



(12) 发明专利

(10) 授权公告号 CN 101438254 B

(45) 授权公告日 2012.12.12

(21) 申请号 200780015888.4

(56) 对比文件

(22) 申请日 2007.05.02

CN 1469258 A, 2004.01.21, 说明书第4页第10行到第6页第24行.

(30) 优先权数据

11/429,025 2006.05.04 US

CN 1762025 A, 2006.04.19,

CN 1564981 A, 2005.01.12,

(85) PCT申请进入国家阶段日

审查员 赵晓春

2008.11.03

(86) PCT申请的申请数据

PCT/US2007/068005 2007.05.02

(87) PCT申请的公布数据

W02007/131024 EN 2007.11.15

(73) 专利权人 英特尔公司

地址 美国加利福尼亚州

(72) 发明人 J·鲁德利克

(74) 专利代理机构 中国专利代理(香港)有限公司

72001

代理人 柯广华 陈景峻

(51) Int. Cl.

G06F 12/02(2006.01)

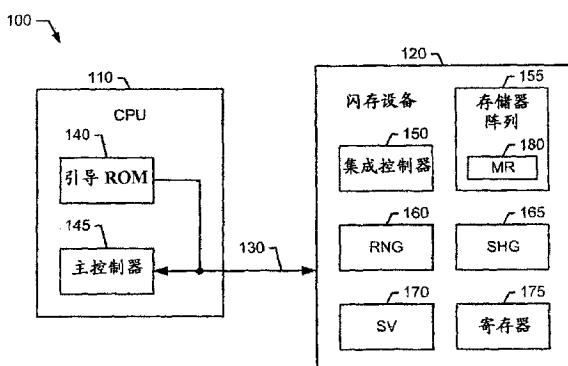
G11C 16/02(2006.01)

权利要求书 2 页 说明书 7 页 附图 5 页

(54) 发明名称

用于提供闪存设备关联的读访问控制系统的
方法和装置

(57) 摘要

本文主要描述用于提供闪存设备关联的读访问
控制系统的方法和装置的实施例。其它实施例
可被描述且要求其权益。

1. 一种用于提供与闪存设备关联的读访问控制系统的装置，包括：

由闪存设备接收读访问命令，所述读访问命令配置为禁止在读取所述闪存设备的存储器阵列的存储器范围内的数据之后对所述存储器范围的读访问；

在所述闪存设备的集成控制器处由所述闪存设备基于签名验证协议来验证所述读访问命令，其中所述集成控制器可操作地耦合到处理器单元，所述处理器单元提供访问所述闪存设备的存储器范围的所述读访问命令；

由所述闪存设备基于经验证的读访问命令提供对所述存储器阵列的存储器范围的读访问，其中基于所述签名验证协议确定所述经验证的读访问命令是有效的动态读访问命令；

禁止在执行所述经验证的读访问命令之后对所述存储器范围的读访问，以及

在重置所述闪存设备之前由所述闪存设备基于接收到另一个有效的动态读访问命令来启动对所述存储器阵列的之前禁止的存储器范围的另外读访问，其中基于所述签名验证协议预先确定所述另一个有效的动态读访问命令是有效的动态读访问命令。

2. 如权利要求 1 中所述的方法，还包括：由所述闪存设备响应于检测到指示所述闪存设备重置的条件来启动所述存储器范围的读访问。

3. 如权利要求 1 中所述的方法，还包括：由所述闪存设备接收第三读访问命令，所述第三读访问命令配置为禁止在读取所述存储器范围内的数据之后对所述存储器范围的读访问；

由所述闪存设备基于验证密钥验证所述第三读访问命令，其中确定所述第三读访问命令是有效的验证密钥；以及

阻止对所述存储器范围的读访问。

4. 如权利要求 3 中所述的方法，包括响应于所述阻止来向所述处理器单元提供预定值。

5. 如权利要求 1 中所述的方法，其中在提供对所述存储器阵列的存储器范围的读访问之后，通过设置所述集成控制器的易失性位来禁止所述存储器范围，其中所述易失性位与动态读访问模式关联。

6. 如权利要求 1 中所述的方法，还包括：在与所述闪存设备关联的寄存器中存储预定值，其中所述预定值与所述存储器范围关联。

7. 一种用于提供与闪存设备关联的读访问控制系统的装置，包括：

具有存储器范围的存储器阵列；以及

可操作地耦合到所述存储器阵列的控制器，用于：接收读访问命令，所述读访问命令配置为禁止在读取所述存储器范围内的数据之后对所述存储器范围的读访问；基于签名验证协议验证来自处理器单元的访问所述存储器范围的所述读访问命令；基于经验证的读访问命令提供对所述存储器阵列的存储器范围的读访问，其中基于所述签名验证协议确定所述经验证的读访问命令是有效的动态读访问命令；禁止在执行所述经验证的读访问命令之后对所述存储器范围的读访问；在重置所述设备之前基于接收到另一个有效的动态读访问命令来启动对禁止的存储器范围的另外读访问，其中基于所述签名验证协议确定所述另一个有效的动态读访问命令是有效的，并且其中所述控制器通过闪存接口可操作地耦合到所述处理器单元。

8. 如权利要求 7 中所述的装置,其中所述控制器配置为响应于检测到指示所述闪存设备重置的条件来启动所述处理器单元对所述存储器范围的读访问。

9. 如权利要求 7 中所述的装置,其中所述控制器配置为响应于接收到第三读访问命令来阻止所述处理器单元对所述存储器范围的读访问。

10. 如权利要求 7 中所述的装置,其中所述控制器配置为通过设置所述控制器的非易失性 (NV) 位来禁止所述存储器范围,其中所述非易失性位与静态读访问模式关联。

11. 如权利要求 7 中所述的装置,还包括寄存器,所述寄存器响应于检测到指示所述存储器范围被禁止读访问的条件来存储提供给所述处理器单元的预定值。

12. 一种处理系统,包括:

处理器单元;以及

闪存设备,所述闪存设备通过闪存接口可操作地耦合到所述处理器单元,所述闪存设备具有存储器阵列和集成控制器,所述集成控制器用于:接收读访问命令,所述读访问命令配置为禁止在读取所述存储器阵列的存储器范围内的数据之后对所述存储器范围的读访问;基于签名验证协议验证来自处理器单元的访问所述存储器阵列的存储器范围的所述读访问命令;基于经验证的读访问命令提供对所述存储器阵列的存储器范围的读访问,其中基于所述签名验证协议确定所述经验证的读访问命令是有效的读访问命令;禁止在执行所述经验证的读访问命令之后对所述存储器范围的读访问;在重置所述闪存设备之前基于接收到另一个有效的动态读访问命令来启动对之前禁止的存储器范围的另外读访问,其中基于所述签名验证协议确定所述另一个有效的动态读访问命令是有效的动态读访问命令。

