(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 101040265 B
(45)授权公告日 2014.05.07

(21)申请号 200580035237.2
(22)申请日 2005.10.18
(30)优先权数据
10/968,741 2004.10.19 US
(85)PCT国际申请进入国家阶段日
2007.04.16
(86)PCT国际申请的申请数据
PCT/US2005/037178 2005.10.18
(87)PCT国际申请的公布数据
WO2006/044749 EN 2006.04.27
(73)专利权人 晶像股份有限公司
地址 美国加利福尼亚州
(72)发明人 D·J·诺斯卡特 黄承浩
J·D·莱尔 J·G·汉科
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 钱慰民
(51)Int.Cl.
G06F 11/30(2006.01)
H04L 9/32(2006.01)
(56)对比文件
US 2002/0136406 A1,2002.09.26,说明书第3页第0042段,第4页第0053段至第0057段,第6页第0072段至第7页第0074段、附图10,11,15.
US 2002/0136406 A1,2002.09.26,说明书第3页第0042段,第4页第0053段至第0057段,第6页第0072段至第7页第0074段、附图10,11,15.
US 2002/0136406 A1,2002.09.26,说明书第3页第0042段,第4页第0053段至第0057段,第6页第0072段至第7页第0074段、附图10,11,15.
审查员 郑嘉青

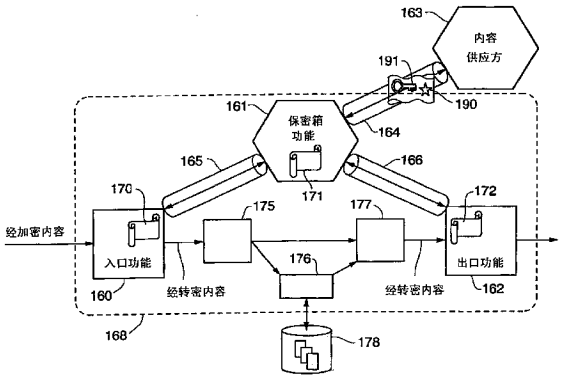
权利要求书2页 说明书56页 附图17页

(54)发明名称

个人数字网络环境中的内容保护的方法和装置

(57)摘要

在一些实施例中,本发明是一种个人数字网络("PDN"),它包括被配置成转加密进入该PDN的经加密内容的硬件(有时称为入口电路)。通常,转加密(解密然后重新加密)是在入口电路内的硬件中执行的,并且重新加密在经解密内容可由入口电路外部的硬件或软件访问之前进行。通常,离开入口电路的经转加密内容在PDN内在各集成电路之间传送或可通过软件容易地访问时总是保持经重新加密的形式,直至其在用于显示或回放或从该PDN输出的硬件(有时称为出口电路)内被解密。通常,PDN被实现为使入口或出口电路中没有任何机密(供入口或出口电路使用或由其传送)能以未加密的形式为该PDN内的软件或固件、或由该PDN外部的任何实体所访问。本发明的其它方面有保护PDN(例如,开放式计算系统)中的内容的方法、以及在PDN中使用的设备(例如,多媒体图形卡、机顶盒或视频处理器等)。



CN 101040265 B

1. 一种个人数字网络，包括：

至少一个入口节点，被配置成执行授权操作以响应所述入口节点的保密箱电路接收一个或者多个机密值，其中所述授权操作包括在所述入口节点的硬件中以安全方式转加密进入所述个人数字网络的内容，由此生成受控内容，所述入口节点的所述保密箱电路被配置以与另一保密箱电路交换机密值；

至少一个出口节点，被配置成执行授权操作以响应所述出口节点的保密箱电路接收一个或者多个机密值，其中所述授权操作包括在所述出口节点内的硬件中以安全方式将所述受控内容解密，由此生成所述内容的明文版本，并将所述内容的明文版本的经处理版本向所述个人数字网络之外的实体、显示设备、以及回放设备中的至少一个断言，所述出口节点的所述保密箱电路被配置以与所述入口节点的保密箱电路交换机密值；以及

包含保密箱电路的第三节点，其中所述第三节点的保密箱电路被配置成存储许可证书数据以及至少一个所述入口节点和至少一个所述出口节点执行授权操作所需的至少一个机密值，所述第三节点传送许可证书数据到所述出口节点，其中所述内容及所述机密值均不以明文形式出现在所述个人数字网络除安全子系统内之外的任何地方。

2. 如权利要求 1 所述的个人数字网络，其特征在于，所述入口节点是一包含执行固件的至少一个微处理器的集成电路，所述出口节点是另一包含执行固件的至少一个微处理器的集成电路，并且所述入口节点、所述出口节点和所述第三节点的保密箱电路都不包含被配置成执行软件的可编程处理器。

3. 如权利要求 1 所述的个人数字网络，其特征在于，所述入口节点被配置成转加密进入所述个人数字网络的经加密内容以使所述明文形式的内容不可为所述入口节点之外的硬件或软件访问。

4. 如权利要求 1 所述的个人数字网络，其特征在于，还包括：

至少一个设备，该设备耦合以接收所述受控内容并向所述出口节点断言所述受控内容和所述受控内容的经处理版本中的至少一个。

5. 如权利要求 4 所述的个人数字网络，其特征在于，所述设备是数据存储单元。

6. 如权利要求 4 所述的个人数字网络，其特征在于，所述设备是视频处理器。

7. 如权利要求 1 所述的个人数字网络，其特征在于，所述个人数字网络被配置成没有任何出现在所述第三节点的保密箱电路、所述入口节点和所述出口节点中的任一个中供所述第三节点的保密箱电路、所述入口节点和所述出口节点中的任一个使用或向其传送的机密值以未加密形式在所述第三节点的保密箱电路、所述入口节点和所述出口节点中的任一个之间发送，并且没有任何机密值以明文形式为所述个人数字网络内的软件或所述个人数字网络之外的任何实体所访问。

8. 如权利要求 7 所述的个人数字网络，其特征在于，所述个人数字网络被配置成没有任何机密值可为在所述个人数字网络的任何元件上运行的固件所访问，并且没有任何机密值以明文形式出现在所述个人数字网络内除安全硬件内之外的任何地方。

9. 如权利要求 1 所述的个人数字网络，其特征在于，每个所述入口节点被配置成仅对所述内容执行授权操作，每个所述出口节点被配置成仅对所述受控内容执行授权操作，并且每个所述入口节点和每个所述出口节点在执行任何所述授权操作之前将向所述第三节点的保密箱电路要求至少一个机密值。

10. 如权利要求 9 所述的个人数字网络，其特征在于，所述第三节点的保密箱电路被配置成除非该第三节点的保密箱电路已确定所述出口节点被授权执行由所述机密值允许所述出口节点执行的每个操作，否则不向所述出口节点提供任何所述机密值。

11. 如权利要求 9 所述的个人数字网络，其特征在于，所述第三节点的保密箱电路被配置成除非该第三节点的保密箱电路已根据与所述出口节点的认证交换的结果确定所述出口节点被授权执行由所述机密值允许所述出口节点执行的每个操作，否则不向所述出口节点提供任何所述机密值。

12. 如权利要求 9 所述的个人数字网络，其特征在于，所述第三节点的保密箱电路被配置成除非该第三节点的保密箱电路已确定所述入口节点被授权执行由所述机密值允许所述入口节点执行的每个操作，否则不向所述入口节点提供任何所述机密值。

13. 如权利要求 9 所述的个人数字网络，其特征在于，所述第三节点的保密箱电路被配置成除非该第三节点的保密箱电路已根据与所述入口节点的认证交换的结果确定所述入口节点被授权执行由所述机密值允许所述入口节点执行的每个操作，否则不向所述入口节点提供任何所述机密值。

14. 如权利要求 1 所述的个人数字网络，其特征在于，所述入口节点的保密箱电路被配置成通过所述入口节点与所述第三节点的保密箱电路之间的至少一个安全通道与所述第三节点的保密箱电路交换机密值，并且所述出口节点的保密箱电路被配置成通过所述出口节点与所述第三节点的保密箱电路之间的至少一个安全通道与所述第三节点的保密箱电路交换机密值。

个人数字网络环境中的内容保护的方法和装置

[0001] 相关申请的参照

[0002] 本申请是于2003年10月3日提交的题为“Method and Apparatus for Content Protection Within an Open Architecture System(开放式架构系统内的内容保护的方法和装置)”的待批美国专利申请No.10/679,055的继续申请,并要求于2003年1月13日提交的题为“Method and Apparatus for Content Protection Within an Open Architecture System (开放式架构系统内的内容保护的方法和装置)”的美国临时申请No.60/439,903的优先权。

技术领域

[0003] 本发明涉及个人数字网络(“PDN”)环境中的内容保护的方法和装置。PDN的一个示例是安装在用户家中的包括数字视频(及音频)存储、回放和处理设备以及用于与这些设备通信或控制这些设备的个人计算机的网络。根据本发明,进入PDN的经加密内容(例如,高清晰度数字视频)在硬件中被安全地转加密(transcrypt,解密并重新加密)(除非该内容在进入该PDN时已用所需格式加密)。该内容随后在该PDN内(例如,其在各集成电路之间传送或者可通过软件或未授权实体容易地访问时总是)保持为此经转加密的形式,直至它在用于呈现(即,显示和/或回放)的硬件内被再次安全地解密(以及可任选地在该硬件中进行其它的处理)以供在该PDN外部使用。在典型的实施例中,用于所接收内容的转加密或是经加密内容的解密的机密(例如,密钥数据或证书)均不可由PDN内部或外部的软件访问(以明文形式)。这显式地排除通过PDN的组件内任何形式的软件对机密信息的访问。

背景技术

[0004] 这里的表述“使用限制集”(或“Use Restriction Set”)是指(特定类型的)内容应受的所有使用限制的集合。针对特定内容的使用限制集可包括任意数目的使用限制(例如,一个使用限制或多个使用限制)。例如,对于定义了一部电影的视频和音频数据的使用限制集可阻止将该数据传送到指定位置(例如,单个设备或网络)以外而不禁止在该位置内对该数据的任何使用。又如,对于定义了一部电影的视频和音频数据的使用限制集可阻止除在指定位置处单纯观看该电影(单纯观看该视频数据并回放相应的音频数据)(例如,单纯通过特定设备或指定类型的设备集观看和回放,或是单纯通过指定网络的任何设备观看和回放)以外对该数据的所有使用。

[0005] 本发明涉及个人数字网络环境中的内容保护的方法和装置,其中“个人数字网络环境”(“PDNE”)是指由“个人数字网络”定义的环境。这里的表述“个人数字网络”(“PDN”)是指能够接收受使用限制集约束的内容(例如,数字图像数据、视频数据或音频数据)、并被配置成以不为该使用限制集所禁止的至少一种方式(以及可任选地,以多种或所有方式)使用该内容的(各自由硬件以及可任选地还有软件或固件的某种组合构成的组件的)网络。PDM的一个示例是安装在网络用户家中的网络,它包括数字视频(及音频)存储、呈现(即,显示或回放)和处理设备、以及能够与此类设备通信或控制此类设备的个人计算机(或具有开

放式架构的其它计算系统)。简单PDN的一个示例是具有被配置成接收经加密视频和音频内容(例如,通过从高清晰度DVD或其它盘读取该内容)以及显示该内容的视频部分并回放该内容的音频部分的开放式架构(例如,具有外围设备的个人计算机)的计算系统。进入PDNE的内容可以是视频或音频数据但并非必须如此,并且可以是指示可被数字地存储的任何信息(诸如但不限于图片、文本、游戏、财务记录、以及个人信息)的数据或包括此类数据。

[0006] PDN可以(但并非必须)是家庭娱乐网络或包括家庭娱乐网络。例如,可在商务环境中或其它地方实现PDN,以保护财务数据或其它既非数字视频、亦非数字音频的内容。

[0007] 尽管PDN可包括个人计算机,但是并非必须要有一个人计算机。例如,PDN可以是并非个人计算机但本质上是同等级家用电器(例如,音频/视频接收机、盘播放器、和/或记录/回放单元)的设备的集合,并且网络管理功能可被分布在此类设备间而无需集中的主控制器。网络管理功能的分布在诸如(例如)需要或期望从PDN的任意设备(或多个设备中的任一个)执行必要的网络管理功能的情形中常常是合乎需要的。

[0008] 具有开放式架构的计算系统(这里有时称为“开放式架构系统”或“开放式系统”)是被配置成允许终端用户方便地添加或移除硬件组件和/或软件模块的计算系统。应当注意,家用电器可与个人计算机共有设计和实现特征,这两类设备之间的区别由其用户可见的接口和功能定义。

[0009] 这里的表述“视听子系统”(或“视听系统”)有时用来指能够响应于视频数据显示图像和/或响应于音频数据发出声音的系统或设备。视听子系统通常通过某种形式的串行链路耦合到PDN。视听系统的示例包括:HDTV监视器(包括能够将通过HDMI链路接收的经HDCP加密视频和音频数据解密的HDMI接收器)、扬声器、数字录像机(DVR)、以及音频/视频处理器。

[0010] 在本发明的典型实施例中,进入PDN的内容可在该PDN内以不与由涉及该内容的知识产权的所有者(或许可人)所设置的限制相冲突的任何方式(例如,以不违反该PDN的用户或所有人合法获取该内容所遵循的协议条款的任何方式)来使用。例如,一PDN能够接收定义一部电影的加密视频和音频数据的卫星传送,并且对于该数据的使用限制集可阻止除解密该数据、以及由该PDN的任何一个或多个设备在指定时段(例如,特定的一天或一周)内对该电影任意次数的观看(即,对该视频数据和/或相应的音频数据任意次数的回放)、或是(由该PDN的任意一个或多个设备)对该电影最多达最大可允许观看次数的任意次数的观看以外对该数据的所有使用。本发明的优选实施例允许进入PDNE的内容通过该PDN的设备解密、复制、存储、显示和/或回放,并在该PDN的各设备之间传送,只要对于该内容的使用限制集不禁止此类使用即可。

[0011] 根据本发明的典型实施例,对于由一PDN接收的内容的使用限制集由在进入该PDNE时与该内容相关联的数据(本文中有时称为“权限数据”或“许可使用数据”或“许可使用标志”)指示,并且此关联根据映射到该使用限制集的基本规则集在该内容于该PDNE内的整个存在期间得到安全地维持。

[0012] 这里的表述经加密数据(根据第一协议加密的数据)的“转加密”是指将该经加密数据解密,接着根据第二协议重新加密该经解密数据,所有这些都是在物理安全的设备或系统(例如,PDN的物理安全子系统)内执行的,从而这些数据在该设备之外决不可以未加密形式访问。第二协议通常与第一协议不同,但也可与第一协议相同(例如,如果使用了与

执行原始加密所使用的密钥不同的密钥来执行重新加密)。根据本发明,只要有经加密内容从另一域(例如,从诸如有线或卫星传送系统等安全传输域,或从类 DVD 盘分发机构)进入 PDNE 就执行转加密,除非该内容在进入该 PDNE 时就已用所需格式加密。

[0013] 现代的个人计算机(PC)已经从严格的计算设备进化成通信和娱乐设备。结果,用户期望能够在其 PC 上观看包括正片长度电影在内的预先录制的视频娱乐。此外,性能提高了的处理器使得在 PC 的处理器上使用软件来例如解码和播放 DVD 电影显得有利。但是,娱乐知识产权(例如,电影版权)的所有者当然关心在相关内容进入这样的 PC 时对其产权的未授权使用和复制。

[0014] 预期内容的消费者将组装 PDN (每个 PDN 可包括但常常并不包括至少一台 PC),并且内容供应商将在了解进入每个 PDN 的内容将在该 PDN 内以不被该内容的知识产权所有者(或许可人)禁止的任何方式使用的情况下将内容提供给 PDN。但是,此类知识产权的所有者当然关心在相关内容进入 PDN 时对其产权的未授权使用和复制。这是因为 PC 的开放式系统特性使取得高价值内容(诸如音乐或影片)并将拷贝分发给不具有该相关高价值知识产权所有人许可的数不清的用户以访问此内容轻而易举。

[0015] 不幸的是,正是由于软件解码(无论是在开放式还是在封闭式系统设备实现中)的这一特性,内容在采用软件来解密内容的常规 PDNE 中不能被有效地保护。在软件解码过程期间的某一点,密钥和经解密内容(例如,明文的视频和音频数据)在该设备的寄存器和 / 或存储器内均可用,因此无需相关知识产权所有人的许可即可制作并分发这些密钥和内容的未授权拷贝。

[0016] 如果可制作并经由例如因特网来广为分发电影或其它作品的高质量拷贝,则此类内容的知识产权对于所有者而言迅速失去其价值。为了保护一些此类内容,创建了内容加扰系统(CSS)来为 DVD 加密视频内容。CSS 是在原始的原视频数据的 MPEG 压缩版本之上使用的密码加扰机制。能够播放 DVD 内容的每个设备必须具有允许该内容被解扰(即,解密)的一个或多个密钥。

[0017] 封闭式系统(例如,独立 DVD 播放器或其它独立的家用电器设备)若被配置成使密钥和经解密内容停留在该封闭式系统内,则可提供可观的内容保护。如果密钥和经解密内容均停留在该封闭式系统内,则没有“破解”该内容保护方法的简单方法。“封闭式”系统(例如,独立 DVD 播放器)不提供由用户添加或移除硬件或软件的方式。由此,要确保密钥以不被泄露到该封闭式系统之外的方式在该封闭式系统内存储和使用是相对简单的。值得注意的是,即使是预期封闭的系统也可能与开放式系统受相同弱点之苦。例如,如果使用类似于 PC 的由软件处理密钥的架构来实现有线或卫星机顶盒(STB),则该软件可能被修改从而会使此机密素材泄密。

[0018] 但是,封闭式系统内对内容的保护带来了其它问题。例如,如何将密钥和内容安全地传递给封闭式系统? 如果密钥和内容走同一路径,则存在流向封闭式系统的阻碍良好认证方法的使用的固有单向信息流。本发明优选实施例的一个重要方面是这些实施例允许(但不要求)密钥和内容在 PDN 内、甚至在 PDN 内的一内容处理集成电路(例如,本发明的入口或出口节点的集成电路实施例)内走不同路径。本发明的这些实施例可通过确保密钥构造素材决不会对软件直接可见来使密钥分发和管理比在常规的封闭式或开放式系统中安全得多。这是由于这样的事实 :集成电路提供由于其封装所固有的物理安全性而比在软

件实现中可达到的高得多的安全度，提供对要从中提取信息所需的少有且昂贵的设备的大得多的投资，并提供可采取的保护机密信息的手段。此外，因为此方法允许实现验证一设备(例如，PDN 的一封闭式子系统)被正当地许可并被允许使用内容(受对于该内容的使用限制集约束)的更佳方法，所以更为安全。本发明提高了封闭式和开放式系统两者中的内容保护的当前技术水平。

[0019] 当前标准清晰度的 DVD 内容可在是开放式系统而非封闭式系统的 PC 上用软件解码。在该软件解码过程期间的某一点，CSS 密钥和经解密视频内容在该 PC 的寄存器和 / 或存储器内均可用。因为，在 PC 中，用户可有意或无意地加载恶意程序或驱动程序，并且此类模块可获得对这些密钥和 / 或内容的访问，CSS 保护容易被规避。事实上，进行了两种广泛公开的攻击。第一，通过对该软件模块进行反向工程而找到用于 Xing 软件解码器的 CSS 密钥，并且此密钥在黑客间交易。另外，称为 DeCSS 的 CSS 解密程序被创建并分发。

[0020] 迄今为止，内容保护系统的这些破坏的经济损害还有限，因为标准清晰度视频的图像质量比剧场质量要低得多。亦即，原始电影的许多本征值在从原始高清晰度到标准的电视清晰度的转换中被丢失。此外，直到最近，要在用户之间传送如经解密电影等大文件还是不实际的。

[0021] 如今，高清晰度电视(HDTV)已经变得越来越普及，并且有望在若干年里取代标准清晰度电视。为了向消费者提供足够质量的预先录制的素材，正在设计 HDTV DVD(HD-DVD)。与在标准 DVD 播放器的情形中一样，带有类似 CSS 的 HD-DVD 用独立播放器应当提供强大的内容保护。

[0022] 但是，在常规的开放式系统或其它常规 PDN 内解码内容(例如，HD-DVD 内容)会产生弱点。此弱点常常称为内容保护系统中的“软件漏洞”。“软件漏洞”弱点的本质在于，如果开放式系统(或 PDN 的其它元件)内的软件操纵未加密密钥或明文内容，则这些密钥或内容很容易泄漏供未授权使用。例如，如果采用以软件编程的开放式计算系统来解密内容，则密钥和解密程序均必须为处理器可见，并因此为该系统内所加载的其它潜在恶意软件可见。该软件漏洞是个严重的问题，因为如果可制作二进制数据(指示视听内容)的未授权拷贝，则这些拷贝将允许以本质上与原始剧院版本相同的质量来显示和回放该内容。此外，现代的网络技术将容易地允许电影拷贝的类 Napster 交易。结果，知识产权的所有者将很快发现该产权变得毫无价值。

[0023] 当起初使用标准 DVD 的软件解密时，“软件漏洞”还没有被完全理解。解密软件内的密钥被隐藏并被认为是安全的。当 Xing 密钥被提取时，这种“通过隐藏实现的安全”很快显示是虚假的。从那时起，计算机产业的许多努力都是针对存储解密密钥的安全方法(例如，Microsoft Palladium Initiative，后来重命名为Next Generation Secure Computing Base)。但是，尽管这使得窃取密钥更具有挑战性，但是它本质上没有提高密钥的安全性，并且没有为保护内容做任何事。注意，如果授权播放器无需手动干涉(例如，用户输入解密内容保护密钥所需的口令)即可获得密钥，则使用同一过程或算法的任何其它程序也能获得该密钥。如果这一程序是以恶意方式编写的，则该密钥可例如在数秒里通过因特网被发送给数以百万计的其他人。类似地，因为软件解码器要求密钥和解密过程或算法为处理器可见，所以它可被攻击者观察到并仿效，由此导致该内容未经授权的解密。

[0024] 以上引述的美国专利申请 No.10/679,055 记载了通过在开放式系统内的封闭式

子系统中保护内容和密钥两者来避免(开放式系统中的)软件漏洞问题的方法和装置,其中“封闭式子系统”是指不向用户提供向其添加硬件或软件、或从其移除硬件或软件的便利方式的子系统(例如,单个集成电路)。美国专利申请No.10/679,055教示该封闭式子系统应被设计成防止该封闭式子系统中的密钥数据(由该封闭式子系统使用)和未经加密内容在该封闭式子系统外被揭露。

[0025] 美国专利申请No.10/679,055的封闭式子系统可称为被“嵌入”到开放式系统中,并且通常被配置成通过在硬件中解密传入的内容以生成原内容、然后使用不同的内容保护协议(也在硬件中,并且在生成原内容的同一芯片中)重新加密该原内容,而不向该开放式系统中该封闭式子系统之外的任何元素泄漏该原内容来生成被保护的内容。原内容和用于生成或重新加密该原内容的密钥数据均不会泄露给该开放式系统中该封闭式子系统之外的任何元素。该封闭式子系统可被配置成直接向外部系统(该开放式系统外部的系统)断言经重新加密的内容。该外部系统可包括密码设备,并且该封闭式子系统可被配置成按需向该密码设备公开密钥数据(例如,作为验证操作的一部分)以允许该密码设备将该经重新加密的内容解密。或者,从该封闭式子系统通过该开放式系统的至少一个其它元素向外部系统断言该经重新加密的内容(例如,该经重新加密的内容通过该开放式系统被“隧穿”到该外部系统)。

[0026] 向显示设备发送视频内容的业界趋势是将该内容以数字形式通过串行链路来传递。

[0027] 各种用于发送经加密或未经加密数据的串行链路是公知的。主要用于家用电器(例如,用于视频数据从机顶盒向电视机的高速传送)或用于视频数据从主机处理器(例如,个人计算机)向监视器的高速传送的一种常规串行链路称为跳变最小化差分信令接口(“TMDS”链路)。TMDS链路的特性包括以下:

[0028] 1.视频数据被编码,然后作为已编码字被传送(在传送之前,数字视频数据的每个8位字都被转换到已编码的10位字);

[0029] a.该编码确定一组“频带内”字和一组“频带外”字(编码器可响应于视频数据仅生成“频带内”字,尽管它也可响应于控制或同步信号生成“频带外”字。每个频带内字是由一个输入视频数据字的编码所产生的已编码字。在该链路上传送的所有非频带内字为“频带外”字);

[0030] b.视频数据的编码以使频带内字跳变最小化的方式执行(频带内字序列具有减少或最小化数目的跳变);

[0031] c.视频数据的编码以使频带内字DC平衡的方式执行(该编码防止用于传送频带内字序列的每个传送电压波形偏离基准电势大于预定阈值。具体而言,每个“频带内”字的第10位指示其它9位中的8位是否在编码过程期间反转,以校正先前编码的数据位流中1和0的流动计数之间的失衡);

[0032] 2.该已编码视频数据和视频时钟信号被作为差分信号传送(该视频时钟和经编码视频数据被作为差分信号通过导体对传送);

[0033] 3.采用三个导体对来传送该经编码视频,并且采用第4导体对来传送视频时钟信号;以及

[0034] 4.信号传送在一个方向上从发送器(通常与台式或便携式计算机或其它主机相关

联）到接收器（通常是监视器或其它显示设备的元素）进行。

[0035] TMDS 串行链路的一个用途是数字显示工作组采用的“数字可视接口”（“DVI”链路）。DVI 链路可被实现为包括两条 TMDS 链路（共用一公共导体对来传送视频时钟信号）或一条 TMDS 链路，以及发送器与接收器之间附加的控制线。DVI 链路包括发送器、接收器、以及发送器与接收器之间以下的导体：4 个导体对（通道 0、通道 1、和通道 2 用于视频数据，而通道 C 用于视频时钟信号）；显示数据通道（“DDC”）线，用于发送器和与接收器相关联的监视器之间根据常规显示数据通道标准（视频电子标准协会的“显示数据通道标准”，版本 2.0，1996 年 4 月 9 日）的双向通信；热插拔检测（HPD）线（监视器在其上发送使与该发送器相关联的处理器能标识该监视器的存在的信号）；模拟线（用于向接收器发送模拟视频）；以及电源线（用于向接收器和与该接收器相关联的监视器提供 DC 电源）。显示数据通道标准规定发送器和与接收器相关联的监视器之间的双向通信协议，包括由监视器发送规定显示器的各种特性的扩展显示标识（“EDID”）消息，以及由发送器发送对监视器的控制信号。

[0036] 另一种串行链路是由 Silicon Image 有限公司、松下电子、皇家飞利浦电子、索尼公司、Thomson Multimedia、东芝公司和日立开发的“高清晰度多媒体接口”（有时称为“HDMI”链路或接口）。

[0037] 如今使用称为“高带宽数字内容保护（“HDCP”）协议”的密码协议来加密要通过 DVI 或 HDMI 链路传送的视频、并在 DVI（或 HDMI）接收器处将该数据解密是惯常的做法。HDCP 协议在 Intel 公司 2000 年 2 月 17 日的文献“High-bandwidth Digital Content Protection System（高带宽数字内容保护系统）”修订版 1.0、以及 Intel 公司 2001 年 3 月 19 日的文献“High-bandwidth Digital Content Protection System Revision1.0Erratum（高带宽数字内容保护系统修订版 1.0 勘误）”中记载。这两个文献的全文援引包含于此。

[0038] 实现 HDCP 协议的 DVI 顺应（或 HDMI 顺应）发送器在每个活动周期（即，当 DE 为高时）断言一伪随机生成的称为 cout[23:0] 的 24 位字流。在 DVI 顺应系统中，每个活动周期是一活动视频周期。在 HDMI 顺应系统中，每个活动周期是发送视频、音频或其它数据的周期。cout 数据的每个 24 位字与输入到该发送器的 RGB 视频数据的 24 位字“异或”（在该发送器的逻辑电路中），以将该视频数据加密。经加密的数据随后被编码（根据 TMDS 标准）以供传送。在接收器中也生成相同的 cout 字序列。在接收器处接收的已编码的经加密数据进行 TMDS 解码之后，cout 数据在逻辑电路中与该已解码视频被一并处理，以将该已解码数据解密并恢复原始的输入视频数据。

[0039] 在发送器开始发送经 HDCP 加密的已编码视频数据之前，发送器和接收器彼此双向通信以执行一认证协议（为验证该接收器被授权接收受保护内容，并建立供输入数据加密和已发送的经加密数据解密时使用的共有机密值）。更具体地，发送器和接收器各自用称为密钥选择矢量的 40 位字以及 40 个 56 位私钥的阵列预编程（例如，在工厂中）。为发起发送器与接收器之间的认证交换的第一部分，发送器向接收器断言其密钥选择矢量（称为“AKSV”）以及伪随机生成的会话值（“An”）。响应于此，接收器将其密钥选择矢量（称为“BKSV”）和转发器位（指示接收器是否为转发器）发送给发送器，并且接收器还实现使用“AKSV”和接收器的 40 个私钥的阵列来计算机密值（“Km”）的预定算法。响应于来自接收器的“BKSV”值，发送器实现与接收器相同的使用该“BKSV”值和发送器的 40 个私钥的阵列来计算同一机密值（“Km”）的算法。

[0040] 发送器和接收器随后各自使用共有的“Km”值、会话值“An”和转发器位来计算共有机密值(会话密钥“Ks”)、在确定认证是否成功时使用的值(“R0”)和在该认证交换的第二部分期间使用的值(“M0”)。仅在转发器位指示该接收器是一转发器的情况下才执行认证交换的第二部分,以确定耦合到该转发器的一个或多个下游设备的状态是否要求接收器认证的撤消。

[0041] 在认证交换的第一部分之后,并且(如果执行该认证交换的第二部分)如果作为认证交换的第二部分的结果,接收器的密钥选择矢量没有被撤消,则发送器和接收器各自生成一个 56 位帧密钥 Ki(用于发起视频数据帧的加密或解密)、初始化值 Mi、以及用于链路完整性验证的值 Ri。Ki、Mi 和 Ri 值响应于在发送器的适当电路处接收的控制信号(在图 1 中标示为“ctl3”)而生成,并且还在每个垂直消隐周期,即当 DE 为低时由发送器发送给接收器。如图 1 的时序图中所示,控制信号“ctl3”是单个高走脉冲。响应于 Ki、Mi 和 Ri 值,发送器和接收器各自生成伪随机生成的 24 位字序列 cout[23:0]。由发送器生成的 cout 数据的每个 24 位字与视频数据帧的一个 24 位字“异或”(在发送器的逻辑电路中)(以将该视频数据加密)。由接收器生成的 cout 数据的每个 24 位字被与经加密视频数据的第一接收帧的一个 24 位字“异或”(以将此经加密视频数据解密)。由发送器生成的 24 位字 cout[23:0] 是内容加密密钥(用于加密一行输入视频数据),而由接收器生成的 24 位字 cout[23:0] 是内容解密密钥(用于解密所接收的和已解码的一行经加密视频数据)。

[0042] 在控制信号 ctl3 的断言之后的每个水平消隐周期(响应于数据使能信号 DE 的每个下降沿)期间,发送器执行密钥重新编制操作,并且接收器执行相同的密钥重新编制操作以更改(以预定方式)要在下一活动视频周期断言的 cout 数据字。这一直持续到下一垂直消隐周期,即控制信号 ctl3 再次被断言以致使发送器和接收器各自计算新的一组 Ki 和 Mi 值(响应于控制信号 ctl3 的每次断言,索引“i”增 1)。Ri 值每 128 帧更新一次。输入视频数据的实际加密或所接收的已解码视频数据的实际解密(或在 HDMI 顺应系统的情形中对输入视频、音频或其它数据的加密、或所接收的已解码视频、音频或其它数据的解密)是仅当 DE 为高时(不是在垂直或水平消隐间隔期间)才使用响应于最新的一组 Ks、Ki 和 Mi 值生成的 cout 数据字来执行的。

[0043] 发送器和接收器各自包括图 2 中所示类型的 HDCP 密码电路(本文中有时称为“HDCP 密码”)。HDCP 密码包括线性反馈移位寄存器(LFSR)模块 80、耦合到 LFSR 模块 80 的输出端的分组模块(block module)81、以及耦合到分组模块 81 的输出端的输出模块 82。LFSR 模块 80 被用来响应于使能信号(图 2 中所示的信号“ReKey”)的每次断言来使用会话密钥(Ks)和当前帧密钥(Ki)对分组模块 81 重新编制密钥。分组模块 81 在会话开始时生成(并向模块 80 提供)密钥 Ks,并在每个视频数据帧开始时(响应于在帧的第一垂直消隐间隔里发生的控制信号“ctl3”的上升沿)生成(并向模块 80 应用)密钥 Ki 的新值。信号“ReKey”在 DE 信号的每个下降沿(即,在每个垂直和每个水平消隐间隔开始时)、以及在信号“ctl3”的每个上升沿之后的短暂初始化周期(模块 81 在此期间生成帧密钥 Ki 的更新值)被断言到图 2 的电路。

[0044] 模块 80 包含 4 个线性反馈移位寄存器(具有不同长度)和耦合到这些移位寄存器的组合电路,该组合电路被配置成在 DE 为低(即,在每行视频数据的水平消隐间隔里)时在从信号“ReKey”的每次断言开始的固定数目时钟周期(例如,56 个周期)的每个周期期间向

分组模块 81 断言每个时钟间隔单个输出位。此输出位流由分组模块 81 用来就在每行视频数据的发送或接收开始之前对它自己重新编制密钥。

[0045] 分组模块 81 包含两半，即图 3 中所示的“轮函数（round function）K”和“轮函数 B”。轮函数 K 包括如图所示地连接的 28 位寄存器 Kx、Ky 和 Kz、在图 3 中统一标示为“S 盒 K”的 7 个 S 盒（每个 4 输入位 4 输出位 S 盒包括一张查找表）、以及线性变换单元 K。轮函数 B 包括如图所示地连接的 28 位寄存器 Bx、By 和 Bz、在图 3 中统一标示为“S 盒 B”的 7 个 S 盒（每个 4 输入位 4 输出位 S 盒包括一张查找表）、以及线性变换单元 B。轮函数 K 和轮函数 B 在设计上是相似的，但是轮函数 K 响应于 LFSR 模块 80 的输出每个时钟周期执行一轮分组密码以断言不同的一对 28 位轮密钥（Ky 和 Kz），而轮函数 B 响应于来自轮函数 K 的每个 28 位轮密钥 Ky 和 LFSR 模块 80 的输出每个时钟周期执行一轮分组密码以每个时钟周期断言不同的一对 28 位轮密钥（By 和 Bz）。发送器在认证协议开始时生成值 An，而接收器在认证过程期间对此作出响应。值 An 被用来使会话密钥随机化。分组模块 81 响应于认证值（An）和在每一帧开始时（在控制信号“ctl3”的每个上升沿处）由输出模块 82 更新的初始化值（Mi）来操作。

[0046] 线性变换单元 K 和 B 每个时钟周期各自输出 56 位。这些输出位是每个变换单元中 8 个扩散网络的组合输出。线性变换单元 K 的每个扩散网络响应于寄存器 Ky 和 Kz 的当前输出位中的 7 位生成 7 个输出位。线性变换单元 B 的 4 个扩散网络各自响应于寄存器 By、Bz 和 Ky 的当前输出位中的 7 位生成 7 个输出位，并且线性变换单元 B 的其它 4 个扩散网络各自响应于寄存器 By 和 Bz 的当前输出位中的 7 位生成 7 个输出位。

[0047] 在轮函数 K 中，寄存器 Ky 的 1 位在 ReKey 信号被断言时从由模块 80 断言的位流中取其输入。在轮函数 B 中，寄存器 By 的 1 位在 ReKey 信号被断言时从由模块 80 断言的位流中取其输入。

