



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0066716
(43) 공개일자 2024년05월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/0819 (2013.01)
H04L 9/0861 (2013.01)
(21) 출원번호 10-2022-0147861
(22) 출원일자 2022년11월08일
심사청구일자 2022년11월08일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암
동5가)
(72) 발명자
이상진
서울시 종로구 사직로8길 20 파크팰리스 101동
1503호
강홍구
서울특별시 용산구 서빙고로51길 12 (대원서빙고
아파트) 112호
(뒷면에 계속)
(74) 대리인
특허법인위솔

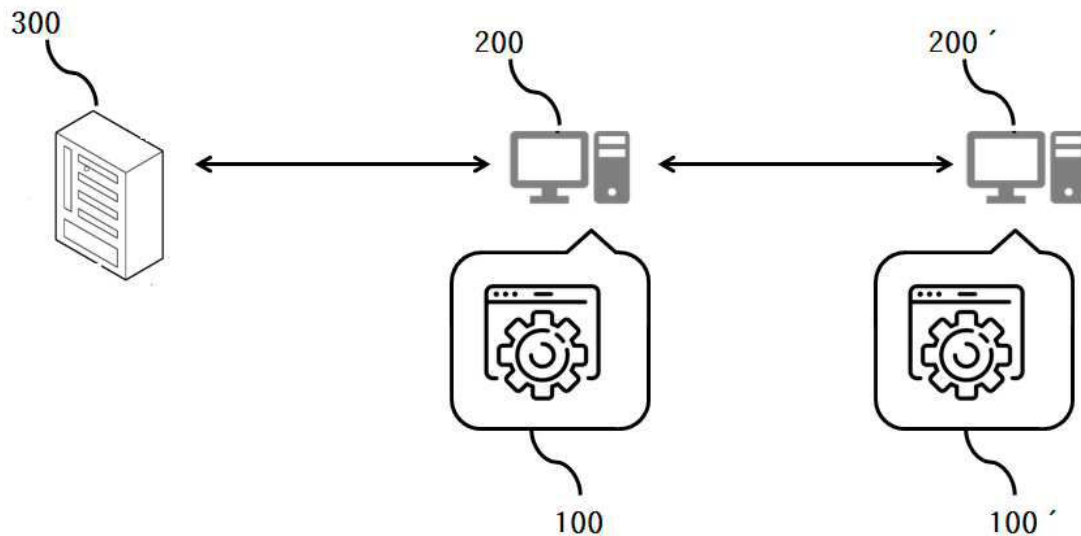
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 콘텐츠 복호화 키를 관리하는 방법 및 이를 위한 장치

(57) 요약

본 발명의 일 실시 예에 따른 프로세서 및 스토리지를 포함하는 장치가 콘텐츠 복호화 키를 관리하는 방법은 (a) 콘텐츠 제공 서버로부터 콘텐츠 키(Content Key)를 사용하여 콘텐츠를 암호화한 콘텐츠 SFX(Self eXtracting archive) 패키지를 수신하여 실행하는 단계, (b) 상기 암호화한 콘텐츠 SFX 패키지를 복호화하기 위해 상기 프
(뒷면에 계속)

대표도 - 도2



로세서 내에서 신뢰 실행 환경(Trusted Execution Environment, TEE)을 활성화하는 단계, (c) 상기 콘텐츠를 최초로 실행하는 것인지 판단하는 단계, (d) 상기 (c) 단계의 판단 결과, 상기 콘텐츠를 최초로 실행하는 것이라면, 상기 활성화한 신뢰 실행 환경 내에서 공개 키(Public Key) 및 인증 정보를 상기 콘텐츠 제공 서버에 발송하는 단계, (e) 상기 콘텐츠 제공 서버로부터 상기 인증 정보를 확인하여 상기 콘텐츠 키를 상기 공개 키로 암호화한 콘텐츠 키를 수신하는 단계, (f) 상기 활성화한 신뢰 실행 환경 내에서 상기 수신한 암호화한 콘텐츠 키를 상기 공개 키에 대한 개인 키(Private Key)로 복호화하여 복호화한 콘텐츠 키 및 라이선스를 획득하는 단계 및 (g) 상기 활성화한 신뢰 실행 환경 내에서 상기 획득한 콘텐츠 키를 사용하여 상기 암호화한 콘텐츠 SFX 패키지를 복호화하고, 상기 콘텐츠를 획득하는 단계를 포함한다.

(52) CPC특허분류

H04L 9/3263 (2013.01)

H04L 2209/603 (2013.01)

(72) 발명자

구정현

서울특별시 양천구 목동서로 100 (목동신시가지아
파트3단지) 313동 804호

박성하

서울특별시 용산구 한강대로46길 10 (한강로2가)
502호

명세서

청구범위

청구항 1

프로세서 및 스토리지를 포함하는 장치가 콘텐츠를 복호화 키를 관리하는 방법에 있어서,

- (a) 콘텐츠 제공 서버로부터 콘텐츠 키(Content Key)를 사용하여 콘텐츠를 암호화한 콘텐츠 SFX(Self eXtracting archive) 패키지를 수신하여 실행하는 단계;
- (b) 상기 암호화한 콘텐츠 SFX 패키지를 복호화하기 위해 상기 프로세서 내에서 신뢰 실행 환경(Trusted Execution Environment, TEE)을 활성화하는 단계;
- (c) 상기 콘텐츠를 최초로 실행하는 것인지 판단하는 단계;
- (d) 상기 (c) 단계의 판단 결과, 상기 콘텐츠를 최초로 실행하는 것이라면, 상기 활성화한 신뢰 실행 환경 내에서 공개 키(Public Key) 및 인증 정보를 상기 콘텐츠 제공 서버에 발송하는 단계;
- (e) 상기 콘텐츠 제공 서버로부터 상기 인증 정보를 확인하여 상기 콘텐츠 키를 상기 공개키로 암호화한 콘텐츠 키를 수신하는 단계;
- (f) 상기 활성화한 신뢰 실행 환경 내에서 상기 수신한 암호화한 콘텐츠 키를 상기 공개 키에 대한 개인 키(Private Key)로 복호화하여 복호화한 콘텐츠 키 및 라이선스를 획득하는 단계; 및
- (g) 상기 활성화한 신뢰 실행 환경 내에서 상기 획득한 콘텐츠 키를 사용하여 상기 암호화한 콘텐츠 SFX 패키지를 복호화하고, 상기 콘텐츠를 획득하는 단계;

를 포함하는 콘텐츠 복호화 키를 관리하는 방법

청구항 2

제1항에 있어서,

상기 (b) 단계에서 상기 프로세서 내에서 신뢰 실행 환경의 활성화는,

인클레이브(Enclave)를 신규 생성하는 것인,

콘텐츠 복호화 키를 관리하는 방법

청구항 3

제1항에 있어서,

상기 (c) 단계는,

상기 공개 키, 개인 키 및 암호화한 콘텐츠 키를 포함하는 키 세트(Set)가 상기 스토리지에 저장되어 있는지 판단하는 것인,

콘텐츠 복호화 키를 관리하는 방법

청구항 4

제1항에 있어서,

상기 (d) 단계는,

(d-1) 상기 활성화한 신뢰 실행 환경 내에서 임의의 공개 키 및 이에 대한 개인 키를 생성하는 단계;

(d-2) 상기 콘텐츠 제공 서버와 보안 채널을 생성하는 단계; 및

(d-3) 상기 생성한 보안 채널을 이용하여 상기 생성한 공개 키를 상기 콘텐츠 제공 서버에 발송하는 단계;

를 포함하는 콘텐츠 복호화 키를 관리하는 방법

청구항 5

제1항에 있어서,

상기 (d) 단계 및 (e) 단계에서의 인증 정보는,

상기 장치 사용자의 ID/PW를 포함하는 식별 정보, 상기 장치 사용자의 상기 콘텐츠에 대한 구매 내역에 관한 정보 및 SFX의 위변조 여부에 대한 정보 중 어느 하나 이상을 포함하는,

콘텐츠 복호화 키를 관리하는 방법

청구항 6

제1항에 있어서,

(h) 상기 공개 키, 개인 키 및 암호화한 콘텐츠 키를 포함하는 키 세트(Set)를 상기 스토리지에 저장하는 단계;

를 더 포함하며,

상기 (h) 단계에서의 개인 키는,

상기 활성화한 신뢰 실행 환경 내에서 루트 봉인 키(Root Seal Key), MRENCLAVE 및 보안 업체 번호(Security Vendor Number, SVN)를 이용해 유도한 봉인 키(Sealing Key)를 이용하여 봉인한 개인 키인,

콘텐츠 복호화 키를 관리하는 방법.

청구항 7

제6항에 있어서,

(i) 상기 장치 사용자 소유의 또 다른 프로세서 및 스토리지를 포함하는 장치' - 상기 장치'는 해당 프로세서 내에서 신뢰 실행 환경을 활성화함 - 와 보안 채널을 생성하는 단계;

(j) 상기 장치'로부터 공개 키를 수신하는 단계;

(k) 상기 스토리지에 저장한 봉인한 개인 키의 봉인을 해지하여 상기 암호화한 콘텐츠 키를 복호화하고, 복호화한 콘텐츠 키를 획득하는 단계;

(l) 상기 (k) 단계에서 복호화한 콘텐츠 키를 상기 (j) 단계에서 수신한 공개 키로 암호화하여 상기 장치'에 발송하는 단계;

를 더 포함하는 콘텐츠 복호화 키를 관리하는 방법.

청구항 8

제7항에 있어서,

상기 (i) 단계와 (j) 단계 사이에,

(i') 상기 장치'를 인증하는 단계;

를 더 포함하며,

상기 (i') 단계에서의 인증은,

상기 장치'로부터 SFX의 위변조 여부에 대한 정보를 수신하여 확인하는,

콘텐츠 복호화 키를 관리하는 방법.

