[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 7/167 (2006.01)
H04N 7/16 (2006.01)
H04N 5/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 00814503.2

[45] 授权公告日 2008 年 8 月 6 日

[11] 授权公告号 CN 100409685C

[22] 申请日 2000.10.19 [21] 申请号 00814503.2

[30] 优先权

[32] 1999.10.19 [33] US [31] 60/160355

[86] 国际申请 PCT/US2000/028942 2000.10.19

[87] 国际公布 WO2001/030083 英 2001.4.26

[85] 进入国家阶段日期 2002.4.18

[73] 专利权人 汤姆森许可公司

地址 法国布洛涅

[72] 发明人 D·J·杜菲尔德 M·S·戴斯

[56] 参考文献

WO9907150A1 1999.2.11

EP0858184A2 1998.8.12

US5420866A 1995.5.30

WO9922372A1 1999.5.6

审查员 龚锦玲

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 陈景峻 陈 霁

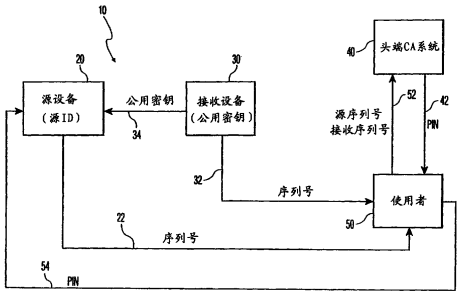
权利要求书 4 页 说明书 5 页 附图 2 页

[54] 发明名称

用于通信保护内容的验证权限的系统和方法

[57] 摘要

在一个条件访问系统中，使用标识代码对许可一个源设备传送不同的保护内容到一个接收设备进行验证的方法。



1. 一种用于验证一个与接收设备耦合的源设备被许可传送被保护的内容到该接收设备的方法，包括:

在所述源设备上接收一个认可代码，该认可代码是通过使用分别跟所述源设备和接收设备相关联的数据来确定的;

使用分别跟所述源设备和接收设备相关联的数据在所述源设备中确定一个本地代码; 和

对所述认可代码和所述本地代码进行比较，由此所述源设备响应于所述比较结果，而对将所述被保护的内容传送给所述接收设备的许可进行验证。

2. 按照权利要求 1 的方法，其中使用和所述源设备唯一相关联的识别符、基于一个散列计算来确定所述认可代码，以及使用来自所述接收设备的数据和预先存储在所述源设备中的所述识别符、基于一个散列计算来确定所述本地代码。

3. 按照权利要求 2 的方法，其中用于确定所述本地代码的、和所述源设备相关联的所述数据不是公用信息，而其中用于确定所述本地代码的、和所述接收设备相关联的所述数据是公用信息。

4. 按照权利要求 2 的方法，其中所述识别符是序列号或一个使用者可访问的其它的识别码，而其中在所述散列计算中使用的、来自所述接收设备的所述数据是一个公用密钥。

5. 权利要求 1 的方法，进一步包括所述源设备延迟对所述比较的认可，并响应于该认可而将所述源设备是否被许可提供所述内容给所述接收设备的信息传送给一个使用者。

6. 一种用于验证一个与接收设备耦合的源设备被许可传送被保护的内容到该接收设备的方法，包括:

提供唯一的、跟所述源设备和接收设备相关联的识别符给一个验证权限机构;

从所述验证权限机构接收一个认可代码，所述认可代码通过使用相应于所述识别符的数据被确定;

使用跟所述源设备和接收设备相关联的数据在所述源设备中确定一个本地代码; 和

对所述认可代码和所述本地代码进行比较，由此所述源设备响应于所述比较结果，而对将所述被保护的内容传送给所述接收设备的许可进行验证。

7. 权利要求 6 的方法，进一步包括所述验证权限机构把所述认可代码提供给一个使用者，和所述使用者把所述认可代码提供给所述源设备。

8. 权利要求 6 的方法，其中由所述使用者把所述唯一的识别符提供给所述验证权限机构。

9. 权利要求 6 的方法，其中所述源设备是从一个访问设备和一个媒体播放机中选择的一个，而其中所述接收设备是一个数字电视。

10. 权利要求 6 的方法，其中和所述源设备相关联的所述数据是保密的以致于不易被使用者发现。

11. 权利要求 6 的方法，其中跟所述源设备和接收设备相关联的所述数据包括指示所述源设备的一个唯一的标识和跟所述接收设备相关联的一个公用加密密钥。

12. 权利要求 11 的方法，其中指示所述源设备的所述唯一的标识对于所述源设备的一个使用者是保密的。

13. 一种处理用于访问被保护内容的至少一个安全密钥和至少一个识别符的方法，所述方法包括:

在源设备上与所述内容一起接收多个安全密钥;

在所述跟一个接收设备耦合的源设备上接收被用于提供所述内容到该接收设备的所述识别符，所述识别符与所述接收设备相关联;

使用所述源设备选择所述多个安全密钥的其中之一; 和

使用所述源设备和选择的安全密钥把所述内容提供给所述接收设备。

14. 按照权利要求 13 的方法，进一步包括把用于访问所述内容的指示所述接收设备的一个序列标识提供给一个验证权限机构。

15. 按照权利要求 14 的方法，进一步包括使用所述序列标识确定和所述接收设备相关联的一个识别符。

16. 权利要求 13 的方法，其中所述多个安全密钥被索引在密钥的一个表中，以及所述识别符是密钥表中的一个选择密钥和所述识别符的一个散列函数的结果的索引。

17. 一种通过使用一个验证权限机构来验证具有唯一识别符和序列号的并与接收设备耦合的源设备和具有唯一密钥和序列号的接收设备应当可访问内容的方法，其中所述唯一的识别符被保密而不被所述源设备的一个使用者访问，所述方法包括:

把所述序列号提供给所述验证权限机构;

所述验证权限机构使用所述序列号来确定所述唯一的识别符；和，如果访问所述内容是被许可的，

所述验证权限机构使用所述唯一的识别符来确定一个许可识别符;

所述源设备使用所述唯一的识别符来确定一个本地识别符；和

如果所述许可识别符和本地识别符彼此相对应，则证实所述源设备和接收设备应当可访问该内容。

18. 权利要求 17 的方法，进一步包括所述验证权限机构提供所述许可识别符的所述至少一部分给一个使用者，和所述使用者提供所述许可识别符给所述源设备。

19. 一种验证一个与数字电视耦合的置顶盒被许可传送被保护的内容到该数字电视的方法，包括:

在所述置顶盒上接收一个认可代码，该认可代码是通过使用分别跟所述置顶盒和所述数字电视相关联的数据来确定的;

使用跟所述置顶盒和所述数字电视相关联的数据在所述置顶盒中确定一个本地代码；和

对所述认可代码和所述本地代码进行比较，由此所述置顶盒响应于所述比较结果，而对将所述被保护的内容传送给所述数字电视的许可进行验证。

20. 权利要求 19 的方法，其中使用置顶盒和数字电视的各自的序列号产生认可代码。

21. 一种验证一个与数字电视耦合的数字视频记录器被许可来传送被保护的内容到该数字电视的方法，包括:

在所述数字视频记录器上接收一个认可代码，该认可代码是通过使用分别跟所述数字视频记录器和所述数字电视相关联的数据来确定的;

使用跟所述数字视频记录器和所述数字电视相关联的数据在所述数字视频记录器中确定一个本地代码；和

对所述认可代码和所述本地代码进行比较，由此所述数字视频记录器响应于所述比较结果，而对将所述被保护的内容传送给所述数字电视的许可进行验证。

22. 权利要求 21 的方法，其中使用数字视频记录器和数字电视的各自的序列号产生认可代码。

用于通信保护内容的验证权限的系统和方法

技术领域

本发明一般涉及数字音频/视频传输系统，并尤其涉及用于鉴别访问不同保护内容的一种方法和系统。

背景技术

在整个传输和存储过程中，扩展的条件访问（XCA）是用于保护数字编码的音频/视频（A/V）内容的一个系统。根据 XCA 系统，经济价值的内容被扰乱，或被加密，以防止无权限的访问。XCA 允许记录扰乱的内容，但不允许对不合法的内容进行解密。合法的内容例如是原始的或者由版权拥有者另外授权的。当然，去扰乱涉及解密的处理。由于没有合法的内容不被扰乱，因而不能观看它。

XCA 体系结构一个明显的特点是条件访问（CA）和本地保护的概念。CA 指定访问保护的内容，比如编程。可移动的安全设备执行相关的安全功能。是用一个 CA 业务输送经济价值的内容。例如，数字卫星扰乱视频内容并去扰乱密钥来大批分布给他们的用户。一些用户可以决定购买该内容，在此情况下，他们被提供所需的密钥以恢复/获得去扰乱的密钥。那些没有选择购买该内容的用户不被提供访问这些密钥。在 XCA 术语中，这是 CA 的处理。

