3

DRM(Digital Rights Management) 기술

성균관대학교 ▌최동현 · 이병희 · 김승주* · 원동호*

1. 서 론

최근 디지털 기술의 발전으로 인해 콘텐츠 제작자들은 텍스트, 오디오, 비디오, 등의 콘텐츠를 고품질의 디지털 형태로 제작할 수 있게 되었다. 또한 인터넷의 확산과 통신 기술의 발전은 컴퓨터간의 상호 연결성을 증대시켰고, 이로 인해 디지털 콘텐츠를 쉽게 전파 할 수 있게 되었다. 이러한 디지털 콘텐츠에 대한 유통 환경의 변화에 따라 디지털 음악, 이미지, 영상물, 출판물 등 디지털 콘텐츠에 대한 수요가 급격히 증가하고 있다. 그러나 디지털 콘텐츠는 그 특성상 원본과 복사본의 품질이 동일하고, 콘텐츠에 대한 수정이나 복사가 간편할 뿐만 아니라 인터넷을 통해 전 세계 어디라도 짧은 시간 내에 전파될 수 있다. 이러한 특징은 디지털 콘텐츠에 대한 손쉬운 접근과 배포를 가능하게 하여 디지털 콘텐츠 시장 활성화와 같은 순기능을 제공하기도 하지만, 다른 한편으로는 무분별한 불법복제의 원인이 되기도 한다. 이러한 불법복제로 인해 콘텐츠 저작권자는 디지털 콘텐츠 유통에 부정적인 입장을 보이고 있는데 실제로 아직 개봉되지 않은 영화가 P2P를 통해 배포되거나 판매중인 음반이 mp3파일로 배포되는 경우가 빈번히 발생하고 있다.

디지털 콘텐츠의 불법복제에 따른 문제를 해결하고, 저작권자의 권리를 보호하기 위해서 제안된 기술이 DRM이다. 이는 콘텐츠의 불법복제를 방지하고 지정된 사용자에게 허가된 범위 내에서 콘텐츠를 사용하게 하여 디지털 콘텐츠의 안전하고 투명한 유통을 가능하게 하는 기술이다. 현재 DRM기술은 인터넷 방송, 모바일 기기, UCC 서비스, 문서보안 등 이미 다양한 분야에서 활용되고 있다.

본고에서는 이러한 DRM의 핵심기술에 대해 알아보고, DRM 시스템을 분석, 설명 하고자 한다.

2. DRM 핵심 기술 요소

2.1 사용 규칙 제어기술

사용자의 구매형태에 따라 콘텐츠의 사용 횟수와 사용기간, 콘텐츠 재배포, 수정 등을 제어하기 위해 다음과 같은 기술을 필요로 한다.

2.1.1 콘텐츠 식별체계(Identification)

공공기관에서는 각 문서마다 고유의 식별 번호를 할당하고, 도서에는 국제적 주민등록번호라 할 수 있는 ISBN(International Standard Book Number)을 할당하여 식별 및 관리를 용이하게 하고 있다. 이와 같이 디지털 콘텐츠의 체계적인 관리 및 통제, 접근, 이용 효율성을 위해 콘텐츠를 식별할 수 있는 체계 및 변환 시스템을 필요로 한다. 대표적인 식별 체계로는 DOI (Digital Object Identifier)가 있으며, prefix와 suffix 구조로 구성되어 ISBN과 같은 기존의 아날로그 식별체계를 수용한다는 장점을 가지고 있다. DOI 시스템에서 콘텐츠의 관리자는 RA(Registration Agency) 시스템을 통해 DOI 데이터와 메타 데이터를 등록한다. RA 시스템을 통해 등록된 DOI 식별번호와 URL 정보는 DOI 시스템에 저장 관리되며, 콘텐츠 사용자는 DOI에 대한 URL 정보 변환 요청을 통해 실제 콘텐츠의 접근정보를 얻어서 콘텐츠를 이용할 수 있게 된다[8].

