(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113626818 B
(45)授权公告日 2023.10.20

(21)申请号 202010390095.8
(22)申请日 2020.05.08
(65)同一申请的已公布的文献号
申请公布号 CN 113626818 A
(43)申请公布日 2021.11.09
(73)专利权人 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 苗欣 于克雄
(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
专利代理师 罗英 刘芳
(51)Int.Cl.
G06F 21/57(2013.01)
G06F 21/74(2013.01)

(56)对比文件
CN 106547618 A,2017.03.29
CN 108205502 A,2018.06.26
CN 109960582 A,2019.07.02
CN 110730159 A,2020.01.24
US 2019318087 A1,2019.10.17

审查员 高民芳

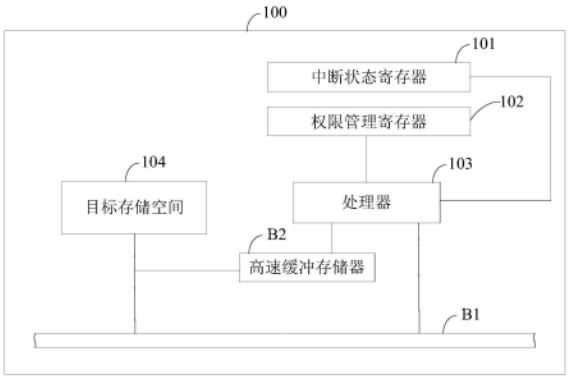
权利要求书3页 说明书19页 附图7页

(54)发明名称

计算机系统、服务处理方法、可读存储介质及芯片

(57)摘要

本申请实施例提供一种计算机系统、服务处理方法、可读存储介质及芯片，其中，通过在计算机系统中设置轻量级的权限管理寄存器，并通过权限管理寄存器以及中断状态寄存器共同管理目标存储空间的访问权限，使对目标存储空间的访问只能够在特定的安全模式(例如TEE)实现，从而搭建了安全性较高的TEE。且本申请实施例提供的计算机系统可以应用于各种芯片架构中，设计较为简单，通用性较高，且权限管理寄存器的成本较低，在实现可靠的安全访问环境的同时有效降低了芯片成本。



CN 113626818 B

1.一种计算机系统,其特征在于,包括:中断状态寄存器、权限管理寄存器、处理器以及目标存储空间;

其中,所述系统调用目标服务;

所述处理器用于根据所述目标服务触发的第一中断配置所述中断状态寄存器中所述第一中断对应的标志位为第一中断标志,以及配置所述权限管理寄存器中所述第一中断对应的标志位为第一调用标志;其中,所述第一中断标志和所述第一调用标志用于指示是否允许访问所述目标存储空间;

所述处理器用于根据所述第一中断标志和所述第一调用标志,确定是否允许所述处理器访问所述目标存储空间,以及用于确定允许所述处理器访问所述目标存储空间时,在TEE模式获取所述目标存储空间的第一信息;

所述处理器还用于根据所述第一信息执行所述目标服务。

2.根据权利要求1所述的系统,其特征在于,所述第一中断标志和所述第一调用标志用于指示是否允许访问所述目标存储空间,包括:

若所述第一中断标志和所述第一调用标志均指示允许所述处理器访问所述目标存储空间,则允许所述处理器访问所述目标存储空间;

若所述第一中断标志或所述第一调用标志指示不允许所述处理器访问所述目标存储空间,则不允许所述处理器访问所述目标存储空间。

3.根据权利要求1或2所述的系统,其特征在于,所述第一中断为不可屏蔽NMI中断。

4.根据权利要求1至3任一项所述的系统,其特征在于,所述处理器具体用于根据所述第一中断的优先级,配置所述第一调用标志。

5.根据权利要求4所述的系统,其特征在于,所述处理器具体用于

确定所述第一中断是否为当前优先级最高的中断;

在所述处理器确定所述第一中断为当前优先级最高的中断时,所述处理器配置所述第一调用标志;

在所述处理器确定所述第一中断不是当前优先级最高的中断时,所述处理器用于在执行优先级高于所述第一中断的中断之后,配置所述第一调用标志。

6.根据权利要求1至5任一项所述的系统,其特征在于,所述系统还包括:内存保护单元,所述内存保护单元用于配置所述目标存储空间的第二调用标志;其中,所述第一中断标志、所述第一调用标志以及所述第二调用标志用于指示是否允许所述处理器访问所述目标存储空间;

所述处理器还用于根据所述第一中断标志、所述第一调用标志以及所述第二调用标志,确定是否允许访问所述目标存储空间。

7.根据权利要求6所述的系统,其特征在于,所述第一中断标志、所述第一调用标志以及所述第二调用标志用于指示是否允许所述处理器访问目标存储空间,包括:

若所述第二调用标志指示不允许所述处理器访问目标存储空间,则不允许所述处理器访问所述目标存储空间;

若所述第二调用标志指示允许所述处理器访问目标存储空间,所述第一中断标志或所述第一调用标志指示不允许所述处理器访问所述目标存储空间,则不允许所述处理器访问所述目标存储空间;

若所述第二调用标志指示允许所述处理器访问目标存储空间，所述第一中断标志和所述第一调用标志均指示允许所述处理器访问所述目标存储空间，则允许所述处理器访问所述目标存储空间。

8.根据权利要求1至7任一项所述的系统，其特征在于，所述处理器还用于复位所述中断状态寄存器中所述第一中断对应的标志位。

9.根据权利要求1至8任一项所述的系统，其特征在于，所述处理器还用于根据所述第一中断清除和释放所述目标服务调用的资源。

10.根据权利要求1至9任一项所述的系统，其特征在于，所述目标存储空间包括：非易失性存储和/或易失性存储中的一个或多个存储单元。

11.根据权利要求10所述的系统，其特征在于，所述多个存储单元为连续的多个存储单元或不连续的多个存储单元。

12.一种服务处理方法，其特征在于，应用于计算机系统，所述计算机系统包括中断状态寄存器、权限管理寄存器、处理器以及目标存储空间；所述方法包括：

当目标服务被调用时，根据所述目标服务触发的第一中断配置第一中断标志和第一调用标志，其中，所述第一中断标志和所述第一调用标志用于指示是否允许访问目标存储空间；

若根据所述第一中断标志和所述第一调用标志，确定允许访问所述目标存储空间，则在TEE模式获取所述目标存储空间的第一信息；

根据所述第一信息执行所述目标服务。

13.根据权利要求12所述的方法，其特征在于，所述第一中断标志和所述第一调用标志用于指示是否允许访问所述目标存储空间，包括：

若所述第一中断标志和所述第一调用标志均指示允许所述处理器访问所述目标存储空间，则允许所述处理器访问所述目标存储空间；

若所述第一中断标志或所述第一调用标志指示不允许所述处理器访问所述目标存储空间，则不允许所述处理器访问所述目标存储空间。

14.根据权利要求12或13所述的方法，其特征在于，所述第一中断为不可屏蔽NMI中断。

15.根据权利要求12至14任一项所述的方法，其特征在于，所述根据所述目标服务触发的第一中断配置第一中断标志和第一调用标志，包括：

根据所述第一中断的优先级，配置所述第一调用标志。

16.根据权利要求15所述的方法，其特征在于，所述根据所述第一中断的优先级，配置所述第一调用标志，包括：

在所述第一中断的优先级为当前优先级最高的中断时，配置所述第一调用标志；

在所述第一中断不是当前优先级最高的中断时，执行优先级高于所述第一中断的中断之后，配置所述第一调用标志。

17.根据权利要求12至16任一项所述的方法，其特征在于，所述方法还包括：获取第二调用标志；其中，所述第一中断标志、所述第一调用标志以及所述第二调用标志用于指示是否允许访问目标存储空间。

18.根据权利要求17所述的方法，其特征在于，所述第一中断标志、所述第一调用标志以及所述第二调用标志用于指示是否允许访问目标存储空间，包括：

若所述第二调用标志指示不允许访问目标存储空间，则不允许访问所述目标存储空间；

若所述第二调用标志指示允许访问目标存储空间，所述第一中断标志或所述第一调用标志指示不允许访问所述目标存储空间，则不允许访问所述目标存储空间；

若所述第二调用标志指示允许访问目标存储空间，所述第一中断标志和所述第一调用标志均指示允许访问所述目标存储空间，则允许访问所述目标存储空间。

19.根据权利要求12至18任一项所述的方法，其特征在于，所述方法还包括：

复位所述第一中断对应的标志位。

20.根据权利要求12至19任一项所述的方法，其特征在于，所述方法还包括：

根据所述第一中断清除和释放所述目标服务调用的资源。

21.根据权利要求12至20任一项所述的方法，其特征在于，所述目标存储空间包括：非易失性存储和/或易失性存储中的一个或多个存储单元。

22.根据权利要求21所述的方法，其特征在于，所述多个存储单元为连续的多个存储单元或不连续的多个存储单元。

23.一种可读存储介质，其特征在于，包括：程序；

所述程序被处理器执行时，以执行如权利要求12至22任一项所述的服务处理方法。

24.一种芯片，其特征在于，所述芯片包括一个或多个功能电路，用于实现如权利要求12至22任意一项所述的方法。

计算机系统、服务处理方法、可读存储介质及芯片

技术领域

[0001] 本申请实施例涉及计算机技术领域，尤其涉及一种计算机系统、服务处理方法、可读存储介质及芯片。

背景技术

[0002] 物联网(the internet of things，IoT)，即“万物相连的互联网”，是在互联网基础上延伸和扩展的网络，通过将各种信息传感设备与互联网结合起来形成的一个巨大网络，从而实现在任何时间、任何地点、人、机以及物的互联互通。随着通信技术的不断发展，物联网已迅速广泛应用至各行各业，例如，智慧城市、农业领域等等。然而，“事物”之间的互联互通在营造活跃的环境的同时，也带来了一系列安全问题。

[0003] 针对设备的安全问题，可信执行环境(trusted execution environment，TEE)的概念被提出。具体地，TEE是与设备上的非可信执行环境，例如富执行环境(rich execution environment，TEE)，并存的运行环境，TEE和REE中通常各自运行一套操作系统，这两套操作系统上又可以各自运行不同的应用。TEE的应用能够为REE的应用提供安全服务，例如，在TEE环境下可进行移动支付服务、敏感数据保护、安全认证等等。然而，目前在实现TEE时需要引入过高的芯片成本，无法满足设备低成本、高性能的需求。

发明内容

[0004] 本申请实施例提供一种计算机系统、服务处理方法、可读存储介质及芯片，以实现安全性较高的可信执行环境，且同时降低芯片成本。

[0005] 第一方面，本申请实施例提供一种计算机系统，包括：中断状态寄存器、权限管理寄存器、处理器以及目标存储空间。其中，所述计算机系统调用目标服务。该目标服务位于TEE中。调用目标服务的调用者通常位于REE中。所述处理器用于根据所述目标服务触发的第一中断配置所述中断状态寄存器中所述第一中断对应的标志位为第一中断标志，以及配置所述权限管理寄存器中所述第一中断对应的标志位为第一调用标志；其中，所述第一中断标志和所述第一调用标志共同指示是否允许访问所述目标存储空间；所述处理器用于根据所述第一中断标志和所述第一调用标志，确定是否允许所述处理器访问所述目标存储空间，以及用于确定允许所述处理器访问所述目标存储空间时，在安全模式获取所述目标存储空间的第一信息；所述处理器还用于根据所述第一信息执行所述目标服务。

[0006] 本申请实施例通过在服务处理系统中设置轻量级的权限管理寄存器，并通过权限管理寄存器以及中断状态寄存器管理目标存储空间的访问权限，使对目标存储空间的访问只能够在特定的安全模式(例如TEE)下实现，从而搭建了安全性较高的可信执行环境。且本申请实施例提供的服务处理系统可以应用于各种芯片架构中，设计较为简单，通用性较高，且权限管理寄存器的成本较低，在实现可靠的安全访问环境的同时有效降低了芯片成本。

[0007] 在一些实现方式中，所述第一中断标志和所述第一调用标志用于指示是否允许访问所述目标存储空间，包括：若所述第一中断标志和所述第一调用标志均指示允许所述处

理器访问所述目标存储空间，则允许所述处理器访问所述目标存储空间；若所述第一中断标志或所述第一调用标志指示不允许所述处理器访问所述目标存储空间，则不允许所述处理器访问所述目标存储空间。

