

(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
2024 年 12 月 26 日 (26.12.2024)



(10) 国际公布号
WO 2024/260299 A1

(51) 国际专利分类号:

G06F 21/51 (2013.01)

(21) 国际申请号:

PCT/CN2024/099283

(22) 国际申请日:

2024 年 6 月 14 日 (14.06.2024)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

202310728699.2 2023年6月19日 (19.06.2023) CN

(71) 申请人: 维沃移动通信有限公司(VIVO MOBILE COMMUNICATION CO., LTD.) [CN/CN]; 中国广东省东莞市长安镇维沃路 1 号, Guangdong 523863 (CN)。

(72) 发明人: 苏涛(SU, Tao); 中国广东省东莞市长安镇维沃路 1 号, Guangdong 523863 (CN)。 洪文博

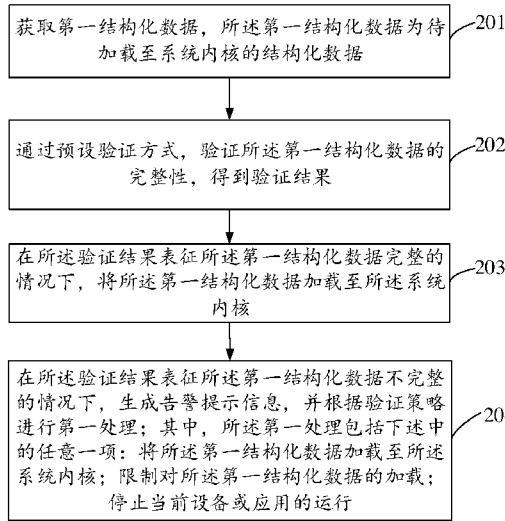
(HONG, Wenbo); 中国广东省东莞市长安镇维沃路 1 号, Guangdong 523863 (CN)。 成明江(CHENG, Mingjiang); 中国广东省东莞市长安镇维沃路 1 号, Guangdong 523863 (CN)。 何文登(HE, Wendeng); 中国广东省东莞市长安镇维沃路 1 号, Guangdong 523863 (CN)。 王尚之(WANG, Shangzhi); 中国广东省东莞市长安镇维沃路 1 号, Guangdong 523863 (CN)。 赵梓伊(ZHAO, Ziyi); 中国广东省东莞市长安镇维沃路 1 号, Guangdong 523863 (CN)。

(74) 代理人: 北京东方亿思知识产权代理有限公司(BEIJING EAST IP LTD.); 中国北京市东城区东长安街 1 号东方广场东方经贸城东 2 座 1601 室, Beijing 100738 (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,

(54) Title: SYSTEM LEGITIMACY VERIFICATION METHOD AND APPARATUS, AND ELECTRONIC DEVICE

(54) 发明名称: 系统合法性验证方法、装置及电子设备



201 ACQUIRE FIRST STRUCTURED DATA, WHEREIN THE FIRST STRUCTURED DATA IS STRUCTURED DATA TO BE LOADED TO A SYSTEM KERNEL
202 BY USING A PRESET VERIFICATION MODE, VERIFY THE INTEGRITY OF THE FIRST STRUCTURED DATA TO OBTAIN A VERIFICATION RESULT
203 IF THE VERIFICATION RESULT INDICATES THAT THE FIRST STRUCTURED DATA IS COMPLETE, LOAD THE FIRST STRUCTURED DATA TO THE SYSTEM KERNEL
204 IF THE VERIFICATION RESULT INDICATES THAT THE FIRST STRUCTURED DATA IS INCOMPLETE, GENERATE ALARM PROMPT INFORMATION, AND PERFORM FIRST PROCESSING ACCORDING TO A VERIFICATION POLICY, WHEREIN THE FIRST PROCESSING COMPRISES ANY ONE OF THE FOLLOWING: LOADING THE FIRST STRUCTURED DATA TO THE SYSTEM KERNEL; LIMITING THE LOADING OF THE FIRST STRUCTURED DATA; AND STOPPING THE RUNNING OF A CURRENT DEVICE OR APPLICATION

图 2

(57) Abstract: The present application relates to the field of kernel security and discloses a system legitimacy verification method and apparatus, and an electronic device. The method of the present application comprises: acquiring first structured data, wherein the first structured data is structured data to be loaded to a system kernel; by using a preset verification mode, verifying the integrity of the first structured data to obtain a verification result; if the verification result indicates that the first structured data is complete, loading the first structured data to the system kernel; and if the verification result indicates that the first structured data is incomplete, generating alarm prompt information, and performing first processing on the first structured data according to a verification policy, wherein the first processing comprises one of the following: loading the first structured data to the system kernel; limiting the loading of the first structured data; and stopping the running of a current device or application.

CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))。

(57) 摘要: 本申请公开了一种系统合法性验证方法、装置及电子设备, 属于内核安全领域。本申请的方法包括: 获取第一结构化数据, 所述第一结构化数据为待加载至系统内核的结构化数据; 通过预设验证方式, 验证所述第一结构化数据的完整性, 得到验证结果; 在所述验证结果表征所述第一结构化数据完整的情况下, 将所述第一结构化数据加载至所述系统内核; 在所述验证结果表征所述第一结构化数据不完整的情况下, 生成告警提示信息, 并根据验证策略, 对所述第一结构化数据进行第一处理; 其中, 所述第一处理包括下述中的一项: 将所述第一结构化数据加载至所述系统内核; 限制对所述第一结构化数据的加载; 停止当前设备或应用的运行。

系统合法性验证方法、装置及电子设备

相关申请的交叉引用

本申请主张在2023年06月19日在中国提交的中国专利申请202310728699.2的优先权，
5 其全部内容通过引用包含于此。

技术领域

本申请属于内核安全领域，具体涉及一种系统合法性验证方法、装置及电子设备。

10 背景技术

在移动终端启动的过程中，加载系统的合法性对设备安全性十分关键。如果加载的系统被破坏，例如加载了非法镜像，加载非法的内核模块等场景中，可以导致端侧系统被root、运行远程控制的病毒或木马等。进而导致用户手机内隐私数据的丢失、窃取，用户手机被远程控制等情况，造成用户对于手机的信任度降低。对于上述问题，现在主要的解决方案
15 为安全启动（Secure Boot）和验证启动（Verified Boot）。但是现有的安全启动和验证启动都仅是对于静态的系统镜像合法性进行的验证，无法实现对结构化数据的合法验证。

发明内容

本申请实施例的目的是提供一种系统合法性验证方法、装置及电子设备，能够解决现
20 有技术无法实现对结构化数据的合法验证的问题。

第一方面，本申请实施例提供了一种系统合法性验证方法，该方法包括：

获取第一结构化数据，所述第一结构化数据为待加载至系统内核的结构化数据；

通过预设验证方式，验证所述第一结构化数据的完整性，得到验证结果；

在所述验证结果表征所述第一结构化数据完整的情况下，将所述第一结构化数据加载
25 至所述系统内核；

在所述验证结果表征所述第一结构化数据不完整的情况下，生成告警提示信息，并根据验证策略进行第一处理；其中，所述第一处理包括下述中的任意一项：

将所述第一结构化数据加载至所述系统内核；

限制对所述第一结构化数据的加载；

30 停止当前设备或应用的运行。

第二方面，本申请实施例提供了一种系统合法性验证装置，包括：

第一获取模块，用于获取第一结构化数据，所述第一结构化数据为待加载至系统内核的结构化数据；

验证模块，用于通过预设验证方式，验证所述第一结构化数据的完整性，得到验证结

果；

第一处理模块，用于在所述验证结果表征所述第一结构化数据完整的情况下，将所述第一结构化数据加载至所述系统内核；

5 第二处理模块，用于在所述验证结果表征所述第一结构化数据不完整的情况下，生成告警提示信息，并根据验证策略进行第一处理；其中，所述第一处理包括下述中的任意一项：

将所述第一结构化数据加载至所述系统内核；

限制对所述第一结构化数据的加载；

停止当前设备或应用的运行。

10 第三方面，本申请实施例提供了一种电子设备，该电子设备包括处理器和存储器，所述存储器存储可在所述处理器上运行的程序或指令，所述程序或指令被所述处理器执行时实现如第一方面所述的系统合法性验证方法的步骤。

第四方面，本申请实施例提供了一种可读存储介质，所述可读存储介质上存储程序或指令，所述程序或指令被处理器执行时实现如第一方面所述的系统合法性验证方法的步骤。

15 第五方面，本申请实施例提供了一种芯片，所述芯片包括处理器和通信接口，所述通信接口和所述处理器耦合，所述处理器用于运行程序或指令，实现如第一方面所述的系统合法性验证方法。

第六方面，本申请实施例提供一种计算机程序产品，该计算机程序产品被存储在存储介质中，该计算机程序产品被至少一个处理器执行以实现如第一方面所述的系统合法性验证方法。

20 第七方面，本申请实施例提供了一种电子设备，所述电子设备被配置成执行如第一方面的系统合法性验证方法。

在本申请实施例中，首先，获取第一结构化数据，所述第一结构化数据为待加载至系统内核的结构化数据；然后，通过预设验证方式，验证所述第一结构化数据的完整性，得到验证结果；最后，在所述验证结果表征所述第一结构化数据完整的情况下，将所述第一结构化数据加载至所述系统内核；在所述验证结果表征所述第一结构化数据不完整的情况下，生成告警提示信息，并根据验证策略进行第一处理；其中，所述第一处理包括下述中的任意一项：将所述第一结构化数据加载至所述系统内核；限制对所述第一结构化数据的加载；停止当前设备或应用的运行，这样通过增加对于内核中加载结构化数据的合法性验证，将系统合法性验证的范围由静态的镜像合法性验证拓展到内核动态地加载的结构化数据合法性验证，从而实现了结构化数据的合法性验证。

