(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 108475316 B
(45)授权公告日 2022.07.26

(21)申请号 201680076027.6
(22)申请日 2016.03.08
(65)同一申请的已公布的文献号
申请公布号 CN 108475316 A
(43)申请公布日 2018.08.31
(85)PCT国际申请进入国家阶段日
2018.06.22
(86)PCT国际申请的申请数据
PCT/US2016/021375 2016.03.08
(87)PCT国际申请的公布数据
WO2017/155516 EN 2017.09.14
(73)专利权人 惠普发展公司,有限责任合伙企业
地址 美国德克萨斯州
(72)发明人 C·佩罗内 D·梅达利亚 W·斯泰勒 C·瓦尔拉思
(74)专利代理机构 中国专利代理(香港)有限公司 72001
专利代理师 李雪娜 陈岚
(51)Int.Cl.
*G06F 21/60*(2006.01)
*G06F 21/72*(2006.01)
*G06F 21/78*(2006.01)
(56)对比文件
US 2004003273 A1,2004.01.01
US 2004003273 A1,2004.01.01
US 8281388 B1,2012.10.02
US 2014006799 A1,2014.01.02
US 2005044433 A1,2005.02.24
US 2010153752 A1,2010.06.17
CN 101154195 A,2008.04.02
审查员 李华芳

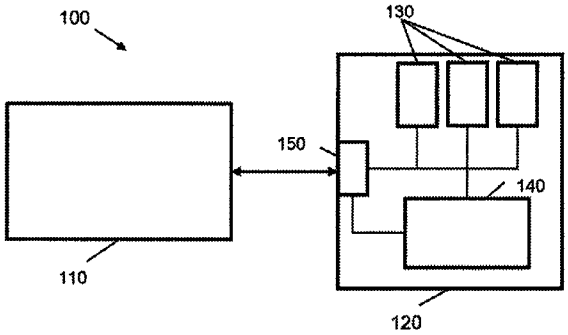
权利要求书2页 说明书9页 附图3页

(54)发明名称

使数据安全

(57)摘要

本文中描述用于使计算设备上的数据安全的系统和方法的示例。响应于系统的操作状态从第一操作状态到第二操作状态的改变,在计算设备的存储器模块中存储的数据的至少一部分上执行一个或多个密码学操作。




CN 108475316 B

1.一种用于使数据安全的系统,包括:

第一功率供给;

备份功率供给;

计算设备;

非易失性存储器模块;以及

密码学引擎;

其中所述非易失性存储器模块在系统的第一操作状态期间存储从计算设备接收的数据,在第一操作状态中,所述非易失性存储器模块由第一功率供给供电;以及

其中响应于系统的操作状态从第一操作状态到第二操作状态的改变,所述密码学引擎:

对没有使用加密而存储在非易失性存储器模块中的数据的第一部分进行加密,而同时所述密码学引擎由备份功率供给供电,并且使在没有使用加密而存储在非易失性存储器模块中的数据的第二部分保持不加密;

其中所述第二操作状态与第一操作状态相比是相对较低的功率状态。

2.根据权利要求1所述的系统,其中所述第一操作状态和第二操作状态是非易失性存储器模块和计算设备中的一个或多个的功率状态。

3.根据权利要求2所述的系统,其中所述第二操作状态是断电状态。

4.根据权利要求3所述的系统,其中所述备份功率供给是可充电的功率源,其被布置成在第一操作状态期间被充电。

5.根据权利要求1所述的系统,其中响应于操作状态从第二操作状态到第三操作状态的改变,所述密码学引擎对非易失性存储器模块中加密的数据的第一部分进行解密。

6.根据权利要求5所述的系统,其中所述密码学引擎通过使待解密的数据的第一部分流水线化来对非易失性存储器模块中加密的数据的第一部分执行一个或多个解密操作和/或并行地执行两个或多个解密操作。

7.一种用于使数据安全的方法,包括:

从计算设备接收数据;

在包括计算设备和非易失性存储器模块的系统的第一操作状态期间将数据存储到非易失性存储器模块,其中在第一操作状态期间,所述非易失性存储器模块由第一功率供给供电;以及

响应于系统的操作状态中从第一操作状态到第二操作状态的改变,由密码学引擎对没有使用加密而存储在非易失性存储器模块中的数据的第一部分进行加密,而同时所述密码学引擎由备份功率供给供电,并且使在没有使用加密而存储在非易失性存储器模块中的数据的第二部分保持不加密;

其中所述第二操作状态与第一操作状态相比是相对较低的功率状态。

8.根据权利要求7所述的方法,其中所述第一操作状态和第二操作状态是非易失性存储器模块和计算设备中的一个或多个的功率状态。

9.根据权利要求7所述的方法,其中所述第二操作状态包括断电状态。

10.根据权利要求8所述的方法,其中所述备份功率供给是可再充电的功率源,其在第一操作状态期间被再充电。

11.根据权利要求7所述的方法,其中所述方法还包括对非易失性存储器模块中所存储的数据的第一部分进行解密。

12.一种存储器模块,其包括:

非易失性存储器单元;以及

密码学引擎,

其中所述存储器模块可操作成在其中存储器模块由第一功率供给供电的系统的第一操作状态期间在非易失性存储器单元中不使用加密的方式存储由存储器模块所接收的数据;并且

其中所述密码学引擎被布置成:响应于系统的操作状态从第一操作状态到第二操作状态的改变,对没有使用加密而存储在非易失性存储器模块单元中的数据的第一部分进行加密,而同时所述密码学引擎由备份功率供给供电,并且使在没有使用加密而存储在非易失性存储器模块单元中的数据的第二部分保持不加密;

