2004 年 3 月　　北京广播学院学报(自然科学版)　　Mar.2004
第 11 卷　第 1 期　　JOURNAL OF BEIJING BROADCASTING INSTITUTE　　Vol.11,No.1
(SCIENCE AND TECHNOLOGY)

基于 DVB 机顶盒的条件接收模块设计

陈文飞[1],杜薇[2]
(1. 北京广播学院数字化工程中心,北京 100024;
2. 广东电视台,广州 510066)

摘　要:条件接收技术是数字电视接收控制的重要保障,它是实现付费电视与互动业务平台关键。本文简要阐述了 DVB 系统中的条件接收技术原理,特别是机顶盒中的条件接收技术,重点介绍基于 DVB 数字机顶盒中条件接收功能模块的设计及实现方法。

关键词:条件接收技术;条件接收模块;授权管理信息;授权控制信息;机顶盒
中图分类号:TP 948.55　**文献标识码**:A　**文章编号**:1007－8819(2004)01－0019－07

1　引言

目前,付费电视与互动业务平台的条件接收系统 CAS(Conditional Access System)正成为整个业务平台的核心部分,也是实现平台服务的关键。它包括前端系统和终端的实现,终端 CA 的实现也是在整个系统的实现上具有非常重要的地位。本文主要论述机顶盒端的 CA 技术以及具体的实现。

2　条件接收系统原理

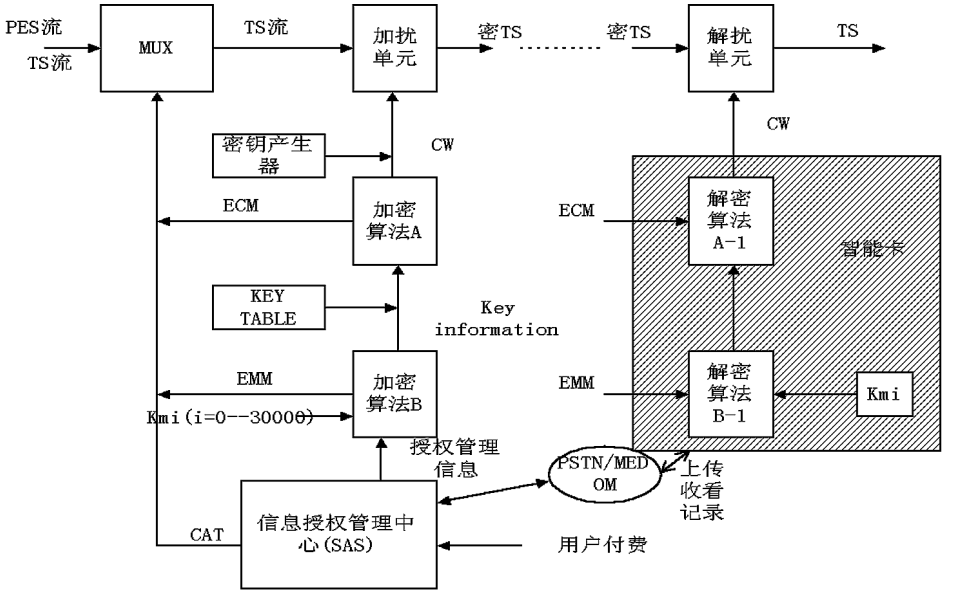
一般的条件接收系统由用户管理系统、节目信息管理系统、加密/解密系统、加扰/解扰系统等构成。图 1 为 CA 系统的实现原理框图。

CA 系统工作原理如下:

在信号的发送端,首先由控制字发生器产生控制字(CW),将它提供给加扰器和加密器 A;CW 的典型字长为 60bit,每隔 2～10s 改变一次。加扰器根据控制字发生器提供的控制字,对来自复用器的 MPEG－2 传送比特流进行加扰运算,此时,加扰器的输出为加扰后的 MPEG－2 TS 流,CW 为加扰器加扰所用的密钥。加密器接收到来自控制字发生器的 CW 后,则根据用户授权系统提供的业务密钥(SK)对 CW 进行加密运算,加密器 A 的输出结果即为经过加密以后的控制字,称为授权控制信息(ECM)。SK 在送给加密器 A 的同时也被提供给了加密器 B,加密器 B 与加密器 A 稍有不同,它自己能够产生密钥,并可以用此密钥对授权控制系统送来的业务密钥(Service Key)进行加密,加密器 B 的输出为加密后的业务密钥,称为授权管理信息(EMM)。经过上面过程产生的 ECM 和 EMM 信息均送至 MUX 同 PES 流或 TS 流进行复用输出。

在 MPEG－2 系统标准中,对在数据包中放置条件接收控制信息及密钥的位置有一定规定,所以,ECM 和 EMM 信息均可以打入 MPEG－2 数据包中。另外,在发送端还有用户管理系统和用户授权系统,用户管理系统是根据用户订购节目和收看节目的情况,一方面向授权控制系统发出指令,决定哪些用户被授权收看哪些节目或接受哪些服务;另一方面还可以向用户发出账单。用户授权控制系统则是根据用户授权管理系统的指令,产生哪些用户该授权收看和接收信息的权力,即产生出业务密钥(SK)。

收稿日期:2003－09－15



CA系统实现框图

图1 CA系统实现原理框图

在信号的接收端,经过解调后的加扰比特流,在最开始的瞬间,控制字还没有恢复出来以前,该加扰比特流在没有解扰的情况下,通过解扰器送至解复用器,由于ECM和EMM信号被放置于MPEG—2传送比特流包头的固定位置,因此,解复用器便很容易解出ECM和EMM信号,被分别送至智能卡(Smart Card)中的解密器A和解密器B,解密器A和解密器B与智能卡中的安全处理器共同工作,从而恢复出控制字(CW),并将它送至解扰器。恢复控制字的过程十分地短暂,一旦在接收端恢复出正确控制字以后,解扰器便能正常解扰,将加扰比特流恢复成正常比特流。

从上面所述,我们可以看出基于DVB的条件接收系统安全性得到三层保护。第一层保护是用控制字(CW)对复用器输出的图像、声音和数据信号比特流进行加扰,扰乱正常的比特流使其在接收端不解扰就收看、收听不到不正常的图像、声音及数据信息;第二层保护是通过对CW用业务密钥加密(SK)从而使控制字在传送给用户的过程中即使被盗,被盗者也无法对加密后的CW进行解密;第三层保护是对SK的加密,它使得整个系统的安全性更强,使非授权用户在即使得到加密业务密钥的情况下,也不能轻易解出。因为,解不出业务密钥就解不出正确的CW,没有正确CW就无法解出并获得正常信号的比特流。

3 机顶盒端的解扰原理

终端机顶盒上实现CA的框图如图2所示。

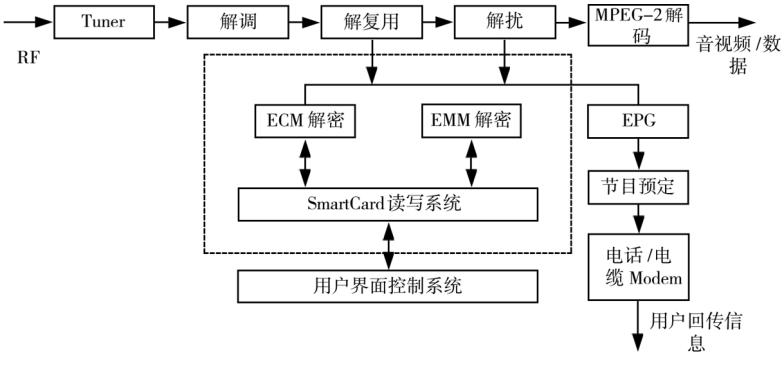


图2 机顶盒端解扰原理框图

3.1 解复用和解扰的功能

RF 信号进入机顶盒后,经过高频头调谐,转换为 QAM 或 QPSK 信号。解调器对此信号进行解调,还原出数字的 TS 流,该 TS 流包含了 DVB 的 SI/PSI 信息、加扰的节目流和 CA 解密所需的专有信息(ECM 和 EMM)等。

