(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102150391 A
(43)申请公布日 2011.08.10

(21)申请号 200880129100.7

(22)申请日 2008.05.09

(85)PCT申请进入国家阶段日
2010.11.09

(86)PCT申请的申请数据
PCT/US2008/063280 2008.05.09

(87)PCT申请的公布数据
WO2009/136944 EN 2009.11.12

(71)申请人 惠普开发有限公司
地址 美国德克萨斯州

(72)发明人 W·G·弗里 V·Y·阿利曼努埃尔·诺沃亚

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 李娜 王洪斌

(51)Int.Cl.
H04L 9/20(2006.01)
G06F 12/14(2006.01)
G06F 21/00(2006.01)

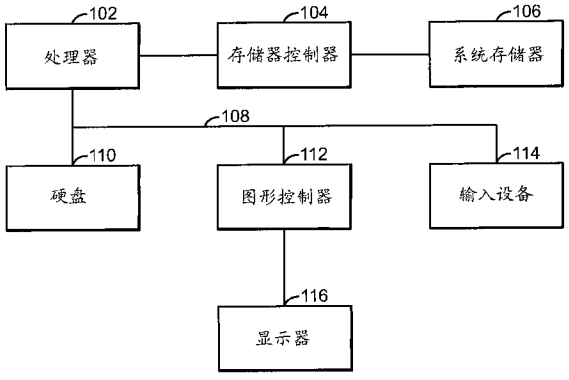
权利要求书 2 页 说明书 3 页 附图 3 页

(54)发明名称

用于提供对系统存储器的安全访问的系统和方法

(57)摘要

提供了一种提供对存储于计算机系统的系统存储器中的数据的安全访问的方法，该计算机系统包括用于向系统存储器写入数据和从系统存储器读取数据的存储器控制器。该方法包括每当引导计算机系统时生成随机加密密钥并且在存储器控制器的易失性存储器区中存储随机加密密钥。该方法还包括使用随机加密密钥对数据进行加密以创建加密数据并且在系统存储器中存储加密数据。也提供一种用于执行该方法的存储器子系统和计算机系统。



CN 102150391 A

1. 一种提供对存储于计算机系统的系统存储器中的数据的安全访问的方法，所述计算机系统包括用于向所述系统存储器写入数据和从所述系统存储器读取数据的存储器控制器，所述方法包括：

每当引导所述计算机系统时生成随机加密密钥；

在所述存储器控制器的易失性存储器区中存储所述随机加密密钥；

使用所述随机加密密钥对数据进行加密以创建加密数据；并且

在所述系统存储器中存储所述加密数据。

2. 如权利要求 1 所述的方法，包括：

从所述系统存储器读取所述加密数据；并且

使用所述随机加密密钥对所述加密数据进行解密。

3. 如权利要求 1 所述的方法，其中所述存储器控制器的所述易失性存储器区包括只写 / 一次性写入寄存器。

4. 如权利要求 1 所述的方法，包括在执行系统复位时复位所述存储器控制器的所述易失性存储器区。

5. 如权利要求 1 所述的方法，其中对所述数据进行加密包括使用所述数据和所述随机加密密钥来执行 XOR 运算。

6. 如权利要求 1 所述的方法，其中每当引导所述计算机系统时由系统基本输入 - 输出系统 (BIOS) 生成所述随机加密密钥。

7. 如权利要求 1 所述的方法，包括：

生成至少一个后续随机加密密钥；并且

使用所述至少一个后续随机加密密钥对数据进行加密。

8. 一种计算机系统的存储器子系统，所述存储器子系统包括：

存储器控制器，其适合于：每当所述计算机系统被引导时接收随机加密密钥、在所述存储器控制器中的易失性存储器区中存储所述随机加密密钥、使用所述随机加密密钥对数据进行加密并且在系统存储器中存储加密数据。

