신기술 논고

방송환경에서의 일반적인 제한수신 구조

은성경, 김신효, 조현숙
한국전자통신연구소

— 요 약 —

방송사업자가 광고 및 저작권료에 의지하지 않고 전문적인 방송을 가능케하는 유료방송은 제한수신 서비스로 가능하다. 본 논문에서는 제한수신 서비스의 종류와 이를 가능케하는 제한수신 시스템의 기능/구조/동작원리에 대하여 기술하여 방송환경에 적용할 수 있는 일반적인 제한수신구조를 제시한다.

1. 서 론

현재 유럽을 비롯한 많은 선진국에서는 방송 서비스 개념이 구조적, 기술적으로 많은 변화가 일어나고 있다. 우리나라도 기존의 정부 주도하의 공영 TV 서비스로부터 민영화에 따른 방송사업자의 구조적인 변화와 더불어, 인간의 기본 욕구가 경제 발전으로 인해 어느 정도 성취됨에 따라 이제는 오락(entertainment)에 대한 또다른 욕구가 일어나게 되었다.

이러한 변화는 광고 및 저작권료만으로 방송 사업을 운영해 오던 지상 TV방송 서비스가 이제는 한계에 부딪치게 되어 이에 대처할 수 있는 몇가지 방안 즉, 케이블네트웍과 직접방송위성(Direct Broadcasting Satellite)을 이용한 새로운 기술들의 개발은 시청자들에게 보다 많은 프로그램과 양질의 방송을 제공하는 유료-TV 및 Pay-Per-View 서비스를 가능케 하였다. 이로써 사청자는 다양한 프로그램중 본인이 원하는 프로그램을 선정하여 시청한다는 가입자 위주의 서비스로 바뀌게 되었다.

제한수신 시스템이란 방송에 가입자 개념을 도입하여 정당한 시청 권한을 가진 가입자만이 프로그램을 수신할 수 있게하는 시스템으로, (EBU-FM)이의 적용은 가입자 대비 광고료 산출을 가능케 하여 방송 사업자들이 광고료 없이 시청료만으로 방송사 운영이 가능할 수 있게 하여 전문적인 방송을 가능케 한다.

본 논문에서는 제한수신 서비스의 종류에 대해서 알아보고, 이러한 서비스의 실현에 필요한 기능 및 시스템의 구조에 대하여 논한다.

2. 제한수신 서비스의 종류

- Subscription
  시청자들이 일정기간 동안, 즉 월 단위 또는 분기 별로 프로그램을 구매하여 시청하는 서비스로서, 가입 방법은 주제별(스포츠, 음악 등), 개별 프로그램별로 가능하다.
- Pre-Booked Pay-Per-View
  시청자들은 이미 각 가입자들에게 알려진 프로그램 정보를 통해서 본인이 시청을 원하는 특정 프로그램을 관리 센터에 알려 주어 해당 시간에 프로그램을 시청할 수 있는 방법이다.
- Impulse Pay-Per-View
  시청자들이 프로그램 방송중 혹은 방송 바로 시작 전에 프로그램을 선정하여 중앙의 관리 센터의 직접적인 개입 없이 본인의 수신기 조작만으로 해당 프로그램을 시청할 수 있는 방법이다.
- Maturity Rating
  주로 성인용 프로그램에 해당하는 서비스로서 프로그램

에 등급을 주어 서비스 신청시 PIN(Personal Indentification Number)을 관리 센터에 등록하고 시청자가 해당 프로그램을 시청하고자 할때 미리 등록해 놓은 등급과 비교를 하여 서비스를 실시하므로 성인용 프로그램에 무방비로 노출될 수 있는 청소년들을 보호할 수 있는 방법이다.

▫ Blackout

지역 코드를 부여하여 서비스 제공 가능 지역이외에서는 시청이 불가능하게 하는 방법으로 다민족/다언어 국가에서는 유용하게 이용할 수 있다.

