(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 5 月 19 日 (19.05.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/100014 A1

(51) 国际专利分类号:
G06F 9/4401 (2018.01)

(21) 国际申请号: PCT/CN2021/089877

(22) 国际申请日: 2021 年 4 月 26 日 (26.04.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011256577.0 2020年11月11日 (11.11.2020) CN

(71) 申请人: 苏州浪潮智能科技有限公司 (INSPUR SUZHOU INTELLIGENT TECHNOLOGY CO., LTD.) [CN/CN]; 中国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, Jiangsu 215000 (CN)。

(72) 发明人: 黄帅 (HUANG, Shuai); 中国江苏省苏州市吴中区郭巷街道官浦路1号9幢, Jiangsu 215000 (CN)。 朱英澍 (ZHU, Yingshu); 中国江苏省苏州市吴中区郭巷街道官浦路1号9幢, Jiangsu 215000 (CN)。 王文志 (WANG, Wenzhi); 中国江苏省苏州市吴中区郭巷街道官浦路1号9幢, Jiangsu 215000 (CN)。

(74) 代理人: 北京集佳知识产权代理有限公司 (UNITALEN ATTORNEYS AT LAW); 中国北京市朝阳区建国门外大街22号赛特广场7层, Beijing 100004 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,

(54) **Title:** METHOD AND APPARATUS FOR CONTROLLING SYSTEM STARTUP, DEVICE AND READABLE STORAGE MEDIUM

(54) **发明名称:** 一种系统启动控制方法、装置、设备及可读存储介质

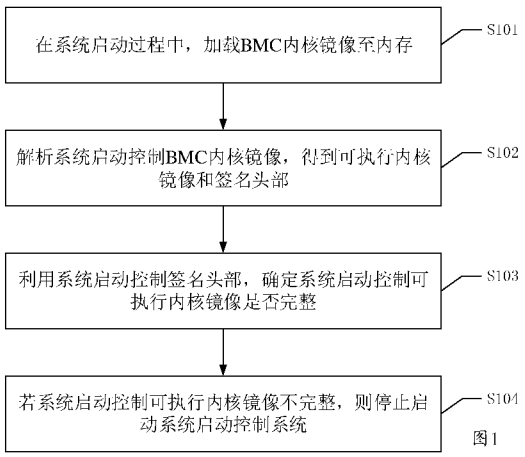


图1

S101 Load a BMC kernel mirroring to a memory during a system startup process
S102 Parse the BMC kernel mirroring for system startup control to obtain an executable kernel mirroring and a signature header
S103 Determine, by using the signature header for system startup control, whether the executable kernel mirroring for system startup control is complete
S104 If the executable kernel mirroring for system startup control is incomplete, stop startup of the system for system startup control

(57) **Abstract:** A method and an apparatus for controlling system startup, a device and a readable storage medium. The method comprises: loading a BMC kernel mirroring to a memory during a system startup process; parsing the BMC kernel mirroring to obtain an executable kernel mirroring and a signature header; determining, by using the signature header, whether the executable kernel mirroring is complete; and if the executable kernel mirroring is incomplete, stopping startup of the system. In the method, when a BMC is attacked, the completeness of an executable kernel mirroring is detected, and startup of a system is stopped when incompleteness is detected so as to prevent data information of the system from being attacked, so that a malicious attack can be effectively blocked during the system startup phase.

(57) **摘要:** 一种系统启动控制方法、装置、设备及可读存储介质，该方法包括：在系统启动过程中，加载BMC内核镜像至内存；解析BMC内核镜像，得到可执行内核镜像和签名头部；利用签名头部，确定可执行内核镜像是否完整；若可执行内核镜像不完整，则停止启动系统。该方法在BMC遭受攻击的情况下，通过检测可执行内核镜像的完整性，在检测出不完整时，停止启动系统来避免系统的数据信息遭受攻击，能够在系统启动阶段有效阻拦恶意攻击。

WO 2022/100014 A1

[见续页]

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) **指定国**(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

一种系统启动控制方法、装置、设备及可读存储介质

本申请要求于 2020 年 11 月 11 日提交中国专利局、申请号为202011256577.0、发明名称为“一种系统启动控制方法、装置、设备及可读存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及信息安全技术领域，特别是涉及一种系统启动控制方法、装置、设备及可读存储介质。

背景技术

随着信息技术的迅速发展，各行各业在享受信息技术带来诸多便利的同时，其背后也伴随着层出不穷的信息安全问题。享受信息时代的高效便捷及其创造的巨大利益的同时，同样受到信息安全的困扰。现在各种类型的物理服务器、白盒交换机已经广泛布置于各大数据中心，为医疗、教育、通讯等不同领域提供计算和存储能力。

但是，服务器或交换机在启动阶段其对于内部攻击所采取的防范能力十分有限。例如，在系统启动过程中对BMC（Baseboard Management Controller，基板管理控制器）这种关键的板级固件进行攻击，系统往往很难察觉，更谈不上对攻击的防御措施了。

综上所述，如何有效地解决系统启动过程中的安全防御等问题，是目前本领域技术人员急需解决的技术问题。

发明内容

本发明的目的是提供一种系统启动控制方法、装置、设备及可读存储介质，能够在系统启动过程中进行安全防御。

为解决上述技术问题，本发明提供如下技术方案:

一种系统启动控制方法，包括:

在系统启动过程中，加载BMC内核镜像至内存;