9. 如权利要求 8 所述的存储器子系统，其中所述存储器控制器适合于从所述系统存储器读取所述加密数据并且使用所述随机加密密钥对所述加密数据进行解密。

10. 如权利要求 8 所述的存储器子系统，其中所述存储器控制器的所述易失性存储器区包括只写 / 一次性写入寄存器。

11. 如权利要求 8 所述的存储器子系统，其中在执行系统复位时复位所述存储器控制器的所述易失性存储器区。

12. 如权利要求 8 所述的存储器子系统，其中所述存储器控制器适合于通过使用所述数据和所述随机加密密钥执行 XOR 运算对所述数据进行加密。

13. 如权利要求 8 所述的存储器子系统，包括：系统基本输入 - 输出系统 (BIOS)，其适合于每当所述计算机系统被引导时生成所述随机加密密钥。

14. 如权利要求 8 所述的存储器子系统，其中所述存储器控制器适合于使用至少一个后续随机加密密钥对数据进行加密。

15. 一种计算机系统，包括：

硬盘，其适合于存储供所述计算机系统使用的数据；

处理器，其适合于读取所述硬盘上存储的数据；

存储器控制器，其适合于：每当所述计算机系统被引导时接收随机加密密钥、在所述存储器控制器中的易失性存储器区中存储所述随机加密密钥、从所述处理器接收数据、使用所述随机加密密钥对所述数据进行加密并且在系统存储器中存储加密数据；以及

系统存储器，其适合于存储从所述存储器控制器接收的加密数据。

16. 如权利要求 15 所述的计算机系统，其中所述存储器控制器适合于从所述系统存储器读取所述加密数据并且使用所述随机加密密钥对所述加密数据进行解密。

17. 如权利要求 15 所述的计算机系统，其中所述存储器控制器的所述易失性存储器区包括只写 / 一次性写入寄存器。

18. 如权利要求 15 所述的计算机系统，其中在执行系统复位时复位所述存储器控制器的所述易失性存储器区。

19. 如权利要求 15 所述的计算机系统，其中所述存储器控制器适合于通过使用所述数据和所述随机加密密钥执行 XOR 运算对所述数据进行加密。

20. 如权利要求 15 所述的计算机系统，包括：系统基本输入 - 输出系统 (BIOS)，其适合于每当所述计算机系统被引导时生成所述随机加密密钥。

用于提供对系统存储器的安全访问的系统和方法

背景技术

[0001] 在典型的计算机系统中，其中使用系统存储器作为安全密钥和证书的暂时储存器。近年来，黑客已经开始尝试通过从用户的计算机物理地移除存储器模块、可能地冻结存储器模块以延迟其中所含数据的毁坏来获得对安全数据的非法访问。黑客随后将窃取的存储器模块安装到另一计算机中以读取它们的内容。以这样的方式，黑客可以能够取回存储器模块中存储的安全密钥和证书并且使用窃取的信息以获得对用户的敏感数据的未授权访问。

附图说明

[0002] 在下文详细描述中参照附图描述某些示例实施例，在附图中：

[0003] 图 1 是根据本发明一个示例实施例的计算机系统的框图；

[0004] 图 2 是根据本发明一个示例实施例的图 1 中所示计算机系统的存储器子系统的框图；并且

[0005] 图 3 是示出根据本发明一个示例实施例的操作受保护的系统存储器的方法的流程图。

具体实施方式

[0006] 图 1 是根据本发明一个示例实施例的计算机系统的框图。计算机系统大体上由标号 100 表示。本领域普通技术人员将理解计算机系统 100 可以包括硬件单元（包括电路）、软件单元（包括存储于机器可读介质上的计算机代码）或者硬件和软件单元的组合。此外，图 1 中所示功能块仅是可以在本发明的一个示例实施例中实施的功能块的一个例子。本领域普通技术人员将容易能够基于针对特定计算机系统的设计考虑来限定具体功能块。