其中所述第二操作状态与第一操作状态相比是相对较低的功率状态。

# 使数据安全

## 背景技术

[0001] 使计算设备上的数据安全呈现许多挑战。可以在设备的操作期间“在途地(in-transit)”使数据安全,或者当数据在设备的存储器中是静态的时候“静息地(at-rest)”使数据安全。典型地,使在途的数据安全是高成本的操作,其需要正在设备的存储器上写入和从设备的存储器读取的数据的加密和解密。非易失性存储器在设备掉电的时候存储数据,并且因此呈现其自己的安全性挑战。

## 附图说明

[0002] 本公开内容的各种特征从随后结合附图而理解的详细描述中将是显而易见的,所述附图共同地作为示例图示了本公开内容的特征,并且其中:

[0003] 图1是根据示例的用于使存储器模块中存储的数据安全的系统的示意图;

[0004] 图2是根据另一示例的用于使存储器模块中的数据安全的、耦合到功率供给的系统的示意图;

[0005] 图3是根据示例的图示了用于使存储器模块中存储的数据安全的方法的示意图;

[0006] 图4是根据示例的图示了对系统的操作状态的改变进行标识的方法的示意图;以及

[0007] 图5是根据示例的计算机系统的示意性框图。

## 具体实施方式

[0008] 在随后的描述中,为了解释的目的,阐明了某些示例的众多特定细节。在说明书中对“示例”或类似语言的参考意指结合示例所描述的特定特征、结构或特性被包括在至少那一个示例中,但是不一定被包括在其它示例中。

[0009] 本文中所描述的某些示例提供用于使从计算设备接收的数据安全的方法和系统。使计算设备所访问的数据安全的常见方法、诸如加密和认证方法可以被部署在许多不同的上下文中,这取决于计算设备的安全性要求。在一个示例中,在途地加密数据。计算设备包括专用于使对计算设备的存储器的读取和写入访问安全的板上密码学硬件模块和/或软件。在另一情况中,当设备掉电的时候,静息地在长期存储中使数据安全。例如,计算设备可以被耦合到提供批量数据加密的存储设备。当计算设备掉电时或可替换地应用户的请求,存储设备上的数据被加密。当计算设备再次请求对数据的访问时、诸如当设备上电、例如给定适当的授权和/或用户证书的情况下,数据被解密。在针对在途数据的安全性的情况中,所感知的安全性威胁是能够在计算设备上执行应用期间探查微处理器或其存储器组件的侵犯者。这是高级别的安全性,并且因而,与设备性能的权衡典型地在真实应用中是显著的。特别地,为每个读取和写入访问执行密码学操作例如在执行时间方面并且还在功率消耗方面是昂贵的。在使静息数据安全的后一示例中,一个安全性威胁采用例如能够从计算机窃取硬驱动器的侵犯者的形式。对于具有用于存储的静息数据加密的设备,在存储组件被窃取并且被应用到数据的加密算法是安全的情况中,保证数据的安全性。然而,当设备在

使用中的时候在对存储器的读取和写入操作期间的在途数据的安全性不被保证。此外，当设备在使用中的时候，对硬盘读取和写入数据是低效的。因此，在计算设备的操作期间，数据可能保持未被加密。

[0010] 近年来，计算设备中基于传统硬盘驱动器(HDD)的存储已经利用相对较快的固态存储器而被增强，并且甚至被其所取代。存储器可以被布置到嵌入在计算设备中的模块中，或被布置到独立的设备中，所述独立的设备诸如存储器卡、USB闪速驱动器和固态驱动器，其可以例如被连接到计算设备以及从计算设备断开。这样的存储器设备包括闪速存储器——一种形式的非易失性存储器，其基于电可擦除可编程只读存储器(EEPROM)。闪速存储器例如具有在存储器开始劣化之前只能容忍有限数目的写入循环的缺陷。此外，闪速存储器以字节块来存储数据，并且不是字节可寻址的。出于这些原因，闪速存储器典型地最佳适于作为辅存储装置。另一方面，其它形式的非易失性存储器已经开始变成对于诸如静态和动态随机存取存储器(SRAM/DRAM)之类的主易失性存储器的可行置换。示例包括磁阻性RAM(MRAM)、铁电RAM(FRAM)、电池支持的(backed)SRAM、电池支持的DRAM、电阻性RAM(RRAM，其基于忆阻器)以及相变RAM(PCRAM)。这些形式的存储器具有以下优点：既是非易失性的、在设备处于掉电状态中的时候保持数据，并且还作为一种形式的主存储器，其中在相应计算设备的操作期间数据可以直接被写到所述主存储器和从所述主存储器读取。特别地，这些形式的存储器可以是字节可寻址的。可以看到这些形式的非易失性存储器致力于一种形式的通用存储器，其具有较早前形式的存储器的最合期望的性质，但是没有其某些所感知的缺点。

[0011] 从安全性的视角，非易失性存储器在某些应用中可以被感知为是不利的，因为数据在存储器中持久，甚至当存储器不能访问功率源的时候。例如，在设备上基于web的浏览活动中所使用的会话密钥的情况中，事实上可能合期望的是将密钥和其它敏感数据存储在易失性存储器中。然而，如先前所标识的，本技术要么针对加密对存储器的所有读取/写入操作，其相对于长期存储批量加密方法具有性能缺陷，并且其在提供高级别安全性的同时经常被设计用于以字节块存储数据的存储设备。此外，对在途数据进行加密的联机(in-line)加密方法基于强攻击模型，所述强攻击模型要求侵犯者在操作期间具有对设备的完全访问。在较新形式的字节可寻址的非易失性存储器取代现存存储器的时候，在这两个极端之间的解决方案是合期望的。