청구항 9

하나 이상의 프로세서;

네트워크 인터페이스;

상기 프로세서에 의해 수행되는 컴퓨터 프로그램을 로드(Load)하는 메모리; 및

대용량 네트워크 데이터 및 상기 컴퓨터 프로그램을 저장하는 스토리지를 포함하되,

상기 컴퓨터 프로그램은 상기 하나 이상의 프로세서에 의해,

(A) 콘텐츠 제공 서버로부터 콘텐츠 키(Content Key)를 사용하여 콘텐츠를 암호화한 콘텐츠 SFX(Self eXtracting archive) 패키지를 수신하여 실행하는 오퍼레이션;

(B) 상기 암호화한 콘텐츠 SFX 패키지를 복호화하기 위해 상기 프로세서 내에서 신뢰 실행 환경(Trusted Execution Environment, TEE)을 활성화하는 오퍼레이션;

(C) 상기 콘텐츠를 최초로 실행하는 것인지 판단하는 오퍼레이션;

(D) 상기 (C) 오퍼레이션의 판단 결과, 상기 콘텐츠를 최초로 실행하는 것이라면, 상기 활성화한 신뢰 실행 환경 내에서 공개 키(Public Key) 및 인증 정보를 상기 콘텐츠 제공 서버에 발송하는 오퍼레이션;

(E) 상기 콘텐츠 제공 서버로부터 상기 인증 정보를 확인하여 상기 콘텐츠 키를 상기 공개키로 암호화한 콘텐츠 키를 수신하는 오퍼레이션;

(F) 상기 활성화한 신뢰 실행 환경 내에서 상기 수신한 암호화한 콘텐츠 키를 상기 공개 키에 대한 개인 키(Private Key)로 복호화하여 복호화한 콘텐츠 키 및 라이선스를 획득하는 오퍼레이션; 및

(G) 상기 활성화한 신뢰 실행 환경 내에서 상기 획득한 콘텐츠 키를 사용하여 상기 암호화한 콘텐츠 SFX 패키지를 복호화하고, 상기 콘텐츠를 획득하는 오퍼레이션;

을 실행하는 콘텐츠 복호화 키를 관리하는 장치.

청구항 10

컴퓨팅 장치와 결합하여,

(AA) 콘텐츠 제공 서버로부터 콘텐츠 키(Content Key)를 사용하여 콘텐츠를 암호화한 콘텐츠 SFX(Self eXtracting archive) 패키지를 수신하여 실행하는 단계;

(BB) 상기 암호화한 콘텐츠 SFX 패키지를 복호화하기 위해 상기 프로세서 내에서 신뢰 실행 환경(Trusted Execution Environment, TEE)을 활성화하는 단계;

(CC) 상기 콘텐츠를 최초로 실행하는 것인지 판단하는 단계;

(DD) 상기 (CC) 단계의 판단 결과, 상기 콘텐츠를 최초로 실행하는 것이라면, 상기 활성화한 신뢰 실행 환경 내에서 공개 키(Public Key) 및 인증 정보를 상기 콘텐츠 제공 서버에 발송하는 단계;

(EE) 상기 콘텐츠 제공 서버로부터 상기 인증 정보를 확인하여 상기 콘텐츠 키를 상기 공개키로 암호화한 콘텐츠 키를 수신하는 단계;

(FF) 상기 활성화한 신뢰 실행 환경 내에서 상기 수신한 암호화한 콘텐츠 키를 상기 공개 키에 대한 개인 키(Private Key)로 복호화하여 복호화한 콘텐츠 키 및 라이선스를 획득하는 단계; 및

(GG) 상기 활성화한 신뢰 실행 환경 내에서 상기 획득한 콘텐츠 키를 사용하여 상기 암호화한 콘텐츠 SFX 패키지를 복호화하고, 상기 콘텐츠를 획득하는 단계;

를 실행하는 컴퓨터로 판독 가능한 매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술 분야

본 발명은 콘텐츠 복호화 키를 관리하는 방법 및 이를 위한 장치에 관한 것이다. 보다 자세하게는 공격자로부터 콘텐츠를 안전하게 보호할 수 있음과 동시에 다양한 유스 케이스를 지원함으로써 사용자의 편의성까지 고려한 콘텐츠 복호화 키를 관리하는 방법 및 이를 위한 장치에 관한 것이다.

배경 기술

- [0002] 코로나 19로 인한 일상 생활의 비대면화와 다국적 OTT(Over The Top) 기업들의 출현은 디지털 콘텐츠의 폭발적인 소비 증가로 이어졌으며, 전 세계적으로 많은 사람들이 개인용 PC나 모바일 단말 등을 통해 디지털 콘텐츠를 소비하고 있다.
- [0003] 한편, 디지털 콘텐츠의 소비가 늘어남에 따라 불법 다운로드나 무단 재배포 등과 같은 불법적인 방법으로의 사용도 현저하게 증가하고 있으며, 콘텐츠 제공자들은 DRM(Digital Rights Management) 기술을 이용하여 자신 또는 자사의 정책에 맞게 사용자들의 콘텐츠 이용을 제한하고 있다.
- [0004] 여기서 DRM 기술이란 디지털 콘텐츠에 대한 지적 자산을 디지털 방식으로 제어하고 관리하는 기술을 의미하는바, 이상적인 DRM 기술이란 크게 보안성(Security)과 사용자 친화성(User friendly)이라는 성질을 만족시켜야 하며, 관련 기술 분야에서는 이를 위해 많은 연구가 활발하게 진행되고 있다.
- [0005] 보다 구체적으로 DRM 기술에서 보안성이란 콘텐츠와 복호화 키, 라이선스 및 DRM 자체에 대한 보호에 관한 것으로서, 예를 들어 안전한 콘텐츠 암호화와 키 관리를 통한 비인가 복제 방지, 콘텐츠와 키 및 라이선스의 안전한 배포, 라이선스에 기반한 조건부 접근, DRM 컨트롤러와 라이선스에 대한 위변조 방지, 콘텐츠 이용 및 인가에 대한 추적성 제공 등을 포함하며, 사용자 친화성은 사용자의 사용 실태를 반영하여 다양한 사용자 유스 케이스를 지원하는 콘텐츠 인가 편의성과 콘텐츠 이동의 편의성에 관한 것인바, 예를 들어 사용자가 오프라인 상태에서 콘텐츠를 이용하거나 동일 사용자 소유의 여러 단말에서 콘텐츠를 이용하려는 경우, 이를 가능하게 하는 방안 등을 들 수 있다.
- [0006] 그럼에도 불구하고 종래의 DRM 기술의 주요 특성은 때로는 상충하기도 하며, 단일 기술로 모든 특성을 충족시킬 수도 없다는 문제점이 있는바, 보안성과 사용자 친화성 모든 성질을 만족시킬 수 있는 새롭고 진보한 기술이 요구된다. 본 발명은 이에 관한 것이다.

선행기술문헌

특허문헌

- [0007] (특허문헌 0001) 대한민국 공개특허공보 제 10-2019-0085602호(2019.07.19)

발명의 내용

해결하려는 과제

- [0008] 본 발명이 해결하고자 하는 기술적 과제는 사용자 및 제3 자를 포함하여 콘텐츠 제공자를 제외한 모두가 복호화된 콘텐츠 키를 확인할 수 없게 함으로써 콘텐츠를 안전하게 보호할 수 있는 콘텐츠 복호화 키를 관리하는 방법 및 이를 위한 장치를 제공하는 것이다.
- [0009] 본 발명이 해결하고자 하는 또 다른 기술적 과제는 종래 콘텐츠를 안전하게 보호하는데 치중한 DRM 기술이 지원하지 못했던 사용자 친화성을 향상시킬 수 있는 콘텐츠 복호화 키를 관리하는 방법 및 이를 위한 장치를 제공하는 것이다.
- [0010] 본 발명의 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

- [0011] 상기 기술적 과제를 달성하기 위한 본 발명의 일 실시 예에 따른 프로세서 및 스토리지를 포함하는 장치가 콘텐츠 복호화 키를 관리하는 방법은 (a) 콘텐츠 제공 서버로부터 콘텐츠 키(Content Key)를 사용하여 콘텐츠를 암호화한 콘텐츠 SFX(Self eXtracting archive) 패키지를 수신하여 실행하는 단계, (b) 상기 암호화한 콘텐츠 SFX 패키지를 복호화하기 위해 상기 프로세서 내에서 신뢰 실행 환경(Trusted Execution Environment, TEE)을 활성화하는 단계, (c) 상기 콘텐츠를 최초로 실행하는 것인지 판단하는 단계, (d) 상기 (c) 단계의 판단 결과, 상기 콘텐츠를 최초로 실행하는 것이라면, 상기 활성화한 신뢰 실행 환경 내에서 공개 키(Public Key) 및 인증 정보를 상기 콘텐츠 제공 서버에 발송하는 단계, (e) 상기 콘텐츠 제공 서버로부터 상기 인증 정보를 확인하여 상기 콘텐츠 키를 상기 공개키로 암호화한 콘텐츠 키를 수신하는 단계, (f) 상기 활성화한 신뢰 실행 환경 내에서 상기 수신한 암호화한 콘텐츠 키를 상기 공개 키에 대한 개인 키(Private Key)로 복호화하여 복호화한 콘텐츠

츠 키 및 라이선스를 획득하는 단계 및 (g) 상기 활성화한 신뢰 실행 환경 내에서 상기 획득한 콘텐츠 키를 사용하여 상기 암호화된 콘텐츠 SFX 패키지를 복호화하고, 상기 콘텐츠를 획득하는 단계를 포함한다.

