[19] 中华人民共和国国家知识产权局

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

[12] 发明专利说明书

专利号 ZL 200710062695.6

[45] 授权公告日 2009 年 5 月 13 日

[11] 授权公告号 CN 100487715C

[22] 申请日 2007.1.12
[21] 申请号 200710062695.6
[73] 专利权人 深圳兆日技术有限公司
地址 518040 广东省深圳市福山区泰然九路 213 栋 6 层 C－3 座
[72] 发明人 乔 椿 刘长生 王 梓 王庆军 张 璐
[74] 专利代理机构 北京律诚同业知识产权代理有限公司
代理人 梁 挥 祁建国
[56] 参考文献
CN1218598C 2005.9.7
CN1211776A 1999.3.24
JP2003－134102A 2003.5.9
US2006/0288232A1 2006.12.21
CN1571949A 2005.1.26
审查员 张 勇

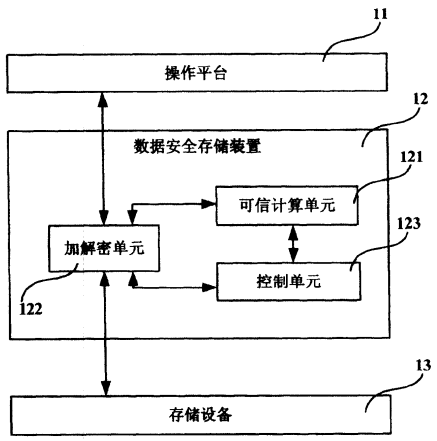
权利要求书 6 页 说明书 19 页 附图 6 页

[54] 发明名称

一种数据安全存储系统和装置及方法

[57] 摘要

本发明公开了一种数据安全存储系统和装置及方法，包括操作平台，存储设备，还包括可信计算单元，用于保护对操作平台和存储设备间读写的数据进行加解密的密钥；加解密单元，用于从可信计算单元读取密钥，利用相应的设定的加解密算法，对操作平台与存储设备之间读写的数据进行加解密；控制单元，用于对可信计算单元和加解密单元进行初始化，并控制加解密单元利用密钥加解密在操作平台和存储设备间读写的数据。 其对用户操作要求低，使用过程简单，适应用户的要求。



1、一种数据安全存储系统，包括操作平台，存储设备，其特征在于，还包括可信计算单元，加解密单元，其中：

所述可信计算单元，用于对所述操作平台的唯一性标识进行唯一性标识匹配判断，所述唯一性标识为第一唯一性标识，并控制所述操作平台对所述存储设备的数据安全存储读写，从而保护对操作平台和存储设备间读写的数据进行加解密的密钥；

所述加解密单元，用于获取密钥，并利用相应的设定的加解密算法，对操作平台与存储设备之间读写的数据进行加解密。

2、根据权利要求 1 所述的数据安全存储系统，其特征在于，还包括控制单元，用于对可信计算单元和加解密单元进行初始化，并控制加解密单元利用密钥加解密在操作平台和存储设备间读写的数据。

3、根据权利要求 1 所述的数据安全存储系统，其特征在于，所述密钥存储于可信计算单元。

4、根据权利要求 1 所述的数据安全存储系统，其特征在于，所述可信计算单元还存储用于匹配判断的操作平台的第一唯一性标识。

5、根据权利要求 2 所述的数据安全存储系统，其特征在于，所述控制单元包括密钥判断子单元，读写控制子单元，其中：

密钥判断子单元，用于判断可信计算单元中是否有密钥，是否需要对操作平台与存储设备间的读写数据进行加解密，并根据判断结果读取操作平台的第二唯一性标识；

读写控制子单元，用于在操作平台读取存储设备中的数据时，控制加解密单元对操作平台和存储设备之间的读写数据进行加解密。

6、根据权利要求 5 所述的数据安全存储系统，其特征在于，所述控制单元还包括初始化子单元，用于操作平台硬件加电，对初始化软件进行初始化时，加载可信计算环境，并初始化可信计算环境。

7、根据权利要求 1 所述的数据安全存储系统，其特征在于，所述加解密单元包括读取数据解密子单元和写入数据加密子单元，其中：

读取数据解密子单元，用于在操作平台向存储设备读取数据时，将该数据

截获并解析，得到原始的加密数据，将该数据解密，得到未加密数据，然后按原传输格式将未加密数据打包，传输给操作平台；

写入数据加密子单元，用于在操作平台对存储设备写入数据时，将该数据截获并解析，得到原始的未加密数据，将该数据加密，得到加密数据，然后按原传输格式将加密数据打包，写入到存储设备中去。

8、根据权利要求 5 所述的数据安全存储系统，其特征在于，所述可信计算单元包括匹配控制子单元，用于读取所述第一唯一性标识，并将所述第一唯一性标识与所述密钥判断子单元读取的所述第二唯一性标识匹配检查。

9、根据权利要求 8 所述的数据安全存储系统，其特征在于，所述可信计算单元还包括密钥存储子单元，用于存储加解密密钥和第一唯一性标识。

10、根据权利要求 9 所述的数据安全存储系统，其特征在于，所述可信计算单元还包括密钥生成子单元，用于根据操作平台第一唯一性标识，生成相应的加解密密钥。

11、根据权利要求 1 所述的数据安全存储系统，其特征在于，所述操作平台为计算机系统平台，或者单片机系统平台，或者手机、PDA、U 盘、MP3、MP4 和操作所述手机、PDA、U 盘、MP3、MP4 的网络共同组成的主从架构的网络平台。

12、根据权利要求 1 所述的数据安全存储系统，其特征在于，所述存储设备是 RAM，或者硬盘，或者闪存中的一种以上的组合。

13、根据权利要求 1 所述的数据安全存储系统，其特征在于，所述唯一性标识，对计算机系统而言，包括：

计算机主板的系列号；或者

中央处理器序列号；或者

设备序列号；或者

操作系统序列号；或者

应用软件序列号中的一种以上的组合。

14、根据权利要求 1 所述的数据安全存储系统，其特征在于，所述唯一性标识，对通信网络系统而言，包括：

手机的 SIM 卡号；或者

手机的国际移动电话识别码中的一种或者两者组合。

15、根据权利要求 1 所述的数据安全存储系统，其特征在于，所述唯一性标识为对操作平台中表示软件平台、硬件平台的特征数据进行哈希运算，所得计算结果的完整性度量值。

16、根据权利要求 10 所述的数据安全存储系统，其特征在于，所述密钥生成子单元是通过哈希函数生成加解密密钥。

17、根据权利要求 1 所述的数据安全存储系统，其特征在于，所述加解密算法为 DES 算法、IDEA 算法、AES 算法、RSA 算法、Diffie-Hellman 算法、ECC 算法中的一种以上的组合。

18、一种数据安全存储装置，与操作平台和存储设备电连接，其特征在于，包括可信计算单元，加解密单元，其中：

所述可信计算单元，用于对所述操作平台的唯一性标识进行唯一性标识匹配判断，所述唯一性标识为第一唯一性标识，并控制所述操作平台对所述存储设备的数据安全存储读写，从而保护对操作平台和存储设备间读写的数据进行加解密的密钥；

所述加解密单元，用于获取密钥，利用相应的设定的加解密算法，对操作平台与存储设备之间读写的数据进行加解密。

19、根据权利要求 18 所述的数据安全存储装置，其特征在于，还包括控制单元，用于对可信计算单元和加解密单元进行初始化，并控制加解密单元利用密钥加解密在操作平台和存储设备间读写的数据。

20、根据权利要求 18 所述的数据安全存储装置，其特征在于，所述密钥存储于可信计算单元。

21、根据权利要求 18 所述的数据安全存储装置，其特征在于，所述可信计算单元还存储用于匹配判断的操作平台的第一唯一性标识。

22、根据权利要求 18 所述的数据安全存储装置，其特征在于，所述控制单元包括密钥判断子单元，读写控制子单元，其中：

密钥判断子单元，用于判断可信计算单元中是否有密钥，是否需要对操作平台与存储设备间的读写数据进行加解密，并根据判断结果读取操作平台的第二唯一性标识；

读写控制子单元，用于在操作平台读取存储设备中的数据时，控制加解密单元对操作平台和存储设备之间的读写数据进行加解密。

23、根据权利要求 22 所述的数据安全存储装置，其特征在于，所述控制单元还包括初始化子单元，用于操作平台硬件加电，对初始化软件进行初始化时，加载可信计算环境，并初始化可信计算环境。

24、根据权利要求 18 所述的数据安全存储装置，其特征在于，所述加解密单元包括读取数据解密子单元和写入数据加密子单元，其中：

读取数据解密子单元，用于在操作平台向存储设备读取数据时，将该数据截获并解析，得到原始的加密数据，将该数据解密，得到未加密数据，然后按原传输格式将未加密数据打包，传输给操作平台；