[0048] 输出模块 82 对在每个时钟周期期间由模块 81 向其断言的 28 位密钥（By、Bz、Ky 和 Kz）（总计 112 位）执行压缩操作，以在每个时钟周期生成一个 24 位伪随机数位块 cout[23:0]。模块 82 的这 24 个输出位各自由如下的 9 项异或而成：(B0*K0)+(B1*K1)+(B2*K2)+(B3*K3)+(B4*K4)+(B5*K5)+(B6*K6)+(B7*K7)，其中“*”表示逻辑与操作，而“+”表示逻辑异或操作。

[0049] 在发送器中，逻辑电路 83（图 2 中所示）接收 cout 数据的每个 24 位字以及每个输入的 24 位 RGB 视频数据字，并且对其执行逐位异或操作以加密该视频数据，由此来生成图 2 中所示的“经加密数据”字。通常，随后该经加密数据在被传送给接收器之前进行 TMDS 编码。在接收器中，逻辑电路 83（图 2 中所示）接收 cout 数据的每个 24 位块以及每个恢复的 24 位 RGB 视频数据字（在所恢复的输入已进行 TMDS 解码之后），并对其执行逐位异或运算以将所恢复的视频数据解密。

[0050] 贯穿本说明书，将使用表述“类 TMDS 链路”来表示能够从发送器向接收器发送已编码数据（例如，已编码数字视频数据），以及可任选地还包括该已编码数据用时钟、并且可任选地还能够在发送器与接收器之间发送（双向或单向地）一个或多个附加信号（例如，已编码数字音频数据或其它已编码数据）的串行链路，这即为 TMDS 链路或具有 TMDS 链路的部分但不是全部特性的链路，或包括这些链路。类 TMDS 链路的示例包括仅因将数据编码为 N 位码字（其中 N 不等于 10，由此这些码字不是 10 位 TMDS 码字）而与 TMDS 链路不同的

链路、以及仅因通过多于或少于三个导体对传送已编码视频而与 TMDS 链路不同的链路。一些类 TMDS 链路使用不同于在 TMDS 链路中使用的专用算法的编码算法将所要传送的输入视频数据(及其它数据)编码成比传入数据包含更多位的已编码字,将已编码视频数据作为频带内字符、并将其它已编码数据作为频带外字符(HDMI 顺应系统根据与对视频数据采用的编码方案不同的编码方案来编码音频数据供传送)来传送。这些字符无需根据其是否满足跳变最小化和 DC 平衡准则被分类成频带内或频带外字符。相反,可使用其它分类准则。不同于 TMDS 链路中使用的编码算法、但可在类 TMDS 链路中使用的编码算法的一个示例是 IBM8b10b 编码。(频带内与频带外字符之间的)分类无需仅基于大或小数目的跳变。例如,频带内和频带外字符各自的跳变数目(在一些实施例中)可在单个范围里(例如,由最小和最大跳变数目定义的中间范围)。

[0051] 这里使用术语“发送器”来广义地表示能够通过链路传送数据、并且可任选地将所要传送的数据编码和 / 或加密的任何单元。这里使用术语“接收器”来广义地表示能够接收通过链路传送的数据(并且可任选地还将所接收的数据解码和 / 或解密)的任何单元。除非另有规定,否则链路可以但并非必须是类 TMDS 链路或其它串行链路。术语发送器可表示执行发送器功能以及接收器功能的收发器。

[0052] 这里的表述“内容密钥”是指可由密码设备用来加密内容(例如,视频、音频或其它内容)的数据、或表示可由密码设备用来将经加密内容解密的数据。

[0053] 这里使用术语“密钥”来表示内容密钥、或是能由密码设备用来生成或者获得(根据内容保护协议)内容密钥的数据。表述“密钥”和“密钥数据”在这里可互换地使用。

[0054] 如这里所使用的术语数据“流”是指所有数据是相同类型、并且被从源传送到目的设备。一数据“流”的所有或部分数据一起可构成单个逻辑实体(例如,电影或歌曲、或其一部分)。

[0055] 这里使用术语“HDCP 协议”来广义地表示常规 HDCP 协议和近似于常规 HDCP 但在一个或多个方面与其不同的经修改的 HDCP 协议。本发明的部分而非所有实施例实现 HDCP 协议。常规 HDCP 协议在活动视频周期期间、而非诸活动视频周期之间的消隐间隔加密(或解密)数据。经修改的 HDCP 协议的一个示例是与常规 HDCP 协议的不同之处仅在于完成诸活动视频周期之间传送的数据的解密(以及在活动视频周期里要传送的视频数据的解密)或完成诸活动视频周期之间要传送的数据的加密(以及在活动视频周期里要传送的视频数据的加密)的所需程度的内容保护协议。

[0056] 作为常规 HDCP 协议的修改版本的 HDCP 协议的一个示例是常规 HDCP 协议基础上的“上游”变形方案(称为“上游”协议)。上游协议的一个版本在 Intel 公司 2001 年 1 月 26 日的 Upstream Link for High-bandwidth Digital Content Protection(高带宽数字内容保护用上游链路)修订版 1.00 (以下称为“上游规范”)中记载。在该上游协议中,“发送器”是以用于实现该上游协议来与图形控制器(该图形控制器起到“接收器”的作用)通信的软件编程的处理器。这一处理器可在根据该“上游”协议执行认证交换之后向图形控制器发送视频数据。该处理器和图形控制器可以是被配置成从图形控制器向显示设备发送经加密视频数据的个人计算机的元件。该图形控制器和显示设备可被配置成执行另一种加密协议(例如,在此上下文中可称为“下游”HDCP 协议的上述常规 HDCP 协议)以允许图形控制器(此时起到“发送器”作用)加密视频数据并将经加密的视频发送给显示设备,并允许显示

设备(起到“接收器”作用)将该经加密数据解密。

[0057] 但是,与本发明形成对比,该上游协议将不会对个人计算机或PDN的处理器中存在的原内容提供足够的保护,该处理器以用于实现该上游协议(处理器起到“发送器”作用)以与起到“接收器”作用的图形控制器通信(并向其发送该原内容)、并允许图形控制器(此时起到“发送器”作用)将该原内容加密并将所得到的经加密内容(根据“下游”HDCP协议)传送给该开放式系统外部的设备(例如,显示设备)的软件编程。

[0058] 在该上游协议中存在若干结构缺陷,并且实现该上游协议的个人计算机或PDN将易受攻击者能访问该个人计算机或PDN内存在的原内容这样的至少一种攻击。这种攻击的一个例子有“man-in-the-middle”攻击,其中上游认证请求(来自图形控制器)被截取并且相应的响应(至图形控制器)被伪造。实现该上游协议的个人计算机由于一个根本原因而易受攻击:这些系统元件中的至少两个(应用和视频驱动程序)是软件形式。它们可被调试、反编译、变更和复制,从而任何结果的“破坏”潜在地将在因特网上迅速和容易地分发。由此,该上游协议根本上是有缺陷的,并且将允许普通技术人员(并且不使用任何特殊硬件或工具)规避预期的HDCP保护。此外,这可能大规模地发生,并且不容易被察觉或抵抗。

[0059] 本发明的各个方面是上面引述的美国专利申请No.10/679,055的教示的概括。本发明的这些及一些其它方面是包括通过避免上述软件漏洞问题来保护PDN中内容的方法和装置。根据本发明的一些方面,用于完成内容解密的明文内容和机密在PDN的硬件(例如,一个或多个集成电路)内受到保护,并且在出现在该PDN中的该硬件以外时总是被加密的。

发明内容

[0060] 在一类实施例中,本发明是一种包括“入口”电路(有时称为入口“单元”)个人数字网络(“PDN”),该“入口”电路被配置成转加密进入该PDN的所有数字内容(例如,高清晰度数字视频或其它视频数据和/或音频数据)(除非该内容在进入该PDN时已用所需格式加密)。该转加密(即,从输入格式解密,接着重新加密成内部PDN格式)是在该入口电路内的硬件中以安全方式执行的,并且重新加密在该经解密内容可通过该入口电路以外的硬件或软件访问或易受其攻击之前进行。该入口电路将不对在进入该PDN时已经是所需加密格式(例如,如果内容分发源使用与由本发明PDN实现的相同的内容保护方法)的内容执行转加密。

[0061] 这里表述“受控内容”有时用来表示包括“经转加密内容”(通过根据本发明转加密内容而生成的内容)、和PDN中的尚未在该PDN中(例如,在该PDN的入口电路中)进行转加密但具有与由该PDN的电路所生成的经转加密内容相同的加密格式的经加密内容(例如,PDN中在进入该PDN时已具有所需加密格式的经加密内容)的一类经加密内容。表述“PDN加密格式”用来表示由PDN的入口电路生成(并从其输出)的经转加密内容的加密格式。在本发明PDN的典型实施例的操作中,PDN的入口电路对内容执行转加密以生成具有PDN加密格式的经转加密内容。在本发明PDN的一些实施例中,PDN的出口电路(后述)对内容执行转加密以生成可(但无需)具有PDN加密格式的经转加密内容。

[0062] 在一类实施例中,PDN中的受控内容(例如,在PDN的入口电路中生成的经转加密内容,或在进入该PDN时已具有PDN加密格式的经加密内容)在该PDN内在各集成电路之间

传送时或者可通过软件或任何其它未授权实体容易地访问时总是保持 PDN 加密格式，直至该受控内容在该 PDN 中的“出口”电路(有时称为出口“单元”)内的硬件中以安全方式解密以供在该 PDN 内消费(例如，显示和 / 或回放)和 / 或从该 PDN 输出。可任选地，出口电路不仅对受控内容执行硬件解密以将该内容变成明文形式，而且还对该明文内容(可以是经压缩的数据)执行附加处理。例如，出口电路可在硬件中格式化并重新加密该明文内容以供在该 PDN 内消费或从该 PDN 输出(例如，至外部视听系统)。例如，该出口电路将把明文内容转换成带 DTCP 加密的常规 IEEE1394 格式，以允许该内容从该 PDN 被导出到外部记录和回放设备。又如，该出口电路可包括用于根据经压缩的明文内容生成原音频和视频数据的 MPEG 音频和视频解压缩硬件、以及用于对该原音频和视频执行 HDCP 加密(以及其它处理)以生成可经由 HDMI 链路安全地传送给接收器的经 HDCP 加密的 HDMI 格式化数据。通常，本发明的 PDN 被实现为使得没有任何存在于入口或出口电路中以供该入口或出口电路使用或传送的机密(例如，在转加密由 PDC 接收的内容的入口电路、或在用于解密受控内容的出口电路中使用的密钥数据)能以未加密形式通过该 PDN 内的软件或该 PDN 外部的任何实体访问。

[0063] 在一类实施例中，本发明的 PDN 包括含加锁箱电路(这里有时称为“Lockblx”)的至少一个设备。每个此类设备(称为 PDN 的“节点”)由硬件(以及可任选地还由软件或固件)构成，并且可以是集成电路或包括集成电路。PDN 通常包括至少两个节点(例如，实现视频或音频存储、回放和处理功能的节点)。每个节点可(但无需)包括入口电路和出口电路之一或其两者以及加锁箱电路。包括入口电路(这里有时将入口电路称为入口单元)和加锁箱电路的节点将称为“入口节点”。包括出口电路(这里有时将出口电路称为出口单元)和保密箱电路的节点将称为“出口节点”。每个入口节点和出口节点能够接收受使用限制集约束的内容(例如，数字视频数据和数字音频数据之一或其两者)，并被配置成以该使用限制集所不禁止的至少一种方式(以及可选地，以多种或所有方式)使用该内容。

[0064] 在本发明 PDN 的一些实施例中，每个节点内的保密箱、每个入口节点内的入口电路、以及每个出口节点内的出口电路以硬件实现。在本发明 PDN 的一类实施例中，每个保密箱、每个入口节点内的入口电路、以及每个出口节点内的出口电路被实现为集成电路或多芯片集(可包括以固件编程的微处理器)，但不包括以软件编程的外部 CPU。在一些实施例中，体现本发明的 PDN 的每个节点可任选地还包括以固件或软件编程的、受每个节点被配置成使(未加密形式的)机密在该节点内仅可在硬件中处理而不将其中任何机密泄露给该节点中的软件或固件的限制约束的至少一个元件。经加密的机密(例如，根据本发明在节点的硬件中加密的机密)可被泄露(以经加密形式)给该节点内的软件或固件、或该节点以外的实体。由此，每个入口节点内的入口电路、以及每个出口节点内的出口电路都包括安全硬件，并且可任选地还包括以固件或软件编程的至少一个元件，但是每个节点中的入口电路和 / 或出口电路被配置成仅在硬件中处理(未加密形式的)机密而不将其中任何(未加密形式的)机密泄漏给该节点以外的任何实体或该节点内的软件或固件。节点内的加锁箱通常包括(但无需包括)安全硬件，并且可但无需包括以固件或软件编程的至少一个元件(例如，加锁箱可以是以固件或软件编程的处理器)。但是，每个节点(以及节点内的每个加锁箱)都被配置成仅以不将其中任何机密泄漏(以未加密形式)给该节点以外的任何实体(或该节点中的软件或固件)的方式处理机密(用于包含该节点的 PDN 中的内容保护)。一节点(和 / 或节点内的保密箱)可被配置成在以防止其中任何机密被泄露(以未加密形式)给该节点以外

的任何实体(或该节点中的软件或固件)的方式实现处理机密的情况下在安全硬件中处理(未加密形式的)机密。

[0065] 每个入口单元(在PDN的入口节点中)被配置成将进入该PDN的经加密内容解密并重新加密(在硬件中)。通常,该解密和重新加密(即,转加密)是在入口单元内的硬件中以安全方式执行的,并且该重新加密在经解密内容可通过该入口单元以外的任何实体(硬件或软件)访问或易受其攻击之前进行。离开入口单元的经重新加密的内容在该PDN内于各集成电路之间传送、或者通过软件或未授权实体容易访问时总是保持经重新加密的形式。每个出口单元(在PDN的出口节点中)被配置成以安全方式解密经重新加密的内容(在硬件中)以供该PDN显示(和/或回放)和/或从该PDN输出。每个节点内的保密箱电路("加锁箱")通常能够存储并且通常的确存储至少一个入口和/或出口单元执行授权操作所需的机密。当入口节点或出口节点内的保密箱与另一节点内的加锁箱通信(例如,以从后一节点获得内容密钥)时,它仅通过在这两个加锁箱之间建立的安全信道来进行。"内容密钥"是用来解密或加密PDN内的内容、并由PDN中的这些节点保密的密钥(较佳地,使用密码性良好的随机源来安全生成的密钥)。节点内(例如,在入口节点内的保密箱与入口电路之间)的通信可用任何安全方式来实现(例如,以实现节点之间的通信的相同方式或以不同方式)。没有任何存在于PDN的节点中供该节点内的加锁箱、入口和出口电路中的任一个使用(或向其传送)的机密以未加密形式传送给该PDN的另一节点,并且通常,没有此类未加密形式的机密可通过该PDN内的软件或固件、或该PDN以外的任何实体访问(尽管它可由节点内的硬件访问)。在典型实施例中,该PDN采用有效的认证机制来挫败攻击者试图仿效一节点来获得对内容的未授权访问的企图(例如,必须在入口(或出口)节点与另一节点之间成功完成认证交换之后,其中任一节点才会向另一节点传送可能对攻击者有用的任何机密,并且攻击者将不具备成功完成这一交换的能力)。为了规避本发明PDN的此类实施例所提供的保护,将需要执行闯入节点内的保密箱、入口和出口电路中的一个或多个并修改(或本质上修改)每个开放式硬件单元内的电路的非常困难(并且通常是不切实际)的操作。此外,此活动将必须针对所要攻击的每个物理系统执行,并且不能简单地通过因特网分发和下载(如用软件可以做的那样)。

[0066] 在本发明PDN的典型实施例中,为了使入口节点能执行入口操作(例如,使用内容密钥来转加密内容),该节点的加锁箱必须或者使内容密钥存储其中(或者等效地必须使其安全地存储在外部,并具有将其本地高速缓存并从此类高速缓存检索之的能力),或者必须从另一节点的保密箱安全地请求并获得该内容密钥。一节点内的电路和通信(例如,一节点内的保密箱和入口电路之间的通信)可用任何方式实现,尽管最好是尽可能地简单。无论使用什么机制在一PDN中的各节点之间通信,都必须有可能在各节点之间安全地通信——即,以能确保信息仅能在两个授权节点之间交换而没有任何第三方可读取、修改或重放这些通信的方式。如果一节点被实现为单块芯片,则该芯片的封装必须对该节点的各元件之间的通信提供足够的安全性,从而对于该芯片内各元件之间的通信不需要任何其它的安全措施(超出该芯片所提供的物理安全性)。如果一节点的元件在同一PC板上或同一盒或机柜内实现,则这些元件之间的安全通信可使用强健性足够的简单密码机制(例如,通过安全地创建并彼此就会话密钥达成一致)来实现。与此相反,节点之间的通信总是以标准化方式(例如,执行初始交换以认证端点并在这些节点之间建立安全通道,随后通过安全的点对点通

道以经加密形式发送要在这些节点之间发送的任何机密）来执行的。例如，在包括两个节点的 PDN 中，这些节点之一的制造商所专用的密码机制可用于该节点内各元件之间的节点内通信，而另一机制可被用于另一节点内的节点内通信，但两个节点均将被配置成以标准化方式相互通信。在一类实施例中，一节点被配置成使用对称加密机制来与其它节点通信，并使用同一机制进行其各元件之间的节点内通信，由此允许节点内和节点间通信共用硬件（更具体地，节点通常将被配置成使用非对称机制来彼此认证和交换要用于后续对称加密的密钥。在这样的认证和密钥交换之后，可使用对称机制直至有必要替换对称密钥，此时这些节点将再次使用非对称机制来完成对称密钥的替换。也可使用一些类型的密钥扩展 / 排程方法在所需间隔用更新的密钥来替换对称密钥）。在制造要使用同一对称机制来与其它节点通信及进行节点内通信的节点时，可将同一对称密钥存储（例如，作为集成电路制造技术的结果）在该节点的保密箱中，并存储在该节点中可参与与该保密箱的节点间通信的所有其它元件中（此对称密钥可被用于传送其它更暂时性的对称密钥以减少密钥素材的重复使用）。

[0067] 在本发明 PDN 的一些实施例中，PDN 的一些设备是节点（每个节点包括一保密箱，并且可任选地还包括入口和 / 或出口电路），而 PDN 的其它设备不包括保密箱因而不是节点。预期本发明 PDN 的典型实施例的不同元件（例如，不同节点）将由不同且独立的供应商制造并提供，尽管并非必须如此。

[0068] 在本发明 PDN 的典型实现中，每个入口（或出口）节点内的入口（或出口）电路被配置成仅执行授权操作，并且在对内容执行任何授权操作（例如，任何授权解密操作）之前必须从保密箱获得至少一个机密。但是，每个保密箱被配置成在没有首先确定（例如，作为认证交换的结果）另一节点被授权执行该机密将允许该另一节点执行的每个操作的情况下就不向该另一节点提供任何此类机密。节点还可能需要交换关于可应用的内容使用限制集的信息。为了使出口（入口）电路能对内容执行操作，两个节点可能需要协商、和 / 或其中一个节点可能需要向另一个提供状态信息、和 / 或其中一个节点可能需要放弃它自己对内容的权利（例如，以允许另一节点对该内容执行特定操作）。例如，第一节点中的保密箱可（在向出口节点提供密钥或其它机密之后）从出口节点撤消许可，除非该出口节点在预定时间窗内向该第一节点提供特定的状态信息。例如，出口节点可能需要告知第一节点中的保密箱该出口节点中的出口电路实际上已经（或者尚未）呈现了特定内容、或将该内容变成供在另一个地方使用的形式。当然为安全和成本原因限制节点之间的互换的复杂性是合乎需要的。在一些实施例中，实现许可撤消的复杂性最低的（由此是优选的）技术可能是要求出口或入口节点以有规律的间隔向第二（许可给予）节点断言请求以使许可得以继续，其中每个请求包含当前状态数据（例如，指示该出口或入口节点已完成了操作序列中的多少操作的数据），并要求出口或入口节点配置第二节点的保密箱以使其能够（自动）撤消授予该出口或入口节点的许可（在其拒绝将该出口或入口节点执行该出口或入口节点希望执行的操作所需的至少一个机密给予该出口或入口节点的意义上），除非它接收到预定的请求和 / 或状态数据。例如，出口节点可能需要一个密钥序列来执行所要求的操作，并且第二节点的保密箱可被配置成在其已向该出口节点提供了该序列中的一个密钥之后，它将仅在从该出口节点接收到预定类型的状态数据之后才向该出口节点提供该序列中的下一密钥。在其它实施例中，这些目的可通过使出口节点监视它自己的状态并且在其不再能够确保使用限制集条

件得到满足的情况下丢弃该内容密钥来实现。

[0069] 使用在前一段落中所述类型的技术，可防止 PDN 中的所有出口和入口电路不同于授权方式和授权格式地生成(或输出)内容。例如，如果 PDN 被授权以经 HDCP 加密格式通过 HDMI 链路输出内容，则该 PDN 的出口电路可被配置成使用从保密箱获得的一个或多个机密以将经重新加密的内容(由该 PDN 的入口电路生成)解密，使用 HDCP 协议将该内容重新加密并格式化该经 HDCP 加密的内容供通过 HDMI 链路传送，并通过 HDMI 链路向该 PDN 外部的 HDMI 接收器传送该经格式化的内容，从而仅被许可的 HDMI 接收器(例如，高清晰度监视器中的)能够解密并显示所传送的内容。例如，出口节点可连续解密一视频流(并允许其被解压缩)，该视频流进而在 HDCP 下被重新加密以供通过 HDMI 链路传送。在 HDMI 链路报告该 HDCP 连接不再有效的情况下，出口节点将停止对该流的解密，丢弃该内容密钥，并报告该异常。又如，如果本发明 PDN 的一个实施例被授权输出明文内容的按比例缩小的模拟版本，则其出口电路可被配置成使用从保密箱获得的一个或多个机密以允许(响应于指示由该 PDN 的入口电路生成的经重新加密内容的数字数据)生成指示该明文内容的模拟信号、并将该模拟信号从该 PDN 输出到接收器(例如，模拟显示设备)。在两个例子中，保密箱均根据本发明来配置以在不首先确定(例如，作为认证交换的结果)该出口单元被授权执行该机密允许该出口单元执行的每个操作的情况下就不会向该出口单元提供任何此类机密。此外，可依靠该出口节点来准确地报告其意欲对该内容的使用，并且该保密箱将不会向其所陈述的使用可能违反与该内容相关联的使用限制集的出口节点提供内容密钥。

[0070] 保密箱(在根据本发明的 PDN 的节点中使用)通常被配置成在不首先确定(例如，作为认证交换的结果)另一节点被授权执行该机密允许该另一节点执行的每个操作的情况下就不向该另一节点提供任何机密。当保密箱向永久安装在与该保密箱同一节点中的出口(或入口)电路(例如，该保密箱和出口电路在永久安装于一机顶盒内的不同芯片中实现的情况)提供机密时，此类认证交换可以是(并且很可能将是)隐式的。如果在设备制造期间，共有的机密被永久地存储在各保密箱和出口(或入口)电路中(例如，通过将该共有机密烤入硅中或烧制在各出口或入口电路及保密箱中)，则可在永久安装在通用设备(可用作节点)中的保密箱和出口(或入口)电路之间执行隐式的认证交换。这一共用机密随后可由该保密箱和出口(或入口)电路用来相互认证并从该保密箱向该出口或入口电路分发密钥素材(例如，以周期性地更新由该出口或入口电路用来操作内容的密钥，以限制密钥重复使用并藉此降低该设备易受各种攻击影响的程度)。

[0071] 在一类实施例中，根据本发明，进入 PDN 的内容在硬件中(例如，芯片内的入口电路)解密，并且在根据本发明明文内容被曝露在该硬件之外之前(例如，在该经解密的内容离开包括该入口电路的芯片之前)，该经解密的(明文)内容在该硬件中被重新加密(例如，使用 256 位的 AES、CTR 模式、协议)。以此方式，仅经重新加密的内容(不是该内容的明文版本)被曝露在安全解密硬件(该硬件还执行重新加密)之外，并且即使在硬件中初始解密后内容在该 PDN 内也得到了很好的保护。就在该经重新加密的内容离开该 PDN 或在该 PDN 内被消费(例如，显示)之前，它根据本发明在硬件(例如，芯片内的出口电路)中解密而不在该硬件之外曝露经解密的(明文)内容。

[0072] 在另一类实施例中，本发明是一种方法和装置，用于在硬件中对进入 PDN 的内容执行解密和重新加密、并在其离开该转加密硬件(例如，芯片内的入口电路)之后和该内容

进入其中它将被解密(以及可任选地进行其它处理)以供该PDN显示和/或回放(和/或从该PDN输出)的另一硬件单元(例如,另一芯片内的出口电路)之前将其在该PDN内保持为经重新加密的形式。没有任何在该PDN中用来实现内容转加密或受控内容解密的机密(例如,密钥数据或证书)以未经加密形式可通过该PDN内的软件或固件、或该PDN之外的任何实体访问。应当理解,在本发明PDN的许多实施例中由保密箱、入口和出口电路使用的证书不需要保密。实际上,此类证书在PDN内常常是开放式和自由共用的(而不是作为机密处理),只要它们是密码可验证的(可通过数字签名追踪到信任根)即可。

[0073] 在一些实施例中,本发明PDN是一种具有开放式系统架构的计算系统(例如,PC)。例如,常规的开放式计算系统可根据本发明修改以包括第一节点、入口节点、及出口节点(每个节点通常但并非必须被实现为单独的芯片),其中根据本发明,入口节点被耦合并配置成使得进入该系统的内容在该入口节点的入口电路中被转加密以保护该系统内的内容。

[0074] 本发明的其它方面是保护PDN(例如,开放式计算系统)中的内容的方法、可由本发明PDN的任意实施例(或保密箱电路、入口电路和出口电路中的一个或多个)实现的方法、在PDN中使用的保密箱电路(例如,芯片)、在PDN中使用的入口电路(例如,芯片)、在PDN中使用的出口电路(例如,芯片)、包括沿总线(例如,PCI总线)连接的入口、保密箱和出口芯片供在个人计算机中使用的卡(例如,多媒体图形卡)、以及被配置成在PDN中使用并包括保密箱电路、入口电路和出口电路中的至少一个的设备(例如,机顶盒或视频接收器或处理器)。

[0075] 在一类实施例中,本发明是一种配置成在PDN中使用的设备(例如,用于从远程源接受内容的机顶盒、或者视频接收器或处理器)。该设备包括可以是被配置用于本发明PDN的至少一个实施例的任何类型的入口(或出口)电路和保密箱电路。一类这样的设备被配置成接收并解密具有N种不同格式中的任一种格式的内容(例如,根据N中不同内容保护协议中的任一种加密的内容)、并采用入口电路来输出仅具有单种格式的(例如,根据单种内容保护协议受保护的)内容的经转加密版本。另一类这样的设备被配置成采用出口电路来接收并解密仅具有一种格式的受控内容(例如,经转加密的内容),并能处理该经解密内容以生成具有M种不同格式中的任一种格式的输出内容(例如,根据M种不同内容保护协议中的任一种加密的输出内容)。因为这两类设备中的每一类均根据本发明来配置(即,其每个入口单元输出、并且其每个出口单元接收已根据单种内容保护协议加密的受控内容),所以两个此类设备可被耦合在一起以生成能够接收具有N种不同格式中的任一种的内容、响应于此生成具有M种不同格式中的任一种的输出内容、并通过从不在安全硬件之外(例如,在一个设备内的入口芯片或在另一设备的出口芯片以外)曝露该内容的明文版本来保护该内容的设备对。这一设备对中的每个设备均能够在其具有不超过N倍复杂性(响应于具有单种格式的输入生成具有N种格式中的任一种格式的输出、或响应于具有N种格式中的任一种格式的输入生成具有单种格式的输出的能力)或M倍复杂性(响应于具有单种格式的输入生成具有M种格式中的任一种的输出、或响应于具有M种格式中的任一种格式的输入生成具有单种格式的输出的能力)的意义上以简单方式实现。相反,能接收具有N种不同格式中的任一种格式的内容、并响应于此生成具有M种不同格式中的任一种的输出内容的常规设备在通过决不在该设备之外曝露该内容的明文版本来保护该内容的同时,将具有更大的复杂性(即,(N*M)-倍复杂性)。假定N和M各自大于1,并且N和M中的至少一个大于2,则该常规设备将比与该常规设备具有相同总能力的两个本发明的设备(一并考虑)更为复杂。当N

和 M 各自比 2 大得多时，该常规设备将比这样一对本发明设备（一并考虑）复杂得多。

[0076] 在一些实施例中，本发明的保密箱被配置成在适当时间使从内容供应方或其它外部源接收的具有仅在规定时间里授权其使用的限制的每个机密（例如，密钥数据集）不可访问（例如，删除），从而该机密具有预定的过期时间。优选的是，保密箱被配置成以高成本效益的方式执行此功能（例如，使用防止对机密的超出上舍入到与 N 秒间隔最接近的整数的预定过期时间的未授权使用的简单、廉价的电路，其中 N 是大于 1 的小数字，而要防止对该机密的超出确切预定过期时间的未授权使用将需要在该保密箱中包含昂贵得多的电路）。例如，优选的是保密箱包括防止对机密的超过按日计的授权使用期过期仅数秒的未授权使用的简单、廉价的电路，而要防止对该机密的不超过授权使用期过期仅几分之一秒的未授权使用将需要昂贵得多的电路。在一些实施例中，保密箱包括单调递增的计数器（其计数值在保密箱断电时不归零）或抗篡改时钟（其在保密箱断电时不复位）供确定何时要删除一具有过期时间的密钥（或者使其不可访问）时使用。或者，该保密箱被配置成周期性地（或在上电时）访问外部防篡改时钟以获得供确定何时要删除一具有过期时间的密钥（或者使其不可访问）时使用的当前时间数据。

[0077] 在典型的实施例中，本发明的保密箱被配置成与 PDN 内的其它设备（节点）通信和 / 或经由因特网（或以其它方式）与该 PDN 之外的实体通信。例如，该保密箱的集成电路实现可被配置成在该保密箱芯片和其它芯片沿其连接的 PCI 总线上经由软件执行芯片至芯片的通信。又如，该保密箱可包括用于与远程设备通信（经由因特网和 PDN 软件）的 SSL 端接电路。例如，在保密箱内使用 SSL 端接电路，该保密箱可使 PDN 的软件登录到因特网（例如，使用该 PDN 的一 PC 的 TCP/IP 功能）并中继往返该 SSL 端接电路的经加密消息（从因特网接收或要通过因特网发送）。远程设备还可使在 PDN 的 PC 上运行的软件执行该设备要通过因特网向该保密箱内的 SSL 端接电路发送经加密消息所需的 TCP 层功能。SSL 端接电路可执行解密该消息和加密保密箱的响应（要经由该 PDN 软件通过因特网发送）所需的 SSL 层功能。或者，保密箱可被配置成使用用于在 PDN 内各节点之间通信的协议扩展来与该 PDN 内的设备（除节点外）通信和 / 或与该 PDN 之外（例如，通过因特网）的设备通信。此协议通常是某种形式的使用公钥密码（用于签名和某种加密）和证书的简单问答协议。

[0078] 在本发明 PDN 的优选实施例中，明文内容以及用于重新加密（在入口单元中）、经重新加密内容的解密（在出口单元中）或其它功能的任何机密（例如，密钥数据）都不出现在该 PDN 中的可被寻求获取对其未授权访问的用户或实体访问（或至少容易访问）的任何节点、链路或接口处。在这些实施例中的一些典型例中，没有任何在该 PDN 内部（或外部）的设备上运行的软件或固件可访问该明文内容或任何此类此类机密。例如，尽管软件可指示出口节点从 PDN 中的存储取回特定内容（先前已由入口节点转加密），使用特定密钥解密所取回的内容并将该经解密的内容重新加密成特定格式供输出，但是该软件将决不会看到该密钥（除了可能以经加密的形式）并将决不会看到内容的明文版本。相反，出口节点将通过使用存储在该出口节点的保密箱内的机密（包括该密钥）、或通过向另一节点寻求执行这些规定操作所需的所有许可和机密（包括该密钥）来响应该指令。仅当第二节点确定该出口节点被授权执行这些操作时，该第二节点才向出口节点提供这些项，并且该第二节点将仅以加密形式向出口节点提供这些项（从而仅该出口节点能够解密这些项）。在一些实施例中，在 PDN 一节点内的嵌入式处理器（例如，微控制器）上运行的固件可访问明文、和 / 或用于内容的重

新加密(在入口单元中)或是经重新加密内容的解密(在出口电路中)的机密,但该明文内容和任何此类机密均不出现在该 PDN 中的可被寻求获得对其未授权访问的用户或实体访问(或至少容易访问)的任何节点、链路或接口。每个节点内的保密箱电路除了能向软件断言一标志以指示有消息(在该保密箱电路的发件箱中)供软件传递给规定实体以外可以是被动实体。或者,节点内的保密箱电路可实现用于将消息传递给其它实体(例如,其它节点)的一些其它技术,诸如(但不限于)使用 DMA 引擎或专用微控制器的技术。响应于指示保密箱电路的发件箱中有消息应被传递的标志,软件可将该消息从发件箱传递到规定接收方的收件箱中(通常,该消息将被加密使该软件不能将其解密)。在其它实施例中,节点内的保密箱电路可以是主动实体(例如,在它能主动向其它节点传送消息,并且可任选地还主动地执行密钥管理操作和其它操作的意义上)。仅那些包含机密素材的消息(在保密箱之间发送)需要被加密,但(在本发明的优选实施例中)在保密箱之间发送的所有消息至少被数字地签名(以标识其起源并确保其既未被变更也未被重放)。

[0079] 本发明的另一个方面是一种用于在系统(其中该系统既包括硬件又包括软件)的硬件子系统中安全地执行内容的加密和解密、而将该系统的软件用作在这些硬件子系统之间传递消息(通常是经加密或签名的消息)但不能理解这些消息(或不能理解其中经加密的那些消息)的无害实体(“中间人”)的内容保护方法和装置。例如,当这些消息是指示经加密的机密(例如供一个或多个硬件子系统使用的内容密钥)的经加密消息时,该软件如果没有将其解密所需的密钥就不能将其解密,从而不能理解这些消息。该软件可用于实现整个系统的各安全硬件子系统之间的安全通道,并且这些安全通道对要保护内容的“中间人”攻击免疫。但是,该系统使用软件作为中间人来传递消息。

[0080] 在既包括硬件又包括软件并体现本发明的一些系统中,在该系统的各硬件子系统之间传递消息的软件可(并且优选地的确)理解其中一些类型的消息。例如,该软件可理解要向该系统的许多(或所有)元件广播以请求特定的密钥或其它特定项被发送给该消息的发送者的每个消息。这一广播消息(或另一类消息)可使用数字签名来保护,并且当不需要或不想要加密该内容以及该软件必须理解该消息(例如,以更有效地广播或路由它)时,可以未加密形式为软件访问。

[0081] 在本发明的一类实施例中,要保护的内容是已使用第一内容保护协议加密的视频数据(例如,高清晰度数字视频数据)、或包括此类视频数据。当该内容进入一入口单元时,它在该入口单元的硬件中被解密(变为明文形式),并且在离开该入口单元之前,该明文内容被用不同的内容保护协议重新加密。该经重新加密的内容(这里有时称其为“受控”内容或“经转加密”内容)可在 PDN 的各元件之间传送和/或存储在各元件内直至其进入出口单元。在出口单元中,该经重新加密的内容被再次解密(变成明文),该明文内容可任选地还被进一步处理,并且明文内容(或其经处理的版本)随后被重新加密或者格式化以供从该出口单元输出。例如,该出口单元可根据 HDCP 协议重新加密该明文内容,并根据 HDMI 标准(或 DVI 标准)格式化该经 HDCP 加密的内容以供经由 HDMI 链路(或 DVI 链路)从该出口单元向外部视听系统输出。或者,该出口电路以供通过除 HDMI 或 DVI 链路以外的类 TMDS 链路、通过除类 TMDS 链路以外的串行链路、或通过某种其它数字或模拟链路传送的格式输出内容。

