(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 105446926 B
(45)授权公告日 2020.09.22

(21)申请号 201510746463.7

(22)申请日 2015.09.08

(65)同一申请的已公布的文献号
申请公布号 CN 105446926 A

(43)申请公布日 2016.03.30

(30)优先权数据
62/048,142 2014.09.09 US
14/608,900 2015.01.29 US

(73)专利权人 纳瑞塔有限责任公司
地址 美国科罗拉多州

(72)发明人 耶罗默·珀赖因 赫维·古比尔
莫里斯·杰勒德·范里克
威廉·比尔斯 尼古拉斯·费歇尔
本杰明·布赖恩·艾里斯
格雷戈里·杜瓦尔

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 倪斌

(51)Int.Cl.
G06F 13/42(2006.01)
G06F 13/20(2006.01)

(56)对比文件
CN 101199205 A,2008.06.11
CN 103535044 A,2014.01.22
CN 1413025 A,2003.04.23
EP 2541959 A1,2013.01.02
US 8505064 B2,2013.08.06

审查员 张娜娜

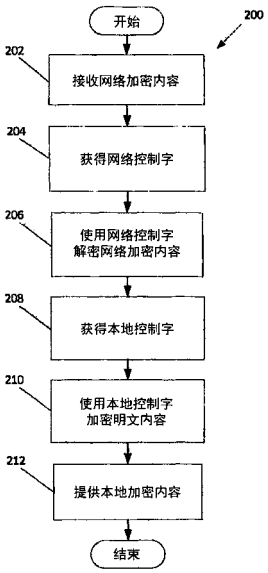
权利要求书3页 说明书24页 附图17页

(54)发明名称

用于执行传输I/O的USB接口

(57)摘要

描述了一种用于实现传输I/O系统的系统和方法。可由一装置接收网络加密内容。该装置可将网络加密内容提供给安全处理器，如智能卡。该安全处理器获得网络控制字，该网络控制字可被用于解密该网络加密内容。安全处理器可以解密该网络加密内容以产生明文内容。在实施例中，安全处理器随后可以使用本地控制字来产生专用于该装置的本地加密内容。该装置随后可以从安全处理器接收本地加密内容并且使用共享的本地加密密钥来进行对本地加密内容的解密。安全处理器可以经由标准连接器，如经由USB 3.0连接器，来连接到该装置。



CN 105446926 B

1.一种可拆卸安全装置,包括:

至少一个处理器;以及

存储器,存储指令,所述指令在由所述至少一个处理器执行时执行一种方法,所述方法包括:

接收第一网络加密基本流,其中所述第一网络加密基本流是依照第一时钟恢复机制接收的;

接收第二网络加密基本流,其中所述第二网络加密基本流是依照所述第一时钟恢复机制接收的;

使用至少一个网络控制字来解密所述第一和第二网络加密基本流,以产生第一和第二明文内容流,其中解密所述第一和第二网络加密基本流至少部分基于所述第一时钟恢复机制;

获取至少一个本地控制字;

加密所述第一和第二明文内容流以产生第一和第二本地加密内容流,其中所述第一和第二本地加密内容流是使用所述至少一个本地控制字产生的;

将所述第一和第二本地加密内容流复用到输出流;

向视频处理装置提供所述输出流,其中所述输出流是依照所述第一时钟恢复机制提供的,

其中所述本地控制字是所述视频处理装置独有的。

2.根据权利要求1的可拆卸安全装置,其中所述可拆卸安全装置是智能芯片。

3.根据权利要求1的可拆卸安全装置,其中所述可拆卸安全装置包括USB3.0连接器。

4.根据权利要求3的可拆卸安全装置,其中所述方法还包括:

将Receive-管脚配置为SC_out-接口;

将Receive+管脚配置为SC_out+接口;

将Transmit-管脚配置为SC_IN-接口;以及

将Transmit+管脚配置为SC_IN+接口。

5.根据权利要求1的可拆卸安全装置,其中加密所述第一和第二明文内容流利用了传输模式加密。

6.根据权利要求1的可拆卸安全装置,其中加密所述第一和第二明文内容流利用了批量模式加密。

7.根据权利要求1的可拆卸安全装置,其中所述可拆卸安全装置和所述视频处理装置使用LVDS信令进行通信。

8.根据权利要求1的可拆卸安全装置,其中所述至少一个本地控制字是由所述可拆卸安全装置产生的。

9.根据权利要求1的可拆卸安全装置,还包括:

获得第一本地控制字,其中使用所述第一本地控制字加密所述第一明文内容流;以及

获得可选的附加本地控制字,其中使用所述可选的附加本地控制字加密可选的附加网络内容流,并且其中部分或者全部本地控制字是不相同的。

10.一种编码有计算机可执行指令的计算机存储媒体,所述指令当被安全装置的至少一个处理器执行时,执行一种方法,所述方法包括:

接收第一网络加密基本流，其中所述第一网络加密基本流包括第一时钟恢复数据；

接收第二网络加密基本流，其中所述第二网络加密基本流包括第二时钟恢复数据；

使用至少一个网络控制字来解密所述第一和第二网络加密基本流，以产生第一和第二明文内容流，其中解密所述第一和第二网络加密基本流至少部分基于所述第一和第二时钟恢复数据；

获取至少一个本地控制字；

加密所述第一和第二明文内容流以产生第一和第二本地加密内容流，其中所述第一和第二本地加密内容流是使用所述至少一个本地控制字产生的；

将所述第一和第二本地加密内容流复用到输出流中；

向所述输出流增加第三时钟恢复数据；以及

向视频处理装置提供所述输出流，

其中所述本地控制字是所述视频处理装置独有的。

11.根据权利要求10的计算机存储媒体，其中第一网络控制字被用于使用所述第一时钟恢复数据解密所述第一网络加密基本流，而第二网络控制字被用于使用所述第二时钟恢复数据解密所述第二网络加密基本流，并且其中所述第一和第二网络控制字是不相同的。

12.根据权利要求10的计算机存储媒体，其中所述至少一个本地控制字是由可拆卸安全装置产生的。

13.根据权利要求10的计算机存储媒体，其中所述方法还包括：

获得第一本地控制字，其中使用所述第一本地控制字加密所述第一明文内容流；以及

获得可选的附加本地控制字，其中使用所述可选的附加本地控制字加密可选的附加网络内容流，并且其中部分或者全部本地控制字是不相同的。

14.根据权利要求10的计算机存储媒体，其中通过连接器提供所述输出流。

15.根据权利要求14的计算机存储媒体，其中所述连接器是USB 3.0连接器。

16.一种在安全装置上执行的使用传输I/O系统来接入内容的方法，包括：

接收第一网络加密基本流，其中所述第一网络加密基本流包括第一时钟恢复数据；

接收第二网络加密基本流，其中所述第二网络加密基本流包括第二时钟恢复数据；

使用至少一个网络控制字来解密所述第一和第二网络加密基本流，以产生第一和第二明文内容流，其中解密所述第一和第二网络加密基本流至少部分基于所述第一和第二时钟恢复数据；

获取至少一个本地控制字；

加密所述第一和第二明文内容流以产生第一和第二本地加密内容流，其中所述第一和第二本地加密内容流是使用所述至少一个本地控制字产生的；

将所述第一和第二本地加密内容流复用到输出流中；

向所述输出流增加第三时钟恢复数据；以及

向视频处理装置提供所述输出流，

其中所述本地控制字是所述视频处理装置独有的。

17.根据权利要求16的方法，其中第一网络控制字被用于使用所述第一时钟恢复数据解密所述第一网络加密基本流，而第二网络控制字被用于使用所述第二时钟恢复数据解密所述第二网络加密基本流，并且其中所述第一和第二网络控制字是不相同的。

18.根据权利要求16的方法,其中所述至少一个本地控制字是由可拆卸安全装置产生的。

19.根据权利要求16的方法,其中所述方法还包括:

获得第一本地控制字,其中使用所述第一本地控制字加密所述第一明文内容流;以及

获得可选的附加本地控制字,其中使用所述可选的附加本地控制字加密可选的附加网络内容流,并且其中部分或者全部本地控制字是不相同的。

20.根据权利要求16的方法,其中通过连接器提供所述输出流。

21.根据权利要求20的方法,其中所述连接器是USB 3.0连接器。

用于执行传输I/O的USB接口

背景技术

[0001] 数字视频广播(DVB)是国际上认可的用于通过有线、卫星以及其他传输媒介传输数字电视的标准。DVB架构的缺点在于用于解密内容的网络控制字很容易在互联网上共享，从而允许非订户接入广播内容。本发明的实施例的提出正是针对这一通常的环境。

发明内容

[0002] 本发明的实施例涉及使用传输(transport)I/O系统来接入内容的系统和方法。在实施例中，安全处理器接收网络加密内容。该安全处理器可能使用网络控制字解密网络加密内容。在该实施例中，网络控制字从来不离开安全处理器，并且因此防止了被未授权的用户拦截。

[0003] 在另一些实施例中，在解密网络加密内容后，安全处理器可能使用本地控制字来重新加密内容从而产生本地加密内容。该本地加密内容可以是针对特定装置独有加密的，所述特定装置例如是机顶盒、片上系统，或者能够接收和修改内容的任意其他类型的装置。在实施例中，安全处理器向该装置提供本地加密内容。

[0004] 该装置可以接收本地加密内容并且获得本地控制字。使用该本地控制字，该装置可以解密本地加密内容以产生明文内容。该明文内容可被该装置处理。例如，该装置可以显示该内容或者存储该内容以便于后续使用。在实施例中，安全处理器可以利用标准连接来实现与多种不同类型的装置的交互。

[0005] 发明内容被提供用于以简化的形式介绍对概念的选择，这些概念在下文的具体实施方式中详细描述。发明内容并非用于标明请求保护的主题的关键特征或者必要特征，也不旨在限制要求保护的主题的范围。

附图说明

[0006] 在所有附图中相同的附图标记表示相同的单元或者相同类型的单元。

[0007] 附图1示出了可以用于传输I/O系统以保护内容的通信系统100。

[0008] 附图2是示出执行网络内容解密的方法200的实施例的流程图。

[0009] 附图3是用于处理本地加密内容的方法300的实施例。

[0010] 附图4是用于使用传输I/O系统来接收和处理保护的内容的方法400的实施例。

[0011] 附图5是可被用于重置安全装置的功能的方法500的实施例。

[0012] 附图6是包调节方法600的实施例。

[0013] 附图7是示出了在ISO-7816智能卡和能够支持本文公开的系统和方法的智能卡之间的兼容性的实施例。

[0014] 附图8是可以用于本文描述的系统或者执行本文描述的方法的安全处理装置800的实施例。

[0015] 附图9是可被用于执行传输I/O系统方法并且是本文公开的系统的一部分的机顶盒的实施例。

[0016] 附图10示出了用于实现本文公开的系统和方法的计算机环境和计算机系统1000的实施例。

[0017] 附图11示出了可以与智能芯片一起使用的示例性连接器1100。

[0018] 附图12是使用了连接器的条件接入系统1200的实施例。

[0019] 附图13是用于确定是否为条件接入模式配置连接器的方法1300的实施例。

[0020] 附图14是用于确定是否执行条件接入操作的方法1400的实施例。

[0021] 附图15是表示用于通过标准连接器执行网络内容解密的方法1500的实施例的流程图。

[0022] 附图16是用于处理通过连接器接收的本地加密内容的方法1600的实施例。

[0023] 附图17是安全处理装置1700的实施例。

具体实施方式

[0024] 本文描述的各种实施例一般提供用于通过使用传输I/O系统来保护流传输的内容的系统和方法。在实施例中，传输I/O系统可被用于解密内容(例如，但是不限制于，没有将网络加密密钥泄露给未授权部分的网络广播流)而不会将网络加密密钥泄露给未授权方。例如，在实施例中，其中传输I/O系统在数字视频广播环境中运行的实施例中，传输I/O系统可以将控制字维护在智能卡上并且在智能卡上使用该控制字来解密网络广播，而不是将解密的控制字提供给不是智能卡的一部分的解扰器。在其他实施例中，传输I/O系统通过对控制体提供附加加密，将控制字安全传送给其他部件等等方式，来保护控制字不被泄露。本领域技术人员将会明白传输I/O系统可以使用降低控制字的泄露风险的任何其他方式。

[0025] 在实施例中，本文公开的系统和方法可被应用在数字视频广播(DVB)兼容系统中。DVB是一组国际上接受的用于广播数字电视的开放标准。DVB标准定义了分布式系统的物理层和数据链路层二者。存在定义通过多种不同媒体分配内容的DVB标准。例如，在DVB-S、DVB-S2以及DVB-SH规范中定义了卫星传输。在DVB-C和DVB-C2规范中定义了有线传输。在DVB-T和DVB-T2规范中定义了针对标准电视格式的地面电视传输，以及在DVB-H和DVB-H2规范中定义了针对移动电视(例如，用于诸如移动电话之类的手持装置的电视)传输的地面电视传输。在DVB-MT、DVB-MC以及DVB-MS标准中定义了微波传输。

[0026] 除了定义物理曾和数据链路层之外，DVB标准集合还包括用于提供对传输的内容的条件接入保护的标准。例子包括DVB-CA、DVB-CSA以及DVB-CI标准。条件接入是通过在接入内容之前要求装置满足某些标准来保护内容的方法。条件接入在确保广播内容仅仅对于具体广播系统(例如，有线和卫星用户等等)的订户是可用的方面起到了重要作用。通常的架构使用全局密钥，称为网络控制字(NCW)，以便执行条件接入。一个或者多个NCW被用于在数据被广播给订户之前对数据进行加密。由头端(例如卫星或者有线电视提供商)在授权控制消息(ECM)中向订户装置发送NCW。ECM在被传输给用户装置之前通常会进行加密。订户装置(例如，无论是硬件或者软件形式的智能卡或者其他条件接入模块)的条件接入系统使用在从头端传输来的授权管理消息(EMM)中接收的信息解密该ECM。该订户装置于是能够使用NCW来解密头端广播的内容。通常，NCW在特定时间周期或者密码周期内使用。一旦密码周期到期，新的密码周期就开始。该头端于是可以向订户装置(一个或多个)传送新的NCW，并且进而使用新的NCW来解密该广播内容。

[0027] DVB条件接入架构的一个主要缺点是:NCW能够被解密并且容易在互联网上共享。由于内容被广播给很多用户,必须针对每个订户,以相同的密钥(例如相同的网络控制字)对内容进行加密。因此,一旦网络控制字被发现,接入到网络的任何未授权的用户(例如非订户)可以使用网络控制字来解密该广播内容。通常,NCW由八(8)比特构成。密码周期的持续时间通常在五(5)到六十(60)秒之间变化。因此,非订户可以基于发现八(8)比特NCW(这是可以在典型的加密周期的持续时间内实现的任务)来击败DVB条件接入架构,。通常,在智能卡获得NCW之后,智能卡将NCW提供给外部装置或者部件。外部装置或部件使用NCW来解密广播内容。但是,该NCW可被截获并且共享给他人,从而允许对内容的未授权共享。

[0028] 尽管本发明将传输I/O系统作为针对DVB条件接入的缺点的解决方案来描述,但是本领域技术人员应该意识到本文公开的方法和系统可被应用来保护在不与DVB架构兼容的其他类型的数据传输流和/或广播(例如,但是不限制于,互联网上的流媒体)中的内容。下面将会参考附图详细描述本文公开的针对传输I/O系统的系统和方法。

[0029] 附图1示出了可以用于传输I/O系统以保护内容的通信系统100。该通信系统包括头端装置102,其从内容提供商104接收内容并且通过通信网络106将内容分配给多个接收装置108。该接收装置可以接入内容并且将其显示给用户。单个接收装置108可以是能够通过通信网络106接收和解码数据传输流的任何装置。这种装置包括,但是不限制于:移动电话、智能电话、个人数字助理(PDA)、卫星或有线机顶盒、台式电脑、膝上电脑、平板电脑、电视、无线广播设备、视频处理装置或者任意其他本领域公知的装置。在实施例中,订户的接收装置108通常能够接入用于解密内容的加密密钥,而在不避开通过通信网络106广播内容的头端装置102使用的安全措施的情况下,非订户不能够接入该加密密钥。

[0030] 在实施例中,头端装置102可以是有线电视提供商的分配点、卫星电视提供商的分配点(例如卫星)、地面无线网络、通过互联网广播内容的服务器,或者能够通过通信网络分配内容的任意其他类型的装置。本领域技术人员能够意识到头端装置102可能是能够通过网络接收、加密以及广播内容的任意类型的装置或装置集合(根据具体情况而定)。

[0031] 在一个实施例中,可以由头端装置102产生在通信系统100上的内容广播。在其他实施例中,头端装置102可以从一个或者多个内容提供商104接收内容。在这种实施例中,头端装置102与一个或者多个内容提供商104电通信。例如,内容提供商可以是通过有线(例如电缆、光纤、或者互联网连接)或者无线连接(例如,通过射频、微波、或者卫星通信)将内容传输给头端装置102的有线、地面或者卫星电视站。在其他例子中,内容可以存储在与头端装置102电通信的数据库中。虽然附图1中将内容提供商104描述为与头端装置102分离的实体,但是在其他实施例中,内容提供商104和头端装置102可以是单个实体。

[0032] 头端装置102具有通过通信网络106向多个接收装置108分配内容的任务。在实施例中,通信网络106可以是互联网、电缆网络、光纤网络、卫星通信网络、地面广播网络(例如通过射频或者微波传输介质进行通信的网络通信)、蜂窝数据网络、广域网(WAN)、局域网(LAN)、老式电话业务(POTS)网、互联网、或者能够流传输、广播和/或以其他方式有助于在多个装置之间数据传输的任意其他类型的通信网络。本领域技术人员将意识到,无论用于在装置之间传输数据的通信网络,本文公开的系统和方法都可被实现为。在很多情况下,头端装置102可以通过通信网络在数据传输流中广播内容而不是将内容发送给某个装置。由于内容是通过通信网络106进行广播,该传输可被能够与通信网络106交互的任意数量的装

置接收到。为了防止未授权用户接入广播的数据传输流，由头端装置102可以在通过通信网络106广播数据传输流之前对数据传输流进行加密。由于网络广播的内容可被多个装置使用，可以使用公共加密密钥(例如网络控制字)来加密网络广播的内容(例如网络加密内容)。在实施例中，网络广播内容可能是网络加密流，其包括内容(如网络加密内容)以及数据。在实施例中，数据包括关于流的信息，例如，但是不限制于，加密信息、定时信息、压缩信息或者任意其他类型的信息。尽管附图1中没有示出，通信网络也还被用于执行在头端装置102和接收装置108之间的双向通信。