解析所述BMC内核镜像，得到可执行内核镜像和签名头部；

利用所述签名头部，确定所述可执行内核镜像是否完整；

若所述可执行内核镜像不完整，则停止启动所述系统。

优选地，利用所述签名头部，确定所述可执行内核镜像是否完整，包括：

从所述签名头部中，提取参考镜像散列值；

对所述可执行内核镜像进行散列值计算，得到实际镜像散列值；

若所述参考镜像散列值和所述实际镜像散列值一致，则确定所述可执行内核镜像完整。

优选地，从所述签名头部中，提取参考镜像散列值，包括：

从所述签名头部中读取出参考镜像散列值密文；

利用预设密钥，对所述参考镜像散列值密文进行解密；

若解密失败，则确定所述BMC内核镜像的来源不可信，停止启动所述系统；

若解密成功，则得到所述参考镜像散列值。

优选地，在本次启动所述系统之前，还包括：

在所述系统处于运行状态下，对BMC原始系统内核进行编译，生成所述可执行内核镜像；

在所述可执行内核镜像前增加所述签名头部，得到所述BMC内核镜像。

优选地，所述对BMC原始系统内核进行编译，生成所述可执行内核镜像，包括：

对所述BMC原始系统内核进行编译，生成linux内核镜像、文件系统镜像和设备树镜像；

将所述linux内核镜像、所述文件系统镜像和所述设备树镜像确定为所述可执行内核镜像。

优选地，在所述可执行内核镜像前增加所述签名头部，得到所述BMC内核镜像，包括：

获取参考镜像散列值密文、创建时间、镜像大小和内核加载地址；

将所述创建时间、所述镜像大小、所述内核加载地址以及所述参考镜像散列值密文确定为所述签名头部;

将所述签名头部添加至所述可执行内核镜像前，得到所述BMC内核镜像。

优选地，所述获取参考镜像散列值密文，包括:

利用安全哈希算法对所述可执行内核镜像进行散列值计算，得到参考镜像散列值;

利用预设密钥对所述参考镜像散列值进行加密，得到所述参考镜像散列值密文。

一种系统启动控制装置，包括:

内核加载模块，用于在系统启动过程中，加载BMC内核镜像至内存;

内核解析模块，用于解析所述BMC内核镜像，得到可执行内核镜像和签名头部;

镜像检测模块，用于利用所述签名头部，确定所述可执行内核镜像是否完整;

启动控制模块，用于若所述可执行内核镜像不完整，则停止启动所述系统。

一种电子设备，包括:

存储器，用于存储计算机程序;

处理器，用于执行所述计算机程序时实现上述系统启动控制方法的步骤。

一种可读存储介质，所述可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现上述系统启动控制方法的步骤。

应用本发明实施例所提供的方法，在系统启动过程中，加载BMC内核镜像至内存;解析系统启动控制BMC内核镜像，得到可执行内核镜像和签名头部;利用系统启动控制签名头部，确定系统启动控制可执行内核镜像是否完整;若系统启动控制可执行内核镜像不完整，则停止启动系统启动控制系统。

考虑到，在BMC遭受攻击后，会影响BMC的可执行内核镜像的完整性。

基于此，在本方法中，通过在BMC内核镜像中增设签名头部，在系统启动过程中，加载了BMC内核镜像之后，对其进行解析，得到可执行内核镜像和签名头部。然后，利用签名头部对可执行内核镜像的完整进行检测。在确定可执行内核镜像不完整的情况下，停止启动系统。如此，在BMC遭受攻击的情况下，通过检测可执行内核镜像的完整性，在检测出不完整时，停止启动系统来避免系统的数据信息遭受攻击，能够在系统启动阶段有效阻拦恶意攻击。

相应地，本发明实施例还提供了与上述系统启动控制方法相对应的系统启动控制装置、设备和可读存储介质，具有上述技术效果，在此不再赘述。

附图说明

为了更清楚地说明本发明实施例或相关技术中的技术方案，下面将对实施例或相关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发明的一些实施例，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，还可以根据这些附图获得其他的附图。

图1为本发明实施例中一种系统启动控制方法的实施流程图；

图2为本发明实施例中一种BMC内核镜像生成示意图；

图3为本发明实施例中一种内核镜像验证示意图；

图4为本发明实施例中一种系统启动控制装置的结构示意图；

图5为本发明实施例中一种电子设备的结构示意图；

图6为本发明实施例中一种电子设备的具体结构示意图。

具体实施方式

为了使本技术领域的人员更好地理解本发明方案，下面结合附图和具体实施方式对本发明作进一步的详细说明。显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，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，都属于本发明保护的范围。

请参考图1，图1为本发明实施例中一种系统启动控制方法的流程图，该方法可应用于具有BMC固件的系统（或称设备）中，如服务器、交换机等。

BMC固件是服务器或交换机的关键组成部分，它能够使得上层的指令传输到硬件层，并指挥硬件层进行上下电等关键操作；当设备通电并开始运行时，即系统启动过程中，系统首条指令就是在BMC固件中执行。可见BMC固件将是最早掌握系统控制器的部件，其对于设备的安全起到非常重要的作用。举例说明，假设在固件中设定相应的后门程序，便能够以一种隐蔽的方式获取系统的重要数据信息。

基于此，为了解决具有BMC固件的系统的安全启动问题，本发明实施例所提供的系统启动控制方法可从最基本的启动过程入手，确保设备启动过程中的关键固件是可信的。该方法包括以下步骤:

S101、在系统启动过程中，加载BMC内核镜像至内存。

其中，系统可以为具有BMC，且需要在系统启动过程中对数据信息安全进行有效保障的任意一个系统。

其中，BMC内核镜像即BMC固件运行所需的内核镜像。需要注意的是，在本发明实施例中，BMC内核镜像具体指镜像前具有签名头部。

S102、解析系统启动控制BMC内核镜像，得到可执行内核镜像和签名头部。

解析BMC内核镜像，即按照编码规则，从BMC内核镜像中解析出可执行内核镜像以及签名头部。

其中，签名头部具体包括能够用于验证可执行内核镜像是否完整的信息，例如镜像大小、创建时间、加载地址、以及可执行内核镜像对应的唯一标识（如可执行内核镜像的散列值）中的至少一种信息。

S103、利用系统启动控制签名头部，确定系统启动控制可执行内核镜像是否完整。

解析出签名头部和可执行内核镜像之后，便可利用该签名头部确定可

执行内核镜像是否完整。具体的，若签名头部包括镜像大小，则可判断可执行内核镜像的大小与该镜像大小是否一致，如果不一致，则确定可执行内核镜像不完整；若签名头部包括创建时间，则可判断可执行内核镜像的创建时间与签名头部中的创建时间是否一致，如果不一致，则确定可执行内核镜像不完整；若签名头部包括内核加载地址，则可判断可执行内核镜像的实际加载地址与该内核加载地址是否一致，如果不一种，则确定可执行内核镜像不完整；若签名头部包括可执行内核镜像对应的唯一标识，而该唯一标识与解析得到的可执行内核镜像不匹配，则可确定可执行内核镜像不完整。

