(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1295763 B
(45)授权公告日 2010.06.23

(21)申请号 99804446.6

(22)申请日 1999.12.27

(30)优先权数据
99200244.4 1999.01.28 EP

(85)PCT申请进入国家阶段日
2000.09.25

(86)PCT申请的申请数据
PCT/EP1999/010488 1999.12.27

(87)PCT申请的公布数据
WO00/45598 EN 2000.08.03

(73)专利权人 爱迪德艾恩德霍芬公司
地址 荷兰霍夫多普

(72)发明人 B·J·范里恩塞维尔

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 吴增勇 傅康

(51)Int.Cl.
H04N 7/167(2006.01)

审查员 丰学民

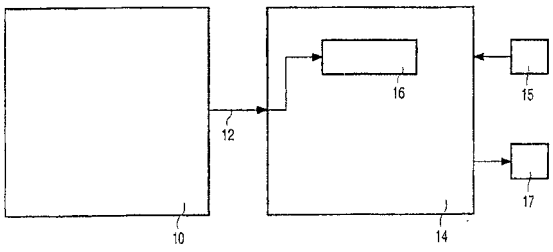
权利要求书 1 页 说明书 4 页 附图 1 页

(54)发明名称

传输系统

(57)摘要

传输系统包括发射机(10)和接收机(14)。发射机(10)可以向接收机(14)发送多路复用信号(12),例如MPEG-2传送流。多路复用信号(12)包含分别包括加密的数据分组和解密分组的第一和第二段。第一和第二段由所述第一和第二段的相同部分链接在一起。解密分组包含解密密钥(48)。数据分组可依靠解密密钥(48)解密,解密密钥(48)被重发多次。第一和第二部分还包含标题(20),后者包括表示所使用的解密密钥的变化的信息。接收机(14)包含滤波装置(16),用于根据这一信息滤出第二和其他相同解密密钥(48)事件。



CN 1295763 B

1. 用于从发射机 (10) 向接收机 (14) 发送多路复用信号 (12) 的方法，该方法包括：上述发射机 (10) 使所述多路复用信号 (12) 包含第一和第二段，所述第一段包含加密的数据分组，所述第二段包含解密分组，所述解密分组包含解密密钥 (48)，使得所述第一和第二段的至少一部分是相同的，所述第一和第二段由所述相同的部分链接在一起，上述接收机 (14) 使用一个滤波器以从上述多路复用信号 (12) 获得加密的数据分组和解密分组，并且上述接收机 (14) 还通过解密密钥 (48) 解密所述加密的数据分组。

2. 按照权利要求 1 的方法，其特征在于：所述发射机 (10) 使所述多路复用信号 (12) 包含的第一和第二段分别包含第一和第二标题 (20)，使得所述相同的部分被包含在所述标题 (20) 中。

3. 按照权利要求 1 或 2 的方法，其特征在于：所述发射机 (10) 使所述多路复用信号 (12) 包含的第一段中包括含 IP 分组的加密数据分组。

4. 按照权利要求 1 或 2 的方法，其特征在于：所述发射机 (10) 重发所述解密密钥 (48) 多次。

5. 按照权利要求 2 的方法，其特征在于：所述发射机 (10) 使所述第一和第二标题 (20) 包含表示所使用的解密密钥 (48) 变化的信息。

6. 按照权利要求 5 的方法，其特征在于：所述接收机 (14) 使用滤波装置 (16) 来根据所述信息滤出相同解密密钥 (48) 的第二和进一步的事件。

7. 一种在接收机接收从发射机 (10) 发送的多路复用信号 (12) 的方法，该方法包括：上述接收机 (14) 使用一个滤波器来获得包含在上述多路复用信号 (12) 的第一段中的加密的数据分组和获得包含在所述多路复用信号 (12) 的第二段中的解密分组，所述第一和第二段中至少一部分是相同的，使得所述第一和第二段由所述相同的部分链接在一起，使用所述滤波器、通过滤出包含所述相同部分的上述第一段和上述第二段中包括的所有的数据分组来获得所述加密的数据分组和所述解密分组，所述接收机 (14) 还通过所述解密密钥 (48) 解密所述加密的数据分组。

