(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114780929 A
(43)申请公布日 2022.07.22

(21)申请号 202210348362.4

(22)申请日 2022.04.01

(71)申请人 联想(北京)有限公司
地址 100085 北京市海淀区上地西路6号2幢2层201-H2-6

(72)发明人 胡斌 翁振业

(74)专利代理机构 北京乐知新创知识产权代理事务所(普通合伙) 11734
专利代理师 张永喆

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/60(2013.01)
G06F 21/64(2013.01)
G06F 21/78(2013.01)

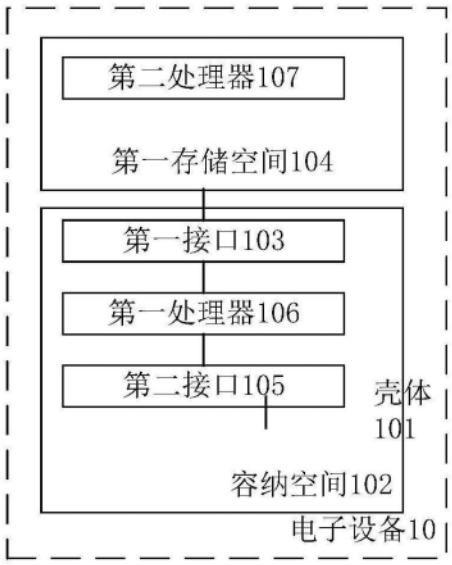
权利要求书2页 说明书8页 附图5页

(54)发明名称

一种电子设备及处理方法

(57)摘要

本申请公开了一种电子设备及处理方法,该电子设备包括:壳体,形成有容纳空间,所述壳体上和/或所述容纳空间内设置有第一接口,通过所述第一接口能够获得存储于与所述第一接口连接的第一存储空间中的第一文件,所述第一文件为用于支持第一系统运行的文件,所述第一系统用于初始化所述电子设备。通过第一接口获取用于支持第一系统运行的第一文件,有效保证第一系统运行的安全性。



CN 114780929 A

1.一种电子设备,包括:

壳体,形成有容纳空间,所述壳体上和/或所述容纳空间内设置有第一接口,通过所述第一接口能够获得存储于与所述第一接口连接的第一存储空间中的第一文件,所述第一文件为用于支持第一系统运行的文件,所述第一系统用于初始化所述电子设备。

2.根据权利要求1所述的电子设备,所述壳体上和/或所述容纳空间内还设置有:

第二接口,用于在所述第一系统对所述初始化后能够通过第二接口传送数据。

3.根据权利要求1所述的电子设备,所述电子设备还包括:

第一处理器,用于通过所述第一接口获得所述第一文件,并对所述第一文件进行安全验证,以使得通过所述安全验证的第一文件支持所述第一系统运行。

4.根据权利要求3所述的电子设备,所述电子设备还包括:

第二处理器,与所述第一接口相关联,用于接收所述第一处理器访问所述第一接口的访问请求,基于所述访问请求对所述第一处理器进行身份验证,并在所述第一处理器的身份验证通过的情况下,允许所述第一处理器通过所述第一接口获取数据。

5.一种处理方法,所述方法包括:

通过不需要初始化的第一接口,获得存储于与所述第一接口连接的第一存储空间的第一文件,所述第一文件为用于支持第一系统运行的文件,所述第一系统用于初始化电子设备;

基于所述第一文件,支持所述第一系统启动。

6.根据权利要求5所述的方法,所述基于所述第一文件,支持所述第一系统启动,包括:

基于所述第一文件,支持第一系统的第一部分运行,所述第一系统的第一部分用于对电子设备进行初始化;

通过第二接口获取与所述第二接口连接的第二存储空间中的第二文件;

基于所述第二文件,支持第一系统的第二部分运行,所述第一系统的第二部分用于引导操作系统启动。

7.根据权利要求6所述的方法,所述基于所述第一文件,支持第一系统的第一部分运行,包括:

对所述第一文件进行安全验证,以使得通过所述安全验证的第一文件支持所述第一系统的第一部分运行。

8.根据权利要求6所述的方法,所述第一文件包括所述第一系统的第一子文件和第二子文件,所述第一子文件根据为所述第一系统配置的私钥生成,所述私钥存储在独立于所述电子设备的第三存储空间;相应的,

所述基于所述第一文件,支持第一系统的第一部分运行,包括:

根据预先存储的公钥对所述第一子文件进行解密,得到解密结果;

将所述解密结果与预存验证数据进行比对,以验证所述第一文件的安全性;

在所述解密结果与预存验证数据一致的情况下,运行所述第一文件,以支持所述第一系统的第一部分运行;

其中,所述公钥与所述私钥相对应。

9.根据权利要求5所述的方法,在通过不需要初始化的第一接口从与所述第一接口连接的第一存储空间中获取第一文件之前,所述方法还包括:

响应于启动所述电子设备的触发信号，请求获取所述电子设备的第一系统的启动密码；

接收所述启动密码；

对所述启动密码进行验证；

在所述启动密码验证通过的情况下，执行前述过程，以使得所述电子设备启动。

10.根据权利要求5至9中任一项所述的方法，所述第一文件为加密文件；相应的，

所述基于所述第一文件，支持所述第一系统启动，包括：

对所述第一文件进行安全验证；

在所述第一文件验证通过的情况下，根据所述第一文件对第三文件进行验证，第三文件的存储位置与第一文件不同，且第三文件为基本输入输出系统文件。

一种电子设备及处理方法

技术领域

[0001] 本申请涉及信息安全技术领域,尤其涉及一种电子设备及处理方法。

背景技术

[0002] 随着计算机信息技术的发展,电子设备的安全性越来越受到重视。PC(Personal Computer,计算机)的启动主要从BIOS(Basic Input and Output System,基本输入输出系统)开始,如果BIOS不安全,那么整个PC的安全性就无法保证。

发明内容

[0003] 本申请实施例提供一种电子设备及处理方法。

[0004] 根据本申请第一方面,提供了一种电子设备,包括:壳体,形成有容纳空间,所述壳体上和/或所述容纳空间内设置有第一接口,通过所述第一接口能够获得存储于与所述第一接口连接的第一存储空间中的第一文件,所述第一文件为用于支持第一系统运行的文件,所述第一系统用于初始化所述电子设备。

