(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 108475376 A
(43)申请公布日 2018.08.31

(21)申请号 201680076779.2

(22)申请日 2016.12.01

(30)优先权数据
62/271,428 2015.12.28 US

(85)PCT国际申请进入国家阶段日
2018.06.28

(86)PCT国际申请的申请数据
PCT/IB2016/057249 2016.12.01

(87)PCT国际申请的公布数据
WO2017/115174 EN 2017.07.06

(71)申请人 莫比威孚公司
地址 加拿大魁北克蒙特利尔

(72)发明人 朱利安·奥利维耶
文森特·阿利米
塞巴斯蒂安·方丹

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 杨敏 杨明钊

(51)Int.Cl.
G06Q 20/40(2006.01)
G06F 21/36(2006.01)
H04W 12/06(2006.01)

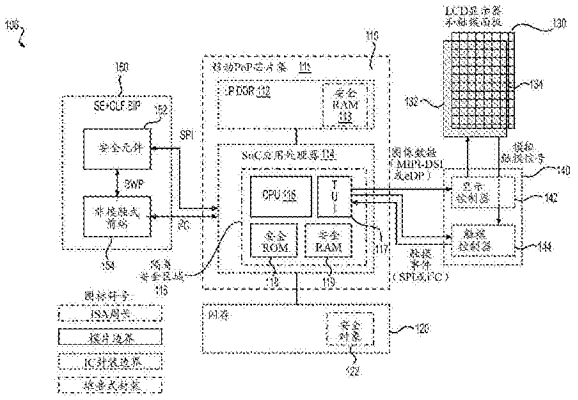
权利要求书4页 说明书13页 附图5页

(54)发明名称

在设备上认证用户的系统和方法

(57)摘要

一种用于操作设备的系统和方法。该方法包括:生成对应表、热点布局和加扰键盘的视觉表示;发送对应表、加扰键盘的视觉表示和热点布局。该方法还包括使由显示控制器在显示屏上显示加扰键盘的视觉表示;由触摸屏控制器检测通过触摸屏来自用户的触摸事件输入;由触摸屏控制器基于触摸事件输入和热点布局来生成按键事件;对按键事件加密;以及将加密的按键事件发送到安全元件。该方法还包括对加密的按键事件解密;以及基于按键事件和对应表来重构与用户相关联的个人识别码(PIC)。



CN 108475376 A

1.一种用于操作设备的方法，所述设备包括处理器，所述处理器包括隔离安全区域；显示屏，其操作地连接到显示屏控制器；所述显示屏控制器，其操作地连接到所述处理器；触摸屏，其操作地连接到触摸屏控制器；所述触摸屏控制器，其操作地连接到所述处理器；安全元件，其与所述处理器相关联，所述方法包括：

生成对应表、热点布局和加扰键盘的视觉表示；

向所述安全元件发送所述对应表；

向所述显示控制器发送所述加扰键盘的视觉表示；

向所述触摸屏控制器发送所述热点布局；

使由所述显示控制器在所述显示屏上显示所述加扰键盘的视觉表示；

由所述触摸屏控制器检测在触摸板上的来自用户的触摸事件输入；

由所述触摸屏控制器基于所述触摸事件输入和所述热点布局来生成按键事件；

由所述触摸屏控制器对所述按键事件加密；

将加密的按键事件发送到所述安全元件；

由所述安全元件对所述加密的按键事件解密；以及

由所述安全元件基于所述按键事件和所述对应表来重构与所述用户相关联的个人识别码(PIC)。

2.根据权利要求1所述的方法，还包括在向所述安全元件发送所述对应表之前将所述对应表加密。

3.根据权利要求2所述的方法，还包括在将所述对应表加密之后由所述安全元件将所述对应表解密。

4.根据权利要求1到3中的任一项所述的方法，其中，所述PIC的未加密版本在任何给定时间处对所述处理器、所述显示控制器、所述触摸屏控制器和所述处理器的所述隔离安全区域中的任何一个保持不可访问。

5.根据权利要求1到4中的任一项所述的方法，其中，所述PIC的未加密版本仅由所述安全元件可访问。

6.根据权利要求1到5中的任一项所述的方法，其中，所述隔离安全区域仅访问所述PIC的加密版本。

7.根据权利要求1到6中的任一项所述的方法，其中，所述触摸屏控制器在任何给定时间处不具有对所述对应表的访问权也不具有对所述加扰键盘的视觉表示的访问权。

8.根据权利要求1到7中的任一项所述的方法，其中，所述安全元件安全地连接到所述处理器。

9.根据权利要求1到8中的任一项所述的方法，其中，所述处理器的所述隔离安全区域包括可信用户界面。

10.根据权利要求9所述的方法，其中，所述触摸屏控制器安全地连接到所述可信用户界面。

11.根据权利要求1到10中的任一项所述的方法，其中，所述方法还包括通过在按键事件发生之后修改所述对应表来将所述加扰键盘的视觉表示的至少一部分重新加扰。

12.根据权利要求1到11中的任一项所述的方法，其中，在触摸事件发生之前生成多个对应表、热点布局和加扰键盘的视觉表示。

13.根据权利要求1到12中的任一项所述的方法，其中，所述加扰键盘的视觉表示是图像和视频流中的至少一个。

14.根据权利要求1到13中的任一项所述的方法，其中，所述方法还包括使由所述显示控制器显示先前与所述用户相关联的安全指示符。

15.根据权利要求14所述的方法，其中，先前与所述用户相关联的所述安全指示符被存储在所述处理器的所述隔离安全区域中。

16.根据权利要求1到15中的任一项所述的方法，还包括：

由所述安全元件对重构的PIC加密；以及

将加密的重构的PIC发送到所述处理器。

17.根据权利要求1到16中的任一项所述的方法，其中，所述安全元件是操作地连接到所述处理器的硬件元件、由所述处理器运行的软件部件、所述隔离安全区域和所述隔离安全区域的一部分中的至少一个。

18.根据权利要求1到17中的任一项所述的方法，其中，由所述处理器的所述隔离安全区域和所述安全元件之一来执行生成所述对应表、所述热点布局和所述加扰键盘的视觉表示。

19.根据权利要求1到18中的任一项所述的方法，其中，重构与所述用户相关联的所述PIC包括使用所述对应表将所述按键事件映射到值。

20.一种用于操作设备的方法，所述设备包括处理器，所述处理器包括隔离安全区域，所述隔离安全区域界定安全元件；显示屏，其操作地连接到显示屏控制器；所述显示屏控制器，其操作地连接到所述处理器；触摸屏，其操作地连接到触摸屏控制器；所述触摸屏控制器，其操作地连接到所述处理器；所述方法包括：

生成对应表、热点布局和加扰键盘的视觉表示；

向所述安全元件发送所述对应表；

向所述显示控制器发送所述加扰键盘的视觉表示；

向所述触摸屏控制器发送所述热点布局；

使由所述显示控制器在所述显示屏上显示所述加扰键盘；

由所述触摸屏控制器检测在触摸板上的来自用户的触摸事件输入；

由所述触摸屏控制器基于所述触摸事件输入来生成按键事件；

由所述触摸屏控制器对所述按键事件加密；

将加密的按键事件发送到所述安全元件；

由所述安全元件对所述加密的按键事件解密；以及

由所述安全元件基于所述按键事件和所述对应表来重构与所述用户相关联的个人识别码(PIC)。

21.一种用于验证用户的计算机实现的系统，所述系统包括：

处理器；

隔离安全区域，其与所述处理器相关联；

非临时计算机可读介质，其操作地连接到所述处理器；

显示屏，其操作地连接到显示屏控制器；

所述显示屏控制器，其操作地连接到所述处理器；

触摸屏，其操作地连接到触摸屏控制器；

所述触摸屏控制器，其操作地连接到所述处理器；

安全元件，其与所述处理器相关联；

所述处理器被配置为使得：

生成对应表、热点布局和加扰键盘的视觉表示；向所述安全元件发送所述对应表；

将所述加扰键盘的视觉表示发送到所述显示控制器；

向所述触摸屏控制器发送所述热点布局；

使由所述显示控制器在所述显示屏上显示所述加扰键盘；

由所述触摸屏控制器检测在触摸板上的来自所述用户的触摸事件输入；

由所述触摸屏控制器基于所述触摸事件输入来生成按键事件；

由所述触摸屏控制器对所述按键事件加密；

向所述安全元件发送加密的按键事件；

由所述安全元件对所述加密的按键事件解密；以及

由所述安全元件基于所述按键事件和所述对应表来重构与所述用户相关联的个人识别码(PIC)。

22.根据权利要求21所述的系统，其中，所述处理器包括所述隔离安全区域。

23.根据权利要求21所述的系统，其中，所述隔离安全区域被托管在不同于所述处理器的第二处理器上。

24.根据权利要求21至23中的任一项所述的系统，其中，所述处理器还被配置为使得：在向所述安全元件发送所述对应表之前对所述对应表加密。

25.根据权利要求21至23中的任一项所述的系统，其中，所述处理器还被配置为使得：在对所述对应表加密之后由所述安全元件对所述对应表解密。

26.根据权利要求21至25中的任一项所述的系统，其中，所述PIC的未加密版本在任何给定时间处对所述处理器、所述显示控制器、所述触摸屏控制器和所述处理器的所述隔离安全区域中的任何一个保持不可访问。

