[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
*G06F 21/02 (2006.01)*
*G06F 12/14 (2006.01)*

[12] 发明专利申请公布说明书

[21] 申请号 200710125219.4

[43] 公开日 2009 年 6 月 24 日

[11] 公开号 CN 101464934A

[22] 申请日 2007.12.18
[21] 申请号 200710125219.4
[71] 申请人 中国长城计算机深圳股份有限公司
地址 518057 广东省深圳市南山区科技园长城计算机大厦
[72] 发明人 贾 兵 林诗达 石 明 张拥军 姚文泽 宋 靖

[74] 专利代理机构 深圳中一专利商标事务所
代理人 张全文

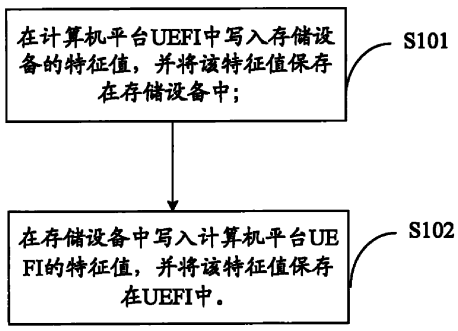
权利要求书 3 页 说明书 8 页 附图 3 页

[54] 发明名称

# 一种计算机平台与存储设备相互绑定、认证方法及计算机

[57] 摘要

本发明适用于信息安全计算机领域，提供了一种计算机平台与存储设备相互绑定、认证方法及计算机。 所述计算机平台与存储设备相互绑定方法包括步骤：在计算机平台的 UEFI 中写入存储设备的特征值，并将所述存储设备的特征值保存在存储设备中；在存储设备中写入计算机平台 UEFI 的特征值，并将所述 UEFI 的特征值保存在 UEFI 中。 所述计算机平台与存储设备相互认证方法包括步骤：将计算机平台的 UEFI 中的 UEFI 特征值与存储设备中的 UEFI 特征值进行对比；若相同，则 UEFI 认证存储设备通过；将计算机平台的 UEFI 中的存储设备特征值与存储设备中的存储设备特征值进行对比；若相同，则存储设备认证 UEFI 通过。 本发明确保存储设备数据的安全。



1、一种计算机平台与存储设备相互绑定方法，其特征在于，所述方法包括以下步骤:

在计算机平台的统一可扩展固件接口 UEFI 中写入存储设备的特征值，并将所述存储设备的特征值保存在存储设备中;

在存储设备中写入计算机平台 UEFI 的特征值，并将所述 UEFI 的特征值保存在 UEFI 中。

2、如权利要求 1 所述的计算机平台与存储设备相互绑定方法，其特征在于，在所述计算机平台的 UEFI 和存储设备中分别开设有两个地址段; UEFI 第一地址段及存储设备第二地址段保存有存储设备的特征值，UEFI 第二地址段及存储设备第一地址段保存有 UEFI 的特征值。

3、如权利要求 1 所述的计算机平台与存储设备相互绑定方法，其特征在于，所述存储设备的特征值由随机发生器产生，或由加密系统生成的 Key 作为特征值，或存储设备中写入的一部分受保护的代码作为特征值。

4、如权利要求 1 所述的计算机平台与存储设备相互绑定方法，其特征在于，所述 UEFI 的特征值由 UEFI 的随机发生器产生，或由加密系统生成的 Key 作为特征值，或 UEFI 中写入的一部分受保护的代码作为特征值。

5、如权利要求 1 所述的计算机平台与存储设备相互绑定方法，其特征在于，所述 UEFI 特征值及存储设备特征值都进行加密，加密的密钥通过可信平台模块 TPM 加密后分别存储在 UEFI 和存储设备中。

6、如权利要求 1 所述的计算机平台与存储设备相互绑定方法，其特征在于，所述存储设备为硬盘。

7、一种计算机平台与存储设备相互认证方法，其特征在于，所述方法包括以下步骤:

将计算机平台的 UEFI 中的 UEFI 特征值与存储设备中的 UEFI 特征值进行对比; 若相同，则 UEFI 认证存储设备通过;

将计算机平台的 UEFI 中的存储设备特征值与存储设备中的存储设备特征值进行对比；若相同，则存储设备认证 UEFI 通过。

8、如权利要求 7 所述的计算机平台与存储设备相互认证方法，其特征在于，所述将计算机平台的 UEFI 中的 UEFI 特征值与存储设备中的 UEFI 特征值进行对比步骤具体包括以下步骤：

