



[12] 发明专利说明书

专利号 ZL 03814832.3

[45] 授权公告日 2009 年 1 月 7 日

[11] 授权公告号 CN 100449558C

[22] 申请日 2003.6.20 [21] 申请号 03814832.3

[30] 优先权

[32] 2002.6.26 [33] US [31] 10/185,887

[86] 国际申请 PCT/US2003/019597 2003.6.20

[87] 国际公布 WO2004/003711 英 2004.1.8

[85] 进入国家阶段日期 2004.12.24

[73] 专利权人 英特尔公司

地址 美国加利福尼亚州

[72] 发明人 D·格劳科克 D·普斯纳

[56] 参考文献

WO01/63994A2 2001.8.30

US2001/0018736A1 2001.8.30

US6188257B1 2001.2.13

EP0965902A2 1999.12.22

US6275933B1 2001.8.14

US5533123 1996.7.2

EP1085396A1 2001.3.21

审查员 刘 梯

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 钱慰民

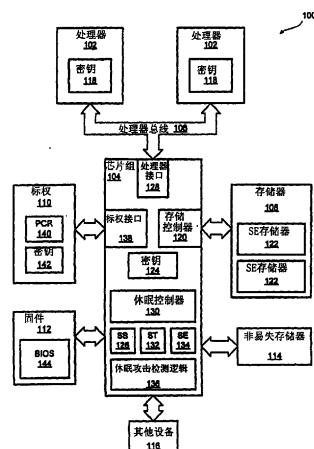
权利要求书 4 页 说明书 11 页 附图 4 页

[54] 发明名称

休眠保护

[57] 摘要

描述方法，装置，和机器可读介质，它们试图保护秘密免受休眠攻击。在某些实施例中，在进入休眠状态之前加密该秘密并卸除安全增强环境。在某些实施例中，响应于唤醒事件，还重建安全增强环境并解密该秘密。



1.一种用于防御休眠攻击的方法，所述休眠攻击是在从休眠状态唤醒时试图访问秘密信息，所述方法包括：

检测可能的休眠攻击；

判定存储单元是否包含未加密的秘密信息；和

响应于判定所述存储单元可能包含未加密的秘密信息，调用休眠攻击响应，所述休眠攻击响应保护秘密信息免受可能的休眠攻击。

2.如权利要求 1 的方法，其特征在于，还包括：

响应休眠事件，判断存储单元是否可能包含秘密信息；和

响应于判定所述存储单元可能包括秘密信息，调用所述休眠攻击响应。

3.如权利要求 1 的方法，其特征在于，还包括：

响应休眠事件，加密存储单元的一个或多个部分中的内容。

4.如权利要求 3 的方法，其特征在于还包括：

产生内容证明，以证明所述存储单元的一个或多个部分中的内容。

5.如权利要求 3 的方法，其特征在于，还包括：

产生标识所述存储单元的一个或多个部分的结构；和

产生一个或多个证明，以证明所述结构和所述存储单元的一个或多个部分中的内容。

6.如权利要求 5 的方法，其特征在于，还包括：

将所述结构和所述一个或多个证明密封到计算设备的监视单元。

7.如权利要求 1 的方法，其特征在于，还包括：

响应于调用所述休眠攻击响应来产生系统复位。

8.一种芯片组，其特征在于包括：

休眠攻击检测逻辑单元，以检测休眠攻击，所述休眠攻击是在从休眠状态唤醒时试图访问秘密信息；

秘密信息指示器，指示存储单元是否包含未加密的秘密信息；

其中响应于检测到的休眠攻击以及存储单元包含未加密的秘密信息的指示，所述休眠攻击检测逻辑单元调用攻击响应。

9. 如权利要求 8 的所述芯片组，其特征在于，还包括休眠使能存储器，所述休眠使能存储器用于指示进入休眠状态；

所述休眠攻击检测逻辑单元还根据所述休眠使能存储器指示进入休眠状态而检测休眠攻击。

10. 如权利要求 9 的所述芯片组，其特征在于，还包括休眠类型存储器以指示所请求的休眠状态；

所述休眠攻击检测逻辑单元还根据所述休眠类型存储器指示特定休眠状态而检测休眠攻击。

11. 如权利要求 9 的所述芯片组，其特征在于，还包括一接口，所述接口支持对秘密信息的可信核查。

12. 如权利要求 9 的所述芯片组，其特征在于，还包括一接口，所述接口在允许更新所述秘密信息指示器之前需要接收一个或多个消息。

13. 一个包括操作系统及位于更高特权级别的监视单元的系统；

所述操作系统接收休眠事件，并将所述休眠事件的处理传输给所述监视单元；和

响应于所述休眠事件，所述监视单元加密存储单元的一个或多个页面，并指示所述存储单元不包含未加密的秘密信息。

14. 如权利要求 13 的系统，其特征在于，所述监视单元还更新一秘密信息存储器，以指示所述存储单元不包含未加密的秘密信息。

15. 如权利要求 13 的系统，其特征在于，

所述监视单元将所述休眠事件的处理返回给所述操作系统；和

所述操作系统将存储单元的加密的和未加密的页面写到非易失存储器。

16. 如权利要求 13 的系统，其特征在于，

所述监视单元将所述休眠事件的处理返回给所述操作系统；和

所述操作系统使所述系统进入休眠状态。

17. 如权利要求 16 的系统，其特征在于，所述操作系统更新一休眠类型存储器以指示拟进入的所述休眠状态，并更新一休眠使能存储器以指示进入所述休眠状态。

18. 如权利要求 13 的系统，其特征在于，所述监视单元还产生内容证明，所述内容证明是用于证明所述存储单元的所述加密的页面。

19. 如权利要求 18 的系统，其特征在于，所述监视单元还产生标识所述加密的页面的结构，并产生用于证明所述结构的结构证明。

20. 如权利要求 19 的系统，其特征在于，所述监视单元还向所述监视单元密封：所述内容证明、所述结构证明、和解密所述经加密页面的监视单元密钥。

21. 一种用于防御休眠攻击的系统，所述休眠攻击是在从休眠状态唤醒时试图访问秘密信息，所述系统包括：

易失存储器，包括安全增强区域；

秘密信息存储器，指示所述易失存储器是否可能包含未加密的秘密信息；

休眠使能存储器，指示进入休眠状态；

处理器，响应于休眠事件而加密所述安全增强区域，并响应于加密所述安全增强区域而更新所述秘密信息存储器，以指示所述易失存储器不包含未加密的秘密信息；和

休眠攻击检测逻辑单元，响应于所述休眠使能存储器被更新为指示进入休眠状态并响应于所述秘密信息存储器指示所述易失存储器可能包含未加密的秘密信息，而调用休眠攻击响应，所述休眠攻击响应保护秘密信息免受可能的休眠攻击。

