(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 111752604 A
(43)申请公布日 2020.10.09

(21)申请号 201910238090.0

(22)申请日 2019.03.27

(71)申请人 阿里巴巴集团控股有限公司
地址 开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 陈晨 朱涛涛 刘畅

(74)专利代理机构 北京思睿峰知识产权代理有限公司 11396
代理人 谢建云 赵爱军

(51)Int.Cl.
G06F 9/30(2006.01)
G06F 21/74(2013.01)

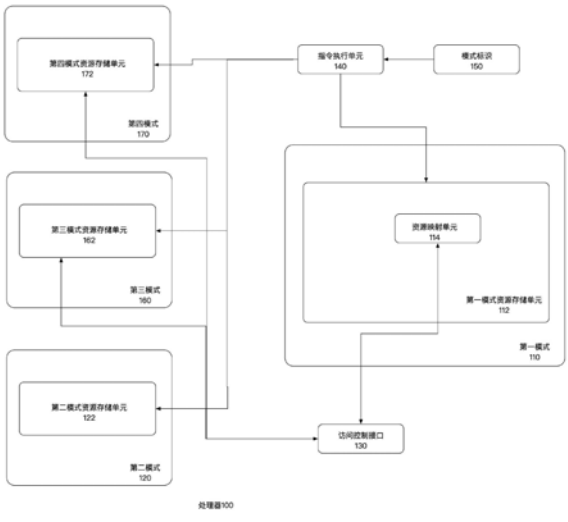
权利要求书2页 说明书9页 附图5页

(54)发明名称

一种具有多个运行模式的处理器

(57)摘要

本发明公开了一种具有多个运行模式的处理器，包括：第一模式资源存储单元，适于存储在处理器以第一模式运行时的第一模式资源；第二模式资源存储单元，适于存储在该处理器以第二模式运行时的第二模式资源；以及指令执行单元，适于在处理器以第一模式运行时，执行指令以访问第一模式资源，以及在处理器以第二模式运行时，执行指令以访问第二模式资源，其中第一模式资源存储单元还包括资源映射单元，适于提供第二模式资源，处理器还包括访问控制接口，耦接到资源映射单元和第二模式资源存储单元，适于为资源映射单元提供到第二模式资源存储单元的访问通道，以及指令执行单元适于在处理器以第一模式运行时，执行指令访问资源映射单元，以便经由访问控制接口来访问第二模式资源存储单元中的第二模式资源。本发明还公开了包含该处理器的片上系统。



CN 111752604 A

1.一种具有多个运行模式的处理器,包括:

第一模式资源存储单元,适于存储在所述处理器以第一模式运行时的第一模式资源;

第二模式资源存储单元,适于存储在所述处理器以第二模式运行时的第二模式资源;以及

指令执行单元,适于在所述处理器以第一模式运行时,执行指令以访问所述第一模式资源,以及在所述处理器以第二模式运行时,执行指令以访问所述第二模式资源,

其中所述第一模式资源存储单元还包括资源映射单元,适于提供所述第二模式资源,

所述处理器还包括访问控制接口,耦接到所述资源映射单元和所述第二模式资源存储单元,适于为所述资源映射单元提供到所述第二模式资源存储单元的访问通道,以及

所述指令执行单元适于在所述处理器以第一模式运行时,执行指令访问所述资源映射单元,以便经由所述访问控制接口来访问所述第二模式资源存储单元中的第二模式资源。

2.如权利要求1所述的处理器,其中所述第一模式资源存储单元、第二模式资源存储单元和资源映射单元为寄存器。

3.如权利要求1或者2所述的处理器,其中所述第一模式为超级用户模式,且所述第二模式为普通用户模式。

4.如权利要求3所述的处理器,其中所述第一模式资源包括超级用户模式堆栈指针,且第二模式资源包括普通用户模式堆栈指针。

5.如权利要求1或者2所述的处理器,其中所述第一模式为可信世界模式,且第二模式为非可信世界模式。

6.如权利要求5所述的处理器,其中所述第一模式资源包括下列中的一个或者多个:可信世界堆栈指针、可信世界程序状态、可信世界异常入口基址、可信世界异常保留状态和可信世界异常保留程序计数器,

以及其中所述第二模式资源包括下列中的一个或者多个:非可信世界堆栈指针、非可信世界程序状态、非可信世界异常入口基址、非可信世界异常保留状态和非可信世界异常保留程序计数器。

7.如权利要求1或者2所述的处理器,还包括:

第三模式资源存储单元,适于存储在所述处理器以第三模式运行时的第三模式资源;

第四模式资源存储单元,适于存储在所述处理器以第四模式运行时的第四模式资源;以及

所述指令执行单元还适于在所述处理器以第三模式运行时,执行指令以访问所述第三模式资源,以及在所述处理器以第四模式运行时,执行指令以访问所述第四模式资源,

其中所述资源映射单元进一步适于提供所述第三和第四模式资源,

所述访问控制接口进一步耦接到所述第三和第四模式资源存储单元,适于为所述资源映射单元提供到所述第三和第四模式资源存储单元的访问通道,以及

所述指令执行单元适于在所述处理器以第一模式运行时,执行指令访问所述资源映射单元,以便进一步通过所述访问控制接口分别访问所述第二、第三和第四模式资源存储单元中的第二、第三和第四模式资源。

8.如权利要求7所述的处理器,其中,所述第一模式为可信世界超级用户模式,第二模式为可信世界普通用户模式,第三模式为非可信世界超级用户模式,以及第四模式为非可

信世界普通用户模式。

9.如权利要求8所述的处理器，其中所述第一模式资源包括下列中的一个或者多个：可信世界超级用户堆栈指针、可信世界程序状态、可信世界异常入口基址、可信世界异常保留状态和可信世界异常保留程序计数器；

所述第二模式资源包括可信世界普通用户堆栈指针；

所述第三模式资源包括下列中的一个或者多个：非可信世界超级用户堆栈指针、非可信世界程序状态、非可信世界异常入口基址、非可信世界异常保留状态和非可信世界异常保留程序计数器；以及

所述第四模式资源包括非可信世界普通用户堆栈指针。

10.一种具有多个运行模式的处理器，包括：

普通用户模式堆栈指针寄存器，适于存储所述处理器处于普通用户模式下的堆栈指针；

超级用户模式寄存器组，适于存储所述处理器处于超级用户模式下的各寄存器值，所述超级用户寄存器组包括映射寄存器，所述映射寄存器适于提供所述普通用户堆栈指针；

访问控制接口，耦接到所述映射寄存器和所述普通用户堆栈指针寄存器，适于为所述映射寄存器提供到所述普通用户堆栈指针寄存器的访问通道；

处理器状态寄存器，具有模式标识位来指示所述处理器处于普通用户模式还是超级用户模式，以及

指令执行单元，适于根据所述模式标识位的值来确定所述处理器处于普通用户模式还是超级用户模式下，并且在所述处理器处于超级用户模式下时，执行指令以访问所述映射寄存器，从而经由所述访问控制接口来访问所述普通用户堆栈指针寄存器中的普通用户堆栈指针。