附图说明

图1是本发明实施例的系统合法性验证框图之一；

35 图2是本发明实施例的系统合法性验证方法的流程示意图；

图 3 是本发明实施例的系统合法性验证框图之二；

图 4 是本发明实施例的系统合法性验证装置的模块示意图；

图 5 是本发明实施例的电子设备的硬件结构示意图之一；

图 6 是本发明实施例的电子设备的硬件结构示意图之二。

5

具体实施方式

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获得的所有其他实施例，都属于本申请保护的范围。

10 本申请的说明书和权利要求书中的术语“第一”、“第二”等是用于区别类似的对象，而不用来描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便本申请的实施例能够以除了在这里图示或描述的那些以外的顺序实施，且“第一”、“第二”等所区分的对象通常为一类，并不限定对象的个数，例如第一对象可以是一个，也可以是多个。此外，说明书以及权利要求中“和/或”表示所连接对象的至少其中之一，字符
15 “/”，一般表示前后关联对象是一种“或”的关系。

需要说明的是，本发明实施例的方法是在安全启动和验证启动的基础上，增加的对于系统内核中加载的结构化数据的完整性验证，该方法是以系统加载的结构化数据完整性为基础，辅助验证运行系统的合法性。

参见图 1，系统合法性验证依次包括安全启动阶段、验证启动阶段和结构化数据完整性
20 验证阶段。具体包括以下步骤：

步骤 101，移动终端在启动过程中，通过安全启动验证硬件相关的模块。

即在硬件作为最先启动加载的模块，对后续加载的模块进行签名验证。只有在签名验证通过后才加载对应的模块，否则不允许加载（即启动失败）。

步骤 102，完成安全启动验证硬件相关模块后，进入验证启动阶段。即由最先启动的模
25 块，对之后需要加载的镜像进行哈希值验证。只有在哈希值验证通过后，加载对应的系统镜像，否则进行报错（启动可以继续）。

这里，最先启动的模块通常为安全启动验证的 Boot Loader，Boot Loader 为引导加载程序，其在操作系统内核运行之前运行。

步骤 103，完成验证启动的步骤后，系统内核镜像被加载，拉起内核 init 进程（内核中的第一个进程）。之后，进入结构化数据完整性验证阶段。具体的，进程启动后，通过在特定位置添加 hook 的方式，对加载进入内存的结构化数据进行哈希值计算，并且将哈希值传递给运行于可信执行环境（Trusted Execution Environment, TEE）中的受信任的应用（Trusted Application, TA）进行本地验证，或者通过远程证明协议进行远程验证。
30

下面结合附图，通过具体的实施例及其应用场景对本申请实施例提供的系统合法性验证方法进行详细地说明。
35

如图 2 所示，为本发明实施例提供的系统合法性验证方法的流程示意图。该方法可具体包括：

步骤 201，获取第一结构化数据，所述第一结构化数据为待加载至系统内核的结构化数据；

5 可选地，所述第一结构化数据包括第二结构化数据和第三结构化数据，其中，所述第二结构化数据为上层系统中所包含的结构化数据，所述第三结构化数据为上层系统的应用中所包含的结构化数据。

其中，上层系统安装于执行该方法的电子设备内，是在系统内核之上的系统，应理解为高级操作系统（High-level Operation System, HLOS）。这里，上层系统需要加载至系统内
10 核的结构化数据包括但不限于：内核模块的结构化数据和系统服务的结构化数据。

步骤 202，通过预设验证方式，验证所述第一结构化数据的完整性，得到验证结果；

这里，预设验证方式包括本地验证方式和远程验证方式两种。其中，本地验证方式指的是利用运行于 TEE 中的 TA 进行本地验证的方式，远程验证方式指的是利用运行于 TEE 中 TA，通过与 TA 通信的远程服务器（第三方服务器）进行远程验证的方式。具体的验证
15 过程参见下述实施例部分。

步骤 203，在所述验证结果表征所述第一结构化数据完整的情况下，将所述第一结构化数据加载至所述系统内核；

需要说明的是，验证结果表征第一结构化数据完整，则说明系统运行的服务和操作系统是安全的，没有被攻击的风险。此时，将第一结构化数据加载至该系统内核。

20 步骤 204，在所述验证结果表征所述第一结构化数据不完整的情况下，生成告警提示信息，并根据验证策略进行第一处理；其中，所述第一处理包括下述中的任意一项：

将所述第一结构化数据加载至所述系统内核；

限制对所述第一结构化数据的加载；

停止当前设备或应用的运行。

25 这里，验证结果表征第一结构化数据不完整，则说明系统运行的服务和/或操作系统是不安全的，有被攻击的风险。此时，生成告警提示信息，用于提示用户当前设备的系统完整性被破坏；另外是否将第一结构化数据加载至该系统内核由验证策略决定。这里，根据预设策略将所述第一结构化数据加载至所述系统内核，是考虑到有些结构化数据若不加载的话会导致系统死机或者软件崩溃。

