(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112639855 A
(43)申请公布日 2021.04.09

(21)申请号 201980056736.1

(22)申请日 2019.09.30

(30)优先权数据
62/740,352 2018.10.02 US
16/205,119 2018.11.29 US
16/351,441 2019.03.12 US

(85)PCT国际申请进入国家阶段日
2021.02.26

(86)PCT国际申请的申请数据
PCT/US2019/053849 2019.09.30

(87)PCT国际申请的公布数据
WO2020/072373 EN 2020.04.09

(71)申请人 第一资本服务有限责任公司
地址 美国弗吉尼亚州

(72)发明人 凯特琳·纽曼 科林·哈特
杰弗里·鲁尔 劳拉·莫斯勒
索菲·贝穆德兹 迈克尔·莫索巴
韦恩·卢茨
查尔斯·纳森·克兰克
梅丽莎·亨 凯文·奥斯本
金柏莉·海恩斯
安德鲁·科格斯韦尔
拉媞卡·古拉蒂
莎拉·简·坎宁安
詹姆斯·阿什菲尔德

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

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

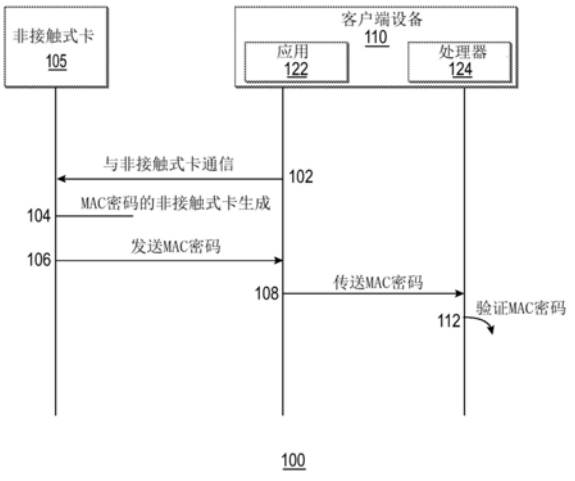
权利要求书2页 说明书32页 附图14页

(54)发明名称

用于非接触式卡的密码认证的系统和方法

(57)摘要

提供了用于在发送设备和接收设备之间进行安全通信的系统和方法的示例实施例。在一个实施例中,一种方法可以包括:启动操作,暂停操作直到认证了用户标识为止,在发送设备进入接收设备的通信领域中并且将加密的标识数据从发送设备传输到接收设备应用之后认证用户标识,以及完成操作。



CN 112639855 A

1.一种用于安全通信的系统,包括:

发送设备,所述发送设备具有处理器和存储器,所述发送设备的存储器包含多样化的主密钥、发送数据和计数器值;

应用,所述应用包括用于在具有处理器和存储器的接收设备上执行的指令,所述接收设备的存储器包含主密钥;

其中,所述发送设备被配置为:

使用所述多样化的主密钥、一个或多个密码算法以及所述计数器值来生成多样化的密钥,

使用所述一个或多个密码算法和所述多样化的密钥生成包含所述计数器值的密码结果,

使用所述一个或多个密码算法和所述多样化的密钥对所述发送数据进行加密,以产生经加密的发送数据,并且

将所述密码结果和所述经加密的发送数据发送给所述应用;

其中,所述应用被配置为:

基于所述主密钥和唯一的标识符,生成认证多样化的密钥;

基于所述认证多样化的密钥和所述密码结果生成会话密钥;并且

使用所述一个或多个密码算法和所述会话密钥来解密所述经加密的发送数据并验证接收到的密码结果;

其中,在启动操作时,所述应用还被配置为:

请求用户标识;

暂停所述操作,直到认证了所述用户标识为止;并且

一旦认证了所述用户标识,就完成了所述操作,

其中所述用户标识是在所述发送设备进入到所述接收设备的通信领域之后提供的。

2.根据权利要求1所述的用于安全通信的系统,其中,所述应用被配置为与一个或多个服务器进行通信来认证所述用户标识。

3.根据权利要求1所述的用于安全通信的系统,其中,所述用户标识由所述发送设备提供。

4.根据权利要求1所述的用于安全通信的系统,其中:

所述接收设备是服务器;并且

所述密码结果和所述经加密的发送数据由所述发送设备经由一个或多个中间设备发送给所述应用。

5.一种使操作安全的方法,所述方法包括以下步骤:

提供包括处理器和存储器的发送设备,并且所述发送设备的存储器包含多样化的主密钥、标识数据和计数器值;

提供包括用于在具有处理器和存储器的接收设备上执行的指令的应用,所述接收设备的存储器包含主密钥;

其中,所述发送设备被配置为:

使用所述多样化的主密钥、一个或多个密码算法以及计数器来生成多样化的密钥,

使用所述一个或多个密码算法和所述多样化的密钥生成包含所述计数器值的密码结

果，

使用所述一个或多个密码算法和所述多样化的密钥对所述标识数据进行加密，以产生经加密的标识数据，并且

将所述密码结果和经加密的标识数据发送给所述应用；

其中，所述应用被配置为：

基于所述主密钥和唯一的标识符，生成认证多样化的密钥；

基于所述认证多样化的密钥和所述密码结果生成会话密钥；并且

使用所述一个或多个密码算法和所述会话密钥来解密所述经加密的标识数据并验证接收到的密码结果；

启动操作；

暂停所述操作，直到认证了用户标识为止；

在所述发送设备进入到所述接收设备的通信领域之后认证所述用户标识，从而将经加密的标识数据从所述发送设备发送给所述应用，其中所述用户标识是在所述发送设备进入到所述通信领域之后提供的；并且

完成所述操作。

6.根据权利要求5所述的方法，其中，所述操作包括金融交易。

7.根据权利要求6所述的方法，其中，暂停所述操作的步骤发生在发送与所述金融交易相关联的金融数据之前。

8.根据权利要求6所述的方法，其中，所述金融交易包括从账户提取资金。

9.根据权利要求5所述的方法，其中，所述操作包括访问物理空间。

10.根据权利要求5所述的方法，其中，所述操作包括登记入住旅馆。

11.根据权利要求5所述的方法，其中，所述操作包括自动填充在线表格。

12.根据权利要求5所述的方法，其中，所述操作包括解锁车辆。

13.根据权利要求5所述的方法，其中，所述操作包括操作车辆。

14.根据权利要求5所述的方法，其中，所述操作包括访问医疗记录。

15.根据权利要求5所述的方法，其中，所述操作包括访问个人信息。

16.根据权利要求5所述的方法，其中，所述操作包括呼叫客户服务代理。

17.根据权利要求5所述的方法，其中，所述操作包括改变旅馆预订。

18.根据权利要求5所述的方法，其中，所述操作包括编辑密码。

19.根据权利要求5所述的方法，其中，所述操作包括编辑邮寄地址。

20.根据权利要求5所述的方法，还包括将密码发送到移动设备并在完成所述操作之前请求所述密码的步骤。

用于非接触式卡的密码认证的系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求于2019年3月12日提交的美国专利申请16/351,441的优先权,其是2018年11月29日提交的美国专利申请16/205,119的部分继续并要求其优先权,并且本申请要求来自2018年10月2日提交的美国临时专利申请No.62/740,352的优先权,其全部公开内容通过引用合并于此。

技术领域

[0003] 本公开涉及密码术,更具体地,涉及用于非接触式卡的密码认证的系统和方法。

背景技术

[0004] 数据安全性和交易完整性对企业和消费者至关重要。随着电子交易在商业活动中所占份额越来越大,这种需求持续增长。

[0005] 电子邮件可以用作验证交易的工具,但是电子邮件容易受到攻击,并且容易受到黑客攻击或其他未经授权的访问。也可以使用短消息服务(SMS)消息,但这也容易受到损害。而且,甚至数据加密算法(例如三重DES算法)也具有类似的漏洞。

[0006] 激活许多卡,包括例如金融卡(例如信用卡和其他支付卡)涉及持卡人拨打电话号码或访问网站并输入或以其他方式提供卡信息的耗时过程。此外,尽管基于芯片的金融卡的日渐增多的使用针对个人购买提供了比以前技术(例如,磁条卡)更安全的功能,但是帐户访问仍然可能依赖于登录凭据(例如,用户名和密码)以确认持卡人的身份。但是,如果登录凭据被泄露,则其他人可以访问该用户的帐户。

[0007] 存在这些和其他缺陷。因此,需要为用户提供克服这些缺陷的适当解决方案,以提供用于非接触式卡的数据安全性、认证和验证。此外,需要一种改进的激活卡的方法、以及一种改进的用于帐户访问的认证。

发明内容

[0008] 所公开的技术的方面包括用于非接触式卡的密码认证的系统和方法。各种实施例描述了用于实现和管理非接触式卡的密码认证的系统和方法。

[0009] 本公开的实施例提供了一种用于安全通信的系统,包括:具有处理器和存储器的发送设备,该发送设备的存储器包含多样化(diversified)的主密钥、发送数据和计数器值;包括用于在具有处理器和存储器的接收设备上执行的指令的应用,该接收设备的存储器包含主密钥;其中,所述发送设备被配置为:使用多样化的主密钥、一个或多个密码算法以及计数器值来生成多样化的密钥,使用一个或多个密码算法和多样化的密钥生成包含计数器值的密码结果,使用一个或多个密码算法和多样化的密钥对发送数据进行加密,以产生经加密的发送数据,以及将密码结果和经加密的发送数据发送给应用;其中,该应用被配置为:基于主密钥和唯一的标识符,生成认证多样化的密钥;基于认证多样化的密钥和密码结果生成会话密钥;并且使用一个或多个密码算法和会话密钥来解密经加密的发送数据并

验证接收到的密码结果;其中,在启动操作时,该应用还被配置为:请求用户标识;暂停操作,直到认证了用户标识为止;并且一旦认证了用户标识,就完成了操作,其中用户标识是在发送设备进入到接收设备的通信领域之后提供的。

[0010] 本公开的实施例提供了一种使操作安全的方法,该方法包括以下步骤:提供包括处理器和存储器的发送设备,并且该发送设备的存储器包含多样化的主密钥、标识数据和计数器值;提供包括用于在具有处理器和包含主密钥的存储器的接收设备上执行的指令的应用;其中,所述发送设备被配置为:使用多样化的主密钥、一个或多个密码算法以及计数器来生成多样化的密钥,使用一个或多个密码算法和多样化的密钥生成包含计数器值的密码结果,使用一个或多个密码算法和多样化的密钥对标识数据进行加密,以产生经加密的标识数据,以及将密码结果和经加密的标识数据发送给应用;其中,该应用被配置为:基于主密钥和唯一的标识符,生成认证多样化的密钥;基于认证多样化的密钥和密码结果生成会话密钥;并且使用一个或多个密码算法和会话密钥来解密经加密的标识数据并验证接收到的密码结果;启动操作;暂停操作,直到认证了用户标识为止;在发送设备进入接收设备的通信领域之后认证用户标识,从而将经加密的标识数据从发送设备发送给应用,其中用户标识是在发送设备进入通信领域之后提供的;以及完成操作。

[0011] 在下文中参考附图中示出的具体示例实施例来更详细地解释所公开的设计的其他特征以及由此提供的优点,其中,相似的元件由相似的参考标记表示。

附图说明

[0012] 图1A是根据示例实施例的数据传输系统的图。

[0013] 图1B是示出根据示例实施例的用于提供认证访问的序列的图。

[0014] 图2是根据示例实施例的数据传输系统的图。

[0015] 图3是根据示例实施例的使用非接触式卡的系统的图。

[0016] 图4是示出根据示例实施例的密钥多样化的方法的流程图。

[0017] 图5A是根据示例实施例的非接触式卡的示图。

[0018] 图5B是根据示例实施例的非接触式卡的接触片(contact pad)的示图。

[0019] 图6是描绘根据示例实施例的与设备进行通信的消息的示图。

[0020] 图7是描绘根据示例实施例的消息和消息格式的示图。

[0021] 图8是示出根据示例实施例的键操作的流程图。

[0022] 图9是根据示例实施例的密钥系统的图。

[0023] 图10是根据示例实施例的生成密码的方法的流程图。

[0024] 图11是示出根据示例实施例的密钥多样化的过程的流程图。

[0025] 图12是示出根据示例实施例的用于卡激活的方法的流程图。

[0026] 图13是示出根据示例实施例的使用非接触式卡访问受限特征和信息的方法的流程图。

[0027] 图14是示出根据示例实施例的使用非接触式卡联系客户支持的方法的流程图。

具体实施方式

[0028] 实施例的以下描述提供了参考数字的非限制性代表示例,以特别地描述本发明的

不同方面的特征和教导。从实施例的描述中，应当认识到，所描述的实施例能够与其他实施例分开地或组合地实现。回顾实施例的描述的本领域普通技术人员应该能够学习和理解本发明的不同描述的方面。实施例的描述应在某种程度上促进对本发明的理解，使得未具体覆盖但是在阅读了实施例的描述的本领域技术人员的知识范围内的其他实现将被理解为与本发明的应用一致。

[0029] 本公开的一些实施例的目的是将一个或多个密钥构建到一个或多个非接触式卡中。在这些实施例中，非接触式卡可以执行认证和许多其他功能，否则，除了非接触式卡之外，用户可能还需要用户携带单独的物理令牌。通过采用非接触式界面，可以为非接触式卡提供一种在用户的设备(例如移动电话)与卡本身之间进行交互和通信的方法。例如，作为许多信用卡交易基础的EMV协议包括以下认证过程，该过程满足了Android®操作系统的要求，但给iOS®带来了挑战——它对近场通信(NFC)的使用更为严格，因为仅能以只读方式使用。本文描述的非接触式卡的示例性实施例利用了NFC技术。

[0030] 图1A示出了根据示例实施例的数据传输系统。如下面进一步讨论的，系统100可以包括非接触式卡105，客户端设备110，网络115和服务器120。尽管图1A示出了组件的单个实例，但是系统100可以包括任何数量的组件。

[0031] 系统100可以包括一个或多个非接触式卡105，下面将参照图5A-5B进一步说明。在一些实施例中，非接触式卡105可以在示例中利用NFC与客户端设备110进行无线通信。

[0032] 系统100可以包括客户端设备110，其可以是启用网络的计算机(network-enabled cmputer)。如本文所指，启用网络的计算机可以包括但不限于计算机设备或通信设备，其包括例如服务器、网络应用设备、个人计算机、工作站、电话、手持式PC、个人数字助理、瘦客户端、胖客户端、Internet浏览器或其他设备。客户端设备110也可以是移动设备。例如，移动设备可以包括来自Apple®的iPhone、iPod、iPad或运行Apple的iOS®操作系统的任何其他移动设备，运行Microsoft的Windows®Mobile操作系统的任何设备，运行Google的Android®操作系统的任何设备，和/或任何其他智能手机、平板电脑或类似的可穿戴移动设备。

[0033] 客户端设备110设备可以包括处理器和存储器，并且应当理解，处理电路可以包含附加组件，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，安全性原语和防篡改硬件，如执行本文所述功能所需的。客户端设备110还可以包括显示器和输入设备。显示器可以是用于呈现视觉信息的任何类型的设备，例如计算机监视器、平板显示器和移动设备屏幕，包括：液晶显示器、发光二极管显示器、等离子面板和阴极射线管显示器。输入设备可以包括用于将信息输入到用户设备中以由用户设备可用和支持的任何设备，例如触摸屏、键盘、鼠标、光标控制设备、触摸屏、麦克风、数码相机、视频录像机或便携式摄像机。这些设备可用于输入信息并与此处描述的软件和其他设备进行交互。

[0034] 在一些示例中，系统100的客户端设备110可以执行一个或多个应用，例如软件应用，其使得例如能够与系统100的一个或多个组件进行网络通信并且发送和/或接收数据。

[0035] 客户端设备110可以经由一个或多个网络115与一个或多个服务器120通信，并且可以作为与服务器120进行的相应前端对后端配对来操作。客户端设备110可以例如从在客

户端设备110上执行的移动设备应用而向服务器120发送一个或多个请求。一个或多个请求可以与从服务器120检索数据相关联。服务器120可以从客户端设备110接收一个或多个请求。基于来自客户端设备110的一个或多个请求，服务器120可以被配置为从一个或多个数据库(未示出)检索所请求的数据。基于从一个或多个数据库接收到所请求的数据，服务器120可以被配置为将所接收的数据发送到客户端设备110，其中所接收的数据响应于一个或多个请求。

[0036] 系统100可以包括一个或多个网络115。在一些示例中，网络115可以是无线网络、有线网络、或无线网络和有线网络任意组合中的一个或多个，并且可以被配置为将客户端设备110连接到服务器120。例如，网络115可以包括以下一个或多个：光纤网络、无源光网络、电缆网络、因特网网络、卫星网络、无线局域网(LAN)、全球移动通信系统、个人通信服务、个人局域网、无线应用协议、多媒体消息服务、增强消息服务、短消息服务、基于时分多路复用的系统、基于码分多址的系统、D-AMPS、Wi-Fi、固定无线数据、IEEE 802.11b，802.15.1、802.11n和802.11g、蓝牙、NFC、射频识别(RFID)、Wi-Fi等。

[0037] 另外，网络115可以包括但不限于：电话线、光纤、IEEE以太网902.3、广域网、无线个人局域网、LAN或诸如因特网的全球网络。另外，网络115可以支持因特网网络，无线通信网络，蜂窝网络等或其任何组合。网络115可以进一步包括一个网络，或者上述任何数量的示例性类型的网络，其作为独立网络运行或彼此协作。网络115可以利用它们通信地耦合到的一个或多个网络元件的一个或多个协议。网络115可以转换为网络设备的一个或多个协议或从其他协议转换为网络设备的一个或多个协议。尽管网络115被描绘为单个网络，但是应当理解，根据一个或多个示例，网络115可以包括多个互连的网络，例如因特网、服务提供商的网络、有线电视网络、公司网络(例如信用卡关联网络)和家庭网络。

[0038] 系统100可以包括一个或多个服务器120。在一些示例中，服务器120可以包括耦合到存储器的一个或多个处理器。服务器120可以被配置为中央系统，服务器或平台，以在不同时间处控制和调用各种数据以执行多个工作流动作。服务器120可以被配置为连接到一个或多个数据库。服务器120可以连接到至少一个客户端设备110。

[0039] 图1B是示出根据本公开的一个或多个实施例的用于提供认证访问的示例序列的时序图。系统100可以包括非接触式卡105和客户端设备110，其可以包括应用122和处理器124。图1B中的部件可以参考如图1B中所示的类似部件。

[0040] 在步骤102，应用122与非接触式卡105通信(例如，在被带到非接触式卡105附近之后)。应用122和非接触式卡105之间的通信可以包括：非接触式卡105足够靠近客户端设备110的卡读取器(未示出)，以使得能够在应用程序122和非接触式卡105之间进行NFC数据传输。

[0041] 在步骤104，在客户端设备110与非接触式卡105之间建立了通信之后，非接触式卡105生成消息认证码(MAC)密码。在一些示例中，这可以在应用程序122读取非接触式卡105时发生。特别地，这可以发生在读取(例如，NFC读取)近场数据交换(NDEF)标签时，其可以根据NFC数据交换格式来创建。例如，诸如应用122之类的读取器可以发送消息诸如小应用程序选择消息，其具有产生NDEF的小程序的小程序ID。在确认选择之后，可以发送选择文件消息随后是读取文件消息的序列。例如，序列可以包括“选择功能文件”，“读取功能文件”和“选择NDEF文件”。此时，可以更新或递增由非接触式卡105维护的计数器值，其后可以是“读

