[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/22 (2006.01)
G06F 9/445 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810111682.8

[43] 公开日 2008 年 10 月 8 日

[11] 公开号 CN 101281577A

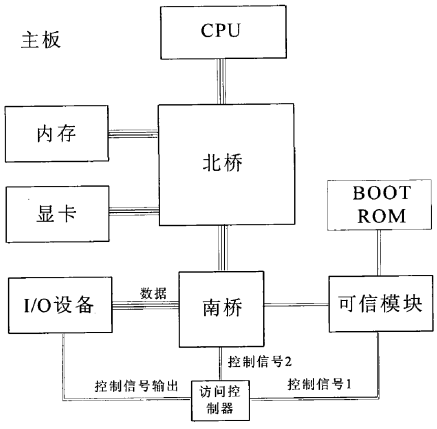
[22] 申请日 2008.5.16
[21] 申请号 200810111682.8
[71] 申请人 北京工业大学
地址 100124 北京市朝阳区平乐园 100 号
[72] 发明人 张 兴 毛军捷 刘贤刚 姜广智 孙 瑜 庄俊玺 李萌萌 李 瑜
[74] 专利代理机构 北京思海天达知识产权代理有限公司
代理人 刘 萍
权利要求书 3 页 说明书 10 页 附图 6 页

[54] 发明名称

一种对 BIOS 进行保护的可信计算系统及其应用方法

[57] 摘要

一种对 BIOS 进行保护的可信计算系统及其应用方法属于信息安全领域，特征在于可信计算模块与 BOOT ROM 的物理连接方式：先将所述可信计算模块连接到系统主板上，再通过通信总线将 BOOT ROM 连接到可信计算模块上。 可信计算模块包括 DMA 控制器、FIFO 单元、安全隔离单元；DMA 控制器用于将 BIOS 代码读入到可信计算模块的 FIFO 单元或者将 BIOS 代码从 FIFO 单元中读出到可信计算模块 I/O 总线上；FIFO 用于暂存待处理的 BIOS 代码；安全隔离单元用于防止可信计算模块外部恶意程序读取可信计算模块内部存储单元机密信息。本发明对 BIOS 代码的读写和更新都需要对当前操作用户进行身份认证和口令认证，保证 BIOS 关键代码自身的安全性；通过硬件方法实现设备访问控制，达到对主板外围设备进行主动控制的效果。



1．一种可信计算系统，包括主板及主板外围设备，主板包括可信计算模块 TCM、中央处理器 CPU、主板设备控制器，BOOT ROM；

所述可信计算模块包括：自主密码引擎、自主密码算法模块和自主密钥生成器，I/O 总线；

所述可信计算模块用于，不可篡改地存储核心可信度量根、可信存储根、可信报告根，对外围设备和 BIOS 关键代码进行完整性度量与读写保护；

所述 CPU 用于，接收到可信计算模块对 BIOS 关键代码度量完成的指示后，加载并执行 BIOS 代码中的初始化和启动部分；

主板外围设备用于，接受可信计算模块的权限访问控制，针对不同的用户提供不同的服务；

所述 BOOT ROM 用于，存储可信计算系统的初始化和启动代码；

其特征在于：所述可信计算模块与 BOOT ROM 的物理连接方式：先将所述可信计算模块连接到系统主板上，再通过通信总线将 BOOT ROM 连接到可信计算模块上；用于保护 BIOS 代码，防止恶意程序对其篡改。

2．如权利要求 1 所述的可信计算系统，其特征在于，可信计算模块内部包括 DMA 控制器、专用 FIFO 单元、安全隔离单元；

所述可信计算模块内部的 DMA 控制器用于将 BIOS 代码读入到所述可信计算模块的专用 FIFO 单元或者将 BIOS 代码从所述可信计算模块内部专用 FIFO 单元中读出到所述可信计算模块 I/O 总线上；

所述可信计算模块内部的 FIFO 单元，用于暂存待处理的 BIOS 代码；

所述可信计算模块内部的安全隔离单元，用于防止可信计算模块外部恶意程序读取可信计算模块内部存储单元机密信息；

3．如权利要求 1 所述的可信计算系统，其特征在于，所述可信计算模块的 I/O 总线，包括至少一组主从复用的 LPC 总线和一组 SPI 总线；

所述输出模式 LPC 总线，可信 计算模块通过使用 LPC 总线，被当作设备接在系统设备控制器上，或者作为访问发起端，访问其他设备；

所述输出模式 SPI 总线，可信 计算模块通过使用 SPI 总线，被当作设备接在系统设备控制器上，或者作为访问发起端，访问其他设备。

4．如权利要求 1 所述的可信计算系统，其特征在于，所述系统进一步包括身份识别设备，所述身份识别设备通过身份设备总线直接连接到可信计算

模块；

所述身份识别设备总线是通用输入输出 GPIO 总线、USB 总线、ISO7816 总线通讯总线。

5. 如权利要求 1 所述的可信计算系统，其特征在于，可信计算模块与 BOOT ROM 之间的通讯总线，是通用输入输出 GPIO 总线、主从模式 LPC 总线、主从 SPI 总线、USB 总线、ISO7816 总线。

6. 如权利要求 1 所述的可信计算系统，其特征在于，在主板设备控制器与主板外围硬件设备的控制信号线之间添加一个访问控制器，由可信计算模块负责控制该设备访问控制器，阻断或者接通系统设备控制器与主板外围硬件设备的控制信号线；

所述访问控制器，系统 CPU 通过该设备访问控制器发出设备访问信号，访问主板上的所有硬件设备；

所述访问控制器的输入信号线，至少包括一条接在系统设备控制器上，一条接在所述可信计算模块的 I/O 总线上。

7. 一种应用权利要求 1 所述可信计算系统的方法，其特征在于：

系统启动阶段及非可信环境下 BIOS 代码读取流程，CPU 读取 BIOS 的工作流程如下：

1）CPU 向可信计算模块发出读取 BIOS 代码的请求信号；

2）可信计算模块检查工作状态，如果可信计算模块处在功能使能状态，则 CPU 执行一条等待指令，直到可信计算模块准备好 BOOT ROM 的地址映射；如果可信计算模块处在功能禁用状态，则直接将 BOOT ROM 总线接口映射到可信计算模块的 LPC 总线对应的地址范围上；

3）CPU 等待的同时，可信计算模块执行身份认证和口令认证相结合的安全措施；如果认证成功则执行 BIOS 的完整性检查，如果不成功则结束对 BIOS 的读取操作，计算机下电重启；