S104、若系统启动控制可执行内核镜像不完整，则停止启动系统启动控制系统。

若可执行内核镜像不完整，则表明该可执行内核镜像可能因遭受恶意攻击等应用导致其不完整，此时继续启动系统，可能会造成不可估量的损失。因此，在确定可执行内核镜像不完整的情况下，可停止启动系统。

应用本发明实施例所提供的方法，在系统启动过程中，加载BMC内核镜像至内存；解析系统启动控制BMC内核镜像，得到可执行内核镜像和签名头部；利用系统启动控制签名头部，确定系统启动控制可执行内核镜像是否完整；若系统启动控制可执行内核镜像不完整，则停止启动系统启动控制系统。

考虑到，在BMC遭受攻击后，会影响BMC的可执行内核镜像的完整性。基于此，在本方法中，通过在BMC内核镜像中增设签名头部，在系统启动过程中，加载了BMC内核镜像之后，对其进行解析，得到可执行内核镜像和签名头部。然后，利用签名头部对可执行内核镜像的完整进行检测。在确定可执行内核镜像不完整的情况下，停止启动系统。如此，在BMC遭受攻击的情况下，通过检测可执行内核镜像的完整性，在检测出不完整时，停止启动系统来避免系统的数据信息遭受攻击，能够在系统启动阶段有效阻拦恶意攻击。

需要说明的是，基于上述实施例，本发明实施例还提供了相应的改进

方案。在优选/改进实施例中涉及与上述实施例中相同步骤或相应步骤之间可相互参考，相应的有益效果也可相互参照，在本文的优选/改进实施例中不再一一赘述。

在本发明的一种具体实施方式中，步骤S103利用系统启动控制签名头部，确定系统启动控制可执行内核镜像是否完整，包括:

步骤一、从系统启动控制签名头部中，提取参考镜像散列值。

即，在签名头部包括参考镜像散列值。散列值即哈希值，可采用哈希算法在对完整的可执行内核镜像进行哈希计算(即散列值计算)，而得到的参考镜像散列值。

进一步地，步骤一可具体包括:

步骤1、从系统启动控制签名头部中读取出参考镜像散列值密文;

步骤2、利用预设密钥，对系统启动控制参考镜像散列值密文进行解密;

步骤3、若解密失败，则确定系统启动控制BMC内核镜像的来源不可信，停止启动系统启动控制系统;

步骤4、若解密成功，则得到系统启动控制参考镜像散列值。

对于参考镜像散列值还可采用加密方式存储在签名头部，并且可以通过解密情况，确定BMC内核镜像的来源是否可信。具体的，若采用预设密钥无法解密参考镜像散列值密文，则说明BMC内核镜像的来源不可信，此时可直接停止启动系统，以避免因来源不可信的BMC内核镜像导致系统安全受到威胁。当然，在解密成功的情况下，便可得到参考镜像散列值。需要注意的是，对参考镜像散列值进行加密和解密的预设密钥应当对应。例如，若采用对称密钥，则加密和解密均采用同一个密钥;若采用非对称密钥，则加密和加密分别采用对应的公钥和私钥。在本实施例中，对预设密钥的具体形式不作限定。

步骤二、对系统启动控制可执行内核镜像进行散列值计算，得到实际镜像散列值。

在解析得到可执行内核镜像之后，可对可执行内核镜像进行散列值计算，得到实际镜像散列值。需要注意的是，参考镜像散列值即为针对完整的可执行内核镜像进行散列值计算得到的结果，而实际镜像散列值即为针

对解析出的可执行内核镜像进行散列值计算得到的结果。计算参照镜像散列值和计算实际镜像散列值所用的算法应当为同一算法，例如可采用SHA1算法（Secure Hash Algorithm，一种安全哈希算法）进行计算。

步骤三、若系统启动控制参考镜像散列值和系统启动控制实际镜像散列值一致，则确定系统启动控制可执行内核镜像完整。

若参考镜像散列值与实际镜像散列值一致，基于散列计算特性，则可确定解析得到可执行内核镜像是完整的。相应地，若参考镜像散列值与实际镜像散列值不一致，则可确定解析得到的可执行内核镜像不是完整。需要注意的是，在本实施例中可执行内核镜像不完整，可具体为可执行内核镜像相对于正常可执行内核镜像而言，包括但不限于存在缺失、增加、修改等导致与注册内核镜像不同的情况。

在本发明的一种具体实施方式中，在本次启动系统启动控制系统之前，即执行步骤S101之前，生成BMC内核镜像的具体实现过程，包括:

步骤一、在系统启动控制系统处于运行状态下，对BMC原始系统内核进行编译，生成系统启动控制可执行内核镜像。

也就是说，系统再次启动之前，在处于运行状态下，需对BMC原始系统内核进行编译，生成可执行内核镜像。

其中，系统启动控制对BMC原始系统内核进行编译，生成系统启动控制可执行内核镜像，可包括:

步骤1、对系统启动控制BMC原始系统内核进行编译，生成linux内核镜像、文件系统镜像和设备树镜像;

步骤2、将系统启动控制linux内核镜像、系统启动控制文件系统镜像和系统启动控制设备树镜像确定为系统启动控制可执行内核镜像。

也就是说，可执行内核镜像具体包括linux内核镜像、文件系统镜像和设备树镜像。对于如何对BMC原始系统内核进行编译，得到linux内核镜像、文件系统镜像和设备树镜像的具体过程，可参照镜像编译生成规则与实现，在此不再一一赘述。

步骤二、在系统启动控制可执行内核镜像前增加系统启动控制签名头

部，得到系统启动控制BMC内核镜像。

相较于相关技术中可执行内核镜像即为BMC内核镜像不同，本发明实施例中，BMC内核镜像不仅包括可执行内核镜像，还包括签名头部，且该签名头部位于可执行内核镜像前。

在实际应用中，上述步骤二可具体包括:

步骤1、获取参考镜像散列值密文、创建时间、镜像大小和内核加载地址。

其中，参考镜像散列值密文、创建时间、镜像大小和内核加载地址均与正常的可执行内核镜像对应，在确定二者不对应的情况下，可确定可执行内核镜像不完整。

其中，参考镜像散列值密文即参考镜像散列值进行加密所得密文。系统启动控制获取参考镜像散列值密文，可具体包括:

步骤1.1、利用安全哈希算法对系统启动控制可执行内核镜像进行散列值计算，得到参考镜像散列值;

步骤1.2、利用预设密钥对系统启动控制参考镜像散列值进行加密，得到系统启动控制参考镜像散列值密文。

举例说明，可以采用SHA1算法（一种安全哈希算法）对可执行内核镜像进行散落在计算，得到参考镜像散列值。然后，采用RSA算法（一种非对称密钥）对应私钥对参考镜像散列值进行签名（即加密），得到加密后的（或称为签名后的）参考镜像散列值密文。

步骤2、将系统启动控制创建时间、系统启动控制镜像大小、系统启动控制内核加载地址以及系统启动控制参考镜像散列值密文确定为系统启动控制签名头部。

即签名头部可包括创建时间、系统启动控制镜像大小、系统启动控制内核加载地址以及系统启动控制参考镜像散列值密文。

步骤3、将系统启动控制签名头部添加至系统启动控制可执行内核镜像前，得到系统启动控制BMC内核镜像。

即，BMC内核镜像包括签名头部和可执行内核镜像。

为便于本领域技术人员更好地理解本发明实施例所提供的系统启动控制方法，下面结合具体的应用场景为例，对系统启动控制方法进行详细说明。

BMC内核层主要包括U_Boot（Universal Boot Loader，通用引导加载程序）以及操作系统内核两个模块，其中U_Boot作为BMC上电后的第一段执行代码，主要功能包括关闭看门狗、初始化SDRAM（Synchronous Dynamic Random Access Memory，同步动态随机存储器）、读取Flash（Flash Memory，闪存）以及启动操作系统内核等；采用本发明实施例所提供的系统启动控制方法后，可在U_Boot原有功能的基础上增加BMC内核校验模块，实现启动阶段的内核镜像完整性校验功能，确保系统启动的可信性。

在原来的可执linux内核镜像zImage的前面增加一个签名头部，签名头部包括自身的签名信息、头部校验值、创建时间、镜像大小等参数，U_Boot在加载linux内核时会获取该签名头部，通过对签名头部的检测确定镜像是否遭到破坏。

具体的，请参考图2和图3，其中图2为本发明实施例中一种BMC内核镜像生成示意图，图3为本发明实施例中一种内核镜像验证示意图。

其中，采用了本发明实施例所提供的系统启动控制方法后，BMC内核镜像生成过程，包括:

1、首先对BMC原始系统内核进行编译，生成原始系统镜像zImage（即可执行内核镜像），镜像内容包括linux内核镜像、文件系统镜像、设备树镜像。

2、通过SHA1算法对原始系统镜像进行散列计算，得到原始镜像的散列值V-sha1（即参考镜像散列值）。

3、通过RSA算法，利用私钥对V-sha1进行签名，得到签名后的原始镜像散列值RV-sha1（即参考镜像散列值密文）。

4、最后将RV-sha1、镜像创建时间、镜像大小、加载地址等信息（即签名头部）与原始系统镜像zImage整合生成新的镜像（即BMC内核镜像）。

其中，采用了本发明实施例所提供的系统启动控制方法后，系统启动过程，对内核镜像的验证过程，即U_Boot验证BMC内核镜像主要包括以下

几个步骤:

1、将BMC内核镜像加载到内存中，之后根据镜像头部信息，解析出RV-sha1和原始镜像zImage。

2、利用RSA公钥来对RV-sha1进行解密。

其中，RSA公钥可以具体为BMC管理员通过终端输入，当然也可从存储介质中直接读取得到。若为BMC管理员通过终端输入，根据RSA非对称加密算法的特性，如果BMC管理员输入的公钥能够完成解密，那说明该镜像头部中RV-sha1信息可信，同时可以解密得到V-sha1；若解密失败，则说明镜像来源不合法，BMC内核镜像不可信，执行失败操作（即停止启动系统）。特别地，在解密失败时，还可再次进行解密，直到到达预设解密次数，如3次，则可确定解密失败而执行失败操作。

3、对解析出的zImage原始镜像，采用相同的HAS1算法进行散列计算，重新获取原始镜像的散列值（即实际镜像散列值），并与V-sha1进行对比；若两者相等，说明可执行内核镜像内容是完整的，因此可以确定整个BMC内核镜像的来源真实，内容完整；如果两者不相等，则说明镜像遭到篡改，自然就不具备完整性特征，执行失败操作。

由此可见，本发明实施例所提供的系统启动控制方法，在实际应用中，U-Boot阶段的BMC内核镜像检测，会最大限度提前发现内核镜像的恶意篡改或破坏风险，并提供对应的处理机制，防止产生更严重破坏。BMC内核加密以及校验过程的严谨性和完整性。即，通过U-Boot阶段对BMC内核镜像的校验，提高系统启动的完整性，避免启动过程中的固件攻击而造成的严重故障，对提升产品整体的安全性具有很大的帮助。

相应于上面的方法实施例，本发明实施例还提供了一种系统启动控制装置，下文描述的系统启动控制装置与上文描述的系统启动控制方法可相互对应参照。

参见图4所示，该装置包括以下模块:

内核加载模块101，用于在系统启动过程中，加载BMC内核镜像至内存;

内核解析模块102，用于解析系统启动控制BMC内核镜像，得到可执行内核镜像和签名头部；

镜像检测模块103，用于利用系统启动控制签名头部，确定系统启动控制可执行内核镜像是否完整；

启动控制模块104，用于若系统启动控制可执行内核镜像不完整，则停止启动系统启动控制系统。

应用本发明实施例所提供的装置，在系统启动过程中，加载BMC内核镜像至内存；解析系统启动控制BMC内核镜像，得到可执行内核镜像和签名头部；利用系统启动控制签名头部，确定系统启动控制可执行内核镜像是否完整；若系统启动控制可执行内核镜像不完整，则停止启动系统启动控制系统。