2.1.2 메타 데이터(Meta-data)

콘텐츠가 식별된 후, 저작권자 정보, 출판 날짜, 출판 장소, 콘텐츠 식별번호, 콘텐츠 제목 등과 같이 콘텐츠에 대한 요약정보를 나타내는 메타데이터를 필요로 한다[1]. 현재 DRM에서는 표준화되지 않은 다양한 메타 데이터의 사용으로 인해 발생하는 시간 및 비용의 비효율성을 해결하기 위해 표준화의 필요성이 대두되고 있다. 유럽을 중심으로 지적재산권을 위한 데이터 모델 개발, 지적재산권 자체 및 상거래에 참여하는 사람, 업무를 서술하고 식별할 수 있는 정형적 구조의 표준화 작업으로 INDECS(Interoperability of Data in ECommerce Systems)가 대표적인 예이다[3].

2.1.3 권리표현기술(Right Expression)

권리표현기술은 콘텐츠에 대한 권리 규칙을 설정하

* 종신회원

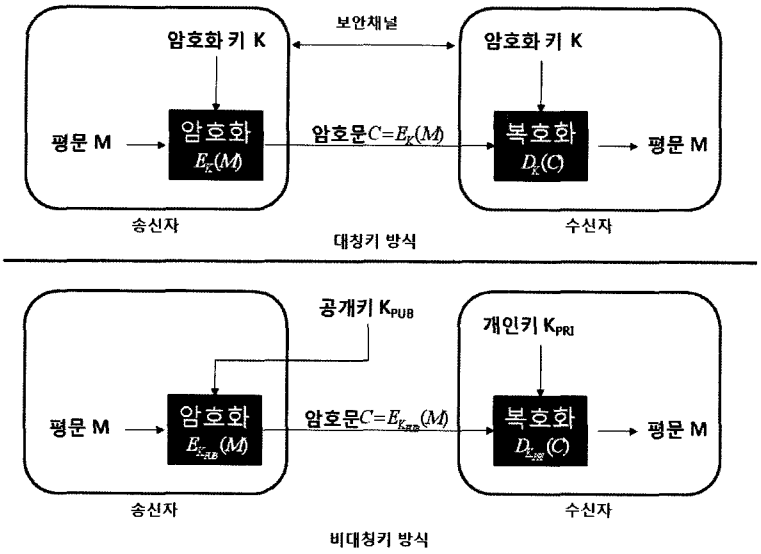

그림 1 암호화 및 복호화 과정

는 것을 의미하는 것으로 어느 사용자가 어떠한 권한과 어떠한 조건으로 콘텐츠를 이용할 수 있는지를 나타낸다[4]. 권리 표현 기술의 사용권한은 크게 사용자에게 콘텐츠가 표현되고 이용되는 권리 형태를 정의한 Render Permission, 사용자간에 권리의 교환이 이루어지는 권리 형태를 정의한 Transport Permission, 콘텐츠에 대한 추출 및 변형이 가능한 권리형태를 정의한 Derivative Permission으로 나눌 수 있다. 그리고 콘텐츠의 사용기간, 사용횟수 등과 같은 사용조건에 의해 사용이 제한될 수 있다. 권리표현 방식은 콘텐츠에 투명하고 폭넓게 사용할 수 있는 유연하고 상호 운용 가능한 메커니즘 및 기계 가독형을 제공하기 위해 주로 XML 기반으로 한 권리표현 언어가 개발되고 있으며, 대표적인 기술로는 XrML(eXtensible rights mark-up language)이 있다[2].

2.2 저작권 보호기술

콘텐츠를 구매한 사용자가 자신이 가지고 있는 사용규칙 범위 안에서만 콘텐츠를 사용하도록 사용자의 콘텐츠 사용을 제한하기 위해 다음과 같은 기술이 필요하다.

2.2.1 암호화

DRM 시스템에서는 인가된 사용자만이 디지털 콘텐츠를 사용할 수 있도록 하기 위해 암호화 기술을 적용하고 있다. 암호 기술은 특정키를 이용하여 디지털 콘텐츠를 암호화함으로써 해당키를 가진 사용자만이 디지털 콘텐츠를 복호화 하여 열람할 수 있도록 하는 기술이다.

