$를 계산한다. 이와 같은 계산을 가능하게 하기 위해, 장치(3)에는 컴퓨터(2)로부터, 또는 이와 달

리, 암호화부(1)로부터, 암호값 $E_{K2}(x \oplus c)$가 제공되어야만 한다.

도 1에 도시된 것과 같은 시스템에 비해, 암호값들 $h_{K1}(x)$와 $E_{K2}(x \oplus c)$를 누설함으로써, 접근 키들 K_1, K_2와 문자열 c에 대한 정보가 덜 누출된다. 이와 같은 구성은, 그들 마음대로 더욱 더 많은 암호문을 갖는 해커들에 대해 접근통제 시스템을 더욱 더 안전하게 만든다.

본 발명에 따른 접근통제 시스템의 또 다른 실시예를 도 3에 나타내었다. 도 2에 도시된 시스템과 비교한 차이점은, 파라미터 c가 고정되지 않으며, PC 응용 프로그램 또는 컴퓨터(2)가 갱신될 때마다 이 파라미터가 변할 수 있다는 사실이다. 따라서, 함수 g는 다음과 같이 정의된다: $g:Z_2^m \times Z_2^m :(c_1,c_2) \rightarrow \equiv g(c_1,c_2)$.

이와 같은 함수 g는 특정한 응용 프로그램의 제약에 따라 선택된다. 파라미터 c, c_1 및 c_2는 반드시 동일한 비트 길이를 가질 필요는 없다. 그후, 2개의 파라미터들 중에서 1개, 특히 도 2에 도시된 것과 같은 실시예의 문자열 c를 대체하는 문자열 부분 c_2는 장치(3) 상에 저장되므로, 고정된다. 가변 문자열 부분 c_1을 변경함으로써, 전체 문자열 c가 변경된다. 갱신시에, 암호화부(1)는 새로운 문자열 부분 c_1을 선택하고, 문자열 $c=g(c_1,c_2)$를 계산한다. 그후, 컴퓨터(2) 상에, 데이터 $h_{K1}(x)$, c_1 및 $E_{K2}(x \oplus c)$가 저장된다. 컴퓨터(2)는 전술한 것과 같이 다시 키 록커 키 KLK를 계산하는 한편, 장치(3)는 다음 관계에 따라 키 록커 키 KLK를 계산할 수 있다: $KLK=f(A, h_{K1}(D_{K2}(E_{K2}(x \oplus c)) \oplus g(c_1,c_2))))$. 이 함수는 장치에게만 알려지므로, PC 응용 프로그램을 해킹하여 노출되는 것이 불가능하다. PC 응용 프로그램 또는 컴퓨터(2)가 갱신될 때마다, 암호화부(1)가 서로 다른 문자열들 x, c_1을 선택한다. 이것은 새로운 문자열 c, 이에 따라 새로운 암호값들 $h_{K1}(x)$ 및 $E_{K2}(x \oplus c)$를 제공하게 된다. PC 응용 프로그램 또는 컴퓨터(2)가 갱신될 때마다 문자열 c가 변경될 수도 있다는 사실은, 평문 x 및 $x \oplus c$에 더 큰 무작위성을 도입한다. 따라서, 암호문 $h_{K1}(x)$, $E_{K2}(x \oplus c)$에서 더 적은 정보가 얻어질 수 있다.

도 1에 도시된 것과 같은 접근통제 시스템에 따르면, 평문 x만이 무작위로 선택될 수 있다. (정보이론의 관점에서) 접근 키들 K_1, K_2에 대한 모든 정보가 노출되기 전에, 4k 비트의 암호문이 노출되어야 한다는 것을 알 수 있다. 키 길이가 암 호문 길이와 동일한 차수를 갖는 경우에, 이것은 컴퓨터(2)의 PC 응용 프로그램이 2번 파손된 후에 발생한다. 따라서, 유니시티 거리(unicity distance)를 증가시키기 위해서는, 암호값 h, E의 길이보다 큰 길이를 갖는 접근 키들 K_1, K_2를 사용하는 것이 더욱 더 유리하다. 이때, 이것은, 양호한 암호함수 E_K이 경우에서와 같이, 접근 키들 K_1, K_2를 발견하는 것이 여전히 연산적으로 가능하지 않을 수 있으므로, 접근통제 시스템이 실제적으로 파손된다는 것을 의미하는 것은 아니라는 점에 주목하기 바란다.