27.根据权利要求21至26中的任一项所述的系统，其中，所述PIC的未加密版本仅由所述安全元件可访问。

28.根据权利要求21至27中的任一项所述的系统，其中，所述隔离安全区域仅访问所述PIC的加密版本。

29.根据权利要求21至28中的任一项所述的系统，其中，所述触摸屏控制器在任何给定时间处不具有对所述对应表的访问权也不具有对所述加扰键盘的视觉表示的访问权。

30.根据权利要求21至29中的任一项所述的方法，其中，所述安全元件安全地连接到所述处理器。

31.根据权利要求21至30中的任一项所述的系统，其中，所述处理器的所述隔离安全区域包括可信用户界面。

32.根据权利要求31所述的系统，其中，所述触摸屏控制器安全地连接到所述可信用户界面。

33.根据权利要求21至32中的任一项所述的系统，其中，所述处理器还配置成使得：在触摸事件发生之后将所述对应表和所述加扰键盘的视觉表示的至少一部分重新加扰。

34.根据权利要求21至33中的任一项所述的系统，其中，在触摸事件发生之前生成多个对应表、热点布局和加扰键盘的视觉表示。

35.根据权利要求21至34中的任一项所述的系统，其中，所述加扰键盘的视觉表示是图像和视频流中的至少一个。

36.根据权利要求21至35中的任一项所述的系统，其中，所述处理器还被配置成使得：使由所述显示控制器显示先前与所述用户相关联的安全指示符。

37.根据权利要求36所述的系统，其中，先前与所述用户相关联的所述安全指示符被存储在所述处理器的所述隔离安全区域中。

38.根据权利要求21至37中的任一项所述的系统，其中，所述处理器还配置成使得：

由所述安全元件对重构的PIC加密；以及

将加密的重构的PIC发送到所述处理器。

39.根据权利要求21至38中的任一项所述的系统，其中，所述安全元件是操作地连接到所述处理器的硬件元件、由所述处理器运行的软件部件、所述隔离安全区域和所述隔离安全区域的一部分中的至少一个。

40.根据权利要求21至39中的任一项所述的系统，其中，由所述处理器的所述隔离安全区域和所述安全元件之一来执行生成所述对应表、所述热点布局和所述加扰键盘的视觉表示。

41.根据权利要求21至40中的任一项所述的系统，其中，重构与所述用户相关联的所述PIC包括使用所述对应表将所述按键事件映射到值。

在设备上认证用户的系统和方法

[0001] 交叉引用

[0002] 本申请要求2015年12月28日提交的标题为“SYSTEM FOR AND METHOD OF AUTHENTICATING A USER ON A DEVICE”的美国临时专利申请号62/271,428的公约优先权，该美国临时专利申请通过引用以其整体并入本文。

[0003] 领域

[0004] 本技术涉及用于在移动设备上认证用户的系统和方法。该系统和方法可以在移动设备上进行交易(更特别地，安全金融交易)的背景中被使用。

[0005] 背景

[0006] 本章旨在向读者介绍可能与本公开的在下面被描述和/或要求保护的各个方面相关的技术的各个方面。这个讨论被认为在向读者提供背景信息以便于更好地理解本技术的各个方面时是有帮助的。因此，应该理解，这些陈述将在这个角度中被理解，而不是作为对现有技术的承认。

[0007] 也被称为销售点(POS)终端的支付终端在本领域中已被完善。它们用于在零售商和消费者之间的电子资金转移，其中通过使用POS终端刷支付卡、插支付卡或轻敲(tapping)支付卡来进行交易。一些POS终端仅支持磁条技术(刷)，而其他终端此外或专门支持所谓的芯片卡或智能卡，其包括嵌入卡中的微处理器芯片。该芯片提供了高级别的安全性，抵御以克隆卡片或危害在其内存储的敏感信息为目的的逻辑和物理攻击。

[0008] 为了在涉及芯片卡的金融交易期间确保安全性，诸如Europay、MasterCard和Visa(EMV)交易标准的安全标准已被开发并用于保证支付终端和支付卡。然而，由于各种因素，包括满足安全标准所需的技术复杂性，用于进行安全金融交易的支付终端通常是笨重的、昂贵的且仅专门用于进行金融交易的设备。

[0009] 移动支付系统和数字钱包(例如ApplePay®、AndroidPay®和Samsung Pay®)允许消费者将他们的信用卡信息存储在他们的移动设备上，并使用他们的设备来通过近场通信(NFC)或射频识别(RFID)在适合的非接触式销售点终端上进行支付。

[0010] 然而，移动设备可能不具备被用作支付终端所需的安全标准，不是在各处都被接受，且因此不能完全消除对专用支付终端的需要。

[0011] 作为对上面详述的技术的至少一些缺点的响应，已经开发了允许通用移动设备(例如但不限于智能电话)转变为支付终端的方法。这种方法包括美国专利公开2014/0324698的方法、设备、附加装置和安全元件，其中提供了用于进行安全金融交易的方法和设备，该设备包括CPU和安全元件，其中获取从金融账户借记的购买金额，获取与金融账户相关的数据，并且获取来自与金融交易相关的金融机构的交易授权，该授权至少部分地基于仅由安全元件处理的数据而与由CPU处理的数据无关。

[0012] 此外，已经开发了方法和系统，以解决当在专用销售点终端处使用支付卡进行金融交易时通过用户的个人识别号(PIN)来安全地认证他/她的需要。这样的方法和系统(支付终端借此充当PIN输入设备(PED))旨在满足在国际标准(例如ISO 9564、支付卡行业(PCI)(PIN交易安全(PTS)和其他可适用的PCI标准))中规定的所需级别的安全性，这些标

准是为在零售银行业务中的PIN安全和管理而开发的，这些标准包括对PIN长度、选择、发行、交付、加密算法、存储、传输、安全输入的要求以及对在ATM和POS系统中的离线PIN处理的要求。

[0013] 最近已经开发了各种方法，以便确保在PIN的输入期间的一定级别的安全性。这种方法通常聚焦于庞大的支付终端，其中加扰的PIN填充图像由设备接收，叠加在底层键盘的顶部上，使得用户输入他的PIN的编码版本，且然后编码版本优选地被发送到远程服务器并被解码以处理PIN。然而，这样的方法可能不完全符合金融安全标准，可能不允许离线处理和/或可能不在移动设备上被启用来用作支付终端。

[0014] 因此，在本领域中需要一种方法和系统，其用于在移动设备上获得个人识别码(PIC)，同时提供一定级别的安全性，最小化增加的成本和/或对设计的破坏(例如，通过限制和/或消除由于其他原因还不存在于设备上的硬件部件的需要)。这种级别的安全性可以但不一定被选择以便符合某些安全标准。

[0015] 概述

[0016] 本技术的实施例基于发明人的下面的认识而被开发：在一些情况下可以不依赖于用于安全PIN输入的已知方法来在移动设备上进行符合金融行业标准的安全金融交易。因此改进是合乎需要的，特别是在旨在确保PIC被存储在安全环境中或者以加密形式存储在非安全环境中并且因此对于在主处理器上运行的不可信软件不可访问的特定改进是合乎需要的。

[0017] 本技术由发明人所做出的观察得出：虽然移动设备的使用已经大众化，但是由于缺乏在移动设备上进行PIC输入的安全方法，仍然使用庞大的支付终端来进行大多数金融交易。然而，按照在本领域中的最新发展，发明人已经设计了一种用于在提供一定级别的安全性的同时在移动设备上进行安全金融交易的方法和系统。

[0018] 本技术的目的是提供一种用于操作设备的方法和系统，该设备包括：处理器，该处理器包括隔离安全区域；显示屏，其操作地连接到显示屏控制器，该显示屏控制器操作地连接到处理器；触摸屏，其操作地连接到触摸屏控制器，该触摸屏控制器操作地连接到处理器；以及安全元件，其与处理器相关联。该方法和系统包括：生成对应表、热点布局以及加扰键盘的视觉表示；向安全元件发送对应表；向显示控制器发送加扰键盘的视觉表示；向触摸屏控制器发送热点布局；使由显示控制器在显示屏上显示加扰键盘的视觉表示；由触摸屏控制器检测在触摸板上的来自用户的触摸事件输入；由触摸屏控制器基于触摸事件输入和热点布局来生成按键事件；由触摸屏控制器对按键事件加密；将加密的按键事件发送到安全元件；由安全元件对加密的按键事件解密；以及由安全元件基于按键事件和对应表来重构与用户相关联的个人识别码(PIC)。

[0019] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，该方法和系统还包括在向安全元件发送对应表之前将对应表加密。

[0020] 一般来说，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，该方法和系统还包括在将对应表加密之后由安全元件将对应表解密。

[0021] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中PIC的未加密版本在任何给定时间处对处理器、显示控制器、触摸屏控制器和处理器的隔离安全区域中的任何一个保持不可访问。

[0022] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中PIC的未加密版本仅由安全元件可访问。

[0023] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中隔离安全区域仅访问PIC的加密版本。

[0024] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中触摸屏控制器在任何给定时间处不具有对对应表的访问权也不具有对加扰键盘的视觉表示的访问权。

[0025] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中安全元件安全地连接到处理器。

[0026] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中处理器的隔离安全区域包括可信用户界面。

[0027] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中触摸屏控制器安全地连接到可信用户界面。

[0028] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中该方法还包括通过在按键事件发生之后生成对应表来将加扰键盘的视觉表示的至少一部分重新加扰。

[0029] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中在触摸事件发生之前生成多个对应表、热点布局和加扰键盘的视觉表示。

[0030] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中加扰键盘的视觉表示是图像、视频流和键盘的视觉表示中的至少一个。

[0031] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中该方法还包括使由显示控制器显示先前与用户相关联的安全指示符。

[0032] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中先前与用户相关联的安全指示符被存储在处理器的隔离安全区域中。

[0033] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，该方法和系统还包括：由安全元件对重构的PIC加密；以及将加密的重构的PIC发送到处理器。

[0034] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中安全元件是操作地连接到处理器的硬件元件、由处理器运行的软件部件、隔离安全区域和隔离安全区域的一部分中的至少一个。

[0035] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中由处理器的隔离安全区域和安全元件之一来执行生成对应表、热点布局和加密键盘的视觉表示。

