(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 110018841 A
(43)申请公布日 2019.07.16

(21)申请号 201910300459.6

(22)申请日 2019.04.15

(71)申请人 苏州浪潮智能科技有限公司
地址 215100 江苏省苏州市吴中区吴中经济开发区郭巷街道官浦路1号9幢

(72)发明人 刘平

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 罗满

(51)Int.Cl.
G06F 8/654(2018.01)

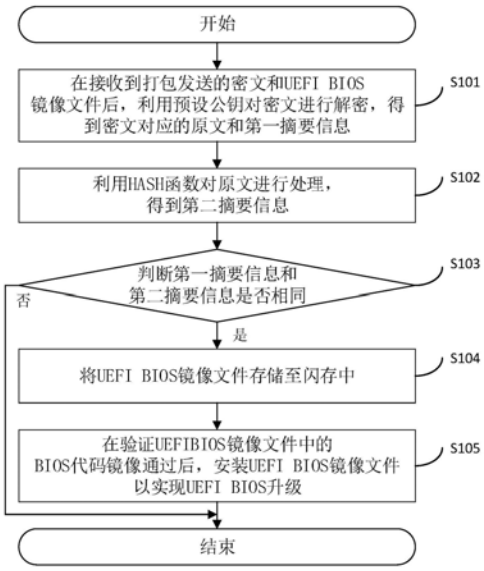
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种UEFI BIOS升级方法、系统及相关装置

(57)摘要

本申请所提供的一种UEFI BIOS升级方法，包括：在接收到打包发送的密文和UEFI BIOS镜像文件后，利用预设公钥对密文进行解密，得到密文对应的原文和第一摘要信息；利用HASH函数对原文进行处理，得到第二摘要信息；判断第一摘要信息和第二摘要信息是否相同；若是，则将UEFI BIOS镜像文件存储至闪存中；在验证UEFI BIOS镜像文件中的BIOS代码镜像通过后，安装UEFI BIOS镜像文件以实现UEFI BIOS升级。该方法判断第一摘要信息和第二摘要信息是否相同；若是，则认定该UEFI BIOS镜像文件是可信的，最终安装该UEFI BIOS镜像文件以实现UEFI BIOS升级，由于该UEFI BIOS镜像文件是可信的，避免给服务器带来很大的安全问题。本申请还提供一种UEFI BIOS升级系统、设备及计算机可读存储介质，均具有上述有益效果。



CN 110018841 A

1.一种UEFI BIOS升级方法,其特征在于,包括:

在接收到打包发送的密文和UEFI BIOS镜像文件后,利用预设公钥对所述密文进行解密,得到所述密文对应的原文和第一摘要信息;

利用HASH函数对所述原文进行处理,得到第二摘要信息;

判断所述第一摘要信息和所述第二摘要信息是否相同;

若是,则将所述UEFI BIOS镜像文件存储至闪存中;

在验证所述UEFI BIOS镜像文件中的BIOS代码镜像通过后,安装所述UEFI BIOS镜像文件以实现UEFI BIOS升级。

2.根据权利要求1所述的UEFI BIOS升级方法,其特征在于,所述在验证所述UEFI BIOS镜像文件中的BIOS代码镜像通过后,安装所述UEFI BIOS镜像文件以实现UEFI BIOS升级,包括:

利用所述UEFI BIOS镜像文件中的验证组件验证所述BIOS代码镜像是否通过;

若验证所述BIOS代码镜像通过,则安装所述UEFI BIOS镜像文件以实现所述UEFI BIOS升级。

3.根据权利要求2所述的UEFI BIOS升级方法,其特征在于,若验证所述BIOS代码镜像不通过,包括:

验证并刷新预先存储在SP中的可信UEFI BIOS镜像文件。

4.根据权利要求1所述的UEFI BIOS升级方法,其特征在于,所述在接收到打包发送的密文和UEFI BIOS镜像文件后,利用预设公钥对所述密文进行解密,得到所述密文对应的原文和第一摘要信息,包括:

接收使用数字签名技术加密的所述密文和所述UEFI BIOS镜像文件;

利用所述预设公钥对所述密文进行解密,得到所述密文对应的原文和第一摘要信息。

5.一种UEFI BIOS升级系统,其特征在于,包括:

解密模块,用于在接收到打包发送的密文和UEFI BIOS镜像文件后,利用预设公钥对所述密文进行解密,得到所述密文对应的原文和第一摘要信息;

