(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2018 年 1 月 4 日 (04.01.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/001277 A1

(51) 国际专利分类号:
G06F 15/78 (2006.01) *G06Q 20/32* (2012.01)
G06F 13/40 (2006.01)

(21) 国际申请号: PCT/CN2017/090591

(22) 国际申请日: 2017 年 6 月 28 日 (28.06.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610512240.9 2016年7月1日 (01.07.2016) CN

(71) 申请人: 华 为 技 术 有 限 公 司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 潘 时 林 (PAN, Shilin); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京龙双利达知识产权代理有限公司 (LONGSUN LEAD IP LTD.); 中国北京市海淀区北清路68号院3号楼101, Beijing 100094 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,

(54) **Title:** SYSTEM-ON-CHIP AND TERMINAL

(54) **发明名称:** 一种系统级芯片和终端

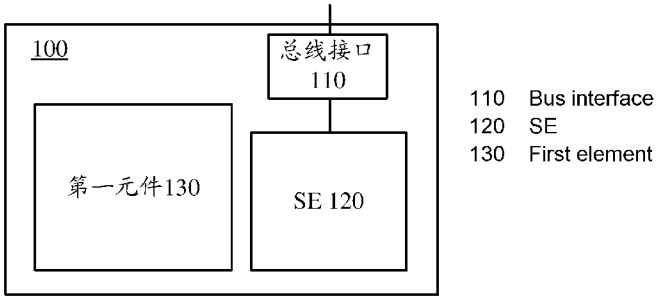

图1b

(57) Abstract: A system-on-chip (SOC) and a terminal. The SOC comprises a bus interface (110), a security element (SE) (120) and a first element (130) integrated in the SOC; the bus interface (110) is used for connecting a I/O device (710); the SE (120) is used for accessing the I/O device (710) through the bus interface (110) in a security scene to acquire first data input by the I/O device (710) and perform security processing on the first data, and used for controlling the first element (130) to access the I/O device (710) in a common scene, the security scene representing a scene requiring security inputting, and the common scene representing a scene does not require security inputting; and the first element (130) is used for acquiring second data input by the I/O device (710) in the common scene under the control of the SE (120). The SOC and the terminal can improve inputting security.

(57) 摘要: 一种系统级芯片SOC和终端。该SOC包括集成在该SOC内的总线接口(110)、安全元件SE(120)以及第一元件(130)；该总线接口(110)用于连接I/O设备(710)；该SE(120)用于在安全场景下通过该总线接口(110)访问该I/O设备(710)，获取该I/O设备(710)输入的第一数据，并对第一数据进行安全处理，以及控制该第一元件(130)在普通场景下对该I/O设备(710)的访问，其中，该安全场景表示需要安全输入的场景，该普通场景表示不需要安全输入的场景；该第一元件(130)用于通过该SE(120)的控制，在该普通场景下，获取该I/O设备(710)输入的第二数据。SOC和终端，能够提高输入的安全性。

WO 2018/001277 A1

[见续页]

LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

一种系统级芯片和终端

本申请要求于2016年7月1日提交中国专利局、申请号为201610512240.9、申请名称为“一种系统级芯片和终端”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及信息技术领域，并且更具体地，涉及一种系统级芯片（System on Chip，SOC）和终端。

背景技术

手机支付也称为移动支付（Mobile Payment），是指允许移动用户使用其移动终端（通常是手机）对所消费的商品或服务进行账务支付的一种服务方式。手机实现移动支付目前主要有三种方式，分别是通过安全数字（Secure Digital，SD）卡，通过客户识别模块（Subscriber Identity Module，SIM）卡，或通过近场通信（Near Field Communication，NFC）和嵌入式安全元件（embedded Secure Element，eSE）的全终端方案来实现。eSE也称为外置安全元件，是将安全元件（Secure Element，SE）芯片组合到手机产品板上，完成金融等应用服务。全终端方案是手机与销售点（Point of Sales，POS）机进行非接触式刷卡，NFC和SE（预置银行的应用以及数据）共同作用，完成支付交易。

当前智能机，触摸屏是唯一可以让用户便捷的输入密码或其他数据的装置，然而用户输入到触摸屏的数据并不是真正安全的输入，输入的触摸点以及屏幕的数据理论上存在被恶意应用软件截获，从而获得用户的银行密码等安全敏感数据。

对于目前的SD卡，SIM卡以及eSE的方案，SOC芯片与触摸屏通过集成电路间总线（Inter－Integrated Circuit，I2C）或者其他总线直接连接，输入的触摸屏数据和显示的位置数据都先由SOC上的应用处理器（Application Processor，AP）获知，安全性级别较低。

申请内容

本申请实施例提供了一种系统级芯片和终端，能够提高输入的安全性。

第一方面，提供了一种系统级芯片SOC，包括：集成在该SOC内的总线接口、安全元件SE以及第一元件；该总线接口，用于连接输入/输出I/O设备；该SE，用于在安全场景下，通过该总线接口访问该I/O设备，获取该I/O设备输入的第一数据，并对该第一数据进行安全处理，以及控制该第一元件在普通场景下对该I/O设备的访问，其中，该安全场景表示需要安全输入的场景，该普通场景表示不需要安全输入的场景；该第一元件，用于通过该SE的控制，在该普通场景下，获取该该I/O设备输入的第二数据。

本申请实施例的SOC中，SE可以直接访问总线接口，这样，安全场景下的输入数据直接由SE获得，不会通过第一元件，从而能够提高输入的安全性。

在一些可能的实现方式中，该SE还用于在该安全场景下，控制该I/O设备显示数据输入界面。

在一些可能的实现方式中，该SE还用于将安全处理后的数据发送给服务器。

例如，在安全支付时，SE 通过总线接口向用户显示输入密码的界面；用户在此界面输入密码；SE 通过总线接口获取用户输入的密码数据，并用 SE 中保存的 PIN 密钥对密码数据进行加密，将加密后的数据发送给金融行业的校验服务器进行校验，这样能够提高支付的安全性。

在一些可能的实现方式中，该 SE 还用于根据当前访问所述 I/O 设备的应用，确定当前的应用环境为该安全场景或该普通场景。

在一些可能的实现方式中，该 SE 用于在该普通场景下，通过该总线接口访问该 I/O 设备，获取该第二数据，并将该第二数据发送给该第一元件。

在一些可能的实现方式中，该总线接口设置于该 SE 中。

在一些可能的实现方式中，该总线接口由运行在该 SE 中的系统软件控制。

在一些可能的实现方式中，该 SE 用于在该安全场景下配置该总线接口的访问模式为仅该 SE 访问，在该普通场景下配置该总线接口的访问模式为该第一元件访问。

在一些可能的实现方式中，该 SE 可以配置该总线接口的访问模式，该第一元件不能配置总线接口的访问模式。

该总线接口的访问模式包括仅该 SE 访问和该第一元件访问。

在一些可能的实现方式中，该总线接口包括第一总线接口和第二总线接口；该 SE 用于，在该安全场景下控制该第二总线接口与该 I/O 设备连接，并通过该第二总线接口访问该 I/O 设备；在该非安全场景下控制该第一总线接口与该 I/O 设备连接，以使该第一元件通过该第一总线接口访问该 I/O 设备。