[0012] 本文中描述的方法和系统提供当访问存储器的计算设备处于相对低供电状态中的时候使存储器中存储的数据安全的手段。在示例中，一种系统将操作状态从第一操作状态改变到第二操作状态，所述系统包括计算设备和非易失性存储器模块。响应于操作状态的改变，耦合到非易失性存储器模块中的一个或多个非易失性存储器单元的密码学引擎可以被布置成在被存储在非易失性存储器单元中的数据上执行一个或多个密码学操作。

[0013] 在本文中所描述的某些示例中，系统的操作状态包括计算设备的功率状态。例如，计算设备的第一操作状态可以是“上电”，其中计算设备可以执行对非易失性存储器单元的读取和写入操作。第二操作状态于是可以是“断电”，其中设备不再执行相应地从或向非易失性存储器单元的读取和写入操作。

[0014] 在该场景中，密码学引擎可以被布置成检测何时计算设备移动到和/或处于相对较低供电(例如断电)状态。在本文中所述的某些示例中，在第一操作状态期间，非易失性存

储器可以由计算设备本身供电，所述计算设备具有和/或充当第一功率源。然而，在第二操作状态中，非易失性存储器和密码学引擎可以被提供有第二功率源和/或由第二功率源供电。通过为密码学引擎提供第二功率源，有可能独立于第一功率源地执行密码学操作，所述第一功率源在计算设备从第一操作状态移到第二操作状态的时候可能是“关断的”。密码学引擎被布置成当计算设备处于第二操作状态中的时候对非易失性存储器单元中存储的数据加密，所述第二操作状态是相对较低供电的状态，因而使得在计算设备已经掉电之后持续的非易失性存储器中的数据安全。在该示例中，使得非易失性存储器单元中存储的数据安全。这在例如由希望得到对被写入到非易失性存储器单元中的安全信息的访问的攻击者获得非易失性存储器模块的情况下保护数据，即使非易失性存储器模块变成从计算设备解耦。当系统返回到第一操作状态、或到不同于先前操作状态的新的第三操作状态的时候，非易失性存储器单元中存储的数据被解密。例如，在一个场景中，当计算设备被带入相对较高供电的状态中的时候，诸如当设备被开启或带出睡眠或休眠模式的时候，在给定适当授权或用户证书(诸如密码)的情况下，非易失性存储器单元中存储的数据被解密。可替换地，可以在已知种类的可信平台模块中使密钥安全。

[0015] 在一个示例中，当从非易失性存储器单元中读取数据的时候，在经加密的数据上执行解密操作。在另一个情况中，可以通过如下来执行一个或多个解密操作：使要经由密码学引擎解密的数据流水线化，或通过在很可能首先被需要的数据上开始解密操作。这可以例如响应于设备改变操作状态、诸如被带出睡眠或休眠状态，或被供电或引导或像这样的。在另一示例中，诸如加密或解密操作的密码学操作并行地被执行。

[0016] 在可替换的示例中，包含非易失性存储器模块的非易失性存储器设备被布置成从第一操作状态改变到第二操作状态。在一种情况中，非易失性存储器设备被布置成检测由于诸如从计算设备断开之类的外部改变所引起的操作状态中的改变，或可替换地通过检测物理侵入来检测操作状态中的改变。与先前描述的示例类似地，当处于第二操作状态中的时候，耦合到非易失性存储器设备中的非易失性存储器模块的密码学引擎可以由第二功率源供电，以便执行一个或多个密码学操作，诸如对非易失性存储器单元中存储的数据进行加密。第二功率源可以独立于第一功率源，所述第一功率源在第一操作状态期间为非易失性存储器设备供电。例如，非易失性存储器设备在第一操作状态期间可能已经通过其与计算设备的连接而被供电。

[0017] 在其它示例中，存储器可以包括易失性存储器，并且密码学引擎可以被布置成例如当检测到相应系统的操作状态的改变的时候对易失性存储器中存储的数据进行加密。当然，在易失性存储器的情况下，操作状态的改变将不包括易失性存储器的断电状态，因为存储器将会需要功率以便运转。操作状态的改变可以因此是例如切换到相对较低功率模式(如不同于断电模式的)，改变到安全级别或所感知的风险改变，如将在下文中所描述的。

[0018] 图1是根据示例的系统100的简化示意图。图1中所示的系统100包括在该实例中连接到非易失性存储器模块120的计算设备110。图1中所示的非易失性存储器模块120可以是在计算设备内部的模块，或可替换地可以是在耦合到计算设备110的非易失性存储器设备内的模块。在图1中所示的示例中，非易失性存储器模块120被布置成响应于从计算设备110接收到数据而将数据存储在一个或多个非易失性存储器单元130(其中的三个被示出)中。根据本文中所述的示例，非易失性存储器模块120可以被实现为单芯片或多芯片组件。所述