[0036] 一般而言，在说明书中描述的主题的另一方面可以体现在一种方法和系统中，其中重构与用户相关联的PIC包括将按键事件映射到对应表上。

[0037] 一般而言，在说明书中描述的主题的另一方面可以被体现为在移动设备上用于在至少两个移动设备之间进行安全金融交易(“对等银行业务”)的方法和系统。

[0038] 在其他方面中，本技术的各种实现提供了一种存储用于在设备上进行安全PIC输入的程序指令的非临时计算机可读介质，程序指令由基于计算机的系统的处理器可执行以执行上述方法中的一个或更多个。

[0039] 在其他方面中，本技术的各种实现提供了一种基于计算机的系统，例如但不限制性地是包括至少一个处理器和存储用于在设备上进行安全PIC输入的程序指令的存储器的设备，程序指令由基于计算机的系统的一个或更多个处理器可执行以执行上述方法中的一个或更多个。

[0040] 在附图和下面的描述中阐述本说明书的主题的一个或更多个实施例的细节。从描述、附图和权利要求中，主题的其他特征、方面和优点将变得明显。

[0041] 附图简述

[0042] 关于下面的描述、所附权利要求和附图，本技术的这些和其他特征、方面和优点将变得更好理解，其中：

[0043] 图1是根据本技术的实施例的设备的部件和特征的图示；

[0044] 图2a是根据本技术的实施例的可能的对应表的图示；

[0045] 图2b是根据本技术的实施例的可能的热点布局的图示；

[0046] 图2c是根据本技术的实施例的加扰键盘的可能布置的图示；

[0047] 图3是根据本技术的实施例的可能的个人识别码(PIC)认证屏幕的图示；

[0048] 图4是根据本技术的实施例的在处理器、显示控制器、触摸屏控制器和安全元件之间的通信流的流程图表示；以及

[0049] 图5是根据本技术的非限制性实施例所执行的方法的图示。

[0050] 附图的详细描述

[0051] 将在下文中参考附图更充分地描述所述技术的各种示例性实施例，在附图中示出示例性实施例。然而，当前的发明性概念可以体现在很多不同的形式中并且不应被解释为限于本文所阐述的示例性实施例。更确切地，提供这些示例性实施例，使得本公开将是彻底和完整的，且将本发明性概念的范围完全传达给本领域中的技术人员。在附图中，为了清楚起见，层和区域的尺寸和相对尺寸可能被放大。相似的数字始终指相似的元件。

[0052] 将理解，尽管术语第一、第二、第三等在本文中可用于描述各种元件，但这些元件不应被这些术语限制。这些术语用来将一个元件与另一个元件区分开。因此，下面讨论的第一元件可以被称为第二元件，而不偏离本发明性概念的教导。如本文所使用的，术语“和/或”包括相关联的所列的项中的一个或更多个的任意组合和所有组合。

[0053] 将理解，当元件被称为被“连接”或“耦合”到另一个元件时，它可以被直接连接或耦合到另一个元件，或介于其间的元件可以存在。相反，当元件被称为被“直接连接”或“直接耦合”到另一个元件时，不存在介于其间的元件。用于描述在元件之间关系的其他词应该以类似的方式被解释(例如，“在…之间”相对于“直接在…之间”、“相邻”相对于“直接相邻”等)。

[0054] 本文使用的术语仅意欲描述特定示例性实施例的目的，而不意欲限制本发明性概念。如本文使用的，单数形式“一(a)”、“一(an)”和“该(the)”意欲也包括复数形式，除非上下文清楚地指示相反的情况。还应该理解，用在本说明书中的术语“包括(comprise)”和/或“包括(comprising)”指定了所陈述的特征、整体、步骤、操作、元件和/或部件的存在，但不排除一个或更多个其他特征、整体、步骤、操作、元件、部件和/或它们的群组的存在。

[0055] 贯穿本公开，参考安全交易(例如但不限制性地是接触式和非接触式交易)、安全元件(例如但不限制性地是芯片集、安全芯片集、硬件嵌入式安全部件、软件嵌入式安全部

件或固件嵌入式安全部件)和安全标准。安全标准的示例包括但不限制性地是来自Europay、MasterCard和Visa(EMV)、EMVCo、MasterCard®、Visa®、American Express®、JCB®、Discover®和来自MasterCard®、Visa®、American Express®、Discover®和JCB®建立并特别处理用于金融交易的安全标准的定义的PCI SSC(支付卡行业安全标准委员会)的认证标准。对安全交易、安全元件和安全标准的参考是为了说明的目的而做出，并且意欲为本技术的示例而不是其范围的限制。

[0056] 处理器:在这项技术的背景下，处理器的定义包括片上系统(SoC)，一种将计算机的部件集成在单个芯片中的集成电路。典型的SoC可以包括但不限于一个或更多个通用微处理器或中央处理单元(CPU)、协处理器，例如数字信号处理器(DSP)、图形处理单元(GPU)以及多媒体协处理器，诸如MPEG和JPEG编码器和解码器。SoC还可以包括用于各种无线通信接口(包括蜂窝(例如LTE/4G、3G、GSM、CDMA等)、蓝牙和无线保真(Wi-Fi)(IEEE 802.11))的调制解调器。SoC可以包括用于与裸片上或外部DRAM存储器芯片和裸片上存储器块(包括各种ROM、SRAM、DRAM、EEPROM和闪存)通过接口连接的存储器控制器。SoC此外可以包括定时源、外围设备(包括计数器-定时器、实时定时器和上电复位发生器)、调试工具、JTAG和测试设计(DFT)接口、外部接口、模拟接口、稳压器、功率管理电路等。SoC还可以包括连接部件，例如遵循ARM高级微控制器总线体系结构(AMBA)规范的如在本领域中已知的将这些块连接在一起的连接部件，例如简单的总线或片上网络。一些块可以单独地被封装并堆叠在SoC的顶部上，在本领域中被称为堆叠式封装(PoP)的一种设计。可选地，一些块可以被包括在不同的集成电路(或裸片)中但被封装在一起，在本领域中被称为系统级封装(SiP)的一种设计。

[0057] 处理器的隔离安全区域:以特定硬件和/或软件部件为特征的处理实体受到认证，其根据特定安全标准确保特定级别的安全性。隔离安全区域确保敏感数据在保持高处理速度和大量可访问的存储器的同时在处理器的安全和可信环境中被存储、处理和保护。隔离安全区域可以提供隔离执行、安全存储、远程认证、安全供应、可信启动和可信路径。隔离安全区域允许处理器在两种逻辑模式下操作:正常世界或安全世界。正常世界由处理器的非安全区域运行，且可以包括非安全富操作系统(Rich OS)和在富OS的顶部上运行的软件部件和应用。正常世界被排斥在为了在安全世界中的排他使用而提供的访问资源之外。安全世界由隔离安全区域运行，该安全区域是具有对为了专门在安全区域中使用而供应的资源的访问权的唯一实体，例如ROM或RAM存储器、处理器或协处理器配置寄存器的某些所描绘的范围以及某些外围设备，例如显示控制器或触摸屏控制器及其相关联的配置寄存器。为了隔离安全区域的排他使用而供应的一些资源可以与SoC在同一裸片或封装上，而其他资源可以被包含在不同的裸片或封装中。一些资源可以在某些时间处为了隔离安全区域的排他使用而被动态地供应，而在其他时间处它们可以可用来由正常世界使用。隔离安全区域仅运行经授权和可信的应用，并提供安全性以抵御在富OS环境中生成的逻辑攻击、旨在危害启动固件的攻击、利用调试工具和测试接口的攻击以及其他非侵入性攻击。处理器的隔离安全区域的非限制性示例包括可信执行环境(TEE)、英特尔可信执行技术(TXT)、可信平台模块(TPM)、Hengzhi芯片和IBM嵌入式安全子系统(ESS)芯片。在一些实施例中，处理器的隔离安全区域被设计成不被访问，甚至不被人类管理员访问。在一些实施例中，隔离安全区域可以部分地或完全地经由专用硬件元件来实现，专用硬件元件是例如但不限于如在下面

的段落中定义的安全元件。隔离安全区域的其他变型也可由在本技术的领域中的技术人员设想而不偏离本技术的范围。

[0058] 安全元件：以特定硬件和/或软件部件为特征的处理实体受到认证，其根据特定安全标准确保特定级别的安全性。从硬件角度来看，安全元件包括在计算实体中存在的常见部件：至少一个微处理器(例如CPU)、存储器(例如ROM、RAM或闪存)、通信接口等。还可以包括特定硬件部件以实现安全元件所独有的特定功能。例如，可以包括加密加速器。此外，可以包括各种防篡改、篡改检测和/或篡改响应特征，以防止恶意人员从安全元件提取敏感信息。防篡改措施可以包括硬件方面、软件方面或硬件和软件的组合。此外，在安全元件中可以包括防止旨在恢复加密密钥或其他敏感信息的边信道攻击的某些对策。对抗边信道攻击的对策可包括硬件方面、软件方面或两者。此外，可以包括减少EM发射的措施，例如屏蔽，以保护安全元件免受窃听。在金融交易的背景下，安全元件的认证确保各种金融实体愿意使用安全元件来存储和处理关键金融数据，并使用关键金融数据来执行安全金融交易。在一些实施例中，安全元件可以仅由软件部件来表征。在一些实施例中，安全元件可以部分地或完全地被实现为处理器的隔离安全区域，例如，如在上面的段落中描述的隔离安全区域，在这种情况下，安全元件可以被实现(例如但没有限制性地)为TEE、TPM和/或ESS。安全元件的其他变型也可由在本技术的领域中的技术人员设想而不偏离本技术的范围。