[0008] 本申请实施例，采用两个标志共同控制目标存储空间的访问权限，设计简单，在实现可靠的安全访问环境的同时有效降低了芯片成本。

[0009] 在一些实现方式中，所述第一中断为不可屏蔽(non maskable interrupt，NMI)中断。

[0010] 在一些实现方式中，所述处理器具体用于根据所述第一中断的优先级，配置所述第一调用标志。

[0011] 在一些实现方式中，所述处理器具体用于确定所述第一中断是否为优先级最高的中断；在所述处理器确定所述第一中断为优先级最高的中断时，所述处理器配置所述第一调用标志；在所述处理器确定所述第一中断不是优先级最高的中断时，所述处理器用于在执行优先级高于所述第一中断的中断之后，配置所述第一调用标志。

[0012] 本申请实施例中，处理器根据中断的优先级处理各个中断，保证了计算机系统对各个中断都能够有正确的响应，从而提高计算机系统的可靠性。

[0013] 在一些实现方式中，所述系统还包括：内存保护单元，所述内存保护单元用于配置所述目标存储空间的第二调用标志；其中，所述第一中断标志、所述第一调用标志以及所述第二调用标志共同指示是否允许访问目标存储空间；所述处理器还用于根据所述第一中断标志、所述第一调用标志以及所述第二调用标志，确定是否允许访问所述目标存储空间。

[0014] 本申请实施例，通过设置内存保护单元，并通过内存保护单元、中断状态寄存器以及权限管理寄存器共同管理目标存储空间的访问权限，进一步提高了服务系统的安全性。

[0015] 在一些实现方式中，所述第一中断标志、所述第一调用标志以及所述第二调用标志用于指示是否允许所述处理器访问目标存储空间，包括：在所述第二调用标志指示不允许所述处理器访问目标存储空间时，不允许所述处理器访问所述目标存储空间；若所述第二调用标志指示允许所述处理器访问目标存储空间，所述第一中断标志或所述第一调用标志指示不允许所述处理器访问所述目标存储空间，则不允许所述处理器访问所述目标存储空间；若所述第二调用标志指示允许所述处理器访问目标存储空间，所述第一中断标志和所述第一调用标志均指示允许所述处理器访问所述目标存储空间，则允许所述处理器访问所述目标存储空间。

[0016] 需要说明的是，采用一个或多个标志指示是否允许处理器访问目标存储空间可以有多种实现方式。以两个标志为例，该两个标志可以分别是第一中断标志和第一调用标志，若第一中断标志和第一调用标志均指示允许访问目标存储空间，则处理器可以访问目标存储空间；若第一中断标志和第一调用标志中任一标志指示不允许处理器访问目标存储空间，则处理器不可以访问目标存储空间；以三个标志为例，该三个标志可以分别是：第一中断标志、第一调用标志和第二调用标志，该三个标志可以共同指示是否允许处理访问目标存储空间，规则例如是当三个标志均指示允许处理器访问目标存储空间时，则处理器可以访问目标存储空间，若三个标志中任一标志指示不允许处理器访问目标存储空间，则不允许处理器访问目标存储空间；或者该三个标志也可以独立指示是否允许处理器访问目标存储空间，规则例如是当三个标志中的任意一个标志或者某个指定的标志指示不允许访问

时,则不允许处理器访问目标存储空间,当三个标志均指示允许处理器访问目标存储空间时,则处理器可以访问目标存储空间,等实现方式,采用更多标志控制目标存储空间的访问权限的情况可参考上述采用两个或三个标志控制目标存储空间的访问权限的实现方式,在此不一一举例。

[0017] 在一些实现方式中,所述处理器还用于复位所述中断状态寄存器中所述第一中断对应的标志位。

[0018] 本申请实施例,通过在TEE中复位中断状态寄存器中第一中断对应的标志位,从而保护了目标存储空间,减小了计算机系统的攻击面,提高了计算机系统的安全性。

[0019] 在一些实现方式中,所述处理器还用于根据所述第一中断清除和释放所述目标服务调用的资源。

[0020] 本申请实施例中,计算机系统可通过执行上述复位中断状态寄存器以及权限管理寄存器中第一中断对应的标志位,清除和释放目标服务调用的堆、栈中涉及的敏感信息和中间结果等,退出第一中断,并返回目标服务的处理结果,完成整个目标服务的处理过程。

[0021] 在一些实现方式中,所述目标存储空间包括:非易失性存储(non-volatile memory,NVM)和/或易失性存储(volatile memory)中的一个或多个存储单元。

[0022] 在一些实现方式中,所述多个存储单元为连续的多个存储单元或不连续的多个存储单元。

[0023] 需要说明的是,非易失性存储例如可以为可编程只读内存(programmable read-only memory,PROM)、电可改写只读内存(electrically alterable read only memory,EAROM)、可擦可编程只读内存(erasable programmable read only memory、EPROM)、电可擦可编程只读内存(electrically erasable programmable read only memory、EEPROM)、闪存(flash memory)、一次编程只读存储器(one time programmable read only memory,OTPROM)等等。易失性存储例如为随机存取存储器(random-access memory,RAM)等。

[0024] 本申请实施例中,存储不同目标服务对应的第一信息的目标存储空间可根据目标服务的不同而具备差异,例如,一些目标服务对应的第一信息在任何情况下都不能被修改,则存储该目标服务对应的第一信息的目标存储空间可以为OTPROM;又如,一些目标服务对应的第一信息需要保持动态的变化,则存储该目标服务对应的第一信息的目标存储空间例如可以为EPROM。

[0025] 其中,存储器通常包括大量的存储元,把这些存储元进行分组,组内所有的存储元同时进行读出或写入的操作,这样的一组存储元为一个存储单元,存储单元是处理器访问存储器的基本单元,在本方案中,目标存储空间包括的多个存储单元可以为连续的存储单元或不连续的存储单元,使本申请实施例提供的计算机系统具有较高的灵活性,可适用于各种类型的存储器。

[0026] 第二方面,本申请实施例提供一种服务处理方法,该服务处理方法应用于第一方面任一项所述的计算机系统,该计算机系统包括:中断状态寄存器、权限管理寄存器、处理器以及目标存储空间;所述方法包括:当计算机系统调用目标服务时,其中,该目标服务位于TEE中,调用目标服务的调用者通常位于REE中,根据目标服务触发的第一中断配置第一中断标志和第一调用标志,其中,所述第一中断标志和所述第一调用标志用于指示是否允许访问目标存储空间;若根据所述第一中断标志和所述第一调用标志,确定允许访问所述

目标存储空间，则在安全模式获取目标存储空间的第一信息；根据所述第一信息执行所述目标服务。

[0027] 本申请实施例提供的服务处理方法，通过第一调用标志和第一中断标志共同管理目标存储空间的访问权限，使对目标存储空间的访问只能够在特定的安全模式(例如TEE)下实现，从而搭建了安全性较高的可信执行环境。本实施例提供的服务处理方法可通过在各种芯片架构中增加轻量级的权限管理寄存器实现，设计较为简单，通用性较高，且权限管理寄存器的成本较低，在实现可靠的安全访问环境的同时有效降低了芯片成本。

[0028] 在一些实现方式中，所述第一中断标志和所述第一调用标志用于指示是否允许访问所述目标存储空间，包括：若所述第一中断标志和所述第一调用标志均指示允许所述处理器访问所述目标存储空间，则允许所述处理器访问所述目标存储空间；若所述第一中断标志或所述第一调用标志指示不允许所述处理器访问所述目标存储空间，则不允许所述处理器访问所述目标存储空间。

[0029] 本申请实施例，采用两个标志共同控制目标存储空间的访问权限，设计简单，在实现可靠的安全访问环境的同时有效降低了芯片成本。

[0030] 在一些实现方式中，所述第一中断为NMI中断。

[0031] 在一些实现方式中，所述根据所述目标服务触发的第一中断配置第一中断标志和第一调用标志，包括：根据所述第一中断的优先级，配置所述第一调用标志。

[0032] 在一些实现方式中，所述根据所述第一中断的优先级，配置所述第一调用标志，包括：在所述第一中断的优先级为当前优先级最高的中断时，配置所述第一调用标志；在所述第一中断不是当前优先级最高的中断时，则执行优先级高于所述第一中断的中断之后，配置所述第一调用标志。

[0033] 本申请实施例中，处理器根据中断的优先级处理各个中断，保证了计算机系统对各个中断都能够有正确的响应，从而提高计算机系统的可靠性。

[0034] 在一些实现方式中，所述方法还包括：获取第二调用标志；其中，所述第一中断标志、所述第一调用标志以及所述第二调用标志用于指示是否允许访问目标存储空间。

[0035] 本申请实施例，通过设置内存保护单元，并通过内存保护单元共同管理目标存储空间的访问权限，进一步提高了服务系统的安全性。

[0036] 在一些实现方式中，所述第一中断标志、所述第一调用标志以及所述第二调用标志用于指示是否允许访问目标存储空间，包括：若所述第二调用标志指示不允许访问目标存储空间，则不允许访问所述目标存储空间；若所述第二调用标志指示允许访问目标存储空间，所述第一中断标志或所述第一调用标志指示不允许访问所述目标存储空间，则不允许访问所述目标存储空间；若所述第二调用标志指示允许访问目标存储空间，所述第一中断标志和所述第一调用标志均指示允许访问所述目标存储空间，则允许访问所述目标存储空间。

[0037] 需要说明的是，采用一个或多个标志指示是否允许处理器访问目标存储空间可以有多种实现方式。以两个标志为例，该两个标志可以分别是第一中断标志和第一调用标志，若第一中断标志和第一调用标志均指示允许访问目标存储空间，则处理器可以访问目标存储空间；若第一中断标志和第一调用标志中任一标志指示不允许处理器访问目标存储空间，则处理器不可以访问目标存储空间；以三个标志为例，该三个标志可以分别是：第一中

断标志、第一调用标志和第二调用标志，该三个标志可以共同指示是否允许处理访问目标存储空间，规则例如是当三个标志均指示允许处理器访问目标存储空间时，则处理器可以访问目标存储空间，若三个标志中任一标志指示不允许处理器访问目标存储空间，则不允许处理器访问目标存储空间；或者该三个标志也可以独立指示是否允许处理器访问目标存储空间，规则例如是当三个标志中的任意一个标志或者某个指定的标志指示不允许访问时，则不允许处理器访问目标存储空间，当三个标志均指示允许处理器访问目标存储空间时，则处理器可以访问目标存储空间，等实现方式，采用更多标志控制目标存储空间的访问权限的情况可参考上述采用两个或三个标志控制目标存储空间的访问权限的实现方式，在此不一一举例。

[0038] 在一些实现方式中，所述方法还包括：复位所述第一中断标志。

[0039] 本申请实施例，通过在TEE中复位中断状态寄存器中第一中断对应的标志位，从而保护了目标存储空间，减小了计算机系统的攻击面，提高了计算机系统的安全性。

[0040] 在一些实现方式中，所述方法还包括：根据所述第一中断清除和释放所述目标服务调用的资源。

[0041] 本申请实施例中，计算机系统可通过执行上述复位中断状态寄存器以及权限管理寄存器中第一中断对应的标志位，清除和释放目标服务调用的堆、栈中涉及的敏感信息和中间结果等，退出第一中断，并返回目标服务的处理结果，完成整个目标服务的处理过程。

[0042] 在一些实现方式中，所述目标存储空间包括：非易失性存储和/或易失性存储中的一个或多个存储单元。

[0043] 在一些实现方式中，所述多个存储单元为连续的多个存储单元或不连续的多个存储单元。

[0044] 需要说明的是，非易失性存储例如可以为可编程只读内存(programmable read-only memory，PROM)、电可改写只读内存(electrically alterable read only memory，EAROM)、可擦可编程只读内存(erasable programmable read only memory、EPROM)、电可擦可编程只读内存(electrically erasable programmable read only memory、EEPROM)、闪存(flash memory)、一次编程只读存储器(one time programmable read only memory，OTPROM)等等。易失性存储例如为随机存取存储器(random-access memory，RAM)等。

[0045] 本申请实施例中，存储不同目标服务对应的第一信息的目标存储空间可根据目标服务的不同而具备差异，例如，一些目标服务对应的第一信息在任何情况下都不能被修改，则存储该目标服务对应的第一信息的目标存储空间可以为OTPROM；又如，一些目标服务对应的第一信息需要保持动态的变化，则存储该目标服务对应的第一信息的目标存储空间例如可以为EPROM。

