무선환경에서의 디지털 저작권 관리 기술

주학수, 김대엽°, 김지연, 박해룡, 이재일
한국정보보호진흥원, 삼성종합기술연구소°

Digital Rights Management System in the wireless environment

Hak-Soo Ju, Dae-Youb Kim°, Jee-yeon Kim, Hae-ryong Park, Jae-il Lee
KISA, SAIT°

요 약

인터넷 통신의 빠른 발전에 따라 인터넷은 상거래에서 디지털 컨텐츠의 분배를 위한 가장 효율적인 통신로가 되었다. 현재 이 통신로는 무선 환경으로 넓혀지고 있다. 디지털 컨텐츠의 특성상 불법복제와 유통으로 인한 저작권 침해문제가 발생하였고, 이를 해결하기 위해 DRM(Digital Rights Management)기술을 이용하게 되었다. 이에 본 논문에서는 무선환경에서의 DRM에 대한 기술들을 분석하고자 한다.

1. 서론

무선에서의 컨텐츠를 보호할 수 있는 기술은 사용되는 기반 암호기술에 따라, 크게 2가지로 분류할 수 있다. PKI기반의 DRM 기술을 그대로 무선에서 사용하는 무선 PKI기반 DRM 방법과, 공개키 기반이 아닌 브로드캐스트 암호화(Broadcast Encryption) 방법을 기반으로 컨텐츠를 보호하는 방법이 있다.

먼저 무선 PKI 기반한 DRM 방식은 PKI 기반 DRM 모델과 유사하게 설계할 수 있다. 단, 컨텐츠를 모바일과 같은 단말기에 다운받는 방식만 차이가 있을 뿐이다. 본 논문에서는 무선 PKI 기반 DRM방식에 대해 알아본다.

한편, PKI가 아닌 브로드캐스트 방법을 주로 사용하고 있는 곳은 홈네트워킹에 사용되는 4C 사의 xCP Cluster 프로토콜 등이 있다. 본 논문에서는 이 브로드캐스트 암호화 방식과 이 프로토콜 방식에 대해 설명하고자 한다.

2. 무선환경에서의 DRM 기술

2.1 모바일 DRM(MDRM : Mobile Digital Rights Managements) 기술

다양한 DRM 기술들이 현재 서로 경쟁을 하고 있지만 보편적으로 사용될 수 있는 DRM 표준은 없는 상태이다. IBM社, Intertrust Real Networks社, Sony社 등이 자신들의 기술을 서로 호환되게 하는 기술들을 만들고 있으며 MS社 또한 Window Media DRM을 업체 표준으로 만들려고 하는 중이다. 향후 모바일 영역에서도 유사하게 표준화를 위한 충돌이 예상되고 있다.

OMA(Open Mobile Alliance)가 벨소리, MMS (Multimedia Messaging Service)를 대상으로 하는 모바일 DRM을 표준화하였고 현재 Nokia 등과 같은 선두 단말기 제조업체들이 자신들의 제품에 이 표준을 구현하고 있다. 그러나, IBM社, MS社, Real Network社 등과 같은 선두 DRM 업체들은 플랫폼에 독립적인 DRM 제품을 만들었으며, 이를 이용하여 모방일 플랫폼에 적합한 솔루션들을 제공하고 있다.

또한, 1998년 설립된 3GPP(The 3rd Generation Partnership Project)도 2003년 6월 3GPP Release 6에 DRM 표준을 포함시킬 계획이며, GSM Association이 무선 인터넷 응용을 위한 발판 마련을 목표로 설립한 M-Service Initiative에서 발행하는 M-Service Guidelines Phase II에서 DRM을 향후 진행될 영역으로 분류하고 있다[1]. 이에, 이 절에서는 모바일 DRM 기술에

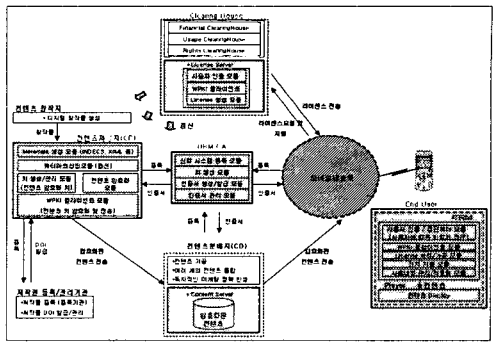
대해 설명하고자 한다.

