(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 102023935 A
(43)申请公布日 2011.04.20

(21)申请号 201010297646.2

(22)申请日 2010.09.21

(30)优先权数据
89644/09 2009.09.22 KR
12/728,325 2010.03.22 US

(71)申请人 三星电子株式会社
地址 韩国京畿道

(72)发明人 李愚贤 柳范锡

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 钱大勇

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

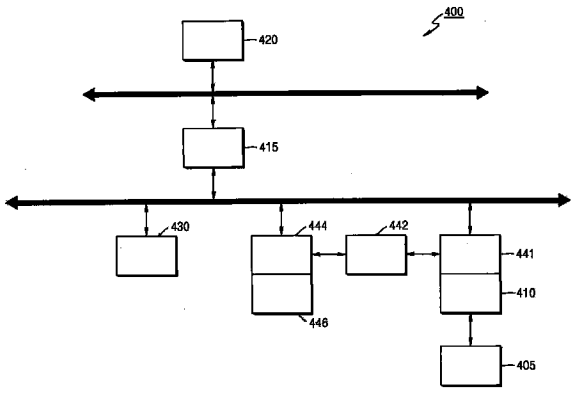
权利要求书 5 页 说明书 10 页 附图 10 页

(54)发明名称

具有密钥的数据存储设备及其方法

(57)摘要

一种存储设备包括：存储单元，用于存储数据；处理器单元，用于根据从外部装置接收的命令来处理数据；密钥单元，用于存储多个秘密密钥；和解码器单元，用于根据从所述外部装置接收的命令的地址信息来选择所述秘密密钥之一。硬件加密相对管理而言更安全且不太复杂。



