[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04N 5/00 (2006.01)
G11B 20/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 01810516.5

[45] 授权公告日 2006 年 5 月 24 日

[11] 授权公告号 CN 1257629C

[22] 申请日 2001.3.20 [21] 申请号 01810516.5

[30] 优先权

[32] 2000. 4. 7 [33] US [31] 60/196,009

[32] 2000.10.26 [33] US [31] 09/697,656

[86] 国际申请 PCT/US2001/008832 2001.3.20

[87] 国际公布 WO2001/078075 英 2001.10.18

[85] 进入国家阶段日期 2002.12.2

[71] 专利权人 通用器材公司

地址 美国宾夕法尼亚州

[72] 发明人 E·J·斯普兰克

审查员 王 靖

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 李家麟

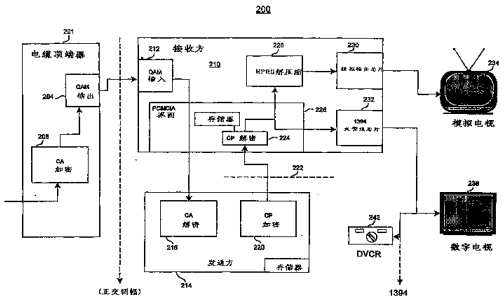
权利要求书 2 页 说明书 7 页 附图 4 页

[54] 发明名称

数据安全传送的方法

[57] 摘要

一种设备和方法被用于通过界面在发送方和接收方之间传送数据。 可向发送方和接收方提供共享密钥、接收方密钥以及发送方密钥。 可将付费下载信息和密钥结合以产生用于通过界面传送的唯一信息。 可在传送的接收端使用相同的输入和相同的算法以验证付费下载信息。 可使用得到的确认付费下载信息与验证付费下载信息来验证付费下载信息。



1．一种通过界面在发送方和接收方之间传送数据的方法，其中，发送方和接收方通过界面通信，该方法包括：

为所述发送方提供共享密钥；

为所述接收方提供所述共享密钥；

为所述接收方提供接收方密钥；

从所述接收方向所述发送方传送所述接收方密钥；

向所述发送方提供发送方密钥；

从所述发送方向所述接收方传送所述发送方密钥；

向所述发送方提供付费下载信息；

在所述发送方至少使用所述共享密钥、所述接收方密钥和所述发送方密钥以产生验证付费下载信息；

通过所述界面从所述发送方向所述接收方传送所述付费下载信息；

通过所述界面从所述发送方向所述接收方传送所述验证付费下载信息；

在所述接收方通过至少使用所述共享密钥、所述接收方密钥和所述发送方密钥来产生确认验证付费下载的信息；

利用所述的验证付费下载信息和所述的确认验证付费下载信息以验证所述的由所述接收方从所述验证付费下载信息获得的付费下载信息，其中，所述接收方通过比较所述确认验证付费下载信息和所述验证付费下载信息以判定所述的验证付费下载信息是否等同于所述的确认验证付费下载信息。

