[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04N 7/167

[12] 发明专利说明书

[21] ZL 专利号 01804165.5

[45] 授权公告日 2004 年 9 月 22 日

[11] 授权公告号 CN 1168313C

[22] 申请日 2001.1.24 [21] 申请号 01804165.5

[30] 优先权

[32] 2000. 1.28 [33] CH [31] 0166/2000

[32] 2000. 8.21 [33] US [31] 60/226,769

[86] 国际申请 PCT/IB2001/000094 2001.1.24

[87] 国际公布 WO2001/056287 英 2001.8.2

[85] 进入国家阶段日期 2002.7.26

[71] 专利权人 纳格拉卡德股份有限公司

地址 瑞士舍索 - 苏尔 - 洛桑

[72] 发明人 安德烈·库德斯基 马库·塞塞里

审查员 黄金龙

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所

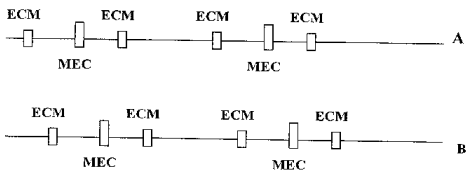
代理人 李 强

权利要求书 2 页 说明书 5 页 附图 1 页

[54] 发明名称 加密信息的传输方法和传输系统

[57] 摘要

在利用多信道信号传播付费电视时，每个信道与授权报文(ECM)相联系，该报文容许根据用户权力对此信道解密。 当改变信道时，在人们确定与新信道相关的这些新权力之前可接受的是一个很短的时间。 这样就可以排除庞大的加密算法。 为避免这一缺点，对于信道解密提出了一种系统，该系统利用用于信道的授权信息(ECM)并藉助快速算法利用用于信道组的授权报文(MECM)进行加密。 对这些后者利用一个高安全性算法加密，于是解密较慢。



ISSN1008-4274

1.一种用于收费电视的加密信息多信道传输系统，包括一个管理中心和至少一个用户单元，此管理中心传输加密信号和为每个信道加密的单信道授权报文，其特征在于它包含由一组信道共用的多信道授权报文，这些报文与用于当前接收的信道的单信道授权报文相结合以便对其解密。

2.如权利要求 1 的多信道传输系统，其特征在于所述多信道授权报文是利用一个与用来对单信道授权报文加密的算法不同的算法加密的。

3.如权利要求 1 或 2 的多信道传输系统，其特征在于所述多信道授权报文是按照一个与单信道授权报文的周期不同的周期进行修改的。

4.如权利要求 1 或 2 的多信道传输系统，其特征在于包含在多信道授权报文中的信息是与包含在单信道授权报文中的信息通过加、减、“ 异”、乘运算而结合的。

5.如权利要求 1 或 2 的多信道传输系统，其特征在于用户单元包含一个由单信道授权报文确定控制字的密码单元，容许用户装置对加密信号进行解密，所述多信道授权报文的内容与密码装置的密码计算的参数相结合。

6. 如权利要求 3 的多信道传输系统，其特征在于包含在多信道授权报文中的信息是与包含在单信道授权报文中的信息通过加、减、“ 异”、乘运算而结合的。

7.如权利要求 3 的多信道传输系统，其特征在于用户单元包含一个由单信道授权报文确定控制字的密码单元，容许用户装置对加密信号进行解密，所述多信道授权报文的内容与密码装置的密码计算的参数相结合。

8.一种付费电视多信道加密信号的传输方法，包括:

-传输多信道信号到用户单元，

-传输为每个信道加密的单信道授权报文，

-对由一个密码单元当前接收的信道的授权报文进行解密，解密的信息表示了对适用于该当前接收的信道的信号进行解密所需的控制字，

其特征在于其包括：

-传输一组信道共用的多信道授权报文，

-对这些多信道授权报文进行解密并将解密的信息与获得控制字所需的信息相结合。

9.如权利要求 8 的多信道加密信号的传输方法，其特征在于上述结合是对密码单元的参数进行的。

10.如权利要求 8 或 9 的多信道加密信号的传输方法，其特征在于根据一个与单信道授权报文的修正周期不同的一个周期对所述多信道授权报文进行修正。

11.如权利要求 8 或 9 的多信道加密信号的传输方法，其特征在于包括根据一个与用来加密单信道授权报文的算法不同的一个算法对此多信道授权报文进行加密。

12.如权利要求 10 的多信道加密信号的传输方法，其特征在于包括根据一个与用来加密单信道授权报文的算法不同的一个算法对此多信道授权报文进行加密。

加密信息的传输方法和传输系统

技术领域

本发明涉及在管理系统和用户译码器中间的解密信息(数据)传输的过程和系统。

背景技术

付费电视用户的译码器包含一个可以处理通过缆线或赫兹传输的到达信号的解密单元。这些信号可以是模拟信号或数字信号。

这些信号有多种类型，依其是否包含音频信息，视频信息或控制信息而定。

后一类包括管理报文(称为 EMM 报文)，即包含指向译码器或译码器组的控制信号，和控制报文(称为 ECM 报文)，即特别是包含授权报文，允许传输中的信号进行解密的信息。

在本申请中，我们涉及的是目标为解密音频和视频信号的授权报文(ECM)。

建议向付费电视用户提供的内容包括多个根据一个或多个密钥进行加密的信道。这之所以必要是因为用户可订购一个信道而无权使用其他信道。

授权报文(ECM)利用适合于管理系统的密钥进行加密。用户的译码器包括一个可解密这些报文的安全密码装置。由于安全的原因，容许解密有用信号(视频和音频)的授权报文定期改变。管理系统在加密形式下将这些报文(ECM)传输到可解密这些报文的密码装置，管理授权并根据用户的权力将解密视频和音频信号所必需的信息传输给译码器。

由密码装置译码的结果称为“控制字”，缩写为“CW”。此控制字驾驭译码器而用户就可以充分利用所传输的信息。

如上所述，这些控制字定期改变以防止侵权者藉助功能强大的计算机计算出这一控制信息而从付费机构免费受益。这就是为何这些控制字定期改变，改变周期通常为 1 至 20 秒。这一周期称为密码周期。

授权报文(ECM)的发送频率较密码周期的发送频率高，比如每 100 毫秒。这是必不可少的，一方面是在开始译码服务时，另一方面是在变更信道时。

事实上，为了能够显现所要求的传输内容，必须有控制字才能将信号解密。但如果需要在屏幕前等候 5 秒钟图像才能清晰出现就不好了。

在第二种场合，每个信道都有控制字，人们需要等候密码周期结束来接收容许对新信道的信号进行解密的授权报文。如前面所述，人们不能接受改变信道时发生数秒的延迟。

这就是为何在实际中授权报文(ECM)的发送频率为 5~20/秒。

当改变信道时，分隔用户命令和显像所要求的信道的时间必须很短。按照通常的标准，500 毫秒的长度被认为是可以接受的。

在此时间内执行如下的操作：

-将音频、视频和控制滤波器置于新信道；

-等待包含所述信道的加密控制字的下一个报文(ECM)；

-接收此报文(ECM)并传输到密码装置用来解密；以及

-由密码装置执行此解密算法并返回解密控制字，将此控制字传输到译码器；

-开始 MPEG 解压并等待图像完全同步。

通过链接这些操作，可以看到，它不可能并行执行，并且其中的每一个都加入到决定改变信道时所需的最大时间长度。

已知，加密算法的安全性越高，解密所需的运算就越长。另一方面，直接参加信道转换时间计算的解密时间不可能延长来改进加密的质量。这也就是用来取得控制字的算法的安全性受到这些时间约束的强制限制的原因。

在文献 EP 0583202 中描述了一种已知方法，其构成在于向现用频

道发送的不仅包含有关信道的授权报文(ECM)，而且还包含其他信道的授权报文。这些后者是以较低频率传输以便不致发生传输拥塞。

这一方法的缺点是以不需要的报文使信道拥塞并且需要牢记更换信道时所使用的所有的授权报文。此文献另外一个未解决的问题是提高译码运算的质量(从而增加时间长度)不应该增加在信道间转换信道的时间。

发明内容

本发明的目的是提供一种加密信息的方法和传输系统，能够保证译码器的目标控制字的高安全性而无需延长特定信道的控制字的处理时间。

此目的可利用一个控制字而彻底达到，该控制字系通过将应用于每个信道的授权报文(ECM)的解密和一组信道共用的授权报文的解密结合起来而得到。

在下面的描述中，每个信道的报文称为“ 单信道授权报文(ECM)”，而一组信道的共用报文称为“ 多信道授权报文(MECM)”(主 ECM)。

处理报文(ECM)的算法是快速型，因而提供的是有限的安全性。这是由于从一个信道过渡的另一个信道的时间要求要很短所致。

另一方面，根据本发明，不可能只通过处理单信道授权报文(ECM)就得到控制字(CW)。密码装置要能够解密单信道授权报文(ECM)就必须包含接收到的多信道授权报文(MECM)中的信息。后者由一个称为系统的密钥解密，因为它独立于不同的信道。