22. 如权利要求 21 的系统，其特征在于，所述处理器还产生一证明安全增强区域的内容证明，并若所述内容证明指示所述安全增强区域不可靠时，响应于唤醒事件而调用休眠攻击响应。

23. 如权利要求 22 的系统，其特征在于，所述处理器还将所述内容证明和解密所述安全增强区域的密钥密封到所述系统。

24. 如权利要求 23 的系统，其特征在于，若解密封所述内容证明和所述密钥失败，所述处理器则响应于唤醒事件调用休眠攻击响应。

25. 一种用于防御休眠攻击的方法，所述休眠攻击是在从休眠状态唤醒时试图访问秘密信息，所述方法包括：

响应休眠事件加密存储单元的内容；和

产生证明所述存储单元的所述内容的内容证明。

26. 如权利要求 25 的方法，其特征在于，还包括：

响应于唤醒事件，使用所述内容证明来验证所述内容的可靠性；和

响应于判定所述存储单元的所述内容不可靠，调用休眠攻击响应。

27. 如权利要求 26 的方法，其特征在于，还包括：

响应于休眠事件，将所述内容证明和解密所述存储单元的所述内容的密钥密封到一特定系统；

响应于唤醒事件解密封所述内容证明及所述密钥，且

响应于解密所述内容证明及所述密钥的失败，调用休眠攻击响应。

28. 一种用于防御休眠攻击的系统，所述休眠攻击是在从休眠状态唤醒时试图访问秘密信息，所述系统包括：

用于响应休眠事件加密存储单元内容的装置；和

用于产生证明所述存储单元的所述内容的内容证明的装置。

29. 如权利要求 28 的系统，其特征在于，还包括：

用于响应于唤醒事件，使用所述内容证明来验证所述内容的可靠性的装置；和

用于响应于判定所述存储单元的所述内容不可靠，调用休眠攻击响应的装置。

30. 如权利要求 29 的系统，其特征在于，还包括：

用于响应于休眠事件，将所述内容证明和解密所述存储单元的所述内容的密钥密封到所述系统的装置；

用于响应于唤醒事件解密封所述内容证明及所述密钥的装置，且

用于响应于解密所述内容证明及所述密钥的失败，调用休眠攻击响应的装置。

休眠保护

技术领域

本发明涉及计算机设备，尤其是，涉及一种能够使计算机设备免受休眠攻击的方法和系统。

背景技术

财经和个人事务越来越多地在计算设备上完成。然而，这种财经和个人事务的持续增长部分地取决于建立安全增强的环境（SE），该环境试图防止私密的丢失，数据的破坏，数据的误用。SE 环境可以利用各种技术来防止不同类型的攻击或对受保护数据或秘密（如社会保障号、帐号、银行平衡帐、密钥、授权密码等）的非授权的访问。SE 环境试图防止的一类攻击是休眠攻击。

例如，许多计算设备支持挂起到存储器的休眠状态，如在 Advanced Configuration and Power Interface（ACPI-高级配置与电源接口）规范 2000 年 7 月 27 日的 2.0 版本中描述的 S3 休眠状态。在进入到挂起的存储器休眠状态之后，计算设备切断到计算设备的各种组件和/或子组件的电源，但继续向系统存储器供电，以保持系统存储器的内容。作为切断电源的结果，计算设备可能将给用于保护储存在系统存储器中秘密的线路的电源切断。在从休眠状态唤醒之后，计算设备能将电源返回给用于保护储存在系统存储器中的秘密的线路。然而，返回电源之后，保护线路可能处在复位状态，且实际上不能保护系统存储器中的秘密。攻击者可以在重建保护线路提供的保护之前成功地获得对存储的秘密的访问。

发明内容

根据本发明的一个方面，提供了一种用于防御休眠攻击的方法，所述休眠攻击在从休眠状态唤醒时试图访问秘密信息，所述方法包括：检测可能的休眠攻击；判定存储单元是否包含未加密的秘密信息；和响应于判定所述存储单元可能包含未加密的秘密信息，调用休眠攻击响应，所述休眠攻击响应保护秘密信息免受可能的休眠攻击。

根据本发明的另一个方面，提供了一种芯片组，其特征在于包括：休眠攻击检测逻辑单元，以检测休眠攻击，所述休眠攻击是在从休眠状态唤醒时试图访问秘密信息；秘密信息指示器，指示存储单元是否包含未加密的秘密信息；其中响应于检测到的休眠攻击以及存储单元包含未加密的秘密信息的指示，所述休眠攻击检测逻辑单元调用攻击响应。

根据本发明的另一个方面，提供了一个包括操作系统及位于更高特权级别的监视单元的系统；所述操作系统接收休眠事件，并将所述休眠事件的处理传输给所述监视单元；和响应于所述休眠请求，所述监视单元加密存储单元的一个或多个页面，并指示所述存储单元不包含未加密的秘密信息。

根据本发明的又一个方面，提供了一种用于防御休眠攻击的系统，所述休眠攻击是在从休眠状态唤醒时试图访问秘密信息，所述系统包括：易失存储器，包括安全增强区域；秘密信息存储器，指示所述易失存储器是否可能包含未加密的秘密信息；休眠使能存储器，指示进入休眠状态；处理器，响应于休眠事件而加密所述安全增强区域，并响应于加密所述安全增强区域而更新所述秘密信息存储器，以指示所述易失存储器不包含未加密的秘密信息；和休眠攻击检测逻辑单元，响应于所述休眠使能存储器被更新为指示进入休眠状态并响应于所述秘密信息存储器指示所述易失存储器可能包含未加密的秘密信息，而调用休眠攻击响应，所述休眠攻击响应保护秘密信息免受可能的休眠攻击。

根据本发明的还有一个方面，提供了一种用于防御休眠攻击的方法，所述休眠攻击是在从休眠状态唤醒时试图访问秘密信息，所述方法包括：响应休眠事件加密存储单元的内容；和产生证明所述存储单元的所述内容的内容证明。

同时，本发明也提供了对应上述方法的一种用于防御休眠攻击的系统。

附图说明

这里描述的本发明在附图中作为例子而不作为限制地示出。为说明的简单和清楚，在图中示出的单元不必按比例画出。例如，为了清楚起见某些单元的尺寸相对于其他单元被夸大了。此外，在认为合适的地方，参照号在各图中重复使用，以表示对应的或类似的单元。