13. 如权利要求 12 中所述的系统,其中所述集成控制器配置为响应于检测到指示所述闪存设备的重置的条件来启动所述处理器单元对所述存储器范围的读访问。

14. 如权利要求 12 中所述的系统,其中所述集成控制器配置为根据所述所述集成控制器的非易失性 (NV) 位禁止所述存储器范围,其中所述非易失性位与静态读访问模式关联。

15. 如权利要求 12 中所述的系统,其中所述集成控制器配置为响应于检测到指示禁止所述存储器范围的读访问的条件来将存储在所述存储器阵列的寄存器中的预定值提供给所述处理器单元。

用于提供闪存设备关联的读访问控制系统的方法和装置

技术领域

[0001] 本公开一般涉及闪速存储器系统,更具体地说,涉及用于提供与闪存设备关联的读访问控制系统的方法和装置。

背景技术

[0002] 随着越来越多人携带和 / 或使用电子设备在各种位置 (如办公室、学校、机场、咖啡店等) 工作、教育和 / 或娱乐,技术开发被进行以便在降低成本和 / 或能源消耗的同时提供更强的移动性和 / 或访问。更具体地说,闪速存储器是非易失性存储器,它除了可电编程和擦除电子信息外,还可无需能源保持信息。无需移动部件诸如硬盘、闪速存储器,也可适于便携式或移动电子设备,诸如存储卡、通用串行总线 (USB) 闪存设备、数字音频播放器 (如 MPEG 音频层 3 (MP3) 播放器)、数字相机、手持计算机、手持游戏设备、移动电话和 / 或医疗设备。

附图说明

[0003] 图 1 是根据本文公开的方法和装置的实施例基于闪速存储器的示例处理系统的示意图。

[0004] 图 2 描述存储器阵列配置的一个示例。

[0005] 图 3 描述存储器阵列配置的另一示例。

[0006] 图 4 描述存储器阵列配置的又一示例。

[0007] 图 5 是用以提供读访问控制系统的一种方式的示意流程图。

[0008] 图 6 是用以提供读访问控制系统的另一方式的示意流程图。

[0009] 图 7 是可用于实现图 1 中的示例闪速存储器系统的示例处理器系统的示意框图。

具体实施方式

[0010] 一般来说,用于提供读访问控制系统的方法和装置与闪存设备关联。本文描述的方法和装置并不限于此点。

[0011] 参考图 1,基于闪速存储器的示例处理系统 100 可包括中央处理单元 (CPU) 110 和闪存设备 120。一般来说,基于闪速存储器的处理系统 100 可在电子设备 (未示出) 中实现。例如,基于闪速存储器的处理系统 100 可在桌面计算机、网络服务器、膝上计算机、手持计算机、平板计算机、移动电话 (如智能电话)、寻呼机、音频和 / 或视频播放器 (如 MP3 播放器或 DVD 播放器)、游戏设备、数字相机、导航设备 (如全球定位系统 (GPS) 设备)、医疗设备 (如心率监视器、血压监视器等)、存储卡、USB 闪存设备,和 / 或其它合适的相对静止的、移动的和 / 或便携式电子设备中实现。

[0012] CPU110 可通过闪存接口 130 可操作地耦合到闪存设备 120。例如,闪存接口 130 可包括 CPU110 和闪存设备 120 之间的总线和 / 或直接链路。CPU110 可包括引导只读存储器 (ROM) 140 和主控制器 145。在一个示例中,引导 ROM140 可将引导代码提供给闪存设备 120

用于初始化。备选地，闪存设备 120 可从它自身直接引导。主控制器 145(如应用处理器)可执行 CPU110 的各种操作。例如，主控制器 145 可处理范围包括运行操作系统(OS)、如上所述调用引导 ROM140 的应用和 / 或其它合适的应用的操作。

[0013] 闪存设备 120 可包括集成控制器 150、存储器阵列 155、随机数字发生器(RNG)160、安全散列发生器(secure hash generator)(SHG)165、签名验证器(SV)170 和寄存器 175。一般来说，闪存设备 120 可内部验证操作以保护它自己免于恶意的和 / 或不当的修改。在执行请求的操作(诸如读、写、补丁、检索和 / 或其它合适的操作)之前，闪存设备 120 可内部验证所请求的操作。如果所请求的操作是可信的，则闪存设备 120 可执行操作。否则如果所请求的操作是不可信的，则闪存设备 120 可忽视该请求。

[0014] 在一个示例中，集成控制器 150 可控制如下详细描述的存储器阵列 155 的读访问。更具体地说，存储器阵列 155 可包括一个或多个浮棚晶体管(floating gate transistor)或单元(未示出)以便存储数据、代码和 / 或其它合适的信息。为了检索存储在存储器阵列 155 中的数据、代码或信息，CPU110 可发送读访问命令给集成控制器 150，从而请求存储器阵列 155 的一个或多个存储器范围(memory range)(如存储器范围 180)的读访问。尽管图 1 只描述了一个存储器范围，但是存储器阵列 155 可包括另外的存储器范围。

[0015] 闪存设备 120 可根据签名验证确定读访问命令是否可信。简单来说，CPU110 可从闪存设备 120 请求临时值(nonce value)。随机数字发生器 160 可产生临时值并将其存储在寄存器 175 中。相应地，集成控制器 150 可提供临时值给 CPU110。

[0016] CPU110(如通过主控制器 145)可计算第一散列值。第一散列值可关联于从 CPU110 到闪存设备 120 的消息。例如，消息可包括到闪存设备 120 的命令、相应的数据和 / 或从闪存设备 120 请求的临时值。CPU110 可通过私有密钥(如验证签名)签署第一散列值。在一个示例中，CPU110 可根据非对称验证算法(如由 Rivest、Shamir 和 Adleman(RSA)开发的公共密钥加密)进行操作。备选地，CPU110 可根据由国家标准技术研究所(NIST)开发的加密标准(诸如高级加密标准(AES)(2001 年 11 月 26 日发布)、数据加密标准(DES)(1977 年 1 月 15 日发布)、这些标准的变型和 / 或演变，和 / 或其它合适的加密标准、算法或技术进行操作。CPU110 可将消息和验证签名(如 RSA 签名)转发给闪存设备 120。