4）通过安全认证后，可信计算模块应将 BIOS 的代码读入到 FIFO 中，并完成完整性检查；BIOS 通过了可信计算模块的完整性检查，则可信计算模块将 BOOT ROM 总线接口映射到可信计算模块 LPC 总线对应的地址范围上；

5）可信计算模块完成对 BOOT ROM 地址空间的映射后，CPU 直接读取并执行 BIOS 代码；CPU 读取完 BIOS 代码后，整个读 BIOS 代码操作结束；

可信环境建立后 BIOS 代码读取流程

1）CPU 向 TCM 发出读取 BIOS 的请求信号；

2）可信计算模块检查工作状态，如果可信计算模块处在功能使能状态，则 CPU 执行一条等待指令，直到可信计算模块准备好 BOOT ROM 的地址映射；如果可信计算模块处在功能禁用状态，则直接将 BOOT ROM 总线接口映射到可信计算模块的 LPC 总线对应的地址范围上；

4）可信计算模块将 BOOT ROM 总线接口映射到可信计算模块的 LPC 总线对应的地址范围上；

5）可信计算模块完成对 BOOT ROM 地址空间的映射后，CPU 直接读取并执行 BIOS 代码；CPU 读取完 BIOS 代码后，整个读 BIOS 操作结束；

计算机 CPU 对 BIOS 代码进行更新，具体步骤如下：

1）CPU 向可信计算模块发出读取 BIOS 代码的请求信号；

2）可信计算模块检查工作状态，如果可信计算模块处在功能使能状态，则 CPU 执行一条等待指令，直到可信计算模块完成对当前用户身份认证和口令认证操作；如果可信计算模块处于功能禁用状态，则可信计算模块将 BOOT ROM 总线接口映射到可信计算模块的 LPC 总线地址空间；并向 CPU 发出写 BIOS 代码响应信号；CPU 收到写 BIOS 代码响应信号后，直接将 BIOS 代码写入到 BOOT ROM 中；

3）可信计算模块执行身份认证和口令认证操作。如果当前用户通过身份认证和口令认证，则可信计算模块读取 BIOS 代码；如果没有通过认证，则退出对 BIOS 代码的更新操作，然后由管理员执行相应的预定义的处理策略；

4）可信计算模块给 CPU 发出 BIOS 代码更新响应信号，读取 BIOS 代码到可信计算模块中的 FIFO 中；可信计算模块根据完整性参考值的计算方法，对依次读入的 BIOS 关键代码进行杂凑计算，得出完整性参考值；完成对所有 BIOS 代码的完整性参考值计算后，将完整性参考值写入到可信计算模块中；

5）可信计算模块中的 DMA 控制器通过可信计算模块与 BOOT ROM 之间定义的连接线，将 FIFO 中计算过的 BIOS 代码写入到 BOOT ROM 中；完成 BIOS 代码的写入操作后，整个 BIOS 代码的更新过程结束。

一种对 BIOS 进行保护的可信计算系统及其应用方法

技术领域

本发明涉及信息安全领域，尤其涉及一种可信计算系统硬件平台实现及对硬件平台安全可信保护的方法。

背景技术

近些年来可信计算已经成为信息安全领域一个新的发展方向，越来越多的引起相关研究单位的重视。可信计算系统的主要以可信安全芯片为基础，建立一个用户可以预期的安全计算环境，保证计算软硬件资源会被恶意篡改。

可信计算组织（Trusted Computing Group，TCG）最早提出并指定了可信计算行业标准。通过在主板上引入安全芯片来逐级建立信任链，并保证信任链的安全，最后在计算机硬件系统上构建一个安全可信的工作环境。

TCG 组织已经相继推出了两个版本的可信计算规范，其中规定了可信安全芯片的硬件组成结构、芯片内部功能、芯片指令接口、芯片硬件接口、芯片链接到主板的方式、芯片的使用方式等相关内容。

现有的可信计算系统平台中，TPM、主板外围设备和 BOOT ROM 被安置在系统设备控制器的总线上，作为从设备，由该系统设备控制器操作。因此，TPM 无法在 CPU 执行 BIOS 代码后，通过系统设备控制器对主板外围设备和 BOOT ROM 进行保护，也就无法对该系统设备控制器芯片自身的启动及该启动之前的动作提供可信的计算环境；并且，TCG 规范中只提供了操作系统（Operating System，OS）层以下的可信传递流程，但并未给出信任传递的具体实现方法，以及对系统硬件平台的安全要求和具体实现方法，且无法为 OS 层以上的计算提供可信的计算环境。

此前，有两种保护 BIOS 代码的方法，一是将 BIOS 启动代码放入到 TPM 模块内部、二是将 BIOS 代码固化到 ROM 只读存储体中。方法一：好处是保证了 BIOS 代码和系统平台的安全。缺点没有考虑到实际上 BIOS 代码的容量大，做到 TPM 芯片内部费用无法接受；方法二：好处是保证了 BIOS 代码和系统平台的安全。缺点没有考虑到实际上 BIOS 代码的实时更新的需要。

发明内容

有鉴于此，本发明的目的在于提供一种可信计算系统硬件平台实现及对硬件平台安全可信保护的方法，以建立可信计算环境。

为达到上述目的，本发明的技术方案具体是这样实现的：

一种可信计算系统，包括主板及主板外围设备，主板包括可信计算模块、中央处理器 CPU、内存、主板设备控制器，BOOT ROM；

所述可信计算模块包括：自主密码引擎、自主密码算法模块和自主密钥生成器，I/O 总线；

所述可信计算模块用于，实现可信度量功能、可信存储功能、可信报告功能，对外围设备和 BOOT ROM 关键代码进行完整性度量与读写保护；

所述 CPU 用于，接收到可信计算模块对 BOOT ROM 关键代码度量完成的指示后，加载并执行 BOOT ROM 中的初始化和启动代码；

主板外围设备用于，接受可信计算模块的权限访问控制，针对不同的用户提供不同的服务；

所述 BOOT ROM 用于，存储可信计算系统的初始化和启动代码；

其特征在于：所述可信计算模块与 BOOT ROM 的物理连接方式：先将所述可信计算模块连接到系统主板上，再通过通信总线将 BOOT ROM 连接到可信计算模块上。用于保护 BIOS 代码，防止恶意程序对其篡改。

可信计算模块内部包括 DMA 控制器、FIFO 单元、安全隔离单元；

所述可信计算模块内部的 DMA 控制器用于将 BIOS 代码读入到所述可信计算模块的 FIFO 单元或者将 BIOS 代码从所述可信计算模块内部 FIFO 单元中读出到所述可信计算模块 I/O 总线上；

