(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106980800 B
(45)授权公告日 2020.05.19

(21)申请号 201710195945.7

(22)申请日 2017.03.29

(65)同一申请的已公布的文献号
申请公布号 CN 106980800 A

(43)申请公布日 2017.07.25

(73)专利权人 山东超越数控电子股份有限公司
地址 250104 山东省济南市高新区孙村镇科航路2877号

(72)发明人 朱书杉 包汉彬 李岩 蒋海波

(74)专利代理机构 北京连和连知识产权代理有限公司 11278
代理人 杨帆

(51)Int.Cl.
G06F 21/80(2013.01)

(56)对比文件
CN 104598843 A,2015.05.06,
CN 104090853 A,2014.10.08,
CN 103559461 A,2014.02.05,
CN 101458743 A,2009.06.17,
CN 101504704 A,2009.08.12,

审查员 甄红欣

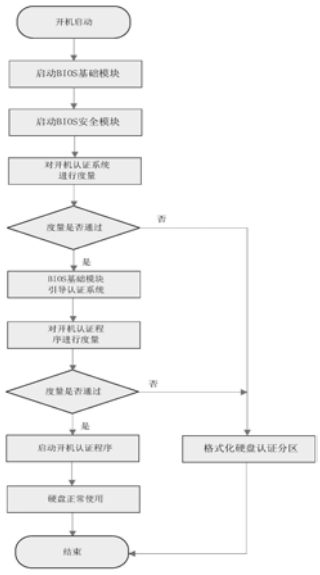
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种加密固态硬盘认证分区的度量方法和系统

(57)摘要

本发明提供一种加密固态硬盘认证分区的度量方法，包括以下步骤：读取认证系统并对认证系统进行度量，计算第一度量值，第一度量值与第一预期值进行比较；若比较的第一结果通过，引导认证系统；认证系统对认证程序进行度量，计算第二度量值，将第二度量值与第二预期值进行比较；若比较的第二结果通过，启动认证程序，进行登录认证；若登录认证通过，加密固态硬盘的用户分区可见。本发明提供的加密固态硬盘认证分区的度量方法具有以下优点：通过对认证系统和认证程序的度量，避免了加密固态硬盘的认证环节被绕过或被修改后直接访问用户分区的问题。



CN 106980800 B

1.一种加密固态硬盘认证分区的度量方法,其特征在于,包括以下步骤:

S00:读取所述加密固态硬盘中的认证系统并对所述认证系统进行度量,计算第一度量值,将所述第一度量值与第一预期值进行比较,所述第一度量值通过与硬盘固件协商的私有指令传输到所述硬盘固件;

S10:若S00中比较的第一结果通过,引导所述认证系统;

S20:所述认证系统对认证程序进行度量,计算第二度量值,将所述第二度量值与第二预期值进行比较;

S30:若S20中比较的第二结果通过,启动所述认证程序,进行登录认证;

S40:若所述登录认证通过,所述加密固态硬盘的用户分区可见。

2.根据权利要求1所述的加密固态硬盘认证分区的度量方法,其特征在于,

步骤S00中若比较的所述第一结果不通过,格式化所述加密固态硬盘认证分区;

步骤S20中若比较的所述第二结果不通过,格式化所述加密固态硬盘认证分区。

3.根据权利要求2所述的加密固态硬盘认证分区的度量方法,其特征在于,进一步包括以下步骤:重新对所述加密固态硬盘灌装认证系统和认证程序。

4.根据权利要求1所述的加密固态硬盘认证分区的度量方法,其特征在于,

步骤S00中通过哈希算法计算所述第一度量值;

和/或步骤S20中通过哈希算法计算所述第二度量值。

5.根据权利要求4所述的加密固态硬盘认证分区的度量方法,其特征在于,

所述哈希算法是MD5算法或SHA-1算法。

6.根据权利要求1所述的加密固态硬盘认证分区的度量方法,其特征在于,

S40中所述登录认证通过前,所述认证分区可见,所述用户分区不可见;

