(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 110929283 A
(43)申请公布日 2020.03.27

(21)申请号 201911240731.2

(22)申请日 2019.12.06

(71)申请人 中电长城(长沙)信息技术有限公司
地址 410205 湖南省长沙市长沙高新开发区尖山路39号长沙中电软件园一期17号栋

(72)发明人 李攀峰 黄辉伟 欧阳泳

(74)专利代理机构 长沙市融智专利事务所(普通合伙) 43114
代理人 龚燕妮

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/44(2013.01)

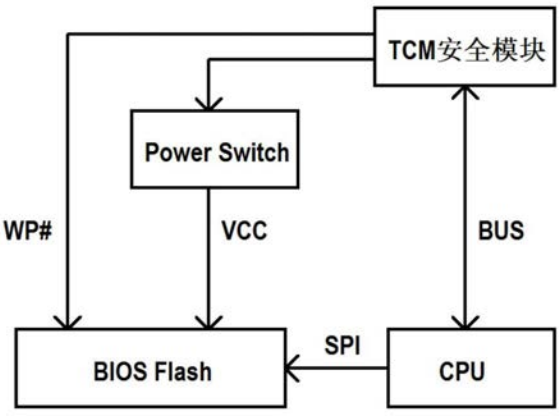
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种UEFI BIOS的分级保护系统和相应的实现方法

(57)摘要

本发明公开了一种UEFI BIOS的分级保护系统和相应的实现方法,其中方法包括:UEFI BIOS和TCM安全模块建立安全通道;UEFI BIOS在启动操作系统之前发送读写禁用命令给TCM安全模块,TCM安全模块将BIOS Flash芯片的写保护引脚和电源控制引脚的电平均拉低,使BIOS Flash芯片处于不可访问状态;UEFI BIOS启动到操作系统之后,仅UEFI BIOS能够通过UEFI BIOS内部API修改BIOS FLASH的访问权限,确保了除了UEFI BIOS之外的其他软件(包括操作系统)对BIOS FLASH都没有访问权限。本发明在满足UEFI规范的前提下,提高BIOS FLASH的安全性能。



CN 110929283 A

1.一种UEFI BIOS的分级保护系统,其特征在于,包括BIOS Flash芯片、CPU、TCM安全模块;

所述BIOS Flash芯片,用于存放UEFI BIOS代码;

所述CPU通过SPI总线与BIOS Flash芯片通信连接,用于执行UEFI BIOS代码的基本功能;

所述TCM安全模块,一方面与CPU通信连接,另一方面与BIOS Flash芯片的写保护引脚和BIOS Flash芯片的电源控制引脚连接,用于在CPU执行操作系统调用UEFI BIOS内部API以对BIOS FLASH芯片进行访问控制时,对UEFI BIOS所发送的访问权限命令进行安全验证,并在验证通过后,根据该访问权限命令对BIOS FLASH芯片的写保护引脚电平进行修改;还用于在接收到UEFIBIOS发送的读写禁用命令时,将BIOS Flash芯片的写保护引脚和电源控制引脚的电平均拉低,使BIOS Flash芯片处于不可访问状态;

其中,所述访问权限命令,是UEFI BIOS根据UEFI BIOS内部API对BIOS FLASH芯片进行访问控制的类型进行设置。

2.一种带分级保护机制的UEFI BIOS的实现方法,其特征在于,包括以下步骤:

UEFI BIOS和TCM安全模块,通过随机生成的传输密钥和公私钥对建立两者间的安全通道;

在CPU将UEFIBIOS启动到操作系统之前:UEFI BIOS发送读写禁用命令给TCM安全模块,TCM安全模块将BIOS Flash芯片的写保护引脚和电源控制引脚的电平均拉低,使BIOS Flash芯片处于不可访问状态;

在CPU将UEFIBIOS启动到操作系统之后,当操作系统调用UEFI BIOS内部API需要对BIOS FLASH芯片进行读写的访问控制时,包括以下步骤:

a1)UEFI BIOS根据UEFI BIOS内部的该API对BIOS FLASH芯片进行访问控制的类型设置访问权限命令;

a2)UEFI BIOS将访问权限命令通过所述安全通道发送给TCM安全模块;

a3)TCM安全模块对访问权限命令进行验证,并在验证通过后,根据访问权限命令对BIOS Flash芯片的写保护引脚和电源控制引脚的电平状态进行修改;

a4)当UEFIBIOS完成读写的访问控制任务后,UEFI BIOS发送读写禁用命令给TCM安全模块,TCM安全模块将BIOS Flash芯片的写保护引脚和电源控制引脚的电平均拉低,使BIOS Flash芯片处于不可访问状态。