CN 102023935 A

1. 一种存储设备，包括：

存储单元，用于存储数据；

处理器单元，用于根据从外部装置接收的命令来处理数据；和

密钥单元，用于当所述处理器单元处理数据时，同时地处理与所述命令对应的加密。

2. 如权利要求 1 所述的存储设备，其中所述密钥单元同时地处理所述加密而不中断所述处理器单元。

3. 如权利要求 1 所述的存储设备，其中所述密钥单元处理所述加密而无需所述处理器单元的控制。

4. 如权利要求 1 所述的存储设备，其中所述处理器单元处理数据而不中断所述密钥单元。

5. 如权利要求 1 所述的存储设备，其中在所述密钥单元完成所述加密的处理之后，所述密钥单元和所述处理器单元相互通信。

6. 如权利要求 1 所述的存储设备，其中所述密钥单元和所述处理器单元同时地处理所述加密和所述数据，并且所述数据的处理不同于所述加密的处理。

7. 如权利要求 1 所述的存储设备，其中所述数据的处理和所述加密的处理不具有根据所述命令顺序地执行所述加密的处理和所述数据的处理的顺序的优先级。

8. 如权利要求 1 所述的存储设备，其中所述数据的处理和所述加密的处理互不干扰。

9. 如权利要求 1 所述的存储设备，其中所述数据的处理包括根据所述命令将逻辑地址映射到物理地址的映射操作。

10. 如权利要求 1 所述的存储设备，其中所述处理器单元根据所述加密的处理的结果执行该数据的另外的处理。

11. 如权利要求 1 所述的存储设备，其中

第一时段被花费来顺序地处理加密和数据；

第二时段被花费来同时地处理加密和数据；和

所述第二时段短于所述第一时段。

12. 如权利要求 1 所述的存储设备，其中同时地处理加密和数据的速度快于顺序地处理加密和数据的速度。

13. 一种存储设备，包括：

存储单元，用于存储数据；

处理器单元，用于根据从外部装置接收的命令来处理数据；

密钥单元，用于存储多个秘密密钥；和

解码器单元，用于根据从所述外部装置接收的命令的地址信息来选择所述秘密密钥之一。

14. 如权利要求 13 所述的存储设备，其中一旦接收到所述命令，所述处理器单元和所述解码器单元同时地分别执行数据的处理和秘密密钥的选择。

15. 如权利要求 13 所述的存储设备，还包括：

加密单元，用于根据所选择的秘密密钥来执行加密数据的加密操作。

16. 如权利要求 15 所述的存储设备，其中：

所述处理器单元根据处理后的数据和加密操作将信号输出到所述外部装置。

17. 如权利要求 15 所述的存储设备，其中：

在当所述解码器单元选择所述秘密密钥并且所述加密单元执行加密操作时的期间内，所述处理器单元处理数据。

18. 如权利要求 15 所述的存储设备，其中：

当所述加密单元完成加密操作时，所述处理器单元被允许输出从处理后的数据生成的信号。

19. 如权利要求 13 所述的存储设备，其中所述解码器单元生成指示对所述处理器单元的加密操作的信号。

20. 如权利要求 13 所述的存储设备，其中所述解码器单元将地址信息与基准相比较以便生成选择用于加密所述数据的秘密密钥的信号。

21. 如权利要求 13 所述的存储设备，其中所述解码器单元生成表示选择一个秘密密钥的密钥标志。

22. 如权利要求 13 所述的存储设备，其中所述多个秘密密钥包括多个 64 位。

23. 如权利要求 13 所述的存储设备，其中所述处理器单元根据所述命令而不执行所述解码器单元的加密操作。

24. 如权利要求 13 所述的存储设备，其中所述解码器单元包括命令分析单元，用于分析来自所述外部装置的命令以便实时获得所述地址信息。

25. 如权利要求 13 所述的存储设备，其中所述解码器单元包括地址转换单元，用于将所述地址信息实时连接到与所述地址信息对应的所述一个秘密密钥。

26. 如权利要求 13 所述的存储设备，其中：

加密操作是根据所选择的秘密密钥完成的；和

根据所述数据的处理和加密操作的完成，所述处理器单元将其它数据输出到所述外部装置。

27. 如权利要求 13 所述的存储设备，还包括：

接口单元，用于接收来自所述外部装置的命令，

其中所述处理器单元和所述解码器单元接收来自所述接口单元的命令，以便根据接收到的命令分别执行数据的处理和加密操作。

28. 如权利要求 15 所述的存储设备，还包括：

数据总线，连接到所述处理器单元和所述解码器单元，用于将所述命令发送到所述处理器单元和所述解码器单元中的相应一个。

29. 如权利要求 16 所述的存储设备，其中所述数据总线包括连接到所述处理器单元的第一端和连接到所述解码器单元的第二端。

30. 如权利要求 13 所述的存储设备，还包括：

可连接到所述外部装置的外壳，用于容纳所述存储单元、所述处理器单元、所述密钥单元和所述解码器单元，

其中所述处理器单元和所述解码器单元在所述外壳内彼此间隔地分开。

31. 如权利要求 13 所述的存储设备，其中在加密操作中选择秘密密钥期间，所述解码器单元不被所述处理器单元控制。

32. 一种存储设备，包括：

处理器单元，用于根据从外部装置接收的命令执行数据的处理；

解码器单元，用于根据从所述外部装置接收的命令的地址信息执行秘密密钥的选择，

其中一旦接收到所述命令，所述处理器单元和所述解码器单元同时地分别执行数据的处理和秘密密钥的选择。

33. 一种存储系统，包括：

主机设备，用于生成命令；和

存储设备，可连接到所述主机设备，所述存储设备包括：

存储单元，用于存储数据；

处理器单元，用于根据从外部装置接收的命令来处理数据；

密钥单元，用于存储多个秘密密钥；和

解码器单元，用于根据从所述外部装置接收的命令的地址信息来选择所述秘密密钥之一。

34. 一种存储系统，包括：

主机设备，用于生成命令；和

存储设备，可连接到所述主机设备，所述存储设备包括：

处理器单元，用于根据从外部装置接收的命令执行数据的处理；

解码器单元，用于根据从所述外部装置接收的命令的地址信息执行秘密密钥的选择，

其中一旦接收到所述命令，所述处理器单元和所述解码器单元同时地分别执行数据的处理和秘密密钥的选择。

35. 如权利要求 34 所述的存储系统，其中：

所述主机设备生成对应于用户窗口的接口信号以便改变所述秘密密钥。

36. 如权利要求 35 所述的存储系统，其中：

所述解码器单元执行改变后的秘密密钥的选择。

37. 一种存储设备，包括：

密钥单元，用于存储多个秘密密钥；

解码器单元，用于根据从外部装置接收的地址信息来选择所述秘密密钥之一；

存储单元，用于存储数据；和

控制处理器单元，用于使用所选择的秘密密钥管理来自所述存储单元的读和写数据，

其中所述解码器单元独立于所述控制处理器单元选择所述秘密密钥之一。

38. 一种固态盘驱动器，包括：

密钥单元，用于存储多个秘密密钥；

解码器单元，用于根据从外部装置接收的地址信息来选择所述秘密密钥之一；

存储单元，用于存储数据；和

控制处理器单元，用于使用所选择的秘密密钥管理来自所述存储单元的读和写数据，

其中所述解码器单元独立于所述控制处理器单元选择所述秘密密钥之一。

39. 一种数据系统，包括：

主机设备，用于生成命令；和

存储设备，可连接到所述主机设备，所述存储设备包括：

密钥单元，用于存储多个秘密密钥；

解码器单元，用于根据从外部装置接收的地址信息来选择所述秘密密钥之一；

存储单元，用于存储数据；和

控制处理器单元，用于使用所选择的秘密密钥管理来自所述存储单元的读和写数据，

其中所述解码器单元独立于所述控制处理器单元选择所述秘密密钥之一。

40. 一种加密数据的方法，所述方法包括步骤：

接收命令；

根据所述命令解析地址；

接收逻辑块地址范围；

生成与所述逻辑块地址范围对应的密钥标志；和

使用所述密钥标志选择秘密密钥。

41. 一种加密数据的方法，所述方法包括步骤：

接收写请求；

根据所述写请求解析地址；

接收逻辑块地址范围；

生成与所述逻辑块地址范围对应的密钥标志；

使用所述密钥标志选择秘密密钥；

使用所述秘密密钥来加密数据；和

将加密后的数据写入存储器。

42. 一种解密数据的方法，所述方法包括步骤：

接收命令；

根据所述命令解析地址；

接收逻辑块地址范围；

生成与所述逻辑块地址范围对应的密钥标志；和

使用所述密钥标志选择秘密密钥。

43. 一种解密数据的方法，所述方法包括步骤：

接收读请求；

根据所述读请求解析地址；

接收逻辑块地址范围；

生成与所述逻辑块地址范围对应的密钥标志；

使用所述密钥标志选择秘密密钥；

使用所述秘密密钥来解密数据；和

从存储器读取解密后的数据。

44. 一种在存储设备中执行加密操作的方法，所述方法包括：

接收命令；和

同时地根据所述命令处理数据并且根据所述命令的地址信息执行秘密密钥的选择。

45. 一种包括计算机可读代码的计算机可读介质，所述计算机可读代码作为用于执行在存储设备中执行加密操作的方法的程序，所述方法包括：

接收命令；和

同时地根据所述命令处理数据并且根据所述命令的地址信息执行秘密密钥的选择。

具有密钥的数据存储设备及其方法

[0001] 相关申请的交叉引用

[0002] 本申请要求于2009年9月22日向韩国工业产权局提交的韩国专利申请No.2009-89644的优先权，其公开合并于此作为参考。

技术领域

[0003] 本总的发明构思涉及一种加密和解密数据的数据存储设备和方法，且更具体地涉及一种处理秘密密钥(crypto key)的设备及其方法

背景技术

[0004] 通常，数据存储装置是一种从存储媒体读取数据并且将数据写入存储媒体的计算装置。 数据存储装置可以包含移动部件，或者可以不具有任何显著的移动部件。 具有移动部件的数据存储装置的一个示例是传统的盘驱动器，其中例如旋转唱片的盘旋转并且具有用于读写数据的一个或多个头。 不具有任何显著的移动部件的数据存储装置通常被称作固态驱动器。

[0005] 安全盘驱动器使用一种部分或整盘加密技术来支持驱动器处的数据加密，在该技术中使用加密密钥来加密存储媒体上的数据。 在常规系统中，响应读或写命令，从存储器取回加密的数据，并且对解密的数据进行加密和存储。 尽管加密或安全密钥可被存储在安全盘驱动器上，但是加密和解密由主机装置中的外部处理器或者安全盘驱动器中的微处理器处理。 因为数据在按照读或写命令控制被处理之前必须首先被加密或解密，因此用于加密和解密的软件解决方案具有大的吞吐量并且对性能产生影响。

发明内容

[0006] 本总的发明构思提供了更快的性能和更好的安全性。 因为加密密钥是在驱动硬件内生成并存储的，因此它们从未脱离其范围并且从未保存在操作系统中或者从未被应用软件保存。 硬件加密相对管理而言更安全且不太复杂。

[0007] 本总的发明构思的附加方面和优点将部分地阐述于随后的描述中，且部分地从所述描述中显而易见，或者可以通过本总的发明构思的实践来获知。

[0008] 本总的发明构思的上述和/或其它方面和效用可以通过提供一种存储设备来实现，所述存储设备包括：存储单元，用于存储数据；处理器单元，用于根据从外部装置接收的命令来处理数据；和密钥单元，用于当所述处理器单元处理数据时，同时地处理与所述命令对应的加密。

[0009] 本总的发明构思的上述和/或其它方面和效用也可以通过提供一种存储设备来实现，所述存储设备包括：存储单元，用于存储数据；处理器单元，用于根据从外部装置接收的命令来处理数据；密钥单元，用于存储多个秘密密钥；和解码器单元，用于根据从所述外部装置接收的命令的地址信息来选择所述秘密密钥之一。

[0010] 本总的发明构思的上述和/或其它方面和效用也可以通过提供一种存储设备来

实现，所述存储设备包括：处理器单元，用于根据从外部装置接收的命令执行数据的处理；解码器单元，用于根据从所述外部装置接收的命令的地址信息执行秘密密钥的选择，其中一旦接收到所述命令，所述处理器单元和所述解码器单元同时地分别执行数据的处理和秘密密钥的选择。

[0011] 本总的发明构思的上述和/或其它方面和效用也可以通过提供一种存储系统来实现，所述存储系统包括：主机设备，用于生成命令；和存储设备，可连接到所述主机设备，所述存储设备包括：存储单元，用于存储数据；处理器单元，用于根据从外部装置接收的命令来处理数据；密钥单元，用于存储多个秘密密钥；和解码器单元，用于根据从所述外部装置接收的命令的地址信息来选择所述秘密密钥之一。

[0012] 本总的发明构思的上述和/或其它方面和效用也可以通过提供一种存储系统来实现，所述存储系统包括：主机设备，用于生成命令；和存储设备，可连接到所述主机设备，所述存储设备包括：处理器单元，用于根据从外部装置接收的命令执行数据的处理；解码器单元，用于根据从所述外部装置接收的命令的地址信息执行秘密密钥的选择，其中一旦接收到所述命令，所述处理器单元和所述解码器单元同时地分别执行数据的处理和秘密密钥的选择。

[0013] 本总的发明构思的上述和/或其它方面和效用也可以通过提供一种存储设备来实现，所述存储设备包括：密钥单元，用于存储多个秘密密钥；解码器单元，用于根据从外部装置接收的地址信息来选择所述秘密密钥之一；存储单元，用于存储数据；和控制处理器单元，用于使用所选择的秘密密钥管理来自所述存储单元的读和写数据，其中所述解码器单元独立于所述控制处理器单元选择所述秘密密钥之一。

[0014] 本总的发明构思的上述和/或其它方面和效用也可以通过提供一种固态盘驱动器来实现，所述固态盘驱动器包括：密钥单元，用于存储多个秘密密钥；解码器单元，用于根据从外部装置接收的地址信息来选择所述秘密密钥之一；存储单元，用于存储数据；和控制处理器单元，用于使用所选择的秘密密钥管理来自所述存储单元的读和写数据，其中所述解码器单元独立于所述控制处理器单元选择所述秘密密钥之一。

[0015] 本总的发明构思的上述和/或其它方面和效用也可以通过提供一种数据系统来实现，所述数据系统包括：主机设备，用于生成命令；和存储设备，可连接到所述主机设备，所述存储设备包括：密钥单元，用于存储多个秘密密钥；解码器单元，用于根据从外部装置接收的地址信息来选择所述秘密密钥之一；存储单元，用于存储数据；和控制处理器单元，用于使用所选择的秘密密钥管理来自所述存储单元的读和写数据，其中所述解码器单元独立于所述控制处理器单元选择所述秘密密钥之一。

[0016] 本总的发明构思的上述和/或其它方面和效用也可以通过提供一种加密数据的方法来实现，所述方法包括步骤：接收命令；根据所述命令解析地址；接收逻辑块地址范围；生成与所述逻辑块地址范围对应的密钥标志；和使用所述密钥标志选择秘密密钥。

[0017] 本总的发明构思的上述和/或其它方面和效用也可以通过提供一种加密数据的方法来实现，所述方法包括步骤：接收写请求；根据所述写请求解析地址；接收逻辑块地址范围；生成与所述逻辑块地址范围对应的密钥标志；使用所述密钥标志选择秘密密钥；使用所述秘密密钥来加密数据；和将加密后的数据写入存储器。

[0018] 本总的发明构思的上述和 / 或其它方面和效用也可以通过提供一种解密数据的方法来实现，所述方法包括步骤：接收命令；根据所述命令解析地址；接收逻辑块地址范围；生成与所述逻辑块地址范围对应的密钥标志；和使用所述密钥标志选择秘密密钥。

[0019] 本总的发明构思的上述和 / 或其它方面和效用也可以通过提供一种解密数据的方法来实现，所述方法包括步骤：接收读请求；根据所述读请求解析地址；接收逻辑块地址范围；生成与所述逻辑块地址范围对应的密钥标志；使用所述密钥标志选择秘密密钥；使用所述秘密密钥来解密数据；和从存储器读取解密后的数据。

[0020] 本总的发明构思的上述和 / 或其它方面和效用也可以通过提供一种在存储设备中执行加密操作的方法来实现，所述方法包括：接收命令；和同时地根据所述命令处理数据并且根据所述命令的地址信息执行秘密密钥的选择。

[0021] 本总的发明构思的上述和 / 或其它方面和效用也可以通过提供一种包括计算机可读代码的计算机可读介质，所述计算机可读代码作为用于执行在存储设备中执行加密操作的方法的程序，所述方法包括：接收命令；和同时地根据所述命令处理数据并且根据所述命令的地址信息执行秘密密钥的选择。