XCA 系统使用一个返回信道接收本地密钥的鉴别并对用于访问内容的本地密钥进行识别。这就产生了一个问题，某些类别的方法中，多数设备需要具有一个返回路径来作出这种工作。

需要一种改进的方法，用于在 XCA 中和进行条件访问的其他的系统中，鉴别用于访问不同保护内容的密钥和识别符。

发明内容

一种方法，用于在一个条件访问系统中，对批准一个源设备通信不同的保护内容（例如，扰乱业务）到一个接收设备进行验证，该方法包括：提供有关源和接收设备的充分唯一的识别符给一个验证权限机构。验证权限机构使用有关源和接收设备的数据确定一个认可代码，

该数据相应于通信的识别符；和，源设备使用有关源和接收设备的数据确定一个本地代码，并让至少一部分的认可代码与至少一部分的本地代码相比较，以便验证源设备被批准通信该内容到接收设备。

附图说明

图 1 示例了按照本发明一个方面的一个系统；和

图 2 示例了按照本发明第二个方面的一个系统。

具体实施方式

按照本发明，在一个 XCA 系统中设备的一个拥有者，或使用者或操作者作为一个可行返回路径的一部分。然而，当利用一个设备的操作者作为一个返回信道时会出现一个主要的问题。不能期望一个使用者精确的读取或输入一个 768-比特数。但是，需要大数目来防止强行密码分析的攻击，即对每种可能的特征符进行尝试直到一个工作过程完成。问题是对有效的接收的讯息即公用密钥进行验证。使用这种做法的证书或签名典型的是至少 20 比特长度，并通常接近 100 比特。特征符必须具有足够可能的价值以使不易受到强行攻击。按照本发明，用一种最小的密钥空间完成相同的目的，通过限制能被用于作出强行攻击的资源。

图 1 示例了用于批准访问不同保护内容的一个系统 10。系统 10 包括具有一个相关识别符（源 ID）的一个源设备 20，具有一个相关数字密钥（公用密钥）的一个接收设备，源设备 20 的一个使用者或操作者，和一个头端 CA，委托第三方（TTP），系统 40。

源设备 20 可以采取一个访问设备的形式，比如一个卫星置顶盒（STB）或媒体播放机，比如数字视频录像（DVHS）播放机或数字光盘（DVD）播放机，同时接收设备可以采取一个数字电视（DTV）的形式。按照本发明的另一个方面，源设备 20 和接收设备 30 具有公共可访问的序列号。

通常，为了保护从源设备 20 到接收设备 30 传输的内容以使它不致于被非法复制或其他不正当的使用，接收设备 30 的公用密钥被传送到源设备 20。使用接收设备 30 的公用密钥扰乱由源设备 20 提供的的内容，并以扰乱的形式发送到接收设备 30。接收设备使用相应的私人密钥解除扰乱的内容并使它能经接收设备 30 适当地显示。此外，使用

两个阶段处理也可以完成上述的实现方式，其中使用一种对称算法扰乱内容，并使用公用密钥发送用于这种扰乱的控制字。

使用设备的序列号，通过TTP分别确定接收和源设备30，20的公用密钥和源 ID。然后由设备 20，30 和 TTP 单独使用确定的公用密钥和源 ID，以便验证设备20，30可以结合访问该内容进行操作。

使用者 50 分别从的源和接收设备 20，30 获得序列号（例如，通过从设备读取它们），并呼叫头端 CA 系统以使源和接收设备 20，30 能够结合使用。经通信 52 使用者 50 把这些序列号提供给头端 CA 系统。例如，这些序列号能以一种语音通信或电子的形式，或听觉上的。头端 CA 系统必须访问一个数据库，把提供的序列号转换成源 ID 和公用密钥数据。因此，头端 CA 系统从这些通信的序列号中可以识别源设备 20 和接收设备 30 的源 ID 和公用密钥，例如通过使用查找。按照本发明的另一个方面，重要的是，序列号和源 ID 之间的关系不是公共的，并不容易被确定。