[0017] 根据与来自 CPU110 的消息关联的命令和对应数据以及存储在寄存器 175 中的临时值，安全散列发生器 165 可产生第二散列值。签名验证器 170 可验证与来自 CPU110 的消息关联的验证签名。相应地，集成控制器 150 可比较第一散列值与第二散列值。如果第一散列值匹配第二散列值，则来自 CPU110 的消息可被验证。否则，来自 CPU110 的消息不可被验证。

[0018] 此外，如下详细地描述，寄存器 175 可存储对应于存储器范围 180 的一个或多个预定值。更具体地说，如果存储器范围 180 被禁止读访问，则集成控制器 150 可提供预定值给 CPU110。

[0019] 尽管图 1 中给出的组件被描述为闪存设备 120 中分开的模块(block)，但是这些模块中的一些执行的功能可被集成在单个半导体电路内或者可利用两个或多个分开的集成电路实现。例如，尽管随机数字发生器 160 和安全散列发生器 165 被描述为闪存设备 120 中分开的块，但是随机数字发生器 160 和安全散列发生器 165 可被集成到单个组件中。本文描述的方法和装置并不限于此点。

[0020] 然而为了进一步保护敏感信息,集成控制器 150 可直接控制存储器阵列 155 的分区的读访问。一般来说,存储器范围 180 可根据读访问模式(诸如下面进一步详细描述的静态读访问模式或动态读访问模式)进行操作。在静态读访问模式中,例如,集成控制器 150 可在准许 CPU110 访问存储器范围 180 之后禁止存储器范围 180 的读访问。闪存设备 120 重置之后,存储器范围 180 可再次被启动读访问。备选地,闪存设备 120 重置之后存储器范围 180 可被禁止读访问。

[0021] 在动态读访问模式中,集成控制器 150 可开启或关闭(toggle on or off)存储器范围 180 的读访问。与在静态读访问模式中的操作相似地,在动态读访问模式中集成控制器 150 也可在闪存设备 120 重置之后启动存储器范围 180 的读访问。然而集成控制器 150 也可启动存储器范围 180 的读访问以响应于来自 CPU110 的验证的动态读访问命令的接收。通过控制存储器范围 180 的读访问,集成控制器 150 可确定存储在存储器范围 180 中的信息对运行在 CPU110 上的各种应用是否可访问。因此,本文描述的方法和装置可将应用彼此隔离和 / 或将安全应用与非安全应用隔离。

[0022] 如上所述,存储器阵列(如图 1 中的存储器阵列 155)可存储各种信息(如代码、数据等)。转到图 2,例如,存储器阵列配置 200 可包括一个或多个分区,一般示为 210、220、230、240、250、260 和 270。尽管图 2 描述了特定数目的分区,但是存储器阵列配置 200 可包括更多或更少的分区。此外,尽管图 2 描述特定顺序的分区,但是本文描述的方法和装置显然可适用于其它合适的存储器阵列配置。

[0023] 更具体地说,存储器阵列配置 200 可包括用于存储可执行代码的分区,诸如引导分区 210、操作系统(OS)分区 220 以及一个或多个系统库分区 230。存储器阵列配置 200 还可包括用于存储敏感信息(如用户名、密码、账号等)的一个或多个分区,一般示为存储器范围 240(MR₁)、250(MR₂)、260(MR_{n-1}) 和 270(MR_n)。尽管图 2 描述了用于存储敏感信息的四个存储器范围,但是存储器阵列配置 200 可包括更多或更少的存储器范围。

[0024] 为了访问存储器阵列配置 200 的每一个分区,CPU110 可要求验证。在一个示例中,第一存储器范围 240 可存储数据 245 而第二存储器范围 250 可存储数据 255。CPU110 可使用一种验证密钥以便具有第一存储器范围 240 的读访问以及使用另一种验证密钥以便具有第二存储器范围 250 的读访问。相应地,CPU110 可通过适当的验证密钥访问存储在第一存储器范围 240 中的数据 245 以及存储在第二存储器范围 255 中的数据 255。

[0025] 集成控制器 150 可启动第一存储器范围 240 的读访问使得 CPU110 可通过与第一存储器范围 240 关联的验证密钥获得数据 245。在另一示例中,集成控制器 150 可启动第二存储器范围 250 的读,使得 CPU110 可通过与第二存储器范围 250 关联的验证密钥查询数据 255。如下详细地描述,如果集成控制器 150 禁止存储器范围 180 的读访问,则集成控制器 150 会将存储在寄存器 175 中的预定值提供给 CPU110,尽管 CPU110 可具有与存储器范围 180 关联的验证密钥。

[0026] 在图 3 的示例中,存储器阵列配置 300 可包括一个或多个分区,一般示为 310、320、330、340、350、360 和 370。分区 310、320、330、340、350、360 和 370 可分别对应于如上结合图 2 所述的分区 210、220、230、240、250、260 和 270。更具体地说,CPU110 可具有与第一和第二存储器范围 340 和 350 的每个均关联的验证密钥。在启动第一存储器范围 340 的读访问的条件下,集成控制器 150 可将存储在第一存储器范围 340 中的数据(如数据 345)提供

给 CPU110。

[0027] 与图 2 中存储器阵列配置 200 的第二存储器范围 250 相反, 集成控制器 150 禁止第二存储器范围 350 的读访问。因此, 即使 CPU110 具有与第二存储器范围 350 关联的验证密钥, 存储在第二存储器范围 350 中的数据对 CPU110 来说也可能是不可得到的 (如对 CPU110 隐瞒)。相替代地, 集成控制器 150 可将存储在寄存器 175 中的预定值 355 提供给 CPU110。本文描述的方法和装置并不限于此点。

[0028] 转到图 4, 再例如, 存储器阵列配置 400 可包括一个或多个分区, 一般示为 410、420、430、440、450、460 和 470。分区 410、420、430、440、450、460 和 470 可分别对应于如上结合图 3 所述的分区 310、320、330、340、350、360 和 370。CPU110 可具有与第一和第二存储器范围 440 和 450 中每一个均关联的验证密钥。在启动第二存储器范围 450 的读访问的条件下, 集成控制器 150 可将存储在第二存储器范围 450 中的数据 (如数据 455) 提供给 CPU110。

