이학석사 학위논문

DRM 시스템을 위한 익명성을 갖는 효율적인 라이센스 다운로드 방식

지도교수 박 지 환

이 논문을 [illegible] 학위 논문으로 제출함

2003년 2월

부경대학교 대학원

전 자 계 산 학 과

김 소 진

김소진의 이학석사 학위논문을 인준함

2002년 12월 26일

주 심 공학박사 정순호 

위 원 이학박사 조성진 

위 원 공학박사 박지환 

차 례

[표 차례]

<그림차례>

An Efficient License Download Method with Anonymity for DRM System

So Jin Kim

Dept. of Computer Science, PuKyong Nat'l University

ABSTRACT

The DRM(Digtal Rights Management) system prevents the unlawful use of digital contents and protects the copyright of onwer. It is a total solution to support all processings that is needed to the creation, distribution, usage, management of contents. And it provides the paid service of digital contents. The user (customer) should be pay money to use them fairly and be issued a license from clearinghouse in DRM system. Usually, the license is encrypted with user's public key. Therorfce, the computational cost of user may be expensive. Specially if the user is in mobile DRM environment, the computational cost of user may be more expensive. In addition, anonymity that identity is not exposured for the user's private life protection is not offered. To overcome this problem, we propose an efficient license download method with anonymity to apply one-time proxy signature scheme and Signcryption scheme for DRM. The former reduces the computational cost of user and the latter reduces the added computational cost of clearinghouse. The proposed scheme can be applied in mobile DRM.

Ⅰ. 서론

뉴 밀레니엄 시대를 맞은 현재 산업 분야의 화제는 정보통신 산업이고 정보통신 산업의 핵심 기술은 유선 인터넷과 무선 인터넷이다. 인터넷이 각광을 받기 시작한 것은 최근의 일이지만, 인터넷에 접속하는 사용자의 수가 기하급수적으로 증가하고 있고 향상된 통신 속도로 소리, 영상, 문자 등의 멀티미디어 정보들이 인터넷을 통해 자유롭게 전송, 교환되고 있다. 그러나 오프라인(off-line)에서만 제공되었던 정보들이 온라인(on-line)으로 제공되기 시작하면서 새로운 문제가 발생하였다. 온라인에서 디지털 정보의 교환은 손쉬운 복사와 배포를 가능하게 하고, 이것을 불법적으로 사용하게 한다. 그리하여 저작권의 침해를 가져오고 이에 대한 추적도 쉽지않아 유통기업의 수익창출을 어렵게 한다. 또한 컨텐츠를 소유한 사람들은 디지털의 '무한복사'의 특성 때문에 사업화에 많은 어려움을 겪고 있다. 기존의 보안 기술은 서버로의 침입을 감지하고 방어하는 개념이 주를 이루고 시스템에 대한 바이러스 예방이나 파일에 대해 암호를 설정하는 등의 방법이 있었지만 어느 것도 이러한 디지털 컨텐츠의 불법 복제는 해결해 주지 못했다. 그래서 디지털 저작권 관리 기술인 DRM(Digital Right Management)이 제안되었다[1-4].

DRM은 다양한 채널을 통해 유통되는 전자서적, 음악파일, 영상정보, 게임, 소프트웨어 등의 각종 디지털 컨텐츠를 여러 형태의 불법 복제로부터 안전하게 보호하고, 이렇게 보호된 컨텐츠를 사용하게 함으로 컨텐츠 서비스의 유료화를 가능하게 하는 기술이다. 단순히 불법복제만을 막는 기술이 아니라 안전한 저작권과 승인내역, 권리와 승인의 집행, 인증된 환경과 서비스 인프라 등을 가능하게 하는 하드웨어와 소프트웨어를 모두 포함한 디지털 저작권 관리에 관한 기술·절차·처리·알고리즘 등을 의미한다. 이러한 DRM 시스템을 통해 불법유통과 불법복제로부터 저작권을 보호하고 저작권자들의 수익을 효율적으로 분배하여 소비자에

게는 보다 질 좋은 컨텐츠를 제공할 수 있고, 디지털 컨텐츠의 유료화 시장은 정착될 수 있다. 그러므로 디지털 컨텐츠의 정당한 사용을 위해서 사용자(consumer)는 소정의 돈을 지불하고, 클리어링하우스(clearinghouse)로부터 컨텐츠 사용에 대한 승인을 받아야 한다. 이것은 라이센스(lisence)의 발급을 의미한다.

라이센스는 컨텐츠 사용의 시작일, 사용기간, 운용횟수, 운용방식 등에 관한 권한을 규정하고, 컨텐츠 ID, 컨텐츠 복호키, 라이센스 인증서 등을 포함한다. 그리고 일반적으로 사용자의 공개키로 암호화되기 때문에 계산적 부담이 크다. 특히 무선 DRM 환경인 경우, 사용자의 단말기가 제한적인 메모리 용량과 계산력으로 부담은 더욱 크게 된다. 또한 전자상거래 환경과 같이 DRM 시스템의 사용자도 자신의 신분이 노출되는 것을 꺼려한다. 사용자의 개인정보가 불법적으로 악용될 수 있고, 프라이버시(privacy)가 침해될 수 있기 때문이다.

따라서 본 논문에서는 일회용 대리서명[5]과 Signcryption[6]을 이용한 익명성을 갖는 효율적인 라이센스 다운로드 방식을 제안한다. 일회용 대리서명을 통해서는 사용자의 서명을 클리어링하우스가 대신 수행하여 사용자의 계산량을 감소시키고, Signcryption을 통해서는 대리서명에 따른 클리어링하우스의 추가된 계산량을 줄이고자 한다. 그리고 임시 비밀키/공개키 쌍을 가지고 컨텐츠를 구입하는 사용자의 신분을 보호한다.

본 논문의 구성은 다음과 같다. Ⅱ장은 연구배경으로 DRM과 Microsoft의 WMRM을 설명하고, Ⅲ장은 관련연구로 일회용 대리서명과 Singcryption에 대해 설명한다. 그리고 Ⅳ장에서는 DRM 시스템을 위한 익명성을 갖는 효율적인 라이센스 다운로드 방식을 제안하며, Ⅴ장은 제안 방식의 성능을 평가 및 고찰한다. 끝으로 Ⅵ장에서는 결론을 제시한다.

Ⅱ. 연구배경

1. DRM(Digital Rights Management)

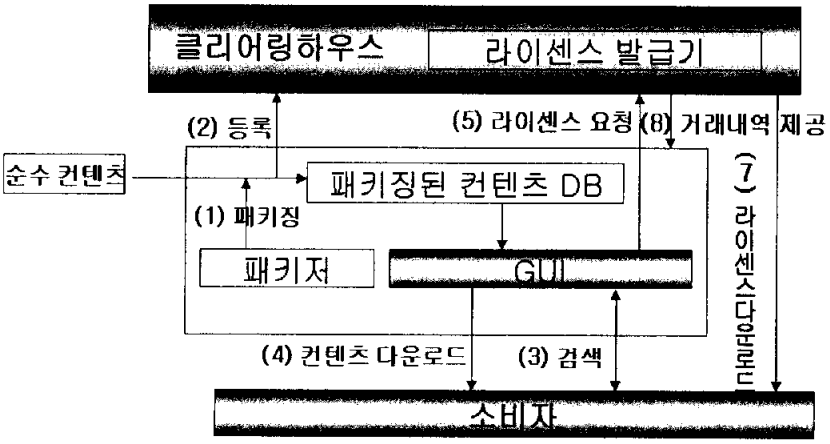
(1) DRM의 개요

새로운 가치로 등장한 디지털 컨텐츠와 과거 산업화 시대의 주력 상품인 자동차, 전자제품과의 다른 특성은 다음과 같이 크게 다섯 가지로 정리할 수 있다.

- 인터넷을 통해 상품 자체가 유통된다.
- 상품 복제가 매우 쉽다.
- 복제본과 원본의 질이 차이가 나지 않는다.
- 복제품과 원본의 구분이 힘들다.
- 저작권 보호가 힘들다.

21세기에 개인과 기업, 국가 경쟁력의 판도를 바꿀만큼 무한한 가치를 내재한 디지털 컨텐츠는 이러한 특성으로 인해 오히려 컨텐츠 제공자에게는 유료화의 걸림돌로, 기업 내에서는 보안의 장애요인으로 작용해 왔다. 그리하여 디지털 컨텐츠의 저작권 보호와 컨텐츠 유통의 기반마련을 위해 제안된 기술이 바로 DRM(Digital Rights Management :디지털 저작권 관리)이다[1-4].

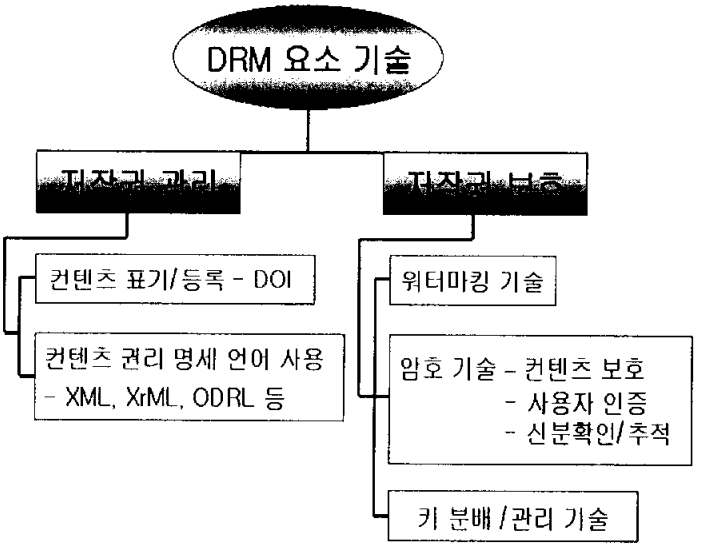
DRM은 컨텐츠 제공자의 권리와 이익을 보호하며, 디지털 컨텐츠의 불법 복제를 막고, 사용료 부과와 결제대행 등 컨텐츠의 생성에서 유통, 사용, 관리까지를 일괄 지원하는 기술이다. 그림1은 소비자가 쇼핑몰을 통해 원하는 컨텐츠를 자유로이 다운로드 받고, 이 컨텐츠의 정당한 사용을 위해 클리어링하우스에게 라이센스 요청을 하는 일반 DRM 체계를 나타낸다.



