(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117993030 A
(43)申请公布日 2024.05.07

(21)申请号 202410048429.1

(22)申请日 2024.01.11

(71)申请人 国民技术股份有限公司
地址 518057 广东省深圳市南山区西丽街道松坪山社区宝深路109号国民技术大厦1楼

(72)发明人 李柯 黄健

(74)专利代理机构 深圳市力道知识产权代理事务所(普通合伙) 44507
专利代理师 郑永敏

(51)Int.Cl.
G06F 21/79(2013.01)
G06F 21/60(2013.01)

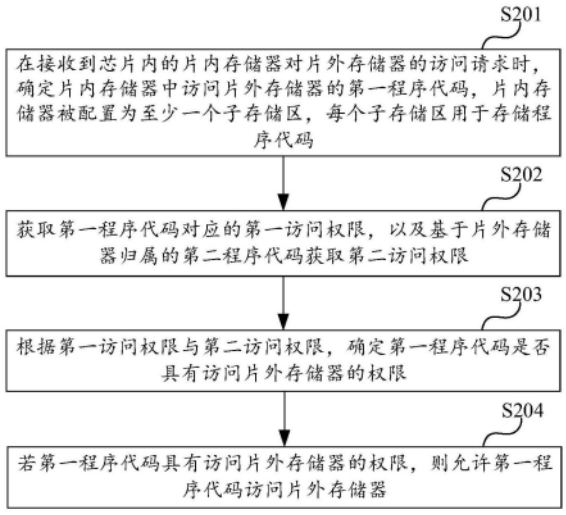
权利要求书2页 说明书11页 附图4页

(54)发明名称

存储器的管理方法、芯片、电子设备和可读存储介质

(57)摘要

本申请公开了一种存储器的管理方法、芯片、电子设备和计算机可读存储介质,该存储器的管理方法包括:在接收到芯片内的片内存储器对片外存储器的访问请求时,确定片内存储器中访问片外存储器的第一程序代码;获取第一程序代码对应的第一访问权限,以及基于片外存储器归属的第二程序代码获取第二访问权限;根据第一访问权限与第二访问权限,确定第一程序代码是否具有访问片外存储器的权限;若第一程序代码具有访问片外存储器的权限,则允许第一程序代码访问片外存储器。上述存储器的管理方法,可以实现对片外存储器进行用户归属划分和设置访问权限,防止片外存储器中的程序代码与数据被非法访问及篡改,提高了片外存储器的安全性。



CN 117993030 A

1.一种存储器的管理方法,其特征在于,所述方法包括:

在接收到芯片内的片内存储器对片外存储器的访问请求时,确定所述片内存储器中访问所述片外存储器的第一程序代码,所述片内存储器被配置为至少一个子存储区,每个所述子存储区用于存储程序代码;

获取所述第一程序代码对应的第一访问权限,以及基于所述片外存储器归属的第二程序代码获取第二访问权限;

根据所述第一访问权限与所述第二访问权限,确定所述第一程序代码是否具有访问所述片外存储器的权限;

若所述第一程序代码具有访问所述片外存储器的权限,则允许所述第一程序代码访问所述片外存储器。

2.根据权利要求1所述的存储器的管理方法,其特征在于,所述片内存储器包括闪存和静态随机存取存储器;所述确定所述片内存储器中访问所述片外存储器的第一程序代码之前,所述方法还包括:

将所述闪存划分为至少一个子存储区,以及将所述静态随机存取存储器划分为一个子存储区;

分别设置每个所述子存储区的访问权限。

3.根据权利要求1所述的存储器的管理方法,其特征在于,所述第二程序代码为所述片内存储器中配置所述片外存储器的寄存器属性的程序代码;所述基于所述片外存储器归属的第二程序代码获取第二访问权限,包括:

获取所述第二程序代码对应的访问权限;

根据所述第二程序代码对应的访问权限,确定所述第二访问权限。

4.根据权利要求1所述的存储器的管理方法,其特征在于,所述片内存储器包括静态随机存取存储器;所述基于所述片外存储器归属的第二程序代码获取第二访问权限,还包括:

若所述片内存储器未存在用于配置所述片外存储器的寄存器属性的程序代码,则根据所述静态随机存取存储器中的程序代码,确定所述第二程序代码;

根据所述第二程序代码对应的访问权限,确定所述第二访问权限。

5.根据权利要求1所述的存储器的管理方法,其特征在于,所述确定所述第一程序代码是否具有访问所述片外存储器的权限之后,所述方法还包括:

若所述第一程序代码未具有访问所述片外存储器的权限,则生成用于表示非法访问的越权预警信息,并上报所述越权预警信息。

6.根据权利要求1所述的存储器的管理方法,其特征在于,所述允许所述第一程序代码访问所述片外存储器之前,所述方法还包括:

从预设的密钥寄存器加载安全密钥,以供所述片外存储器基于所述安全密钥进行硬件解密,所述片内存储器中的程序代码均无读取所述密钥寄存器的权限;

所述允许所述第一程序代码访问所述片外存储器,所述方法还包括:

在所述片外存储器完成硬件解密后,允许所述第一程序代码访问硬件解密后的所述片外存储器。

7.根据权利要求6所述的存储器的管理方法,其特征在于,所述芯片还包括安全存储区,所述安全存储区用于存储所述安全密钥;所述方法还包括:

在所述芯片上电或硬件复位时,将所述安全存储区中的安全密钥加载至所述密钥寄存器。

8.根据权利要求6所述的存储器的管理方法,其特征在于,所述方法还包括:

在接收到对所述密钥寄存器的密钥配置请求时,获取所述密钥配置请求对应的目标程序代码的访问权限;

若所述目标程序代码的访问权限与所述片外存储器对应的第二访问权限一致,则允许所述目标程序代码对所述密钥寄存器中的安全密钥进行配置;

在所述目标程序代码完成密钥配置后,使能所述密钥寄存器中的配置后的安全密钥的加解密功能。

9.根据权利要求6所述的存储器的管理方法,其特征在于,所述方法还包括:

在接收到对所述密钥寄存器中的安全密钥的加解密功能的关闭操作时,清除所述密钥寄存器中的安全密钥。

10.一种芯片,其特征在于,所述芯片包括片内存储器和存储器保护单元,所述存储器保护单元用于执行如权利要求1至9任一项所述的存储器的管理方法。

11.一种电子设备,其特征在于,所述电子设备包括如权利要求10所述的芯片。

12.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质存储有计算机程序,所述计算机程序被处理器执行时实现如权利要求1至9任一项所述的存储器的管理方法。