[0005] 根据本申请一实施方式,所述壳体上和/或所述容纳空间内还设置有:第二接口,用于在所述第一系统对所述初始化后能够通过第二接口传送数据。

[0006] 根据本申请一实施方式,所述电子设备还包括:第一处理器,用于通过所述第一接口获得所述第一文件,并对所述第一文件进行安全验证,以使得通过所述安全验证的第一文件支持所述第一系统运行。

[0007] 根据本申请一实施方式,所述电子设备还包括:第二处理器,与所述第一接口相关联,用于接收所述第一处理器访问所述第一接口的访问请求,基于所述访问请求对所述第一处理器进行身份验证,并在所述第一处理器的身份验证通过的情况下,允许所述第一处理器通过所述第一接口获取数据。

[0008] 根据本申请第二方面,还提供一种处理方法,所述方法包括:通过不需要初始化的第一接口,获得存储于与所述第一接口连接的第一存储空间的第一文件,所述第一文件为用于支持第一系统运行的文件,所述第一系统用于初始化电子设备;基于所述第一文件,支持所述第一系统启动。

[0009] 根据本申请一实施方式,所述基于所述第一文件,支持所述第一系统启动,包括:基于所述第一文件,支持第一系统的第一部分运行,所述第一系统的第一部分用于对电子设备进行初始化;通过第二接口获取与所述第二接口连接的第二存储空间中的第二文件;基于所述第二文件,支持第一系统的第二部分运行,所述第一系统的第二部分用于引导操作系统启动。

[0010] 根据本申请一实施方式,所述基于所述第一文件,支持第一系统的第一部分运行,包括:对所述第一文件进行安全验证,以使得通过所述安全验证的第一文件支持所述第一系统的第一部分运行。

[0011] 根据本申请一实施方式,所述第一文件包括所述第一系统的第一子文件和第二子

文件，所述第一子文件根据为所述第一系统配置的私钥生成，所述私钥存储在独立于所述电子设备的第三存储空间；相应的，所述基于所述第一文件，支持第一系统的第一部分运行，包括：根据预先存储的公钥对所述第一子文件进行解密，得到解密结果；将所述解密结果与预存验证数据进行比对，以验证所述第一文件的安全性；在所述解密结果与预存验证数据一致的情况下，运行所述第一文件，以支持所述第一系统的第一部分运行；其中，所述公钥与所述私钥相对应。

[0012] 根据本申请一实施方式，在通过不需要初始化的第一接口从与所述第一接口连接的第一存储空间中获取第一文件之前，所述方法还包括：响应于启动所述电子设备的触发信号，请求获取所述电子设备的第一系统的启动密码；接收所述启动密码；对所述启动密码进行验证；在所述启动密码验证通过的情况下，执行前述过程，以使得所述电子设备启动。

[0013] 根据本申请一实施方式，所述第一文件为加密文件；相应的，所述基于所述第一文件，支持所述第一系统启动，包括：对所述第一文件进行安全验证；在所述第一文件验证通过的情况下，根据所述第一文件对第三文件进行验证，第三文件的存储位置与第一文件不同，且第三文件为基本输入输出系统文件。

[0014] 本申请实施例提供的电子设备及处理方法，该电子设备包括：壳体，形成有容纳空间，所述壳体上和/或所述容纳空间内设置有第一接口，通过所述第一接口能够获得存储于与所述第一接口连接的第一存储空间中的第一文件，所述第一文件为用于支持第一系统运行的文件，所述第一系统用于初始化所述电子设备。通过第一接口获取用于支持第一系统运行的第一文件，有效保证第一系统运行的安全性。

[0015] 需要理解的是，本申请的教导并不需要实现上面所述的全部有益效果，而是特定的技术方案可以实现特定的技术效果，并且本申请的其他实施方式还能够实现上面未提到的有益效果。

附图说明

[0016] 通过参考附图阅读下文的详细描述，本申请示例性实施方式的上述以及其他目的、特征和优点将变得易于理解。在附图中，以示例性而非限制性的方式示出了本申请的若干实施方式，其中：

[0017] 在附图中，相同或对应的标号表示相同或对应的部分。

[0018] 图1示出了本申请实施例电子设备的组成结构示意图；

[0019] 图2示出了本申请实施例电子设备的应用示例的组成结构示意图；

[0020] 图3示出了本申请第一实施例提供的处理方法的实现流程示意图；

[0021] 图4示出了本申请第二实施例提供的处理方法的实现流程示意图；

[0022] 图5示出了本申请第三实施例提供的处理方法的实现流程示意图；

[0023] 图6示出了本申请第四实施例提供的处理方法的实现流程示意图；

[0024] 图7示出了本申请第五实施例提供的处理方法的实现流程示意图。

具体实施方式

[0025] 下面将参考若干示例性实施方式来描述本申请的原理和精神。应当理解，给出这些实施方式仅仅是为使本领域技术人员能够更好地理解进而实现本申请，而并非以任何方

式限制本申请的范围。相反,提供这些实施方式是为使本申请更加透彻和完整,并能够将本申请的范围完整地传达给本领域的技术人员。

[0026] 下面结合附图和具体实施例对本申请的技术方案进一步详细阐述。

[0027] 图1示出了本申请实施例电子设备的组成结构示意图。

[0028] 参考图1,本申请实施例电子设备10,包括:壳体101,形成有容纳空间102,壳体101上和/或容纳空间102内设置有第一接口103,通过第一接口103能够获得存储于与第一接口103连接的第一存储空间104中的第一文件,第一文件为用于支持第一系统运行的文件,第一系统用于初始化电子设备10。

[0029] 在本申请这一实施方式中,电子设备10可以是便携式笔记本电脑、台式机或服务器等。第一接口103可以是符合NVMe(Non Volatile Memory Express,非易失性内存主机控制器接口规范)的逻辑接口,在EC上电后可直接使用。