在由一个信道改变或转换到另一个信道时，包含在单信道授权报文(ECM)中的适合新信道的信息与包含在已经在密码装置中的多信道授权报文(MECM)中的信息相结合，后者是两个信道共用的。这样，报文(MECM)的解密时间不像上述那样插入到转换时间的计算中。因此，报文(MECM)的解密算法可以更有效并需要更长的时间但却不会影响转换时间。另外，仅仅使用不同的算法就可增加系统的安全性。

多信道授权报文(MECM)的内容可根据对报文(ECM)完全相同的周期(密码周期)或根据此周期的倍数而改变。

如果两个单信道授权报文(ECM)之间的时间很重要，因为它直接插入两个信道之间的最大转换时间的计算中，它对于两个多信道授权报文(MECM)之间的时间是不同的。由于此报文对一组信道是共用的，它可以具有较长的时间。事实上，它的重复周期只在译码器加压时插入。在附图的场合，可以看到，每秒 1 至 2 个报文的重复是足够的。

附图说明

本发明通过下面的参考示例性而非限制性的附图的详细描述可以得到更好的理解，其中

-图 1 表示在两个信道 A 和 B 上(ECM)和(MECM)的传输;

-图 2 表示安全性密码装置。

具体实施方式

在图 1 中在两条线上示意地示出容许对视频和音频信号解密的报文。可以看到每个信道的单信道授权报文(ECM)都是以规律的间隔传输。在 “ A” 信道传输 “ A” 单信道授权报文(ECM)。在 “ B” 信道传输 “ B” 单信道授权报文(ECM)。信道 A 和 B 共用的多信道授权报文(MECM)在两个信道上传输。

在采用模拟传播的实现模式中，单信道和多信道授权报文在每个信道上都可以有效地传输，一个信道与一个频率相联系。另一方面，在数字传播系统中，不存在与频率相联系的信道的概念。多信道授权报文(MECM)可以在用于此信道的报文中相加或者以全局方式传输到信息流而不必在每个信道上重复。

根据此示例，多信道授权报文(MECM)的周期性比单信道授权报文(ECM)的周期性低一半。报文(MECM)的周期性由第一次使用时解码时间是可接受的来确定。在此场合，可以在收到至少一个报文(ECM)和一个报文(MECM)之后对信号进行解密。这就是为何对于报文(ECM)

大约 1 秒的重复是可接受的并且不会阻碍系统的通(频)带的原因。一旦收到报文(MECM) 并进行处理，它立刻可以在利用新的报文(ECM)改变信道时使用。

本发明的另一个方面是根据信道考虑从密码周期开始起的减缩。事实上，控制字的改变可根据信道在不同的时刻进行。因此，比如，在 “ A”信道，控制字(CW)改变，从 CW-A1 变为 CW-A2。根据本发明，此控制字是从那时起由于多信道授权报文(MECM-2)而得到的。另一方面，在假设新信道 B 永远要利用控制字(CW-B1)工作的场合，必须使用多信道授权报文(MECM-1)。这就是为何每个报文(MECM)包含数个密码周期的信息的原因，因此使信道同步没有差异。

图 2 示出在多信道授权报文(MECM)中传输的这些数据的功能。单信道授权报文(ECM)包含加密形式的控制字(CW)并传输到能够对此信息进行解密的密码装置(CU)。为此，它对定义与一般系统特别是与信道相关的权力的参数 P1，P2 至 Pn 进行处理。这一装置藉助于这些参数计算控制字(CW)。根据本发明，由报文(MECM)传输的数据一旦解密，就可以修改密码装置(CU)上游或其下游的参数。

