



## [12] 发明专利说明书

专利号 ZL 200410011932.2

[45] 授权公告日 2009 年 6 月 3 日

[11] 授权公告号 CN 100495364C

[22] 申请日 2004.9.21

[21] 申请号 200410011932.2

[30] 优先权

[32] 2003.11.25 [33] US [31] 10/721,562

[73] 专利权人 微软公司

地址 美国华盛顿州

[72] 发明人 B·A·雷斯 D·B·克罗斯

D·G·布莱斯 顾建荣

R·Y·那加 S·A·菲尔德

[56] 参考文献

CN1445680A 2003.10.1

US5825878A 1998.10.20

US2002/0099946A1 2002.7.25

审查员 毛习文

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 陈斌

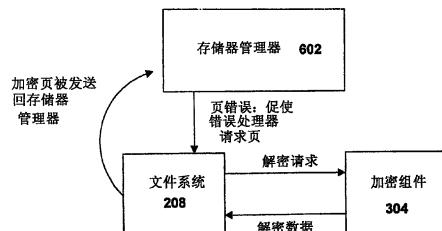
权利要求书 3 页 说明书 9 页 附图 6 页

[54] 发明名称

系统分页文件的加密

[57] 摘要

操作系统将数据从存储器页复制到盘上的分页文件，以释放存储器中的空间。揭示了一种机制，它促使该数据在被复制到分页文件时被加密，由此保护了该分页数据免遭非授权(或非期望)的观察。储存在分页文件中的数据使用会话密钥来加密，会话密钥在分页文件所在的机器启动短暂之后创建。会话密钥用于分页文件数据的加密和解密，储存在易失存储器中，使得该密钥不跨机器的启动被持久保存。由于密钥不跨启动被持久保存，在最近一次启动之前储存的旧分页文件不能被恢复成明文，由此保护了数据免遭观察。



1. 一种提供计算环境的系统，所述环境包括虚拟存储器，其特征在于，所述系统包括：

一虚拟存储器管理器，它通过在易失存储器和储存在硬盘上的分页文件之间移动或复制数据来提供所述虚拟存储器，所述系统通过加密储存在所述分页文件上的数据来保护所述虚拟存储器的内容；以及

一生成会话密钥的密钥生成器，所述会话密钥用于加密所述数据，并且所述会话密钥还要用于随后的加密数据的解密，其中所述会话密钥是以如果在所述会话密钥生成之后出现启动则促使所述密钥变得不可用的方式非持久储存的；

其中，在生成所述会话密钥之前，一存储器块被保留，所述存储器块用作以下任一：

在维护所述分页文件的文件系统和使用所述会话密钥执行所述数据的加密和解密的加密组件之间传递数据的缓存；以及

由加密组件在生成所述会话密钥之前使用的工作空间。

2. 如权利要求 1 所述的系统，其特征在于，所述虚拟存储器管理器向一文件系统传递所述数据，其中，所述文件系统使所述数据在储存到所述分页文件中之前被加密。

3. 如权利要求 2 所述的系统，其特征在于，所述文件系统将所述分页文件标记为加密，并且其中，所述分页文件在接收将所述数据储存在所述分页文件中的请求之后，确定所述分页文件被标记为加密，并与一加密组件进行通信来加密所述数据。

4. 如权利要求 1 所述的系统，其特征在于，所述系统还通过确保没有所述会话密钥的持久存储来保护所述虚拟存储器的内容。

5. 如权利要求 1 所述的系统，其特征在于，所述数据的加密依照以下算法的一个或多个来执行：

数据加密标准 DES；

三重 DES3DES；或

高级加密标准 AES。

6. 如权利要求 1 所述的系统，其特征在于，所述系统还通过确保当储存在所

述分页文件中时，储存在所述虚拟存储器中的所有用户模式应用程序和数据都被加密，来保护所述虚拟存储器的内容。

7. 一种保护虚拟存储器的方法，其特征在于，它包括：

在易失存储器的多个页中储存数据；

确定将所述多个页中的第一个的内容从所述易失存储器移动到一储存在盘上的分页文件；

用将所述内容储存到分页文件中的指令将所述内容提供给一文件系统，所述分页文件被标记为要加密，所述文件系统促使所述内容使用一密钥来加密，再将所述内容储存在所述分页文件中，需要所述密钥来解密包含在所述分页文件中的信息，所述密钥被以储存所述密钥的机器的重起将导致所述密钥丢失的方式储存；

在生成所述密钥之前，保留所述虚拟存储器的一个块用作工作空间，其中，所述工作空间的使用避免了在生成所述会话密钥之前将虚拟存储器内容复制到盘的需求。

8. 如权利要求 7 所述的方法，其特征在于，它还包括：

在所述机器的启动之后生成所述密钥。

9. 如权利要求 7 所述的方法，其特征在于，所述文件系统促使所述内容通过与一加密组件进行通信来加密，所述加密组件加密由所述文件系统标记为加密的文件。

10. 如权利要求 9 所述的方法，其特征在于，它还包括：

保留所述虚拟存储器的一个块，可在其中将数据在所述文件系统和所述加密组件之间来回传递。

11. 一种维护为计算机储存虚拟存储器数据的加密分页文件的系统，其特征在于，所述系统包括：

一加密组件，它接收数据并使用一密钥在所述数据上执行加密和解密；

一生成所述密钥的机制；

一所述计算机中的存储位置，它以促使所述密钥不跨越所述计算机的启动被持久保存的方式储存所述密钥；以及

一虚拟存储器管理器，它通过请求一文件系统在一一分页文件中储存复制或移动的数据，将数据从易失存储器复制或移动到盘，所述文件系统访问所述加密组件以使用所述密钥加密所复制或移动的数据；