考虑到，在BMC遭受攻击后，会影响BMC的可执行内核镜像的完整性。基于此，在本装置中，通过在BMC内核镜像中增设签名头部，在系统启动过程中，加载了BMC内核镜像之后，对其进行解析，得到可执行内核镜像和签名头部。然后，利用签名头部对可执行内核镜像的完整进行检测。在确定可执行内核镜像不完整的情况下，停止启动系统。如此，在BMC遭受攻击的情况下，通过检测可执行内核镜像的完整性，在检测出不完整时，停止启动系统来避免系统的数据信息遭受攻击，能够在系统启动阶段有效阻拦恶意攻击。

在本发明的一种具体实施方式中，镜像检测模块103，具体用于从系统启动控制签名头部中，提取参考镜像散列值；对系统启动控制可执行内核镜像进行散列值计算，得到实际镜像散列值；若系统启动控制参考镜像散列值和系统启动控制实际镜像散列值一致，则确定系统启动控制可执行内核镜像完整。

在本发明的一种具体实施方式中，镜像检测模块103，具体用于从系统启动控制签名头部中读取出参考镜像散列值密文；利用预设密钥，对系统启动控制参考镜像散列值密文进行解密；若解密失败，则确定系统启动控制BMC内核镜像的来源不可信，停止启动系统启动控制系统；若解密成功，则得到系统启动控制参考镜像散列值。

在本发明的一种具体实施方式中，还包括：BMC内核镜像编译模块，用于在本次启动系统启动控制系统之前，在系统启动控制系统处于运行状态下，对BMC原始系统内核进行编译，生成系统启动控制可执行内核镜像；在系统启动控制可执行内核镜像前增加系统启动控制签名头部，得到系统启动控制BMC内核镜像。

在本发明的一种具体实施方式中，BMC内核镜像编译模块，具体用于对系统启动控制BMC原始系统内核进行编译，生成linux内核镜像、文件系统镜像和设备树镜像；将系统启动控制linux内核镜像、系统启动控制文件系统镜像和系统启动控制设备树镜像确定为系统启动控制可执行内核镜像。

在本发明的一种具体实施方式中，BMC内核镜像编译模块，具体用于获取参考镜像散列值密文、创建时间、镜像大小和内核加载地址；将系统启动控制创建时间、系统启动控制镜像大小、系统启动控制内核加载地址以及系统启动控制参考镜像散列值密文确定为系统启动控制签名头部；将系统启动控制签名头部添加至系统启动控制可执行内核镜像前，得到系统启动控制BMC内核镜像。

在本发明的一种具体实施方式中，BMC内核镜像编译模块，具体用于利用安全哈希算法对系统启动控制可执行内核镜像进行散列值计算，得到参考镜像散列值；利用预设密钥对系统启动控制参考镜像散列值进行加密，得到系统启动控制参考镜像散列值密文。

相应于上面的方法实施例，本发明实施例还提供了一种电子设备，下文描述的一种电子设备与上文描述的一种系统启动控制方法可相互对应参照。

参见图5所示，该电子设备包括：

存储器332，用于存储计算机程序；

处理器322，用于执行计算机程序时实现上述方法实施例的系统启动控制方法的步骤。

具体的，请参考图6，为本实施例提供的一种电子设备的具体结构示意

图，该电子设备可因配置或性能不同而产生比较大的差异，可以包括一个或一个以上处理器（central processing units，CPU）322（例如，一个或一个以上处理器）和存储器332，存储器332存储有一个或一个以上的计算机应用程序342或数据344。其中，存储器332可以是短暂存储或持久存储。存储在存储器332的程序可以包括一个或一个以上模块（图示没标出），每个模块可以包括对数据处理设备中的一系列指令操作。更进一步地，中央处理器322可以设置为与存储器332通信，在电子设备301上执行存储器332中的一系列指令操作。

电子设备301还可以包括一个或一个以上电源326，一个或一个以上有线或无线网络接口350，一个或一个以上输入输出接口358，和/或，一个或一个以上操作系统341。

上文所描述的系统启动控制方法中的步骤可以由电子设备的结构实现。

相应于上面的方法实施例，本发明实施例还提供了一种可读存储介质，下文描述的一种可读存储介质与上文描述的一种系统启动控制方法可相互对应参照。

一种可读存储介质，可读存储介质上存储有计算机程序，计算机程序被处理器执行时实现上述方法实施例的系统启动控制方法的步骤。

该可读存储介质具体可以为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存储程序代码的可读存储介质。

本领域技术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。本领域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。

权 利 要 求

1、一种系统启动控制方法，其特征在于，包括:

在系统启动过程中，加载 BMC 内核镜像至内存;

解析所述 BMC 内核镜像，得到可执行内核镜像和签名头部;

利用所述签名头部，确定所述可执行内核镜像是否完整;

若所述可执行内核镜像不完整，则停止启动所述系统。

2、根据权利要求 1 所述的系统启动控制方法，其特征在于，利用所述签名头部，确定所述可执行内核镜像是否完整，包括:

从所述签名头部中，提取参考镜像散列值;

对所述可执行内核镜像进行散列值计算，得到实际镜像散列值;

若所述参考镜像散列值和所述实际镜像散列值一致，则确定所述可执行内核镜像完整。

3、根据权利要求 2 所述的系统启动控制方法，其特征在于，从所述签名头部中，提取参考镜像散列值，包括:

从所述签名头部中读取出参考镜像散列值密文;

利用预设密钥，对所述参考镜像散列值密文进行解密;

若解密失败，则确定所述 BMC 内核镜像的来源不可信，停止启动所述系统;

若解密成功，则得到所述参考镜像散列值。

4、根据权利要求 1 所述的系统启动控制方法，其特征在于，在本次启动所述系统之前，还包括:

在所述系统处于运行状态下，对 BMC 原始系统内核进行编译，生成所述可执行内核镜像;

在所述可执行内核镜像前增加所述签名头部，得到所述 BMC 内核镜像。

5、根据权利要求 4 所述的系统启动控制方法，其特征在于，所述对 BMC 原始系统内核进行编译，生成所述可执行内核镜像，包括:

对所述 BMC 原始系统内核进行编译，生成 linux 内核镜像、文件系统镜像和设备树镜像;

