# 효율적 다중 라이센스 서비스를 제공하는 스트림 방식의 DRM 시스템에 관한 연구

김소진, 박지환
부경대학교 정보보호학과

# A Study on DRM System for Streaming Digital Contents with an Efficient Multi-License Service

So-Jin Kim, Ji-Hwan Park
Dept of Information Security, PuKyong University

요 약

일반적으로 스트림 방식의 DRM(Digital Rights Management) 시스템은 한번에 하나의 컨텐츠만을 구매할 수 있다. 그러므로 다중 디지털 컨텐츠의 구매 시에 매번의 인증, 지불, 라이센스 획득 단계가 필요하다. 게다가 구매한 모든 컨텐츠의 라이센스 키들의 안전한 저장 공간이 필요함으로 라이센스 키 관리의 어려움이 있다. 따라서 본 논문은 Atallah와 Li[1]의 스마트카드를 이용한 라이센스 키 관리 방식의 문제점을 지적하고, 스트림 방식의 DRM 시스템에서 다중 컨텐츠 구매를 위한 효율적인 다중 라이센스(multi-license) 서비스를 제안한다.

## 1. 서론

DRM(Digital Rights Management) 시스템은 다양한 채널을 통해 유통되는 각종 디지털 컨텐츠를 불법 복제로부터 안전하게 보호하고, 이러한 컨텐츠 서비스의 유료화를 가능하게 하는 기술이다. 일반적으로 DRM의 서비스 방식은 다음과 같이 구분된다.

- 스트림(stream) 방식
  영화, 교육, 게임, 음악 등 실시간 서비스가 가능한 디지털 컨텐츠를 사용자(customer)의 하드웨어에 저장할 수 없도록 하는 일회성의 방식이다.
- 다운로드(download)방식
  음악, 전자서적, 소프트웨어와 같은 계속적 사용이 가능한 컨텐츠를 다운로드하여 사용자의 하드웨어에 저장할 수 있는 방식이다.

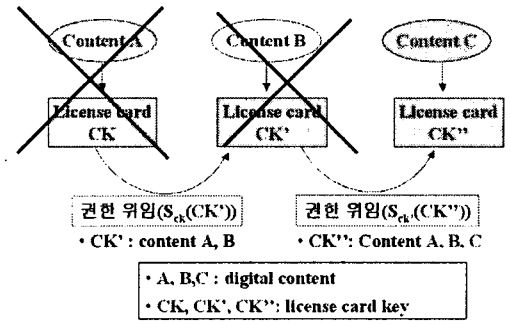
DRM 시스템에 등록된 디지털 컨텐츠는 대응하는 하나의 라이센스 키(license key)와 사용조건(usage rule)을 가진다. 그러나 일반적으로 사용자는 한번에 하나의 컨텐츠만을 구매할 수 있다. 특히 스트림 방식의 DRM 시스템은 디지털 컨텐츠의 다중구매 시에 각 컨텐츠에 대응하는 라이센스 키를 정당한 사용자에게 어떻게 전달할 것인가가 중요하다. 또한 구매한 모든 컨텐츠의 라이센스 키들의 안전한 저장 공간이 필요함으로 사용자의 라이센스 키 관리에 대한 문제점을 고려해야 한다. 게다가 무선 DRM 환경을 고려한다면, 더욱 사용자는 라이센스 획득과 라이센스 키 관리를 위한 작업량과 메모리 용량의 한계를 가질 것이다.

따라서 본 논문은 Atallah와 Li[1]의 스마트카드를 이용한 라이센스 키 관리 방식의 문제점을 지적하고, 스트림 방식의 DRM 시스템에서 다중 컨텐츠 구매를 위한 다중 라이센스(multi-license) 서비스를 제안한다. 제안 방식은 DPRL, XrML과 같은 권리 명세 언어의 사용 없이, Key Revocation 암호 기법[2]을 이용하여 각 컨텐츠의 라이센스를 제어할 수 있다.