가. 무선 PKI기반의 모바일 DRM

일반적으로 모바일에서의 DRM의 구조는 앞 절에서 설명된 일반적인 DRM의 구조에서 설명하였듯이, 패키지 단계, 판매단계, 소비단계, Super-distribution 단계로 분류할 수 있다. 패키지(Package) 단계는 컨텐츠 저자와 제공자가 컨텐츠의 암호화, 컨텐츠에 대한 사용권한 및 정책설정 등을 수행하고, 판매단계는 서비스 제공자가 해당 컨텐츠를 보호하고 사용자에게 분배하는 단계로 구성된다. 소비단계에서 사용자는 해당 컨텐츠를 이용하기 위해 컨텐츠에 대한 라이센스를 지불을 통해 획득하고 superdistribution 단계에서 다른 사용자에게 암호화된 컨텐츠를 다른 사용자에게 분배할 수 있다.

현재 PKI기반 모바일 DRM은 3GPP Release 6에서 표준화가 될 예정[1]이며 아직까지 문서로 공개되어 있지는 않다. 무선 PKI 기반한 MDRM 방식을 PKI 기반 DRM모델과 유사하게 설계를 하면 그림 1과 같다. PKI기반과 유사하게 WPKI기술은 참여하는 모든 거래 당사자들의 인증기능을 제공해 줄 수 있어, MDRM의 참여자들은 기본적으로 WPKI의 CA서버에 등록되어 있는 것으로 가정할 수 있다. 그림 1에서 알 수 있듯이 컨텐츠 제공자(CP)와 DRM 서버가 CA에 등록되어 있으며, 사용자는 클라이언트 S/W를 모바일에 설치후 공개키 개인키 쌍을 생성하여 등록하는 방식으로 구성할 수 있다. 컨텐츠 B2B거래 주체들(예를 들어, CP와 CD간)의 거래 전에 먼저 인증과정과 DRM 서버와 클라이언트간의 인증과정이 있을 수 있으며, DRM 클라이언트들간의 인증(예 : 모바일을 이용한 superdistribution[2])이 공개키 인증서를 통해 이루어질 수 있다. 또한, 거래되는 컨텐츠 및 라이센스가 정당한 컨텐츠 분배자, 제공자로부터 배포된 것인지를 확인하기 위해 공개키 기반구조에서 사용되는 전자서명 및 해쉬함수가 기본적으로 사용될 수 있다.

단, 본 논문에서는 일반적인 DRM모델에서와 유사하게 라이센스를 구매하기 위해 필요한 안전한 전자결제시스템을 가정하였듯이 모바일을 이용한 전자결제방식이 있다는 것을 가정한다.



(그림 1) 무선 PKI기반 DRM 모델

그림 1의 모바일 네트웍은 인증서를 다운받는 부분과 컨텐츠 및 사용규칙을 다운로드받는 방식으로 분류할 수 있다.

인증서를 다운로드받는 방식의 경우, 크게 WAP PKI방식과 ME PKI방식이 표준으로 제시되고 있다. WAP에서의 PKI기술은 기본적으로 WTLS 계층의 보안을 전제로 전체 PKI를 설명하고 있으며, ME에서는 SSL기반의 보안을 전제로 PKI가 구축되었다.

WAP방식은 현재 2.0이 발표된 상태이며 무선망과 기존의 유선인터넷망을 연동하기 위해 WAP게이트웨이를 두고 있다. 사용자의 단말기와 게이트웨이는 WAP에서 정의된 프로토콜로 통신이 이루어지며, 게이트웨이와 기존 유선망과의 통신은 HTTP를 통하여 이루어진다. ME방식은 WAP게이트웨이가 할 일을 무선단말기내의 브라우저가 하도록 하고 있으며, 내부적으로 기존의 HTTP방식과 호환이 되며 HTML을 축약한 M-HTML을 사용하고 있다.

컨텐츠 및 사용규칙을 다운로드받는 방식으로, 현재 사용되는 방식은 벨소리, 아이콘 등을 다운받기 위해 SMS을 사용하는 방법과 자바(MIDP) 어플리케이션을 다운받을 수 있는 자바 표준[3]이 있다. 최근 일반적인 컨텐츠를 다운로드 받는 방식에 대한 표준으로 OMA가 표준화를 하였다[4].