- [0012] 일 실시 예에 따르면, 상기 (b) 단계에서 상기 프로세서 내에서 신뢰 실행 환경의 활성화는, 인클레이브(Enclave)를 신규 생성하는 것일 수 있다.
- [0013] 일 실시 예에 따르면, 상기 (c) 단계는, 상기 공개 키, 개인 키 및 암호화된 콘텐츠 키를 포함하는 키 세트(Set)가 상기 스토리지에 저장되어 있는지 판단하는 것일 수 있다.
- [0014] 일 실시 예에 따르면, 상기 (d) 단계는, (d-1) 상기 활성화한 신뢰 실행 환경 내에서 임의의 공개 키 및 이에 대한 개인 키를 생성하는 단계, (d-2) 상기 콘텐츠 제공 서버와 보안 채널을 생성하는 단계 및 (d-3) 상기 생성한 보안 채널을 이용하여 상기 생성한 공개 키를 상기 콘텐츠 제공 서버에 발송하는 단계를 포함할 수 있다.
- [0015] 일 실시 예에 따르면, 상기 (d) 단계 및 (e) 단계에서의 인증 정보는, 상기 장치 사용자의 ID/PW를 포함하는 식별 정보, 상기 장치 사용자의 상기 콘텐츠에 대한 구매 내역에 관한 정보 및 SFX의 위변조 여부에 대한 정보 중 어느 하나 이상을 포함할 수 있다.
- [0016] 일 실시 예에 따르면, (h) 상기 공개 키, 개인 키 및 암호화된 콘텐츠 키를 포함하는 키 세트(Set)를 상기 스토리지에 저장하는 단계;를 더 포함하며, 상기 (h) 단계에서의 개인 키는, 상기 활성화한 신뢰 실행 환경 내에서 루트 봉인 키(Root Seal Key), MRENCLAVE 및 보안 업체 번호(Security Vendor Number, SVN)를 이용해 유도한 봉인 키(Sealing Key)를 이용하여 봉인한 개인 키일 수 있다.
- [0017] 일 실시 예에 따르면, (i) 상기 장치 사용자 소유의 또 다른 프로세서 및 스토리지를 포함하는 장치' - 상기 장치'는 해당 프로세서 내에서 신뢰 실행 환경을 활성화함 - 와 보안 채널을 생성하는 단계, (j) 상기 장치'로부터 공개 키를 수신하는 단계, (k) 상기 스토리지에 저장한 봉인한 개인 키의 봉인을 해지하여 상기 암호화된 콘텐츠 키를 복호화하고, 복호화된 콘텐츠 키를 획득하는 단계, (l) 상기 (k) 단계에서 복호화된 콘텐츠 키를 상기 (j) 단계에서 수신한 공개 키로 암호화하여 상기 장치'에 발송하는 단계를 더 포함할 수 있다.
- [0018] 일 실시 예에 따르면, 상기 (i) 단계와 (j) 단계 사이에, (i') 상기 장치'를 인증하는 단계를 더 포함하며, 상기 (i') 단계에서의 인증은, 상기 장치'로부터 SFX의 위변조 여부에 대한 정보를 수신하여 확인하는 것일 수 있다.
- [0019] 상기 기술적 과제를 달성하기 위한 본 발명의 또 다른 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치는 하나 이상의 프로세서, 네트워크 인터페이스, 상기 프로세서에 의해 수행되는 컴퓨터 프로그램을 로드(Load)하는 메모리 및 대용량 네트워크 데이터 및 상기 컴퓨터 프로그램을 저장하는 스토리지를 포함하되, 상기 컴퓨터 프로그램은 상기 하나 이상의 프로세서에 의해, (A) 콘텐츠 제공 서버로부터 콘텐츠 키(Content Key)를 사용하여 콘텐츠를 암호화한 콘텐츠 SFX(Self eXtracting archive) 패키지를 수신하여 실행하는 오퍼레이션, (B) 상기 암호화된 콘텐츠 SFX 패키지를 복호화하기 위해 상기 프로세서 내에서 신뢰 실행 환경(Trusted Execution Environment, TEE)을 활성화하는 오퍼레이션, (C) 상기 콘텐츠를 최초로 실행하는 것인지 판단하는 오퍼레이션, (D) 상기 (C) 오퍼레이션의 판단 결과, 상기 콘텐츠를 최초로 실행하는 것이라면, 상기 활성화한 신뢰 실행 환경 내에서 공개 키(Public Key) 및 인증 정보를 상기 콘텐츠 제공 서버에 발송하는 오퍼레이션, (E) 상기 콘텐츠 제공 서버로부터 상기 인증 정보를 확인하여 상기 콘텐츠 키를 상기 공개키로 암호화한 콘텐츠 키를 수신하는 오퍼레이션, (F) 상기 활성화한 신뢰 실행 환경 내에서 상기 수신한 암호화된 콘텐츠 키를 상기 공개 키에 대한 개인 키(Private Key)로 복호화하여 복호화된 콘텐츠 키 및 라이선스를 획득하는 오퍼레이션 및 (G) 상기 활성화한 신뢰 실행 환경 내에서 상기 획득한 콘텐츠 키를 사용하여 상기 암호화된 콘텐츠 SFX 패키지를 복호화하고, 상기 콘텐츠를 획득하는 오퍼레이션을 실행한다.
- [0020] 상기 기술적 과제를 달성하기 위한 본 발명의 또 다른 실시 예에 따른 매체에 저장된 컴퓨터 프로그램은 컴퓨팅 장치와 결합하여, (AA) 콘텐츠 제공 서버로부터 콘텐츠 키(Content Key)를 사용하여 콘텐츠를 암호화한 콘텐츠 SFX(Self eXtracting archive) 패키지를 수신하여 실행하는 단계, (BB) 상기 암호화된 콘텐츠 SFX 패키지를 복호화하기 위해 상기 프로세서 내에서 신뢰 실행 환경(Trusted Execution Environment, TEE)을 활성화하는 단계, (CC) 상기 콘텐츠를 최초로 실행하는 것인지 판단하는 단계, (DD) 상기 (CC) 단계의 판단 결과, 상기 콘텐츠를 최초로 실행하는 것이라면, 상기 활성화한 신뢰 실행 환경 내에서 공개 키(Public Key) 및 인증 정보를 상기 콘텐츠 제공 서버에 발송하는 단계, (EE) 상기 콘텐츠 제공 서버로부터 상기 인증 정보를 확인하여 상기 콘텐츠 키를 상기 공개키로 암호화한 콘텐츠 키를 수신하는 단계, (FF) 상기 활성화한 신뢰 실행 환경 내에서 상기 수신한 암호화된 콘텐츠 키를 상기 공개 키에 대한 개인 키(Private Key)로 복호화하여 복호화된 콘텐츠 키

및 라이선스를 획득하는 단계 및 (GG) 상기 활성화한 신뢰 실행 환경 내에서 상기 획득한 콘텐츠 키를 사용하여 상기 암호화된 콘텐츠 SFX 패키지를 복호화하고, 상기 콘텐츠를 획득하는 단계를 실행한다.

발명의 효과

- [0021] 상기와 같은 본 발명에 따르면, 프로세서 내의 보안 영역인 신뢰 실행 환경 내에서 복호화가 이루어지므로 콘텐츠 제공자를 제외한 모두가 복호화된 콘텐츠 키를 확인할 수 없으므로 콘텐츠를 안전하게 보호할 수 있다는 효과가 있다.
- [0022] 또한, 이러한 보안성으로 인해 여러 공격들로부터 콘텐츠와 콘텐츠 복호화 키 그리고 라이선스를 안전하게 보호할 수 있다는 효과가 있다.
- [0023] 또한, 신뢰 실행 환경을 활용하기 때문에 외부 공격자는 물론이고 악의적인 사용자도 민감한 데이터를 확인할 수 없게 된다는 효과가 있다.
- [0024] 또한, 종래 DRM 기술이 지원하지 못했던 P2P 키의 전달과 오프라인 콘텐츠 실행 등과 같이 다양한 유스 케이스를 지원함으로써 사용자 친화성을 향상시킬 수 있다는 효과가 있다.
- [0025] 본 발명의 효과들은 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해 될 수 있을 것이다.

도면의 간단한 설명

- [0026] 도 1은 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치가 포함하는 전체 구성을 예시적으로 도시한 도면이다.
- 도 2는 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법이 수행되는 시스템 상의 전체 구성 모식도이다,
- 도 3은 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법의 대표적인 단계를 나타낸 순서도이다.
- 도 4는 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법에 있어서, 공개 키 및 인증 정보를 콘텐츠 제공 서버에 발송하는 S340 단계를 구체화한 순서도이다.
- 도 5는 본 발명의 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법의 대표적인 단계를 나타낸 순서도이다.
- 도 6은 본 발명의 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법의 성능에 대한 시뮬레이션 결과이다.
- 도 7은 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치를 개념도로 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0027] 본 발명의 목적과 기술적 구성 및 그에 따른 작용 효과에 관한 자세한 사항은 본 발명의 명세서에 첨부된 도면에 의거한 이하의 상세한 설명에 의해 보다 명확하게 이해될 것이다. 첨부된 도면을 참조하여 본 발명에 따른 실시 예를 상세하게 설명한다.
- [0028] 본 명세서에서 개시되는 실시 예들은 본 발명의 범위를 한정하는 것으로 해석되거나 이용되지 않아야 할 것이다. 이 분야의 통상의 기술자에게 본 명세서의 실시 예를 포함한 설명은 다양한 응용을 갖는다는 것이 당연하다. 따라서, 본 발명의 상세한 설명에 기재된 임의의 실시 예들은 본 발명을 보다 잘 설명하기 위한 예시적인 것이며 본 발명의 범위가 실시 예들로 한정되는 것을 의도하지 않는다.
- [0029] 도면에 표시되고 아래에 설명되는 기능 블록들은 가능한 구현의 예들일 뿐이다. 다른 구현들에서는 상세한 설명의 사상 및 범위를 벗어나지 않는 범위에서 다른 기능 블록들이 사용될 수 있다. 또한, 본 발명의 하나 이상의 기능 블록이 개별 블록들로 표시되지만, 본 발명의 기능 블록들 중 하나 이상은 동일 기능을 실행하는 다양한 하드웨어 및 소프트웨어 구성들의 조합일 수 있다.
- [0030] 또한, 어떤 구성요소들을 포함한다는 표현은 “개방형”의 표현으로서 해당 구성요소들이 존재하는 것을 단순히 지칭할 뿐이며, 추가적인 구성요소들을 배제하는 것으로 이해되어서는 안 된다.