[0046] 其中，存储器通常包括大量的存储元，把这些存储元进行分组，组内所有的存储元同时进行读出或写入的操作，这样的一组存储元为一个存储单元，存储单元是处理器访问存储器的基本单元，在本方案中，目标存储空间包括的多个存储单元可以为连续的存储单元或不连续的存储单元，使本申请实施例提供的计算机系统具有较高的灵活性，可适用于各种类型的存储器。

[0047] 第三方面，本申请实施例还提供一种可读存储介质，计算机可读存储介质存储有计算机程序，计算机程序包含至少一段代码，至少一段代码由计算机执行，以控制计算机执

行第二方面本申请任一实施例的服务处理方法。

[0048] 其中，程序可以全部或者部分存储在与处理器封装在一起的存储介质上，也可以部分或者全部存储在不与处理器封装在一起的存储器上。

[0049] 第四方面，本申请实施例提供一种电子设备，包括：存储器、处理器以及计算机程序指令；

[0050] 所述存储器存储所述计算机程序指令；

[0051] 所述处理器执行所述计算机程序指令，以执行如第二方面本申请任一实施例的服务处理方法。

[0052] 其中，上述电子设备可以为终端设备或者网络设备，也可以为用于终端设备或网络设备上的芯片；存储器可以与处理器集成在同一块芯片上，也可以分别设置在不同的芯片上。

[0053] 第五方面，本申请实施例还提供一种处理器，该处理器包括：

[0054] 至少一个电路，用于调用目标服务，并根据所述目标服务触发的第一中断配置第一中断标志和第一调用标志，其中，所述第一中断标志和所述第一调用标志共同指示是否允许访问目标存储空间；

[0055] 至少一个电路，用于若根据所述第一中断标志和所述第一调用标志，确定允许访问所述目标存储空间，则在TEE模式获取所述目标存储空间的第一信息；

[0056] 至少一个电路，用于根据所述第一信息执行所述目标服务。

[0057] 其中，上述处理器可以为芯片。

[0058] 第六方面，本申请实施例还提供一种芯片，该芯片包括实现前述任意一种方法的功能电路，或者该芯片包含处理器(或者称之为处理器核)和存储单元，所述存储单元包含计算机程序，所述计算机程序在被所述处理器执行时实现前述任意一种方法，或者该芯片包含功能电路、处理器核以及存储单元，前述任意一种方法的部分功能由功能电路这种硬件方式实现，另外部分功能由存储单元和处理器这种软件方式实现。

附图说明

[0059] 图1为本申请一实施例提供的计算机系统的结构示意图；

[0060] 图2为本申请另一实施例提供的计算机系统的结构示意图；

[0061] 图3为本申请一实施例提供的服务处理方法的流程图；

[0062] 图4为本申请另一实施例提供的服务处理方法的流程图；

[0063] 图5a为本申请另一实施例提供的计算机系统的结构示意图；

[0064] 图5b为本申请提供的采用图5a所示的计算机系统执行安全服务的流程图；

[0065] 图6为本申请另一实施例提供的计算机系统的架构示意图；

[0066] 图7为本申请另一实施例提供的服务处理方法的流程图；

[0067] 图8为本申请一实施例提供的电子设备的结构示意图；

[0068] 图9为本申请另一实施例提供的电子设备的结构示意图。

具体实施方式

[0069] 目前，为了解决移动安全问题，人们提出了TEE的概念，TEE具有以下安全特点：受

硬件机制保护、快速通信机制以及可抵御硬件攻击，因此，TEE广泛用于特定敏感数据的保护、移动支付服务以及安全认证等等。

[0070] 传统的方式中，实现TEE对设备的硬件性能要求较高，会导致引入较高的硬件成本。例如，基于Armv8M架构设计实现TEE时，需要设备具有能够支持Armv8M架构的内核，但通常支持Armv8M架构的内核成本较高。尤其是针对一些对成本以及性能较为敏感的设备来说，传统的方式无法适用，从而可能导致设备存在安全隐患。

[0071] 基于现有技术中存在的问题，本申请实施例提供一种计算机系统，该计算机系统通过设置轻量级的元器件，并利用该轻量级的元器件实现对目标存储空间的访问控制，使设备在特定的安全模式(例如TEE)下才能够访问目标存储空间，从而构建可靠性较高的TEE，并在TEE下执行系统调用的服务。本申请实施例提供的计算机系统，设计简单，可以适用于各种电子设备，例如，智能手机、IPAD、计算机、物联网设备、服务器等，具有较高的通用性。

[0072] 需要说明的是，本申请实施例描述的系统架构或应用场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对本申请实施例提供的技术方案的限定，本领域技术人员可知，随着系统架构的演变和新应用场景的出现，本申请实施例提供的技术方案针对类似的技术问题，同样适用。下面结合具体的实施例来进行详细说明。

[0073] 图1为本申请一实施例提供的计算机系统的结构示意图。如图1所示，该计算机系统100包括：中断状态寄存器101、权限管理寄存器102、处理器103以及目标存储空间104。

[0074] 其中，中断状态寄存器101用于标识中断状态。具体地，中断状态寄存器101可包括一个或多个标志位，每个标志位对应一个中断。中断被触发时，中断状态寄存器101中该中断对应的标志位被置位。需要说明的是，计算机系统调用目标服务触发中断可以通过控制中断触发寄存器的方式实现，具体地，计算机系统调用目标服务时，处理器通过控制中断触发寄存器，从而触发中断。

[0075] 权限管理寄存器102，用于控制目标存储空间104的访问权限。具体地，权限管理寄存器102可包括一个或多个标志位，每个标志位对应一个中断；若某个中断对应的标志位被置位，则表示该中断可以访问对应的目标存储空间104。其中，若权限管理寄存器102包括多个标志位，则表示该权限管理寄存器102可管理多个中断分别对其对应的目标存储空间104的访问权限。

[0076] 可选地，多个中断可对应不同的目标存储空间104，或者，多个中断也可以对应同一目标存储空间104，本申请实施例对此不作限制。

[0077] 在本方案中，该权限管理寄存器102无法被用户通过代码或其他方式直接访问，只有当第一中断被触发，处理器103跳转至第一中断的入口时，由处理器103自动置位。

[0078] 需要说明的是，在本方案中，中断状态寄存器101和权限管理寄存器102共同管理目标存储空间的访问权限。

[0079] 目标存储空间104用于存储第一信息，该第一信息能够用于执行目标服务。示例性地，该第一信息可以为根密钥，例如，该根密钥可以用于密钥派生，通过派生得到的密钥加密密钥、工作密钥等可以用于执行安全服务；又如，该根密钥还可以用于权限认证，权限认证通过后系统可以执行目标服务。当然，目标存储空间104的第一信息不仅可以为根密钥，还可以为其他信息或数据，上述仅为示例性描述，并不是对第一信息的限制。

[0080] 可选地,目标存储空间104可以包括非易失性存储和/或易失性存储中一个或多个存储单元。其中,非易失性存储是指当电流关掉后,所存储的数据不会消息的存储器,非易失性存储例如可以为可编程只读内存(programmable read-only memory,PROM)、电可改写只读内存(electrically alterable read only memory,EAROM)、可擦可编程只读内存(erasable programmable read only memory、EPROM)、电可擦可编程只读内存(electrically erasable programmable read only memory、EEPROM)、闪存(flash memory)、一次编程只读存储器(one time programmable read only memory,OTPROM)等等。易失性存储是指电流关掉后,无法保存数据的存储器,易失性存储例如为随机存取存储器(random-access memory,RAM)等。例如,RAM例如可以为静态随机存取存储器(Static Random-Access Memory,SRAM)、同步动态随机存取内存(synchronous dynamic random-access memory,SDRAM)等等。

[0081] 本申请实施例中,存储不同目标服务对应的第一信息的目标存储空间可根据目标服务的不同而具备差异,例如,一些目标服务对应的第一信息在任何情况下都不能被修改,则存储该目标服务对应的第一信息的目标存储空间可以为OTPROM;又如,一些目标服务对应的第一信息需要保持动态的变化,则存储该目标服务对应的第一信息的目标存储空间例如可以为EPROM。

[0082] 可选地,若目标存储空间包括多个存储单元,则该多个存储单元可以为连续的多个存储单元或不连续的多个存储单元。本申请实施例对此不作限制。

[0083] 本申请实施例中,目标存储空间包括的多个存储单元可以为连续的存储单元或不连续的存储单元,使本申请实施例提供的计算机系统具有较高的灵活性,可适用于各种类型的存储器。

[0084] 处理器103是实现运算的核心单元,能够实现数据的运算与处理。处理器103在运行的过程中,可以从存储单元中获取指令、数据,并完成代码运行、数据处理以及控制外设等工作。其中,处理器103,例如可以是中央处理器(central processing unit,CPU)、网络处理器(Network Processor,NP)或者CPU和NP的组合、图形处理器(graphics processing unit,GPU)、AI处理器、协处理器、微型处理器等等。

[0085] 在本方案中,处理器103用于根据目标服务触发的第一中断配置中断状态寄存器101中该第一中断对应的标志位为第一中断标志,以及配置权限管理寄存器102中第一中断对应的标志位为第一调用标志。

[0086] 可选地,该第一中断为NMI中断。NMI中断是中断请求的一种,本方案中,NMI中断是无法被禁止的。

[0087] 处理器103还用于根据第一中断标志和第一调用标志,确定是否允许处理器103访问目标存储空间104;若确定允许处理器103访问目标存储空间104,则处理器103还用于获取目标存储空间104的第一信息,并根据第一信息执行目标服务。

[0088] 一种可能的实现方式,处理器103可通过系统总线B1访问目标存储空间104,获取目标存储空间104的第一信息。系统总线B1是连接计算机系统的重要组件,系统总线B1上可以传输数据信息、地址信息以及控制信息等。在本方案中,处理器103可以通过系统总线B1访问目标存储空间104,并将目标存储空间104的第一信息读取至其他存储单元以执行目标服务。这里的其他存储单元可以为除目标存储空间外的任意存储单元。

[0089] 另一种可能的实现方式，处理器103可通过高速缓冲存储器(cache)B2访问目标存储空间104，获取目标存储空间104的第一信息。

[0090] 在一些情况下，系统总线B1和高速缓冲存储器B2可以同时存在。

[0091] 在本方案中，中断状态寄存器101和权限管理寄存器102共同管理目标存储空间104的访问权限，即第一中断对应的第一中断标志和第一中断对应的第一调用标志均被置位时，此时，系统由REE(或称为REE模式)进入TEE(或称为TEE模式)，处理器103能够在TEE中访问目标存储空间104。

[0092] 本实施例提供的计算机系统的工作流程如下：当系统调用目标服务时，系统在REE中根据目标服务触发第一中断；处理器103根据第一中断配置中断状态寄存器101中该第一中断对应的标志位为第一中断标志，即将断状态寄存器101第一中断对应的标志位置位；且处理器103根据第一中断配置权限管理寄存器102中该第一中断对应的标志位为第一调用标志，即将权限管理寄存器102中第一中断对应的标志位置位；处理器103根据第一中断标志以及第一调用标志确定被允许处理器103访问目标存储空间104时，此时，计算机系统由REE进入TEE，处理器103在TEE中获取目标存储空间104的第一信息，并在TEE中根据该第一信息执行目标服务。

[0093] 在实际应用中，计算机系统可能调用多个服务，每个服务触发一个中断。计算机系统可根据中断的类型或者服务的类型或者其他因素，预先为各个中断配置相应的优先级，则系统可按照中断的优先级顺序依次执行各个中断。

[0094] 若计算机系统当前存在多个未处理的中断时，则处理器103具体用于在根据目标服务触发第一中断时，配置中断状态寄存器101中第一中断对应的标志位为第一中断标志；并根据第一中断的优先级，配置权限管理寄存器102中第一中断对应的标志位为第一调用标志。

[0095] 这样的情况下，计算机系统的工作流程如下：当计算机系统调用目标服务时，系统在REE中根据目标服务触发第一中断；处理器103根据第一中断配置中断状态寄存器101中该第一中断对应的标志位为第一中断标志，即将中断状态寄存器101第一中断对应的标志位置位；处理器103根据第一中断的优先级确定第一中断是否为当前优先级最高的中断；若确定第一中断为当前优先级最高的中断，则处理器103配置权限管理寄存器102中该第一中断对应的标志位为第一调用标志，即将权限管理寄存器102中第一中断对应的标志位置位；若确定第一中断不是当前优先级最高的中断，则处理器103执行其他优先级高于第一中断的中断之后，再配置权限管理寄存器102中第一中断对应的标志位为第一调用标志；接着，处理器103根据第一中断标志以及第一调用标志确定被允许访问目标存储空间104时，此时，系统由REE进入TEE，处理器103在TEE中获取目标存储空间104的第一信息，并在TEE模式下根据该第一信息执行目标服务。