30 需要说明的是，限制对第一结构化数据的加载指的是不对第一结构化数据进行加载，或者是禁止加载第一结构化数据。

本发明实施例的系统合法性验证方法，以系统加载的结构化数据完整性为基础，辅助验证运行系统的合法性，降低了系统被非法刷机和攻破的风险。

在一可选地实施例中，上述步骤 201，获取第一结构化数据，具体包括：

35 步骤 2011，在完成安全启动和验证启动后，且在系统文件的预设存储位置检测到待验

证的所述第一结构化数据的情况下，在所述预设存储位置获取所述第一结构化数据。

具体的，基于预先存储的系统度量策略配置文件，在系统文件的预设存储位置检测是否存在需要进行验证的第一结构化数据。这里，预设存储位置是预先存储于系统度量策略配置文件中的需要进行数据完整性验证的结构化数据对应的文件存储位置，由系统编译服务器下发给执行该方法的电子设备。

具体的，可以通过在预设存储位置添加 hook（如内核 XXX_exec() 和 XXX_execve() 函数中）的方式，抽取第一结构化数据。

也就是说，在实际应用中，并不是所有的结构化数据都需要进行数据完整性验证，这样的话会导致系统启动速度慢效率低，所以只是对需要进行数据完整性验证的结构化数据进行验证，而哪些结构化数据是需要进行数据完整性验证的，是由系统安全工程师根据经验标定出的，从而确保这些结构化数据在已知的情况下，系统的合法性已知。

在一可选地实施例中，上述步骤 202，通过预设验证方式，验证所述第一结构化数据的完整性，得到验证结果，包括：

步骤 2021，对所述第一结构化数据进行哈希计算，得到第一哈希值；

其中，第一哈希值可以包括内核模块的结构化数据经哈希计算后的哈希值、系统服务的结构化数据经哈希计算后的哈希值和上层系统中的应用需要加载至系统内核的结构化数据经哈希计算后的哈希值。

步骤 2022，将所述第一哈希值传递至运行于可信执行环境中的受信任的应用 TA；

步骤 2023，通过 TA，将所述第一哈希值进行验证处理，获得验证结果。

这里的 TA 设置于执行该方法的电子设备中，可以是参与本地验证的 TA，也可以是参与远程验证的 TA。

下面说明该 TA 为参与本地验证的 TA 时，通过 TA，将所述第一哈希值进行验证处理，获得验证结果，具体可包括：

步骤 20231a，通过 TA，将所述第一哈希值与预先存储的第二哈希值进行比较，获得比较结果，所述第二哈希值为预先对所述第一结构化数据进行哈希计算后得到的正确哈希值；

这里，需要进行数据完整性验证的结构化数据经哈希计算后对应的正确哈希值预先存储在验证 TA 策略配置文件中，该验证 TA 策略配置文件由系统编译服务器下发给执行该方法的电子设备。

步骤 20232a，在比较结果为所述第一哈希值与所述第二哈希值相同的情况下，得到表征所述第一结构化数据完整的验证结果；

步骤 20233a，在比较结果为所述第一哈希值与所述第二哈希值不同的情况下，得到表征所述第一结构化数据不完整的验证结果。

参见图 3，下面通过一示例从安全启动阶段、验证启动阶段和结构化数据完整性验证阶段（该阶段中结构化数据完整性验证通过 TA 执行本地验证实现），整体说明系统合法性验证的实现过程。

步骤 301, 移动终端在启动过程中, 首先加载 bootROM, 通过存储于该模块中的公钥对 XBL 模块 (即启动模块) 进行签名验证, 签名验证成功后进入步骤 302; 否则停止启动。

其中, bootROM 是嵌入处理器芯片内的一小块掩膜 ROM 或写保护内存, 它包含处理器在上电或复位时执行的第一个代码。bootROM 由芯片供应商提供, 该模块被认为是设备的可信根, 由芯片厂商硬化在芯片中, 模块代码无法进行更改。芯片厂商将自身相关模块签名使用的公私钥对中的公钥存储于该模块。

步骤 302, XBL 模块加载后, 使用公钥对 TEE 模块进行签名验证, 签名验证成功后进入步骤 303; 否则停止启动。

需要说明的是, 该步骤中的公钥上述步骤 301 中的公钥。

10 步骤 303, TEE 模块加载后, 启动基于 TEE 的哈希值验证 TA, 并使用公钥对虚拟机管理程序 Hypervisor 模块进行签名验证, 签名验证成功后进入步骤 304; 否则停止启动。

步骤 304, Hypervisor 模块加载后, 启动基于 hypervisor 的虚拟机运行哈希值验证 TA, 并使用公钥对 APPSBL 模块 (即上层系统的启动模块) 进行签名验证, 签名验证成功后进入步骤 305; 否则停止启动。

15 上述步骤 301~步骤 304 对应的是安全启动阶段。

步骤 305, Hypervisor 模块加载上层系统的镜像, 至此, 启动进入验证启动阶段。加载镜像的哈希值和存储于系统分区 (如 vbmeta 分区) 的白名单进行对比, 当匹配时正常加载镜像, 否则发出警告。

