(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118556246 A
(43)申请公布日 2024.08.27

(21)申请号 202280083026.X

(22)申请日 2022.11.23

(30)优先权数据
17/551,670 2021.12.15 US

(85)PCT国际申请进入国家阶段日
2024.06.14

(86)PCT国际申请的申请数据
PCT/US2022/050885 2022.11.23

(87)PCT国际申请的公布数据
WO2023/113986 EN 2023.06.22

(71)申请人 第一资本服务有限责任公司
地址 美国

(72)发明人 凯文·奥斯本 杰基尚·普拉萨德 约瑟·卡塔拉·卡斯特利亚尔

(74)专利代理机构 北京品源专利代理有限公司 11332
专利代理师 谭营营 胡彬

(51)Int.Cl.
G06Q 20/38(2006.01)
G06Q 20/32(2006.01)
G06Q 20/34(2006.01)
G06Q 20/36(2006.01)

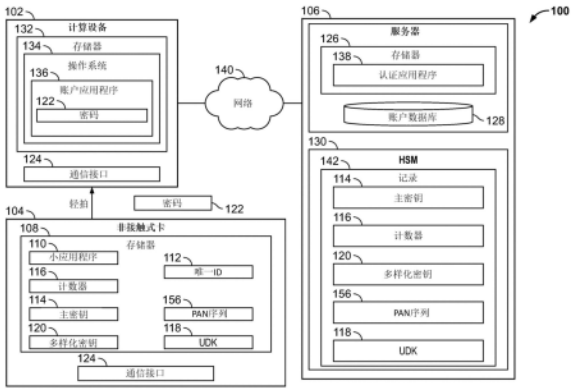
权利要求书2页 说明书19页 附图18页

(54)发明名称

基于非接触式卡认证的密钥恢复

(57)摘要

用于基于非接触式卡密码的密钥恢复的系统、方法、装置和计算机可读介质。服务器可以从应用程序接收恢复用于数字钱包的私钥的请求，该请求包括由非接触式卡生成的第一密码。服务器可以基于用于非接触式卡的密钥来解密该第一密码。服务器可以基于该解密确定非接触式卡的唯一标识符以及与数字钱包相关联的多样化因子。服务器可以基于该唯一标识符和多样化因子生成私钥。服务器可以经由网络将私钥传送到应用程序。



CN 118556246 A

1.一种方法,包括:

由服务器从应用程序接收恢复用于数字钱包的私钥的请求,所述请求包括由非接触式卡生成的第一密码;

由所述服务器基于用于所述非接触式卡的密钥来解密所述第一密码;

由所述服务器基于所述解密确定所述非接触式卡的唯一标识符和与所述数字钱包相关联的多样化因子;

由所述服务器基于所述唯一标识符和所述多样化因子生成所述私钥;以及

由所述服务器经由网络向所述应用程序传送所述私钥。

2.根据权利要求1所述的方法,其中,所述多样化因子包括所述非接触式卡的应用程序主账号(PAN)序列号。

3.根据权利要求1所述的方法,其中,所述多样化因子包括所述非接触式卡的应用程序交易计数器(ATC)。

4.根据权利要求1所述的方法,还包括在接收到所述请求之前:

由所述服务器从所述应用程序接收由所述非接触式卡生成的第二密码;

由所述服务器解密所述第二密码;

由所述服务器基于所述第二密码的解密生成所述私钥;

由所述服务器基于所述私钥生成公钥,并基于所述公钥生成用于所述数字钱包的钱包地址;以及

由所述服务器向所述应用程序传送所述私钥、所述公钥和所述钱包地址。

5.根据权利要求4所述的方法,其中,所述非接触式卡的所述唯一标识符和所述多样化因子是基于所述数字钱包的钱包地址来确定的。

6.根据权利要求5所述的方法,还包括基于所述第一密码的解密生成所述数字钱包的钱包地址。

7.根据权利要求1所述的方法,其中,所述服务器还确定与所述数字钱包相关联的盐值,其中,所述服务器还基于所述盐值生成所述私钥,所述方法还包括:

由所述应用程序基于所述私钥访问所述数字钱包。

8.一种非暂时性计算机可读存储介质,所述计算机可读存储介质包括指令,所述指令在由处理器执行时致使所述处理器:

从应用程序接收恢复用于数字钱包的私钥的请求,所述请求包括由非接触式卡生成的第一密码;

基于用于所述非接触式卡的密钥来解密所述第一密码;

基于所述解密确定所述非接触式卡的唯一标识符和与所述数字钱包相关联的多样化因子;

基于所述唯一标识符和所述多样化因子生成所述私钥;以及

经由网络向所述应用程序传送所述私钥。

9.根据权利要求8所述的非暂时性计算机可读存储介质,其中,所述多样化因子包括所述非接触式卡的应用程序主账号(PAN)序列号。

10.根据权利要求8所述的非暂时性计算机可读存储介质,其中,所述多样化因子包括所述非接触式卡的应用程序交易计数器(ATC)。

11.根据权利要求8所述的非暂时性计算机可读存储介质,其中,所述指令还致使所述处理器在接收到所述请求之前:

从所述应用程序接收由所述非接触式卡生成的第二密码;

解密所述第二密码;

基于所述第二密码的解密生成所述私钥;

基于所述私钥生成公钥,并基于所述公钥生成用于所述数字钱包的钱包地址;以及

向所述应用程序传送所述私钥、所述公钥和所述钱包地址。

12.根据权利要求11所述的非暂时性计算机可读存储介质,其中,所述非接触式卡的所述唯一标识符和所述多样化因子是基于所述数字钱包的钱包地址来确定的。

13.根据权利要求12所述的非暂时性计算机可读存储介质,其中,所述指令还将所述计算机配置为基于所述第一密码的解密生成所述数字钱包的钱包地址。

14.根据权利要求8所述的非暂时性计算机可读存储介质,其中,所述处理器还确定与所述数字钱包相关联的盐值,其中,所述处理器还基于所述盐值生成所述私钥。

15.一种计算装置,包括:

处理器;以及

存储指令的存储器,所述指令在由所述处理器执行时致使所述处理器:

从应用程序接收恢复用于数字钱包的私钥的请求,所述请求包括由非接触式卡生成的第一密码;

基于用于所述非接触式卡的密钥来解密所述第一密码;

基于所述解密确定所述非接触式卡的唯一标识符和与所述数字钱包相关联的多样化因子;

基于所述唯一标识符和所述多样化因子生成所述私钥;以及

经由网络向所述应用程序传送所述私钥。

16.根据权利要求15所述的计算装置,其中,所述多样化因子包括所述非接触式卡的应用程序主账号(PAN)序列号。

17.根据权利要求15所述的计算装置,其中,所述多样化因子包括所述非接触式卡的应用程序交易计数器(ATC)。

18.根据权利要求15所述的计算装置,其中,所述指令还致使所述装置在接收到所述请求之前:

从所述应用程序接收由所述非接触式卡生成的第二密码;

解密所述第二密码;

基于所述第二密码的解密生成所述私钥;

基于所述私钥生成公钥,并基于所述公钥生成用于所述数字钱包的钱包地址;以及

向所述应用程序传送所述私钥、所述公钥和所述钱包地址。

19.根据权利要求18所述的计算装置,其中,所述非接触式卡的所述唯一标识符和所述多样化因子是基于所述数字钱包的钱包地址来确定的,其中,所述指令还将所述处理器配置为基于所述第一密码的解密生成所述数字钱包的钱包地址。

20.根据权利要求15所述的计算装置,其中,所述处理器还确定与所述数字钱包相关联的盐值,其中,所述处理器还基于所述盐值生成所述私钥。

基于非接触式卡认证的密钥恢复

[0001] 相关申请的交叉引用

[0002] 本申请要求2021年12月15日提交的标题为“KEY RECOVERY BASED ON CONTACTLESS CARD AUTHENTICATION”的美国专利申请序列号17/551,670的优先权。前述申请的内容通过引用以其整体并入本文。

背景技术

[0003] 数字钱包具有许多优点,但提出了安全和隐私方面的挑战。最常见的风险包括被盗和丢失(或遗忘)访问密钥。此外,托管钱包(custodial wallet)与特定机构挂钩,并且不允许可携带性。代理钱包(proxy wallet)具有安全漏洞和/或被盗的风险,导致访问密钥被泄露。硬件钱包可以提供恢复种子,但这些种子容易被盗和/或其他类型的丢失(例如,当用户无法回忆种子或无法找到他们对种子的记录时)。

发明内容

[0004] 用于基于非接触式卡认证的密钥恢复的系统、方法、装置和计算机可读介质。在一个方面,一种方法包括:由服务器从应用程序接收对恢复用于数字钱包的私钥的请求,该请求包括由非接触式卡生成的第一密码;由服务器基于用于非接触式卡的密钥解密该第一密码;由服务器基于该解密确定非接触式卡的唯一标识符和与硬件安全模块中的数字钱包相关联的多样化因子;由服务器基于该唯一标识符和多样化因子生成私钥;并由服务器经由网络向应用程序传送该私钥。

附图说明

[0005] 为了容易地标识任何特定元件或行为的讨论,附图标记中的最高有效数字是指其中首次引入该元件的图号。

[0006] 图1A示出了根据一个实施例的主题的一个方面。

[0007] 图1B示出了根据一个实施例的主题的一个方面。

[0008] 图1C示出了根据一个实施例的主题的一个方面。

[0009] 图2A示出了根据一个实施例的主题的一个方面。

[0010] 图2B示出了根据一个实施例的主题的一个方面。

[0011] 图2C示出了根据一个实施例的主题的一个方面。

[0012] 图3A示出了根据一个实施例的主题的一个方面。

[0013] 图3B示出了根据一个实施例的主题的一个方面。

[0014] 图4示出了根据一个实施例的例程400。

[0015] 图5示出了根据一个实施例的例程500。

[0016] 图6示出了根据一个实施例的例程600。

[0017] 图7A示出了根据一个实施例的非接触式卡。

[0018] 图7B示出了根据一个实施例的非接触式卡104。

[0019] 图8示出了根据一个实施例的数据结构800。

[0020] 图9示出了根据实施例的系统900的示例。

[0021] 图10示出了根据实施例的逻辑模型1000的示例。

[0022] 图11示出了根据实施例的逻辑模型1100的示例。

[0023] 图12示出了根据一个实施例的计算机架构1200。

具体实施方式

[0024] 本文公开的实施例提供了用于使用非接触式卡安全恢复用于访问数字钱包(诸如加密货币钱包)的密码密钥的技术。为了创建数字钱包,计算设备可以指示非接触式卡生成密码。在计算设备上执行的应用程序可以经由与非接触式卡的无线通信来接收密码并将密码传送到服务器以用于验证。如果服务器验证了该密码,则服务器可以创建私钥,该私钥是使用数字钱包访问或以其他方式执行操作所需的。服务器然后可以创建对应于私钥的公钥并且基于该公钥为数字钱包生成钱包地址。服务器然后可以存储对用于在硬件安全模块(hardware security module,HSM)中创建私钥的密码算法的一个或多个输入。该输入可以包括与非接触式卡相关联的密钥(或多个密钥)、非接触式卡的唯一标识符和多样化因子中的一个或多个。在一些实施例中,密钥可以被存储在HSM中,而唯一标识符和多样化因子可以作为输入提供给HSM以用于多样化私钥(例如,唯一标识符和多样化因子不需要被存储在HSM中)。

[0025] 服务器可以将私钥、公钥和钱包地址安全地传送到应用程序,该应用程序可以生成数字钱包并将私钥、公钥和钱包地址存储在其中。在一些实施例中,当用户试图访问数字钱包时,使用非接触式卡的密码验证可以被用于认证对数字钱包的访问。如果密码验证不成功,则可能会限制用户访问钱包,从而提高钱包的安全性。

[0026] 因为数字钱包存储私钥的模糊版本,用户可能丢失、忘记或以其他方式不能够提供私钥作为利用数字钱包执行交易的先决条件(例如,转移加密货币等)。有利地,本文公开的实施例提供了使用非接触式卡恢复私钥的安全解决方案。通常,为了恢复私钥,非接触式卡可以生成由服务器验证的密码。如果服务器能够验证该密码,则用于生成私钥的输入可以被提供给HSM。服务器然后可以重新创建私钥,并且在一个或多个部分中将重新创建的私钥传送到进行请求的应用程序和/或设备。

[0027] 有利地,本文公开的实施例提供了安全技术,以使用由非接触式卡生成的密码来恢复用于访问数字钱包的私钥。通过利用密码,本公开的实施例可以以最小的欺诈活动风险安全地验证用户的身份。此外,这样做可以确保只有当用户可以访问非接触式卡时才能恢复私钥,这有助于与服务器进行密码验证。此外,通过要求密码验证作为访问数字钱包和/或恢复私钥的先决条件,增强了数字钱包的安全性。

[0028] 一般参考本文中使用的符号和命名法,本文的详细描述可以在计算机或计算机网络上执行的编程程序方面呈现。这些程序描述和表示被本领域技术人员用来有效地将其工作的实质传达给本领域技术人员。

[0029] 这里的程序(并且通常)被设想为导致期望结果的自洽序列的操作。这些操作是那些需要物理量的物理操作的操作。通常,尽管不是必须的,这些量采取能够被存储、转移、组合、比较和以其他方式操纵的电、磁或光信号的形式。事实证明,有时,主要是出于常见用途

的原因,将这些信号称为比特、值、元素、符号、字符、术语、数字或类似物是方便的。然而,应该注意的是,所有这些和类似的术语都要与适当的物理量相关联,并且仅仅是应用于这些量的方便标签。

[0030] 此外,所执行的操作通常是指诸如相加或比较等的术语,其通常与由人类操作者执行的心理操作相关联。人类操作者的这种能力在本文所述的任何操作中都不是必要的,或者在大多数情况下不是期望的,这些操作形成一个或多个实施例的一部分。相反,操作是机器操作。用于执行各种实施例的操作的有用机器包括数字计算机或类似设备。

[0031] 一些实施例可以使用表述“耦合的”和“连接的”连同它们的衍生物来描述。这些术语不一定旨在作为彼此的同义词。例如,一些实施例可以使用术语“连接的”和/或“耦合的”来描述,以指示两个或更多个元件彼此直接物理接触或电接触。然而,术语“耦合的”也可能意味着两个或多个元件彼此不直接接触,但仍然彼此合作或相互作用。

[0032] 各种实施例还涉及用于执行这些操作的装置或系统。这种装置可以是为了所需目的而特别构造的或者它可以包括计算机,该计算机由存储在计算机中的计算机程序选择性地激活或重新配置。本文所呈现的程序并非固有地与特定计算机或其它装置相关。各种机器可以与根据本文教导编写的程序一起使用,或者可以证明构造更专门的装置以执行所需的方法步骤是方便的。用于各种这些机器的所需结构将从给出的描述中显现。

[0033] 现在参考附图,其中相同的附图标记自始至终用于指代相同的元件。在下面的描述中,为了解释的目的,阐述了许多具体细节以便提供对其的透彻理解。然而,可以在没有这些具体细节的情况下实践新颖的实施例。在其它实例中,以框图形式示出结构和设备以便有助于对其进行描述。其意图是覆盖与所要求保护的主题一致的所有修改、等同物和替代方案。

[0034] 在附图和随附的描述中,标“a”和“b”和“c”(以及类似的指定符)旨在是表示任何正整数的变量。因此,例如,如果实施方式为a=5设置值,那么图示为部件123-1至123-a(或123a)的一整套部件123可以包括部件123-1、123-2、123-3、123-4和123-5。实施例在此上下文中不受限制。

[0035] 图1A描绘了与公开的实施例一致的示例性计算架构100,也称为系统。尽管图1A至图1C中示出的计算架构100在特定拓扑中具有有限数量的元件,但可以意识到,计算架构100可以如针对给定实施方式所期望的那样在替代拓扑中包括更多或更少的元件。

[0036] 计算架构100包括一个或多个计算设备102、一个或多个服务器106、以及一个或多个非接触式卡104。非接触式卡104代表任何类型的卡,诸如信用卡、借记卡、ATM卡、礼品卡、支付卡、以及智能卡等等。非接触式卡104可以包括一个或多个通信接口124,诸如射频识别(radio frequency identification,RFID)芯片,其被配置为经由NFC、EMV标准或无线通信中的其他短距离协议与计算设备102的通信接口124(本文中也称为“读卡器”、“无线读卡器”、和/或“无线通信接口”)通信。尽管NFC在本文中被用作示例通信协议,但本公开同样适用于其它类型的无线通信,诸如EMV标准、蓝牙和/或Wi-Fi。

[0037] 计算设备102代表任何数量和类型的计算设备,诸如智能手机、平板计算机、可穿戴设备、膝上型计算机、便携式游戏设备、虚拟化计算系统、商家终端、销售点系统、服务器、以及台式计算机等等。移动设备可被用作计算设备102的示例,但不应被认为是对本公开的限制。服务器106代表任何类型的计算设备,诸如服务器、工作站、计算集群、云计算平台、以

及虚拟化计算系统等等。尽管为了清楚起见没有描绘,但计算设备102、非接触式卡104和服务器106各自包括一个或多个处理器电路,例如,以执行程序、代码和/或指令。

[0038] 如图所示,非接触式卡104的存储器108包括小应用程序110、计数器116、一个或多个主密钥114、一个或多个多样化密钥120、唯一ID 112、主账号(primary account number,PAN)序列号156、以及一个或多个唯一派生密钥(Unique Derived Key,UDK)118。唯一ID 112可以是相对于其他非接触式卡104唯一地标识非接触式卡104的任何标识符。PAN序列156可以包括由非接触式卡104存储的计数值。小应用程序110是被配置为执行本文描述的一些或全部操作的可执行代码。计数器116是在非接触式卡104和服务器106之间同步的值。计数器116可以包括每次在非接触式卡104和服务器106(和/或非接触式卡104与计算设备102)之间交换数据时改变的数字。计数器116、主密钥114、多样化密钥120、UDK 118、PAN序列156和/或唯一ID 112用于如下文更详细描述的那样在系统100中提供安全性。