도 2에 도시된 것과 같은 실시예에 따르면, 문자열 x 및 c가 시작시에만 무작위로 선택될 수 있다. 이때, 3번의 갱신을 거친 후에, 키 길이가 암호값들의 길이와 유사하다면, 원칙적으로 접근 키들 K_1, K_2를 결정하기 위해 충분한 정보를 사용할 수 있다는 것을 알 수 있다. 마찬가지로, 전술한 것과 같은 이유로, 암호값들보다 길이가 긴 접근 키들을 사용하는 것이 더 유리하다. 그러나, 양호한 암호 함수들 h_{K1}, E_{K2}에 대해서는, 이것이 여전히 연산적으로 실현불가능하게 된다.

마지막으로, 도 3에 도시된 것과 같은 실시예에 따르면, 새로운 문자열 x와 문자열 부분 c_1이 갱신할 때마다 선택될 수 있다. 이때, 접근 키들 K_1, K_2와 문자열 부분 c_2에 대한 불확실성은 알려진 암호문들의 수와 무관하다는 것을 알 수 있다. 따라서, 이 시스템의 보안성 레벨이 전술한 것과 같은 시스템들의 보안성 레벨보다 훨씬 높아진다.

파라미터 c가 변경될 수 있는 것과 동일한 방법으로, 접근 키들 K_1 및 K_2가 변경될 수도 있다는 점에 주목하기 바란다. 이것을 가능하게 하기 위해 추가적인 함수들이 정의되어야만 한다.

(57) 청구의 범위

청구항 1.

키 록커 키에 의해 암호화된 키 록커에 저장된 콘텐트 키들에 의해 암호화된 콘텐트에 대한 접근을 통제하는 방법에 있어서,

암호화부에 의해 적어도 2개의 접근 키와 1개의 문자열을 정의하는 단계와,

상기 접근 키들을 사용하여 상기 암호화부에 의해 상기 문자열을 암호화하여 적어도 2개의 암호값들을 얻는 단계와,

상기 콘텐트를 접근하도록 구성된 컴퓨터 상에 상기 암호값들을 저장하여, 상기 컴퓨터가 상기 키 록커 키를 계산할 수 있도록 하는 단계와,

상기 콘텐트를 접근하도록 구성된 장치 상에 상기 접근 키들을 저장하고, 상기 컴퓨터 또는 상기 암호화부로부터 상기 장치로 상기 암호값들 중에서 적어도 1개를 전송하여, 상기 장치가 상기 키 록커 키를 계산할 수 있도록 하는 단계를 포함하는 것을 특징으로 하는 접근 통제방법.

청구항 2.
제 1항에 있어서,

상기 콘텐트 및 상기 키 록커는 정보매체, 특히 CD 또는 DVD 등의 광 디스크에 저장되고, 상기 키 록커 키는 상기 정보매체의 고유 매체 식별자와 상기 암호값들 중에서 한 개에서 유도되는 것을 특징으로 하는 접근 통제방법.

청구항 3.
제 2항에 있어서,

상기 매체 식별자는 상기 정보매체에 접근할 때 상기 컴퓨터에 의해 상기 정보매체로부터 판독되고, 상기 매체 식별자는, 상기 정보매체에 접근할 때, 상기 컴퓨터로부터 상기 장치로 전송되거나, 상기 정보매체로부터 상기 장치에 의해 판독되는 것을 특징으로 하는 접근 통제방법.

청구항 4.
제 1항에 있어서,

상기 콘텐트는 서로 다른 콘텐트 키에 의해 각각 암호화된 MP3 파일들 등의 데이터 파일들을 포함하고, 상기 콘텐트는 상기 키 록커에 저장되며, 상기 데이터 파일들은 상기 암호값과 함께 상기 컴퓨터로부터 상기 장치로 전송되는 것을 특징으로 하는 접근 통제방법.