[0030] 第一存储空间可以是SSD等具有符合NVMe的逻辑接口的非易失性存储设备。

[0031] 第一系统可以是BIOS。

[0032] 在本申请这一实施方式中,第一文件可以至少包括BIOS系统启动的数字签名或数字证书。还可以包括部分或全部的BIOS系统文件。

[0033] 在本申请这一实施方式中,壳体101上和/或容纳空间102内还设置有第二接口105,第二接口105用于在第一系统对初始化后能够通过第二接口105传送数据。

[0034] 在本申请这一实施方式中,第二接口需要通过对第一系统进行初始化之后使用,通过所述第二接口能够获取到与所述第二接口连接的第二存储空间中的第二文件,所述第二文件与所述第一文件组成用于支持所述第一系统运行的完整文件。举例说明,如果第一文件仅包括BIOS系统启动的数字签名或数字证书,则第二文件为的BIOS系统的完整文件。如果第一文件包括BIOS系统启动的数字证书和部分的BIOS系统文件,则第二文件为的BIOS系统文件中除第一文件所包含的部分之外的其他文件。

[0035] 在本申请这一实施方式中,电子设备10还包括:第一处理器106,用于通过第一接口103获得第一文件,并对第一文件进行安全验证,以使得通过安全验证的第一文件支持第一系统运行。

[0036] 在本申请这一实施方式中,第一处理器106可以是CPU或SOC或Chipset(芯片组),例如:北桥和南桥。

[0037] 在本申请这一实施方式中,电子设备10还包括:第二处理器107,与第一接口103相关联,用于接收第一处理器106访问第一接口103的访问请求,基于访问请求对第一处理器106进行身份验证,并在第一处理器106的身份验证通过的情况下,允许第一处理器106通过第一接口103获取数据。

[0038] 在本申请这一实施方式中,第二处理器107可以是NVMe存储设备自带的处理芯片,NVMe存储设备可以是固态硬盘等自带的处理芯片。

[0039] 在本申请这一实施方式中,通过第一接口103获取的数据可以是第一文件,也可以是其它文件。

[0040] 此外,需要说明的是,第二接口105、第一处理器106以及第二处理器107为本发明更为优选的实施例中所包括的,在本申请这一实施例中,对此不做具体限定。

[0041] 图2示出了本申请实施例电子设备的应用示例的组成结构示意图。

[0042] 参考图2,应用本申请实施例电子设备,将BIOS文件分为两部分,其中一部分保存至具有符合NVMe的接口的存储设备中,例如:固态硬盘。可以基于如图2所示的电子设备,通过以下操作流程保证电子设备的安全性:

[0043] 1、使用电子设备的所有者的私钥对存储至具有SPI接口的存储空间的BIOS文件以及存储至具有NVMe接口的存储空间的BIOS文件进行加密,得到数字证书。

[0044] 2、将加密得到的数字证书存储至设定位置,例如:可以将数字证书存储存储至具有NVMe接口的固态硬盘中。

[0045] 3、在电子设备上电开始启动时通过NVMe启动分区技术从外置的具有NVMe接口的固态硬盘中获得数字证书,然后对存储至Boot FW SPI FLASH(具有SPI接口的硬盘)的第一部分BIOS文件和存储至NVMe BIOS FW(具有符合NVMe的接口的固态硬盘)的第二部分BIOS文件分别进行验证。如果验证通过,则可以正常Boot(开机),若验证不通过,则执行halt(停机)操作。

[0046] 需要说明的是,在本申请的实施例中也将具有NVMe接口的固态硬盘称为NVMe密钥盘。

[0047] 4、如果电子设备设置了开机BIOS密码,则可以把加密后的开机BIOS密码的密文存储至具有符合NVMe的接口的固态硬盘中。例如:可以在设置开机BIOS密码的过程中,使用MD5摘要值算法计算开机BIOS密码的第一哈希值,并将开机BIOS密码的第一哈希值存储至具有符合NVMe的接口的固态硬盘中,在后续对开机BIOS密码进行验证时使用。在电子设备下次开机过程中,接收到电子设备开机请求的情况下,检测开机BIOS密码,并在检测到电子设备的使用者输入的开机BIOS密码时,计算所接收到的开机BIOS密码的第二哈希值,然后将第二哈希值与第一哈希值进行比对,如果相同则判定开机BIOS密码通过。

[0048] 此外,还可以在启动BIOS之前就进行身份验证。举例说明,可以生成一个BootKey(启动密码),用电子设备的所有者的私钥对BootKey进行加密,将加密后的BootKey存储至具有符合NVMe的接口的固态硬盘中。当检测到电子设备的开机请求时,CPU可以利用NVMe Boot Partition(NVMe启动分区)技术读取加密后的BootKey,然后使用与私钥相对应的公钥对加密后的BootKey进行验证,验证通过则正常执行BIOS的后续启动流程。若电子设备设置了开机BIOS密码,则在验证启动密码之后需要验证开机BIOS密码,并在开机BIOS密码也验证通过的情况下,正常执行BIOS的后续启动流程。

[0049] 图3示出了本申请第一实施例提供的处理方法的实现流程示意图。

[0050] 参考图3,本申请实施例处理方法,至少包括如下操作流程:操作301,通过不需要初始化的第一接口,获得存储于与第一接口连接的第一存储空间的第一文件,第一文件为用于支持第一系统运行的文件,第一系统用于初始化电子设备;操作302,基于第一文件,支持第一系统启动。

[0051] 在操作301中,通过不需要初始化的第一接口,获得存储于与第一接口连接的第一存储空间的第一文件,第一文件为用于支持第一系统运行的文件,第一系统用于初始化电子设备。

[0052] 在本申请这一实施例中,第一接口可以是符合NVMe的接口。

[0053] 在操作302中,基于第一文件,支持第一系统启动。

[0054] 在本申请这一实施例中,第一文件至少包括BIOS系统的数字证书,还可以包括部

分BIOS文件。这里首先以第一文件包括BIOS系统的数字证书为例，对本申请实施例进行说明。

[0055] 举例说明，CPU在获取到BIOS系统的数字证书的情况下，CPU可以根据自身存储的公钥对第一文件进行解密，得到解密得到的数据。将解密得到的数据与预存验证数据进行比对，以验证第一文件的安全性。