## 2. 라이센스 키 관리의 기법[1,3]

사용자의 효율적 라이센스 키 관리를 위해서 스마트카드(smartcard)에 라이센스 키를 저장할 수 있는 방식이 Aura와 Gollmann에 의해 제안되었다[3].

이 기법은 각 컨텐츠마다 대응하는 두개의 인증서와 하나의 라이센스 카드 키(smartcard key)를 포함하는 라이센스 카드를 발행하고, 각 카드는 권한 위임 인증서를 기반으로 다른 카드에 자신의 라이센스 권한을 위임할 수 있다. 그러므로 사용자는 오직 하나의 라이센스 카드로 구매한 모든 라이센스 키들을 관리할 수 있다.




(그림1) 라이센스 카드 키 권한위임의 예

이후, Atallah와 Li는 이 방식을 개선하였다[1]. 기존 방식은 권한을 위임한 카드는 완전 폐기되어야 함으로 이를 보완한 부분위임과 확장성, 유연성을 가지도록 라이센스 정보 테이블(license information table)을 제안하였다. 각 카드에 포함된 라이센스 키 목록을 작성하여 이것을 사용자의 하드웨어에 저장하는 것이다.

<표1> $K_C$의 라이센스 정보 테이블

| License *ID* | License *Key* | Certificate |
|---|---|---|
| License 1 | $K_{L_1}, \{K_{L_1}, K_{L_1}^{-1}\}_{K_C}$ | $\{K_{L_1}, A\}_{K_{SP}^{-1}}$ |
| License 2 | $K_{L_2}, \{K_{L_2}, K_{L_2}^{-1}\}_{K_C}$ | $\{K_{L_2}, A\}_{K_{SP}^{-1}}$ |
| License 3 | $K_{L_3}, \{K_{L_3}, K_{L_3}^{-1}\}_{K_C}$ | $\{K_{L_3}, B\}_{K_{SP}^{-1}}$ |

- $K_C$ : license card key, $K_L$ : license key
- $K_{SP}$ : content Publisher key
- $K_C$ 라이센스 카드는 3개의 라이센스 권한를 가짐
  - A 컨텐츠: 2개의 라이센스 키 권한
  - B 컨텐츠: 1개의 라이센스 키 권한

Atallah와 Li의 방식은 스마트카드를 이용하여 라이센스 키를 관리할 수 있어 사용자에게 효율성을 제공한다. 하지만 라이센스 권한위임에 대한 위임 인증서 수가 증가하고, 부분 위임을 위하여 각 카드마다 라이센스 정보 테이블을 가져야함으로 사용자가 저장해야 하는 정보량이 증가한다. 그러므로 본 논문에서는 한번에 다중 컨텐츠 구매가 가능하며, Atallah와 Li의 문제점을 해결할 수 있는 다중 라이센스 서비스를 제공하는 DRM 시스템을 제안한다.

## 3. 다중 라이센스 키를 이용한 스트림 방식의 DRM 모델 제안

제안 방식은 스트림 방식의 DRM 시스템에서 컨텐츠 구매에 대한 사용자의 불편함과 라이센스 키 관리의 어려움을 고려하여 다중 라이센스 서비스가 가능한 DRM의 모델을 제시한다. 제안 DRM 센터는 신뢰센터로 가정하고, 시스템의 구성요소와 설정은 다음과 같다.

<표2> DRM 시스템의 구성요소

| DRM 센터(DRM) |
|---|
| • 회원등록 모듈 *(DRM_RM)*<br>- DRM 시스템의 초기화<br>- 구매자의 회원등록<br>• 다중 라이센스 키 서비스 모듈 *(DRM_KSM)*<br>- New 컨텐츠의 라이센스 등록 및 발행<br>- 다중 라이센스 키 관리<br>• 라이센스 키 제어 모듈 *(DRM_KCM)*<br>- 컨텐츠의 사용기간이 만료된 라이센스 키 관리 |
| **스트리밍 서비스 제공자(SCP)** |
| - 암호화된 컨텐츠의 스트리밍 서비스 |
| **컨텐츠 제공자(CP)** |
| - Content Publisher or Original Ownership<br>- Packaging of Original Content: 컨텐츠 암호화 |
| **구매자(U)** |
| - DRM 시스템에서 디지털 컨텐츠를 구매 |