S40中所述登录认证通过后,所述认证分区不可见,所述用户分区可见。

7.一种使用如权利要求1-6中任一项所述的加密固态硬盘认证分区的度量方法的加密固态硬盘认证分区的度量系统,包括计算机,置于所述计算机内的加密固态硬盘和BIOS模块,其特征在于,

所述加密固态硬盘包括:

用户分区;

认证分区,存储有认证系统和认证程序,所述认证系统用于加载和度量所述认证程序;

硬盘固件,与所述认证分区通信,用于比较第一度量值与第一预期值、第二度量值与第二预期值;

主控芯片,内置安全区域以用于存储所述第一预期值和/或所述第二预期值;

所述BIOS模块包括:

BIOS基础模块,用于引导所述认证系统;

BIOS安全模块,与所述硬盘固件通信,用于读取和度量所述认证系统。

8.根据权利要求7所述的加密固态硬盘认证分区的度量系统,其特征在于,

所述BIOS安全模块用于度量所述认证系统,是先计算第一度量值,然后将所述第一度量值传输到所述硬盘固件,所述第一度量值通过与所述硬盘固件协商的私有指令传输到所述硬盘固件,基于所述硬盘固件返回的所述第一度量值与所述第一预期值比较的第一结果判断所述认证系统的度量结果。

9.根据权利要求7所述的加密固态硬盘认证分区的度量系统,其特征在于,

所述认证系统用于计算第二度量值,然后基于所述第二度量值与所述第二预期值比较的第二结果判断所述认证程序的度量结果。

一种加密固态硬盘认证分区的度量方法和系统

技术领域

[0001] 本发明涉及数据安全领域，具体涉及一种加密固态硬盘认证分区的度量方法和系统。

背景技术

[0002] 随着加密固态硬盘产品在数据安全存储领域应用日益广泛，对加密固态硬盘产品提出了越来越高的安全性要求，而目前加密固态硬盘产品在关键的用户身份认证环节容易被绕过和被修改，从而威胁存储在硬盘中数据的安全，针对此问题本发明提出一种加密固态硬盘认证分区的度量方法和系统。

发明内容

[0003] 针对上述现有技术中加密固态硬盘在用户身份认证环节容易被绕过或被修改的问题，本发明的目的在于提供一种加密固态硬盘认证分区的度量方法和系统。

[0004] 为了实现上述目的，本发明采用的技术方案如下：

[0005] 一种加密固态硬盘认证分区的度量方法，包括以下步骤：

[0006] S00：读取认证系统并对所述认证系统进行度量，计算第一度量值，将第一度量值与第一预期值进行比较；

[0007] S10：若S00中比较的第一结果通过，引导认证系统；

[0008] S20：认证系统对认证程序进行度量，计算第二度量值，将第二度量值与第二预期值进行比较；

[0009] S30：若S20中比较的第二结果通过，启动认证程序，进行登录认证；

[0010] S40：若登录认证通过，加密固态硬盘的用户分区可见。

[0011] 进一步地，步骤S00中若比较的第一结果不通过，格式化加密固态硬盘认证分区；步骤S20中若比较的第二结果不通过，格式化加密固态硬盘认证分区。

[0012] 进一步地，包括以下步骤：重新对加密固态硬盘灌装认证系统和认证程序。

[0013] 进一步地，步骤S00中通过哈希算法计算第一度量值；和/或步骤S20中通过哈希算法计算第二度量值。

[0014] 进一步地，哈希算法是MD5算法或SHA-1算法。

[0015] 进一步地，S40中登录认证通过前，认证分区可见，用户分区不可见；S40中登录认证通过后，认证分区不可见，用户分区可见。

[0016] 一种加密固态硬盘认证分区的度量系统，包括计算机，置于计算机内的加密固态硬盘和BIOS模块，

[0017] 加密固态硬盘包括：用户分区；认证分区，存储有认证系统和认证程序，认证系统用于加载和度量认证程序；硬盘固件，与认证分区通信，用于比较第一度量值与第一预期值、第二度量值与第二预期值；主控芯片，内置安全区域以用于存储第一预期值和/或第二预期值；