图 1 示出计算设备的实施例。

图 2 示出能由图 1 的计算设备建立的安全增强（SE）环境为实施例。

图 3 示出图 1 的计算设备的休眠方法的实施例。

图 4 示出图 1 的计算设备的唤醒方法的实施例。

具体实施方式

下面内容描述用于保护秘密免受休眠攻击的技术。在下面描述中，为提供本发明的更透彻的理解列出许多具体的细节，如逻辑工具，操作码，指定操作数的方法，资源划分/共享/复制工具，系统组件的类型和相互关系，和逻辑划分/集成选择等。然而本专业技术人员可以理解，即使没有上述这些具体细节，本发明还是可以实施。在其他情况，为了不模糊本发明，不详细示出控制结构，门线线路，和全部软件指令序列。用这里包括的描述，本专业技术人员能实现合适的功能而不必过多的实践。

在本说明中对“单个实施例”，“一个实施例”，“一个示例实施例”等的引用表明，所描述的实施例可以包括特定的特征，结构或特点，但不必要每个实施例都包括特定的特征，结构或特点。此外，这样的短语不必要关系到同一实施例。而且当结合一个实施例描述特定的特征，结构或特点时，应该理解在本专业的技术人员的知识范围内，可以结合其他实施例实现这样的特征结构或特点，，而无需是否明确描述。

这里对“对称”密码术，密钥，加密或解密的引用，指的是同一密钥用于加密和解密的密码技术。在 1993 年作为美国联邦信息处理标准 FIPS PUB 46-2 发布的众知的数据加密标准（DES）和在 2001 年作为 FIPS PUB 197 发布的高级加密标准（AES）是两个对称密码术的例子。这里对“非对称”密码术、密钥、加密或解密的引用指的是对加密和解密使用不同但有关的密钥的密码技术。包括众知的公开密钥算法（RSA-Rivest-Shamir-Adleman）技术的所谓“公开密钥”密码技术是非对称密钥术的例子。非对称密码系统的两个相关密钥之一在这里称为私有密钥（因为它通常保持秘密），另一密钥称为公开密钥（因为它通常免费可得）。在某些实施例中，私有或公开密钥均能用于加密，而另一密钥用于关联的解密。

这里使用的术语“对象”拟作为广义上的术语，它包括一个或多个位的任何组合而不管其结构，格式，或表示。而且动词“散列”及有关的格式在这里用于意指在操作数或消息上完成操作，以产生摘要值或“散列值”。理想上，散列操作生成摘要值，从该值在计算上不可能找到带有那个散列值的消息，且从该值人们不可能确定有关带有那个散列值的消息的任何有用信息。此外，散列操作理想上产生散列值，使得在计算上不可能确定产生同一散列值的两个消息。虽然散列操作理想上具有上述特征，实际上如 Message Digest5 函数（MD5）和 Secure Hashing Algorithm1(SHA-1)那样的单向函数产生散列值，从它推导消息是困难的，计算量大的，和/或实际上不可行的。

本发明的实施例能以硬件、固件、软件、或其任何组合实现。本发明的实施例也能作为存储在机器可读介质上的指令实现，该介质能由一个或多个处理器读出并执行。机器可读介质是包括以机器（如计算设备）可读的形式存储或发送信息的任何机制。例如，机器可读介质能包括只读存储器（ROM）；随机访问存储器（RAM）；磁盘存储介质；光存储介质；闪存设备；电、光、声或其他形式的传播信号（如载波、红线外信号、数字信号等）。

图 1 中示出计算设备 100 的示例实施例。计算设备 100 能包括通过处理器总线 106 连接芯片组 104 的一个或多个处理器 102。芯片组 104 能包括一个或多个集成电路封装或芯片，它们将处理器 102 耦合到系统存储器 108，权标（token）110，固件 112，非易失存储器 114（如硬盘、软盘、光盘、闪盘、可编程只读存储器等）和/或其他设备 116（如鼠标、键盘、视频控制器等）。

处理器 102 能支持安全进入 (SENTER) 指令的执行，以起动建立 SE 环境，如图 2 中的示例 SE 环境。处理器 102 还能进一步支持安全退出 (SEXIT) 指令，以起动 SE 环境的卸除。在一个实施例中，处理器 102 能在处理器总线 106 上发出与 SENTER、SEXIT 和其他指令的执行关联的总线消息。

处理器 102 还能进一步包括密钥 118，例如对称密码密钥、非对称密码密钥、或某些其他类型密钥。处理器 102 能使用处理器密钥 118 在执行认证代码 (authentic code, AC) 模块以前认证一认证代码 (AC) 模块。在一实施例中，处理器密钥 118 包括只有处理器 102 具有对其访问的非对称私有密钥。

处理器 102 能支持一个或多个操作模式，如实模式、保护模式、虚拟实模式、和虚拟机器模式 (VMX 模式)。此外，处理器 102 在每个支持的操作模式中能支持一个或多个特权级或环。一般而言，处理器 102 的操作模式和特权级定义了可用于执行的指令和执行这样的指令的效果。更具体而言，仅当处理器 102 处在合适的模式和/或特权级时，处理器 102 才被允许执行某些特权指令。

芯片组 104 包括一个或多个芯片或集成电路封装，它们将处理器 102 接口到计算设备 100 的各组件，如系统存储器 108、权标 110、非易失性存储器 114，和其他设备 116。在一个实施例中，芯片组 104 包括存储控制器 120。然而，在另外实施例中，处理器 102 能包括整个或部分存储控制器 120。一般而言，存储控制器 120 为计算设备 100 的各组件提供访问系统存储器 108 的接口。此外，芯片组 104 和/或处理器 102 的存储控制器 120 能将存储器 108 的某些区域定义为安全增强 (SE) 存储器 122。在一个实施例中，处理器 102 在处于合适的操作模式 (如保护模式) 和特权级 (如 OP) 时，只能访问 SE 存储器 122。

此外，芯片组 104 能包括密钥 124，它可用于在执行之前认证 AC 模块。类似于处理器密钥 118，芯片组密钥 124 能包括对称密码密钥、非对称密码密钥、或某些其他类型密钥。在一个实施例中，芯片组密钥 124 包括只有芯片组 104 能对其访问的非对称私有密钥。在另一实施例中，芯片组 104 包括存储在计算设备 100 的另一组件中非对称芯片组密钥 124 的散列。芯片组 104 能检索芯片组密钥 124，并使用该散列认证该密钥 124。

