(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 110602689 A
(43)申请公布日 2019.12.20

(21)申请号 201910696909.8

(22)申请日 2019.07.30

(71)申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 夏雪峰

(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
代理人 申健

(51)Int.Cl.
H04W 12/00(2009.01)
H04W 12/02(2009.01)
H04W 12/06(2009.01)
H04L 29/06(2006.01)

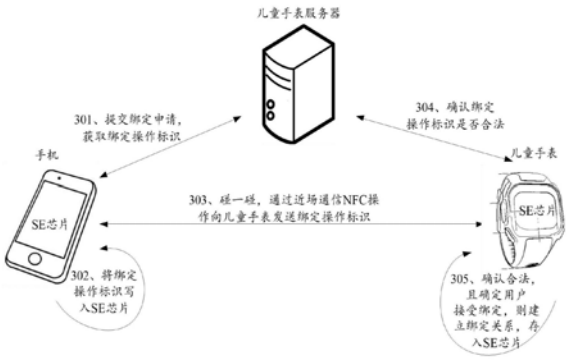
权利要求书3页 说明书19页 附图7页

(54)发明名称

一种设备安全操作的方法和装置

(57)摘要

本申请实施例提供一种设备安全操作的方法和装置，涉及终端技术领域，解决了现有技术中账号绑定操作繁琐，且账号信息安全性不够高，存在泄露用户隐私、威胁用户安全的问题。具体方案包括：第一终端设备通过近场通信NFC操作接收第二终端设备发送的绑定操作标识，该绑定操作标识包括第二终端设备向服务器发送的绑定请求所对应的标识；第一终端设备确认该绑定操作标识是否合法；若该绑定操作标识合法，且第一终端设备确定接受第二终端设备的绑定，则第一终端设备建立第一终端设备与第二终端设备的绑定关系。



CN 110602689 A

1.一种设备安全操作的方法,其特征在于,所述方法包括:

第一终端设备通过近场通信NFC操作接收第二终端设备发送的绑定操作标识,所述绑定操作标识包括所述第二终端设备向服务器发送的绑定请求所对应的标识;

所述第一终端设备确认所述绑定操作标识是否合法;

若所述绑定操作标识合法,且所述第一终端设备确定接受所述第二终端设备的绑定,则所述第一终端设备建立所述第一终端设备与所述第二终端设备的绑定关系。

2.根据权利要求1所述的方法,其特征在于,所述第一终端设备与所述第二终端设备的绑定关系包括:

所述第一终端设备的用户身份证明UID与所述第二终端设备的UID之间的映射关系。

3.根据权利要求2所述的方法,其特征在于,所述方法还包括:

所述第一终端设备接收所述服务器发送的第一秘钥的公钥,和所述第二终端设备的UID、账号绑定时间信息;

所述第一终端设备将所述映射关系、所述第一秘钥的公钥、以及所述账号绑定时间信息存储在所述第一终端设备的嵌入式安全单元SE中或者可信执行环境TEE中;

所述第一终端设备控制所述SE或所述TEE生成第二秘钥,并将所述第二秘钥的公钥发送给所述服务器。

4.根据权利要求3所述的方法,其特征在于,所述方法还包括:

所述第一终端设备接收所述第二终端设备的用户请求信息,其中,所述用户请求信息是所述第二终端设备使用所述第二秘钥的公钥加密处理的;

所述第一终端设备控制所述SE或所述TEE根据所述第二秘钥的私钥对所述用户请求信息进行解密处理,得到所述第二终端设备是否通过认证的确认结果;

所述第一终端设备控制所述SE或所述TEE根据所述第一秘钥的公钥对所述确认结果进行加密处理后发送给所述服务器;

所述第一终端设备接收所述服务器发送的所述确认结果,所述确认结果是所述服务器通过所述第一秘钥的私钥解密得到的;

若所述确认结果指示所述第二终端设备认证通过,则根据所述用户请求信息将所述第一终端设备对应的用户信息发送给所述第二终端设备。

5.根据权利要求3或4所述的方法,其特征在于,所述方法还包括:

所述第一终端设备接收所述第二终端设备的解除绑定请求信息,其中,所述解除绑定请求信息是所述第二终端设备使用所述第二秘钥的公钥加密处理的;

所述第一终端设备控制所述SE或所述TEE根据所述第二秘钥的私钥对所述解除绑定信息进行解密处理,得到所述第二终端设备是否通过认证的确认结果;

所述第一终端设备控制所述SE或所述TEE根据所述第一秘钥的公钥对所述确认结果进行加密处理后发送给所述服务器;

所述第一终端设备接收所述服务器发送的所述确认结果,所述确认结果是所述服务器通过所述第一秘钥的私钥解密得到的;

若所述确认结果指示所述第二终端设备认证通过,则所述第一终端设备控制所述SE或所述TEE删除所述第一终端设备与所述第二终端设备的绑定关系。

6.一种设备安全操作的方法,其特征在于,所述方法包括:

通信装置存储第一终端设备与第二终端设备之间的绑定关系；

所述通信装置接收服务器发送的第一秘钥的公钥；

所述通信装置生成第二秘钥，将所述第二秘钥的公钥发送给所述服务器。

7.根据权利要求6所述的方法，其特征在于，所述第一终端设备与所述第二终端设备的绑定关系包括：

所述第一终端设备的用户身份证明UID与所述第二终端设备的UID之间的映射关系。

8.根据权利要求7所述的方法，其特征在于，所述方法还包括：

所述通信装置接收所述第二终端设备通过所述第一终端设备发送的用户请求信息，其中，所述用户请求信息是所述第二终端设备使用所述第二秘钥的公钥加密处理的；

所述通信装置根据所述第二秘钥的私钥对所述用户请求信息进行解密处理，得到所述第二终端设备是否通过认证的确认结果；

所述通信装置根据所述第一秘钥的公钥对所述确认结果进行加密处理后发送给所述服务器。

9.根据权利要求7或8所述的方法，其特征在于，所述方法还包括：

所述通信装置接收所述第二终端设备通过所述第一终端设备发送的解除绑定请求信息，其中，所述解除绑定请求信息是所述第二终端设备使用所述第二秘钥的公钥加密处理的；

所述通信装置根据所述第二秘钥的私钥对所述解除绑定请求信息进行解密处理，得到所述第二终端设备是否通过认证的确认结果；

所述通信装置根据所述第一秘钥的公钥对所述确认结果进行加密处理后发送给所述服务器。

10.一种终端设备，其特征在于，所述终端设备为第一终端设备，所述第一终端设备包括处理器，以及与处理器连接的存储器，所述存储器用于存储指令，当所述指令被所述处理器执行时，使得所述第一终端设备用于执行：

通过近场通信NFC操作接收第二终端设备发送的绑定操作标识，所述绑定操作标识包括所述第二终端设备向服务器发送的绑定请求所对应的标识；

确认所述绑定操作标识是否合法；

若所述绑定操作标识合法，且确定接受所述第二终端设备的绑定，则建立所述第一终端设备与所述第二终端设备的绑定关系。

11.根据权利要求10所述的终端设备，其特征在于，所述第一终端设备与所述第二终端设备的绑定关系包括：

所述第一终端设备的用户身份证明UID与所述第二终端设备的UID之间的映射关系。

12.根据权利要求11所述的终端设备，其特征在于，所述第一终端设备还用于执行：

接收所述服务器发送的第一秘钥的公钥，和所述第二终端设备的UID、账号绑定时间信息；

将所述映射关系、所述第一秘钥的公钥、以及所述账号绑定时间信息存储在嵌入式安全单元SE中或者可信执行环境TEE中；

控制所述SE或所述TEE生成第二秘钥，并将所述第二秘钥的公钥发送给所述服务器。

13.根据权利要求12所述的终端设备，其特征在于，所述第一终端设备还用于执行：

接收所述第二终端设备的用户请求信息，其中，所述用户请求信息是所述第二终端设备使用所述第二秘钥的公钥加密处理的；

控制所述SE或所述TEE根据所述第二秘钥的私钥对所述用户请求信息进行解密处理，得到所述第二终端设备是否通过认证的确认结果；

控制所述SE或所述TEE根据所述第一秘钥的公钥对所述确认结果进行加密处理后发送给所述服务器；

接收所述服务器发送的所述确认结果，所述确认结果是所述服务器通过所述第一秘钥的私钥解密得到的；

若所述确认结果指示所述第二终端设备认证通过，则根据所述用户请求信息将所述第一终端设备对应的用户位置信息发送给所述第二终端设备。

14.根据权利要求12或13所述的终端设备，其特征在于，所述第一终端设备还用于执行：

接收所述第二终端设备的解除绑定请求信息，其中，所述解除绑定请求信息是所述第二终端设备使用所述第二秘钥的公钥加密处理的；

控制所述SE或所述TEE根据所述第二秘钥的私钥对所述解除绑定信息进行解密处理，得到所述第二终端设备是否通过认证的确认结果；

控制所述SE或所述TEE根据所述第一秘钥的公钥对所述确认结果进行加密处理后发送给所述服务器；

接收所述服务器发送的所述确认结果，所述确认结果是所述服务器通过所述第一秘钥的私钥解密得到的；

若所述确认结果指示所述第二终端设备认证通过，则控制所述SE或所述TEE删除所述第一终端设备与所述第二终端设备的绑定关系。

15.一种通信装置，应用于终端设备，其特征在于，所述通信装置用于执行如权利要求6-9任一项所述的设备安全操作的方法。

16.一种芯片系统，其特征在于，所述芯片系统应用于终端设备；所述芯片系统包括一个或多个接口电路和一个或多个处理器；所述接口电路和所述处理器通过线路互联；所述接口电路用于从所述终端设备的存储器接收信号，并向所述处理器发送所述信号，所述信号包括所述存储器中存储的计算机指令；当所述处理器执行所述计算机指令时，所述终端设备执行如权利要求1-9中任一项所述的设备安全操作的方法。

17.一种可读存储介质，其特征在于，所述可读存储介质中存储有指令，当所述可读存储介质在终端设备上运行时，使得所述终端设备执行权利要求1-9任一项所述的设备安全操作的方法。

18.一种计算机程序产品，其特征在于，当所述计算机程序产品在计算机上运行时，使得所述计算机执行权利要求1-9任一项所述的设备安全操作的方法。

一种设备安全操作的方法和装置

技术领域

[0001] 本申请涉及终端技术领域，尤其涉及一种设备安全操作的方法和装置。

背景技术

[0002] 随着智能终端设备的应用越来越广泛，可穿戴设备也逐渐受到用户的支持，例如智能手环和儿童手表。这类设备通常需要与管理者用户的智能手机之间进行账号绑定、请求信息或是解除绑定等信息交互，而在该类设备中可能存储着用户的位置信息、运动轨迹、健康指数、行为习惯和生活偏好等隐私信息，因此，信息交互中个人隐私泄露的危险大大增加。

[0003] 目前可穿戴设备的保护账号信息安全的方法，例如儿童手表的账号信息安全是通过服务器用户账号鉴权(Service Token)的方式，即服务器判断申请信息交互的设备携带的Service Token认证是否匹配，匹配通过即认为是合法请求。但是服务器用户账号鉴权的方式安全性不够高，存在撞库盗取账号信息的隐患，从而泄露个人隐私，威胁到可穿戴设备的用户安全。另外，可穿戴设备的账号绑定操作通常通过扫描二维码方式完成，绑定操作较为繁琐，用户体验不好。

发明内容

[0004] 本申请提供一种设备安全操作的方法和装置，解决了现有技术中账号绑定操作繁琐，且账号信息安全性不够高，存在泄露用户隐私、威胁用户安全的问题。

[0005] 为达到上述目的，本申请采用如下技术方案：

[0006] 第一方面，提供一种设备安全操作的方法，该方法包括：第一终端设备通过近场通信NFC操作接收第二终端设备发送的绑定操作标识，绑定操作标识包括第二终端设备向服务器发送的绑定请求所对应的标识；第一终端设备确认绑定操作标识是否合法；若绑定操作标识合法，且第一终端设备确定接受第二终端设备的绑定，则第一终端设备建立第一终端设备与第二终端设备的绑定关系。