<표3> 매개 변수와 시스템 설정

| | |
|---|---|
| $p$ | · 512비트 이상의 큰 소수, 공개 |
| $q$ | · $q \mid p-1$인 큰 소수, 공개 |
| $Z_p^*$ | · *modulo* $p$인 정수의 곱셈군 |
| $g$ | · 위수가 $q$인 $Z_p^*$상의 생성자 |
| $h()$ | · 일방향 해쉬함수 |
| $E()$ | · 대칭키 암호 알고리즘 |
| $E'()$ | · 공개키 암호 알고리즘 |
| $Sig()$ | · 서명 알고리즘 |
| $C_i$ | · 스트림형 디지털 컨텐츠 $i$ |
| $s_i$ | · $C_i$의 세션키 |

| | |
|---|---|
| $ID_{U_k}$ | · 사용자 $U_k$의 $ID$ |
| $DRM_{U_k}$ | · 사용자 $U_k$의 비밀 회원정보 $(k, f(k))$ |
| $x_{DRM}, y_{DRM}$ | · DRM 센터의 비밀키, 공개키 $x_{DRM} \in Z_q^*$, $y_{DRM} \equiv g^{x_{DRM}} (\mathrm{mod}\ p)$ |
| $x_{CP}, y_{CP}$ | · 컨텐츠 제공자의 비밀키, 공개키 $x_{CP} \in Z_q^*$, $y_{CP} \equiv g^{x_{CP}} (\mathrm{mod}\ p)$ |
| $x_{SCP}, y_{SCP}$ | · 스트리밍 서비스 제공자의 비밀키, 공개키 $x_{SCP} \in Z_q^*$, $y_{SCP} \equiv g^{x_{SCP}} (\mathrm{mod}\ p)$ |
| $x_{U_k}, y_{U_k}$ | · 구매자 $U_k$의 비밀키, 공개키 $k \in \{1, 2, \ldots, n\}$ $x_k \in Z_q^*$, $y_k \equiv g^{x_k} (\mathrm{mod}\ p)$ |

### 가. 시스템의 초기화

$DRM_RM$은 DRM 전체 시스템을 초기화한다.

- 차수가 $Z$인 비밀 다항식을 만든다.

$f(x) \in Z_q^*$, $f(x) = a_0 + a_1 x + \cdots + a_z x^z$

- $f(x)$에 대한 $z$개의 인덱스 값 $(a_1, f(a_1)), (a_2, f(a_2)), \cdots, (a_z, f(a_z))$을 선택하고, 대응하는 $z$개의 $g^{f(a_i)}$값을 계산한다.
- 다음의 값들은 시스템의 공개값으로 공개한다.

$\langle g, g^{a_0}, (a_1, g^{f(a_1)}), (a_2, g^{f(a_2)}) \cdots (a_z, g^{f(a_z)}) \rangle$

### 나. 등록

#### (a) DRM 서비스 등록 – DRM 관리

① 사용자의 회원등록

- 사용자 $U_k$가 DRM 시스템의 가입을 요청한다.
- $DRM_RM$은 $U_k$의 가입정보 $ID_{U_k}$를 저장하고, DRM 시스템 사용을 위한 비밀값 $DRM_{U_K} = (k, f(k))$를 선택하여 $U_k$에게 다음과 같은 회원증(smartcard)을 발행한다.

$DRM\_Card = \{ ID_{U_k}, DRM_{U_k}, Sig_{x_{DRM}}(ID_{U_k}, DRM_{U_k}) \}$

$k \in Z_q^*$는 이미 등록된 사용자들에게 제공되지 않은 값이다.