原文处理模块,用于利用HASH函数对所述原文进行处理,得到第二摘要信息;

摘要信息判断模块,用于判断所述第一摘要信息和所述第二摘要信息是否相同;

存储模块,用于若所述第一摘要信息和所述第二摘要信息相同,则将所述UEFI BIOS镜像文件存储至闪存中;

镜像文件安装模块,用于在验证所述UEFI BIOS镜像文件中的BIOS代码镜像通过后,安装所述UEFI BIOS镜像文件以实现UEFI BIOS升级。

6.根据权利要求5所述的UEFI BIOS升级系统,其特征在于,所述镜像文件安装模块,包括:

验证单元,用于利用所述UEFI BIOS镜像文件中的验证组件验证所述BIOS代码镜像是否通过;

镜像文件安装单元,用于若验证所述BIOS代码镜像通过,则安装所述UEFI BIOS镜像文件以实现所述UEFI BIOS升级。

7.根据权利要求6所述的UEFI BIOS升级系统,其特征在于,所述镜像文件安装模块,包括:

验证刷新单元，用于若验证所述BIOS代码镜像不通过，则验证并刷新预先存储在SP中的可信UEFI BIOS镜像文件。

8.根据权利要求5所述的UEFI BIOS升级系统，其特征在于，所述解密模块，包括：

接收单元，用于接收使用数字签名技术加密的所述密文和所述UEFI BIOS镜像文件；

解密单元，用于利用所述预设公钥对所述密文进行解密，得到所述密文对应的原文和第一摘要信息。

9.一种设备，其特征在于，包括：

存储器和处理器；其中，所述存储器用于存储计算机程序，所述处理器用于执行所述计算机程序时实现如权利要求1至4任一项所述的UEFI BIOS升级方法的步骤。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求1至4任一项所述的UEFI BIOS升级方法的步骤。

一种UEFI BIOS升级方法、系统及相关装置

技术领域

[0001] 本申请涉及UEFI BIOS升级技术领域，特别涉及一种UEFI BIOS升级方法、系统、设备及计算机可读存储介质。

背景技术

[0002] UEFI是统一可扩展固件接口规范，连接着操作系统和平台固件，为操作系统启动前的运行状态提供了标准的环境。与传统BIOS(Basic Input Output System，基本输入输出系统)相比，UEFI采用了全新的启动流程，虽然解决了传统BIOS的很多问题，具有启动更快、扩展性更好的优点，但UEFI也存在一些安全缺陷。UEFI BIOS通常是由原始的制造商OEM和独立BIOS供应商合作开发的，以售卖商品的形式分发出去。由于各种原因修补BUG是必需的，兼容新硬件、打补丁等各种目的来更新UEFI BIOS。因UEFI BIOS的独特性，以及它在计算机系统中特殊的作用使得由恶意的程序对UEFI BIOS进行的未经授权的更改很可能对计算机系统造成巨大的威胁，因此需要对UEFI BIOS进行安全升级。目前，相关技术中对UEFI BIOS进行升级时无法保证用于升级的UEFI BIOS镜像文件是可信的，导致给服务器带来很大的安全问题。

[0003] 因此，如何保证用于UEFI BIOS升级的UEFI BIOS镜像文件是可信的，进而避免给服务器带来很大的安全问题是本领域技术人员亟需解决的技术问题。

发明内容

[0004] 本申请的目的是提供一种UEFI BIOS升级方法、系统、设备及计算机可读存储介质，能够保证用于UEFI BIOS升级的UEFI BIOS镜像文件是可信的，进而避免给服务器带来很大的安全问题。