2．权利要求1所述的方法，其特征在于，所述的向所述接收方提供所述接收方密钥，包含在所述接收方产生所述的接收方密钥。

3．权利要求2所述的方法，其特征在于，所述的产生所述接收方密钥，包含利用所述接收方密钥的现时。

4．权利要求2所述的方法，其特征在于，所述向所述发送方传送所述接收方密钥，包含通过所述界面传送所述的接收方密钥。

5．权利要求1所述的方法，其特征在于，所述的向所述发送方提供所述发送方密钥，包含在所述发送方产生所述的发送方密钥。

6．权利要求5所述的方法，其特征在于，所述的产生所述发送方密钥，包含利用所述发送方密钥的现时。

7．权利要求 5 所述的方法，其特征在于，所述向所述接收方传送所述发送方密钥，包含通过所述界面传送所述的发送方密钥。

8．权利要求 1 所述的方法，其特征在于，还包含，与所述接收方密钥一起，从所述接收方向所述发送方传送交易标识符。

9．权利要求 8 所述的方法，其特征在于，所述的产生验证付费信息，包含使用所述的交易标识符。

10．权利要求 1 所述的方法，其特征在于，还包含，与所述发送方密钥一起，从所述发送方向所述接收方传送交易标识符。

11．权利要求 1 中所述的方法，其特征在于，还包含，当交换所述发送方密钥和所述接收方密钥时，确认交易标识符。

12．权利要求 1 所述的方法，其特征在于，还包含利用一交易标识符产生所述的验证付费下载信息。

13．权利要求 1 所述的方法，其特征在于，还包含，至少使用一交易标识符以产生所述的确认验证付费下载信息。

数据安全传送的方法

技术领域

本发明总的来说涉及数据的安全传送。更确切地说，本发明涉及用来在发送单元和接收单元之间建立信息安全交换的系统。

背景技术

在发送方和接收方之间的数据传送中，需要这样一种系统，当发送单元和接收单元还未建立数据可通过它进行传送的安全信道时，该系统可允许安全交易的发生。MENEZES,OORSCHOT,VANSTONE: "Handbook of applied cryptograph（应用密码手册）"CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, US, （离散数学及其应用中的循环冗余码校验公开系列，美国）BOCA RATON, FL, CRC PRESS, 1997, XP002171432, ISBN:0-8493-8523-7 第 400－402 页以及第 497－499 页描绘了在发送方和接收方之间传送数据的不同装置。比如，讨论由对称密钥技术完成的询问响应就如基于(键控的)单向函数的询问响应。D1 还论述了根据对称加密对密钥传输的使用。要分开的安全信道存在经常是困难的。因此，需要这样一种系统，当这样的分开安全信道不存在时，该系统可在发送单元和接收单元之间进行信息的安全交换。

比如，在一种情况中，发送单元需要向接收单元发送管理信息。该管理信息可不需要加密。但是，它可能需要验证。因而，就需要保证，发送的管理信息在其通过传送信道的传送当中没有被，比如攻击者破坏。希望破坏传送信息的攻击者为了破坏数据可以在传送上设置"中间人"的攻击。因此，需要一种防止这种破坏的系统。

发明内容

本发明提供了经过发送单元和接收单元之间界面传送数据的方法和设备。该系统能够为发送方提供共享密钥；为接收方提供共享密钥；为接收方提供接收方密钥；向发送方传送接收方密钥；向发送方提供发送方密钥；向接收方传送发送方密钥；提供付费下载信息；产生至少使用共享密钥、接收方密钥和发送方密钥的验证

付费下载信息；产生确认验证付费下载的信息；以及利用验证的付费下载信息和确认验证的付费下载信息以便验证付费下载的信息。交易的标识符也可与共享密钥、接收方密钥以及发送方密钥一起使用，以产生验证付费下载的信息和确认验证付费下载的信息。

根据本发明，提供一种通过界面在发送方和接收方之间传送数据的方法，其中，发送方和接收方通过界面通信，该方法包括：为所述发送方提供共享密钥；为所述接收方提供所述共享密钥；为所述接收方提供接收方密钥；从所述接收方向所述发送方传送所述接收方密钥；向所述发送方提供发送方密钥；从所述发送方向所述接收方传送所述发送方密钥；向所述发送方提供付费下载信息；在所述发送方至少使用所述共享密钥、所述接收方密钥和所述发送方密钥以产生验证付费下载信息；通过所述界面从所述发送方向所述接收方传送所述付费下载信息；通过所述界面从所述发送方向所述接收方传送所述验证付费下载信息；在所述接收方通过至少使用所述共享密钥、所述接收方密钥和所述发送方密钥来产生确认验证付费下载的信息；利用所述的验证付费下载信息和所述的确认验证付费下载信息以验证所述的由所述接收方从所述验证付费下载信息获得的付费下载信息，其中，所述接收方通过比较所述确认验证付费下载信息和所述验证付费下载信息以判定所述的验证付费下载信息是否等同于所述的确认验证付费下载信息。

本发明的其它特征，对于技术熟练人士来说，从该结合附图的说明书中将变得明显，在其中描绘了实现本发明的某些方法和设备。应该理解的是，本发明并非限制于所揭示的细节，而是包括了处于本发明精神和所附权利要求范围之内的所有变化和修改。

附图说明

图 1a、1b 和 1c 描绘了实现本发明一个实施例的流程图。

图 2 描绘了实现本发明一个实施例的电路。

具体实施方式

通过界面传送数据的方法总的来说，可描述为在发送方和接收方之间建立界面，并为发送方和接收方提供共享密钥。接收方也被提供接收方密钥，而发送方也被提供发送方密钥。接收方和发送方交换他们各自的密钥；从而，发送方获得了接收方密钥，而接收方获得了发送方密钥。随后提供付费下载信息，也就是，需要验

证的信息。验证付费下载的信息至少使用共享密钥、接收方密钥以及发送方密钥产生。同时产生确认验证付费下载的信息。最后，利用验证付费下载信息和确认验证付费下载的信息以验证原始的付费下载信息。