② 컨텐츠 제공자의 라이센스 등록

- 컨텐츠 제공자 $CP_k$는 $\langle E_{y_{DRM}}(s_i) \rangle$을 전송하여 new 컨텐츠 $C_i$에 대한 세션키 정보값 $s_i$의 등록을 요청한다.
- $DRM_KSM$은 $C_i$의 다중 라이센스 서비스를 위한 $ML_{U_k}$의 생성정보 $l_i$를 선택하고, $s_i$와 함께 $l_i$를 비밀DB에 저장한다.

$l_i \in Z_q^*$, $l_{i-1} \neq l_i \neq l_{i+1}$, $i = C_i$의 인덱스

〈표4〉 라이센스 비밀정보 Table

| | 컨텐츠 $C_i$의 라이센스 정보 (비밀) | | | |
|---|---|---|---|---|
| $index = i$ | 1 | 2 | 3 | ··· |
| $s_i$ | $s_1$ | $s_2$ | $s_3$ | ··· |
| $l_i \in Z_q^*$ | $l_1$ | $l_2$ | $l_3$ | ··· |
| $r_i \in Z_q^*$ | $r_1$ | $r_2$ | $r_3$ | ··· |

#### (b) Streaming 서비스 등록 – SCP 관리

① 컨텐츠 제공자의 스트리밍 서비스 등록

- $CP_k$는 암호화된 컨텐츠 $\langle i, h(i \| C_i), E_{s_i}(C_i) \rangle$를 스트리밍 서비스 제공자 SCP에게 등록한다.

② DRM의 스트리밍 서비스 등록

- $DRM_KSM$도 등록된 컨텐츠의 스트림 서비스를 위해 $\langle i, h(i \| ST_i), ST_i \rangle$을 계산하여 SCP에게 등록한다.

$ST_i = ST_{i_1} \| ST_{i_2} \| ST_{i_3}$

$ST_{i_1} = s_i g^{r_i a_0}$, $r_i \in Z_q^*$, $r_{i-1} \neq r_i \neq r_{i+1}$

$ST_{i_2} = l_i g^{r_i}$

$ST_{i_3} = (a_1, g^{r_i f(a_1)}), (a_2, g^{r_i f(a_2)}) \cdots (a_z, g^{r_i f(a_z)})$

### 다. 다중 라이센스 서비스

- 사용자 $U_k$는 $\langle m_1, h(m_1 \| m_2 \| ID_{U_k}), E_{y_{DRM}}(ID_{U_k} \| m_2) \rangle$로 DRM에게 다중 구매를 요청한다.

$m_1$ = 구매 컨텐츠의 목록 || 각 컨텐츠의 사용기간

$m_2 = U_k$의 지불정보

- $DRM_KSM$은 $ID_{U_k}$를 인증하여 요청한 컨텐츠 그룹에 대한 다중 라이센스 정보 $MK_{U_k}$를 생성하고, 이에 대응하는 분리값 $LD_{U_k}$ 그룹도 계산하여 $U_k$에게 $\langle MK_{U_k}, LD_{U_k} \rangle$을 전송한

다.

$\langle MK_{U_k} = (\Pi(l_i))^{f(k)},\ LD_{U_k} = \{LD_{U_k(i)}\}\rangle$

$\Pi(l_i)$= 구매한 컨텐츠 그룹의 모든 생성정보의 곱

$LD_{U_k}$ = {구매한 컨텐츠 수와 동일한 분리값 그룹}

$LD_{U_k(i)} = (\Pi(l_{i제외}))^{f(k)}$

$\Pi(l_{i제외})$= 구매한 컨텐츠 그룹 중 복호하려는 하나의 컨텐츠 $C_i$의 생성정보를 제외한 나머지 생성정보들의 곱

- 사용기간 정보 $m_2$는 $DRM_KCM$가 관리한다.

**라. 디지털 컨텐츠의 스트리밍 서비스**

- SCP는 $CP_k$와 $DRM$의 등록정보 값으로 $CP_k$의 $C_i$ 요구사항에 맞게 스트리밍 서비스 $\langle ST_i, E_{s_i}(C_i)\rangle$를 수행한다.