[0056] 具体的，可以利用公钥对数字证书进行解密，得到第一散列值，并对第一文件进行哈希运算，得到第二散列值，在第一哈希值与第二哈希值相同的情况下，判定第一文件验证通过。此时可以对电子设备的BIOS进行初始化，以使得CPU能够通过第二接口传输数据，以通过第二接口获得第二文件，完成第一系统的启动。

[0057] 其中，公钥为预先为BIOS配置的公钥，并且公钥与存储在独立于电子设备的第三存储空间的私钥相对应。第三存储空间可以是云端、专用密钥存储设备、U盘或存储密钥的电脑端等。

[0058] 图4示出了本申请第二实施例提供的处理方法的实现流程示意图。

[0059] 参考图4，本申请实施例处理方法，至少包括如下操作流程：

[0060] 操作401，通过不需要初始化的第一接口，获得存储于与第一接口连接的第一存储空间的第一文件，第一文件为用于支持第一系统运行的文件，第一系统用于初始化电子设备。

[0061] 操作402，基于第一文件，支持第一系统的第一部分运行，第一系统的第一部分用于对电子设备进行初始化。

[0062] 举例说明，第一存储空间具有符合NVMe接口规范的接口与主板连接的存储器，第二存储空间为SPI Flash(具有SPI接口的存储器)。第一系统为BIOS。第一文件包括BIOS系统启动的数字证书部分的BIOS系统文件。

[0063] 在获得第一文件后，首先对参考上述操作302对数字证书进行安全验证。在安全验证通过的情况下，运行从第一存储空间获得的部分的BIOS系统文件，以完成BIOS系统的初始化，BIOS的初始化至少包括对第二接口的初始化，在完成BIOS初始化后，可以执行如下操作403，通过第二接口获取与第二接口连接的第二存储空间中的第二文件。

[0064] 操作403，通过第二接口获取与第二接口连接的第二存储空间中的第二文件。

[0065] 操作404，基于第二文件，支持第一系统的第二部分运行，第一系统的第二部分用于引导操作系统启动。

[0066] 在本申请这一实施方式中，支持第一系统的第一部分和第二部分运行后，即可完成BIOS启动。

[0067] 举例说明，利用CPU中存储的公钥对第一存储空间的数字证书进行安全验证。在数字证书验证通过的情况下，从第一存储空间获取支持BIOS运行的第一部分，从利用数字证书对BIOS的第一部分进行安全验证。对BIOS的第一部分进行安全验证通过的情况下，从第二存储空间获取支持BIOS运行的第二部分，并再次根据数字证书对支持BIOS运行的第二部分进行验证。在支持BIOS运行的第一部分和第二部分均验证通过的情况下，运行支持BIOS运行的第一部分和第二部分，完成BIOS的初始化。

[0068] 由此，对BIOS两个部分的文件交叉验签，两个部分中任何一部分被破坏或者被篡改均禁止开机，有效保证电子设备的数据安全性。

[0069] 在本申请这一实施方式中，对第一文件进行安全验证，以使得通过安全验证的第一文件支持第一系统运行，并由此实现基于第一文件，支持第一系统的第一部分运行。

[0070] 其中，操作401的具体实现过程与图1所示实施例中操作101的具体实现过程相类似，这里不再赘述。

[0071] 图5示出了本申请第三实施例提供的处理方法的实现流程示意图。

[0072] 参考图5，本申请实施例处理方法，第一文件包括第一系统的第一子文件和第二子文件，第一子文件根据为第一系统配置的私钥生成，私钥存储在独立于电子设备的第三存储空间，至少包括如下操作流程：

[0073] 操作501，通过不需要初始化的第一接口，获得存储于与第一接口连接的第一存储空间的第一文件，第一文件为用于支持第一系统运行的文件，第一系统用于初始化电子设备。

[0074] 操作502，根据处理器自身存储的公钥对第一子文件进行解密，得到解密结果，其中，公钥为第一系统配置的公钥，并且公钥与私钥相对应。

[0075] 操作503，将解密结果与预存验证数据进行比对，以验证第一文件的安全性。

[0076] 操作504，在解密结果与预存验证数据一致的情况下，运行第一文件。

[0077] 其中，操作501～504的具体实现过程与图1所示实施例中操作101～102的具体实现过程相类似，这里不再赘述。

[0078] 图6示出了本申请第四实施例提供的处理方法的实现流程示意图。

[0079] 参考图6，本申请实施例处理方法，至少包括如下操作流程：

[0080] 操作601，响应于启动电子设备的触发信号，请求获取电子设备的第一系统的启动密码。

[0081] 操作602，接收启动密码。

[0082] 操作603，对启动密码进行验证。

[0083] 操作604，在启动密码验证通过的情况下，执行前述过程，以使得电子设备启动。

[0084] 具体的，BIOS的启动分为3个阶段：第1阶段是BIOS启动的上电自检过程；第2阶段是BIOS启动，电子设备初始化的过程；第3阶段是引导操作系统启动的过程。

[0085] 以上图3-5中的操作均在BIOS启动的第二阶段执行。

[0086] 在本申请这一实施方式中，在BIOS启动的第一阶段，即在启动BIOS之前就进行身份验证。举例说明，可以生成一个BootKey(启动密码)，用电子设备的所有者的私钥对BootKey进行加密，将加密后的BootKey存储至具有符合NVMe的接口的固态硬盘中。当检测到电子设备的开机请求时，CPU可以利用NVMe Boot Partition(NVMe启动分区)技术读取加密后的BootKey，然后使用与私钥相对应的公钥对加密后的BootKey进行验证，验证通过则正常执行BIOS的后续启动流程。若电子设备设置了开机BIOS密码，则在验证启动密码之后需要验证开机BIOS密码，并在开机BIOS密码也验证通过的情况下，正常执行BIOS的后续启动流程。

[0087] 操作605，通过不需要初始化的第一接口，获得存储于与第一接口连接的第一存储空间的第一文件，第一文件为用于支持第一系统运行的文件，第一系统用于初始化电子设备。