上述步骤 305 对应的是验证启动阶段。

20 步骤 306, HLOS 启动后, 通过在内核特定位位置添加 hook (如内核 XXX_exec()和 XXX_execve()函数中) 的方式, 对加载至内存的结构化数据进行哈希值计算并且将哈希值传递给参与本地验证的 TA。

这里, 加载至内存的结构化数据包括但不限于: 内核模块的结构化数据和系统服务的结构化数据。

25 同理, 运行在 HLOS 中的 APP (上层系统的应用) 需要加载至系统内存的结构化数据进行哈希值计算, 并将哈希值传递给参与本地验证的 TA。

步骤 307, 参与本地验证的 TA 在接收到哈希值后, 与存储于可信环境中的白名单进行对比; 如果对比出错, 则对发出告警, 或者限制对应的结构化数据加载, 停止设备或应用的使用。

30 应理解, 可信环境中的白名单中包括结构化数据经哈希计算后对应的正确哈希值。

步骤 306~步骤 307 对应的是结构化数据完整性验证阶段。

下面说明该 TA 为参与远程验证的 TA 时, 通过 TA, 将所述第一哈希值进行验证处理, 获得验证结果, 具体可包括:

35 步骤 20231b, 由该 TA, 利用第一随机数对所述第一哈希值进行签名, 并将签名后的第一哈希值发送至远程服务器, 其中, 所述第一随机数通过所述 TA 与所述远程服务器之间的

交互获得；

步骤 20232b，获取所述远程服务器发送的验证结果，所述验证结果由所述远程服务器基于所述签名后的第一哈希值对所述第一结构化数据进行完整性验证后得到。

该实施例中，结构化数据的完整性验证由远程服务器（第三方）完成，这样可以减轻
5 执行电子设备的处理负担。

需要说明的是，在实际应用中，并不是所有的结构化数据都需要进行数据完整性验证，这样的话会导致系统启动速度慢效率低，所以只是对需要进行数据完整性验证的结构化数据进行验证，而哪些结构化数据是需要进行数据完整性验证的，是由系统安全工程师根据经验标定出的。步骤如下：

10 步骤 401，系统安全工程师根据经验标定出需要进行验证的结构化数据，确保这些结构化数据在已知的情况下，系统的合法性已知。

这就需要对于系统内核和系统框架（如安卓框架）镜像有深层次的了解。其中可通过结构化数据的文件系统的位置，类型等属性设定系统度量策略。

步骤 402，系统编译工程师根据步骤 401 生成的列表，在不同型号的设备进行系统编译
15 的过程中，更新系统度量策略配置文件。

其中，系统度量策略配置文件的文件信息包括对于该设备型号的系统需要执行计算的结构化数据列表，以及对应结构化数据的位置指示信息。这样待之后下发给电子设备后，该电子设备的内核依据该系统度量策略配置文件中的结构化数据列表和位置指示信息，对加载至内核的结构化数据进行计算（比如进行哈希计算）。

20 步骤 403，系统 TA 工程师根据步骤 401 生成的列表，将结构化数据的正确哈希值进行记录，并且生成对应的验证 TA 策略配置文件。

其中，验证 TA 策略配置文件的文件信息包括需要进行数据完整性验证的结构化数据列表、结构化数据经哈希计算后得到的正确哈希值以及不同的结构化数据验证失败时对应的验证策略。这样待之后下发给电子设备后，该电子设备中的验证 TA 依据该验证 TA 策略配
25 置文件，对加载的结构化数据进行验证。

步骤 404，系统编译服务器通过新机部署或 OTA 下发的方式，将系统度量策略配置文件和验证 TA 策略配置文件配置到电子设备。即在一可选地实施例中，本发明的方法还可包括：

步骤 405，获取系统编译服务器下发的系统度量策略配置文件和验证 TA 策略配置文件；

30 其中，所述系统度量策略配置文件用于获取所述第一结构化数据；所述系统度量策略配置文件的文件信息包括需要进行数据完整性验证的结构化数据列表和位置指示信息，所述位置指示信息用于指示需要进行数据完整性验证的结构化数据对应的文件存储位置；

所述验证 TA 策略配置文件用于在验证所述第一结构化数据不完整情况下，获取所述验证策略；所述验证 TA 策略配置文件的文件信息包括：需要进行数据完整性验证的结构化数据列表、需要进行数据完整性验证的结构化数据经哈希计算后得到的正确哈希值以及不同
35

