利用自加密驱动器加密盘驱动器上的数据的方法和系统

本发明提供了一种利用自加密驱动器加密盘驱动器上的数据的方法和系统。所述方法包括，对计算设备的数据组件进行加密。所述方法还包括，把已加密数据组件与计算设备的加密密钥索引相关联。此外，所述方法还包括，接收对应于数据组件的给定逻辑块地址的加密密钥索引。所述方法还包括，基于针对盘驱动器的数据组件的加密密钥索引确定将被用来对数据组件进行加密的加密密钥。
1. 一种用于利用自加密驱动器 (SED) 对盘驱动器上的数据进行加密的方法，所述方法包括以下步骤：

通过一个或多个计算机处理器对计算设备的数据组块进行加密；

通过所述一个或多个计算机处理器把已加密数据组块与计算设备的加密密钥索引相关联，其中所述加密密钥索引指定要用于每一个组块的加密密钥，以及其中所述加密密钥被保持在所述自加密驱动器中并且不离开所述自加密驱动器；

通过所述一个或多个计算机处理器接收对应于数据组块的索引逻辑块地址的加密密钥索引；其中数据组块被读取或写入到盘驱动器上的逻辑块地址；以及

通过所述一个或多个计算机处理器，基于针对盘驱动器的数据组块的加密密钥索引来确定被用来对应数据组块进行加密的加密密钥。

2. 如权利要求1所述的方法，其中，所述加密密钥索引为计算设备的数据组块提供安全性，并且其中由加密密钥索引保护的数据组块不需要是紧接的，所有组块也不需要具有相同的尺寸。

3. 如权利要求1所述的方法，其中，通过一个或多个计算机处理器接收对应于数据组块的逻辑块地址的加密密钥索引，其中数据组块的逻辑块地址被读取或写入到盘驱动器的步骤还包括以下步骤：通过所述一个或多个计算机处理器访问盘驱动器的给定卷和逻辑块地址的逻辑地址范围上的数据组块。

4. 如权利要求3所述的方法，其中，所述卷是盘驱动器的存储元件，并且其中所述卷的存储元件是能够读/从盘驱动器进行写入/读取的盘驱动器的可用存储容量。

5. 如权利要求4所述的方法，其中，所述卷被存储在一个或多个盘驱动器上，并且其中所述一个或多个盘驱动器能够包含属于多个卷的数据。

6. 如权利要求1所述的方法，其还包括以下步骤：

通过所述一个或多个计算机处理器接收所述逻辑块地址和加密密钥索引以作为盘驱动器的输入；以及

通过所述一个或多个计算机处理器将所接收到的逻辑块地址和已加密密钥索引组合成经过修改的逻辑块地址，其中所述经过修改的逻辑块地址被盘驱动器接受。

7. 如权利要求1所述的方法，其中，所述盘驱动器是自加密驱动器，其对保持在所述自加密驱动器内部的加密密钥和所述密钥索引数据进行读出，其中所述自加密驱动器利用内部密码密钥对写入到其中的数据进行加密并且对从其读取的已加密数据进行解密。

8. 一种用于利用自加密驱动器 (SED) 对盘驱动器上的数据进行加密的计算机系统，所述计算机系统包括：

一个或多个处理器、一个或多个计算机可读存储器、一个或多个计算机可读有形存储设备以及程序指令，所述程序指令被存储在所述一个或多个存储设备的至少其中之一上，以便由所述一个或多个处理器的至少其中之一经由所述一个或多个存储器的至少其中之一来执行，所述程序指令包括：

用以对计算设备的数据组块进行加密的程序指令；

用以把已加密数据组块与计算设备的加密密钥索引相关联的程序指令，其中所述加密密钥索引指定要用于每一个组块的加密密钥，以及其中所述加密密钥被保持在所述自加密驱动器中并且不离开所述自加密驱动器；

9. 如权利要求8所述的计算机系统，其特征在于所述程序指令进一步包括以下步骤：

通过所述一个或多个计算机处理器接收所述逻辑块地址和加密密钥索引以作为盘驱动器的输入；以及

通过所述一个或多个计算机处理器将所接收到的逻辑块地址和已加密密钥索引组合成经过修改的逻辑块地址，其中所述经过修改的逻辑块地址被盘驱动器接受。
用以接收对应于数据组块的给定逻辑块地址的加密密钥索引的程序指令，其中数据组块被读取或写入到盘驱动器上的逻辑块地址，以及

用以基于针对盘驱动器的数据组块的加密密钥索引来确定被用来对数据组块进行加密的加密密钥的程序指令。

9. 如权利要求8所述的计算机系统，其中，所述加密密钥索引为计算设备的数据组块提供安全性，并且其中由加密密钥索引保护的数据组块不需是连接的，所有组块也不必具有相同的尺寸。