11.一种具有多个运行模式的处理器，包括：

非可信世界寄存器组，适于存储所述处理器处于非可信世界模式下的各寄存器值；

可信世界寄存器组，适于存储所述处理器处于可信世界模式下的各寄存器值，所述可信世界寄存器组包括一个或者多个映射寄存器，每个映射寄存器适于提供所述非可信世界寄存器组中的一个非可信世界寄存器值；

访问控制接口，耦接到所述映射寄存器和所述非可信世界寄存器，适于为所述映射寄存器提供到所述非可信世界寄存器的访问通道；

处理器状态寄存器，具有可信标识位来指示所述处理器处于非可信世界模式还是可信世界模式，以及

指令执行单元，适于根据所述可信标识位的值来确定所述处理器处于可信世界模式还是非可信世界模式下，并且在所述处理器处于可信世界模式下时，执行指令以访问所述映射寄存器，从而经由所述访问控制接口来访问所述非可信世界寄存器中的寄存器值。

12.一种片上系统，包括如权利要求1-11中任一个所述的处理器。

一种具有多个运行模式的处理器

技术领域

[0001] 本发明涉及处理器领域，尤其涉及在具有多个运行模式的处理器领域。

背景技术

[0002] 在处理器领域，为了安全考虑，可以让处理器以超级用户模式和普通用户模式这两种不同的模式来运行。当处理器处于超级用户模式下时，可以获得更多的处理器权限并可以访问更多的处理器资源。让一般的应用程序在处理器中以普通用户模式来执行，而让操作系统内核以超级用户模式来运行，可以增加处理器的安全性。

[0003] 为了进一步加强安全性，在处理器的运行模式中新增一种可信世界状态，可信世界状态是一种安全、可信赖的运行模式，将处于可信世界的处理器、可信属性的系统IP以及其他系统中敏感、重要的软硬件资源划分到可信世界中，并通过硬件机制保证可信世界中的资源只能被可信世界中的成员所访问，从而实现可信世界与非可信世界的隔离，进一步确保安全资源的机密性以及完整性。

[0004] 在支持以多个模式运行的处理器结构中，处理器为每个模式提供了专门用于该模式的资源如寄存器组等。这样，以一个运行模式运行的处理器就不能直接访问在其它运行模式下的各种处理器资源，从而保证了处理器的安全。处理器需要进行模式切换以访问在其它模式下的处理器资源。

[0005] 然后，对于具有高权限的运行模式而言，在权限的许可下，应当可以访问具有较低权限的运行模式下的处理器资源。现有的模式切换方式使得访问过程开销较大，需要一种更为直接高效的方式，让高权限运行模式下的处理器直接访问低权限运行模式下的处理器资源。

发明内容

[0006] 为此，本发明提供了一种新的处理器，以力图解决或者至少缓解上面存在的至少一个问题。

[0007] 根据本发明的一个方面，提供了一种具有多个运行模式的处理器，包括：第一模式资源存储单元，适于存储在该处理器以第一模式运行时的第一模式资源；第二模式资源存储单元，适于存储在该处理器以第二模式运行时的第二模式资源；以及指令执行单元，适于在处理器以第一模式运行时，执行指令以访问第一模式资源，以及在处理器以第二模式运行时，执行指令以访问第二模式资源，其中第一模式资源存储单元还包括资源映射单元，适于提供第二模式资源，处理器还包括访问控制接口，耦接到资源映射单元和第二模式资源存储单元，适于为资源映射单元提供到第二模式资源存储单元的访问通道，以及指令执行单元适于在处理器以第一模式运行时，执行指令访问资源映射单元，以便经由访问控制接口来访问第二模式资源存储单元中的第二模式资源。

[0008] 可选地，在根据本发明的处理器中，第一模式资源存储单元、第二模式资源存储单元和资源映射单元为寄存器。

[0009] 可选地，在根据本发明的处理器中，第一模式为超级用户模式，且第二模式为普通用户模式。

[0010] 可选地，在根据本发明的处理器中，第一模式资源包括超级用户模式堆栈指针，且第二模式资源包括普通用户模式堆栈指针。

[0011] 可选地，在根据本发明的处理器中，第一模式为可信世界模式，且第二模式为非可信世界模式。

[0012] 可选地，在根据本发明的处理器中，第一模式资源包括下列中的一个或者多个：可信世界堆栈指针、可信世界程序状态、可信世界异常入口基址、可信世界异常保留状态和可信世界异常保留程序计数器，第二模式资源包括下列中的一个或者多个：非可信世界堆栈指针、非可信世界程序状态、非可信世界异常入口基址、非可信世界异常保留状态和非可信世界异常保留程序计数器。

[0013] 可选地，根据本发明的处理器还包括：第三模式资源存储单元，适于存储在处理器以第三模式运行时的第三模式资源；第四模式资源存储单元，适于存储在处理器以第四模式运行时的第四模式资源；以及指令执行单元还适于在处理器以第三模式运行时，执行指令以访问第三模式资源，以及在处理器以第四模式运行时，执行指令以访问第四模式资源，其中资源映射单元进一步适于提供第三和第四模式资源，访问控制接口进一步耦接到第三和第四模式资源存储单元，适于为资源映射单元提供到第三和第四模式资源存储单元的访问通道，以及指令执行单元适于在处理器以第一模式运行时，执行指令访问资源映射单元，以便进一步通过访问控制接口分别访问第二、第三和第四模式资源存储单元中的第二、第三和第四模式资源。

[0014] 可选地，在根据本发明的处理器中，第一模式为可信世界超级用户模式，第二模式为可信世界普通用户模式，第三模式为非可信世界超级用户模式，以及第四模式为非可信世界普通用户模式。

[0015] 可选地，在根据本发明的处理器中，第一模式资源包括下列中的一个或者多个：可信世界超级用户堆栈指针、可信世界程序状态、可信世界异常入口基址、可信世界异常保留状态和可信世界异常保留程序计数器；第二模式资源包括可信世界普通用户堆栈指针；第三模式资源包括下列中的一个或者多个：非可信世界超级用户堆栈指针、非可信世界程序状态、非可信世界异常入口基址、非可信世界异常保留状态和非可信世界异常保留程序计数器；以及第四模式资源包括非可信世界普通用户堆栈指针。。

[0016] 根据本发明的另一个方面，提供了一种片上系统，包括根据本发明的处理器。

[0017] 根据本发明的方案，在处理器具有较高权限的运行模式中引入资源映射单元，资源映射单元可以通过访问控制接口直接映射在较低权限的运行模式中的相应处理器资源。这样，当指令在较高权限运行模式下执行时，可以通过访问资源映射单元而直接访问在较低权限运行模式中的相应处理器资源，从而可以不用通过模式切换来获取较低权限运行模式下的处理器资源，减少了由于进行模式切换而产生的处理器开销，提高了处理器执行效率。

