

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷
H04N 7/16



[12] 发 明 专 利 说 明 书

[21] ZL 专利号 00127913.0

[43] 授权公告日 2003 年 6 月 11 日

[11] 授权公告号 CN 1111335C

[22] 申请日 2000.12.15 **[21]** 申请号 00127913.0

[74] 专利代理机构 上海东亚专利代理有限公司

[71] 专利权人 上海南广电子技术有限公司

代理人 罗习群

地址 200030 上海市漕溪北路 336 号慧谷大厦 4 层

[72] 发明人 庞志平 周 欣 韩永强

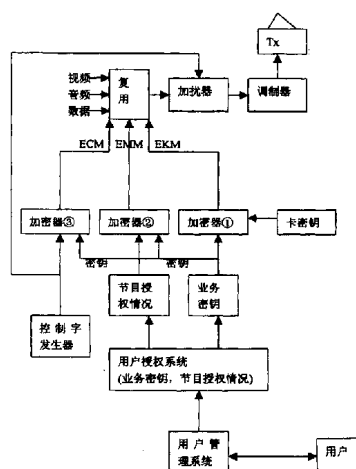
审查员 陈 曦

权利要求书 1 页 说明书 4 页 附图 2 页

[54] 发明名称 宽带数据广播中窄带条件接收方法

[57] 摘要

本发明是在数据传送的发送端,合并业务密钥(即不同的节目用相同的业务密钥),增加独立授权信息,用户的授权系统产生两路信息,一路是业务密钥,另一路是独立出来的节目授权信息,对不同节目的授权用同样的业务密钥,但增加“允许/不允许”来控制控制字的输出,在数据接收端用卡密钥(私钥)对授权加密信息解密、得到业务密钥,用业务密钥经解密器对授权控制信息和控制字信息解密,并判断节目授权情况是否允许,如允许,则得到控制字,由控制字产生解扰序列进行解扰。



ISSN 1008-4274

知识产权出版社出版

1, 一种宽带数据广播中窄带条件接收方法, 其特征在于: 在数据传送的发送端, 合并业务密钥, 增加独立授权信息, 用户授权系统产生两路信息, 一路是业务密钥, 另一路是独立出来的节目授权信息, 对不同节目的授权用同样的业务密钥, 但增加“允许/不允许”来控制控制字的输出, 业务密钥进入加密器(1)、加密器(2)和加密器(3), 节目授权情况进入加密器(2), 业务密钥在加密器(1)中经卡密钥(公钥)加密后, 成为授权加密信息 (BKM); 在加密器(2)中用业务密钥对节目授权情况进行加密, 形成授权管理信息 (EMM); 同时, 加密器(3)中业务密钥对控制字进行加密, 形成控制字信息 (ECM), 所有信息包括 (EKM)、(ECM)、(EMM) 打包后和各种业务信息一起复用传输; 在数据接收端, 解密器用卡密钥(私钥)对授权加密信息 (EKM) 解密, 得到业务密钥, 用业务密钥由解码器 (2) 和解码器(3)分别对授权管理信息 (EMM) 和控制字信息 (ECM) 解密, 判断节目授权情况是否“允许”, 若允许, 则得到控制字, 由控制字产生解扰序列进行解扰。

2, 按权利要求 1 所述的宽带数据广播中窄带条件接收方法, 其特征在于: 发送端的第二加密器(2)以 1: 1 的比例传送数据。

3, 按权利要求 1 所述的宽带数据广播中窄带条件接收方法, 其特征在于: 该方法与第一加密器 (1)、第二加密器 (2)、第三加密器 (3), 第一解密器 (1)、第二解密器 (2)、第三解密器 (3) 采用何种算法无关。