[0082] 根据本发明受保护的内容可以是视频或音频数据但并非必须如此。此类内容可以是指示能被数字地存储的任何信息(诸如但不限于图片、文本和个人信息)的数据或包括此

类数据。

[0083] 优选的是，本发明的保密箱被实现为仅包括实现所需内容保护功能的最小硬件特征集以便于成本合算地实现。例如，在保密箱将不接收和存储仅在有限时间里有效的任何机密的应用中，该保密箱可被实现为不带用于在预定时间间隔结束时删除存储在该保密箱中的机密的硬件(例如，包括单调递增计数器或抗篡改时钟的硬件)。

[0084] 在一类实施例中，个人计算机根据本发明被更改成包含沿系统总线(例如，PCI 总线)连接的三个分离的集成电路(其一实现入口节点、另一实现出口节点、其三实现另一节点)。这三块芯片可在被配置成容易安装在个人计算机中的卡(例如，多媒体图形卡)上实现。或者，三块芯片可在各自均被配置成容易安装在个人计算机上的分离卡上(例如，如果这些芯片被配置成彼此执行显式的认证交换以建立可供它们以安全方式相互通信的安全通道)实现。本发明的其它方面有在个人计算机中使用的入口节点、保密箱及出口节点芯片。

[0085] 在另一类实施例中，个人计算机根据本发明被更改成仅包含一个节点而不是像前段示例中那样包含三个分离的节点。该节点可以是入口节点、或出口节点、或既非入口节点也非出口节点的节点。在本发明的其它实施例中，个人计算机本身起到PDN的节点的作用。

[0086] 在本发明的PDN的典型实施例中，由入口单元生成的经重新加密的内容可被存储在可移动盘上或者以能容易地从该PDN移除的方式存储在该PDN中。在此类实施例中，由节点(例如，由节点内的入口和出口电路)使用的机密也可(以加密形式)存储在可移动盘或者以能容易地从该PDN移除的方式存储在该PDN中。例如，保密箱可使用永久和安全地存储在该保密箱内(例如，烤入该保密箱的硅中)的密钥加密此类机密供存储。因为仅该PDN的授权硬件(即，出口节点的保密箱)才必须或能够获得解密该经重新加密的内容所需的机密以生成其明文版本，并且仅该PDN的授权硬件(即，保密箱)将具有解密该经加密的机密所需的密钥，所以即使从该PDN移除，该经重新加密的内容(或机密)也不能以未授权方式被使用。内容的重新加密(和/或所要存储的机密的加密)是以该PDN独有的方式完成的，由此该经重新加密的内容不需要被安全地存储，并且经加密的机密不需要被安全地存储。相反，该经重新加密的内容(和/或经加密的机密)可用不安全的方式(例如，盘上)存储在PDN中和/或以不安全的方式通过该PDN从入口单元传送到出口单元。相反，其他人也提出了通过将内容安全地锁定在PDN的每个设备内并保护PDN各设备之间的所有链路来保护该PDN中的内容。

[0087] 如果进入PDN的预先加密的内容在其于入口节点中被解密(并重新加密)之前就从该PDN移除，则该内容将不会被使用，除非首先执行了授权交易(例如，与数字权限管理系统或以某种其他方式与该内容的所有者)。此类交易往往包括额外费用的支付。

[0088] 根据本发明的典型实施例，内容供应商(例如，经由卫星向PDN的机顶盒传送内容的实体)或PDN之外的其他实体可将机密加载到该PDN的保密箱中(在确立该保密箱被授权接收它之后)，并且该保密箱随后可将该机密提供给出口或入口电路(在包含该保密箱的节点内)或在适当情况下提供给另一节点。或者，在需要机密时，该保密箱中可能没有存储该机密。在后一种情形中，保密箱可(例如，响应于来自出口或入口节点的请求)从该PDN内的另一保密箱(一“对等”保密箱)寻求所请求的机密和/或(例如，如果它没有从对等保密箱获得该机密)从该PDN之外的实体(例如，内容供应方、服务供应方、或数字权限管理服务)

寻求该机密。在所有情形中，应用于相关内容的使用限制集确定如何以及何时可交换该机密。例如，假定入口节点准备好从外部源接收内容，并且该入口节点的保密箱询问第二节点的保密箱(经由例如作为在上电时在这些极点之间执行的认证交换的结果已在这些节点之间建立的安全通道)该入口节点是否能够对此内容执行特定解密和重新加密(转加密)操作。如果该第二节点的保密箱确定(例如，作为这两个节点之间的交换的结果，在交换中预存在该入口节点中的证书由该入口节点的保密箱提供给第二节点)回答是肯定的，则该第二节点的保密箱向该入口节点的保密箱提供执行规定的转加密操作所需的机密。该第二节点的保密箱仅在该入口节点的保密箱向该第二节点的保密箱证明该入口节点是被许可的设备之后，以及在该第二节点的保密箱向该入口节点的加锁箱证明该第二节点是被许可的设备之后，才通过该 PDN 内的安全链路经由认证交换将该机密发送给入口节点。当出口节点的保密箱请求从该 PDN 内接收经重新加密的内容、并对其执行特定操作(例如，解密、然后进行一种不同的加密，并格式化该内容以供从该 PDN 输出)时，这一交换还在出口节点与第二节点的保密箱之间发生。当入口单元已从保密箱接收到执行规定转加密操作所需的机密时，内容供应方可向该入口单元发送内容，并且该入口单元可使用该机密来接收和转加密该内容，并将经重新加密的内容(例如，在盘上)存储在该 PDN 中。以后，出口节点可使用机密(从该保密箱获得的)来访问所存储的经重新加密的内容并对其执行经授权的操作。

[0089] 进入本发明 PDN 的内容具有一使用限制集，它(如上所定义)是该内容所受的所有使用限制的集合。在典型实施例中，PDN 的保密箱中预先存储了指示该使用限制集(例如，通过指示该使用限制集不禁止的对该内容的操作)的基元(例如，这里是称为“权限数据”的数据)。尽管指示使用限制集的基元可被预先存储在保密箱中，当时使用限制集也可随时间改变(例如，它可响应于诸如预定事件的发生而限制性变强，或可在诸如用户为获得对该内容增强的访问而付费的情况下限制性变弱)。响应于使用限制集的每次改变，存储在保密箱中的相应基元也将改变(例如，更新后的基元将被存储，并且过时的基元被删除)。PDN 的保密箱中还在其中预先存储了对内容执行不为该使用限制集所禁止的至少一个操作(例如，解密)所需的至少一个机密(例如，密钥数据)。通常，这些基元(指示使用限制集的)和机密(对该内容执行至少一个操作所需的)存储在保密箱中的存储器(例如，非易失性存储器)中。或者，这些基元和机密存储在该保密箱之外的存储器(例如，非易失性存储器)中，从而所存储的基元和机密的明文形式仅可为该保密箱访问。在典型实施例中，当PDN的入口(或出口)节点准备好接收内容时，该入口(出口)节点向第二节点的保密箱断言许可对该内容执行一个或多个规定操作(例如，转加密或解密，接着重新格式化以供显示)的请求。如果该保密箱决定准许该请求(例如，在将指示所请求操作的数据与预先存储在该保密箱中的权限数据作比较之后)，则该保密箱向该入口(或出口)节点断言至少一个机密以使该入口(或出口)节点能执行每个所请求的操作。该入口(或出口)节点不持久地存储任何此类机密，因此每个此类机密与会话密钥相似。在一个实施例中，这些节点使用实际的会话密钥来保护它们之间的通信，并确保存储在该保密箱节点中并且必须被安全传送给出口节点以便于使用该内容(根据该内容的使用限制集)的内容密钥的安全。通常，在入口(或出口)节点内使用此类机密的入口(或出口)电路不具有在其中持久存储该机密的存储器，尽管它可具有用于在其中双重缓冲该机密(例如，以允许该机密能容易地为该机密的更新后版本所替代)的少量缓存。通常，在 PDN 各节点之间传送的机密、并且有时还有在节点之间传送的请求或其它非机

密数据以加密形式通过作为这些节点之间的初步认证交换的结果而在其间建立的安全通道传送，并且在认证交换其间，每个节点必须向另一节点证明其身份。节点可被配置成加密它们相互发送的所有消息(例如，如果这将简化通信协议)，但它们或者可被配置成仅加密包含机密信息的那些消息(例如，入口节点可不加密它向另一节点发送的对会话密钥的请求，其中此类请求不包括会帮助攻击者获得对内容的未授权访问的信息，并且这些请求的加密本身可能向攻击者泄漏关于用来加密这些请求的密钥的信息)。

[0090] 即使在入口(或出口)电路从保密箱接收到内容密钥之后，通常对该入口(出口)电路能使用该内容密钥来做什么有限制，并且该入口(或出口)电路应被配置成除顺应这些限制之外不能操作。例如，为适应内容密钥授权出口单元解密内容、在监视 HDCP 安全性的同时使用 HDCP 协议将该内容重新加密并通过 HDMI 链路发送它的情形，倘若在确定 HDCP 安全已被破坏(即，当出口单元确定 HDMI 接收器是未授权的)时出口单元必须停止 HDCP 加密和 HDMI 发送，则该出口单元应被配置成确切地以该授权方式来操作(例如，它应不能继续 HDCP 加密和 HDMI 传送操作，除非它周期地接收或生成 HDCP 安全性的某种确认)。

[0091] 在优选实施例中，本发明 PDN 及其每个保密箱被实现成在诉求或不诉求外部授权机构的情况下允许包括入口和 / 或出口电路的设备被关联到该 PDN 中。在一些实施例中，PDN 的保密箱被配置并操作成请求内容所有者同意向该 PDN 添加特定设备或能力。优选的是，用户可能想要包括在该 PDN 中的每个设备的保密箱被配置成使得机密能被持久和安全地、但不可撤消地存储在其中以指示该保密箱(以及包含该保密箱的设备)是该 PDN 的授权元件(节点)。通常，该机密是证书或包括证书，由此在本文中该机密有时将被称为“结婚证书”。但是应当认识到，结婚证书可能不是或不包括真正的证书(例如，结婚证书可以是公钥而不是真正的证书)。保密箱可被配置成具有在其与该 PDN 相关联时在其中存储(至少临时地)结婚证书的能力。每个保密箱可被配置成包括可编程(例如，一次性可编程)存储器，以存储结婚证书或确定其它节点是否为该 PDN 的授权成员(即，确定其它节点是否拥有有效的结婚证书并因此与该 PDN“结婚”)所需的其它数据(例如，证书)。每个此类可编程存储器可被实现为保密箱内的闪存或 EEPROM(或类似的)，但优选地被实现为保密箱内比闪存或 EEPROM 便宜的元件。在一些实施例中，该可编程存储器是节点以外(或该节点的保密箱以外但在该节点内部)但能以安全方式为该节点的保密箱访问的非易失性存储器(例如，该保密箱可用加密形式将所需数据发送到外部非易失性存储器以供存储，并且该存储器可响应于来自该保密箱的读取所存储数据的请求以加密形式将该数据发回给该保密箱)。在其它实施例中，每个可编程存储器是一旦不再需要即可被丢弃(或不再使用)但一旦被永久性编程为特定状态即不能再修改的一次性可编程熔丝组。例如，在保密箱中可有 16 (或其它数目)组熔丝，每组熔丝可被编程一次以存储一结婚证书，并且该保密箱可被配置成当需要访问其结婚证书时仅使用最近被编程的那组熔丝(即，忽略各其它熔丝)。存储在第一节点的保密箱中的结婚证、以及存储在第二节点的保密箱中的相关数据(例如，允许后一保密箱确定另一节点是否拥有有效结婚证书的数据)可在这些节点之间的简单认证交换中用来在第一节点作为 PDN 的元件操作之前建立其间的安全通道。

[0092] 在一类实施例中，本发明是 PDN 中的内容保护方法，它包括以下步骤：在该 PDN 的入口硬件中转加密进入该PDN的内容，由此生成受控内容；以及在该PDN的出口硬件中解密该受控内容以生成经解密内容，从而明文形式的内容以及由该入口硬件和该出口硬件中的

至少一个用来对该内容或该受控内容执行授权操作的任何机密都不可为在该 PDN 的任何元件上运行的软件或固件所访问，并且除了在安全硬件内之外，该内容决不会以明文形式出现在该 PDN 内，由此该受控内容可在该 PDN 的各元件间被自由传送，并存储在该 PDN 内。在一些此类实施例中，入口硬件是一集成电路，出口硬件是另一集成电路，并且该内容被维持在该 PDN 内，从而除在集成电路内以外该内容决不会以明文形式出现在该 PDN 内。

[0093] 在另一类实施例中，本发明是一种内容保护方法，包括以下步骤：在个人数字网络的入口节点中转加密进入该个人数字网络的内容，由此生成受控内容；以及在该个人数字网络的出口节点中解密该受控内容以生成经解密内容，从而除了该个人数字网络的安全子系统内以外，该内容以及由该入口节点和该出口节点中的至少一个用来对该内容的任何版本执行授权操作的任何机密都不会以明文形式出现在该个人数字网络内。例如，这一机密（或明文形式的内容）可由在该入口节点或出口节点的安全子系统内的嵌入式处理器上运行的固件（例如，在该入口或出口节点的安全子系统内的微控制器上运行的固件）访问，但该明文内容以及任何此类机密都不在该个人数字网络中可为寻求获得对其未授权访问的用户或实体访问（或至少容易访问）的任何节点、链路或接口处出现。

[0094] 在另一类实施例中，本发明是一种内容保护方法，它包括以下步骤：在 PDN 的入口硬件中转加密进入该 PDN 的内容，由此生成受控内容；在该 PDN 的出口硬件中解密该受控内容以生成经解密内容；以及可任选地还从该出口硬件向该 PDN 之外的实体（例如，一设备或系统）断言该经解密内容和该经解密内容的经处理版本中的至少一个。该经解密内容以及由该入口硬件和出口硬件中的任何一个用来对该内容和该受控内容执行授权操作的任何机密都不可为在该 PDN 的任何元件上运行的软件或固件访问。通常，该入口硬件是一集成电路，并且该出口硬件是另一集成电路。

[0095] 在另一类实施例中，本发明是一种内容保护方法，它包括以下步骤：使用从 PDN 的保密箱获得（由出口硬件）的至少一个机密在该 PDN 的出口节点的出口硬件中解密内容，由此生成经解密内容。该保密箱在该出口节点内部，但该保密箱可从该 PDN 的另一节点内所包含的另一保密箱（或从该 PDN 之外的源）获得该机密。可任选地，该方法还包括以下步骤：从该出口节点向该 PDN 之外的实体（例如，一设备或系统）断言该经解密内容和该经解密内容的经处理版本中的至少一个。

[0096] 在一些实施例中，进入本发明 PDN 的内容是经加密视频（例如，已从 HD-DVD 读取的、并由 CSS 或类似于 CSS 的内容保护方案保护的高清晰度视频）或包括经加密视频，并且该 PDN 的出口单元被配置成生成经解密的压缩视频（例如，MPEG 或 MPEG-2 压缩视频），对该压缩视频执行解压缩以生成经解密的解压缩视频（“原”视频），并重新加密该原视频。在一些实施例中，该出口单元根据 HDCP 协议执行重新加密，并通过一条或多条 HDMI 链路将经重新加密的原数据传送给外部视听系统。在其它实施例中，该出口单元根据除 HDCP 外的其它内容保护协议重新加密原（经解密）数据，并通过除 HDMI 链路以外的一链路向外部设备断言经重新加密的数据。在其它实施例中，该出口单元通过一条或多条 DVI 链路向外部设备断言经重新加密的数据。在其它实施例中，该出口单元通过一条或多条类 TMDS 链路（它们均非 HDMI 或 DVI 链路）或通过一条或多条串行链路（它们均非类 TMDS 链路）断言经重新加密的数据。

[0097] 在其它实施例中，进入 PDN 的内容被转加密并用合适的使用限制集标记（或者在

进入该 PDN 时已经是 PDN 加密格式的内容用合适的使用限制集标记，除非其已用该使用限制集标记)，并且该受控内容(例如，新转加密的内容) 被存储在外部硬盘驱动器(HDD) 阵列中。在此情形中，PDN 可能不再能够维持对该内容的控制(例如，该 HDD 可能从其机壳中被卸下并被连接到通用 PC，从而将所存储的内容曝露于各种攻击)。但是，因为该内容在被存储之前被加密(以 PDN 加密格式)(根据本发明的典型实施例)，所以所存储的内容(甚至是大量的存储内容) 将长时间地(例如，许多年) 保持安全而不受确定的攻击。根据本发明的典型实施例，一旦受控内容出现在 PDN 中(例如，一旦进入该 PDN 的内容在入口电路中被转加密)，则可使用(即，呈现)它的唯一方式是在其相关联的内容密钥可用的情况下。因此，该受控内容的安全性完全依赖于保密箱和出口节点(其可包含解密该受控内容以将其变成明文形式所需的未加密版本的内容密钥) 的安全性，由此该受控内容能以任何方式被传送或存储(包括经由因特网自由分发) 而无需担心会违反该内容的使用限制集。

[0098] 根据本发明，提供一种个人数字网络，包括 ：至少一个入口节点，被配置成执行授权操作以响应所述入口节点的保密箱电路接收一个或者多个机密值，其中所述授权操作包括在所述入口节点的硬件中以安全方式转加密进入所述个人数字网络的内容，由此生成受控内容，所述入口节点的所述保密箱电路被配置以与另一保密箱电路交换机密值 ；至少一个出口节点，被配置成执行授权操作以响应所述出口节点的保密箱电路接收一个或者多个机密值，其中所述授权操作包括在所述出口节点内的硬件中以安全方式将所述受控内容解密，由此生成所述内容的明文版本，并将所述内容的明文版本的经处理版本向所述个人数字网络之外的实体、显示设备、以及回放设备中的至少一个断言，所述出口节点的所述保密箱电路被配置以与所述入口节点的保密箱电路交换机密值 ；以及包含保密箱电路的第三节点，其中所述第三节点的保密箱电路被配置成存储许可证书数据以及至少一个所述入口节点和至少一个所述出口节点执行授权操作所需的至少一个机密值，所述第三节点传送许可证书数据到所述出口节点，其中所述内容及所述机密值均不以明文形式出现在所述个人数字网络除安全子系统内之外的任何地方。

[0099] 较佳地，所述入口节点是一包含执行固件的至少一个微处理器的集成电路，所述出口节点是另一包含执行固件的至少一个微处理器的集成电路，并且所述入口节点、所述出口节点和所述第三节点的保密箱电路都不包含被配置成执行软件的可编程处理器。

[0100] 较佳地，所述入口节点被配置成转加密进入所述个人数字网络的经加密内容以使所述明文形式的内容不可为所述入口节点之外的硬件或软件访问。

[0101] 较佳地，所述个人数字网络还包括 ：至少一个设备，该设备耦合以接收所述受控内容并向所述出口节点断言所述受控内容和所述受控内容的经处理版本中的至少一个。

[0102] 较佳地，所述设备是数据存储单元。

[0103] 较佳地，所述设备是视频处理器。

[0104] 较佳地，所述个人数字网络被配置成没有任何出现在所述第三节点的保密箱电路、所述入口节点和所述出口节点中的任一个中供所述第三节点的保密箱电路、所述入口节点和所述出口节点中的任一个使用或向其传送的机密值以未加密形式在所述第三节点的保密箱电路、所述入口节点和所述出口节点中的任一个之间发送，并且没有任何机密值以明文形式为所述个人数字网络内的软件或所述个人数字网络之外的任何实体所访问。

[0105] 较佳地，所述个人数字网络被配置成没有任何机密值可为在所述个人数字网络的

任何元件上运行的固件所访问，并且没有任何机密值以明文形式出现在所述个人数字网络内除安全硬件内之外的任何地方。

[0106] 较佳地，每个所述入口节点被配置成仅对所述内容执行授权操作，每个所述出口节点被配置成仅对所述受控内容执行授权操作，并且每个所述入口节点和每个所述出口节点在执行任何所述授权操作之前将向所述第三节点的保密箱电路要求至少一个机密值。

[0107] 较佳地，所述第三节点的保密箱电路被配置成除非该第三节点的保密箱电路已确定所述出口节点被授权执行由所述机密值允许所述出口节点执行的每个操作，否则不向所述出口节点提供任何所述机密值。

[0108] 较佳地，所述第三节点的保密箱电路被配置成除非该第三节点的保密箱电路已根据与所述出口节点的认证交换的结果确定所述出口节点被授权执行由所述机密值允许所述出口节点执行的每个操作，否则不向所述出口节点提供任何所述机密值。

[0109] 较佳地，所述第三节点的保密箱电路被配置成除非该第三节点的保密箱电路已确定所述入口节点被授权执行由所述机密值允许所述入口节点执行的每个操作，否则不向所述入口节点提供任何所述机密值。

[0110] 较佳地，所述第三节点的保密箱电路被配置成除非该第三节点的保密箱电路已根据与所述入口节点的认证交换的结果确定所述入口节点被授权执行由所述机密值允许所述入口节点执行的每个操作，否则不向所述入口节点提供任何所述机密值。

[0111] 较佳地，所述入口节点的保密箱电路被配置成通过所述入口节点与所述第三节点的保密箱电路之间的至少一个安全通道与所述第三节点的保密箱电路交换机密值，并且所述出口节点的保密箱电路被配置成通过所述出口节点与所述第三节点的保密箱电路之间的至少一个安全通道与所述第三节点的保密箱电路交换机密值。

附图说明

[0112] 图 1 是使用常规高带宽数字内容保护(“HDCP”)协议常规地生成以将要通过 DVI 链路传送的数字视频数据加密的信号的时序图。

[0113] 图 2 是用于加密要通过 DVI 链路传送的数字视频数据的常规电路的框图。

[0114] 图 3 是图 3 的模块 81 的简化框图。

[0115] 图 4 是能体现本发明的个人数字网络(“PDN”)的框图。图 4 的 PDN 包括个人计算机 1 (一开放式计算系统)、监视器 2、以及扬声器 3。

[0116] 图 5 是能体现本发明的另一系统的框图。

[0117] 图 6 是图 4 或图 5 的盘驱动器 4 的一个实施例的各元件的框图。

[0118] 图 7 是图 4 的卡 10 的一个实施例的框图。

[0119] 图 8 是图 4 的卡 10 的替代品的框图。

[0120] 图 9 是图 4 的卡 10 的替代品的框图。

[0121] 图 10 是图 5 系统的变体中卡 20 的替代品的框图。

[0122] 图 11 是能体现本发明的另一系统的框图。

[0123] 图 12 是能体现本发明的又一系统的框图。

[0124] 图 13 是图 12 的盘驱动器 104 的一个实施例的各元件的框图。

[0125] 图 14 是能体现本发明的个人数字网络(“PDN”)以及耦合到该 PDN 的各种设备和

系统的框图。

[0126] 图 15 是体现本发明并包括沿 PCI 总线连接的设备的开放式架构计算系统的框图。

[0127] 图 16 是体现本发明的个人数字网络(PDN168)的一些元件(例如,入口节点 160、节点 161 及出口节点 162)、耦合到该 PDN 的存储单元(178)、以及能与该 PDN 通信的内容供应方(163)的框图。

[0128] 图 17 是图 16 的 PDN168 和存储单元 178 的框图,其中 PDN168 处于不同于图 16 中所示的状态。

[0129] 图 18 是(本发明 PDN 的一个实施例的)用于在保密箱和入口电路之间以及在该保密箱与出口电路之间建立安全通信通道的各元件的示图。

[0130] 图 19 是图 18 的 PDN 元件的示图,其中在保密箱和入口电路之间以及在该保密箱与出口电路之间有安全通信通道。

[0131] 图 20 是本发明入口节点的一个实施例的框图。

[0132] 图 21 是本发明出口节点的一个实施例的框图。

[0133] 图 22 是本发明节点(既非入口节点也非出口节点)的一个实施例的框图。

[0134] 图 23 是包括被配置成转加密具有 N 种不同格式中的任何一种的内容、并输出经转加密的具有单种格式的内容的入口电路的设备(例如,机顶盒)的框图。

[0135] 图 24 是包括被配置成接收具有单种格式的受控内容并生成该受控内容的经解密(明文)版本、并处理(例如,重新加密并可任选地还进行其它处理)该明文内容以产生具有 M 种不同格式中的任一种格式的经处理内容的出口电路的设备(例如,视频处理器)的框图。

具体实施方式

[0136] 首先将参考图 4 到 13 对上面引述的美国专利申请 No. 10/679,055 的教示进行概述。

[0137] 在以下说明中,表述“不受保护的”数据是指由一设备(例如,HD-DVD 驱动器)接收的、可能受或不受知识产权保护、但该设备被配置成将其识别为能以非加密形式向开放式计算系统断言的数据。

[0138] 在这里表述“SATA 接口”是指被配置成用于通过顺应 SATA 标准的至少一条串行链路通信的接口。这里的表述“SATA 标准”是指由串行 ATA 工作组于 2001 年 8 月 29 日采用的用于通过一条或多条串行链路在主机与一个或多个存储设备之间通信的称为串行 ATA 的标准修订版 1.0。

[0139] 在美国专利申请 No. 10/679,055 中记载的开放式计算系统的一个典型实施例中,该开放式系统的一封闭式子系统包含接收经加密内容(例如,来自该开放系统之外的源)、对所接收的内容执行解密及任何所需的解压缩以生成原内容、并重新加密该原内容的封闭式单元(有时称为“DDR”单元)。所接收的内容可以是经加密视频(例如,已从 HD-DVD 读取并由 CSS 或类似于 CSS 的内容保护方案保护的高清晰度视频)或包括经加密视频。DDR 单元可被配置成对该经加密视频执行解密以生成经解密的压缩视频(例如,MPEG 或 MPEG-2 压缩视频),对该压缩视频执行解压缩以生成经解密的解压缩视频(“原”视频),并重新加密该原视频以供从该开放式系统输出(例如,至外部视听系统)。

[0140] 以下参照图 4 和 5 说明的每个系统的一个方面是用于将 DDR 单元的输出与开放式

系统的标准(未被保护)图形和音频输出组合的电路。通常,现代 PC 具有两类图形系统之一。低端 PC 具有集成到其芯片集中的图形控制器(例如,集成到图 4 的 GMCH 芯片 6 中),并使用 AGP 数字显示卡(例如,与图 4 的卡 10 类似或相同的 ADD 卡)来将该数字视频连接路由到隔板 HDMI-DVI 连接器。较高端的 PC 通常直接在 AGP 或 PCI-Express 图形卡(例如,与图 5 的卡 20 类似的媒体 / 图形卡)上使用的更复杂的图形控制器。较早的 PC 使用在 AGP、PCI 或 ISA 总线上的图形控制器。在任一情形中,通常在该系统中有向该系统提供视频输出的单板。我们将称此板为“图形卡”而不拘于它是哪种类型的卡。

[0141] 在图 4 中,个人计算机(PC)1 是耦合到包含 HDTV 监视器 2 (包含 HDMI 接收器)和由 HDTV 监视器 2 驱动的扬声器 3 的外部视听系统的开放式系统。PC1 包含 HD-DVD 驱动器 4。在图 6 的盘驱动器 4 的实现中,驱动器控制器 30 将向多路复用器 31 断言从 HD-DVD 盘(未示出)读取的数据。多路复用器 31 可包含用于检测来自控制器 30 的数据是否是不受保护数据(例如,不受保护的菜单信息等)的电路。当多路复用器 31 检测到来自控制器 30 的数据是不受保护的数据时,多路复用器 31 向 SATA 接口 34 断言该数据。否则(例如,当多路复用器 31 检测到来自控制器 30 的数据是受版权保护的内容,例如受版权保护的高清晰度视频时),多路复用器 31 向 DVD 解码器 32 断言来自控制器 30 的该数据。

[0142] 通常,除了用于读写不受保护数据的数据接口(例如,带连接器 34A 的图 6 的 SATA 接口 34,或带合适连接器的 ATA 或 SCSI 接口)之外,HD-DVD 驱动器 4 还将包含 HDMI 接口(例如,图 6 的 HDMI 接口,包含 HDMI 发送器 33 和用于将发送器 33 耦合到 HDMI 电缆的连接器 33A)。HDMI 接口将提供与由数据接口提供的相分离的连接,这类似于 CD-ROM 用于向 PC 的声卡提供 CD 音频的单独模拟音频连接。

[0143] 但是,驱动器 4 与卡 10 之间单独的 HDMI 连接(与驱动器 4 的用于读写不受保护数据的数据接口分离)不是必要的。在一些实施例中(例如,将参照图 12 说明的实施例),经 HDCP 加密的数据从 DDR (开放式计算系统的一封闭式子系统)经由用于读写不受保护数据的同一数据接口“隧穿”到开放式计算系统。在后面的这些实施例中,HDMI 接口将加密(例如,重新加密)受保护内容,由此生成经 HDCP 加密的数据,并且该经 HDCP 加密的数据将通过该开放式计算系统传播到封闭式系统内的 HDMI 接收器(例如,HDTV 监视器或其它显示设备内的 HDMI 接收器)。即使该开放式计算系统能访问该经 HDCP 加密的内容,它也不能解密该经加密内容,而是只能使其通过并传递给该封闭式系统中的 HDMI 接收器。

[0144] PC1 还包含耦合以从 SATA 接口 34 接收数据的 I/O 控制器集线器(ICH) 芯片 5。ICH 芯片 5 控制 PC1 的 I/O 功能(例如,USB 功能)。ICH 芯片 5 经由图形和存储器控制器集线器(GMCH)芯片 6 耦合到 CPU7。GMCH 芯片 6 处理诸如 PCI (外围通信互连)总线功能、2 级高速缓存活动、以及 AGP (加速图形端口)活动等功能。存储器 9 和 AGP 数字显示(ADD)卡 10 被耦合到 GMCH 芯片 6。

[0145] 来自盘驱动器 4 的 SATA 接口 34 的数据可经由 ICH 芯片 5 和 GMCH 芯片 6 流入存储器 9,由 CPU7 处理,并且可能导致图形数据或不受版权保护的视频数据被输出到 ADD 卡 10 和监视器 2。元件 5、6、7 和 9 由此包括具有开放式系统架构的 PC1 的计算子系统,并且被配置成生成用于经由 ADD 卡 10 向监视器 2 断言的数据。

[0146] 卡 10 包括对来自芯片 6 的数字视频和音频数据执行 HDCP 加密的 HDCP 发送器(例如,图 7 的发送器 40)。卡 10 被配置成通过 HDMI 链路向监视器 2 断言将结果所得的经 HDCP

加密的数据视频和音频。从 GMCH 芯片 6 向 ADD 卡 10 断言的数据可以是 DVO（数字视频输出）格式。

[0147] 当盘驱动器 4 如图 6 所示地实现时，DVD 解码器 32 执行高清晰度视频数据（来自 HD DVD 盘）的解密和解压缩，并且 HDMI 发送器 33 重新加密结果所得的原视频数据（根据 HDCP 协议），并将经重新加密的视频数据通过 HDMI 链路（包含 HDMI 连接器 33A）直接发送到 ADD 卡 10。卡 10 通常起到 HDMI 转发器的作用，用于将经重新加密的视频数据通过另一 HDMI 链路发送到监视器 2。盘驱动器 4 还通过 HDMI 链路（用于向监视器 2 转发）直接向卡 10 发送监视器 2 解密该经重新加密的视频数据所需的任何密钥数据（例如，在 HDCP 认证交换期间所使用的密钥数据）。PC1 中除嵌入在 PC1 内的封闭式子系统以外的其它元件（盘驱动器 4、ADD 卡 10 的属于该封闭式子系统的每个元件、以及驱动器 4 和卡 10 之间的 HDMI 链路）不能访问经重新加密的视频数据或密钥数据。

[0148] 图 5 是图 4 系统的变体的框图。图 5 中与图 4 中相同的元件在两图中编号相同。在图 5 中，ADD 卡 10 被媒体 / 图形卡 20 所替换，并且 GMCH 芯片 6（包含集成图形电路）被 GMCH 芯片 16 所替换。芯片 16 被配置成向卡 20 断言 AGP 格式数据。卡 20 被配置成通过 HDMI 链路向监视器 2 断言经 HDCP 加密的数字视频，并直接向扬声器 3 断言模拟音频数据（在卡 20 内的 DAC 中生成）。媒体 / 图形卡 20 还起到 HDMI 收发器的作用，它通过第二 HDMI 链路向监视器重新发送经 HDCP 加密的视频数据（通过第一 HDMI 链路从驱动器 4 接收）、并从通过第一 HDMI 链路接收的数据提取经 HDCP 加密的音频、将该音频解密并对其执行数模转换、并直接向扬声器 3 断言结果所得的模拟音频。

[0149] 图 12 是图 4 系统的另一变体的框图。图 12 中与图 4 中相同的元件在两图中编号相同。图 12 的 PC101 与图 4 的 PC1 的不同之处在于 ADD 卡 110 替换了 ADD 卡 10（图 4），并且 HD-DVD 驱动器 104 替换了 HD-DVD 驱动器 4（图 4）。

[0150] 盘驱动器 104 可如图 13 中所示地实现。图 13 中与图 6 中相同的元件在两图中编号相同，并且图 13 的盘驱动器 104 的实现与图 6 的盘驱动器 4 的实现在以下方面不同。在图 13 的盘驱动器 104 的实现中，HDMI 连接器 33A 被省略，SATA 接口 34 被 SATA 接口 36（具有连接器 36A）所替换，并且 HDMI 发送器 33 被 HDCP 加密单元 35（其输出被耦合到 SATA 接口 36 的第二输入端）所替换。SATA 接口 36 被配置成（向连接器 36A）断言具有 SATA 格式的、指示接口 36 从驱动器控制器 30（经由多路复用器 31）接收的数据、或指示接口 36 从加密单元 35 接收的经 HDCP 加密数据的数据。当盘驱动器 104 的多路复用器 31 检测到来自控制器 30 的数据是受版权保护的高清晰度视频数据（和 / 或受版权保护的音频数据）时，多路复用器 31 向 DVD 解码器 32 断言该数据。响应于此，解码器 32 解码（解密）该数据并对其执行任何必要的解压缩，并向 HDCP 加密单元 35 的输入端断言结果所得的原（已解码的、或已解码并解压缩的）高清晰度视频（和 / 或音频）数据。响应于此，加密单元 35 向 SATA 接口 36 的输入端断言该原高清晰度视频（和 / 或音频）数据的经 HDCP 加密版本。该经 HDCP 加密的数据通过 SATA 接口 36（在具有 SATA 格式的数据流内）“隧穿”到 ICH 芯片 5，并从 ICH 芯片 5 经由 GMCH 芯片 6 和 ADD 卡 110 隧穿到监视器 2。当（盘驱动器 104 的）多路复用器 31 检测到来自控制器 30 的数据是不受保护的数据时，多路复用器 31 向 SATA 接口 36 的另一输出端断言该数据。具有 SATA 格式并指示该不受保护数据的数据流由接口 36 向 ICH 芯片 5 断言，并从 ICH 芯片 5 经由 GMCH 芯片 6 和 ADD 卡 110 向监视器 2 断言。

[0151] 图 12 的 ADD 卡 110 包含对来自芯片 6 的数字视频和 / 或音频数据执行 HDCP 加密，并将经加密的视频和音频通过 HDMI 链路向监视器 2 断言。在芯片 6 将经 HDCP 加密的数据从盘驱动器 104 转发到卡 110 的模式下，卡 110 内的 HDCP 发送器的加密电路被禁用或旁路。图 12 的卡 110 与图 4 的 ADD 卡的不同之处在于 :卡 110 没有被直接耦合到盘驱动器 104(其中卡 10 被直接耦合到盘驱动器 4)。卡 110 不需要包括其输出端被耦合到卡 110 与监视器 2 之间的 HDMI 链路的转换开关。相反，图 4 的卡 10 包含用于选择性地向监视器 2 断言来自其内部 HDCP 发送器(例如，图 7 的发送器 40)的数据、或直接从盘驱动器 4 接收的 HDMI 格式的经 HDCP 加密的数据。

