(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 106991299 A
(43)申请公布日 2017.07.28

(21)申请号 201710313173.2

(22)申请日 2017.05.05

(71)申请人 济南浪潮高新科技投资发展有限公司
地址 250100 山东省济南市高新区孙村镇科航路2877号研发楼一楼

(72)发明人 李清石 金长新 刘强

(74)专利代理机构 济南信达专利事务所有限公司 37100
代理人 孟峣

(51)Int.Cl.
G06F 21/12(2013.01)
G06F 21/45(2013.01)
G06F 21/60(2013.01)

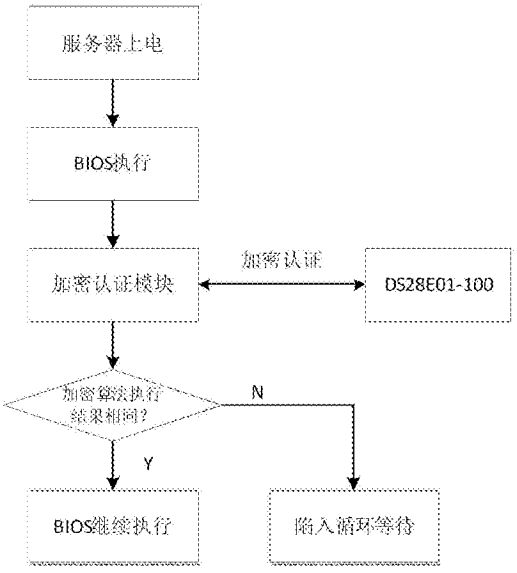
权利要求书1页 说明书3页 附图2页

(54)发明名称

一种加密认证模块及基于该模块的BIOS固件保护方法

(57)摘要

本发明公开了一种加密认证模块及基于该模块的BIOS固件保护方法，其实现过程为，在BIOS中添加一个工作在驱动执行环境DXE阶段的加密认证模块，此加密认证模块是一个DXE Driver，通过GPIO模拟1-Wire总线时序访问实现加密认证功能，对BIOS固件进行保护。本发明的一种加密认证模块及基于该模块的BIOS固件保护方法与现有技术相比，只需对现有硬件方案增加很少的器件便可对BIOS固件实现有效的保护，避免BIOS固件被非法窃取，实用性强，适用范围广泛，易于推广。



CN 106991299 A

1.一种加密认证模块，其特征在于，添加在BIOS中，应用于驱动执行环境DXE阶段，包括，

接口单元，在系统上电后接收BIOS的启动消息及认证请求，并通过模拟对应接口来访问加密芯片；

加密认证单元，通过配合加密芯片，实现加密认证功能；

比较单元，比较加密认证单元的加密结果与加密芯片的加密结果相同，则认证成功，不相同则认证失败。

2.根据权利要求1所述的一种加密认证模块，其特征在于，所述接口单元通过GPIO模拟1-Wire总线时序访问加密芯片，实现加密认证功能，对BIOS固件进行保护。

3.根据权利要求1或2所述的一种加密认证模块，其特征在于，在加密认证单元中，通过脚本执行SHA-1加密算法进行加密，同时加密芯片响应认证请求并通过与加密认证单元相同的密钥执行SHA-1加密算法进行加密。

4.根据权利要求3所述的一种加密认证模块，其特征在于，在比较单元中，当加密认证单元的SHA-1加密算法的执行结果与加密芯片的SHA-1加密算法的执行结果相同则认证成功，否则认证失败。

5.一种基于加密认证模块的BIOS固件保护方法，其特征在于，其实现过程为，在BIOS中添加一个工作在驱动执行环境DXE阶段的加密认证模块，此加密认证模块是一个DXE Driver，通过GPIO模拟1-Wire总线时序访问实现加密认证功能，对BIOS固件进行保护。

6.根据权利要求5所述的一种基于加密认证模块的BIOS固件保护方法，其特征在于，其具体实现步骤为，

一、系统上电，BIOS启动并执行加密认证模块；

二、加密认证模块发起加密认证过程；

三、如果认证通过，BIOS继续执行后续代码完成系统的引导启动；

四、如果认证未通过，BIOS启动CPU循环等待，系统启动过程无法进行。

7.根据权利要求6所述的一种基于加密认证模块的BIOS固件保护方法，其特征在于，在步骤二中，加密认证模块的加密认证单元通过脚本执行SHA-1加密算法进行加密，同时加密芯片响应认证请求并通过与加密认证单元相同的密钥执行SHA-1加密算法进行加密。

8.根据权利要求7所述的一种基于加密认证模块的BIOS固件保护方法，其特征在于，在步骤四中，通过加密认证模块的比较单元，当加密认证单元的SHA-1加密算法的执行结果与加密芯片的SHA-1加密算法的执行结果相同则认证成功，否则认证失败。

