



(12) 发明专利

(10) 授权公告号 CN 1875341 B

(45) 授权公告日 2012.05.23

(21) 申请号 200480031824.X

(22) 申请日 2004.10.28

(30) 优先权数据

10/697,635 2003.10.29 US

(85) PCT申请进入国家阶段日

2006.04.27

(86) PCT申请的申请数据

PCT/US2004/036287 2004.10.28

(87) PCT申请的公布数据

W02005/043336 EN 2005.05.12

(73) 专利权人 高通股份有限公司

地址 美国加利福尼亚州

(72) 发明人 布赖恩·哈罗德·凯利

拉梅什·钱德拉塞卡尔

(74) 专利代理机构 北京律盟知识产权代理有限

责任公司 11287

代理人 王允方 刘国伟

(51) Int. Cl.

G06F 7/00(2006.01)

(56) 对比文件

US 6175916 B1, 2001.01.16, 全文.

CN 1486093 A, 2004.03.31, 全文.

CN 1412995 A, 2003.04.23, 全文.

US 6594671 B1, 2003.07.15, 全文.

US 6349355 B1, 2002.02.19, 摘要, 说明书第6栏第1-6行, 第8栏第19-28行, 第11栏第8行至第12栏第13行, 第13栏第37-42, 56-62行, 第14栏第13-31行.

US 6274064 B1, 2001.06.12, 全文.

审查员 郭全萍

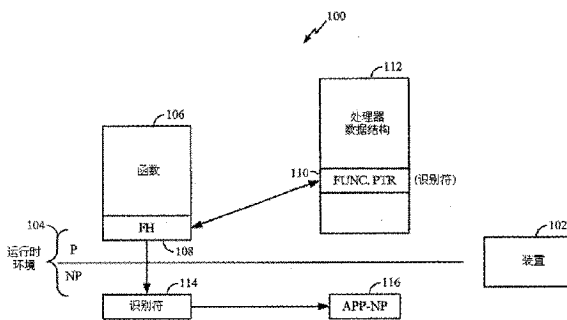
权利要求书 1 页 说明书 5 页 附图 3 页

(54) 发明名称

用于装置中特权模式挂接的动态注册的系统

(57) 摘要

本发明提供一种用于在一装置中动态注册特权模式挂接(hooks)的系统。所述系统包含一种在一装置中动态注册一函数的方法,所述装置包含包括一特权模式和一非特权模式在内的至少两个操作模式。所述方法包括:识别一将识别符映射到函数的数据结构中的一可用槽(slot);和存储一与所述槽中的所述函数关联的指针。所述方法还包括:检索一与所述槽关联的识别符;和使非特权应用程序可访问所述识别符。



1. 一种用于在一装置中动态地注册一特权函数的方法,所述装置包含包括一特权模式和一非特权模式在内的至少两个操作模式,所述方法包括:

识别一将识别符映射到特权函数的数据结构中的一可用槽;

存储一指向所述槽中的所述特权函数的指针;

检索一与所述槽关联的识别符;

将所述识别符存储在可被非特权应用程序访问的位置中;和

通过所述识别符来访问所述特权函数以便为特权应用程序和非特权应用程序执行服务。

2. 根据权利要求 1 所述的方法,其中所述数据结构为一将识别符映射到函数的表。

3. 根据权利要求 2 所述的方法,其中所述识别符为一进入所述表的索引。

4. 根据权利要求 1 所述的方法,其中所述装置为一无线装置。

5. 根据权利要求 1 所述的方法,其进一步包括在装置初始化期间执行所述注册。

6. 一种用于在一装置中动态地注册一特权函数的设备,所述装置包含包括一特权模式和一非特权模式在内的至少两个操作模式,所述设备包括:

用以识别一将识别符映射到特权函数的数据结构中的一可用槽的构件;

用以存储一指向所述槽中的所述特权函数的指针的构件;

用以检索一与所述槽关联的识别符的构件;