10. 如权利要求8所述的计算机系统，其中，用以接收对应于数据组块的逻辑块地址的加密密钥索引，其中数据组块的逻辑块地址被读取或写入到盘驱动器的程序指令还包括：

- 用以通过一个或多个计算机处理器访问盘驱动器的逻辑块地址的逻辑地址范围上的数据组块的程序指令。

11. 如权利要求10所述的计算机系统，其中，所述卷是盘驱动器的存储元件，并且其中所述卷的存储元件能够向/从盘驱动器进行写入/读取的盘驱动器的可用存储容量。

12. 如权利要求11所述的计算机系统，其中，所述卷被存储在一个或多个盘驱动器上，并且其中所述一个或多个盘驱动器能够包含属于多于一个的卷的数据。

13. 如权利要求8所述的计算机系统，其还包括：

- 用以接收所述逻辑块地址和加密密钥索引以作为盘驱动器的输入的程序指令；以及

- 用于将所接收到的逻辑块地址和加密密钥索引组合成经过修改的逻辑块地址的程序指令，其中所述经过修改的逻辑块地址被盘驱动器接受。

14. 如权利要求8所述的计算机系统，其中，所述盘驱动器是自加密驱动器，其对保持在所述自加密驱动器内部的加密密钥和所述加密密钥索引进行映射，并且其中所述自加密驱动器利用内部密码密钥对写入到其中的数据进行加密并且对从中读取的已加密数据进行解密。

15. 一种用于利用自加密驱动器(SED)对盘驱动器上的数据进行加密的系统，其包括用于实施权利要求1-7中的任一方法的所有步骤的部件。
利用自加密驱动器加密盘驱动器上的数据的方法和系统

技术领域
[0001] 本发明总体上涉及计算系统，更具体来说涉及利用自加密驱动器 (SED) 对存储设备上的数据进行多卷加密。

背景技术
[0002] 存储系统通常包括一个或多个存储设备，可以按照期望将数据输入其中并且可以从中获得数据。所述存储系统可以根据多种存储架构来实施，其中包括但不限于网络附属存储环境、存储区域网络以及直接附属于客户端或主机计算机的盘套件。存储系统通常是盘驱动器，其中术语“盘”通常描述整装式旋转磁性介质存储设备。存储系统内的盘通常被组织成一个或多个组，其中每一组被操作为一个独立存储单元阵列 (RAID)。此外，大多数RAID实现方式增强了数据存储的可靠性和完整性，这是通过在RAID中的给定数目的物理盘上的数据“条带”的冗余写入以及关于分条数据的冗余信息的适当存储而实现的。所述冗余信息允许在存储系统不可操作或故障时恢复丢失的数据。此外，存储系统的盘或存储阵列是包含多个盘驱动器的盘存储系统。举例来说，通过使用附加的冗余组件 (控制器、电力供应部件、风扇等等)，盘阵列提供了增强的可用性、弹性和可维护性，并且常常达到了从设计中消除所有单点故障 (SPOF) 的程度。

[0003] 此外，存储系统通常为计算系统提供数据的逻辑卷，其中每一个数据卷代表逻辑存储单元，但是实际上通常被实施在例如RAID的几个物理设备上。相反，存储系统的自加密盘 (SED) 驱动器支持对驱动器中的相对较小数目的邻接数据块进行加密。例如来说，SED允许驱动器的受保护硬件内的集成的加密和访问控制。自加密驱动器还为全盘加密提供了行业优选的解决方案，从而在机器或驱动器丢失或被盗时以及在改变用途 (re-purposed)、保修和使用寿命结束后保护数据。

发明内容
[0004] 在一个实施例中，提供一种用于利用自加密驱动器 (SED) 对盘驱动器的数据进行加密的方法。所述方法包括，通过一个或多个计算机处理器对计算设备的数据块进行加密。所述方法还包括，通过一个或多个计算机处理器把加密数据块与设备的加密密钥索引相关联，所述加密密钥索引指定将要用于每一个数据块的加密密钥。所述方法还包括，通过一个或多个计算机处理器接收对应于数据块的给定逻辑块地址的加密密钥索引，其中数据块被读取或写入到盘驱动器上的逻辑块地址。所述方法还包括，通过一个或多个计算机处理器，基于针对盘驱动器的数据块的加密密钥索引来确定将被用来对数据块进行加密的加密密钥。

[0005] 在另一个实施例中，提供一种用于利用自加密驱动器 (SED) 对盘驱动器上的数据进行加密的计算机系统。所述计算机系统包括一个或多个处理器，一个或多个计算机可读存储器、一个或多个计算机可读有形存储设备以及程序指令，所述程序指令被存储在所述一个或多个存储设备的至少其中之一上，以便由所述一个或多个处理器的至少其中之一经
由所述一个或多个存储器的至少其中之一来执行。所述计算机系统还包括用以对计算设备上的数据组块进行加密的程序指令。所述计算机系统还包括用于把加密数据组块与设备的加密密钥索引相关联的程序指令，其中所述加密密钥索引指定将用于每一个组块的加密密钥。所述计算机系统还包括用于通过一个或多个计算机处理器接收对应于数据组块的给定逻辑块地址的加密密钥索引的程序指令，其中数据组块被读取或写入到存储器上的逻辑块地址。所述计算机系统还包括用于基于对盘驱动器的数据组块的加密密钥索引来确定将被用来对数据组块进行加密的加密密钥的程序指令。