[0007] 本申请实施例中，第二终端设备通过“碰一碰”操作，利用NFC技术向第一终端设备发送请求绑定操作对应的绑定操作标识，操作便捷、快速，可以提高用户在设备之间绑定操作的便捷性，提升用户体验。另外，第一终端设备确认上述第二终端设备申请的绑定操作标识是合法的后，建立与第二终端设备的绑定关系，从而可以提高用户设备之间的绑定设置的安全性，保护用户隐私信息。

[0008] 在一种可能的设计方式中，第一终端设备与第二终端设备的绑定关系包括：第一终端设备的用户身份证明UID与第二终端设备UID之间的映射关系。上述可能的实现方式中，第一终端设备与第二终端设备的绑定关系包括第一终端设备UID与第二终端设备UID之间的映射关系，从而根据映射关系判断两个设备的唯一绑定关系，提高安全性。

[0009] 在一种可能的设计方式中，该方法还包括：第一终端设备接收服务器发送的第一秘钥的公钥，和第二终端设备的UID、账号绑定时间信息；第一终端设备将映射关系、第一秘

钥的公钥、以及账号绑定时间信息存储在第一终端设备的嵌入式安全单元SE中或者可信执行环境TEE中；第一终端设备控制SE或TEE生成第二秘钥，并将第二秘钥的公钥发送给服务器。上述可能的实现方式中，第一终端设备接收服务器的加密公钥，并将与第二终端设备的绑定关系和该加密公钥存储在SE中或者TEE中，以便后续进行用户隐私信息的请求或者发送时，对请求设备的身份验证，提高设备操作的安全性，保护用户隐私信息。

[0010] 在一种可能的设计方式中，该方法还包括：第一终端设备接收第二终端设备的用户请求信息，其中，用户请求信息是第二终端设备使用第二秘钥的公钥加密处理的；第一终端设备控制SE或TEE根据第二秘钥的私钥对用户请求信息进行解密处理，得到第二终端设备是否通过认证的确认结果；第一终端设备控制SE或TEE根据第一秘钥的公钥对确认结果进行加密处理后发送给服务器；第一终端设备接收服务器发送的确认结果，确认结果是服务器通过第一秘钥的私钥解密得到的；若确认结果指示第二终端设备认证通过，则将第一终端设备对应的用户位置信息发送给第二终端设备。上述可能的实现方式中，第一终端设备接收到的第二终端设备的隐私信息请求是进行加密处理的，第一终端设备根据绑定关系判断该请求设备是否是管理员设备，并将判断结果用服务器的秘钥进行加密，发送给服务器，如此，可以提高设备操作的安全性，保护用户隐私信息。

[0011] 在一种可能的设计方式中，该方法还包括：第一终端设备接收第二终端设备的解除绑定请求信息，其中，解除绑定请求信息是第二终端设备使用第二秘钥的公钥加密处理的；第一终端设备控制SE或TEE根据第二秘钥的私钥对解除绑定信息进行解密处理，得到第二终端设备是否通过认证的确认结果；第一终端设备控制SE或TEE根据第一秘钥的公钥对确认结果进行加密处理后发送给服务器；第一终端设备接收服务器发送的确认结果，确认结果是服务器通过第一秘钥的私钥解密得到的；若确认结果指示第二终端设备认证通过，则第一终端设备控制所述SE或所述TEE删除第一终端设备与第二终端设备的绑定关系。上述可能的实现方式中，第一终端设备接收到的第二终端设备的隐私信息请求是进行加密处理的，第一终端设备根据绑定关系判断该请求设备是否是管理员设备，并将判断结果用服务器的秘钥进行加密，发送给服务器，如此，可以提高设备操作的安全性，保护用户隐私信息。

[0012] 第二方面，提供一种设备安全操作的方法，该方法包括：通信装置存储第一终端设备与第二终端设备之间的绑定关系；通信装置接收服务器发送的第一秘钥的公钥；通信装置生成第二秘钥，将第二秘钥的公钥发送给服务器。

[0013] 在一种可能的设计方式中，第一终端设备与第二终端设备的绑定关系包括：第一终端设备的用户身份证明UID与第二终端设备的UID之间的映射关系。

[0014] 在一种可能的设计方式中，该方法还包括：通信装置接收第二终端设备通过第一终端设备发送的用户请求信息，其中，用户请求信息是第二终端设备使用第二秘钥的公钥加密处理的；通信装置根据第二秘钥的私钥对用户请求信息进行解密处理，得到第二终端设备是否通过认证的确认结果；通信装置根据第一秘钥的公钥对确认结果进行加密处理后发送给服务器。

[0015] 在一种可能的设计方式中，该方法还包括：通信装置接收第二终端设备通过第一终端设备发送的解除绑定请求信息，其中，解除绑定请求信息是第二终端设备使用第二秘钥的公钥加密处理的；通信装置根据第二秘钥的私钥对解除绑定请求信息进行解密处理，

得到第二终端设备是否通过认证的确认结果;通信装置根据第一秘钥的公钥对确认结果进行加密处理后发送给服务器。

[0016] 第三方面,提供一种终端设备,该终端设备为第一终端设备,第一终端设备包括处理器,以及与处理器连接的存储器,存储器用于存储指令,当指令被处理器执行时,使得第一终端设备用于执行:通过近场通信NFC操作接收第二终端设备发送的绑定操作标识,绑定操作标识包括第二终端设备向服务器发送的绑定请求所对应的标识;确认绑定操作标识是否合法;若绑定操作标识合法,且确定接受第二终端设备的绑定,则建立第一终端设备与第二终端设备的绑定关系。

[0017] 在一种可能的设计方式中,第一终端设备与第二终端设备的绑定关系包括:第一终端设备的用户身份证明UID与第二终端设备的UID之间的映射关系。

[0018] 在一种可能的设计方式中,第一终端设备还用于执行:接收服务器发送的第一秘钥的公钥,和第二终端设备的UID、账号绑定时间信息;将映射关系、所述第一秘钥的公钥、以及账号绑定时间信息存储在嵌入式安全单元SE中或者可信执行环境TEE中;控制SE或TEE生成第二秘钥,并将第二秘钥的公钥发送给服务器。

[0019] 在一种可能的设计方式中,第一终端设备还用于执行:接收第二终端设备的用户请求信息,其中,用户请求信息是第二终端设备使用第二秘钥的公钥加密处理的;控制SE或TEE根据第二秘钥的私钥对用户请求信息进行解密处理,得到第二终端设备是否通过认证的确认结果;控制SE或TEE根据第一秘钥的公钥对确认结果进行加密处理后发送给服务器;接收服务器发送的确认结果,确认结果是服务器通过第一秘钥的私钥解密得到的;若确认结果指示第二终端设备认证通过,则将第一终端设备对应的用户位置信息发送给第二终端设备。

[0020] 在一种可能的设计方式中,第一终端设备还用于执行:接收第二终端设备的解除绑定请求信息,其中,解除绑定请求信息是第二终端设备使用第二秘钥的公钥加密处理的;控制SE或TEE根据第二秘钥的私钥对解除绑定信息进行解密处理,得到第二终端设备是否通过认证的确认结果;控制SE或TEE根据第一秘钥的公钥对确认结果进行加密处理后发送给服务器;接收服务器发送的确认结果,确认结果是服务器通过第一秘钥的私钥解密得到的;若确认结果指示第二终端设备认证通过,则控制所述SE或所述TEE删除第一终端设备与第二终端设备的绑定关系。

[0021] 第四方面,提供一种通信装置,应用于第一终端设备,该通信装置用于执行:存储第一终端设备与第二终端设备之间的绑定关系;接收服务器发送的第一秘钥的公钥;生成第二秘钥,将第二秘钥的公钥发送给服务器。

[0022] 在一种可能的设计方式中,第一终端设备与第二终端设备的绑定关系包括:第一终端设备的用户身份证明UID与第二终端设备的UID之间的映射关系。

[0023] 在一种可能的设计方式中,该通信装置还用于执行:接收第二终端设备通过第一终端设备发送的用户请求信息,其中,用户请求信息是第二终端设备使用第二秘钥的公钥加密处理的;根据第二秘钥的私钥对用户请求信息进行解密处理,得到第二终端设备是否通过认证的确认结果;根据第一秘钥的公钥对确认结果进行加密处理后发送给服务器。

[0024] 在一种可能的设计方式中,该通信装置还用于执行:接收第二终端设备通过第一终端设备发送的解除绑定请求信息,其中,解除绑定请求信息是第二终端设备使用第二秘

钥的公钥加密处理的;根据第二秘钥的私钥对解除绑定请求信息进行解密处理,得到第二终端设备是否通过认证的确认结果;根据第一秘钥的公钥对确认结果进行加密处理后发送给服务器。

[0025] 第五方面,提供一种芯片系统,该芯片系统应用于终端设备;该芯片系统包括一个或多个接口电路和一个或多个处理器;接口电路和处理器通过线路互联;接口电路用于从终端设备的存储器接收信号,并向处理器发送信号,信号包括存储器中存储的计算机指令;当处理器执行计算机指令时,使得终端设备执行第一方面及其任一种可能的设计方式的方法。

[0026] 第六方面,提供一种可读存储介质,该可读存储介质中存储有指令,当可读存储介质在终端设备上运行时,使得终端设备执行第一方面及其任一种可能的设计方式的方法。

[0027] 第七方面,提供一种计算机程序产品,当该计算机程序产品在计算机上运行时,使得计算机执行第一方面及其任一种可能的设计方式的方法。

[0028] 可以理解地,上述提供的任一种设备安全操作的的终端设备、通信装置、芯片系统、可读存储介质和计算机程序产品,均用于执行上文所提供的对应的方法,因此,其所能达到的有益效果可参考上文第一方面及其任一种可能的设计方式所对应的有益效果,此处不再赘述。

附图说明

[0029] 图1为本申请实施例提供的一种电子设备的硬件架构图;

[0030] 图2为本申请实施例提供的一种电子设备的的软件系统架构图;

[0031] 图3A为本申请实施例提供的一种设备安全操作的流程示意图;

[0032] 图3B为本申请实施例提供的一种设备安全操作的界面示意图;

[0033] 图3C为本申请实施例提供的另一种设备安全操作的界面示意图;

[0034] 图4为本申请实施例提供的一种设备安全操作的方法流程示意图;

[0035] 图5为本申请实施例提供的另一种设备安全操作的方法流程示意图;

[0036] 图6为本申请实施例提供的另一种设备安全操作的方法流程示意图;

[0037] 图7为本申请实施例提供的另一种设备安全操作的方法流程示意图;

[0038] 图8为本申请实施例提供的另一种设备安全操作的方法流程示意图;

[0039] 图9为本申请实施例提供的一种设备安全操作的装置的结构示意图。

具体实施方式

[0040] 以下,术语“第一”、“第二”仅用于描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”的特征可以明示或者隐含地包括一个或者更多个该特征。在本实施例的描述中,除非另有说明,“多个”的含义是两个或两个以上。

[0041] 在介绍本申请的实施例之前,首先对涉及到的技术做如下介绍:

[0042] 可穿戴设备:即可以直接穿或佩带在用户身上,或是整合到用户的衣服或配件的一种便携式设备,例如,儿童手表和智能手环等。可穿戴设备可以通过与其他终端设备之间的数据交互或云端服务来实现通信功能。

[0043] 安全元件(Secure Element,SE):即嵌入式安全单元SE,通常以芯片形式存在,也称为SE芯片,可以用于防止外部恶意解析攻击,保护数据安全。具体在芯片中具有加密/解密逻辑电路,可以生成秘钥,对数据进行加密保护。

[0044] 可信执行环境(Trusted execution environment,TEE):是主处理器内的安全区域,通常用来进行数字版权管理(Digital Rights Management,DRM)、移动支付和敏感数据保护。TEE通常运行在一个独立的环境中且与操作系统并行运行,通过同时使用硬件和软件来保护TEE中加载的数据和代码。

