(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 112789643 A
(43)申请公布日 2021.05.11

(21)申请号 201980064448.0

(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
16/546,657 2019.08.21 US

(85)PCT国际申请进入国家阶段日
2021.03.30

(86)PCT国际申请的申请数据
PCT/US2019/053736 2019.09.30

(87)PCT国际申请的公布数据
WO2020/072340 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 杰弗里·鲁尔 梅丽莎·亨 詹姆斯·阿什菲尔德 科林·哈特 拉伊科·埃琳西克 韦恩·卢茨

(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 20/40(2012.01)
G06Q 20/34(2012.01)
H04B 5/00(2006.01)
H04W 4/80(2018.01)
H04W 12/06(2021.01)

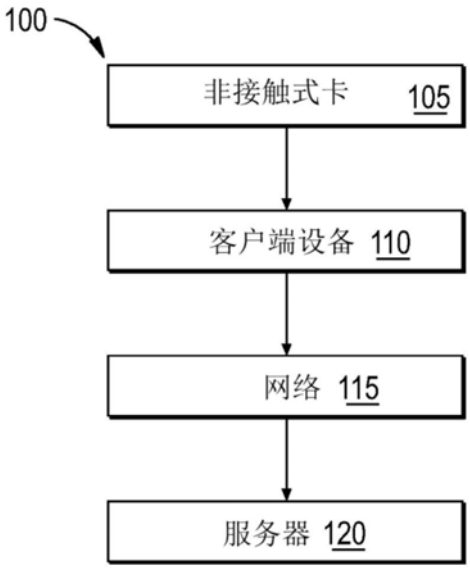
权利要求书2页 说明书33页 附图13页

(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

提供了用于非接触式卡、客户端设备和一个或多个服务器之间的数据传输的系统和方法的示例实施例。非接触式卡可以包括一个或多个处理器和存储器。存储器可以包括一个或多个小应用程序。客户端设备可以包括一个或多个处理器和存储器。客户端设备可以与非接触式卡进行数据通信。一个或多个服务器可以与客户端设备进行数据通信。可以将第一信息集合从非接触式卡传送到客户端设备。第一信息集合可以包括用于激活非接触式卡的一个或多个链接。客户端设备可以被配置为从非接触式卡接收第一信息集合。在验证第一信息集合之后，可以激活非接触式卡。



CN 112789643 A

1.一种卡激活系统,包括:

非接触式卡,包括一个或多个处理器和存储器,其中所述存储器包含一个或多个小应用程序;

客户端应用程序,包括用于在包括一个或多个处理器和存储器的客户端设备上执行的指令;和

一个或多个服务器,

其中,在所述非接触式卡进入通信场时,所述非接触式卡被配置为向所述客户端应用程序传送第一信息集合,所述第一信息集合包括被配置为激活所述非接触式卡的一个或多个链接;

其中,所述客户端应用程序被配置为接收来自所述非接触式卡的第一信息集合,并将其传送到所述一个或多个服务器进行验证,并且

其中,在验证所述第一信息集合之后,所述非接触式卡被激活。

2.根据权利要求1所述的卡激活系统,其中,所述第一信息集合包括第一链接,所述第一链接包括用于激活所述非接触式卡的一个或多个信息元素。

3.根据权利要求2所述的卡激活系统,其中,第一信息元素包括电话号码,第二信息元素包括一个或多个逗号,第三信息元素包括加密的有效载荷。

4.根据权利要求3所述的卡激活系统,其中,所述电话号码是动态生成的。

5.根据权利要求3所述的卡激活系统,其中,所述第二信息元素包括一个或多个逗号,其表示与所述客户端应用程序发起的电话呼叫相关联的持续性停顿。

6.根据权利要求3所述的卡激活系统,其中,所述第三信息元素是通过所述一个或多个服务器用一个或多个密钥解密的。

7.根据权利要求4所述的卡激活系统,其中,从所述非接触式卡接收包括多个电话号码的列表。

8.根据权利要求7所述的卡激活系统,其中,基于认证的目的,从所述列表中选择电话号码。

9.根据权利要求1所述的卡激活系统,其中,所述第一信息集合包括用于激活所述非接触式卡的卡验证值。

10.根据权利要求1所述的卡激活系统,其中,所述非接触式卡被配置为在所述客户端应用程序从所述一个或多个服务器接收到所述非接触式卡被激活的通知之后,停止所述第一信息集合的动态生成。

11.一种激活非接触式卡的方法,所述方法包括以下步骤:

使所述非接触式卡进入通信场;

由包含在所述非接触式卡中的一个或多个小应用程序经由所述通信场向客户端应用程序传送第一信息集合,所述客户端应用程序包括用于在客户端设备上运行的指令,所述第一信息集合包括被配置为激活所述非接触式卡的一个或多个链接;

由所述客户端应用程序将所述第一信息集合传送到一个或多个服务器;

由所述一个或多个服务器执行一个或多个密码操作以验证所述第一信息集合;以及

在验证所述第一信息集合后,激活所述非接触式卡。

12.根据权利要求11所述的方法,其中,所述第一信息集合包括第一链接,所述第一链

接包括用于激活所述非接触式卡的一个或多个信息元素。

13.根据权利要求12所述的方法，其中，第一信息元素包括电话号码，第二信息元素包括一个或多个逗号，第三信息元素包括加密的有效载荷。

14.根据权利要求13所述的方法，其中，所述电话号码是从预先配置的列表中检索的。

15.根据权利要求13所述的方法，其中，所述一个或多个逗号表示与所述客户端应用程序发起的电话呼叫相关的持续性停顿。

16.根据权利要求13所述的方法，其中，所述第三信息元素是通过所述一个或多个服务器用一个或多个密钥解密的。

17.根据权利要求11所述的方法，其中，所述第一信息集合包括用于激活所述非接触式卡的卡验证值。

18.根据权利要求11所述的方法，其中，从所述非接触式卡接收包括多个电话号码的列表，并且基于认证的目的，从所述列表中选择电话号码。

19.根据权利要求11所述的方法，其中，所述非接触式卡被配置为在所述客户端应用程序从所述一个或多个服务器接收到所述非接触式卡被激活的通知之后，停止所述第一信息集合的动态生成。

20.一种非接触式卡，包括：

处理器；

存储器，其中所述存储器包含一个或多个小应用程序以及第一信息集合，

其中，在所述非接触式卡进入通信场时，所述一个或多个小应用程序被配置为传送第一信息集合，

其中，所述第一信息集合包括被配置为激活所述非接触式卡的一个或多个链接，所述一个或多个链接包括第一信息元素和第二信息元素，并且

其中，所述第一信息元素包括电话号码，所述第二信息元素包括加密的有效载荷。

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8月21日提交的美国专利申请号16/546,657(该申请是于2018年11月29日提交的美国专利申请号16/205,119的部分延续并要求其优先权)的优先权,并要求于2018年10月2日提交的美国临时专利申请号62/740,352的优先权,这些专利申请的公开内容通过引用整体结合于此。

技术领域

[0003] 本公开涉及密码术,并且更具体地,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] 数据安全和交易完整性对企业和消费者至关重要。随着电子交易构成越来越大的商业活动份额,这种需求继续增长。

[0005] 电子邮件可能被用作验证交易的工具,但电子邮件容易受到攻击,并且容易受到黑客或其他未经授权的访问的损坏。也可以使用短消息服务(Short message service,SMS)消息,但这也会受到损害。而且,甚至数据加密算法(诸如三重DES算法)也有类似的漏洞。

[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以及输入或以其他方式提供卡信息的耗时过程。进一步,尽管基于芯片的金融卡的越来越多的使用为个人购买提供了相比于以前的技术(例如,磁条卡)更安全的特征,但账户访问仍然可能依赖登录凭证(例如,用户名和密码)来确认持卡人的身份。但是,如果登录凭证受到破坏,则其他人可能会访问该用户的帐户。

[0007] 这些和其他缺陷是存在的。因此,需要为用户提供克服这些缺陷的适当解决方案,以为非接触式卡提供数据安全性、认证和验证。进一步,需要激活卡的改进的方法和账户访问的改进的认证。

发明内容

[0008] 所公开技术的各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施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非接触式卡激活系统,包括:非接触式卡,包括一个或多个处理器和存储器,其中所述存储器包含一个或多个小应用程序;客户端应用程序,包括用于在包括一个或多个处理器和存储器的客户端设备上执行的指令;和一个或多个服务器,其中,在非接触式卡进入通信场中时,非接触式卡被配置为向客户端应用程序传送第一信息集合,所述第一信息集合包括被配置为激活非接触式卡的一个或多个链接;其中,客户端应用程序被配置为接收来自非接触式卡的第一信息集合,并将其传送到服务器进行验证,并且其中,在验证了第一信息集合之后,非接触式卡被激活。

[0010] 本公开的实施例提供了一种激活非接触式卡的方法，该方法包括以下步骤：使非接触式卡进入通信场；由包含在非接触式卡中的一个或多个小应用程序经由所述通信场向客户端应用程序传送第一信息集合，所述客户端应用程序包括用于在客户端设备上运行的指令，所述第一信息集合包括被配置为激活非接触式卡的一个或多个链接；由客户端应用程序将第一信息集合传送到一个或多个服务器；由一个或多个服务器执行一个或多个密码操作以验证第一信息集合；以及在验证第一信息集合后，激活非接触式卡。

[0011] 本公开的实施例提供了一种非接触式卡，包括：处理器；存储器，其中，存储器包含一个或多个小应用程序以及第一信息集合，其中，在非接触式卡进入通信场时，一个或多个小应用程序被配置为传送第一信息集合，其中，第一信息集合包括被配置为激活非接触式卡的一个或多个链接，一个或多个链接包括第一信息元素和第二信息元素，并且其中，第一信息元素包括电话号码，第二信息元素包括加密的有效载荷。

[0012] 在下文中参考附图中示出的特定示例实施例，更详细地说明了所公开的设计的其他特征以及由此提供的优点。

附图说明

[0013] 图1A是根据示例实施例的数据传输系统的图。

[0014] 图1B是示出根据示例实施例的用于提供经认证的访问的序列的图。

[0015] 图2是根据示例实施例的数据传输系统的图。

[0016] 图3是根据示例实施例的使用非接触式卡的系统的图。

[0017] 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。

[0018] 图5A是根据示例实施例的非接触式卡的图示。

[0019] 图5B是根据示例实施例的非接触式卡的接触垫的图示。

[0020] 图6是描绘根据示例实施例的用于与设备通信的消息的图示。

[0021] 图7是描绘根据示例实施例的消息和消息格式的图示。

[0022] 图8是示出根据示例实施例的密钥操作的流程图。

[0023] 图9是根据示例实施例的密钥系统的图。

[0024] 图10是根据示例实施例的生成密码的方法的流程图。

[0025] 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。

[0026] 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。

[0027] 图13是根据示例实施例的卡激活系统。

[0028] 图14是根据示例实施例的用于激活非接触式卡的方法。

具体实施方式

[0029] 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。审阅了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施方式将被理解为与本发明的应用一致。

[0030] 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，这些功能可能需要用户携带分离的物理令牌。通过采用非接触式接口，可以为非接触式卡提供用于在用户的设备(诸如移动电话)和卡本身之间进行交互和通信的方法。例如，EMV协议(其是许多信用卡交易的基础)包括认证过程，该认证过程足以满足Android®操作系统，但对iOS®提出了挑战，该iOS®在近场通信(near field communication，NFC)使用方面限制更严格，因为它只能以只读方式使用。本文描述的非接触式卡的示例实施例利用了NFC技术。

[0031] 图1A示出了根据示例实施例的数据传输系统。如下文进一步讨论的，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可以包括任意数量的组件。

[0032] 系统100可以包括一个或多个非接触式卡105，这将在下面参考图5A至图5B进一步解释。在一些实施例中，非接触式卡105可以利用示例中的NFC与客户端设备110进行无线通信。

[0033] 系统100可以包括客户端设备110，其可以是支持网络的计算机。如本文所指，支持网络的计算机可以包括但不限于计算机设备或通信设备，包括例如服务器、网络应用程序、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、因特网浏览器或其他设备。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®的的iPhone、iPod、iPad或运行苹果的iOS®操作系统的任何其他移动设备、运行微软Windows®Mobile操作系统的任何设备、运行谷歌的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。

[0034] 客户端设备110设备可以包括处理器和存储器，并且应当理解的是，处理电路可以包含执行本文描述的功能所必需的附加组件，包括处理器、存储器、错误和奇偶校验/CRC检查器、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。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，诸如计算机监控器、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的设备中的任何设备，该设备是可用的并且由用户设备支持，诸如触摸屏、键盘、鼠标、光标控制设备、触摸屏、麦克风、数码相机、录像机或便携式摄像机。这些设备可以用于输入信息并与软件和本文描述的其他设备交互。

[0035] 在一些示例中，系统100的客户端设备110可以执行实现例如与系统100的一个或多个组件的网络通信以及传送和/或接收数据的一个或多个应用程序，诸如软件应用程序。

[0036] 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，并且可以与服务器120作为相应前端到后端对来操作。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程序向服务器120传送一个或多个请求。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可以接收来自客户端设备110的一个或多个请求。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传送到客户端设备110,所接收的数据是响应于一个或多个请求的。

[0037] 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的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、多媒体消息传递服务、增强消息传递服务、短消息服务、基于时分复用的系统、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。

[0038] 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、无线个人区域网、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,但是应当理解的是,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、线缆电视网络、诸如信用卡协会网络的公司网络、以及家庭网络。

[0039] 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可以被配置为用于在不同时间控制和调用各种数据来执行多个工作流动作的中央系统、服务器或平台。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。

[0040] 图1B是示出根据本公开的一个或多个实施例的用于提供经认证的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,该客户端设备可以包括应用程序122和处理器124。图1B可以引用如图1A所示的类似组件。

[0041] 在步骤102,应用程序122(例如,在被带到非接触式卡105附近之后)与非接触式卡105通信。应用程序122和非接触式卡105之间的通信可以涉及非接触式卡105足够接近客户端设备110的读卡器(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数据传递。

[0042] 在步骤104,在客户端设备110与非接触式卡105之间已经建立了通信之后,非接触式卡105生成消息认证码(MAC)密码。在一些示例中,这可能在应用程序122读取非接触式卡105时发生。特别地,这可以在读取(例如,NFC读取)近场数据交换(NDEF)标签时发生,该近场数据交换(NDEF)标签可以根据NFC数据交换格式来创建。例如,诸如应用程序122之类的读取器可以传送具有诸如NDEF产生小应用程序的小应用程序ID的消息,诸如小应用程序选择消息。在确认选择之后,可以传送选择文件消息的序列,随后是读取文件消息。例如,序列可以包括“选择能力文件”,“读取能力文件”和“选择NDEF文件”。此时,由非接触式卡105维护的计数器值可以被更新或递增,随后可以是“读取NDEF文件”。此时,可以生成可以包括报头和共享秘密(secret)的消息。然后可以生成会话密钥。MAC密码可以根据消息创建,该消息可以包括报头和共享秘密。MAC密码然后可以与一个或多个随机数据块连接,并且MAC密码和随机数(random number,RND)可以用会话密钥加密。此后,密码和报头可以被级联,并

被编码为ASCII十六进制,并(响应“读取NDEF文件”消息)以NDEF消息格式返回。

[0043] 在一些示例中,MAC密码可以作为NDEF标签来传送,并且在其他示例中,MAC密码可以与统一资源指示符一起被包括(例如,作为格式化的字符串)。

[0044] 在一些示例中,应用程序122可以被配置为向非接触式卡105传送请求,该请求包括用于生成MAC密码的指令。

[0045] 在步骤106,非接触式卡105向应用程序122发送MAC密码。在一些示例中,MAC密码的传输经由NFC发生,然而,本公开不限于此。在其他示例中,这种通信可以经由蓝牙、Wi-Fi或其他无线数据通信方式进行。

[0046] 在步骤108,应用程序122将MAC密码传送给处理器124。

[0047] 在步骤112,处理器124根据来自应用程序122的指令来验证MAC密码。例如,如下所述,可以验证MAC密码。

[0048] 在一些示例中,验证MAC密码可以由除了客户端设备110的设备(诸如与客户端设备110进行数据通信的服务器120(如图1A所示))来执行。例如,处理器124可以输出MAC密码以便传送到服务器120,该服务器可以验证MAC密码。

[0049] 在一些示例中,MAC密码可以用作用于验证目的的数字签名。其他数字签名算法(诸如公钥非对称算法,例如数字签名算法和RSA算法、或者零知识协议)可以用于执行这种验证。

[0050] 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通信的发送设备205、接收设备210。发送设备205可以与上面参考图1A讨论的客户端设备110相同或相似。接收设备210可以与上面参考图1A讨论的客户端设备110相同或相似。网络215可以类似于上面参考图1A讨论的网络115。服务器220可以类似于上面参考图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。

[0051] 当使用对称加密算法(诸如加密算法、基于哈希的消息认证码(HMAC)算法和基于密码的消息认证码(CMAC)算法)时,重要的是,密钥在最初使用对称算法和密钥处理受保护的数据的一方与使用相同加密算法和相同密钥接收和处理数据的一方之间保持是秘密的。

[0052] 同样重要的是,相同的密钥不被使用太多次。如果密钥使用或重复使用过于频繁,该密钥可能会被泄露。每次使用密钥时,它向攻击者提供额外的数据样本,该数据样本是由加密算法使用相同的密钥处理的。攻击者拥有的用相同密钥处理的数据越多,攻击者发现密钥值的可能性就越大。频繁使用的密钥可能包含在各种不同的攻击中。