其中所述加密组件在启动后保留一存储器块，所述存储器块用作所述加密组件生成所述密钥之前的工作空间，由此，在生成所述密钥之前在所述易失存储器中存在用于储存所述加密组件的操作数据的足够空间。

12. 如权利要求 11 所述的系统，其特征在于，所述存储器块用作在所述文件系统和所述加密组件之间来回传递信息的缓存。

13. 如权利要求 11 所述的系统，其特征在于，所述密钥在所述虚拟存储器将所述数据的存储定向到所述分页文件之前生成。

14. 如权利要求 11 所述的系统，其特征在于，所述密钥储存在所述易失存储器中，并且其中，没有所述密钥的副本储存在所述计算机的任一非易失存储器或存储设备中。

15. 一种在计算机启动后发生的方法，其特征在于，所述方法包括：  
生成一会话密钥；  
以不会跨越机器启动继续存在的非持久方式储存所述会话密钥；  
检索指示储存在盘上的虚拟存储器数据要被加密的信息；  
将一分页文件标记为加密文件；  
从一存储器管理器接收要储存在盘上的所述分页文件中的来自易失存储设备的数据；

通过在将所述数据储存到所述分页文件之前使用一会话密钥加密所接收的数据，来保护所接收的数据免遭观察；以及

在生成所述会话密钥之前保留一存储器块，其中，所述存储器块用作以下任一：

在维护所述分页文件的文件系统和使用所述会话密钥执行所述数据的加密和解密的加密组件之间传递数据的缓存；以及

由加密组件在生成所述会话密钥之前使用的工作空间。

16. 如权利要求 15 所述的方法，其特征在于，所述会话密钥储存在所述易失存储设备中，并且没有所述会话密钥的副本储存在盘上。

## 系统分页文件的加密

### 技术领域

本发明一般涉及计算文件，尤其涉及用于加密和解密虚拟存储器分页文件的机制。

### 背景技术

现代计算机系统通常提供虚拟存储器工具以提供超过物理随机存取存储器（RAM）的大小的可用存储器容量。虚拟存储器系统提供了一虚拟地址空间，它可以大于物理地址空间。为防止虚拟存储器溢出物理地址空间的内容，当需要物理存储器中的更多空间时从物理存储器中复制出页，而当程序需要访问这些页时，将页复制回物理存储器中。当页被从物理存储器复制出时，页的内容被储存在盘上的文件中，称为“分页文件”。

在盘上储存存储器页映象—即使是临时的—的一个问题是很难保护这些页的内容免遭未授权观察。物理存储器一般是易失存储器，如果移除了系统的电源，则其内容丢失。因此，可以保证，如果系统被切断电源、崩溃或重新启动，储存在易失存储器中的任何机密数据都不能被未授权观察者恢复。然而，如果来自易失存储器的数据被复制到分页文件，则该数据可由对盘具有访问权限的任何人观察，并且在断开电源事件、崩溃或重启之后，该数据仍在盘上存在。如果该数据是机密的或敏感的，该可能性造成了一个安全风险，因为攻击者可从盘获取这一数据。

鉴于上述内容，需要一种克服现有技术的缺点的机制来保护分页文件。

### 发明内容

本发明通过加密储存于分页文件中的数据保护了分页文件。依照本发明，分页文件被标记来用于加密。分页文件储存在具有文件加密工具的文件系统中。提供文件加密的文件系统在美国专利号 6,249,866 中描述，该专利通过引用结合于此。当虚拟存储器管理器向文件系统传递要储存在分页文件中的数据时，文件系统看见该分页文件被标记用于加密，并促使在分页文件中储存数据之前加密该数据。文件

系统可与加密组件进行通信以执行实际的加密。加密组件从文件系统接收明文、应用加密密钥来创建密文、并将密文传回文件系统以储存在分页文件中。

现有文件加密系统一般加密文件，并也持久保存解密该文件所需的密钥的副本。持久密钥存储在普通文件的情况下是有意义的，因为这些文件用于长期储存，并通常需要能够在机器的多次启动后还可解密这些文件。分页文件不同于普通文件：分页文件是仅在计算环境的单个例示（如介于机器的启动之间）的上下文中有意义的数据的临时储存库。由此，分页文件数据在系统被重起之后几乎没有价值，并且以可使用的形式储存这一数据就其造成安全风险的意义而言是一种缺点。由此持久保存解密分页文件数据所需要的密钥可能是危险的，因为这样做会允许数据—包括机密或敏感数据—在某一不可预测的上下文环境中（如在硬盘被从其预期的机器上移除并被安装到黑客的机器上之后）解密。依照本发明的一个特征，每次启动生成一个会话密钥，并且该会话密钥用于仅在系统的单次运行中（如在启动和关闭之间）加密和解密分页文件的内容。该会话密钥不跨越机器的多次启动被持久保存。

由于可能在启动后的任何时刻必须将物理存储器的页复制到分页文件，较佳地在机器启动十分短暂之后生成该会话密钥，以确保该密钥准备好服务写分页文件的任一请求。较佳地，生成密钥的组件在启动十分短暂之后保存了物理存储器的一个块。该保存的存储器可用作加密组件用于加密以分页文件为目标的数据的工作空间，和/或在文件系统和加密组件之间传递数据的缓存。

下文描述了本发明的其它特征。

#### 附图说明

当结合附图阅读时，可以更好地理解决述，以及以下较佳实施例的详细描述。为说明本发明的目的，附图中示出了本发明的示例性构造；然而，本发明并不局限于所揭示的具体方法和手段。附图中：