存储器的管理方法、芯片、电子设备和可读存储介质

技术领域

[0001] 本申请涉及存储器技术领域,尤其涉及一种存储器的管理方法、芯片、电子设备和计算机可读存储介质。

背景技术

[0002] 随着物联网接入的设备越来越多,对MCU(Micro controller Unit,微控制器,又称硬件管理单元)的需求量越来越多。由于物联网面临诸多安全威胁,这些安全威胁从不同层面直接或间接地影响到IoT(Internet of Things,物联网)系统、设备和应用的安全性,因此安全问题是新基建物联网建设中亟待解决的首要问题。在相关技术中,芯片厂商只关注片内存储器的数据安全,而片外存储器的数据安全容易被忽略。

[0003] 因此,如何提高访问片外存储器的安全性成为亟需解决的问题。

发明内容

[0004] 本申请提供了一种存储器的管理方法、芯片、电子设备和计算机可读存储介质,解决了相关技术中容易忽略片外存储器的数据安全的问题。

[0005] 第一方面,本申请提供了一种存储器的管理方法,所述方法包括:

[0006] 在接收到芯片内的片内存储器对片外存储器的访问请求时,确定所述片内存储器中访问所述片外存储器的第一程序代码,所述片内存储器被配置为至少一个子存储区,每个所述子存储区用于存储程序代码;获取所述第一程序代码对应的第一访问权限,以及基于所述片外存储器归属的第二程序代码获取第二访问权限;根据所述第一访问权限与所述第二访问权限,确定所述第一程序代码是否具有访问所述片外存储器的权限;若所述第一程序代码具有访问所述片外存储器的权限,则允许所述第一程序代码访问所述片外存储器。

[0007] 上述存储器的管理方法,在片内存储器中的第一程序代码访问外存储器时,通过比较第一程序代码的第一访问权限与片外存储器归属的第二程序代码对应的第二访问权限,当第一程序代码具有访问片外存储器的权限时允许第一程序代码访问片外存储器,可以实现对片外存储器进行用户归属划分和设置访问权限,防止片外存储器中的程序代码与数据被非法访问及篡改,提高了片外存储器的安全性。

[0008] 第二方面,本申请还提供了一种芯片,所述芯片包括片内存储器和存储器保护单元,所述存储器保护单元用于执行如上述的存储器的管理方法。

[0009] 第三方面,本申请还提供了一种电子设备,所述电子设备包括上述的芯片。

[0010] 第四方面,本申请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存储有计算机程序,所述计算机程序被处理器执行时实现如上述的存储器的管理方法。

附图说明

[0011] 为了更清楚地说明本申请实施例技术方案,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。

[0012] 图1是本申请实施例提供的一种电子设备的结构示意图;

[0013] 图2是本申请实施例提供的一种芯片的结构示意图;

[0014] 图3是本申请实施例提供的一种存储器的管理方法的示意性流程图;

[0015] 图4是本申请实施例提供的另一种存储器的管理方法的示意性流程图;

[0016] 图5是本申请实施例提供的一种配置安全密钥的子步骤的示意性流程图;

[0017] 图6是本申请实施例提供的一种权限管理的示意性流程图;

[0018] 图7是本申请实施例提供的一种管理安全密钥的示意性流程图。

具体实施方式

[0019] 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一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0020] 附图中所示的流程图仅是示例说明,不是必须包括所有的内容和操作/步骤,也不是必须按所描述的顺序执行。例如,有的操作/步骤还可以分解、组合或部分合并,因此实际执行的顺序有可能根据实际情况改变。

[0021] 应当理解,在此本申请说明书中所使用的术语仅仅是出于描述特定实施例的目的而并不意在限制本申请。如在本申请说明书和所附权利要求书中所使用的那样,除非上下文清楚地指明其它情况,否则单数形式的“一”、“一个”及“该”意在包括复数形式。

[0022] 还应当理解,在本申请说明书和所附权利要求书中使用的术语“和/或”是指相关联列出的项中的一个或多个的任何组合以及所有可能组合,并且包括这些组合。

[0023] 在物联网的嵌入式产品研发过程中,有时会存在单个芯片内部需要多个用户分阶段进行应用软件开发的场景,在此场景中,各用户的程序代码及数据可能出于版权或安全考虑,不方便公开给其他用户共享。在相关技术中,芯片厂商只关注片内存储器的数据安全,而片外存储器的数据安全容易被忽略。在数据存储和传输过程中,一般采用密码技术来保障数据的机密性、完整性、可用性、不可抵赖性、真实性、隐私性,这也是保障物联网安全性的核心。但是仅仅通过密码技术并不能完全防范物联网攻击,如针对通信管道的中间攻击、数据协议分析、数据劫持、针对平台的未授权访问、敏感数据挖取、伪造请求攻击等风险。

[0024] 为此,本申请的实施例提供一种存储器的管理方法、芯片、电子设备和计算机可读存储介质,在片内存储器中的第一程序代码访问外存储器时,通过比较第一程序代码的第一访问权限与片外存储器归属的第二程序代码对应的第二访问权限,当第一程序代码具有访问片外存储器的权限时允许第一程序代码访问片外存储器,可以实现对片外存储器进行用户归属划分和设置访问权限,防止片外存储器中的程序代码与数据被非法访问及篡改,提高了片外存储器的安全性。

[0025] 下面结合附图,对本申请的一些实施方式作详细说明。在不冲突的情况下,下述的实施例及实施例中的特征可以相互组合。

[0026] 请参阅图1,图1是本申请实施例提供的一种电子设备10的结构示意图,如图1所示,电子设备10可以包括芯片100。

[0027] 示例性的,芯片100可以包括主控制器,也可以包括微控制器。当芯片100同时包括主控制器和微控制器时,主控制器可以通过系统总线与微控制器连接,其中,系统总线可以包括但不限于高级系统总线(Advanced System Bus,ASB)、高级外设总线(Advanced Peripheral Bus,APB)、高级高性能总线(Advanced High-performance Bus,AHB)以及高级跟踪总线(Advanced Trace Bus,ATB)等总线。

[0028] 示例性的,主控制器可以包括但不限于中央处理器(Central Processing Unit,CPU)、数字信号处理器(Digital Signal Processing,DSP)、ARM(Advanced RISC Machine)处理器、专用集成电路(Application Specific Integrated Circuit,ASIC)以及现场可编程门阵列(Field-Programmable Gate Array,FPGA)等等。微控制器可以是电子设备10内置的微处理器,其功能与主控制器类似,具备指令能力,可扩展性强,可以代替主控制器完成部分功能;同时,微控制器占用极少的资源,可以以较高频率运行。在本申请实施例中的存储器的管理方法可以由主控制器执行,也可以由微控制器执行,为了便于说明,下文将以微控制器作为执行主体说明如何管理存储器。