计算机平台的 UEFI 获取存储设备第一地址段中的 UEFI 特征值；

UEFI 将 UEFI 第二地址段中特征值的加密密钥发给 TPM 让其解密，得到密钥 K1；

UEFI 调用加密系统，通过密钥 K1 将存储设备第一地址段中的 UEFI 特征值和 UEFI 第二地址段中的 UEFI 特征值进行解密；

在加密系统中进行对比所述解密后的两个 UEFI 特征值。

9、如权利要求 7 所述的计算机平台与存储设备相互认证方法，其特征在于，所述将计算机平台的 UEFI 中的存储设备特征值与存储设备中的存储设备特征值进行对比步骤具体包括以下步骤：

计算机平台的 UEFI 将 UEFI 第一地址段中的存储设备特征值发送到加密系统中；

计算机平台的 UEFI 并将存储设备第二地址段中的加密密钥发送到 TPM 进行解密，得到密钥 K2；

加密系统通过密钥 K2 对 UEFI 第一地址段中的存储设备特征值和存储设备第二地址段中的存储设备特征值进行解密；

在加密系统中进行对比所述解密后的两个存储设备特征值。

10、如权利要求 7 所述的计算机平台与存储设备相互认证方法，其特征在于，所述方法还包括以下步骤：

若 UEFI 认证存储设备不通过或存储设备认证 UEFI 不通过均进入重新绑定或重新初始化流程。

11、如权利要求 10 所述的计算机平台与存储设备相互认证方法，其特征在

于，所述重新绑定流程包括以下步骤：

输入安全员密码，系统进行对比存储设备中安全员的密码与输入的密码是否相同；如果相同，则 UEFI 中写入存储设备的特征值，并将所述存储设备的特征值保存在存储设备中；在存储设备中写入 UEFI 的特征值，并将所述 UEFI 的特征值保存在 UEFI 中。

12、如权利要求 10 所述的计算机平台与存储设备相互认证方法，其特征在于，所述重新初始化流程包括以下步骤：

存储设备微操作系统在检测到存储设备第一地址段和第二地址段中没有存放任何数据时，存储设备则将权限打开，UEFI 将 UEFI 的特征值写入到存储设备的第一地址段，并将所述 UEFI 的特征值写入到 UEFI 第二地址段；UEFI 第一地址段中写入存储设备的特征值，并将所述存储设备的特征值保存在存储设备第二地址段中。

13、一种计算机，包括存储设备及 UEFI，其特征在于，所述存储设备中保存有 UEFI 特征值及存储设备特征值；所述 UEFI 中保存有 UEFI 特征值及存储设备特征值；所述存储设备中保存的 UEFI 特征值与 UEFI 中保存的 UEFI 特征值相同；所述存储设备中保存的存储设备特征值与 UEFI 中保存的存储设备特征值相同。

# 一种计算机平台与存储设备相互绑定、认证方法及计算机

## 技术领域

本发明属于信息安全计算机领域，尤其涉及一种计算机平台与存储设备相互绑定、认证方法及计算机。

## 背景技术

随着计算机的不断普及，信息安全越来越受人们的关注。信息安全存在着多种多样的问题，有网络攻击带来的安全威胁；有系统漏洞带来的安全隐患，机器自身保护不够带来的信息泄露等等。要从根本上解决以上的问题，首先，要在平台上保证操作平台的可信。随着 TCG（Trusted Computing Group，可信计算组织）的成立，TPM（Trusted Platform Module，可信平台模块）芯片的普及应用，计算机平台在信息安全领域得到了突飞猛进的发展。在现在的信息安全产品中，由于各计算机生产商对可信计算机的理解和应用的不同，产品也不尽相同。现有的产品中，平台的可信尤为重要，信任链的传递贯穿整个平台。但是，可信并不完全代表着安全，在平台的可信上，由于没有与存储设备非常紧密地联系在一起，所以在用户最为关注的计算机存储设备的保护上，都没能起到很好的保护作用。