[0006] 在另一个实施方案中，提供一种用于利用自加密驱动器 (SED) 对盘驱动器上的数据进行加密的计算机程序产品。所述计算机程序产品包括一个或多个计算器可读存储设备以及存储在所述一个或多个存储设备的至少其中之一的程序指令。所述计算机程序产品还包括用于对计算设备上的数据组块进行加密的程序指令。所述计算机程序产品还包括用于把加密数据组块与设备的加密密钥索引相关联的程序指令，其中所述加密密钥索引指定将用于每一个组块的加密密钥。所述计算机程序产品还包括用于通过一个或多个计算处理器接收对应于数据组块的给定逻辑块地址的加密密钥索引的程序指令，其中数据组块被读取或写入到盘驱动器上的逻辑块地址。所述计算机程序产品还包括用于基于对盘驱动器的数据组块的加密密钥索引来确定将被用来对数据组块进行加密的加密密钥的程序指令。

附图说明
[0007] 在所附权利要求书中阐述了本发明的独特特性。但是通过结合附图阅读后对于本发明的详细描述，本发明本身及其优选使用模式、其他的目的和优点将会得到更好的理解，其中相同的附图标记表示相同的组件，并且：

[0008] 图1A-1B是根据本发明的实施例的存储介质环境100的功能方块图，其用于利用自加密驱动器 (SED) 的灵活密钥管理对存储介质环境100的盘驱动器内的数据组块进行加密。

[0009] 图2是描绘出根据本发明的实施例的由存储介质环境的存储阵列控制器施行的各个步骤的流程图，其用于利用自加密驱动器 (SED) 的灵活密钥管理对存储介质环境100的盘驱动器内的数据组块进行加密。

[0010] 图3A-3D是描绘出根据本发明的实施例的由存储阵列控制器施行来处理用于写入存储介质环境的加密数据的SED操作的各个步骤的流程图。

[0011] 图4示出了根据本发明的实施例的计算机系统的各个组件的方块图。

具体实施方式
[0012] 现在将参照附图来详细描述本发明。现在参照图1，其中示出了存储介质环境100，其用于利用灵活的密钥管理对存储介质环境100的盘驱动器内的数据组块进行加密，所述灵活密钥管理支持利用不同的加密密钥来对不同的数据组块进行加密，其中所述密钥并不离开驱动器。每一个密钥可以保护存储介质环境100的任意位置处的数据组块。受其给定密钥保护的数据一定必须是连续的，所述数据的所有区段也不需是相同的。

[0013] 举例来说，盘驱动器上的不同数据组块可能在安全性要求方面有所不同。一个组块可能没有限制，另一个组块可能与一个用户/应用相关联，而第三个组块则与不同的应用相
关联。通过在外部对加密密钥进行管理，允许对于利用某一密钥加密什么数据的高度控制，但是将密钥本身存储在外部则有安全隐患。另一方面，自加密盘 (SED) 通过确保密钥不会离开驱动器而提供了安全的密钥使用，但是在将密钥映射到数据的方式方面不够灵活。本发明特别提供了存储计算环境的 SED 之外的各个间接层级，其中包括与密钥索引相关联的每一个数据块。与不同密钥索引相关联的数据被利用不同密钥加密，正如后面更加详细地描述的那样。

【0014】SED 接收被编码为将要读取或写入的数据的逻辑块地址 (LBA) 的一部分的密钥索引，并使用密钥索引来取回内部加密密钥。举例来说，考虑利用 SED 的加密被写入在存储计算环境 100 的存储控制器的 0x100-0x200 块处的卷 A 的数据。此外，考虑对应于卷 A 的密钥索引为 0x53。存储控制器将把 0x53 组合到 0x100 的 LBA，从而得到 0x00530000100，并且利用相关的数据向该 LBA 发送写入命令。SED 从内部取回与密钥索引 0x53 相关联的密钥，并且利用该密钥对实际被写入到存储介质的数据进行加密。在另一个实例中，考虑将从 0x4000-0x4010 块读取存储计算环境 100 的卷 B 的数据，并且对应于卷 B 的密钥索引为 0x42。存储控制器将把 0x42 组合到 0x4000 的 LBA，从而得到 LBA 为 0x004200004000，并且向该 LBA 发送读取命令。SED 将从内部取回与密钥索引 0x42 相关联的加密密钥，并且在读取自存储介质的数据继续传递到存储控制器之前利用该加密密钥对其进行解密。所支持的不同密钥的数目可以有很多，并且每一个加密密钥可以保护任意的数据段，其中受到不给定密钥保护的数据不一定必须是连续的，并且受保护数据的所有段也不需要具有相同的尺寸。

【0015】举例来说，在例如 SAN 类似的面向块的存储系统中，逻辑存储单元 (LUN) 或卷通常分散在几个驱动器上。此外，一个卷的存储在特定驱动器上的该部分的物理位置可以动态地改变，例如在所述卷被调整尺寸的情况下，或者在另一个驱动器上发生故障并且需要把冗余数据重新分配在其他驱动器之间的情况下。现有的 SED 无法很好地服务于这样的使用情况，其可以被配置或利用特定密钥仅对邻接的地址范围内或带进行加密。按照这种方式，如果属于不同卷的存储被存储在相同的带间，则将利用相同的密钥对其加密。通过指定将要使用哪一个密钥而不是连续将被读取或写入的数据的密钥本身，可以确保由驱动器利用不同的密钥对不同的卷进行加密，而不管数据被存储的物理位置如何。