将所述 linux 内核镜像、所述文件系统镜像和所述设备树镜像确定为所述可执行内核镜像。

6、根据权利要求 4 所述的系统启动控制方法，其特征在于，在所述可执行内核镜像前增加所述签名头部，得到所述 BMC 内核镜像，包括:

获取参考镜像散列值密文、创建时间、镜像大小和内核加载地址;

将所述创建时间、所述镜像大小、所述内核加载地址以及所述参考镜像散列值密文确定为所述签名头部;

将所述签名头部添加至所述可执行内核镜像前，得到所述 BMC 内核镜像。

7、根据权利要求 6 所述的系统启动控制方法，其特征在于，所述获取参考镜像散列值密文，包括:

利用安全哈希算法对所述可执行内核镜像进行散列值计算，得到参考镜像散列值;

利用预设密钥对所述参考镜像散列值进行加密，得到所述参考镜像散列值密文。

8、一种系统启动控制装置，其特征在于，包括:

内核加载模块，用于在系统启动过程中，加载 BMC 内核镜像至内存;

内核解析模块，用于解析所述 BMC 内核镜像，得到可执行内核镜像和签名头部;

镜像检测模块，用于利用所述签名头部，确定所述可执行内核镜像是否完整;

启动控制模块，用于若所述可执行内核镜像不完整，则停止启动所述系统。

9、一种电子设备，其特征在于，包括:

存储器，用于存储计算机程序;

处理器，用于执行所述计算机程序时实现如权利要求 1 至 7 任一项所述系统启动控制方法的步骤。

10、一种可读存储介质，其特征在于，所述可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求 1 至 7 任一项

所述系统启动控制方法的步骤。

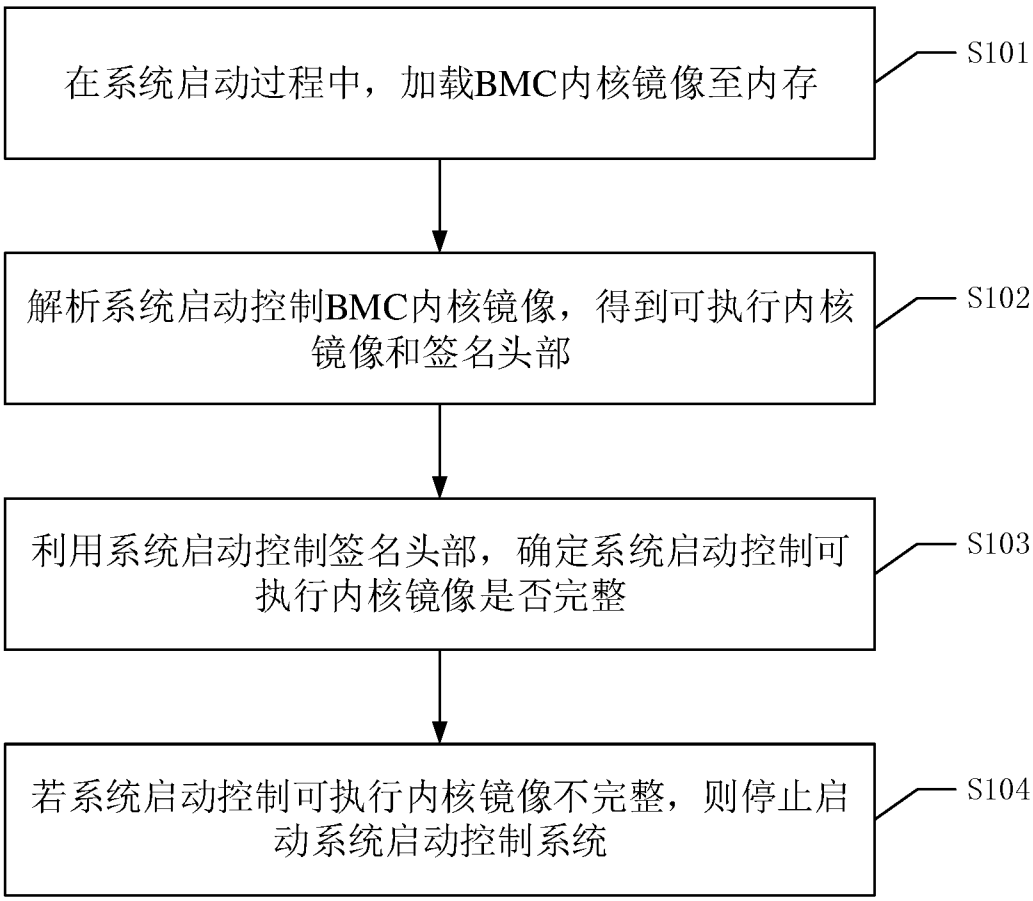

在系统启动过程中，加载BMC内核镜像至内存
S101
解析系统启动控制BMC内核镜像，得到可执行内核镜像和签名头部
S102
利用系统启动控制签名头部，确定系统启动控制可执行内核镜像是否完整
S103
若系统启动控制可执行内核镜像不完整，则停止启动系统启动控制系统
S104