取NDEF文件”。此时，可以生成可包括报头(header)和共享机密的消息。然后可以生成会话密钥。可以从消息创建MAC密码，该消息可以包括报头和共享机密。然后可以将MAC密码与一个或多个随机数据块级联，然后可以用会话密钥对MAC密码和随机数(RND)进行加密。此后，可以将密码和报头进行级联，并编码为ASCII十六进制，并以NDEF消息格式返回(响应于“读取NDEF文件”消息)。

[0042] 在一些示例中，MAC密码可以作为NDEF标签被发送，并且在其他示例中，MAC密码可以以统一资源指示符(例如，作为格式化的字符串)被包括。

[0043] 在一些示例中，应用122可以被配置为向非接触式卡105发送请求，该请求包括用于生成MAC密码的指令。

[0044] 在步骤106，非接触式卡105将MAC密码发送到应用122。在一些示例中，MAC密码的传输经由NFC发生，但是，本公开不限于此。在其他示例中，该通信可以经由蓝牙、Wi-Fi或其他无线数据通信的方式发生。

[0045] 在步骤108，应用122将MAC密码传送给处理器124。

[0046] 在步骤112，处理器124根据来自应用122的指令来验证MAC密码。例如，如下所述，可以验证MAC密码。

[0047] 在一些示例中，可以由除客户端设备110之外的设备(诸如与客户端设备110进行数据通信的服务器120)执行验证MAC密码的操作(如图1A所示)。例如，处理器124可以输出MAC密码以传输到服务器120，服务器120可以验证MAC密码。

[0048] 在一些示例中，为了验证的目的，MAC密码可以用作数字签名。其他数字签名算法诸如公钥非对称算法，例如数字签名算法(Digital Signature Algorithm)和RSA算法，或零知识协议，可以用于执行该验证。

[0049] 图2示出了根据示例实施例的数据传输系统。系统200可以包括例如经由网络215与一个或多个服务器220通信的传输或发送设备205，接收或接收者设备210。传输或发送设备205可以与以上参考图1A讨论的客户端设备110相同或相似。接收或接收者设备210可以与以上参考图1A讨论的客户端设备110相同或相似。网络215可以类似于以上参考图1A讨论的网络115。服务器220可以类似于以上参考图1A讨论的服务器120。尽管图2示出了系统200的组件的单个实例，但是系统200可以包括任何数量的所示组件。

[0050] 当使用对称加密算法，例如加密演算法、基于哈希的消息认证码(HMAC)算法和基于密文的消息认证码(CMAC)算法时，重要的是，密钥保持在最初处理使用对称算法和密钥进行保护的数据的一方、与使用相同密码算法和相同密钥接收和处理数据的一方之间。

[0051] 还重要的是，相同密钥不使用太多次。如果密钥使用或重用过于频繁，则可能会损害该密钥。每次使用密钥时，都会向攻击者提供已由密码算法使用相同密钥处理的额外数据样本。攻击者拥有的使用相同密钥处理的数据越多，攻击者可能发现密钥值的可能性就越大。经常使用的密钥可能被包含在各种不同的攻击中。

[0052] 此外，每次执行对称密码算法时，它可能会揭示有关在对称密码操作期间使用的密钥的信息，诸如副信道数据(side-channel data)。副信道数据可能包括微小的功率波动，其在使用密钥时执行加密算法时发生。可以对副信道数据进行足够的测量，以揭示有关密钥的足够信息，以使其能够被攻击者恢复。使用相同的密钥交换数据将反复地揭示由相同密钥处理的数据。

[0053] 但是，通过限制将使用的特定密钥的次数，攻击者能够收集的副信道数据量受到限制，从而减少了暴露于此和其他类型攻击。如本文中进一步描述的，参与密码信息交换的各方(例如，发送者和接收者)可以独立地从初始共享主对称密钥结合计数器值来生成密钥，由此周期性地替换正在使用的共享对称密钥，连同需要依靠任何形式的密钥交换以使各方保持同步。通过周期性地更改发送者和接收者使用的共享秘密对称密钥，上述攻击变得不可能。

[0054] 回到图2，系统200可以被配置为实现密钥多样化。例如，发送者和接收者可能希望经由各自的设备205和210交换数据(例如，原始敏感数据)。如上所述，尽管可以包括发送设备205和接收设备210的单个实例，但是应当理解，可以涉及一个或多个发送设备205和一个或多个接收设备210，只要每一方共享相同的共享秘密对称信息即可。在一些示例中，可以向发送设备205和接收设备210提供相同的主对称密钥。此外，应当理解，拥有相同秘密对称密钥的任何一方或设备都可以执行发送设备205的功能，并且相似地，拥有相同秘密对称密钥的任何一方都可以执行接收设备210的功能。在一些示例中，对称密钥可以包括共享秘密对称密钥，该共享秘密对称密钥对除了涉及交换安全数据的发送设备205和接收设备210之外的所有其他方保持秘密。还应理解的是，发送设备205和接收设备210都可以被提供有相同的主对称密钥，并且进一步地，在发送设备205和接收设备210之间交换的数据的一部分包括至少一部分数据，可以称为计数器值。计数器值可以包括每次在发送设备205和接收设备210之间交换数据时改变的数字。

[0055] 系统200可以包括一个或多个网络215。在一些示例中，网络215可以是以下中的一个或多个:无线网络，有线网络或者无线网络和有线网络的任意组合，并且可以被配置为将一个或多个发送设备205和一个或多个接收设备210连接到服务器220。例如，网络215可以包括以下中的一个或多个:光纤网络、无源光网络、电缆网络、因特网网络、卫星网络、无线LAN、全球移动通信系统、个人通信服务、个人局域网、无线应用协议、多媒体消息服务、增强消息服务，短消息服务、基于时分多路复用的系统、基于码分多址的系统、D-AMPS、Wi-Fi、固定无线数据、IEEE802.11b、802.15.1、802.11n和802.11g、蓝牙、NFC、RFID、Wi-Fi等。

[0056] 另外，网络215可以包括但不限于:电话线、光纤、IEEE以太网902.3、广域网、无线个人局域网、LAN或诸如因特网的全球网络。另外，网络215可以支持因特网网络、无线通信网络、蜂窝网络等或其任何组合。网络215可以进一步包括一个网络，或者上述任何数量的示例性类型的网络，其作为独立网络运行或彼此协作。网络215可以利用它们通信地耦合到的一个或多个网络元件的一个或多个协议。网络215可以转换为网络设备的一个或多个协议或从其他协议转换为网络设备的一个或多个协议。尽管网络215被描绘为单个网络，但是应当理解，根据一个或多个示例，网络215可以包括多个互连的网络，例如，因特网、服务提供商的网络、有线电视网络、公司网络(例如信用卡关联网络)和家庭网络。

[0057] 在一些示例中，一个或多个发送设备205和一个或多个接收设备210可以被配置为在没有通过网络215的情况下在彼此之间进行数据通信、发送和接收数据。例如，一个或多个发送设备205与一个或多个接收设备210之间的通信可以经由NFC、蓝牙、RFID、Wi-Fi等中的至少一种发生。

[0058] 在框225处，当发送设备205正准备使用对称密码操作来处理敏感数据时，发送者可以更新计数器。另外，发送设备205可以选择适当的对称密码算法，该对称密码算法可以

包括:对称加密算法、HMAC算法和CMAC算法中的至少一种。在一些示例中,用于处理多样化值的对称算法可以包括:根据需要用于生成期望的长度多样化对称密钥的任何对称密码算法。对称算法的非限制性示例可以包括:诸如3DES或AES128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。应当理解,如果所选对称算法的输出没有生成足够长的密钥,则诸如用不同的输入数据和相同的主密钥处理对称算法的多次迭代的技术可能会产生多个输出,其可以根据需要进行组合以产生足够长的密钥。

[0059] 在框230处,发送设备205可以采用所选密码算法,并且使用主对称密钥来处理计数器值。例如,发送者可以选择对称加密算法,并且使用随着发送设备205和接收设备210之间的每次对话而更新的计数器。然后,发送设备205可以使用主对称密钥通过所选对称加密算法对计数器值进行加密,从而创建多样化对称密钥。

[0060] 在一些示例中,计数器值可以没有加密。在这些示例中,可以在框230处在发送设备205和接收设备210之间发送计数器值而无需加密。

[0061] 在框235处,在将结果发送到接收设备210之前,可以使用多样化对称密钥来处理敏感数据。例如,发送设备205可以使用使用多样化对称密钥的对称加密算法来对敏感数据进行加密,其中输出包括受保护的加密数据。然后,发送设备205可以将受保护的加密数据以及计数器值发送到接收设备210以进行处理。

[0062] 在框240处,接收设备210可以首先获取计数器值,然后使用该计数器值作为对加密的输入并使用主对称密钥作为用于加密的密钥来执行相同的对称加密。加密的输出可以是相同的由发送者创建的多样化对称密钥值。

[0063] 在框245处,接收设备210然后可以获取受保护的加密数据,并且使用对称解密算法以及多样化对称密钥来解密受保护的加密数据。

[0064] 在框250,作为解密受保护的加密数据的结果,可以揭示原始敏感数据。

[0065] 下次需要经由相应的发送设备205和接收设备210将敏感数据从发送者发送到接收者时,可以选择不同的计数器值来产生不同的多样化对称密钥。通过使用主对称密钥和相同的对称密码算法处理计数器值,发送设备205和接收设备210都可以独立地产生相同的多样化对称密钥。这种多样化对称密钥而不是主对称密钥被用于保护敏感数据。

[0066] 如上所述,发送设备205和接收设备210均初始具有共享的主对称密钥。共享的主对称密钥不用于加密原始敏感数据。由于多样化对称密钥是由发送设备205和接收设备210均独立创建的,因此它永远不会在双方之间传输。因此,攻击者无法截取多样化对称密钥,并且攻击者永远不会看到使用主对称密钥处理过的任何数据。使用主对称密钥处理仅计数器值,而不是敏感数据。结果,揭示了关于主对称密钥的减少的副信道数据。而且,发送设备205和接收设备210的操作可以由关于多久创建新的多样化值以及因此的新的多样化对称密钥的对称性要求所控制。在一个实施例中,可以为发送设备205和接收设备210之间的每次交换创建新的多样化值,并因此创建新的多样化对称密钥。

[0067] 在一些示例中,密钥多样化值可以包括计数器值。密钥多样化值的其他非限制性示例包括:每次需要新的多样化密钥时生成的随机数(random nonce),所述随机数从发送设备205发送到接收设备210;从发送设备205和接收设备210发送的计数器值的全值;从发送设备205和接收设备210发送的计数器值的一部分;由发送设备205和接收设备210独立保持、但不在两个设备之间发送的计数器;在发送设备205和接收设备210之间交换的一次性

密码;以及敏感数据的密码哈希。在一些示例中,各方可以使用密钥多样化值的一个或多个部分来创建多个多样化密钥。例如,可以将计数器用作密钥多样化值。此外,可以使用上述示例性密钥多样化值中的一个或多个的组合。

[0068] 在另一个示例中,计数器的一部分可以用作密钥多样化值。如果各方之间共享多个主密钥值,则可以通过本文所述的系统和过程来获得多个多样化密钥值。可以根据需要经常创建新的多样化值,以及因此的新的多样化对称密钥。在最安全的情况下,可以为发送设备205和接收设备210之间的每次敏感数据交换创建新的多样化值。实际上,这可以创建一次性使用密钥,例如一次性会话密钥。

[0069] 图3示出了使用非接触式卡的系统300。系统300可包括非接触式卡305,一个或多个客户端设备310,网络315,服务器320、325,一个或多个硬件安全模块330以及数据库335。尽管图3示出了组件的单个实例,但是系统300可以包括任何数量的组件。

[0070] 系统300可以包括一个或多个非接触式卡305,下面相对于图5A-5B进一步说明。在一些示例中,非接触式卡305可以与客户端设备310进行无线通信,例如NFC通信。例如,非接触式卡305可以包括一个或多个芯片诸如射频识别芯片,其被配置为经由NFC或其他短距离协议进行通信。在其他实施例中,非接触式卡305可以通过其他方式与客户端设备310通信,该其他方式包括但不限于:蓝牙,卫星,Wi-Fi,有线通信和/或无线和有线连接的任意组合。根据一些实施例,非接触式卡305可以被配置为当非接触式卡305在卡读取器313的范围内时,通过NFC与客户端设备310的卡读取器313通信。在其他示例中,与非接触式卡305的通信可以通过物理接口(例如,通用串行总线接口或卡刷取接口)来实现。

[0071] 系统300可以包括客户端设备310,其可以是启用网络的计算机。如本文所指,启用网络的计算机可以包括但不限于:例如计算机设备,或通信设备,包括:例如服务器,网络应用设备,个人计算机,工作站,移动设备,电话,手持式PC,个人数字助理,瘦客户端,胖客户端,Internet浏览器或其他设备。一个或多个客户端设备310也可以是移动设备。例如,移动设备可以包括Apple®的iPhone,iPod,iPad或运行Apple的iOS®操作系统的任何其他移动设备,运行Microsoft的Windows®Mobile操作系统的任何设备,运行Google的Android®操作系统的任何设备,和/或任何其他智能手机或类似的可穿戴移动设备。在一些示例中,客户端设备310可以与参考图1A或图1B描述的客户端设备110相同或相似。

[0072] 客户端设备310可以经由一个或多个网络315与一个或多个服务器320和325通信。客户端设备310可以例如从在客户端设备310上执行的应用311向一个或多个服务器320和325发送一个或多个请求。该一个或多个请求可以与从一个或多个服务器320和325检索数据相关联。服务器320和325可以从客户端设备310接收一个或多个请求。基于来自客户端设备310的一个或多个请求,一个或多个服务器320和325可以被配置为从一个或多个数据库335检索所请求的数据。基于从一个或多个数据库335接收到所请求的数据,一个或多个服务器320和325可以被配置为将所接收的数据发送到客户端设备310,所述所接收的数据响应于一个或多个请求。

[0073] 系统300可以包括一个或多个硬件安全模块(HSM)330。举例来说,一个或多个HSM 330可被配置为执行一个或多个密码操作,如本文所公开的。在一些示例中,一个或多个HSM 330可以被配置为专用安全设备,其被配置为执行一个或多个密码操作。HSM 330可以被配

置为使得密钥永远不会在HSM 330外部泄露，而是被保持在HSM 330内。例如，一个或多个HSM 330可以被配置为执行密钥派生、解密和MAC操作中的至少一项。一个或多个HSM 330可以被包含在服务器320和325内或者可以与服务器320和325进行数据通信。

[0074] 系统300可以包括一个或多个网络315。在一些示例中，网络315可以是无线网络、有线网络、或无线网络和有线网络的任何组合中的一个或多个，并且可以被配置为将客户端设备315连接到服务器320和325。例如，网络315可以包括以下一个或多个：光纤网络，无源光网络，电缆网络，蜂窝网络，因特网网络，卫星网络，无线LAN，全球移动通信系统，个人通信服务，个人局域网，无线应用协议，多媒体消息服务，增强消息服务，短消息服务，基于时分多路复用的系统，基于码分多址的系统，D-AMPS，Wi-Fi，固定无线数据，IEEE802.11b，802.15.1，802.11n和802.11g，蓝牙，NFC，RFID，Wi-Fi和/或其网络的任何组合。作为非限制性示例，来自非接触式卡305和客户端设备310的通信可以包括：NFC通信，客户端设备310与运营商之间的蜂窝网络，以及运营商与后端之间的因特网。

[0075] 另外，网络315可以包括但不限于：电话线，光纤，IEEE以太网902.3，广域网，无线个人局域网，局域网或诸如因特网的全球网络。另外，网络315可以支持因特网网络，无线通信网络，蜂窝网络等或其任意组合。网络315可以进一步包括一个网络，或者上述任何数量的示例性类型的网络，其作为独立网络运行或彼此协作。网络315可以利用它们通信地耦合到的一个或多个网络元件的一个或多个协议。网络315可以转换为网络设备的一个或多个协议或从其他协议转换为网络设备的一个或多个协议。尽管网络315被描绘为单个网络，但是应当理解，根据一个或多个示例，网络315可以包括多个互连的网络，例如，因特网，服务提供商的网络，有线电视网络，公司网络(例如信用卡关联网络)和家庭网络。

[0076] 在根据本公开的各种示例中，系统300的客户端设备310可以执行一个或多个应用311，并且包括一个或多个处理器312以及一个或多个卡读取器313。举例来说，可将一个或多个应用311(例如，软件应用程序)配置为启用例如与系统300的一个或多个组件的网络通信，并发送和/或接收数据。应该理解，尽管在图3中仅示出了客户端设备310的组件的单个实例，但可以使用任何数量的设备310。卡读取器313可以被配置为从非接触式卡305读取和/或与非接触式卡305通信。结合一个或多个应用311，卡读取器313可以与非接触式卡305通信。

[0077] 客户端设备310中的任何一个的应用311可以使用短距离无线通信(例如，NFC)与非接触式卡305通信。应用311可以被配置为与客户端设备310的卡读取器313对接，其被配置为与非接触式卡305进行通信。应当注意，本领域技术人员将理解，小于二十厘米的距离与NFC范围一致。

[0078] 在一些实施例中，应用311通过关联的读取器(例如，卡读取器313)与非接触式卡305进行通信。

[0079] 在一些实施例中，卡激活可以在没有用户认证的情况下发生。例如，非接触式卡305可以通过NFC通过客户端设备310的卡读取器313与应用311通信。通信(例如，卡靠近于客户端设备310的卡读取器313的轻拍(tap))允许应用311读取与卡相关联的数据并执行激活。在某些情况下，轻拍可以激活或启动应用311，然后发起一个或多个动作或与账户服务器325的通信以激活卡以用于随后的使用。在某些情况下，如果在客户端设备310上未安装应用311，则对着卡读取器313的轻拍可以发起应用311的下载(例如，导航到应用下载页

面)。在安装之后,轻拍可以激活或启动应用311,然后发起(例如,经由应用或其他后端通信)卡的激活。激活后,该卡可用于各种交易,包括商业交易。

[0080] 根据一些实施例,非接触式卡305可以包括虚拟支付卡。在那些实施例中,应用311可以通过访问在客户端设备310上实现的数字钱包来检索与非接触式卡305相关联的信息,其中,数字钱包包括虚拟支付卡。在一些示例中,虚拟支付卡数据可以包括一个或多个静态或动态生成的虚拟卡号。

[0081] 服务器320可以包括与数据库335通信的网络服务器。服务器325可以包括帐户服务器。在一些示例中,服务器320可以被配置为通过与数据库335中的一个或多个证书进行比较来验证来自非接触式卡305和/或客户端设备310的一个或多个证书。服务器325可以被配置为授权来自非接触式卡305和/或客户端设备310的一个或多个请求,例如支付和交易。

[0082] 图4示出了根据本公开的示例的密钥多样化的方法400。方法400可以包括与图2中参照的发送设备205和接收设备210相似的发送设备和接收设备。

[0083] 例如,发送者和接收者可能希望经由发送设备和接收设备交换数据(例如,原始敏感数据)。如上所述,尽管可以包括这两个方,但是应理解可以涉及一个或多个发送设备和一个或多个接收设备,只要每一方共享相同的共享的秘密对称密钥即可。在一些示例中,可以向发送设备和接收设备提供相同的主对称密钥。此外,应当理解,持有相同秘密对称密钥的任何一方或设备都可以执行发送设备的功能,并且类似地,持有相同秘密对称密钥的任何一方都可以执行接收设备的功能。在一些示例中,对称密钥可以包括共享的秘密对称密钥,该共享的秘密对称密钥对除了涉及交换安全数据的发送设备和接收设备之外的所有其他方保持秘密。还应理解,发送设备和接收设备都可以被提供有相同的主对称密钥,并且进一步地,在发送设备和接收设备之间交换的数据的一部分包括:可以被称为计数器值的数据的至少一部分。该计数器值可以包括:每次在发送设备和接收设备之间交换数据时都会改变的数字。