[0059] 触摸屏：具有输入和/或输出接口的触敏传感器设备通常叠加在信息处理系统的电子可视显示器的顶部上。触摸屏通常通过检测与触摸屏显示器的触觉和/或触感接触来工作。触摸屏技术可以包括但不限于电阻式、声表面波、电容式、投射式电容、红外栅格、红外丙烯酸投影(infrared acrylic projection)、光学成像、色散信号技术和声脉冲识别触摸屏。触摸屏可以包括力敏感部件以检测施加到屏幕的压力。触摸屏还可以包括触觉反馈部件。触摸屏的其他变型也可由在本技术的领域中的技术人员设想而不偏离本技术的范围。

[0060] 触摸屏控制器：检测由触摸屏输出的模拟触摸信号的控制器可以执行模拟输出的模数转换，可以执行信号处理步骤以调节信号并推导与一个或更多个触摸事件相关联的屏幕坐标。一般但非限制性地，触摸事件的坐标将使用低带宽串行接口(包括串行外围接口(SPI)和集成电路间(I^2C)接口)来输出到处理器，如本在领域中已知的。触摸屏控制器可以与显示控制器或任何其他块集成在一起。触摸屏控制器的其他变型也可由在本技术的领域中的技术人员设想而不偏离本技术的范围。

[0061] 显示屏：用于向用户传达可视信息的具有输入和/或输出接口的电子可视显示设备。显示屏技术可以包括但不限于液晶显示器(LCD)、基于有机发光二极管(OLED)技术的显示器、基于有源矩阵有机发光二极管(AMOLED)技术的显示器。

[0062] 显示屏控制器：能够从在存储器中的帧缓冲器或从标准数字接口(例如MIPI或eDP)输入数字图像数据，并以适当的帧速率(例如，使用LVDS)输出适于与特定显示屏技术通过接口连接的模拟或数字视频信号的设备。显示控制器可以被包括在与处理器SoC相同的裸片或封装中，或者是分立部件，或者与显示屏集成在一起，或者组合。显示控制器可包括用于图像按比例放大、按比例缩小、旋转和混合的功能。

[0063] 可信用户界面(TUI)：软件、硬件和外围资源的组合，这些资源可以被保留用于隔离安全区域的排他使用，并且可以被配置为将显示屏(或其一部分)和触摸传感器的排他和

不可中断的控制给予隔离安全区域，并且保持所显示的图像和由触摸传感器和控制器生成的触摸事件的完整性和保密性。在设备中的TUI可以受到认证，其根据特定的安全标准确保特定级别的安全性。TUI自动检测并且仅允许经授权或可信的应用来访问安全屏幕存储器的内容。在一个实施例中，TUI是一种特定模式，其中设备由处理器的隔离安全区域控制，以确保在触摸屏上显示的信息来自可信源并且与操作系统隔离。TUI的其他变型也可由在本技术的领域中的技术人员设想而不偏离本技术的范围。

[0064] 信息/数据：术语“信息”和“数据”可互换地使用，并且为了本公开的目的而具有相似的含义。

[0065] 安全标准可以包括多个安全级别，例如但没有限制性地是级别1、级别2或级别3。作为示例但没有限制性地，级别1可以对应于比级别2更高级别的安全性，而级别2又可以对应于比级别3更高级别的安全性。例如但没有限制性地，EMCo标准可以提供安全级别以及批准和认证标准的示例，例如终端类型批准过程、安全评估过程、卡类型批准过程或移动类型批准过程。

[0066] 例如，终端类型批准过程可以是测试符合Europay、MasterCard和Visa(EMV)规范的机制。终端类型批准可以提供一定级别的置信度：在兼容的应用之间的互操作性和一致行为可以被实现。在一个示例中，终端类型批准测试可以分为两个级别：级别1和级别2。级别1类型批准过程可测试与在EMV规范中定义的机电特性、逻辑接口和传输协议要求的兼容性。级别2类型批准可测试与如在EMV规范中定义的借记/信贷应用要求的兼容性。此外，终端类型批准测试可以包括级别3批准，其保证在终端上执行的应用与金融机构之间的安全通信。

[0067] 尽管上面定义的各种部件每个与定义相关联，但是应当理解，各种部件中的每一个不应被解释为仅限于在相关联的定义中提供的特定功能和/或细节。相反，可以添加、移除或组合其他功能和/或细节而不偏离本技术的范围。另外，功能和/或细节可以从一个部件切换到另一个部件而不偏离本技术的范围(例如，与触摸屏相关联的功能可以切换到触摸屏控制器)。各种部件中的一些也可以部分地或完全地合并在一起而不偏离本技术的范围(例如，触摸屏和触摸屏控制器可以合并在一起以定义单个部件，或者显示控制器和处理器可以合并在一起以定义单个部件)。

[0068] 图1是示出根据本技术的一个实施例的说明性设备100的各种示例性部件和特征的框图。

[0069] 根据本文描述的至少一个实施例，提供了一种用于在设备上进行安全金融交易的方法和系统。该设备包括：处理器，该处理器包括隔离安全区域；显示屏，其操作地连接到显示屏控制器，该显示屏控制器操作地连接到处理器；触摸屏，其操作地连接到触摸屏控制器，该触摸屏控制器操作地连接到处理器；以及安全元件，其与处理器相关联。

[0070] 在一些实施例中，该设备可以被实现为包括执行在下文详述的方法和系统所需的部件的任何设备。在一些实施例中，该设备可以包括智能手机、平板手机、智能手表和/或穿戴式计算机、PDA、平板电脑和计算机。在一些可选的实施例中，设备还可以嵌在不仅仅专用于计算和/或信息处理功能的对象之中或之上，例如但不限于车辆、一件家具、器具等。

[0071] 在所示的实施例中，设备100包括移动堆叠式封装(PoP)芯片集110、叠加在LCD显示器130上的投射式电容触摸面板、显示控制器和触摸屏控制器140、安全元件和非接触式

前端150以及闪存120。

[0072] 在非限制性实施例中，移动PoP芯片集110包括与SoC应用处理器114堆叠的低功率双数据速率(LP DDR)存储器112。SoC应用处理器114包括隔离安全区域(ISA)115、中央处理单元(CPU)116、可信用户界面(TUI)117、安全只读存储器(ROM)118和安全随机存取存储器(RAM)119。LP DDR 112包括安全RAM存储器113。移动PoP芯片集110连接到包括安全对象122的闪存120。

[0073] 在本技术的一些实施例中，设备可以执行非安全操作系统(OS)。在SoC应用处理器114上运行的OS的示例包括但不限于可从苹果公司获得的iOS®的版本或其衍生物；可从Google公司获得的Android OS®的版本或其衍生物；可以从RIM公司获得的PlayBook OS®的版本或其衍生物。应当理解，可以同等地使用其他专有OS或定制OS而不偏离本技术的范围。

[0074] 在本技术的一些实施例中，隔离安全区域可以执行安全OS，该安全OS与由处理器的非安全区域执行的OS是分离的、不同的和隔离的。安全OS通常具有比非安全OS更高的特权级别，这允许它例如将非安全OS排除在访问敏感资源之外。安全OS可以与非安全OS(例如安全微核)完全不同，或者可以与非安全OS(例如Android OS®的修改版本)实质上相同。

[0075] 触摸屏控制器144通过串行外围接口(SPI)或内部集成电路(I^2C)接口(在本领域中已知的用于将集成电路(IC)附接到处理器和微控制器的串行接口)连接到可信用户界面116。如本领域中的技术人员将认识到的，触摸屏控制器144使用在主机和设备之间的MIPI显示串行接口(MIPI-DSI)或嵌入式显示端口(eDP)连接、通信协议和串行总线连接到可信用户界面116和显示控制器142。透射式电容触摸面板134叠加在LCD显示器132上。安全元件152通过SPI总线接口连接到SoC应用处理器114。非接触式前端140使用i^2C接口连接到SoC应用处理器114。在一些实施例中，触摸屏控制器144可以安全地连接到TUI 117，使得在触摸屏控制器144和TUI 117之间的数据的每次传输都被加密。在一些实施例中，安全元件152安全地连接到非接触式前端154和SoC应用处理器114，使得在安全元件152、非接触式前端152和SoC应用处理器之间的数据的每次传输都被加密。如本技术的领域中的技术人员将认识到的，设备和连接的这种示例仅为了说明目的而被提出，并且其他变型也是可能的。

[0076] 现在转到图2a，示出了对应表200的非限制性示例。在一些实施例中，对应表200可以是数组。对应表200的每一列可以表示在键盘上的位置202。与每个位置202相关联的是值204。在一些实施例中，伪随机数生成器(PRNG)可以生成每个值204，使得每个值在对应表200中只有一次出现，并且每个值同等可能地出现在给定位置上。对应表200然后可以用于生成加扰键盘，例如图2c的加扰键盘。如本领域中的技术人员将认识到的，对应表的其他实施例也是可能的，其中值由字母或符号代替。在一些实施例中，对应表一旦生成，就可以被发送到安全元件以用于PIC的后续重构。

[0077] 现在转到图2b，示出热点布局240的图形表示的非限制性示例。热点布局240对应于可由用户在触摸屏上按下的每个键的几何形状和位置。作为非限制性示例，热点布局可以规定：表示在键盘上的位置1的键245对应于其坐标位于由坐标242和244定义的矩形内的每个触摸事件。热点布局240可以被发送到触摸屏控制器，并且触摸屏控制器可以根据热点布局来处理触摸事件以输出按键事件。

[0078] 现在转到图2c，示出了加扰键盘280的视觉表示的非限制性示例。可以通过组合在

对应表220和热点布局240中的信息来生成具有值285的加扰键盘280的视觉表示。在其他实施例中，加扰键盘280可以由其他类型的对应表和热点布局生成。应当理解，如本领域中的技术人员将认识到的，加扰键盘280仅由于说明性目的而呈现，并且加扰键盘的其他形式和布置是可能的。在一些实施例中，加扰键盘280可以是PIC输入屏幕(例如图3的PIC输入屏幕)的一部分，并且被发送以由显示控制器显示在显示屏幕上。