传输系统

技术领域

[0001] 本发明涉及用于从发射机到接收机传输多路复用信号的传输系统，所述多路复用信号包含第一和第二段，所述第一段包含加密的数据分组。

[0002] 本发明还涉及用于发送多路复用信号的发射机、用于接收多路复用信号的接收机和包含某一段的多路复用信号。

背景技术

[0003] 从文件草案 EN 301 192 V1.1.1 欧洲标准“数字视频广播 (DVB)；用于数据广播的 DVB 规范”中知道按照前序的传输系统。在现代数字广播系统中，发射机，即头端，通常向多个接收机、例如象电视机和机顶盒发送大量业务（或频道）。这样的业务可包含音频 / 视频数据流、交互式应用程序（例如以 MHEG-5 格式）、其它类型的数据或这些要素的组合。MPEG-2 传送流是若干业务的多路复用。通常，发射机发送几个传送流给机顶盒。机顶盒可以调谐到特定的传送流，然后可以从传送流检索信息。这样的机顶盒通常只有一个调谐器并因此一次只能接收单个传送流。当用户想看电视节目、或想运行交互式应用程序、或想访问其它类型的数据时，机顶盒或电视机调谐到对应的传送流，并接收和处理那个时刻正被广播的业务数据。

[0004] 在这样的系统中，希望只有有限数量的用户，例如只有已付费用或属于某个组的那些用户访问业务。这样有条件的访问业务可以通过对数据加密、通过发送加密的数据给接收机、和通过只向被授权享有所述数据的那些用户提供用于将所述数据解密所需的解密密钥来实现。借助所述解密密钥，接收机可以将所述数据解密。由于安全原因，解密密钥必须在一定的时期后或传输一定数量的数据后改变。向新的解密密钥的转换必须在发射机和接收机之间同步。

[0005] 在已知的传输系统中，发射机向多个接收机广播包含大量数据业务的传送流。每一个数据业务包括许多嵌入到单个数据部分中的加密的数据分组。

发明内容

[0006] 本发明的目的是提供传输系统，其中接收机或机顶盒可以有效地处理数据分组的解密。

[0007] 根据本发明，提供了一种用于从发射机向接收机发送多路复用信号的传输系统，上述发射机布置为使所述多路复用信号包含第一和第二段，所述第一段包含加密的数据分组，所述第二段包含解密分组，所述解密分组包含解密密钥，所述第一和第二段的至少一部分是相同的，所述第一和第二段由所述相同的部分链接在一起，其特征在于：上述接收机含有一个滤波器以从上述多路复用信号获得加密的数据分组和解密分组，上述接收机还包括通过解密密钥解密所述加密数据分组的装置。

[0008] 所述发射机布置为使所述所述多路复用信号的第一和第二段分别包含第一和第二标题，所述相同的部分被包含在所述标题中。所述发射机布置为使所述第一和第二标题

包含表示所使用的解密密钥变化的信息。通过在所述标题中包含这一信息，接收机可准确地确定何时开始使用新解密密钥。

[0009] 所述接收机包括滤波装置，用于根据所述信息滤出相同解密密钥的第二和进一步事件。借助这种措施，所述接收机仅仅必须处理解密密钥的第一事件。这意味着，例如在所述解密密钥本身被编码的情况下，所述接收机免于对第二和进一步的相同解密密钥事件进行编码。

[0010] 所述发射机布置为使所述所述多路复用信号的第一段中包括含 IP 分组的数据分组。这样，可利用 DVB 适应的基础结构来安全地广播定义在 IP 级的数据业务。

[0011] 所述发射机布置为重发所述解密密钥多次。借助这种措施，接收机可以迅速地访问所述解密密钥，以便实现对所述数据业务的快速访问。

[0012] 本发明还提供了一种用于向接收机发送多路复用信号的发射机，所述发射机布置为使所述多路复用信号包含第一和第二段，所述第一段包含加密的数据分组，其特征在于：所述第二段包含解密分组，所述解密分组包含解密密钥，所述第一和第二段中至少一部分是相同的，所述第一和第二段由所述相同的部分链接在一起，所述数据分组可依靠所述解密密钥解密。