写入数据加密子单元，用于在操作平台对存储设备写入数据时，将该数据截获并解析，得到原始的未加密数据，将该数据加密，得到加密数据，然后按原传输格式将加密数据打包，写入到存储设备中去。

25、根据权利要求 22 所述的数据安全存储装置，其特征在于，所述可信计算单元包括匹配控制子单元，用于读取所述第一唯一性标识，并将所述第一唯一性标识与所述密钥判断子单元读取的所述第二唯一性标识匹配检查。

26、根据权利要求 25 所述的数据安全存储装置，其特征在于，所述可信计算单元还包括密钥存储子单元，用于存储加解密密钥和唯一性标识。

27、根据权利要求 26 所述的数据安全存储装置，其特征在于，所述可信计算单元还包括密钥生成子单元，用于根据操作平台唯一性标识，生成相应的加解密密钥。

28、根据权利要求 18 所述的数据安全存储装置，其特征在于，所述数据安全存储装置是一种独立于操作平台和存储设备的硬件设备。

29、一种数据安全存储方法，其特征在于，包括下列步骤：

步骤 A，在需要处理存储设备中的数据时，对操作平台上电并初始化，并初始化可信计算环境，对所述操作平台的唯一性标识进行匹配判断，所述唯一性标识为第一唯一性标识，并控制操作平台对存储设备的数据安全存储读写；

步骤 B，在确认需要对存储设备进行数据安全存储读写后，读取密钥，利用相应的设定的加解密算法，对操作平台与存储设备之间读写的数据进行加解密。

30、根据权利要求 29 所述的数据安全存储方法，其特征在于，所述步骤 A 中，通过唯一性标识匹配判断并控制操作平台对存储设备的数据安全存储读

写，具体包括下列步骤：

步骤 A1，判断可信计算环境中是否有密钥，如果没有则转步骤 A2；否则转步骤 A4；

步骤 A2，判断该操作平台与存储设备间读写数据是否需要进行加解密；如果否，则正常启动，不对操作平台与存储设备之间读写的数据进行任何处理，用户正常使用后结束；否则转步骤 A3；

步骤 A3，生成相应的加解密密钥，转到步骤 B；

步骤 A4，如果可信计算单元中已经有密钥存在，则读取第一唯一性标识，将该第一唯一性标识与从本操作平台上读取的第二唯一性标识进行匹配检查；

步骤 A5，如果匹配通过，则检查通过，得到密钥，转到步骤 B；否则，给出信息后，结束返回。

31、根据权利要求 30 所述的数据安全存储方法，其特征在于，所述步骤 A4 还包括下列步骤：

在读取第一唯一性标识时指定要求用户核对口令，如果用户输入口令与该第一唯一性标识的口令不同，则不允许用户得到该第一唯一性标识。

32、根据权利要求 29 至 31 任一项所述的数据安全存储方法，其特征在于，所述步骤 B 中对操作平台与存储设备之间读写的数据进行加解密，具体包括下列步骤：

步骤 B1，在操作平台读取存储设备中的数据时，将该数据截获并解析，得到原始的加密数据，将该数据解密，得到未加密数据，然后按原传输格式将未加密数据打包，传输给操作平台；

步骤 B2，在操作平台对存储设备写入数据时，将该数据截获并解析，得到原始的未加密数据，将该数据加密，得到加密数据，然后按原传输格式将加密数据打包，写入到存储设备中去。

33、根据权利要求 29 至 31 任一项所述的数据安全存储方法，其特征在于，所述唯一性标识，对计算机系统而言，包括：

计算机主板的系列号；或者

中央处理器序列号；或者

设备序列号；或者

操作系统序列号；或者

应用软件序列号中的一种以上的组合。

34、根据权利要求 29 至 31 任一项所述的数据安全存储方法，其特征在于，所述唯一性标识，对通信网络系统而言，包括：

手机的 SIM 卡号；或者

手机的国际移动电话识别码中的一种或者两者组合。

35、根据权利要求 29 至 31 任一项所述的数据安全存储方法，其特征在于，所述唯一性标识为对操作平台中表示软件平台、硬件平台的特征数据进行哈希运算，所得计算结果的完整性度量值。

36、根据权利要求 30 所述的数据安全存储方法，其特征在于，所述密钥生成为根据唯一性标识由哈希函数生成加解密密钥。

37、根据权利要求 36 所述的数据安全存储方法，其特征在于，所述加解密算法为 DES 算法、IDEA 算法、AES 算法、RSA 算法、Diffie-Hellman 算法、ECC 算法中的一种以上的组合。

一种数据安全存储系统和装置及方法

技术领域

本发明涉及数据安全领域，特别是涉及一种可信的数据的加解密安全存储的系统和装置及方法。

背景技术

随着现代通讯技术的快速发展，在通讯设备中对数据的处理量也越来越大，通讯设备中的很多数据也需要在运行过程中，或者在运行结束后存储到不同的存储设备中，如随机读取存储器（RAM），硬盘，或者闪存（Flash）等。这样的通讯设备既有微型计算机（PC），也有小、中、大型服务器，以及笔记本电脑，还有手机、PDA、U盘，MP3、MP4等各种新型的移动通讯设备。

通讯设备中存储的数据，如计算机中的数据，常常存储在硬盘上，而如果用硬盘来存储一些安全性较高的数据，如商业秘密，国家安全秘密，国防安全数据等等，如果该硬盘丢失或者失窃将会带来很大的危险，尤其是对于便携式设备和移动设备，它们通常会更方便携带，也就更危险，安全保护方面的要求更高，安全威胁会更大。

一般地，为了数据在存储中的安全，通讯设备的用户可能会利用一些加解密方法对数据进行加密，然后才存储到相应的存储设备中。

对临时或永久存储在存储设备中的数据，以及通讯传输数据的加密和解密的方法，在本领域普通技术人员中都已经有实现的产品。大多数技术人员采用加解密方法是用一个密钥来加密数据，同时，通常要求接收加密传输的数据或者从存储在存储设备读取加密数据的一方拥有跟加密一方相同或者配对的密钥才能解密。因此，任何一方未经授权的人员都不应当知道或者获得密钥，不得加解密数据，不能获得相关的数据，从而达到对存储数据的安全保护。

中国专利申请号：200610000047.3 公开了 一种移动存储设备的数据安全存储和处理方法，它涉及移动存储设备的数据保护技术，特别涉及独立于智能密码钥匙而独立使用的专用移动存储设备的数据存储、处理方法。它用移动保

险柜系统工具为移动存储设备中需要加密保护的数据创建专属于合法用户的虚拟加密文件目录。合法用户可以在其中创建、修改和删除文件，可以把移动存储设备中未加密保护的数据拖放到移动保险柜中实施加密，也可以把移动保险柜中被加密保护的数据拖放到移动存储设备中未加密保护的公共区域，以实施解密。对于非法用户，移动保险柜永远是一个加密的磁盘文件，不能打开，也不能获取其中的内容。

中国专利申请号：200510124652.7 也公开了一种用于存储数据的透明端到端安全的设备、系统和方法。该发明包括与服务器进行通信的一个或多个客户机。客户机期望将存储结构发送到存储服务器。客户机与服务器关于传输密钥进行协商。客户机产生专门与存储结构相关联的存储密钥。客户机使用存储密钥将存储结构加密，使用传输密钥将存储密钥加密。将加密的存储结构和加密的存储密钥发送到服务器。服务器使用传输密钥将存储密钥解密。服务器在与用于存储密钥的存储设备不同的存储设备上存储结构。最好是，跟踪关于存储结构位置、存储密钥位置，或存储结构名的任何变化，并对关于存储结构的位置和对应存储密钥的位置的关联进行适当修改。

但是，现有的加解密被存储数据的安全保护方法，对用户要求过高，使用过程较为复杂，不能适应用户的要求。

发明内容

本发明的目的在于提供一种数据安全存储系统和装置及方法，其对用户操作要求低，使用过程简单，适应用户的要求。

为实现本发明目的而提供的一种数据安全存储系统，包括操作平台，存储设备，还包括可信计算单元，加解密单元，其中：

所述可信计算单元，用于保护对操作平台和存储设备间读写的数据进行加解密的密钥；

所述加解密单元，用于从可信计算单元读取密钥，利用相应的设定的加解密算法，对操作平台与存储设备之间读写的数据进行加解密。

所述的数据安全存储系统，还可以包括控制单元，用于对可信计算单元和加解密单元进行初始化，并控制加解密单元利用密钥加解密在操作平台和存储设备间读写的数据。

所述可信计算单元的保护，为通过唯一性标识匹配判断并控制操作平台对存储设备的数据安全存储读写。

所述密钥存储于可信计算单元。

所述可信计算单元还存储用于匹配判断的操作平台的第一唯一性标识。

所述控制单元可以包括密钥判断子单元，读写控制子单元，其中：

密钥判断子单元，用于判断可信计算单元中是否有密钥，是否需要对操作平台与存储设备间的读写数据进行加解密，并根据判断结果读取操作平台的第二唯一性标识；

读写控制子单元，用于在操作平台读取存储设备中的数据时，控制加解密单元对操作平台和存储设备之间的读写数据进行加解密。

所述控制单元还可以包括初始化子单元，用于操作平台硬件加电，对初始化软件进行初始化时，加载可信计算环境，并初始化可信计算环境。

所述加解密单元可以包括读取数据解密子单元和写入数据加密子单元，其中：

读取数据解密子单元，用于在操作平台向存储设备读取数据时，将该数据截获并解析，得到原始的加密数据，将该数据解密，得到未加密数据，然后按原传输格式将未加密数据打包，传输给操作平台；