所述可信计算模块内部的 FIFO 单元，用于暂存待处理的 BIOS 代码；

所述可信计算模块内部的安全隔离单元，用于防止可信计算模块外部恶意程序读取可信计算模块内部存储单元机密信息；

所述可信计算模块的 I/O 总线，包括至少一组主从复用的 LPC 总线和一组 SPI 总线；

所述输出模式 LPC 总线， 可信 计算模块通过使用 LPC 总线，被当作设备接着系统设备控制器上，或者作为访问发起端，访问其他设备（如 BOOT ROM）。

所述输出模式 SPI 总线， 可信 计算模块通过使用 SPI 总线，作为访问发起端，访问其他设备（如 BOOT ROM）。

所述系统进一步包括身份识别设备，所述身份识别设备通过身份设备总线直接连接到可信计算模块；

所述身份识别设备总线是通用输入输出 GPIO 总线、USB 总线、ISO7816 总线中的一种。

可信计算模块对主板外围硬件设备的安全访问控制，首先先通过可信计算模块读取用户身份识别设备，判断用户身份权限，再通过对用户身份级别的分类，控制用户对主板硬件设备的使用权限。

可信计算模块与 BOOT ROM 之间的通讯总线，是通用输入输出 GPIO 总线、主从模式 LPC 总线、主从 SPI 总线、USB 总线、ISO7816 总线。

在主板设备控制器与主板外围硬件设备的控制信号线之间添加一个设备访问控制器，由可信计算模块负责控制该设备访问控制器，阻断或者接通系统设备控制器与主板外围硬件设备的控制信号线；

所述的设备访问控制器，系统 CPU 发出的设备访问信号通过该设备访问控制器发送给主百外围硬件设备，达到对主板上的所有硬件设备的访问控制；

所述设备访问控制器的输入信号线，至少包括一条接在系统设备控制器上，一条接在所述可信计算控制模块的 I/O 总线上。

所述可信计算模块内部的 FIFO，其特征在于，用于在读写和更新 BIOS 代码时，缓存系统 CPU 与 BOOT ROM 之间传输的数据。其大小由可信计算模块与系统 CPU 之间的数据传输速度、可信计算模块与 BOOT ROM 的数据传输速度和可信计算模块对 BIOS 代码度量速度共同决定。

可信计算模块与系统CPU之间的数据传输速度大小应由系统体系结构规定的传输规范决定；可信计算模块与BOOT ROM的数据传输速度应根据具体采用的传输总线和实际制定的传输频率决定，可以不遵守系统体系结构规定的总线传输速度；可信计算模块对BIOS代码度量速度由可信计算模块中执行单元的处理速度和FIFO中数据的装载量决定。

附图说明

图1是TCG规范中规定的可信计算平台模块的系统结构图

图2是TCG规范中规定的可信计算系统结构图

图3是本发明实施例提供的可信计算模块安全芯片体系结构

图4是本发明实施例提供的可信计算系统结构图

图5是本发明实施例提供的系统启动阶段及非可信环境下BIOS代码读取流程图

图6是本发明实施例提供的可信环境建立后BIOS代码读取流程图

图7是本发明实施例提供的计算机CPU对BOOT ROM中BIOS代码的写操作

图8是本发明实施例提供的基于可信计算模块的安全计算机工作流程

具体实施方式

安全体系结构

以INTEL架构为基础的可信计算机终端为例，针对现有技术对可信平台模块TPM对可信计算系统硬件平台的安全保护措施不完善的问题，提出了基于可信计算模块的一种可信计算系统硬件平台实现及对硬件平台安全可信保护的方法，以建立可信计算环境。

相对于TCG规定的传统TPM可信平台模块系统结构及主板布线方法(如图1、图2)，本发明中提出的可信计算模块系统结构及主板布线方法（如图3、图4）具体改进如下：

在可信计算模块内部增加了FIFO单元，用于读入BIOS关键代码，提高可信计算模块和BOOT ROM之间的数据传输频率。FIFO由FLASH实现。加入DMA控制器，提高数据传输速度；

用硬件或者固件的形式实现对BIOS代码的保护。

如图 4 所示，BOOT ROM 通过通信总线连接到可信计算模块上，然后可信计算模块再通过 LPC 总线连接到计算机主板南桥上的设备控制器上（AMD 架构中，是直接连接到总线控制器上）。

在可信计算硬件平台上的外围设备和南桥上的设备控制器之间再引入一个设备访问控制器，用于实现不同用户对硬件设备的使用权限划分。访问控制器的控制信号 1 上，可信计算模块提供的对外围设备的访问控制信号；控制信号 2 是南桥对外围设备的控制信号。控制信号 1，决定南桥发出的控制信号 2 是否对外围设备有效。当控制信号 2 对外围设备无效时，外围设备被认为是禁用状态，否则为可用状态。可信计算机启动时候，默认状态是除键盘、鼠标，显示器外，其他所有输入输出设备都处于禁用状态。对外围设备的访问控制由可信计算模块内部的用户管理表维护。

可信计算模块中设置 N KB 的 FLASH 实现 FIFO 单元，用于存储计算机主板 BIOS 代码。主要目的是为了缩短系统启动时间。为了提高效率，可以在每次关机前将 BOOT 前 N k bit 大小的代码读入。N 的设定主要和以下三个因素有关：

可信计算模块和 BOOT ROM 之间的数据传输速度 V1。

可信计算模块和南桥设备控制器之间数据传输速度决定 V2。

可信计算模块对 BIOS 关键代码的完整性检查速度 V3。

可信计算模块使能状态下，计算机 CPU 上电后，跳转到 0XFFFFFFF0H 地址空间后，执行的第一条指令是等待指令。当可信计算模块对 BIOS 代码的完整性检查完成后，计算机 CPU 才可以继续执行 BIOS 所有代码。如果没有通过完整性检查，根据预定义策略执行相应操作。

可信计算模块使能状态下，计算机 CPU 要完成对 BOOT ROM 的写操作时，可信计算模块先判定当前用户身份是是否合法，而后才可以对 BIOS 进行更新。为了加大对 BIOS 代码的保护力度，同样可以混合使用用户身份认证和可信计算模块的口令认证方式，进一步提高系统安全性。

可信计算模块仍然提供使能和禁用的选择功能。当可信计算模块功能禁用时，可信计算模块可以接受功能使能指令。同时可信计算模块不再通过 FIFO 转存 BOOT ROM 中 BIOS 代码，而是直接将 BOOT ROM 的总线接口直接映