在一些可能的实现方式中，该 SOC 还包括多路开关；该 SE 用于在该安全场景下控制该多路开关切换，使得该第二总线接口与该 I/O 设备连接，在该普通场景下控制该多路开关切换，使得该第一总线接口与该 I/O 设备连接。

在一些可能的实现方式中，该多路开关设置于该 SE 中。

在一些可能的实现方式中，该第二总线接口设置于该 SE 中。

在一些可能的实现方式中，该 SE 还用于在确定进入该安全场景时，向该用户发送安全指示。

在一些可能的实现方式中，该 SE 可以根据当前需要输入的应用为该 SE 中的应用确定需要安全输入，即确定进入该安全场景。

在一些可能的实现方式中，该 SE 具体用于在确定进入该安全场景时，控制点亮安全指示灯。

在一些可能的实现方式中，该 I/O 设备包括数据采集传感器、触摸屏或显示器。

在一些可能的实现方式中，该总线接口包括集成电路间总线 I2C 接口或移动产业处理器接口 MIPI。

在一些可能的实现方式中，该第一元件包括应用处理器、可信环境 TEE 中的处理器核、数字信号处理器或专用集成电路。

本申请实施例的 SOC 能够实现 SE 级别的安全。

采用本申请实施例的 SOC 的手机或其他移动终端开放平台具有 POS 机的安全输入能力，换言之，手机或其他移动终端设备可以具有 POS 机功能。

第二方面，提供了一种终端，该终端包括第一方面或第一方面的任一种可能的实现方式中的 SOC，以及 I/O 设备。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1a 是本申请实施例的一个应用架构图。

图 1b 是本申请一个实施例的 SOC 的示意性框图。

图 2 是本申请另一实施例的 SOC 的示意性框图。

图 3 是本申请又一实施例的 SOC 的示意性结构图。

图 4 是本申请又一实施例的 SOC 的示意性结构图。

图 5 是本申请又一实施例的 SOC 的示意性框图。

图 6a 是本申请又一实施例的 SOC 的示意性结构图。

图 6b 是本申请又一实施例的 SOC 的示意性结构图。

图 7 是本申请一个实施例的终端的示意性框图。

图 8 是本申请另一实施例的终端的示意性结构图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请的一部分实施例，而不是全部实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动的前提下所获得的所有其他实施例，都应属于本申请保护的范围。

本申请实施例的 SOC 芯片可以应用于支持移动支付的终端（例如手机）中，用于提高终端的输入或输出的安全性。

为了便于理解本申请实施例的技术方案，下面首先对本申请实施例中的相关术语进行说明。

现有技术中，安全元件（Secure Element，SE）为一种防篡改的芯片，它能确保数据存储在安全的地方，且信息仅对经授权的应用程序和人员开放，它类似用户个人和设备本身的身份证。例如，在安全支付时，SE 中存储银行的应用以及数据。

移动支付产品经过多种形态的迭代，手机、可穿戴设备等产品逐步成为实现移动支付的主流应用承载对象，其易用性、安全性、可携带性、交互界面等方面相较传统方式有着较大优势。目前这些产品的金融功能都基于一个核心组件——嵌入式安全元件（embedded Secure Element，eSE）。eSE 也称为外置 SE，其大小不一，设计也可不同，并可嵌入在任意一种移动设备中。eSE 可以较为方便安全的实现在移动支付产品中对金融应用的管理和控制。

在本申请实施例中，在 SOC 芯片中内置 SE，称为集成安全元件（integrated Secure Element，inSE），也就是说，在 SOC 中集成 SE 子系统，而不是采用嵌入式 SE（eSE）。inSE 也可以表示为 In-SOC SE。

在本申请实施例中，可选地，SE 可以包括至少一个处理器，用于执行 SE 的各种操作，例如，数据访问、数据处理、控制等操作，以实现本申请实施例中 SE 的相应功能。

可选地，SE 中还可以包括：存储器，用于存储数据或指令等；通信接口，用于与其他部件之间进行通信。应理解，以上只是 SE 的一种具体实现形式，本申请对此并不限定，也就是说，SE 还可以采用其他可能的可以实现本申请实施例中 SE 的相应功能的实现形式。

在本申请实施例中，第一元件为芯片中除 SE 之外的处理元件，例如，第一元件可以为应用处理器，或者，在可信环境（Trust Execute Environment，TEE）中运行的处理器核，数字信号处理器（Digital Signal Processor，DSP），专用集成电路（Application Specific Integrated Circuit，ASIC）等。

图 1a 是本申请实施例的一个应用架构图。如图 1a 所示，在本申请实施例中，在 SOC 芯片中集成 SE，而不是采用 eSE。SOC 芯片中除 SE 之外的处理元件称为第一元件。对于 SE 和第一元件，图 1a 中以处理器和存储器示例，但本申请对此并不限定。也就是说，SE 和第一元件中可以包括更多或更少的部件或模块，即其中的部件或模块的数量和种类可以根据实际需要而设置。

本申请实施例在集成 SE 的 SOC 芯片中，将与输入/输出（input/output，I/O）设备（例如触摸传感器）对接的总线接口设置在 SE 中或由 SE 控制对其的访问，从而可以做到真正的 SE 级别的安全。

图 1b 示出了根据本申请实施例的 SOC 100 的示意性框图。如图 1b 所示，该 SOC 100 包括集成在该 SOC 100 内的总线接口 110、SE 120 和第一元件 130。

在本申请实施例中，在 SOC 100 中集成 SE 120。SE 120 中存储防篡改的数据。例如，在安全支付时，SE 中存储银行的应用以及数据，如个人身份号码（Personal Identification Number，PIN）密钥。

总线接口 110 用于连接 I/O 设备。I/O 设备为终端的输入/输出设备，例如，I/O 设备可以为数据采集传感器、触摸屏或显示器。

数据采集传感器为具有数据采集功能的传感器（sensor），包括通过体感、虹膜、脑电波等交互方式进行数据的采集的传感器，例如触控传感器。

触摸屏可以包括触控传感器和液晶显示器（Liquid Crystal Display，LCD）。

显示器可以包括 LCD、有机发光二极管（Organic Light-Emitting Diode，OLED）屏、电子墨水屏、等离子显示板（Plasma Display Panel，PDP）等。

总线接口 110 可以为 I2C 接口，移动产业处理器接口（Mobile Industry Processor Interface，MIPI）或者其他可以与 I/O 设备连接的总线接口。