[0029] 请参阅图2,图2是本申请实施例提供的一种芯片100的结构示意图,如图2所示,芯片100可以包括片内存储器101和存储器保护单元102。其中,片内存储器101和存储器保护单元102可以通过总线连接,该总线比如为I^2C(Inter-integrated Circuit,集成电路)总线等任意适用的总线。

[0030] 示例性的,芯片100还可以包括存储介质(图中未示出),存储介质可存储操作系统和计算机程序。该计算机程序包括程序指令,该程序指令被执行时,可使得存储器保护单元102执行任意一种存储器的管理方法。其中,存储介质可以是存储器保护单元102内置的存储介质,也可以是片内存储器101,还可以是芯片100中的其它存储器。

[0031] 需要说明的是,存储器保护单元(Memory Protect Unit,MPU)102是一种用于保护存储器的硬件单元,它可以实施对存储器(主要是内存和外设寄存器)的保护,以使软件更加健壮和可靠。

[0032] 示例性的,片内存储器101可以包括闪存(Flash EEPROM Memory,简称FLASH)和静态随机存取存储器(Static Random Access Memory,SRAM)。

[0033] 可以理解的是,当芯片100为主控制器时,主控制器可以包括片内存储器101和存储器保护单元102,片外存储器可以是微控制器中的存储器,也可以是电子设备10中的其它存储器,还可以是电子设备10外接的存储设备。当芯片100为微控制器时,微控制器可以包括片内存储器101和存储器保护单元102,片外存储器可以是主控制器中的存储器,也可以是电子设备10中的其它存储器,还可以是电子设备10外接的存储设备。

[0034] 在一个实施例中,存储器保护单元102用于运行存储在存储介质中的计算机程序,以实现如下步骤:

[0035] 在接收到芯片内的片内存储器对片外存储器的访问请求时,确定片内存储器中访问片外存储器的第一程序代码,片内存储器被配置为至少一个子存储区,每个子存储区用于存储程序代码;获取第一程序代码对应的第一访问权限,以及基于片外存储器归属的第二程序代码获取第二访问权限;根据第一访问权限与第二访问权限,确定第一程序代码是

否具有访问片外存储器的权限;若第一程序代码具有访问片外存储器的权限,则允许第一程序代码访问片外存储器。

[0036] 在一个实施例中,片内存储器包括闪存和静态随机存取存储器;存储器保护单元102在实现确定片内存储器中访问片外存储器的第一程序代码之前,还用于实现:

[0037] 将闪存划分为至少一个子存储区,以及将静态随机存取存储器划分为一个子存储区;分别设置每个子存储区的访问权限。

[0038] 在一个实施例中,第二程序代码为片内存储器中配置片外存储器的寄存器属性的程序代码;存储器保护单元102在实现基于片外存储器归属的第二程序代码获取第二访问权限时,用于实现:

[0039] 获取第二程序代码对应的访问权限;根据第二程序代码对应的访问权限,确定第二访问权限。

[0040] 在一个实施例中,片内存储器包括静态随机存取存储器;存储器保护单元102在实现基于片外存储器归属的第二程序代码获取第二访问权限时,用于实现:

[0041] 若片内存储器未存在用于配置片外存储器的寄存器属性的程序代码,则根据静态随机存取存储器中的程序代码,确定第二程序代码;根据第二程序代码对应的访问权限,确定第二访问权限。

[0042] 在一个实施例中,存储器保护单元102在实现确定第一程序代码是否具有访问片外存储器的权限之后,还用于实现:

[0043] 若第一程序代码未具有访问片外存储器的权限,则生成用于表示非法访问的越权预警信息,并上报越权预警信息。

[0044] 在一个实施例中,存储器保护单元102在实现允许第一程序代码访问片外存储器之前,还用于实现:

[0045] 从预设的密钥寄存器加载安全密钥,以供片外存储器基于安全密钥进行硬件解密,片内存储器中的程序代码均无读取密钥寄存器的权限。

[0046] 在一个实施例中,存储器保护单元102在实现允许第一程序代码访问片外存储器时,用于实现:

[0047] 在片外存储器完成硬件解密后,允许第一程序代码访问硬件解密后的片外存储器。

[0048] 在一个实施例中,芯片还包括安全存储区,安全存储区用于存储安全密钥;存储器保护单元102还用于实现:

[0049] 在芯片上电或硬件复位时,将安全存储区中的安全密钥加载至密钥寄存器。

[0050] 在一个实施例中,存储器保护单元102还用于实现:

[0051] 在接收到对密钥寄存器的密钥配置请求时,获取密钥配置请求对应的目标程序代码的访问权限;若目标程序代码的访问权限与片外存储器对应的第二访问权限一致,则允许目标程序代码对密钥寄存器中的安全密钥进行配置;在目标程序代码完成密钥配置后,使能密钥寄存器中的配置后的安全密钥的加解密功能。

[0052] 在一个实施例中,存储器保护单元102还用于实现:

[0053] 在接收到对密钥寄存器中的安全密钥的加解密功能的关闭操作时,清除密钥寄存器中的安全密钥。

[0054] 请参阅图3,图3是本申请实施例提供的一种存储器的管理方法的示意性流程图。如图3所示,该存储器的管理方法包括步骤S201至步骤S204。

[0055] 步骤S201、在接收到芯片内的片内存储器对片外存储器的访问请求时,确定片内存储器中访问片外存储器的第一程序代码,片内存储器被配置为至少一个子存储区,每个子存储区用于存储程序代码。

[0056] 在本申请实施例中,该存储器的管理方法可以应用于芯片内的片内存储器中的程序代码访问片外存储器的场景中。其中,片外存储器可以是独立于芯片的存储器,例如,片外存储器可以是电子设备中的其它存储器,还可以是电子设备外接的存储设备。

[0057] 在一些实施例中,在接收到芯片内的片内存储器对片外存储器的访问请求时,确定片内存储器中访问片外存储器的第一程序代码,片内存储器被配置为至少一个子存储区,每个子存储区用于存储程序代码。

[0058] 需要说明的是,在本申请实施例中,存储器保护单元可以预先将片内存储器划分为多个子存储区,每个子存储区用于存储程序代码。并且分别对每个子存储区设置访问权限,以避免在片内存储器中的不同用户通过CPU指令直接读取或修改其他用户对应的子存储区中的程序代码。可以理解的是,每个子存储区中的程序代码在具备访问权限时可以访问片外存储器,但不能访问其它子存储区。

[0059] 示例性的,在接收到芯片内的片内存储器对片外存储器的访问请求时,确定片内存储器中访问片外存储器的第一程序代码。例如,可以根据访问权限中的识别码或地址确定访问片外存储器的程序代码所在的目标子存储区,再将目标子存储区中的程序代码确定为第一程序代码。