<그림1> 일반 DRM 체계

(2) DRM의 요소 기술 및 요구사항

DRM의 요소 기술은 저작권 관리와 저작권 보호 측면으로 구분하여 그림2와 같이 설명할 수 있다[4].



<그림2> DRM의 기술 분류

저작권 관리는 온라인 환경에서 일어나는 저작자 및 출판자에 대한 저작권을 지속적으로 관리하는 기술이다. 저작권 보호는 저작자 및 출판자의 컨텐츠를 안전하게 포장(packaging)하여 다양한 사업 모델에 적용할 수 있도록 하는 기술이다.

1) 저작권 관리 기술

가. 디지털 컨텐츠 식별자(Digital Object Identifier)[7]

- 인덱스 메타 데이터 체제와 연계하여 거래 정보의 상호 작용 및 갱신 기능을 수반한 디지털 저작물의 저작권 거래와 처리 및 관리

나. 컨텐츠 권리명세(XML, XrML 등)[8]

- 컨텐츠의 사용규칙을 정의

2) 저작권 보호 기술

가. 디지털 워터마킹(Watermarking) 기술[9,10]

- 컨텐츠내에 특정한 정보를 은닉시키는 방식으로 디지털 컨텐츠의 저작권을 안전하게 보호

나. 암호 기술[11]

- 컨텐츠 인증, 사용자 인증, 거래 및 사용규칙 강제화, 거래에 대한 부인방지 기능 등을 위하여 암호화, 전자서명 그리고 인증 등 다양한 암호 요소 기술들이 사용
- 컨텐츠에 대한 판별기능을 제공하여 정품과 불법 컨텐츠를 판별하고, 추적 기술을 제공함으로써 적극적으로 불법 복제를 방지
- **컨텐츠 암호화**: 대칭키 방식을 주로 사용하지만 대칭키의 단점을 보완하기 위해 공개키/대칭키 방식을 사용 가능
- **핑거프린팅(Fingerprinting) 기술[12,13]**: 컨텐츠에 삽입되는 값이 구매자의 정보이므로 컨텐츠가 불법 유통되었을 경우, 어떤 구매자에게 판매된 컨텐츠인지를 식별할 수 있고 법적인 조치 가능

다. **키 분배 및 관리 기술**: 대칭키와 공개키를 구분하여 컨텐츠의 특성 및 적용 환경에 따라 적절한 키 관리 매커니즘을 선택

DRM의 다양한 기능을 만족하려면 다음과 같은 사항이 필요하다.

① **컨텐츠의 패키징 및 컨텐츠 인증**: 암호화된 컨텐츠와 함께 컨텐츠 사용규칙 및 컨텐츠 식별기호를 하나의 포장으로 묶어 불법적인 접근과 사용을 방지하고 구매자는 컨텐츠의 저작권자, 공급자 등의 관련정보를 확인함으써 컨텐츠 진위여부를 인증한다.

② **사용자 인증**: 출판자와 분배자, 분배자와 소비자 등 거래 당사자들간에 서로를 인증한다.

③ **사용권리 적용**: 컨텐츠 사용에 대한 규칙적용을 의미하며 라이센스 형태로 제공된다.

④ **라이센스 보호**: 라이센스는 컨텐츠 사용 규칙이나 컨텐츠의 복호화 정보를 포함해야 한다.

⑤ **컨텐츠의 지속적인 저작권 보호**: 사용자의 컨켄트 사용 내역정보를 지속적으로 추적 관리함으로써 불법적인 컨텐츠의 사용을 방지한다.

⑥ **재분배(redistribution) 기술**: 일차적으로 컨텐츠에 대한 사용권리를 획득한 사용자가 다른 사용자에게 컨텐츠를 제공한다.

⑦ **사용내역의 측정 및 과금(clearinghouse)**: 사용 규칙에 따라 사용된 내역을 수집하여 요금을 부과함으로써 컨텐츠의 저작자 및 공급자에게 금전적인 보상을 제공한다.

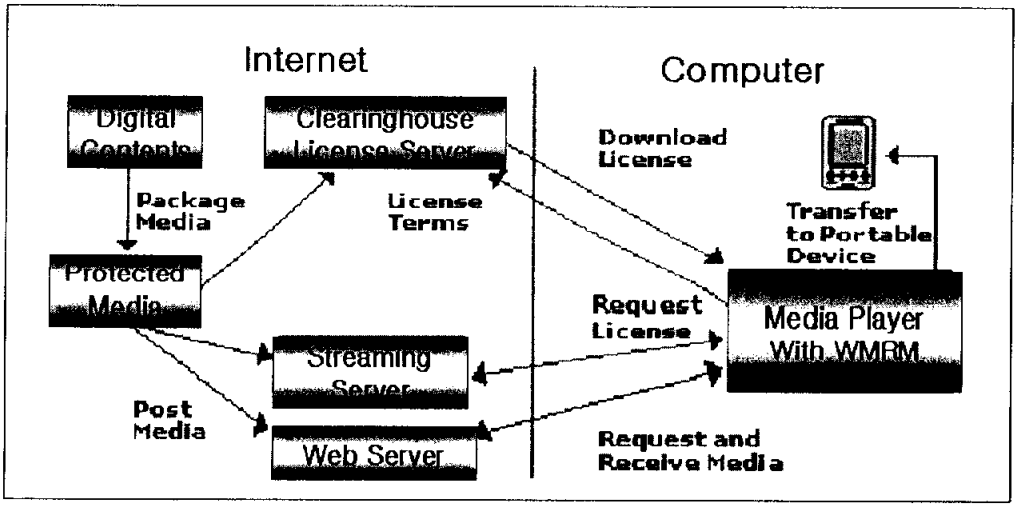
DRM은 디지털 컨텐츠 보호를 위한 단순 암호화 기술의 변종이 아니라 지식정보화 시대의 새로운 인프라로 평가되고 있다.

2. Microsoft WMRM(Windows Media Rights Manager)

DRM시장은 초반 장악력에서 InterTrust[14]가 독주하였으나 2000년 이후부터 DRM 솔루션을 무료로 배포하기 시작한 Microsoft[15]가 빠르게 추격하고 있다. Microsoft의 DRM인 WMRM(Windows Media Rights Manager)은 자사의 Windows OS에 포함하고 있는 윈도우 미디어플레이어 버전6.4부터 이미 탑재되어 배포되었으므로 전 세계적으로 4억개 가까이 설치되어 있다. 따라서 사용자는 별도의 클라이언트 모듈을 설치할 필요가 없기 때문에 WMRM이 널리 사용되고 있다.

(1) WMRM의 작동절차

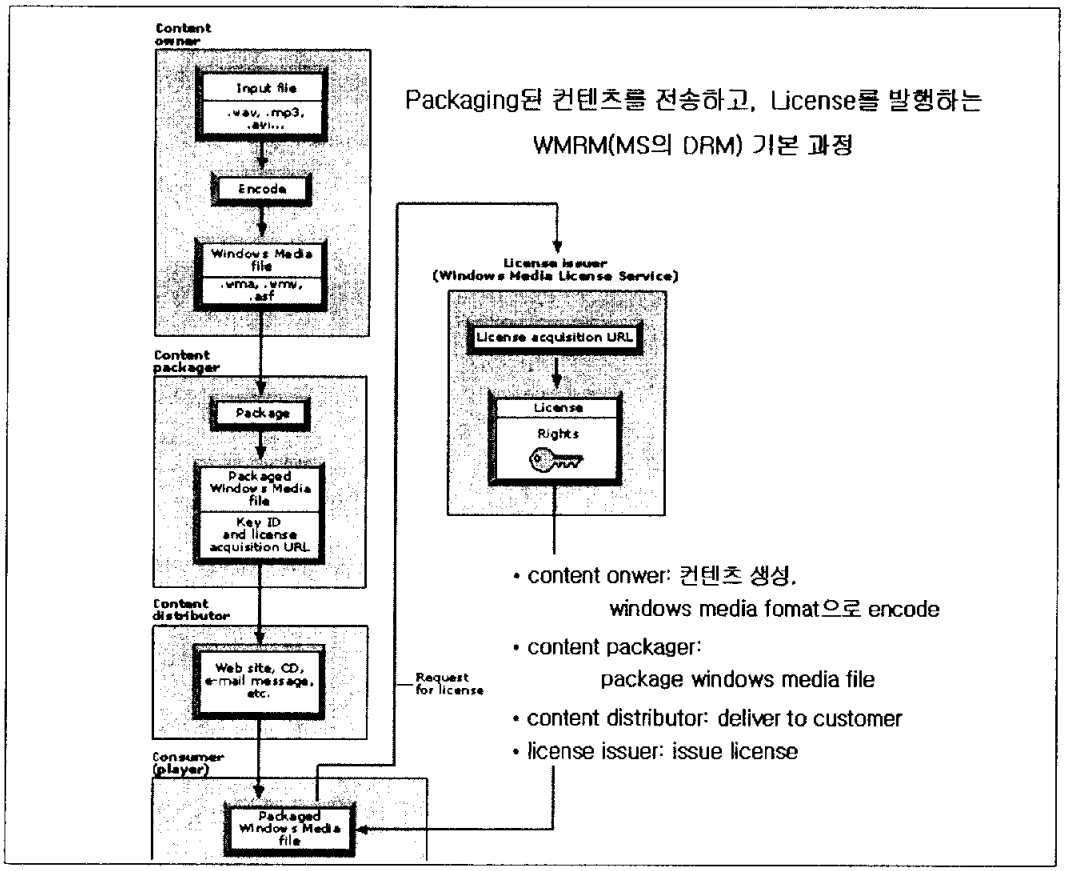
그림3의 WMRM은 컨텐츠와 라이센스가 분리되어 유통되도록 한다. 컨텐츠는 공개 서버에 올려져 자유로이 다운로드가 가능하고, 이에 대한 라이센스는 클리어링하우스의 인증을 통해서 발급받게 된다. 따라서 시스템의 관리과 용이하다.