现在参考图 1a、1b 和 1c 中的流程图 100，可以看到实现本发明一个实施例的方法。在框 104 中，发送方被提供共享密钥。“发送方”被当作是通过通讯信道广播或发送诸如二进制数据流之类的信号的发送单元，比如发送器。共享密钥经常是保密密钥。也就是说，“共享密钥”是由发送方和接收方共同拥有用于建立验证交易的密钥；但是，并不一定局限于这样的应用。比如，它可以是在发送方和接收方之间交换作为另一处理的一部分的密钥，该处理诸如加密/解密处理。因此，发送方和接收方都将具有共享密钥的复制。具有共享密钥的接收方反映在框 108 中。“接收方”被当作是能够接收发送单元经通讯信道所发送信号的接收单元。在框 112 中，产生接收方密钥。“接收方密钥”是产生于界面接收端上的密钥。接收方密钥的一个例子是“现时”。现时是产生的号码，比如随机产生的号码，它只在系统中用一次。现时非常有用，因为它们可被用于防止“重演”的攻击。因此，如果在接收方和发送方之间使用一次现时，则若再次为现时使用相同的号码，接收方和发送方将意识到重演的攻击。在框 116 中，接收方密钥被存储在，比如，接收方的存储器中。如果现时被用于接收方密钥和发送方密钥，它们可分别被称为接收现时和发送现时。另外，如果现时必须随机产生，这样的接收方密钥可被称为接收方随机号码现时。

在框 120 中，产生了交易标识符。交易标识符识别发送方和接收方之间信息交换的处理。由此，发送方和接收方将交易标识符与发送方和接收方之间交换的信息进行结合，从而识别被交换信息的目的。在特定的相关处理中，交易标识符将识别正在进行的验证交易。因此，在框 124 中，在交易标识符被产生之后，它可被存储在，比如接收方。在框 128 中，先前产生的接收方密钥被传送给发送方。较佳地，该发送的发生是通过将接收方密钥与交易标识符一起通过界面传送给发送方，如框 128 和 132 所描绘的。以这种方式，交易标识符可与接收方密钥结合，从而发送方将确认传送的目的。

在图 1b 的框 136 中，已向发送方发送或传送的接收方密钥被存储在发送方。在框 140 中，在接收方产生的交易标识符也被存储在发送方。

通常在如框 144、148、152 和 156 所示的发送方密钥的产生中重复处理。“发送方密钥”是在界面的发送方一侧产生的密钥。由此，发送方密钥如 144

中所示地产生。再次，发送方密钥可以为随机的号码现时，以防止在发送方密钥的交换中发生的重演攻击。在框 148 中，发送方密钥被存储在发送方。随后，发送方密钥可如 152 所示地被传送给接收方。如前面所述的，可通过使用交易标识符完成在发送方和接收方之间的信息交换，其中的交易标识符附着于发送方和接收方之间交换的信息。这如框 156 所示。

在框 160 中，将与发送方密钥一起传送的交易标识符的值与同接收方密钥一起发送的交易标识符的存储值进行比较。如果比较确认，交易标识符与存储值一样，则处理继续。但是，如果交易标识符发送变化，则作为验证步骤的一部分，数据不予处理。这如框 164 所示。如框 168 所示，如果交易标识符被确认，则发送方密钥可随后被存储在接收方的接收方存储器中。

框 172 展示了付费下载信息的形成。付费下载信息是将由发送方发送并得到验证的相关的信息。因此，它是使验证步骤成为必要的的信息。付费下载信息的例子是表示对于 MPEG 编码数据流四种不同级别版权保护的两比特信息包。验证是指由用户或信息来源证明他拥有此权利的过程。因此，验证允许诸如付费下载信息的信息就其来源得到确认。

在框 176 中，形成了验证付费下载信息。验证付费下载信息是被比如，由接收方使用以验证由发送方发送的付费下载信息的信息。验证付费下载信息通过使用由发送方和接收方共同拥有的数据值来形成。例如，验证付费下载信息可通过使用共享密钥、发送方密钥以及接收方密钥来形成。另外，也可使用交易标识符和/或附加的数据值来产生验证付费下载信息。通过在附加数据集上附加这些不同的密钥和/或标识符并完成散列算法，可导出独一无二的验证付费下载信息。使用哪一种算法散列数据字段并不是重要的。预计，可使用任何根据唯一数据输入产生唯一结果的算法。