3. 제한 수신 시스템의 기능

제한 수신 시스템의 실현을 위새서 다음 3가지 기능 즉, 원래의 신호를 특정 가입자에게만 해석할 수 있도록 하기 위한 스크램블링/디스트램블링 기능(Scrambling /Descrambling Function), 자격 제어 기능(Entitlement Control Function) 및 시청 권한의 부여를 위한 자격 관리 기능(Entitlement Management Function) 등이 요구된다. 〈EBU-FM〉, 〈EBU-GC〉

▫ 스크램블링/디스크램블링 기능

스크램블링은 원래의 신호에 변형을 가하여 스크램블된 형태의 신호만으로는 수신 권한이 없는 수신자는 시청할 수 없도록 하는 것으로 신호의 종류(Video/Audio/Data) 및 신호의 형태(Analoge/Digital)에 따라 스크램블링 방식이 달라질 수 있다. 디스크램블링은 제어 단어(Control Word, CW)를 취득할 수 있는 수신자만이 가능하다.

▫ 자격 제어 기능

자격 제어 기능은 난수 발생 초기치인 CW를 디스크램블링에 이용토록 암호화하여 자격 제어 메시지(Entitlement Control Message, ECM)에 실어서 수신자에게 전달하는 기능으로서 주기적으로 전송되며 그때마다 새로운 CW가 암호화된다. ECM내에는 암호화된 CM외에 Control Parameter가 전송된다. 모든 수신기는 전송된 자격 통제 메시지를 수신할 수 있으며 그 중 Control Parameter와 Authorization Parameter와 비교하여 정당한 수신자로 판명되면 스마트 카드내의 서비스 키를 이용하여 CW를 해독하고 디스크램블링에 필요한 난수의 초기치를 발생한다.

▫ 자격 관리 기능

자격 관리 기능은 수신기에 자격을 부여하거나 갱신하는 기능을 지원하며 확장된 자격관리시스템에서는 각 수신자의 주소에 의한 인식 기능을 이용하여 각 수신자의 서비스 키를 바꾸거나 통제하는 통제 취득 기능의 지원도 가능하다. 자격 관리 기능은 미래의 프로그램에 대한 정보관리 기능이므로 배치동작으로 처리된다. 따라서 전송할 프로그램과 동기화되어 전달될 필요는 없으며 자격 정보(Entitlement)는 특수 채널을 통해 방송되거나 우편 등의 매체로도 전달 가능하다.

그림 1은 위에서 언급한 제한수신 서비스의 각 기능별 연결관계와 송신부의 동작을 보여준다.

4. 제한 수신 시스템의 구조

그림 2는 제한수신 시스템의 논리적인 구조를 보여준다.

4.1 송신부

▫ Scrambler

인코더에 의하여 디지털로 변환된 소스 신호는 Scrambler에 의하여 단순한 방법으로는 알아볼 수 없는 행태로 변환된다. Scrambler는 여러가지 형태로 구현될 수 있지만 그 한가지로 PRBS(Pseudo Random Bit Sequencer)를 이용하는 것을 생각할 수 있다. PRBS는 초기화 단어(Initialization Word)에 의하여 초기화되어 임의의 비트열을 발생시킨다. Scrambler는 PRBS에서 발생된 비트열과 소스의 비트열을 혼합하여 알아볼 수 없는 형태의 비트열을 생성한다.

▫ 초기화 단어 생성기(Initialization Word Generator)

초기화 단어 생성기는 Control Word와 소스에서 추출한 Clock 정보에 의하여 조종된다. PRBS는 Control Word만으로도 초기화 될 수 있지만 Control Word를 자주 생성 해야 하는 번거로움을 덜기 위하여 Clock정보를 이용하여 변화를 줄 수 있도록 한 것이다.