[0018] 另外，根据本发明的方案，可以与其它处理器资源相同的方式来定义资源映射单元，例如在处理器资源为各个寄存器内容时，可以将资源映射单元定义为一个或者一组专门的寄存器。这样，不需要对指令集进行扩充，通过在指令中访问为资源映射单元所定义的

寄存器就可以直接访问在其它低权限运行模式下的处理器资源，从而方便了处理器指令的设计和使用。

附图说明

[0019] 为了实现上述以及相关目的，本文结合下面的描述和附图来描述某些说明性方面，这些方面指示了可以实践本文所公开的原理的各种方式，并且所有方面及其等效方面旨在落入所要求保护的主题的范围内。通过结合附图阅读下面的详细描述，本公开的上述以及其它目的、特征和优势将变得更加明显。遍及本公开，相同的附图标记通常指代相同的部件或元素。

[0020] 图1示出了根据本发明一个实施例的处理器100的示意图；

[0021] 图2示出了根据本发明另一个实施例的处理器200的示意图；

[0022] 图3示出了根据本发明还有一个实施例的处理器300的示意图；

[0023] 图4示出了根据本发明还有另一个实施例的处理器400的示意图；以及

[0024] 图5示出了根据本发明还有另一个实施例的片上系统500的示意图。

具体实施方式

[0025] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0026] 图1示出了根据本发明一个实施例的处理器100的示意图。如图1所示，处理器100可以第一模式110和第二模式120运行。根据处理器200的结构设计，处理器200可以各种方式来定义运行模式。根据本发明的一个实施例，可以根据指令执行的身份而把处理器100的运行模式划分为超级用户运行模式110和普通用户运行模式120。根据另一种实施例，可以根据指令运行环境而将处理器100的运行模式划分为可信世界模式110和非可信世界模式120。本发明不受限于各个模式的具体划分形式，而且上面提及的执行模式可以进一步组合而形成更多的执行模式，例如，可信世界模式110和非可信世界模式120可以进一步细分为可信世界超级用户运行模式、可信世界普通用户运行模式、非可信世界超级用户运行模式和非可信世界普通用户运行模式。所有可以在处理器中定义各种不同运行模式的方式都在本发明的保护范围之内。

[0027] 当处理器100以一种运行模式运行时，处理器100为该运行模式提供在该模式下可用的资源。如图1所示，在处理器100包括在第一模式110下的第一模式资源存储单元112和在第二模式120下的第二模式资源存储单元122。

[0028] 第一模式资源存储单元112存储在处理器100以第一模式110运行时所提供的资源，而第二模式资源存储单元122存储在处理器100以第二模式120运行时所提供的资源。处理器100可以提供各种资源，例如各种寄存器，包括用于暂存数据的通用寄存器、用于矢量计算的通用矢量寄存器、控制寄存器和堆栈指针寄存器等。处理器100还可以提供专用于某个模式的存储空间，例如与模式相关的堆栈等。本发明不受限于资源的具体内容，所有专用于特定模式的资源都在本发明的保护范围之内。

[0029] 处理器在第一模式110下提供的资源和在第二模式120下提供的资源可以不同。在第一模式110具有高于第二模式120的权限的情况下，处理器在第一模式110下提供的资源通常多于在第二模式120下提供的资源。例如，当第一模式110为超级用户运行模式而第二模式120为普通用户运行模式时，处理器除了在第一模型110和第二模型120下都提供了用于堆栈指针的资源(例如，第一模式资源存储单元112包括用于超级用户模式堆栈指针的超级用户模式堆栈指针寄存器和第二模式资源存储单元122包括用于普通用户模式堆栈指针的普通用户模式堆栈指针寄存器)之外，在第一模式110下，处理器100还提供了多个用于存储处理器出现异常时的处理器现场内容寄存器。例如，第一模式资源存储单元112还包括用于保存异常入口基址的寄存器。

[0030] 为了能够在具有较高权限的第一模式中直接访问第二模式下的处理器资源，第一模式资源存储单元还包括资源映射单元114。资源映射单元114提供了第二模式资源存储单元122中所存储的内容。即，资源映射单元114提供了到第二模式资源存储单元122的访问接口，也就是说，资源映射单元114映射了第二模式资源存储单元122。当在第一模式下访问资源映射单元114时，就可以访问第二模式资源存储单元122中的内容。例如，在第一模式下，可以读取资源映射单元114的内容，从而读取第二模式资源存储单元122中的内容，而在资源映射单元114中写入内容，就可以在第二模式资源存储单元122中写入相应的内容。

[0031] 根据一种实施方式，为了便于处理器的执行和指令操作，资源映射单元114可以具有与所要映射的第二模式资源存储单元122相同的形式。例如，当要映射的第二模式资源存储单元122为寄存器时，则资源映射单元114也可以采用寄存器的形式。当要映射的第二模式资源存储单元122为一段存储空间时，资源映射单元114也可以是一段存储空间的形式。

[0032] 根据一种实施方式，处理器在第一模式和第二模式下都提供了多种资源，根据需要资源映射单元114可以仅仅对其中的一些资源进行映射，即资源映射单元114可以对第二模式资源存储单元122中的一个或者多个单元进行映射。例如，在第一模式110为超级用户运行模式而第二模式120为普通用户运行模式时，资源映射单元114可以对第二模式资源存储单元122中的普通用户模式堆栈指针寄存器进行映射，从而可以在超级用户模式下就可以获取到普通用户模式下的堆栈指针。

[0033] 为了让资源映射单元114可以对第二模式资源存储单元122进行映射，处理器100还包括访问控制接口130。访问控制接口130耦接到资源映射单元114和第二模式资源存储单元122，以便为资源映射单元114提供到第二模式资源存储单元122的访问通道。这样，当在处理器100以第一模式运行时，在读取资源映射单元114的内容时，就经由访问控制接口130读取第二模式资源存储单元122中存储的第二模式资源内容；以及在资源映射单元114中写入内容时，经由访问控制接口130在第二模式资源存单元122中写入第二模式资源内容。

[0034] 可以有多种方式来实现访问控制接口130。根据本发明的一种实施方式，当处理器100每次只能以一种模式来运行时，例如在第一模式100为可信世界模式而第二模式120为非可信世界模式时，如果处理器100仅仅可以每次要么以可信世界模式来执行要么以非可信世界模式来执行，则访问控制接口130可以获取在从第二模式120切换到第一模式110之前、第二模式资源存储单元在存储空间中的存储位置，在处理器100以第一模式110执行时，将该存储位置与资源映射单元114相关联，例如在处理器100切换到第一模式110时，从该存

储位置读取内容到资源映射单元114中，而在处理器100切换出第一模式110时，将资源映射单元114的内容写入到该存储位置处，从而实现了资源存储单元114和第二模式资源存单元122的映射。