청구항 5.
제 1항에 있어서,

상기 키 록커 키는, 상기 접근 키들과 상기 수신된 암호값을 이용하여, 먼저 상기 수신된 암호값을 복호화하여 상기 문자열을 재구성한 후, 상기 재구성된 문자열을 암호화하여 상기 다른 암호값을 얻음으로써, 상기 장치에 의해 계산되는 것을 특징으로 하는 접근 통제방법.

청구항 6.
제 1항에 있어서,

상기 암호화부는, 제 1 가변 문자열과, 마찬가지로 상기 장치 상에 저장되는 제 2 고정 문자열을 정의하고,

상기 적어도 2개의 암호값들 중에서 한 개는 상기 제 1 문자열만을 암호화하여 얻어지고, 상기 적어도 2개의 암호값들 중에서 한 개는 상기 제 1 및 제 2 문자열의 조합을 암호화하여 얻어지는 것을 특징으로 하는 접근 통제방법.

청구항 7.
제 6항에 있어서,

상기 제 2 문자열은 제 1 가변 문자열 부분과 제 2 고정 문자열 부분을 포함하고,

상기 제 1 문자열 부분은 상기 암호화부로부터 직접 또는 상기 컴퓨터를 통해 상기 장치로 전송되며,

상기 제 2 문자열 부분은 상기 장치 상에 저장되는 것을 특징으로 하는 접근 통제방법.

청구항 8.
제 1항에 있어서,

상기 문자열은, 정기적으로, 또는 상기 컴퓨터 상에 저장된 암호값들이 부정변조되 었을 때 갱신되는 것을 특징으로 하는 접근 통제방법.

청구항 9.
키 록커 키에 의해 암호화된 키 록커에 저장된 콘텐트 키들에 의해 암호화된 콘텐트에 대한 접근을 통제하는 접근통제 시스템에 있어서,

적어도 2개의 접근 키와 1개의 문자열을 정의하며, 상기 접근 키들을 사용하여 상기 문자열을 암호화함으로써 적어도 2개의 암호값을 얻는 암호화부와,

상기 콘텐트를 접근하도록 구성되고, 상기 암호값들을 저장하여, 상기 키 록커 키를 계산할 수 있는 컴퓨터와,

상기 콘텐트를 접근하도록 구성되고, 상기 접근 키들을 저장하며, 상기 컴퓨터 또는 상기 암호화부로부터 상기 암호값들 중에서 적어도 1개를 수신하여, 상기 키 록커 키를 계산할 수 있는 장치를 구비한 것을 특징으로 하는 접근통제 시스템.

청구항 10.
키 록커 키에 의해 암호화된 키 록커에 저장된 콘텐트 키들에 의해 암호화된 콘텐트에 대한 접근을 통제하는 접근통제 시스템에 사용되는 암호화부에 있어서,

상기 암호화부는, 적어도 2개의 접근 키들과 1개의 문자열을 정의하고, 상기 접근 키들을 사용하여 상기 문자열을 암호화함으로써, 적어도 2개의 암호값들을 얻도록 구성되고,

상기 암호값들은 상기 콘텐트에 접근하도록 구성된 컴퓨터 상에 저장되어, 상기 컴 퓨터가 상기 키 록커 키를 계산할 수 있도록 하며,

상기 접근 키들은 상기 콘텐트에 접근하도록 구성된 장치 상에 저장되고,

상기 암호값들 중에서 적어도 1개가 상기 컴퓨터로부터 또는 상기 암호화부로부터 상기 장치로 전송되어, 상기 장치가 상기 키 록커 키를 계산할 수 있도록 구성된 것을 특징으로 하는 암호화부.