**마. 스트림 방식의 디지털 컨텐츠 복호**

- 사용자 $U_k$는 $\langle ST_i, E_{s_i}(C_i)\rangle$를 수신하면, 먼저 $DRM_{U_k}$, $MK_{U_k}$와 복호하려는 $C_i$에 대응하는 분리값 $LD_{U_k(i)}$를 이용하여 $ST_i$에서 $s_i$를 계산하고, $s_i$를 이용하여 컨텐츠 $C_i$를 복호한다.

$$s_i = \frac{ST_{i_1}}{ST_{i_2}^{f(k)\lambda} \cdot ST_{i_3}^{\lambda_i} \cdot LD_{U_k(i)}^{\lambda}} \cdot MK_{U_k}^{\lambda}$$

$$= \frac{s_i g^{r_i a_0} \cdot (\Pi(l_i))^{f(k)\lambda}}{(l_i g^{r_i})^{f(k)\lambda} \cdot \Pi_{t=0}^{z-1}(g^{r_i f(a_t)\lambda_i}) \cdot LD_{U_k(i)}^{\lambda}}$$

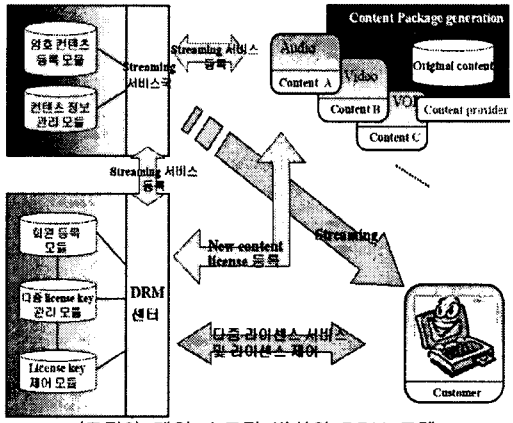
이때, $\lambda$는 Lagrange 계수이다.

**바. 각 컨텐츠의 라이센스 키 제어**

- $DRM_KCM$은 컨텐츠 $C_i$의 계약기간이 만료된 사용자 $c$명의 $DRM_{U_k}$값으로 $C_i$의 인덱스를 만들고, $z-c$개의 사용되지 않은 나머지 인덱스를 만든 $\langle i, h(ST_{i_3}), E_{y_{SCP}}(ST_{i_3})\rangle$을 SPC에게 갱신하도록 알린다.

$$ST_{i_3} = \langle (k_1, g^{r_1 f(k_1)}), \cdots (k_c, g^{r_1 f(k_c)}), (a_1, g^{r_1 f(a_1)}), \cdots, (a_{z-c}, g^{r_1 f(a_{z-c})})\rangle$$

- 갱신된 값으로 $C_i$의 스트리밍 서비스 시, 계약기간이 만료된 사용자들은 세션키 $s_i$를 획득할 수 없게 된다.




(그림2) 제안 스트림 방식의 DRM 모델

## 4. 제안 방식의 안전성 및 특성 분석

▸ **안전성 분석**

제안 방식의 안전성은 Diffie-Hellman 문제의 어려움에 기반한다.

**[정리1]** 회원정보 $DRM_{U_k}$은 DRM 센터만이 생성할 수 있다.

- $DRM_{U_k}$은 $f(x)$의 인덱스 값 $(k, f(k))$으로 $Z$명 이하의 사용자들이 공모하여 다른 사용자의 $DRM_{U_k}$를 알아낼 확률은 무시할 수 있다[4].