模块可以是一个或多个嵌入式硬件芯片。可替换地，在另一示例中，非易失性存储器模块是包括一个或多个芯片的可拆卸模块。

[0019] 初始地，诸如图1中所示的系统100之类的系统以第一操作状态而操作。系统100的操作状态可以涉及计算设备110和非易失性存储器模块120中的任一个或二者，或者在某些其它情况中，涉及计算设备110或非易失性存储器模块120的组件。非易失性存储器模块120可以包括通信地耦合到非易失性存储器单元130的密码学引擎140。密码学引擎140具有对非易失性存储器单元130中所存储的数据的读取和写入访问。

[0020] 根据示例，密码学引擎140可以被实现为非易失性存储器模块120内的基于硬件的模块。在这样的情况中，密码学引擎140可以包括微处理器或微控制器组件，例如具有其自己的可寻址的存储器(未示出)，所述存储器可以在密码学操作期间被使用。可替换地，可以在非易失性存储器单元130中预留空间用于在被存储在非易失性存储器单元130中别处的数据上执行密码学操作。在任何情况中，微处理器被布置成执行程序代码以用于在被存储在一个或多个非易失性存储器单元130中的数据上实现密码学操作。

[0021] 根据第二示例，密码学引擎140被实现为非易失性存储器模块120中的软件或固件。在该情况中，密码学引擎140可以被通用处理单元取代。在这样的情况中，通用处理单元可以被布置成访问非易失性存储器模块130中的存储器，所述存储器存储了用于实现所述一个或多个密码学操作的程序代码。其它示例可以部署硬件、软件和/或固件的组合以实现所述一个或多个密码学操作。

[0022] 在图1中所示的系统100中，密码学引擎140和非易失性存储器单元130连接到控制组件150。根据示例，控制组件150包括在非易失性存储器模块120内的电路，所述电路对系统的操作状态的改变敏感。控制组件还提供对系统的计算设备110的接口。特别地，经由与计算设备110的连接，控制组件150被布置成检测何时系统100从第一操作状态改变到第二操作状态。例如，在一种情况中，控制组件150被布置成检测在计算设备110和非易失性存储器模块120之间的连接中的电压的改变。在这样的情况中，电压的改变可以是响应于其中嵌入了非易失性存储器模块120的计算设备110切换到较低功率模式、或者非易失性存储器设备中的非易失性存储器模块120变成从计算设备110断开。

[0023] 密码学引擎140耦合到控制组件150并且可由控制组件响应于控制组件150检测到系统100的操作状态从第一操作状态到第二操作状态的期望的或实际的改变而被控制。例如，控制组件可以在计算设备110变成从非易失性存储器模块120断开之前响应于软件“弹出(eject)”请求。可替换地，如果非易失性存储器模块具有可替换的功率供给(如以下更详细地所描述的)，则控制组件150可以在功率供给变成断开的时候响应于电压中的伴随的下降。作为响应，密码学引擎140可以将数据从非易失性存储器单元130读取到其自己的存储器(未示出)中，并且在数据(或该数据的一部分)上执行一个或多个密码学操作。在执行了所述一个或多个密码学操作之后，密码学引擎140于是可以将经修改的数据写回到非易失性存储器单元130中。根据示例，可以针对非易失性存储器单元中存储的数据的不同部分、以不同级别的安全性来执行密码学操作。例如，第一部分可以保持未被加密，第二部分可以利用128位密钥来加密，并且第三部分可以利用256位密钥来加密。在一种情况中，用于对数据的部分进行加密的安全性级别可以基于例如对数据的可访问性的期望级别。

[0024] 在某些示例中，密码学引擎140访问以字节块、以单个字节或甚至以位而存储在非

易失性存储器单元130中的数据，并且在非易失性存储器单元130中存储的数据上执行另外的密码学操作之前在该数据上执行密码学操作。在另一情况中，密码学引擎140被布置成以非顺序方式访问字节，例如由此可以在分离的单元中存储的数据上并行地执行一个或多个密码学操作。在又一示例中，系统的操作状态的改变可以包括来自计算设备110的对锁定非易失性存储器单元130的单个块(或一个或多个被标识的块)的指示。在这样的情况中，密码学引擎140被布置成从非易失性存储器单元130访问单个存储器单元，并且在存储器单元中存储的数据上执行密码学操作。

[0025] 在一些示例中，密码学引擎140被布置成在非易失性存储器单元130中存储的数据上实现常规的密码学功能，诸如加密/解密、认证、验证、数据完整性校验和密码学散列。在加密/解密操作的情况中，密码学引擎130访问非易失性存储器模块120中存储的密钥以对数据进行加密或解密。密钥可以是非易失性存储器模块120的防篡改区段中存储的制造商的密钥，或者它可以是被加载到计算设备110上和从计算设备110检索的用户密钥。