[0053] 而且,每次执行对称密码算法时,它可能会揭示关于在对称密码操作期间使用的密钥的信息,诸如边信道数据。边信道数据可以包括在使用密钥的同时加密算法执行时出现的微小功率波动。可以对边信道数据进行充分的测量以揭示关于密钥的足够信息,从而允许其被攻击者恢复。使用相同密钥交换数据会重复揭示通过相同密钥处理的数据。

[0054] 然而,通过限制特定密钥将被使用的次数,攻击者能够收集的边信道数据量是有限的,并且从而减少了暴露于这种攻击和其他类型攻击。如本文进一步描述的,参与密码信息交换的各方(例如,发送者和接收者)可以结合计数器值根据初始共享主对称密钥独立地生成密钥,并且从而周期性地替换正在使用的共享对称密钥,而不需要依靠任何形式的密钥交换来保持各方同步。通过周期性地改变由发送者和接收者使用的共享秘密对称密钥,

以上描述的攻击变得不可能。

[0055] 转回参考图2，系统200可以被配置为实施密钥多样化。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)。如以上所解释的，尽管可以包括发送设备205和接收设备210的单个实例，但是应当理解的是，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密钥。在一些示例中，发送设备205和接收设备210可以被提供有相同的主对称密钥。进一步，应当理解的是，持有相同秘密对称密钥的任何一方或设备可以执行发送设备205的功能，并且类似地，持有相同秘密对称密钥的任何一方可以执行接收设备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参与交换安全数据的发送设备205和接收设备210之外的所有方保持是秘密的。还应当理解的是，发送设备205和接收设备210两者可以被提供有相同的主对称密钥，并且还应当理解的是，发送设备205和接收设备210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。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。

[0056] 系统200可以包括一个或多个网络215。在一些示例中，网络215可以是无线网络、有线网络或无线网络和有线网络的任意组合中的一个或多个，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可以包括光纤网络、无源光网络、线缆网络、互联网、卫星网络、无线LAN、全球移动通信、个人通信服务、个人局域网、无线应用协议、多媒体消息收发服务、增强型消息收发服务、短消息服务、基于时分复用的系统、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、RFID、Wi-Fi和/或其他中的一个或多个。

[0057] 此外，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、无线个人区域网、LAN或诸如因特网的全球网络。此外，网络215可以支持因特网网络、无线通信网络、蜂窝网络等，或者它们的任意组合。网络215还可以包括作为独立网络进行操作的一个网络，或者彼此协作地操作的任何数量的以上提及的示例性类型的网络。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可以转换到网络设备的一个或多个协议，或者从其他协议转换到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，但是应当理解的是，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、线缆电视网络、诸如信用卡协会网络的公司网络、以及家庭网络。

[0058] 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可以被配置为在彼此之间进行通信以及传送和接收数据，而不经过网络215。例如，一个或多个发送设备205和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等中的至少一个发生。

[0059] 在框225，当发送设备205准备用对称密码操作处理敏感数据时，发送者可以更新计数器。此外，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算法中的至少一个。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对称加密算法，诸如3DES或AES128；对称HMAC算法，诸如HMAC-SHA-256算法；以及对称CMAC算法，诸如AES-CMAC。应当理解的是，如果所选择的对称算法的

输出没有生成足够长的密钥,则诸如利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以产生多个输出,这些输出可以根据需要进行组合以产生足够长的密钥。

[0060] 在框230,发送设备205可以采用所选择的加密算法,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可以利用所选择的对称加密算法,使用主对称密钥创建多样化对称密钥,对计数器值进行加密。

[0061] 在某些示例中,计数器值可能未加密。在这些示例中,可以在框230处在发送设备205与接收设备210之间传送计数器值而没有加密。

[0062] 在框235,多样化对称密钥可以用于在将结果传送到接收设备210之前处理敏感数据。例如,发送设备205可以使用多样化对称密钥,使用对称加密算法来加密敏感数据,其中输出包括受保护的加密数据。发送设备205然后可以将受保护的加密数据连同计数器值一起传送到接收设备210以便进行处理。

[0063] 在框240,接收设备210可以首先获取计数器值,并且然后使用计数器值作为加密的输入以及主对称密钥作为用于加密的密钥,来执行相同的对称加密。加密的输出可以与发送方创建的多样化对称密钥值相同。

[0064] 在框245,接收设备210然后可以获取受保护的加密数据,并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。

[0065] 在框250,作为解密受保护的加密数据的结果,原始敏感数据可以被揭示。

[0066] 下一次敏感数据需要从发送者经由相应发送设备205和接收设备210发送到接收者时,可以选择不同的计数器值,从而产生不同的多样化对称密钥。通过利用主对称密钥和相同的对称加密算法处理计数器值,发送设备205和接收设备210两者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。

[0067] 如上所解释的,发送设备205和接收设备210两者最初各自拥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。因为多样化对称密钥是由发送设备205和接收设备210两者独立创建的,所以它从不在双方之间传送。因此,攻击者不能截取多样化对称密钥,并且攻击者决不会看到利用主对称密钥处理的任何数据。只有计数器值是利用主对称密钥处理的,而敏感数据不是利用主对称密钥处理的。因此,所揭示的关于主对称密钥的边信道数据被减少。而且,发送设备205和接收设备210的操作可以由多久创建一次新的多样化值以及因此创建新的多样化对称密钥的对称要求来管控。在实施例中,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。

[0068] 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随机随机数,该随机随机数从发送设备205发送到接收设备210;从发送设备205和接收设备210发送计数器值的全部值;从发送设备205和接收设备210发送计数器值的一部分;计数器由发送设备205和接收设备210独立维护,但不在两个设备之间发送;在发送设备205和接收设备210之间交换的一次性密码;以及敏感数据的加密哈希。在一些示例中,可以由各方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。进一步,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。

[0069] 在另一示例中，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获得多个多样化密钥值。可以每当需要时创建新的多样化值，以及因此创建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之间的敏感数据的每次交换创建新的多样化值。实际上，这可能会创建一次性使用的密钥，诸如单次使用的会话密钥。

[0070] 图3示出了使用非接触式卡的系统300。系统300可以包括非接触式卡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和数据库335。尽管图3示出了组件的单个实例，但是系统300可以包括任意数量的组件。

[0071] 系统300可以包括一个或多个非接触式卡305，这在下面参照图5A-5B进行进一步说明。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可以包括被配置为经由NFC或其他短程协议进行通信的一个或多个芯片，诸如射频识别芯片。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，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何组合。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在读卡器313的范围内时，通过NFC与客户端设备310的读卡器313通信。在其他示例中，可以通过物理接口(例如，通用串行总线接口或刷卡接口)来实现与非接触式卡305的通信。

[0072] 系统300可以包括客户端设备310，客户端设备310可以是支持网络的计算机。如本文所述，支持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、网络家电、个人计算机、工作站、移动设备、电话、手持PC、个人数字助理、瘦客户端、胖客户端、因特网浏览器或其他设备。一个或多个客户端设备310也可以是移动设备；例如，移动设备可以包括来自Apple®的的iPhone、iPod、iPad或运行苹果的iOS®操作系统的任何其他移动设备、运行微软Windows®Mobile操作系统的任何设备、运行谷歌的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。

[0073] 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进行通信。客户端设备310可以例如从在客户端设备310上执行的应用程序311向一个或多个服务器320和325传送一个或多个请求。一个或多个请求可以是与从一个或多个服务器320和325检索数据相关联的。服务器320和325可以接收来自客户端设备310的一个或多个请求。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传送到客户端设备310，所接收的数据是响应于一个或多个请求的。

[0074] 系统300可以包括一个或多个硬件安全模块(HSM)330。例如，一个或多个HSM 330可以被配置为执行本文公开的一个或多个密码操作。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，这些专用安全设备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决不会在HSM 330之外泄露，而是保持在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操作中的至少一个。一个或多个HSM 330可以包含在服务器320和325内，或者可以与服务器320和325进行数据通信。

[0075] 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意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可以包括光纤网络、无源光网络、线缆网络、蜂窝网络、互联网、卫星网络、无线LAN、全球移动通信、个人通信服务、个人局域网、无线应用协议、多媒体消息收发服务、增强型消息收发服务、短消息服务、基于时分复用的系统、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、RFID、Wi-Fi和/或其网络的任何组合中的一个或多个。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和运营商之间的蜂窝网络以及运营商和后端之间的因特网。

[0076] 此外，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、无线个人区域网、局域网或诸如因特网的全球网络。此外，网络315可以支持因特网、无线通信网络、蜂窝网络等，或者它们的任意组合。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可以转换到网络设备的一个或多个协议，或者从其他协议转换到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，但是应当理解的是，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、线缆电视网络、诸如信用卡协会网络的公司网络、以及家庭网络。

[0077] 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程序311，并且包括一个或多个处理器312以及一个或多个读卡器313。例如，一个或多个应用程序311(诸如软件应用程序)可以被配置为实现例如与系统300的一个或多个组件的网络通信，并传送和/或接收数据。应当理解的是，尽管在图3中仅示出了客户端设备310的组件的单个实例，但是可以使用任何数量的设备310。读卡器313可以被配置为从非接触式卡305读取和/或与该非接触式卡通信。结合一个或多个应用程序311，读卡器313可以与非接触式卡305通信。

[0078] 客户端设备310中的任何一个的应用程序311可以使用短程无线通信(例如，NFC)与非接触式卡305通信。应用程序311可以被配置为与被配置为与非接触式卡305进行通信的客户端设备310的读卡器313对接。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。

[0079] 在一些实施例中，应用程序311通过关联的读取器(例如，读卡器313)与非接触式卡305进行通信。

[0080] 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的读卡器313与应用程序311通信。通信(例如，卡靠近客户端设备310的读卡器313进行轻击)允许应用程序311读取与卡相关联的数据并执行激活。在一些情况下，轻击可以激活或启动应用程序311，并且然后发起一个或多个动作或与账户服务器325的通信，以激活卡供后续使用。在一些情况下，如果应用程序311没有安装在客户端设备310上，则将卡靠着读卡器313进行的轻击可以发起应用程序311的下载(例如，导航到应用程序下载页面)。在安装之后，轻击卡可以激活或启动应用程序311，并且然后(例如，经由应用程序或其他后端通信)发起卡的激活。在激活后，卡可以用于各种交易，包括商业交易。

[0081] 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，应用程序311可以通过访问在客户端设备310上实施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。

[0082] 服务器320可以包括与数据库335通信的web服务器。服务器325可以包括账户服务器。在一些示例中，服务器320可以被配置为通过与数据库335中的一个或多个凭证进行比较来验证来自非接触式卡305和/或客户端设备310的一个或多个凭证。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，诸如支付和交易。

[0083] 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可以包括类似于图2中引用的发送设备205和接收设备210的发送设备和接收设备。

[0084] 例如，发送者和接收者可能期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，尽管可以包括这些两方，但是应当理解的是，可以涉及一个或多个发送设备和一个或多个接收设备，只要每方共享相同的共享秘密对称密钥。在一些示例中，发送设备和接收设备可以被提供有相同的主对称密钥。进一步，应当理解的是，持有相同秘密对称密钥的任何一方或设备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秘密对称密钥，该共享秘密对称密钥对除了参与交换安全数据的发送设备和接收设备之外的所有方保持是秘密的。还应当理解的是，发送设备和接收设备两者可以被提供有相同的主对称密钥，并且还应当理解的是，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。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改变的数字。

[0085] 在框410，发送设备和接收设备可以被提供有相同的主密钥，诸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，发送方可以更新计数器。此外，发送设备可以选择适当的对称加密算法，该对称加密算法可以包括对称加密算法、HMAC算法和CMAC算法中的至少一个。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加密算法。对称算法的非限制性示例可以包括对称加密算法，诸如3DES或AES128；对称HMAC算法，诸如HMAC-SHA-256；以及对称CMAC算法，诸如AES-CMAC。应当理解的是，如果所选择的对称算法的输出没有生成足够长的密钥，则诸如利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以产生多个输出，这些输出可以根据需要进行组合以产生足够长的密钥。

[0086] 发送设备可以采用所选择的加密算法，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。

[0087] 在框420，发送设备然后可以使用主对称密钥利用所选择的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。多样化对称密钥可以用于在将结果传送到接收设备之前处理敏感数据。例如，发送设备可以使用多样化对称密钥、使用对称加密算法来加密敏感数据，其中输出包括受保护的加密数据。发送设备然后可以将受保护的加密数据连同计数器值一起传送到接收设备以便进行处理。在一些示例中，可以执行除加密之外的密码操作，并且在传送到受保护数据之前，可以使用多样化对称密钥来执行多个密码操作。

[0088] 在某些示例中，计数器值可能未加密。在这些示例中，可以在框420处在发送设备和接收设备之间发送计数器值而没有加密。

[0089] 在框430，可以使用一个或多个加密算法和多样化密钥来保护敏感数据。多样化会话密钥(其可以通过使用计数器的密钥多样化来创建)可以与一个或多个加密算法一起使用来保护敏感数据。例如，可以使用第一多样化会话密钥，通过MAC处理数据，并且可以使用第二多样化会话密钥来加密所得到的输出，从而产生受保护的数据。

[0090] 在框440，接收设备可以使用计数器值作为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的相同的多样化对称密钥值。例如，接收设备可以使用计数器独立地创建其自己的第一多样化会话密钥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操作来处理最终的数据。

[0091] 在框450，接收设备可以利用一个或多个密码算法来使用多样化密钥以验证受保护的数据。

[0092] 在框460，可以验证原始数据。如果MAC操作的输出(通过使用第一个多样化会话密钥的接收设备)与解密揭示的MAC输出匹配，则可以认为该数据有效。

[0093] 下一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，这产生不同的多样化对称密钥。通过利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两者可以独立地产生相同的多样化对称密钥。这种多样化的对称密钥(而不是主对称密钥)用于保护敏感数据。

[0094] 如以上所解释的，发送设备和接收设备两者最初各自拥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。由于多样化的对称密钥是由发送设备和接收设备两者独立创建的，因此它决不会在双方之间传送。因此，攻击者不能截取多样化对称密钥，并且攻击者决不会看到利用主对称密钥处理的任何数据。只有较小的计数器值是利用主对称密钥处理的，而敏感数据不是利用主对称密钥处理的。因此，所揭示的关于主对称密钥的边信道数据被减少。而且，发送者和接收者可以例如通过事先安排或其他方式来商定多久创建一次新的多样化值并且因此创建新的多样化对称密钥。在实施例中，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，并因此创建新的多样化对称密钥。

[0095] 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随机数，该随机随机数从发送设备传送到接收设备；从发送设备和接收设备发送的计数器值的全部值；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维护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；敏感数据的加密哈希。在一些示例中，可以由各方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。

[0096] 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获得多个多样化密钥值。可以每当需要时创建新的多样化值，以及因此创建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敏感数据的每次交换创建新的多样化值。实际上，这可能会创建一次

性使用的密钥，诸如单个会话密钥。

[0097] 在其他示例中，诸如为了限制主对称密钥的使用次数，可以由发送设备的发送者和接收设备的接收者商定：新的多样化值并且因此新的多样化对称密钥将仅周期性地发生。在一个示例中，这可以是在预定次数的使用(诸如在发送设备和接收设备之间每10次传输)之后。在另一示例中，这可以是在某个时间段之后、传输之后的某个时间段之后，或者周期性地(例如，每天在指定时间；每周在指定日期的指定时间)。在另一示例中，这可以是每当接收设备向发送设备发信号通知它期望在下一次通信中改变密钥时。这可以根据策略来控制，并且可以由于例如由接收设备的接收者所感知的当前风险水平而变化。

[0098] 图5A示出了一个或多个非接触式卡500，该一个或多个非接触式卡可以包括由显示在卡500的正面或背面的服务提供商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标识卡。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可以包括基底510，该基底可以包括由塑料、金属和其他材料构成的单层或一个或多个层压层。示例性基底材料包括聚氯乙烯、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500可以具有符合ISO/IEC 7810标准的ID-1格式的物理特性，并且非接触式卡可以另外符合ISO/IEC 14443标准。然而，应当理解的是，根据本公开的非接触式卡500可以具有不同的特性，并且本公开不要求非接触式卡实施为支付卡。

[0099] 非接触式卡500还可以包括显示在卡的正面和/或背面的识别信息515，以及接触垫520。接触垫520可被配置为与另一通信设备(诸如用户设备、智能电话、膝上型电脑、台式电脑或平板电脑)建立联系。非接触式卡500还可以包括处理电路、天线和图5A中未示出的其他组件。这些组件可以位于接触垫520的后面或者基底510上的其他地方。非接触式卡500还可以包括可以位于卡的背面上(图5A中未示出)的磁条或磁带。

[0100] 如图5B所示，图5A的接触垫520可以包括用于存储和处理信息的处理电路525，该处理电路包括微处理器530和存储器535。应当理解的是，处理电路525可以包含执行本文描述的功能所必需的附加组件，包括处理器、存储器、错误和奇偶校验/CRC检查器、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。

[0101] 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。只读存储器可以是工厂可编程的只读存储器或一次性可编程存储器。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芯片出厂后的某个时间点进行编程。一旦存储器被编程，它会无法重写，但它可以被多次读取。读/写存储器出厂后可以进行多次编程和重新编程。它也可以被多次读取。