[0007] 处理器 102（如中央处理单元或者 CPU）适合于控制计算机系统 100 的整体操作。处理器 102 连接到适合于从系统存储器 106 读取数据和向系统存储器 106 写入数据的存储器控制器 104。存储器控制器 104 可以包括如下存储器，该存储器包括非易失性存储器区和易失性存储器区。如下文详细阐述的那样，本发明的一个示例实施例适合于通过提供在存储器控制器 104 与系统存储器 106 之间的安全通信来防止数据窃取。

[0008] 系统存储器 106 可以包括多个存储器模块，如本领域普通技术人员将理解的。此外，系统存储器 106 可以包括非易失性和易失性部分。系统基本输入－输出系统 (BIOS) 可以存储于系统存储器 106 的非易失性部分中。系统 BIOS 适合于控制启动或者引导过程并且控制计算机系统 100 的低级操作。

[0009] 处理器 102 连接到至少一个系统总线 108 以允许在处理器 102 与其它系统设备之间的通信。系统总线可以在诸如外围部件互连 (PCI) 总线的变型等标准协议下操作。在图 1 中所示示例实施例中，系统总线 108 将处理器 102 连接到硬盘驱动器 110、图形控制器 112 和至少一个输入设备 114。硬盘驱动器 110 为计算机系统所用的数据提供非易失性存储。图形控制器 112 又连接到显示设备 116，该显示设备基于由计算机系统 100 进行的活动来向

用户提供图像。

[0010] 图 2 是根据本发明一个示例实施例的图 1 中所示计算机系统的存储器子系统的框图。存储器子系统大体上由标号 200 表示。存储器子系统 200 包括存储器控制器 104 和系统存储器 106。

[0011] 当计算机系统 100 被引导或者以别的方式接收到系统复位时，存储器控制器 106 接收存储在易失性存储器区 202 中的随机加密密钥。在本发明的一个示例实施例中，易失性存储器区 202 包括经由系统复位来复位的只写 / 一次性写入寄存器。随机加密密钥可以由系统 BIOS 生成，该系统 BIOS 在计算机系统被引导时执行各种初始化功能。如下文详细说明的那样，随机加密密钥用来加密向系统存储器 106 写入的数据。

[0012] 在本发明的一个示例实施例中，后续随机加密密钥由存储器控制器 104 选择性地用来加密数据。后续随机加密密钥可以例如由存储器控制器 104 生成。可选地，后续随机加密密钥可以由计算机系统 100 的另一部件如系统 BIOS 提供。如果使用后续随机加密密钥，则系统存储器 106 的不同区域将用不同的随机加密密钥进行加密。多个随机加密密钥的使用使得黑客难以使用数字生成器来标识用来对系统存储器 106 的内容进行加密的所有随机加密密钥。

[0013] 存储器控制器 104 的加密块 204 使用当前随机加密密钥对向系统存储器 106 写入的所有数据进行加密。在本发明的一个示例实施例中，简单加密算法如 XOR 算法可以由加密块 204 使用以最小化对存储器子系统 200 的吞吐量的影响。示例 XOR 算法包括使用向系统存储器写入的数据和随机加密密钥执行 XOR 操作。以下例子说明本发明的一个示例实施例如何针对存储于系统存储器中的数据提供增强的安全性。假设数据元 A 和 B 在已经使用随机加密密钥 R 进行 XOR 加密之后要写入到系统存储器。可以使用以下等式来描述这一过程：

[0014] $A \oplus R = C$

[0015] $B \oplus R = D$

[0016] 其中 C 是 A 的加密版本且 D 是 B 的加密版本。加密数据 C 和 D 存储于系统存储器中，而不是 A 或者 B 本身被存储。利用一些数学操纵，获得以下结果：

[0017] $C \oplus D = A \oplus B$

[0018] 因此，知识渊博的黑客可能能够操纵来自窃取的存储器模块的数据以重建 A 和 B 的某种聚集 (conglomeration)。然而，在不能访问随机加密密钥 R 的情况下获得 A 和 B 本身仍然非常困难。本发明示例实施例的使用显著增加了对来自系统存储器的数据进行未授权恢复的难度。