2.2 홈네트워킹의 컨텐츠 보호기법

컨텐츠 보호를 위한 브로드캐스트 암호화를 상업화시키기 위해 IBM사, Intel사, Matsushita사, Toshiba

1) 표준화의 현상태는 3GPP와 OMA의 회원들에게만 알려져 있는 상태임

2) superdistribution이란 암호화된 컨텐츠를 보유하고 있는 사용자가 다른 사용자에게 전달할 수 있도록 하며 컨텐츠를 전달받은 사용자가 암호화된 컨텐츠를 이용하기 위해서는 라이센스를 따라 발급받도록 하는 배포방법

3) Java Community Process(JCP)는 Java 컨텐츠(MIDP application)를 다운로드 받는 방법을 표준화하였으며 이는 MIDP OTA 표준 명세서에 설명되어 있음

4) 2002년 2월부터 WAP 포럼(현재는 OMA로 통합됨)이 모바일 DRM 표준화를 시작하였으며, OMA는 현재 "Digital Rights Management Version 2.0"을 공개한 상태에 있음

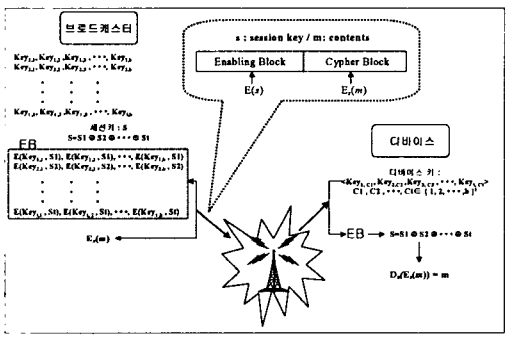
사는 1998년 4C Entity 회사를 설립하였고 DVD등과 같은 Recodable Media의 컨텐츠 보호기술(CPRM : Content Protection for Recordable Media technology)을 개발하였다. 현재 CPRM을 사용하는 디바이스는 DVD 오디오 플레이어, DVD 비디오 레코더, 그리고 플레쉬 메모리를 이용한 플레이어에 탑재되어 상용화되고 있다. 또한, 홈네트워킹에서 사용되는 모든 컨텐츠들의 보호를 위해 CPSA라는 컨텐츠 보호시스템을 개발하였으며, 이 CPSA에 기반 프로토콜로 xCP프로토콜을 사용하고 있다. 이 xCP프로토콜은 브로드캐스트 암호를 상업화에 처음으로 적용한 프로토콜이다[5]. 이 절에서는 먼저 브로드캐스트 방법에 대해 알아보고 4C가 개발한 xCP 프로토콜에 대해 설명하고자 한다.

가. 브로드캐스트 암호화

브로드캐스트 암호화은 실제 컨텐츠를 세션키 S를 사용해서 암호화한 암호블럭(Cyper Block)과 그 세션키를 모든 사용자들에게 브로드캐스트하기 위해 만든 권한블럭(Enabling Block)으로 구성된다. 합법적인 개인키를 갖고 있는 임의의 디바이스는 권한블럭으로부터 세션키를 얻어낼 수 있고 세션키로 암호화된 실제 컨텐츠를 암호블럭으로부터 계산할 수 있다.

전체 브로드캐스팅 암호화 과정을 설명하기 위해, Naor의 방법[2]을 예를 들어 설명하면 다음과 같다.

<브로드캐스팅 암호화 방법 예 : Naor 방법[2]>



(그림 2) 브로드캐스트 암호화 방법 예

- 브로드캐스터(컨텐츠 제공자) 설정 : 브로드캐스터는 b개의 키를 갖는 t개의 집합을 생성한다. 여기서는 i번째 집합을 key{i,1},…,key{i,b}로 표기하기로 한다.
- 디바이스(사용자) 설정 : 각각의 디바이스는 브로드캐스터가 생성한 t 개의 집합으로부터 하나씩의 키를 획득하게 된다. 디바이스는 자신만의 id에 대응하는 코드워드 (c1,c2,…,ct)∈{1,2,…,b}t에 대응하는 디바이스 키 key{1,c1},…,key{1,ct}를 브로드캐스트되는 EB(Enabling Block)을 통해 얻게된다.
- 세션 송신 : 컨텐츠 제공자는 각 세션키 S를 t개의 랜덤한 부분 세션키 S1, S2,…,St의 값들을 XOR하여 만든다. 모든 집합들에 대하여 세션블럭은 i번째 집합에 있는 키들을 가지고 각각의 부분 세션키 Si를 암호화한 값으로 구성된다. 디바이스는 각 i번 째 집합에 대응하는 하나의 키들을 갖고 있기 때문에 b개의 암호문 중에서 하나를 암호문을 복화화 할 수 있고 따라서 전체 세션키 S를 얻어냄으로써 실제 컨텐츠를 복호화 할 수 있다.