在图 1 中，头端 CA 系统 40 计算这两个值的一个散列码，例如，源 ID 和公用密钥作为一种许可散列计算，并把它提供给使用者 50 作为一个个人识别号（PIN）（如通信 42 所示）。使用者 50 然后输入该 PIN 进入源设备 20（如通信 54 所示），已经计算了相同的散列，例如作为一个本地散列计算，使用驻留在源设备 20 中的源 ID 和由接收设备 30 提供的公用密钥（如通信 34 所示）。如果 PIN 匹配该散列，则源设备 20 确认从接收设备 30 经通信 34 提供的公用密钥是有效用于使用的，头端 CA 系统已经被给出了这个密钥，并且头端 CA 系统 40 许可使用它，以致于源设备 20 和接收设备 30 被批准彼此结合操作。

按照本发明的另一个方面，如前所述，用于计算散列的源 ID 和/或算法是保持保密的。作为本领域的普通技术人员应该明白，潜在的非法翻印不能输入该散列函数的这种事实有效的防止了具有更为强大计算机的强行攻击。

按照本发明的另一个方面，PIN 码具有足够长的间距，用于有效特征符的彻底的搜索需要花费很长的时间，该时间是受到限制的。实现这种操作的一个方法是源设备 20 必须花费有效的时间认可 PIN 码，例如，使用一种复杂的计算，或者用在计算之后的一个等待周期。用

于这种应用的一个建议值，例如用于家庭 A/V 网络的复制保护，可以是 9 或 10 个数字 PIN，以及一秒的计算时间。这就强迫 5×10^8 或 5×10^9 秒的一个平均彻底搜索时间，或接近 16 或 160 年。

按照本发明一个可替换的方面，另一种输入散列函数可以是一个诸如一个磁带或 DVD 标题代码或媒体的序列号。例如，这就允许单独的标题或磁带被许可或不许可来用于使用。一种方法能通过在头端 CA 系统 40 中为一个给定使用者 50 存储序列号来实现节省有效时间，以便使用者 50 不必每次业务处理都要提供它们。

按照本发明的另一个可替换的方面，另一种输入散列函数可以是由第一许可引起的全部运行时间或流逝时间的指示。这允许在一个设置时间或使用之后该认可自动地期满到时。如果一个额外的时间代码是需要的，这可以从源设备 20 到使用者 50 发信号通知。时间代码应该是充分随机的以便使用者 50 不能有效的猜测或其他方式的预测下一个时间代码是什麽。如果使用者 50 能够这样做，他可以事先呼叫，并实质上预先准许他的系统，通过在他们被要求之前得到该 PIN 码。

此外，按照本发明的另一个可替换的方面，另一种基于系统的 PIN 码是建立在割据或把本地网络的密钥间距分成较小的段的基础上，而不用唯一预先的网络密钥到安全极限。

图 2 示例了访问不同的保护内容的使用中适用于鉴别密钥和识别符的另一个系统 100。系统 100 包括具有一个相关源 ID 的一个源设备 120，具有一个相关公用密钥的一个接收设备 130，源设备 120 的一个使用者或操作者 150，和一个头端 CA 系统 140。

用相当小数的私人密钥做成接收设备，例如 10，000。使用者 150 读取接收设备 130 和源设备 120 的序列号（如分别示例的通信 132，122）。使用者 150 然后呼叫头端 CA 系统 140，提供接收设备 130 和源设备 120 的序列号，并接收用于该接收设备 130 的 PIN 码（如通信 152，142 所示）。经过一个查找表或适当的计算可以确定 PIN 码。使用者 150 接着输入该 PIN 码进入源设备 120（如通信 154 所示），并使用公用密钥 160 的一个表，源设备 120 索引正确的公用密钥来用于接收设备 130。

公用密钥 160 的表的大小是相对于源设备 120 本身的存储。表 160

被加密，并存储在预先记录的媒体的开头上（例如，磁带）。对于当需要获得公用密钥（PUBLICKEY）时这是一种容易的机理，因为任何预先记录的磁带可以用于初始化网络。此后，系统 100 将工作在其自身上，由于源设备 120 将记住适当的密钥或与接收设备 130 使用。

诸如磁带之类的预先记录的媒体用某些其他更强的加密系统方法被加密。在本发明中，只有从源设备 120 到接收设备 130 的数字链路使用这种较弱的本地密钥被加密。尽管本地密钥对该网络不是唯一的，但要想有利可图的制造复制的材料是非常困难的，如果需要 10，000 不同的磁带版本用于每个标题。

