

(12) 发明专利

(10) 授权公告号 CN 1913427 B

(45) 授权公告日 2011.09.21

(21) 申请号 200610108186.8

(22) 申请日 2006.07.31

(30) 优先权数据

05107065.4 2005.07.29 EP

(73) 专利权人 捷讯研究有限公司

地址 加拿大安大略省沃特卢市

(72) 发明人 迈克尔·K·布朗 奈尔·P·亚当斯
赫伯特·A·利特尔

(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 王玮

(51) Int. Cl.

H04L 9/00(2006.01)

H04L 9/18(2006.01)

H04L 9/32(2006.01)

G07F 7/10(2006.01)

(56) 对比文件

US 5721781 A, 1998.02.24, 摘要, 说明书

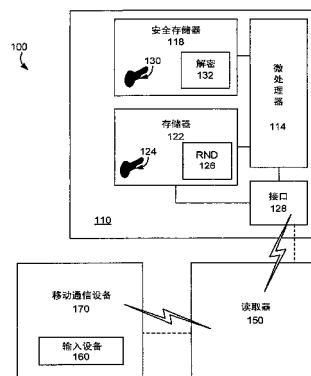
权利要求书 2 页 说明书 5 页 附图 2 页

(54) 发明名称

用于加密智能卡 PIN 输入的系统与方法

(57) 摘要

提供一种智能卡、系统和方法，用于使用智能卡安全地授权用户或用户设备。将智能卡配置成在初始化时或请求认证时，向用户输入设备提供公钥，从而在通过智能卡读取器向智能卡传送之前，加密用户输入的 PIN 或口令。然后智能卡解密 PIN 或口令，以授权用户。优选地，将智能卡配置成向用户输入设备提供公钥和随机数，然后用户输入设备在向智能卡传送之前，加密随机数与用户输入的 PIN 或口令的串连或其它组合。因此，智能卡读取器无法无阻碍地接收 PIN 或口令的拷贝，从而允许将智能卡与不可靠的智能卡读取器共同使用。



1. 一种用于使用与物理上分离的智能卡读取器进行无线通信的用户设备通过智能卡进行认证的方法,所述智能卡包括微处理器和用于存储私钥和公钥的存储器,所述存储器包括用于存储私钥、解密算法和预定认证信息的安全存储器;所述方法包括:

在无线通信链路上,通过所述智能卡读取器从所述智能卡向用户设备传送询问,询问包括公钥;

在无线通信链路上,在所述智能卡处通过所述智能卡读取器从用户设备接收对所述询问的响应,所述响应包括用所述询问加密的、接收到的用户输入的认证信息;

在所述智能卡处使用私钥解密接收到的用户输入的认证信息;

在所述智能卡处将接收到的用户输入的认证信息与预定认证信息相比较;以及

如果接收到的用户输入的认证信息与预定认证信息相匹配,则从所述智能卡向用户设备传送验证信号。

2. 根据权利要求1所述的方法,其中还向智能卡的存储器提供随机数产生功能,所述方法还包括产生和存储随机数的步骤,其中所述询问还包括随机数,从而使接收到的用户输入的认证信息包括在由用户设备接收的询问中包括的随机数,以及比较接收到的用户输入的认证信息的步骤包括将存储的随机数和在接收到的认证信息中包括的随机数相比较。

3. 根据权利要求1或2所述的方法,其中向用户设备传送询问的步骤发生在接收到认证请求之后。

4. 根据权利要求1或2所述的方法,还包括步骤:

在向用户设备传送询问的步骤之前,向智能卡传送认证请求;

提示在用户设备处的认证信息的用户输入;

在用户设备处使用询问加密接收为用户输入的认证信息;

通过智能卡读取器向智能卡传送已加密的用户输入的认证信息;以及
从所述智能卡接收验证信号。

5. 根据权利要求1或2所述的方法,其中用户设备包括移动通信设备。

6. 根据权利要求5所述的方法,还包括在从智能卡接收到验证信号时,解密或数字签名电子消息的步骤。

7. 根据权利要求6所述的方法,其中解密或数字签名电子消息的步骤包括访问第二私钥,以执行解密或数字签名的步骤。

8. 一种用于在用户设备处认证用户的智能卡,所述智能卡包括:

适配成存储私钥、公钥和预定认证信息的存储器,存储器的安全部分中至少存储私钥;

接口,适配成用于与用户设备物理上分离的智能卡读取器通信;在无线通信链路上,通过所述智能卡读取器向用户设备传送包括至少公钥的询问;以及在无线通信链路上,响应于所述询问,通过所述智能卡读取器,从用户设备接收已加密的认证信息,所述已加密的认证信息包括由公钥加密的用户输入的认证信息;以及

处理器,适配成用于使用私钥,对接收到的已加密认证信息执行解密算法,以获得已解密认证信息;将已解密认证信息与预定认证信息进行比较;以及如果已解密认证信息与预定认证信息匹配,则产生验证信号。

9. 根据权利要求8所述的智能卡,还包括适配成用于产生存储在存储器中的随机数的

处理器,其中所述接口被适配成传送至少包括公钥和随机数的询问,接收包括随机数的已加密认证信息,比较已解密认证信息的处理器被适配成将已解密信息与预定认证信息和存储的随机数相比较。

10. 根据权利要求 8 或 9 所述的智能卡,其中接口被适配成通过智能卡读取器,从用户设备接收认证请求。

11. 根据权利要求 8 或 9 所述的智能卡,其中用户设备在数字签名或解密电子消息中使用私钥。

12. 根据权利要求 11 所述的智能卡,其中所述存储器还被适配成存储第二私钥和相应的第二公钥,用户设备在数字签名或解密电子消息中可使用第二私钥。

13. 一种用于认证的系统,包括:

智能卡,包括微处理器和用于存储私钥、公钥和预定认证信息的存储器,所述存储器包括用于至少存储私钥的安全存储器,将微处理器配置成使用私钥执行解密算法,并执行预定认证信息与接收到的认证信息之间的比较;

用户设备,用于从接收用户输入,将用户设备配置成加密输入;以及

与用户设备物理上分离并进行无线通信的智能卡读取器,用于提供智能卡与用户移动通信设备之间的通信装置;

其中当智能卡通过智能卡读取器与用户设备通信时,

将智能卡配置成向用户设备传送包括公钥的询问,

将用户设备配置成使用公钥加密接收作为用户输入的认证信息,并响应于所述询问,通过智能卡读取器向智能卡传送已加密认证信息,以及

将智能卡进一步配置成使用解密算法和私钥,解密已加密认证信息并从用户设备进行接收,以提供已解密的认证信息,从而使微处理器执行预定认证信息与接收到的认证信息之间的比较,并且使智能卡读取器避免接收或通信未加密认证信息。

14. 根据权利要求 13 所述的系统,其中所述微处理器还被配置为产生随机数并将随机数存储在存储器中,从而当智能卡通过智能卡读取器与用户设备通信时,智能卡被配置为传送公钥和随机数,以及用户设备被配置为使用公钥来加密从智能卡接收的随机数和接收作为用户输入的认证信息的串连,并将由此加密的信息传送给智能卡,所述智能卡还被配置为使用解密算法和私钥来解密从用户设备接收的已加密的认证信息,以提供已解密的认证信息和已解密的随机数,从而使微处理器执行预定认证信息和所存储的随机数与已解密的认证信息和已解密的随机数的比较。

用于加密智能卡 PIN 输入的系统与方法

技术领域

[0001] 本发明总体上涉及用于授权用户的智能卡，具体涉及用于向智能卡认证用户的个人身份号码或口令的加密。

背景技术

[0002] 智能卡，也称作芯片卡或集成电路卡，是用作敏感数据或用户认证的存储设备的具有嵌入式集成电路（例如微处理和 / 或存储器）的存储的设备。智能卡可以包括用于存储财务或个人数据，或者私人数据（例如用在 S/MIME（安全多用途因特网邮件扩展）加密技术中的私钥）的存储器。优选地，可以使用 PIN（个人身份号码）或口令作为访问控制措施来保护一些这种类型的数据。为了访问卡存储器中存储的受保护数据，用户必须通过提供正确的 PIN 或口令来被证实。