청구항 11.
키 록커 키에 의해 암호화된 키 록커에 저장된 콘텐트 키들에 의해 암호화된 콘텐트에 대한 접근을 통제하는 접근통제 시스템에 사용되는 컴퓨터에 있어서,

적어도 2개의 접근 키들과 1개의 문자열이 정의되고, 상기 문자열이 암호화부에 의해 상기 접근 키들을 사용하여 암호화되어 적어도 2개의 암호값들을 얻으며,

상기 컴퓨터는, 상기 콘텐트에 접근하고, 상기 암호값들을 저장하여, 상기 컴퓨터가 상기 키 록커 키를 저장할 수 있도록 구성되고,

상기 접근 키들은 상기 콘텐트에 접근하도록 구성된 장치 상에 저장되며,

상기 암호값들 중에서 적어도 1개는 상기 컴퓨터로부터 또는 상기 암호화부로부터 상기 장치로 전송되어, 상기 장치가 상기 키 록커 키를 계산할 수 있도록 구성된 것을 특징으로 하는 컴퓨터.

청구항 12.
키 록커 키에 의해 암호화된 키 록커에 저장된 콘텐트 키들에 의해 암호화된 콘텐 트에 대한 접근을 통제하는 접근통제 시스템에 사용되는 장치에 있어서,

적어도 2개의 접근 키들과 1개의 문자열이 정의되고, 상기 문자열이 암호화부에 의해 상기 접근 키들을 사용하여 암호화되어 적어도 2개의 암호값들을 얻으며,

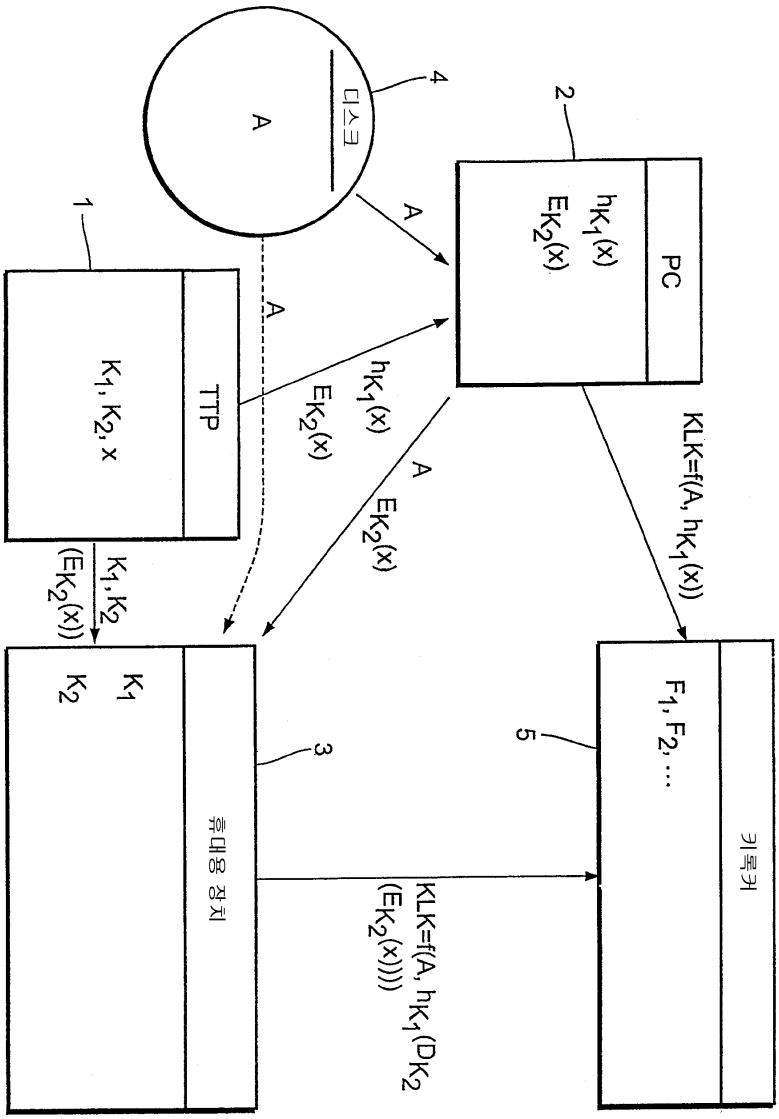
상기 암호값들은 상기 콘텐트에 접근하도록 구성된 컴퓨터 상에 저장되어, 상기 컴퓨터가 상기 키 록커 키를 계산할 수 있으며,

상기 장치는, 상기 콘텐트에 접근하고, 상기 접근 키들을 저장하고 상기 컴퓨터로부터 또는 상기 암호화부로부터 상기 암호값들 중에서 적어도 1개를 수신함으로써, 상기 키 록커 키를 계산할 수 있도록 구성된 것을 특징으로 하는 장치.