一种加密认证模块及基于该模块的BIOS固件保护方法

技术领域

[0001] 本发明涉及计算机服务器技术领域，具体地说是一种加密认证模块及基于该模块的BIOS固件保护方法。

背景技术

[0002] BIOS是服务器系统中的重要组成部分，体现了一个服务器厂商的竞争力。市场中大量部署的是四路双路等中低端服务器，这类产品差异不大，导致一个厂家生产的服务器上的BIOS在另一个厂家生产的服务器上可以不经修改直接运行，这对服务器厂商的知识产权保护和企业利益不利。如何简单有效地保护BIOS固件不被非法窃取是需要解决的重要问题。基于此，现提供一种加密认证模块及基于该模块的BIOS固件保护方法。

发明内容

[0003] 本发明的技术任务是针对以上不足之处，提供一种加密认证模块及基于该模块的BIOS固件保护方法。

[0004] 本发明是一种加密认证模块，添加在BIOS中，应用于驱动执行环境DXE阶段，包括，

接口单元，在系统上电后接收BIOS的启动消息及认证请求，并通过模拟对应接口来访问加密芯片；

加密认证单元，通过配合加密芯片，实现加密认证功能；

比较单元，比较加密认证单元的加密结果与加密芯片的加密结果相同，则认证成功，不相同则认证失败。

[0005] 所述接口单元通过GPIO模拟1-Wire总线时序访问加密芯片，实现加密认证功能，对BIOS固件进行保护。

[0006] 在加密认证单元中，通过脚本执行SHA-1加密算法进行加密，同时加密芯片响应认证请求并通过与加密认证单元相同的密钥执行SHA-1加密算法进行加密。

[0007] 在比较单元中，当加密认证单元的SHA-1加密算法的执行结果与加密芯片的SHA-1加密算法的执行结果相同则认证成功，否则认证失败。

[0008] 一种基于加密认证模块的BIOS固件保护方法，其实现过程为，在BIOS中添加一个工作在驱动执行环境DXE阶段的加密认证模块，此加密认证模块是一个DXE Driver，通过GPIO模拟1-Wire总线时序访问实现加密认证功能，对BIOS固件进行保护。

[0009] 其具体实现步骤为，

一、系统上电，BIOS启动并执行加密认证模块；

二、加密认证模块发起加密认证过程；

三、如果认证通过，BIOS继续执行后续代码完成系统的引导启动；

四、如果认证未通过，BIOS启动CPU循环等待，系统启动过程无法进行。

[0010] 在步骤二中，加密认证模块的加密认证单元通过脚本执行SHA-1加密算法进行加密，同时加密芯片响应认证请求并通过与加密认证单元相同的密钥执行SHA-1加密算法进

行加密。

[0011] 在步骤四中，通过加密认证模块的比较单元，当加密认证单元的SHA-1加密算法的执行结果与加密芯片的SHA-1加密算法的执行结果相同则认证成功，否则认证失败。

[0012] 本发明的一种加密认证模块及基于该模块的BIOS固件保护方法和现有技术相比，具有以下有益效果：

本发明的一种加密认证模块及基于该模块的BIOS固件保护方法，通过GPIO模拟1-Wire总线时序访问加密芯片实现加密认证功能，对BIOS固件进行保护；只需对现有硬件方案增加很少的器件便可对BIOS固件实现有效的保护，避免BIOS固件被非法窃取，实用性强，适用范围广泛，易于推广。

附图说明

[0013] 附图1为本发明设备的结构示意图。

[0014] 附图2为本发明方法的结构示意图。

具体实施方式

[0015] 下面结合附图及具体实施例对本发明作进一步说明。

[0016] 如附图1所示，本发明提供一种加密认证模块，添加在BIOS中，应用于驱动执行环境DXE阶段，包括，

接口单元，在系统上电后接收BIOS的启动消息及认证请求，并通过模拟对应接口来访问加密芯片；

加密认证单元，通过配合加密芯片，实现加密认证功能；

比较单元，比较加密认证单元的加密结果与加密芯片的加密结果相同，则认证成功，不相同则认证失败。

[0017] 所述接口单元通过GPIO模拟1-Wire总线时序访问加密芯片，实现加密认证功能，对BIOS固件进行保护。

[0018] 在加密认证单元中，通过脚本执行SHA-1加密算法进行加密，同时加密芯片响应认证请求并通过与加密认证单元相同的密钥执行SHA-1加密算法进行加密。

[0019] 在比较单元中，当加密认证单元的SHA-1加密算法的执行结果与加密芯片的SHA-1加密算法的执行结果相同则认证成功，否则认证失败。

[0020] 如附图2所示，一种基于加密认证模块的BIOS固件保护方法，其实现过程为，在BIOS中添加一个工作在DXE(Driver Execution Environment，驱动执行环境)阶段的加密认证模块，此加密认证模块是一个DXE Driver，通过GPIO模拟1-Wire总线时序访问实现加密认证功能，对BIOS固件进行保护。

