情報保護學會論文誌
第 21 卷 第 3 號, 2011. 6

스마트카드를 이용한 프록시 재 암호화 기법 기반 콘텐츠 공유 메커니즘에 관한 연구*

박 승 환,[1†] 구 우 권[1], 김 기 탁[1], 문 혜 란[2], 이 동 훈[1‡]
[1]고려대학교 정보보호대학원, [2]한국전자통신연구원

A Study on Contents Sharing Mechanism based on Proxy Re-Encryption Scheme using the Smart Card*

Seunghwan Park[1†], Woo Kwon Koo[1], Kitak Kim[1], Hyeran Mun[2], Dong Hoon Lee[1‡]
[1]Graduate School of Information Security, Korea University,
[2]Electronics and Telecommunications Research Institute

요 약

OMA(Open Mobile Alliance)는 모바일 디바이스 분야에서 DRM 기술에 대한 가장 활발한 표준화 활동을 벌이고 있으며, 2007년에는 OMA-DRM v2.1 표준을 발표하였다. 이후 2009년에는 OMA-DRM v2.1의 확장이라고 할 수 있는 OMA-SRM(Secure Removable Media)과 SCE (Secure Contents Exchange)등 DRM 기술과 공유 모델에 대한 표준을 발표하였다. SCE는 사용자도메인을 구성하여 OMA-DRM v2.1에서 정의된 모바일 디바이스뿐만 아니라 일반 가전기기(Phone, PC, 카오디오 등)간의 콘텐츠 및 권리(Rights)를 공유할 수 있다. 본 논문에서는 OMA-DRM과 SCE의 기술과 공유 모델에 대하여 분석을 하고, 프록시 재 암호기법을 사용하여 공유된 콘텐츠와 권리를 이용하기 위한 각 개체들의 키 분배방법을 제시하고자 한다.

ABSTRACT

OMA(Open Mobile Alliance) is one of the most active group about DRM technology in mobile device field. OMA announced an OMA-DRM v 2.1 standardization in 2007. After then OMA announced OMA-SRM(Secure Removable Media) and SCE(Secure Contents Exchanges) that are the extension of OMA-DRM v2.1. In SCE, a user can form user domain to share contents and rights. So the user can share contents and rights with not only the OMA-DRM v2.1 but also home devices like mobile phones, personal computers and audios. In this paper, we analyze a sharing technology of OMA-DRM and SCE, and then propose key distribution method using proxy re-encyption and smart card to use shared contents and rights.

Keywords: DRM, OMA-DRM, Proxy re-encryption

I. 서 론

1.1. 개요

DRM(Digital Right Management)은 정당하게 구매한 사용자만이 콘텐츠 사용권한을 제공받고 구매하지 않은 사용자의 콘텐츠에 대한 불법적인 접근을 차단하는 솔루션으로서 현재 많은 표준/서비스

접수일(2010년 4월 6일), 수정일(2010년 9월 10일)
게재확정일(2010년 12월 9일)
* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2010-0029121).
† 주저자, sgusa@lycos.co.kr
‡ 교신저자, donghlee@korea.ac.kr

안들이 제시되고 있다. Open Mobile Alliance에서는 OMA-DRMv1.0[5]을 시작으로 2007년에는 OMA-DRMv2.1[5] 표준을 내놓으면서 DRM기술에 관련하여 많은 연구를 하고 있다. DRM은 일반적으로 "디지털 콘텐츠의 불법유통과 복제를 방지하고, 적법한 사용자만이 콘텐츠를 사용케 하며, 과금 서비스 등을 통하여 디지털 콘텐츠 저작권을 관리하는 기술"로 설명할 수 있다. 즉, 멀티미디어 콘텐츠의 제작에서부터 유통, 소비에 이르기까지의 멀티미디어 콘텐츠의 모든 생명주기에서, 콘텐츠 제작자, 유통업자 및 최종 사용자가 쉽게 사용하고, 다양한 멀티미디어 콘텐츠와 관련된 사업 모델들을 통합하며, 멀티미디어 프레임워크 표준이라고 할 수 있다.[9]

OMA DRM 시스템의 표준에서는 콘텐츠 공유를 위한 각 콘텐츠 발급자, 권리 발급자, 사용자 혹은 DRM Agent 등 각 개체를 정의하였고, 콘텐츠나 키 값들이 전송되는 프로토콜을 정의하였다. OMA DRM 시스템에서는 콘텐츠의 공유를 위하여 다양한 특징을 갖는 암호시스템을 이용하였다. 데이터의 무결성을 제공하기 위한 MAC, 데이터를 빠르게 암호화하기 위한 대칭키 암호 AES 그리고 키 관리가 용이한 공개키 암호 RSA이다. 이 때 대칭키 암호와 공개키 암호는 KEM-DEM 구조로 사용된다. 이 구조는 대칭키 암호와 공개키 암호의 장점을 모두 수용하기 위하여 용량이 큰 데이터인 경우에는 대칭키 암호시스템을 사용하고(Data Encapsulation Mechanism), 대칭키 암호에 쓰였던 비밀키를 공개키 암호시스템을 사용하여 암호화한 후에 공개키를 분배한다(Key Encapsulation Mechanism). OMA DRM 시스템의 표준 역시 두 암호시스템의 장점을 이용하기 위하여 용량이 큰 콘텐츠를 대칭키 암호를 사용하여 패키징 하였고, 콘텐츠 암호화 키, 권리 암호화 키 등 단계적인 암호화에도 대칭키 암호를 사용하였으며, 최종적으로 쓰였던 비밀키를 공개키 암호를 사용하여 암호화 하는 방식으로 연산의 효율성을 높였으며, 공개키 암호의 사용으로 키 관리에도 용이하게 제안했다.

OMA DRM 시스템의 표준은 콘텐츠 발급자, 권리 발급자가 사용자에게 콘텐츠와 콘텐츠 이용에 관한 권리증서를 분배하는 것에는 매우 효율적으로 나타나 있다. 하지만 사용자가 다른 사용자와의 콘텐츠 공유를 위해서는 키 분배 절차에 불편함이 있다. 사용자 A의 공개키로 암호화된 권리 암호화 키 암호문을 사용자 B에게 공유를 위해서는 복호화 이후에 사용자 B의 공개키로 다시 암호화하는 절차가 필요하기 때문이다. 이러한 복호화와 암호화 두 번의 절차 없이 한 번의 알고리즘 수행으로 해결할 수 있다면 더 효율적인 공유 방법이 될 수 있을 것이다.