用以将所述识别符存储在可被非特权应用程序访问的位置中的构件;和

通过所述识别符来访问所述特权函数以便为特权应用程序和非特权应用程序执行服务的构件。

7. 根据权利要求 6 所述的设备,其中所述数据结构为一将识别符映射到函数的表。

8. 根据权利要求 7 所述的设备,其中所述识别符为一进入所述表的索引。

9. 根据权利要求 6 所述的设备,其中所述装置为一无线装置。

10. 根据权利要求 6 所述的设备,其进一步包括用以在装置初始化期间执行所述注册的构件。

## 用于装置中特权模式挂接的动态注册的系统

### 技术领域

[0001] 本发明大体上涉及一装置的有效操作,且更特定地说涉及一种用于在一装置中的特权模式挂接的动态注册的系统。

### 背景技术

[0002] 技术进步促成了家庭、办公和个人用途的各种装置的发展。举例而言,例如桌上型计算机、笔记本计算机和平板计算机的计算机系统已成为用于家庭或办公环境的强大工具。例如无线电话、个人数字助理(PDA)和传呼装置的个人装置也已变得更加强大且正被广泛使用。

[0003] 如今许多装置包括运行例如 UNIX、LINUX 的操作系统或类似操作系统的复杂硬件和软件。通常,这些操作系统提供多种操作模式。举例而言,大多数系统提供特权操作模式和非特权操作模式。允许以特权操作模式执行的程序无限制地访问存储器和系统资源。限制以非特权模式执行的程序访问特定存储区域和/或装置系统。此配置对于重要的存储器或装置函数提供某种程度的保护。举例而言,通过以非特权模式执行第三方应用程序,可保护重要的存储区域和装置函数免遭非授权访问。并且,此配置允许系统在执行期间将故障隔离开来。

[0004] 随着时间推移,这些系统已变得更加复杂以便满足装置和装置用户的日益增长的需要。举例而言,使用函数模块或函数来提供多种系统服务。随着装置已变得更加复杂且具有丰富特征,与这些特征关联的函数的数量和复杂性也已增加。

[0005] 不幸的是,常规系统在支援函数模块方面具有若干局限性。举例而言,常规系统可具有用以访问函数的有限数量的挂接。举例而言,系统可具有用以访问函数的有限数量的陷阱。此外,将陷阱定义编译成一个在装置上运行的可执行二进制,此对系统灵活性造成固有限制。

[0006] 因此,需要这样一种系统,其提供动态地注册对特权函数的挂接的方式。所述系统应允许在系统初始化期间注册函数,藉此提供灵活性并避免常规系统中固有的将陷阱定义编译成可执行的潜在版本确定问题。所述系统也应允许注册无限数量的函数,藉此克服与常规系统相关的将固定数量的可用陷阱与函数相关联的局限性。

### 发明内容

[0007] 在一或一个以上实施例中,提供一种包括方法和/或设备的系统,所述系统运行以便提供装置中特权模式挂接的动态注册。在一实施例中,不同程序模块在系统初始化期间安装挂接。每一函数模块在安装时均分配有一识别符,且所述模块将此识别符保留于非特权应用程序可读取的一变量中。当从一以非特权模式执行的应用程序中调用时,所述模块从变量检索其挂接识别符以便执行所述挂接。此避免常规系统中固有的将函数与编译为可执行二进制的固定数量的陷阱相关联的潜在版本确定问题。

[0008] 在一实施例中,提供一种用于在装置中动态地注册一函数的方法,所述装置包含

包括特权模式和非特权模式在内的至少两种操作模式。所述方法包括：识别将识别符映射到函数的数据结构中的可用槽；和存储与所述槽中的所述函数关联的指针。所述方法还包括：检索与所述槽关联的识别符；和使非特权应用程序可访问所述识别符。

[0009] 在另一实施例中，提供一种用于在装置中动态地注册一函数的设备，所述装置包含包括特权模式和非特权模式在内的至少两种操作模式。所述设备包括：用以识别将识别符映射到函数的数据结构中的可用槽的逻辑；和用以存储与所述槽中的所述函数关联的指针的逻辑。所述设备还包括：用以检索与所述槽关联的识别符的逻辑；和用以使非特权应用程序可访问所述识别符的逻辑。