3.根据权利要求2所述的方法,其特征在于,在步骤a3)中,根据访问权限命令对BIOS Flash芯片的写保护引脚和电源控制引脚的电平状态进行修改的具体方法为:

如果UEFI BIOS内部的该API对BIOS FLASH芯片进行访问控制的命令类型为只读,则设置访问权限命令为SPI_READ_ENABLE,此时TCM安全模块将BIOS Flash芯片的电源控制引脚电平拉高,将BIOS Flash芯片的写保护引脚拉低,BIOS Flash芯片为只读状态;

如果UEFI BIOS内部的该API对BIOS FLASH芯片进行访问控制的命令类型为可写,则设置访问权限命令为SPI_READ_WRITE_ENABLE,此时TCM安全模块将BIOS Flash芯片的电源控制引脚电平拉高,将BIOS Flash芯片的写保护引脚拉高,BIOS Flash芯片为可写状态。

4.根据权利要求2所述的方法,其特征在于,所述安全通道的建立方法为:

b1)TCM安全模块在生产环节时预置私钥SK,UEFI BIOS预置与TCM安全模块的私钥对应

的公钥SK.pub；

b2)主板启动后，UEFI BIOS初始化TCM安全模块的通信接口，并发送密钥请求命令给TCM安全模块；

b3)TCM安全模块接收密钥请求命令，并判断是否为上电后第一次收到该密钥请求命令：若是，则随机产生一个密钥AUTH_SK，并使用私钥SK对密钥AUTH_SK加密后作为密钥请求命令的返回值发送给UEFI BIOS；若否，则退出安全通道建立流程；

b4)UEFI BIOS收到密钥请求命令的返回值后，使用公钥SK.pub解密得到密钥AUTH_SK，并将该密钥放置于安全区域内，完成安全通道的建立。

5.根据权利要求2所述的方法，其特征在于，TCM安全模块对访问权限命令进行验证的方法为：

c1)设访问权限命令的格式为：command header+data1+data2，其中，command header是指访问权限命令的命令头，data1是指访问权限命令的命令内容，data2是使用AUTH_SK对data1进行加密得到的数据；

c2)当TCM安全模块接收到访问控制命令后，使用密钥AUTH_SK对接收到的访问控制命令中的data2'进行解密得到data1"，并与得到的接收到的访问控制命令中的data1'进行比较，如果相同，则为验证成功；否则验证失败，不改变BIOS Flash芯片的读写状态。

一种UEFI BIOS的分级保护系统和相应的实现方法

技术领域

[0001] 本发明属于计算机系统领域,具体是指一种UEFI BIOS的分级保护系统和相应的实现方法。

背景技术

[0002] 在大多数计算机平台上面,BIOS FLASH通过引脚WP#(write protect)挂载于SPI总线上面:当WP#被拉低时,BIOS FLASH被设置为只读;当WP#被拉高时,BIOS FLASH被设置为可写。因此挂载于SPI总线的BIOS FLASH,其读写方法是公开的,这就导致了BIOS具有以下几方面被攻击的风险问题:

[0003] 1、通过修改BIOS FLASH里面的内容来攻击整个系统:无论是直接破坏BIOS内容使系统无法正常启动,还是植入BIOS后门都会造成很大的破坏;

[0004] 2、对于实现了可信BIOS的平台,任何对于BIOS FLASH的非授权修改都会造成可信链的破坏,导致系统失去安全保护;

[0005] 3、可以随意读取BIOS的内容,分析BIOS里面的漏洞和秘密信息:因为业界大部分的BIOS的源码都由知名的几家BIOS提供商提供,同时UEFI规范也是公开的,所以这种威胁对于UEFI标准的BIOS来说是尤其不可忽略的。

[0006] 目前业界对BIOS FLASH的保护方法有如下几种:

[0007] 1、通过一个硬件的跳帽来控制BIOS FLASH的WP#:这种做法的缺点是当机器出厂后BIOS FLASH处于只读状态;而对基于UEFI标准的BIOS,要求BIOS即使在启动到OS之后也要有读写BIOS FLASH的权限。因此,这种方法虽然能解决上述第1种被攻击的风险问题,但不适用于UEFI BIOS的系统。