写入数据加密子单元，用于在操作平台对存储设备写入数据时，将该数据截获并解析，得到原始的未加密数据，将该数据加密，得到加密数据，然后按原传输格式将加密数据打包，写入到存储设备中去。

所述可信计算单元可以包括匹配控制子单元，用于读取第一唯一性标识，并将该第一唯一性标识与密钥判断子单元读取的第二唯一性标识匹配检查。

所述可信计算单元还可以包括密钥存储子单元，用于存储加解密密钥和第一唯一性标识。

所述可信计算单元还可以更进一步包括密钥生成子单元，用于根据操作平台第一唯一性标识，生成相应的加解密密钥。

所述操作平台的计算机系统平台，或者单片机系统平台，或者手机、PDA、U 盘、MP3、MP4 和操作所述手机、PDA、U 盘、MP3、MP4 的网络共同组成的主从架构的网络平台。

所述存储设备是 RAM，或者硬盘，或者闪存中的一种或者一种以上的组

合。

所述唯一性标识，对计算机系统而言，包括：

计算机主板的系列号；或者

中央处理器序列号；或者

设备序列号；或者

操作系统序列号；或者

应用软件序列号中的一种或者一种以上的组合。

所述唯一性标识，对通信网络系统而言，包括：

手机的 SIM 卡号；或者

手机的国际移动电话识别码中的一种或者两者组合。

所述唯一性标识为对操作平台中表示软件平台、硬件平台的特征数据进行哈希运算，所得计算结果的完整性度量值。

所述密钥生成子单元可以是通过哈希函数生成加解密密钥。

所述加解密算法为 DES 算法，或者 IDEA 算法，或者 AES 算法，或者 RSA 算法，或者 Diffie-Hellman 算法，ECC 算法中的一种或者一种以上的组合。

为实现本发明目的还提供一种数据安全存储装置，与操作平台和存储设备电连接，包括可信计算单元，加解密单元，其中：

所述可信计算单元，用于保护对操作平台和存储设备间读写的数据进行加解密的密钥；

所述加解密单元，用于从可信计算单元读取密钥，利用相应的设定的加解密算法，对操作平台与存储设备之间读写的数据进行加解密。

所述的数据安全存储系统，还可以包括控制单元，用于对可信计算单元和加解密单元进行初始化，并控制加解密单元利用密钥加解密在操作平台和存储设备间读写的数据。

所述可信计算单元的保护，为通过唯一性标识匹配判断并控制操作平台对存储设备的数据安全存储读写。

所述密钥存储于可信计算单元。

所述可信计算单元还存储用于匹配判断的操作平台的第一唯一性标识。

所述控制单元可以包括密钥判断子单元，读写控制子单元，其中：

密钥判断子单元，用于判断可信计算单元中是否有密钥，是否需要对操作

平台与存储设备间的读写数据进行加解密，并根据判断结果读取操作平台的第二唯一性标识；

读写控制子单元，用于在操作平台读取存储设备中的数据时，控制加解密单元对操作平台和存储设备之间的读写数据进行加解密。

所述控制单元还可以包括初始化子单元，用于操作平台硬件加电，对初始化软件进行初始化时，加载可信计算环境，并初始化可信计算环境。

所述加解密单元可以包括读取数据解密子单元和写入数据加密子单元，其中：

读取数据解密子单元，用于在操作平台向存储设备读取数据时，将该数据截获并解析，得到原始的加密数据，将该数据解密，得到未加密数据，然后按原传输格式将未加密数据打包，传输给操作平台；

写入数据加密子单元，用于在操作平台对存储设备写入数据时，将该数据截获并解析，得到原始的未加密数据，将该数据加密，得到加密数据，然后按原传输格式将加密数据打包，写入到存储设备中去。

所述可信计算单元可以包括匹配控制子单元，用于读取第一唯一性标识，并将该第一唯一性标识与密钥判断子单元读取的第二唯一性标识匹配检查。

所述可信计算单元还可以包括密钥存储子单元，用于存储加解密密钥和唯一性标识。

所述可信计算单元还可以进一步包括密钥生成子单元，用于根据操作平台唯一性标识，生成相应的加解密密钥。

所述数据安全存储装置，或者是一种独立于操作平台和存储设备的硬件设备，或者是存储设备控制装置的一部分，或者是操作平台中的硬件平台的一部分，或者是 BIOS 芯片加载的一段软件，或者是 EFI 芯片加载的一段软件。

为实现本发明目的还提供一种数据安全存储方法，包括下列步骤：

步骤 A，在需要处理存储设备中的数据时，对操作平台上电并初始化，并初始化可信计算环境，通过唯一性标识匹配判断并控制操作平台对存储设备的数据安全存储读写；

步骤 B，在确认需要对存储设备进行数据安全存储读写后，读取密钥，利用相应的设定的加解密算法，对操作平台与存储设备之间读写的数据进行加解密。

所述步骤 A 中，通过唯一性标识匹配判断并控制操作平台对存储设备的数据安全存储读写，具体包括下列步骤：

步骤 A1，判断可信计算环境中是否有密钥，如果没有则转步骤 A2；否则转步骤 A4；

步骤 A2，判断该操作平台与存储设备间读写数据是否需要进行加解密；如果否，则正常启动，不对操作平台与存储设备之间读写的数据进行任何处理，用户正常使用后结束；否则转步骤 A3；

步骤 A3，生成相应的加解密密钥，转到步骤 B；

步骤 A4，如果可信计算单元中已经有密钥存在，则读取第一唯一性标识，将该第一唯一性标识与从本操作平台上读取的第二唯一性标识进行匹配检查；

步骤 A5，如果匹配通过，则检查通过，得到密钥，转到步骤 B；否则，给出信息后，结束返回。

所述步骤 A4 还包括下列步骤：

在读取第一唯一性标识时指定要求用户核对口令，如果用户输入口令与该第一唯一性标识的口令不同，则不允许用户得到该第一唯一性标识。

所述步骤 B 中对操作平台与存储设备之间读写的数据进行加解密，具体包括下列步骤：

步骤 B1，在操作平台读取存储设备中的数据时，将该数据截获并解析，得到原始的加密数据，将该数据解密，得到未加密数据，然后按原传输格式将未加密数据打包，传输给操作平台；

步骤 B2，在操作平台对存储设备写入数据时，将该数据截获并解析，得到原始的未加密数据，将该数据加密，得到加密数据，然后按原传输格式将加密数据打包，写入到存储设备中去。

所述唯一性标识，对计算机系统而言，包括：

计算机主板的系列号；或者

中央处理器序列号；或者

设备序列号；或者

操作系统序列号；或者

应用软件序列号中的一种或者一种以上的组合。

所述唯一性标识，对通信网络系统而言，包括：

手机的 SIM 卡号；或者

手机的国际移动电话识别码中的一种或者两者组合。

所述唯一性标识为对操作平台中表示软件平台、硬件平台的特征数据进行哈希运算，所得计算结果的完整性度量值。

所述密钥生成可以为根据唯一性标识由哈希函数生成加解密密钥。

所述加解密算法为 DES 算法，或者 IDEA 算法，或者 AES 算法，或者 RSA 算法，或者 Diffie-Hellman 算法，ECC 算法中的一种或者一种以上的组合。

本发明的有益效果是：本发明的数据安全存储系统和装置及方法，对操作平台（如计算机系统，或者移动通信数据传输系统等）在存储设备中读写的数据进行加密和解密，并且加密和解密密钥由系统中的具有平台绑定特性的可信计算单元保护和管理，使得对于平台的操作系统和应用软件而言，数据的读写过程是透明的，而且是安全的；进一步地，构造和管理密钥是由可信计算单元保证的，即具有硬件级别的安全性，该可信计算单元与操作平台绑定，不访问该操作平台就无法对所加密数据进行解密，从而更加保证其安全性，即如果这一存储设备重新装入其他的操作平台中，存储在该存储设备中的数据将不能被解密读写，这对于便携设备用户、军方用户或者有敏感数据需要保护的用户来说具有重要意义。