【0016】例如考虑当前占用 SED 的前 100000 块的一个卷。如果该卷被调整尺寸从而需要另外的 50000 块，但是下一个邻接区域不可用，则存储控制器可以将数据写入在驱动器上的任何位置处，只要其与原始的 100000 块的相同密钥索引相关联即可。此外，一个驱动器上存储有两个不同的卷，一个利用与密钥索引 1 相关联的密钥“a”加密，另一个利用与密钥索引 2 相关联的密钥“b”加密。存储控制器例如可以将这些卷交织或者将其写入在盘的完全分离的部分中，并且只要连续数据一起正确地发送密钥索引，则由一个卷使用的加密密钥将不会被另一个卷使用。

【0017】存储计算环境 100 例如可以是存储或盘阵列。盘阵列是可以包含多个盘驱动器的盘存储系统。举例来说，盘存储系统是其中通过各种电子、磁性、光学或机械改变把数据记录到一个或多个旋转盘的表面层的存储机制的总体类别。盘驱动器是实施这样的存储机制的设备，并且通常不同于盘介质。值得注意的类型有包含不可移除盘的硬盘驱动器 (HDD)、软盘驱动器 (FDD) 及其可移除软盘以及各种光盘驱动器和相关联的光盘介质。存储计算环
境100例如还可以是服务器计算系统，比如管理服务器、web服务器或者任何其他电子设备或计算系统。服务器计算系统也可以代表通过一个或多个网络互连的计算机的“云”，其中在通过存储计算环境访问时，所述服务器计算系统可以是对应于利用群集计算机的计算系统的主服务器。

0018  如图1中所描绘的那样，存储计算环境100包括存储阵列控制器110和自加密盘（SED）120。本领域技术人员将认识到，存储计算环境100包括未在图1中描绘出的其他计算设备。存储阵列控制器110是可选地来自存储计算环境100的主机的针对存储计算环境100的存储请求的存储设备。存储阵列控制器110还可以在各个物理盘驱动器之间管理逻辑存储单元。存储阵列控制器110还可以实施硬件RAID。

0019  独立盘冗余阵列（RAID）是将多个盘驱动器组件组合到一个或多个逻辑单元中的存储技术。根据本发明的实施例，取决于所要的冗余度和性能水平，通过被称作“RAID层级”的几种方式的其中之一将存储阵列控制器110的数据分布至各个驱动器上。在所描绘的实施例中，存储阵列控制器110接收数据请求命令130，以便在存储阵列控制器110的给定逻辑块访问范围读取或写入给定卷上的数据。数据请求命令130请求接收自存储计算环境100的系统管理员或主机。根据至少一个实施例，数据请求命令130访问可以是读取或写入命令，其中所述数据是将要读取或写入的数据。所述数据还可以是以加密形式存储在存储阵列控制器110上的数据。举例来说，数据请求命令的卷135还可以是存储计算环境100的主机或系统管理员希望访问的存储阵列控制器110的逻辑单元号（LUN），其通常采取逻辑单元号（LUN）的形式，正如后文将描述的那样。

0020  LUN代表被用来标识存储阵列控制器110的逻辑单元的编号。LUN还可以支持存储计算环境100的读取/写入操作，例如在这种情况下，数据请求命令130的数据请求的数据是将要读取或写入的数据。举例来说，针对访问存储计算环境100的数据请求命令130请求的处理可以包括从逻辑单元号17读取存储计算环境100的逻辑块地址1000到1010。这种情况下数据是从存储阵列控制器110的指定存储位置返回的数据。此外，在另一个实例中，针对访问存储计算环境100的数据请求命令130还可以包括针对逻辑单元号32的包括全零的写入，其是对应于从逻辑块地址500处开始的700个的存储阵列控制器110的卷。

0021  卷135可以是存储阵列控制器110的一个存储元件，其例如包括可以从存储计算环境100写入或读取的一定数量的可用存储容量。卷135还可以被实施在一个或多个存储设备上，比如存储计算环境100的硬盘驱动器或固态盘。卷135也被称作逻辑单元，其由存储阵列控制器110的LUN标识。举例来说，存储阵列控制器110的LUN17例如可以代表一个17千兆字节容量的卷，并且LUN42代表一个34千兆字节容量的卷。

0022  逻辑块地址（LBA）是存储阵列控制器110的存储数据的逻辑块的地址，即该块与包含该块的卷的块地址空间的开头的偏移量。举例来说，存储阵列控制器110的LBA513指向存储阵列控制器110的给定卷中的第513个数据块的地址。卷密钥索引表140是存储阵列控制器110的包括一个或多个表列的数据表，其决定哪一个密钥索引对应于存储阵列控制器110中的哪一个卷。