공개키 암호방식에 비해 브로드캐스트 암호 방식의 장점은 크게 두 가지를 생각할 수 있다. 첫째, 브로드캐스트 암호화 방법은 대칭형 암호알고리즘을 사용하기 때문에 공개키 암호방식보다 빠르며 또한 디바이스로 하여금 낮은 오버헤드를 갖게 함으로써 디바이스 제조업자와 사용자들의 비용을 적게 들게 한다. 둘째, 프로토콜이 일방향으로 진행됨으로써, 공개키 방식의 양방향 프로토콜 방식보다 안전하다는 점이다[3]. 보통 공개키 시스템은 링크레벨에서 암호키를 공유하기 위한 핸드쉐이크 과정이 일어나는데, 이 과정에서 두 개의 취약점을 가지고 있다. 먼저 비밀키를 찾기가 쉽고, 컨텐츠가 보호되지 않는 인터페이스를 찾기가 더 쉽다. 실제 사례로 Beale Screamer가 공개키 암호시스템을 사용하고 있는 Windows Media Player을 공격하여 성공하였다[4].

전체 시스템에서 손상된 개인키를 폐지할 수 있는 방법은 중요하다. 공개키 암호방식에서 손상된 개인키를 폐지시키기 위해서는 인증서 폐지 리스트를 전달하여야 하는데 시간이 지날수록 인증서 폐지 리스트의 크기가 커져 비효율적이다. 반면, 브로드캐스트 방식에서는 브로드캐스트 되는 정보 중 키 관리 블록에 폐지 정보를 삽입하여 손상된 개인키를 폐지시킴으로써 공개키 암호의 이점이었던 개인키를 폐지할 수 있는 방법을 해결할 수 있었다. 공개키 암호방식과 유사하게 브로드캐스트 방식에서도 인증서 폐지 리스트의 크기를 줄이는 방식이 중요한 이슈였지만, 최근 Dalit Naor[6]가 공개키 방식에서의 인증서 폐지 리스트의 크기만큼 키관리 블록을 줄일 수 있는 방법을 제시하였다. 그러나, 공개키 암호방식에 비해 브로드캐스트 암호방식의 단점은 부인봉쇄 서비스를 지원해주는 전

자서명기능을 제공하지 못한다는 점이다. 브로드캐스트 암호방법을 사용하는 홈네트워킹과 같은 응용환경에서 정당한 디바이스들만이 프로토콜에 참여할 수 있게 하기 위해 전자서명 대신 MAC값을 계산하도록 하고있다.

따라서, 브로드캐스트 암호화가 공개키 암호방식보다 속도 및 키관리 부분에서 더 효율적이지만, 공개키 암호방식이 지원해주는 전자서명 기능을 제공하지 못하기 때문에, 통신하는 상대방의 실제 ID를 인증해주어야 하는 전자화폐의 전달(Electronic Funds Transfer), SSL 등과 같은 응용환경에는 적합하지 않다[3].

나. IBM사의 xCP Cluster Protocol

4C 사는 홈네트워킹[5]에서 컨텐츠 보호를 위한 컨텐츠 보호 시스템 구조 CPSA(Content Protection System Architecture)를 개발하였다. CPSA는 컨텐츠 보호를 위해 워터마킹과 암호화를 이용하여 아날로그와 디지털 컨텐츠를 모두 보호하는 구조로 구성되어 있다. 현재 CPSA에서 사용되는 저작권 보호기술은 아래와 같다.