[0033] 在实施例中，使用一个或者多个密钥(例如，但是不限制于，网络控制字(NCW))来加密数据传输流。该NCW可在某一个时间段(例如密码周期)内用于加密数据传输流，由此得到网络加密内容的创建。在实施例中，网络加密内容可以是使用公共密钥(例如NCW)加密的，使得网络加密内容可被授权用户(例如订户)解密。该NCW在头端装置102和各个接收装置108之间共享。在一个实施例中，通信系统100根据DVB架构运行。在该实施例中，NCW可以是控制字(CW)，其作为在加密内容时使用的密钥。在该环境中，头端102可以使用ECM消息周期性地将NCW传输给各个订户装置。此外，头端102将包括解密ECM和恢复NCW所需的信息的EMM消息传输给各个订户。在该实施例中，由安全装置或者处理器解密EMM以恢复NCW，所述安全装置或者处理器例如是作为接收装置的一部分或者连接到接收装置的智能卡。该智能卡于是可以将NCW提供给其他部件以进行解密内容，该其他部件是接收装置的一部分或者与接收装置通信。但是，一旦从安全装置和/或处理发送NCW，CW可能被拦截并且与他人共享，从而提供对内容的未授权接入。

[0034] 在实施例中，传输I/O系统通过将解密的控制字维护在安全处理装置(例如，在智能卡、安全处理器、安全存储器，或者该装置的任意其他安全装置或者安全部件上)中来解决这一问题。在该实施例中，解密的CW被维护在安全装置上，因而防止了CW的拦截和共享。在这一实施例中，安全内容(例如，加密的广播或者加密的内容)可以在安全处理装置上被解密。安全处理装置随后可能提供明文内容(例如，解密的内容)。虽然该明文内容可能被拦截以及共享，由于内容的大小和共享该内容所需的带宽决定了其不像共享内容不是那么容易的那么简单。在另一个实施例中，安全处理装置可以唯一地加密内容以便于供被特定装置使用(例如接收装置108)。例如，在该实施例中，使用本地加密密钥或者本地控制字(LCW)的方法可被用于创建本地加密内容。该本地控制字对于本地装置可能是唯一的。安全处理器或者安全处理装置可以随后将本地加密内容提供给本地装置。此外，在实施例中，本地加密内容被唯一加密以用于可以是针对特定装置(例如，但是不限制于，机顶盒、片上系统，或者任意其他类型能够接收和修改内容的任意其他类型的装置)被独有加密。

[0035] 附图2是表示执行网络内容解密的方法200的实施例的流程图。在实施例中，方法200由安全装置或者安全处理器执行。安全装置的一个例子是智能卡。该流程开始于步骤202，在步骤202中从通过安全装置接收网络加密内容的步骤步骤202开始。在实施例中，网络安全内容可以是使用NCW加密的内容。该NCW可以是通用控制字或者加密密钥，其被用于加密和解密发送给多个用户或者订户的内容。在一个实施例中，网络加密内容可以是单一个数据流。在可选实施例中，网络加密内容可以包括多个网络加密流，例如网络加密基本流。网络加密基本流可以是包括例如音频数据、视频数据、闭合字幕数据或者其他类型的数据的流。网络加密基本流可以由来自单一源(例如特定的网络或者信道)的压缩数据构成，

例如特定的网络或者信道。在网络加密内容可以包括多个网络加密基本流的实施例中，在步骤202中，一个或者多个网络加密基本流可被分别接收。但是，在可选实施例中，在步骤202中，可以接收包括多个网络加密基本流的网络加密内容。在该实施例中，可以过滤出各个网络流，例如通过执行PID过滤或者其他类型的过滤，从而在步骤202隔离一个或者多个单独的网络加密基本流。一旦接收网络加密内容，流程继续到获得网络控制字的步骤204。在一个实施例中，网络控制字是由内容提供商(例如，但不限制于，传输内容的头端或者服务器)提供的控制字。在实施例中，网络控制字可以是执行方法200的装置事先已知的。在另一个实施例中，网络控制字可被装置接收。在该实施例中，网络控制字可被加密，并且步骤204可以包括解密该网络控制字。例如，在实施例中，网络控制字可以通过解密包括该网络控制字的ECM来获得。可以通过使用来自于其他消息(例如，EMM)的信息来解密该ECM。虽然ECM和EMM消息是DVB架构的一部分，但是本领域技术人员可以意识到其他内容传输系统和结构可以与本文公开的系统和方法一起使用。

[0036] 流程继续前进到步骤206，在步骤206中使用网络控制字解密该网络加密内容(例如，一个网络加密基本流或者多个网络加密基本流)。在一个实施例中，单个网络控制字被用于解密网络加密内容。在可选实施例中，例如，当网络加密内容包括多个已经各自使用不同的网络控制字加密的网络加密基本流时，多个控制字被用于解密网络加密内容。在这一例子中，在步骤204中获得多个网络控制字，并且随后在步骤206这多个网络控制字被用于解密多个网络基本流。然而，在其他实施例中，单个网络控制字可被用于解密多个网络内容基本流。在这种实施例中，单个网络控制字可被用于解密多个网络加密基本流。在步骤206中的对网络加密内容的解密可以得到明文内容，也就是，内容不受加密保护。因为步骤202-206由安全装置或者安全处理器(例如，但不限制于，智能卡)执行，所以网络控制字被保留在安全装置上。通过将网络控制字维护在装置上，未授权的订户不能够拦截在智能卡和装置(例如机顶盒)之间传输的网络控制字，从而防止了未授权订户接入内容。在附图2未示出的实施例中，在解密步骤206之后，安全处理器可以将明文内容提供用于显示或者存储。然而，在示出的实施例中，可以通过执行本地链路加密来增加保护的附加层。在实施例中，本地链路加密可以包括使用本地控制字(LCW)重新加密明文内容。该本地控制字可以是特定装置独有的加密码密钥。例如，在机顶盒环境中，LCW可以是仅仅与执行方法200的智能卡可与之通信的具体机顶盒共享的加密密钥。在实施例中，针对本地链路加密，可以执行不同类型的加密模式。在一个实施例中，不是所有的表示内容的数据都使用本地链路加密来加密。例如，可以使用传输模式加密。在实施例中，传输模式加密包括确定数据的哪些比特要基于MPEG2传输加密米加密。在另一个实施例中，可以执行批量(Bulk)模式加密。在批量(Bulk)模式加密中，在本地链路加密期间，可以加密所有表示数据的比特。批量(Bulk)模式加密可被用于在装置之间以安全方式交换数据。例如，批量(Bulk)模式加密可被用于将传输输入(例如内容)与由参与对内容的加密/解密的一个或多个部件使用的内部数据进行混合。在其他实施例中，批量(Bulk)模式加密可被用于支持可以提供附加特征的其他类型的内容流，例如互联网协议电视(IPTV)内容流。对加密模式的选择可以基于内容中或者包括该内容的数据流中存在的数据。例如，一个或者多个比特可以是明文内容的一部分或者可被增加到明文内容，从而标识在本地链路加密期间执行的加密模式。此外，在实施例中，在本地链路加密期间执行的加密算法通常符合ATIS-08000006标准。但是，本领域技术人员可以意

识到任何类型的加密算法都可以用于本地链路加密，只要相同的加密算法在智能卡和装置二者上都是可获得的。

[0037] 在实施例中，用于选择将要用于本地链路加密的密钥的密钥设置可以跨安全边界发生。例如，密钥交换可以作为密钥设置的一部分，在智能卡和机顶盒之间发生。交换的密钥可以由安全装置(例如智能卡)产生，并且被传输给正与安全装置通信的特定装置，例如机顶盒。因为本地链路加密是特定针对单个装置的，而不是特定针对网络传输的，所以对本地链路加密密钥的拦截不会向未授权用户提供全面接入广播的网络内容的能力。在实施例中，多个密钥可被用于本地链路加密。例如，智能卡可以能够同时处理多个输入流并且输出多个本地加密流。在这种实施例中，每一个本地加密流可以是使用独有的本地链路加密密钥进行加密的。但是，在其他实施例中，可以使用相同的本地链路加密密钥来加密每一个本地加密流。

[0038] 流程继续前进到步骤208，在步骤208中获取本地控制字。本地控制字可以是任意类型的加密密钥。在实施例中，本地控制字可以是特定装置独有的加密密钥。在实施例中，本地控制字可以从普通软件寄存器、硬件密钥阶梯(key ladder)、随机密钥产生器，或者从任意其他源中获得。在一个实施例中，本地控制字可以是动态地产生的，并且与接收装置共享。在这种实施例中，可以基于该装置的特性来产生密钥。在实施例中，在获取步骤208期间可以选择多个密钥。例如，可以从密钥阶梯中选择两个密钥。密钥阶梯可以存储或者以其他方式标识多个相关的密钥。在实施例中，本文公开的实施例可以使用任意类型的加密密钥，例如，固定加密密钥、动态加密密钥、随机产生的加密密钥等等。

[0039] 在获得本地控制字后，流程继续前进到步骤210，在步骤210中，使用本地控制字来重新加密网络解密内容，以产生本地加密内容。如先前讨论的，在步骤210中可以使用不同类型的加密模式和加密算法来加密内容。在实施例中，加密可以基于在步骤208中获得的密钥。在获得多个密钥的实施例中，在步骤210中，密钥之一可被选择，并且在加密期间使用。例如，可以基于内容中的标识符选择合适的密钥。该标识符可以是内容的一部分，或者可在方法200期间它被处理时被增加到内容或与内容关联的头部。该标识符可以是标识偶数或者奇数密钥(在获得两个密钥的实施例中)的单一比特。这一标识符提供了对在步骤210的加密处理期间使用的密钥的自动选择。

[0040] 在另一个实施例中，除了加密内容之外，内容的大小也增加了。为了使得在网络上共享内容变得更困难，增加内容的大小可能是有利的。例如，增加内容大小将会需要更高的带宽来通过网络与未授权的用户正确地共享内容。例如，可以向广播流添加数据，以使得其更难以处理或者与未授权用户共享。在内容被流传输(例如音频和/或视频内容)的实施例中，非内容数据包可被增加到内容流并且带宽率将被增加。这种带宽的增加以及非内容数据的附加通过使得内容更难被共享和处理，在内容离开执行方法200的安全装置和/或安全处理器时为内容提供了附加安全性。在2009年4月27日申请的题目为“Methods and Apparatus for Securing Communications Between a Decryption Device and a Television Receiver(用于在解密装置和电视接收机之间的安全通信的方法和设备)”的U.S专利No.8,385,542中提供了关于流扩展的更多细节，在此通过参考将该专利全文并入本文。

[0041] 尽管方法200的实施例将解密网络加密内容以及随后本地加密该解密的网络加密

内容作为两个分离步骤进行描述，但是本领域技术人员应该意识到，在实施例中，该解密和加密可以顺序执行，作为单个步骤执行，或者并行执行。在实施例中，本领域技术人员将意识到流扩展也可以在单个解密/加密步骤中执行。如此，本领域技术人员将意识到参考附图2描述的方法可以使用与在此示出的步骤更少或者更多的步骤来执行。

[0042] 在又一个实施例中，方法200可以操作用于流数据。在该实施例中，在步骤202中可以接收网络加密流，在步骤204中通过解密网络加密流来产生明文内容流，以及在步骤212中产生本地加密流。本领域技术人员将意识到在此参考附图2(以及参考附图3-4)公开的实施例也可以操作用于流数据以及以任意其他形式传输的数据。

[0043] 对于附图2示出的实施例，在执行本地加密后，流程还可以继续前进到步骤212，在步骤212中本地加密内容被提供给另一装置。例如，在机顶盒环境中，在步骤212中，智能卡可以将本地加密内容提供给机顶盒的其他部件以供存储和/或显示。在通用计算装置中，在步骤212中，将本地加密内容从安全处理器提供给通用处理器和/或未保护存储器以供存储和/或显示。本领域技术人员将会明白该方法200通过下述方式提供了对在此描述的问题的解决方案：将本地加密内容提供给不安全部件，而不是像不支持本文描述的传输I/O系统的实施例的装置和方法通常执行的那样提供控制字或者加密密钥。此外，本领域技术人员将会明白：当数据从安全装置和/或处理器传输给通用装置时，在这种内容保护系统中，很小的安全泄露有可能发生。但是，本文公开的实施例通过下述方式解决了这一缺点：提供本地加密内容(优选地，其数据和带宽被扩展的内容)，从而使得未授权用户更难处理、共享和接入内容，即使当该内容在安全装置和/或安全处理器系统/架构内部传输时被拦截也是如此。

[0044] 在一个实施例中，本地加密内容可以作为各个单独的本地加密基本流来提供。例如，在接收和解密多个网络加密基本流的实施例中，多个基本流可被分别单独加密并且分别作为单独的本地加密基本流来返回。在可选实施例中，多个网络加密基本流可被复用到单个输出流中。在这种实施例中，在步骤212中，可以本地加密和随后提供单个输出流。在实施例中，可以在执行步骤210的本地加密之前或者在本地加密步骤210之后，将多个基本流复用到单个输出流。

[0045] 附图3是用于处理本地加密内容的方法300的实施例。在实例中，方法300由诸如机顶盒、膝上电脑、平板电脑、智能电话、电视或者其他类型的通用计算装置之类的装置来执行。流程开始于步骤302，在步骤302中接收本地加密内容。在实施例中，本地加密内容可以是从执行参考附图2描述的方法200的安全装置和/或安全处理器中接收的。例如，在非限制性实施例中，本地加密内容可以从与机顶盒通信的智能卡中接收。在另一个实施例中，本地加密内容可以从与通用处理器和/或通用存储器通信的安全处理器中接收。

[0046] 一旦接收到本地加密内容，流程前进到步骤304，在步骤304中接收本地控制字。本地控制字可以是任何类型的加密密钥。在实施例中，本地控制字可以是执行方法300的装置独有的加密密钥。在实施例中，本地控制字可以从使用普通软件寄存器、硬件密钥阶梯、随机密钥产生器的智能卡或者从该装置独有的任何其他源获得。在一个实施例中，本地控制字可以从执行方法200的安全装置和/或处理器中获得。在另一个实施例中，本地控制字可以由执行方法300的装置产生。在这种实施例中，本地控制字可以事先已被与创建步骤302中接收的本地加密内容的安全处理装置和/或安全处理器共享。本地控制字可以是随机产

生的。在实施例中，可以使用单一本地控制字。在其他实施例中，可以使用多个本地控制字。在这种实施例中，本地控制字可以周期性地改变，使得在设定的时间段后，该本地控制字被作废，而启用新的本地控制字。

[0047] 该流程前进到步骤306，在步骤306中使用本地控制字解密本地加密内容。解密本地加密内容将会产生应用可接入的明文内容。本领域技术人员可以意识到：很多类型的加密模式和/或算法可被用于解密本地加密内容。如此，在步骤306中可以使用某种类型的解密算法来利用本地控制字解密内容。此外，执行解密的装置可以能够操作和处理本地加密内容，尽管本地加密内容的带宽由于非内容数据而增加。在这种实施例中，步骤306中对本地加密内容的解密可以包括：识别和从内容中移除非内容数据。在另一个实施例中，直到明文内容被处理以供显示或者存储，才会发生对非内容数据的移除。

[0048] 流程前进到步骤308，在步骤308中提供明文内容。在一个实施例中，提供明文内容包括：解码、显示和/或以其他方式呈现明文内容。例如，明文内容可被显示在电视机、监视器和/或显示器上，该电视机、监视器和/或显示器可以是执行方法300的装置的一部分或与执行方法300的装置通信。在另一个实施例中，提供明文内容可以包括：将明文内容存储到数据存储器中，所述数据存储器可以是执行方法300的装置的一部分或者与执行方法300的装置相连。

[0049] 在可选实施例中，持久加密可以不是通过如附图3所描述的立即解密本地加密内容来执行的。在这种实施例中，持久加密可被应用于内容，例如从广播的网络传输接收的MPEG传输包。在这种实施例中，安全装置仍可以如附图2中所示那样执行网络解密和本地链路加密；但是，接收本地加密内容的装置可以不立即执行本地链路解密。替代地，接收本地加密内容的装置可以存储本地加密内容(按它加密后的样子)，供以后使用。这允许对内容进行加密以便于安全的本地存储，但是安全装置仍然可以例如通过在稍后的时间提供解密密钥来控制何时解密内容。

[0050] 附图4是用于使用传输I/O系统接收和处理受保护内容的方法400的实施例。在实施例中，方法400可以由机顶盒、智能电话、膝上电脑、平板电脑、电视或者任意类型的通用计算装置，例如参考附图1讨论的接收装置，来执行。在实施例中，执行方法400的装置可以包括安全处理装置和/或安全处理器，或者与安全处理装置和/或安全处理器通信。安全处理装置和/或安全处理器可以是该装置的可拆卸部件。例如，安全处理器可以合并到该可拆卸智能卡中，该智能卡可被插入执行方法400的装置以及从该装置中移除。

[0051] 流程开始于步骤402，在步骤402中接收网络加密内容。网络加密内容可以从头端装置接收。在实施例中，网络加密内容可以通过无线或者有线网络接收。例如，网络加密内容可以从卫星电视提供商、有线电视提供商接收，从地面传输接收，从蜂窝网络提供商接收，或者从互联网上的服务器接收。在实施例中，网络加密内容是可被传输给多个不同装置的内容。如此，网络加密内容可以使用对于所有接收内容的装置公共的网络控制字来加密。一旦接收到网络加密内容，流程前进到步骤404，在步骤404中使用安全处理装置和/或安全处理器来解密网络加密内容。在这种实施例中，在步骤404中，网络加密内容可被提供给安全处理装置和/或安全处理器。在一个实施例中，当通过网络接收到网络加密内容时，网络加密内容可被提供给安全处理器以进行解密。在另一个实施例中，在被安全处理器解密之前，网络加密内容可被缓存。

[0052] 如先前所述，安全处理装置和/或安全处理器可以是执行方法400的装置的一部分或者是执行方法400的装置的可拆卸部件(例如智能卡)。在安全处理器和/或安全处理装置是可拆卸部分的实施例中，安全处理器和/或安全处理装置可以具有规格(form factors)，使得其符合传统系统。例如，智能卡可以具有规格，以便不仅可以操作支持本文公开的用于执行传输I/O的系统和方法的模式下外，还可以操作在ISO-7816模式(或者任意其他类型模式)下。

[0053] 在一个实施例中，网络加密内容可以以未过滤的方式提供给安全处理器。例如，一个或者多个未过滤的MPEG传输流可被提供。在该实施例中，MPEG传输流可以如其接收到的那样被提供，无需预先移除通过包标识符(PID)标识的包。在另一实施例中，在使用安全处理器解密网络加密内容之前，该装置可以先对网络加密内容进行过滤。例如，通过移除通过PID识别的包，可以将一个或者多个过滤后的MPEG传输流提供给安全处理器以供解密。在又一个实施例中，多个流可被复用并且提供给安全处理器以进行解密。例如，两个或者多个MPEG传输流可被复用以创建组合的流。该组合的流被提供给安全处理器以进行解密。

[0054] 在实施例中，解密步骤404也可以执行参考附图2讨论的方法200。在这种实施例中，步骤404的结果还可以产生本地加密内容。流程前进到步骤406，在步骤406中本地加密内容被解密。在实施例中，在步骤406中可以使用参考附图3描述的方法300来解密本地加密内容。在实施例中，对本地加密内容的解密是由在执行方法400的装置上的并非安全处理器的一部分的部件来执行的。例如，由通用处理器来执行解密。在实施例中，解密本地加密内容可以产生未加密的内容的流。