[0102] 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和客户标识符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卡小应用程序。然而，应理解，小应用程序540不限于Java卡小应用程序，而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可以标识

客户和分配给该客户的账户两者，并且可以进一步标识与该客户的账户相关联的非接触式卡。

[0103] 参照接触垫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。应当理解的是，这些元件可以在垫520之外实施、或者与该垫完全分离、或者作为位于接触垫520内的处理器530和存储器535元件之外的其他元件。

[0104] 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可以放置在非接触式卡500内并且在接触垫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是一体的，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可以在接触垫520和处理电路525的外部。

[0105] 在实施例中，非接触式卡500的线圈可以充当空芯变压器的次级线圈。终端可以通过切断电力或调幅与非接触式卡500通信。非接触式卡500可以使用非接触式卡的电力连接件中的间隙来推断从终端传送的数据，该电力连接可以通过一个或多个电容器在功能方面进行保持。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通信。可以通过干扰在终端线圈中检测负载调制。

[0106] 如以上解释的，非接触式卡500可以构建在可在智能卡或具有有限的存储器的其他设备(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程序或小应用程序。小应用程序可以被添加到非接触式卡中，以在各种基于移动应用程序的用例中为多因素认证(multifactor authentication，MFA)提供一次性密码(one-time password，OTP)。小应用程序可以被配置为响应来自读取器(诸如移动NFC读取器)的一个或多个请求(诸如近场数据交换请求)，并且产生包括被编码为NDEF文本标签的加密安全OTP的NDEF消息。

[0107] 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众所周知的类型文本标签。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：众所周知类型、文本、编码英语(en)、小应用程序ID：D2760000850101；功能：只读访问；编码：认证消息可以编码为ASCII十六进制；类型-长度-值(TLV)数据可以被提供为可以用于生成NDEF消息的个性化参数。在实施例中，认证模板可以包括具有用于提供实际动态认证数据的众所周知的索引的第一记录。

[0108] 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，如果要添加附加标签，则第一字节可以改变以指示消息开始，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>。

[0109] 在一些示例中，可以通过在安全通道协议2下实施STORE DATA(E2)，从而在个性化时将数据存储在非接触式卡中。一个或多个值可以由个性化局从(在由小应用程序ID指定的部分中的)EMBOSS文件读取，并且一个或多个存储数据命令可以在认证和安全信道建立之后被传送到非接触式卡。

[0110] pUID可以包括16位BCD编码的数字。在一些示例中，pUID可以包括14个数字。

[0111]

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
卡共享的随机数	4 字节	否	4 字节真实随机数（预生成的）
NTLV	X 字节	否	用于 NDEF 消息的 TLV 数据

[0112] 在一些示例中，一个或多个小应用程序可以被配置为保持其个性化状态，以仅在解锁且认证的情况下才允许个性化。其他状态可以包括标准状态预个性化。在进入终止状态时，一个或多个小应用程序可以被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被配置为停止响应所有应用协议数据单元(APDU)请求。

[0113] 一个或多个小应用可以被配置为维护可以在认证消息中使用的小应用程序版本(2字节)。在一些示例中，这可以被解释为最高有效字节主版本、最低有效字节次版本。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。对于次版本，除了错误修复、安全强化等之外，这可以包括不对认证消息或加密算法进行更改，以及不对静态标签内容进行更改。

[0114] 在一些示例中，一个或多个小应用程序可以被配置为仿真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，呈现可以指示非接触式卡的真实性的不同的加密数据。基于一个或多个应用程序，可以处理标签的NFC读取，可以将令牌传送到诸如后端服务器的服务器，并且可以在服务器处验证令牌。

[0115] 在一些示例中，非接触式卡和服务器可以包括使得卡可以被正确标识的某些数据。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，计数器可以被配置为更新。在一些示例中，每次读取卡时，卡会被传送到服务器以便进行验证，并确定计数器是否相等(作为验证的一部分)。

[0116] 一个或多个计数器可以被配置为防止重放攻击。例如，如果已经获得并重放密码，如果计数器已经被读取、使用，则该密码立即被拒绝或以其他方式被忽略。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不同于被更新用于交易的计数器。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，该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。

[0117] 在一些示例中，计数器可能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,从而使得计数器被更新,并且由非接触式卡生成新的通信,但是该通信可以不被传送到一个或多个处服务器处进行处理。这可能导致非接触式卡的计数器和一个或多个服务器处维护的计数器脱离同步。这可能会无意地发生,包括例如,在卡保存在靠近设备(例如,被携带在带有设备的袋中)的情况下,以及在非接触式卡以一定角度被读取的情况下,可能包括卡未对准或未被定位成使得非接触式卡在NFC场中被上电但不可读。如果非接触式卡被定位为靠近设备,则设备的NFC场可以被打开以向非接触式卡供电,从而导致其中的计数器被更新,但是设备上没有应用程序接收该通信。

[0118] 为了保持计数器同步,可以执行应用程序(诸如后台应用程序),该应用程序将被配置为检测移动设备何时醒来并与指示由于检测而发生读取的一个或多个服务器同步,然后使计数器向前计数。由于非接触式卡的计数器和一个或多个服务器的计数器可能脱离同步,所以一个或多个服务器可以被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次数或预定次数,并且仍然被认为是有效的。例如,如果计数器被配置为对于每次出现指示非接触式卡激活而递增(或递减)1,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为有效,或者允许阈值范围(例如,从1到10)内的任何计数器值。此外,一个或多个服务器被配置为:如果其读取的计数器值已超过10但是低于另一阈值范围值(诸如1000),则请求与非接触式卡相关联的手势,诸如用户轻击。通过用户轻击,如果计数器值在期望或接受范围内,则认证成功。

[0119] 图8是示出根据示例实施例的密钥操作800的流程图。如图8所示,在框810,两个发卡行识别码(bank identifier number,BIN)级主密钥可以与账户标识符和卡序列号结合使用,以每张卡产生两个唯一派生密钥。在一些示例中,发卡行识别码可以包括一个编号或一个或多个编号的组合(诸如由一个或多个服务器提供的账号或不可预测的编号),其可以用于会话密钥生成和/或多样化。在个性化过程期间,UDK(AUTKEY和ENCKEY)可以存储在卡上。

[0120] 在框820,计数器可以被用作多样化数据,由于它随着每次使用而改变,并且每次提供不同的会话密钥,这与针对每个卡产生唯一的一组密钥的主密钥派生相反。在一些示例中,优选的是针对两种操作都使用4字节方法。因此,在框820,可以为来自UDK的每个交易创建两个会话密钥,即,来自AUTKEY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,根据AUTKEY创建的会话密钥),OTP计数器的两个字节的低位可以用于多样化。对于ENC密钥(即,根据ENCKEY创建的会话密钥),可以将OTP计数器的全长用于ENC密钥。

[0121] 在框830,MAC密钥可以用于准备MAC密码,而ENC密钥可以用于对密码进行加密。例如,MAC会话密钥可以用于准备密码,并且结果可以在其被传送到一个或多个服务器之前利用ENC密钥进行加密。

[0122] 在框840,简化了MAC的验证和处理,因为在支付HSM的MAC认证功能中直接支持2字节的多样化。密码的解密是在MAC验证之前执行的。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)可以用于对数据进行解密,而第一派生密钥(即,MAC会话密钥)可以用于对解密的数据进行验证。

[0123] 对于非接触式卡,将派生出不同的唯一标识符,其可以与卡中编码的应用程序主

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,将其与主密钥一起作为输入,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(卡密码生成/认证密钥-Card-Key-Auth),并且可以进一步被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(卡数据加密密钥-Card-Key-DEK),并且可以进一步被多样化以创建在加密和解密加密数据时使用的ENC会话密钥。在一些示例中,可以通过将发行者主密钥与卡的唯一ID号(pUID)和支付小应用程序的PAN序列号(PAN sequence number,PSN)相结合而将发行者主密钥多样化来创建第一密钥和第二密钥。pUID可以包括16位数字值。如以上解释的,pUID可以包括16位BCD编码的数字。在一些示例中,pUID可以包括14位数字值。

[0124] 在一些示例中,由于EMV会话密钥派生方法可以在2^16次使用时结束,所以诸如全32位计数器的计数器可以被添加到多样化方法的初始化数组中。

[0125] 在诸如信用卡的其他示例中,编号(诸如账号或由一个或多个服务器提供的不可预测的编号)可以用于会话密钥生成和/或多样化。

[0126] 图9示出了被配置为实施本公开的一个或多个实施例的系统900的示意图。如以下解释的,在非接触式卡创建过程期间,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,该算法由非接触式卡中的硬件实施。通过使用密钥多样化过程,可以基于针对需要密钥的每个实体的可唯一标识信息,从主密钥派生出一个或多个密钥。

[0127] 关于主密钥管理,对于发行一个或多个小应用程序的选集(portfolio)的每个部分,会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),并且第二主密钥910可以包括发行者数据加密密钥(Iss-Key-DEK)。如本文进一步解释的,两个发行者主密钥905、910被多样化为卡主密钥925、930,其对于每个卡都是唯一的。在一些示例中,可以将网络配置文件记录ID(pNPR)915和派生密钥索引(pDKI)920作为后台数据,该后台数据可以用于标识在加密过程中使用哪个发行者主密钥905、910,以便进行认证。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pNPR915和pDKI 920的值。

[0128] 在一些示例中,为了增加解决方案的安全性,可以派生会话密钥(诸如每个会话的唯一密钥),但不是使用主密钥,而是唯一的卡派生密钥和计数器可以被用作多样化数据,如以上所解释的。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,用于生成密码和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,并且利用一个或多个算法、使用应用程序交易计数器(pATC)945对会话密钥进行派生。为了使数据适合一个或多个算法,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可以包括3DES ECB,并且MK可以包括卡唯一派生的主密钥。

[0129] 如本文所述,可以使用pATC 945计数器的较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击时，pATC 945被配置为被更新，并且卡主密钥Card-Key-AUTH 925和Card-Key-DEK 930被进一步多样化为会话密钥Aut-Session-Key 935和DEK-Session-KEY 940。pATC 945可以在个性化或小应用程序初始化时初始化为零。在一些示例中，pATC计数器945可以在个性化时或之前初始化，并且可以被配置为在每次NDEF读取时递增1。

[0130] 进一步，每个卡的更新可以是唯一的，并且可以通过个性化来分配，或者通过pUID或其他标识信息在算法上进行分配。例如，奇数编号的卡可以递增或递减2，而偶数编号的卡可以递增或递减5。在一些示例中，更新也可以在顺序读取时变化，使得一个卡可以按顺序递增1、3、5、2、2、……重复。特定序列或算法序列可以在个性化时定义，或者根据一个或多个过程从唯一标识符派生出。这使得重放攻击者更难从较少数量的卡实例中进行归纳。

[0131] 认证消息可以作为呈十六进制ASCII格式的文本NDEF记录的内容传递。在一些示例中，可以仅包括认证数据和8字节随机数(后跟认证数据的MAC)。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。在另外的示例中，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，可以添加附加的8字节块来匹配由MAC算法产生的块。作为另一示例，如果所采用的算法使用16字节的块，甚至可以使用该块大小的倍数，或者输出可以被自动或手动填充到该块大小的倍数。

[0132] MAC可以通过功能密钥(AUT-Session-Key)935来执行。密码中指定的数据可以利用javacard.signature方法:ALG_DES_MAC8_ISO9797_1_M2_ALG3处理，从而与EMV ARQC验证方法相关。如以上解释的，用于这个计算的密钥可以包括会话密钥AUT-Session-Key 935。如以上解释的，计数器的低阶两个字节可以用于使一个或多个MAC会话密钥多样化。如以下解释的，AUT-Session-Key935可以用于MAC数据950，并且可以使用DEK-Session-Key 940对所得到的数据或密码A 955和随机数RND进行加密，以创建在消息中发送的密码B或输出960。

[0133] 在一些示例中，可以处理一个或多个HSM命令用于解密，使得最终的16(二进制、32十六进制)字节可以包括使用CBC模式的3DES对称加密，其中随机数的第四个零后面是MAC认证数据。用于这种加密的密钥可以包括从Card-Key-DEK 930派生出的会话密钥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pATC 945的最低有效字节。

[0134] 下面的格式表示二进制版本示例实施例。进一步，在一些示例中，第一个字节可以被设置为ASCII‘A’。

[0135]

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 的				
2	8	4	4	18 字节输入数据
版本	pUID	pATC	共享秘密	

[0136]

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

密码 A (MAC)	**8 字节**			
MAC 的				
2	8	4	4	18 字节输入数据
版本	pUID	pATC	共享秘密	

密码 B	**16**		
对称加密的			
8	8		
随机数	密码 A		

[0137] 另一示例性格式在下文示出。在这个示例中，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)

8 字节				
8	8	4	4	18 字节输入数据
pUID	pUID	pATC	共享秘密	

[0140]

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	共享秘密	
密码 B	**16**			
对称加密的				
8	8			
随机数	密码 A			

[0141] 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派生出该特定卡的卡主密钥(Card-Key-Auth 925和Card-Key-DEK930)。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)字段可以用于派生该特定卡的会话密钥(Aut-Session-Key935和DEK-Session-Key 940)。密码B 960可以使用DEK-Session-KEY进行解密,这产生密码A 955和RND,并且RND可以被丢弃。UID字段可以用于查找非接触式卡的共享秘密,该共享秘密与消息的Ver、UID和pATC字段一起可以通过密码MAC、使用重新创建的Aut-Session-Key进行处理,以创建MAC输出,诸如MAC'。如果MAC'与密码A 955相同,则这表明消息解密和MAC检查全部已通过。然后,可以读取pATC以确定它是否有效。

[0142] 在认证会话期间,一个或多个应用程序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(诸如Aut-Session-Key 935)使用具有方法2填充的ISO 9797-1算法3,将一个或多个密码生成为3DES MAC。输入数据950可以采取以下形式:版本(2),pUID(8),pATC(4),共享秘密(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,共享秘密可以由一个或多个随机数发生器生成,该随机数发生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,共享秘密可以包括在个性化时注入到卡中的随机4字节二进制数,其为认证服务所知。在认证会话期间,共享秘密可以不从一个或多个小应用程序提供给移动应用程序。方法2填充可以包括将强制性0x'80'字节添加到输入数据的末尾,以及将0x'00'字节添加到结果数据的末尾,直到8字节边界。所得的密码可以包括8个字节的长度。

[0143] 在一些示例中,利用MAC密码将非共享随机数加密为第一块的一个益处是,在使用对称加密算法的CBC(块链接)模式时,其充当初始化向量。这允许逐块地"加扰",而不必预先建立固定的或动态的IV。

[0144] 通过将应用程序交易计数器(pATC)包括作为包括在MAC密码中的数据的一部分,认证服务可以被配置为确定明文数据中输送的值是否已经被篡改。此外,通过将版本包含在一个或多个密码中,攻击者难以在试图降低加密解决方案的强度时有目的地篡改应用程序版本。在一些示例中,pATC可以从零开始,并在每次一个或多个应用程序生成认证数据时更新1。认证服务可以被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

据使用等于或低于由认证服务接收的先前值的pATC时，这可能被解释为试图重放旧消息，并且被认证的消息可能被拒绝。在一些示例中，当pATC大于先前接收的值时，可以对其进行评估以确定它是否在可接受的范围或阈值内，并且如果它超过范围或阈值或在范围或阈值之外，则验证可以被认为已经失败或不可靠。在MAC操作936中，使用Aut-Session-Key 935、通过MAC处理数据950，以产生加密的MAC输出(密码A)955。

[0145] 为了提供针对暴露卡上密钥的暴力攻击的附加保护，期望的是对MAC密码955进行加密。在一些示例中，密文中包括的数据或密码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发生器生成，该随机数发生器可以被配置为通过一个或多个安全过程来确保随机数是不可预测的。用于加密这个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，以产生加密的数据，即密码B 960。可以在密文块链接模式下使用3DES对数据955加密，以确保攻击者必须对全部密文进行任何攻击。作为非限制性示例，可以使用其他算法，诸如高级加密标准(Advanced Encryption Standard，AES)。在一些示例中，可以使用0x'0000000000000000'的初始化向量。试图强行破解用于加密这个数据的密钥的任何攻击者将无法确定何时已经使用了正确的密钥，因为正确解密的数据由于其随机出现而无法与不正确解密的数据区分开来。

[0146] 为了使认证服务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以明文的方式将以下数据从一个或多个小应用程序传递到移动设备：版本号，用于确定所使用的密码方法和用于密码的验证的消息格式，这使得该方法在将来能够改变；pUID，用于检索密码资产，并派生卡密钥；以及pATC，用于派生用于密码的会话密钥。

[0147] 图10示出了用于生成密码的方法1000。例如，在框1010，可以使用网络配置文件记录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，以便进行认证。在一些示例中，该方法可以包括执行如下的认证：在认证时检索非接触式卡的pNPR和pDKI的值。

[0148] 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。

[0149] 在框1030，可以通过使发行者主密钥多样化以生成可以用于生成MAC密码的会话密钥，来创建Card-Key-Auth和Card-Key-DEK(唯一卡密钥)。

[0150] 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，从而得到会话密钥Aut-Session-Key和DEK-Session-Key。

[0151] 图11描绘了示出根据一个示例的密钥多样化的示例性过程1100。最初，发送者和接收者可以被提供有两个不同的主密钥。例如，第一主密钥可以包括数据加密主密钥，并且第二主密钥可以包括数据完整性主密钥。发送者具有可以在框1110处被更新的计数器值以及发送者可以与接收者安全共享的其他数据(诸如要保护的数据)。