芯片组 104 还能包括秘密存储器 126 以表明系统存储器 108 是否可能包含未经加密的秘密。在一实施例中，秘密存储器 126 能包括一标志，它能被置位以表明系统存储器 108 可能包含未经加密的秘密，并能清除以表明系统存储器 108 不包含未经加密的秘密。在另外实施例中，秘密存储器 126 能位于其他任何处，如权标 110，处理器 102，或计算设备 100 的其他组件。

在一实施例中，秘密存储器 126 能作为具有由电池支撑的后备电源的单个易失存储器位实现。由电池提供的后备电源经历系统复位，休眠事件，系统关闭，系统掉电，或其他电源移除/丢失事件时，保持秘密存储器 126 的内容。芯电组 104 还能包括电池检测线路 (未示出)，以检测由电池提供电源的中断。

该线路还能更新秘密存储器 126，以表明响应检测电源中断，系统存储器 108 能包含秘密。在另外实施例中，秘密存储器 126 作为如闪存位那样的非易失存储器位实现，它不需要电池后备来经历电源移除/丢失事件而保持其内容。在一个实施例中，秘密存储器 126 用能置位或清除的单个存储器位实现。然而，另外实施例能包括具有不同存储容量和/或利用不同状态编码的秘密存储器 126。

芯片组 104 还能保护秘密存储器 126 免遭未经授权的更新。在一实施例中，芯片组 104 包括处理器接口 128 来解码处理器总线 106 的事务和/或从处理器 102 接收消息。处理器 104 能响应执行请求芯片组 104 更新该秘密存储器 126 的一个或多条特权指令，产生总线事务和/或消息。处理器接口 128 接收总线事务和/或消息，并能根据解码的总线事务和/或消息更新秘密存储器 126。在一实施例中，特权指令的有效执行限于在特定处理器的特权级上的软件执行。例如，在一实施例中，特权指令的有效执行被限于在最高特权的处理器级上执行的监视程序（见图 2）。

芯片组 104 还能允许秘密存储器 126 的非特权的更新。在一实施例中，响应于执行一条或多条特权指令，处理器 102 能产生总线事务和/或消息，它们请求芯片组 104 允许秘密存储器 126 的非特权更新。此外，响应于执行一条或多条非特权或特权指令，处理器 102 能产生总线事务和/或消息，它们请求芯片组 104 拒绝对秘密存储器 126 的非特权更新。响应于执行一条或多条非特权指令，处理器 102 能产生总线事务和/或消息，它们请求芯片组 104 更新秘密存储器 126。处理器接口 128 能接收总线事务和/或消息，并根据解码的总线事务和/或消息能允许非特权更新，拒绝非特权更新，和/或更新秘密存储器 126。在一实施例中，为请求非特权更新的特权指令的有效执行被限于在特定处理器特权级上的软件执行。例如，在一实施例中这些特权指令的有效执行被限于在最高特权处理级上执行的监视程序，从而允许监视程序授予选定的非特权代码（如 AC 模块）对秘密存储器 126 的写访问。

芯片组 104 还包括休眠控制器 130，休眠类型存储器 132，休眠使能存储器 134。在一实施例中，休眠控制器 130 根据休眠类型存储器 132 和休眠使能存储器 134 可选地为组件和/或子组件供电。在一实施例中，值能存储在休眠类型存储器，以表明休眠控制器 130 将计算设备 100 置于哪个休眠状态（如 ACPI 休眠状态 S1, S2, S3, S4）。休眠使能存储器 134 能被更新，以调用由休眠状态存储器 132 表明的休眠状态的入口。例如，休眠使能存储器 134 能包括一标志，响应于对其的置位，使休眠控制器 130 将计算设备 100 置于所请求的休眠状态。

芯片组 104 还能包括休眠攻击检测逻辑 136，它检测可能的休眠攻击。在一实施例中，休眠方法更新秘密存储器 126，以表明在更新休眠使能存储器到起动休眠进入过程之前，系统存储器 108 未包含没有加密的秘密。因而，在一

个实施例中，休眠攻击检测逻辑 136 判断，休眠攻击可能响应于：(i) 秘密存储器 126 表明系统存储器 108 可能包含未加密的秘密，和 (ii) 休眠使能存储器 134 请求调用休眠进入过程。响应于检测可能的休眠攻击，休眠攻击检测逻辑 136 起动休眠攻击响应，如产生系统复位事件、系统暂停事件、系统关闭事件、系统掉电事件、或某些其他响应，以保护存储在系统存储器 108 中的秘密。

在另外实施例中，休眠攻击检测逻辑 136 还根据拟进入的休眠状态判断，是否调用休眠攻击响应。例如，用于保护存储在 SE 存储器 122 的秘密的线路能在给定的休眠状态期间保持有效。因而，休眠攻击检测逻辑 136 或者能确定未发生休眠攻击，或确定若休眠类型存储器 132 表明处在 SE 存储器保护保持有效的休眠状态，则不调用休眠攻击响应。

芯片组 104 也能支持在 I/O 总线上的标准 I/O 操作，I/O 总线如：外设部件互连 (PCI) 总线、图形加速端口 (AGP)、通用串行总线 (USB)，低引脚计数 (LPC-Low Pin Count) 总线，或任何其他类型 I/O 总线 (未示出)。尤其是，芯片组 104 能包括权标接口 138，将芯片组 104 与包括一个或多个平台配置寄存器 (PCR) 140 的权标 110 连接。在一个实施例中，权标接口 138 能包括 LPC 总线接口 (LPC 接口规范，Intel 公司，1997 年 12 月 29 日版本 1.0)。

一般而言，权标 110 能以安全增强方式记录规格 (metrics)，以安全增强方式引用规格，能将秘密密封到特定环境 (当前或未来的)，且能将秘密解密封到它们以前被密封的环境。权标 110 能包括用于支持上述操作的一个或多个密钥 142。权标密钥 142 能包括对称密钥，非对称密钥，和/或某种其他类型密钥。权标 110 还能包括一个或多个平台配置寄存器 (PCR 寄存器) 140，以安全增强的方式记录和报告规格。在一个实施例中，权标 110 支持 PCR 扩充的操作，它以安全增强的方式在标识的 PCR 寄存器 140 中记录接收的规格。