附图说明

[0022] 从结合附图的实施例的下列描述中，本总的发明构思的这些和 / 或其它方面和优点将变得明显和更容易理解，附图中：

[0023] 图 1A 和图 1B 是图示根据本总的发明构思的实施例与主机设备通信的存储设备的视图；

[0024] 图 2A 和图 2B 是图示根据本总的发明构思的实施例与主机设备通信的存储设备的视图；

[0025] 图 3 是图示根据本总的发明构思的实施例的存储设备的一部分的视图；

[0026] 图 4 是图示根据本总的发明构思的实施例的存储设备的方块图；

[0027] 图 5 是图示根据本总的发明构思的实施例的帧信息系统的视图；

[0028] 图 6 是图示根据本总的发明构思的实施例的帧信息系统的视图；

[0029] 图 7 是图示根据本总的发明构思的实施例的帧信息系统的视图；

[0030] 图 8 是图示根据本总的发明构思的实施例的包括存储设备的计算机架构的视图；

[0031] 图 9 是图示根据本总的发明构思的实施例的包括存储设备的计算机架构的视图；

[0032] 图 10 是图示根据本总的发明构思的实施例的包括存储设备的计算机架构的视图；

[0033] 图 11 是图示根据本总的发明构思的实施例的包括存储设备的计算机架构的视图；

[0034] 图 12 是图示根据本总的发明构思的实施例的用于在存储设备上加密或解密数据的方法的流程图；

[0035] 图 13 是图示根据本总的发明构思的实施例的用于在存储设备上加密或解密数据

的方法的流程图。

具体实施方式

[0036] 现在将对本总的发明构思的实施例进行详细参考，其示例图示于附图中，其中全文中相似的附图标号指代相似的元件。 下面在参考附图的同时描述实施例以便解释本总的发明构思。

[0037] 整盘加密解决方案 (Full disk encryption solutions) 使用若干安全或加密密钥用以加密不同的分区。 如果未授权的用户获得对计算机的访问，则该未授权的用户并不能访问所有文件。 文件和文件夹加密对于盘的不同部分允许不同的密钥。 因此未授权的用户不能从仍旧加密的文件和文件夹中提取信息。

[0038] 硬件加密相对于仅程序加密手段的优点包括性能更快且安全性更好。 因为在驱动器硬件内产生并存储加密密钥，因此它们从未脱离其界限并且从未保存在操作系统中或者从未被应用软件保存。 硬件加密相对管理而言更安全且不太复杂。

[0039] 下文中可替换地使用的术语“加密密钥”、“安全密钥”或“秘密密钥”，可以结合加密和 / 或解密数据的高级加密标准 (AES) 或数据加密标准 (DES)、或者适当的其它加密系统来使用。

[0040] 图 1A、1B、2A 和 2B 是图示根据本总的发明构思的示例性实施例的安全存储设备 100 和 200 的视图。

[0041] 参考图 1A 和图 1B，安全存储设备 100 包括接口 110、处理器 120、存储单元 130 和密钥单元 140。 安全存储设备 100 与位于主机设备 105 中的主机处理器 108 通信。

[0042] 在图 1A 中，安全存储设备 100 在包括主机处理器 108 的主机设备 105 的外部，并且通过接口 110 通信。 安全存储设备 100 可以通过其中的端子可拆卸地附着到主机设备 105。

[0043] 在图 1B 中，安全存储设备 100 位于主机设备 105 的内部，并且通过接口 110 与主机处理器 108 通信。 安全存储设备 100 可被安装在主机设备 105 中。 该主机设备 105 可以具有至少一个安装在其中的附加存储设备。

[0044] 用户使用主机设备 105。 主机设备 105 与安全存储设备 100 通信，该安全存储设备 100 显然地加密和解密存储在安全存储设备 100 上的数据。 用户可以在引导或启动时输入口令，以便访问处于加锁状态的安全存储设备 100。可替换地，用户可以在未加锁状态下毫无限制地不输入口令而可以访问安全存储设备 100。在加锁或未加锁状态下，数据已被加密。 在加锁状态下，用户通过设置口令来控制安全密钥。

[0045] 可能的是，用户可以输入口令来根据存储在存储单元 130 中的数据生成具有不同的限制或加密 / 解密级别或范围的文档。

[0046] 在加锁状态下，可以使用数种技术来找回丢失的口令。 可以使用挑战 / 响应序列来找回丢失的口令。 可替换地，可以在安全空间内生成并且存储受口令保护的加密密钥文件。

[0047] 处理器 120 根据从主机处理器 108 接收的命令，例如读 / 写命令，处理数据。 处理器 120 可以是微处理器、微控制器、数字信号处理器、专用或通用编程芯片。

[0048] 存储单元 130 存储数据。 存储单元 130 可以是存储数据的半导体固态盘驱动器

(SSD)。 存储单元 130 可以是其它类型的存储器，例如闪速存储器、多个半导体存储芯片的模块或封装、存储卡等。 可替换地，存储单元 130 可以是其它类型的存储器，例如传统的硬盘驱动器 (HDD)、光盘驱动器 (ODD) 等。 存储单元 130 具有用于存储数据或信息的存储空间（或物理存储空间）。

[0049] 密钥单元 140 同时地处理与从主机处理器 108 接收的读 / 写命令对应的加密和解密，同时处理器单元 120 响应从主机处理器 108 接收的命令而处理数据。在本总的发明构思的示例性实施例中，密钥单元解析用于从命令中找回地址的命令，使用该地址查找安全密钥，并且根据读 / 写命令执行数据的加密或解密。 密钥单元 140 可以是分离单元，具有用于存储安全密钥列表的存储器以及用于执行安全密钥查找和数据加密的专用或通用微处理器。

[0050] 所述命令可以包括与处理器 110 进行的数据处理对应的第一命令和与密钥单元 140 进行的加密或解密对应的第二命令。 而且，所述命令可以被处理器 120 和密钥单元 140 同时解释以便同时执行数据处理和加密或解密。

[0051] 安全密钥列表与存储单元 130 相关。 存储单元 130 被划分为 n 个范围，并且每个范围具有与在加密和解密其中包含的数据时使用的其相关联的唯一安全密钥。 该范围可以由制造商限定，并且是数据量。 安全密钥列表包含与存储单元 130 的 n 个范围对应的 n 个安全密钥。 每个范围中的数据可以具有固定的块大小，例如 64 位、128 位、192 位、256 位等，并且每个范围的安全密钥可以是例如 64 位、128 位、192 位、256 位等。从自主机处理器 108 接收的读 / 写命令解析的地址，可以结合安全密钥列表被用来利用所解析的地址确定加密和 / 或解密特定数据所需要的安全密钥。

[0052] 当使用根据从自主机处理器 108 接收的读 / 写命令解析的地址从安全密钥列表中已经选择安全密钥时，密钥单元 140 使用该安全密钥来加密和 / 或解密数据。 密钥单元 140 可以使用加密和 / 或解密数据的高级加密标准 (AES) 或数据加密标准 (DES)，或者可以使用适当的其它加密系统。

[0053] 密钥单元 140 从命令中解析地址，并且不利用处理器 120 地处理加密和 / 或解密。因此，处理器 120 可以处理如在命令中指定的数据，而密钥单元 140 同时地处理数据的加密和 / 或解密。密钥单元 140 能够加密或解密数据而不中断处理器 120 或需要控制，同时处理器 120 能够处理数据而不中断密钥单元 140。 密钥单元 140 和处理器 120 彼此都不具有优于对方的优先级，并且密钥单元 140 和处理器 120 彼此不干扰 (interfere with)。

[0054] 处理器 120 处理数据，可以包括执行映射操作以便根据命令将逻辑地址映射到存储单元 130 中的对应物理地址。 处理器 120 可以在通过密钥单元 140 进行加密的处理之后，执行数据的附加处理。

[0055] 处理器 120 可以等待或延迟数据的处理直到密钥单元 140 完成加密或解密处理为止。处理器 120 可以在密钥单元 140 进行的加密或解密处理期间执行一部分的数据处理。处理器 120 可以在密钥单元 140 进行的加密或解密处理期间准备数据的处理，从而一旦密钥单元 140 完成加密或解密处理，处理器 120 就可以根据命令完成数据的处理。

[0056] 同时地处理加密和数据的速度快于顺序地处理加密和数据的速度。 被花费来同时地处理加密和数据的时间段可以是单个时钟周期或者其它时间段，它短于顺序地处理加密和数据所花费的时间段。

[0057] 参考图 2A 和图 2B，安全存储设备 200 包括接口 210、处理器 220、存储单元 230 和安全单元 240，安全单元 240 包括解码器单元 242、密钥单元 244 和加密单元 246。 安全存储设备 200 与位于主机设备 205 中的主机处理器 208 通信。

[0058] 在图 2A 中，安全存储设备 200 在包括主机处理器 208 的主机装置 205 的外部，并且通过接口 210 通信。 安全存储设备 200 可以通过其中的端子可拆卸地附着到主机设备 205。

[0059] 在图 2B 中，安全存储设备 200 位于主机设备 205 的内部，并且通过接口 210 与主机处理器 208 通信。 安全存储设备 200 可被安装在主机设备 205 中。 该主机设备 105 可以具有至少一个安装在其中的附加存储设备。

[0060] 用户使用主机设备 205。 主机设备 205 与安全存储设备 200 通信，该安全存储设备 200 显然地加密和解密存储在安全存储设备 200 上的数据。 用户可以在引导或启动时输入口令，以便访问处于加锁状态的安全存储设备 200。可替换地，用户可以在未加锁状态下毫无限制地不输入口令而可以访问安全存储设备 200。在加锁状态或未加锁状态下，数据均已经被加密。 在加锁状态下，用户通过设置口令来控制安全密钥。

[0061] 可能的是，用户可以输入口令来根据存储在存储单元 230 中的数据生成具有不同的限制或加密 / 解密级别或范围的文档。

[0062] 在加锁状态下，可以使用数种技术来找回丢失的口令。 可以使用挑战 / 回应 (challenge/response) 序列来找回丢失的口令。 可替换地，在安全空间内可以生成并且存储受口令保护的加密密钥文件。

[0063] 处理器 220 根据从主机处理器 208 接收的命令，例如读 / 写命令，处理数据。处理器 220 可以是微处理器、微控制器、数字信号处理器、专用或通用编程芯片。