[0029] 与图 3 中存储器阵列配置 300 的第一存储器范围 340 相反, 集成控制器 150 可禁止第一存储器范围 440 的读访问。因此, 即使 CPU110 具有与第一存储器范围 440 关联的验证密钥, 数据 445 对 CPU110 来说也可能是不可得到的 (如对 CPU110 隐瞒)。相替代地, 集成控制器 150 可将存储在寄存器 175 中的预定值 445 提供给 CPU110。本文描述的方法和装置并不限于此点。

[0030] 如上所述, 集成控制器 150 可具有存储器范围 180 的静态读访问控制或动态读访问控制。更具体地说, 静态读访问控制可禁止存储器范围 180 的读访问直到闪存设备 120 被重置。在一个示例中, 静态读访问控制可用于保护引导过程 (如无线 (over-the-air) 广播应用代码, 诸如更新补丁) 中使用的信息。在被 CPU110 访问之后, 除非闪存设备 120 被重置, 否则该信息可能无法访问。静态读访问控制的状态可通过集成控制器 150 的非易失性 (NV) 位指示。

[0031] 与静态读访问控制相似, 动态读访问控制也可禁止存储器阵列 180 的读访问, 直到闪存设备 120 被重置。然而动态读访问控制可响应于验证的读访问命令来启动存储器范围 180 的读访问。相应地, 动态读访问控制可开启或关闭存储器范围 180 的读访问。在一个示例中, 动态读访问控制可用于在应用和对应的数据之间提供隔离。因此当应用没有运行时, 动态读访问控制可保护应用的敏感数据。动态读访问控制的状态可通过集成控制器 150 的 RAM 位指示。

[0032] 图 5 和图 6 描述了多种方式, 其中图 1 中基于闪速存储器的示例处理系统 100 可提供与闪存设备 (如图 1 中的闪存设备 120) 关联的读访问控制系统。图 5 和 6 中的示例过程 500 和 600 可利用存储在任意组合的机器可访问介质 (诸如易失性或非易失性存储器或其它大容量存储设备 (如软盘、CD 和 DVD)) 中的任意多种不同的程序代码分别被实现为机器可访问的指令。例如, 机器可访问指令可被包括在机器可访问介质诸如可编程门阵列、专用集成电路 (ASIC)、可擦除可编程只读存储器 (EPROM)、ROM、RAM、磁性介质、光学介质和 / 或任意其它合适类型的介质中。

[0033] 此外, 尽管行为的特定顺序在图 5 和 6 中都被描述, 但是这些行为可以其它时间顺序被执行。例如, 图 5 和 / 或 6 中描述的行为可以重复、串行和 / 或并行的方式被执行。此外, 结合图 1 中装置, 示例过程 500 和 600 仅提供和描述为提供与闪存设备关联的读访问控制系统的示例。

[0034] 在静态读访问模式中,例如,图 5 中描述的过程 500 可开始于监视(如通过集成控制器 150)来自 CPU110 的读访问命令的闪存设备 120(模块 510)。更具体地说,CPU110 可请求访问存储器阵列 155 的特定存储器范围(如图 1 中的存储器范围 180)。如果闪存设备 120 不从 CPU110 接收读访问命令,则集成控制器 150 可继续监视读访问命令。

[0035] 否则如果在模块 510 闪存设备 120 接收来自 CPU 的读访问命令,则集成控制器 150 可确定读访问命令是否是验证的读访问命令(模块 520)。在一个示例中,读访问命令可根据 RSA 签名协议被验证。如果读访问命令不是验证的读访问命令,则控制可返回模块 510。然而如果读访问命令是验证的读访问命令,则集成控制器 150 可确定闪存设备 120 是否被重置(模块 530)。在一个示例中,闪存设备 120 可在引导过程之前和 / 或引导过程期间从集成控制器 150 接收重置命令。

[0036] 如果闪存设备 120 被重置,则集成控制器 150 可将存储在存储器范围 180 中的数据提供给 CPU110(模块 540)。相应地,集成控制器 150 可禁止存储器范围 180 的读访问(模块 550)。否则如果在模块 530 闪存设备 120 没有被重置,则集成控制器 150 可拒绝存储器范围 180 的读访问并且将存储在寄存器 185 中的预定值提供给 CPU110(模块 560)。本文描述的方法和装置并不限于此点。

[0037] 在动态读访问模式中,例如,图 6 中描述的过程 600 可开始于监视(如通过集成控制器 150)来自 CPU110 的读访问命令的闪存设备 120(模块 610)。更具体地说,CPU110 可请求访问存储器阵列 155 的特定存储器范围(如图 1 中的存储器范围 180)。如果闪存设备 120 不从 CPU110 接收读访问命令,则集成控制器 150 可继续监视读访问命令。

[0038] 否则,如果在模块 610,闪存设备 120 从 CPU 接收读访问命令,则集成控制器 150 可确定读访问命令是否是验证的读访问命令(模块 620)。如果读访问命令不是验证的读访问命令,则控制可返回模块 510。然而如果读访问命令是验证的读访问命令,则集成控制器 150 可监视许可命令(grant command)以便验证存储器范围 180 的读访问(模块 630)。

[0039] 如果集成控制器 150 检测到许可命令,则集成控制器 150 可将存储在存储器范围 180 的数据提供给 CPU110(模块 640)。更具体地说,许可命令可启动存储器范围 180 的读访问。相应地,集成控制器 150 可禁止存储器范围 180 的读访问(模块 650)。否则如果在模块 630,集成控制器 150 没有成功检测到许可命令,则集成控制器 150 可确定闪存设备 120 是否被重置(模块 660)。

[0040] 如果闪存设备 120 被重置,则集成控制器 150 可将存储在存储器范围 180 中的数据提供给 CPU110(模块 640)。相应地,集成控制器 150 可禁止存储器范围 180 的读访问(模块 650)。否则如果在模块 660,闪存设备 120 没有被重置,则集成控制器 150 可拒绝存储器范围 180 的读访问并且将存储在寄存器 175 中的预定值提供给 CPU110(模块 670)。本文描述的方法和装置并不限于此点。

[0041] 尽管上述示例仅描述了两种读访问模式(如静态读访问模式和动态读访问模式),本文描述的方法和装置显然也适于根据其它合适的读访问模式进行操作。尽管本文公开的方法和装置在图 5 和 6 中被描述为以特定的方式进行操作,本文公开的方法和装置无需图 5 和 6 中描述的特定模块显然也可应用。此外,尽管图 5 和 6 描述了特定模块,这些模块中的一些执行的行为也可被集成在单个模块中或者可利用两个或多个分开的模块来实现。