[0079] 加扰键盘为PIC输入提供了一定级别的安全性，因为它使由恶意人员或软件进行PIC的直接观察的过程变得更加麻烦。即使恶意人员或软件具有对触摸事件输出或按键事件的访问权，也不可能在不知道加扰键盘的对应表的情况下重构PIC。在每个触摸事件之后重新加扰键盘可以增加额外级别的安全性。

[0080] 现在转到图3，示出了用于进行安全交易的个人识别码(PIC)输入屏幕的非限制性实施例。在本技术的实施例中，PIC是个人识别号码(PIN)。PIN输入屏幕可以是由CPU和/或设备的处理器的隔离安全区域运行的应用或软件的一部分。在其他实施例中，PIN输入屏幕可以是独立应用、另一应用的扩展的一部分，但不限于此，或者可以在需要安全PIN输入时由来自另一应用的过程调用来调用。PIN输入屏幕300可以显示在屏幕的一部分或整个屏幕上，并且可以与出现在屏幕的不同部分上的另一应用并行地运行。在该实施例中，标识310显示在PIN输入屏幕300的顶部上。提示用户输入她的/他的PIN的文本320显示在标识310下。带有与由用户在触摸屏上按下的键相对应的星号的数据输入字段330显示在提示文本320下。加扰键盘340显示在数据输入字段330下，具有正确、确认和验证按钮350。与用户相关联的安全指示符360显示在屏幕的底部上。安全指示符360包括在用户和可信实体(例如但不限于持有他的账户的金融机构)之间共享的秘密。共享秘密可以是图像、标语或由用户识别的任何其他秘密信息，并且被显示，使得用户可以确信他正在安全地连接到他/她的金融机构的可信服务器的可信应用上输入他的PIC。安全指示符360可以是视频流，其中每个单帧包含安全指示符的一部分，例如恶意人员或软件可能不能从单个照片或截屏再现安全指示符。在一些实施例中，加扰键盘可以由不同的符号和/或数字和/或字母组成。在可选的实施例中，安全指示符可以是视觉的和/或听觉的和/或嗅觉的和/或触觉的，假定设备具有支持这样的实施例所需的技术。如本技术的领域中的技术人员将认识到的，该示例仅用于说明性目的，并且可以定义PIC输入屏幕的许多版本。

[0081] 图4是根据本技术的方法和系统的实施例在SoC应用处理器404的隔离安全区域、显示控制器406、触摸屏控制器408和安全元件402之间的通信流的流程图表示。在当前技术的其他实施例中，显示控制器406和触摸屏控制器408可以合并在单个部件中。在其他实施例中，安全元件的角色可以由云中的安全服务器担任。在该实施例中，SoC应用处理器404的隔离安全区域生成对应表、加扰键盘的图像和坐标，以界定在加扰键盘中的每个键，这也称为本领域中的热点布局。SoC应用处理器404将加扰键盘图像发送到显示控制器406。SoC应用处理器404将热点布局发送到触摸屏控制器408。SoC应用处理器404将对应表加密并将其发送到安全元件402。

[0082] 在其他实施例中，由SoC应用处理器404的隔离安全区域控制的TUI可以生成对应表、热点布局、加扰键盘图像，并将加扰键盘图像发送到显示控制器406，将热点布局发送到触摸屏控制器408，并将对应表发送到安全元件402。在可选的实施例中，安全元件402可以生成对应表、热点布局、加扰键盘图像，并将加扰键盘图像发送到显示控制器406，并将热点

布局发送到触摸屏控制器408。触摸屏控制器408(其已经接收到热点布局并从而知道由处理器404的隔离安全区域定义的键的位置和尺寸,但不知道它们的值)可以由用户用热点布局来处理触摸事件输入,以创建一个或更多个按键事件,并加密因而产生的按键事件。触摸屏控制器408可以向安全元件402发送加密的按键事件。在一些实施例中,触摸屏控制器408直接连接到安全元件402。在其他实施例中,触摸屏控制器408可以向SoC应用处理器404的隔离安全区域发送加密的按键事件,且隔离安全区域404然后可以向安全元件408发送加密的按键事件。最后,安全元件402可以将加密的按键事件和加密的对应表解密以重构PIC。在一些实施例中,安全元件402是能够将加密的对应表和加密的按键事件解密的唯一部件。在其他实施例中,安全元件402是能够从对应表和按键事件的未加密版本重构PIC的唯一部件。在可选的实施例中,安全元件402是具有对PIC的未加密版本的访问权的唯一部件。在重构PIC之后,安全元件402可以将重构的PIC加密,并将加密的PIC发送到隔离安全区域404。在一些实施例中,在重构PIC之后,在将PIC与其他信息一起加密之前,PIC可以与其他信息组合。例如,在金融交易的情况下,PIN可以与个人账户号(PAN)组合以形成PIN块,如由ISO 9564标准规定的。在加密的PIC被发送到隔离安全区域之后,隔离安全区域可以通过互联网或其他网络、可能通过处理器的非安全区域的通信接口来将加密的PIC发送到持有用户账户的金融机构,使得交易可以被授权。

[0083] 参考图1至图4描述了与使用PIC进行交易的问题相关地使用的系统和计算机实现的方法的一些非限制性示例实例,现在我们将参考图5描述对该问题的一般解决方案。

[0084] 更特别地,图5示出了说明用于在设备上进行安全PIC输入的第一计算机实现的方法500的流程图。在一些实施例中,安全PIC输入指使用移动设备的安全金融交易。在一些实施例中,第一计算机实现的方法500可以(完全或部分地)在移动设备100上实现。

[0085] 方法500以步骤502开始,生成对应表、热点布局和加扰键盘图像,例如但不限于图2a的对应表、图2b的热点布局和图2c的加扰键盘图像。在一些实施例中,可以在处理器115的隔离安全区域中生成对应表、热点布局和加扰键盘图像。在可选的实施例中,可以在安全元件152中生成对应表、热点布局和加扰键盘图像。在其他实施例中,对应表、热点布局和加扰键盘图像可以由外部安全模块生成,并安全地发送到处理器115的隔离安全区域。在一些实施例中,对应表、热点布局和加扰键盘图像可以由外部设备或服务器生成,由通信网络加密并发送到设备。根据本技术的可选实施例,可以同时生成一个或更多个对应表、热点布局和加扰键盘图像。根据其他实施例,可以在不同时间处生成一个或更多个对应表、热点布局和加扰键盘图像。

[0086] 一般但非限制性地,为了生成加扰键盘,首先创建对应表或数组,其中数组的大小对应于键盘中的键的数量。数组中的从0到9的每个位置具有针对值的随机数,使得从0到9的每个数字在数组中作为值只出现一次。然后可以从对应数组生成加扰键盘图像,其中每个键的位置具有对应的值。还可以生成热点布局,其中定义了可操作的键的位置和几何形状。在一些实施例中,热点布局的几何形状和位置也可以被随机化和/或编码,并且可以进一步被加密。如本领域中的技术人员将认识到的,用于生成对应表、热点布局和加扰键盘图像的不同方法也是可能的。

[0087] 加扰键盘图像然后可以整合在PIC输入屏幕中,例如来自图3的PIC输入屏幕。加扰键盘的视觉表示可以以图像的形式生成。在本技术的另一个实施例中,加扰键盘可以以视

频流的形式生成，其中视频流的每个单帧包含键盘的一部分，并且帧的快速连续性使视频流对人眼呈现为静态图像。这可以通过使借助于拍摄设备或屏幕捕获来捕获加扰键盘的过程更加麻烦而增加一层安全性，因为没有单个帧包含足够的信息来重构加扰键盘，并从而获得对应表的知识。

[0088] 接下来在步骤504处，加扰键盘的对应表被发送到安全元件152。在一些实施例中，对应性可以在被发送到安全元件152之前被加密。

[0089] 接下来在步骤506处，加扰键盘图像被发送到显示控制器142。在一些实施例中，包括不同加扰键盘的多个不同PIC输入屏幕可以被发送到显示控制器142。在其他实施例中，TUI 117可以生成对应表、热点布局、加扰键盘图像，并将加扰键盘图像发送到显示控制器142。在一些实施例中，PIC输入屏幕可以包括安全指示符。在其他实施例中，加扰键盘图像在被发送到显示控制器142之前从安全元件发送到隔离安全区域。在可选的实施例中，对应表、热点布局和加扰键盘图像可以在安全元件115中生成，其中安全元件115直接连接到显示控制器142，且然后被发送到显示控制器。

[0090] 在步骤508处，热点布局被发送到触摸屏控制器。在一些实施例中，热点布局在处理器的隔离安全区域中生成，并被发送到触摸屏控制器。在其他实施例中，热点布局在安全元件中生成，被加密并发送到触摸屏控制器。

[0091] 在步骤510处，显示控制器142使在显示屏132上显示加扰键盘图像。加扰键盘图像可以显示在显示屏132的任何部分上。在一些实施例中，加扰键盘图像的每个键可以显示在包括嵌入式屏幕的相应物理键上。在其他实施例中，安全指示符可以与加扰键盘同时显示。