[0088] 操作606，基于第一文件，支持第一系统启动。

[0089] 其中，操作605和606的具体实现过程与图1所示实施例中操作101和102的具体实现过程相类似，这里不再赘述。

[0090] 图7示出了本申请第五实施例提供的处理方法的实现流程示意图。

[0091] 参考图7，本申请实施例处理方法中，第一文件为加密文件，本申请实施例处理方法至少包括如下操作流程：

[0092] 操作701，通过不需要初始化的第一接口，获得存储于与第一接口连接的第一存储空间的第一文件，第一文件为用于支持第一系统运行的文件，第一系统用于初始化电子设备。

[0093] 操作702，对第一文件进行安全验证。

[0094] 操作703，在第一文件验证通过的情况下，根据第一文件对第三文件进行验证，第三文件的存储位置与第一文件不同，且第三文件为BIOS文件。

[0095] 举例说明，CPU可以首先从具有符合NVMe的接口的固态硬盘中获取BIOS的数字证书。利用CPU中预先存储的为BIOS配置的公钥对数字证书进行解密，以对数字证书进行安全验证。在数字证书验证通过的情况下，从硬盘获得BIOS文件，并根据数字证书对BIOS文件进行验证。

[0096] 其中，操作701～703的其他具体实现过程与图1所示实施例中操作101～102的具体实现过程相类似，这里不再赘述。

[0097] 通过以上处理方法，将BIOS的密钥存储至具有符合NVMe的接口的存储空间，必须将具有符合NVMe的接口的存储空间连接至电子设备并且对BIOS的数字证书验证通过的情况下，才能完成对电子设备的BIOS进行初始化，并进一步启动电子设备。具有符合NVMe的接口的存储空间为能够独立保存的物理设备，由此，充分利用电子设备的物理设备之间的依赖关系，有效提高电子设备的数据安全性。若缺失具有符合NVMe的接口的存储空间的情况下，则无法完成对BIOS的验证，也无法完成电子设备的开机操作。

[0098] 本申请实施例提供的电子设备及处理方法，该电子设备包括：壳体101，形成有容纳空间102，壳体101上和/或容纳空间102内设置有第一接口，通过第一接口能够获得存储于与第一接口连接的第一存储空间中的第一文件，第一文件为用于支持第一系统运行的文件，第一系统用于初始化电子设备。通过第一接口获取用于支持第一系统运行的第一文件，有效保证第一系统运行的安全性。

[0099] 同理，基于上文处理方法，本申请实施例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程序，当程序被处理器执行时，使得处理器至少执行如下的操作步骤：操作301，通过不需要初始化的第一接口，获得存储于与第一接口连接的第一存储空间的第一文件，第一文件为用于支持第一系统运行的文件，第一系统用于初始化电子设备；操作302，基于第一文件，支持第一系统启动。

[0100] 这里需要指出的是：以上对针对图1和2电子设备实施例的描述，与前述图2至7所示的方法实施例的描述是类似的，具有同图2至7所示的方法实施例相似的有益效果，因此不做赘述。对于本申请设备实施例中未披露的技术细节，请参照本申请图2至7所示的处理方法实施例的描述而理解，为节约篇幅，因此不再赘述。

[0101] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而

且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0102] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的，例如，单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性的、机械的或其它形式的。

[0103] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显示的部件可以是、或也可以不是物理单元；既可以位于一个地方，也可以分布到多个网络单元上；可以根据实际的需要选择其中的部分或全部单元来实现本实施例方案的目的。

[0104] 另外，在本申请各实施例中的各功能单元可以全部集成在一个处理单元中，也可以是各单元分别单独作为一个单元，也可以两个或两个以上单元集成在一个单元中；上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0105] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：移动存储设备、只读存储器(Read Only Memory，ROM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0106] 或者，本申请上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机、服务器、或者网络设备等)执行本申请各个实施例方法的全部或部分。而前述的存储介质包括：移动存储设备、ROM、磁碟或者光盘等各种可以存储程序代码的介质。

