(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 1633809 B
(45)授权公告日 2010.04.21

(21)申请号 02828452.6
(22)申请日 2002.12.13
(30)优先权数据
2,405,865 2002.10.01 CA
10/037,914 2002.01.02 US
(85)PCT申请进入国家阶段日
2004.09.02
(86)PCT申请的申请数据
PCT/US2002/040051 2002.12.13
(87)PCT申请的公布数据
WO2003/061173 EN 2003.07.24
(73)专利权人 索尼电子有限公司
地址 美国新泽西州
(72)发明人 B·L·坎德洛尔 R·A·昂格尔
L·M·小佩罗 G·米尔斯基
M·K·艾尔
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 程天正 陈景峻
(51)Int.Cl.
H04N 7/167(2006.01)
(56)对比文件
US 6229895 B1,2001.05.08, 全文.
US 5915018 A,1999.06.22, 全文.
审查员 刘园园

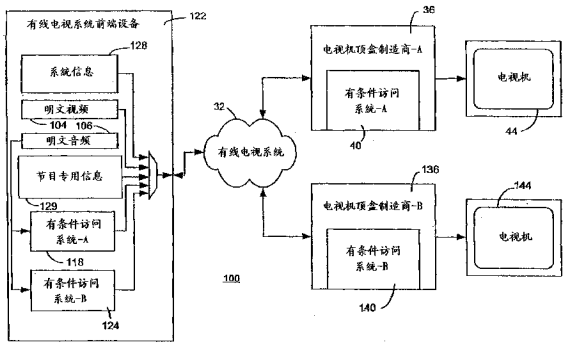
权利要求书 2 页 说明书 28 页 附图 16 页

(54)发明名称

基本流部分加密

(57)摘要

用于对电视节目多重加密的加密安排。本发明实施例的系统仅对完全呈现电视节目所需的一部分数据进行多重加密,以允许在单个系统中有与多个制造商的机顶盒相关的多个有条件访问加密系统共存。在一个实施例中,仅有音频数据是加密的,视频保持为明文。通过仅对节目的一部分进行加密,与其它对所有电视节目进行多重加密相比,消耗少得多的带宽,从而可以在同样带宽上传送更多的节目,同时使得在单个有线电视系统中有多个有条件访问系统共存。



CN 1633809 B

1. 一种对数字电视信号进行多重加密的方法，包括：

根据第一加密方法对数字电视信号的所选定基本流加密，以形成第一加密基本流；

根据第二加密方法对数字电视信号的所选定基本流加密，以形成第二加密基本流；以及

将第一加密基本流和第二加密基本流与数字电视信号的至少一个未加密的基本流组合起来，以形成部分多重加密的电视信号。

2. 如权利要求 1 的方法，其中，用分组标识符 (PID) 或业务流标识符 (SSID) 标识出所述选定的基本流分组以便进行加密。

3. 如权利要求 1 或 2 的方法，还包括在有线电视系统、地面广播系统和卫星系统之一中发布所述部分多重加密的电视信号。

4. 如权利要求 1 的方法，其中，所述多重加密包括对被标识为音频基本流分组、视频基本流分组和系统信息基本流分组之一的分组进行多重加密。

5. 如权利要求 1 的方法，其中，所述选定的基本流是分组化的，并且，所述分组由分组标识符 (PID) 来标识，并且在节目映射表 (PMT) 中引用所述分组标识符。

6. 一种电视信号接收设备，包括：

接收器，接收双重部分加密的电视信号，该信号包括用第一加密算法和第二加密算法加密的基本分组流以及未加密的分组；

解密器，从所述接收器接收用第一加密算法加密的基本流分组，并用第一解密算法对所述加密的基本流分组进行解密；以及

解码器，对所述解密的基本流分组和未加密的分组进行接收和解码，以便形成适于在电视接收器上播放的电视信号。

7. 如权利要求 6 的设备，其中，所述接收器还丢弃用第二加密算法加密的基本流分组。

8. 如权利要求 6 或 7 的设备，其中，用分组标识符 (PID) 或业务流标识符 (SSID) 标识出选定的基本流分组以便进行加密。

9. 如权利要求 6 的设备，其中，所述多重加密包括对被标识为音频基本流分组、视频基本流分组和系统信息基本流分组之一的分组进行多重加密。

10. 如权利要求 6 的设备，其中，选定的基本流分组由分组标识符 (PID) 来标识，并且在节目映射表 (PMT) 中引用所述分组标识符。

11. 如权利要求 6 的设备，其中，从地面广播系统、卫星系统和有线电视系统之一中接收所述双重部分加密的电视信号。

12. 一种对多重部分加密的电视信号进行解码的方法，包括：

接收具有多重加密基本流和未加密部分的电视信号，其中，所述多重加密的基本流包括用第一加密方法加密的第一加密基本流部分和用第二加密方法加密的所述基本流部分的一个复制品；

对第一加密的基本流进行解密，以形成解密的基本流；

对解密的基本流和未加密部分进行解码，以形成解码的电视信号。

13. 如权利要求 12 的方法，其中，所述解码的信号适于在电视机上播放。

14. 如权利要求 12 或 13 的方法，其中，所述第一加密基本流是由与用来对第一加密基本流进行解密的第一解密算法相关联的第一分组标识符 (PID) 来标识的，而由第二加密算

法加密的基本流部分的复制是由用于对基本流部分的复制品解密的第二解密算法相关联的第二分组标识符 (PID) 来标识的。

15. 如权利要求 14 的方法，还包括通过 PID 过滤丢弃所述第二加密算法加密的音频部分。

16. 如权利要求 12 的方法，它是在集成电路、电视接收器设备、电视和电视机顶盒之一中执行的。

基本流部分加密

[0001] 相关文件的交叉引用

[0002] 本申请涉及Candelore等人的US临时专利申请第60/296,673号、Unger等人的临时专利申请第60/304,241号、Candelore等人的临时专利申请第60/304,131号以及Candelore等人的US临时专利申请第60/_____号。其中,临时US临时专利申请第60/296,673号于2001年6月6日提交,题为“在内容传送系统中通过明文发送某些内容的视频而使多个CA供应商互操作的方法以及音频的双重传输和用于其它内容的视频和音频的双重传输(Method for Allowing MultipleCA Providers to Interoperate in a Content Delivery System bySending Video in the Clear for Some Content,and Dual Carriageof Andio and Dual Carriage of Video and Audio for OtherContent)”;临时专利申请第60/304,241号于2001年7月10日提交,题为“用于双重传输的节目内容的无约束选择性加密(IndependentSelective Encryption of Program Content for Dual Carriage)”;临时专利申请第60/304,131号于2001年7月10日提交,题为“在内容传送系统通过根据时间片部分扰乱内容而使多个CA供应商互操作的方法(Method for Allowing Multiple CA Providers to Interoperatein a Content Delivery System by Partial Scrambling Content ona Time Slice Basis)”;US临时专利申请第60/_____号于2001年10月26号提交,题为“电视加密系统(Television EncryptionSystems)”,文档号为SNY-R4646P。本文引用了这些专利申请以作参考。

[0003] 本申请与下列文件同时提交:Unger等人的文档号为SNY-R4646.01的专利申请,题为“关键部分加密(Critical Packet PartialEncryption)”,序列号为_____;Candelore等人的文档号为SNY-R4646.02的专利申请,题为“时分部分加密(Time DivisionPartial Encryption)”,序列号为_____;Unger等人的文档号为SNY-R4646.04的专利申请,题为“部分加密和PID映射(PartialEncryption and PID Mapping)”,序列号为_____;以及,Unger等人的文档号为SNY-R4646.05的专利申请,题为“对部分加密的信息进行解码和解密(Decoding and Decrypting of Partially EncryptedInformation)”,序列号为_____。本文引用了这些同时提交的专利申请以作参考。

[0004] 版权声明

[0005] 本专利文件的公开内容的一部分包括受版权保护的材料。版权拥有者不反对在专利商标事务所的专利文件或记录中影印复制专利文件或专利公开内容,但在任何情况下都保留所有的版权。

发明领域

[0006] 本发明在总体上涉及加密系统领域。具体地说,本发明涉及用于对电视信号的数字进行部分加密和解密的系统、方法和设备。

[0007] 发明背景

[0008] 电视被用来将娱乐和教育信息传送给观众。源材料(音频、视频等)被多路复合成组合信号,这种信号被用来调制载波。所述载波一般称为频道。(一个典型的频道可以

载送一个模拟节目、一个或两个高清晰 (HD) 数字节目或若干（例如九个）标准清晰数字节目）。在地面系统中，这些频道对应于政府安排的频率并在空中传播。节目被传送给有调谐器的接收机，调谐器接收来自空中的信号并将其传送给解调器，解调器则将视频提供给显示器并将音频提供给扬声器。在有线电视系统中，在电缆上传送经调制的频道。还可以在波段内或波段外馈送节目指南，以指示什么节目是可用的以及指示相关调谐信息。有线频道的数量是有限的，受限于设备 / 电缆的带宽。有线发布系统需要巨大的资金投入，并且升级昂贵。

[0009] 大量电视内容对其制片商来说是有价值的，所以，版权持有者要控制访问并限制拷贝。典型的受保护材料的实例包括故事片、体育赛事以及成人节目。有条件访问 (CA) 系统用于控制诸如有线电视系统之类的内容传送系统中的节目的可用性。CA 系统是匹配的成套装置 -- 一部分集成在有线电视系统的前端设备中并对有效负载进行加密，另一部分则进行解密并被嵌在安装在用户家中的机顶盒 (STB) 内。在有线电视产业中使用多种 CA 系统，包括 NDS(Newport Beach，加利福尼亚州）、摩托罗拉 (Schaumberg，伊利诺斯州）和 Scientific Atlanta（亚特亚大，乔治亚州）所提供的系统。CA 系统的这种匹配装置方面具有这样的效果 :“传统的”销售商被锁定为附加的 STB 的供应商。由于用于有条件访问的多种技术并不是相互兼容的（通常是专有的），故任何新的潜在的供应商都被迫要对传统 CA 授权。因此，有线电视经营者会发现它们自己不能从其它机顶盒制造商那里获得更新的技术或有竞争力的技术，这是因为，技术的拥有者通常不愿意合作或收取合理的许可费。当一些具有完全不同的 CA 系统的有线电视公司相合并时，这种不灵活性特别麻烦。服务供应商因多种理由而喜欢有一个以上的用于 STB 的节目源。

[0010] 一旦有线电视经营者选取了一种加密方案，在不引入向后兼容的解码设备（例如机顶盒）的情况下很难改变或升级该内容加密方案。即便技术对 STB 销售商是可用的从而 STB 销售商能提供多种解密能力，在新式机顶盒中提供处理多种加密系统的多模式能力也会显著增加任何新式机顶盒的成本。

[0011] 唯一已知的避免传统销售商的支配（不进行大量替换）的当前选择是使用“全双重传输”。全双重传输意味着对每个加密的节目都进行重复的传输 ---- 每个传输使用一种类型的 CA 加密。为了提供全双重传输，要增强前端设备 (headend)，以便同时提供各种形式的 CA。传统 STB 不应受到影响，并且无论有任何变化仍应继续执行它们的功能。但是，全双重传输通常会因带宽影响而有较高的价格，从而会减少可用的特色节目的数量。一般地说，较高收费频道的数量贫乏会使观众可用的选择的数量受到限制，有线电视经营者所能提供的价值也会受到限制。

[0012] 传统的有线电视系统安排如图 1 所示。在这种系统中，有线电视经营者在有线电视系统前端设备 22 处靠来自制造商 A（系统 A) 的 CA 技术用与系统 A 兼容的 CA 加密设备 18 处理音频 / 视频 (A/V) 内容 14。加密的 A/V 内容连同系统信息 (SI)26 和节目专用信息 (PSI) 被多路复用到一起并经有线电视系统 32 被传给用户的 STB36。STB36 包括来自系统 A（制造商 A) 的对 A/V 内容进行解密的解密 CA 设备。解密后的 A/V 内容随后可被提供给电视机 44 以供用户观看。

[0013] 在诸如图 1 中的有线电视系统中，数字节目流被分成了分组以进行传输。节目的每个组成部分的分组（视频、音频、辅助数据等）都标有分组标识符或 PID。频道内载送的

这些用于所有节目的各个组成部分的分组流被集合成一个复合流。还包括额外的分组以便提供解密密钥和其它开销信息。另外，未使用的带宽用空分组填充。带宽预算通常被调节成利用约 95％的可用频道带宽。

[0014] 开销信息通常包括指南数据，它说明什么节目是可用的，以及如何确定相关频道和组成部分的位置。这种指南数据也称为系统信息或 SI ：SI 可在波段内（在频道内编码的数据的一部分）或在波段外（用专用于此目的特殊频道）传送给 STB。以电子方式传送的 SI 可以按更传统的形式（即报纸和杂志中出版的网格）来部分地复制。

[0015] 为了使得观众有满意的电视体验，一般需要观众能清楚地访问音频和视频内容。某些模拟有线电视系统业已使用多种过滤技术来使视频模糊不清，从而防止非授权观众接收尚未付费的节目。在这种系统中，模拟音频有时是以明文 (in the clear) 发送的。在 C 波段卫星传输中使用的摩托罗拉 VideoCipher2Plus 系统中，使用了强数字音频加密和较弱的模拟视频保护（用同步倒置）。在航空公司的飞机电影系统中，只能通过租用耳机利用音频，从而仅为付费的顾客提供完整的音频和视频。

[0016] 附图简述

[0017] 后附权利要求书具体说明了被认为是新颖的本发明特征。但是，通过参照以下对本发明的详细说明可以在组织和操作方法及其目的和优点方面更好地理解本发明自身，以下的内容连同附图说明了本发明的某些示例性实施例，在附图中 ：

[0018] 图 1 是传统的有条件访问有线电视系统的框图 ；

[0019] 图 2 是与本发明一个实施例相一致的系统的框图，其中，连同明文视频一道传输双重加密的音频 ；

[0020] 图 3 是与本发明一个实施例相一致的系统的框图，其中，根据时间片机制对部分节目进行了双重加密 ；

[0021] 图 4 是与本发明某些实施例相一致的双重加密处理的流程图 ；

[0022] 图 5 是与本发明某些实施例相一致的解密处理的流程图 ；

[0023] 图 6 是与本发明一个实施例相一致的系统的框图，其中，在分组基础上对部分节目进行了双重加密 ；

[0024] 图 7 是与本发明某些实施例相一致的双重加密处理的流程图 ；

[0025] 图 8 是与本发明某些实施例相一致的解密处理的流程图 ；

[0026] 图 9 是与本发明一个实施例相一致的系统的框图，其中，对系统信息进行了加密，并且以明文发送节目 ；

[0027] 图 10 是与本发明多个实施例相一致的一般系统的框图 ；

[0028] 图 11 是有线电视系统前端设备中与本发明实施例相一致的加密系统的实现形式的第一实施例的框图 ；

[0029] 图 12 是有线电视系统前端设备中与本发明实施例相一致的加密系统的实现形式的第二实施例的框图 ；

[0030] 图 13 是用于在有线电视系统前端设备中实现本发明某些实施例的整个加密处理的流程图 ；

[0031] 图 14 是与本发明实施例相一致的解码系统的机顶盒实现形式的第一实施例的框图 ；

[0032] 图 15 是有线电视系统 STB 中与本发明实施例相一致的解码系统的实现形式的第二实施例的框图；

[0033] 图 16 是有线电视系统 STB 中与本发明实施例相一致的解码系统的实现形式的第三实施例的框图；

[0034] 图 17 说明了在机顶盒 PID 重映射器的一个实施例中实现的 PID 重映射过程；

[0035] 图 18 是可以在依照本发明的电视机顶盒中使用的示例性解码器芯片的框图。

[0036] 发明详述

[0037] 尽管本发明有多种不同形式的实施例，但在附图中示出并详细说明了具体的实施例，应该认识到，本公开内容应被认为是本发明原理的实例，而不是要将本发明限于所示和所说明的具体实施例。在以下的说明中，相同的标号用于说明多个图中相同、相似或相应的部分。术语“扰乱”和“加密”以及它们的变化形式在本文中是同义的。还有，术语“电视节目”和类似的术语可用通常的传统意义来解释，该术语也指可在电视机或类似监视器设备上显示的 A/V 内容的任何片段。

[0038] 概述

[0039] 现代数字有线电视网络一般使用可完全加密数字音频和视频的 CA 系统，以使得除那此已适当订购的人以外不能由其他人访问节目。这种加密被设计成能阻止黑客和非订户接收未经付费的节目。但是，由于有线电视经营者希望向其订户提供来自不同制造商的机顶盒，故他们会因需要传输用与各个 STB 制造商的 CA 系统相兼容的多种加密技术来加密的单个节目的多个拷贝而感到失望。

[0040] 这种传输节目的多个拷贝（称为“全双重传输”）的需要会耗尽有价值的带宽，而这种有价值的带宽可用于向观众提供额外的节目内容。本发明的某些实施例可以解决这一问题，其中，可以使将同样的内容提供给多个传输的带宽需求达到最小。结果可以称为“虚拟双重传输”，因为在没有全带宽成本的情况下提供了全双重传输的好处。本文中提出的本发明的若干实施例可用于实现有效地部分扰乱。这些实施例随用于选择要加密的部分的标准而变。所选择的部分则又会影响额外的带宽要求以及加密的效果。应该以与本发明实施例相一致的方式使用一种加密处理或若干加密处理的组合。

[0041] 本文所述的部分双重加密的某些实现形式使用了用于各个复制的组成部分的额外（次）PID。这些次 PID 被用于利用额外的加密方法来标记载送复制内容的分组。增强 PSI 以便按下述方式传输有关新 PID 存在的信息：所插入的 PID 被传统 STB 忽略，但可很容易被新 STB 提取。

[0042] 部分双重加密的某些实现形式包括仅复制用给定 PID 标记的特定分组。下文详述用于选择要加密哪些分组的方法。原始（即传统）PID 继续标记用传统加密来加密的分组以及明文传送的其它分组。新 PID 用于标记用第二加密方法来加密的分组。带有次 PID 的分组遮蔽用主 PID 标记的加密分组。构成加密对的分组可以按两种顺序出现，但在优选实现形式中，可按 PID 流的明文部分来保持顺序。正如从以下说明中可以看出的那样，通过使用主次 PID，位于机顶盒内的解码器可很容易地确定哪些分组可用与该机顶盒相关的解密方法来解密。后面将更详细地说明用于操作 PID 的处理过程。

[0043] （根据一种分类方法）本文所述的加密技术可以大致分成三种基本变化形式：仅加密主要部分（即音频）、仅加密 SI、仅加密选定的分组。一般地说，本文所公开的实施例

中使用的每种加密技术都试图对 A/V 信号或相关信息的一部分进行加密，同时使 A/V 信号的另一部分保持为明文，以便节省带宽。由于相同的明文部分可以发送给所有不同的机顶盒，故可以节省带宽。用多种方法来选择要加密的信息部分。这样，本发明的多个实施例可以消除在一种特定扰乱方案中加密整个内容的传统“强力”技术，而这意味着在希望有其它扰乱方案的情况下对带宽的冗余使用。此外，本文所述的每个部分双重加密方案可在不脱离本发明实施例的情况下被用作单个的部分加密方案。

[0044] 本发明的多种实施例以单独或组合的方式使用了多种处理过程，以便以明文的方式发送内容的主要部分，同时只对正确再现内容所需的少量信息进行加密。所以，与完全复制每一个所期望的节目流相反，所传输的按特定扰乱方案进行独特加密的信息的量只占内容的一小部分。就本文件中的示例性系统而言，加密系统 A 始终被认为是传统系统。以下详述上述几种加密技术中的每一种技术。