[0042] 图 7 是适于实现本文公开的方法和装置的示例处理器系统 2000 的框图。处理器系统 2000 可以是桌面计算机、膝上计算机、手持计算机、平板计算机、PDA、服务器、因特网应用和 / 或其它类型的计算设备。

[0043] 图 7 中描述的处理器系统 2000 可包括芯片组 2010, 它包括存储器控制器 2012 和输入 / 输出 (I/O) 控制器 2014。芯片组 2010 可提供存储器和 I/O 管理功能, 还有多个通用寄存器和 / 或专用寄存器、计时器等, 它们可被处理器 2020 访问或使用。处理器 2020 可利用一个或多个处理器、WPAN 组件、WLAN 组件、WMAN 组件、WWAN 组件和 / 或其它合适的处理组件来实现。例如, 处理器 2020 可利用一个或多个^{英特尔®}酷睿™技术、^{英特尔®}奔腾®技术、^{英特尔®}安腾®技术、^{英特尔®}迅驰®技术、^{英特尔®}至强™技术和 / 或^{英特尔®}XScale®技术来实现。作为备选, 其它处理技术可用于实现处理器 2020。处理器 2020 可包括高速缓冲存储器 2022, 它可利用第一级统一缓冲存储器 (L1)、第二级统一缓冲存储器 (L2)、第三级统一缓冲存储器 (L3) 和 / 或任意其它合适的结构存储数据来实现。

[0044] 存储器控制器 2012 可执行启动处理器 2020 通过总线 2040 访问并与包括易失性存储器 2032 和非易失性存储器 2034 的主存储器 2030 通信的功能。易失性存储器 2032 可通过同步动态随机访问存储器 (SDRAM)、动态随机访问存储器 (DRAM)、RAMBUS 动态随机访问存储器 (RDRAM) 和 / 或任意其它类型的随机访问存储器设备来实现。非易失性存储器 2034 可利用闪速存储器、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM) 和 / 或任意其它期望类型的存储器设备来实现。

[0045] 处理器系统 2000 还可包括耦合到总线 2040 的接口电路 2050。接口电路 2050 可利用任意类型的接口标准 (诸如以太网接口、通用串行总线 (USB)、第三代输入 / 输出 (3GIO) 接口和 / 或任意其它合适类型的接口) 来实现。

[0046] 一个或多个输入设备 2060 可被连接到接口电路 2050。输入设备 2060 容许个体将数据和命令输入到处理器 2020。例如, 输入设备 2060 可由键盘、鼠标、触控式显示器 (touch-sensitive display)、跟踪板、跟踪球、网格 (isopoint) 和 / 或语音识别系统来实现。

[0047] 一个或多个输出设备 2070 也可连接到接口电路 2050。例如, 输出设备 2070 可由显示设备 (如发光二极管 (LED)、液晶显示器 (LCD)、阴极射线管 (CRT) 显示器、打印机和 / 或扬声器) 来实现。接口电路 2050 可包括尤其是图形驱动卡。

[0048] 处理器系统 2000 还可包括一个或多个大容量存储设备 2080 以存储软件和数据。这种大容量存储设备 2080 的示例包括软盘及驱动、硬盘驱动、压缩磁盘及驱动, 还有数字多功能磁盘 (DVD) 及驱动。

[0049] 接口电路 2050 还可包括通信设备 (诸如调制解调器或网络接口卡), 从而促进通过网络与外部计算机的数据交换。处理器系统 2000 和网络之间的通信链路可以是任意类型的网络连接, 诸如以太网连接、数字用户线路 (DSL)、电话线路、移动电话系统、同轴电缆等。

[0050] 输入设备 2060、输出设备 2070、大容量存储设备 2080 和 / 或网络的访问可由 I/O 控制器 2014 进行控制。更具体地说, I/O 控制器 2014 可执行启动处理器 2020 通过总线 2040 和接口电路 2050 与输入设备 2060、输出设备 2070、大容量存储设备 2080 和 / 或网络进行通信的功能。

[0051] 尽管图 7 中给出的组件被描述为处理器系统 2000 内分开的模块，这些模块中的一些执行的功能也可集成在单个半导体电路内或者可利用两个或多个分开的集成电路来实现。例如，尽管存储器控制器 2012 和 I/O 控制器 2014 被描述为芯片组 2010 中分开的模块，存储器控制器 2012 和 I/O 控制器 2014 也可集成在单个半导体电路内。

[0052] 尽管本文已经描述了某些示例性的方法、装置和制品，但是本公开的覆盖范围并不限于此。相反，本公开逐条地或教义等价地覆盖属于所附权利要求范围内的所有方法、装置和制品。例如，尽管上面公开的示例系统包括尤其是在硬件上执行的软件或固件，但是应该注意这样的系统仅仅是描述性的并且不应该被认为是限制性的。更具体地说，可以预期任意或全部公开的硬件、软件和 / 或固件组件可被专门包括在硬件中、专门在软件中、专门在固件中或者在硬件、软件和 / 或固件的某些组合中。

