DRM에서 키 관리 기술에 관한 연구

양성훈*, 한대열, 김성훈, 박익수, 이경효, 정석원, 서재현, 김종화, 오병균
*목포대학교 정보공학부

e-mail: {bbs510d, dyh, seilpart, upark, mediakh, jsw, jhseo, kimjh, obk}@mokpo.ac.kr

A Study on Key Management Technology for DRM

*Seong-Hoon Yang, Dea-yul Han, Seong-Hoon kim, Ik-Su Park, Kyoung Hyo Lee, Seok Won Jung, Jae Hyun Seo, Jong-Hwa Kim, Byeong-Kyun Oh

*Division of Information Engineering, MokPo National University

요 약

DRM에서 키 관리 기술은 중앙 집중 키 관리 방식, Enveloping 방식 등이 있다. 본 논문에서는 암호화 키를 콘텐츠에 함께 동봉하는 키 관리 방식을 기반으로 새로운 DRM 키 관리 기술을 제안한다. 제안하는 키 관리 기술은 사용자 인증에서 사용된 인증정보를 콘텐츠 암호화 키로 사용함으로 콘텐츠 암호화 키를 암호화하여 전송할 필요가 없는 장점이 있다.

1. 서론

DRM은 디지털 형태로 제작된 콘텐츠에 대한 권리를 안전하게 보호하고 관리하기 위한 기술적인 메커니즘으로 허가되지 않은 사용자로부터 디지털 콘텐츠의 접근을 통제하기 위하여 암호기술을 기본으로 키의 배포 및 관리를 해야한다.

DRM에서 키 관리 기술은 중앙 집중 키 관리 방식과 암호화 키를 콘텐츠와 함께 동봉(Enveloping)하는 키 관리 방식 등이 있다[2-4].

중앙 집중 키 관리 방식은 콘텐츠를 암호화할 때 사용하였던 비밀키를 중앙 인증서버에 보관하였다가 사용자가 콘텐츠를 사용하고자 라이센스 요구 시 인증서버에 보관된 비밀키를 전송하여 암호화된 콘텐츠를 복호화하여 사용하도록 한다. 이 방식은 비밀키가 인증서버에서 관리됨으로 키 전송 과정에서 보안 취약성, 키 관리 서버의 보안성 강화, 대규모 데이터의 백업 및 유지보수 관리 부담 등의 단점이 있다[2-4]. 동봉(Enveloping) 키 관리 방식은 콘텐츠를 암호화할 때 사용했던 암호화 키를 콘텐츠와 함께 동봉(enveloping)해서 관리하는 방식으로 동봉되는 암호화 키는 배포되는 패키징된 콘텐츠에 포함되어 관리되므로 키 관리 부담을 최소화할 수 있다[1-3].

본 논문에서는 암호화 키를 콘텐츠에 함께 동봉하는 키 관리 방식을 기반으로 새로운 DRM 키 관리 기술을 제안한다. 논문의 구성은 2장에서는 DRM 키 관리 기술을 소개하고, 3장에서는 새로운 DRM 키 관리 기술을 제안한다.

2. DRM 키 관리 기술

DRM에서 허가되지 않은 사용자로부터 콘텐츠의 접근을 통제하기 위하여 암호화된 콘텐츠를 복호화할 수 있는 비밀키의 전송은 중요하다. 이때 콘텐츠를 암호화하는 비밀키는 콘텐츠의 비밀성을 유지하기 위해서 매우 안전하게 관리되고 전송되지 않으면 안 된다. DRM에서 키 관리 기술은 콘텐츠 암호화 키 관리에 따라 중앙 집중 키 관리 방식과 동봉(Enveloping) 키 관리 방식으로 구별될 수 있다[1-3]. 본 장에서는 기존에 사용되고 있는 DRM 키 관리 기술에 대하여 논의한다.