[0084] 在框410处,可以向发送设备和接收设备提供相同的主密钥,例如相同的主对称密钥。当发送设备准备使用对称密码操作处理敏感数据时,发送者可以更新计数器。另外,发送设备可以选择适当的对称密码算法,该对称密码算法可以包括:对称加密算法,HMAC算法和CMAC算法中的至少一种。在一些示例中,用于处理多样化值的对称算法可以包括根据需要用于生成期望长度的多样化对称密钥的任何对称密码算法。对称算法的非限制性示例可以包括:诸如3DES或AES128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。应当理解,如果所选对称算法的输出没有生成足够长的密钥,则诸如用不同的输入数据和相同的主密钥处理对称算法的多次迭代的技术可能会产生多个输出,其可以根据需要进行组合以产生足够长的密钥。

[0085] 发送设备可以采用所选密码算法,并使用主对称密钥来处理计数器值。例如,发送者可以选择对称加密算法,并使用随着发送设备和接收设备之间的每次对话而更新的计数器。

[0086] 在框420处,发送设备然后可以使用主对称密钥通过所选对称加密算法来加密计数器值,从而创建多样化对称密钥。在将结果发送到接收设备之前,可以使用多样化对称密钥来处理敏感数据。例如,发送设备可以使用使用多样化对称密钥的对称加密算法对敏感数据进行加密,其中输出包括受保护的加密数据。然后,发送设备可以将受保护的加密数据

以及计数器值发送到接收设备进行处理。在一些示例中，可以执行除加密之外的密码操作，并且可以在传输受保护的数据之前使用多样化对称密钥来执行多个密码操作。

[0087] 在一些示例中，计数器值可能未加密。在这些示例中，可以在框420处在没有加密的情况下在发送设备和接收设备之间发送计数器值。

[0088] 在框430处，可以使用一种或多种密码算法和多样化密钥来保护敏感数据。可通过使用了计数器的密钥多样化而创建的多样化会话密钥可以与一种或多种密码算法一起使用以保护敏感数据。例如，可以使用第一多样化会话密钥由MAC处理数据，并且可以使用产生受保护数据的第二多样化会话密钥对结果输出进行加密。

[0089] 在框440处，接收设备可以使用计数器值作为对加密的输入并且使用主对称密钥作为用于加密的密钥来执行相同的对称加密。加密的输出可以是与发送者创建了的相同的对称密钥值。例如，接收设备可以使用计数器独立地创建其自己的第一和第二多样化会话密钥的副本。然后，接收设备可以使用第二多样化会话密钥来解密受保护的数据，以揭示由发送设备创建的MAC的输出。接收设备然后可以使用第一多样化会话密钥通过MAC操作来处理结果数据。

[0090] 在框450，接收设备可以将多样化密钥与一种或多种密码算法一起使用以验证受保护的数据。

[0091] 在框460，可以验证原始数据。如果MAC操作的输出(经由接收设备使用第一多样化会话密钥)与由解密揭示的MAC输出匹配，则该数据可以被视为有效。

[0092] 下次需要将敏感数据从发送设备发送到接收设备时，可以选择不同的计数器值，这会产生不同的多样化对称密钥。通过使用主对称密钥和相同的对称密码算法处理计数器值，发送设备和接收设备都可以独立地产生相同的多样化对称密钥。这种多样化对称密钥而不是主对称密钥用于保护敏感数据。

[0093] 如上所述，发送设备和接收设备均初始都具有共享的主对称密钥。共享的主对称密钥不用于加密原始敏感数据。由于多样化对称密钥是由发送设备和接收设备独立创建的，因此它永远不会在双方之间传输。因此，攻击者无法截取多样化对称密钥，并且攻击者永远不会看到使用主对称密钥处理过的任何数据。使用主对称密钥处理仅较小的计数器值，而不是敏感数据。结果，揭示了关于主对称密钥的减少的副信道数据。而且，发送者和接收者可以例如通过先前的布置或其他方式来同意多久创建新的多样化值、以及因此的新的多样化对称密钥。在一个实施例中，可以为发送设备和接收设备之间的每次交换创建新的多样化值、以及因此的新的多样化对称密钥。

[0094] 在一些示例中，密钥多样化值可以包括计数器值。密钥多样化值的其他非限制性示例包括：每次需要新的多样化密钥时生成的随机数，所述随机数从发送设备发送到接收设备；从发送设备和接收设备发送的计数器值的全值；从发送设备和接收设备发送的计数器值的一部分；由发送设备和接收设备独立保持但不在两者之间发送的计数器；在发送设备和接收设备之间交换的一次性密码；敏感数据的密码哈希。在一些示例中，各方可以使用密钥多样化值的一个或多个部分来创建多个多样化密钥。例如，可以将计数器用作密钥多样化值。

[0095] 在另一个示例中，计数器的一部分可以用作密钥多样化值。如果各方之间共享多个主密钥值，则可以通过本文描述的系统和过程来获得多个多样化密钥值。可以根据需要

经常创建新的多样化值，以及因此的新的多样化对称密钥。在最安全的情况下，可以为发送设备和接收设备之间的每次敏感数据交换创建新的多样化值。实际上，这可以创建一次性使用密钥，例如单个会话密钥。

[0096] 在其他示例中，例如为了限制主对称密钥的使用次数，由发送设备的发送者和接收设备的接收者可以同意新的多样化值、以及因此的新的多样化对称密钥将只会定期地发生。在一个示例中，这可以是在预定次数的使用之后，诸如在发送设备和接收设备之间的每十次传输之后。在另一示例中，这可以是在一定时间段之后，在传输之后的特定时间段之后，或者是周期性的(例如，在指定时间的每天；在指定日期的指定时间每周地)。在另一示例中，这可以是接收设备每次向发送设备发信号通知其希望在下一次通信中改变密钥时。这可以在策略上进行控制并且可以由于例如接收设备的接收者所感知的当前风险水平而改变。

[0097] 图5A示出了一个或多个非接触式卡500，其可以包括由显示在卡500的正面或背面上的服务提供商505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500与支付卡无关，并且可以包括但不限于身份证。在一些示例中，支付卡可以包括双接口非接触式支付卡。非接触式卡500可以包括基板510，其可以包括由塑料、金属和其他材料构成的单层或者一个或多个层压层。示例性的基材材料包括：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，阳极氧化的钛，钯，金，碳，纸和可生物降解的材料。在一些示例中，非接触式卡500可以具有符合ISO/IEC7810标准的ID-1格式的物理特性，并且非接触式卡可以以其他方式符合ISO/IEC14443标准。然而，应当理解，根据本公开的非接触式卡500可以具有不同的特性，并且本公开不需要在支付卡中实现非接触式卡。

[0098] 非接触式卡500还可包括显示在卡的正面和/或背面上的识别信息515，以及接触片520。接触片520可以被配置为与另一通信设备建立联系，所述另一通信设备诸如用户设备，智能电话，膝上型计算机，台式计算机或平板计算机。非接触式卡500还可以包括处理电路，天线和其他在图5A中未示出的组件。这些组件可以位于接触片520的后面或基板510上的其他位置。非接触式卡500还可以包括磁条或磁带，其可以位于卡的背面(图5A中未示出)。

[0099] 如图5B所示，图5A的接触片520可以包括：用于存储和处理信息的处理电路525，包括微处理器530和存储器535。应当理解，处理电路525可以包含附加组件，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，以如所需的执行本文所述的功能。

[0100] 存储器535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500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是一次性可编程的。一次性编程功能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芯片出厂后的某个时间点进行编程。一旦对存储器进行编程，就可能无法对其进行重写，但是可以对其进行多次读取。读/写存储器可以在出厂后进行多次编程和重新编程。它也可以被多次读取。

[0101] 存储器535可以被配置为存储一个或多个小应用程序540，一个或多个计数器545以及客户标识符550。一个或多个小应用程序540可以包括被配置为在一个或多个非接触式卡上执行的一个或多个软件应用程序，诸如Java Card小应用程序。然而，应理解，小应用程

序540不限于Java Card小应用程序,而是可以是可在非接触式卡或具有有限存储器的其他设备上操作的任何软件应用程序。一个或多个计数器545可包括足以存储整数的数字计数器。客户标识符550可以包括分配给非接触式卡500的用户的唯一字母数字标识符,并且该标识符可以将非接触式卡的用户与其他非接触式卡用户区分开。在一些示例中,客户标识符550可以识别客户和分配给该客户的账户,并且可以进一步识别与客户的账户相关联的非接触式卡。

[0102] 参照接触片描述了前述示例性实施例的处理器和存储元件,但是本公开不限于此。应当理解,这些元件可以在片520的外部实现或与片520完全分离,或者作为位于接触片520内的处理器530和存储器535之外的其他元件实现。

[0103] 在一些示例中,非接触式卡500可以包括一个或多个天线555。一个或多个天线555可以被放置在非接触式卡500内并且在接触片520的处理电路525周围。例如,一个或多个天线555可以与处理电路525一体形成,并且一个或多个天线555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555可以在接触片520和处理电路525的外部。

[0104] 在一个实施例中,非接触式卡500的线圈可以用作空芯变压器的次级。终端可以通过切断功率或幅度调制来与非接触式卡500通信。非接触式卡500可以使用非接触式卡的电源连接中的间隙来推断从终端发送的数据,该间隙可以被一个或多个电容器功能性地保持。非接触式卡500可以通过切换非接触式卡的线圈上的负载或负载调制来进行回传。可以通过干扰来在终端的线圈中检测到负载调制。

[0105] 如上所述,非接触式卡500可以建立在可在智能卡或具有有限存储器的其他设备(例如JavaCard)上操作的软件平台上,并且可以安全地执行一个或多个应用或小应用程序。在各种基于移动应用程序的使用案例中,可以将小应用程序添加到非接触式卡以提供一次性密码(OTP)以进行多因素认证(MFA)。小应用程序可以配置为响应来自读取器(例如移动NFC读取器)的一个或多个请求(例如近场数据交换请求),并生成NDEF消息,该消息包括被编码为NDEF文本标签的加密安全OTP。

[0106] 图6示出了根据示例实施例的NDEF短记录布局(SR=1)600。一个或多个小应用程序可以配置为将OTP编码为NDEF类型4,其是众所周知类型的文本标签。在一些示例中,NDEF消息可以包括一个或多个记录。小应用程序可以配置为除了OTP记录外还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:众所周知的类型,文本,编码英语(en);Applet ID:D2760000850101;功能性:只读访问;编码:认证消息可以编码为ASCII十六进制;可以提供类型长度值(type-length-value,TLV)数据作为可用于生成NDEF消息的个性化参数。在一个实施例中,认证模板可以包括第一记录,其具有用于提供实际动态认证数据的众所周知的索引。

[0107] 图7示出了根据示例实施例的消息710和消息格式720。在一个示例中,如果要添加额外标签,则第一个字节可以更改以指示消息开始而不是结束,并且可以添加后续记录。因为ID长度为零,所以从记录中省略了ID长度字段和ID。消息示例可以包括:UDK AUT密钥;派生的AUT会话密钥(使用0x00000050);版本1.0;pATC=0x00000050;RND=4838FB7DC171B89E;MAC=<八个计算的字节>。

[0108] 在一些示例中,可以通过在安全通道协议2下实现STORE DATA(E2)来在个性化时间将数据存储在非接触式卡中。可以由个性化局从EMBOSS文件(在AppletID指定的部分中)

读取一个或多个值，并且可以在认证和安全通道建立后将一个或多个存储数据命令发送到非接触式卡。

[0109] pUID可以包含16位BCD编码的数字。在一些示例中，pUID可以包括14个数字。

[0110]

项	长度（字节）	加密的？	注解
pUID	8	否	
AutKey	16	是	用于派生 MAC 会话密钥的 3DES 密钥
AutKCV	3	否	密钥检查值
DEKKey	16	是	用于派生加密会话密钥的 3DES 密钥
DEKKCV	3	否	密钥检查值
Card Shared Random	4 字节	否	4 字节真随机数（预生成的）
NTLV	X 字节	否	用于 NDEF 消息的 TLV 数据

[0111] 在一些示例中，一个或多个小应用程序可以被配置为维持其个性化状态以允许仅在被解锁和认证后的个性化。其他状态可以包括标准状态的预个性化。在进入终止状态时，一个或多个小应用程序可以配置为移除个性化数据。在终止状态下，一个或多个小应用程序可以配置为停止响应所有应用协议数据单元(APDU)请求。

[0112] 一个或多个小应用程序可以配置为维护小应用程序版本(2字节)，其可以在认证消息中使用。在一些示例中，这可以被解释为最高有效字节主要版本，最低有效字节次要版本。用于每个版本的规则被配置为解释认证消息：例如，关于主要版本，这可以包括：每个主要版本包括特定的认证消息布局和特定的算法。对于次要版本，这可以包括：对认证消息或密码算法的不更改，并且除了错误修复、安全性增强等之外，还对静态标签内容的更改。

[0113] 在一些示例中，一个或多个小应用程序可以被配置为模拟RFID标签。RFID标签可以包括一个或多个多态标签。在一些示例中，每次读取标签时，都会呈现不同的密码数据，这些数据可以指示非接触式卡的真实性。基于一个或多个应用，可以处理标签的NFC读取，可以将令牌发送到服务器，例如后端服务器，并且可以在服务器上验证令牌。

[0114] 在一些示例中，非接触式卡和服务器可以包括某些数据，使得可以正确地识别卡。非接触式卡可以包括一个或多个唯一标识符。每次发生读取操作时，可以将计数器配置为更新。在一些示例中，每次读取卡时，将其发送到服务器以进行验证并确定计数器是否相等(作为验证的一部分)。

[0115] 一个或多个计数器可以被配置为防止重放攻击(replay attack)。例如，如果已经获取并重放了密码，则如果计数器已被读取或使用或以其他方式传递，则该密码将立即被拒绝。如果尚未使用该计数器，则可以重放它。在一些示例中，在卡上更新的计数器与针对交易更新的计数器不同。在一些示例中，非接触式卡可以包括第一小应用程序和第二小应用程序，第一小应用程序可以是交易小应用程序。每个小应用程序可以包括计数器。

[0116] 在一些示例中，计数器可以在非接触式卡和一个或多个服务器之间不同步。例如，非接触式卡可以被激活以致使计数器被更新并且非接触式卡生成新的通信，但是该通信可以不被发送以为了在一个或多个服务器处进行处理。这可能导致非接触式卡的计数器与在一个或多个服务器上维护的计数器不同步。例如，这可能会无意地发生，包括：例如，卡临近于设备而存储(例如，随设备一起放在口袋中)时，和非接触式卡以一定角度读取时，可能包括卡未对齐或未定位，使得非接触式卡被加电NFC场，但是无法读取。如果非接触式卡与设备相邻放置，则设备的NFC场可能会打开以为非接触式卡供电，从而导致其中的计数器被更新，但是设备上没有应用接收到通信。

[0117] 为了使计数器保持同步，可以执行诸如后台应用之类的应用，其将被配置为检测移动设备何时醒来并与一个或多个服务器同步以指示由于检测到而发生读取然后使计数器向前移动。由于非接触式卡的计数器和一个或多个服务器可能不同步，因此一个或多个服务器可以配置为允许非接触式卡的计数器在其被一个或多个服务器读取之前被更新阈值或预定次数，并且仍然被视为有效。例如，如果将计数器配置为针对指示非接触式卡的激活的每次出现而递增(或递减)一，则一个或多个服务器可以允许其从非接触式卡读取的任何计数器值都是有效的，或者在阈值范围(例如，从1到10)内的任何计数器值都是有效的。而且，一个或多个服务器可以被配置为请求与非接触式卡相关联的姿势(gesture)，例如用户的轻拍，如果它读取了计数器值已经超过10但又低于另一阈值范围值(例如1000)的话。通过用户的轻拍，如果计数器值在期望或接受范围内，则验证成功。

[0118] 图8是示出根据示例实施例的键操作800的流程图。如图8所示，在框810处，可以将两个银行标识符号(BIN)级别的主密钥与账户标识符和卡序列号结合使用，以产生每张卡两个唯一的派生密钥(UDK)。在一些示例中，银行标识符号码可以包括一个号码或一个或多个号码的组合，例如由一个或多个服务器提供的帐号或不可预测的号码，其可以用于会话密钥生成和/或多样化。UDK(AUTKEY和ENCKEY)可以在个性化过程期间存储在卡上。

[0119] 在框820处，计数器可以用作多样化数据，因为它随着每次使用而改变并且每次都提供不同的会话密钥，这与主密钥派生相反——在其中产生了每张卡一个唯一的密钥集合。在一些示例中，最好对两个操作都使用4字节方法。因此，在框820处，可以为来自ETDK的每个交易创建两个会话密钥，即，来自AEGTKEU的一个会话密钥和来自ENCKEY的一个会话密钥。在卡中，对于MAC密钥(即，从AGTEKEU创建的会话密钥)，可以将OTP计数器的两个字节的低位用于多样化。对于ENC密钥(即从ENCKEY创建的会话密钥)，可以将OTP计数器的全长用于ENC密钥。

[0120] 在框830处,MAC密钥可以用于准备MAC密码,而ENC密钥可以用于加密密码。例如,MAC会话密钥可以用于准备密码,并且可以在结果被发送到一个或多个服务器之前用ENC密钥对其进行加密。

[0121] 在框840,简化了MAC的验证和处理,这是因为在支付HSM的MAC认证功能中直接支持2字节的多样化。密码的解密在对MAC的验证之前执行。会话密钥是在一个或多个服务器上独立派生的,从而产生第一会话密钥(ENC会话密钥)和第二会话密钥(MAC会话密钥)。第二派生密钥(即,ENC会话密钥)可以用于解密数据,并且第一派生密钥(即,MAC会话密钥)可以用于验证被解密的数据。

[0122] 对于非接触式卡,派生出不同的唯一标识符,该标识符可与卡中编码的应用主帐号(PAN)和PAN序列号有关。密钥多样化可以被配置为接收标识符作为与主密钥的输入,从而可以为每个非接触式卡创建一个或多个密钥。在一些示例中,这些多样化的密钥可以包括第一密钥和第二密钥。第一密钥可以包括认证主密钥(Card Crypotogram Generation/Authentication Key—Card-Key-Auth),并且可以进一步多样化以创建在生成和验证MAC密码时使用的MAC会话密钥。第二密钥可以包括加密主密钥(Card Data Encryption Key—Card-Key-DEK),并且可以进一步多样化以创建在加密和解密经加密的数据时使用的ENC会话密钥。在一些示例中,可以通过将发行者主密钥与支付小应用程序的卡的唯一ID号(pUTD)和PAN序列号(PSN)组合在一起来使发行者主密钥多样化,以创建第一密钥和第二密钥。该pUID可以包括16位数字值。如上所述,pUID可以包括16位BCD编码的数字。在一些示例中,pUTD可以包括14位数字值。

[0123] 在一些示例中,由于EMV会话密钥派生方法可以在2^16使用时进行包装(wrap),因此可以将计数器(例如完整的32位计数器)添加到多样化方法的初始化数组中。

[0124] 在其他示例中,例如信用卡中,可以将一个或多个服务器提供的数字(例如帐号或不可预测的数字)用于会话密钥的生成和/或多样化。

[0125] 图9示出了被配置为实现本公开的一个或多个实施例的系统900的图。如下所述,在非接触式卡创建过程中,可以为每个卡唯一地分配两个密码密钥。密码密钥可以包括可以在数据的加密和解密中使用的对称密钥。EMV可以使用三重DES(3DES)算法,并且该算法由非接触式卡中的硬件实现。通过使用密钥多样化过程,可以基于需要密钥的每个实体的唯一可识别信息而从主密钥派生一个或多个密钥。