[0013] 本发明最后提供了一种用于接收从发射机发送的多路复用信号的接收机，上述接收机含有一个滤波器以获得包含在上述多路复用信号的第一段中的加密的数据分组和包含在所述多路复用信号的第二段中的解密分组，所述第一和第二段中至少一部分是相同的，所述第一和第二段由所述相同的部分链接在一起，其特征在于所述滤波器通过滤出包含所述相同部分的上述第一段和上述第二段中的所有的数据分组来获得所述加密的数据分组和解密分组，所述接收机还包括通过所述解密密钥解密所述加密的数据分组的装置。

[0014] 从下面参考附图对最佳实施例的描述中，本发明的上述目的和特征将更加明显。

附图说明

[0015] 图 1 示出按照本发明的传输系统的方框图。

[0016] 图 2 示出被包含在一个部分中的数据分组的结构图。

[0017] 图 3 示出 SPI 字段的结构图的例子。

具体实施方式

[0018] 图 1 示出按照本发明的传输系统的方框图。在这样的传输系统中，代表许多数据业务的许多数据信号 12 或复合信号 12 由发射机 10 发送到接收机 14。该传输系统可以包括其它接收机 14。终端用户可以通过例如象键盘或遥控单元的输入装置 15 来控制接收机 14。被选择的业务可以显示在显示装置 17 上。可以借助数据信号 12，通过发射机 10 把数据分组、例如 IP 分组广播到许多接收机 14。

[0019] 在这样的传输系统中，最好只有有限数量的接收机 14 的用户、例如只有那些已经付费或属于某个组的用户，访问数据业务。这种有条件的访问数据业务可以通过在发射机 10 加密数据并发送该加密的数据到接收机 14 来实现。而且，解密数据所需的解密密钥本身被加密并且只有那些被授权享有所述数据的接收机 14 才能够对所述解密密钥解密。依靠解密密钥，接收机 14 可以将所述数据解密。解密密钥可以发送许多次，以便接收机 14 能够

迅速地访问解密密钥。

[0020] 发射机 10 以所谓的授权控制消息 (Entitlement Control Message) 或 ECM 的形式将解密密钥传送到接收机 14。这种可嵌入在 IP 分组中的 ECM 包含解密密钥或控制字的加密形式。通过在接收机 14 中将 ECM 解密，例如依靠包括在接收机 14 中的智能卡，如果接收机还具有相应的数据业务或授权，则该解密密钥可被揭示。出于安全的目的，控制字值经常改变，例如在一定的时期后或在一定数量的数据传输后。在控制字值已经改变的情况下，新 ECM 必须传送到接收机。因此 ECM 流与每一个可以有条件地访问的数据业务相联系。可能需要重发未改变的 ECM 好几次，以便减小接收机 14 访问所述业务占用的时间。（为了访问业务，接收机 14 必须首先获取相应的 ECM。）接收机 14 中可以包括滤波装置 16，用于滤出第二和进一步的相同解密密钥事件的目的。

[0021] 用于计算机网络环境下的、例如因特网的广播数据业务的传输系统的例子可从文件 RFC 1825“用于互联网协议的安全体系结构”(1995 年 8 月）中了解到。在这一文件中，描述了 IP 分组加密的两种方式：

[0022] 传送方式：IP 分组的有效载荷被加密。

[0023] 隧道方式：整个 IP 分组被加密，并且新的 IP 标题位于加密后的分组前。这种方式，例如，用来加密通过非受托网络的虚拟专用网的业务。

[0024] 在两种方式中，所谓的 ESP(Encapsulating Security Payload- 封装安全有效载荷）标题包括在包含加密的数据的新建立的 IP 分组中。这种 ESP 标题从被称为安全参数索引 (SPI) 的 32 位的字段开始。与目标地址一道，SPI 尤其限定了哪些密钥用于解密、使用哪些解密算法以及怎样应用解密算法。

[0025] 从文件草案 EN 301 192 V1.1.1 欧洲标准“数字视频广播 (DVB)；用于数据广播的 DVB 规范”中知道用于广播数据业务的传输系统。这种已知的传输系统例如可以在有线电视 (CATV) 网络环境中实现。在这种环境中，发射机 10 包括 CATV 网络的头端，接收机 14 包括终端用户的机顶盒、电视机或个人计算机 (PCs)。数字信号 12 包含多路复用信号 12，后者可以以 MPEG-2 传送流的形式实现。MPEG-2 传送流是许多所谓业务的多路复用。这样的业务可包含音频 / 视频流、交互式应用程序（例如以 MHEG-5 格式）、其它类型的数据（例如 IP 分组）或这些成分的组合。通常，头端 10 向机顶盒 14 发送几个传送流 12。这样，大量业务（或频道）能通过头端 10 广播到许多机顶盒 14。