[0035] 根据另一个实施方式，在处理器以第二模式120运行时，访问控制接口130可以实时监控第二模式资源存储单元122的值，并将其写入到存储空间中的预定存储位置。在处理器100以第一模式110执行时，将该存储位置与资源映射单元114相关联，例如在处理器100切换到第一模式110时，从该存储位置读取内容到资源映射单元114中，而在处理器100切换出第一模式110时，将资源映射单元114的内容写入到该存储位置处。而当处理器100切换回到第二模式时，可以从该存储位置读取内容写入到第二模式资源存储单元122中，从而实现了资源存储单元114和第二模式资源存单元122的映射。

[0036] 根据还有一种实施方式，处理器支持同时以第一模式110和第二模式120运行。例如，处理器100为多核处理器，其中的一个处理器内核以第一模式(可信世界模式)运行，而其它的处理器内核以第二模式(非可信世界模式)运行。此时，访问控制接口130可以使用存储空间中的专门存储区域，并实时监控在第二模式122下第二模式资源存储单元122中的值，并将其值写入到存储空间中的专门存储区域中。在处理器100在第一模式110下读取资源映射单元114的内容时，从该专门存储区域获取内容；当把内容写入到资源映射单元114中时，将该内容同样写入到专门存储区域中，并随后同步给第二模式资源存储单元122，从而实现了资源映射单元114和第二模式资源存储单元122的映射。

[0037] 本发明不受限于访问控制接口130的具体实现方式，所有可以在资源映射单元114和第二模式资源存储单元122之间建立映射关系的方式都在本发明的保护范围之内。

[0038] 处理器100支持以对应指令集编写的指令，并定义了在各种执行模式下提供的资源的对应指令或者操作数形式。例如，处理器100可以定义在第一模式110下提供的资源列表和第二模式120下提供的资源列表。并且处理器100还可以定义在第一模式110下的资源映射单元114的操作数形式。如上所述，资源映射单元114可以具有和要映射的第二模式资源存储单元122相同的形式，从而方便指令处理。

[0039] 如图1所示，处理器100还包括指令执行单元140。指令执行单元140执行经过译码后的指令。当处理器处于第一模式下时，指令执行单元140执行指令以访问在第一模式下提供的资源，而在处理器处于第二模式下时，执行指令以访问第二模式下提供的资源。当处理器100处于第一模式下时，如果指令中包括对资源映射单元114的访问，则指令执行单元140执行该指令以访问相应的资源映射单元114，从而进一步访问所映射的第二模式资源存储单元122中的内容。

[0040] 可选地，根据本发明的一个实施例，处理器100还包括模式标识150，以指示处理器100当前正处于哪个运行模式下。指令执行单元140可以根据该模式标识150的值所指示的运行模式(第一或者第二模式等)来访问在相应模式下的处理器资源。

[0041] 可选地，根据本发明的另一个实施例，处理器100还可以包括更多的运行模式。例如，处理器100可以包括第三模式160和第四模式170。相应地，处理器100包括第三模式资源存储单元160和第四模式资源存储单元170。第三模式资源存储单元162存储在处理器100处于第三模式160下提供的资源，而第四模式资源存储单元172存储在处理器100以第四模式170下提供的资源。

[0042] 资源映射单元114可以进一步提供到第三模式资源存储单元162和第四模式资源存储单元172的映射，从而处理器100以最高权限的第一模式110运行时，可以经由资源映射单元114访问分别在第二、第三和第四模式资源存储单元122、162和172中的内容。

[0043] 类似地，访问控制接口130还需要提供资源映射单元114到第三模式资源存储单元162和第四模式资源存储单元172的访问通道。

[0044] 应当注意的是，本发明可以扩展到具有更多模式的处理器100，并通过在较高权限的运行模式下的资源存储单元中提供资源映射单元，以便映射较低权限资源存储单元，从而可以在较高权限的操作模式下直接访问在较低权限的操作模式下的处理器资源。

[0045] 图2示出了图1所示的处理器100的一种具体实现方式的处理器200的示意图。在图2中，与图1所示的处理器100相同或者相似的部件以相同和相似的标号来表示，并且不再进行赘述。如图2所示，处理器200可以在两种模式下运行。第一模式110为超级用户模式，而第二模式120为普通用户模式。第一模式资源存储单元112包括超级用户模式寄存器组。超级用户寄存器组包括异常入口基址寄存器216、异常保留状态寄存器217和异常保留程序计数器寄存器218和超级用户模式堆栈指针寄存器219。第二模式资源存储单元122包括普通用户模式堆栈指针寄存器224。资源映射单元114为在超级用户模式寄存器组中的映射寄存器214，映射在第二模式下的普通用户模式堆栈指针寄存器224。

[0046] 模式标识150实现为处理器状态寄存器250中存储的寄存器值的状态位S。当S位的值为1时，处理器200处于超级用户模式下，而当S位值为0时，处理器200处于普通用户模式下。指令执行单元140根据S位的值来确定处理器200处于哪种模式下。

[0047] 根据本发明的一个实施方式，在处理器200所支持的指令集规范中，用相同的堆栈指针寄存器来分别在普通用户模式和超级用户模式下存储堆栈指针。指令执行单元140在执行指令时，如果处理器状态寄存器250中的状态位S位指示处理器200处于超级用户模式下，则堆栈指针寄存器用作超级用户模式堆栈指针寄存器219，并且从中可以获得超级用户模式堆栈指针；如果状态位S指示处理器200处于普通用户模式下，则堆栈指针寄存器用作普通用户模式堆栈指针寄存器224，并且从中可以获得普通用户模式堆栈指针。如果要在超级用户模式下获取普通用户模式堆栈指针的值，则可以执行指令来访问映射寄存器214，以通过访问控制接口130来访问普通用户模式堆栈指针。

[0048] 图3示出了图1所示的处理器100的一种具体实现方式的处理器300的示意图。在图3中，与图1所示的处理器100相同或者相似的部件以相同和相似的标号来表示，并且不再进行赘述。如图3所示，处理器300可以在两种模式下运行。第一模式110为可信世界模式，而第二模式120为非可信世界模式。第一模式资源存储单元112包括可信世界寄存器组。可信世界寄存器组包括通用寄存器GPR 311、矢量通用寄存器VGPR 312、控制寄存器CR 313、可信处理器状态寄存器T_PSR 314等。第二模式资源存储单元122也包括非可信世界寄存器组。非可信世界寄存器组除了包括与可信世界寄存器组中相对应的通用寄存器GPR 321、矢量通用寄存器VGPR 322、控制寄存器CR 323、非可信处理器状态寄存器NT_PSR 324之外，还包括非可信世界异常入口基址寄存器325、非可信世界异常保留状态寄存器326和非可信世界异常保留程序计数器寄存器327。资源映射单元114为在可信世界寄存器组中的映射寄存器组或者多个映射寄存器，可以分别对非可信世界模式下的非可信程序状态寄存器NT_PSR 324、非可信世界异常入口基址寄存器325、非可信世界异常保留状态寄存器326和非可信世