[0045] 本发明的各种实施例允许独立操作每个参与的 CA 系统。每个 CA 系统均与其它的 CA 系统互不相关。不需要前端设备中的密钥共事，这是因为各系统均对自己的分组加密。各 CA 系统均可使用不同的密钥出现时间。例如，用摩托罗拉专有加密法来加密的分组可利用嵌入式安全 ASIC 而使用快速变化的加密密钥，而用 NDS 的基于智能卡的系统来加密的分组则可使用变化较慢的密钥。对 Scientific Atlanta 和摩托罗拉传统加密来说，上述实施例可以同样好地工作。

[0046] 加密的基本流

[0047] 现参照图 2，将可以减少对额外带宽的需要而提供多个传输的系统的一个实施例说明为系统 100。在这一实施例中，系统利用了这样的事实：通常不希望在没有音频的情况下观看电视节目。尽管有例外（例如成人节目、某些体育赛事等），但一般的观众不可能接受在不能听到声音的情况下对电视节目作日常性的观看。因此，在前端设备 122 处，以明文（未加密）的方式提供视频信号 104，同时将明文音频 106 提供给多个 CA 系统，以便在有线电视网络上广播。在示例性的系统 100 中，明文音频 106 被提供给加密系统 118，系统 118 用加密系统 A 对音频数据加密（加密系统 A 在整个文件中被看作是传统的系统）。同时，明文音频 106 被提供给加密系统 124，系统 124 用加密系统 B 对音频数据加密。明文视频与来自 118 的加密音频（音频 A）、来自 124 的加密音频（音频 B）、系统信息 128 和节目专用信息 129 多路复用到一起。

[0048] 在经由有线电视系统 32 发布之后，视频、系统信息、节目专用信息、音频 A 和音频 B 都被传送给机顶盒 36 和 136。在传统 STB36 处，显示视频并且在 CA 系统 A40 对加密的音频进行解密，以便在电视机 44 上播放。同样，在新 STB136，显视视频并且在 CA 系统 B 对加密的音频进行解密，以便在电视机 144 上播放。

[0049] 与完整的 A/V 节目（甚至只是视频部分）相比，音频具有较低的带宽要求。384Kb/秒的立体声音频的当前最大的位速率约为 3.8Mb/ 秒的电视节目的 10％。因此，就带有用 256QAM（正交调幅）来传输的 10 个频道的系统中的加密音频（视频按明文方式传输）的双重传输而言，仅会损失约一个频道的带宽。所以，可传输约九个频道。这对所有频道的双重加密的要求来说是显著的改进，对所有频道的双重加密会使可用的频道从十个降至五个。在认为必要的情况下，对于例如体育赛事、付费观看、成人节目等，如果需要仍可对音频和视频两者进行双重加密。

[0050] 传统的和新机顶盒可以按常规方式发挥作用，即接收明文视频并以与用于对加密的 A/V 内容进行完全解密相同的方式对音频进行解密。如果用户没有订购按上述方案加密的节目，用户最多只能看到视频，但不能听到音频。就对视频的增强的安全性而言，也可能使用本发明的其它实施例（后面将予以说明）。（例如，可以扰乱 SI，以使得未授权的机顶盒更难以调谐到节目的视频部分）。尚未被黑客修改的未授权的机顶盒会因为接收到加密的音频而使视频消隐。

[0051] 授权的机顶盒接收授权控制消息 (ECM)，该消息用于取得访问标准和去扰乱密钥。机顶盒尝试将密钥应用于视频和音频。由于视频未被扰乱，故视频会不受影响地通过机顶盒的去扰乱器。机顶盒不管视频是明文的。对被扰乱的音频和明文视频来说，未经修改且未订购的机顶盒表现为未被授权。视频以及实际被扰乱的音频会被消隐。TV 上会出现屏幕上显示，以指示观众需要订购节目。这理想地完全禁止偶然的观众听到或看到内容。

[0052] 在本发明的一个实施例中，加密的音频作为数字分组在 A/V 频道上传输。传输根据系统机顶盒使用的两个（或多个）加密系统所加密的两个（或更多）音频流。为了使两个（或多个）STB 能正确地对各自的音频流进行解密和解码，从有线电视系统的前端设备 122 传输 SI（系统信息）数据，前端设备 122 使用所传输的用来确定音频位置的服务标识符来标识在其中可找到音频的特定频道。这一点是通过将第一分组标识符 (PID) 分配给系统 A 的音频并将第二分组标识符 (PID) 分配给系统 B 的音频而实现的。举例来说（但不是为了限制），可发送节目专用信息 (PSI) 以标识用于两个系统的音频的位置，这两个系统一个使用 NDS 有条件访问，另一个使用摩托罗拉有条件访问。本领域熟练技术人员应该能理解如何使这种信息适用于本文后述的部分加密的其它实施例。

[0053] SI 可以独立地被传送给传统和非传统机顶盒。可发送 SI 信息，以使传统和非传统机顶盒可以基本没有冲突地进行操作。在发送给传统机顶盒的 SI 中，VCT（虚拟频道表）会表明期望的节目（例如标记为节目号 1 的 HBO）在服务 ID“1”上并且设置了 VCT 访问控制位。发送给第一 STB 的网络信息表 (NIT) 会指出服务 ID“1”在频率＝ 1234 处。在发送给非传统机顶盒的 SI 中，VCT 表明期望的节目（例如标记为节目号 1001 的 HBO）在服务 ID“1001”上并且设置了 VCT 访问控制位。发送给非传统 STB 的网络信息表会指出服务 ID“1001”在频率 1234 处。以下的示例性节目关联表 PSI 数据被发送给传统和非传统机顶盒（按 MPEG 数据结构格式）：

[0054]

在 PID = 0x0000 上发送的 PAT
PAT0x0000
- 传输流 ID
-PAT 版本
- 节目号 1
-PMT0x0010
- 节目号 2
-PMT0x0020
- 节目号 3
-PMT0x0030
- 节目号 4
-PMT0x0040
- 节目号 5
-PMT0x0050
- 节目号 6
-PMT0x0060
- 节目号 7
-PMT0x0070
- 节目号 8
-PMT0x0080
- 节目号 9
-PMT0x0090
- 节目号 1001
-PMT0x1010
- 节目号 1002
-PMT0x1020
- 节目号 1003
-PMT0x1030
- 节目号 1004
-PMT0x1040
- 节目号 1005

-PMT0x1050
- 节目号 1006
-PMT0x1060
- 节目号 1007
-PMT0x1070
- 节目号 1008
-MT0x1080
- 节目号 1009
-PMT0x1090

[0055] 传统和非传统机顶盒有选择地接收以下示例性节目映射表 PSI 数据（按 MPEG 数

据结构格式）：

[0056]

在 PID ＝ 0x0010 上发送的 PMT PMT0x0010 -PMT 节目号 1 -PMT 段版本 10 -PCRPID0x0011 - 基本流 - 流类型（视频 0x02 或 0x80） - 基本 PID(0x0011) - 描述符 - 用于 CA 供应商 #1 的 CA 描述符 (ECM) - 基本流 - 流类型（音频 0x81） - 基本 PID(0x0012) - 描述符 - 用于 CA 供应商 #1 的 CA 描述符 (ECM)
在 PID ＝ 0x1010 上发送的 PMT PMT0x1010 -PMT 节目号 1010 -PMT 段版本 10 -PCRPID0x0011 - 基本流 - 流类型（视频 0x02 或 0x80） - 基本 PID(0x0011) - 描述符 - 用于 CA 供应商 #2 的 CA 描述符 (ECM) - 基本流 - 流类型（音频 0x81） - 基本 PID(0x0013) - 描述符 - 用于 CA 供应商 #2 的 CA 描述符 (ECM)

[0057] 考虑期望在用摩托罗拉或 Scientific Atlanta 和 NDS CA 的系统中发送节目的实例，上述通信与摩托罗拉和 Scientific Atlanta 在它们的 CA 系统中所发送的 PSI 相一致，只有很小的改变。改变节目关联表 (PAT) 以索引一个用于每个节目的附加节目映射表 (PMT)。此实施例中的每个节目在 PAT 中都有两个节目号。在上表中，节目号 1 和节目号 1001 除了索引不同的音频 PID 和 CA 描述符以外是同一节目。为创建多个 PMT 并将新 PAT 和 PMT 信息与数据流多路复用，可以使系统有所变化，从而可以适当地修改有线电视系统的前端设备。再有，本领域熟练技术人员应会认识到如何使这些消息适用于本文所述的其它部分加密方案。这种方法的优点在于，对前端设备或传统和非传统的机顶盒来说，不需要特别的硬件或软件来传送用该方案进行传统和非传统加密的音频。

[0058] 这项技术可以使尚未付费的收费节目听不见从而阻止用户使用该节目，但黑客可能会尝试调谐到视频。为了防止这一点，如果需要的话，可以同时使用在依照本发明的其它加密技术中使用的机制（如后所述）。由于闭路字幕一般是作为视频数据的一部分来传输的，故用户仍能获得可读的音频信息以及明文视频。因此，尽管对某些应用来说是适用的，但本技术本身不能对所有的情况都提供适当的保护。在另一个实施例中，还可以额外地扰乱包含作为有效负载一部分的闭路字幕信息的视频分组。

[0059] 在一个替换实施例中，可用分配给每一组加密视频的独立 PID 仅对视频作双重或多重加密。尽管这会为一般节目提供更安全的加密（因为视频可能比音频更重要），但与完全双重传输相比的带宽节省量仅约 10％，这是因为在所有的机顶盒中仅能共享音频。但是，这种方法可用于特定内容（例如成人和体育节目）并且有助于减少用于该内容的带宽开销，而音频加密方法则可用于其它类型的内容。在用于 DirecTV™ 业务的数字卫星业务 (DSS) 传输标准中，可用被认为是等效的服务频道标识 (SCID) 来标识音频分组以便进行加密。

[0060] 时间分片

[0061] 依照本发明的另一个实施例在本文中称为时间分片 (timeslicing)，并在图 3 中被说明为系统 200。在这一实施例中，每个节目的一部分均在时间相关的基础上以干扰观看节目的方式进行加密，除非是用户已经为节目付费。本发明的这一实施例可实现为 :部分加密的视频和明文音频、明文视频和部分加密的音频或者部分加密的视频和音频。被加密的时间片的持续时间为整个时间的一定百分比，可以对该持续时间进行选择，以便满足带宽使用和防黑客安全性之间的任何适当的期望平衡。一般地说，在本文所述的任何一个实施例中，对少于 100％的内容进行加密，以便生成期望的部分加密。下面的实例详细说明了部分加密的视频和音频。

[0062] 举例来说（但不是为了限制），考虑具有九个节目的系统，这九个节目均要依照本发明示例性实施例进行双重部分加密。这九个频道作为多路复用的分组流被馈送给有线电视前端设备并用分组标识符 (PID) 进行数字编码，以便标识出与九个节目中特定的一个相关联的分组。在这一实例中，假定这九个节目具有标号为 101-109 的视频 PID 以及标号为 201-209 的音频 PID。依照这一实施例的部分加密是在各节目中间进行时间多路复用，因此，在任一给定的时间都仅对来自单个节目的分组进行加密。这种方法无需知道内容是什么。

[0063] 参照下面的表 1，说明了与本发明一个实施例相一致的时间片双重加密方案的示例性实施例。就具有主视频 PID101 和主音频 PID201 的节目 1 而言，在第一时间段内，用加密系统 A 来加密具有 PID101 和 PID201 的分组进行加密，同时以明文方式发送表示其它节目的其它分组。在这一实施例中，次 PID 也被分配给视频和音频。对节目 1 而言，次 PID 分别是用于视频的 PID111 和用于音频的 PID211。在第一时间段内，用加密系统 B 来加密带有次 PID 的分组，并以明文的方式发送接下来的八个时间段。之后就时间段 10 而言，具有上述四个 PID 中任何一个的分组被再次加密，然后是以明文方式发送接下来的八个时间段。按相类似的方式，在第二时间段中，用加密系统 A 来加密具有主视频 PID102 和主音频 PID202 的节目 2，用加密系统 B 来加密带有相关次 PID 的分组，并在接下来的八个时间段中以明文方式发送，后面依此类推。通过检查头九行，可以在表 1 清楚地看出这种模式。在不脱离本

发明的情况下，可根据这种技术对音频和视频分组两者进行加密或者只对音频或视频进行加密。还有，音频和视频可具有它们自己的单独加密序列。在表 1 中，P1 表示时间段号 1，P2 表示时间段号 2，后面依此类推。EA 表示用 CA 系统 A 对信息加密，EB 表示用 CA 系统 B 对信息加密。

[0064]

节目	视频 PID	音频 PID	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	...
1	PID101	PID201	EA	明文	明文	明文	明文	明文	明文	明文	明文	EA	明文	明文	...
2	PID102	PID202	明文	EA	明文	明文	明文	明文	明文	明文	明文	明文	EA	明文	...
3	PID103	PID203	明文	明文	EA	明文	明文	明文	明文	明文	明文	明文	明文	EA	...
4	PID104	PID204	明文	明文	明文	EA	明文	明文	明文	明文	明文	明文	明文	明文	...
5	PID105	PID205	明文	明文	明文	明文	EA	明文	明文	明文	明文	明文	明文	明文	...
6	PID106	PID206	明文	明文	明文	明文	明文	EA	明文	明文	明文	明文	明文	明文	...
7	PID107	PID207	明文	明文	明文	明文	明文	明文	EA	明文	明文	明文	明文	明文	...
8	PID108	PID208	明文	明文	明文	明文	明文	明文	明文	EA	明文	明文	明文	明文	...
9	PID109	PID209	明文	明文	明文	明文	明文	明文	明文	明文	EA	明文	明文	明文	...
1	PID111	PID211	EB									EB			...
2	PID112	PID212		EB									EB		...
3	PID113	PID213			EB									EB	...
4	PID114	PID214				EB									...
5	PID115	PID215					EB								...
6	PID116	PID216						EB							...
7	PID117	PID217							EB						...
8	PID118	PID218								EB					...
9	PID119	PID219									EB				...

[0065] 表 1

[0066] 为了保持与已建立的传统加密系统（加密系统 A）的兼容性，用加密系统 A 来加密用于节目 1 至 9 的每一个的加密周期。传统 STB 设备会接受这种部分加密的 A/V 数据流，透明地传送未加密的分组并对加密的分组进行解密。但是，期望用加密系统 A 和加密系统 B 这两者来获得双重加密。为了做到这一点，对指定的节目分配主 PID（例如对节目 1 分配

视频 PID101 和音频 PID201) 和次 PID(例如对节目 1 分配视频 PID111 和音频 PID211),以便载送用于给定收费频道的基本数据流。

[0067] 参照图 3,系统 200 在总体上说明了有线电视系统前端设备 222 的功能,其中,将前端设备 222 处的 N 个频道的明文视频 208 提供给智能切换器 216(在一个编程处理器的控制下工作),该切换器可选择传递要以明文方式传输的将在 220 处被分配主 PID 的分组。要加密的分组被选择传递至有条件访问系统 A 的加密器 218 和有条件访问系统 B 的加密器 224。一经加密,这些来自 218 和 224 的被加密的分组就在 220 处被分别分配主或次 PID。来自 228 的系统信息及来自 229 的 PSI 被与明文分组、系统 A 加密的分组、系统 B 加密的分组多路复用或组合并在有线电视系统 32 上被广播。

[0068] 出于讨论的目的,如果时间片周期为 100 毫秒,则如表 1 所示,对所有九个节目来说,每秒平均起来有总计为 111 毫秒的一个多加密周期。如果时间片周期 50 毫秒,则有总计为 111 毫秒的两个多加密周期。试图调谐视频的非预订机顶盒若能维持任何种类的图像锁定,都将会获得非常低劣的图像,并且音频是错乱的。

[0069] 以与上述双重音频加密实例略有不同的方式处理用于部分扰乱的流的 PSI。相同的 SI 和 PAT PSI 信息本质上可被发送给传统和非传统的机顶盒。不同在于 PMT PSI 信息。传统机顶盒解析 PMT PSI 并同以前一样获得主视频和音频 PID。非传统的机顶盒同传统机顶盒一样获得主 PID,但必须查看 PMT PSI 中的 CA 描述符以检查流是否被部分地扰乱。对于特定的 CA 供应商,特别地扰乱次 PID,因此,用特定 CA 供应商专用的 CA 描述符来发送 PID 信号是有意义的。本发明通过允许有一个以上的次 PID 而允许两个以上的 CA 供应商共存。次 PID 对特定的 CA 供应商来说应该是唯一的。机顶盒知道用于它所具有的 CA 的 CA ID 并且能检查所有 CA 描述符以找到与之相关的那一个。

[0070] 尽管可以作为用于 ECM 的同一 CA 描述符中的私有数据来发送次 PID 数据,但优选实施例使用了独立的 CA 描述符。次 PID 被放在 CA PID 字段内。这就允许前端设备处理设备在不必解析 CA 描述符的私有数据字段的情况下能“看到”该 PID。为了能分辨 ECM 和次 PID CA 描述符之间的差别,可发送一个伪私有数据值。

[0071]

在 PID = 0x0010 上发送的 PMT
PMT0x0010
-PMT 节目号 1
-PMT 段版本 10
-PCRPID0x0011
- 基本流
- 流类型（视频 0x02 或 0x80）
- 基本 PID(0x0011)
- 描述符
- 用于 CA 供应商 #1 的 CA 描述符 (ECM)
- 用于 CA 供应商 #2 的 CA 描述符 (ECM)
- 用于 CA 供应商 #2 的 CA 描述符（次 PID）
- 基本流
- 流类型（音频 0x81）
- 基本 PID(0x0012)
- 描述符
- 用于 CA 供应商 #1 的 CA 描述符 (ECM)
- 用于 CA 供应商 #2 的 CA 描述符 (ECM)
- 用于 CA 供应商 #2 的 CA 描述符（次 PID）-

[0072] 用于 CA 供应商 #2 的 CA 描述符 (ECM)

[0073]

描述符
- 标记 :有条件访问 (0x09)
- 长度 :4 字节
- 数据
-CA 系统 ID :0x0942（第二 CA 供应商）
-CAPID(0x0015)

[0074] 用于 CA 供应商 #2 的 CA 描述符（次 PID）

[0075]

描述符
- 标记 :有条件访问 (0x09)
- 长度 :5 字节
- 数据
-CA 系统 ID :0x1234（第二 CA 供应商）
-CAPID(0x0016)
- 私有数据

[0076] 在 CA 系统 A 下工作的传统 STB36 接收数据、忽略次 PID、对在 CA 系统 A 下加密的分组进行解密并将节目提供给电视机 44。新的或非传统的 STB236 接收 SI228。它接收

PSI229 并使用 PMT 来识别在第二 CA 描述符中调出的与被观看的节目相关的主、次 PID。在 CA 系统 A 下加密的分组被丢弃，在 CA 系统 B 下加密的具有次 PID 的分组由 CA 系统 B240 来解密并被插进明文数据流，以便解码并显示在电视机 224 上。

[0077] 图 4 说明了一种用于在有线电视系统前端设备处进行编码的处理过程，它可用于实现本发明的一个实施例，其中，CA 系统 A 是传统的系统，CA 系统 B 是要引入的新型系统。在 250 处接收到用于给定节目的明文分组时，如果对分组（或帧）不进行加密（即就该节目而言不是用于加密的当前时间片），则传送明文分组 (C) 以便在 254 处插进输出流。如果由于当前分组是加密时间片的一部分而对当前分组进行加密，则将分组传给分组加密处理 A258 和分组加密处理 B262 以用于加密。来自 258 处的加密处理 A 的加密分组 (EA) 被传至 254 以便插进输出流。来自 262 处的加密处理 B 的加密分组 (EB) 在 264 处被分配次 PID，以便在 254 处插进输出流。对节目中的所有分组都重复上述过程。