[0045] 可信服务管理(Trusted Service Manager,TSM):是一个兼具公信力和开放性等特点,提供应用发行管理和安全模块管理等功能的系统。TSM的业务功能大致包括安全域管理、应用管理、用户管理以及SE芯片管理等几个方面,本申请实施例中主要用于管理SE芯片的应用。

[0046] RSA加密算法:是一种非对称加密算法。由RSA加密算法得到的一对RSA密钥,如使用其中一个加密,则需要用另一个才能解密。具体可以为,其中一个是保密密钥,由用户保存,称为私钥;另一个为公开密钥,可对外公开,甚至可在网络服务器中注册,可称为公钥。为提高保密强度,RSA密钥至少为500位长,一般推荐使用2048位。RSA算法的名字是以发明者的名字Ron Rivest,Adi Shamir和Leonard Adleman来命名的。

[0047] 本申请实施例提供一种设备安全操作的方法,该方法可以应用于穿戴型电子设备和其管理员电子设备,具体可以应用于管理员电子设备对穿戴型电子设备进行用户账号绑定操作、请求用户信息操作或者解除绑定操作等信息交互的过程中,将隐私信息存储在SE芯片或者TEE系统中。通过该方法,可以解决现有的设备之间上述信息交互的安全性不够高,存在泄露用户隐私、威胁用户安全的问题,同时,还能解决账号绑定操作较为繁琐的问题。

[0048] 示例性的,本申请实施例中的电子设备可以包括第一终端设备和第二终端设备,其中,第一终端设备可以是可穿戴设备,例如儿童手表、智能手环、智能眼镜或智能球鞋等电子设备,本申请实施例对上述电子设备的具体形态不作特殊限制。第二终端设备可以是手机、平板电脑、桌面型、膝上型、手持计算机、笔记本电脑、超级移动个人计算机(ultra-mobile personal computer,UMPC)、上网本,以及蜂窝电话和个人数字助理(personal digital assistant,PDA)等。

[0049] 下面将结合附图对本申请实施例的实施方式进行详细描述。图1示出了电子设备100的结构示意图。

[0050] 电子设备100可以包括处理器110,SE安全芯片111,外部存储器接口120,内部存储器121,通用串行总线(universal serial bus,USB)接口130,充电管理模块140,电源管理模块141,电池142,天线1,天线2,移动通信模块150,无线通信模块160,音频模块170,扬声器170A,受话器170B,麦克风170C,耳机接口170D,传感器模块180,按键190,马达191,指示器192,摄像头193,显示屏194,以及用户标识模块(subscriber identification module,SIM)卡接口195等。

[0051] 其中传感器模块180可以包括压力传感器180A,陀螺仪传感器180B,气压传感器180C,磁传感器180D,加速度传感器180E,距离传感器180F,接近光传感器180G,指纹传感器180H,温度传感器180J,触摸传感器180K,环境光传感器180L,骨传导传感器180M等。

[0052] 可以理解的是,本发明实施例示意的结构并不构成对电子设备100的具体限定。在本申请另一些实施例中,电子设备100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。图示的部件可以以硬件,软件或软件和硬件的组合实现。

[0053] 处理器110可以包括一个或多个处理单元,例如:处理器110可以包括应用处理器(application processor,AP),调制解调处理器,图形处理器(graphics processing unit,GPU),图像信号处理器(image signal processor,ISP),控制器,存储器,视频编解码器,数字信号处理器(digital signal processor,DSP),基带处理器,和/或神经网络处理器(neural-network processing unit,NPU)等。其中,不同的处理单元可以是独立的器件,也可以集成在一个或多个处理器中。

[0054] SE安全芯片111可以是一个微型处理器,通过安全芯片和芯片操作系统实现数据安全存储、加解密运算等功能;也可以封装成各种形式,常见的有智能卡和嵌入式安全模块等。针对近场通信NFC终端设备开发的SE安全芯片,采用满足终端设备安全等级要求的智能安全芯片,内置安全操作系统,满足终端设备的安全密钥存储、数据加密服务等需求。

[0055] 其中,控制器可以是电子设备100的神经中枢和指挥中心。控制器可以根据指令操作码和时序信号,产生操作控制信号,完成取指令和执行指令的控制。

[0056] 处理器110中还可以设置存储器,用于存储指令和数据。在一些实施例中,处理器110中的存储器为高速缓冲存储器。该存储器可以保存处理器110刚用过或循环使用的指令或数据。如果处理器110需要再次使用该指令或数据,可从所述存储器中直接调用。避免了重复存取,减少了处理器110的等待时间,因而提高了系统的效率。

[0057] 在一些实施例中,处理器110可以包括一个或多个接口。接口可以包括集成电路(inter-integrated circuit,I2C)接口,集成电路内置音频(inter-integrated circuit sound,I2S)接口,脉冲编码调制(pulse code modulation,PCM)接口,通用异步收发传输器(universal asynchronous receiver/transmitter,UART)接口,移动产业处理器接口(mobile industry processor interface,MIPI),通用输入输出(general-purpose input/output,GPIO)接口,用户标识模块(subscriber identity module,SIM)接口,和/或通用串行总线(universal serial bus,USB)接口等。

[0058] 可以理解的是,本发明实施例示意的各模块间的接口连接关系,只是示意性说明,并不构成对电子设备100的结构限定。在本申请另一些实施例中,电子设备100也可以采用上述实施例中不同的接口连接方式,或多种接口连接方式的组合。

[0059] 充电管理模块140用于从充电器接收充电输入。其中,充电器可以是无线充电器,也可以是有线充电器。在一些有线充电的实施例中,充电管理模块140可以通过USB接口130接收有线充电器的充电输入。在一些无线充电的实施例中,充电管理模块140可以通过电子设备100的无线充电线圈接收无线充电输入。充电管理模块140为电池142充电的同时,还可以通过电源管理模块141为电子设备供电。

[0060] 电源管理模块141用于连接电池142,充电管理模块140与处理器110。电源管理模块141接收电池142和/或充电管理模块140的输入,为处理器110,内部存储器121,外部存储器,显示屏194,摄像头193,和无线通信模块160等供电。电源管理模块141还可以用于监测电池容量,电池循环次数,电池健康状态(漏电,阻抗)等参数。在其他一些实施例中,电源管

理模块141也可以设置于处理器110中。在另一些实施例中，电源管理模块141和充电管理模块140也可以设置于同一个器件中。

[0061] 电子设备100的无线通信功能可以通过天线1，天线2，移动通信模块150，无线通信模块160，调制解调处理器以及基带处理器等实现。

[0062] 电子设备100通过GPU，显示屏194，以及应用处理器等实现显示功能。GPU为图像处理的微处理器，连接显示屏194和应用处理器。GPU用于执行数学和几何计算，用于图形渲染。处理器110可包括一个或多个GPU，其执行程序指令以生成或改变显示信息。

[0063] 显示屏194用于显示图像，视频等。显示屏194包括显示面板。显示面板可以采用液晶显示屏(liquid crystal display，LCD)，有机发光二极管(organic light-emitting diode，OLED)，有源矩阵有机发光二极体或主动矩阵有机发光二极体(active-matrix organic light emitting diode的，AMOLED)，柔性发光二极管(flex light-emitting diode，FLED)，Miniled，MicroLed，Micro-oLed，量子点发光二极管(quantum dot light emitting diodes，QLED)等。在一些实施例中，电子设备100可以包括1个或N个显示屏194，N为大于1的正整数。

[0064] 电子设备100可以通过ISP，摄像头193，视频编解码器，GPU，显示屏194以及应用处理器等实现拍摄功能。

[0065] 电子设备100可以通过音频模块170，扬声器170A，受话器170B，麦克风170C，耳机接口170D，以及应用处理器等实现音频功能。例如音乐播放，录音等。

[0066] 电子设备100的软件系统可以采用分层架构，事件驱动架构，微核架构，微服务架构，或云架构。本发明实施例以分层架构的Android系统为例，示例性说明电子设备100的软件结构。

[0067] 图2是本发明实施例的电子设备100的软件结构框图。分层架构将软件分成若干个层，每一层都有清晰的角色和分工。层与层之间通过软件接口通信。在一些实施例中，将Android系统分为四层，从上至下分别为应用程序层，应用程序框架层，安卓运行时(Android runtime)和系统库，以及内核层。

[0068] 应用程序层可以包括一系列应用程序包。如图2所示，应用程序包可以包括相机，图库，日历，通话，地图，导航，WLAN，蓝牙，音乐，视频，短信息等应用程序。

[0069] 应用程序框架层为应用程序层的应用程序提供应用编程接口(application programming interface，API)和编程框架。应用程序框架层包括一些预先定义的函数。

[0070] 如图2所示，应用程序框架层可以包括窗口管理器，内容提供器，视图系统，电话管理器，资源管理器，通知管理器等。

[0071] 窗口管理器用于管理窗口程序。窗口管理器可以获取显示屏大小，判断是否有状态栏，锁定屏幕，截取屏幕等。

[0072] 内容提供器用来存放和获取数据，并使这些数据可以被应用程序访问。所述数据可以包括视频，图像，音频，拨打和接听的电话，浏览历史和书签，电话簿等。

[0073] 视图系统包括可视控件，例如显示文字的控件，显示图片的控件等。视图系统可用于构建应用程序。显示界面可以由一个或多个视图组成的。例如，包括短信通知图标的显示界面，可以包括显示文字的视图以及显示图片的视图。

[0074] 电话管理器用于提供电子设备100的通信功能。例如通话状态的管理(包括接通，

挂断等)。

[0075] 资源管理器为应用程序提供各种资源,比如本地化字符串,图标,图片,布局文件,视频文件等等。

[0076] 通知管理器使应用程序可以在状态栏中显示通知信息,可以用于传达告知类型的消息,可以短暂停留后自动消失,无需用户交互。比如通知管理器被用于告知下载完成,消息提醒等。通知管理器还可以是以图表或者滚动条文本形式出现在系统顶部状态栏的通知,例如后台运行的应用程序的通知,还可以是以对话窗口形式出现在屏幕上的通知。例如在状态栏提示文本信息,发出提示音,电子设备振动,指示灯闪烁等。

[0077] Android Runtime包括核心库和虚拟机。Android runtime负责安卓系统的调度和管理。核心库包含两部分:一部分是java语言需要调用的功能函数,另一部分是安卓的核心库。

[0078] 应用程序层和应用程序框架层运行在虚拟机中。虚拟机将应用程序层和应用程序框架层的java文件执行为二进制文件。虚拟机用于执行对象生命周期的管理,堆栈管理,线程管理,安全和异常的管理,以及垃圾回收等功能。

[0079] 系统库可以包括多个功能模块。例如:表面管理器(surface manager),媒体库(Media Libraries),三维图形处理库(例如:OpenGL ES),2D图形引擎(例如:SGL)等。

[0080] 表面管理器用于对显示子系统进行管理,并且为多个应用程序提供了2D和3D图层的融合。

[0081] 媒体库支持多种常用的音频,视频格式回放和录制,以及静态图像文件等。媒体库可以支持多种音视频编码格式,例如:MPEG4、H.264、MP3、AAC、AMR、JPG或PNG等。

[0082] 三维图形处理库用于实现三维图形绘图、图像渲染、合成、和图层处理等。2D图形引擎是2D绘图的绘图引擎。

[0083] 内核层是硬件和软件之间的层。内核层至少包含显示驱动,摄像头驱动,音频驱动,传感器驱动。

[0084] 以下实施例中的方法均可以在具有上述硬件结构和软件结构的电子设备100中实现。本申请的以下实施例仅以第一终端设备为儿童手表,和第二终端设备为手机作为示例,儿童手表服务器侧生成的秘钥称为第一秘钥,儿童手表生成的秘钥称为第二秘钥为例,进行详细说明。

[0085] 如图3A所示,本申请实施例提供一种设备安全操作的方法,其中,当手机和儿童手表上都安装有SE芯片时,手机向儿童手表申请绑定操作的过程可以包括:

[0086] 301:手机向儿童手表服务器发送绑定操作申请,获取绑定操作标识。

[0087] 手机可以通过儿童手表服务器,申请与儿童手表进行账号绑定操作,该手机与儿童手表的账号绑定成功后,手机即可作为管理员设备对儿童手表进行功能设置或者个人信息请求,例如,对儿童手表的用户信息进行查看或者设置,获取儿童手表的用户所在位置,还可以进行账号解除绑定的操作。

[0088] 其中,儿童手表服务器可以为儿童手表提供数据处理和数据存储服务,可以用于接收管理员设备如手机的操作信息,并进行处理和保存,建立管理员设备列表并进行信息维护和更新;还用于保存儿童手表的各种数据信息,例如位置信息,位置轨迹记录,运动信息和个人设置信息等。具体的,儿童手表服务器可以为能够为儿童手表提供远程数据处理

的云端设备或者服务器。

[0089] 进一步的,手机上可以安装有儿童手表对应的应用程序(Application,APP),用户可以通过手机上的儿童手表APP对儿童手表发送绑定操作申请。例如,如图3B所示,用户可以打开儿童手表APP,点击进入“儿童手表绑定设置”页面,点击请求绑定操作下显示的“进入”按钮,则儿童手表APP向儿童手表服务器发送绑定该儿童手表的操作请求。其中,可以点击“绑定指南”,查看绑定操作相关的提示信息;如果收到其他管理员设备的绑定操作邀请,可以点击页面上显示的“如果已收到主管理员邀请,请点击”。

[0090] 其中,儿童手表APP向儿童手表服务器发送的绑定请求,具体可以包括手机设备标识、手机的用户账号标识和操作类型。其中,手机设备标识、手机用户账号标识都是唯一的,用来指示该手机设备,操作类型可以指示该操作申请为绑定操作或者解除绑定操作等。

[0091] 儿童手表服务器接收到上述绑定请求后,生成该手机向该儿童手表发送的绑定请求所对应的标识,即为绑定操作标识,将该绑定操作标识发送给手机。

[0092] 302:手机将绑定操作标识写入手机上的SE芯片。

[0093] 进一步的,手机上可以安装有SE芯片,该SE芯片可以用于写入和读取数据,并可以根据写入的数据判断当前请求数据是否与预先存储的匹配。

[0094] 303:手机与儿童手表“碰一碰”,通过近场通信NFC操作向儿童手表发送绑定操作标识。

[0095] “碰一碰”操作,也就是通过两个设备彼此靠近,即可利用近场通信NFC进行通信,具体为手机向儿童手表发送绑定操作标识。

[0096] 其中,该绑定操作标识可以使手机向儿童手表服务器发送的绑定请求所对应的标识。该绑定操作标识相对于用户的一次绑定请求是唯一的,用于建立手机与儿童手表的绑定关系。

[0097] 304:儿童手表确认绑定操作标识是否合法。

[0098] 具体的,儿童手表确认该绑定操作标识是否合法,可以通过将绑定操作标识发送给儿童手表服务器,由儿童手表服务器与前述生成的绑定操作标识进行验证后,确认是否合法,将验证结果发送给儿童手表。

[0099] 儿童手表接收到确认结果是合法的后,儿童手表可以在的界面显示提示消息,如图3C所示,请儿童手表的用户确认是否接受该手机的绑定申请,儿童手表界面显示“是否同意授权xx用户管理”,用户可以点击界面上的“同意”或者“拒绝”按钮进行操作。其中,儿童手表的用户点击“同意”,则表示确认儿童手表接受该手机的绑定,则执行步骤406;儿童手表的用户点击“拒绝”,则表示拒绝儿童手表接受该手机的绑定,则儿童手表返回拒绝消息给儿童手表服务器,结束任务。

[0100] 305:若绑定操作标识合法,且儿童手表确定接受绑定,则儿童手表建立与手机的绑定关系,并将其存入儿童手表的SE芯片。

[0101] 其中,儿童手表与该手机的绑定关系,可以包括该手机的用户身份证明(User Identification,UID)与该儿童手表的UID的映射关系。

[0102] 其中,步骤302与步骤305中的SE芯片可以替换为可信执行环境TEE系统,其中,TEE系统是与电子设备的操作系统可以并行处理的系统,TEE系统可以对传输数据进行加密处理和解密处理,还可以写入信息,对信息进行安全存储。

[0103] 也就是说,步骤302中手机侧可以将绑定操作标识写入手机上的TEE系统中,步骤305中的儿童手表与手机的绑定关系可以存储在儿童手表的TEE系统中。具体的通过SE芯片或者TEE加密的绑定操作流程可以参考下述的实施例一和实施例二。

[0104] 上述实施例中,手机通过碰一碰操作实现便捷的绑定申请,同时,将手机与儿童手表的绑定信息存储在SE芯片或者TEE系统中,后续手机向儿童手表进行敏感信息操作的申请时,都需要先到儿童手表的SE芯片或者TEE系统中做设备身份鉴权,从而提高儿童手表用户信息的安全性,提升用户使用体验。

[0105] 实施例一:

[0106] 本申请实施例提供一种设备安全操作的方法,手机和儿童手表都安装有SE芯片,采用SE芯片进行数据传输中的加密和解密操作。

[0107] 结合图3A所示,基于SE芯片的设备安全操作的方法实施例中,手机管理儿童手表的通信网络还可以包括TSM服务器。

[0108] 其中,TSM服务器,是用来管理手机上的SE芯片和儿童手表上的SE芯片,所有需要存储到SE芯片的数据收发,都要通过TSM服务器来实现。通过TSM服务器还可以向儿童手表发送应用协议数据单元(ApplicationProtocolDataUnit,APDU)指令,用于指示儿童手表安装安全域和应用。

[0109] 其中,APDU是智能卡与智能卡读卡器之间传送的信息单元,在本申请的下述实施例中,手机被模拟为智能卡,儿童手表被模拟为智能卡读卡器。一个APDU指令可以是一个命令,也可以是命令的响应。

[0110] 进一步的,手机与儿童手表进行账号绑定的具体过程如图4,可以包括:

[0111] 401:手机向儿童手表服务器发送绑定请求。

[0112] 402:儿童手表服务器将绑定操作标识发送给手机。

[0113] 儿童手表服务器接收到手机的绑定请求后,生成该绑定请求对应的绑定操作标识。同时,儿童手表服务器可以配置该绑定操作标识在10分钟内有效,如果超过10分钟儿童手表服务器没有收到儿童手表的响应信息,则该次绑定请求失效,儿童手表服务器可以发送信息给手机,手机上的APP显示提示信息,请用户重新提交绑定请求,或者退出绑定申请的操作。

[0114] 403:手机接收绑定请求标识,将该绑定请求标识存储在手机上的嵌入式安全单元SE中。

[0115] 404:儿童手表通过近场通信NFC操作接收手机发送的绑定请求标识。

[0116] 具体操作可以为用户将手机与儿童手表碰一碰,设备近距离接触后,手机可以通过NFC通信将绑定请求标识发送给儿童手表。

[0117] 405:儿童手表确认绑定请求标识是否合法,如确认该绑定请求标识合法则儿童手表显示询问消息,获取用户指示。

[0118] 406:若绑定请求标识合法,且儿童手表确定接受该手机的绑定,则儿童手表建立儿童手表与该手机的绑定关系。

[0119] 其中,绑定关系包括该手机UID与该儿童手表UID的映射关系。

[0120] 进一步的,儿童手表将该映射关系发送给儿童手表服务器进行存储。

[0121] 407:儿童手表与TSM服务器交互,完成安装安全域和应用。

[0122] 具体的，儿童手表向TSM服务器发起安装安全域和应用的请求，获取APDU指令，该APDU指令用于指示儿童手表上的SE芯片完成安全域和应用的安装。儿童手表上的SE芯片完成安全域和应用的安装后，返回信息给TSM服务器。TSM服务器再向儿童手表发送安装完成消息。

[0123] 其中，安全域是指同一环境内有相同的安全保护需求、相互信任、并具有相同的安全访问控制和边界控制策略的系统。

[0124] 安装安全域可以用于TSM服务器对电子设备上的SE芯片进行管理的操作代理，TSM服务器可以利用此操作代理，授权程序进行加载、安装、删除相关的应用。同时，安全域的空间管理由TSM服务器完成，具体的空间管理包括签约空间管理和应用大小管理两种模式。

[0125] 408：儿童手表向儿童手表服务器发送个人化申请。

[0126] 其中，该个人化申请是在儿童手表接收到用户确认接收该手机的绑定申请后，儿童手表自动生成的，是用于指示TSM服务器完成该手机与儿童手表的账号设备账号绑定操作的。

[0127] 409：儿童手表服务器生成第一秘钥。

[0128] 儿童手表服务器收到该个人化申请后，生成服务器的第一秘钥，具体可以为RSA公私钥。其中，公钥和私钥是成对的，它们互相解密。一般为发送方将信息通过接收方生成的公钥进行加密，接收方通过之前生成的该公钥对应的私钥进行解密，即可获取发送方传递的信息。

[0129] 410：儿童手表服务器向TSM服务器发送手机UID、绑定时间信息和第一秘钥的公钥。

[0130] 411：TSM服务器向儿童手表SE芯片发送APDU指令，将绑定关系写入儿童手表的SE芯片。

[0131] 具体的，TSM服务器向儿童手表发送APDU指令，用于将手机UID与儿童手表UID的映射关系、绑定时间信息和第一秘钥的公钥进行信息处理后，生成SE芯片可以识别的、符合传输协议规范的APDU指令，发送给儿童手表的SE芯片。

[0132] 进一步的，TSM服务器可以通过安全级别的加密通道传输该APDU指令给儿童手表的SE芯片，并且可以对该APDU指令进行消息认证码(Message Authentication Code，MAC)计算。儿童手表的SE芯片接收到APDU指令之后，SE芯片操作系统进行解析和MAC校验处理，以便确认数据的安全性和完整性。其中，MAC校验为通过一定的算法，识别接收的指令数据是否与期望的一致，从而可以确认该APDU指令的数据完整性。

[0133] 儿童手表的SE芯片通过解析APDU指令，获取手机UID与儿童手表UID的映射关系、绑定时间信息和第一秘钥的公钥，根据手机UID与儿童手表UID的映射关系、绑定时间信息建立该手机对该儿童手表的管理员信息，并将其管理员信息写入儿童手表的SE芯片，也就是存储在对应的SE芯片内部的文件系统(存储单元)中，以备后续进行信息交互过程中的管理员确认。

[0134] 同时，儿童手表的SE芯片存储儿童手表服务器公钥，也就是第一秘钥的公钥，以便于后续向儿童手表服务器发送用户的隐私信息时，用该儿童手表服务器公钥进行加密传送，保证用户信息的安全性。

[0135] 412：儿童手表向儿童手表服务器返回执行结果。

[0136] 儿童手表向儿童手表服务器发送是否成功将手机UID、绑定时间信息和第一秘钥的公钥写入儿童手机的SE芯片的返回消息。

[0137] 413:TSM服务器向儿童手表发送APDU指令,用于请求儿童手表的第二秘钥的公钥。

[0138] 其中,该第二秘钥是指儿童手表上的SE芯片生成的RSA秘钥中的公钥和公钥,其中,第二秘钥的公钥也可以称之为SE芯片公钥。

[0139] 414:儿童手表的SE芯片产生第二秘钥。

[0140] 具体的,第二秘钥可以为儿童手表控制SE芯片生成的一对RSA公钥和私钥,进行加密操作和解密操作。

[0141] 415:儿童手表的SE芯片发送第二秘钥的公钥给TSM服务器。

[0142] 416:TSM服务器发送第二秘钥的公钥给儿童手表服务器。

[0143] 417:儿童手表服务器向儿童手表发送个人化完成消息。

[0144] 儿童手表服务器接收到儿童手表发送的第二秘钥的公钥,进行存储,以便于后续向儿童手表发送用户隐私信息时,用该儿童手表的SE芯片的公钥进行加密传送。

[0145] 418:手机向儿童手表服务器发送请求消息,查询绑定操作是否已完成。

[0146] 其中,该请求信息用于指示查询该手机的绑定操作是否已经完成。

[0147] 419:儿童手表服务器向手机返回消息。

[0148] 如该绑定操作已完成,则儿童手表服务器向手机返回消息,用于指示该绑定操作已完成;如该绑定操作未完成,则儿童手表服务器向向手机返回消息,用于指示该绑定操作未完成。