## 发明内容

本发明实施例所要解决的技术问题在于提供一种能够在计算机平台与存储设备之间保证信息安全的计算机平台与存储设备相互绑定、认证方法及计算机。

为解决上述技术问题，本发明实施例提供一种计算机平台与存储设备相互绑定方法，所述方法包括以下步骤：

在计算机平台的 UEFI 中写入存储设备的特征值，并将所述存储设备的特

征值保存在存储设备中；

在存储设备中写入计算机平台 UEFI 的特征值，并将所述 UEFI 的特征值保存在 UEFI 中。

本发明实施例还提供一种计算机平台与存储设备相互认证方法，所述方法包括以下步骤：

将计算机平台的 UEFI 中的 UEFI 特征值与存储设备中的 UEFI 特征值进行对比；若相同，则 UEFI 认证存储设备通过；

将计算机平台的 UEFI 中的存储设备特征值与存储设备中的存储设备特征值进行对比；若相同，则存储设备认证 UEFI 通过。

本发明实施例还提供一种计算机，包括存储设备及 UEFI，所述存储设备中保存有 UEFI 特征值及存储设备特征值；所述 UEFI 中保存有 UEFI 特征值及存储设备特征值；所述存储设备中保存的 UEFI 特征值与 UEFI 中保存的 UEFI 特征值相同；所述存储设备中保存的存储设备特征值与 UEFI 中保存的存储设备特征值相同。

在本发明实施例中，通过将计算机平台与存储设备相互绑定，达到二者相互依赖、紧密结合为一体。一旦存储设备离开绑定的计算机平台，则不能被其他的计算机平台所识别，从而确保存储设备数据的安全。

## 附图说明

图 1 是本发明实施例提供的计算机平台与存储设备相互绑定方法的实现流程示意图。

图 2 是本发明实施例提供的计算机平台与存储设备相互认证方法的实现流程示意图。

图 3 是本发明实施例提供的计算机的结构示意图。

## 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。

在本发明实施例中，通过将计算机平台与存储设备相互绑定，达到二者相互依赖、紧密结合为一体。一旦存储设备离开绑定的计算机平台，则不能被其他的计算机平台所识别，从而确保存储设备数据的安全。

本发明中所述的存储设备可为磁盘、硬盘、软盘或者是其他存储设备（如U盘）等。本发明实施例以存储设备为硬盘为例详细描述本发明。

请参阅图 1，本发明实施例提供的计算机平台与存储设备相互绑定方法包括以下步骤:

步骤 S101，在计算机平台 UEFI（Unified Extensible Firmware Interface，统一可扩展固件接口）中写入存储设备的特征值，并将该特征值保存在存储设备中;

步骤 S102，在存储设备中写入计算机平台 UEFI 的特征值，并将该特征值保存在 UEFI 中。

在硬盘和计算机平台 UEFI 的保护区域中分别开设有两个地址段。在计算机平台与硬盘初始化时，将硬盘微操作系统生成的特征值写入到计算机平台 UEFI 的 UEFI 第一地址段（地址段 1）中，同时把这个特征值写入到硬盘的第二地址段（地址段 2）中。UEFI 地址段 1 存放着硬盘的特征值，该硬盘的特征值是由硬盘微操作系统产生的，可以通过随机发生器产生特征值，或硬盘生成的 Key 作为特征值，或硬盘出厂时写入的一部分受保护的代码作为特征值，这部分代码只有通过特殊指令才能进行读取。

将计算机平台 UEFI 生成的特征值写入到硬盘的第一地址段(地址段 1)中，同时把这个特征值写入到 UEFI 的第二地址段（地址段 2）中。硬盘的地址段 1 存放着 UEFI 的特征值，该 UEFI 的特征值可以是由 UEFI 的随机发生器产生，或由其他加密系统生成的 Key 作为特征值，或主板出厂时写入的一部分受保护

的代码作为特征值，这部分代码也是需要通过特殊的指令才能调用。

上述所有写入的特征值数据都进行加密，加密的密钥通过 TPM 加密后分别存储在 UEFI 的地址段 2 和硬盘的地址段 2 中。上述所述的特征值主要特点是具有唯一性，不可更改性，不同的平台和不同的硬盘其特征值不同，它们需要进行保护后才存储起来。