[0008] 2、通过一个GPIO(GPIO可以连接在芯片组,BMC等)控制BIOS FLASH的WP#:这种做法可以通过软件编程的方法控制BIOS FLASH的读写状态,比前一种保护方法灵活,但是GPIO的编程接口也是公开的,很容易被破解。

发明内容

[0009] 本发明所要解决的技术问题在于,提供一种UEFI BIOS的分级保护系统和相应的实现方法,可以在满足UEFI规范的前提下,提高BIOS FLASH的安全性能。

[0010] 为实现上述技术目的,本发明采用如下技术方案:

[0011] 一种UEFI BIOS的分级保护系统,包括BIOS Flash芯片、CPU、TCM安全模块;

[0012] 所述BIOS Flash芯片,用于存放UEFI BIOS代码;

[0013] 所述CPU通过SPI总线与BIOS Flash芯片通信连接,用于执行UEFI BIOS代码的基本功能;

[0014] 所述TCM安全模块,一方面与CPU通信连接,另一方面与BIOS Flash芯片的写保护引脚和BIOS Flash芯片的电源控制引脚连接,用于在CPU执行操作系统调用UEFI BIOS内部API以对BIOS FLASH芯片进行访问控制时,对UEFI BIOS所发送的访问权限命令进行安全验

证,并在验证通过后,根据该访问权限命令对BIOS FLASH芯片的写保护引脚电平进行修改;还用于在接收到UEFI BIOS发送的读写禁用命令时,将BIOS Flash芯片的写保护引脚和电源控制引脚的电平均拉低,使BIOS Flash芯片处于不可访问状态;

[0015] 其中,所述访问权限命令,是UEFI BIOS根据UEFI BIOS内部API对BIOS FLASH芯片进行访问控制的类型进行设置。

[0016] 本发明还提供一种带分级保护机制的UEFI BIOS的实现方法,包括以下步骤:

[0017] UEFI BIOS和TCM安全模块,通过随机生成的传输密钥和公私钥对建立两者间的安全通道;

[0018] 在CPU将UEFI BIOS启动到操作系统之前:UEFI BIOS发送读写禁用命令给TCM安全模块,TCM安全模块将BIOS Flash芯片的写保护引脚和电源控制引脚的电平均拉低,使BIOS Flash芯片处于不可访问状态;

[0019] 在CPU将UEFI BIOS启动到操作系统之后,当操作系统调用UEFI BIOS内部API需要对BIOS FLASH芯片进行读写的访问控制时,包括以下步骤:

[0020] a1)UEFI BIOS根据UEFI BIOS内部的该API对BIOS FLASH芯片进行访问控制的类型设置访问权限命令;

[0021] a2)UEFI BIOS将访问权限命令通过所述安全通道发送给TCM安全模块;

[0022] a3)TCM安全模块对访问权限命令进行验证,并在验证通过后,根据访问权限命令对BIOS Flash芯片的写保护引脚和电源控制引脚的电平状态进行修改;

[0023] a4)当UEFI BIOS完成读写的访问控制任务后,UEFI BIOS发送读写禁用命令给TCM安全模块,TCM安全模块将BIOS Flash芯片的写保护引脚和电源控制引脚的电平均拉低,使BIOS Flash芯片处于不可访问状态。

[0024] 进一步地,在步骤a3)中,根据访问权限命令对BIOS Flash芯片的写保护引脚和电源控制引脚的电平状态进行修改的具体方法为:

[0025] 如果UEFI BIOS内部的该API对BIOS FLASH芯片进行访问控制的命令类型为只读,则设置访问权限命令为SPI_READ_ENABLE,此时TCM安全模块将BIOS Flash芯片的电源控制引脚电平拉高,将BIOS Flash芯片的写保护引脚拉低,BIOS Flash芯片为只读状态;

[0026] 如果UEFI BIOS内部的该API对BIOS FLASH芯片进行访问控制的命令类型为可写,则设置访问权限命令为SPI_READ_WRITE_ENABLE,此时TCM安全模块将BIOS Flash芯片的电源控制引脚电平拉高,将BIOS Flash芯片的写保护引脚拉高,BIOS Flash芯片为可写状态。