解复用模块需要将现在正在观看节目的基本流传递给解扰芯片,将不需要的基本流滤掉。此外,解复用模块还要过滤出机顶盒模块需要的 SI/PSI 信息、CA 模块需要的 ECM/EMM 信息,并将收到的信息发送到相应的模块。其中 SI/PSI 信息是机顶盒接收节目的基本条件,在其中定义了机顶盒索引频道和其他一些 EPG 信息。

如果节目没有加扰,则解扰器不对码流进行处理,直接将单路节目的码流传输给 MPEG－2 解码模块 . 如果节目加扰,则解扰芯片根据 CA 模块发送的控制字 CW 对节目流进行实时解扰;然后将透明码流传输给 MPEG －2 解码器 .MPEG－2 解码器将 MPEG－2 信号转换为模拟的 A/V 信号输出,CW 由授权的智能卡发出控制解扰器工作。

3.2 机顶盒端的解密机制

当智能卡插入机顶盒时,解码器将从中读取智能卡的 CA _ System _ ID 及其它智能卡信息;在 TS 流中过滤并找到 CAT 表(PID 号为 0x01),并从中查找 CA 描述子,找出对应 CA _ System _ ID 的 CA _ PID,此即为 EMM 码流的 PID 号;获取 EMM 码流后(EMM 码流中包含了经过用户个人分配密钥 PDK 加密处理的用户密钥 SK,PDK 固化在智能卡中,并以加密形式存储),用户需提供相应的口令才能解密使用,接着智能卡将解密出业务密钥 SK。完成以上步骤后,解码器再从 PMT 表中找到 CA 描述子,并找出对应的 ECM 码流的 PID 号(ECM 码流中包含了由业务密钥 SK 加密处理后的 CW 信息),用得到的 SK 对 ECM 解密就可得到 CW,将 CW 填入解码芯片的相应寄存器中,可对码流数据进行解扰,恢复出原始信号。

4 CA 在 STB 中的功能模块及接口调度

在机顶盒的 CA 设计中,主要实现以下功能:

(1) 对加密节目解扰、接收;

(2) 对加密节目按次付费功能的实现(PPV);

(3) 对加密节目的即时购买功能的实现(IPPV);

(4) 对邮件的接收;

(5) 智能卡的认证;

根据以上的功能,机顶盒在设计中主要有以下主要模块:

(1) SI 管理器模块;

(2) 智能卡管理器模块;

(3) CA 管理器模块;

(4) MODEM 上传模块。

下面就以上各功能模块和接口调度分别进行详细叙述。

4.1 SI 管理器模块

SI(服务信息)功能模块的作用是控制从信息流中得来的 SI 信息,设置解复用器参数来管理数据接收通道。SI 管理器并非专门为实现 CA 功能而创建的,但该管理器为实现 CA 功能,需从 CAT,PMT 中析取 ECM、EMM,并分别将 ECM,EMM 数据发送给相应的接收者。

本机顶盒中对 EMM PID 的提取流程如图 3 所示:

(1) 机顶盒首先设置解复用参数,从多路节目流中过滤出 CAT 表;

(2) 在 CAT 表中可能具有多个 CA 描述子存在,MPEG－2 中规定 CA 描述子的标号为 0X09,在 CAT 分段中先找到 CA 描述子,因为每个 CA 描述子标识一个指定的 CA 系统 ID 和对应的 EMM _ PID;

(3) 在找到 CA 描述子后,每个 CA 描述子标识一个指定的 CA 系统 ID 和对应的 CA _ PID;