[0096] 在本实施例中，在计算机系统中设置轻量级的权限管理寄存器，并通过权限管理寄存器以及中断状态寄存器共同管理目标存储空间的访问权限，使对目标存储空间的访问只能够在特定安全模式(例如TEE)下实现，从而搭建了安全性较高的TEE。本实施例提供的计算机系统可以应用于各种芯片架构中，设计简单，通用性较高，且权限管理寄存器的成本较低，需要的逻辑电路的规模和体积较小，在实现可靠的可信执行环境的同时有效降低了芯片成本。

[0097] 图2为本申请另一实施例提供的计算机系统的结构示意图。如图2所示，本实施例提供的计算机系统在图1所示实施例的基础上，计算机系统还包括：内存保护单元106。

[0098] 其中，内存保护单元106，用于配置目标存储空间104的第二调用标志。其中，第一中断标志、第一调用标志以及第二调用标志共同指示是否允许访问目标存储空间104。在本方案中，内存保护单元106能够提供目标存储空间104的访问权限的管理，具体包括：读、写、执行以及域锁闭权限。可选地，内存保护单元106还可以用于配置其他存储空间的访问权限，其他存储空间为与目标存储空间不同的存储空间，例如，内存保护单元106可以配置内存区域的保护权限。

[0099] 示例性地，内存保护单元106是能够提供系统资源硬件访问权限管理的单元。内存保护单元106，例如可以为ARM的MPU单元，或者还可以为Risc V的PMP单元，当然，内存保护单元106还可以其他类型的单元，其只要具备能够提供系统资源硬件访问权限管理的功能即可。

[0100] 例如，内存保护单元106为处理器103配置的系统资源的访问权限可如表1所示：

[0101] 表1

[0102]

	非第一中断	第一中断
普通内存	(RWXL)	(RWXL)
外设空间	(RWXL)	(RWXL)
目标存储空间	-	(RWXL)
中断向量表	(R)XL	(R)XL
中断处理函数	(R)XL	(R)XL

[0103] 在表1中，R表示读权限，W表示写权限，X表示执行权限，L表示配置域锁闭。

[0104] 如表1中所示访问权限，处理器103可在第一中断下以及非第一中断下，对普通内存以及外设空间都具备上述读写执行以及配置域锁闭权限。处理器103仅在第一中断下不具备对目标存储空间104的读写执行以及配置域锁闭权限。处理器103在第一中断下以及非第一中断下，对中断向量表以及中断处理函数具备读权限，且中断向量表和中断处理函数具备执行权限以及配置域锁闭权限。

[0105] 需要说明的是，内存保护单元106还可配置中断向量表和中断处理函数的访问权限，具体如表1中所示。当然，内存保护单元106也可以为目标存储空间、中断向量表和中断处理函数配置其他访问权限，例如，处理器103在第一中断下以及非第一中断下，对中断向量表以及中断处理函数不具备读权限，但中断向量表和中断处理函数具备执行权限以及配置域锁闭权限。

[0106] 在实际应用中，针对不同的系统资源，上述权限可以根据实际需要进行组合，例如，对目标存储空间，可配置处理器103在第一中断下具备读权限，不具备写权限、执行权限以及配置域锁闭权限；对中断向量表和中断处理函数，可配置处理器103在第一中断和非第一中断下均执行权限和配置域锁闭权限，不具备读权限。

[0107] 可选地，内存保护单元106可在系统初始化阶段或者系统处于空闲状态，配置系统资源的访问权限。具体地，内存保护单元106可以在系统初始化阶段或者系统处于空闲状态，配置处理器103对目标存储空间104的访问权限，该权限可如表1中所示。

[0108] 可选地，内存保护单元106管理目标存储空间104配置的访问权限的优先级高于权

限管理寄存器102和中断状态寄存器101共同管理的目标存储空间104的访问权限，即第二调用标志的优先级高于第一调用标志和第一中断标志的优先级。

[0109] 具体地，若第二调用标志指示不允许处理器103访问目标存储空间104，则无论第一调用标志和第一中断标志共同决定是否允许处理器103访问目标存储空间104，处理器103都无法访问目标存储空间104。

[0110] 若第二调用标志指示允许处理器103访问目标存储空间104，第一调用标志和第一中断标志共同决定允许处理器103访问目标存储空间104，则处理器103可在进入第一中断时访问目标存储空间104。这样的情况说明系统当前处于TEE模式，处理器103执行的是可信操作。

[0111] 若第二调用标志指示允许处理器103访问目标存储空间104，但第一调用标志和第一中断标志共同决定不允许处理器103访问目标存储空间104，则处理器103无法访问目标存储空间104。这样的情况可能是由于处理器103处于非第一中断造成的，此时这样的权限管理机制保护了目标存储空间104中的第一信息无法被篡改，保护了系统的安全。

[0112] 本实施例中，在计算机系统中设置轻量级的权限管理寄存器，并通过权限管理寄存器以及中断状态寄存器共同管理目标存储空间的访问权限，使对目标存储空间的访问只能够在特定的TEE模式下实现，从而搭建了安全性较高的TEE。本实施例提供的计算机系统可以应用于各种芯片架构中，通用性较高，且权限管理寄存器的成本较低，在实现可靠的可信执行环境的同时有效降低了芯片成本。本实施例提供的计算机系统通过进一步设置内存保护单元，并通过内存保护单元共同管理目标存储空间的访问权限，进一步提高了服务系统的安全性。

[0113] 可选地，在图1以及图2所示实施例的基础上，处理器103还用于复位中断状态寄存器中第一中断对应的标志位。具体地，处理器103可在根据第一信息执行目标服务之后，复位中断状态寄存器中第一中断对应的标志位。本方案中，通过在TEE模式下复位中断状态寄存器中第一中断对应的标志位，从而保护了目标存储空间，减小了计算机系统的攻击面。

[0114] 可选地，在图1以及图2所示实施例的基础上，处理器103还用于根据第一中断清除和释放目标服务调用的资源。具体地，处理器103可在根据第一信息执行目标服务之后，根据第一中断调用相关的程序，从而清除和释放目标服务调用的系统资源。

[0115] 可选地，在图1以及图2所示实施例的基础上，处理器103还用于复位权限管理寄存器中第一中断对应的标志位。具体地，处理器103可在执行完目标服务，并清除和释放目标服务调用的资源之后，复位权限管理寄存器中第一中断对应的标志位，并退出第一中断。

[0116] 可选地，计算机系统退出第一中断后，还可以向目标服务的调用者返回目标服务的处理结果。具体地，若目标服务是用户应用触发的，则该计算机系统向用户应用返回处理结果；若目标服务是操作系统触发，则该计算机系统向操作系统返回处理结果。

[0117] 计算机系统通过执行上述复位中断状态寄存器以及权限管理寄存器中第一中断对应的标志位，清除和释放目标服务调用的资源，退出第一中断，并返回目标服务的处理结果，完成整个目标服务的处理过程。

[0118] 可选地，在图1以及图2所示实施例的基础上，计算机系统100还包括：外设105；其中，外设105(也可以称为外部设备、外围设备等其他名称)是指芯片内部控制外围设备、总线的控制器，外设105例如I2C(inter－integrated circuit)总线控制器、安全数字输入输

出卡(secure digital input and output card,SDIO)总线控制器等。

[0119] 图3为本申请一实施例提供的服务处理方法的流程图。本实施例提供的服务处理方法可应用于上述图1或图2所示的计算机系统。如图3所示,本实施例的方法包括:

[0120] S101、调用目标服务,并根据目标服务触发第一中断。

[0121] 具体地,计算机系统在REE中调用目标服务,并根据目标服务触发第一中断;其中,目标服务可以是通过用户应用触发的,该用户应用例如可以为第三方应用,或者还可以为系统应用。

[0122] 具体地,计算机系统可以在REE线程模式下调用目标服务,并在根据目标服务触发第一中断。可选地,该第一中断可以为NMI中断。其中,线程模式为一般代码运行时,处理器的工作模式,可以是内核态或用户态(user mode)。内核态和用户态是处理器的工作模式,内核态和用户态是一种能够用来保护数据和阻止恶意行为的机制。

[0123] S102、根据第一中断配置第一中断标志和第一调用标志。

[0124] 具体地,计算机系统的处理器根据目标服务触发的第一中断配置中断状态寄存器中第一中断对应的第一中断标志,并根据第一中断配置权限管理寄存器中第一中断对应的第一中断标志。其中,关于中断状态寄存器以及权限管理寄存器可参照上述图1所示实施例中的详细描述,此处不再赘述。

[0125] 具体地,处理器根据第一中断配置中断状态寄存器中第一中断对应的第一中断标志,以及配置权限管理寄存器中第一中断对应的第一中断标志的过程是由硬件控制的,软件是无法访问的。通过这样的方式,保证了权限管理寄存器在工作过程中的安全性,从而实现安全的访问环境。

[0126] S103、根据第一中断标志和第一调用标志确定是否允许访问目标存储空间。

[0127] 本方案中,第一中断标志和第一调用标志用于指示是否允许处理器访问目标存储空间。若处理器根据第一中断标志和第一调用标志确定允许处理器访问目标存储空间,则执行S104;若处理器根据第一中断标志和第一调用标志确定不允许处理器访问目标存储空间,则计算机系统可返回指示拒绝执行目标服务的相关指示信息,返回指示拒绝执行目标服务的相关指示信息可以保证计算机系统对于中断的处理具有正确的响应,同时保证目标存储空间存储的第一信息的安全性。

[0128] S104、在TEE模式获取目标存储空间的第一信息。

[0129] 具体地,若处理器根据第一中断标志和第一调用标志确定允许处理器访问目标存储空间,则计算机系统由REE模式进入TEE模式;计算机系统在TEE模式下获取目标存储空间的第一信息,并在TEE模式下根据中断向量表跳转至相应的中断入口。

[0130] 处理器可在TEE模式下通过系统总线或cache访问目标存储空间,并获取目标存储空间的第一信息。其中,目标存储空间的第一信息可参照上文中的详细描述,此处不再赘述。

[0131] S105、根据第一信息执行目标服务。

[0132] 具体地,计算机系统根据第一信息执行目标服务相关的处理。示例性地,第一信息为根密钥,则计算机系统可根据根密钥执行权限认证、密钥派生等相关操作,并可根据密钥派生得到的密钥加密密钥、工作密钥等执行目标服务。

[0133] 需要说明的是,计算机系统执行S104以及S105时,处理器可以工作在TEE handler

模式，其中，handler模式是中断、异常处理时处理器的工作模式，通常为内核态。由于应用程序无法自由进入内核态，只能够通过系统提供的接口调用进入或者中断被动进入，因此，处理器在TEE handler模式执行目标服务，能够防止应用程序进行越权的操作，保证目标服务的安全性。

[0134] 需要说明的是，处理器的工作模式可以根据处理器的架构或设计而不同，本实施例中所示仅为示例。

[0135] 本实施例提供的服务处理方法，通过第一调用标志和第一中断标志共同管理目标存储空间的访问权限，使对目标存储空间的访问只能够在特定安全模式(例如TEE模式)下实现，从而搭建了安全性较高的安全访问环境。本实施例提供的服务处理方法可通过在各种芯片架构中增加轻量级的权限管理寄存器实现，设计较为简单，通用性较高，且权限管理寄存器的成本较低，在实现可靠的安全访问环境的同时有效降低了芯片成本。

[0136] 图4为本申请另一实施例提供的服务处理方法的流程图。如图4所示，本实施例的方法包括：

[0137] S201、调用目标服务，并根据目标服务触发第一中断。

[0138] 本实施例中步骤S201与图3所示实施例中S101类似，可参照图3所示实施例中的详细描述，此处不再赘述。

[0139] 图3所示实施例中S102可以包括本实施例中的S202-S205。

[0140] S202、根据第一中断配置第一中断标志。

[0141] S203、确定第一中断是否为当前优先级最高的中断。若确定不是，则执行S204以及S205；若确定是，则执行S205。

[0142] S204、执行优先级高于第一中断的中断。

[0143] 示例性地，计算机系统可以在REE handler模式下执行优先级高于第一中断的中断，需要说明的是，计算机系统是在REE handler模式下执行优先级高于第一中断的中断，或者是在TEE handler模式下执行优先级高于第一中断的中断，可根据要执行的中断确定，或者可根据要执行的中断对应的服务确定，或者也可以是系统指定的模式下执行，本申请实施例对此不作限制。本实施例中仅是示例，并不是对执行优先级高于第一中断的中断时，处理器的工作模式的限制。