[0021] 在UEFIBIOS的实现中，DXE Driver是DXE阶段所要执行的众多模块的一个统称，DXE Driver被DXE Core所读取，用来做各种硬件的初始化，产生Protocol和其他Service，比如实现网络ARP功能的ArpDxe、实现网络DHCP功能的Dhcp4Dxe、实现USB功能的EhciDxe等。本发明需要访问加密芯片，需要操作硬件，因此放入DXE阶段执行，类似于一个Driver，除了可以实现加密功能，还可以将相关访问接口实现为Protocol和Service，以供其他模块使用。

[0022] 其具体实现步骤为，

一、系统上电，BIOS启动并执行加密认证模块；

二、加密认证模块发起加密认证过程；

三、如果认证通过，BIOS继续执行后续代码完成系统的引导启动；

四、如果认证未通过，BIOS启动CPU循环等待，系统启动过程无法进行。

[0023] 在步骤二中，加密认证模块的加密认证单元通过脚本执行SHA-1加密算法进行加密，同时加密芯片响应认证请求并通过与加密认证单元相同的密钥执行SHA-1加密算法进行加密。

[0024] 在步骤四中，通过加密认证模块的比较单元，当加密认证单元的SHA-1加密算法的执行结果与加密芯片的SHA-1加密算法的执行结果相同则认证成功，否则认证失败。

[0025] 所述加密芯片采用DS28E01-100，基于此，本发明即为通过操作一个GPIO模拟1-Wire总线时序访问DS28E01-100加密芯片实现加密认证功能。

[0026] 所述的加密认证模块是一个DXE Driver，GPIO此时已可用，DXE Driver操作一个GPIO模拟1-Wire总线时序向DS28E01-100加密芯片发起加密认证请求，并通过软件方式基于DXE Driver中硬编码的密钥执行SHA-1加密算法，加密芯片响应此认证请求通过硬件方式基于加密芯片已写入的与DXE Driver中硬编码的密钥相同的密钥执行SHA-1加密算法。若DXE Driver软件SHA-1加密算法的执行结果与加密芯片硬件SHA-1加密算法的执行结果相同则认证成功。

[0027] 下面给出一个实施例：

有服务器主板一块，PCH(Platform Controller Hub)的一个GPIO上挂接DS28E01-100。BIOS固件放置在SPI Flash中，通过SPI接口挂接在PCH上。

[0028] 服务器上电，BIOS执行加密认证模块，此DXE Driver的主要功能是通过GPIO模拟1-Wire总线时序和发送加密认证请求并通过软件方式执行SHA-1加密算法，通过对比软件SHA-1加密算法的执行结果与加密芯片硬件SHA-1加密算法的执行结果判断BIOS是继续执行还是使CPU进入循环等待状态。

[0029] 设想BIOS固件被窃取，除非窃取者知道SHA-1加密算法的系统公共密钥，否则BIOS执行时CPU会被锁住，系统无法完成启动过程，这样就起到了保护BIOS固件的作用，从其他厂家服务器产品的SPI Flash中读取到的BIOS固件因为不能通过加密认证操作便不能被应用到其他板卡。

[0030] 通过上面具体实施方式，所述技术领域的技术人员可容易的实现本发明。但是应当理解，本发明并不限于上述的具体实施方式。在公开的实施方式的基础上，所述技术领域的技术人员可任意组合不同的技术特征，从而实现不同的技术方案。