위의 그림에서처럼 암호화키와 복호화 키의 동일 여부에 따라 암호 기술은 크게 비대칭키 암호 방식과 대칭키 암호 방식으로 분류할 수 있다. 암호화키와 복호화 키가 서로 다른 비대칭키 방식에는 RSA, ElGamal 등이 있으며, 이러한 비대칭키 방식은 암호화할 때의 키와 복호화할 때의 키가 서로 다르기 때문에 키를 효과적으로 분배할 수 있다는 장점이 있으나, 연산시간이 오래 걸린다는 단점이 있다. 반면, 암호화키와 복호화 키가 동일한 DES, SEED, AES 등의 대칭키 암호 방식은 비대칭키 방식에 비해 연산시간이 빠르지만, 키 분배에서의 문제점을 드러내고 있다. 이러한 특성을 이용하여, 용량이 큰 디지털 콘텐츠는 대칭키 암호화 방식을 이용하여 암호화함으로써 연산 속도를 줄이고, 동시에 비대칭키 방식을 활용하여 대칭키를 분배함으로써 DRM 시스템의 보안성을 높일 수 있다.

2.2.2 위변조 방지(tamper-proofing)[6]

Tamper-proofing 기술은 부정조작, 즉 콘텐츠의 위변조에 대한 방어기술이다. 여러 가지 tampering 기법이 소프트웨어에 적용될 수 있겠지만, 대표적으로 콘텐츠에 위변조가 가해졌을 때 tampering 검출 시스템을 통하여 콘텐츠의 위변조를 감지하게 되고, 프로그램이 오류 동작을 하게끔 만드는 기술이 tamper-proofing 기술이다.

2.2.3 워터마킹(Watermarking)[7]

워터마킹 기술이란 콘텐츠의 저작권 보호를 위해서 개발되기 시작한 기술로써 콘텐츠에 저작권 정보를 은닉하여 향후에 저작권 분쟁이 일어났을 때, 저작권 확인 등을 위해서 사용될 수 있는 기술이다. 이러한 워터마킹 기술은 가시적으로 확인이 가능한 워터마킹과 확인이 불가능한 워터마킹 기술로 나눌 수 있고, 또한 워터마킹 정보를 추출하기 위해서 원본이 필요한 경

우와 그렇지 않은 경우로 나눌 수 도 있다.

이러한 워터마킹 기술은 그 응용분야가 매우 다양하며, 은닉되는 정보가 저작권자에 대한 정보인 경우에는 워터마킹(Watermarking)으로, 사용자에 대한 정보이면 핑거프린팅(Fingerprinting)으로 구분된다. 즉, 핑거프린팅 기술은 출력문서의 어느 한 부분에 사용자에 대한 정보를 함께 출력함으로써 향후 내부 문서가 유출되었을 때, 유출자를 추적하는데 활용할 수 있는 것이다. 가장 손쉬운 방법은 출력문서의 하단에 가시적으로 출력시간과 출력자에 대한 정보를 인쇄함으로써 사용자에게 유출에 대한 경각심을 심어주는 것이다. 그러나 이러한 가시적인 정보의 경우 사용자에 의해서 제거될 가능성이 매우 높기 때문에 이 같은 정보를 사용자가 가시적으로 볼 수 없지만 문서 내부에 정보를 은닉함으로써 추적에 활용하는 기법이 더욱 적절한 방법이 될 수 있다.

3. DRM

3.1 DRM 정의

DRM(Digital Rights Management)이란 디지털 콘텐츠의 불법 유통과 복제를 방지하고, 적법한 사용자만이 콘텐츠를 사용케 하여, 사용에 대한 과금을 통해 저작권자의 권리 및 이익을 보호하는 시스템을 의미한다. DRM은 크게 두 가지의 형태로 구분할 수 있다. 하나는 콘텐츠를 정당한 권리를 가진 사용자에게만 안전하게 전송하고 허가된 사용범위 내에서 사용하게 제한하는 방법이다. 다른 하나는 불법으로 콘텐츠가 복제되어 유포됐을 때, 해당 콘텐츠의 저작권자가 누구인지를 증명하고 어떤 경로를 통하여 불법 복제되고 유통되었는지를 추적하는 기능이다.

3.2 DRM 시스템의 요구사항[2]

3.2.1 지속적인 보호

DRM의 가장 기본적이며 중요한 기능은 지적 자산의 완벽한 보호이다. 배포된 콘텐츠 중 단 하나만이라도 보호되지 못한다면 그 피해는 심각하기 때문이다. 이를 위해 DRM은 허가되지 않은 사용자의 콘텐츠 접근을 차단해야 하며, 접근 권한을 가지고 있는 사용자라 할지라도 부여된 권한 내에서만 콘텐츠를 사용할 수 있도록 통제해야 한다. 또한 콘텐츠가 악의적인 사용자에 의해서 무단 변경되는 것을 막아야하며, 콘텐츠 배포과정에서의 무결성과 비밀성을 보장해야 한다. 콘텐츠를 관리하는 DRM 에이전트는 공격으로부터 강인성을 유지할 수 있어야 한다.