请参阅图 2，本发明实施例提供的计算机平台与存储设备相互认证方法包括以下步骤：

步骤 S201，计算机平台 UEFI 通过特殊指令获取硬盘地址段 1 中的 UEFI 特征值；

步骤 S202，UEFI 将 UEFI 地址段 2 中特征值的加密密钥（密钥通过 TPM 加密）发给 TPM 让其解密，得到密钥 K1；

步骤 S203，UEFI 调用加密系统，通过 K1 把硬盘地址段 1 中的 UEFI 特征值和 UEFI 地址段 2 中的 UEFI 特征值解密；

步骤 S204，在加密系统中进行对比该解密后的两个特征值是否相同，如果两个特征值对比相同，UEFI 开放 UEFI 地址段 1 给硬盘调用，则代表着计算机平台认证硬盘成功；若对比不相同，则进入到步骤 S209 重新绑定计算机平台与硬盘；

步骤 S205，计算机平台 UEFI 将 UEFI 地址段 1 中的硬盘特征值发送到加密系统中；

步骤 S206，计算机平台 UEFI 并将硬盘地址段 2 中的加密密钥发送到 TPM 进行解密，得到密钥 K2；

步骤 S207，加密系统通过 K2 对 UEFI 地址段 1 中的特征值和硬盘地址段 2 中的特征值进行解密；

步骤 S208，在加密系统中进行对比该解密后的两个特征值，如果对比该解密后的两个特征值相同，则表示硬盘对平台的认证成功；完成这个认证过程后，代表着平台与硬盘是相互可信的，硬盘的微操作系统打开硬盘的控制权限给计

算机平台 UEFI，UEFI 可以通过正常的 ATA（Advanced Technology Attachment，高级技术配件）指令操作硬盘；如果对比不相同，硬盘始终处于禁止访问的一个保护状态，则进入到步骤 S209 重新绑定计算机平台与硬盘；

步骤 S209，重新绑定流程必须拥有安全员的密码才能完成，用户在输入安全员密码后，系统会进行对比硬盘中安全员的密码与输入的密码是否相同，如果相同，则进行重新绑定，硬盘地址段 1 会写入 UEFI 的特征值，同时 UEFI 地址段 1 也会写入硬盘的特征值；在完成整个的重新绑定过程后，硬盘的所有数据都可以保留，这便于主板平台的升级，或损坏后更换；

另一种方式是重新初始化，重新初始化是进行平台与硬盘的初始化，这个初始化与第一次的初始化有些相似；在完成重新初始化后，硬盘中的所有数据将会被全部清除掉，用户需要在重新进行分区才能正常使用硬盘，这个流程是任何人都可以进行的，不需要任何条件；确保硬盘丢失后数据不会被丢失，遵循宁可毁坏数据，不可泄露数据的原则。

下面详细描述 UEFI 与硬盘的初始化过程。

进行初始化的依据是硬盘地址段 1 中未写入任何数据。由于硬盘地址段 1 只有通过 UEFI 写入 UEFI 特征值数据后才能执行后面的硬盘特征值写入到硬盘地址段 2 和 UEFI 地址段 1。所以说硬盘地址段 2 也应该是空的。也就是说，新的硬盘在没进行过与计算机平台 UEFI 相互绑定，是需要进行一次初始化，这个初始化是第一次初始化，因为只要它进行过绑定，硬盘地址段 1 才会写入数据。

UEFI 与硬盘进行初始化的过程，硬盘微操作系统在检测到硬盘地址段 1 和地址段 2 中没有存放任何数据时，硬盘会将权限打开，让 UEFI 往里面写数据。首先，UEFI 先把 UEFI 的特征值写入到硬盘的地址段 1，同时也把 UEFI 的特征值写入到 UEFI 地址段 2，完成第一步的绑定。然后硬盘提供硬盘的特征值给 UEFI，UEFI 把硬盘的特征值写入到 UEFI 的地址段 1，同时也写入到硬盘的地址段 2，完成第二步绑定。在完成两次的绑定后，平台与硬盘的初始化算

是完成了。完成初始化后，计算机在开机后就必须先完成平台与硬盘的相互认证过程，只有完成平台与硬盘的相互认证过程后硬盘才能打开控制权限给UEFI。

在上述的所有操作过程中，UEFI调用地址段数据的指令都是特殊的指令，指令都是由加密系统进行加密的，密钥通过TPM加密保存起来。指令发出后，需要TPM把密钥解密，同时发出授权证书，硬盘的微操作系统在拿到指令密钥和授权证书后才能对指令进行解密，然后执行，完成整个交互过程的指令传输安全。