[0055] 流程前进到步骤408，在步骤408中处理明文内容。在一个实施例中，通过将内容提供给作为执行方法400的装置的一部分或者连接到执行方法400的装置的显示器和/或音频装置来处理该明文内容。在另一个实施例中，在步骤408中，明文内容可被存储在存储器中或者非易失性存储设备中。本领域技术人员将意识到，在步骤408中，可以执行对明文内容的任何类型的处理。

[0056] 如参考方法400的实施例描述的，执行该方法的装置可以包括用于执行方法400的不同步骤的不同部件。例如，对网络加密内容的解密可以由作为装置的一部分的安全部件来执行。在实施例中，安全部件可以是可拆卸的，例如智能卡。本地解密和处理步骤可以由不同于安全部件的其他部件来执行。但是，由于对网络加密内容的解密是由安全部件来执行的，网络控制字不易被拦截和共享。因此，方法400是对解密网络加密内容的更安全的处理，不会泄露解密网络加密内容所需的一个或者多个密钥。

[0057] 在安全处理器是可拆卸的(例如，但是不限制于，智能卡)实施例中，当执行方法400的装置在与可拆卸安全处理器通信时，可以使用不同的数据率。在一个实施例中，可以将固定数据率用于在该装置和可拆卸安全处理器之间的所有通信。在另一个实施例中，数据率可以依赖于在该装置和该可拆卸安全处理器之间交换的内容类型和/或消息类型而变化。在另一个实施例中，不同类型的信令可被用于在该装置和可拆卸安全处理器之间通信。例如，在可拆卸安全处理器是智能卡的实施例中，可以使用低压差分信令(LVDS)。

[0058] 在另一个实施例中，可以同时针对不同的网络内容执行方法400，从而处理多个网络加密流或者网络加密内容的多个片段。例如，在机顶盒环境中，该装置可以能够一次处理多个数据流。例如，机顶盒可以允许用户观看一个信道，同时记录一个或者多个其他信道。

在该实施例中，机顶盒可以同时对多个流使用方法400，以解密网络加密内容。在该实施例中，可拆卸安全处理器，例如，智能卡，能够同时解密多个网络加密内容流并且创建多个不同的本地加密流。在这种实施例中，可以使用不同的网络控制字来解密不同的网络加密内容，并且可以使用不同的本地控制字来创建不同的本地加密内容

[0059] 附图5是可被用于在保持传输流功能的同时重置安全装置(如智能卡)的功能的方法500的实施例。该流程开始于步骤502，在步骤502中安全装置接收重置指令。在实施例中，该指令可以指示将独立于传输功能来重置内核功能。例如，内核功能可以涉及用于操作安全设备的操作指令，例如，内核软件。例如，内核软件可被重置，以例如执行软件升级，故障恢复，或者由于不同步等等引起的重置。但是，由于安全装置处理网络加密流，与由不是安全装置的部分的部件处理网络加密流的现有方案不同，所以安全装置必须被重置且不中断流传输的数据。在此描述的实施例中，如果安全装置被完全重置，在重置期间流传输的数据的传输可能被中断。在实施例中，在步骤502中接收的信号可以指示部分重置(例如，仅重置内核功能和/或软件)，或者安全装置可以做出执行部分重置的决定。

[0060] 流程前进到步骤504，在步骤504中安全装置在保持传输功能的同时重置内核功能。在实施例中，安全装置的执行内核功能的部件可被重置，同时执行传输功能的部件继续运行。如此，可以对安全装置的内核功能执行维护，而不中断对安全装置接收的数据流的处理。例如，在重置安全装置的内核功能的同时，安全装置仍然能够接收传输流，处理传输数据(例如通过执行附图2的方法200)，以及将处理后的包(例如本地加密内容)提供给其他装置。通过执行部分重置，在装置重置期间，网络加密内容仍可被解密和本地加密，因此给安全装置提供了在执行维护的期间继续提供内容的能力。流程随后前进到步骤506，在步骤506中安全装置的内核功能被重启并且完成维护。

[0061] 在实施例中，由于安全装置正在处理网络数据，例如网络加密内容，变化带宽的数据被提供给安全装置。这不同于现有系统，在该现有系统中安全装置(例如智能卡)接收固定带宽量的数据。为了处理变化带宽的数据，本文描述的安全装置的实施例可以执行包调节(packet pacing)算法。附图6是包调节方法600的实施例，其可被在可变带宽环境中运行的安全装置使用。在实施例中，方法600是一个闭环反馈机制，其中安全装置可以提供允许发送(CTS)消息或信号以通知：允许与安全装置通信的装置(例如机顶盒或者片上系统)向安全设备发送附件数据包。在实施例中，方法600被用于确保安全装置能够从多个固定输入流中提取变化数量的数据，同时通过使用一个或者多个CTS消息调节(throttle)有效数据的量。在实施例中，通过安全装置向与其通信的装置发送CTS消息或信号会触发该装置发送感兴趣的包(例如，包含诸如传输数据、控制数据等的有用数据的包)。在实施例中，当安全装置没有发送CTS消息时，安全装置可以从与其通信的装置接收填充包。

[0062] 在实施例中，安全装置可以使用先进先出(FIFO)缓冲器来执行包调整。安全装置可以监视FIFO缓冲器，从而控制对安全装置接收的可变带宽数据的包调节。例如，安全装置可以监视FIFO缓冲器的容量和/或充满度。如果在FIFO中排队的包的数量减少到低于阈值，安全装置可以向与安全装置通信的装置发送CTS消息，以触发对附加数据的接收。在实施例中，在FIFO缓冲器中可以保持较低等级的数据，从而确保排队的具有高优先级的实时包具有最小等待时间。在高活动性期间，安全装置通过维持小的FIFO缓冲器可以确保实时包获得更好的优先级。

[0063] 流程开始于步骤602，在步骤602中监视FIFO缓冲器。监视FIFO缓冲器可以包括检查FIFO缓冲器中的项目数量。在实施例中，在步骤602中可以执行用于监视缓冲器或者缓冲器的内容的任意方法。流程前进行判决步骤604，在步骤604中做出FIFO缓冲器中的内容的数量是否低于预定阈值的判定。在一个实施例中，该阈值可以是基于缓冲器中的包的处理时间。在另一个实施例中，该阈值可以是基于计算。如果在FIFO缓冲器中的项目的数量低于阈值，附图6示出了流程分支“是”前进到步骤606，在步骤606中发送CTS消息或信号以触发对附加数据包的接收并且流程返回到步骤602。例如，CTS消息可被发送给视频处理装置、机顶盒、或者命令该装置向安全处理器发送附加数据的其他类型的装置。如果项目的数量不低于阈值，附图6示出了分支“否”并且返回步骤602。尽管实施例被描述为具有FIFO缓冲器，但是可以使用其他类型的队列而不超出本发明的范围。

[0064] 在安全处理器是可拆卸部件的实施例中，安全处理器被设计为使得其能够在传统系统中工作。在实施例中，安全处理器是具有传统的规格的可拆卸部件。例如，智能卡可被设计为支持ISO-7816信号和用于本文描述的传输I/O系统的信号。附图7是示出了在ISO-7816智能卡和能够支持本文公开的系统和方法的智能卡之间的兼容性的实施例。智能卡702是兼容ISO-7816的智能卡的实施例。智能卡704是兼容ISO-7816以及本文公开的传输I/O系统和方法的智能卡。在示出的实施例中，智能卡704包括与ISO-7816标准(例如支持传统的规格)兼容所必需的所有接点。此外，智能卡704包括六个接点(contacts)，由椭圆706标识，其能够被用于执行本文描述的系统和方法。在这种实施例中，智能卡704能够与现有系统(例如本领域中部署的传统装置)和具有传输I/O能力的系统一起工作。

[0065] 在实施例中，执行方法400的装置和/或可拆卸安全装置在启动时可以做出是以传统模式(例如ISO-7816模式)还是传输I/O系统可兼容模式运行的决定。在一个实施例中，该决定可以基于在初始化时发送到可拆卸安全装置的信号做出。在2011年7月18口申请的题目为“Multiple-Speed Interface(多速度接口)”的U.S专利申请No.13/184,831中提供了关于做出这一决定的更为详细的细节，该专利申请要求了于2011年7月16日申请的U.S临时专利申请No.61/364,854的优先权，在此通过参考将其全文并入本文。

[0066] 附图8是可以本文描述的系统可以使用的或者可以用于执行本文描述的方法的安全处理装置800的实施例。在实施例中，该安全处理装置可以是智能卡。但是，本领域技术人员可以意识到本文描述的系统和方法可以使用任何其他类型的安全装置。在实施例中，安全处理装置可以是执行本文通过参考附图4描述的方法400的装置的一部分。在另一个实施例中，安全处理装置800可以是执行方法400的装置的可拆卸部件。

[0067] 在实施例中，安全处理装置800包括一个或者多个处理单元802。在一些实施例中，本文描述的方法的一个或者多个部分是由一个或者多个处理单元802来执行的。例如，一个或者多个处理单元802可被用于如在附图2的方法200中描述的解密网络加密内容，创建本地加密内容，以及创建非内容数据。

[0068] 安全处理装置800还可以包括存储器804。存储器804包括，但不限制于，RAM、ROM、EEPROM、闪存或者其他存储技术，或者用于存储信息且可被安全处理装置800和一个或者多个处理单元802存取的任意其他有形媒体。存储器804还存储用于执行本文描述的方法的可执行指令。例如，存储器804可以包括用于解密网络加密内容(NEC)806的指令。存储器还可以存储用于加密明文内容以创建本地加密内容(LEC)808的指令。

[0069] 安全处理装置800还可以包括允许该装置与其他装置通信的一个或多个通信连接810。通信连接810是通信媒体的一个例子。通信媒体可以具体表现为调制的数据信号，例如载波或者其他传输机制，并且包括任意的信息传递媒体，其可以包括计算机可读指令、数据结构、程序模块、或者具有调制数据信号形式的其他数据。术语“调制的数据信号”意思是具有其特征集中的一个或多个特征的信号或者以将信息或消息编码在数据信号中的方式改变的信号。作为举例而非限制，通信媒体包括有线媒体(例如有线网络或者直接有线连接)，以及无线媒体(例如声音、RF、红外以及其他无线媒体)。在实施例中，网络加密内容例如可以通过通信连接810接收。本地加密内容可以通过通信连接810传输。在又一个实施例中，执行在此描述的传输I/O方法的指令可以经由通信连接810来接收。例如，头端可以用执行本文公开的方法的指令来更新安全处理装置800。该指令可被存储在存储器804中。通信连接810因此允许头端使用执行本文公开的方法的指令来更新在本领域中部署的智能卡。通信连接还为安全处理装置800提供从一装置接收网络加密内容以及将本地加密内容返回给该装置的能力。在实施例中，通信连接可被作为接点添加在智能卡上，例如，但不限制于，在附图7中的标记为具有传输I/O能力的接点706的接点。

[0070] 尽管安全处理装置800的实施例被示出为具有包括执行本文公开的方法的指令的存储器804，但是在可选实施例中，用于执行本文公开的方法的指令可由作为安全处理装置800的一部分的专用集成电路(ASIC)来执行。

[0071] 附图9是一个机顶盒的实施例，其可被用于执行传输I/O系统和方法并且是本文公开的系统的一部分。在另一个实施例中，可以使用包含图9中示出的一些部件的不同的接收装置，例如，但是不限制于智能电话、平板电脑、膝上电脑或者任意其他类型的装置。虽然附图9示出了各种部件，但是很多部件都是本领域公知的并且无须解释。仅描述可被用于执行本文公开的方法的部件。到达机顶盒900的信号904经历广泛的处理。电视转换器900可以包括一个或者多个调谐装置906、946、948，其可以接收信号904。信号904可以是卫星信号、有线电视信号或者通过有线或者无线网络接收的其他类型的信号。在这一实施例中，调谐装置906、946、948从头端或者内容提供商获得信号904。调谐装置906、946、948可以初始处理信号904。信号904可以是包括网络加密内容(例如，一个或者多个网络加密流)、多个明文内容(例如一个或者多个明文内容流)和/或包含与该数据流或者构成该数据率的多个加密的和/或明文的流有关的信息的元数据的数据流。调谐装置906、946、948还可以从控制电子单元902接收具有信号形式的订户命令。来自控制电子单元902的信号可以包括，但是不限制于，用于调谐到应答器(其作为选择某个频道以便于在外部装置上观看这一处理的一部分)的信号。本领域技术人员将明白：调谐装置906、946、948可以包括更少，更多的部件或者不同的部件。信号904可以包括通过网络控制字编码的内容。信号904还可以包括一个或者多个ECM和EMM。

[0072] 在接收到信号904之后，第一步骤之一可以是解调908信号904。信号904可以作为“携带”数据的模拟信号(例如数据被调制到模拟信号上)到达。可以通过调制处理的逆处理来完成解调908。可以通过多种途径完成调制。调制可以包括调幅(AM)或者调频(FM)。如果携带的数据是数字的，调制方法包括，但不限制于：二进制移相键控(BPSK)、四相移键控(QPSK)、或者八相移键控(8PSK)。本领域技术人员可以意识到其他的用于调制和解调信号904的方法是可能的。第一步骤中的另一个可以是对信号904进行纠错908。纠错908的一个

例子是前向纠错(FEC)。FEC 908可以包括，但是不限制于，检查可伴随信号904的一个或多个校验位。本领域技术人员将会明白：很多用于纠错的方法都是可行的。出于讨论目的，下面将讨论使用数字数据的实施例。但是，本领域技术人员可以意识到：采用模拟数据或者组合模拟和数字的数据的系统都是可能的，并且在此是可以预期的。

[0073] 在实施例中，机顶盒900包括接收信号904的控制电子单元902。在实施例中，控制电子单元902可以包括智能卡接口。本领域技术人员可以意识到该控制电子902可以接收其他信号，包括，但不限制于来自有线电视、卫星或者广播电视分配器的信号。在这一实施例中，控制电子单元902包括利用共享总线910组合到单个电路中的分离的电子部件。在其他实施例中，控制电子单元902可被不同地配置。例如，在机顶盒900中的控制电子单元902部件中的一个或者多个被合并或者省略。如又一个示例中，机顶盒900中的控制电子单元902部件中的一个或者多个可以不共享总线910，而是通过某种其他方式可操作连接的。本领域技术人员将会明白机顶盒900以及控制电子单元902的其他配置是可能的并且在本发明的范围内容。本领域技术人员还可以意识到机顶盒900和控制电子单元902的一些部件可以以硬件或者软件来实现。该控制电子单元902可以在软件程序、固件程序，或者存储在存储器中的某个其他程序或者控制逻辑的控制下运行。本领域技术人员可以意识到控制电子单元902可以包括用于转送或者处理信号的其他电子部件或者结构。

[0074] 控制电子单元902可以包括一个或者多个中央处理单元(CPU)912或者处理器。在这一实施例中，控制电子单元902包括单个CPU 912，CPU 912可操作地连接到共享总线。在这一实施例中，CPU 912可被用于针对机顶盒900功能的逻辑操作等等，包括，但不限制于，信道选择、记录控制、EPG显示和控制、以及系统维护。本领域技术人员将会明白CPU 912可以与存储器或者其他分离的电子部件集成在一起。在实施例中，CPU 912可被用于执行本文公开的系统和方法。例如，CPU 912可被用于执行如参考附图3描述的解密本地加密内容的方法。但是，在实施例中，本地解密可以由其它部件执行，例如专用密码引擎(未示出)。本领域技术人员将会明白，尽管参考附图9描述了特定的部件，本文公开的该系统和方法可以由其它部件或者其他类型的装置执行，而不偏离本公开的精神。

[0075] 控制电子单元902可以包括一个或者多个易失性存储器部件914。易失性存储器部件914可以包括，但是不限制于，一个或者多个SDRAM存储器芯片。类似的，控制电子单元902还可以包括一个或者多个非易失性存储器部件916。非易失性存储器916可以包括一个或者多个存储器芯片，包括，但是不限制于，ROM、EEPROM以及闪存。本领域技术人员应该意识到该易失性存储器914以及非易失性存储器916可被集成到其他电子部件中。本领域技术人员还会意识到其他存储器部件可被包括在机顶盒900以及控制电子单元902中。本领域技术人员会意识到存储器914、916可被用于很多目的，包括，但不限制于，存储EPG数据以及存储被CPU 912使用的数据。在实施例中，易失存储器部件914和/或一个或者多个非易失性存储器部件916可被用于存储用于执行本文公开的方法300和400的指令。非易失性存储器916可被用于存储本地加密内容或者明文内容。在其他实施例中，硬盘驱动器950可被用于存储本地加密内容或者明文内容。

[0076] 通过外围接口924将机顶盒900连接到一个或者多个外部电子装置。这些外部装置可以包括智能卡936。在实施例中，智能卡936充当条件接入系统。在这种实施例中，智能卡936执行本文公开的方法200和400。在实施例中，智能卡936可以是能够支持传统操作模式

和传输I/O操作模式二者的诸如智能卡504之类的智能卡。在又一个实施例中，智能卡936可以具有参考附图8描述的部件。外围接口924还可以充当向显示装置(例如，但是不限制于，电视和扬声器)提供明文内容的I/O连接，。

[0077] 参考附图10，用于实现在此描述的各个实施例的计算环境的实施例包括计算机系统，例如计算机系统1000。所描述的实施例的任意部件和全部部件(例如，DVR、内容存储服务器、膝上电脑、移动装置、个人电脑、智能电话、安全处理装置等)可以作为客户端计算机系统、服务器计算机系统、客户端和服务器计算机系统的组合、手持装置以及本文描述的其他可能的计算环境或系统来执行，或者在客户端计算机系统、服务器计算机系统、客户端和服务器计算机系统的组合、手持装置以及本文描述的其他可能的计算环境或系统上执行。如此，下面将描述可用于所有这些环境的基本计算机系统。

[0078] 在其最基本的配置中，计算机系统1000包括至少一个处理单元或者处理器1004以及系统存储器1006。附图10通过虚线1002示出了计算机系统1000的最基本配置。在一些实施例中，所描述的系统的一个或者多个部件被装载到系统存储器1006中并且由处理单元1004从系统存储器1006中执行。取决于计算机系统1000的确切配置和类型，系统存储器1006可以是易失性的(例如RAM)、非易失性的(例如ROM，闪存等等)，或者它们两者的组合。

[0079] 此外，计算机系统1000还可以具有附加特征/功能。例如，计算机系统1000可以包括附加存储器媒体1008，例如可拆卸的和/或不可拆卸的存储设备，包括，但不限制于，磁盘或者光盘或者磁带或者固态存储器。在一些实施例中，软件或可执行代码以及用于所描述的系统的任意数据可以永久存储在存储器媒体1008中。存储器媒体1008包括以用于信息存储(例如用于计算机可读指令、数据结构、程序模块或者其他的数据的存储)的任意方法或者技术实现的易失性的和非易失性的、可拆卸和非可拆卸的媒体。