界异常保留程序计数器寄存器327进行映射。

[0049] 在处理器300中，模式标识150实现为处理器状态寄存器的状态位T。当T位的值为1时，处理器300处于可信世界模式下，而当T位值为0时，处理器300处于非可信世界模式下。指令执行单元140根据T位的值来确定处理器300处于哪种模式下。

[0050] 处理器300还包括分别位于可信世界模式110和非可信世界模式120中的可信处理器状态寄存器T_PSR 314和非可信程序状态寄存器NT_PSR 324。这两个寄存器具有基本相同的结构，并且可以相同的逻辑方式，即处理器状态寄存器PSR的名义提供访问。即当处理器300处于可信世界模式下时，当处理器300中的指令访问处理器状态寄存器PSR时，指令访问的是可信处理器状态寄存器T_PSR 314。当处理器300处于非可信世界模式中时，当处理器300中的指令访问PSR时，此时指令访问的是NT_PSR 324。

[0051] T_PSR 314和NT_PSR 324中具有可信世界状态位T做为模式标识150。当T的值为1时，指示处理器300当前处于可信世界模式下。当T的值为0时，指示处理器300当前处于非可信世界模式中。因此，T_PSR 314的T位值固定为1，而NT_PSR 324的T位值固定为0。

[0052] 指令执行单元140在执行指令时，如果处理器状态寄存器PSR中的状态位T位指示处理器300处于可信世界模式下，则可以访问可信世界寄存器组；如果状态位T指示处理器300处于非可信世界模式下，则可以访问非可信世界寄存器组。如果要在可信世界模式下获取非可信世界寄存器组中一些寄存器的值，则可以执行指令来访问映射寄存器组114中的映射寄存器，以通过访问控制接口130来访问非可信世界寄存器组中的相应非可信世界寄存器。

[0053] 图4示出了图1所示的处理器100的一种具体实现方式的处理器400的示意图。在图4中，与图1所示的处理器100相同或者相似的部件以相同和相似的标号来表示，并且不再进行赘述。如图4所示，处理器400可以在四种模式下运行。第一模式110为可信世界超级用户模式、第二模式120为可信世界普通用户模式、第三模式160为非可信世界超级用户模式、以及第四模式170为非可信世界普通用户模式。第一模式资源存储单元112包括可信世界超级用户寄存器组。可信世界超级用户寄存器组包括通用寄存器GPR 411、矢量通用寄存器VGPR 412、控制寄存器CR 413、可信处理器状态寄存器T_PSR 414和可信世界超级用户堆栈指针寄存器315等。第二模式资源存储单元122也包括可信世界普通用户寄存器组。可信世界普通用户寄存器组包括可信世界普通用户堆栈指针寄存器422。第三模式资源存储单元162包括非可信世界超级用户寄存器组。非可信世界超级用户寄存器组除了包括相应的通用寄存器GPR 461、矢量通用寄存器VGPR 462、控制寄存器CR 463、非可信处理器状态寄存器NT_PSR 464之外，还包括非可信世界异常入口基址寄存器465、非可信世界异常保留状态寄存器466、非可信世界异常保留程序计数器寄存器467和非可信世界超级用户堆栈指针寄存器468。第四模式资源存储单元172包括非可信世界普通用户寄存器组。非可信世界普通用户寄存器组包括非可信世界普通用户堆栈指针寄存器472。

[0054] 资源映射单元114为在可信世界超级用户寄存器组中的映射寄存器组或者多个映射寄存器，可以分别对可信世界普通用户模式下的可信世界普通用户堆栈指针寄存器212，非可信世界超级用户模式下的非可信世界处理器状态寄存器NT_PSR 464、非可信世界异常入口基址寄存器465、非可信世界异常保留状态寄存器466和非可信世界异常保留程序计数器寄存器467，以及非可信世界普通用户模式下的非可信世界普通用户堆栈指针寄存器472

进行映射。

[0055] 在处理器400中，模式标识150实现为处理器状态寄存器的状态位T和状态位S。当T的值为1且S的值为1时，处理器400处于可信世界超级用户模式下；当T的值为1且S的值为0时，处理器400处于可信世界普通用户模式下；当T的值为0且S的值为1时，处理器400处于非可信世界超级用户模式下；而当T的值为0且S的值为0时，处理器400处于非可信世界普通用户模式下。指令执行单元140根据T位和S位的值来确定处理器400处于哪种模式下。

[0056] 根据本发明的处理器结构，可以在较高权限的运行模式下的资源存储单元中提供资源映射单元，以便映射较低权限运行模式下的资源存储单元，从而可以在较高权限的操作模式下直接访问在较低权限的操作模式下的处理器资源。这样就不用通过处理器进行模式切换就可以访问在低权限的操作模式下的处理器资源，从而节省了处理器开销。

[0057] 上面参考图1-4所描述的处理器可以包含在处理系统中。处理系统还可以包括其它部件如各种中断源、协处理器和存储设备等。这些部件和处理器一起构成了一个处理系统。根据一种实施方式，这种处理系统包括SoC(片上系统)等。

[0058] 图5示出了根据本发明一个实施例的片上系统(SoC)500的示意图。片上系统500包括参考图1-4所述的处理器100-400(在图5中以标号510表示)、各种中断源520、存储空间530和协处理器540等。片上系统500可以集成在一块电路板上，并构成了一个相对完整的处理系统。中断源520例如为各种外设接口，接收外部输入并且输出处理器510经过处理之后的输出。存储空间530可以为处理器510提供外部存储空间，用于存储处理器510要执行的代码和产生的各种输出数据。协处理器540为一种专门的处理器，用于执行专门的处理任务，例如图像运算等。

[0059] 应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0060] 本领域那些技术人员应当理解在本文所公开的示例中的设备的模块或单元或组件可以布置在如该实施例中所描述的设备中，或者可替换地可以定位在与该示例中的设备不同的一个或多个设备中。前述示例中的模块可以组合为一个模块或者此外可以分成多个子模块。

[0061] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0062] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0063] 此外，所述实施例中的一些在此被描述成可以由计算机系统的处理器或者由执行所述功能的其它装置实施的方法或方法元素的组合。因此，具有用于实施所述方法或方法元素的必要指令的处理器形成用于实施该方法或方法元素的装置。此外，装置实施例的在此所述的元素是如下装置的例子：该装置用于实施由为了实施该发明的目的的元素所执行的功能。

[0064] 如在此所使用的那样，除非另行规定，使用序数词“第一”、“第二”、“第三”等等来描述普通对象仅仅表示涉及类似对象的不同实例，并且并不意图暗示这样被描述的对象必须具有时间上、空间上、排序方面或者以任意其它方式的给定顺序。