图 1 是可在其中实现本发明的各方面的示例计算环境的框图；

图 2 计算机存储器及其与文件系统的关系的框图；

图 3 是加密文件的机制的框图；

图 4 是为分页文件加密准备系统的过程的流程图；

图 5 是用于加密要储存在分页文件中的存储器数据的过程的流程图；

图 6 是从加密分页文件检索页的存储器管理器的框图。

## 具体实施方式

### 综述

虚拟存储器管理器提供了大于机器的物理易失存储器的虚拟地址空间。虚拟存储器管理器通过在需要时将数据复制到和复制出易失存储器来执行这一任务。当将数据从易失存储器复制出时，该数据储存在盘上的分页文件中。本发明提供了一种机制，其中，通过以加密形式储存分页文件数据，储存在分页文件中的数据可被保护以免遭非授权的观察。

### 示例计算布置

图 1 示出了适合在其中实现本发明的各方面的示例性计算环境 100。计算系统环境 100 仅为合适的计算环境的一个示例，并非建议对本发明的使用或功能的范围的局限。也不应将计算环境 100 解释为对示例性操作环境 100 中示出的任一组件或其组合具有依赖或需求。

本发明可以使用众多其它通用或专用计算系统环境或配置来操作。适合使用本发明的众所周知的计算系统、环境和/或配置包括但不限于：个人计算机、服务器计算机、手持式或膝上设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费者电子设备、网络 PC、小型机、大型机、包括任一上述系统或设备的分布式计算环境等等。

本发明可在计算机可执行指令的一般上下文环境中描述，计算机可执行指令如由计算机执行的程序模块。一般而言，程序模块包括例程、程序、对象、组件、数据结构等等，执行特定的任务或实现特定的抽象数据类型。本发明也可以在分布式计算环境中实践，其中，任务由通过通信网络或其它数据传输机制连接的远程处理设备来执行。在分布式计算环境中，程序模块和其它数据可以位于本地和远程计算机存储媒质中，包括存储器存储设备。

参考图 1，用于实现本发明的示例性系统包括以计算机 110 形式的通用计算装置。计算机 110 的组件可包括但不限于，处理单元 120、系统存储器 130 以及将包括系统存储器的各类系统组件耦合至处理单元 120 的系统总线 121。处理单元 120 代表多个逻辑处理单元，如多线程处理器所支持的。系统总线 121 可以是若干种总线结构类型的任一种，包括存储器总线或存储器控制器、外围总线以及使用各类总

线体系统结构的局部总线。作为示例而非局限，这类体系结构包括工业标准体系结构 (ISA) 总线、微通道体系结构 (MCA) 总线、增强 ISA (EISA) 总线、视频电子技术标准协会 (VESA) 局部总线以及外围部件互连 (PCI) 总线（也称为 Mezzanine 总线）。系统总线 121 也可以被实现为点对点连接、交换结构等通信设备。

计算机 110 通常包括各种计算机可读媒质。计算机可读媒质可以是可由计算机 110 访问的任一可用媒质，包括易失和非易失媒质、可移动和不可移动媒质。作为示例而非局限，计算机可读媒质包括计算机存储媒质和通信媒质。计算机存储媒质包括以用于储存信息的任一方法或技术实现的易失和非易失，可移动和不可移动媒质，信息如计算机可读指令、数据结构、程序模块或其它数据。计算机存储媒质包括但不限于，RAM、ROM、EEPROM、闪存或其它存储器技术、CDROM、数字多功能盘 (DVD) 或其它光盘存储、磁盒、磁带、磁盘存储或其它磁存储设备、或可以用来储存所期望的信息并可由计算机 110 访问的任一其它媒质。通信媒质通常在诸如载波或其它传输机制的已调制数据信号中包含计算机可读指令、数据结构、程序模块或其它数据，并包括任一信息传送媒质。术语“已调制数据信号”指以对信号中的信息进行编码的方式设置或改变其一个或多个特征的信号。作为示例而非局限，通信媒质包括有线媒质，如有线网络或直接连线连接，以及无线媒质，如声学、RF、红外和其它无线媒质。上述任一的组合也应当包括在计算机可读媒质的范围之内。

系统存储器 130 包括以易失和/或非易失存储器形式的计算机存储媒质，如只读存储器 (ROM) 131 和随机存取存储器 (RAM) 132。基本输入/输出系统 133 (BIOS) 包括如在启动时帮助在计算机 110 内的元件之间传输信息的基本例程，通常储存在 ROM 131 中。RAM 132 通常包含处理单元 120 立即可访问或者当前正在操作的数据和/或程序模块。作为示例而非局限，图 1 示出了操作系统 134、应用程序 135、其它程序模块 136 和程序数据 137。

计算机 110 也可包括其它可移动/不可移动、易失/非易失计算机存储媒质。仅作示例，图 1 示出了对不可移动、非易失磁媒质进行读写的硬盘驱动器 141、对可移动、非易失磁盘 152 进行读写的磁盘驱动器 151 以及对可移动、非易失光盘 156，如 CD ROM 或其它光媒质进行读写的光盘驱动器 155。可以在示例性操作环境中使用的其它可移动/不可移动、易失/非易失计算机存储媒质包括但不限于，磁带盒、闪存卡、数字多功能盘、数字视频带、固态 RAM、固态 ROM 等等。硬盘驱动器

141 通常通过不可移动存储器接口，如接口 140 连接到系统总线 121，磁盘驱动器 151 和光盘驱动器 155 通常通过可移动存储器接口，如接口 150 连接到系统总线 121。