<그림3> Windows Media Rights Manager Flow

1) WMRM의 기본 작동 절차<그림4>

다음과 같이 5단계로 구분된다.

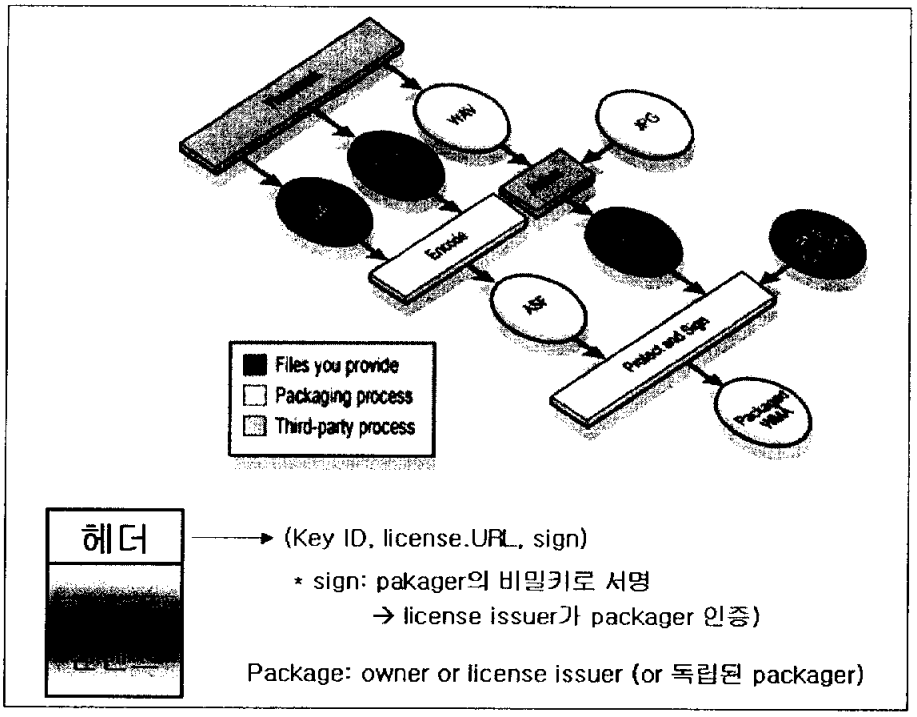


<그림4> 컨텐츠 패키징에서 유통 및 라이센스 획득 과정

가. 패키징<그림5>

- media files을 windows media file로 변환
- 변환된 파일은 비밀키를 사용하여 암호화
- 비밀키: 암호화된 라이센스에 저장되고 별도로 유통
- 라이센스를 확보할 수 있는 URL 정보를 컨텐츠(media file) 헤더에 추가

- 패키징된 파일: Windows Media Audio format (.wma) or Windo ws Media Video format (.wmv)으로 저장



<그림5> 컨텐츠의 패키징 과정

나. 유 통

- 암호화된 컨텐츠: 다운로드 용으로 웹사이트에 올려지거나, 스트리밍 용으로 미디어 서버에 올려지고, CD 또는 e-Mail로 고객들에게 유통
- WMRM을 활용해서 고객들은 복사한 컨텐츠를 또다른 사용자에게 전송 가능

다. 라이센스 서버(clearinghouse: 클리어링하우스)

- 라이센스 규정/권리를 보관하고 사용자를 인증하여 라이센스 서비스를 수행

라. 라이센스 획득

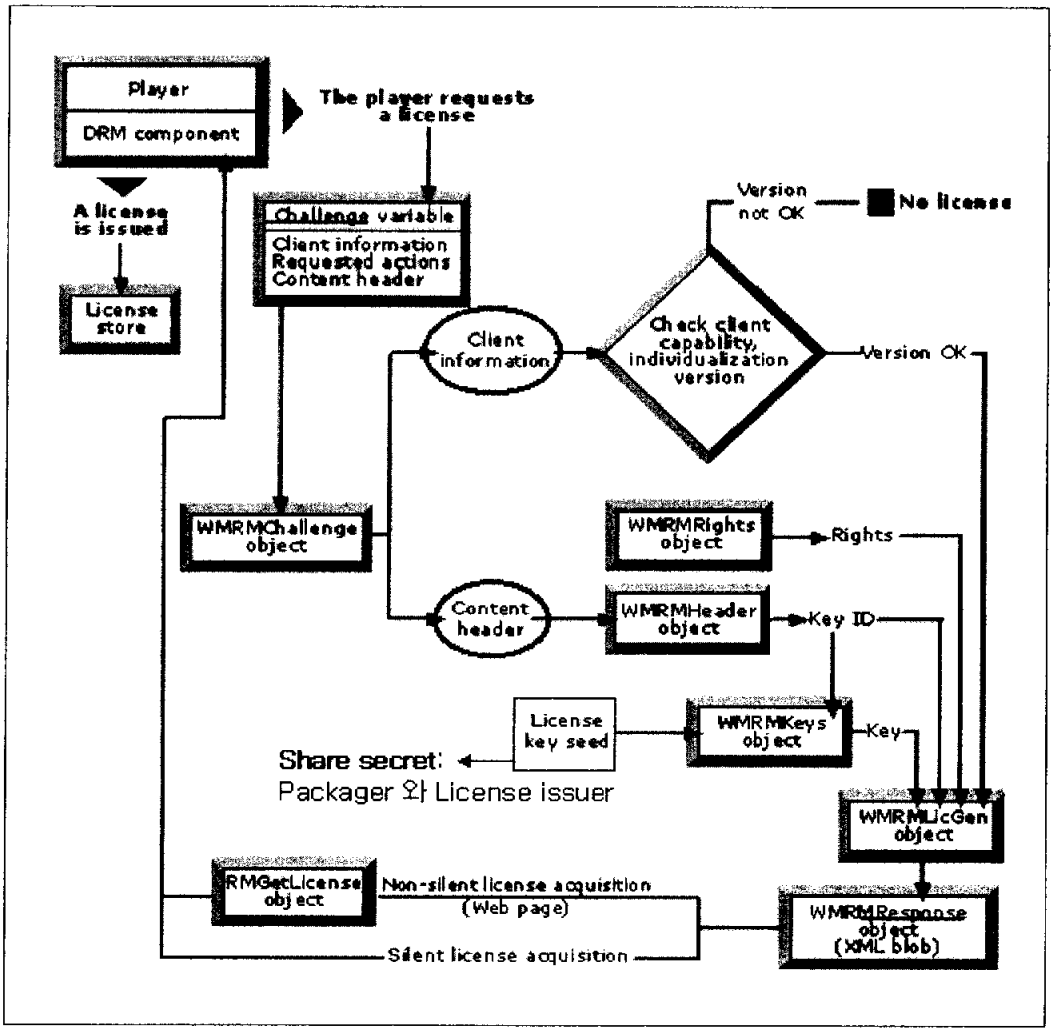
- 사용자는 암호화된 컨텐츠를 재생하기 위해서 필요한 라이센스 키가 필요
- 라이센스 확보 절차: 컨텐츠를 처음 재생하려고 할 때 자동으로 시작

마. 컨텐츠 재생 하기

- WMRM을 지원하는 media player 필요
- 라이센스에 포함된 규정 권리에 따라 컨텐츠 재생

WMRM에서는 컨텐츠와 라이센스가 분리되어 배포된다. 그래서 전체적인 시스템의 관리가 용이하다. 컨텐츠는 미리 대칭키 암호로 암호화되어 있고, 쇼핑몰과 같은 공개장소에서 자유로이 다운로드 및 재분배가 가능하다. 라이센스(license)는 처음 컨텐츠의 사용시, 혹은 사용자(customer)의 요청에 의해 클리어링하우스(clearighouse)에서 발행된다.

그림6은 사용자의 정보와 패키징된 컨텐츠의 헤더 정보를 이용하여 컨테츠의 사용규칙과 복호화 정보 등을 포함한 라이센스의 생성 및 발생 과정을 보여준다. 여기서 생성된 라이센스가 바로 WMRMLicGenobject이다. 클리어링하우스는 DRM의 핵심 부분으로 사용자 인증, 라이센스 발행 서비스 및 정산처리 등을 담당한다. 라이센스는 컨텐츠 사용의 시작일, 사용기간, 운용횟수, 운용방식 등에 관한 권한을 규정하고, 컨텐츠 ID, 컨텐츠 복호키, 라이센스 인증서 등을 포함한다. 그리고 PC-대-PC 라이센싱 정책으로 라이센스의 양도는 불가능하다. 따라서 라이센스 키를 가진 컴퓨터에서만 컨텐츠 재생이 가능하다.



<그림6> 라이센스 생성 및 발행 과정

(2) WMRM의 라이센스 다운로드 방식[16]