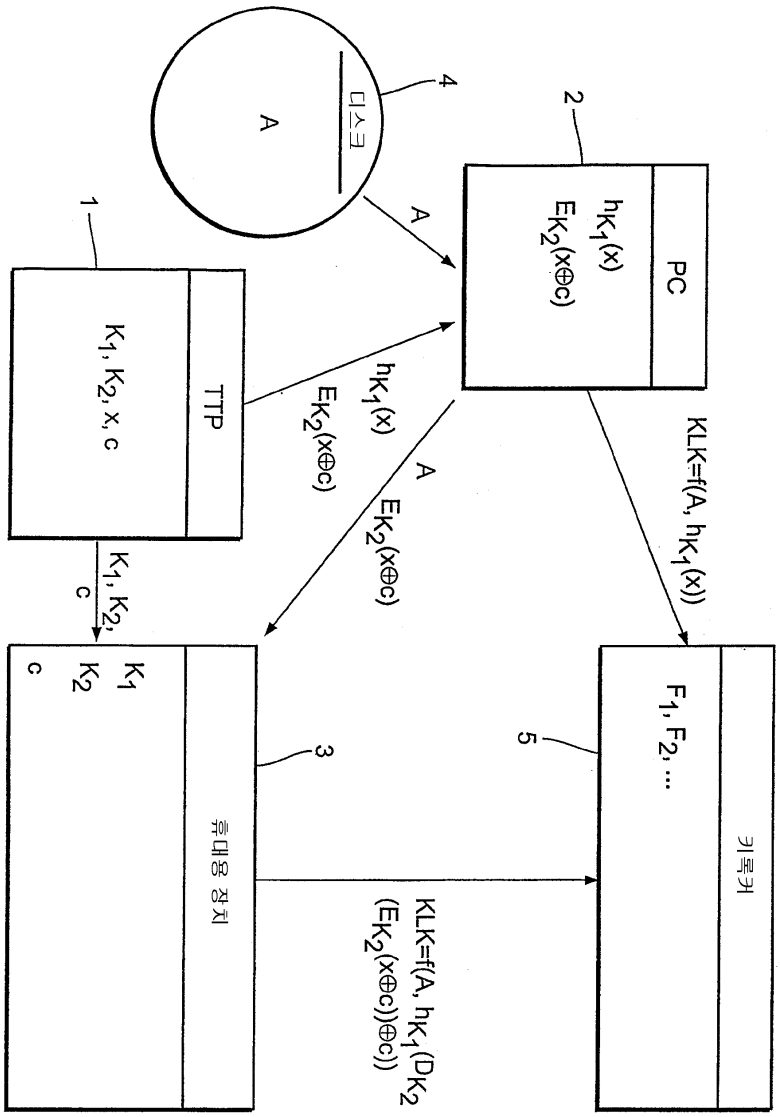
청구항 13.
컴퓨터 프로그램이 청구항 9에 기재된 접근통제 시스템의 1개 이상의 구성요소 상에서 실행될 때, 컴퓨터가 청구항 1에 기재된 방법의 단계들을 수행하도록 하는 컴퓨터 프로그램 코드수단을 포함하는 것을 특징으로 하는 컴퓨터 프로그램.