0023  举例来说，卷密钥索引表140可以包括两列，其中例如包括具有卷LUN的一列以及具有相应的密钥索引的另一列。举例来说，该表的第一条目可以包含LUN57和密钥索引31415，该表的第二条目可以包含LUN14和密钥索引7172，后面以此类推。
修改器145是存储阵列控制器110的功能单元，其接受LBA和密钥索引作为输入，并且将其组合成经过修改的LBA。SEDI20可以接受所述经过修改的LBA，并且后面描述了SEDI20的密钥索引提取器的反向操作。举例来说，LBA修改器145适于将密钥索引的各个比特逻辑“OR（或）”到LBA的本将是全零的最高有效部分中。例如考虑下面的情形，其中给定10字节长的LBA地址空间以及0x00000000000003000（十六进制）的LBA和0x1234（十六进制）的密钥索引，所得到的新的LBA将是0x12340000000003000（十六进制）。

[0024] 图1是根据本发明的实施例的示出存储计算环境100中的自加密盘(SED)120的细节的功能方块图。SEDI20是对存储计算环境100的数据进行加密的加密存储设备。SEDI20还保护存储在计算环境100的硬盘中的写入到其中的用户数据，并且还可以利用内部密码密钥对从中读取的相同数据进行解密。此外，根据SEDI20，存储在计算环境100的硬盘中的数据总是被保持加密，并且用户可以选择性地开启和关闭加密功能。

[0025] 此外，SEDI20采用单加密码锁和认证密钥来控制用于直接加密数据的针对盘的访问。在这里，认证密钥的数列值被存储在硬盘中，并且被用来对用户进行认证以及被用来在用户被成功认证之后对盘加密密钥进行加密。SEDI20包括LBA+密钥索引121、密钥索引提取器122、密钥索引123、密钥表124、加密引擎125、加密数据126以及驱动器介质127。如前所述，逻辑块地址(LBA)+密钥索引121是由存储阵列控制器110的LBA修改器生成的存储计算环境100的索引密钥与LBA的组合。密钥索引123是由密钥索引提取器122提取的密钥索引。在给定经过修改的LBA的形式的组合密钥索引123和LBA地址的情况下，密钥索引提取器122提取出原始LBA和SEDI20的密钥索引，对经过修改的LBA进行逆向操作，正如前面所描述的那样。举例来说，给定10字节长的LBA地址空间以及0x12340000000003000的组合LBA，密钥索引提取器将输出0x00000000000003000的LBA和0x1234的密钥索引。密钥索引123是进入密钥表的条目，其例如包括0x1234。密钥表124是具有列的表，其中该表的第一条目可以包含密钥索引31415和密钥0x3174802103936398945034112785446，该表的第二条目可以包含密钥索引7172以及例如密钥0x25712815906582353554531872087397。加密引擎125是在给定密钥密钥的情况下利用标准加密算法（比如高级加密标准AES）对数据施行加密和解密的单元。加密数据是已经通过标准加密算法并且利用加密密钥进行了加密的数据。驱动器介质127是SEDI20的物理介质，SEDI20的数据被永久性地存储在其上并且在需要时被取回。

[0026] 图2是根据本发明的实施例的描绘出由存储阵列控制器110施行来利用存储计算环境100的SEDI20的灵活密钥管理和对盘驱动器上的数据进行加密的步骤的流程图。存储阵列控制器110对例如包括存储计算环境110的计算设备的数据组件进行加密（步骤210）。举例来说，所述盘驱动器可以是SEDI20，其中SEDI20利用内部密码密钥对被写入到其中的数据进行加密，并且对从中读取的已加密数据进行解密。SEDI20对保持在SEDI20内部的加密密钥索引和加密密钥进行映射。

[0027] 此外，存储阵列控制器110把已加密数据组件与存储计算环境100的加密密钥索引相关联。举例来说，加密密钥索引指定将对于存储阵列控制器110的每一个组件使用的加密密钥（步骤220）。加密密钥索引为存储计算环境100的数据组件提供了安全性。此外，由加密密钥索引保护的数据组件不需要是独立的，并且所有组件不需要具有相同的尺寸。此外，存储阵列控制器110接收对应于数据组件的给定逻辑块地址的加密密钥索引，其中所述数据
组块被读取或写入到盘驱动器上的逻辑块地址（步骤230）。举例来说，存储阵列控制器110访问给定卷135和盘驱动器的逻辑块地址的一定逻辑地址范围上的数据组块。

【0028】举例来说，卷135是盘驱动器的存储元件，其中所述卷的存储元件是可以向/从盘驱动器写入和读取的盘驱动器的可用存储容量。卷135可以被存储在一个或多个盘驱动器上，并且其中所述一个或多个盘驱动器可以包含属于多个卷的数据。此外，存储阵列控制器110接收逻辑块地址和加密密钥索引与作为SEDI120的盘驱动器的输入。

【0029】存储阵列控制器110还把所接收到的逻辑块地址和加密密钥索引组合成经过修改的逻辑块地址，其中所述经过修改的逻辑块地址被盘驱动器接收。此外，存储阵列控制器110基于针对盘驱动的数据组块的加密密钥索引定义，被用来对数据组块进行加密的加密密钥（步骤240）。