[0065] 尽管根据有限数量的实施例描述了本发明，但是受益于上面的描述，本技术领域内的技术人员明白，在由此描述的本发明的范围内，可以设想其它实施例。此外，应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

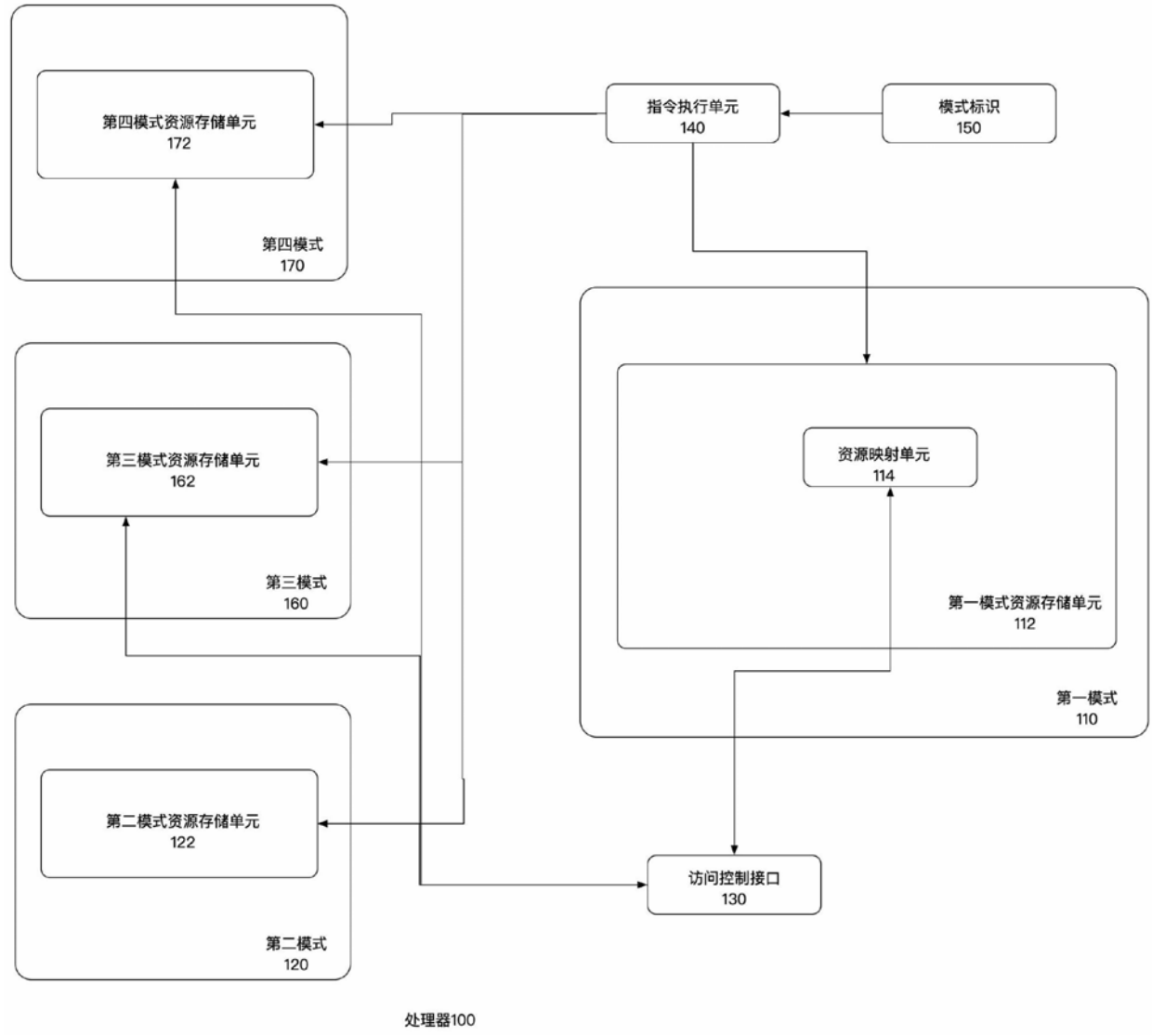

第四模式资源存储单元
172
第四模式
170
指令执行单元
140
模式标识
150
第三模式资源存储单元
162
第三模式
160
资源映射单元
114
第一模式资源存储单元
112
第一模式
110
第二模式资源存储单元
122
第二模式
120
访问控制接口
130
处理器100