**[정리2]** 다중 라이센스 정보 $MK_{U_k}$는 DRM 센터만이 생성할 수 있다.

- $MK_{U_k}$는 Diffie-Hellman 문제의 어려움에 기반하여 $(\Pi(l_i))^{f(k)}$에서 생성정보 $\Pi(l_i)$을 계산할 수 없고, $ST_{i_2} = l_i g^{r_i}$에서 이산대수 문제의 어려움으로 $r_i$을 계산할 수 없으므로 $l_i$를 구할 수 없다. 또한 정당한 사용자들이 공모하여 구매하지 않은 컨텐츠 $C_i$의 라이센스를 획득하는 것은 불가능하다. 각 사용자의 $MK_{U_k}$, $LD_{U_k}$는 구매하지 않은 컨텐츠의 $l_i$을 포함하지 않고, $r_i$의 값도 계산할 수 없으므로 세션키 $s_i$를 획득할 수 없다.

**[정리3]** 스트리밍 서비스 제공자는 부정할 수 없다.

- 컨텐츠 제공자는 암호화된 컨텐츠 $E_{s_i}(C_i)$를 등록하기 때문에 대응하는 세션키 $s_i$를 알아야만 복호할 수 있다. 하지만 $DRM_{U_k}$, $MK_{U_k}$,

$LD_{U_k}$없이는 불가능하다. 그리고 각 컨텐츠의 라이센스 제어를 위해 $ST_i$ 값을 갱신하지 않으면 스트리밍 서비스 제공자의 부정행위로 간주됨으로 $ST_i$ 갱신 요청 시, 갱신해야 한다.

그러므로 [정리1~3]에 의해서 제안 방식의 컨텐츠 $C_i$의 사용은 $DRM_{U_k}$와 $MK_{U_k}$, $LD_{U_k}$를 가진 정당한 사용자 $U_k$만이 가능하다.

▸ **제안 방식의 특성**

① 다중 라이센스 서비스 제공

- 제안 스트림 방식의 DRM 시스템은 동시에 다중 컨텐츠 구매가 가능하도록 다중 라이센스 서비스를 제공한다. 이때, 사용자의 중요한 정보값인 $DRM_{U_k}$와 $ID_{U_k}$는 스마트카드에 저장하기 때문에 다중 라이센스 정보인 $MK_{U_k}$, $LD_{U_k}$은 공개되어도 안전하다. 그리하여 Atallah와 Li의 방식의 문제점인 위임 인증서와 라이센스 정보 테이블 저장을 위한 메모량의 증가를 해결할 수 있다. 그리고 무선 DRM 사용자 단말기의 효율성을 위해 적용 가능하다.

② 라이센스 키 제어성

- 권리명세 언어인 DPRL, XrML 등을 사용하지 않고, Key Revocation 암호 기법[2]으로 계약이 만료된 컨텐츠 $C_i$의 라이센스 키 사용을 제어할 수 있다. DRM 센터는 $ST_{i_3}$만을 갱신하여 스트리밍 서비스 제공자에게 알려주면 된다.

## 5. 결론

일반적으로 DRM 시스템은 다운로드 방식과 스트리밍 방식으로 구분된다. 하지만, 스트림 방식은 라이센스 키 관리 문제로 다중 구매가 어렵다. 따라서 본 논문에서는 한번에 다중 구매가 가능하고, Atallah와 Li의 문제점을 해결할 수 있는 다중 컨텐츠 구매를 위한 DRM 시스템의 모델을 제안하였다. 제안 방식은 사용자의 편의성과 효율성을 제공함으로 무선 DRM 시스템에도 적용 가능하다.

## 참고문헌

[1] Mikhanil J. Atallah and Jiangtao Li, "Enhanced Smart-card based License Management", Proceeding of the IEEE Conference on E-Commerce 2003, p.111

[2] Kaoru Kurosawa and Yvo Desmedt, " Optimum Traitor Tracing and Asymmetric Schemes", Journal of Eurocrypt 1998, Lecture Notes in Computer Science, 1403, p.145-157

[3] Tuomas Aura and Dieter Gollmann, "Software license management with smart cards", the USENIX Workshop on Smartcard Technology 1999

[4] A.Narayanan, "Practical Pay TV schemes", Proceeding of ACISP 2003, p.192-203