(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 111444528 A
(43)申请公布日 2020.07.24

(21)申请号 202010246323.4

(22)申请日 2020.03.31

(71)申请人 海信视像科技股份有限公司
地址 266555 山东省青岛市经济技术开发区前湾港路218号

(72)发明人 王双优 姜超 初德进

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 贾敏

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/57(2013.01)
G06F 21/64(2013.01)

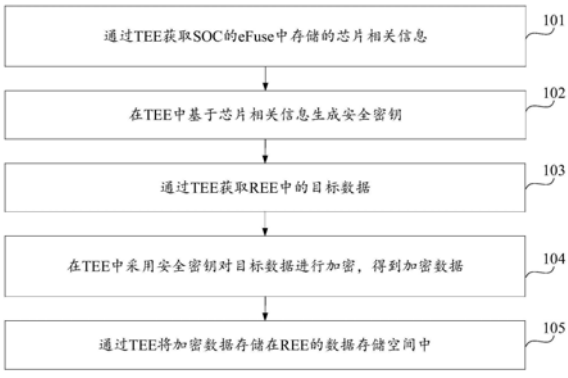
权利要求书2页 说明书13页 附图6页

(54)发明名称

数据安全保护方法、装置及存储介质

(57)摘要

本申请公开了一种数据安全保护方法、装置及存储介质，属于数据安全领域。所述方法包括：通过TEE获取SOC的eFuse中存储的芯片相关信息；在TEE中基于芯片相关信息生成安全密钥；通过TEE获取REE中的目标数据；在TEE中采用安全密钥对目标数据进行加密，得到加密数据；通过TEE将加密数据存储在REE的数据存储空间中。由于每个设备的SOC的eFuse存储信息都是独一无二的，且eFuse存储信息只有在TEE中可以读取，TEE从软件和硬件上对读写操作进行了保护，攻击者无法获取eFuse信息和安全密钥，因此也就无法对REE的加密数据进行解密，从而保护了数据安全，避免了数据被窃取或篡改。



CN 111444528 A

1.一种数据安全保护方法,其特征在于,所述方法包括:

通过可信执行环境TEE获取系统级芯片SOC的eFuse中存储的芯片相关信息;

在所述TEE中基于所述芯片相关信息生成安全密钥;

通过所述TEE获取富执行环境REE中的目标数据;

在所述TEE中采用所述安全密钥对所述目标数据进行加密,得到加密数据;

通过所述TEE将所述加密数据存储在所述REE的数据存储空间中。

2.根据权利要求1所述的方法,其特征在于,所述在所述TEE中基于所述芯片相关信息生成安全密钥,包括:

在所述TEE中,采用对称性密钥生成算法对所述芯片相关信息进行处理,得到所述安全密钥。

3.根据权利要求2所述的方法,其特征在于,所述在所述TEE中,采用对称性密钥生成算法对所述芯片相关信息进行处理,得到所述安全密钥,包括:

在所述TEE中,采用对称性密钥生成算法对所述芯片相关信息和预设信息进行处理,得到所述安全密钥;

其中,所述预设信息包括预设字符串、所述SOC的芯片标识或者所述数据存储空间的芯片标识。

4.根据权利要求2或3所述的方法,其特征在于,所述通过所述TEE将所述加密数据存储在所述REE的数据存储空间中之后,还包括:

通过所述TEE获取所述REE中的所述加密数据;

在所述TEE中采用所述安全密钥对所述加密数据进行解密,得到所述目标数据。

5.根据权利要求1所述的方法,其特征在于,所述在所述TEE中基于所述芯片相关信息生成安全密钥,包括:

在所述TEE中,采用非对称性密钥生成算法对所述芯片相关信息进行处理,生成一对私钥和公钥;

通过所述TEE将所述公钥存储在所述数据存储空间中的指定分区中,所述指定分区是指具有安全特性的分区;

所述在所述TEE中采用所述安全密钥对所述目标数据进行加密,得到加密数据,包括:

在所述TEE中,采用预设摘要提取算法提取所述目标数据的摘要,得到第一摘要;

在所述TEE中,采用所述私钥对所述第一摘要进行加密,得到签名信息;

将所述目标数据和所述签名信息,确定为所述加密数据。

6.根据权利要求5所述的方法,其特征在于,所述在所述TEE中,采用非对称性密钥生成算法对所述芯片相关信息进行处理,生成一对私钥和公钥,包括:

在所述TEE中,采用非对称性密钥生成算法对所述芯片相关信息和预设信息进行处理,生成所述私钥和公钥;

其中,所述预设信息包括预设字符串、所述SOC的芯片标识或者所述数据存储空间的芯片标识。

7.根据权利要求5或6所述的方法,其特征在于,所述通过所述TEE将所述加密数据存储在所述REE的数据存储空间中之后,还包括:

通过所述REE获取所述数据存储空间中的加密数据;

通过所述REE从所述数据存储空间中的指定分区中获取所述公钥；

在所述REE中，采用所述公钥对所述加密数据中的数据进行安全校验。

8.根据权利要求7所述的方法，其特征在于，所述采用所述公钥对所述加密数据中的数据进行安全校验，包括：

采用所述公钥对所述加密数据中的签名信息进行解密，得到所述第一摘要；

采用所述预设摘要提取算法提取所述加密数据中数据的摘要，得到第二摘要；

若所述第一摘要与所述第二摘要相同，则确定所述加密数据中的数据通过安全校验。

9.一种数据安全保护装置，其特征在于，所述装置包括：

处理器；

用于存储处理器可执行指令及数据的存储器；

其中，所述处理器被配置为执行权利要求1-8所述的任一项方法的步骤。

10.一种计算机可读存储介质，所述计算机可读存储介质上存储有指令，其特征在于，所述指令被处理器执行时实现权利要求1-8所述的任一项方法的步骤。

数据安全保护方法、装置及存储介质

技术领域

[0001] 本申请涉及数据安全领域，特别涉及一种数据安全保护方法、装置及存储介质。

背景技术

[0002] 设备的CPU(Central Processing Unit，中央处理器)在运行时，CPU的执行环境一般分为REE(Rich Execution Environment，富执行环境)和TEE(Trust Execution Environment，可信执行环境)。其中，REE和TEE在物理上是隔离的，REE和TEE各自运行独立的软件。REE一般用于运行Linux或Android等操作系统软件。TEE一般用于执行安全性要求相对较高的行为，如指纹识别或支付等。而且，REE和TEE可以共享内存，TEE可以访问REE的内存，但REE不能访问TEE的私有内存。

[0003] 由于TEE的执行环境安全性较高，因此TEE中的数据不易被窃取或篡改，但是REE的执行环境安全性相对较低，因此，为了保护REE的数据安全，防止数据被窃取或篡改，需要对REE的数据安全进行保护。