如框 180 所示，付费下载信息从发送方通过界面被传送给接收方。“界面”被当作是两台设备之间分界的物理点。因此，有界面的接收方一端和界面的发送方一端。在框 182 中在接收方存储了该付费下载信息。在图 1c 的框 184 中，验证付费下载信息被传送给接收方。验证付费下载信息随后如框 186 所示地被存储在接收方。另外，交易标识符可如框 188 中所示地，与验证付费下载信息一起传送。如框 190 所示，再次在由接收方存储的交易标识符的值和与验证付费下载信息一起传送的交易标识符的值之间进行比较。如果交易标识符与先前发送的值不匹配，则如框 192 所示，验证付费下载信息不予处理。

在框 194 中，产生了确认验证付费下载的信息。该确认验证付费下载的信息是使用与在验证付费下载信息的产生中使用的相同信息或数据值在界面的接收方一端产生的。因此，例如，确认验证付费下载的信息通过接收方使用共享密钥、接收方密钥和发送方密钥来产生。或者，如果交易标识符被用于产生验证付费下载信息，它也将被使用以产生确认验证付费下载的信息。如被用于产生验证付费下载信息一样，使用相同的算法以产生确认验证付费下载的信息。因此，使用与验证付费下载信息相同信息的确认验证付费下载的信息应与验证付费下载信息等同。为了判定它们是否等同，如框 196 所示，确认验证付费下载的信息与验证付费下载信息进行比较。在框 197 中进行这样的测试以判定两个值的等同性。如果两个值不等同，则如框 198 所示地放弃处理。但是，如果确认验证付费下载的信息等同于验证付费下载信息，则验证是完整的或被完成，且可如框 199 所示地可使用付费下载信息。

图 2 展示了图 1a、图 1b 和图 1c 所示方法的实际例子。在电缆电视的行业中，包含置顶盒部件和集成为单独芯片的电缆系统可调存取系统部件的置顶盒已被使用。但是，1996 年的电缆法和 1998 年的 FCC 细则及规则要求，导航设备要通过将安全功能分成单独的模块来面对竞争。因此现在，在置顶盒的可调存取系统和置顶盒的其它部分之间有一个信道，该信道面对着被那些希望获得电缆传送内容的人的攻击。图 2 显示了利用图 1a、图 1b 和图 1c 中所描述方法的实现。在电路 200 中，电缆头端 201 获得由电缆存取加密系统 208 加密的输入信号。该加密信号被随后发送至正交调幅输出 204。QAM 输出信号被传送到置顶盒接收方 210 的 QAM 输入 212。一旦接收到，该信号就通过界面 222 被发送到发送方 214。在发送方，可调存取信息在框 216 中解密。发送方 214 也包含版权保护加密单元 220 和存储器 222。可调存取信息的一个方面是版权保护的信息。例如，电缆头端可表示对于特定电缆节目可被允许复制的级别。因此，如果节目是非常有价值的，则它可具有表示不允许在置顶盒复制的版权保护。另外，如果节目没有价值，则版权保护信息可表示，置顶盒自由地多次复制节目。作为另一个可替换实施例，版权保护信息可表示，允许一个附加的复制由置顶盒产生。因此，这便促使将节目从置顶盒分配到一个以上的设备。因此，节目的版权保护信息可包含在少到一比特或两比特之中。

版权包含信息，也被称为 CCI 信息，需要通过界面 222 被传送到置顶盒。发送方 214 和接收方 210 之间的界面是暴露在外的，因此在发送 CCI 信息当中

需要验证的级别。攻击者可能试图改变 CCI 信息，从而使置顶盒产生多重复制的有价值节目。因此，CCI 信息应该被验证以保证，攻击者不会将 CCI 信息破坏到保护的较低级别。可使用以上在流程图 100 中描述的方法以完成该任务。也就是说，发送方和接收方将从较早的交易共享加密/解密密钥，在该交易中，这种密钥被存储在接收方和发送方。因而，它们都有共享密钥的复制。另外，如上所述，它们可交换现时以防止重演的攻击。随后，可将 CCI 信息用作付费下载信息，同时可使用共享密钥、接收方密钥和发送方密钥以实现散列算法。一旦付费下载数据被验证，则在框 224 中，在接收方 210 解密版权保护信息。版权保护信息被解密后，节目信号可被分配到端用户设备。由此，在框 228 中，可完成 MPEG 信号的解压缩并将其输送至不同的换能器芯片。例如，为了产生与模拟电视兼容的信号，可将模拟输出芯片 230 用作端用户设备 234。另外，如果数字电视 238 是端用户设备，则 MPEG 信号可被发送到 1394 火警线芯片 232。这种情况对于数字 VCR242 也是一样的，如图 2 所示。