[0080] 系统存储器1006和存储器媒体1008是计算机存储媒体的例子。计算机存储媒体包括，但不限制于RAM、ROM、EEPROM、闪存或者其他存储器技术，CD-ROM、数字视频盘(DVD)或者其他光存储器、磁带盒、磁带、磁盘存储器、其他磁存储装置、固态存储器或者任意其他实体媒体，其被用于存储期望的信息以及被计算机系统1000和处理器1004存取。任何这种计算机存储媒体可以是计算机系统1000的一部分。在一些实施例中，系统存储器1006和/或存储器媒体1008可以存储用于执行本文公开的方法或形成本文公开的系统的数据。在其他实施例中，系统存储器1006可以存储信息，例如本地控制字1014以及逻辑电路1016，以执行本文描述的解密本地加密内容的方法。

[0081] 计算机系统1000还可以包括通信连接1010，其允许该装置与其他装置通信。通信连接1010是通信媒体的例子。通信媒体可以具体实现为调制的数据信号，例如载波或者其他的传输机构，并且包括任意的信息递送媒体，其可以具备实现为计算机可读指令、数据结构、程序模块或者在调制的数据信号中的其他数据。术语“调制的数据信号”意思是具有其特征集中的一个或者多个特征的信号或者以将信息或消息编码在数据信号中的方式改变的信号。作为举例而非限制，通信媒体包括有线媒体(例如有线网络或者直接有线连接)，以及无线媒体(例如声音、RF、红外以及其他无线媒体)。在实施例中，内容和元数据可以通过通信连接1010传输。

[0082] 在一些实施例中，计算机系统1000还包括输入和输出连接1012，以及与外部装置的接口，例如图形用户界面。输入装置还被称为用户接口选择装置，并且包括，但不限制于：

键盘、鼠标、手写笔、语音输入装置、触摸输入装置等。输出装置还被称为显示器，并且包括，但不限制于：阴极射线管显示器、等离子屏幕显示器、液晶屏幕显示器、扬声器、打印机等等。在本文的描述的，连接到输入和输出连接1012的这些设备，无论是单独地还是作为组合，被用于显示信息。所有这些装置都是本领域中公知的并且无需在此进行长篇讨论。在又一个实施例中，输入和输出连接1012可被用于与可拆卸安全处理器(例如，但不限制于，智能卡)通信。

[0083] 在又一个实施例中，计算机系统1000可以包括安全处理器1018和安全存储器1020，其可被用于执行本文公开的方法中的一些方法。在实施例中，计算机系统1000的安全处理器1018和安全存储器1020可以包括安全区域1022，计算机系统1000的其它部件或者在计算机系统1000上执行的其他处理通常不能够访问该安全区域1022。在实施例中，安全存储器可以存储用于如参考附图2描述的解密网络加密内容和创建本地加密内容的指令。这种指令可被安全处理器1018执行。在这种实施例中，网络控制字可以保留在安全区域1022中，从而降低了被未授权方拦截和共享的机会。

[0084] 在一些实施例中，在此描述的部件包括如可存储在计算机存储媒体和其他有形媒体上的以及可通过通信媒体传输的且可由计算机系统1000执行的这种模块或者指令。计算机存储媒体包括以用于信息存储(例如用于计算机可读指令、数据结构、程序模块或者其他的数据的存储)的任意方法或者技术实现的易失性的和非易失性的、可拆卸和非可拆卸的媒体。上述媒体中的任意媒体的组合应当被包括在可读媒体的范围内。在一些实施例中，计算机系统1000是在远程存储器中存储供计算机系统1000使用的数据的网络的一部分。

[0085] 有时，条件接入系统需要使用庞大且昂贵的规格。例如，传统的DVB-CI条件接入模块(CAM)使用PCMCIA(PCCARD)规格和连接器，以及标准ISO-7816。能够接收和呈现内容(例如视频和/或音频内容)的装置的数量持续增加。例如，很多智能电话、膝上电脑、平板电脑、平板手机、电视机或者其他装置能够用于接收内容和向用户呈现内容。通常，由于传统的条件接入系统接口的规格和成本，这种装置不包括传统的条件接入系统接口。如此，内容提供商和分配器不能够依赖的传统条件接入系统(例如对智能卡、PC卡等等的使用)来保护在这些装置上的内容。

[0086] 此外，由于成本和规格的问题，很多装置生产商不愿意并入传统的条件接入系统接口。但是，很多这类装置包括其他标准的接口和/或连接。本文公开的实施例利用标准连接来使用能够与很多不同类型的装置交互的条件接入智能芯片。一个这种标准接口是USB 3.0接口。但是，虽然本文公开的实施例描述了对具有USB 3.0连接器的智能芯片的使用，本领域技术人员可以意识到，在不超出本发明的范围的情况下，本文公开的实施例可以使用其他接口和/或连接器。

[0087] 附图11示出了示例性的连接器1100，其可与智能芯片1102(例如具有传输I/O能力的芯片)一起使用来执行条件接入。在实施例中，智能芯片1102可以执行本文公开的方法。出于说明目的，示例性连接器1100被作为USB 3.0连接进行描述。但是，虽然使用USB 3.0连接来描述示例性的连接器1100，本领域技术人员可以意识到，本文公开的实施例可以使用其他标准的连接(例如USB 2.0连接、mini USB连接、SCSI连接、IEEE 1394连接等等)来执行传输I/O条件接入。在该实施例中，其他标准连接器可被修改以在传输I/O条件接入期间传输数据和/或消息。

[0088] 示例性的连接器1100包括9个信号管脚。在实施例中，信号管脚1104a-d可以根据USB 2.0协议进行操作和/或使用。例如，信号管脚1104a可被用作接地管脚，信号管脚1104b可被用作Data+管脚，信号管脚1104c可被用作Data-管脚，而信号管脚1104d可被作用VCC管脚，如USB 2.0标准所定义的那样。信号管脚1106a-e可以是可根据USB 3.0协议操作和/或使用的信号管脚。但是，在实施例中，能够执行本文公开的传输I/O方法的智能芯片1102可以将管脚1106a-e映射到智能卡接触706，该智能卡接触706是参考附图7描述的智能卡704的一部分。例如，USB 3.0规范定义了分别作为Receive-和Receive+管脚的管脚1106a和1106b。然而，能够执行本文公开的实施例的智能芯片1102可以将管脚1106a和1106b分别用作参考附图7的智能卡704所描述的SC_out-以及SC_out+接点。类似的，USB 3.0协议定义了分别作为Transmit-和Transmit+管脚的管脚1106d和1106e。然而，同样，在实施例中，能够执行本文公开的实施例的智能芯片1102可以将管脚1106d和1106e分别用为作为附图7的智能卡704的一部分的SC_IN-和SC_IN+接点。如此，智能芯片1102可以利用USB3.0规格成为传输I/O系统的一部分，和/或执行本文公开的传输I/O方法。

[0089] 然而，示例性连接器1110不具有足够的管脚来直接映射到附图7所示的全部的传输I/O接点706。在将管脚1106a和1106b映射到针对(图7)智能卡704讨论的SC_out-和SC_out+接点(pad)以及将管脚1106d和1106e映射到针对(图7)智能卡704讨论的SC_IN-以及SC_IN+接点之后，只有管脚1106c(被USB3.0标准定义为接地)仍未映射。但是，智能卡704(附图7)包括两个附加接点，CLK+和CLK-接点。CLK+和CLK-接点被用于在智能卡404与机顶盒、片上系统(SoC)或能够接收和修改内容的者任意其他类型的装置之间的数据同步。在实施例中，由于内容(例如视频内容、电视内容、音频内容等)在智能卡704(附图7)与其他装置之间持续地流传输，可以使用时钟信号来同步在智能卡704(附图7)与其他装置之间的通信。但是，示例性的连接器1100不具有足够的可用管脚以与智能卡704(附图7)类似的方式传输时钟信号。为了通过连接器1100同步智能芯片1102与SoC、装置、膝上电脑等等，可以使用时钟恢复机制。在实施例中，使用连接器1100来执行本文公开的传输I/O实施例的智能芯片1102可以传输和接收自身时钟数据。在实施例中，时钟恢复机制可以使用锁相环、8B/10B编码、八-至-十四调制或者其他类型的公知的时钟恢复技术。

[0090] 当USB 3.0装置初始化时(例如当其首次连接时)，USB 2.0管脚(例如管脚1104a-d)被用于建立初始连接。一旦初始化，USB 3.0装置与其连接的主机进行协商，以确定主机是否支持USB 3.0管脚。如果两者均支持USB 3.0，该USB装置和主机同意使能USB 3.0管脚(例如管脚1106a-e)，并且在USB装置与主机之间通信根据USB 3.0标准来进行。传输I/O智能芯片和/或装置还可以执行协商以确定两者是否都能够支持传输I/O(或者其他类型的)条件接入。例如，当智能芯片1102初始使用连接器1100连接到主机装置时，管脚1104a-e可被用于根据USB 2.0协议建立连接。但是，在初始连接后，作为执行用以确定主机是否支持USB 3.0的协商的替代，该协商可被用于确定主机是否支持本文公开的传输I/O实施例。如此，管脚1106a和1106b可被配置为以与智能卡704(附图7)的SC_out-以及SC_out+接点类似的方式传输和/或接收数据。例如，可以使用管脚1106a和1106b将网络加密内容传输给智能芯片。类似的，管脚1106d和1106e可被配置为以与智能卡704(附图7)的SC_IN-以及SC_IN+接点类似的方式传输和/或接收数据。例如，可以使用管脚1106d和1106e将本地加密内容从智能芯片1102传输给主机。

[0091] 附图12是使用连接器1206的条件接入系统1200的实施例。在实施例中，可以通过连接器1206将智能芯片1202连接到条件接入SoC 1204。为了便于说明，连接器1206在本公开中被作为USB 3.0连接器进行描述。但是，本领域技术人员可以意识到在本文公开的实施例中可以使用其他标准连接(例如，USB 2.0连接、mini USB连接、SCSI连接、以及IEEE 1394连接等等)。当智能芯片1202通过连接器1206连接到条件接入SoC 1204时，智能芯片1202和条件接入SoC 1204开始协商以确定是否两者都支持条件接入模式。当智能芯片1202和条件接入SoC 1204都支持类似的条件接入协议(例如传输I/O)时，高速线路1214(例如，使用附图11的管脚1106a-e的通信线路)，被配置为根据条件接入协议(例如传输I/O协议)进行操作，并且数据路径连接器1208在条件接入控制器1210和条件接入智能芯片1202之间路由通信。在这种条件下，通过通信线路1214将网络加密内容传输给智能芯片1202，而本地加密内容或者在替换实施例中的明文内容通过通信线路1214返回给条件接入SoC。在这种实施例中，通信线路1216可以使用利用USB 2.0协议的USB 2.0管脚来传输附加数据(例如指令和控制包、重置信号等等)。

[0092] 在可选实施例中，如果智能芯片1202和条件接入SoC 1204不支持相同的条件接入协议，则数据路径连接器1208通过高速线路1214将通信路由到USB控制器1212，并且根据USB协议执行操作，例如，可以在包括条件接入SoC 1204的装置与USB装置之间传输数据。在连接器1206使用不同的接口和/或协议(例如SCSI、IEEE 1394等)的可选实施例中，数据路径连接器1208可以将数据路由到针对该特定的接口和/或协议的控制器。如此，本发明的实施例提供了可以包括在任意类型的装置(例如膝上电脑、平板电脑、智能电话、电视等)内并且通过标准连接(例如USB 3.0接口)连接到外部装置的条件接入SoC 1204，从而有利于实现到两个条件接入部件(例如智能芯片1202)和其他类型的部件(例如，USB棒)的连接。

[0093] 附图13是用于确定是否配置用于条件接入模式的连接器的方法1300的实施例。该方法1300可以使用软件、硬件、或者软件和硬件的组合来实现。在实施例中，方法1300可以由条件接入SoC(例如来自附图12的智能芯片1202)执行。流程开始于步骤1302，在步骤1302中检测与其他装置的连接。例如，可以通过从外部装置接收通信信号或者功率来检测连接。本领域技术人员可以意识到在步骤1302可以执行本领域中公知的用于检测连接的任意方法。流程前进到，在步骤1304中与智能芯片所连接的装置执行协商。在实施例中，步骤1304可以包括智能芯片与该装置交换标识该装置是否支持条件接入协议和/或所支持的条件接入协议是否相同的信息。流程前进到判决步骤1306，在判决步骤1306中，基于该协商，作出所连接的装置和智能芯片是否支持公共条件接入协议的判决。如果该装置不支持条件接入，或者不支持相同的条件接入协议，则流程分支NO(否)到步骤1308，并且可以产生或者以其他方式提供指示该装置不支持条件接入的错误通知。备选地，返回到判决步骤1306，如果该装置和智能芯片支持相同的条件接入协议，例如本文公开的传输I/O实施例，则流程分支YES到步骤1310。在步骤1310中，连接器被配置为支持条件接入模式。例如，如果连接器是USB 3.0连接器，则返回去参考附图11中的示例性连接器，管脚1106a和1106b可被配置为SC_out-以及SC_out+连接，而管脚1106c和1106d可被配置为SC_IN-以及SC_IN+连接。流程随后前进到步骤1312，在步骤1312中根据条件接入协议执行操作。例如，在步骤1312中，传输I/O智能芯片(例如附图11中的示例性的智能芯片1102)可以经由管脚1106a和1106b(附图11)接收网络加密内容，解密网络加密内容，执行本地加密，以及经由管脚1106c和1106d

(附图11)提供本地加密内容。

[0094] 附图14是用于确定是否执行条件接入操作的方法1400的实施例。方法1400可以使用软件、硬件、或者软件和硬件的组合来实现。在实施例中，方法1400可以由能够连接到条件接入智能芯片的装置来执行。在可选实施例中，方法1400可以由条件接入SoC执行。流程开始于步骤1402，在步骤1402中在执行方法1400的装置或SoC(例如附图12中的装置1204)与连接到该装置或SoC的外部装置之间执行协商。在实施例中，步骤1402可以包括交换标识装置是否支持条件接入协议和/或所支持的条件接入协议是否相同的信息。流程前进到判决步骤1404，在判决步骤1404中，基于该协商，作出所连接的装置(例如智能芯片)是否支持条件接入协议的判决。如果所连接的装置不支持条件接入，或者不支持相同的条件接入协议，则作出所连接的装置不是智能芯片或者以其他方式不能够执行条件接入的决定。一旦作出如此决定，流程分支NO到步骤1406并且与外部装置的通信被路由到连接器控制器。在实施例中，连接器控制器可被配置为根据基于所使用的连接器的类型(例如USB 2.0、USB 3.0、SCSI、IEEE 1394等等)的协议执行操作。流程随后前进到步骤1408，在步骤1408中使用连接器协议执行操作。例如，如果连接器是USB 3.0连接器，在步骤1408中，根据USB 3.0协议执行操作。

[0095] 返回到判决步骤1404，如果该装置确实支持条件接入协议，流程分支YES(是)到步骤1410。在步骤1410中，与外部装置的通信可被路由到条件接入控制器(例如附图12中的控制器1210)。例如，与外部装置的通信可被路由到传输I/O控制器。流程随后前进到步骤1412，在步骤1412中根据条件接入协议执行操作。例如，在步骤1412中，网络加密内容可被发送给外部装置并且可从外部装置接收本地加密内容。

[0096] 附图15是表示经由标准连接器(例如，USB 3.0连接器)执行网络内容解密的方法1500的方法。在实施例中，方法1500可以由安全装置或者安全处理器来执行。在另一个实施例中，方法1500可由智能芯片(例如附图11的智能芯片1102)来执行。在实施例中，方法1500可在附图13的步骤1312期间执行。可以使用软件、硬件、或者软件和硬件的组合来实现方法1500。流程开始于步骤15102，在步骤1502中由安全装置接收网络加密内容。在实施例中，网络安全内容可以是使用NCW加密的内容。该NCW可以是用于加密和解密发送给多个用户或者订户的内容的公共控制字或加密密钥。在一个实施例中，网络加密内容是单个数据流。在可选实施例中，网络加密内容可以包括多个网络加密流，例如网络加密基本流。网络加密基本流可以是包含例如音频、视频数据、闭合字幕数据或者其他类型的数据的流。网络加密基本流可以由来自单一源(例如特定的网络或者信道)的压缩数据构成。在网络加密内容可以包括多个网络加密基本流的实施例中，在步骤1502中可以分别接收一个或者多个网络加密基本流。但是，在可选实施例中，在步骤1502中可以接收包括多个网络加密基本流的网络加密内容。在这种实施例中，可以过滤出各个网络流，例如通过执行PID过滤或者其他类型的过滤，从而在步骤1502中隔离一个或者多个单独的网络加密基本流。

[0097] 如先前讨论的，在实施例中，连接器可能不具有足够的连接点(例如管脚)来映射传输I/O智能卡(例如附图7的智能卡704)的所有接点。如此，在步骤1502中接收的网络加密内容可以是以依照时钟恢复机制的格式来接收的。不同的时钟恢复机制可被用于本文公开的系统和方法。例如，本文公开的实施例在实践中可以使用不同的时钟恢复机制，包括，但不限制于：锁相环、8B/10B编码、八-至-十四调制，或者现有技术已知的任意其他类型的时

钟恢复机制。在一些实施例中，时钟恢复数据可被包含在步骤1502接收的网络加密内容一起。在实施例中，网络加密内容中包含的时钟恢复数据的类型可以基于所使用的时钟恢复机制的类型。在实施例中，作为网络加密内容的一部分接收的时钟恢复数据可被执行方法1500的装置(例如智能芯片)使用以同步通信。

[0098] 一旦接收到网络加密内容，流程前进到步骤1504，在步骤1504中获得网络控制字。在一个实施例中，网络控制字可以是由内容提供商(例如，但不限制于，传输内容的头端或者服务器)提供的控制字。在实施例中，该网络控制字可以事先就已经被执行方法1500的装置获知。在另一实施例中，网络控制字可被装置接收。在这种实施例中，网络控制字可被加密，并且步骤1504可以包括解密该网络控制字。例如，在实施例中，可以通过解密包含网络控制字的ECM来获得网络控制字。可以使用来自于其他消息(例如，EMM)的信息来解密该ECM。虽然ECM和EMM消息是DVB架构的一部分，但是本领域技术人员可以意识到本文公开的系统和方法可以使用其他内容递送系统和结构。