▫ 제어 단어 생성기(Control Word Generator)

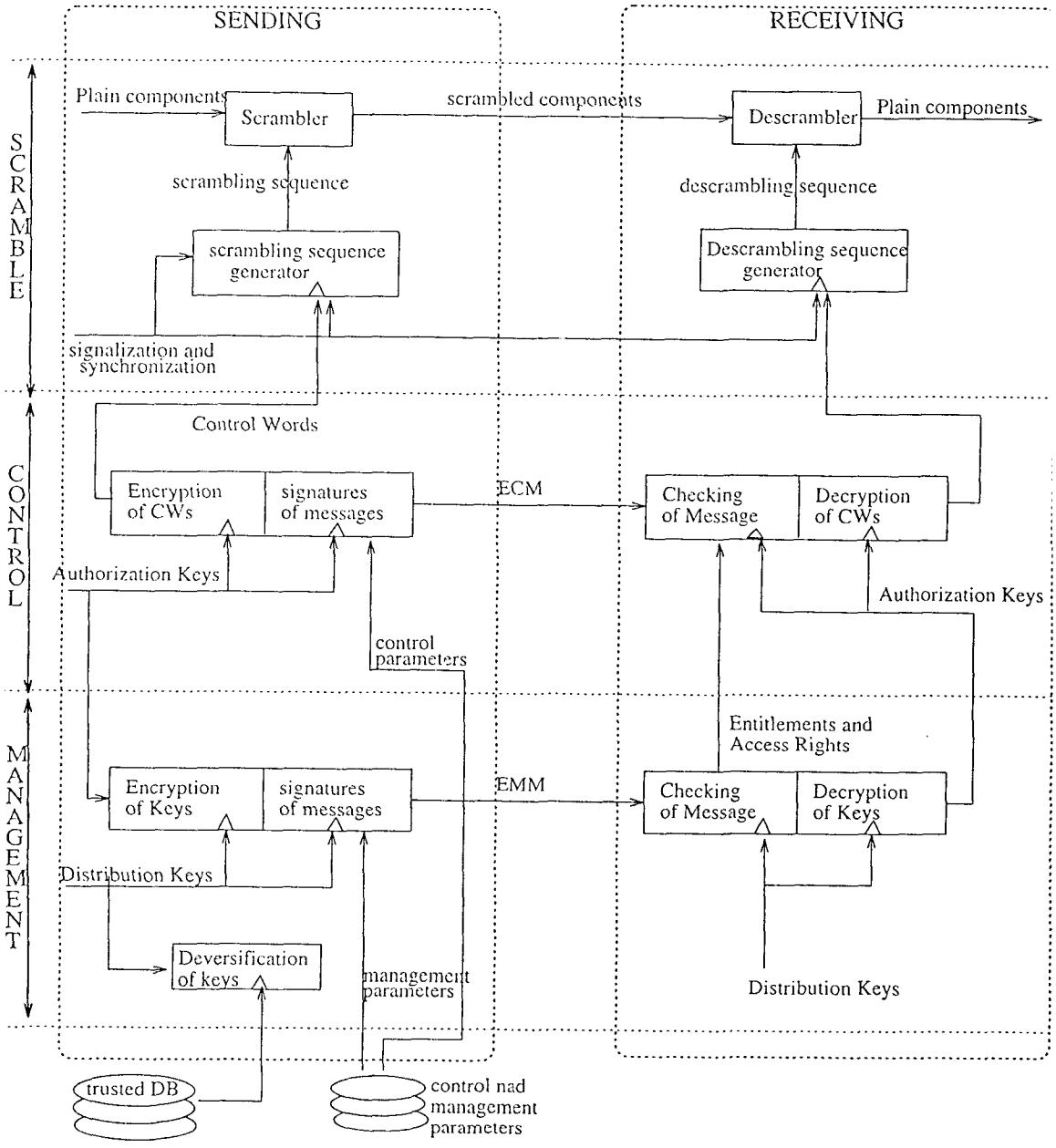

그림 1. Conditional Access의 Framework

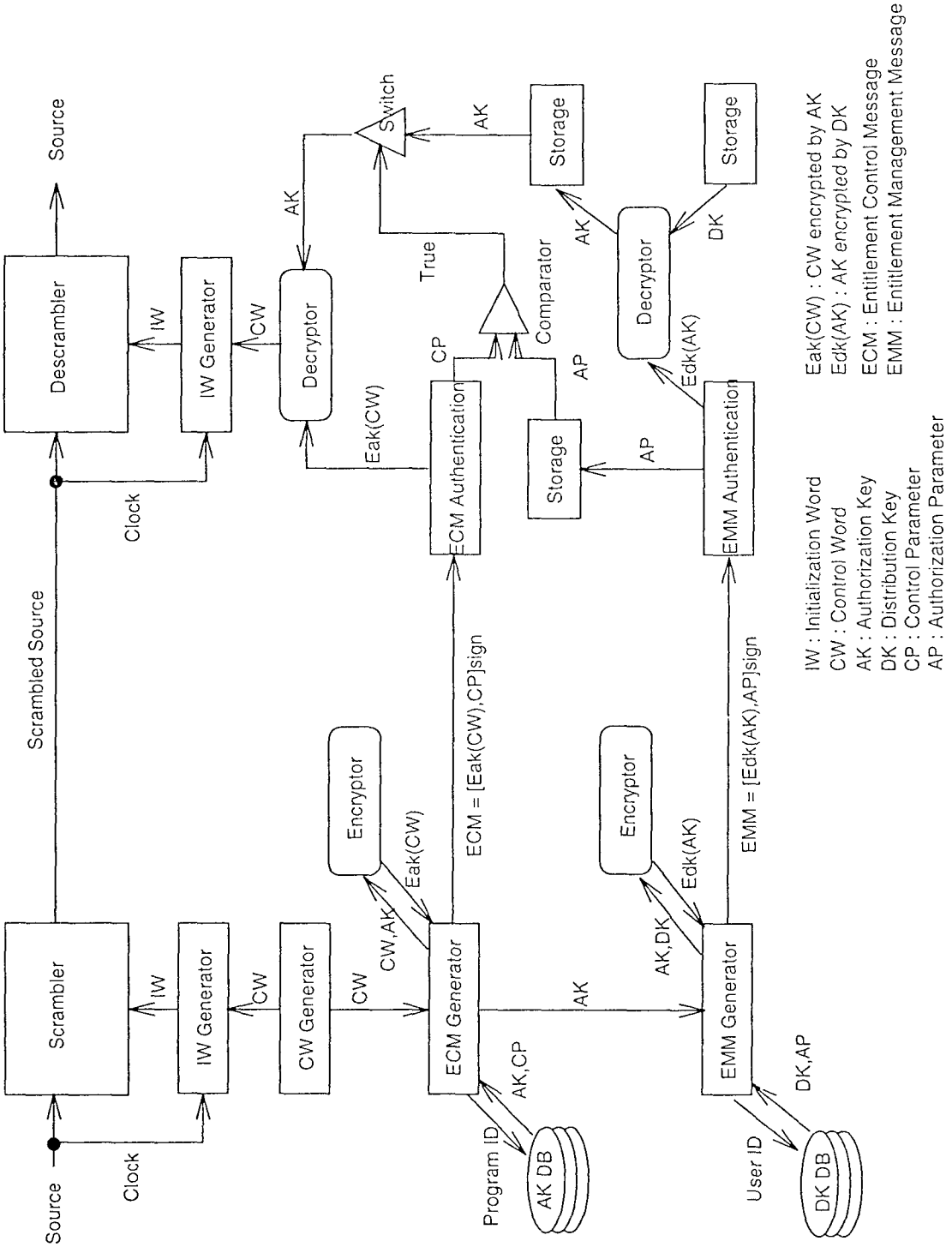

그림 2. CAS의 논리적 구조

제어 단어 생성기는 Scrambler와 Descrambler를 조종하는데 기준이 되는 정보를 발생시킨다. Control Word의 생성주기를 작게 하면 허가없이 디스크램블링할 수 있는 가능성은 그만큼 줄어드나 Control Word를 만들고 수신측에 전달해야 하는 부담이 커진다. 따라서 Control Word의 생성주기와 크기는 Scrambler의 종류와 비도에 의하여 결정해야 할 사항이다.

