(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 101699458 B
(45)授权公告日 2013.05.29

(21)申请号 200910222182.6
(22)申请日 2005.12.13
(30)优先权数据
11/051,499 2005.02.03 US
60/642,340 2005.01.07 US
(62)分案原申请数据
200580046121.9 2005.12.13
(73)专利权人 苹果公司
地址 美国加利福尼亚州
(72)发明人 乔纳森·杰克·鲁宾斯坦
安东尼·M.·菲德尔
杰希·L·多罗古斯克尔
米特切尔·安德勒尔
约翰·维斯雷·阿奇贝尔德
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 李镇江
(51)Int.Cl.
G06F 21/44(2013.01)
(56)对比文件
WO 03/073688 A1,2003.09.04,
CN 1759367 A,2006.04.12,
WO 03/073688 A1,2003.09.04,
CN 1381016 A,2002.11.20,
Alfred J.Menezes,Paul C.Van Oorschot and Scott.Identification and Entity Authentication.《Handbook of Applied Cryptography》.1997,
审查员 孟子山

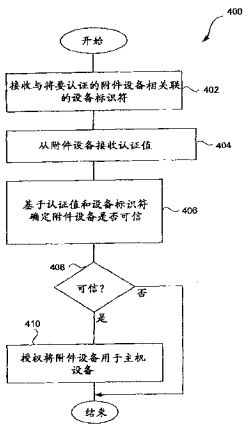
权利要求书2页 说明书16页 附图23页

(54)发明名称

用于电子设备的附件认证

(57)摘要

本申请涉及用于电子设备的附件认证，并公开了控制将附件设备用于电子设备的改进的技术。该技术可以用密码方法认证电子设备，即彼此互连和通信的电子设备。一个方面涉及用于认证电子设备（如附件设备）的技术。另一个方面关于由或为电子设备（如主机设备）提供软件特征（例如功能）。可以例如根据认证的不同程度或等级或根据制造商或产品不同地提供不同的电子设备。另一个方面涉及用附件（或适配器）将外围设备（如USB设备）转换为主机设备（如USB主机）。该技术特别适合于可以接收附件设备的电子设备，如媒体设备。媒体设备的一个例子是可以呈现（例如播放）媒体项目（或媒体资产）的媒体播放器，诸如手持媒体播放器（如音乐播放器）。



CN 101699458 B

1. 一种用于便携电子设备的附件设备，包括：

输入 / 输出端口，用于与所述便携电子设备交互；

存储设备，存储有认证算法并存储有与所述附件设备相关联的认证密钥；

认证控制器，其以可操作方式连接到所述输入 / 输出端口，其中，所述认证控制器由单一的集成电路芯片实现，所述认证控制器被配置成：

从所述便携电子设备接收随机数；

使用与所述附件设备相关联的第一密钥对所述随机数进行加密以生成经加密的随机数；

把所述经加密的随机数传送给所述便携电子设备；并且

从所述便携电子设备接收关于所述附件设备是否至少部分地基于所述经加密的随机数而受到认证的指示；和

附件电路，其被配置成：

响应于失败的认证，通过所述输入 / 输出端口访问所述便携电子设备的受限制的一组功能；并且

响应于成功的认证，通过所述输入 / 输出端口访问所述便携电子设备的完整一组功能，其中，所述受限制的一组功能包括的功能比所述完整一组功能少，并且其中，所述受限制的一组功能包括至少一个功能。

2. 如权利要求 1 的附件设备，其中，所述附件设备还包括：

与所述附件设备相关联的设备标识符。

3. 如权利要求 1 或 2 的附件设备，其中所述认证密钥是私钥，并且其中，所述认证控制器使用所述私钥加密一个值。

4. 如权利要求 1 或 2 的附件设备，其中，所述附件设备是外围适配器，并且

其中，所述附件电路至少包括升压器，该升压器接收第一电压并且输出第二电压，当将所述附件设备连接到所述便携电子设备时，从所述便携电子设备接收所述第一电压，并且当所述便携电子设备已经认证了所述附件设备时，输出所述第二电压。

5. 一种附件设备，包括：

通信装置，用于与便携电子设备通信；

认证装置，用于向所述便携电子设备认证所述附件设备，其中，所述认证装置在单一的集成电路芯片内实现，并被配置成：

从所述便携电子设备接收随机数；

使用与所述附件设备相关联的第一密钥对所述随机数进行加密以生成经加密的随机数；

把所述经加密的随机数传送给所述便携电子设备；并且

从所述便携电子设备接收关于所述附件设备是否被至少部分地基于所述经加密的随机数而受到认证的指示；以及

控制装置，用于通过所述通信装置控制所述便携电子设备，其中，所述控制装置被配置成：

如果所述认证失败，则通过所述通信装置执行所述便携电子设备的受限制的一组功能；并且

如果所述认证成功，则通过所述通信装置执行所述便携电子设备的完整一组功能，其中，所述受限制的一组功能包括至少一个功能。

用于电子设备的附件认证

[0001] 本申请是申请日为 2005 年 12 月 13 日、申请号为 200580046121.9(国际申请号 PCT/US2005/045040)、名称为“用于电子设备的附件认证”的发明专利申请的分案申请。

技术领域

[0002] 本发明涉及电子设备,并且更具体地涉及接收附件设备的电子设备,诸如媒体播放器。

背景技术

[0003] 媒体播放器存储可以在媒体播放器上显示或播放的媒体资产,诸如音频轨迹或相片。媒体播放器的一个例子是可从 Cupertino, CA 的 Apple Computer 公司得到的iPod®媒体播放器。通常媒体播放器从主计算机获得其媒体资产,主计算机起使得用户能够管理媒体资产的作用。作为例子,主计算机可以执行媒体管理应用以便管理媒体资产。媒体管理应用的一个例子是 Apple Computer 公司出品的iTunes®。

[0004] 媒体播放器典型地包括一个或多个可以用作与该媒体播放器间的接口的连接器或端口。例如,连接器或端口使得媒体播放器能够耦合到主计算机,插入对接系统或接收附件设备。当前有可以互连到媒体播放器的许多不同类型的附件设备。例如,可以将远程控制器连接到连接器或端口,以便允许用户远程地控制媒体播放器。作为另一个例子,汽车可以包括连接器,并且可以将媒体播放器插入该连接器,从而汽车的媒体系统可以与该媒体播放器交互,从而允许在汽车内播放该媒体播放器上的媒体内容。

[0005] 当前,只要使用兼容的连接器或端口,媒体播放器的连接器或端口通常是自由使用的。因此,许多第三方已经开发了用于其他制造商的媒体播放器的附件设备。一个困难在于媒体播放器的制造商不能控制可以被连接到媒体播放器的各种不同的附件设备。这是成问题的,因为第三方附件设备可能是劣质的、易于出错的、有破坏性的(例如,资源泄露)、或甚至对媒体播放器本身是有损害的。另一个问题是未经媒体播放器的制造商授权的第三方附件设备可能会试图以不适当或不希望的方式使用媒体播放器的特征。

[0006] 因此,需要改进的技术,使得电子设备的制造商能够控制可以与他们的电子设备一起使用的附件设备的性质和程度。

发明内容

[0007] 广泛地讲,本发明关于控制将附件设备用于电子设备的改进的技术。该改进的技术可以使用密码方法认证电子设备,即,彼此互连和通信的电子设备。

[0008] 本发明的一个方面关于用于认证电子设备(诸如附件设备)的技术。本发明的另一个方面关于由或为电子设备(诸如主机设备)提供软件特征(例如,功能)。可以,例如,根据认证的不同程度或等级或根据制造商或产品不同地提供不同的电子设备。本发明的另一个方面关于使用附件(或适配器)将外部设备(例如,USB 设备)转换为主机设备(例如,USB 主机)。本发明的实施例可以与此处公开的这些方面或其它方面中的一个或多个有

关。

[0009] 可以用各种方式实现本发明，包括作为方法、系统、设备、装置（包括图形用户接口）或计算机可读介质来实现本发明。下面描述本发明的若干实施例。

[0010] 作为便携电子设备，本发明的一个实施例至少包括：媒体存储设备，其存储一个或多个媒体项目的媒体内容；媒体呈现模块，其从媒体存储设备中检索至少一个所述媒体项目的媒体内容，并且使得为便携电子设备的用户呈现该媒体内容；认证表，其存储被授权耦合到便携电子设备并与便携电子设备交互的各种附件设备的认证信息；和认证模块，其基于存储在认证表内的认证信息的至少一部分，确定是否授权耦合到便携电子设备的特定附件设备与便携电子设备互操作。

[0011] 作为用于便携电子设备的附件设备，本发明的一个实施例至少包括：与便携电子设备交互的输入／输出端口；认证算法；与附件设备相关联的认证密钥；用于至少使用该认证算法和认证密钥执行认证操作的操作上连接到输入／输出端口的认证控制器；执行与附件设备相关联的操作的附件电路。

[0012] 作为用于将附件设备连接到媒体播放器的连接器，本发明的一个实施例至少包括：连接器主体；附在连接器主体内并且用于提供附件设备和媒体播放器间的电连接的多个电触点；和布置在连接器主体内并且提供允许附件设备被媒体播放器认证的认证密钥的控制器。

[0013] 作为授权将附件设备用于电子设备的方法，本发明的一个实施例至少包括下列活动：从附件设备接收设备标识符；从附件设备接收认证值；基于认证值确定附件设备是否可信；和当确定附件设备可信时，授权将附件设备用于电子设备。

[0014] 作为授权将附件设备用于电子设备的方法，本发明的另一个实施例至少包括下列活动：检测附件设备附接到电子设备；在检测到附件设备的附接后，向附件设备发送随机数；随后从附件设备接收编码值；从附件设备接收设备标识符；基于设备标识符获得密码密钥；使用该密码密钥对编码值解码以便产生解码值；确定该解码值是否相应于该随机数；和当确定解码值相应于该随机数时，授权将附件设备用于电子设备。

[0015] 作为用于授权将附件设备用于电子设备的方法，本发明的另一个实施例至少包括下列活动：检测附件设备附接到电子设备；在检测到附件设备的附接后，向附件设备发送至少包括一个随机数的认证请求；随后接收来自附件设备的认证响应，该认证响应是对认证请求的响应，并且该认证响应至少包括附件设备的编码值和设备标识符；基于设备标识符获得密码密钥；使用该密码密钥对该编码值解码以便产生解码值；和基于解码值和随机数间的相应关系，授权将附件设备用于电子设备。

[0016] 作为用于授权将附件设备用于电子设备的方法，本发明的另一个实施例至少包括下列活动：从电子设备接收随机数；使用在附件设备内提供的密码密钥对随机数编码，从而产生编码值；和向电子设备发送编码值和设备标识符。

[0017] 作为控制媒体播放器和附件设备间的交互的方法，本发明的一个实施例至少包括下列活动：确定附件设备的分类；识别附件设备的授权等级；和基于附件设备的分类和授权等级，选择性地激活可以结合该附件设备使用的媒体设备的特征。

[0018] 作为媒体播放器系统，本发明的一个实施例至少包括：存储媒体内容和支持多个预定功能的媒体播放器，以及能够连接到媒体播放器的附件设备。媒体播放器与附件设备

交互，以便执行认证处理，并且基于该认证处理，选择性地激活媒体播放器的特定功能，从而可以由附件设备使用。

[0019] 从下面结合以示例方式说明本发明的原理的附图进行的详细描述中，可以明了本发明的其他方面和优点。

附图说明

[0020] 易于结合附图从下面的详细描述中理解本发明，其中相同的标号指代相同的结构元件，并且其中：

[0021] 图 1A 是根据本发明的一个实施例的附件认证系统的方框图；

[0022] 图 1B 是根据本发明的另一个实施例的附件认证系统的方框图；

[0023] 图 1C 是根据本发明的另一个实施例的附件认证系统的方框图；

[0024] 图 2A 是根据本发明的一个实施例的认证控制器的方框图；

[0025] 图 2B 是根据本发明的一个实施例的认证管理器的方框图；

[0026] 图 3 是根据本发明的一个实施例的认证设备的方框图；

[0027] 图 4A 是根据本发明的一个实施例的主机认证处理的流程图；

[0028] 图 4B 是根据本发明的一个实施例的附件认证处理的流程图；

[0029] 图 5A 和 5B 是根据本发明的一个实施例的主机设备处理的流程图；

[0030] 图 6A 和 6B 是根据本发明的一个实施例的附件设备处理的流程图；

[0031] 图 6C 是根据本发明的一个实施例的授权表的图；

[0032] 图 7A 和 7B 是根据本发明的一个实施例的附件设备处理的流程图；

[0033] 图 8A-8C 是根据本发明的一个实施例的主机设备处理的流程图；

[0034] 图 9A-9C 是根据本发明的一个实施例的附件设备处理的流程图；

[0035] 图 10A 和 10B 是根据本发明的一个实施例的主机设备处理的流程图；

[0036] 图 11 是根据本发明的一个实施例的媒体管理系统的方框图；

[0037] 图 12 是根据本发明的一个实施例的媒体播放器的方框图。

具体实施方式

[0038] 本发明关于控制将附件设备用于电子设备的改进的技术。该改进的技术可以使用密码方法认证电子设备，即，彼此互连和通信的电子设备。

[0039] 该改进的技术特别适用于可以接收附件设备的电子设备，诸如媒体设备。媒体设备的一个例子是可以呈现（例如，播放）媒体项目（或媒体资产）的媒体播放器，诸如手持媒体播放器（例如，音乐播放器）。媒体设备的附件的例子包括：录音机、FM 收发机、外围总线设备（例如，Fire Wire®或 USB 设备）、媒体设备（例如，媒体阅读器、显示器、照相机等），电源（例如，电源适配器、电池包等），扬声器（耳机或扬声器系统），远程控制设备，网络设备或汽车集成单元。

[0040] 本发明的一个方面关于用于认证电子设备诸如附件设备的技术。本发明的另一个方面关于由或为电子设备（例如，主机设备）提供软件特征（例如，功能）。可以，例如，根据认证的不同程度或等级或根据制造商或产品不同地提供不同的电子设备。本发明的另一个方面关于使用附件（或适配器）将外围设备（例如，USB 设备）转换为主机设备（例如，

USB 主机）。本发明的实施例可以与此处公开的这些方面或其它方面中的一个或多个有关。

[0041] 下面参考图 1-12 讨论本发明的实施例。然而，本领域的技术人员易于理解，此处针对这些图给出的详细描述是出于示例的目的，因为本发明延及这些有限的实施例之外。

[0042] 图 1A 是根据本发明的附件认证系统 100 的方框图。附件认证系统 100 包括移动计算设备 102。移动计算设备 102 还可以称为主机设备。另外，移动计算设备 102 可以例如属于媒体播放器、个人数字助理或移动电话。移动计算设备 102 包括用于接收连接器的连接器端口 104。

[0043] 附件认证系统 100 还包括具有连接器 108 和连接器端口 110 的认证设备 106。认证设备 106 可以附于移动计算设备 102。具体地，当将认证设备 106 附于移动计算设备 102 时，由移动计算设备 102 的连接器端口 104 接收认证设备 106 的连接器 108。当将连接器 108 耦合到连接器端口 104 内时，认证设备 106 物理地和电子地连接到移动计算设备 102。

[0044] 附件认证系统 100 还包括附件设备 112。当附件设备 112 通过认证设备 106 与移动计算设备 102 互连时，附件设备 112 给移动计算设备 102 提供某些功能。为了便于这种互连，附件设备 112 包括连接器 114 和电缆 116。电缆 116 将连接器 114 连接到附件设备 112。可以将连接器 114 耦合到认证设备 106 的连接器端口 110。当进行这种连接时，附件设备 112 通过认证设备 106 与移动计算设备 102 进行电子通信。

[0045] 虽然附件认证系统 100 包括连接器 114 和电缆 116 的端部，可以将连接器 114 集成在附件设备 112 内。换言之，在另一个实施例中，不需要电缆 116。

[0046] 根据本发明的一个方面，认证设备 106 起向移动计算设备 102 认证其自身的作用。认为授权认证的设备与移动计算设备 102 交互。另外，一旦被授权，就可以控制认证的设备 106（或附件设备 102）和移动计算设备 102 之间的交互性质和程度。因此，一旦被授权，移动计算设备 102 可以认为认证设备 106 是可信任的合作方，允许其访问移动计算设备 102 的功能、特征或操作。在另一方面，如果移动计算设备 102 确定认证设备 106 不与可信任的合作方相关联，则移动计算设备 102 可以阻止或限制与认证设备 106 或附件设备 112 的交互。认证设备 106 本身可以被认为是移动计算设备 102 的附件设备。

[0047] 在一个实施例中，认证设备 106 起总线接口适配器诸如 USB 或 Fire Wire®适配器的作用。在这种实施例中，认证设备 106 起使得移动计算设备 102 与总线主机设备（例如，USB 或 Fire Wire®主机）匹配的作用。附件设备 112 有利地仅需作为总线外围设备（例如，USB 或 Fire Wire®设备）操作。

[0048] 图 1B 是根据本发明的另一个实施例的附件认证系统 150 的方框图。附件认证系统 150 包括具有连接器端口 154 的移动计算设备 152。移动计算设备 152 还可以称为主机设备。另外，移动计算设备 152 可以例如属于媒体播放器、个人数字助理或移动电话。

[0049] 附件认证系统 150 还包括附件设备 156。附件设备 156 包括连接器 158 和认证设备 160。在该实施例中，认证设备 160 内置于附件设备 156。可以通过将连接器 158 插入连接器端口 154，将附件设备 156 耦合到移动计算设备 152。一旦建立这种连接，附件设备 156 被电子地连接到移动计算设备 152。然而，移动计算设备 152 可以与认证设备 160 交互，以便使得移动计算设备 152 能够认证附件设备 156。当被认证时，认为授权附件设备 156 与移动计算设备 152 交互。一旦被授权，就可以控制附件设备 156 和移动计算设备 152 之间的交互性质和程度。因此，一旦被授权，移动计算设备 152 可以认为附件 156 是可信任的合作