图 1 讨论并示出的驱动器及其关联的计算机存储媒质为计算机 110 提供了计算机可读指令、数据结构、程序模块和其它数据的存储。例如，在图 1 中，示出硬盘驱动器 141 储存操作系统 144、应用程序 145、其它程序模块 146 和程序数据 147。注意，这些组件可以与操作系统 134、应用程序 135、其它程序模块 136 和程序数据 137 相同，也可以与它们不同。这里对操作系统 144、应用程序 145、其它程序模块 146 和程序数据 147 给予不同的标号来说明至少它们是不同的副本。用户可以通过输入设备，如键盘 162 和定位设备 161（通常指鼠标、跟踪球或触摸板）向计算机 110 输入命令和信息。其它输入设备（未示出）可包括麦克风、操纵杆、游戏垫、圆盘式卫星天线、扫描仪等等。这些和其它输入设备通常通过耦合至系统总线的用户输入接口 160 连接至处理单元 120，但是也可以通过其它接口和总线结构连接，如并行端口、游戏端口或通用串行总线（USB）。监视器 191 或其它类型的显示设备也通过接口，如视频接口 190 连接至系统总线 121。除监视器之外，计算机也包括其它外围输出设备，如扬声器 197 和打印机 196，通过输出外围接口 195 连接。

计算机 110 可以在使用到一个或多个远程计算机，如远程计算机 180 的逻辑连接的网络化环境中操作。远程计算机 180 可以是个人计算机、服务器、路由器、网络 PC、对等设备或其它公用网络节点，并通常包括许多或所有上述与计算机 110 相关的元件，尽管在图 1 中仅示出了存储器存储设备 180。图 1 描述的逻辑连接包括局域网（LAN）171 和广域网（WAN）173，但也可包括其它网络。这类网络环境常见于办公室、企业范围计算机网络、内联网以及因特网。

当在 LAN 网络环境中使用时，计算机 110 通过网络接口或适配器 170 连接至 LAN 171。当在 WAN 网络环境中使用时，计算机 110 可包括调制解调器 173 或其它装置，用于通过 WAN 173，如因特网建立通信。调制解调器 172 可以是内置或外置的，通过用户输入接口 160 或其它合适的机制连接至系统总线 121。作为示例而非局限，图 1 示出了远程应用程序 185 驻留在存储器设备 181 上。可以理解，示出的网络连接是示例性的，也可以使用在计算机之间建立通信的其它装置。

### 存储器页在分页文件中的存储

图 2 示出了计算机存储器以及可在其中储存存储器页的文件系统。计算机系统包括存储器，如 RAM 132。RAM 132 包括可被组织成页的若干字节的存储器。每一页是确定尺寸的存储字节的连续的块—例如，典型的系统可支持 4 千字节或 4 兆字节的页尺寸，或同时支持这两种尺寸。在图 2 的示例中，RAM 132 包含页 202(1)、202(2)、202(3)、202(4)、202(5)、…、202(n)。

文件系统 208 以文件的形式在盘上储存数据，并也包括组织文件（如，通过维护文件的目录）、执行文件的存储和检索并执行与文件维护相关的其它任务所需要的软件和/或硬件。在图 2 的示例中，文件系统 208 储存文件 204(1)、204(2)、…、204(m)。另外，文件系统 208 可储存一个或多个分页文件，如分页文件 206。分页文件 206 是用于储存来自盘的页的副本的文件。任一程序可维护分页文件，尽管最典型的是由操作系统（如图 1 所示的操作系统 134）维护分页文件为所有应用程序和进程所共享。在该示例中，分页文件 206 是由操作系统 134 维护的分页文件。MICROSOFT WINDOWS 操作系统是维护这一分页文件的操作系统的示例。当需要释放存储器空间时，操作系统 134 将存储器的页复制到分页文件 206 中。例如，操作系统 134 可决定通过将页 202(4)的内容复制到文件 206，然后重新分配页 202(4)的物理存储器用于储存其它数据，来释放 RAM 132 中的空间。相反，当操作系统 134 接收访问未储存在 RAM 132 中的数据的请求时，因为该数据位于先前复制到分页文件 206 的页上（如，当基于访问被标记为在虚拟地址翻译表中“不存在”的页的尝试而生成页错误异常时），操作系统 134 将被搜索的页的内容从分页文件 206 复制出来，并将其放入 RAM 132 的物理页帧中（并且同时调整地址翻译表以指向新的页位置）。

可由文件系统 208 提供的一个特征是文件加密组件，如图 3 所示。文件系统 208 储存多个文件（如，文件 204(1)、204(2)、204(3)），如结合图 2 先前所示出并讨论的。加密组件 304 展现使用密钥 302 加密并解密文件的功能。较佳地，文件系统 208 能以加密或明文的形式储存文件。在这一情况下，依照该文件是否以加密形式被维护，储存在文件系统 208 中的每一文件与可以被设置或未设置的标志相关联。在图 3 的示例中，标志 310（与文件 204(2)）关联被设置，指示文件 204(2)被加密。

加密组件 304 展现加密和解密文件的功能。由此，当文件系统 208 接收在文

件 204(2)（或其标志被标记为加密的任一其它文件）中储存数据的请求时，文件系统 208 调用加密组件 304，并将要储存的明文 306 传递到加密组件 304。加密组件 304 然后使用密钥 302 来加密明文 306，并将密文 308 传递回文件系统 208。密文 308 然后被储存在文件 204(2)中。如果文件系统 208 接收一从文件 204 (2)检索信息的请求，文件系统 208 将在那一时刻看到文件 204(2)被标记为加密，并且将加密的密文从该文件传递到加密组件 304。加密组件 304 然后使用密钥 302 解密该密文，并返回明文；文件系统 208 然后将明文传回请求者。在一个较佳的实施例中，加密组件 304 使用对称密钥算法，如数据加密标准（DES）、三重 DES（3DES）或高级加密标准（AES）来执行加密和解密。