[0018] BIOS模块包括:BIOS基础模块,用于引导认证系统;BIOS安全模块,与硬盘固件通信,用于读取和度量认证系统。

[0019] 进一步地,BIOS安全模块用于度量认证系统,是先计算第一度量值,然后将第一度量值传输到硬盘固件,基于硬盘固件返回的第一度量值与第一预期值比较的第一结果判断认证系统的度量结果。

[0020] 进一步地,认证系统用于计算第二度量值,然后基于第二度量值与第二预期值比较的第二结果判断所述认证程序的度量结果。

[0021] 进一步地,第一度量值通过与硬盘固件协商的私有指令传输到硬盘固件。

[0022] 本发明通过以上技术方案,能够获得的有益技术效果是:

[0023] (1)通过对认证系统和认证程序的度量,避免了加密固态硬盘的认证环节被绕过或被修改后直接访问用户分区的问题;

[0024] (2)第一度量值通过与硬盘固件协商的私有指令传输,确保第一度量值不被篡改;

[0025] (3)当对认证系统和认证程序的度量不通过时,格式化认证分区,保证用户分区中信息的安全。

[0026] 当然,实施本发明的任一产品必不一定需要同时达到以上所述的所有技术效果。

附图说明

[0027] 此处所说明的附图用来提供对本发明的进一步理解,构成本发明的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

[0028] 图1为本发明实施例所述的加密固态硬盘认证分区的度量方法的流程图;

[0029] 图2为本发明实施例所述的加密固态硬盘认证分区的度量系统的结构框图。

具体实施方式

[0030] 如在说明书及权利要求当中使用了某些词汇来指称特定组件。本领域技术人员应可理解,硬件制造商可能会用不同名词来称呼同一个组件。本说明书及权利要求并不以名称的差异来作为区分组件的方式,而是以组件在功能上的差异来作为区分的准则。如在通篇说明书及权利要求当中所提及的“包括”为一开放式用语,故应解释成“包括但不限定于”。说明书后续描述为实施本发明的较佳实施方式,然所述描述乃以说明本发明的一般原则为目的,并非用以限定本发明的范围。本发明的保护范围当视所附权利要求所界定者为准。

[0031] 实施例1

[0032] 如图1所示,本实施例提供的一种加密固态硬盘认证分区的度量方法,包括以下步骤,首先,开机启动,计算机加电,BIOS安全模块启动,然后对加密固态硬盘中用于开机的认证系统进行度量。对认证系统的度量过程中,读取认证系统并计算第一度量值,将第一度量值与第一预期值进行比较,比较的结果记为第一结果,若比较的第一结果通过,BIOS基础模块读取并引导认证程序。然后认证系统对认证程序进行度量。对认证程序的度量过程中,计算第二度量值,将第二度量值与第二预期值进行比较,比较的结果记为第二结果,若比较的第二结果通过,启动用于开机的认证程序,进行登录认证,若登录认证通过,加密固态硬盘的用户分区可见,硬盘正常使用。通过对认证系统和认证程序的分别度量,以避免加密固态

硬盘的认证环节被绕过或被修改,防止用户分区被非法访问。

[0033] 其中,对认证系统的度量过程中,用哈希算法计算第一度量值;对认证程序的度量过程中,用哈希算法计算第二度量值;该哈希算法可以是MD5算法、SHA-1算法或其他算法。

[0034] 进一步地,若第一度量值与第一预期值进行比较的第一结果不通过,即数值不相符或不符合其他通过条件,或者第二度量值与第二预期值进行比较的第二结果不通过,即数值不相符或不符合其他通过条件,格式化加密固态硬盘的认证分区。此时需重新对加密固态硬盘灌装认证系统及认证程序方可继续使用。

[0035] 进一步地,若登录认证通过前,认证分区可见,用户分区不可见;若登录认证通过后,认证分区不可见,用户分区可见。即加密固态硬盘的硬盘固件通过登录认证的结果控制认证分区和用户分区是否可见。登录认证结果通过前,加密固态硬盘对外呈现为认证分区,认证结果通过后,对外呈现为用户分区,两个分区不会同时呈现。