[0060] 在一些实施例中,片内存储器可以包括闪存和静态随机存取存储器;在确定片内存储器中访问片外存储器的第一程序代码之前,还可以包括:将闪存划分为至少一个子存储区,以及将静态随机存取存储器划分为一个子存储区;分别设置每个子存储区的访问权限。

[0061] 示例性的,可以将闪存(FLASH)划分为至少一个子存储区,例如,划分为子存储区USER1、USER2和USER3。可以将静态随机存取存储器(SRAM)划分为一个子存储区,例如子存储区USER4,当然,也可以将静态随机存取存储器(SRAM)划分为多个子存储区,在此不作限定。然后,分别对子存储区USER1、USER2、USER3以及USER4设置访问权限。例如,对子存储区USER1、USER2和USER3可以设置读取权限和写入权限,对子存储区USER4可以设置读取权限、写入权限和擦除权限。

[0062] 上述实施例,通过将闪存划分为至少一个子存储区,以及将静态随机存取存储器划分为一个子存储区,并分别设置每个子存储区的访问权限,可以防止片内存储器中的不同用户通过CPU指令直接读取或修改其他用户对应的子存储区中的程序代码,提高了程序代码的安全性。

[0063] 步骤S202、获取第一程序代码对应的第一访问权限,以及基于片外存储器归属的第二程序代码获取第二访问权限。

[0064] 示例性的,在确定片内存储器中访问片外存储器的第一程序代码之后,存储器保护单元可以获取第一程序代码对应的第一访问权限。例如,第一程序代码可以表示为U1D2,可以获取第一程序代码U1D2对应的第一访问权限,第一访问权限可以表示为T1。第一访问

权限T1可以包括读取权限、写入权限以及擦除权限中的至少一项。

[0065] 示例性的,存储器保护单元还可以基于片外存储器归属的第二程序代码获取第二访问权限。其中,第二程序代码为片内存储器中配置片外存储器的寄存器属性的程序代码。可以在片内存储器中的多个子存储区中,将配置片外存储器的寄存器属性的程序代码,确定为第二程序代码。例如,当配置片外存储器的寄存器属性的程序代码为U1D1时,可以将程序代码U1D1确定为第二程序代码。

[0066] 需要说明的是,片外存储器可以视为一个整体的用户区域,片外存储器中的程序代码归属于片内存储器中配置片外存储器的程序代码。在本申请实施例中,可以预先定义配置片外存储器的寄存器属性的程序代码具有访问片外存储器的权限,而未配置片外存储器的寄存器属性的程序代码不具有访问片外存储器的权限。

[0067] 示例性的,可以将配置片外存储器的寄存器属性的程序代码对应的访问权限,设置为片外存储器中的程序代码对应的访问权限,即片外存储器中的程序代码对应的访问权限与配置片外存储器的寄存器属性的程序代码对应的访问权限一致。例如,若片外存储器的寄存器属性由子存储区USER1的程序代码配置,则片外存储器中的程序代码归属于子存储区USER1的程序代码,并且片外存储器中的用户代码的访问权限与子存储区USER1的程序代码的访问权限一致。

[0068] 通过获取第一程序代码对应的第一访问权限,以及基于片外存储器归属的第二程序代码获取第二访问权限,后续可以对第一访问权限与第二访问权限进行比对,以确定第一程序代码是否具有访问片外存储器的权限。

[0069] 在一些实施例中,基于片外存储器归属的第二程序代码获取第二访问权限,可以包括:获取第二程序代码对应的访问权限;根据第二程序代码对应的访问权限,确定第二访问权限。

[0070] 示例性的,当第二程序代码为U1D1时,可以获取第二程序代码U1D1对应的访问权限,将第二程序代码U1D1对应的访问权限确定为第二访问权限。其中,第二访问权限可以表示为T2。

[0071] 示例性的,第二访问权限T2可以包括读取权限、写入权限以及擦除权限中的至少一项。

[0072] 上述实施例,通过获取第二程序代码对应的访问权限,可以将第二程序代码对应的访问权限确定为第二访问权限。

[0073] 在一些实施例中,基于片外存储器归属的第二程序代码获取第二访问权限,还可以包括:若片内存储器未存在用于配置片外存储器的寄存器属性的程序代码,则根据静态随机存取存储器中的程序代码,确定第二程序代码;根据第二程序代码对应的访问权限,确定第二访问权限。

[0074] 需要说明的是,在本申请实施例中,若片内存储器中未存在用于配置片外存储器的寄存器属性的程序代码,则可以默认片外存储器的程序代码归属于静态随机存取存储器中的程序代码。

[0075] 示例性的,可以将静态随机存取存储器中的程序代码,确定为第二程序代码,并将第二程序代码对应的访问权限,确定为第二访问权限。

[0076] 上述实施例,在片内存储器未存在用于配置片外存储器的寄存器属性的程序代码

时,通过根据静态随机存取存储器中的程序代码对应的访问权限,确定第二访问权限,可以实现灵活地确定第二访问权限。

[0077] 步骤S203、根据第一访问权限与第二访问权限,确定第一程序代码是否具有访问片外存储器的权限。

[0078] 在一些实施例中,在获取第一程序代码对应的第一访问权限,以及基于片外存储器归属的第二程序代码获取第二访问权限之后,可以根据第一访问权限与第二访问权限,确定第一程序代码是否具有访问片外存储器的权限。

[0079] 示例性的,可以将第一访问权限与第二访问权限进行对比,若第一访问权限与第二访问权限一致,则确定第一程序代码具有访问片外存储器的权限;若第一访问权限与第二访问权限不一致,则确定第一程序代码不具有访问片外存储器的权限。例如,若第一访问权限包括读取权限、写入权限以及擦除权限,第二访问权限包括读取权限和写入权限,则可以确定第一访问权限与第二访问权限不一致。又例如,若第一访问权限包括读取权限,第二访问权限包括读取权限,则可以确定第一访问权限与第二访问权限一致。

[0080] 上述实施例,通过对第一访问权限与第二访问权限进行对比,可以确定第一程序代码是否具有访问片外存储器的权限。

[0081] 步骤S204、若第一程序代码具有访问片外存储器的权限,则允许第一程序代码访问片外存储器。

[0082] 示例性的,在根据第一访问权限与第二访问权限,确定第一程序代码是否具有访问片外存储器的权限之后,若第一程序代码具有访问片外存储器的权限,则允许第一程序代码访问片外存储器。