[0027] 进一步地,所述安全通道的建立方法为:

[0028] b1)TCM安全模块在生产环节时预置私钥SK,UEFI BIOS预置与TCM安全模块的私钥对应的公钥SK.pub;

[0029] b2)主板启动后,UEFI BIOS初始化TCM安全模块的通信接口,并发送密钥请求命令给TCM安全模块;

[0030] b3)TCM安全模块接收密钥请求命令,并判断是否为上电后第一次收到该密钥请求命令:若是,则随机产生一个密钥AUTH_SK,并使用私钥SK对密钥AUTH_SK加密后作为密钥请求命令的返回值发送给UEFI BIOS;若否,则退出安全通道建立流程;

[0031] b4)UEFI BIOS收到密钥请求命令的返回值后,使用公钥SK.pub解密得到密钥AUTH_SK,并将该密钥放置于安全区域内,完成安全通道的建立。

[0032] 进一步地,TCM安全模块对访问权限命令进行验证的方法为:

[0033] c1)设访问权限命令的格式为:command header+data1+data2,其中,command header是指访问权限命令的命令头,data1是指访问权限命令的命令内容,data2是使用AUTH_SK对data1进行加密得到的数据;

[0034] c2)当TCM安全模块接收到访问控制命令后,使用密钥AUTH_SK对接收到的访问控制命令中的data2'进行解密得到data1",并与得到的接收到的访问控制命令中的data1'进行比较,如果相同,则为验证成功;否则验证失败,不改变BIOS Flash芯片的读写状态。

[0035] 有益效果

[0036] 本发明的有益效果为:

[0037] 1、在满足UEFI规范的前提下,提高BIOS FLASH的安全性能;

[0038] 2、对BIOS FLASH的读写权限的控制通过UEFI BIOS内部软件控制,不需要通过硬件跳帽的机制,比较灵活;同时这个控制权限由安全芯片保证安全;

[0039] 3、对BIOS FLASH的读权限也进行了控制。防止恶意软件通过分析BIOS FLASH内容来寻找漏洞;

[0040] 4、对UEFI BIOS需要的权限安照信息安全的最小化原则进行分级控制,把读写的权限单独控制,保证每个API只拥实现该API功能所需要的最小权限。而且在UEFI BIOS不需要使用SPI FLASH的时候,把SPI FLASH置于不可访问的状态,杜绝了黑客读取SPI FLASH里面内容进行分析和攻击。

附图说明

[0041] 图1为本发明实施例所述的系统架构图;

[0042] 图2为本发明实施例所述的BIOS FLASH的权限状态图;

[0043] 图3为本发明实施例所述建立安全通道的流程图。

具体实施方式

[0044] 本发明通过把BIOS FLASH的写保护引脚WP#和电源控制引脚VCC连接到一个安全芯片,由这个安全芯片通过控制VCC和WP#的电平状态,进而控制BIOS FLASH的读写状态,实现本发明可按照信息安全的最小化原则对BIOS FLASH的访问权限进行分级控制:级别一:无法访问,不可读不可写;级别二:可读,不可写;级别三:可读可写。

[0045] 下面对本发明的实施例作详细说明,本实施例以本发明的技术方案为依据开展,给出了详细的实施方式和具体的操作过程,对本发明的技术方案作进一步解释说明。

[0046] 实施例一提供一种UEFI BIOS的分级保护系统,如图1所示,包括BIOS Flash芯片、CPU、TCM安全模块;

[0047] 所述BIOS Flash芯片,用于存放UEFI BIOS代码;

[0048] 所述CPU通过SPI总线与BIOS Flash芯片通信连接,用于执行UEFI BIOS代码的基本功能;

[0049] 所述TCM安全模块,一方面与CPU通信连接,另一方面与BIOS Flash芯片的写保护引脚WP#和电源控制引脚VCC,用于在CPU执行操作系统调用UEFI BIOS内部API以对BIOS FLASH芯片进行访问控制时,对UEFI BIOS所发送的访问权限命令进行安全验证,并在验证

通过后,根据该访问权限命令对BIOS FLASH芯片的写保护引脚WP#和电源控制引脚VCC的电平进行修改,使BIOS Flash芯片处于可读状态或可读写状态;还用于在接收到UEFI BIOS发送的读写禁用命令时,将BIOS Flash芯片的写保护引脚和电源控制引脚的电平均拉低,使BIOS Flash芯片处于不可访问状态;在本实施例中,写保护引脚WP#为低电平有效;