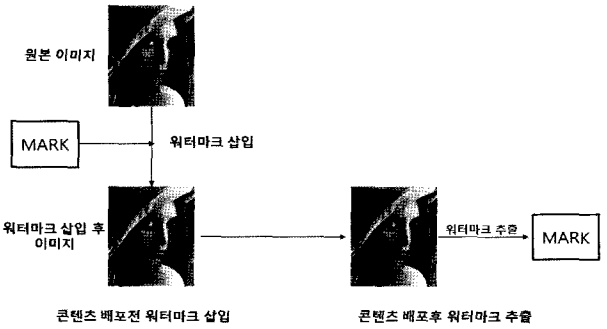

그림 2 워터마킹

3.2.2 사용 편리성

DRM은 콘텐츠의 저작권 보호를 위해 사용자에게 불편을 초래해서는 안된다. DRM의 보안성을 강화하다 보면 사용자의 편리성은 떨어질 수밖에 없다. 하지만 그렇다 할지라도 사용자가 디지털 콘텐츠를 쉽게 검색하고 얻을 수 있어야 하며, 허용된 권리 내에서는 자유롭게 콘텐츠를 사용하는 것을 보장해야 한다.

3.2.3 유연성

DRM은 문서, 멀티미디어 콘텐츠, 웹 기반의 콘텐츠, 소프트웨어 그 밖의 디지털콘텐츠 등 여러 종류의 디지털 콘텐츠 형식이라도 지원할 수 있어야 한다. 또한, 여러 종류의 DRM간의 연동을 통해서 DRM 시스템의 상이함으로 인해 발생하는 사용자의 권리 제한 문제를 해결해야 한다.

3.3 DRM 구조

다음 그림은 디지털 콘텐츠 유통의 일반적인 형태를 보여준다. 일반적으로 다음 순서에 따라 프로세스가 진행된다.

a. 패키징 - 패키징은 보호된 콘텐츠를 만들기 위해 디지털 콘텐츠를 암호화 하는 과정이다. 일반적으로 대칭키 암호화 시스템을 사용한다. 암호화된 디지털 콘텐츠는 추가적으로 저작권 정보, 미디어 정보를 포함하고 있는 메타데이터를 가지고 있다. 일반적으로 헤더 파일은 암호화 되지 않으며 여기에는 라이선스를 얻어 올 수 있는 URL정보가 포함된다.

b. 유통 - 패키징된 디지털 콘텐츠를 소비자에게 분배하는 과정이다. 콘텐츠는 비즈니스 모델에 따라 웹 서버, 스트리밍 서버, 혹은 CD나 DVD 같은 매체를 통해서 사용자에게 전달된다.

c. 라이선스 발급 및 획득 - 라이선스 서버가 디지털 콘텐츠를 구매한 정당한 사용자에게 라이선스를 발급하는 과정이다. 이러한 과정은 사용자를 인증하는 것으로부터 시작된다. 라이선스에는 디지털 콘텐츠 사용 규칙과 콘텐츠 암호화키가 들어 있다.