- [0031] 나아가 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급될 때에는, 그 다른 구성요소에 직접적으로 연결 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 한다.
- [0032] 이하에서는 도면들을 참조하여 본 발명의 세부적인 실시 예들에 대해 살펴보도록 한다.
- [0033] 도 1은 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치(100)가 포함하는 전체 구성을 예시적으로 도시한 도면이다.
- [0034] 그러나 이는 본 발명의 목적을 달성하기 위한 바람직한 실시 예일 뿐이며, 필요에 따라 일부 구성이 추가되거나 삭제될 수 있고, 어느 한 구성이 수행하는 역할을 다른 구성이 함께 수행할 수도 있음은 물론이다.
- [0035] 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치(100)는 프로세서(10), 네트워크 인터페이스(20), 메모리(30), 스토리지(40) 및 이들을 연결하는 데이터 버스(50)를 포함할 수 있으며, 기타 본 발명의 목적을 달성함에 있어 요구되는 부가적인 구성들을 더 포함할 수 있음은 물론이라 할 것이다.
- [0036] 프로세서(10)는 각 구성의 전반적인 동작을 제어한다. 프로세서(10)는 CPU(Central Processing Unit), MPU(Micro Processor Unit), MCU(Micro Controller Unit) 또는 본 발명이 속하는 기술 분야에서 널리 알려져 있는 형태의 프로세서 중 어느 하나일 수 있다. 아울러, 프로세서(10)는 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법을 수행하기 위한 적어도 하나의 애플리케이션 또는 프로그램에 대한 연산을 수행할 수 있다.
- [0037] 네트워크 인터페이스(20)는 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치(100)의 유무선 인터넷 통신을 지원하며, 그 밖의 공지의 통신 방식을 지원할 수도 있다. 따라서 네트워크 인터페이스(20)는 그에 따른 통신 모듈을 포함하여 구성될 수 있다.
- [0038] 메모리(30)는 각종 정보, 명령 및/또는 정보를 저장하며, 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법을 수행하기 위해 스토리지(40)로부터 하나 이상의 컴퓨터 프로그램(41)을 로드할 수 있다. 도 1에서는 메모리(30)의 하나로 RAM을 도시하였으나 이와 더불어 다양한 저장 매체를 메모리(30)로 이용할 수 있음은 물론이다.
- [0039] 스토리지(40)는 하나 이상의 컴퓨터 프로그램(41) 및 대용량 네트워크 정보(42)를 비임시적으로 저장할 수 있다. 이러한 스토리지(40)는 ROM(Read Only Memory), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM), 플래시 메모리 등과 같은 비휘발성 메모리, 하드 디스크(HDD), 보조 저장 매체(SSD), 착탈형 디스크, 또는 본 발명이 속하는 기술 분야에서 널리 알려져 있는 임의의 형태의 컴퓨터로 읽을 수 있는 기록 매체 중 어느 하나일 수 있다.
- [0040] 컴퓨터 프로그램(41)은 메모리(30)에 로드되어, 하나 이상의 프로세서(10)에 의해, (A) 콘텐츠 제공 서버(300)로부터 콘텐츠 키(Content Key)를 사용하여 콘텐츠를 암호화한 콘텐츠 SFX(Self eXtracting archive) 패키지를 수신하여 실행하는 오퍼레이션, (B) 상기 암호화한 콘텐츠 SFX 패키지를 복호화하기 위해 상기 프로세서 내에서 신뢰 실행 환경(Trusted Execution Environment, TEE)을 활성화하는 오퍼레이션, (C) 상기 콘텐츠를 최초로 실행하는 것인지 판단하는 오퍼레이션, (D) 상기 (C) 오퍼레이션의 판단 결과, 상기 콘텐츠를 최초로 실행하는 것이라면, 상기 활성화한 신뢰 실행 환경 내에서 공개 키(Public Key) 및 인증 정보를 상기 콘텐츠 제공 서버에 발송하는 오퍼레이션, (E) 상기 콘텐츠 제공 서버로부터 상기 인증 정보를 확인하여 상기 콘텐츠 키를 상기 공개키로 암호화한 콘텐츠 키를 수신하는 오퍼레이션, (F) 상기 활성화한 신뢰 실행 환경 내에서 상기 수신한 암호화한 콘텐츠 키를 상기 공개 키에 대한 개인 키(Private Key)로 복호화하여 복호화한 콘텐츠 키 및 라이선스를 획득하는 오퍼레이션 및 (G) 상기 활성화한 신뢰 실행 환경 내에서 상기 획득한 콘텐츠 키를 사용하여 상기 암호화한 콘텐츠 SFX 패키지를 복호화하고, 상기 콘텐츠를 획득하는 오퍼레이션을 실행할 수 있다.
- [0041] 이상 간단하게 언급한 컴퓨터 프로그램(41)이 수행하는 오퍼레이션은 컴퓨터 프로그램(41)의 일 기능으로 볼 수 있으며, 보다 자세한 설명은 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법에 대한 설명에서 후술하도록 한다.
- [0042] 데이터 버스(50)는 이상 설명한 프로세서(10), 네트워크 인터페이스(20), 메모리(30) 및 스토리지(40) 사이의 명령 및/또는 정보의 이동 경로가 된다.
- [0043] 이상 설명한 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치(100)는 독립된 디바이스의 형태, 예를 들어 전자 기기나 서버(클라우드 포함)의 형태일 수 있으며, 후자의 경우 전용 애플리케이션의 형태로 사

용자 단말(200) 등에 설치되어 구동할 수 있을 것이다.

- [0044] 한편, 여기서 전자 기기는 스마트폰, 태블릿 PC, 노트북 PC, PDA, PMP 등과 같이 휴대가 용이한 포터블 기기 뿐만 아니라 한 장소에 고정 설치되어 사용하는 데스크톱 PC 등이라도 무방하며, 콘텐츠 제공 서버와 보안 채널을 생성해야 하기 때문에 네트워크 기능만 보유하고 있다면 전자 기기는 어떠한 것이라도 무방하다 할 것이다.
- [0045] 이하, 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치(100)가 독립된 디바이스인 전자 기기 형태 중, 서버의 형태임을 전제로 사용자 단말(200)에 설치된 전용 어플리케이션을 통해 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법에 대하여 도 2 내지 도 7을 참조하여 설명하도록 한다.
- [0046] 도 2는 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법이 수행되는 시스템 상의 전체 구성 모식도이며, 도 3은 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법의 대표적인 단계를 나타낸 순서도이다.
- [0047] 그러나 이는 본 발명의 목적을 달성함에 있어서 바람직한 실시 예일 뿐이며, 필요에 따라 일부 단계가 추가 또는 삭제될 수 있음은 물론이고, 어느 한 단계가 다른 단계에 포함되어 수행될 수도 있다.
- [0048] 한편, 각 단계는 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치(100)를 통해 이루어지는 것을 전제로 하며, 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치(100)가 서버의 형태임을 전제로 하였기 때문에 사용자 단말(200)에 설치된 전용 어플리케이션을 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치(100)와 동일한 의미로 볼 것이고, 설명의 편의를 위해 이들 모두를 "장치(100)"로 명명하도록 한다.
- [0049] 더 나아가, 장치(100)가 사용자 단말(200)에 설치된 어플리케이션과 동일한 의미이기 때문에 장치(100)의 사용자는 사용자 단말(200)의 사용자인 일반 사용자, 보다 구체적으로 콘텐츠를 이용할 정당한 라이선스를 보유한 자와 동일한 자로 해석하기로 하며, 콘텐츠의 경우 콘텐츠의 실질적인 내용을 구별함이 없이 최광의의 해석을 통해 모든 종류의 디지털 콘텐츠를 포함함을 미리 밝혀두는 바이다.
- [0050] 아울러, 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법은 도 2에 도시된 구성 모식도가 포함하는 콘텐츠 제공 서버(300)와 사용자 단말(200), 보다 구체적으로 사용자 단말(200)에 전용 어플리케이션 형태로 설치된 장치(100)와의 사이에서 수행되는 방법이라 할 것이다.
- [0051] 우선, 장치(100)가 콘텐츠 제공 서버(300)로부터 콘텐츠 키(Content Key)를 사용하여 콘텐츠를 암호화한 콘텐츠 SFX(Self eXtracting archive) 패키지를 수신하여 실행한다(S310).
- [0052] 여기서 콘텐츠 제공 서버(300)은 사용자 단말(200)에 콘텐츠를 제공하는 역할을 수행하는 구성으로서, 일반적인 OTT 기업의 서버나 웹하드 기업의 서버 등의 서버일 수 있으며, 이뿐만 아니라 다수의 콘텐츠를 저장하고 있는 서버라면 어느 것이나 콘텐츠 제공 서버(300)이 될 수 있다.
- [0053] 콘텐츠 제공 서버(300)는 콘텐츠 키를 사용하여 콘텐츠를 암호화한 콘텐츠 SFX 패키지를 보유하고 있으며, 콘텐츠 제공 서버(300)로부터 암호화한 콘텐츠 SFX 패키지를 수신하는 것은 장치(100)를 실행시킨 상태에서 사용자 단말(200)이 콘텐츠 제공 서버(300)에 접속하여 암호화한 콘텐츠 SFX 패키지를 다운로드 받는 것으로 볼 수 있다 할 것이다.
- [0054] 한편, 장치(100)는 암호화한 콘텐츠 SFX 패키지를 수신하여 바로 실행하는바, 암호화한 콘텐츠 SFX 패키지는 압축 파일 형태기 때문에 여기서의 실행은 압축을 해지하기 위한 실행으로 볼 수 있다 할 것이다.
- [0055] 암호화한 콘텐츠 SFX 패키지를 수신하여 실행했다면, 장치(100)가 암호화한 콘텐츠 SFX 패키지를 복호화하기 위해 프로세서(10) 내에서 신뢰 실행 환경(Trusted Execution Environment, TEE)을 활성화한다(S320).
- [0056] 활성화하는 신뢰 실행 환경이란 프로세서(10)라 불리우는 전자 기기의 CPU 내부에 있는 별도로 독립된 안전한 보안 영역(Secure Area)을 의미하며, 실행되는 응용 프로그램의 무결성과 자산의 기밀성 등 보안 기능을 제공하는바, 일반 영역과 정보 교환이 통제되고 보안 소프트웨어가 안전하게 실행될 수 있는바, 신뢰 실행 환경을 프로세서(10)에서 구현한 대표적인 것으로서 Intel의 SGX와 ARM의 TrustZone을 들 수 있으나, 본 발명에서 프로세서(10)는 이에 한정하지는 않는다 할 것이다.
- [0057] 여기서 신뢰 실행 환경을 활성화시킨다는 것은 프로세서(10) 내에서 일반 영역과 구별되는 독립된 보안 영역을 활성화한다는 것으로써, 프로세서(10)가 Intel의 SGX인 경우 인클레이브(Enclave)를 신규로 생성하는 것일 수 있는바, 이를 통해 프라이빗 메모리 영역에서 애플리케이션 격리가 가능해질 수 있다.