虽然已将本发明的多种实施例作为实现本发明的方法或设备进行了描述。应该理解的是，本发明可通过结合于计算机的码，比如，在计算机上的码或可由计算机进行存取的码，来实现。例如，可使用软件以实现许多上述的方法。从而，除了发明由硬件完成的实施例之外，还应该指出的是，这些实施例可利用产品来完成，该产品包含计算机可用媒质，该媒质具有结合在其中的计算机可读程序码，该程序码产生本说明书中所述的功能的启动。因此，需要以上所表示的实施例被认为也可以它们的程序码装置为形式被该专利保护。

同样可以预计的是，本发明的实施例可作为结合在载波中的计算机信号来完成，也可以作为在传送媒质中传播的信号(例如，电的和光的)来完成。由此，上述的多种信息可以诸如数据结构的结构被格式化，并通过传送媒质作为电信号被传送或存储在计算机可读媒质上。

还要指出的是，此处所述的许多结构和效果可分别作为用于完成功能的装置或完成功能的步骤来叙述。因此，应该理解的是，这样的语言有权覆盖所有在本说明书及其等效文件中所披露的这样的结构或效果，包括通过参考结合的内容。

我们认为，本发明实施例的设备和方法以及伴随其的优点都将从该说明书中被理解，且明显的是，在不脱离本发明精神和范围或牺牲其所有实质优点的前提下，可在有关部件的形式、结构和配置作出不同的变化，此处在被描述前