附图说明

图 1 为本发明数据安全存储系统结构示意图；

图 2 为图 1 中可信计算单元结构示意图；

图 3 为图 1 中加解密单元结构示意图；

图 4 为图 1 中控制单元结构示意图；

图 5 为本发明数据安全存储方法流程图；

图 6 为图 5 中判断控制读写数据过程方法流程图；

图 7 为本发明透明的数据安全存储系统示例图。

具体实施方式

为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明的一种数据安全存储系统和装置及方法进行进一步详细说明。

应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

如图 1 所示，本发明的数据安全存储系统，包括操作平台 11，存储设备 13，可信计算单元 121，加解密单元 122 和控制单元 123。

操作平台 11，用于对操作数据进行处理，其既可以是计算机系统平台，也可以是其他的主从架构的类似计算机系统平台的系统平台，如单片机系统平台；一种移动通讯设备，如手机、PDA、U 盘、MP3、MP4 和操作其通讯读写数据的网络，如手机的移动通信网络等组成的主从架构的网络平台。

该操作平台 11 包括硬件平台 72 和软件平台 71。对计算机系统平台而言，该操作平台 11 既包括对操作数据进行处理的所必需具备的硬件平台 72，即中央处理器（CPU），控制总线，输入输出设备，以及其他的外围设备等；也包括在硬件平台 72 上运行的软件平台 71，即初始化系统软件（BIOS 软件、EFI 软件等），操作系统 712（Windows 操作系统、Unix 操作系统、Linux 操作系统等），设备驱动程序 713，应用软件 711（如办公自动化软件等），以及其他的软件（如查杀毒软件等）。

对通信网络平台而言，该操作平台 11 既包括硬件平台 72，即手机，以及通信网络中的其他硬件，如路由器，服务器实体设备等；也包括软件平台 71，即服务器控制软件，路由器控制软件，手机控制软件等。

存储设备 13 用于存储加密数据，其可以是随机读写存储器（RAM）、硬盘、闪存（Flash）等存储设备 13 中的一种或者一种以上的组合。当然，本领域的普通技术人员可以理解，在一般的理解中，本发明所述的存储设备 13 也可以是操作平台 11 中硬件平台 72 的一部分。

本领域的普通技术人员也可以理解，在本发明这样的系统结构下，该存储设备 13 还包括一个设备驱动器和一个驱动控制器，用于读写存储设备 13 中的在存储扇区中的数据。

可信计算单元 121，用于保护对操作平台 11 和存储设备 13 间读写的数据进行加解密的密钥。其通过唯一性标识匹配判断并控制操作平台对存储设备的数据安全存储读写，从而保护对操作平台 11 和存储设备 13 间读写的数据进行加解密的密钥。该密钥和唯一性标识可以保存在可信计算单元中，也可以保存在用户预设的其他存储单元中。

该操作平台 11 的唯一性标识，可以包括以下唯一性标识该操作平台 11 的硬件平台 72 唯一性标识和软件平台 71 唯一性标识。

对计算机系统而言，包括：

1） 计算机主板的系列号；或者

2） 中央处理器（CPU）序列号；或者

3） 设备（如网卡）序列号；或者

4） 操作系统 712 序列号；或者

5） 应用软件 711 序列号等。

对通信网络系统而言，包括：

1） 手机的 SIM 卡号；或者

2） 手机的国际移动电话识别码(International Mobile Equipment Identity，IMEI)等。

这些能够唯一标识操作平台 11 的硬件平台 72 和软件平台 71 唯一性标识，一般由生产商在出厂时为标识该产品的唯一性而随机生成，具有唯一性。例如，主板系列号能够标识整台计算机的来源；手机 SIM 卡号可以标识该用户等。并且，这些唯一性标识都可以被读取。因此，在本发明中，通过读取这些唯一性标识中的一个或者多个，然后利用唯一性标识进行匹配检查，从而使得利用密钥的加解密操作与操作平台 11 绑定。

该唯一性标识也可以是一个完整性度量值，该完整性度量值是对操作平台 11 中软件平台 71、硬件平台 72 的特征数据进行 HASH 运算（也就是杂凑运算）所得计算结果。该结果为操作平台 11 的完整性度量值。这些完整性度量值被视为操作平台的唯一性标识，标识操作平台 11 的配置信息或者平台特征。

作为一种可实施方式，该对操作平台 11 和存储设备 13 间读定的数据进行加解密的密钥，由操作平台的唯一性标识生成。

可信计算单元 121 从指定操作平台 11（一般为与可信计算单元 121 电连接的操作平台）读取该操作平台 11 的唯一性标识，利用唯一性标识通过密钥生成方法（或称算法、函数）与加解密算法相对应的密钥。

利用唯一性标识，通过密钥生成方法，生成与加解密算法相对应的密钥。

在本发明实施例中，作为一种可实施的方法，利用唯一性标识，通过哈希

（HASH）函数生成密钥。

哈希函数，也叫散列函数或者杂凑函数，就是把任意长度的输入（又叫做预映射， pre-image），通过散列算法，变换成固定长度的输出，该输出就是散列值。简单的说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。利用一个或者多个唯一性标识，通过哈希函数，生成唯一的散列值。

即利用哈希函数计算标识的密钥：HASH（标识）＝mac；其中 mac 是用哈希函数 HASH 计算的唯一的散列值。

较佳地，利用该唯一的散列值，根据不同的加解密算法，由该加解密算法的密钥生成中心，再生成相应的唯一的加解密密钥。

对于一般的加解密算法，如对称加解密算法，由于其密钥唯一性，因此可以再次利用哈希函数，再次生成唯一的散列值，作为加解密密钥。

但对于非对称加密算法，由于其密钥为密钥对，即公钥和私钥。因此，只能由该非对称加密算法相应的密钥中心，利用该唯一的散列值，生成公钥和私钥，得到密钥对。

作为本发明的较佳实施例，该加解密算法为对称加解密算法，这样，密钥生成过程可以由哈希函数一次生成，也可以两次生成。而对称加解密算法较为安全，加解密速度很快，使得存储设备 13 的读写运行效率不会受到损失。

在本发明实施例中，需要特别说明的是，该对操作平台 11 和存储设备 13 间读定的数据进行加解密的密钥，并不一定由操作平台的唯一性标识生成。其也可以用其他方法而生成，例如利用随机数生成，然后存储到可信计算单元中。

加解密单元 122，用于从可信计算单元 121 读取密钥，利用相应的设定的加解密算法，对操作平台 11 与存储设备 13 之间读写的数据进行加解密。

也就是说，利用从可信计算单元 121 读取的密钥，加密操作平台 11 写入到该存储设备 13 的数据，同时，对操作平台 11 从存储设备 13 读取的数据，进行解密后发送给操作平台 11 处理。

在加解密单元 122 中设定的加解密算法，可以是各种与密钥相应的现有的加解密算法，可以是对称加解密算法或者非对称加解密算法中的一种或者多种。

对称加解密算法，包括出自 IBM 公司而被美国政府正式采纳的数据加密算法（Data Encryption Standard，DES）算法、由中国学者 Xuejia Lai 和 James

L. Massey 在苏黎世的 ETH 开发的国际数据加密算法 IDEA（International Data Encryption Algorithm）算法、比利时 Joan Daemen 和 Vincent Rijmen 提交，被美国国家标准和技术研究所（US National Institute of Standards and Technology，NIST）选为美国高级加密标准的 AES（Advanced Encryption Standard）算法等。

其中，DES 是 Data Encryption Standard（数据加密标准）的缩写。它是由 IBM 公司研制的一种加密算法，美国国家标准局于 1977 年公布把它作为非机要部门使用的数据加密标准，二十年来，它一直活跃在国际保密通信的舞台上，扮演了十分重要的角色。

DES 是一个分组加密算法，他以 64 位为分组对数据加密。同时 DES 也是一个对称算法：加密和解密用的是同一个算法。它的密匙长度是 56 位（因为每个第 8 位都用作奇偶校验）。

非对称加解密算法，包括有 RSA（Rivest,Shamir 和 Adlernan）算法、Diffie-Hellman 算法、ECC（Elliptic Curves Cryptography,椭圆曲线密码编码学）算法等。

在本实施例中，以支持 IDE/SATA 控制器 712 的存储设备 13 为例，将加解密单元 122 连接在 IDE/SATA 控制器 712 上，这样就可以支持不同种类的支持 IDE/SATA 控制器 712 接口的硬盘，对于这些不同的存储设备 13 不需要因为本发明而对存储设备 13 做任何改变就能实现数据的加解密。