[0126] 关于主密钥管理,对于发行一个或多个小应用程序的布局的每个部分,可能需要两个发行者主密钥905、910。例如,第一主密钥905可以包括发行者密码生成/认证密钥(Iss-Key-Auth),而第二主密钥910可以包括发行者数据加密密钥(Iss-Key-DEK)。如本文中进一步解释的,使两个发行者主密钥905、910多样化为卡主密钥925、930,这对于每个卡都是唯一的。在一些示例中,可以将作为后台数据的网络简档记录ID(pNPR)915和派生密钥索引(pDKI)920用于标识在加密过程中使用哪个发行者主密钥905、910进行认证。执行认证的系统可以被配置为在认证时检索非接触式卡的pNPR 915和pDKI 920的值。

[0127] 在一些示例中,为了提高解决方案的安全性,可以派生会话密钥(例如每个会话唯一的密钥),但是不使用主密钥,而是可以将派生自唯一卡的密钥和计数器用作多样化数据,如上所述。例如,每次在操作中使用卡时,可以使用不同的密钥来创建消息认证码(MAC)并执行加密。关于会话密钥生成,用于生成密码并加密一个或多个小应用程序中的数据的

密钥可以包括基于卡唯一密钥(Card-Key-Auth 925和Card-Key-Dek 930)的会话密钥。会话密钥(Aut-Session-Key 935和DEK-Session-Key 940)可以由一个或多个小应用程序生成,并且可以通过一种或多种算法使用应用交易计数器(pATC)945来派生。为了使数据适合一种或多种算法,仅使用4字节pATC 945的2个低位字节。在一些示例中,四字节会话密钥派生方法可以包括:F1:=PATC(较低2个字节)||'F0'||00'||PATC(四个字节)F1:=PATC(较低2个字节)||0F'||00'||PATC(四个字节)SK:={(ALG(MK)[F1])||ALG(MK)[F2]},其中ALG可包含3DES ECB,而MK可包含卡唯一派生的主密钥。

[0128] 如本文所述,可使用pATC 945计数器的低两个字节来派生一个或多个MAC会话密钥。在非接触式卡的每次轻拍时,将pATC 945配置为进行更新,并且卡主密钥Card-Key-AEiTH 925和Card-Key-DEK 930进一步多样化为会话密钥Aut-Session-Key 935和DEK-Session-Key 940。可以在个性化时或小应用程序初始化时间处将pATC 945初始化为零。在一些示例中,pATC计数器945可以在个性化时或个性化之前被初始化,并且可以被配置为在每次NDEF读取时增加1。

[0129] 此外,每个卡的更新可以是唯一的,并且可以通过个性化分配,也可以通过pETID或其他标识信息以算法地分配。例如,奇数编号的卡可增加或减少2,而偶数编号的卡可增加或减少5。在一些示例中,更新也可以在顺序读取中变化,使得一张卡可以以1、3、5、2、2...的重复而依次递增。特定序列或算法序列可以在个性化时定义,或者基于从唯一标识符派生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概括。

[0130] 认证消息可以作为十六进制ASCII格式记录的文本NDEF的内容传递。在一些示例中,可以仅包括认证数据和认证数据的MAC之后的8字节随机数。在一些示例中,随机数可以在密码A之前并且可以是一个块长。在其他示例中,对随机数的长度可能没有限制。在进一步的示例中,总数据(即,随机数加上密码)可以是块大小的倍数。在这些示例中,可以添加额外8字节块以匹配由MAC算法产生的块。作为另一示例,如果所采用的算法使用了16字节块,则甚至可以使用该块大小的倍数,或者可以自动或手动将输出填充为该块大小的倍数。

[0131] 可以通过功能密钥(AUT-Session-Key)935来执行MAC。密码中指定的数据可以用javacard.signature方法进行处理:ALG_DES_MAC8_ISO9797_1_M2_ALG3,以与EMV ARQC验证方法相关。如上所述,用于该计算的密钥可以包括会话密钥AUT-Session-Key 935。如上所述,计数器的低位两个字节可用于使一个或多个MAC会话密钥多样化。如下所述,AUT-Session-Key 935可以用于MAC数据950,并且可以使用DEK-Session-Key 940对结果数据或密码A 955和随机数RND进行加密,以创建密码B或以消息发送的输出960。

[0132] 在一些示例中,可以处理一个或多个HSM命令以进行解密,以使得最后的16个(二进制,32个十六进制)字节可以包括使用CBC模式的3DES对称加密,其中随机数为零IV,然后是MAC认证数据。用于此加密的密钥可以包括从Card-Key-DEK 930派生的会话密钥DEK-Session-Key 940。在这种情况下,用于会话密钥派生的ATC值是计数器pATC945的最低有效字节。

[0133] 以下格式表示二进制版本示例实施例。此外,在一些示例中,第一字节可以被设置为ASCII'A'。

[0134]

消息格式				
1	2	4	8	8
0x43 (消息类型‘A’)	版本	pATC	RND	密码 A (MAC)
密码 A (MAC)	**8 字节**			
MAC of				
2	8	4	4	18 字节输入
版本	pUID	pATC	共享机密	

[0135]

消息格式			
1	2	4	16
0x43 (消息类型‘A’)	版本	pATC	密码 B

[0136]

密码 A (MAC)	**8 字节**			
MAC of				
2	8	4	4	18 字节输入数据
版本	pUID	pATC	共享机密	
密码 B	**16**			
Sym 加密 of				
8	8			
RND	密码 A			

[0137] 另一示例性格式如下所示。在该示例中,标签可以以十六进制格式编码。

[0138]

消息格式				
2	8	4	8	8
版本	pUID	pATC	RND	密 码 A (MAC)

[0139]

8 字节				
8	8	4	4	18 字节输入数据
pUID	pUID	pATC	共享机密	

消息格式			
2	8	4	16
版本	pUID	pATC	密码 B

8 字节			

8		4	4	18 字节输入数据
pUID	pUID	pATC	共享机密	

密码 B	**16**		
Sym 加密 of			

8	8		
RND	密码 A		

[0140] 可以提取接收到的消息的UID字段,以从主密钥Iss-Key-AUTH 905和Iss-Key-DEK 910派生卡主密钥(Card-Key-Auth 925和Card-Key-DEK 930)以用于该特定卡。通过使用卡主密钥(Card-Key-Auth 925和Card-Key-DEK 930),接收到的消息的计数器(pATC)字段可用于派生会话密钥(Aut-Session-Key 935和DEK-Session-Key 940)以用于该特定卡。可以使用DEK-Session-KEY解密密码B 960,这产生了密码A 955和RND,并且RND可以被丢弃。UID字段可用于查找非接触式卡的共享机密(shared secret),其连同消息的Ver、LTD和pATC字段一起,可使用重新创建的Aut-Session-Key通过密码MAC来处理,以创建MAC输出,诸如MAC'。如果MAC'与密码A 955相同,则表明消息解密和MAC检查均已通过。然后,可以读取

pATC以确定其是否有效。

[0141] 在认证会话期间,一个或多个应用可以生成一个或多个密码。例如,可以经由一个或多个会话密钥(例如Aut-Session-Key 935)使用具有方法2填充的ISO 9797-1算法3而将一个或多个密码生成为3DES MAC。输入数据950可以采用以下形式:版本(2),pETID(8),pATC(4),共享机密(4)。在一些示例中,括号中的数字可以包括以字节为单位的长度。在一些示例中,共享机密可以由一个或多个随机数生成器生成,该随机数生成器可以被配置为通过一个或多个安全过程来确保该随机数是不可预测的。在一些示例中,共享机密可以包括在认证服务已知的个性化时间注入到卡中的随机的4字节二进制数。在认证会话期间,可能不会从一个或多个小应用程序向移动应用程序提供共享机密。方法2填充可包括在输入数据的末尾添加强制的0x'80'字节、及0x'00'字节,其可被添加到结果数据的末尾直到8字节边界。所得密码可以包括8个字节的长度。

[0142] 在一些示例中,使用MAC密码将未共享的随机数作为第一块进行加密的一个益处是,在使用对称加密算法的CBC(块链接)模式时它充当初始化向量。这允许块之间的"加扰"而不必预先建立固定的或动态的IV。

[0143] 通过将应用交易计数器(pATC)作为MAC密码中包含的数据的一部分包括在内,认证服务可以配置为确定清除数据中传达的值是否已被篡改。此外,通过将版本包括在一个或多个密码中,攻击者很难以尝试降低密码解决方案的强度的方式有目的地错篡改应用版本。在一些示例中,pATC可以从零开始并且每次一个或多个应用生成认证数据时以1更新。认证服务可以配置为跟踪在认证会话期间使用的pATC。在一些示例中,当认证数据使用等于或小于由认证服务接收到的先前值的pATC时,这可以被解释为重放旧消息的尝试,并且被认证的可以被拒绝。在一些示例中,如果pATC大于先前收到的值,则可以对其进行评估以确定它是否在可接受的范围或阈值之内,并且如果它超出该范围或阈值或者在其之外,则可以认为验证失败或不可靠。在MAC操作936中,通过MAC使用Aut-Session-Key 935处理数据950,以产生经加密的MAC输出(密码A)955。

[0144] 为了提供抵抗暴露于卡上的密钥的蛮力攻击的额外保护,期望对MAC密码955进行加密。在一些示例中,要包括在密文中的数据或密码A 955可以包括:随机数(8),密码(8)。在一些示例中,括号中的数字可以包括以字节为单位的长度。在一些示例中,随机数可以由一个或多个随机数生成器生成,该随机数生成器可以被配置为通过一个或多个安全过程来确保该随机数是不可预测的。用于加密该数据的密钥可以包括会话密钥。例如,会话密钥可以包括DEK-Session-Key 940。在加密操作941中,使用DEK-Session-Key 940处理数据或密码A 955和RND,以生成经加密的数据,密码B 960。可以使用3DES在密码块链接模式下对数据955进行加密,以确保攻击者必须对所有密文进行任何攻击。作为非限制性示例,可以使用其他算法,例如高级加密标准(AES)。在一些示例中,可以使用0x'0000000000000000'的初始化向量。试图蛮力攻击用于加密此数据的密钥的任何攻击者都将无法确定何时使用了正确的密钥,因为正确解密的数据将由于其随机出现而与错误解密的数据区是不能区分的。

[0145] 为了使认证服务能够验证由一个或多个小应用程序提供的一个或多个密码,必须在认证会话期间将以下数据从一个或多个小应用程序中以明文(in the clear)递送到移动设备:版本号,期用于确定所用的加密方法和消息格式以验证密码,这使该方法将来可以

更改;pUID,其用于检索密码资产并派生卡密钥;和pATC,其用于派生用于密码的会话密钥。

[0146] 图10示出了用于生成密码的方法1000。例如,在框1010,可以使用网络简档记录ID(pNPR)和派生密钥索引(pDKI)来标识在加密过程中使用哪个发行者主密钥进行认证。在一些示例中,该方法可以包括执行认证以在认证时检索非接触式卡的pNPR和pDKI的值。

[0147] 在框1020,可以通过将发行者主密钥与卡的唯一ID号(pUID)和一个或多个小应用程序(例如支付小应用程序)的PAN序列号(PSN)组合来使发行者主密钥多样化。

[0148] 在框1030,可以通过使发行者主密钥多样化以生成可用于生成MAC密码的会话密钥来创建Card-Key-Auth和Card-Key-DEK(唯一卡密钥)。

[0149] 在框1040,用于生成密码并加密一个或多个小应用程序中的数据的密钥可以包括:基于卡唯一密钥(Card-Key-Auth和Card-Key-DEK)的框1030的会话密钥。在一些示例中,这些会话密钥可以由一个或多个小应用程序生成并通过使用pATC派生,从而导致会话密钥Aut-Session-Key和DEK-Session-Key。

[0150] 图11描绘了根据一个示例的示出密钥多样化的示例性过程1100。最初,可以为发送者和接收者提供两个不同的主密钥。例如,第一主密钥可以包括数据加密主密钥,第二主密钥可以包括数据完整性主密钥。发送者具有计数器值,该计数器值可以在框1110处更新,以及其他数据,例如要保护的数据,其可以确保与接收者共享。

[0151] 在框1120,计数器值可以由发送者使用数据加密主密钥来加密以产生数据加密派生的会话密钥,并且计数器值也可以由发送者使用数据完整性主密钥来加密以产生数据完整性派生的会话密钥。在一些示例中,可以在两个加密期间使用整个计数器值或计数器值的一部分。

[0152] 在一些示例中,计数器值可能未加密。在这些示例中,计数器可以在明文即没有加密的情况下在发送者和接收者之间发送。

[0153] 在框1130,发送者使用数据完整性会话密钥和密码MAC算法通过密码MAC操作来处理要保护的数据。可以使用会话密钥(AUT-Session-Key)之一将受保护的数据(包括纯文本和共享机密)用于生成MAC。

[0154] 在框1140,可以由发送者使用数据加密派生的会话密钥结合对称加密算法对要保护的数据进行加密。在一些示例中,MAC与相等数量的随机数据(例如,每个8字节长)组合在一起,然后使用第二个会话密钥(DEK-Session-Key)进行加密。

[0155] 在框1150,将经加密的MAC从发送者发送到接收者,其具有足够信息以标识额外机密信息(例如共享机密,主密钥等),以验证密码。

[0156] 在框1160,接收者使用接收到的计数器值来从两个主密钥独立地派生出两个派生的会话密钥,如上所述的那样。

[0157] 在框1170,将数据加密派生的会话密钥与对称解密操作结合使用以解密受保护的数据。然后将发生对交换的数据的额外处理。在一些示例中,在提取MAC之后,期望再现并匹配MAC。例如,当验证密码时,可以使用适当生成的会话密钥将其解密。可以重建受保护的数据以进行验证。可以使用适当生成的会话密钥来执行MAC操作,以确定其是否与被解密的MAC相匹配。由于MAC操作是不可逆的过程,因此验证的唯一方法是尝试从源数据重新创建它。

[0158] 在框1180,将数据完整性派生的会话密钥与密码MAC操作结合使用以验证受保护

的数据尚未被修改。

[0159] 在当满足以下条件时，本文描述的方法的一些示例可以有利地确认何时确定出成功的认证。首先，验证MAC的能力表明派生的会话密钥是正确的。仅当解密成功并产生正确的MAC值时，MAC才是正确的。成功的解密可以表明正确派生的加密密钥已用于解密经加密的MAC。由于派生的会话密钥是使用仅对发送者(例如，发送设备)和接收者(例如，接收设备)已知的主密钥创建的，因此可以相信最初创建MAC并对MAC加密的非接触式卡确实是可信的。而且，用于派生第一会话密钥和第二会话密钥的计数器值可以被示出为有效的并且可以用于执行认证操作。

[0160] 此后，可以丢弃两个派生的会话密钥，并且数据交换的下一次迭代将更新计数器值(返回到框1110)，并且可以创建新的会话密钥集(在框1120)。在一些示例中，组合的随机数据可以被丢弃。

[0161] 本文描述的系统和方法的示例实施例可以被配置为提供安全因素认证。安全因素认证可以包括多个过程。作为安全因素认证的一部分，第一过程可以包括经由在设备上执行的一个或多个应用来登录并验证用户。作为第二过程，响应于经由一个或多个应用对第一过程的成功登录和验证，用户可以参与与一个或多个非接触式卡相关联的一个或多个行为。实际上，安全因素认证可以包括安全地证明用户的身份以及参与与非接触式卡相关联的一种或多种类型的行为，包括但不限于一种或多种轻拍姿势。在一些示例中，一个或多个轻拍姿势可以包括用户对设备的非接触式卡轻拍。在一些示例中，该设备可以包括移动设备，电脑亭(kiosk)，终端，平板电脑或被配置为处理接收到的轻拍姿势的任何其他设备。

[0162] 在一些示例中，非接触式卡可以向着诸如一个或多个电脑亭或终端之类的设备轻拍，以验证身份以便接收响应于购买(诸如咖啡)的交易项目。通过使用非接触式卡，可以建立一种在忠诚度计划中证明身份的安全方法。以与仅扫描条形卡不同的方式来建立安全地证明身份以例如获得奖励、优惠券、要约等，或收益的接收。例如，非接触式卡和设备之间可能发生加密交易，该交易可以配置为处理一个或多个轻拍姿势。如上所述，一个或多个应用可以被配置为验证用户的身份，然后例如经由一个或多个轻拍姿势使用户动作或响应它。在一些示例中，可以将诸如消费积分、忠诚度积分、奖励积分、医疗保健信息等的数据写回到非接触式卡。

[0163] 在一些示例中，非接触式卡可以向着诸如移动设备的设备轻拍。如上所述，可以通过一个或多个应用来验证用户的身份，该一个或多个应用然后将基于对身份的验证来向用户授予期望的利益。

[0164] 在一些示例中，非接触式卡可以通过轻拍诸如移动设备之类的设备来激活。例如，非接触式卡可以通过NFC通信经由设备的卡读取器与设备的应用进行通信。其中靠近设备的卡读取器轻拍卡的通信可以允许设备的应用读取与非接触式卡相关联的数据并激活卡。在一些示例中，激活可以授权卡用于执行其他功能，例如购买、访问帐户或受限信息或其他功能。在一些示例中，轻拍可以激活或启动设备的应用，然后发起一个或多个动作或与一个或多个服务器的通信以激活非接触式卡。如果应用未安装在设备上，则靠近卡读取器轻拍非接触式卡可以发起应用的下载，例如导航至应用的下载页面。在安装之后，轻拍非接触式卡可以激活或启动应用，然后例如经由应用或其他后端通信来发起非接触式卡的激活。在激活之后，非接触式卡可以用于各种活动，包括但不限于商业交易。

[0165] 在一些实施例中，专用应用可以被配置为在客户端设备上执行以执行非接触式卡的激活。在其他实施例中，网络门户，基于网络的应用，小应用程序等可以执行激活。激活可以在客户端设备上执行，或者客户端设备可以仅充当非接触式卡和外部设备(例如，账户服务器)之间的通道。根据一些实施例，在提供激活时，应用可以向账户服务器指示执行激活的设备的类型(例如，个人计算机，智能电话，平板电脑或销售点(POS)设备)。此外，取决于所涉及的设备的类型，应用可以向账户服务器输出不同和/或额外的数据以进行传输。例如，这样的数据可以包括与商人相关联的信息，例如商人类型，商人ID，以及与设备类型本身相关联的信息诸如POS数据和POS ID。

[0166] 在一些实施例中，示例认证通信协议可以模仿EMV标准的离线动态数据认证协议，其通常在交易卡和销售点设备之间执行，具有一些修改。例如，由于示例认证协议本身并未用于完成与发卡行者/支付处理器的支付交易，因此不需要某些数据值，并且可以执行认证而无需涉及到发卡行者/支付处理器的实时在线连接。如本领域中已知的，销售点(POS)系统向卡发行者提交包括交易值的交易。发行者是批准还是拒绝交易可以基于卡发行者是否识别出交易值。同时，在本公开的某些实施例中，源自移动设备的交易缺乏与POS系统相关联的交易值。因此，在一些实施例中，可以将虚拟交易值(即，卡发行者可识别的值并且足以允许发生激活)作为示例认证通信协议的一部分来传递。基于POS的交易还可基于交易尝试的次数(例如，交易计数器)拒绝交易。超出缓冲值的尝试次数可能会导致软拒绝(soft decline)；该软拒绝在接受交易之前需要进一步验证。在一些实施方式中，可以修改交易计数器的缓冲值以避免拒绝合法交易。

[0167] 在一些示例中，非接触式卡可以根据接收者设备选择性地传送信息。一旦轻拍，非接触式卡就可以识别该轻拍所指向的设备，并且基于该识别，非接触式卡可以为该设备提供适当的数据。有利地，这允许非接触式卡仅发送完成即时动作或交易所需的信息，例如支付或卡认证。通过限制数据的传输并避免不必要的数据的传输，可以提高效率和数据安全性。信息的识别和选择性通信可以应用于各种情况，包括卡激活、余额转移、帐户访问尝试、商业交易和减少欺诈。