射到可信计算模块对外的I/O地址空间上，进而计算机南桥总线控制器可以直接读取到BIOS代码。

与TCG规范中不同，本方案设计的可信计算模块安全芯片内部设置了安全隔离单元，防止计算机平台上的恶意代码读写可信计算模块内部存储区，进而也保证了可信计算模块自身的安全性。

工作流程

系统启动阶段及非可信环境下BIOS代码读取流程

如图5，当计算机系统启动阶段和进入到非可信工作环境下对BIOS代码的访问，都需要对BIOS关键代码进行完整性检查。CPU读取BIOS代码的工作流程如下：

CPU通过南桥总线控制器（AMD架构中没有南桥的概念，认为是通过设备总线控制器）向可信计算模块发出读取BIOS代码的请求信号。

可信计算模块检查工作状态，如果可信计算模块处在功能使能状态，则CPU执行一条等待指令，直到可信计算模块主备好BOOT ROM的地址映射。

CPU等待的同时，可信计算模块执行身份认证和口令认证相结合的安全措施。如果认证成功则执行BIOS代码的完整性检查，如果不成功则结束BIOS代码的读取操作，交由管理员执行相应预定义处理策略。

当通过安全认证后，可信计算模块应将BOOT ROM中BIOS的关键代码依次读入到FIFO中，并完成完整性检查。

如果BIOS代码通过了可信计算模块的完整性检查，则可信计算模块将BOOT ROM总线接口映射到可信计算模块的LPC总线对应的地址范围上。

如果在步骤2）中，可信计算模块处在功能禁用状态，则直接将BOOT ROM总线接口映射到可信计算模块的LPC总线对应的地址范围上。

可信计算模块完成对BOOT ROM地址空间的映射后，CPU可以直接读取并执行BIOS代码。

CPU读取完BIOS代码后，整个读BIOS代码操作结束。

可信环境建立后BIOS代码读取流程

如图6，当计算机系统的完成了信任链的建立后，进入到了可信的工作环境中。则此后对BIOS代码的读取操作就可以认为是可信的操作，不用再对

BIOS 的关键代码做完整性检查。具体步骤与系统启动阶段读取 BIOS 代码流程类似。

计算机 CPU 对 BOOT ROM 中 BIOS 代码的写操作

如图 7 ，计算机中的 CPU 同样可以对 BIOS 代码进行更新。具体步骤如下：

CPU 通过南桥设备控制器向可信计算模块发出写 BIOS 代码的请求。

可信计算模块接到写 BIOS 代码的请求后，首先检查可信计算模块当前所处的工作状态。

在 2）步骤中，如果可信计算模块处在功能使能状态，则可信计算模块先向发送等待指令。CPU 执行等待指令，直到可信计算模块完成对当前用户身份认证和口令认证等安全保障操作。

可信计算模块通过执行身份认证和口令认证操作，提高系统的安全性，防止恶意代码的破坏。

如果当前用户通过身份认证和口令认证，则可信计算模块从南桥总线上读取 BIOS 代码。如果没有通过认证，则退出对 BIOS 代码的更新操作，然后由管理员执行相应的预定义的处理策略。

可信计算模块给 CPU 发出 BIOS 代码更新响应信号，从南桥 LPC 总线上依次读取 BIOS 代码到可信计算模块中的 FIFO 中。可信计算模块根据完整性参考值的计算方法，对依次读入的 BIOS 关键代码进行杂凑计算，得出完整性参考值。

可信计算模块中的 DMA 控制器通过可信计算模块与 BOOT ROM 之间定义的连接线，将 FIFO 中计算过的 BIOS 代码写入到 BOOT ROM 中。

完成对所有 BIOS 代码的完整性参考值计算后，将完整性参考值写入到可信计算模块中的非挥发失性存储空间中。

如果步骤 2）中检测的结果是可信计算模块处于功能禁用状态，则可信计算模块将 BOOT ROM 的总线接口映射到可信计算模块的 LPC 总线地址空间。并通过南桥控制器，向 CPU 发出写 BIOS 代码响应信号。

CPU 收到写 BIOS 代码响应信号后，直接将 BIOS 代码写入到 BOOT ROM 中。

完成 BIOS 代码的写入操作后，整个 BIOS 代码更新过程结束。

基于可信计算模块的安全计算机工作流程

如图 8 ，工作流程分为三个部分：可信工作模式流程、非可信工作模式流程和异常处理工作流程。

可信工作环境建立流程：

计算机开机，可信计算模块需要完成 STEP1（STEP1 指功能禁用状态或者是处于出错状态）、STEP2（STEP2 包括出错状态检查、初始化自检、度量 BIOS 关键代码、认证绑定操作）操作。经用户登录，可信计算模块可以响应计算机 CPU 发出的读 BIOS 代码请求信号。CPU 读取并执行 BIOS 代码，开始进入可信工作模式。

接收指令：如果没有接收到指令则处于等待接收指令状态。

口令判断：指令集部分指令需要通过授权口令判断才能执行。如果没有通过口令判断，则应该向可信计算平台返回指令失败应答信号，装换到空闲等待接收指令状态。

指令解析：将接收到的指令进行细化分析，转换成可复用的原语操作。

访问权限检查：如果指令需要使用到硬件设备时，需要检查当前用户对该设备的使用权限。通过检查的指令可以继续执行，没有通过检查的指令不能执行，并向可信计算平台返回指令失败应答信号。

指令执行：执行通过检查的指令包含的所有原语操作。

返回成功应答：当指令包含的所有原语操作都执行完成后，应向可信计算平台发送指令执行成功应答信号。

可信计算平台掉电判断：当向可信计算平台发送指令执行成功应答信号后，应做可信计算平台掉电判断。如果有掉电请求，则应执行平台掉电操作。如果没有掉电请求，则应回到等待接收指令状态。

非可信工作模式流程：

计算机平台上电启动后，可信计算模块进行 STEP1 状态判断。如果出于 STEP1 状态，则应按照下面流程完成功能可信计算模块禁用状态或者出错状态处理流程：

用户登录：当 TPCM 处于功能禁用状态或者处于出错状态后，系统提示用户登录。如果登录的是管理员，则可以进入到对可信计算模块的使能状态设置操作流程。如果是普通用户登录，则可以进入到非可信工作环境。