[0005] 为解决上述技术问题，本申请提供一种UEFI BIOS升级方法，包括：

[0006] 在接收到打包发送的密文和UEFI BIOS镜像文件后，利用预设公钥对所述密文进行解密，得到所述密文对应的原文和第一摘要信息；

[0007] 利用HASH函数对所述原文进行处理，得到第二摘要信息；

[0008] 判断所述第一摘要信息和所述第二摘要信息是否相同；

[0009] 若是，则将所述UEFI BIOS镜像文件存储至闪存中；

[0010] 在验证所述UEFI BIOS镜像文件中的BIOS代码镜像通过后，安装所述UEFI BIOS镜像文件以实现UEFI BIOS升级。

[0011] 优选地，所述在验证所述UEFI BIOS镜像文件中的BIOS代码镜像通过后，安装所述UEFI BIOS镜像文件以实现UEFI BIOS升级，包括：

[0012] 利用所述UEFI BIOS镜像文件中的验证组件验证所述BIOS代码镜像是否通过；

[0013] 若验证所述BIOS代码镜像通过，则安装所述UEFI BIOS镜像文件以实现所述UEFI BIOS升级。

[0014] 优选地，若验证所述BIOS代码镜像不通过，包括：

[0015] 验证并刷新预先存储在SP中的可信UEFI BIOS镜像文件。

[0016] 优选地，所述在接收到打包发送的密文和UEFI BIOS镜像文件后，利用预设公钥对所述密文进行解密，得到所述密文对应的原文和第一摘要信息，包括：

[0017] 接收使用数字签名技术加密的所述密文和所述UEFI BIOS镜像文件；

[0018] 利用所述预设公钥对所述密文进行解密，得到所述密文对应的原文和第一摘要信息。

[0019] 本申请还提供一种UEFI BIOS升级系统，包括：

[0020] 解密模块，用于在接收到打包发送的密文和UEFI BIOS镜像文件后，利用预设公钥对所述密文进行解密，得到所述密文对应的原文和第一摘要信息；

[0021] 原文处理模块，用于利用HASH函数对所述原文进行处理，得到第二摘要信息；

[0022] 摘要信息判断模块，用于判断所述第一摘要信息和所述第二摘要信息是否相同；

[0023] 存储模块，用于若所述第一摘要信息和所述第二摘要信息相同，则将所述UEFI BIOS镜像文件存储至闪存中；

[0024] 镜像文件安装模块，用于在验证所述UEFI BIOS镜像文件中的BIOS代码镜像通过后，安装所述UEFI BIOS镜像文件以实现UEFI BIOS升级。

[0025] 优选地，所述镜像文件安装模块，包括：

[0026] 验证单元，用于利用所述UEFI BIOS镜像文件中的验证组件验证所述BIOS代码镜像是否通过；

[0027] 镜像文件安装单元，用于若验证所述BIOS代码镜像通过，则安装所述UEFI BIOS镜像文件以实现所述UEFI BIOS升级。

[0028] 优选地，所述镜像文件安装模块，包括：

[0029] 验证刷新单元，用于若验证所述BIOS代码镜像不通过，则验证并刷新预先存储在SP中的可信UEFI BIOS镜像文件。

[0030] 优选地，所述解密模块，包括：

[0031] 接收单元，用于接收使用数字签名技术加密的所述密文和所述UEFI BIOS镜像文件；

[0032] 解密单元，用于利用所述预设公钥对所述密文进行解密，得到所述密文对应的原文和第一摘要信息。

[0033] 本申请还提供一种设备，包括：

[0034] 存储器和处理器；其中，所述存储器用于存储计算机程序，所述处理器用于执行所述计算机程序时实现上述所述的UEFI BIOS升级方法的步骤。

[0035] 本申请还提供一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述所述的UEFI BIOS升级方法的步骤。

[0036] 本申请所提供的一种UEFI BIOS升级方法，包括：在接收到打包发送的密文和UEFI BIOS镜像文件后，利用预设公钥对所述密文进行解密，得到所述密文对应的原文和第一摘要信息；利用HASH函数对所述原文进行处理，得到第二摘要信息；判断所述第一摘要信息和所述第二摘要信息是否相同；若是，则将所述UEFI BIOS镜像文件存储至闪存中；在验证所述UEFI BIOS镜像文件中的BIOS代码镜像通过后，安装所述UEFI BIOS镜像文件以实现UEFI BIOS升级。

[0037] 该方法利用预设公钥对所述密文进行解密，得到所述密文对应的原文和第一摘要信息；利用HASH函数对所述原文进行处理，得到第二摘要信息；判断所述第一摘要信息和所述第二摘要信息是否相同；若是，则将所述UEFI BIOS镜像文件存储至闪存中，即认定该UEFI BIOS镜像文件是可信的，最终安装该UEFI BIOS镜像文件以实现UEFI BIOS升级，由于该UEFI BIOS镜像文件是可信的，避免给服务器带来很大的安全问题。本申请还提供一种UEFI BIOS升级系统、设备及计算机可读存储介质，均具有上述有益效果，在此不再赘述。