应理解，上述对 I/O 设备和总线接口 110 的举例说明，只是为了帮助本领域技术人员更好地理解本申请实施例，而非限制本申请实施例的范围。以下为了描述方便，以 I/O 设备为触摸传感器，总线接口 110 为 I2C 接口为例进行说明。

SE 120 用于在安全场景下，通过总线接口 110 访问 I/O 设备，获取 I/O 设备输入的第一数据，并对第一数据进行安全处理，以及控制第一元件 130 在普通场景下对 I/O 设备的访问。

安全场景表示需要安全输入的场景，例如在安全支付时需要安全输入和显示的场景；普通场景表示不需要安全输入的场景。

可选地，SE 120 可以根据当前访问所述 I/O 设备的应用，确定当前的应用环境为安全场景或普通场景。例如，当前需要所述 I/O 设备输入数据的应用为 SE 120 中的应用，SE 120 可以确定需要安全输入，即当前的应用环境为安全场景，否则为普通场景。

在本申请实施例中，SE 120 在安全场景下通过总线接口 110 访问 I/O 设备，即 SE 120 可以在安全场景下直接对总线接口 110 进行访问，进而访问 I/O 设备，获取 I/O 设备输入的第一数据。该第一数据不会通过第一元件 130，从而能够提高安全场景下输入的安全性。

可选地，SE 120 还用于在安全场景下，控制 I/O 设备显示数据输入界面。

具体而言，在需要安全输入时，例如，SE 120 根据当前需要输入的应用为 SE 120 中的应用确定需要安全输入，SE 120 通过总线接口 110 访问 I/O 设备，先向用户输出显示界面；用户根据显示界面输入第一数据；SE 120 再通过总线接口 110 获取用户输入的第一数据。

可选地，SE 120 还用于对第一数据进行安全处理，并将安全处理后的数据发送给校验服务器。

例如，在安全支付时，SE 120 通过总线接口 110 向用户显示输入密码的界面；用户在此界面输入密码；SE 120 通过总线接口 110 获取用户输入的密码数据，并用 SE 120 中保存的 PIN 密钥对密码数据进行加密，将加密后的数据发送给金融行业的校验服务器进行校验，这样能够提高支付的安全性。

应理解，在本申请的各种实施例中，数据访问、数据处理、控制等操作可以通过 SE 中的处理器实现，数据发送可以通过 SE 中的通信接口实现，但本申请对此并不限定。

第一元件 130 用于通过 SE 120 的控制，在普通场景下，获取 I/O 设备输入的第二数据。

在普通场景下，即不需要安全输入的场景，第一元件 130 可以在 SE 120 的控制下，获取 I/O 设备输入的第二数据。

在本申请实施例中，SE 120 与总线接口 110 的位置以及连接关系可以有多种方式，相应地，SE 120 的控制方式也可以有多种，以下分别进行说明。

可选地，在本申请一个实施例中，SE 120 在普通场景下，通过总线接口 110 访问 I/O 设备，获取该第二数据，并将该第二数据发送给第一元件 130。

在本实施例中，SE 120 可以直接访问总线接口 110，而第一元件 130 不能直接访问总线接口 110。例如，如图 2 所示，总线接口 110 设置于 SE 120 中。由于 SOC 100 内集成 SE 120，SE 120 的性能和延迟响应可以做到较好。直接将总线接口 110 放到集成的 SE 120 中，由 SE 120（例如，运行在 SE 120 中的系统软件）控制。在这种情况下，对于普通场景，即不需要安全输入的场景，第一元件 130 对总线接口 110 的访问通过 SE 120 转发。对于安全场景，即需要安全输入的场景，SE 120 不再转发数据，即仅 SE 120 能够通过总线接口 110 获取用户输入的数据，从而提高输入的安全性。

可选地，SE 120 还可以在确定进入安全场景时，向用户发送安全指示。例如，控制点亮安全指示灯，通过点亮安全指示灯通知用户进入安全场景。

例如，SE 120 根据当前需要输入的应用为 SE 120 中的应用确定需要安全输入，即确定进入安全场景。

图 3 为本申请实施例的 SOC 的一个示例。如图 3 所示，I2C 接口 310 设置于 SE 320 中。SE 320 对应于前述 SE 120，SE 320 中具体可以包括处理器 321，用于执行 SE 320 的各种操作，存储器 322，通用输入/输出（General Purpose Input Output，GPIO）323 等，GPIO 323 连接安全指示灯 340。应理解，SE 320 中还可以包括其他模块，并且 SE 320 中模块的数量和种类可以根据实际需要而设置，本申请对此并不限定。AP 330 对应于前

述第一元件 130，AP 330 中具体可以包括处理器 331，存储器 332 等。应理解，AP 330 中还可以包括其他模块，并且 AP 330 中模块的数量和种类可以根据实际需要而设置，本申请对此也不限定。

I2C 接口 310 连接触摸传感器 350，MIPI 360 连接 LCD 370。

当不是安全输入的场景时，触摸传感器 350 的消息和数据由 SE 320 的芯片操作系统（Chip Operation System，COS）转发（例如通过邮箱通信）给主 AP 330；当 COS 系统软件判断需要进行安全输入时，点亮安全指示灯 340（或其他可以通知用户的安全指示，本申请不限定为安全指示灯），并不再将触摸传感器 350 的消息和数据转发给主 AP 330，直到用户输入完成，用户点击确认（OK），灭掉安全指示灯 340 后，方可继续转发给 AP 330。

在图 3 中，I2C 接口 310 设置于 SE 320 中，MIPI 360 不在 SE 320 中。应理解，对接 LCD 370 的 MIPI 360 也可以放入 SE 320 中，换句话说，I2C 接口 310 和 MIPI 360 可以都设置于 SE 320 中，本申请对此并不限定。

可选地，在本申请另一个实施例中，SE 120 在安全场景下配置总线接口 110 的访问模式为仅 SE 120 访问，在普通场景下配置总线接口 110 的访问模式为第一元件 130 访问。

在本实施例中，SE 120 可以配置总线接口 110 的访问模式，而第一元件 130 不能配置总线接口 110 的访问模式。在安全场景下 SE 120 配置总线接口 110 的访问模式为仅 SE 120 访问，在此场景下，仅 SE 120 访问总线接口 110，第一元件 130 不能访问总线接口 110；当退出安全场景时，SE 120 配置总线接口 110 的访问模式为第一元件 130 访问，在此场景下，第一元件 130 可以访问总线接口 110。

可选地，SE 120 还可以在确定进入安全场景时，向用户发送安全指示。例如，控制点亮安全指示灯，通过点亮安全指示灯通知用户进入安全场景。

例如，图 4 为本申请实施例的芯片的另一个示例。在图 4 中，SE 420 配置 I2C 接口 410 的访问模式。SE 420 对应于前述 SE 120，SE 420 中具体可以包括处理器 421，用于执行 SE 420 的各种操作，存储器 422，GPIO 423 等，GPIO 423 连接安全指示灯 440。应理解，SE 420 中还可以包括其他模块，并且 SE 420 中模块的数量和种类可以根据实际需要而设置，本申请对此并不限定。AP 430 对应于前述第一元件 130，AP 430 中具体可以包括处理器 431，存储器 432 等。应理解，AP 430 中还可以包括其他模块，并且 AP 430 中模块的数量和种类可以根据实际需要而设置，本申请对此也不限定。