[0026] 机顶盒 14 可以调谐到特定的传输流 12，然后可从传输流 12 检索信息。这样的机顶盒通常只有一个调谐器并因此一次只能接收单一传输流 12。当用户想要看电视节目时，或想要运行交互式应用程序时，或想要访问其它类型的数据时，机顶盒 14 调谐到相应的传输流 12，并从那个时刻正被广播的业务中检索和 / 或处理所需要的数据。

[0027] 图 2 示出数据分组的结构图，该数据分组被包含在第一段中。DVB 已定义了用于数据广播的 6 个协议栈。这些协议栈之一是所谓的多协议封装 (multi-protocol encapsulation) 或 MPE。在这种情况下，在数据分组和 MPEG 段之间存在着一对一的映射。并且 MPEG 段通常以几个 MPEG-2 传送流分组的形式发送。MPEG 段具有特定的类型，如协议层 DSM-CC 专用数据和 DVB 多协议封装所定义的。在图 2 所示的结构图中，数据分组是 IP 分组，它包含 IP 标题 22、ESP 标题 24 和加密的 IP 有效载荷或数据字段 26。数据字段 26 可依靠改变的解密密钥 48 来解密。ESP 标题包含所谓的安全参数索引 (SPI) 字段。MPE 段

标题 20 表明数据分组被嵌入到 MPE 段。ECSs 也可嵌入到相同的结构中。包含 ECM 的分组称为解密分组。解密分组最好被包括在与包含数据分组的第一段链接的第二段中。第一和第二段依靠第一和第二段的至少一部分而链接在一起，所述一部分对所述两段来说是相同的。通过把加密的数据分组和与其有关的解密分组集中在链接在一起的部分中，接收机利用滤出所有包含所述相同部分的分组的单个滤波器可以容易地获得所述数据分组和解密所述数据分组所需的解密分组。所述相同的部分最好被包括在所述部分标题 20 中。例如，在文件草案 EN 301192V1.1.1 欧洲标准“数字视频广播 (DVB)；用于数据广播的 DVB 规范”中，表 3 中定义的 MPE 段标题 20 的 table_id 和 / 或 MAC_address 部分可以用以这一目的。

[0028] 图 3 示出 SPI 字段结构图的例子。这是用于因特网的所有不同 IP 解密方法的仅有强制字段，因此这一字段是不变的。其目的是标识（与目的地址一道）接收机 14 应当使用哪些密钥和算法解密数据。在本实施例中，SPI 字段的开始 14 位被用来存储 ECM 流参考符号 30，后者提供 ECM 流和加密的数据之间的关联。第 15 位用来存储表示密钥变化的信息 32。依靠这一信息 32，可以在传输系统中使控制字的变化同步。当用以加密数据的控制字改变其值时，同步位 32 相应改变其值。这允许接收机 14 准确地确定何时开始使用新控制字值。SPI 字段的第 16 位 34 被保留将来使用。SPI 字段的最后 16 位被用来存储传输系统使用的有条件访问系统的标识符 36。

[0029] 表明解密密钥变化的信息 32 也可以存储在多位计数器中。

[0030] 对于接收机 14 中的智能卡来说，处理 ECM 是花费时间的。因此为了避免对加密数据的扩大缓冲的需要，在实际使用相应的控制字之前的一些时候应发送新 ECM。在接收机 14 还使用旧控制字解密数据时，它必须存储新控制字。通常将相同的 ECM 发送几次，以便减少业务访问时间。为了将业务解密，首先必须将 ECM 解码，以便获得控制字。如果没有传输误差，ECM 包含单一控制字就足够了。可是如果 ECM 包含两个连续的控制字，则可得到更健全的系统。如果在 ECM 中有两个或更多连续的控制字，重发相同的 ECM 在由于传输误差而可能丢失 ECM 时增加了接收到控制字的可能性。