[0107] 以上，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

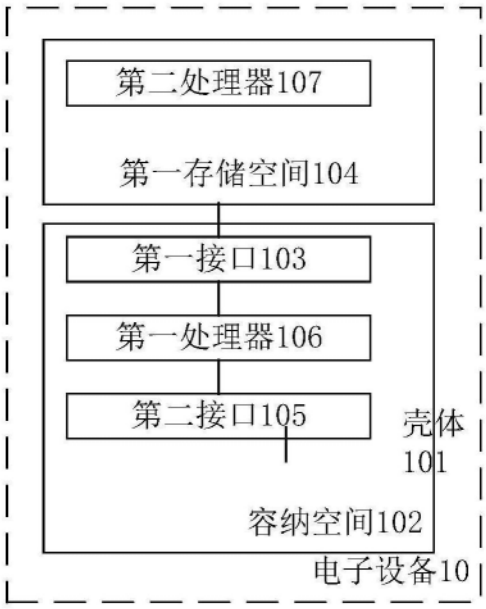

第二处理器107
第一存储空间104
第一接口103
第一处理器106
第二接口105
壳体
101
容纳空间102
电子设备10

图1

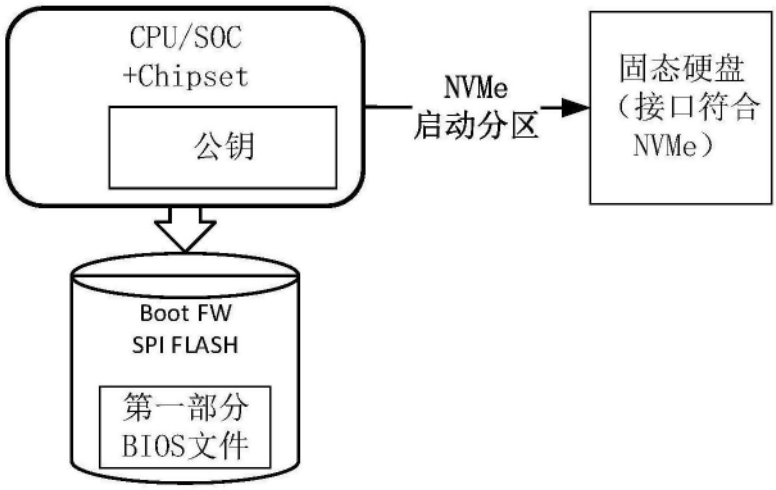

CPU/SOC
+Chipset
公钥
NVMe
启动分区
固态硬盘
（接口符合
NVMe）
Boot FW
SPI FLASH
第一部分
BIOS文件

图2

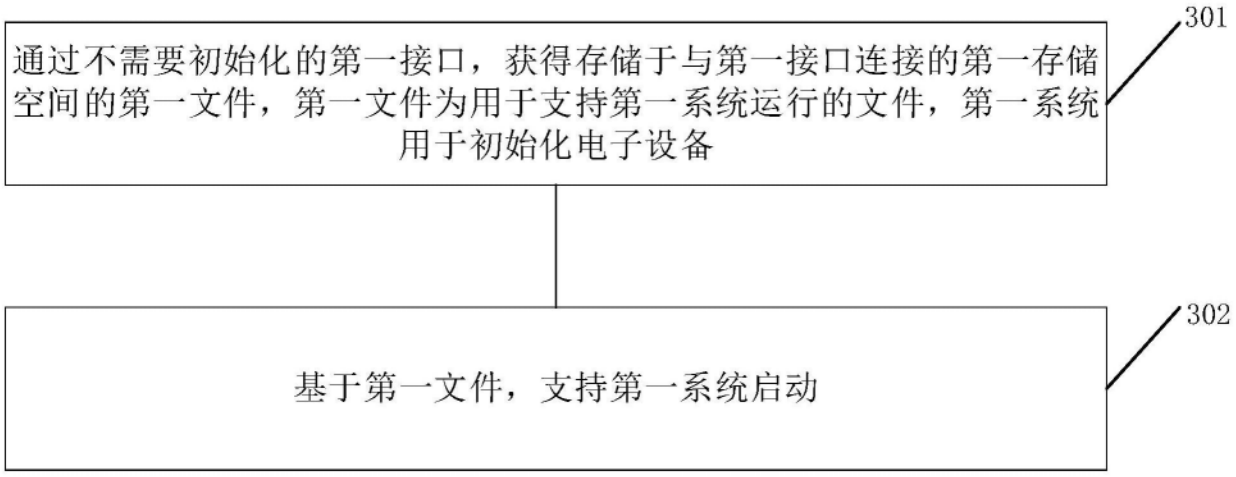

通过不需要初始化的第一接口，获得存储于与第一接口连接的第一存储空间的第一文件，第一文件为用于支持第一系统运行的文件，第一系统用于初始化电子设备
301
基于第一文件，支持第一系统启动
302

图3

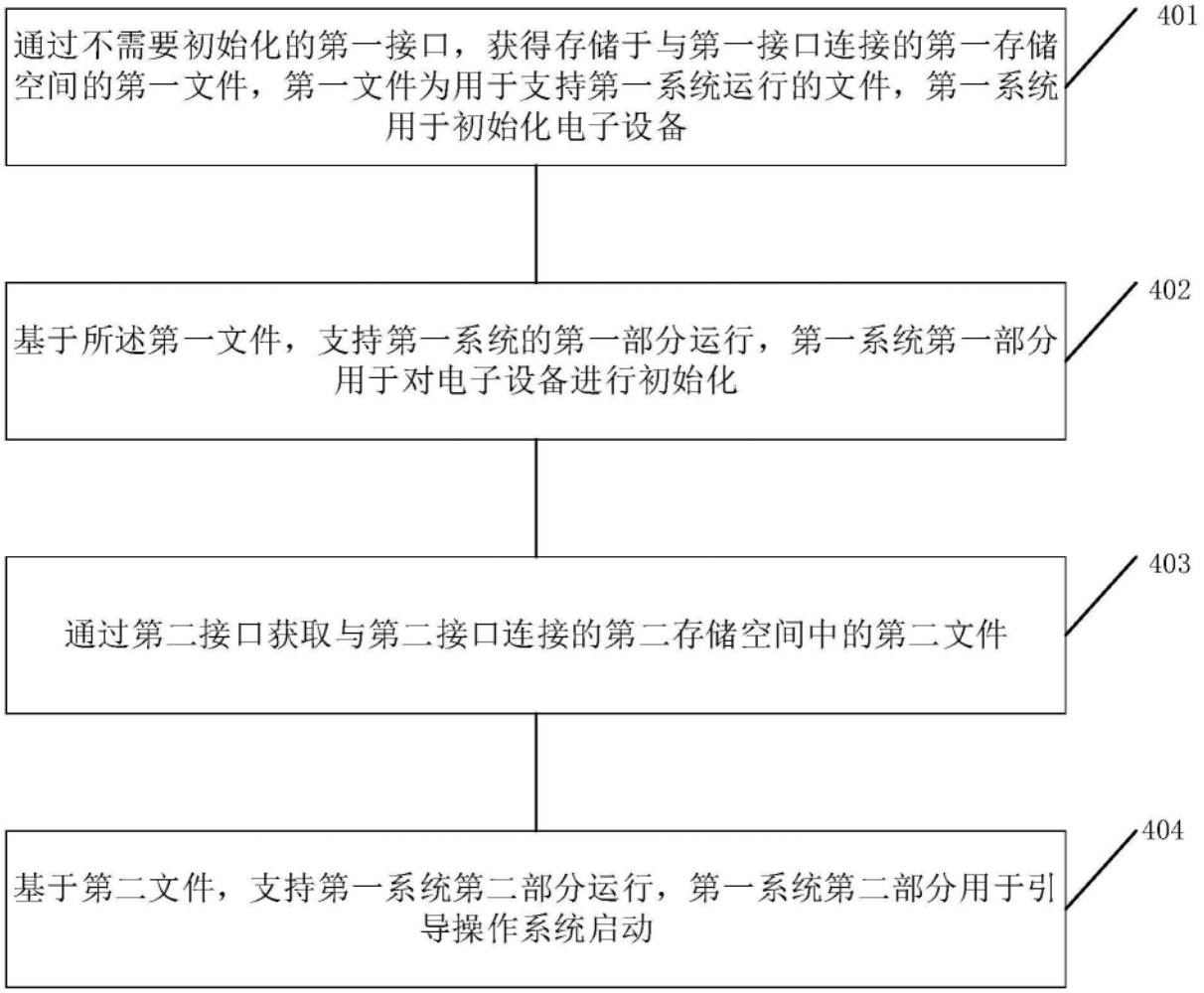

通过不需要初始化的第一接口，获得存储于与第一接口连接的第一存储空间的第一文件，第一文件为用于支持第一系统运行的文件，第一系统用于初始化电子设备
401
基于所述第一文件，支持第一系统的第一部分运行，第一系统第一部分用于对电子设备进行初始化
402
通过第二接口获取与第二接口连接的第二存储空间中的第二文件
403
基于第二文件，支持第一系统第二部分运行，第一系统第二部分用于引导操作系统启动
404