[0083] 上述实施例中,在片内存储器中的第一程序代码访问外存储器时,通过比较第一程序代码的第一访问权限与片外存储器归属的第二程序代码对应的第二访问权限,当第一程序代码具有访问片外存储器的权限时允许第一程序代码访问片外存储器,可以实现对片外存储器进行用户归属划分和设置访问权限,防止片外存储器中的程序代码与数据被非法访问及篡改,提高了片外存储器的安全性。

[0084] 请参阅图4,图4是本申请实施例提供的另一种存储器的管理方法的示意性流程图。如图4所示,该存储器的管理方法可以包括步骤S301至步骤S304。

[0085] 步骤S301、在接收到芯片内的片内存储器对片外存储器的访问请求时,确定片内存储器中访问片外存储器的第一程序代码,片内存储器被配置为至少一个子存储区,每个子存储区用于存储程序代码。

[0086] 步骤S302、获取第一程序代码对应的第一访问权限,以及基于片外存储器归属的第二程序代码获取第二访问权限。

[0087] 步骤S303、根据第一访问权限与第二访问权限,确定第一程序代码是否具有访问片外存储器的权限。

[0088] 可以理解,步骤S301至步骤S303与上述步骤S201至步骤S203相同,在此不再赘述。

[0089] 步骤S304、若第一程序代码未具有访问片外存储器的权限,则生成用于表示非法访问的越权预警信息,并上报越权预警信息。

[0090] 示例性的,在确定第一程序代码是否具有访问片外存储器的权限之后,若第一程序代码未具有访问片外存储器的权限,则生成用于表示非法访问的越权预警信息,并上报

越权预警信息。存储器保护单元可以上报越权预警信息给CPU,由CPU对越权预警信息进行记录或进行其它操作等等。

[0091] 需要说明的是,在本申请实施例中,可以支持上报子存储区及受保护的片外存储器的越权预警信息,所有越权操作都将触发异常报警,开发者可以根据返回的越权预警信息采取应对措施,从而实现片外存储器中的数据的安全存储和访问。

[0092] 上述实施例,通过在第一程序代码未具有访问片外存储器的权限时,生成用于表示非法访问的越权预警信息并上报越权预警信息,可以使得开发者根据返回的越权预警信息采取应对措施,从而实现片外存储器中的数据的安全存储和访问,达到实现防泄漏、防复制、防篡改、防擦除的目的。

[0093] 在一些实施例中,在允许第一程序代码访问片外存储器之前,还可以包括:从预设的密钥寄存器加载安全密钥,以供片外存储器基于安全密钥进行硬件解密。其中,片内存储器中的程序代码均无读取密钥寄存器的权限。

[0094] 需要说明的是,芯片还可以包括安全存储区,安全存储区用于存储安全密钥,其中,安全存储区独立于子存储区。在本申请实施例中,安全密钥默认存放在安全存储区,片内存储器中的程序代码或其它CPU程序无读取安全存储区的权限。在芯片上电或硬件复位时,会自动加载安全存储区中的安全密钥至密钥寄存器。密钥寄存器用于保存从安全存储区加载的安全密钥和支持用户自定义配置安全密钥,并且密钥寄存器只有写入权限,无读取权限,从而可以有效防止安全密钥泄露。

[0095] 示例性的,存储器保护单元可以从密钥寄存器加载安全密钥,以供片外存储器基于安全密钥进行硬件解密。其中,硬件解密的具体过程,在此不作限定。

[0096] 需要说明的是,安全密钥用于对片外存储器进行硬件解密以及硬件加密。例如,在程序代码访问片外存储器之前,可以加载从密钥寄存器加载安全密钥,以供片外存储器基于安全密钥进行硬件解密。又例如,在程序代码完成访问片外存储器时,片外存储器可以基于安全密钥进行硬件加密。

[0097] 上述实施例,由于片内存储器中的程序代码均无读取密钥寄存器的权限,通过从密钥寄存器加载安全密钥,由片外存储器基于安全密钥进行硬件解密,可以实现第一程序代码在片外存储器基于安全密钥进行硬件解密后才能访问,可以防止片外存储器中的数据与代码被非法访问和篡改,提高了片外存储器的安全性。

[0098] 在一些实施例中,允许第一程序代码访问片外存储器,还可以包括:在片外存储器完成硬件解密后,允许第一程序代码访问硬件解密后的片外存储器。

[0099] 示例性的,存储器保护单元在确定片外存储器完成硬件解密后,可以允许第一程序代码访问硬件解密后的片外存储器。

[0100] 需要说明的是,在本申请实施例中,通过在片外存储器完成硬件解密后,允许第一程序代码访问硬件解密后的片外存储器,可以实现对片外存储器进行访问权限校验和安全密钥管控的双重保护,可以进一步提高了片外存储器的安全性。

[0101] 在一些实施例中,本申请实施例提供的存储器的管理方法还可以包括:在芯片上电或硬件复位时,将安全存储区中的安全密钥加载至密钥寄存器。

[0102] 需要说明的是,由于内存储器中的程序代码或其它CPU程序无读取安全存储区的权限,因此需要在芯片上电或硬件复位时,自动加载安全存储区中的安全密钥至密钥寄存

器。

[0103] 上述实施例,通过自动加载安全存储区中的安全密钥至密钥寄存器,可以实现在片内存储器中的程序代码访问片外存储器时,从密钥寄存器加载安全密钥,以供片外存储器基于安全密钥进行硬件解密,确保程序代码能够正常访问片外存储器。

[0104] 在本申请实施例中,芯片内的有效程序代码均有权限配置密钥寄存器中的安全密钥,其中,有效程序代码是片外存储器归属的程序代码。以下将详细说明如何配置安全密钥。

[0105] 请参阅图5,图5是本申请实施例提供的一种配置安全密钥的子步骤的示意性流程图。如图5所示,包括步骤S401至步骤S403。

[0106] 步骤S401、在接收到对密钥寄存器的密钥配置请求时,获取密钥配置请求对应的目标程序代码的访问权限。

[0107] 示例性的,存储器保护单元在接收到对密钥寄存器的密钥配置请求时,获取密钥配置请求对应的目标程序代码的访问权限。示例性的,若目标程序代码为U1D3,则可以获取目标程序代码U1D3的访问权限,例如目标程序代码U1D3的访问权限可以表示为T3。

[0108] 步骤S402、若目标程序代码的访问权限与片外存储器对应的第二访问权限一致,则允许目标程序代码对密钥寄存器中的安全密钥进行配置。

[0109] 示例性的,可以将目标程序代码的访问权限T3与片外存储器对应的第二访问权限T2进行比对,若目标程序代码的访问权限与片外存储器对应的第二访问权限一致,则确定目标程序代码为片外存储器中的程序代码归属的程序代码,此时,可以允许目标程序代码对密钥寄存器中的安全密钥进行配置。若目标程序代码的访问权限与片外存储器对应的第二访问权限不一致,则禁止目标程序代码对密钥寄存器中的安全密钥进行配置。