[0152] 在框1120，计数器值可以由发送者使用数据加密主密钥进行加密，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进行加密，以产

生数据完整性派生的会话密钥。在一些示例中，在两次加密期间，可以使用整个计数器值或计数器值的一部分。

[0153] 在一些示例中，计数器值可能未加密。在这些示例中，计数器可以在发送者和接收者之间以明文的方式传送，即没有加密。

[0154] 在框1130，发送者使用数据完整性会话密钥和密码MAC算法，利用密码MAC操作来处理要保护的数据。受保护的数据(包括明文和共享秘密)可以被用于使用会话密钥之一(AUT-Session-Key)来产生MAC。

[0155] 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，将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)对其进行加密。

[0156] 在框1150，将加密的MAC与足够的信息从发送者传送到接收者，以标识用于验证密码的附加秘密信息(例如共享秘密、主密钥等)。

[0157] 在框1160，接收方使用接收到的计数器值来如上所述从两个主密钥独立地派生出两个派生的会话密钥。

[0158] 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。然后将对交换的数据进行其他处理。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。

[0159] 在框1180，将数据完整性派生的会话密钥与加密MAC操作结合使用，以验证受保护的数据尚未被修改。

[0160] 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。如果解密成功并产生正确的MAC值，则MAC才可能是正确的。成功解密可以表明正确派生的加密密钥已用于解密加密的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进行了加密的非接触式卡确实是真实的。此外，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。

[0161] 此后，可以丢弃两个派生的会话密钥，并且数据交换的下一个迭代将更新计数器值(返回到框1110)，并且可以创建新的一组会话密钥(在框1120)。在一些示例中，可以丢弃组合的随机数据。

[0162] 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程序登录并验证用户。作为第二过程，响应于经由一个或多个应用程序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，安全因素认证可以既包括安全地证明用户的身份，又包括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击手势。在一些示例中，一个或多个轻击手势可以包括用户将非接触式卡对着设备进行轻击。在一些示例中，该设备可以包括移动设备、信息亭、终端、平板电脑或被配置为处理接收到的轻击手势的任何其

他设备。

[0163] 在一些示例中，可以将非接触式卡对着设备(诸如一个或多个计算机信息亭或终端)轻击，以验证身份，从而接收响应于购买的交易物品，诸如咖啡。通过使用非接触式卡，可以建立在忠诚计划(loyalty program)中证明身份的安全方法。以不同于仅仅扫描条码卡的方式来建立安全地证明身份，例如以获得奖励、优惠券、优惠等或益处的接收。例如，加密的交易可以发生在非接触式卡和设备之间，该设备可以被配置为处理一个或多个轻击手势。如以上解释的，一个或多个应用程序可以被配置为验证用户的身份，并且然后使用户例如经由一个或多个轻击手势来行动或对其进行响应。在一些示例中，数据例如奖金积分、忠诚度积分、奖励积分、医疗保健信息等可以被写回到非接触式卡。

[0164] 在一些示例中，可以将非接触式卡对着诸如移动设备的设备轻击。如以上解释的，用户的身份可以由一个或多个应用程序验证，然后该应用程序将基于身份的验证向用户授予期望的益处。

[0165] 在一些示例中，可以通过对着诸如移动设备的设备轻击来激活非接触式卡。例如，非接触式卡可以通过NFC通信、经由设备的读卡器与设备的应用程序进行通信。在通信中，卡靠近设备的读卡器进行轻击，可以允许设备的应用程序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、访问账户或受限信息、或其他功能。在一些示例中，轻击可以激活或启动设备的应用程序，并且然后发起一个或多个动作或与一个或多个服务器的通信来激活非接触式卡。如果该应用程序没有安装在该设备上，则在读卡器附近轻击非接触式卡可以发起该应用程序的下载，诸如导航到该应用程序的下载页面。安装之后，轻击非接触式卡可以激活或启动应用程序，并且然后例如经由应用程序或其他后端通信发起非接触式卡的激活。激活后，非接触式卡可以用于各种活动，包括但不限于商业交易。

[0166] 在一些实施例中，专用应用程序可以被配置为在客户端设备上运行，以执行非接触式卡的激活。在其他实施例中，网络门户、基于web的应用程序、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)之间的媒介。根据一些实施例，在提供激活时，应用程序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、智能手机、平板电脑或销售点(point-of-sale，POS)设备)。进一步，取决于所涉及的设备类型，该应用程序可以向账户服务器输出不同的和/或附加的数据用于传输。例如，这样的数据可以包括与商家相关联的信息，诸如商家类型、商家ID、以及与设备类型本身相关联的信息，诸如POS数据和POS ID。

[0167] 在一些实施例中，示例认证通信协议可以模仿通常在交易卡和销售点设备之间执行的、具有一些修改的EMV标准的离线动态数据认证协议。例如，因为示例认证协议本身不用于完成与卡发行者/支付处理器的支付交易，所以某些数据值是不需要的，并且可以在不涉及与卡发行者/支付处理器的实时在线连接的情况下执行认证。如本领域所知，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。然而，在本公开的某些实施例中，源自移动设备的交易缺少与POS系统相关联的交易值。因此，在一些实施例中，伪交易值(即，卡发行者可识别的并且足以允许激活发生的值)可以作为示例认证通信协议的一部分而通过。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。超出缓冲区值的尝试次数可能会导致软拒绝

(soft decline);软拒绝在接受交易前需要进一步验证。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。

[0168] 在一些示例中,非接触式卡可以根据接收方设备选择性地传送信息。一旦轻击,非接触式卡就可以识别轻击所指向的设备,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。这有利地允许非接触式卡仅传送完成即时动作或交易(诸如支付或卡认证)所需的信息。通过限制数据传输和避免不必要的数据传输,可以提高效率和数据安全性两者。信息的识别和选择性传送可以应用于各种场景,包括卡激活、余额转移、账户访问尝试、商业交易和逐步(step-up)欺诈减少。

[0169] 如果非接触式卡轻击是针对运行苹果iOS®操作系统的设备(例如iPhone、iPod或iPad)进行的,则非接触式卡可以识别iOS®操作系统并传送适当的数据来与这个设备通信。例如,非接触式卡可以经由例如NFC提供使用NDEF标签认证卡所需的加密的身份信息。类似地,如果非接触式卡轻击是针对运行Android®操作系统的设备(例如,Android®智能手机或平板电脑)进行的,则非接触式卡可以识别Android®操作系统,并传送适当的数据(诸如,通过本文描述的方法进行认证所需的加密的身份信息)以与这个设备通信。

[0170] 作为另一示例,非接触式卡轻击可以是针对POS设备(包括但不限于信息亭、结账登记器、支付站或其他终端)进行的。在执行轻击时,非接触式卡可以识别POS设备,并且仅传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,非接触式卡可以根据EMV标准传送完成交易所需的支付信息。

[0171] 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,例如设备特定的信息、位置特定的信息和交易特定的信息。例如,一旦POS设备从非接触式卡接收到数据通信,POS设备就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。

[0172] 在一些示例中,POS设备可以附属于授权商家或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其他实体。然而,应当理解的是,所描述的方法的执行不要求这种附属关系。

[0173] 在一些示例中,诸如购物商店、杂货店、便利店等,可以在移动设备上轻击非接触式卡而不必打开应用程序,以指示利用奖励积分、忠诚度积分、优惠券、优惠等中的一个或多个来覆盖一次或多次购买的期望或意图。因此,提供了购买背后的意图。

[0174] 在一些示例中,一个或多个应用程序可以被配置为确定它是经由非接触式卡的一个或多个轻击手势启动的,使得启动发生在下午3:51、交易在下午3:56处理或发生,以便验证用户的身份。

[0175] 在一些示例中,一个或多个应用程序可以被配置为响应于一个或多个轻击手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、确定最便宜的购买和/或实时地重新配置到另一动作。

[0176] 在一些示例中,可以对轻击行为收集数据作为生物特征/手势认证。例如,密码安全且不易被截取的唯一标识符可以被传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。辅助信息可以包括关于用户的个人可标识信息。在一些示例中,辅助信息可以存储在非接触式卡中。

[0177] 在一些示例中,该设备可以包括在多个个人之间划分支付的账单或支票的应用程

序。例如,每个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。这些个人中的每一个可以经由应用程序在他们的设备上接收推送通知,以划分购买。可以使用其他非接触式卡,而不是接受仅一个卡轻击来指示支付。在一些示例中,具有不同金融机构的个人可能拥有非接触式卡,以提供信息来发起来自卡轻击个人的一个或多个支付请求。

[0178] 以下示例用例描述了本公开的特定实施方式的示例。这些仅旨在用于解释目的,而非用于限制目的。在一种情况下,第一个朋友(付款人)欠第二个朋友(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或需要经由端对端应用程序进行交换。收款人在其智能手机上登录到适当的应用程序,然后选择付款请求选项。作为响应,该应用程序请求通过收款人的非接触式卡进行认证。例如,应用程序输出一个显示,要求收款人轻击其非接触式卡。一旦收款人在具有所支持的应用程序的智能手机的屏幕上轻击他的非接触式卡,非接触式卡就会被读取和验证。接下来,应用程序显示付款人轻击他的非接触式卡以发送付款的提示。在付款人轻击其非接触式卡之后,应用程序读取卡信息,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,应用程序输出以便显示交易的状态指示符。

[0179] 在另一示例情况下,信用卡客户可以以邮件的方式接收新的信用卡(或借记卡、其他支付卡或需要激活的任何其他卡)。客户可以决定经由他或她的设备(例如,诸如智能手机的移动设备)上的应用程序来激活卡,而不是通过呼叫与卡发行者相关联的所提供的电话号码或访问网站来激活卡。客户可以从设备的显示器上显示的应用程序菜单中选择卡激活功能。该应用程序可以提示客户在屏幕上轻击他或她的信用卡。在将信用卡对着设备的屏幕轻击时,应用程序可以被配置为与服务器(诸如激活客户的卡的卡发行者服务器)通信。然后,应用程序可以显示指示卡的成功激活的消息。然后卡激活将完成。

[0180] 图12示出了根据示例实施例的用于卡激活的方法1200。例如,卡激活可以由包括卡、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引用前面参考图1A、图1B、图5A和图5B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。

[0181] 在框1210,卡可以被配置为动态地生成数据。在一些示例中,该数据可以包括诸如账号、卡标识符、卡验证值或电话号码的信息,这些信息可以从卡传送到设备。在一些示例中,数据的一个或多个部分可以经由本文公开的系统和方法加密。

[0182] 在框1220,动态生成的数据的一个或多个部分可以经由NFC或其他无线通信被传送到设备的应用程序。例如,在设备附近轻击卡可以允许设备的应用程序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,如果设备不包括帮助激活卡的应用程序,则轻击卡可以指引设备或提示客户到软件应用程序商店下载相关联的应用程序来激活卡。在一些示例中,可以提示用户将卡朝向设备的表面充分地做手势、放置或定向,诸如以某个角度或者平坦地放置在设备的表面上、附近或邻近该设备的表面。响应于卡的充分调整位置、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的部分传送到一个或多个服务器。

[0183] 在框1230,数据的一个或多个部分可以被传送到一个或多个服务器,诸如卡发行

者服务器。例如，数据的一个或多个加密的部分可以从设备传送到卡发行者服务器以激活卡。

[0184] 在框1240，一个或多个服务器可以经由本文公开的系统和方法解密数据的一个或多个加密的部分。例如，一个或多个服务器可以从设备接收加密的数据，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进行的对数据的一个或多个解密的部分的所得到的比较产生成功的匹配，则卡可以被激活。如果由一个或多个服务器进行的对数据的一个或多个解密部分的所得到的比较产生不成功的匹配，则可以发生一个或多个过程。例如，响应于不成功匹配的确定，可以提示用户再次轻击、刷或挥动卡。在这种情况下，可能存在包括准许用户激活卡的尝试次数的预定阈值。可替选地，用户可以接收一种通知，诸如在他或她的设备上的消息，该消息指示卡验证的不成功尝试并且用于呼叫、发邮件或文本信息的方式联系相关联的服务以帮助激活卡；或者另一种通知，诸如在他或她的设备上的电话呼叫，该电话呼叫指示卡验证的不成功尝试以及用于呼叫、发邮件或文本信息方式联系相关联的服务以帮助激活卡；或者另一种通知，诸如邮件，该邮件指示卡验证的不成功尝试并且用于呼叫、发邮件或文本信息的方式联系相关联的服务以帮助激活卡。

[0185] 在框1250，一个或多个服务器可以基于卡的成功激活来传送回传消息。例如，该设备可以被配置为接收来自一个或多个服务器的输出，其指示该一个或多个服务器对卡的成功激活。设备可以被配置为显示指示卡的成功激活的消息。一旦卡被激活，卡可以被配置为不继续动态生成数据，以避免欺诈性使用。以这样的方式，此后该卡可以不被激活，并且通知一个或多个服务器该卡已经被激活。

[0186] 在另一示例中，客户想要在他或她的手机上访问金融账户。客户在移动设备上启动应用程序(例如，银行应用程序)并输入用户名和密码。在此阶段，客户可能会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因素认证。因此，应用程序请求用户提供用于账户验证的交易卡(例如，信用卡)。然后，用户将其信用卡对着移动设备轻击，应用程序将验证该信用卡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。

[0187] 本文描述的系统和方法提供了非接触式卡，可以将该非接触式卡朝向移动设备做出手势以发起电话呼叫，将令牌传递到电话系统并激活非接触式卡。在一个示例中，这可以在不利用应用程序的情况下通过移动电话系统发生。因此，这些技术提供了多种好处，包括更有效的卡激活方式，为消费者和发行机构提供更高的安全性，以及消除了用户使用应用程序的需求。

[0188] 图13示出了卡激活系统1300，其包括非接触式卡1305、客户端设备1310和一个或多个服务器1320。尽管图13示出了组件的单个实例，但是系统1300可以包括任何数量的组件。非接触式卡1305、客户端设备1310和一个或多个客户端应用程序1316以及一个或多个服务器1320可以引用先前参考图1A、图1B、图5A和图5B说明的相同或相似的组件，例如非接触式卡105、客户端设备110和服务器120。

[0189] 非接触式卡1305可以包括一个或多个处理器1307和存储器1309。存储器1309可以

包括一个或多个小应用程序1311。在一些示例中，当将非接触式卡1305做出手势时，包括但不限于一个或多个手势，使得非接触式卡1305可以进入客户端设备1310的通信场(例如，NFC场)以建立通信(例如与之的NFC通信)，非接触式卡的一个或多个小应用程序1311可以生成可由客户端设备1310和/或一个或多个客户端应用程序1316读取的NDEF文件。客户端设备1310可以包括一个或多个处理器1312和存储器1314，并且可以包含一个或多个客户端应用程序1316，该客户端应用程序1316包括用于在客户端设备上执行的指令。一个或多个客户端应用程序1316可以是被配置为执行本文描述的客户端设备功能的软件应用程序。客户端设备1310和/或客户端应用程序1316可以经由通信接口(未示出)与非接触式卡1305进行数据通信。在一些示例中，一个或多个手势可以至少包括将非接触式卡进行轻击、挥动或其他手势，使得非接触式卡1305进入客户端设备1310的通信场。例如，可以将非接触式卡1305对着客户端设备(诸如移动设备)轻击，以发起电话呼叫。

[0190] NDEF文件可以发起与客户端设备1310上一个或多个客户端应用程序1316的一个或多个通信。如以下讨论的，非接触式卡1305的一个或多个小应用程序1311可以动态地生成信息，例如电话号码以及可以附加到电话号码的ID令牌或有效载荷。在一些示例中，可以使用电话号码向一个或多个服务器1320进行电话呼叫，并且一个或多个服务器1320可以被配置为监视电话呼叫并接收被解密的输入。例如，可以将NDEF文件从非接触式卡1305读取到客户端设备1310和/或一个或多个客户端应用程序1316，并且可以进行到电话系统的切换，该电话系统应答所述呼叫并接受数字或有效负载的自动输入，并将其传送到一个或多个服务器1320，在此呼叫被解密并认证，然后将其发送回电话系统，以指示成功认证或认证失败(带有一个或多个回退选项)。在某些示例中，所述呼叫不是基于IP的，即，不是使用IP语音(VoIP)或其他基于IP的呼叫机制进行的。一个或多个服务器1320可以与客户端设备1310和/或一个或多个客户端应用程序1316进行数据通信。

[0191] 在一些示例中，可以利用一个或多个过程来激活非接触式卡1305。示例性过程包括但不限于发起的电话呼叫。

[0192] 例如，可以生成被配置为在客户端设备1310上发起电话呼叫的链接。该电话呼叫可以由客户端设备1310的默认电话程序发起，或者在其他示例中，可以使用不同的或指定的电话程序。根据该链接，可以发起电话呼叫，然后是暂停，再然后可以提供ID令牌。以这种方式，非接触式卡1305可以被配置为发起电话呼叫。下面提供了一个示例性链接：

[0193] tel://1234567890,,,1234567##

[0194] 在一些示例中，链接可以包括一个或多个信息元素。在一些示例中，链接可以包括第一信息元素、第二信息元素和第三信息元素。例如，第一信息元素可以在第二信息元素之前，并且第二信息元素可以在第三信息元素之前。