图4

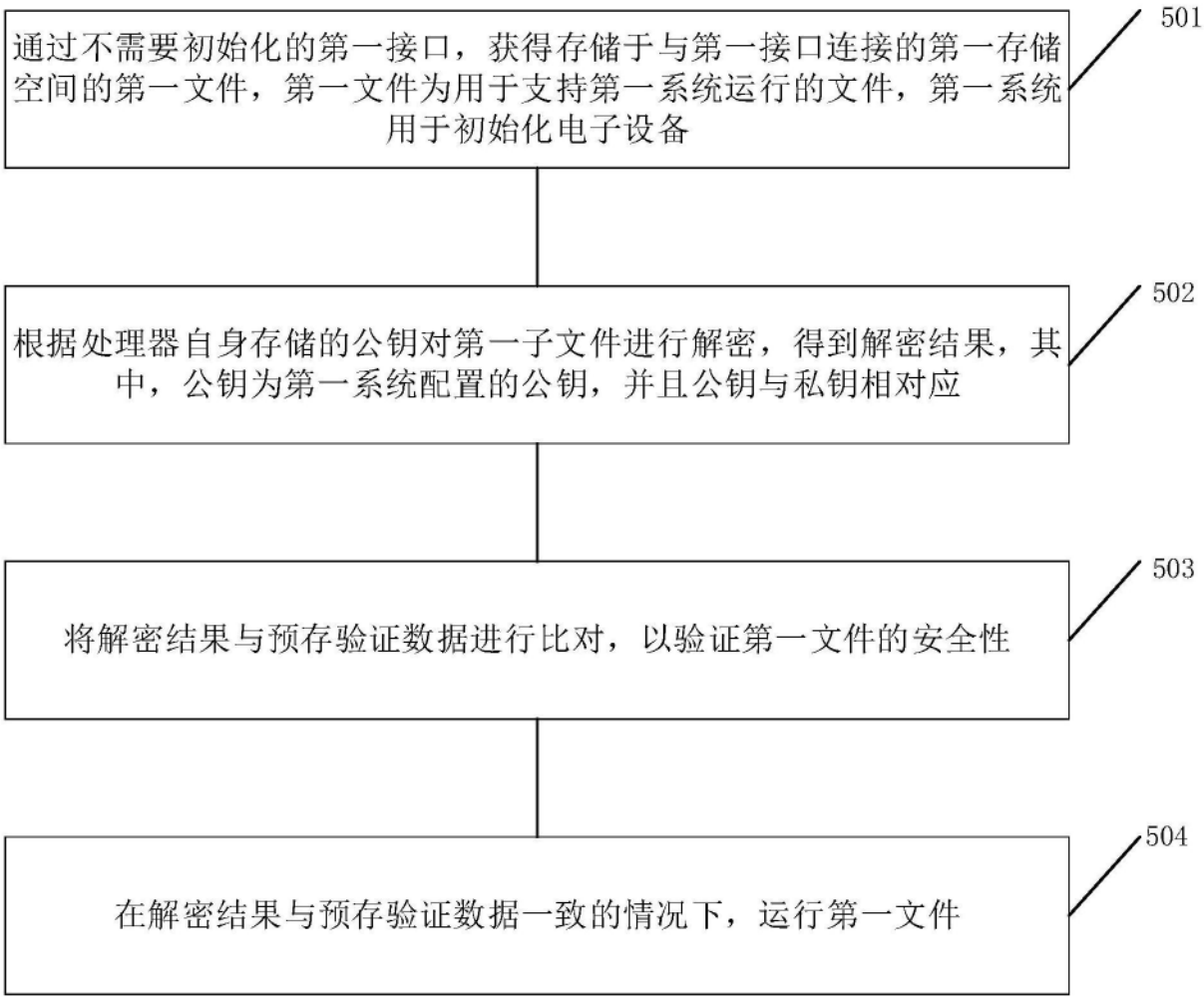

通过不需要初始化的第一接口，获得存储于与第一接口连接的第一存储空间的第一文件，第一文件为用于支持第一系统运行的文件，第一系统用于初始化电子设备
501
根据处理器自身存储的公钥对第一子文件进行解密，得到解密结果，其中，公钥为第一系统配置的公钥，并且公钥与私钥相对应
502
将解密结果与预存验证数据进行比对，以验证第一文件的安全性
503
在解密结果与预存验证数据一致的情况下，运行第一文件
504