[0099] 流程继续前进到步骤1506，在步骤1506中使用网络控制字解密网络加密内容(例如，一个网络加密基本流或者多个网络加密基本流)。在一个实施例中，可以使用单个网络控制字来解密网络加密内容。在可选实施例中，可以使用多个控制字来解密网络加密内容，例如当网络加密内容包括多个已经各自使用不同网络控制字加密的网络加密基本流时就是如此。在这种实施例中，在步骤1504中可以获得多个网络控制字，并且随后在步骤1506它们被用于解密多个网络基本流。但是，在其他方案中，可以使用单个网络控制字来加密多个网络内容基本流。在这种实施例中，单个网络控制字可被用于解密多个网络加密基本流。步骤1506中的对网络加密内容的解密可以得到明文内容，即没有被加密保护的内容。由于步骤1502-1506由安全装置或者安全处理器执行(例如，但不限制于，智能卡和/或智能芯片)，网络控制字保留在安全装置上。通过将网络控制字维护在装置上，未授权的订户不能够拦截在智能卡和装置(例如机顶盒)之间传输的网络控制字，从而防止了未授权用户接入内容。在未在附图15示出的实施例中，在解密步骤1506之后，可由安全处理器(例如处理芯片)提供明文内容以供显示和/或存储。但是，在示出的实施例中，可以通过执行本地链路加密来添加附加的保护层。在实施例中，本地链路加密可以包括使用本地控制字(LCW)重新加密明文内容。该本地控制字可以是特定装置独有的加密密钥。例如，LCW可以是仅仅与执行方法1500的智能芯片可以与之通信的特定装置(例如，电视、计算机等)共享的加密密钥。在可选实施例中，例如，当安全处理器正在与其他类型的装置(例如，但不限制于智能电话、膝上电脑、平板电脑等)通信时，LCW可以是仅仅与和安全处理器通信的特定装置共享的加密密钥。在实施例中，对于本地链路加密，可以使用不同类型的加密模式。在一个实施例中，不是所有的表示内容的数据都使用本地链路加密来加密。例如，可以使用传输模式加密。在实施例中，传输模式加密包括确定数据的哪些比特要基于MPEG2传输加密来加密。在另一个实施例中，可以执行批量(Bulk)模式加密。在批量(Bulk)模式加密中，在本地链路加密期间，可以加密所有表示数据的比特。批量(Bulk)模式加密可被用于在装置之间以安全方式交换数据。例如，批量(Bulk)模式加密可被用于将传输输入(例如内容)与由参与对内容的加密/解密的一个或多个部件使用的内部数据进行混合。在其他实施例中，批量(Bulk)模式加密可被用于支持可以提供附加特征的其他类型的内容流，例如互联网协议电视(IPTV)内容流。对加密模式的选择可以基于内容中或者包括该内容的数据流中存在的数据。例如，一个或

者多个比特可以是明文内容的一部分或者可被增加到明文内容，从而标识在本地链路加密期间执行的加密模式。此外，在实施例中，在本地链路加密期间执行的加密算法通常符合ATIS-08000006标准。但是，本领域技术人员可以意识到任何类型的加密算法都可以用于本地链路加密，只要相同的加密算法在智能芯片和装置二者上都是可获得的。在实施例中，可以使用与用于接收网络加密内容的连接不同的连接来向安全装置发送定义加密类型的控制包。例如，如果使用USB 3.0连接器，则可以在使用USB 3.0管脚流式传输网络加密内容和本地加密内容的同时使用USB 2.0管脚发送控制包。

[0100] 在实施例中，用于选择将要用于本地链路加密的密钥的密钥设置可以跨安全边界发生。例如，密钥交换可以作为密钥设置的一部分，在智能卡和机顶盒之间发生。交换的密钥可以由安全装置(例如智能卡)产生，并且被传输给正与安全装置通信的特定装置。因为本地链路加密是特定针对单个装置的，而不是特定针对网络传输的，所以对本地链路加密密钥的拦截不会向未授权用户提供全面接入广播的网络内容的能力。在实施例中，多个密钥可被用于本地链路加密。例如，智能卡可以能够同时处理多个输入流并且输出多个本地加密流。在这种实施例中，每一个本地加密流可以是使用独有的本地链路加密密钥进行加密的。但是，在其他实施例中，可以使用相同的本地链路加密密钥来加密每一个本地加密流。在实施例中，密钥交换可以使用与用于接收网络加密内容的连接不同的连接来传输。例如，如果使用USB 3.0连接器，则在使用USB 3.0管脚流式传输网络加密内容和本地加密内容的同时，可以使用USB 2.0管脚进行密钥交换。

[0101] 流程前进到步骤1508，在步骤1508中获得本地控制字。本地控制字可以是任意类型的加密密钥。在实施例中，本地控制字可以是特定装置专用的加密密钥。在实施例中，本地控制字可以从普通软件寄存器、硬件密钥阶梯(key ladder)、随机密钥产生器，或者从任意其他源中获得。在一个实施例中，本地控制字可以是动态地产生的，并且与接收装置共享。在这种实施例中，可以基于该装置的特性来产生密钥。在实施例中，在获取步骤1508期间可以选择多个密钥。例如，可以从密钥阶梯中选择两个密钥。密钥阶梯可以存储或者以其他方式标识多个相关的密钥。在实施例中，本文公开的实施例可以使用任意类型的加密密钥，例如，固定加密密钥、动态加密密钥、随机产生的加密密钥等等。

[0102] 在获得本地控制字后，流程继续前进到步骤1510，在步骤1510中，使用本地控制字来重新加密网络解密内容，以产生本地加密内容。如先前讨论的，在步骤1510中可以使用不同类型的加密模式和加密算法来加密内容。在实施例中，加密可以基于在步骤1508中获得的密钥。在获得多个密钥的实施例中，在步骤1510中，密钥之一可被选择，并且在加密期间使用。例如，可以基于内容中的标识符选择合适的密钥。该标识符可以是内容的一部分，或者可在方法1500期间它被处理时被增加到内容或与内容关联的头部。该标识符可以是标识偶数或者奇数密钥(在获得两个密钥的实施例中)的单一比特。这一标识符提供了对在步骤1510的加密处理期间使用的密钥的自动选择。

[0103] 在另一个实施例中，除了加密内容之外，内容的大小也增加了。为了使得在网络上共享内容变得更困难，增加内容的大小可能是有利的。例如，增加内容大小将会需要更高的带宽来通过网络与未授权的用户正确地共享内容。例如，可以向广播流添加数据，以使得其更难以处理或者与未授权用户共享。在内容被流传输(例如音频和/或视频内容)的实施例中，非内容数据包可被增加到内容流并且带宽率将被增加。这种带宽的增加以及非内容数

据的附加通过使得内容更难被共享和处理，在内容离开执行方法1500的安全装置和/或安全处理器时为内容提供了附加安全性。在2009年4月27日申请的题目为“Methods and Apparatus for Securing Communications Between a Decryption Device and a Television Receiver(用于在解密装置和电视接收机之间的安全通信的方法和设备)”的U.S专利No.8,385,542中提供了关于流扩展的更多细节，在此通过参考将该专利全文并入本文。

[0104] 在实施例中，流程前进到可选步骤1512，其中时钟恢复数据被添加到本地加密内容。在实施例中，网络加密内容中包含的时钟恢复数据的类型可以基于所使用的时钟恢复机制的类型。例如，本文公开的实施例在实践中可以使用不同的时钟恢复机制，包括，但不限制于：锁相环、8B/10B编码、八-至-十四调制，或者现有技术已知的任意其他类型的时钟恢复机制。步骤1512是可选的，因为一些时钟恢复机制不需要添加时钟恢复数据(例如锁相环)。在这种实施例中，在步骤1514中，可以根据所选择的时钟恢复机制提供数据。

[0105] 尽管方法1500的实施例将解密网络加密内容、随后本地加密该解密的网络加密内容、以及然后添加时钟恢复数据作为三个分离步骤进行描述，但是本领域技术人员应该意识到，在实施例中，该解、加密和/或添加时钟恢复数据可以顺序执行，作为单个步骤执行，作为两个步骤执行、或者并行执行。在实施例中，本领域技术人员将意识到流扩展也可以在单个解密/加密步骤中执行。如此，本领域技术人员将意识到参考附图15描述的方法可以使用与在此示出的步骤更少或者更多的步骤来执行。

[0106] 在又一个实施例中，方法1500可以操作用于流数据。在该实施例中，在步骤1502中可以接收网络加密流，在步骤1504中通过解密网络加密流来产生明文内容流，以及在步骤1512中产生本地加密流。本领域技术人员将意识到在此参考附图15公开的实施例也可以操作用于流数据以及以任意其他形式传输的数据。

[0107] 对于附图15示出的实施例，在执行本地加密后，流程还可以继续前进到步骤1512，在步骤1512中本地加密内容连同时钟恢复数据被提供给另一装置。例如，在步骤1514中，智能芯片可以将具有时钟恢复数据的本地加密内容提供给条件接入SoC、智能电话、膝上电脑、平板电脑或者所连接的以其他方式与智能芯片通信的任意其他装置。此外，当连接器没有提供时钟信号的传输时，包含时钟恢复数据可以允许同步在执行方法1500的安全处理器和其他装置之间的通信。在通用计算装置中，在步骤1512中，将本地加密内容从安全处理器(例如，智能芯片)提供给通用处理器和/或未保护存储器以供存储和/或显示。本领域技术人员将会明白该方法1500通过下述方式提供了对在此描述的问题的解决方案：将本地加密内容提供给不安全部件，而不是像不支持本文描述的传输I/O系统的实施例的装置和方法通常执行的那样提供控制字或者加密密钥。此外，本领域技术人员将会明白：当数据从安全装置和/或处理器传输给通用装置时，在这种内容保护系统中，很小的安全泄露有可能发生。但是，本文公开的实施例通过下述方式解决了这一缺点：提供本地加密内容(优选地，其数据和带宽被扩展的内容)，从而使得未授权用户更难处理、共享和接入内容，即使当该内容在安全装置和/或安全处理器系统/架构内部传输时被拦截也是如此。

[0108] 在一个实施例中，本地加密内容可以作为各个单独的本地加密基本流来提供。例如，在接收和解密多个网络加密基本流的实施例中，多个基本流可被分别单独加密并且分别作为单独的本地加密基本流来返回。在这种实施例中，每个流可以包括时钟恢复数据。在

可选实施例中，多个网络加密基本流可被复用到单个输出流中。在这种实施例中，在步骤1514中，可以本地加密和随后提供单个输出流。该单个输出流可以包括时钟恢复数据。在实施例中，可以在执行步骤1510的本地加密之前或者在本地加密步骤1510之后，将多个基本流复用到单个输出流。

[0109] 附图16是用于处理经由连接器(例如，USB 3.0连接器)接收的本地加密内容的方法1600的实施例。在实施例中，方法1600可以由诸如机顶盒、膝上电脑、平板电脑、智能电话、电视或者其他类型的通用计算装置之类的装置来执行。在实施例中，方法1600可以在附图14的步骤1412期间执行。可以使用软件、硬件、或者软件和硬件的组合来实现方法1600。流程开始于步骤1602，在步骤1602中本地加密内容被接收。在实施例中，本地加密内容可以是从执行参考附图15描述的方法1500的安全装置(例如安全处理器和/或智能芯片)接收的。例如，在非限制性实施例中，本地加密内容可以从经由连接器(例如，USB 3.0)与装置通信的智能芯片接收。

[0110] 如先前讨论的，在实施例中，在安全装置(例如智能芯片)与执行方法1600的装置之间的连接器不具有足够的连接点(例如管脚)来映射的传输I/O智能卡(例如附图7的智能卡704)的所有接点。如此，在步骤1602中接收的本地加密内容可以是以依照时钟恢复机制的格式来接收的。不同的时钟恢复机制可被用于本文公开的系统和方法。例如，本文公开的实施例在实践中可以使用不同的时钟恢复机制，包括，但不限制于：锁相环、8B/10B编码、八-至-十四调制，或者现有技术已知的任意其他类型的时钟恢复机制。在一些实施例中，时钟恢复数据可被包含在步骤1602接收的网络加密内容一起。在实施例中，网络加密内容中包含的时钟恢复数据的类型可以基于所使用的时钟恢复机制的类型。在实施例中，作为网络加密内容的一部分接收的时钟恢复数据可被执行方法1600的装置(例如条件接入SoC、智能电话、膝上型计算机等)使用以同步通信。

[0111] 一旦接收到具有时钟恢复数据的本地加密内容，流程前进到步骤1604，在步骤1604中接收本地控制字。本地控制字可以是任何类型的加密密钥。在实施例中，本地控制字可以是专用于执行方法1600的装置的加密密钥。在实施例中，本地控制字可以从使用普通软件寄存器的智能芯片、硬件密钥阶梯、随机密钥产生器或者该装置专用的任意类型的源中获得。在一个实施例中，本地控制字可以从安全装置(例如执行方法1500的智能芯片和/或处理器)接收。在这种实施例中，可以经由另一连接接收本地控制字。例如，可以经由与用于接收本地加密内容的连接不同的连接(例如不同的管脚)来接收本地控制字。例如，如果使用USB 3.0连接器，则在使用USB 3.0管脚流式传输网络加密内容和本地加密内容的同时，可以使用USB 2.0管脚进行本地控制字交换。

[0112] 在另一个实施例中，本地控制字可以由执行方法1600的装置产生。在这种实施例中，可以先前已经与创建在步骤1602中接收的本地加密内容的安全处理装置、智能芯片和/或安全处理器共享本地控制字。本地控制字可以是随机产生的。在实施例中，可以使用单个本地控制字。在其他实施例中，可以使用多个本地控制字。在这种实施例中，本地控制字可以周期性地改变，使得在设定的时间段后，该本地控制字被作废，而启用新的本地控制字。

[0113] 流程前进到步骤1606，在步骤1606中使用本地控制字解密本地加密内容。对本地加密内容的解密将会产生应用可接入的明文内容。本领域技术人员可以意识到很多类型的加密模式和/或算法可被用于解密本地加密内容。如此，在步骤1606中可以使用某种类型的

解密算法来利用本地控制字解密内容。此外，执行解密的装置可以能够操作和处理本地加密内容，尽管本地加密内容的带宽由于非内容数据而增加。在这种实施例中，步骤1606中对本地加密内容的解密可以包括：识别和从内容中移除非内容数据。在另一个实施例中，直到明文内容被处理以供显示或者存储，才会发生对非内容数据的移除。当在步骤1606中解密本地加密内容时，执行方法1600的装置还可以使用时钟恢复数据。

[0114] 流程前进步骤1608，在步骤1608中提供明文内容。在一个实施例中，提供明文内容可以包括解码、显示和/或以其他方式呈现明文内容。例如，明文内容可被显示在电视、监视器和/或显式器上，该电视、监视器和/或显式器可以是为执行方法1600的装置的一部分或者与执行方法1600的装置通信。在另一实施例中，提供明文内容可以包括将明文内容存储到数据存储器中，该数据存储器可以是执行方法1600的装置的一部分或者连接到执行方法1600的装置。

[0115] 在可选实施例中，持久加密可以不是通过如附图16所描述的立即解密本地加密内容来执行的。在这种实施例中，持久加密可被应用于内容，例如从广播的网络传输接收的MPEG传输包。在这种实施例中，安全装置仍可以如附图1500中所示那样执行网络解密和本地链路加密；但是，接收本地加密内容的装置可以不立即执行本地链路解密。替代地，接收本地加密内容的装置可以存储本地加密内容(按它加密后的样子)，供以后使用。这允许对内容进行加密以便于安全的本地存储，但是安全装置仍然可以例如通过在稍后的时间提供解密密钥来控制何时解密内容。

[0116] 附图17是本文公开的系统可以使用的或者可以用于执行本文公开的方法的安全处理器装置1700的实施例。在实施例中，该安全处理装置可以是智能芯片。但是，本领域技术人员可以意识到本文描述的系统和方法可以使用任何其他类型的安全装置。在实施例中，安全处理装置1700可被连接到执行本文通过参考附图4描述的方法400的装置。在另一个实施例中，安全处理装置1700可以是执行方法400的装置的可拆卸部件。在实施例中，安全处理装置1700可以执行参考附图13描述的方法1300。在另一个实施例中，安全处理装置1700可以执行参考附图15描述的方法1500。

[0117] 在实施例中，安全处理器装置1700包括一个或者多个智能芯片1702。该一个或者多个智能芯片可以包括一个或者多个处理单元。在一些实施例中，本文描述的方法的一个或者多个部分是由一个或者多个智能芯片1702执行的。例如，一个或者多个智能芯片1702可被用于如附图15的方法1500中描述的解密网络加密内容，创建本地加密内容，以及创建非内容数据。

[0118] 安全处理装置1700还可以包括存储器1704。存储器1704包括计算机存储媒体，例如，但不限制于，RAM、ROM、EEPROM、闪存或者其他存储技术，或者用于存储信息且可被安全处理装置1700和一个或者多个处理单元1702存取的任意其他有形媒体。存储器1704还存储用于执行本文描述的方法的可执行指令。例如，存储器1704可以包括用于解密网络加密内容(NEC)1706的指令。存储器还可以存储用于加密明文内容以创建本地加密内容(LEC)1708的指令。此外，存储器1704可以包括执行本文描述的USB/传输I/O协商1710的指令。此外，USB/传输I/O协商指令1710可以包括用于基于该协商来配置连接(例如重配置USB 3.0连接器中的管脚)的指令。

[0119] 安全处理装置1700还可以包括允许该装置与其他装置通信的一个或多个通信连

接1712。通信连接1712可以包括标准连接器，诸如USB 2.0连接器、USB3.0连接器、SCSI连接器、IEEE1394连接器等等。通信连接1712可被用于发送通信媒体。通信媒体可以具体表现为调制的数据信号，例如载波或者其他传输机制，并且包括任意的信息传递媒体，其可以包括计算机可读指令、数据结构、程序模块、或者具有调制数据信号形式的其他数据。术语“调制的数据信号”意思是具有其特征集中的一个或多个特征的信号或者以将信息或消息编码在数据信号中的方式改变的信号。作为举例而非限制，通信媒体包括有线媒体(例如有线网络或者直接有线连接)，以及无线媒体(例如声音、RF、红外以及其他无线媒体)。在实施例中，网络加密内容例如可以通过通信连接1712接收。本地加密内容可以通过通信连接1712传输。在又一个实施例中，执行在此描述的传输I/O方法的指令可以经由通信连接1712来接收。例如，头端可以用执行本文公开的方法的指令来更新安全处理装置1700。该指令可被存储在存储器1704中。通信连接1710因此允许头端使用执行本文公开的方法的指令来更新在本领域中部署的安全装置。通信连接还为安全处理装置1700提供从一装置接收网络加密内容以及将本地加密内容返回给该装置的能力。

[0120] 尽管安全处理装置1700的实施例被示出为具有包括用于执行本文公开的方法的指令的存储器1704，但是在可选实施例中，用于执行本文公开的方法的指令可由作为安全处理装置1700的一部分的专用集成电路(ASIC)来执行。

[0121] 本文公开的实施例提供了用于使用安装在多个不同装置上的通用连接器(例如USB 3.0连接器)执行条件接入(例如本文公开的传输I/O实施例)的系统、方法和装置。尽管已经在文中公开了特定实施例，但是本领域技术人员可以意识到，在不超出本发明的范围内，可以使用其他方法来利用通用连接器执行条件接入。例如，USB 3.0协议堆栈可被如是使用以封装数据包，所述数据包包括命令和控制数据、重置数据、网络加密内容和/或本地加密内容。

