(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 114342314 A
(43)申请公布日 2022.04.12

(21)申请号 202080062786.3

(22)申请日 2020.09.03

(30)优先权数据
62/900,045 2019.09.13 US
16/808,174 2020.03.03 US

(85)PCT国际申请进入国家阶段日
2022.03.08

(86)PCT国际申请的申请数据
PCT/IB2020/058194 2020.09.03

(87)PCT国际申请的公布数据
WO2021/048708 EN 2021.03.18

(71)申请人 国际商业机器公司
地址 美国纽约

(72)发明人 G·加奎特

(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
代理人 冯雯

(51)Int.Cl.
H04L 9/08(2006.01)

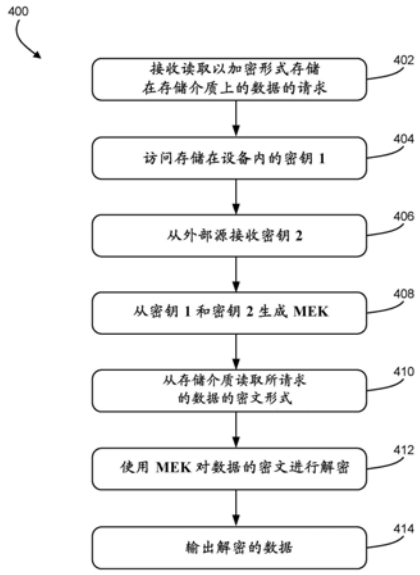
权利要求书3页 说明书19页 附图10页

(54)发明名称

经由内部和/或外部动作的密码擦除

(57)摘要

一种设备实现的方法，用于经由内部动作和外部动作实现和/或执行密码擦除。在一个说明性方面中，在被配置为在存储介质上执行数据操作的设备处接收读取数据的请求，数据以加密形式存储在存储介质上。在一种方式中，访问存储在设备内的第一密钥。在另一方式中，检索存储在存储介质上和/或与存储介质一起存储的第一密钥。从外部源接收第二密钥。使用第一密钥和第二密钥生成介质加密密钥。从存储介质读取数据的加密形式。使用介质加密密钥来解密数据的加密形式。输出解密的数据。还呈现了用于写入加密数据的方法。



CN 114342314 A

1.一种设备实现的方法,包括:

在被配置为在存储介质上执行数据操作的设备处接收读取数据的请求,所述数据以加密形式存储在所述存储介质上;

访问存储在所述设备内的第一密钥;

从外部源接收第二密钥;

使用所述第一密钥和所述第二密钥生成介质加密密钥;

从所述存储介质读取所述数据的加密形式;

使用所述介质加密密钥对所述数据的加密形式进行解密;以及

输出解密的数据。

2.如权利要求1所述的设备实现的方法,其中所述第一密钥以原始形式存储在所述设备中。

3.如权利要求1所述的设备实现的方法,其中,所述第一密钥以包装形式存储在所述设备中,并且包括接收用于解开所述第一密钥的信息。

4.如权利要求1所述的设备实现的方法,其中所述设备被配置为禁止将所述第一密钥转移到所述设备的外部。

5.如权利要求1所述的设备实现的方法,其中所述存储介质包含非易失性存储器。

6.如权利要求5所述的设备实现的方法,其中所述第一密钥在所述设备中被存储在作为与所述存储介质不同类型的存储器的非易失性存储器中。

7.如权利要求1所述的设备实现的方法,其中所述设备为带驱动器,其中所述存储介质为磁记录带。

8.如权利要求1所述的设备实现的方法,包括:接收用于存储在所述存储介质上的第二数据;从第二外部源接收第三密钥;使用所述第一密钥和所述第三密钥生成第二介质加密密钥;使用所述第二介质加密密钥加密数据;以及将加密的数据写入所述存储介质。

9.一种用于实现和/或执行密码擦除的计算机程序产品,所述计算机程序产品包括计算机可读存储介质,所述计算机可读存储介质具有随其体现的程序指令,所述程序指令可由被配置为在存储介质上执行数据操作的设备执行以使所述设备执行如权利要求1所述的方法。

10.一种系统,包括:

被配置为在存储介质上执行数据操作的设备,所述设备具有处理器以及与所述处理器集成、可由所述处理器执行、或者与所述处理器集成且可由所述处理器执行的逻辑,所述逻辑被配置为使所述设备执行如权利要求1所述的方法。

11.一种设备实现的方法,包括:

在被配置为在存储介质上执行数据操作的设备处接收读取数据的请求,所述数据以加密形式存储在所述存储介质上;

检索存储在所述存储介质上和/或与所述存储介质一起存储的第一密钥;

从外部源接收第二密钥;

使用所述第一密钥和所述第二密钥生成介质加密密钥;

从所述存储介质读取所述数据的加密形式;

使用所述介质加密密钥对所述数据的加密形式进行解密;以及

输出解密的数据。

12.如权利要求11所述的设备实现的方法,其中所述存储介质包含非易失性存储器。

13.如权利要求12所述的设备实现的方法,其中所述第一密钥在所述设备中被存储在作为与所述存储介质不同类型的存储器的非易失性存储器中。

14.如权利要求11所述的设备实现的方法,其中所述设备为带驱动器,其中所述存储介质为磁记录带。

15.如权利要求11所述的设备实现的方法,其中所述设备被配置为禁止将所述第一密钥转移到所述设备的外部。

16.如权利要求11所述的设备实现的方法,其中所述第一密钥以原始形式存储在所述存储介质上和/或与所述存储介质一起存储。

17.如权利要求11所述的设备实施的方法,其中所述第一密钥以包装形式存储在所述存储介质上和/或与所述存储介质一起存储,并且包括接收用于解开所述第一密钥的信息。

18.如权利要求11所述的设备实现的方法,包括:接收用于存储在所述存储介质上的第二数据;从第二外部源接收第三密钥;使用所述第一密钥和所述第三密钥生成第二介质加密密钥;使用所述第二介质加密密钥加密数据;以及将加密的数据写入所述存储介质。

19.一种系统,包括:

被配置为在存储介质上执行数据操作的设备,所述设备具有处理器以及与所述处理器集成、可由所述处理器执行、或者与所述处理器集成且可由所述处理器执行的逻辑,所述逻辑被配置为执行如权利要求11所述的方法。

20.一种设备实现的方法,包括:

在被配置为在存储介质上执行数据操作的设备处接收将数据以加密形式写入所述存储介质的请求;

访问存储在所述设备内的第一密钥;

从外部源接收第二密钥;

使用所述第一密钥和所述第二密钥生成介质加密密钥;以及

使用所述介质加密密钥将所请求的数据以加密形式写入所述存储介质。

21.如权利要求20所述的设备实现的方法,其中所述设备被配置为禁止将所述第一密钥转移到所述设备的外部。

22.一种系统,包括:

被配置为在存储介质上执行数据操作的设备,所述设备具有处理器以及与所述处理器集成、可由所述处理器执行、或者与所述处理器集成且可由所述处理器执行的逻辑,所述逻辑被配置为使所述设备执行如权利要求20所述的方法。

23.一种设备实现的方法,包括:

在被配置为在存储介质上执行数据操作的设备处接收将数据以加密形式写入所述存储介质的请求;

检索存储在所述存储介质上和/或与所述存储介质一起存储的第一密钥;

从外部源接收第二密钥;

使用所述第一密钥和所述第二密钥生成介质加密密钥;以及

使用所述介质加密密钥将所请求的数据以加密形式写入所述存储介质。

24.如权利要求23所述的设备实现的方法,其中所述设备被配置为禁止将所述第一密钥转移到所述设备的外部。

25.一种系统,包括:

被配置为在存储介质上执行数据操作的设备,所述设备具有处理器以及与所述处理器集成、可由所述处理器执行、或者与所述处理器集成且可由所述处理器执行的逻辑,所述逻辑被配置为使所述设备执行如权利要求23所述的方法。

经由内部和/或外部动作的密码擦除

技术领域

[0001] 本发明涉及密码擦除，并且更具体地，本发明涉及用于经由内部动作和/或外部动作实现密码擦除的技术和系统。

背景技术

[0002] 术语“密码擦除”通常指禁止访问以某种方式解密数据所需的加密密钥。这可以例如通过擦除加密密钥的所有副本、移除加密密钥的一部分、禁用对生成或解锁加密密钥所需的子密钥的访问等来完成。通过永久地禁用加密密钥，用该加密密钥加密的数据不能被解密；加密的数据被有效地呈现为不可加密的。

[0003] 已经规定，当今的数据中心具有不能明确地密码擦除所有出故障的或停用的自加密驱动器(SED)的主要问题。例如，SED可能以其不再能够通信至其所在的系统的方式出故障。在这种出故障状态下，SED不能接收密码擦除的命令或者以指示密码擦除的命令成功完成的状态来响应这种命令。对于不愿意冒从出故障的SED(其不能被明确地密码擦除)的固态驱动器(SSD)或硬盘驱动器(HDD)存储器取证地恢复数据的风险的数据中心，这是问题。如今，这些数据中心通常求助于物理地破坏那些驱动器以努力防止取证恢复。由于害怕公开数据，用户不能凭良心将那些驱动器返回至制造商或再使用它们。

[0004] 应注意，用于加密和解密SED上的数据的介质加密密钥(MEK)不以明文存储在现代SED中。相反，MEK被加密地包装，例如自身被加密或以其他方式被混淆。人们认为，在非常长久的运行中，这可能不够强大，以至于在可预见的未来可能破解密钥包装技术(例如，经由量子计算)。

[0005] 不管问题的范围或是否应当存在包裹密钥可以被解密或破译的任何有效担忧，可能非常正确的是，存在不希望依赖或完全信任驱动器来处理MEK的非易失性存储和MEK的密码擦除的实体。这样的用户可能非常偏好于在每个上电循环之后将MEK提供至驱动器，而不是将MEK存储在SED上，以确保MEK可以被破坏并且用它创建的所有密文被密码擦除。这使用户控制MEK，并且所述用户不必担心驱动器以不允许由驱动器执行密码擦除的方式出故障的情况。因为MEK仅被非易失性地存储在驱动器外部，所以它可以被用户破坏，独立于SED如何出故障。然而，对保持MEK的用户密钥存储装置的破坏或者对该MEK到SED的通信的窃听(并且破坏周围的任何保护措施)致使MEK易受捕获或检索的攻击。

[0006] 使得能够有在外部密码擦除SED的能力的一种方式是通过使用由LTO-4(第一具有加密能力的LTO带驱动器生成)使用的直接密钥服务模型。注意，如何在具有加密能力的设备外部处理密钥确定了它们是否是可密码擦除的。但是，当然，如果实体的密钥管理被适当地完成，则应当能够明确地密码擦除与出故障的SED驱动器相关联的MEK的所有副本。然而，通常制作密钥的副本并且将其存储在分布式位置中，以确保密钥保持可用于对数据进行解密，因为如果没有留下密钥的副本，则在该密钥下加密的数据(即，密文)将不是可解密的，并且因此有效地使得不可访问或“密码擦除”。因此，随着制作越来越多的密钥的副本，密钥管理变得明显更难以安全。

[0007] 在LTO-4的时间之后,SED技术围绕符合可信计算组(TCG)规范(诸如,它们的TCG存储的安全子系统类别(SSC),包括(最初)企业和(最近)Opal)而标准化。这两个SSC都以多种不同方式支持密码擦除。例如,在Opal的情况下,存在至少四种不同方式来调用密码擦除。但是TCG SSC都不支持独立于SED本身的外部实体的密码擦除,即,如果SED不能履行SSC指定的方法(命令)。MEK总是存储在SED中,通常以加密包装的形式。如果某人可以某种方式了解如何破解开被包裹的MEK,则该人可恢复存储在出故障的SED中的所有相关联的密文。

发明内容

[0008] 根据本发明的一方面,一种设备实现的方法包括在被配置为在存储介质上执行数据操作的设备处接收读取数据的请求,该数据以加密形式存储在该存储介质上。访问存储在设备内的第一密钥。从外部源接收第二密钥。使用第一密钥和第二密钥生成介质加密密钥。从存储介质读取数据的加密形式。使用介质加密密钥来解密数据的加密形式。输出解密的数据。该方法使得能够通过内部动作和外部动作两者来对本地加密的数据进行密码擦除。

[0009] 根据本发明的另一方面,一种设备实现的方法包括在被配置为在存储介质上执行数据操作的设备处接收读取数据的请求,该数据以加密形式存储在该存储介质上。检索存储在存储介质上和/或与存储介质一起存储的第一密钥。从外部源检索第二密钥。使用第一密钥和第二密钥生成介质加密密钥。从存储介质读取数据的加密形式。使用介质加密密钥来解密数据的加密形式。输出解密的数据。该方法使得能够通过内部动作和外部动作两者来对本地加密的数据进行密码擦除。在使用可移动存储介质的情况下,第一密钥随介质一起行进,但是数据保持安全,直到提供第二密钥。