I2C 接口 410 连接触摸传感器 450，MIPI 460 连接 LCD 470。

安全场景下，SE 420 将对接触摸传感器 450 的 I2C 接口 410 配置为仅 SE 访问（SE Access Only），即仅 SE 420 的处理器 421 能够访问，其他任何处理器，例如处理器 431，都不能访问；当退出安全场景时，只有 SE 420 能够配置将 I2C 接口 410 退出 SE Access Only 模式，退出后，第一元件的处理器，例如，处理器 431，可以访问 I2C 接口 410。

在图 4 中，SE 420 配置 I2C 接口 410 的访问模式，SE 420 不配置 MIPI 460 的访问模式。应理解，SE 420 也可以配置 MIPI 460 的访问模式。换句话说，I2C 接口 410 和 MIPI 460 都可以由 SE 420 控制访问模式，本申请对此并不限定。

可选地，在本申请另一个实施例中，如图 5 所示，总线接口 110 可以包括第一总线接口 111 和第二总线接口 112。

SE 120 访问第二总线接口 112。可选地，第二总线接口 112 可设置于 SE 120 中。

第一元件 130 访问第一总线接口 111。

在这种情况下，SE 120 在安全场景下控制第二总线接口 112 与 I/O 设备连接，并通过第二总线接口 112 访问 I/O 设备；在普通场景下控制第一总线接口 111 与 I/O 设备连接，以使第一元件 130 通过第一总线接口 111 访问 I/O 设备。

在本实施例中，对对接 I/O 设备的管脚进行内部复用，即可切换第一总线接口 111 和第二总线接口 112 分别与 I/O 设备连接，其中切换由 SE 120 控制。具体地，SE 120 在安全场景下控制第二总线接口 112 与 I/O 设备连接，这样，SE 120 通过第二总线接口 112 访问 I/O 设备；SE 120 在普通场景下控制第一总线接口 111 与 I/O 设备连接，这样，第一元件 130 通过第一总线接口 111 访问 I/O 设备。

可选地，切换可以通过多路开关 140 实现。具体地，SE 120 在安全场景下控制多路开关 140 切换，使得第二总线接口 112 与 I/O 设备连接，这样，SE 120 通过第二总线接口 112 访问 I/O 设备；SE 120 在普通场景下控制多路开关 140 切换，使得第一总线接口 111 与 I/O 设备连接，这样，第一元件 130 通过第一总线接口 111 访问 I/O 设备。

可选地，多路开关 140 可设置于 SE 120 中。

可选地，SE 120 还可以在确定进入安全场景时，向用户发送安全指示。例如，控制点亮安全指示灯，通过点亮安全指示灯通知用户进入安全场景。

例如，图 6a 为本申请实施例的芯片的另一个示例。在图 6a 中，SE 620 控制多路开关 680 以切换 I2C 接口 611 和 I2C 接口 612 分别与触摸传感器 650 连接。SE 620 对应于前述 SE 120，SE 620 中具体可以包括处理器 621，用于执行 SE 620 的各种操作，存储器 622，GPIO 623 等，GPIO 623 连接安全指示灯 640。可选地，SE 620 还可以通过 GPIO 623 控制多路开关 680。SE 620 也可以通过其他方式控制多路开关 680，例如通过设置的寄存器逻辑控制多路开关 680。应理解，SE 620 中还可以包括其他模块，并且 SE 620 中模块的数量和种类可以根据实际需要而设置，本申请对此并不限定。AP 630 对应于前述第一元件 130，AP 630 中具体可以包括处理器 631，存储器 632 等。应理解，AP 630 中还可以包括其他模块，并且 AP 630 中模块的数量和种类可以根据实际需要而设置，本申请对此也不限定。

MIPI 660 连接 LCD 670。

当不是安全输入的场景时，SE 620 控制多路开关 680 切换为 I2C 接口 611 与触摸传感器 650 连接，用户输入的数据直接送给 I2C 接口 611，以便于 AP 630 访问；当 COS 系统软件判断需要进行安全输入时，点亮安全指示灯 640（或其他可以通知用户的安全指示，本申请不限定为安全指示灯），并控制多路开关 680 切换为 I2C 接口 612 与触摸传感器 650 连接，I2C 接口 611 不再能获得触摸传感器 650 的数据，直到用户输入完成，用户点击 OK，灭掉安全指示灯 640 后，方可控制多路开关 680 切换为 I2C 接口 611 与触摸传感器 650 连接以继续工作。

应理解，MIPI 660 也可以采用双接口设计，并由 SE 620 控制切换，本申请对此并不限定。

图 6b 为本申请实施例的芯片的另一个示例。在图 6b 中，多路开关 680 设置于 SE 620 中，由 SE 620 直接控制。图 6b 中芯片的具体工作过程与图 6a 类似，在此不再赘述。

本申请实施例的 SOC 芯片中，SE 可以直接访问总线接口，这样，安全场景下的输入数据直接由 SE 获得，不会通过第一元件，因此不会被恶意应用软件截获，从而能够提

高输入的安全性。

因此，本申请实施例的SOC能够实现SE级别的安全。采用本申请实施例的SOC的手机或其他移动终端开放平台具有POS机的安全输入能力，换言之，手机或其他移动终端设备可以具有POS机功能。

图7示出了根据本申请实施例的终端700的示意性框图。如图7所示，该终端700可以包括前述本申请实施例的SOC 100，以及I/O设备710，其中I/O设备710可以为前述本申请实施例中描述的I/O设备。

终端700可以支持移动支付，采用本申请实施例的SOC，能够实现SE级别的安全，具有POS机的安全输入能力，即可以作为POS机。

本领域技术人员可以理解，终端700还可以包括图7中未示出的其他部件，例如，终端700作为手机时还可以包括射频（Radio Frequency，RF）电路等部件，本申请对此并不限定。

例如，图8示出了根据本申请实施例的终端800的示意性结构图。如图8所示，终端800可以包括处理器810、I/O设备820、收发器830和天线840。处理器810可以为前述本申请实施例的SOC，为了简洁，在此不再赘述。I/O设备820可以为前述本申请实施例中描述的I/O设备。收发器830通过天线840实现与其他设备的通信。本领域技术人员可以理解，图8中示出的终端结构并不构成对终端的限定，终端可以包括比图示更多或更少的部件，或者组合某些部件，或者拆分某些部件，或者不同的部件布置。

应理解，以上描述中的具体的例子只是为了帮助本领域技术人员更好地理解本申请实施例，而非限制本申请实施例的范围。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