权标 110 还能支持 PCR 引用操作，它返回被标识的 PCR 寄存器 140 的引用或内容。权标 110 还能支持密封操作和非密封操作。响应于密封操作，权标 110 产生包括密封到权标 110 的对象和规定的设备环境的密封的对象。相反，仅当一对象用权标 110 的密钥密封，且当前的设备环境满足对该密封的对象规定的环境准则时，权标 110 才能响应于未密封的操作返回密封对象的对象。在一实施例中，权标 110 能包括可信的平台模块 (TPM-Trusted Platform Module)，如在 2001 年 12 月 1 日发表的 Trusted Computing Platform Alliance (TCPA) 主规范版本 1.1a 或其变种所描述。

在一个实施例中，固件 112 包括基本输入/输出系统例程 (BIOS) 144。BIOS 144 能包括 AC 模块、休眠程序、唤醒程序、系统起动程序和/或结构。例如，BIOS 144 能包括 ACPI 结构和 ACPI 源语言 (ASL) 代码，它能在休眠事件处理、唤醒事件处理、和/或计算设备初始化期间被访问和/或执行。

图 2 中示出 SE 环境 200 的一实施例。SE 环境 200 能响应各种事件起动，如系统起动、应用程序请求、操作系统请求等。如图所示，SE 环境 200 能包括可信的虚拟机内核或监视程序 202、一个或多个标准虚拟机（标准 VM）204。和一个或多个可信的虚拟机（可信的 VM）206。在一实施例中，SE 环境 200 的监视程序 202 在最高特权的处理器环（如 0P）上以受保护的方式执行，以管理安全性并提供在虚拟机 204、206 之间的壁垒。

标准的 VM 204 还包括在 VMX 方式的最高特权的处理器环（如 0D）处执行的操作系统 208，和在 VMX 方式的较低特权的处理器环（如 3D）处执行的一个或多个应用程序 210。因为监视程序 202 执行的处理器环比操作系统 208 执行的处理器环具有更高特权，操作系统 208 不具有计算设备 100 无拘束（unfettered）的控制，而相反，受监视程序 202 的控制和限制。尤其是，监视程序 202 能防止操作系统 208 及其应用程序 210 直接访问 SE 存储器 122 和权标 110。

监视程序 202 还能包括休眠逻辑 212 和一个或多个监视程序密钥 214，来加密和/或保护信息。休眠逻辑 212 包括执行一个或多个休眠操作，如对存储器内容加密和加证明。监视程序密钥 214 能包括对称密码密钥、非对称密码密钥、或监视程序 202 对其具有独占控制的其他密钥。例如，监视程序密钥 214 能包括对称根密钥和一个或多个用该对称根密钥加密的非对称密钥。

监视程序 202 能执行对可信的内核 216 的一个或多个测量，如内核代码的散列，以获得一个或多个规格，能使权标 110 用该内核 216 的规格扩充 PCR 寄存器 140，能在储存在 SE 存储器 122 中的有关 PCR 日志中记录该规格，监视程序 202 还能在 SE 存储器 122 中建立可信的 VM 206，并在该已建立的可信的 VM 206 中起动可信的内核 216。

类似地，可信的内核 216 能对小应用程序或应用程序 218 的一个或多个测量，例如小应用程序代码的散列，以获得一个或多个规格。然后经过监视程序 202，可信的内核 216 能使物理权标（physical token）110 用小应用程序 218 的规格扩充 PCR 寄存器 140。可信的内核 216 还在储存在 SE 存储器 122 中的有关 PCR 日志中记录该规格。此外，可信的内核 216 能在 SE 存储器 122 的已建立的可信的 VM 206 中起动可信的小应用程序 218。

响应于起动图 2 的 SE 环境 200，计算设备 100 还在权标 110 的一个或多个 PCR 寄存器 140 中记录监视程序 202 和该计算设备 100 的硬件组件的规格。例如，处理器 102 能获得硬件标识符，如处理器族，处理器版本，处理器微代码版本，芯片组版本，和处理器 102、芯片组 104 及物理权标 110 的物理权标的版本。然后，处理器 102 能在一个或多个 PCR 寄存器 140 中记录获得的硬件标识符。

现参考图 3，示出进入休眠状态的方法的实施例。计算设备 100 能响应于

休眠事件执行该方法。例如若设备和/或操作系统检测到一个设备在一段定长时
间内保持空闲，响应于此以产生休眠事件。响应于该休眠事件，在块 300 中操
作系统 208 确定是否当前建立 SE 环境 200。响应于确定没有建立 SE 环境，在
块 302 中计算设备 100 能调用休眠进入过程（下面详述），将计算设备 100 置
于所请求的休眠状态。

响应于确定建立 SE 环境 200 的请求，在块 304 中监视程序 202 能对 SE 存
储器 122 的内容加密和加证明。在一实施例中，监视程序 202 使用监视程序密
钥 214 之一加密 SE 存储器 122 的页面，并用加密的页面替代那些页面。监视
程序 202 能保留包含监视程序 202 的 SE 存储器的部分或含有监视程序 202 的
休眠逻辑的 SE 存储器的部分而不加密，使得处理器 102 能继续执行休眠逻辑
212。

在块 304 中，监视程序 202 还加证明到 SE 存储器 122 的内容。在一实施
例中，监视程序 202 能通过将 SE 存储器 122 的加密的内容求散列值以获取存
储器散列值，来产生内容的证明。在另外实施例中，监视程序 202 能通过只对
在唤醒过程之后保留在 SE 存储器 122 的页面求散列来产生内容的证明。例如，
唤醒过程能从非易失存储器 114 重新加载监视程序 202 和/或其他代码。因为
SE 存储器 122 的这些部分被重新加载，计算设备 100 能在进入休眠状态之前从
系统存储器 108 擦除这些部分，和/或不将它们存入非易失存储器 114。在另外
实施例中，监视程序 202 能通过嵌入内容证明到 SE 存储器 122 经证实的内容
中，来加证明到 SE 存储器 122 的内容，所述内容证明包括例如水印、签名、
和/或其它信息。

在块 306，监视程序 202 能产生和加证明到数据结构（如页面表、页面列
表、区列表等）以标识在块 304 中加密的系统存储器 122 的页面/段/区域。
在一实施例中，监视程序 202 能通过对数据结构求散列以获得数据结构散列，
来产生数据结构证明。在另外实施例中，监视程序 202 能通过在被加证明的数
据结构中嵌入数据结构证明（如水印、签名、和/或其他信息）对数据结构加证
明。