[0064] 存储单元 230 存储数据。 存储单元 230 可以是存储数据的半导体固态盘驱动器 (SSD)。 存储单元 230 可以是其它类型的存储器，例如闪速存储器、多个半导体存储芯片的模块或封装、存储卡等。 可替换地，存储单元 230 可以是其它类型的存储器，例如传统的硬盘驱动器 (HDD)、光盘驱动器 (ODD) 等。 存储单元 230 具有用于存储数据或信息的存储空间 (或物理存储空间)。

[0065] 安全单元 240 包括解码器单元 242、密钥单元 244 和加密单元 246。

[0066] 解码器单元 242 根据从自主机设备 208 接收的命令解析地址信息，并且选择相应的安全密钥。 解码器单元 242 可以是分离的专用或通用电路，它可以经由处理器 220 接收来自接口 210 的命令或者可以从接口 210 直接接收命令并且对该命令解码。

[0067] 所述命令可以包括与处理器 210 进行的处理数据对应的第一命令和与解码器单元 242 进行的加密或解密对应的第二命令。 而且，所述命令可以被处理器 220 和解码器单元 242 同时解释以便同时执行数据处理和加密或解密。

[0068] 解码器单元 242 解析所述命令并且根据所述命令确定地址。 根据自主机处理器 208 接收的读 / 写命令解析的地址，可以结合密钥单元 244 中存储的密钥列表被用来利用所解析的地址确定加密和 / 或解密特定数据所需要的安全密钥。

[0069] 在本总的发明构思的示例性实施例中，密钥单元 244 存储安全密钥列表。 密钥单元 244 可以是包含密钥列表的分离的存储单元，或者可以位于存储单元 230 上。 安全密钥列表与存储单元 230 相关。 存储单元 230 被划分为 n 个范围，并且每个范围具有与

在加密和解密其中包含的数据时使用的其相关联的唯一安全密钥。 该范围可以由制造商限定，并且是数据量。 安全密钥列表包含与存储单元 230 的 n 个范围对应的 n 个安全密钥。 每个范围中的数据可以具有固定的块大小，例如 64 位、128 位、192 位、256 位等，并且每个范围的安全密钥可以是例如 64 位、128 位、192 位、256 位等。

[0070] 解码器单元 242 可以使用地址来从存储在存储单元 230 上的密钥列表中直接选择相应的安全密钥，或者解码器单元 242 可以使用从接收到的命令解析的地址来生成密钥标志。 该密钥标志随后可被用来从存储在存储单元 230 上的密钥列表中选择相应的安全密钥。 解码器单元 242 可以将地址与基准相比较，以便生成用于选择加密或解密数据的安全密钥的密钥标志。

[0071] 加密 (cipher) 单元 246 执行加密操作以便根据所选的秘密密钥加密数据。 加密单元 246 可以是分离的专用或通用电路，它可以是高级加密系统 (AES) 或者数据加密系统 (DES) 加密器 (cipher)、或任何合适的加密器。

[0072] 当通过解码器单元 242 使用从自主机处理器 208 接收的读 / 写命令解析的地址从存储在密钥单元 250 中的安全密钥列表中已经选择安全密钥时，加密单元 246 使用该安全密钥来加密和 / 或解密数据。 加密单元 246 可以使用加密和 / 或解密数据的高级加密标准 (AES) 或数据加密标准 (DES)，或者可以使用适当的其它加密系统。

[0073] 解码器单元 242 从命令中解析地址，并且加密单元 246 不利用处理器 220 来处理加密和 / 或解密。 因此，处理器 220 可以处理如在命令中指定的数据，而解码器单元 242 同时地选择安全密钥。 加密单元 246 能够加密或解密数据而不中断处理器 220 或需要控制，同时处理器 220 能够处理数据而不中断加密单元 246。 解码器单元 242 和处理器 220 都不具有优于对方的优先级，并且解码器单元 242 和处理器 120 彼此不干扰 (interfere with)。

[0074] 处理器 220 处理数据，可以包括执行映射操作以便根据命令将逻辑地址映射到存储单元 230 中的对应物理地址。 处理器 220 可以在通过加密单元 260 进行加密的处理之后，执行数据的附加处理。 根据处理的数据和加密操作，处理器 220 可以将信号输出到主机设备 205。

[0075] 处理器 220 可以等待或延迟数据的处理直到解码器单元 242 完成加密或解密处理为止。 处理器 220 可以在解码器单元 242 进行的加密或解密处理期间执行一部分的数据处理。 处理器 220 可以在解码器单元 242 进行的加密或解密处理期间准备数据的处理，从而一旦解码器单元 242 完成加密或解密处理，处理器 220 就可以根据命令完成数据的处理。

[0076] 同时地处理加密和数据的速度快于顺序地处理加密和数据的速度。 被花费来同时地处理加密和数据的时间段可以是单个时钟周期或者其它时间段，它短于顺序地处理加密和数据所花费的时间段。

[0077] 一旦接收到命令，处理器 220 和解码器单元 242 就同时地分别执行数据的处理和安全密钥的选择。 主机设备 205 可以通过生成对应于用户窗口的接口信号来与用户通信，以便改变安全密钥。 解码器单元 242 可以选择变化后的安全密钥。 解码器单元 242 独立于处理器 220 或主机处理器 208 选择安全密钥之一。

[0078] 因此，处理器 220 在从存储在存储单元 244 上的密钥列表中选择安全密钥时不执

行加密或解密或者控制解码器单元 242。处理器 220 根据处理后的数据和加密操作将信号输出到主机设备 205。处理器 220 在当解码器单元 242 选择安全密钥和加密单元 246 执行加密操作时的时间段内处理数据。当加密单元 246 完成加密操作时，处理器 220 被允许输出根据处理后的数据生成的信号。解码器单元 242 生成指示对处理器 220 的加密操作的信号。

[0079] 参考图 3，图示了表示本总的发明构思的示例性实施例的安全单元 340。下文中参考安全单元 340 更详细地描述图 2 的解码器单元 242、密钥单元 244 和加密单元 246，所述安全单元 340 包括解码器单元 342、密钥单元 344 和加密单元 346。

[0080] 图 3 包括解码器单元 342、密钥单元 344 和加密单元 346。解码器单元 342 接收命令并且根据该命令解析地址。地址可以是逻辑块地址 (LBA)。地址或 LBA 被用来从密钥单元 344 选择安全密钥。密钥单元 344 包括密钥 1、密钥 2... 密钥 n。每个密钥对应于图 2 的示例性实施例的存储单元 230 的范围。安全密钥在加密单元 346 中使用，该加密单元 346 可以是高级加密系统 (AES) 或数据加密系统 (DES) 加密器或任何合适的加密器。

[0081] 参考图 4，图示了表示本总的发明构思的示例性实施例的存储设备 400 的方块图。存储设备 400 经由总线 415 与处理器 420 通信，并且通过接口 410 通信到外部设备 405。可以使用串行 ATA 驱动器和接口，或者可以使用任何其它合适的驱动器和接口标准。可以使用发送命令并从外部存储器接收数据的任何合适的处理器或主机。处理器 400 可以包括附加的存储单元，例如 ROM 或 RAM，以便执行数据处理。

[0082] 取代 0 传统上执行的处理器 42，命令解析器 441 解析命令，例如读或写命令，并且提取地址。下文中在图 5 到图 7 中图示了命令解析器 441 的操作。

[0083] 由命令解析器 441 解析的地址 (可以是 LBA) 被 LAB 解码单元 442 结合密钥单元 444 用来生成安全密钥。该安全密钥在加密单元 446 中被用来加密或解密存储在存储设备 400 上的存储器 430 中的数据。在加密或解密之后，数据被传递到处理器 420 用于处理。因为在单个硬件解决方案中发生了解析、解码和加密 / 解码，因此数据在响应命令被传递到处理器 420 之前不被传递到处理器 420 用于加密 / 解密。

[0084] 可替换地，LBA 解码单元 442 可以使用地址来生成密钥标志。密钥标志随后被传递到加密单元 446，该加密单元 446 使用密码标志来从密钥单元 444 中选择安全密钥。该安全密钥随后被加密单元 446 使用来加密或解密存储器 430 中存储的数据，如上。

[0085] 命令解析器 441 可以通过总线 415 将子命令发送到处理器 420 并且还发送到 LBA 解码单元 442。一旦接收到命令，处理器 420 和 LBA 解码单元 442 就可以同时地分别执行数据的处理和安全密钥的选择。

[0086] 图 5 图示了图 4 的命令解析器 441 的示例性操作。命令解析器 441 接收来自外部设备例如主机装置 405 的命令，以帧为形式，并且解析该帧以便确定该帧中指定的地址。串行 ATA 硬件架构实现中的传统主机到装置帧信息结构 (FIS) 包括 ：帧开始 (SOF) 分隔符、包括传输层信息的有效载荷、循环冗余码校验 (CRC) 和帧结束 (EOF) 分隔符。FIS 也包括逻辑块地址 500，它的形式可以是圆柱形、头形和扇形，并且包括 Cyl 高和 Cyl 低、以及 Cyl 高 (exp) 和 Cyl 低 (exp)。Cyl 高包括存储单元 430 的圆柱体高寄存器的内容，并且 Cyl 低包括存储单元 430 的圆柱体低寄存器的内容。Cyl 高 (exp) 和 Cyl 低 (exp)

包括存储单元 430 的扩展地址字段的内容。 逻辑块地址 500 被命令解析器 441 解析并且被 LBA 解码单元 442 和密钥单元 444 用来生成安全密钥或密钥标志。

[0087] 图 6 图示了在由图 4 的命令解析器 441 使用的串行 ATA 硬件架构实现中的装置到主机帧信息结构 (FIS)。 逻辑块地址 600 的形式可以是圆柱形、头形和扇形，并且包括 Cyl 高和 Cyl 低、以及 Cyl 高 (exp) 和 Cyl 低 (exp)。 逻辑块地址 600 被命令解析器 441 解析并且被 LBA 解码单元 442 和密钥单元 444 用来生成安全密钥或密钥标志。