的结构化数据验证失败时对应的验证策略。

应理解，不同的结构化数据验证失败时对应的验证策略也就是上述实施例中的验证策略。

步骤 406，存储所述系统度量策略配置文件和所述验证 TA 策略配置文件。

5 之后，电子设备通过系统度量策略配置文件，对加载的结构化数据进行计算，例如 do_exec(), open_exec() 等，并将计算结果传递给验证 TA。

验证 TA 根据验证 TA 策略配置文件，验证结构化数据，并作出对应反馈。

本发明实施例的系统合法性验证方法，首先，获取第一结构化数据，所述第一结构化数据为待加载至系统内核的结构化数据；然后，通过预设验证方式，验证所述第一结构化数据的完整性，得到验证结果；最后，在所述验证结果表征所述第一结构化数据完整的情况下，将所述第一结构化数据加载至所述系统内核；在所述验证结果表征所述第一结构化数据不完整的情况下，生成告警提示信息，并根据验证策略进行第一处理；其中，所述第一处理包括下述中的任意一项：将所述第一结构化数据加载至所述系统内核；限制对所述第一结构化数据的加载；停止当前设备或应用的运行，这样通过增加对于内核中加载结构化数据的合法性验证，将系统合法性验证的范围由静态的镜像合法性验证拓展到内核动态地加载的结构化数据合法性验证，从而实现了对于结构化数据的合法性验证。

本申请实施例提供的系统合法性验证方法，执行主体可以为系统合法性验证装置。本申请实施例中以系统合法性验证装置执行系统合法性验证方法为例，说明本申请实施例提供的系统合法性验证装置。

20 如图 4 所示，本发明实施例还提供一种系统合法性验证装置，该装置 400 可包括：

第一获取模块 410，用于获取第一结构化数据，所述第一结构化数据为待加载至系统内核的结构化数据；

验证模块 420，用于通过预设验证方式，验证所述第一结构化数据的完整性，得到验证结果；

25 第一处理模块 430，用于在所述验证结果表征所述第一结构化数据完整的情况下，将所述第一结构化数据加载至所述系统内核；

第二处理模块 440，用于在所述验证结果表征所述第一结构化数据不完整的情况下，生成告警提示信息，并根据验证策略进行第一处理；其中，所述第一处理包括下述中的任意一项：

30 将所述第一结构化数据加载至所述系统内核；

限制对所述第一结构化数据的加载；

停止当前设备或应用的运行。

可选地，所述第一获取模块 410 包括：

35 第一获取单元，用于在完成安全启动和验证启动后，且在系统文件的预设存储位置检测到待验证的所述第一结构化数据的情况下，在所述预设存储位置获取所述第一结构化数

据。

可选地，所述第一结构化数据包括第二结构化数据和第三结构化数据，其中，所述第二结构化数据为上层系统中所包含的结构化数据，所述第三结构化数据为上层系统的应用中所包含的结构化数据。

5 可选地，所述验证模块 420，包括：

第一计算单元，用于对所述第一结构化数据进行哈希计算，得到第一哈希值；

第一处理单元，用于将所述第一哈希值传递至运行于可信执行环境中的受信任的应用 TA；

验证单元，用于通过 TA，将所述第一哈希值进行验证处理，获得验证结果。

10 可选地，所述装置 400 还包括：

第二获取模块，用于获取系统编译服务器下发的系统度量策略配置文件和验证 TA 策略配置文件；

存储模块，用于存储所述系统度量策略配置文件和所述验证 TA 策略配置文件；

15 其中，所述系统度量策略配置文件用于获取所述第一结构化数据；所述系统度量策略配置文件的文件信息包括需要进行数据完整性验证的结构化数据列表和位置指示信息，所述位置指示信息用于指示需要进行数据完整性验证的结构化数据对应的文件存储位置；

20 所述验证 TA 策略配置文件用于在验证所述第一结构化数据不完整情况下，获取所述验证策略；所述验证 TA 策略配置文件的文件信息包括：需要进行数据完整性验证的结构化数据列表、需要进行数据完整性验证的结构化数据经哈希计算后得到的正确哈希值以及不同的结构化数据验证失败时对应的验证策略。

25 本发明实施例的系统合法性验证装置，首先，获取第一结构化数据，所述第一结构化数据为待加载至系统内核的结构化数据；然后，通过预设验证方式，验证所述第一结构化数据的完整性，得到验证结果；最后，在所述验证结果表征所述第一结构化数据完整的情况下，将所述第一结构化数据加载至所述系统内核；在所述验证结果表征所述第一结构化数据不完整的情况下，生成告警提示信息，并根据验证策略进行第一处理；其中，所述第一处理包括下述中的任意一项：将所述第一结构化数据加载至所述系统内核；限制对所述第一结构化数据的加载；停止当前设备或应用的运行，这样通过增加对于内核中加载结构化数据的合法性验证，将系统合法性验证的范围由静态的镜像合法性验证拓展到内核动态地加载的结构化数据合法性验证，从而实现了结构化数据的合法性验证。

30 本申请实施例中的系统合法性验证装置可以是电子设备，也可以是电子设备中的部件，例如集成电路或芯片。该电子设备可以是终端，也可以为除终端之外的其他设备。示例性的，电子设备可以为手机、平板电脑、笔记本电脑、掌上电脑、车载电子设备、移动上网装置（Mobile Internet Device, MID）、增强现实(augmented reality, AR)/虚拟现实(virtual reality, VR)设备、机器人、可穿戴设备、超级移动个人计算机(ultra-mobile personal computer, UMPC)、上网本或者个人数字助理（personal digital assistant, PDA）等，网络附属存储器