[0078] 图 5 说明了在 STB236 中使用的处理过程，STB236 具有新引入的 CA 系统 B，以便对接收到的数据流进行解密和解码，而所接收到的数据流包含有带所述的主、次 PID 的 C、EA 和 EB 分组。当在 272 接收到分组时，就检查它是否具有所关心的主 PID。如果没有，就在 274 处检查该分组是否具有所关心的次 PID。如果分组既没有主 PID，也没有次 PID，则在 278 处忽略或丢弃该分组。丢弃不是主或次 PID 的在 EA 与 EB 分组之间的任何插入的分组。是否能在接收到替代匹配的 EA 或 EB 分组之前解码器接收到连续的多个 EA 或 EB，是一个实现形式问题并主要是一个缓存问题。此外，很容易对在主分组之前而不是在主分组之后来到的次分组进行检测。还可以设计这样一种电路，其中可出现两种情况，即 :次分组在主分组之前或者在主分组之后。如果分组具有所关心的主 PID，则在 284 处检查该分组以确定它是否被加密。如果没有，则在 288 处将分组 (C) 直接传给解码器以便解码。如果分组在 284 处被确定为加密，则认为它是 EA 分组并在 278 处丢弃或忽略。在某些实现形式中，在 284 处不检查主分组的加密。相反，仅在 284 处检查其相对次分组的位置，从而将其标识出来以便替换。

[0079] 如果分组在 274 处被确定为具有次 PID，则在 292 处将该 PID 重映射至主 PID（或等价地将主 PID 重映射至次 PID 值）。然后在 296 处对分组进行解密，并在 288 处将其发送至解码器以便解码。当然，本领域熟练技术人员应认识到，在不脱离本发明的情况下可以有多种变化形式，例如，292 和 296 的次序或者 272 和 274 的次序可以颠倒。如前所述，284 可用检查主分组相对次分组的位置来代替。本领域熟练技术人员可以想到其它变化形式。

[0080] 在加密系统 A 下工作的传统 STB36 完全忽略了次 PID 分组。如果必要的话，对带有主 PID 的分组进行解密，并在它们是明文的情况下将其不解密地传给解码器。因此，在加密系统 A 下工作的所谓“传统”STB 会对与主 PID 相关的部分加密的数据流进行适当的解密和解码并在没有修改的情况下忽略次 PID。对在加密系统 B 下工作的 STB 进行编程，以便忽略与主 PID 相关的所有加密分组并使用所传输的具有与特定频道相关的次 PID 的加密分组。

[0081] 因此，每个双重部分加密的节目都具有两组与之相关的 PID。就所示的有适当时间片间隔的系统而言，如果如所述那样逐周期地进行加密，则图像在两种解密都不具备的 STB 上基本上不可观看。

[0082] 为了实现图 6 的前端设备 322 中的这种系统，可以修改 SI 和 PSI 以包括第二组 CA

描述符信息。传统机顶盒可能无法容许未知的 CA 描述符。因此，在机顶盒中，替换地可以对内容 PID 和 / 或 SI/PSI 以及 ECM PID 相对传统 CA PID 作“硬编码”偏移。或者可发送并行的 PSI。例如，对非传统的机顶盒来说，可在 PID1000 而不是 PID0 上发送辅助 PAT。它可以索引在传统 PAT 中未找到的辅助 PMT。辅助 PMT 可包含非传统的 CA 描述符。由于辅助 PMT 对传统机顶盒来说是未知的，故不存在互操作问题。

[0083] 在系统 A 与摩托罗拉或 Scientific Atlanta 所制造的传统机顶盒相对应的系统中，不需要修改 STB。对兼容系统 B 的 STB 来说，就本文所述的部分加密的节目的双重传输而言，视频和音频解码器适于监听两个 PID（主 PID 和次 PID）而不是仅监听一个 PID。按照所使用的非传统 CA 系统的数量的不同，可以有一个或多个影子 PID，但是，适合于特定 STB 所使用的 CA 方法，该特定机顶盒仅监听次 PID 之一。此外，理想地忽略来自载送主要为明文的视频或音频的 PID 的加密分组。由于忽略“坏分组”（不能很容易地照原样进行解码的分组）可能已经是许多解码器所执行的功能，故不需进行修改。对带有不忽略坏分组的解码器的系统而言，可以使用过滤功能。应该认识到，时间片加密技术可仅应用于视频或音频。还有，视频可以是按时间片加密的，而音频则如在先前实施例中一样是双重加密的。时间片技术可同时应用于多个节目。在一段时间内加密的节目的数量主要是带宽分配问题，尽管上述实例讨论的是每次扰乱单个的节目，但本发明并不局限于此。对本领域熟练技术人员来说，还可以想到本文件所述的加密技术的其它组合。

[0084] 第 M 和 N 分组的加密

[0085] 依照本发明的另一个实施例在本文中称为第 M 和 N 分组的加密。这是图 3 中被说明为系统 200 的实施例的一种变化形式。在这一实施例中，表示节目的每个 PID 的分组按能干扰观看节目的方式进行加密，除非用户已为节目付费。在这一实施例中，M 表示加密事件开始之间的分组的数量，N 表示一旦加密开始后被连续加密的分组的数量。N 小于 M。如果 M ＝ 9 且 N ＝ 1，则每九个分组都有一个持续一个分组的加密事件。如果 M ＝ 16 且 N ＝ 2，则每十六个分组都有一个持续两个分组的加密事件。和在先前实施例中一样，用 CA 系统 A218 和 CA 系统 B224 复制和处理要双重部分加密的各个分组。这一实施例与先前时间分片技术之间操作上的不同在于切换器 216 选择分组以便在编程处理器的控制下进行加密的操作。

[0086] 举例来说（但不是为了限制），考虑具有九个节目频道的系统，这些频道要根据本示例性实施例进行双重加密。这九个频道用分组标识符 (PID) 进行数字编码，以便标识出与九个节目中特定的一个相关的分组。在本实例中，假定这九个节目具有标号为 101-109 的视频 PID 和标号为 201-209 的音频。依照本实施例，随机逐节目地进行加密，因此，可同时对来自其它节目的分组进行加密。以下的表 2 对此进行了说明，其中，M ＝ 6，N ＝ 2 并且只加密了视频，但这不应认为是限制性的。这种方法不需要知道内容是什么。在表 2 中，PK1 表示分组号 1，PK2 表示分组号 2，后面依此类推。

[0087]

节目	视频	PK1	PK2	PK3	PK4	PK5	PK6	PK7	PK8	PK9	PK10	PK11	PK12	...
1	PID101	EA	EA	明文	明文	明文	明文	EA	EA	明文	明文	明文	明文	...

节目	视频	PK1	PK2	PK3	PK4	PK5	PK6	PK7	PK8	PK9	PK10	PK11	PK12	...
2	PID102	明文	明文	明文	EA	EA	明文	明文	明文	明文	EA	EA	明文	...
3	PID103	明文	明文	EA	EA	明文	明文	明文	明文	EA	EA	明文	明文	...
4	PID104	明文	明文	明文	EA	EA	明文	明文	明文	明文	EA	EA	明文	...
5	PID105	明文	明文	EA	EA	明文	明文	明文	明文	EA	EA	明文	明文	...
6	PID106	EA	明文	明文	明文	明文	EA	EA	明文	明文	明文	明文	EA	...
7	PID107	EA	EA	明文	明文	明文	明文	EA	EA	明文	明文	明文	明文	...
8	PID108	明文	EA	EA	明文	明文	明文	明文	EA	EA	明文	明文	明文	...
9	PID109	EA	明文	明文	明文	明文	EA	EA	明文	明文	明文	明文	EA	...
1	PID111	EB	EB					EB	EB					...
2	PID112				EB	EB					EB	EB		...
3	PID113			EB	EB					EB	EB			...
4	PID114				EB	EB					EB	EB		...
5	PID115			EB	EB					EB	EB			...
6	PID116	EB					EB	EB					EB	...
7	PID117	EB	EB					EB	EB					...
8	PID118		EB	EB					EB	EB				...
9	PID19	EB					EB	EB					EB	...

[0088] 表 2

[0089] 在表 2 的实例中，用 M = 6 且 N = 2 的加密方案完全彼此独立地对各节目加密。再有，所述实例仅对视频加密，但也可以按上述或另外的安排对音频进行加密。如果仅应用于视频，则可如先前实施例那样对音频进行双重扰乱或进行时间片加密。或者，如果仅应用于音频，则可如先前实施例那样对视频进行时间分片。

[0090] 本领域熟练技术人员应该认识到，可以依照本文所公开的部分扰乱构想设计出上述技术的多种变化形式。例如，五个明文、两个是加密的、随后是两个明文、再后面是一个加密的这样一种模式 (CCCCCEECCE CCCCCEECCE...) 符合此部分加密思想的变化形式，而 M 和 N 的随机值、伪随机值和半随机值可用于选择分组以便进行加密。对分组的随机、伪随机或

半随机（本文统称为“随机”）选择会使得黑客在试图恢复所记录的被扰乱的内容的后处理过程中难以在算法上重新构造分组。本领域熟练技术人员应该认识到如何使上述信息适用于本文后述的部分加密的其它实施例。某些实施例可结合起来使用以便更有效地对内容进行保密。

[0091] 数据结构加密

[0092] 本发明实施例的另一种部分加密方法以数据结构为基础进行加密。举例但不是为了进行限制，一种用于加密的通常数据结构是 MPEG 视频帧。以下的表 3 说明了这一点（同样仅用于视频），其中，每隔九个视频帧就进行加密。在这一实施例中，每个节目的十帧加密周期对于各频道是彼此不同的，但这不应认为是限制性的。这种思想可以看作是时间片的变化形式或以视频或音频帧（或其它数据结构）为基础的第 M 和 N 部分加密安排（或其它模式），所述示例性实施例中 M ＝ 10、N ＝ 1。当然，M 和 N 的其它值可以用于类似的实施例。在表 3 中，F1 表示帧号 1，F2 表示帧号 2，后面依此类推。

[0093]

节目	视频	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	...
1	PID101	EA	明文	明文	明文	明文	明文	明文	明文	明文	明文	EA	明文	...
2	PID102	明文	明文	明文	EA	明文	明文	明文	明文	明文	明文	明文	明文	...
3	PID103	明文	明文	EA	明文	明文	明文	明文	明文	明文	明文	明文	明文	...
4	PID104	明文	明文	明文	明文	EA	明文	明文	明文	明文	明文	明文	明文	...
5	PID105	明文	明文	明文	EA	明文	明文	明文	明文	明文	明文	明文	明文	...
6	PID106	EA	明文	明文	明文	明文	明文	明文	明文	明文	明文	EA	明文	...
7	PID107	明文	EA	明文	明文	明文	明文	明文	明文	明文	明文	明文	EA	...
8	PID108	明文	EA	明文	明文	明文	明文	明文	明文	明文	明文	明文	EA	...
9	PID109	EA	明文	明文	明文	明文	明文	明文	明文	明文	明文	EA	明文	...
1	PID111	EB										EB		...
2	PID112				EB									...
3	PID113			EB										...
4	PID114					EB								...
5	PID115				EB									...

节目	视频	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	...
6	PID116	EB										EB		...
7	PID117		EB										EB	...
8	PID118		EB										EB	...
9	PID119	EB										EB		...

[0094] 表 3

[0095] 因此，同样地每个被加密的节目均有两组与其相关的PID。如果如前所述那样逐周期地进行加密，则对所示的系统来说，图像基本上是不能观看的。对所示的每秒 30 帧的九节目系统而言，每秒约加密三个帧。对未被授权观看节目的观众来说，他们的 STB 至多能偶尔捕获到静止帧，因为 STB 要不断地尝试进行同步和恢复。业已订购了节目的观众能很容易地观看到节目。用于这种加密安排的带宽成本取决于进行加密的频率。在上述实例中，对每个节目来说都传输额外 1/9 的数据。在这一实例中，使用了约一个节目的带宽。在有更多数量的节目的情况下，对每个节目加密较少的分组，而加密系统的安全性会略微降低。如在随机化的 M 和 N 方法中一样，可以选择随机帧。就视频而言，选择随机帧会有助于确保影响到所有类型的帧 - 内编码帧 (I 帧)、预测帧 (P 帧)、双向编码 (B 帧) 和 DC 帧。

[0096] 在本发明的一种变化形式中，可以对较少的分组进行加密，以便获得可接受的安全级别。也就是说，也许在九节目系统中，只需要加密每秒一个帧，就可以获得可接受的安全级别。在这种系统中，总开销为每个节目每秒一个加密周期或者约为在总开销中传输的数据的 1/30。这种总开销级别比与在两个加密系统下的全双重传输加密相关的 50％的带宽损失，有显著的改进。在本发明的另一个变化形式中，可以仅对特定视频帧进行加密，以便获得可接受的安全级别。例如，对 MPEG 内容来说，可以只扰乱内编码帧 (I 帧)，以便进一步减少带宽总开销并仍保持可接受的安全级别。这与全双重传输所需的带宽相比提供了显著的改进。

[0097] 关键分组加密

[0098] 利用有选择的逐分组双重加密技术，可以在带宽使用方面有很高的效率。在这一实施例中，根据分组对节目内容的音频和 / 或视频的正确解码的重要性来选择分组以便进行加密。

[0099] 与加密内容的全双重传输相比，这一实施例通过仅扰乱一小部分分组而可以减少带宽需求。明文分组在两个 (或多个) 双重传输 PID 之间共享。在一个优选实施例中，正如要公开的那样，使用了总内容带宽的少于约百分之一。在采用传统加密方案的系统中，明文节目内容分组可以由传统的和新式机顶盒接收。如上所述，加密的分组由带有适当 CA 的相应机顶盒来进行双重传输和处理。每个 CA 系统均为互不相关。不需要密钥共享，并且备 CA 系统可以使用不同的密钥出现时间。例如，具有摩托罗拉专用加密法的系统可用嵌入式安全 ASIC 生成快速变化的加密密钥，而基于 NDS 智能卡的系统则可生成变化稍慢的密钥。对 Scientific Atlanta 和摩托罗拉传统加密来说，本实施例可同样很好地工作。

[0100] 参照图 6，依照本发明一个实施例的系统的框图被说明为系统 300，其中逐分组地对部分节目进行双重加密。在这一系统中，用例如传统 CA 系统 A 和新 CA 系统 B 对备节目的分组进行双重加密。根据分组对视频和 / 或音频流的正确解码的重要来选择被加密的分组。

[0101] 在图 6 所示的系统中，有线电视系统前端设备 322 在分组选择器 316 处选择 A/V 内容 304 的分组以便加密。对为了加密而选择的分组进行选定，以使得未接收（通过一个未付费的解码器）这些分组就会严重地影响对节目的实时解码并且会影响对所记录内容的后处理。也就是说，只对关键分组加密。对视频和音频而言，这一点可通过下述方法实现：对包含作为有效载荷的一部分的 PES（分组化基本流）报头和其它报头的“帧起始”传输流分组进行加密，因为没有这些信息 STB 解码器不能对经 MPEG 压缩的数据进行解压缩。MPEG2 流用传输头标中的“分组单元起始指示符”来标识“帧起始”分组。一般地说，载送包含有一组图像头标或视频序列头标的有效载荷的分组可被用于实现本发明的扰乱技术。

[0102] MPEG（运动图象专家组）兼容的压缩视频可将基本数据流重新分组进具有 188 字节数据的稍微任意的有效负载形式的传输流中。因此，可以在选择器 136 处选择包含 PES 头标的传输流分组以进行加密，并通过 CA 系统 A 加密器 318 和 CA 系统 B 加密器 324 对这些分组双重加密。可复制要被双重部分加密的分组，并且如在先前实施例中一样，可在 330 处将由加密器 324 加密的复制分组的 PID 重映射至次 PID。以明文方式传送其余的分组。明文分组、系统 A 加密的分组、系统 B 加密的分组以及系统信息 328 以及来自 329 的 PSI 被多路复用到一起，以便在有线电视系统 32 上广播。

[0103] 同先前系统一样，传统 STB36 接收明文数据以及在 CA 加密系统 A 下加密的数据并以透明的方式将与用 CA 解密 A40 加以解密的数据相结合的未加密的数据传给解码器。在新型 STB336 中，将节目分配给主和次 PID。接收带有主 PID 的明文分组并将其传给解码器。丢弃带有主 PID 的加密分组。对带有次 PID 的加密分组进行解密，然后将其与数据流（例如通过将分组重映射至主 PID）重新组合起来以便进行解码。

[0104] 以使用视频为例，每个样本均称为帧，抽样率一般为每秒 30 帧。如果将样本编码成适合于 3.8Mbps，则每一帧会占用 127K 比特的带宽。对 MPEG 传输而言，将此数据分成 188 字节的分组，每个帧的第一个或头几个分组都包含用于指示对帧数据主体进行处理的头标。仅对第一头标分组（1504 个额外比特）进行双重加密需要仅为 1.2%（1504/127K）的额外带宽。对高清晰（19Mbps）流来说，该百分比甚至更少。

[0105] 如前所述，依照本实施例，包含 PES 头标的传输流分组是优选的加密目标。这些分组包含序列头标、序列扩展头标、图像头标、量化和其它解码表（它们也都在同一个分组内）。如果这些分组不能够被解码（也即黑客在没有支付订购费用的情况下试图观看未授权的节目），则无法观看那怕是一小部分节目。总之，任何要调谐到该节目的企图都有可能遇到黑屏，并且也没有音频，因为已知的解码器集成电路使用 PES 头标来实时地同步诸如视频和音频之类的基本流。通过对 PES 头标进行加密，未授权的机顶盒中的解码引擎甚至不能启动。包含 PES 头标的分组中动态变化的关键信息能阻止例如对所存储内容进行后处理攻击。本领域熟练技术人员将会注意到，对本发明的这一实施例的实现形式来说，还可以标识出能在不脱离本发明的情况下严格地阻止未授权的观看的其它关键或重要的分组或内容单元以便进行加密。例如，可以对 MPEG 内编码或 I 帧图像分组进行加密以阻止对节目

的视频部分进行观看。本发明的实施例可与任何其它实施例结合起来使用，例如，可以与扰乱包含 PES 头标的分组以及其它分组的随机、第 M 和 N 或数据结构加密结合起来使用。关键分组加密可应用于视频加密，同时将不同的方法用于音频。例如，可对音频作双重加密。对本领域熟练技术人员来说，可以想到本发明范围内的其它变化形式。

[0106] 图 7 是说明诸如可在图 6 的前端设备处使用的示例性编码处理过程的流程图。当在 350 处接收到传输流分组时，对该分组进行检查，以便判断它是否满用于加密的选择标准。在这一优选实施例中，该选择标准是存在作为分组有效载荷一部分的 PES 头标。如果不满足标准，则将该分组作为明文未加密的分组 (C) 传送，以便在 354 处插进输出数据流。如果分组满足上述标准，则在 358 处用 CA 加密系统 A 对其加密，以生成一个加密的分组 EA。在 362 处还对该分组进行复制并用 CA 加密系统 B 进行加密，以生成一个加密的分组。将这一被加密的分组在 366 处映射至次 PID，以生成一个加密的分组 EB。在 354 处将加密的分组 EA 和 EB 连同明文分组 C 插进输出数据流。优选的是，EA 和 EB 分组被插在数据流中原先获得用于加密的单个原始分组的位置处，以使数据的排序基本上保持相同。

[0107] 当在诸如图 6 的 336 之类的与 CA 加密系统 B 相兼容的 STB 处接收到来自 354 的输出数据流时，可以利用诸如图 8 的处理过程（与图 5 的处理过程相类似）之类的处理过程对节目进行解密和解码。当在 370 处接收到具有主或次 PID 的分组时，在 370 处判断分组是明文 (C) 还是用系统 A(EA) 来加密的，或者在 374 处判断分组是否是用系统 B(EB) 来加密的。如果分组是明文的，则将其直接传给解码器 378。在某些实施例中，可用主分组在次分组之前或之后的相对位置来发信号通知在流中替换该主分组。并不特别需要检查主分组的扰乱状态。如果分组是 EA 分组，则在 380 处将其丢弃。如果分组是 EB 分组，则在 384 处对其解密。这时，在 388 处将次 PID 分组和 / 或主 PID 分组重映射至相同的 PID。在 378 处对解密的分组和明文分组进行解码。