[0088] 图 7 图示了在由图 4 的命令解析器 441 使用的串行 ATA 硬件架构实现中的另一装置到主机帧信息结构 (FIS)。 逻辑块地址 700 的形式可以是圆柱形、头形和扇形，并且包括 Cyl 高和 Cyl 低、以及 Cyl 高 (exp) 和 Cyl 低 (exp)。 逻辑块地址 700 被命令解析器 441 解析并且被 LBA 解码单元 442 和密钥单元 444 用来生成安全密钥或密钥标志。

[0089] 图 8 到图 11 图示了本总的发明构思的实施例的各种示例性简化的计算机架构。

[0090] 参考图 8，使用下面图 12 中描述的方法， CPU 810 经由串行 ATA 接口 820 与光盘驱动器 (ODD)830 通信。 ODD 830 可以包括如上面参考图 1 所述的在加密和解密数据中使用的处理器和密钥单元，该 ODD 830 被 CPU 810 使用。 可替换地， ODD 830 可以包括如上面参考图 2 所述的在加密和解密数据中使用的处理器、密钥单元、解码单元和加密单元，该 ODD 830 被 CPU 810 使用。

[0091] 参考图 9，CPU 910 经由串行 ATA 接口 920 与硬盘驱动器 (HDD)930 通信。HDD 930 可以包括如上面参考图 1 所述的在加密和解密数据中使用的处理器和密钥单元，该 HDD 930 被 CPU 910 使用。 可替换地，HDD 930 可以包括如上面参考图 2 所述的在加密和解密数据中使用的处理器、密钥单元、解码单元和加密单元，该 HDD 930 被 CPU 910 使用。

[0092] 参考图 10，CPU 1010 经由多媒体卡控制器 1020 与多媒体卡 1030 通信。 多媒体卡 1030 可以包括如上面参考图 1 所述的在加密和解密数据中使用的处理器和密钥单元，该多媒体卡 1030 被 CPU 1010 使用。 可替换地，多媒体卡 1030 可以包括如上面参考图 2 所述的在加密和解密数据中使用的处理器、密钥单元、解码单元和加密单元，该多媒体卡 1030 被 CPU 1010 使用。

[0093] 参考图 11， CPU 1110 经由安全数字接口 1120 与安全数字卡 (SD 卡)1130 通信。 SD 卡 1130 可以包括如上面参考图 1 所述的在加密和解密数据中使用的处理器和密钥单元，该 SD 卡 1130 被 CPU 1110 使用。 可替换地， SD 卡 1130 可以包括如上面参考图 2 所述的在加密和解密数据中使用的处理器、密钥单元、解码单元和加密单元，该 SD 卡 1130 被 CPU 1110 使用。

[0094] 图 12 示出了本总的发明构思的实施例的流程图。 为了图示目的，使用图 4 的存储设备 400 来描述图 12。 在操作 S1205，存储设备 400 接收命令。 在操作 S1210，命令解析器 441 解析该命令。 从该命令中解析逻辑块地址 (LBA)，并且通过 LBA 解码单元 442 将该 LBA 与当前 LBA 相比较。 如果 LBA 不同，则在操作 S1215，新 LBA 被 LBA 解码单元 442 使用。 如果 LBA 相同，则在加密和解密中加密单元 446 使用当前 LBA 和安全密钥。 在操作 S1220，新 LBA 在 LBA 解码单元 442 中被用来生成合适的密钥标志。 根据 LBA 解码单元 442 生成的密钥标志，在操作 S1225 从密钥单元 444 选择安全密钥，并且之后在加密和解密数据中由加密单元 446 使用该安全密钥。

[0095] 类似地，在图 1 的安全存储设备 100 中，安全存储设备 100 接收命令。同时地，处理器 120 响应该命令来处理数据，并且密钥单元 140 使用该命令的地址信息来选择安全密钥。密钥单元 140 使用该安全密钥来加密或解密数据。

[0096] 类似地，在图 1 的安全存储设备 200 中，安全存储设备 200 接收读 / 写请求。解码单元 242 从可以是逻辑块地址的读 / 写请求中解析地址，并且生成与该逻辑块地址对应的密钥标志。密钥单元 244 使用该密钥标志选择安全密钥，并且加密单元 246 使用该安全密钥来解密数据或加密数据，如读 / 写请求所指定的。当数据被解密或加密时，数据被传递到处理器 220 用以进一步处理，包括将解密后的数据传递到主机设备 205 或者将加密后的数据写入存储器 230。

[0097] 图 13 示出了本总的发明构思的实施例的流程图。为了图示目的，使用图 1A 和图 1B 的存储设备 100 来描述图 13。在操作 S1305，存储设备 100 从主机设备 105 接收命令。该命令被同时地传递到处理器 120 和密钥单元 140。在操作 S1310，处理器 120 开始根据命令处理数据。密钥单元 140 在操作 S1215 执行数据的加密或解密。当完成加密或解密时，处理器 120 在操作 S1220 完成加密后或解密后的数据的处理。因此，处理器 120 开始处理数据，同时密钥单元 140 正在执行数据的加密或解密，并且当完成加密或解密时，通过处理器 120 来完成加密后或解密后的数据的处理。

[0098] 本总的发明构思还可以具体为计算机可读介质上的计算机可读代码。计算机可读介质可以包括计算机可读记录介质和计算机可读传输介质。所述计算机可读记录介质是可以将数据存储为其后可由计算机系统读取的程序的任何数据存储装置。计算机可读记录介质的示例包括只读存储器 (ROM)、随机存取存储器 (RAM)、CD-ROM、磁带、软盘、光数据存储装置。计算机可读记录介质还可以分布在与计算机系统耦接的网络上，从而以分布式方式来存储和运行计算机可读代码。计算机可读传输介质可以发送载波或信号（例如，通过因特网的有线或无线数据传输）。另外，用于实现本总的发明构思的功能程序、代码和代码段能够被本总的发明构思所属领域的编程技术人员容易地解读。

[0099] 虽然已经示出并描述了本总的发明构思的数个实施例，但是本领域的普通技术人员将会理解，在这些实施例中可以进行变化，而不脱离本总的发明构思的原理和精神，本总的发明构思的范畴限定于所附权利要求及它们的等效物中。