[0168] 如果将非接触式卡的轻拍引导到运行Apple iOS®操作系统的设备(例如iPhone，iPod或iPad)，则非接触式卡可以识别iOS®操作系统并发送适当的数据数据以与此设备进行通信。例如，非接触式卡可以经由例如NFC使用NDEF标签来提供认证卡所需的加密身份信息。同样，如果将非接触式卡的轻拍引导到运行Android®操作系统的设备(例如Android®智能手机或平板电脑)，则非接触式卡可以识别Android®操作系统并发送适当的数据以与该设备进行通信(例如通过此处描述的方法的认证所需的加密身份信息)。

[0169] 作为另一示例，非接触式卡的轻拍可以被引导到POS设备，该POS设备包括但不限于电脑亭，结帐台，支付站或其他终端。在执行轻拍时，非接触式卡可以识别POS设备并仅发送动作或交易所需的信息。例如，在识别出用于完成商业交易的POS设备后，非接触式卡可以传送在EMV标准下完成交易所需的支付信息。

[0170] 在一些示例中，参与交易的POS设备可以要求或指定要由非接触式卡提供的附加信息，例如，设备特定信息，位置特定信息和交易特定信息。例如，一旦POS设备从非接触式卡接收到数据通信，则POS设备可以识别非接触式卡并请求完成动作或交易所需的附加信

息。

[0171] 在一些示例中，POS设备可以隶属于熟悉某些非接触式卡或习惯于执行某些非接触式卡交易的授权商人或其他实体。但是，应当理解，执行所描述的方法不需要这种从属关系。

[0172] 在一些示例中，例如购物店，杂货店，便利店等，可以在不必打开应用的情况下将非接触式卡向移动设备轻拍，以指示利用奖励点数、忠诚度点数、优惠券、优惠等中的一种或多种以涵盖一次或多次购买的愿望或意图。因此，提供了购买背后的意图。

[0173] 在一些示例中，一个或多个应用可以被配置为确定：其是通过非接触式卡的一个或多个轻拍姿势启动的，使得启动发生在下午3:51，交易在下午3:56处理或发生，以验证用户身份。

[0174] 在一些示例中，一个或多个应用可以被配置为响应于一个或多个轻拍姿势来控制一个或多个动作。例如，一个或多个动作可以包括收集奖励、收集积分、确定最重要的购买，确定成本最低的购买和/或实时地重新配置为另一动作。

[0175] 在一些示例中，可以收集关于轻拍行为的数据作为生物统计/姿势认证。例如，可以将加密上安全的并且不容易被拦截的唯一标识符发送到一个或多个后端服务。可以将唯一标识符配置为查找有关个人的辅助信息。次要信息可以包括关于用户的个人可识别信息。在一些示例中，辅助信息可以存储在非接触式卡内。

[0176] 在一些示例中，该设备可以包括在多个个人之间分割账单或检查付款的应用。例如，每个人都可以拥有非接触式卡，并且可以是同一发行金融机构的客户，但这不是必需的。这些人中的每个人都可以通过应用在其设备上收到推送通知，以拆分购买。不是仅接受一个卡的轻拍来指示付款，而是可以使用其他非接触式卡。在一些示例中，具有不同金融机构的个人可以拥有非接触式卡，以提供信息以发起来自对卡进行轻拍的个人的一个或多个支付请求。

[0177] 以下示例用例描述了本公开的特定实现的示例。这些仅用于说明目的，而不是为了限制。在一种情况下，第一位朋友(付款人)欠第二位朋友(收款人)一笔钱。付款人希望使用非接触式卡通过收款人的智能手机(或其他设备)付款，而不是去ATM或要求通过对等应用进行交换。收款人在其智能手机上登录到适当的应用，然后选择付款请求选项。作为回应，该应用经由收款人的非接触式卡请求认证。例如，应用输出一个显示，以请求收款人轻拍其非接触式卡。一旦收款人在应用被启用的其智能手机的屏幕上轻拍其非接触式卡，便读取并验证非接触式卡。接下来，该应用为付款人显示轻拍其非接触式卡进行付款的提示。付款人轻拍其非接触式卡后，应用将读取卡信息，并通过关联的处理器将付款请求发送给付款人的卡发行者。卡发行者处理交易并将交易的状态指示符发送到智能手机。然后，应用输出以显示交易的状态指示符。

[0178] 在另一示例情况下，信用卡客户可以在邮件中接收新的信用卡(或借记卡，其他支付卡或任何其他需要激活的卡)。客户可以决定通过他或她的设备(例如，诸如智能手机之类的移动设备)上的应用来激活卡，而不是通过拨打与卡发行者相关联的提供的电话号码或访问网站来激活卡。客户可以从设备显示屏上显示的应用菜单中选择卡激活功能。该应用可提示客户在屏幕上轻拍其信用卡。在设备屏幕上轻拍信用卡后，应用可以配置为与服务器进行通信，诸如激活客户的卡的卡发行者服务器。然后，该应用可以显示指示卡成功激

活的消息。然后卡的激活将完成。

[0179] 图12示出了根据示例实施例的用于卡激活的方法1200。例如，卡激活可以通过包括卡、设备和一个或多个服务器的系统来完成。非接触式卡、设备和一个或多个服务器可以指代参照上面图1A、图1B、图5A和图5B先前解释的相同或相似的组件，诸如非接触式卡105、客户端设备110和服务器120。

[0180] 在框1210中，卡可以被配置为动态生成数据。在一些示例中，该数据可以包括诸如帐号、卡标识符、卡验证值或电话号码之类的信息，该信息可以从卡发送到设备。在一些示例中，可以经由本文公开的系统和方法来加密数据的一个或多个部分。

[0181] 在框1220中，可以经由NFC或其他无线通信将动态生成的数据的一个或多个部分传送到设备的应用。例如，卡靠近设备的轻拍可以允许设备的应用读取与非接触式卡相关联的数据的一个或多个部分。在一些示例中，如果设备不包括用于辅助卡的激活的应用，则卡的轻拍可以引导设备或提示用户到软件应用商店以下载相关联的应用以激活卡。在一些示例中，可以提示用户将卡朝向设备的表面充分地表现姿势、放置或定向，例如以一定角度或平坦地放置在设备的表面上、放置在其附近或靠近其放置。响应于卡的充分的表现姿势、放置和/或定向，设备可以继续将从卡接收的数据的一个或多个加密部分发送到一个或多个服务器。

[0182] 在框1230中，可以将数据的一个或多个部分传送到一个或多个服务器，例如卡发行者服务器。例如，可以将数据的一个或多个加密部分从设备发送到卡发行者服务器以激活卡。

[0183] 在框1240中，一个或多个服务器可以经由本文公开的系统和方法对数据的一个或多个加密部分进行解密。例如，一个或多个服务器可以从设备接收经加密的数据，并且可以对其进行解密，以便将接收到的数据与一个或多个服务器可访问的记录数据进行比较。如果由一个或多个服务器对数据的一个或多个解密部分进行的比较结果得出成功匹配，则可以激活卡。如果由一个或多个服务器对数据的一个或多个解密部分进行的比较结果得出不成功匹配，则可能会发生一个或多个过程。例如，响应于对不成功匹配的确定，可以提示用户再次轻拍卡、刷卡或挥动卡。在这种情况下，可以存在预定阈值，该预定阈值包括允许用户激活卡的尝试次数。可替代地，用户可以接收一个通知，诸如在他或她的设备上指示未成功尝试卡验证的消息并且呼叫、发送电子邮件或发短信给相关服务以协助激活卡；或另一通知，诸如在他或她的设备上指示未成功尝试卡验证的电话呼叫并且呼叫、发送电子邮件或发短信给相关服务以协助激活卡；或另一通知，诸如指示未成功尝试卡验证的电子邮件并且呼叫、发送电子邮件或发短信给相关服务以协助激活该卡。

[0184] 在框1250中，一个或多个服务器可以基于卡的成功激活来发送返回消息。例如，该设备可以被配置为从一个或多个服务器接收指示出该一个或多个服务器成功激活卡的输出。该设备可以被配置为显示指示卡成功激活的消息。一旦激活了卡，就可以将卡配置为断开动态生成数据，从而避免欺诈性使用。以此方式，此后可以不激活卡，并且向一个或多个服务器通知该卡已经被激活。

[0185] 在另一示例情况下，客户想要在他或她的移动电话上访问他的财务帐户。客户在移动设备上启动应用(例如，银行应用程序)并输入用户名和密码。在此阶段，客户可以看到第一级帐户信息(例如，最近购买的商品)，并且能够执行第一级帐户选项(例如，支付信用

卡)。但是,如果用户尝试访问第二级帐户信息(例如支出限额)或执行第二级帐户选项(例如转移到外部系统),则他必须具有第二级认证。因此,应用请求用户提供用于账户验证的交易卡(例如,信用卡)。然后,用户向移动设备轻拍其信用卡,应用将验证该信用卡是否与该用户的帐户相对应。此后,用户可以查看第二级帐户数据和/或执行第二级帐户功能。

[0186] 在一些示例中,可能要求用户在使用应用、利用应用或设备的增强或受限特征、查看敏感信息或采取某些动作之前确认他或她的身份。如本文所述的诸如非接触式卡的发送设备可以被用作确认用户身份并访问这些特征的装置。敏感信息的示例包括但不限于学术信息、财务信息、历史信息、医疗信息和技术信息。受限特征的示例包括但不限于访问或修改敏感信息,生成附加的敏感信息,购买、出售或转让资产或敏感信息,以及销毁或以其他方式处置资产或敏感信息。

[0187] 用户可以通过例如经由发送设备提供用户标识来确认他或她的身份。用户标识可以包括不广为人知的与用户有关的某些信息。用户标识信息的示例包括但不限于用户的出生日期、家庭地址、工作地址、电话号码、信用卡号码、银行帐号、帐单邮政编码、安全号码、密码、生物标识信息(例如,面部、视网膜或指纹扫描、语音识别)、个人标识号、与发送设备相关的标识信息(例如,唯一标识号、算法确定值、计数器值)或其组合。用户标识可以由发送设备通过本文描述的方法发送,并且可以在传输之前加密。

[0188] 例如,用户可能希望使用与具有本文所述的通信和加密功能的非接触式卡或其他发送设备相关联的增强安全特征来保护他或她的个人的、财务的、医疗的或其他敏感信息。用户可以建立安全特征,该安全特征在执行较高风险或其他敏感操作之前需要身份认证,这些操作包括但不限于:从帐户中转出钱或贷款(例如,从ATM提取现金)、修改联系信息、编辑密码或更改布局位置。其他敏感操作可以包括但不限于允许访问或传送个人数据、医疗数据和/或财务数据。用户可以在执行某些敏感操作之前登录应用并建立要求身份认证的所需安全特征。当用户希望执行这样的操作时,她可以通过用他或她的非接触式卡、智能手机或接收设备附近的其他发送设备轻拍或以其他方式打手势来认证她的身份。接收设备可以检测发送设备的使用,并使用此处描述的通信和加密功能来认证用户的身份。一旦用户身份已被认证,并且认证已从接收设备传送到应用,则可以允许访问敏感信息或执行所需的敏感操作。

[0189] 在一些示例中,非接触式卡可以与终端、电脑亭、接收设备和/或移动设备一起使用,以将保险数据传送给医生、医务人员、支持人员和/或计费代理。在一些示例中,传送保险信息有助于计费操作并向用户计费适当的金额。在一些示例中,传送保险信息有助于帐单和/或发票的准备,该帐单和/或发票可以根据应用于用户的保险范围的特定类型和/或数量而变化。

[0190] 在一些示例中,用户可以在移动设备上执行应用,该应用通过服务器和与医疗提供者相关联的计费和/或账单应用进行通信。用户可以使用非接触式卡向在移动设备上运行的应用认证其身份。然后,移动设备可以将用户的保险信息传送到医疗提供商,以用于计费目的。

[0191] 图13示出了用户访问应用的一个或多个受限特征或使用该应用访问敏感信息的方法1300。方法1300可以在用户已经通过本文描述的方法认证他或她的发送设备之前或之后执行。方法1300在框1310处开始,用户访问应用或热线。该应用可以被安装在接收设备

(例如本文所述的启用网络的计算机或移动设备)上,和/或由该接收设备执行。

[0192] 在框1320处,在继续利用应用的增强特征之前或在访问敏感信息之前,应用或热线请求用户认证他或她的身份。在框1330处,用户将具有本文所述的通信和加密功能的发送设备移动到接收设备附近。在框1340处,接收设备认证用户标识。在框1350处,接收设备将用户认证的标识传送到应用。在框1360处,应用允许用户利用应用的增强特征或访问敏感信息。在一些示例中,用户可用的增强特征和敏感信息将基于与用户经认证的身份相关联的用户信息而变化。

[0193] 在另一个示例中,用户可能希望认证他或她的身份,以便发起与客户服务代理的安全聊天或呼叫。在这种情况下,安全地认证用户的身份可以允许用户向代理商提供对他或她的个人信息、帐户信息、交易历史记录、通话历史记录、以前的记录和/或其他信息的访问,而无需代理商独立地验证用户身份。在一些示例中,用户可以呼叫或以其他方式联系代理商,并且代理商可以使用具有本文所述的通信和加密功能的发送设备和接收设备来请求用户认证他或她的身份。用户可以在接收设备附近对发送设备进行轻拍、滑动、挥动或执行任何手势或其组合。接收设备可以向代理商和/或代理商正在使用的应用传送用户已认证他或她的身份,并允许代理商访问用户的信息。在一些示例中,这将节省用户向一个或多个代理商提供他或她的出生日期、地址、密码、社会保险号和/或其他标识信息的时间。在一些示例中,这可以节省时间并为用户的敏感信息提供更大的保护,因为不需要将这些信息提供给人类代理商。

[0194] 在一些示例中,在完全连接到代理商之前,应用可以要求用户认证他或她的身份作为第一步。在一些示例中,应用可以最初基于用户经认证的身份将用户定向到特定的代理商或代理商类别。在一些示例中,用户经认证的身份可与等级、类别或积分系统相关联,该等级、类别或积分系统可赋予用户某些利益,诸如例如,更快地访问代理商、访问具有一定经验水平的代理商、访问具有一定质量等级的代理商、访问具有一定增强授权的代理商。这样的授权可以包括,例如,向用户退款或贷款某些美元值的授权,向用户提供某些高级特征或利益的授权,免除某些收费或费用的授权,续订、协商和/或修改合同或其他协议的授权,提供免费或减价运输的授权,和/或向用户提供附加或优质服务的授权。

[0195] 图14描绘了根据示例实施例的用户基于用户使用诸如非接触式卡之类的发送设备来认证他或她的身份而联系客户支持并接收不同服务的方法1400。方法1400在框1410处开始,其中用户访问客户支持应用和/或拨打客户支持热线。该应用可以被安装在接收设备(例如本文所述的启用网络的计算机或移动设备)上,和/或由接收设备执行,并且热线可以通过蜂窝电话或陆线电话、启用互联网协议的语音设备或其他电话通信装置访问。在一些示例中,热线可以经由人类操作员、录音操作员、语音聊天代理商或其他音频通信装置与用户通信,并且用户与热线的交互可以包括与安装在接收设备上的应用的互动。

[0196] 在框1420处,应用或热线请求用户认证他或她的身份。在框1430处,用户将发送设备例如非接触式卡移动到接收设备附近。在框1440处,接收设备对用户的标识进行认证。在框1450处,接收设备将用户经认证的标识传送到应用或热线。

[0197] 在接收到用户经认证的标识之后,应用或热线可以继续进行框1460、1470或1480中的任何一个。在框1460处,应用或热线向人类操作员提供用户的帐户信息,从而节省用户将该信息转发给操作员的时间。在框1470处,应用或热线基于与用户身份相关联的用户信

息(例如等级)而将用户的呼叫路由到特定类别的人类操作员。在框1480中,应用或热线基于与用户身份相关联的用户信息(例如交易历史)而将用户的呼叫路由到第一可用的人类操作员,从而允许优选客户避免排队等候。

[0198] 在一些示例中,用户可能希望使用具有本文所述的通信和加密功能的发送设备以及与该应用进行通信的接收设备来向应用提供信息。在这样的示例中,用户的信息可以记录在发送设备和/或接收设备上。此类信息可以包括但不限于用户的姓名、生日、家庭地址、工作地址、电话号码、信用卡号码、银行帐号、帐单邮政编码、安全号码、密码和/或偏好。当提示提供此类信息时,用户可以对具有本文所述通信和加密功能的非接触式卡、智能手机或其他发送设备进行轻拍、滑动、挥动或执行任何手势或其组合,以将他或她的身份认证到接收设备。这可以将信息从发送设备传送到接收设备和/或授权接收设备将用户的信息传送给应用,从而减少或消除了用户手动输入他或她的信息的需求,并创建了更安全的数据传输。

[0199] 在一些示例中,应用可以记录与用户的身份认证行为有关的信息。这样的信息可以包括例如认证时间、认证位置、所使用的发送设备的类型、所使用的单独的发送设备、所使用的接收设备的类型、所使用的单独的接收设备和/或与用于身份认证进行的移动或轻拍、滑动、挥动或执行任何手势或其组合的定时相关的信息。在一些示例中,可以对记录的信息进行分析,以便开发用户的行为简档。这样的简档可以用于检测潜在的欺诈指示符。此类指示符可以包括用户建立的行为简档之外的行为。在一些示例中,可以在确定活动为欺诈性或潜在欺诈性之前确定预定变化量。在一些示例中,可接受的行为变化量可以基于在用户的行为简档中检测到的变化量。可以使用这种示例,以便当与使用多个发送设备从多个位置频繁地认证他或她的身份的用户相比时,设置较低变化阈值,以用于检测具有使用特定的非接触式卡仅从她家认证他或她的身份的长期建立的记录的用户的潜在欺诈性活动。在一些示例中,可以使用人工智能或机器学习技术来分析用户的行为信息,以便建立简档模式以及这些模式中的可变性程度。

[0200] 在一些示例中,用户的行为简档可以包括与应用或要求身份认证信息的应用类型有关的信息。该信息可用于向用户提供目标广告、特征、内容或其他利益。在一些示例中,如果用户将具有本文所述的通信和加密功能的非接触式卡用于游戏应用,则可以向该用户提供与以下有关的附加内容:游戏、用户玩的特定游戏或提供与游戏有关的产品或服务的业务。在一些示例中,如果用户将具有本文所述的通信和加密功能的非接触式卡用于旅行应用,则基于用户的行为简档可以向该用户提供与以下有关的附加内容:旅行、该用户可能感兴趣的目的地、旅馆、水疗中心、景点或提供与旅行有关的产品或服务或位于用户可能感兴趣的特定目的地的其他业务。

[0201] 在一些示例中,在访问敏感信息或执行敏感操作之前,作为多步骤安全性过程的第一步,应用可以要求用户认证他或她的身份。在这样的示例中,在应用向用户发送密码或密码之前,应用可以要求用户使用具有本文所述的通信和加密功能的发送设备来认证他或她的身份。在一些示例中,在应用向用户的智能手机发送一次性的、有时间限制的密码之前,可能需要认证用户身份的步骤。在一些示例中,可以要求用户使用非接触式卡或非用户智能手机的其他发送设备来认证他或她的身份。在此类示例中,用户必须同时实际拥有用户的非接触式卡和用户的智能手机,才能从应用中生成并接收一次性使用密码。这种布置

可以通过要求多层安全性来帮助减少或防止欺诈性活动。在一些示例中，仅当应用检测到用户已建立的行为简档之外的活动时，才可以实现这种增强的安全特征。例如，如果应用检测到用户正试图访问来自不同国家的敏感数据，则应用可以要求用户执行多因素身份认证。