[0039] 如图所示,计算设备102的存储器132包括操作系统134的实例。示例操作系统包括Android®OS、iOS®、macOS®、Linux®和Windows®操作系统。如图所示,操作系统134包括帐户应用程序136。账户应用程序136允许用户执行各种账户相关操作,诸如管理数字钱包、使用钱包处理交易、处理区块链和/或加密货币交易、激活支付卡、查看账户余额、购买物品、以及处理支付等等。在一些实施例中,用户可以使用认证凭证进行认证以访问帐户应用程序136的某些特征。例如,认证凭证可以包括用户名(或登录名)和密码、以及生物识别凭证(例如,指纹、面部ID等)等等。

[0040] 如图所示,服务器106的存储器126包括认证应用程序138和帐户数据库128。账户数据库128通常包括与账户持有者(例如,一个或多个用户)、账户持有者的一个或多个账户、以及账户的一个或多个非接触式卡104相关的信息。

[0041] 如所陈述的,帐户应用程序136可被用于创建、管理、访问或以其他方式使用数字钱包。数字钱包允许一方与另一方进行电子交易。在一些实施例中,数字钱包是存储用于加密货币的私钥和/或公钥的加密货币钱包。加密货币可以是任何类型的加密货币,诸如比特币、以及以太坊等等。为了创建数字钱包,用户可以使用验证凭据对该帐户进行认证。帐户应用程序136然后可以指示用户将非接触式卡104轻拍到计算设备102。

[0042] 在图1A所描绘的实施例中,用户可以轻拍非接触式卡104至计算设备102(或以其他方式将非接触式卡104带入设备102的通信接口124的通信范围内)。帐户应用程序136然后可以指示小应用程序110生成密码122。可以基于任何合适的密码技术来生成密码122。在一些实施例中,密码122可以基于非接触式卡104的唯一ID 112。在一些实施例中,小应用程序110可以包括密码122和未加密标识符(例如,计数器116、PAN序列156、唯一ID 112和/或任何其他唯一标识符)作为包括密码122的数据包的一部分。在至少一个实施例中,数据包是NDEF文件。

[0043] 如所陈述的,计算架构100被配置为实施密钥多样化以使数据安全,其在本文中可被称为密钥多样化技术。通常,服务器106(或另一计算设备)和非接触式卡104可被预分配有相同的主密钥114(也称为主对称密钥)。更具体地,每个非接触式卡104用在服务器106的硬件安全模块(HSM)130中具有对应的对的不同主密钥114进行编程。例如,当非接触式卡104被制造时,唯一主密钥114可以被编程到非接触式卡104的存储器108中。类似地,唯一主密钥114可以被存储在HSM 130中的记录142中。

[0044] 此外,当给定卡104被制造时,UDK 118可以经由HSM函数从主密钥114而被多样化,该HSM函数将多样化因子和对HSM 130中的主密钥114索引(例如,对记录142的索引)的引用作为输入。在一些实施例中,多样化因子可以是非接触式卡104的唯一ID 112和PAN序列156。该UDK 118可以被存储在非接触式卡104和HSM 130的记录142中。主密钥114和UDK 118可以对非接触式卡104和服务器106以外的所有各方保密,从而增强系统100的安全性。尽管被描绘为存储在记录142中,但在一些实施例中,计数器116和/或PAN序列156不被存储在HSM 130中。例如,唯一ID 112、计数器116和PAN序列156可以被存储在账户数据库128中。

[0045] 在一些实施例中,为了生成密码122,小应用程序110可以提供UDK 118、唯一ID 112和多样化因子作为密码算法的输入,从而产生多样化密钥120。在一些实施例中,多样化因子是计数器116。在其它实施例中,PAN序列156是多样化因子。多样化密钥120然后可被用于加密一些数据,诸如多样化因子(例如计数器116和/或PAN序列156)或其它敏感数据。小应用程序110和服务器106可以被配置为加密相同类型的数据以促进密码的解密和/或验证处理。

[0046] 如所陈述的,非接触式卡104的UDK 118和服务器106可以与计数器116结合使用,以使用密钥多样化来增强安全性。如所陈述的,计数器116包括在非接触式卡104和服务器106之间同步的值。计数器116可以包括每次在非接触式卡104和服务器106(和/或非接触式卡104与计算设备102)之间交换数据时改变的数字。当准备发送数据(例如,到服务器106和/或设备102)时,非接触式卡104的小应用程序110可以递增计数器116。非接触式卡104的小应用程序110然后可以将UDK 118、唯一ID 112和计数器116作为输入提供给密码算法,其产生多样化密钥120作为输出。密码算法可以包括加密算法、基于散列的消息认证码(hash-based message authentication code,HMAC)算法、以及基于密码的消息认证码(cipher-based message authentication code,CMAC)算法等等。密码算法的非限制性示例可以包括诸如3DES或AES107的对称加密算法;诸如HMAC-SHA-256的对称HMAC算法;以及诸如AES-CMAC的对称CMAC算法。在2018年11月29日提交的美国专利申请16/205,119中更详细地描述了密钥多样化技术的示例。前述专利申请通过引用以其全部内容并入本文。在一些实施例中,PAN序列156代替计数器116被用作密码算法的输入,以生成多样化密钥120,例如通过加密UDK 118、唯一ID 112和PAN序列156。

[0047] 小应用程序110然后可以使用多样化密钥120和数据作为密码算法的输入来加密一些数据(例如,唯一ID 112、计数器116、PAN序列156、命令和/或任何其他数据)。例如,用多样化密钥120加密唯一ID 112可以导致经加密的唯一ID 112(例如密码122)。如所陈述的,小应用程序110和服务器106可以被配置为加密相同的数据。

[0048] 在一些实施例中,可以生成两个多样化密钥120,例如基于输入到密码函数的一个或多个部分。在一些实施例中,基于两个不同的主密钥114、两个不同的UDK 118、唯一ID 112和计数器116(或PAN序列156)生成两个多样化密钥120。在这种实施例中,使用多样化密钥120中的一个生成消息认证码(message authentication code,MAC),并且可以使用多样化密钥120中的另一个来加密该MAC。MAC可以基于输入到MAC算法的任何合适的数据来生成,诸如敏感数据、唯一ID 112、计数器116和/或PAN序列156。更一般地,小应用程序110和服务器106可以被配置为基于相同的数据生成MAC。在一些实施例中,密码122被包括在诸如NDEF文件的数据包中。帐户应用程序136然后可以经由计算设备102的通信接口124读取包

括密码122的数据包。

[0049] 图1B描绘了其中帐户应用程序136将密码122传送到服务器106的实施例。服务器106可以至少部分地基于由服务器106存储的主密钥114和/或UDK 118的实例将密码122提供给认证应用程序138和/或HSM 130以进行验证。在一些实施例中,认证应用程序138和/或HSM 130可以使用被提供给服务器106的未加密的唯一ID 112来识别UDK 118(或主密钥114)和计数器116。在PAN序列156被用于生成密码122的示例中,服务器106可以使用未加密的唯一ID 112在账户数据库128和/或HSM 130中识别PAN序列156。在一些示例中,认证应用程序138可以将UDK 118、唯一ID 112和计数器116作为输入提供给HSM 130的密码函数,其产生一个或多个多样化密钥120作为输出。在其他实施例中,服务器加密UDK 118、唯一ID 112和PAN序列156以生成多样化密钥120。所得到的多样化密钥120可以对应于非接触式卡104的多样化密钥120,其可以被用于解密密码122和/或一旦解密就验证MAC。例如,服务器106可以基于与小应用程序110相同的数据(诸如敏感数据、唯一ID 112、计数器116和/或PAN序列156)生成MAC。如果由服务器106生成的MAC与密码122中经解密的MAC相匹配,则服务器106可以验证或以其他方式认证密码122。

[0050] 不管所使用的解密技术如何,认证应用程序138和/或HSM 130可以成功地解密密码122并验证MAC,从而验证或认证密码122。如果解密和/或MAC验证成功,则认证应用程序138和/或HSM 130可以为用户生成数字钱包144。通常,为了创建数字钱包144,可以生成私钥146。在一些实施例中,提供随机数作为到加密(或散列)算法中的输入,诸如SHA-2算法或任何其他合适的算法,以生成任何长度的私钥146。在其他实施例中,非接触式卡104的唯一ID 112和PAN序列156被级联并被提供作为到散列算法的输入以生成私钥146。在其他实施例中,非接触式卡104的唯一ID 112和计数器116被级联并被提供作为到散列算法的输入以生成私钥146。

[0051] 在其它实施例中,非接触式卡104的主密钥114、唯一ID 112和计数器116被级联并被提供作为到散列算法的输入以生成私钥146。在主密钥114被用于生成私钥146的实施例中,非接触式卡104的第一主密钥114可被用于生成密码122,并且非接触式卡104的第二主密钥114可被用于生成私钥146,其中第一主密钥和第二主密钥是不同的密钥。在其他实施例中,非接触式卡104的多样化密钥120中的一个、唯一ID 112和计数器116被级联并被提供作为到散列算法的输入以生成私钥146。在其他实施例中,非接触式卡104的UDK 118中的一个、唯一ID 112和计数器116被级联并被提供作为到散列算法的输入以生成私钥146。无论被用于生成私钥146的输入如何,在一些实施例中,盐(例如,随机数据)被包括在用于生成私钥146的散列算法的输入中。

[0052] 私钥146然后可被用于生成对应的公钥148。在一些实施例中,可以基于私钥146使用椭圆曲线数字签名算法(Elliptic Curve Digital Signature Algorithm,ECDSA)来生成公钥148。在一些实施例中,公钥148可以被级联(或压缩),例如使用散列算法。在一些实施例中,盐被用于生成公钥148。可以基于公钥148为数字钱包144生成钱包地址150,例如通过散列公钥148。尽管被描绘为被存储在HSM 130中,在一些实施例中,数字钱包144不是永久地被存储在HSM 130中。而是,如本文更详细地描述的,被用于重新创建私钥146的元素可以被存储在HSM 130和/或账户数据库128中。例如,唯一ID 112和计数器116可以被存储在HSM 130和/或账户数据库128中。在另一示例中,唯一ID 112和PAN序列156可以被存储在

HSM 130和/或账户数据库128中。

[0053] 在一些实施例中,私钥146和/或公钥148可以被进一步多样化,例如,以便创建分层次的确定性密钥。例如,私钥146可以利用计数器116、唯一ID 112、盐值154、或任何其他预定种子值而被多样化。这样做可以使私钥146多样化。类似地,公钥148可以利用计数器116、唯一ID 112、盐值154或任何其他预定种子值而被多样化,以创建多样化的公钥148。在这种实施例中,被用于使私钥146和/或公钥148多样化的任何种子值都可以被存储在帐户数据库128和/或HSM 130的恢复记录152中。更一般地,私钥146和/或公钥148可以使用种子值被多次多样化,从而生成多样化私钥146和/或多样化公钥148的树(或层次结构)。在此类实施例中,树(或层次结构)的一个或多个路径可以被用于指定不同的多样化密钥。更一般地,树的每个节点可以对应于多样化的公钥和/或多样化的子密钥。给定树的一个节点的私钥和公钥,可以派生树中所有后代节点的多样化私钥和公钥。此外,树中的每个叶节点可以对应于多样化的公钥和/或多样化的子密钥。在一些实施例中,路径进一步被用于指定用于交易的属性,诸如货币、货币的量、用于交易的第一钱包地址(例如,发送方钱包地址)、用于交易的第二钱包地址(例如,接收方钱包地址)以及任何其他属性。这些属性可以被存储在树的给定节点中。

[0054] 返回到解密,如果认证应用程序138无法解密密码122(和/或无法验证MAC)则认证应用程序138不使密码122生效。在这种示例中,认证应用程序138确定抑制生成数字钱包。认证应用程序138可以向计算设备102传送失败的解密和/或验证的指示。

[0055] 图1C描绘了其中认证应用程序138将数字钱包144传送到计算设备102的实施例。如图所示,帐户应用程序136可以存储数字钱包144(在存储器132和/或非易失性存储器中,为了清楚起见未图示),其包括私钥146、公钥148和钱包地址150。帐户应用程序136可以散列、加密或以其他方式混淆私钥146、公钥148和/或钱包地址150。帐户应用程序136可以用认证控制(诸如用户名和/或密码、生物识别凭证等)来保护数字钱包144。此外和/或可替选地,帐户应用程序136可以要求使用非接触式卡104的密码解密和/或验证来访问数字钱包144(例如,非接触式卡104生成由如本文所述的服务器106验证的密码)。此外,在一些实施例中,帐户应用程序136可以要求用户提供私钥146来访问数字钱包144和/或使用数字钱包144执行操作。更一般地,帐户应用程序136可以提供各种接口以访问、使用或以其他方式管理数字钱包144。

[0056] 在一些实施例中,数字钱包144可以被存储在基于云的钱包中,例如在服务器106或向客户端提供基于云的钱包服务的另一计算系统中。实施例在此上下文中不受限制。基于云的钱包可以提供用于访问或以其他方式使用数字钱包144(例如经由账户应用程序136)的接口。

[0057] 如图所示,服务器106已经基于数字钱包144的创建在账户数据库128中创建了恢复记录152。恢复记录152包括用于生成私钥146的唯一ID 112、多样化因子158(例如计数器116和/或PAN序列156)以及任何盐154(如果使用的话)。在一些实施例中,恢复记录152可以基于钱包144的钱包地址150而被索引。在其它实施例中,恢复记录152可以基于存储非接触式卡104的密钥的HSM 130的记录142而被索引。在其它实施例中,恢复记录152基于非接触式卡104的唯一ID 112而被索引。恢复记录152然后可以被用于重新创建私钥146,例如基于唯一ID 112、多样化因子158和/或盐154以及适当的算法。在多样化密钥120、UDK 118或主

密钥114被用于生成私钥146的实施例中,有利地,多样化密钥120、UDK 118或主密钥114不被存储在恢复记录152中以提高安全性。在这种实施例中,HSM 130可以存储被用于重新创建私钥146的主密钥114、UDK 118和/或多样化密钥120,而唯一ID 112、多样化因子158和/或盐154可以被存储在账户数据库128中。

[0058] 图2A是示出其中用户请求恢复私钥146的实施例的示意图200。如图所示,为了恢复私钥146,帐户应用程序136可以指示用户将非接触式卡104轻拍到计算设备102,这致使非接触式卡104生成密码208。该密码208可以如上参考密码122所述的那样被生成。例如,小应用程序110可以递增计数器116并且加密一个或多个UDK 118、唯一ID 112和计数器116以生成一个或多个多样化密钥120。该一个或多个多样化密钥120可以被用于基于一些数据生成MAC并加密该MAC和/或该数据。在一些实施例中,MAC是基于钱包地址150以及多样化密钥120之一而被生成的。在这种实施例中,钱包地址150和MAC使用多样化密钥120中的另一个密钥来加密,以生成密码208。作为另一示例,公钥148可以被用于生成MAC,并且公钥148可以用MAC来加密。

[0059] 图2B描绘了其中帐户应用程序136将密码208传送到服务器106以进行验证的实施例。通常,服务器106可以递增计数器116并加密非接触式卡104的UDK 118、唯一ID 112和计数器116,以生成与由非接触式卡104生成的密钥相对应的一个或多个多样化密钥120。该一个或多个多样化密钥120可以被用于解密密码208和/或验证MAC。

[0060] 如果服务器106能够解密密码208和/或验证MAC,则服务器106可以基于恢复记录152重新创建私钥146。在钱包地址150在密码208中被加密的实施例中,恢复记录152可以基于钱包地址150而被索引(例如,搜索),并且服务器106可以使用经解密的钱包地址150访问恢复记录152。在公钥148在密码208中被加密的实施例中,服务器106可以使用公钥148重新生成钱包地址150,并且使用该重新生成的钱包地址150索引账户数据库128。在其他实施例中,帐户数据库128使用唯一ID 112来索引以识别恢复记录152。在这种实施例中,基于被包括在密码208中的唯一ID 112的未加密版本来确定唯一ID 112。

[0061] 一旦服务器106识别出恢复记录152,则恢复记录152可以被用于重新创建私钥146。例如,恢复记录152的唯一ID 112、多样化因子158和盐154(如果使用的话)可以被提供作为HSM 130中的用于初始创建私钥146的函数的输入。这样做重新创建私钥146。

[0062] 在一些实施例中,服务器106进一步基于主密钥114或UDK 118重新创建私钥146。例如,服务器106可以提供非接触式卡104的主密钥114和恢复记录152中的数据(例如,唯一ID 112、多样化因子158和任何盐154)作为HSM 130中的被用于创建私钥146的函数的输入。这样做重新创建私钥146。作为另一示例,服务器106可以提供非接触式卡104的UDK 118和恢复记录152中的数据(例如,唯一ID 112、多样化因子158和任何盐154)作为HSM 130中的被用于创建私钥146的函数的输入。这样做也重新创建私钥146。

[0063] 在一些实施例中,UDK 118、唯一ID 112、多样化因子158和任何盐154被输入到HSM 130中的函数以生成用于生成私钥146的多样化密钥120。可以提供多样化密钥120、多样化因子158和任何盐154作为对HSM 130中的函数的输入以重新创建私钥146。

[0064] 在另一方面,如果HSM 130无法解密密码122和/或验证MAC,则HSM 130不使密码122生效。在这种示例中,认证应用程序138确定抑制恢复私钥146。认证应用程序138可以向计算设备102传送失败的解密和/或MAC验证的指示。在这种实施例中,用户被限制使用恢复