[0110] 通过获取密钥配置请求对应的目标程序代码的访问权限,并判断目标程序代码的访问权限与片外存储器对应的第二访问权限是否一致,可以避免不是片外存储器归属的程序代码非法修改密钥寄存器中的安全密钥,提高了安全密钥的安全性。

[0111] 步骤S403、在目标程序代码完成密钥配置后,使能密钥寄存器中的配置后的安全密钥的加解密功能。

[0112] 示例性的,存储器保护单元在确定目标程序代码完成密钥配置后,使能密钥寄存器中的配置后的安全密钥的加解密功能。其中,加解密功能包括加密功能和解密功能。

[0113] 通过使能密钥寄存器中的配置后的安全密钥的加解密功能,可以使得片内存储器中的程序代码在访问片外存储器时,片外存储器基于密钥寄存器中的安全密钥进行硬件解密,确保片内存储器中的程序代码能够正常访问片外存储器。

[0114] 在一些实施例中,本申请实施例提供的存储器的管理方法还可以包括:在接收到对密钥寄存器中的安全密钥的加解密功能的关闭操作时,清除密钥寄存器中的安全密钥。

[0115] 示例性的,存储器保护单元在接收到对密钥寄存器中的安全密钥的加解密功能的关闭操作时,清除密钥寄存器中的安全密钥。

[0116] 需要说明的是,通过在接收到对安全密钥的加解密功能的关闭操作时,清除密钥寄存器中的安全密钥,可以有效防止安全密钥被泄露。

[0117] 请参阅图6,图6是本申请实施例提供的一种权限管理的示意性流程图。如图6所示,当程序代码U1D2访问片外存储器,程序代码U1D1配置片外存储器的寄存器的程序代码

为U1D1,即片外存储器归属于程序代码U1D1时,存储器保护单元MPU可以判断程序代码U1D2是否有访问程序代码U1D1的权限。若程序代码U1D2有访问程序代码U1D1的权限,则允许程序代码U1D2访问片外存储器。若程序代码U1D2无访问程序代码U1D1的权限,则禁止程序代码U1D2访问片外存储器,上报越权预警信息。

[0118] 通过判断程序代码U1D2是否有访问程序代码U1D1的权限,当程序代码U1D2具有访问片外存储器的权限时允许程序代码U1D2访问片外存储器,可以实现对片外存储器进行用户归属划分和设置访问权限,防止片外存储器中的程序代码与数据被非法访问及篡改,提高了片外存储器的安全性。

[0119] 请参阅图7,图7是本申请实施例提供的一种管理安全密钥的示意性流程图。如图7所示,在芯片上电或系统复位时,自动加载安全存储区中的安全密钥至密钥寄存器。

[0120] 如图7所示,在接收到程序代码U1D3对密钥寄存器的密钥配置请求时,判断程序代码U1D3的访问权限是否与程序代码U1D1的访问权限一致;若程序代码U1D3的访问权限与程序代码U1D1的访问权限一致,则允许程序代码U1D3对密钥寄存器中的安全密钥进行配置,若程序代码U1D3的访问权限与程序代码U1D1的访问权限不一致,则确认配置失败。

[0121] 在程序代码U1D3请求配置密钥寄存器中安全密钥时,判断程序代码U1D3的访问权限与程序代码U1D1是否一致,可以避免不是片外存储器归属的程序代码非法修改密钥寄存器中的安全密钥,提高了安全密钥的安全性。

[0122] 如图7所示,在接收到对密钥寄存器中的安全密钥的加解密功能的关闭操作时,清除密钥寄存器中的安全密钥。通过在接收到对安全密钥的加解密功能的关闭操作时,清除密钥寄存器中的安全密钥,可以有效防止安全密钥被泄露。

[0123] 本申请的实施例中还提供一种计算机可读存储介质,该计算机可读存储介质存储有计算机程序,该计算机程序中包括程序指令,处理器执行上述程序指令,以实现本申请实施例提供的任一项存储器的管理方法。

[0124] 例如,该程序被处理器加载,可以执行如下步骤:

[0125] 在接收到芯片内的片内存储器对片外存储器的访问请求时,确定片内存储器中访问片外存储器的第一程序代码,片内存储器被配置为至少一个子存储区,每个子存储区用于存储程序代码;获取第一程序代码对应的第一访问权限,以及基于片外存储器归属的第二程序代码获取第二访问权限;根据第一访问权限与第二访问权限,确定第一程序代码是否具有访问片外存储器的权限;若第一程序代码具有访问片外存储器的权限,则允许第一程序代码访问片外存储器。

[0126] 其中,计算机可读存储介质可以是前述实施例的电子设备的内部存储电路,例如电子设备的硬盘或内存。计算机可读存储介质也可以是电子设备的外部存储设备,例如电子设备上配备的插接式硬盘,智能存储卡(Smart Media Card,SMC),安全数字卡(Secure Digital Card,SD Card),闪存卡(Flash Card)等。

[0127] 进一步地,计算机可读存储介质可主要包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需的程序等;存储数据区可存储根据各程序所创建的数据等。