[0050] 其中,所述访问权限命令,是UEFI BIOS根据UEFI BIOS内部API对BIOS FLASH芯片进行访问控制的类型进行设置。

[0051] 如图2所示的BIOS FLASH权限状态图,如果UEFI BIOS内部的该API对BIOS FLASH芯片进行访问控制的命令类型为只读,则设置访问权限命令为SPI_READ_ENABLE,此时TCM安全模块将BIOS Flash芯片的电源控制引脚电平拉高,将BIOS Flash芯片的写保护引脚拉低,BIOS Flash芯片为只读状态;

[0052] 如果UEFI BIOS内部的该API对BIOS FLASH芯片进行访问控制的命令类型为可写,则设置访问权限命令为SPI_READ_WRITE_ENABLE,此时TCM安全模块将BIOS Flash芯片的电源控制引脚电平拉高,将BIOS Flash芯片的写保护引脚拉高,BIOS Flash芯片为可写状态。

[0053] 本实施例,修改BIOS FLASH访问级别的API只能UEFI BIOS内部访问,可以确保其他外部代码无法通过这个API修改BIOS FLASH访问权限。而且,修改BIOS FLASH访问级别的UEFI BIOS内部API必须通过专门的认证方式开启和安全模块的安全通道之后,安全模块才会接受访问权限命令对BIOS FLASH的访问状态修改,可以确保只有这个UEFI BIOS内部的API能够控制BIOS FLASH访问级别,其他软件代码不能冒充这个API来控制BIOS FLASH访问权限。

[0054] 实施例二提供一种带分级保护机制的UEFI BIOS的实现方法,是在按上述实施例一提供的UEFI BIOS的分级保护系统进行通信连接,方法包括以下步骤:

[0055] UEFI BIOS和TCM安全模块,通过随机生成的传输密钥和公私钥对建立两者间的安全通道;

[0056] 在CPU将UEFI BIOS启动到操作系统之前:UEFI BIOS发送读写禁用命令给TCM安全模块,TCM安全模块将BIOS Flash芯片的写保护引脚和电源控制引脚的电平均拉低,使BIOS Flash芯片处于不可访问状态;

[0057] 在CPU将UEFI BIOS启动到操作系统之后,当操作系统调用UEFI BIOS内部API需要对BIOS FLASH芯片进行读写的访问控制时,包括以下步骤:

[0058] a1)UEFI BIOS根据UEFI BIOS内部的该API对BIOS FLASH芯片进行访问控制的类型设置访问权限命令。

[0059] a2)UEFI BIOS将访问权限命令通过所述安全通道发送给TCM安全模块;

[0060] 其中,如图3所示,安全通道的建立方法为:

[0061] b1)TCM安全模块在生产环节时预置私钥SK,UEFI BIOS预置与TCM安全模块的私钥对应的公钥SK.pub;

[0062] b2)主板启动后,UEFI BIOS初始化TCM安全模块的通信接口,并发送密钥请求命令给TCM安全模块;

[0063] 其中,主板启动可以理解为按下电脑的电源键开机,主板启动流程为:计算机硬件开始执行CPU和其他外设要求的上电时序;CPU上电时序完成后,CPU开始执行UEFI BIOS。另外,在本实施例中,密钥请求命令的具体名称为GET_SM_KEY命令,以下记载的GET_SM_KEY命

令即是指密钥请求命令；

[0064] b3)TCM安全模块接收GET_SM_KEY命令，并判断是否为上电后第一次收到该GET_SM_KEY命令：若是，则随机产生一个密钥AUTH_SK，并使用私钥SK对密钥AUTH_SK加密后作为GET_SM_KEY命令的返回值发送给UEFI BIOS；若否，则退出安全通道建立流程；

[0065] b4)UEFI BIOS收到GET_SM_KEY命令的返回值后，使用公钥SK.pub解密得到密钥AUTH_SK，并将该密钥放置于安全区域内，完成安全通道的建立。

[0066] a3)TCM安全模块对访问权限命令进行验证，并在验证通过后，根据访问权限命令对BIOS Flash芯片的写保护引脚和电源控制引脚的电平状态进行修改：