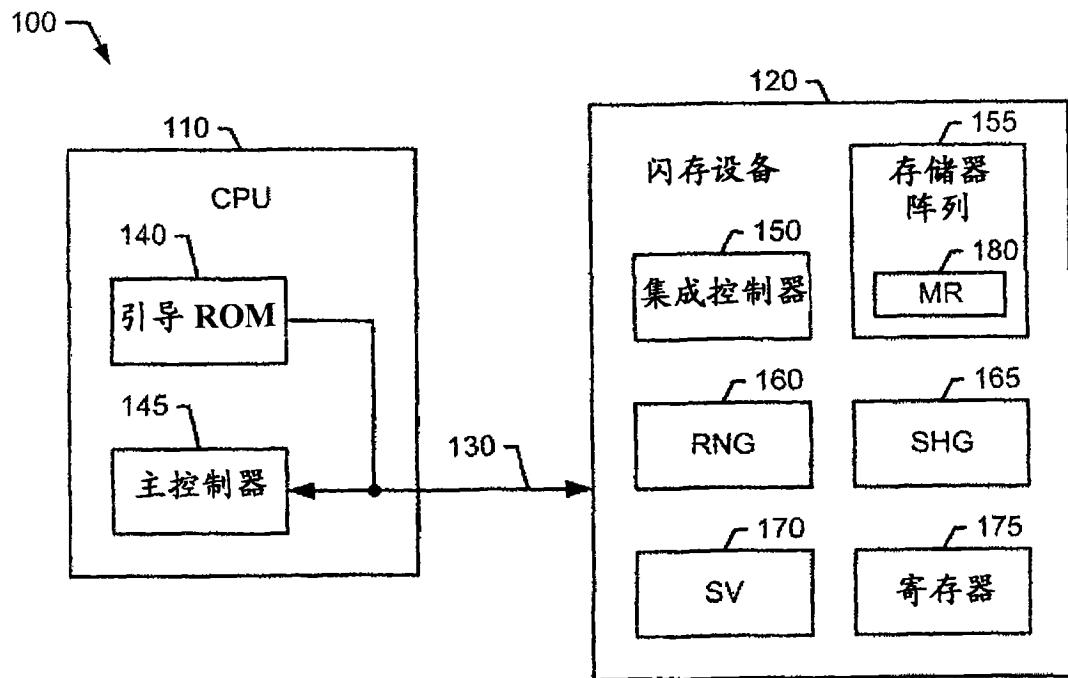


图 1

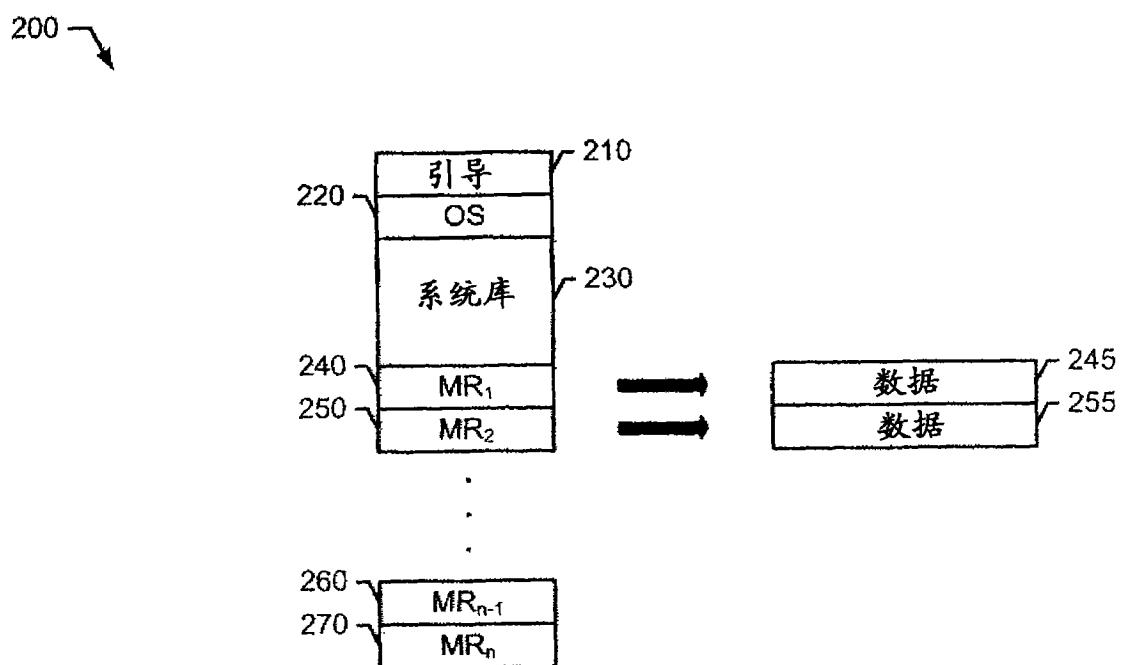


图 2