附图说明

[0038] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图。

[0039] 图1为本申请实施例所提供的一种UEFI BIOS升级方法的流程图；

[0040] 图2为本申请实施例所提供的一种UEFI BIOS升级系统的结构框图。

具体实施方式

[0041] 本申请的核心是提供一种UEFI BIOS升级方法，能够保证用于UEFI BIOS升级的UEFI BIOS镜像文件是可信的，进而避免给服务器带来很大的安全问题。本申请的另一核心是提供一种UEFI BIOS升级系统、设备及计算机可读存储介质。

[0042] 为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0043] 目前，相关技术中对UEFI BIOS进行升级时无法保证用于升级的UEFI BIOS镜像文件是可信的，导致给服务器带来很大的安全问题。本申请实施例能够保证用于UEFI BIOS升级的UEFI BIOS镜像文件是可信的，进而避免给服务器带来很大的安全问题，具体请参考图1，图1为本申请实施例所提供的一种UEFI BIOS升级方法的流程图，该UEFI BIOS升级方法具体包括：

[0044] S101、在接收到打包发送的密文和UEFI BIOS镜像文件后，利用预设公钥对密文进行解密，得到密文对应的原文和第一摘要信息；

[0045] S102、利用HASH函数对原文进行处理，得到第二摘要信息；

[0046] 本申请实施例中，将SP(Service Processor，服务处理器)作为系统的RTU(Root of Trust for Update，可更新的信任根)。为了启动UEFI BIOS升级，为了将来UEFI BIOS可以访问SP环境，主机上的系统管理软件可以和SP通信，发送待升级的UEFI BIOS镜像文件存储在SP环境中，也可以通过SP网络的带外通信将待升级的BIOS镜像发送到SP，故在本申请实施例中要保证SP是可信的，所有SPI flash区域在系统复位时都被解锁。本申请实施例对上述密文的加密算法不作具体限定，通常在编译生成UEFI BIOS镜像文件后，运用数字签名技术，对UEFI BIOS镜像文件进行签名。数字签名的内容分为两个部分：第一部分即为UEFI BIOS镜像文件本身的信息，包括发行时间、镜像文件的大小、UEFI BIOS标识号等；第二部分

即为对UEFI BIOS镜像文件运行密码算法后得出的签名值。具体地，在生成UEFI BIOS镜像文件时使用SM3算法生成一个对应的第一摘要信息，UEFI BIOS供应商利用自己的私钥对生成的第一摘要信息进行加密，然后将加密后的密文和待升级的UEFI BIOS镜像文件一起打包发送给SP，同时将对应私钥的公钥提供给客户端。本申请实施例中SP在接收到打包发送的密文和UEFI BIOS镜像文件后，利用预设公钥对密文进行解密，得到密文对应的原文和第一摘要信息。其中，预设公钥是与上述私钥对应的。进一步地，在接收到打包发送的密文和UEFI BIOS镜像文件后，利用预设公钥对密文进行解密，得到密文对应的原文和第一摘要信息，通常包括：接收使用数字签名技术加密的密文和UEFI BIOS镜像文件；利用预设公钥对密文进行解密，得到密文对应的原文和第一摘要信息。

[0047] 本申请实施例在得到密文对应的原文和第一摘要信息后，利用HASH函数对原文进行处理，得到第二摘要信息。在此对HASH函数不作具体限定，应由本领域技术人员根据实际情况作出相应的设定。在此对第二摘要信息也不作具体限定，该第二摘要信息和上述第一摘要信息均是摘要，至于第二摘要信息和第一摘要信息是否相同需根据实际情况而定。

[0048] S103、判断第一摘要信息和第二摘要信息是否相同；

[0049] 本申请实施例在得到第一摘要信息和第二摘要信息后，需判断第一摘要信息和第二摘要信息是否相同，故有两种情况：1、第一摘要信息和第二摘要信息相同；2、第一摘要信息和第二摘要信息不相同。本申请实施例对判断第一摘要信息和第二摘要信息是否相同的依据不作具体限定，通常是根据第一摘要信息和第二摘要信息匹配相似度进行判断，若匹配相似度达到预设的阈值，则可判定第一摘要信息和第二摘要信息相同；若匹配相似度没有达到预设的阈值，则可判定第一摘要信息和第二摘要信息不相同。在此对预设的阈值不作具体限定，应由本领域技术人员根据实际情况作出相应的设定。例如，可以将阈值设置为100％，即只有当第一摘要信息和第二摘要信息的匹配相似度达到100％才可认定第一摘要信息和第二摘要信息相同。