[0152] HDTV 监视器 2 通常被实现为封闭式系统。如图 12 中所示，监视器 2 通常包含 HDMI 接收器 112、以及耦合到接收器 12 的显示设备 114(例如，CRT 或 LED 显示器)。设备 114 被配置成显示在接收器 112 中生成的经解密视频数据。接收器 112 包含被配置成将从卡 110 接收的经加密音频和视频数据解密的 HDCP 解密电路，并被配置成向扬声器 3 断言该经解密音频(通常在对其执行其它处理，诸如重新格式化等之后) 并向显示设备 114 断言该经解密视频(通常在对其执行其它处理，诸如重新格式化之后)。

[0153] 在图 12 的实施例中，盘驱动器 104 内的 HDCP 加密电路将由盘驱动器 140 接收(例如，由盘驱动器 104 从盘读取) 的受保护内容的已解码版本加密(重新加密)，由此生成经 HDCP 加密的数据。经 HDCP 加密的数据通过 PC101(开放式计算系统)传播到外部设备(HDTV 监视器 2) 内的 HDMI 接收器 112。即使 PC101 能访问该经 HDCP 加密的内容，但是因为没有所需的密钥，所以它也不能将该经 HDCP 加密的内容解密，而是仅仅使该经 HDCP 加密的内容通过并传递到监视器 2 中的 HDMI 接收器 112。

[0154] 在替换实施例中，开放式系统中的 DDR 单元与盘驱动器分离并独立。例如，DDR 单元可被配置成接收、解密并解压缩、以及重新加密来自因特网或本发明的开放式系统之外的其它源的受保护内容。

[0155] 当 DDR 单元被嵌入开放式系统中时，通常将设置将 DDR 单元的输出与该开放式系统的标准(不受保护的) 图形和音频输出组合的电路。例如，PC 的图形卡(例如，图 4 的卡 10 或图 5 的卡 20)可用另一封闭式子系统扩充，用于处理受保护内容(包括通过将 DDR 单元的输出与该 PC 的标准图形和 / 或音频输出组合)。该封闭式子系统优选地包括用于接收从 DDR 单元(通常集成在 HD-DVD 驱动器中)提供的经重新加密数据的 HDMI 连接器、以及将该经重新加密数据与该开放式系统的标准图形和 / 或音频输出组合(例如，时分多路复用、或组合成画中画格式) 的机构。优选的是，该扩充图形卡的输出本身是具有 HDCP 版权保护能力的 HDMI 连接，并且该扩充图形卡被配置成仅当该图形卡的输出端被连接到也支持 HDCP 的外部设备(例如，HD 监视器) 时才将来自 DDR 单元的经 HDCP 加密数据转发给外部设备。这防止受保护的内容流到该扩充图形卡，除非该外部设备(终端设备) 支持 HDCP 保护机制。

[0156] 该扩充图形卡中可能的最简单组合机构(“组合器电路”) 是被配置成选择 DVD 视频或系统图形输出的切换开关(例如，图 7 的切换开关 41)。该切换开关可以是用户致动的，从而用户可选择在屏幕上观看受保护内容(例如，图 7 中标为“HDMI 输入”的来自盘驱动器 4 的信号)，或观看 PC 图形的输出(图 7 中标为“(S)DVO”)。在图 7 的实施例中，ADD 卡 10 包括如图所示地连接的 HDMI 发送器 40 和切换开关 41。发送器 40 接收图 4 的 GMCH 芯片 6 的输出，对其执行 HDCP 加密，并通过 HDMI 链路向切换开关 41 断言经 HDCP 加密的数据。切换

开关 41 起到(通过另一 HDMI 链路)向监视器 2 转发发送器 40 的输出或 DDR 单元的输出(例如,图 6 的盘驱动器 4 的 HDMI 发送器 33 的输出)的 HDMI 转发器的作用。本发明的封闭式子系统的一个示例是驱动器 4 内的 DDR 单元(例如,图 6 的驱动器 4 的元件 31、32 和 33)和切换开关 41 (在图 7 的 ADD 卡 10 内)。

[0157] 在一些实施例中,该扩充图形卡将作为根据 HDCP 规范的“HDCP 转发器”。这一转发器将仅仅在原始源(DDR 单元)与目的地(例如,监视器)之间传递 HDCP 授权消息而不涉及协商。

[0158] 更精细的组合器电路(例如,在卡 10 内)也是可能的。例如,该组合器电路可被配置成将该视频显示嵌入屏幕的一部分中(例如,在图形窗口所位于的地方),或甚至将受保护内容重新调节到另一分辨率并将其嵌入在由不受保护内容确定的显示中(以生成外观与常规电视机中的画中画显示类似或相同的组合显示)。

[0159] 扩充图形卡中的该封闭式子系统被配置成确保仅当输出端被连接到启用 HDCP 的设备时,受保护内容(即,经 HDCP 加密的内容)才呈现在该输出上。在此类型的一些实施例中,该扩充卡包含将允许该扩充图形卡将来自 DDR 单元的流解密、以所允许的方式(例如,重新调节)更改该经解密数据、然后在将其发送到输出之前重新加密该经修改数据的 HDCP 认证机制。此类实施例通常将要求添加执行解密的组件、用于保存数据的一个或多个存储器缓冲器、可任选的调节模块、重定时和定位机构、以及重新加密机构。所有这些组件将被视为该扩充图形卡的封闭式子系统(以及本发明开放式系统的封闭式子系统)的一部分,并且它们将被设计成在 HDCP 加密没有被应用于该数据的情况下防止在该封闭式子系统之外观察到经解密数据或将其路由到该封闭式子系统之外。

[0160] 例如,图 8 的 ADD 卡 50 (在图 4 系统中可替换图 7 的卡 10)包含如图所示地连接的 HDCP 逻辑 53、HDMI 接收器 54、调节器 55、切换开关 51 及 HDMI 发送器 52。切换开关 51 的一个输入端接收图 4 的 GMCH 芯片 6 的输出端。当切换开关 51 传递此数据时,HDMI 发送器 52 可对其执行 HDCP 加密,并通过 HDMI 链路向监视器 2 断言经 HDCP 加密的数据。HDMI 接收器 54 接收 DDR 单元的输出端(例如,图 6 的盘驱动器 4 的 HDMI 发送器 33 的输出端),并将此数据解密。HDCP 逻辑 53 与接收器 54 和发送器 52 一起操作,以允许接收器 54 与 DDR 单元执行 HDCP 认证交换,并允许发送器 52 与监视器 2 中的 HDMI 接收器执行 HDCP 认证交换。从接收器 54 输出的经解密内容或可直接向切换开关 51 的第二输入端断言,或可在调节器 55 中被调节,并且随后调节器 55 的输出向切换开关 51 的第三输入端断言。切换开关 51 可被控制以使其任一输入端处的数据被传递到 HDMI 发送器 52。HDMI 发送器 52 对由切换开关 51 传递的数据执行 HDCP 加密,并将经 HDCP 加密的数据通过 HDMI 链路向监视器 2 断言。

[0161] 在作为从 DDR 单元向 HDMI 接收器 54 转发经 HDCP 加密的数据并由接收器 54 向切换开关 51 (或由接收器向调节器 55、并从调节器 55 向切换开关 51)断言此经 HDCP 加密数据的经解密版本的结果而到达切换开关 51 的情形中,发送器 52 仅需对由切换开关 51 传递的数据执行 HDCP 加密。发送器 52 无需对从图 4 的 GMCH 芯片 6 向切换开关 51 断言、并由切换开关 51 传递给发送器 52 的数据执行 HDCP 加密(相反,发送器 52 可通过 HDMI 链路向监视器 2 发送此数据的未经加密版本)。

[0162] 又如,图 9 的 ADD 卡 60(在图 4 的系统中可替换图 7 的卡 10)包含如图所示地连接

的 HDCP 逻辑 53、HDMI 接收器 54、调节器 55、音频编解码器 70、切换开关 71 及 HDMI 发送器 52。切换开关 71 的一个输入端接收从编解码器 70 输出的音频数据(可由编解码器 70 响应于来自图 4 的 GMCH 芯片 6 的数据而生成)。切换开关 71 的第二输入端接收从图 4 的 GMCH 芯片 6 输出的视频数据。由切换开关 71 传递给 HDMI 发送器 52 的数据在发送器 52 中进行 HDCP 加密,并且该经 HDCP 加密的数据通过 HDMI 链路向监视器 2 断言。HDMI 接收器 54 接收 DDR 单元的输出(例如,图 6 的盘驱动器 4 的 HDMI 发送器 33 的输出),并将此数据解密。HDCP 逻辑 53 与接收器 54 和发送器 52 一起操作以允许接收器 54 执行与 DDR 单元的 HDCP 认证交换,并允许发送器 52 执行与监视器 2 中的 HDMI 接收器的 HDCP 认证交换。从接收器 54 输出的经解密内容或可向切换开关 71 的第三输入端直接断言,或可在调节器 55 中被调节,并且随后调节器 55 的输出向切换开关 71 的第四输入端断言。切换开关 71 可将在其任一输入端处的数据传递给 HDMI 发送器 52。

[0163] 又如,图 10 的媒体 / 图形卡 80 (它可替换图 5 系统的变体中的卡 20,其中数字音频数据与数字视频一起被发送给监视器、但模拟音频不从媒体 / 图形卡输出)包括如图所示地连接的 HDCP 逻辑 53、HDMI 接收器 54、调节器 55、音频编解码器 84、图形加速器 82、帧缓冲器 83、切换开关 71 及 HDMI 发送器 52。切换开关 71 的一个输入端接收从编解码器 84 输出的音频数据(可由编解码器 84 响应于来自图 5 的 GMCH 芯片 16 的数据而生成)。切换开关 71 的第二输入端接收从图形加速器 82 输出的视频数据。该视频数据通常是在图形加速器 82 中响应于来自图 5 的 GMCH 芯片 16 而生成,被写入帧缓冲器 83,然后从帧缓冲器 83 向切换开关 71 断言。由切换开关 71 传递给 HDMI 发送器 52 的数据在发送器 52 中进行 HDCP 加密,并且该经 HDCP 加密的数据通过 HDMI 链路向监视器 2 断言。HDMI 接收器 54 接收 DDR 单元的输出(例如,图 6 的盘驱动器 4 的 HDMI 发送器 33 的输出),并将此数据解密。HDCP 逻辑 53 与接收器 54 和发送器 52 一起操作,以允许接收器 54 执行与 DDR 单元的 HDCP 认证交换,并允许发送器 52 执行与监视器 2 中的 HDMI 接收器的 HDCP 认证交换。从接收器 54 输出的经解密内容或可直接向切换开关 71 的第三输入断言,或可在调节器 55 中被调节,然后调节器 55 的输出向切换开关 71 的第四输入端断言。切换开关 71 可将其任一输入端的数据传递给 HDMI 发送器 52。

[0164] 在另一类实施例中,图 6 的多路复用器 31、解码器 32、HDMI 发送器 33 和 SATA 接口 34 被实现为 PC 的与 DVD 驱动器分离并独立的封闭式子系统(该 PC 甚至可不包含 DVD 驱动器)。例如,多路复用器 31 可被耦合到从因特网向 PC1 断言的接收数据。当多路复用器 31 检测到该数据为不受保护的内容时,多路复用器 31 向 SATA 接口 34 断言该数据。或者(例如,当多路复用器 31 检测到来自控制器 30 的数据是受版权保护的内容时),多路复用器 31 向解码器 32 断言来自控制器 30 的数据。解码器 32 被配置成执行数据(可以是例如高清晰度视频数据或其它视频数据)的解密和解压缩。HDMI 发送器 33 根据 HDCP 协议重新加密结果所得的原数据(例如原视频数据),并将该经重新加密的数据通过 HDMI 链路发送,例如直接发送到 ADD 卡 10 (或其变体)或者媒体 / 图形卡 20 (或其变体)。DDR 单元将优选地实现安全密钥交换、过期和撤消机制(例如,此类机制可在 HDMI 发送器 33 内实现)。

[0165] 在前一段落中给出的示例的变体中,SATA 接口 34 被其它某种类型(例如,PCI、ATA 或 SCSI 接口)的数据接口所替换。更一般化地,预期各种各样的数据传送接口可在体现美国专利申请 No. 10/679,055 的教示的许多类型的开放式系统中的任一种、以及在根据美国

专利申请No.10/679,055的教示配置成嵌入开放式系统的许多所构想的封闭式系统的任一种中使用。在一些情形中(例如,参考图4和6说明的实施例的变体、以及以下参考图5、12和13说明的实施例),该开放式系统采用除SATA接口以外的数据接口来在其各元件之间传送(例如,从PC的HD-DVD驱动器或其它盘驱动器向I/O控制器集线器芯片,其中该开放式系统是一PC)不受保护的数据(或受保护和不受保护的数据两者)。例如,在一些实施例中,该开放式系统采用PCI、ATA或SCSI接口(带合适的连接器)而不是SATA接口(例如,如图6中所示的带连接器34A的SATA接口34、或如图13中所示的带连接器36A的SATA接口36)来在其各元件之间传送不受保护的数据。

[0166] 在往上第二段中所说明的实施例中,解码器32优选被实现为安全解码器(在本发明开放式系统的封闭式子系统的DDR单元内),从而该DDR单元可被用于以与本地HD-DVD盘相同程度的保护来传递基于因特网的内容。在此类实施例的变体中,经加密和压缩的数据经由该DDR单元的SATA端口被提供(例如从因特网)给DDR单元(在PC或其它开放式系统的封闭式子系统中、但不在DVD驱动器内实现),并且该DDR单元仅输出经HDMI重新加密的数据(例如,通过HDMI链路)。

[0167] 例如,如果顾客想要观看最新的流行电影(其中这里有时将“电影”称作“标题”),则可给予该顾客的解码器单元(在该顾客的开放式系统的DDR单元内)在有限时间内有效的一次性密钥。然后电影的拷贝经由因特网发送,在该过程中它用该密钥加密。只有该用户能够观看该标题,并且仅能在有限时间内观看。即使该电影数据被其它某人截取或被保存到盘中,它在任何其它解码器(不拥有该密钥)或在该密钥到期之后的任何时间都将是无用的。

[0168] 一种替换方案是令分发方具有每个标题的在有限持续时间里有效的密钥(例如当日密钥),并且每天(或其它合适的时段)以一新密钥编码每个标题的一个拷贝。当日被授权观看该电影的任何用户将被给予该标题和合适的密钥、以及该密钥的过期时间。一旦该时间过去,该电影实例的任何拷贝将不可播放。在下一日,将为该日的顾客加密一新的版本。

[0169] 开放式系统的封闭式子系统的DDR单元可被用作数字权限管理集线器(例如,在用户家中安装的PDN内)。例如,在图11中,DDR单元92被包括在开放式计算系统95的封闭式子系统中。开放式系统95还包括HD-DVD驱动器90。该封闭式子系统还包括接口电路93。在DDR单元92内,来自驱动器90的经加密的压缩高清晰度视频可被解密、解压缩、并重新加密(根据HDCP协议)。该经重新加密的数据随后可从开放式系统95通过HDMI链路被传送到监视器91。类似地,经加密内容(“CPPM”数据)可从因特网经由接口93向DDR单元92断言。DDR单元92(经由接口93)实现完成CPPM数据的解密所需的任何密钥交换和验证操作,并且DDR单元92随后将该数据解密(如有必要还将其解压缩),然后将结果所得的数据重新加密(优选地根据HDCP协议)。该经重新加密的数据随后可从该开放式系统通过HDMI链路被传送到监视器91。本质上,DDR单元92起到能保存和使用各种用途密钥的库的作用。但是,不止是库,它还包含在该集线器内在受保护格式(例如,HD-DVD和HDCP)之间转换的资源。其结果是这些密钥以及任何外经加密的内容都决不会为非授权使用可用。

[0170] 一般而言,当有各种格式或当格式的集合快速改变时,媒体数据的软件解码(解密和/或解压缩)比硬件解码有优势。此情况在流数据通过因特网为家庭PC可用的当今世界是典型的。有许多竞争的音频和视频格式,并且用户通常在需要时下载解码器程序的新拷

贝。

[0171] 软件解码的一般缺点是它可消耗很大部分的系统处理能力。因为系统之间处理速度和应用负载的变化，一致良好的呈现并不总是可能的。

[0172] 但是，当一格式被标准化并变成通用格式（例如 CD 和 DVD 格式）时，软件解码的优势就微不足道了。通常专用解码器要比现代的 PC 处理器便宜，并且可确保呈现质量一致良好。这是因为与在 PC 上不同，专用解码器上不可能有非预期的应用在运行。

[0173] 硬件解码有优势的另一领域是在保持对内容的知识产权保护上。如果使用的是软件解码，则密钥和经解码的内容将以明文出现在 PC 的存储器系统中。因为其它应用可同时运行，所以恶意的程序可能危害保护系统。此外，家庭用户通常对其系统具有管理员的权限，因此能加载“木马”设备驱动程序或使用其它后门攻击来获得对密钥或内容的访问。一旦大规模生产格式的密钥被危害，内容保护战役实际上就失败了。与之相对，因为专用硬件解码器将不允许其它程序加载并且仅允许经签名的固件更新，所以实际上除了最厉害的解密高手以外，其它所有人均不可能获得访问。

[0174] 专用硬件的使用将不会排除不受版权保护内容的软件解码。体现本发明和 / 或美国专利申请 No. 10/679,055 的教示的开放式系统可区别对待内容生产方的有价值的知识产权和不受版权保护的内容（例如，一些家庭电影）。并且，可实现体现本发明的安全硬件（例如，入口和出口电路）和 / 或开放式系统的封闭式子系统（如美国专利申请 No. 10/679,055 中所说明的）以防止软件（例如，由该开放式系统运行的消费者视频编辑软件）修改受版权保护的内容。

[0175] 美国专利申请 No. 10/679,055 还记载了一种在具有开放式系统架构的计算系统中保护内容并将该内容提供给外部系统的方法，包括以下步骤：(a) 在该计算系统的封闭式子系统中，通过解密以及可任选地对经加密的内容执行其它处理来生成原内容；(b) 在该封闭式子系统中，通过重新加密该原内容来生成受保护的内容；以及 (c) 从该封闭式子系统向该外部系统断言该受保护的内容，而不向该计算子系统提供对该受保护内容的访问。该经加密内容可从该计算系统外部的源接收（例如，经由因特网）。该经加密的内容可以是从盘读取的数字视频数据。步骤 (a) 可包括将该经加密内容解密以生成经解密内容，以及对该经解密数据执行解压缩以生成原内容的步骤。在一些实施例中，数字视频数据是从盘中读取的高清晰度数字视频数据，并且步骤 (a) 包括将该高清晰度数字视频数据解密以生成经解密数据，以及对该经解密数据执行解压缩以生成原内容的步骤。

[0176] 本发明的各个方面是美国专利申请 No. 10/679,055 的教示（如前所述）的一般化。本发明的这些和一些其它方面是在 PDN（可以但不必是参考图 4、5、11 和 12 所说明的任一类型的开放式计算系统）中保护内容的方法和装置。根据本发明的一些方面，明文内容和用于实现内容解密的机密在开放式计算系统或其它 PDN 的硬件（例如，集成电路）内得到保护，并且只要出现在 PDN 中的此类硬件之外总是被加密。

[0177] 如从以下说明显而易见的，图 4、5、11 和 12 中任一个图的开放式计算系统均可体现本发明。例如，如果在图 4 或 5 的盘驱动器 4、或图 12 的盘驱动器 104、或图 11 的 DDR 单元 92 中单个集成电路（实现为芯片的“入口节点”）的硬件中实现了内容转加密（解密并重新加密），并且如果没有任何出现在入口节点中的机密（供执行转加密时使用）以未加密形式为该开放式计算系统的软件或该入口节点之外的其它任何实体（硬件或软件）可访问（例

如，每个此类机密均保留在该入口节点内，或只要出现在该入口节点之外就是经加密的），则图 4、5、11 和 12 中任何一个的开放式计算系统可体现本发明。例如，图 4 的盘驱动器 4 可根据本发明实现为图 6 中所示的其中元件 32 和 33 被实现为集成在单块芯片内的硬件（由此无需安全通道就可在元件 32 内的解密电路与元件 33 内的重新加密电路之间通信）的设备的变体。这一芯片可被配置成包含保密箱电路的入口节点，该保密箱电路被配置成（从外部内容供应方）获得执行期望解密或重新加密操作所需的不在该芯片内呈现的任何机密。可任选地，图 6 的盘驱动器的这一变体被配置成使在驱动器的 SATA 接口 34 接收到的经加密内容（来自外部内容供应方）可被传送到转加密芯片（其中集成了元件 32 和 33，并且被配置成入口节点）内的解密电路，以在该芯片内解密然后重新加密供从该设备输出。

[0178] 我们接下来对能够体现本发明的一类 PDN 进行说明。例如，图 14 的 PDN100 可体现本发明。PDN100 包含被配置成从天线 102 接收已从卫星向天线 102 传送的内容的卫星接收器 120（通常实现为机顶盒）、DVD 播放器 122（能够从盘 103 读取内容）、被配置成接收通过电缆 106 传送的内容的有线接收器 124（通常实现为机顶盒）、以及调谐器 126（能够接收向天线 108 广播的内容并对其执行任何必要的解调）。可任选地，调谐器 126 被配置成用于通过因特网与远程服务器 111 双边通信（例如，向远程服务器 111 发送经 SSL 加密的数据和从其接收经 SSL 加密的数据）。可任选地，接收器 124 具有数字视频记录能力（例如，它被配置成在耦合到接收器 124 的存储单元 131 中记录内容）。

[0179] PDN100 还包含耦合并配置成从元件 120、122 和 124 中的任一个接收音频和视频内容并对其进行处理的音频 / 视频接收器 128，并向视频处理器 132 和监视器 116 之一或其两者断言经处理的内容。PDN100 还包含耦合并配置成从调谐器 126 和接收器 128 之一或其两者接收音频和视频内容、处理该视频内容（例如，通过对其执行调节、格式转换、和 / 或解交织）、以及向监视器 118（以及耦合到监视器 118 的扬声器）断言音频和经处理的视频的视频处理器 132。处理器 132 可任选地还具有数字视频记录能力（例如，被配置成在耦合到处理器 132 的存储单元 133 中记录经处理的内容）。

[0180] 监视器 118 和扬声器由 HDMI 串行链路耦合到视频处理器 132，并且监视器 116 和扬声器（未示出）由另一 HDMI 串行链路耦合到接收器 128。

[0181] PDN100 还包含耦合并配置成从接收器 124 接收音频和视频内容、并向监视器 113、耦合到监视器 113 的扬声器、以及可任选地还有其它显示或回放设备断言该音频和视频（或其经处理的版本）的个人计算机（“PC”）130。监视器 113（和扬声器）可由 DVI 链路、HDMI 链路或另一链路耦合到 PC130。

[0182] PDN100 的这些元件以适合其特定实现的方式，诸如通过公知的 WiFi、以太网、、HPNA、MOCA、USB、HomePlug 和 1334 链路中的一个或多个相互耦合。

[0183] 当 PDN100 根据本发明的典型实施例实现时，元件 120、122、124、126、128、130 和 132 中的每一个均为包含实现下述的保密箱电路以及入口电路和出口电路之一或两者的硬件的节点。例如，个人计算机 130 可包含保密箱芯片，元件 120、122、124 和 126 中的每一个均可包括一含保密箱和入口电路的芯片，元件 128 和 132 中的每一个均可包括一含保密箱和出口电路的芯片，而元件 120、122、124、126、128、130 和 132 中的每一个的保密箱电路都可被耦合并配置成用于经由软件（在 PC130 上运行）与元件 120、122、124、126、128、130 和 132 中的另一个通信。尽管图 14 没有示出用于 PC130 与元件 120、122、124、126、128 和

132 中的每一个之间的双边通信的链路，但是当 PDN100 是根据本发明的典型实施例实现时(例如，由此可经由 PC130 中的软件在沿 PC130 中的 PCI 总线连接的保密箱芯片与元件 120、122、124 和 126 中的任一个的包含保密箱和入口电路的芯片之间、或在沿 PC130 中的 PCI 总线连接的保密箱芯片与元件 128 或 132 中包含保密箱和出口电路的芯片之间交换经加密消息)，则存在此类链路。

[0184] 考虑其中 PDN100 是根据本发明的一个实施例实现的，并且元件 128、130 和 132 中的每一个均为包含保密箱电路和出口电路的节点的一个示例。在此例中，元件 128、130 和 132 中的每一个里的出口电路可用于(倘若已获得了必要的密钥数据)将受控内容(例如，从 PDN100 的另一元件接收的经转加密内容、或是在进入 PDN100 时已为 PDN 加密格式的受控内容)解密以生成经解密内容。优选的是，以使明文形式的内容以及出口电路用来对该内容的任何版本执行授权操作的任何机密可为在 PDN100 的任何元件上运行的软件访问、并使该内容除在安全硬件内以外决不会以明文形式出现在 PDN100 内的方式实现解密。在此例中，元件 128、130 和 132 中的每一个里的出口电路还可用于向 PDN100 之外的实体(分别是元件 116、113 或 118) 断言经解密内容(或其经处理的版本)。在此例的变体中，元件 128、130 和 132 中的每一个里的出口电路可用于向出于某些目的而在 PDN100 内部(例如，其包含在该 PDN 内部的一子系统)、但处于其它目的而在 PDN100 外部(例如，它包括该 PDN 内部的一子系统) 的实体(例如，元件 116、113 或 118 的变体) 断言经解密内容(或其经处理的版本)。一般而言，在根据本发明的 PDN 的出口电路中生成的经解密内容(或该经解密内容的经处理版本) 在一些情形中在该 PDN 内显示(或者“消费”)，而在其它情形中在该 PDN 之外消费。

[0185] 当然，除图 14 的 PDN100 以外的许多类型的个人数字网络(例如，比 PDN100 更简单或更复杂的 PDN)可体现本发明。例如，在一类实施例中，本发明是一种具有开放式架构、并包括 CPU (以软件编程)和被配置成接收经加密视频和音频内容(例如，通过从高清晰度 DVD 或其它盘读取该内容)、显示该内容的视频部分、并完成该内容的音频部分的回放的至少一个外围设备的计算系统。并且，如前所述，图 4 或图 5 的 PC1 也可体现本发明。

[0186] 在典型实施例中，本发明的 PDN 包含设备或组件(本文中有时称为该 PDN 的“节点”或“成员”)，每个设备或组件都包含保密箱电路，该保密箱电路被耦合并配置成与该 PDN 的至少一个其它节点的保密箱电路双边通信。每个节点可任选地包括入口和 / 或出口硬件(稍后说明) 以及保密箱硬件。每个节点本身是本发明的另一个方面。

[0187] 包含入口电路(本文中有时将入口电路称为入口单元) 以及保密箱电路的节点将被标示为“入口节点”。包含出口电路(这里有时将出口电路称为出口单元) 以及保密箱电路的节点将被标示为“出口节点”。每个入口节点和出口节点均能够接收受内容限制级约束的内容(例如，数字视频数据和数字音频数据之一或其两者)，并被配置成以不为该使用限制级所禁止的至少一种方式(以及可任选的，以多种或所有方式) 使用该内容。

[0188] 在本发明 PDN 的一些实施例中，每个节点内的保密箱、每个入口节点内的入口电路、以及每个出口节点内的出口电路以硬件实现。在本发明 PDN 的一类实施例中，每个保密箱、每个入口节点内的入口电路、以及每个出口节点内的出口电路被实现为集成电路或多芯片集(可包括以固件编程的微处理器)，但不包括以软件编程的 CPU。在其它实施例中，体现本发明的 PDN 的每个节点可任选地还包括以固件或软件编程的受每个节点被配置成使

机密(未加密形式)在该节点内仅可用硬件处理而不向该节点中的软件或固件泄露任何未加密机密的限制的至少一个元件。在其它实施例中,在安全地嵌入 PDN 的节点内的处理器上运行的固件可访问明文内容和/或用于内容的重新加密(在入口单元中)或经重新加密内容的解密(在出口电路中)的机密,但该明文内容以及任何此类机密都不出现在该 PDN 的可为寻求获得对其未授权访问的用户或实体访问(或至少容易访问)的任何节点、链路或接口中。经加密的机密(例如,已根据本发明在节点中用硬件加密的机密)可被泄露(以经加密形式)给该节点内的软件或固件、或该节点之外的实体。每个入口节点内的入口电路、以及每个出口节点内的出口电路包含安全硬件,并且可任选地还包括以固件或软件编程的至少一个元件,但每个节点中的入口电路和/或出口电路被配置成仅在硬件中处理机密(未加密形式),而不将任何此类机密(未加密形式)泄露给该节点之外的任何实体或该节点中的软件或固件。

[0189] 节点内的保密箱通常包括(但无需包括)安全硬件,并可以但无需包括以固件或软件编程的至少一个元件。在一些实施例中,保密箱(例如,元件 120、122、124、126、128、130 和 132 中的任一个内的保密箱)完全由硬件(或包括用固件编程的微处理器的硬件)组成。在其它实施例中,保密箱(例如,元件 120、122、124、126、128、130 和 132 中的任一个内的保密箱)是以固件或软件编程的处理器或计算系统、或包括此类处理器或计算系统(例如,图 14 的一些实现的 PC130 的 CPU 可用起到元件 120、122、124、126、128、130 和 132 之一的保密箱作用的软件编程,从而 PC130 与元件 120、122、124、126、128、130 和 132 中相关的一个一起用作 PDN 的节点)。保密箱可用管理密钥库或从该保密箱和另一保密箱往返移动消息的软件编程。在一些实施例中,PC(例如,图 14 的一些实现的 PC130)本身起到 PDN 的节点的作用,例如,在该 PC 包含完全由硬件构成的保密箱的情形中,以及在该 PC 的 CPU 以起到保密箱作用的软件编程的情形中。但是,更一般化地,每个节点(以及节点内的每个保密箱)被配置成仅以不将任何机密泄露(以未加密形式)给该节点之外的任何实体(或该节点内的软件或固件)的方式来处理机密(用于包含该节点的 PDN 中的内容保护)。如果保密箱用软件实现,则该保密箱软件将必须以苛刻的方式被限制(至少在该软件可访问经加密的机密时,它不能将这些机密解密,由此该软件不能有效地变更对要由包含该保密箱的 PDN 保护的内容的任何使用限制集)。在一类实施例中,节点(和/或节点内的保密箱)被配置成在安全硬件中以防止任何机密被泄露(以未加密形式)给该节点之外的任何实体(或在该节点内存在软件或固件的情况下,被泄露给该节点内的软件或硬件)的方式处理机密(供包含该节点的 PDN 中的内容保护所用)的未加密版本。

[0190] 将参考图 15 对本发明的一类实施例进行说明。在这些实施例中,本发明是一种具有开放式架构并包含沿总线(例如,PCI 总线)连接的设备的计算系统。该系统被配置成接收经加密视频和音频内容(例如,通过从高清晰度 DVD 或其它盘读取该内容,或接收广播内容或通过电缆传送的内容),并可显示该内容的视频部分并播放其音频部分。图 15 是这一系统的一部分的框图,包括 PCI(外围通信互连)总线、CPU147、耦合到 PCI 总线的 I/O 控制器(例如,“南桥”芯片或“I/O 控制器集线器”)145、以及耦合在控制器 145 与 CPU147 之间的图形和存储器控制器(例如,“北桥”芯片集或“图形和存储器控制器集线器”)。存储器 149 和图形处理单元(“GPU”)150 被耦合到控制器 146。

[0191] GPU150 被耦合到外部视听系统,该外部收听系统通常包含监视器(例如,含 HDMI

接收器的 HDTV 监视器）和由该监视器驱动的扬声器。

[0192] 另外三个芯片（或芯片集）沿该 PCI 总线连接：包括调谐器和解调电路 143 以及电路 144（含入口和保密箱电路）的芯片（或芯片集）140、包含保密箱电路 151 和存储电路 152 的芯片（或芯片集）142、以及包含电路 154（含出口和保密箱电路）以及解码器电路 155 的芯片（或芯片集）148。为简明起见，电路 140、142 和 148 将被称为“芯片”，尽管它们可能是多芯片集或单块芯片。如果电路 140、142 和 148 中的任何一个被实现为多芯片集，则该芯片集应被实现为使得其中的明文内容以及其中的任何未加密机密（例如，未加密密钥数据和 / 或证书）决不会被曝露在该芯片集的各芯片之外，或者以其它方式使其受到保护而不被该芯片集之外的任何实体访问（以未加密形式）。可任选地，外部存储单元 153 被耦合到存储电路 152。通常，芯片 140、142 和 148 被实现为配置成能方便地插入到个人计算机中的卡（例如，“多媒体图形卡”）。

[0193] 为便于说明，在本文中有时将保密箱电路 151 称为“保密箱”151。并且，块 144 内的入口电路有时被称为入口单元，而块 154 内的出口电路有时被称为出口单元。

[0194] 在一典型实现中，电路 143 被配置成接收和解调广播视频，并向电路 144 的入口电路断言视频和音频（指示所接收的内容）。通常，向入口单元断言的数字内容是加密的，并且该入口单元被配置成将其解密（将其变成明文形式），并在该明文内容被曝露在该入口单元外之前将该明文内容加密（即，假定在其被入口单元接收时加密的情况下将其重新加密）。经重新加密的内容随后经由 PCI 总线向该系统的另一元件断言。如将在以下更加详细地说明的，入口单元（电路 144 内）使用对中间人攻击免疫的加密协议将该内容重新加密。在一典型实现中，单元 144 使用常规 256 位高级加密标准（“AES”）协议的公知计数器（“CTR”）模式变体来将内容重新加密。因为该内容在硬件中（在电路 144 中）被解密为明文形式，然后根据本发明在其离开该解密硬件之前被重新加密，所以内容在图 15 的系统中得到很好的保护。

[0195] 在本发明的所有实施例中，用于重新加密（在入口单元中）的密码协议应对中间人攻击免疫。在典型实施例中，该密码协议还应允许经重新加密的内容由不与其中生成该经重新加密内容的入口节点直接（实时地）通信的出口节点解密。取决于特定应用，满足这些标准的第一准则并优选地还满足其中第二准则的许多不同密码协议中的任一种可能适合。例如，在至少一些应用中，入口节点可被实现为执行根据 AES 协议的更强变体中的任一种的重新加密。在许多应用中，256 位 AES 协议的 CTR 模式变体很可能合适，因为它是更强 AES 变体之一，易于在集成电路中用硬件（例如，流水线电路）实现，并且具有可验证的安全特性。在 AES 协议的其它操作模式当中还有“输出反馈”（OFB）模式、“密码反馈”（CFB）模式、“电子密码本”（ECB）模式、以及“密码分组链接”（CBC）模式，其中任何一种模式均适合在本发明的一些实施例中实现入口节点。体现本发明的节点可被实现为采用至少两种不同密码协议中选定的任一种来将要与其它节点共享的内容重新加密。优选的是，节点将被实现为采用不多于少数几种不同的协议来将要在各节点间共享的内容重新加密，从而降低实现每个节点的成本并使可互操作性最大化。

[0196] 进入图 15 的系统（经由芯片 140）的内容伴随着使用限制集（定义如上）。指示该使用限制集（以及与每个此类集合相关联的至少一个机密）的基元被持久地预先存储在芯片 142 内的保密箱 151（或与保密箱 151 相关联的存储单元 153）中。通常，在芯片 140 开