[0010] 在另一实施例中，提供一种用于在装置中动态地注册一函数的设备，所述装置包含包括特权模式和非特权模式在内的至少两种操作模式。所述设备包括：用以识别将识别符映射到函数的数据结构中的可用槽的构件；和用以存储与所述槽中的所述函数关联的指针的构件。所述设备还包括：用以检索与所述槽关联的识别符的构件；和用以使非特权应用程序可访问所述识别符的构件。

[0011] 在另一实施例中，提供一种包括指令的计算机可读媒体，当装置中的处理器执行所述指令时，所述指令运行以在所述装置中动态地注册一函数。所述装置包含包括特权模式和非特权模式在内的至少两种操作模式。所述计算机可读媒体包括：用以识别将识别符映射到函数的数据结构中的可用槽的指令；和用以存储与所述槽中的所述函数关联的指针的指令。所述计算机可读媒体还包括：用以检索与所述槽关联的识别符的指令；和用以使非特权应用程序可访问所述识别符的指令。

[0012] 在阅读下述附图说明、具体实施方式和权利要求书之后，将更容易了解本发明的其他方面、优点和特征。

## 附图说明

[0013] 结合附图参看以下具体实施方式，将更容易了解本文中所描述的实施例的前述方面和相应优点，在附图中：

[0014] 图 1 展示动态注册系统的一实施例，所述动态注册系统运行以便提供装置中的特权模式挂接的动态注册；

[0015] 图 2 展示一包括动态注册系统的一实施例的装置的方框图；且

[0016] 图 3 展示说明用于装置中的动态注册系统的一实施例操作的流程图。

## 具体实施方式

[0017] 以下具体实施方式描述一种动态注册系统，其运行以便提供装置中的特权模式挂接的动态注册。举例而言，所述系统运行以便允许在装置初始化过程期间或在调用函数之前的任何时刻注册函数挂接。在一实施例中，注册过程产生存储于静态变量中的函数识别符，所述静态变量可由特权和非特权两种应用程序读取。特权或非特权应用程序通过获得识别符而可访问所述函数所提供的服务。因为通过每一注册函数自身的接口来访问每一注册函数，所以所述系统克服了常规系统中将函数与固定数量的陷阱相关联的相关问题。

[0018] 在一或一个以上实施例中，注册系统与执行于装置上的运行环境（或操作系统）互动，所述运行环境（例如）通过提供对于装置特定资源的一般调用来简化装置操作。此

类运行环境中的一种为由加州圣地亚哥市的 QUALCOMM 公司开发的无线二进制运行环境™(BREW™) 软件平台。以下实施方式描述一执行例如 BREW 软件平台的运行环境的装置。然而,在一个或一个以上实施例中,所述注册系统适合于与其他类型的运行环境一起使用,以便提供多种装置中的特权函数挂接的快速且有效的注册,所述多种装置包含产生系统或其他控制或监视程序。举例而言,所述装置可包含(但不限于)桌上型计算机、笔记本计算机、手提计算机,和例如无线电话、传呼机、PDA、电子邮件装置、平板计算机的便携式装置,或其他类型计算装置。

[0019] 图 1 展示动态注册系统 100 的一实施例,所述动态注册系统 100 运行以便提供在装置 102 中的特权模式挂接的动态注册。系统 100 可为家用计算机、办公计算机或例如无线电话或 PDA 的个人装置或者任何其他类型计算装置的一部分。

[0020] 在一实施例中,装置 102 包含一运行环境 104(意即, BREW),其提供至少两种操作模式,即非特权模式(NP)和特权模式(P)。非特权操作模式用来限制对运行于装置上的应用程序的访问并提供故障检测。举例而言,将以非特权模式运行的应用程序限制于选定的存储区域,且可拒绝其访问装置寄存器或其他资源。特权操作模式允许在此模式下运行的应用程序不受限制地访问存储器或装置资源。