在本申请所提供的几个实施例中，应该理解到，所揭露的装置，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口、装置或单元的间接耦合或通信连接，也可以是电的，机械的或其它的形式连接。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本申请实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以是两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，

可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分，或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括: U 盘、移动硬盘、只读存储器（Read-Only Memory，ROM）、随机存取存储器（Random Access Memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

权利要求

1. 一种系统级芯片 SOC，其特征在于，包括集成在所述 SOC 内的总线接口、安全元件 SE 以及第一元件；

所述总线接口，用于连接输入/输出 I/O 设备；

所述 SE，用于在安全场景下，通过所述总线接口访问所述 I/O 设备，获取所述 I/O 设备输入的第一数据，并对所述第一数据进行安全处理，以及控制所述第一元件在普通场景下对所述 I/O 设备的访问，其中，所述安全场景表示需要安全输入的场景，所述普通场景表示不需要安全输入的场景；

所述第一元件，用于通过所述 SE 的控制，在所述普通场景下，获取所述 I/O 设备输入的第二数据。

2. 根据权利要求 1 所述的 SOC，其特征在于，所述 SE 还用于在所述安全场景下，控制所述 I/O 设备显示数据输入界面。

3. 根据权利要求 1 或 2 所述的 SOC，其特征在于，所述 SE 还用于将安全处理后的数据发送给服务器。

4. 根据权利要求 1 至 3 中任一项所述的 SOC，其特征在于，所述 SE 还用于根据当前访问所述 I/O 设备的应用，确定当前的应用环境为所述安全场景或所述普通场景。

5. 根据权利要求 1 至 4 中任一项所述的 SOC，其特征在于，所述 SE 用于在所述普通场景下，通过所述总线接口访问所述 I/O 设备，获取所述第二数据，并将所述第二数据发送给所述第一元件。

6. 根据权利要求 5 所述的 SOC，其特征在于，所述总线接口设置于所述 SE 中。

7. 根据权利要求 1 至 4 中任一项所述的 SOC，其特征在于，所述 SE 用于在所述安全场景下配置所述总线接口的访问模式为仅所述 SE 访问，在所述普通场景下配置所述总线接口的访问模式为所述第一元件访问。

8. 根据权利要求 1 至 4 中任一项所述的 SOC，其特征在于，所述总线接口包括第一总线接口和第二总线接口；

所述 SE 用于，在所述安全场景下控制所述第二总线接口与所述 I/O 设备连接，并通过所述第二总线接口访问所述 I/O 设备；

在所述非安全场景下控制所述第一总线接口与所述 I/O 设备连接，以使所述第一元件通过所述第一总线接口访问所述 I/O 设备。

9. 根据权利要求 8 所述的 SOC，其特征在于，所述 SOC 还包括多路开关；

所述 SE 用于在所述安全场景下控制所述多路开关切换，使得所述第二总线接口与所述 I/O 设备连接，在所述普通场景下控制所述多路开关切换，使得所述第一总线接口与所述 I/O 设备连接。

10. 根据权利要求 9 所述的 SOC，其特征在于，所述多路开关设置于所述 SE 中。

11. 根据权利要求 8 至 10 中任一项所述的 SOC，其特征在于，所述第二总线接口设置于所述 SE 中。

12. 根据权利要求 1 至 11 中任一项所述的 SOC，其特征在于，所述 SE 还用于在确定进入所述安全场景时，向所述用户发送安全指示。

13. 根据权利要求 1 至 12 中任一项所述的 SOC，其特征在于，所述 I/O 设备包括数据采集传感器、触摸屏或显示器。

14. 根据权利要求 1 至 13 中任一项所述的 SOC，其特征在于，所述总线接口包括集成电路间总线 I2C 接口或移动产业处理器接口 MIPI。

15. 根据权利要求 1 至 14 中任一项所述的 SOC，其特征在于，所述第一元件包括应用处理器、可信环境 TEE 中的处理器核、数字信号处理器或专用集成电路。