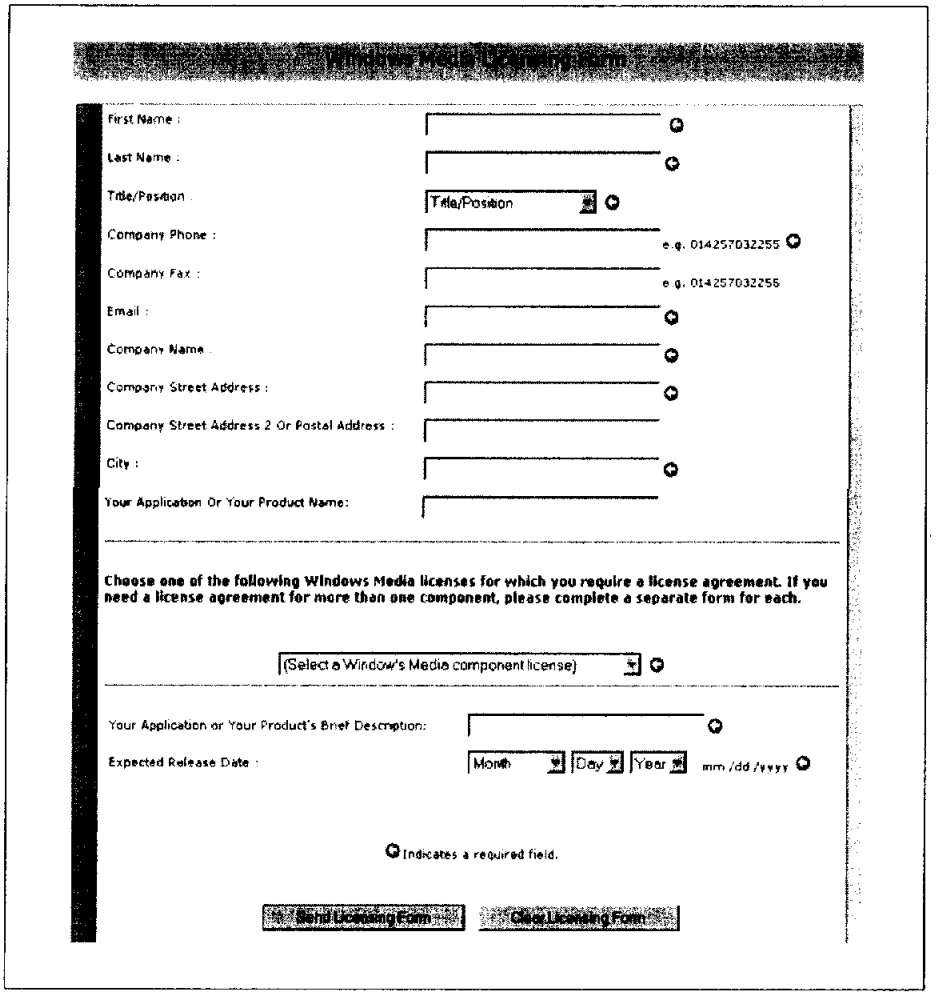
[표1] 매개변수와 시스템 설정(i)

x_u, y_u	• 사용자의 비밀키, 공개키 • $x_u \in Z_q^*$, $y_u \equiv g^{x_u} \pmod{p}$
x_c, y_c	• 클리어링하우스의 비밀키, 공개키 • $x_c \in Z_q^*$, $y_c \equiv g^{x_c} \pmod{p}$
req_u	• 사용자가 작성한 컨텐츠의 사용조건
$S_u(\cdot)$, ID_u	• 사용자의 서명, 사용자의 ID
m	• 라이센스 $m = (Key\ ID,\ Key,\ rights,\ certificate_{license}$ 등)
Key	• 컨텐츠의 복호키
$rights$	• 권리명세언어로 생성된 컨텐츠의 사용조건
$S_c(\cdot)$	• 클리어링하우스의 서명
$E_{y_u}(\cdot)$	• 사용자의 공개키 (y_u)로 암호화

가. 라이센스 요청

① **문서(inf_u, req_u)작성**: 사용자는 그림7과 같이 개인정보(inf_u)를 작성하고, 컨텐츠에 대한 사용조건(req_u)도 작성한다.

② **사용자의 문서 (inf_u, req_u, S_u, $certificate_u$)와 컨텐츠 헤더정보 전송**: 사용자는 작성된 inf_u, req_u를 자신의 비밀키로 서명하고, 인증서, 컨텐츠 헤더정보(*Key ID* 등) 등과 함께 클리어링하우스로 전송하고, 라이센스를 요청한다.



<그림7> 라이센스 요청 - 사용자의 정보 작성

나. 인증 및 라이센스 발급

① **인증 및 서명 검증**: 클리어링하우스는 전달받은 인증서와 서명값으로 정당한 사용자임을 확인하고, 정당한 문서임을 확인한다.

② **라이센스 생성**: 요청된 컨텐츠의 사용요구 조건에 맞게 다음과 같은 정보들을 포함한 라이센스(m)를 생성한다.

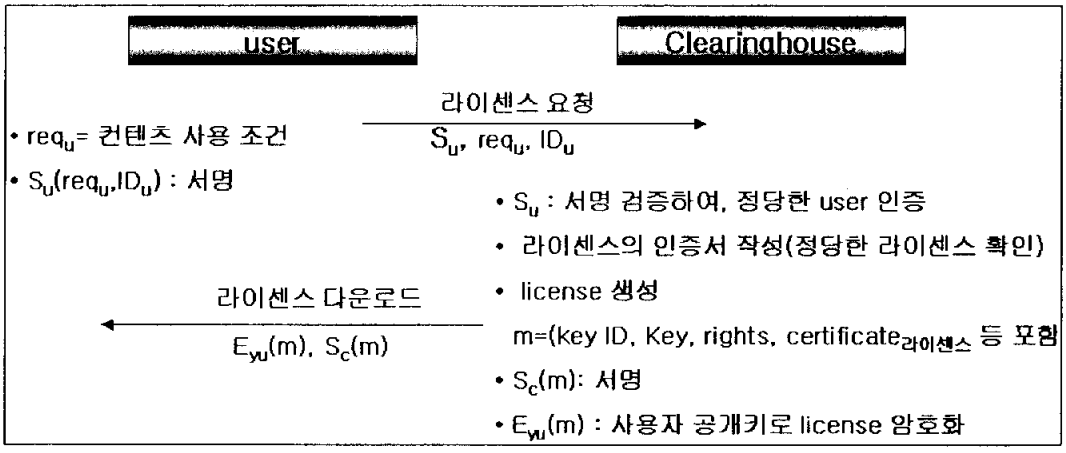
$m = (Key\ ID,\ Key,\ rights,\ certificate_{license}$ 등)

③ **라이센스 서명 및 암호화**: 클리어링하우스는 생성된 라이센스를 자신의 비밀키로 서명하고, 사용자의 공개키로 암호화한다.
($E_{y_u}(m)$, $S_c(m)$)

다. 라이센스 전송

클리어링하우스는 암호화된 라이센스를 서명값과 함께 안전한 채널을 통해 사용자에게 전송한다.

다음은 사용자의 개인정보, 인증서 등을 생략한 WMRM의 라이이센스 다운로드 과정을 보여준다.



<그림8> 라이센스 다운로드 과정

이 방식에서 라이센스는 공개키 암호를 사용하기 때문에 라이센스에 많은 정보와 기능을 부가할수록 라이센스 검증 및 획득시 사용자의 계산적 부담이 커진다. 특히 무선 DRM 시스템인 경우, 사용자의 단말기가 제한적인 메모리 용량과 계산력으로 부담은 더 크게 될 것이다. 그러므로 이러한 점을 개선해야 한다.

Ⅲ. 관련연구

1. 일회용 대리서명(One-Time Proxy Signature)

대리서명[17,18]은 원 서명자가 지정한 사람이 대신해서 서명을 하는 방식이다. KBLK 방식[19]에서는 모발 에이전트를 이용한 전자상거래 환경에서 호스트의 부정을 방지하기 위해 실패-중단 서명 기법[20]을 응용한 일회용 대리서명을 제안하였다. 이 방식은 사용자의 계산량을 줄여주기 위해서 호스트가 오직 한 개의 메세지에 대해서만 주어진 위임키로 대리서명을 수행하는 방식이다. 그러나 대리서명을 위한 서명키 생성 과정에서 많은 키들이 계산되고, 사용되며 전자상거래에 적용시 사용자의 신분을 보호 할 수 없어 프라이버시(privacy)도 보장받지 못한다. 그리하여 KCP 방식[5]에서는 이를 개선한 익명성을 갖는 효율적인 일회용 대리서명을 제안하였다.

[가정 1] KCP 방식에서는 다음의 가정을 전제한다.

(1) 사용자의 요구조건인 req_u는 시간정보를 포함한 값이므로 일정한 값으로 설정된다.

(2) 모든 공개키에 대한 인증과 공개를 위해서 등록센터를 가정한다

(3) 사용자의 익명성을 보장하기 위한 임시 비밀키/공개키 쌍은 등록센터를 통해 생성하고, 등록한다.

그리고 그 개요를 간략히 나타내면 다음과 같다.

[표2] 매개변수와 시스템 설정(ii)

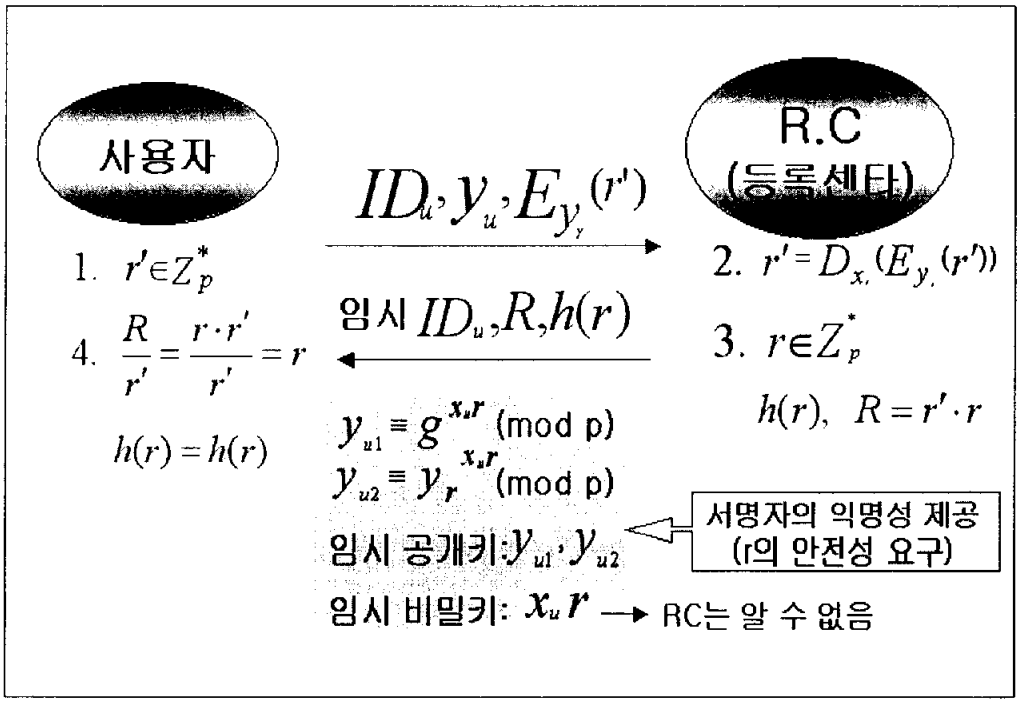
x_u, y_u	• 사용자(구매자)의 비밀키, 공개키 • $x_u \in Z_q^*$, $y_u \equiv g^{x_u} \pmod{p}$
x_{h_i}, y_{h_j}, y_{h_k}	• 호스트(판매자)의 비밀키, 공개키 • $x_{h_i} \in Z_q^* \quad i=\{1,2,3,4\}$ • $y_{h_j} \equiv g^{x_{h_j}} \quad j=\{1,2\}$, $y_{h_k} \equiv y_r^{x_{h_k}} \quad k=\{3,4\}$
ID_u	• 사용자의 ID
ID_h	• 호스트의 ID
req_u	• 사용자의 주문조건(요구사항)
bid_h	• 호스트의 확인/판매 정보
msg	• 서명대상 메시지 • $h(ID_u, ID_h, req_u, bid_h)$
$h(\cdot)$	• 안전한 일방향 해쉬함수