[0019] 本领域普通技术人员将理解除了对随机加密密钥与将向系统存储器写入的数据进行 XOR 之外的加密算法也可以用来对向系统存储器 106 写入的数据进行加密。另外，加密块 204 运用的具体加密算法并非本发明的基本特征。

[0020] 当从系统存储器 106 读取加密数据时，它由存储器控制器 104 内的解密块 208 解密。解密块 208 使用曾由加密块 204 用来执行数据加密的随机加密密钥来执行解密。然后可以向处理器 102 提供解密数据。本发明的一个示例实施例通过向系统存储器 106 仅写入加密数据来提供增强的数据安全。

[0021] 通过在存储器控制器 104 内的易失性存储器区中存储随机加密密钥，本发明的一

个示例实施例减小了如下风险：黑客或者其他潜在数据窃取者将能够恢复加密密钥并且获得对用特定随机加密密钥加密并且随后存储于系统存储器 106 中的数据的访问。不能反工程设计或者“剥离”存储器控制器 104 以确定密钥，因为密钥的值在存储器控制器断电后不会存在于非易失性存储区 202 中。即使以某种方式（例如通过冻结构成系统存储器的存储器模块等）保存了系统存储器中存储的数据，这仍然将防止对已经使用特定随机加密密钥加密的数据的访问。

[0022] 图 3 是示出了根据本发明一个示例实施例的操作受保护的系统存储器如系统存储器 106（图 1）的方法的流程图。该方法大体上由标号 300 表示。该过程始于块 302。

[0023] 在块 304，每当引导计算机系统如计算机系统 100（图 1）时生成随机加密密钥。如在块 306 所示，在存储器控制器（如存储器控制器 104（图 1））的易失性存储器区中存储随机加密密钥。

[0024] 如在块 308 所示，使用随机加密密钥对数据进行加密。如在块 310 所示，在系统存储器中存储加密数据。在块 312，该过程结束。

[0025] 本发明的一个示例实施例提供一种在存储器控制器与例如包括多个存储器模块的系统存储器之间的安全通信方法。这样的示例实施例保护系统存储器免受各种各样的黑客攻击。具体而言，本发明的一个示例实施例适合于保护系统存储器免受物理攻击和引导攻击。另外，可以使用标准存储器部件和模块。当引入新一代存储器技术时无需附加工作。本发明的一个示例实施例提供系统存储器安全而不明显影响系统性能并且不影响操作系统和软件应用性能。最后，可以在对总系统成本和复杂度的影响最小的情况下实施本发明的示例实施例。