[0149] 进一步的,手机可以重复多次地向儿童手表服务器请求绑定操作结果是否已完成,如确定结果为已完成,则手机可以通过儿童手表APP展示绑定操作完成的界面。

[0150] 进一步可选的,在完成绑定操作和存储的流程后,儿童手表还可以根据需要查询管理员列表,向儿童手表的SE芯片发送查询管理员列表的请求,儿童手表的SE芯片将管理员列表数据用服务器公钥(第一秘钥的公钥)加密发送给儿童手表服务器,儿童手表服务器用服务器私钥(第一秘钥的私钥)进行解密处理,获取相关的管理员列表数据;同时,儿童手表服务器将本次的绑定操作标识对应的状态更新为绑定完成状态。其中,管理员列表数据可以包括上述存入SE芯片的手机UID与绑定时间信息。

[0151] 上述实施例,通过一系列信息交互,将手机向儿童手表的绑定请求所生成的手机与儿童手表的绑定关系,通过信息加密传送的方式,存储在儿童手表的SE芯片中,以便于后续进行敏感信息的操作申请时,进行管理员身份的验证。从而确保儿童手表的用户隐私信息不会发送给没有进行过绑定操作的手机设备,从而保证了用户的安全性。

[0152] 实施例二:

[0153] 本申请实施例提供一种设备安全操作的方法,手机和儿童手表都安装有TEE系统,TEE系统可以用于存储用户的隐私信息,还用于生成秘钥,以进行儿童手表和儿童手表服务器之间的数据传输中的加密处理和解密处理。如图5所示,具体绑定操作流程可以包括:

[0154] 501:手机向儿童手表服务器发送绑定请求。

[0155] 502:儿童手表服务器将绑定操作标识发送给手机。

[0156] 503:手机接收绑定请求标识,将该绑定请求标识存储在TEE中。

[0157] 其中,可信执行环境TEE是可以与手机的操作系统并行处理的系统,可以进行加密

信息的传输，信息的解密处理，和用户隐私信息的存储。

[0158] 504：儿童手表通过近场通信NFC操作接收手机发送的绑定请求标识。

[0159] 505：儿童手表确认绑定请求标识是否合法，如确认该绑定请求标识合法则儿童手表显示询问消息，获取用户指示。

[0160] 506：若绑定请求标识合法，且儿童手表确定接受绑定，则儿童手表建立儿童手表与该手机的绑定关系。

[0161] 507：儿童手表上的TEE产生第二秘钥。

[0162] 具体的，第二秘钥可以为该儿童手表控制TEE系统生成的一对公钥和私钥，可以分别进行加密操作和解密操作。

[0163] 508：发送个人化申请，并发送第二秘钥的公钥。

[0164] 将儿童手表上的TEE产生的公钥发送给儿童手表服务器，以便于后续儿童手表服务器向儿童手表发送隐私信息时，可以用通过该儿童手表公钥进行加密传送。

[0165] 509：儿童手表服务器保存第二秘钥的公钥，并生成第一秘钥。

[0166] 儿童手表服务器生成的第一秘钥可以是一对公钥和私钥，可以分别进行加密操作和解密操作。

[0167] 510：儿童手表服务器向儿童手表发送手机UID、绑定时间信息和第一秘钥的公钥。

[0168] 儿童手表接收到儿童手表服务器发送的第一秘钥的公钥，也就是服务器公钥，进行存储，以便于后续向儿童手表服务器发送用户隐私信息时，用该服务器公钥进行加密传送。

[0169] 511：儿童手表向儿童手表服务器返回操作结果。

[0170] 512：儿童手表服务器向儿童手表发送TEE个人化结束的消息。

[0171] 513：手机向儿童手表服务器发送请求消息，查询绑定操作是否已完成。

[0172] 514：儿童手表服务器向手机返回消息。

[0173] 如该绑定操作已完成，则儿童手表服务器向手机返回消息，用于指示该绑定操作已完成；如该绑定操作未完成，则儿童手表服务器向向手机返回消息，用于指示该绑定操作未完成。

[0174] 进一步的，手机可以重复多次地向儿童手表服务器请求绑定操作结果是否已完成，如确定结果为已完成，则手机可以通过儿童手表APP展示绑定操作完成的界面。

[0175] 进一步可选的，在完成绑定操作和存储的流程后，儿童手表还可以根据需要查询管理员列表，向儿童手表的TEE系统发送查询管理员列表的请求，儿童手表的TEE系统将管理员列表数据用服务器公钥(第一秘钥的公钥)加密发送给儿童手表服务器，儿童手表服务器用服务器私钥(第一秘钥的私钥)进行解密处理，获取相关的管理员列表数据；同时，儿童手表服务器将本次的绑定操作标识对应的状态更新为绑定完成状态。其中，管理员列表数据可以包括上述存入TEE系统的手机UID与绑定时间信息。

[0176] 上述实施例，通过一系列信息交互，将手机向儿童手表的绑定请求所生成的手机与儿童手表的绑定关系，通过信息加密传送的方式，存储在儿童手表的TEE系统中，以便于后续进行敏感信息的操作申请时，进行管理员身份的验证。从而确保儿童手表的用户隐私信息不会发送给没有进行过绑定操作的手机设备，从而保证了用户的安全性。

[0177] 在另一种实施方式中，手机与儿童手表建立绑定关系完成之后，手机可以请求获

取该儿童手表的用户的隐私信息，又称用户请求信息；该用户请求信息可以包括，例如，用户的位置信息、运动轨迹或者健康信息等。示例性的，手机请求儿童手表的位置信息的具体过程如图6，可以包括：

[0178] 601：手机向儿童手表服务器发送请求定位信息。

[0179] 用户可以通过操作手机上儿童手表APP上的相应按钮，触发手机向儿童手表服务器发送请求定位信息，例如，在手机APP上点击“获取儿童手表用户的当前位置”。

[0180] 602：儿童手表服务器向儿童手表发送推送消息。

[0181] 其中，该推送消息用于指示手机对该儿童手表存在服务请求。

[0182] 603：儿童手表服务器向手机返回该推送消息ID。

[0183] 其中，推送消息ID可以为上述推送消息对应的标识ID，用于向手机反馈已将推送消息发送给儿童手表。

[0184] 604：儿童手表向儿童手表服务器发送请求获取推送消息的内容。

[0185] 605：儿童手表发送第二秘钥的公钥加密处理的用户请求信息给儿童手表服务器。

[0186] 其中，用户请求信息具体可以为，手机向儿童手表申请的请求定位信息。

[0187] 儿童手表服务器向儿童手表发送加密信息，该加密信息是将请求定位信息用儿童手表侧的公钥，也就是第二秘钥的公钥进行加密处理后的信息。

[0188] 其中，第二秘钥的公钥可以是儿童手表上的SE芯片生成的公钥，也可以是TEE生成的公钥。

[0189] 606：儿童手表控制SE或者TEE根据第二秘钥的私钥对用户请求信息进行解密处理，得到该手机是否通过认证的确认结果。

[0190] 具体的，儿童手表上的SE芯片或者TEE系统接收该加密信息后，进行解密处理，获取请求定位信息，根据SE芯片或者TEE系统中存储的管理员设备列表中出具，确定该请求定位信息是否是管理员设备发送的。具体可以为SE芯片或者TEE系统根据该请求定位信息中携带的手机UID，将该手机UID与管理员设备列表中绑定的手机UID列表进行匹配，如果匹配成功则返回该手机是管理员设备的确认结果；如果匹配不成功，则返回该手机不是管理员设备的确认结果。

[0191] 607：儿童手表控制SE或TEE根据第一秘钥的公钥对确认结果进行加密处理后发送给儿童手表服务器。

[0192] 608：儿童手表服务器进行解密处理后，将确认结果发送给儿童手表。

[0193] 如果该确认结果为该手机是儿童手表的管理员设备，则执行步骤609；如果该确认结果为该手机不是儿童手表的管理员设备，则结束任务。

[0194] 609：儿童手表获取当前设备的位置信息。

[0195] 具体的，儿童手表可以根据GPS卫星全球定位系统、基站定位或者Wi-Fi定位等技术，获取儿童手表的当前位置信息，也就代表儿童手表的用户的当前位置信息。

[0196] 610：儿童手表向儿童手表服务器发送位置信息。

[0197] 具体的，儿童手表将位置信息发送给儿童手表服务器后，儿童手表服务器向手机发送通知消息，表示该儿童手表的位置信息已更新，手机可以根据需要进行查询，获取位置信息。同时，儿童手表服务器更新其上存储的该儿童手表的位置信息后，儿童手表服务器还可以向儿童手表发送响应消息，表示已将位置信息进行更新。

[0198] 611:手机向儿童手表服务器获取位置信息。

[0199] 手机向儿童手表服务器发送查询请求,儿童手表服务器接收到该查询请求后,将上述更新的位置信息发送给手机。

[0200] 进一步的,手机可以重复多次地向儿童手表服务器请求儿童手表的当前位置信息,儿童手表服务器判断请求的设备合法性,并根据更新位置信息返回给手机,则手机可以通过儿童手表APP显示儿童手表的位置信息。

[0201] 上述实施例通过儿童手表获取的儿童所在位置,属于极其敏感的安全信息,用户不希望暴露被他人知晓或利用,因此,本申请实施例中,儿童手表受到的所有敏感操作请求,都需要先通过儿童手表的SE芯片或者TEE系统确认家长手机设备的合法性,确认是管理设备列表中的管理员设备,才能进行下一步业务操作,从而确保用户隐私信息的安全性,提高用户的使用体验。

[0202] 需要说明的是,上述实施例仅以手机向儿童手表请求位置信息作为示例进行介绍,该用户请求信息还可以包括儿童手表用户的运动轨迹信息、生活习惯记录或者健康信息等,上述实施例并不对本申请的保护范围形成一定的限制。

[0203] 在另一种实施方式中,手机与儿童手表建立绑定关系之后,根据需要手机可以随时解除与该儿童手表的绑定关系,例如,手机和儿童手表上安装SE芯片,则手机请求儿童手表解除绑定关系的具体过程如图7所示,可以包括:

[0204] 701:手机向儿童手表服务器发送解除绑定请求信息。

[0205] 用户可以通过操作手机上儿童手表APP上的相应按钮,触发手机向儿童手表服务器发送解除绑定请求信息,例如,在手机APP上点击“解除绑定关系”。

[0206] 702:儿童手表服务器向儿童手表发送推送消息。

[0207] 其中,该推送消息用于指示手机向该儿童手表存在服务请求。

[0208] 703:儿童手表服务器向手机发送推送消息ID。

[0209] 其中,该推送消息ID用于指示上述推动消息的类型,用于向手机反馈,已将推送消息发送给儿童手表。

[0210] 704:儿童手表向儿童手表服务器发送请求推送消息的内容。

[0211] 其中,该请求推送消息的内容可以为,手机向儿童手表申请的解除绑定请求信息。

[0212] 705:儿童手表服务器发送第二秘钥的公钥加密处理的解除绑定请求信息给儿童手表。

[0213] 具体可以为,儿童手表服务器向儿童手表发送加密信息,该加密信息是将解除绑定请求信息用儿童手表侧的公钥,也就是第二秘钥的公钥进行加密处理后的信息。其中,儿童手表侧的公钥可以是SE芯片生成的公钥。

[0214] 706:儿童手表控制SE确认该手机是否是管理员设备。

[0215] 具体的,儿童手表上的SE芯片接收该加密信息后,根据第二秘钥的私钥进行解密处理,获取解除绑定请求信息。

[0216] SE芯片根据存储的管理员设备列表中数据确定该手机是否是管理员设备的。具体可以为SE芯片该解除绑定关系的请求消息中携带的手机UID,将该手机UID与管理员设备列表中绑定的手机UID列表进行匹配,如果匹配成功则返回该手机是管理员设备的确认结果;如果匹配不成功,则返回该手机不是管理员设备的确认结果。