方（或与可信任的合作方相关联），允许其访问移动计算设备 152 的功能、特征或操作。在另一方面，如果移动计算设备 152 确定附件设备 156 不是可信任的合作方（或不与可信任的合作方相关联），则移动计算设备 152 可以阻止或限制与附件设备 156 的交互。

[0050] 图 1C 是根据本发明的另一个实施例的附件认证系统 170 的方框图。附件认证系统 170 包括具有连接器端口 174 的移动计算设备 172。移动计算设备 172 还可以称为主机设备。移动计算设备 172 可以例如属于媒体播放器、个人数字助理或移动电话。附件认证系统 170 还包括附件设备 176。附件设备 176 包括连接器 178 和认证设备 180。在该实施例中，认证设备 180 耦合到连接器 178 或与连接器 178 集成在一起。认证设备可以相对较小，并且从而耦合到连接器 178 或与连接器 178 集成在一起。通过在连接器 178 内提供认证设备 180，可以容易地制造提供认证功能的附件设备。

[0051] 可以通过将连接器 178 插入连接器端口 174，将附件设备 176 耦合到移动计算设备 172。一旦建立这种连接，附件设备 176 被电子地连接到移动计算设备 172。然而，移动计算设备 172 可以与认证设备 180 交互，以便使得移动计算设备 172 能够认证附件设备 176。当被认证时，认为授权附件设备 176 与移动计算设备 172 交互。一旦被授权，就可以控制附件设备 176 和移动计算设备 172 之间的交互性质和程度。因此，一旦被授权，移动计算设备 172 可以认为附件 176 是可信任的合作方（或与可信任的合作方相关联），允许其访问移动计算设备 172 的功能、特征或操作。在另一方面，如果移动计算设备 172 确定附件设备 176 不是可信任的合作方（或不与可信任的合作方相关联），则移动计算设备 172 可以阻止或限制与附件设备 172 的交互。

[0052] 另外，虽然图 1A-1C 涉及用于为移动计算设备认证附件设备的认证设备，应当理解这种认证设备可替换地可以用于为附件设备认证移动计算设备。在任何情况下，以安全的方式诸如使用密码技术进行要执行的认证。密码技术不仅主要起防止使用伪造的附件设备的作用，而且使得“进行哄骗 (spoofing)”的机会减少了。在一个实施例中，密码技术使用公 - 私密钥组形成有效的数字签名。

[0053] 图 2A 是根据本发明的一个实施例的认证控制器 200 的方框图。认证控制器 200 包括处理器 202、随机访问存储器 (RAM) 204、和只读存储器 (ROM) 206。ROM206 包括私钥 208 和认证算法 210。认证控制器 200 还接收电源线 212 和通信总线（链路）214。例如，可以由认证控制器 200 的连接器，诸如，图 1A 中所示的连接器 108、图 1B 中所示的连接器 158 或图 1C 中所示的连接器 178 提供电源线 212 和通信总线 214。

[0054] 处理器 202 典型地与移动计算设备交互（通过通信总线 214），以便认证附件设备（或认证设备）。在认证过程中，处理器 202 使用存储在认证控制器 200 内的认证算法 210 和私钥 208。认证算法 210 可以随不同的实现而改变，并且适合的认证算法是本领域的技术人员已知的。

[0055] 虽然图 2A 中未示出，认证控制器 200 或包括或利用认证控制器 200 的认证设备或附件设备还可以包括设备标识符和附加电路。设备标识符可以例如属于产品标识符和 / 或制造商标识符。附加电路可以随实现而改变。当附加电路在附件设备内时，附加电路可以称为附件电路。

[0056] 在一个实施例中，在单个集成电路（即，单个芯片）上实现认证控制器 200。通过在单个集成电路上提供认证控制器 200，可以大体上避免对私钥 208 和认证算法 210 的外

部访问。结果，认证处理不仅在密码学上是安全的，而且由于受限的物理访问还是物理安全的。

[0057] 图 2B 是根据本发明的一个实施例的认证管理器 250 的方框图。认证管理器 250 例如被提供在电子设备内，诸如图 1A 中所示的移动计算设备 102、图 1B 中所示的移动计算设备 152 或图 1C 中所示的移动计算设备 172。在该实施例中，电子设备的认证管理器 250 认证附件设备（或认证设备）。

[0058] 认证管理器 250 包括认证模块 252、授权表 254 和端口接口 256。认证模块 252 操作以便评耦合接到端口接口 256 的特定附件设备（或认证设备）是否是可信的，并且从而允许与该电子设备互操作。端口接口 256 可以给附件设备（或认证设备）提供电源和通信总线 258。授权表 254 存储由认证模块 252 使用以便评估某个附件设备（或认证设备）是否可信的认证信息。如前所述，认证管理器 250 被提供在可被称为主机设备的电子设备内。

[0059] 电子设备（或主机设备）典型地具有可以调用或利用的各种操作特征。在一个实施例中，由认证管理器 250 认证的附件设备可以完全访问电子设备（或主机设备）上的所有可用特征。在另一个实施例中，授权表 254 可以控制电子设备或主机设备的特征对附件设备可用的方式。作为一个例子，如果电子设备（或主机设备）提供可以利用的多个不同特征，授权表 254 可以包含关于允许特定附件设备利用这些可用特征中的哪一些的指示。例如，可以给授权分级或分类，它们中的每一个具有不同的授权。授权还可以指明不同特征被授权使用的方式。因此，以受限的方式授权使用特征。例如，授权在与电子设备间的慢的通信接口（例如，串行）上使用一个特征，并且不授权在与电子设备间的快的通信接口（例如，Fire Wire®或 USB）上使用。换言之，在该例子中，仅授权在某些接口机构上使用这些特征。

[0060] 图 3 是根据本发明的一个实施例的认证设备 300 的方框图。在该实施例中，认证设备 300 不仅包含用于其自身或耦合到其上的附件设备的认证的电路，而且包含用于由认证设备 300 提供其他功能的附加电路。具体地，认证设备 300 设计为耦合到电子设备并且连接到附件设备。如图 3 中所示，认证设备 300 包括包含存储器 304 的控制器 302。作为例子，控制器 302 可以属于图 2A 中所示的认证控制器 200。控制器 302 可以耦合到端口连接器 306，端口连接器 306 又可以连接到电子设备。端口连接器 306 可以通过电源线 (Pin) 从电子设备给控制器 302 和升压转换器 308 提供电能。另外，控制器 302 可以借助于传输和接收通信线 (TX，RX) 通过端口连接器 306 与电子设备通信。通过这种通信，电子设备可以确定认证设备 300 是否被授权与用于该电子设备。如果电子设备确定认证设备 300 被授权了，则控制器 302 可以使用使能信数 (EN) 使能升压转换器 208。一旦被使能，在来自端口连接器 306 的电源线 (Pin) 上接收输入电压的升压转换器 308 可以在到 USB 连接器 310 的电源线 (Pout) 上输出升压输出电压。例如，输入电压可以是 3.3V 并且升压输出电压可以是 5.0V。USB 连接器 310 还接收来自端口连接器 306 的一对差分数据线 (D+，D-)，以便允许电子设备和可以耦合到 USB 连接器 310 的附件设备间的数据传输。

[0061] 在该实施例中，认证设备 300 可以操作以便将电子设备转换为主机设备，诸如 USB 主机。典型地，电子设备是 USB 设备，而不是主机设备，但是认证设备 300 到电子设备的附加可以将电子设备转换为主机设备。主机设备可以是 USB 兼容的，从而可以将任何 USB 设备连接到 USB 连接器 310。在该情况下，可以通过认证设备 300 将带有 USB 端口的任何附件

连接到该电子设备。

[0062] 可以使用本发明采用的认证技术，以便允许主机设备认证附件设备，或可以允许附件设备认证主机设备。在认证设备和主机设备之间的耦合期间，可以在任何时刻启动主机设备和附件设备间的认证处理。例如，可以在将附件设备连接到主机设备时、在第一次使用受限制的特征时或周期地启动认证处理。

[0063] 图 4A 是根据本发明的一个实施例的认证处理 400 的流程图。由例如主机设备执行主机认证处理 400。

[0064] 主机认证处理 400 最初接收 402 与将要认证的附件设备相关联的设备标识符。另外，从附件设备接收 404 认证值。此处，主机设备执行认证处理；因此，附件设备将认证值提供给主机设备。在一个实施例中，在确定认证值时，附件设备利用随机数和私钥。可以由主机设备将随机数提供给附件设备，或可以从附件设备得到随机数。

[0065] 接着，主机认证处理 400 基于认证值和设备标识符确定 406 附件设备是否可信。然后判断 408 基于在方框 406 做出的确定，确定附件设备是否可信。当判断 408 确定附件设备已被确定为是可信的，则授权 410 将附件设备用于主机设备。授权 410 使用的性质可以根据实现改变。例如，授权 410 的使用可以允许对附件设备的完全使用，或可以允许附件设备的受限的使用。

[0066] 在另一方面，当判断 408 确定附件设备不可信时，则旁路方框 410 从而不授权将附件设备用于主机设备。在该情况下，由于附件设备未被确定为是可信的，大体上限制或阻止将附件设备用于主机设备。在方框 410 或旁路方框 410 之后，主机认证处理 400 完成并且结束。

[0067] 图 4B 是根据本发明的一个实施例的附件认证处理的流程图。由例如附件设备执行附件认证处理 450。

[0068] 附件认证处理 450 向主机设备发送 452 与附件设备相关联的私钥标识符。主机设备使用私钥标识符获得适当的私钥，在产生发送给附件设备的认证值时主机设备使用该私钥。附件设备从主机设备接收 454 认证值。

[0069] 接着，附件认证处理 450 基于认证值和公钥确定 456 主机设备是否可信。典型地，公钥被在内部提供给附件设备。然后判断 458 确定主机设备是否被确定为可信。当判断 458 确定主机设备已被认为可信时，则授权 460 将主机设备用于附件设备。授权 460 使用的性质可以根据实现改变。例如，授权 460 的使用可以允许对主机设备的完全使用，或可以允许主机设备的受限的使用。

[0070] 在另一方面，当判断 458 确定主机设备不可信时，则旁路方框 460，从而大体上限制或阻止将主机设备用于附件设备。在方框 460 或旁路方框 460 之后，附件认证处理 450 完成并且结束。

[0071] 图 5A 和 5B 是根据本发明的一个实施例的主机设备处理 500 的流程图。由电子设备，诸如，图 1A 中所示的移动计算设备 152、图 1B 中所示的移动计算设备 152 或移动计算设备 172 执行主机设备处理 500。

[0072] 主机设备处理 500 以判断 502 开始，判断 502 确定是否从附件设备接收到认证信息。当判断 502 确定未接收到认证信息时，主机设备处理 500 等待对认证信息的接收。一旦判断 502 确定已经在主机设备处接收到认证信息，则主机设备处理 500 继续。即，在主机

设备处产生 504 随机数。典型地，在主机设备处随机地产生 504 随机数，诸如使用随机数产生器。接着，将认证请求发送 506 到附件设备。此处，认证请求至少包括随机数。

[0073] 然后判断 508 确定是否从附件设备接收到认证响应。当判断 508 确定仍未接收到认证响应时，则主机设备处理 500 等待对这种认证响应的接收。一旦判断 508 确定已经接收到认证响应，从认证响应中提取 510 编码数字和设备标识符。

[0074] 然后，使用该设备标识符，可以获得 512 公钥。在一个实施例中，主机设备包括分配给各个不同附件设备的多个公钥。在这种实施例中，设备标识符可用于指定特定的附件设备，并且从而允许选择这些公钥中适当的一个。接着，使用公钥对编码数字进行密码解码 514，以便产生解码数字。然后将解码数字与随机数进行比较 516。换言之，将从在认证响应中从附件设备接收到的编码数字得出的解码数字与以前在认证请求中发送给附件设备的随机数进行比较。然后判断 518 确定解码数字是否与随机数匹配。当判断 518 确定解码数字不与随机数匹配时，可以可选择地通知用户该附件设备未被授权。可以通过视觉装置或音频装置实现这种通知。例如，视觉通知可以呈现在与主机设备或附件设备相关联的显示设备上。

[0075] 在另一方面，当判断 518 确定解码数字不与随机数匹配时，获得 522 与设备标识符相关联的授权的特征。然后，使能 524 对被授权特征的使用。接着，判断 526 可以确定是否从主机设备移去（或拆卸下）附件设备。当判断 526 未移去附件设备时，则主机设备处理 500 可以继续允许对被授权特征的使用。然而，一旦判断 526 确定已经移去附件设备，则禁止 528 对主机设备的所有特征的使用。换言之，作为例子，可以认为在一个会话过程中使能对被授权特征的使用。只要附件设备保持附于主机设备，则会话可以保持为激活。一旦被拆卸下，则会话结束并且后续的重新附加需要重新认证。在操作 528 之后，以及在操作 520 之后，主机设备处理 500 完成并且结束。

[0076] 图 6A 和 6B 是根据本发明的一个实施例的附件设备处理 600 的流程图。由附件设备，诸如，图 1A 中所示的附件设备 112、图 1B 中所示的附件设备 156 或图 1C 中所示的附件设备 176 执行附件设备处理 600。附件设备处理 600 代表图 5A 和 5B 中所示的主机设备处理 500 的配对处理。

[0077] 附件设备处理 600 以判断 602 开始，判断 602 确定是否给附件设备供电。当判断 602 确定未给附件设备供电时，附件设备处理 600 等待可用电能。典型地，一旦将附件设备连接到主机设备，就给附件设备供电。因此，可替换地判断 602 可以确定附件设备是否连接到了主机设备。

[0078] 一旦判断 602 确定已给附件设备供电，可以将认证信息发送 604 给主机设备。在一个实施例中，认证信息可以包括指示所支持的一个或多个认证版本的信息。然后判断 606 确定是否接收到认证请求。当判断 606 确定未接收到认证请求时，则附件设备处理 600 等待这种请求。一旦判断 606 确定已经接收到认证请求，提取 608 在认证请求中提供的随机数。从认证设备获得 610 私钥。出于安全的原因，私钥可以存储在认证设备内部，并且不能够容易地从认证设备的外部访问。接着，使用密钥私钥对该随机数密码编码 612，以便产生编码数字。

[0079] 此后，向主机设备发送 614 认证响应。此处，认证响应至少包括该编码数字和设备标识符。在已经发送 614 认证响应之后，判断 616 确定是否已经授权对主机设备的特征的

访问。可以主动地或被动地确定判断616。例如，主机设备可以通知附件设备它已被授权访问主机设备的一个或多个特征。作为另一个例子，主机设备可以不通知附件设备，而是允许附件设备访问已授权的主机设备的一个或多个特征。在任何情况下，当判断616确定未授权对主机设备上的某些特征的访问时，禁止附件设备的操作620，如果有的话，使用主机设备的某些特征。实际上，在一个实施例中，主机设备可以阻止附件设备的任何操作。作为例子，主机设备可以阻止与附件设备的通信和/或停止给附件设备供电。

[0080] 在另一方面，当判断616确定已经授权对主机设备的某些特征的访问时，则可以根据授权的特征操作618附件设备。换言之，如果被授权，附件设备能够与主机设备交互，以便利用由主机设备提供的某些特征。

[0081] 在操作618和620之后，判断622确定是否移去了附件设备，即，附件设备是否从主机设备断开。当判断622确定附件设备保持连接或附加于主机设备时，则适当的操作618或620可以继续。可替换地，当判断622确定已经移去了附件设备时，则不再授权附件设备与主机设备交互，并且因此不再能够利用以前授权的由主机设备支持的特征。在该情况下，附件设备处理600结束。然而，通过再次执行附件设备处理600，可以随后重新授权附件设备。

[0082] 在附件设备处理600中，与认证响应一起提供设备标识符。在可替换的实施例中，可以不同地将设备标识符提供给主机设备，诸如与认证信息一起提供。还可以单独地将设备标识符提供给主机设备。

[0083] 图6C是根据本发明的一个实施例的授权表650的图。该授权表适合于，例如，用作图2B中所示的授权表254。一般地，可以使用授权表650确定针对给定附件设备的授权特征。授权表650包括设备标识符栏652、公钥栏654和授权特征栏656。授权表650将设备标识符、公钥和授权的特征关联在一起。使用设备标识符，主机设备可以确定在确定是否可以认证使用特定设备标识符标识的附件设备时将使用的适当的公钥。在对附件设备的认证成功的情况下，可以在授权特征栏656中标识出与设备标识符相关联的授权的特征。

[0084] 根据本发明的一个方面，主机设备可以操作，以便认证耦合到主机设备的附件设备。允许能够被认证的那些附件设备在较大的程度上与主机设备互操作。因此主机设备可以控制附件设备可以与主机设备互操作的性质和程度。例如，当不能认证附件设备时，主机设备可以限制、约束或阻止附件设备与主机设备互操作。可替换地，当附件设备被认证时，主机设备可以允许与主机设备的较多的互操作。

[0085] 图7A和7B是根据本发明的一个实施例的附件设备处理700的流程图。图8A-8C是根据本发明的一个实施例的主机设备处理800的流程图。在与主机设备的认证处理过程中，由附件设备执行附件设备处理700。在与附件设备的认证处理过程中，由主机设备执行主机设备处理800。主机设备处理800是附件设备处理700的配对处理。换言之，在认证处理中，在附件设备内的主机设备间存在信息交换。因此，图7A和7B表示在认证处理的一个实施例中，由附件设备执行的处理，并且图8A-8C表示由主机设备执行的处理。应当理解，虽然在这些图中示出的认证处理被示出为大体上是顺序的，一般地，可以认为认证处理是一种协议，附件设备和主机设备使用该协议交换不仅用于认证，而且用于后续操作的信息。在一个实施例中，可以认为这种协议大体上是并行的，诸如在客户机-服务器或主-从实现中。