发明内容

[0004] 本申请实施例提供了一种数据安全保护方法、装置及存储介质，可以用于解决相关技术中存在的数据安全较低的问题。所述技术方案如下：

[0005] 一方面，提供了一种数据安全保护方法，所述方法包括：

[0006] 通过可信执行环境TEE获取系统级芯片SOC的eFuse中存储的芯片相关信息；

[0007] 在所述TEE中基于所述芯片相关信息生成安全密钥；

[0008] 通过所述TEE获取富执行环境REE中的目标数据；

[0009] 在所述TEE中采用所述安全密钥对所述目标数据进行加密，得到加密数据；

[0010] 通过所述TEE将所述加密数据存储在所述REE的数据存储空间中。

[0011] 可选地，所述在所述TEE中基于所述芯片相关信息生成安全密钥，包括：

[0012] 在所述TEE中，采用对称性密钥生成算法对所述芯片相关信息进行处理，得到所述安全密钥。

[0013] 可选地，所述在所述TEE中，采用对称性密钥生成算法对所述芯片相关信息进行处理，得到所述安全密钥，包括：

[0014] 在所述TEE中，采用对称性密钥生成算法对所述芯片相关信息和预设信息进行处理，得到所述安全密钥；

[0015] 其中，所述预设信息包括预设字符串、所述SOC的芯片标识或者所述数据存储空间的芯片标识。

[0016] 可选地，所述通过所述TEE将所述加密数据存储在所述REE的数据存储空间中之后，还包括：

[0017] 通过所述TEE获取所述REE中的所述加密数据；

[0018] 在所述TEE中采用所述安全密钥对所述加密数据进行解密，得到所述目标数据。

[0019] 可选地，所述在所述TEE中基于所述芯片相关信息生成安全密钥，包括：

[0020] 在所述TEE中，采用非对称性密钥生成算法对所述芯片相关信息进行处理，生成一对私钥和公钥；

[0021] 通过所述TEE将所述公钥存储在所述数据存储空间中的指定分区中，所述指定分区是指具有安全特性的分区；

[0022] 所述在所述TEE中采用所述安全密钥对所述目标数据进行加密，得到加密数据，包括：

[0023] 在所述TEE中，采用预设摘要算法提取所述目标数据的摘要，得到第一摘要；

[0024] 在所述TEE中，采用所述私钥对所述第一摘要进行加密，得到签名信息；

[0025] 将所述目标数据和所述签名信息，确定为所述加密数据。

[0026] 可选地，所述在所述TEE中，采用非对称性密钥生成算法对所述芯片相关信息进行处理，生成一对私钥和公钥，包括：

[0027] 在所述TEE中，采用非对称性密钥生成算法对所述芯片相关信息和预设信息进行处理，生成所述私钥和公钥；

[0028] 其中，所述预设信息包括预设字符串、所述SOC的芯片标识或者所述数据存储空间的芯片标识。

[0029] 可选地，所述通过所述TEE将所述加密数据存储在所述REE的数据存储空间中之后，还包括：

[0030] 通过所述REE获取所述数据存储空间中的加密数据；

[0031] 通过所述REE从所述数据存储空间中的指定分区中获取所述公钥；

[0032] 在所述REE中，采用所述公钥对所述加密数据中的数据进行安全校验。

[0033] 可选地，所述采用所述公钥对所述加密数据中的数据进行安全校验，包括：

[0034] 采用所述公钥对所述加密数据中的签名信息进行解密，得到所述第一摘要；

[0035] 在所述REE中，采用所述预设摘要算法提取所述加密数据中数据的摘要，得到第二摘要；

[0036] 若所述第一摘要与所述第二摘要相同，则确定所述加密数据中的数据通过安全校验。

[0037] 另一方面，提供了一种数据安全保护装置，所述装置包括：

[0038] 第一获取模块，用于通过可信执行环境TEE读取系统级芯片SOC的eFuse中存储的芯片相关信息；

[0039] 生成模块，用于在所述TEE中基于所述芯片相关信息生成安全密钥；

[0040] 第二获取模块，用于通过所述TEE获取富执行环境REE中的目标数据；

[0041] 加密模块，用于在所述TEE中采用所述安全密钥对所述目标数据进行加密，得到加密数据；

[0042] 存储模块，用于通过所述TEE将所述加密数据存储在所述REE的数据存储空间中。

[0043] 可选地，所述生成模块用于：

[0044] 在所述TEE中，采用对称性密钥生成算法对所述芯片相关信息进行处理，得到所述安全密钥。

[0045] 可选地，所述生成模块用于：

[0046] 在所述TEE中，采用对称性密钥生成算法对所述芯片相关信息和预设信息进行处理，得到所述安全密钥；

[0047] 其中，所述预设信息包括预设字符串、所述SOC的芯片标识或者所述数据存储空间的芯片标识。

[0048] 可选地，所述装置还包括：

[0049] 第三获取模块，用于通过所述TEE获取所述REE中的所述加密数据；

[0050] 第一解密模块，用于在所述TEE中采用所述安全密钥对所述加密数据进行解密，得到所述目标数据。

[0051] 可选地，所述生成模块用于：

[0052] 在所述TEE中，采用非对称性密钥生成算法对所述芯片相关信息进行处理，生成一对私钥和公钥；

[0053] 通过所述TEE将所述公钥存储在所述数据存储空间中的指定分区中，所述指定分区是指具有安全特性的分区；

[0054] 所述加密模块用于：

[0055] 在所述TEE中，采用预设摘要算法提取所述目标数据的摘要，得到第一摘要；

[0056] 在所述TEE中，采用所述私钥对所述第一摘要进行加密，得到签名信息；

[0057] 将所述目标数据和所述签名信息，确定为所述加密数据。

[0058] 可选地，所述生成模块用于：

[0059] 在所述TEE中，采用非对称性密钥生成算法对所述芯片相关信息和预设信息进行处理，生成所述私钥和公钥；

[0060] 其中，所述预设信息包括预设字符串、所述SOC的芯片标识或者所述数据存储空间的芯片标识。

[0061] 可选地，所述装置还包括：

[0062] 第四获取模块，用于通过所述REE获取所述数据存储空间中的加密数据；

[0063] 第五获取模块，用于通过所述REE从所述数据存储空间中的指定分区中获取所述公钥；

[0064] 校验模块，用于在所述REE中，采用所述公钥对所述加密数据中的数据进行安全校验。

[0065] 可选地，所述校验模块用于：

[0066] 采用所述公钥对所述加密数据中的签名信息进行解密，得到所述第一摘要；

[0067] 在所述REE中，采用所述预设摘要算法提取所述加密数据中数据的摘要，得到第二摘要；

[0068] 若所述第一摘要与所述第二摘要相同，则确定所述加密数据中的数据通过安全校验。

[0069] 另一方面，提供了一种数据安全保护装置，所述装置包括：

[0070] 处理器；

[0071] 用于存储处理器可执行指令的存储器；

[0072] 其中，所述处理器被配置为执行上述任一种数据安全保护方法的步骤。

[0073] 另一方面，提供了一种计算机可读存储介质，所述计算机可读存储介质上存储有

指令,所述指令被处理器执行时实现上述任一种数据安全保护方法的步骤。

[0074] 另一方面,提供了一种计算机程序产品,当所述计算机程序产品被执行时,用于实现上述任一种数据安全保护方法的步骤。

[0075] 本申请实施例提供的技术方案带来的有益效果是:

[0076] 本申请实施例中,可以在TEE中基于系统级芯片SOC的eFuse中存储的芯片相关信息生成安全密钥,并使用安全密钥对REE中的数据进行加密,以对REE中的数据进行安全保护。由于每个设备的SOC的eFuse存储信息都是独一无二的,且eFuse存储信息只有在TEE中可以读取,TEE从软件和硬件上对读写操作进行了保护,攻击者无法获取eFuse信息和安全密钥,因此也就无法对REE的加密数据进行解密,从而保护了数据安全,避免了数据被窃取或篡改。

附图说明

[0077] 为了更清楚地说明本申请实施例中的技术方案,下面将对实施例描述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。

[0078] 图1是本申请实施例提供的一种数据安全保护方法的流程图;

[0079] 图2是本申请实施例提供的一种安全密钥生成过程示意图;

[0080] 图3是本申请实施例提供的另一种安全密钥生成过程示意图;

[0081] 图4是本申请实施例提供的一种数据加密过程示意图;

[0082] 图5是本申请实施例提供的另一种数据加密过程示意图;

[0083] 图6是本申请实施例提供的一种数据解密过程示意图;

[0084] 图7是本申请实施例提供的一种数据安全校验过程示意图;