[0092] 在步骤512处，触摸屏控制器144检测在来自用户的在触摸屏134上的一个或更多个触摸事件输入。触摸事件输入可以由用户用她的/他的手指、用触笔/笔或者用由触摸屏134可以感测到的任何东西来输入。作为非限制性示例，触摸屏134可以使用投射式电容(p-cap)技术来感测输入，其中电容式传感器检测导电的或具有不同于空气的介电常数的任何东西。电容式传感器包括单独的电极或电极交叉点，这些电极或电极交叉点由触摸屏控制器重复和迭代地扫描，以便检测电容的变化。具有相应状态(例如触摸或释放)的精确x-y触摸坐标可以通过内插来自多个相邻电极或交叉点的电容值来确定。在一些实施例中，触摸屏134还可以包括压力传感器以检测压力的不同水平。在可选的实施例中，在每次触摸事件输入之后，在屏幕上显示的键盘可以被处理器115的隔离安全区域重新加扰或改变为不同的布局，使得在由用户每次触摸输入之后出现不同的加扰键盘。在可选的实施例中，鼠标、触控板或触摸屏可以连接到设备，并且相应的事件可以由触摸屏控制器或处理器的隔离安全区域处理。

[0093] 在步骤514处，触摸屏控制器144基于由用户在步骤512处的触摸事件输入来生成一个或更多个按键事件。触摸屏控制器首先将用户的模拟触摸事件输入处理成数字触摸事件输出。基于由用户在触摸屏上的触摸事件输入来生成触摸事件输出在本技术的领域中是已知的。在一些实施例中，如果触摸屏134包括压力传感器，则还可以生成z触摸坐标。在可选的实施例中，触摸屏控制器144可以不考虑不是单个触摸输入的每个手势，例如但不限于划动手势或多触摸手势。在一些实施例中，多个触摸事件输出可以对应于单个按键事件。通过将触摸事件输出坐标与热点布局进行比较，可以将触摸事件输出坐标转换成按键事件，其中触摸事件可以对应于在加扰键盘上的位置“2”，因为触摸事件的输出坐标落在位置“2”

处的热点的限制内。

[0094] 在步骤516处，触摸屏控制器144对在步骤514处生成的一个或更多个按键事件加密。在一些实施例中，一个或更多个按键事件可以使用非对称密码术来加密，而在其他实施例中可以使用对称密码术。在一些实施例中，可以使用分组密码，而在其他实施例中，可以使用流密码。在另一些其他实施例中，可以使用白盒密码术。如果使用非对称密码术，则可以使用公共或私有加密密钥来对按键事件加密。一些实施例可以采用RSA算法，而其他实施例可以采用基于椭圆曲线、离散对数问题或其他数学原理的算法。如果使用对称密码术，则密钥是秘密的，并且加密算法可以是DES、TDES或AES或者本领域中已知的其他加密方法。在一些实施例中，触摸屏控制器可以根据金融业的加密安全标准来对触摸事件加密。在一些实施例中，所使用的密钥可以针对每个交易而改变，并且对于每个设备是唯一的。更特别地，可以根据ANSI X9.24规范和每交易动态唯一密钥(DUKPT)方法来改变密钥。

[0095] 在步骤518处，触摸屏控制器144发送步骤516的加密的按键事件。在一些实施例中，触摸屏控制器144将加密的按键事件发送到安全元件152。在其他实施例中，触摸屏控制器144可以直接连接到安全元件152。在可选的实施例中，触摸屏控制器可以将加密的按键事件发送到处理器115的隔离安全区域，且加密的按键事件然后可以通过处理器的隔离安全区域被发送到安全元件152。

[0096] 如对本领域中的技术人员将容易明显的，图5中的一些步骤的各种其他顺序是可能的。例如在一些实施例中，可在步骤506和/或步骤508之后执行步骤504。在一些实施例中，步骤504和518可以同时执行。在其他实施例中，可以在步骤518之后执行步骤504。

[0097] 在步骤520处，安全元件152将加密的按键事件解密。在一些实施例中，可以使用私有加密密钥来将加密的按键事件解密。在其中加扰键盘的对应表先前已被加密的实施例中，它在加密的触摸事件之前、之后或同时被解密。

[0098] 在步骤522处，安全元件152基于一个或更多个按键事件和加扰键盘的对应表来重构与用户相关联的PIC。在一些实施例中，通过执行通过找到与按键事件的位置相对应的值来输出PIC的功能来重构PIC。通过查阅对应表，该功能可以确定对应于“2”的按键事件与值5相关联。然后，该功能可以确定按键事件对应于5的PIC输入。如在本技术的领域中的技术人员可以认识到的，该示例仅作为用于重构PIC的说明性示例被提供，并且是用于确定对应的按键事件的可能方法之一。

[0099] 在一些实施例中，重构的PIC由安全元件加密。在一些实施例中，加密的PIC在被安全元件加密之后被发送到处理器的隔离安全区域。加密的PIC然后可以经由通信网络发送到远程服务器以完成交易。在其中对应表先前已被加密的可选实施例中，加扰键盘的加密对应表和加密按键事件可在被远程服务器解密和重构到PIC之前被发送到远程服务器。在可选的实施例中，可以提示用户提供附加的验证方法，包括但不限于生物统计数据、第二PIC或与用户相关联的任何其他计算机可读信息。

[0100] 本方法和系统可以在不同的非限制性上下文中被使用。示例性使用是在客户和商家之间的金融交易期间，其中移动设备(例如电话或平板电脑)实现该方法和系统，并且可以由商家用作支付终端。客户可以在设备上轻敲他的卡以进行支付，该卡包括RFID或NFC芯片，该设备还包括RFID或NFC接口以与卡通信。设备可以呈现带有与用户相关联的安全指示器的PIC输入屏幕，并提示用户输入他的PIC以确认交易。在一些实施例中，客户可以从商家

和/或持有与客户相关联的相关账户的金融机构接收交易的确认。

[0101] 另一示例性使用是在对等交易期间，其中拥有支付卡的第一人可以将资金转移到拥有移动设备的第二人。第一人可以在第二人的移动设备上轻敲他或她的卡，该卡包括RFID或NFC芯片，该设备还包括RFID或NFC接口以与卡通信。第二人可以向设备呈现包括与第一人相关联的安全指示器的PIC输入屏幕，并提示第一人输入他的PIC以确认交易。也可以相反的方式进行支付，其中资金从第二人的设备转移到第一人的卡，在这种情况下，第二人在他自己的设备上输入他自己的PIC。

[0102] 另一示例性使用是在两个人之间的交易期间，这两个人具有启用NFC或RFID的设备。这两个人可以通过使他们的设备靠近在一起来交换资金。可选地，这两个人可以通过通信网络远程发起和执行交易。在任一情况下，为了确认交易，可以用PIC确认屏幕来提示至少一个人完成交易。

[0103] 值得注意的是，上述特征和示例并不意味着将本公开的范围限制到单个实施例，因为其他实施例通过一些或所有所述或所示的元件的交换是可能的。此外，在可以使用已知部件部分地或全部实现本公开的某些元件的情况下，仅描述了理解本公开所必需的这种已知部件的那些部分，并且省略了对这种已知部件的其他部分的详细描述，以便不使本公开模糊。在本说明书中，示出单个部件的实施例不应限于包括多个相同部件的其他实施例，反之亦然，除非在本文中明确地说明。此外，申请人并不打算将说明书或权利要求书中的任何术语归因于不寻常或特殊的含义，除非如此明确地阐述。此外，本公开包括在本文通过说明而提及的已知部件的当前和未来的已知等同物。

[0104] 具体实施例的前述描述所以充分揭示本公开的一般性质，其他人可以通过应用在相关领域的技术范围内的知识(包括在本文通过引用而引证和合并的文档的内容)来在没有过度实验的情况下容易修改和/或适应这样的具体实施例的各种应用而在不偏离本公开的一般概念。因此，基于本文提出的教导和指导，这样的适应和修改被规定为在所公开的实施例的意义或等同物范围之内。应当理解，本文中的短语或术语是为了说明而不是限制的目的，使得本说明书的术语或短语应由技术人员根据本文提出的教导和指导结合在相关领域中的技术人员的知识来解释。

[0105] 尽管已经参考以特定顺序执行的特定步骤描述和示出了上述实现，但是将理解，这些步骤可以被组合、细分或重新排序而不偏离本技术的教导。这些步骤可以并行或串行地执行。因此，步骤的顺序和分组不是本技术的限制。

[0106] 虽然上面已经描述了本公开的各种实施例，但是应当理解，它们仅借助于示例而不是限制来呈现。对于相关领域中的技术人员将明显，可以在其中进行形式和细节上的各种改变而不偏离本公开的精神和范围。因此，本公开不应由上面所描述的示例性实施例中的任一个限制，而应当仅仅根据接下来的权利要求以及它们的等同物来限定。