앞에서 말한 문제점을 해결하기 위해서 본 논문에서 제안하는 방법이 바로 프록시 재암호화 기법을 이용한 권리 암호화 키 분배 방법이다. 프록시 재암호화 기법은 사용자 A의 공개키로 암호화되어 있는 암호문을 재암호화 알고리즘 한 번의 수행으로 복호화 과정 없이 사용자 B의 공개키로 암호화되어 있는 암호문으로 바꿀 수 있는 기법이다. 두 사용자 이외에 프록시라는 제 3자에 의하여 재암호화 과정이 이루어지며, 이때에는 두 사용자의 키 값에 의해 생성된 재암호화 키가 사용된다. 프록시는 재암호화 키를 가지고 두 사용자의 비밀키와 평문에 대한 어떤 정보도 알 수 없으며, 오로지 재암호화 알고리즘만 수행할 수 있다. 프록시 재암호화 기법은 Libert[1] 등에 의해서 소개된 복호화 권리를 위임하는 암호화 기법 이후로 Blaze[3] 등에 의해서 처음으로 재암호화 기법이 제안되었다. 그러나 Blaze 등의 기법에서는 악의적인 프락시가 A에서 B로 암호문을 변환시키는 재암호화 키를 받게 되면 B에서 A로 암호문을 변환시키는 재암호화 키를 쉽게 도출할 수 있는 양방향성(Bidirectional)의 성질을 가진다. 양방향성은 프락시에게 추가적인 재암호화 권리를 제공하므로 바람직하지 않다. 최근에는 양방향성 대신 단방향성(Unidirectionality)의 성질을 지니는 재암호화 기법들이 주요하게 연구되고 있다[4,1]. 참고로 단일방향성을 제공하는 기법이 존재하면 양방향성을 제공하는 기법을 쉽게 구현할 수 있다. 한편, 재암호화된 암호문을 다시 재암호화 할 수 있는, 즉 재사용성(Multiple use capability)을 제공하는 기법도 연구되고 있다[4].

1.2. 기여도

본 논문에서는 먼저 OMA의 표준인 OMA-DRM v2.x와 SCE를 분석한다. OMA-DRM v2.x 같은 경우에는 음악, 영화 등 다양한 콘텐츠들의 저작권한이 문제가 되면서 이전부터 많은 논문에서 언급되고 분석되어져 왔었다. 하지만 콘텐츠에 대한 저작권한 문제가 사용자의 권리 측면에서도 대두되었고, 같은 사용자에 대한 기기들의 공유 혹은 다른 사용자들에 대한 공유도 하나의 이슈가 되었다. 이에 OMA에서는 OMA-DRM v2.x를 기반 하에 콘텐츠 공유에 대한 표준으로 SCE를 2009년에 내놓았다. 본 논문에서는 공유할 때 이동

하는 콘텐츠와 사용된 암호화키의 분배 및 관리 중심으로 SCE를 분석하여 각 객체간의 신뢰도를 도출해 보고 OMA-DRM v2.x와 비교하여 본다.

또한 OMA의 키 관리 방법을 기초로 하여 콘텐츠 공유를 위한 프록시 재암호화 기법을 이용하여 콘텐츠 공유를 위한 키 값들을 사용자간에 공유하는 방법을 제안한다. 기존의 OMA DRM 시스템에서 제안한 방법과 마찬가지로 콘텐츠나 콘텐츠 암호화 키, 권리 암호화 키, MAC 값 등은 연산 속도가 빠른 대칭키 암호로 이루어지며, 대칭키 암호의 비밀키 공유를 위해서는 OMA DRM 시스템에서 쓰였던 RSA 공개키 암호 기법을 쓰지 않고, 암호문의 위임시 복호화 과정이 필요 없는 프록시 재암호화 기법을 사용한다. 여기서 쓰이는 프록시 재암호화 기법은 단방향성과 재사용성을 제공하는 기법이어야 한다. 사용자 간의 공유는 한 번 이상 이루어지기 때문에 재사용성이 필요하며, 역으로 콘텐츠와 권리가 이동하는 일은 없기 때문에 단방향성 성질을 만족하여야 한다.

이후 논문의 구성은 다음과 같다. Ⅱ장에서는 OMA DRM 시스템에서 제안하고 있는 공유 모델에 관하여 간단히 살펴본다. Ⅲ장에서는 프록시 재암호화 기법에 대하여 간단히 알아보고, 프록시 재암호화 기법을 이용한 키 분배 방법을 제안하고 기존의 OMA DRM 시스템에서의 키 관리 방법과 분석해 보인다. Ⅳ장에서는 Ⅲ장에서 제안한 기법에 스마트카드를 이용한 방법을 제안하고 분석한다. Ⅴ장에서는 결론을 내린다.

II. OMA의 공유 모델

OMA DRM 시스템은 콘텐츠 발행자의 DRM 콘텐츠 분배와 권한 관리자에게 DRM콘텐츠에 관한 권리증서(Right Object) 분배를 가능하게 한다. 이번 절에서는 OMA DRM을 구성하는 구성 요소 소개와 OMA-DRMv2.1[5,8]의 공유 모델, SCE에서의 도메인 구성과 디바이스간의 공유 모델과 이 공유 모델들에서의 키 관리 방법에 대해서 살펴본다.

2.1 OMA-DRM v2.x

OMA DRM 구성요소들은 DRM 시스템에서 각각 특별한 역할을 수행한다. 구성요소들의 역할은 다음과 같다.