[0010] 根据本发明的又一方面,一种设备实现的方法包括在被配置为在存储介质上执行数据操作的设备处接收将数据以加密形式写入存储介质的请求。访问存储在设备内的第一密钥。从外部源接收第二密钥。使用第一密钥和第二密钥生成介质加密密钥。使用介质加密密钥将所请求的数据以加密形式写入存储介质。该方法使得写入的加密数据能够通过内部动作和外部动作二者而被密码擦除。

[0011] 根据本发明的又一方面,一种设备实现的方法包括在被配置为在存储介质上执行数据操作的设备处接收将数据以加密形式写入存储介质的请求。检索存储在存储介质上和/或与存储介质一起存储的第一密钥。从外部源接收第二密钥。使用第一密钥和第二密钥生成介质加密密钥。使用介质加密密钥将所请求的数据以加密形式写入存储介质。该方法使得写入的加密数据能够通过内部动作和外部动作二者而被密码擦除。

[0012] 在各种方法中,执行各个方法中的任一个方法的设备优选地被配置为禁止将第一密钥转移到设备外部。因而,因为第一密钥不能离开设备,所以从设备删除第一密钥有效地密码擦除设备上的加密数据。

[0013] 本文描述的各种方法可应用于许多类型的存储介质,包括非易失性存储器和磁记录带。

[0014] 本发明的其他方面和方法将从以下详细描述中变得清楚,当结合附图时,以下详细描述通过示例的方式说明本发明的原理。

附图说明

[0015] 图1是根据本发明的一个方面的网络架构的示图。

[0016] 图2是根据本发明的一个方面的可以与图1的服务器和/或客户端相关联的代表性硬件环境的示图。

[0017] 图3是根据本发明的一个方面的分层数据存储系统的示图。

[0018] 图4是根据本发明的一个方面的方法的流程图。

[0019] 图5是根据本发明的一个方面的方法的流程图。

[0020] 图6是根据本发明的一个方面的方法的流程图。

[0021] 图7是根据本发明的一个方面的方法的流程图。

[0022] 图8是描绘用于引退并且保护使用SED的标准存储产品的现有技术的图表。

[0023] 图9是描绘根据本发明的一个方面的用于引退并且保护使用SED的存储产品的说明性过程的图表。

[0024] 图10是描绘根据本发明的一个方面的用于引退并且保护使用SED的存储产品的说明性过程的图表。

具体实施方式

[0025] 以下描述是为了说明本发明的一般原理而进行的，并且不意味着限制在此要求保护的发明概念。另外，本文描述的特定特征可以以各种可能组合和置换中的每一种与其他描述的特征组合使用。

[0026] 除非本文中另外特别限定，否则所有术语都将被给予它们的最广泛的可能解释，包括从说明书中暗示的含义以及本领域技术人员所理解的含义和/或如在词典、论文等中限定的含义。

[0027] 还必须注意的是，如在说明书和所附权利要求中使用的，单数形式“一”、“一个”和“该”包括复数指示物，除非另外指明。还将理解，术语“包括”和/或“包含”当在本说明书中被使用时，指定所述特征、整体、步骤、操作、元件和/或部件的存在，但不排除一个或多个其他特征、整体、步骤、操作、元件、部件和/或其组的存在或添加。

[0028] 本文的描述公开了用于使得本地加密的数据能够通过内部动作和外部动作两者而被密码擦除的系统、方法和计算机程序产品的若干优选方式。在一种方式中，用于加密/解密数据的介质加密密钥(MEK)被分成两个部分--一个密钥份额(密钥1)与数据一起存储，并且另一个密钥份额(密钥2)在外部被管理。在一种方式中，处于非易失性形式的密钥1仅与数据一起存储，可选地以包装形式(例如，被加密或以其他方式保护)。可以以非易失性形式存储的密钥2仅存储在具有数据的设备/产品外部，并且因此密钥2必须被提供给读取数据的设备以实现加密和/或解密。MEK可仅在设备具有密钥1和密钥2两者时被计算。

[0029] 在一种一般方式中，数据被存储在自加密驱动器(SED)中。密钥1在SED内部被管理，并且可以以原始形式或以包装形式存储在SED中。在电力循环和/或其他冷启动之后至少一次将密钥2提供至SED，以允许在SED内部计算MEK。

[0030] 在另一种一般方式中，数据存储在诸如磁记录磁带之类的存储介质上、存储在非易失性随机存取存储器(NVRAM，诸如固态存储器、硬盘等)等中。密钥1存储在存储介质上和/或与存储介质一起存储，并且可以以包装形式存储。向驱动器、计算机等提供密钥2以允

许驱动器、计算机等计算MEK。

[0031] 在本发明的一个示范性方面中，一种设备实现的方法包括在被配置为在存储介质上执行数据操作的设备处接收读取数据的请求，该数据以加密形式存储在该存储介质上。访问存储在设备内的第一密钥。从外部源接收第二密钥。使用第一密钥和第二密钥生成介质加密密钥。从存储介质读取数据的加密形式。使用介质加密密钥来解密数据的加密形式。输出解密的数据。

[0032] 在本发明的另一示范性方面中，一种设备实现的方法包括在被配置为在存储介质上执行数据操作的设备处接收读取数据的请求，该数据以加密形式存储在该存储介质上。检索存储在存储介质上和/或与存储介质一起存储的第一密钥。从外部源检索第二密钥。使用第一密钥和第二密钥生成介质加密密钥。从存储介质读取数据的加密形式。使用介质加密密钥来解密数据的加密形式。输出解密的数据。

[0033] 在本发明的另一示范性方面中，一种设备实现的方法包括在被配置为在存储介质上执行数据操作的设备处接收将数据以加密形式写入存储介质的请求。访问存储在设备内的第一密钥。从外部源接收第二密钥。使用第一密钥和第二密钥生成介质加密密钥。使用介质加密密钥将所请求的数据以加密形式写入存储介质。

[0034] 在本发明的另一示范性方面中，一种设备实现的方法包括在被配置为在存储介质上执行数据操作的设备处接收将数据以加密形式写入存储介质的请求。检索存储在存储介质上和/或与存储介质一起存储的第一密钥。从外部源接收第二密钥。使用第一密钥和第二密钥生成介质加密密钥。使用介质加密密钥将所请求的数据以加密形式写入存储介质。

[0035] 说明性计算环境

[0036] 图1示出了根据一种方式的架构100。如图1所示，提供包括第一远程网络104和第二远程网络106的多个远程网络102。网关101可耦合在远程网络102与邻近网络108之间。在本架构100的上下文中，网络104、106可以各自采取任何形式，包括但不限于局域网(LAN)、广域网(WAN)(诸如互联网)、公共交换电话网(PSTN)、内部电话网等。

[0037] 在使用中，网关101充当从远程网络102到邻近网络108的入口点。这样，网关101可以起到路由器和交换机的作用，路由器能够引导到达网关101的给定数据分组，交换机为给定分组提供进出网关101的实际路径。

[0038] 还包括至少一个数据服务器114，其耦合到邻近网络108，并且可经由网关101从远程网络102访问。应当注意，(一个或多个)数据服务器114可以包括任何类型的计算设备/群件。耦合到每个数据服务器114的是多个用户设备116。用户设备116也可以通过网络104、106、108之一直接连接。这样的用户设备116可以包括台式计算机、膝上型计算机、手持式计算机、打印机或任何其他类型的逻辑。应注意，在一种方式中，用户设备111也可以直接耦合至任何网络。

[0039] 外围设备120或一系列外围设备120(例如，传真机、打印机、联网的和/或本地的存储单元或系统等)可以耦合到网络104、106、108中的一个或多个。应当注意，数据库和/或附加部件可以与耦合到网络104、106、108的任何类型的网络元件一起使用或集成到耦合到网络104、106、108的任何类型的网络元件中。在本说明书的上下文中，网络元件可以指网络的任何部件。

[0040] 根据一些方式，本文描述的方法和系统可以利用虚拟系统和/或模拟一个或多个

其他系统的系统来实现以及/或者在虚拟系统和/或模拟一个或多个其他系统的系统上实现，诸如模拟IBM® z/OS®环境的UNIX®系统、虚拟托管Microsoft® Windows®环境的UNIX®系统、模拟IBM® z/OS®环境的Microsoft® Windows®系统等。在一些方式中，这种虚拟化和/或模拟可以通过使用VMware®软件来增强。

[0041] 在更多的方式中，一个或多个网络104、106、108可以表示通常称为“云”的系统集群。在云计算中，共享资源(诸如处理能力、外围设备、软件、数据、服务器等)以按需关系被提供给云中的任何系统，从而允许跨许多计算系统访问和分布服务。云计算通常涉及在云中操作的系统之间的互联网连接，但也可以使用连接系统的其他技术。

[0042] 图2示出了根据一个方式的与图1的用户设备116和/或服务器114相关联的代表性硬件环境。这样的图示出工作站的典型硬件配置，该工作站具有中央处理单元210(诸如微处理器)以及经由系统总线212互连的多个其他单元。

[0043] 图2中所示的工作站包括随机存取存储器(RAM)214，只读存储器(ROM)216，用于将诸如盘存储单元220之类的外围设备连接到总线212的输入/输出(I/O)适配器218，用于将键盘224、鼠标226、扬声器228、麦克风232和/或诸如触摸屏和数字相机(未示出)之类的其他用户接口设备连接到总线212的用户接口适配器222，用于将工作站连接至通信网络235(例如，数据处理网络)的通信适配器234以及用于将总线212连接至显示设备238的显示适配器236。

[0044] 工作站可以具有驻留在其上的操作系统，诸如Microsoft Windows®操作系统(OS)、macOS®、UNIX®OS等。将明白，优选的方式还可以在除了所提及的那些平台和操作系统之外的平台和操作系统上实施。优选的方式可以使用可扩展标记语言(XML)、C和/或C++语言或其他编程语言以及面向对象的编程方法来编写。可以使用已经变得越来越多地用于开发复杂应用的面向对象编程(OOP)。

[0045] 现在参考图3，示出了根据一个方式的存储系统300。要注意的是，根据各种方面，图3中所示的一些元件可以被实施为硬件和/或软件。存储系统300可以包括用于与至少一个较高存储层302和至少一个较低存储层306上的多个介质和/或驱动器通信的存储系统管理器312。(一个或多个)较高存储层302优选地可以包括一个或多个随机存取和/或直接存取介质304，诸如硬盘驱动器(HDD)中的硬盘、非易失性存储器(NVM)、固态驱动器(SSD)中的固态存储器、闪存、SSD阵列、闪存阵列等，和/或本文指出的或本领域已知的其他介质。(一个或多个)较低存储层306可以优选地包括一个或多个较低性能存储介质308，包括顺序访问介质(诸如，带驱动器中的磁带和/或光学介质)、较慢访问的HDD、较慢访问的SSD等、和/或本文中指出的或本领域已知的其它介质。一个或多个附加存储层316可以包含系统300的设计者所期望的存储存储器介质的任何组合。而且，较高存储层302和/或较低存储层306中的任一者可以包含存储设备和/或存储介质的某种组合。

[0046] 存储系统管理器312可以通过网络310与(一个或多个)较高存储层302和(一个或多个)较低存储层306上的驱动器和/或存储介质304、308通信，网络310诸如存储区域网络(SAN)，如图3所示，或一些其他合适的网络类型。存储系统管理器312还可以通过主机接口314与一个或多个主机系统(未示出)通信，该主机接口314可以是或可以不是存储系统管理器312的一部分。存储系统管理器312和/或存储系统300的任何其他部件可以在硬件和/或

软件中实现，并且可利用用于执行本领域中已知的类型的命令的处理器(未示出)，诸如中央处理单元(CPU)、现场可编程门阵列(FPGA)、专用集成电路(ASIC)等。当然，可以使用存储系统的任何布置，如本领域技术人员在阅读本说明书时将清楚的。

[0047] 在更多的方式中，存储系统300可以包括任何数量的数据存储层，并且可以在每个存储层内包括相同或不同的存储存储器介质。例如，每个数据存储层可以包括相同类型的存储存储器介质，诸如HDD、SSD、顺序存取介质(带驱动器中的带、光盘驱动器中的光盘等)、直接存取介质(CD-ROM、DVD-ROM等)或介质存储类型的任何组合。在一个这样的配置中，较高存储层302可以包括用于在较高性能的存储环境中存储数据的大部分SSD存储介质，并且包括较低存储层306和附加存储层316的剩余存储层可以包括用于在较低性能的存储环境中存储数据的SSD、HDD、带驱动器等的任何组合。以此方式，可将更频繁存取的数据、具有较高优先级的数据、需要更快速存取的数据等存储到较高存储层302，而可将不具有这些属性中的一者的数据存储到附加存储层316，包含较低存储层306。当然，本领域技术人员在阅读本说明书时，可以根据本文提出的方式和方面设计存储介质类型的许多其他组合以实现成不同的存储方案。