- DVD 또는 Flash와 같은 녹화 가능한 미디어의 저장을 보호하기 위한 CPRM (Content Protection Recording Module)
- Pre-recorded DVD-audio를 보호하기 위한 CPPM (Content Protection for Pre-recorded Media)
- Pre-recorded DVD video를 보호하기 위한 CSS (Content Scrambling System)
- IEEE 1394와 USB를 통한 디지털 전송 중 컨텐츠를 보호하기 위한 DTCP(Data Transmission Copy Protection)
- 디지털 디스플레이어와의 high-bandwidth 인터페이스 접근을 보호하기 위한 HDCP(High-bandwidth Digital Content Protection)
- 케이블이나 위성을 통한 컨텐츠의 전달을 보호하기 위한 조건적 접근제어
- 음성용 CMI 워터마크의 삽입과 추출을 위한 4C/Verance 워터마킹 기법[6]
- DVD CCA(Copy Control Association)[7]에 의해 선택된 비디오 워터마킹 기법

xCP 홈네트워크란 암호로 보호된 영역(Encrpytion Domain)으로 CPSA박스로 생각할 수 있다. 컨텐츠 소유자는 CPSA에서의 워터마킹 기술을 사용하여 컨텐츠 보호 및 복사를 제어(CCI : Copy Control Information)할 수 있다. 그러나, 홈네트워크 안에서는 아무런 제약없이 디바이스에서 디바이스로 이동 및 저장할 수 있으며, 보호된 컨텐츠가 CPSA 박스를 벗어나면 컨텐츠는 CPRM 혹은 DTCP를 통해 외부로 전송된다.

홈네트워크 안에서 디바이스들은 클러스터(Cluster)[8]를 형성하고 있으며, 하나의 클러스터에 있는 모든 디바이스들은 통신객체(peer)로 생각할 수 있다. 한 클러스터 안에는 media key block을 관리하고 업데이트 시킬 수 있는 하나의 mkbserver와 새롭게 가입하고자 하는 디바이스를 허가해주는 권한(authorizer)서버, 그리고 xCP clients인 디바이스들로 구성된다. xCP 클러스터에서는 사용자가 디바이스를 구매하고 자신의 홈에 인스톨시킬 때, 디바이스는 자동으로 클러스터에 있는 디바이스 들 중 어떤 것이 권한서버(authorizer)인지를 인식하고, 권한서버에게 클러스터에 가입하는 것을 요청하도록 되어있다. 그러나, 새로운 디바이스를 추가하는 것이 한 클러스터의 기준치를 벗어난다면 외부 관리 센터(external authorization center)에 자동으로 연결되도록 구성된다[5].

클러스터에 있는 컨텐츠 혹은 컨텐츠 스트리밍은 하나의 키로 보호되는데 이러한 키들을 "title key"라 부른다. 각 "title key"는 "binding key"라 하는 홈에 있는 마스터키로 암호화된다. 컨텐츠를 플레이시키기 위해, 디바이스는 컨텐츠 파일에 삽입된 암호화된 "title key"를 읽어서 "binding key"로 복호화한다. 그리고 나서 "title key"로 디바이스는 암호화된 컨텐츠를 복호화하여 플레이 할 수 있다.

이 때 사용되는 "binding key"는 "media key", 네트웍의 "binding ID", 네트웍의 "auth.table"의 해쉬값으로 계산된다.

Kb = G(Km , IDb⊕hash(auth-table))

- Kb : binding key
- Km : media key
- IDb : binding ID
- G : DES와 같은 일방향 함수

이 때 media key Km 은 media key block으로부터

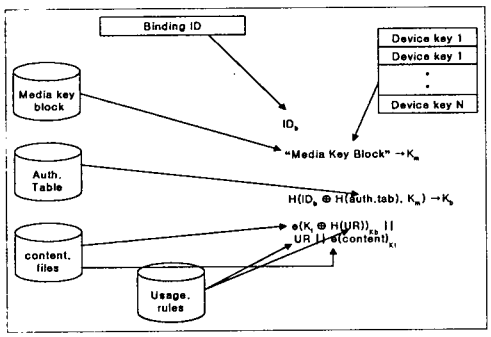
5) 홈 네트워킹이란 정보를 처리, 관리, 전달 및 저장함으로써 가정 내의 여러 계산, 관리, 감시 및 통신 장치들을 연결 및 통합할 수 있게 해주는 구성요소들의 모임이며, 이는 데이터와 통신의 공유와 상호이동을 가능하게 하는 2 개 이상의 장비(노드)의 조합을 말함