[0086] 图 7A 和 7B 是根据本发明的一个实施例的附件设备处理 700 的流程图。附件设备处理 700 开始于判断 702。判断 702 确定附件设备是否连接到主机设备。典型地，判断 702 检测附件设备借助于连接器到主机设备的最近的连接。在任何情况下，当判断 702 确定附件设备未连接到主机设备时，附件设备处理 700 可以有效地等待这种连接。换言之，当附件设备连接到主机设备时，可以认为调用了附件设备处理 700。

[0087] 一旦判断 702 确定附件设备连接到了主机设备，附件设备处理 700 继续。当附件设备处理 700 继续时，将认证控制信息从附件设备发送 704 到主机设备。作为例子，认证控制信息可以指明附件设备的类型、是否支持认证、何时认证、和 / 或附件设备的功率要求。附件设备的类型的特定例子是 :麦克风、simple remote、display remote、远程用户接口、RF 发射器和 USB 控制主机。在附件设备的通电初期或响应来自主机设备的命令或确认，清除 706 附件设备的认证状态。此处，当连接附件设备时，通过清除 706 认证状态，附件设备可以知道它必须被主机设备认证。

[0088] 接着，判断 710 确定是否收到了设备认证信息请求。此处，由主机设备向附件设备发送设备认证信息请求。设备认证信息请求起请求来自附件设备的某些信息的作用，主机设备在认证处理过程中使用该信息。当判断 710 确定仍未接收到设备认证信息请求时，附件设备处理 700 等待这种请求。一旦判断 710 确定已经接收到设备认证信息请求，从附件设备获得 712 设备认证信息。作为例子，设备认证信息可以包括设备标识符和版本指示器。设备标识符可以属于供应商标识符、产品标识符或两者。版本指示器可以属于支持的协议版本。然后，将设备认证信息发送 714 到主机设备。

[0089] 然后判断 716 确定是否从主机设备接收到认证请求。此处，认证请求是来自主机设备以便提供包含用于认证附件设备的数字签名的认证响应的请求。当判断 716 确定未接收到认证请求时，附件设备处理 700 等待这种请求。一旦判断 716 确定收到了认证请求，则从认证请求中提取 718 主机随机数。认证请求至少包括在认证处理中使用的主机随机数。

[0090] 然后获得 720 附件设备内部的私钥。然后可以至少使用主机随机数、私钥和设备随机数计算 722 设备数字签名。在附件设备内产生或可得到设备随机数。设备数字签名是主机设备将用于认证附件设备的加密值。向主机设备发送 724 认证响应。这样形成认证响应，从而它至少包括该设备数字签名。

[0091] 然后判断 726 确定是否从主机设备收到设备认证状态。当判断 726 确定未收到设备认证状态时，附件设备处理 700 等待这种信息。一旦判断 726 确定已经收到设备认证状态，可以将设备认证状态存储 728 在附件设备上。在方框 728 之后，附件设备处理 700 结束。

[0092] 图 8A-8C 是根据本发明的一个实施例的主机设备处理 800 的流程图。主机设备处理 800 开始于判断 802，判断 802 确定是否从附件设备收到认证控制信息。当判断 802 确定未收到认证控制信息时，主机设备处理 800 等待这种信息。一旦判断 802 确定已经收到了认证控制信息，主机设备处理 800 继续。换言之，一旦收到认证控制信息，则有效地调用主机设备处理 800。

[0093] 当主机设备处理 800 继续时，可以重置（即，清除）804 设备认证状态。因此，认为附件设备不可信，直到认证处理能够认证附件设备为止。该操作可能已经自动地在主机设备处发生了，诸如当从主机设备断开附件设备时。

[0094] 然后判断 806 基于认证控制信息确定附件设备是否支持认证。当判断 806 确定附

件设备不支持认证时，主机设备处理 800 结束，而不认证附件设备。在该情况下，可以约束，甚至阻止附件设备与主机设备互操作。

[0095] 在另一方面，当判断 806 确定附件设备支持认证时，主机设备处理 800 继续。此时，向附件设备发送 808 设备认证信息请求。然后判断 810 确定是否收到设备认证信息。当判断 810 确定未收到设备认证信息时，主机设备处理 800 等待接收这种信息。一旦判断 810 确定已经收到设备认证信息，判断 812 确定此时是否执行认证。此处应当理解，主机设备处理 800 可以在将附件设备连接到主机设备时即刻就执行认证，或可以推迟认证直到稍后的时刻，诸如当附件设备希望（例如，第一次希望）使用仅对认证的设备可用的主机设备的扩展特征时周期地进行。因此，当判断 812 确定不立刻需要认证时，主机设备处理 800 可以等待适合的时刻执行认证处理。一旦判断 812 确定应当执行认证，则产生 814 主机随机数。接着，向附件设备发送 816 认证请求。该认证请求至少包括已经产生 814 的主机随机数。

[0096] 然后判断 818 确定是否从附件设备收到认证响应。当判断 818 确定已经收到认证响应时，从认证响应中提取 820 设备数字签名。还获得 822 用于附件设备的公钥。在一个实施例中，主机设备包括与不同设备标识符相关联的多个公钥。因此，来自附件设备的设备认证信息可以包括用于附件设备的设备标识符。在获得 822 用于附件设备的公钥时可以使用该设备标识符。作为例子，可以使用认证表，诸如图 6C 中所示的认证表 650 获得公钥。

[0097] 接着，使用公钥验证 824 设备数字签名。在一个实施例中，数字设备签名的验证 824 还使用主机随机数。然后判断 826 确定是否已经验证了数字设备签名。当判断 826 确定已经验证了数字设备签名时，认为 828 附件设备可信。可以更新 830 与附件设备相关联的命令访问许可，从而主机设备允许附件设备使用被认证的设备允许的那些命令。在另一方面，当判断 826 确定未验证数字设备签名时，认为 832 附件设备不可信。在方框 830 和 832 之后，向附件设备发送 834 设备认证状态。设备认证状态起通知附件设备主机设备是否已经认证该附件设备的作用。

[0098] 如果设备认证状态指出附件设备被认为可信，则附件设备可以进而根据对使用的授权程度与主机设备交互。作为另一个例子，当设备认证状态指出附件设备被认为不可信时，则可以约束，甚至阻止附件设备与主机设备交互。在任何情况下，当认为附件设备可信时，将附件设备用于主机设备的授权程度更大。

[0099] 图 9A-9C 是根据本发明的一个实施例的附件设备处理 900 的流程图。图 10A 和 10B 是根据本发明的一个实施例的主机设备处理 1000 的流程图。在认证处理中当试图认证主机设备时，由附件设备执行附件设备处理 900。在关于附件设备的认证处理中，由主机设备执行主机设备处理 1000。主机设备处理 1000 是附件设备处理 900 的配对处理。换言之，在认证处理中，在附件设备内的主机设备间存在信息交换。因此，图 9A-9C 表示在认证处理的一个实施例中，由附件设备执行的处理，并且图 10A 和 10B 表示由主机设备执行的处理。应当理解，虽然在这些图中示出的认证处理被示出为大体上是顺序的，可以认为认证处理是一种协议，附件设备和主机设备使用该协议交换不仅用于认证，而且用于后续操作的信息。在一个实施例中，可以认为这种协议大体上是并行的，诸如在客户机 - 服务器或主 - 从实现中。

[0100] 图 9A-9C 是根据本发明的一个实施例的附件设备处理 900 的流程图。当试图认证与附件设备连接的主机设备时，由附件设备执行附件设备处理 900。

[0101] 附件设备处理 900 开始于判断 902。判断 902 确定附件设备是否连接到主机设备。当判断 902 确定附件设备未连接到主机设备时，附件设备处理 900 等待这种连接。换言之，当附件设备连接到主机设备时，有效地调用附件设备处理 900。在一个实施例中，一旦确定附件设备刚刚新近连接到主机设备，则调用附件设备处理 900。然而，在其他实施例中，可以稍后（例如，推迟）执行认证处理。

[0102] 一旦判断 902 确定附件设备连接到了主机设备，则向主机设备发送 904 认证控制信息。然后判断 906 确定是否确认了认证控制信息。当判断 906 确定已经确认了认证控制信息时，可以清除 908 附件设备的认证状态。此处，当连接主机设备时，通过清除 908 认证状态，由附件设备认证。

[0103] 接着向主机设备发送 910 主机认证信息请求。然后判断 912 确定是否从主机设备收到主机认证信息。当判断 912 确定未从主机设备收到主机认证信息时，附件设备处理 900 等待这种信息。

[0104] 一旦判断 912 确定收到了主机认证信息，判断 914 确定是否应在此时执行认证。此处，应当注意，可以立刻执行认证处理，诸如在检测到连接后立刻进行，或可以推迟直到稍后的一个时刻为止，诸如当需要主机设备的命令或扩展功能时。在任何情况下，当判断 914 确定此时不执行认证处理时，附件设备处理 900 可以等待适合的时刻执行认证。

[0105] 一旦判断 914 确定应当执行认证，则产生 916 设备随机数。然后，向主机设备发 918 认证请求。认证请求通常至少包括设备随机数和私钥数。私钥数用于在主机设备处选择私钥。

[0106] 接着，判断 920 确定是否从主机设备收到认证响应。当判断 920 确定未收到认证响应时，则附件设备处理 900 等待这种响应。一旦判断 920 确定已经收到认证响应，则从认证响应中提取 922 主机数字签名。另外，基于公钥索引获得 924 公钥。在一个实施例中，将公钥索引与主机认证信息一起提供给附件设备。在一个实施例中，使用公钥索引在附件设备处确定公钥。例如，附件设备可以包括多个不同的公钥，并且可由公钥索引标识这些公钥中将使用的适当的一个。

[0107] 然后，使用公钥验证 926 主机数字签名。验证 926 还使用设备随机数。之后，判断 928 确定是否已经验证了主机数字签名。当判断 928 确定已经验证了主机数字签名时，认为 930 主机设备可信。从而，更新 932 由该主机设备使用的命令访问许可。例如，由于验证了主机设备，认为至少在命令访问许可的程度上，主机设备和附件设备间的交互被授权了。可替换地，当判断 928 确定未验证主机设备时，认为 934 主机设备不可信。在方框 932 和 934 之后，可以将主机认证状态发送 936 给主机设备。此处，主机认证状态向主机设备通知认证处理的结果。在方框 936 之后，附件设备处理 900 完成并且结束。

[0108] 图 10A 和 10B 是根据本发明的一个实施例的主机设备处理 1000 的流程图。在与附件设备交互的同时，在主机设备上执行主机设备处理 1000。主机设备处理 1000 表示认证处理中附件设备处理 900 的配对处理。

[0109] 主机设备处理 1000 开始于判断 1002，判断 1002 确定是否从附件设备收到认证控制信息。当判断 1002 确定未收到认证控制信息时，主机设备处理 1000 等待这种信息。一旦判断 1002 确定已经收到了认证控制信息，主机设备处理 1000 继续。换言之，一旦收到认证控制信息，则有效地调用主机设备处理 1000。

[0110] 当主机设备处理1000继续时，重置1004设备认证状态，从而清除它可能具有的任何以前的认证状态。然后判断1006确定是否收到主机认证信息请求。当判断1006确定未收到主机认证信息请求时，主机设备处理1000等待这种请求。一旦判断1006确定已经收到主机认证信息请求，在主机设备处获得1008主机认证信息。然后将主机认证信息发送1010到附件设备。在一个实施例中，主机认证信息至少包括版本信息和公钥索引。

[0111] 接着，判断1012确定是否收到认证请求。当判断1012确定未收到认证请求时，主机设备处理1000等待这种请求。一旦判断1012确定已经收到认证请求，则从认证请求中提取1014设备随机数和私钥数。在该实施例中，应当理解，从附件设备收到的认证请求至少包括可由主机设备使用的设备随机数和私钥数。然后，基于私钥数获得1016私钥。此处，将获得1016的私钥在主机设备内部，并且通过使用私钥数标识。

[0112] 然后使用设备随机数、私钥和主机随机数计算1018主机数字签名。可以在主机设备处产生或可得到主机随机数。然后主机设备处理1000向附件设备发送1020认证响应。该认证响应至少包括主机数字签名。

[0113] 之后，判断1022确定是否收到了主机认证状态。当判断1022确定未收到主机认证状态时，主机设备处理1000等待这种信息。一旦判断1022确定已经收到主机认证状态，则将主机认证状态存储1024在主机设备处。此时，主机设备知道了它具有的关于附件设备的认证状态，并且从而可以操作。在方框1024之后，主机设备处理1000完成并且结束。

[0114] 根据本发明的另一个方面，电子设备或主机设备还可以连接主计算机，诸如个人计算机。该个人计算机可以存储、使用和管理媒体项目。媒体项目的管理不仅可以针对主计算机，而且可以针对电子设备。

[0115] 图11是根据本发明的一个实施例的媒体管理系统1100的方框图。媒体管理系统1100包括主计算机1102和媒体播放器1104。主计算机1102典型地是个人计算机。除了其他传统组件之外，主计算机包括管理模块1106，管理模块1106是软件模块。管理模块1106提供对不仅在主计算机1102上而且在媒体播放器1104上的媒体项目（和/或播放列表）的集中管理。更具体地，管理模块1106管理存储在与主计算机1102相关联的媒体存储1108内的媒体项目。管理模块1106还与媒体数据库1110交互，以便在媒体存储1108内存储与媒体项目相关联的媒体信息。

[0116] 媒体信息与媒体项目的特性或属性有关。例如，在音频或影音媒体的情况下，媒体信息可以包括下面的一个或多个：标题、相集、轨迹、演员、创作者和流派。媒体信息的这些类型特定于特定的媒体项目。另外，媒体信息可以与媒体项目的质量特性有关。媒体项目的质量特性的例子包括下面的一个或多个：位速率、采样速率、均衡器设置、音量调整、开始/停止和整个时间。

[0117] 另外，主计算机1102包括播放模块1112。播放模块1112是软件模块，其可以用于播放存储在媒体存储1108内的某些媒体项目。播放模块1112还可以显示（在显示屏上）或使用来自媒体数据库1110的媒体信息。典型地，感兴趣的媒体信息相应于将由播放模块1112播放的媒体项目。

[0118] 主计算机1102还包括通信模块1114，其与媒体播放器1104内的相应的通信模块1116耦合。连接或链路1118可去除地耦合通信模块1114和1116。在一个实施例中，连接或链路1118是本领域公知的提供数据总线诸如FIREWIRE™总线或USB总线的电缆。在另

一个实施例中，连接或链路 1118 是无线信道或通过无线网络的连接。因此，取决于实现，通信模块 1114 和 1116 可以用有线或无线的方式通信。

[0119] 媒体播放器 1104 还包括存储媒体播放器 1104 内的媒体项目的媒体存储 1120。可选择地，媒体存储 1120 还可以存储数据，即，非媒体项目存储。通常通过连接或链路 1118 从主计算机 1102 接收存储到媒体存储 1120 的媒体项目。更具体地，管理模块 1106 将所有或某些驻留在媒体存储 1108 上的媒体项目在连接或链路 1118 上发送到媒体播放器 1104 内的媒体存储 1120。另外，可以将同样从主计算机 1102 传递到媒体播放器 1104 的媒体项目的相应的媒体信息存储在媒体数据库 1122 内。就此而言，可以在连接或链路 1118 上将来自主计算机 1102 内的媒体数据库 1110 的某些媒体信息发送到媒体播放器 1104 内的媒体数据库 1122。另外，可以由管理模块 1106 将标识某些媒体项目的播放列表在连接或链路 1118 上发送到媒体存储 1120 或媒体播放器 1104 内的媒体数据库 1122。

[0120] 另外，媒体播放器 1104 包括耦合到媒体存储 1120 和媒体数据库 1122 的播放模块 1124。播放模块 1124 是软件模块，其可用于播放存储在媒体存储 1120 内的某些媒体项目。播放模块 1124 还可以显示（在显示屏上）或使用来自媒体数据库 1122 的媒体信息。典型地，感兴趣的媒体信息相应于将由播放模块 1124 播放的媒体项目。

[0121] 根据一个实施例，为了在媒体播放器 1104 上支持认证处理，媒体播放器 1104 还可以包括认证模块 1126 和认证表 1128。在一个实现中，认证模块 1126 和认证表 1128 可以分别相应于上面参考图 2B 描述的认证模块 252 和认证表 254。

[0122] 如前所述，附件设备可以耦合到媒体播放器。因此，图 11 还示出了能够耦合到媒体播放器 1104 的附件设备 1130。根据一个实施例，附件设备 1130 还可以包括认证设备 1132。根据一个实施例，认证设备 1132 操作以便支持媒体播放器 1104 上的认证处理。在一个实现中，认证设备 1132 可以相应于上面参考图 2A 描述的认证控制器 200。

[0123] 在一个实施例中，媒体播放器 1104 具有有限的或没有能力管理媒体播放器 1104 上的媒体项目。然而，主计算机 1102 内的管理模块 1106 可以间接地管理驻留在媒体播放器 1104 上的媒体项目。例如，为了将媒体项目“添加”到媒体播放器 1104，管理模块 1106 起识别媒体存储 1108 中将要添加到媒体播放器 1104 的媒体项目，并且然后使得识别出的媒体项目被传递到媒体播放器 1104 的作用。作为另一个例子，为了从媒体播放器 1104“删除”媒体项目，管理模块 1106 起识别将要从媒体存储 1108 中删除的媒体项目，并且然后使得从媒体播放器 1104 删除识别出的媒体项目的作用。作为另一个例子，如果在主计算机 1102 处使用管理模块 1106 进行媒体项目的特性的改变（即，更改），则这种特性也可以被延及到媒体播放器 1104 上的相应的媒体项目。在一个实现中，在媒体播放器 1104 上的媒体项目和主计算机 1102 上的媒体项目的同步过程中，在批类处理中发生添加、删除和 / 或改变。