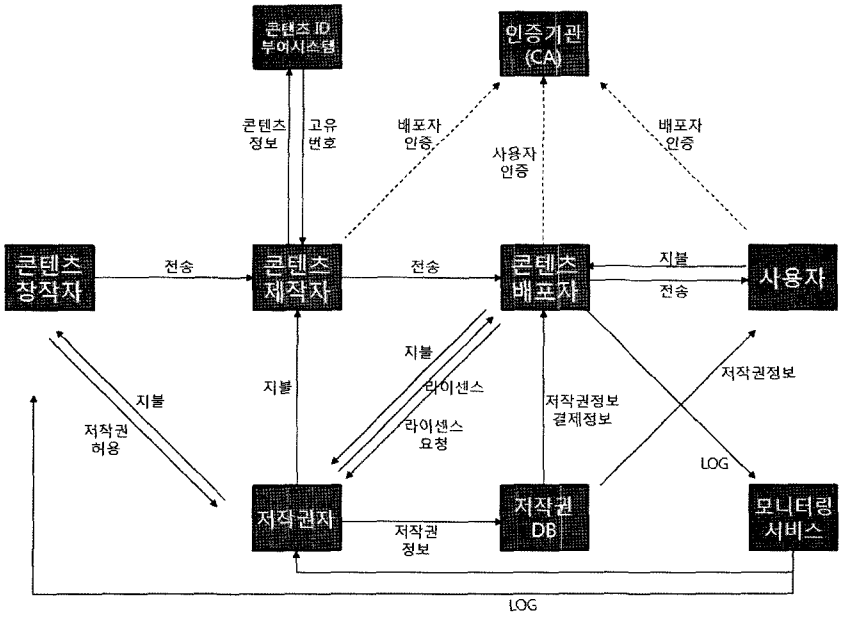

그림 3 MPEG21 멀티미디어 콘텐츠 유통 모델

d. 콘텐츠 사용 - 사용자가 자신이 가지고 있는 DRM 에이전트를 이용해서 배포 받은 디지털 콘텐츠와 획득한 라이선스를 이용해서 디지털 콘텐츠를 사용하는 과정이다. 이때 사용자는 주어진 권한 내에서만 콘텐츠를 사용하도록 에이전트에 의해서 관리되어진다.

3.4 대표적인 DRM 시스템

대표적인 DRM 시스템으로 Microsoft사의 WMDRM을 들 수 있다. 이는 Windows media 형식의 디지털 콘텐츠의 보호를 위한 DRM으로 콘텐츠 소유자, 라이선스 서버 그리고 사용자 PC에 설치된 플레이어 사이에 적용된다. WMDRM은 라이선스와 미디어가 각각 분리되어 배포되며, 라이선스의 조건 변경이 쉽고, 대여나 회원제 형태의 비즈니스 모델을 적용하거나, 미리보기의 제한 등의 세부 기능이 있어 유연한 DRM 시스템의 사용이 가능하다.

mp3플레이어인 애플의 iPod에 사용되는 DRM인 Fair-Play는 iTunes라는 애플사의 음악다운로드 서비스와 iPod를 연결하는 DRM으로 다른 웹 서비스나 다른 디바이스간의 연동을 허락하지 않는 성격을 가지고 있다.

IBM은 Cryptolope라는 암호화 패키징 제품을 이용한 디지털 뮤직 저작권 보호 기술인 EMMS(Electronic

표 1 대표적인 DRM 시스템[9]

이름	사용	년도	특성
FaiaPlay	iTunes Library, iPod	2003	구매된 음악 파일은 AAC 형태로 인코딩되고 이러한 형식은 iTunes와 iPod에서만 사용 가능함
3-day-or-3-play	Microsoft Zune	2006	다른 Zune 장치에서 무선으로 받은 음악파일을 장치에서 오직 3번만 재생가능하며, 재생 여부와 관계없이 3일이 지나면 만료되는 방식. 수신자는 음악을 재전송할 수 없다.
Janus WMA DRM	All PlaysForSure Devices	2004	janus는 휴대용 장치를 한 Windows Media DRM의 버전임
Content-scrambling system	DVD Discs	1996	DVD 비디오를 40비트의 스트림 암호로 암호화 하는 방식을 이용
VHS Macrovision	대부분의 VHS Video	1984	보호된 테이프를 복제하려고 할때 화면을 주기적으로 어둡게 하는 방식을 사용함
DVD Region Code	DVD	1996	많은 DVD Video 디스크들은 하나 혹은 그 이상의 지역 코드를 가지고 있어서 지역코드가 같은 기기에서만 재생 가능함
OMA DRM	550여개 이상의 핸드폰	2004	Open Mobile Alliance에 의해서 개발된 DRM 시스템으로 모바일 기기 상의 콘텐츠를 보호한다.
Windows Media DRM	온라인 비디오	1999	WMDRM은 IP네트워크를 통해서 PC나 재생 장치로 오디오나 비디오 콘텐츠를 안전하게 제공하는 기능을 함

Media Management System)을 개발 하였으며 xCP(eXtensible Content Protection)이라는 전략을 이용 좀 더 유연한 DRM 시스템을 개발하고 있다. 또한 Adobe사는 acrobat을 이용 문서의 암호화와 전자서명, 접근권한 설정 등을 지원하고 있다.