도면

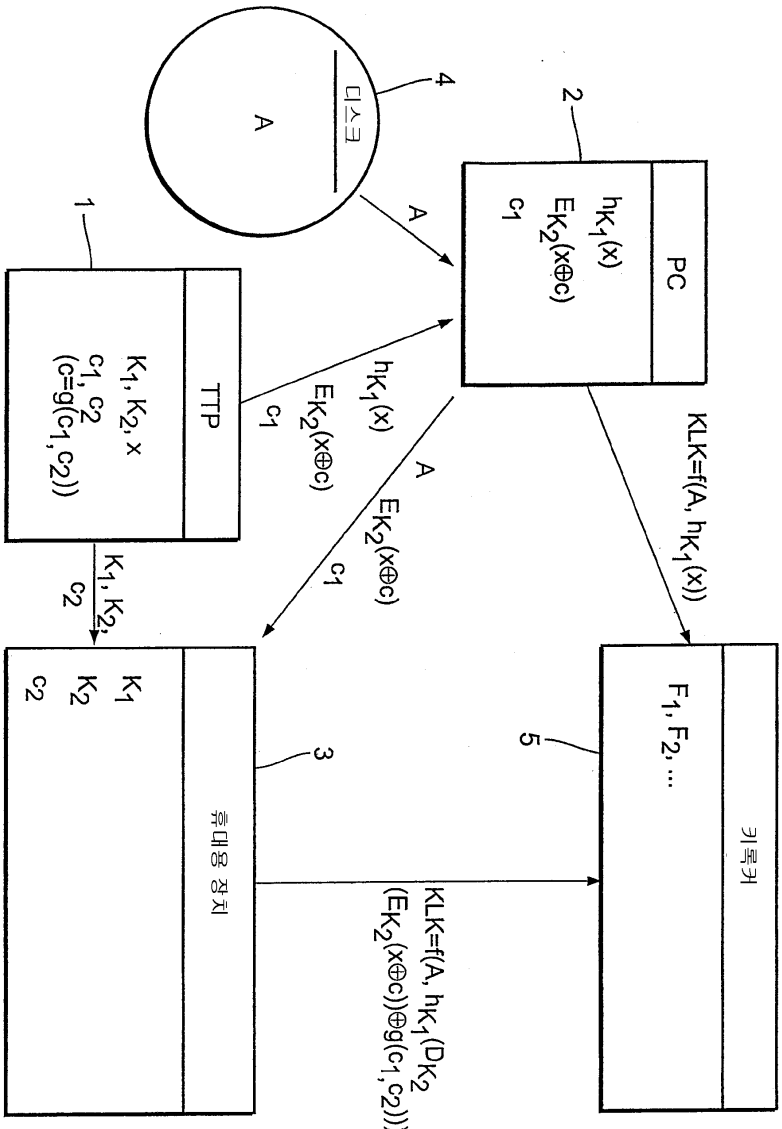
도면1


A
디스크
4
2
PC
$h_{K_1}(x)$
$E_{K_2}(x)$
A
1
K_1, K_2, x
TTP
A
$h_{K_1}(x)$
$E_{K_2}(x)$
A
$E_{K_2}(x)$
KLK=f(A, $h_{K_1}(x)$)
K_1, K_2
$(E_{K_2}(x))$
K_1
K_2
3
휴대용 장치
5
$F_1, F_2, \ldots$
키록커
KLK=f(A, $h_{K_1}(D_{K_2}$
$(E_{K_2}(x)))$

도면2


디스크
A
4
2
PC
$h_{K_1}(x)$
$E_{K_2}(x \oplus c)$
1
TTP
K_1, K_2, x, c
A
$h_{K_1}(x)$
$E_{K_2}(x \oplus c)$
A
$E_{K_2}(x \oplus c)$
KLK=f(A, $h_{K_1}(x)$)
K_1, K_2, c
K_1
K_2
c
3
휴대용 장치
5
$F_1, F_2, \ldots$
키록커
KLK=f(A, $h_{K_1}(D_{K_2}(E_{K_2}(x \oplus c)) \oplus c)$)

도면3


디스크
A
4
2
PC
$h_{K_1}(x)$
$E_{K_2}(x \oplus c)$
c_1
A
1
TTP
K_1, K_2, x
c_1, c_2
$(c=g(c_1, c_2))$
$h_{K_1}(x)$
$E_{K_2}(x \oplus c)$
c_1
A
$E_{K_2}(x \oplus c)$
c_1
KLK=f(A, $h_{K_1}(x)$)
$K_1, K_2,$
c_2
K_1
K_2
c_2
휴대용 장치
3
5
$F_1, F_2, \ldots$
키록커
KLK=f(A, $h_{K_1}(D_{K_2}$
$(E_{K_2}(x \oplus c)) \oplus g(c_1, c_2))$)