35

(Network Attached Storage, NAS)、个人计算机(personal computer, PC)、电视机(television, TV)、柜员机或者自助机等, 本申请实施例不作具体限定。

本申请实施例中的系统合法性验证装置可以为具有操作系统的装置。该操作系统可以为安卓(Android)操作系统, 可以为 IOS 操作系统, 还可以为其他可能的操作系统, 本申请实施例不作具体限定。

本申请实施例提供的系统合法性验证装置能够实现图 1 至图 3 的方法实施例实现的各个过程, 为避免重复, 这里不再赘述。

可选地, 如图 5 所示, 本申请实施例还提供一种电子设备 500, 包括处理器 501 和存储器 502, 存储器 502 上存储有可在所述处理器 501 上运行的程序或指令, 该程序或指令被处理器 501 执行时实现上述系统合法性验证方法实施例的各个步骤, 且能达到相同的技术效果, 为避免重复, 这里不再赘述。

需要说明的是, 本申请实施例中的电子设备包括上述所述的移动电子设备和非移动电子设备。

图 6 为实现本申请实施例的一种电子设备的硬件结构示意图。

该电子设备 600 包括但不限于: 射频单元 601、网络模块 602、音频输出单元 603、输入单元 604、传感器 605、显示单元 606、用户输入单元 607、接口单元 608、存储器 609、以及处理器 610 等部件。

本领域技术人员可以理解, 电子设备 600 还可以包括给各个部件供电的电源(比如电池), 电源可以通过电源管理系统与处理器 610 逻辑相连, 从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。图 6 中示出的电子设备结构并不构成对电子设备的限定, 电子设备可以包括比图示更多或更少的部件, 或者组合某些部件, 或者不同的部件布置, 在此不再赘述。

其中, 处理器 610 用于:

获取第一结构化数据, 所述第一结构化数据为待加载至系统内核的结构化数据;

通过预设验证方式, 验证所述第一结构化数据的完整性, 得到验证结果;

在所述验证结果表征所述第一结构化数据完整的情况下, 将所述第一结构化数据加载至所述系统内核;

在所述验证结果表征所述第一结构化数据不完整的情况下, 生成告警提示信息, 并根据验证策略进行第一处理; 其中, 所述第一处理包括下述中的任意一项: 将所述第一结构化数据加载至所述系统内核; 限制对所述第一结构化数据的加载; 停止当前设备或应用的运行。

本发明实施例的电子设备, 通过增加对于内核中加载结构化数据的合法性验证, 将系统合法性验证的范围由静态的镜像合法性验证拓展到内核动态地加载的结构化数据合法性验证, 从而实现了结构化数据的合法性验证。

可选地, 处理器 610 还用于:

在完成安全启动和验证启动后，且在系统文件的预设存储位置检测到待验证的第一结构化数据的情况下，在所述预设存储位置获取所述第一结构化数据。

可选地，所述第一结构化数据包括第二结构化数据和第三结构化数据，其中，所述第二结构化数据为上层系统中所包含的结构化数据，所述第三结构化数据为上层系统的应用中所包含的结构化数据。

可选地，处理器 610 还用于：

对所述第一结构化数据进行哈希计算，得到第一哈希值；

将所述第一哈希值传递至运行于可信执行环境中的受信任的应用 TA；

通过 TA，将所述第一哈希值进行验证处理，获得验证结果。

可选地，处理器 610 还用于：

获取系统编译服务器下发的系统度量策略配置文件和验证 TA 策略配置文件；

存储所述系统度量策略配置文件和所述验证 TA 策略配置文件；

其中，所述系统度量策略配置文件用于获取所述第一结构化数据；所述系统度量策略配置文件的文件信息包括需要进行数据完整性验证的结构化数据列表和位置指示信息，所述位置指示信息用于指示需要进行数据完整性验证的结构化数据对应的文件存储位置；

所述验证 TA 策略配置文件用于在验证所述第一结构化数据不完整情况下，获取所述验证策略；所述验证 TA 策略配置文件的文件信息包括：需要进行数据完整性验证的结构化数据列表、需要进行数据完整性验证的结构化数据经哈希计算后得到的正确哈希值以及不同的结构化数据验证失败时对应的验证策略。

应理解的是，本申请实施例中，输入单元 604 可以包括图形处理器 (Graphics Processing Unit, GPU) 6041 和麦克风 6042，图形处理器 6041 对在视频捕获模式或图像捕获模式中由图像捕获装置（如摄像头）获得的静态图片或视频的图像数据进行处理。显示单元 606 可包括显示面板 6061，可以采用液晶显示器、有机发光二极管等形式来配置显示面板 6061。用户输入单元 607 包括触控面板 6071 以及其他输入设备 6072 中的至少一种。触控面板 6071，也称为触摸屏。触控面板 6071 可包括触摸检测装置和触摸控制器两个部分。其他输入设备 6072 可以包括但不限于物理键盘、功能键（比如音量控制按键、开关按键等）、轨迹球、鼠标、操作杆，在此不再赘述。