[0003] 典型地，智能卡不包括直接输入用于用户认证的 PIN 或口令所用的数据输入设备。典型地，结合与输入设备通信的智能卡读取器来使用智能卡。当智能卡与智能卡读取器通信时，用户可以通过输出设备向智能卡读取器无阻碍地提供 PIN 或口令。然后读取器可以将用户输入的 PIN 或口令传递给智能卡，用于验证，从而使智能卡能够认证用户。

[0004] 虽然这种现有技术的智能卡解决方案对于用户熟悉的硬件系统是令人满意的，用户熟悉的硬件系统例如是在工作地点环境内使用的智能卡认证系统，其中智能卡读取器是可靠的，但是这种系统在硬件不可靠的外部环境表现出增加的风险。因为用户向智能卡读取器无阻碍地提供 PIN 或口令，所以智能卡读取器可以访问该认证信息；用户不知道智能卡读取器是否将保留 PIN 或口令的拷贝，或将信息传递给不利者。

[0005] 因此，需要提供一种用于在通过输入设备输入时保护用户 PIN 或口令的系统和方法，以保证不可靠的硬件不会捕获或复制该敏感信息。

发明内容

[0006] 根据优选实施例，提供一种增强的智能卡，用于在智能卡读取器接收数据之前加密用户输入的认证数据。智能卡包括：适配成存储私钥、公钥和预定认证信息的装置，安全存储器中至少存储私钥；适配成用于与智能卡读取器通信的装置；适配成用于通过智能卡读取器向用户设备传送至少包括公钥的询问的装置；适配成用于通过智能卡读取器从用户设备接收已加密认证信息的装置，已加密认证信息由公钥加密；适配成用于使用私钥，对接收到的已加密认证信息执行解密算法，以获得已解密认证信息的装置；适配成用于比较已解密认证信息与预定认证信息的装置；以及适配成用于在已解密认证信息与预定认证信息相匹配时，产生验证信号的装置。

[0007] 优选地，智能卡还包括适配成用于产生并存储随机数（nonce）的装置，并将适配成用于传送询问的装置进一步适配成传送至少包括公钥和随机数的询问，将适配成用于接收已加密认证信息的装置进一步适配成接收包括随机数的已加密认证信息，并且将适配成比较已解密认证信息的装置进一步适配成将已解密信息与预定认证信息和存储的随机数

相比较。智能卡还可以包括适配成通过智能卡读取器，从用户设备接收认证请求的装置。用户设备可以在数字签名或解密电子消息中使用私钥，但是智能卡或用户设备可以还包括适配成存储用在数字签名或解密消息中的另外的私钥和另外的公钥的装置。

[0008] 在优选实施例中，提供一种用于使用智能卡认证用户设备的系统，包括：智能卡，包括微处理器和用于存储私钥、公钥和预定认证信息的存储器，存储器包括用于存储至少私钥的安全存储器，将微处理器配置成使用私钥执行解密算法，并执行预定认证信息与接收到的认证信息之间的比较；用户设备，用于从用户接收输入，将用户设备配置成加密输入；以及智能卡读取器，用于提供智能卡与用户设备之间的通信装置；其中当智能卡通过智能卡读取器与用户设备通信时，将智能卡配置成向用户设备传送公钥，将用户设备配置成使用该公钥，加密来自用户的输入认证信息，并向智能卡传送已加密认证信息，并将智能卡进一步配置成使用解密算法和私钥，解密接收到的已加密认证信息，从而使微处理器可以执行预定认证信息与接收到的认证信息之间的比较，并且使智能卡读取器无法接收或通信未加密认证信息。优选地，将微处理器进一步配置成产生随机数并在存储器中存储随机数，从而在智能卡通过智能卡读取器与用户设备通信时，将智能卡配置成传送公钥和随机数，并将用户设备配置成使用公钥加密随机数与来自用户的输入认证信息的串连，并向智能卡传送已加密的信息，将智能卡进一步配置成使用解密算法和私钥，解密接收到的已加密信息，从而使微处理器可以执行预定认证信息和接收到的随机数与接收到的认证信息和存储的随机数之间的比较。