图5

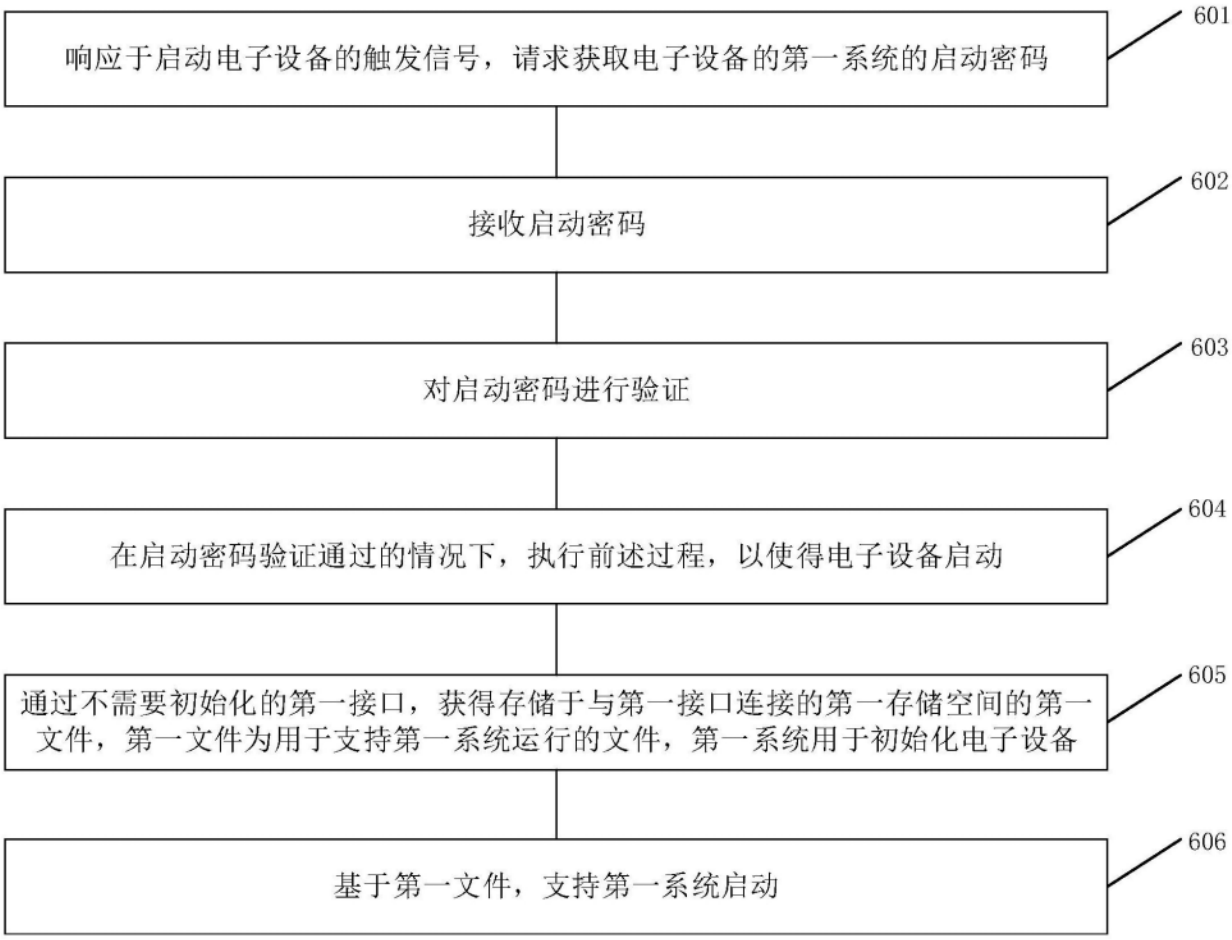

响应于启动电子设备的触发信号，请求获取电子设备的第一系统的启动密码
601
接收启动密码
602
对启动密码进行验证
603
在启动密码验证通过的情况下，执行前述过程，以使得电子设备启动
604
通过不需要初始化的第一接口，获得存储于与第一接口连接的第一存储空间的第一文件，第一文件为用于支持第一系统运行的文件，第一系统用于初始化电子设备
605
基于第一文件，支持第一系统启动
606

图6

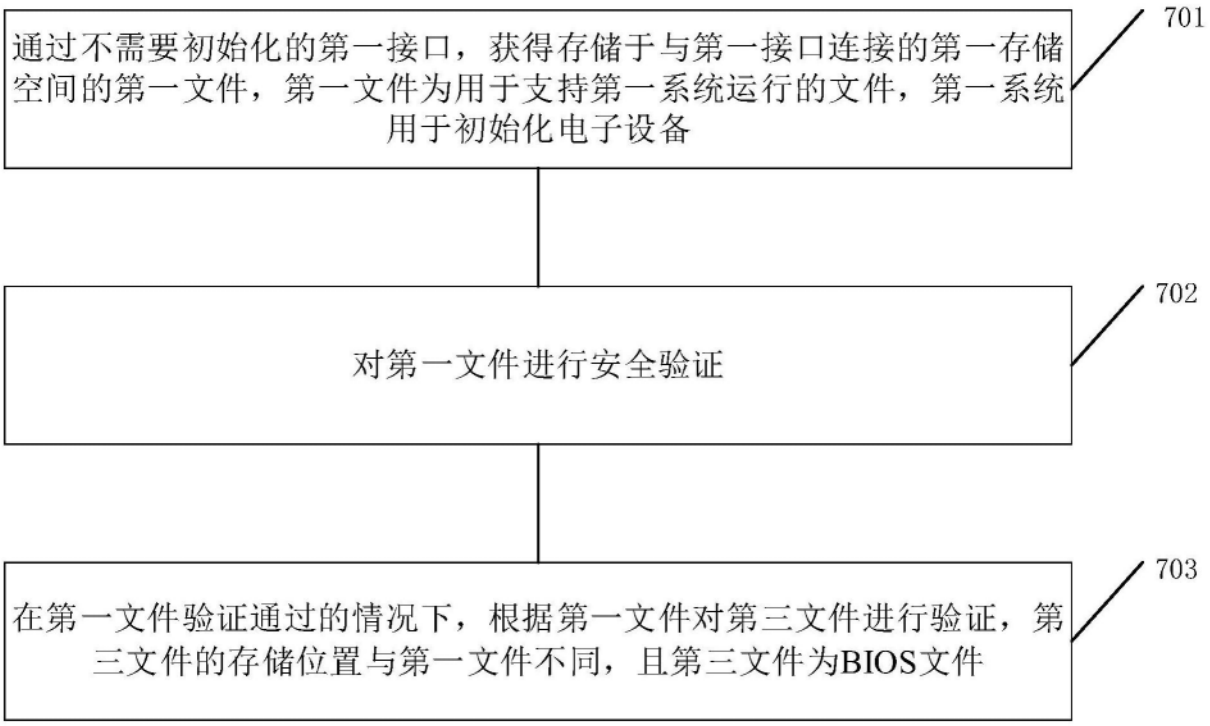

通过不需要初始化的第一接口，获得存储于与第一接口连接的第一存储空间的第一文件，第一文件为用于支持第一系统运行的文件，第一系统用于初始化电子设备
701
对第一文件进行安全验证
702
在第一文件验证通过的情况下，根据第一文件对第三文件进行验证，第三文件的存储位置与第一文件不同，且第三文件为BIOS文件
703

图7