[표3] 등록센터(R.C)의 설정

Z_p^*	• modulo p인 정수의 곱셈군
x_r, y_r	• 등록센터의 비밀키, 공개키 • $x_r \in Z_q^*$, $y_r \equiv g^{x_r} \pmod{p}$
p	• 512비트 이상의 큰 소수, 공개
q	• $q \mid p-1$인 큰 소수, 공개
g	• $\alpha \in Z_p^{order\ q}$, 공개

가. 등록

임시 키쌍을 생성할 때는 안전성을 고려하여 영지식 증명법 등을 이용하기도 하지만, 계산량이 많아져 무선으로의 확장이 어렵다. 그러므로 임시 비밀키/공개키 쌍을 얻기 위해 그림9와 같은 과정을 수행하여 사용자는 임시ID_u를 얻고, 자신이 계산한 $h(r)$ 값과 전송받은 $h(r)$ 값이 같으면, y_{u_1}, y_{u_2}, $x_u r$를 생성한다. 이때 r의 유효 기간에 따라 등록 횟수는 달라진다. 만약 r의 유효 기간을 설정하지 않는다면, 등록은 한번만 하면 된다. 그러면 다음 등록 단계는 생략하고, 라이센스 요청 단계를 수행하면 된다. 등록센터는 자신의 DB에 ID_u, y_u, $E_{y_r}(r)$를 저장하고, 모든 임시 공개키는 공개한다.



<그림9> 임시 비밀키/공개키 생성 과정 - 익명성 제공

나. 위임키 생성

등록 단계에서 생성한 임시ID_u, y_{u_1}, y_{u_2}, $x_u r$를 가지고 사용자는 아래와 같이 위임키를 생성하여 호스트에게 전송한다.

① $k \in Z_{p-1}$, $K_1 \equiv g^k$, $K_2 \equiv y_r{}^k \pmod{p}$

② 임시ID_u, req_u, K_1, K_2로 다음을 계산한다.

$e = h(\text{임시}ID_u, req_u, K_1, K_2)$

③ 자신의 임시 비밀키 $x_u r$로 위임키 생성한다.

$s \equiv x_u r \cdot e + k \pmod{q}$

④ 호스트에게 임시ID_u, K_1, K_2, s, req_u, e를 전송한다.

다. 검증 및 대리서명

호스트는 컨텐츠 확인/판매 정보 bid_h를 이용하여 서명할 메시지 $msg = h(\text{임시}ID_u, ID_h, req_u, bid_h)$를 계산한 후, y_{u_1}, y_{u_2}, K_1, K_2, s, req_u를 이용하여 위임키를 검증하고, 대리서명을 수행한다.

① $g^s \equiv y_{u_1}{}^{h(\text{임시}ID_u,\ req_u,\ K_1,\ K_2)} \cdot K_1 \pmod{p}$

$y_r{}^s \equiv y_{u_2}{}^{h(\text{임시}ID_u,\ req_u,\ K_1,\ K_2)} \cdot K_2 \pmod{p}$

② 대리 서명키 s_1, s_2, s_3, s_4 생성한다.

$s_1 \equiv s + x_{h_1}$, $s_2 \equiv s + x_{h_2} \pmod{q}$

$s_3 \equiv s + x_{h_3}$, $s_4 \equiv s + x_{h_4} \pmod{q}$

④ 대리 서명에 대한 공개키 β 계산한다.

$\beta \equiv g^{(s_1 + s_2)} \cdot y_r{}^{(s_3 + s_4)} \pmod{p}$

⑤ 메세지 msg에 대한 대리서명 σ_1, σ_2 생성한다.

$$\sigma_1 \equiv (s_1 + s_2)/(msg + x_{h_1} - x_{h_2}) \pmod{q}$$

$$\sigma_2 \equiv (s_3 + s_4)/(msg + x_{h_3} - x_{h_4}) \pmod{q}$$

호스트는 ID_h, bid_h, msg, β, σ_1, σ_2를 사용자에게 전송한다.

라. 대리서명 검증

사용자는 전달받은 ID_h, bid_h, msg, β, σ_1, σ_2값들을 이용하여 호스트의 정당한 대리서명을 인증한다.

① $m = h(\text{임시}ID_u, ID_h, req_u, bid_h)$로 $m = msg$ 를 검사한다.

② 서명 공개키를 검증하여 호스트가 서명키를 정당하게 생성했는지 검증한다.

$$\beta \equiv y_{u_1}{}^{2e} \cdot K_1^2 \cdot y_{h_1} \cdot y_{h_2} \cdot y_{u_2}{}^{2e} \cdot K_2^2 \cdot y_{h_3} \cdot y_{h_4} \pmod{p}$$

③ 서명을 검증한다.

$$\beta \equiv (y_{h_1} \cdot y_{h_2}{}^{-1} \cdot g^{msg})^{\sigma_1} \cdot (y_{h_3} \cdot y_{h_4}{}^{-1} \cdot y_r^{msg})^{\sigma_2} \pmod{p}$$

위의 방식은 호스트가 악의를 가지고 위임키를 2번 이상 사용할 경우, 호스트의 비밀키가 노출되기 때문에 일회성을 보장하는 대리서명 기법이다. 그리고 사용자들의 신분을 보호할 수 있게 익명성이 추가되었다.

2. Signcryption

송/수신자가 공개 통신망에서 비밀 메시지를 교환하고자 한다면 메시지에 대한 전자 서명은 별개의 과정에 따라 암호화되어 상대방에게 전해지는 것이 일반적이다(signature-then-encryption 방식). 1997년 Zheng은 이러한 과정을 하나로 통합한 새로운 개념의 Signcryption 기법을 제안

하였다. Signcryption 방식[6]은 signature-then-encryption 방식에 비해 전체적인 계산량과 통신량이 낮아 효율적이다. 그리고 전자서명의 부인봉쇄 기능과 암호화의 기밀성도 제공한다.

다음은 SDSS1과 SDSS2로 명명된 두 가지의 Signcryption 방식을 나타낸다.

[표4] 매개변수와 시스템 설정(iii)

x_u, y_u	· 송신자의 비밀키, 공개키 · $x_u \in Z_q^*$, $y_u \equiv g^{x_u} \pmod{p}$
x_h, y_h	· 수신자의 비밀키, 공개키 · $x_h \in Z_q^*$, $y_h \equiv g^{x_h} \pmod{p}$
$E(\cdot)$, $D(\cdot)$	· 비밀키를 사용하는 암호화/복호화 알고리즘
$KH(\cdot)$	· Keded 일방향 해쉬함수
$h(\cdot)$	· 안전한 일방향 해쉬함수

가. Signcryption

생성	· $x \in Z_p^*$ · $K = h(y_h^x \bmod p)$ · $K = K_1 \| K_2$ · $r = KH_{K_2}(m)$ · [SDSS1] $s = x(r + x_u)^{-1} \bmod q$ · [SDSS2] $s = x(1 + x_u r)^{-1} \bmod q$ · $c = E_{K_1}(m)$

나. 전송

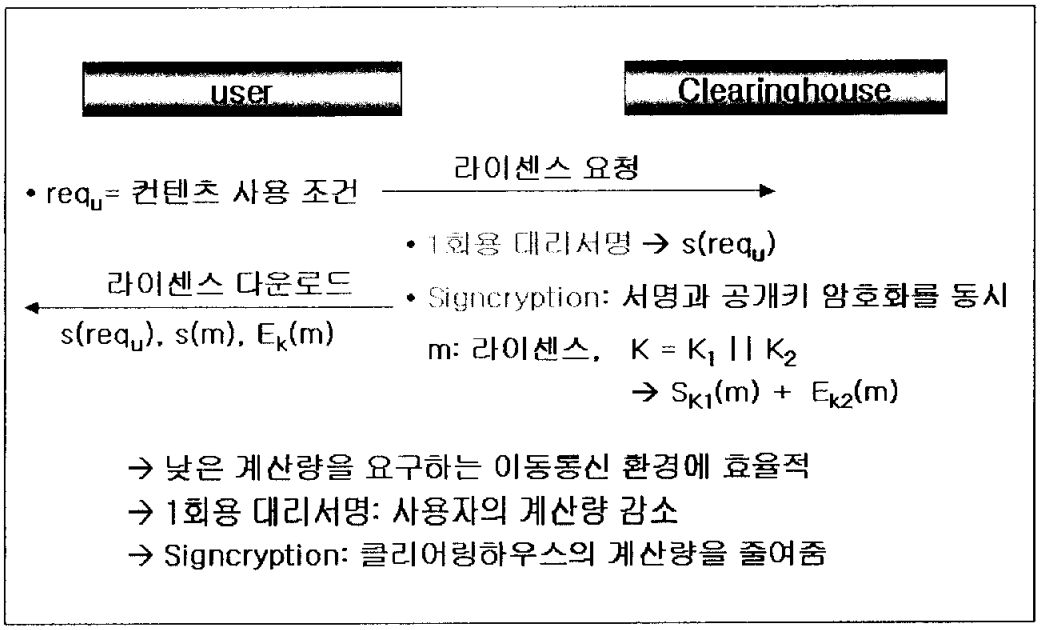
통신	· c, r, s

다. Unsigncryption

검증 및 복호	· [SDSS1] $K = h((y_u g^r)^{s \cdot x_h} \bmod p)$
	· [SDSS2] $K = h((y_u^r g)^{s \cdot x_h} \bmod p)$
	· $K = K_1 \| K_2$
	· $m = D_{K_1}(c)$
	· check if $r = KH_{K_2}(m)$

Ⅳ. 제안 방식

본 장에서는 DRM 시스템을 위한 익명성을 갖는 효율적인 라이센스 다운로드 방식을 제안한다. DRM의 라이센스 발급은 정당한 컨텐츠 사용을 위해서 중요하다. 하지만 라이센스가 공개키로 암호화되기 때문에 사용자의 계산적 부담이 크다. 그러므로 제안 방식은 일회용 대리서명[1]과 Signcrypiton[2]을 이용하여 효율성을 높인다. 일회용 대리 서명은 사용자의 서명을 클리어링하우스가 대신 수행하여 사용자의 계산량을 감소시키고, Singcryption은 대리 서명에 따른 클리어링하우스의 추가된 계산량을 줄이고자 한다. Signcryption 기법은 클리어링하우스가 생성한 라이센스의 서명과 암호화를 한꺼번에 해결하기 위해 사용된다.