在块 308 中，监视程序 202 能密封内容证明、数据结构证明、和/或监视程
序密钥 214，以保护它们免受未经授权的访问和/或更改。在一实施例中，监视
程序 202 通过一个或多个权标 110 的密封操作密封内容证明、数据结构证明和
监视程序密钥 214，以获取一个或多个密封的重续对象。在一实施例中，密封
操作使用包含监视程序 202 的规格的 PCR 寄存器 140，以有效地防止如诈骗监
视程序那样的另外监视程序访问和/或更改密封的重续对象的非加密的内容。

在块 310 中，监视程序 202 卸除 SE 环境 200。监视程序 202 能完成作为
卸除过程的部分的各种操作。在一实施例中，监视程序 202 更新秘密存储器 126，
以表明系统存储器 108 不包含未加密的秘密。例如，监视程序 208 能清除秘密

存储器 126 的标志，以表明系统存储器 108 不包含未加密的秘密。此外，监视程序 202 能关闭可信的虚拟机 206 并能退出 VMX 处理器方式。监视程序 202 还能擦除在唤醒过程中将要从非易失存储器 114 重新加载的系统存储器 108 的那些区域。

在块 312 中，计算设备 100 能停止监视程序 202 的执行，并回到操作系统 208 的执行。在一实施例中，作为返回到操作系统 208 的结果，监视程序 202 提供 SE 环境重续信息给操作系统 208，SE 环境重续信息标识响应被密封的重续对象的唤醒和其定位和大小拟执行的监控器 202 的位置和大小。然而，计算设备 100 能利用其他机制使操作系统 208 能在唤醒过程中检索监视程序 202 和密封的重续对象。例如，监视程序 202 和/或密封的重续对象能储存在预定位置或由 BIOS 144 设置的位置。

在块 314，操作系统 208 能保存重续信息，使得它能成为唤醒过程的一部分而被检索。操作系统 208 能在系统存储器 108 的预定位置、由 BIOS 144 设置的位置、芯片组 104 的非易失寄存器、和/或其他位置存储 SE 环境恢复信息。在一实施例中，监视程序 202 在块 312 中将信息储存在合适的位置处，从而使操作系统 208 不必在块 314 保存该信息。

操作系统 208 和/或 BIOS 144 在块 302 中能完成休眠进入过程。例如，操作系统 208 和/或 BIOS 144 能将休眠类型标识符号写入休眠类型存储器 132，以表明计算设备 100 进入哪个休眠状态，且能更新休眠使能存储器 134，以调用进入该休眠状态的入口。在一实施例中，操作系统 208 和/或 BIOS 144 能使计算设备 100 进入不同于所请求的休眠状态的休眠状态。操作系统 208 和/或 BIOS 144 能为了各种理由选择改变休眠状态，例如由于计算设备 100 的一个或多个组件不支持所请求的休眠状态。响应于更新休眠类型存储器 132 和休眠使能存储器 134，休眠控制器 130 能使计算设备 100 进入休眠状态，并能完成休眠过程。例如，休眠控制器 130 能切断计算设备 100 的组件和/或子组件电源，能要求组件和/或子组件进入低能耗操作模式，和/或能将系统存储器 108 的内容写入非易失存储器 114。

现参考图 4，示出从休眠状态唤醒的方法。计算设备 100 能响应唤醒事件执行唤醒方法。能响应各种激励源产生唤醒事件，如调制解调器检测振铃事件，网络控制器检测网络活动，键盘控制器检测键按下等。响应唤醒事件，在块 400 休眠控制器 130 能完成一个或多个唤醒操作，例如唤醒处理器 102 和将保存的状态信息从非易失存储器 114 传输到系统存储器 108。在一实施例中，休眠控制器 130 能响应于执行 BIOS 144 的 ASL 和/或其他代码，完成一个或多个唤醒操作。在完成唤醒操作之后，休眠控制器 130 能将控制转移给操作系统 208。在一实施例中，休眠逻辑 212 从由唤醒矢量标识的位置调用操作系统 208 的执行。

在块 402 中，操作系统 208 能完成一个或多个唤醒操作，如唤醒网络控制器、调制解调器、和/或计算设备 100 的其他设备。在块 404，操作系统 208 判断是否根据储存的重续信息和/或在缺少储存的重续信息情况下恢复 SE 环境 200。响应于确定恢复 SE 环境 200，操作系统 208 完成各种操作。例如，操作系统 208 能加载、认证、和起动执行配置计算设备 100 和/或验证计算设备 100 的配置的 AC 模块。此外，在块 406，操作系统 208 能加载和调用重续信息标识的监视程序 202 的执行。

在块 408，监视程序 202 能通过权标 110 的一个或多个解密封操作，解密封被密封的重续对象，以获得内容的证明、数据结构的证明、和监视程序密钥 214。响应于检测到解密封操作失败（块 410），在块 412 中监视程序 202 调用休眠攻击响应，以解决可能的休眠攻击。在一实施例中，监视程序 202 通过写到芯片线 104 的复位寄存器调用系统复位，来调用休眠攻击响应。然而，监视程序 202 能以其他方式作出响应，例如，暂停处理器 102，擦除系统存储器 108，调用系统关闭，切断计算设备 100 电源，和/或保护秘密免受未授权的访问和/或更改的其他活动。

在块 414，监视程序 202 根据数据结构的证明验证数据结构的可靠性。在一实施例中，监视程序 202 求数据结构的散列，以获得计算的数据结构的证明。监视程序 202 还将计算的数据结构与从密封的重续对象获得的数据结构证明进行比较，并响应于具有对未密封的证明的预定关系（如相等）计算的证明，来确定该数据结构是可靠的。响应于确定该数据结构是不可靠的或被更改的，在块 412 监视程序 202 调用休眠攻击响应以解决可能的休眠攻击。