▫ ECM 생성기

Descrambler는 CW에 의하여 조정되므로 CW를 수신측에 그대로 전송할 수는 없다. 따라서 허가된 수신측에서만 디스크램블할 수 있도록 암호화해서 전송해야 한다. 전송해야 할 프로그램이 여러개일 경우 각 프로그램별로 다르게 암호화해야 하므로 ECM생성기는 프로그램 별로 Authorization Key를 가지고 있는 Authorization Key Date Base에서 해당 프로그램에 대한 Authorization Key를 넘겨 받아 Encryptor를 이용하여 암호화한다. ECM은 또한 수신측의 수신조건(Authorization Parameter)과 비교하여 맞는 조건을 가진 수신기만이 해독할 수 있도록 해당 프로그램에 대한 Control Parameter를 추가하고 CW 및 Control Parameter를 임의로 수정할 수 없도록 전자서명을 첨가하여 만들어 진다.

▫ EMM 생성기

Authorization Key는 프로그램별로 다르게 설정되어 있는 것으로 ECM만을 이용해서는 각 수신기별로 수신권리를 할당해 줄 수 는 없다. 따라서 수신기별로 수신권리를 할당할 수 있는 방법이 필요한데 EMM이 그 역할을 수행한다. 수신권리는 수신 가능기간, 수신 가능횟수 등을 생각할 수 있다. EMM 생성기는 각 수신기별로 부여된 Distribution Key를 이용하여 Authorization Key를 암호화하고, 수신기 별로 다른 수신조건인 Authorization Parameter를 첨가하여 EMM을 생성한다. 생성된 EMM은 임의로 수정할 수 없도록 전자서명을 첨가한다.

▫ Encryptor

특정한 데이터를 어떤 키에 의하여 암호화하는 장치로 ECM의 경우 데이터는 Control Word, 키는 Autorization Key가 되고, EMM의 경우 데이터는 Authorization Key, 키는 Distribution Key가 된다.

▫ Authorization Key Date Base

Authorization Key Data Base는 각 프로그램에 할당된 Authorization Key와 Control Parameter를 저장하는 곳으로 ECM 생성기에 의하여 검색된다.

▫ Distribution Key Date Base

Distribution Key Date Base는 각 수신기에 할당된 Distribution Key와 Authorization Parameter를 저장하는 곳으로 EMM 생성기에 의하여 검색된다;

4.2 수신부

▫ ECM Authentication

ECM Authentication은 전자서명을 확인하여 송신기에 보낸 메시지 원본임을 확인하고 ECM중 암호화된 Control Word와 Control Parameter를 분리하여 Control Word는 Decryptor로 Control Parameter는 비교기로 보낸다.

▫ EMM Authentication

EMM Authentication은 전자서명을 확인하여 송신기에 보낸 메시지 원본임을 확인하고 EMM 중 암호화된 Distribution Key와 Authorization Parameter를 분리하여 Distribution Key는 Decryptor로 Authorization Parameter는 기억장치로 보낸다. 암호화된 Distribution Key는 기억장치로부터 Distribution Key를 넘겨 받아 해독한 다음 Authorization Key를 저장하는 기억장치로 넘긴다.

▫ Decryptor

특정한 데이터를 어떤 키에 의하여 해독하는 장치로 ECM의 경우 데이터는 암호화된 Control Word, 키는 Authorization Key가 되고 EMM의 경우 데이터는 암호화된 Authorization Key, 키는 Distribution Key가 된다.