[0144] S205、根据第一中断配置第一调用标志。

[0145] 由于计算机系统当前可能存在多个未执行的中断，则计算机系统可根据第一中断的优先级，配置权限管理寄存器中第一中断对应的标志位为第一调用标志。其中，根据第一中断的优先级配置第一调用标志满足的原则为：第一中断为当前优先级最高的中断时，配置权限管理寄存器中该第一中断对应的标志位为第一调用标志。

[0146] S206、根据第一中断标志和第一调用标志确定是否允许访问目标存储空间。

[0147] 本方案中，第一中断标志和第一调用标志用于指示是否允许处理器访问目标存储空间。若处理器根据第一中断标志和第一调用标志确定允许处理器访问目标存储空间，则执行S104；若处理器根据第一中断标志和第一调用标志确定不允许处理器访问目标存储空间，则计算机系统可返回指示拒绝执行目标服务的相关指示信息，返回指示拒绝执行目标服务的相关指示信息可以保证计算机系统对于中断的处理具有正确的响应，同时保证目标存储空间存储的第一信息的安全性。

[0148] S207、在TEE模式获取目标存储空间的第一信息。

[0149] S208、根据第一信息执行目标服务。

[0150] 本实施例中的步骤S206-S208分别与图3所示实施例中的S103-S106类似，可参照图3所示实施例的详细描述，此处不再赘述。

[0151] 本实施例提供的服务处理方法，通过第一调用标志和第一中断标志共同管理目标存储空间的访问权限，使对目标存储空间的访问只能够在特定的安全模式(例如，TEE模式)下实现，从而搭建了安全性较高的TEE。本实施例提供的服务处理方法可通过在各种芯片架构中增加轻量级的权限管理寄存器实现，设计较为简单，通用性较高，且权限管理寄存器的成本较低，在实现可靠的安全访问环境的同时有效降低了芯片成本。

[0152] 可选地，在一些实施例中，S208根据第一信息执行目标服务之后，还可以包括：

[0153] S209、复位第一中断标志。

[0154] S210、根据第一中断清除和释放目标服务调用的资源。

[0155] S211、复位第一调用标志。

[0156] S213、退出第一中断。

[0157] S213、返回目标服务。

[0158] 在实际应用中，计算机系统可通过执行上述复位中断状态寄存器以及权限管理寄存器中第一中断对应的标志位，清除和释放目标服务调用的堆、栈中涉及的敏感信息和中间结果等，退出第一中断，并返回目标服务的处理结果，完成整个目标服务的处理过程。

[0159] 需要说明的是，在一些实施例中，S209也可在S208之前执行。具体地，若系统确认无需再访问目标存储空间时，则可以执行S209，这样的情况下，S209可与S208并行执行，或者S209也可在S208之前执行。其中，在执行复位第一中断标志之前，处理器可根据第一中断标志和第一调用标志多次访问目标存储空间。

[0160] 在一个具体的实施例中，结合图5a以及图5b对本申请实施例提供的计算机系统以及服务处理方法进行详细说明。其中，图5a示出了计算机系统的结构示意图；图5b示出了采用图5a所示的计算机系统执行安全服务的处理流程。

[0161] 参照图5a所示，该计算机系统包括：CPU、NMI状态寄存器、权限管理寄存器、PMP单元以及目标存储空间(即图5a中所示的eFuse)。可选地，该计算机系统还可以包括：SRAM、Flash eFuse以及外设。

[0162] 在图5a所示的计算机系统中，CPU通过系统总线与eFuse、SRAM、Flash eFuse以及外设连接，CPU可通过系统总线访问eFuse、SRAM、Flash eFuse以及外设。

[0163] NMI状态寄存器，系统启动后默认清零，在触发NMI中断后置位。

[0164] 权限管理寄存器，系统启动后默认清零，且软件不可访问；权限管理寄存器在系统跳转至NMI中断入口时，由CPU自动置位。

[0165] NMI状态寄存器和权限管理寄存器均置位时，系统总线和高速缓冲存储器(cache)才被允许访问目标存储空间；即NMI状态寄存器和权限管理寄存器均置位时，CPU才被允许通过系统总线或高速缓冲存储器访问eFuse。

[0166] 在计算机系统包括PMP单元的情况下，PMP单元可以配置系统资源的访问权限，即PMP单元可以对eFuse、SRAM、Flash eFuse以及外设进行访问权限控制。具体地，在PMP单元配置CPU具备对eFuse访问权限的前提下，NMI状态寄存器和权限管理寄存器均置位时，CPU

才被允许访问eFuse，若PMP单元配置CPU不具备对eFuse的访问权限，则NMI状态寄存器和权限管理寄存器无论是否被置位，CPU都无法访问eFuse。

[0167] 目标存储空间(eFuse)内存储设备的根密钥，该根密钥即为前述实施例中描述的第一信息，在本实施例中，根密钥用于执行安全服务。且本实施例中，利用eFuse只能编辑一次的特性达到根密钥的不可篡改。

[0168] 在图5a所示的实施例中，eFuse存储的根密钥可以用于进行安全服务，例如：执行关键数据加解密、密钥加密、密钥管理、证书管理等。结合图5a以及图5b所示，当调用安全服务时，计算机系统通过TEE客户端接口eFuse存储的根密钥；根据根密钥进行密钥管理，获得工作密钥，根据工作密钥执行相应的安全服务。

[0169] 在另一个具体的实施例中，结合图6以及图7对用户任务申请加密存储以存储敏感数据进行详细说明。其中，图6中示出了执行安全存储服务时的计算机系统的架构图；图7示出了执行该安全服务的处理流程。

[0170] 参照图6所示，在软件层，用户基于操作系统可运行N个用户任务，其中，N为正整数；用户任务1在运行过程中，可以申请安全存储服务，并触发NMI中断，其中，该安全存储服务的目的是对敏感数据进行加密存储，安全存储服务即为上述实施例中的目标服务。在硬件层，包括CPU、权限管理寄存器、中断状态寄存器、eFuse以及Flash，其中，eFuse中存储根密钥，Flash可以存储根据根密钥派生的密钥加密密钥以及工作密钥，Flash还可以存储根据工作密钥对敏感数据进行加密得到的密文。

[0171] 在图6所示的系统架构的基础上，执行安全存储服务可以参照图7所示，具体可以包括以下步骤：

[0172] S301、中断状态寄存器以及权限管理寄存器执行初始化。

[0173] 具体地，中断状态寄存器以及权限管理寄存器可在系统上电时，由硬件自动清零。

[0174] S302、加载镜像代码。

[0175] 镜像代码可以包括但不限于为中断向量表、可执行代码等。

[0176] S303、配置PMP保护。

[0177] 具体地，通过PMP单元配置系统资源的访问权限，例如，配置中断向量表以及NMI处理函数的访问权限为可读、可执行、不可写，并锁闭寄存器。

[0178] S304、系统执行其他模块或单元的初始化。

[0179] S305、启动操作系统并运行用户应用。

[0180] S306、确定申请安全存储服务时，调用TEE客户端接口。

[0181] 具体地，运行用户应用的过程中，确定需要提供安全存储服务时，用户应用通过TEE客户端接口(TEE Client API)传入服务类型、明文地址、密文存储地址等用于安全存储服务的参数，从而申请安全存储服务。

[0182] S307、生成数据报文，并触发NMI中断。

[0183] 具体地，TEE Client API可以先验证上述参数的合法性，并在验证通过后根据上述参数以及其他信息生成数据报文，触发NMI中断。

[0184] S308、读取根密钥。

[0185] 具体地，CPU根据NMI中断，将中断状态寄存器中该NMI中断对应的标志位置位，并将权限管理管理寄存器中该NMI中断对应的标志位置位；接着，CPU根据NMI中断对应的中断

标志以及调用标志，确定是否允许CPU访问eFuse中存储的根密钥；若确定允许CPU访问eFuse，则CPU读回eFuse中存储的根密钥。

[0186] 需要说明的是，若计算机系统当前存在多个未执行的中断，则CPU将中断状态寄存器中该NMI中断对应的标志位进行置位，并确定该NMI中断是否为当前优先级最高的中断，若是，则将权限管理管理寄存器中该NMI中断对应的标志位置位；若不是，则CPU执行优先级高于该NMI中断的其他中断后，将权限管理管理寄存器中该NMI中断对应的标志位置位。

[0187] S309、复位中断状态寄存器中NMI中断对应的标志位。

[0188] S310、根据根密钥生成密钥加密密钥，并根据密钥加密密钥生成工作密钥A。

[0189] 具体地，CPU根据根密钥获得密钥加密密钥，使用密钥加密密钥结合步骤S307中生成的数据报文，解密获得该安全存储服务所需的工作密钥A。

[0190] 在实际应用中，一个服务可以对应多个工作密钥，多个不同的服务也可以对应同一个工作密钥，工作密钥的选择以及派生与调用服务时，通过TEE Client API获取的相关。

[0191] S311、根据工作密钥A执行安全存储服务。

[0192] 具体地，根据工作密钥A以及数据报文中包括的明文信息以及密文存储地址，执行明文信息的加密以及存储。

[0193] S312、清除和释放安全存储服务调用的资源。

[0194] 具体地，清除执行安全存储服务时使用的堆、栈中涉及的敏感信息以及中间结果等。

[0195] S313、退出NMI中断。

[0196] S314、复位权限管理寄存器中NMI中断对应的标志位。

[0197] 之后，可返回用户应用。

[0198] 在上述过程中，S309也可以在S310或S311之后执行，并不限于上述的执行顺序。

[0199] 在该实施例中，本实施例通过权限管理寄存器构建轻量级的TEE，使eFuse中存储的根密钥的访问依赖于权限管理寄存器以及中断状态寄存器的共同管理，只有当中断状态寄存器以及权限管理寄存器中该NMI中断对应的标志位均置位时，系统由REE模式进入TEE模式，CPU在TEE模式下通过系统总线或cache访问eFuse，获取其中的根密钥，并在TEE模式下执行安全存储服务。且eFuse只能编辑一次的特性使根密钥无法被篡改，保证了工作密钥的可靠性。

[0200] 图8为本申请另一实施例提供的一种电子设备的结构示意图。如图8所示，本实施例所述的电子设备800可以是前述方法实施例中提到的终端设备(或者可用于终端设备的部件)或者网络设备(或者可用于网络设备的部件)。电子设备可用于实现上述方法实施例中描述的计算机系统执行的方法，具体参见上述方法实施例中的说明。

[0201] 所述电子设备800可以包括一个或多个处理器801，所述处理器801也可以称为处理单元，可以实现一定的控制或者处理功能。所述处理器801可以是通用处理器或者专用处理器等。例如可以是基带处理器、或中央处理器。基带处理器可以用于对通信协议以及通信数据进行处理，中央处理器可以用于对电子设备进行控制，执行软件程序，处理软件程序的数据。

[0202] 在一种可选的设计中，处理器801也可以存有指令803或者数据(例如中间数据)。其中，所述指令803可以被所述处理器运行，使得所述电子设备执行上述方法实施例中描述

的对应于终端设备或者网络设备的方法。

[0203] 在又一种可能的设计中,电子设备可以包括电路,所述电路可以实现前述方法实施例中发送或接收或者通信的功能。

[0204] 可选的,所述电子设备中可以包括一个或多个存储器802,其上可以存有指令804,所述指令可在所述处理器上被运行,使得所述电子设备执行上述方法实施例中描述的方法。

[0205] 可选的,所述存储器中也可以是存储有数据。所述处理器和存储器可以单独设置,也可以集成在一起。

[0206] 可选的,所述电子设备800还可以包括收发器805和/或天线806。所述处理器801可以称为处理单元,对电子设备(终端设备或者网络设备)进行控制。所述收发器805可以称为收发单元、收发机、收发电路、或者收发器等,用于实现电子设备的收发功能。

[0207] 在一个设计中,若该电子设备800用于实现上述各实施例中计算机系统的操作时,例如,可以由处理器801调用目标服务,并根据所述目标服务触发的第一中断配置第一中断标志和第一调用标志,其中,所述第一中断标志和所述第一调用标志用于指示是否允许访问目标存储空间;若根据所述第一中断标志和所述第一调用标志,确定允许访问所述目标存储空间,则在TEE模式获取所述目标存储空间的第一信息;以及根据第一信息执行上述目标服务。