控制单元 123，用于对可信计算单元 121 和加解密单元 122 进行初始化，并控制加解密单元利用密钥加解密在操作平台和存储设备间读写的数据。

当操作平台 11 需要使用可信计算单元 121 确保读写到存储设备 13 中的数据安全时，操作平台 11 首先需要对处理数据的硬件加电，对初始化软件如 BIOS 软件或者 EFI 软件进行初始化，这时，在 BIOS 软件或者 EFI 软件中，加载可信计算单元 121，初始化可信计算环境，设定从操作平台 11 读写到存储设备 13（如硬盘）中的数据是否利用可信计算单元 121 中的密钥，通过加解密单元 122 加/解密。

本领域的普通技术人员也可以理解，可信计算单元 121 中可以产生和存储多个不同的密钥，读写存储设备 13 中的不同的区域，例如：密钥 A 读写硬盘中的 C 盘且对其它区域不可见，密钥 B 读写 D 盘且对其他区域不可见，依此

类推；而对可信计算单元 121 中的密钥，也可以根据不同的级别进行管理，如一般操作人员不能读写修改密钥，而超级管理员可以读取密钥并修改原来的密钥，例如，原密钥只是由主板唯一性标识生成，现在需要增加一个应用软件 711 唯一性标识生成的密钥，则超级管理员读取密钥，并利用新的唯一性标识（主板标识+应用软件标识），生成新的密钥，然后利用原密钥读取存储设备 13 中的写入数据，解密后利用新的密钥加密再写入存储设备 13，最后，把新的密钥覆盖删除原密钥。

本发明的数据安全存储系统中的控制单元，可以是独立的控制模块芯片，也可以是合成到可信计算单元中的一个控制功能电路单元。

本发明的数据安全存储系统，对操作平台 11（如计算机系统，或者移动通信数据传输系统等）在存储设备 13 中读写的数据进行加密和解密，并且加密和解密密钥由具有平台绑定特性的可信计算单元 121 保护和管理，使得对于平台的操作系统 712 和应用软件 711 而言，数据的读写过程是透明的，而且是安全的。

相应地，本发明还提供一种数据安全存储装置 12，与操作平台 11 和存储设备 13 电连接，其包括可信计算单元 121，加解密单元 122 和控制单元 123。其中：

可信计算单元 121，用于保护与指定操作平台 11 绑定的对操作平台 11 和存储设备 13 间读写的数据进行加解密的密钥。其通过唯一性标识匹配判断并控制操作平台对存储设备的数据安全存储读写，从而保护对操作平台 11 和存储设备 13 间读写的数据进行加解密的密钥。该密钥和唯一性标识可以保存在可信计算单元中，也可以保存在用户预设的其他存储单元中。。

如图 2 所示，可信计算单元 121，包括密钥生成子单元 1211，密钥存储子单元 1212，匹配控制子单元 1213，其中：

匹配控制子单元 1213，用于读取原来存储的唯一性标识，并将该唯一性标识与初始化时读取的操作平台的唯一性标识匹配检查。

作为一种可实施的方法，匹配控制子单元 1213 在利用加解密密钥进行存储设备密钥保护，开始释放加解密密钥进行数据加解密时，可信计算单元 121 利用本次运算生成的完整性度量值与平台配置寄存器中保存的完整性度量值进行匹配检查。只有在完整性度量值匹配的情况下，才释放密钥，否则，拒绝

释放密钥。

作为另一种可实施的方法，匹配控制子单元 1213 在确认可信计算单元 121 中已经有密钥存在，则从可信计算单元 121 中读取唯一性标识，并将唯一性标识与从本操作平台 11 上读取的相应唯一性标识进行匹配检查，如果匹配通过，则检查通过，利用该密钥对读写数据进行加/解密；否则，给出信息（如“抱歉，你无权读取硬盘！”）后，结束返回。

更进一步，作为另外一种可实施的方法，如果密钥由唯一性标识生成，则在可信计算单元中只保存密钥，匹配控制子单元 1213 在确认可信计算单元 121 中已经有密钥存在，则从可信计算单元 121 中读取该密钥，然后控制可信计算单元 121 将该密钥解密，还原得到操作平台 11 的唯一性标识，并由匹配控制子单元 1213 将解密出来的唯一性标识与从本操作平台 11 上读取的相应唯一性标识进行匹配检查，如果匹配通过，则检查通过，利用该密钥对读写数据进行加/解密；否则，给出信息后结束返回。

从密钥中通过利用与生成密钥相反的过程，即逆过程，即可以得到相应的生成该密钥的一个或者多个唯一性标识，如上述哈希函数生成的密钥，利用哈希函数的逆过程和该密钥，就能得到原唯一性标识。

对具有多个唯一性标识的密钥，因为计算机系统平台启动过程有先后顺序，因此，可以先后多次核对多个序列号，每核对正确一部分序列号后，可以对某一部分数据进行读写，这样，既能保证操作平台 11 能够启动，也能够保证数据的安全。

当这些过程完成后，用户可以如同使用普通的操作平台 11 一样使用本发明的数据安全存储系统，可以安装操作系统 712、应用软件 711 等等。

密钥生成子单元 1211，用于生成相应的加解密密钥。

作为一种可实施的方式，控制单元 123 从操作平台 11 中读取相应的一个或者多个操作平台 11 唯一性标识，由可信计算单元 121 根据所述的一个或者多个操作平台 11 唯一性标识生成密钥，例如，如果用户欲将对硬盘的读写限制在本台计算机上，则读取主板序列号生成密钥，利用加解密单元 122 中的加解密算法加/解密该计算机对该存储设备 13 的数据读写；如果用户不但将对硬盘的读写限制在本台计算机上，而且限制在 Windows XP 操作系统和应用软件 711（例如本公司的办公软件上），则读取主机主板系列号，Windows XP 操作

系统序列号，应用软件 711 序列号，由可信计算单元 121 生成密钥并保存，然后加解密单元 122 从可信计算单元 121 中读取密钥，利用相应的加解密算法加/解密该计算机在 Windows XP 操作系统上的应用软件 711，对该存储设备 13 的数据读写。

密钥存储子单元 1212，用于存储加解密密钥和唯一性标识。

作为本发明的一个可实施方式，密钥存储子单元是在可信计算单元 121 内部设置的一组平台配置寄存器，其存储操作平台 11 的唯一性标识和密钥。

作为本发明的另一个可实施方式，如果密钥由唯一性标识生成，则也可以不存储该唯一性标识，而通过生成密钥的逆过程，从密钥得到该唯一性标识。

从密钥中通过利用与生成密钥相反的过程，即逆过程，即可以得到相应的生成该密钥的一个或者多个唯一性标识，如上述哈希函数生成的密钥，利用哈希函数的逆过程和该密钥，就能得到原唯一性标识。

加解密单元 122，用于从可信计算单元 121 读取密钥，利用相应的设定的加解密算法，对操作平台 11 与存储设备 13 之间读写的数据进行加解密。

如图 3 所示，所述加解密单元 122，包括读取数据解密子单元 1221 和写入数据加密子单元 1222，其中：

读取数据解密子单元 1221，用于在操作平台 11 向存储设备 13 读取数据时，将该数据截获并解析，得到原始的加密数据，将该数据解密，得到未加密数据，然后按原传输格式将未加密数据打包，传输给操作平台 11。

写入数据加密子单元 1222，用于在操作平台 11 对存储设备 13 写入数据时，将该数据截获并解析，得到原始的未加密数据，将该数据加密，得到加密数据，然后按原传输格式将加密数据打包，写入到存储设备 13 中去。

控制单元 123，用于对可信计算单元 121 进行初始化，并控制加解密单元利用密钥加解密在操作平台和存储设备间读写的数据。

如图 4 所示，所述控制单元 123，包括初始化子单元 1231，密钥判断子单元 1232，读写控制子单元 1233，其中：

初始化子单元 1231，用于操作平台 11 硬件加电，对初始化软件进行初始化时，加载可信计算环境，并初始化可信计算环境，设定从操作平台 11 读写到存储设备 13 中的数据利用密钥通过加解密单元 122 加解密。

由于本发明中的加解密单元 122 和可信计算单元 121，这两个单元都是被

动设备，因此要使系统能够正确的实施，还必须有控制单元 123 来支持运行，控制单元 123 可以被引导运行，能完成可信计算单元 121 的初始化工作并协调可信计算单元 121 和加解密单元 122。具体而言，由于在有操作系统 712 的环境下实现这样的控制不能实现对操作系统 712 本身处理数据的保护，因此，该控制单元 123 可以运行在无操作系统 712 的环境下。以个人计算机为例，现有计算在启动时，需要先于操作系统 712 运行 BIOS 或者 EFI，这时，加载可信计算单元 121，初始化可信计算环境，即将可信计算环境加载到 BIOS 或者 EFI 环境中，初始化可信计算环境的参数，可载程序代码等。