根据本发明的一个具体形式，最终控制字(CW)是利用包含在报文(MECM)和报文(ECM)中间的逻辑运算得到的，这些逻辑运算为加、减、 “ 异”或乘。

根据本发明的一个具体形式，包含在报文(MECM)中的信息用作对单信道授权报文(ECM)的内容解密的第二密钥。

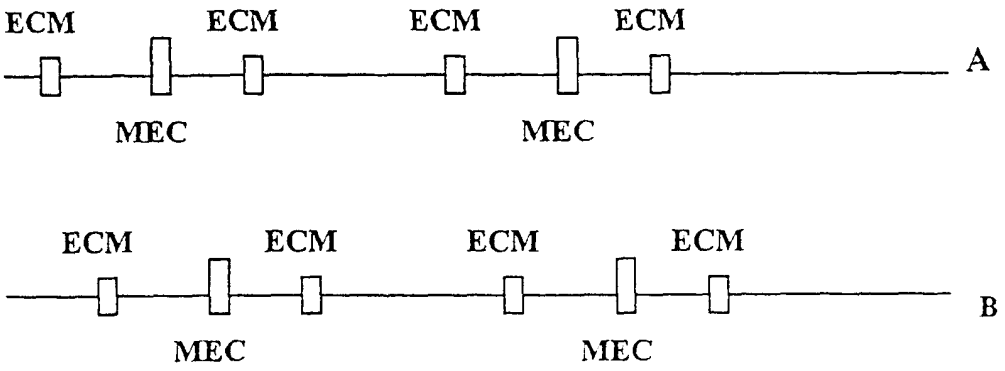

ECM
ECM
ECM
ECM
A
MEC
MEC
ECM
ECM
ECM
ECM
B
MEC
MEC

图 1

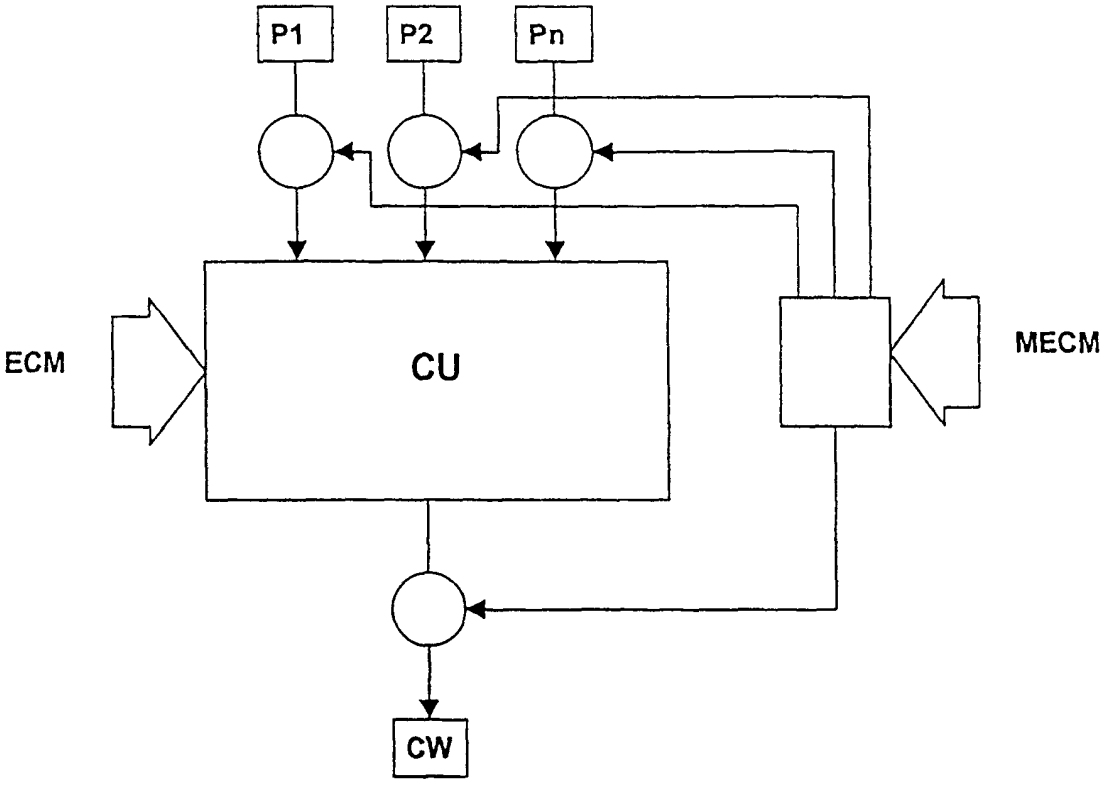

P1
P2
Pn
ECM
CU
MECM
CW

图 2