[0085] 图8是本申请实施例提供的一种数据安全保护装置的框图;

[0086] 图9是本申请实施例提供的一种终端900的结构框图。

具体实施方式

[0087] 为使本申请的目的、技术方案和优点更加清楚,下面将结合附图对本申请实施方式作进一步地详细描述。

[0088] 在对本申请实施例进行详细地解释说明之前,先对本申请实施例涉及的名词进行解释。

[0089] REE:CPU的富执行环境,一般用于运行Linux或Android等操作系统软件,或者其他常规任务。

[0090] TEE:CPU的可信执行环境,用于执行安全性要求相对较高的行为,如指纹识别或支付等。

[0091] SOC(System on Chip,系统级芯片):也称片上芯片,是一个有专用目标的集成电路,其中包含完整系统并有嵌入软件的全部内容。

[0092] eFuse:是一种重要的非易失性存储单元,由熔丝结构构成,通过熔丝可以在芯片上编程并存储信息。eFuse通常为一次性可编程存储器。CPU可以使用eFuse存储芯片相关信

息。

[0093] eMMC(Embedded Multi Media Card,嵌入式多媒体存储卡):用于存储文件等,存储内容断电可保存。

[0094] RPMB(Replay Protected Memory Block,重放保护存储块):eMMC中一个具有安全特性的分区。写入数据到RPMB时,需要校验数据的合法性,只有指定的Host(执行主体,如TEE)才能够写入。读数据时,也提供了签名机制,保证Host读取到的数据是RPMB内部数据,而不是攻击者伪造的数据。

[0095] 接下来对本申请实施例的实施环境进行简单介绍。

[0096] 本申请实施例提供的方法用于保护数据安全。作为一个示例,本申请可以对用户使用过程中生成的隐私数据进行安全保护,如对用户账户密码、支付信息或系统快照等隐私数据进行安全保护。

[0097] 数据安全的需求主要有防窃取和防篡改。防窃取需要对完整的数据进行加密,防篡改可以对数据提取摘要后,只对摘要进行加密,验证解密后的摘要与读取数据的摘要是否一致即可确认数据是否可用。本申请中,利用eFuse生成的安全密钥在对称性加密方案和非对称性加密方案中均适用,且对称性加密方案和非对称性加密方案均可实现防窃取和防篡改。比如,可以通过对称性加密方案实现数据的防窃取,通过非对称性加密方案实现数据的放篡改。

[0098] 接下来对本申请实施例提供的数据安全保护方法进行详细介绍。

[0099] 图1是本申请实施例提供的一种数据安全保护方法的流程图,该方法应用于电子设备中,电子设备可以为终端或服务器等,终端可以为手机、平板电脑或计算机等。如图1所示,该方法包括如下步骤:

[0100] 步骤101:通过TEE获取SOC的eFuse中存储的芯片相关信息。

[0101] 也即是,在TEE中读取SOC的eFuse中存储的芯片相关信息。

[0102] 其中,eFuse是一种重要的非易失性存储单元,由熔丝结构构成,通过熔丝可以在芯片上编程并存储信息。eFuse通常为一次性可编程存储器。CPU可以使用eFuse存储芯片相关信息。

[0103] 需要说明的而是,每个设备的SOC的eFuse存储信息都是独一无二的,且eFuse存储信息只有在TEE中才可以读取,因此,只能通过TEE读取eFuse中存储的芯片相关信息。

[0104] 步骤102:在TEE中基于芯片相关信息生成安全密钥。

[0105] 作为一个示例,在TEE中基于芯片相关信息生成安全密钥可以应用于对称性加密场景中,也可以应用于非对称加密场景中,根据应用场景的不同,生成安全密钥的过程包括以下两种实现方式:

[0106] 1)对称性加密场景:在TEE中,采用对称性密钥生成算法对芯片相关信息进行处理,得到安全密钥。

[0107] 其中,该安全密钥为对称性加密所使用的安全密钥。对称性加密方案中,加密过程和解密过程使用相同的安全密钥。

[0108] 作为一个示例,对称性密钥生成算法可以为HMAC(Hash-based Message Authentication Code,哈希消息认证码)或MD5(Message Digest Algorithm MD5,第五版摘要提取算法)等。

[0109] 作为另一示例,还可以基于芯片相关信息和预设信息生成安全密钥。比如,在TEE中,采用对称性密钥生成算法对芯片相关信息和预设信息进行处理,得到安全密钥。

[0110] 其中,该预设信息为轻易不会改变的数据。比如,可以为预设字符串、SOC的芯片标识或者REE的数据存储空间的芯片标识等。

[0111] 其中,SOC的芯片标识可以为SOC的芯片ID(Identity Document,身份标识)等。数据存储空间的芯片标识可以为数据存储空间的芯片ID。该数据存储空间可以为eMMC、UFS(Universal Flash Storage,通用闪存存储)或SD(Secure Digital Memory Card,安全数码卡)等。

[0112] 请参考图2,在TEE中,可以获取eFuse中存储的芯片相关信息,然后基于芯片相关信息,或者芯片相关信息和预设信息生成安全密钥。

[0113] 2)非对称性加密场景:在TEE中,采用非对称性密钥生成算法对芯片相关信息进行处理,生成一对私钥和公钥。

[0114] 其中,该私钥和公钥为非对称性加密所使用的安全密钥。非对称性加密方案中,通常使用私钥进行加密,使用公钥进行解密。

[0115] 作为另一示例,还可以基于芯片相关信息和预设信息生成安全密钥。比如,在TEE中,采用非对称性密钥生成算法对芯片相关信息和预设信息进行处理,得到安全密钥。其中,该预设信息为轻易不会改变的数据,比如,可以为预设字符串、SOC的芯片标识或者REE的数据存储空间的芯片标识等。

[0116] 另外,在生成私钥和公钥之后,还可以通过TEE将公钥存储在REE的数据存储空间中的指定分区中,指定分区是指具有安全特性的分区。

[0117] 通过将公钥保存在具有安全特性的指定分区中,可以保证公钥不会被攻击者轻易读取和篡改,从而保证公钥的安全性。

[0118] 示例的,若该数据存储空间为eMMC,则指定分区可以为eMMC的RPMB。RPMB具有安全特征,写入数据到RPMB时,需要校验数据的合法性,只有指定的Host(执行主体,如TEE)才能够写入。读数据时,也提供了签名机制,保证Host读取到的数据是RPMB内部数据,而不是攻击者伪造的数据。

[0119] 请参考图3,在TEE中,可以获取eFuse中存储的芯片相关信息,基于芯片相关信息,或者芯片相关信息和预设信息生成一对私钥和公钥,然后将公钥写入到eMMC的RPMB分区。

[0120] 步骤103:通过TEE获取REE中的目标数据。

[0121] 由于TEE可以读取REE的内存,因此,可以通过REE读取REE中的数据,作为待加密的目标数据。

[0122] 其中,目标数据可以为安全性要求较高的数据或者用户的隐私数据等,比如,目标数据可以为用户账户密码、支付信息或系统快照等。

[0123] 步骤104:在TEE中采用安全密钥对目标数据进行加密,得到加密数据。

[0124] 根据应用场景的不同,采用安全密钥对目标数据进行加密的过程可以包括以下几种实现方式:

[0125] 1)对称性加密场景:在TEE中采用安全密钥对目标数据进行加密,将加密处理后的目标数据作为加密数据。

[0126] 2)非对称性加密场景:在TEE中,采用预设摘要提取算法提取目标数据的摘要,得

到第一摘要，采用私钥对第一摘要进行加密，得到签名信息，将目标数据和签名信息，确定为加密数据。

[0127] 其中，预设摘要提取算法用于提取目标数据的摘要。示例的，预设摘要提取算法可以为SHA256(哈希长度为256的哈希算法)或MD5等。

[0128] 由于每个SOC芯片的eFuse存储信息都是唯一的，保存到数据存储空间中的数据在另一SOC芯片上是无法被解密的，基于此特性，本申请实现了加密信息与芯片的绑定，即采用SOC芯片的eFuse存储信息生成的安全密钥对数据进行加密，使得使隐私数据不会被其他芯片使用，也无法被随意修改，保护数据安全。

[0129] 步骤105：通过TEE将加密数据存储在REE的数据存储空间中。

[0130] 也即是，通过TEE将加密数据写入到REE的数据存储空间中。该数据存储空间可以为eMMC、UFS或SD等。

[0131] 1)对称性加密场景：将采用安全密钥对目标数据进行加密得到的加密数据，存储在数据存储空间中。

[0132] 请参考图4，TEE可以获取REE的数据，然后使用安全密钥对获取的数据进行加密，得到加密数据，再将加密数据写入到REE中。

[0133] 2)非对称性加密场景：将目标数据和签名信息作为加密数据存储在该数据存储空间中。

[0134] 请参考图5，TEE可以获取REE的数据，然后提取数据的摘要，使用私钥对摘要进行加密，得到签名信息，将目标数据和签名信息作为加密数据写入到REE中。

[0135] 步骤106：获取数据存储空间中的加密数据，对加密数据进行解密或者进行安全校验。

[0136] 1)对称性加密场景：通过TEE获取REE中的加密数据，在TEE中采用安全密钥对所述加密数据进行解密，得到目标数据。

[0137] 也即是，在TEE中获取REE的加密数据，并在TEE中使用安全密钥对加密数据进行解密。

[0138] 通过使用安全密钥对数据进行加密，则在获取到加密数据之后，使用安全密钥对加密数据进行解密才能获取到加密前的原始数据。如此，即使其他设备获取到REE的加密数据，由于没有安全密钥，也无法对加密数据进行解密来获取原始数据，从而减小了数据被窃取的风险，保护了数据安全。

[0139] 请参考图6，TEE可以读取REE的加密数据，然后使用安全密钥对加密数据进行解密，得到加密前的数据。

[0140] 2)非对称性加密场景：通过REE获取数据存储空间中的加密数据，通过REE从数据存储空间的指定分区中获取公钥，在REE中，采用公钥对加密数据中的数据进行安全校验。

[0141] 也即是，在REE中获取加密数据，并从指定分区获取公钥，然后使用公钥对加密数据中的数据进行安全校验，以验证加密数据中的数据是否可用。

[0142] 作为一个示例，采用公钥对加密数据中的数据进行安全校验的操作可以包括：采用公钥对加密数据中的签名信息进行解密，得到第一摘要；采用预设摘要提取算法提取加密数据中数据的摘要，得到第二摘要；若第一摘要与第二摘要相同，则确定加密数据中的数据通过安全校验，即加密数据中的数据可用，未被篡改。另外，若第一摘要与第二摘要不同，

则确定加密数据中的数据未通过安全校验，即加密数据中的数据有可能被篡改，数据是不安全的。

[0143] 由上可知，通过使用非对称性方案进行加密和解密，可以防止数据被篡改，保证数据的安全性。

[0144] 请参考图7，REE可以从eMMC的RPMB分区中读取公钥，然后读取加密数据，该加密数据包括数据和签名信息，之后，使用预设摘要提取算法提取数据的摘要，得到一个摘要，使用公钥对签名信息进行解密，得到另一个摘要，若两个摘要相同，则表示数据通过安全校验，该数据可用。

[0145] 本申请实施例中，数据的安全校验可以完全在REE中实现。在计算安全密钥时，TEE已经将公钥写入到RPMB分区，REE中可以读取此公钥，但是无法对RPMB分区进行修改，所以可以保证公钥不被随意修改。REE读取数据，并对数据计算摘要，再利用公钥对签名信息进行解密得到另一摘要，如果两者一致，数据未被篡改，否则认为数据是不安全的。

[0146] 需要说明的是，本申请实施例仅是以将基于eFuse中存储的芯片相关信息生成的安全密钥应用于上述场景中为例进行说明，而实际应用中，基于eFuse中存储的芯片相关信息生成的安全密钥还可以应用于其他场景中，本申请实施例对此不作限定。

[0147] 本申请实施例中，可以在TEE中基于系统级芯片SOC的eFuse中存储的芯片相关信息生成安全密钥，并使用安全密钥对REE中的数据进行加密，以对REE中的数据进行安全保护。由于每个设备的SOC的eFuse存储信息都是独一无二的，且eFuse存储信息只有在TEE中可以读取，TEE从软件和硬件上对读写操作进行了保护，攻击者无法获取eFuse信息和安全密钥，因此也就无法对REE的加密数据进行解密，从而保护了数据安全，避免了数据被窃取或篡改。

[0148] 图8是本申请实施例提供的一种数据安全保护装置的框图，如图8所示，该装置包括：第一获取模块801、生成模块802、第二获取模块803、加密模块804和存储模块805。

[0149] 第一获取模块801，用于通过可信执行环境TEE读取系统级芯片SOC的eFuse中存储的芯片相关信息；

[0150] 生成模块802，用于在所述TEE中基于所述芯片相关信息生成安全密钥；

[0151] 第二获取模块803，用于通过所述TEE获取富执行环境REE中的目标数据；

[0152] 加密模块804，用于在所述TEE中采用所述安全密钥对所述目标数据进行加密，得到加密数据；

[0153] 存储模块805，用于通过所述TEE将所述加密数据存储在所述REE的数据存储空间中。

[0154] 可选地，所述生成模块802用于：

[0155] 在所述TEE中，采用对称性密钥生成算法对所述芯片相关信息进行处理，得到所述安全密钥。

[0156] 可选地，所述生成模块802用于：

[0157] 在所述TEE中，采用对称性密钥生成算法对所述芯片相关信息和预设信息进行处理，得到所述安全密钥；

[0158] 其中，所述预设信息包括预设字符串、所述SOC的芯片标识或者所述数据存储空间的芯片标识。

[0159] 可选地，所述装置还包括：

[0160] 第三获取模块，用于通过所述TEE获取所述REE中的所述加密数据；

[0161] 第一解密模块，用于在所述TEE中采用所述安全密钥对所述加密数据进行解密，得到所述目标数据。

[0162] 可选地，所述生成模块802用于：

[0163] 在所述TEE中，采用非对称性密钥生成算法对所述芯片相关信息进行处理，生成一对私钥和公钥；

[0164] 通过所述TEE将所述公钥存储在所述数据存储空间中的指定分区中，所述指定分区是指具有安全特性的分区；

[0165] 所述加密模块804用于：

[0166] 在所述TEE中，采用预设摘要算法提取所述目标数据的摘要，得到第一摘要；

[0167] 在所述TEE中，采用所述私钥对所述第一摘要进行加密，得到签名信息；

[0168] 将所述目标数据和所述签名信息，确定为所述加密数据。

[0169] 可选地，所述生成模块802用于：

[0170] 在所述TEE中，采用非对称性密钥生成算法对所述芯片相关信息和预设信息进行处理，生成所述私钥和公钥；

[0171] 其中，所述预设信息包括预设字符串、所述SOC的芯片标识或者所述数据存储空间的芯片标识。

[0172] 可选地，所述装置还包括：

[0173] 第四获取模块，用于通过所述REE获取所述数据存储空间中的加密数据；

[0174] 第五获取模块，用于通过所述REE从所述数据存储空间中的指定分区中获取所述公钥；

[0175] 校验模块，用于在所述REE中，采用所述公钥对所述加密数据中的数据进行安全校验。

[0176] 可选地，所述校验模块用于：

[0177] 采用所述公钥对所述加密数据中的签名信息进行解密，得到所述第一摘要；

[0178] 在所述REE中，采用所述预设摘要算法提取所述加密数据中数据的摘要，得到第二摘要；

[0179] 若所述第一摘要与所述第二摘要相同，则确定所述加密数据中的数据通过安全校验。

[0180] 本申请实施例中，可以在TEE中基于系统级芯片SOC的eFuse中存储的芯片相关信息生成安全密钥，并使用安全密钥对REE中的数据进行加密，以对REE中的数据进行安全保护。由于每个设备的SOC的eFuse存储信息都是独一无二的，且eFuse存储信息只有在TEE中可以读取，TEE从软件和硬件上对读写操作进行了保护，攻击者无法获取eFuse信息和安全密钥，因此也就无法对REE的加密数据进行解密，从而保护了数据安全，避免了数据被窃取或篡改。