始接收、解密和重新加密内容之前，保密箱 151 将已确认芯片 140 被授权执行这些操作，并向芯片提供执行这些操作所需的任何机密（例如，内容密钥）。由保密箱 151 使用的这些基元和机密可被存储在保密箱 151 内的非易失性存储器（或易失性存储器）中，或存储在远离保密箱 151 但仅可由保密箱 151 访问其未加密形式（例如，经由存储电路 152 以安全方式）的存储器（例如，存储单元 153）中。例如，卫星供应商可将这些基元和机密加载到保密箱 151 中（在确立保密箱 151 被授权接收这些信息之后），并且当保密箱 151 确定合适（通常作为通过安全通道与电路 144 或 154 内的保密箱电路的交换的结果）时，保密箱 151 可将这些机密中相关的那些作为内容密钥提供给电路 144 内的保密箱电路（和 / 或电路 154 内的保密箱电路）。

[0197] 在一些应用中可能优选的是从图 15 的系统中省略元件 152 和 153，而改为在保密箱 151 内包含充足的非易失性存储器以满足保密箱 151 的所有持久存储需要。在其它应用中，可能优选的是实现带较少非易失性存储器（或不带非易失性存储器）的保密箱 151，并提供存储电路 152（沿 PCI 总线连接）和存储单元 153（耦合到电路 152）以根据需要以安全方式允许保密箱 151 从单元 153（经由电路 152）读取数据并将该数据高速缓存（在保密箱 151 内的存储器中）。例如，存储在单元 153 中的所有数据（也可由保密箱 151 经由电路 152 访问）可以是经加密数据。此经加密数据可在被高速缓存在保密箱 151 中或由其使用之前被解密（在保密箱 151 内）。当保密箱 151 发起从单元 153 访问该数据的读操作时，此类数据可用加密形式从单元 153 经由电路 152 传送到保密箱 151。

[0198] 存储单元 153 通常是非易失性存储单元，但（在一些实施例中）可以是易失性存储器。在一些实施例中，保密箱 151 包含易失性存储器但不包含非易失性存储器。

[0199] 通常，在上电时，通过使用标准密码手段使得建立各安全通道的过程（以及一旦安全通道被建立时使用该安全通道的操作）不易受攻击（优选地不易受所有攻击，包括但不限于中间人攻击、蛮力攻击、差分错误分析攻击、以及重放攻击），电路 144 内的保密箱电路与保密箱 151 建立安全通道，并且电路 154 内的保密箱电路与保密箱 151 建立安全通道。当该过程不易受中间人攻击时，可访问在电路 144（或 154）与保密箱 151 之间发送的消息（例如，在建立安全信道之前的认证交换期间）的设备（“人”）既不能读取这些消息，也不能生成预期接收方可理解的消息的经修改版本。重放攻击能容易地通过标准密码手段来防止，例如通过将设备（电路 144 和保密箱 151、或电路 154 和保密箱 151）配置成使用一次性的随机会话密钥（用于一次会话）用于在设备之间建立安全通道。中间人可拒绝服务（即，中断安全通道的建立），但这是它能成功实现的唯一攻击。

[0200] 当电路 144 准备好接收和处理内容时，电路 144 内的保密箱电路可向保密箱 151（经由以下述方式建立的安全通道）发送请求以确定电路 144 是否被授权解密和重新加密该内容。保密箱 151 可进行此确定，因为来自电路 144 的请求规定了将对该内容进行的使用，并且因为保密箱 151 知道对该内容的什么用途是被使用限制集所禁止的，并且保密箱 151 知道电路 144 的身份和能力（因为在保密箱 151 与电路 144 之间建立安全链路的交换期间，电路 144 已向保密箱 151 证明其身份），并且因为保密箱 151 被配置成将该请求内的相关数据与指示使用限制集所禁止的使用的数据相比较。如果保密箱 151 确定电路 144 被授权执行所请求的操作（例如，将内容解密并重新加密），则保密箱 151 向电路 144 提供电路 144 内的入口电路执行这些操作所需的机密（即，内容密钥）。电路 144 内的入口电路不持久地存

储该密钥(它没有用于存储的存储器),仅可对内容执行该机密使其能够执行的操作,并仅可在该密钥有效的有限时间里(例如,在一会话期间)执行这些操作。

[0201] 当电路 144 (或电路 154,如下将说明地)已从保密箱 151 接收到内容密钥时,通常有与电路 144 (或 154)能使用该密钥来做什么相关联的限制。单元 144 和 154 的每一个均被构建成各自必须遵照此类限制。例如,密钥可授权电路 154 解密内容,使用 HDCP 协议将该经解密(明文)内容重新加密,并使该经 HDCP 加密的内容通过 HDMI 链路被传送,前提是如果电路 154 确定 HDCP 安全已被破坏(即,如果电路 154 确定 HDMI 接收器不是被授权的),则 HDCP 加密和 HDMI 传送操作必须停止。单元 144 和 154 的每一个均被构建为仅可确切地以授权方式操作。

[0202] 为了使内容离开图 15 的系统,该内容(经重新加密的形式)必须通过 PCI 总线向芯片 148 断言以在芯片 148 内通过电路 154 内的出口电路解密。芯片 148 通常还重新加密该明文内容(例如,使用 HDCP 协议)以输出明文内容但不在芯片 148 之外曝露该明文内容(例如,该内容在其离开芯片 148 之前被重新加密以从图 15 的系统输出)。芯片 148 内的电路(例如,解码器 155)也对经解密(明文)内容执行任何必要的解压缩,并可任选地还对经解密和解压缩的明文内容执行其它处理(例如,格式化和 / 或重新加密以供输出)。例如,在一些实现中,芯片 148 将明文内容变为 HDMI (或 DVI)格式,供向图形处理单元 150 输出并从单元 150 通过 HDMI (或 DVI)链路向外部设备或系统输出,包括通过使用常规用来将要通过 HDMI (或 DVI)链路传送的数据加密的 HDCP 协议来重新加密该内容。如将在稍后更加详细地说明的,芯片 148 仅能以授权方式和授权格式(向 GPU150)输出内容。例如,如果图 15 的系统被授权通过 HDMI 链路以经 HDCP 加密的格式输出内容,则芯片 148 使用 HDCP 协议来重新加密内容并以经 HDCP 加密的 HDMI 格式向 GPU150 断言之供从 GPU150 通过 HDMI 链路传送,从而仅被许可的 HDMI 接收器(例如,在高清晰度监视器中)能解密并显示该经 HDCP 加密的内容。又如,如果图 15 的系统被授权输出明文内容的模拟版本,并且芯片 148 包括 DAC (数模转换电路),则芯片 148 将使用该 DAC 来生成指示明文内容的模拟信号,并将该模拟信号输出到 GPU150 或可由图 15 的系统之外的设备或系统(例如,模拟显示设备)访问的连接器(未示出)。为了规避由图 15 的系统提供的保护,将需要执行非常困难(并且通常是不实际)的操作来闯入一块或多块芯片 140 和 148、并修改(或本质上修改)每个开放的硬件单元内的电路。

[0203] 当电路 154 内的出口电路准备好接收和处理经重新加密的内容(来自沿 PCI 总线连接的设备)时,电路 154 可向保密箱 151 (经由以下述方式建立的安全通道)发送请求以确定电路 154 是否被授权解密和进一步处理该内容。保密箱 151 可进行此确定,因为来自电路 154 的请求规定了要对该内容进行的使用,并且因为保密箱 151 知道对内容的什么用途是为使用限制集所禁止的,并且保密箱 151 知道电路 154 的身份和能力(因为在保密箱 151 与电路 154 内的保密箱之间建立安全链路的交换期间,电路 154 已向保密箱 151 证明其身份),并且因为保密箱 151 被配置成将该请求中的相关数据与指示由使用限制集禁止的用途的数据相比较。如果保密箱 151 确定电路 154 被授权执行所请求的操作(例如,将该经重新加密的内容解密并进一步处理),则保密箱 151 向电路 154 提供电路 154 执行这些操作所需的机密(即,内容密钥)。电路 154 内的出口电路不持久存储该密钥(它没有用于存储的存储器),仅能对该内容执行该机密使其能够执行的那些操作,并仅可在该密钥有效的有限时间

(即,在一会话期间)里执行这些操作。

[0204] 用于保密箱 151 与电路 144 (或电路 145)内的保密箱电路之间的双边通信的安全通道可用各种不同方式中的任一种来建立,包括用以下参考图 18 和 19 说明的其中在图 18 的各保密箱之间建立安全通道的方式。

[0205] 在图 15 的实施例的变体中,芯片(或芯片集)142 被省略。在此类替换实施例中,芯片 140 和 148 的每一个(各为一芯片集)将根据需要使用其自己的保密箱电路(例如,块 144 内的保密箱电路),以例如从其它保密箱电路获得所需的密钥。

[0206] 一般而言,可采用两种不同认证协议中的任一种在本发明 PDN 的各设备(例如,保密箱)之间进行通信 :显式(例如,二阶段)认证 ;和隐式(例如,一阶段)认证。在设备相互陌生的情况下应使用显式认证,并且显式认证通常采用公钥密码和全认证交换(包括证书)。在设备必然相互知道(例如,因为在制造这些设备的过程中永久建立的基本关系)的情况下可使用隐式认证。显式认证协议基本是在黑盒之间,因而它们必须被很好地标准化(在 PDN 的所有节点(除了在单块芯片内的节点实现、以及可能还有在单个封闭式系统内实现的节点)、以及潜在可能成为该 PDN 的节点的所有设备被配置成在它们相互通信时使用相同的(标准)显式认证协议的意义上)。隐式认证协议通常在芯片内(或可能地,在 PDN 的单个封闭式子系统内的各设备之间)使用,并且可以是非标准化的和应用相关的。例如,如果保密箱和入口电路在同一块芯片内,则它们之间的通信根本不需要任何特殊协议。或者,如果两个设备在由同一制造商制作的不同芯片中实现,并且特别设计成一起工作,则可使用专用协议来进行它们之间的通信,只要该专用协议充分隐藏机密即可。

[0207] 在一类实施例中,本发明 PDN 被配置成防止 PDN 内的内容以使该内容能在该 PDN 之外以非授权方式使用的形式从该 PDN 移除,并防止内容在该 PDN 内以非授权方式使用。进入这一 PDN 的内容立即由入口硬件(通常实现为集成电路)转加密(解密并重新加密),除非该内容已根据该转加密操作的重新加密阶段所使用的相同协议被重新加密,并且明文内容以及 PDN 用来执行解密和重新加密的任何未加密机密在该 PDN 的集成电路之外都不可访问。从入口电路输出的经重新加密内容可在该 PDN 的各设备间自由传送(即使是以不安全的方式),可由该 PDN 内的软件访问,或甚至可由该 PDN 之外的硬件或软件访问,并且可用不安全的方式存储在该 PDN 的设备中(例如,存储在该 PDN 的盘驱动器中的盘上)。仅该 PDN 内的出口电路就将具有解密该经重新加密的内容以生成该内容的明文版本所需的机密。该出口电路仅可从该 PDN 内的保密箱,并且仅在该出口电路向该保密箱证明其身份、并向该保密箱证明该出口电路被授权以对该内容执行规定的操作,并且在该保密箱与出口电路之间建立起用于从该保密箱向该出口电路传送这些机密的安全通道之后获得这些机密。由此,即使该经重新加密的内容被从该 PDN 移除(例如,如果包含该经重新加密数据的盘从该 PDN 移除),该经重新加密的内容也不能(实际上)以未授权方式解密或使用。经重新加密的内容已被加密成该 PDN 独有的形式,从而该 PDN 无需操心如何保护该经重新加密的内容。相反,在现有技术中提出了通过试图将内容安全地锁定在 PDN 的每个元件内并试图保护 PDN 各元件之间的所有链路来在 PDN 内保护内容。

[0208] 将参考图 16 和 17 对本发明的个人数字网络(PDN)的一类实施例进行说明。图 16 的 PDN168 体现本发明并包括如图所示地连接的入口节点 160 (实现为集成电路,并包括保密箱和入口电路)、节点 161 (实现为另一集成电路,并包括保密箱电路)、出口节点 162 (实

现为第三集成电路，并包括保密箱和出口电路）、视频处理器 175、存储控制器 176、以及视频处理器 177。存储单元 178 被耦合到控制器 176 并由其控制，并且在 PDN168 之外。内容供应方 163 和节点 161 内的保密箱电路被配置成在彼此之间建立安全信道 164，并通过该信道彼此通信。内容供应方 163 在图 17 中没有示出，因为图 17 假设内容供应方 163 已向节点 161 提供了权限数据 190 和密钥数据 191，该数据 190 和 191 已被存储在节点 161 内保密箱电路中的非易失性存储器里，并且内容供应方 163 与节点 161 之间的通信已经终止。

[0209] 根据本发明由入口电路（例如，在图 15 的电路 144 或图 16 的节点 160 内）用来将经解密（明文）内容重新加密、以及由出口电路（例如，在图 15 的电路 154 内或图 16 的节点 162 内）用来将该经重新加密的内容解密的重新加密协议应对中间人攻击免疫。通常，该重新加密协议不是要求经加密数据的发送方和接收方（将接收并解密该数据的设备）在包含发送方与接收方之间的认证交换、会话期间要使用的密钥数据的确定（例如，发送方和接收方中密钥数据的生成，或从密钥给予方向需要该密钥数据的各设备提供密钥数据）、以及该经加密数据向接收方的传送的会话中彼此直接通信的链路保护协议（例如，HDCP 协议）。相反，该重新加密协议通常是仅要求转加密电路到内容转加密开始时已经获得了执行转加密所需的密钥数据，而不要求密钥给予方、转加密电路和内容供应方直接相互通信（例如，在单次会话期间“实时”通信）的类型的协议（例如，CTR 模式的 256 位 AES 协议）。在本发明 PDN 的优选实施例中，在不同节点的保密箱之间建立安全链路所需的证书被预先存储在这些保密箱中。或者，当使用自证明类型的非对称加密在保密箱之间建立安全链路时，用于建立该安全链路的证书蕴含在链路建立交换期间由保密箱执行的数学计算中，因此不需要在保密箱中预先存储任何证书供在这一交换中使用。一旦建立起安全链路，一保密箱就通过该安全链路向另一保密箱发送内容密钥。内容密钥既可起到使入口电路开始接收、解密和重新加密内容的指令（或使出口电路开始接收和解密经重新加密内容的指令）的作用，又可作为入口（或出口）电路执行授权密码操作所需的密钥。每个入口节点（根据定义包含入口电路）被配置成不首先从保密箱接收到相关指令（例如，以密钥形式）就不能操作以接收和转加密内容。每个出口节点（根据定义包含出口电路）被配置成不首先从保密箱接收到相关指令（例如，以密钥形式）就不能操作以接收和解密经重新加密的内容。本发明依赖于保密箱之间、以及保密箱与内容供应方之间的信任链，但不要求（在典型实现中）所有保密箱和内容供应方直接彼此通信（例如，在单次会话期间“实时”通信）。相反，在本发明 PDN 的优选实施例中，这些保密箱和内容供应方实际上能间接彼此通信（不是实时地或在单次会话中）。

[0210] 在图 16 的示例中，证书数据 170 被存储在入口节点 160 中，证书数据 171 被存储在节点 161 内的保密箱电路中，并且证书数据 172 被存储在节点 162 内的保密箱电路中。证书数据 171 可在制造时存储在节点 161 中。证书数据 170 和 172 可包含在制造节点 160 和 162 时分别存储在节点 160 和 162 中的数据，并且还可包括在其中节点 160 和 162（或包括其中每一个的设备）被识别为 PDN168 的元件的“结婚”操作（下述类型）期间由节点 161 分别存储在节点 160 和 162（在制造之后）中的数据（例如，确定下述类型的“结婚证书”的数据）。在节点 161 内的保密箱电路响应于来自入口节点 160 的对密钥（节点 160 内的入口电路对所要接收的内容执行转加密操作所需）的请求之前，入口节点 160 和节点 161 必须已使用预先存储的证书数据 170 和 171 执行认证交换，以（在其间）建立通过其可将密钥从节点

161 传送到入口节点 160 的安全通道 165。然后，当入口节点 160 想要接收、解密和重新加密内容时，入口节点 160 内的保密箱电路通过该安全通道向节点 161 内的保密箱电路断言密钥请求。该密钥请求指示要对该内容执行的操作(例如，该密钥请求包含指示要对该内容执行的操作的权限数据 180)。该保密箱随后通过例如将来自节点 160 的权限数据 180 (在图 17 的节点 161 内标识为标有问号的星形)与指示入口节点 160 被授权执行的操作的权限数据 190 (预先存储在节点 161 中)相比较来确定是否准许该密钥请求。如果节点 161 决定准许该密钥请求，则节点 161 通过安全通道 165 向入口节点 160 发送该密钥(例如，图 17 的密钥数据 181)。节点 160 内的入口电路不具有其中可存储该密钥的非易失性存储器，由此在节点 160 上电之后(在断电之后)该密钥不能被入口电路使用。

[0211] 在本发明 PDN 的一些实施例的操作中，一外部设备(例如，由内容供应方操作的设备)向(PDN 的)保密箱传送权限数据(该 PDN 确立该 PDN 的哪些元件被授权执行内容转加密所需)和该 PDN 的元件执行内容转加密所需的密钥数据。保密箱持久地存储这些权限数据和密钥数据(例如，存储在该保密箱内的非易失性存储器中)供以后使用。例如，如图 16 中所示，内容供应方 163 可向节点 161 内的保密箱电路传送权限数据 190 和密钥数据 191，并且保密箱电路然后可持久地存储数据 190 和 191，如图 17 所示。更具体地，在图 16 和 17 的示例中，内容供应方 163 和节点 161 内的保密箱电路建立一安全通道 164 (在执行认证交换以建立信任关系并确立节点 161 被授权接收密钥数据和权限数据)。然后内容供应方 163 经由通道 164 向节点 161 发送权限数据 190 和密钥数据 191。节点 161 内的保密箱电路将数据 190 和 191 存储在节点 161 内的非易失性存储器中。然后，当入口节点 160 内的入口电路准备好从外部源(例如，从内容供应方 163 或由内容供应方 163 授权的源)接收内容时，入口节点 160 (从该内容供应方)获得指示该内容供应方认为入口节点 160 将对要提供给入口节点 160 的内容执行的操作的权限数据 180。入口节点 160 内的保密箱电路随后通过安全通道 165(在节点 160 上电时已在节点 160 与 161 之间建立)向节点 161 内的保密箱电路断言一请求。该请求包含权限数据 180。响应于该请求，保密箱将权限数据 180 与权限数据 190 (预先存储在节点 161 中)相比较。权限数据 190 指示入口节点 160 被授权(或不被授权)执行的操作。如果作为数据 180 与数据 190 比较的结果，节点 161 中的保密箱电路决定准许该密钥请求，则节点 161 通过安全通道 165 将密钥数据 181 (指示内容密钥)发送给入口节点 160。在入口节点 160 已获得密钥数据 181 之后，其入口电路开始从内容供应方接收经加密内容，并使用密钥数据 181 将该经加密内容转加密，并向视频处理器 175 断言经转加密内容(通常包含视频和音频内容)。处理器 175 可经由视频处理器 177 向出口节点 162 断言该经转加密内容，或可将该经转加密内容向存储控制器 176 断言，并由其使该经转加密内容被存储在存储单元 178 中(例如，供后续读出并经由处理器 177 向出口节点 162 断言)。节点 160 内的入口电路不具有能在其中存储密钥数据 181 的存储器，因此在入口节点 160 上电之后(在断电之后)密钥数据 181 不能由入口电路使用。

[0212] 当节点 162 内的出口电路准备好向域 168 之外的设备断言内容时(或在此前)，出口节点 162 获得指示要由出口节点 162 对该内容执行的操作的权限数据 195，并且节点 162 内的保密箱电路通过安全通道 166 (在节点 162 上电时在节点 162 与 161 之间建立)向节点 161 内的保密箱电路断言一请求。该请求包括权限数据 195。响应于该请求，该保密箱将权限数据 195 与权限数据 190 (预先存储在节点 161 中)作比较。权限数据 190 指示出

口节点 162 被授权(或不被授权)执行的操作。如果作为数据 195 与数据 190 比较的结果，节点 161 内的保密箱电路决定准许该密钥请求，则节点 161 通过安全通道 166 向出口节点 162 发送密钥数据 194 (指示密钥)。在任何可能的情况下(即，只要使用权限允许)，就可在节点 162 内的出口电路准备好向外部设备断言内容之前在这些保密箱之间交换权限数据、请求、及密钥数据来改善用户体验(例如，在节点 162 是移动 MP3 或视频播放器或仅偶尔连接到 PDN 的其它设备或在其内实现时)。在出口节点 162 已获得了密钥数据 194 之后，它开始从 PDN178 的元件(例如，从处理器 177)接收受控内容，使用密钥数据 194 将此内容解密(并可任选地还对其执行其它处理)，并将经解密内容格式化(和 / 或重新加密)以供向预期目的地输出。例如，节点 162 内的出口电路可格式化经解密视频和音频内容供通过 HDMI 链路向与 PDN168 之外的监视器相关联的 HDMI 接收器传送。节点 162 内的出口电路不具有可在其中存储密钥数据 194 的非易失性存储器，因此在出口节点 162 上电之后(在断电之后)密钥数据 181 不能被入口电路使用。

[0213] 从前例应当认识到，仅在入口节点 160 已向节点 161 “证明”入口电路 160 被授权对内容执行规定操作之后(例如，仅在入口节点 160 向节点 161 证明入口节点 160 是被许可设备之后)，并且仅在节点 161 向入口节点 160 证明(例如，在用于建立安全通道 165 的认证交换期间)节点 161 是被许可设备之后，密钥数据 181 才被给予入口节点 160。类似地，仅在出口节点 162 向节点 161 “证明”出口节点 162 被授权对内容执行规定操作(例如，仅当出口节点 162 向节点 161 证明出口电路 162 是被许可设备之后)，并且仅当节点 161 已向出口节点 162 证明(例如，在用于建立安全通道 166 的认证交换期间)节点 161 是被许可设备之后，密钥数据 194 才被给予出口节点 162。

[0214] 接下来，我们参考图 18 和 19 对根据本发明的一些实施例执行以在保密箱之间建立安全通道(例如，图 16 和 17 的通道 165 和 166)的多个步骤的示例进行说明。此例仅为示例性，而并不旨在表示可在保密箱和 / 或本发明 PDN 的实施例的其它元件之间建立安全通道的唯一方式。图 18 和 19 各自是其中元件 200 代表本发明 PDN 的一个实施例的软件(例如，编程图 15 的 CPU147 的软件)的逻辑软件示图，并且软件 200 与 PDN 的三个节点(入口节点、出口节点、及第三节点)之间的硬件接口由虚线表示。其中每个节点由硬件(通常包括执行固件的微处理器，诸如图 20、21 和 22 的微处理器 240、260 或 280)构成，但不包括可编程的通用 CPU 或软件。其中每个节点包含保密箱电路，但只有入口节点包含入口电路(未示出)，并且只有出口节点包含出口电路(未示出)。第三节点将称为“保密箱”节点，因为它包括保密箱电路但不包括入口或出口电路。

[0215] 更一般化地，在本发明 PDN 的一类优选实施例中，至少一个节点的保密箱电路可包含以安全方式嵌入该节点的硬件中(优选在集成电路内)的决策逻辑或在安全地嵌入节点中的处理器上运行的决策固件。在这一节点中，保密箱电路可包括安全地嵌入这一节点内的处理器，并且在该处理器上运行的固件可访问密钥数据或该节点内用来支持或用于对内容执行授权操作的其它机密，但此类机密都不应以可为寻求获得对其未授权访问的用户或实体访问(或至少容易访问)的方式出现在该节点中。

[0216] 参见图 18 和 19，软件 200 可与这三个节点中的每一个内的保密箱电路的寄存器交互。这些寄存器包括入口节点中的邮箱(具有“收件”部分 201 和“发件”部分 202)、出口节点中的邮箱(具有“收件”部分 205 和“发件”部分 206)、以及包含该保密箱节点的保密箱电

路的能力表 207 的寄存器。中断线与这些寄存器相关联。

[0217] 入口节点可被(由固件)编程为每次它上电时,该入口节点就自动尝试建立用于与保密箱节点通信的安全通道。或者,仅当入口节点需要不存在于该入口节点的保密箱中的机密时,该入口节点才与保密箱节点建立这一安全通道。作为这一操作的初始步骤,入口节点在其邮箱的“发件”部分 202 中放置一经加密消息,并使一中断被断言。响应于此,软件 200 将该消息传递给保密箱节点的邮箱的“收件”部分 203。响应于此,保密箱节点将一经加密消息放置在其邮箱的“发件”部分 204 中,并使一中断被断言。响应于此,软件 200 将此消息传递给入口节点的邮箱的“收件”部分 201。以此方式继续,入口节点和保密箱节点就经由软件 200 执行了认证交换(使用预先存储在其中的证书数据 170 和 171,如图 16 中所示)。在成功完成认证交换之后,入口节点和保密箱节点进入其中它们以仿佛其间存在安全通道(在图 19 中标识为“安全通道 0”)那样操作的状态。在此类状态中,入口和保密箱节点在知道彼此的身份并知道各自是被许可设备的情况下相互通信,而不再执行进一步的认证操作来确定此信息。但是,在入口节点与保密箱节点之间经由软件 200 传送(在入口节点与保密箱节点之间建立安全通道的交换期间,以及在该安全信道已被建立之后)的所有消息(或被视为机密或“重要”的所有消息)被加密。由此,尽管软件 200 可对此类经加密消息做任何事(例如,保存它们和试图在稍后重放它们、修改它们、或将它们发送给除预期目的地以外的其它设备),但是软件 200 可对它们执行的将具有有用结果的唯一操作是将它们各自(不经修改地)传递到其预期目的地。例如,如果软件 200 将预期目标为保密箱节点的消息传递给另一设备,或在将其传递给保密箱节点之前对其进行修改,则接收方将不能将它们解密,从而使此类误传递(或讹误消息的传递)除了使得发送节点与保密箱节点之间不能成功通信以外没有其它任何效果。

[0218] 类似地,出口节点可被编程为每当它上电时,出口节点就自动尝试建立用于与保密箱节点通信的安全通道。或者,仅当出口节点需要尚未在出口节点的保密箱中出现的机密时出口节点才尝试与保密箱节点建立这一安全通道。作为这一操作的初始步骤,出口节点内的保密箱电路将一经加密消息放置在其邮箱的“发件”部分 206 中,并使一中断被断言。响应于此,软件 200 将该消息传递到保密箱节点的邮箱的“收件”部分 203 中。响应于此,保密箱节点将一经加密消息放在其邮箱的“发件”部分 204 中,并使一中断被断言。响应于此,软件 200 将此消息传递给出口节点的邮箱的“收件”部分 205。以此方式继续,出口与保密箱节点就能经由软件 200 执行认证交换(使用预先存储在其中的证书数据 172 和 171,如图 16 中所示)。一旦成功完成认证交换,出口和保密箱节点就进入其中它们以仿佛其间存在安全通道(在图 19 中标识为“安全通道 1”)那样地操作的状态。在此类状态中,出口节点与保密箱节点在知道彼此的身份并且知道各自是被许可设备的情况下相互通信,而不执行进一步的认证操作来确定此信息。但是,在出口节点与保密箱节点之间经由软件 200 传送(在出口与保密箱节点之间建立安全通道的交换期间,以及在该安全通道已被建立之后)的所有消息(或被视为“机密”或“重要”的消息)。由此,尽管软件 200 可能尝试对该经加密消息做任何事(例如,将它们保存并试图在稍后将它们重放,修改它们,或将它们发送到除预期目的地以外的其它设备),但是软件 200 可对它们执行的将具有有用结果的唯一操作是将它们各自(不经修改地)传递到其预期目的地。例如,如果软件 200 将消息(预期目的地为保密箱节点)从出口节点传递到除该保密箱节点以外的设备、或在将它们传递给保

密箱节点之前对它们进行修改，则接收方将不能将它们解密，从而此类误传递（或讹误消息的传递）除了使得出口节点与保密箱节点之间不能成功通信以外没有其它任何效果。

[0219] 在本发明 PDN 的典型实施例中，可在该 PDN 的任何一对节点的保密箱电路之间建立安全通道。例如，软件可在邮箱中放置目的地为出口节点的消息，并且当被传递（例如，通过软件）给该出口节点时，该消息将使出口节点准备好接收和处理要由入口节点经由该 PDN 的规定硬件向该出口节点（从入口节点 160 经由图 16 的处理器 177 向出口节点 162）断言的经重新加密内容。在此例中，出口节点将通过与其它某个节点建立安全通道并执行与其的安全交换来获得（从该其它节点）执行该消息规定的操作所需的密钥来响应于该消息。

[0220] 在典型实施例中，本发明的保密箱电路（或“保密箱”）存储指示涉及内容（和 / 或与之相关）的一组权限的数据。例如，保密箱可包括含存储此类数据的寄存器（或其它存储器）的能力表（例如，图 18 和 19 的能力表 207）。该能力表中的各个存储位置可存储用于使入口或出口电路能对特定类型的内容执行特定操作（或一组操作）的密钥数据。例如，表 207 中的“第 N 个”存储位置可存储出口节点将来自特定内容供应方的经重新加密视频解密、并将该经解密视频重新加密（并重新格式化）以通过 HDMI 链路传送所需的密钥数据。例如，PDN 的入口节点可向图 18 的保密箱节点发送（经由软件 200）要求该保密箱节点将表 207 中的第 N 个存储位置的内容发送给特定出口节点的消息。软件 200 可将此消息中继给该保密箱节点，但将不能访问表 207 的此存储位置的内容。响应于该消息，保密箱节点将加密相关密钥数据（表 207 中第 N 个存储位置的内容），并使软件 200 将经加密密钥数据传递给合适的出口节点。软件（例如，图 18 的软件 200）可传递该经加密密钥数据，但将不能访问原（未加密）密钥数据，因为它将不能解密要传递的经加密数据。如果软件 200 要将该经加密密钥数据传递给除预期出口节点以外的设备，或要在向预期出口节点传递之前修改该经加密密钥数据，则接收方将不能解密该误传递（或经修改）的经加密密钥数据，由此软件 200 的此类误传递（或经修改消息的传递）除了使保密箱与预期接收方节点之间不能成功通信之外没有其它任何效果。

[0221] 又如，系统用户将不能始发指示入口节点或出口节点执行未授权操作的消息，使用软件（例如，图 18 的软件 200）来向入口或出口节点传递该消息，并使接收方执行该未授权操作。相反，接收方节点将在响应于此采取任何其它行动之前解密这一消息（在由接收方已与其建立安全通道的节点生成并加密该数据的假设下）。此解密操作将有效地摧毁该消息的内容，因为该系统用户将不能访问加密该消息所需的密钥数据（安全地存储在该系统的节点中的硬件里），从而该消息的经解密版本（由接收该消息的节点的保密箱电路生成）将是接收方节点能识别的指令。

[0222] 接下来，我们参考图 20 对可以是并且通常被实现为单个集成电路的本发明入口节点的一个实施例进行说明。图 20 的入口节点 258 包含沿总线 246 连接的微处理器 240、以及耦合到微处理器 240 的指令存储器 241 和数据存储器 242。存储器 241 存储可由微处理器 240 执行的固件，而数据存储器 242 存储微处理器 240 将对其进行操作的数据。微处理器 240 不是通用 CPU，并且不可用软件编程。相反，微处理器 240 通常是实现简单状态机的简单微处理器（例如，控制器）。图 20 的实施例的变体包括另一种类型和 / 或具有不同架构的微处理器电路（例如，与用于存储数据和固件两者的共用存储器耦合的微处理器）、或是以软件编程的处理器。微处理器 240（或节点 258 内保密箱电路的另一元件）可被配置

成将要传送到节点 258 之外的消息加密，并将从节点 258 之外的实体(例如，另一保密箱)接收的经加密消息(例如，包含经加密内容密钥数据或其它经加密机密数据的消息)解密。

[0223] 入口节点 258 还包括如图所示地全部沿总线 246 连接的非易失性存储器 243(用于存储证书数据和 / 或其它数据)、邮箱 245、输入接口 247、解密引擎 249、重新加密引擎 251、以及输出接口 253。

[0224] 元件 240、241、242、243 和 245 (以及可任选地还有未示出的其它元件)构成入口电路 258 的保密箱电路，并且元件 247、249、251 和 253 (以及可任选地还有其它元件)构成入口节点 258 的入口电路。

[0225] 邮箱 245 是图 18 的具有“收件”部分 201 和“发件”部分 202 的邮箱的一个示例。邮箱 245 用于在入口节点 258 与 PDN 的另一节点的保密箱电路之间(经由该 PDN 的软件)的上述类型的通信。

[0226] 存储器 243 存储入口节点 258 的操作所需的所有证书。证书数据可在图 20 的电路制造时被存储在存储器 243 中以供例如在与节点 258 寻求与之相关联的 PDN 的节点(即，节点 258 寻求成为其授权成员，或换言之节点 258 寻求与之“结婚”的 PDN)的保密箱电路的认证交换中使用。在这一交换中，入口节点 258 将把其身份提供给该另一节点(使用存储在存储器 243 中的证书数据)，并且如果该另一节点的保密箱电路确定入口节点 258 是被授权成为该 PDN 成员的被许可设备，则从该另一节点获得“结婚证书”数据。结婚证书数据(指示入口节点 258 是该 PDN 的授权成员)通常还将存储在存储器 243 中供后续与 PDN 的另一节点的保密箱电路的认证交换(当节点 258 与该 PDN 相关联时各自在例如节点 258 上电时执行)。时使用，其中入口节点 258 再次向该另一节点证明其身份以与该另一节点建立安全链路，并在有必要的情况下如上所述地从该另一节点接收内容密钥(通过该安全链路)。

[0227] 更一般化地，根据本发明的优选实施例，PDN 及其节点被实现为在诉求或不诉求外部授权机构的情况下允许包含保密箱电路和入口(或出口)电路的设备被关联到该 PDN 中。例如，图 14 的设备 120、122、124、126、128 和 132 中的任一个只要包括适当配置的保密箱电路即可被关联到这一 PDN 中。在一些实施例中，PDN 的节点被配置并操作以请求内容所有者准许向该 PDN 添加特定设备(并由此添加至少一个特定能力)。优选的是，包含用户想要在 PDN 中包括的入口或出口电路的每个设备的保密箱电路应被配置成使机密可被持久地(和安全地)但可撤消地存储在其中以指示该设备是该 PDN 的授权成员(节点)。通常，这一机密是证书，由此指示这一机密的数据在本文中称为结婚证书数据。能够或的确向另一节点传送结婚证书数据的保密箱电路(例如，入口节点或出口节点)通常包括它自己的可编程(例如，一次性可编程)存储器，用于存储确定它与之通信的每个节点是否为该 PDN 的授权成员(即，该节点是否拥有有效结婚证书数据并由此与该“PDN”结婚)所需的数据。

[0228] 入口节点 258 (图 20)的存储器 243 可包含在入口节点 258 与 PDN 相关联时其中存储结婚证书数据的可编程(例如，一次性可编程)存储器(即，存储器 243 的部分 243A)。如果是这样，则存储器 243 还将包括在制造节点 258 时其中将存储标识节点 258 的证书数据的只读非易失性存储器部分。存储器 243 的可编程部分 243A 可以是可编程闪存或 EEPROM(或类似存储器)。但是，存储器 243 的可编程部分 243A 优选以比实现闪存或 EEPROM 所需便宜的方式来实现。例如，存储器 243 的部分 243A 可以是在不再需要时不再被使用、但一旦被永久编程成特定状态就不能被修改的一次性可编程熔丝组。例如，可编程存储器部分

243A 可包括 16（或其它数目）组此类熔丝，每组熔丝可被编程一次以存储一组结婚证书数据。当将指示节点 258 的当前有效结婚证书的数据放在邮箱 245 中时，入口节点 258（即，其微处理器 240）将优选地被配置成仅使用存储器部分 243A 的最近编程的一组熔丝（即忽略其它各组熔丝）。如果节点 258 从 PDN 被移除（即，如果它与该 PDN“离婚”）并与一新的 PDN 相关联（即，与该新的 PDN“重新结婚”），则该新 PDN 的保密箱将使存储器部分 243A 中的另一组熔丝以指示节点 258 与该新 PDN 的关联的新的一组结婚证书数据编程。