【0030】图3A是根据本发明的实施例的描绘出存储阵列控制器110可以采取来处理针对存储计算环境100的加密卷的写入的步骤的流程图。存储阵列控制器110接收来自存储计算环境100的主机或系统管理员的写入命令（步骤310）。举例来说，所述命令包含目标逻辑单元号（LUN）和所述要存储的数据的逻辑块地址，以及存储计算环境100的数据本身。存储阵列控制器110接收到用户定义的映射表将LUN映射到一个卷。举例来说，将数据写入到LUN12上的LBA500，其中LUN12映射到卷1。存储阵列控制器110识别出与卷相关联的密钥索引（K1）（步骤320）。可以利用通常所知的技术对于每一个卷保持一个密钥索引，比如线性阵列、散列表、二进制树等等，在判定330处，存储阵列控制器110确定是否找到密钥索引。如果没有找到密钥索引，则在步骤340处，存储阵列控制器110返回错误。

【0031】举例来说，如果没有找到密钥索引，则尽管所述卷被指定为加密，但是没有与该卷相关联的密码密钥。应对所述错误的一种方式例如可以包括生成密钥索引，正如前面在图3D中所描述的那样。但是如果找到密钥索引，则在步骤350处，存储阵列控制器110按照预定义方式组合密钥索引和LBA，从而使得SEDI120能够正确无误地提取出原始值。举例来说，可以将密钥索引写入入LBA的最高有效位中，从而可以得到超出存储计算设备的存储范围的地址。在步骤360处，存储程序利用所得到的LBA和存储计算环境100的原始数据向SEDI发送写入请求。

【0032】图3B是根据本发明的实施例的描绘出由SEDI120施行来写入存储计算环境100的加密数据的步骤的流程图。SEDI120从存储阵列控制器110接收针对一定地址范围的带有数据的写入请求或命令。所述写入请求例如可以包括针对存储阵列控制器110的地址范围A的数据D访问的命令（步骤410）。在判定420处，SEDI120确定所述地址范围（比如A）是否包含密钥索引。举例来说，这一确定可以是基于密钥索引是否被与原始LBA组合。

【0033】如果没有找到密钥，则在步骤430处，SEDI120将所述请求处理为常规写入请求。但是如果找到密钥索引，则由SEDI120在步骤440处取出相应的加密密钥。所述密钥例如可以利用线性阵列、散列表或二进制树来存储。SEDI120在判定450处确定所取回的密钥索引是否包括密钥。如果找到密钥，则在步骤460处，SEDI120在适当模式下（比如XTS）利用加密算法（比如AES）将其写入到存储阵列控制器110的存储介质。但是如果找到密钥，则SEDI120在步骤470处发送错误以显示。

【0034】图3C是根据本发明的实施例的描绘出由存储阵列控制器110施行来处理从存储计算环境100的加密卷进行读取的步骤的流程图。存储阵列控制器110接收针对来自存储计
算环境100的已加密卷的读取命令(步骤510)。举例来说，系统管理员向存储计算环境100的存储阵列控制器110发送读取命令。

【0035】所述命令例如包含目标逻辑单元号(LUN)和将从存储阵列控制器110读取的数据的逻辑块地址(LBA)以及将要读取的数据的数量。与标准实践相同，存储阵列控制器110利用用户定义的映射表把所述LUN映射到一个卷。举例来说，从LUN12上的LBA500读取1个块的数据，其中LUN12映射到卷V1。此外，在目的地卷被配置为已加密的情况下，查找与该卷相关联的密钥索引(KI)。此外，可以利用通常所知的技术对于每一个卷保持一个密钥索引，比如线性阵列、散列表、二进制树等等(步骤520)。在判定530处，存储阵列控制器110确定是否找到密钥索引。如果没有找到密钥索引，则在步骤540处，存储阵列控制器110返回错误。举例来说，所述错误消息可以表明虽然所述卷被指定为已加密，但是没有与之相关联的密码密钥。

【0036】如果找到密钥索引，则在步骤550处按照预定义方式组合密钥索引和逻辑块地址(LBA)，从而使得SEDI20驱动器能够明确无误地提取出原始数值。举例来说，可以将密钥索引写入LBA的最高有效位中，从而如果按照字面意义来解释的话将得到超出设备的存储范围的地址。此外，在步骤560处，存储阵列控制器110向相应的一个或多个盘发送读取请求。该请求由在前一步骤中创建的组合LBA和将要读取的数据的数量构成。

【0037】图3D是描绘由存储阵列控制器110执行来生成用于已加密卷的密钥的步骤的流程图。存储阵列控制器110接收针对创建存储计算环境100的一个已加密卷的请求(步骤610)。举例来说，存储计算环境中100的系统存储管理员指定将要创建一个已加密卷。存储阵列控制器110在卷-密钥索引表中建立一个新的条目(步骤620)。举例来说，存储阵列控制器110生成密钥索引并且将其连同卷标识符一起存储在阵列、散列表、二进制树或者其他通常所知的用于存储密钥和数值的方法中。所述密钥索引可以是随机数、单调递增的数值或者特定于系统的信息的编码，只要其在系统中是唯一的即可。