[0122] 可以使用软件、硬件、或者软件和硬件的组合来利用本文描述的实施例，以实现和执行本文公开的系统和方法。尽管在整个说明书中，特定的装置已经被描述为执行特定功能，但是本领域技术人员可以意识到，这些装置是出于说明目的而提供的，并且可以使用其他装置来执行本文公开的功能而不超出本发明的范围。

[0123] 通过参考附图，本说明书描述了本发明的一些实施例，其中仅仅是示出了可能的实施例中的一些实施例。然而，其他方案可以以多种不同的形式来具体实现，并且不应该视为限于本文公开的实施例。此外，提供这些实施例是为了使得本公开是全面且完整的，而且向本领域技术人员完全传递了可能的实施例的范围。

[0124] 尽管在此描述了特定实施例，但是本发明的范围不限于这些特定实施例。本领域技术人员可以想到在本发明的范围和精神内的其他实施例或者改进。因此，特定的结构、步骤或者媒体仅仅是作为示意性说明而公开的。本发明的范围由所附的权利要求及其等同替换来定义。

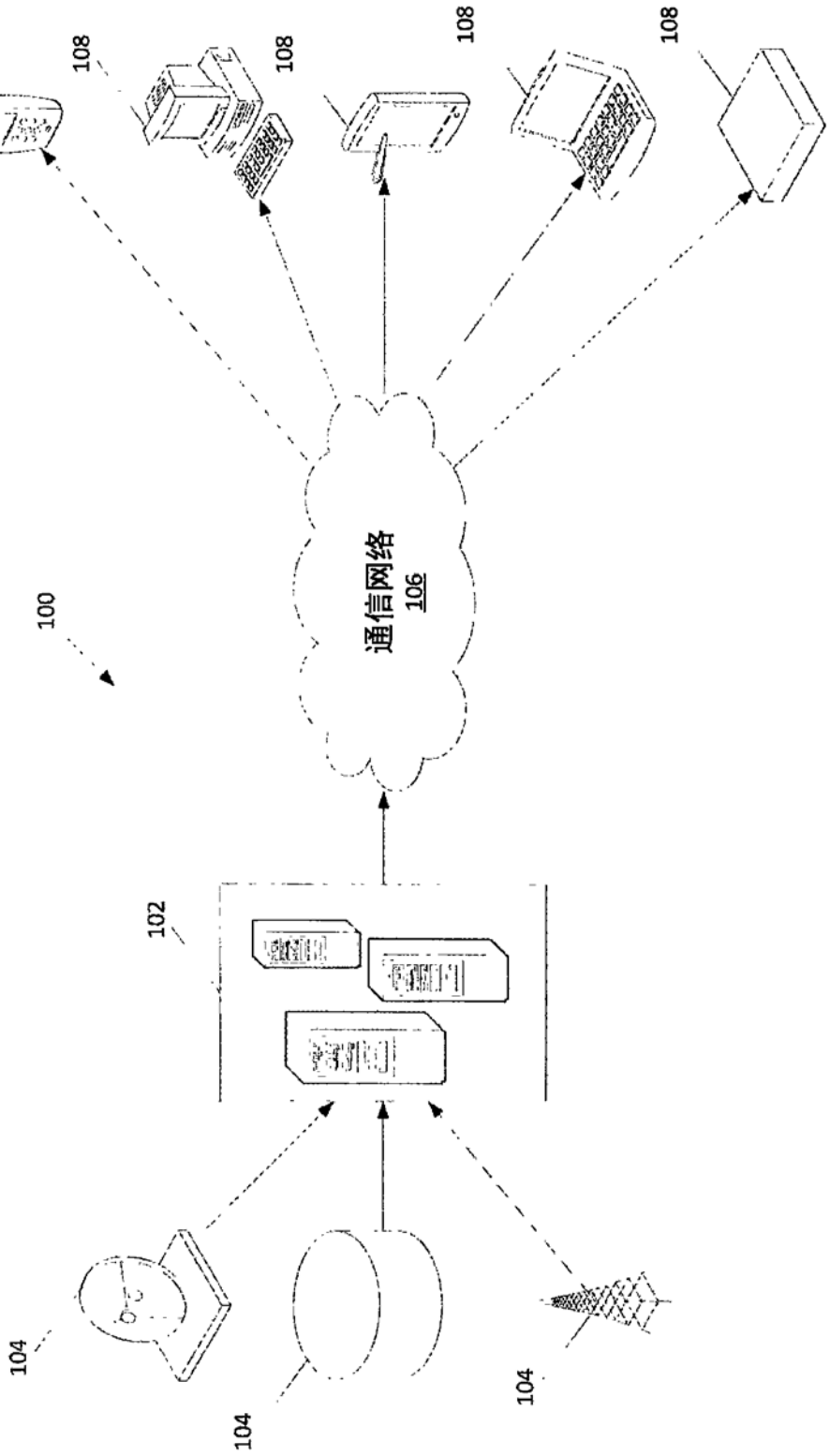


图1

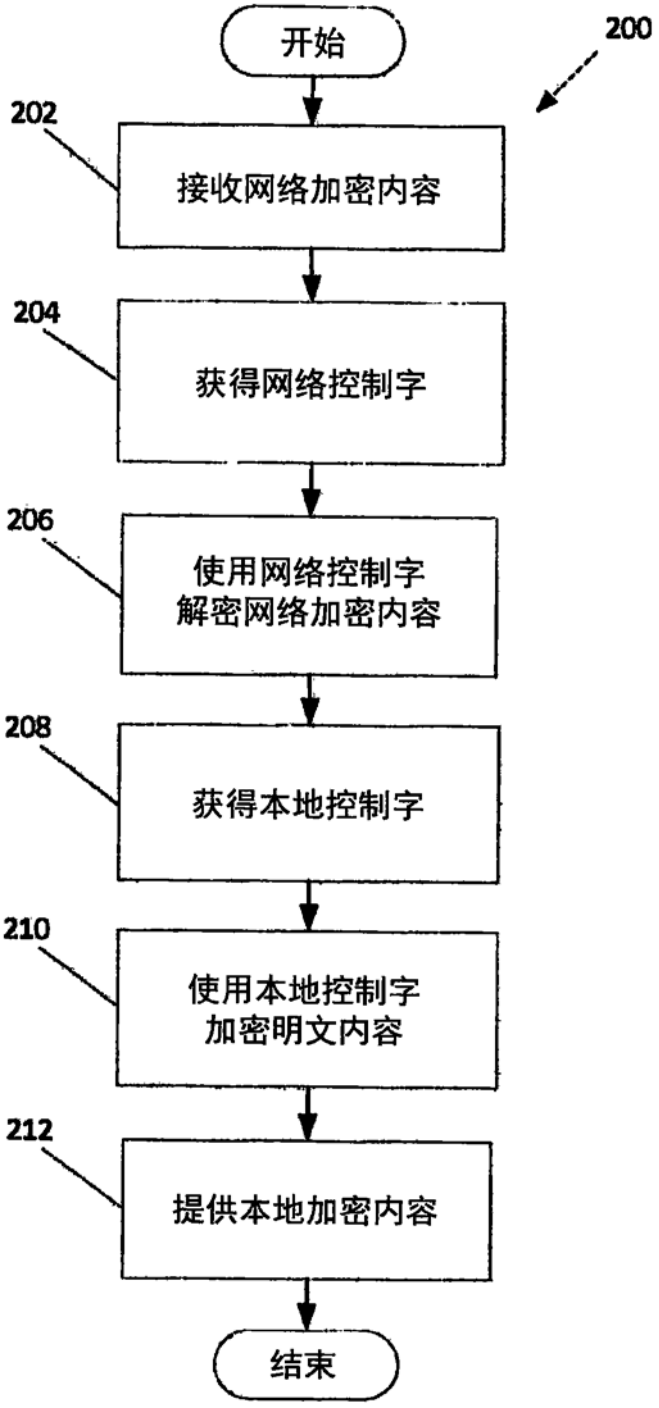

开始
200
202
接收网络加密内容
204
获得网络控制字
206
使用网络控制字
解密网络加密内容
208
获得本地控制字
210
使用本地控制字
加密明文内容
212
提供本地加密内容
结束