[0026] 图2是根据示例的系统200的示意图。在图2中，系统200被示出为连接到第一功率供给210。系统200包括在该实例中耦合到非易失性存储器模块230的计算设备220，其类似于图1中所示的系统100的等同组件。非易失性存储器模块230包括一个或多个非易失性存储器单元240(如先前那样，三个被示出)以及通信地耦合到一个或多个非易失性存储器单元240的密码学引擎250。如图1中所示的系统100那样，非易失性存储器模块230可以是计算设备220的组件，或可替换地可以是耦合到计算设备220的非易失性存储器设备(未示出)的组件。密码学引擎250被布置成响应于系统200的操作状态的改变而访问被存储在非易失性存储器单元240上的数据。非易失性存储器模块230连接到第二功率供给260。第二功率供给260被布置成在系统200的第二操作状态期间为非易失性存储器模块230的组件供给功率。系统200的第一操作状态对应于如下的状态：其中计算设备上电并且其中被供给到非易失性存储器模块230的功率来自第一功率供给210。系统的第二操作状态对应于如下的状态：其中计算设备220不再被供给有来自第一功率供给210的功率。与图1中的非易失性存储器模块100类似地，图2中的非易失性存储器模块230包括控制组件270，所述控制组件操作为与计算设备的接口并且被布置成检测系统200的操作状态的改变。控制组件可以例如包括已知种类的阈值检测电路(未示出)，其在检测到由于来自第一功率供给210的功率的丢失所致的电压中的下降的情况下自动切换到第二功率供给260。可替换地，所述电路可以驻留在第二功率供给本身内。在任何事件中，在目前情况下，当检测到操作状态的改变的时候，控制组件270被布置成通过使用来自第二功率供给260的功率而控制密码学引擎250，以读取一个或多个非易失性存储器单元240中的数据，以及在数据上执行一个或多个密码学操作。在数据上执行一个或多个密码学操作之后，密码学引擎250被布置成将数据写回到一个或多个非易失性存储器单元240中。

[0027] 图2中所示的系统200的组件的可替换配置是可能的。例如，在一种情况中，计算设备220具有第一功率供给210，并且非易失性存储器模块230直接从与计算设备的连接得到功率。这可以是在例如膝上型计算设备中的情况，所述膝上型计算设备包含与非易失性存储器模块230类似的非易失性存储器模块。在该情况中，系统200的操作状态对应于计算设备220的一个或多个功率状态。例如，第一操作状态对应于如下的状态：其中计算设备上电并且从第一功率供给210得到功率。例如，计算设备可以是移动设备或膝上型计算机，并且

第一功率供给可以是为计算设备供电的锂离子电池。计算设备的操作状态的改变对应于计算设备进入相对较低供电的操作模式。例如，计算设备可以进入休眠模式(挂起到硬盘)或睡眠模式(挂起到RAM)。在这样的实例中，控制组件250被布置成检测计算设备的电压的改变。密码学引擎由来自第二功率供给的功率控制，并且在计算设备的操作状态的改变的时候执行一个或多个非易失性存储器单元中存储的数据的一个或多个密码学操作。

[0028] 在可替换的实施例中，系统200的操作状态对应于非易失性存储器模块230的功率状态。系统200的第一操作状态对应于如下状态：其中非易失性存储器模块230已经从第二功率供给260得到功率以便对所存储的数据进行加密(例如，响应于其中系统200由第一功率供给供电的操作状态的先前的改变)。随后，系统200将操作状态改变到如下功率状态：其中系统被供给有来自第一功率供给的功率。作为响应，密码学引擎250于是可以被布置成在一个或多个非易失性存储器单元240中存储的数据上执行一个或多个密码学操作。例如，在非易失性存储器单元240中存储的数据上的第一密码学操作可以包括在其中功率由第二功率供给所供给的系统操作状态中的加密操作。响应于系统将操作状态改变到其中由第一功率供给210来供给功率的功率状态，密码学引擎250可以执行一个或多个解密操作。

[0029] 前述的典型示例是如下情形：其中在连接到干线供给的膝上型计算机的非易失性存储器模块中存储的数据变成从干线功率供给断开。响应于膝上型计算机的状态的改变，密码学引擎在非易失性存储器单元中存储的数据上执行加密操作，其中加密操作由来自膝上型计算机中的电池模块的功率所支持。当膝上型计算机重连接到干线功率供给的时候，密码学引擎在非易失性存储器单元中的经加密的数据上执行解密操作，这由干线功率供给所支持。

[0030] 在其中提供第二功率供给的实例中，功率供给可以包括可再充电的电池。电池于是可以在第一操作状态期间再充电。可替换地，第二功率源可以包括多个电池、超级电容器、干线功率源或其它种类的可替换功率源。

[0031] 图3图示了根据示例的方法300，其在该实例中被存储在非易失性存储器模块的非易失性存储器单元中的数据上执行一个或多个密码学操作。图3的方法300可以结合图1和2中所示的系统100和200被使用。

[0032] 在框310处，从计算机设备接收数据。例如，图1中所示的计算设备110被布置成发送由非易失性存储器模块120所接收的数据。在一个示例中，被布置成接收数据的非易失性存储器模块可以是在计算设备本身中的非易失性存储器模块。可替换地，被布置成接收数据的设备可以是包括一个或多个非易失性存储器模块的非易失性存储器设备。例如，非易失性存储器设备可以是可移除介质，诸如“USB棒”或便携式“闪速驱动器”。在还另外的示例中，通过远程或联网的连接从计算设备接收数据，例如通过与包括非易失性存储器的第二设备的无线连接、LAN、蓝牙连接或移动网络连接。

[0033] 在框320处，在系统的第一操作状态期间，数据被存储在非易失性存储器中，所述系统包括计算设备和非易失性存储器。可以在不使用任何种类的加密的情况下存储数据(尽管预计到某些软件应用可能已经应用了诸如加密之类的安全性措施——例如作为密码保护的结果)。当结合图1和2中所示的系统100和200而使用方法300的时候，非易失性存储器包括具有一个或多个非易失性存储器单元(130、240)的非易失性存储器模块(130、230)。在系统处于第一操作状态中的时候，所述非易失性存储器存储数据。在一种情况中，第一操