的形式仅仅是本发明的典型实施例。

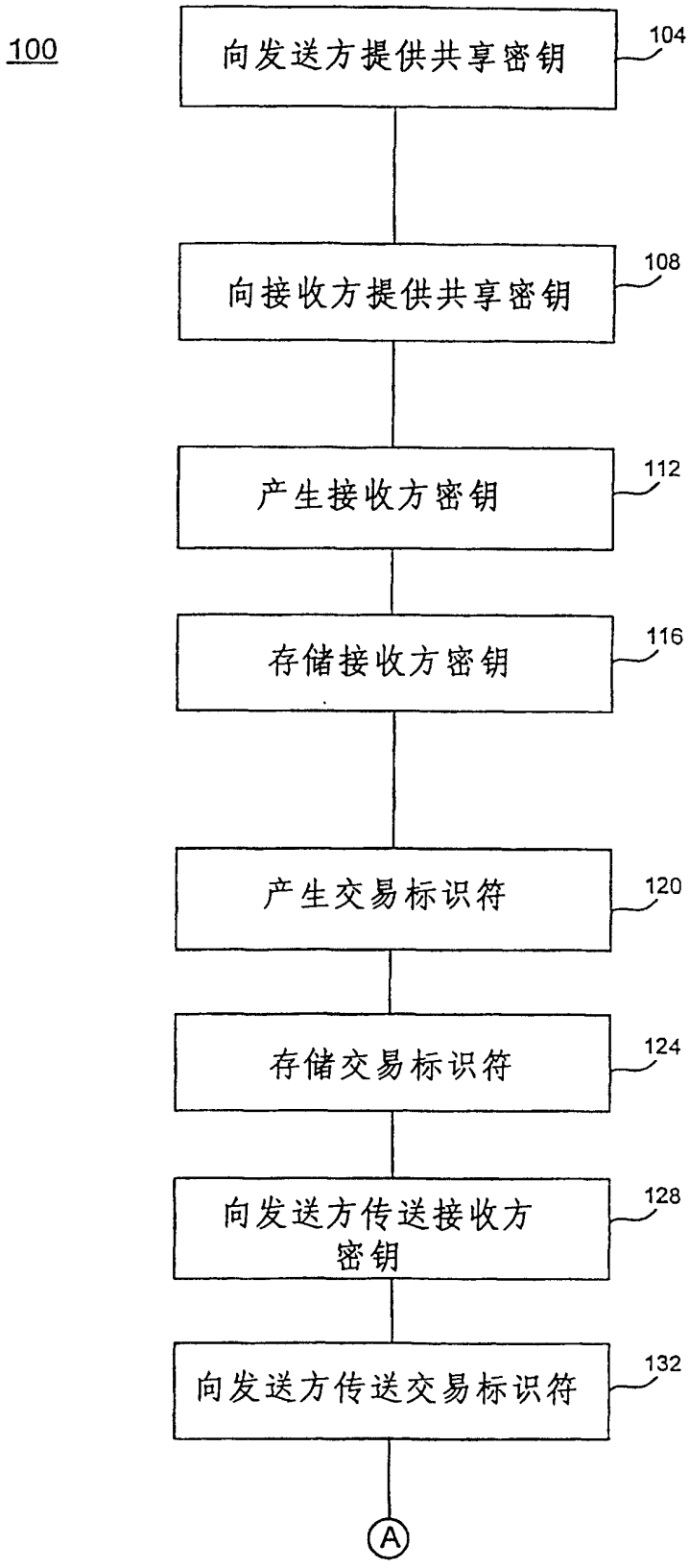

100
向发送方提供共享密钥
104
向接收方提供共享密钥
108
产生接收方密钥
112
存储接收方密钥
116
产生交易标识符
120
存储交易标识符
124
向发送方传送接收方密钥
128
向发送方传送交易标识符
132
A