[0229] 更一般化地，已变成与本发明 PDN 的一特定实施例相关联的所有设备包含该域独有的数据（证书或类证书数据）。在本文中有时将此类数据称为“结婚证书数据”。能被包含在这一 PDN 中的每个被许可设备，无论其实际是否与该 PDN 相关联，均具有永久存储（在制造期间）在其至少一个集成电路（例如，保密箱芯片）中以指示其为被许可设备的证书数据。后一种类型的证书数据与上述“结婚证书数据”不同。当与第一 PDN 相关联的设备从第一 PDN 被移除（即，与第一 PDN“离婚”时），则在其与另一 PDN（第二 PDN）相关联（“重新结婚”）之前其结婚证书数据应被有效地删除，从而它失去对因与第一 PDN 结婚而获得访问的所有机密的访问。本发明的设备（可以成为 PDN 的节点）的优选实施例可被实现为使得存储在其中的任何结婚证书数据（作为先前与第一 PDN 相关联的结果）将在该设备与第二 PDN 相关联时被有效地删除（并且第二 PDN 的新的结婚证书数据将被存储在其中）。本发明设备的优选实施例还被实现为使每个此类设备能与不多于预定最大数目的 PDN 相关联。可任选地，可在本发明的设备中内建其它限制（例如，内建在其保密箱电路中）以限制其与特定 PDN 相关联的资格。

[0230] 本发明的保密箱电路的优选实施例还可被配置成使保密箱电路能高效地确定（例如，以高成本效益的方式）另一节点与 PDN 的关联何时应被撤消，并允许此类撤消被高效地实现。

[0231] 预期当节点 258 寻求关联到 PDN 中（即，成为该 PDN 的授权成员）时将在（PDN 的）保密箱与入口节点 258 之间执行全认证交换（例如，公钥证书签名或“PKCS”交换）。由此，持久地存储在节点 258 的存储器 243 中的证书数据应为适合执行这一全认证交换的类型。在节点 258 关联到 PDN 中之后，每当节点 258 寻求建立通过它可从该 PDN 的其它任何节点获得内容密钥的安全通道时可在节点 258 与该其它节点的保密箱电路之间执行简单得多的认证交换。存储器 243（例如，存储器 243 的可编程部分 243A）还可包括适合执行这一较简单的认证交换的少量证书数据。例如，用于建立安全通道（通过其可传送内容密钥）的这一“较简单”的认证交换可使用比通常用来执行常规公钥证书签名（“PKCS”）交换的工业标准 PDCS 证书轻量级的证书来执行。如果是这样，则与需要能存储更复杂的 PKCS 证书数据的情况相比，存储器 243 的可编程部分 243A 可更简单和更便宜地实现。或者，可执行认证交换以在 PDN 的两个节点之间建立安全通道而完全无需在这些节点之间交换任何证书。

[0232] 仍参考图 20，内容（例如，视频和 / 或音频数据）在接口 247 处进入入口节点 258，并在入口节点 258 内从输入接口 247 流到解密引擎 249，从解密引擎 249 流到重新加密引擎 251，并从重新加密引擎 251 流到输出接口 253。内容不能在元件 247、249、251 和 253 中的任一个与微处理器 240、存储器 243 和邮箱 265 中的任一个之间流动。微处理器 240 控制元件 247、249、251 和 253 的操作。接口 247 是被配置成执行与内容源的所有必需握手以使内容以所需形式进入节点 258 的流处理器。接口 247（在必要的程度下在微处理器 240 的控

制下）执行所有必要的内容流控制，并向内容源断言所有必要的确认等。在一些实施例中，接口 247 被配置成仅接收一种格式的内容（例如，通过 USB 链路、1394 链路、无线链路或任何其它链路接收的内容）。在其它实施例中，接口 247 被配置成以两种或多种不同格式的任一种接收内容。通常，由接口 247 接收的内容（并由接口 247 向解密引擎 249 断言）是压缩的经加密数据，并根据内容提供方所使用的任何传输和加密方案加密。

[0233] 解密引擎 249 通常使用先前由入口节点 258 从保密箱（例如，图 22 的保密箱节点 298）获得的内容密钥将向其断言的内容解密。保密箱和入口节点 258 通常被实现为分离的芯片，并且内容密钥通常以加密形式从保密箱（经由软件）向节点 258 的邮箱 245 发送，然后由节点 258 内的合适电路解密以将其变成可由引擎 249 使用的形式。解密引擎 249 通常输出内容的压缩明文版本，但不对该压缩内容执行解压缩。重新加密引擎 251 随后通常使用先前由入口节点 258 从保密箱（例如，图 22 的保密箱节点 298）获得的内容密钥将该明文内容加密。将由引擎 251 生成的经重新加密（转加密）内容向输出接口 253 断言，并从接口 253 向 PDN 的任一元件断言。接口 253 是被配置成与接收经转加密内容的设备执行所有必要握手的流处理器。

[0234] 接下来，我们将参考图 21 对本发明的通常可实现为单个集成电路的出口节点的一个实施例进行说明。图 21 的出口节点 278 包含沿总线 266 连接的微处理器 260、以及耦合到微处理器 260 的指令存储器 261 和数据存储器 262。存储器 261 存储可由微处理器 260 执行的固件，而数据存储器 262 存储由微处理器 260 操作的数据。微处理器 260 不是通用 CPU，并且不可用软件编程。相反，微处理器 260 通常是实现简单状态机的简单微处理器（例如，控制器）。图 21 的实施例的变体包含另一种类型的和 / 或具有不同架构的微处理器电路（例如，与用于存储数据和固件两者的共用存储器耦合的微处理器）、或用软件编程的处理器。微处理器 260（或节点 278 内保密箱电路的另一元件）可被配置成将要传送到节点 278 之外的消息加密，并将从节点 278 之外的实体（例如，另一保密箱）接收的经加密消息（例如，包含经加密内容密钥数据或其它经加密机密数据的消息）解密。

[0235] 出口节点 278 还包括全部如图所示地沿总线 266 连接的非易失性存储器 263（用于存储证书数据和 / 或其它数据）、邮箱 265、输入接口 267、解密引擎 269、解码电路 271、多路分解器 273、HDMI 发送器 277。多路分解器 273 的一个输出端耦合到 HDMI 发送器 277 的输入端。多路分解器 273 的另一输出端耦合到调节器 275 的输入端，并且调节器 275 的输出端被耦合到编码和 DAC 电路 279 的输入端。

[0236] 元件 260、261、262、263 和 265（以及可选地还有未示出的其它元件）构成出口节点 278 的保密箱电路，并且元件 267、269、271、273、275、277 和 279（并且可任选地还有其它未示出的元件）构成出口节点 278 的出口电路。

[0237] 邮箱 265 是图 18 的具有“收件”部分 205 和“发件”部分 206 的邮箱的一个示例。邮箱 265 用于经由该 PDN 的软件在出口节点 278 与保密箱（包含在 PDN 中的节点 278 中）之间的上述类型的通信。

[0238] 存储器 263 存储出口节点 278 的操作所需的所有证书。证书数据可在制造图 21 的电路时被存储在存储器 263 中供例如在与节点 278 寻求与之相关联（换言之，节点 278 寻求与之“结婚”）的 PDN 的节点的保密箱电路的认证交换中使用。在这一交换中，出口节点 278 将向该另一节点证明（使用存储在存储器 263 中的证书数据）其身份，并且如果该另一节点

的保密箱电路确定出口节点 278 是被授权成为该 PDN 成员的被许可设备，则从该另一节点获得“结婚证书”数据。该结婚证书数据（指示该出口节点 278 是该 PDN 的授权成员）通常还将存储在存储器 273 中供后续在节点 278 与 PDN 的其它节点之间的认证交换（各自在节点 278 与该 PDN 相关联的情况下在节点 278 上电时执行）时使用，其中出口节点 278 再次向另一节点证明其身份以与该另一节点建立安全链路并根据需要如上所述地从该另一节点（通过该安全链路）接收内容密钥。

[0239] 存储器 263 可包括其中在出口节点 278 与 PDN 相关联时存储结婚证书数据的可编程（例如，一次性可编程）存储器（即，存储器 263 的部分 263A）。如果是这样，则存储器 263 还将包括其中在制造节点 278 时将存储标识节点 278 的证书数据的只读非易失性存储器部分。存储器 263 的可编程部分 263A 可以是可编程闪存或 EEPROM（或类似存储器）。但是，存储器 263 的可编程部分 263A 优选以比实现闪存或 EEPROM 便宜的方式实现。例如，存储器 263 的部分 263A 可以是在不再被需要时不再使用、但一旦被永久编程成特定状态时就不能再被修改的一次性可编程熔丝组。例如，可编程存储器部分 263A 可包括 16（或其它某个数目）组此类熔丝，每组熔丝可被编程一次以存储一组结婚证书数据。出口节点 278（即，其微处理器 260）将优选地被配置成仅在例如将指示节点 278 的当前有效结婚证书的数据放置在邮箱 265 中时使用存储器部分 263A 的最近被编程的一组熔丝（即，忽略其它每组熔丝）。如果节点 278 从 PDN 被移除（即，如果它与该 PDN “离婚”），并与新的 PDN 相关联（即，与该新 PDN “重新结婚”），则该新 PDN 的另一节点的保密箱电路将使存储器部分 263A 中的另一组熔丝用指示节点 278 与该新 PDN 的关联的新的一组结婚证书数据编程。

[0240] 预期当节点 278 寻求成为 PDN 的授权成员时，将在出口节点 278 与该 PDN 的节点的保密箱电路之间执行全认证交换（例如，公钥证书签名交换）。由此，持久存储在节点 278 的存储器 263 中的证书数据应当是适合执行这一全认证交换的类型。在节点 278 关联到 PDN 之后，每次节点 278 寻求与 PDN 的另一节点建立安全通道（例如，节点 278 可通过其获得内容密钥的安全通道）时可在节点 278 与该另一节点之间执行简单得多的认证交换。存储器 263（例如，存储器 263 的可编程部分 263A）还可包括适合执行这一较简单认证交换的少量证书数据。例如，用于建立安全通道（可通过其传送内容密钥）的这一“较简单”认证交换可使用比通常用来执行常规公钥证书签名（“PKCS”）交换的工业标准 PDCS 证书轻量级的证书来执行。如果是这样，则与需要能存储更复杂的 PKCS 证书数据的情况相比，存储器 263 的可编程部分 263A 可更简单和更便宜地实现。

[0241] 仍参见图 21，出口节点 278 被配置成使内容（例如，视频和 / 或音频数据）在接口 267 处进入出口节点 278，并从输入接口 267 流到解密引擎 269，从解密引擎 269 流到解码电路 271，并从电路 271 流到多路分解器 273。内容不能在元件 267、269、271 和 273 中的任一个与微处理器 260、存储器 263 和邮箱 265 中的任一个之间流动。微处理器 260 控制元件 267、269、271 和 273 的操作。接口 267 是被配置成与内容源执行所有必要的握手以使内容以所要求的形式进入节点 278 的流处理器。接口 267（在必要的程度下在微处理器 260 的控制下）执行所有必要的内容流控制，并向内容源断言任何所要求的确认等。在一些实施例中，接口 267 被配置成从 PDN 的一个元件接收内容（仅以一种格式）。在其它实施例中，接口 267 被配置成从 PDN 的一个或多个元件以两种或多种不同格式中的任一种接收内容。通常由接口 267 接收并向解密引擎 269 断言的内容是已在出口节点 278 所属的 PDN 的入口节点

中被转加密的压缩的经转加密数据。

[0242] 解密引擎 269 通常使用先前由出口节点 278 从另一节点的保密箱(例如,图 22 的保密箱 298)获得的内容密钥来将向其断言的内容解密。当出口节点 278 和该另一节点的保密箱被实现为分离的芯片时,内容密钥通常以加密形式从该另一节点的保密箱(经由软件)发送到节点 278 的邮箱 265,然后由节点 278 内的适当电路解密以将其变成可由引擎 269 使用的形式。解密引擎 269 通常被配置成输出内容的压缩明文版本。解码电路 271 对压缩内容执行任何必要的解压缩,并将原(解压缩的)明文内容向多路分解器 273 断言。

[0243] 当微处理器 260 将多路分解器 273 置于第一状态时,原明文内容从多路分解器 273 向 HDMI 发送器 277 断言。发送器 277 将该原明文内容重新加密(根据 HDCP 协议)并将经重新加密的内容通过 HDMI 链路传送到 HDMI 接收器(例如,在含显示设备的视听系统中)。当微处理器 260 已将多路分解器 273 置于第二状态时,多路分解器 273 向调节器 275 断言原明文内容。调节器 275 对该内容执行任何必要的调节(例如,将视频内容重新调节到另一分辨率)。该内容(通常在调节器 275 内进行了调节)然后向编码和 DAC 电路 279 断言,在那里它根据需要被编码并格式化(供输出),并被转换成模拟形式供从出口节点 278 输出。

[0244] 注意,微处理器 260 (由此还有出口节点 278) 在其仅可执行其内部固件和它已从保密箱接收的任何内容密钥(和 / 或许可数据等)允许其执行的操作的意义上被配置成仅以授权方式操作。出口节点 278 仅将在向另一节点证明(例如,使用存储在存储器 263 中的证书数据)它被授权执行该内容密钥(和 / 或许可数据)允许其执行的操作之后才会通过安全通道从该另一节点的保密箱电路接收该内容密钥(和 / 或许可数据)。例如,如果通过安全通道从另一节点的保密箱电路接收的许可数据使微处理器 260 将多路分解器 273 置于将原明文内容路由到 HDMI 发送器 277 (以允许通过 HDMI 链路从发送器 277 向外部接收器传送该内容的经 HDCP 编码的版本)的状态,则没有任何外部实体能使微处理器 260 改为将多路分解器 273 置于将原明文内容路由到调节器 275 的状态。由此,没有任何外部实体能使出口节点 278 使用编码和 DAC 电路 279 执行内容的明文模拟版本的未授权输出。

[0245] 构想了图 21 的出口节点的结构的许多变体。例如,在一些此类变体中,出口节点可使从解密引擎 269 输出的压缩明文内容得到保存(例如,作为 MPEG 视频数据保存在该出口单元之外的存储器中)而不是向该出口节点的解码器断言。

[0246] 接下来,我们将参考图 22 对本发明的可被(并且通常被)实现为单个集成电路、并且可以是 PDN 的节点(本文中有时称为“保密箱节点”)的保密箱电路的一个实施例进行说明。图 22 的保密箱电路(“保密箱”)298 包括沿总线 286 连接的微处理器 280、以及耦合到微处理器 280 的指令存储器 281 和数据存储器 282。存储器 281 存储可由微处理器 280 执行的固件,而数据存储器 282 存储由微处理器 280 操作的数据。微处理器 280 不是通用 CPU,并且不可用软件编程。相反,微处理器 280 通常是实现简单状态机的简单微处理器(例如,控制器)。图 22 的实施例的变体包含另一类型和 / 或具有不同架构的微处理器(例如,与用于存储数据和固件两者的共用存储器耦合的微处理器)、或用软件编程的处理器。微处理器 280 (或保密箱 298 的另一元件)可被配置成将要传送到保密箱 298 之外的消息加密,并将从保密箱 298 之外的实体(例如,另一保密箱)接收的经加密消息(例如,包含经加密机密数据的消息)解密。

[0247] 保密箱 298 还包括如图所示全部沿总线 286 连接的随机数生成器 283、非易失性存

储器 285（用于存储证书数据）、非易失性存储器 284（用于存储密钥数据）、附加非易失性存储器 289、邮箱 287、非递减计数器（或计时器）291、SSL 端接电路 293、以及接口电路 295。

[0248] 邮箱 287 是图 18 的具有“收件”部分 203 和“发件”部分 204 的邮箱的一个示例。邮箱 287 用于保密箱 298 与 PDN 的入口或出口节点（经由该 PDN 的软件）的上述类型的通信。

[0249] 存储器 289 存储指示涉及内容的一组权限（和 / 或与之相关）的数据，并可任选地还存储供保密箱 298 使用的其它数据。例如，存储器 289 中的各个存储位置可存储能被发送（以加密形式）到其它节点以使此类其它节点的入口或出口电路能对特定类型的内容执行特定操作（或一组操作）的密钥数据。例如，存储器 289 中的“第 N 个”存储位置可存储出口电路将来自特定内容供应方的经重新加密视频解密、并将该经解密视频重新加密（并重新格式化）以供通过 HDMI 链路传送所需的密钥数据。

[0250] 存储器 285 存储保密箱 298 的操作所需的证书。证书数据可在制造图 21 的电路时存储在存储器 285 中，以供例如在与寻求关联于（“结婚”）包含保密箱 298 的 PDN 的入口或出口节点认证交换时使用。在这一交换中，保密箱 298 将向入口或出口节点证明其身份，确定（使用存储在存储器 285 和 / 或存储器 289 中的证书数据）入口或出口节点是否是授权成为该 PDN 的成员的被许可设备，并在确定该入口或出口节点是被授权成为该 PDN 的成员的被许可设备时向该入口或出口节点提供结婚证书数据（可被预先存储在存储器 285 和 / 或存储器 289 中）。存储器 285（和 / 或存储器 289）还可存储供与入口或出口节点（与该 PDN 相关联）进行认证交换时使用的证书数据，在该认证交换中入口（出口）节点寻求与保密箱 298 建立保密箱 298 可通过其向该入口（出口）节点发送内容密钥的安全链路。

[0251] 存储器 284 存储作为保密箱 298 独有的机密的设备密钥。保密箱 298 被配置成使用该设备密钥来以只有保密箱 298 可检索并将这些机密解密的方式将机密加密以供存储在保密箱 298 之外。使用该设备密钥，保密箱 298 可扩展其内部非易失性存储容量。以加密形式存储在保密箱 298 之外的机密（已使用存储在存储器 284 中的该设备密钥加密）将保持安全。由此，该外部存储将在功能上等效于该保密箱内部的非易失性存储。可由保密箱 298 访问的外部存储的一个示例是图 15 的存储单元 153，保密箱 298（在作为图 15 的保密箱电路 151 的角色时）可向其写入经加密机密（经由存储电路 152），并且保密箱 298 可从中读取这些经加密机密（也是经由存储电路 152）。在图 22 的实施例的变体中，本发明的保密箱不包含存储器 284，并且依赖于内部存储器来存储所有机密。

[0252] 在一些实施例中，本发明的保密箱（例如，图 22 的保密箱的实现）在制造时被初始化为包含（例如，持久地存储）：从不共享或曝露的私钥、自由共享和曝露的匹配公钥、可信证书授权机构的一个或多个公钥、定义设备类型（例如，可被用作 PDN 的节点并且其中包含保密箱的设备的类型）和该设备的基本属性的信息、由授权的证书授权机构（例如，对包含该保密箱的 PDN 的授权的证书授权机构）颁发的证书、标识并与设备（其中包含该保密箱，并且可被用作 PDN 的节点）的其它元件安全通信所需的所有密码信息、以及标识并与其它保密箱安全通信所需的所有密码信息。

[0253] 保密箱 298 使用随机数生成电路 283 来生成执行例如认证交换所需的任何随机或伪随机密钥数据（或其它随机或伪随机数据）。优选的是，电路 283 是统计上良好的随机源，并被配置成使其不能被攻击者（例如，通过控制其操作的温度或电压条件）所击败。电路 283

可用许多不同方式的任一种实现，从而例如通过其输出指示的随机或伪随机数具有许多不同长度中的任一种长度。例如，电路 283 的一种实现可输出指示 N 位随机或伪随机数的数据，其中 N 是小数字，而电路 283 的另一种实现可输出指示 M 字节随机或伪随机数的数据，其中 M 是大数字。

[0254] 或者，电路 283 可由定序器替换，或者保密箱 298 可包含电路 283 和定序器两者。定序器类似于随机数发生器，并提供基本相同的功能。定序器不以随机或伪随机方式操作，但是改为遵循预定序列。简单的计数器是定序器的一个示例。保密箱所实现的加密协议所固有的分散性将实质上使定序器的影响随机化，并提供所需的对抗重放和已知文本攻击的保护。在该序列充分长，并且当该序列中的位置保密并且不能被攻击者所复位或重新初始化时，此类保护最为有效。定序器可被用来传达与分组和 / 或密钥的排序或同步相关的信息。它们还被用来实现不存储密钥、但可按需重新推导密钥的各种滚动码机制。

[0255] 设置非递减(即，单调递增)计数器 291 以防止对保密箱 298 的重放攻击，并防止攻击者在适当的时机使保密箱 298 断电(和上电) 以尝试在密钥(访问内容所需) 被排程为过期之后获得对内容的未授权访问的其它攻击。在尝试进行重放攻击时，PDN 内的软件可保存该软件向保密箱 298 传递的消息(例如，来自入口或出口节点的合法的经签名消息)，并在稍后将这些消息重新传递给保密箱 298 以试图模仿该入口或出口节点。根据标准密码手段可使用非递减计数器 291 (或可被防篡改时钟或其它计时器替换) 以防止此类重放攻击。

[0256] 非递减计数器 291 (或作为其替代的防篡改时钟或其它计时器)还可被保密箱 298 (例如，保密箱 298 的微处理器 280)用来在预定时间、例如在保密箱 298 从外部源(例如，内容供应方) 接收到机密以及其使用仅被授权规定时间、由此该机密具有预定过期时间的限制的情况下删除机密(例如，密钥数据)。优选的是，计数器 291 被配置成尽可能地简单，以允许保密箱 298 以高成本效益的方式完成该功能。例如，计数器 291 可使用允许保密箱 298 防止对机密的未授权使用超过上舍入到数秒(例如，10 秒)间隔的最接近整数的预定过期时间的简单、便宜的电路来实现，而计数器 291 将需要以复杂和昂贵得多的方式来实现，以允许保密箱 298 防止对该机密的未授权使用超出确切预定过期时间的几分之一秒。又如，计数器 291 可被实现为允许保密箱 298 防止对机密的未授权使用超过按日计的授权使用期过期仅数秒的简单、廉价的电路，而要防止对机密的未授权使用不超过授权使用期过期几分之一秒将需要将计数器 291 实现为昂贵得多的电路。计数器 291 可被实现为仅提供对所述类型的攻击的有限保护。例如，计数器 291 可具有不在上电(或断电) 时复位的最高有效数位和在上电或断电时复位的最低有效数位，从而攻击者可通过在适当时机使保密箱上电和断电来获得对内容少量(例如，相当于数秒的) 额外的未授权访问。

[0257] 计数器 291 可以是在保密箱断电时计数值不归零的单调递增计数器。或者，保密箱 298 可包含防篡改时钟(不在保密箱断电时复位)，作为计数器 291 的替代。

[0258] 或者，保密箱 298 既不包括计数器 291 也不包括计时器，而是改为被配置成周期性地(或在上电时) 访问外部防篡改时钟以获得当前时间数据，供例如确定何时删除具有过期时间的密钥或者防止重放攻击时使用。例如，保密箱 298 可被配置成 :每当保密箱 298 上电时就使用 SSL 端接电路 293 来使 PDN 的软件登录到因特网以访问正确的时间，并从因特网接收并解密由保密箱 298 的软件中继的所需“时间数据”。

[0259] SSL 端接电路 293 向保密箱 298 提供了与其它设备——无论它在 PDN 内部还是外

部——通信的能力。电路 293 的一典型实现允许保密箱 298 经由 PDN 软件通信(例如,如果保密箱 298 和执行该软件的 PC 沿 PCI 总线连接则通过该 PCI 总线)。例如,保密箱 298 可使用 SSL 端接电路 293 通过使用保密箱 298 之外的 PDN 能力(例如,PDN 的 PC 的 TCP/IP 功能)来使 PDN 软件登录到因特网,并通过因特网向保密箱 298 发送消息。或者,保密箱 298 可使用 SSL 端接电路 293 来使 PDN 软件改为中继保密箱 298 与该 PDN 之内或之外的一个或多个设备之间的通信。保密箱 298 可使用 SSL 端接电路 293 来使 PDN 软件中继保密箱 298 与该 PDN 中另一保密箱之间的通信。PDN 的个人计算机可用常规方式配置成使用 TCP 层建立通信、并使用 SSL 层执行实现该通信所需的密码功能(例如,任何必要的认证)来通过因特网通信。保密箱 298 之外的设备可使在(PDN 的)PC 上运行的操作系统软件(例如,Windows 操作系统)执行该设备通过因特网向保密箱 298 的 SSL 端接电路 293 发送经加密消息所需的 TCP 层功能。电路 293 将执行将该消息解密并加密保密箱 298 的响应(要经由操作系统软件通过因特网来发送)所需的 SSL 层功能。电路 293 不需要被配置成实现 TCP/IP 层。相反,PDN 软件可根据需要运行 TCP 栈、并将有效负荷从 TCP 栈向外转发到电路 293,从而电路 293 仅需实现顶层的 SSL 协议。接口电路 295 可被配置成发起经由电路 293 和 PDN 软件与保密箱 298 之外的设备的通信。

[0260] 接口电路 295 提供在保密箱 298 与其它设备(无论是在 PDN 内部还是外部)之间通信的能力。例如,接口电路 295 可被配置成允许保密箱 298 和外部设备之间经由单条链路(例如,USB 链路、1394 链路、WiFi 或其它无线链路、以及以太网链路中的一种)的通信。在其它实施例中,接口电路 295 被配置成允许保密箱 298 与外部设备之间经由两条或多条不同链路(例如,USB 链路、1394 链路、WiFi 链路及以太网链路)中的任一条的通信。

[0261] 构想了图 22 的保密箱的结构的许多变体。例如,在一些此类变体中,省略了元件 283、284、291、293 和 295 中的一个或多个。

[0262] 在一类实施例中,本发明是一种被配置成在 PDN 中使用(例如,作为该 PDN 的节点)的设备(例如,用于从远程源接收内容的机顶盒、或视频接收器或处理器)。每个此类设备包括保密箱电路以及被配置成在本发明 PDN 的至少一个实施例中使用的入口(或出口)电路。图 23 的设备 300 是这种设备的一个示例。可以但不需要是用于从最多达 N 个不同远程源接收内容的机顶盒的设备 300 包含如图所示地连接的接口电路 301 和电路 302。电路 302 包括保密箱电路和入口电路(有时被称为入口单元 302)。设备 300 还可任选地包括其它组件(未示出)。接口电路 301 被配置成接收 N 个输入内容流(I1、I2、……、和 IN)中的任一个并可任选地对其执行初始处理,并响应于这些输入内容流中被接收的那一个向单元 302 内的入口电路断言内容流 PI1、PI2、……和 PIN 中的任一个。电路 301 响应于这些输入内容流中的第“m”个(“Im”)向入口电路 302 的输入端断言第“m”个内容流(“PIm”)。这些输入内容流的每一个都具有不同格式,并且每一个可根据一不同的内容保护协议加密。例如,一个输入内容流可以是从卫星接收的数字视频,另一个可以是通过 HDMI 链路接收的 HDMI 格式内容中的内容,诸如此类。向入口单元 302 断言的每个内容流“PIm”可与相应的输入内容流(“Im”)相同、或者可以是相应输入内容流的经处理版本。入口单元 302 内的输入接口(例如,图 20 的接口 247 的一种实现)被配置成接收从电路 301 向入口单元 302 断言的内容流中的任一个,并将每个接收到的内容流向入口单元 302 内的转加密电路断言。单元 302 内的转加密电路被配置成响应于这些内容流中的任一个 PIm 输出具有单个格式的经转

加密内容流(“输出”)。经转加密的内容流不拘于这 N 个不同内容流 PIm 中的哪一个由入口单元 302 转加密而具有相同的格式。

[0263] 图 24 的设备 310 是前一段落中说明的一类中的另一示例性设备。可以但不需要是视频处理器的设备 310 包括如图所示地连接的电路 311 和接口电路 312。电路 311 包括保密箱电路和出口电路(有时称为出口单元 311)。设备 310 还可包括其它组件(未示出)。出口单元 311 被配置成接收并解密单个受控内容流(“输入”)以生成该内容流的明文版本。向单元 311 断言的该受控内容流可以是从图 23 的入口单元 302 输出的经转加密内容流。出口单元 311 包含被配置成响应于由设备 310 接收的单个输入流输出内容的 M 个内容流(O1、O2、……和 OM)的电路。通常,这 M 个输出流 O1、O2、……和 OM 各自具有不同的格式,并且出口单元 311 被配置成除了解密和格式化以生成输出流 O1、O2、……和 OM 之外还执行其它操作(例如重新加密)。接口电路 312 被配置成接收其从出口单元 311 接收的内容流 O1、O2、……OM 中的每一个并对之进行操作(例如,重新格式化和 / 或放大),并响应于其从单元 311 接收的内容流输出 M 个经处理输出流 PO1、PO2 和 POM。电路 312 响应于来自单元 311 的第“m”个内容流(“Om”)断言第“m”个内容流“POm”。第“m”个内容流“POm”可与相应的输入流(“Om”)相同,或者可以是相应输入流(“Om”)的经处理版本。通常,输出流(PO1、PO2、……和 POM)中的每一个具有不同的格式(例如,一个此类输出流可以是 DVI 格式的内容以供通过 DVI 链路传送,另一个可以是通过 HDMI 链路接收的 HDMI 格式内容的内容,诸如此类),并且这些输出流中的每一个可根据不同的内容保护协议来加密。由此,设备 310 包含被配置成接收具有单种格式的受控内容、生成该受控内容的解密(明文)版本、并对该明文内容执行其它处理(例如,重新格式化以及可任选地还重新加密)以生成 M 个输出内容流的出口电路。这 M 个输出内容流中的每一个可具有不同格式,并且可根据不同的内容保护协议加密。

[0264] 因为设备 300 和 310 各自根据本发明配置(以使其各自的入口单元输出,并且各自的出口单元接收,根据单种内容保护协议加密的受控内容),这些设备可被耦合在一起(与由设备 300 生成的向设备 310 的输入端断言的输出流)以生成能够接收具有 N 种不同格式中的任一种的内容、响应于此生成具有 M 种不同格式中的任一种的输出内容、并通过决不在安全硬件之外(例如,在一个设备内的集成入口电路或另一设备内的集成出口电路之外)曝露该内容的明文版本来保护该内容的设备对。这一设备对的每个设备可用其具有不超过 N 倍复杂性(响应于具有单种格式的输入生成具有 N 种格式中的任一种的输出、或响应于具有 N 种格式中的任一种的输入生成具有单种格式的输出的能力)或 M 倍复杂性(响应于具有单种格式的输入生成具有 M 种格式中的任一种的输出、或响应于具有 M 种格式中的任一种的输入生成具有单种格式的输出的能力)的意义上的简单方式来实现。相反,能够接收具有 N 种不同格式中的任一种的内容并响应于此生成具有 M 种不同格式中的任一种的输出内容的常规设备在通过决不在该设备之外曝露该内容的明文版本来保护该内容的同时,将具有更大的复杂性(即,(N*M)- 倍复杂性)。由此,假定 N 和 M 各自大于 1,并且 N 和 M 中的至少一个大于 2,则该常规设备将比与该常规设备具有相同总能力的两个本发明设备(一并考虑)更为复杂。当 N 和 M 比 2 大得多时,该常规设备将比这样的一对本发明设备(一并考虑)复杂得多。

[0265] 如果 PDN 根据本发明实现,则该 PDN 内要被保护的内容的明文版本决不出现在该

PDN 的任何外部可见(可访问)的链路、接口或节点处。该 PDN 优选地还被实现为使没有任何出现在其入口或出口电路中的、供该入口或出口电路使用或传送的机密(例如,入口电路中用于转加密由 PDN 接收到的内容、或出口电路中用于解密受控内容的密钥数据)以未加密形式可为该 PDN 内部的软件或固件或为该 PDN 之外的任何实体访问。否则,该 PDN 将易受攻击。在优选实施例中,在 PDN 的任何设备上运行的软件将决不能访问要保护内容的明文版本或用于在该 PDN 内保护内容的密钥数据的明文版本。

[0266] 本发明的另一个方面是一种内容保护方法和装置,它在系统(其中该系统包括硬件和软件两者)的硬件子系统中安全地执行内容的加密和解密、但使用该系统的软件作为在这些硬件子系统之间传递消息(通常可以是经加密消息)但不能理解这些消息的无害实体(“中间人”)。这些消息可以是指示经加密机密的经加密消息(例如,由这些硬件子系统中的一个或多个使用的内容密钥),但该软件不具有解密这些消息所需的密钥并且不能将这些消息解密。该软件可用于实现整个系统的各安全硬件子系统之间的安全通道,并且这些安全通道对于对要保护内容的“中间人”攻击免疫。但是,该系统使用软件作为中间人来传递消息。

[0267] 在一类实施例中,本发明是 PDN 中的内容保护方法,包括以下步骤:在该 PDN 的入口硬件中转加密进入该 PDN 的内容,由此生成受控内容;以及在该 PDN 的出口硬件中将该受控内容解密以生成经解密内容,从而使得明文形式的内容、以及由该入口硬件和出口硬件中的至少一个用来对内容和受控内容中的任一个执行授权操作的任何机密都不可为在该 PDN 的任一元件上运行的软件或固件访问,并且使得该内容决不会以明文形式出现在该 PDN 内除安全硬件内以外的其它地方,由此受控内容可在该 PDN 的各元件之间自由传送并存储在该 PDN 内。在一些此类实施例中,入口硬件是一集成电路,出口硬件是另一集成电路,并且内容在 PDN 内保持,从而该内容决不会以明文形式出现在该 PDN 内除集成电路内以外的任何地方。

[0268] 在另一类实施例中,本发明是一种内容保护方法,包括以下步骤:在 PDN 的入口硬件中转加密进入该 PDN 的内容,由此生成受控内容;在该 PDN 的出口硬件中将该受控内容解密以生成经解密内容;以及将该经解密内容和该经解密内容的经处理版本中的至少一个从该出口硬件向该 PDN 之外的实体(例如,一设备或系统)断言,从而使得该经解密内容以及该入口硬件和出口硬件中的任一个用来对该内容和受控内容中的任一个执行授权操作的任何机密都不可为软件或固件所访问(除了这一机密的经加密版本可为软件或固件访问之外)。通常,入口硬件是一集成电路,而该出口硬件是另一集成电路。

[0269] 本发明的其它方面是用于在 PDN(例如,开放式计算系统)中保护内容的方法、可由本发明 PDN 的任一实施例(或保密箱电路、入口电路和出口电路中的一个或多个)实现的方法、在 PDN 中使用的保密箱电路(例如,保密箱芯片)、在 PDN 中使用的入口电路(例如,入口芯片)、在 PDN 中使用的出口电路(例如,出口芯片)、在个人计算机中使用的包括沿总线(例如,PCI 总线)连接的入口、保密箱和出口芯片的卡(例如多媒体图形卡)、以及被配置成在 PDN 中使用并包括保密箱电路、入口电路和出口电路中的任何一个的设备(例如,机顶盒、视频接收器或视频处理器)。

[0270] 接下来,我们阐述根据本发明可在各保密箱之间执行的交换(例如,以在其间建立安全通道)的具体示例。保密箱可形成其间的链路、通道或连接(例如,以相互认证包含这些

保密箱的节点并交换数据)。此类链路、通道或连接(“关系”)根据需要被形成、改变、断开和重新形成以实现期望目的。

[0271] 在其中一些示例中将使用以下记法：

[0272] “PuKi[文本]”是指该文本已用发起方的公钥加密；

[0273] “PrKi[文本]”是指该文本已用发起方的私钥加密；

[0274] “PuKr[文本]”是指该文本已用应答方的公钥加密；

[0275] “PrKr[文本]”是指该文本已用应答方的私钥加密；

[0276] “SHA-1[文本]”是指形成了该文本的 SHA-1 摘要。

[0277] 在一些实施例中，消息摘要是使用 CBC-MAC-AES 模式(而不是 SHA-1 模式)的某种变体来生成的。在此类实施例中，用于加密消息(例如，要在节点之间传送的消息)的 AES 加密器还用来生成每个消息的“消息认证码”(摘要)。在表述“CBC-MAC-AES”中，“CBC”是指“密码分组链接”，即构想了一个分组的密码输出被用作下一分组的密钥。