计算机 CPU 执行 BIOS 代码：完成用户登录后，可信计算模块可响应计算机 CPU 发出的读取 BIOS 代码的信号。CPU 读取并执行 BIOS 代码。

普通用户登录：如果 1）步骤中普通用户登录，则可以选择是否继续启动，进入到非可信操作系统中，或者是平台、TPCM 都掉电，并退出系统。

管理员登录：如果 1）步骤中管理员登录，则可以选择是否使能可信计算模块，并执行平台掉电重新启动，或者是平台掉电，并退出系统。

异常处理工作流程：

可信计算模块上电启动后，当处于功能使能状态，应进行出 STEP2 操作并判断操作结果。如果 STEP2 操作中有任意一项不能完成，则应按照下面流程完成异常处理工作：

处于出错状态：可信计算模块启动后需要检查可信计算模块是否处于出错状态，如果在出错状态，则需要保存审计日志，并交由管理员处理错误。

初始化、自检：可信计算模块启动后需要执行初始化和主动自检工作，并保存审计日志。

度量 BIOS 关键代码：可信计算模块中的可信度量功能对可信计算平台 BIOS 关键代码主动进行完整性度量，保存度量日志。

认证绑定：可信计算模块启动后需要认证当前所在平台是否是上次可信计算平台绑定操作中被绑定的对象。如果不是，则给出出错信号，并保存审计日志。

保存失败类型：如果出现上述四种情况之一，则应保存失败类型及审计日志。

用户登录：失败信息保存后，需要提示用户登陆。

管理员登录：只有管理员登陆，才可以对失败信息进行处理。

计算机 CPU 执行 BIOS 代码：保存失败类型后，应响应计算机 CPU 读取 BIOS 代码的信号，并执行 BIOS 代码。可信计算模块也可以在此时关闭平台上的除鼠标/键盘/显示器以外的其它部件，进一步控制平台的启动环境。

显示失败信息：当计算机 CPU 执行 BIOS 代码后，应根据保存的失败类型，向用户显示失败类型信息。

异常处理操作：由管理员根据失败原因进行相应的异常处理操作。

禁用可信计算模块：当管理员不能及时对失败信息进行处理时，可以由管理员发出可信计算模块的功能禁用操作。功能禁用后，系统的启动流程不发生变化。

如果执行了可信计算模块禁用操作，则应给可信计算平台发出可信计算模块禁用信号。并通过执行 BIOS 代码显示给用户。

平台重启：管理员可以执行平台掉电、重新启动操作。

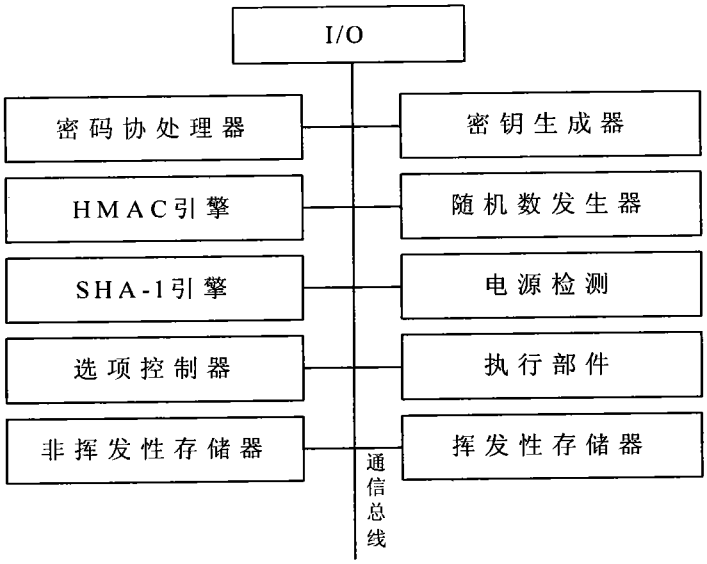

I/O
密码协处理器
HMAC引擎
SHA-1引擎
选项控制器
非挥发性存储器
密钥生成器
随机数发生器
电源检测
执行部件
挥发性存储器
通信总线

图 1

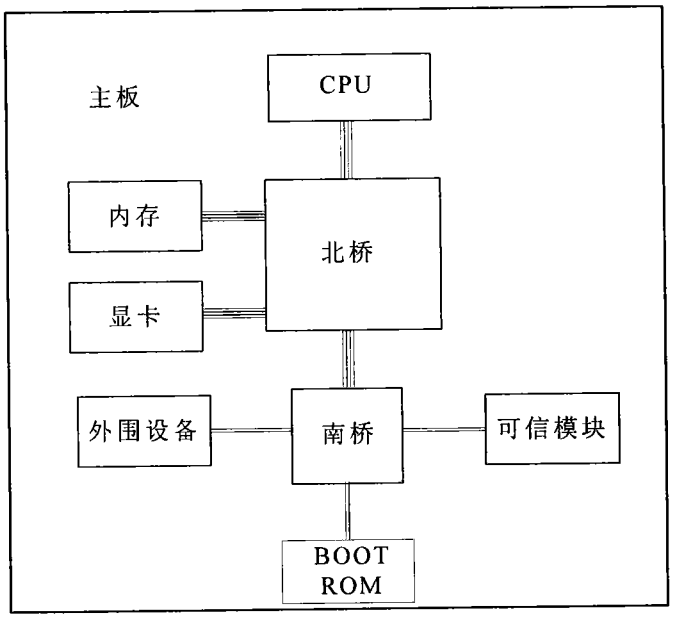

主板
CPU
内存
显卡
北桥
外围设备
南桥
可信模块
BOOT ROM

图 2

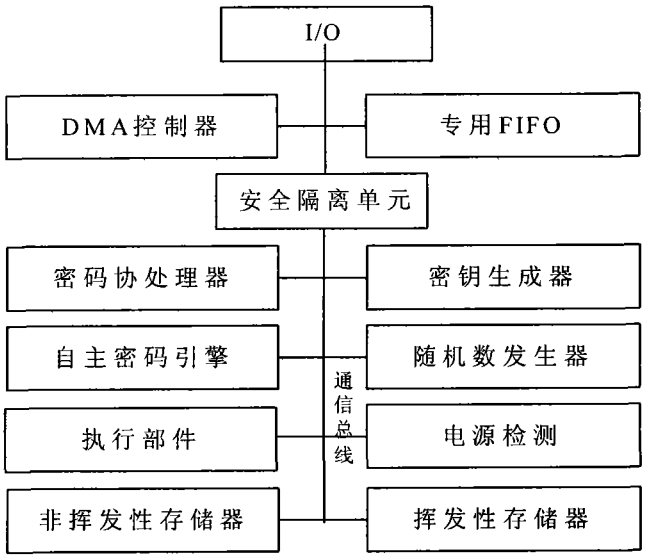

I/O
DMA控制器
专用FIFO
安全隔离单元
密码协处理器
密钥生成器
自主密码引擎
随机数发生器
通信总线
执行部件
电源检测
非挥发性存储器
挥发性存储器