[0009] 此外，在优选实施例中，提供一种用于使用智能卡认证用户设备的方法，包括步骤：提供包括微处理器和用于存储私钥和公钥的存储器的智能卡，存储器包括用于存储私钥、解密算法和预定认证信息的安全存储器；向用户设备传送询问，该询问包括公钥；从用户设备接收包括用询问加密的所接收认证信息的响应；使用私钥解密接收到的认证信息；将接收到的认证信息与预定认证信息相比较；如果接收到的认证信息与预定认证信息相匹配，则向用户设备传送验证信号。优选地，还向智能卡的存储器提供随机数产生功能，从而使向用户设备传送询问的步骤包括传送包括公钥和随机数的询问，使比较接收到的认证信息的步骤还包括存储的随机数和预定认证信息与接收到的认证信息之间的比较。

[0010] 该方法还可以包括步骤：在向用户设备传送询问之前，向智能卡传送认证请求；提示用户设备的用户输入认证信息；在用户设备，使用询问加密接收到的认证信息；向智能卡传送已加密的接收到的认证信息；以及从智能卡接收验证信号。用户设备可以包括移动通信设备，该方法还可以包括在从智能卡接收到验证信号时，解密或数字签名电子消息的步骤。

附图说明

[0011] 在仅示出本发明优选实施例以作示例的图中，

[0012] 图 1 是智能卡和智能卡系统的方框图。

[0013] 图 2 是使用智能卡认证用户的方法的流程图。

具体实施方式

[0014] 参考图 1，示出智能卡系统 100 的优选实施例。智能卡系统 100 包括智能卡 110、智

能卡读取器 150 和输入设备 160。输入设备可以包括在移动通信设备 170 中。在移动通信设备 170 的情况下,可以用智能卡 110 授权由移动通信设备 170 执行的特定功能,例如由移动通信设备 170 发送和 / 或接收的消息的加密、解密和数字签名。如果输入设备 160 包括在移动通信设备 170 中,则移动通信设备 170 可以通过直接有线连接(例如通过 USB(通用串行总线))或通过根据标准(例如,针对无线局域网的电气和电子工程师协会(IEEE)802.11a/b/g 标准、蓝牙(Bluetooth®)、Zigbee® 等,或针对无线通信,特别是短程的未来标准)的无线通信链接,与智能卡读取器 150 通信。

[0015] 如本领域技术人员将理解的,智能卡 110 可以是接触式智能卡或非接触式智能卡。优选地,向接触式智能卡提供根据由国际标准组织发布的符合 ISO/IEC 7816 的物理接触部分,其中,接触部分提供用于卡 110 与读取器 150 之间数据通信的、与智能卡读取器 150 的接口,还向卡本身提供任何必要的电量。优选地,根据分别针对紧耦合式、邻近式和短距离智能卡定义标准的 ISO/IEC 10536、14443 或 15693,提供非接触式智能卡。非接触式智能卡不需要保持与读取器 150 的物理接触来执行功能,而是用天线和射频接口与读取器 150 通信,并由在读取器 150 处产生的电磁场供电。在以下描述中,将理解不论是接触式还是非接触式智能卡,智能卡 110 的接口包括执行智能卡 110 的接口功能的智能卡部分。虽然智能卡 110 可以包括在另一尺寸规格(form factor)或提供用于与智能卡读取器 150 通信的功能的设备中,但是针对智能卡 110 的典型尺寸规格是“信用卡”型的尺寸规格。