记录152恢复私钥146。

[0065] 图2C描绘了其中HSM 130已经基于恢复记录152重新创建私钥146并且将私钥146传送到帐户应用程序136的实施例。在一些实施例中,服务器106可以在一个或多个数据部分中传送私钥146。更一般地,服务器106可以使用与计算设备102的安全连接来传送私钥146。计算设备102然后可以显示私钥146,从而允许用户恢复私钥146。用户然后可以使用私钥146来执行使用数字钱包144和/或与数字钱包144相关联的任何加密货币的一个或多个操作。例如,私钥146可被用于在区块链906中生成交易。

[0066] 在一些实施例中,私钥146不被传送到计算设备102。例如,在基于云的钱包实施例中,私钥146可以被用于签署交易或其他类型的数据。在这种示例中,用户可以使用账户认证凭证在账户应用程序136中认证他们的账户并且提供预期交易(例如,购买、加密货币转移等)的细节。帐户应用程序136可以将交易细节提供给服务器106。在一些实施例中,帐户应用程序136在密码和/或包括该密码的数据包中提供该交易细节。该密码可以类似于密码122和/或密码208。服务器106然后可以从恢复记录152检索被用于使它们密钥多样化的数据(例如,唯一ID 112、计数器116、PAN序列156和/或盐154)。来自恢复记录152的数据可以被提供给HSM 130,该HSM 130使用来自恢复记录的数据和主密钥114和/或UDK 118生成用于交易的数字签名。这样做会生成交易所需的签名。例如,通过生成有效签名,交易可以使用公钥148进行验证。在这种示例中,交易可以被添加到区块链以反映已验证的交易。

[0067] 图3A是示出其中非接触式卡104被轻拍到计算设备102(例如,以便恢复私钥146)的实施例的示意图300a。如所陈述的,当非接触式卡104被轻拍到计算设备102时,小应用程序110可以生成密码(例如密码122和/或密码208)。该密码和任何其它数据(例如,未加密的唯一ID 112)可以被包括在数据包中,诸如NDEF文件,其由计算设备102读取。计算设备102然后可以将密码传送到服务器106以用于如本文所述的验证(例如,解密和/或MAC验证)。

[0068] 图3B是示出其中服务器106验证了图3A中生成的密码的实施例的示意图300b。基于该验证,服务器106可以基于恢复记录152重新创建私钥146。服务器106然后可以将私钥146传送到帐户应用程序136。如图所示,帐户应用程序136然后可以将私钥146作为一串字符显示在显示器上。在一些实施例中,可以生成矩阵化代码302以表示私钥146。这样做允许对矩阵化代码302进行扫描以确定私钥146。

[0069] 用于所公开的实施例的操作可以参考以下附图来进一步描述。附图中的一些可以包括逻辑流。尽管本文中呈现的此类图可以包括特定逻辑流,但应当理解,逻辑流仅仅提供如本文中所描述的一般功能可以被如何实施的示例。此外,给定的逻辑流不一定必须以所呈现的顺序执行,除非另有说明。而且,在一些实施例中,在一个逻辑流中图示的所有动作可能并非都是必需的。此外,给定的逻辑流可以由硬件元件、由处理器执行的软件元件或其任意组合来实施。实施例在此上下文中不受限制。

[0070] 图4示出了逻辑流或例程400的实施例。逻辑流400可以是由本文所述的一个或多个实施例执行的操作中的一些或全部的代表。例如,逻辑流400可以包括用于创建数字钱包的操作中的一些或全部。实施例在此上下文中不受限制。

[0071] 在块402中,服务器106可以从在计算设备102上执行的帐户应用程序136接收生成数字钱包的请求。该请求可以包括由非接触式卡104生成并传送到计算设备102的密码。在块404中,服务器可以通过基于主密钥114、UDK 118和计数器116生成一个或多个多样化密

钥120来解密密码。服务器106可以进一步验证密码,例如确定由服务器106生成的MAC与经解密的密码中的MAC匹配。

[0072] 在块406中,服务器106基于在块404处密码的成功解密和/或验证来生成私钥146。私钥146可以基于对HSM 130的密码函数的输入。该输入可以包括唯一ID 112和多样化因子158(例如非接触式卡104的计数器116和/或PAN序列156)。在一些实施例中,输入可以进一步包括主密钥114、UDK 118和/或多样化密钥120。在块408中,服务器106可以基于私钥146生成公钥148。服务器可以进一步基于公钥148为数字钱包144创建钱包地址150。在块410中,服务器可以向应用程序传送私钥146、公钥148和钱包地址150。在块412中,服务器106在账户数据库128中存储用于生成私钥的一个或多个输入(例如,唯一ID 112和多样化因子158)。

[0073] 图5示出了逻辑流或例程500的实施例。逻辑流500可以是由本文所述的一个或多个实施例执行的操作中的一些或全部的代表。例如,逻辑流500可以包括访问用于数字钱包的操作中的一些或全部。实施例在此上下文中不受限制。

[0074] 在块502中,例程500通过服务器106从在计算设备102上执行的帐户应用程序136接收访问数字钱包144的请求,该请求包括密码。在块504中,服务器106可以通过基于主密钥114、UDK 118和计数器116生成一个或多个多样化密钥120来解密密码。服务器106可以进一步验证密码,例如确定由服务器106生成的MAC与经解密的密码中的MAC匹配。在块506中,服务器可以基于成功的解密和验证生成授权。该授权通常可以指示对数字钱包144的所请求的访问将被允许。在块508中,服务器将授权传送到帐户应用程序136。该授权可以致使账户应用程序136允许对数字钱包144的所请求的访问。然而在一些实施例中,访问数字钱包144还进一步要求私钥146。

[0075] 图6示出了逻辑流或例程600的实施例。逻辑流600可以是由本文描述的一个或多个实施例执行的操作中的一些或全部的代表。例如,逻辑流600可以包括用于为数字钱包恢复私钥的操作中的一些或全部。实施例在此上下文中不受限制。

[0076] 在块602中,例程600通过服务器106从帐户应用程序136接收用于为数字钱包144恢复私钥146的请求。该请求可以包括由非接触式卡104基于密钥多样化(例如基于主密钥114、UDK 118和一个或多个多样化密钥120)生成的密码。在块604中,服务器106可以通过基于主密钥114、UDK 118和计数器116生成一个或多个多样化密钥120来解密密码。服务器106可以进一步验证密码,例如确定由服务器106生成的MAC与经解密的密码中的MAC匹配。

[0077] 在块606中,服务器106可以基于解密和验证,确定账户数据库128中的非接触式卡104的唯一ID 112和多样化因子158(例如计数器116和/或PAN序列156)。在块608中,服务器106基于唯一ID 112、多样化因子158和任何盐154重新创建私钥146。在一些实施例中,服务器106基于主密钥114、唯一ID 112、多样化因子158和任何盐154重新创建私钥146。在一些实施例中,服务器106基于UDK 118、唯一ID 112、多样化因子158和任何盐154重新创建私钥146。在一些实施例中,服务器106基于多样化密钥120、唯一ID 112、多样化因子158和任何盐154重新创建私钥146。在块610中,服务器106经由网络将重新创建的私钥146传送到帐户应用程序136。

[0078] 图7A是示出非接触式卡104的示例配置的示意图700,其可以包括由在非接触式卡104的正面或背面显示为服务提供商标记702的服务提供商发行的支付卡,诸如信用卡、借

记卡或礼品卡。在一些示例中,非接触式卡104不与支付卡相关,并且可以包括但不限于身份卡。在一些示例中,交易卡可以包括双接口非接触式支付卡、奖励卡等等。非接触式卡104可以包括基板704,其可以包括单层或由塑料、金属和其它材料构成的一个或多个层压的层。示例性的基板材料包括聚氯乙烯、聚氯乙烯乙酸酯、丙烯腈丁二烯苯乙烯、聚碳酸酯、聚酯、阳极化钛、钯、金、碳、纸和生物可降解材料。在一些示例中,非接触式卡104可以具有符合ISO/IEC 7816标准的ID-1格式的物理特性,并且交易卡可以以其他方式符合ISO/IEC 14443标准。然而,应当理解,根据本公开的非接触式卡104可以具有不同的特征,并且本公开不要求以支付卡实施交易卡。

[0079] 非接触式卡104还可以包括显示在卡的正面和/或背面上的标识信息706,以及接触垫708。接触垫708可以包括一个或多个垫并且被配置为经由交易卡与另一客户端设备(诸如ATM、用户设备、智能手机、膝上型计算机、台式机或平板电脑)建立接触。接触垫可以根据一个或多个标准来设计,诸如ISO/IEC 7816标准,并且使能根据EMV协议的通信。非接触式卡104还可以包括处理电路、天线和其他部件,如将在图7B中进一步讨论的那样。这些部件可以位于接触垫708后面或基板704上的其他地方,例如基板704的不同层内,并且可以与接触垫708电气耦合和物理耦合。非接触式卡104还可以包括磁条或磁带,其可以位于卡的背面(图7A中未示出)。非接触式卡104还可以包括与能够经由NFC协议进行通信的天线耦合的近场通信(Near-Field Communication,NFC)设备。实施例不以这种方式受到限制。

[0080] 如图7B所示,非接触式卡104的接触垫708可以包括用于存储、处理和传送信息的处理电路710,该处理电路710包括处理器712、存储器108和一个或多个通信接口124。应当理解,处理电路710可以包含用于执行本文所述的功能所必需的附加部件,该附加部件包括处理器、存储器、错误和奇偶校验/CRC校验器、数据编码器、防冲突算法、控制器、命令解码器、安全原语和防篡改硬件。

[0081] 存储器108可以是只读存储器、一次写入多次读取存储器或读/写存储器,例如,RAM、ROM和EEPROM,并且非接触式卡104可以包括这些存储器中的一个或多个。只读存储器可以在工厂可编程为只读或一次性可编程。一次性可编程提供了一次写入然后多次读取的机会。一次写入/多次读取存储器可以在存储器芯片出厂后的某个时间点被编程。一旦存储器被编程,它不可以被重写,但它可以被多次读取。读/写存储器可以在出厂后被多次编程和重新编程。读/写存储器也可以在出厂后被多次读取。在一些实例中,存储器108可以是利用由处理器712执行的加密算法来加密数据的加密存储器。

[0082] 存储器108可以被配置为存储一个或多个小应用程序110、一个或多个计数器116、唯一ID 112、主密钥114、UDK 118、多样化密钥120以及PAN序列156。该一个或多个小应用程序110可以包括被配置为在一个或多个非接触式卡104上执行的一个或多个软件应用程序,诸如Java®卡小应用程序。然而,应当理解,小应用程序110不限于Java卡小应用程序,而是可以是在非接触式卡或具有有限存储器的其它设备上可操作的任何软件应用程序。该一个或多个计数器116可以包括足以存储整数的数值计数器。唯一ID 112可以包括被分配给非接触式卡104的唯一字母数字标识符,并且该标识符可以将非接触式卡104与其它非接触式卡104区分开。在一些示例中,唯一ID 112可以标识客户和分配给该客户的帐户两者。

[0083] 参照接触垫708描述了前述示例性实施例的处理器712和存储器元件,但本公开不限于此。应当理解,这些元件可以被实施在接触垫708之外或与其完全分开,或者作为除了

位于接触垫708内的处理器712和存储器108之外的另外的元件来实施。

[0084] 在一些示例中,非接触式卡104可以包括一个或多个天线714。该一个或多个天线714可以被放置在非接触式卡104内并围绕接触垫708的处理电路710。例如,该一个或多个天线714可与处理电路710集成并且该一个或多个天线714可以与外部升压线圈一起使用。作为另一示例,一个或多个天线714可以在接触垫708和处理电路710的外部。

[0085] 在实施例中,非接触式卡104的线圈可以充当空气芯变压器的次级。终端可以通过切断功率(cutting power)或幅度调制与非接触式卡104通信。非接触式卡104可以使用非接触式卡104的电源连接中的间隙推断从终端传送的数据,该间隙可以通过一个或多个电容器在功能上保持。非接触式卡104可以通过切换非接触式卡104的线圈上的负载或负载调制来回传。负载调制可以通过干扰在终端的线圈中被检测到。更一般地,使用天线714、处理器712和/或存储器108,非接触式卡104提供通信接口以经由NFC、蓝牙和/或Wi-Fi通信进行通信。

[0086] 如上所解释的,非接触式卡104可以被构建在可在智能卡或具有有限存储器的其它设备(诸如JavaCard)上操作的软件平台上,并且一个或多个或多个应用程序或小应用程序可以被安全地执行。小应用程序110可以被添加到非接触式卡,以在各种基于移动应用程序的用例中提供用于多因子认证(multifactor authentication,MFA)的一次性密码(OTP)。小应用程序110可以被配置为响应来自读取器(诸如移动NFC读取器(例如,移动计算设备102或销售点终端))的一个或多个请求,诸如近场数据交换请求,并产生NDEF消息,该NDEF消息包括被编码为NDEF文本标签的密码安全OTP。NDEF消息可以包括诸如密码122或密码208的密码以及任何其他数据。

[0087] NDEF OTP的一个示例是NDEF短记录布局(SR=1)。在这种示例中,一个或多个小应用程序110可以被配置为将OTP编码为NDEF类型4公知类型的文本标签。在一些示例中,NDEF消息可以包括一个或多个记录。小应用程序110可以被配置为除了OTP记录之外添加一个或多个静态标签记录。

[0088] 在一些示例中,一个或多个小应用程序110可以被配置为模拟RFID标签。RFID标签可以包括一个或多个多态性标签。在一些示例中,每次读取标签时,呈现可以指示非接触式卡的真实性的不同密码数据。基于一个或多个小应用程序110,标签的NFC读取可以被处理,数据可以被传送到服务器,诸如银行系统的服务器,并且数据可以在服务器处被验证。

[0089] 在一些示例中,非接触式卡104和服务器可以包括某些数据,使得卡可以被正确地识别。非接触式卡104可以包括一个或多个唯一标识符(未图示)。每次发生读取操作时,计数器116可以被配置为递增。在一些示例中,每次读取(例如,通过移动设备)来自非接触式卡104的数据时,计数器116被传送到服务器以用于验证,并且确定计数器116是否等于(作为验证的一部分)服务器的计数器。

[0090] 一个或多个计数器116可以被配置为防止重放攻击。例如,如果已经获得和重放了密码,则如果计数器116已经被读取或使用或以其他方式过去了,则该密码立即被拒绝。如果计数器116还没有被使用,则它可以被重放。在一些示例中,在非接触式卡104上递增的计数器不同于针对交易而递增的计数器。非接触式卡104无法确定应用程序交易计数器116,因为在非接触式卡104上的小应用程序110之间没有通信。在一些示例中,非接触式卡104可以包括第一小应用程序440-1,其可以是交易小应用程序,以及第二小应用程序440-2。每个

小应用程序440-1和440-2可以包括相应的计数器116。

[0091] 在一些示例中,计数器116可能会不同步。在一些示例中,为了考虑发起交易的意外读取,诸如以某个角度读取,计数器116可以递增但应用程序不处理计数器116。在一些示例中,当设备102被唤醒时,NFC可以被启用并且计算设备102可以被配置为读取可用标签,但是没有响应于读取而采取任何动作。

[0092] 为了使计数器116保持同步,应用程序(诸如后台应用程序)可以被执行为将被配置为检测计算设备102何时唤醒并与银行系统的服务器同步,指示由于检测而发生的读取,然后向前移动计数器116。在其他示例中,可以利用散列的一次性密码使得失同步的窗口可以被接受。例如,如果在阈值10内,则计数器116可以被配置为向前移动。但是如果在不同的阈值数内,例如在10或600内,则可以处理用于执行重新同步的请求,该请求经由一个或多个应用程序请求用户经由用户的设备进行轻拍、做出手势或以其它方式指示一次或多次。如果计数器116以适当的顺序增加,则可以知道用户已经这样做了。

[0093] 本文参考计数器116、主密钥114、UDK 118和多样化密钥120描述的密钥多样化技术是加密和/或解密密钥多样化技术的一个示例。该示例密钥多样化技术不应被认为是对本公开的限制,因为本公开同样适用于其他类型的密钥多样化技术。

[0094] 在非接触式卡104的创建过程期间,每个卡可以被唯一地分配两个密码密钥。该密码密钥可以包括对称密钥,该对称密钥可以被用于数据的加密和解密两者。三重DES(3DES)算法可以由EMV使用并且其由非接触式卡104中的硬件实施。通过使用密钥多样化过程,可以基于要求密钥的每个实体的唯一可识别信息从主密钥导出一个或多个密钥。

[0095] 在一些示例中,为了克服3DES算法的缺陷(其可能容易受到漏洞的影响),可以导出会话密钥(诸如每个会话的唯一密钥)但不是使用主密钥,唯一的卡导出的密钥(例如UDK 118)和计数器可以被用作多样化数据。例如,每次在操作中使用非接触式卡104时,不同的密钥可以被用于创建消息认证码(MAC)和用于执行加密。这会产生三重加密层。会话密钥可以由一个或多个小应用程序生成,并通过使用应用程序交易计数器连同一个或多个算法(如EMV 4.3Book 2A1.3.1Common Session Key Derivation中定义的)来导出。

[0096] 此外,针对每个卡的递增可以是唯一的,并且或者通过个性化来分配,或者通过一些识别信息来在算法上分配。例如,奇数编号的卡可以递增2并且偶数编号的卡可以递增5。在一些示例中,该递增也可以在顺序读取中变化,使得一个卡可以按序列1、3、5、2、2、...重复来递增。特定序列或算法序列可以在个性化时被限定,或者从源自唯一标识符的一个或多个过程定义。这会使重放攻击者更难从少量卡实例中进行泛化。