[0050] S104、若第一摘要信息和第二摘要信息相同，则将UEFI BIOS镜像文件存储至闪存中；

[0051] 本申请实施例在判断出第一摘要信息和第二摘要信息相同时，则认定UEFI BIOS镜像文件是可信的，将UEFI BIOS镜像文件存储至闪存中。具体地，若UEFI BIOS镜像文件是可信的，即UEFI BIOS镜像文件验证通过，则SP通过与系统flash的SPI控制器进行通信来执行flash刷新操作，甚至在主机系统引导后SP也可以继续和系统flash的SPI控制器通信执行flash刷新操作，也就是将UEFI BIOS镜像文件存储至闪存中。在UEFI BIOS闪存中必须存在一种锁机制，这样除了RTU没有实体可以在运行时对UEFI BIOS闪存进行写访问。对于若第一摘要信息和第二摘要信息不相同这种情况，在此对其后续执行操作不作具体限定，应由本领域技术人员根据实际情况作出相应的设定。若第一摘要信息和第二摘要信息不相同，即UEFI BIOS镜像文件验证不通过，则UEFI BIOS会通过和SPI控制器通信来锁定BIOS flash闪存到“锁直到重置”区域，这个区域包含UEFI BIOS镜像。当锁被设置，对这个SPI区域锁寄存器的访问会变为只读，这样“锁直到重置”设置就不能被修改。这个区域锁会被优先执行，然后再退出RTU。

[0052] S105、在验证UEFIBIOS镜像文件中的BIOS代码镜像通过后，安装UEFI BIOS镜像文件以实现UEFI BIOS升级。

[0053] 本申请实施例在验证UEFIBIOS镜像文件中的BIOS代码镜像通过后，安装UEFI BIOS镜像文件以实现UEFI BIOS升级。进一步地，上述在验证UEFI BIOS镜像文件中的BIOS代码镜像通过后，安装UEFI BIOS镜像文件以实现UEFI BIOS升级，通常包括：利用UEFI BIOS镜像文件中的验证组件验证BIOS代码镜像是否通过；若验证BIOS代码镜像通过，则安装UEFI BIOS镜像文件以实现UEFI BIOS升级。具体地，在将UEFI BIOS镜像文件存储至闪存中后，每次系统重启时，执行权被传递给RTU-V验证组件，由RTU-V验证组件验证系统BIOS的剩余部分，该剩余部分即为BIOS代码镜像；如果RTU-V验证组件验证BIOS代码镜像通过，RTU-V验证组件将控制权传递给系统BIOS的剩余部分，进而安装UEFI BIOS镜像文件以实现UEFI BIOS升级。其中，系统BIOS镜像其实是包括两个部分的，一部分是RTU-V验证组件，一部分就是BIOS代码镜像，其中，RTU-V验证组件是锁定的，而BIOS代码镜像是未锁定的。在此对RTU-V验证组件验证BIOS代码镜像的验证方法不作具体限定，应由本领域技术人员根据实际情况作出相应的设定，通常也是采用数字签名验证算法进行验证。

[0054] 在此对于验证BIOS代码镜像不通过这种情况的后续执行操作不作具体限定，应由本领域技术人员根据实际情况作出相应的设定。若验证BIOS代码镜像不通过，通常会验证并刷新预先存储在SP中的可信UEFI BIOS镜像文件。具体地，若验证BIOS代码镜像不通过，即验证失败，上述UEFI BIOS镜像文件将不会被安装，RTU-V验证组件将告知SP上的BIOS RTU验证失败的消息，SP会访问之前存储在SP上的可信UEFI BIOS镜像文件，验证并刷新该可信UEFI BIOS镜像文件，然后SP会强制系统重启以启动RTU-V验证组件进行验证，最后进入新的BIOS。

[0055] 本申请利用预设公钥对密文进行解密，得到密文对应的原文和第一摘要信息；利用HASH函数对原文进行处理，得到第二摘要信息；判断第一摘要信息和第二摘要信息是否相同；若是，则将UEFI BIOS镜像文件存储至闪存中，即认定该UEFI BIOS镜像文件是可信的，最终安装该UEFI BIOS镜像文件以实现UEFI BIOS升级，由于该UEFI BIOS镜像文件是可信的，避免给服务器带来很大的安全问题。

[0056] 下面对本申请实施例提供的一种UEFI BIOS升级系统、设备及计算机可读存储介质进行介绍，下文描述的UEFI BIOS升级系统、设备及计算机可读存储介质与上文描述的UEFI BIOS升级方法可相互对应参照。