- [0058] 한편, 신뢰 실행 환경을 활성화하는 S320 단계는 암호화한 콘텐츠 SFX 패키지를 수신하여 실행하는 S310 단계 이전에 수행될 수도 있는바, S310 단계 이전에 수행되었다면 암호화한 콘텐츠 SFX 패키지 자체를 활성화한 신뢰 실행 환경 하에서 수신하여 실행할 수 있을 것이며, S310 단계 이후에 수행된다면 암호화한 콘텐츠 SFX 패키지의 수신 및 실행이 신뢰 실행 환경 활성화의 트리거(Trigger)로 동작하게 된다 할 것이나, 그 순서의 선후는 어느 것이든 무방하다 할 것이다.
- [0059] 신뢰 실행 환경까지 활성화되었다면, 장치(100)가 콘텐츠를 최초로 실행하는 것인지 판단한다(S330).
- [0060] 여기서 콘텐츠를 최초로 실행하는 것인지 판단하는 것은 장치(100)가 설치된 사용자 단말(200) 상에서 해당 콘텐츠를 처음으로 이용 또는 재생하려고 하는 것인지 판단한다는 것인바, 보다 구체적으로 공개 키, 개인 키 및 암호화한 콘텐츠 키를 포함하는 키 세트(Set)가 스토리지(40)에 저장되어 있는지 판단하는 것이나, 이에 대해서는 뒤에서 보다 자세하게 설명하도록 한다.
- [0061] 한편, S330 단계에서의 판단 결과 스토리지(40)에 구체적으로 공개 키, 개인 키 및 암호화한 콘텐츠 키를 포함하는 키 세트가 저장되어 있다면 이전에 해당 콘텐츠를 실행한 적이 있다는 것이기에 S340 단계로 넘어가지 않고 스토리지(40)로부터 공개 키, 개인 키 및 암호화한 콘텐츠 키를 포함하는 키 세트를 로딩하면 되며(S335), 판단 결과 스토리지(40)에 구체적으로 공개 키, 개인 키 및 암호화한 콘텐츠 키를 포함하는 키 세트가 저장되어 있지 않는다면 이들을 생성하고 획득하기 위한 다음 프로세스를 진행해야 한다.
- [0062] S330 단계에서의 판단 결과 콘텐츠를 최초로 실행하는 것이라면, 장치(100)가 S320 단계에서 활성화한 신뢰 실행 환경 내에서 공개 키(Public Key) 및 인증 정보를 콘텐츠 제공 서버(300)에 발송한다(S340).
- [0063] 암호화한 콘텐츠 SFX 패키지가 콘텐츠 제공 서버(300)만 보유하고 있는 콘텐츠 키로 암호화되었기 때문에 이를 복호화하기 위해서는 콘텐츠 키가 필요하며, S340 단계는 장치(100)가 콘텐츠 제공 서버(300)로부터 콘텐츠를 키를 획득하기 위한 첫 번째 프로세스에 해당한다. 이하, 도 4를 참조하여 자세히 설명하도록 한다.
- [0064] 도 4는 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법에 있어서, 공개 키 및 인증 정보를 콘텐츠 제공 서버(300)에 발송하는 S340 단계를 구체화한 순서도이다.
- [0065] 그러나 이는 본 발명의 목적을 달성함에 있어서 바람직한 실시 예일 뿐이며, 필요에 따라 일부 단계가 추가 또는 삭제될 수 있음은 물론이고, 어느 한 단계가 다른 단계에 포함되어 수행될 수도 있다.
- [0066] 우선, 장치(100)가 활성화한 신뢰 실행 환경 내에서 임의의 공개 키 및 이에 대한 개인 키를 생성한다(S340-1).
- [0067] 여기서 공개 키 및 개인 키란 암호화할 때 사용하는 키와 복호화할 때 사용하는 키가 상이한 비대칭키 방식에서 사용하는 키로서, 공개 키는 사람들에게 공개된 키, 정보를 암호화할 수 있는 키이며, 비밀키는 사용자만 알고 있는 암호를 풀 수 있는 키를 의미하는바, 임의의 공개 키 및 이에 대한 개인 키 생성은 하나의 세트로 이루어질 수 있으며, 생성한 임의의 공개 키로 암호화된 정보는 함께 생성한 개인 키를 통해서만 복호화될 수 있다.
- [0068] 임의의 공개 키 및 이에 대한 개인 키 까지 생성했다면, 장치(100)는 콘텐츠 제공 서버(300)와 보안 채널을 생성하며(S340-2), 생성한 보안 채널을 이용하여 S340-1 단계에서 생성한 공개 키를 콘텐츠 제공 서버(300)에 발송한다(S340-3).
- [0069] S340-3 단계에서 공개 키가 S340-2 단계에서 생성한 보안 채널을 통해 콘텐츠 제공 서버(300)로 발송되므로 발송 과정에서 공개 키가 외부에 유출되는 상황이 발생할 여지가 없으며, 장치(100)로부터 공개 키를 수신한 콘텐츠 제공 서버(300)는 콘텐츠를 복호화할 수 있는 콘텐츠 키를 수신한 공개 키로 암호화한다.
- [0070] 여기서 콘텐츠 제공 서버(300)가 콘텐츠를 키를 공개 키로 암호화하기 위해서는 공개 키를 발송한 장치(100)가 설치된 사용자 단말(200)이 해당 콘텐츠를 실행할 수 있는 권한을 가진 자인지 확인하는 절차가 요구되는바, 그에 따라 S340 단계에서는 공개 키와 더불어 인증 정보를 콘텐츠 제공 서버(300)에 함께 발송하는 것이다.
- [0071] 장치(100)가 공개 키와 함께 콘텐츠 제공 서버(300)에 발송하는 인증 정보는 장치(100) 사용자의 ID/PW를 포함하는 식별 정보, 장치(100) 사용자의 콘텐츠에 대한 구매 내역에 관한 정보 및 SFX의 위변조 여부에 대한 정보 중 어느 하나 이상을 포함할 수 있으며, 이들 정보를 전부 포함하여 확인하도록 함이 가장 바람직하다 할 것이다.
- [0072] 여기서 장치(100) 사용자는 앞서 사용자 단말(200)의 사용자인 일반 사용자라고 했던바, 사용자의 ID/PW를 포함하는 식별 정보와 사용자의 콘텐츠에 대한 구매 내역에 관한 정보를 확인함으로써 해당 ID/PW를 보유한 사용자가 해당 콘텐츠를 실행할 정당한 권한을 보유하고 있는 자인지 판단할 수 있으며, SFX의 위변조 여부에 대한 정

보를 확인함으로써 장치(100)가 설치된 사용자 단말(200)이 콘텐츠 키를 안전하게 수신할 수 있는 상태인지 판단할 수 있을 것이다.

[0073] 다시 도 3에 대한 설명으로 돌아가도록 한다.

[0074] 공개 키 및 인증 정보를 콘텐츠 제공 서버(300)에 발송했다면, 장치(100)가 콘텐츠 제공 서버(300)로부터 인증 정보를 확인하여 콘텐츠 키를 공개키로 암호화한 콘텐츠 키를 수신하며(S350), 활성화한 신뢰 실행 환경 내에서 수신한 암호화한 콘텐츠 키를 공개 키에 대한 개인 키(Private Key)로 복호화하여 복호화한 콘텐츠 키 및 라이선스를 획득한다(S360).

[0075] 장치(100)가 콘텐츠 제공 서버(300)로부터 암호화한 콘텐츠 키를 수신하였기 때문에 이를 복호화해야만 콘텐츠 키를 획득할 수 있으므로 앞서 S340-1 단계에서 생성한 개인 키로 암호화한 콘텐츠 키를 복호화하는 것이며, 해당 개인 키로 복호화할 수 있는 것은 콘텐츠 키가 해당 개인 키에 대한 공개 키로 암호화되었기 때문이다.

[0076] 한편, 복호화는 신뢰 실행 환경, 보다 구체적으로 앞서 S320 단계에서 신규 생성한 인클레이브 내부에서 이루어질 수 있으므로 복호화 과정에서 콘텐츠 키와 라이선스가 외부로 유출될 가능성을 원천적으로 제거할 수 있을 것이다.

[0077] 복호화한 콘텐츠 키 및 라이선스까지 획득했다면, 장치(100)가 활성화한 신뢰 실행 환경 내에서 획득한 콘텐츠 키를 사용하여 암호화한 콘텐츠 SFX 패키지를 복호화하고, 콘텐츠를 획득하며(S370), 콘텐츠를 로컬 스트리밍 방식으로 실행할 수 있을 것이다.

[0078] 지금까지 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법에 대하여 설명하였다. 이와 같은 본 발명은 암호화한 콘텐츠 SFX 패키지의 수신부터 이를 복호화하여 콘텐츠를 획득하는 일련의 프로세스에 관한 것인바, 콘텐츠 제공 서버(300)로부터 암호화한 콘텐츠 키를 처음으로 수신했다면, 개인 키를 이용하여 이를 곧바로 복호화할 수 있으나, 사용자가 반복적으로 콘텐츠를 실행할 수 있도록 지원하기 위해서는 콘텐츠 키의 지속적인 저장 기능이 필요하다 할 것이다.

[0079] 그러나 일반적인 TPM(Trusted Platform Module)과 달리 신뢰 실행 환경에서는 물리적인 비휘발성 저장 공간을 보유하고 있지 않기에 외부 저장 공간에 개인 키와 암호화된 콘텐츠 키를 저장해볼 수 있을 것이나, 이 경우 악성 사용자가 콘텐츠 키를 확인할 수 있게 되므로 본 발명에서는 신뢰 실행 환경, 보다 구체적으로 인클레이브의 봉인(Sealing) 기능을 활용해보고자 하며, 이것이 앞서 S330 단계에서 설명을 보유한 스토리지(40)에 저장된 키 세트에 관한 것이다.

