



(12)发明专利

(10)授权公告号 CN 103270519 B

(45)授权公告日 2016.09.21

(21)申请号 201180061987.2

(73)专利权人 英特尔公司

(22)申请日 2011.12.20

地址 美国加利福尼亚州

(65)同一申请的已公布的文献号

(72)发明人 M·D·伍德 Y·圣希莱尔

申请公布号 CN 103270519 A

(74)专利代理机构 上海专利商标事务所有限公司 31100

(43)申请公布日 2013.08.28

代理人 姬利永

(30)优先权数据

(51)Int.CI.

12/978,457 2010.12.24 US

G06F 21/57(2013.01)

(85)PCT国际申请进入国家阶段日

(56)对比文件

2013.06.21

US 2008/0288783 A1,2008.11.20,

(86)PCT国际申请的申请数据

US 2008/0288783 A1,2008.11.20,

PCT/US2011/066014 2011.12.20

US 2002/0188763 A1,2002.12.12,

(87)PCT国际申请的公布数据

US 2004/0172512 A1,2004.09.02,

W02012/088029 EN 2012.06.28

审查员 李婧雯

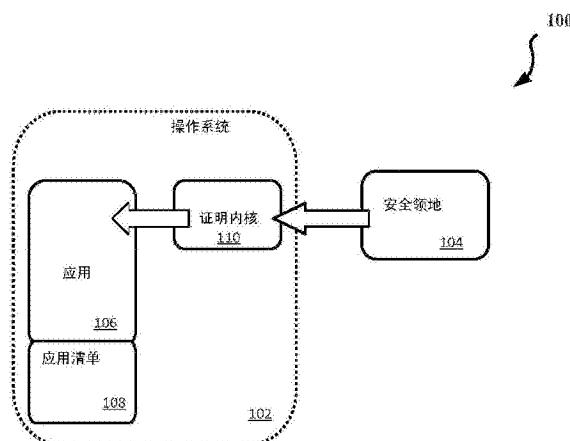
权利要求书3页 说明书6页 附图7页

(54)发明名称

使用动态量度内核的安全应用证明

(57)摘要

描述了使用动态量度内核提供安全应用证明的方法和装置。在一些实施例中，安全应用证明是通过使用动态量度内核来提供的。在不同实施例中，使用P-MAPS(处理器测量的应用保护服务)、安全领地(SE)和/或其组合来提供动态量度内核以支持安全应用证明。还描述了其他实施例。



1. 一种通过动态量度内核提供安全应用证明的方法,所述方法包括:

在应用处从第三方接收证明请求;

响应于所述证明请求将证明内核加载到存储单元中,其中允许存储在所述存储单元中的代码访问所述存储单元外的储存器,而阻止存储在所述存储单元外的代码访问所述存储单元中的任何储存器位置;

对应于所述证明请求并根据存储在所述存储单元中的数据,在硬件逻辑处执行一个或多个操作,以产生清单,其中所述硬件逻辑响应于来自虚拟机管理器的传输执行所述一个或多个操作,其中所述传输由所述虚拟机管理器逻辑响应于所述证明请求而产生;

产生存储在存储单元中的数据的证明;

基于所产生的存储在所述存储单元中的数据的证明和所述清单验证所述应用的状态;

基于所述清单的散列产生应用量度的声明;以及

将所述应用量度、所述清单和所述证明数据发送至所述应用和所述第三方两者。

2. 如权利要求1所述的方法,其特征在于,所述存储单元是证明领地或证明容器中的一个。

3. 如权利要求1所述的方法,其特征在于,验证所述应用的状态包括扫描与应用关联的存储器。

4. 如权利要求1所述的方法,其特征在于,还包括所述虚拟机管理器检查存储在所述存储单元内的数据的证明并发布存储在所述存储单元内的数据的量度,其中所述发送包括发送存储在所述存储单元内的数据的量度。

5. 如权利要求1所述的方法,其特征在于,还包括所述虚拟机管理器检查被存储在所述存储单元内的数据的证明并发布存储在所述存储单元内的数据的量度,其中所述发送包括发送存储在所述存储单元内的数据的量度以及由受信硬件实体产生的引用。

6. 如权利要求1所述的方法,其特征在于,验证所述应用的状态包括扫描与所述应用关联的存储器。

7. 如权利要求1所述的方法,其特征在于,执行所述一个或多个操作是基于所述证明内核执行的。

8. 如权利要求1所述的方法,其特征在于,所述清单包括随机质询随机数。

9. 如权利要求1所述的方法,其特征在于,所述清单由受信实体签名。

10. 如权利要求1所述的方法,其特征在于,还包括对存储在所述存储单元中的数据的证明加密地签名。

11. 一种通过动态量度内核提供安全应用证明的设备,所述设备包括:

用于在应用处从第三方接收证明请求的装置;

用于响应于所述证明请求将证明内核加载到存储单元中的装置,其中允许存储在所述存储单元中的代码访问所述存储单元外的储存器,而阻止存储在所述存储单元外的代码访问所述存储单元中的任何储存器位置;

用于对应于所述证明请求并根据存储在所述存储单元中的数据在硬件逻辑处执行一个或多个操作以产生清单的装置,其中所述硬件逻辑响应于来自虚拟机管理器的传输执行所述一个或多个操作,其中所述传输由所述虚拟机管理器逻辑响应于所述证明请求而产生;

用于产生存储在存储单元中的数据的证明的装置；

用于基于所产生的存储在所述存储单元中的数据的证明和所述清单验证所述应用的状态的装置；

用于基于所述清单的散列产生应用量度的声明的装置；以及

用于将所述应用量度、所述清单和所述证明数据发送至所述应用和所述第三方两者的装置。

12. 如权利要求11所述的设备，其特征在于，所述存储单元是证明领地或证明容器中的一个。

13. 如权利要求11所述的设备，其特征在于，用于验证所述应用的状态的装置包括用于扫描与应用关联的存储器的装置。

14. 如权利要求11所述的设备，其特征在于，还包括用于由所述虚拟机管理器检查存储在所述存储单元内的数据的证明并发布存储在所述存储单元内的数据的量度的装置，其中所述发送包括发送存储在所述存储单元内的数据的量度。

15. 如权利要求11所述的设备，其特征在于，还包括用于由所述虚拟机管理器检查被存储在所述存储单元内的数据的证明并发布存储在所述存储单元内的数据的量度的装置，其中所述发送包括发送存储在所述存储单元内的数据的量度以及由受信硬件实体产生的引用。