16. 一种终端，其特征在于，包括根据权利要求 1 至 15 中任一项所述的系统级芯片 SOC，以及输入/输出 I/O 设备。

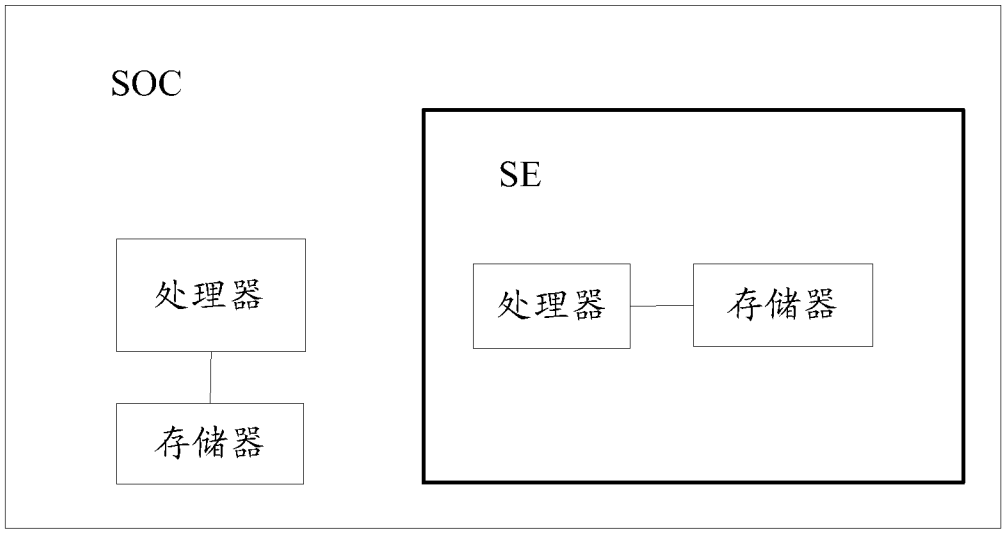

图1a

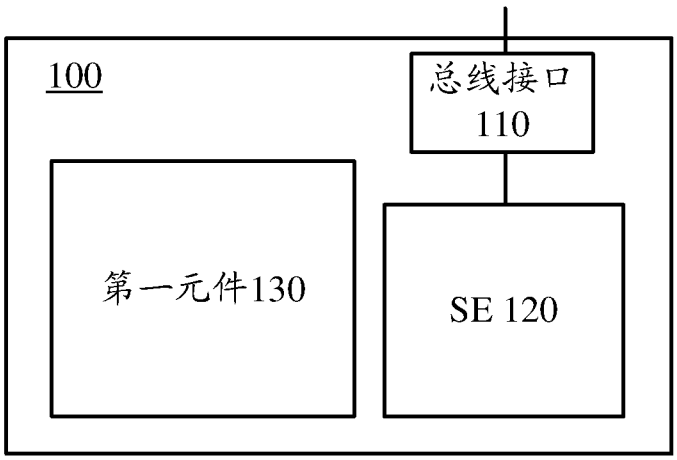

图1b

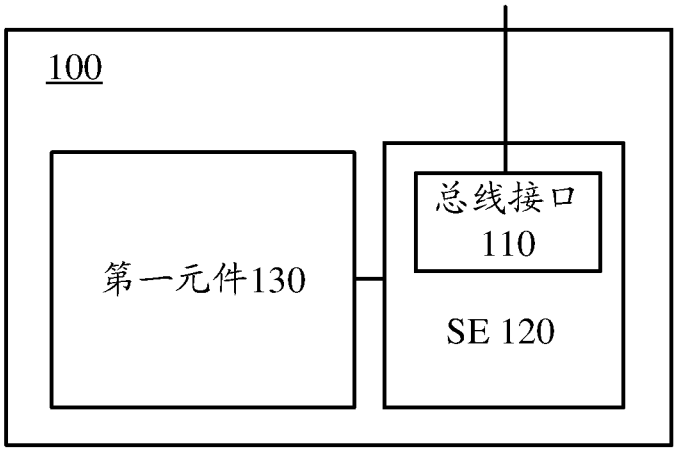
100
第一元件130
总线接口
110
SE 120

图2

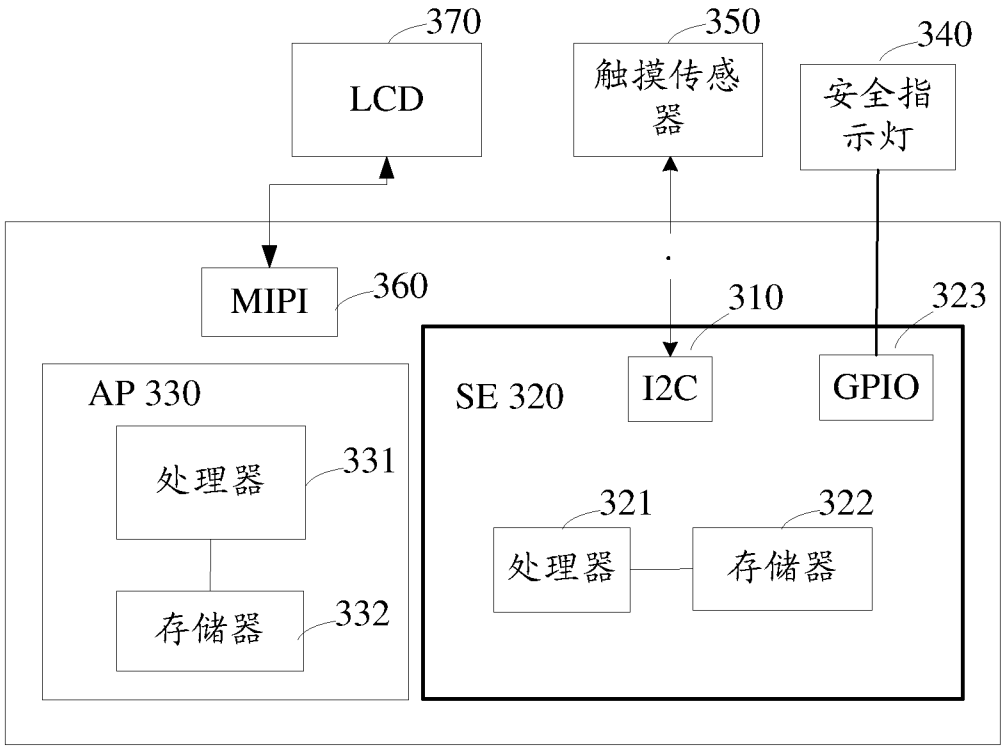
370
LCD
350
触摸传感器
340
安全指示灯
MIPI
360
310
323
AP 330
处理器
331
存储器
332
SE 320
I2C
GPIO
321
处理器
322
存储器

图3

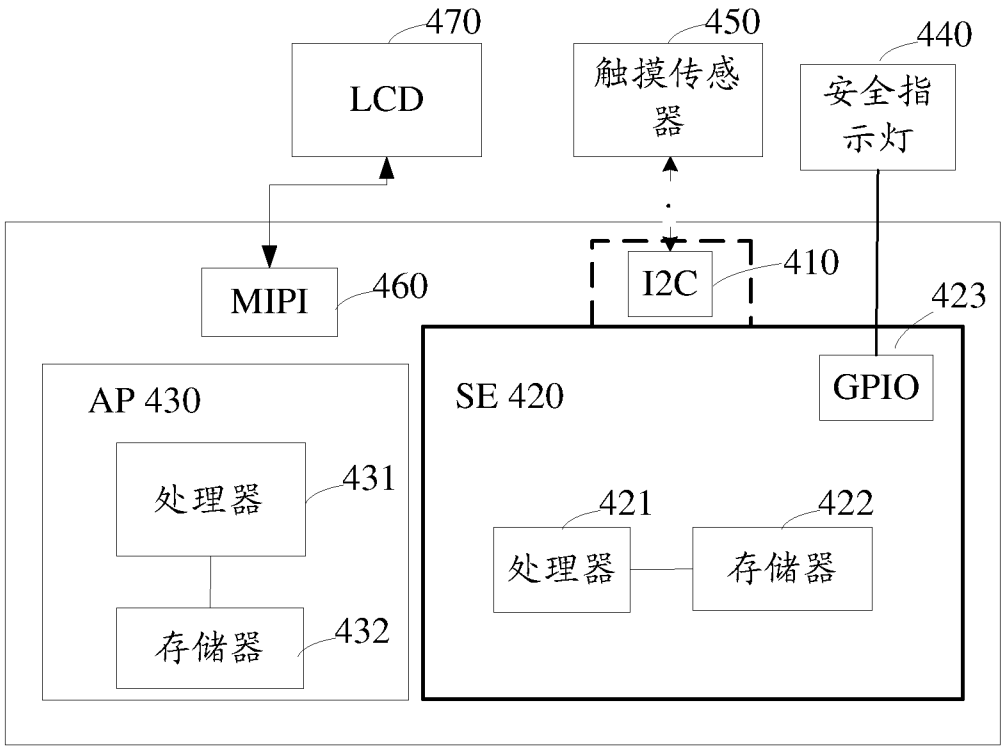
470
LCD
450
触摸传感器
440
安全指示灯
MIPI
460
I2C
410
423
AP 430
处理器
431
存储器
432
SE 420
GPIO
421
处理器
422
存储器