▫ 기억장치(Storage)

키 또는 자격 정보(Authorization Parameter)를 기억하는 장치로 하나 또는 몇개의 분리된 장치로 생각할 수 있

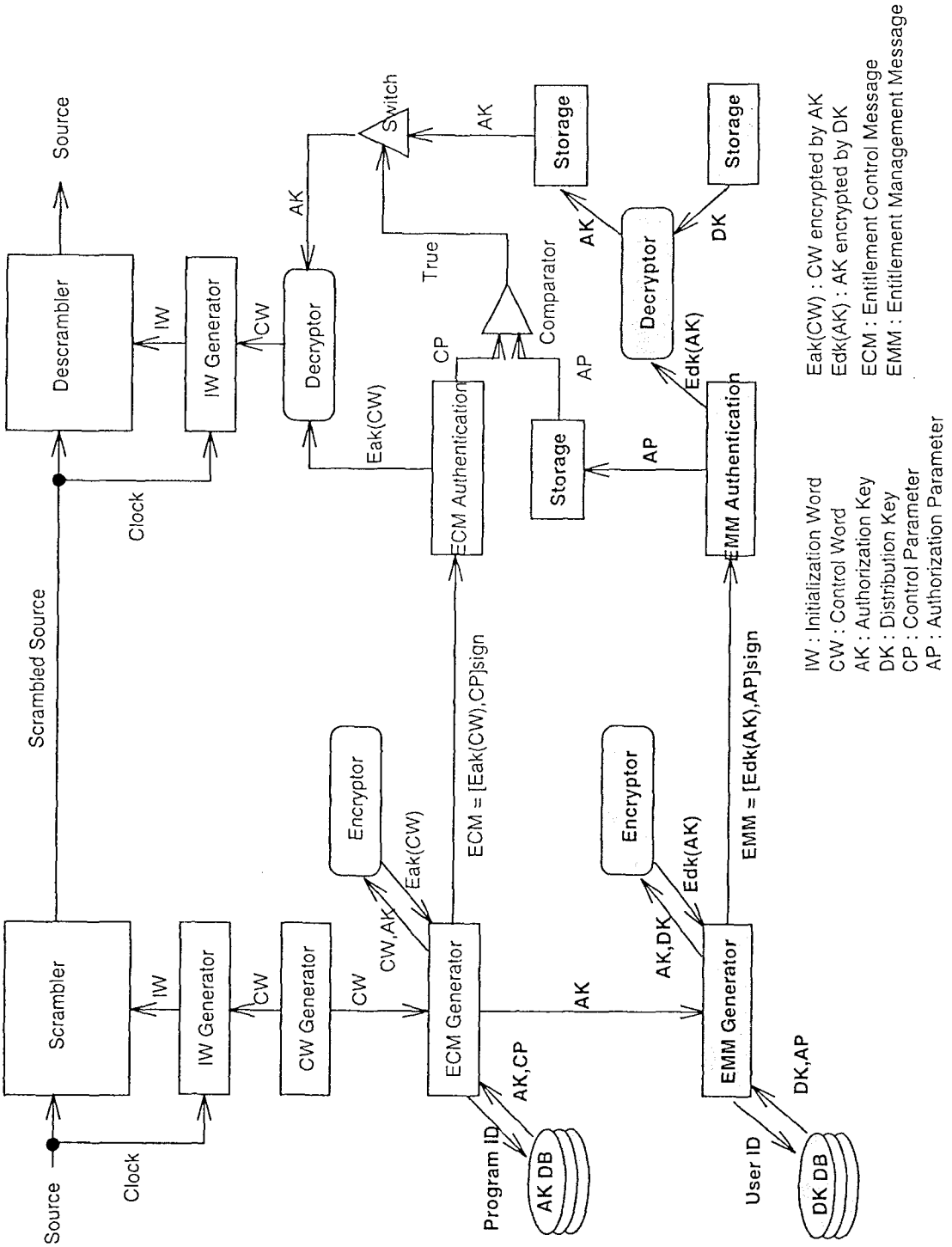

그림 3. 가입신청한 경우의 과정

다.

□ 비교기(Comparator)

비교기에서는 EMM으로 전송되어 온 Authorization Parameter와 ECM으로 전송되어 온 Contrl Parameter를 비교하여 조건이 맞으면 Authorization Key 전송 Switch를 동작시킨다.

□ Switch

Swich는 Storage에 저장된 Authorization Key를 ECM decryptor에 전달하는 중간 과정에 존재하는 것으로 비교기에 나온 결과값이 참일때만 ECM decryptor로 키를 전달한다.