[0128] 以上,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。

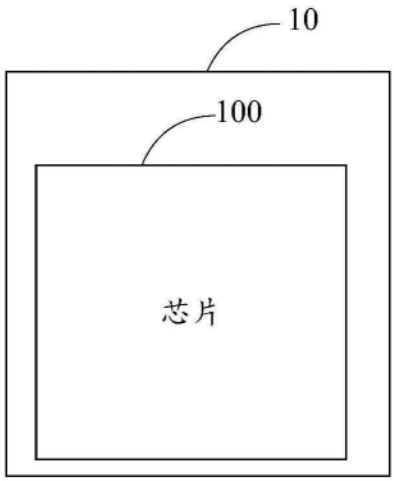


图1

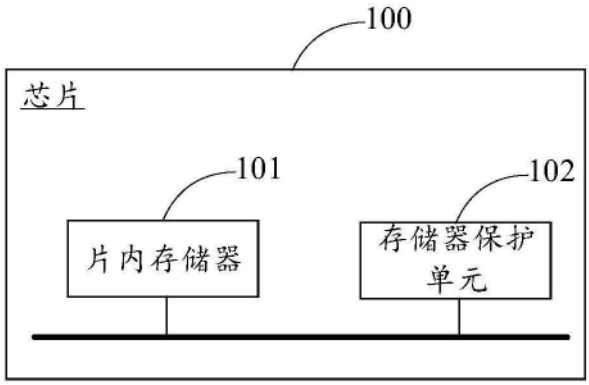


图2

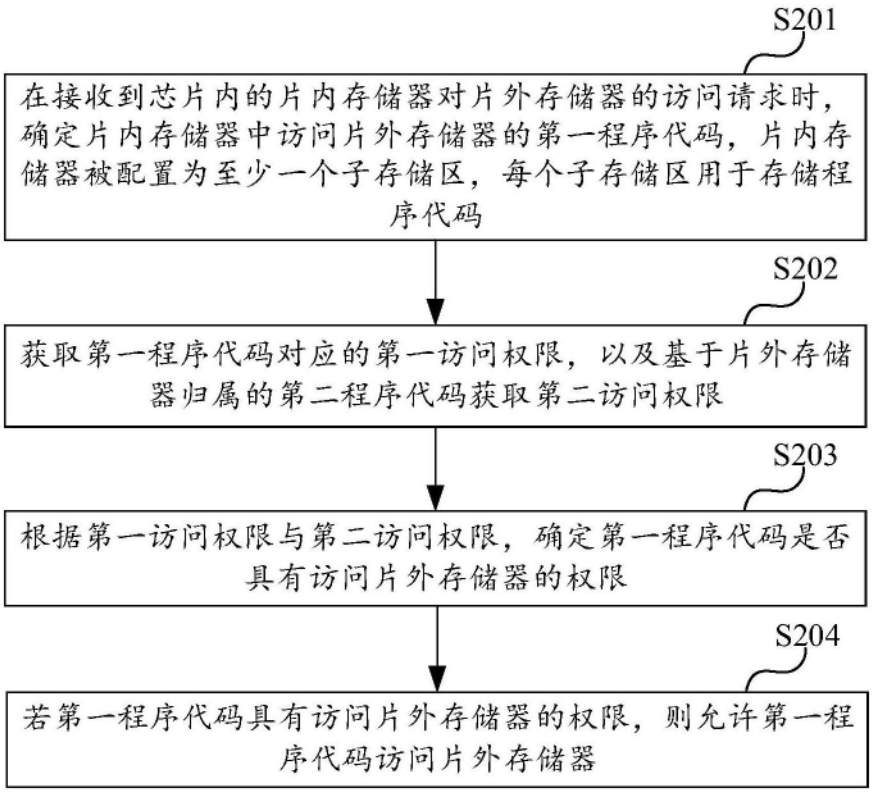

S201
在接收到芯片内的片内存储器对片外存储器的访问请求时，确定片内存储器中访问片外存储器的第一程序代码，片内存储器被配置为至少一个子存储区，每个子存储区用于存储程序代码
S202
获取第一程序代码对应的第一访问权限，以及基于片外存储器归属的第二程序代码获取第二访问权限
S203
根据第一访问权限与第二访问权限，确定第一程序代码是否具有访问片外存储器的权限
S204
若第一程序代码具有访问片外存储器的权限，则允许第一程序代码访问片外存储器

图3

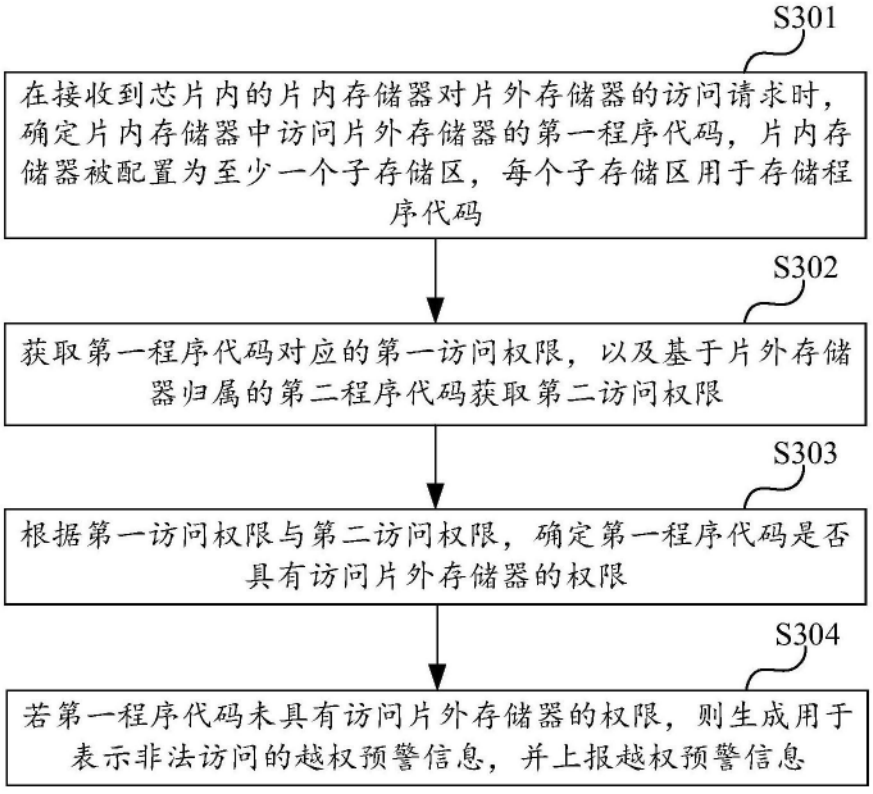

S301
在接收到芯片内的片内存储器对片外存储器的访问请求时，确定片内存储器中访问片外存储器的第一程序代码，片内存储器被配置为至少一个子存储区，每个子存储区用于存储程序代码
S302
获取第一程序代码对应的第一访问权限，以及基于片外存储器归属的第二程序代码获取第二访问权限
S303
根据第一访问权限与第二访问权限，确定第一程序代码是否具有访问片外存储器的权限
S304
若第一程序代码未具有访问片外存储器的权限，则生成用于表示非法访问的越权预警信息，并上报越权预警信息