16. 如权利要求11所述的设备，其特征在于，用于验证所述应用的状态的装置包括用于扫描与所述应用关联的存储器的装置。

17. 如权利要求11所述的设备，其特征在于，执行所述一个或多个操作是基于所述证明内核执行的。

18. 如权利要求11所述的设备，其特征在于，所述清单包括随机质询随机数。

19. 如权利要求11所述的设备，其特征在于，所述清单由受信实体签名。

20. 如权利要求11所述的设备，其特征在于，还包括用于对存储在所述存储单元中的数据的证明加密地签名的装置。

21. 一种通过动态量度内核提供安全应用证明的系统，所述系统包括：

存储器，用以存储与容器对应的一个或多个指令；以及

处理器，具有硬件逻辑并且用以执行所述一个或多个指令以：

在应用处从第三方接收证明请求；

响应于所述证明请求将证明内核加载到存储单元中，其中允许存储在所述存储单元中的代码访问所述存储单元外的存储器，而阻止存储在所述存储单元外的代码访问所述存储单元中的任何存储器位置；

对应于所述证明请求并根据存储在所述存储单元中的数据执行一个或多个操作，以产生清单，其中所述处理器响应于来自虚拟机管理器的传输执行所述一个或多个操作，其中所述传输由所述虚拟机管理器逻辑响应于所述证明请求而产生；

产生存储在所述存储单元中的数据的证明；

基于所产生的存储在所述存储单元中的数据的证明和所述清单验证所述应用的状态；

基于所述清单的散列产生应用量度的声明；以及

将所述应用量度、所述清单和所述证明数据发送至所述应用和所述第三方两者。

22. 如权利要求21所述的系统,其特征在于,所述存储单元是证明领地或证明容器中的一个。

23. 如权利要求21所述的系统,其特征在于,还包括虚拟机管理器,用以检查存储在所述存储单元中的数据的证明并发布存储在所述存储单元中的数据的量度。

24. 如权利要求21所述的系统,其特征在于,还包括对所述清单签名的受信实体。

25. 如权利要求24所述的系统,其特征在于,所述受信实体是受信平台模块。

26. 如权利要求21所述的系统,其特征在于,还包括对存储在所述存储单元中的数据的证明加密地签名的逻辑。

27. 如权利要求21所述的系统,其特征在于,所述清单包括随机质询随机数。

28. 如权利要求23所述的系统,其特征在于,还包括发送存储在所述存储单元中的数据的量度和由受信硬件实体产生的引用的逻辑。

使用动态量度内核的安全应用证明

技术领域

[0001] 本公开总体涉及计算领域。更具体地，本发明的实施例总体涉及使用动态量度内核的安全应用证明。

背景技术

[0002] 随着计算机连接性变得越来越普遍，保护计算设备不受恶意实体、恶意软件等侵害成为更具挑战的任务。一种提高安全性的方式是管理操作系统的特权内核。结果，确保关键应用的状态和能够对第三方证明其完整性可以整体上提高操作系统的安全性。

[0003] 此外，可使用防毒软件来对抗公知类型的攻击。然而，这种软件通常无法解决未知的威胁或破坏操作系统和防毒软件所依赖的服务的软件。

附图说明

[0004] 参照附图提供详细描述。在附图中，附图标记最左边的数字标识标记首次出现的附图。在不同附图中使用相同附图标记来指示相似或相同的项目。

[0005] 图1和图3示出根据本发明一些实施例的系统的实施例。

[0006] 图2、图4A和4B示出根据本发明一些实施例的方法的流程图。

[0007] 图5和图6示出可用来实现本文讨论的一些实施例的计算系统的实施例的框图。

具体实施方式

[0008] 在以下描述中，阐述众多具体细节以提供对各实施例的透彻理解。然而，本发明的各个实施例在没有这些具体细节的情况下也可实践。在其他情形中，众所周知的方法、过程、组件和电路并未进行详细描述以免混淆本发明的特定实施例。此外，本发明实施例的各方面可使用各种手段来执行，诸如集成半导体电路（“硬件”）、组织成一个或多个程序的计算机可读指令（“软件”）或硬件与软件的某种组合。出于本公开的目的，对“逻辑”的引述应表示硬件、软件（包括例如控制处理器的操作的微代码）或其某种组合。

[0009] 一般来说，应付敏感数据的应用需要保护数据不受恶意实体侵害的能力以及向第三方证明该应用保持未经修改和/或正确工作的机制。在一些实现中，安全应用证明是通过使用动态量度内核来提供的。在各实施例中，P-MAPS（处理器测量的应用保护服务）、安全领地（SE）和/或其组合提供动态量度内核以支持安全应用证明。在一个或多个实施例中，P-MAPS提供基于虚拟化的容器，而SE提供基于出现在硬件中的支持特征的解决方案。由此，需要与第三方（例如防毒软件、上下文保护系统等）建立信任的应用可利用本文讨论的一个或多个实施例。

[0010] 更具体地，图1示出根据实施例用以提供安全应用证明的系统100的框图。系统100示出利用SE的系统（它可从Intel®公司获得）。然而，本文讨论的实施例不仅限于SE，并可使用其它具有相同或相似组件的技术。如图1所示，系统100包括操作系统（OS）102和安全领地（SE）104。OS102包括应用106（具有应用清单108）和证明内核110。

[0011] 参见图2,其示出根据实施例用以提供安全应用证明的方法200的流程图。在实施例中,可使用参照图1讨论的组件中的一个或多个来执行参照方法200讨论的操作中的一个或多个。

[0012] 更具体地,SE允许应用中的一段或多段与进程的其余部分(可能是系统的其余部分)隔离。例如,当代码被加载到领地中时,处理器测量该内容。然后使用该测量来证明领地的状态。另外,可使用该测量在随后时间对领地的内容进行复检,以检测意外的变化。在一些实施例中,允许领地内的代码访问领地外的存储器,但不允许领地外的代码访问领地内的存储器。

[0013] 参见图1-2,使用方法200,允许应用产生其状态的证明以供第三方验证。在操作202,应用106从第三方接收证明请求,例如包括随机质询随机数(challenge nonce)(CN),用于新鲜度保证和重放保护。在操作204,应用106将证明内核110加载到存储单元(诸如领地(例如SE104),又被称为证明领地(AE))中(或导致该加载)。

[0014] 在操作206,应用106执行领地(例如SE104)中与证明相关的操作(或通过证明内核110的执行来导致该操作的执行),例如在一个或多个实施例中传递由应用研发者(或其它受信实体,例如信息科技(IT)部门)签名的清单和/或CN作为参数。

[0015] 在操作208,AE(例如SE104)产生其自身状态的证明——被称为领地量度(EM),它例如通过平台被加密地签名。在操作210,AE验证在操作206传递/产生的清单的真实性。在操作212,使用由内向外的能力(即允许领地内的代码访问领地外的存储器,但不允许领地外的代码访问领地内的存储器),AE使用清单内容来通过扫描与应用关联的存储器验证调用应用的状态。