- **DRM Agent**: DRM Agent는 장치 안에 신뢰되는 실체를 구체화하며 DRM 콘텐츠와 관련된 허가 및 제한을 실행함
- **콘텐츠 발급자(Content Issuer)**: DRM 콘텐츠를 전송하는 구성 요소
- **권리 발급자(Right Issuer)**: DRM 콘텐츠에 대한 허가와 제한을 할당하는 구성 요소로서 권리증서를 생성함
- **사용자(User)**: DRM 콘텐츠를 이용하는 자
- DRM 시스템에서는 콘텐츠를 전송하기 전에 비정상적인 접근을 허용하지 않기 위해 콘텐츠를 패키징(Packaging)시켜야 한다. 패키징 된 콘텐츠와 권리는 다음과 같이 분배되어 진다.
- **콘텐츠 패키징**: 콘텐츠는 콘텐츠 암호화 키(CEK, Content Encryption Key)를 통해 암호화되어 DCF 형태로 패키징 된다.
- **DRM Agent 인증**: 모든 DRM Agent는 자신의 공개키, 개인키 쌍과 인증서를 가지고 있음 인증서에는 만든 사람, 디바이스 종류, 소프트웨어 버전, 시리얼 넘버 등이 포함 됨
- **권리증서 생성**: 콘텐츠 암호화키를 포함한 권리증서는 XML 문서로, 콘텐츠와 관련된 사용 권한 및 허가를 나타냄
- **권리증서 보호**: 권리증서가 전송되기 전에, 콘텐츠 암호화키와 같은 비밀정보는 보호되어야 하고, 따라서 권리증서는 DRM Agent의 권리증서 암호화 키(REK, Right Object Encryption Key)로 암호화 됨
- **분배**: 암호화된 권리증서와 DCF(DRM Content Format)는 HTTP/WSP, MMS와 같은 전송 시스템을 통해 DRM Agent에 전송

DRM Agent는 권리 발급자로부터 신뢰되어야 한다. OMA DRM에서는 모든 DRM Agent는 자신의 공개키, 개인키, 인증서 쌍을 가지고 있으므로 이를 이용하여 권리 발급자는 DRM Agent를 인증한다. 만약 DRM Agnet가 더 이상 신뢰되지 않는다면 권리 발급자는 더 이상 콘텐츠를 DRM Agent에게 전송하지 않는다. DCF은 암호화된 콘텐츠를 위한 안전한 콘텐츠 패키지이다. 암호화된 콘텐츠는 신뢰되는 DRM Agent가 복호화를 할 수 있도록 암호화 되지 않은 콘텐츠 요약정보 및 권리 발급자 URI를 포함한다. 암호화한 콘텐츠를 복호화 하기 위해서 DRM Agent는 권리 발급자로부터 인증을 받은 뒤, 권리증서를 발급 받아 복호화 키를 얻는다. 권리증서는

DRM 콘텐츠에 대한 사용 규칙을 명시해 놓은 XML로 DRM 콘텐츠에 대한 제한 및 허가를 포함한다. 또한 DRM 콘텐츠를 복호화를 위한 콘텐츠 암호화키를 포함한다. 권리증서에는 콘텐츠 암호화 키와 같은 비밀정보가 포함되어 있으므로 전송되기 전에 권리증서 암호화키로 암호화 된 후, 권리 발급자의 개인키로 서명된다. 권리 발급자는 권리증서를 분배할 때, DRM Agent로부터 인증을 받아야 하고, DRM 시스템은 권리증서가 재전송되어 공격에 악용되는 것을 막아야 한다.

사용자의 디바이스에 있는 콘텐츠 발급자로부터 얻은 콘텐츠는 Super Distribution이나 도메인(Domain)을 통하여 다른 디바이스로 공유할 수 있다. DRM Agent로부터 다른 DRM Agent로 DCF를 전송할 수 있으며, DCF를 받은 DRM Agent는 콘텐츠를 이용하기 위하여 새로운 권리 증서를 권리 발급자로부터 받아야 한다. 도메인을 통한 공유는 같은 도메인에 속해 있는 DRM Agent간에 DCF와 권리증서를 공유 할 수 있으며, 권리증서는 하나의 도메인키로 암호화되어 있다. 전송받은 권리증서를 이용하기 위해서는 도메인에 가입되어 있어야 하고, 그렇지 않다면 도메인에 가입을 한 이후에 이용을 할 수 있다. 도메인은 권리 발급자에게서 관리되므로 DRM Agent의 도메인 가입과 탈퇴는 권리 발급자로부터 이루어진다.

2.2 SCE

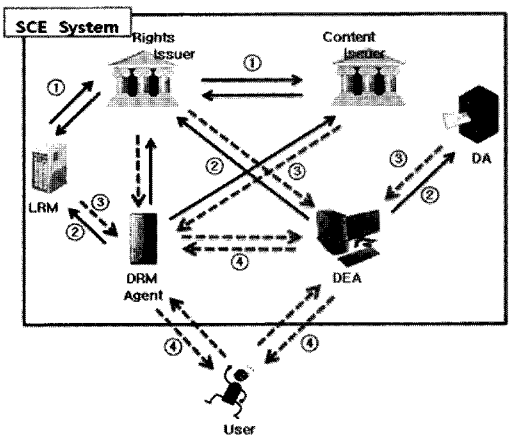
SCE(Secure Content Exchange) 시스템은 OMA DRMv2.x[8]에서 확장된 개념으로 구입한 콘텐츠를 여러 디바이스 사이에서 공유를 가능하게 한다. SCE는 OMA DRMv2.x에 정의된 디바이스뿐만 아니라 일반 가전기기(Phone, PC, 전자기기, 카오디오 등)간의 콘텐츠 및 권리를 공유할 수 있다. 디바이스 기기의 확장과 더불어 SCE는 효율적인 콘텐츠 공유를 위하여 OMA DRMv2.x에서 정의된 도메인보다 더 구체화되고 확장되어진 도메인 모델을 제시하였다. SCE의 구성요소는 다음과 같다.[6]

- **DRM Agent**: OMA DRMv2.x와 같음
- **권리 발급자**: OMA DRMv2.x와 같음
- **DEA(Domain Enforcement Agent)**: 사용자 도메인 정책에 기반 하여 사용자 도메인을 관리함 디바이스들의 집합을 정의하고, 도메인내에서 디바이스간의 콘텐츠 이동을 보증
- **지역 권리 관리자(LRM, Local Rights Manager)**[7]: 권리 발급자의 중개 역할을 하며, 직접 DCF와 권리증서의 생성과 분배를 하기도 함

사용자 도메인의 권리증서를 받아서 소비하려면 DRM Agent는 사용자 도메인을 관리하기 위한 DEA를 등록하여야 한다. DEA를 등록한 후에 DRM Agent는 사용자 도메인의 멤버를 가입시킨다. DEA는 DRM Agent가 사용자 도메인에 가입을 제어할 수 있다. 예를 들면 가입할 수 있는 멤버의 최대수를 제한할 수 있고, 사용자 도메인의 멤버에서 DRM Agent를 제거하거나 탈퇴할 것을 요청할 수도 있다. 권리 발급자나 지역 권리 관리자는 사용자 도메인의 권리증서를 생성하기 위해서는 사용자 도메인을 관리하는 DEA를 등록하여야 한다. 권리 발급자 / 지역 권리 관리자는 권리증서를 생성하기 위한 권한(Permision)을 얻은 후 권리증서 생성과 분배를 한다.