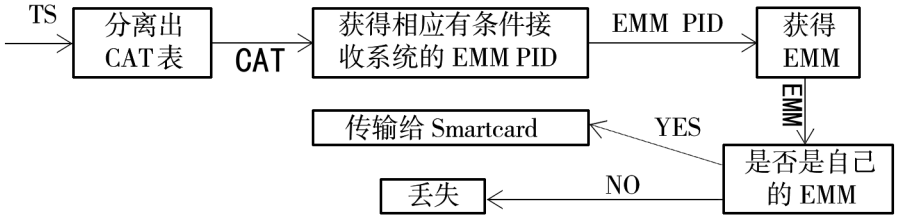


图3 EMM PID的解析流程图

(4)然后逐步比较CA_System_ID(与先期从IC卡中读出的CA_System_ID),找出对应的CA_PID,此CA_PID为EMM_PID,而不一致的则丢掉;

机顶盒必须使用CAT表中的版本信息去检测和处理最新版本的CAT表。

每个被加扰的节目都对应一路ECM流,其对应关系是由PMT表给定(PMT表是用来描述某个特定节目内部属性的,如某个节目由哪些基本码流组成,每个节目都有自己的PMT表)。一个加扰节目的PMT表有一个对应的CA描述子,当CA描述子出现在PMT中时,CA_PID就表示ECM_PID;而当CA描述子出现于CAT表中时,CA_PID就表示EMM_PID。PMT表中的CA描述子(Descriptor tag=0x09)描述当前系统中存在的CA系统的System ID及其ECM_PID。CA_System_ID由DVB组织为每个CA系统的提供商指定。

本机顶盒对ECM_PID的解析流程如下图4所示:

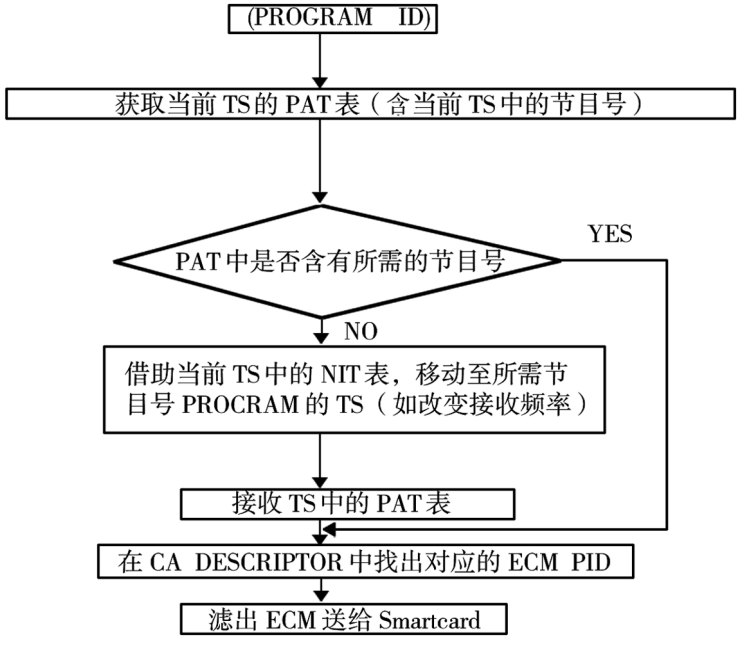


图4 ECM_PID的解析流程图

(1)首先根据节目号,在PAT表中找到PMT_PID;

(2)在使用此PMT_PID设置过滤器,得到该节目的PMT表;

(3)加密的节目中会有一个或多个CA的描述子存在,MPEG—2中规定的CA描述子的标识号为0x09;

(4)在PMT分段中找到CA描述子后,每个CA描述子标识一个指定的CA系统ID和对应的CA_PID;

(5)然后逐步比较CA_System_ID(与先期从IC卡中读出的CA_System_ID),找出对应的

CA _ PID;

(6) 此 CA _ PID 即为 ECM _ PID。

机顶盒必须使用 PMT 表中的版本信息去检测和处理最新版本的 PMT。

获得 ECM、EMM 的 PID 后,通过设置解复用器在传输流里面把 ECM 和 EMM 的数据解析出来,然后在 SI 和 CA 任务之间通过信息传递机制,将数据作为信息的主体发送到 CA TASK。