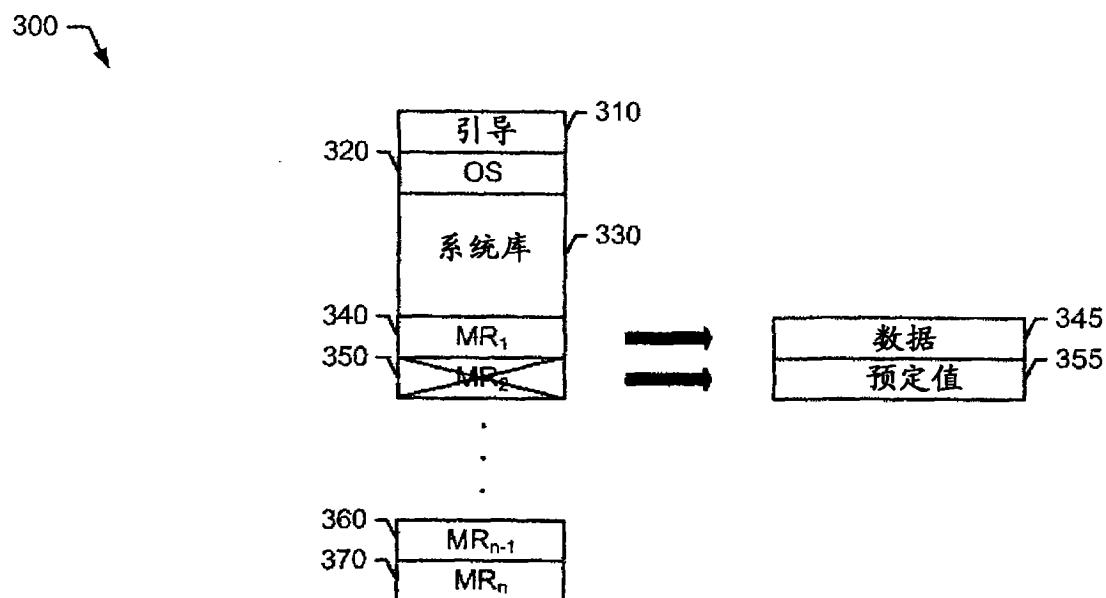


图 3

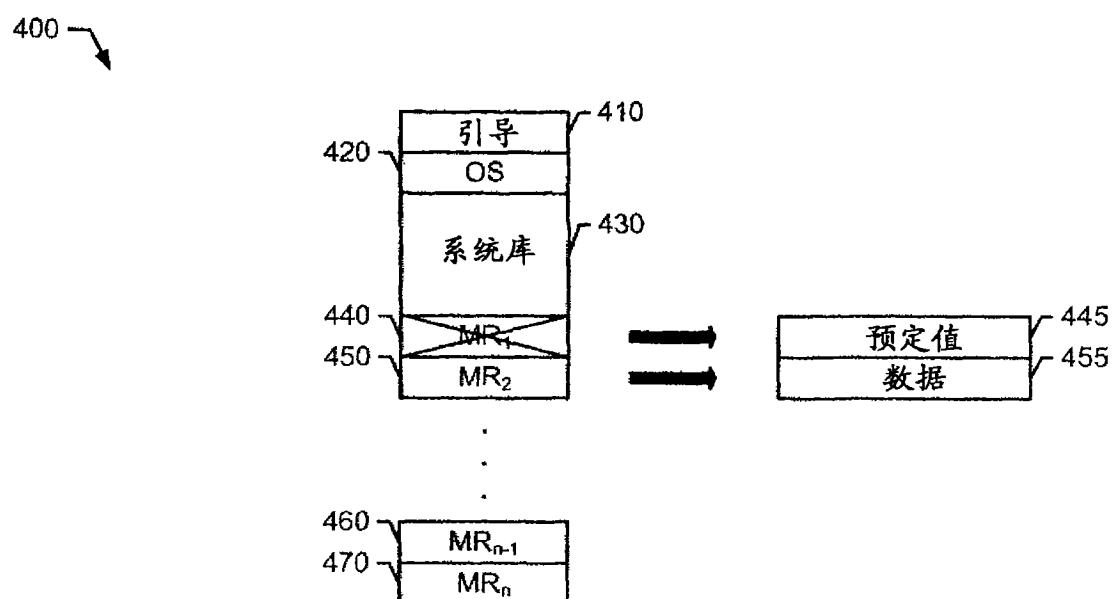


图 4

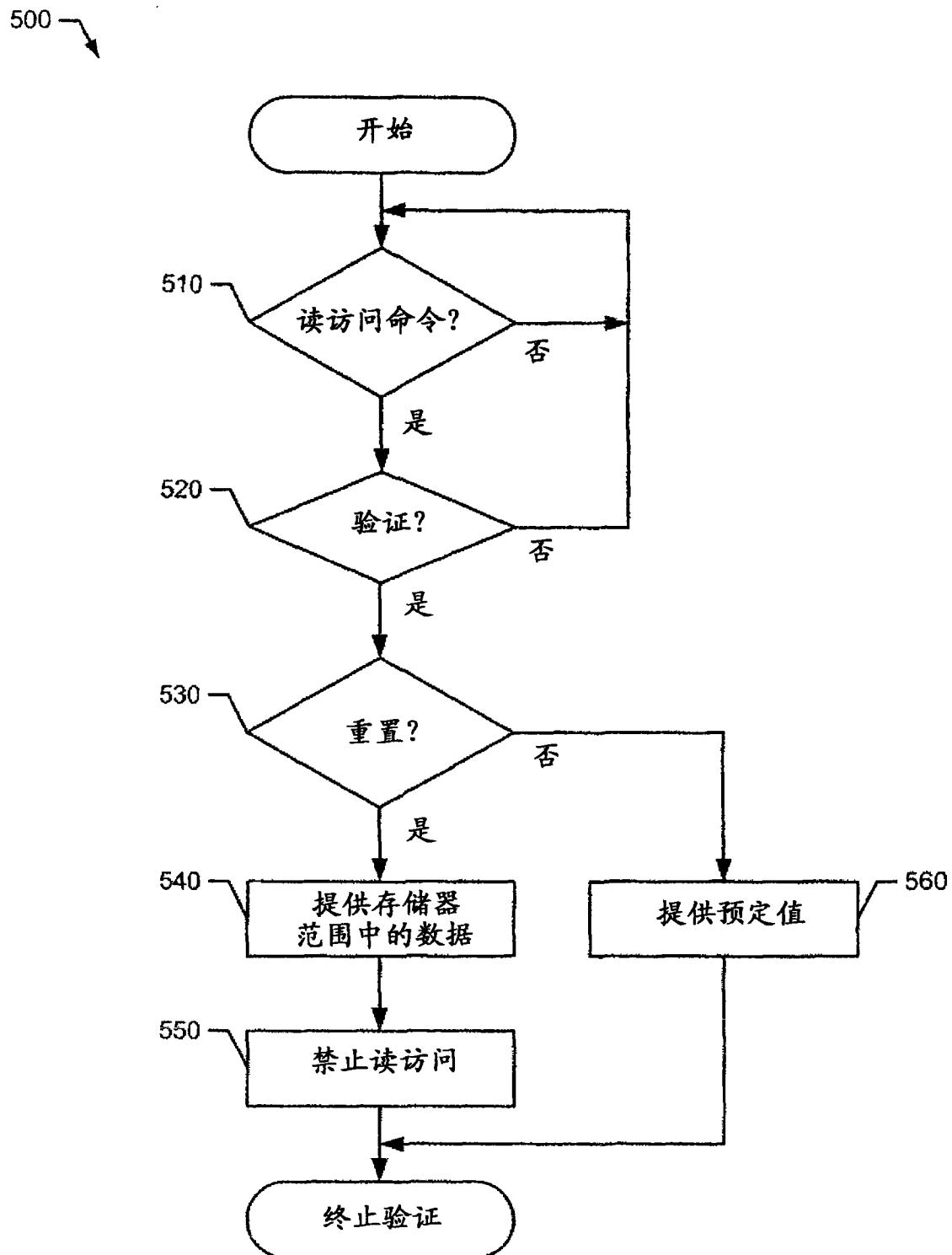