[0016] 在优选实施例中,智能卡 110 具有与安全存储器 118 和较不安全存储器 122 通信的微处理器 114。可以在 ASIC 或智能卡 110 内的多个集成电路中提供这些组件。将微处理器 114 配置成执行任何智能卡操作系统软件和其它软件应用程序,并提供多种命令的执行,例如执行与存储器相关的命令,从安全存储器 118(如果提供的安全存储器是读 / 写存储器)或从较不安全存储器 122(优选地是读 / 写存储器)读取信息和向其中写入信息;执行与安全相关的命令来执行诸如口令检验的认证操作。微处理器 114 和可选的较不安全存储器 122 与接口 128 通信,从而能够在智能卡 110 和智能卡读取器 150 之间交换信息。除了根据由微处理器 114 执行的与安全相关的命令,对于读取器 150,安全存储器 118 的内容不可通过接口获取。安全存储器 118 可以包括在微处理器 114 之内。

[0017] 智能卡 110 的安全存储器 118 包括密钥 130(例如,在 S/MIME 解密或签名中使用的私钥)的存储位置。安全存储器 118 还存储可由微处理器 114 执行的解密功能 132,以及可以相对于用户输入的认证信息(例如, PIN 或口令)进行比较以向智能卡认证用户的认证信息。优选地,在安全存储器 118 中,PIN 或口令不是无阻碍地存储,而是间接(例如,作为散列)存储。较不安全存储器 122 存储公钥和 / 或包含公钥 124 的证书。还可以在较不安全存储器 122 中存储由微处理器 114 执行的随机数产生函数 126。

[0018] 配置智能卡 110,使其在初始化时向智能卡读取器 150 传送包括公钥 124 的询问,其中初始化发生在智能卡 110 被智能卡读取器 150 激活并从智能卡读取器 150 接收到足够电量以执行智能卡功能的时候。读取器 150 向输入设备 160 提供询问,接着将输入设备 160 配置成从用户接收认证信息(例如 PIN 或口令),以用于为智能卡 110 认证用户。进一步将输入设备 160 配置成使用询问数据(例如,公钥 124)来加密用户输入的认证信息。因此,将已加密认证信息从输入设备 160 传送到智能卡读取器 150,并从智能卡读取器 150 传送到智能卡 110。将已加密认证信息传给解密函数 132,解密函数 132 访问私钥 130,解密已加密

认证信息,以获得用户输入的 PIN 或口令。然后智能卡 110 执行验证命令,将已解密认证信息和安全存储器 118 中先前存储的认证信息进行比较。如果已解密认证信息与先前存储的认证信息相匹配,则智能卡 110 授权用户,并通过读取器 150 从智能卡 110 向输入设备 160 传送验证信号。如本领域技术人员将理解的,在本实施例中,无论读取器 150 可靠还是不可靠,智能卡 110 都可以与任何读取器 150 通信来授权用户;读取器 150 也可无阻碍地立即获得认证信息(例如, PIN 或口令)。

[0019] 在最优选的实施例中,询问包括公钥 124 和由随机数产生函数 126 或微处理器 114 产生的随机数。因此,可以将智能卡 110 配置成在初始化时产生包括公钥 124 和随机数的询问,并在存储器中暂时存储随机数。然后,输入设备 160 用随机数和公钥 124(例如,通过串连随机数和认证信息)加密用户输入的认证信息。解密函数 132 访问私钥 130 和由智能卡暂时存储在存储器中的随机数,从而在验证步骤解密接收到的已加密认证信息,并确定用户输入的认证信息和随机数。然后将智能卡 110 配置成将暂时存储的随机数用于单次认证尝试;如果验证步骤失败,则智能卡 110(如果配置成向用户发布进一步询问)产生新的随机数,并将新的随机数作为进一步询问的一部分来传送。通过结合随机数,最小化回复攻击的可能性;即使欺诈性的智能卡读取器 150 捕获已加密认证信息,并且恶意用户稍后尝试回复已加密认证信息,验证也不会成功。