[0080] 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법은 공개 키, 개인 키 및 암호화한 콘텐츠 키를 포함하는 키 세트(Set)를 스토리지(40)에 저장하는 단계(S380)를 더 포함할 수 있으며, S380 단계를 설명의 편의를 위해 S370 단계 이후에 설명하기는 하나, 이는 필수적인 것은 아니며, 공개 키 및 이에 대한 개인 키를 생성(S340)한 즉시 이를 스토리지(40)에 저장할 수 있으며, 암호화한 콘텐츠 키를 수신(S350)한 즉시 이를 스토리지(40)에 저장할 수도 있음은 물론이라 할 것이다.

[0081] 한편, 스토리지(40)에 저장한 개인 키는 암호화한 콘텐츠 키를 복호화할 수 있는 핵심적인 구성인바, 인클레이브의 봉인 기능을 통해 봉인할 필요성이 가장 높은 키이며, 그에 따라 신뢰 실행 환경 내에서 루트 봉인 키(Root Seal Key), MRENCLAVE 및 보안 업체 번호(Security Vendor Number, SVN)를 이용해 유도한 봉인 키(Sealing Key)를 이용하여 봉인하고, 이를 인클레이브의 외부 스토리지(40)에 공개 키 및 암호화한 콘텐츠 키와 함께 키 세트로 저장할 수 있으며, 이 봉인은 해당 키 세트가 다시 인클레이브 내부로 들어와야 해제할 수 있다 할 것이다.

[0082] 이와 별개로 앞서 콘텐츠 제공 서버(300)로부터 암호화한 콘텐츠 키를 처음으로 수신했다면, 개인 키를 이용하여 이를 곧바로 복호화할 수 있다고 했던바, 이번에는 동일한 사용자가 동일한 장치(100)가 설치된 사용자 단말(200)을 통해 동일한 콘텐츠를 실행하는 프로세스에 대하여 설명하도록 한다(이하, 이를 “재실행 프로세스”라 한다). 이는 신뢰 실행 환경이 물리적인 비휘발성 저장 공간을 보유하고 있지 않기에 스토리지(40)로부터 키 세트를 불러와 인클레이브 내부로 들어오는 프로세스에 해당하는 것이다. 이하 설명하도록 한다.

[0083] 재실행 프로세스 역시 앞서 설명한 S310 단계 및 S320 단계가 수행되며, S330 단계에서 콘텐츠를 최초로 실행하는 것인지 판단하여 판단 결과 최초로 실행하는 것이 아닌 것으로 판단하게 될 것인바, 스토리지(40)에 키 세트가 저장되어 있기 때문이다. 그에 따라 장치(100)는 신뢰 실행 환경, 보다 구체적으로 인클레이브 내에서 개인 키를 개봉해 암호화된 콘텐츠 키를 복호화할 수 있으며, 복호화한 콘텐츠 키를 이용해 콘텐츠를 복호화하여 실행

행할 수 있다.

- [0084] 즉, 사용자가 콘텐츠 제공 서버(300)에 최초 1회 인증을 수행하여 적합한 키 세트를 마련해 놓은 후에는 스토리지(40)에 안전하게 키 세트를 저장해두기 때문에 더 이상의 네트워크 상의 인증이 없이도 지속적으로 콘텐츠를 실행할 수 있는 것이며, 그에 따라 장치(100)가 설치된 사용자 단말(200)이 오프라인 상태라 할지라도 콘텐츠를 실행할 수 있게 됨으로써 사용자 친화성을 향상시킬 수 있다.
- [0085] 한편, 오프라인 상태에서의 콘텐츠를 실행하는 정책에 대하여 설명하면, 앞서 S360 단계에서 획득한 라이선스를 이용할 수 있는바, 여기서 라이선스는 라이선스 명세 언어(License Description Language, LDL)로 작성되어 콘텐츠의 사용 가능 기간, 사용 가능 범위, 사용 인가 인원 명단 및 콘텐츠 이용 조건 등을 정의한 문서로 볼 수 있다.
- [0086] 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법은 이러한 라이선스의 기밀성을 유지하고 위변조를 방지하기 위해 콘텐츠 키 및 공개 키로 두 번 암호화할 수 있는바, 공개 키의 복호화가 가능한 개인 키가 신뢰 실행 환경 내에서만 공개되도록 봉인되어 있기 때문에 외부에 저장된 라이선스는 평문으로 노출되지 않을 수 있으며, 라이선스가 콘텐츠 키로도 암호화되기 때문에 설사 공격자가 공개 키를 안다 할지라도 위변조 위험을 원천적으로 차단할 수 있다.
- [0087] 그 외에도 콘텐츠의 추가 결제, 콘텐츠를 실행하는 정책의 변경, 사용자의 추가 기기 인증 등으로 인해 라이선스에서의 통제 항목이 변경되어야 하는 경우에는 콘텐츠를 제외한 라이선스만 새로 제작해 재배포할 수도 있는바, 콘텐츠를 통째로 재암호화할 필요 없이 라이선스 파일만 다시 작성하고 콘텐츠 키와 공개 키로 암호화하면 충분하기에 콘텐츠 제공 서버(300)의 서버 오버 헤드도 최소화될 수 있으며, 서버 오버 헤드를 더욱 감소시키기 위해 장치(100)가 라이선스를 변경하고 새로 저장할 수도 있다 할 것이다.
- [0088] 이번에는 본 발명의 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법에 대하여 설명하도록 한다.
- [0089] 도 5는 본 발명의 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법의 대표적인 단계를 나타낸 순서도이다.
- [0090] 그러나 이는 본 발명의 목적을 달성함에 있어서 바람직한 실시 예일 뿐이며, 필요에 따라 일부 단계가 추가 또는 삭제될 수 있음은 물론이고, 어느 한 단계가 다른 단계에 포함되어 수행될 수도 있다.
- [0091] 본 발명의 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법이 앞서 설명한 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법과 상이한 점은 도 2에 도시된 구성 모식도가 포함하는 사용자 단말(200)과 사용자 단말'(200') 사이에서 수행되는 방법이라는 것인바, 두 개의 사용자 단말 사이에서 이루어지므로 일종의 P2P 방식의 콘텐츠 복호화 키를 관리하는 방법으로 볼 수 있을 것이다.
- [0092] 보다 구체적으로, 본 발명의 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법은 사용자가 새로운 단말에서 기존 콘텐츠를 실행하기 위해 기존 단말에서 새로운 단말로 콘텐츠를 옮기는 방법에 관한 것인바, 이와 별개로 새로운 단말인 사용자 단말'(200')과 콘텐츠 제공 서버(300) 사이에서 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법이 수행될 수 있음 역시 물론이라 할 것이다. 다만, 오프라인 상태에서는 이 역시 불가능한바, 이러한 경우에 콘텐츠 키를 받을 수 있는 방법에 관한 것이다.
- [0093] 한편, 설명에 앞서 앞서 장치(100)가 사용자 단말(200)에 설치된 전용 어플리케이션과 동일한 의미라고 했던바, 이에 대응하여 이번 실시 예에서는 장치'(100')가 사용자 단말'(200')에 설치된 전용 어플리케이션과 동일한 의미임을 추가적으로 명시하도록 한다.
- [0094] 아울러, 설명의 편의를 위해 본 발명의 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법의 시작을 앞서 설명한 S380 단계 이후로 기재하였으나, 스토리지(40)에 공개 키, 개인 키 및 암호화한 콘텐츠 키를 포함하는 키 세트가 저장된 이후라면 언제라도 시작 단계로 설정할 수 있다 할 것이다.
- [0095] 우선, 장치(100)가 해당 장치(100) 사용자 소유의 또 다른 프로세서'(10') 및 스토리지'(40')를 포함하는 장치'(100')와 보안 채널을 생성한다(S610).
- [0096] 여기서 장치'(100')와 보안 채널을 생성하기 이전에 장치'(100')는 프로세서'(10') 내에서 신뢰 실행 환경을 활성화해야 하며, 장치(100)는 이미 신뢰 실행 환경이 활성화된 상태이어야 할 것이다.
- [0097] 한편, 신뢰 실행 환경에 대한 설명은 앞서 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법과 동일하므로 중복서술을 방지하기 위해 자세한 설명은 생략하도록 한다.