[0202] 在一些示例中，用户可能希望促进注册或登记过程。在一些示例中，用户可以使用具有此处所述的通信和加密功能的发送设备和接收设备，以便在旅馆、会议、餐馆、航空公司、机修工办公室、诊所、医院、牙医办公室或接受预订的任何其他位置处认证他或她的身份。在一些示例中，用户可以进入旅馆，并且在可能位于旅馆前台的接收设备附近对具有本文所述的通信和加密功能的发送设备进行轻拍、滑动、挥动或执行任何手势或其组合。接收设备可以向预订系统传送用户身份已认证，以便促进登记过程。在一些实施例中，接收设备可以与自动电脑亭通信，该自动电脑亭可以在接收到用户经认证的标识后发布房间密钥，而无需接待员参与。

[0203] 在一些实施例中，旅馆可以不发行单独的房间密钥，但是可以允许用户使用用户的发送设备访问房间。在这样的示例中，用户可以在配备有接收设备的电脑亭处使用他或她的智能手机来认证他或她的身份。在认证用户的身份后，旅馆可以更新其内部应用，从而允许用户使用他或她的智能手机在一定的时间段内访问特定房间，而无需单独的旅馆房间密钥。

[0204] 在一些实施例中，用户可以使用非接触式卡在房间访问终端(诸如例如，安装在门上的电子锁)上认证他或她的身份。在一些实施例中，用户可以使用与在移动设备上执行的应用通信的非接触式卡来认证他或她的身份。该应用可以直接与访问终端进行交互，也可以使用服务器与后端旅馆应用或数据库进行通信，以如本文所述在用户身份已经建立后，准许用户访问房间。

[0205] 在一些实施例中，当进行预订时，旅馆可以更新内部应用，从而允许用户使用被配置为认证用户身份的非接触式卡访问房间。在一些实施例中，用户可以使用非接触式卡直接与终端和/或其他旅馆设备对接以获取对房间的访问。

[0206] 在一些实施例中，用户可以在移动设备上执行应用，该移动设备通过服务器与旅馆的内部访问和控制系统进行通信。在一些实施例中，用户可以响应于来自移动设备上的应用的提示而对非接触式卡进行轻拍、滑动、挥动或执行任何手势或其组合，以便打开旅馆房间的门。用户的移动设备在使用非接触式卡确认用户的身份之后，可以向旅馆的内部访问和控制系统通知该用户已认证，从而使旅馆的访问和控制系统解锁或打开特定的门。

[0207] 在一些示例中，用户可能希望取消、改变或修改在旅馆的预订。在这样的示例中，旅馆的预订应用可以在允许访问预订信息或允许修改用户的预订之前，请求用户认证他或她的身份。

[0208] 在一些示例中，用户可能希望向旅馆、餐厅或其他地点的工作人员支付或给小费。在这样的示例中，用户可以预先安排一系列的手势来发起某些支付交易。用户可以轻拍由工作人员携带或以其他方式与工作人员相关联的接收设备，以便发起交易。在一些示例中，在交易发起之后，用户可以执行一个或一系列手势以向工作人员支付所需金额。在一个示例中，用户可以将发送设备轻拍到工作人员的接收设备，然后使用发送设备执行一系列横向扫描动作，其中每个横向扫描将一美元或其他货币单位转移给与接收设备相关联的工作

人员。在这样的示例中，用户可以基于所执行的横向扫除运动的次数，根据用户的意愿向工作人员支付或给小费或多或少。在其它示例中，用户可以预先安排发起转移特定金额的手势，例如，每个手势一美元、五美元或十美元。在这样的示例中，用户可以基于预先安排的手势的组合来向工作人员支付或给小费所需的金额。

[0209] 在一些示例中，用户可能希望访问安全物理位置，包括但不限于解锁储物柜、打开上锁的门或解锁保险箱。在这样的示例中，安全物理位置可以配备有接收设备，并且用户可以通过使用具有本文所述的通信和加密功能的发送设备来认证他或她的标识，从而能够访问安全位置。在这样的示例中，用户可以在接收设备附近对非接触式卡、智能手机或其他发送设备进行轻拍、滑动、挥动或执行任何手势或其组合。在认证用户标识之后，接收设备可以解锁安全位置。

[0210] 在一个示例中，用户可能希望解锁配备有接收设备的储物柜。用户可以在接收设备附近对具有本文所述通信和加密功能的非接触式卡或发送设备进行轻拍、滑动、挥动或执行任何手势或其组合，以便认证用户的身份。一旦认证了用户的身份，储物柜就可以打开。在另一示例中，一旦认证用户的身份，接收设备就可以向用户的智能手机或移动设备发送临时密码，从而允许用户通过输入该密码来解锁储物柜。在这种布置下，用户必须实际同时拥有与用户帐户相关联的智能手机或移动设备以及用于认证用户身份的非接触式卡或发送设备。在一些示例中，接收设备可以要求用户使用非接触式卡执行预定手势，从而创建访问储物柜所需的又一层安全性。

[0211] 在一些示例中，用户可以向受控物理位置的操作员提供被授权代表用户访问受控空间的其他个人的列表。在这样的示例中，用户的代理人可以对代理人的非接触式卡进行轻拍、滑动、挥动或执行任何手势或其组合，以便认证他或她作为用户经授权的代理人的身份。在一些示例中，在认证代理人的身份时，代理人可以被授权代表用户访问受控空间。在一些示例中，在认证代理人的身份时，接收设备可以向用户发送文本消息或其他通知，在允许代理人访问受控空间之前询问用户是否希望允许代理人访问受控空间。

[0212] 在某些安全位置，可能要求多个用户通过在接收设备附近在特定时间帧内或基本上同时对非接触式卡进行滑动、轻拍或打手势来认证他或她的身份。这样的示例可以防止任何一个单独的个体在没有其他必要的个体在场的情况下访问受控空间。

[0213] 在另一个示例中，用户可能希望访问已经配备有接收设备的车辆。在这样的示例中，用户可以在接收设备附近对具有本文所述通信和加密功能的非接触式卡或其他发送设备进行轻拍、滑动、挥动或执行任何手势或其组合，以便认证用户的身份并由此访问车辆。在一些示例中，在接收设备附近进行类似的轻拍、滑动、挥动或执行任何手势或其组合可以用来启动车辆的点火或以其它方式访问车辆的驾驶功能。在一些示例中，车辆或与车辆相关联的接收设备可以维护可以代表用户访问和/或操作车辆的经授权的代理人的列表。在一些示例中，可以向某些个体授权允许访问车辆，但不能驾驶或操作该车辆。例如，用户可以授予他或她的每个家庭成员通过对家庭成员的非接触式卡进行滑动、轻拍或打手势来访问车辆的能力，从而认证单个家庭成员的身份。但是，用户可能仅向他或她的配偶授予操作车辆的能力，从而尽管认证了用户孩子的标识，仍阻止用户孩子操作汽车。在一些实施例中，可以仅在某些天和/或时间内授予经授权代理人操作车辆的能力。如果用户有一个正在学习驾驶的十几岁的儿子，但用户不希望他的儿子在晚上开车，则该用户可以修改与儿子

的标识相关联的许可，使得儿子可以随时访问汽车，但是仅可以在晚上7:00之前操作汽车。在一些示例中，发送设备消除了使用单独的钥匙访问和/或操作车辆的必要性。

[0214] 在一些示例中，用户可能希望访问他或她的健康护理或医疗信息。由于此类信息的敏感性质，可能要求用户使用具有本文所述的通信和加密功能的非接触式卡来认证其身份。在这样的示例中，用户可以在接收设备附近对非接触式卡或其他发送设备进行轻拍、滑动、挥动或执行任何手势或其组合，以认证其身份。一旦用户向接收设备认证了他的身份，接收设备就可以将该信息传送给服务器，该服务器随后可以允许用户访问他的医疗信息。通过在授权访问医疗数据之前要求安全身份认证，医院、诊所、大学和其他组织可以减少允许未经授权访问医疗信息的可能性。此外，在一些示例中，患者能够从无人电脑亭访问其自己的医疗信息，从而允许更好地访问用户的信息，而无需附加的工作人员或记录保持人员。

[0215] 在整个说明书中，提到了各种帐户，例如银行帐户、信用卡帐户和借方帐户。然而，应当理解，本公开不限于特定的银行账户，并且可以包括任何金融账户，以及与娱乐、忠诚度计划、公用事业和其他服务有关的账户。

[0216] 在一些示例中，本公开涉及非接触式卡的轻拍。然而，应理解，本公开不限于轻拍，并且本公开包括其他姿势(例如，卡的挥动或其他运动)。

[0217] 在整个说明书和权利要求书中，除非上下文另外明确指出，否则以下术语至少具有本文明确关联的含义。术语“或”旨在表示包含性“或”。进一步地，术语“一”，“一个”和“该”旨在表示一个或多个，除非另有说明或从上下文中清楚地指向单数形式。

[0218] 在该描述中，已经阐述了许多具体细节。然而，应理解，可在没有这些具体细节的情况下实践所公开技术的实施方式。在其他情况下，未详细示出公知的方法，结构和技术，以免混淆对本说明书的理解。引用“一些示例”，“其他示例”，“一个示例”，“示例”，“各种示例”，“一个实施例”，“实施例”，“一些实施例”，“示例实施例”，“各种实施例”，“一个实施方式”，“实施方式”，“示例性实施方式”，“各种实施方式”，“一些实施方式”等表示所描述的所公开技术的实施方式可以包括特定的特征，结构、或特性，但并非每个实现都必须包括特定的特性、结构或特性。此外，尽管可以重复使用短语“在一个示例中”，“在一个实施例中”或“在一个实现方式中”，但不一定指相同的示例、实施例或实现方式。

[0219] 如本文所使用的，除非另有说明，否则使用序数形容词“第一”，“第二”，“第三”等来描述共同的对象，仅表示相似对象的不同实例被引用，而不是指意图暗示这样描述的对象必须在时间、空间、等级或任何其他方式上以给定的顺序。

[0220] 尽管已结合当前被认为是最实际和各种实施方式描述了所公开技术的某些实施方式，但是应当理解，所公开技术不限于所公开实施方式，相反，本公开旨在覆盖所附权利要求的范围内包括的各种修改和等效布置。尽管本文使用了特定术语，但是它们仅在一般和描述性意义上使用，而不是出于限制的目的。

[0221] 本书面描述使用示例来公开所公开技术的某些实施方式，包括最佳模式，并且还使本领域技术人员能够实践所公开技术的某些实施方式，包括制造和使用任何设备或系统以及执行所包括的任何方法。所公开技术的某些实现的可具专利性范围在权利要求中定义，并且可以包括本领域技术人员想到的其他示例。如果这样的其他示例具有与权利要求的字面语言没有不同的结构元件，或者如果它们包括与权利要求的字面语言没有实质性差异的等效结构元件，则它们意图在权利要求的范围内。

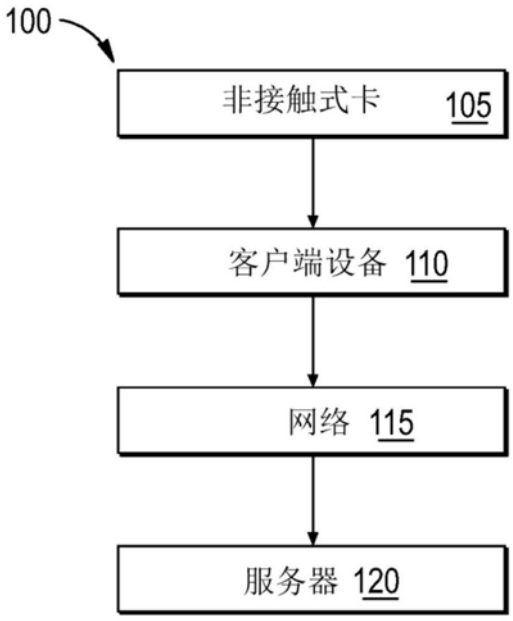

100
非接触式卡 105
客户端设备 110
网络 115
服务器 120

图1A

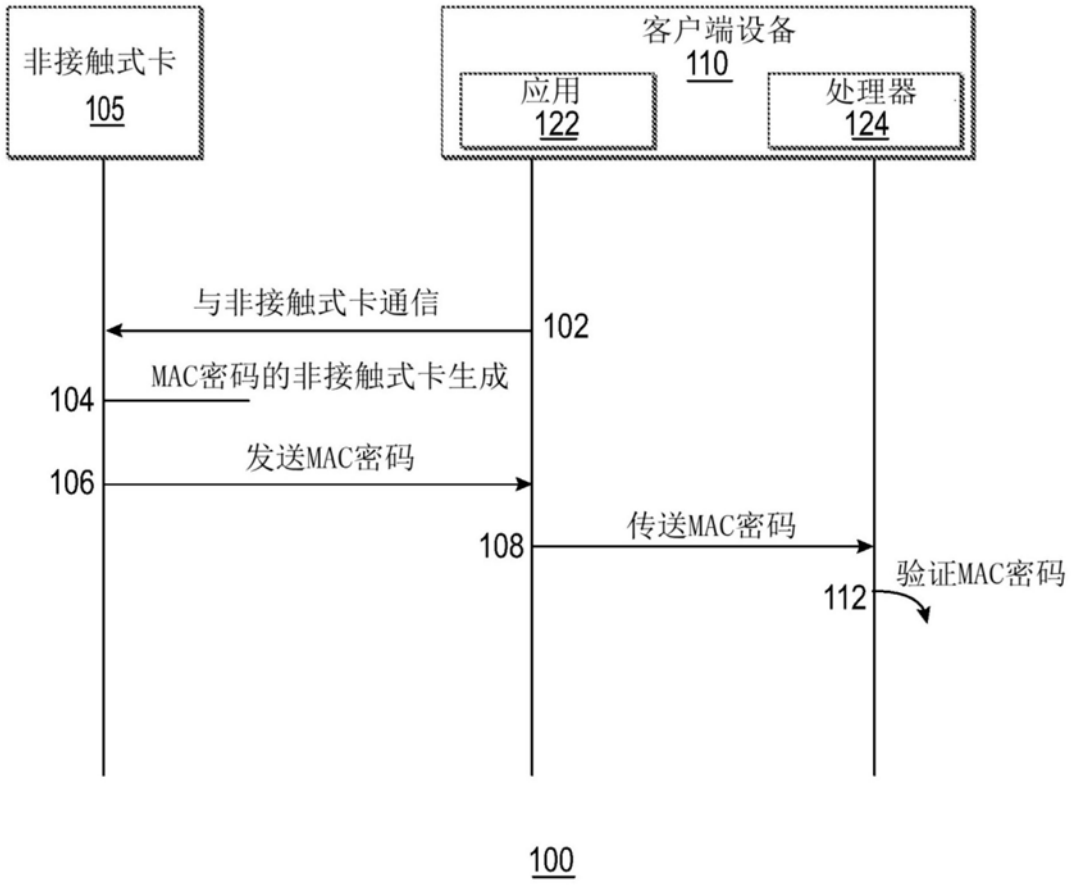

非接触式卡
105
客户端设备
110
应用
122
处理器
124
与非接触式卡通信
102
MAC密码的非接触式卡生成
104
发送MAC密码
106
传送MAC密码
108
验证MAC密码
112
100

图1B

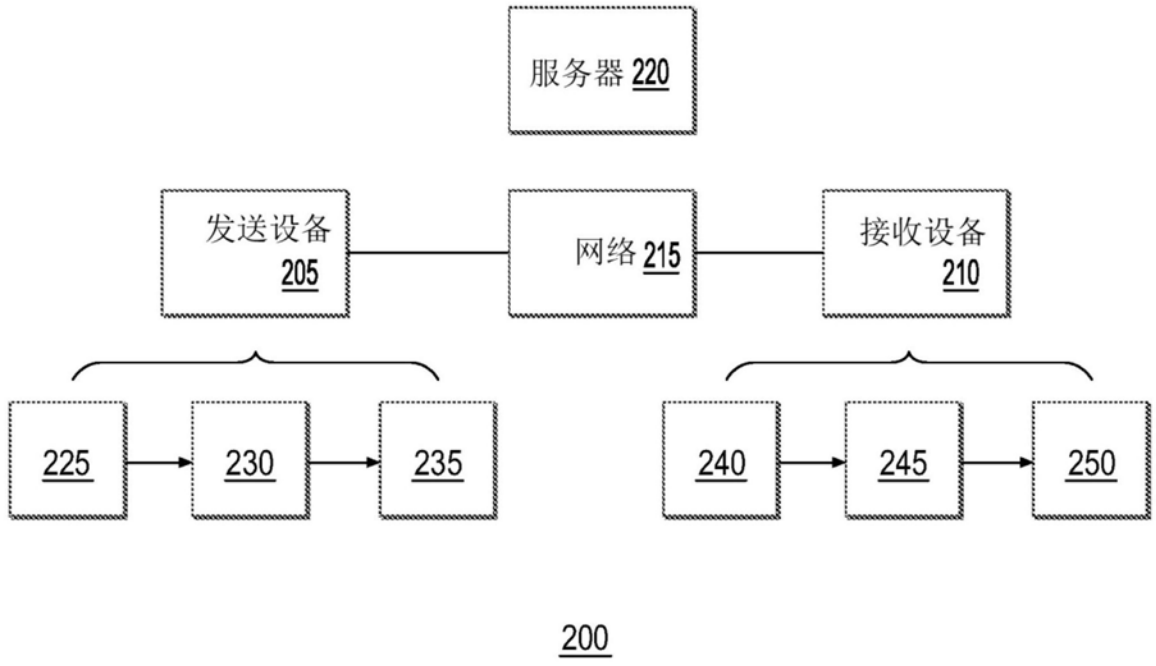

服务器 220
发送设备 205
网络 215
接收设备 210
225
230
235
240
245
250
200

图2

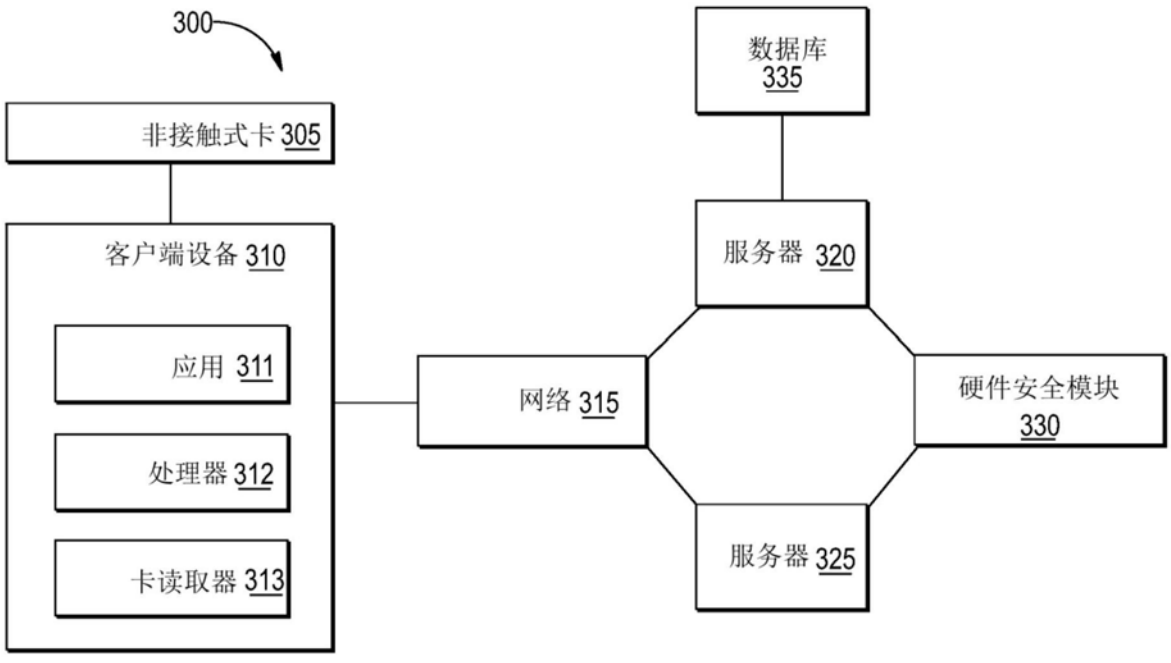

300
非接触式卡 305
客户端设备 310
应用 311
处理器 312
卡读取器 313
网络 315
数据库 335
服务器 320
硬件安全模块 330
服务器 325