[0124] 在另一个实施例中，媒体播放器 1104 具有有限的或没有能力管理媒体播放器 1104 上的播放列表。然而，主计算机 1102 内的管理模块 1106 通过对驻留在主计算机上的播放列表的管理，可以间接地管理驻留在媒体播放器 1104 上的播放列表。就此而言，可以在主计算机 1102 上执行对播放列表的添加、删除或改变，并且然后当被传递到媒体播放器 1104 时，延及媒体播放器 1104。

[0125] 如前所述，同步是一种媒体管理形式。前面在上面和在上面提及的相关应用中也

讨论了自动启动同步的能力。然而，另外，可以限制设备间的同步，从而在主计算机和媒体播放器不认识彼此时防止自动同步。

[0126] 根据一个实施例，当媒体播放器第一次连接到主计算机时（或甚至更一般地，当未出现匹配的标识符时），询问媒体播放器的用户该用户是否希望将媒体播放器纳入主计算机、分配给主计算机或相当于主计算机锁定媒体播放器。当媒体播放器的用户选择将媒体播放器纳入主计算机、分配给主计算机或相当于主计算机锁定媒体播放器时，获得伪随机标识符，并且将其存储在媒体数据库或主计算机和媒体播放器两者的文件内。在一个实现中，标识符是与主计算机或其管理模块相关联（例如，主计算机或其管理模块知道或产生的）标识符，并且将这种标识符发送并且存储在媒体播放器内。在另一个实现中，标识符与媒体播放器相关联（例如，媒体播放器知道或产生的），并且将其发送并且存储在文件或主计算机的媒体数据库内。

[0127] 图 12 是根据本发明的一个实施例的媒体播放器 1200 的方框图。媒体播放器 1200 包括与用于控制媒体播放器 1200 的整体操作的微处理器或控制器有关的处理器 1202。媒体播放器 1200 在文件系统 1204 和缓存 1206 中存储与媒体项目有关的媒体数据。文件系统 1204 典型地是存储设备。文件系统 1204 典型地为媒体播放器 1200 提供高容量的存储能力。例如，该存储设备可以是基于半导体的存储器，诸如 FLASH 存储器。文件系统 1204 不仅可以存储媒体数据，而且可以存储非媒体数据（例如，当在数据模式中操作时）。然而，由于对文件系统 1204 的访问时间相对地慢，媒体播放器 1200 还可以包括缓存 1206。缓存 1206 是例如以半导体存储器提供的随机访问存储器 (RAM)。对缓存 1206 的相对访问时间大体上比对文件系统 1204 的短。然而，缓存 1206 不具有文件系统 1204 的大存储容量。另外，文件系统 1204，当激活时，比缓存 1206 消耗更多电能。当媒体播放器 1200 是由电池（未示出）供电的便携媒体播放器时，电能消耗通常是至关重要的。媒体播放器 1200 还包括 RAM 1220 和只读存储器 (ROM)1222。ROM 1222 可以以非易失方式存储将执行的程序、工具或处理。RAM 1220，诸如为缓存 1206，提供易失的数据存储。在一个实施例中，可以由提供文件系统 1204 的存储设备提供 RAM 1220 和 ROM1222。

[0128] 媒体播放器 1200 还包括允许媒体播放器 1200 的用户与媒体播放器 1200 交互的用户输入设备 1208。例如，用户输入设备 1208 可以采取各种形式，诸如按钮、键盘、拨数盘等。另外，媒体播放器 1200 包括可以由处理器 1202 控制以便向用户显示信息的显示器 1210（屏幕显示）。在触摸屏的情况下，用户输入设备 1208 和显示器 1210 还可以组合在一起。数据总线 1211 可以便于至少文件系统 1204、缓存 1206、处理器 1202 和 CODEC1212 间的数据传输。

[0129] 在一个实施例中，媒体播放器 1200 起在文件系统 1204 内存储多个媒体项目（例如，歌曲）的作用。当用户希望媒体播放器播放特定的媒体项目时，在显示器 1210 上显示可得到的媒体项目的列表。然后，使用用户输入设备 1208，用户可以选择可得到的媒体项目中的一个。在收到对特定媒体项目的选择后，处理器 1202 向编码器 / 解码器 (CODEC)1212 提供特定媒体项目的媒体数据（例如，声音文件）。然后 CODEC 1212 为扬声器 1214 产生模拟输出信数。扬声器 1214 可以是媒体播放器 1200 内部的或媒体播放器 1200 外部的扬声器。例如，认为连接到媒体播放器 1200 的耳机 (headphone 或 earphone) 是外部扬声器。

[0130] 媒体播放器 1200 还包括耦合到数据链路 1218 的网络 / 总线接口 1216。数据链路

1218 允许媒体播放器 1200 耦合到主计算机或附件设备。可以在有线连接或无线连接上提供数据链路 1218。在无线连接的情况下，网络 / 总线接口 1216 可以包括无线收发器。

[0131] 在一个实施例中，主计算机可以利用驻留在主计算机上的应用，以便允许使用播放列表（包括媒体设备列表）以及提供播放列表的管理。一种这样的应用是由 Cupertino，CA 的 Apple Computer 公司出品的iTunes®版本 4.2。

[0132] 媒体项目（媒体资产）可以与一种或多种不同类型的媒体内容有关。在一个实施例中，媒体项目是音频轨迹。在另一个实施例中，媒体项目是图像（例如，相片）。然而，在其它实施例中，媒体项目可以是音频、图形或视频内容的任何组合。

[0133] 上面的讨论提到了用于密码方法以便认证附件设备或主机设备的随机数。上面讨论的密码方法可以使用随机数、公 - 私密钥对和认证算法。随机数还可以称为随机 digest。公 - 私密钥对和认证算法可以使用公 - 私密码系统，诸如公知的 RSA 算法或椭圆曲线密码 (ECC) 算法。使用 ECC 算法是有利的，ECC 算法以与 RSA 实现的典型的较大密钥（例如，1024 位）相比相对较小的密钥（例如，160 位），提供减少的存储器消耗。在提交于 2005 年 2 月 3 日的题目为“SMALLMEMORY FOOTPRINT FAST ELLIPTIC ENCRPTION”的相关美国专利申请 No. :11/____ 中描述了减少存储器的 ECC 算法的例子，通过引用将其结合在内。

[0134] 可以单独或以任意组合使用本发明的各个方面、实施例、实现或特征。

[0135] 本发明可以实现为软件、硬件或硬件和软件的组合。本发明还可以表述为计算机可读介质上的计算机可读代码。计算机可读介质是可以存储数据的任意数据存储设备，之后可以由计算机系统读取该数据。计算机可读介质的例子包括只读存储器、随机访问存储器、CD-ROM、DVD、磁带、光学数据存储设备和载波。计算机可读介质还可以分布在联网计算机系统上，从而以分布的方式存储和执行计算机可读代码。

[0136] 本发明的优点有许多。不同的方面、实施例或实现可以产生下面的一个或多个优点。本发明的一个优点是可以控制对附件设备与主机设备的交互。结果，电子设备可以将对它的某些或全部特征的使用仅限于认为被授权的附件设备。本发明的另一个优点是提供管理被允许用于主机设备的那些附件设备的质量的能力。通过管理附件设备的质量，电子设备的操作不太可能被劣等的附件设备的附接所玷污。本发明的另一个优点是认证处理可以基于制造商或设备控制对电子设备的某些特征的访问。

[0137] 从给出的描述中可以明了本发明的许多特征和优点，并且因此旨在由所附权利要求覆盖本发明的所有这些特征和优点。另外，由于本领域的技术人员容易想到许多修改和变更，本发明不应被限制为示出和描述的确切的构造和操作。因此，可以采用所有适合的修改和等同物，只要其落在本发明的范围内。