密钥判断子单元 1232，用于判断可信计算单元 121 中是否有密钥，是否需要对操作平台 11 与存储设备 13 间的读写数据进行加解密，并根据判断结果读取操作平台 11 的唯一性标识。

密钥判断子单元 1232 判断可信计算单元 121 中是否有密钥，如果没有密钥，则判断该操作平台 11 与存储设备 13 间读写数据是否需要进行加/解密，如果否，则正常启动，不对操作平台 11 与存储设备 13 之间读写的数据进行任何处理，用户正常使用后结束；否则，可信计算单元 121 中的密钥生成子单元生成相应的加解密密钥。

读写控制子单元 1233，用于在操作平台 11 读取存储设备 13 中的数据时，控制加解密单元 122 对操作平台 11 和存储设备 13 之间的读写数据进行加解密。

在操作平台 11 向存储设备 13 读取数据时，读写控制子单元 1233 控制加解密单元 122 将该数据截获并解析，得到原始的加密数据，将该数据解密，得到未加密数据，然后按原传输格式将未加密数据打包，传输给操作平台 11；

在操作平台 11 对存储设备 13 写入数据时，读写控制子单元 1233 控制加解密单元 122 将该数据截获并解析，得到原始的未加密数据，将该数据加密，得到加密数据，然后按原传输格式将加密数据打包，写入到存储设备 13 中去。

这样，在操作平台 11 和存储设备 13 的两端，都只要以与原来相当的方便存储数据，即操作平台 11 与存储设备 13 之间读写数据是透明的，用户既不用关心数据如何加密和解密，也不用担心数据的安全性。

这里需要说明的是，将数据截获并解析，以及将数据按原格式打包，都是本领域的公知常识，因此，在本发明实施例中不再一一详细描述。

较佳地，对操作平台 11 与存储设备 13 读写数据时，对传输中的控制信令，加解密单元 122 不作任何处理，而只对读写数据本身进行加解密。

该数据安全存储装置 12，或者是一种独立于操作平台 11 和存储设备 13 的硬件设备，或者是存储设备 13 控制装置的一部分，或者是操作平台 11 中的硬件平台 72 的一部分，例如连接到计算机主板控制总线上的芯片，或者是连接在操作平台 11 与存储设备 13 间的芯片，或者是 BIOS 芯片加载的一段软件，或者是 EFI 芯片加载的一段软件。

就本发明而言，对于不同种类的存储设备 13，只需要将该安全存储装置连接在不同的总线控制设备上就能实现数据加密和解密。因此，本发明对于操作平台 11 和存储设备 13 而言是透明的，也就是说实现此数据安全存储的操作平台 11 和存储设备 13 不需要进行任何改变。

这里说的一种透明的技术包括两种涵义，其一是指这种技术对于操作平台 11 上运行的操作系统 712 或者应用软件 711 而言是透明的，操作系统 712 和应用软件 711 并不知道数据的加密/解密过程，因此操作系统 712 或者应用软件也不用对加/解密过程做出任何额外的修改。其二是指这种技术对于不同的存储设备 13 而言是透明的，对于不同的存储介质或者设备，其操作的基本原理并不发生变化，只需要在写入数据前加入加解密单元 122 对数据进行加解密，而现有的存储设备 13 本身不需要进行额外改变。

本发明的数据安全存储系统和装置，密钥创建和管理根据操作平台 11 而设计，使得密钥的存储和使用方式的安全性都得到显著提升。

如图 5 所示，下面进一步详细描述本发明的数据安全存储方法，其包括下列步骤：

步骤 S100，在需要处理存储设备 13 中的数据时，对操作平台 11 上电并初始化，并初始化可信计算环境，通过唯一性标识匹配判断并控制操作平台 11 对存储设备 13 的数据安全存储读写；

当操作平台 11 需要处理存储设备 13 中数据时，它首先上电并进行初始化，首先对可信计算环境进行初始化，然后再对整个操作平台 11 进行初始化。可信计算环境初始化包括对可信计算单元 121 的初始化，以及判断确认是否需要加解密，是否有密钥进行加解密等。

步骤 S200，在确认需要对存储设备 13 进行数据安全存储读写后，读取密

钥，利用相应的设定的加解密算法，对操作平台 11 与存储设备 13 之间读写的数据进行加解密。

所述的加解密算法，包括但不限于对称加解密算法或者非对称加解密算法中的一种或者多种。

所述的对称加解密算法，包括 DES 算法，IDEA 算法，AES 算法等。

所述的非对称加解密算法，包括 RSA 算法、Diffie-Hellman 算法、ECC 算法等。

如图 6 所示，在步骤 S100 中，通过唯一性标识匹配判断并控制操作平台 11 对存储设备 13 的数据安全存储读写，具体包括下列步骤：

步骤 S110，判断可信计算环境中是否有密钥，如果没有则转步骤 S120；否则转步骤 S140；

步骤 S120，判断该操作平台 11 与存储设备 13 间读写数据是否需要进行加/解密；如果否，则正常启动，不对操作平台 11 与存储设备 13 之间读写的数据进行任何处理，用户正常使用后结束；否则转步骤 S130；

步骤 S130，生成相应的加解密密钥，转到步骤 S200；

作为一种可实施的方式，利用从操作平台 11 中读取相应的一个或者多个操作平台 11 唯一性标识，由可信计算单元 121 根据所述的一个或者多个操作平台 11 唯一性标识可以生成密钥。

步骤 S140，如果可信计算单元 121 中已经有密钥存在，则读取唯一性标识，将该唯一性标识与从本操作平台 11 上读取的相应唯一性标识进行匹配检查；

作为一种可实施的方法，匹配控制子单元 1233 在利用加解密密钥进行存储设备密钥保护，开始释放加解密密钥进行数据加解密时，可信计算单元 121 利用本次运算生成的完整性度量值与平台配置寄存器中保存的完整性度量值进行匹配检查。只有在完整性度量值匹配的情况下，才释放密钥，否则，拒绝释放密钥。

作为另一种实施方式，如果可信计算单元 121 中已经有密钥存在，而密钥由唯一性标识生成，则从密钥中通过利用与生成密钥相反的过程，即逆过程，即可以得到相应的生成该密钥的一个或者多个唯一性标识，将唯一性标识与从本操作平台 11 上读取的相应唯一性标识进行匹配检查。

更进一步，作为另外一种可实施的方法，在可信计算单元中只保存密钥，匹配控制子单元 1233 在确认可信计算单元 121 中已经有密钥存在，则从可信计算单元 121 中读取该密钥，然后控制可信计算单元 121 将该密钥解密，还原得到操作平台 11 的唯一性标识，并由匹配控制子单元 1233 将解密出来的唯一性标识与从本操作平台 11 上读取的相应唯一性标识进行匹配检查，如果匹配通过，则检查通过，利用该密钥对读写数据进行加/解密；否则，给出信息后结束返回。

更佳地，可以对可信计算环境中的唯一性标识进行保护，即可以指定使用该唯一性标识的口令。换句话说，用户在读取唯一性标识时可以指定使用该唯一性标识时用户的口令，如果用户输入口令与读取该唯一性标识的口令不同，则不允许用户得到该唯一性标识。

如果用户使用口令保护唯一性标识，那么在启动过程中，要求用户输入正确的口令，如果口令正确才能得到唯一性标识。

对具有多个唯一性标识，因为计算机系统平台启动过程有先后顺序，因此，可以先后多次核对多个序列号，每核对正确一部分序列号后，可以对某一部分数据进行读写，这样，既能保证操作平台 11 能够启动，也能够保证数据的安全。

步骤 S150，如果匹配通过，则检查通过，得到密钥，转到步骤 S200；否则，给出信息后，结束返回。

当这些过程完成后，用户可以如同使用普通的操作平台 11 一样使用本发明的数据安全存储系统，可以安装操作系统 712、应用软件 711 等等。

所述步骤 S200 中对操作平台 11 与存储设备 13 之间读写的数据进行加解密。具体包括下列步骤：

在操作平台 11 读取存储设备 13 中的数据时，将该数据截获并解析，得到原始的加密数据，将该数据解密，得到未加密数据，然后按原传输格式将未加密数据打包，传输给操作平台 11；

在操作平台 11 对存储设备 13 写入数据时，将该数据截获并解析，得到原始的未加密数据，将该数据加密，得到加密数据，然后按原传输格式将加密数据打包，写入到存储设备 13 中去。

如图 7 所示，为本发明透明的数据安全存储系统示例图，由于所有的对读

写的数据加/解密读写操作（包括软件控制与硬件处理）都不需要与操作系统712直接进行交互，因此，对操作系统712而言，它并不知道读写的数据被加解密保护；控制单元123运行在BIOS环境或者EFI环境下，在操作系统712装载之前就已经完成了对加解密单元122的密钥装载，并且在操作系统712向存储设备13读写数据时，加解密单元122会自动完成对数据的加解密处理。因此，对存储设备13而言，其也并不知道读写数据被加解密保护，其只是象未加密以前那样将加密数据存储到存储扇区中去，是透明的。