[0057] 请参考图2，图2为本申请实施例所提供的一种UEFI BIOS升级系统的结构框图；该UEFI BIOS升级系统包括：

[0058] 解密模块201，用于在接收到打包发送的密文和UEFI BIOS镜像文件后，利用预设公钥对密文进行解密，得到密文对应的原文和第一摘要信息；

[0059] 原文处理模块202，用于利用HASH函数对原文进行处理，得到第二摘要信息；

[0060] 摘要信息判断模块203，用于判断第一摘要信息和第二摘要信息是否相同；

[0061] 存储模块204，用于若第一摘要信息和第二摘要信息相同，则将UEFI BIOS镜像文件存储至闪存中；

[0062] 镜像文件安装模块205，用于在验证UEFI BIOS镜像文件中的BIOS代码镜像通过后，安装UEFI BIOS镜像文件以实现UEFI BIOS升级。

[0063] 基于上述实施例，本实施例中镜像文件安装模块205通常包括：

[0064] 验证单元，用于利用UEFI BIOS镜像文件中的验证组件验证BIOS代码镜像是否通

过；

[0065] 镜像文件安装单元，用于若验证BIOS代码镜像通过，则安装UEFI BIOS镜像文件以实现UEFI BIOS升级。

[0066] 基于上述实施例，本实施例中镜像文件安装模块205通常包括：

[0067] 验证刷新单元，用于若验证BIOS代码镜像不通过，则验证并刷新预先存储在SP中的可信UEFI BIOS镜像文件。

[0068] 基于上述实施例，本实施例中解密模块201通常包括：

[0069] 接收单元，用于接收使用数字签名技术加密的密文和UEFI BIOS镜像文件；

[0070] 解密单元，用于利用预设公钥对密文进行解密，得到密文对应的原文和第一摘要信息。

[0071] 本申请还提供一种设备，包括：存储器和处理器；其中，存储器用于存储计算机程序，处理器用于执行计算机程序时实现上述任意实施例的UEFI BIOS升级方法的步骤。

[0072] 本申请还提供一种计算机可读存储介质，计算机可读存储介质存储有计算机程序，计算机程序被处理器执行时实现上述任意实施例的UEFI BIOS升级方法的步骤。

[0073] 该计算机可读存储介质可以包括：U盘、移动硬盘、只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0074] 说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。对于实施例提供的系统而言，由于其与实施例提供的方法相对应，所以描述的比较简单，相关之处参见方法部分说明即可。

[0075] 专业人员还可以进一步意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0076] 结合本文中所公开的实施例描述的方法或算法的步骤可以直接用硬件、处理器执行的软件模块，或者二者的结合来实施。软件模块可以置于随机存储器(RAM)、内存、只读存储器(ROM)、电可编程ROM、电可擦除可编程ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

[0077] 以上对本申请所提供的一种UEFI BIOS升级方法、系统、设备及计算机可读存储介质进行了详细介绍。本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想。应当指出，对于本技术领域的普通技术人员来说，在不脱离本申请原理的前提下，还可以对本申请进行若干改进和修饰，这些改进和修饰也落入本申请权利要求的保护范围内。