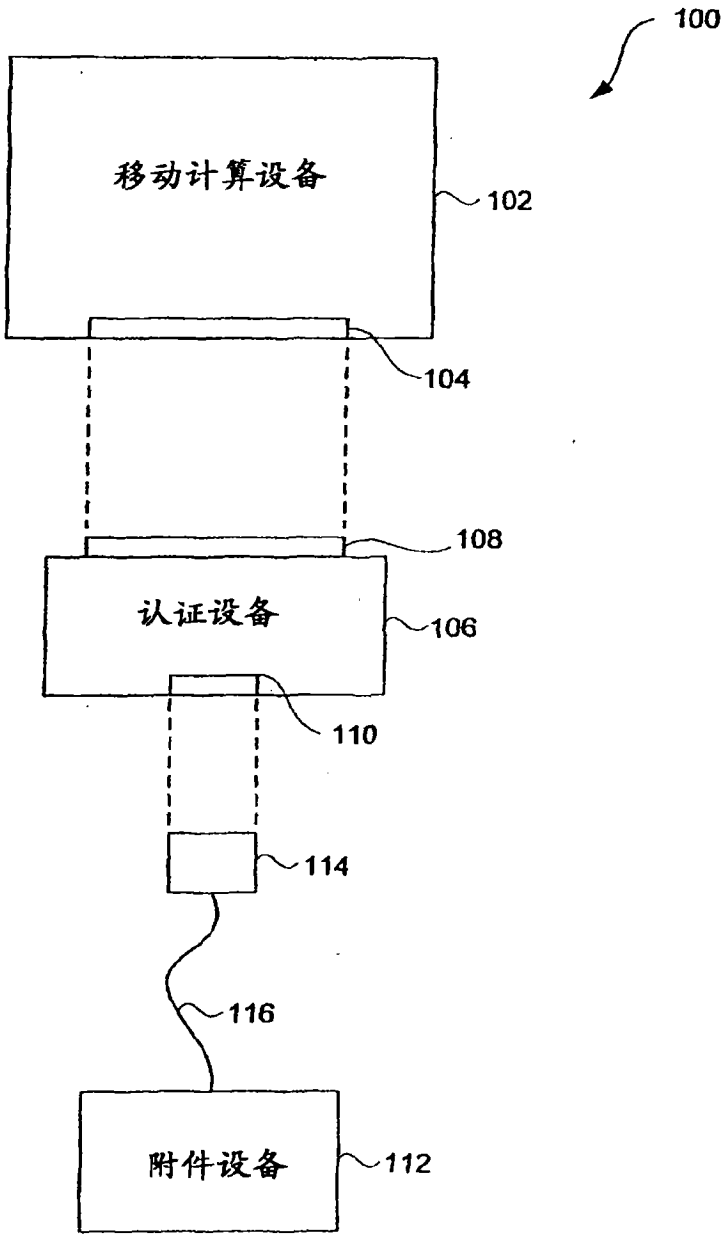


图 1A

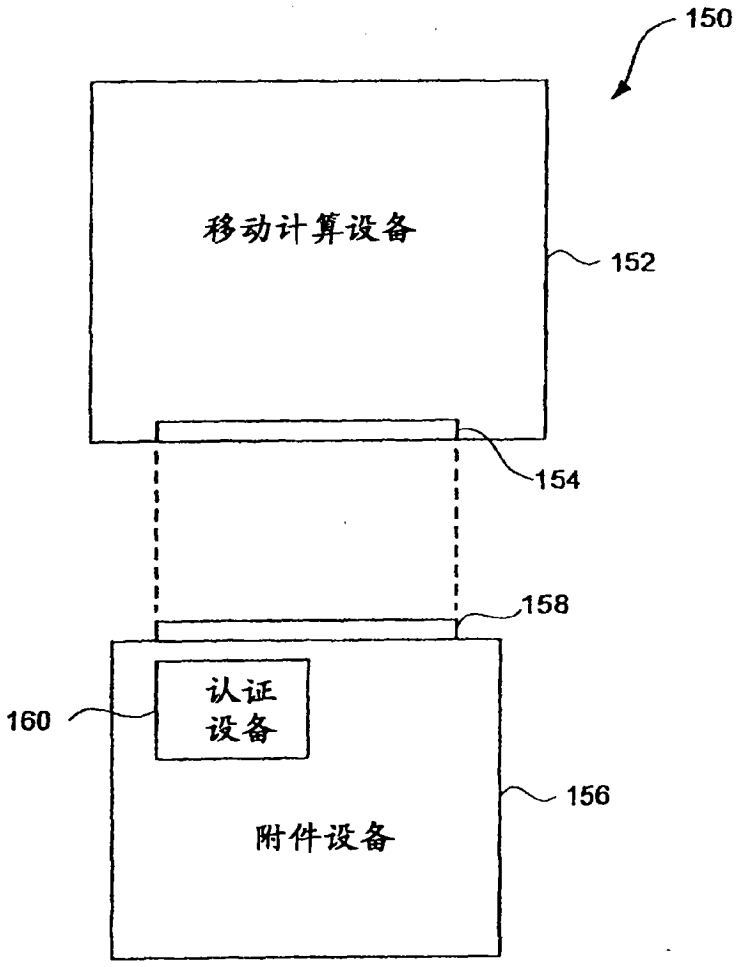


图 1B

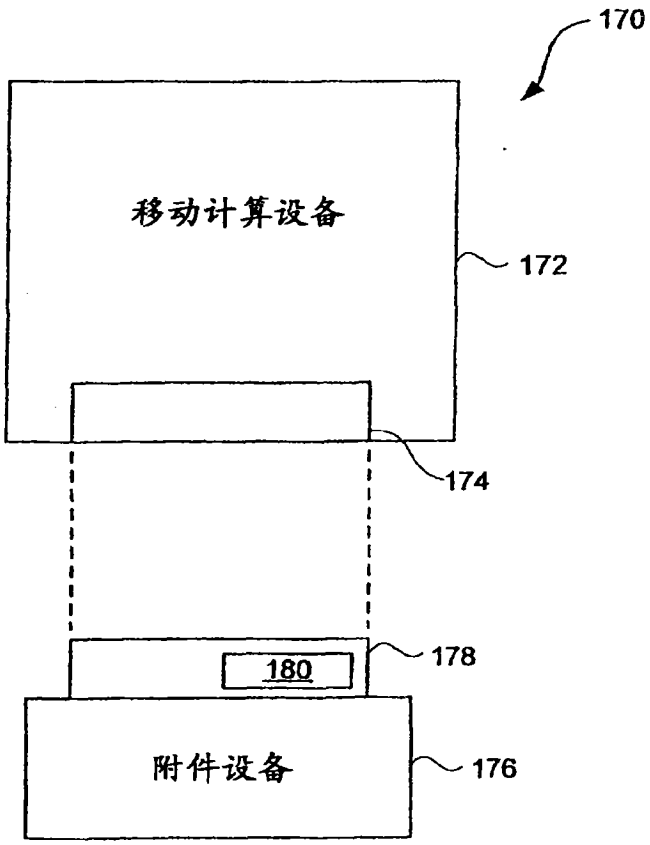

170
移动计算设备
172
174
180
178
附件设备
176

图 1C

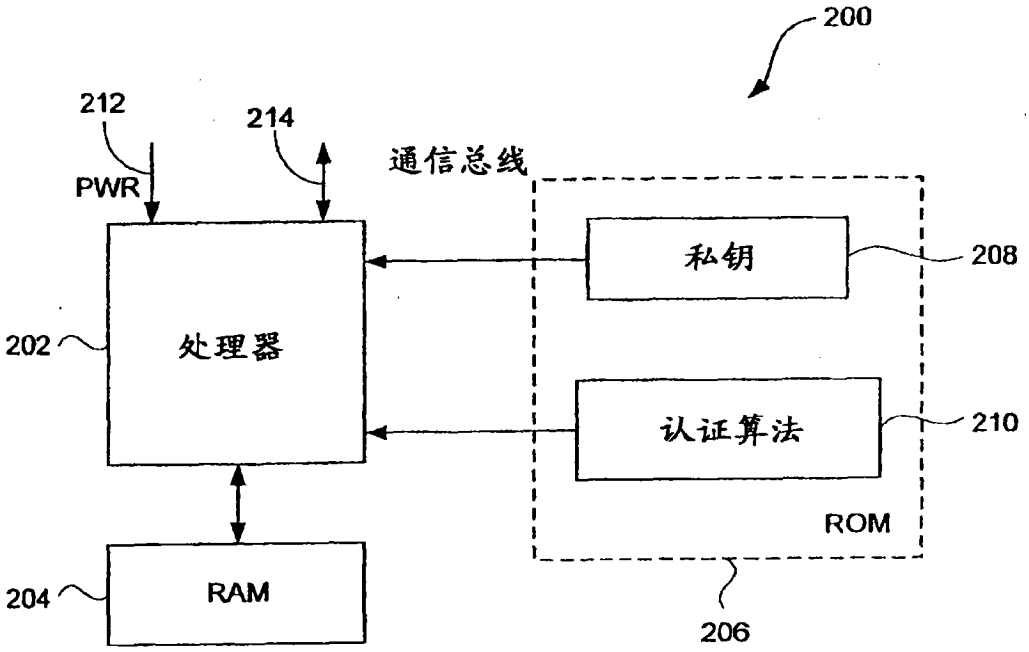

200
212
214
PWR
通信总线
私钥
208
202
处理器
认证算法
210
ROM
RAM
204
206

图 2A

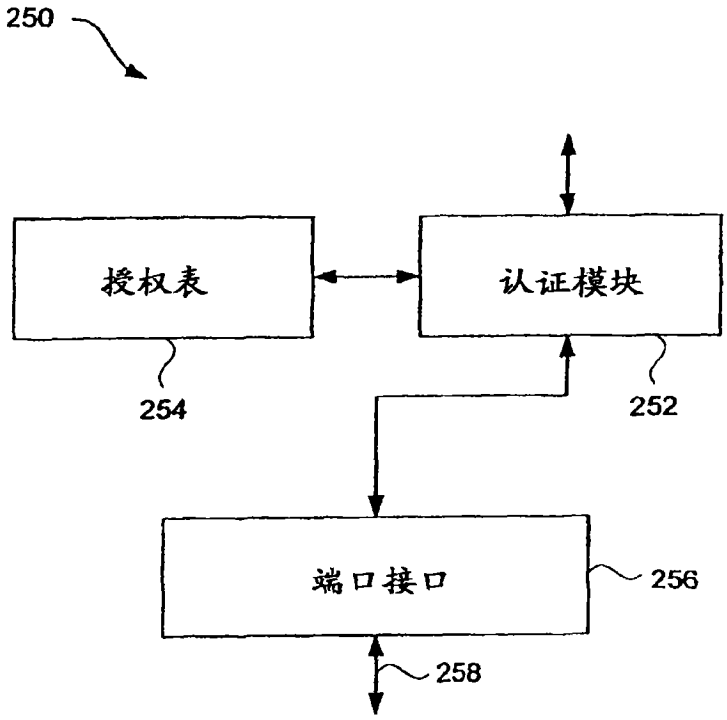

250
授权表
认证模块
254
252
端口接口
256
258

图 2B

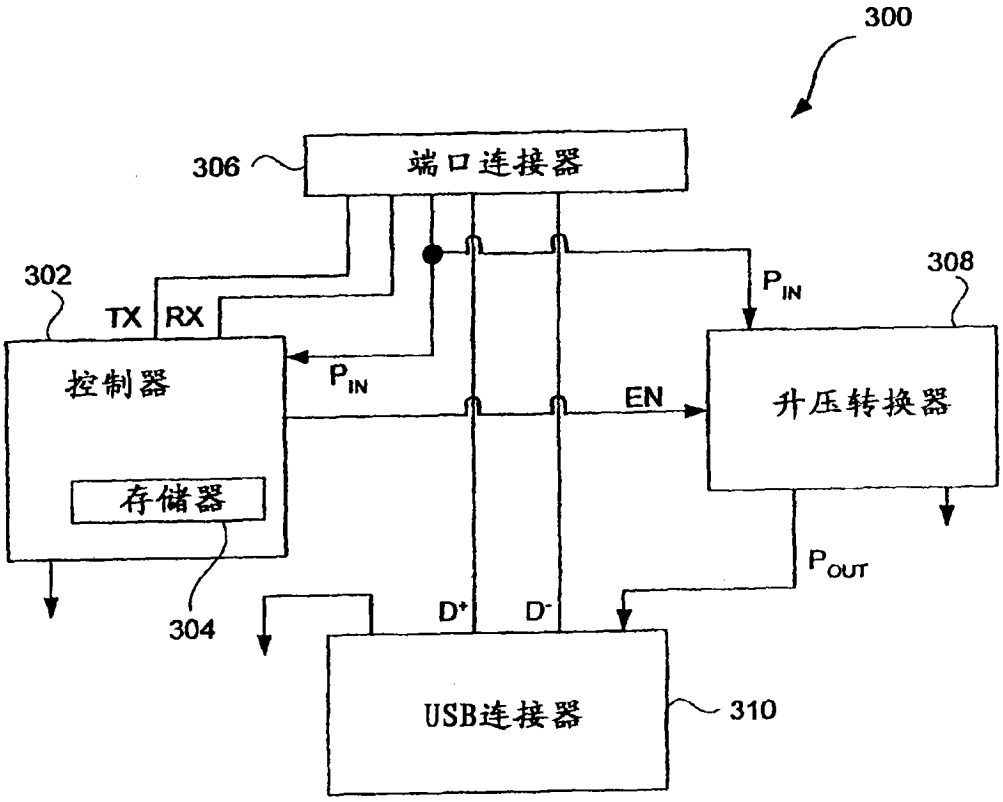

300
306
端口连接器
302
TX
RX
控制器
存储器
304
P_{IN}
P_{IN}
308
EN
升压转换器
P_{OUT}
D^+
D^-
USB连接器
310

图 3

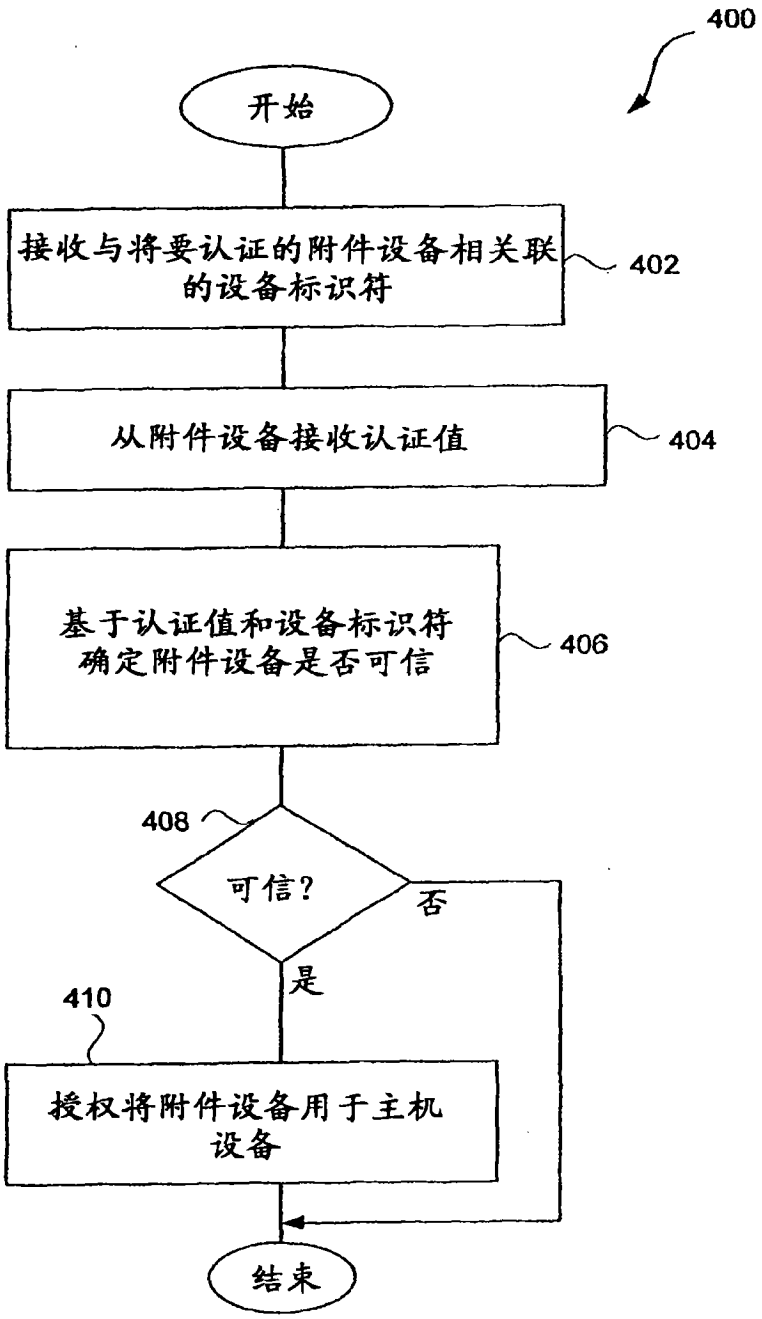

400
开始
接收与将要认证的附件设备相关联的设备标识符
402
从附件设备接收认证值
404
基于认证值和设备标识符确定附件设备是否可信
406
408
可信?
否
是
410
授权将附件设备用于主机设备
结束

图 4A

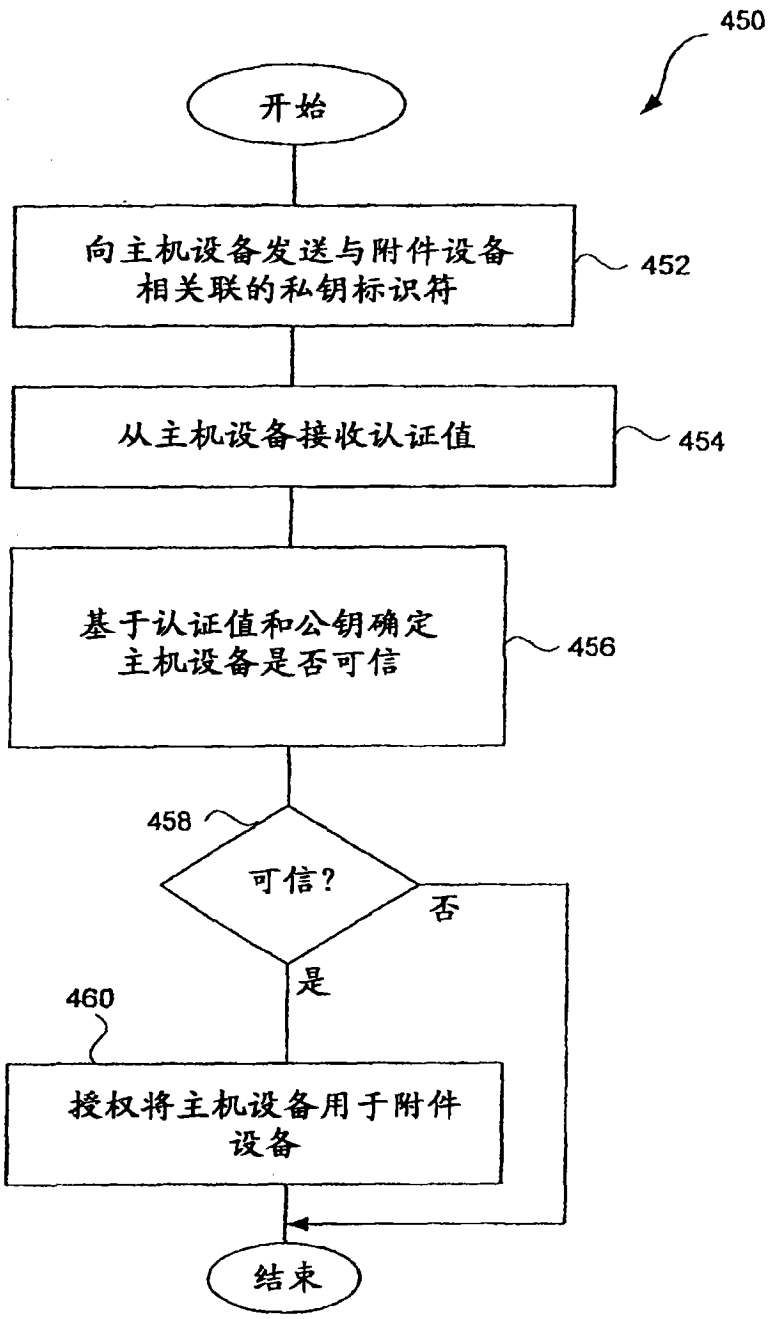

450
开始
向主机设备发送与附件设备相关联的私钥标识符
452
从主机设备接收认证值
454
基于认证值和公钥确定主机设备是否可信
456
458
可信?
否
是
460
授权将主机设备用于附件设备
结束

图 4B

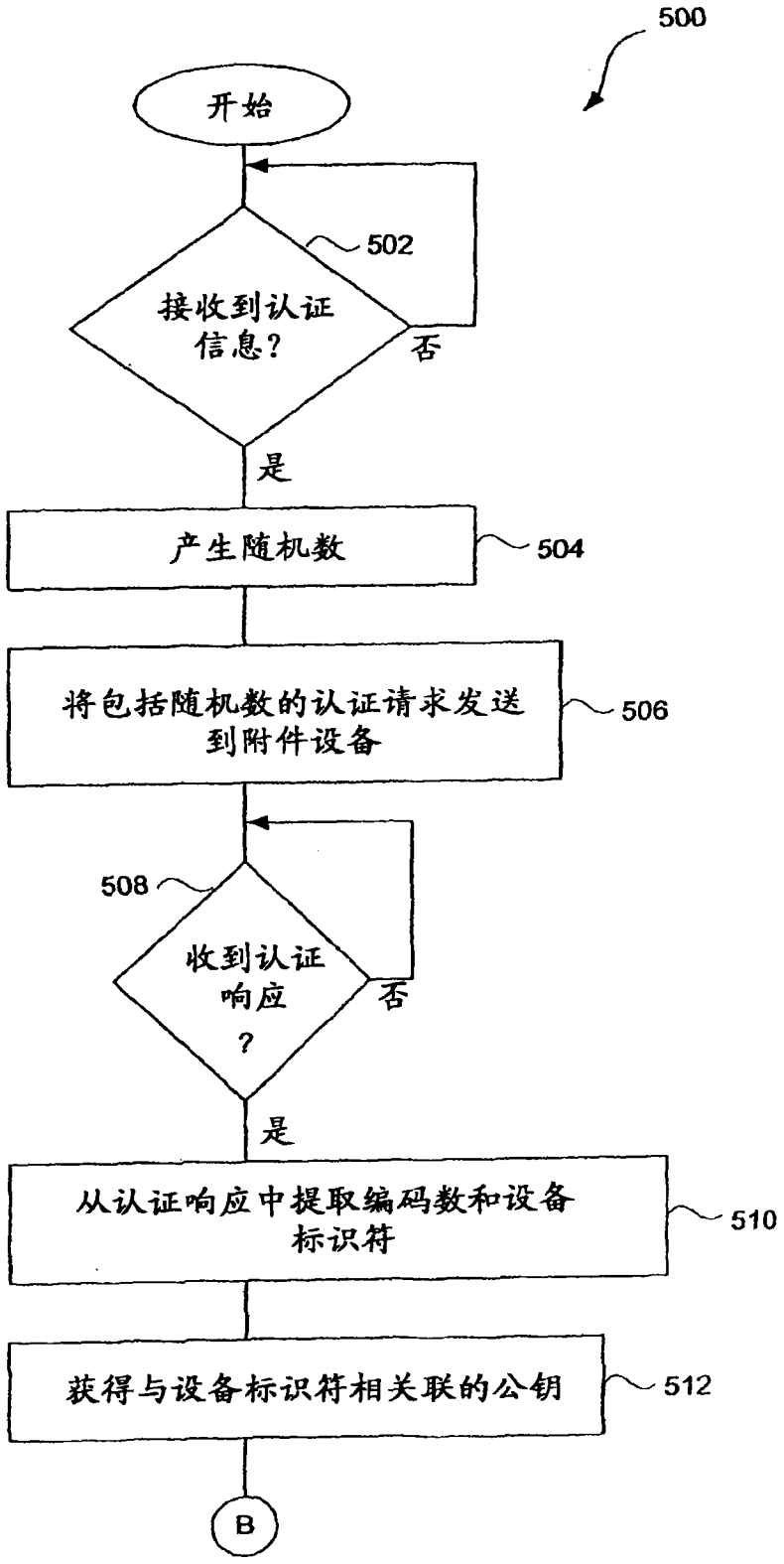

500
开始
502
接收到认证信息?
否
是
产生随机数
504
将包括随机数的认证请求发送到附件设备
506
508
收到认证响应?
否
是
从认证响应中提取编码数和设备标识符
510
获得与设备标识符相关联的公钥
512
B

图 5A

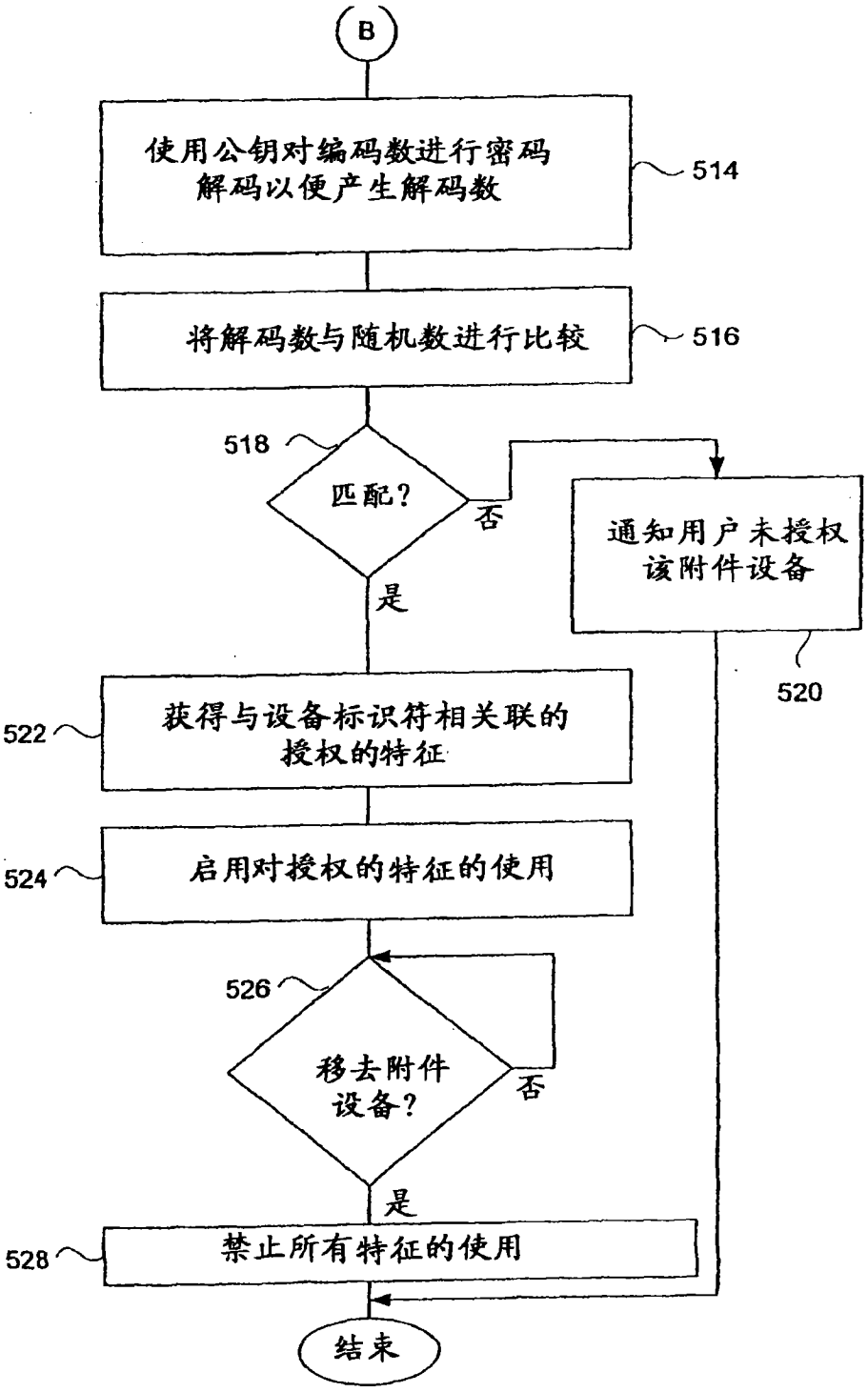

B
使用公钥对编码数进行密码解码以便产生解码数
514
将解码数与随机数进行比较
516
518
匹配?
否
是
通知用户未授权该附件设备
520
522
获得与设备标识符相关联的授权的特征
524
启用对授权的特征的使用
526
移去附件设备?
否
是
528
禁止所有特征的使用
结束