[0067] 如果UEFI BIOS内部的该API对BIOS FLASH芯片进行访问控制的命令类型为只读，则设置访问权限命令为SPI_READ_ENABLE，此时TCM安全模块将BIOS Flash芯片的电源控制引脚电平拉高，将BIOS Flash芯片的写保护引脚拉低，BIOS Flash芯片为只读状态；

[0068] 如果UEFI BIOS内部的该API对BIOS FLASH芯片进行访问控制的命令类型为可写，则设置访问权限命令为SPI_READ_WRITE_ENABLE，此时TCM安全模块将BIOS Flash芯片的电源控制引脚电平拉高，将BIOS Flash芯片的写保护引脚拉高，BIOS Flash芯片为可写状态。

[0069] 其中，TCM安全模块对访问权限命令进行验证的方法为：

[0070] c1)设访问权限命令的格式为：command header+data1+data2，其中，command header是指访问权限命令的命令头，data1是指访问权限命令的命令内容，data2是使用AUTH_SK对data1进行加密得到的数据；

[0071] c2)当TCM安全模块接收到访问控制命令后，使用密钥AUTH_SK对接收到的访问控制命令中的data2’进行解密得到data1”，并与得到的接收到的访问控制命令中的data1’进行比较，如果相同，则为验证成功；否则验证失败，不改变BIOS Flash芯片的读写状态。

[0072] a4)当UEFI BIOS完成读写的访问控制任务后，UEFI BIOS发送读写禁用命令给TCM安全模块，TCM安全模块将BIOS Flash芯片的写保护引脚和电源控制引脚的电平均拉低，使BIOS Flash芯片处于不可访问状态。

[0073] 以上实施例为本申请的优选实施例，本领域的普通技术人员还可以在此基础上进行各种变换或改进，在不脱离本申请总的构思的前提下，这些变换或改进都应当属于本申请要求保护的范围之内。