[0021] 在系统初始化期间,动态地注册函数 106 以便允许执行于装置上的应用程序从函数 106 获得服务。与所述函数关联的函数处理器 108 运行以便在处理器数据结构 112 中查找一可用槽 110。处理器 108 存储一函数指针,所述函数指针指向可用槽 110 中的函数 106。槽 110 具有一相关识别符(或索引),所述相关识别符由处理器 108 检索并存储于非特权应用程序可访问的存储器或其他区域中。举例而言,在一实施例中,将识别符存储于非特权模式可访问的静态变量 114 中。非特权应用程序 116 可读取所述静态变量 114。因此,函数 106 经注册以供执行于装置上的应用程序使用。使用相同处理过程来注册一个或任何数量的函数。每一函数使用处理器数据结构 112 中的可用槽,并将其相关识别符存储于(例如)非特权应用程序可读取的静态变量中。

[0022] 在装置操作期间,应用程序 116 在装置 102 上执行,以便为装置 102 提供信息、功能和/或服务。举例而言,一种类型的应用程序可为查看器应用程序,其在装置 102 上运行以便显示电影、新闻或其他类型多媒体内容。

[0023] 当应用程序 116 在装置 102 上执行时,其在运行环境下运行以便提供所需功能性。如果应用程序 116 需访问函数 106 以获得服务,那么应用程序 114 从静态变量 114 中检索识别符并使用所述识别符来访问函数 106。

[0024] 图 2 展示装置 102 的函数方框图,其包括动态注册系统的一实施例。装置 102 包括处理逻辑 202 和耦接到内部数据总线 204 的装置资源 206。所述装置资源 206 包括硬件、软件、存储器、逻辑和/或允许所述装置连接到各种内部和外部资源、装置或系统的其他资源。代码存储器 208 和数据存储器 210 也耦接到处理逻辑 202。

[0025] 在一或一个以上实施例中,处理逻辑 202 包括 CPU、处理器、门阵列、硬件逻辑、存储器元件、虚拟机、软件、I/O 接口和/或硬件与软件的任何组合。因此,处理逻辑 202 通常包括用来执行机器可读指令的逻辑。举例而言,可从一例如软盘、CDROM、闪存的计算机可读媒体,或通过装置资源 206 而连接到装置 102 的其他计算机可读媒体将指令载入装置 102 中。在另一实施例中,可从一例如网络服务器的网络资源或通过装置资源 206 而连接到装

置 102 的任何其他类型的网络资源将指令下载到装置 102 中。当处理逻辑 202 执行指令时，所述指令提供如本文中所述的动态注册系统的一个或一个以上实施例。

[0026] 在一实施例中，代码存储器 208 包括 RAM、ROM、FLASH、EEROM 或任何其他适宜类型的存储器或其组合。通过存储器管理单元 216 的操作将代码存储器 206 分割成特权区域 (P) 212 和非特权区域 (NP) 214。所述 MMU 216 运行以便限制非特权程序代码的操作，从而使非特权代码对于代码存储器 208 的选定区域具有有限访问权。

[0027] 特权区域 212 包含程序代码，当所述程序代码被执行时，其对于存储器或装置 102 的其他系统具有无限制访问权。举例而言，特权代码区域 212 包括操作系统代码 (OS)、用户接口代码 (UI)、函数处理器 108 和特权函数代码 106。特权代码区域 212 中所展示的代码代表可包含于装置 102 中的类型的特权代码。特权代码区域 212 也可能包含用于在装置 102 上执行的其他类型的特权代码。

[0028] 非特权代码区域 214 包含程序代码，当所述程序代码被执行时，其受到限制而仅访问选定的存储区域。举例而言，非特权代码区域 214 包括 OS 代码和应用程序代码 (App-NP) 116。

[0029] 在一实施例中，数据存储器 210 包括特权区域 216 和非特权区域 218。所述特权区域 226 包括仅可由特权程序代码访问的数据区域。举例而言，特权数据区域 216 包括 OS、UI 所使用的数据和函数 106 所使用的函数数据。数据区域 216 也包括处理器数据结构 112。