[0016] 在操作214,AE产生加密地签名的声明——其被称为应用量度(AM)——例如在一个或多个实施例中包括清单散列和/或随机数。在操作216,AE将EM和AM返回给应用106。在操作218,应用将EM、AM和清单发送给第三方以供验证。

[0017] 图3示出根据实施例用以提供安全应用证明的系统300的框图。系统300示出一种利用基于P-MAPS虚拟化的容器技术(它可从Intel®公司获得)的变例的系统。然而,本文讨论的实施例不仅限于P-MAPS,并可使用其它具有相同或相似组件的技术。如图3所示,系统300包括操作系统(OS)102、应用106、应用清单108、证明内核110、安全VMM(虚拟机管理器)逻辑302(包括证明软件306)、受信执行技术(TXT)逻辑(它可从Intel®公司获得)304。然而,本文讨论的实施例不仅限于TXT,并可使用其它具有相同或相似组件的技术。

[0018] 参见图4A,其示出根据实施例用以提供安全应用证明的方法400的流程图。在实施例中,可使用参照图3讨论的组件中的一个或多个来执行参照方法400讨论的操作中的一个或多个。

[0019] 更具体地,在一些实施例中,可基于Intel®虚拟化技术(例如VT-x、VT-d、TXT等)使用相对小的VMM来实现P-MAPS容器。该容器可包裹整个应用,防止软件对存储器的访问,即便访问来自OS内核。P-MAPS VMM则在其为应用构造容器时验证该应用与签名清单匹配。应用可在运行时从VMM请求其自身的证明。在实施例中,P-MAPS VMM被修改以使其表现更接近基于硬件特征的SE技术。SE硬件技术能在应用的多部分周围构造容器;潜在地能在同一应用中构造多个独立的容器。

[0020] 参见图3-4A,使用方法400,允许应用产生其状态的证明以供第三方验证。在操作

402,应用106从第三方接收证明请求,例如包括随机CN,用于新鲜度保证和重放保护。在操作404,应用106将证明内核(AK)110加载到(例如由安全VMM302创建的)受保护的可证明软件容器(AC)中(或导致该加载)。在实施例中,VMM(例如安全VMM302)使用证明软件306在加载时间对照签名清单检查AK的内容。

[0021] 在操作406,应用106执行VMM和AK中与证明相关的操作(或通过证明内核110的执行来导致该操作的执行),例如在一个或多个实施例中传递由应用研发者(或其它受信实体,例如信息科技(IT)部门)签名的清单和/或CN作为参数。

[0022] 在操作408,AK从VMM(例如安全VMM302)请求VMM状态的证明。在实施例中,VMM使用受信硬件实体,例如TPM(受信平台模块)(它也由TXT304使用),来基于VMM302的安全测量启动提供引用。“所引用的”证明包含VMM启动量度(VMMM)的量度(它在一实施例中被受信硬件实体加密地签名)。在一实施例中,由于VMM的测量启动,受信硬件实体经由TXT(例如TPM)提供该量度。在操作410,VMM(例如安全VMM302)复检/检查和/或发布/返回AK的量度——被称为证明内核量度(AKM),例如VMM加密地对其签名以提供VMM的证明。在一个实施例中,VMM302使用证明软件306以产生先前加载到AC中的AK110的引用。

[0023] 在操作412,AK110验证应用清单真实性并使用清单内容以通过扫描其存储器验证调用应用的状态,例如使用由内向外的能力(即允许AC内的代码访问AC外的存储器,但不允许AC外的代码访问AC内的存储器)。

[0024] 在操作414,AK110产生加密地签名的声明——其被称为应用量度(AM)——例如在一个或多个实施例中包括清单散列和/或随机数。在操作416,AC将VMMM、AKM和AM返回给应用106。在操作418,应用将VMMM、AKM、AM和清单发送给第三方以供验证。

[0025] 在一个或多个实施例中,除了使P-MAPS容器机制的操作更接近基于SE的机制的操作外,本文讨论的实施例可提供额外的优势,包括加载来自不同作者的多个隔离容器的能力以及不位于容器内的代码的性能提升。另外,在一些实施例中使用受硬件保护的代码来测量和证明同一进程中不受保护的代码。

[0026] 图4B示出根据实施例用以提供安全应用证明的方法的流程图。在一个实施例中,可使用参照图3讨论的组件中的一个或多个来执行参照图4B讨论的操作中的一个或多个。

[0027] 如图4B所示,第三方发送证明请求(包括CN),例如通过图4A的操作402讨论的。应用(例如图3的应用106)然后将证明请求(包括例如参照图4A讨论的CN和清单)发送至证明内核(例如图3的证明内核110)。然后将请求转发至VMM(例如图3的VMM302)。VMM进而利用受信硬件实体(例如TPM)来创建引用。受信硬件实体将该引用格式化和签名作为VMMM。所产生的引用(包括VMMM)被转发至VMM。VMM将证明内核量度格式化和签名作为AKM,并向证明内核发送响应(包括VMMM和AKM)。证明内核基于来自VMM的响应来验证清单真实性。证明内核也根据清单验证应用。证明内核将该证明和CN格式化和签名作为AM,并向应用发送响应(包括VMMM、AM和AM)。进而,应用通过VMMM、AM和AM对第三方作出响应。

[0028] 图5示出计算系统500的实施例的框图。在多个实施例中,系统500的一个或多个组件可设置在能执行本文中参照本发明一些实施例所讨论的一个或多个操作的各种电子器件中。例如,系统500中的一个或多个组件可用来执行参照图1-4描述的操作,例如通过根据本文讨论的操作处理指令、执行子例程等。另外,可使用本文描述(例如参照图5和/或图6)的多种存储设备来存储数据、操作结果等,包括例如参照图1-4讨论的操作系统102。在一个

实施例中,参照图5-6讨论的一个或多个处理器(或其它硬件组件)包括图1的SE104、图3的安全VMM302和/或图3的TXT304中的一个或多个。

[0029] 更具体地,计算系统500可包括经由互连网络(或总线)504通信的一个或多个中央处理单元(CPU)502或处理器。因此,本文描述的各操作在一些实施例中可通过CPU来执行。此外,处理器502可包括通用处理器、网络处理器(处理在计算机网络503上通信的数据)或其他类型的处理器(包括精简指令集计算机(RISC)处理器或复杂指令集计算机(CISC))。而且,处理器502可具有单核或多核设计。具有多核设计的处理器502可以在同一块集成电路(IC)管芯上集成不同类型的处理器核。另外,具有多核设计的处理器502可实现为对称或非对称的多处理器。此外,参照图1-4讨论的操作可由系统500的一个或多个组件来执行。