在一个较佳的实施例中，加密组件 304 包括生成密钥 302 的功能，并且加密组件 304 向管理文件系统 208 的软件提供密钥 302。如以下结合图 4 所描述的，在系统启动之后即刻生成密钥 302，并且密钥不在非易失存储中持久保存。

较佳地，系统可具有确定是否应当设置或不设置加密标志来创建分页文件的本地或中央配置安全政策。例如，可以有指示是否要执行分页文件的加密的注册表条目。在启动后一当系统为给定的会话创建分页文件时一系统可检查注册表来确定是否要为该分页文件设置加密标志。

### 为分页文件加密的系统准备

图 4 是为分页文件加密准备系统的过程的流程图。最初，启动将在其中使用加密分页文件的系统（402）。在启动之后，保留存储器块用于某些使用（404）。具体地，保留的存储器块可具有以下用途：首先，某些保留的存储器可被用作可通过其在文件系统和加密组件之间来回写数据的缓存。（如果试图在文件系统和加密组件之间写数据，并且保存的存储器不够，则该写被分割成多个阶段，或者可试图分配更多的存储器。）第二，某些保留的存储器可用作加密组件的工作空间。

下一步，创建用于加密分页文件的会话密钥，并将其储存在不被分页到盘的易失存储器中等（406）。会话密钥较佳地不以跨越启动持久保存密钥的方式储存；由此，在一次启动中生成的加密分页文件数据无法超越当前会话被解密，由此保护了该数据的安全性。（例如，如果硬盘被从计算机系统中移除并被盗，则该硬盘不应当包含会话密钥的副本，该副本将允许当该硬盘被安装在另一机器上时分页文件数据被解密。）较佳地，会话密钥被储存在未分页存储器中，使得它最终不会被分

页到盘。（将密钥分页到盘不仅会产生安全问题，而且也可导致死锁，因为会需要该密钥来解密储存了该密钥的分页文件。）应当注意，尽管图 4 示出了在保留存储器块之后创建会话密钥，然而该序列并非本发明所需。

然后创建分页文件，设置该文件上的加密标志（408）。在这一点上，已为分页文件加密准备了系统。当存储器管理器在存储器和分页文件之间来回移动数据时，使用会话密钥来加密/解密该数据（410）。在存储器和加密分页文件之间移动数据的过程结合图 5 来更具体地描述。

图 5 示出了在分页文件中储存加密数据的过程。在系统的操作过程中的某一点上，存储器管理器确定储存在存储器中的数据将要被移动到盘（如，以释放存储器中的空间）。存储器管理器然后使用将内容写到分页文件的指令将存储器页的内容传递到文件系统（502）。文件系统然后检查分页文件上的加密标志是否被设置（504）。如果加密标志未设置，则将存储器管理器提供的数据作为明文写到分页文件（506）。

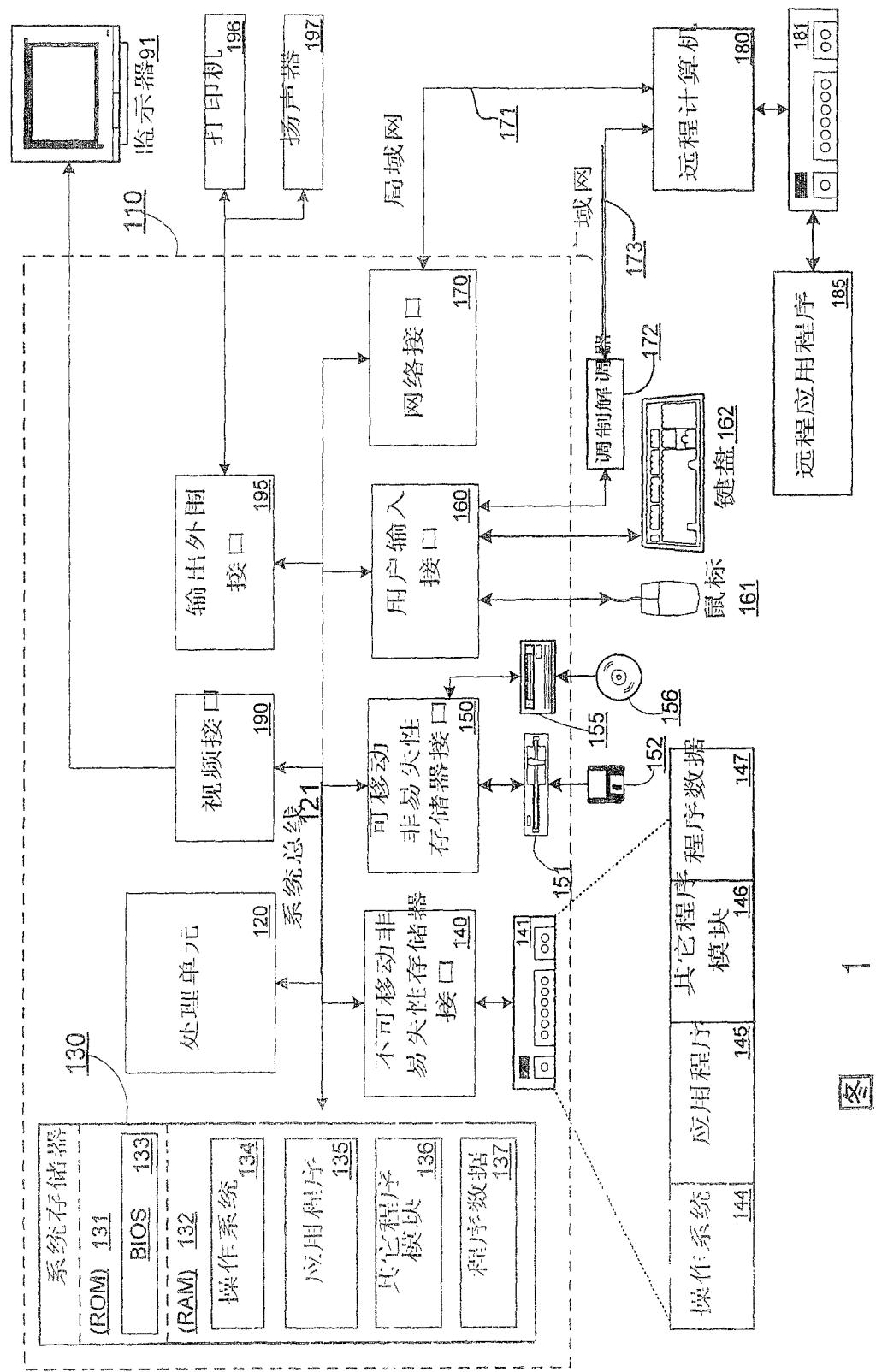
如果为分页文件设置了加密标志，则文件系统调用加密组件来加密该数据（508）。加密组件然后使用会话密钥来加密该数据（510），以生成密文。然后将密文传递回文件系统（512），并且文件系统将该密文储存在分页文件（514）中。应当注意，适用的对称加密算法（如，DES、3DES、AES 等等）通常是以定义大小的块加密数据的分组密码；由此，生成（并写入分页文件）的密文至少是加密算法所适用的块的大小。