图1

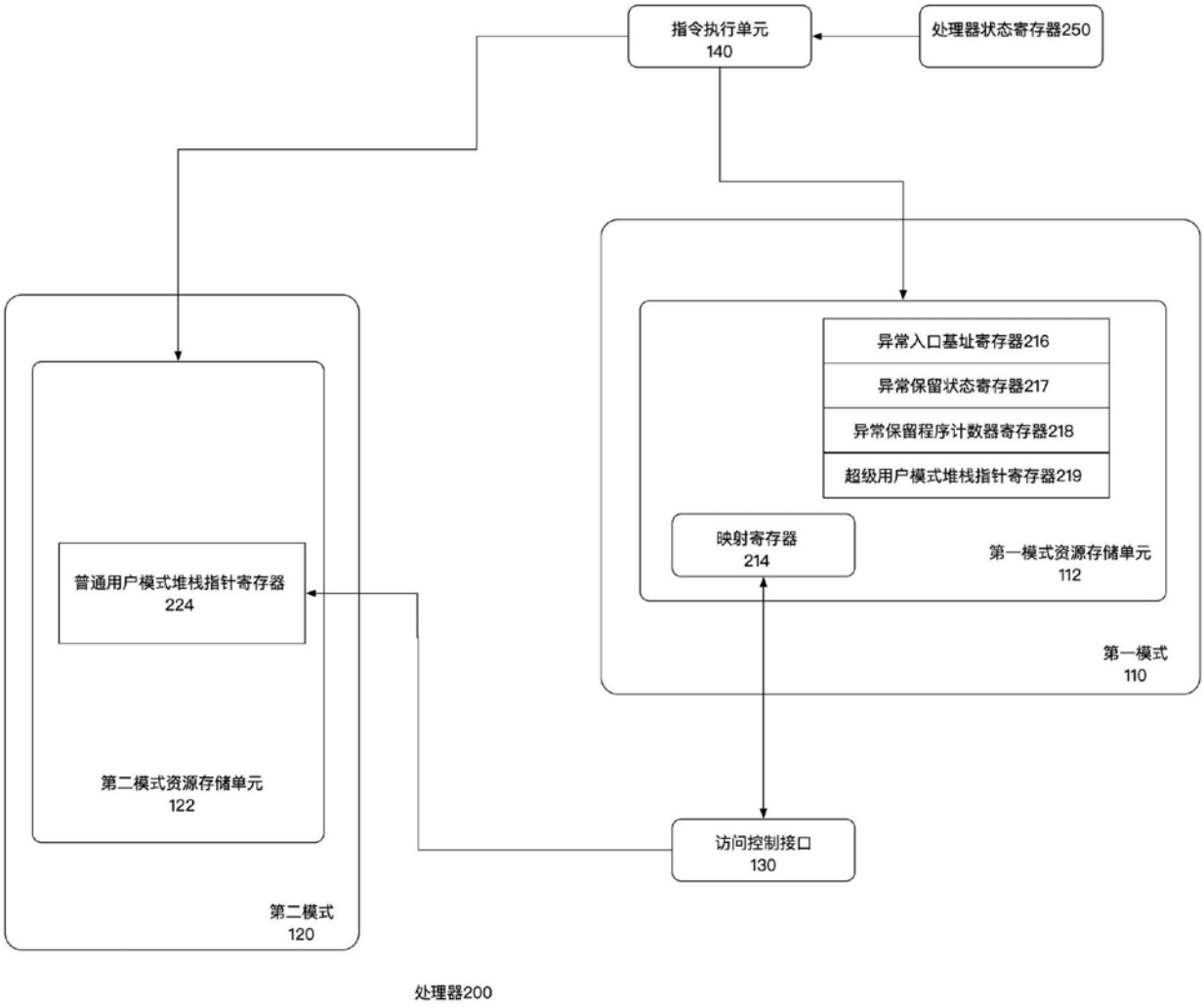

指令执行单元
140
处理器状态寄存器250
异常入口基址寄存器216
异常保留状态寄存器217
异常保留程序计数器寄存器218
超级用户模式堆栈指针寄存器219
映射寄存器
214
第一模式资源存储单元
112
第一模式
110
普通用户模式堆栈指针寄存器
224
第二模式资源存储单元
122
访问控制接口
130
第二模式
120
处理器200

图2

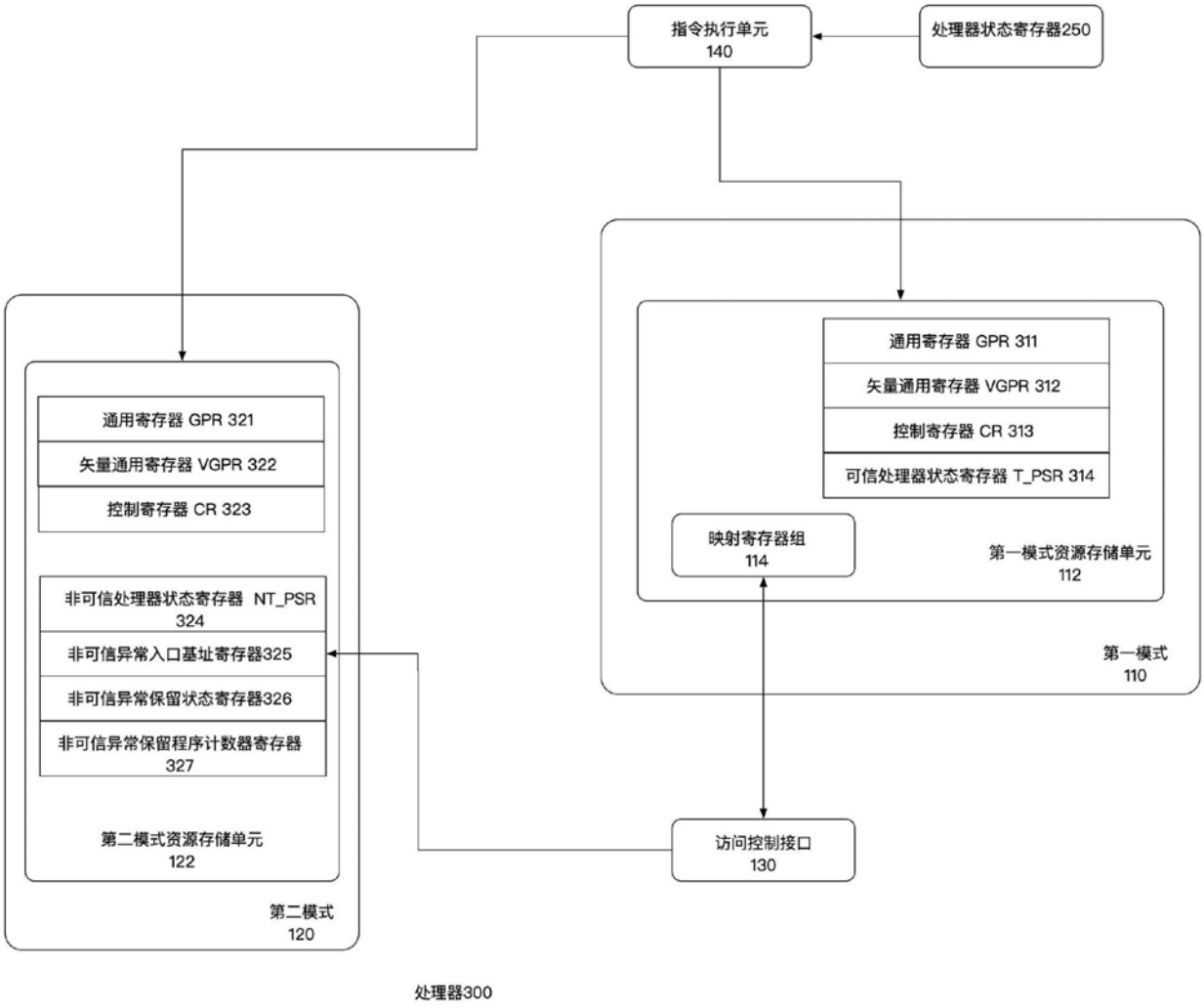

指令执行单元
140
处理器状态寄存器250
通用寄存器 GPR 311
矢量通用寄存器 VGPR 312
控制寄存器 CR 313
可信处理器状态寄存器 T_PSR 314
映射寄存器组
114
第一模式资源存储单元
112
第一模式
110
通用寄存器 GPR 321
矢量通用寄存器 VGPR 322
控制寄存器 CR 323
非可信处理器状态寄存器 NT_PSR
324
非可信异常入口基址寄存器325
非可信异常保留状态寄存器326
非可信异常保留程序计数器寄存器
327
第二模式资源存储单元
122
第二模式
120
访问控制接口
130
处理器300