[0030] 芯片组506也可与互连网络504通信。芯片组506可包括图形和存储器控制中枢(GMCH)508。GMCH508可包括与存储器512通信的存储器控制器510。存储器512可存储数据,包括由CPU502或计算系统500中包括的任何其他设备执行的指令序列。在一实施例中,存储器512可存储操作系统513,该操作系统513可与图1-4的OS102相同或相似。该数据(包含指令)或其至少一部分可被存储在盘驱动器528中和/或处理器502内的一个或多个高速缓存中。在本发明的一个实施例中,存储器512可包括一个或多个易失性存储(或存储器)设备,诸如随机存取存储器(RAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、静态RAM(SRAM)或其他类型的存储设备。也可利用非易失性存储器,诸如硬盘。诸如多个CPU和/或多个系统存储器之类的附加设备可经由互连网络504通信。

[0031] GMCH508也可包括与显示器516通信的图形接口514。在本发明的一个实施例中,图形接口514可经由加速图形端口(AGP)与显示器516通信。在本发明的一实施例中,显示器516可以是平板显示器,其通过例如信号转换器与图形接口514通信,该信号转换器将例如视频存储器或系统存储器等存储设备中存储的图像的数字表示转换成由显示器516解读和显示的显示信号。在由显示器516解读并之后在显示器516上显示之前,由接口514产生的显示信号可经过各种控制设备。在一些实施例中,处理器502以及一个或多个其它组件(例如存储器控制器510、图形接口514、GMCH508、ICH520、外设桥524、芯片组506等)可被设置在同一IC管芯上。

[0032] 中枢接口518可允许GMCH508与输入/输出控制中枢(ICH)520通信。ICH520可向与计算系统500通信的I/O设备提供接口。ICH520可通过诸如外设组件互连(PCI)桥、通用串行总线(USB)控制器或其他类型的外设桥或控制器等外设桥(或控制器)524与总线522通信。桥524可在CPU502与外设设备之间提供数据路径。可以利用其他类型的拓扑结构。另外,多条总线例如可通过多个桥或控制器与ICH520通信。而且,在本发明的各个实施例中,与ICH520通信的其他外设可包括集成驱动电子器件(IDE)或小型计算机系统接口(SCSI)硬驱动、USB端口、键盘、鼠标、并行端口、串行端口、软盘驱动、数字输出支持(例如,数字视频接口(DVI))或其他设备。

[0033] 总线522可与音频设备526、一个或多个盘驱动528以及网络接口设备530通信,该网络接口设备530可与计算机网络503通信。在一实施例中,设备530可以是能够进行无线通信的NIC。其他设备可经由总线522通信。另外,在本发明的一些实施例中,各种组件(诸如网络接口设备530)可与GMCH508通信。此外,可以组合处理器502、GMCH508和/或图形接口514以形成单块芯片。

[0034] 此外,计算系统500可包括易失性和/或非易失性存储器(或存储)。例如,非易失性存储器可包括以下的一个或多个:只读存储器(ROM)、可编程ROM(PROM)、可擦除PROM(EPROM)、电EPROM(EEPROM)、盘驱动器(例如,528)、软盘、压缩盘ROM(CD-ROM)、数字多用盘(DVD)、闪存、磁光盘、或能够存储电子数据(例如,包括指令)的其他类型的非易失性机器可读介质。在一实施例中,系统500的组件可被配置成例如参照图6讨论的点对点(PtP)配置。例如,处理器、存储器和/或输入/输出设备可通过多个点对点接口互连。

[0035] 更具体地,图6示出根据本发明一实施例配置成点对点(PtP)配置的计算系统600。具体而言,图6示出其中处理器、存储器以及输入/输出设备通过多个点对点接口互连的系统。参照图1-5讨论的操作可由系统600的一个或多个组件来执行。

[0036] 如图6中所示,系统600可包括若干个处理器,为清楚起见仅示出其中的两个,即处理器602和604。处理器602、604可各自包括本地存储器控制器中枢(MCH)606、608(它们在一些实施例中可以与图5的GMCH508相同或相似)以与存储器610、612耦合。存储器610和/或612可存储各种数据,例如参照图5的存储器512所讨论的那些数据。

[0037] 处理器602和604可以是任何合适的处理器,例如参照图6的处理器602所讨论的那些。处理器602和604可分别使用点对点(PtP)接口电路616、618经由PtP接口614交换数据。处理器602和604各自可使用点对点接口电路626、628、630和632经由各个PtP接口622和624与芯片组620交换数据。芯片组620还可使用PtP接口电路637经由高性能图形接口636与高性能图形电路634交换数据。

[0038] 本发明的至少一个实施例可通过利用处理器602和604来提供。例如,处理器602和/或604可执行图1-5的操作中的一个或多个。然而,本发明的其他实施例可存在于图6的系统600内的其他电路、逻辑单元或设备中。此外,本发明的其他实施例可分布在图6中所示的若干个电路、逻辑单元或设备中。

[0039] 芯片组620可使用PtP接口电路641耦合到总线640。总线640可具有与之耦合的一个或多个设备,例如总线桥642和I/O设备643。总线桥643可经由总线644耦合至其他设备,例如键盘/鼠标645、参照图6讨论的网络接口设备630(例如调制解调器、网络接口卡(NIC)或可耦合至计算机网络503的类似设备)、音频I/O设备和/或数据存储设备648。数据存储设备648可存储可由处理器602和/或604执行的代码649。

[0040] 在本发明的各个实施例中,本文中例如参照图1-6所讨论的操作可实现为硬件(例如,逻辑电路)、软件(包括例如控制诸如本文所述的处理器之类的处理器的操作的微代码)、固件或其组合,它们可作为计算机程序产品来提供,例如包括其上存储有用于对计算机(例如,计算设备的处理器或其他逻辑)编程以执行本文所讨论的操作的指令(或软件程序)的有形(例如非瞬态)机器可读或计算机可读介质。机器可读介质可包括诸如本文所讨论的那些存储设备。

[0041] 说明书中对“一个实施例”或“实施例”的引述意味着结合该实施例描述的具体特征、结构或特性可被包含于至少一种实现中。本说明书中各处出现的短语“在一个实施例中”可以或可以并非全部指代同一实施例。

[0042] 另外,在本描述和权利要求中,可使用术语“耦合”和“连接”连同其派生词。在本发明的一些实施例中,可使用术语“连接”来指示两个或多个元件彼此直接物理或电气接触。“耦合的”可表示两个或更多个元件直接物理或电接触。然而,“耦合”也可意味着两个或多

个元件可能彼此并未直接接触,但是仍然彼此协作或交互。

[0043] 另外,这样的计算机可读介质可以作为计算机程序产品下载,其中可借助数据信号经由通信链路(例如,总线、调制解调器或网络连接)例如通过载波或其它传播介质将该程序从远程计算机(例如服务器)传输到请求的计算机(例如客户机)。