[0048] 根据一些方式，存储系统(诸如300)可以包括被配置为接收打开数据集的请求的逻辑、被配置为确定所请求的数据集是否以多个相关联部分存储到分层数据存储系统300的较低存储层306的逻辑，被配置为将所请求的数据集的每个相关联部分移动到分层数据存储系统300的较高存储层302的逻辑，以及被配置为在分层数据存储系统300的较高存储层302上从相关联部分组装所请求的数据集的逻辑。

[0049] 当然，根据不同方式，该逻辑可以被实现为任何设备和/或系统上的方法或被实现为计算机程序产品。

[0050] 用于实现密码擦除的本发明方法

[0051] 以下描述公开了用于使得能够通过内部动作和外部动作两者来对本地加密的数据进行密码擦除的系统、方法和计算机程序产品的若干优选方式。在一种方式中，用于加密/解密数据的MEK被分成两个部分--一个密钥份额(密钥1)与数据一起存储(例如，在SED中、在带上等)，并且另一个密钥份额(密钥2)在外部被管理。在一种方式中，处于非易失性形式的密钥1仅与数据一起存储，优选地以包装的形式存储。可以处于非易失性形式的密钥2仅存储在具有数据的设备/产品的外部，并且因此密钥2必须被提供给读取/写入数据的设备以实现加密和/或解密。MEK可仅在设备具有密钥1和密钥2两者时被计算。

[0052] 在一个一般方面中，数据被存储在SED中。密钥1在SED内部被管理，并且可以以原始形式或更优选地以包装形式存储在SED中。密钥2在SED的电力循环和/或冷启动之后被提供至SED至少一次以允许计算MEK。

[0053] 在另一一般方式中，数据存储在诸如磁记录带之类的存储介质上、存储在NVRAM中等。密钥1存储在存储介质上和/或与存储介质一起存储，并且可以以包装形式存储。例如，密钥1可存储在磁记录带的一部分上、带盒存储器中、或两者中。这样，密钥1可随磁记录带携带。类似地，对于NVRAM设备，密钥1可以存储在NVRAM中、单独的存储器中等。向带驱动器、计算机等提供密钥2以允许驱动器、计算机等计算MEK。

[0054] SED中的密码擦除

[0055] 虽然联合利用SED的示例性实现方式呈现了以下描述中的大部分，但是这仅通过

示例的方式进行并且仅为读者提供上下文作为帮助。因此，下文呈现的概念和教导可同样适用于利用存储介质(诸如磁记录带、存储器卡等)的实现方式。

[0056] 现在参考图4，示出了根据一个方式的方法400的流程图。方法400可根据本发明以各种方式尤其在本文所述的其他附图中所描绘的任何环境中执行。当然，如本领域技术人员在阅读本说明书时将理解的，方法400中可包括比图4中具体描述的那些操作更多或更少的操作。

[0057] 方法400的步骤中的每个步骤可由操作环境的任何合适部件执行。例如，在不同方式中，方法400可以部分地或全部地由计算机、驱动器或其中具有一个或多个处理器的某个其他设备来执行。处理器(例如，以硬件和/或软件实现并且优选地具有至少一个硬件部件的(一个或多个)处理电路、(一个或多个)芯片、和/或(一个或多个)模块)可以在任何设备中用于执行方法400的一个或多个步骤。说明性处理器包括但不限于中央处理单元(CPU)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)等、其组合、或本领域已知的任何其他合适的计算设备。

[0058] 如图4所示，方法400可开始于操作402，在操作402中，被配置为在存储介质上执行数据操作(诸如，从存储介质读取数据和/或向存储介质写入数据)的设备接收读取数据的请求，该数据以加密形式存储在存储介质上。该请求可以简单地请求数据，或者可以包括诸如密钥2之类的附加信息(见下文)。

[0059] 在操作404中，例如从设备的存储器、从ASIC等访问存储在设备内的第一密钥(密钥1)。如上所述，在一些方式中，第一密钥以原始(未加密)形式存储在设备中。在其他方式中，第一密钥以包装形式(例如，加密形式、密码保护形式、混淆形式等)存储在设备中。用于解开第一密钥的信息(诸如另一密钥、密码等)可被接收并用于解开第一密钥。

[0060] 在优选方面中，设备被配置为禁止将第一密钥转移到设备的外部。然而，设备内部的控制器可以访问设备内的第一密钥。

[0061] 在操作406中，从外部源接收第二密钥(密钥2)。外部源可以是任何外部源。例如，外部源可以是数据的请求者、密钥存储装置、密钥服务器、由用户(例如，经由键盘、通过插入闪存驱动器等)输入的密钥。

[0062] 在操作408中，使用第一密钥和第二密钥生成介质加密密钥(MEK)。任何已知技术可用于从第一密钥和第二密钥创建MEK，例如通过对第一密钥和第二密钥进行异或运算(XOR)。

[0063] 在操作410中，例如使用常规技术从存储介质读取所请求的数据的加密形式(即，密文)。存储介质可以是本文公开的任何类型，例如，磁带、磁盘、NVRAM等。因此，设备可以是任何类型的数据存储设备，例如，带驱动器、SSD、HDD、具有加密能力的USB驱动器、NVRAM模块等。

[0064] 在操作412中，使用MEK解密所请求的数据的密文，以给出所请求的数据的未加密(即，明文)形式。所请求的数据的密文可被复制到缓冲器中并且随后被解密，可在读取期间“即时”被解密(例如，操作410和412被同时执行)，等等。

[0065] 在操作414中，经解密的数据被输出，例如，通过主机接口等被输出到数据的请求者。

[0066] 如果第二数据要由该设备存储在存储介质上，则接收第二数据。还可以从第二外

部源接收第三密钥。还可以从第一密钥和第三密钥生成第二介质加密密钥。使用第二介质加密密钥对数据进行加密，并且将加密的数据写入存储介质。注意，第二外部源可与上述外部源相同或不同。同样，第三密钥可以与第二密钥不同或相同。如果第三密钥与第二密钥相同，则驱动器通常不必再次接收它。

[0067] 下面提供图4的各种操作的方面。这些方面仅通过示例的方式呈现，并且不旨在是限制性的。此外，根据本发明的多种可能的方式，可以以任何方式组合这些方面。

[0068] MEK可以使用本领域中已知的和/或本领域技术人员在阅读本说明书时将变得清楚的任何技术来从两个单独的密钥创建。例如，创建需要使用密钥1和密钥2两者来计算的MEK密钥的一种方式是使密钥1和密钥2为两个独立产生的随机数，且接着执行需要密钥1和密钥2两者的计算(诸如，这两个值的XOR或串连)来计算MEK。MEK可以替代地使用密钥拆分算法(例如，Shamir的、Blakely的(欧几里德)等)来‘拆分’成两个(或更多个)密钥份额，例如密钥1和密钥2。

[0069] 密钥1可以源自任何可设想的源。密钥1优选地在SED内部被创建，这是最安全的方法，因为除非有意地从SED复制密钥1的副本，否则密钥1的副本将永远不需要存在于SED外部。

[0070] 在其他方式中，可以在SED外部创建密钥1并且将密钥1提供给SED。例如，可以在制造构建期间将密钥1编程到设备中，可以在写入数据时将密钥1编程到设备中，等等。

[0071] 在可包括来自本文描述的任何其他方法的附加特征和操作的另外的方式中，可结合写入数据来计算密钥1和/或密钥2。例如，在可以使用新的MEK的写入的情况下，可以生成MEK(例如，通过随机数生成或其他已知技术)，并且然后可以使用已知的密钥拆分算法(诸如Shamir的、Blakely的(欧几里德)等)从MEK计算密钥1和密钥2密钥份额。MEK生成和密钥份额计算优选地由设备执行。然后，密钥1可以被保留在设备内部并且密钥2可以从其导出以用于外部存储。在各个方面，该MEK生成是抢先地(即，在接收到写入命令之前，使得其不影响处理写入所需的时间)或响应性地(例如，响应于写入命令，在这种情况下，在命令完成写入操作之前，优选地将密钥2从设备中导出以用于外部存储)执行的。

[0072] 在一个方面，密钥1可专用于特定数据集，并且因此设备可存储多个唯一密钥1，每个唯一密钥1与唯一数据集相关联。

[0073] 优选地，SED被配置为不允许密钥1的任何外部可见性或将密钥1转移或复制出SED。

[0074] 可以在SED内部创建密钥2(如果使用密钥拆分算法来创建密钥份额(其将是密钥2)，则这是优选方法)，或者在SED外部创建密钥2，等等。

[0075] 在说明性方式中，密钥1是MEK的第一密钥份额，与MEK的长度相同(以位为单位)的第一随机数。密钥2是MEK的第二密钥份额，与MEK的长度相同的第二随机数。以预定义方式用密钥2处理密钥1以生成所得MEK。例如，可以用密钥2对密钥1进行XOR(等)以生成MEK。可替代地，可使用标准密钥导出技术(例如，使用散列或加密)代替XOR运算(等)来计算MEK。需要处理密钥1和密钥2两者以计算MEK的任何形式的密钥导出是潜在可接受的。在其中密钥拆分被用于从MEK生成密钥1和密钥2的情况下，用于从密钥1和密钥2创建MEK的计算将是(拆分的)互补或反演计算。

[0076] 注意，使用该拆分密钥技术，如果不具有MEK，则计算MEK的唯一方式是具有密钥1

和密钥2两者。通常，在N密钥拆分中的M个的上下文中，这可以被视为需要实现2个密钥份额(这就是密钥1和密钥2)中的2个来重建(MEK)密钥。替代的(尽管较差的)实施例将是将M设置为2并且生成大于2的数量N个密钥份额，但是丢弃或销毁其他密钥份额中除两个密钥份额之外的所有密钥份额并且因此仅使用那些密钥份额中的剩余两个密钥份额(这有效地将密钥拆分减少到2中的2，但是增加了组合计算的复杂度)。

[0077] 实施拆分密钥MEK的一个优选方式是扩展TCG Opal(或其他TCG SSC)以支持这种双密钥份额概念，使得一个密钥份额(密钥1)在SED内部被管理，并且另一个密钥份额(密钥2)在SED外部被管理。熟悉TCG的Opal SSC的复杂度的任何人都将理解有许多、许多方式来实现这个概念，并且因此，本发明不限于这里所给出的示例性描述。

[0078] 在一个说明性方式中，仅将密钥1的包装形式存储在SED中的非易失性存储器中。密钥2仅以非易失性形式存储在SED外部，并且因此必须在电力循环和/或冷启动之后被提供给SED(或由SED访问)至少一次以允许计算MEK。只有当SED具有密钥1和密钥2两者时，才可以计算MEK。因此，密钥2必须以某种形式被提供给SED(或由SED访问)。根据各种方面，有许多方式可以做到这一点。一种方式是使SED支持密钥管理互操作性协议(KMIP)客户端并且通过安全信道从本领域已知类型的外部密钥管理器请求并接收密钥2。可替代地，密钥2可以以与个人标识号(PIN)的方式类似的方式被提供给SED，例如以明文形式，通过安全隧道(例如TLS)等。

[0079] 密钥1优选地以包装形式存储在SED中，并且密钥1是可解开的，直至提供包装密钥(其可取决于被提供给SED以将不同用户认证为SED支持的不同角色的PIN)。因此，从SED的外部提供的包装密钥的任何部分都被提供给SED以允许解开密钥1。一旦SED已经被提供或已经访问了计算MEK所必需的所有所需信息(包括密钥2)，SED就计算MEK，并且然后能够解密现有密文以产生所得明文(例如，以响应主机读取)，或将新接收的明文形式的客户数据加密成密文(例如，以履行主机写入)。

[0080] 在一种方式中，密钥2是与一些管理安全提供者(下文称为“AdminSP”)角色相关联的PIN，一旦授权实体(诸如驱动器所有者)已用系统标识号(SID)或与具有适当权限的角色相关联的一些其他PIN认证，则启用该PIN。

[0081] 可允许改变密钥2的PIN。在一种方式中，密钥2的PIN将以默认值开始，例如，某个预定义值，诸如全零(0x000…)。一个预期的实现方式将允许改变密钥2的PIN，但仅在AdminSP的第一管理权限(例如AdminSP.Admin1)的PIN被定制之前，以不允许通过无意地改变密钥2的PIN来无意地密码擦除由MEK加密的数据。可替代地，可允许密钥2的PIN在任何时间被改变以提供调用密码擦除的替代方式。