[0108] 相对全双重传输的需求，上述双重部分加密安排可以极大地减少带宽要求。对 PES 头标信息进行加密可以有效地保护视频和音频内容，同时允许两个或更多的 CA 系统独立地“共存”于同一有线电视系统中。传统系统 A 的机顶盒不受影响，并且系统 B 的机顶盒仅需要较少的硬件、固件或软件增强来监听分别用于视频和音频的两个 PID。每种类型的 STB（传统和非传统的）都能保持其固有的 CA 方法。前端设备的修改限于选择内容以便加密、引入第二加密器以及提供将它们的组合混合进复合输出流的装置。

[0109] 在一个实施例中，将前端设备设备配置成能随机地扰乱带宽所允许的那么多的内容，而不仅仅是扰乱关键的 PES 头标。这些额外的被扰乱的分组可以位于 PES 有效载荷之中，也可以位于在整个视频 / 音频帧内的其它分组之中，从而使得内容更加安全。

[0110] SI 加密

[0111] 现参照图 9，对任何额外带宽有最小需求的系统的一个实施例被说明为系统 400。在这一实施例中，系统利用了下列事实：对机顶盒来说，需要系统信息 (SI)428 来调谐节目。在有线电视系统中，在波段外（即在正常观看频道外的频率）发送 SI。也可以在波段内发送。如果在波段内发送，则复制 SI428 并在每个流内发送 SI428。出于讨论的目的，假定发送给来自先前的制造商的“传统”机顶盒的 SI 独立于发送给来自新的制造商的诸如 STB436 之类的机顶盒的 SI。因此，SI 的每个版本都可如前所述那样用有条件访问系统 A418 和有条件访问系统 B424 来独立地加以扰乱。明文视频 404 和明文音频 406 以明文的方式

传送，但为理解如何找到它们，需要有 SI 信息 428。

[0112] SI 传送与频道名有关的信息和诸如节目名及开始时间之类的节目指南信息以及每个频道的频率调谐信息。数字频道被多路复用在一起并按特定的频率传送。在本发明的实施例中，对 SI 信息加密，并使该信息仅可由授权的机顶盒使用。如果未接收到用于了解设备中所有 A/V 频率的位置 SI 信息，则不能进行调谐。

[0113] 为了阻止一个对机顶盒进行编程以跟踪或扫描频率的黑客，频道的频率可偏离标准频率。还有，所述频率可按日、周或其它周期或者随机地动态改变。一个典型的有线前端设备可具有约 30 个使用中的频率。各个频率一般都被选定成能特别避免彼此之间的以及与地面广播信号和接收设备的时钟所使用的频率之间的干扰。每个频道均具有至少一个独立的替代频道，该频道如果被使用的话将不会导致干扰或导致相邻频道的频率发生变化。所以，实际可能的频率映射为 2^{30} 或 $1.07x10^{9}$。但是，黑客可以在尝试调谐约 30 个频道的每一个频道时很快地对所述两个频率都进行尝试。如果成功地确定了有内容的频率，则黑客的机顶盒可以解析 PSI429，以知道构成节目的各个 PID。黑客会难以知道“节目 1”是“CNN”、“节目 5”是“TNN”等等。该信息与 SI 一道发送，如前所述，SI 被扰乱并且不能为未授权的机顶盒所使用。但是，固执的黑客可能会通过选择各个频道并检查所传送的内容而推想出这些。所以，为了阻止识别出频道，单个流中的节目的布局可以经常更换，例如在上例中交换节目 2 和节目 5，因此，“节目 1”是“TNN”，“节目 5”是“CNN”。还有，可以用全新的节目组将节目移至完全不同的流。一个典型的数字有线数据转换器可以传送包括音乐在内的 250 个节目内容。每个节目都可以唯一地进行调谐。重排序的可能组合是 250！（阶乘）。在没有由所传送的 SI 提供或由黑客提供的内容映射的情况下，用户面对的是随机选择流中的各个节目以检查它是否是所感兴趣的那一个。

[0114] 因此，在数据转换器 422 中，视频信号 404 和音频信号 406 以明文（未加密）的方式提供，而 SI428 则被提供给多个 CA 系统，以便在有线电视网络上传送。因此，在示例性系统 400 中，明文 SI428 被提供给加密系统 418，该系统用加密系统 A 对 SI 数据加密。同时，明文 SI428 被提供给加密系统 424，该系统用加密系统 B 对 SI 数据加密。然后，将明文视频 404，音频 406 以及 PSI 429 与来自 418 的加密 SI(SIA) 和来自 424 的加密 SI(SIB) 多路复用到一起，以替代波段外系统信息 428。

[0115] 在通过有线电视系统 32 发布之后，视频、音频、PSI、系统信息 A 以及系统信息 B 均被传送给机顶盒 36 和 436。在 STB36 处，加密的 SI 在 CA 系统 A40 处解密，以便将调谐信息提供给机顶盒。机顶盒调谐出特定的节目，以使其能显示在电视机 44 上。与此相似，在 STB436 处，加密的 SI 在 CA 系统 B440 处被解密以将调谐信息提供给机顶盒，以便调谐出特定的节目并显示在电视机 444 上。

[0116] 这种方法的优点是，在内容传送系统（例如有线电视系统）中，不需要额外的 A/V 带宽。只需双重传输 SI。不需要专门的硬件。大多数调谐器都能很容易地适应任何偏离标准频率的频率。可用软件进行 SI 解密，或用硬件辅助 SI 解密。例如，传统的摩托罗拉机顶盒能用内置在解码器 IC 芯片中的硬件解密器对以摩托罗拉波段外方式传送的 SI 进行去扰乱。

[0117] 顽固的黑客可能会在同轴电缆上用频谱分析仪去了解 A/V 频道位于什么地方。还有，黑客可能对机顶盒编程以自动扫描频段，从而了解 A/V 频道的位置（这是一个相对较为

缓慢的过程）。如果 A/V 频道的频率动态地变化，则能阻止黑客，因为需要黑客不断地分析或扫描波段。再有，节目号和所分配的 PID 也可变化。但是，动态改变的频率、节目号和 PID 可能会给服务供应商（例如有线电视经营者）带来操作上的困难。

[0118] 一般性介绍

[0119] 图 10 的系统 500 能在总体上代表各种上述技术。系统 500 具有有线电视系统的前端设备 522，该前端设备具有明文视频 504、明文音频 506、SI528 以及 PSI529，它们中的任何一个都可以被选择性地切换通过由智能处理器控制的切换器 518，切换器 518 还用于将 PID（在需要 PID 分配或再分配的实施例中）分配给有条件访问系统 A520 或有条件访问系统 B524 或以明文的方式传给有线电视系统 32。如前所述，STB36 可对按传统 CA 系统 A 进行加密的节目或 SI 进行正确的解码。如前所述，CA 系统 B 加密的信息由 STB536 来理解并相应地被解密和解码。

[0120] PID 映射考虑因素

[0121] 需要时，上述 PID 映射的思想可以在总体上应用于本文所述的双重部分加密技术。在有线前端设备中，这种一般性的思想是，对由分组构成的数据流进行处理以复制为加密而选择的分组。对这些分组进行复制并用两种不同的加密方法加密。复制的分组被分配予独立的 PID（其中之一与用于明文内容的传统 CA PID 相匹配）并被重新插进数据流中原始选择的分组的位置处以便在有线电视系统中传输。在有线电视系统前端设备的输出端，所出现的分组流具有传统加密的分组和带有同样 PID 的明文分组。次 PID 标识出用新加密系统加密的分组。除在前端设备处进行的 PID 重映射以外，MPEG 分组还使用一种连续计数以保持分组的适当顺序。为了确保正确的解码，应在前端设备处创建分组化的数据流期间正确地维护这种连续计数。这一点是通过确保以通常的方式向带有各 PID 的分组顺序分配连续计数值而实现的。因此，带有次 PID 的分组会载送独立于主 PID 的连续计数。以下以简化的形式进行说明，其中，PID025 是主 PID，PID125 是次 PID，E 表示加密的分组，C 表示明文分组，末端数字表示连续计数。

[0122]

025C04	025E05	125E11	025C06	025C07	025C08	025C09	025E10	125E12

[0123] 在上述分组的示例性片段中，带有 PID025 的分组被看成具有它们自己的连续计数顺序 (04、05、06、07、08、09，.....)。同样，带有次 PID125 的分组也具有它们自己的连续计数顺序 (11、12、.....)。

[0124] 在 STB 处，可以用多种方式对 PID 进行处理，以使带有次 PID 的加密的分组与正确的节目正确地相关联。在一种实现形式中，输入流片段的分组头标如下：

[0125]

025C04	025E05	125E11	025C06	025C07	025C08	025C09	025E10	125E12

[0126] 对上述头标进行处理以创建下面的输出流片段：

[0127]

125C04	025E11	125E05	125C06	125C07	125C08	125C09	025E12	125E10

[0128] 输入流中的主 PID(025) 由用于明文分组 (C) 的次 PID 来代替。对加密的分组来

说，保留主 PID 和次 PID，但交换连续计数。因此，在没有由连续性损失造成的错误的情况下，可用次 PID 对分组流进行正确的解密和解码。也可以在依照本发明的实施例中使用例如将被扰乱的传统分组上的 PID(125) 映射到 NOP PID（所有的）或其它未解码的 PID 值的其它处理 PID 的方法和连续计数。

[0129] 主、次 PID 在作为节目专用信息 (PSI) 数据流的一部分进行传输的节目映射表 (PMT) 中被传送至 STB。在 CA 加密系统 A（“传统”系统）下运行的 STB 可以忽略次 PID 的存在，但在 CA 加密系统 B 下运行的新 STB 则被编程成能够识别出次 PID 被用于传送与主 PID 相关的节目的加密部分。警示机顶盒这样的事实：因在用于 PMT 的“循环”的基本 PID 中存在 CA 描述符而使用这种加密方案。一般有用于视频基本 PID“循环”的 CA 描述符以及音频基本 PID “循环”中的另一种 CA 描述符。CA 描述符用私有数据字节将 CA_PID 标识为 ECM PID 或用作用于部分扰乱的次 PID，从而使在系统 B 下运行的 STB 去查找与单个节目相关的主、次 PID。由于传输头标中的 PID 字段长度为十三位，故有 213 或 8192 个 PID 可用，任何多余的 PID 都可按需用于次 PID。

[0130] 除了为每个节目组成部分或其选定的部分分配 PID 以外，还可以分配新 PID 以便标记在第二加密技术中使用的 ECM 数据。每个分配的 PID 号均可被标注为用户定义的流类型以防传统 STB 的干扰操作。MPEG 定义了这种用于用户定义的数据流类型的号码的保留块。

[0131] 尽管在概念上在有线电视前端设备处的 PID 映射是一种简单的操作，但实际上有线电视前端设备通常是已建立的，所以要按在最少干扰已建立的有线电视系统同时符合成本效益的方式来对其进行修改以便实现这种任务。因此，有线电视系统前端设备中的实际实现形式的细节在某种程度上取决于前端设备中存在的实际传统硬件，以下将详细说明其实例。

[0132] 前端设备的实现形式

[0133] 本领域熟练技术人员应该理解，涉及图 2、3、6、9 和 10 的上述说明在本质上多少有些是概念性的并被用于说明与本发明各种实施例有关的整体思想和概念。在实现本发明的现实实现时，本领域熟练技术人员应该认识到，所面临的重要现实问题是在已有有线电视供应商的现有传统前端设备设备中提供各种部分加密方法的符合成本效益的实现形式。以两种主要的传统有线电视系统为例，以下说明了如何在有线电视前端设备中实现上述技术。

[0134] 首先，考虑使用摩托罗拉牌有条件访问系统的有线电视系统前端设备。在这种系统中，可进行图 11 所示的修改以便为部分双重加密实现形式提供符合成本效益的机制。在典型的摩托罗拉系统中，从卫星提供 HITS（空中前端设备）或类似的数据馈送。这种馈送可以提供集合的数字化内容，这些内容被提供给有线电视供应商并被诸如摩托罗拉集成接收机转发器 (IRT) IRT1000 型和 IRT2000 型以及摩托罗拉模块化处理系统 (MPS) 之类的接收机 / 去扰乱器 / 扰乱器系统 604 所接收。数字化电视数据的明文流可从接收机 / 去扰乱器 / 扰乱器系统 604 的卫星去扰乱器功能块 606 中获得。此明文流可由被示为分组选择器 / 复制器 610 的新功能块所处理。新功能块 610 可实现为编程的处理器或者用硬件、软件或它们的组合来实现。

[0135] 分组选择器 / 复制器 610 选择要用上述任何部分双重加密方法进行双重加密的分

组。然后用新 PID 来复制这些分组，以便可在以后对它们进行标识以进行加密。例如，如果 610 的输入端处的与特定节目相关联的分组具有 PID A，则分组选择器 / 复制器 610 会标识要加密的分组并复制这些分组且分别将它们重映射到 PID B 和 C，以便以后可在两种不同的系统中识别它们以便进行加密。优选的是，复制的分组在现在带有 PID B 和 C 的原始复制的分组的位置处被彼此相邻地插入数据流内，因此它们会保持原始呈现的相同次序（除了在数据流中原先驻有一个分组的地方现在有两个分组）。暂且假定要添加的新 CA 系统是 NDS 加密。在这种情况下，PID A 表示明文分组，PID B 表示 NDS 加密的分组，PID C 表示摩托罗拉加密的分组。带有 PID B 的分组这时可以在 610 中用 NDS 加密来加密或者在以后加密。

[0136] 带有 PID B 和 C 的分组然后被返回至系统 604，在该系统中，根据与摩托罗拉设备有关的控制系统 614 的指示，在有线电视扰乱器 612 处用摩托罗拉加密法对带有 PID C 的分组进行加密。然后，来自有线电视扰乱器 612 的输出流前进至另一个新设备 --PID 重映射器和扰乱器 620，它接收来自 612 的输出流并重映射其余带 PID A 至 PID C 的分组，且在控制系统 624 的控制下用 NDS 加密算法对 PID B 分组进行加密。626 处的输出流具有带有 PID C 的明文未加密的分组和带有 PIDC 的经过选择的分组（这些被选择分组业已被复制并用摩托罗拉加密系统进行了加密）以及带有 PID B 的用 NDS 加密系统进行了加密的分组。然后在 628 处调制这个流（例如进行正交幅度调制和 RF 调制），以便在有线电视系统上发布。上述优选实施例将未加密的分组映射到 PID A 上，以便匹配 PID C 上的被扰乱的分组，因为这样一来在传统节目专用信息 (PSI) 中取出的音频和视频 PID 是正确的。控制计算机、扰乱器以及传统机顶盒只知道 PID C。或者，PID C 上的被扰乱的分组可被映射回 PID A，但这可能意味着对自动生成的 PSI 进行编辑，以便在 PID 重映射器和扰乱器 620 中将 PID 号从 PID C 映射回 PID A。

[0137] 在上述实例中，PID 重映射器和扰乱器 620 还可用于多路分解 PSI 信息、对其进行修改以便反映出增加了 NDS 加密（通过使用 PMT 中的 CA 描述符）、并将修改后的 PSI 信息多路复用回数据流。支持 NDS 加密的 ECM 也可以在 PID 重映射器和扰乱器 620 处被插进数据流（或者可由分组选择器 / 复制器 610 来插入）。

[0138] 因此，为了向使用摩托罗拉设备的有线电视系统前端设备增加 NDS 加密（或另一个加密系统），要复制分组并在来自卫星去扰乱器的数据流中重映射 PID。重映射的 PID 然后用于标识要用各 CA 系统进行扰乱的分组。一旦进行了传统系统加密，就重映射明文 PID，以使传统系统中的明文和加密分组共享相同的 PID。可以用编程处理器或用诸如专用集成电路或可编程逻辑设备或现场可编程门阵列之类的定制或半定制的集成电路来实现如在 620 中的 PID 重映射以及如在 610 中的分组选择和复制。在不脱离本发明的情况下，还可以有其它实现形式。

[0139] 图 12 说明了诸如在基于 Scientific Atlanta 的有线电视前端设备中实现本发明部分双重加密时使用的类似设备配置。在这一实施例中，在 IRD704 处接收 HTITS 馈送或类似的馈送，IRD704 包括卫星去扰乱器 706。其可以是摩托罗拉 IRT 或仅具有卫星去扰乱器功能的 MPS。卫星去扰乱器 706 的输出同样提供明文数据流，该数据流可由新分组选择器 / 复制器 710 来处理，新分组选择器 / 复制器 710 可选择要加密的分组、复制它们并将复制的分组的 PID 映射至新 PID。同样地，例如对以明文方式保留的分组分配以 PID A，对用新系

统（例如NDS）加密的分组分配以PID B，对用Scientific Atlanta加密系统加密的分组分配以PID C。带有PID B的分组可在这时用NDS加密系统进行加密。

[0140] 然后，分组流被发送给多器复用器712（例如Scientific Atlanta多器复用器），在那里，在与多路复用器712相关的控制系统718的控制下在714处用Scientific Atlanta加密系统对带有PID C的分组进行加密。然后，数据流在多路复用器712的内部被提供给QAM调制器720。为了正确地重映射分组，将在多路复用器712的输出端处的经QAM调制的信号提供给新处理器系统724，在该系统中，在QAM解调器730处对经QAM调制的信号进行解调制，并且在由控制系统738控制的PID重映射器734处将明文PID A分组重映射至PID C。还可以在这里而不是在710中实现用NDS加密算法的加密。然后，在742处对带重映射的PID和双重部分加密的数据流进行QAM和RF调制，以便在有线电视系统上发布。

[0141] 在上述实例中，PID重映射器和扰乱器734还可以用于多路分解PSI信息、对其修改以反映出增加了NDS加密（向PMT添加CA描述符）并将修改后的PSI信息多路复用回数据流。支持NDS加密的ECM也可以在PID重映射器和扰乱器734处被插进数据流（或者可由分组选择器/复制器710来插入）。可以用编程处理器或用诸如专用集成电路或可编程逻辑设备或现场可编程门阵列之类的定制或半定制的集成电路来实现如在734中的PID重映射和/或扰乱以及分别如在730和724中的QAM解调制和QAM调制以及如在710中的分组选择和复制。在不脱离本发明的情况下，还可以有其它实现形式。

[0142] 本发明的上述实施例能使传统扰乱设备仅扰乱基本流中所期望的分组而不是整个基本流。可利用不打算被扰乱的分组的PID号（例如PID A）来扰乱基本流的特定分组。将要扰乱的分组放置到PID C上。扰乱设备会扰乱PID C上的分组（业已被选定要扰乱的分组）。在扰乱之后，未被扰乱的分组具有这样的PID号，该PID号被映射到与扰乱的分组相同的PID号----PID A变成PID C。传统机顶盒会接收带有被扰乱和未被扰乱的分组的基本流。

[0143] 以流的形式来处理在这些实施例中的分组。整个流被发送至传统扰乱设备以便进行扰乱。这就会使所有的分组保持精确的时间同步次序。如果分组是从流中提取出的并且被发送至传统扰乱设备，则可能会引入时间抖动。本实施例通过将所有的分组保持在流内而避免了这个问题。本实施例不需要来自传统扰乱设备供应商的合作，因为所述设备不涉及将分组从PID A重映射到PID C。这种重映射是优选的，因为由传统扰乱系统生成的PSI所取出的PID无需改变。传统系统知道PID C，但不知道PID A。在业已指示扰乱系统对其进行扰乱的单个PID上能找到要由传统扰乱设备所扰乱的全部基本流。

[0144] 在上述实例中，将NDS用作第二加密系统不应看作是限制性的。而且，尽管通过举例的方式说明了两种广泛使用的系统----摩托罗拉和Scientific Atlanta，但也可以使用对传统系统的类似的修改以便允许PID重映射和双重部分加密。一般地说，上述技术涉及总的如图13中800所述的处理过程。在806处接收馈送，该馈送在810处被接收时得以去扰乱，从而产生分组的明文数据流。在814处根据所期望的部分双重加密技术（例如仅对音频加密、对包含PES头标的分组加密等等）来选择分组。在818处，复制所选择的分组，并且，将各复制对重映射至两个新PID（例如PID B和PID C）。然后，在822处根据PID对复制的分组进行加密（也就是说，根据传统加密对PID C进行加密，根据新加密系统对PID