图4

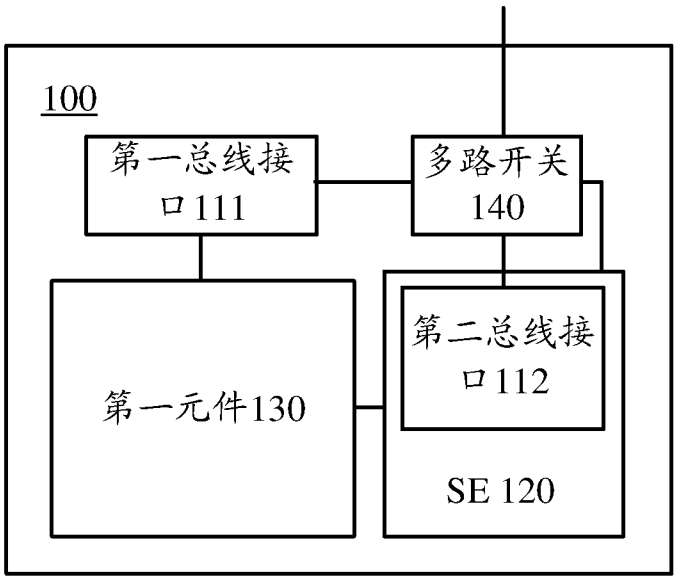
100
第一总线接口111
多路开关140
第一元件130
第二总线接口112
SE 120

图5

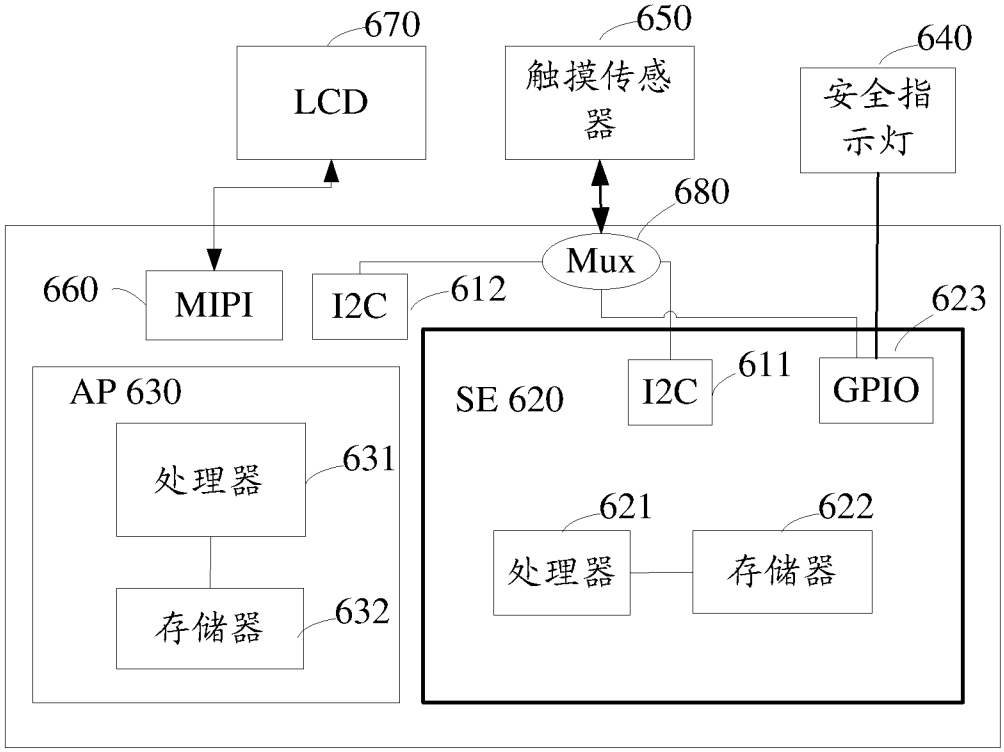
670
LCD
650
触摸传感器
640
安全指示灯
680
Mux
660
MIPI
I2C
612
623
AP 630
处理器
631
存储器
632
SE 620
I2C
611
GPIO
621
处理器
622
存储器

图6a

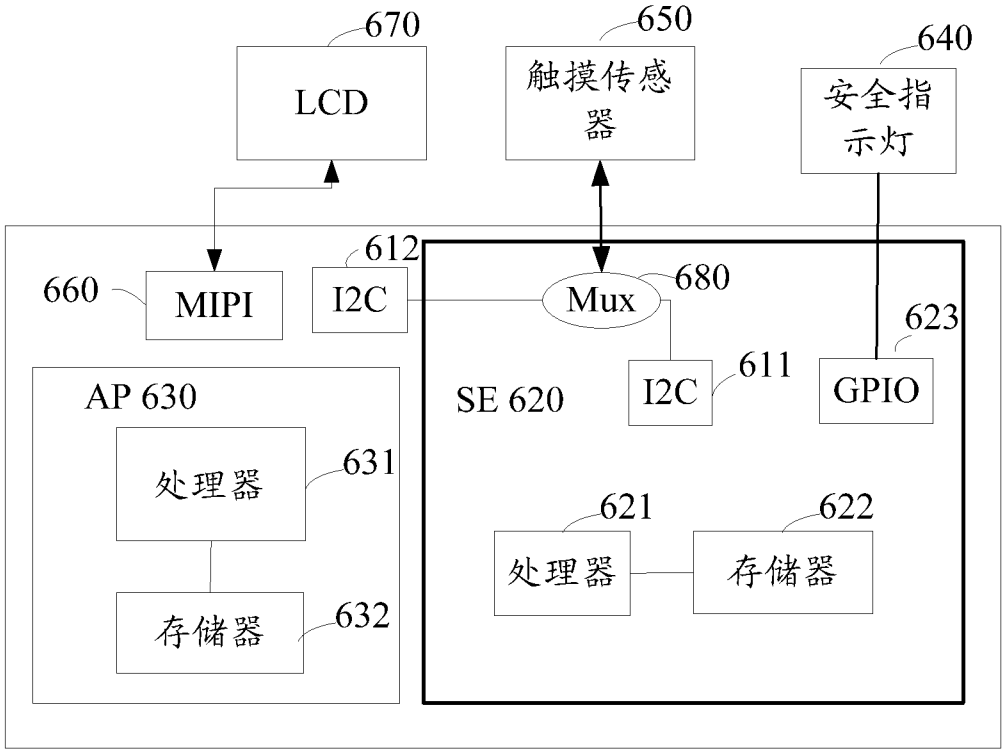
670
LCD
650
触摸传感器
640
安全指示灯
612
660
MIPI
I2C
680
Mux
623
AP 630
处理器
631
存储器
632
SE 620
I2C
611
GPIO
621
处理器
622
存储器