[0020] 参考图 2,提供用于使用上述智能卡认证用户的优选方法。在步骤 200,智能卡读取器 150 检测智能卡 110。检测可以通过轮询智能卡读取器 150 中的接口,直到接收到指示智能卡 110 已由读取器 150 激活并准备与读取器 150 通信的信号。然后在步骤 205,优选地通过智能卡 110 内部操作系统来初始化智能卡。在步骤 210,可选地,当智能卡 110 从智能卡读取器 150 接收到认证请求时,智能卡 110 产生至少包括公钥 124 的询问,但是最优选地是包括公钥 124 和用产生函数 126 产生的随机数,并向智能卡读取器 150 传送该询问,接着在步骤 215,智能卡读取器 150 发信号通知输入设备 160 向用户请求认证信息(例如 PIN)。在步骤 220,输入设备 160 使用询问加密输入的认证信息。然后在步骤 225,通过读取器 150 向智能卡 110 传送已加密认证信息,在步骤 230,智能卡 110 使用私钥 130 解密接收到的已加密认证信息,并将已解密信息与先前存储在智能卡 110 上的信息相比较。如果在步骤 235 信息匹配,则智能卡授权用户。

[0021] 可以在用于使用移动通信设备 170 加密和解密消息的系统中采用这种方法。移动通信设备 170 可以包括输入设备 160。当移动通信设备 170 的用户希望数字签名要从设备 170 发送的消息时,用户激活智能卡 110,使移动设备 170 提示用户根据上述方法提供认证信息。如果用户被授权,则将移动通信设备 170 配置成数字签名消息。相似地,当移动设备 170 的用户接收到已加密消息并希望解密该消息时,用户可以激活智能卡 110,进行上述认证过程,如果用户被授权,则将移动通信设备 170 配置成解密该消息。解密可以使用存储在智能卡 110 的安全存储器 118 中的另外的密钥,只有在智能卡 110 使用存储在卡 110 上的公钥 / 私钥对 124 和 130 之后,才向移动通信设备 170 提供另外的密钥。如本领域技术人员将理解的,只有当用户希望签名消息或解密消息时才必需授权用户,这是因为这些行为典型地需要访问敏感信息,即,私钥。因为可以使用公共可用的接收方公钥执行加密,所以,如果用户只希望加密发送给接收方的消息时,不必使用上述方法授权用户。此外,应该理解,移动通信设备 170 最终用于解密或数字签名消息的公钥 / 私钥对不需要与智能卡 110 用来

授权用户的公钥 / 私钥对相同。可以在移动通信设备 170 的内置存储器中, 或相似地, 在智能卡 110 的存储器中存储移动通信设备 170 所用的公钥 / 私钥对。

[0022] 通过示例详细描述了本发明的多种实施例, 对于本领域技术人员将显而易见, 在不背离本发明的前提下可以进行改变和修改。本发明包括所有在所附权利要求的范围之内的改变和修改。

[0023] 本专利文档的部分公开包含受到版权保护的材料。只要在专利与商标局专利文件或记录中出现, 对于专利文档或专利公开的任何一种的传真再现, 版权所有人不持反对意见, 但是将保留其它所有版权。