[0097] 认证消息可以作为以十六进制ASCII格式的文本NDEF记录的内容被递送。在另一示例中,NDEF记录可以以十六进制格式进行编码。

[0098] 图8示出了根据示例实施例的NDEF短记录布局(SR=1)数据结构800。一个或多个小应用程序110可以被配置为将OTP编码为NDEF类型4公知的类型文本标签。在一些示例中,NDEF消息可以包括一个或多个记录。小应用程序可以被配置为除了OTP记录之外添加一个或多个静态标签记录。示例性标签包括但不限于标签类型:公知类型、文本、编码英语(encoding English,en);小程序ID:D2760000850101;能力:只读访问;编码:认证消息可以被编码为ASCII十六进制;类型长度值(type-length-value,TLV)数据可以作为可被用于生成NDEF消息的个性化参数提供。在实施例中,认证模板可以包括第一记录,其具有用于提供

实际的动态认证数据的公知索引。数据结构800可以包括诸如密码122或密码208的密码以及由小应用程序110提供的任何其他数据。

[0099] 图9描绘了与公开的实施例一致的示例性系统900的示意图。系统900可以包括可通过网络902访问区块链906的系统。

[0100] 系统900可以使用区块链906生成交互的非信誉记录。此外,区块链906可以跨多个计算系统分布,鼓励对存储在区块链906中的记录的有效性的信任。以这种方式,所公开的系统提供了一种创新的技术解决方案,用于至少上述技术问题与常规系统。

[0101] 用户系统904可以包括计算设备102。用户系统904可以被配置为处理使用数字钱包144的交易,与公开的实施例一致。用户系统904可以包括计算设备,诸如服务器、工作站、台式机、或移动设备(例如,膝上型电脑、平板电脑、平板手机、智能电话、智能手表或类似的移动计算设备)。如下文关于图12所述,用户系统904可以被配置有显示器和输入/输出接口。用户系统904可以被配置为使用该显示器和输入/输出接口与用户(未示出)交互。

[0102] 成员系统908可以被配置为处理交易,与公开的实施例一致。成员系统908可以包括一个或多个计算设备,诸如服务器、工作站、台式计算机或专用计算设备。成员系统908可以是独立的,或者它可以是子系统的一部分,子系统可以是更大系统的一部分。例如,成员系统908可以与商业机构相关联。成员系统908可以包括分布式服务器,其远程地定位并且通过公共网络、或者通过专用私有网络与金融机构的其他系统通信。

[0103] 成员系统908可以被配置为接收对处理使用数字钱包144的加密货币的交易的请求。在一些实施例中,成员系统908可以被配置为从系统900的另一个元件(诸如另一个成员系统908和/或用户系统904)接收请求。成员系统908可以被配置为与区块链906交互以处理交易请求。

[0104] 成员系统908可以被配置为在区块链906中存储消息,与公开的实施例一致。在某些方面,成员系统908可以被配置为将包含消息的块添加到区块链906。在各个方面,成员系统908可以被配置为将消息提供给授权系统。授权系统可以被配置为将包含该消息的块添加到区块链906。如下所述关于图10所述,该消息可以包括交易记录。

[0105] 区块链906可以包括分布式数据结构,与公开的实施例一致。区块链906可以是私有区块链。例如,授权系统可以存储区块链906的副本。这些授权系统可以被配置为将块添加到区块链906并将块发布到其他授权系统。授权系统可以被配置为从其他系统接收消息以用于在区块链906中发布。这些其他系统可以具有对区块链906的只读访问。在一些实施例中,一个或多个成员系统908是授权系统。在一些实施例中,一个或多个用户系统904是授权系统。如关于图9详细描述的,区块链906可以被配置为存储来自成员系统的消息,该消息包括交易。

[0106] 网络902可以被配置为在图9的部件之间提供通信。例如,网络902可以是提供通信、交换信息和/或促进信息的交换的任何类型的网络(包括基础设施),诸如因特网、局域网或使认证系统900能够在认证系统900的部件之间发送和接收信息的其它适当连接。

[0107] 图10描绘了示例性区块链906的逻辑模型1000,与公开的实施例一致。区块链906可以包括由许多不同系统(例如,成员系统908,或其他系统)维护的许多这样的区块链。这种示例性区块链可以包括块,诸如块1006a至块1006d。块可以包括消息,诸如消息1008a至消息1008d。通常,块可以包括报头,诸如报头1002a至1002d,其唯一地标识每个块。报头

1002a至1002d可以包括由散列函数生成的散列值。散列函数是可被用于将任意大小的输入数据映射到固定大小的散列值的任何函数。例如,报头可以包括前一个块的散列值、基于块中的任何消息(例如,Merkle根)生成的散列值和时间戳中的至少一个。与公开的实施例一致,系统900可以要求被添加到区块链906的块满足工作证明条件和数字签名条件中的至少一个。例如,报头1002a至1002d可以包括被选择为确保报头满足工作证明条件1004a至1004d的随机数。作为非限制性示例,工作证明条件1004a至1004d可以要求报头的散列落在预定的值范围内。作为附加示例,报头可以用授权系统的密码密钥(例如私钥146)进行数字签名,并且该数字签名可以被包括在报头中。此数字签名可以使用系统900的成员可用的密钥来验证。

[0108] 图11描绘了存储在区块链(例如区块链906的元件)中的消息1008b的逻辑模型1100,与公开的实施例一致。在一些实施例中,消息1008b可以包括索引信息1102。在某些方面,索引信息1102可以包括标识用户的信息。例如,索引信息1102可以是用户的全名、电子邮件地址、电话号码或其他非敏感个人信息中的至少一个。在各个方面,索引信息1102可以包括对私有区块链中的较早块的一个或多个引用。例如,索引信息1102可以包括对与同一用户相关联的一个或多个较早块的一个或多个引用。作为非限制性示例,引用可以包括与同一用户相关联的区块链中的先前块的散列。在一些方面,索引信息1102可以根据本领域技术人员已知的方法进行混淆或加密。例如,索引信息1102可以用密码密钥(诸如私钥146)来加密。作为附加示例,索引信息1102可以包括用户的全名、电子邮件地址、电话号码或其他非敏感个人信息中的至少一个的散列。

[0109] 消息1008b可以包括附加信息1104,与所公开的实施例一致。该附加信息1104可以包括交易细节,例如,正从一个数字钱包144转移到另一个数字钱包144的加密货币的量。在各个方面,附加信息1104可以根据本领域技术人员已知的方法进行混淆或加密。例如,根系统信息1104可以用诸如私钥146的密码密钥来加密。

[0110] 消息1008b可以包括认证记录1106,与公开的实施例一致。在一些方面,认证记录1106可以包括使得能够对交易进行后续审计的信息。例如,认证记录1106可以标识成员系统908、与成员系统908相关联的商业机构、认证记录1106的目的(例如,交易细节)中的至少一个。在某些方面,认证记录1106可以根据本领域技术人员已知的方法被混淆或加密。例如,认证记录1106可以用诸如私钥146的密码密钥来加密。

[0111] 诸如私钥146的密码密钥可以被用于加密块中的消息的元素,与公开的实施例一致。在一些方面,这种密码密钥可以与认证系统900的成员(例如,成员系统908)相关联。在各个方面,至少一些密码密钥可以与授权系统相关联。诸如公共密钥148的对应密码密钥可以被用于解密经加密的消息元素,与公开的实施例一致。例如,当块中的消息的元素用对称密钥来加密时,相同的对称密钥可用于解密该经加密的元素。作为另一示例,当用私钥146加密块中的消息的元素时,对应的公钥148可用于解密该经加密的元素。在一些方面中,对应的密码密钥可以对认证系统的成员(例如,成员系统908)可用。

[0112] 图12示出了适用于实施如前所述的各种实施例的示例性计算机架构1200的实施例。在一个实施例中,计算机架构1200可以包括或被实施为计算架构100的一部分。

[0113] 如在本申请中所使用的,术语“系统”和“部件”旨在指的是计算机相关的实体,要么是硬件、硬件和软件的组合、软件,要么是执行中的软件,其示例由示例性计算计算机架

构1200提供。例如,部件可以是但不限于在处理器上运行的过程、处理器、硬盘驱动器、多个存储驱动器(光学和/或磁性存储介质)、对象、可执行文件、执行线程、程序和/或计算机。通过举例说明,在服务器上运行的应用程序和服务器都可以是部件。一个或多个部件可以驻留在执行的过程和/或线程内,并且部件可以被本地化在一台计算机上和/或分布在两台或更多台计算机之间。另外,部件可以通过各种类型的通信介质通信地彼此耦合以协调操作。该协调可以涉及信息的单向或双向交换。例如,部件可以以通过通信介质进行传送的信号的形式来传送信息。该信息可以被实施为分配给各种信号线的信号。在这样的分配中,每个消息都是一个信号。然而,进一步的实施例可以替代地采用数据消息。这种数据消息可以跨各种连接来发送。示例性连接包括并行接口、串行接口和总线接口。

[0114] 计算机架构1200包括各种通用计算元件,诸如一个或多个处理器、多核处理器、协处理器、存储器单元、芯片组、控制器、外围设备、接口、振荡器、定时设备、视频卡、音频卡、多媒体输入/输出(I/O)部件、电源等等。然而,实施例不限于由计算计算机架构1200实施。

[0115] 如图12所示,计算机架构1200包括计算机1212,该计算机1212包括处理器1202、系统存储器1204和系统总线1206。处理器1202可以是各种市售处理器中的任一种。计算机1212可以代表计算设备102和/或服务器106。

[0116] 系统总线1206提供用于系统部件(包括但不限于系统存储器1204)到处理器1202的接口。系统总线1206可以是可进一步互连到存储器总线(具有或不具有存储器控制器)、外围总线和使用多种市售总线架构中的任一种的局部总线的若干类型的总线结构中的任一种。接口适配器可以经由插槽架构连接到系统总线1206。示例槽架构可以包括但不限于加速图形端口(Accelerated Graphics Port,AGP)、卡总线、(扩展)工业标准架构((Extended)Industry Standard Architecture,(E)ISA)、微通道架构(Micro Channel Architecture,MCA)、NuBus、外围部件互连(扩展)(Peripheral Component Interconnect (Extended),PCI(X))、PCI Express、以及个人计算机存储器卡国际协会(Personal Computer Memory Card International Association,PCMCIA)等等。

[0117] 计算机架构1200可以包括或实施各种制品的制造。制造的制品可以包括存储逻辑的计算机可读存储介质。计算机可读存储介质的示例可以包括能够存储电子数据的任何有形介质,包括易失性存储器或非易失性存储器、可移动或不可移动存储器、可擦除或不可擦除存储器、以及可写或可重写存储器等等。逻辑的示例可以包括使用任何合适类型的代码实施的可执行计算机程序指令,诸如源代码、编译代码、解释代码、可执行代码、静态代码、动态代码、面向对象的代码、以及可视化代码等等。实施例还可以至少部分地实施为包含在非暂时性计算机可读介质中或其上的指令,该指令可以由一个或多个处理器读取和执行以实现本文所述操作的性能。

[0118] 系统存储器1204可以包括各种类型的一个或多个较高速度存储器单元形式的计算机可读存储介质,诸如只读存储器(read-only memory,ROM)、随机存取存储器(random-access memory,RAM)、动态RAM(dynamic RAM,DRAM)、双数据速率DRAM(Double-Data-Rate DRAM,DDRAM)、同步DRAM(synchronous DRAM,SDRAM)、静态RAM(static RAM,SRAM)、可编程ROM(programmable ROM,PROM)、可擦除可编程ROM(erasable programmable ROM,EPROM)、电可擦除可编程ROM(electrically erasable programmable ROM,EEPROM)、闪存、聚合物存储器(诸如铁电聚合物存储器)、双向存储器、相变或铁电存储器、硅-氧化物-氮化物-氧

化物-硅(silicon-oxide-nitride-oxide-silicon,SNONOS)存储器、磁卡或光卡、诸如独立磁盘冗余阵列(Redundant Array of Independent Disks,RAID)驱动器的设备阵列、固态存储器设备(例如,USB存储器、固态驱动器(solid state drives,SSD))和适于存储信息的任何其它类型的存储介质。在图12中所示的实施例中,系统存储器1204可以包括非易失性1208和/或易失性1210。基本输入/输出系统(basic input/output system,BIOS)可以被存储在非易失性1208中。

[0119] 计算机1212可以包括以一个或多个较低速度存储器单元形式的各种类型的计算机可读存储介质,包括内部(或外部)硬盘驱动器1214、从可移动磁盘1218读取或写入到可移动磁盘1218的磁盘驱动器1216、以及从可移动光盘1222(例如CD-ROM或DVD)读取或写入到可移动光盘1222的光盘驱动器1220。硬盘驱动器1214、磁盘驱动器1216和光盘驱动器1220可以分别通过HDD接口1224、以及FDD接口1226和光盘驱动器接口1228连接到系统总线1206。用于外部驱动器实施方式的HDD接口1224可以包括通用串行总线(Universal Serial Bus,USB)和IEEE 1394接口技术中的至少一者或两者。

[0120] 驱动器和相关联的计算机可读介质提供数据、数据结构、以及计算机可执行指令等等的易失性和/或非易失性存储。例如,多个程序模块可以被存储在驱动器和非易失性1208、以及易失性1210中,其包括操作系统1230、一个或多个应用程序1232、其它程序模块1234、和程序数据1236。在一个实施例中,一个或多个应用程序1232、其他程序模块1234和程序数据1236可以包括例如系统100的各种应用程序和/或部件。

[0121] 用户可以通过一个或多个有线/无线输入设备,例如键盘1238和指针设备(诸如鼠标1240),将命令和信息输入到计算机1212中。其它输入设备可以包括麦克风、红外(infra-red,IR)遥控器、射频(radio-frequency,RF)遥控器、游戏垫、触控笔、读卡器、加密狗、指纹读取器、手套、图形平板、操纵杆、键盘、视网膜读取器、触摸屏(例如电容式、电阻式等等)、轨迹球、跟踪垫、传感器、以及触针等等。这些和其它输入设备通常通过耦合到系统总线1206的输入设备接口1242连接到处理器1202,但是可以通过诸如并行端口、IEEE 1394串行端口、游戏端口、USB端口、以及IR接口等等的其它接口连接。

[0122] 监视器1244或其它类型的显示设备也经由接口(诸如视频适配器1246)连接到系统总线1206。监视器1244可以在计算机1212的内部或外部。除了监视器1244之外,计算机典型地包括其他外围输出设备,诸如扬声器、打印机等等。

[0123] 计算机1212可以使用经由有线和/或无线通信到一个或多个远程计算机(诸如远程计算机1248)的逻辑连接在联网环境中操作。远程计算机1248可以是工作站、服务器计算机、路由器、个人计算机、便携式计算机、基于微处理器的娱乐电器、对等设备或其它公共网络节点,并且典型地包括相对于计算机1212描述的许多或所有元件,尽管为了简介起见,仅仅示出了存储器和/或存储设备1250。所描绘的逻辑连接包括到局域网1252和/或更大的网络(例如,广域网1254)的有线/无线连接。这种LAN和WAN联网环境在办公室和公司中是司空见惯的,并且有利于企业范围的计算机网络,诸如内联网,所有这些都可以连接到全球通信网络,例如因特网。

[0124] 当在局域网1252联网环境中使用时,计算机1212通过有线和/或无线通信网络接口或网络适配器1256连接到局域网1252。网络适配器1256可以促进到局域网1252的有线和/或无线通信,其还可以包括设置在其上的无线接入点,用于与网络适配器1256的无线功

能进行通信。

[0125] 当在广域网1254联网环境中使用时,计算机1212可以包括调制解调器1258,或者连接到广域网1254上的通信服务器,或者具有用于通过广域网1254建立通信的其它装置,诸如通过因特网的方式。调制解调器1258,其可以是内部的或外部的以及有线和/或无线设备,经由输入设备接口1242连接到系统总线1206。在联网环境中,相对于计算机1212描绘的程序模块或其部分可以被存储在远程存储器和/或存储设备1250中。应当理解,所示的网络连接是示例性的,并且可以使用在计算机之间建立通信链路的其他手段。

[0126] 计算机1212可操作以使用IEEE 802系列标准与有线和无线设备或实体通信,诸如可操作地设置在无线通信中的无线设备(例如,IEEE 802.11空中调制技术)。这至少包括Wi-Fi(或无线保真)、WiMax和Bluetooth™无线技术等。因此,通信可以是与常规网络一样的预定义结构或者仅仅是至少两个设备之间的自组织通信。Wi-Fi网络使用被称为IEEE 802.11(a,b,g,n,ac,ax等)的无线电技术来提供安全、可靠、快速的无线连接。Wi-Fi网络可以被用于将计算机相互连接、连接到因特网以及连接到有线网络(使用IEEE 802.3相关媒体和功能)。

[0127] 如先前参考图1A至图12所描述的设备的各种元件可以包括各种硬件元件、软件元件或两者的组合。硬件元件的示例可以包括设备、逻辑设备、部件、处理器、微处理器、电路、处理器、电路元件(例如,晶体管、电阻器、电容器、电感器等等)、集成电路、专用集成电路(ASIC)、可编程逻辑设备(PLD)、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、存储器单元、逻辑门、寄存器、半导体设备、微芯片、芯片组等。软件元件的示例可以包括软件部件、程序、应用程序、计算机程序、应用程序程序、系统程序、软件开发程序、机器程序、操作系统软件、中间件、固件、软件模块、例程、子例程、功能、方法、程序、软件接口、应用程序程序接口(API)、指令集、计算代码、计算机代码、代码段、计算机代码段、字、值、符号或其任意组合。然而,确定实施例是否使用硬件元件和/或软件元件来实施可以根据任意数量的因子而变化,诸如,如给定实施方式所期望的,期望的计算速率、功率水平、热容限、处理周期预算、输入数据速率、输出数据速率、存储器资源、数据总线速度和其它设计或性能约束。