[0195] 在实施例中，第一信息元素可以包括电话号码，例如(123)456-7890。在一些示例中，该号码可以是基于美国的，包括区号。在其他示例中，该号码可以是基于非美国的，例如，该号码可以进一步包括国家代码，并且可以导致拨打国际电话。在一些示例中，可以动态生成一个或多个电话号码，或者可以从预先配置的列表中检索一个或多个电话号码。呼叫的电话号码元素可以被硬编码为呼叫卡激活电话号码或其他服务，例如tel://1234567890。

[0196] 在实施例中，第二信息元素可以包括一个或多个字符，例如一个或多个逗号。在一

些示例中，一个或多个逗号可以被解释为一个或多个持续停顿。例如，停顿的持续时间可以包括固定的时间段，例如一秒。因此，如果逗号被解释为一秒钟的持续停顿，则包含四个逗号(如上述示例性链接)可能导致四秒钟的停顿。在一些示例中，逗号的数量可以足够长，以使电话系统能够收听和应答。如下所述，这可以使自动电话系统有时间响应呼叫并等待其他信息元素。

[0197] 在实施例中，该链路可以包括第三信息元素，该第三信息元素可以包括一个或多个有效载荷。例如，递送的有效载荷(例如1234567##)可以被配置为对非接触式卡进行认证。在某些示例中，该数字字符串可以以加密格式传递到电话系统中，并可以用密钥解密。如果解密过程失败(例如，由于静态或其他原因而导致数字丢失)，则此过程可能会触发一个或多个回退选项。例如，一个选项可以包括将呼叫路由到可以接听该呼叫的运营商或客户服务代表。在另一个示例中，另一个选项可以包括该过程可以被路由到另一个系统以输入非接触式卡的卡验证值，如下所述。

[0198] 在一些示例中，如果在非接触式卡1305激活期间使用了不正确的电话号码，则可以标记此事件并将其存储在数据库中以分析潜在的可疑对象。因此，未注册的电话号码可以表示欺诈活动的可能性更高。

[0199] 在一些示例中，诸如非接触式卡1305的卡验证值(CVV)之类的值可以被配置为激活非接触式卡1305。在其他示例中，可以提供比CVV方法更高的安全性，包括利用由一个或多个卡小应用程序1311生成的一次性密码(OTP)，该密码可以由一个或多个服务器加密和解密以认证非接触式卡1305。

[0200] 在一些示例中，电话系统可以解析来自电话呼叫的有效载荷，并将其经由一个或多个web应用程序传递以便进行解密。在一些示例中，令牌可以经由私钥/公钥来加密。例如，私钥可以用于解密数据，并且还可以安全地存储，从而可以在没有私钥的情况下(通过公钥)进行加密，这意味着私钥不需要被传递，因此不容易被第三方拦截。可以由一个或多个服务器1320检查和验证用于发起呼叫的号码，以便确定电话号码的有效性。因此，加密的数据可以被解密，并且非接触式卡1305已经被激活的通知或指示可以包括从一个或多个服务器1320向客户端设备1310和/或一个或多个客户端应用程序1316发送文本消息或电子邮件。

[0201] 在一些示例中，在非接触式卡1305已经被成功激活并且客户端设备1310的一个或多个客户端应用程序1316已经接收到指示激活的通知之后，非接触式卡1305可以被指令为禁用动态数据生成。在一些示例中，如上所述，在已经通过一个或多个过程之一激活了非接触式卡1305之后，可以选择性地将非接触式卡1305的用户导向客户支持，或者可以在POS设备或任何其他系统处使用非接触式卡1305。例如，如果用户使用激活的卡与POS设备进行交互，则可以指示非接触式卡1305停止动态生成号码。在一些示例中，这可能需要诸如支付小应用程序或交易小应用程序之类的小应用程序之间的通信，以指示非接触式卡1305的一个或多个其他小应用程序1311在下一次发生非接触式卡的一个或多个手势(非接触式卡1305凭借该手势进入客户端设备1310的通信场)时停止电话号码的生成。以这种方式，响应于非接触式卡1305的成功激活，非接触式卡1305的动态生成功能可以被关闭或禁用。

[0202] 举例来说，非接触式卡1305可以被配置为或者非接触式卡1305的有效载荷可以被配置为在接收有效载荷的客户端设备中引起以下一项或多项：(i)下载与非接触式卡1305

兼容的应用程序;(ii)在属于非接触式卡1305的用户的一个或多个账户之间转移余额或其他金额;(iii)重置与用户、非接触式卡1305相关联的个人识别码(PIN),或与非接触式卡1305的用户相关联的账户;(iv)将属于用户的账户与发行非接触式卡1305的实体链接,所述用户不是账户;(v)批准或引起从一个或多个帐户到与非接触式卡1305相关联的帐户或从与非接触式卡1305相关联的帐户进行的余额转移;(vi)向非接触式卡1305的发行者请求更换卡;(vii)请求或引起自动清算所(ACH)付款;(viii)批准或引起从或向对应于或属于非接触式卡1305的用户的账户进行电汇;(ix)注册、验证用户的注册或对用户进行认证,以允许与用户关联的帐户或非接触式卡1305附加到与设备1310相关联的付款服务上,包括但不限于ApplePay®、 SamsungPay®、AndroidPay®、GooglePay®、Venmo®或Paypal®;(x)请求与帐户相关联的活动,例如增加信用帐户的债务限额,请求加急交易(例如结算支票)或对交易提出异议。非限制性地,例如,可以通过使用配置有特定NDEF消息的非接触式卡1305来实现以上的一个或多个。

[0203] 在一些示例中,非接触式卡1305可以与客户端设备1310和/或一个或多个客户端应用程序1316进行双向通信。例如,安装在客户端设备1310上的应用程序可以使用其功能,包括但不限于客户端设备1310的NFC介质,以便向非接触式卡1305传送NDEF或其他消息。该消息可以包含例如与从一个或多个服务器1320所关联的服务发送的认证请求的类型相对应的信息。例如,非接触式卡1305从客户端设备1310和/或客户端应用程序1316接收的特定标志或有效载荷可以修改由非接触式卡1305生成的特定有效载荷。在一些示例中,非接触式卡1305可以生成用于指示的特定目的(包括但不限于由用户转移余额)的定制的有效载荷。

[0204] 在一些示例中,用户可能希望将应用程序下载到他或她的客户端设备1310。用户可以通过验证他或她的帐户身份来限制应用程序的下载。在示例实施例中,应用程序管理器可以仅在用户验证后才允许下载特定应用程序。用户可以将他或她的非接触式卡1305在客户端设备1310上轻击,以进入客户端设备1310的通信场,并且如上所述,客户端设备1310和一个或多个客户端应用程序1316可以被配置为接收电话号码和链接到认证的号码。应用程序管理器可以获取此信息,并进一步添加或传递指示用户希望下载哪个用户应用程序的参数。在传送该有效载荷时,客户端设备1310和/或一个或多个客户端应用程序1316可以接收有效载荷以认证非接触式卡1305和/或用户。接收到的有效载荷可以进一步包括与寻求下载的特定应用程序相对应的信息。例如,接收到的有效载荷的一部分可以被加密,并且一旦被应用程序管理器解密,则允许应用程序管理器下载应用程序。以这种方式,确认用户的身份,这允许仅经认证的用户下载想要的应用程序。此外,一个或多个服务器1320可以通过接收有效载荷来维护或以其他方式跟踪哪个用户已经下载了特定应用程序。

[0205] 在一些示例中,用户可能希望将余额从一个帐户转移到另一帐户。这些帐户可以是一个机构内的帐户(例如,储蓄帐户和支票帐户),也可以是属于用户但在不同机构持有的帐户。用户可以发起转移余额的请求。余额转移请求可以发生在物理位置(诸如分支机构)、在线计算机上、或客户端设备1310。在示例实施例中,为了确认用户发起了请求,用户可以在他或她的客户端设备1310上接收通知。该通知可以包括推送通知、电话呼叫或文本消息。用户在接收到通知时可以将例如他或她的非接触式卡1305对着他或她的客户端设备

1310做出手势(例如轻击),使得非接触式卡1305进入客户端设备1310的通信场。非接触式卡1305然后可以将有效载荷传送到客户端设备1310。在接收到有效载荷之后,客户端设备1310然后可以通过电话呼叫向一个或多个服务器传送令牌以验证用户的身份。在示例实施例中,用户必须做出手势,例如轻击,这允许他或她的非接触式卡1305在接收到通知之后的预定时间段内进入客户端设备1310的通信场,以确认他或她期望提出余额转移请求。在接收到有效载荷时,一个或多个服务器1320可以验证用户的身份,并且授权所请求的余额转移发生。

[0206] 在一些示例中,用户可以请求重置与他或她的非接触式卡1305相关联的密码(pin number)。该密码可以与用户帐户所关联的非接触式卡1305相关联,或者可以与另一用户帐户所关联的另一卡(例如借记卡或信用卡)相关联。在示例实施例中,用户可以通过在线门户或通过客户端设备1310发起在物理位置(例如银行)重置他或她的密码的请求。响应于用户请求,与一个或多个服务器1320相关联的服务可以将通知传送给用户。通知的传输可以通过任何介质进行,包括但不限于电子邮件、文本消息、在客户端设备1310上安装的应用程序上的推送通知、或通过电话呼叫进行。在接收到通知之后,用户可以将他或她的非接触式卡1305对着他或她的客户端设备1310轻击,从而非接触式卡1305进入客户端设备1310的通信场。如以上解释的,客户端设备1310可以被配置为从非接触式卡1305接收有效载荷。该有效负载可以包含电话号码、逗号以及逗号后的一串数字。然后,客户端设备1310和/或一个或多个客户端应用程序1316可以响应于对有效载荷的接收而发起电话呼叫,其可以将从非接触式卡1305接收的号码传送至与一个或多个服务器1320相关联的服务。在示例实施例中,如果以电话呼叫的形式接收到通知,则一个或多个服务器1320可以被配置为忽略传送给它的与电话号码相对应的一部分号码。在一些示例中,非接触式卡1305可以被配置为在从客户端设备1310和/或一个或多个客户端应用程序1316接收到指示电话呼叫已经激活的NFC信号时,将有效载荷的形式调整为仅包括与逗号后的令牌对应的部分。然后,该技术可以简化从非接触式卡1305接收的信息,而不必配置一个或多个服务器1320来辨别有效载荷的对应于电话号码的部分和有效载荷的对应于令牌的部分。

[0207] 在示例实施例中,用户可能希望将发行他或她的非接触式卡1305的实体以外的用户帐户与发行他或她的非接触式卡1305的实体的帐户链接。在接收到有效载荷之后,与实体相关联的一个或多个服务器1320可以验证用户的身份,并且授权所请求的余额转移发生。在示例实施例中,用户可以在物理位置(例如银行)、通过在线门户或通过客户端设备1310来发起该请求。响应于用户请求,与一个或多个服务器1320相关联的服务可以将通知传送给用户。通知的传输可以通过任何介质进行,包括但不限于电子邮件、文本消息、在客户端设备1310上安装的应用程序上的推送通知、或通过电话呼叫进行。在接收到该通知之后,用户可以将他或她的非接触式卡1305对着他或她的客户端设备1310进行轻击,使得非接触式卡1305进入客户端设备1310的通信场。如以上解释的,客户端设备1310可以被配置为从非接触式卡1305接收有效载荷。该有效载荷可以包括电话号码、逗号以及逗号后面的一串数字。然后,客户端设备1310和/或一个或多个客户端应用程序1316可以响应于对有效载荷的接收而发起电话呼叫,其可以将从非接触式卡1305接收的号码传递给与一个或多个服务器1320相关联的服务。在示例实施例中,如果以电话呼叫的形式接收到通知,则一个或多个服务器1320可以被配置为忽略传递给它的与电话号码相对应的一部分号码。在另外的

示例实施例中，非接触式卡1305可以被配置为在从客户端设备1310接收到指示电话呼叫已经激活的NFC信号之后，将有效载荷的形式调整为仅包括与逗号后的令牌相对应的部分。然后，这可以简化从非接触式卡1305接收的信息，而不必配置一个或多个服务器1320辨别有效载荷的对应于电话号码的部分和有效载荷的对应于令牌的部分。

[0208] 在一些示例中，用户可能希望请求更换非接触式卡1305。该更换卡1305可以包括与发行了用户非接触式卡的实体的属于该用户、具有上述功能的任何账户相对应的卡。在示例实施例中，该更换卡1305可以包括与任何实体的用户相对应的非接触式卡。在示例实施例中，用户可以在物理位置、通过web服务、通过手机上的应用程序、通过向地点发邮件请求或通过任何合适的通信介质发起请求。响应于接收到该请求，实体可能希望验证已经提出了更换卡1305请求的个人的身份。响应于该请求，与一个或多个服务器1320相关联的服务可以将通知发送给用户以确认他或她的身份。如上所述，这可以采取任何合适的形式。响应于接收到该请求，用户可以通过将非接触式卡1305对着他或她的客户端设备1310做出手势(例如，轻击)，使得非接触式卡1305进入客户端设备1310的通信场来验证他或她的身份。非接触式卡1305可以包括有效载荷，该有效载荷被配置为由客户端设备接收，被处理并发起电话呼叫，并且通过电话呼叫，将与令牌相对应的一串数字传送给与一个或多个服务器相关联的服务。如以上解释的，客户端设备1310可以被配置为从非接触式卡1305接收有效载荷。该有效载荷可以包括电话号码、逗号以及逗号后面的一串数字。然后，客户端设备1310可以响应于对有效载荷的接收而发起电话呼叫，该有效载荷可以将从非接触式卡1305接收的号码传递给与一个或多个服务器1320相关联的服务。在示例实施例中，如果以电话呼叫的形式接收到通知，则一个或多个服务器1320可以被配置为忽略传递给它的与电话号码相对应的一部分号码。在另外的示例实施例中，非接触式卡1305可以被配置为在从客户端设备1310接收到指示电话呼叫已经激活的NFC信号之后，将有效载荷的形式调整为仅包括与逗号后的令牌相对应的部分。然后，这可以简化从非接触式卡1305接收的信息，而不必配置一个或多个服务器1320辨别有效载荷的对应于电话号码的部分和有效载荷的对应于令牌的部分。

[0209] 在一些示例中，用户可能希望通过自动清算所(ACH)付款，请求电汇，或增加其借记帐户的债务限额。在示例实施例中，用户可以在物理位置、通过web服务、通过手机上的应用程序、通过向地点发邮件请求或通过任何其他合适的通信介质发起请求。响应于接收到请求，实体可能希望验证提出请求的个人的身份。如上所述，对用户的认证可以通过电话呼叫发生，该电话呼叫是通过用户将他或她的非接触式卡1305对着客户端设备1310做出手势(例如轻击)，使得非接触式卡1305进入客户端设备1310的通信场而发起的。

[0210] 在示例实施例中，用户可能希望将他或她的非接触式卡1305或其他交易卡注册到诸如Apple Pay、Samsung Pay或Android Pay的支付系统中。如上所述，对用户的认证可以通过电话呼叫发生，该电话呼叫是通过用户将他或她的非接触式卡1305对着客户端设备1310做出手势(例如轻击)，使得非接触式卡1305进入客户端设备1310的通信场而发起的。

[0211] 图14示出了根据示例实施例的用于卡激活的方法1400。方法1400可以引用与以上关于图13所描述的相同或相似的组件。

[0212] 在框1410，当将非接触式卡对着客户端设备做出手势(包括但不限于一个或多个手势)以与客户端设备建议通信时，非接触式卡的一个或多个小应用程序可以生成能够由

客户端设备读取的NDEF文件。在一些示例中，一个或多个手势可以至少包括将非接触式卡进行轻击、挥动或其他手势，使得非接触式卡进入客户端设备的通信场。例如，可以将非接触式卡对着客户端设备(例如移动设备)轻击，以在不使用应用程序的情况下发起电话呼叫。NDEF文件可以发起与客户端设备上不同应用程序的一个或多个通信。如以下讨论的，非接触式卡的一个或多个小应用程序可以动态地生成信息，例如电话号码以及可以附加到电话号码的ID令牌或有效载荷。在一些示例中，可以使用电话号码向一个或多个服务器进行电话呼叫，并且一个或多个服务器可以被配置为监视电话呼叫并接收被解密的输入。例如，可以将NDEF文件从非接触式卡读取到客户端设备，并进行到电话系统的切换，该电话系统应答所述呼叫并接收数字或有效负载的自动输入，将其传送到服务器，在服务器处呼叫被解密并认证，然后将其发送回电话系统，以指示成功认证或认证失败(带有一个或多个回退选项)。在一些示例中，所述呼叫不是基于IP的，即，不是使用IP语音(VoIP)或其他基于IP的呼叫机制进行的。

[0213] 在框1420，可以利用一个或多个过程来激活非接触式卡，每个过程都被分别描述。示例性过程包括但不限于发起的电话呼叫。

[0214] 例如，可以生成被配置为在客户端设备上发起电话呼叫的链接。该电话呼叫可以由客户端设备的默认电话程序发起，或者在其他示例中，可以使用不同的或指定的电话程序。根据该链接，可以发起电话呼叫，然后是暂停，再然后可以提供ID令牌。以这种方式，非接触式卡可以被配置为发起电话呼叫。下面提供了一个示例性链接：

[0215] tel://1234567890,,,1234567##

[0216] 在一些示例中，链接可以包括一个或多个信息元素。在一些示例中，链接可以包括第一信息元素、第二信息元素和第三信息元素。例如，第一信息元素可以在第二信息元素之前，并且第二信息元素可以在第三信息元素之前。