作状态由实现方法300的、从第一功率供给接收功率的系统(诸如从图2中所示的第一功率供给210接收功率的系统200)的一个或多个组件来表征。此外,包括从计算设备接收数据的读取/写入操作可以在图3中所示的方法300中在系统的第一操作状态期间被执行。

[0034] 在框330处,响应于系统的操作状态的改变而执行一个或多个密码学操作。根据示例,密码学操作可以包括加密操作或解密操作。如果结合图1和2中所示的系统100和200被使用,则由位于非易失性存储器模块中的控制组件来检测系统的操作状态的改变。通常,方法300可以在系统上被实现,所述系统包括例如多个非易失性存储器并且其中系统的操作状态的改变的检测是关于系统中的非易失性存储器中的一个。根据示例,执行一个或多个密码学操作的步骤在与图1和2中所示的密码学引擎(140、250)类似的组件上被执行。如先前所指示的,由通用处理器和位于其中已经存储了数据的非易失性存储器中或在所述非易失性存储器外围的存储器来执行密码学操作。在任何情况中,能够执行一个或多个密码学操作的硬件或软件组件被布置成访问非易失性存储器上存储的数据并且执行密码学操作。密码学操作可以包括以下各项中的一个或多个:在非易失性存储器中存储的数据上的加密/解密、认证、验证、数据完整性校验和密码学散列。例如,在一种情况中,实现诸如AES之类的加密算法。

[0035] 图4示出了根据示例的方法400,其在该实例中被存储在系统的非易失性存储器中的数据上执行密码学操作。方法400可以结合图1和2中所示的系统100和200,并且还结合图3中所示的方法300被使用。在框410处,从在系统的第一操作状态中操作的计算设备接收数据。数据可以直接由计算设备中的非易失性存储器模块接收,或者可替换地由连接到第一计算设备(本地或远程地)的第二设备、诸如包括非易失性存储器模块的非易失性存储器设备所接收。可以经由任何数目的介质来发送数据。例如,在其中在远程地相连接的两个设备之间发送数据的情况中,数据可以通过LAN、无线网络或连接(诸如蓝牙连接等等)而被发送。在另一情况中,在包括非易失性存储器模块、诸如USB棒或可移除的盘驱动器、例如闪速存储器的设备处接收数据。在又一情况中,数据通过高速总线被接收并且被存储在一个或多个双列直插式存储器模块(DIMM)中。如先前所描述的,“操作状态”可以涉及其中系统从第一功率供给接收功率的状态。在一个示例中,关于图4中所示的方法400,“第一操作状态”涉及如下的系统状态:其中由第一功率供给为系统供电,类似于在第一操作状态期间从图2中所示的功率供给210接收功率的系统200。

[0036] 在框420处,第二操作状态被标识为计算设备或非易失性存储器的“断电”状态。在结合图2中所示的系统200所使用的方法400的示例中,“断电”状态是系统200从功率供给210断开的结果。在该情况中,计算设备220或非易失性存储器模块230的功率状态是相对低的功率状态,例如,作为系统200从功率供给210断开的结果。如先前所描述的,控制组件270被布置成响应于系统的功率状态的改变,并且作为响应,将非易失性存储器模块的操作切换到辅功率源260。

[0037] 在框430处,在使用来自辅功率源的功率的非易失性存储器中存储的数据上执行一个或多个密码学操作。密码学操作可以包括加密或解密操作中的一个。在一种情况中,可以使用方法400,其中辅功率源是耦合到非易失性存储器模块或包含非易失性存储器模块的非易失性存储器设备的电池模块。电池模块可以包含可以是可代替(当放电时)、可充电和/或可再充电的电池。在该情况中,响应于检测到系统的功率状态已经从“开”状态改变到

“关”状态，电池模块作为功率供给而接管以向能够在非易失性存储器中存储的数据上实施密码学操作的设备供电。特别地，实现方法400的系统可以根据示例被布置成为源自辅可再充电的电池模块的设备的非易失性存储器中持有的数据加密。类似地，当主功率供给或第一功率供给再次变成对系统可用、其表示检测到的操作状态改变的时候，系统可以再次执行方法400，但是代替地对已经存储在非易失性存储器中的经加密的数据进行解密。

[0038] 可替换的示例可以根据不同种类的操作状态中的改变而操作。例如，第一操作状态可以被定义为相对安全的操作状态，而第二操作状态可以被定义为相对不安全的操作状态。安全操作状态可以是当计算设备(诸如计算机或手持式设备)未连接到任何种类的网络的时候。在这样的状态中，与当计算机或设备“在线”并且连接到网络的时候相比，可感知到远程攻击的风险相对低。然后，当计算机或设备连接到网络的时候，这可以触发向根据第二操作状态的操作的切换，其中某个非易失性存储器中的数据根据本发明的实施例而被加密。当例如膝上型计算机被“坞接”到被连接到可以用于与膝上型计算机通信的有线LAN或这样的其它网络的坞接站中的时候可以部署类似的方案。设想到根据其它不同种类的基于安全性的操作状态的操作。仍其它种类的操作状态可以涉及计算设备的位置。例如，在相对安全的环境中(诸如在安全的办公室环境中或在家里)可以不部署加密(处于第一操作状态)，而当在公共环境中时可部署它(处于第二操作状态)，因为计算机或设备可能被窃取或以其它方式被误用的风险更大。