从加密分页文件检索数据的过程类似于图 5 描述的储存过程：当从分页文件检索数据的请求从存储器管理器进入时，如果该分页文件被标记为加密，则文件系统向加密组件提供储存在分页文件中的密文，加密组件适用会话密钥解密该密文并返回明文。可执行该过程的示例系统在图 6 中示出。接收访问存储器的具体页的请求，并且储存器管理器确定（基于页映射）请求的页不在存储器中。页的不存在导致生成页错误。错误处理器作出文件访问请求以从分页文件检索请求的页。文件系统 208 接收该访问请求，并看到该分页文件被标记为加密。由此，文件系统 208 调用加密组件 304 以适用会话密钥解密所请求的页。加密组件 304 然后将解密的页传递回文件系统，文件系统将解密的页返回至存储器管理器 602。存储器管理器 602 然后将检索的页的内容储存到物理存储器页帧中，并调整页映射来反映页在物理存储器中的存在（以及新位置）。较佳地，加密和解密分页文件数据的过程对存储器

管理器是透明的，可在不考虑该数据是否被加密的情况下作出储存和检索数据的请求。

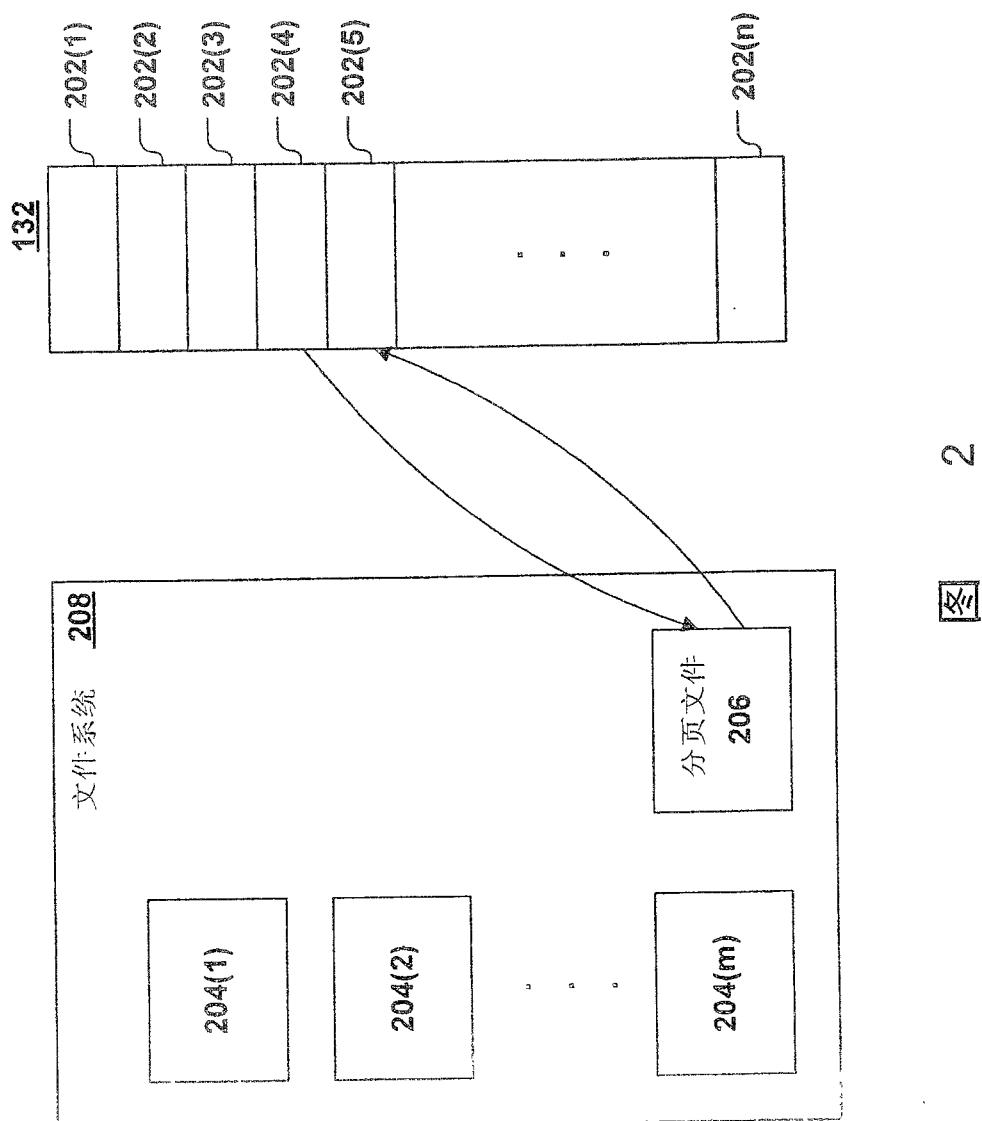
注意，上述示例仅为解释目的提供，并且不应被解释为对本发明的局限。尽管参考各种实施例描述了本发明，可以理解，此处所适用的词语是描述和说明性词语，而非限制性词语。此外，尽管此处参考具体的装置、材料和实施例描述了本发明，本发明并不意味着对此处所揭示的特殊性的限制；相反，本发明延及所有的功能等效结构、方法和用途，如处于所附权利要求书范围内的那些。从本说明书的教导受益的本领域的技术人员可在不脱离本发明的各方面的范围和精神的情况下对其作出各种修改和变化。