图 5

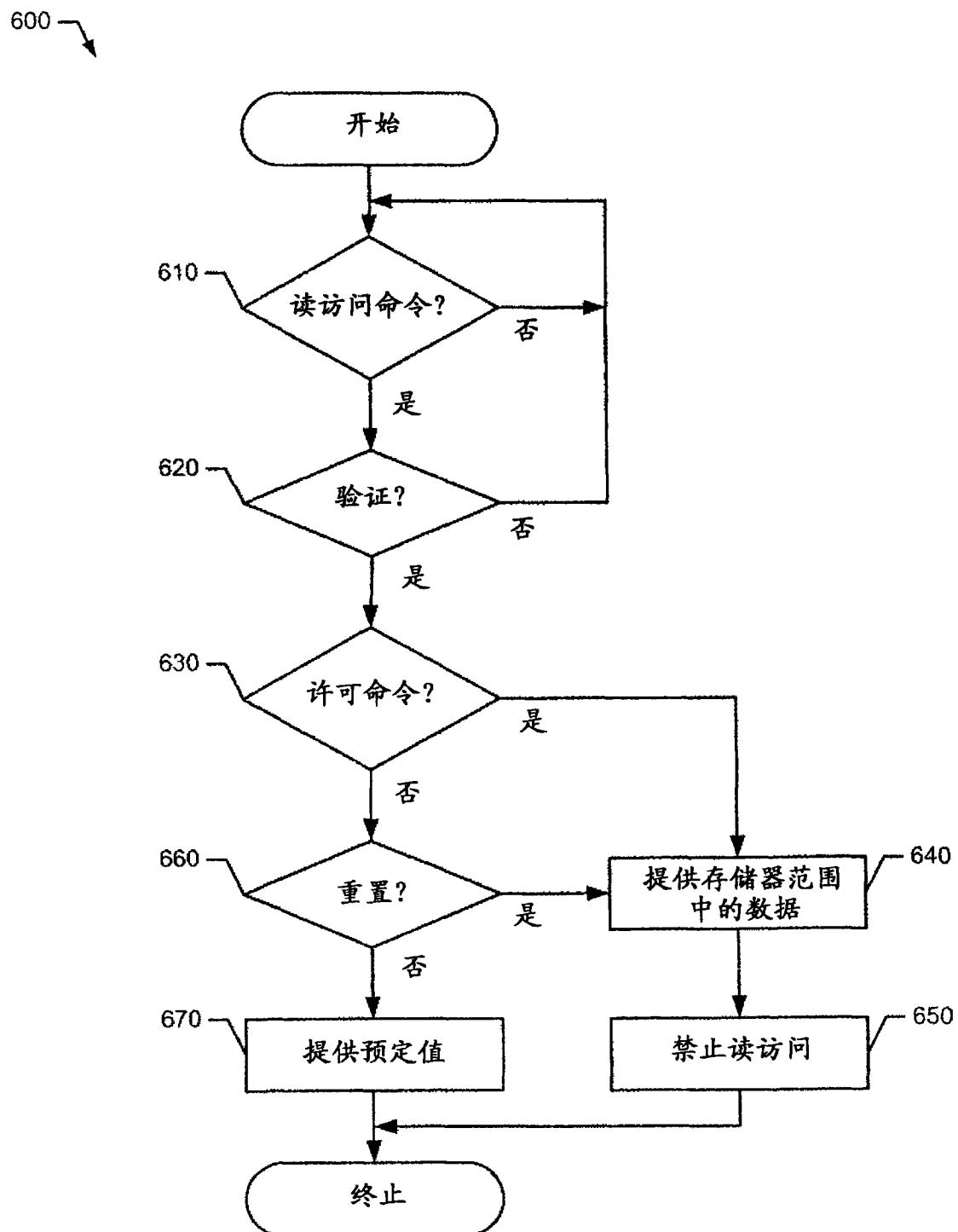


图 6

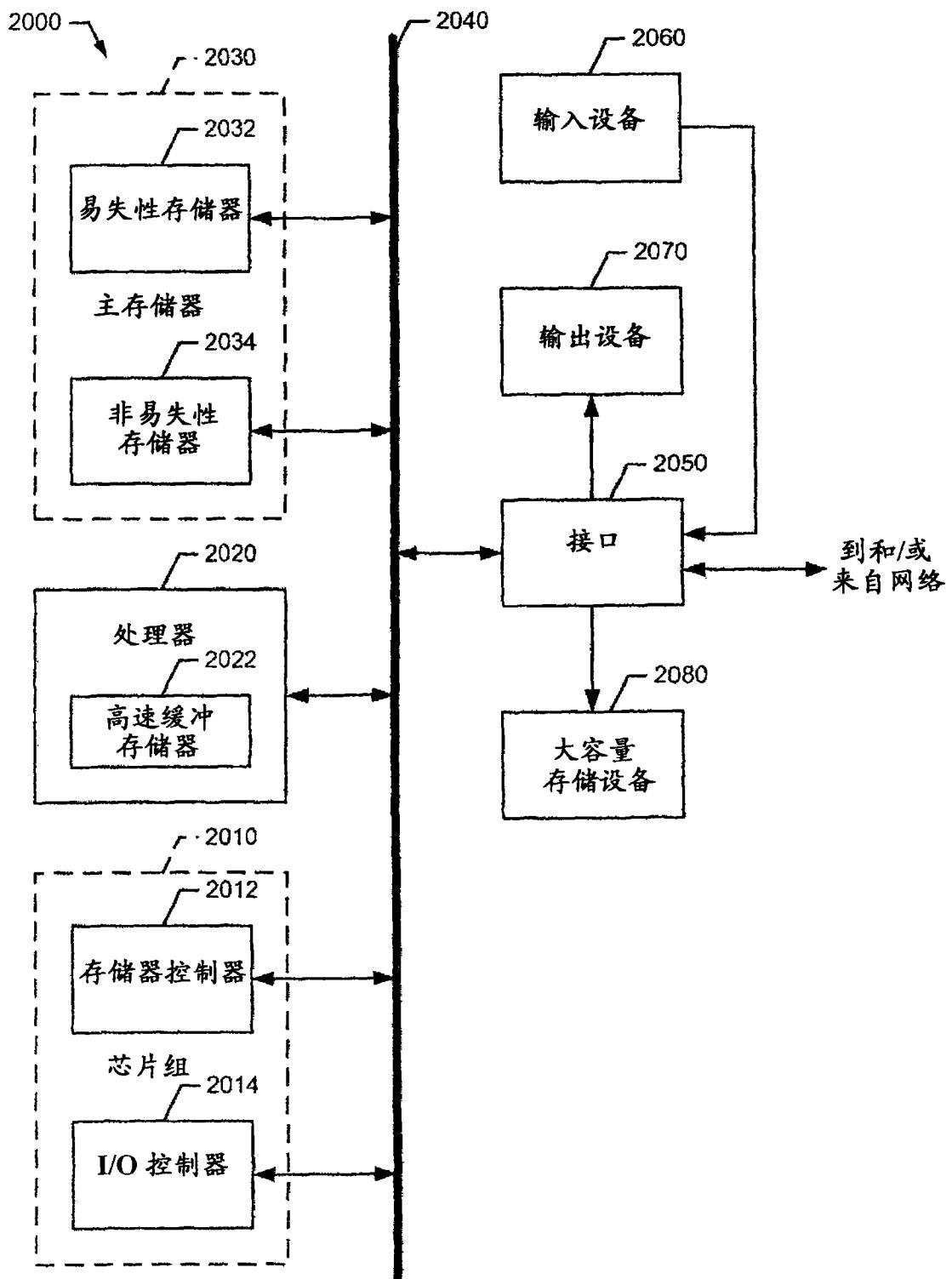


图 7