图 5B

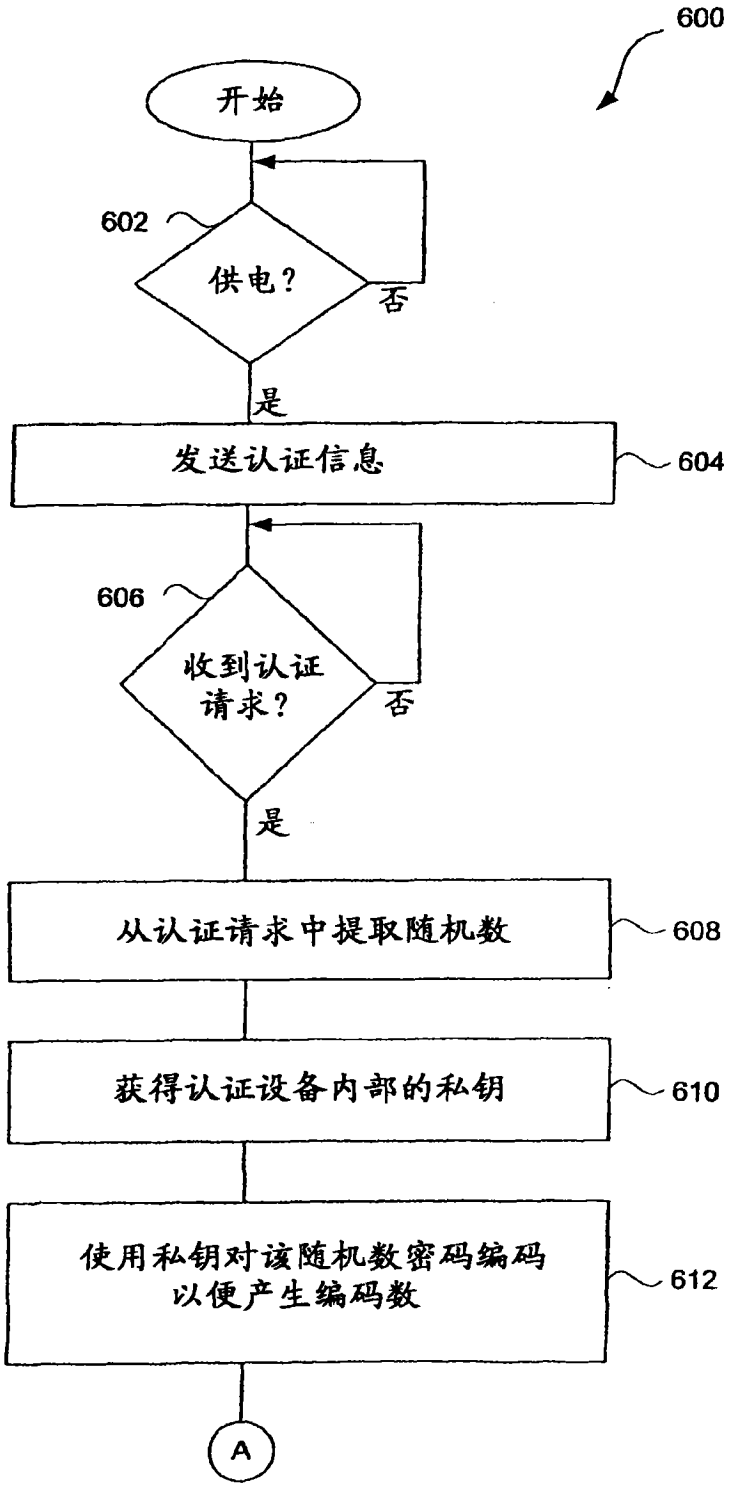

600
开始
602
供电？
否
是
发送认证信息
604
606
收到认证请求？
否
是
从认证请求中提取随机数
608
获得认证设备内部的私钥
610
使用私钥对该随机数密码编码以便产生编码数
612
A

图 6A

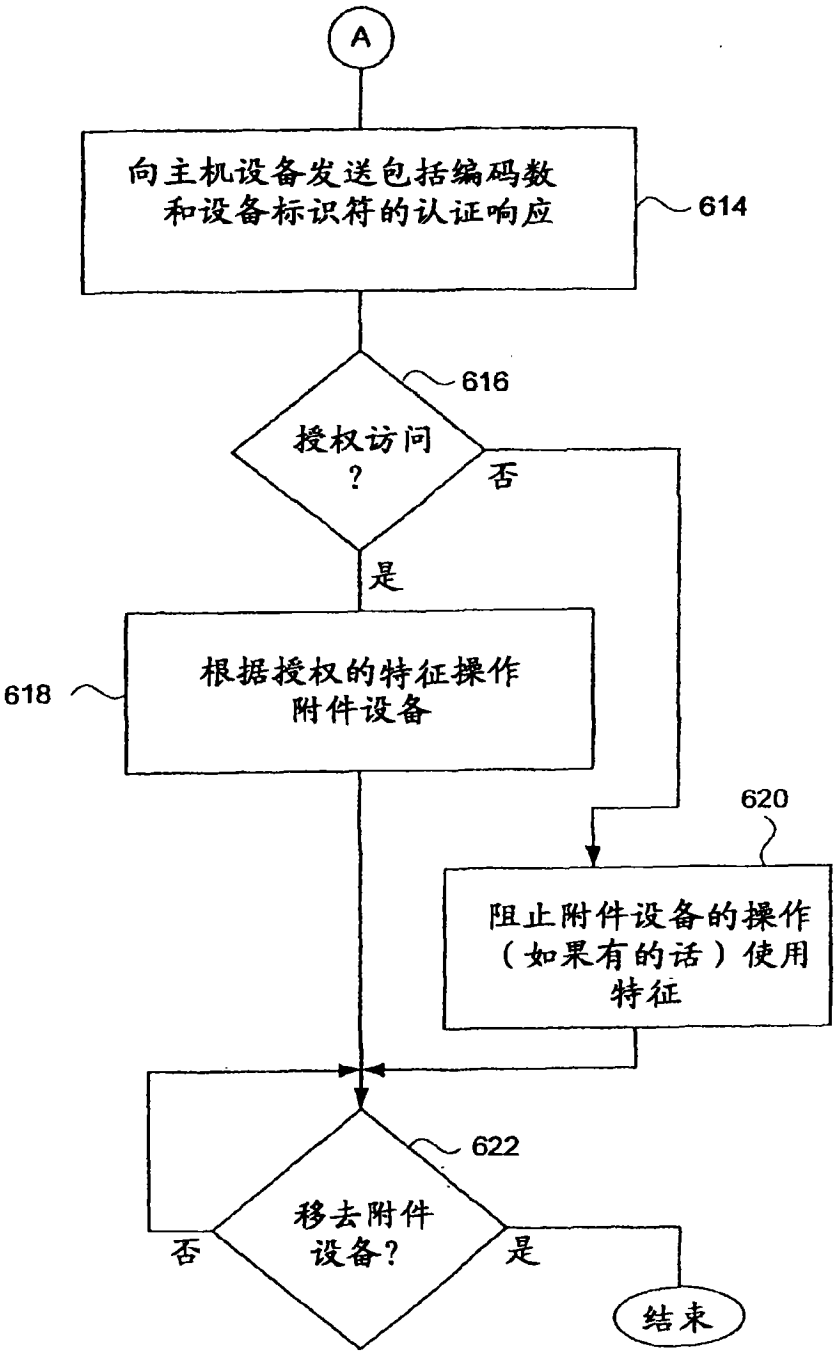

A
向主机设备发送包括编码数和设备标识符的认证响应
614
616
授权访问？
否
是
618
根据授权的特征操作附件设备
620
阻止附件设备的操作（如果有的话）使用特征
622
移去附件设备？
否
是
结束

图 6B

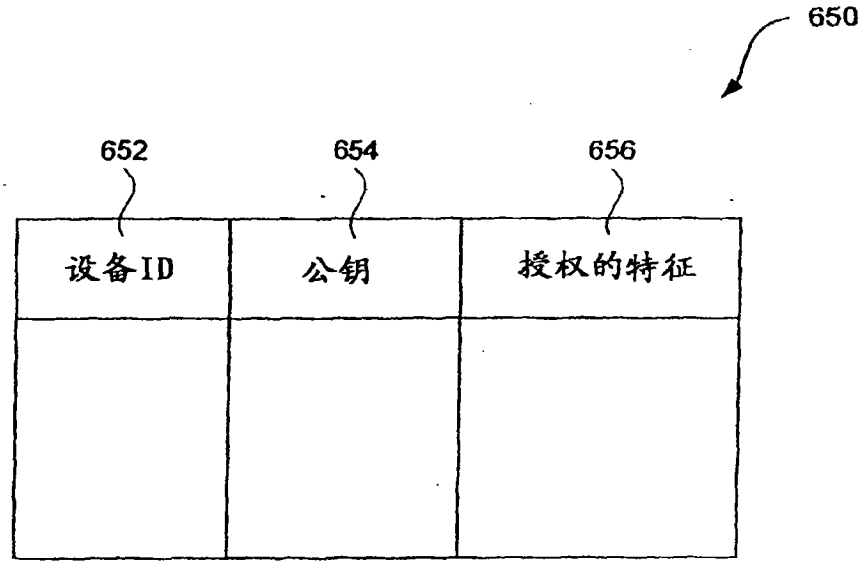


图 6C

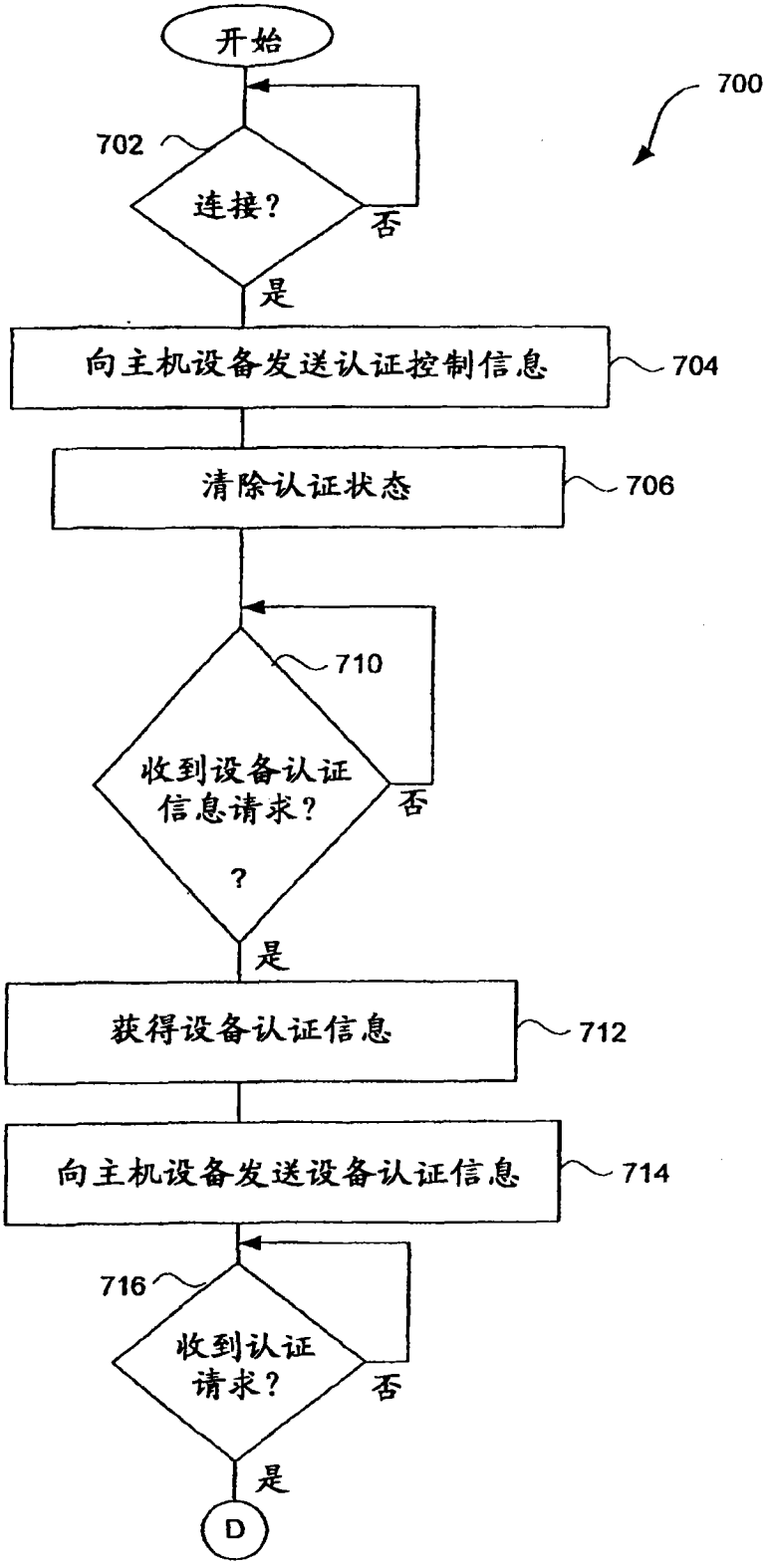

开始
700
702
连接?
否
是
向主机设备发送认证控制信息
704
清除认证状态
706
710
收到设备认证信息请求?
?
否
是
获得设备认证信息
712
向主机设备发送设备认证信息
714
716
收到认证请求?
否
是
D

图 7A

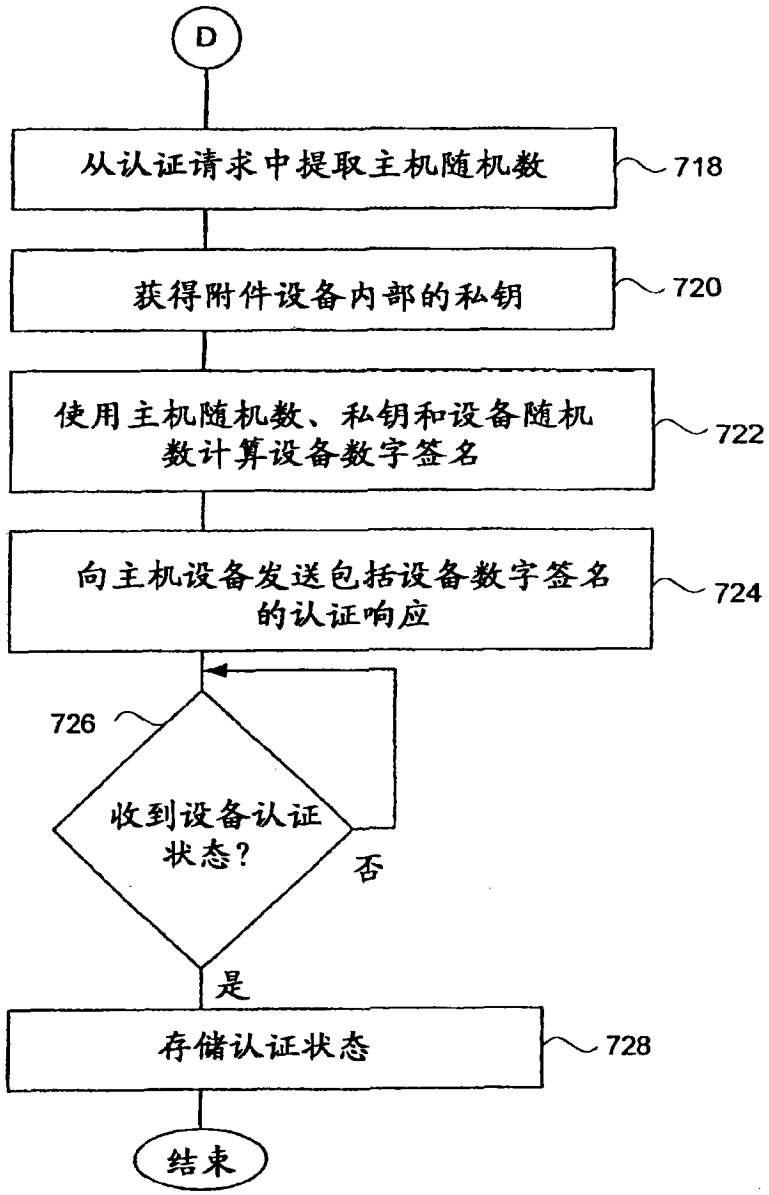

D
从认证请求中提取主机随机数
718
获得附件设备内部的私钥
720
使用主机随机数、私钥和设备随机数计算设备数字签名
722
向主机设备发送包括设备数字签名的认证响应
724
726
收到设备认证状态?
否
是
存储认证状态
728
结束