请参阅图 3，本发明实施例提供了平台与硬盘相互信任的计算机，其主要包括：硬盘以及主板；主板包括UEFI和TPM模块。在计算机平台UEFI中写入硬盘的特征值，并将该特征值保存在硬盘中；在硬盘中写入计算机平台UEFI的特征值，并将该特征值保存在UEFI中。所有写入的特征值数据都进行加密，加密的密钥通过TPM模块进行加密且保存在UEFI及硬盘中。

本发明实施例提供的硬盘嵌有一个微操作系统，由该微操作系统来控制着硬盘的使用权限和硬盘整盘数据的加密。硬盘在出厂时，已经划分出一部分保护分区，这块保护分区可以存放用户的一些重要消息，包括用户口令，微操作系统的安全员（管理员）口令，还有日志等等，硬盘的保护分区有一块地址段，用来存放硬盘和主板平台UEFI完成绑定的重要数据，同时平台UEFI与硬盘的认证过程也是调用这两个地址段中的数据来完成。

UEFI和BIOS类似，是连接上层操作系统和计算机硬件之间的桥梁。

UEFI初始化模块和驱动执行环境通常被集成在一个只读存储器中，好比现在传统 BIOS 固化程序一样。UEFI 初始化程序在系统开机的时候最先得到执行，它负责最初的CPU、北桥、南桥及存储器的初始化工作，当这部分设备就绪后，紧接着它就载入UEFI的DXE（Driver Execution Environment，驱动执行环境）。当DXE被载入时，系统就可以加载硬件设备的UEFI 驱动程序了。DXE使用了枚举的方式加载各种总线及设备驱动，UEFI驱动程序可以放置于系统的

任何位置，只要保证它可以按顺序被正确枚举。借助这一点，可以把众多设备的驱动放置在磁盘的 UEFI 专用保护分区中。当系统正确加载这个磁盘后，这些驱动就可以被读取并应用。UEFI 要加载这个磁盘就必须完成相互的绑定。它和硬盘一样，也有一段地址段存放着完成硬盘和平台绑定需要的重要数据。在完整性检测过程中，硬盘微操作系统将会调用这部分的空间来完成。

由于在各自的地址段中的数据是非常重要的，一般都需要加密后存储，加密密钥也需要经过 TPM 进行加密后才能存储在 UEFI 和硬盘中。如果相互的平台认证不能通过，硬盘将处于禁止使用的保护状态，从而确保硬盘信息的安全。

本发明应用的 UEFI 架构，它与传统的 BIOS 相比较，具有以下明显的优势。

| 传统 BIOS 的缺点 | UEFI 特点 |
|---|---|
| 16 位汇编代码，代码编写维护复杂 | C 语言，方便维护 |
| 即插即用远非完美 | 驱动开发简单、兼容性好 |
| 文本界面，用户操作体验不佳 | 支持图形环境、支持鼠标操作 |
| 代码运行缓慢、启动时间长 | 运行于 32 位或 64 位模式、启动快 |
| 扩展性强 | 强大的可扩展功能 |

UEFI，可以当成是一个简化的操作系统，在现有的计算机发展中，传统的 BIOS 的缺点已经成为制约计算机技术发展的主要因素。它文本界面操作使得用户只能进行简单界面整合操作，而 UEFI 却能从功能和界面上整合硬盘的管理工具，提供用户友好而易操作的用户界面。UEFI 采用 C 语言开发，相对简单，维护相对方便，模块化扩展整合比较强大。UEFI 还拥有自己的 CSM（Compatibility Support Module，兼容性支持模块）模块，所以兼容性比较强。各个模块可以独立开发，然后再集成在 UEFI 中。在整个 UEFI 的维护上比传统的 BIOS 方便好多。

安全计算机的平台与硬盘的绑定功能便是基于 UEFI 之上开发完成的。通过 UEFI 和硬盘内嵌的微操作系统在功能和界面上的整合，用户可以在一个友

好的图形界面中完成操作，而且同时可以支持鼠标。整合后硬盘的加密系统能对 UEFI 需要进行加密的数据进行加密，然后加密的密钥通过 TPM 进行加密后存储在硬盘的保护分区中，或 UEFI 的 BIOS ROM 或 Flash 中。在整个平台的绑定过程中，用户需要完成相互认证写入或读取的地址段信息是通过硬盘加密系统进行加密的，密钥通过 TPM 加密后存放在硬盘的保护空间和主板上 UEFI 的存储器中。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