[0082] 在密钥2将被设置为新生成的随机数的情况下，可能看起来密钥2的PIN将在逻辑上生成于SED外部(例如，由用户和他或她的外部密钥管理基础设施)，尽管该生成实际上可能简单地通过调用SED的随机方法(如果其符合TCG的Opal规范则SED必须支持的命令(其是未认证的服务))。响应于随机方法，SED使用任何已知的可接受技术来计算新的随机数并将其返回(提供)至主机。

[0083] 替代的实现方式包括在一些或所有情况下使SED作为生成密钥2的源。在这种情况下，可从SED读取密钥2。理想地，该实现方式沿着上面建议的一般路径继续，这使其能够利用现有的TCG Opal方法(命令)来完成。例如，一种方式使用SED中的随机方法来生成密钥2。

然后,AdminSP.密钥2的PIN由主机个性化为它刚经由随机从SED读取的相同随机值。注意,通过从密钥2的默认值改变密钥2的PIN,主机已经承担存储该PIN的责任。为此,SED仅将由随机生成的最后随机数存储在易失性存储器中并且然后将生成的该最后随机数指定为候选密钥2。如果AdminSP.密钥2的PIN被设置为该相同值,则SED允许密钥2.PIN被改变为该新值。注意,如果主机尝试将AdminSP.密钥2PIN设置为除了由随机给出的最后随机数之外的值,则SED随后可选地拒绝接受该PIN改变并且发布指示命令失败的适当的错误代码。在这种情况下,SED可继续履行密钥2的PIN的默认值(即,全零=0x000…),这基本上将SED回复至相同的标准操作(即,像符合TCG的Opal的SED现今将操作的那样)。

[0084] 密码学

[0085] 注意,SED认证PIN的一种标准方式是通过对其进行散列并且将其与在其被首次设置(并且此后非易失性地存储在SED中)时计算的那个PIN的散列进行比较。以上讨论具有AdminSP.密钥2的PIN用作密钥2。注意,该特定PIN应当被与其他PIN不同地对待,因为此PIN的散列不应被存储在SED中,因为在将来的某个时刻,这可以可想象地变得不安全(即,如果散列在将来被破解,比如通过量子计算)。如果没有其他,则散列将提供测试蛮力猜测的方式。也就是说,不仅仅依赖于PIN的散列作为认证AdminSP.密钥2的PIN的方式是有正当理由的。因此,密钥2的PIN不能独立于验证MEK本身而被认证,这是为什么密钥2角色除了改变其自身的密码之外优选地不具有授权。这消除了认证该PIN的任何直接、即时的需要。

[0086] 最终,密钥1和密钥2被XOR、组合等以创建MEK。

[0087] 核实所得MEK为正确(例如,相对为一位关闭(one bit off),如果密钥2为一位关闭则其将发生)的一种方式,可使用密钥签名概念。密钥签名概念包括使用密钥来加密已知值,并且随后将所得的密文存储为该密钥的签名。

[0088] 在优选方式中,核实所得MEK为正确的是以这样的方式执行SED内部的密钥管理:具有可用的密钥2是对密钥1被成功解开的要求。例如,密钥流可通过从密钥2的密钥导出来创建,并且在密钥流以非易失性形式存储在设备内之前,该密钥流被用包装密钥结构XOR等。然后,构建到高级加密标准(AES)密钥包装内的8字节校验和用于验证密钥2和用于包装密钥1的任何其他包装密钥二者。因此,密钥2上的密钥导出优选地用于创建足够的衍生密钥材料以跨越完整的包装密钥结构。该密钥流与包装密钥结构(WKS)的XOR创建新的受保护的包装密钥结构(PWKS),其被存储以代替原始WKS。此时,PWKS中的任何位将具有50%的概率是对与错,并且对其的任何推测性‘校正’能够(以足够的收敛校正)基本上选定非常大量的密钥包装结构可能性中的任一个。因而,密钥流与包装密钥结构本身的XOR实际上是第二包装,这允许其中双重包装内部的数据是MEK的又一方式,并且通过执行两次解开来实现组合。

[0089] 应注意,在一些前述方式中,密钥2的PIN已经变成所谓的密码敏感参数(CSP)。如果存在在SED和主机之间传递的数据可被记录的任何机会,则应当利用飞行中数据加密(EDiF)的某种形式(诸如互联网协议安全(IPsec)、光纤信道安全协议(FC-SP)或传输层安全(TLS))来保护它们之间的信道。在一些数据中心中,没有关于数据被来回传递到该环境中的SED的担忧;担忧仅仅是在SED离开该受保护的环境之后该SED所发生的事情,这就是为什么密码擦除的绝对保证是期望的。

[0090] 注意,在XTS加密模式(例如XTS-AES-256)的情况下存在两个加密相关密钥,加密

密钥和单独的调整密钥。在一些方式中，可以从单个根密钥(经由密钥导出)生成这两个密钥。因此，256位的MEK可以被提供并且可以被用于(经由密钥导出)生成XTS-AES-256所要求的两个256位的密钥。

[0091] 已经实现本发明的各个方面的SED中的密码擦除选项包括以下中的一个或多个：

[0092] 1.如果用户想要对操作的SED进行密码擦除，则用户仅调用如本文中建议的这么做的多种不同方式之一。包装密钥结构被覆写，并且密钥1现在是不可恢复的。在这种情况下，不需要也擦除密钥2，MEK是不可恢复的，因为密钥1消失。

[0093] 2.如果用户想要对SED进行密码擦除(可能因为该SED是不响应命令的不可操作的SED，或者丢失的SED)，但是无论出于何种原因都不能进行‘1’，则用户现在具有另一选项—代替地擦除密钥2，密钥2是用户独立于SED控制的。在这种情况下，不需要擦除密钥1的所有包装版本；MEK是不可恢复的，因为密钥2消失。在这种情况下，即使某人在将来的某个时刻可能破解开出故障的SED的包装密钥结构并因此获得对密钥1的访问，他们所做的所有工作也都是徒劳，因为MEK保持不可用。为此，它们需要密钥2，而密钥2已经被擦除。因此，它们仍然留在访问客户数据的唯一可行路径是破解保护用户数据自身的密文的加密算法(例如XTS-AES-256)的情况中。

[0094] 3.如果用户特别担心密码擦除的安全性，则用户可选择删除密钥1和密钥2两者。如果担心密钥2可能已被记录(例如，飞行至SED，即使受到其安全(可能随后)被破坏的某个安全信道保护)，则这种情况可以是最可能的。但是，否则，由于所涉及的密码学，不应有要求删除密钥1和密钥2两者的原因。一个一般方式相当有弹性(例如，对于变得不可操作的SED)是始终尝试擦除密钥1和密钥2两者，但只要验证这两个擦除中的一个擦除成功就满足。

[0095] 用于磁记录带和其他便携式存储器的密码擦除

[0096] 如上所述，在一些方式中，加密数据存储在非易失性存储介质上，诸如磁记录介质(例如，带、盘)或者固态存储器(例如，NAND闪存、NVRAM等)。再次，以上呈现的任何操作、概念等可用于本方式中。

[0097] 现在参考图5，示出了根据一个方式的方法500的流程图。方法500可根据本发明以各种方式尤其在本文所述的其他附图中所描绘的任何环境中执行。当然，如本领域技术人员在阅读本说明书时将理解的，方法500中可包括比图5中具体描述的那些操作更多或更少的操作。

[0098] 方法500的步骤中的每个步骤可由操作环境的任何合适部件执行。例如，在不同方式中，方法500可以部分地或全部地由计算机、驱动器或其中具有一个或多个处理器的某个其他设备来执行。处理器(例如，以硬件和/或软件实现并且优选地具有至少一个硬件部件的(一个或多个)处理电路、(一个或多个)芯片、和/或(一个或多个)模块)可以在任何设备中用于执行方法500的一个或多个步骤。说明性处理器包括但不限于中央处理单元(CPU)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)等、其组合、或本领域已知的任何其他合适的计算设备。

[0099] 如图5所示，方法500可以以操作502开始，在操作502中，被配置为在存储介质上执行数据操作(诸如，从存储介质读取数据和/或向存储介质写入数据)的设备接收读取数据的请求，该数据以加密形式存储在存储介质上。所接收的请求可以仅仅是对数据的请求，或

者可以包括诸如密钥2之类的附加信息(见下文)。

[0100] 在操作504中,检索存储在存储介质上和/或与存储介质一起存储的第一密钥(密钥1)。此过程可包含从存储数据的介质、从物理上耦合到介质的存储器(诸如盒式存储器)等检索第一密钥。

[0101] 存储介质可以是本文公开的任何类型,例如,磁带、磁盘、NVRAM等。因此,设备可以是任何类型的数据存储设备,例如,带驱动器、SSD、HDD等。

[0102] 如上所述,在一些方式中,第一密钥以原始(未加密)的形式存储在存储介质上和/或与存储介质一起存储。在其他方式中,第一密钥以包装形式(混淆形式,例如,加密形式、密码保护形式等)存储在存储介质上和/或与存储介质一起存储。用于解开第一密钥的信息(诸如另一个密钥或PIN、密码等)可以被接收并且用于解开第一密钥。

[0103] 在优选方面中,设备被配置为禁止将第一密钥转移到设备的外部。然而,设备内部的控制器可从存储介质或耦合到存储介质的其他源访问第一密钥。

[0104] 在操作506中,从外部源接收第二密钥(密钥2)。外部源可以是任何外部源。例如,外部源可以是数据的请求者、密码存储装置、密码服务器、由用户(例如,经由键盘等)输入的密钥。

[0105] 在操作508中,使用第一密钥和第二密钥生成介质加密密钥(MEK)。任何已知技术可用于从第一密钥和第二密钥创建MEK。

[0106] 在操作510中,例如使用常规技术从存储介质读取密文形式的所请求的数据。

[0107] 在操作512,使用MEK解密所请求的数据的密文。数据可以被复制到缓冲器中并且然后被解密,可以在读取期间“即时”被解密(例如,操作510和512被同时执行),等等。

[0108] 在操作514中,将解密的数据输出,例如输出到数据的请求者等。

[0109] 如果第二数据要由该设备存储在存储介质上,则接收第二数据。可以从第二外部源接收第三密钥。如果是,则使用第一密钥和第三密钥生成第二介质加密密钥。使用第二介质加密密钥对数据进行加密,并且将加密数据写入存储介质。注意,第二外部源可与上述外部源相同,或由此不同。同样,第三密钥(如果第三密钥被接收到)可以与第二密钥不同或相同。

[0110] 下面提供图5的各种操作的方面。这些方面仅通过示例的方式呈现,并且不旨在是限制性的。此外,根据本发明的多种可能方式,可以以任何方式组合这些方面。例如,方法500可具有或结合与上面关于图4呈现的那些特征类似的特征,例如诸如密钥生成等。

[0111] 密钥1与存储介质一起存储,例如,存储在介质本身上和/或与存储介质一起存储在例如单独的存储器中。密钥1优选地以包装形式存储。例如,密钥1可存储在磁记录带的一部分上、带盒存储器中、或两者中。这样,密钥1可随磁记录带携带。类似地,对于NVRAM设备(诸如记忆棒、存储器卡等),密钥1可以存储在设备的NVRAM中、设备的单独存储器中等。

[0112] 密钥1优选地在操作于存储介质上的设备(例如,驱动器、计算机等)内部被创建。优选地,该设备被配置为不允许密钥1的任何外部可见性或将密钥1复制到该设备的外部,除了与其耦合的存储介质和/或存储器之外。优选地,设备将密钥1转移到与其耦合的存储介质和/或存储器并且从设备中删除密钥1。因此,在一些方式中,密钥1仅驻留于存储介质,诸如与可移动介质设备相关联的那些。

[0113] 在存储介质与设备本身成一体的设备(例如,自加密驱动器(SED)类型的HDD或

SSD、NVRAM模块等)的情况下,密钥1可与设备一起存储。例如,在(可能气密的)密封的SED壳体中,密钥1可被保持在通常矩形边界内的任何地方。在SSD的情况下,主非易失性存储器(其中存储用户数据)通常是NAND闪存。密钥1(可能以包装形式)也可存储在那里。在其他方式中,密钥1可替代地保持在外壳内部的单独(相对于用户数据)的非易失性存储器中,诸如:在不同的NAND闪存或NOR闪存芯片中;在磁性随机存取存储器(MRAM)中;在自旋转移力矩随机存取存储器(STT-RAM)中;在铁电随机存取存储器(FeRAM)中;在相变存储器(PCM)中;在电阻式随机存取存储器(RRAM)中;在其他形式的NVRAM(其比前述术语技术特异性低)中;等等。注意,密钥1也可以以可被擦除的ROM(诸如EEPROM)的形式存储。因此,在各种方式中,密钥1可被存储在与存储用户数据的存储介质不同类型的存储器中。