[0030] 所述非特权数据区域 218 包含可由非特权程序代码访问的数据区域。举例而言，非特权数据区域 218 包括由非特权 OS 和 App-NP 116 所使用的数据。数据区域 218 也包括保存有与函数 106 关联的识别符的静态变量 114。MMU 220 运行以便限制对于非特权和特权数据区域的访问。举例而言，限制非特权应用程序访问特权数据区域 216 中的数据或属于非特权数据区域 218 中其他非特权应用程序的数据。

[0031] 应注意，所述装置 102 的配置仅为一种适合实施所述注册系统的配置。也可能使用本发明范畴内的其他装置配置、功能元件或元件配置来实施注册系统的一个或一个以上实施例。

[0032] 在装置 102 运行期间，动态注册系统在初始化过程期间注册一个或一个以上函数。举例而言，在一实施例中，在初始化期间逐个注册函数直到已注册了所有函数为止。为每一函数判定结构 112 中的一可用槽，且使每一个别槽的识别符可用，从而使得其可由非特权应用程序读取。

[0033] 在一实施例中，所描述的注册系统包括存储于计算机可读媒体上的程序指令，当处理逻辑 202 执行所述程序指令时，所述程序指令提供本文中所描述的功能。在一个或一个以上实施例中，计算机可读媒体包括软盘、CD、存储卡、FLASH 存储装置、RAM、ROM 或任何其他类型的存储装置。

[0034] 图 3 展示一说明在装置（例如装置 102）中使用的注册系统的一实施例的操作流程图 300。为清晰起见，将参看图 2 中所展示的装置 102 来描述流程图 300。将假设所述装置正执行 BREW 运行时环境，且处理逻辑 202 执行存储于代码存储器 208 中的程序指令以便执行下文描述的功能。

[0035] 在方块 302 处，注册过程以找出处理器数据结构中一可用槽而开始。举例而言，处理逻辑 202 执行程序指令以便在数据结构 112 中搜寻一可用槽。在一实施例中，所述数据

结构 112 为一表,且所述表中的每一项均为一槽。每一槽可存储一函数的地址指针,且每一槽具有一相关识别符(例如表索引)。

[0036] 在方块 304 处,在已找到所述可用槽之后,将待注册的函数的指针存储于所述槽中。举例而言,将函数 Func 106 的地址指针存储于可用槽 110 中。

[0037] 在方块 306 处,使槽识别符可用于供非特权应用程序进行读取访问。举例而言,槽识别符存储于非特权应用程序可读取的一静态变量中。举例而言,所述变量可位于一赋予特权应用程序读取/写入特权且赋予非特权应用程序只读特权的数据区域中。

[0038] 在方块 308 处,使用识别符来访问特权函数以便为特权和非特权应用程序执行服务。关于如何使用识别符来访问特权函数,读者可参考标题为“SYSTEM FOR PROVIDING TRANSITIONS BETWEEN OPERATING MODES OF A DEVICE”的代理人案号为第 030620 号的美国专利申请案,其以引用的方式并入本文中。

[0039] 应注意,程序流程图 300 仅说明一实施例,且在不背离本发明范畴的前提下可对程序元件做出变化、添加或重新配置。

[0040] 因此,尽管本文已说明并描述动态注册系统的方法和设备的一个或一个以上实施例,但应了解,在不背离实施例精神或本质特征的前提下可对所述实施例做出各种变化。因此,本文中的揭示内容和描述仅旨在说明而非限定上述权利要求书中所陈述的本发明范畴。