2.2.1 SCE 시스템의 가정

- OMA SCE는 OMA DRM 2.0의 기능을 그대로 사용
- PKI기반 : 인증서가 검증되었다면 개체를 신뢰할 수 있음
- Secure Environment : SCE 개체들 사이의 어떠한 연결타입에서도 프로토콜의 안전을 보장해야 함



[그림 1] SCE 시스템 적용 시, 신뢰 모델

- 프로토콜에서 정보가 흐를 때 권리 암호화 키(REK)값이 노출되면 안됨
- DRM Time : DRM Agent는 공유나 대여시간이 끝나고 나서는 권리증서(RO)를 공유하거나 대여해 줄 수 없음

2.2.2 SCE 시스템의 신뢰모델

① 콘텐츠 발급자와 권리 발급자는 각 개인키를 이용한 PKI 전자서명을 통하여 상호 인증을 수행함으로 서로 신뢰할 수 있다.
② 콘텐츠 발급자는 개인키를 이용한 PKI 전자서명을 통하여 DRM Agent로부터 인증과정을 수행하므로 DRM Agent는 콘텐츠 발급자를 신뢰한다.
③ DRM Agent의 내부프로그램은 악의적인 사용자에 의해 조작될 수 있는 환경이므로, DRM Agent의 전자서명을 콘텐츠 발급자는 신뢰할 수 없다.
④ 사용자가 악의적으로 DRM Agent를 조작할 수 있고, 사용자 자신도 모르게 DRM Agent에 악성프로그램이 설치될 수 있으므로 DRM Agent와 사용자는 상호 신뢰할 수 없다.

2.3 OMA 공유 모델에서의 키 관리

OMA DRMv2.x과 SCE에서 콘텐츠는 콘텐츠 암호화 키(CEK)로 암호화되어 DCF형태의 포맷으로 패키징되고, 콘텐츠 암호화 키는 권리 암호화 키(REK)로 암호화되어 권리증서가 생성되고 분배된다. 권리 암호화키는 DCF와 권리증서와 같이 수신자에게 안전하게 분배되어야 한다. 권리 암호화 키는 KDF 해쉬함수, AWES 대칭키 암호, RSA 공개키 암호를 사용하여 수신자의 공개키를 이용하여 발급자의 개인키를 이용한 MAC 서명과 함께 암호화되어 전송되어진다. 디바이스에 분배되는 권리 암호화키와 MAC값의 암호화 과정은 다음과 같다.[5]

- K_{MAC}, K_{REK} 생성
- KEK 생성(Z는 임의의 값)
  KEK=KDF(I2OSP(Z, mlen), NLL, kekLen)
- C 생성 및 전송
  C_2 = AES-WRAP(KEK, K_MAC | K_REK)
  C_1 = I2OSP(RSA.ENCRYPT($PubKey_{Device}$, Z), mlen)
  C = C_1 | C_2

전송받은 C의 복호화 과정은 다음과 같다.

- C 복호화 및 Z유도
  C_1 | C_2 = C
  c_1 = OS2IP(C_1 ,mLen)
  Z = RSA.DECRYPT($PrivKey_{Device}$, c_1) = c_1^d mod m
- K_{MAC}, K_{REK} 계산
  KEK = KDF(I2OSP(Z, mLen), NULL , kekLen)
  K_{MAC}|K_{REK} = AES-UNWRAP(KEK , C_2)

〔표 3〕OMA DRM과 SCE 비교

	OMA DRM 2.x	SCE
디바이스	모바일 디바이스	모바일 폰과 일반 가전기기(PC, TV, 홈 미디어센터)로의 확장
도메인	권리 발급자를 통한 도메인 생성,가입, 탈퇴 관리 기능 제공	지역 권리 관리자, DEA를 통한 도메인 생성, 가입, 탈퇴 관리기능 제공
Non-OMA DRM	Export	Import
일시적인 공유	일시적인 공유 안됨	사용자도메인안에서의 일시적인 공유가능
Unconnected 디바이스의 공유	Connected 디바이스를 통해 DCF와 권리증서 받음	Connected 디바이스를 통해 DCF와 권리증서 받음
SCE와 OMA DRM 2.x의 관계	2.0 DRM Agent는 사용자도메인에 가입할 때 DEA가 아닌 권리 발급자를 통해 대리가입을 해야하고 사용자도메인에 가입을 하지 않고 콘텐츠를 이용하기 위해서는 권리 발급자에게서 권리증서를 받아야 함	SCE DRM Agent는 지역 권리 관리자와 DEA 사이에서 사용자도메인 가입과 콘텐츠 및 권리증서 공유가 가능

도메인으로 분배되는 권리 암호화키도 위와 같은 방법으로 이루어지며, 디바이스의 공개키 대신에 도메인의 공개키로 암호화되어진다. 지역 권리 관리자(LRM)에서 생성된 권리증서는 DRM Agent로도 전송되어지지만 권리 발급자에게도 전송되어져야 한다. 이때 쓰이는 권리 암호화키도 위와 같은 방법으로 권리 발급자의 공개키로 암호화되어 전송되어진다.

2.4 OMA-DRM v2.x와 SCE 비교

OMA DRM은 권리 발급자로부터 자신이 발급받은 권리증서의 관리 정책에 따라 같은 DRM시스템을 사용하는 디바이스간의 전송을 지원하며, 자신의 디바이스가 아닌 제 3자의 디바이스에서 실행될 수 있는 콘텐츠 및 권리증서를 구매 후 전송 할 수 있다. 또한 사용자는 자신이 구매한 DRM 콘텐츠를 export 기능을 통해 다른 DRM시스템을 사용하는 디바이스에도 전송 할 수 있다. 이외에도 스트리밍 서비스 및 미리보기 서비스 지원, 도메인 관리를 통한 콘텐츠 공유 지원, 디바이스의 훼손이나 분실로 인한 DRM 콘텐츠 복구, 버전이 다른 DRM 시스템 상호호환성 지원, 디바이스 폐기(Device Revoke), 디바이스 미터링(Device Metering)을 제공한다. SCE는 OMA DRM 2.x에서의 확장된 개념으로 OMA DRM v2.x에 정의된 디바이스뿐만 아니라 일반 가전기기(Phone, PC, 전자기기, 카오디오 등)간의 콘텐츠 및 권리증서를 공유할 수 있다. 사용자가 가지고 있는 디바이스간의 공유를 활성화시키기 위해 OMA DRM2.x에서 정의된 도메인 개념을 더 확장하였으며, 지역 권리 관리자와 DEA라는 새로운 개체를 통해 도메인 관리 및 콘텐츠, 권리증서 공유를 지원한다. 또한 자신의 디바이스가 아닌 다른 사용자의 디바이스와도 자신의 도메인 범위 안에서 일시적인 공유를 지원한다.