B 进行加密）。然后在 826 处，将明文分组（例如 PID A）重映射至与传统加密的 PID(PID C) 相同的 PID。

[0145] 图 13 的处理过程的某些单元执行的顺序可随被修改以适应所使用的特定双重加密安排的特定传统系统的不同而变化。例如，可在复制时或者在以后的重映射传统分组时用新加密系统进行加密，如图 11 和 12 所示。此外，可按需进行多种解调制和重调制操作，以适应已有的特定传统系统（图 13 中未示出）。

[0146] 机顶盒的实现形式

[0147] 在本发明的范围内可以有若干种机顶盒实现形式。前端设备中用于选择分组以便加密的方法与 STB 无关。

[0148] 图 14 说明了一种这样的实现形式。在这一实施例中，将来自调谐器和解调器 904 的分组提供给解码器电路 908 的多路分解器 910。分组被缓存进存储器 912（例如使用统一存储器架构）并且由 STB 的主 CPU916 用存储在 ROM 存储器 920 中的软件来加以处理。

[0149] 可通过 STB 的 PID 过滤器从输入的传输中剥离出选定的 PID，对其加以解密并缓存进同步动态随机存取存储器 (SDRAM)，这与个人录像机 (PVR) 应用中准备传输给硬盘驱动器 (HDD) 所需要的初始处理过程相类似。然后，主 CPU916 可“手工”过滤缓存在 SDRAM 中的数据以便消除包含不需要的 PID 的分组。这一处理过程有某些明显的副作用。

[0150] 主机开销据估计约为 CPU 带宽的 1%。在最坏的情况下，对 15Mbit/s 的视频流来说，这等于 40K 字节 / 秒。这种减少是可能的，因为每个分组至多仅有 4 字节被评估，并且其位置位于 188 字节间隔处，所以不必考虑居中的数据。因而，可通过简单的存储器指针处理直接访问 SDRAM 中的各个分组头标。此外，分组被高速缓存在块内并且被一起评估，以减少主机的任务切换。这就会在接收到各个新分组时消除对其它任务的干扰。在频道变化时，这可能会产生有所增加的用于启动对流进行解码的等待时间以便有时间填充高速缓存。根据所分配的 SDRAM 高速缓存缓存器大小这一点是可以忽略的。

[0151] 然后，将 SDRAM 缓存中的经主机过滤的分组通过一个用于处理和模拟 PVR 实现形式的现有硬件 DMA 而传给 A/V 队列。所过滤的分组然后被提供给解码器 922 以便进行解码。

[0152] 图 15 中说明了机顶盒中的实现形式的第二种技术。由于解码器电路 930 中的 RISC 处理器的 A/V 解码器模块 934 处理部分传输 PID 并进行剥离 / 连接以便进行解码，所以可改变解码器 IC930 中的固件以便根据各分组头标中的标准排除部分传输流内的个别分组。或者，多路分解器 910 可设计成排除所说的分组。传统扰乱的分组通过 CA 模块后仍是加密的。利用解码器 IC930 去执行除去传统扰乱的分组并假定用新加密算法（例如 NDS）加密的分组直接与传统加密的分组相邻（或至少在下一个主流视频分组之前），于是削除传统分组实际上完成了将单个的明文流合并进头标区和视频队列。

[0153] 图 16 说明了用于在机顶盒中实现部分加密的第三种技术。在这一实施例中，在诸如专用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或可编程逻辑设备 (PLD)938 之类的电路或放在调谐器和解调器 904 与解码器 IC908 之间的其它定制设计的电路中进行 PID 重映射。在本实施例的一种变化形式中，可以修改解码器 IC908 以便在多路分解器 940 中实现 PID 重映射。在这两种情况下，丢弃传统加密的分组，并在电路 938 或多路分解器 940 重映射非传统的分组。

[0154] 在一个实施例中可用图 17 所示的 PLD 实现上述第三种技术。这种实现形式假定

不存在一个以上的连续出现的特定 PID 的加密分组，因此，可以修改这种实现形式以适应诸如用上述 M 和第 N 加密安排来加密的分组串（后面将予以说明）。输入流通过 PID 识别器 950，该识别器用于根据 PID 对输入流进行多路分解。在 958 检查主 PID 分组连续性。如果检测到连续性错误，就标注该错误并在 960 处重置计数。

[0155] 原始输入分组流包含用多个 PID 标记的分组。PID 识别器 950 将带有所关心的两个 PID（主、次 PID）的分组与所有其它分组分隔开。这种能力可扩展成处理多个 PID 对。其它分组被直接绕送至修正过的输出流。这一处理过程会导致三个或四个字节的时钟延迟。

[0156] PID 识别器 950 将带有次 PID 的分组选路传送至连续计数检查器 945，它验证该 PID 的序列完整性。在 956 处标注任何错误，但对错误的专门处理与理解本发明无关。保留分组的连续值以供检查后来分组的顺序时使用。用独立的主计数对带有主 PID 的分组进行相应的连续性检查 958，在 960 处同样地记录任何的错误。

[0157] 在 962 处检查次分组的次标志。用这个布尔指示符记住自从上一个明文分组以来是否已处理了次分组。明文分组之间的一个以上的次分组在本实施例中是一种错误，并在 964 处标注。通过在 966 处设置次标志而记住次分组的存在。

[0158] 次分组的连续计数在 968 处被改变以适应明文分组序列。用于这种替换的数据来自用于在 958 处检验主流的连续性的值。修改后的分组从 968 处送出并被合并进构成输出流的修改后的流。

[0159] 在业已于 958 处对带主 PID 的分组进行了连续性检查以后，在 970 处通过头标中的扰乱标志而对它们进行区分。如果是被扰乱的分组，则在 974 处查询主标志。主标志布尔指示符用于记住自从上一个明文分组以来是否已处理了加密的主分组。明文分组之间的一个以上的主加密分组在本实施例中是一种错误，在于 978 处将分组丢弃之前于 976 处将其标注下来。通过在 980 处设置主标志而记住加密的主分组的存在。如果对加密的主分组来说没有下游消费者，则可在 978 处将其丢弃。在某些情况下，该分组可能必须继续下去（在这种情况下，其连续计数可使用被丢弃的次连续值）。

[0160] 如果 970 处的主 PID 扰乱测试检测到了明文分组，则在 984 处测试主、次标志的状态。有效条件是同时都未设置和同时都设置，因为加密的分组应以匹配对的方式出现。只有一个而没有另一个的序列应在 988 处标注为错误。然而在本实施例中，出现的次序是无关紧要的。应该注意，除传输头标中的扰乱位（例如 transport_priority）位以外，还可以有其它方式标记要删除的主分组。还有，可以不将任何比特，例如利用主分组在次分组之前或之后的简单位置信息，作为用于替代的指示符。

[0161] 在修改的输出流中被输出之前，带有主 PID 的明文分组的 PID 值在 922 处被改变成次 PID。或者，次 PID 分组可被重映射至主 PID 值。可在向解码器提供正确的 PID（主或次 PID）以便对内客进行解码时，对内容进行解码。明文分组的存在还会清除主、次布尔标志。

[0162] 在所提出的所有实施例中，即使在标记了一系列主分组以便替换时，仍可在与要被替换的主分组相邻的位置处插入次分组。但是，在某些情况下，如果在没有居中分组的情况下可将多个加密的分组插进流内，则可能会便于前端设备的部分扰乱。为了适应多个连续的加密分组（诸如和第 M 和 N 部分加密方法一样），可用计数匹配测试功能来代替使用主、辅标志。因此，代替单元 962、964 和 966，可以增加次加密分组计数。代替单元 970、974、

976 和 980，可以增加主加密分组计数。可通过比较主与次加密分组计数以确保在主、次通路上都接收到同样数量的加密分组来代替单元 984。代替在 992 处清除标志，可以清除计数。利用这种变化形式，可连续地接收多个加密的分组，并将接收到的数量进行比较，以便监视数据流的完整性。本领域熟练技术人员会想到其它变化形式。

[0163] 以上连同图 17 所述的功能可以被集成进 A/V 解码器芯片，其功能类似于商用机顶盒中使用的商业可用的 Broadcom 系列 70xx 或 71xx 解码器。图 18 说明了用于这种解码器芯片的框图，其中，已在商用芯片中提供的功能基本上没变。一般地说，商用解码器芯片希望 PID 与节目组成部分（例如音频或视频）之间是一一对应的。

[0164] 图 18 所述的解码器能通过与 STB 中央处理器的连接以允许把多个 PID 编程进解码器，这样就可为主音频、主视频和用于画中画 (PiP) 功能的次视频处理主、次 PID。在这一实施例中，原始数据流由分组分类器 1002 所接收，分类器 1002 能提供与以上连同图 17 所述的相类似的根据 PID 对分组流进行多路分解的功能。优选的是，图 18 的解码器用硬连线逻辑电路而不是编程的软件来实现 1002 的 PID 分类功能。例如，节目指南和流导航信息被输出以供 STB 的主处理器使用。与主音频节目相关的分组被缓存在 FIFO1006 内、在解密器 1010 中解密、然后被缓存在 1014 处，以便供 MPEG 音频解码器 1018 在需要时获取。随后，作为来自解码器的输出提供解码后 MPEG 音频。

[0165] 按相似的方式，与主视频节目相关的分组被缓存在 FIFO1024 内、在解密器 1028 中解密、然后被缓存在 1032 处，以便供 MPEG 视频解码器 1036 在需要时获取。然后，用于主频道的解码后的 MPEG 视频被提供给合成器 1040，此后作为来自解码器的输出而被提供。与此类似，与画中画视频相关的分组被缓存在 FIFO1044 内、在解密器 1048 中解密、然后被缓存在 1052 处，以便供 MPEG 视频解码器 1056 在需要时获取。用于画中画频道的解码后的 MPEG 视频随后被提供给合成器 1040，在该合成器中，上述视频与主频道视频相组合，此后作为来自解码器的解码视频输出而被提供。丢弃不与主频道或画中画频道相关的其它分组。当然，在不脱离本发明实施例的情况下，其它功能也可以被包括在解码器芯片中或者从中删除。

[0166] 结论

[0167] 如前所述，为了阻止黑客的持久的威胁，可以将若干种上述部分加密安排结合起来以进一步增强安全性。例如，可将关键分组加密与 SI 加密、第 M 和 N、随机加密、时间片和其它技术任意结合使用，以便进一步增强安全性。在一个实施例中，可在可用带宽范围内对尽可能多的分组进行加密。加密的量可取决于内容是常规节目还是付费内容（诸如付费观看或 VOD）、是成人节目还是常规电影以及不同有线电视经营者感到能满意经营的安全级别。本领域熟练技术人员应该理解，在不脱离本发明的情况下，可以有多种其它的组合以进一步增强加密的安全性。

[0168] 业已就使用 MPEG2 编码的数字 A/V 系统在其上述多个实施例中说明了本发明。因此，所具体说明的多个分组名和协议涉及到 MPEG2 编码和解码。但是，本领域熟练技术人员应该认识到，本文所公开和所要求保护的思想不应看作是限制性的。可在不限于 MPEG2 协议的情况下，在任何数字有线电视系统中使用相同或相似的技术。而且，本发明的技术可用于任何其它适当的内容传送场合，包括（但不限于）基于地面广播的内容传送系统、基于因特网的内容传送、诸如例如在 DirecTV™ 系统中使用的数字卫星业务 (DSS) 之类的基于卫星的内容传送系统以及分组媒体（例如 CD 和 DVD）。这些多种替代形式在本文件中被看作是

等效的，示例性 MPEG2 的有线电视实施例应被看作是说明性的示例性实施例。

[0169] 此外，业已就使用电视机顶盒对部分加密的电视节目进行解码这一方面说明了本发明。但是，本解码机制可同样在不需要 STB 的电视接收机内或在诸如 MP3 播放器之类的音乐播放器内实现。这些实施例被看作是等效的。

[0170] 再有，尽管已就用上述加密技术提供电视节目的双重部分加密机制这一方面说明了本发明，但这些部分加密技术可也可用作单个的加密技术或者用于在两个以上的加密系统下作多重加密而没有限制。两种以上的加密系统可用于要进行加密的额外复制分组。或者，用于复制分组之一的加密密钥可在多个加密系统中共享。再有，尽管只具体公开了对电视节目的加密，但本发明也可用于其它内容的一重或双重加密，所述其它内容包括（但不限于）从因特网或其它网络上下载的内容、音乐内容、分组媒体内容以及其它类型的信息内容。在不脱离本发明的情况下，这种内容可在多种播放设备上播放，所述播放设备包括（但不限于）个人数字助理 (PDA)、个人计算机、个人音乐播放器、音频系统、音频 / 视频系统等等。

[0171] 本领域熟练技术人员应该认识到，业已就可用编程处理器实现的示例性实施例说明了本发明。但是，本发明不应受到这样的限制，因为可以用诸如专用硬件和 / 或与所述和所要求保护的本发明等效的专用处理器之类的硬件等效部件来实现本发明。与此相类似，通用计算机、基于微处理器的计算机、微控制器、光学计算机、模拟计算机、专用处理器和 / 或专用硬连线逻辑均可用于构建本发明的替换等效实施例。

[0172] 本领域熟练技术人员应该认识到，在不脱离本发明的情况下，用于实现上述实施例的程序步骤和相关数据可用盘存储器和诸如例如只读存储器 (ROM)、随机存取存储器 (RAM) 设备、光学存储器元件、磁存储器元件、磁 - 光存储器元件、闪存存储器、磁心存储器之类的其它形式的存储器和 / 或其它等效存储技术来实现。这些替换形式的存储器设备可看作是等效的。

[0173] 本发明如本文实施例中所述可用执行编程指令的编程处理器来实现，所述编程指令在以上流程图中作了概括性说明并且可存储在任何适当的电子存储媒体上或者在任何适当的电子通信媒体上传输。但是，本领域熟练技术人员应该认识到，在不脱离本发明的情况下，上述处理过程可用多种变化形式和多种适当的编程语言加以实现。例如，所执行的某些操作的次序通常是可变的，在不脱离本发明的情况下，可以增加额外的操作或删除操作。可以增加和 / 或增强错误捕获，并且可在不脱离本发明的情况下改变用户界面和信息呈现方式。这些变化形式被看作是等效的。

[0174] 尽管连同具体实施例说明了本发明，但是很明显，本领域熟练技术人员可从上述说明中看出多种替换、改进、变更和变化。因此，本发明希望包括落在后附权利要求书范围内的所有这些替换、改进和变化。

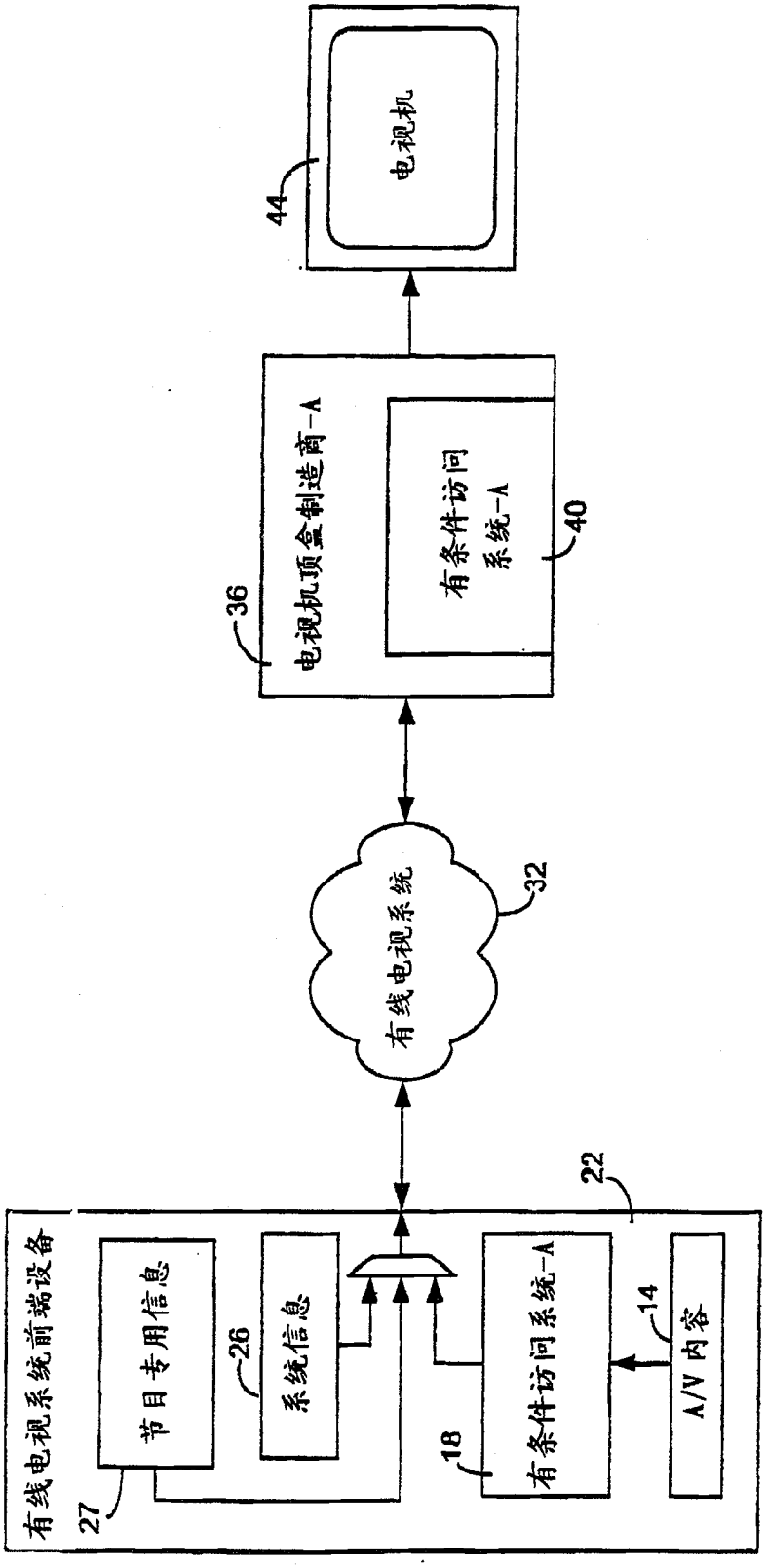

电视机
44
电视机顶盒制造商-A
有条件访问系统-A
40
36
有线电视系统
32
有线电视系统前端设备
节目专用信息
系统信息
有条件访问系统-A
A/V 内容
27
26
18
14
22