[0181] 需要说明的是：上述实施例提供的数据安全保护装置在进行数据安全保护时，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。另外，上述实施例提供的数据安全保护装置与数据安全保护方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0182] 图9是本申请实施例提供的一种终端900的结构框图。该终端900可以是：智能手机、平板电脑、MP3播放器(Moving Picture Experts Group Audio Layer III，动态影像专家压缩标准音频层面3)、MP4(Moving Picture Experts Group Audio Layer IV，动态影像专家压缩标准音频层面4)播放器、笔记本电脑或台式电脑。终端900还可能被称为用户设备、便携式终端、膝上型终端、台式终端等其他名称。

[0183] 通常，终端900包括有：处理器901和存储器902。

[0184] 处理器901可以包括一个或多个处理核心，比如4核心处理器、8核心处理器等。处理器901可以采用DSP(Digital Signal Processing，数字信号处理)、FPGA(Field－Programmable Gate Array，现场可编程门阵列)、PLA(Programmable Logic Array，可编程逻辑阵列)中的至少一种硬件形式来实现。处理器901也可以包括主处理器和协处理器，主处理器是用于对在唤醒状态下的数据进行处理的处理器，也称CPU(Central Processing Unit，中央处理器)；协处理器是用于对在待机状态下的数据进行处理的低功耗处理器。在一些实施例中，处理器901可以在集成有GPU(Graphics Processing Unit，图像处理器)，GPU用于负责显示屏所需要显示的内容的渲染和绘制。一些实施例中，处理器901还可以包括AI(Artificial Intelligence，人工智能)处理器，该AI处理器用于处理有关机器学习的计算操作。

[0185] 存储器902可以包括一个或多个计算机可读存储介质，该计算机可读存储介质可以是非暂态的。存储器902还可包括高速随机存取存储器，以及非易失性存储器，比如一个或多个磁盘存储设备、闪存存储设备。在一些实施例中，存储器902中的非暂态的计算机可读存储介质用于存储至少一个指令，该至少一个指令用于被处理器901所执行以实现本申请中方法实施例提供的数据安全保护方法。

[0186] 在一些实施例中，终端900还可选包括有：外围设备接口903和至少一个外围设备。处理器901、存储器902和外围设备接口903之间可以通过总线或信号线相连。各个外围设备可以通过总线、信号线或电路板与外围设备接口903相连。具体地，外围设备包括：射频电路904、触摸显示屏905、摄像头906、音频电路907、定位组件908和电源909中的至少一种。

[0187] 外围设备接口903可被用于将I/O(Input/Output，输入/输出)相关的至少一个外围设备连接到处理器901和存储器902。在一些实施例中，处理器901、存储器902和外围设备接口903被集成在同一芯片或电路板上；在一些其他实施例中，处理器901、存储器902和外围设备接口903中的任意一个或两个可以在单独的芯片或电路板上实现，本实施例对此不加以限定。

[0188] 射频电路904用于接收和发射RF(Radio Frequency，射频)信号，也称电磁信号。射频电路904通过电磁信号与通信网络以及其他通信设备进行通信。射频电路904将电信号转换为电磁信号进行发送，或者，将接收到的电磁信号转换为电信号。可选地，射频电路904包括：天线系统、RF收发器、一个或多个放大器、调谐器、振荡器、数字信号处理器、编解码芯片组、用户身份模块卡等等。射频电路904可以通过至少一种无线通信协议来与其它终端进行通信。该无线通信协议包括但不限于：城域网、各代移动通信网络(2G、3G、4G及5G)、无线局域网和/或WiFi(Wireless Fidelity，无线保真)网络。在一些实施例中，射频电路904还可

以包括NFC(Near Field Communication,近距离无线通信)有关的电路,本申请对此不加以限定。

[0189] 显示屏905用于显示UI(User Interface,用户界面)。该UI可以包括图形、文本、图标、视频及其它们的任意组合。当显示屏905是触摸显示屏时,显示屏905还具有采集在显示屏905的表面或表面上方的触摸信号的能力。该触摸信号可以作为控制信号输入至处理器901进行处理。此时,显示屏905还可以用于提供虚拟按钮和/或虚拟键盘,也称软按钮和/或软键盘。在一些实施例中,显示屏905可以为一个,设置终端900的前面板;在另一些实施例中,显示屏905可以为至少两个,分别设置在终端900的不同表面或呈折叠设计;在再一些实施例中,显示屏905可以是柔性显示屏,设置在终端900的弯曲表面上或折叠面上。甚至,显示屏905还可以设置成非矩形的不规则图形,也即异形屏。显示屏905可以采用LCD(Liquid Crystal Display,液晶显示屏)、OLED(Organic Light-Emitting Diode,有机发光二极管)等材质制备。

[0190] 摄像头组件906用于采集图像或视频。可选地,摄像头组件906包括前置摄像头和后置摄像头。通常,前置摄像头设置在终端的前面板,后置摄像头设置在终端的背面。在一些实施例中,后置摄像头为至少两个,分别为主摄像头、景深摄像头、广角摄像头、长焦摄像头中的任意一种,以实现主摄像头和景深摄像头融合实现背景虚化功能、主摄像头和广角摄像头融合实现全景拍摄以及VR(Virtual Reality,虚拟现实)拍摄功能或者其它融合拍摄功能。在一些实施例中,摄像头组件906还可以包括闪光灯。闪光灯可以是单色温闪光灯,也可以是双色温闪光灯。双色温闪光灯是指暖光闪光灯和冷光闪光灯的组合,可以用于不同色温下的光线补偿。

[0191] 音频电路907可以包括麦克风和扬声器。麦克风用于采集用户及环境的声波,并将声波转换为电信号输入至处理器901进行处理,或者输入至射频电路904以实现语音通信。出于立体声采集或降噪的目的,麦克风可以为多个,分别设置在终端900的不同部位。麦克风还可以是阵列麦克风或全向采集型麦克风。扬声器则用于将来自处理器901或射频电路904的电信号转换为声波。扬声器可以是传统的薄膜扬声器,也可以是压电陶瓷扬声器。当扬声器是压电陶瓷扬声器时,不仅可以将电信号转换为人类可听见的声波,也可以将电信号转换为人类听不见的声波以进行测距等用途。在一些实施例中,音频电路907还可以包括耳机插孔。

[0192] 定位组件908用于定位终端900的当前地理位置,以实现导航或LBS(Location Based Service,基于位置的服务)。定位组件908可以是基于美国的GPS(Global Positioning System,全球定位系统)、中国的北斗系统、俄罗斯的格雷纳斯系统或欧盟的伽利略系统的定位组件。

[0193] 电源909用于为终端900中的各个组件进行供电。电源909可以是交流电、直流电、一次性电池或可充电电池。当电源909包括可充电电池时,该可充电电池可以支持有线充电或无线充电。该可充电电池还可以用于支持快充技术。