[0044] 由此,尽管已经用结构特征和/或方法动作专用的语言描述了本发明的实施例,但是应该理解所要求保护的主题可并不被限定于所描述的具体特征或动作。相反,这些具体特征和动作是作为实现所要求保护的主题的样本形式而公开的。

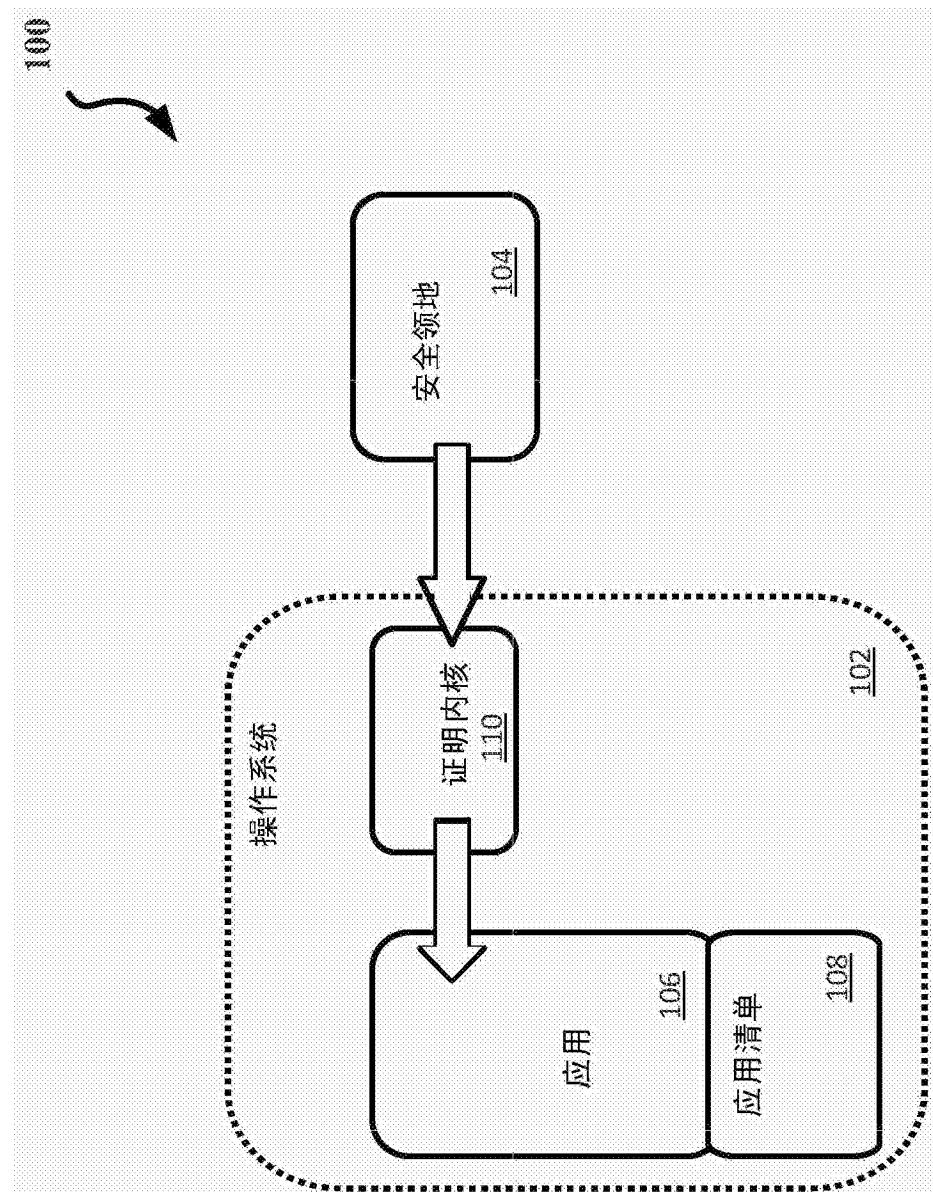


图1

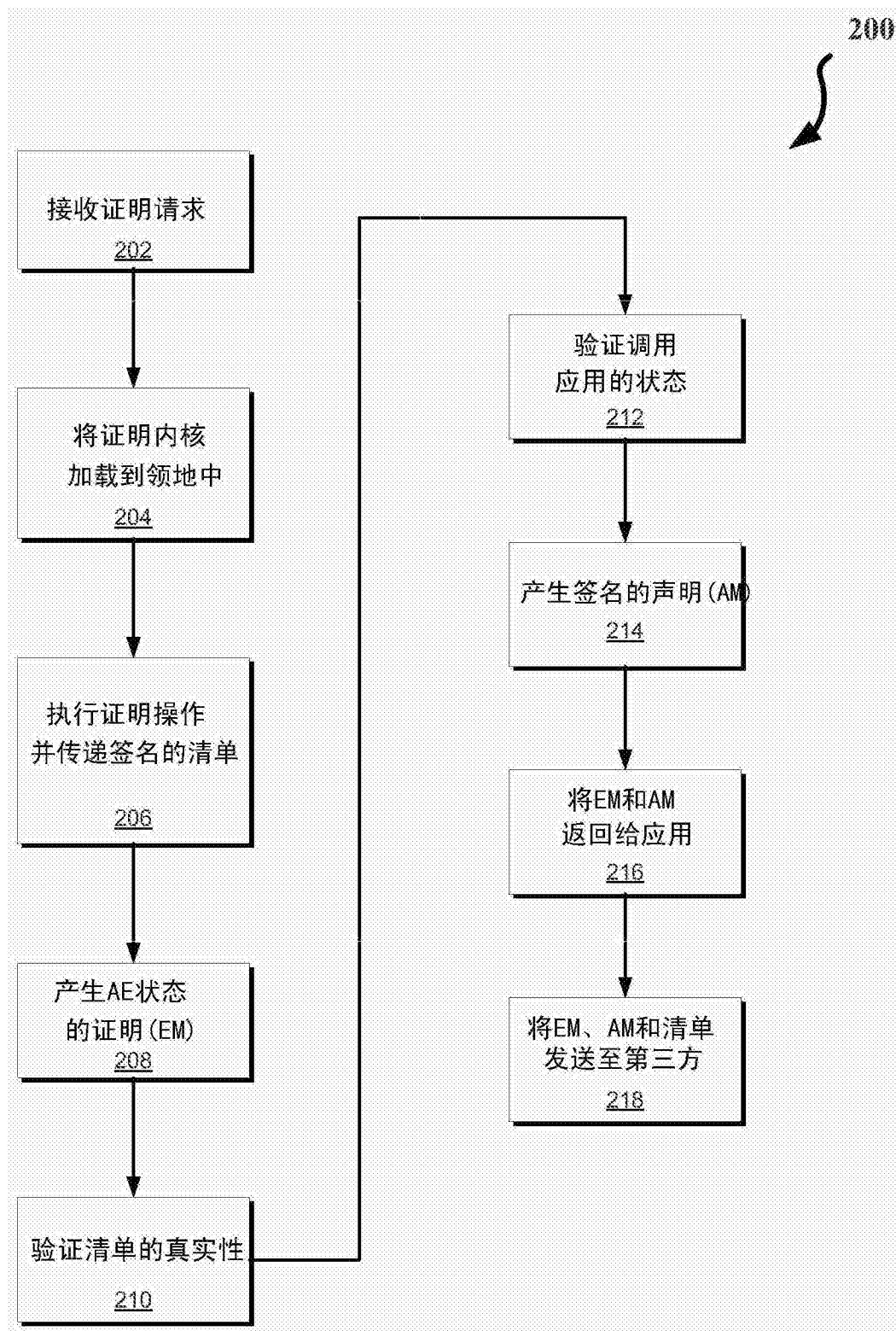


图2