图2

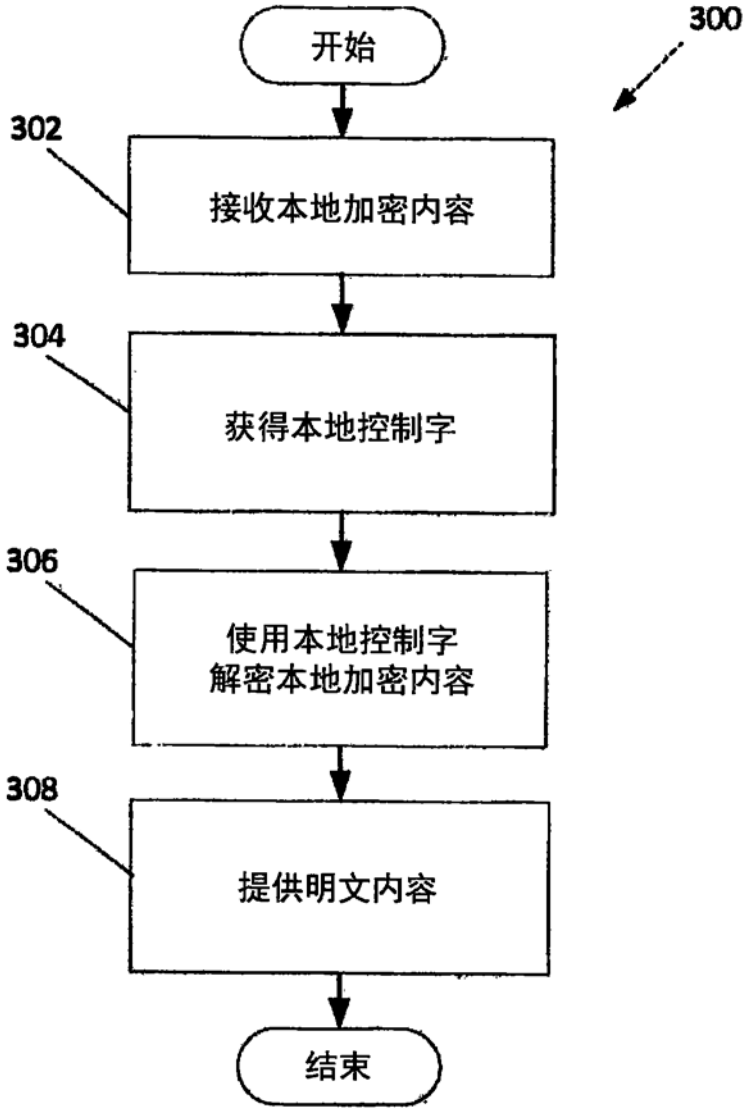

300
开始
302
接收本地加密内容
304
获得本地控制字
306
使用本地控制字
解密本地加密内容
308
提供明文内容
结束

图3

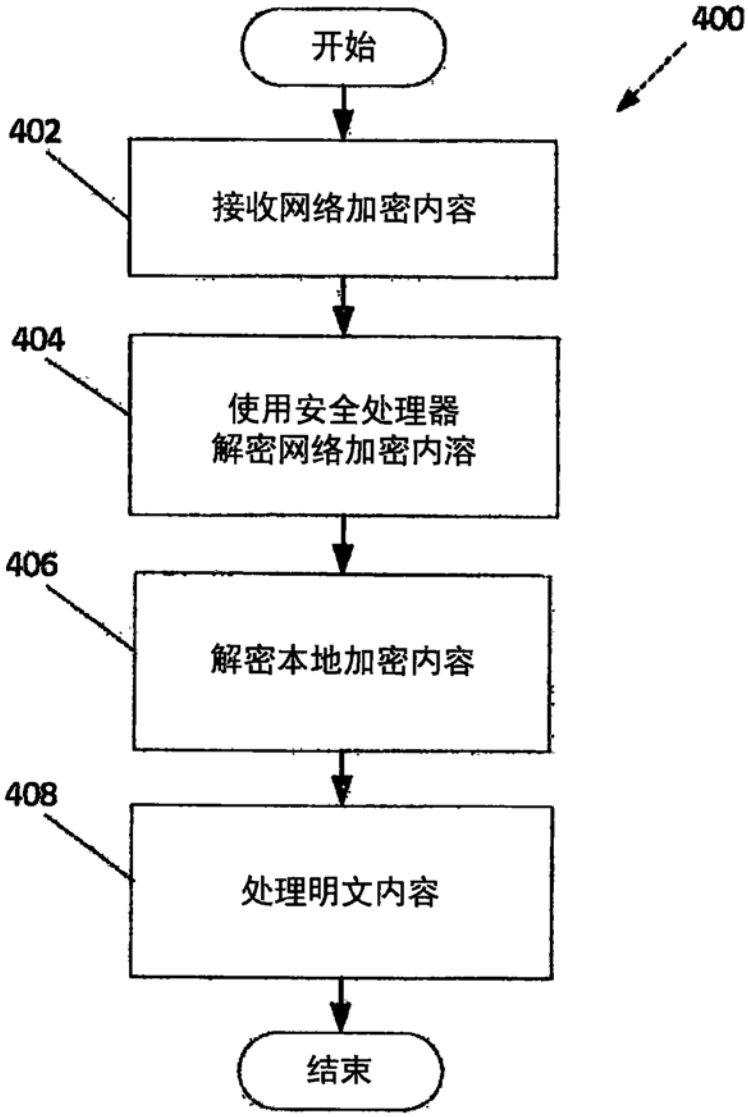

400
开始
402
接收网络加密内容
404
使用安全处理器
解密网络加密内溶
406
解密本地加密内容
408
处理明文内容
结束

图4

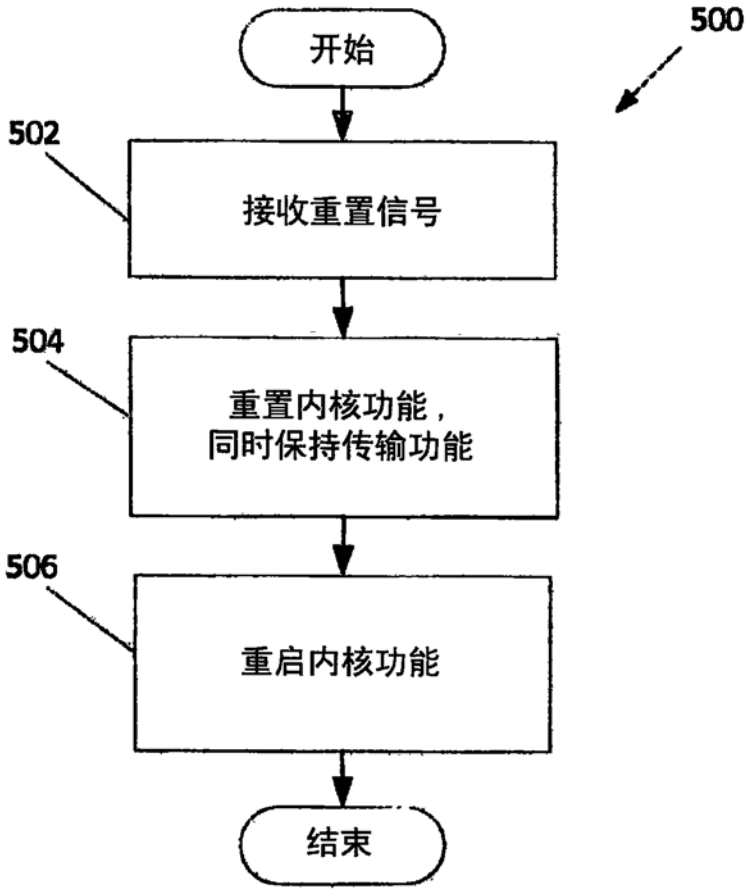


图5

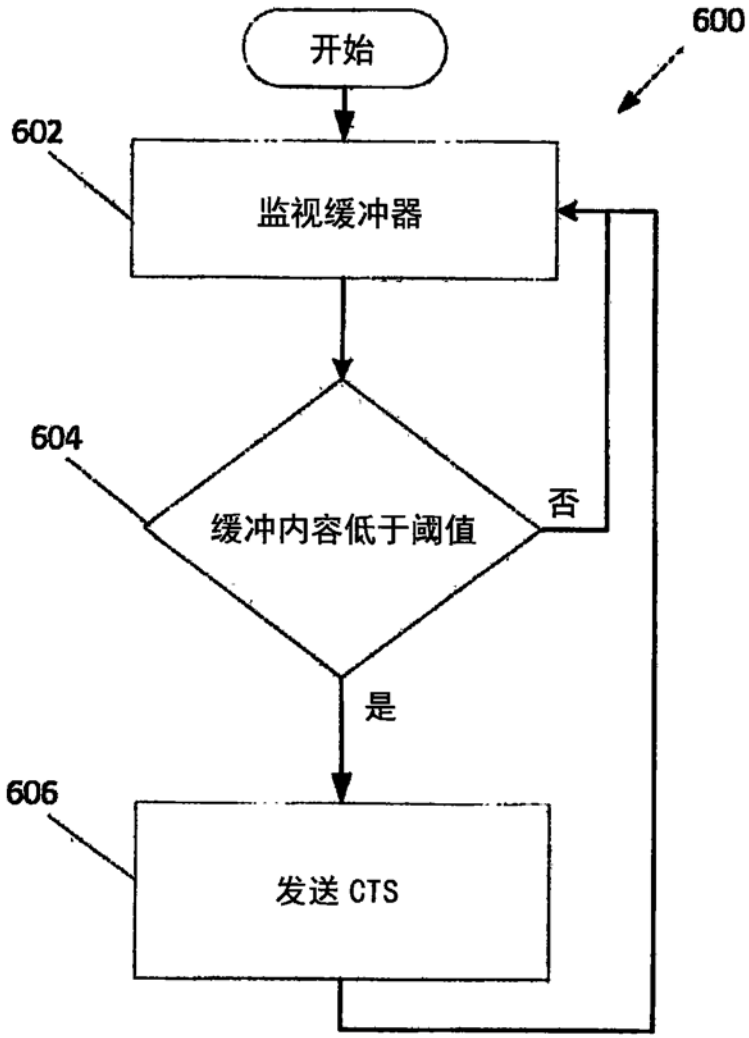


图6

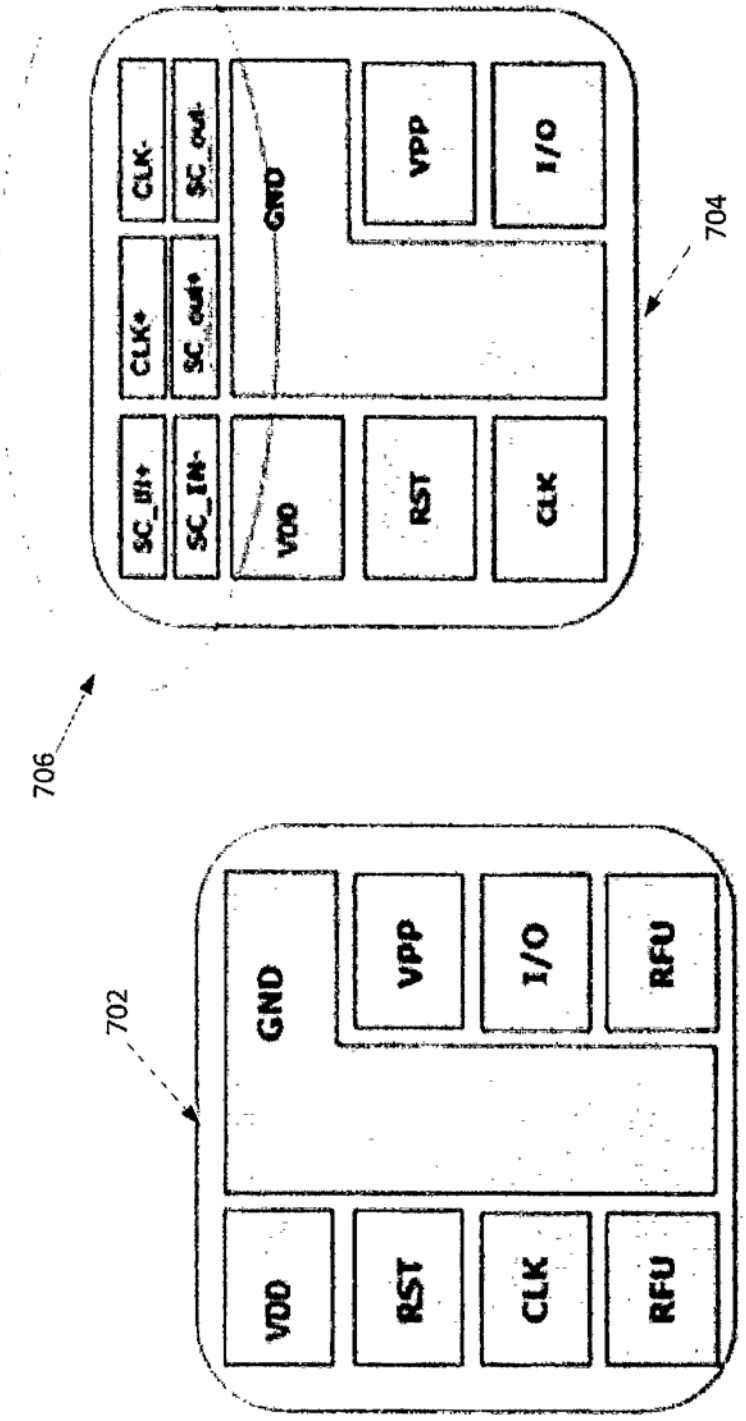

CLK-
SC_out-
GND
VPP
I/O
704
CLK+
SC_out+
SC_IN+
SC_IN-
VDD
RST
CLK
706
702
GND
VPP
I/O
RFU
VDD
RST
CLK
RFU

图7

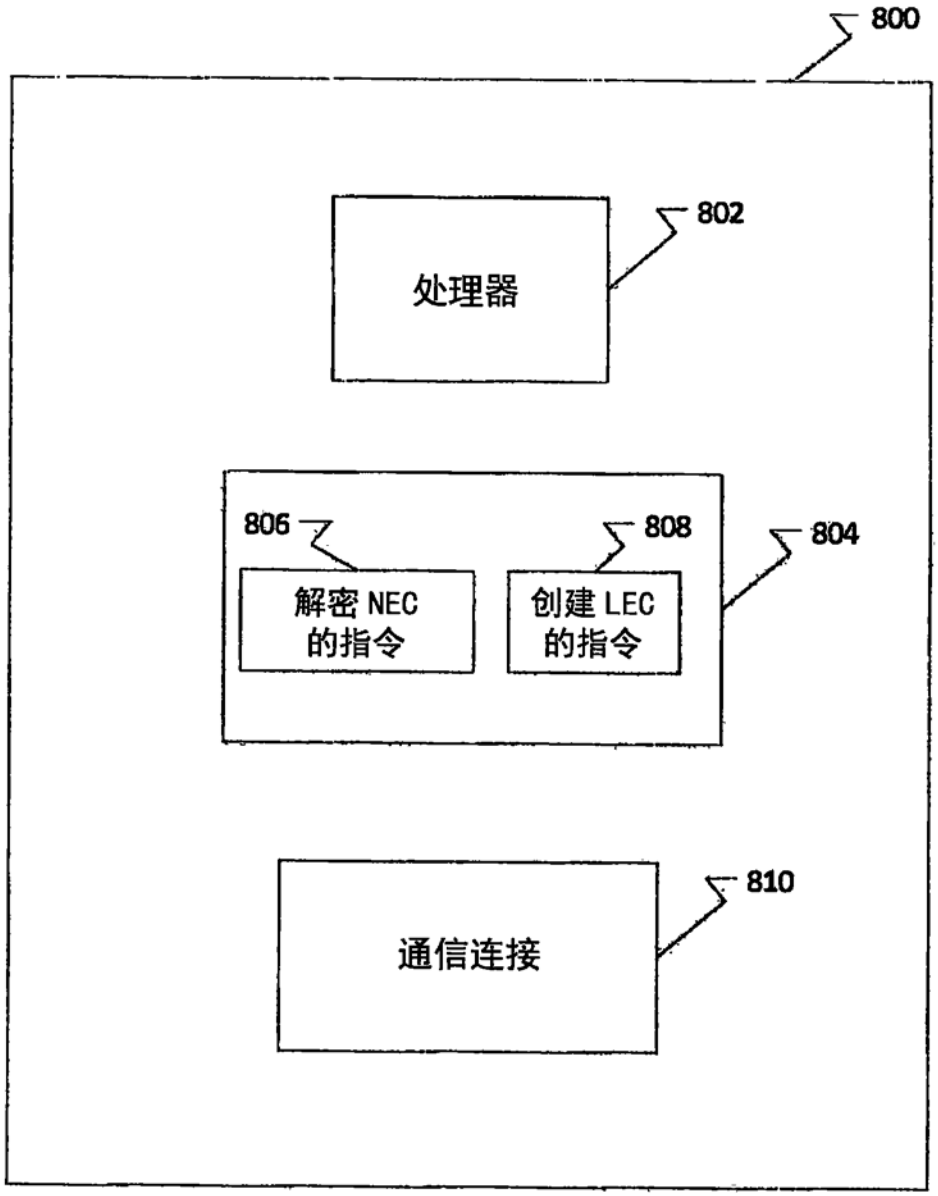


图8

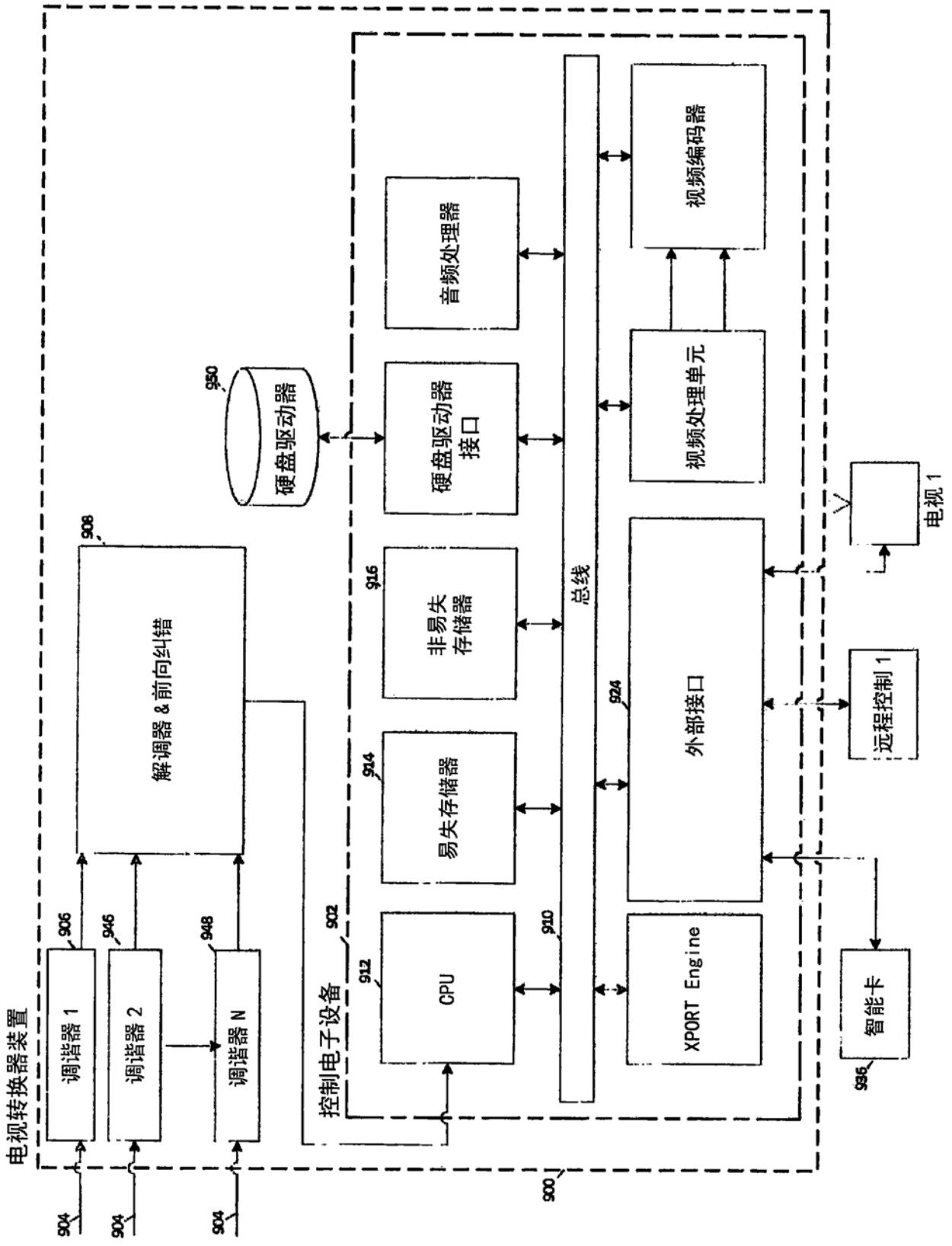

电视转换器装置
调谐器 1
调谐器 2
调谐器 N
解调器 & 前向纠错
控制电子设备
CPU
易失存储器
非易失存储器
硬盘驱动器
硬盘驱动器接口
音频处理器
视频编码器
视频处理单元
总线
外部接口
XPORT Engine
远程控制 1
智能卡
电视 1
900
902
904
906
908
910
912
914
916
924
926
946
948
950

图9

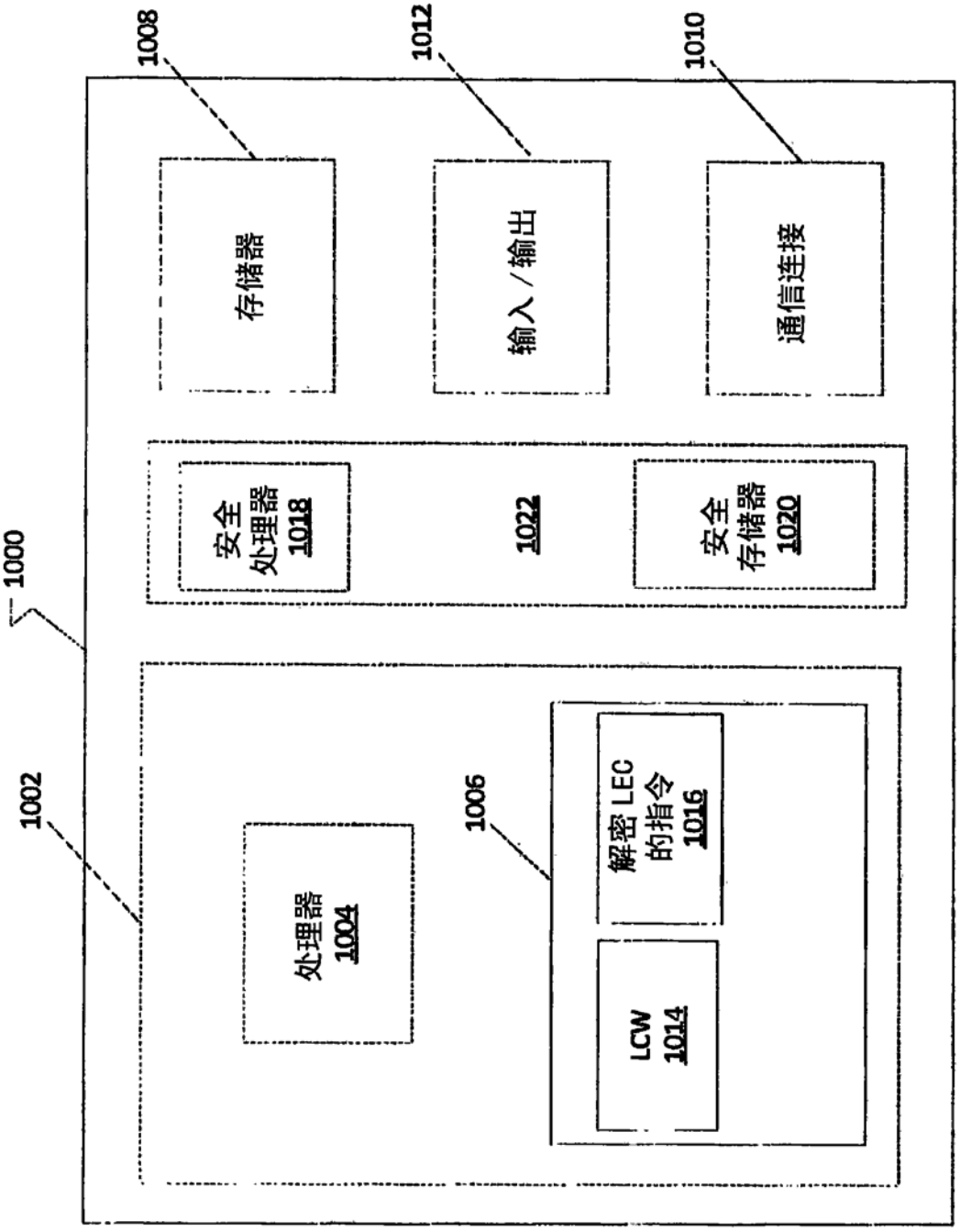

1000
1002
1004
处理器
1006
1014
LCW
1016
解密 LEC
的指令
1018
安全
处理器
1020
安全
存储器
1022
1008
存储器
1010
通信连接
1012
输入 / 输出