[0208] 其中,上述处理器801具体实现过程可以参见上述各实施例的相关描述,此处不再赘述。

[0209] 本申请中描述的处理器801和收发器805可实现在集成电路(integrated circuit,IC)、模拟IC、射频集成电路(radio frequency integrated circuit,RFIC)、混合信号IC、专用集成电路(application specific integrated circuit,ASIC)、印刷电路板(printed circuit board,PCB)、电子设备等上。该处理器和收发器也可以用各种IC工艺技术来制造,例如互补金属氧化物半导体(complementary metal oxide semiconductor,CMOS)、N型金属氧化物半导体(nMetal-oxide-semiconductor,NMOS)、P型金属氧化物半导体(positive channel metal oxide semiconductor,PMOS)、双极结型晶体管(Bipolar Junction Transistor,BJT)、双极CMOS(BiCMOS)、硅锗(SiGe)、砷化镓(GaAs)等。

[0210] 虽然在以上的实施例描述中,电子设备以终端设备或者网络设备为例来描述,但本申请中描述的电子设备的范围并不限于上述终端设备或网络设备,而且电子设备的结构可以不受图8的限制。电子设备可以是独立的设备或者可以是较大设备的一部分。例如所述设备可以是:

[0211] (1)独立的集成电路IC,或芯片,或,芯片系统或子系统;

[0212] (2)具有一个或多个IC的集合,可选的,该IC集合也可以包括用于存储数据和/或指令的存储部件;

[0213] (3)ASIC,例如调制解调器(MSM);

[0214] (4)可嵌入在其他设备内的模块;

[0215] (5)接收机、无线设备、移动单元,网络设备等等;

[0216] (6)其他等等。

[0217] 图9为本申请另一实施例提供的电子设备的结构示意图。该终端设备可包括本申

请上述各实施例中所述的计算机系统。为了便于说明，图9仅示出了终端设备的主要部件。如图9所示，终端设备900包括处理器、存储器、控制电路、天线以及输入输出装置。处理器主要用于对通信协议以及通信数据进行处理，以及对整个终端设备进行控制，执行软件程序，处理软件程序的数据。存储器主要用于存储软件程序和数据。射频电路主要用于基带信号与射频信号的转换以及对射频信号的处理。天线主要用于收发电磁波形式的射频信号。输入输出装置，例如触摸屏、显示屏，键盘等主要用于接收用户输入的数据以及对用户输出数据。

[0218] 当终端设备开机后，处理器可以读取存储单元中的软件程序，解释并执行软件程序的指令，处理软件程序的数据。当需要通过无线发送数据时，处理器对待发送的数据进行基带处理后，输出基带信号至射频电路，射频电路将基带信号进行射频处理后将射频信号通过天线以电磁波的形式向外发送。当有数据发送到终端时，射频电路通过天线接收到射频信号，将射频信号转换为基带信号，并将基带信号输出至处理器，处理器将基带信号转换为数据并对该数据进行处理。

[0219] 本领域技术人员可以理解，为了便于说明，图9仅示出了一个存储器和处理器。在实际的终端中，可以存在多个处理器和存储器。存储器也可以称为存储介质或者存储设备等，本申请实施例对此不做限制。

[0220] 作为一种可选的实现方式，处理器可以包括基带处理器和中央处理器，基带处理器主要用于对通信协议以及通信数据进行处理，中央处理器主要用于对整个终端设备进行控制，执行软件程序，处理软件程序的数据。图9中的处理器集成了基带处理器和中央处理器的功能，本领域技术人员可以理解，基带处理器和中央处理器也可以是各自独立的处理器，通过总线等技术互联。本领域技术人员可以理解，终端设备可以包括多个基带处理器以适应不同的网络制式，终端设备可以包括多个中央处理器以增强其处理能力，终端设备的各个部件可以通过各种总线连接。所述基带处理器也可以表述为基带处理电路或者基带处理芯片。所述中央处理器也可以表述为中央处理电路或者中央处理芯片。对通信协议以及通信数据进行处理的功能可以内置在处理器中，也可以以软件程序的形式存储在存储单元中，由处理器执行软件程序以实现基带处理功能。

[0221] 在一个例子中，可以将具有收发功能的天线和控制电路视为终端设备900的收发模块901，将具有处理功能的处理器视为终端设备900的处理模块902。如图9所示，终端设备900包括收发模块901和处理模块902。收发模块901也可以称为收发器、收发机、收发装置等。可选的，可以将收发模块901中用于实现接收功能的器件视为接收模块，将收发模块901中用于实现发送功能的器件视为发送模块，即收发模块901包括接收模块和发送模块示例性的，接收模块也可以称为接收机、接收器、接收电路等，发送模块可以称为发射机、发射器或者发射电路等。

[0222] 需要说明的是，本申请实施例中对模块的划分是示意性的，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。在本申请的实施例中的各功能模块可以集成在一个处理模块中，也可以是各个模块单独物理存在，也可以两个或两个以上模块集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。

[0223] 所述集成的模块如果以软件功能模块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)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。

[0224] 在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时,可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时,全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质,(例如,软盘、硬盘、磁带)、光介质(例如,DVD)、或者半导体介质(例如固态硬盘Solid State Disk(SSD))等。