4.2 智能卡管理器模块

智能卡管理器模块是机顶盒中的一个模块,但却是一个完整、独立的部分,通过特定的指令系统来交换信息,负责监控智能卡的状态,如插入、拔出、复位等。在卡插入时,或在机顶盒开机时对卡进行复位,完成正确的读写操作,保证数据传输无误,同时还需要在卡复位之后读出 CA _ System _ ID 等系统信息,送给 CA TASK 处理。

智能卡完成的主要功能有:

(1)接收 EMM 和 ECM,同时如果权限允许则由此产生解扰所需的 CW;

(2)临时存储视听账单;

(3)条件满足时,要求将视听账单上传给 SMS;

4.3 CA 管理器模块

CA 完成 ECM、EMM 数据的解密,恢复出 CW,送至解扰器,完成解扰工作,播出正确的视音频流。采用与前端系统中的加扰算法对应的逆算法,将从 SI 管理器得到的 ECM、EMM 数据解密成 ECM、EMM 消息(在 EMM 中会有 IC 卡的 ID 信息,标志该 EMM 所适用的用户),机顶盒根据当时机内所插入的 IC 卡,读出 SMC ID 来决定是否将此 EMM 传递到该 IC 卡中;然后 ECM 的节目授权信息与智能卡的用户授权信息进行比较,对于符合条件的 ECM 消息也将其送给智能卡;然后经 13818—6 标准通信接口送给机顶盒条件接收子系统,对密钥进行解码,并恢复出控制解扰序列所需的信息,并由机顶盒完成解扰工作。

4.4 MODEM 模块

MODEM 模块主要实现机顶盒中的向前端传输数据信息,主要有两点功能:

(1) 在实现 VOD 功能时,把用户点中的节目信息,向前端中心系统发送加密请求数据,从而完成 VOD 节目的点播功能;

(2) 在实现 IPPV 功能时,该模块完成视听账单的上传过程(将其传给 SMS),在 CA 功能实现中,主要用于视听账单数据的上传。

UPLOADING 过程如图 5 所示。

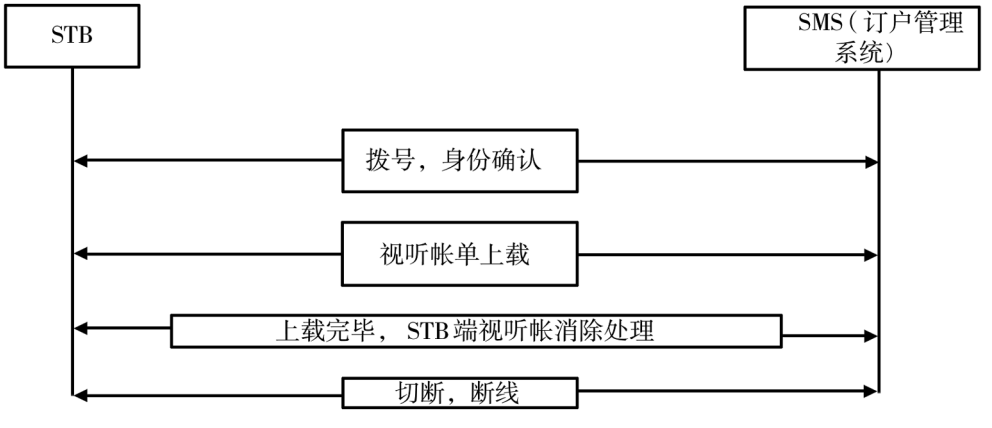


图 5　上传处理过程

4.5 接口调度

CA模块和机顶盒中其他模块的接口有以下几个：

(1)初始化

机顶盒主程序调用CA模块的相应函数完成对CA模块的初始化。在初始化过程中,CA模块清除存储,操作智能卡获取信息,在多线程的操作系统下,可能产生新的内部工作线程。经过初始化后,CA模块待命,准备接收进一步的操作指令。