图 1a

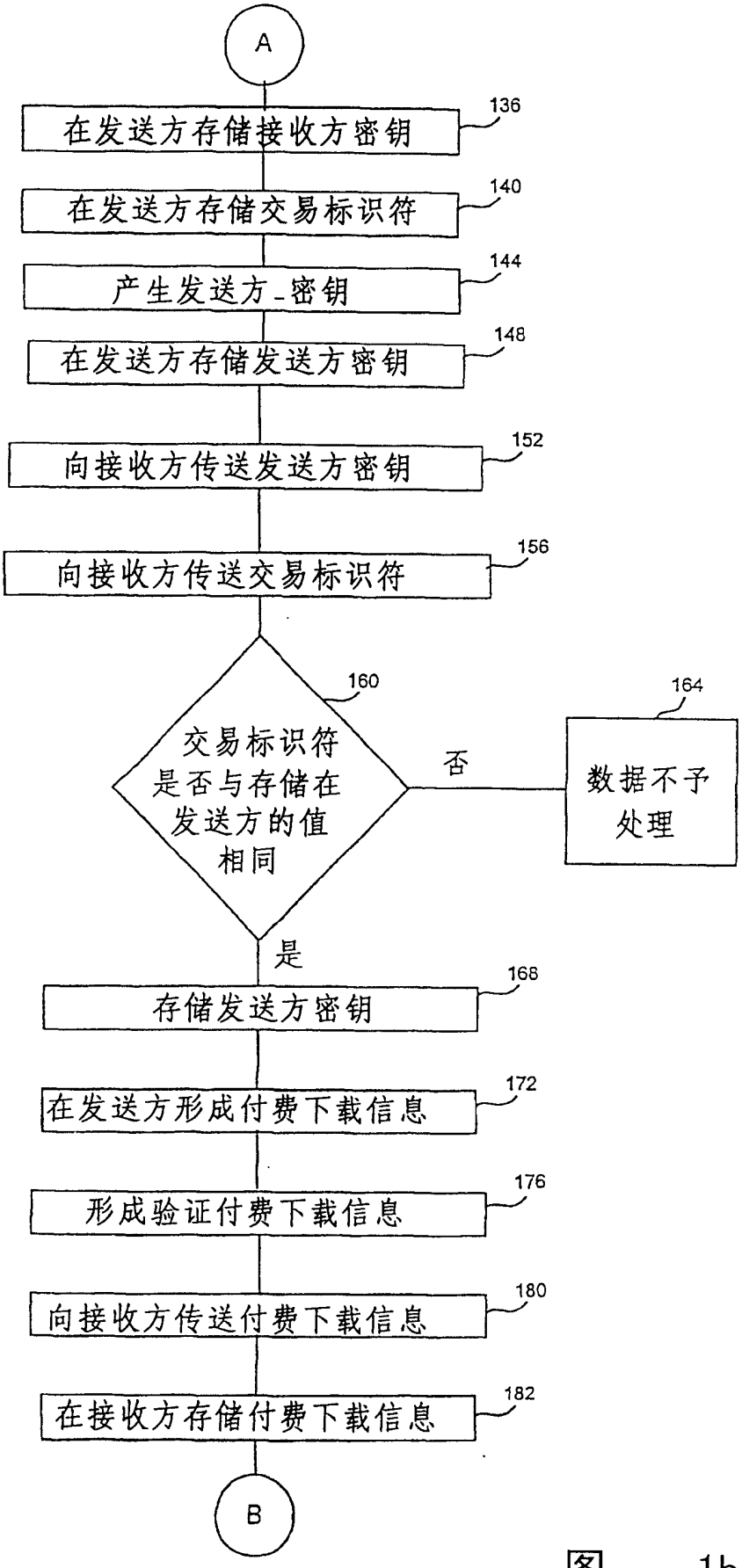

A
在发送方存储接收方密钥
136
在发送方存储交易标识符
140
产生发送方_密钥
144
在发送方存储发送方密钥
148
向接收方传送发送方密钥
152
向接收方传送交易标识符
156
交易标识符是否与存储在发送方的值相同
160
否
数据不予处理
164
是
存储发送方密钥
168
在发送方形成付费下载信息
172
形成验证付费下载信息
176
向接收方传送付费下载信息
180
在接收方存储付费下载信息
182
B

图 1b

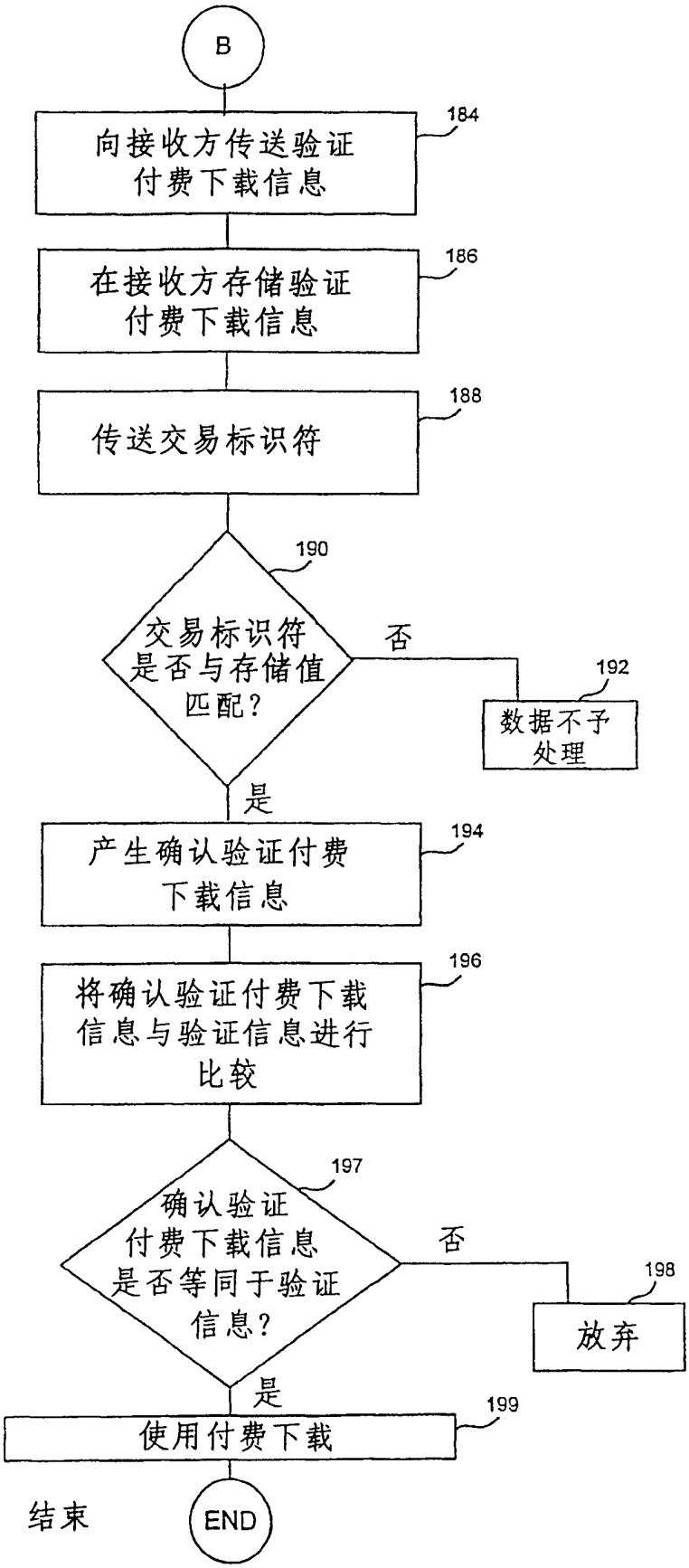

B
向接收方传送验证付费下载信息
184
在接收方存储验证付费下载信息
186
传送交易标识符
188
交易标识符是否与存储值匹配？
190
否
192
数据不予处理
是
产生确认验证付费下载信息
194
将确认验证付费下载信息与验证信息进行比较
196
确认验证付费下载信息是否等同于验证信息？
197
否
198
放弃
是
使用付费下载
199
结束
END