「본 논문은 2004 년도 지역IT협동연구센터 디지털 콘텐츠 저작권 관리기술 연구비 지원에 의하여 연구되었음」

2.1 중앙 집중 키 관리 방식[3]

콘텐츠 제공업자와 라이센스 인증 서버가 공개키를 교환 후 콘텐츠 제공업자는 랜덤하게 생성된 비밀키를 이용하여 콘텐츠를 암호화하고, 라이센스 인증서버 공개키를 이용하여 비밀키를 암호화하여 라이센스 인증서버에 전송하면, 라이센스 인증서버는 비밀키를 보관한다. 암호화된 콘텐츠는 패키징되어 사용자에게 배포된다. 콘텐츠 사용자가 라이센스 인증서버에 사용료 지불 라이센스를 요청하면, 비밀키 정보가 포함된 라이센스를 이용하여 콘텐츠를 복호화한다. 이 방식은 콘텐츠를 암호화 할 때 사용했던 비밀키를 중앙 집중 관리함으로써 키 등록을 위한 전송상의 보안 취약성과 키 관리 서버의 보안성 강화, 그리고 대규모 데이터의 백업 및 유지보수 관리 부담 등의 문제점들을 안고 있다. 그림 1은 중앙 집중 키 관리 방식을 설명하고 있다.

- C : Content
- E : Encryption
- sk : Security Key
- ch_pub_k : Public key of CH
- p_prv_k : Private key of Packager
- H : Hash function
- uk : User key
- L : License

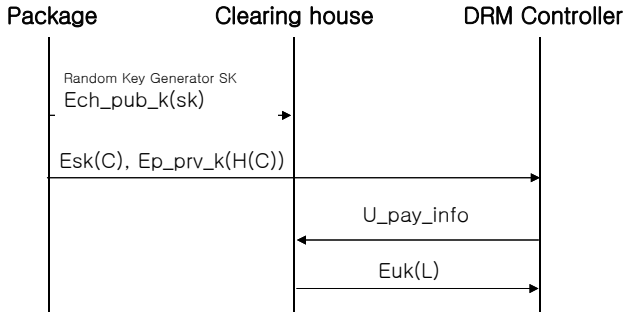

그림 1 중앙 집중 키 관리 방식

2.2 Cyptolop 키 관리방식[3]

콘텐츠 제공업자와 라이센스 인증 서버가 공개키를 교환후 랜덤하게 생성된 비밀키를 이용하여 콘텐츠를 암호화하고, 비밀키를 라이센스 인증서버의 마스터 키로 암호화해서 Cyptolop에 동봉되어 패키징한다. 사용자는 구입하고자하는 콘텐츠의 구매정보와 비밀키를 라이센스 인증서버에 전송하면 라이센스 인증 서버는 동봉되어 전송된 비밀키를 라이센스 인증서버의 개인키를 이용하여 복호화한다. 복호화된 비밀키는 사용자의 공개키로 암호화되어 라이센스 Crytolope에 포함되어 사용자에게 전송한다. 사용자는 전송된 라이센스 Crytolope의 비밀키를 자신의 개인키로 복호화하고, 복호화된 비밀키를 이용하여 콘텐츠를 복호화한다. 이 방식은 콘텐츠 복호화 키가 배포된 Crytolope에 포함되어 관리되므로 라이센스 인증서버의 키 관리 부담이 상당히 감소되는 장점이 있다. 그림 2은 Cryptolope 키 관리 방식을 설명하고 있다.