图 1

（现有技术）

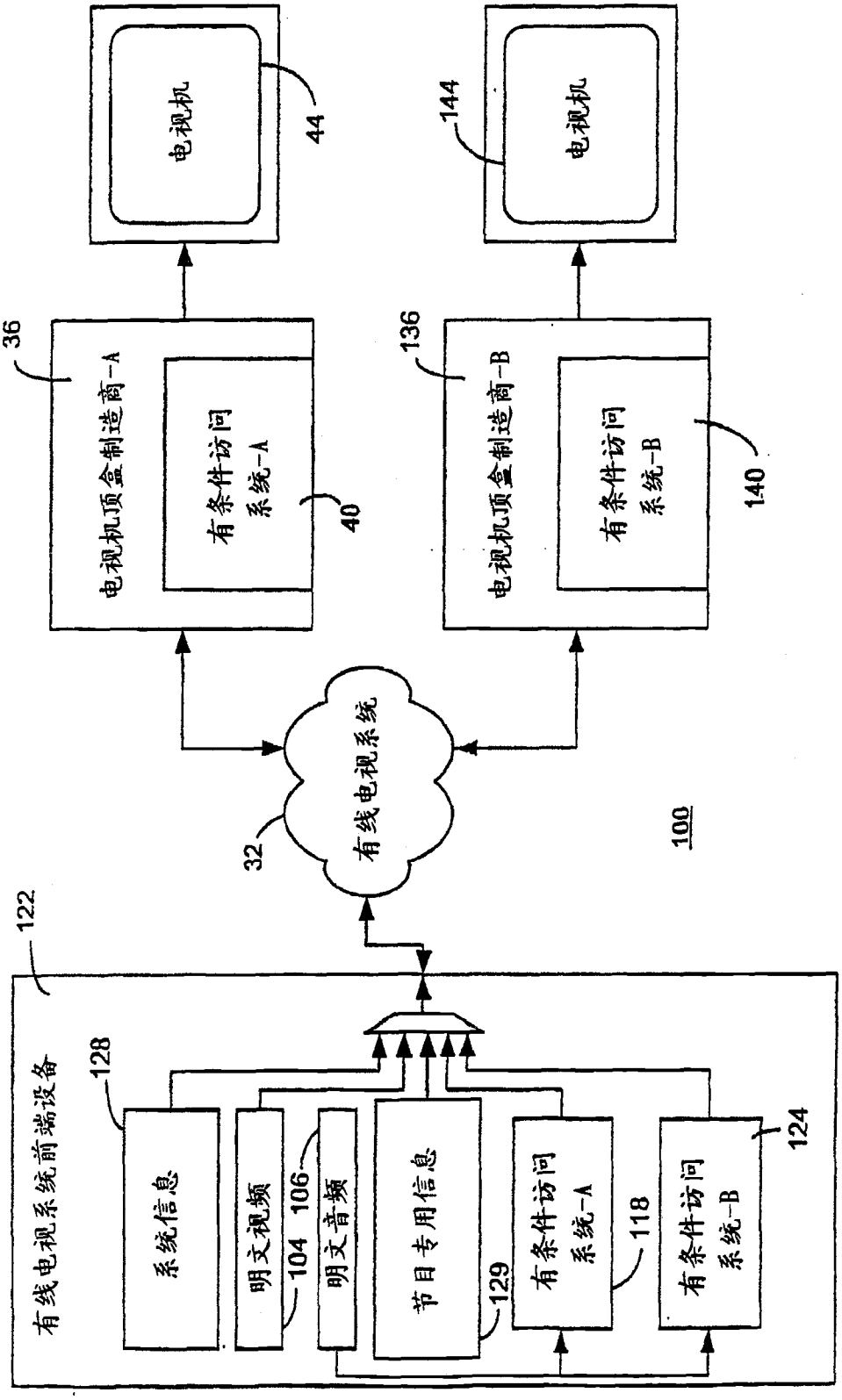

电视机
44
144
电视机
36
电视机顶盒制造商-A
有条件访问
系统-A
40
136
电视机顶盒制造商-B
有条件访问
系统-B
140
32
有线电视系统
100
122
有线电视系统前端设备
128
系统信息
明文视频
104
106
明文音频
节目专用信息
129
有条件访问
系统-A
118
有条件访问
系统-B
124

图 2

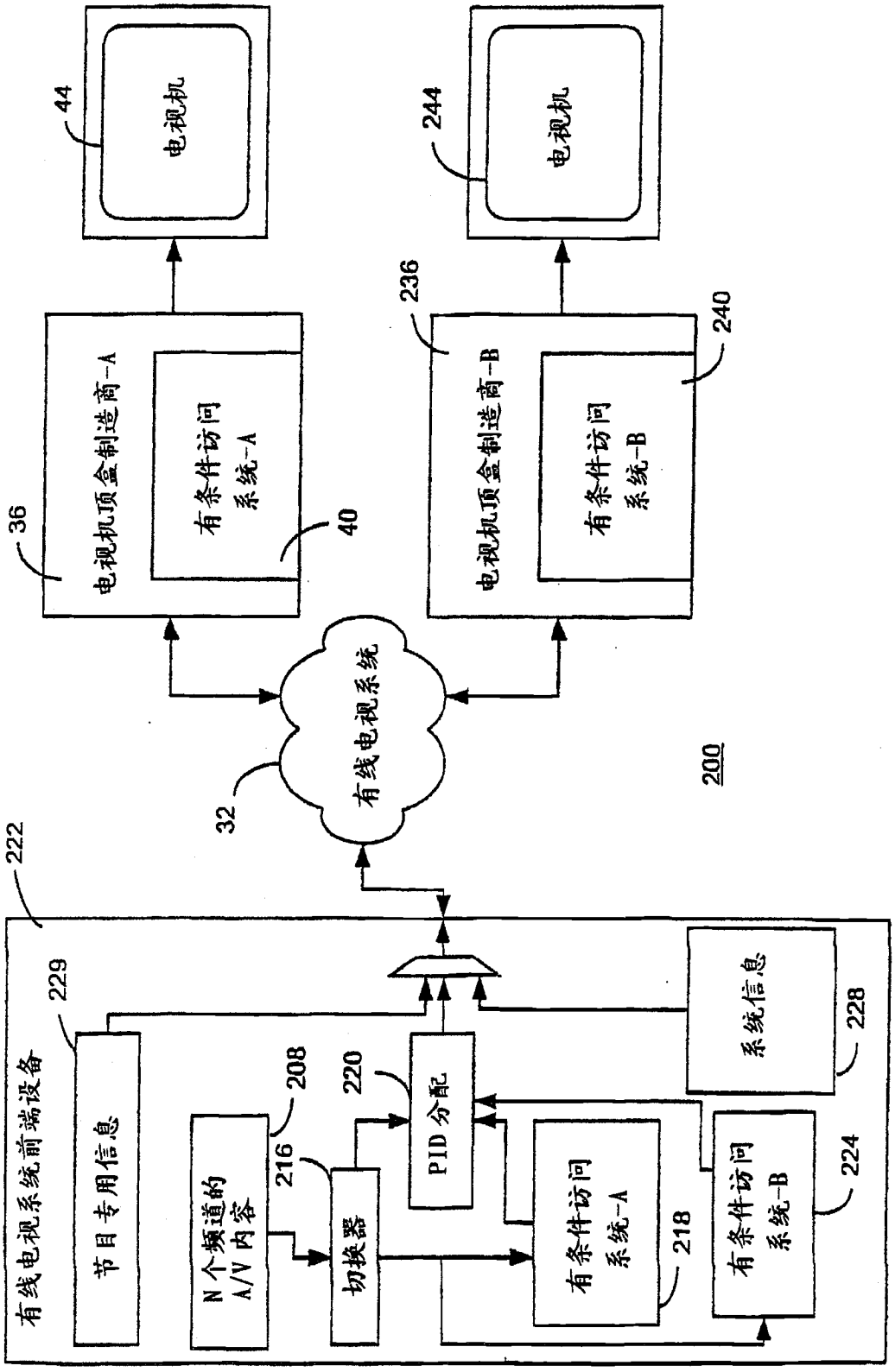

电视机
44
电视机
244
电视机顶盒制造商-A
有条件访问
系统-A
36
40
电视机顶盒制造商-B
有条件访问
系统-B
236
240
有线电视系统
32
200
222
有线电视系统前端设备
节目专用信息
229
N个频道的
A/V内容
208
切换器
216
PID分配
220
系统信息
228
有条件访问
系统-A
218
有条件访问
系统-B
224

图 3

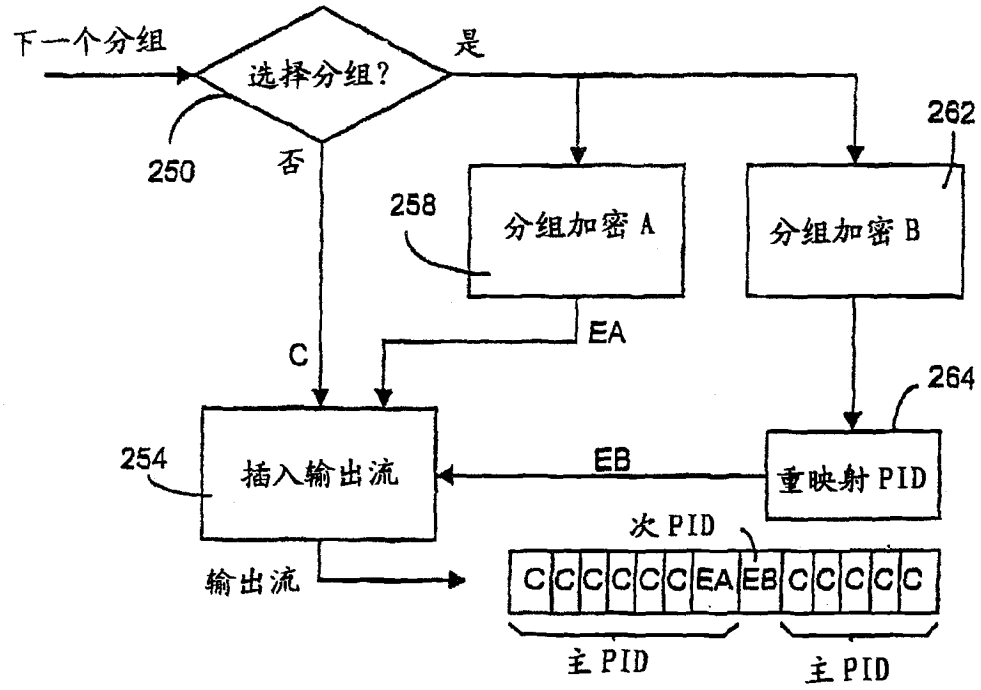

下一个分组
选择分组?
是
否
250
262
258
分组加密 A
分组加密 B
EA
C
264
254
插入输出流
EB
重映射 PID
次 PID
输出流
C C C C C C EA EB C C C C C
主 PID
主 PID

图 4

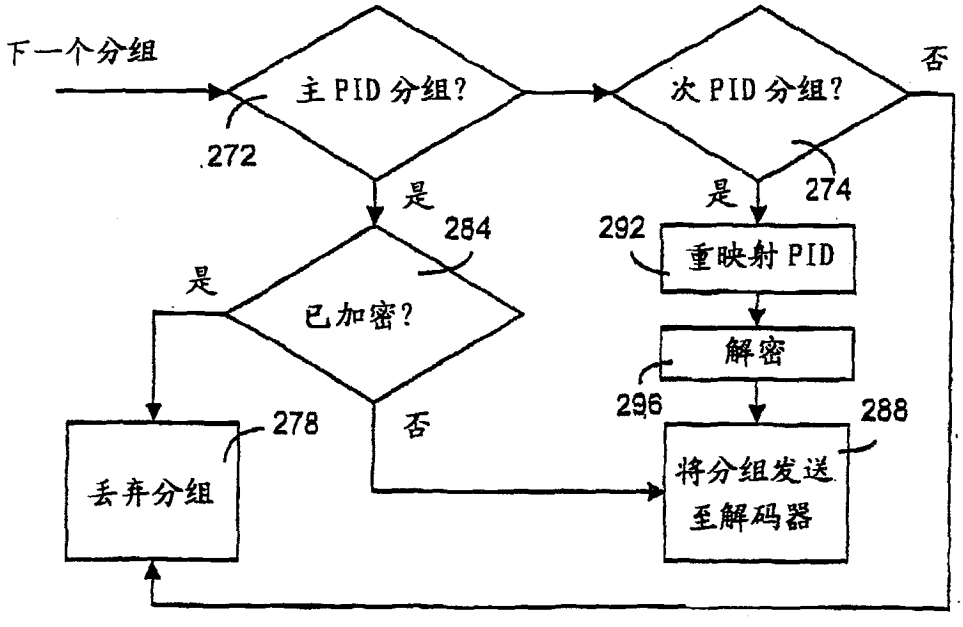

下一个分组
主 PID 分组?
次 PID 分组?
否
272
是
274
是
284
292
重映射 PID
是
已加密?
解密
296
288
278
否
丢弃分组
将分组发送至解码器

图 5

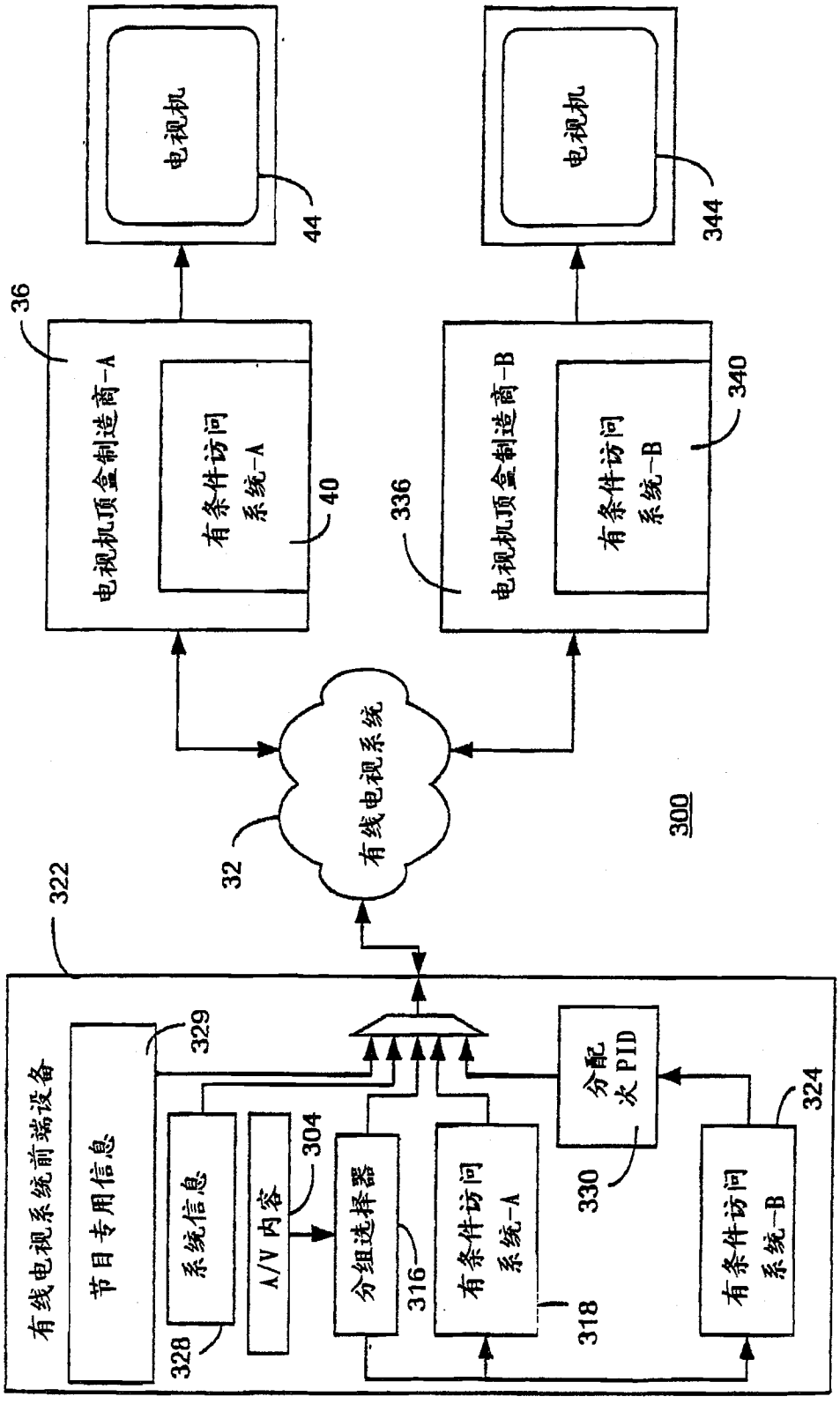

电视机
44
电视机
344
36
电视机顶盒制造商-A
有条件访问
系统-A
40
电视机顶盒制造商-B
有条件访问
系统-B
340
336
有线电视系统
32
300
322
有线电视系统前端设备
节目专用信息
329
系统信息
328
A/V 内容
304
分组选择器
316
有条件访问
系统-A
318
分配
次 PID
330
有条件访问
系统-B
324

图 6

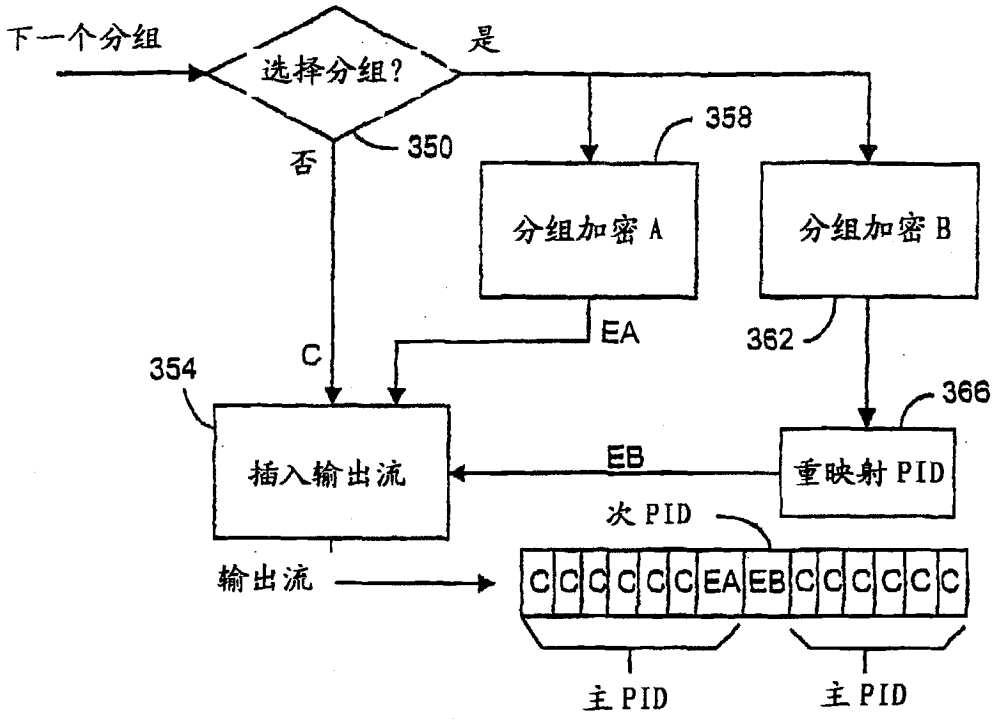

下一个分组
选择分组?
是
否
350
358
分组加密 A
分组加密 B
EA
362
C
354
366
插入输出流
EB
重映射 PID
次 PID
输出流
C C C C C C EA EB C C C C C C
主 PID
主 PID