图 1c

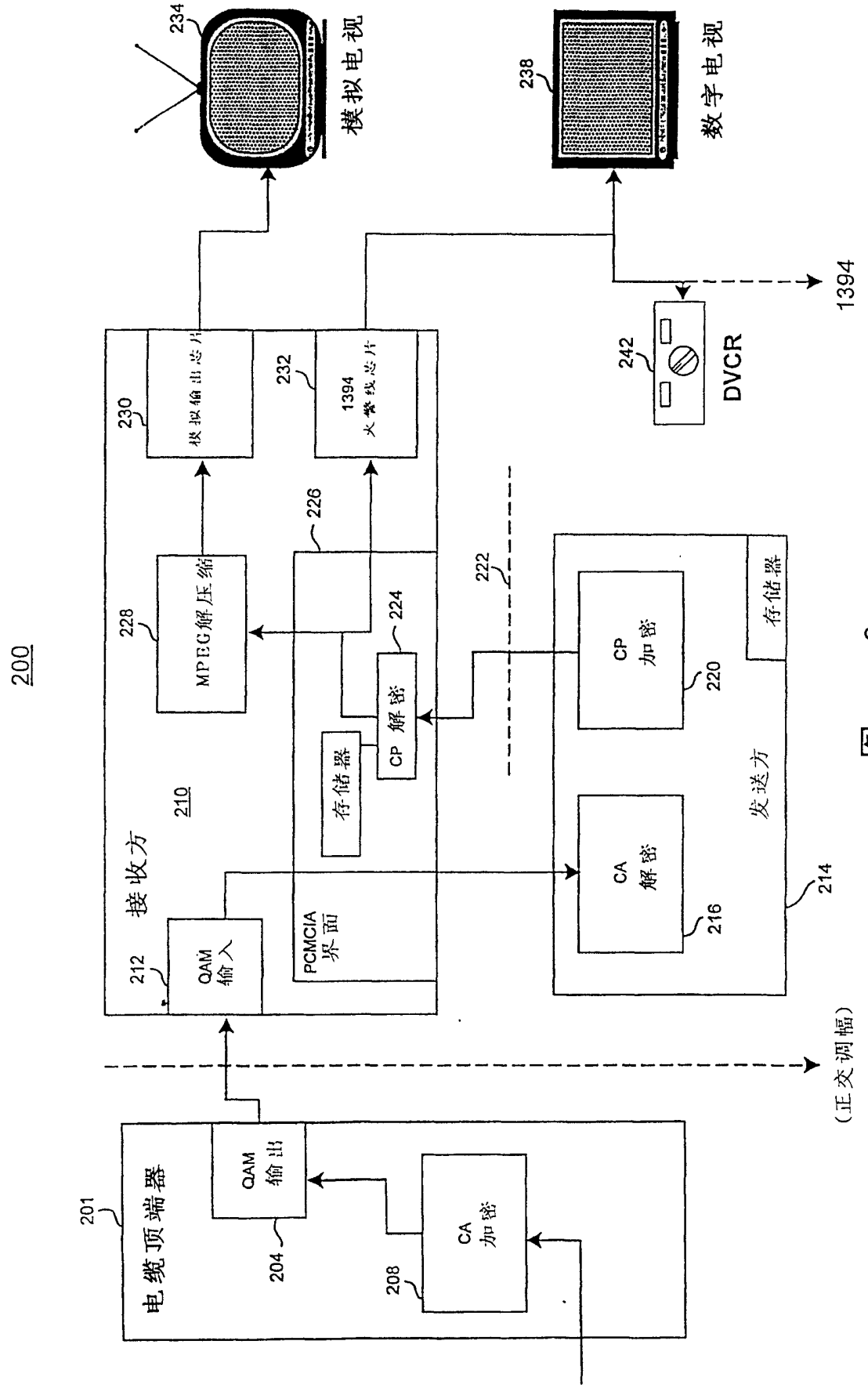

200
电缆顶端器
201
QAM 输出
204
CA 加密
208
(正交调幅)
接收方
210
QAM 输入
212
PCMCIA 界面
存储器
CP 解密
224
MPEG解压缩
228
226
222
230
232
1394
234
模拟电视
238
数字电视
242
DVCR
1394
发送方
CP 加密
220
CA 解密
216
214
存储器

图 2