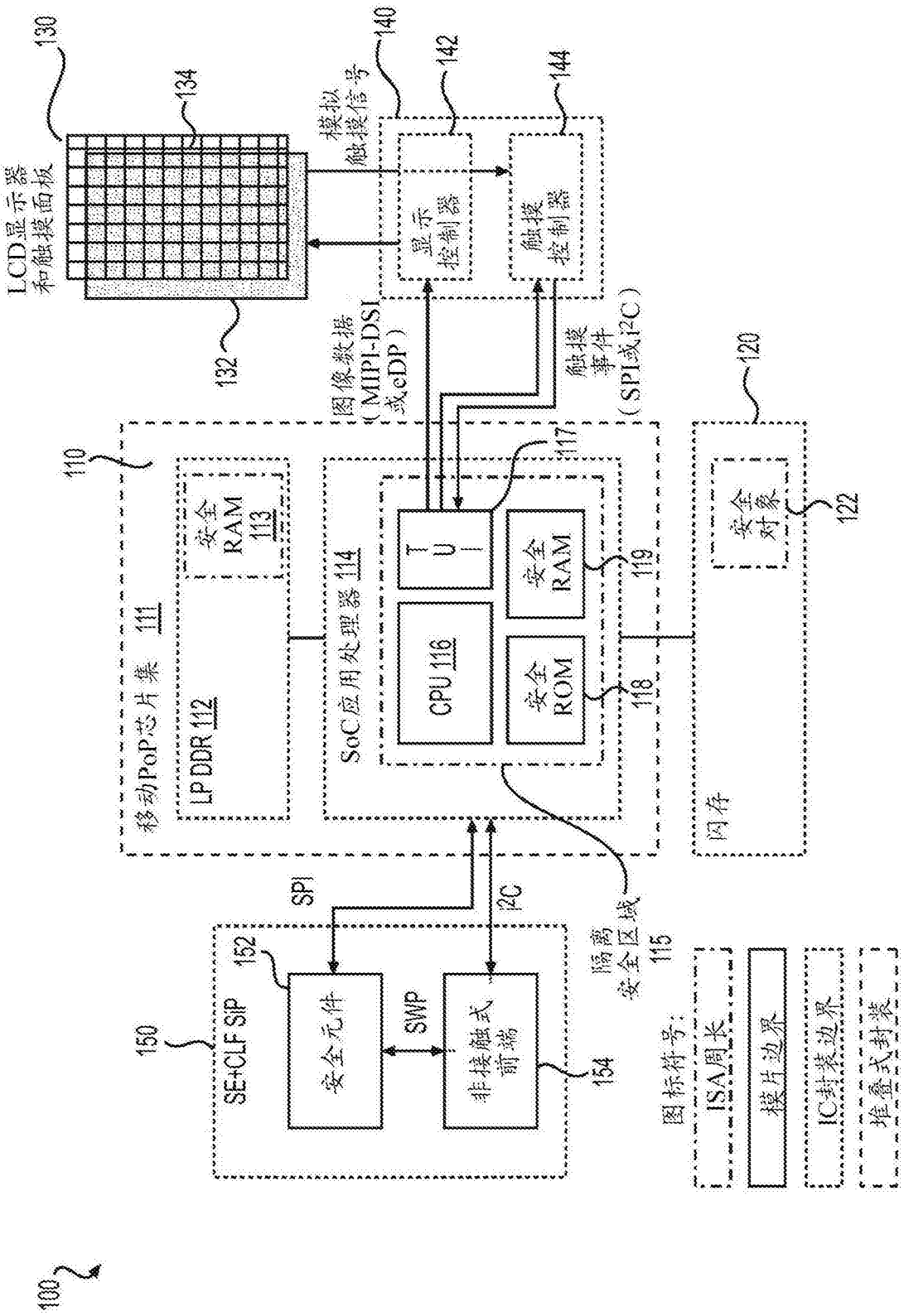
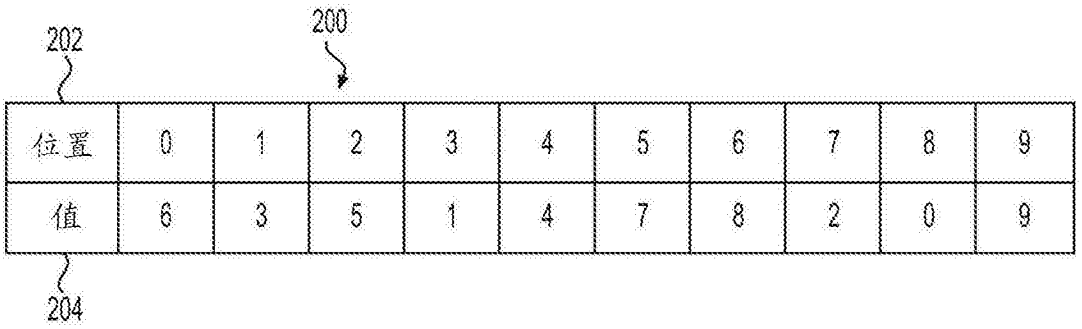

100
110
移动PoP芯片集 111
LP DDR 112
安全 RAM 113
SoC应用处理器 114
CPU 116
TUI 117
安全 RAM 119
安全 ROM 118
闪存 120
安全对象 122
LCD显示器和触摸面板 130
132
134
模拟触摸信号 140
显示控制器 142
触摸控制器 144
图像数据 (MIPI-DSI或eDP)
触摸事件 (SPI或I2C)
隔离安全区域 115
SPI
I2C
SE+CLF SIP 150
安全元件 152
SWP
非接触式前端 154
图标符号:
ISA周长
接片边界
IC封装边界
堆叠式封装