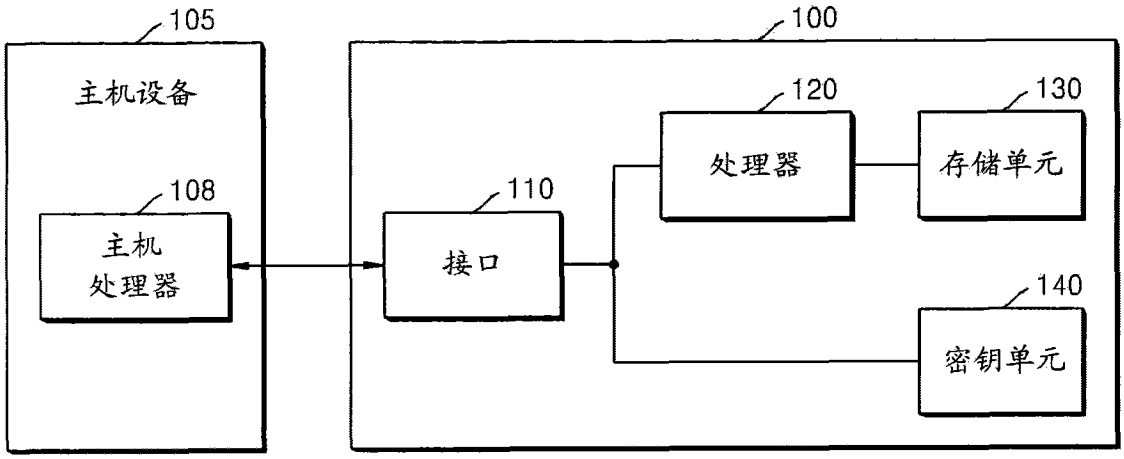

105
主机设备
108
主机
处理器
100
110
接口
120
处理器
130
存储单元
140
密钥单元

图 1A

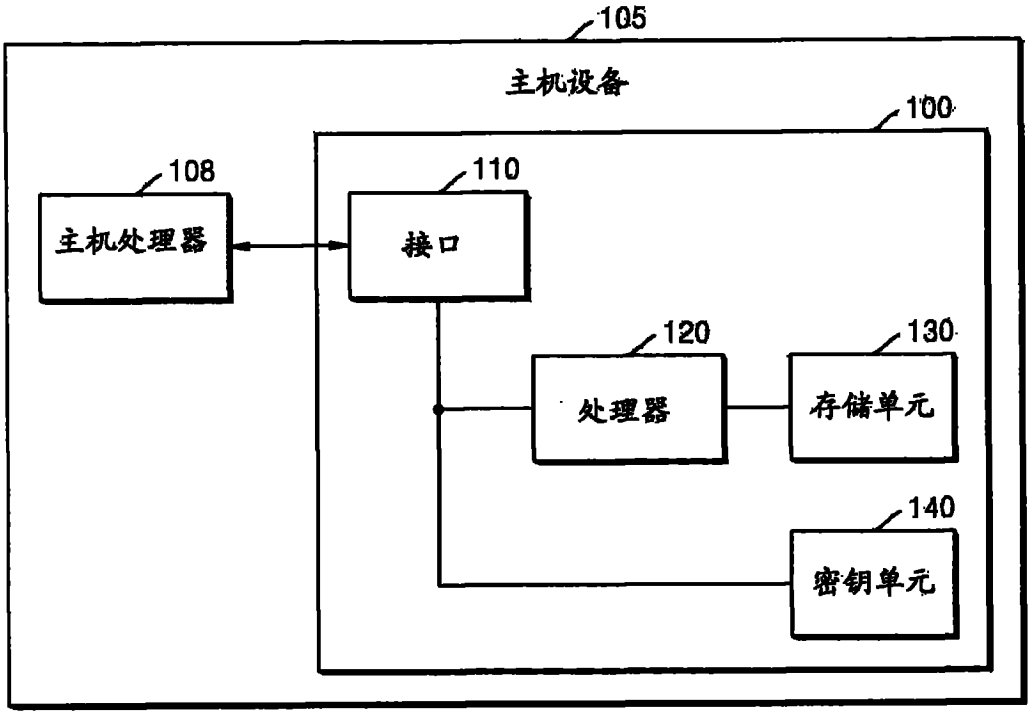

105
主机设备
100
108
主机处理器
110
接口
120
处理器
130
存储单元
140
密钥单元

图 1B

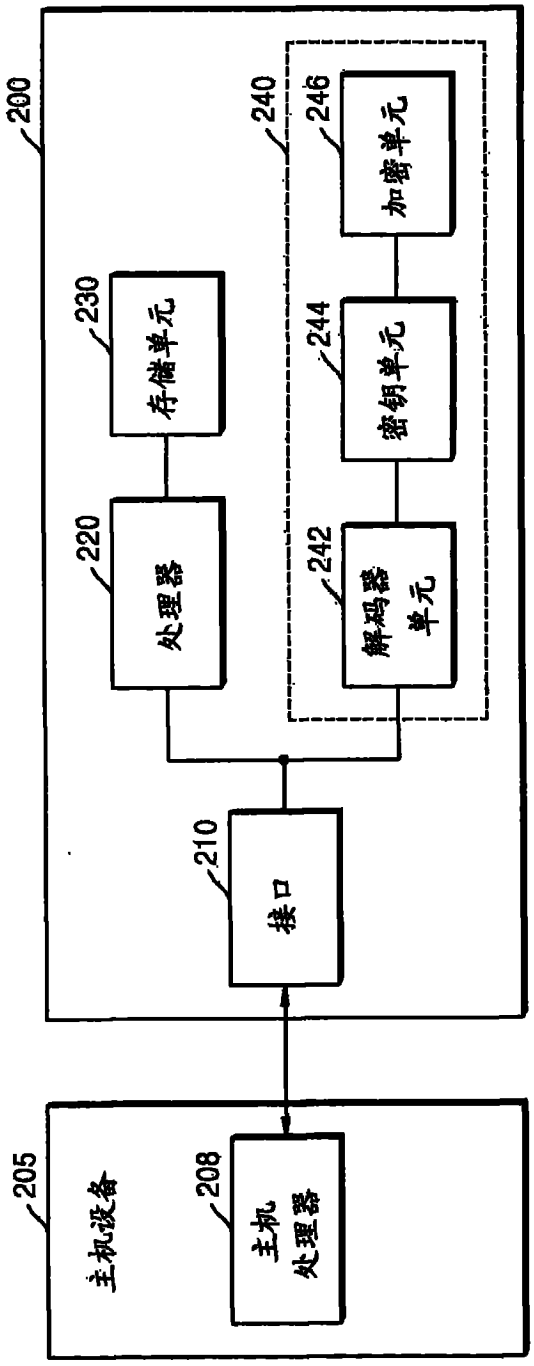

200
240
246
加密单元
230
存储单元
244
密钥单元
220
处理器
242
解码器单元
210
接口
205
主机设备
208
主机处理器

图 2A

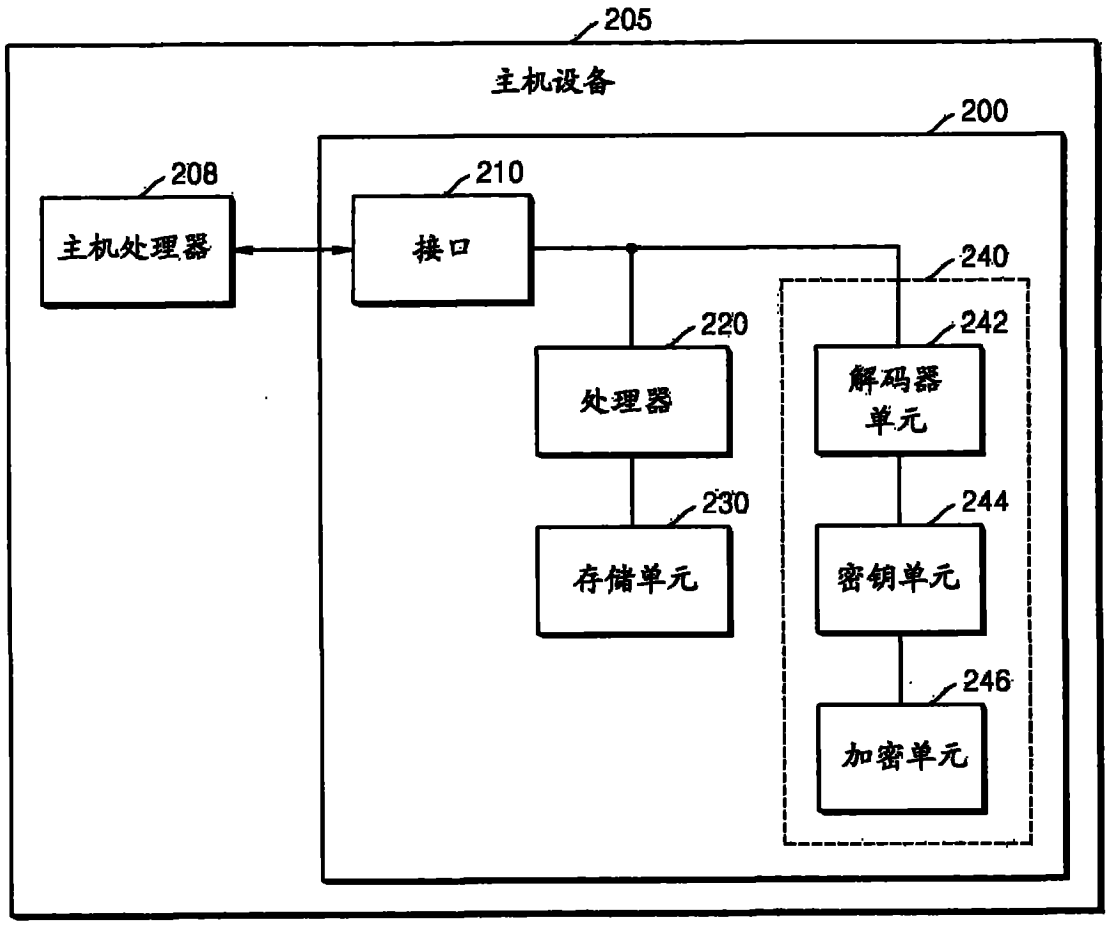

205
主机设备
200
208
主机处理器
210
接口
240
220
处理器
242
解码器
单元
230
存储单元
244
密钥单元
246
加密单元

图 2B

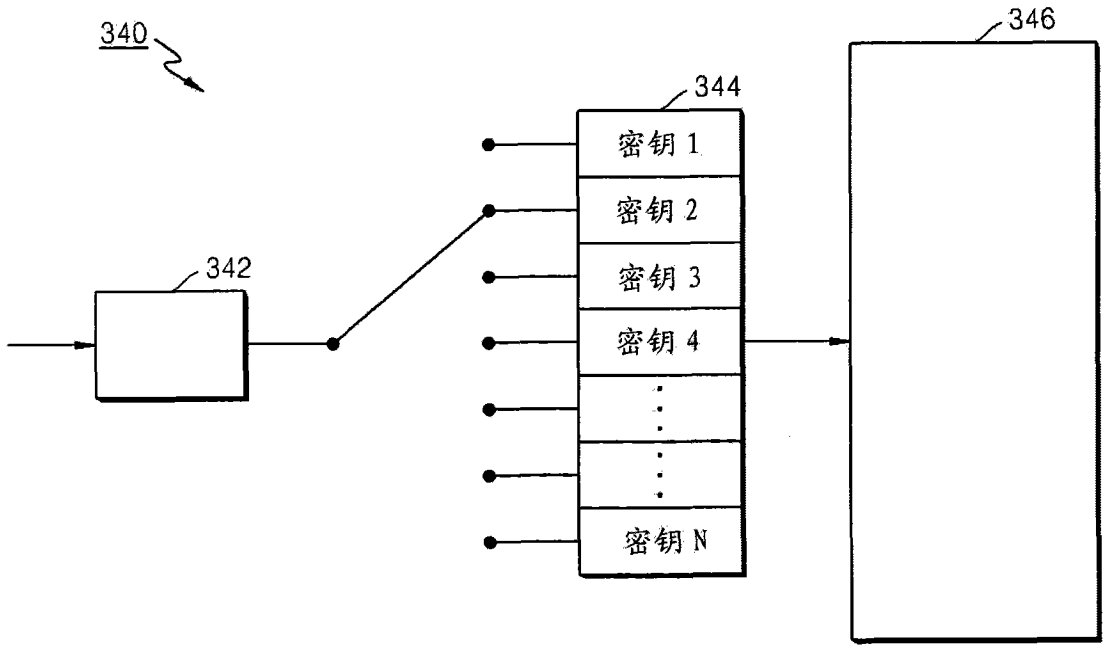