图 3

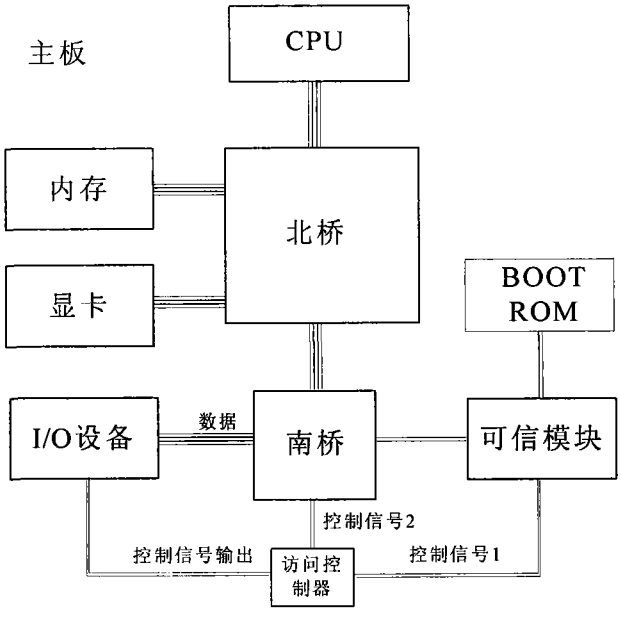

主板
CPU
内存
北桥
显卡
BOOT ROM
I/O设备
数据
南桥
可信模块
控制信号2
控制信号输出
访问控制器
控制信号1

图 4

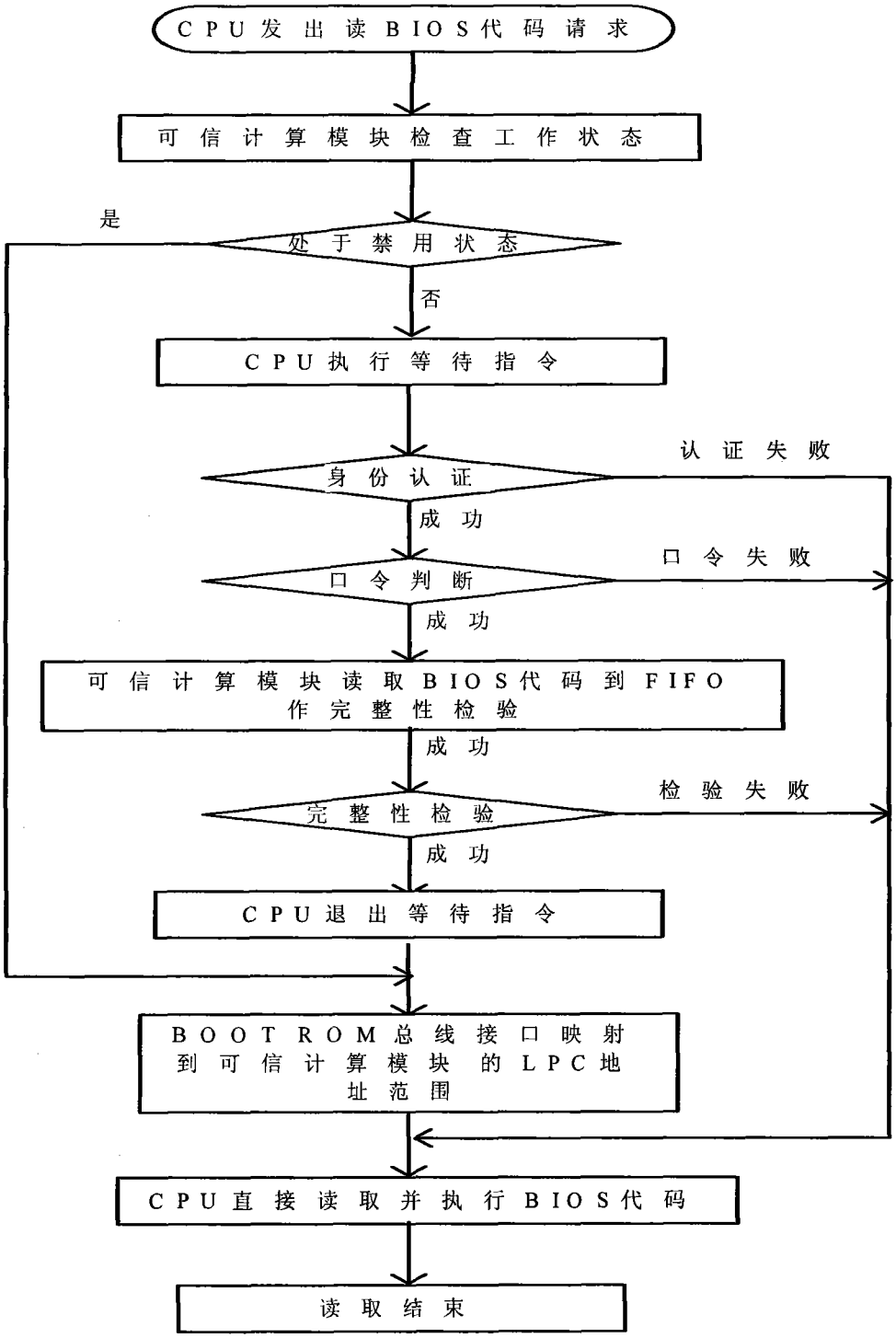

CPU发出读BIOS代码请求
可信计算模块检查工作状态
是
处于禁用状态
否
CPU执行等待指令
身份认证
认证失败
成功
口令判断
口令失败
成功
可信计算模块读取BIOS代码到FIFO作完整性检验
成功
完整性检验
检验失败
成功
CPU退出等待指令
BOOT ROM总线接口映射到可信计算模块的LPC地址范围
CPU直接读取并执行BIOS代码
读取结束