图3

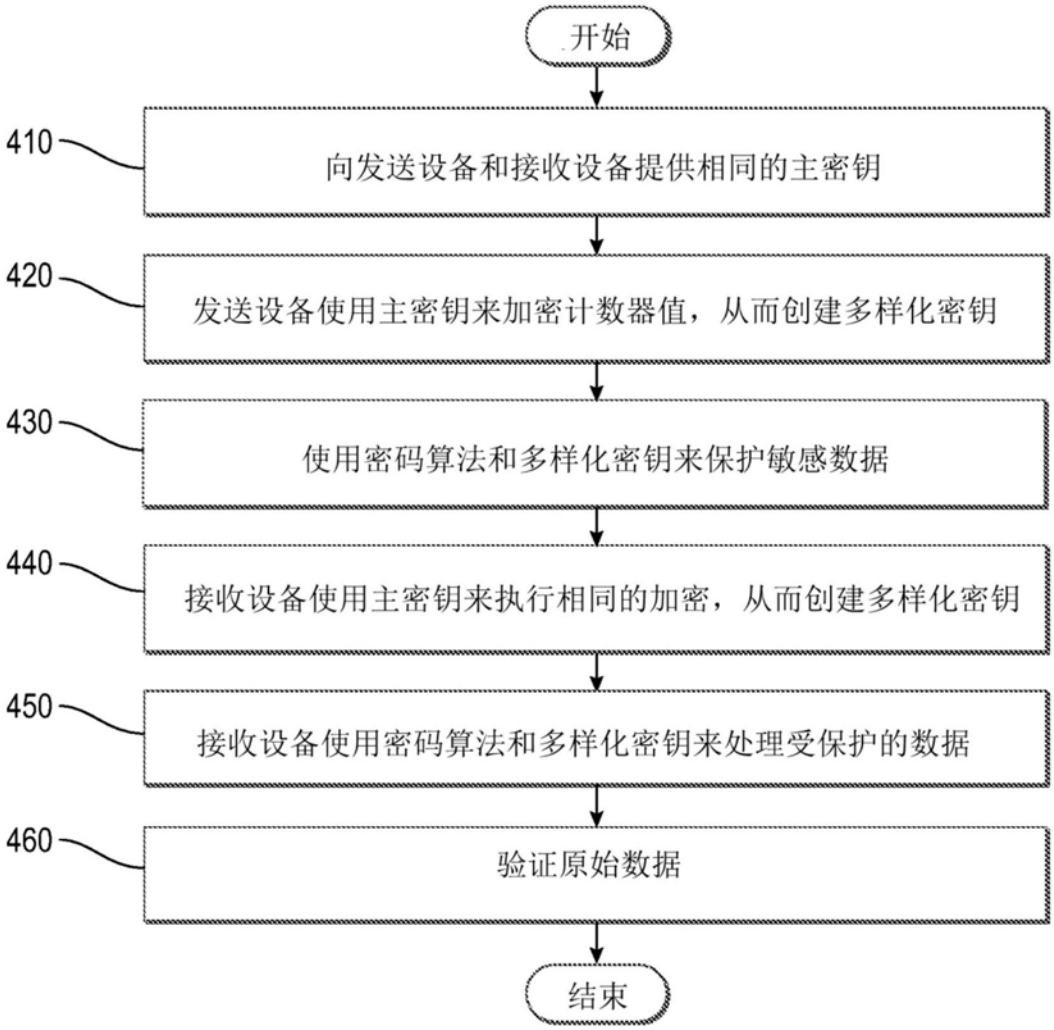

开始
410
向发送设备和接收设备提供相同的主密钥
420
发送设备使用主密钥来加密计数器值，从而创建多样化密钥
430
使用密码算法和多样化密钥来保护敏感数据
440
接收设备使用主密钥来执行相同的加密，从而创建多样化密钥
450
接收设备使用密码算法和多样化密钥来处理受保护的数据
460
验证原始数据
结束
400

图4

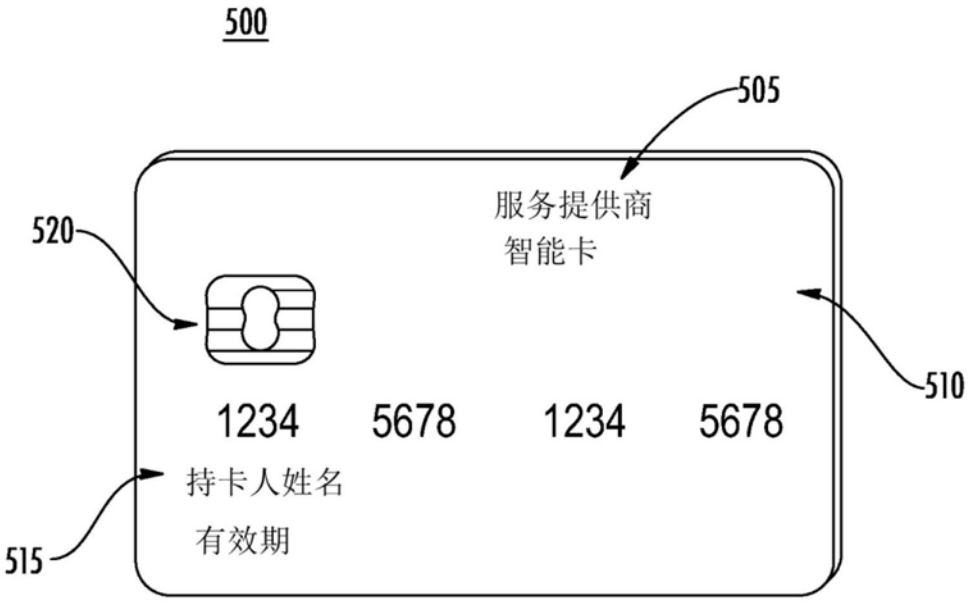


图5A

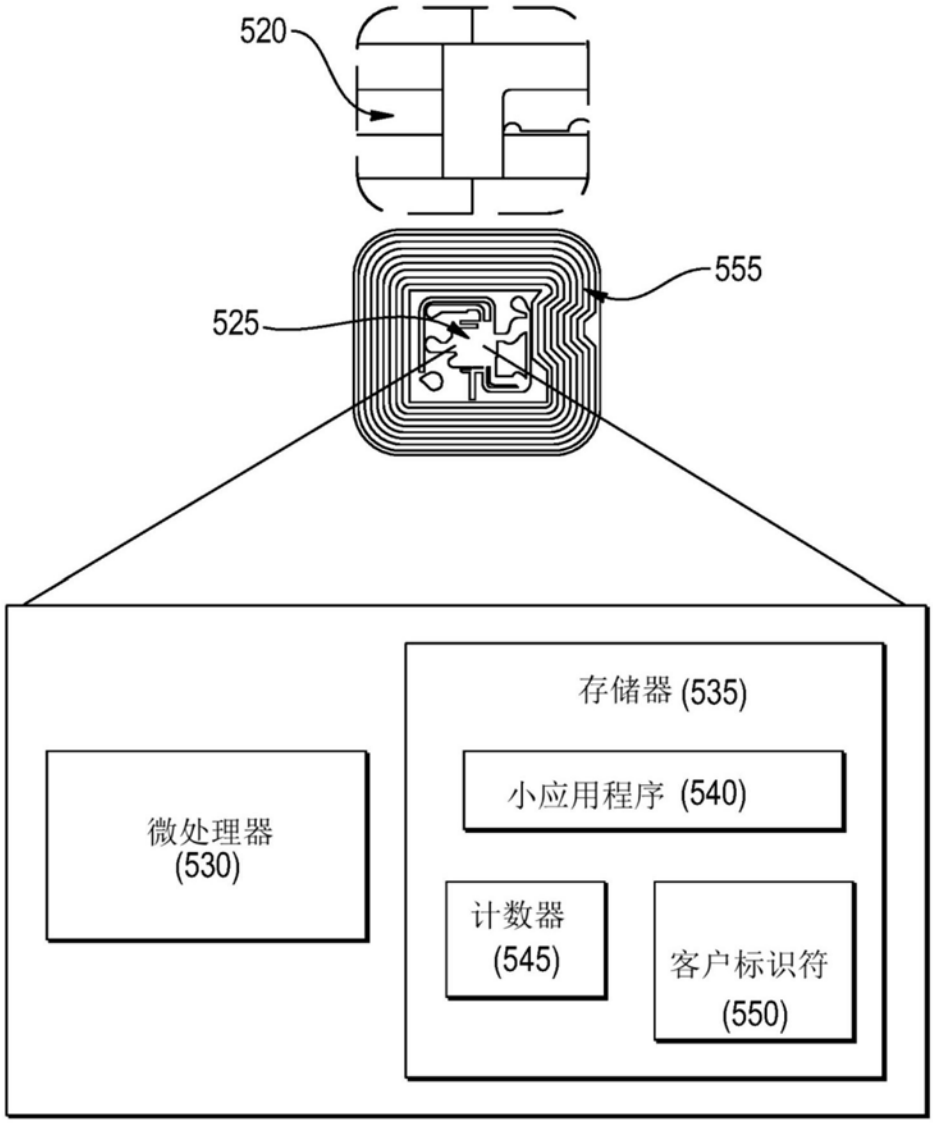
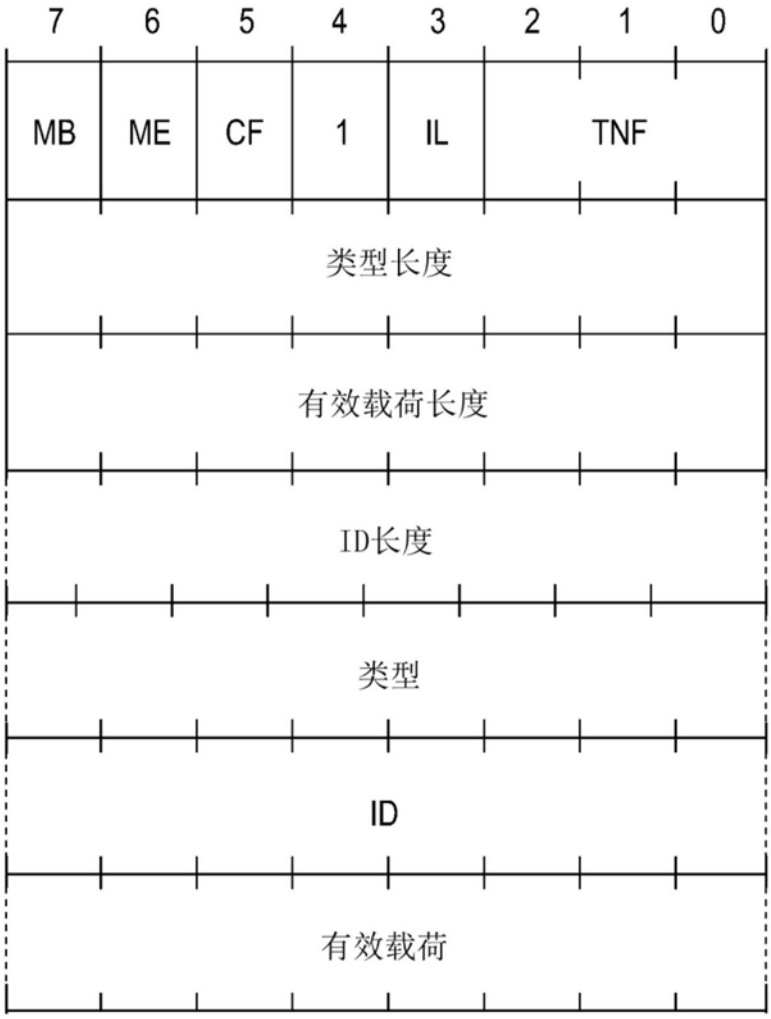


图5B



600

图6

00 D1 (消息开始 , 消息结束 , 短记录 , nolD 长度) 01 (已知类型) 01 01 文本类型
02 <载荷长度包括记录ID和“EN” ,或者内容长度+3) = 45+3 = 48 (DEC)
03 54 ('T')
04 02 记录ID
05 65 6E (语言长度 , 'en')
07 43 01 00 76 a6 62 7b 67 a8 cf bb < 8 mac字节 >
D101305402656E 43010076A6627B67A8CFBB < 8 mac字节 >

710

版本	pUID (8)	pATC	经加密的密码（16）	
0100	0015399555360061	00000050	7D28B8B9D8666E5143153AC9C944E5A6	
经解密的密码				
RANDOM (8)	MAC (8)			
4838FB7DC171B89E	CF3F3B8C56DA0BF1			
	MAC(T=[pVERSION (2 BYTES) | | pUID (8 BYTES) | | pATC (4 BYTES) | | pSHSEC (4 BYTES) | | '80' | | '00 00 00 00 00'])			

720

图7

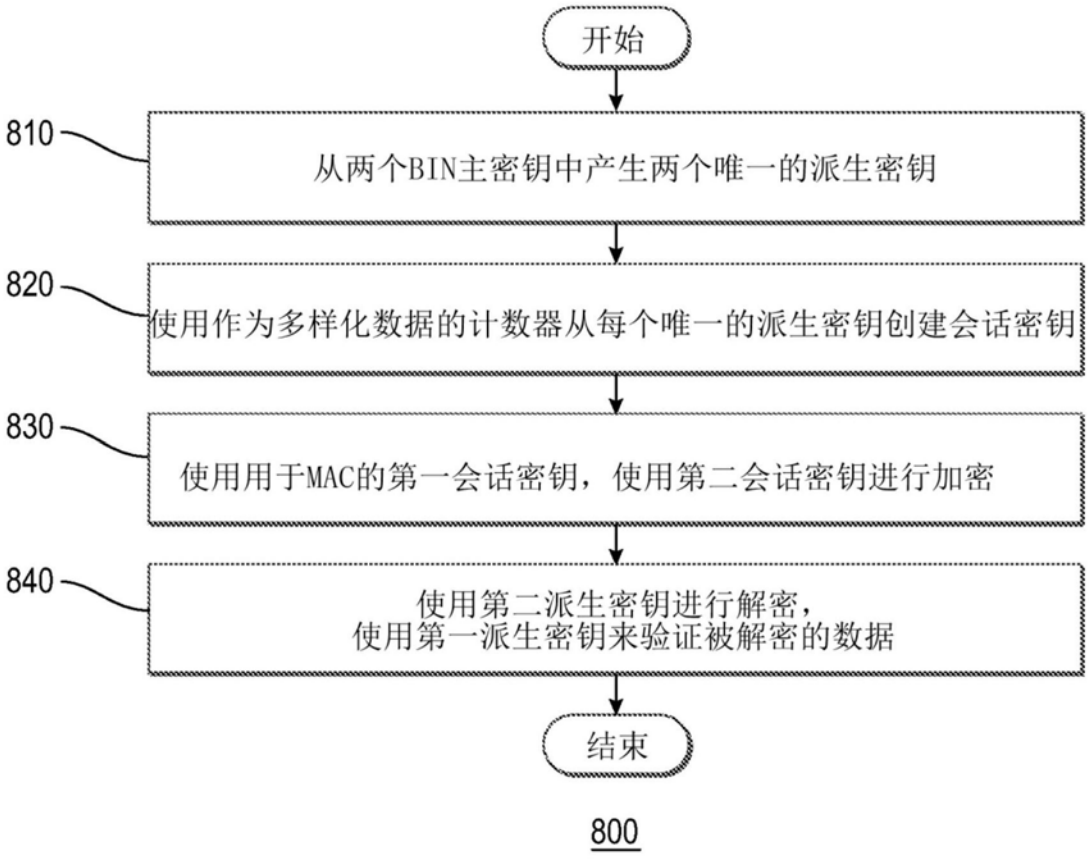

开始
810
从两个BIN主密钥中产生两个唯一的派生密钥
820
使用作为多样化数据的计数器从每个唯一的派生密钥创建会话密钥
830
使用用于MAC的第一会话密钥，使用第二会话密钥进行加密
840
使用第二派生密钥进行解密，
使用第一派生密钥来验证被解密的数据
结束
800

图8

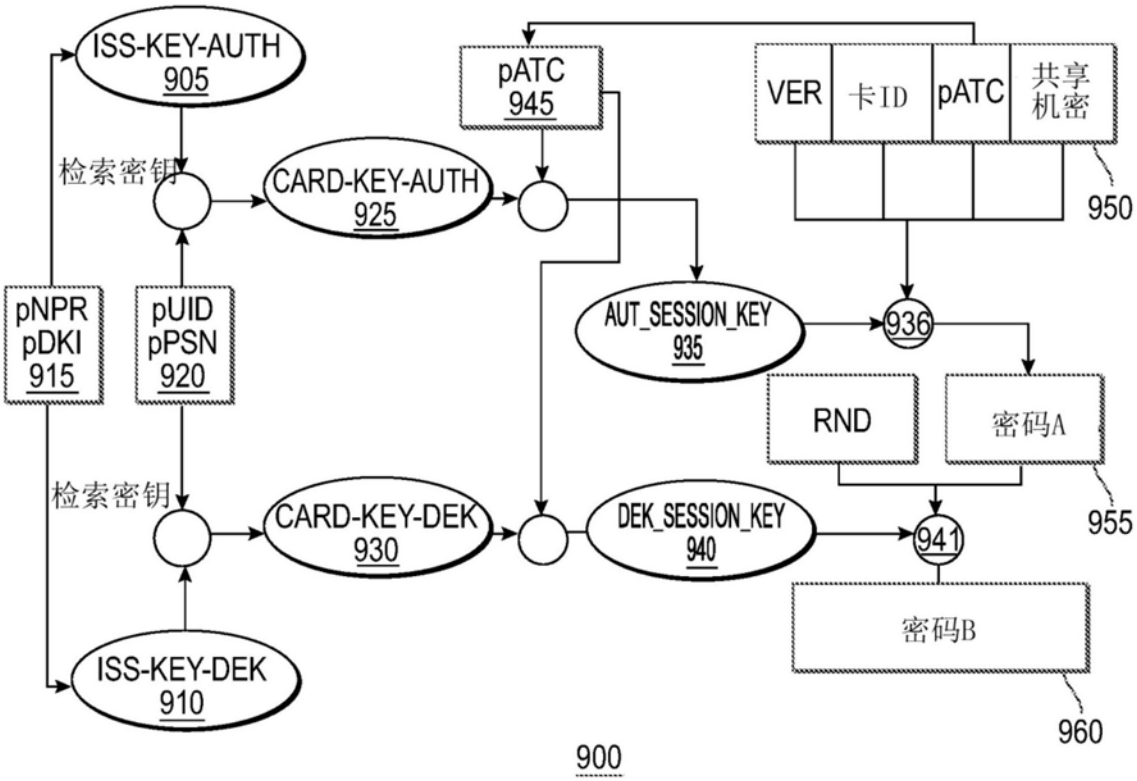

ISS-KEY-AUTH
905
检索密钥
CARD-KEY-AUTH
925
pATC
945
VER
卡ID
pATC
共享
机密
950
pNPR
pDKI
915
pUID
pPSN
920
AUT_SESSION_KEY
935
936
RND
密码A
955
检索密钥
CARD-KEY-DEK
930
DEK_SESSION_KEY
940
941
密码B
960
ISS-KEY-DEK
910
900