图 7

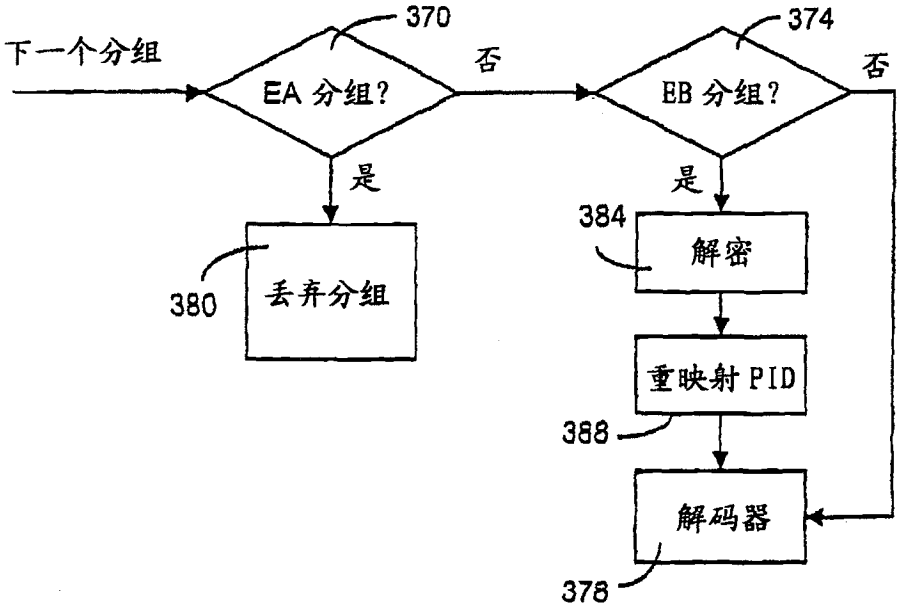

下一个分组
370
EA 分组?
否
374
EB 分组?
否
是
是
384
解密
380
丢弃分组
重映射 PID
388
解码器
378

图 8

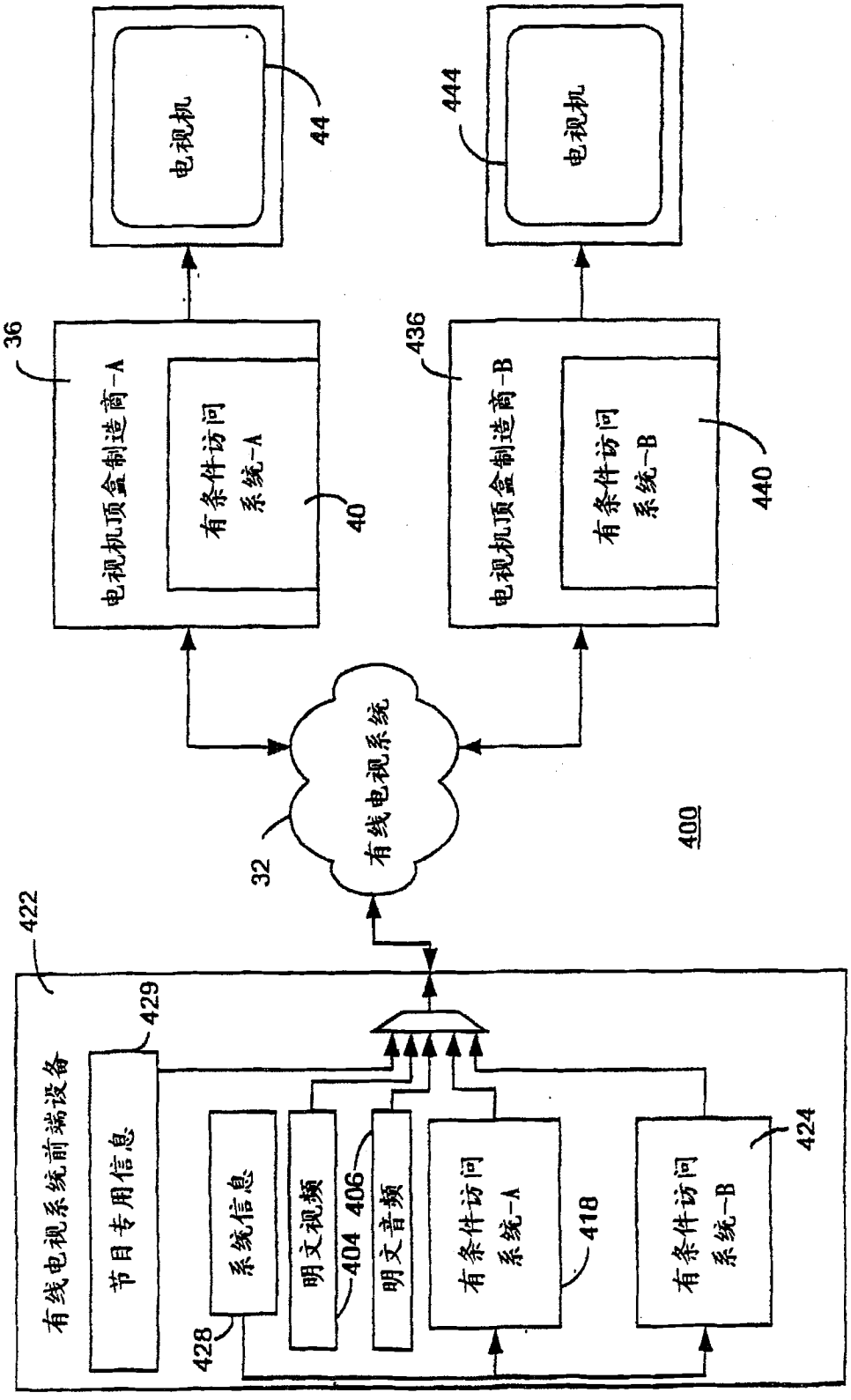

电视机
44
444
电视机
36
电视机顶盒制造商-A
有条件访问
系统-A
40
436
电视机顶盒制造商-B
有条件访问
系统-B
440
有线电视系统
32
400
422
有线电视系统前端设备
429
节目专用信息
系统信息
428
明文视频
404
406
明文音频
有条件访问
系统-A
418
有条件访问
系统-B
424

图 9

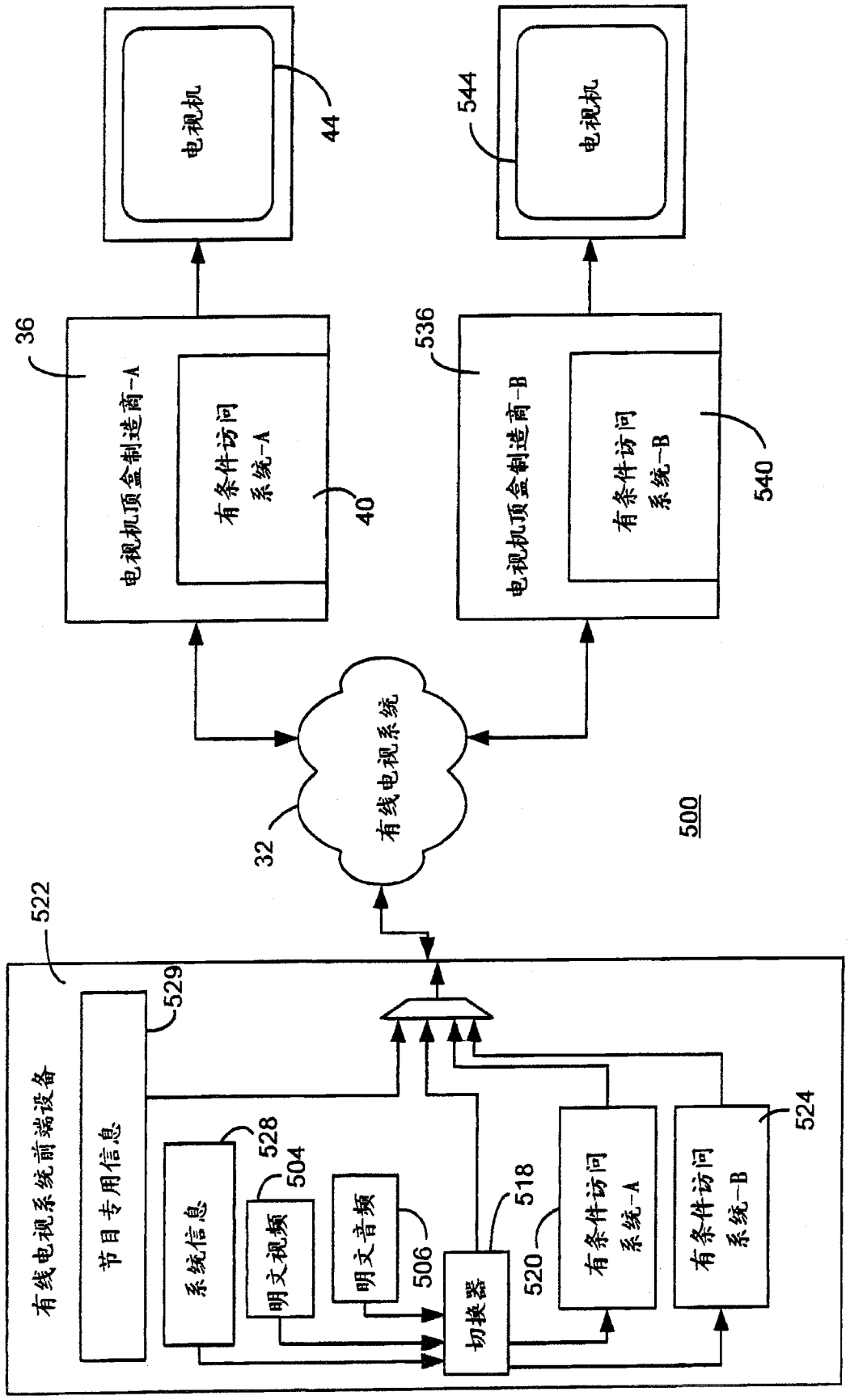

电视机
44
544
电视机
36
电视机顶盒制造商-A
有条件访问
系统-A
40
536
电视机顶盒制造商-B
有条件访问
系统-B
540
有线电视系统
32
500
522
有线电视系统前端设备
节目专用信息
529
系统信息
528
504
明文视频
506
明文音频
518
切换器
520
有条件访问
系统-A
有条件访问
系统-B
524

图 10

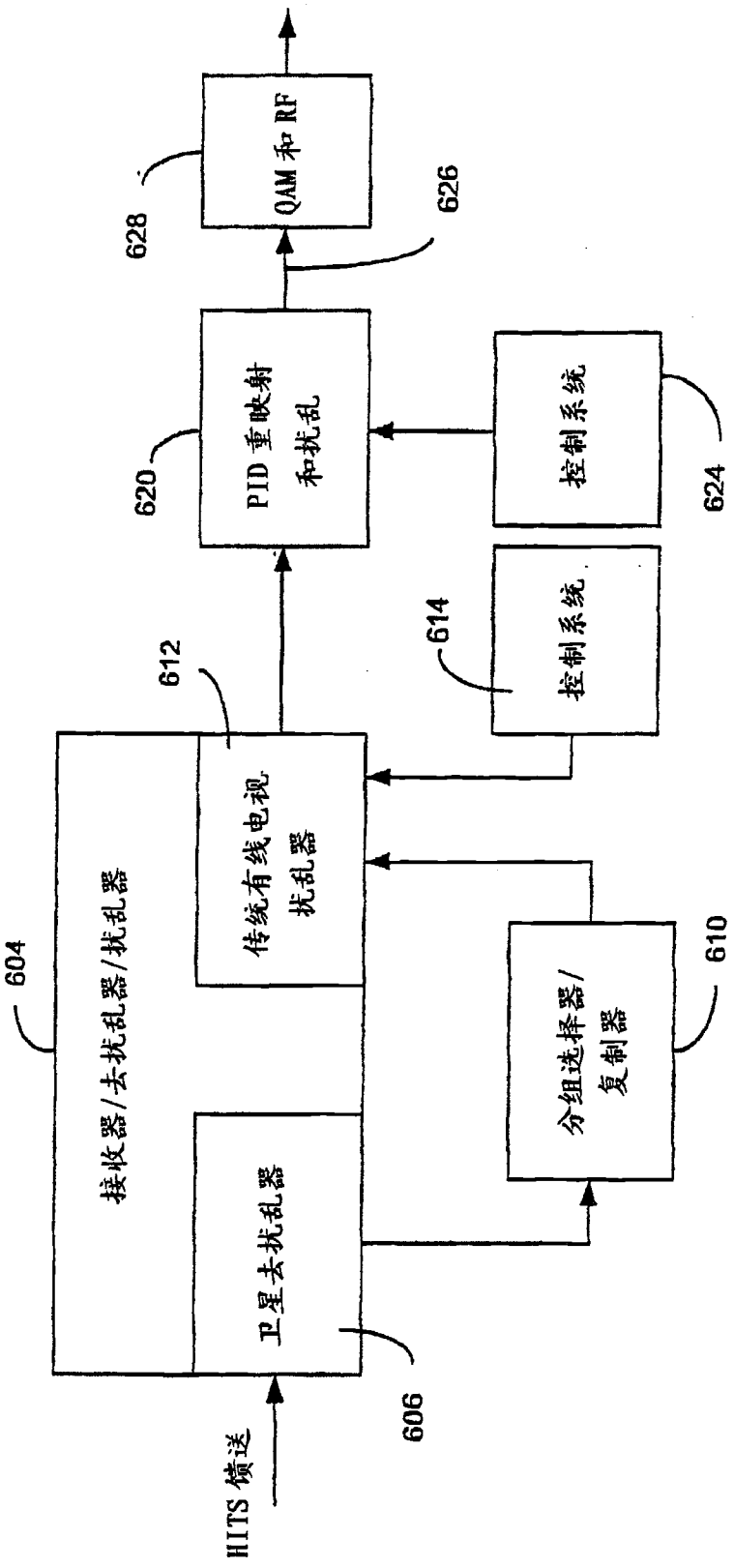

HITS 馈送
卫星去扰乱器
606
接收器/去扰乱器/扰乱器
604
传统有线电视扰乱器
612
分组选择器/复制器
610
控制系统
614
控制系统
624
PID 重映射和扰乱
620
QAM 和 RF
628
626

图 11

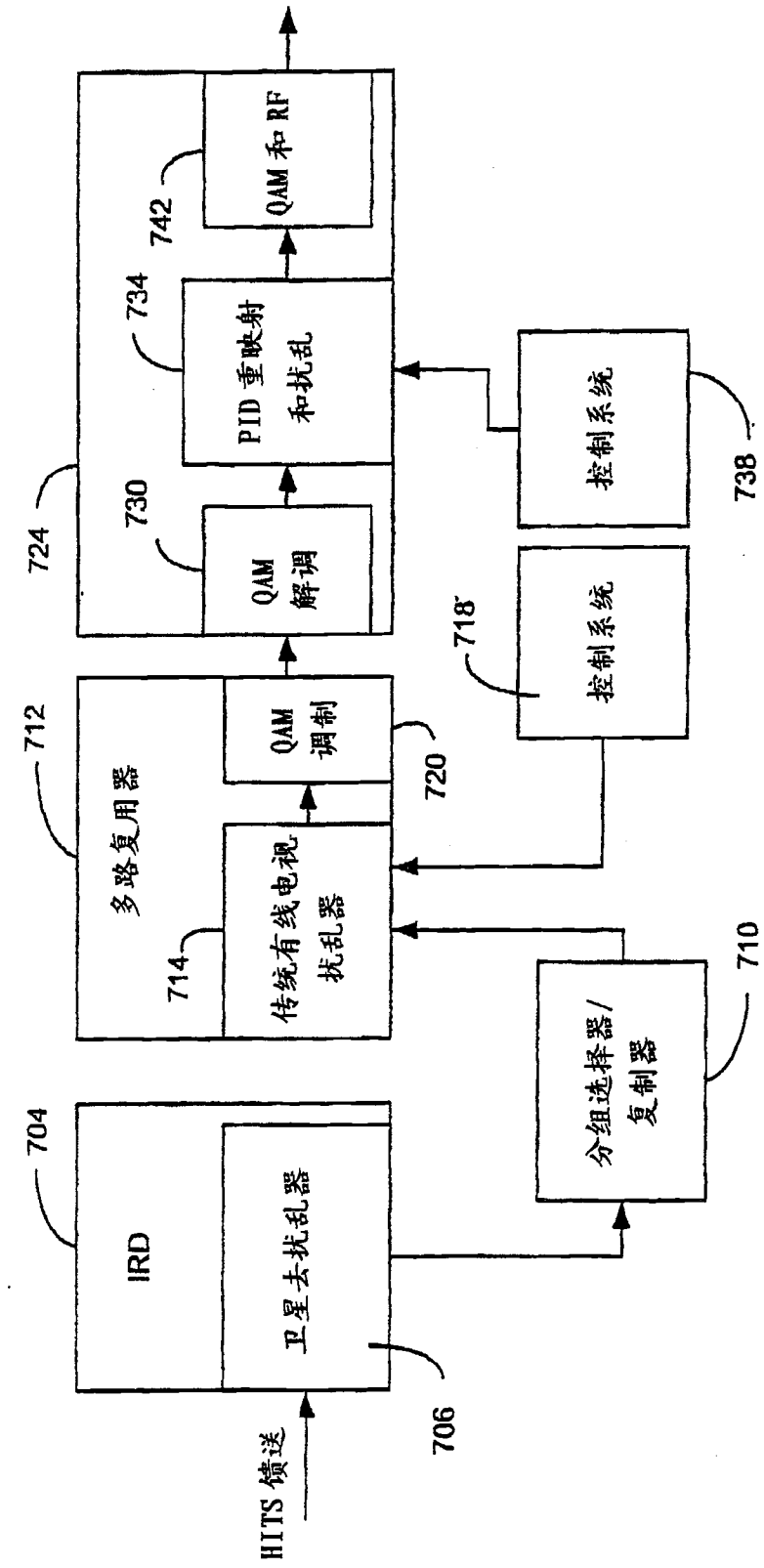

HITS 馈送
706
IRD
卫星去扰乱器
704
多路复用器
712
714
传统有线电视
扰乱器
QAM
调制
720
718'
控制系统
分组选择器/
复制器
710
724
730
QAM
解调
PID 重映射
和扰乱
734
742
QAM 和 RF
控制系统
738

图 12

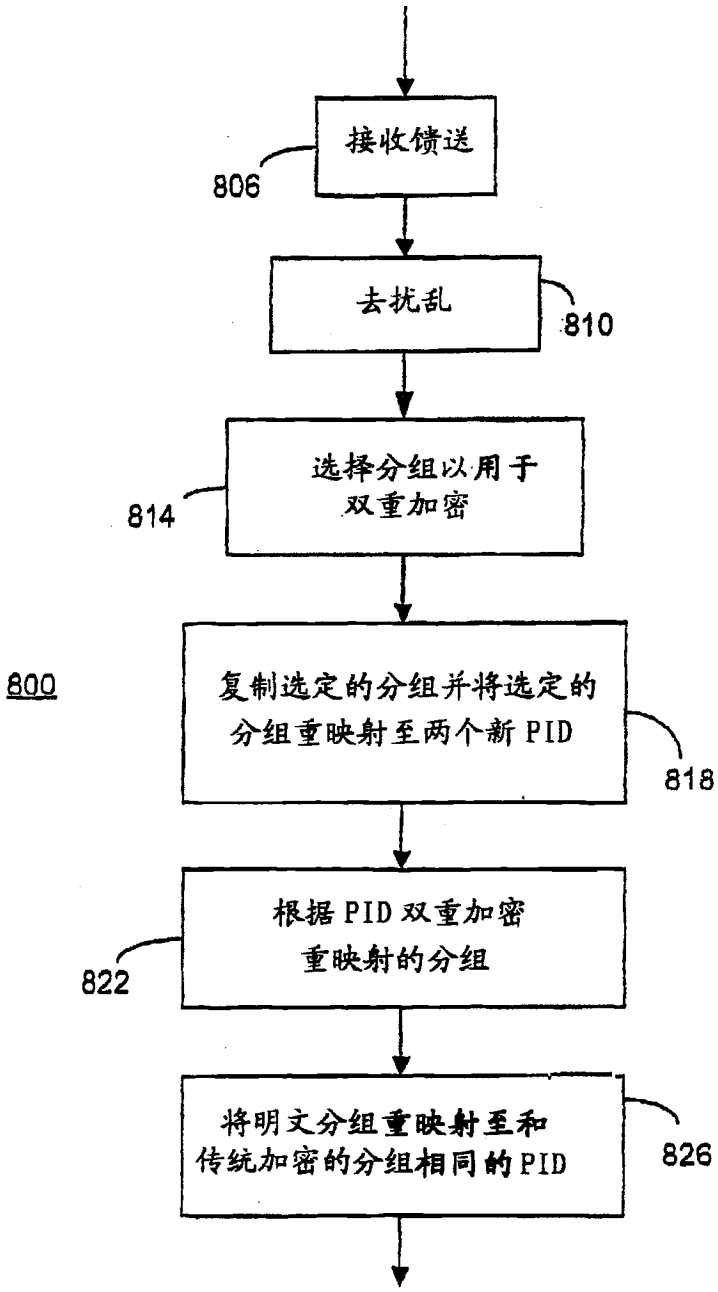

接收馈送
806
去扰乱
810
选择分组以用于双重加密
814
800
复制选定的分组并将选定的分组重映射至两个新 PID
818
根据 PID 双重加密重映射的分组
822
将明文分组重映射至和传统加密的分组相同的 PID
826