[0039] 所有先前提及的可替换示例将会等同地适用于易失性和非易失性存储器类型二者。

[0040] 在参考图1和图2描述的实施例中，控制组件150、270被描述为非易失性存储器模块内的组件，其被适配和布置成确定存储器模块的操作状态的改变。在可替换的实施例中，控制组件的功能性的一部分或全部可以驻留在非易失性存储器模块的外部。例如，检测何时丢失干线功率并且控制何时从电池汲取功率的电路可以驻留在膝上型计算机或可以在干线或电池功率上操作的任何其它设备内。该相同电路(即，在非易失性存储器模块外部)可以用于控制密码学引擎的操作，而无需重现非易失性存储器模块内的电路的全部或至少一部分。

[0041] 本文中所描述的方法和系统提供一种响应于部署非易失性存储器的系统的操作状态的改变而使非易失性存储器中持有的数据安全的手段。系统的示例提供一种通过向耦合到非易失性存储器的密码学引擎提供辅功率而当例如系统丢失功率的时候使非易失性存储器中持久的数据安全的经改进的手段。相比于先前已知的方法，这减少在执行到非易失性存储器中的读取和写入操作的计算设备的操作期间使数据安全的负担。当向存储器写入的计算设备不处于使用中的时候所述系统保护数据免受存储器从系统被窃取或被攻击的现实威胁，而避免联机加密的性能惩罚。

[0042] 如本文中所述的某些方法和系统可以由一个或多个处理器实现，所述处理器处理从非暂时性存储介质检索的程序代码。图5示出了包括耦合到至少一个处理器520的机器可读存储介质510的设备的示例500。机器可读介质510可以是能够包含、存储或维持程序和数据以供指令执行系统使用或结合指令执行系统使用的任何介质。机器可读介质可以包括许多物理介质中的任一中，诸如例如电子的、磁性的、光学的、电磁的或半导体介质。合适的机器可读介质的更特定的示例包括但不限于硬驱动器、随机存取存储器(RAM)、只读存储器

(RAM)、可擦除可编程只读存储器或便携式盘。在图5中，机器可读存储介质包括用以实现一个或多个密码学操作以用于使非易失性存储器中存储的数据安全的程序代码。根据示例，设备500包括通信地耦合到彼此的多个分离的、分布式设备，并且处理器520跨多个设备分布。

[0043] 以上示例要被理解为是说明性的。要理解的是，关于任一个示例所描述的任何特征可以单独地或与所描述的其它特征相组合地被使用，并且还可以与任何其它示例的一个或多个特征、或任何其它示例的任何组合相组合地被使用。此外，还可以采用以上没有描述的等同物和修改。