[0128] 至少一个实施例的一个或多个方面可以通过存储在机器可读介质上的代表性指令来实施,其表示处理器内的各种逻辑,该代表性指令在被机器读取时致使机器制造逻辑以执行本文所述的技术。这种表示,被称为“IP核”可以被存储在有形的、机器可读的介质上,并被提供给各种客户或制造设施,以加载到制造逻辑或处理器的制造机器中。一些实施例可以例如使用可以存储指令或指令集的机器可读介质或制品来实施,该指令或指令集如果由机器执行,可以致使机器执行根据实施例的方法和/或操作。这种机器可以包括例如任何合适的处理平台、计算平台、计算设备、处理设备、计算系统、处理系统、计算机、处理器或类似物,并且可以使用硬件和/或软件的任何合适的组合来实施。该机器可读介质或制品可以包括例如任何合适类型的存储器单元、存储器设备、存储器制品、存储器介质、存储设备、存储制品、存储介质和/或存储单元,例如存储器、可移动或不可移动介质、可擦除或不可擦除介质、可写或可重写介质、数字或模拟介质、硬盘、软盘、光盘只读存储器(CD-ROM)、可记录光盘(CD-R)、可重写光盘(CD-RW)、光学盘、磁性介质、磁光介质、可移动存储卡或磁盘、各种类型的数字多功能盘(DVD)、磁带、盒式磁带或类似物。指令可以包括任何合适类型的代码,诸如源代码、编译代码、解释代码、可执行代码、静态代码、动态代码、加密代码等等,使

用任何合适的高级、低级、面向对象、可视、编译和/或解释的编程语言来实施。

[0129] 以上描述的设备的部件和特征可以使用分立电路、专用集成电路(ASIC)、逻辑门和/或单芯片架构的任何组合来实施。此外,设备的特征可以在适当的情况下使用微控制器、可编程逻辑阵列和/或微处理器或前述的任何组合来实施。应当注意,硬件、固件和/或软件元件在本文中可以被集体地或单独地称为“逻辑”或“电路”。

[0130] 将意识到,在上面描述的框图中示出的示例性设备可以表示许多潜在实施方式的一个功能描述性示例。因此,在附图中描绘的块功能的划分、省略或包含并不暗指用于实施这些功能的硬件部件、电路、软件和/或元件必然被划分、省略或包含在实施例中。

[0131] 至少一个计算机可读存储介质可以包括指令,该指令在被执行时致使系统执行本文所述的计算机实施的方法中的任一者。

[0132] 一些实施方案可以使用表述“一个实施例”或“实施例”连同它们的衍生物来描述。这些术语意味着结合实施例描述的特定特征、结构或特性被包括在至少一个实施例中。说明书中各个地方的短语“在一个实施例中”的出现不一定都指同一实施例。此外,除非另有说明,否则以上描述的特征被认为可以以任何组合一起使用。因此,单独讨论的任何特征可以彼此组合地采用,除非注意到特征彼此不兼容。

[0133] 应当强调,提供本公开内容的摘要以允许读者快速确定本技术公开内容的性质。所提交的理解是,它将不会被用来解释或限制权利要求的范围或含义。此外,在前面的详细描述中,可以看出,出于简化本公开的目的,在单个实施例中将各种特征分组在一起。本公开的方法不应被解释为反映所要求保护的实施例需要比在每个权利要求中明确提及的更多特征的意图。而是,如以下权利要求所反映的,发明性主题在于少于单个公开实施例的所有特征。因此下面的权利要求在此并入详细描述中,其中每个权利要求作为单独的实施例独立存在。在所附权利要求中,术语“包括(including)”和“在其中(in which)”分别被用作相应术语“包含(comprising)”和“其中(wherein)”的简明英语等价物。此外,术语“第一”、“第二”、“第三”等仅用作标签,并不旨在对其对象施加数字要求。

[0134] 以上已经描述的内容包括所公开的架构的示例。当然,不可能描述部件和/或方法的每个可想到的组合,但是本领域普通技术人员可以认识到许多进一步的组合和排列是可能的。因此,新颖的架构旨在包含落入所附权利要求的精神和范围内的所有这样的改变、修改和变型。

[0135] 已经出于说明和描述的目的呈现了示例实施例的前述描述。其不旨在是穷举的或将本公开限制为所公开的精确形式。根据本公开,许多修改和变化是可能的。旨在本公开的范围不受此详细描述的限制,而是受所附权利要求的限制。要求本申请优先权的未来提交的申请可以以不同的方式要求所公开的主题,并且通常可以包括如本文中不同地公开或以其他方式证明的一个或多个限制的任何集合。

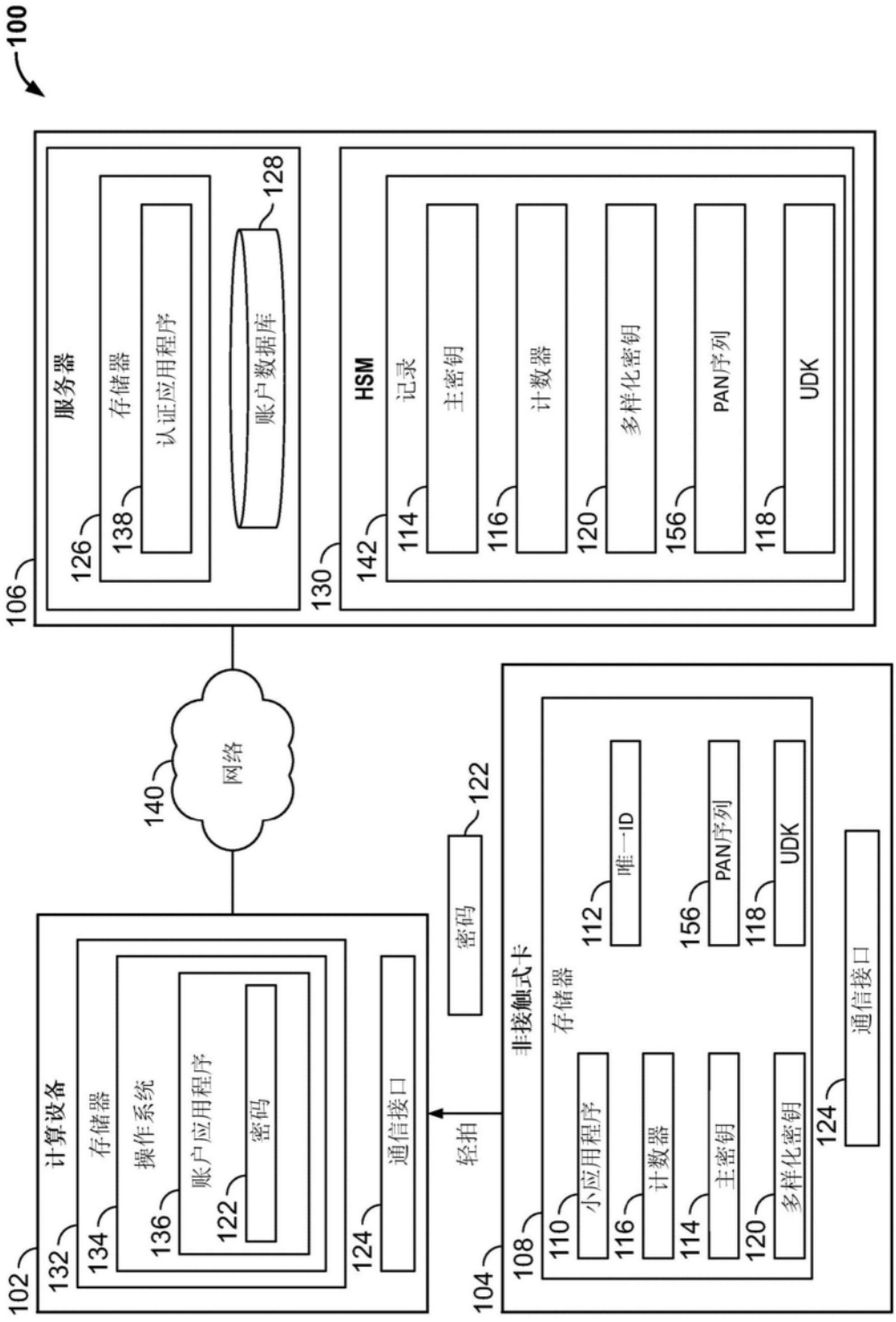

100
服务器
存储器
认证应用程序
账户数据库
126
138
128
106
HSM
记录
主密钥
计数器
多样化密钥
PAN序列
UDK
142
114
116
120
156
118
130
网络
140
密码
122
计算设备
存储器
操作系统
账户应用程序
密码
通信接口
132
134
136
122
124
102
轻拍
非接触式卡
存储器
小应用程序
计数器
主密钥
多样化密钥
唯一ID
PAN序列
UDK
通信接口
108
110
116
114
120
112
156
118
124
104

图1A

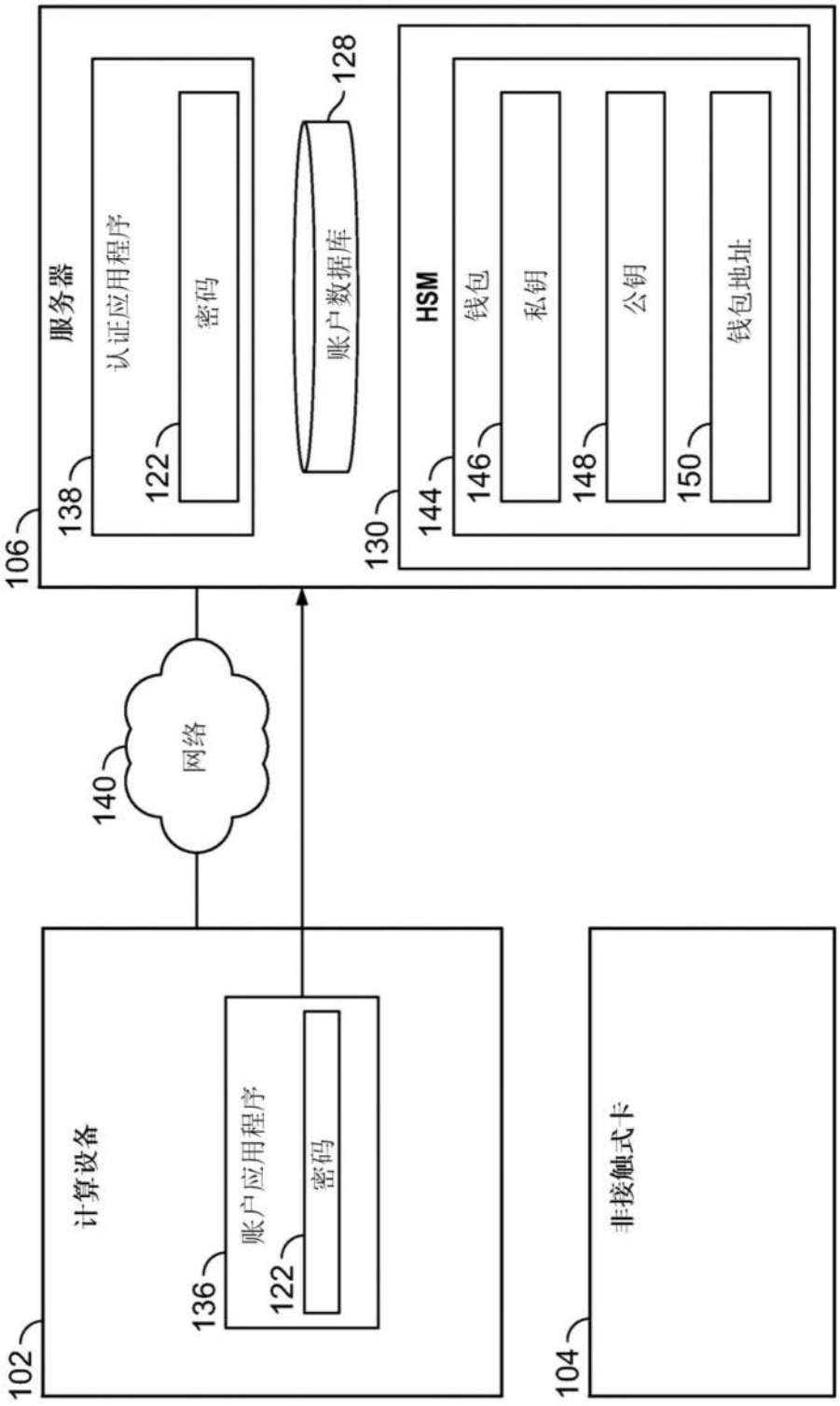

服务器
认证应用程序
密码
122
138
账户数据库
128
HSM
钱包
私钥
公钥
钱包地址
146
148
150
144
130
106
网络
140
计算设备
账户应用程序
密码
136
122
102
非接触式卡
104

图1B

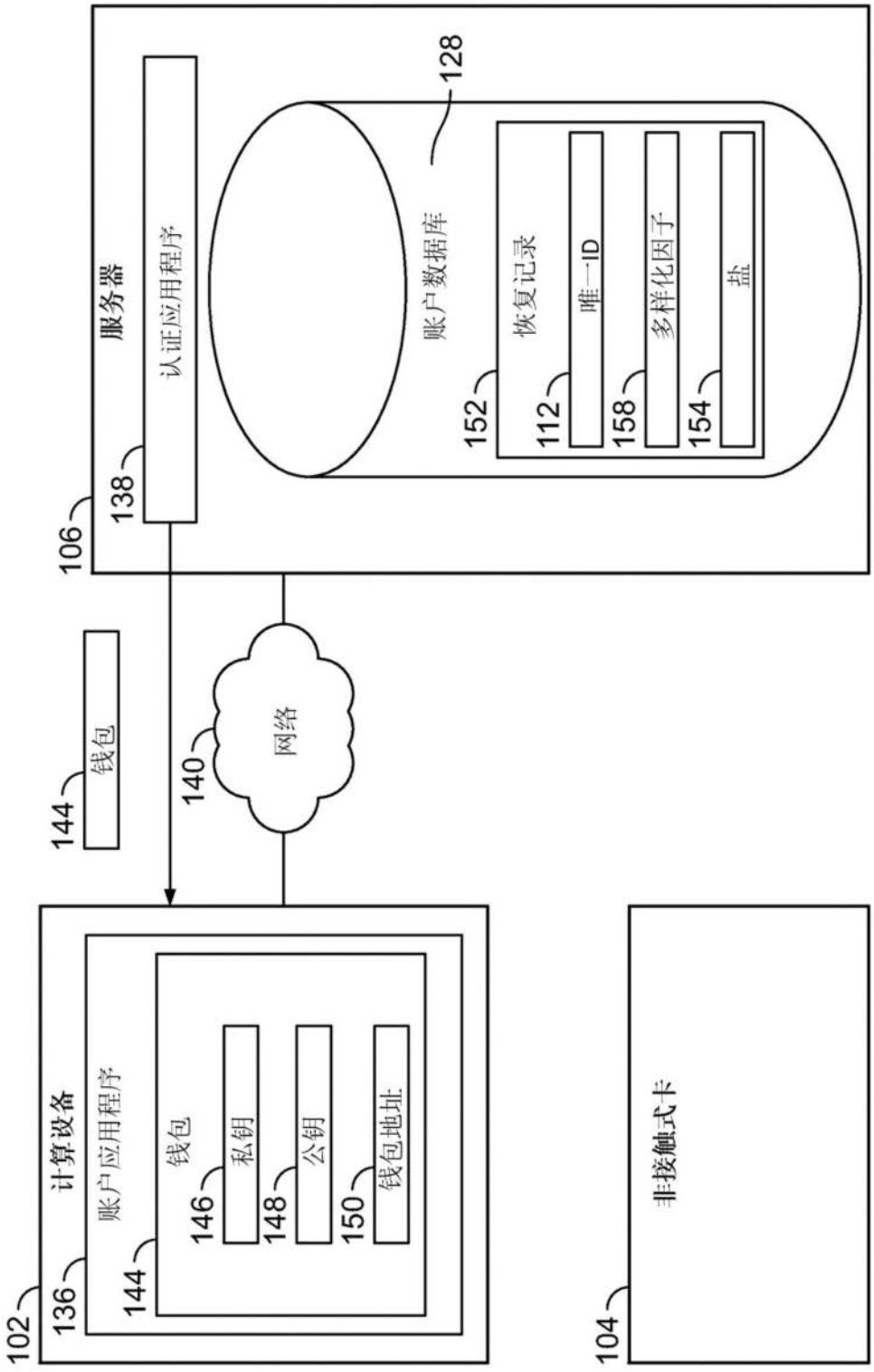

服务器
106
认证应用程序
138
128
账户数据库
恢复记录
152
唯一ID
112
多样化因子
158
盐
154
网络
140
钱包
144
计算设备
102
账户应用程序
136
钱包
144
私钥
146
公钥
148
钱包地址
150
非接触式卡
104