[0114] 在其他方式中,密钥1在设备外部被创建,并且被提供给设备并存储在设备中。

[0115] 可以在设备内部或在设备外部创建密钥2,或者通过联合来自设备内部和外部的贡献创建密钥2。

[0116] 密钥2被提供给和/或存储在带驱动器、计算机等中的易失性存储器(例如,SRAM)中,以允许驱动器、计算机等计算MEK。在一种方式中,密钥2可在每次被需要时输入到带驱动器、计算机等。在另一种方式中,一旦被提供给设备,密钥2可被保留在设备内部,存储在带驱动器、计算机等上的易失性存储器中,在这种情况下密钥2优选地是包装的。

[0117] 应当理解,本文中的不同方法可以用各种各样的存储器介质来实现,包括例如NVRAM技术,诸如NAND闪存存储器、NOR闪存存储器、相变存储器(PCM)、磁阻RAM(MRAM)和电阻式RAM(RRAM)。为了提供上下文并且仅为了帮助读者,可以参考非易失性存储器的类型来描述不同方式。这仅是通过举例的方式完成的,并且不应当被认为是对在权利要求中限定的本发明的限制。

[0118] 在一个说明性方式中,处于非易失性形式的密钥1仅以包装形式与存储介质一起存储。而密钥2虽然可以临时存储在易失性存储器中,但仅以非易失性形式存储在存储介质的外部。

[0119] 在存储介质上操作的驱动器、计算机等从存储介质检索密钥1并且接收或获得密钥2以允许计算MEK。

[0120] 优选地没有本地存储在驱动器、计算机等上的密钥2可以某种形式被提供给驱动器、计算机等。根据不同方面,可以有许多方式来完成,包括在先前部分中列出的任何方式。例如,一种方式是使驱动器、计算机等支持KMIP客户端并且通过安全信道从本领域已知类型的外部KMIP服务器(密钥管理器)接收密钥2。

[0121] 在一些方式中,密钥2本地存储在驱动器、计算机等上,优选地以包装形式。用于解开密钥2的密钥可从用户接收、从密钥管理器接收等。

[0122] 密钥1优选地以包装形式与存储介质一起存储并且在驱动器、计算机等被提供包装密钥(其可以是或取决于被提供给驱动器、计算机等以将不同用户认证为驱动器、计算机等支持的不同角色的个人标识号(PIN))时是不可解开的。因此,包装密钥的从驱动器、计算机等的外部提供的任何部分都被提供给驱动器、计算机等以允许解开密钥1。一旦驱动器、计算机等已经累积了计算MEK所需的所有所需信息(包括密钥2),驱动器、计算机等就计算MEK,并且然后能够解密现有密文以产生所得明文(例如,以响应主机读取),或将明文形式的新客户数据加密成密文(例如,以履行主机写入)。

[0123] 在一种方式中，密钥2是PIN，如前面部分中所述。

[0124] 替代实现方式包括使驱动器、计算机等在一些或所有情况下作为生成密钥2的源。在这种情况下，首先，可以从驱动器、计算机等的存储器读取密钥2。

[0125] 在带驱动器实现的方式中，优选的是密钥1来自带介质，而密钥2来自某个接口，并且MEK的计算在带驱动器内部，并且从不离开带驱动器。

[0126] 利用启用密码擦除的SED的写入

[0127] 虽然联合利用SED的示例性实现方式呈现了以下描述中的大部分，但是这仅通过示例的方式进行并且仅为读者提供上下文作为帮助。因此，下文呈现的概念和教导可同样适用于利用存储介质(诸如磁记录带、存储器卡等)的实现方式。

[0128] 现在参考图6，示出了根据一个方式的方法600的流程图。方法600可根据本发明以各种方式尤其在本文所述的其他附图中所描绘的任何环境中执行。例如，方法600可以具有或结合与以上关于图4所呈现的那些特征类似的特征，并且在一些方面中，可以使得设备能够执行图4和图6的操作。当然，如本领域技术人员在阅读本说明书时将理解的，方法600中可包括比图6中具体描述的那些操作更多或更少的操作。

[0129] 方法600的步骤中的每个步骤可由操作环境的任何合适部件执行。例如，在不同方式中，方法600可以部分地或全部地由计算机、驱动器或其中具有一个或多个处理器的某个其他设备来执行。处理器(例如，以硬件和/或软件实现并且优选地具有至少一个硬件部件的(一个或多个)处理电路、(一个或多个)芯片、和/或(一个或多个)模块)可以在任何设备中用于执行方法600的一个或多个步骤。说明性处理器包括但不限于中央处理单元(CPU)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)等、其组合、或本领域已知的任何其他合适的计算设备。

[0130] 如图6中所示，方法600可以以操作602开始，在操作602中，被配置为在存储介质上执行数据操作(诸如，从存储介质读取数据和/或向存储介质写入数据)的设备接收将数据以加密形式写入存储介质的请求。该请求可以简单地请求写入数据，或者可以包括诸如密钥2之类的附加信息(见下文)。

[0131] 在操作604中，存储在设备内的第一密钥(密钥1)例如从设备的存储器、从ASIC等被访问。如上所述，在一些方式中，第一密钥以原始(未加密)的形式存储在设备中。在其他方式中，第一密钥以包装形式(混淆形式，例如，加密形式、密码保护形式等)存储在设备中。用于解开第一密钥的信息(诸如另一个密钥、密码等)可被接收并且用于解开第一密钥。

[0132] 在优选方面中，设备被配置为禁止将第一密钥转移到设备的外部。然而，设备内部的控制器可以访问设备内部的第一密钥。

[0133] 在操作606中，从外部源接收第二密钥(密钥2)。外部源可以是任何外部源。例如，外部源可以是数据的请求者、密钥存储装置、密钥服务器、由用户(例如经由键盘)输入的密钥等。

[0134] 在操作608中，使用第一密钥和第二密钥生成介质加密密钥(MEK)。任何已知技术可用于从第一密钥和第二密钥创建MEK，例如通过对第一密钥和第二密钥进行XOR。

[0135] 在操作610中，使用介质加密密钥，所请求的数据的加密形式(即，密文)例如经由常规技术被写入存储介质。存储介质可以是本文公开的任何类型，例如，磁带、磁盘、NVRAM等。因此，设备可以是任何类型的数据存储设备，例如带驱动器、SSD、HDD、具有加密能力的

USB驱动器、NVRAM模块等。

[0136] 图6的各种操作和部件的方面优选地类似于上面在描述图4的部分中描述的那些，但可以包括来自本文任何其他部分的特征。这些方面仅通过示例的方式呈现，并且不旨在是限制性的。此外，根据本发明的多种可能方式，可以以任何方式组合这些方面。

[0137] 写入磁记录带和其他便携式存储器

[0138] 如上所述，在一些方式中，加密数据存储在非易失性存储介质上，诸如磁记录介质(例如，带、盘)或者固态存储器(例如，NAND闪存、NVRAM等)。再次，以上呈现的任何操作、概念等可用于本方式中。

[0139] 现在参考图7，示出了根据一个方式的方法700的流程图。方法700可根据本发明以各种方式尤其在本文所述的其他附图中所描绘的任何环境中执行。例如，方法700可以具有或结合与以上关于图4-图5所呈现的那些特征类似的特征，并且在一些方面中，可以使得设备能够执行图5和图7的操作。当然，如本领域技术人员在阅读本说明书时将理解的，方法700中可包括比图7中具体描述的那些操作更多或更少的操作。

[0140] 方法700的步骤中的每个步骤可由操作环境的任何合适部件执行。例如，在不同方式中，方法700可以部分地或全部地由计算机、驱动器或其中具有一个或多个处理器的某个其他设备来执行。处理器(例如，以硬件和/或软件实现并且优选地具有至少一个硬件部件的(一个或多个)处理电路、(一个或多个)芯片、和/或(一个或多个)模块)可以在任何设备中用于执行方法700的一个或多个步骤。说明性处理器包括但不限于中央处理单元(CPU)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)等、其组合、或本领域已知的任何其他合适的计算设备。

[0141] 如图7所示，方法700可以以操作702开始，在步骤702中，被配置为在存储介质上执行数据操作(诸如，从存储介质读取数据和/或向存储介质写入数据)的设备接收将数据以加密形式写入存储介质的请求。所接收的请求可以仅仅是写入数据的请求，或者可以包括诸如密钥2之类的附加信息(见下文)。

[0142] 在操作704中，检索存储在存储介质上和/或与存储介质一起存储的第一密钥(密钥1)。此过程可包含从存储数据的介质、从物理上耦合到介质的存储器(诸如盒式存储器)等检索第一密钥。

[0143] 存储介质可以是本文公开的任何类型，例如，磁带、磁盘、NVRAM等。因此，设备可以是任何类型的数据存储设备，例如，带驱动器、SSD、HDD、具有加密能力的USB驱动器、NVRAM模块等。

[0144] 如上所述，在一些方式中，第一密钥以原始(未加密)的形式存储在存储介质上和/或与存储介质一起存储。在其他方式中，第一密钥以包装形式(混淆形式，例如，加密形式、密码保护形式等)存储在存储介质上和/或与存储介质一起存储。用于解开第一密钥的信息(诸如另一个密钥或PIN、密码等)可以被接收并且用于解开第一密钥。

[0145] 在优选方面中，设备被配置为禁止将第一密钥转移到设备的外部。然而，设备内部的控制器可从存储介质或耦合到存储介质的其他源访问第一密钥。

[0146] 在操作706中，从外部源接收第二密钥(密钥2)。外部源可以是任何外部源。例如，外部源可以是数据的请求者、密钥存储装置、密钥服务器、由用户(例如，经由键盘等)输入的密钥。

[0147] 在操作708中，使用第一密钥和第二密钥生成介质加密密钥(MEK)。任何已知技术可用于从第一密钥和第二密钥创建MEK。

[0148] 在操作710中，使用介质加密密钥，所请求的数据以密文形式(例如，经由常规技术)被写入存储介质。

[0149] 图7的各种操作和部件的方面优选地类似于上面在描述图5的部分中描述的那些，但可以包括来自本文任何其他部分的特征。这些方面仅通过示例的方式呈现，并且不旨在是限制性的。此外，根据本发明的多种可能方式，可以以任何方式组合这些方面。

[0150] 根据各种方式的系统包括被配置为在存储介质上执行数据操作的设备，该设备具有处理器和与处理器集成、可由处理器执行、或与处理器集成且可由处理器执行的逻辑，该逻辑被配置为使设备执行上述操作(例如图4-图7的操作)中的一些或全部。

[0151] 根据各种方式的用于实现密码擦除和/或执行密码擦除的计算机程序产品包括计算机可读存储介质，该计算机可读存储介质具有随其体现的程序指令，这些程序指令可由被配置为执行前述操作(例如图4-图7的操作)中的一些或全部的设备来执行。

[0152] 示例性实施方式

[0153] 根据一种方式的用于保护诸如自加密设备(SED)之类的具有加密能力的存储设备的说明性处理包括以下操作：

[0154] 1.生成密钥1，并将该密钥1以在存储设备内部安全的方式存储在存储设备内部。通常，密钥1将永远不会以明文形式存储在非易失性存储器中。

[0155] 2.生成密钥2，并将该密钥2存储在存储设备外部，其中：

[0156] A.如果密钥2是在存储设备内部创建的，则使密钥2从存储设备被检索

[0157] B.如果密钥2是在存储设备外部创建的，则使密钥2在被需要时被提供给存储设备

[0158] 3.存储设备使用密钥1和密钥2计算介质加密密钥(MEK)

[0159] 4.MEK被直接或间接用于对数据进行加密以生成密文，以及对密文进行解密以生成明文。

[0160] 根据一种方式的在电力丧失或冷启动之后用于重新获得对诸如自加密设备(SED)之类的具有加密能力的存储设备的访问的说明性处理包括以下操作：

[0161] 1.使密钥2被提供给存储设备

[0162] 2.访问存储设备内部的密钥1，这可涉及密码地解开密钥1，其可能需要密钥2以及一个或多个访问密钥(例如，PIN)

[0163] 3.存储设备使用密钥1和密钥2计算介质加密密钥(MEK)