图 7B

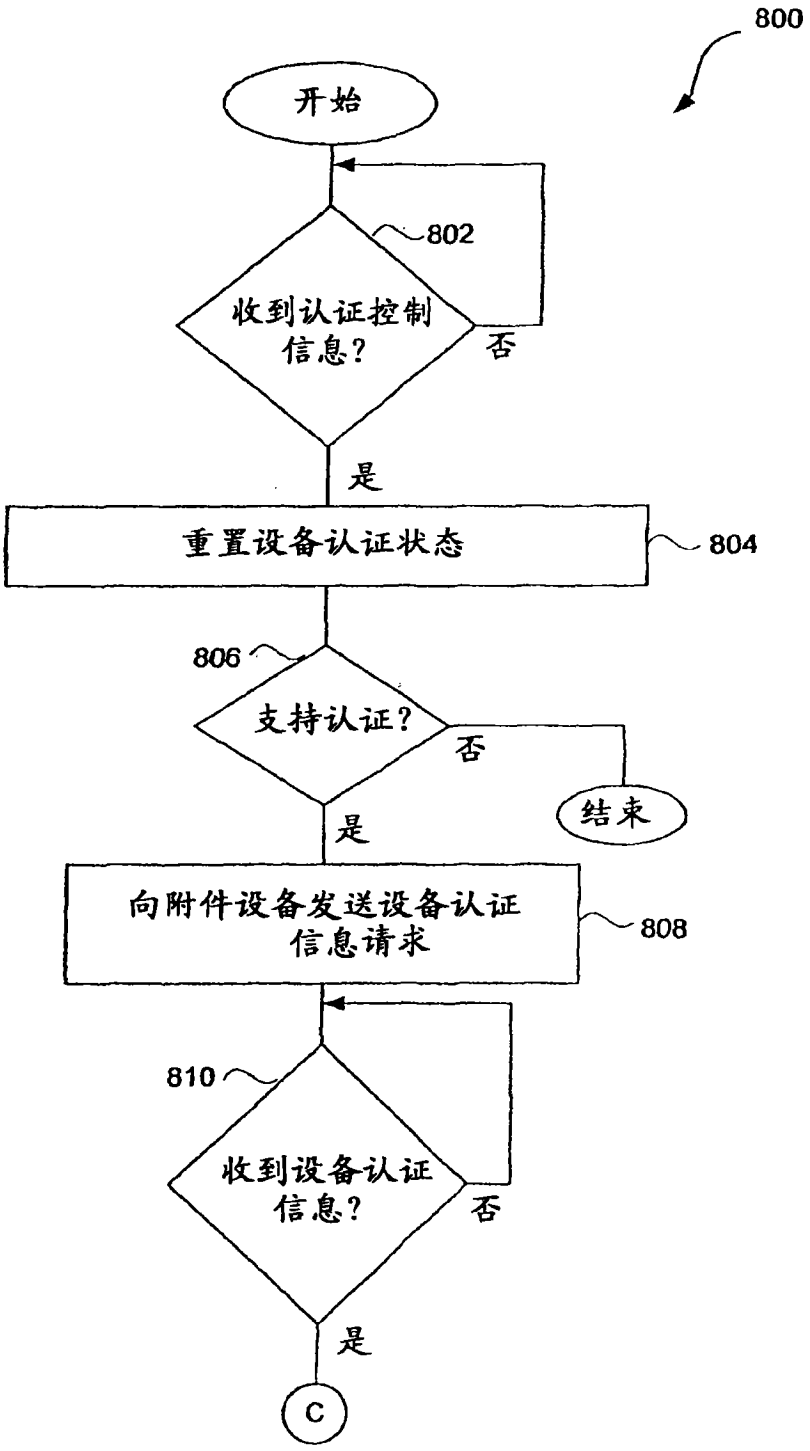

800
开始
802
收到认证控制信息?
否
是
重置设备认证状态
804
806
支持认证?
否
结束
是
向附件设备发送设备认证信息请求
808
810
收到设备认证信息?
否
是
C

图 8A

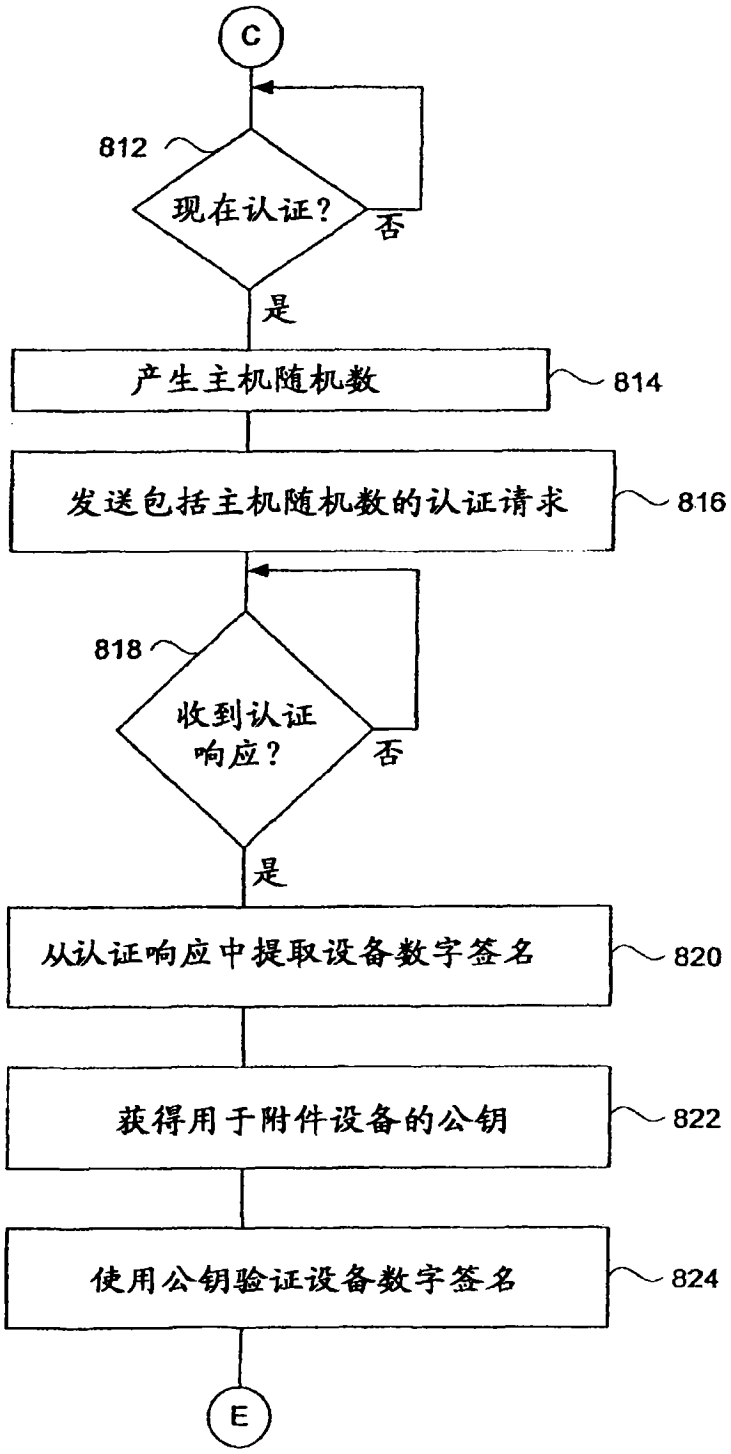

C
812
现在认证？
否
是
产生主机随机数
814
发送包括主机随机数的认证请求
816
818
收到认证响应？
否
是
从认证响应中提取设备数字签名
820
获得用于附件设备的公钥
822
使用公钥验证设备数字签名
824
E

图 8B

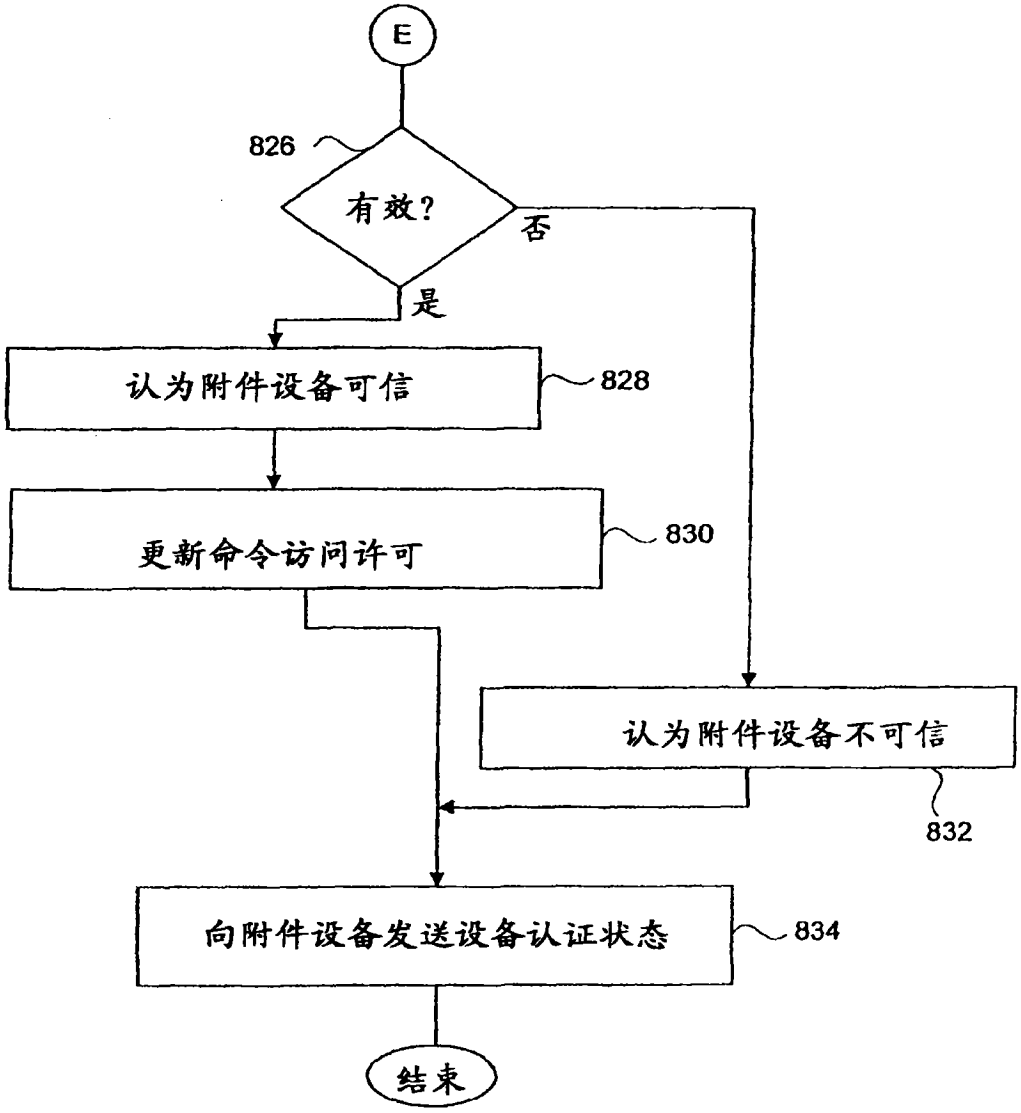

E
826
有效?
否
是
认为附件设备可信
828
更新命令访问许可
830
认为附件设备不可信
832
向附件设备发送设备认证状态
834
结束

图 8C

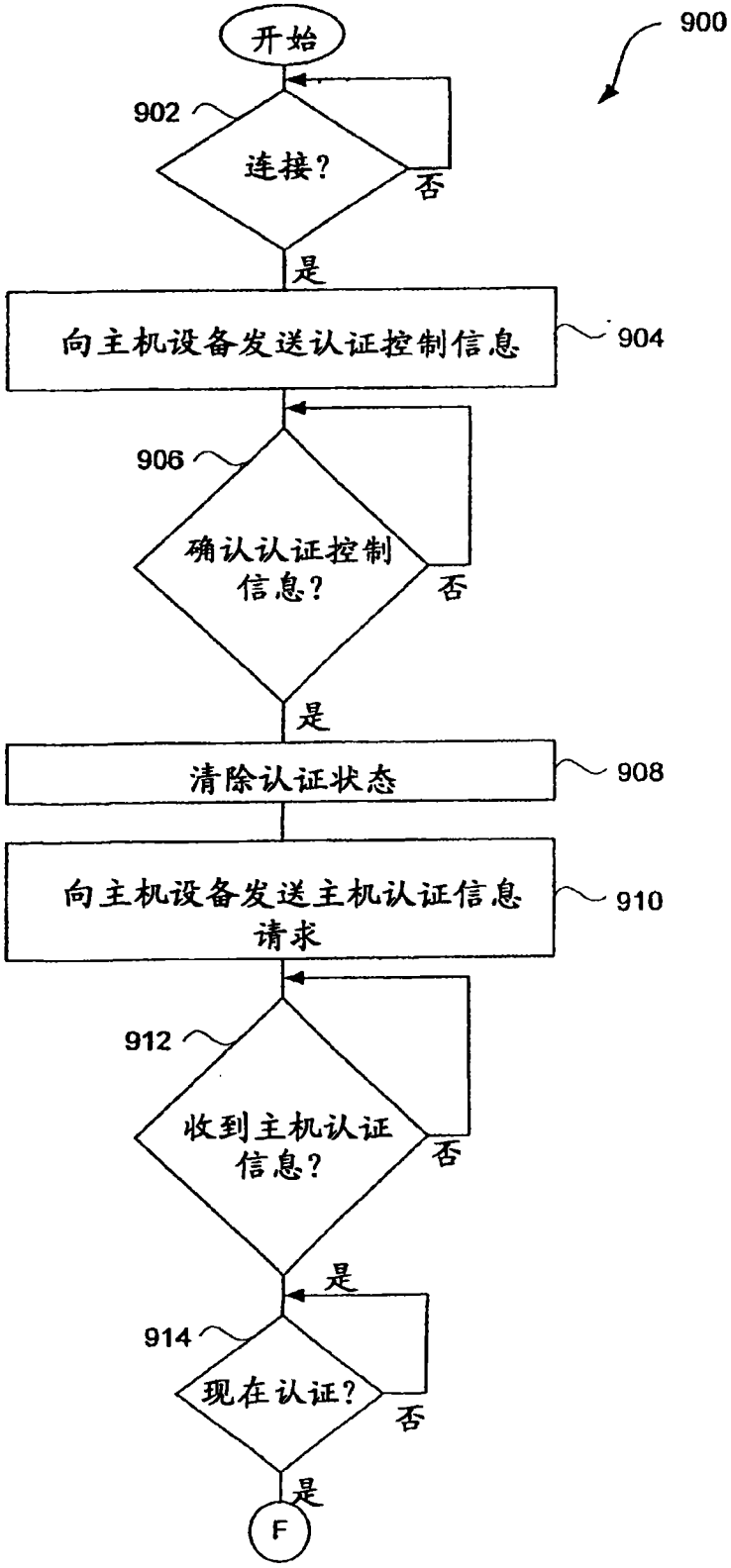

900
开始
902
连接?
否
是
向主机设备发送认证控制信息
904
906
确认认证控制信息?
否
是
清除认证状态
908
向主机设备发送主机认证信息请求
910
912
收到主机认证信息?
否
是
914
现在认证?
否
是
F

图 9A

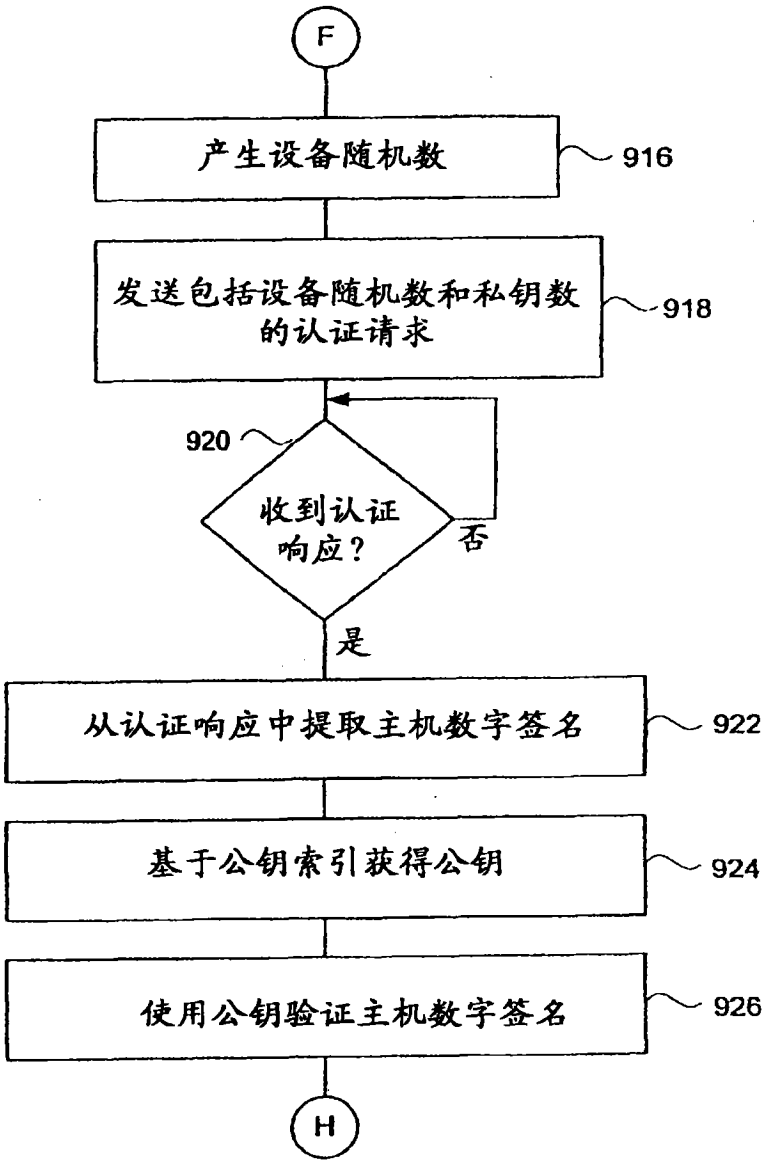

F
产生设备随机数
916
发送包括设备随机数和私钥数的认证请求
918
920
收到认证响应？
否
是
从认证响应中提取主机数字签名
922
基于公钥索引获得公钥
924
使用公钥验证主机数字签名
926
H