图1C

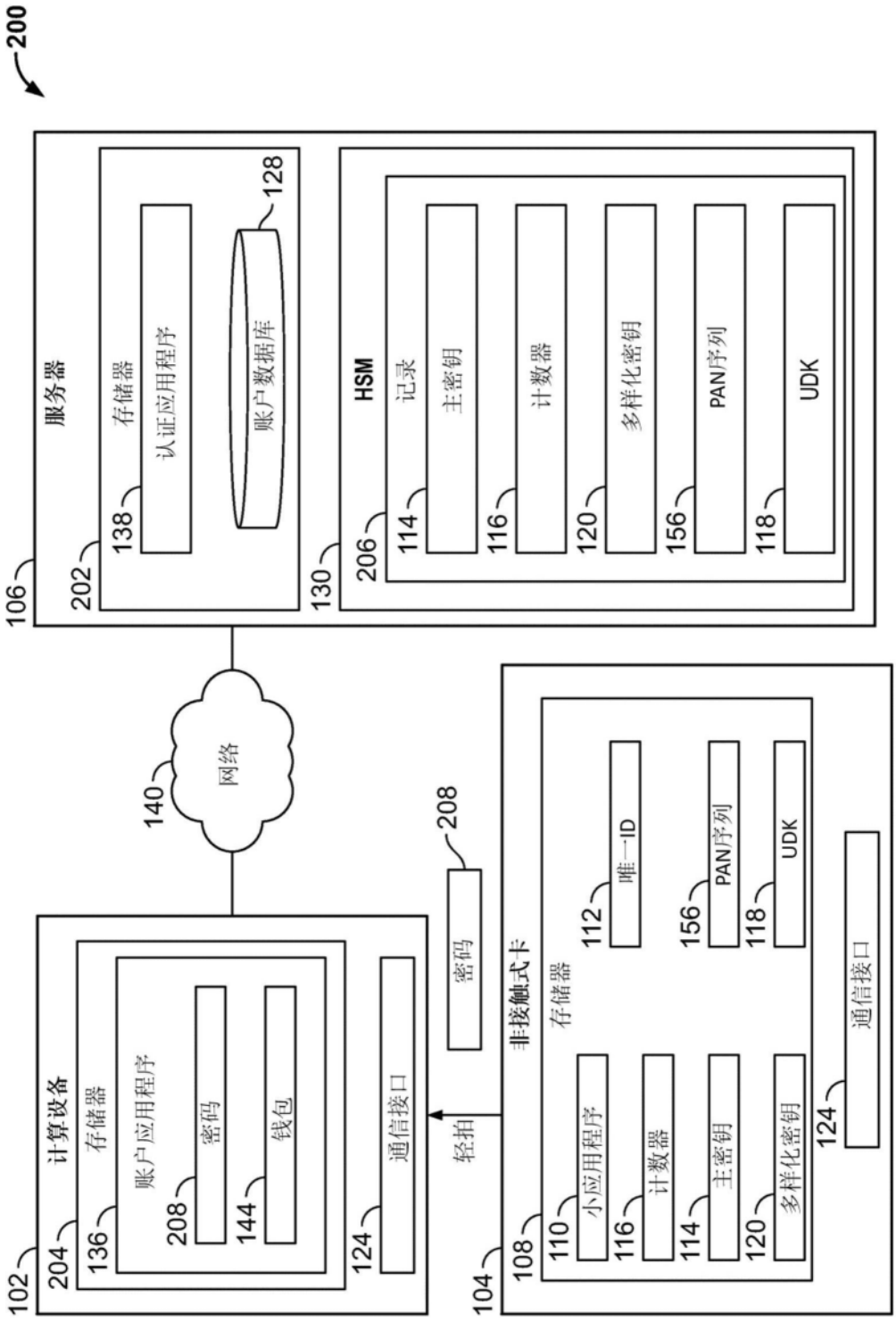

200
服务器
106
存储器
202
认证应用程序
138
账户数据库
128
HSM
130
记录
206
主密钥
114
计数器
116
多样化密钥
120
PAN序列
156
UDK
118
网络
140
计算设备
102
存储器
204
账户应用程序
136
密码
208
钱包
144
通信接口
124
轻拍
密码
208
非接触式卡
104
存储器
108
唯一ID
112
小应用程序
110
计数器
116
主密钥
114
多样化密钥
120
PAN序列
156
UDK
118
通信接口
124

图2A

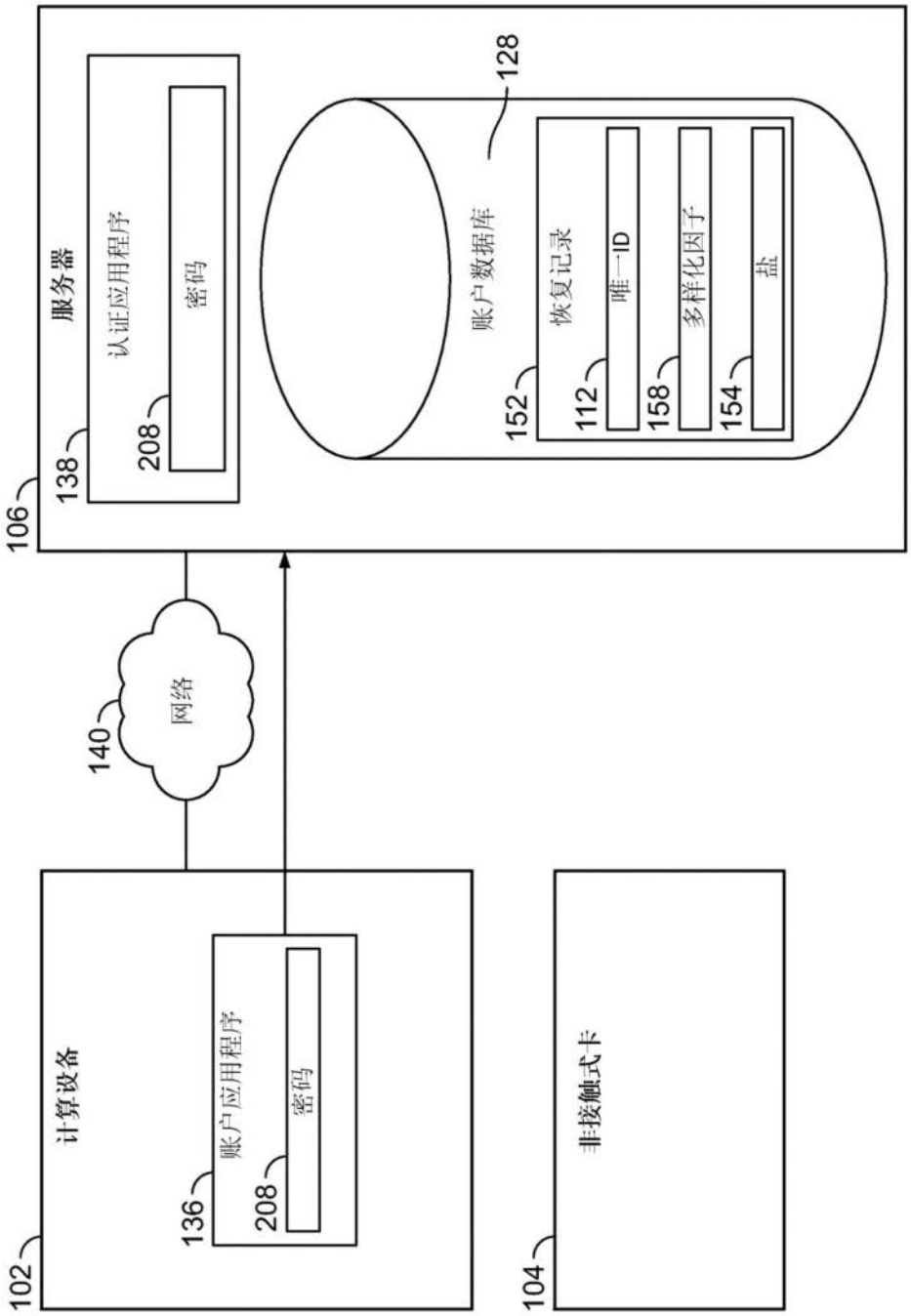

服务器
106
认证应用程序
138
密码
208
128
账户数据库
恢复记录
152
唯一ID
112
多样化因子
158
盐
154
网络
140
计算设备
102
账户应用程序
136
密码
208
非接触式卡
104

图2B

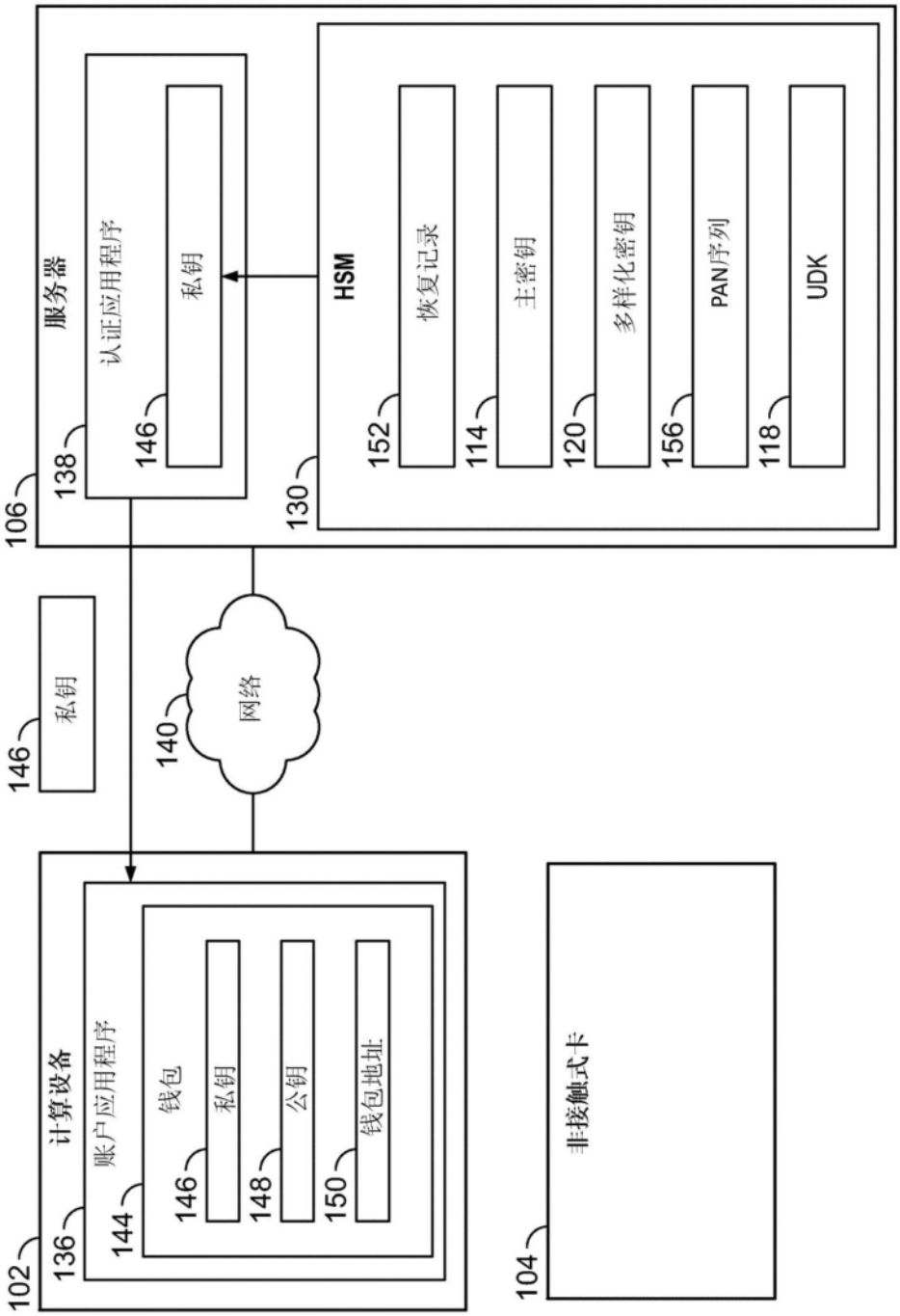

服务器
106
认证应用程序
138
私钥
146
HSM
130
恢复记录
152
主密钥
114
多样化密钥
120
PAN序列
156
UDK
118
私钥
146
网络
140
计算设备
102
账户应用程序
136
钱包
144
私钥
146
公钥
148
钱包地址
150
非接触式卡
104

图2C

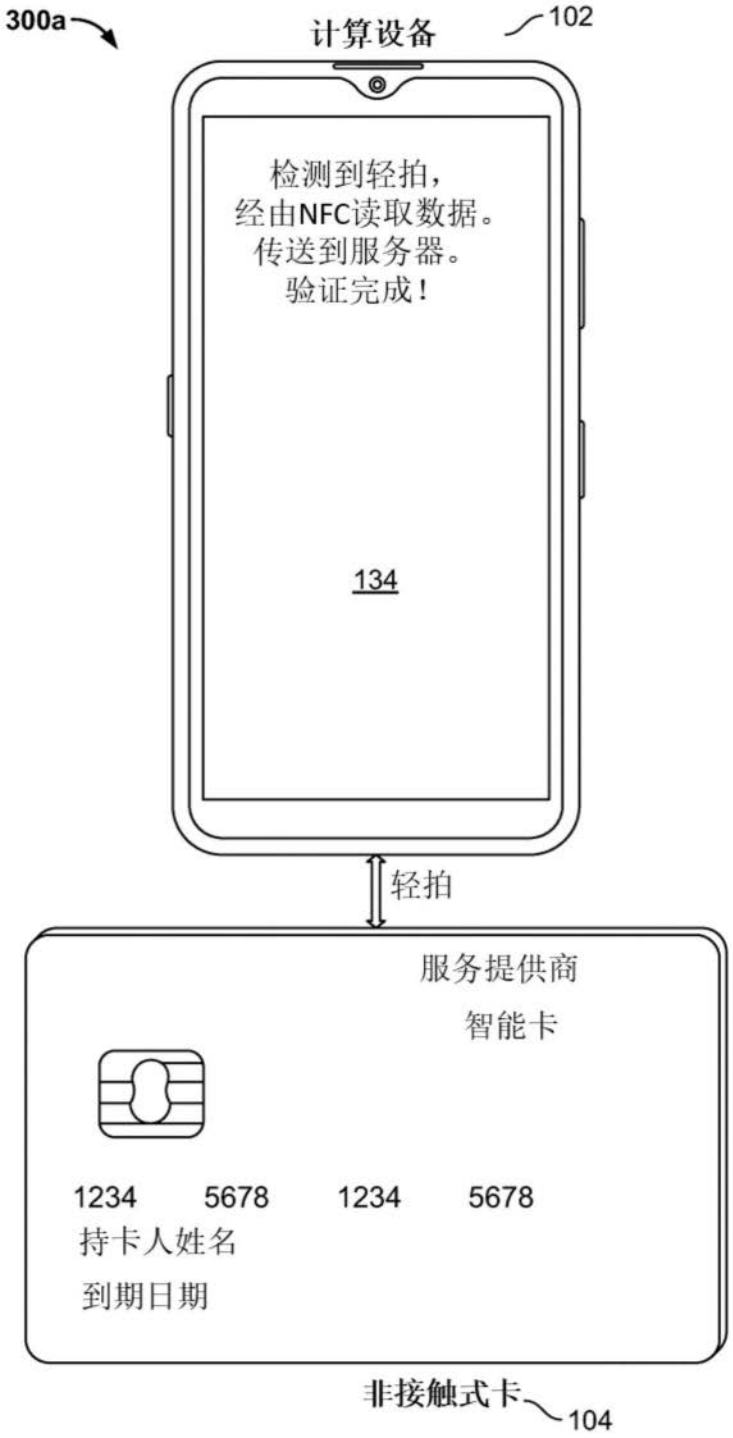

300a
计算设备
102
检测到轻拍，
经由NFC读取数据。
传送到服务器。
验证完成！
134
轻拍
服务提供商
智能卡
1234 5678 1234 5678
持卡人姓名
到期日期
非接触式卡
104