[0164] 4.MEK被直接或间接用于对数据进行加密以生成密文，以及对密文进行解密以生成明文。

[0165] 用于使设备退休或使被盗设备安全的处理

[0166] 根据一种方式的当存储设备要被引退(例如，因为其后台错误率已经变得太大(例如，其可能由于太多写入周期而发生)，或者可能因为其“出故障”并且未能成功完成某些操作)时可以执行的说明性处理包括以下操作：

[0167] 1.向存储设备发送指示其对其密钥1进行密码擦除的命令

[0168] 2.密钥1的密码擦除是否成功完成?如果：

[0169] • 是，在该MEK下加密的数据已经被成功地密码擦除

[0170] • 在这种情况下，虽然不需要破坏密钥2，但是这也可以完成

[0171] • 否，在这种情况下，不能信任已经发生任何密码擦除：

[0172] • 销毁在存储设备外部的密钥2，并且因此通过外部手段密码擦除存储设备

[0173] • 将存储设备断电或冷启动以确保存储设备不保留密钥的易失性映像。

[0174] 注意，密钥删除也可以按相反的顺序完成，其中首先销毁密钥2，优选地随后尝试删除密钥1。根据一种方式的说明性处理包括以下操作：

[0175] 1.销毁在存储设备外部的密钥2，并且因此通过外部手段密码擦除存储设备

[0176] 2.向存储设备发送指示其对其密钥1进行密码擦除的命令

[0177] 3.密钥1的密码擦除是否成功完成?如果：

[0178] • 是，在该MEK下加密的数据已经通过破坏密钥1和密钥2而被成功地密码擦除

[0179] • 将存储设备断电或冷启动以确保存储设备不保留任何密钥的易失性映像

[0180] • 否，但是存储设备外部的密钥2已经被破坏，并且因此通过外部手段实现了密码擦除存储设备。

[0181] 还应注意，如果存储设备被盗，或者在其从存储系统移除之前未被密码擦除并且然后例如在传送到另一位置时丢失了，则由于不再可能通过破坏密钥1对数据进行密码擦除，因为人们没有对存储设备的物理访问，所以人们必须替代地销毁密钥2，这即使在没有对存储设备的物理访问的情况下也是可能的。

[0182] 图8描绘了在没有本发明的情况下当前可实现的示例，而图9和图10描绘了使用本发明的一种或多种方式可操作地可实现的示例。图8至图10中的图表是不言而喻的，并且仅仅通过示例的方式呈现。

[0183] 本发明可以是任何可能的技术细节集成度的系统、方法和/或计算机程序产品。计算机程序产品可包括其上具有用于使处理器执行本发明的方面的计算机可读程序指令的(一个或多个)计算机可读存储介质。

[0184] 计算机可读存储介质可以是可保留和存储供指令执行设备使用的指令的有形设备。计算机可读存储介质可以是，例如但不限于，电子存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备、或者上述的任意合适的组合。计算机可读存储介质的更具体示例的非穷尽列表包括以下各项：便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或闪存存储器)、静态随机存取存储器(SRAM)、便携式紧凑盘只读存储器(CD-ROM)、数字通用盘(DVD)、记忆棒、软盘、诸如其上记录有指令的槽中的凸出结构或穿孔卡之类的机械编码设备、以及上述的任何合适的组合。如本文所使用的计算机可读存储介质不应被解释为暂时性信号本身，诸如无线电波或其他自由传播的电磁波、通过波导或其他传输介质传播的电磁波(例如，穿过光纤线缆的光脉冲)或通过电线传输的电信号。

[0185] 本文中所描述的计算机可读程序指令可以从计算机可读存储介质下载到相应的计算/处理设备，或者经由网络(例如，互联网、局域网、广域网和/或无线网络)下载到外部计算机或外部存储设备。网络可以包括铜传输线缆、光传输纤维、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配器卡或网络接口接收来自网络的计算机可读程序指令，并转发计算机可读程序指令以存储在相应计算/处理设备内的计算机可读存储介质中。

[0186] 用于执行本发明的操作的计算机可读程序指令可以是汇编指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、用于集成电路的配置数据、或以一种或多种编程语言的任何组合编写的源代码或目标代码，这些编程语言包括面向对象的编程语言(诸如Smalltalk、C++等)和过程性编程语言(诸如“C”编程语言或类似编程语言)。计算机可读程序指令可以完全地在用户的计算机上执行、部分在用户的计算机上执行、作为独立软件包执行、部分在用户的计算机上并且部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在后一种情况下，远程计算机可通过任何类型的网络(包括局域网(LAN)或广域网(WAN))连接至用户的计算机，或者可连接至外部计算机(例如，通过使用互联网服务提供商的互联网)。在一些实施例中，包括例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA)的电子电路系统可以通过利用计算机可读程序指令的状态信息来使电子电路系统个性化来执行计算机可读程序指令，以便执行本发明的方面。

[0187] 下面将参照根据本发明的实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图描述本发明的方面。将理解，流程图和/或框图的每个框以及流程图和/或框图中的框的组合可以由计算机可读程序指令实现。

[0188] 这些计算机可读程序指令可被提供给计算机的处理器或其他可编程数据处理装置以产生机器，使得经由计算机的处理器或其他可编程数据处理装置执行的指令创建用于实现在流程图和/或框图的一个或多个框中指定的功能/动作的手段。也可以把这些计算机可读程序指令存储在计算机可读存储介质中，这些指令可以引导计算机、可编程数据处理装置、和/或其他设备以特定方式起作用，使得其中存储有指令的计算机可读存储介质包括包含实现流程图和/或框图中的一个或多个框中指定的功能/动作的方面的指令的制品。

[0189] 也可以把计算机可读程序指令加载到计算机、其他可编程数据处理装置、或其他设备上，以使得在计算机、其他可编程装置或其他设备上执行一系列操作步骤，以产生计算机实现的处理，使得在计算机、其他可编程装置或其他设备上执行的指令实现流程图和/或框图中的一个或多个框中指定的功能/动作。

[0190] 附图中的流程图和框图示出了根据本发明的各种实施例的系统、方法和计算机程序产品的可能实现方式的架构、功能和操作。对此，流程图或框图中的每个框可表示指令的模块、段或部分，其包括用于实现指定的(一个或多个)逻辑功能的一个或多个可执行指令。在一些替代实现方式中，框中标注的功能可以不按照图中标注的顺序发生。例如，连续示出的两个方框实际上可以作为一个步骤完成，同时、基本上同时、以部分或完全时间上重叠的方式执行，或者框有时可以以相反的顺序执行，这取决于所涉及的功能。也要注意的是，框图和/或流程图中的每个框以及框图和/或流程图中的框的组合可以通过执行指定的功能或动作或者执行专用硬件与计算机指令的组合的专用的基于硬件的系统来实现。

[0191] 此外，根据各种实施例的系统可包括处理器和与处理器集成和/或可由处理器执行的逻辑，逻辑被配置为执行本文所述的处理步骤中的一个或多个。处理器可以具有如本文中所描述的任何配置，诸如包括许多部件(诸如处理硬件、存储器、I/O接口等)的离散处理器或处理电路。通过与其集成，意味着处理器具有嵌入在其中的作为硬件逻辑的逻辑，诸如专用集成电路(ASIC)、FPGA等。通过可由处理器执行，意味着逻辑是硬件逻辑；软件逻辑，诸如固件、操作系统的一部分、应用程序的一部分；等等，或可由处理器访问并且被配置为

在由处理器执行时使处理器执行某种功能的软件逻辑和硬件的某种组合。软件逻辑可以存储在任何存储器类型的本地和/或远程存储器上，如本领域中已知的。可以使用本领域已知的任何处理器，诸如软件处理器模块和/或硬件处理器(诸如ASIC、FPGA、中央处理单元(CPU)、集成电路(IC)、图形处理单元(GPU)等)。

[0192] 将清楚的是，前述系统和/或方法的各种特征可以以任何方式进行组合，从而从以上呈现的描述中创建多个组合。

[0193] 还将理解，本发明的方面可以以代表客户部署的服务的形式来提供，以按需提供服务。

[0194] 已经出于说明的目的呈现了本发明的各种方面的描述，但这并不旨在是详尽的或限于所公开的方式。在不脱离所描述的方面的范围的情况下，许多修改和变化对于本领域普通技术人员来说是清楚的。本文使用的术语被选择来最好地解释各种方式的原理、实际应用或对在市场中发现的技术的技术改进，或者使得本领域的其他普通技术人员能够理解本文公开的方式。

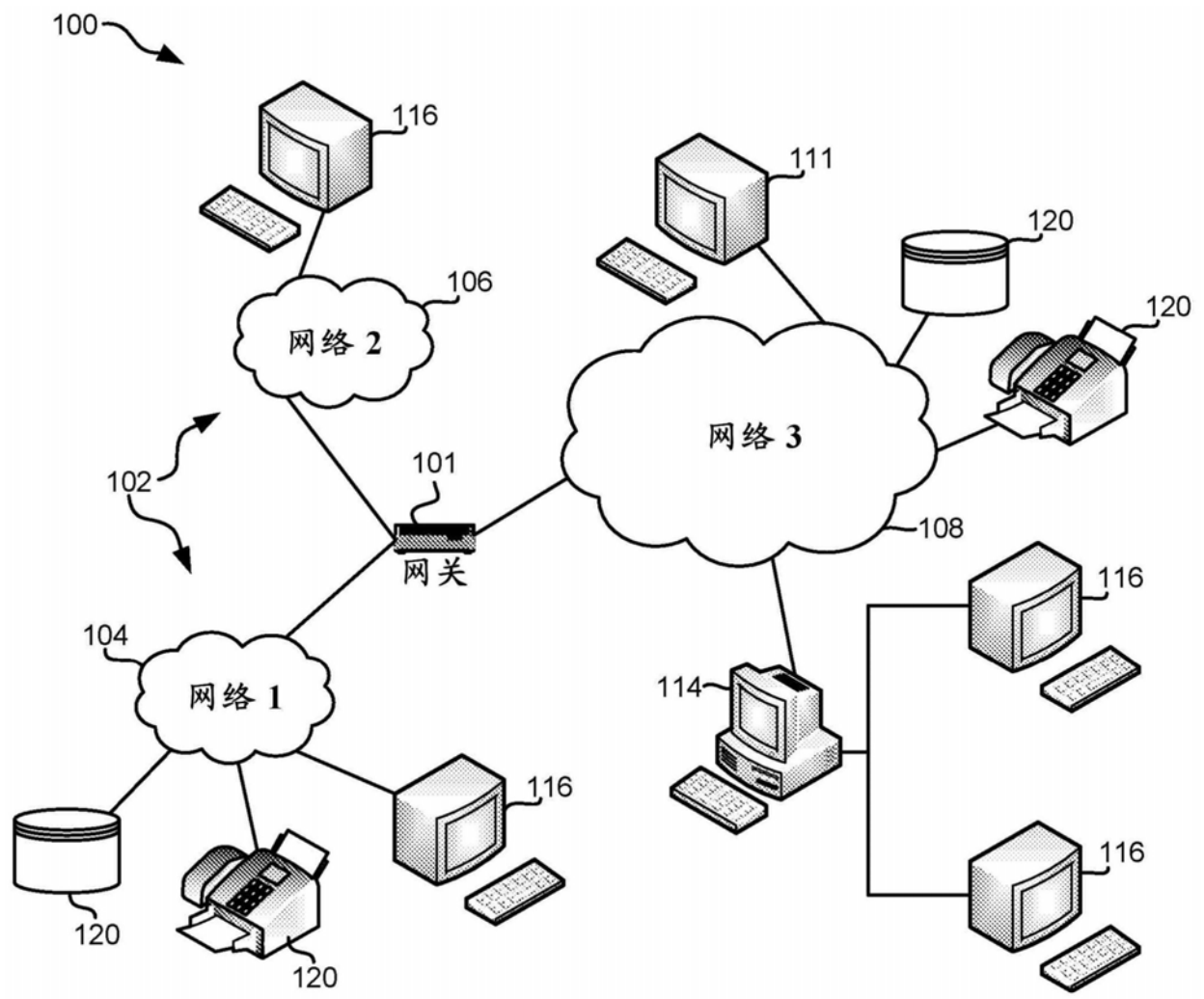

100
116
106
网络 2
111
120
120
网络 3
102
101
网关
108
104
网络 1
116
114
116
116
120
120