[0217] 707:儿童手表上的SE返回确认结果。

[0218] 具体可以为,儿童手表控制SE芯片将生成的确认结果用儿童手表服务器的公钥,也就是第一秘钥的公钥进行加密处理后,发送给儿童手表服务器。

[0219] 708:儿童手表服务器进行解密处理后,将确认结果发送给儿童手表。

[0220] 如果该确认结果为该手机是儿童手表的管理员设备,则执行步骤709;如果该确认结果为该手机不是儿童手表的管理员设备,则结束任务。

[0221] 709:儿童手表向儿童手表服务器发送解除绑定请求信息。

[0222] 710:儿童手表服务器发送手机ID信息给TSM服务器。

[0223] 进一步的,儿童手表服务器将该手机UID、绑定时间信息等发送给TSM服务器。

[0224] 711:TSM服务器向儿童手表发送APDU指令,指示SE芯片解除绑定关系。

[0225] 具体的,TSM服务器向儿童手表发送APDU指令,用于将手机UID、绑定时间等信息进行处理后,生成SE芯片可以识别的、符合传输协议规范的APDU指令,发送给儿童手表的SE芯片。

[0226] 712:儿童手表中的SE芯片将绑定关系从SE芯片删除。

[0227] 具体的可以为,认证通过,则儿童手表控制SE删除儿童手表与该手机的绑定关系。

[0228] 713:儿童手表向TSM服务器返回APDU响应消息。

[0229] 也就是儿童手表向TSM服务器反馈成功将账号绑定信息从儿童手机的SE芯片删除的返回信息。

[0230] 714:TSM服务器向儿童手表服务器发送解除绑定结果。

[0231] 儿童手表服务器接收该绑定关系结果,并更新儿童手表服务器上存储的绑定关系列表的相关信息。

[0232] 715:儿童手表服务器向儿童手表发送解除绑定结果。

[0233] 进一步的,手机可以重复多次地向儿童手表服务器请求查询解除绑定的结果,儿童手表服务器判断解除绑定操作已完成,则返回解除绑定结果,则手机可以通过儿童手表APP展示已解除相关设备的显示界面。

[0234] 在上述可能的实现方式中,手机向儿童手表请求解除绑定操作,需要先通过儿童手表上的SE芯片,确认该手机是否是为合法的管理员设备,通过SE芯片的加密保证验证过程的安全性,在确认手机是管理员设备后,再进行相应的解除绑定的具体操作,从而不会对管理设备造成错误解绑,保证用户信息的安全性。

[0235] 在另一种可能的实施方式中,手机和儿童手表上安装TEE系统,则手机请求儿童手表解除绑定关系的具体过程如图8所示,可以包括:

[0236] 801:手机向儿童手表服务器发送解除绑定请求信息。

[0237] 用户可以通过操作手机上儿童手表APP上的相应按钮,触发手机向儿童手表服务器发送解除绑定请求信息,例如,在手机APP上点击“解除绑定关系”。

[0238] 802:儿童手表服务器向儿童手表发送推送消息。

[0239] 其中,该推送消息用于指示手机向该儿童手表存在服务请求。

[0240] 803:儿童手表服务器向手机发送推送消息ID。

[0241] 其中,推送消息ID用于标识上述推送消息的类型,用于向手机反馈,已将上述推送消息发送给儿童手表。

[0242] 804:儿童手表向儿童手表服务器发送请求推送消息的内容。

[0243] 其中,该请求推送消息的内容可以为,手机向儿童手表申请的解除绑定信息。

[0244] 805:儿童手表服务器控制TEE根据第二秘钥的私钥解除绑定请求信息进行加密后,发送给儿童手表。

[0245] 具体的,儿童手表服务器向儿童手表发送加密信息,该加密信息是将解除绑定请求信息用儿童手表侧的公钥,也就是第二秘钥的公钥进行加密处理后的信息。其中,儿童手表侧的公钥可以是TEE系统生成的公钥。

[0246] 806:儿童手表确认该手机是否是管理员设备。

[0247] 具体的,儿童手表上的TEE系统接收该加密信息后,根据第二秘钥的私钥进行解密处理,获取解除绑定请求信息。

[0248] 根据TEE系统中存储的管理员设备列表中数据确定该手机是否是管理员设备的。具体可以为TEE系统将该解除绑定关系的请求消息中携带的手机UID,将该手机UID与管理员设备列表中绑定的手机UID列表进行匹配,如果匹配成功则返回该手机是管理员设备的确认结果;如果匹配不成功,则返回该手机不是管理员设备的确认结果。

[0249] 807:儿童手表返回确认结果(加密)。

[0250] 具体可以为,儿童手表上的TEE系统将生成的确认结果用儿童手表服务器的公钥,也就是第一秘钥的公钥进行加密处理后,发送给儿童手表服务器。

[0251] 808:儿童手表服务器进行解密处理后,将确认结果发送给儿童手表。

[0252] 儿童手表服务器根据第一秘钥的私钥进行解密处理后,获取确认结果。

[0253] 如果该确认结果为该手机是儿童手表的管理员设备,则执行步骤809;如果该确认结果为该手机不是儿童手表的管理员设备,则结束任务。

[0254] 809:儿童手表向儿童手表服务器发送解除绑定请求信息。

[0255] 810:儿童手表服务器发送手机UID给儿童手表。

[0256] 进一步的,儿童手表服务器将该手机UID、绑定时间信息等信息根据第二秘钥的公钥进行加密处理后,发送给儿童手表。

[0257] 811:儿童手表将绑定关系删除。

[0258] 具体的可以为,儿童手表控制TEE系统根据第二秘钥的私钥,对上述信息进行加密处理后,获取该手机的UID。儿童手表控制TEE系统将该手机UID对应的绑定关系相关的信息进行删除。

[0259] 812:儿童手表向儿童手表服务器返回响应消息。

[0260] 也就是儿童手表向儿童手表服务器反馈成功将账号绑定信息从儿童手机的TEE系统删除的返回信息。

[0261] 813:儿童手表服务器向手机发送解除绑定结果。

[0262] 儿童手表服务器接收该绑定关系结果,并更新儿童手表服务器上存储的绑定关系列表的相关信息。

[0263] 814:儿童手表服务器向儿童手表发送通知消息。

[0264] 儿童手表服务器向儿童手表发送通知消息,用于指示已更新儿童手表绑定关系,儿童手表可以查询并获取更新的绑定关系。儿童手表向儿童手表服务器查询最新的绑定关系,可以通过儿童手表上的APP界面显示最新的绑定关系列表。

[0265] 进一步的，手机可以重复多次地向儿童手表服务器请求查询解除绑定的结果，儿童手表服务器判断解除绑定操作已完成，则返回解除绑定结果，则手机可以通过儿童手表APP展示已解除相关设备的显示界面。

[0266] 在上述可能的实现方式中，手机向儿童手表请求解除绑定操作，需要先通过儿童手表上的TEE系统，确认该手机是否是为合法的管理员设备，通过TEE系统的加密保证验证过程的安全性，在确认手机是管理员设备后，再进行相应的解除绑定的具体操作，从而不会对管理设备造成错误解绑，保证用户信息的安全性。

[0267] 本申请另一些实施例提供了一种电子设备，该电子设备可以包括：存储器和一个或多个处理器，该存储器和处理器耦合。该存储器用于存储计算机程序代码，该计算机程序代码包括计算机指令。当处理器执行计算机指令时，电子设备可执行上述方法实施例中儿童手表执行的各个功能或者步骤。该电子设备的结构可以参考图1所示的电子设备100的结构。

[0268] 本申请另一些实施例提供一种通信装置，其特征在于，该通信装置可以应用于上述电子设备。该装置用于执行上述方法实施例中SE安全芯片执行的各个功能或者步骤。

[0269] 本申请实施例还提供一种芯片系统，如图9所示，该芯片系统包括至少一个处理器901和至少一个接口电路902。处理器901和接口电路902可通过线路互联。例如，接口电路902可用于从其它装置(例如电子设备的存储器)接收信号。又例如，接口电路902可用于向其它装置(例如处理器901)发送信号。示例性的，接口电路902可读取存储器中存储的指令，并将该指令发送给处理器901。当所述指令被处理器901执行时，可使得电子设备执行上述实施例中儿童手表执行的各个步骤。当然，该芯片系统还可以包含其他分立器件，本申请实施例对此不作具体限定。

[0270] 本申请实施例还提供一种计算机存储介质，该计算机存储介质包括计算机指令，当所述计算机指令在上述电子设备上运行时，使得该电子设备执行上述方法实施例中儿童手表执行的各个功能或者步骤。

[0271] 本申请实施例还提供一种计算机程序产品，当所述计算机程序产品在计算机上运行时，使得所述计算机执行上述方法实施例中儿童手表执行的各个功能或者步骤。

[0272] 通过以上实施方式的描述，所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。

[0273] 在本申请所提供的几个实施例中，应该理解到，所揭露的装置和方法，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，所述模块或单元的划分，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装置，或一些特征可以忽略，或不执行。另一点，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，可以是电性，机械或其它的形式。

[0274] 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一个物理单元或多个物理单元，即可以位于一个地方，或者也可以分布到多个不同地方。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实施例方案的

目的。

[0275] 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。

[0276] 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,可以存储在一个可读取存储介质中。基于这样的理解,本申请实施例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个设备(可以是单片机,芯片等)或处理器(processor)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。

[0277] 以上内容,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,任何在本申请揭露的技术范围内的变化或替换,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所述权利要求的保护范围为准。


电子设备100
天线1
天线2
移动通信模块
2G/3G/4G/5G
[150]
无线通信模块
BT/WLAN/GNSS/NFC/IR/FM
[160]
扬声器
[170A]
受话器
[170B]
麦克风
[170C]
耳机接口
[170D]
音频
模块
[170]
显示屏1~N[194]
摄像头1~N[193]
指示器[192]
马达[191]
按键[190]
内部存储器[121]
SIM卡接口1~N
[195]
外部存储器接口
[120]
处理器
[110]
传感器模块[180]
压力传感器[180A]
陀螺仪传感器[180B]
气压传感器[180C]
磁传感器[180D]
加速度传感器[180E]
距离传感器[180F]
接近光传感器[180G]
指纹传感器[180H]
温度传感器[180J]
触摸传感器[180K]
环境光传感器[180L]
骨传导传感器[180M]
USB接口[130]
充电
管理
模块
[140]
电源管理
模块[141]
电池[142]
SE
安全
芯片
[111]
充电输入