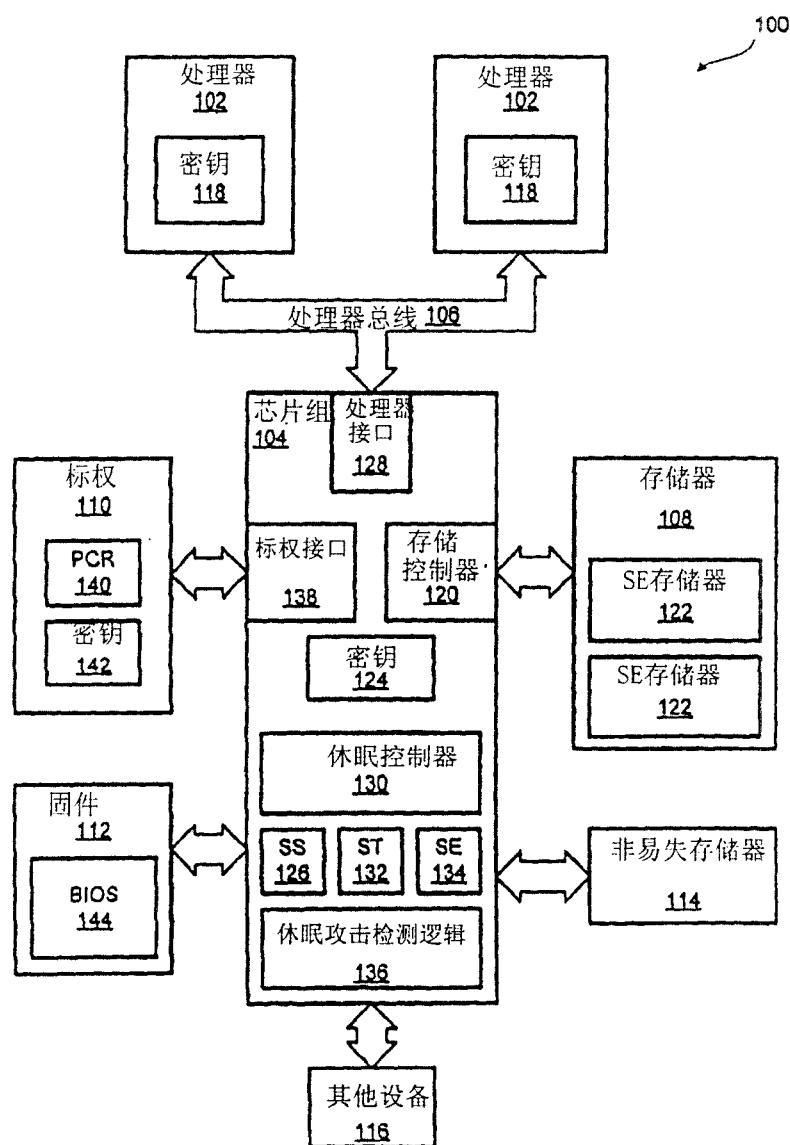
在块 416，监视程序 202 能解密系统存储器 108 的一部分，并将解密的部分存储在 SE 存储器 122 中。监视程序 202 能使用一个或多个未密封的监视程序密钥 214，解密由数据结构标识的系统存储器 108 的诸部分。在块 418，监视程序 202 能验证加密的或解密的 SE 存储器内容的可靠性。在一实施例中，监视程序 202 能对加到 SE 存储器 122 的解密内容求散列，以获得计算的内容证明。在另外实施例中，监视程序 202 能对拟加到 SE 存储器 122 的加密内容求散列，以获得计算的内容证明。监视程序 202 还能将计算的内容证明与未密封的内容证明进行比较，并能响应于具有对未密封的证明的预定关系（如相等）的计算的证明，确定该内容是可靠的（如未更改）。响应于确定该内容是不可靠的（如已更改），在块 412 监视程序 202 能对可能的休眠攻击调用攻击响应。相反，响应于制定该内容是可靠的，监视程序 202 通过调用操作系统 208 的执行完成唤醒过程。

休眠和唤醒方法的上述实施例帮助保护秘密免受攻击。然而，攻击者能试图绕过图 3 的休眠方法，将计算设备 100 置于休眠状态，在该休眠状态中，未加密的秘密驻留在系统存储器 108 和/或未保护的非易失存储器 114 中。为防止

这种绕过，休眠攻击检测逻辑 136 能调用系统复位事件或另外的攻击响应，以响应检测到可能的休眠攻击。在图 3 的休眠方法的一实施例中，监视程序 202 更新秘密存储器 126，以表明在更新休眠使能存储器 134 到起动休眠进入过程之前，系统存储器 108 未包含未加密的秘密。因而，若秘密存储器 420 表明系统存储器 108 能包含未加密的秘密，则休眠攻击检测逻辑 136 能调用休眠攻击响应，以响应休眠使能存储器 134 被更新。

在图 3 的休眠方法的另外实施例中，仅当请求的休眠状态导致 SE 存储器 122 未被保护时，监视程序 202 加密 SE 存储器 122 并更新秘密存储器 126，以表明该系统存储器 108 未包含未加密的秘密。因此，若秘密存储器 420 表明系统存储器 108 可能包含未加密的秘密，且休眠类型存储器 132 表明处在 SE 存储器 122 映射中的休眠状态未被保护时，休眠攻击检测逻辑 136 能调用休眠攻击响应，以响应休眠使能存储器 134 被更新。

虽然参考示例实施例描述了本发明的某些特征，但上述描述并不是在限制的意义上解释。对与本发明有关的专业技术人员显而易见的本发明的示例及其他实施例的各种修改，都被认为是在本发明的精神和范围之内。