【0038】存储阵列控制器110向SEDI20发送密钥索引命令(步骤630)。举例来说，存储阵列控制器110向SEDI20发送创建密钥命令，其中作为参数传递所生成的密钥索引。SEDI20驱动器生成随机密钥并且在指定的密钥索引下对其进行内部存储(步骤640)。举例来说，SEDI20在内部生成随机密码密钥，并且将其存储在内部，从而可以在给出相应的密钥索引的命令下被取回。随后，SEDI20用信号通知所述处理已完成。

【0039】图4是根据本发明的一个实施例的计算机系统的方法图。

【0040】计算机系统400仅仅是适当的计算机系统的一个实例，而不意图暗示关于这里所描述的本发明的实施例的使用或功能范围的任何限制。无论如何，计算机系统400能够被实施和/或执行前面所阐述的任何功能。在计算机系统400中有计算机412，其能够与许多其他通用或专用计算环境区域或配置一起操作。可能适于与计算机412一起使用的众所周知的计算系统、环境和/或配置的实例包括但不限于个人计算机系统、服务器计算机系统、瘦客户端、胖客户端、手持式或膝上型设备、多处理器系统、基于微处理器的系统、芯片级、可编程消费电子部件、网络PC、小型计算机系统、大型计算机系统以及包括任何前述系统或设备的分布式云计算环境。存储计算环境100可以被实施为计算机412的一个实例。

【0041】计算机412可以在由计算机系统执行的计算机系统可执行指令(比如程序模块)的一般情境中来描述。一般来说，程序模块可以包括执行特定任务或者实施特定抽象数据类
型的例程、程序、对象、组件、逻辑、数据结构等等。计算机412可以被实践在分布式云计算环境中，其中各项任务通过通信网络链路的远程处理器设备施行。在分布式云计算环境中，程序模块可以位于包括存储器存储设备的本地和远程计算机系统存储介质中。

[0042] 还如图4中所示，计算机412被显示为通用计算设备的形式。计算机412的组件可以包括但不限于一个或多个处理器或处理单元416、存储器428以及将包括存储器428的各个系统组件耦合到处理单元416的总线418。

[0043] 总线418代表几种类型的总线结构当中的任意一种或更多种，其中包括使用多种总线架构当中的任一种的存储器总线或存储器控制器、外围总线、加速图形端口以及处理器或局部总线。作为举例而非限制，这样的架构包括工业标准架构（ISA）总线、微通道架构（MCA）总线、增强型ISA（EISA）总线、视频电子部件标准协会（VESA）局部总线以及外围组件互连（PCI）总线。

[0044] 计算机412通常包括多种计算机系统可读介质。这样的介质可能是能够由计算机412访问的任何可用介质，并且包括易失性和非易失性介质以及可移除和不可移除介质。

[0045] 存储器428包括获取易失性存储器的形式的计算机系统可读介质，比如随机存取存储器（RAM）430和/或高速缓存432。计算机412还可以包括其他可移除/不可移除、易失性/非易失性计算机系统存储介质。仅仅作为举例，存储系统434可以被提供用于从/向不可移除、非易失性磁性介质（未被示出并且通常被称作“硬盘驱动器”）进行读取和写入。虽然没有示出，但是可以被提供用于向/从可移除、非易失性磁盘（例如“软盘”）进行读取和写入的磁盘驱动器，以及用于从/向可移除、非易失性光盘（例如CD-ROM、DVD-ROM或其他光学介质）进行读取和写入的光盘驱动器。在这样的实例中，其分别可以通过一个或多个数据介质接口连接到总线418。正如如后文将进一步描绘和描述的那样，存储器428可以包括至少一种程序产品，其具有（例如，至少一个）程序模块集合，所述程序模块被配置成实施本发明的实施例的功能。

[0046] 作为举例而非限制，存储阵列控制器110可以被存储在存储器428中，以及操作系统、一个或多个应用程序、其他程序模块以及程序数据。所述操作系统，一个或多个应用程序、其他程序模块以及程序数据当中的每一项或者其某种组合可以包括联网环境的实现方式，程序模块442通常实施这里所描述的本发明的实施例的附图。所述程序模块442可以被实施为程序440的一个实例。

[0047] 计算机412还可以与以下各项通信：一个或多个外部设备414通信，比如键盘、指示设备等等以及显示器424；使得用户能够与计算机412交互的一个或多个设备；以及/或者使得计算机412能够与一个或多个其他计算设备通信的任何设备（例如网络卡、调制解调器等等）。这样的通信经由输入/输出（I/O）接口422发生。此外，计算机412还经由网络适配器420与一个或多个网络通信，比如局域网（LAN）、广域网（WAN）和/或公共网络（例如因特网）。正如如后文所描绘的那样，网络适配器420经由总线418与计算机412的其他组件通信。应当理解的是，虽然没有示出，但是可以结合计算机412使用其他硬件和/或软件组件。这方面的实例包括但不限于：微代码、设备驱动程序、冗余处理单元、外部盘驱动器阵列、RAID系统、带驱动器以及数据存储存储系统等等。