- C : Content
- E : Encryption
- sk : Security Key
- m_k : Public master key_RCC
- u_k : Public key_User
- P : Package Cryptolope
- L : License Cryptolope
- B_i : buy_information Content

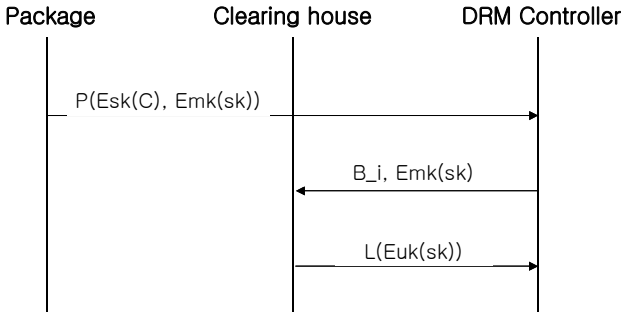

그림 2 Cryptolope 키 관리 방식

2.3 WMRM [3]

콘텐츠 제공업자는 콘텐츠의 암호화를 라이센스 인증서버와 콘텐츠 패키저의 공유키 License Key Seed와 콘텐츠 패키저별로 생성되는 Key ID의 조합으로 생성된 비밀키를 이용하고, 암호화된 콘텐츠와 Key ID 정보를 콘텐츠 파일과 함께 패키징한다. 콘텐츠 사용자가 라이센스 요청시 라이센스 인증서버는 사용자로부터 전송된 헤더 정보 중에서 Key ID 정보를 추출하고, 이를 다시 라이센스 인증서버의 License Key Seed를 조합하여 Key를 생성하여 콘텐츠 사용자에게 전송한다. 이 방식은 콘텐츠를 암호화할 때 사용되었던 비밀키의 정보를 라이센스 인증서버에 전송할 필요가 없기 때문에 키 전송 과정에서 발생할 수 있는 보안상의 위험을 피할 수 있으며, 콘텐츠 별 비밀키를 관리하는 큰 부담을 덜 수 있게 된다[3]. 그림 3은 WMRM 키 관리 방식을

설명하고 있다.

- C : Content
- E : Encryption
- sk : Security Key
- License key seed : Public Package_License Service Provider
- key_id : Content Package
- P : Package
- U_head : Head info of User
- L : License

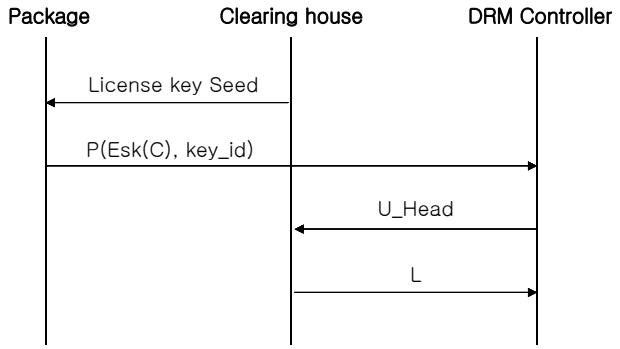

그림 3 WMRM 동봉 키 관리방식

2.4 인증 및 키 분배 프로토콜

DRM에서 콘텐츠 보호를 위해 사용되는 암호기술들의 안전성을 보장하기 위해 안전한 키 관리가 중요하다. 암호 메커니즘에서 보면 라이센스가 전달되는 과정에서 사용자 인증 및 키 분배가 발생하게 되며, 대칭키 방식과 공개키 방식, 사전 키 분배 방식이 사용될 수 있다. 대칭키 방식은 하나의 키 분배 서버로 모든 부하가 집중되고 모든 콘텐츠 거래에 키 분배 서버가 관여하는 단점이 있다. 공개키 방식을 사용할 경우 분산성, 확장성, 상호운용성 등의 장점을 갖게 되나 암호화 키 관리, 암호화 키 도난 방지를 위하여 엄격한 키 관리 정책 및 기술이 필요하다. 사전 키 분배 방식은 키 분배 부담을 덜어낼 수 있어 효율성, 융통성에 큰 장점을 갖게 되나 안전성 측면에서 사전에 분배된 키에 대한 보호 문제가 있다.

3. 새로운 DRM 키 관리 기술

본 장에서는 암호화 키를 콘텐츠에 함께 동봉하는 키 관리 기술을 기반으로 콘텐츠를 암호화할 때 사용하는 비밀키를 [1]에서 제안된 PAP 인증 프로토콜 스킴의 인증 정보를 사용하여 새로운 DRM 키 관리 기술을 제안한다.