图3

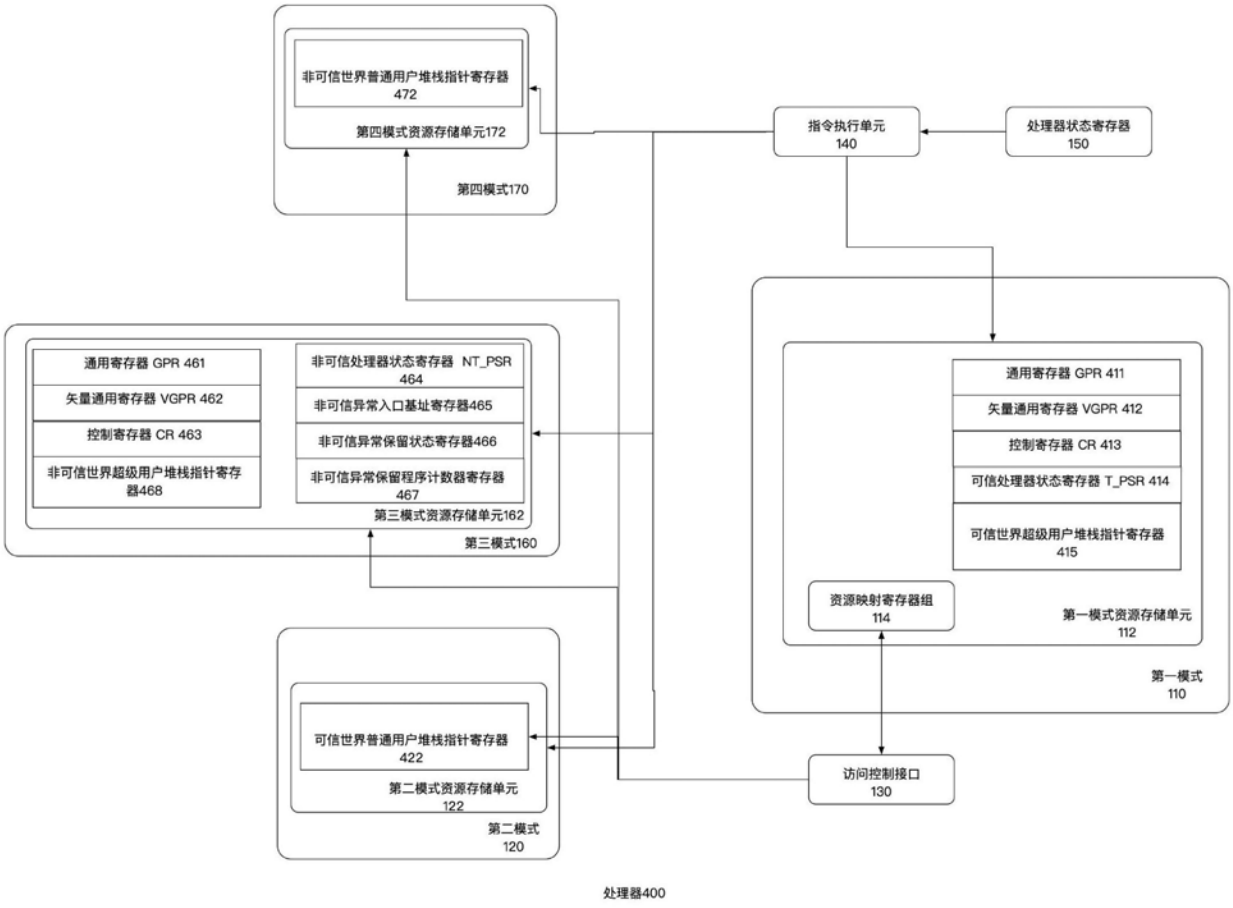

非可信世界普通用户堆栈指针寄存器 472
第四模式资源存储单元172
第四模式170
指令执行单元 140
处理器状态寄存器 150
通用寄存器 GPR 461
矢量通用寄存器 VGPR 462
控制寄存器 CR 463
非可信世界超级用户堆栈指针寄存器468
非可信处理器状态寄存器 NT_PSR 464
非可信异常入口基址寄存器465
非可信异常保留状态寄存器466
非可信异常保留程序计数器寄存器 467
第三模式资源存储单元162
第三模式160
通用寄存器 GPR 411
矢量通用寄存器 VGPR 412
控制寄存器 CR 413
可信处理器状态寄存器 T_PSR 414
可信世界超级用户堆栈指针寄存器 415
资源映射寄存器组 114
第一模式资源存储单元 112
第一模式 110
可信世界普通用户堆栈指针寄存器 422
第二模式资源存储单元 122
第二模式 120
访问控制接口 130
处理器400

图4

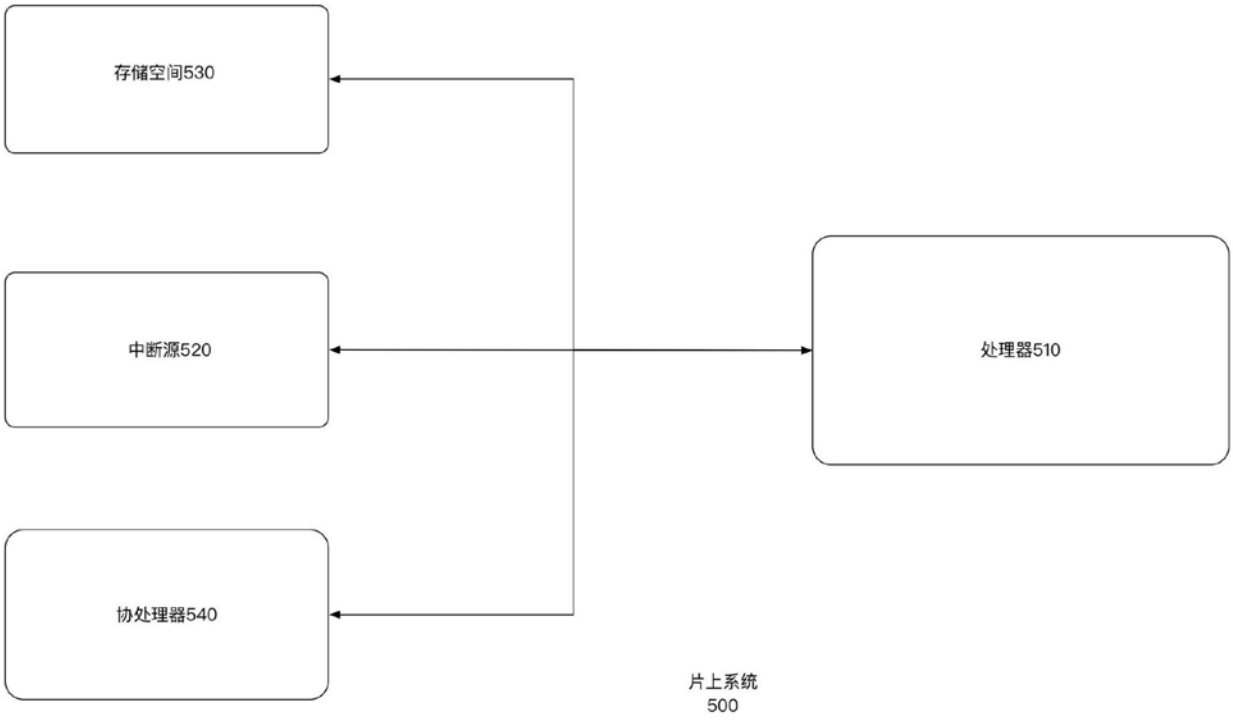


图5