宽带数据广播中窄带条件接收方法

一种宽带数据广播中窄带条件接收方法，属通信技术领域。

数据广播中的条件接收，一般由两个相互独立的部份组成，即加扰和接收控制（通常称数据加密），其中每一部份都是一个特殊的信息过程。

加扰，是 CA 系统较底层的操作，通用的方法是由加扰序列来控制加扰，加扰序列由伪随机发生器产生，在初始条件已知的情况下，可推测出伪随机发生器产生的加扰序列，初始条件受控于一个叫初始字的特殊信号。在接收端也有一个同样的伪随机发生器，如果将初始字发送给这个伪随机发生器，那么就可以获得解扰序列，然后再用解扰序列恢复原始信号。为实现保密，可根据所采用的授权方式，将恢复初始字的有关信息，加以保密形式发送；初始字由控制字和初始修正符组成，而 CA 安全保障的核心，就是相关控制信息的安全传输，在数字视频信号环境中，加扰操作都是由加扰控制字所控制完成，这个控制字就是一把钥匙，有了它就可同步恢复加扰所使用的随机序列对加扰视频信号进行解扰。

控制字的安全传送依赖于业务密钥，经业务密钥加密后与加扰后的数据一同发送，用户接收过程中用业务密钥解密得到控制字，由控制字产生解扰序列进行解密。授权控制信息 ECM 是业务密钥对控制字和控制参数加密后得到的条件接收信息，用户端的解扰器只有在得到现行有效的业务密钥后，才能得到控制字，从而实现对数据解扰。

业务密钥的传递可以通过智能卡等方式固化在芯片内传递，也可以通过授权系统用分配密钥加密经安全渠道传递给用户，通过授权控制信息 EMM 来实现；后一种往往在对安全性要求高的系统中应用；用户授权系统用分配密钥对业务密钥加密后得到的条件接收信息称为授权管理信息 EMM；在接收端，解码器首先要用分配密钥对授权管理信息 EMM

解密，得到业务密钥，然后用业务密钥对控制字信息 ECM 解密得到控制字和控制参数，才能对数据解扰。

按照业务密钥通过智能卡等方式固化在芯片内传递的方式，其加密算法的核心是算法，一旦算法被破解，就可进行大规模的伪冒。

而另一种通过授权系统用分配密钥加密经安全渠道传递给用户的方案，虽然其安全性较上一种方案高，但占用了过多的带宽，它的授权系统把对用户和节目的授权放在一起进行，因此需占用用户数 $\times$ 节目数 $\times$ 业务密钥长度的带宽，这种过多占用带宽，导致延长用户等待接收时间。

本发明的目的是设计一种通过授权系统用分配密钥加密后经安全渠道传送给用户但又不占用过多带宽的宽带数据广播中窄带条件接收方法。

本发明的方案是这样实现的，在数据传送的发送端，合并业务密钥，（即不同的节目用相同的业务密钥，而现行其他做法是不同节目用不同业务密钥），增加独立授权信息，用户授权系统产生两路信息，一路是业务密钥，另一路是独立出来的节目授权信息，对不同节目的授权用同样的业务密钥，但增加“允许/不允许”来控制控制字的输出，业务密钥进入三个加密器，节目授权情况进入其中一个加密器，业务密钥在另一加密器中经卡密钥（公钥）加密后，成为授权加密信息 E K M；在其中一个加密器中用业务密钥对节目授权情况进行加密，形成授权管理信息 E M M；同时，其中一个加密器中业务密钥对控制字进行加密，形成控制字信息 E C M，所有信息包括 E K M、E C M、E M M 打包后和各种业务信息一起复用传输；在数据接收端，一个解密器用卡密钥（私钥）对授权加密信息 E K M 解密，得到业务密钥，用业务密钥由另二个解码器分别对授权管理信息 E M M 和控制字信息 E C M 解密，判断节目授权情况是否“允许”，若允许，则得到控制字，由控制字产生解扰序列进行解扰；发送端的一个加密器以 1:1 的比例传送数据；本方案是一种系统解决方案，与三个加密器和接收端的三个解密器采用何种算法无关。