[0194] 在一些实施例中,终端900还包括有一个或多个传感器910。该一个或多个传感器910包括但不限于:加速度传感器911、陀螺仪传感器912、压力传感器913、指纹传感器914、光学传感器915以及接近传感器916。

[0195] 加速度传感器911可以检测以终端900建立的坐标系的三个坐标轴上的加速度大

小。比如，加速度传感器911可以用于检测重力加速度在三个坐标轴上的分量。处理器901可以根据加速度传感器911采集的重力加速度信号，控制触摸显示屏905以横向视图或纵向视图进行用户界面的显示。加速度传感器911还可以用于游戏或者用户的运动数据的采集。

[0196] 陀螺仪传感器912可以检测终端900的机体方向及转动角度，陀螺仪传感器912可以与加速度传感器911协同采集用户对终端900的3D动作。处理器901根据陀螺仪传感器912采集的数据，可以实现如下功能：动作感应(比如根据用户的倾斜操作来改变UI)、拍摄时的图像稳定、游戏控制以及惯性导航。

[0197] 压力传感器913可以设置在终端900的侧边框和/或触摸显示屏905的下层。当压力传感器913设置在终端900的侧边框时，可以检测用户对终端900的握持信号，由处理器901根据压力传感器913采集的握持信号进行左右手识别或快捷操作。当压力传感器913设置在触摸显示屏905的下层时，由处理器901根据用户对触摸显示屏905的压力操作，实现对UI界面上的可操作性控件进行控制。可操作性控件包括按钮控件、滚动条控件、图标控件、菜单控件中的至少一种。

[0198] 指纹传感器914用于采集用户的指纹，由处理器901根据指纹传感器914采集到的指纹识别用户的身份，或者，由指纹传感器914根据采集到的指纹识别用户的身份。在识别出用户的身份为可信身份时，由处理器901授权该用户执行相关的敏感操作，该敏感操作包括解锁屏幕、查看加密信息、下载软件、支付及更改设置等。指纹传感器914可以被设置终端900的正面、背面或侧面。当终端900上设置有物理按键或厂商Logo时，指纹传感器914可以与物理按键或厂商Logo集成在一起。

[0199] 光学传感器915用于采集环境光强度。在一个实施例中，处理器901可以根据光学传感器915采集的环境光强度，控制触摸显示屏905的显示亮度。具体地，当环境光强度较高时，调高触摸显示屏905的显示亮度；当环境光强度较低时，调低触摸显示屏905的显示亮度。在另一个实施例中，处理器901还可以根据光学传感器915采集的环境光强度，动态调整摄像头组件906的拍摄参数。

[0200] 接近传感器916，也称距离传感器，通常设置在终端900的前面板。接近传感器916用于采集用户与终端900的正面之间的距离。在一个实施例中，当接近传感器916检测到用户与终端900的正面之间的距离逐渐变小时，由处理器901控制触摸显示屏905从亮屏状态切换为息屏状态；当接近传感器916检测到用户与终端900的正面之间的距离逐渐变大时，由处理器901控制触摸显示屏905从息屏状态切换为亮屏状态。

[0201] 本领域技术人员可以理解，图9中示出的结构并不构成对终端900的限定，可以包括比图示更多或更少的组件，或者组合某些组件，或者采用不同的组件布置。

[0202] 在示例性的实施例中，还提供了一种计算机可读存储介质，所述计算机可读存储介质上存储有指令，所述指令被处理器执行时实现上述数据安全保护方法。

[0203] 在示例性实施例中，还提供了一种计算机程序产品，当该计算机程序产品被执行时，其用于实现上述数据安全保护方法。

[0204] 应当理解的是，在本文中提及的“多个”是指两个或两个以上。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。字符“/”一般表示前后关联对象是一种“或”的关系。

[0205] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件

来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0206] 以上所述仅为本申请的可选实施例，并不用以限制本申请，凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

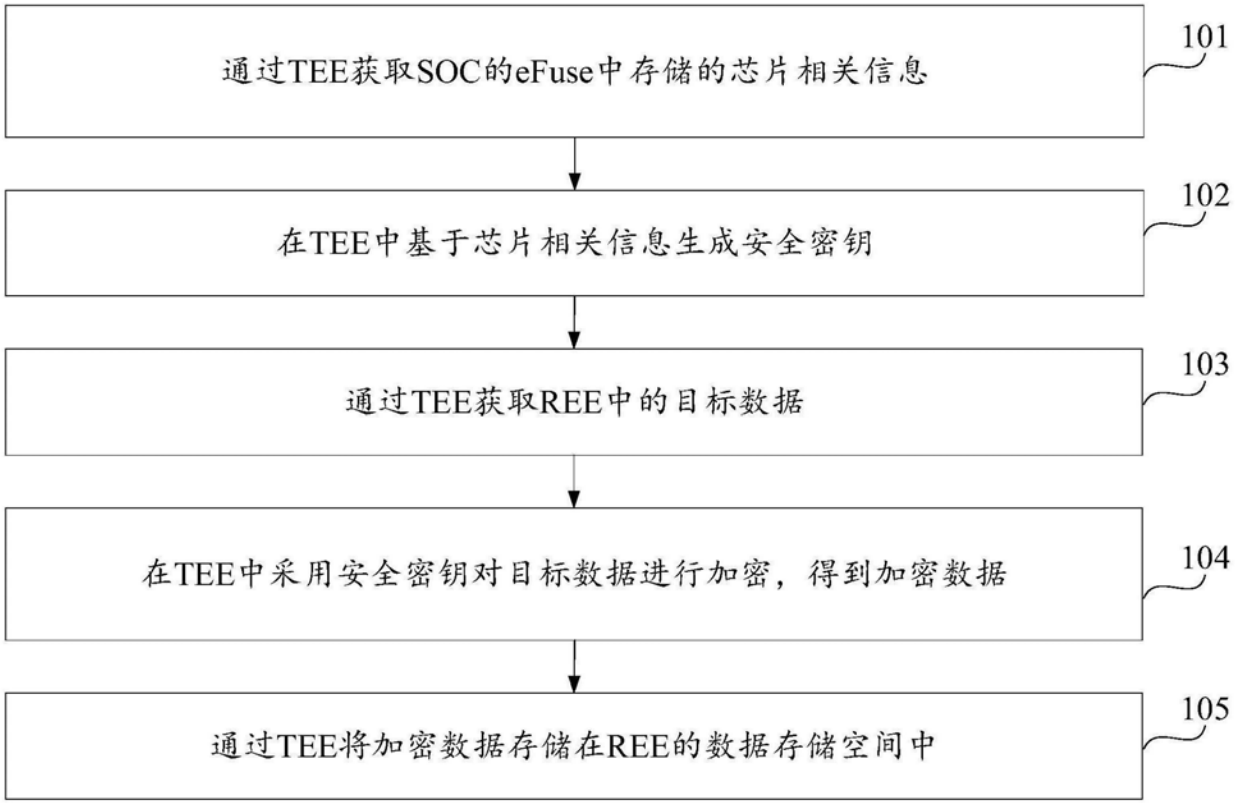

通过TEE获取SOC的eFuse中存储的芯片相关信息
101
在TEE中基于芯片相关信息生成安全密钥
102
通过TEE获取REE中的目标数据
103
在TEE中采用安全密钥对目标数据进行加密，得到加密数据
104
通过TEE将加密数据存储在REE的数据存储空间中
105