计算环境 100



图

1



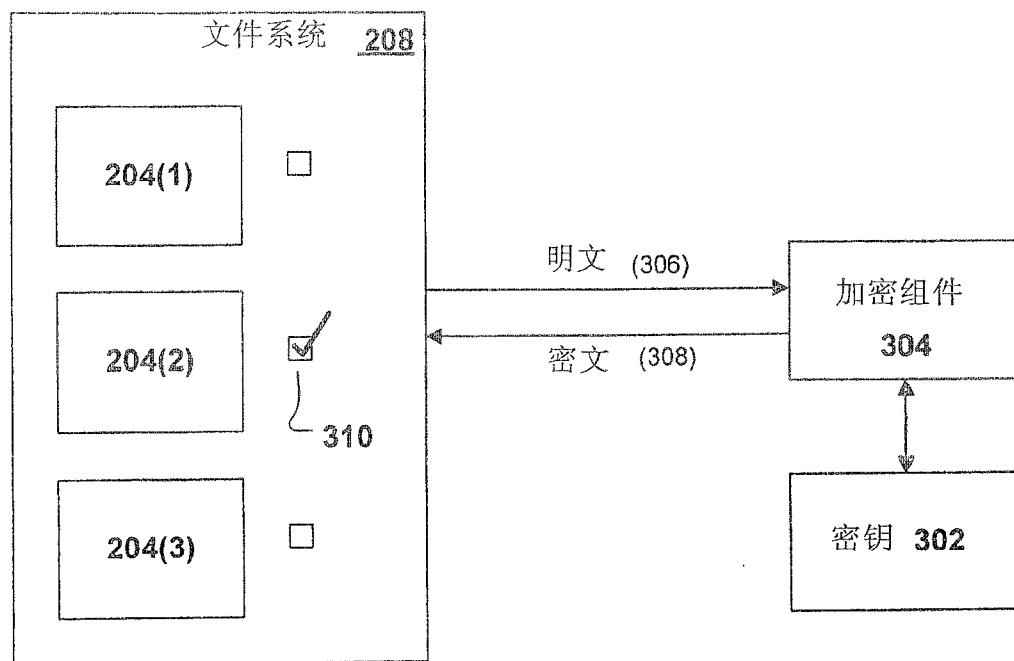


图 3

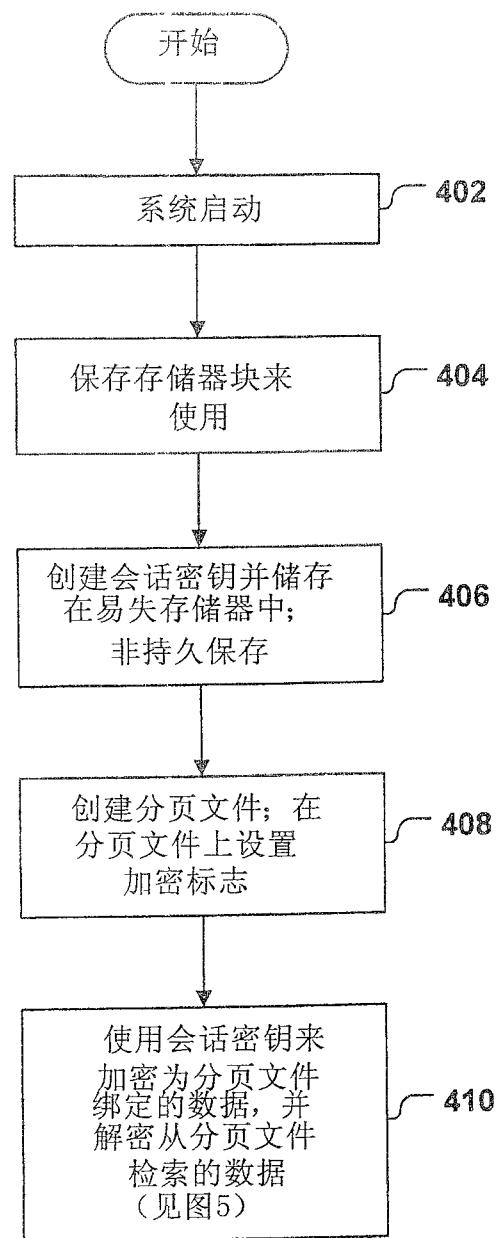