本发明的优点是：

1， 抗攻击能力强

运用两级加密体系，加密算法核心是密钥而不是算法，此方案可以经常更换业务密钥，因此，相对于固定业务密钥方案，业务密钥对控制字的加密算法不用很强，但更为安全可靠，例如，运用在数据广播中，虽然每块算法卡算法相同，但密钥都不同，分析出一块卡只能仿冒一块，要仿冒第二块卡就要重新分析；如果万一其一块卡被破解，我们可以立即查出并通知用户进行更换，与其他传递业务密钥方式相比，由于合并了业务密钥，降低了分配密钥解业务密钥的频率，因此，在相同性能要求下，可加强分配密钥对业务密钥的强度，并适当拉长分配密钥长度，以此提高系统安全可靠性能。

2， 节省带宽

与一般的用户授权不同，我们合并业务密钥（即不同的节目用相同的业务密钥，而现行其他做法是不同节目用不同业务密钥），增加独立授权信息，这样，用户的授权系统产生两路信息，一路是业务密钥，即对用户合法性进行授权，所占用带宽为：用户数 $\times$ 业务密钥长；另一路就是独立出来的节目授权信息，对不同节目授权用同样的业务密钥，但增加“允许/不允许”来控制控制字的输出，占用带宽为：用户数 $\times$ 节目数 $\times$ 2bit，总共占用带宽是：用户数 $\times$ 业务密钥长+用户数 $\times$ 节目数 $\times$ 2bit，远小于一般占用带宽数：用户数 $\times$ 节目数 $\times$ 业务密钥长，大大缩短了用户等待授权的时间。

本发明有如下附图：

附图 1 是本发明的数据发送端原理方框图。

附图 2 是本发明的数据接收端原理方框图。

下面结合附图叙述本发明的实施例：

请参阅附图 1、2，在数据传送的发送端，合并业务密（即不同的节目用相同的业务密钥，而现行其他做法是不同节目用不同业务密钥），增加独立授权信息，这样，用户的授权系统产生两路信息，一路是业务密

钥，另一路是独立出来的节目授权信息，对不同的节目的授权用同样的业务密钥，但增加“允许/不允许”来控制控制字的输出，业务密钥进入加密器 1、加密器 2 和加密器 3，节目授权情况进入加密器 2，业务密钥在加密器 1 中经卡密钥（公钥）加密后，成为授权加密信息 $E K M$ ；在加密器 2 中用业务密钥对节目授权情况进行加密，形成授权管理信息 $E M M$ ，以 1:1 的比例传递数据，同时，加密器 3 中业务密钥对控制字进行加密，形成控制字信息 $E C M$ ，所有信息包括 $E K M$ 、 $E C M$ 、 $E M M$ 打包后和各种业务信息一起复用传输；在数据接收端，解密器 1 用卡密钥（私钥）对授权加密信息 $E K M$ 解密，得到业务密钥，用业务密钥由解码器 2 和解码器 3 分别对授权管理信息 $E M M$ 和控制字信息 $E C M$ 解密，判断节目授权情况是否“允许”，若允许，则输出控制字，由控制字产生解扰序列进行解扰。