[0031] 除说明书所述的技术特征外，均为本专业技术人员的已知技术。

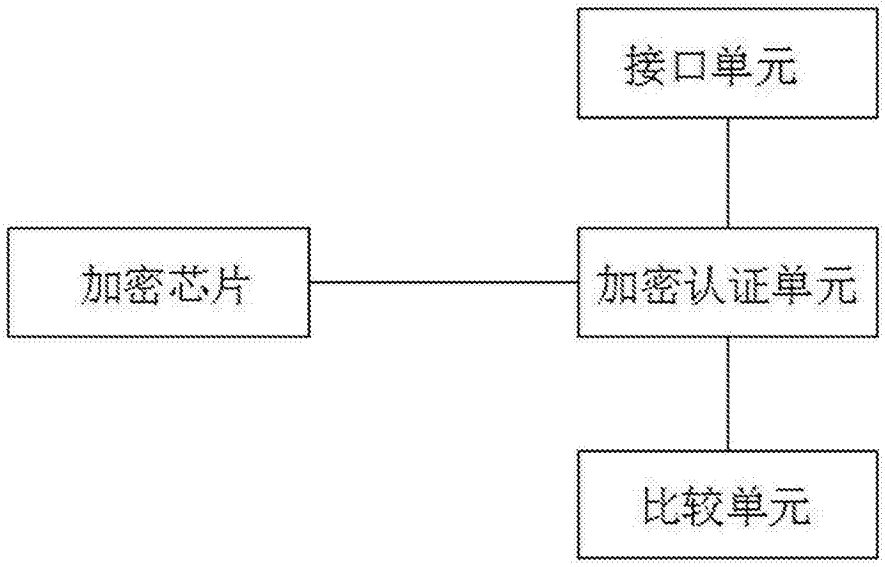


图1

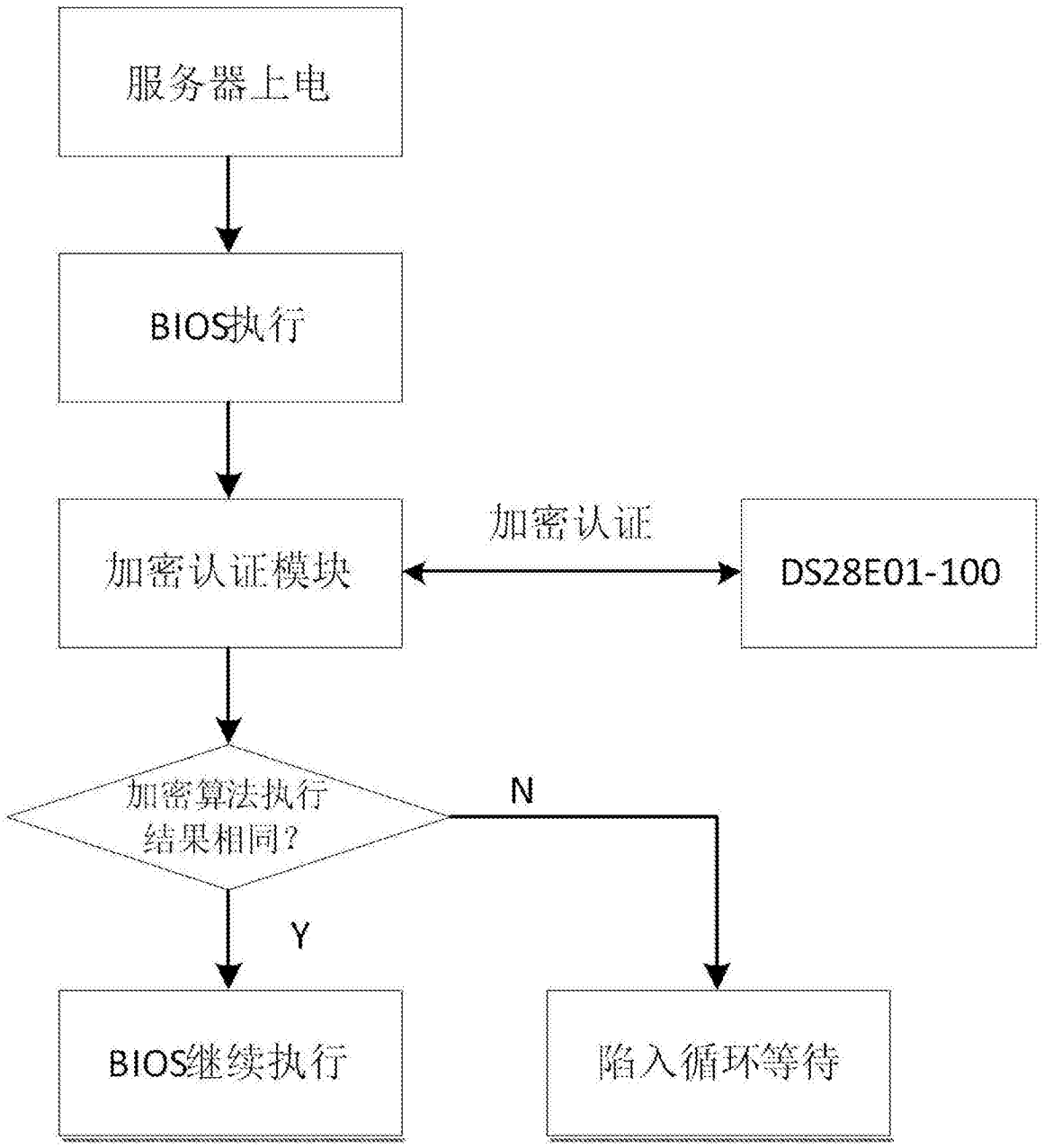

服务器上电
BIOS执行
加密认证模块
加密认证
DS28E01-100
加密算法执行
结果相同?
N
Y
BIOS继续执行
陷入循环等待

图2