[0036] 实施例2

[0037] 如图2所示,本实施例提供的一种加密固态硬盘认证分区的度量系统,包括计算机,计算机内设置有加密固态硬盘和BIOS模块。加密固态硬盘包括用于开机认证的认证分区、用户分区、硬盘固件、主控芯片、以及其他为实现硬盘功能的其他模块。认证分区中存储有认证系统和认证程序,认证系统用于加载和度量认证程序;硬盘固件,与认证分区通信,用于比较第一度量值与第一预期值、第二度量值与第二预期值;主控芯片,内置安全区域以用于存储第一预期值和第二预期值。

[0038] BIOS模块包括BIOS基础模块和BIOS安全模块,以及其他常用的为实现计算机基本功能的其他模块,如CPU、主板等。BIOS基础模块用于初始化内存、SATA接口等硬件、引导操作系统等通用功能以及引导认证系统的功能;BIOS安全模块,与硬盘固件通信,用于读取和度量加密固态硬盘中认证分区中的认证系统。BIOS安全模块内具有度量算法模块,并且BIOS安全模块与BIOS基础模块通信。

[0039] 其中,认证程序负责对用户的认证和对硬盘的管理等操作,用户只有通过认证程序中的登录认证,硬盘固件才将加密固态硬盘的用户分区对外放开。其中认证系统以映像文件的形式存储。加密固态硬盘在灌装认证系统和认证程序后,将用于度量认证系统的第一预期值和用于度量认证程序的第二预期值通过与硬盘固件协商的私有指令存储到加密固态硬盘的主控芯片的安全区域。

[0040] 如图1和图2所示,应用本实施例提供的加密固态硬盘认证分区的度量系统的度量方法如下。

[0041] 包括以下步骤:首先,开机启动,计算机加电,BIOS安全模块启动,BIOS安全模块读取加载加密固态硬盘认证分区中用于开机的认证系统,然后对认证系统进行度量。对认证系统的度量过程中,用哈希算法计算第一度量值,该哈希算法可以是MD5算法、SHA-1算法或其他算法,并将第一度量值通过SATA接口以及与硬盘固件协商的私有指令传输到硬盘固件,硬盘固件读取存储在主控芯片的安全区域的第一预期值,并将第一度量值与第一预期值进行比较,比较的度量结果记为第一结果,然后BIOS安全模块基于硬盘固件返回的比较的第一结果判断认证系统的度量结果,若比较的第一结果通过,BIOS基础模块读取并引导认证系统。认证系统度量通过后,BIOS基础模块将认证系统映像文件加载到CPU,主控权限交给认证系统。然后认证系统对认证程序进行度量。对认证程序的度量过程中,用哈希算法

计算第二度量值，该哈希算法可以是MD5算法、SHA-1算法或其他算法，硬盘固件读取存储在主控芯片的安全区域的第二预期值，并将第二度量值与第二预期值进行比较，比较的结果记为第二结果，认证系统基于硬盘固件返回的比较的第二结果判断认证程序的度量结果，若比较的第二结果通过，启动用于开机的认证程序，进行登录认证，若登录认证通过，加密固态硬盘的用户分区可见，硬盘正常使用。通过对认证系统和认证程序的分别度量，以避免加密固态硬盘的认证环节被绕过或被修改，防止用户分区被非法访问。

[0042] 进一步地，通过与硬盘固件协商的私有指令传输第一度量值、第二度量值，确保第一度量值、第二度量值不被篡改。其中，与硬盘固件数据传输的私有指令是将ATA指令集中的保留区域重新定义，并将修改后的ATA指令集作为外界与硬盘固件传输度量值的私有指令，从而保证数据传输的安全。度量结果通过，包括第一结果、第二结果，或其他结果，可以是比较的数值相等，相符，或其他合适的通过条件。

[0043] 进一步地，若第一度量值与第一预期值进行比较的第一结果不通过，即数值不相符或不符合其他通过条件，或者第二度量值与第二预期值进行比较的第二结果不通过，即数值不相符或不符合其他通过条件，格式化加密固态硬盘的认证分区。此时需重新对加密固态硬盘灌装认证系统及认证程序方可继续使用。