图3A

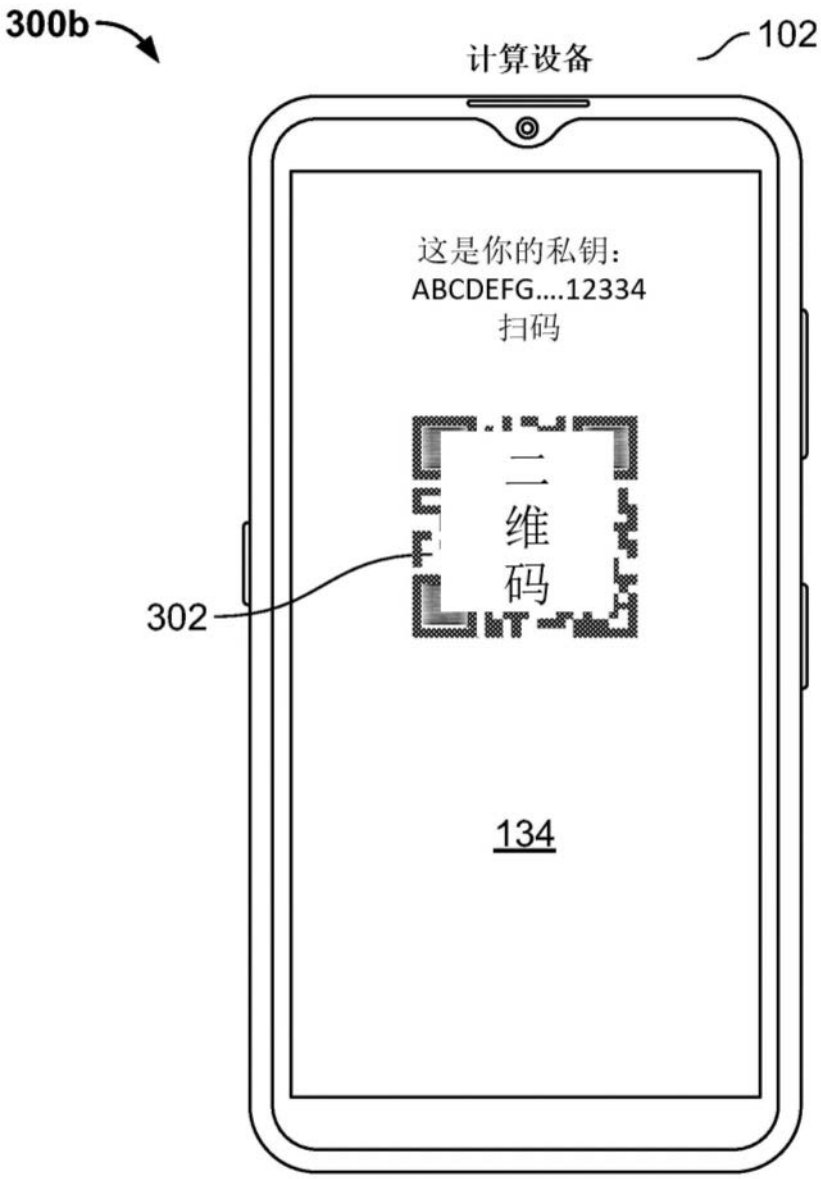


图3B

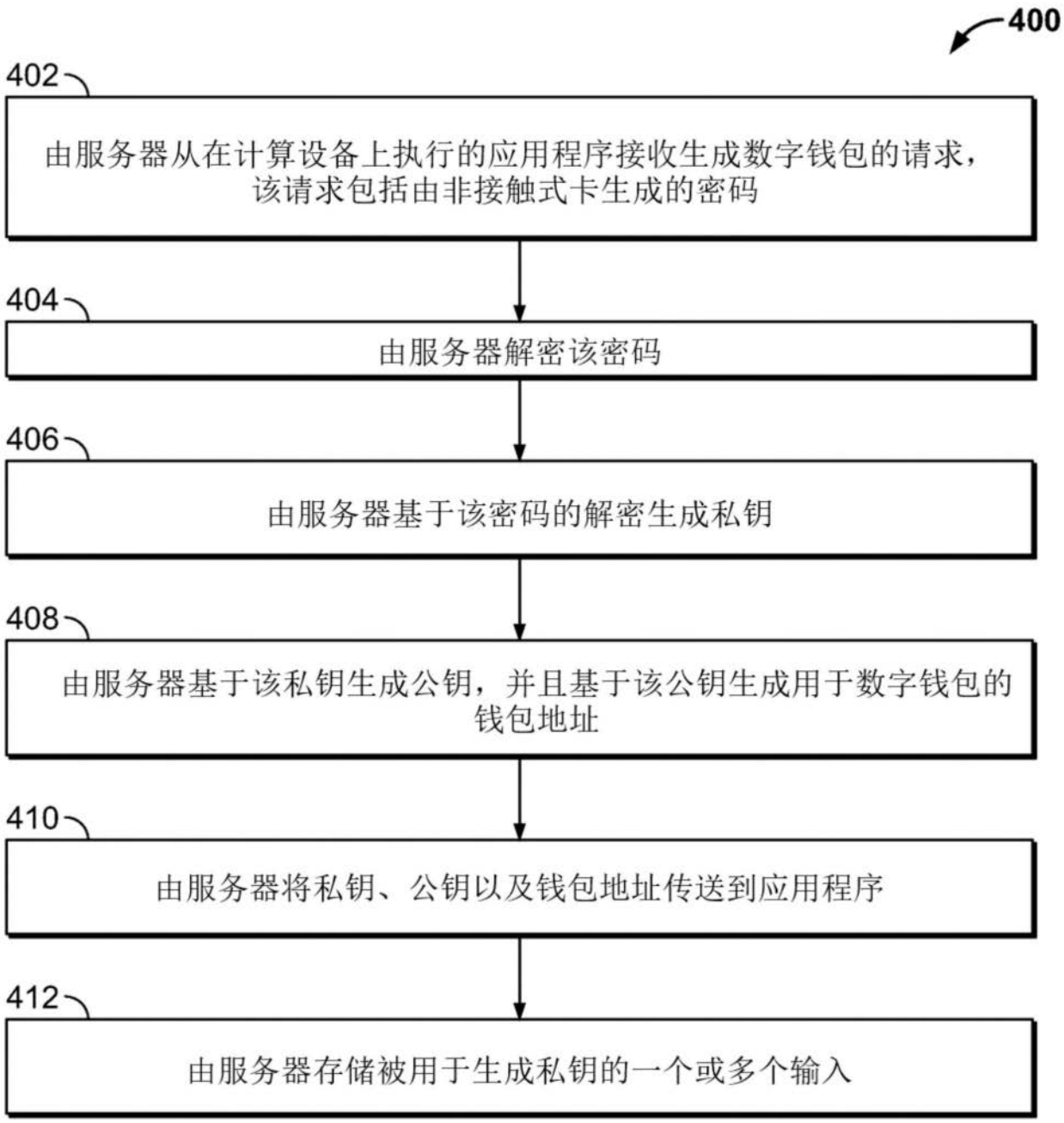

400
402
由服务器从在计算设备上执行的应用程序接收生成数字钱包的请求，该请求包括由非接触式卡生成的密码
404
由服务器解密该密码
406
由服务器基于该密码的解密生成私钥
408
由服务器基于该私钥生成公钥，并且基于该公钥生成用于数字钱包的钱包地址
410
由服务器将私钥、公钥以及钱包地址传送到应用程序
412
由服务器存储被用于生成私钥的一个或多个输入

图4

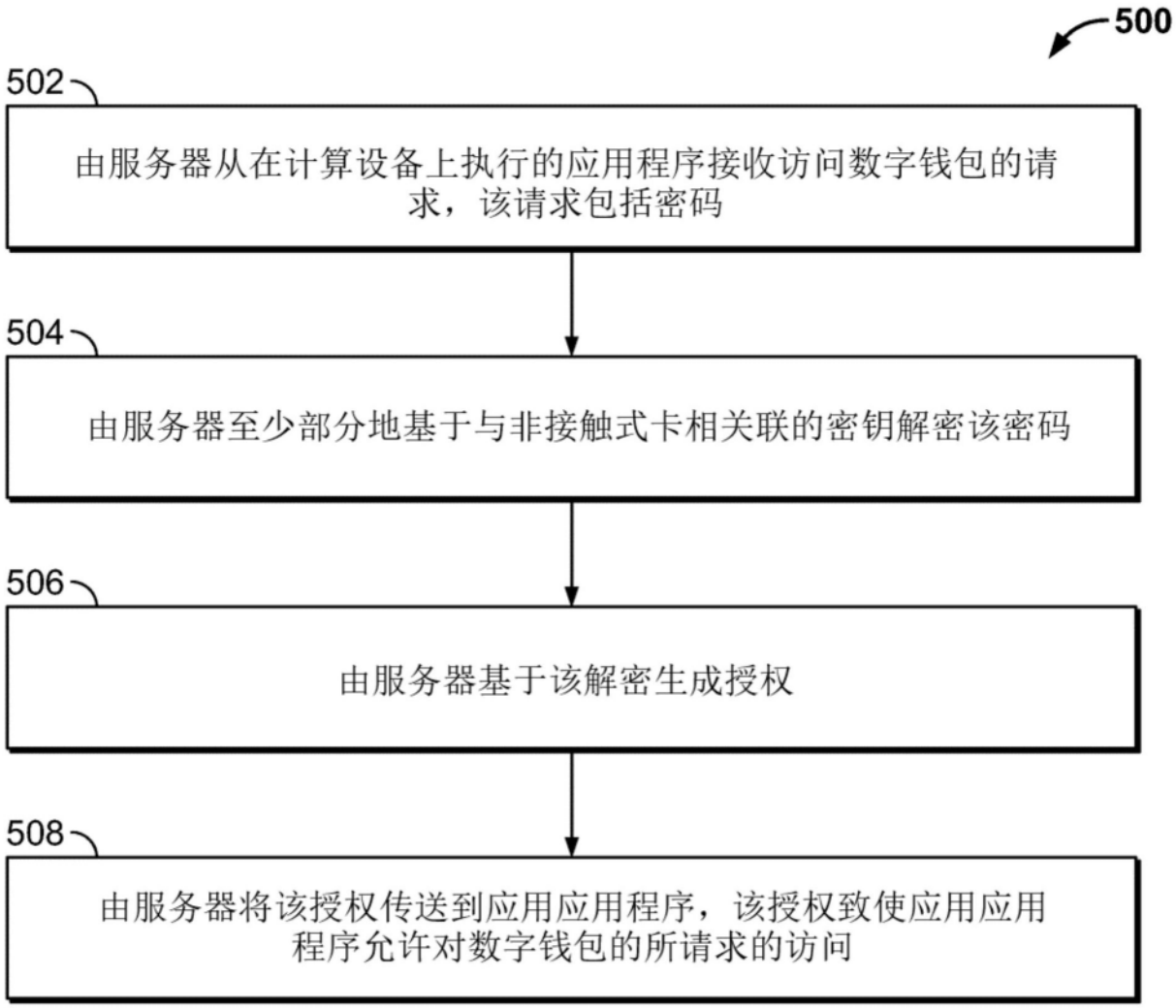

500
502
由服务器从在计算设备上执行的应用程序接收访问数字钱包的请求，该请求包括密码
504
由服务器至少部分地基于与非接触式卡相关联的密钥解密该密码
506
由服务器基于该解密生成授权
508
由服务器将该授权传送到应用应用程序，该授权致使应用应用程序允许对数字钱包的所请求的访问

图5

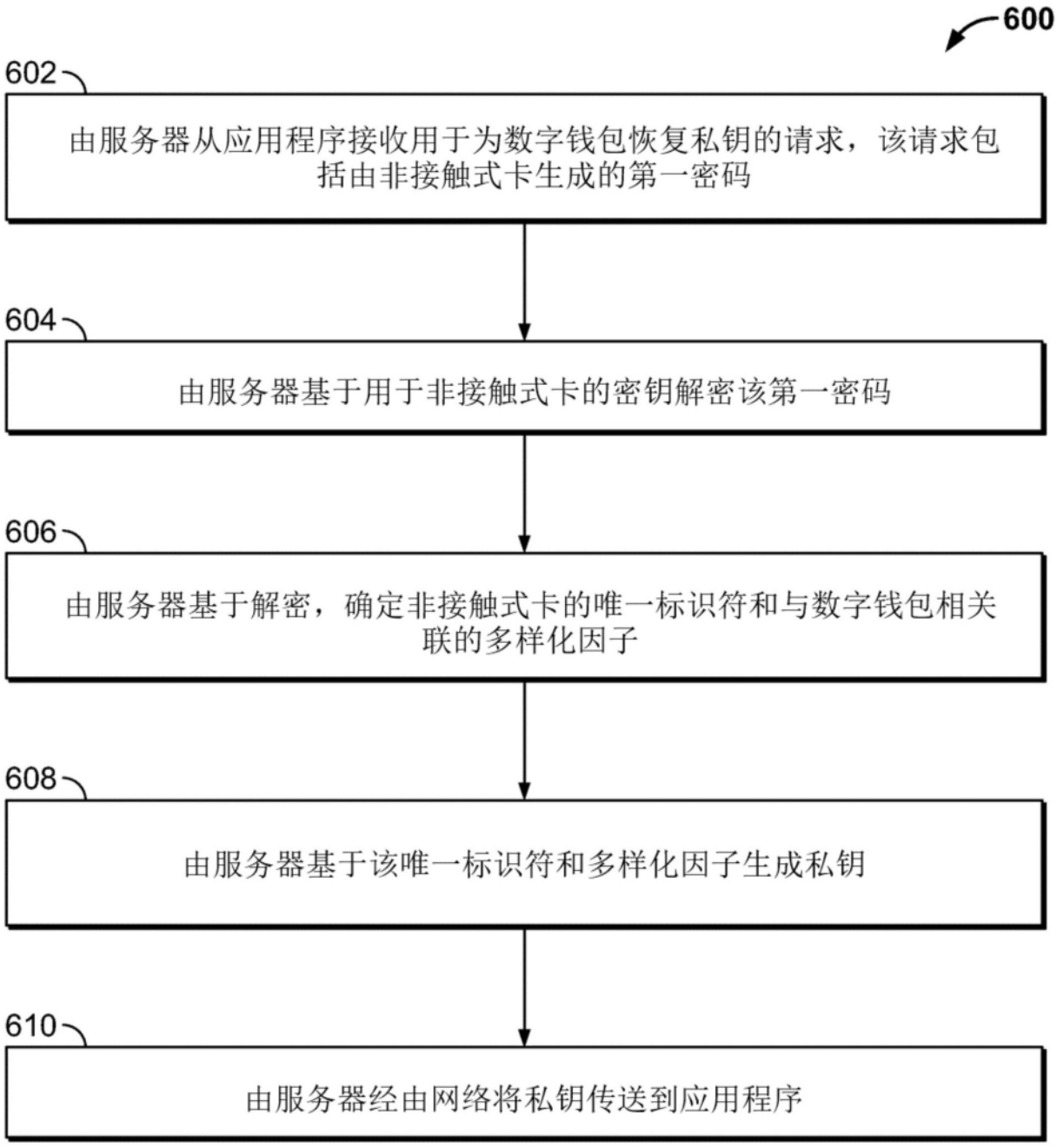

600
602
由服务器从应用程序接收用于为数字钱包恢复私钥的请求，该请求包括由非接触式卡生成的第一密码
604
由服务器基于用于非接触式卡的密钥解密该第一密码
606
由服务器基于解密，确定非接触式卡的唯一标识符和与数字钱包相关联的多样化因子
608
由服务器基于该唯一标识符和多样化因子生成私钥
610
由服务器经由网络将私钥传送到应用程序

图6

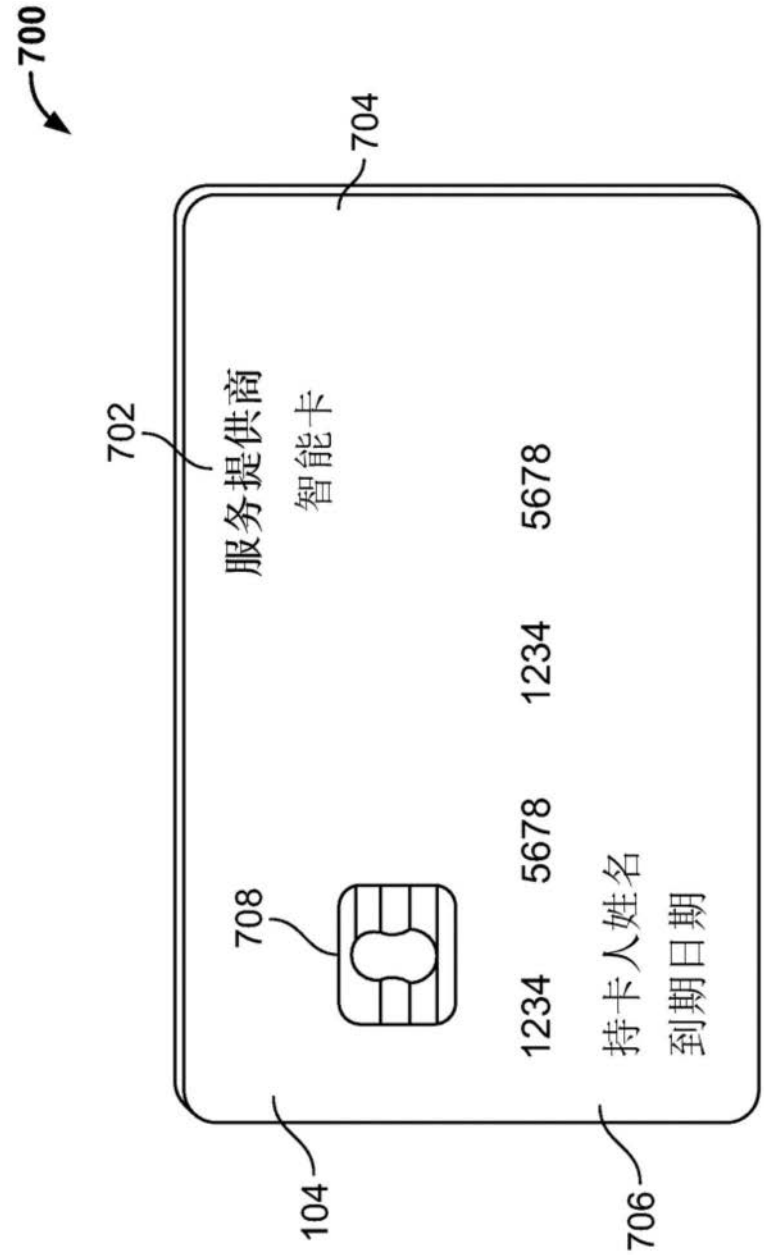

700
704
702
服务提供商
智能卡
5678
1234
5678
1234
708
持卡人姓名
到期日期
104
706

图7A

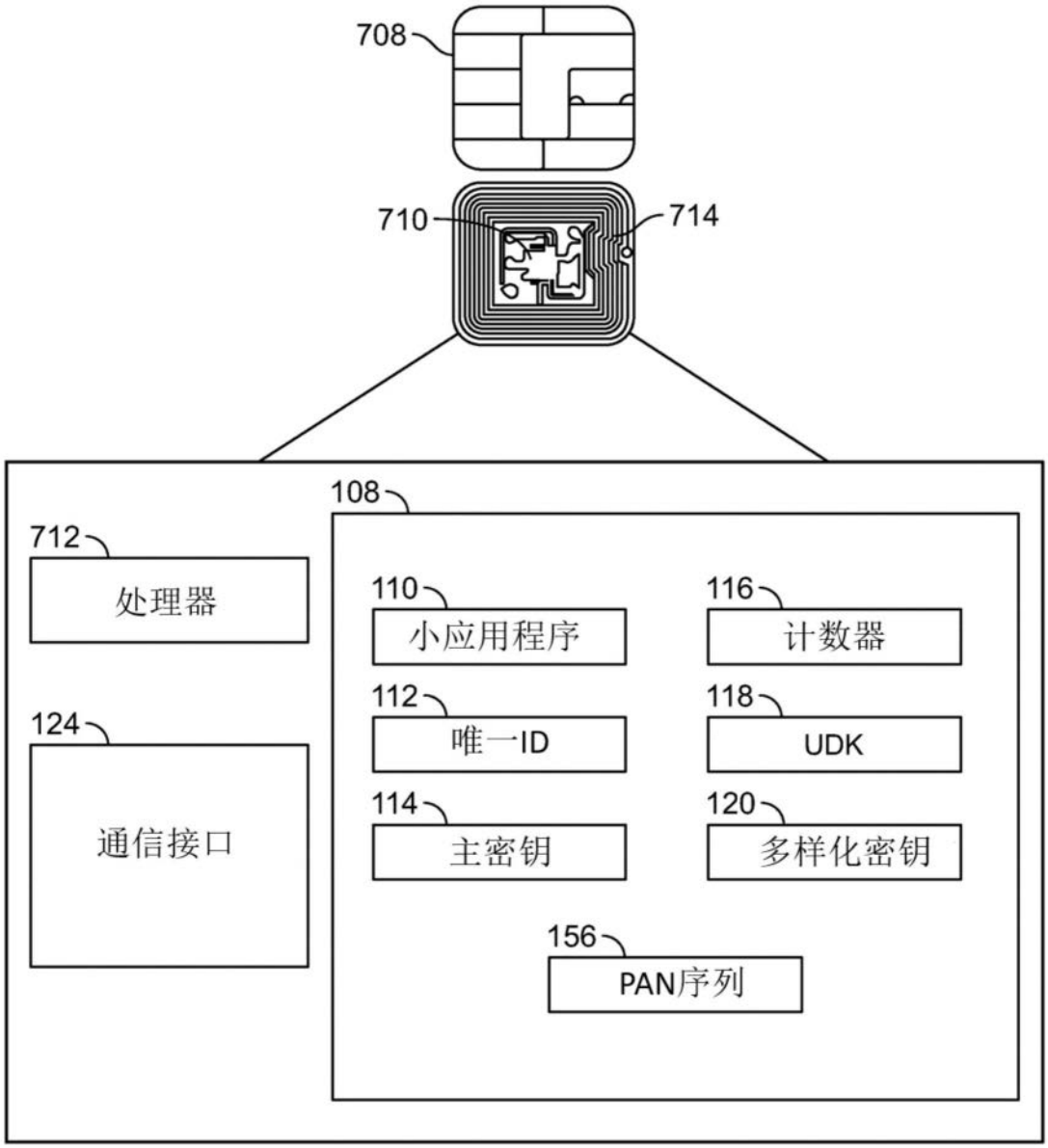

708
710
714
108
712
处理器
110
小应用程序
116
计数器
112
唯一ID
118
UDK
124
通信接口
114
主密钥
120
多样化密钥
156
PAN序列