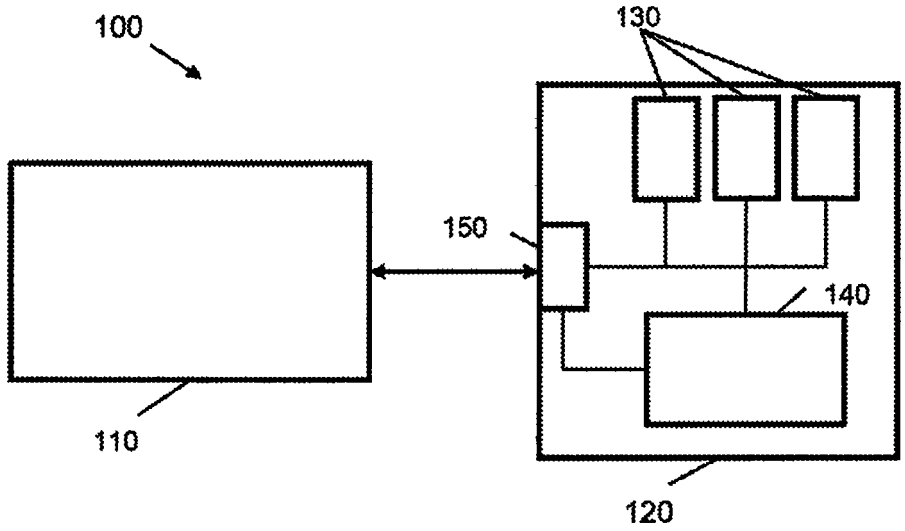



图1

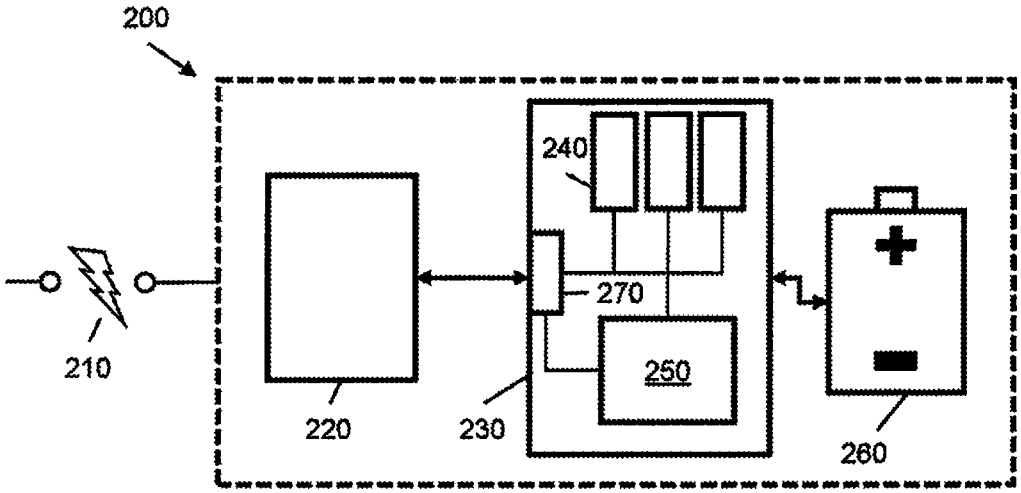



图2

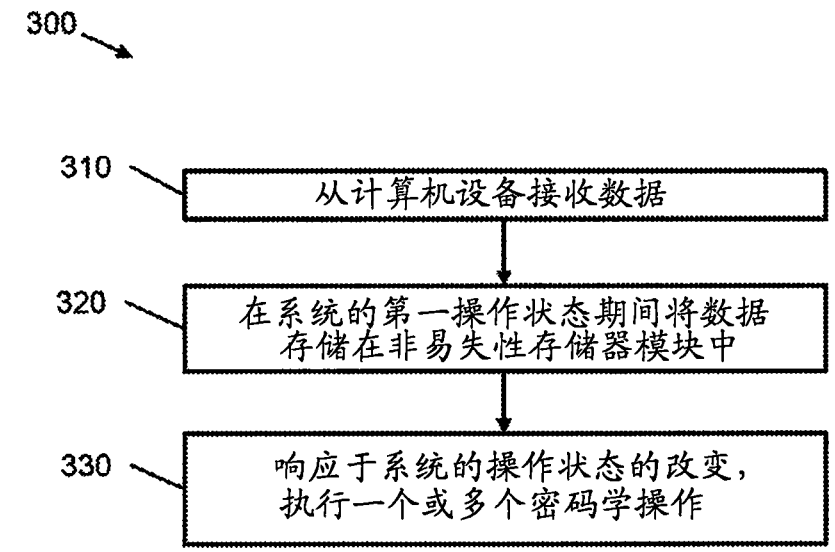

300
310
从计算机设备接收数据
320
在系统的第一操作状态期间将数据存储在非易失性存储器模块中
330
响应于系统的操作状态的改变，执行一个或多个密码学操作

图3

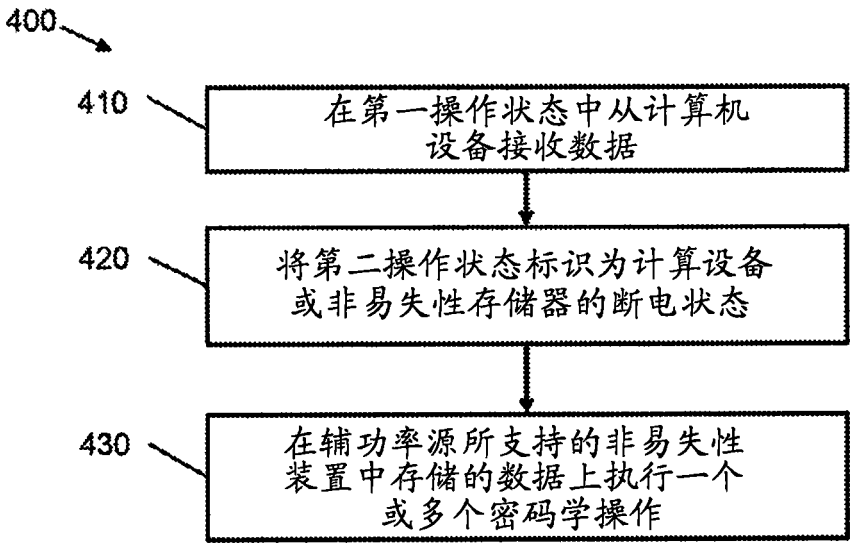

400
410
在第一操作状态中从计算机设备接收数据
420
将第二操作状态标识为计算设备或非易失性存储器的断电状态
430
在辅功率源所支持的非易失性装置中存储的数据上执行一个或多个密码学操作

图4

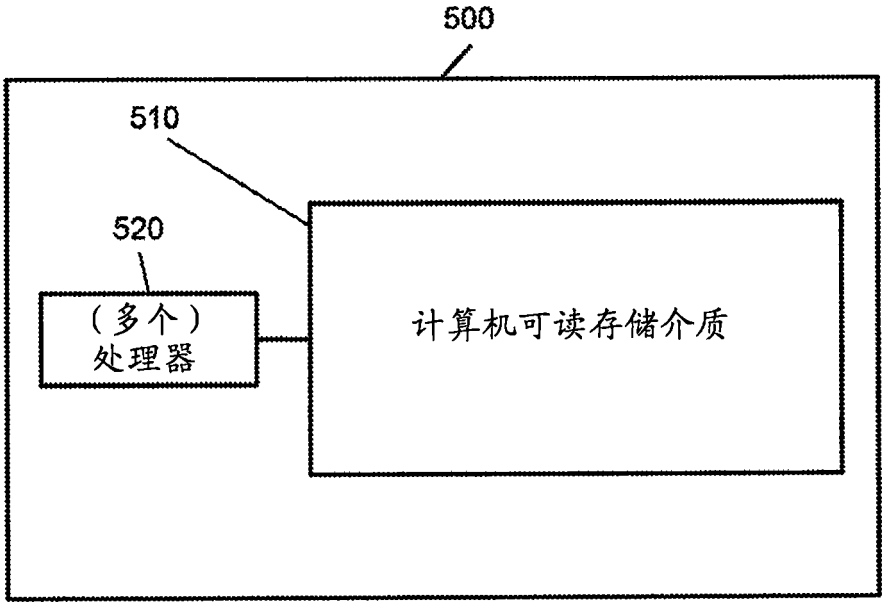



图5