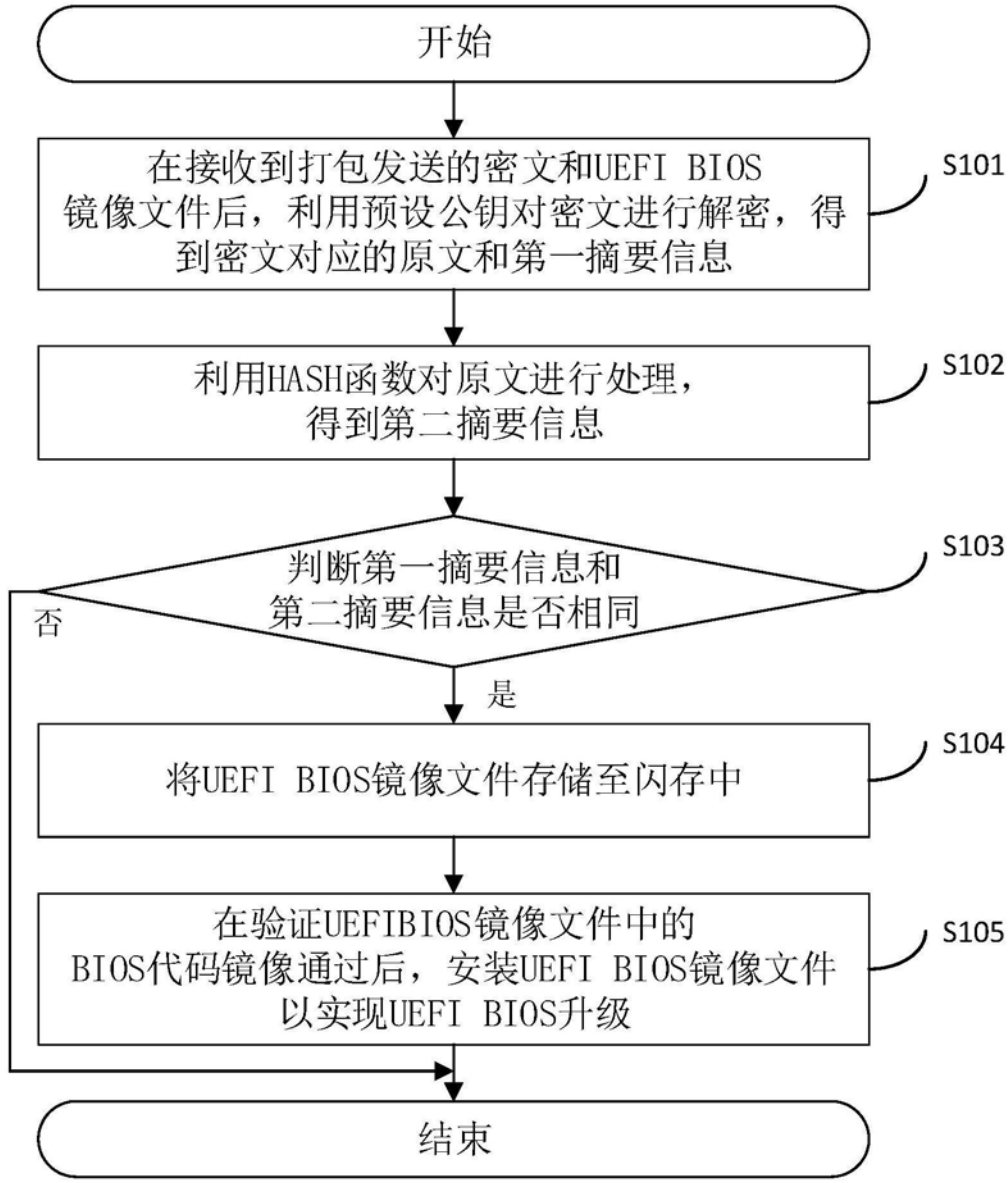

开始
在接收到打包发送的密文和UEFI BIOS镜像文件后，利用预设公钥对密文进行解密，得到密文对应的原文和第一摘要信息
S101
利用HASH函数对原文进行处理，得到第二摘要信息
S102
判断第一摘要信息和第二摘要信息是否相同
S103
否
是
将UEFI BIOS镜像文件存储至闪存中
S104
在验证UEFIBIOS镜像文件中的BIOS代码镜像通过后，安装UEFI BIOS镜像文件以实现UEFI BIOS升级
S105
结束

图1

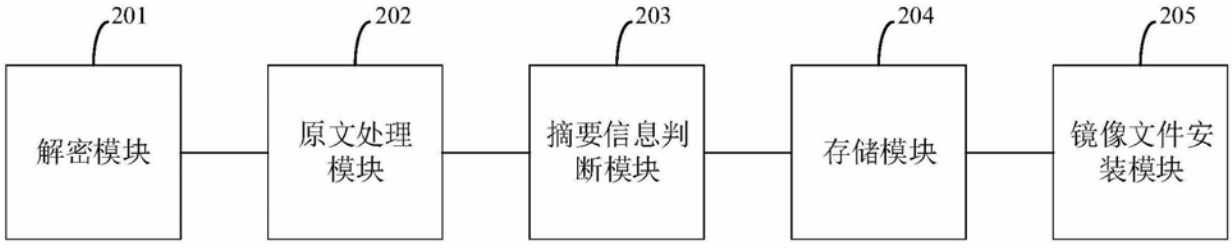

201
解密模块
202
原文处理模块
203
摘要信息判断模块
204
存储模块
205
镜像文件安装模块

图2