III. 제안하는 키 분배 방법

본 절에서는 프록시 재 암호기법을 이용한 키 분배방법을 제안한다. 지역 권리 관리자/권리 발급자는 프록시 재 암호화 환경에서 프록시가 되어서 재 암호화키(Re-encryption Key) RK를 가지고 암호문 C를 변경하게 된다. 구체적인 기법은 다음과 같다.

3.1 프록시 재 암호화 기법 모델

프록시 재 암호화기법(Proxy Re-encryption Scheme, IBRS)은 다음과 같은 6개의 다항식 시간(polynomial-time) 알고리즘들로 구성된다.[2]

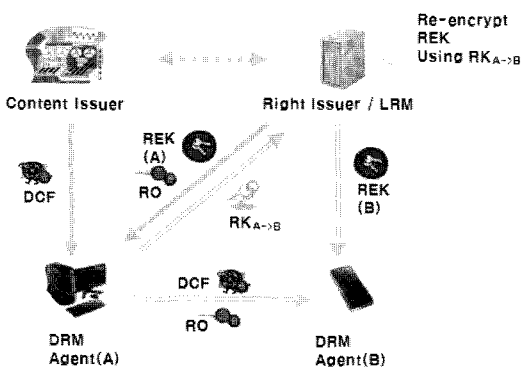
- **Setup**(1^{λ}): 셋업(Setup) 알고리즘은 보안 상수λ을 입력으로 받고 공개키 PK_A, PK_B와 비밀키 SK_A, SK_B을 출력한다.
- **Encryption**(M, PK_A): 암호화 알고리즘은 메시지 M, 공개 상수 PK_A 을 입력으로 받고 메시지 M에 대한 암호문 C_A을 출력한다.
- **RKGen**(PK_B, SK_A): 재 암호화키 생성 알고리즘은 B의 공개키 PK_B의 A의 비밀키 SK_A를 입력 받고 재 암호화키 $RK_{A\rightarrow B}$을 출력한다.
- **ReEncryption**(C_A, $RK_{A\rightarrow B}$): 재 암호화 알고리즘은 A의 공개키로 암호화된 암호문 C_A와 재 암호화키 $RK_{A\rightarrow B}$ 를 입력 받고 B의 공개키로 암호화된 암호문 C_B을 출력한다.
- **Decryption**(C_B, SK_B): 복호화 알고리즘은 암호문 C_B와 비밀키 SK_B 을 입력 받고 암호문에 대한 평문 M을 출력한다.

프록시 재암호화 기법은 설계된 구조에 따라서 다양한 성질을 갖는다. 암호문을 프록시가 A에서 B로 암호문을 변환시키는 재암호화 키를 받게 되면 B에서 A로 암호문을 변환시키는 재암호화 키를 쉽게 도출할 수 있는 양방향성(Bidirectional)의 성질과 반대의 재암호화 키를 도출할 수 없는 단방향성(Unidirectionality) 성질이 있고, 재암호화된 암호문을 다시 재암호화 할 수 있는 재사용성(Multiple use capability)을 제공하는 성질과 한번 재암호화된 암호문은 다시 재암호화 할 수 없는 일회성(Single use)의 성질을 갖기도 한다.

3.2 제안하는 키 분배 방법

DRM Agent(A)는 권리증서를 사용하기 위하여 받은 권리 암호화 키(REK)의 암호화된 값 C_A를 DRM Agent(B)와 공유하기 위하여 지역 권리 관리자(LRM)/권리 발급자(RI)가 프록시가 되어 재 암호화키 $RK_{A\rightarrow B}$를 사용하여 C_A값을 DRM Agent(B)의 공개키로 암호화된 값 C_B으로 바꾸어 전송을 한다.

- A가 DCF와 권리증서(RO)를 B에게 전송 :



〔그림 2〕 재 암호화 기법을 이용한 콘텐츠 공유

DRM Agent(A)는 DRM Agent(B)와 콘텐츠 공유를 하기 위하여 자신이 가지고 있는 패키징된 콘텐츠 DCF와 콘텐츠를 암호화한 키 콘텐츠 암호화 키(CEK)가 포함되어 있는 권리증서(RO)를 DRM Agent(B)에게 전송한다.

- A가 암호문 C_A와 재암호화키 $RK_{A\rightarrow B}$를 LRM/RI에게 전송 : DRM Agent(A)가 가지고 있는 권리 암호화 키(REK)는 DRM Agent(A)의 공개키로 암호화되어있는 C_A와 재암호화키 $RK_{A\rightarrow B}$를 지역 권리 관리자(LRM)/권리 발급자(RI)에게 전송한다.
- 지역 권리 관리자가 암호문 C_B를 B에게 전송 : LRM/RI는 $RK_{A\rightarrow B}$를 이용하여 C_A를 C_B로 재암호화한 후에 C_B를 DRM Agent(B)에게 전송한다.

위와 같은 과정을 하고나면 DRM Agent(B)는 자신의 비밀키를 이용하여 권리 암호화 키 REK를 얻을 수 있고, 콘텐츠를 이용할 수 있다.