图7B

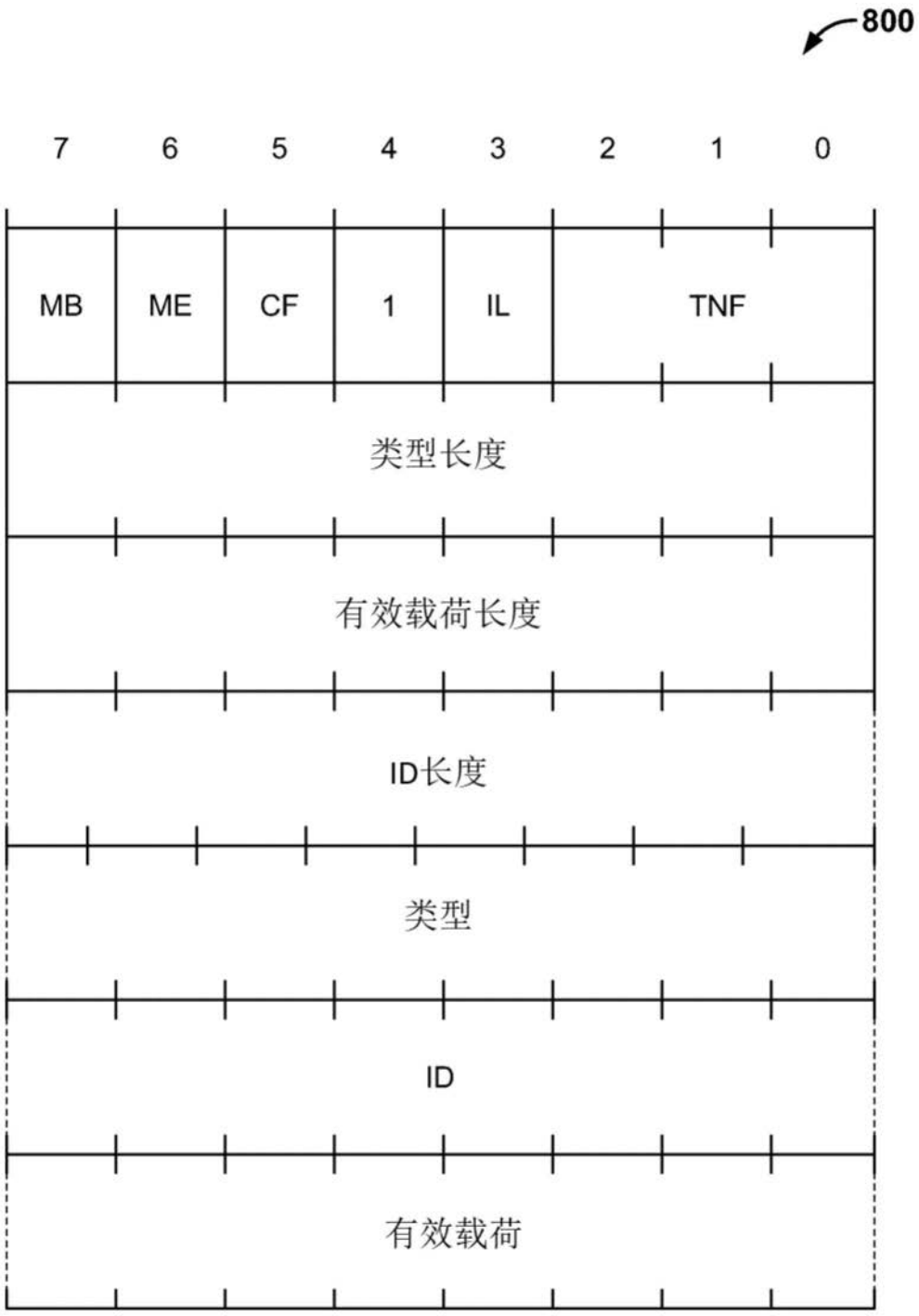


图8

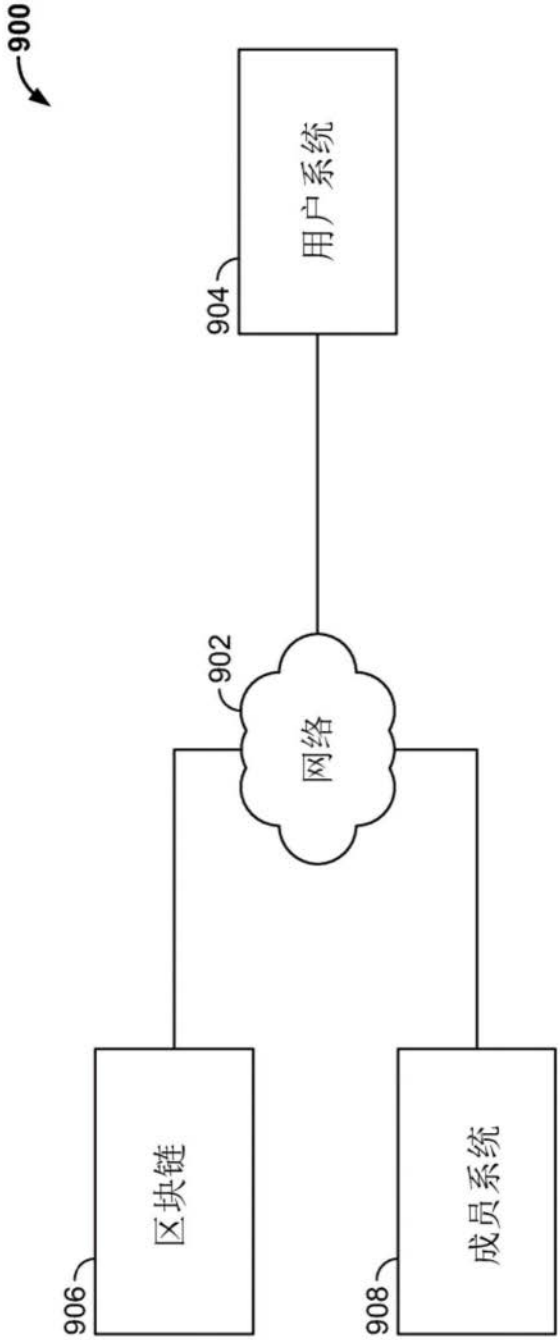


图9

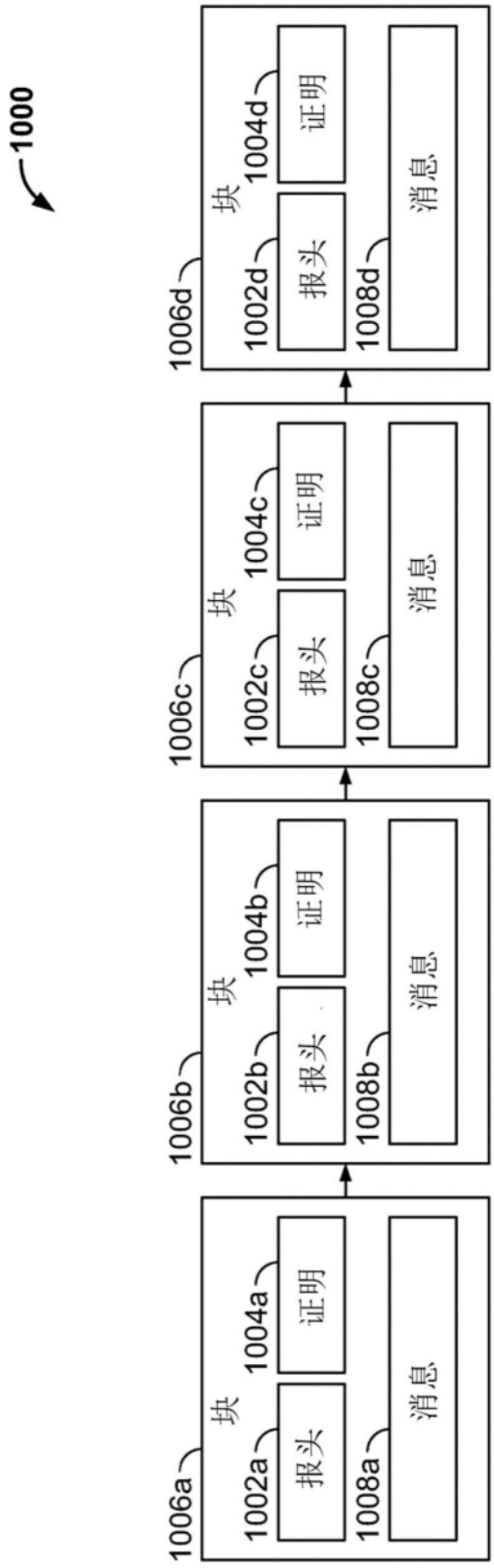

1000
1006a
块
1002a
报头
1004a
证明
1008a
消息
1006b
块
1002b
报头
1004b
证明
1008b
消息
1006c
块
1002c
报头
1004c
证明
1008c
消息
1006d
块
1002d
报头
1004d
证明
1008d
消息

图10

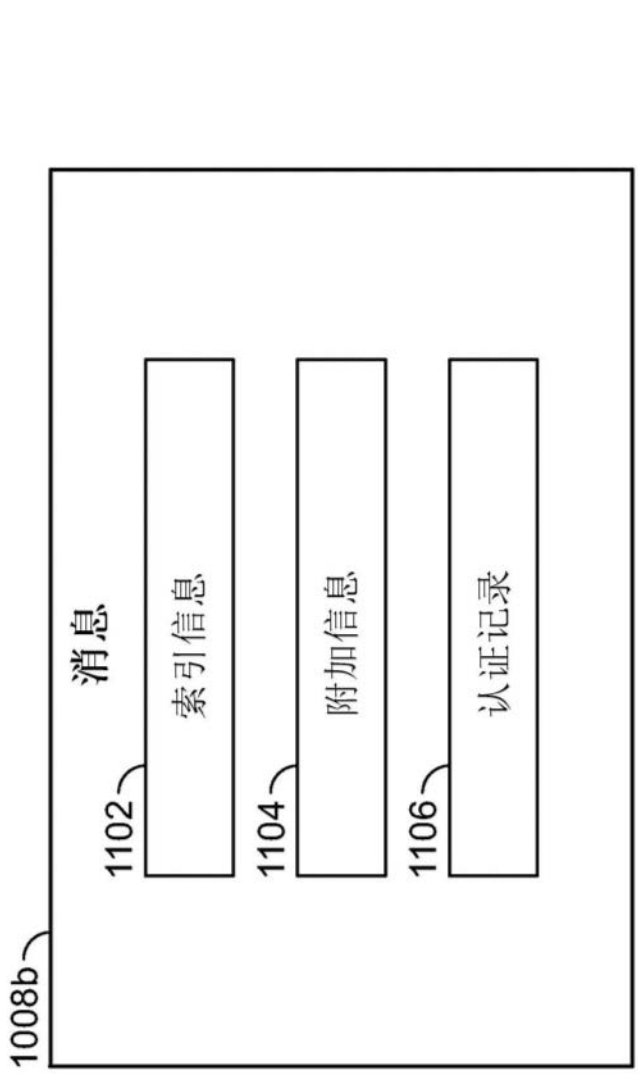


图11

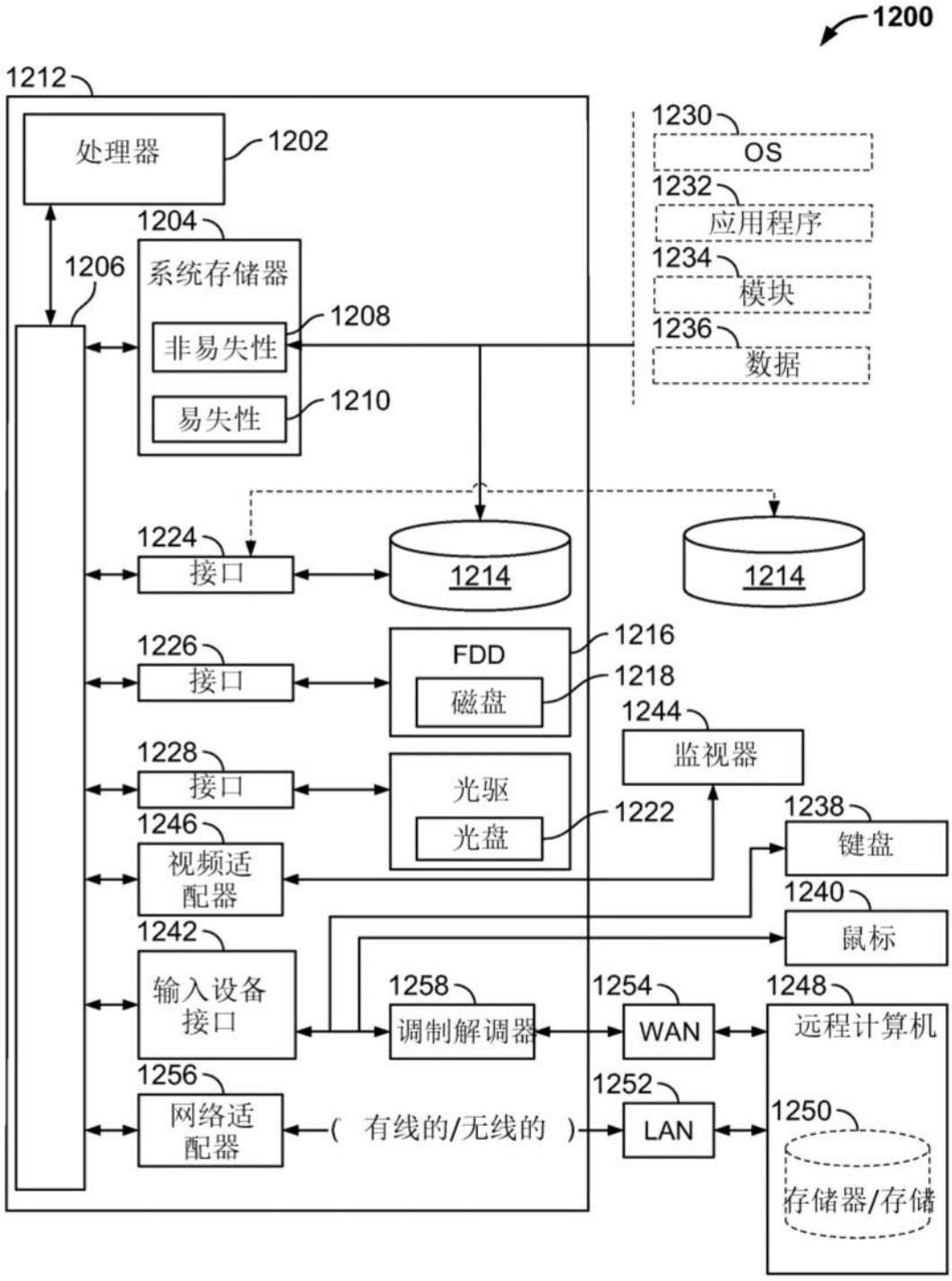

1200
1212
处理器
1202
1204
系统存储器
1206
1208
非易失性
1210
易失性
1230
OS
1232
应用程序
1234
模块
1236
数据
1224
接口
1214
1214
1226
接口
FDD
1216
磁盘
1218
1244
监视器
1228
接口
光驱
光盘
1222
1238
键盘
1246
视频适配器
1240
鼠标
1242
输入设备接口
1258
调制解调器
1254
WAN
1248
远程计算机
1256
网络适配器
(有线的/无线的)
1252
LAN
1250
存储器/存储

图12