图 13

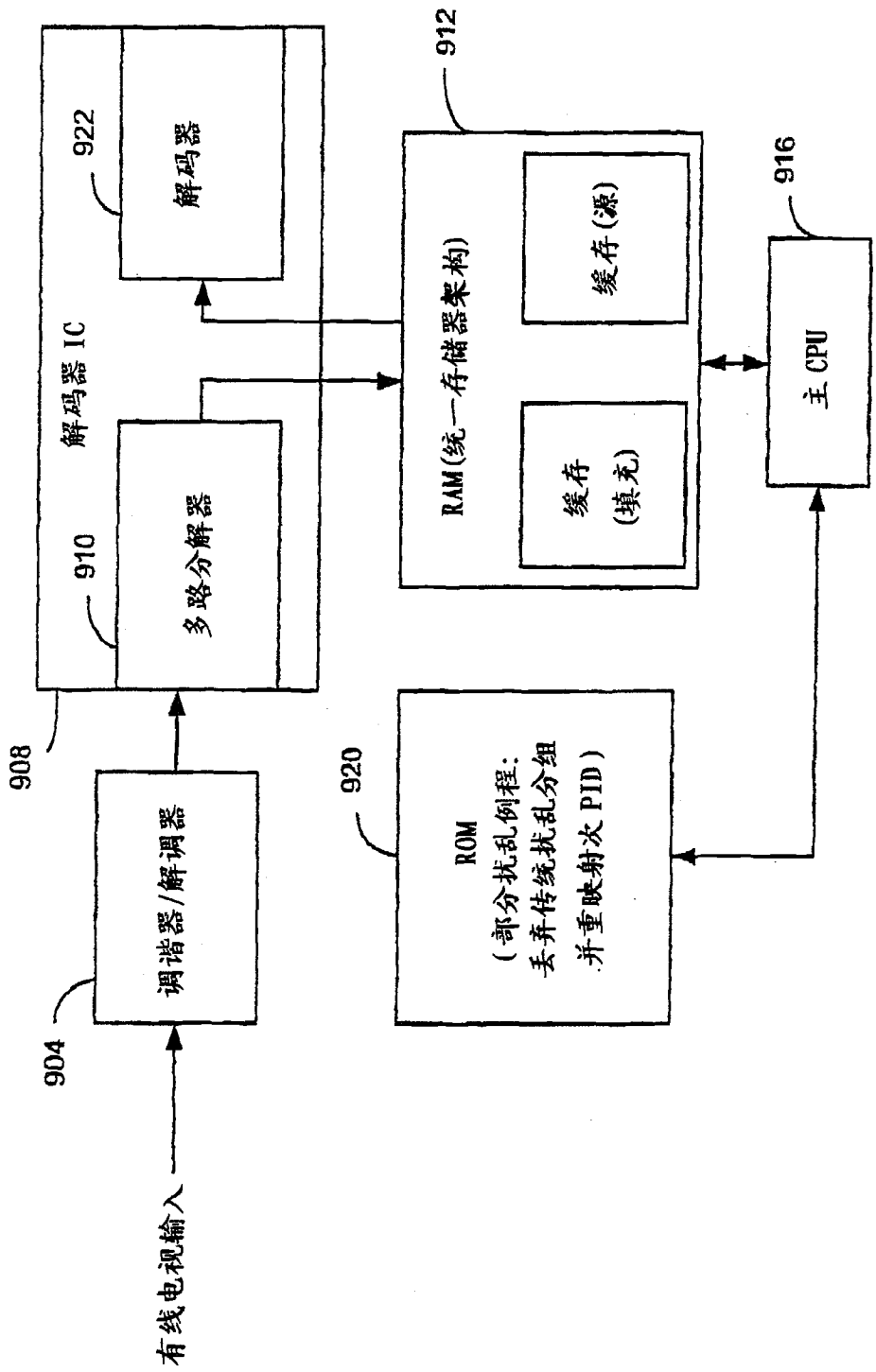

有线电视输入
904
调谐器/解调器
908
解码器 IC
910
多路分解器
922
解码器
912
RAM(统一存储器架构)
缓存
(填充)
缓存(源)
920
ROM
(部分扰乱例程:
丢弃传统扰乱分组
并重映射次 PID)
916
主 CPU

图 14

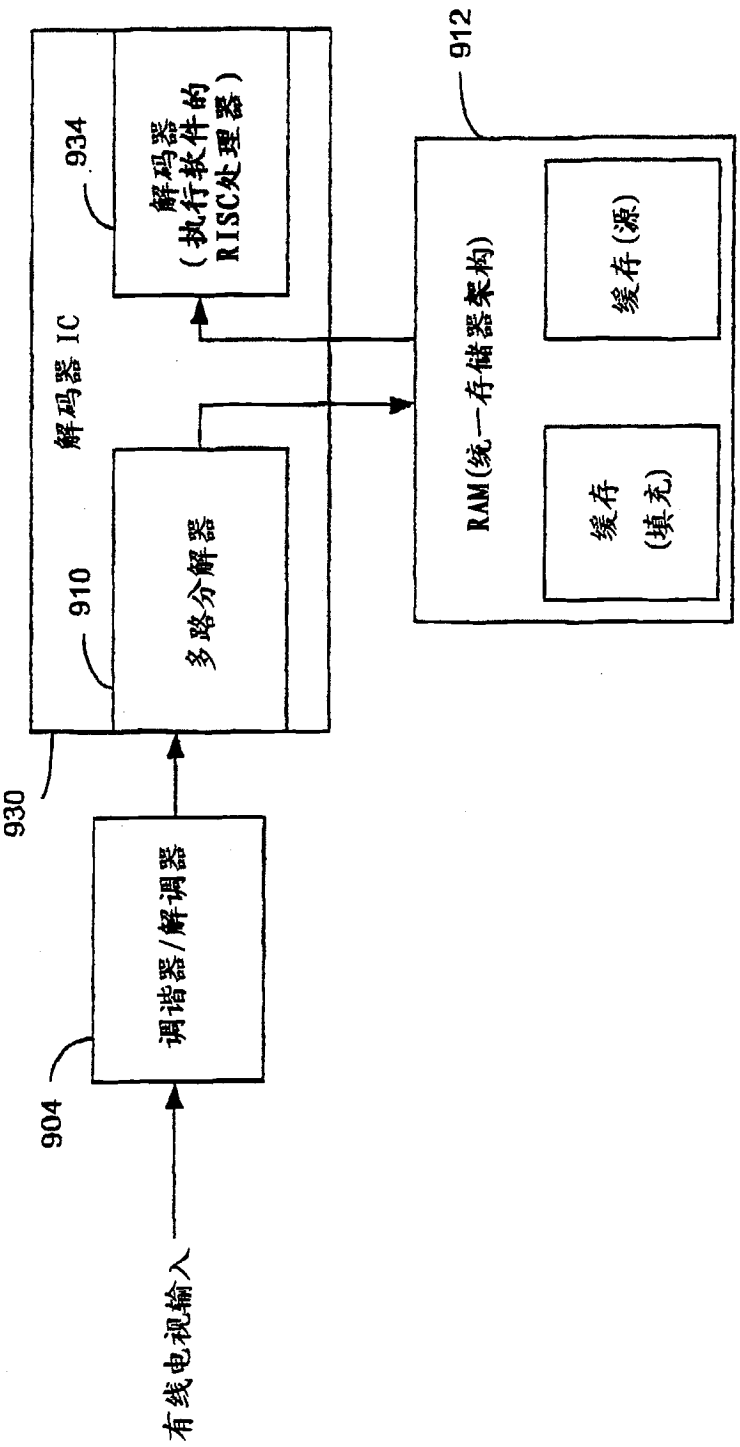

有线电视输入
904
调谐器/解调器
930
解码器 IC
910
多路分解器
934
解码器
(执行软件的
RISC处理器)
912
RAM(统一存储器架构)
缓存
(填充)
缓存(源)

图 15

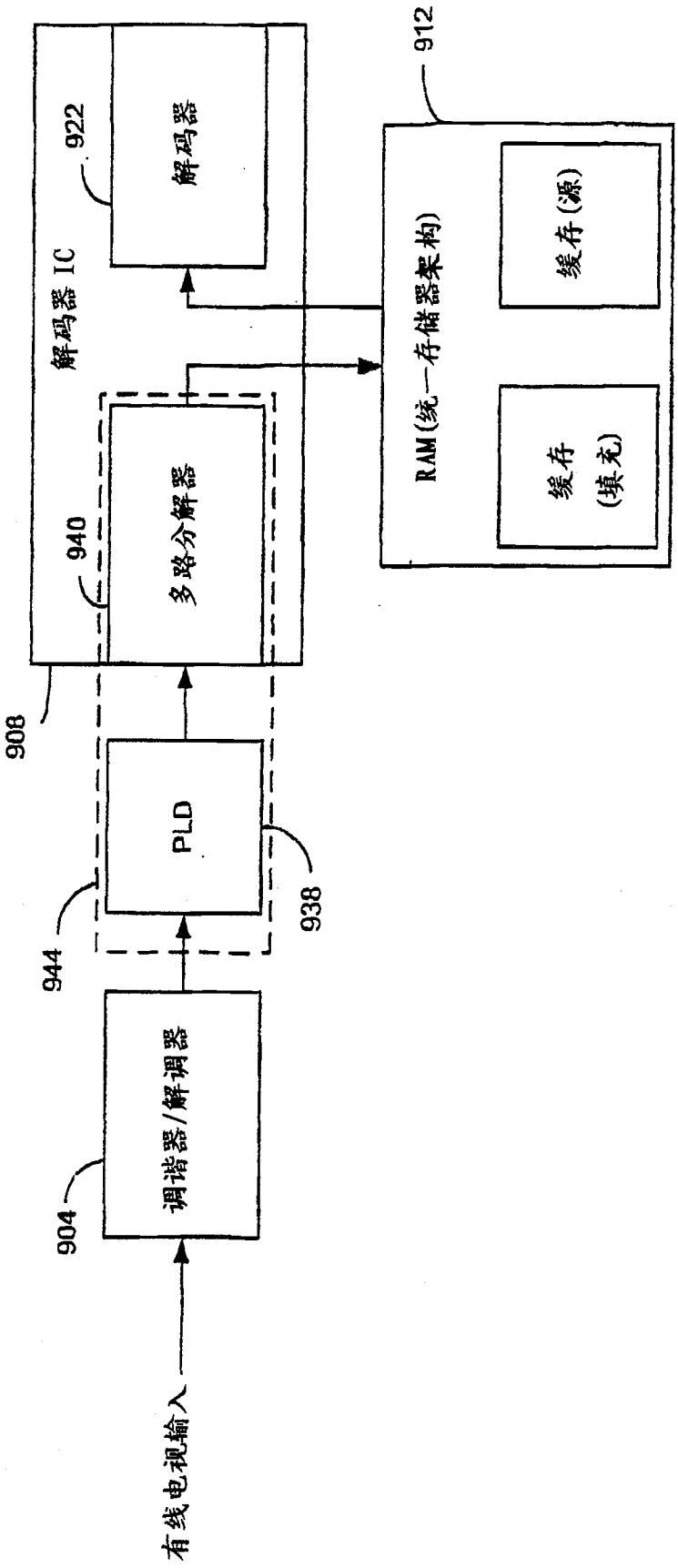

912
922
解码器
解码器 IC
RAM(统一存储器架构)
缓存(源)
缓存
(填充)
940
多路分解器
908
PLD
938
944
调谐器/解调器
904
有线电视输入

图 16

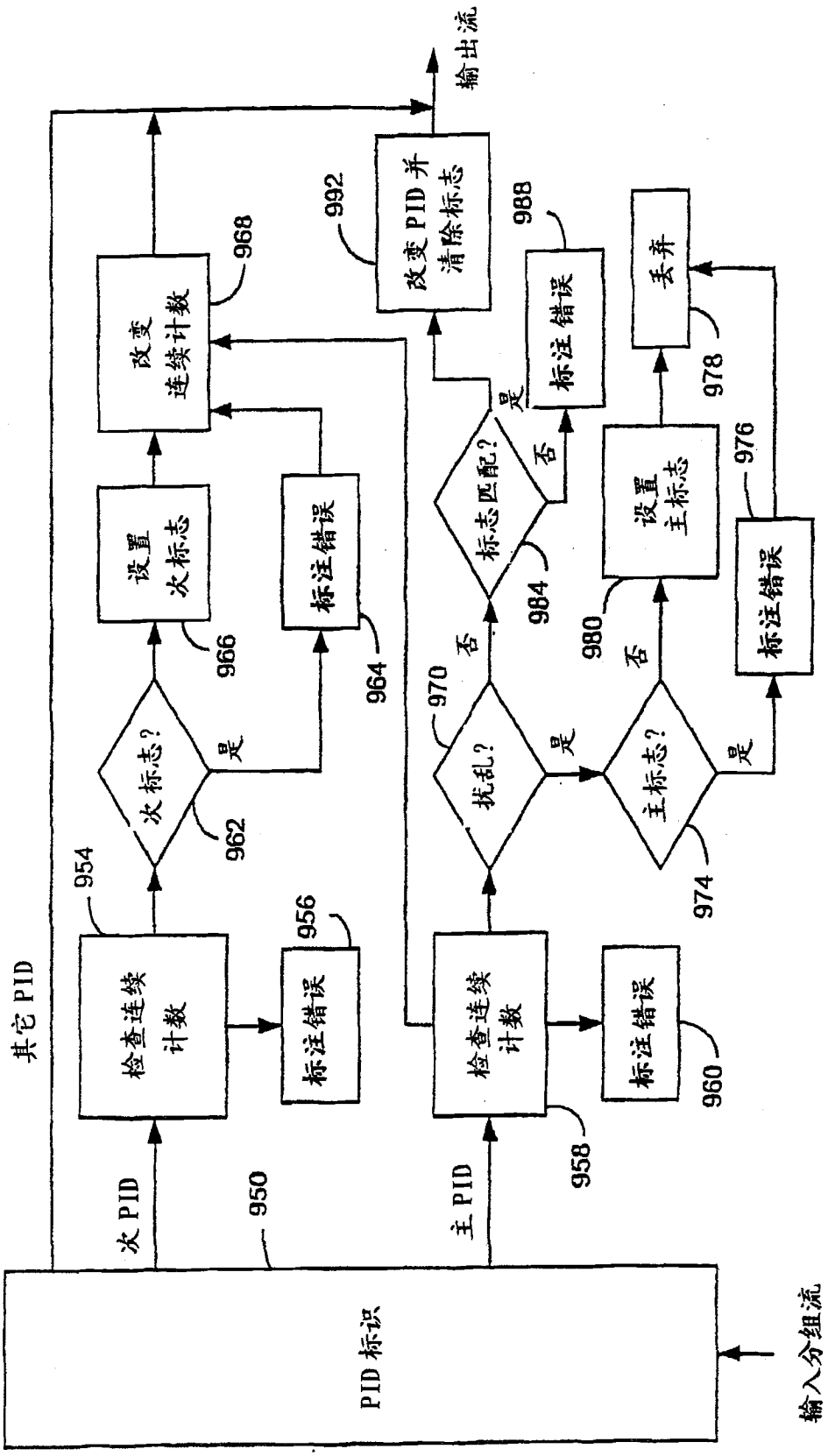

输入分组流
PID 标识
次 PID
主 PID
其它 PID
950
检查连续计数
954
标注错误
956
检查连续计数
958
标注错误
960
次 标志?
962
是
否
标注错误
964
设置次标志
966
改变连续计数
968
扰乱?
970
是
否
检查连续计数
标注错误
主标志?
974
是
否
设置主标志
980
丢弃
978
标注错误
976
标志匹配?
984
是
否
标注错误
988
改变 PID 并清除标志
992
输出流

图 17

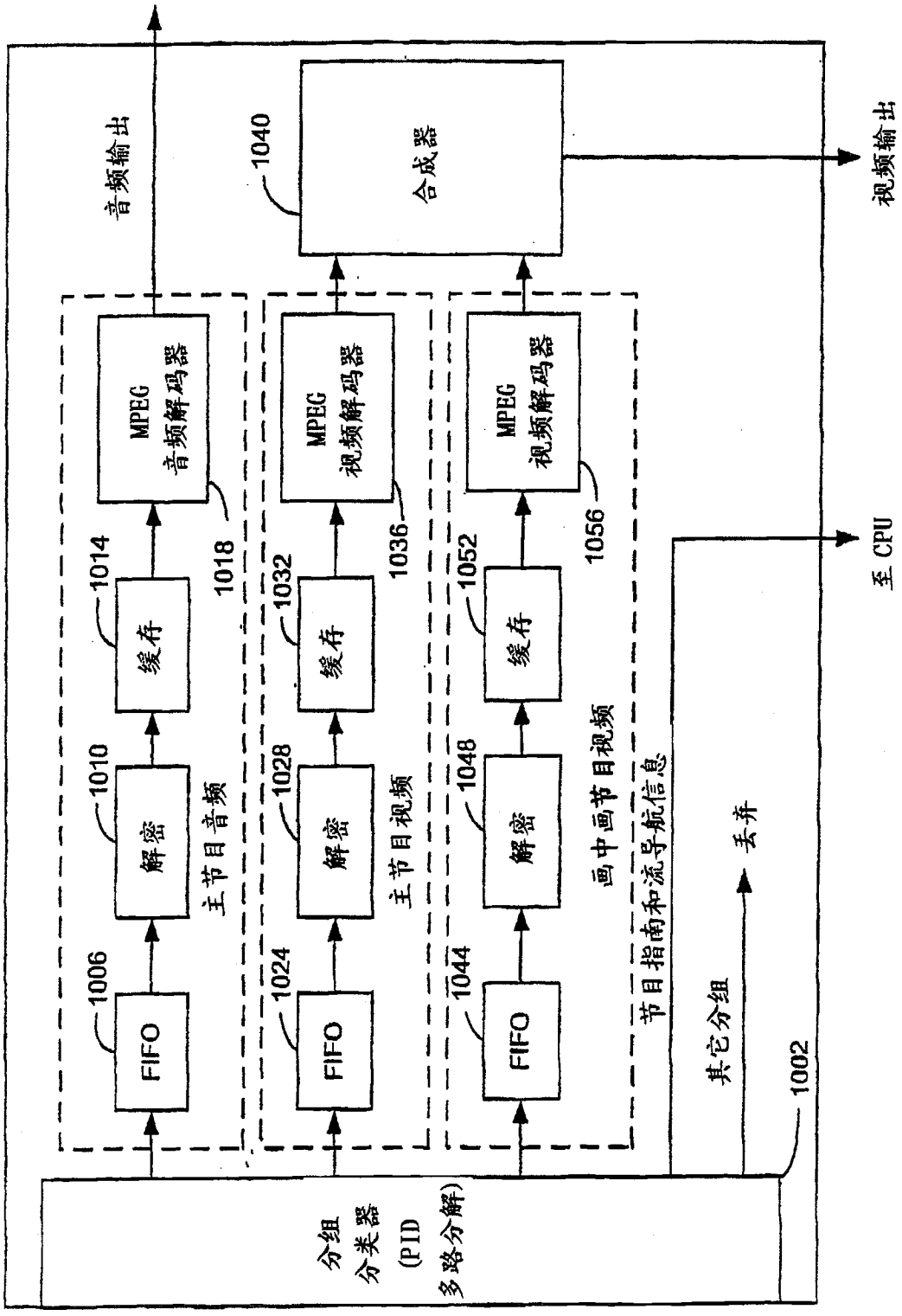

音频输出
1040
合成器
视频输出
MPEG 音频解码器
MPEG 视频解码器
MPEG 视频解码器
1014
1018
1032
1036
1052
1056
缓存
缓存
缓存
1010
1028
1048
解密
解密
解密
主节目音频
主节目视频
画中画节目视频
1006
1024
1044
FIFO
FIFO
FIFO
节目指南和流导航信息
至 CPU
其它分组
丢弃
1002
分组分类器 (PID 多路分解)

图 18