3.3 분석

OMA DRMv2.x과 SCE 공유 모델에서는 권리 암호화 키(REK)와 MAC값을 AES 대칭키 암호로 암호화할 때 쓰이는 키(KEK)를 구할 수 있는 임의의 수 Z를 RSA 공개키 암호를 사용하였다. 제안하는 모델에서는 이때의 RSA 공개키 암호 대신에 프록시 재암호화 기법을 쓴다. 기존의 방법은 사용자 A가 사용자 B와 콘텐츠를 공유하려 했을 때 지역 권리 관리자나 권리 발급자가 사용자 A의 공개키로 암호화된 키를 복호화한 후에 다시 사용자 B의 공개키로 암호화해 주어야 했다. 그러나 프록시 재암호화 기법을 사용하면 복호화 과정없이 한번의 재암호화 과정으로 사용자 A의 비밀키로 복호화 할 수 있었던 암호문을 사용자 B의 비밀키로 복호화 할 수 있는 암호문으로 바꾸어 줄 수 있다. 제안하는 키 분배 과정에서 지역 권리 관리자/권리 발급자는 DRM Agent들의 공개키로 권리 암호화키를 재 암호화하면서 자연스럽게 콘텐츠와 권리의 공유가 이루어진다. 이때 콘텐츠는 사용자끼리 바로 전송 가능하며, 콘텐츠에 대한 권리는 재 암호화 키와 권리 암호화키 등 데이터의 크기가 작은 키 값들만이 전송되는 효율적인 공유를 할 수 있다. 또한 지역 권리 관리자가 프록시가 되는 환경에서 지역 권리 관리자가 공격을 받았을 때 DRM Agent들의 키 역시 공격자에게 노출될 위험이 있다. 하지만 프록시 재암호화 기법의 특성상 재 암호화 키 RK로는 DRM Agent의 어떠한 비밀값도 알 수 없으므로 공격자가 지역 권리 관리자를 공격했다 하더라도 DRM Agent들의 키 정보를 알 수 없다. 따라서 지역 권리 관리자에 대한 신뢰도를 떨어뜨릴 수 있는 장점이 있게 된다. 지역 권리 관리자/권리 발급자는 가지고 있던 A의 권리 암호화 키 REK_A와 DRM Agent(A)에게 받은 $RK_{A\rightarrow B}$를 가지고 DRM Agent(B)의 REK_B를 생성할 수 있어서 DRM Agent(B)에게서 공개키를 받는 프로토콜을 실행하지 않아도 된다.

재 암호화 기법은 구조의 특성상 여러 가지 성질을 갖는다. 재 암호화 기법을 SCE의 공유 환경에 적용시킬 때 빠져서는 안되는 성질은 단방향성(Uni-directional), 재사용성(Multi-use) 등이다. 공유는 한번으로 끝나는 것이 아니라 지속적으로 이루어질 수가 있기 때문에 재사용성 성질과 단방향성 성질을 만족시키는 재 암호화 기법을 써야 한다. 공유를 할 때마다 암호화된 권리 암호화 키 값이 커지는 것은 매우 비효율적이다. 또한 암호화된 권리 암호화 키 값을 가지고 재 암호화키 $RK_{A\rightarrow B}$를 구할 수 없어야 한다. 재 암호화키가 정당한 사용자이외에 알게 되면 안된다. DRM Agent(B)가 $RK_{A\rightarrow B}$를 구해버리게 되면 지역 권리 관리자/권리 발급자의 허가 없이 콘텐츠를 악용할 수 있게 되기 때문이다.

IV. 스마트카드를 이용한 제안 기법의 확장

앞서 제안한 기법은 사용자의 공개키들을 활용하여 재 암호화 기법을 적용한 것이다. 그러나 이러한 기법은 사용자가 권리 암호화키를 바로 얻을 수 있게 된다. 만약 권리 암호화키를 숨길 수 있다면 악의의 사용자가 권리 암호화키와 권리 발급자를 부적법하게 재

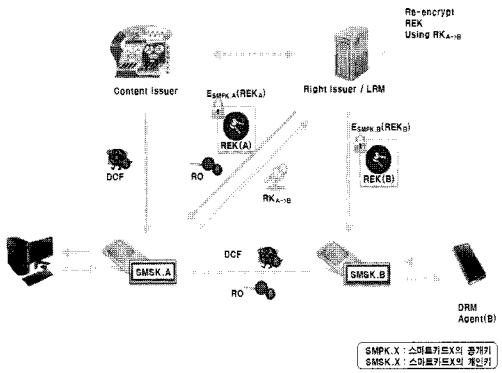
〔그림 3〕 카드 발급 프로토콜

배포하여 DRM 기법을 회피하는 것을 막을 수 있다. 이러한 목적을 달성하기 위하여 스마트카드를 사용할 수 있다. 스마트카드 중에는 조작방지(Temper-proof)기능을 지원하는 것이 있다. 이러한 스마트카드를 활용하여 권리 암호화키가 사용자에게 노출되는 것을 막는 방법을 제안한다. 앞으로 스마트카드에서 조작방지 기능이 되어 있는 부분을 안전한 저장소라고 한다. 스마트카드 제조자는 스마트카드를 제조할 당시에 안전한 저장소 부분에 스마트카드의 비밀키(SMSK: Smarcards'Master Secretk Key)를 저장하여 생산한다. 그리고 이에 대응하는 공개키(SMPK: Smartcards'Master Public Key)는 시스템 전체에 공개한다. 앞에서 설명한 재 암호화 기법을 사용한 DRM 시스템에서는 사용자의 공개키로 권리 암호화 키를 암호화 하였다. 하지만 확장된 제안 기법에서는 사용자의 공개키 대신 스마트카드의 공개키를 사용하여 권리 암호화 키를 암호화 한다. 사용자는 스마트카드의 비밀키를 알 수 없기 때문에 권리 암호화 키 또한 얻을 수 없게 된다. 이를 위하여 스마트카드를 생산할 당시에 다음 그림과 같은 과정을 통해 스마트카드의 비밀키를 안전한 저장소에 저장한다.

4.1 제안하는 확장된 키 분배 방법

지역 권리 관리자(LRM)/권리 발급자(RI)은 권리 암호화 키(REK)를 사용자 A의 스마트카드 공개키로 암호화하여 C_A를 생성하고, 사용자 A의 스마트카드에 권리증서(RO)와 함께 분배한다. 사용자 A는 사용자 B와 콘텐츠를 공유하기 위하여 사용자 B의 스마트카드 공개키와 자신의 스마트카드를 이용하여 재 암호화키 $RK_{A\rightarrow B}$를 생성하고, 이를 지역 권리 관리자(LRM)/권리 발급자(RI)에게 주게 되면, 지역 권리 관리자(LRM)/권리 발급자(RI)는 $RK_{A\rightarrow B}$와 C_A를 이용하여 사용자 B의 스마트카드 공개키로 암호화된 C_B를 생성한 후에 사용자 B의 스마트카드로 전송을 한다.