图1



位置	0	1	2	3	4	5	6	7	8	9
值	6	3	5	1	4	7	8	2	0	9

图2A

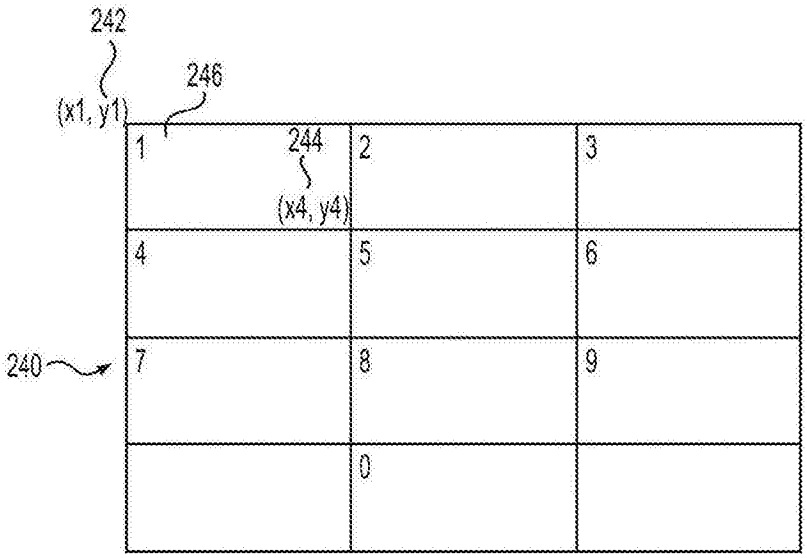


图2B

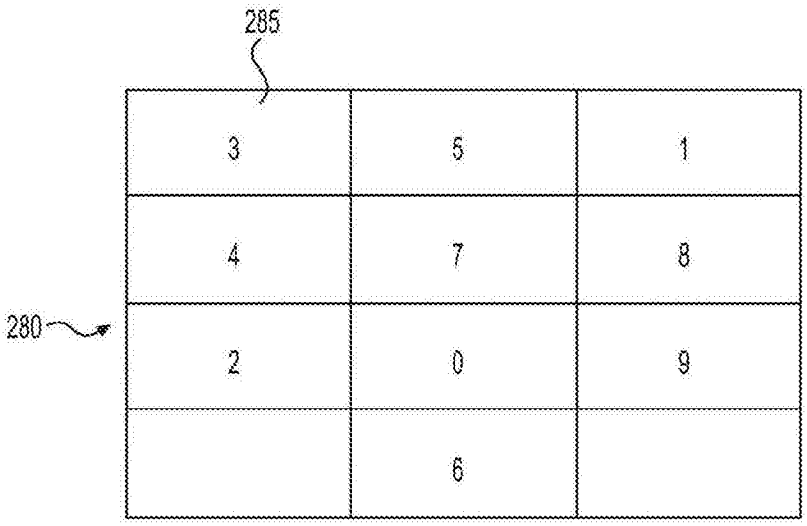


图2C

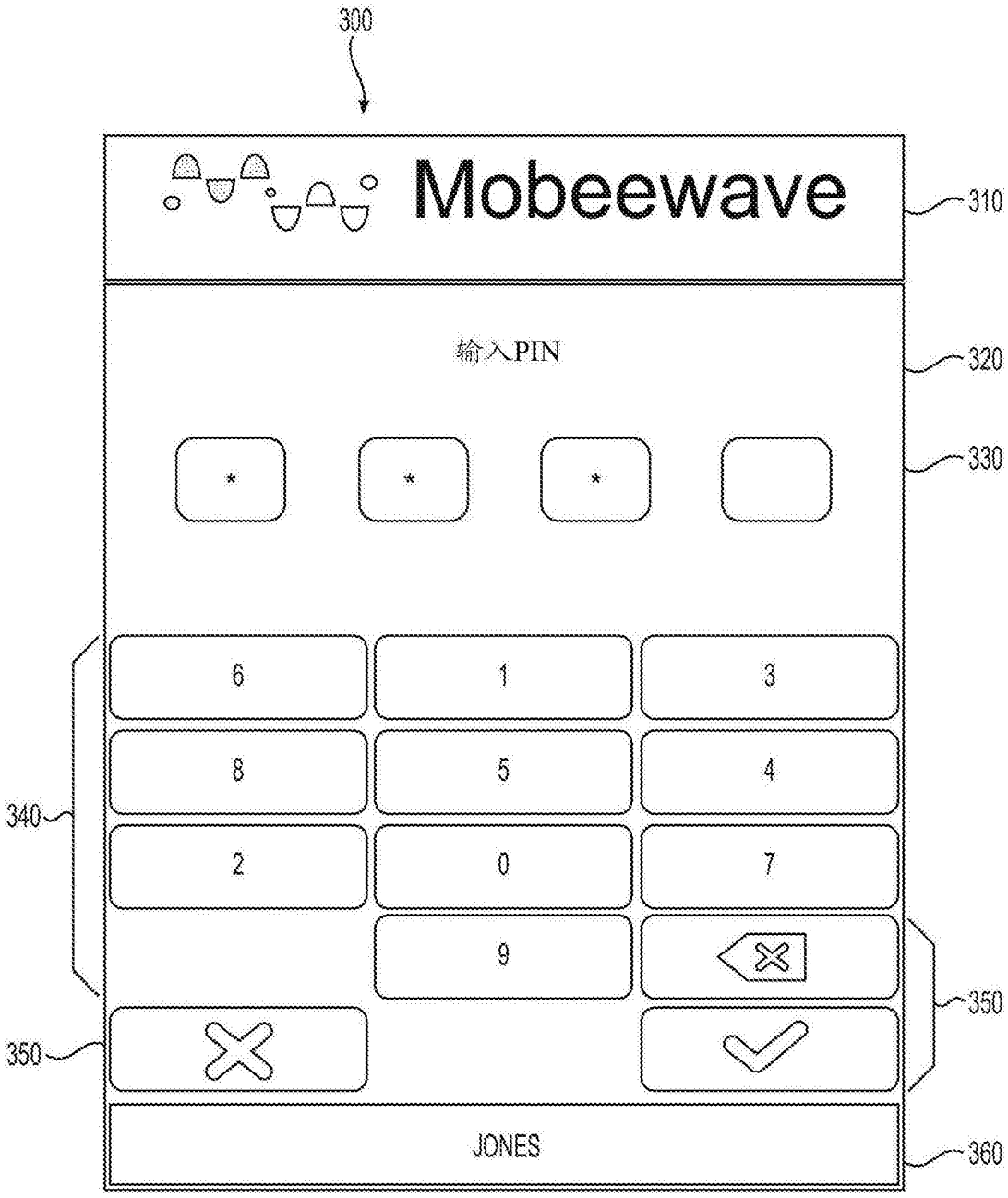

300
Mobeewave
310
输入PIN
320
*
*
*
330
6
1
3
8
5
4
340
2
0
7
9
350
350
JONES
360

图3

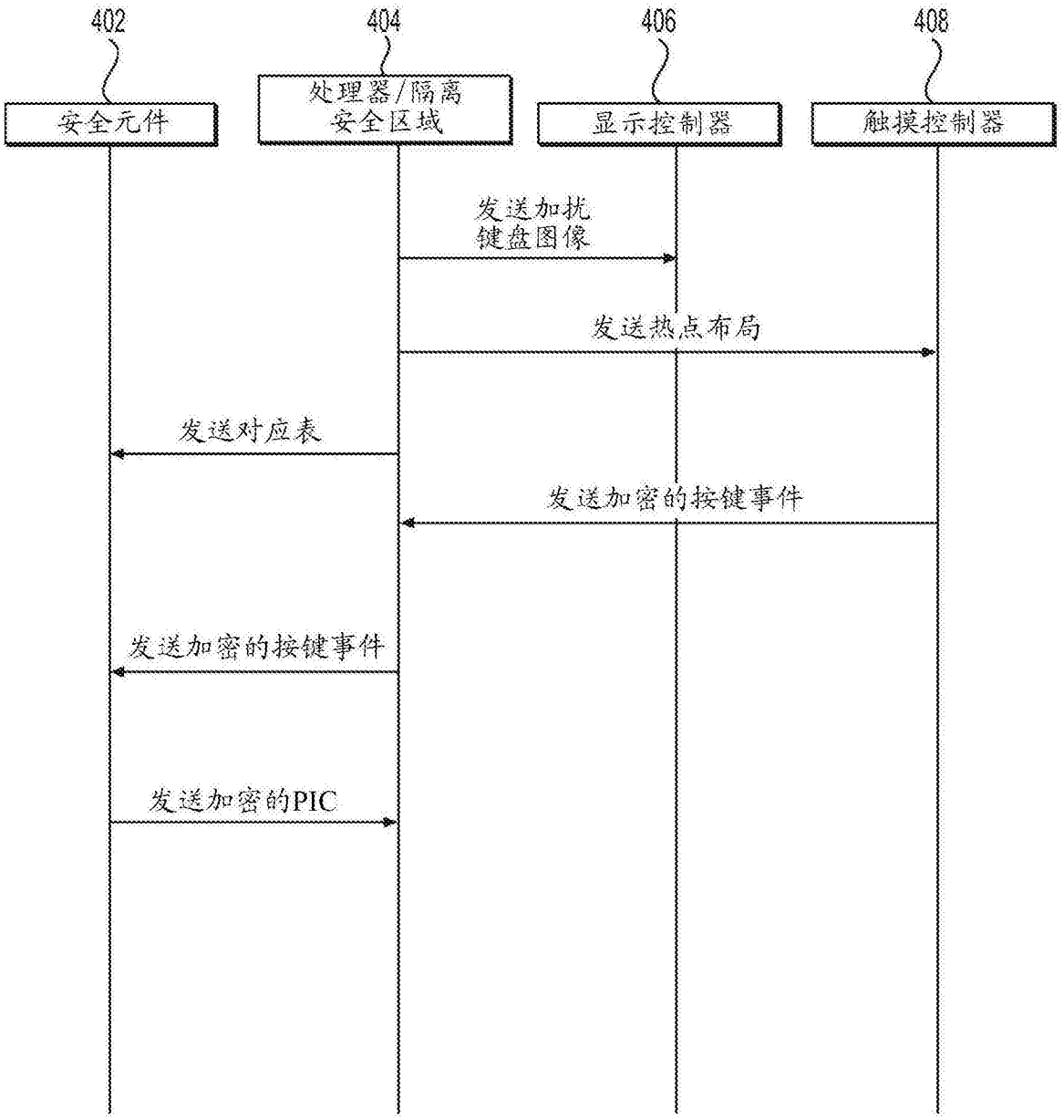

402
404
406
408
安全元件
处理器/隔离
安全区域
显示控制器
触摸控制器
发送加扰
键盘图像
发送热点布局
发送对应表
发送加密的按键事件
发送加密的按键事件
发送加密的PIC

图4

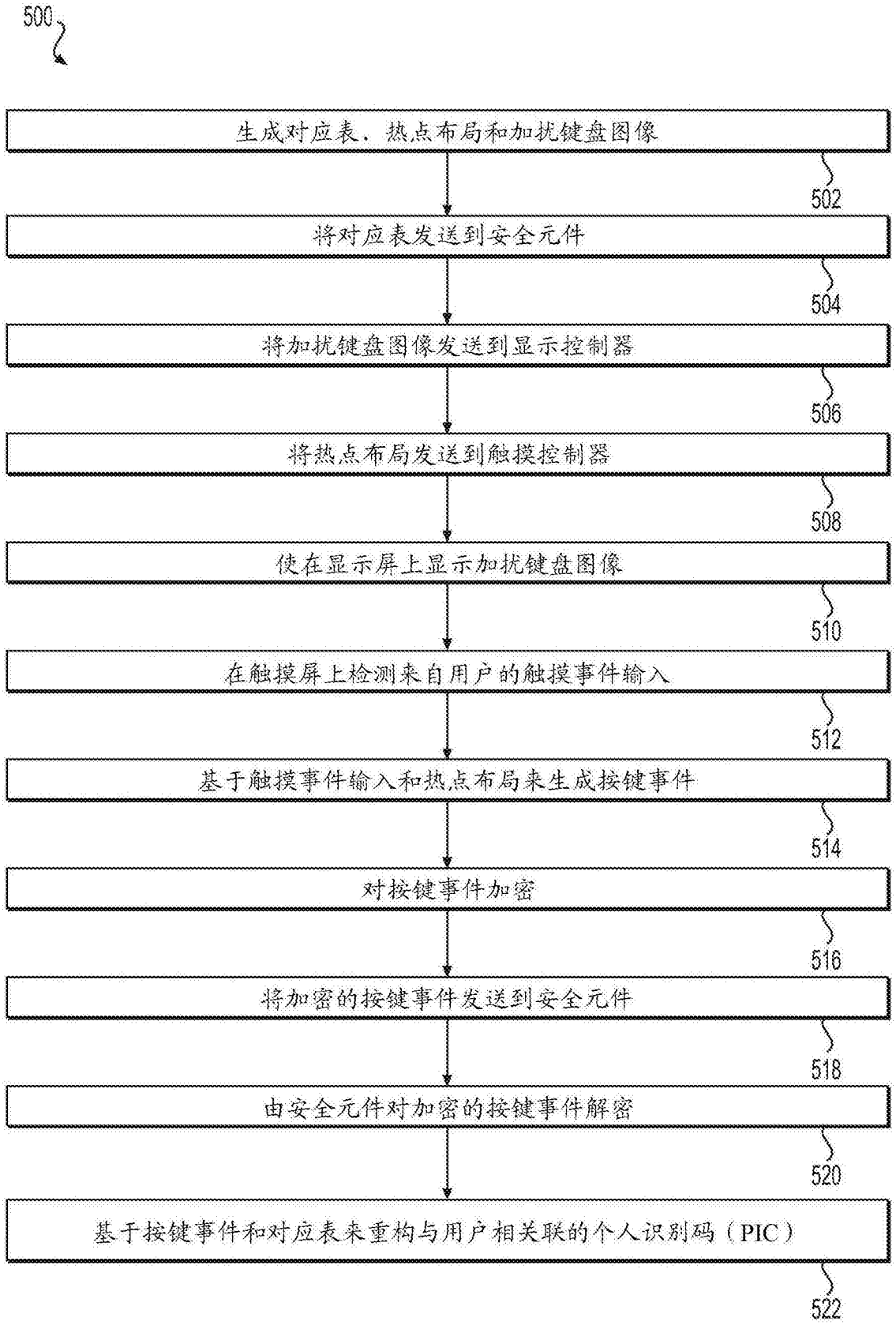

500
生成对应表、热点布局和加扰键盘图像
502
将对应表发送到安全元件
504
将加扰键盘图像发送到显示控制器
506
将热点布局发送到触摸控制器
508
使在显示屏上显示加扰键盘图像
510
在触摸屏上检测来自用户的触摸事件输入
512
基于触摸事件输入和热点布局来生成按键事件
514
对按键事件加密
516
将加密的按键事件发送到安全元件
518
由安全元件对加密的按键事件解密
520
基于按键事件和对应表来重构与用户相关联的个人识别码（PIC）
522

图5