在上述系统 100 的 10，000 本地密钥的一个变为已知的情况下，“私人”使用者可以继续的使用相同的 PIN 码以便使用任何源设备 120 可以播放内容。系统 100 可以被改进，通过使 PIN 码成为源 ID 的一个散列函数，以及索引成公用密钥 160 的表。这就强迫使用者 50 获得一个唯一的 PIN 来用于每个源设备 120。如果在索引表 160 中对于一个给定的公用密钥出现无法抗拒的请求数，则可以被当作一个信号，一个私人密钥已经被泄密。

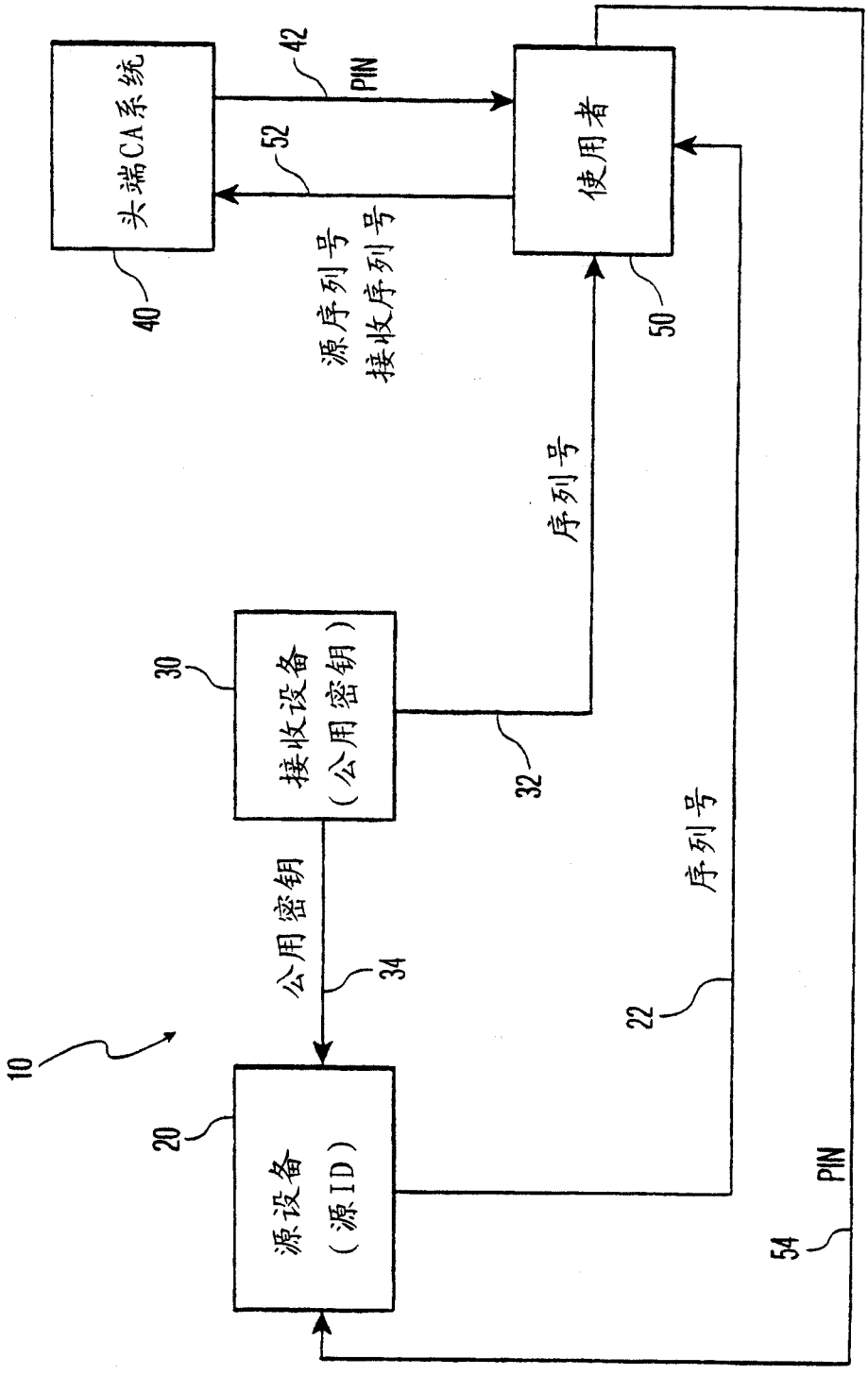

头端CA系统
40
42
PIN
52
源序列号
接收序列号
使用者
50
序列号
30
接收设备
(公用密钥)
32
公用密钥
34
10
20
源设备
(源ID)
22
序列号
54
PIN