图1

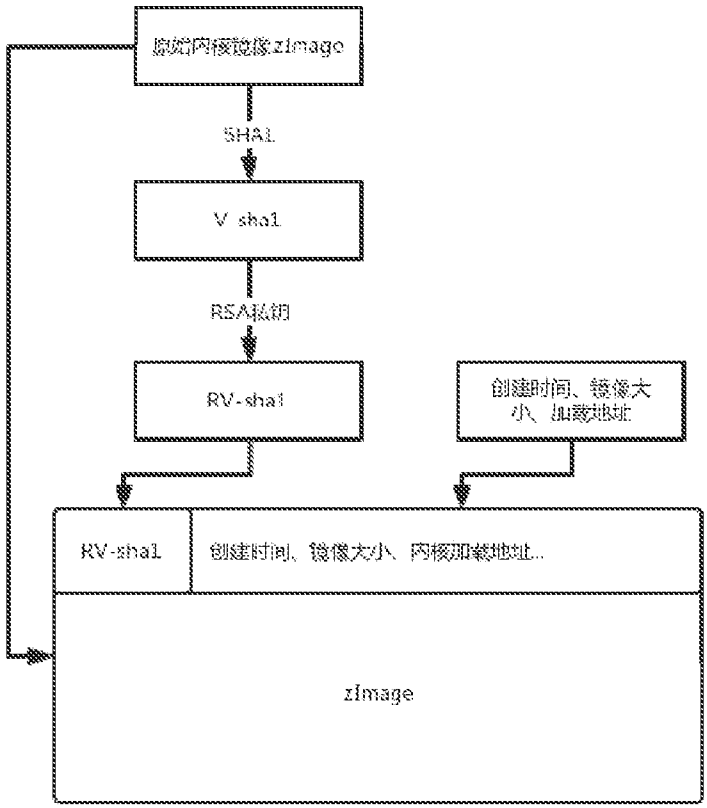

原始内核镜像zImage
SHA1
V sha1
RSA私钥
RV-sha1
创建时间、镜像大小、加载地址
RV-sha1
创建时间、镜像大小、内核加载地址...
zImage

图2

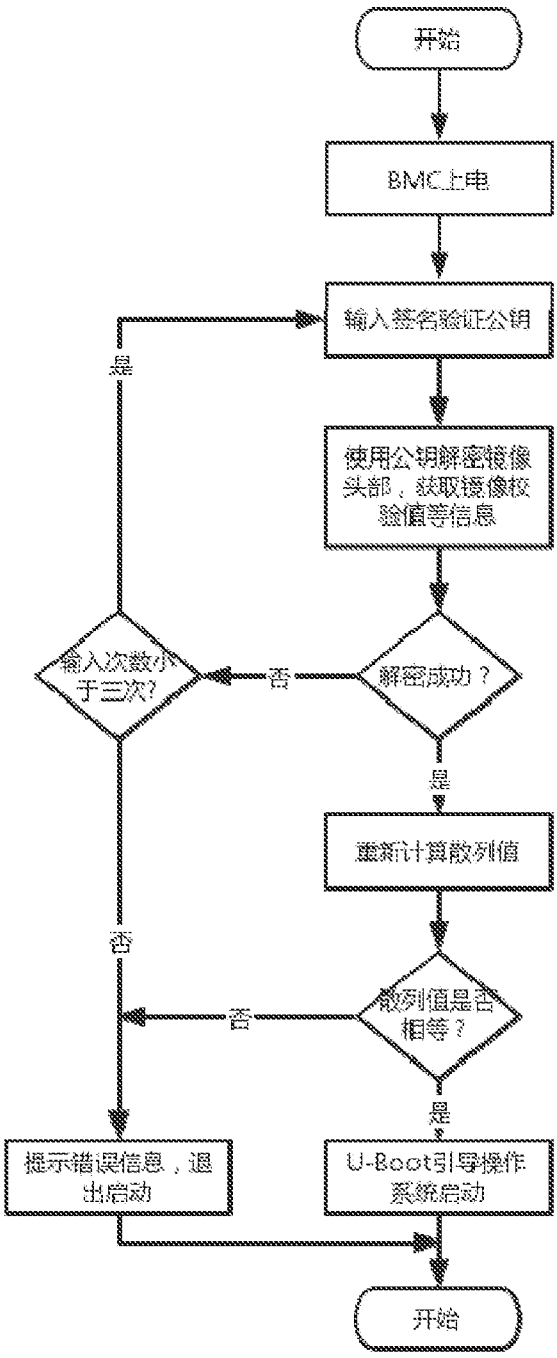

开始
BMC上电
输入签名验证公钥
使用公钥解密镜像头部，获取镜像校验值等信息
解密成功？
否
输入次数小于三次？
是
否
重新计算散列值
散列值是否相等？
否
是
提示错误信息，退出启动
U-Boot引导操作系统启动
开始