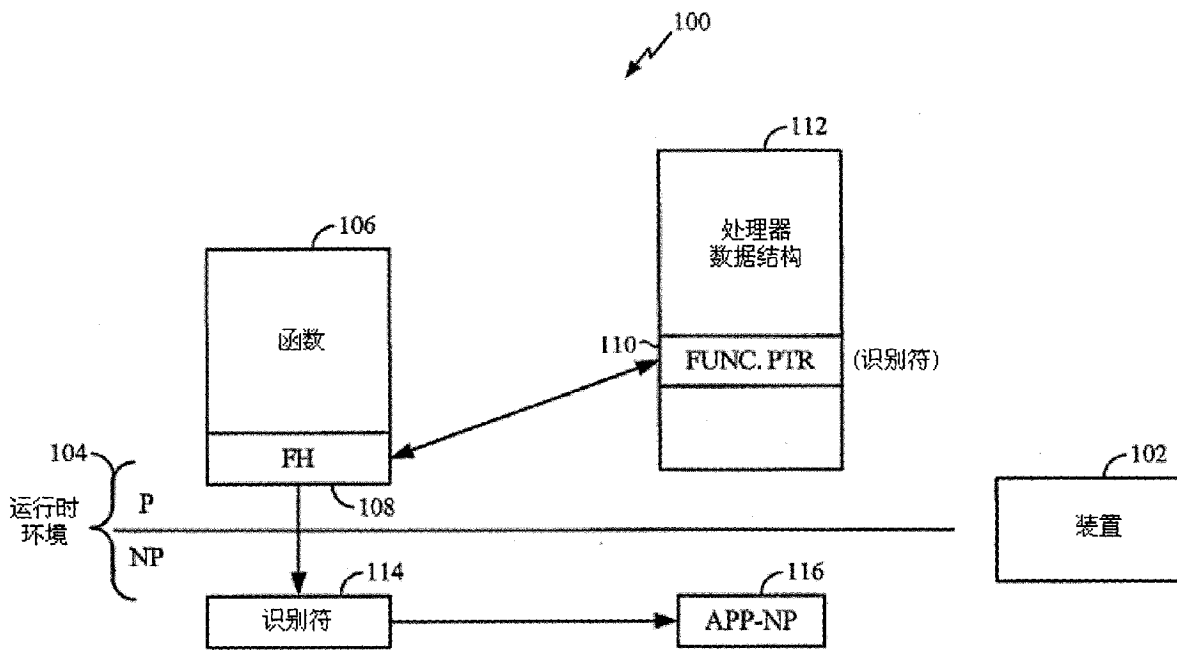


图1

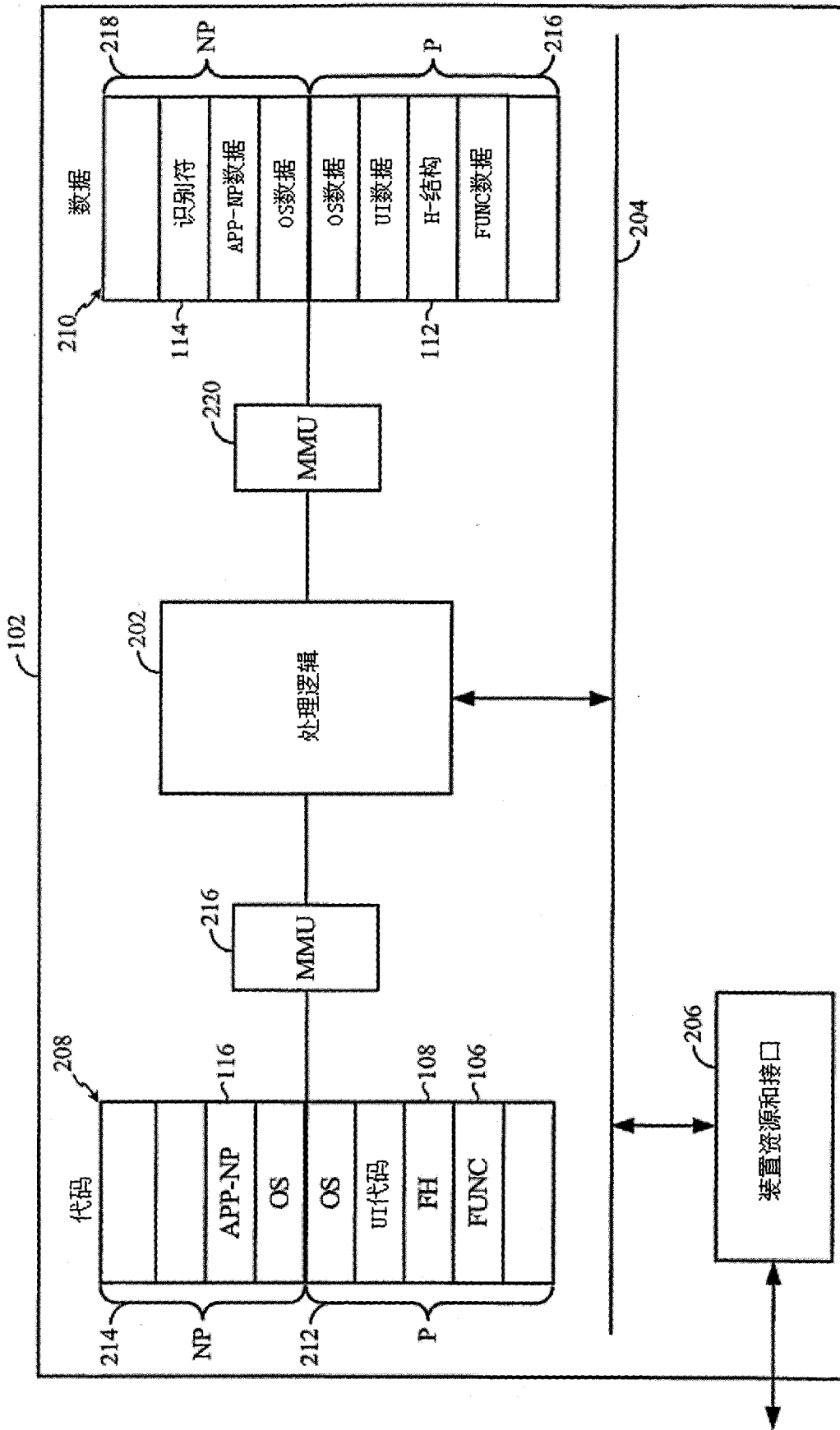