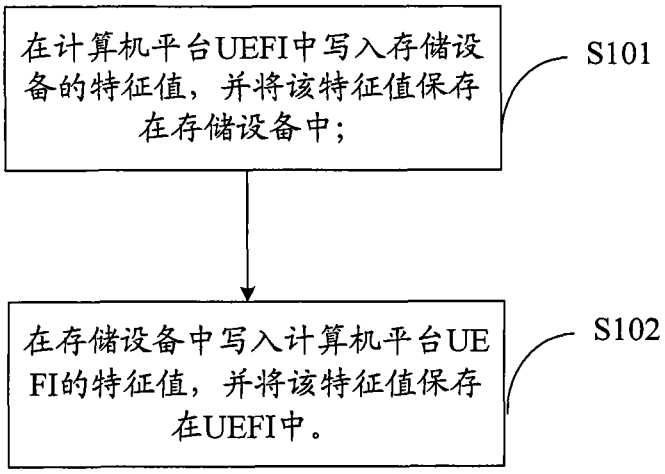

在计算机平台UEFI中写入存储设备的特征值，并将该特征值保存在存储设备中；
S101
在存储设备中写入计算机平台UEFI的特征值，并将该特征值保存在UEFI中。
S102

图 1

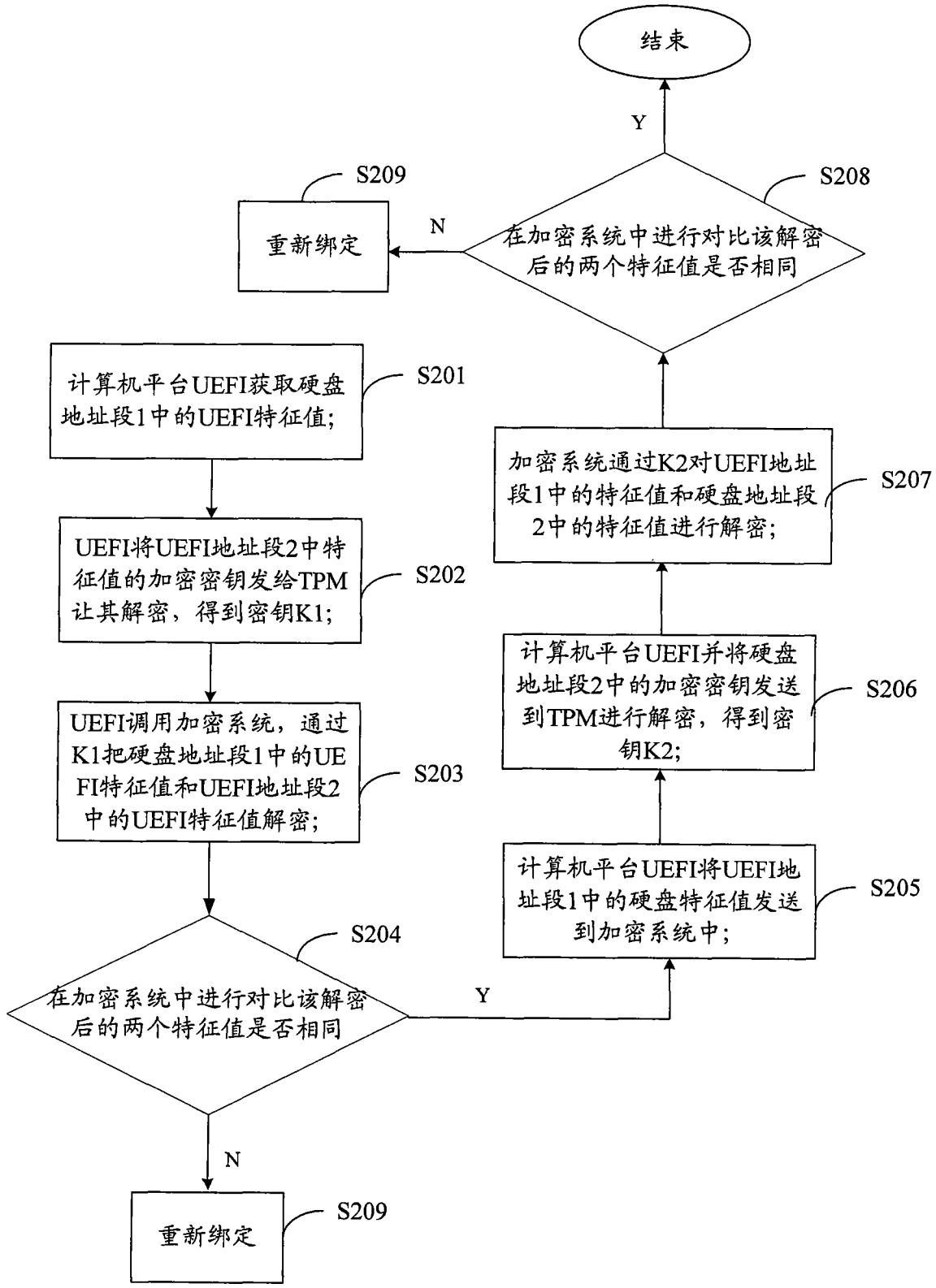

结束
Y
S208
在加密系统中进行对比该解密后的两个特征值是否相同
N
S209
重新绑定
S201
计算机平台UEFI获取硬盘地址段1中的UEFI特征值;
S202
UEFI将UEFI地址段2中特征值的加密密钥发给TPM让其解密，得到密钥K1;