□ Descrambler

Scramble된 신호를 원래의 상태로 환원시키는 장치로 그 과정은 Scrambler와 동일하다.

5. 제한 수신 시스템 동작 원리

5.1 가입신청을 한 경우 Entitlement의 전달

그림3은 Entitlement의 전달 과정에 동작하는 부분을 보여준다.

□ 송신부측의 동작

송신부측에서는 가입신청을 한 수신자에게 해당 프로그램의 Authorization Key와 Entitlement를 전송해 주어야 한다. Authorization Key는 수신자 고유의 Distribution Key를 이용하여 암호화(Encryptor)한 다음 Authorization Parameter와 함께 EMM을 생성해 낸다(EMM 생성기). EMM에는 메시지의 변조를 막기 위하여 전자서명이 추가된다.

□ 수신부측의 동작

수신부측에서는 EMM이 자신에게 발송된 것인지 확인하고(자신의 번호, 지신이 속해 있는 그룹, broadcasting 중 한가지), 전자서명을 검사하여 변조되었는지 확인한다(EMM Authentication). 모두 정상으로 확인되면 자신이 가지고 있는 Distribution Key를 이용하여 Authorization Key를 해독(Decrtptor)하여 Authorization Parameter와 함께 기억장치에 저장한다.

5.2 가입된 프로그램 수신

그림 4는 가입된 프로그램 수신시 동작하는 부분을 보여준다.

□ 송신부측의 동작

수신자가 이미 Authorization Parameter와 Authorization Key를 EMM을 통하여 전달 받았다면 송신부측에서는 Control Word를 Authorization Key를 이용하여 암호화(Encryptor)한 다음, Control Parameter와 함께 ECM을 생성해낸다(ECM생성기). ECM에는 메시지의 변조를 막기 위하여 전자서명이 추가된다. 소스 프로그램은 Control Word에 의하여 제어되는 PRBS의 출력을 이용하여 스크램블하여(Scrambler) 전송한다.

□ 수신부측의 동작

수신부측에서는 전자서명을 검사하여 ECM의 내용이 변조되었는지 확인한다(ECM Authentication). 검사결과 이상이 없으면 암호화된 Control Word 부분은 Decryptor로 Control Parameter부분은 비교기로 보낸다. 비교기에서는 이미 저장되어 있는 Authorization Parameter와 Control Parameter를 비교하여 조건이 맞는지 확인하고 조건이 맞으면 Authorization Key를 Decryptor에게 전달하여 Control Word를 해독하게 한다. 해독된 Control Word는 이것에 의하여 제어되는 PRBS의 출력을 이용하여 프로그램을 디스크램블하는데 사용된다.

6. 결 론

지금까지 살펴 본 제한수신 구조는 디지털 방송을 그 기본 모델로 하였다. 그러나 구조적으로 볼 때 아날로그 방송과 큰 차이가 없으므로 지상파, 위성, 케이블 방송(아날로그/디지털) 등에 적용할 수 있다. 또한 방송의 특성상 모든 수신자가 동시에 신호를 받아볼 수 있어 통신의 내용이 보장되지 않은 환경에서 실현될 수 있는 모델이므로 최근 빠르게 발전하고 있는 양방향서비스에서도 기본 모델로 사용될 수 있을 것이다.