4. 결 론

미래 유비쿼터스 시대에는 더 많은 디지털 콘텐츠들이 생산되고 유통될 것이다. 디지털 콘텐츠 시장이 성장할수록 이에 대한 지적 재산권을 보호하기 위해 DRM 기술의 발전도 더욱 가속화될 전망이며, DRM의 적용이 상업적 콘텐츠뿐만 아니라 비상업적 콘텐츠까지 확장될 것으로 예상된다. 이를 반영 하듯 얼마 전 국내 최대의 음악파일 공유 사이트인 소리바다와 삼성전자가 계약을 맺었다는 기사가 실렸다. 소리바다는 삼성전자로부터 DRM 소프트웨어를 공급받고 삼성전자는 소리바다로부터 음원을 제공받는다는 내용의 계약이다. 이처럼 DRM 시장은 계속해서 성장해가며 여러 비즈니스 모델을 보여주고 있다.

하지만 이러한 DRM 기술에 대한 대부분의 원천기술은 InterTrust, Intel, Microsoft, IBM 등 외국 회사들에 의해서 이미 특허가 등록되어 있는 상태이며, 이러한 특허를 기반으로 국제 표준화가 지속적으로 진행중이다. 국내 DRM 기술의 경우 세계 시장에 수출되기도 하지만 원천 기술에 대한 특허가 부족한 실정이다. 따라서 국내의 DRM 기술이 경쟁력을 가지기 위해서는 새롭게 진행되고 있는 DRM분야의 기술개발에 노력해야 할 것이다.

참고문헌

[1] Commission of The European Communities, "Commission Staff Working Paper : Digital Rights Background, Systems, Assesment", 2002.02.

[2] 강호갑, "DRM 최신 국제표준 기술사양 분석 및 세계 유명제품 동향과 전망에 관한 연구", 2004.

[3] Interoperability of data in e-commerce systems, http://www.indecs.org/

[4] Bill Rosenblatt, "Digital Rights Management : Business and Technology" (ISBN: 0-7645-4889-1), John Wiley & Sons, 2001.

[5] Karen Coyle, Rights Expression Languages: A Report for the Library of Congress, Feb. 2004.

[6] C. S. Collberg and C. Thomberson, "Watermarking, Tamper-Proofing, and Obfuscation - Tools for Software Protection", U. of Arizona, TR, Mar. 2000.

[7] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking Digital Image and Video Data", IEEE SP Mag., Vol.17, no. 5, pp.20-46, Sep. 2000.

[8] 주학수, 김대엽, 장기식, 김승주, "디지털 저작권 관리 시스템(DRM)의 개발현황", 정보보호학회지, 2003.4.

[9] Wikipedia http://www.wikipedia.org

최 동 현

2005. 8 성균관대학교 정보통신공학부 공학사
2007. 2 성균관대학교 컴퓨터공학과 석사
2007. 3~현재 성균관대학교 일반대학원 휴대폰학과 박사과정 재학 중
관심분야 : 암호이론, 네트워크 보안, DRM, 모바일
E-mail : dhchoi@security.re.kr

이 병 희

2005. 2 성균관대학교 정보통신공학부(공학사)
2007. 2 성균관대학교 컴퓨터공학과 석사
2007. 3~현재 성균관대학교 일반대학원 전자전기컴퓨터공학과 박사과정 재학 중
관심분야 : 정보보안, 네트워크 보안, 보안성 평가
E-mail : bhlee@security.re.kr

김 승 주

1994. 2~1999. 2 성균관대학교 정보공학과 (학사, 석사, 박사)
1998. 12~2004. 2 한국정보보호진흥원(KISA) 팀장
2004. 3~현재 성균관대학교 정보통신공학부 교수
2001. 1~현재 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002. 4~현재 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005. 7~현재 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
2006. 2~현재 한국우주통신연구소 암호연구회 운영위원
관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET
E-mail : skim@security.re.kr

원 동 호

1976~1988 성균관대학교 전자공학과 (학사, 석사, 박사)
1978~1980 한국전자통신연구원 전임연구원
1985~1986 일본 동경공업대 객원연구원
1988~2003 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996~1998 국무총리실 정보화추진위원회 자문위원
2002~2003 한국정보보호학회장
현재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, IT 보안성평가연구회 위원장
관심분야 : 암호이론, 정보이론, 정보보호
E-mail : dhwon@security.re.kr