图 3

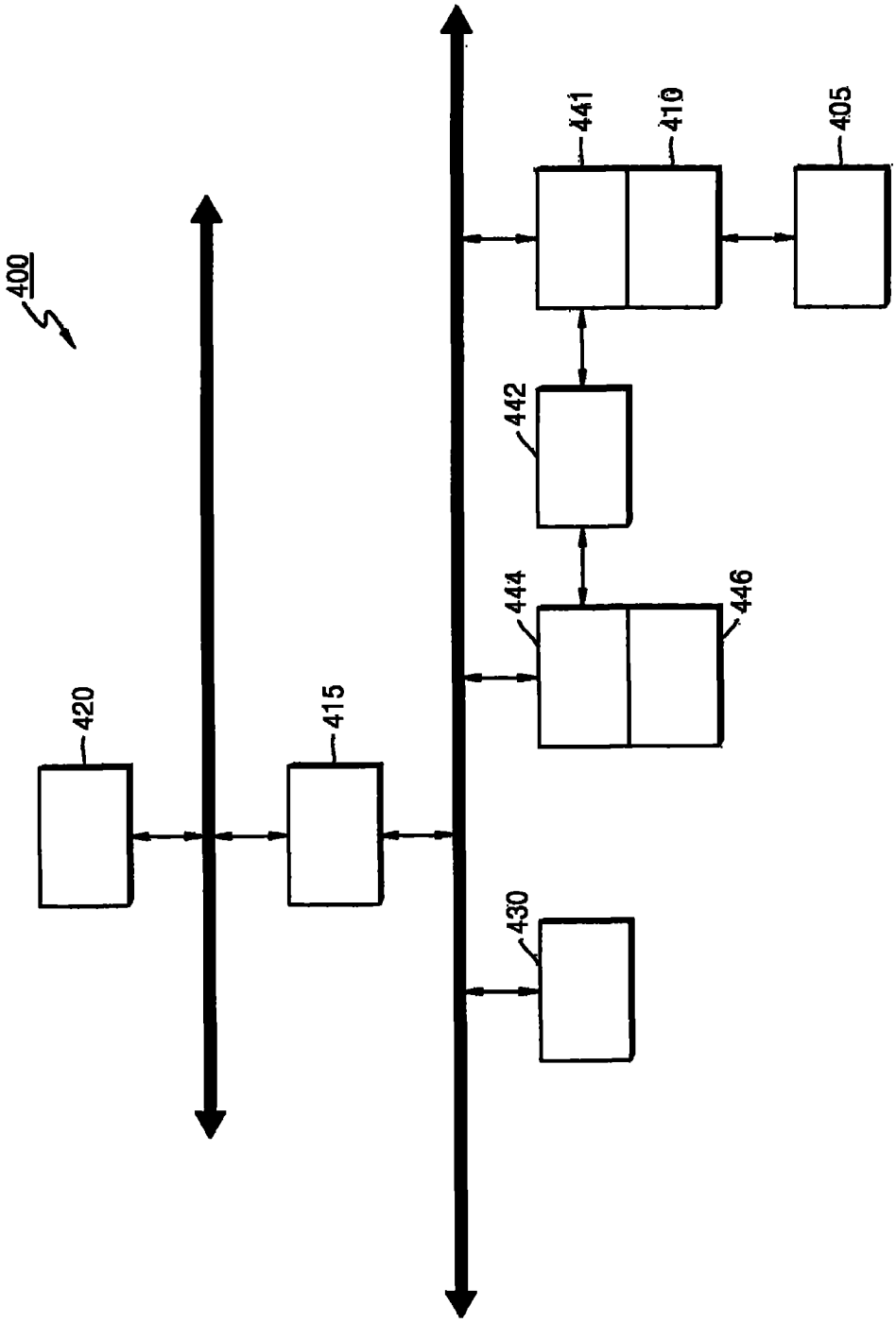


图 4

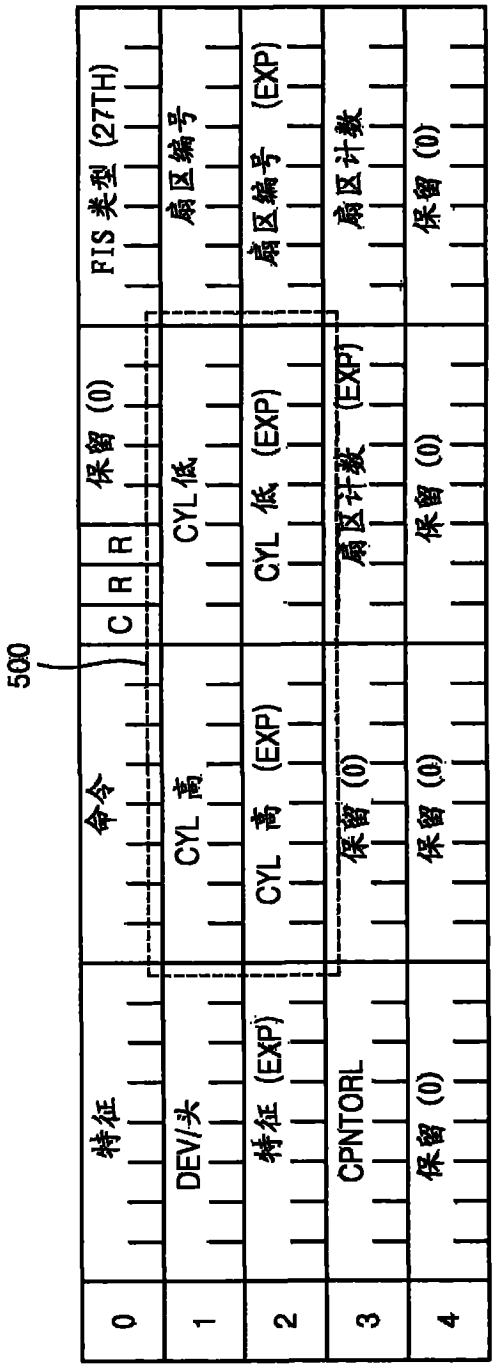

500
0
1
2
3
4
特征
DEV/头
特征 (EXP)
CPNTORL
保留 (0)
命令
CYL 高
CYL 高 (EXP)
保留 (0)
保留 (0)
C
R
R
保留 (0)
CYL 低
CYL 低 (EXP)
扇区计数 (EXP)
保留 (0)
FIS 类型 (27TH)
扇区编号
扇区编号 (EXP)
扇区计数
保留 (0)

图 5

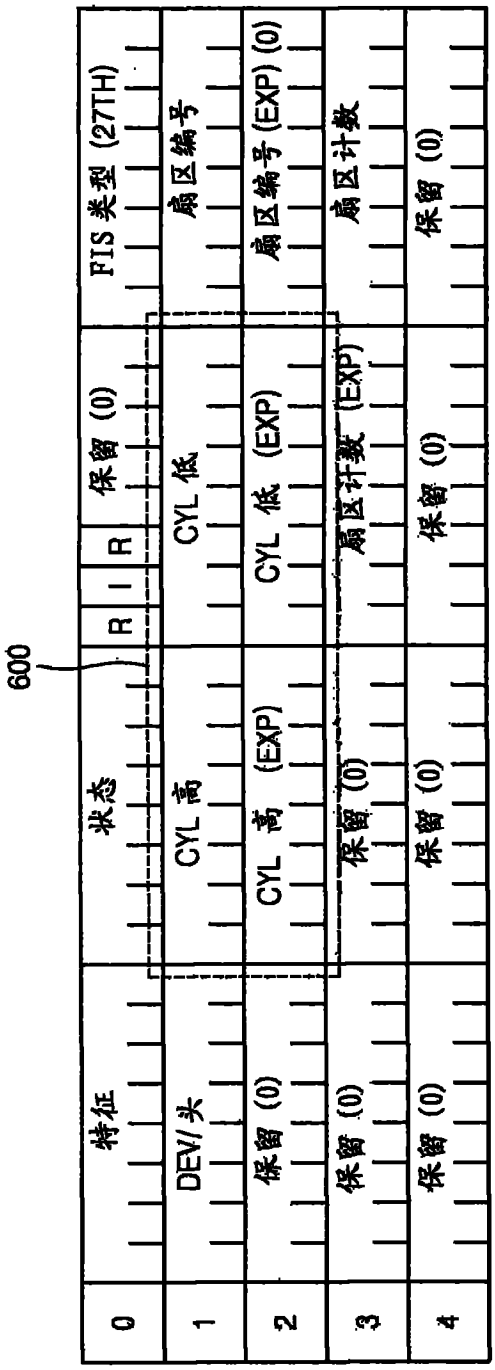

600
0
1
2
3
4
特征
DEV/头
保留 (0)
保留 (0)
保留 (0)
状态
CYL 高
CYL 高 (EXP)
保留 (0)
保留 (0)
R
I
R
保留 (0)
CYL 低
CYL 低 (EXP)
扇区计数 (EXP)
保留 (0)
FIS 类型 (27TH)
扇区编号
扇区编号 (EXP) (0)
扇区计数
保留 (0)