<그림10> One-Time Proxy Signature + Signcrytpion

1. 익명성을 갖는 효율적인 라이센스 다운로드 방식

제안 방식은 일회용 대리서명을 이용함으로 *[가정 1]*의 조건을 전제한다. 그리고 라이센스 요청시 사용자의 개인정보, 인증서 등에 대한 전송은 생략한다.

가. 등록

사용자는 임시 비밀키/공개키 쌍을 얻기 위해 그림9와 같은 과정을 수행하여 임시ID_u를 얻고 y_{u_1}, y_{u_2}, $x_u r$를 생성한다. 이때 r의 유효 기간에 따라 등록 횟수는 달라질 수 있다.

나. 라이센스 요청

등록 단계에서 생성한 임시ID_u, y_{u_1}, y_{u_2}, $x_u r$를 가지고 사용자는 아래와 같이 위임키를 생성하여 클리어링하우스에게 전송하고, 라이센스를 요청한다.

① $k \in Z_{p-1}$, $K_1 \equiv g^k$, $K_2 \equiv y_r{}^k \pmod{p}$

② 임시ID_u, req_u, K_1, K_2로 다음을 계산

$e = h(\text{임시}ID_u, req_u, K_1, K_2)$

③ 자신의 임시 비밀키 $x_u r$로 위임키 생성

$s \equiv x_u r \cdot e + k \pmod{q}$

④ 클리어링하우스에게 임시ID_u, K_1, K_2, s, req_u, e를 전송

다. 위임키 검증 및 대리서명

클리어링하우스는 컨텐츠 확인정보 bid_c를 이용하여 서명할 메시지 $msg = h(\text{임시}ID_u, ID_c, req_u, bid_c)$를 계산한 후, y_{u_1}, y_{u_2}, K_1, K_2, s,

req_u를 이용하여 위임키를 검증하고, 대리서명을 수행한다.

① $g^s \equiv y_{u_1}^{h(\text{임시}ID_u,\ req_u,\ K_1,\ K_2)} \cdot K_1 \pmod{p}$

$y_r^s \equiv y_{u_2}^{h(\text{임시}ID_u,\ req_u,\ K_1,\ K_2)} \cdot K_2 \pmod{p}$

② 대리 서명키 s_1, s_2, s_3, s_4 생성

$s_1 \equiv s + x_{c_1}$, $s_2 \equiv s + x_{c_2} \pmod{q}$

$s_3 \equiv s + x_{c_3}$, $s_4 \equiv s + x_{c_4} \pmod{q}$

④ 대리 서명에 대한 공개키 β 계산

$\beta \equiv g^{(s_1+s_2)} \cdot y_r^{(s_3+s_4)} \pmod{p}$

⑤ 메세지 msg에 대한 대리서명 σ_1, σ_2 생성

$\sigma_1 \equiv (s_1 + s_2)/(msg + x_{c_1} - x_{c_2}) \pmod{q}$

$\sigma_2 \equiv (s_3 + s_4)/(msg + x_{c_3} - x_{c_4}) \pmod{q}$

라. 라이센스 생성

클리어링하우스는 컨텐츠의 *Key ID*, *Key*, *rights* 등을 포함하는 라이센스 $m = (Key\ ID,\ Key,\ rights,\ Certificate_{license}$ 등)를 생성한 후, Signcrytpion을 이용하여 다음과 같이 라이센스를 암호화하고 서명한다.

① 비밀키 K는 사용자의 공개키를 이용해서 생성하고, K_1, K_2 로 분리

$k' \in Z_{p-1}, K = (y_{u_1} \cdot y_{u_2})^{k'} \pmod{p}$

$K = K_1 || K_2$

② K_1, K_2로 라이센스 m를 암호화 및 해쉬함수 적용

$E = E_{K_1}(m)$, $H = Kh_{K_2}(m)$

(암호화 및 해쉬함수에 K를 동시 적용 - 적은 계산량, 효율적)

④ 메세지 H에 대한 서명 τ_1, τ_2 생성

$$\tau_1 \equiv k'/(H + x_{c_1} + x_{c_2}) \pmod{q}$$

$$\tau_2 \equiv k'/(H + x_{c_3} + x_{c_4}) \pmod{q}$$

마. 라이센스 다운로드

클리어링하우스는 자신의 ID_c, 대리서명에 대한 bid_c, msg, β, σ_1, σ_2과 라이센스 발급에 대한 E, H, τ_1, τ_2를 사용자에게 전송한다.

바. 대리서명 검증

사용자는 전달받은 ID_c, bid_c, msg, β, σ_1, σ_2값들을 이용하여 클리어링하우스의 대리서명에 대한 인증을 수행한다.

① $m = h(\text{임시}ID_u, ID_c, req_u, bid_c)$로 $m = msg$ 검사

② 서명 공개키를 검증하여 클리어링하우스가 서명키를 정당하게 생성했는지 검증

$$\beta \equiv y_{u_1}^{2e} \cdot K_1^2 \cdot y_{c_1} \cdot y_{c_2} \cdot y_{u_2}^{2e} \cdot K_2^2 \cdot y_{c_3} \cdot y_{c_4} \pmod{p}$$

③ 서명 검증

$$\beta \equiv (y_{c_1} \cdot y_{c_2}^{-1} \cdot g^{msg})^{\sigma_1} \cdot (y_{c_3} \cdot y_{c_4}^{-1} \cdot y_r^{msg})^{\sigma_2} \pmod{p}$$

사. 라이센스 획득

사용자는 전달받은 E, H, τ_1, τ_2 값들을 이용하여 클리어링하우스가 발급한 라이센스를 획득한다.

① 자신의 비밀키 $x_u r$를 이용하여 다음과 같은 K 값을 계산

$$K \equiv (y_{c_1} \cdot y_{c_2} \cdot g^H)^{\tau_1 \cdot x_u r} \cdot (y_{c_3} \cdot y_{c_4} \cdot y_r^H)^{\tau_2 \cdot x_u r} \pmod{p}$$

② K를 $K_1||K_2$로 나누고, 라이센스 m을 복호화

$m = D_{K_1}(E)$

③ 위의 식에서 얻은 m으로, $H' = h_{K_2}(m)$을 계산

④ $H' = H$인 경우에만, 정당한 라이센스를 획득

사용자의 임시 비밀키/공개키 쌍이 등록센터를 통해 이미 생성되고 등록되었다면, 제안 방식은 다음과 같다.

User

Clearinghouse

가. 라이센스 요청

▶ 등록 단계에서 생성한 임시ID_u, y_{u_1}, y_{u_2}, $x_u r$를 가지고 위임키를 생성

① $k \in Z_{\phi-1}$, $K_1 \equiv g^k$, $K_2 \equiv y_r{}^k$

② 임시ID_u, req_u, K_1, K_2로 다음을 계산

$e = h($임시$ID_u, req_u, K_1, K_2)$

③ 자신의 임시 비밀키 $x_u r$로 위임키 생성

$s \equiv x_u r \cdot e + k$

임시ID_u, s, K_1, K_2, req_u

라이센스 요청 ⟶

나. 위임키 검증 및 대리 서명

▶ 컨텐츠 확인정보 bid_c를 이용하여 서명할 메시지 $msg = h($임시ID_u, ID_c, req_u, $bid_c)$를 계산한 후, y_{u_1}, y_{u_2}, K_1, K_2, s, req_u로 수행

① $g^s \equiv y_{u_1}{}^{h(\text{임시}ID_u,\ req_u,\ K_1,\ K_2)} \cdot K_1$

$y_r{}^s \equiv y_{u_2}{}^{h(\text{임시}ID_u,\ req_u,\ K_1,\ K_2)} \cdot K_2$

② 대리 서명키 s_1, s_2, s_3, s_4 생성

$s_1 \equiv s + x_{c_1}$, $s_2 \equiv s + x_{c_2}$

$s_3 \equiv s + x_{c_3}$, $s_4 \equiv s + x_{c_4}$

③ 대리 서명에 대한 공개키 β 계산

$\beta \equiv g^{(s_1+s_2)} \cdot y_r{}^{(s_3+s_4)}$

④ 메세지 msg에 대한 대리서명 σ_1, σ_2 생성

$\sigma_1 \equiv (s_1 + s_2)/(msg + x_{c_1} - x_{c_2})$

$\sigma_2 \equiv (s_3 + s_4)/(msg + x_{c_3} - x_{c_4})$

<그림11> 제안 라이센스 다운로드 방식

User

Clearinghouse

다. 라이센스 생성

▶ 라이센스 $m=(Key\ ID,\ Key,\ rights,\ Certificate_{라이센스}$ 등)을 생성한 후, Y Zheng의 Signcryption 방식[19]을 이용