图 9B

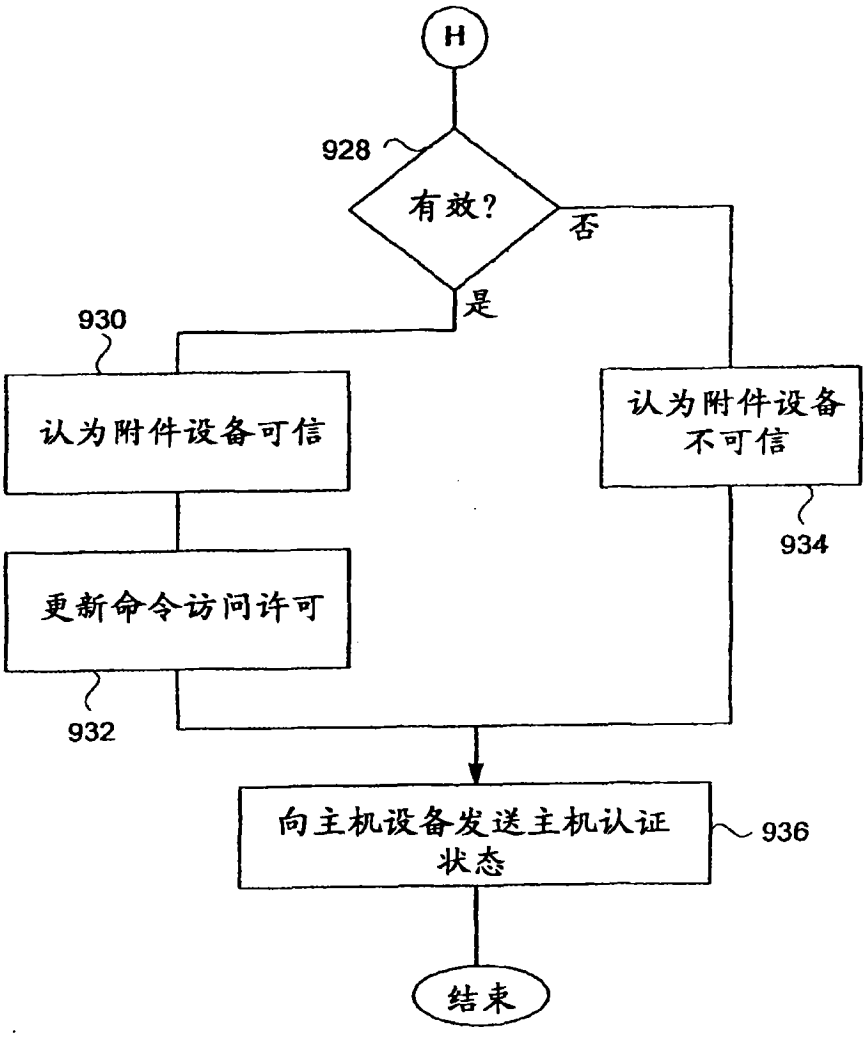

H
928
有效?
否
是
930
认为附件设备可信
认为附件设备不可信
934
更新命令访问许可
932
向主机设备发送主机认证状态
936
结束

图 9C

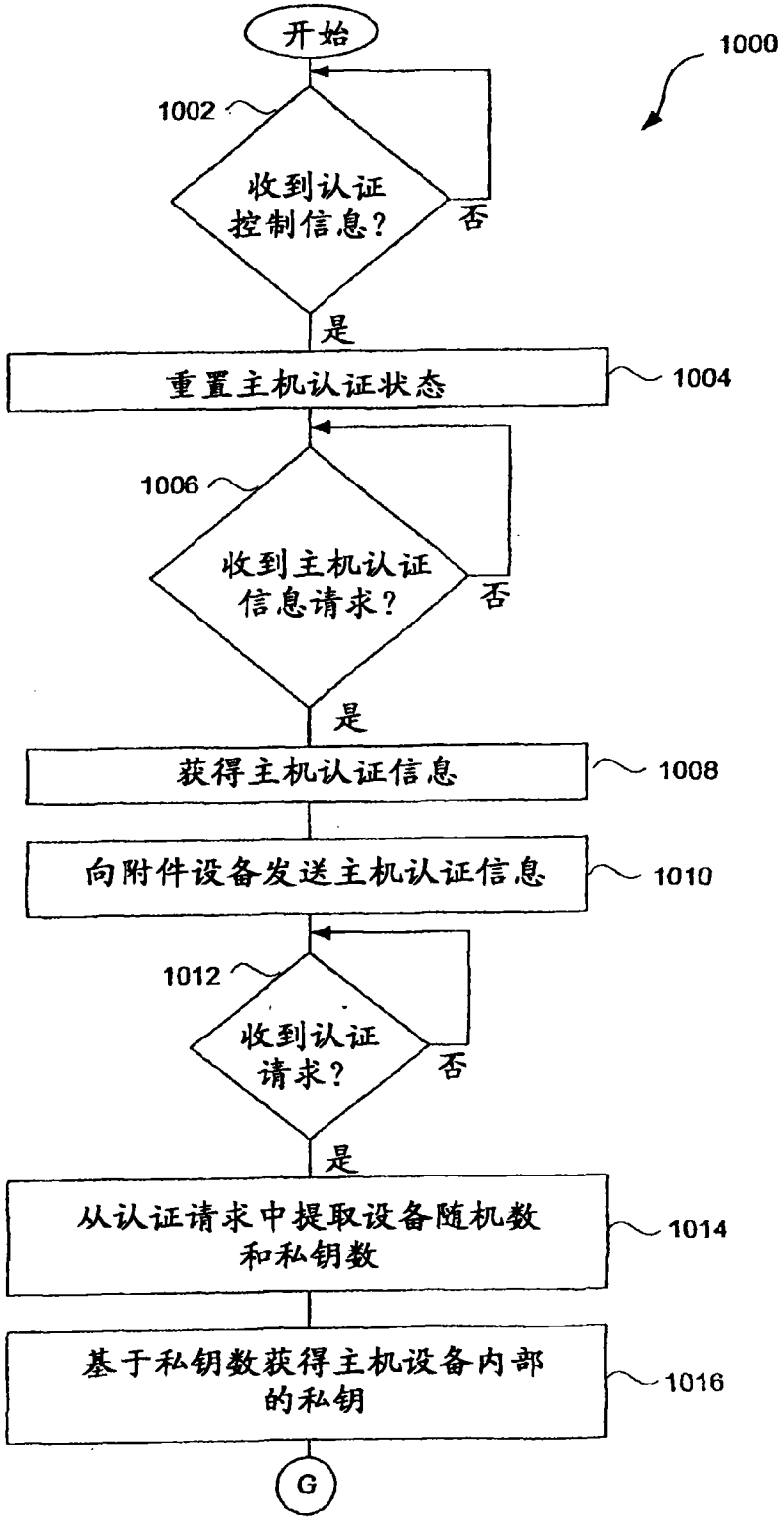

开始
1000
1002
收到认证控制信息?
否
是
重置主机认证状态
1004
1006
收到主机认证信息请求?
否
是
获得主机认证信息
1008
向附件设备发送主机认证信息
1010
1012
收到认证请求?
否
是
从认证请求中提取设备随机数和私钥数
1014
基于私钥数获得主机设备内部的私钥
1016
G

图 10A

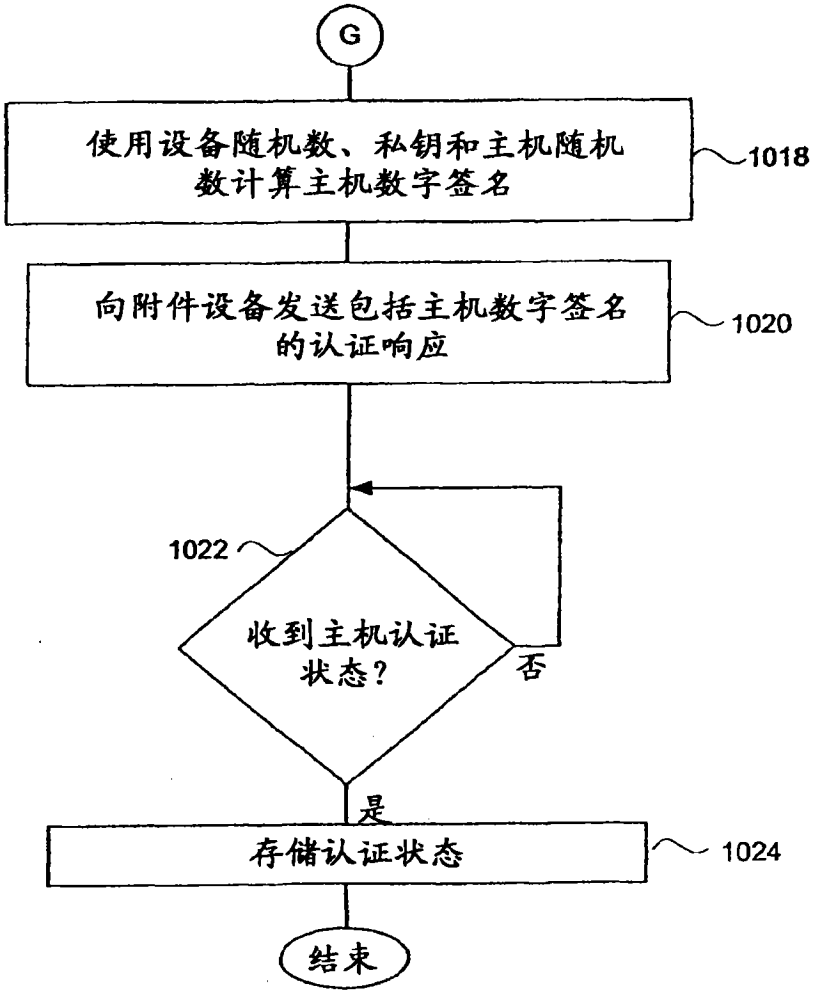

G
使用设备随机数、私钥和主机随机数计算主机数字签名
1018
向附件设备发送包括主机数字签名的认证响应
1020
1022
收到主机认证状态？
否
是
存储认证状态
1024
结束

图 10B

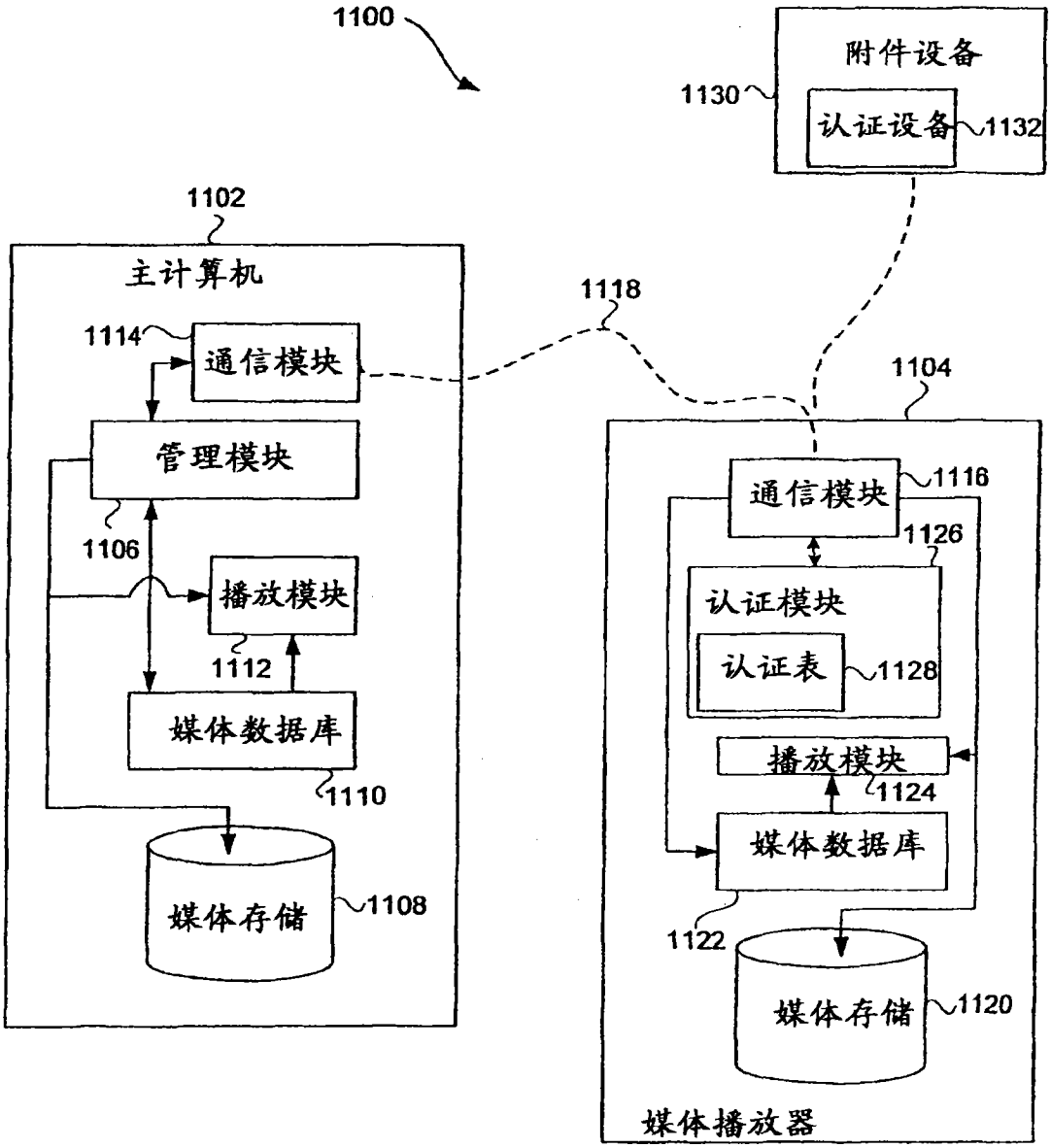

1100
附件设备
1130
认证设备
1132
1102
主计算机
1118
1114
通信模块
1104
管理模块
通信模块
1116
1106
1126
播放模块
认证模块
1112
认证表
1128
媒体数据库
播放模块
1110
1124
媒体数据库
媒体存储
1108
1122
媒体存储
1120
媒体播放器

图 11

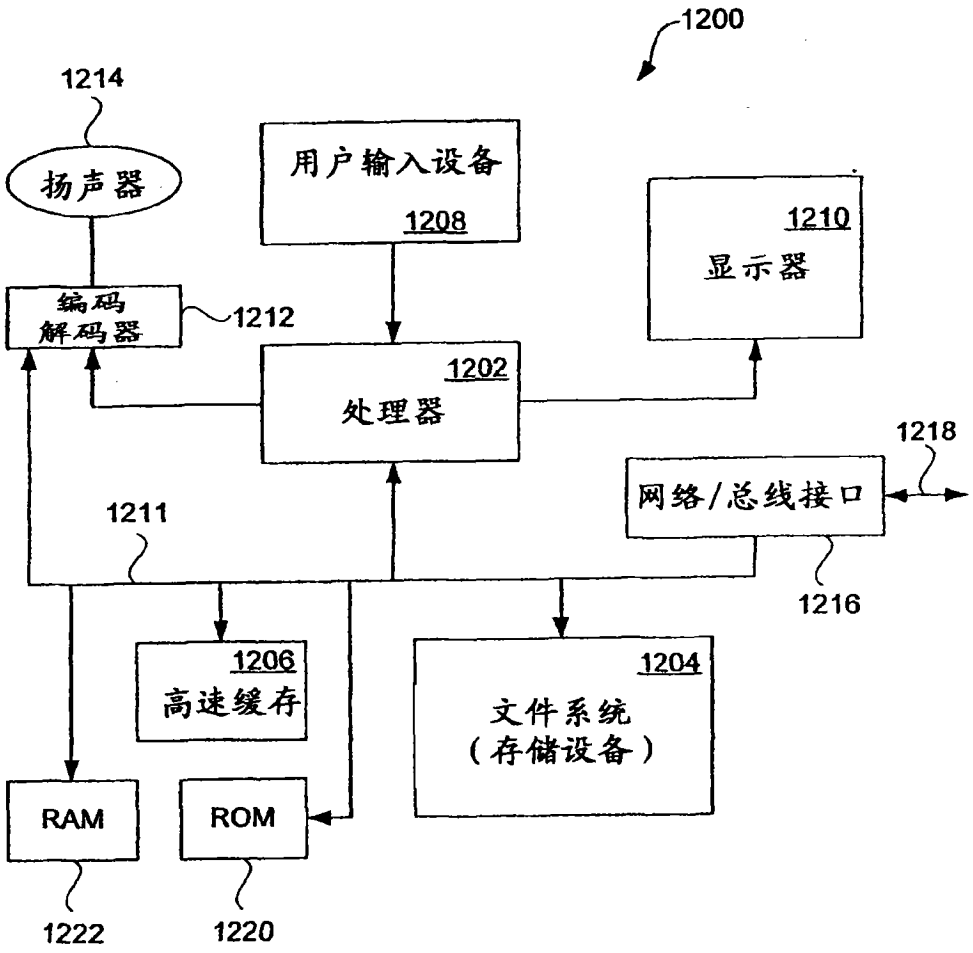

1200
1214
扬声器
用户输入设备
1208
1210
显示器
编码
解码器
1212
1202
处理器
1218
网络/总线接口
1211
1216
1206
高速缓存
1204
文件系统
(存储设备)
RAM
ROM
1222
1220

图 12