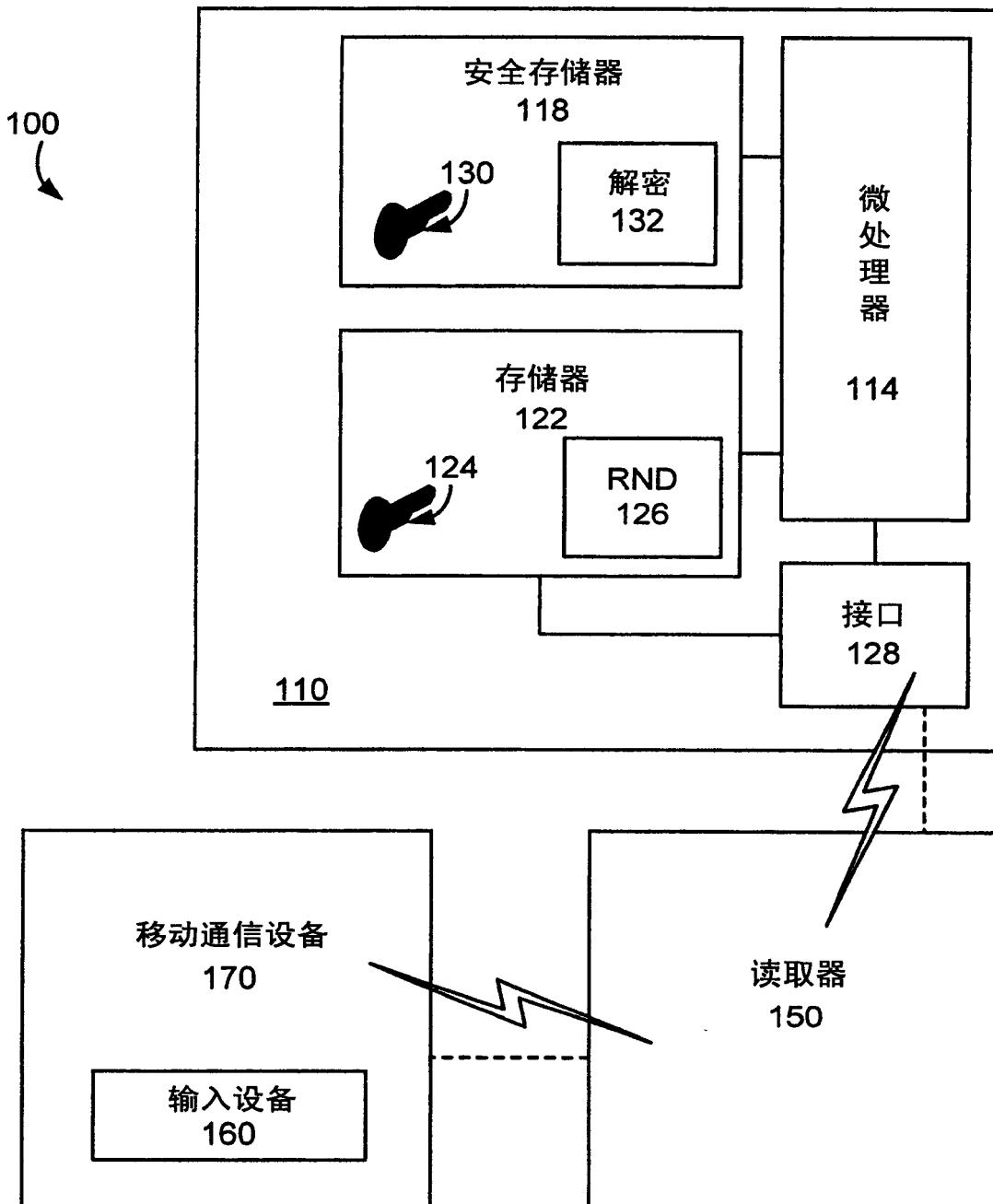


图 1

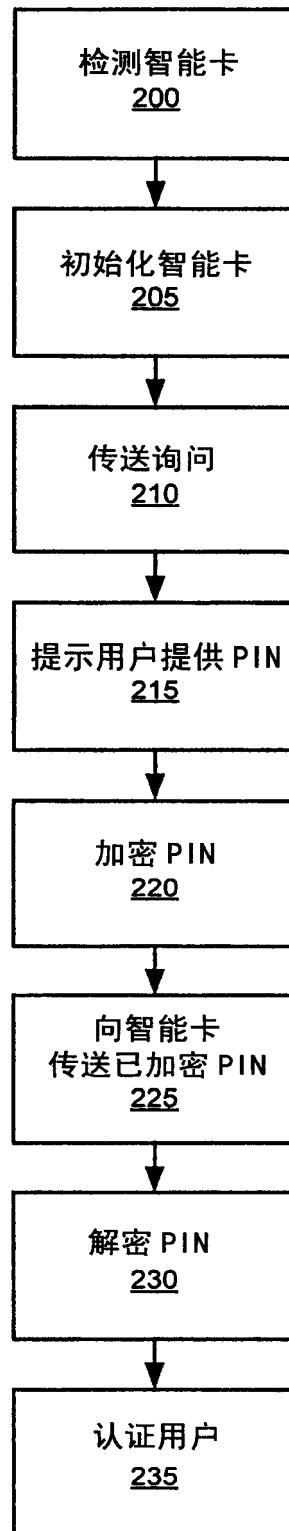


图 2