图1

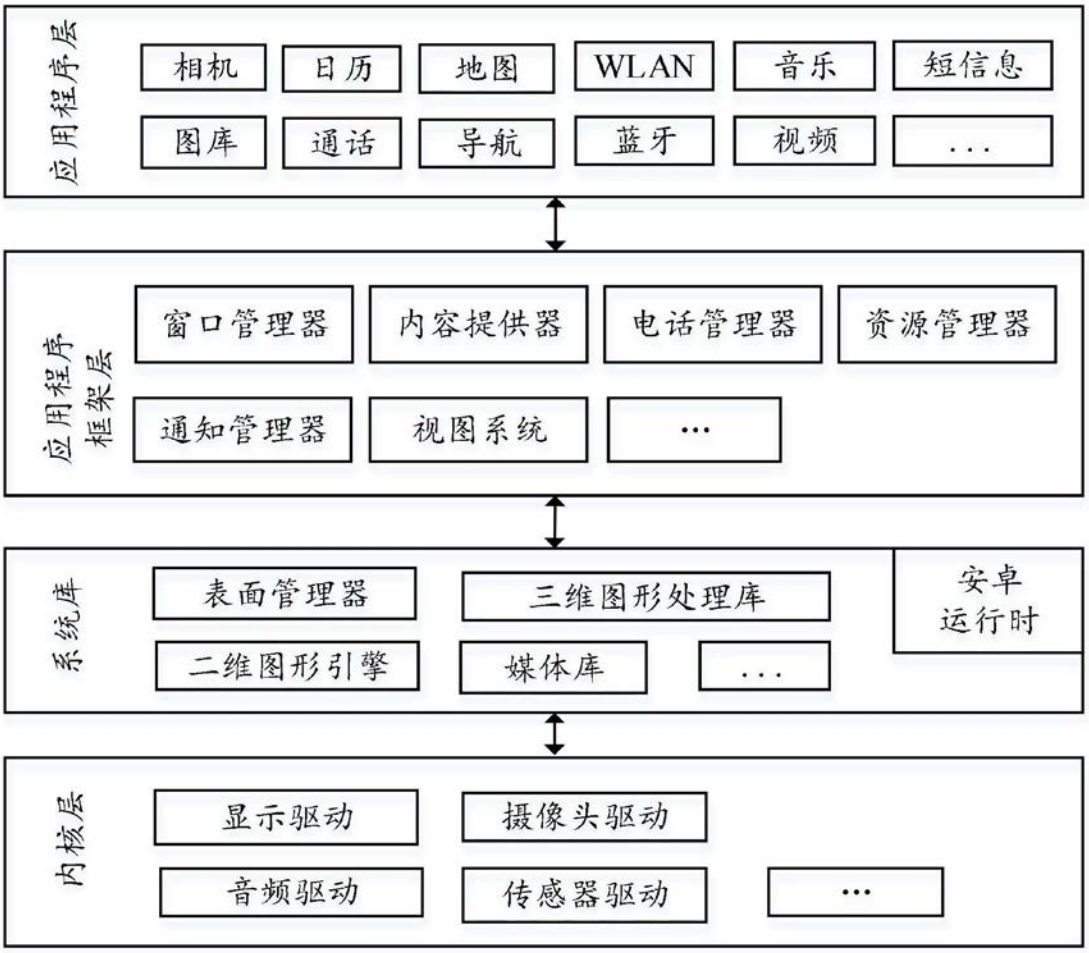

应用程序层
相机
日历
地图
WLAN
音乐
短信息
图库
通话
导航
蓝牙
视频
...
应用程序框架层
窗口管理器
内容提供器
电话管理器
资源管理器
通知管理器
视图系统
...
系统库
表面管理器
三维图形处理库
安卓运行时
二维图形引擎
媒体库
...
内核层
显示驱动
摄像头驱动
音频驱动
传感器驱动
...

图2

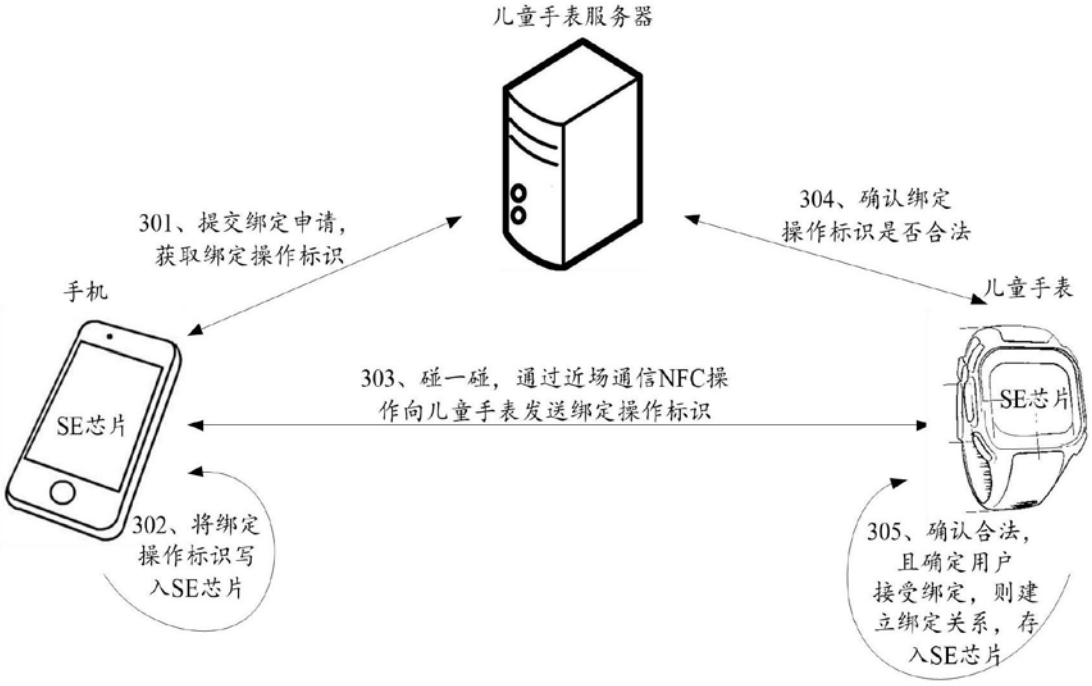

儿童手表服务器
301、提交绑定申请，
获取绑定操作标识
304、确认绑定
操作标识是否合法
手机
儿童手表
SE芯片
303、碰一碰，通过近场通信NFC操
作向儿童手表发送绑定操作标识
SE芯片
302、将绑定
操作标识写
入SE芯片
305、确认合法，
且确定用户
接受绑定，则建
立绑定关系，存
入SE芯片

图3A


中国移动
08:08
儿童手表绑定设置
● 请求绑定
靠近儿童手表感应区，
碰一碰进行绑定
进入
关闭
如果已收到主管理员邀请，请点击
阅读绑定指南

图3B


是否同意授权
xx用户管理?
同意
拒绝

图3C

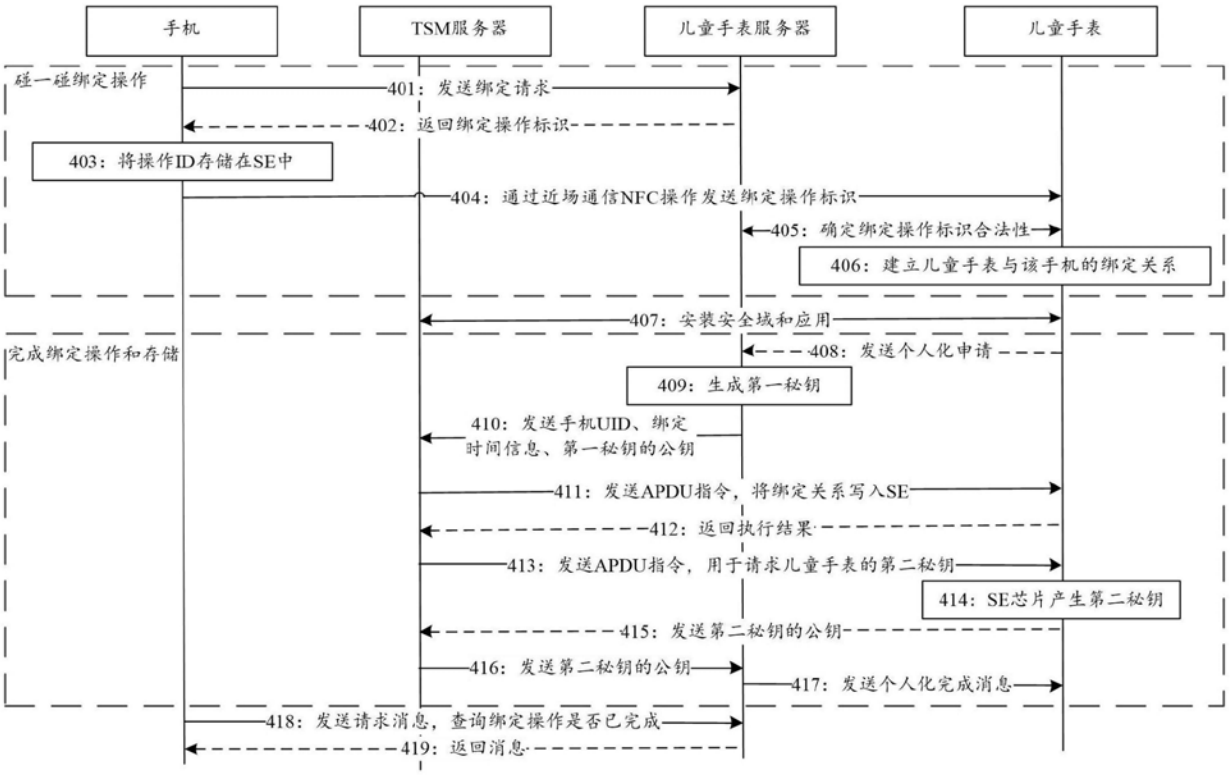

手机
TSM服务器
儿童手表服务器
儿童手表
碰一碰绑定操作
401：发送绑定请求
402：返回绑定操作标识
403：将操作ID存储在SE中
404：通过近场通信NFC操作发送绑定操作标识
405：确定绑定操作标识合法性
406：建立儿童手表与该手机的绑定关系
407：安装安全域和应用
完成绑定操作和存储
408：发送个人化申请
409：生成第一秘钥
410：发送手机UID、绑定时间信息、第一秘钥的公钥
411：发送APDU指令，将绑定关系写入SE
412：返回执行结果
413：发送APDU指令，用于请求儿童手表的第二秘钥
414：SE芯片产生第二秘钥
415：发送第二秘钥的公钥
416：发送第二秘钥的公钥
417：发送个人化完成消息
418：发送请求消息，查询绑定操作是否已完成
419：返回消息

图4

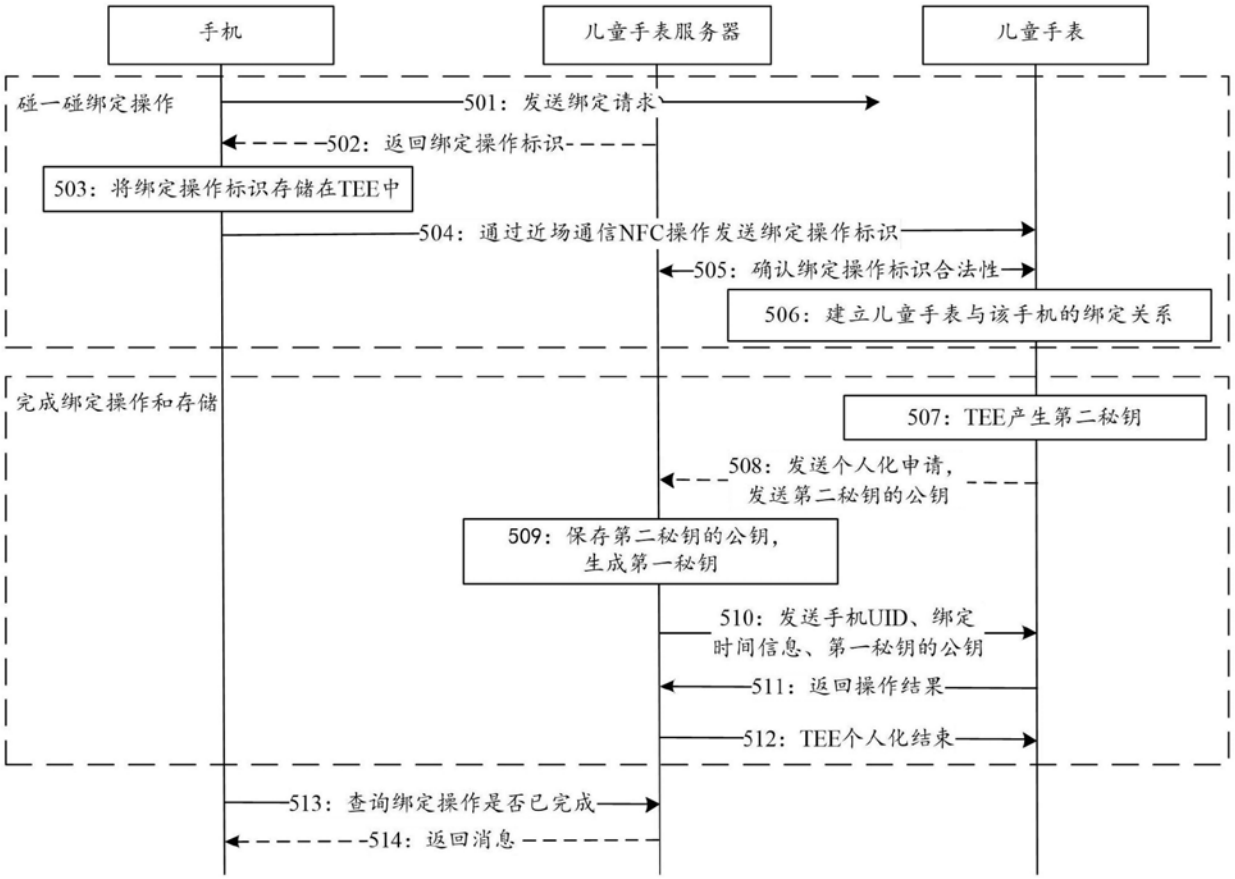

手机
儿童手表服务器
儿童手表
碰一碰绑定操作
501：发送绑定请求
502：返回绑定操作标识
503：将绑定操作标识存储在TEE中
504：通过近场通信NFC操作发送绑定操作标识
505：确认绑定操作标识合法性
506：建立儿童手表与该手机的绑定关系
完成绑定操作和存储
507：TEE产生第二秘钥
508：发送个人化申请，发送第二秘钥的公钥
509：保存第二秘钥的公钥，生成第一秘钥
510：发送手机UID、绑定时间信息、第一秘钥的公钥
511：返回操作结果
512：TEE个人化结束
513：查询绑定操作是否已完成
514：返回消息