- [0098] 보안 채널을 생성했다면, 장치(100)가 장치'(100')를 인증하는바(S620), 여기서 인증은 앞서 설명한 인증 정보와 상이하게 장치'(100')로부터 SFX의 위변조에 여부에 대한 정보만을 수신하여 확인하면 충분하다 할 것이다.
- [0099] 이후, 장치(100)가 장치'(100')으로부터 공개 키를 수신하고(S630), 스토리지(40)에 저장한 봉인한 개인 키의 봉인을 해지하여 암호화한 콘텐츠 키를 복호화하고, 복호화한 콘텐츠 키를 획득하며(S640), S640 단계에서 복호화한 콘텐츠 키를 S630 단계에서 수신한 공개 키로 암호화하여 장치'(100')에 발송한다(S650).
- [0100] 이상의 설명은 본 발명의 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법을 장치(100)를 주체로 하여 설명한 것이며, S650 단계 이후에는 장치(100)가 아닌 장치'(100')가 또 다른 주체가 되어 복호화한 콘텐츠 키를 개인 키로 복호화하고, 콘텐츠를 획득하는 단계가 수행될 수 있다. 아울러, 장치'(100') 역시 자신의 스토리지'(40')에 공개 키, 개인 키 및 암호화한 콘텐츠 키를 포함하는 키 세트를 저장할 수 있다.
- [0101] 중복 서술을 방지하기 위해 자세히 설명하지는 않았지만, 본 발명의 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법은 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법에서 콘텐츠 제공 서버(300)의 역할을 장치(100)가 설치된 사용자 단말(200)이, 장치(100)가 설치된 사용자 단말(200)의 역할을 장치'(100')가 설치된 사용자 단말'(200')이 수행하는 것으로 대체되었다 할 수 있으며, 다만 차이점이라면 본 발명의 제2 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법에서 콘텐츠 제공 서버(300)는 신뢰할 수 있는 공간이기 때문에 별도의 신뢰 실행 환경을 활성화할 필요가 없었으나, 본 발명의 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법은 두 개의 사용자 단말 사이에서 이루어지는 것이므로 두 단말 모두에서 신뢰 실행 환경을 활성화해야 한다는 점과 장치(100)가 키를 송신할 권한이 있는지를 라이선스를 기반으로 확인하는 프로세스가 추가된 점을 들 수 있을 것이며, 나머지 사항은 동일한 설명이 적용된다 할 것이다.
- [0102] 도 6은 본 발명의 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법의 성능, 보다 구체적으로 서로 다른 크기와 값의 암호 키를 P2P 방식으로 전달하는데 소요된 시간을 나타낸 시뮬레이션 결과인바, 키를 전달하는데 소요된 시간은 키의 크기나 값에 따라 차이가 발생하지 않으므로 본 발명의 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법이 매우 실용이라는 것을 확인할 수 있을 것이다.
- [0103] 한편, 콘텐츠 제공자의 보안 정책에 따라 장치(100)가 설치된 사용자 단말(200)과 장치'(100')가 설치된 사용자 단말'(200') 사이에서 라이선스의 차이를 둘 수 있음은 물론이며, 콘텐츠 배포 기능의 오남용을 방지하기 위해 다른 단말로 키를 전달하는 기능을 제한할 수도 있고, 전달 가능한 기한을 설정할 수도 있음은 물론이라 할 것이다. 이 경우 장치'(100')가 콘텐츠 제공 서버(300)에 접속하여 인증을 수행하고 추적 가능한 상태가 된다면, 장치(100)와 동일한 라이선스를 새로 발급하는 등 콘텐츠 제공자의 다양한 보안 정책을 지원할 수 있을 것이다.
- [0104] 지금까지 본 발명의 제2 실시 예 및 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법에 대하여 설명하였다. 본 발명에 따르면, 프로세서(10) 내의 보안 영역인 신뢰 실행 환경 내에서 복호화가 이루어지므로 콘텐츠 제공자를 제외한 모두가 복호화된 콘텐츠 키를 확인할 수 없으므로 콘텐츠를 안전하게 보호할 수 있다. 또한, 이러한 보안성으로 인해 여러 공격들로부터 콘텐츠와 콘텐츠 복호화 키 그리고 라이선스를 안전하게 보호할 수 있다. 아울러, 신뢰 실행 환경을 활용하기 때문에 외부 공격자는 물론이고 악의적인 사용자도 민감한 데이터를 확인할 수 없게 된다. 더 나아가, 종래 DRM 기술이 지원하지 못했던 P2P 키의 전달과 오프라인 콘텐츠 실행 등과 같이 다양한 유스 케이스를 지원함으로써 사용자 친화성을 향상시킬 수 있다.
- [0105] 한편, 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치(100)는 도 7에 도시된 바와 같은 개념도로 나타낼 수도 있는바, 장치(100)는 신뢰 실행 환경을 생성하고 암호 키를 봉인 및 개봉하며, 콘텐츠 복호화를 실시하는 복호화 모듈(110), 콘텐츠 제공 서버(300) 또는 다른 단말과 통신하며 콘텐츠 키 및 라이선스를 송수신하는 통신 모듈(120) 및 장치(100)의 동작 방식과 범위를 통제하는 라이선스(130)를 포함할 수 있으며, 핵심적인 구성인 복호화 모듈(110)은 신뢰 실행 환경의 생성 및 관리와 데이터의 봉인 및 개봉을 담당하는 신뢰 실행 환경 관리부(111), 라이선스를 검증하고 수정할 수 있는 라이선스 관리부(112) 및 암호화/복호화 기능부(113)를 포함할 수 있을 것이고, 본 발명의 제2 실시 예 및 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법에 대한 설명에서 장치(100)는 도 7에 도시된 개념도가 포함하는 각 구성이 해당하는 기능을 수행하는 프로세서로 이해할 수 있을 것이다.
- [0106] 한편, 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치(100)와 본 발명의 제2 실시 예 및 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법은 본 발명의 제4 실시 예에 따른 컴퓨터로 판독 가능한 매체

에 저장된 컴퓨터 프로그램으로 구현할 수도 있는바, 이 경우 컴퓨팅 장치와 결합하여, (AA) 콘텐츠 제공 서버로부터 콘텐츠 키(Content Key)를 사용하여 콘텐츠를 암호화한 콘텐츠 SFX(Self eXtracting archive) 패키지를 수신하여 실행하는 단계, (BB) 상기 암호화한 콘텐츠 SFX 패키지를 복호화하기 위해 상기 프로세서 내에서 신뢰 실행 환경(Trusted Execution Environment, TEE)을 활성화하는 단계, (CC) 상기 콘텐츠를 최초로 실행하는 것인지 판단하는 단계, (DD) 상기 (CC) 단계의 판단 결과, 상기 콘텐츠를 최초로 실행하는 것이라면, 상기 활성화한 신뢰 실행 환경 내에서 공개 키(Public Key) 및 인증 정보를 상기 콘텐츠 제공 서버에 발송하는 단계, (EE) 상기 콘텐츠 제공 서버로부터 상기 인증 정보를 확인하여 상기 콘텐츠 키를 상기 공개키로 암호화한 콘텐츠 키를 수신하는 단계, (FF) 상기 활성화한 신뢰 실행 환경 내에서 상기 수신한 암호화한 콘텐츠 키를 상기 공개 키에 대한 개인 키(Private Key)로 복호화하여 복호화한 콘텐츠 키 및 라이선스를 획득하는 단계 및 (GG) 상기 활성화한 신뢰 실행 환경 내에서 상기 획득한 콘텐츠 키를 사용하여 상기 암호화한 콘텐츠 SFX 패키지를 복호화하고, 상기 콘텐츠를 획득하는 단계를 실행할 수 있을 것이며, 중복 서술을 위해 자세히 기재하지는 않았지만 본 발명의 제1 실시 예에 따른 콘텐츠 복호화 키를 관리하는 장치(100) 및 본 발명의 제2 실시 예 및 제3 실시 예에 따른 콘텐츠 복호화 키를 관리하는 방법 에 적용된 모든 기술적 특징은 본 발명의 제4 실시 예에 따른 컴퓨터로 판독 가능한 매체에 저장된 컴퓨터 프로그램에 모두 동일하게 적용될 수 있음은 물론이라 할 것이다.

[0107]

이상 첨부된 도면을 참조하여 본 발명의 실시 예들을 설명하였지만, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시 예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다.

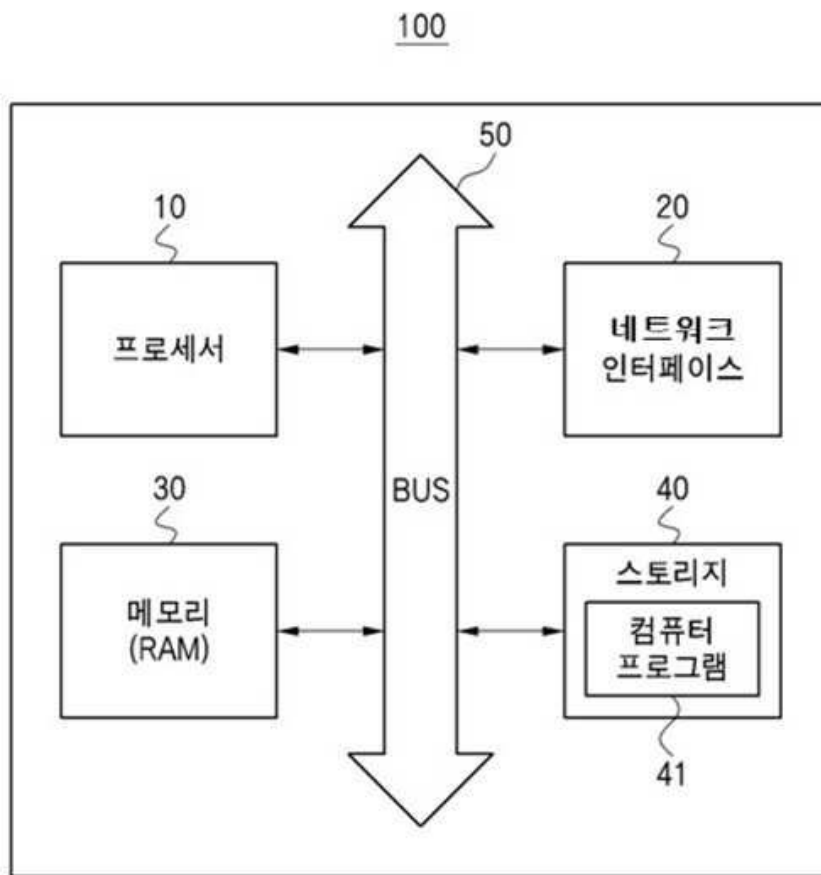
부호의 설명

[0108]

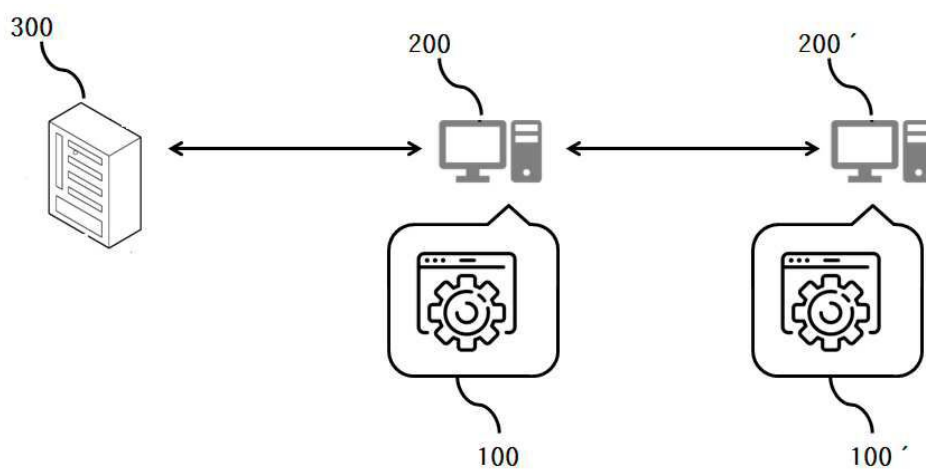
- 10: 프로세서
- 20: 네트워크 인터페이스
- 30: 메모리
- 40: 스토리지
- 41: 컴퓨터 프로그램
- 50: 정보 버스
- 100: 콘텐츠 복호화 키를 관리하는 장치
- 110: 복호화 모듈 120: 통신 모듈 130: 라이선스
- 111: 신뢰 실행 환경 관리부 112: 라이선스 관리부 113: 암호화/복호화 기능부
- 100': 콘텐츠 복호화 키를 관리하는 장치'
- 200: 사용자 단말
- 200': 사용자 단말'
- 300: 콘텐츠 제공 서버