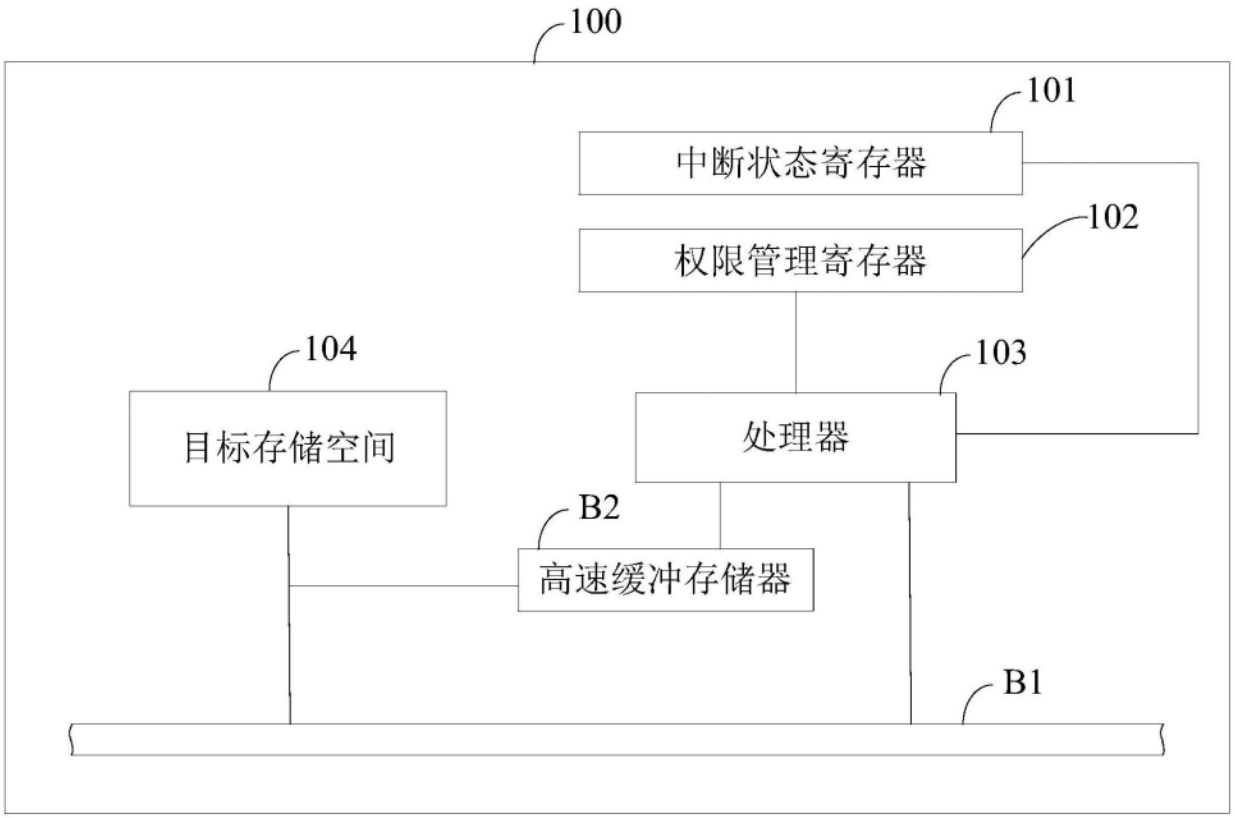

100
101
中断状态寄存器
102
权限管理寄存器
104
103
目标存储空间
处理器
B2
高速缓冲存储器
B1

图1

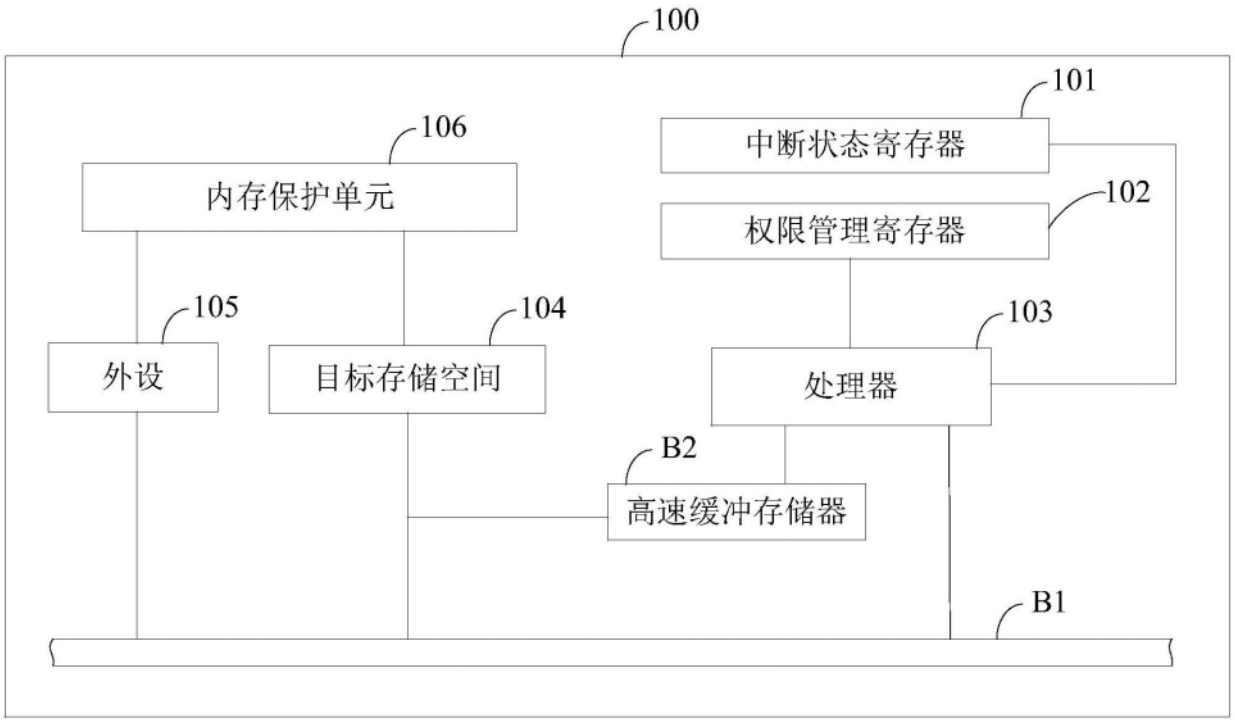

100
101
106
中断状态寄存器
内存保护单元
102
权限管理寄存器
105
104
103
外设
目标存储空间
处理器
B2
高速缓冲存储器
B1

图2

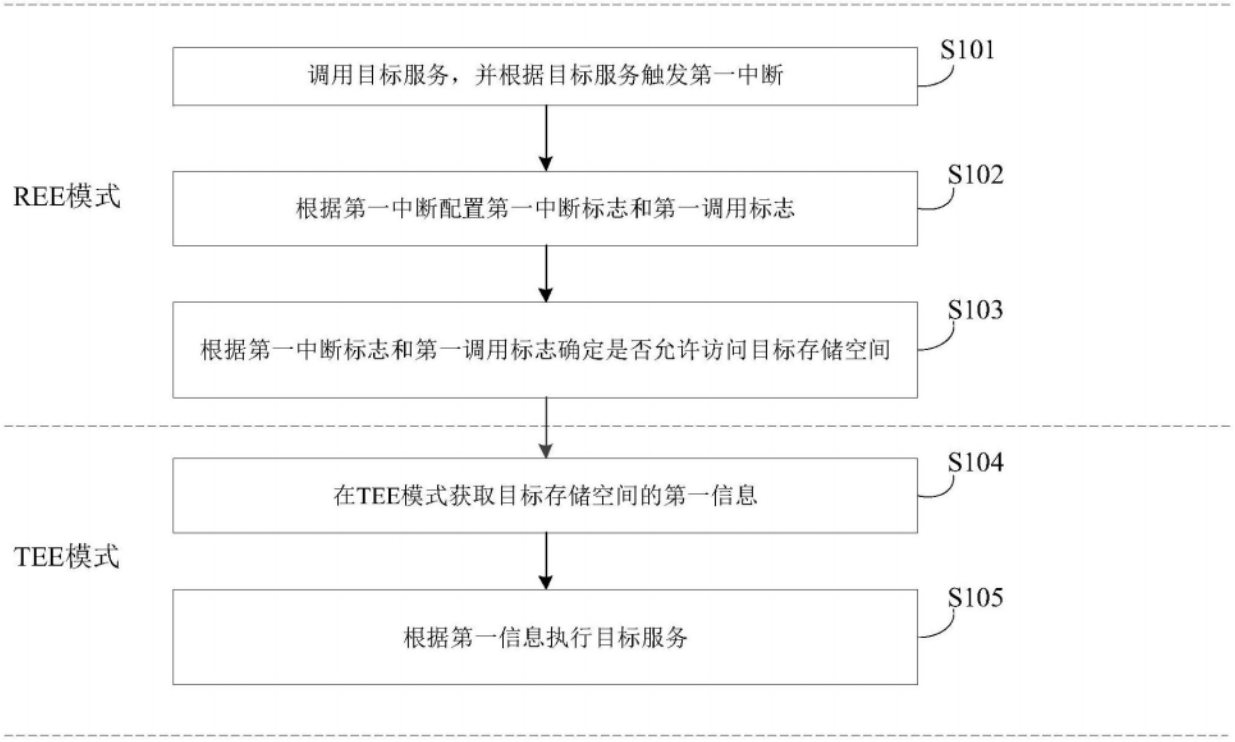

REE模式
调用目标服务，并根据目标服务触发第一中断
S101
根据第一中断配置第一中断标志和第一调用标志
S102
根据第一中断标志和第一调用标志确定是否允许访问目标存储空间
S103
TEE模式
在TEE模式获取目标存储空间的第一信息
S104
根据第一信息执行目标服务
S105

图3

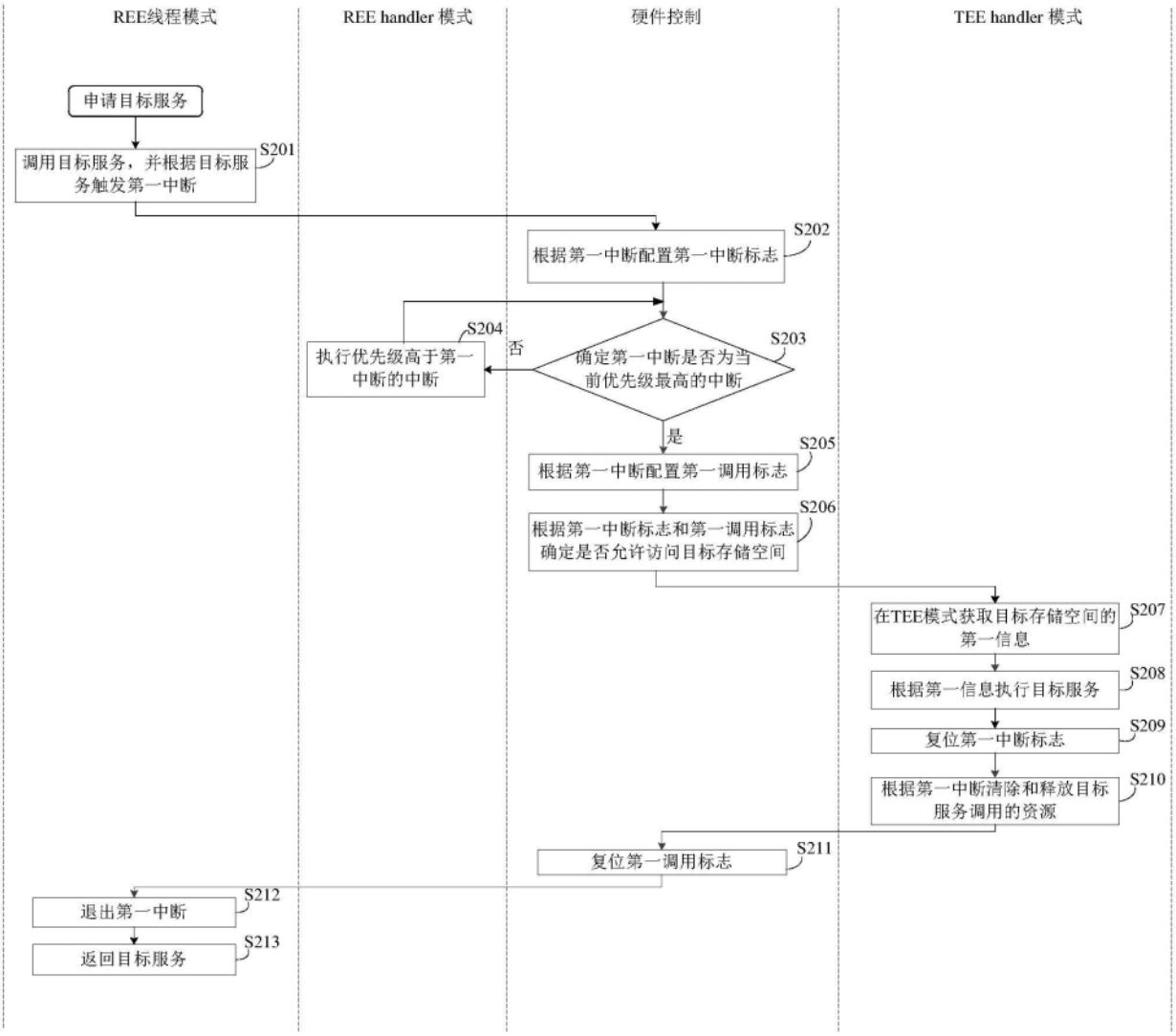

REE线程模式
REE handler 模式
硬件控制
TEE handler 模式
申请目标服务
调用目标服务，并根据目标服务触发第一中断
S201
根据第一中断配置第一中断标志
S202
确定第一中断是否为当前优先级最高的中断
S203
否
执行优先级高于第一中断的中断
S204
是
根据第一中断配置第一调用标志
S205
根据第一中断标志和第一调用标志确定是否允许访问目标存储空间
S206
在TEE模式获取目标存储空间的第一信息
S207
根据第一信息执行目标服务
S208
复位第一中断标志
S209
根据第一中断清除和释放目标服务调用的资源
S210
复位第一调用标志
S211
退出第一中断
S212
返回目标服务
S213

图4

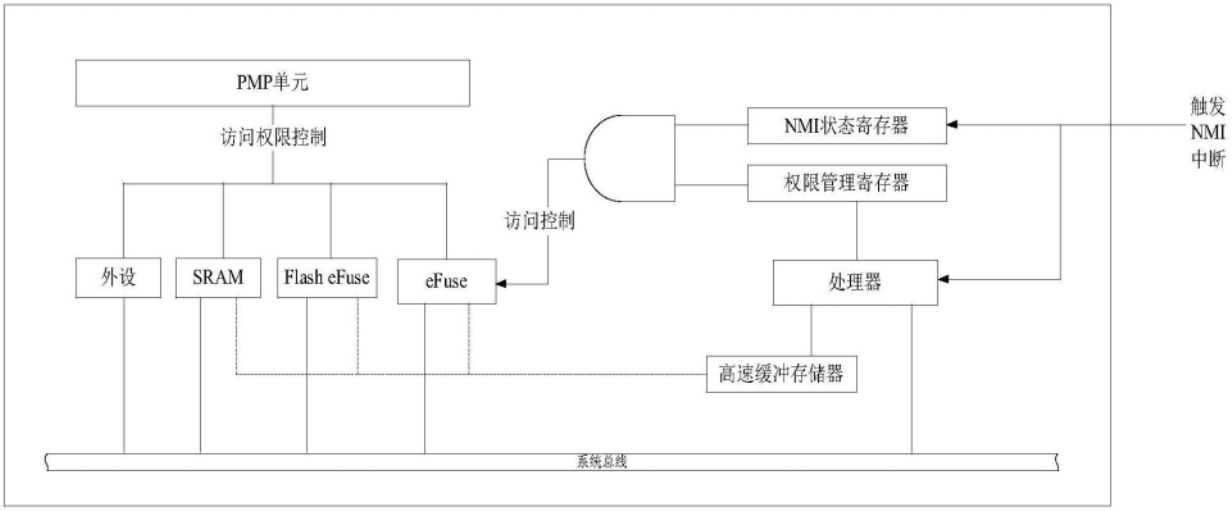

PMP单元
访问权限控制
外设
SRAM
Flash eFuse
eFuse
访问控制
NMI状态寄存器
权限管理寄存器
处理器
触发
NMI
中断
高速缓冲存储器
系统总线

图5a

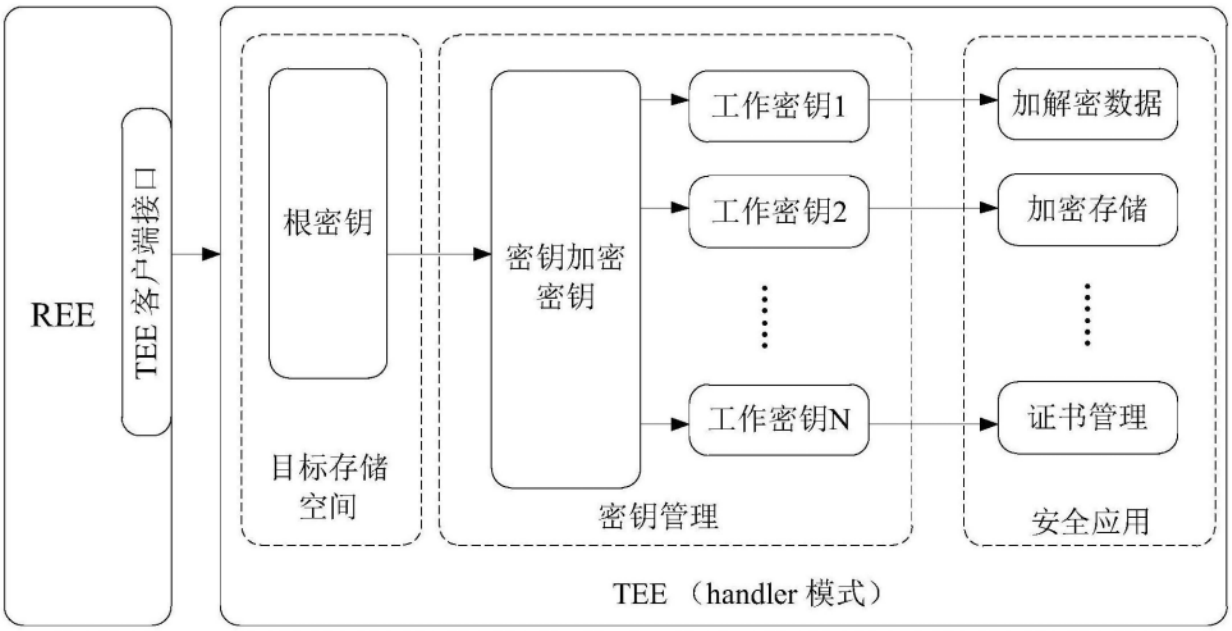

REE
TEE 客户端接口
根密钥
目标存储
空间
密钥加密
密钥
工作密钥1
工作密钥2
工作密钥N
密钥管理
加解密数据
加密存储
证书管理
安全应用
TEE （handler 模式）