3.1 콘텐츠 암호화 키

이 절에서는 콘텐츠 암호화 키로 사용될 비밀키의 설명을 위해 [1]을 소개한다. PAP는 인증 스킴이며, PAPRSA는 공개키 알고리즘 RSA방식을 이용하여 PAP 인증 스킴을 적용한 패스워드 기반 인증 프로토콜이다. PAP 인증 스킴은 등록프로시저와 인증 프로시저로 구성되며, [1]을 참고하기 바란다.

PAPRSA는 PAP 인증 스킴을 공개키 암호 알고리즘 RSA를 이용한 인증 프로토콜로서 인증프로토콜 수행시 도출되는 $(x_1 - x_2)^2 \bmod N$, $(y_1 - y_2)^2 \bmod N$을 본 논문에서 제안하는 콘텐츠 관리 기술에서 콘텐츠 암호화 키로 이용한다.

[등록 프로시저]

Input: id, P.

① Get $N=pq$ and (e, d);

② Publish e and N;

③ Choose y_1 in random and then determine y_2 so that $y_1-y_2=P$;

④ Get $y_1^2 \bmod N$, $y_2^2 \bmod N$ and then store them at id.

[인증 프로시저]

Input: id, p′

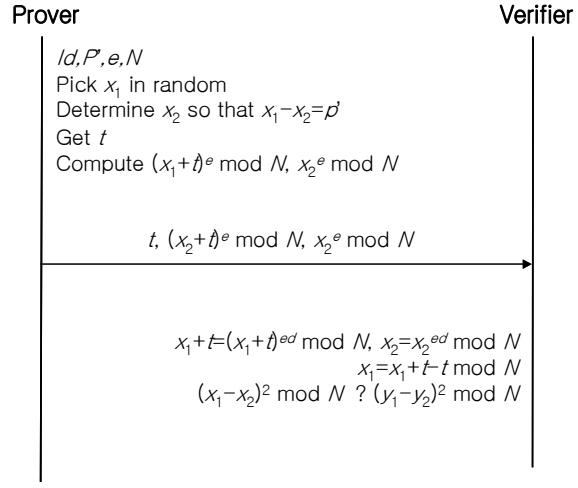

그림 4. 인증 프로토콜[4]

Verifier에는 (e, d), (p, q), N, $y_1^2 \bmod N$, $y_2^2 \bmod N$이 저장되어 있다. 위 그림과 같이 도출된 $(x_1 - x_2)^2 \bmod N$, $(y_1 - y_2)^2 \bmod N$을 비교하여 시스템 접근자가 인가된 사용자인지를 최종확인이 되므로 $(x_1 - x_2)^2 \bmod N$을 콘텐츠를 암호화하는

비밀키로 사용하고자 한다.

3.3 새로운 DRM 키 관리 기술 제안

이 절에서는 PAPRSA 인증 프로토콜에서 인증정보인 $(x_1 - x_2)^2 \bmod N$과 $(y_1 - y_2)^2 \bmod N$을 비밀키로 이용하여 콘텐츠를 암호화하는 새로운 DRM 키 관리 기술을 제안한다.

① 콘텐츠 제공업자는 라이센스 인증서버와 사용자 인증을 한다.

② 인증이 확인되면 인증정보를 비밀키로 하여 콘텐츠를 암호화하고, 암호화된 콘텐츠를 패키징한다.

③ 콘텐츠 사용자가 콘텐츠 암호화 키를 이용하여 라이센스를 요청한다.

④ 라이센스 인증서버는 콘텐츠 사용자가 전송한 콘텐츠 암호화 키와 저장하고 있는 인증정보를 확인하여 라이센스를 발급한다.