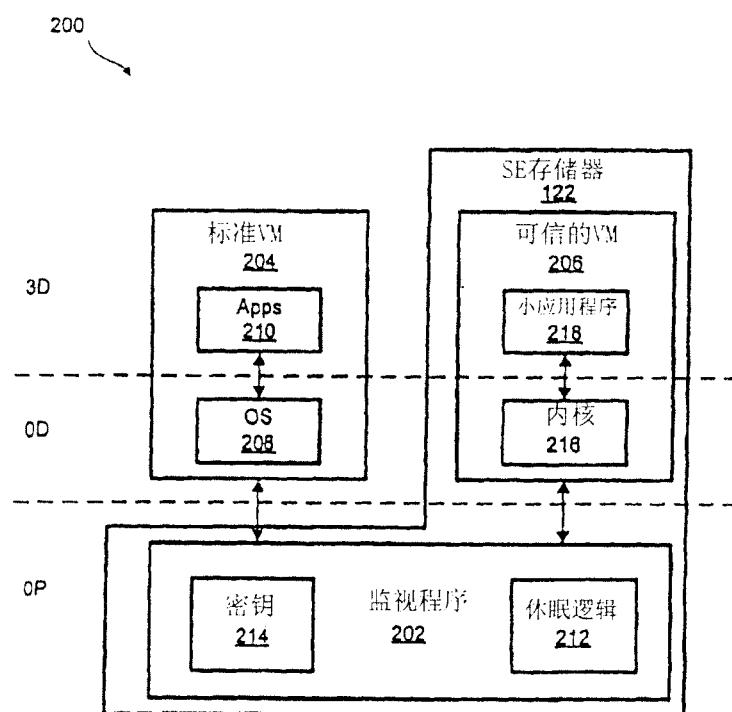


图 2

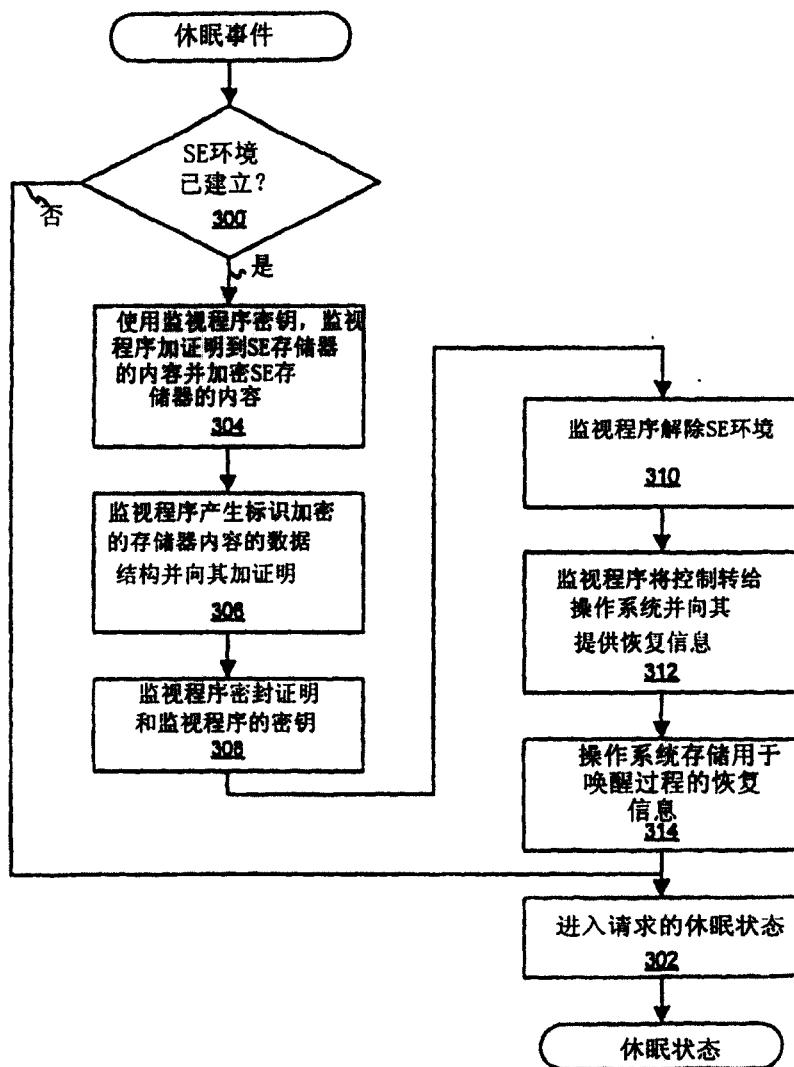


图 3

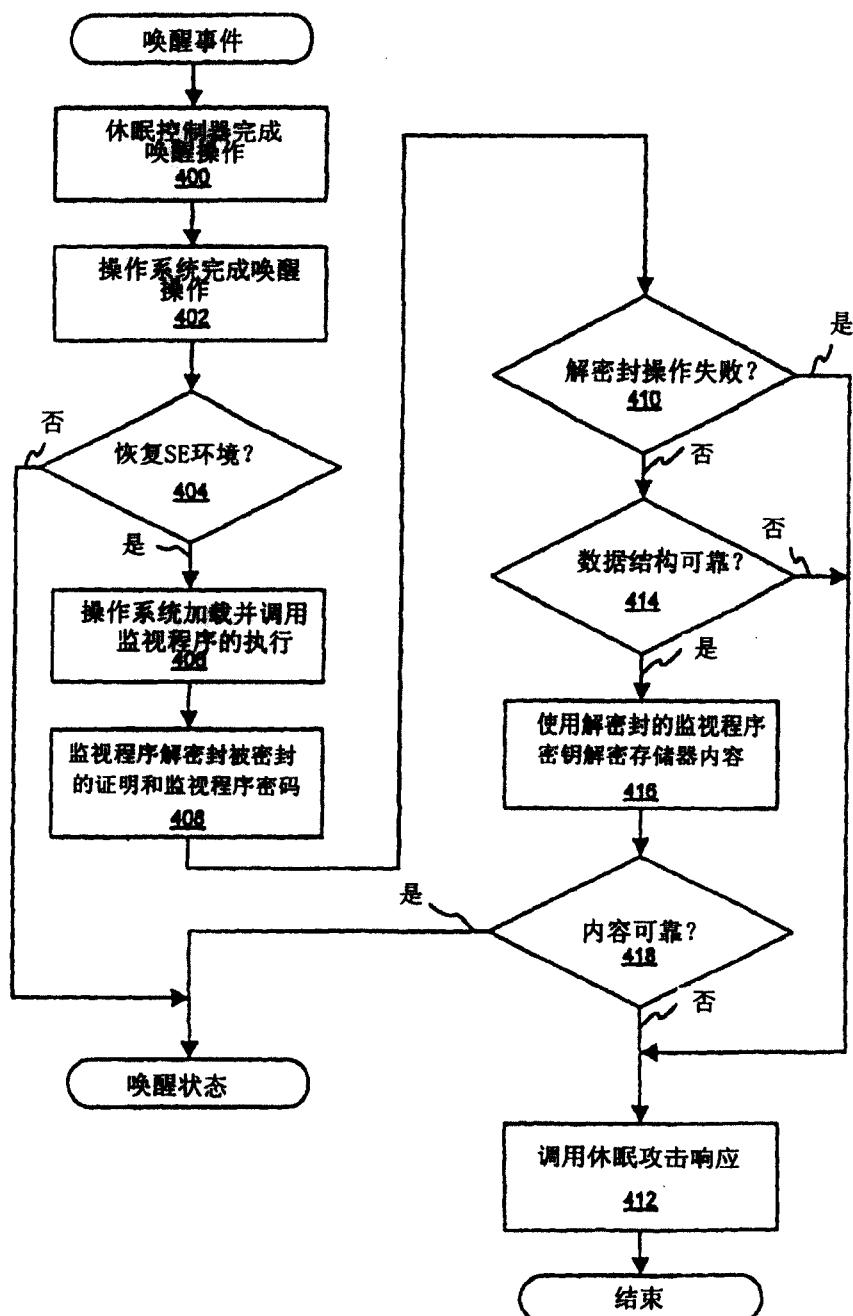


图 4