图5b

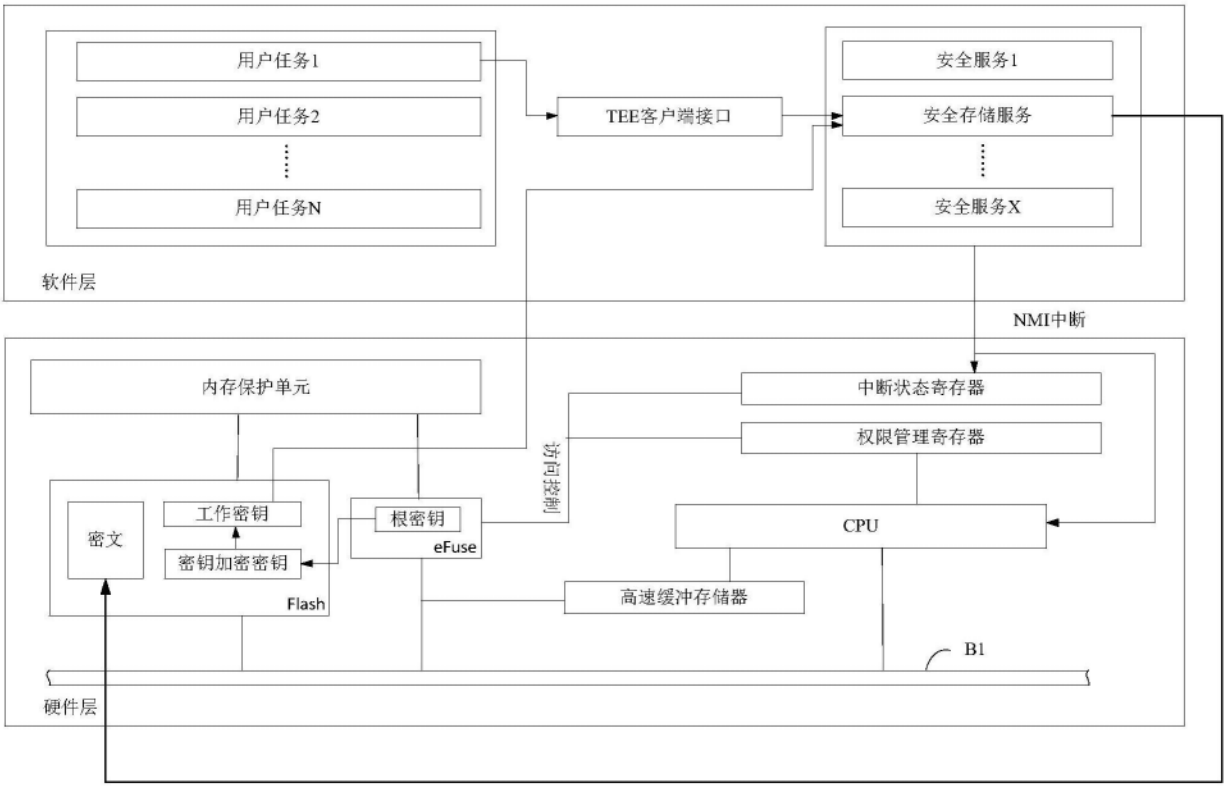

用户任务1
用户任务2
用户任务N
TEE客户端接口
安全服务1
安全存储服务
安全服务X
软件层
NMI中断
内存保护单元
中断状态寄存器
权限管理寄存器
访问控制
密文
工作密钥
密钥加密密钥
根密钥
eFuse
Flash
CPU
高速缓冲存储器
B1
硬件层

图6

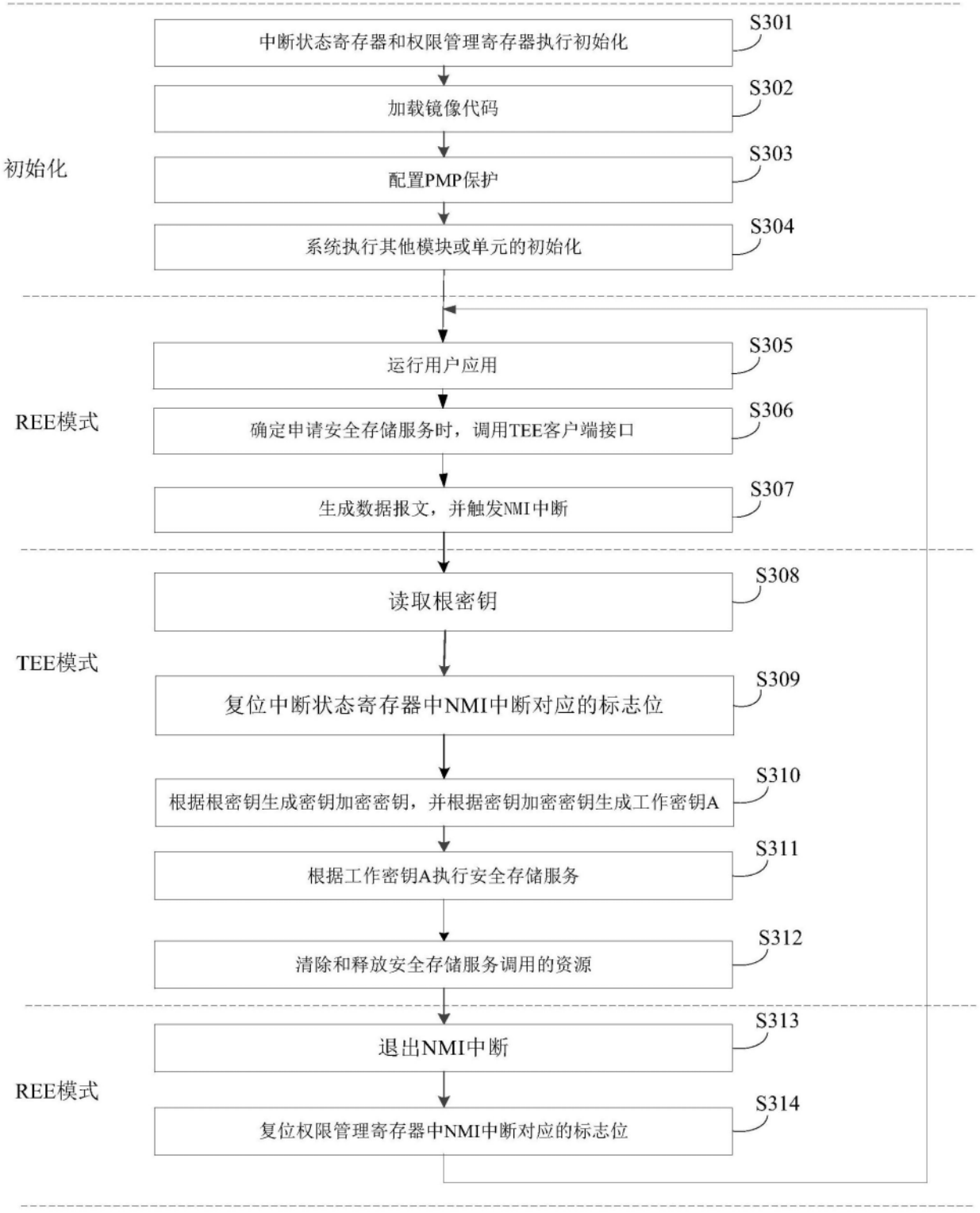

初始化
中断状态寄存器和权限管理寄存器执行初始化
S301
加载镜像代码
S302
配置PMP保护
S303
系统执行其他模块或单元的初始化
S304
REE模式
运行用户应用
S305
确定申请安全存储服务时，调用TEE客户端接口
S306
生成数据报文，并触发NMI中断
S307
TEE模式
读取根密钥
S308
复位中断状态寄存器中NMI中断对应的标志位
S309
根据根密钥生成密钥加密密钥，并根据密钥加密密钥生成工作密钥A
S310
根据工作密钥A执行安全存储服务
S311
清除和释放安全存储服务调用的资源
S312
REE模式
退出NMI中断
S313
复位权限管理寄存器中NMI中断对应的标志位
S314

图7

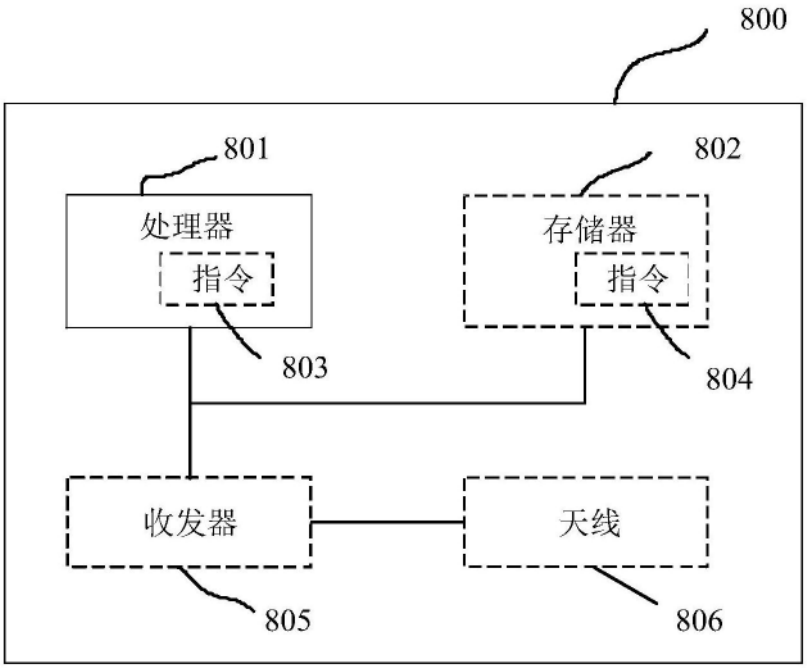

800
801
处理器
指令
802
存储器
指令
803
804
收发器
天线
805
806

图8

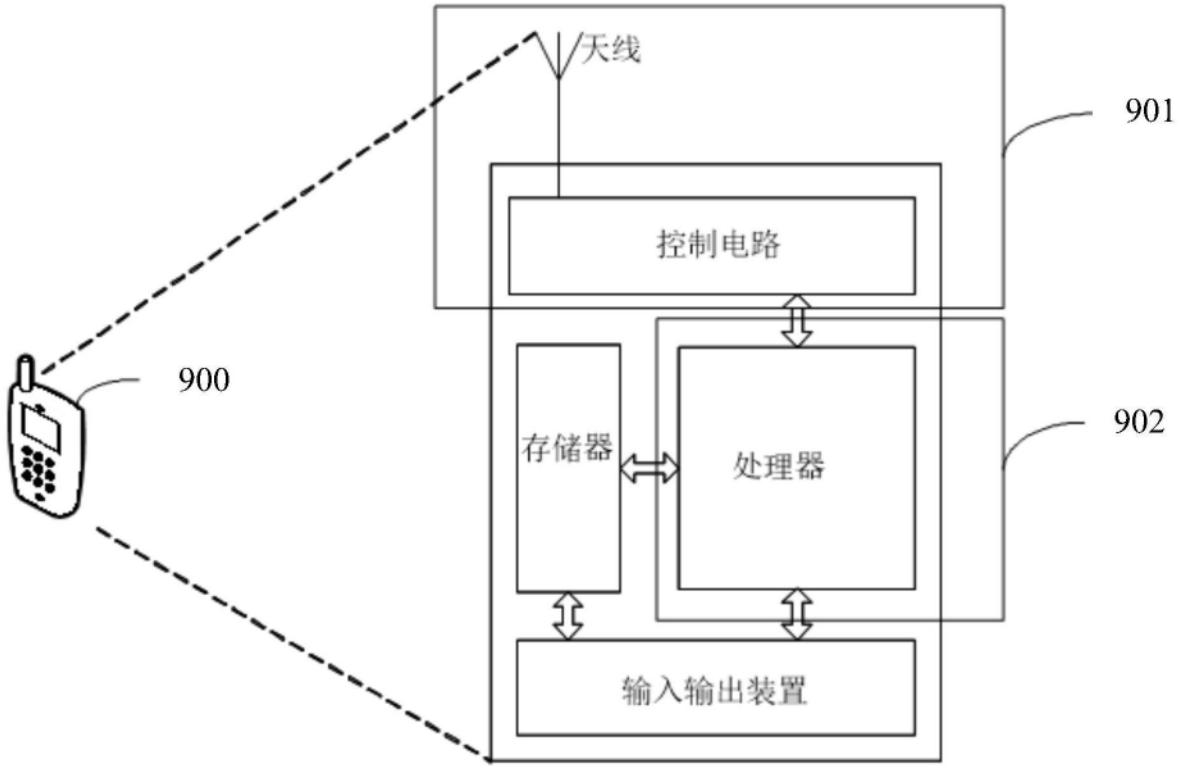

天线
901
控制电路
900
存储器
处理器
902
输入输出装置

图9