- C : Content
- E : Encryption
- sk : $(x_1 - x_2)^2 \bmod N$
- P : Package
- L : License

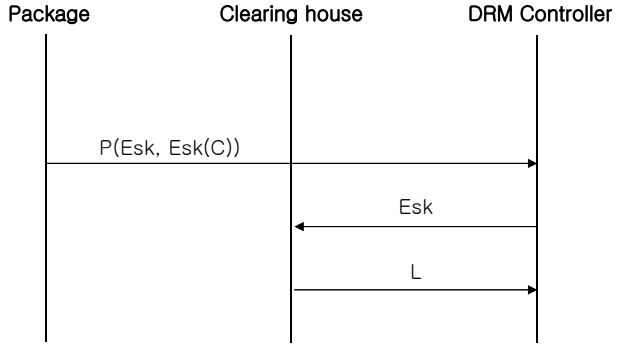

그림 5 제안된 DRM 키 관리방식

제안된 방식은 콘텐츠 암호화 키를 패키저와 라이센스 인증서버의 인증정보를 이용하므로 콘텐츠 사용자가 라이센스 인증서버에 패키저에서 전송받은 인증정보를 전송하면 라이센스 인증서버에서는 저장되어있는 인증정보와 비교하여 같으면 사용자에게 라이센스를 발급한다.

기존에 사용되고 있는 중앙 집중 키 관리 방식과 비교하여 패키저에서 비밀키를 라이센스 인증서버의 공개키로 암호화하여 전송할 필요가 없고, Cyptolop 키 관리 방식과 비교하여 패키저에서 콘텐츠 암호화 키와 암호화된 콘텐츠를 동봉하여 전송시 콘텐츠 암호화 키를 라이센스 인증서버 마스터 키로 암호화할 필요가 없다. 그러나 제안된 방식은 콘텐츠 사용자가 라이센스 인증서버에 라이센스 요구시 비밀키를 전송해야 함으로 비밀키의 관리가 매우 중요시된다. 특히 신뢰할 수 없는 네트워크에서는 비밀키의 노출을 고려 해야 된다.

3.4 비교분석

표 1 기존의 DRM 시스템과 비교[5]

	암호화된 콘텐츠구성	암호화 키관리	복호화키관리
Microsoft	암호화+메타정보	서버+암호화된 콘텐츠파일내속성	라이센스내 포함
Adobe	암호화+라이센스	서버	라이센스내 포함
ContentGuard	암호화+라이센스	별도파일	라이센스내 포함
Present	암호화+인증정보	서버+암호화된 콘텐츠파일내속성	라이센스내 포함

[표 1]은 제안된 DRM 시스템과 기존의 DRM 시스템과의 비교를 하였다.

4. 결론

DRM은 디지털 형태로 제작된 콘텐츠에 대한 권리를 안전하게 보호하고 관리하기 위한 기술적인 메커니즘이다.

본 논문에서는 암호화 키를 콘텐츠에 함께 동봉하는 키 관리방식을 기반으로 새로운 DRM 키 관리 기술을 제안하였다. 제안된 키 관리 기술은 [1]의 사용자 인증에서 사용된 인증정보를 콘텐츠 암호화 키로 사용함으로 패키저와 라이센스 인증서버에서 암호화횟수를 줄일 수 있었다. 향후에는 제안된 키 관리기술을 이용하여 DRM 설계 및 구현이 필요하다.

참고문헌

[1] IkSu P, SeungBae P, ByeonKyun O, "User Authentication Protocol Based on Human Memorable Password and Using RSA", Computational Science and Its Applications-ICCSA 2004, LNCS Vo1.3043, Springr-Verlag, pp.527-536

[2] Joshua. D, Susan. K, "Understanding Drm System : An IDC White Paper", IDC, 2001

[3] 한국정보처리학회, "DRM 최신 국제표준 기술사양 분석 및 세계 유명제품과 전망에 관한 연구", 한국소프트웨어진흥원, 2004

[4] Joshua, D, "Digital Rights Management : A Definition", IDC, 2001