(2)获取CA信息

该接口在初始化后调用,机顶盒来获取当前模块和智能卡的信息。如智能卡是否合法、CA—System—ID、CA的版本号、用户的ID号等。

(3)用户控制接口

该接口是指包括用户通过遥控器对CA模块进行参数配置或控制。如用户修改智能卡的PIN码、查看智能卡信息和购买信息、修改卡内的节目收看级别信息和购买节目等。

(4)界面显示接口

CA模块在运行时,需要在屏幕上显示一些提示信息。如节目是否购买信息、OSD信息、提示插卡信息等。

(5)调度接口

STB接收到TS流中的CA相关SI/PSI表格,如果发现当前节目使用了本模块的CAS来保护,则将相应的CA信息(ECM PID EMM PID和CA私有数据等)发送给CA模块,CA模块会启动相应的任务来解密。如果当前观看的节目没有加扰或没有使用本CA来加扰,则STB通知CA模块暂停运行。

(6)解复用接口

CA模块在运行时,需从码流中接收CA专有信息(ECM EMM)。这个功能是由STB的解复用模块来完成的。

(7)解扰接口

CA模块在接收并解密到当前节目的最新CW后,将CW发送给解扰器,发送过程由此接口来实现。

(8)智能卡驱动接口

CA模块要对智能卡进行操作,需要STB提供基于7816标准的协议,7816的通信协议有T0和T1两种。目前大部分使用T0协议。

各个接口的调用关系见表1。

表1

接口	调用关系	
	机顶盒	CA模块
初始化	→	
获取CA信息	→	
用户控制	→	
界面显示	←	
调度	→	
解复用	←→	
解扰	←	
智能卡	←→	

5 结束语

条件接收系统是数字电视发展的技术保障。通过条件接收建立有效的收费体系,从而保障节目提供商和运营商的利益。从国内外数字电视商业化运作成功经验来看,条件接收系统是推动数字电视发展的重要环节,也是保证节目提供商利益的必要技术保障,同时为数字网络提供丰富的增值业务机会,为传统的广播行业带来生机。强有力的、安全有效的条件接收系统就成为付费电视与互动平台的核心部分,也是实现平台服务的关键,只有采用有条件接收技术,实施健全的广播电视付费机制,才能促进电视事业的蓬勃发展。

参考文献：

[1] DigitalVideo Broadcasting(DVB),Specification for Service Information (SI) in DVB systems,EN300 468 V1.3.1998[S].

[2] Digital Video Broadcasting(DVB),Support for use of scrambling and Conditional Access (CA) within DVB systems, ETSI ETR

1996[S].
[3] 孙苏广 .DVB 条件接收系统简介[J]. 广播与电视技术,1997,(3).
[4] 郑立新,等 . DVB 机顶盒中条件接收系统的设计与实现[J]. 电视技术,2003,(7).
[5] 国家广播电影电视总局标准化规划研究所 .数字电视广播条件接收系统规范,2001[S].
[6] 郑志航 . 数字电视原理与应用[M]. 北京:中国广播电视出版社,2001.

Design of CA module for STB based on DVB

CHEN Wen_fei, DU Wei

(1. Engineering Center for Digital Audio & Video, Beijing Broadcasting Institute. Beijing, 100024 P.R.China
2. TV station of Guangdong Province, Guangzhou, 510066 P.R.China)

Abstract: The technology of Conditional Access is the important guarantee for Digital television Receive and control. Conditional Access is the key to realize the pay TV and interactive TV platform. In this paper we introduce the CA mechanism in DVB systems, then analyze the CA technology in Set_Top_Box. Finally, we introduce the design and implement method of functional module for CA in the Set_Top_Box based on DVB.

Keywords: Conditional Access Technology; CA_Module; EMM; ECM; STB

(责任编辑:韩月珍)