图 5

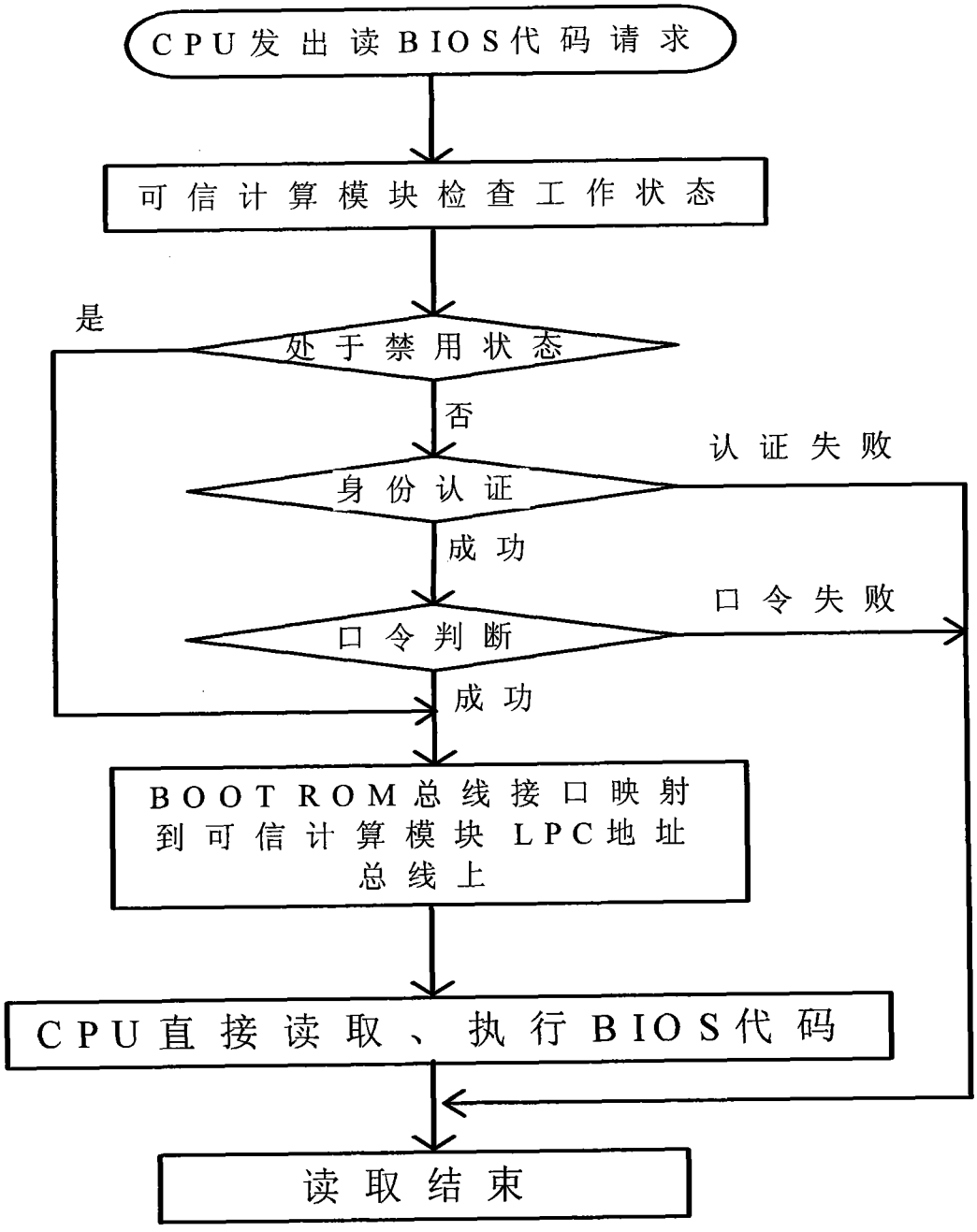

CPU发出读BIOS代码请求
可信计算模块检查工作状态
是
处于禁用状态
否
认证失败
身份认证
成功
口令失败
口令判断
成功
BOOT ROM总线接口映射到可信计算模块LPC地址总线上
CPU直接读取、执行BIOS代码
读取结束