图 6

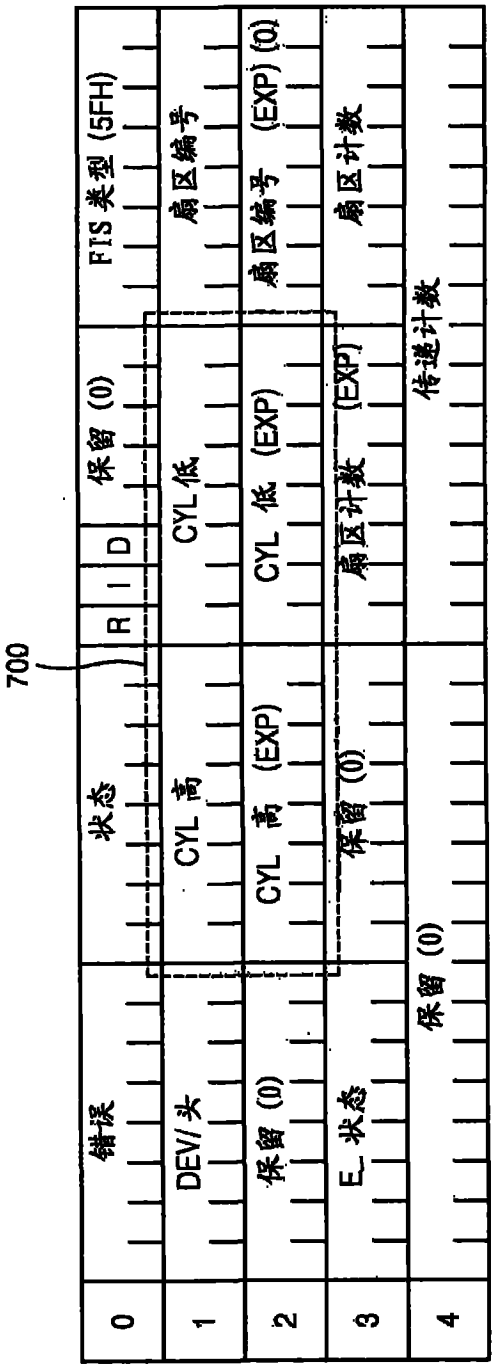

700
0
1
2
3
4
错误
状态
FIS 类型 (5FH)
DEV/ 头
CYL 高
CYL 低
扇区编号
保留 (0)
R
I
D
保留 (0)
CYL 高 (EXP)
CYL 低 (EXP)
扇区编号 (EXP) (0)
E_状态
保留 (0)
扇区计数 (EXP)
扇区计数
保留 (0)
传递计数

图 7

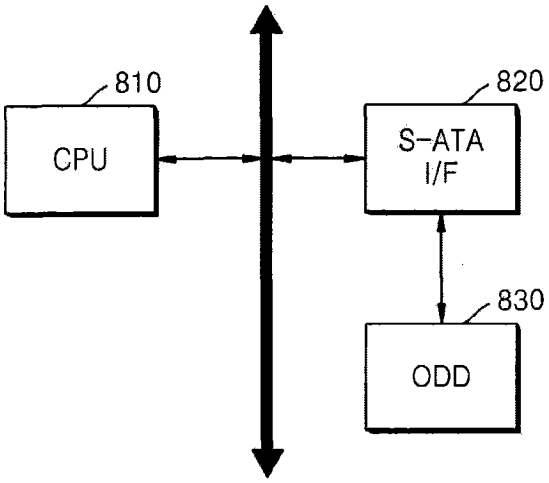

810
CPU
820
S-ATA
I/F
830
ODD

图 8

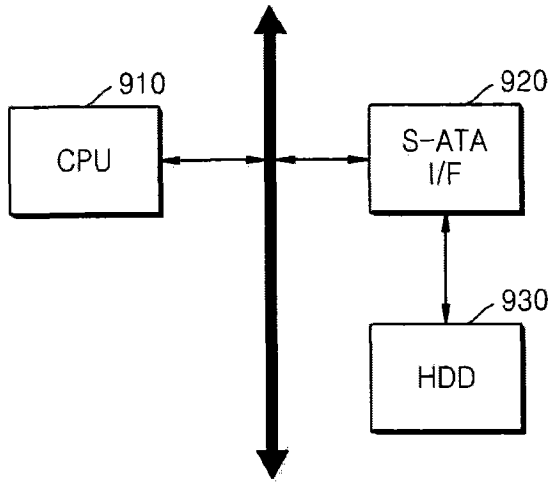

910
CPU
920
S-ATA
I/F
930
HDD

图 9

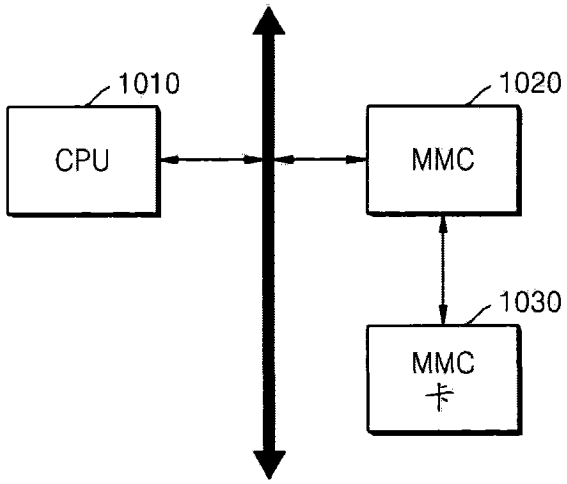

1010
CPU
1020
MMC
1030
MMC
卡

图 10

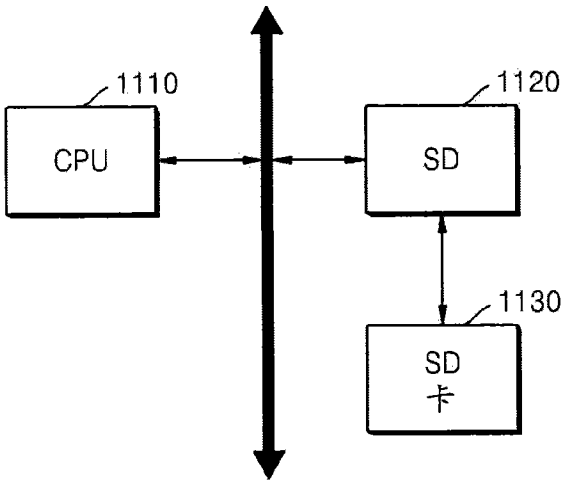

1110
CPU
1120
SD
1130
SD
卡

图 11

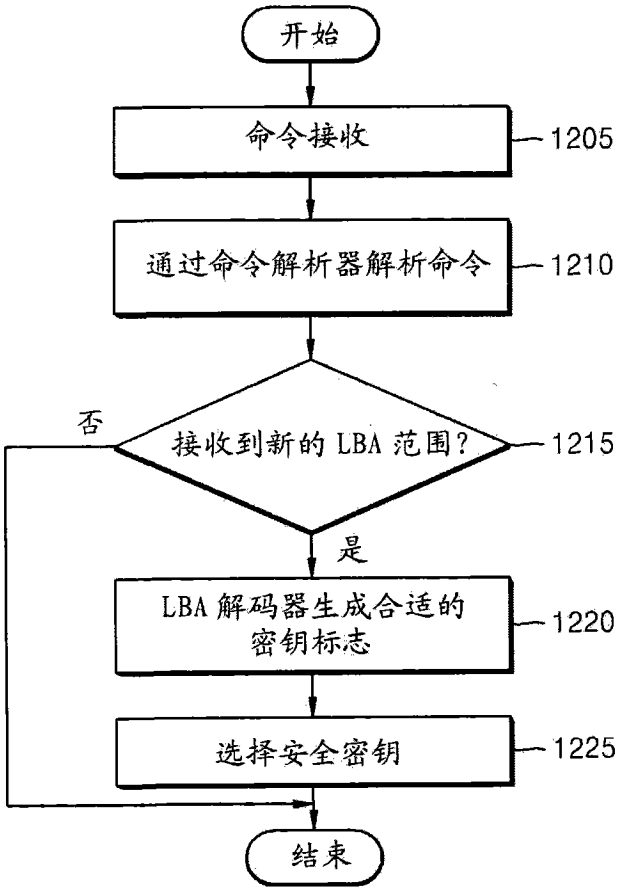

开始
命令接收
1205
通过命令解析器解析命令
1210
否
接收到新的 LBA 范围?
1215
是
LBA 解码器生成合适的密钥标志
1220
选择安全密钥
1225
结束

图 12

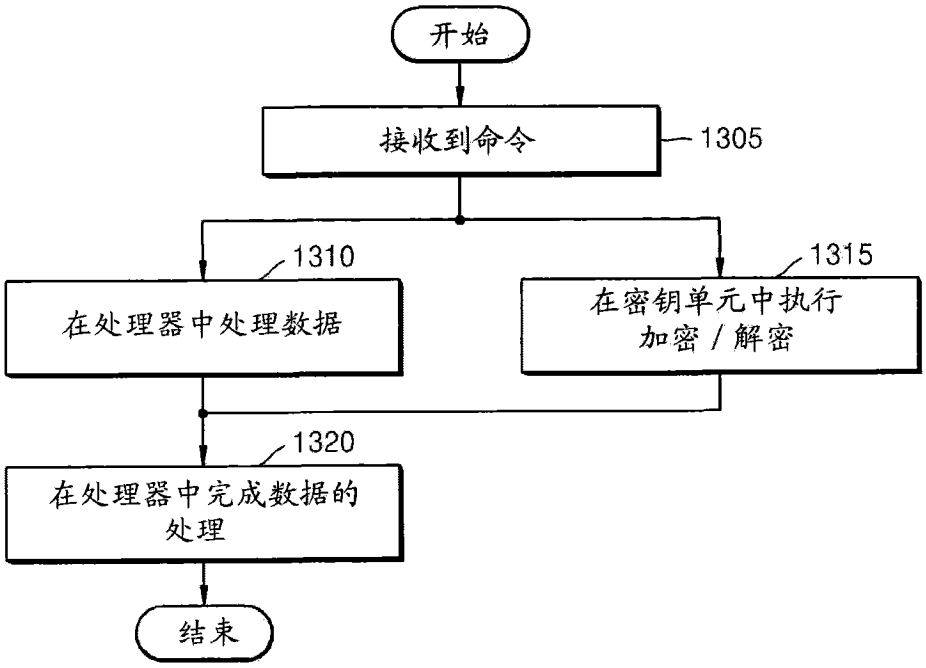

开始
接收到命令
1305
1310
在处理器中处理数据
1315
在密钥单元中执行
加密 / 解密
1320
在处理器中完成数据的
处理
结束

图 13