① 비밀키 K는 사용자의 공개키를 이용해서 생성하고, K_1, K_2로 분리

$$k' \in Z_{\phi-1},\ K=(y_{u_1}\cdot y_{u_2})^{k'}$$

$$K=K_1 \| K_2$$

② K_1, K_2로 라이센스 m를 암호화 및 해쉬함수 적용

$$E=E_{K_1}(m),\quad H=Kh_{K_2}(m)$$

③ 메세지 H에 대한 서명 τ_1, τ_2 생성

$$\tau_1 \equiv k'/(H+x_{c_1}+x_{c_2})$$

$$\tau_2 \equiv k'/(H+x_{c_3}+x_{c_4})$$

라. 라이센스 다운로드

ID_c, bid_c, msg, β, $\sigma_1 \cdot \sigma_2$, E, H, $\tau_1 \cdot \tau_2$

← 라이센스 다운로드 ——

클리어링하우스의 아이디와, 대리서명, 라이센스 생성 단계에서 생성된 값들을 전

마. 대리서명 검증

▶ ID_c, bid_c, msg, β, σ_1, σ_2 값들을 이용

① $m=h($임시$ID_u, ID_c, req_u, bid_c)$로 $m=msg$ 검사

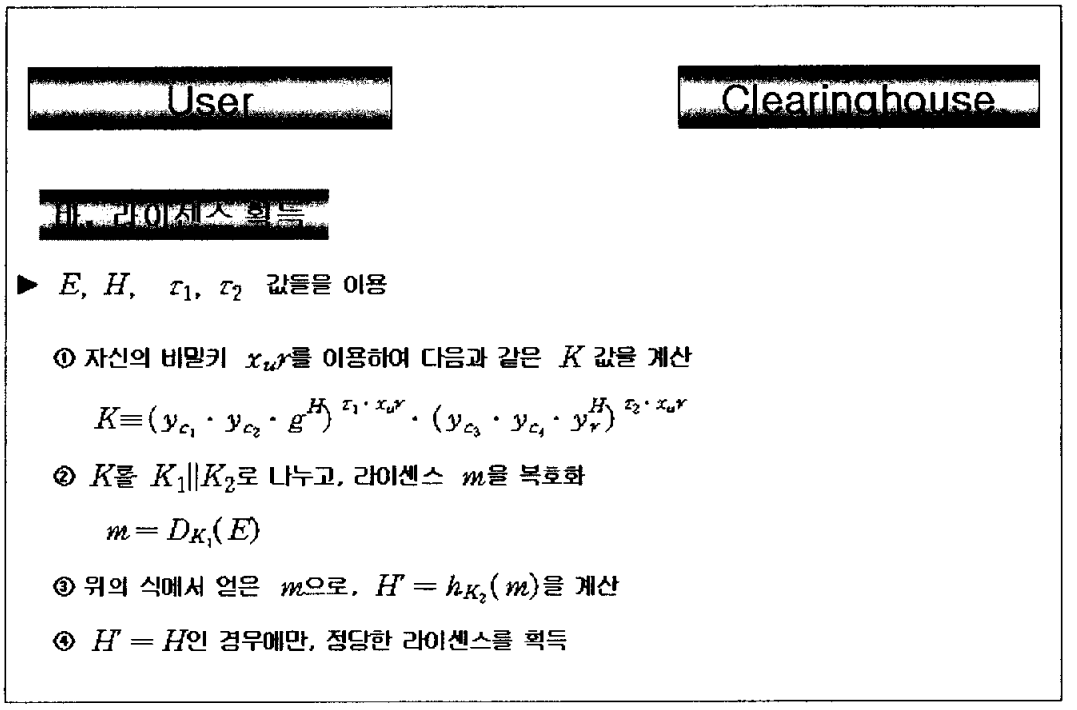
② 서명 공개키를 검증하여 클리어링하우스가 서명키를 정당하게 생성했는지 검증

$$\beta \equiv y_{u_1}^{2e}\cdot K_1^2\cdot y_{c_1}\cdot y_{c_2}\cdot y_{u_2}^{2e}\cdot K_2^2\cdot y_{c_3}\cdot y_{c_4}$$

③ 서명 검증

$$\beta \equiv (y_{c_1}\cdot y_{c_2}^{-1}\cdot g^{msg})^{\sigma_1}\cdot(y_{c_3}\cdot y_{c_4}^{-1}\cdot y_r^{msg})^{\sigma_2}$$

<그림11> 제안 라이센스 다운로드 방식(계속)



<그림11> 제안 라이센스 다운로드 방식(계속)

V. 성능 평가 및 고찰

1. 안전성 분석

본 논문은 전제적으로 이산대수 문제의 어려움에 기반하고, 일회용 대리서명과 Signcrytpion의 안전성에 기반한다.

[정의 1.] 이산대수 문제의 어려움

소수 p와 위수 $t=p-1$인 곱셈상의 군 z_p^*의 생성자 g, 그리고 원소 $y \in Z_p^*$가 주어졌을 때 $y \equiv g^x \bmod p$를 만족하는 $1 \le x \le p-2$ 범위내의 $x = \log_g y \bmod (p-1)$을 구하는 것이다.

(1) 일회용 대리서명의 안전성

[정리1] 원 서명자만이 위임키를 생성할 수 있다. ($s \equiv x_u r \cdot e + k$)

- 위임키에 대한 안전성은 이산대수 문제의 어려움에 기반하여 원 서명자의 비밀키를 모르면 생성할 수 없다.

[정리2] 원 대리서명자만이 대리서명을 할 수 있다.

($s_1 \equiv s + x_{c_1}$, $s_2 \equiv s + x_{c_2}$, $s_3 \equiv s + x_{c_3}$, $s_4 \equiv s + x_{c_4}$)

- 서명키의 안전성도 이산대수 문제의 어려움에 기반함으로 대리자의 비밀키를 모르면 키를 생성할 수 없으며, 서명도 불가능하다.

[정리3] 대리 서명자의 서명이 일회성임을 보장한다.

- 두번 이상 사용하면 아래와 같이 비밀키가 노출된다.

<일회용 대리서명임을 증명>

(1) σ_1 증명

$$\sigma_1(msg + x_{c_1} - x_{c_2}) = s_1 + s_2 \quad ①$$

$$\sigma'_1(msg' + x_{c_1} - x_{c_2}) = s_1 + s_2 \quad ②$$

두 식 ①, ②는 s_1, s_2의 값으로 같다.

$$\sigma_1(msg + x_{c_1} - x_{c_2}) = \sigma'_1(msg' + x_{c_1} - x_{c_2}) \quad ③$$

∴ ③은 식 2개, 미지수 2개로 이것을 계산하면,
대리자의 비밀키 x_{c_1}, x_{c_2}가 노출된다.

(2) σ_2 증명

$$\sigma_2(msg + x_{c_3} - x_{c_4}) = s_3 + s_4 \quad ①$$

$$\sigma'_2(msg' + x_{c_3} - x_{c_4}) = s_3 + s_4 \quad ②$$

두 식 ①, ②는 s_3, s_4의 값으로 같다.

$$\sigma_2(msg + x_{c_3} - x_{c_4}) = \sigma'_2(msg' + x_{c_3} - x_{c_4}) \quad ③$$

∴ ③은 식 2개, 미지수 2개로 이것을 계산하면
대리자의 비밀키 x_{c_3}, x_{c_4}가 노출된다.

대리 서명키를 2번 이상 사용할 경우, 대리 서명키 (s_1, s_2, s_3, s_4)와 클리어링하우스의 비밀키 노출!

[정리4] 서명단계는 실패-중단 서명기법의 안전성과 동일하다.

- 이산대수 문제의 어려움에 기반함으로 서명의 위조는 등록센터의 비밀키 x_r를 알아야 한다.

$$(g^{x_{c_1}} \cdot g^{-x_{c_2}} \cdot g^{msg})^{(\sigma_1 - \tau_1)} = (y_r^{x_{c_3}} \cdot y_r^{-x_{c_4}} \cdot y_r^{msg})^{(\tau_2 - \sigma_2)}$$

$$= (g^{x_{c_3}} \cdot g^{-x_{c_4}} \cdot g^{msg})^{x_r(\tau_2 - \sigma_2)}$$

(2) Signcryption의 안전성

송/수신자를 위한 Signcryption의 키 생성은 이산대수 문제의 어려움에 기반한다. 그러므로 수신자의 임시 비밀키 $x_u r$를 모르면 Signcryption의 키를 복구할 수 없어 메시지의 기밀성을 보장한다.

송신자의 키 생성	· $K=(y_{u_1} \cdot y_{u_2})^{k'}$
수신자의 키 복구	· $K\equiv(y_{c_1} \cdot y_{c_2} \cdot g^{H})^{\tau_1 \cdot x_u r} \cdot (y_{c_3} \cdot y_{c_4} \cdot y_r^{H})^{\tau_2 \cdot x_u r}$

그리고 송/수신자의 정보를 포함하여 서명에 대한 부인방지가 가능하다.

2. 특징 고찰

① **안전성** - 전체적으로 이산대수 문제의 어려움에 기반하며, 일회용 대리서명과 Signcryption의 안전성에 기반한다.

· **대리서명**: 일회용 대리서명의 안전성에 기반한다.

· **라이센스 암호화 및 서명**: Signcryption의 안전성에 기반한다.

② **라이센스의 기밀성** - 이산대수 문제의 어려움에 기반하여 정당한 사용자만이 라이센스를 복호화하고, 서명을 확인할 수 있다.

$$K \equiv (y_{u_1} \cdot y_{u_2})^{k'} \equiv (y_{C_1} \cdot y_{C_2} \cdot g^H)^{r_1 \cdot x_u r} \cdot (y_{C_3} \cdot y_{C_4} \cdot y_r^H)^{r_2 \cdot x_u r}$$

③ **클리어링하우스의 부정 방지** - 대리서명이 1회성을 보장함으로 부정을 방지할 수 있다[정리3].

④ **인증성** - 대리서명과 라이센스 발급시에 송/수신자를 지정하여 계산과정에 포함시켜 인증성을 제공하고, 전송도중 공격자로부터의 위조 및 변경에 대한 확인도 가능하다.

⑤ **효율성** - 라이센스 다운로드 과정은 대리서명과 Signcryption으로 처리함으로 사용자의 계산량이 낮아진다.