图2

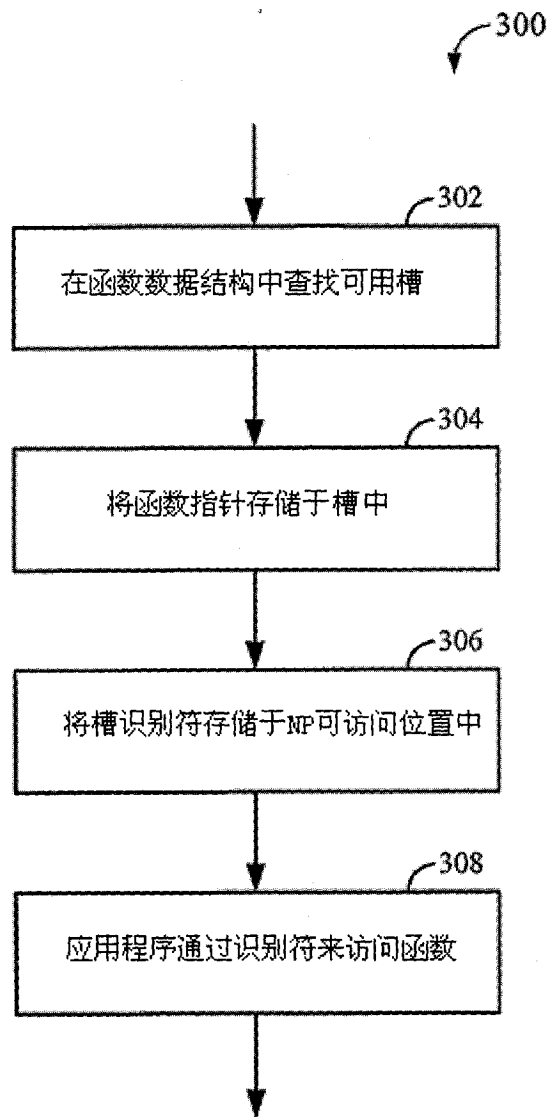


图3