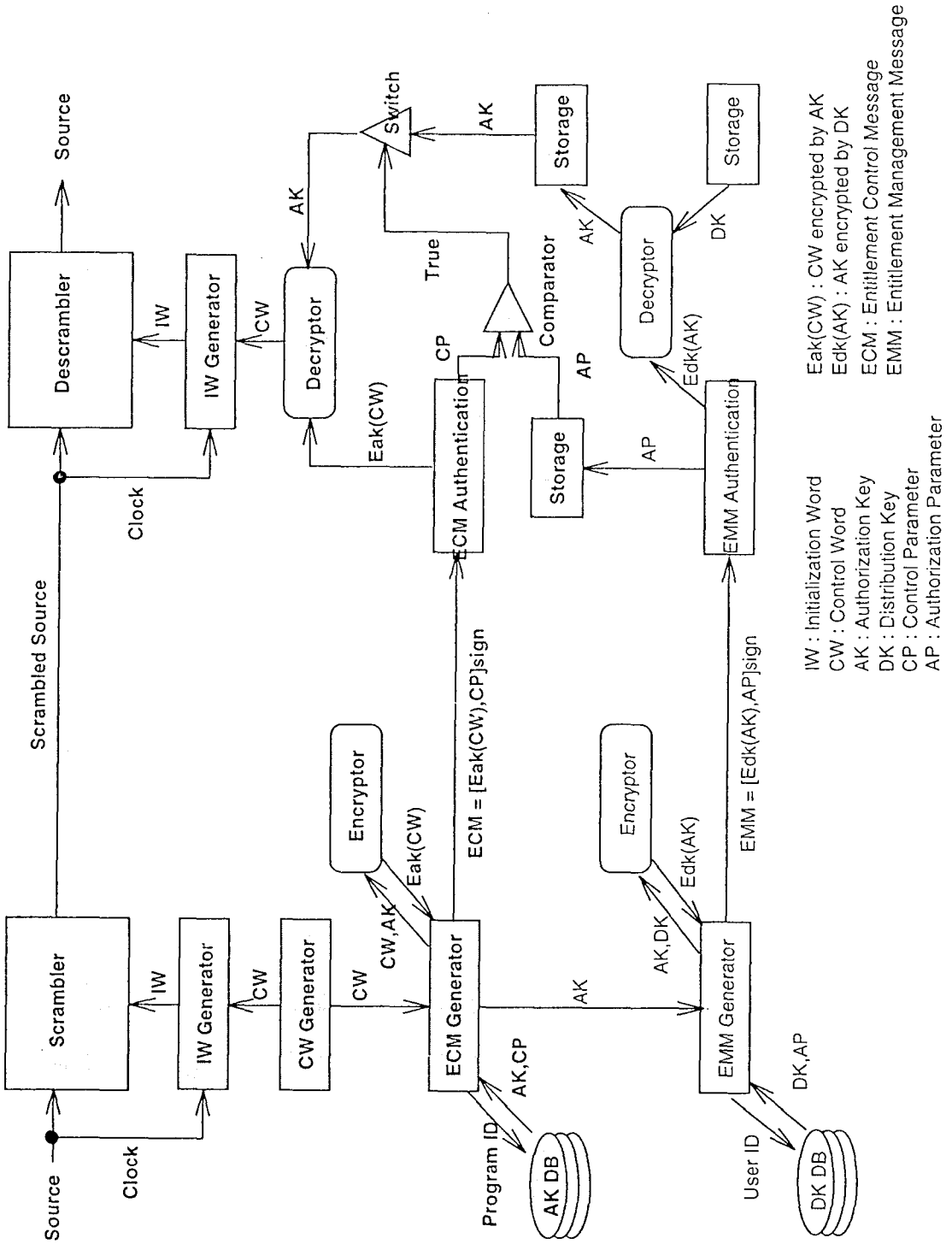

그림 4. 가입된 프로그램의 수신 과정

참고문헌

[EBU-FM] Functional model of a conditional access system, EBU Project Group B/CA. Winter 1995, Switzerland.

[EBU-GC] General Characteristics of a Conditioal-Access Broadcasting System, EBU Report 1079-1

필자소개

은 성 경

1990. 8. 전북대학교 전산 학사
1993. 2. 포항공과대학 전산 석사
1993. 2. 현재 한국전자통신연구원 근무
주관심 분야
-디지털 방송, Network Security

조 현 숙

1980. 2. 전남대학교 수학 석사
1991. 8. 충북대학교 전산학 석사
1982. 3. 현재 한국전자통신연구원 근무
현재 지상 S/W 연구실
주관심분야-Cryptography,
Communication Security

김 신 효

1990. 2. 전남대학교 전산통계 학사
1990. 3. 현재 한국전자통신연구원 근무
주관심분야-Internet Security,
Cryptography