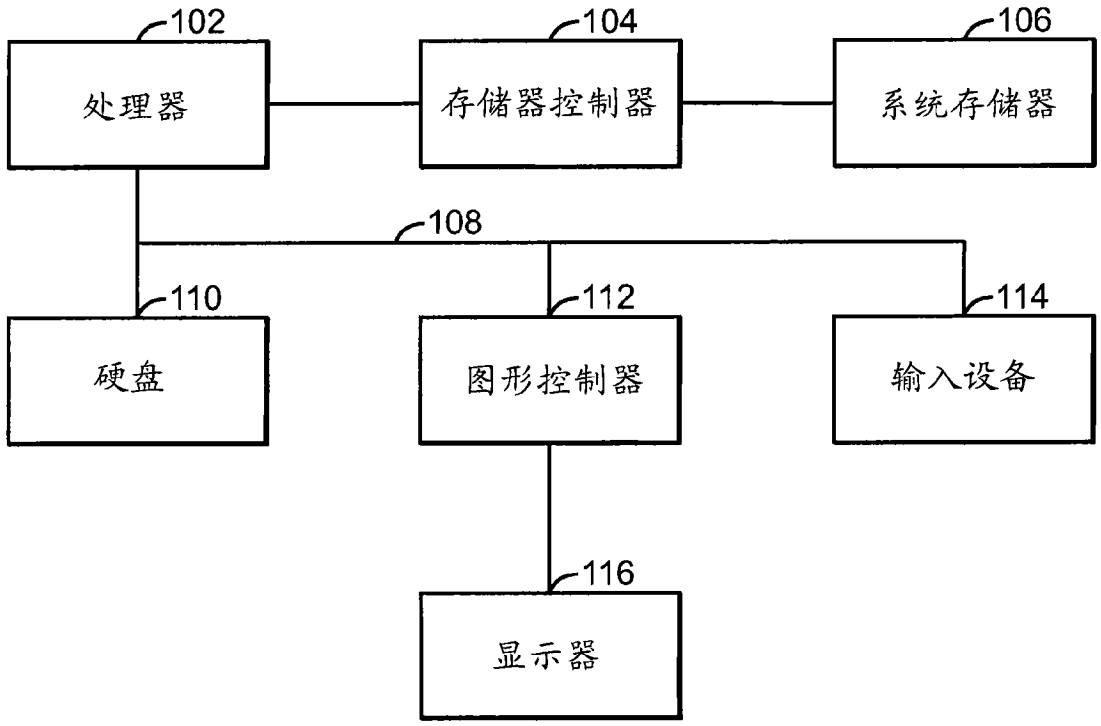

102
处理器
104
存储器控制器
106
系统存储器
108
110
硬盘
112
图形控制器
114
输入设备
116
显示器

图 1

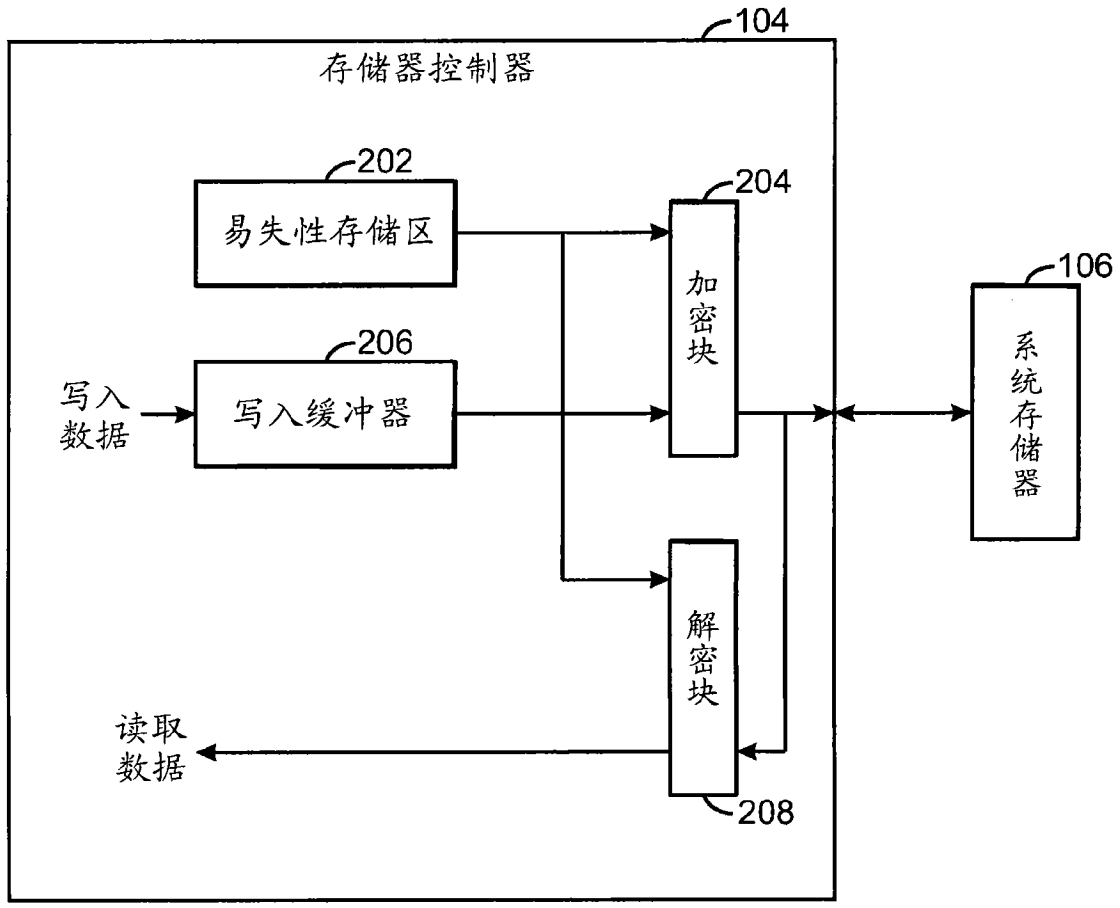

104
存储器控制器
202
易失性存储区
204
加密块
106
系统存储器
206