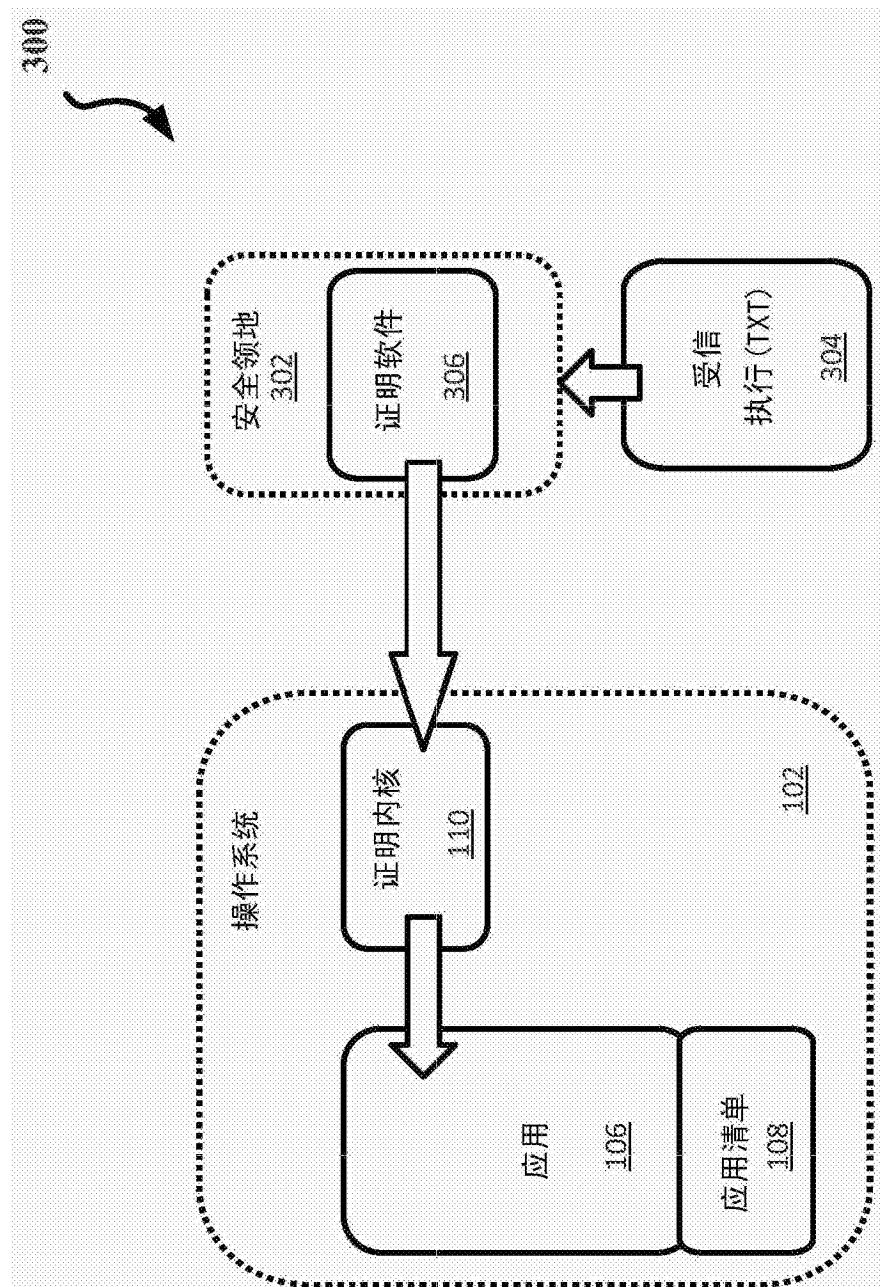


图3

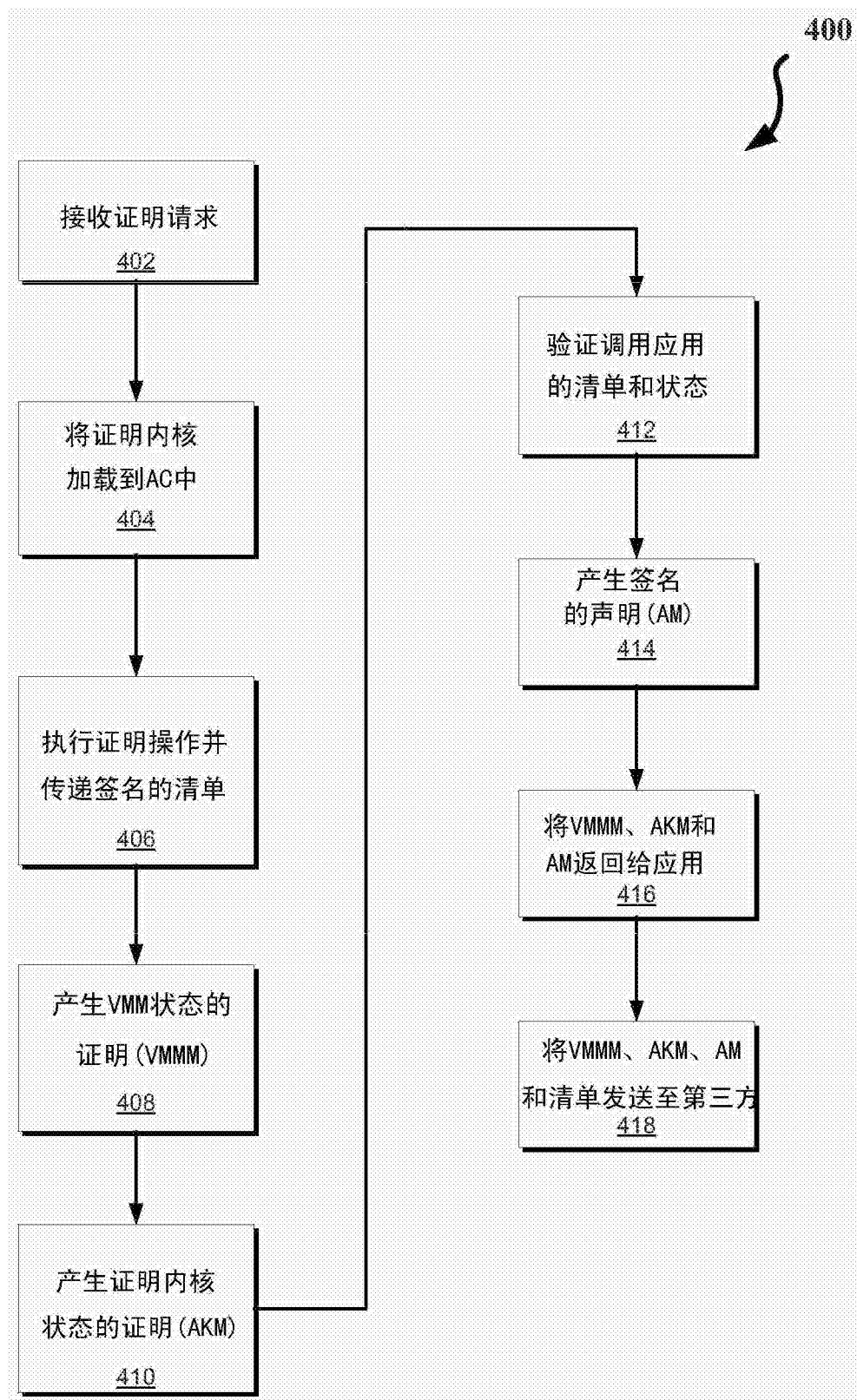


图4A

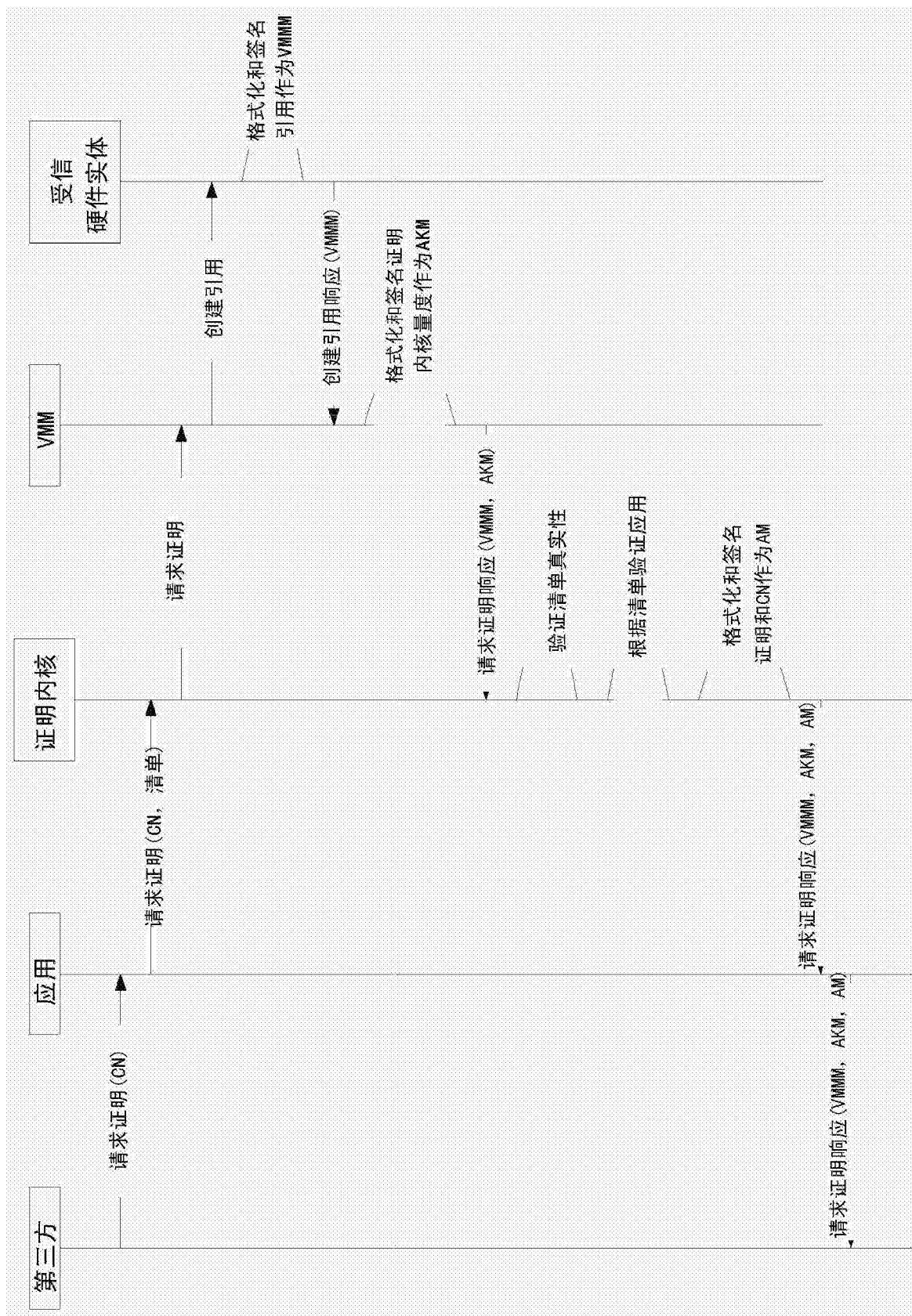