⑥ **부인봉쇄** - 대리서명시 사용자와 대리자의 비밀정보를 포함하고, Singcryption의 키 생성에도 사용자와 클리어링하우스의 비밀정보를 포함하여 서로에 대한 부정을 할 수 없다.

⑦ **익명성** - 제안 1회용 대리서명을 사용하여 사용자의 익명성을 보장한다. 임시 공개키 $y_{u_1} \equiv g^{x_u r}$, $y_{u_2} \equiv y_r^{x_u r}$에서 $x_c r$은 오직 사용자만 알고, 원 공개키 y_u는 등록센터만 알기 때문이다.

3. 계산량 비교

대리서명은 원 서명자를 대신하여 대리자가 서명하는 것으로 전자상거래와 같은 전자시스템 수행시에 사용자의 계산량 부담을 줄여주는 장점을 가진다. 이것은 여러 논문[21-23]에서 제시되었기에 표5의 계산량 비교에서 생략한다. 따라서 라이센스의 서명/암호 알고리즘에 RSA서명/RSA암호, DSS서명/ElGamal암호, Schnorr서명/ElGamal암호의 사용을 가정하고, Signcrytpion[2]의 Table2를 참고하여 표6과 같이 제안방식을 비교한다. 이때 지수연산(exp)에 비해 다른 연산(mul, add 등)들의 계산량은 상대적으로 낮기 때문에 지수연산만을 나타낸다.

[표5] 기존 서명/암호 방식과의 계산량 비교

<table>
<tr><td rowspan="2">사용자측의
계산량</td><td colspan="4">컨텐츠 사용에 대한 서명</td></tr>
<tr><td colspan="4">기존의 RSA 서명, DSS 서명, Schnorr 서명으로 직접서명을 수행하면, 사용자측의 시스템에 부담이 크다. 그러므로 제안 1회용 대리서명 방식으로 사용자측의 부담을 덜어준다.</td></tr>
<tr><td rowspan="3">클리어링하우스측의 계산량</td><td colspan="3">라이센스 서명 후 암호화 방식</td><td rowspan="2">제안 방식
(1회용 대리서명 + Signcryption)</td></tr>
<tr><td>1회용 대리서명
+ RSA 서명과
RSA 암호</td><td>1회용 대리서명
+ DSS 서명과
ElGamal 암호</td><td>1회용 대리서명
+ Schnorr 서명과
ElGamal 암호</td></tr>
<tr><td>Exp: 4번</td><td>Exp: 5번</td><td>Exp: 5번</td><td>Exp: 3번</td></tr>
</table>

제안 방식은 일회용 대리서명을 이용해서 사용자의 계산량을 낮추고, 상대적으로 증가한 클리어링하우스의 계산량은 Signcrytpion을 적용하여 낮추었다. 그리하여 전체적인 계산량이 표5에 제시한 서명과 암호를 사용하는 것에 비해 효율적임을 알 수 있다.

Ⅵ. 결론

DRM은 오디오나 동영상, 텍스트 등 각종 디지털 컨텐츠의 불법 사용을 방지해 저작권자의 이익을 보호하는 솔루션이다. 지금은 시작단계에 있고, 표준화가 미비하여 바라보는 시각에 따라 서로 다른 의견들을 가지고 있어 간혹 혼란스럽기도 하다. 그러나 2~3년 후에는 DRM시장이 폭발적으로 늘어나 디지털 컨텐츠 시대를 열어갈 것이다. 그러므로 DRM 시스템의 활성화를 위해서 사용자는 정당한 디지털 컨텐츠 사용에 대한 요금을 지불하고, 클리어링하우스로부터 라이센스를 발급받아야 한다. 라이센스는 컨텐츠에 대한 정보와 복호키, 사용권리 등의 많은 정보를 포함하고, 공개키로 암호화된다. 그리하여 이를 복호화하는 사용자의 부담이 크다.

따라서 본 논문은 DRM의 라이센스 발급시 사용자의 계산량을 줄여 무선 DRM으로 확장 가능한 효율적인 라이센스 다운로드 방식을 제안하였다. 익명성을 갖는 일회용 대리서명을 이용하여 사용자의 계산량을 감소시켰고, 상대적으로 증가한 클리어링하우스의 계산량은 Signcryption을 이용하여 감소시켰다. 그리고 클리어링하우스가 악의를 가지고 위임키를 두번 이상 사용할 경우, 정리3에 의해 클리어링하우스의 비밀키가 노출되기 때문에 부정을 막을 수 있다. 또한 무선 환경은 유선 환경에 비해 도청자나 그 밖의 위조, 불법적 변경 등과 같은 위협들에 매우 취약하므로 사용자를 보호하는 익명성을 추가하였다.

향후 과제로는 안전한 라이센스 관리를 통한 컨텐츠 불법 사용을 방지하는 연구가 필요하겠다.

참고문헌

[1] http://www.drm.or.kr

[2] http://www.fasoo.com/sub_tech01.html

[3] http://www.markany.com/tech02.htm

[4] 전종민, 최영철, 박상준, 박성준, "DRM 기술 및 제품 동향 분석", 한국정보보호학회지 제 11권 5호, 2001.10

[5] 김소진, 최재귀, 박지환, "익명성을 갖는 효율적인 1회용 대리서명", 정보처리학회 추계학술대회, 2002.11

[6] Y.Zheng, "Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) +Cost(Encryption)", CRYPTO '97, Springer-venlag, LNCS 1294, pp165-179, 1997

[7] http://www.kpa21.or.kr

[8] http://www.rxml.org, "XrML Spec. 1.3" June. 2000

[9] H.J.Lee, J.H.Park, Y.Zheng, "Digital Watermarking Robust Against JPEG Compression", Lecture Notes in Computer Science, Springer, No.1729, pp.167-177, Nov. 1999

[10] J.H.Park, S.E.Jeong, Y. Huh, "A New Digital Watermarking Technique for Text Documents Using Diagonal Profile", Lecture Notes in Computer Science, Springer, No.2195, p.748-755 Oct. 2001

[11] "정보은닉 최신기술 동향 분석", 한국정보보호진흥원, 2001.12

[12] B.Pfitzman and M.Schunter. "Asymmetric Fingerprinting", Eurocrypt'97, Vol. 1070 of LNCS, pp. 84-95

[13] B.Pfitzman and M.Waidner, "Anonymous Fingerprinting", Eurocrypt'97, Vol. 1233 of LNCS, pp.88-102

[14] http://www.intertrust.com/main/research/index.html

[15] http://www.microsoft.com/windows/windowsmedia/drm.asp

[16] http://www.microsoft.com/windows/windowsmedia/wm7/drm/licensing.asp

[17] M.Mambo, K.Usuda and E.Okamoto, "Proxy Signature : Delegation of the power to sign message", IEICE Transaction on Fundam entals, E79-A(9), pp.1338-1354, 1996

[18] S.J.Kim, S.J.Park and D.H.Won, "Proxy Signatures, revisited", Proc. of ICICS'97, LNCS 1334, pp.223-232, 1997

[19] 김희선, 백준상, 이병천, 김광조, "대리서명을 이용한 모발일 에이전트의 안전성 강화 방법", 한국정보보호학회, 종합 학술발표 논문집, Vol. 10, No. 1, pp. 424~437, 2000.

[20] Heyst, E. van and Pedersen, T. P. ,"How to make efficient fail-stop signatures", Eurocrypt'92, Vol. 658 of LNCS, pp366-377, 1993

[21] S.J.Kim, S.J.Park and D.H.Won, "Nomiative Signatures", Procee dings of the 1995 Symposium on Cryptography and Information Security(SCIS'95), pp.B1.1.1~17, 4~27, Jan, 1995

[22] M.Mambo, K.Usuda and E.Okamoto, "Proxy Signatures for delegating signing operation", Proc. Third ACM Conference on Computer and Communications Security, pp. 48~57, 1996

[23] 박희운, 이임영, "이동통신에서 적용 가능한 수신자 지정 대리서명 방식", 한국정보보호학회 논문지 제10권 2호, pp.43-54, 2000.6

감사의 글

어느새 2년이라는 대학원 생활이 지나고 졸업을 앞두고 있습니다. 처음부터 끝까지 이 논문을 무사히 마칠 수 있도록 곁에서 도움을 주신 모든 분들에게 정말 진심으로 감사드립니다.

먼저 부족하기만 한 저를 2년 동안 관심으로 지도해주시고, 학부시절보다 더 많이 배우고, 더 많이 공부하며 더 많은 노력의 필요성을 일깨워 주신 박지환 교수님께 깊은 감사드립니다. 그리고 심사를 맡아 주신 정순호 교수님, 조성진 교수님께도 감사의 말씀을 전합니다. 또한 저에게 학문의 필요성을 일깨워주시고, 늘 조언과 격려를 아끼지 않으시는 학부 교수님인 권순량 교수님과 손영선 교수님 그리고 최대우 교수님께 감사드립니다.

지금은 이 자리에 없지만 연구가 어려워 힘들 때나 힘든 시기에 고민을 같이 해주고 항상 물신양면으로 도움을 주셨던 최재귀 선배, 이혜란 선배, 임태훈 선배 그리고 이진홍 선배, 강현호 선배, 박영란 선배에게 감사드립니다. 또한 가족과도 같은 멀티미디어 보호 및 응용 연구실의 김문수 선생님, 임쌍학 선생님 외 모든 일반대학원, 교육대학원, 산업대학원의 선·후배 여러분께도 감사드리며, 컴퓨터 그래픽스 연구실의 이영숙 선배와 생활의 활력이 되어준 친구에게도 감사드립니다. 특히 이번 졸업논문에 있어서 가장 큰 도움과 격려를 주시고 지금도 많은 도움을 주고 있는 최재귀 선배께 다시 한번 감사의 마음을 전합니다.

끝으로 사랑하는 우리가족~ *^^*

가장 든든한 후원자이자 영원한 팬인 아버지(김세창)와 어머니(조정남). 언제나 자식들을 위해 희생하시고, 길을 열어주시는 두 분께 사랑한다는 말과 함께 이 논문을 받칩니다. 그리고 너무도 착한 저의 소중한 언니(김소은)와 힘든 공부를 묵묵히 해내고 있는 저의 동생(김민욱)에게도 이 논문을 받칩니다.