图1

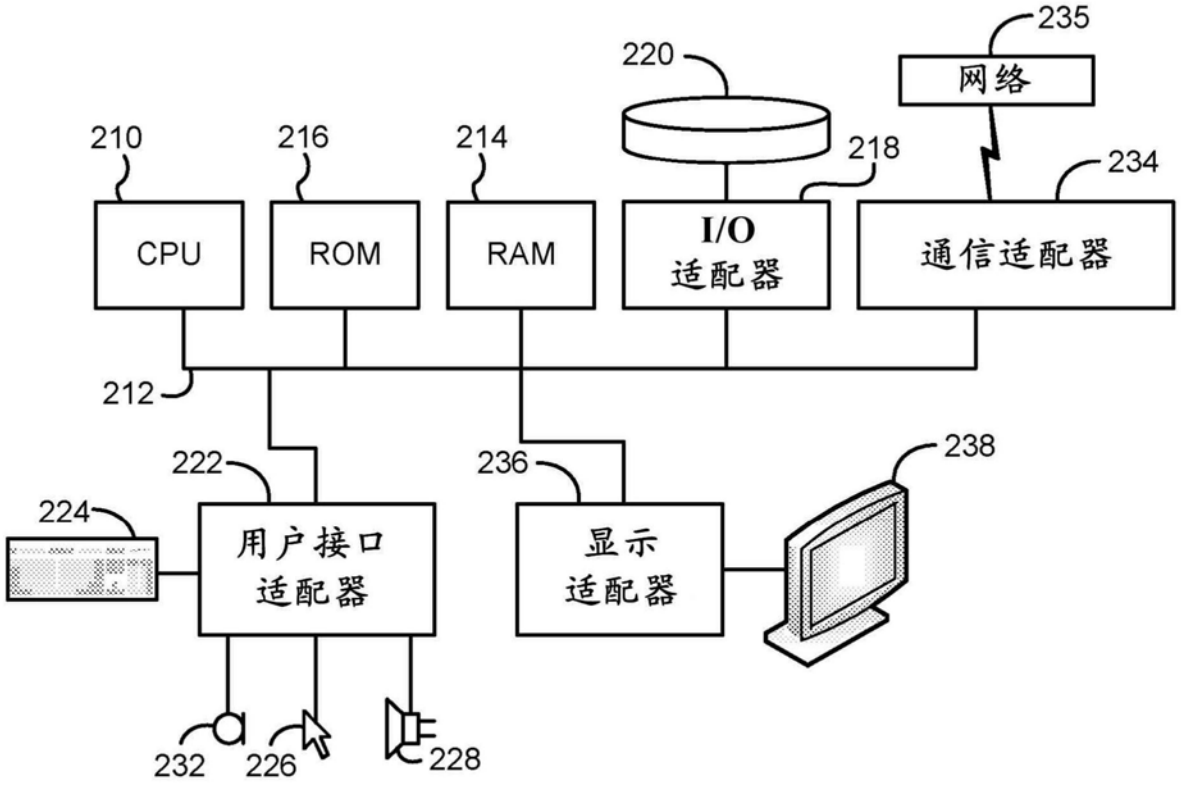

235
网络
220
210
216
214
218
234
CPU
ROM
RAM
I/O
适配器
通信适配器
212
222
236
238
224
用户接口
适配器
显示
适配器
232
226
228

图2

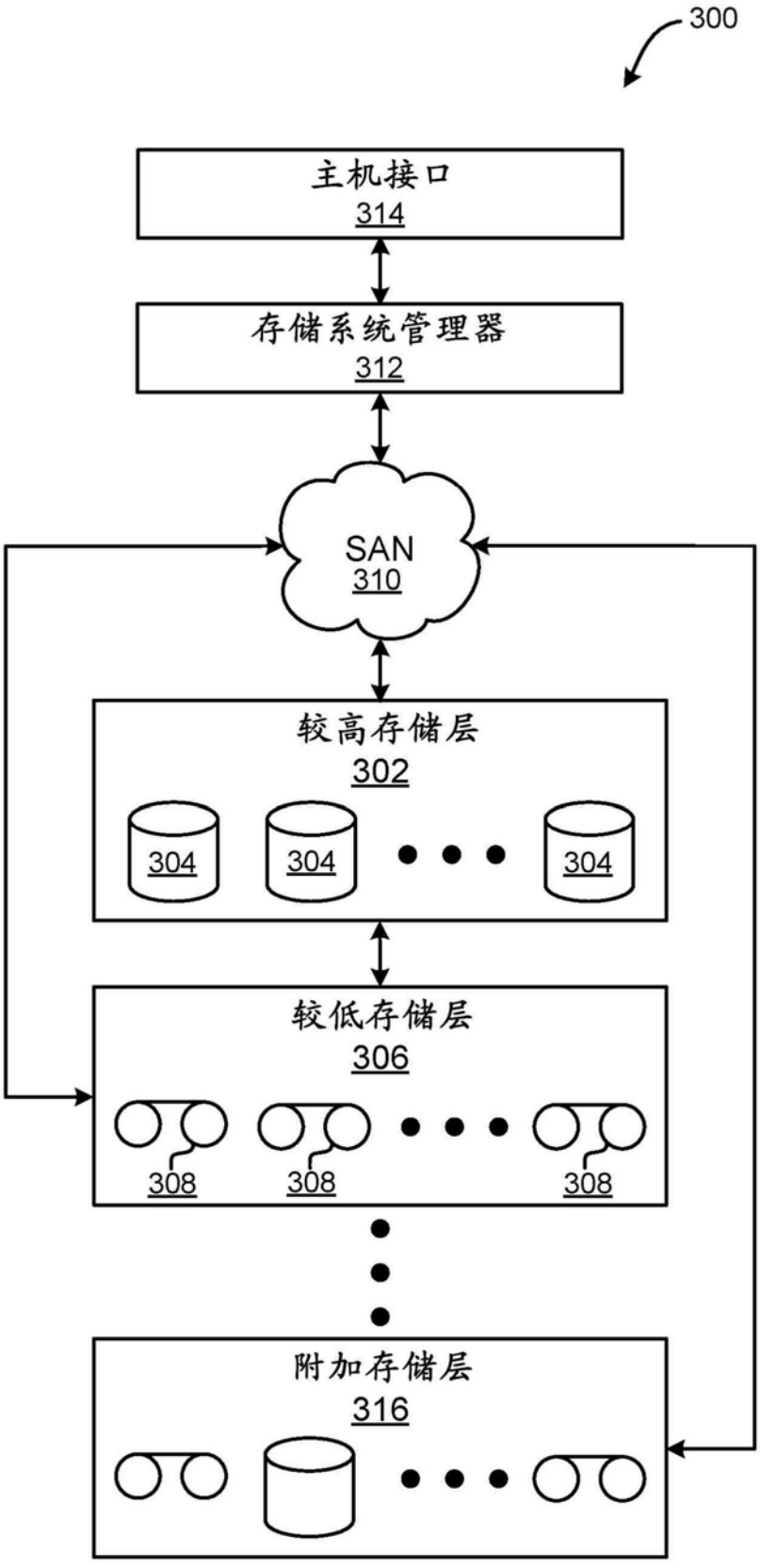

300
主机接口
314
存储系统管理器
312
SAN
310
较高存储层
302
304
304
304
较低存储层
306
308
308
308
附加存储层
316

图3

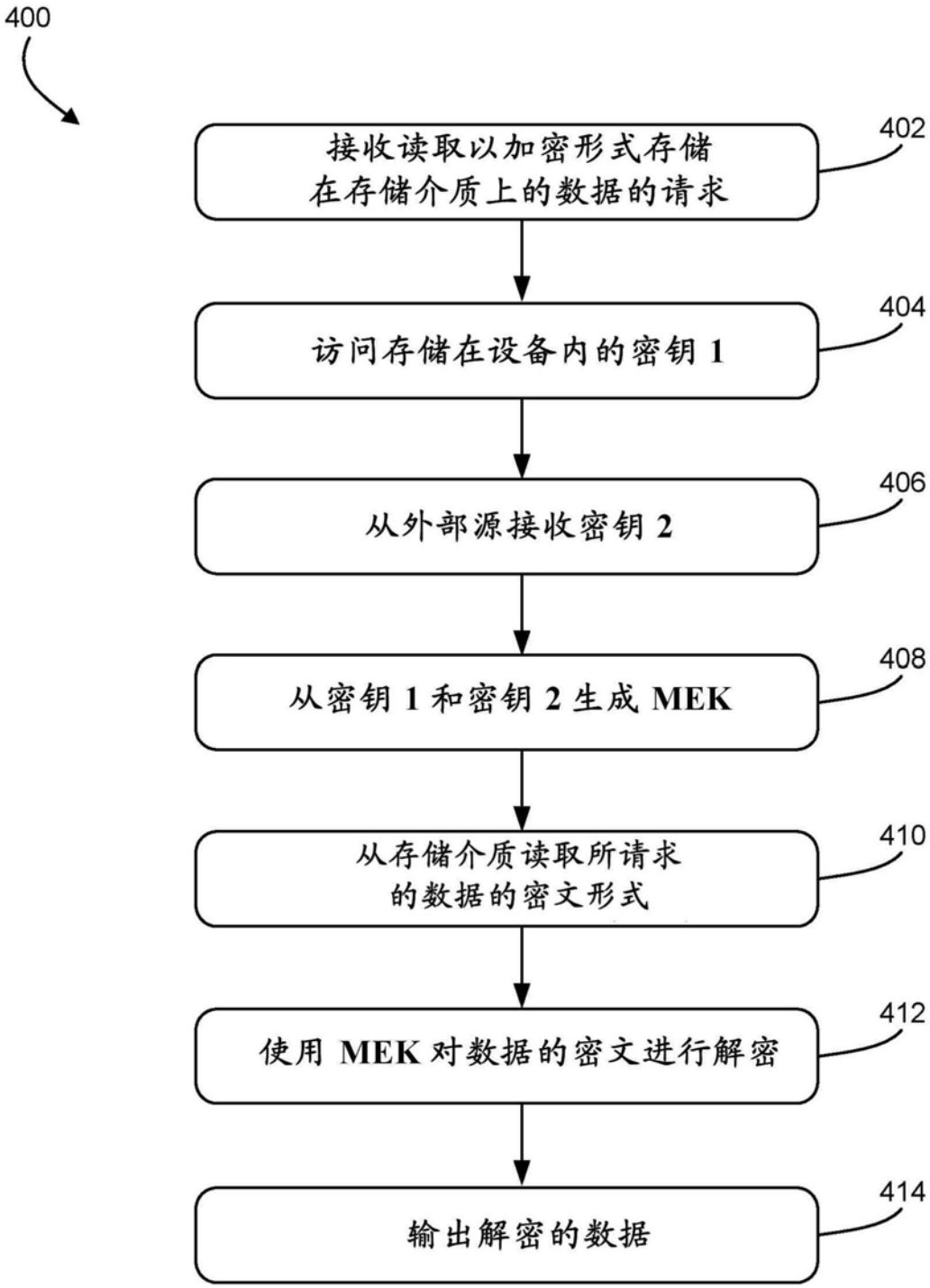

400
接收读取以加密形式存储
在存储介质上的数据的请求
402
访问存储在设备内的密钥 1
404
从外部源接收密钥 2
406
从密钥 1 和密钥 2 生成 MEK
408
从存储介质读取所请求
的数据的密文形式
410
使用 MEK 对数据的密文进行解密
412
输出解密的数据
414