[0044] 其中，若认证程序的登录认证通过前，认证分区可见，用户分区不可见；若认证程序的登录认证通过后，认证分区不可见，用户分区可见。即加密固态硬盘的硬盘固件通过登录认证结果控制认证分区和用户分区是否可见。登录认证结果通过前，加密固态硬盘对外呈现为认证分区，登录认证结果通过后，对外呈现为用户分区，两个分区不会同时呈现。主控芯片的安全区域只允许硬盘固件对其访问，加密固态硬盘在进行灌装认证系统和认证程序时，通过与硬盘固件协商的私有指令将第一预期值和第二预期值传输到固件，并最终通过硬盘固件存储到主控芯片安全区域中。

[0045] 术语解释：

[0046] BIOS:Basic Input/Output System，基本输出输入系统。

[0047] 哈希算法:Hash，哈希算法将任意长度的二进制值映射为较短的固定长度的二进制值。

[0048] MD5算法:Message Digest Algorithm MD5，消息摘要算法第五版。

[0049] SHA-1算法:Secure Hash Algorithm-1，安全散列算法。

[0050] CPU:Central Processing Unit，中央处理器。

[0051] 本实施例提供的一种加密固态硬盘认证分区的度量方法和系统，具有以下优点：

[0052] (1)通过对认证系统和认证程序的度量，避免了加密固态硬盘的认证环节被绕过或被修改后直接访问用户分区的问题；

[0053] (2)第一度量值通过与硬盘固件协商的私有指令传输，确保第一度量值不被篡改；

[0054] (3)当对认证系统和认证程序的度量不通过时，格式化认证分区，保证用户分区中信息的安全。

[0055] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要

素的过程、方法、商品或者设备中还存在另外的相同要素。

[0056] 以上所述仅为本发明的若干实施例而已，并不用于限制本发明。对于本领域技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本发明的权利要求范围之内。