[0278] 在一些实施例中，在一保密箱寻求与另一保密箱通信时，保密箱执行初始的“相互介绍”交换。这一交换可包括公布阶段，接着是发起阶段，然后是响应阶段。

[0279] 在这一公布阶段中，一个保密箱以可被可能需要使用信息的其它保密箱(在 PDN 的其它节点内)访问的方式“公布”关于其自身的一些信息。此信息可包括包含该保密箱的节点的“公”钥、以及网络地址信息(例如，IP 地址、端口、代理信息等)。所公布的信息可用下述方式签名：

[0280] [PuKi+ 信息 +PrKi[SHA-1[信息]]]

[0281] 尽管公布的信息均不必保密，但是优选的是出于私密和安全性原因它不应被混杂地共用。因此，在一些实施例中，信息的“公布”具体而言并不意味着向世界普遍公布，而仅意味着由第一节点向第一节点想要与之通信的至少一个其它节点公布。这可在进行控制的用户的要求下发生，该用户可根据需要按下按钮或转动钥匙或打入口令来验证该操作。

[0282] 在公布之后，一节点可通过发送一发起消息来发起与另一节点的关系。该发起消息优选地包含以下信息：

[0283] 发起方节点的公钥；

[0284] 可任选地，发起方节点的证书(应包括该证书，除非该发起阶段已知为在前关系的刷新)；

[0285] 发起方节点的能力：

[0286] 所需关系的类型(例如，信息交换、“加入网络”关系、刷新在前关系(例如，交换新密钥数据、更新状态、或更新持续时间)、或在前关系的撤消)；以及

[0287] 所请求的持续时间(例如，一次性(仅针对此次交换)、临时(针对很短的间隔或时间段)、或进行中(直至被撤消))；

[0288] 在发起消息中，公钥和证书(若包含)不被加密。该数据的其余部分可被非对称地加密。由此，最终形式可为：

[0289] [PuKi+PrKi[PuIr[PuKi+ 消息]]]+ 证书(若包含)]

[0290] 在接收到发起消息时，应答方节点将该消息解密并验证这些内容(通过核查预期形式)。一旦满足该请求具有正确形式，应答方即就分析该请求并可返回以下结果中的任何一个：

[0291] 是(表示该连接被接受)；

[0292] 否(该连接被拒绝)；或

[0293] 重试(因为临时性原因，例如，因为证书需要被验证，或因为需要向进行控制的用户要求指示，所以该连接目前不能被接受)。

[0294] 这一“是”的响应可包括要用于后续通信的会话密钥、限制该会话密钥的范围的间隔码、以及(可任选地)应答方的证书。该证书应被包括在内，除非该响应已知为在前关系的刷新。

[0295] “否”响应可包括解释码，和 / 或可指示该连接可被接受的替换状态 / 能力。

[0296] “重试”响应可包括解释码、和 / 或建议的间隔码。

[0297] 每个响应(无论是“是”、“否”还是“重试”响应)均可被签名并加密如下：

[0298] [PuKr+PrKr[PuKi[PuKr+ 消息]]+ 证书(若包含)]

[0299] 在保密箱之间的另一类交换中，证书被请求或至少一个证书被交换。这一交换可用分层结构方式实现(例如，一保密箱可向第二保密箱请求证书，并且第二保密箱可将该请求中继到第三保密箱，并往回中继第三保密箱的响应)。可执行证书请求 / 交换类型的交换以通过例如向所有证书(除实质上被硬编码在芯片中的最终证书之外)随附过期日期来简化在 PDN 中实现撤消的方法。这一最终证书可以是证书授权机构的公钥，并且可以有一个以上的最终证书。

[0300] 保密箱所使用的证书可包含以下信息：

[0301] 被证明实体的公钥；

[0302] 标识被证明实体的设备类型的信息；

[0303] 过期日期和时间；

[0304] 证书授权机构的公钥；以及

[0305] 由证书授权机构生成的、每个证书的数字签名。

[0306] 在保密箱之间的另一类交换中，信息被请求或交换。加入 PDN 的任何节点通常将需要知道关于该 PDN 的其它成员的更多情况，以便于实现高效并且高安全性的内容和密钥共享。此过程可称为“自举”，并且在每个节点被介绍给该 PDN (在被允许的情况下)其它节点时发生，并且每对节点被允许执行认证交换。定义节点的信息优选地本身以与 PDN 内的(受保护)内容相同的方式来处理(例如，此信息可根据与用于转加密内容的相同协议来加密，并可由应用于内容的相同使用规则来保护)。

[0307] 可由 PDN 的保密箱请求或在其间交换的信息的具体类型的示例包括如下：

[0308] 网络树结构信息(例如，PDN 中节点的数目和种类及其地理位置)；

[0309] 节点标识和地址信息(例如，IP 地址、代理、电子邮件和域、设备名称和描述、以及地理位置)；

[0310] 用户标识和个人信息(例如，用于实现“家长”控制或其它访问控制的信息、和 / 或个人观看历史)；以及

[0311] 用于控制用户 ID 和地址信息的信息(例如，在支付当场交易时使用的信用卡号)。

[0312] 构想了本发明的实施例可被配置成转加密许多不同类型中的一种或多种的内容，并且经转加密内容可具有许多不同格式中的任一种格式。尽管本发明的实施例可被配置成处理具有常用格式的内容，但是构想了(随着时间过去)例如在需要保护新形的内容和 / 或

向内容提供新类型的知识产权保护时，此类实施例可被修改或补充以处理其它格式的内容以及实现内容格式之间的更多转换。

[0313] 这里(包括在权利要求书中)使用第一项“包括”第二项的表述来表示第一项是第二项或包含第二项。

[0314] 应当理解，尽管这里例示并说明了本发明的一些实施例，但是本发明由权利要求定义并且不限于所说明和示出的特定实施例。

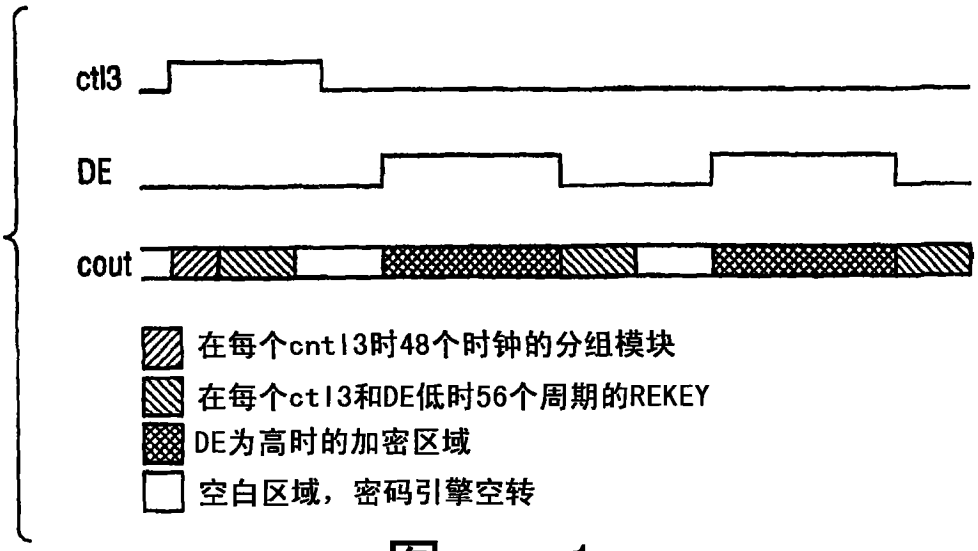


图 1

现有技术

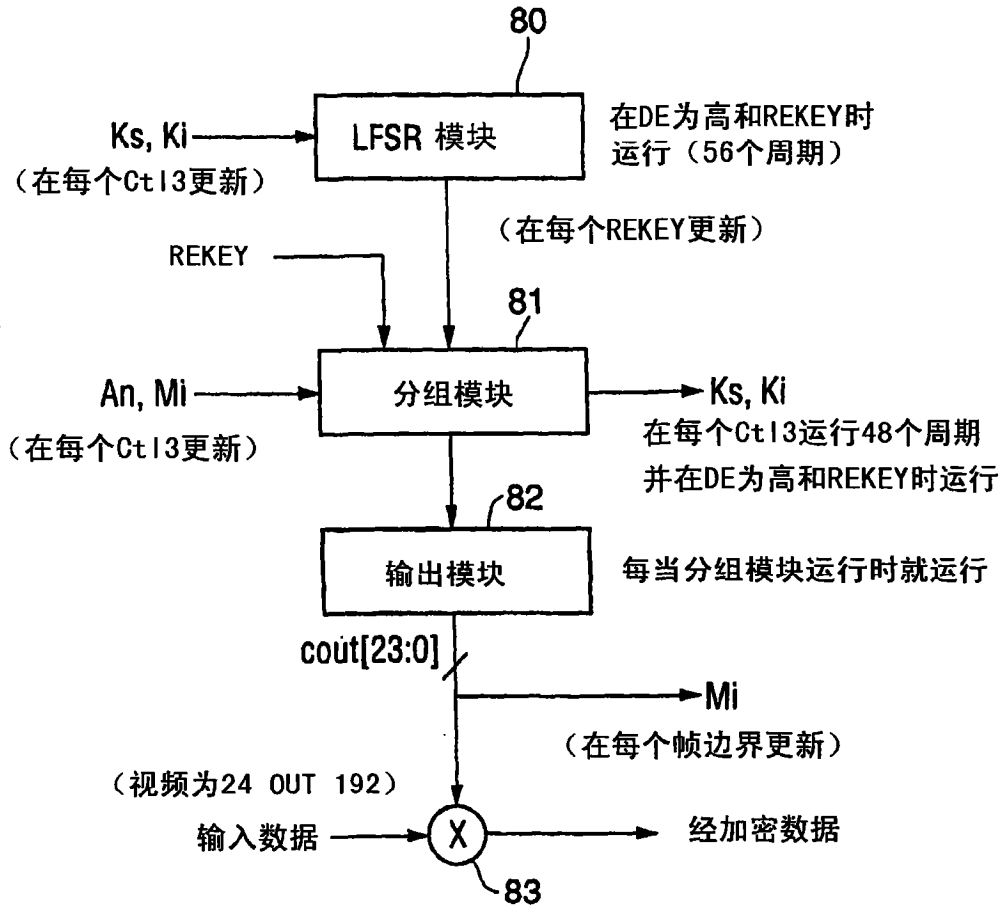


图 2

现有技术

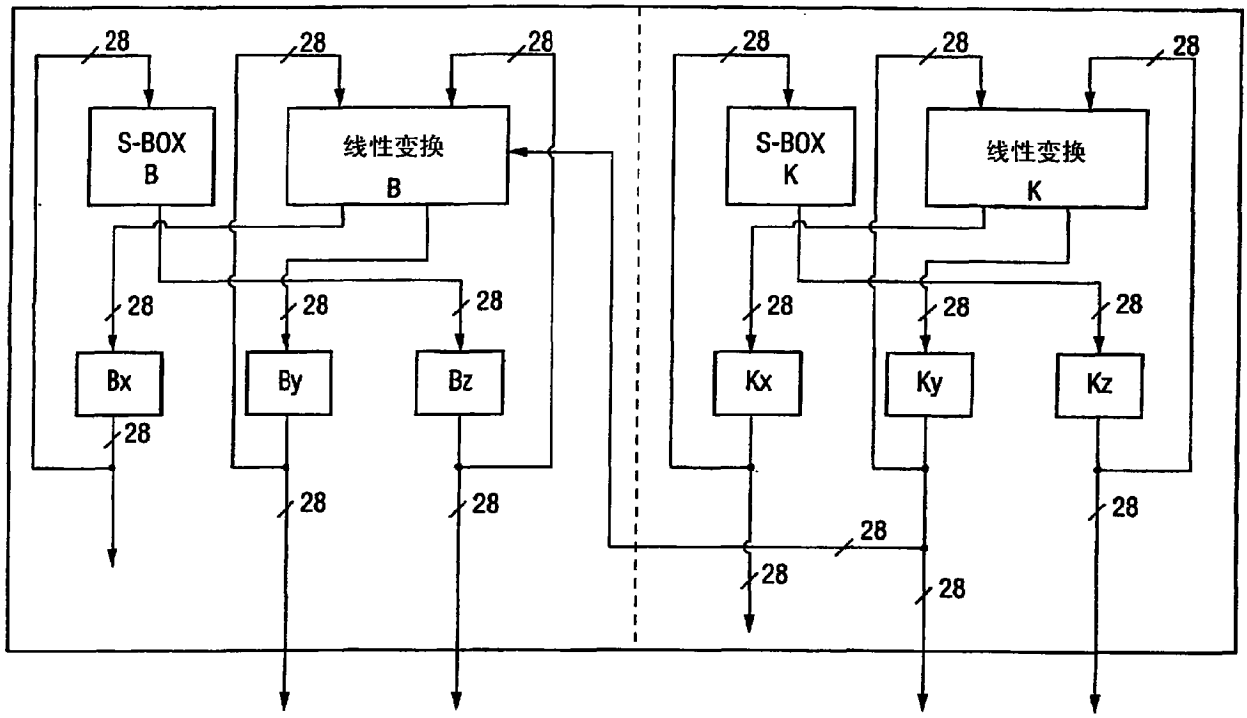


图 3

现有技术

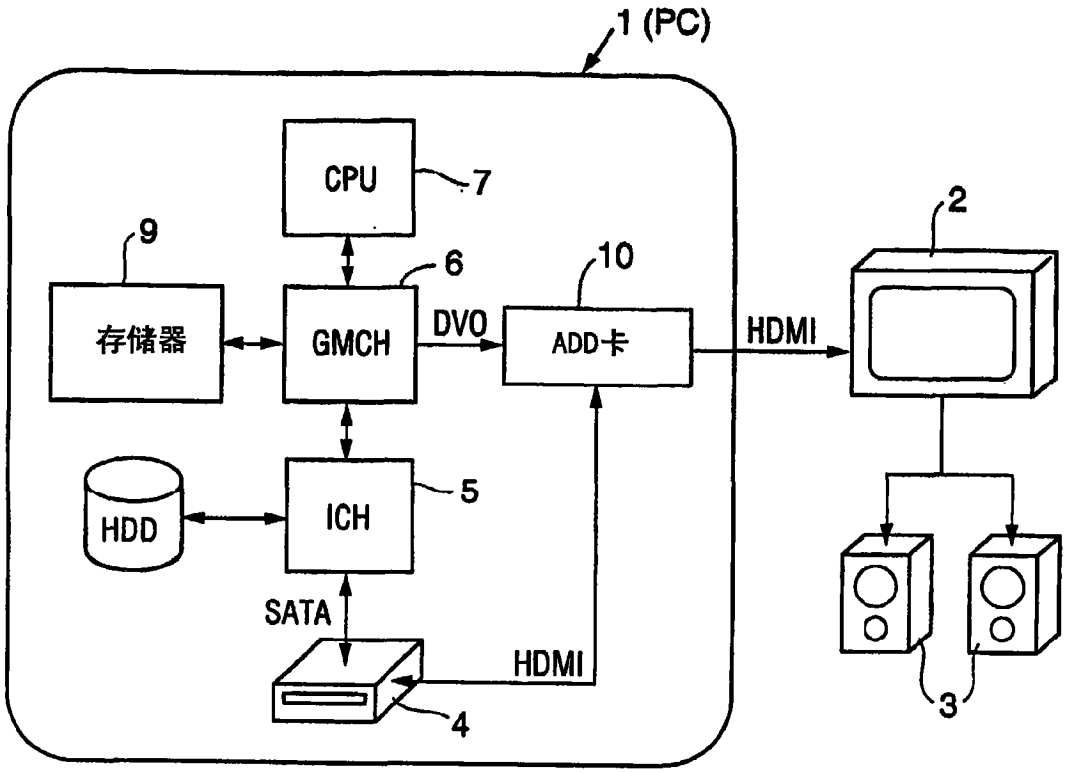

1 (PC)
CPU
7
9
6
10
存储器
GMCH
DVO
ADD卡
HDMI
2
HDD
ICH
5
SATA
HDMI
4
3

图 4

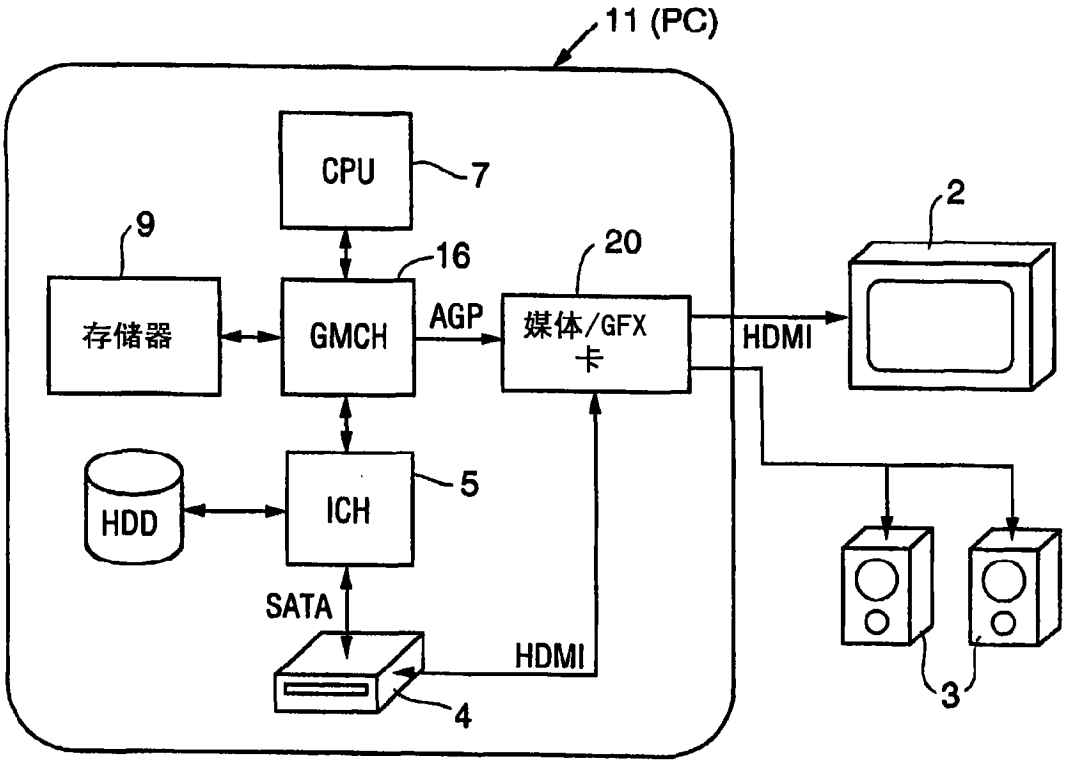

11 (PC)
CPU
7
9
16
20
存储器
GMCH
AGP
媒体/GFX
卡
HDMI
2
HDD
ICH
5
SATA
HDMI
4
3

图 5

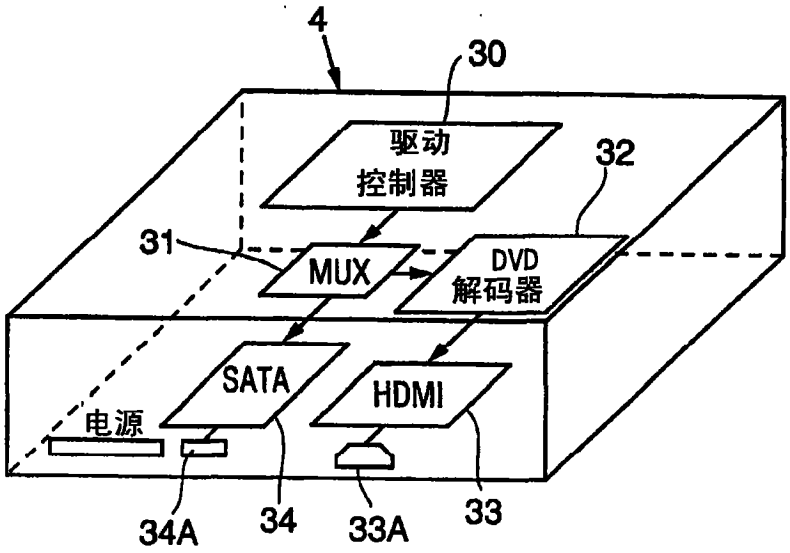

4
30
驱动
控制器
32
31
MUX
DVD
解码器
SATA
HDMI
电源
34A
34
33A
33

图 6

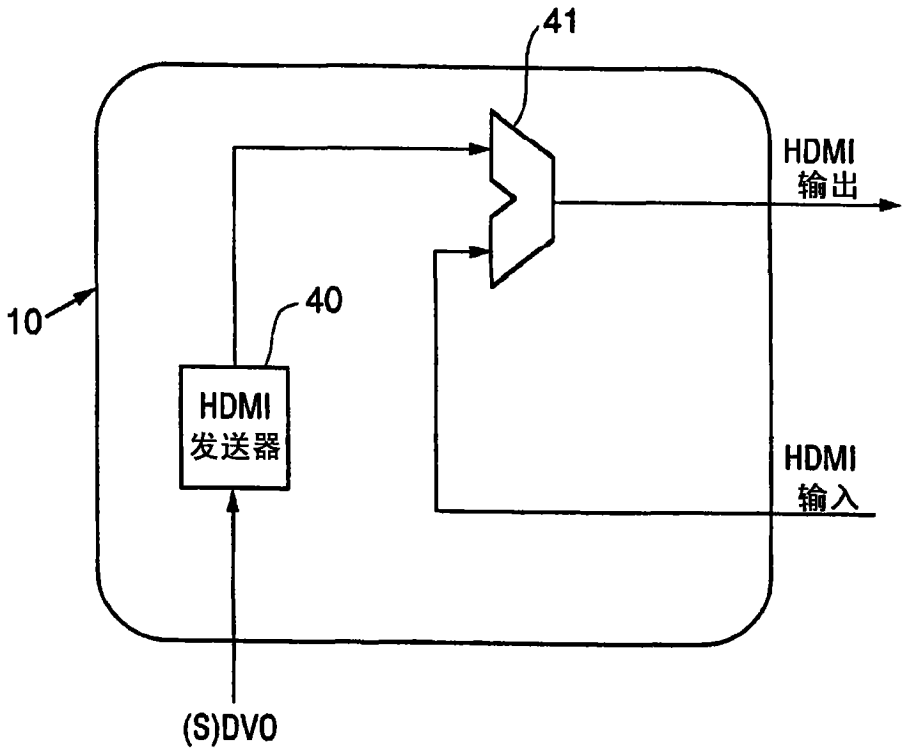

41
HDMI
输出
10
40
HDMI
发送器
HDMI
输入
(S)DVO

图 7

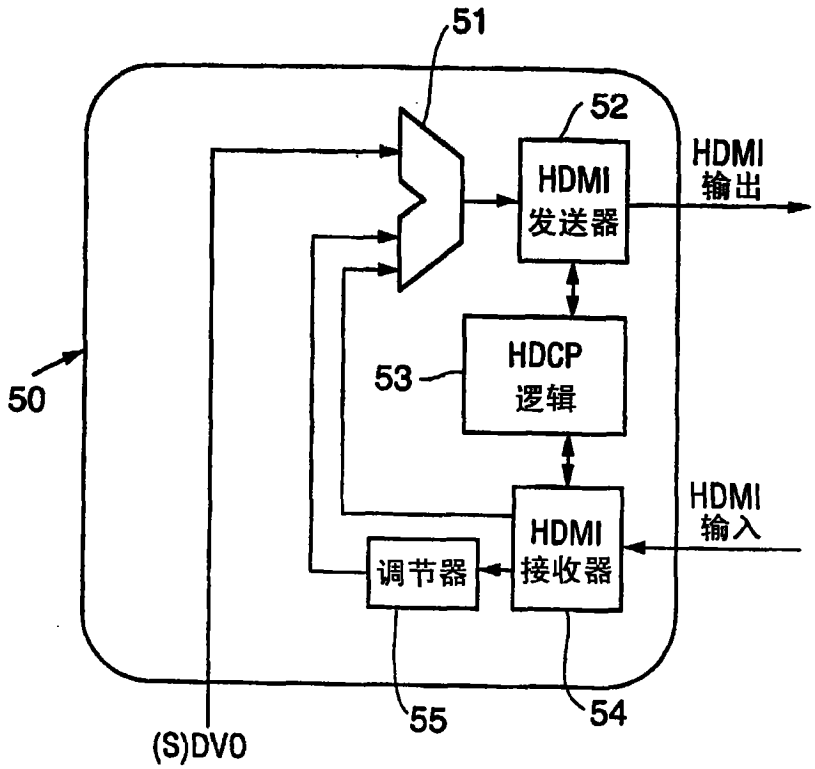

51
52
HDMI
发送器
HDMI
输出
50
53
HDCP
逻辑
HDMI
输入
HDMI
接收器
调节器
55
54
(S)DVO

图 8

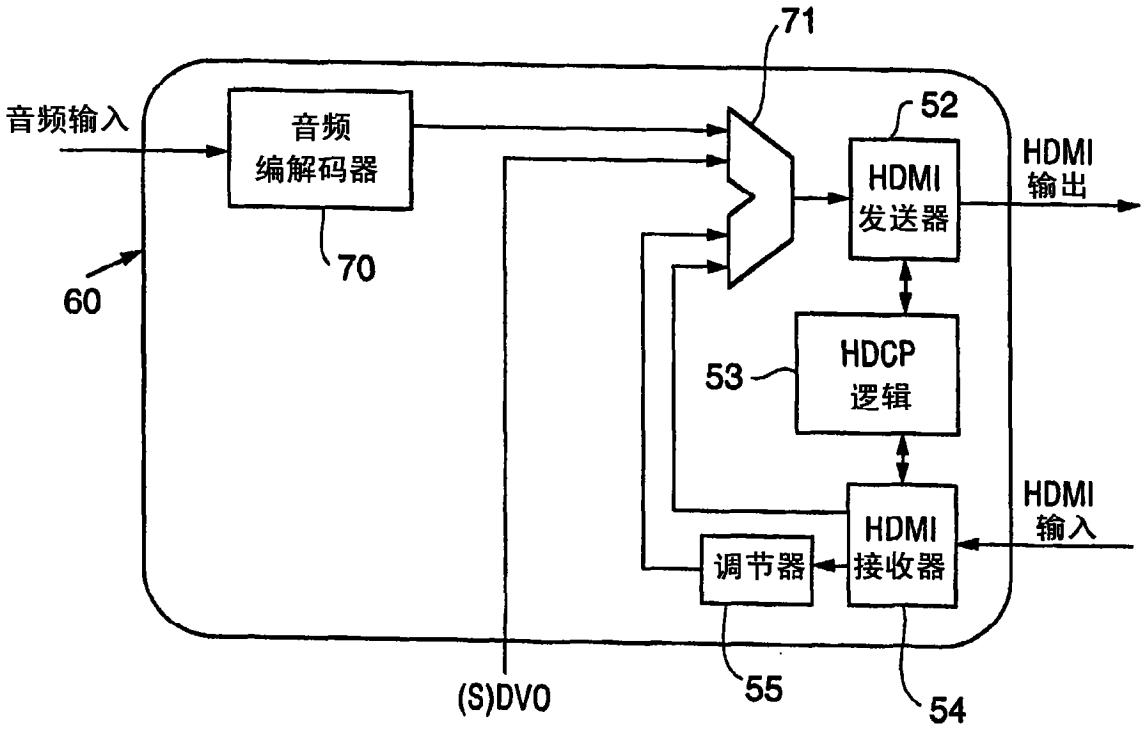

71
音频输入
音频
编解码器
52
HDMI
发送器
HDMI
输出
70
60
53
HDCP
逻辑
HDMI
输入
HDMI
接收器
调节器
55
54
(S)DVO

图 9

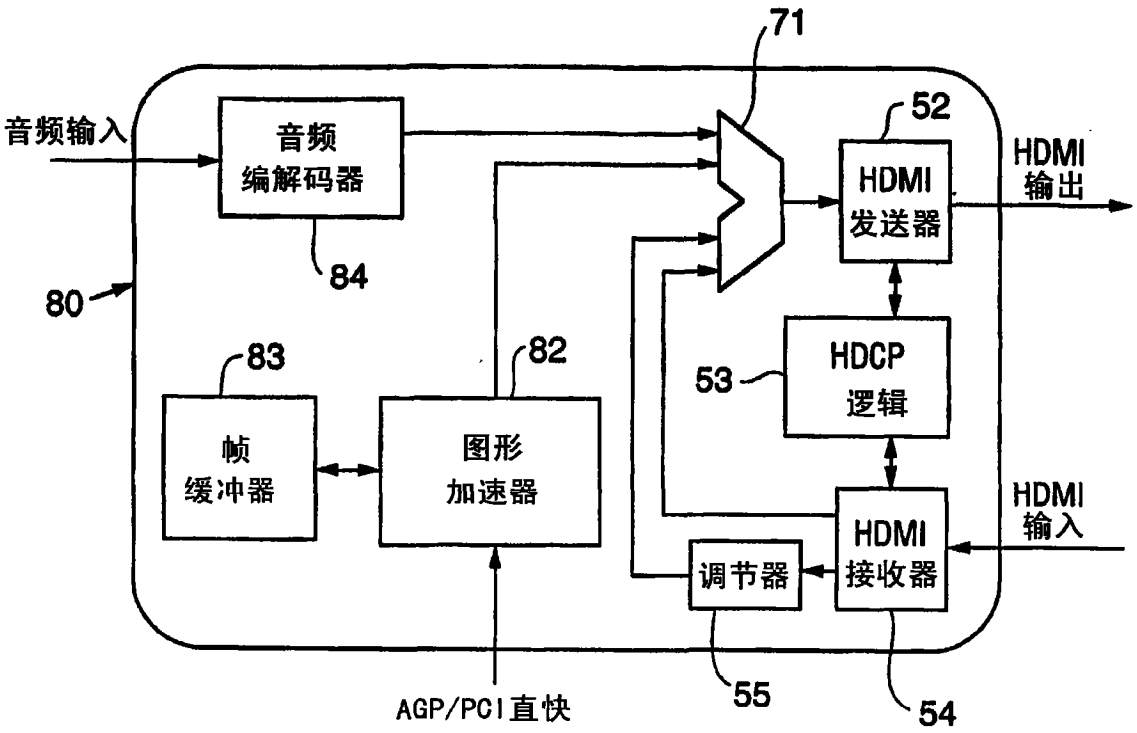

71
音频输入
音频
编解码器
84
80
52
HDMI
发送器
HDMI
输出
83
82
帧
缓冲器
图形
加速器
53
HDCP
逻辑
HDMI
输入
HDMI
接收器
调节器
AGP/PCI直快
55
54