图4B

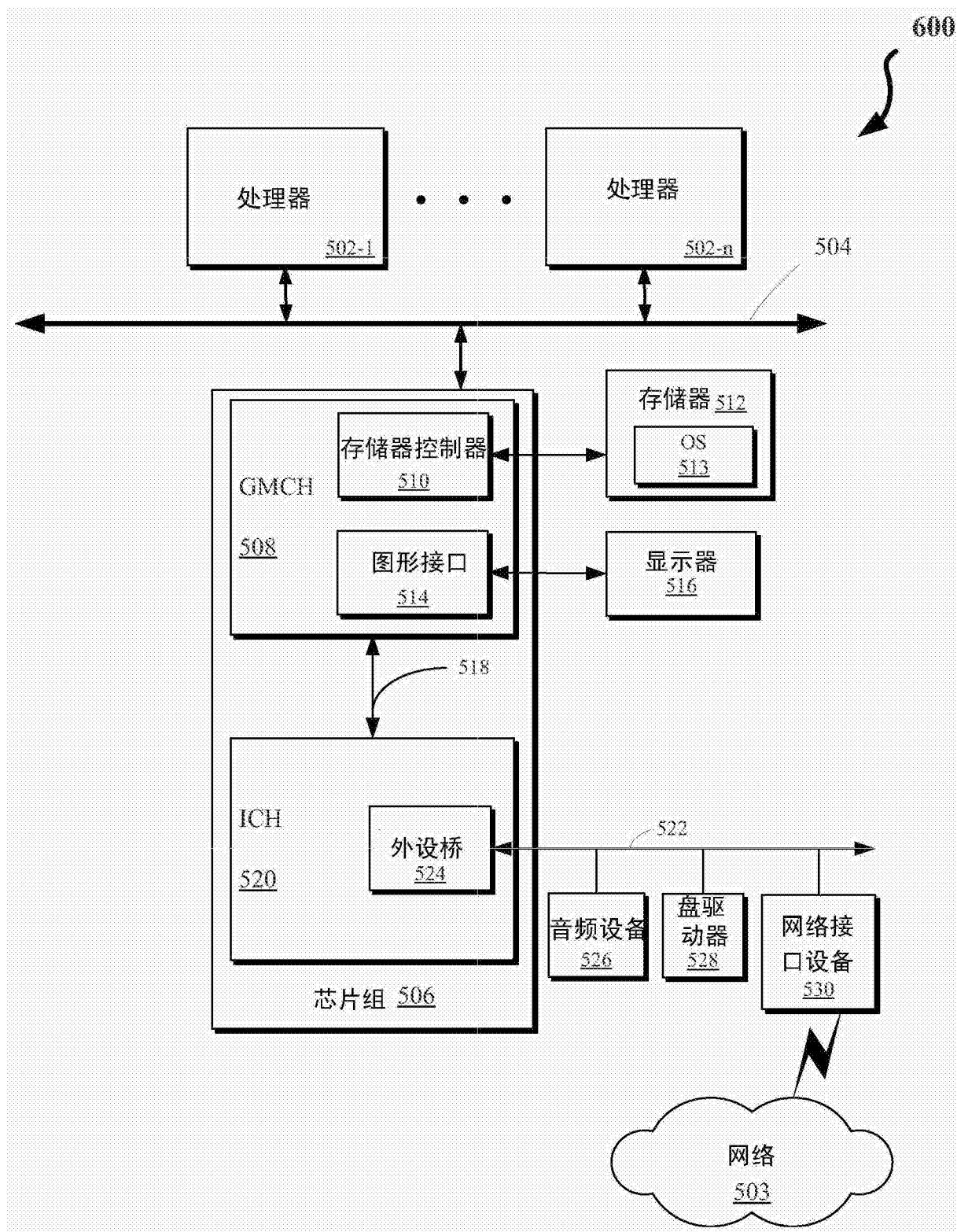


图5

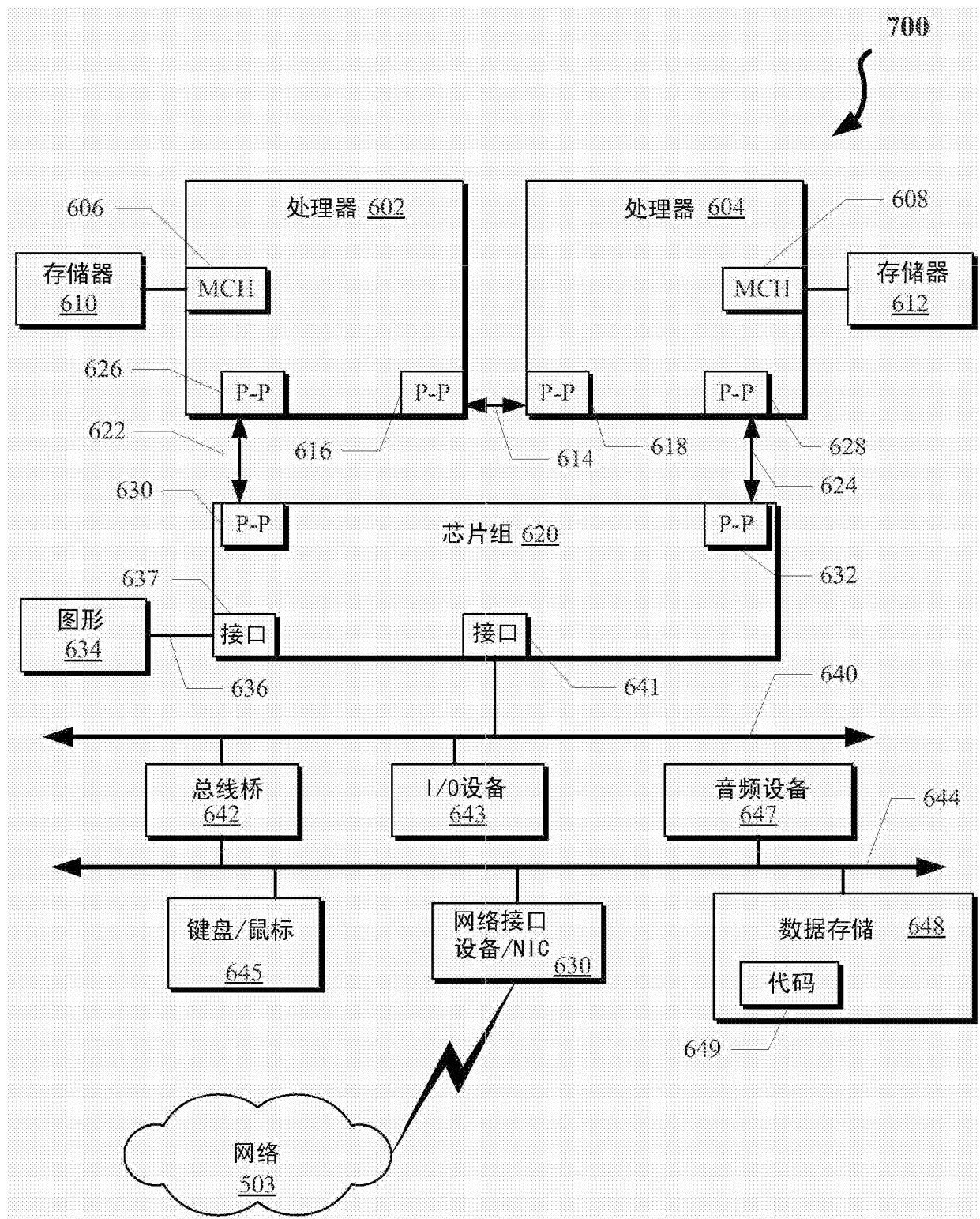


图6