这样，在操作平台11和存储设备13的两端，都只要以与原来相当的方便存储数据，即操作平台11与存储设备13之间读写数据是透明的，用户既不用关心数据如何加密和解密，也不用担心数据的安全性。

换言之，本发明的数据安全存储方法，提供了一种透明的技术方法，用于加密和解密操作平台11与存储设备13之间读写的数据。这一加密/解密方法，通过采用可信计算单元121对与操作平台11绑定的加密/解密密钥，采用加解密单元122对数据进行加密/解密操作。

通过以上结合附图对本发明具体实施例的描述，本发明的其它方面及特征对本领域的技术人员而言是显而易见的，因而不再一一详细描述。

本发明的数据安全存储系统和装置及方法，对操作平台（如计算机系统，或者移动通信数据传输系统等）在存储设备中读写的数据进行加密和解密，并且加密和解密密钥由系统中的具有平台绑定特性的可信计算单元保护和管理，使得对于平台的操作系统和应用软件而言，数据的读写过程是透明的，而且是安全的；进一步地，构造和管理密钥是由可信计算单元保证的，即具有硬件级别的安全性，该可信计算单元与操作平台绑定，不访问该操作平台就无法对所加密数据进行解密，从而更加保证其安全性，即如果这一存储设备重新装入其他的操作平台中，存储在该存储设备中的数据将不能被解密读写，这对于便携设备用户、军方用户或者有敏感数据需要保护的用户来说具有重要意义。

以上对本发明的具体实施例进行了描述和说明，这些实施例应被认为其只是示例性的，并不用于对本发明进行限制，本发明应根据所附的权利要求进行解释。

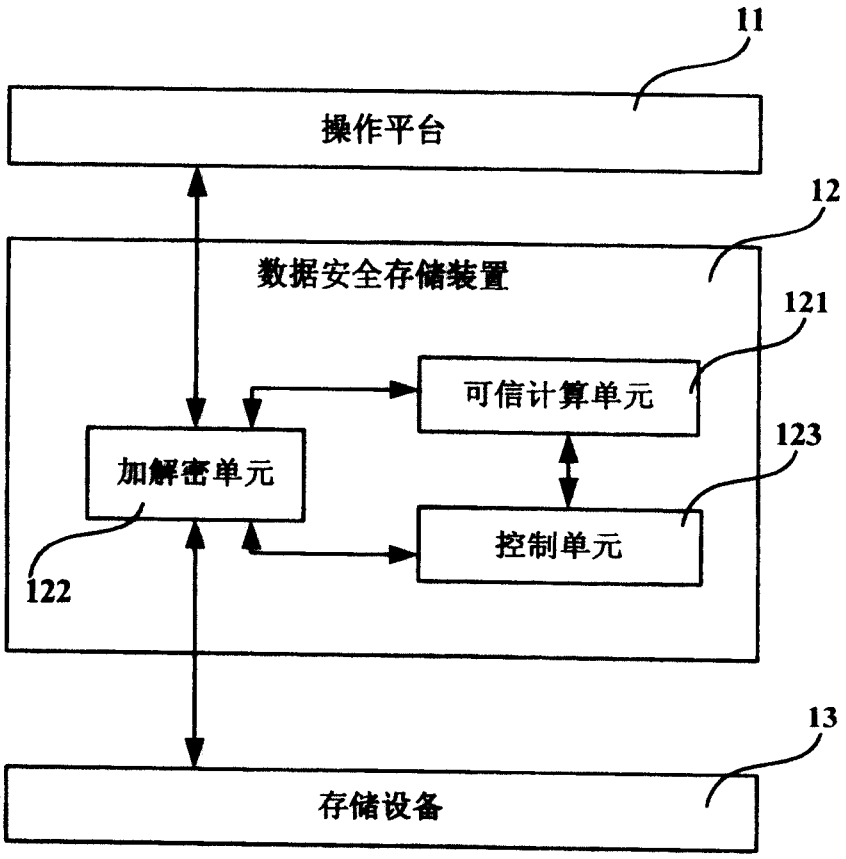


图 1

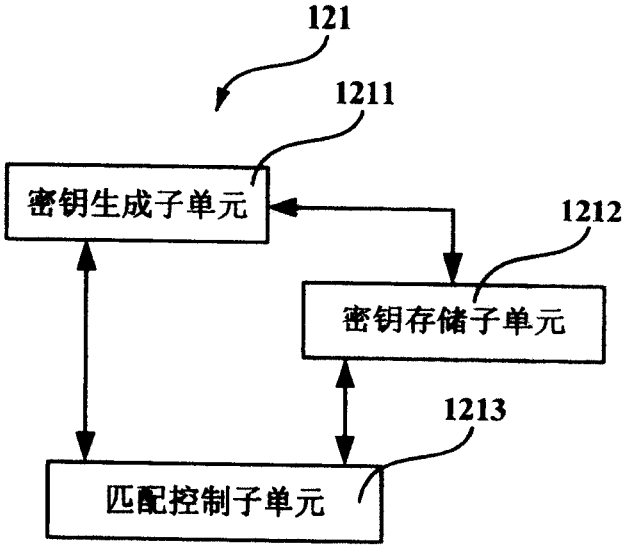

121
1211
密钥生成子单元
1212
密钥存储子单元
1213
匹配控制子单元

图 2

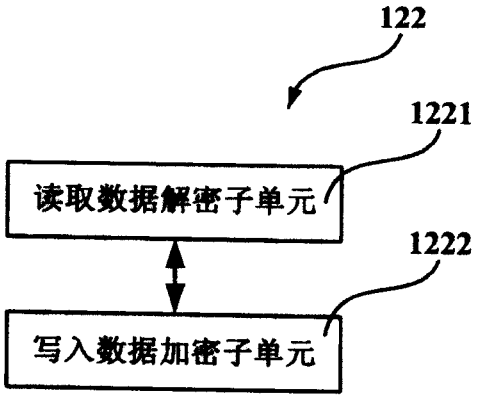

122
1221
读取数据解密子单元
1222
写入数据加密子单元

图 3

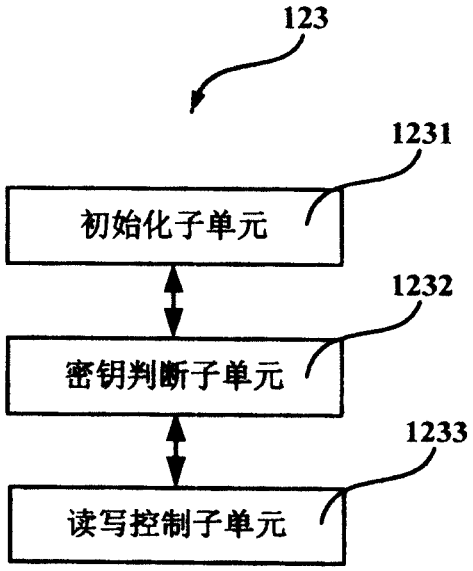


图 4

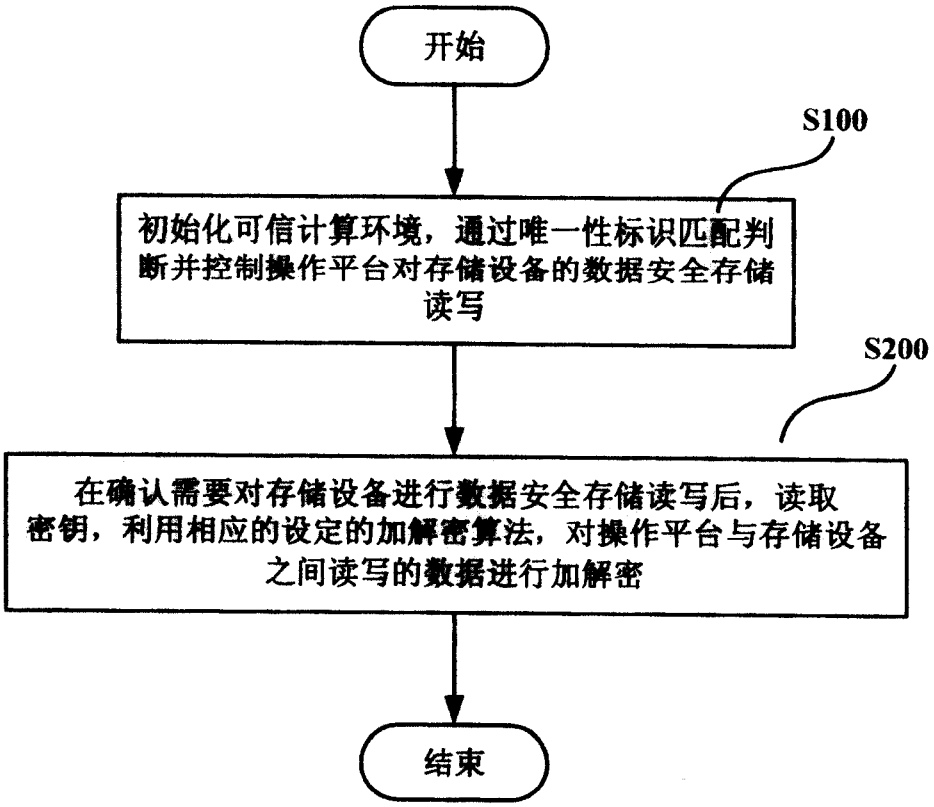

开始
S100
初始化可信计算环境，通过唯一性标识匹配判断并控制操作平台对存储设备的数据安全存储读写
S200
在确认需要对存储设备进行数据安全存储读写后，读取密钥，利用相应的设定的加解密算法，对操作平台与存储设备之间读写的数据进行加解密
结束