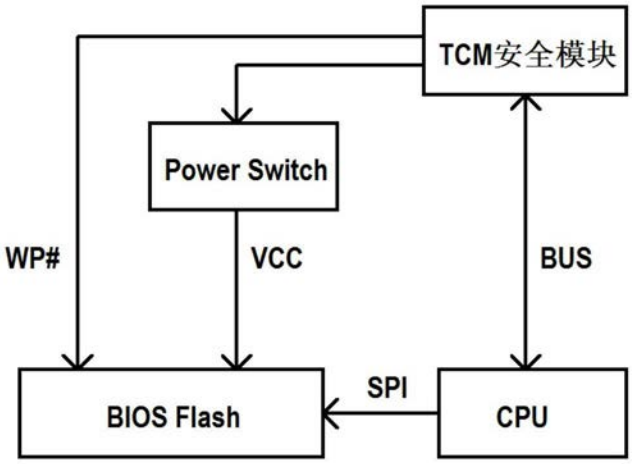

TCM安全模块
Power Switch
WP#
VCC
BUS
SPI
BIOS Flash
CPU

图1

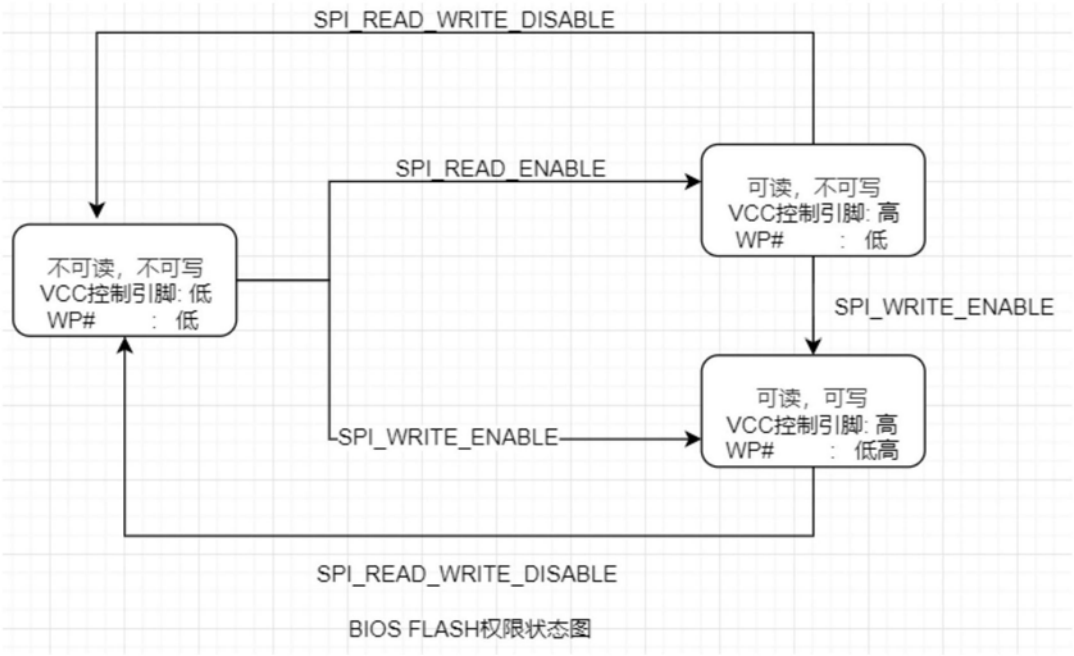

SPI_READ_WRITE_DISABLE
SPI_READ_ENABLE
可读，不可写
VCC控制引脚: 高
WP# : 低
不可读，不可写
VCC控制引脚: 低
WP# : 低
SPI_WRITE_ENABLE
可读，可写
VCC控制引脚: 高
WP# : 低高
SPI_WRITE_ENABLE
SPI_READ_WRITE_DISABLE
BIOS FLASH权限状态图

图2

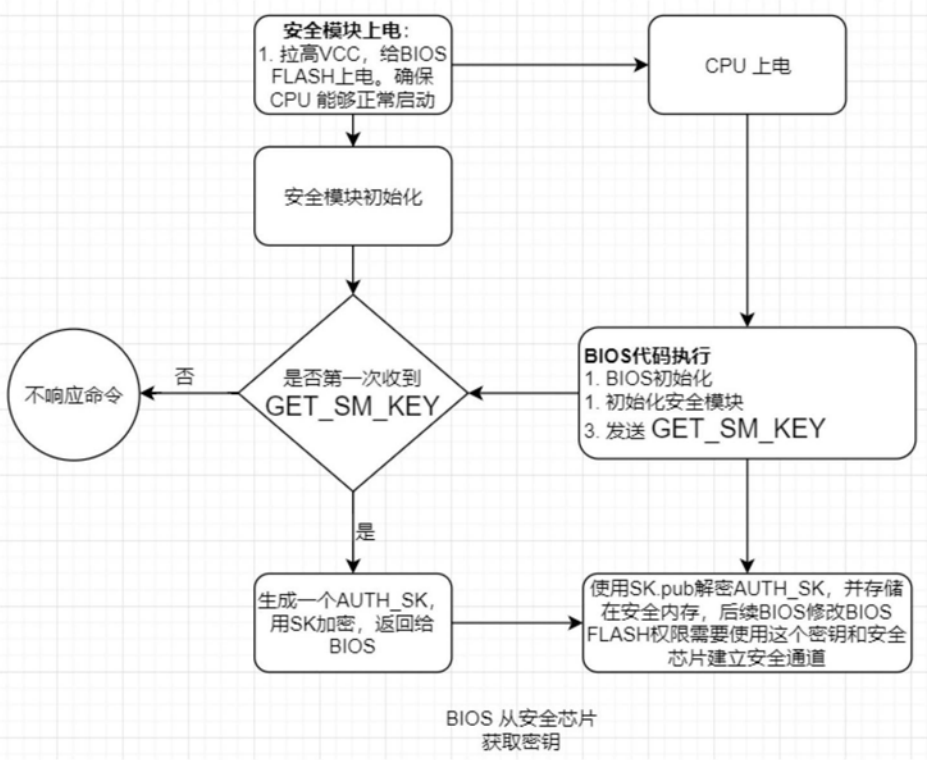

安全模块上电：
1. 拉高VCC，给BIOS FLASH上电。确保CPU 能够正常启动
CPU 上电
安全模块初始化
BIOS代码执行
1. BIOS初始化
1. 初始化安全模块
3. 发送 GET_SM_KEY
是否第一次收到 GET_SM_KEY
否
不响应命令
是
生成一个AUTH_SK，用SK加密，返回给BIOS
使用SK.pub解密AUTH_SK，并存储在安全内存，后续BIOS修改BIOS FLASH权限需要使用这个密钥和安全芯片建立安全通道
BIOS 从安全芯片获取密钥

图3