[0048] 附图中的流程图和方块图示出了根据本发明的各个实施例的系统、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。在这方面，所述流程图或方块图中的每一个
方块可以代表代码的一个模块、片段或部分，其包括用于实施（各项）指定功能的一条或多条可执行指令，还应当提到的是，在一些替换实施方式中，在方块中提到的各项功能可以按照不同于在附图中提到的顺序发生。举例来说，取决于所涉及的功能，被相继示出的两个方块实际上可以被基本上同时执行，或者各个方块有时可以按照相反顺序被执行。还应当提到的是，所述方块图和/或流程图图示的每一个方块以及所述方块图和/或流程图图示中的各种方块组合由施加指定功能或步骤的基于专用硬件的系统实施，或者由专用硬件与计算机指令的组合实施。

[0049] 本领域技术人员将认识到，本发明的实施例可以被具体实现为系统、方法或计算机程序产品。相应地，本发明的实施例可以采取完全硬件实施例的形式、完全软件实施例（包括固件、驻留软件、微代码等等）的形式或者通常在这里可以全部被称作“电路”、“模块”或“系统”的组合软件与硬件方面的实施例的形式。此外，本发明的实施例可以采取具体实现的一种或多种计算机可读介质中的计算机程序产品的形式，所述计算机可读介质具有具体实施在其上的计算机可读程序代码。

[0050] 此外，可以利用一种或更多种计算机可读介质的任意组合。所述计算机可读介质可以是计算机可读信号介质或计算机可读存储介质。计算机可读存储介质例如可以是（但不限于）电子、磁性、光学、电磁、红外或半导体系统、装置或设备或者前述各项的任意适当组合。计算机可读存储介质的更加具体的实例（非穷举列表）将包括以下各项：具有一条或多条连线的电连接，便携式计算机磁盘，硬盘，随机存取存储器（RAM），只读存储器（ROM），可擦写可编程只读存储器（EPROM或闪存），光盘，便携式紧凑盘只读存储器（CD-ROM），光学存储设备，磁性存储设备，或者前述各项的任意适当组合。在本文献的上下文中，计算机可读存储介质可以是包含或存储用于由指令执行系统、装置或设备使用或者与之相结合地使用的程序的任何有形介质。

[0051] 计算机可读信号介质可以包括其中具体实现有计算机可读程序代码的传播数据信号，比如具体实现的基带中或者作为载波的一部分。这样的传播信号可以采取多种形式当中的任何一种，其中包括但不限于电磁、光学或者其任意适当组合。计算机可读信号介质可以是并非计算机可读存储介质并安传送、传播或传输用于由指令执行系统、装置或设备使用或者与之相结合地使用的程序的任何计算机可读介质。

[0052] 具体实现的计算机可读存储介质的程序代码可以利用任何适当的介质来发送，其中包括但不限于无线、有线、光纤线缆、RF等等或者前述各项的任意适当组合。用于实施本发明的实施例的操作的计算机程序代码可以用一种或更多种编程语言的任意组合来编写，其中包括例如Java、Smalltalk、C++等面向对象的编程语言，例如“C”编程语言之类的传统过程性编程语言，例如Verilog之类的硬件描述语言，或者类似的编程语言。所述程序代码可以完全在用户的计算机上执行，部分地在用户的计算机上执行，作为独立式软件包来执行，部分地在用户的计算机上并且部分地在远程计算机上执行或者完全在远程计算机上执行。在后一种情形下，远程计算机可以通过任何类型的网络连接到用户的计算机，其中包括局域网（LAN）或广域网（WAN），或者可以连接到外部计算机（例如利用互联网服务提供商通过因特网连接）。所述计算机程序指令还可以被加载到计算机、其他可编程数据处理装置或者其他设备上，以使得在所述计算机、其他可编程装置或其他设备上施加一系列操作步骤从而实现计算机实施的处理，从而使得在计算机或其他可编程装置上执行的指令提
用于实施在流程图或方块图的一个或多个方块中规定的功能/步骤的处理。

基于前述内容，公开了一种用于利用自加密驱动器 (SED) 对盘驱动器上的数据进行加密的方法。但是，在不背离本发明的范围的情况下，可以做出许多修改和替换。在这方面，流程图或方块图中的每一个方块可以代表代码的一个模块、片段或部分，其包括用于实施（多项）指定逻辑功能的一条或多条可执行指令。还应当提到的是，在一些替换实现方式中，在方块中提到的各项功能可以按照不同于在附图中提到的顺序发生。因此，本发明是通过举例而非限制的方式来公开的。
图2

存储计算环境的存储阵列控制器接收针对一个已加密卷的写入命令

查找对应于该卷的密钥索引 KI

是否找到 KI？

是

组合 KI 与原始 LBA

利用所得到的 LBA 和原始数据项 SED 发送写入请求

图3A
图3B

存储计算环境的存储阵列控制器（SC）
接收针对一个已加密卷的读取命令

查找对应于该卷的密钥索引 KI

是否找到 KI？

是
组合 KI 与原始 LBA
利用所得到的 LBA 向存储计算环境的 SED 发送读取请求

图3C