도면

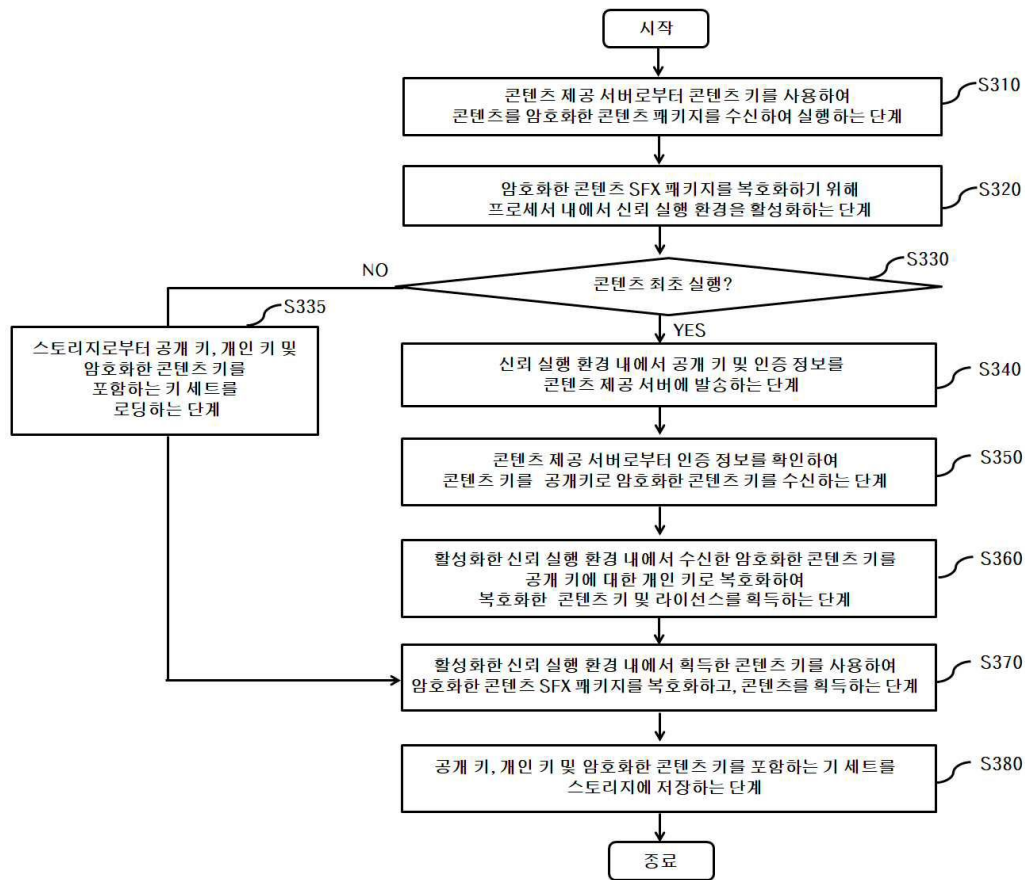
도면1



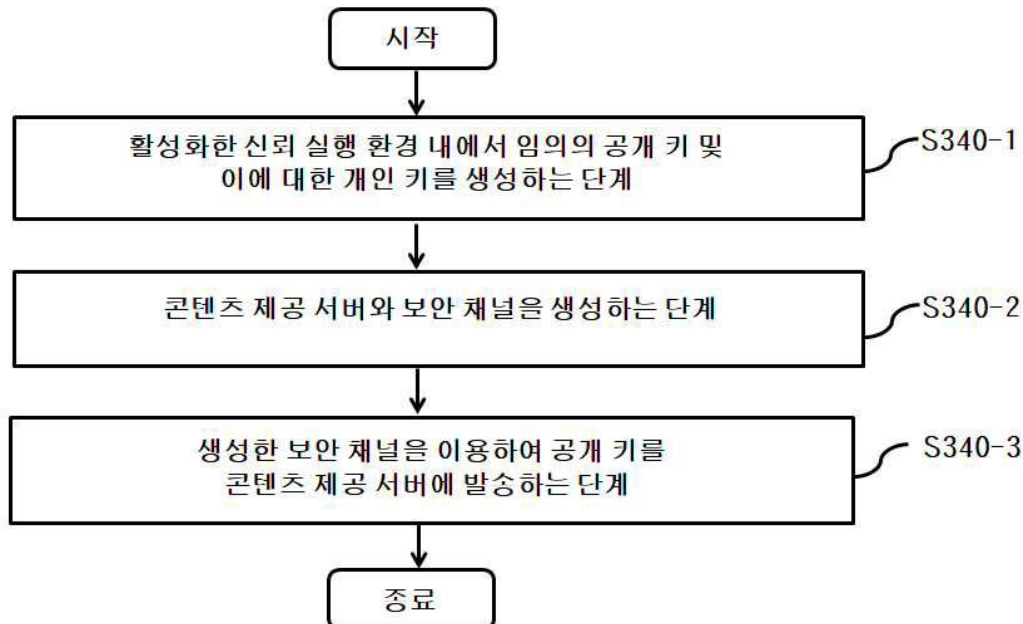
도면2



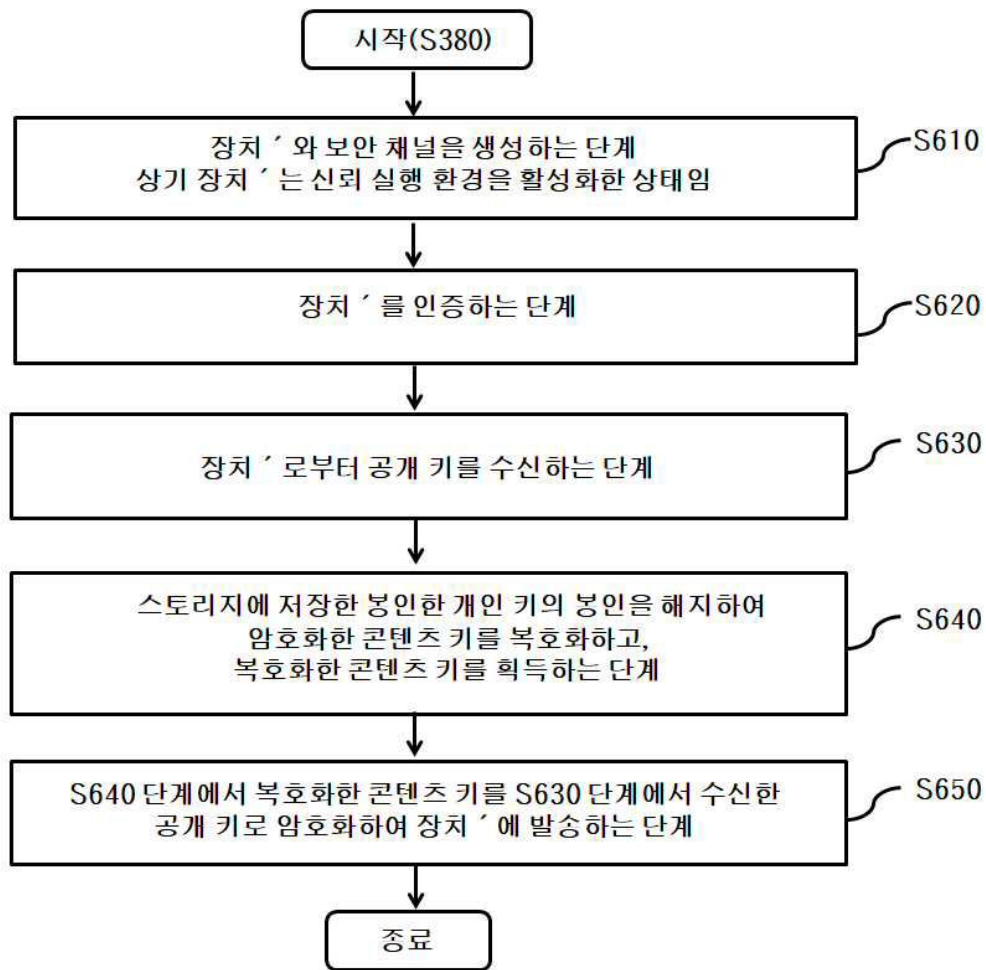
도면3



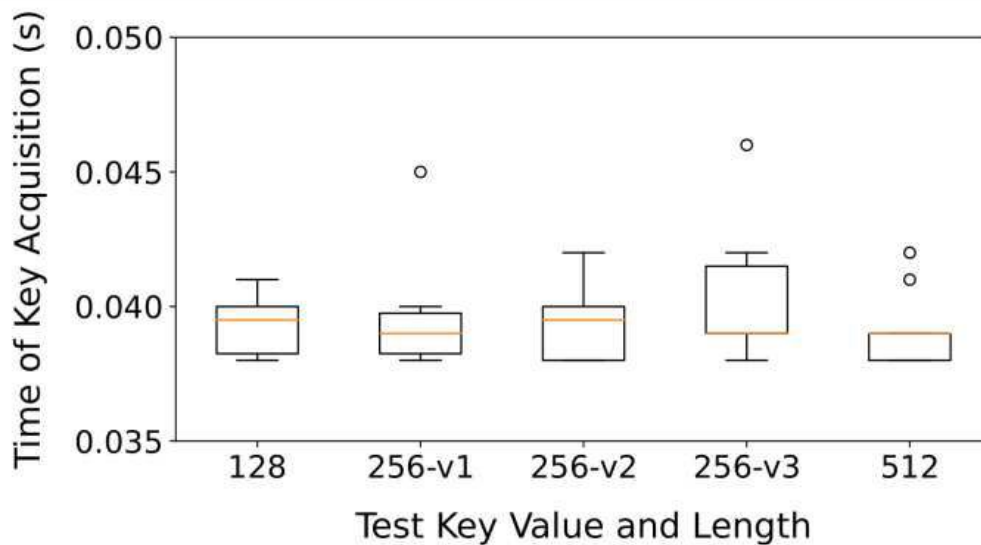
도면4



도면5



도면6



도면7