图4

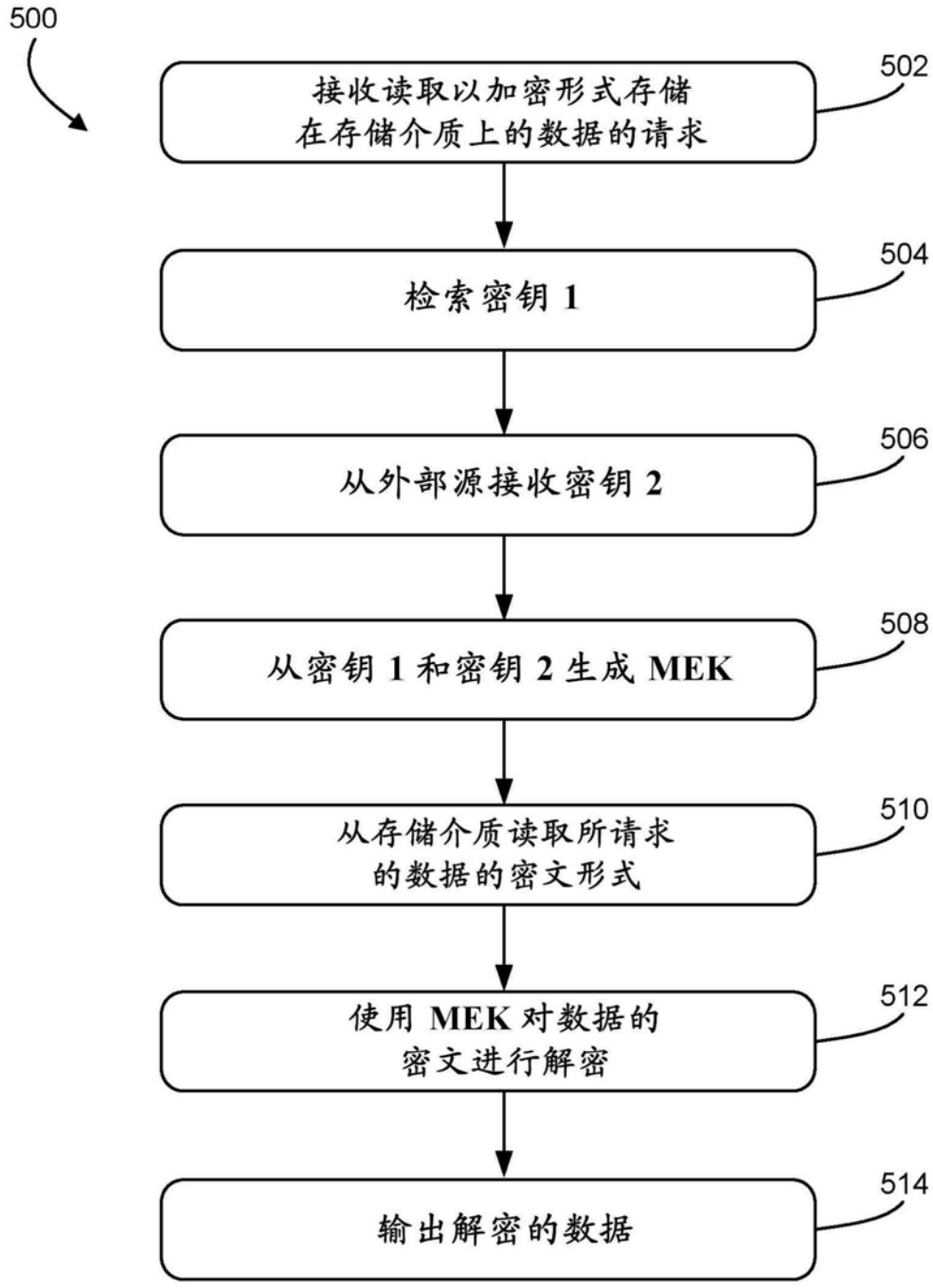

500
接收读取以加密形式存储
在存储介质上的数据的请求
502
检索密钥 1
504
从外部源接收密钥 2
506
从密钥 1 和密钥 2 生成 MEK
508
从存储介质读取所请求
的数据的密文形式
510
使用 MEK 对数据的
密文进行解密
512
输出解密的数据
514

图5

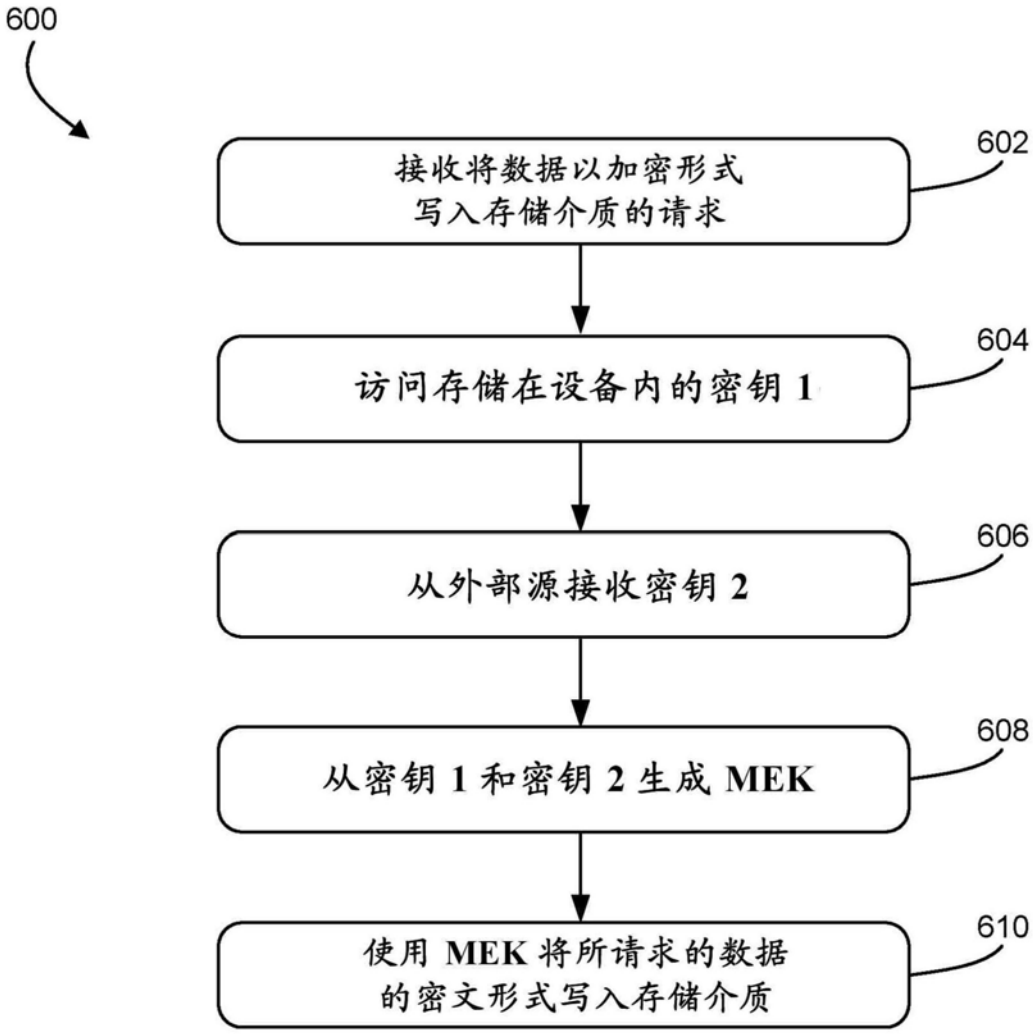

600
接收将数据以加密形式写入存储介质的请求
602
访问存储在设备内的密钥 1
604
从外部源接收密钥 2
606
从密钥 1 和密钥 2 生成 MEK
608
使用 MEK 将所请求的数据的密文形式写入存储介质
610

图6

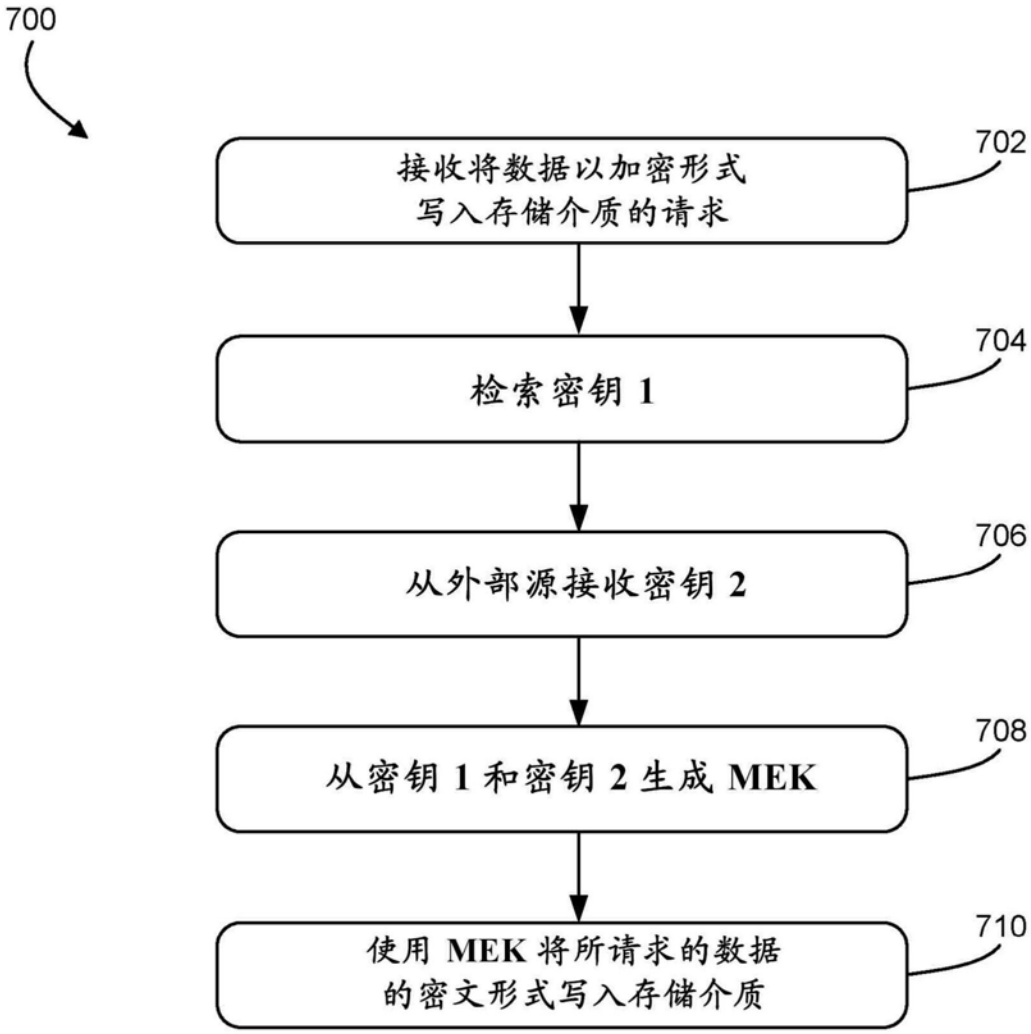

700
接收将数据以加密形式写入存储介质的请求
702
检索密钥 1
704
从外部源接收密钥 2
706
从密钥 1 和密钥 2 生成 MEK
708
使用 MEK 将所请求的数据的密文形式写入存储介质
710

图7

担心的情况	在系统级别启用的加密？	首先做什么？	格式化成功了吗？	在格式化后安全了吗？	其次做什么？	然后 SED 安全了吗？
被盗 SED *3	是	什么也不能做	未应用	未应用	什么也不能做	部分 *1
出故障的 SED	是	包括密码擦除的格式化	否 *2	部分 *1	什么也不能做	部分 *1
			是	是	发送至退休者	是 *4

图例：

*1 SED 安全取决于攻击者从未获得对包装密钥的访问
并且从未能破解在密钥包装中使用的密码

*2 除非 SED 已以阻止其接收命令或用好状态
响应的方式出故障，否则格式化应当成功

*3 如果出故障的 SED 未被格式化，并且在其被发送至
退休者（例如，引退（擦除或破坏）介质或驱动器的制造商等）
时的传送中丢失了，则其基本上处于与被盗相同的困境

*4 SED 是安全的，因为包装 MEK 被覆写了并且
因此是不可恢复的，无论某人是否也有对包装密钥的访问

图8

担心的情况	在系统级别启用的加密？	首先做什么？	格式化成功了吗？	在格式化后安全了吗？	其次做什么？	然后 SED 安全了吗？
被盗 SED *3	是	前往下一步	未应用	未应用	破坏密钥 2	是 *5
出故障的 SED	是	包括密码擦除的格式化	否 *2	部分 *1	破坏密钥 2	是 *5
			是	是	发送至退休者	是 *4

图例：

*1 SED 安全取决于攻击者从未获得对包装密钥的访问并且从未能破解在密钥包装中使用的密码

*2 除非 SED 已以阻止其接收命令或用好状态响应的方式出故障，否则格式化应当成功

*3 如果出故障的 SED 未被格式化，并且在其被发送至退休者时的传送中丢失了，则其基本上处于与被盗相同的困境

*4 SED 是安全的，因为包装 MEK 被覆写了并且因此是不可恢复的，无论某人是否也有对包装密钥的访问

*5 SED 是安全的，因为密钥 2 已被破坏

图9

担心的情况	在系统级别启用的加密？	首先做什么？	其次做什么？	格式化成功了吗？	在格式化后安全了吗？	然后 SED 安全了吗？
被盗 SED *3	是	破坏密钥 2	前往下一步	未应用	未应用	是 *5
出故障的 SED	是	破坏密钥 2	包括密码擦除的格式化	否 *2	部分 *1	是 *5
				是	是	是 *4

图例：

*1 SED 安全取决于攻击者从未获得对包装密钥的访问并且从未能破解在密钥包装中使用的密码

*2 除非 SED 已以阻止其接收命令或用好状态响应的方式出故障，否则格式化应当成功

*3 如果出故障的 SED 未被格式化，并且在其被发送至退休者时的传送中丢失了，则其基本上处于与被盗相同的困境

*4 SED 是安全的，因为包装 MEK 被覆写了并且因此是不可恢复的，无论某人是否也有对包装密钥的访问

*5 SED 是安全的，因为密钥 2 已被破坏

图10