图4

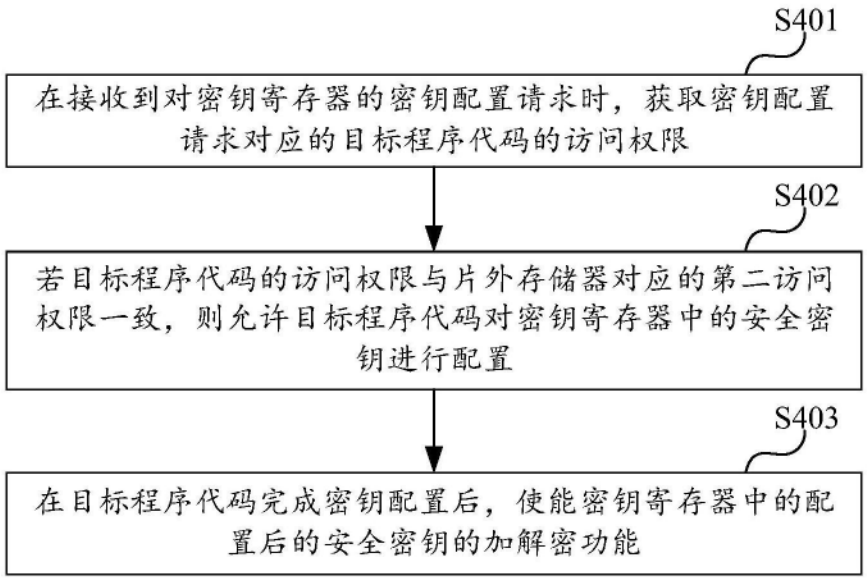

S401
在接收到对密钥寄存器的密钥配置请求时，获取密钥配置请求对应的目标程序代码的访问权限
S402
若目标程序代码的访问权限与片外存储器对应的第二访问权限一致，则允许目标程序代码对密钥寄存器中的安全密钥进行配置
S403
在目标程序代码完成密钥配置后，使能密钥寄存器中的配置后的安全密钥的加解密功能

图5

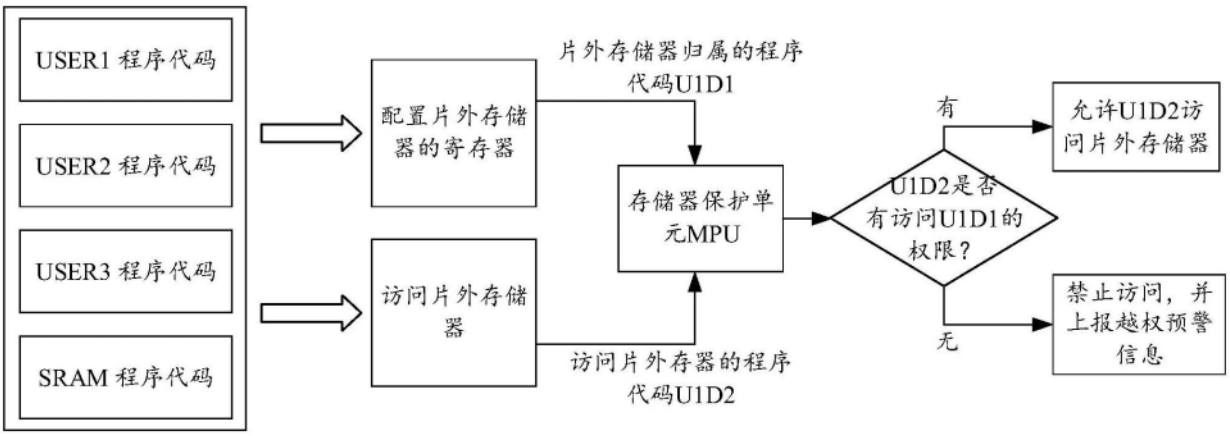

USER1 程序代码
USER2 程序代码
USER3 程序代码
SRAM 程序代码
配置片外存储器的寄存器
访问片外存储器
片外存储器归属的程序代码U1D1
访问片外存器的程序代码U1D2
存储器保护单元MPU
U1D2是否有访问U1D1的权限？
有
无
允许U1D2访问片外存储器
禁止访问，并上报越权预警信息

图6

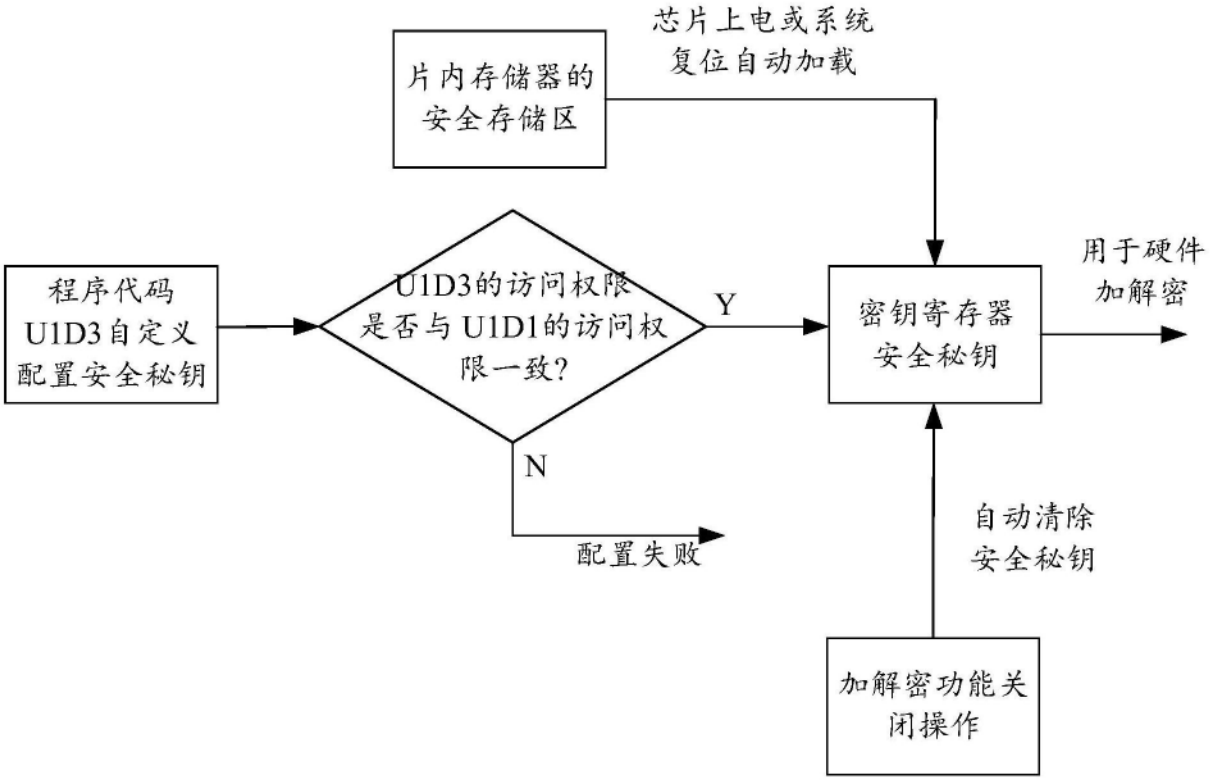

芯片上电或系统
复位自动加载
片内存储器的
安全存储区
程序代码
U1D3自定义
配置安全秘钥
U1D3的访问权限
是否与U1D1的访问权
限一致?
Y
N
配置失败
密钥寄存器
安全秘钥
用于硬件
加解密
自动清除
安全秘钥
加解密功能关
闭操作

图7