图6b

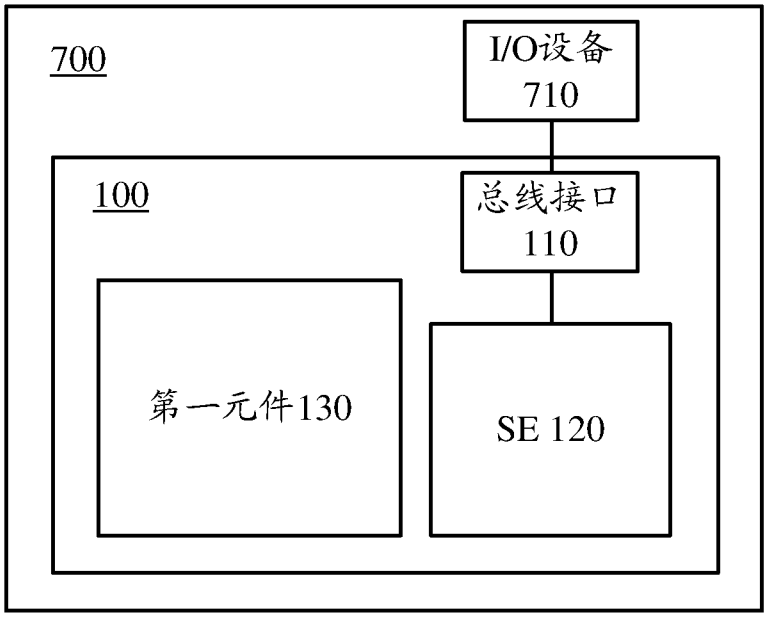
700
I/O设备
710
100
总线接口
110
第一元件130
SE 120

图7

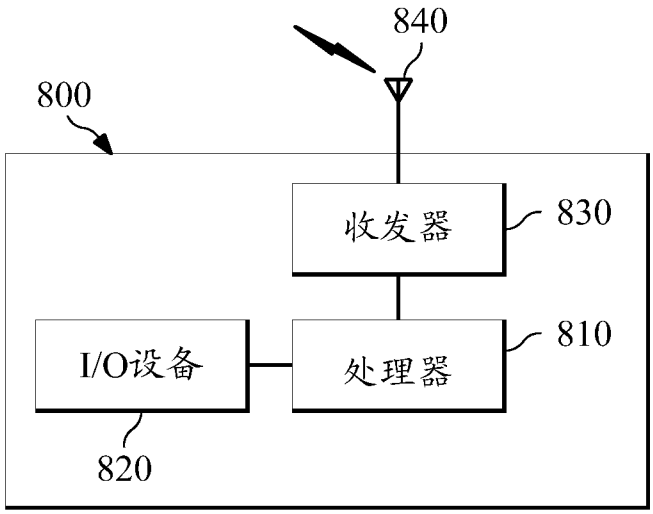
840
800
收发器
830
I/O设备
处理器
810
820

图8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/090591

A. CLASSIFICATION OF SUBJECT MATTER

G06F 15/78 (2006.01) i; G06F 13/40 (2006.01) i; G06Q 20/32 (2012.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F; G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, EPODOC, WPI, IEEE: bus interface, SOC, system on chip, bus, I2C, secure element, SE, pay+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104778401 A (NXP B.V.), 15 July 2015 (15.07.2015), description, paragraphs 0066-0074, and figures 2-3	1-16
A	CN 104471586 A (QUALCOMM INC.), 25 March 2015 (25.03.2015), the whole document	1-16
A	CN 201917963 U (BEIJING TONGFANG MICROELECTRONICS CO., LTD.), 03 August 2011 (03.08.2011), the whole document	1-16
A	US 2016078223 A1 (BROADCOM CORP.), 17 March 2016 (17.03.2016), the whole document	1-16
A	US 2015186879 A1 (ORTIZ, E.U. et al.), 02 July 2015 (02.07.2015), the whole document	1-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 September 2017 (18.09.2017)	**11 October 2017 (11.10.2017)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **LIU, Tianfei** Telephone No.: (86-10) **62414060**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/090591

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104778401 A	15 July 2015	US 2015199509 A1	16 July 2015
		EP 2894588 A1	15 July 2015
CN 104471586 A	25 March 2015	KR 20150036423 A	07 April 2015
		EP 2873025 A1	20 May 2015
		US 2014020114 A1	16 January 2014
		WO 2014011687 A1	16 January 2014
		JP 2015522199 A	03 August 2015
		BR 112015000809 A2	27 June 2017
		IN 201408760 P4	01 July 2016
CN 201917963 U	03 August 2011	None	
US 2016078223 A1	17 March 2016	US 2014156872 A1	05 June 2014
		US 9224013 B2	29 December 2015
US 2015186879 A1	02 July 2015	CA 2830260 A1	17 April 2014
		US 9082119 B2	14 July 2015
		US 2014108263 A1	17 April 2014
		US 2015235212 A1	20 August 2015
		US 2014279552 A1	18 September 2014
		US 2017161735 A1	08 June 2017
		US 2016019536 A1	21 January 2016

国际检索报告

国际申请号

PCT/CN2017/090591

A. 主题的分类

G06F 15/78(2006.01)i; G06F 13/40(2006.01)i; G06Q 20/32(2012.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F; G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT,CNKI,EPODOC,WPI,IEEE:系统级芯片，总线接口，安全元件，支付，SOC，system on chip，bus，I2C，secure element，SE，pay+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 104778401 A (恩智浦有限公司) 2015年 7月 15日 (2015-07-15) 说明书第0066-0074段、附图2-3	1-16
A	CN 104471586 A (高通股份有限公司) 2015年 3月 25日 (2015-03-25) 全文	1-16
A	CN 201917963 U (北京同方微电子有限公司) 2011年 8月 3日 (2011-08-03) 全文	1-16
A	US 2016078223 A1 (BROADCOM CORP.) 2016年 3月 17日 (2016-03-17) 全文	1-16
A	US 2015186879 A1 (ORTIZ, EDISON U. 等) 2015年 7月 2日 (2015-07-02) 全文	1-16

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 9月 18日	2017年 10月 11日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 刘天飞 电话号码 (86-10)62414060

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/090591

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	104778401	A	2015年 7月 15日	US	2015199509	A1	2015年 7月 16日
				EP	2894588	A1	2015年 7月 15日
CN	104471586	A	2015年 3月 25日	KR	20150036423	A	2015年 4月 7日
				EP	2873025	A1	2015年 5月 20日
				US	2014020114	A1	2014年 1月 16日
				WO	2014011687	A1	2014年 1月 16日
				JP	2015522199	A	2015年 8月 3日
				BR	112015000809	A2	2017年 6月 27日
				IN	201408760	P4	2016年 7月 1日
CN	201917963	U	2011年 8月 3日		无		
US	2016078223	A1	2016年 3月 17日	US	2014156872	A1	2014年 6月 5日
				US	9224013	B2	2015年 12月 29日
US	2015186879	A1	2015年 7月 2日	CA	2830260	A1	2014年 4月 17日
				US	9082119	B2	2015年 7月 14日
				US	2014108263	A1	2014年 4月 17日
				US	2015235212	A1	2015年 8月 20日
				US	2014279552	A1	2014年 9月 18日
				US	2017161735	A1	2017年 6月 8日
				US	2016019536	A1	2016年 1月 21日