写入数据
写入缓冲器
解密块
读取数据
208

图 2

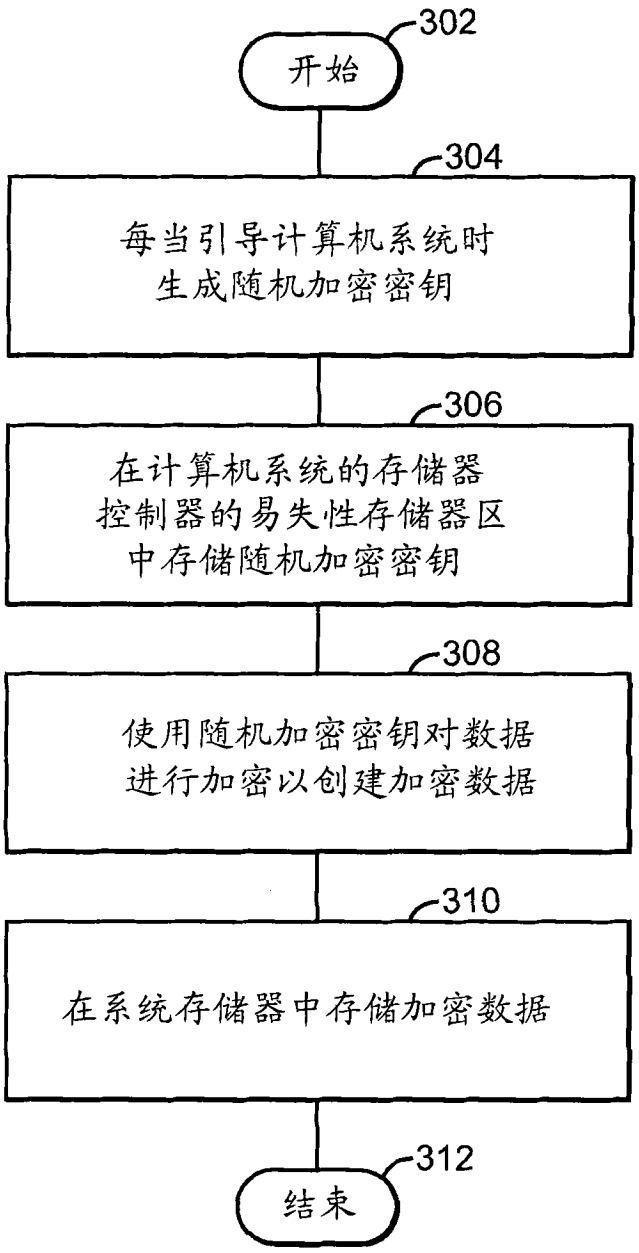

302
开始
304
每当引导计算机系统时
生成随机加密密钥
306
在计算机系统的存储器
控制器的易失性存储器区
中存储随机加密密钥
308
使用随机加密密钥对数据
进行加密以创建加密数据
310
在系统存储器中存储加密数据
312
结束
300

图 3