图1

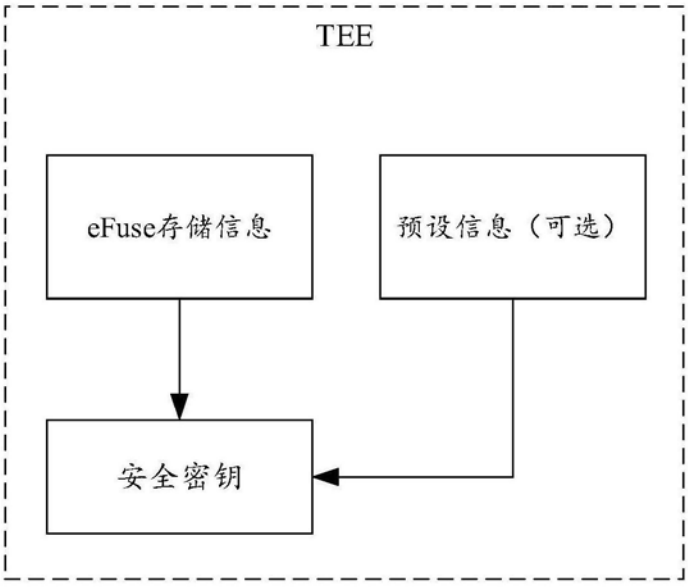

TEE
eFuse存储信息
预设信息（可选）
安全密钥

图2

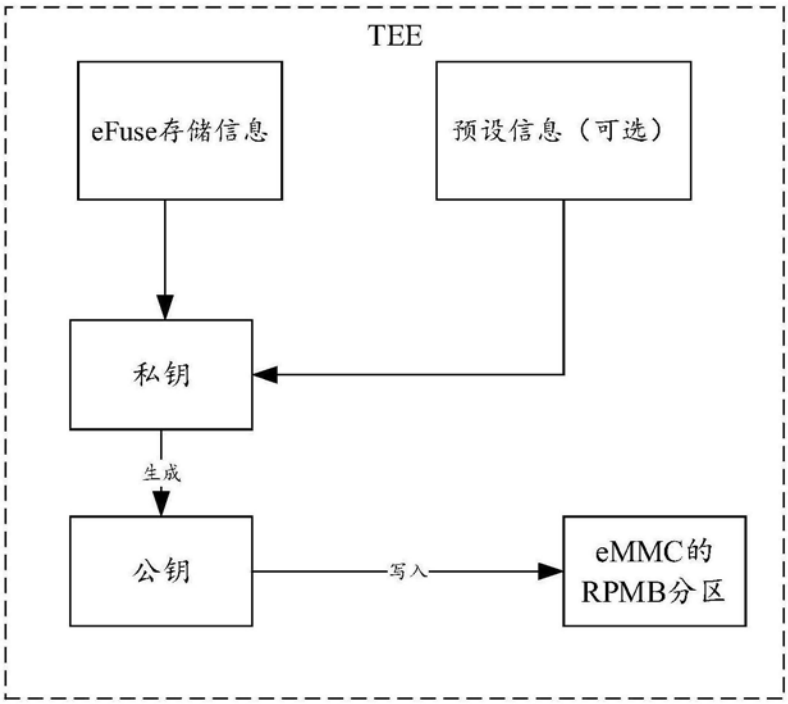

TEE
eFuse存储信息
预设信息（可选）
私钥
生成
公钥
写入
eMMC的
RPMB分区

图3

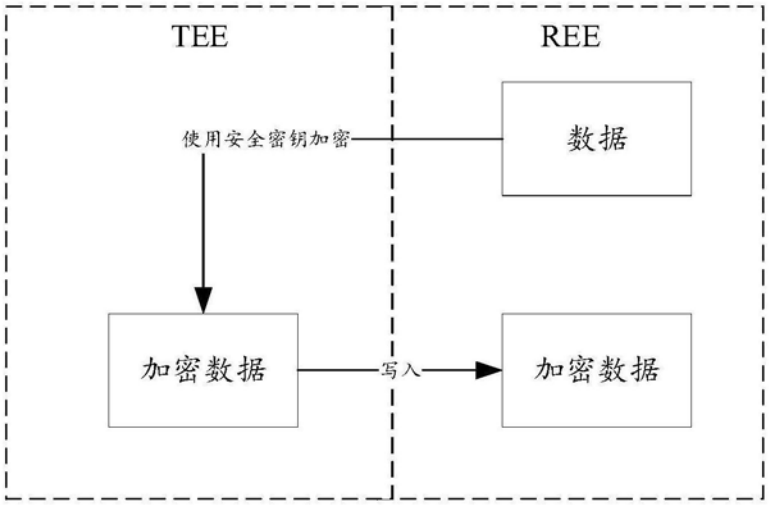

TEE
REE
使用安全密钥加密
数据
加密数据
写入
加密数据

图4

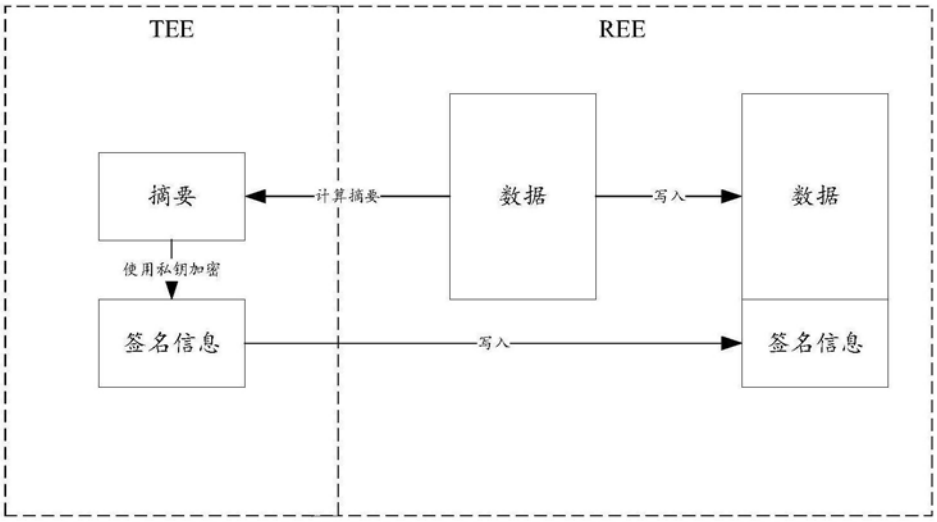

TEE
REE
摘要
计算摘要
数据
写入
数据
使用私钥加密
签名信息
写入
签名信息

图5