图5

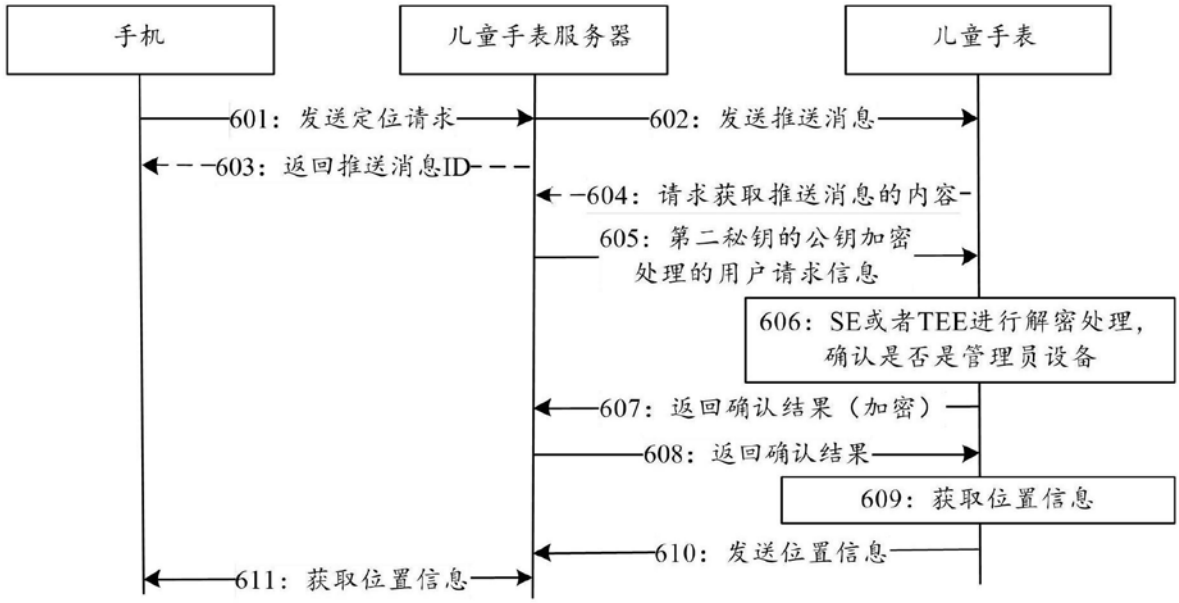

手机
儿童手表服务器
儿童手表
601：发送定位请求
602：发送推送消息
603：返回推送消息ID
604：请求获取推送消息的内容
605：第二秘钥的公钥加密处理的用户请求信息
606：SE或者TEE进行解密处理，确认是否是管理员设备
607：返回确认结果（加密）
608：返回确认结果
609：获取位置信息
610：发送位置信息
611：获取位置信息

图6

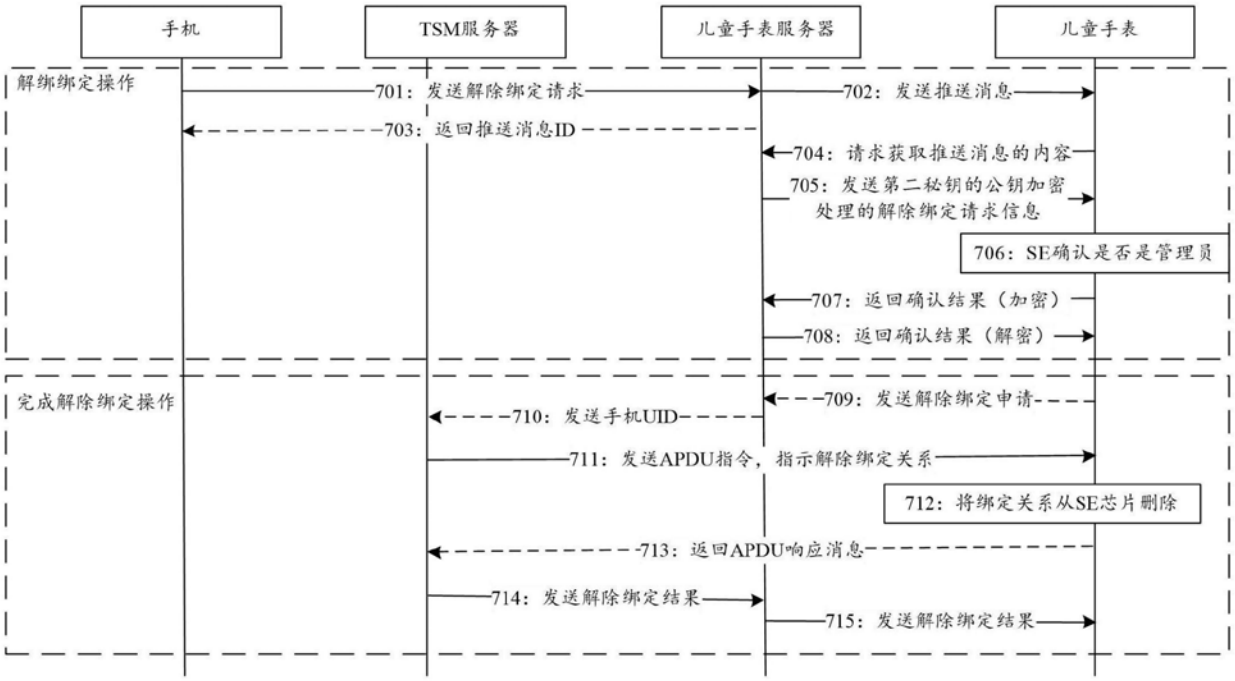

手机
TSM服务器
儿童手表服务器
儿童手表
解绑绑定操作
701：发送解除绑定请求
702：发送推送消息
703：返回推送消息ID
704：请求获取推送消息的内容
705：发送第二秘钥的公钥加密处理的解除绑定请求信息
706：SE确认是否是管理员
707：返回确认结果（加密）
708：返回确认结果（解密）
完成解除绑定操作
709：发送解除绑定申请
710：发送手机UID
711：发送APDU指令，指示解除绑定关系
712：将绑定关系从SE芯片删除
713：返回APDU响应消息
714：发送解除绑定结果
715：发送解除绑定结果

图7

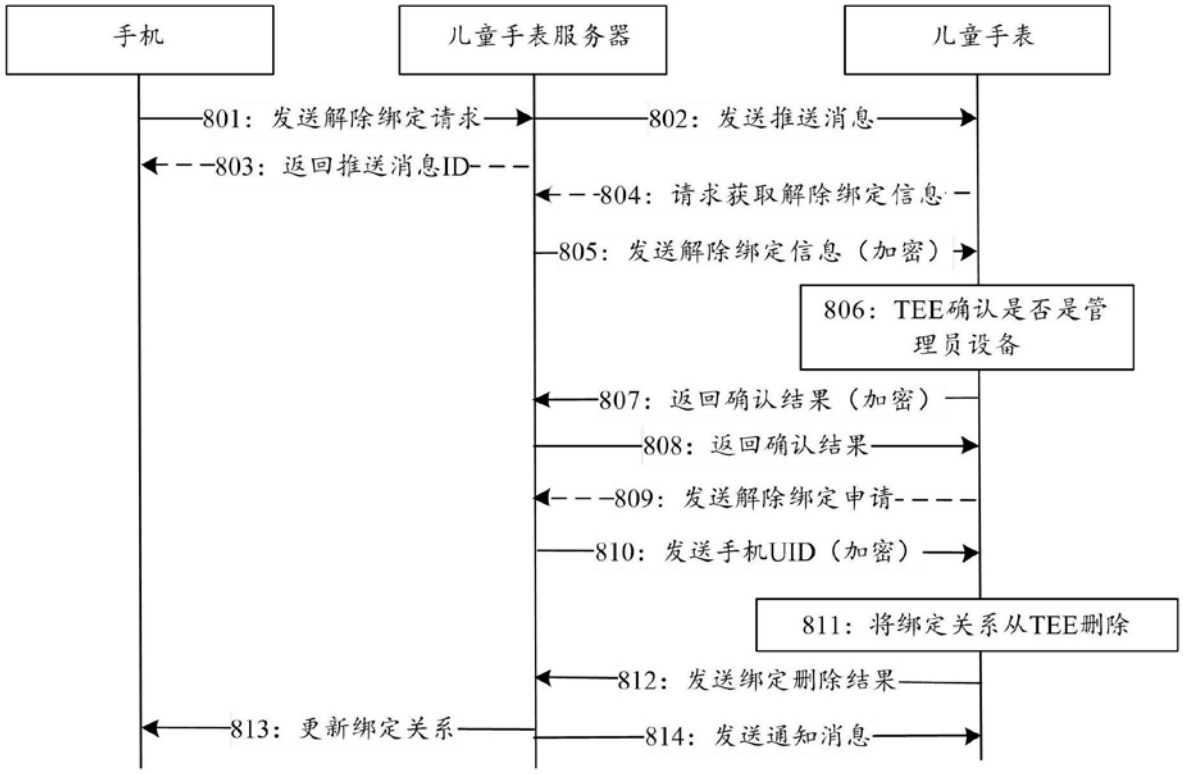

手机
儿童手表服务器
儿童手表
801：发送解除绑定请求
802：发送推送消息
803：返回推送消息ID
804：请求获取解除绑定信息
805：发送解除绑定信息（加密）
806：TEE确认是否是管理员设备
807：返回确认结果（加密）
808：返回确认结果
809：发送解除绑定申请
810：发送手机UID（加密）
811：将绑定关系从TEE删除
812：发送绑定删除结果
813：更新绑定关系
814：发送通知消息

图8

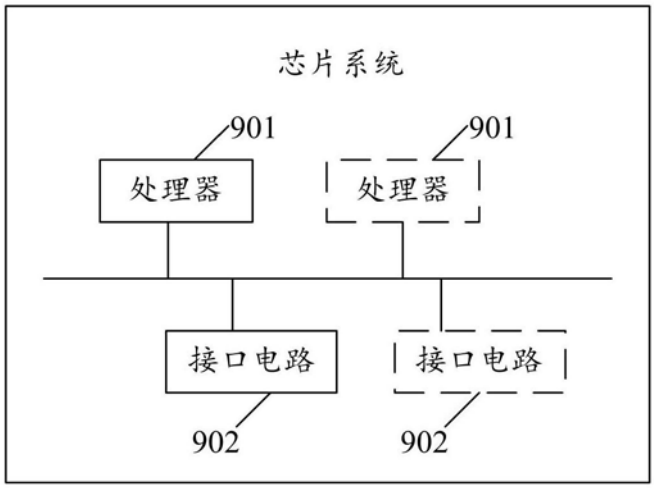


图9