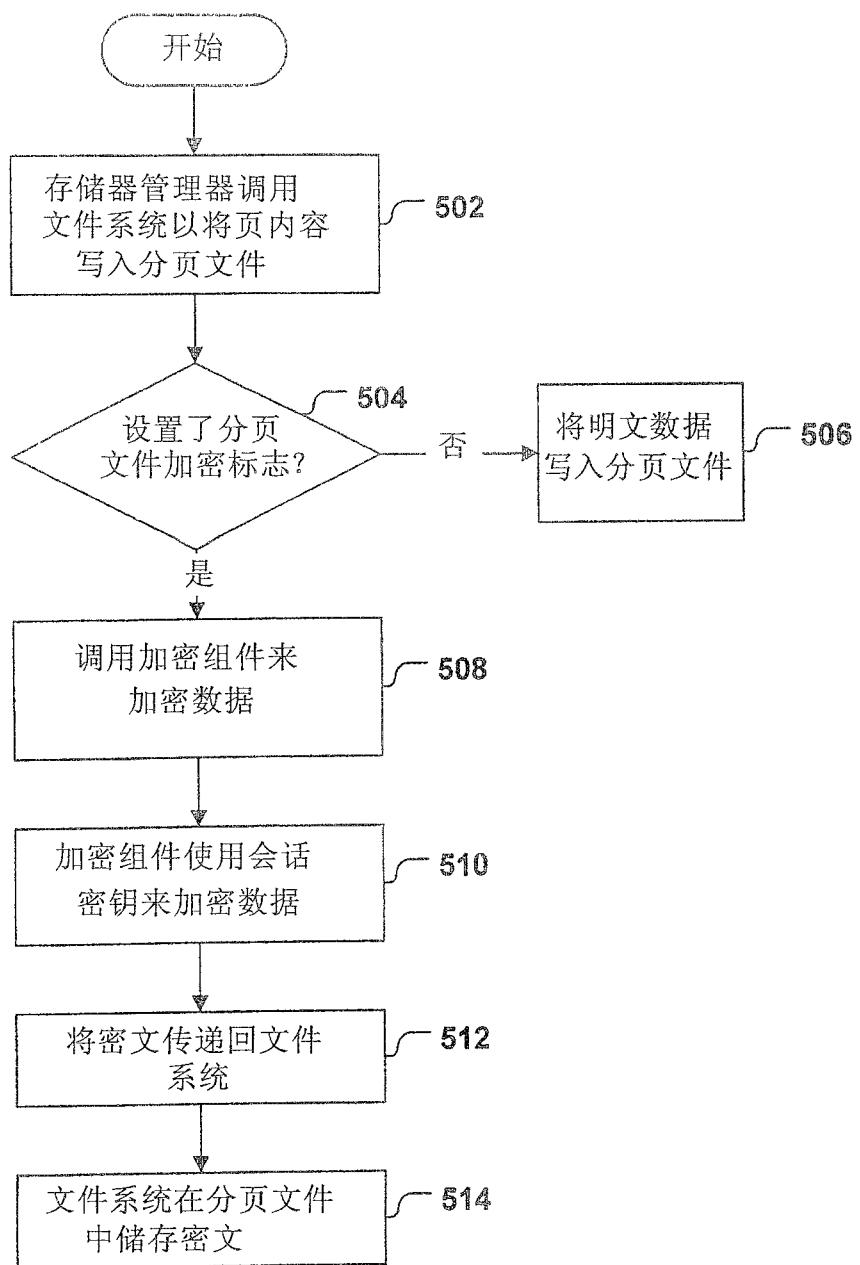
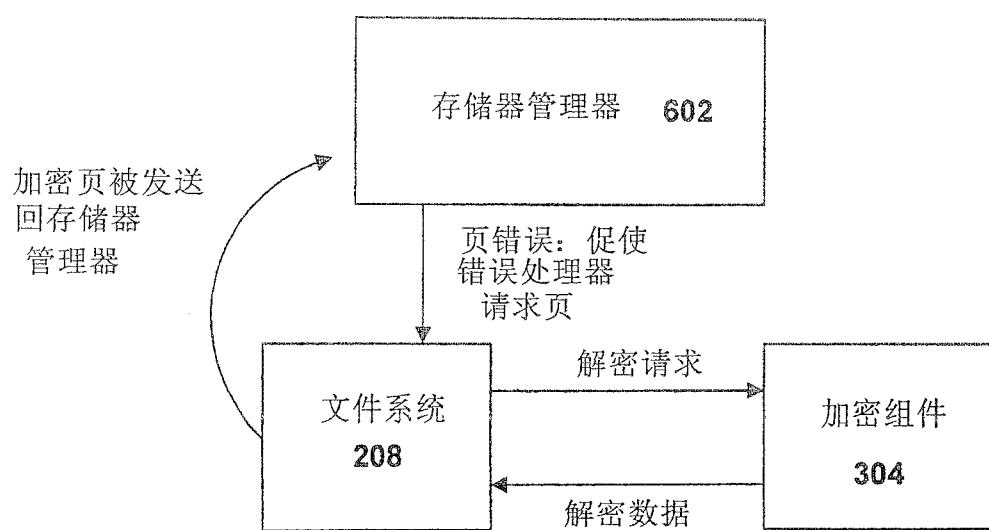


图 4





图

6