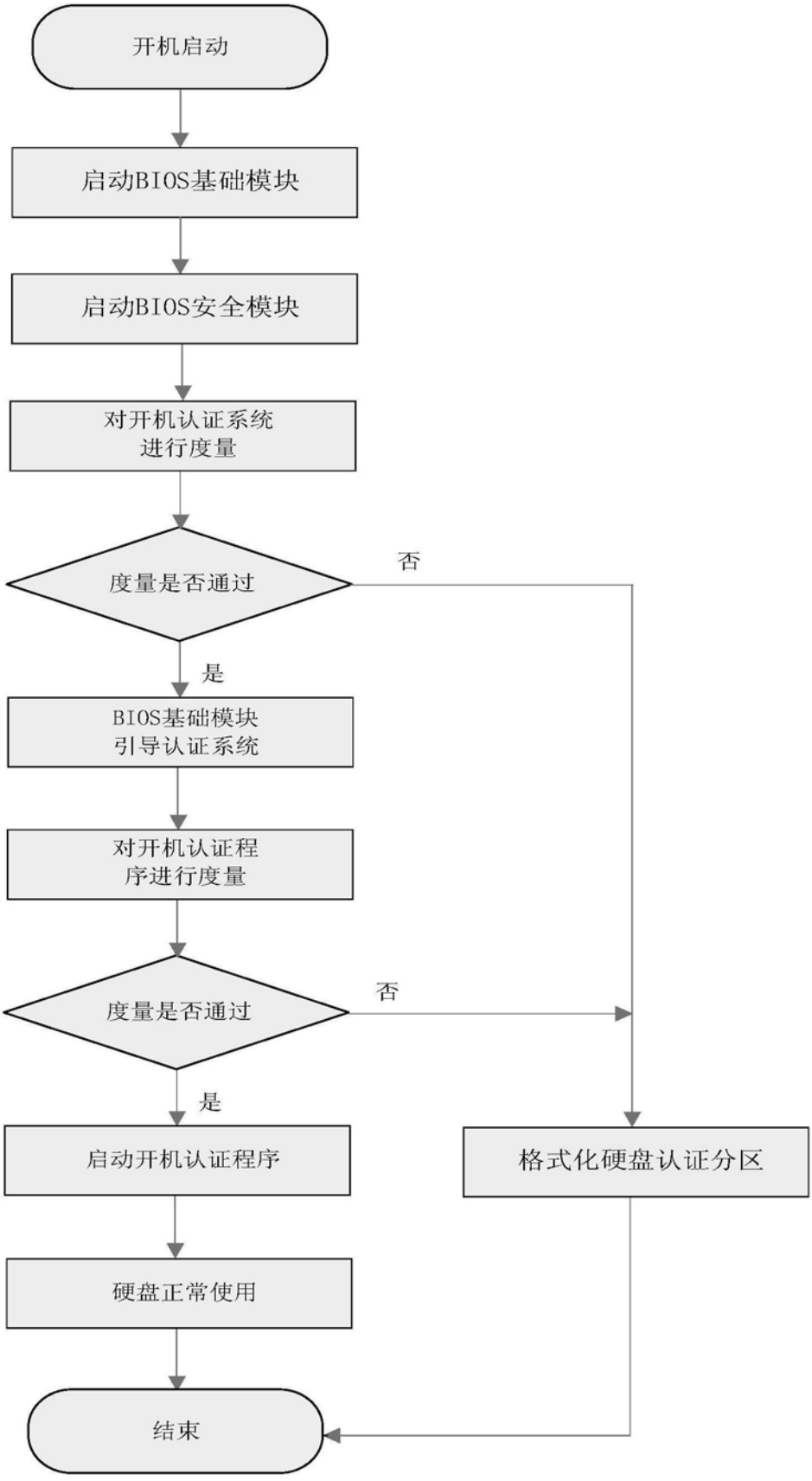

开机启动
启动BIOS基础模块
启动BIOS安全模块
对开机认证系统
进行度量
度量是否通过
否
是
BIOS基础模块
引导认证系统
对开机认证程
序进行度量
度量是否通过
否
是
启动开机认证程序
格式化硬盘认证分区
硬盘正常使用
结束

图1

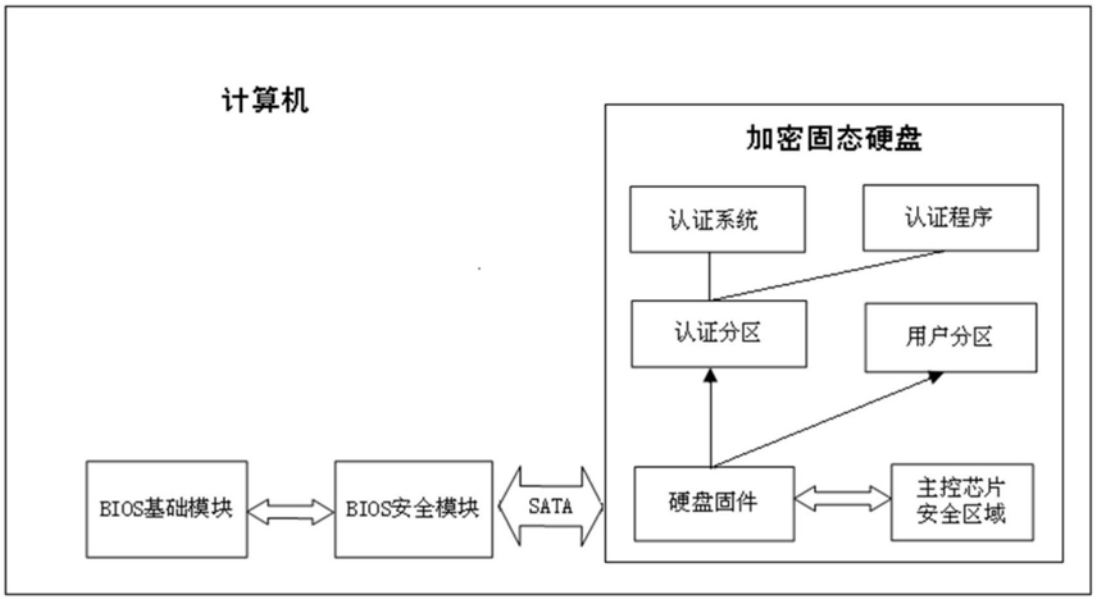

计算机
加密固态硬盘
认证系统
认证程序
认证分区
用户分区
BIOS基础模块
BIOS安全模块
SATA
硬盘固件
主控芯片
安全区域

图2