[0031] 在 MPE 段的标题 20 中，已经定义所谓的 payload_scrambling_control 字段（两位），用来表示改变到另一个控制字（见文件草案 EN 301 192 V1.1.1 欧洲标准“数字视频广播 (DVB)；用于数据广播的 DVB 规范”中表 3）。对于包含数据的 IP 分组，这些同步位表示内容被加密 (11) 或没有被加密 (00)。对于传送 ECM 的 IP 分组，所述位表示控制字是偶数 (01) 或非偶数 (10)。这些同步位可被最好是硬件滤波器的滤波装置 16 使用，用来滤出多个相同 ECM 情况，以便不必由软件来去除这些相同 ECM 情况。如果使用加密，则滤波装置 16 在 (1x) 和 (x1) 之间交替。最初，滤波装置 16 使用滤波器 1x。这意味着当第一控制字（非偶数）已通过滤波装置 16 时开始使用滤波器 x1。第一控制字的第二和进一步的事件被滤波装置 16 滤出。第二控制字（偶数）的第一事件通过滤波装置 16，之后，滤波装置 16 开始使用滤波器 1x。第二控制字的第二和进一步的事件被滤波装置 16 滤出。第三控制字的第一事件现在可以通过滤波装置 16 等等。

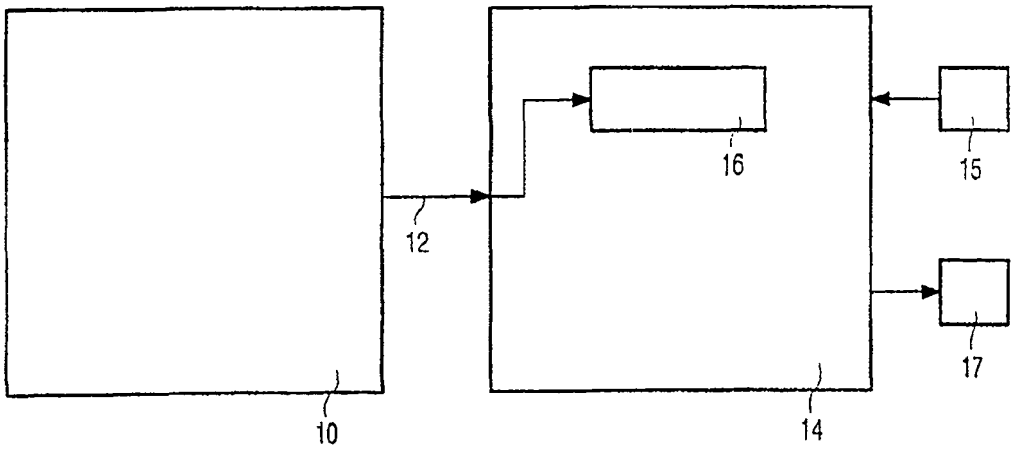


图 1

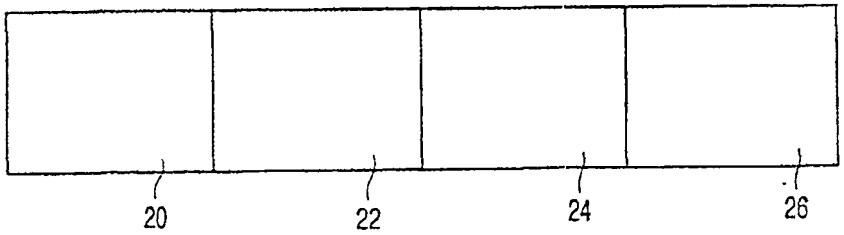


图 2

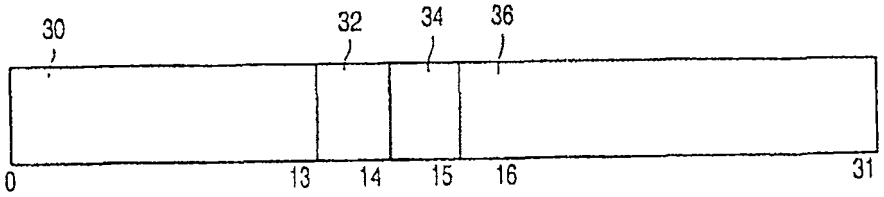


图 3