图3

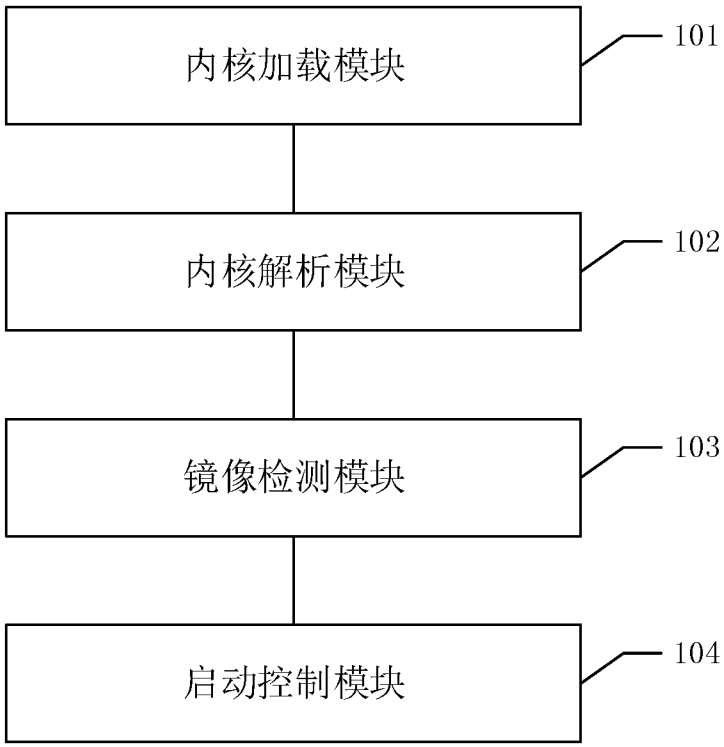


图4

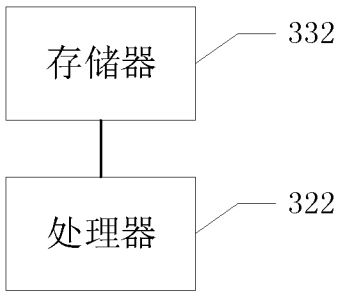


图5

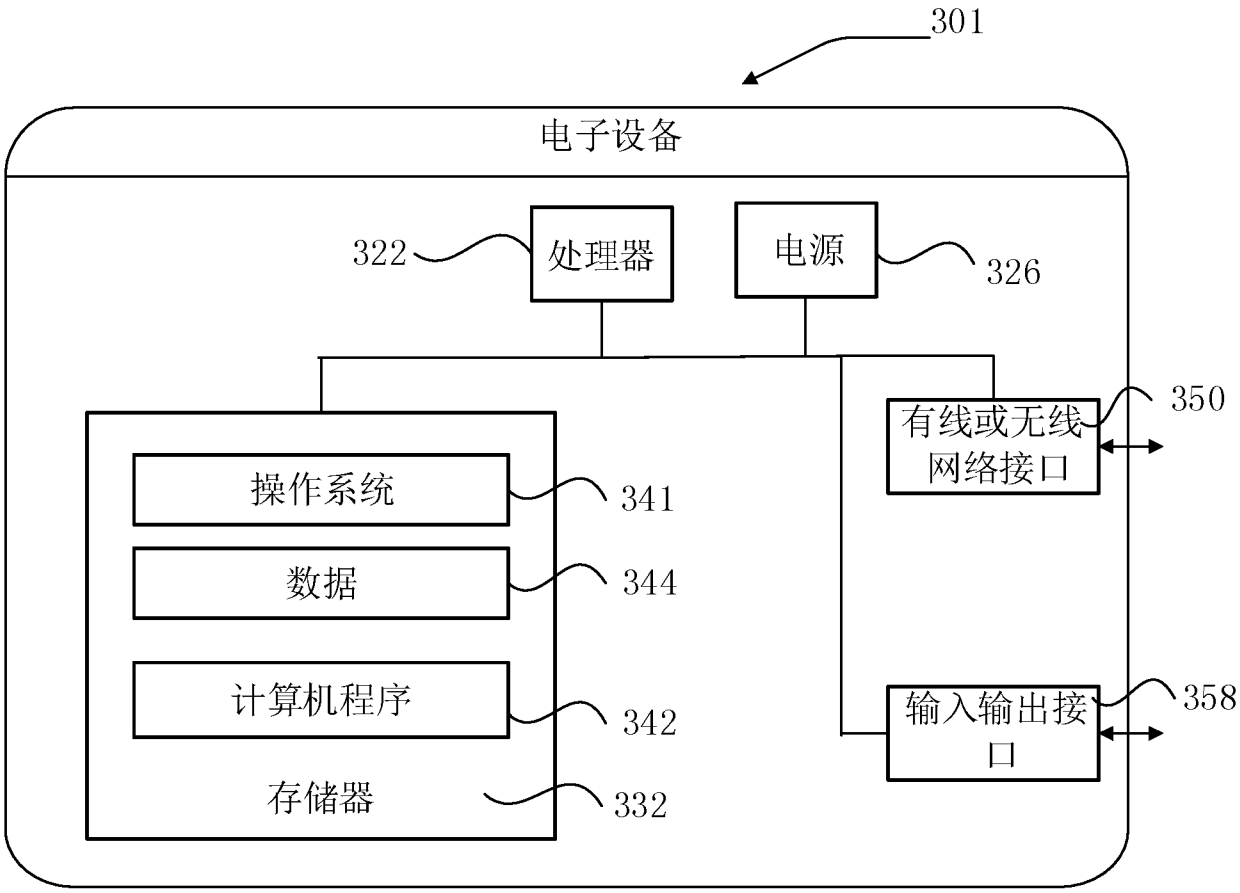

301
电子设备
322
处理器
电源
326
有线或无线网络接口
350
操作系统
341
数据
344
计算机程序
342
存储器
332
输入输出接口
358

图6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/089877

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/4401(2018.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: 启动, 安全, 签名, 验证, 镜像, 散列, 哈希, 编译, BMC, linux, startup, boot, kernel, mirror, image, hash, signature

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112463224 A (SUZHOU INSPUR INTELLIGENT TECHNOLOGY CO., LTD.) 09 March 2021 (2021-03-09) claims 1-10	1-10
X	CN 104156659 A (UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA) 19 November 2014 (2014-11-19) description, paragraphs [0038]-[0098] and figure 4	1-10
A	CN 109376550 A (ZHENGZHOU YUNHAI INFORMATION TECHNOLOGY CO., LTD.) 22 February 2019 (2019-02-22) entire document	1-10
A	CN 106384052 A (LANGCHAO ELECTRONIC INFORMATION INDUSTRY CO., LTD.) 08 February 2017 (2017-02-08) entire document	1-10
A	US 2010062844 A1 (BALLY GAMING, INC.) 11 March 2010 (2010-03-11) entire document	1-10

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2021	**11 August 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/089877

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 112463224 A	09 March 2021	None	
CN 104156659 A	19 November 2014	None	
CN 109376550 A	22 February 2019	None	
CN 106384052 A	08 February 2017	None	
US 2010062844 A1	11 March 2010	WO 2011059905 A1	19 May 2011

国际检索报告

国际申请号
PCT/CN2021/089877

A. 主题的分类

G06F 9/4401(2018.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT, CNKI, WPI, EPODOC：启动，安全，签名，验证，镜像，散列，哈希，编译，BMC，linux，startup，boot，kernel，mirror，image，hash，signature

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 112463224 A (苏州浪潮智能科技有限公司) 2021年 3月 9日 (2021-03-09) 权利要求1-10	1-10
X	CN 104156659 A (电子科技大学) 2014年 11月 19日 (2014-11-19) 说明书第[0038]-[0098]段以及附图4	1-10
A	CN 109376550 A (郑州云海信息技术有限公司) 2019年 2月 22日 (2019-02-22) 全文	1-10
A	CN 106384052 A (浪潮电子信息产业股份有限公司) 2017年 2月 8日 (2017-02-08) 全文	1-10
A	US 2010062844 A1 (BALLY GAMING, INC.) 2010年 3月 11日 (2010-03-11) 全文	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2021年 7月 20日	2021年 8月 11日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国 北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 梁艳 电话号码 86-(10)-53961298

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/089877

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 112463224 A	2021年 3月 9日	无	
CN 104156659 A	2014年 11月 19日	无	
CN 109376550 A	2019年 2月 22日	无	
CN 106384052 A	2017年 2月 8日	无	
US 2010062844 A1	2010年 3月 11日	WO 2011059905 A1	2011年 5月 19日