图 10

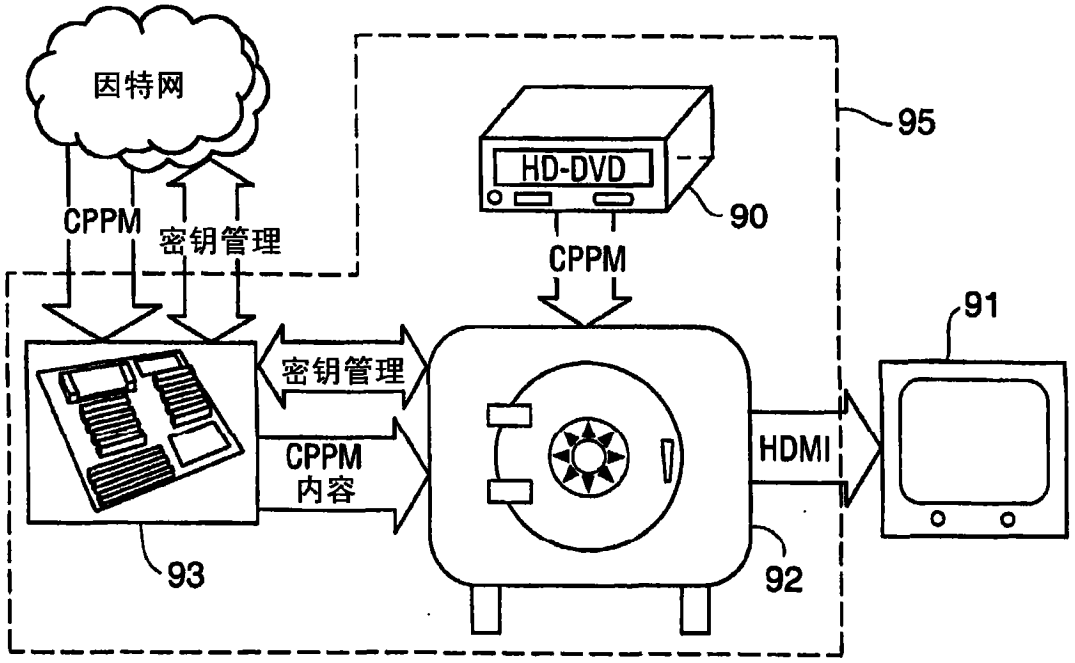

因特网
95
HD-DVD
90
CPPM
密钥管理
CPPM
91
密钥管理
CPPM
内容
HDMI
93
92

图 11

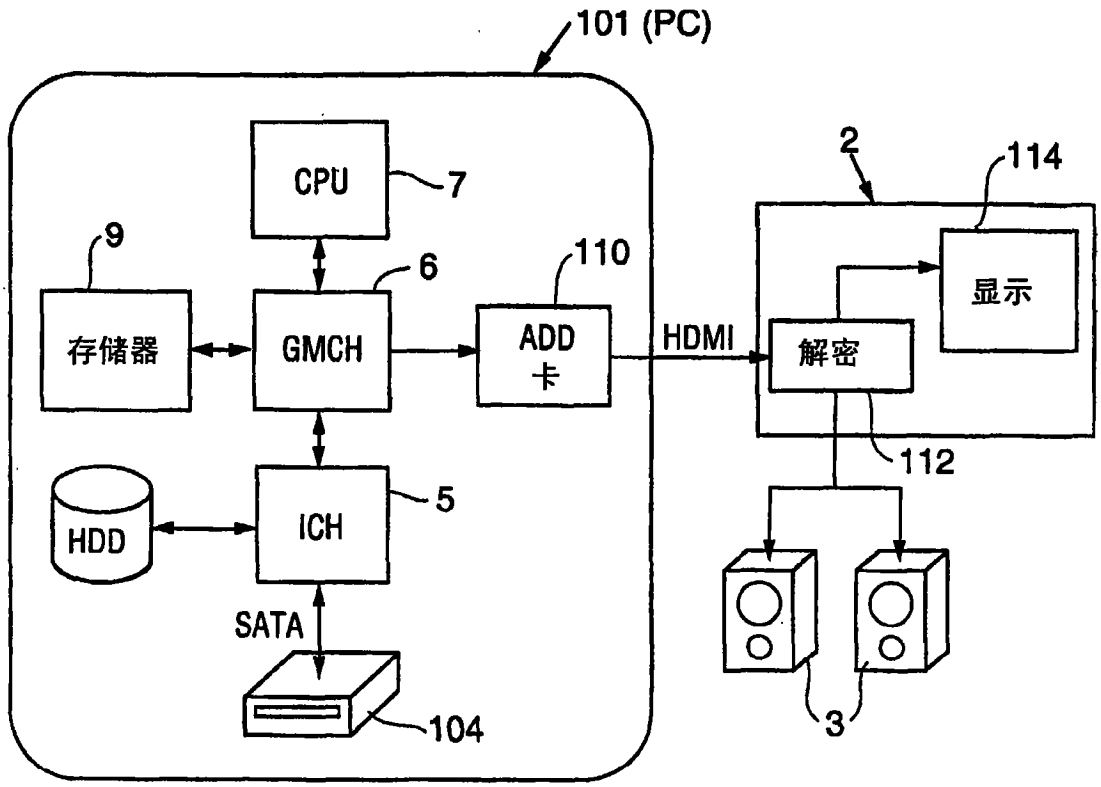

101 (PC)
CPU
7
9
6
110
存储器
GMCH
ADD
卡
HDMI
2
114
显示
解密
112
HDD
ICH
5
SATA
104
3

图 12

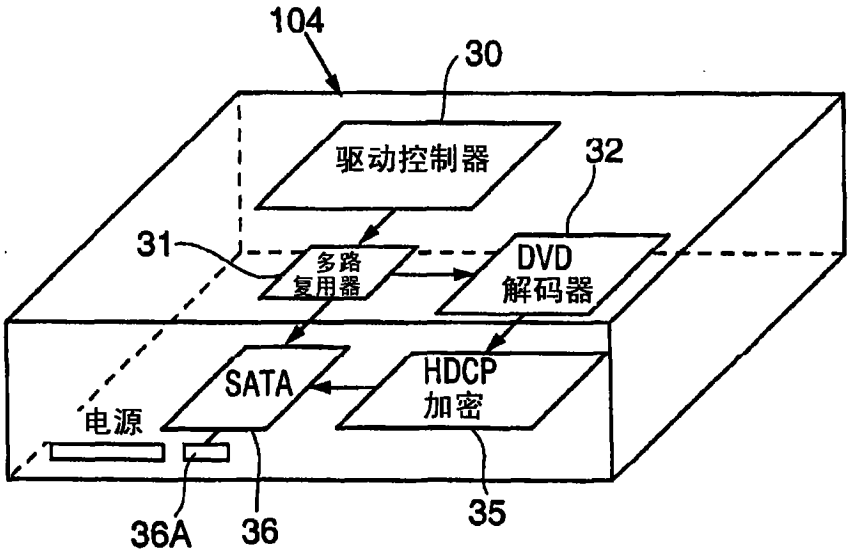

104
30
驱动控制器
32
31
多路
复用器
DVD
解码器
SATA
HDCP
加密
电源
36A
36
35

图 13

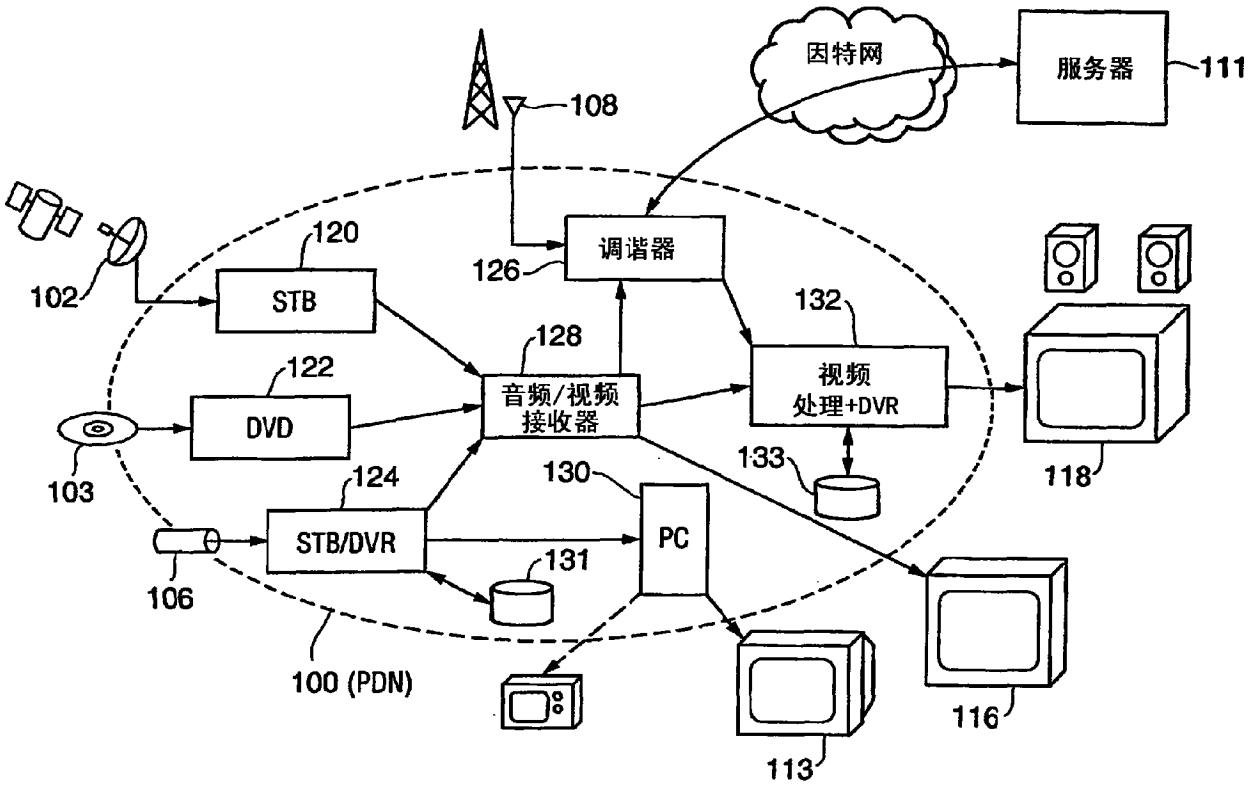

因特网
服务器
111
108
102
120
STB
126
调谐器
132
128
122
DVD
音频/视频
接收器
视频
处理+DVR
103
133
130
118
124
STB/DVR
PC
131
106
100 (PDN)
116
113

图 14

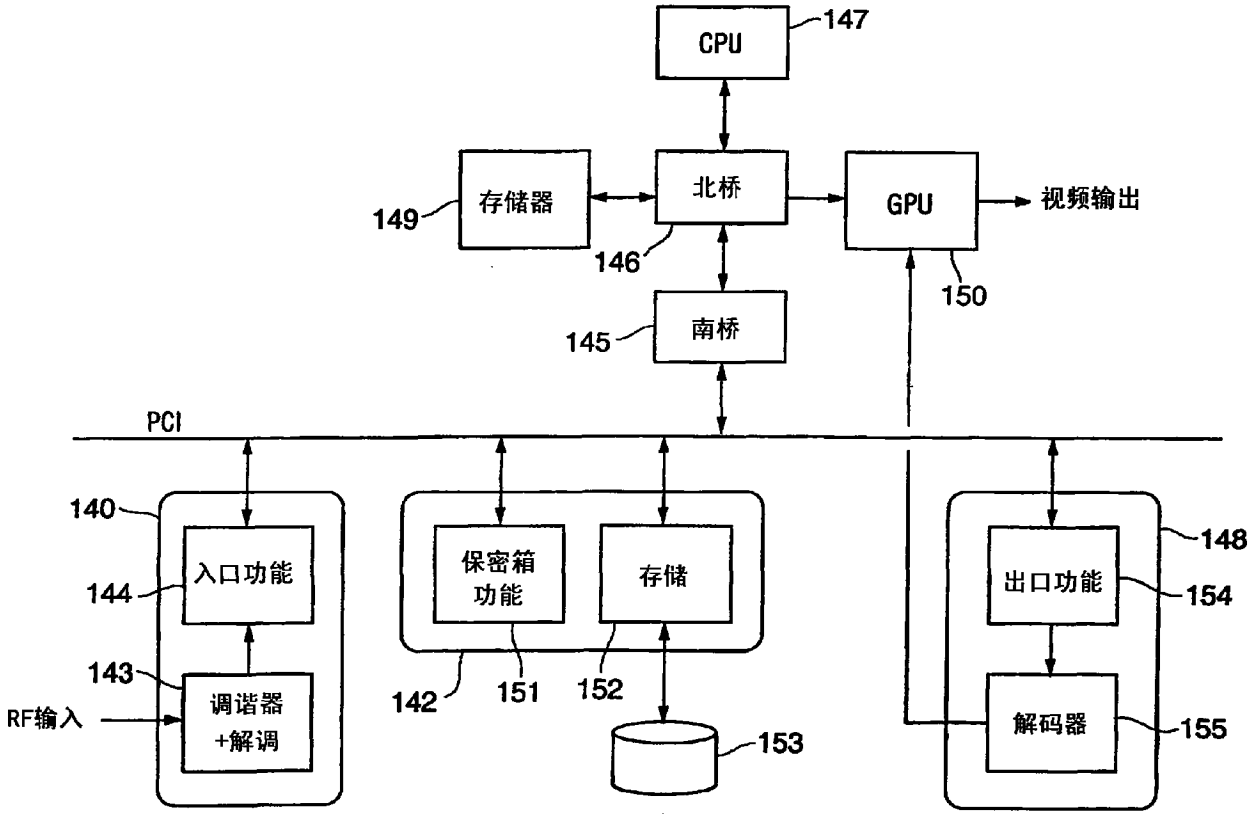

CPU
147
存储器
149
北桥
GPU
视频输出
146
150
南桥
145
PCI
140
入口功能
144
143
调谐器
+解调
RF输入
保密箱
功能
存储
142
151
152
153
出口功能
148
154
解码器
155

图 15

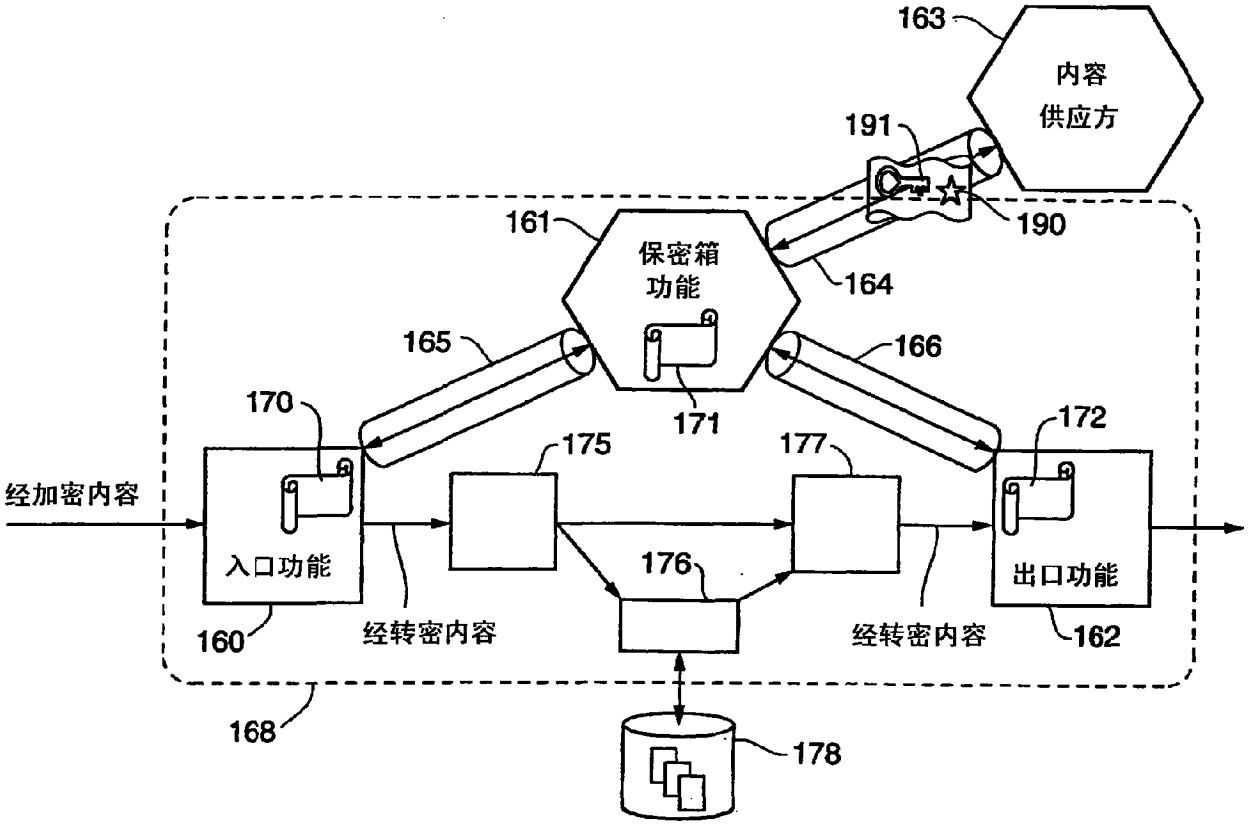

163
内容
供应方
191
190
161
保密箱
功能
164
165
166
171
170
172
175
177
经加密内容
入口功能
176
出口功能
160
经转密内容
经转密内容
162
168
178

图 16

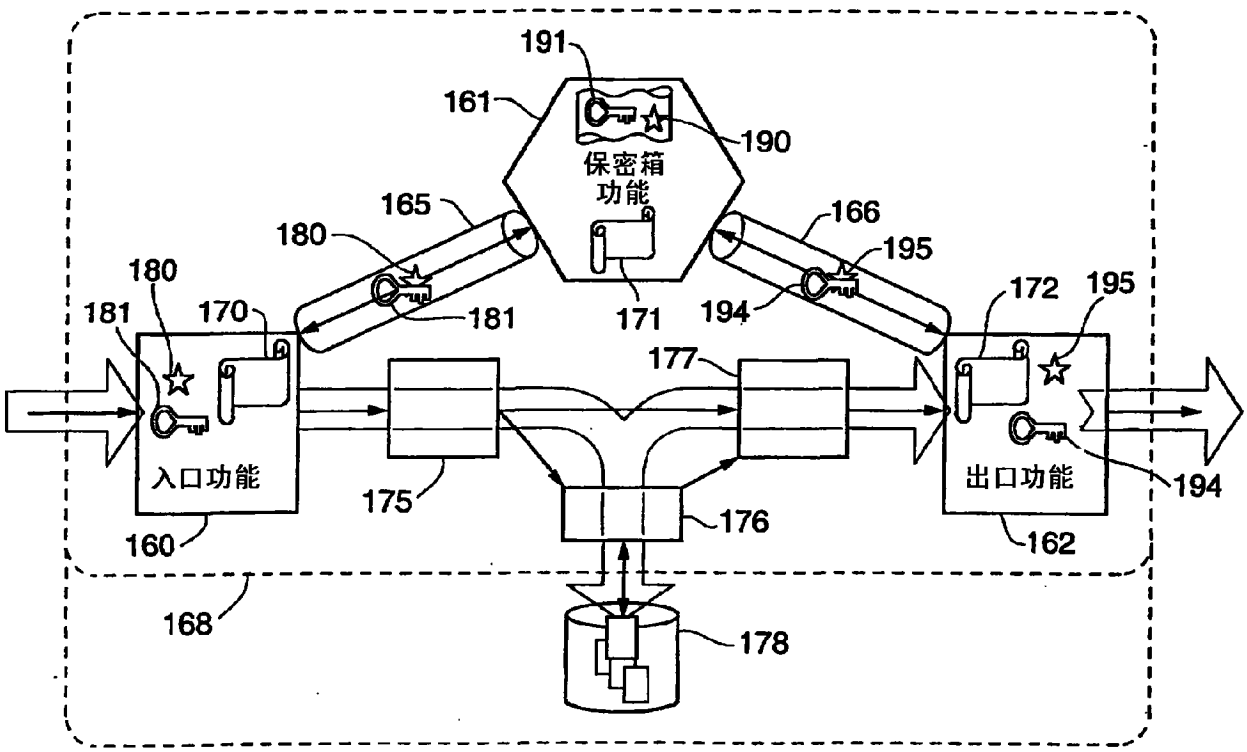

191
161
190
保密箱
功能
165
180
166
195
180
181
170
181
171
194
172
195
177
入口功能
175
176
出口功能
194
160
162
168
178

图 17

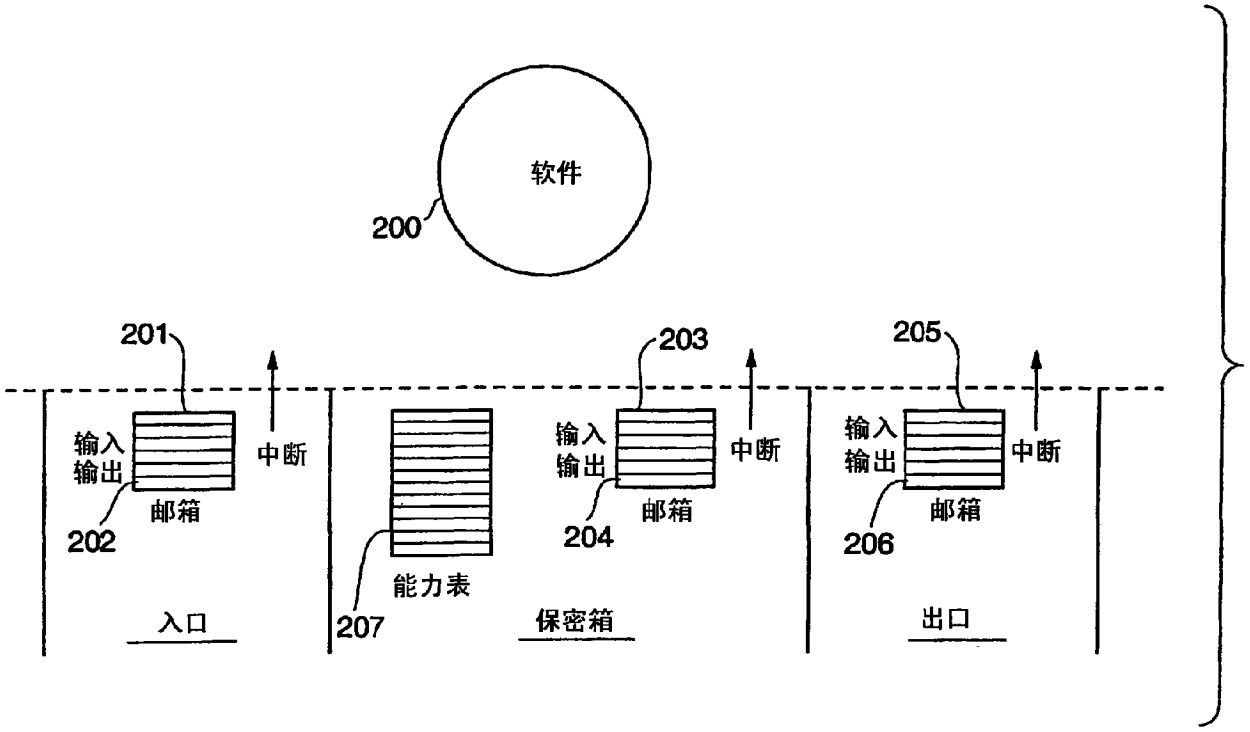

软件
200
201
输入
输出
中断
邮箱
202
入口
207
能力表
保密箱
203
输入
输出
中断
邮箱
204
205
输入
输出
中断
邮箱
206
出口

图 18

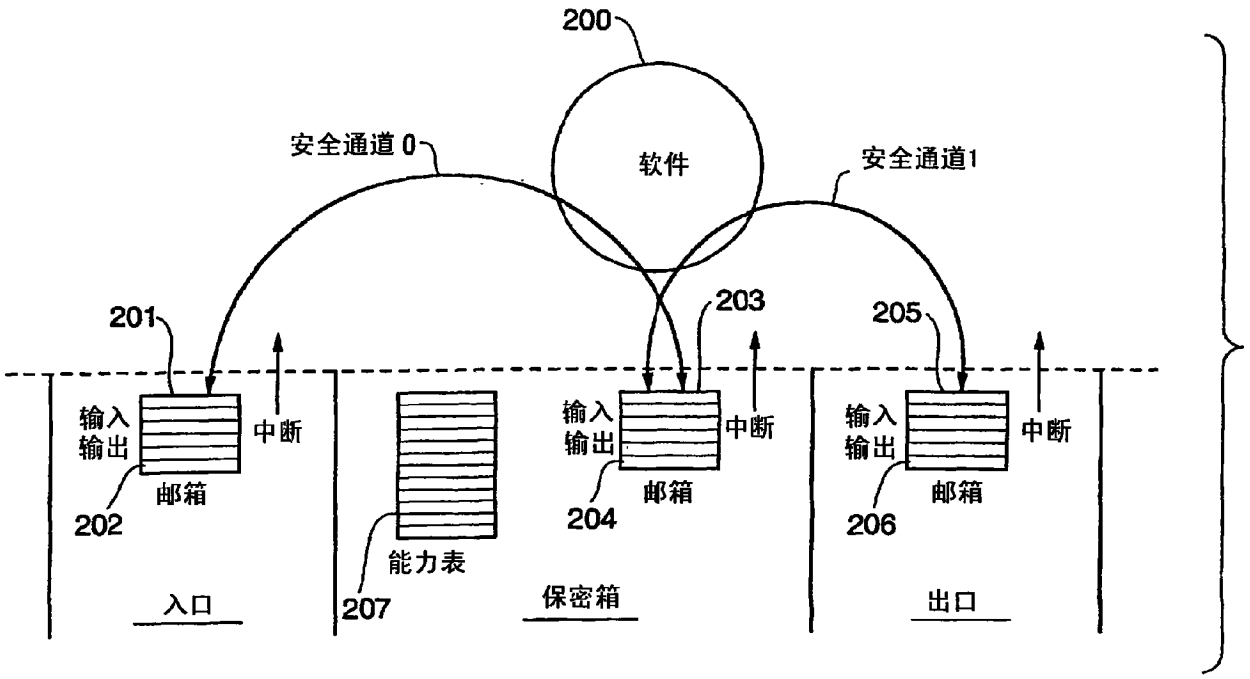

200
软件
安全通道 0
安全通道1
201
203
205
输入
输出
中断
邮箱
202
能力表
207
204
206
入口
保密箱
出口

图 19

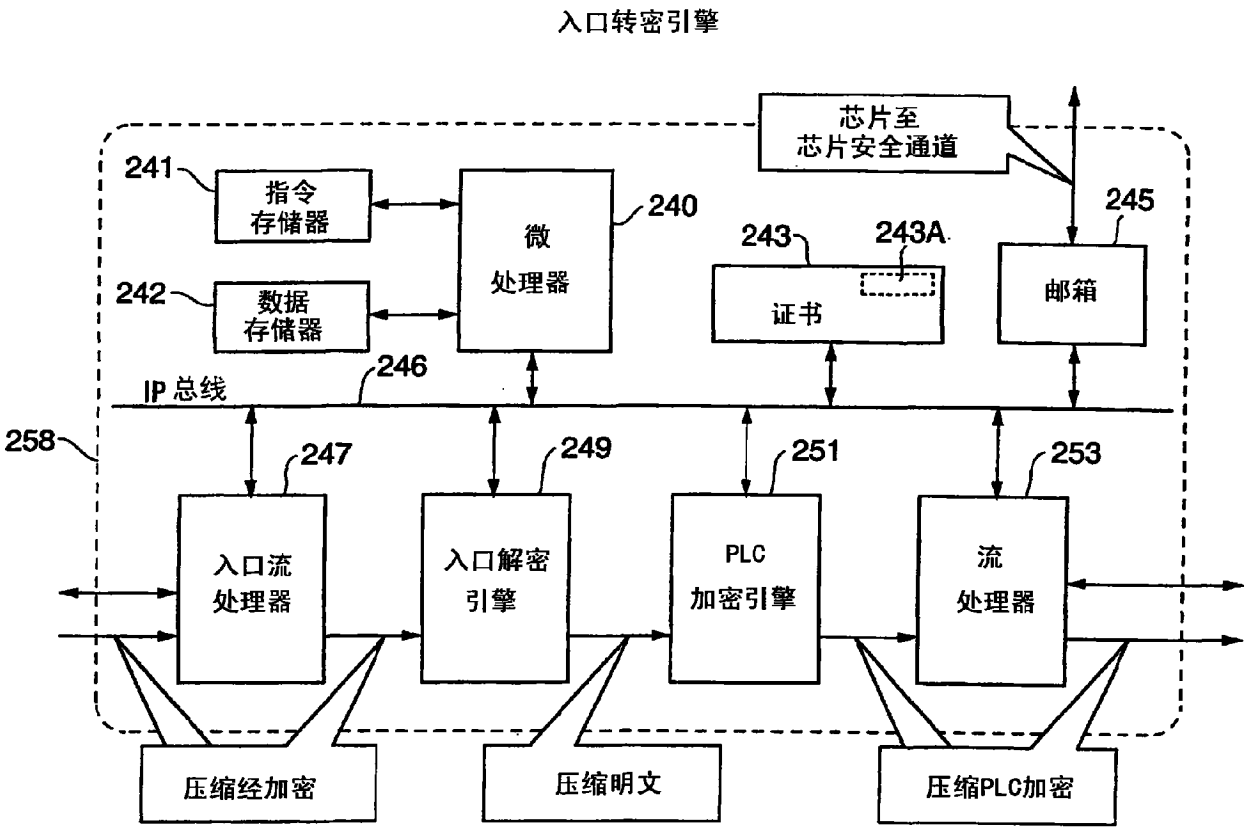

入口转密引擎
芯片至
芯片安全通道
241
指令
存储器
240
微
处理器
243
243A
245
242
数据
存储器
证书
邮箱
246
IP 总线
258
247
249
251
253
入口流
处理器
入口解密
引擎
PLC
加密引擎
流
处理器
压缩经加密
压缩明文
压缩PLC加密

图 20

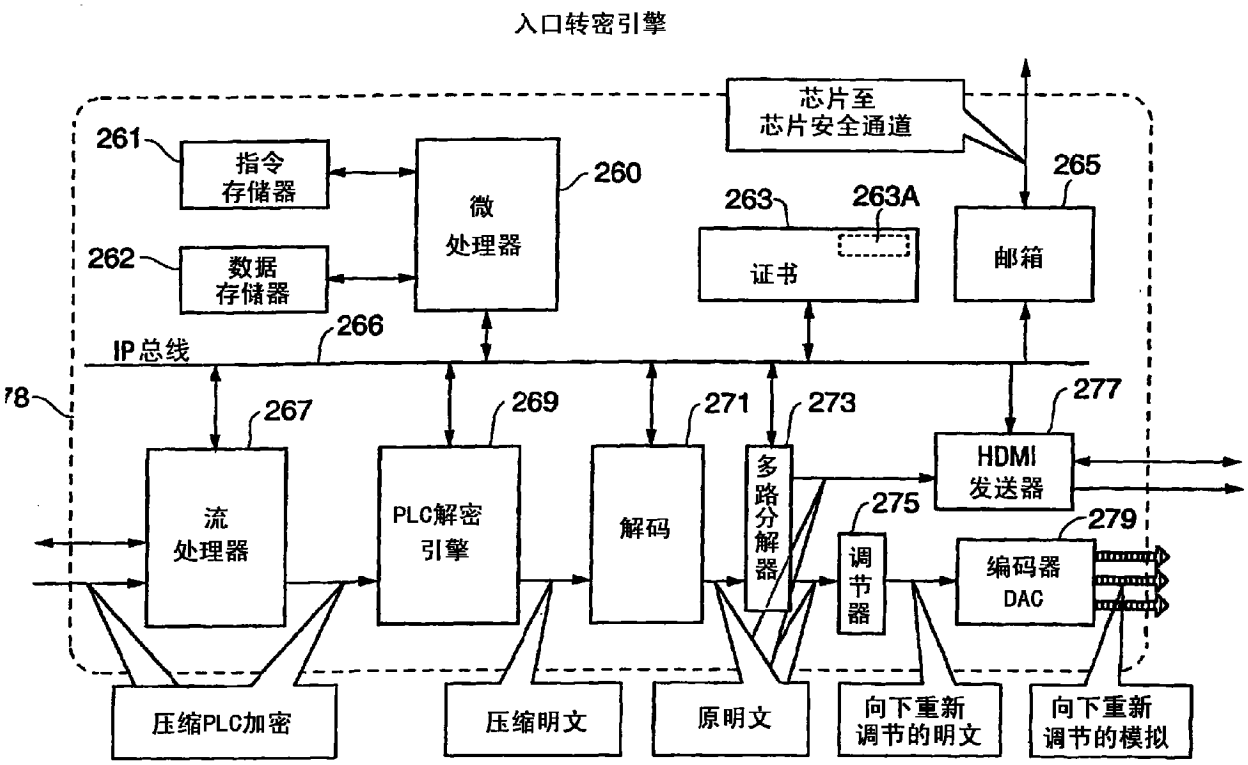

入口转密引擎
芯片至
芯片安全通道
261
指令
存储器
260
微
处理器
263
263A
265
262
数据
存储器
证书
邮箱
IP总线
266
78
267
269
271
273
277
流
处理器
PLC解密
引擎
解码
多
路
分
解
器
HDMI
发送器
275
279
调
节
器
编码器
DAC
压缩PLC加密
压缩明文
原明文
向下重新
调节的明文
向下重新
调节的模拟

图 21

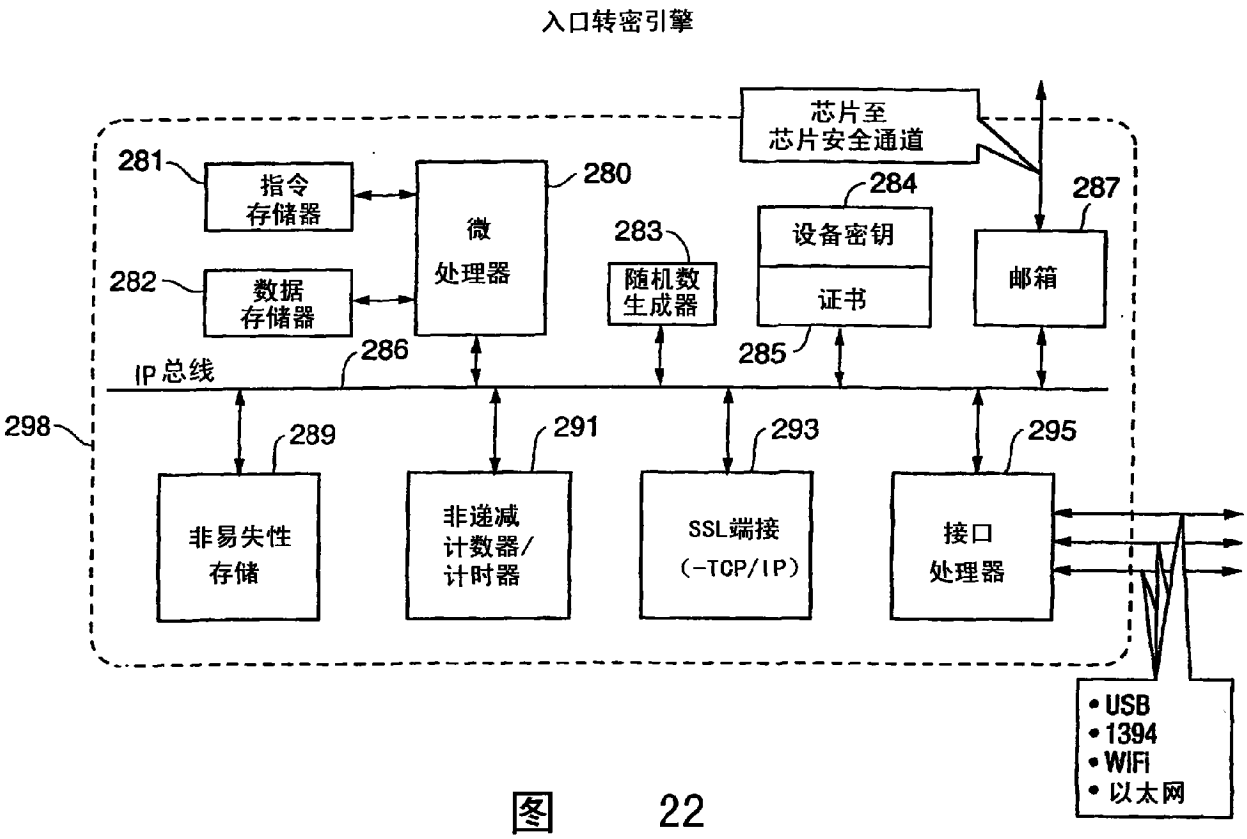

入口转密引擎
芯片至
芯片安全通道
281
指令
存储器
280
微
处理器
284
设备密钥
证书
287
邮箱
283
随机数
生成器
282
数据
存储器
286
IP总线
285
298
289
291
293
295
非易失性
存储
非递减
计数器/
计时器
SSL端接
(-TCP/IP)
接口
处理器
• USB
• 1394
• WiFi
• 以太网

图 22

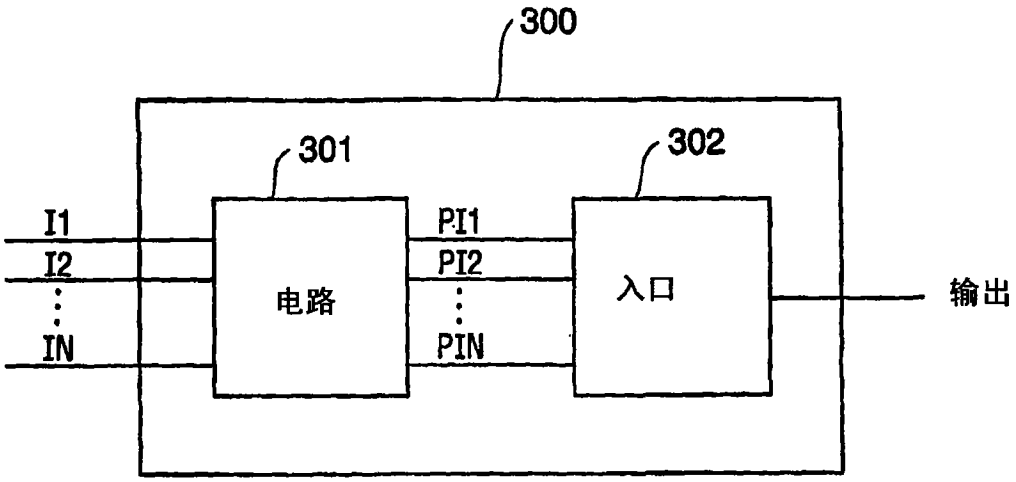

300
301
302
I1
I2
IN
电路
PI1
PI2
PIN
入口
输出

图 23

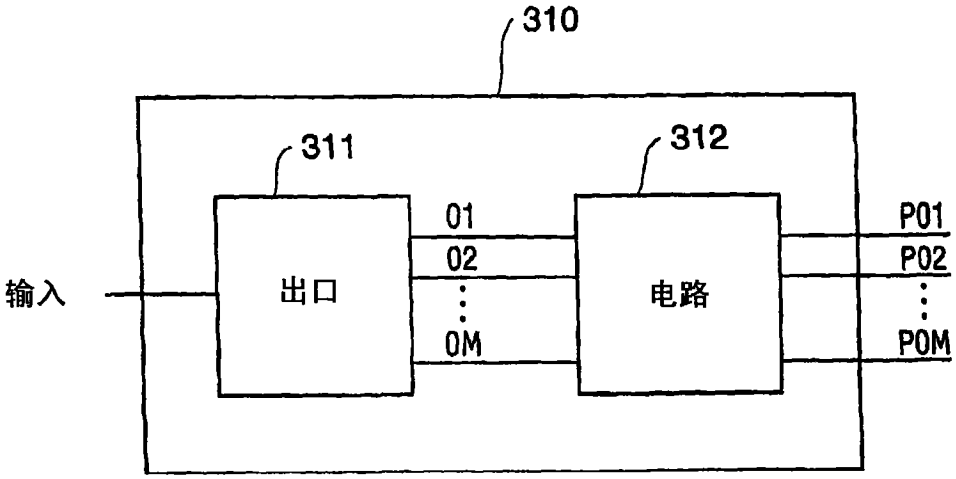

310
311
312
输入
出口
01
02
0M
电路
P01
P02
P0M

图 24