[0217] 在实施例中，第一信息元素可以包括电话号码，例如(123)456-7890。在一些示例中，该号码可以是基于美国的，包括区号。在其他示例中，该号码可以是基于非美国的，例如，该号码可以进一步包括国家代码，并且可以导致拨打国际电话。在一些示例中，可以动态生成一个或多个电话号码，或者可以从预先配置的列表中检索一个或多个电话号码。呼叫的电话号码元素可以被硬编码为呼叫卡激活电话号码或其他服务，例如tel://1234567890。

[0218] 在实施例中，第二信息元素可以包括一个或多个字符，例如一个或多个逗号。在一些示例中，一个或多个逗号可以被解释为一个或多个持续停顿。例如，停顿的持续时间可以包括固定的时间段，例如一秒。因此，如果逗号被解释为一秒钟的持续停顿，则包含四个逗号(如上述示例性链接)可能导致四秒钟的停顿。在一些示例中，逗号的数量可以足够长，以使电话系统能够收听和应答。如下所述，这可以使自动电话系统有时间响应呼叫并等待其他信息元素。

[0219] 在实施例中，该链路可以包括第三信息元素，该第三信息元素可以包括一个或多个有效载荷。例如，递送的有效载荷(例如1234567##)可以被配置为对非接触式卡进行认证。在某些示例中，该数字字符串可以以加密格式传递到电话系统中，并可以用密钥解密。如果解密过程失败(例如，由于静态或其他原因而导致数字丢失)，则此过程可能会触发一个或多个回退选项。例如，一个选项可以包括将呼叫路由到可以接听该呼叫的运营商或客

户服务代表。在另一个示例中，另一个选项可以包括该过程可以被路由到另一个系统以输入非接触式卡的卡验证值，如下所述。

[0220] 在一些示例中，如果在非接触式卡激活期间使用了不正确的电话号码，则可以标记此事件并将其存储在数据库中以分析潜在的可疑对象。因此，未注册的电话号码可以表示欺诈活动的可能性更高。

[0221] 在一些示例中，诸如非接触式卡的CVV的值可以被配置为激活非接触式卡。在其他示例中，可以提供比CVV方法更高的安全性，包括利用由一个或多个卡小应用程序生成的一次性密码(OTP)，该密码可以由一个或多个服务器加密和解密以认证非接触式卡。

[0222] 在框1430，在这种情况下，电话系统可以解析来自电话呼叫的有效载荷，并将其通过一个或多个网络应用程序传递以便进行解密。在一些示例中，令牌可以经由私钥/公钥来加密。例如，私钥可以用于解密数据，并且还可以安全地存储，从而可以在没有私钥的情况下(通过公钥)进行加密，这意味着私钥不需要被传递，因此不容易被第三方拦截。可以由一个或多个服务器检查和验证用于发起呼叫的号码，以便确定电话号码的有效性。因此，加密的数据可以被解密，并且非接触式卡已经被激活的通知或指示可以包括从一个或多个服务器向客户端设备传送文本消息或电子邮件。

[0223] 在框1440，在非接触式卡已经被成功激活并且客户端设备已经接收到指示激活的通知之后，可以指示非接触式卡禁用动态数据生成。在一些示例中，如上所述，在已经通过一个或多个过程之一激活了非接触式卡之后，可以选择性地将非接触式卡的用户导向客户支持，或者非接触式卡可以在POS设备上使用或任何其他系统。例如，如果用户使用激活的卡与POS设备进行交互，则可以指示非接触式卡停止动态生成号码。在一些示例中，这可能需要诸如支付小应用程序或交易小应用程序之类的小应用程序之间的通信，以指示非接触式卡的一个或多个其他小应用程序在下一次发生非接触式卡的一个或多个手势时停止电话号码的生成。以这种方式，响应于非接触式卡的成功激活，非接触式卡的动态生成功能可以被关闭或禁用。

[0224] 举例来说，非接触式卡可以被配置为或者非接触式卡的有效载荷可以被配置为在接收有效载荷的客户端设备中引起以下一项或多项：(i)下载与非接触式卡兼容的应用程序；(ii)在属于非接触式卡的用户的一个或多个账户之间转移余额或其他金额；(iii)重置与用户、非接触式卡相关联的个人识别码(PIN)，或与非接触式卡的用户相关联的账户；(iv)将属于用户的账户与发行非接触式卡的实体链接，所述用户不是账户；(v)批准或引起从一个或多个帐户到与非接触式卡相关联的帐户或从与非接触式卡1305相关联的帐户进行的余额转移；(vi)向非接触式卡的发行者请求更换卡；(vii)请求或引起自动清算所(ACH)付款；(viii)批准或引起从或向对应于或属于非接触式卡的用户的账户进行的电汇；(ix)注册、验证用户的注册或对用户进行认证，以允许与用户关联的帐户或非接触式卡附加到与设备相关联的付款服务上，包括但不限于ApplePay®、SamsungPay®、AndroidPay®、GooglePay®、Venmo®或Paypal®；(x)请求与帐户相关联的活动，例如增加信用帐户的债务限额，请求加急交易(例如结算支票)或对交易提出异议。非限制性地，例如，可以通过使用配置有特定NDEF消息的非接触式卡来实现以上的一个或多个。

[0225] 在一些示例中，非接触式卡可以与客户端设备进行双向通信。例如，安装在客户端设备上的应用程序可以使用其功能，包括但不限于客户端设备的NFC介质，以便向非接触式卡传送NDEF或其他消息。该消息可以包含例如与从一个或多个服务器所关联的服务发送的认证请求的类型相对应的信息。例如，非接触式卡从客户端设备接收的特定标志或有效载荷可以修改由非接触式卡生成的特定有效载荷。在一些示例中，非接触式卡可以生成用于指示的特定目的(包括但不限于由用户转移余额)的定制的有效载荷。如前所述，可以通过用户做出手势(诸如将他或她的非接触式卡对着客户端设备进行轻击)来发起电话呼叫以执行对用户的授权，包括但不限于应用程序下载、余额转移、密码重置、帐户关联、卡更换和支付处理。

[0226] 在一些示例中，本公开涉及非接触式卡的轻击。然而，应当理解的是，本公开不限于轻击，并且本公开包括其他手势(例如，挥动卡或卡的其他移动)。

[0227] 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”旨在表示包含性的“或”。此外，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。

[0228] 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，以免混淆对本描述的理解。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”等指示如此描述的所公开技术的一个或多个实施方式可以包括特定特征、结构或特性，但并非每个实施方式都必须包括该特定的特征、结构或特性。此外，虽然可以重复使用短语“在一个示例中”、“在一个实施例中”或“在一种实施方式中”，但是不一定是指相同的示例、实施例或实施方式。

[0229] 如本文所使用的，除非另外指定，否则使用序数形容词“第一”、“第二”、“第三”等来描述共同的对象，仅指示相同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呈现给定的顺序。

[0230] 尽管已结合当前被认为是最实际可行的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的实施方式，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。

[0231] 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内容。所公开技术的某些实施方式的可专利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相同的结构元件，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。

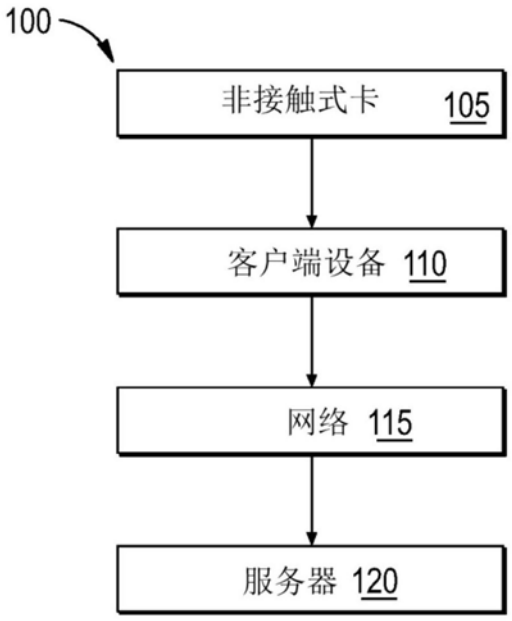

100
非接触式卡 105
客户端设备 110
网络 115
服务器 120

图1A

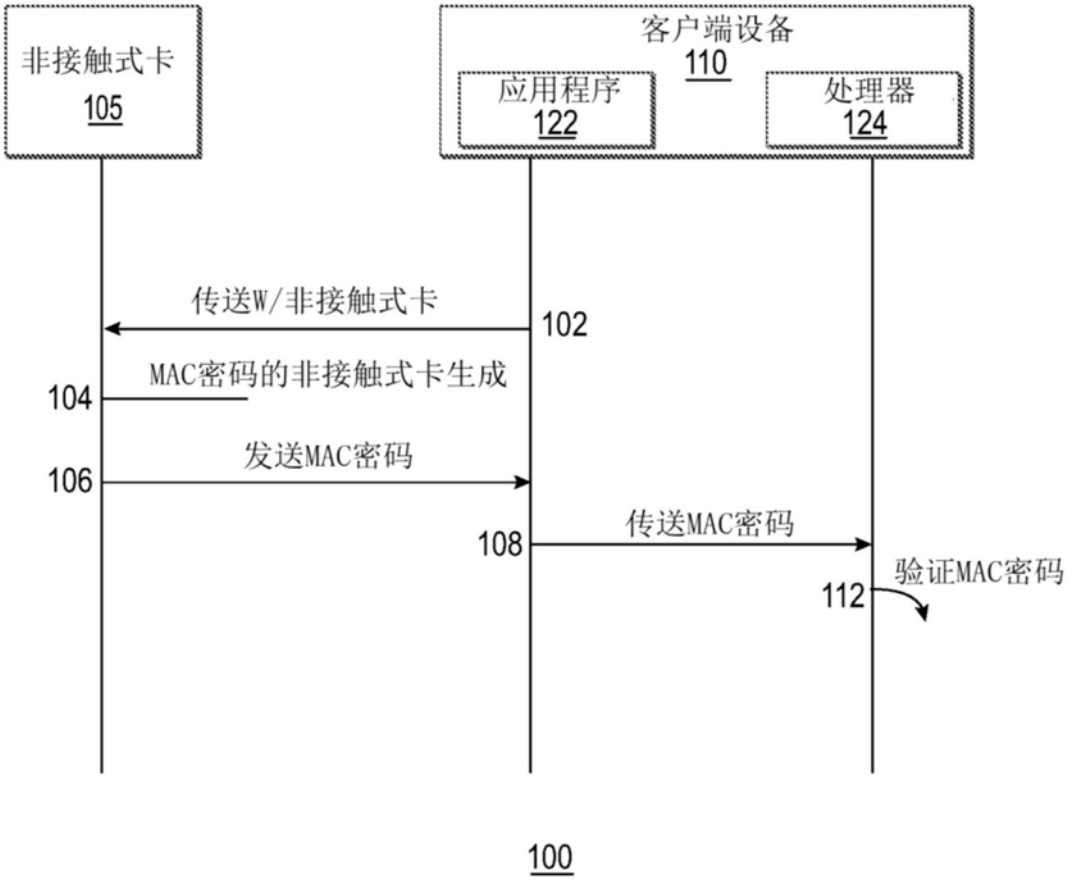

非接触式卡
105
客户端设备
110
应用程序
122
处理器
124
传送W/非接触式卡
102
MAC密码的非接触式卡生成
104
发送MAC密码
106
传送MAC密码
108
验证MAC密码
112
100

图1B

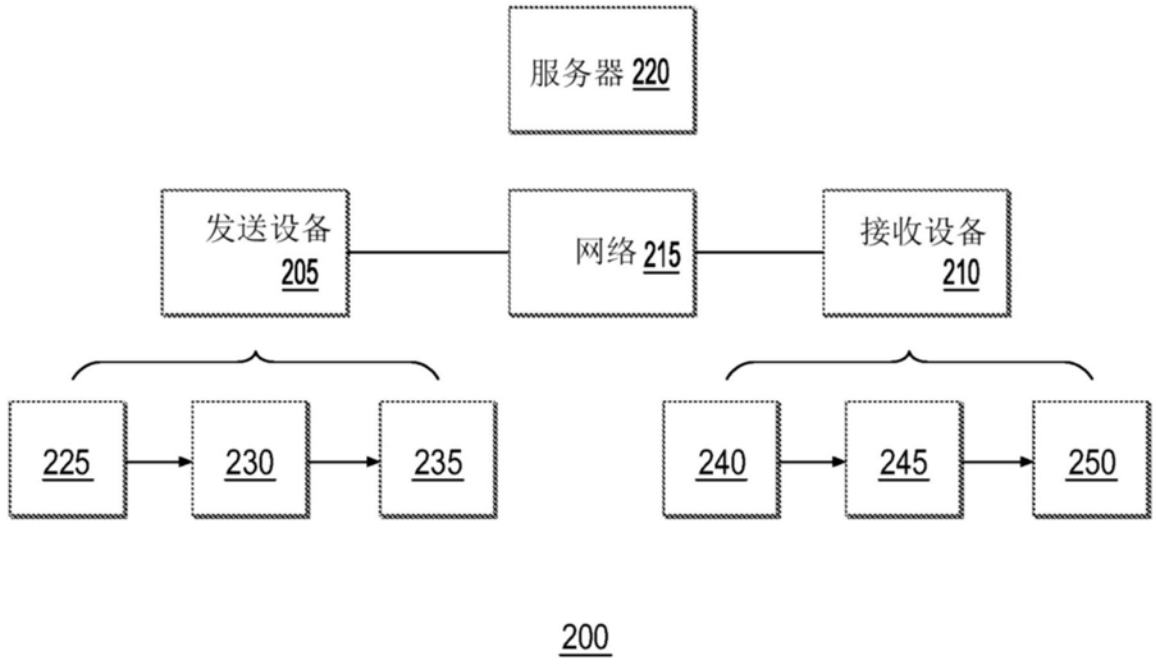

服务器 220
发送设备 205
网络 215
接收设备 210
225
230
235
240
245
250
200

图2

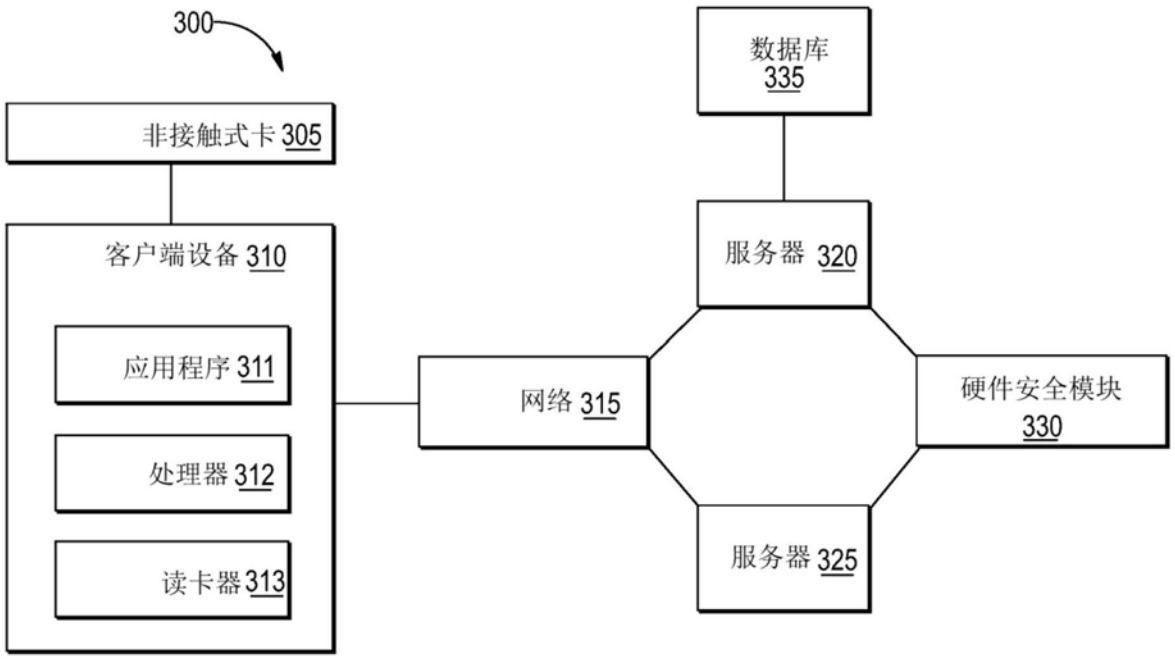

300
非接触式卡 305
客户端设备 310
应用程序 311
处理器 312
读卡器 313
网络 315
数据库 335
服务器 320
硬件安全模块 330
服务器 325