6) http://www.verance.com

7) http://www.dvdcca.org

8) 인접해 있거나 기능적으로 유사하여 하나의 단위로 취급되도록 구성하는 방법

계산되어진다. 이 media key가 브로드캐스트 암호화에서의 세션키에 해당한다고 생각할 수 있다. 정당한 디바이스들에게는 media key를 복호화 할 수 있는 자신만의 키 정보를 갖고 있다. 이 방법은 기본적으로 브로드캐스트 암호의 안전성에 의존하고 있기 때문에, 정당하지 않은 디바이스가 media key를 알 수 없게 함으로써 binding key를 계산할 수 없게 하고 title key를 복호화할 수 없게 해 최종적으로 컨텐츠를 복호화할 수 없게 만든다. 두 번째 요소인 네트웍 binding ID는 네트웍에 연결된 첫 번째 서버에 의해 수행되며 ID가 네트웍 밖으로 알려지지 않도록 유지된다. 정당한 디바이스들은 이 ID를 비밀로 유지한다. 세 번째 요소인 네트웍 "authorization table"은 단순한 파일로 구성되어 있지만, 이 값을 binding key 계산에 포함하여 네트웍에 있는 디바이스들을 서로 고립시켜 네트웍에서의 "Man-in-the-middle-attack"을 방지한다. 안전성을 위해, binding key는 새로운 디바이스가 홈에 들어오거나 혹은 "media key block"이 외부로부터 가져올 때마다 변경된다. "binding key"가 변경될 때마다, 클러스터에 있는 모든 디바이스는 모든 "title key"를 다시 암호화한다. 위와 같이 일어나는 브로드캐스트 암호 기반의 xCP Protocol 방식을 정리하면 그림 3과 같다.



(그림 3) xCP Cluster 프로토콜의 세부 구조

3. 결론

디지털 컨텐츠의 불법복제와 유통으로 인한 저작권 침해문제를 해결하기 위해 DRM(Digital Rights Management)기술이 최근 이슈가 되고 있다. 본 고에서는 먼저 DRM 기술의 정의, 기본모델, 요소기술들에 대해 알아보고 PKI를 기반으로 하는 DRM 모델과 DRM의 보안체계에 대해 설명하였다.

그리고 무선에서의 컨텐츠를 보호할 수 있는 기술을 살펴보기 위해 사용되는 기반 암호기술에 따라 크게 2가지로 분류하여 설명하였다. 먼저 PKI기반의 DRM 기술을 그대로 무선에서 사용하는 무선 PKI기반 DRM 방법과, 공개키 기반이 아닌 브로드캐스트 암호화(Broadcast Encryption) 방법을 기반으로 컨텐츠를 보호하는 방법으로 분류하였다. 특히 후자의 경우, 브로드캐스트 암호화를 처음 홈네트워킹에 적용시킨 IBM社의 xCP Cluster 프로토콜 방식에 대해 설명하였다.

공개키 암호방식(PKI)과 브로드캐스트 암호방법의 기본적인 차이는 공개키 암호방식이 통신하는 참여자의 실제 ID를 보장해주는 방법인 반면 브로드캐스트 암호방법은 참여자로 하여금 다른 참여자가 같은 그룹에 소속되어 있다는 것을 보장해주는 방법이라는 점이다. 브로드캐스트 암호화가 공개키 암호방식보다 속도 및 키관리 부분에서 더 효율적이지만, 공개키 암호방식이 지원해주는 전자서명 기능을 제공하지 못하기 때문에, 통신하는 상대방의 실제 ID를 인증해주어야 하는 전자화폐의 전달(Electronic Funds Transfer), SSL 등과 같은 응용환경에는 적합하지 않다. 따라서, 응용환경에 따라 공개키 기반구조를 사용할지 브로드캐스트 암호방식으로 키 관리를 할지를 결정하여야 한다.

[참고문헌]

[1] Tobias Ryberg, "Mobile content protection and DRM', 2002.

[2] Amos Fiat, Moni Naor, "Broadcast Encryption", Advances in Cryptology(Crypto93), Lecture Notes in Computer Science 773, Springer-Verlag, New York, 1994.

[3] Jeffrey Lotspiech, Stefan Nusser, Florian Pestoni, "Broadcast Encryption's Bright Future", IEEE Cover Feature, 2002.8.

[4] http:/cryptome.org/ms-drm.htm

[5] IBM Research Division Almaden Research Center, "xCP eXtensible Content Protection"

[6] D.Naor, M.Naor, and J.Lotspiech, " Revocation and Tracing Routines for Stateless Receivers," Advances in Cryptology(Crypto 2001), Lecture Notes in Computer Science 2139, Springer-Verlag, New York, 2001.