- LRM/RI이 C_A와 RO를 A에게 전송 : 지역 권리 관리자(LRM)/권리 발급자(RI)는 사용자 A의 스마트카드 공개키를 이용하여 권리 암호화 키 REK를 암호화한 C_A와 RO를 사용자 A의 스마트카드로 분배한다.
- A가 DCF와 RO를 B에게 전송 : 사용자 A는 사용자 B와 콘텐츠 공유를 하기 위하여 자신이 가지고 있는 패키징된 콘텐츠 DCF와 콘텐츠 암호화한 키 CEK가 포함되어 있는 권리증서 RO를 사용자 B의 스마트카드로 전송한다.
- A가 C_A와 $RK_{A\rightarrow B}$를 LRM/RI에게 전송 : 사용자 A는 자신의 스마트카드와 사용자 B의 스마트카드 공개키를 이용하여 $RK_{A\rightarrow B}$를 생성한다. 사용자 A는 C_A와 재 암호화키 $RK_{A\rightarrow B}$ 를 지역 권리 관리자(LRM)/권리 발급자(RI)에게 전송한다.
- LRM/RI가 C_B를 B에게 전송 : 지역 권리 관리자(LRM)/권리 발급자(RI)는 $RK_{A\rightarrow B}$를 이용하여 C_A를 C_B로 재 암호화한 후에 C_B를 사용자 B의 스마트카드에 전송한다.



〔그림 4〕 스마트카드 기반 재 암호화 기법을 이용한 콘텐츠 공유

위와 같은 과정을 거치고 나면 사용자 B는 자신의 스마트카드를 이용하여 권리 암호화 키 REK를 얻을 수 있고, DRM Agent를 통해 콘텐츠를 이용할 수 있다.

4.2 분석

제안하는 키 분배 과정에서 지역 권리 관리자/권리 발급자는 DRM Agent들의 공개키가 아닌 사용자가 가지고 있는 스마트카드의 공개키로 권리 암호화키를 암호화하고 콘텐츠 공유과정에서는 프록시 재 암호화

기법을 통해 콘텐츠와 권리의 공유가 이루어진다. 사용자는 새로운 키 분배과정이 없어도 자신의 스마트카드를 이용하여 소유한 디바이스에 한해 콘텐츠를 자유롭게 이용할 수 있다. DCF와 권리증서는 암호화 되어 있기 때문에 스마트카드의 안전하지 않은 저장 공간에 저장되어도 되며, 스마트카드의 비밀키(SMSK)는 저장되어야 한다. 재 암호화키 생성 연산과 권리 암호화키와 콘텐츠 암호화키의 복호화 연산은 스마트카드의 안전한 공간에서 이루어지기 때문에 스마트카드의 비밀키(SMSK), 콘텐츠 암호화키와 권리 암호화키는 사용자에게 노출되지 않는다.

기존의 시스템에서는 지역 권리 관리자가 공격을 받았을 때 사용자들의 키 역시 공격자에게 노출될 위험이 있었다. 하지만 본 논문에서 제안하고 있는 프록시 재 암호화 기법의 특성상 재 암호화키로는 사용자의 어떠한 비밀값도 알 수 없으므로 공격자가 지역 권리 관리자를 공격했다 하더라도 사용자들의 키 정보를 알 수 없다. 프록시 재암호화 기법에서 프록시는 신뢰되지 않는 3자로 가정을 하고 설계를 하기 때문에 프록시가 여러 사용자간의 재암호화 키를 가지고 있더라도 사용자들의 비밀키나 암호문에 대한 평문의 어떤 정보도 알 수가 없다. 그렇기 때문에 제안한 방법을 사용하면 지역 권리 관리자에 대한 신뢰도를 떨어뜨릴 수 있는 장점이 있게 된다. 지역 권리 관리자/권리 발급자는 가지고 있던 REK_A와 사용자A에게 받은 $RK_{A\rightarrow B}$를 가지고 사용자 B의 REK_B를 생성할 수 있어서 사용자B에게서 공개키를 받는 프로토콜을 실행하지 않아도 된다.

본 장에서 제안한 키 분배 방법은 앞의 장에서 제안한 프록시 재암호화 기법을 이용한 키 분배 기법의 확장이기 때문에 앞의 장에서 제안한 기법의 성질을 갖는다. 재 암호화 기법의 성질인 단방향성, 재사용성 성질과 암호화된 권리 암호화키 값을 가지고 재 암호화키 $RK_{A\rightarrow B}$를 구할 수 없는 성질이 그것이다. [표 2]는 OMA시스템과 제안하는 기법의 차이점을 나타낸다.

OMA 시스템은 콘텐츠와 콘텐츠 암호화키를 암호화하므로 기밀성이 보장되고 MAC을 사용함으로 인해 무결성도 보장된다. 또한 인증기능을 제공하기위하여 콘텐츠 암호화키와 같은 비밀정보가 포함 된 권리증서는 권리 암호화키로 암호화 된 후, 권리 발급자의 개인키로 서명된다. OMA 시스템은 권리 암호화키를 소유한 개체만이 정보에 접근할 수 있기 때문에 접근제어가 가능하며, Nonce를 이용한 시도-응답(Challenge response)과정을 통해 메시지 제거공격에도 안전하다. 또한 전자서명을 통해 임의의 메시지를 삽입할 수 없다. 하지만 OMA 시스템은 DOS 공격과 지역 권리 관리자나 DEA, DRM Agent가 변질(Compromise)되었을 때와 수동적인 공격에 대한 보안은 제공하지 않는다. SCE에서 지역 권리 관리자가 권리 발급자와 콘텐츠 발급자의 정보제공 부하량을 줄여주기는 하지만 DOS공격에 대한 완벽한 대안이 되지는 못한다. 제안하는 기법은 OMA 시스템이 기본으로 제공하는 보안 요구사항은 만족한다. 프록시 재암호화 기법을 사용하기 때문에 지역 권리 관리자 변질(LRM Compromise)를 막을 수는 없더라도 지역 권리 관리자가 알 수 있는 키 정보는 사용자의 공개키뿐이므로 지역 권리 관리자의 신뢰도는 떨어뜨릴 수 있다. 또한 사용자의 비밀키는 스마트카드의 안전한 저장소에 저장되어 있으며, 연산 또한 스마트카드의 안전한 저장소에서 일어나므로 사용자는 콘텐츠 암호화키나 권리 암호화키를 알 수 없어서 DRM Agent가 변질되더라도 콘텐츠와 키 정보는 안전하다.