图3

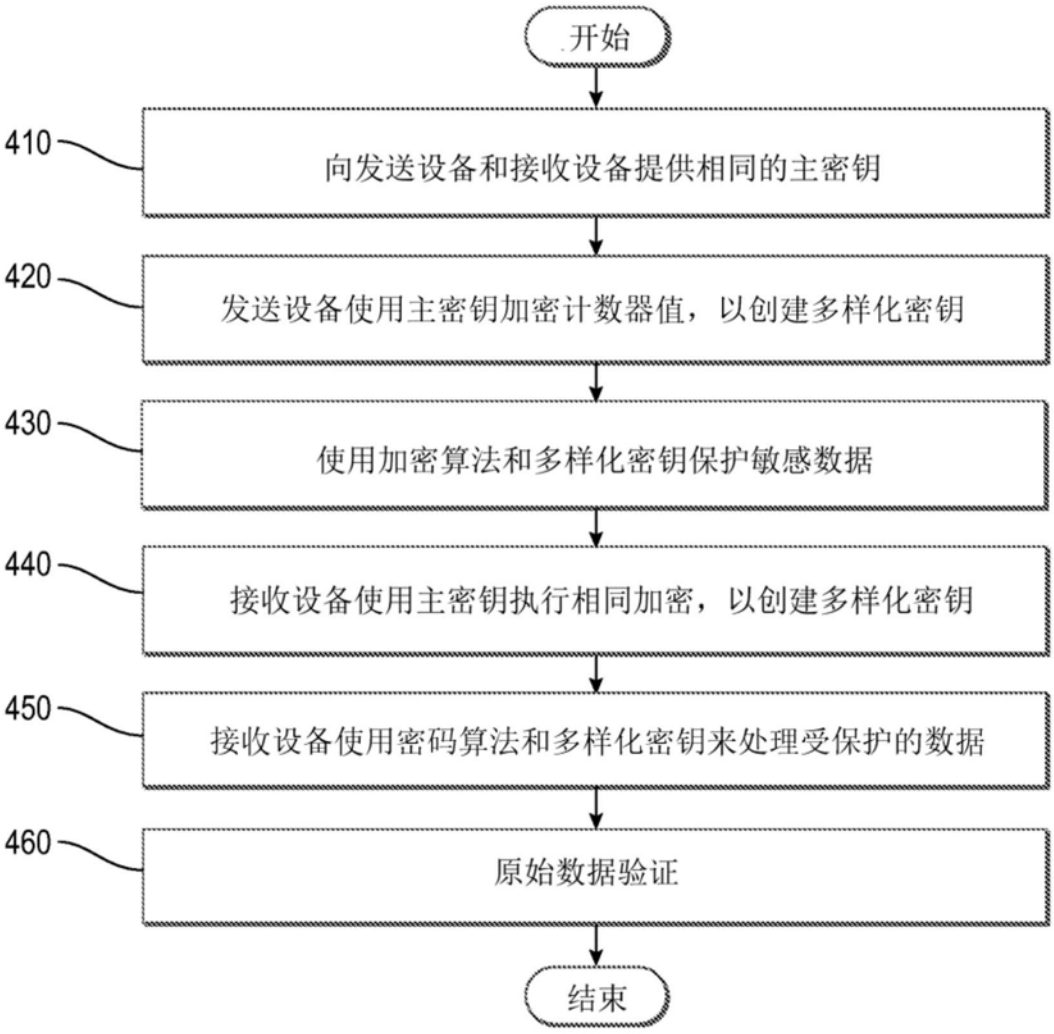

开始
410
向发送设备和接收设备提供相同的主密钥
420
发送设备使用主密钥加密计数器值，以创建多样化密钥
430
使用加密算法和多样化密钥保护敏感数据
440
接收设备使用主密钥执行相同加密，以创建多样化密钥
450
接收设备使用密码算法和多样化密钥来处理受保护的数据
460
原始数据验证
结束
400

图4

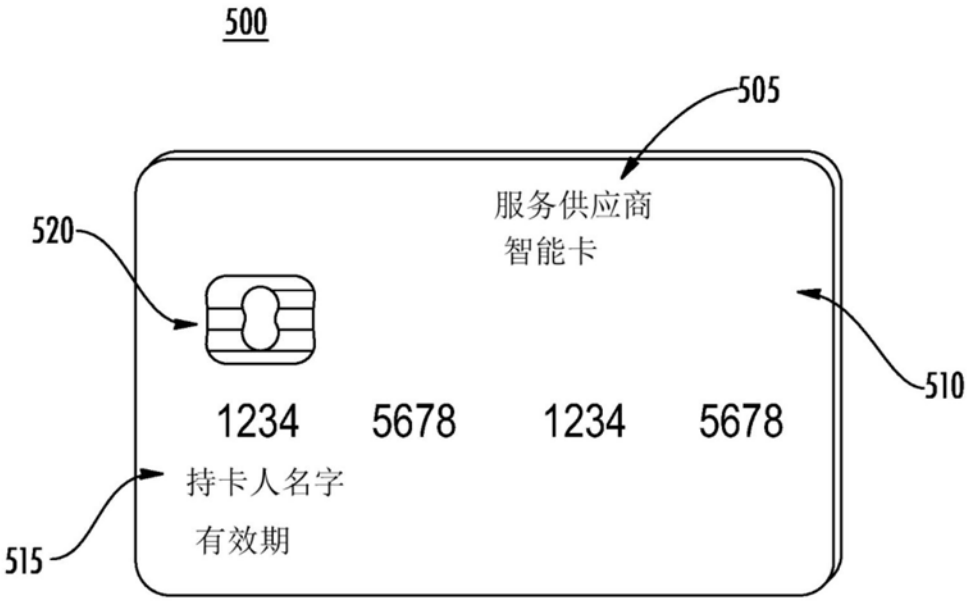


图5A

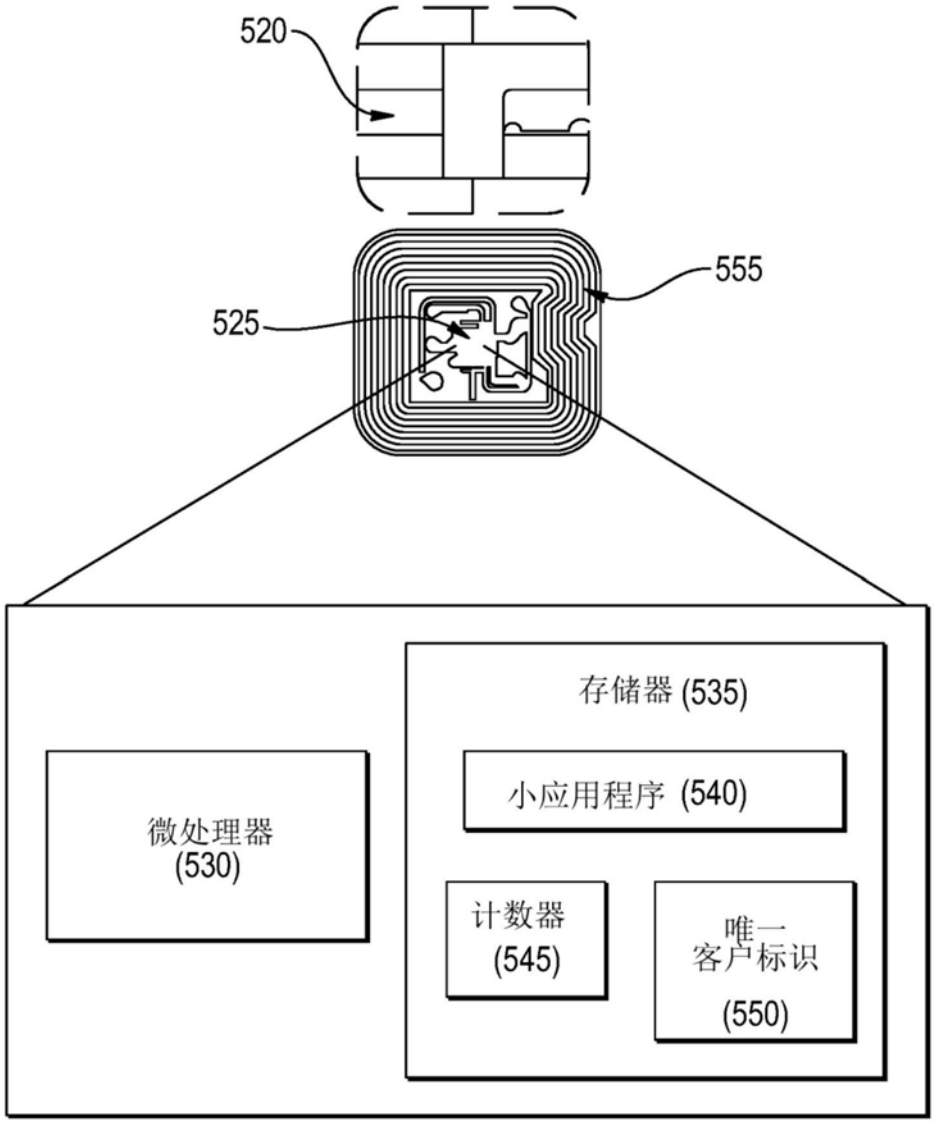


图5B

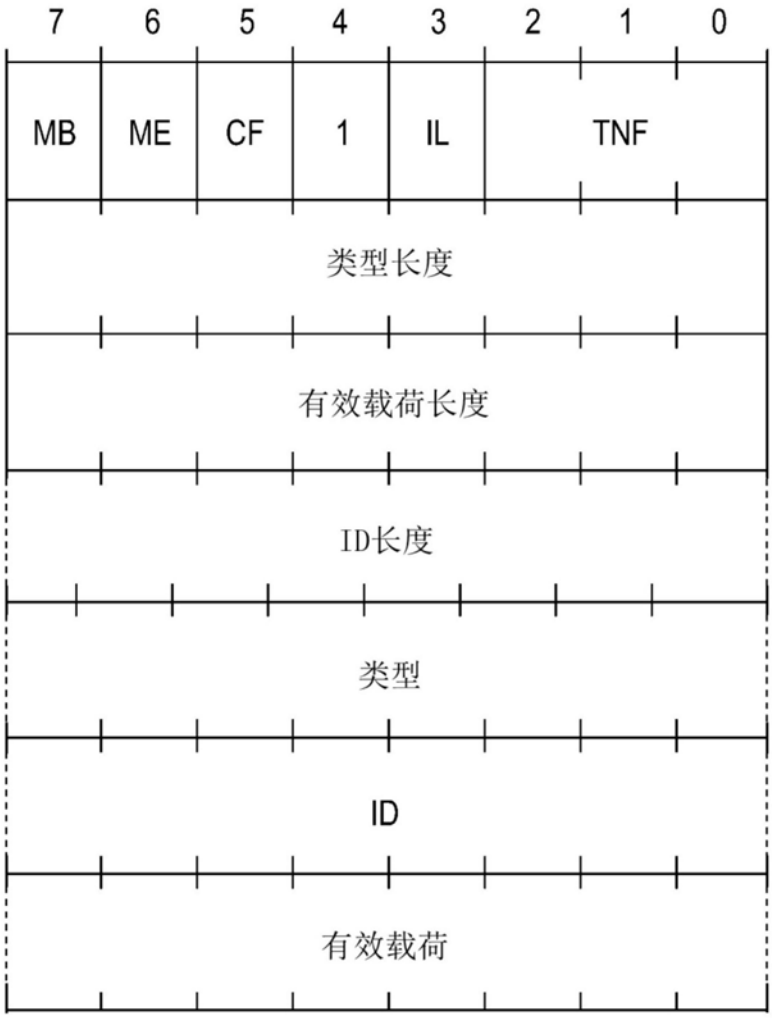


图6

00 D1 (Message Begin, Message End, Short Record, noID length) 01 (well known type) 01 01 Text type 02 <Payload Length including recordID and "EN", or contentlength+3) = 45+3 = 48 (DEC) 03 54 ('T') 04 02 record ID 05 65 6E (language length, 'en') 07 43 01 00 76 a6 62 7b 67 a8 cf bb <eight mac bytes> D101305402656E 43010076A6627B67A8CFBB <eight mac bytes>

710

版本	pUID (8)	pATC	加密的密码（16）	
0100	0015399555360061	00000050	7D28B8B9D8666E5143153AC9C944E5A6	
解密的密码				
随机数（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

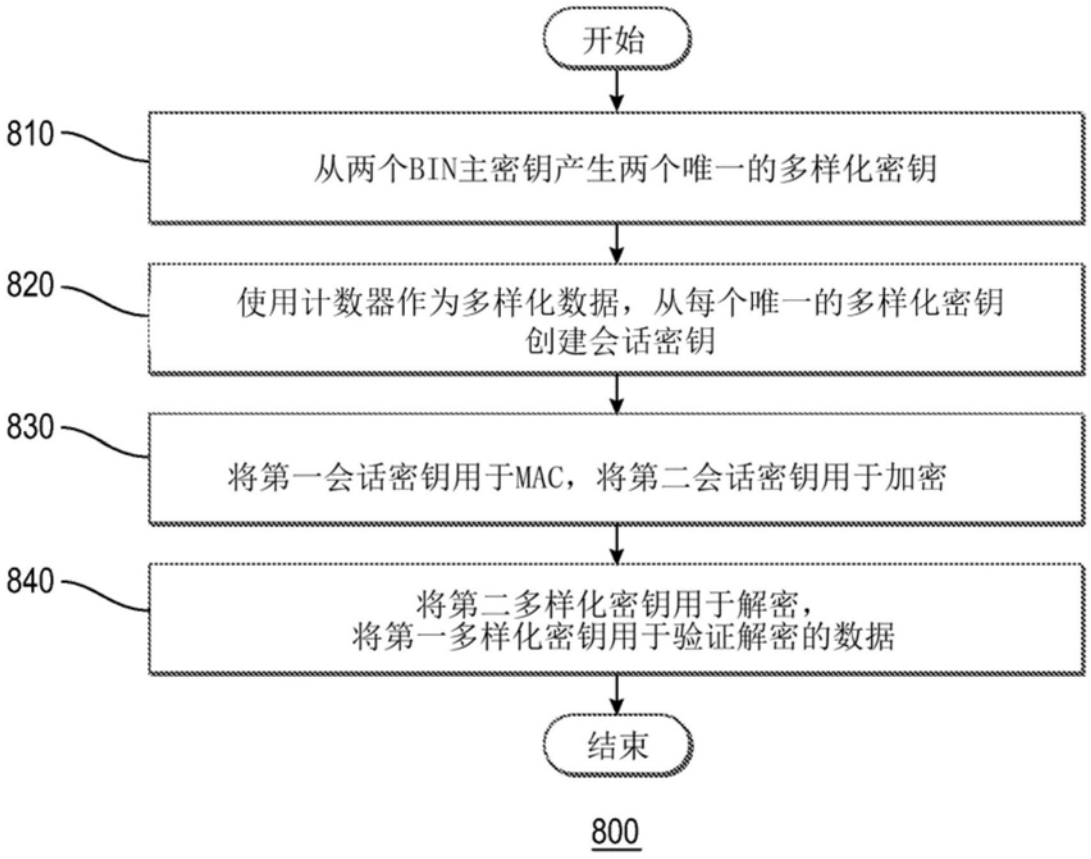

开始
810
从两个BIN主密钥产生两个唯一的多样化密钥
820
使用计数器作为多样化数据，从每个唯一的多样化密钥
创建会话密钥
830
将第一会话密钥用于MAC，将第二会话密钥用于加密
840
将第二多样化密钥用于解密，
将第一多样化密钥用于验证解密的数据
结束
800

图8

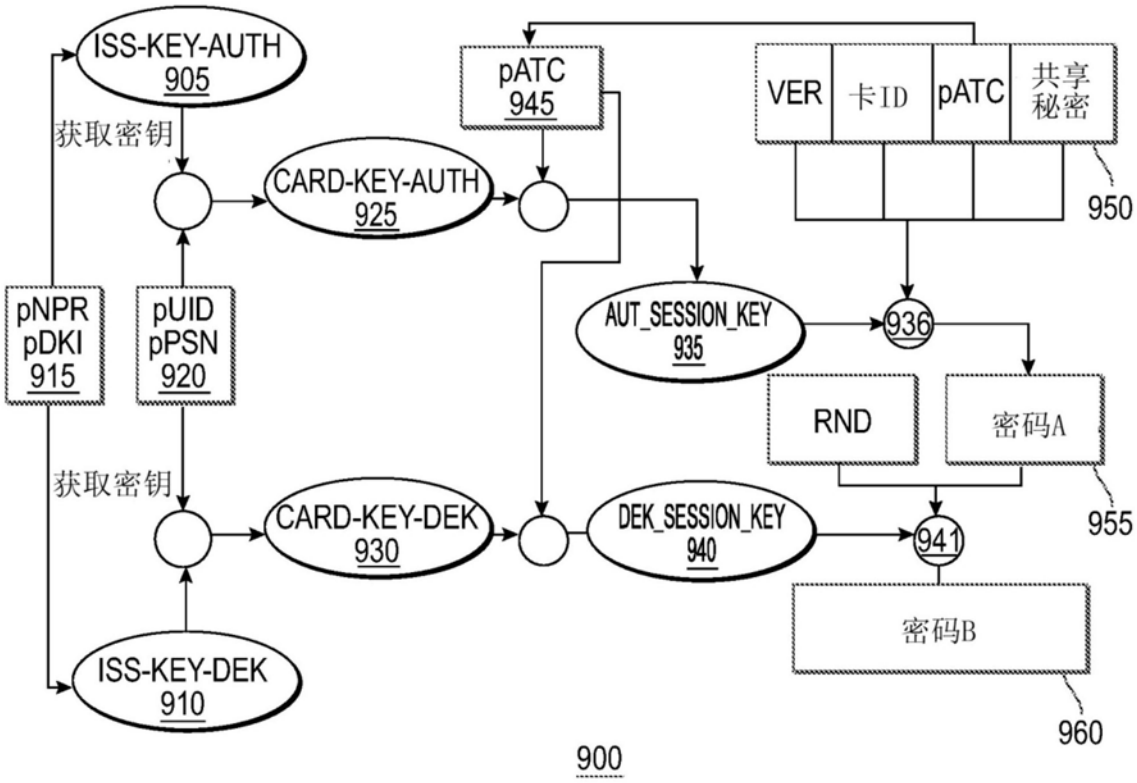

ISS-KEY-AUTH
905
获取密钥
CARD-KEY-AUTH
925
pATC
945
VER
卡ID
pATC
共享
秘密
950
pNPR
pDKI
915
pUID
pPSN
920
AUT_SESSION_KEY
935
936
RND
密码A
955
获取密钥
CARD-KEY-DEK
930
DEK_SESSION_KEY
940
941
密码B
960
ISS-KEY-DEK
910
900