图10

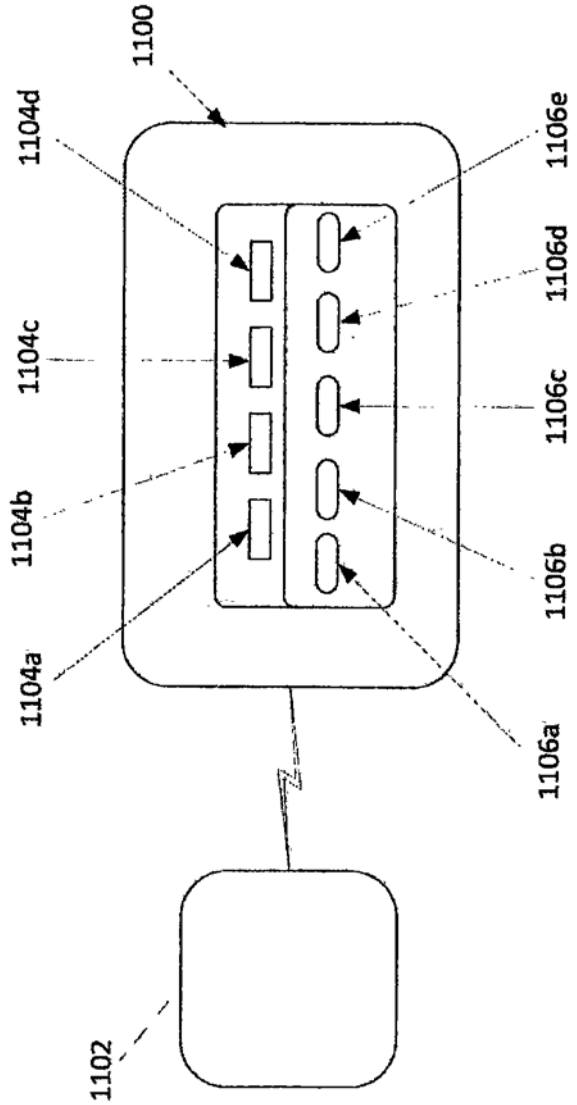

1100
1104d
1106e
1106d
1104c
1106c
1104b
1106b
1104a
1106a
1102

图11

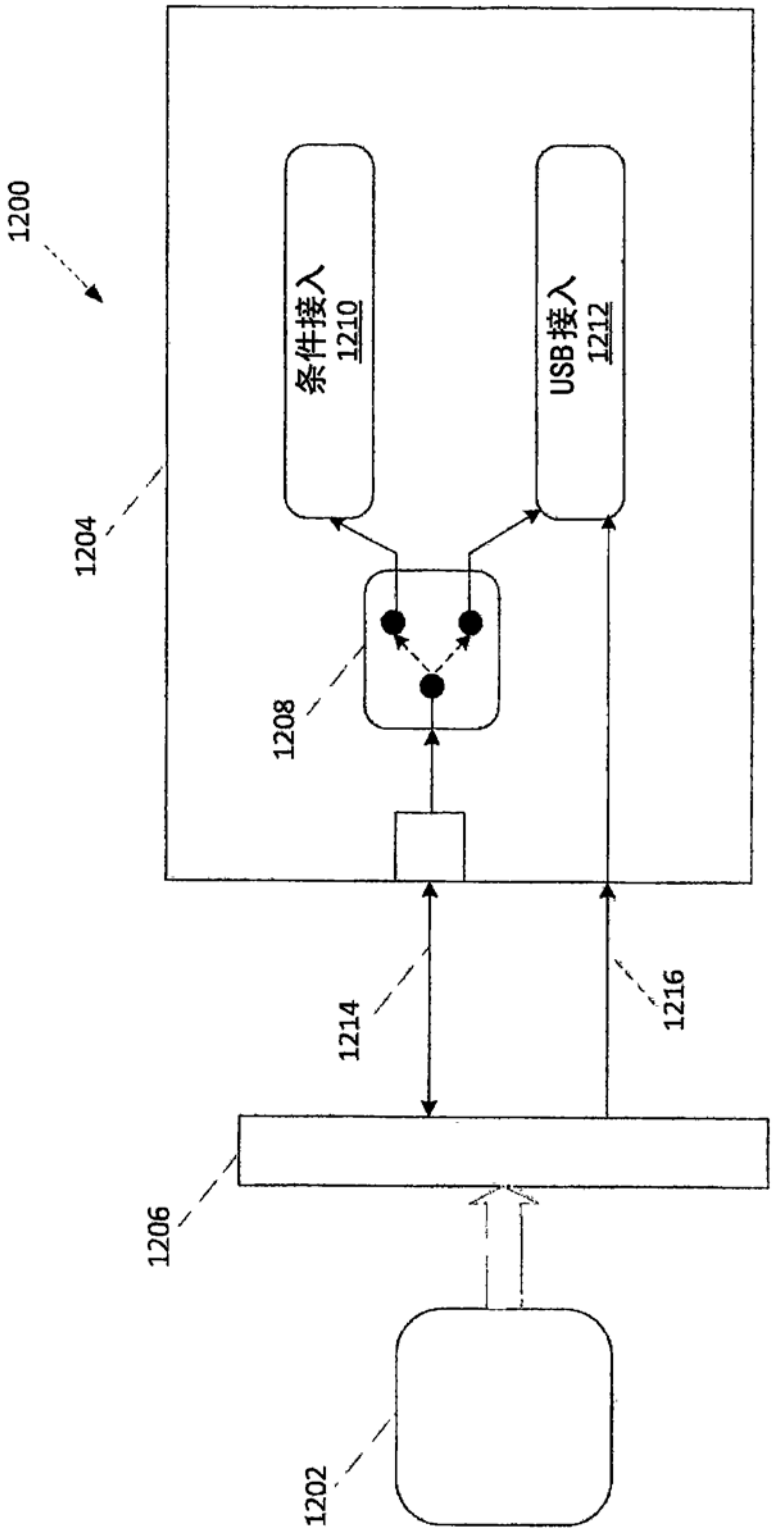


图12

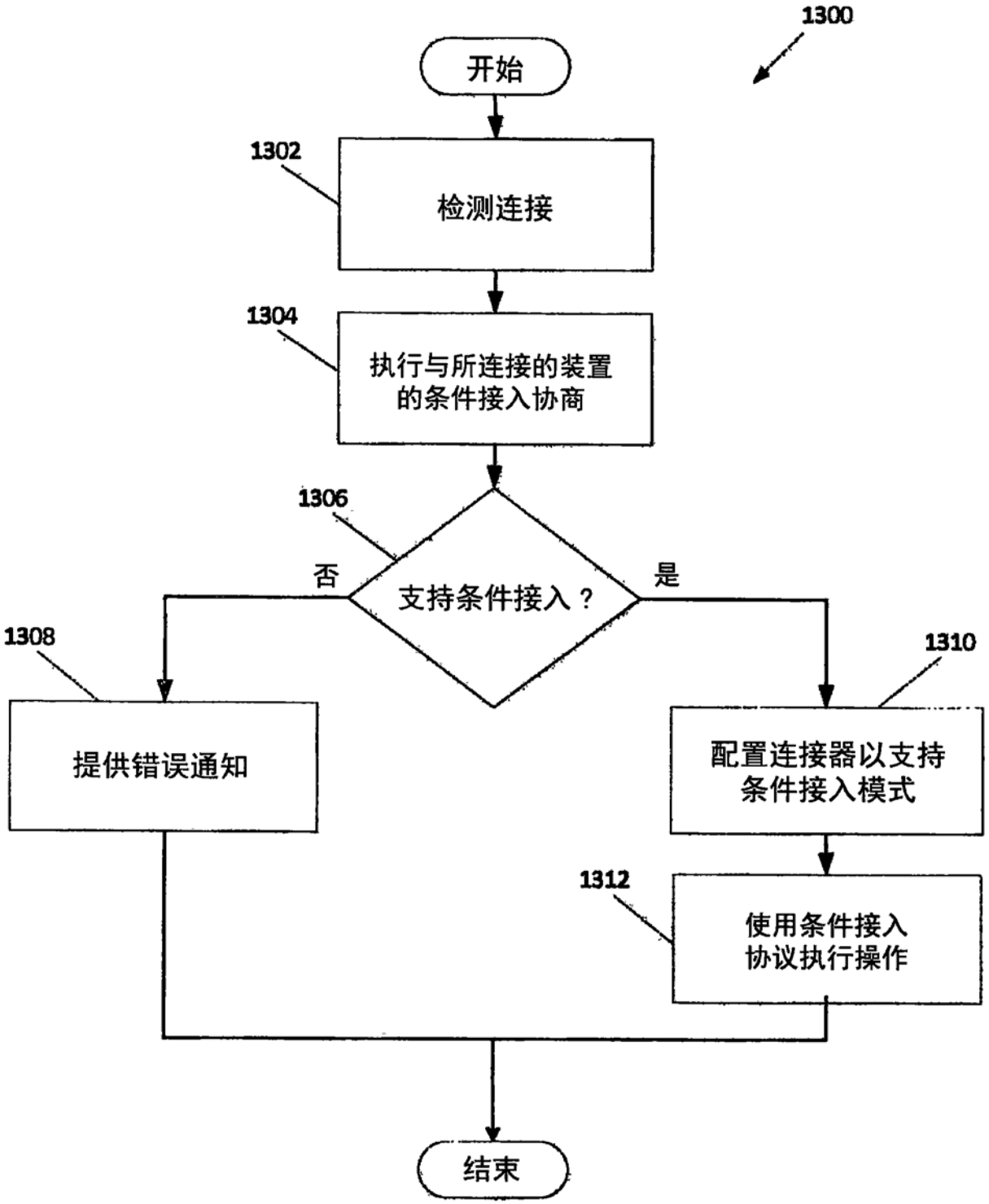

1300
开始
1302
检测连接
1304
执行与所连接的装置的条件接入协商
1306
支持条件接入？
否
是
1308
提供错误通知
1310
配置连接器以支持条件接入模式
1312
使用条件接入协议执行操作
结束

图13

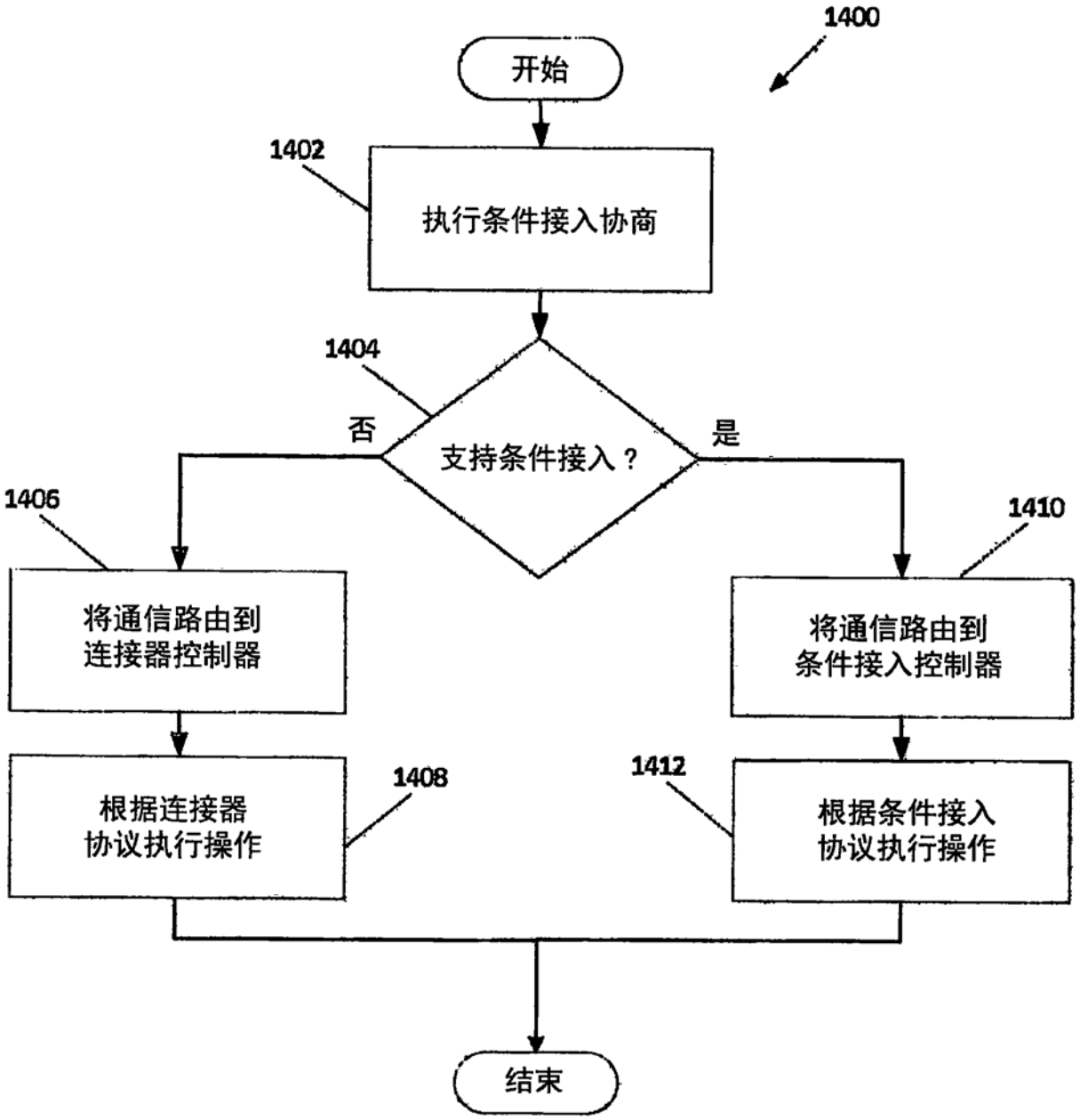

1400
开始
1402
执行条件接入协商
1404
支持条件接入？
否
是
1406
将通信路由到
连接器控制器
1410
将通信路由到
条件接入控制器
1408
根据连接器
协议执行操作
1412
根据条件接入
协议执行操作
结束

图14

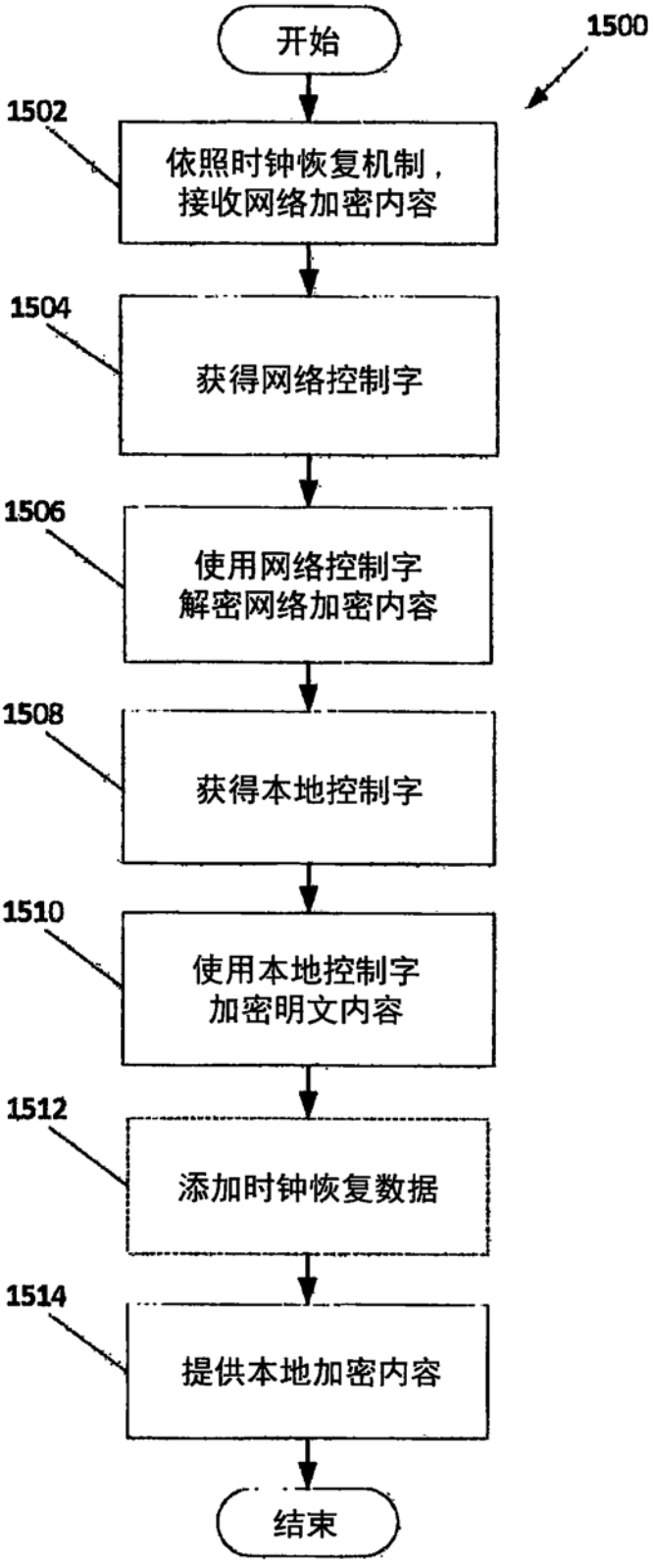

开始
1500
1502
依照时钟恢复机制，
接收网络加密内容
1504
获得网络控制字
1506
使用网络控制字
解密网络加密内容
1508
获得本地控制字
1510
使用本地控制字
加密明文内容
1512
添加时钟恢复数据
1514
提供本地加密内容
结束

图15

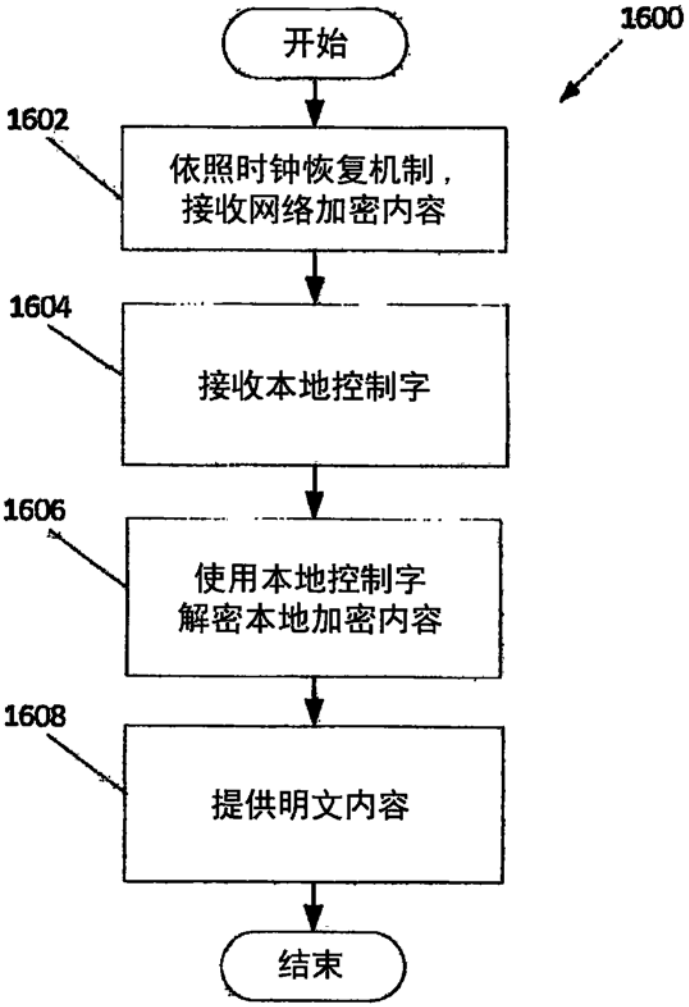

1600
开始
1602
依照时钟恢复机制，
接收网络加密内容
1604
接收本地控制字
1606
使用本地控制字
解密本地加密内容
1608
提供明文内容
结束

图16

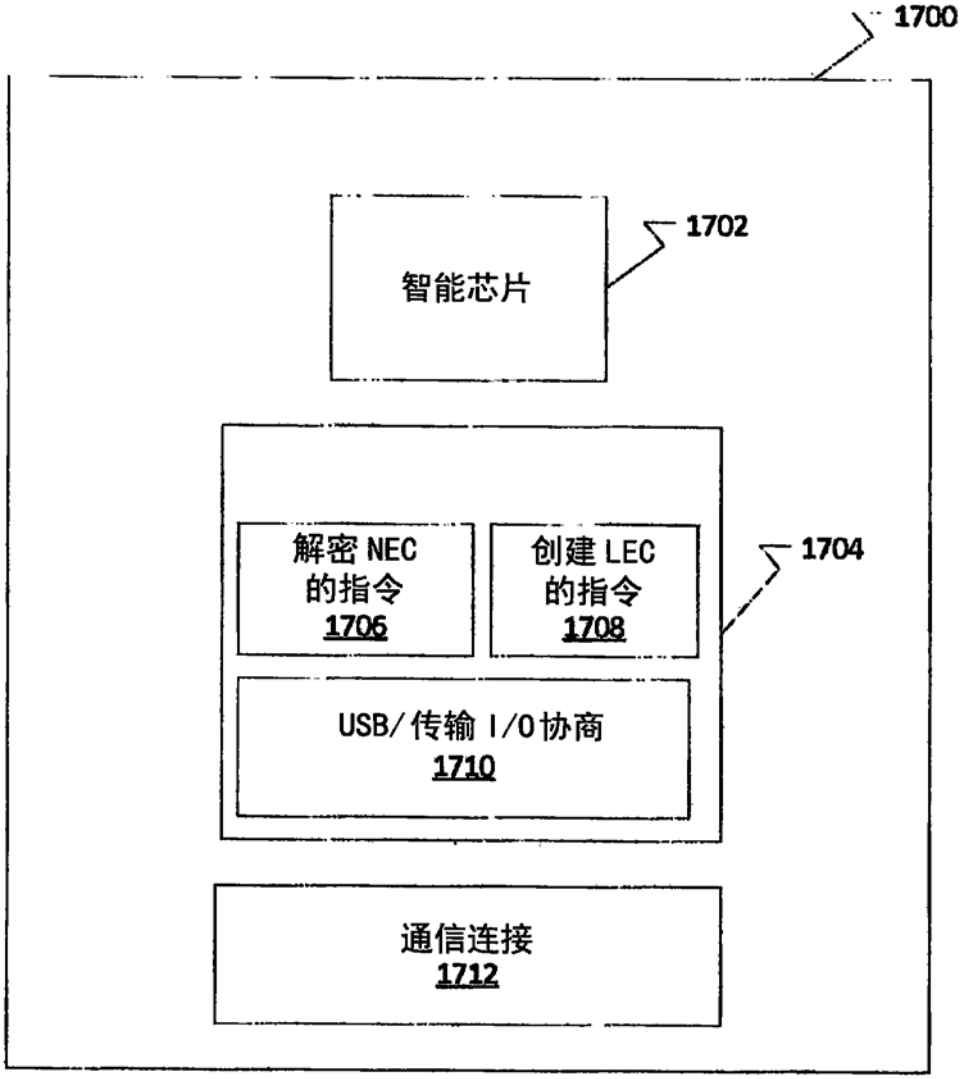

1700
智能芯片
1702
解密 NEC 的指令 1706
创建 LEC 的指令 1708
1704
USB/传输 I/O 协商 1710
通信连接 1712

图17