图9

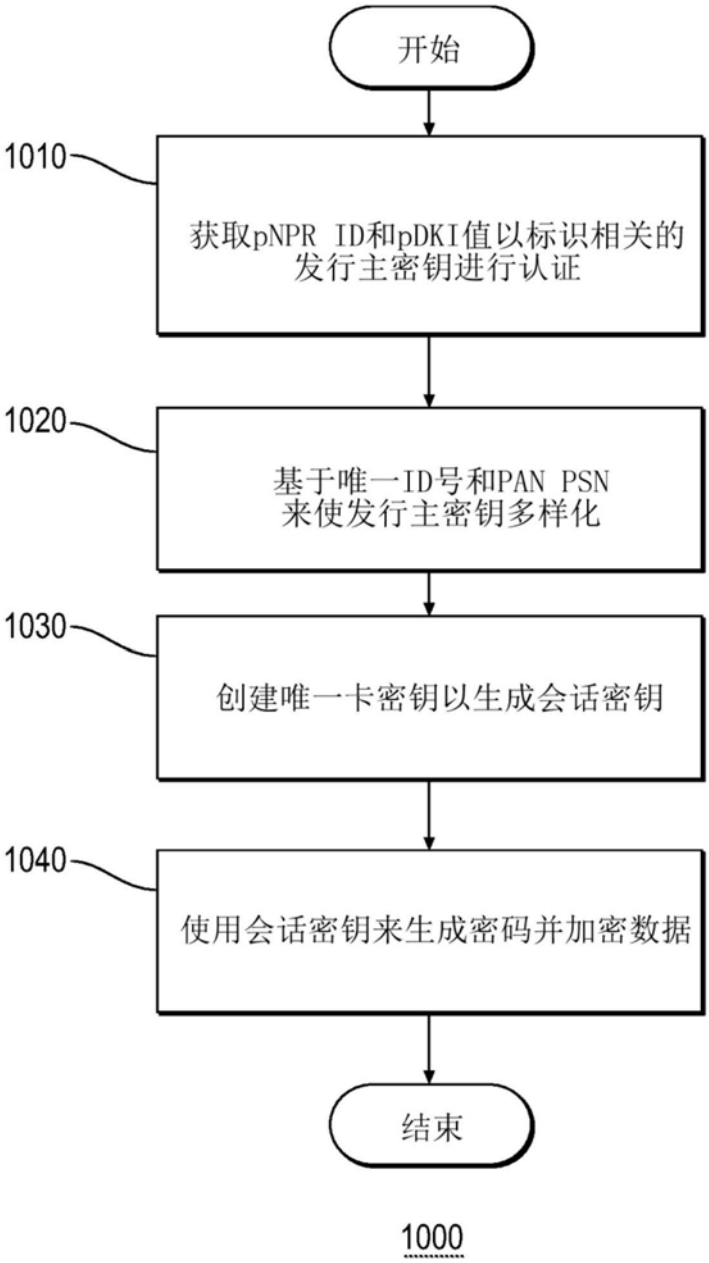

开始
1010
获取pNPR ID和pDKI值以标识相关的发行主密钥进行认证
1020
基于唯一ID号和PAN PSN来使发行主密钥多样化
1030
创建唯一卡密钥以生成会话密钥
1040
使用会话密钥来生成密码并加密数据
结束
1000

图10

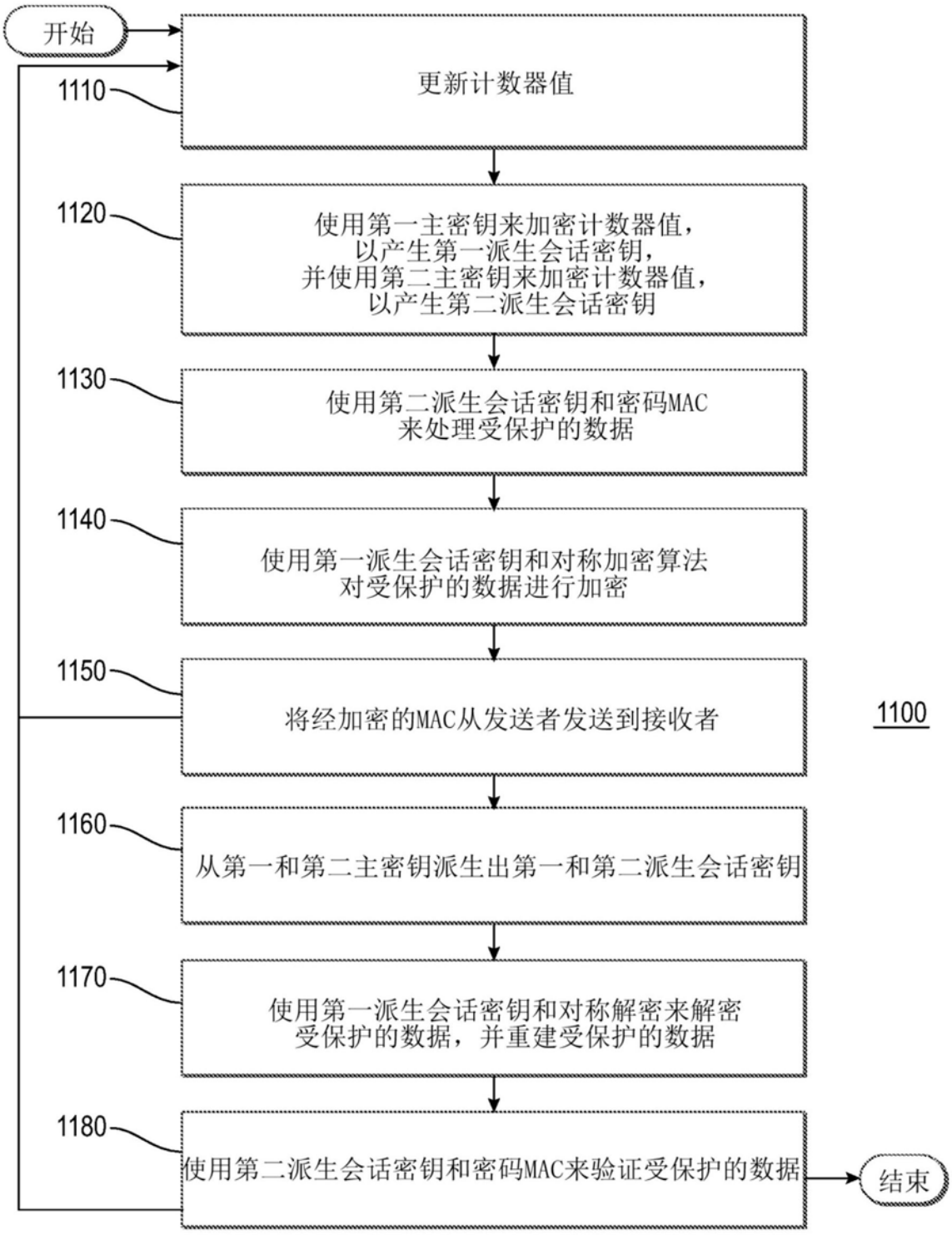

开始
1110
更新计数器值
1120
使用第一主密钥来加密计数器值，
以产生第一派生会话密钥，
并使用第二主密钥来加密计数器值，
以产生第二派生会话密钥
1130
使用第二派生会话密钥和密码MAC
来处理受保护的数据
1140
使用第一派生会话密钥和对称加密算法
对受保护的数据进行加密
1150
将经加密的MAC从发送者发送到接收者
1100
1160
从第一和第二主密钥派生出第一和第二派生会话密钥
1170
使用第一派生会话密钥和对称解密来解密
受保护的数据，并重建受保护的数据
1180
使用第二派生会话密钥和密码MAC来验证受保护的数据
结束

图11

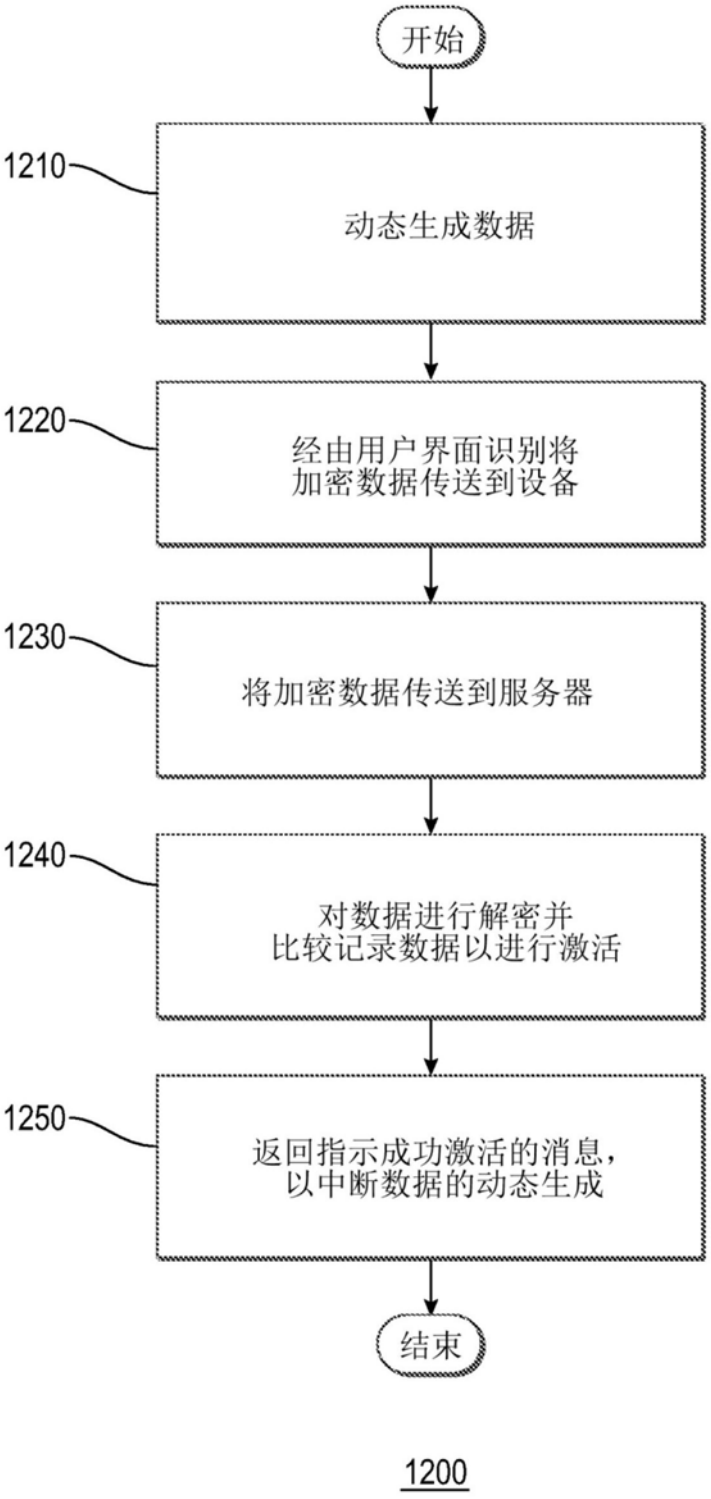

开始
1210
动态生成数据
1220
经由用户界面识别将
加密数据传送到设备
1230
将加密数据传送到服务器
1240
对数据进行解密并
比较记录数据以进行激活
1250
返回指示成功激活的消息，
以中断数据的动态生成
结束
1200

图12

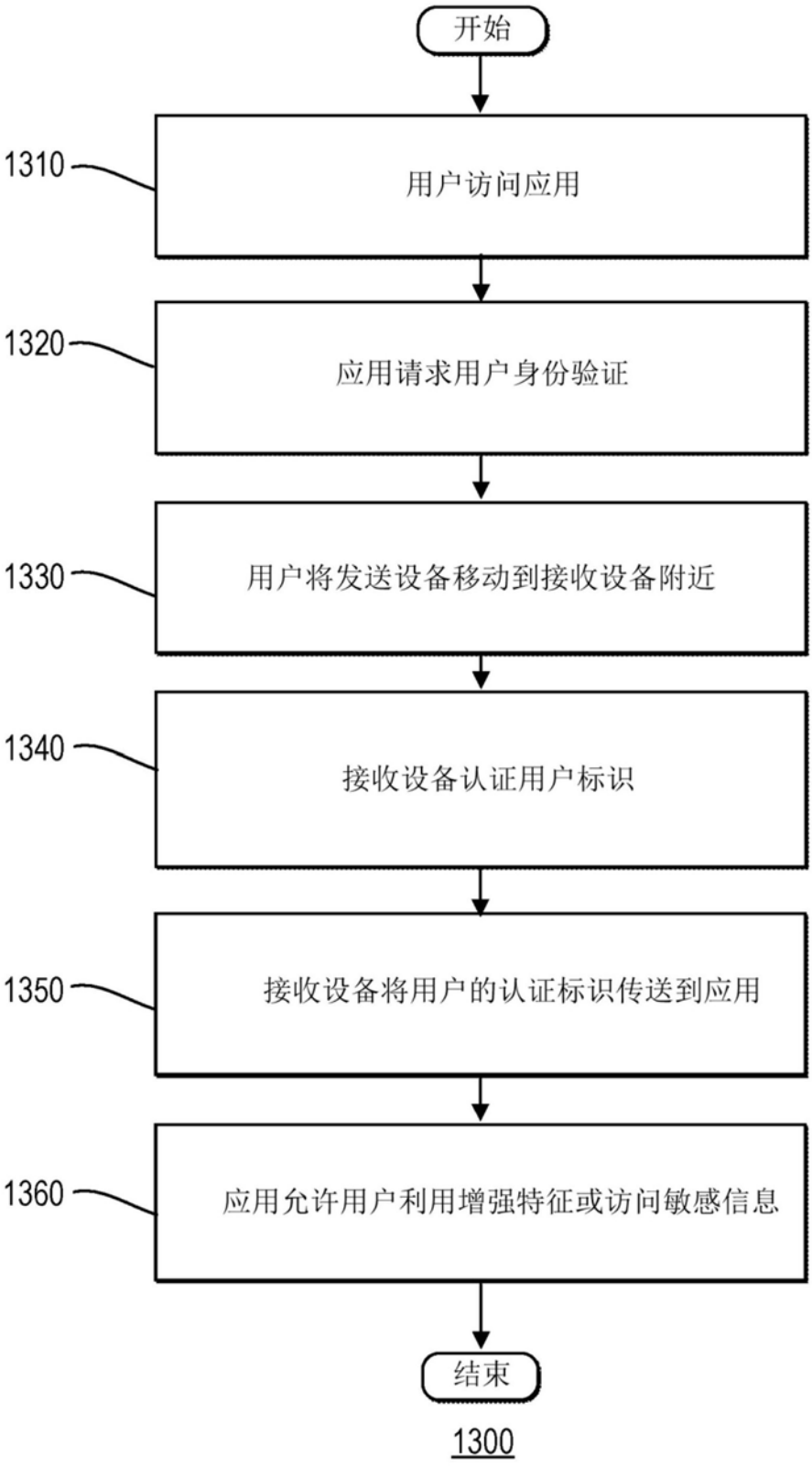
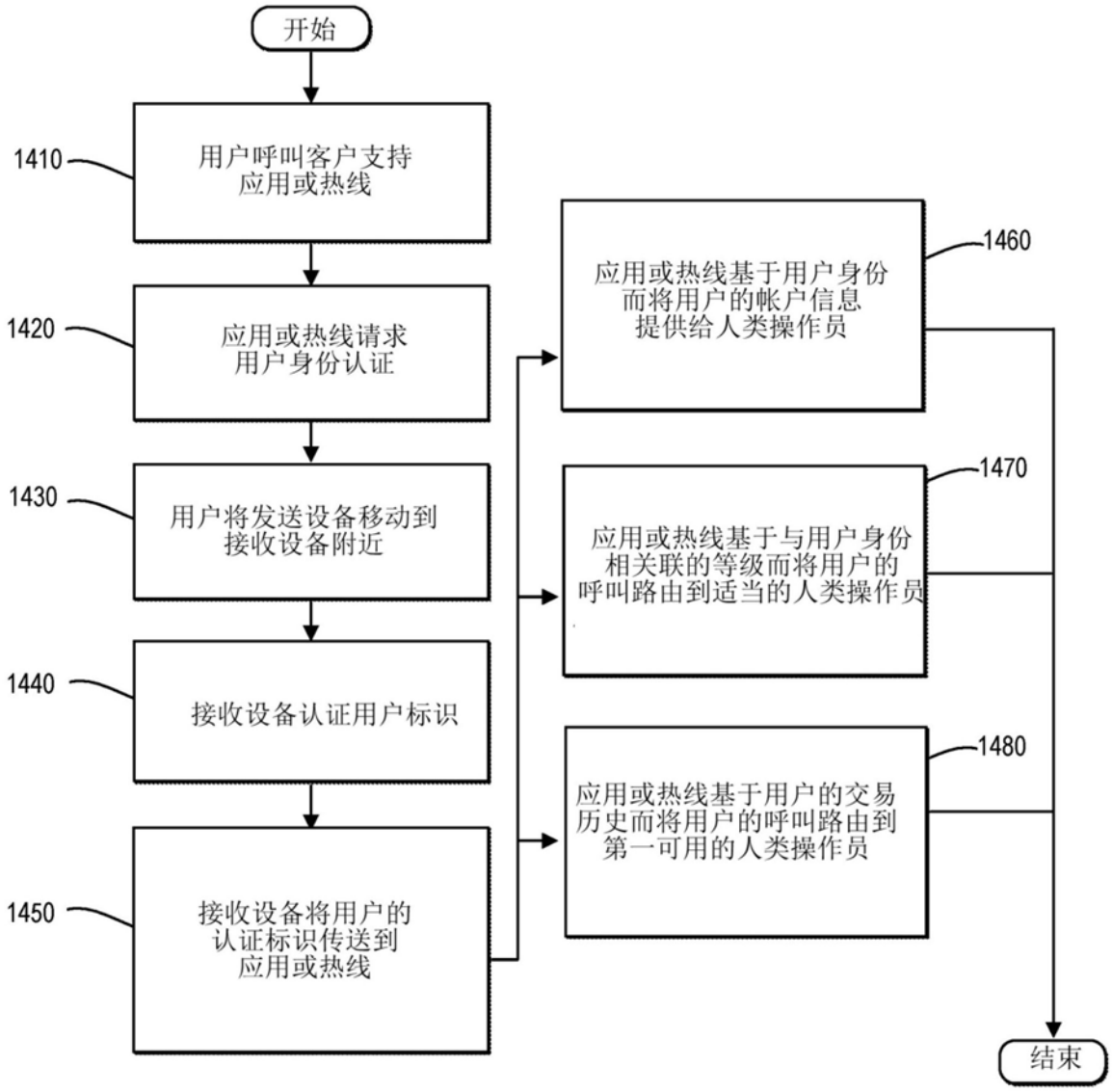

开始
1310
用户访问应用
1320
应用请求用户身份验证
1330
用户将发送设备移动到接收设备附近
1340
接收设备认证用户标识
1350
接收设备将用户的认证标识传送到应用
1360
应用允许用户利用增强特征或访问敏感信息
结束
1300

图13


开始
1410
用户呼叫客户支持应用或热线
1420
应用或热线请求用户身份认证
1430
用户将发送设备移动到接收设备附近
1440
接收设备认证用户标识
1450
接收设备将用户的认证标识传送到应用或热线
1460
应用或热线基于用户身份而将用户的帐户信息提供给人类操作员
1470
应用或热线基于与用户身份相关联的等级而将用户的呼叫路由到适当的人类操作员
1480
应用或热线基于用户的交易历史而将用户的呼叫路由到第一可用的人类操作员
结束

1400

图14