图9

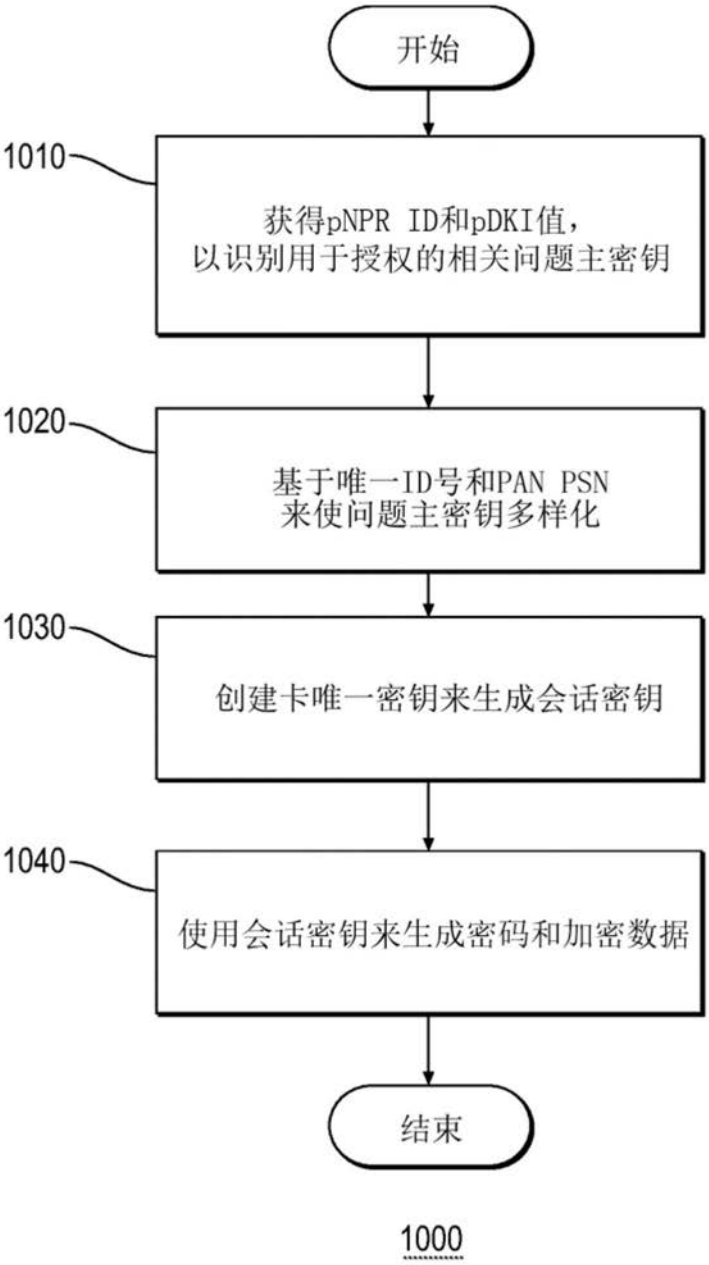

开始
1010
获得pNPR ID和pDKI值，
以识别用于授权的相关问题主密钥
1020
基于唯一ID号和PAN PSN
来使问题主密钥多样化
1030
创建卡唯一密钥来生成会话密钥
1040
使用会话密钥来生成密码和加密数据
结束
1000

图10

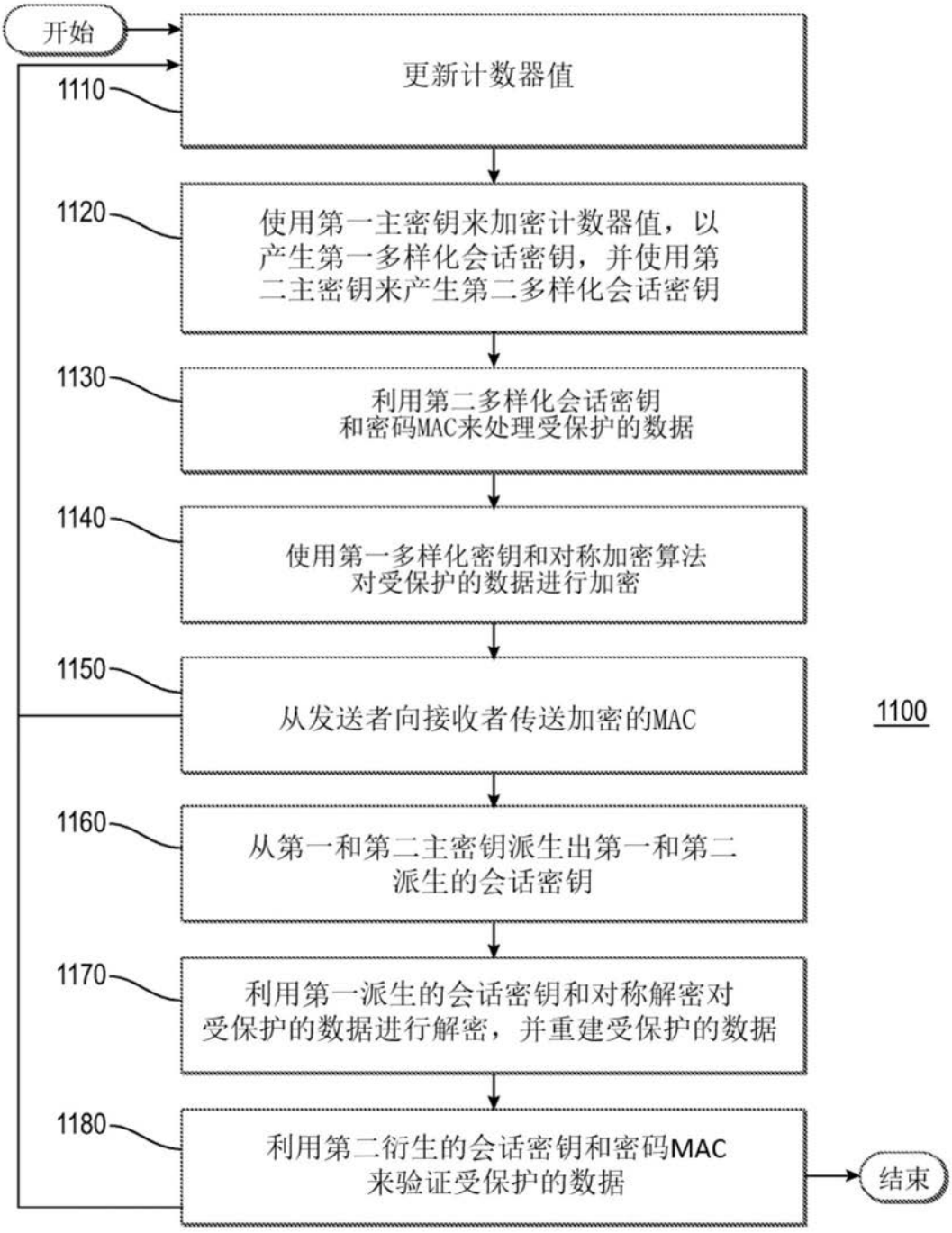

开始
更新计数器值
1110
使用第一主密钥来加密计数器值，以产生第一多样化会话密钥，并使用第二主密钥来产生第二多样化会话密钥
1120
利用第二多样化会话密钥和密码MAC来处理受保护的数据
1130
使用第一多样化密钥和对称加密算法对受保护的数据进行加密
1140
从发送者向接收者传送加密的MAC
1150
1100
从第一和第二主密钥派生出第一和第二派生的会话密钥
1160
利用第一派生的会话密钥和对称解密对受保护的数据进行解密，并重建受保护的数据
1170
利用第二衍生的会话密钥和密码MAC来验证受保护的数据
1180
结束

图11

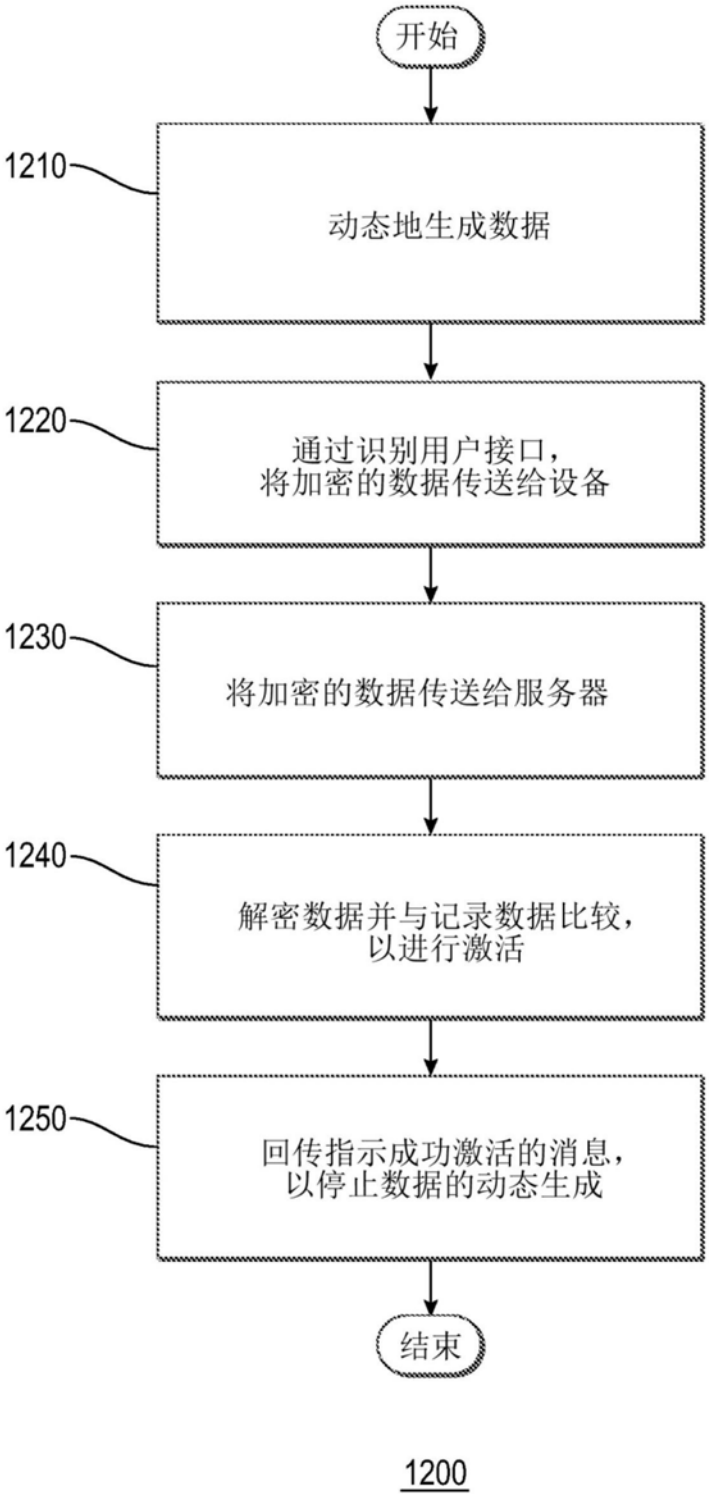

开始
1210
动态地生成数据
1220
通过识别用户接口，
将加密的数据传送给设备
1230
将加密的数据传送给服务器
1240
解密数据并与记录数据比较，
以进行激活
1250
回传指示成功激活的消息，
以停止数据的动态生成
结束
1200

图12

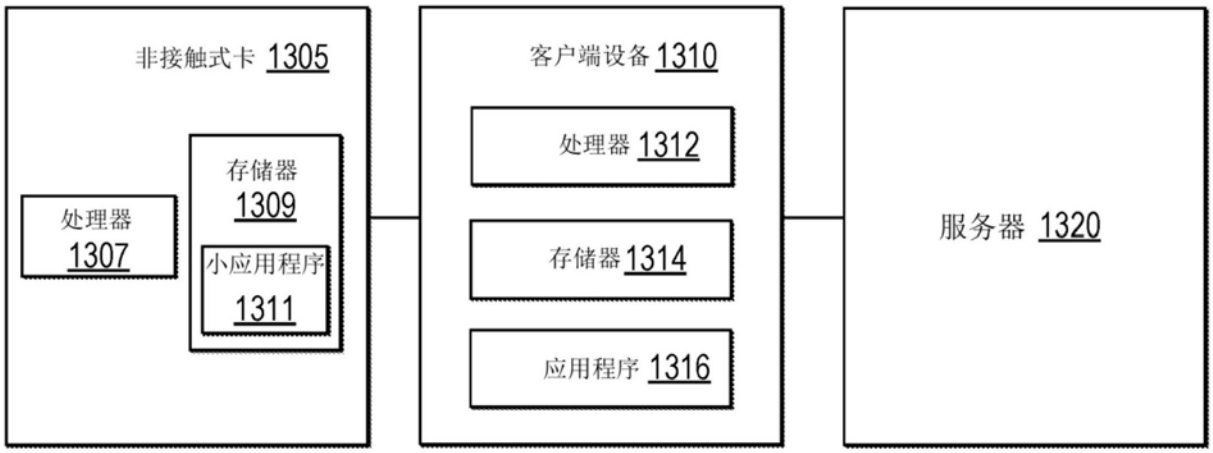

非接触式卡 1305
处理器 1307
存储器 1309
小应用程序 1311
客户端设备 1310
处理器 1312
存储器 1314
应用程序 1316
服务器 1320

图13

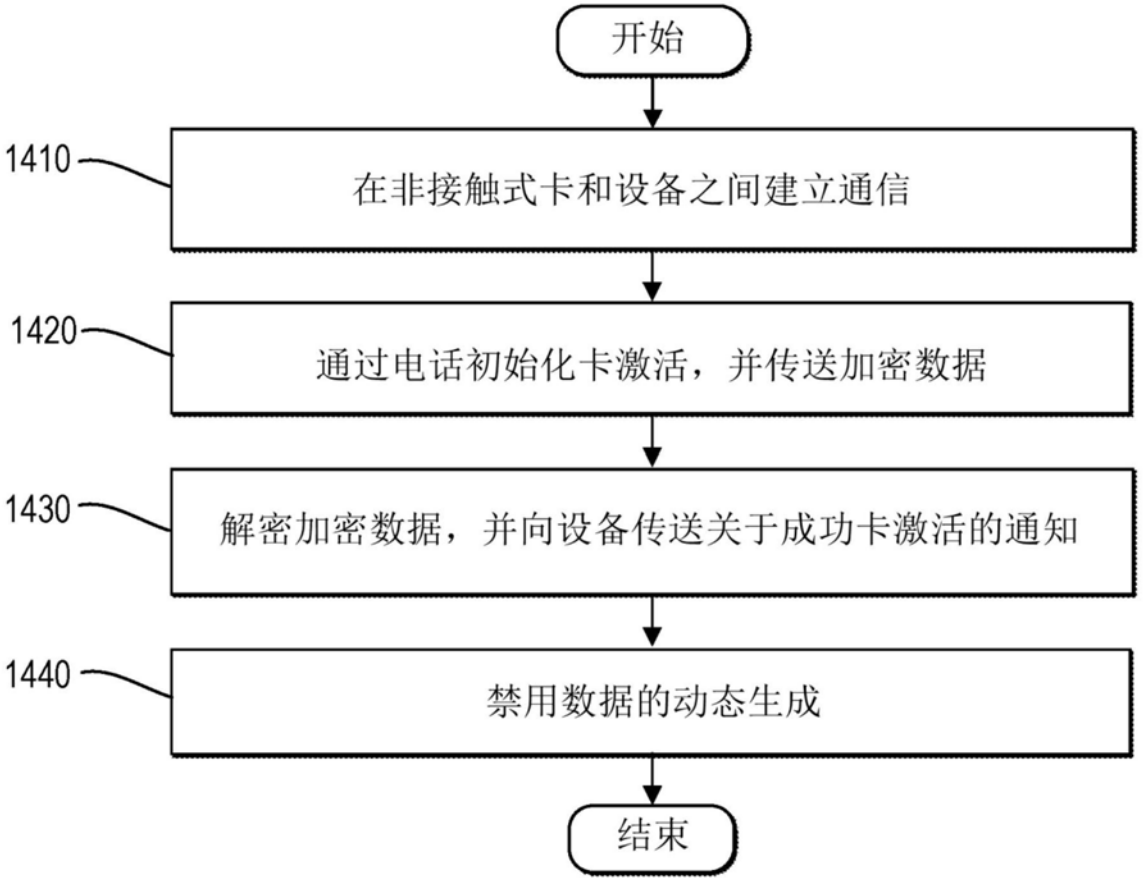

开始
1410
在非接触式卡和设备之间建立通信
1420
通过电话初始化卡激活，并传送加密数据
1430
解密加密数据，并向设备传送关于成功卡激活的通知
1440
禁用数据的动态生成
结束

图14