S203
UEFI调用加密系统，通过K1把硬盘地址段1中的UEFI特征值和UEFI地址段2中的UEFI特征值解密;
S204
在加密系统中进行对比该解密后的两个特征值是否相同
Y
N
S209
重新绑定
S205
计算机平台UEFI将UEFI地址段1中的硬盘特征值发送到加密系统中;
S206
计算机平台UEFI并将硬盘地址段2中的加密密钥发送到TPM进行解密，得到密钥K2;
S207
加密系统通过K2对UEFI地址段1中的特征值和硬盘地址段2中的特征值进行解密;

图 2

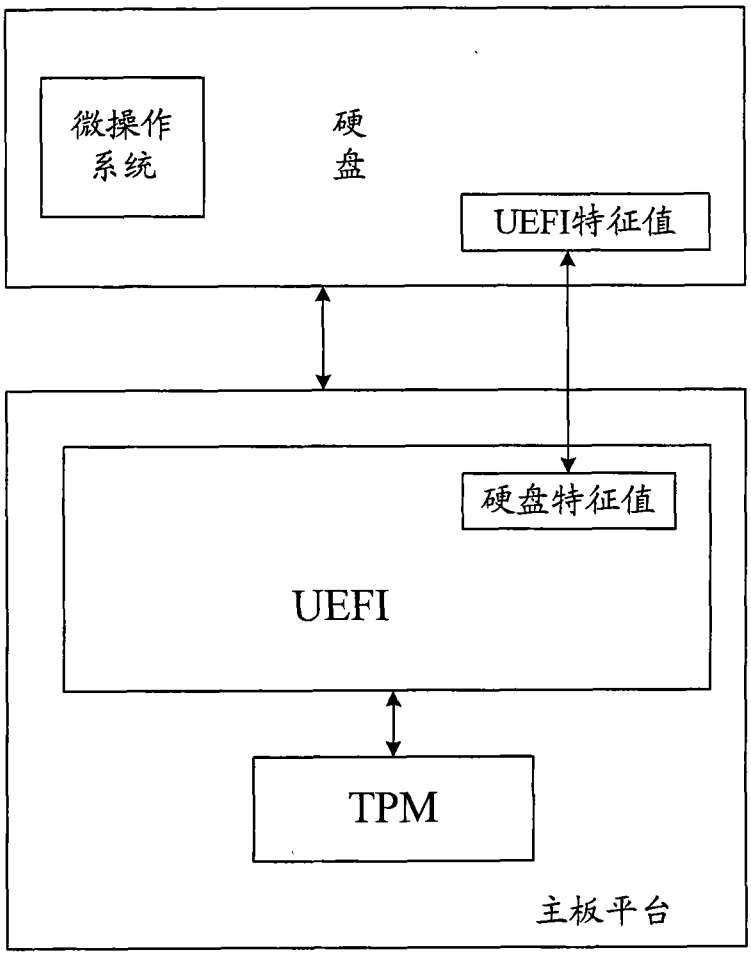



图 3