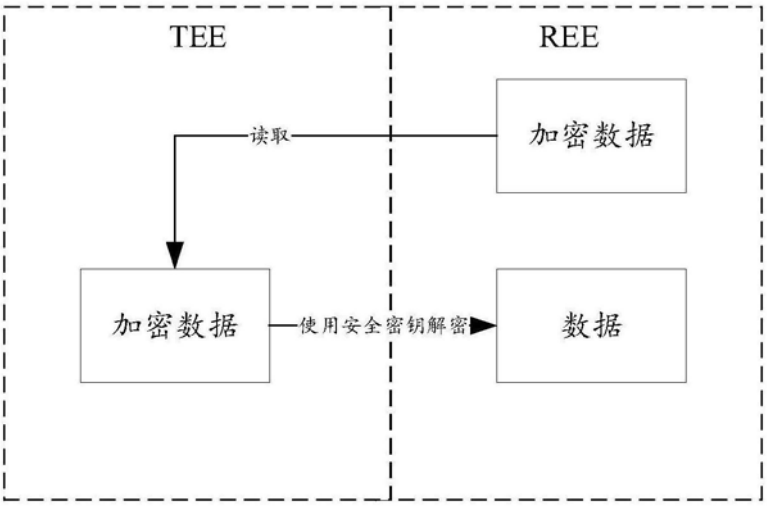

TEE
REE
读取
加密数据
加密数据
使用安全密钥解密
数据

图6

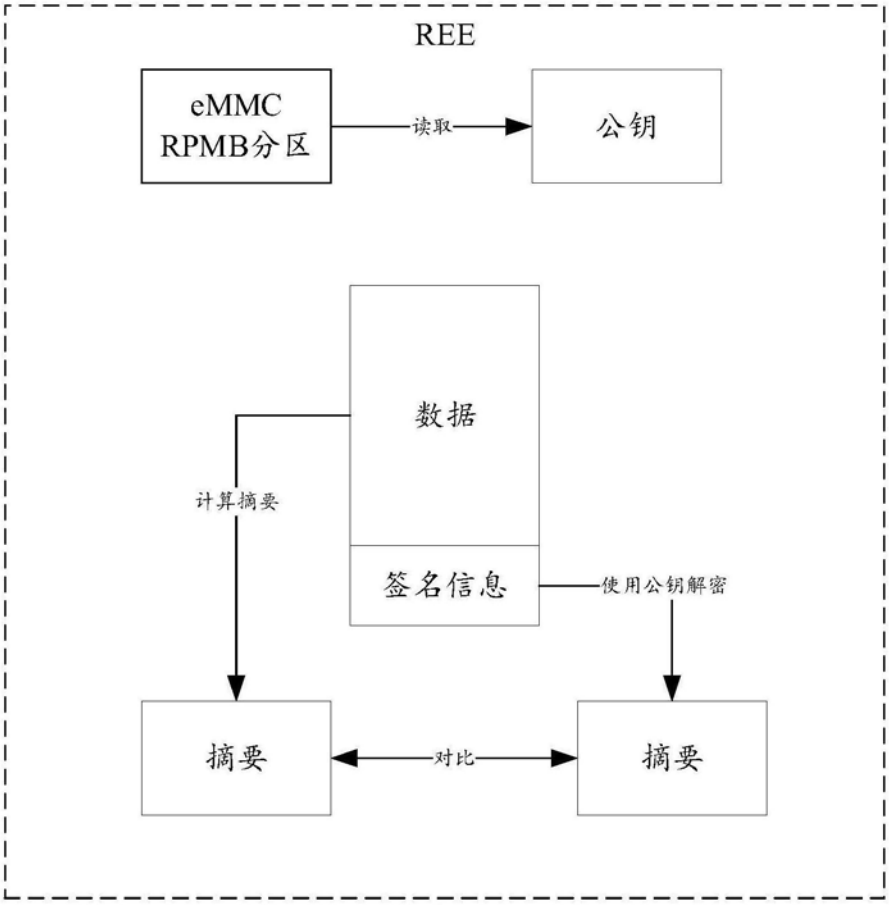


图7

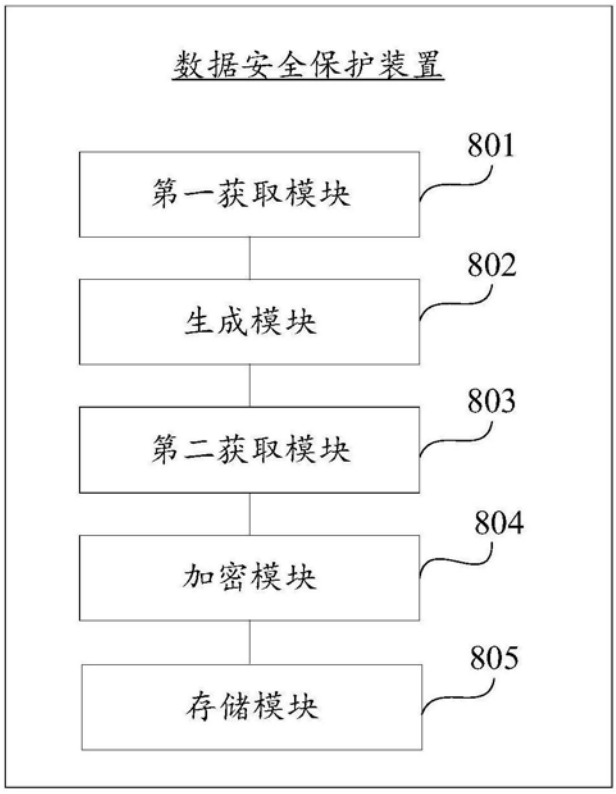


图8

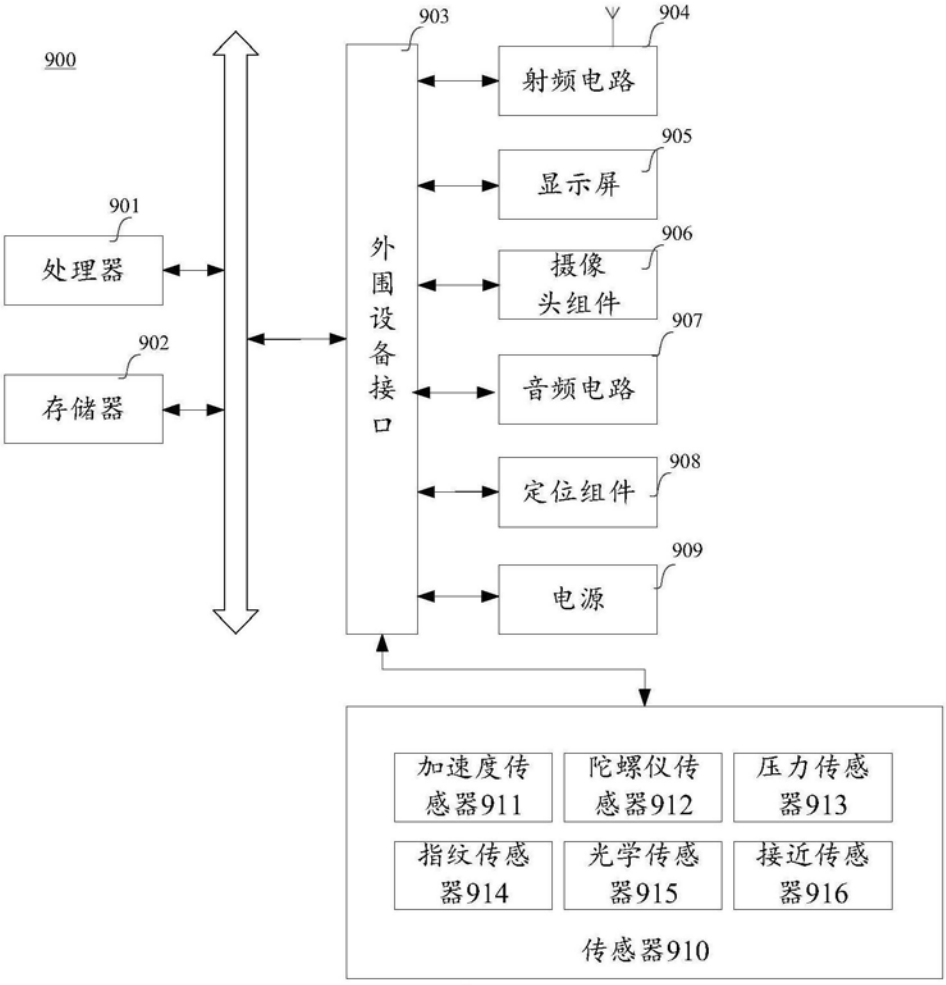

900
903
904
射频电路
905
显示屏
901
处理器
外围设备接口
906
摄像头组件
907
音频电路
902
存储器
908
定位组件
909
电源
加速度传感器911
陀螺仪传感器912
压力传感器913
指纹传感器914
光学传感器915
接近传感器916
传感器910

图9