图 5

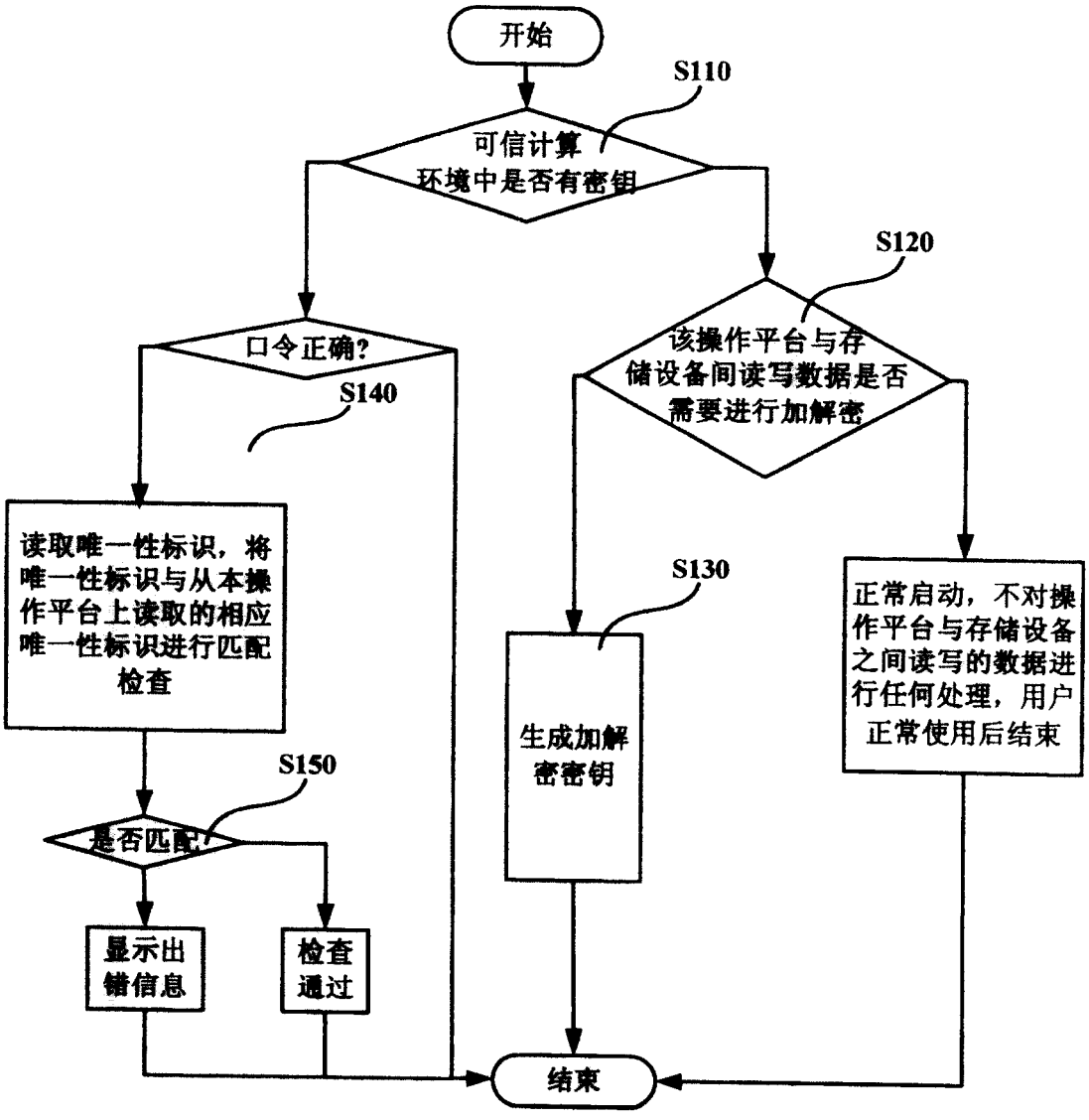

开始
S110
可信计算环境中是否有密钥
S120
该操作平台与存储设备间读写数据是否需要进行加解密
口令正确?
S140
读取唯一性标识，将唯一性标识与从本操作平台上读取的相应唯一性标识进行匹配检查
S130
生成加解密密钥
正常启动，不对操作平台与存储设备之间读写的数据进行任何处理，用户正常使用后结束
S150
是否匹配?
显示出错信息
检查通过
结束

图 6

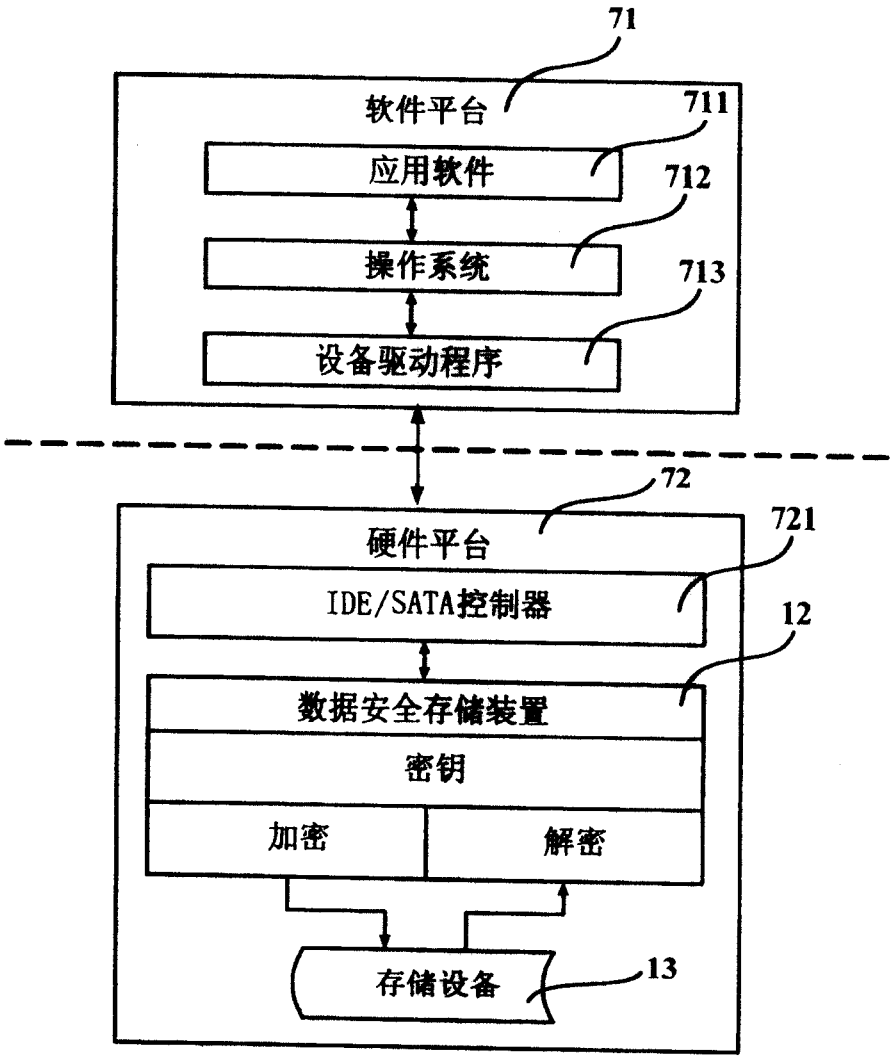

71
软件平台
711
应用软件
712
操作系统
713
设备驱动程序
72
硬件平台
721
IDE/SATA控制器
12
数据安全存储装置
密钥
加密
解密
存储设备
13

图 7