图 1

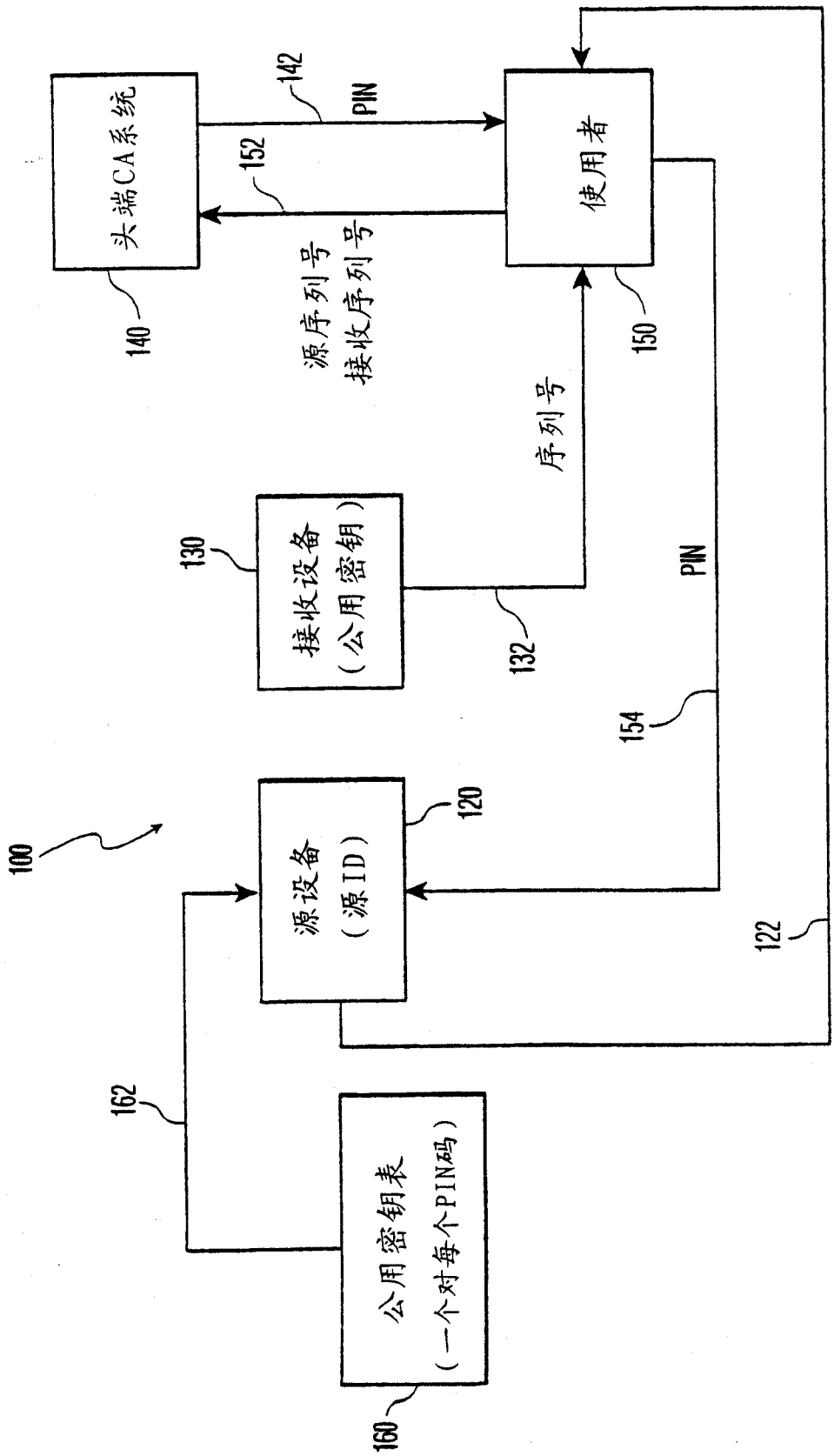

100
头端CA系统
140
142
PIN
152
源序列号
接收序列号
使用者
150
序列号
接收设备
(公用密钥)
130
132
PIN
154
源设备
(源ID)
120
122
162
公用密钥表
(一个对每个PIN码)
160

图 2