〔표 4〕 OMA의 표준과 제안한 방법의 비교 분석

	OMA 시스템	제안하는 기법
기밀성	O	O
무결성	O	O
인증	O	O
부인방지	O	O
접근제어	O	O
메시지제거/삽입	O	O
LRM Compromise	X	△
DEA Compromise	X	X
DRM Agent Compromise	X	O
공유시 수행 알고리즘	복호화알고리즘 암호화알고리즘	재암호화 알고리즘

V. 결 론

본 논문에서는 OMA-DRM과 SCE에서 콘텐츠 공유 방법에 대해서 분석을 하였고, OMA-DRM과 SCE의 콘텐츠 공유 환경에서 적용될 수 있는 스마트카드 기반 프록시 재 암호화 기법을 이용한 키 분배 방법을 제시하였다. 재 암호화 기법을 사용함으로서 지역 권리 관리자/권리 발급자가 크기가 작은 권리 암

호화 키의 이동만으로도 콘텐츠의 공유가 어떻게 이루지고 있는지 알 수가 있고, SCE에서는 지역 권리 관리자의 신뢰도를 떨어트릴 수 있는 장점이 있었다. OMA-DRM와 지역 권리 관리자에서 재 암호화 기법을 적용시킬 때 반드시 갖추어야하는 재 암호화 기법의 성질로는 재사용성과 단방향성이 있었다. 이 성질들을 갖추지 않으면 키 분배가 효율적이지 못하고, 안전성이 떨어지게 된다. 또한 스마트카드의 안전한 저장장소를 이용함으로서 키 관리와 복호화 연산에서 기존의 기법보다 나은 안전성을 제공하였고, 사용자가 자신의 디바이스들에서 콘텐츠를 공유할 때의 키 분배 효율성을 높였다.

참고문헌

[1] B. Libert and D. Vergnaud, "Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption," In: PKC 2008. LNCS, vol. 4939, pp. 360 - .379. Springer, Heidelberg 2008.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM TISSEC 9(1), pp. 1 - .30 Feb. 2006

[3] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," In: Proceedings of Eurocrypt '98. Volume 1403. pp. 127 - 44, May. 1998

[4] M. Green and G. Ateniese, "Identity Based Proxy Re-encryption," In: Katz. J, Yung. M, (eds.) ACNS 2007. LNCS, vol. 4521, pp. 288 - .306. Springer, Heidelberg 2007.

[5] OMA: DRM Specification-OMA-TS-DRM_DRM-V2_1-20081106-A. Available online at http://www.openmobilealliance.org/Technical/release_program/drm_v2_1.aspx, 2008

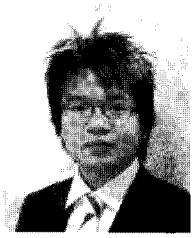
[6] OMA: DRM Specification-SCE Extension -OMA-TS-SCE_DRM-V1_0-20090526-C. Available online at http://www.openmobilealliance.org/Technical/release_program/SCE_v1_0.aspx, 2009

[7] OMA: Local Right Manager for Secure Content Exchange-OMA-TS-SCE_LRM-V1_0-20090526-C. Available online at http://www.openmobilealliance.org/Technical/release_program/SCE_v1_0.aspx, 2009

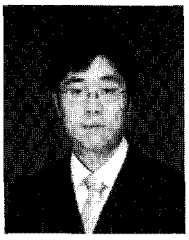
[8] OMA: Secure Content Exchange Architecture - OMA-AD-SCE -V1_0-20081209-C. Available online at http://www.openmobilealliance.org/Technical/release_program/SCE_v1_0.aspx, 2008

[9] 박승환, 구우권, 김기탁, 이동훈, "프록시 재암호화 기법을 이용한 콘텐츠 공유 메커니즘에 관한 연구," 정보보호학회 동계학술대회, 12월. pp. 229-233, 2009년 12월.

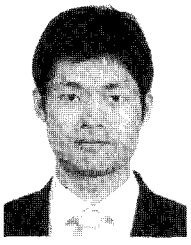
〈著者紹介〉



박 승 환 (Seunghwan Park) 학생회원
2009년 2월: 숭실대학교 수학과 학사 졸업
2009년 3월~현재: 고려대학교 정보경영공학과 석사과정
〈관심분야〉 정보보호이론, 암호 프로토콜, 프라이버시향상기술(PET)

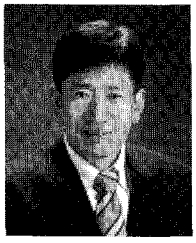


구 우 권 (Woo Kwon Koo) 학생회원
2006년 2월: 고려대학교 수학과 학사 졸업
2008년 2월: 고려대학교 정보경영공학과 공학 석사 졸업
2008년 3월~현재: 고려대학교 정보경영공학과 박사과정
〈관심분야〉 정보보호이론, 암호 프로토콜, 프라이버시향상기술(PET)



김 기 탁 (Kitak Kim) 학생회원
2006년 8월: 고려대학교 수학과 졸업
2008년 8월: 고려대학교 정보경영공학과 공학 석사 졸업
2008년 9월~현재: 고려대학교 정보경영공학과 박사과정
〈관심분야〉 정보보호이론, 암호 프로토콜, 프라이버시향상기술(PET)

문 혜 란 (Hyeran Mun) 정회원
2007년: 서울여자대학교 정보보호공학 학사 졸업
2009년: 한국과학기술원 정보통신공학 석사 졸업
2009년~현재: 한국전자통신연구원 지식정보보호연구팀 연구원
〈관심분야〉 콘텐츠 보호, 이동통신 보안



이 동 훈 (Dong Hoon Lee) 정회원
1983년: 고려대학교 경제학과 학사 졸업
1987년:Oklahoma University 전산학 석사 졸업
1992년:Oklahoma University 전산학 박사 졸업
1993년~1997년:고려대학교 전산학과 조교수
1997년~2001년:고려대학교 전산학과 부교수
2001년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 정보보호이론, 암호 프로토콜, USN, 키 교환, 프라이버시향상기술(PET), 익명성 연구