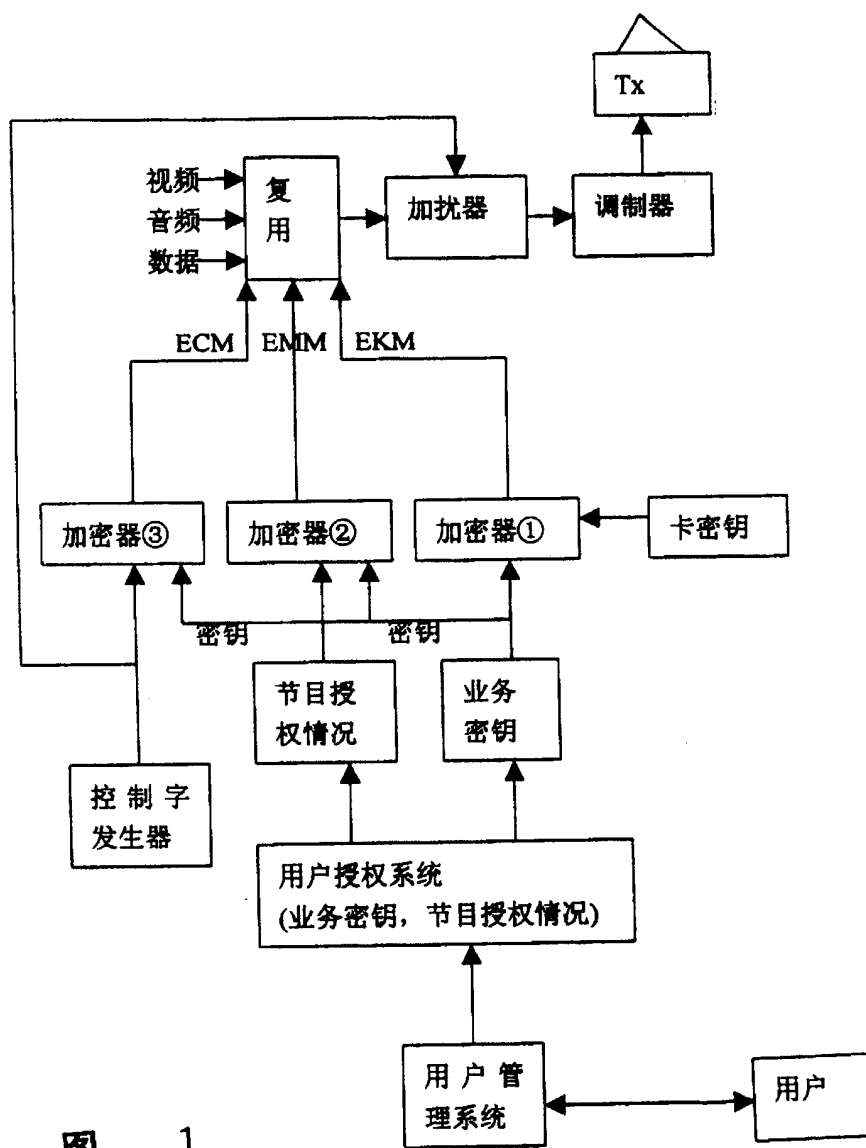


图 1

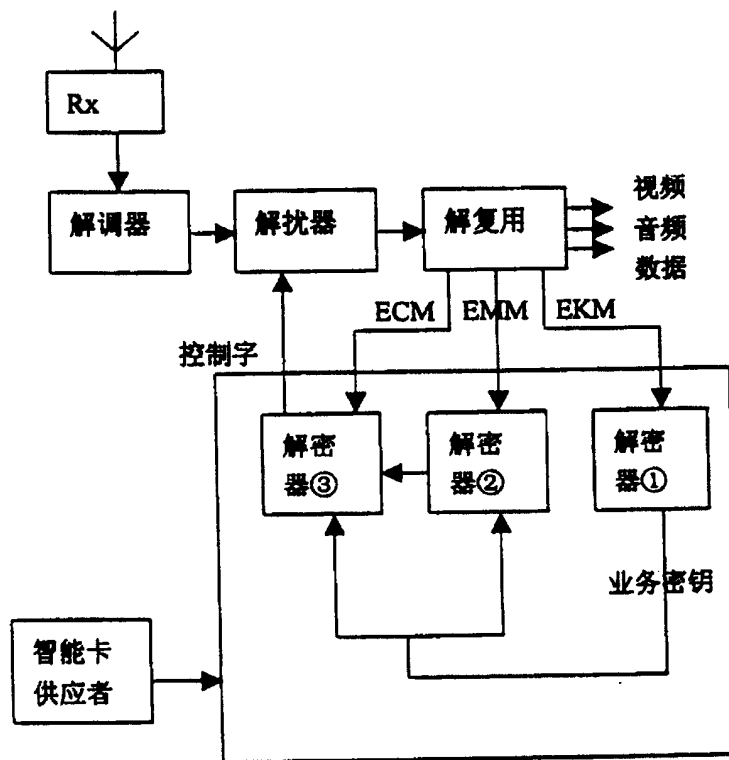


图 2