图 6

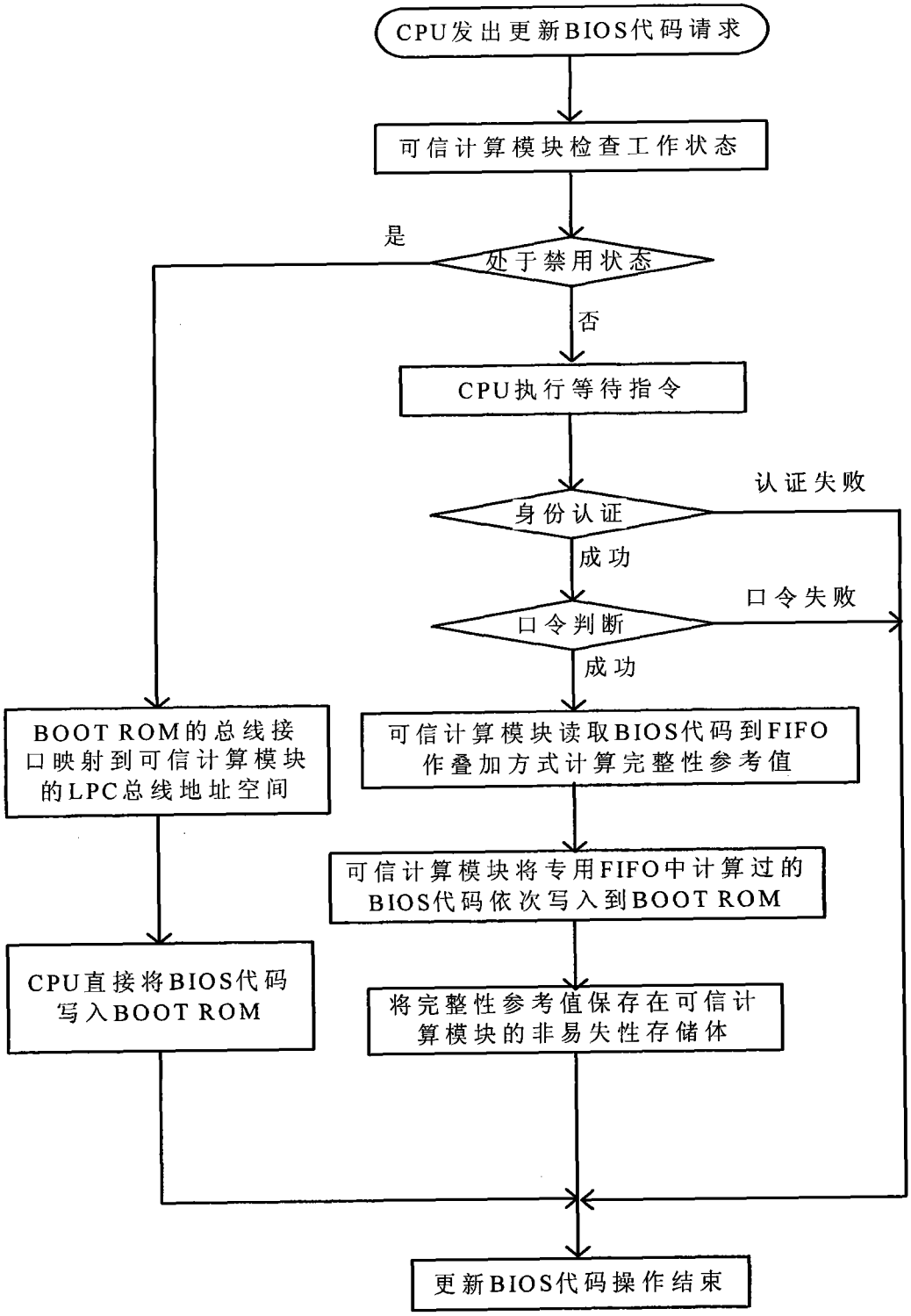

CPU发出更新BIOS代码请求
可信计算模块检查工作状态
是
处于禁用状态
否
CPU执行等待指令
认证失败
身份认证
成功
口令失败
口令判断
成功
BOOT ROM的总线接口映射到可信计算模块的LPC总线地址空间
可信计算模块读取BIOS代码到FIFO作叠加方式计算完整性参考值
可信计算模块将专用FIFO中计算过的BIOS代码依次写入到BOOT ROM
CPU直接将BIOS代码写入BOOT ROM
将完整性参考值保存在可信计算模块的非易失性存储体
更新BIOS代码操作结束

图 7

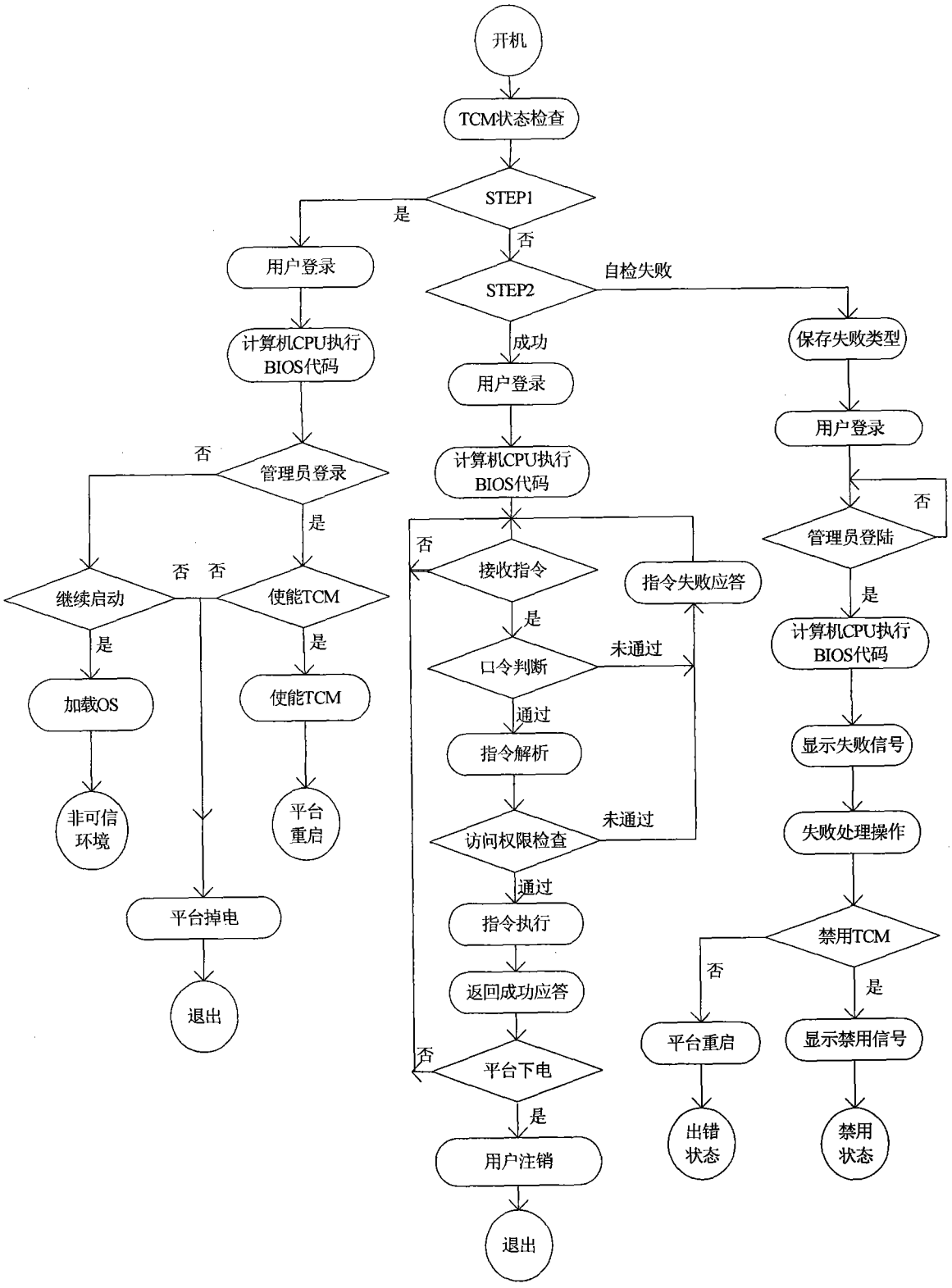

开机
TCM状态检查
STEP1
是
否
用户登录
计算机CPU执行BIOS代码
管理员登录
否
是
继续启动
否
否
使能TCM
是
是
加载OS
使能TCM
非可信环境
平台重启
平台掉电
退出
STEP2
自检失败
成功
用户登录
计算机CPU执行BIOS代码
否
接收指令
是
口令判断
未通过
通过
指令解析
访问权限检查
未通过
通过
指令执行
返回成功应答
否
平台下电
是
用户注销
退出
指令失败应答
保存失败类型
用户登录
否
管理员登陆
是
计算机CPU执行BIOS代码
显示失败信号
失败处理操作
禁用TCM
否
是
平台重启
显示禁用信号
出错状态
禁用状态

图 8