存储器 609 可用于存储软件程序以及各种数据。存储器 609 可主要包括存储程序或指令的第一存储区和存储数据的第二存储区，其中，第一存储区可存储操作系统、至少一个功能所需的应用程序或指令（比如声音播放功能、图像播放功能等）等。此外，存储器 609 可以包括易失性存储器或非易失性存储器，或者，存储器 609 可以包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(Read-Only Memory, ROM)、可编程只读存储器(Programmable ROM, PROM)、可擦除可编程只读存储器(Erasable PROM, EPROM)、电可擦除可编程只读存储器(Electrically EPROM, EEPROM)或闪存。易失性存储器可以是随机存取存储器(Random Access Memory, RAM)，静态随机存取存储器(Static

RAM, SRAM)、动态随机存取存储器(Dynamic RAM, DRAM)、同步动态随机存取存储器(Synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器(Double Data Rate SDRAM, DDRSDRAM)、增强型同步动态随机存取存储器(Enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器(Synch link DRAM, SLDRAM)和直接内存总线随机存取存储器(Direct Rambus RAM, DRRAM)。本申请实施例中的存储器 609 包括但不限于这些和任意其它适合类型的存储器。

处理器 610 可包括一个或多个处理单元;可选的,处理器 610 集成应用处理器和调制解调处理器,其中,应用处理器主要处理涉及操作系统、用户界面和应用程序等的操作,调制解调处理器主要处理无线通信信号,如基带处理器。可以理解的是,上述调制解调处理器也可以不集成到处理器 610 中。

本申请实施例还提供一种可读存储介质,所述可读存储介质上存储有程序或指令,该程序或指令被处理器执行时实现上述系统合法性验证方法实施例的各个过程,且能达到相同的技术效果,为避免重复,这里不再赘述。

其中,所述处理器为上述实施例中所述的电子设备中的处理器。所述可读存储介质,包括计算机可读存储介质,如计算机只读存储器 ROM、随机存取存储器 RAM、磁碟或者光盘等。

本申请实施例另提供了一种芯片,所述芯片包括处理器和通信接口,所述通信接口和所述处理器耦合,所述处理器用于运行程序或指令,实现上述系统合法性验证方法实施例的各个过程,且能达到相同的技术效果,为避免重复,这里不再赘述。

应理解,本申请实施例提到的芯片还可以称为系统级芯片、系统芯片、芯片系统或片上系统芯片等。

本申请实施例提供一种计算机程序产品,该计算机程序产品被存储在存储介质中,该计算机程序产品被至少一个处理器执行以实现如上述系统合法性验证方法实施例的各个过程,且能达到相同的技术效果,为避免重复,这里不再赘述。

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。此外,需要指出的是,本申请实施方式中的方法和装置的范围不限按示出或讨论的顺序来执行功能,还可包括根据所涉及的功能按基本同时的方式或按相反的顺序来执行功能,例如,可以按不同于所描述的次序来执行所描述的方法,并且还可以添加、省去、或组合各种步骤。另外,参照某些示例所描述的特征可在其他示例中被组合。

通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者

是更佳的实施方式。基于这样的理解，本申请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计算机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（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端（可以是手机，计算机，服务器，或者网络设备等等）执行本申请各个实施例所述的方法。

- 5 上面结合附图对本申请的实施例进行了描述，但是本申请并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本申请的启示下，在不脱离本申请宗旨和权利要求所保护的范围情况下，还可做出很多形式，均属于本申请的保护之内。

权 利 要 求 书

1. 一种系统合法性验证方法，包括：

获取第一结构化数据，所述第一结构化数据为待加载至系统内核的结构化数据；

通过预设验证方式，验证所述第一结构化数据的完整性，得到验证结果；

5 在所述验证结果表征所述第一结构化数据完整的情况下，将所述第一结构化数据加载至所述系统内核；

在所述验证结果表征所述第一结构化数据不完整的情况下，生成告警提示信息，并根据验证策略进行第一处理；其中，所述第一处理包括下述中的任意一项：

将所述第一结构化数据加载至所述系统内核；

10 限制对所述第一结构化数据的加载；

停止当前设备或应用的运行。

2. 根据权利要求 1 所述的方法，其中，所述获取第一结构化数据，包括：

在完成安全启动和验证启动后，且在系统文件的预设存储位置检测到待验证的所述第一结构化数据的情况下，在所述预设存储位置获取所述第一结构化数据。

15 3. 根据权利要求 1 所述的方法，其中，所述第一结构化数据包括第二结构化数据和第三结构化数据，其中，所述第二结构化数据为上层系统中所包含的结构化数据，所述第三结构化数据为上层系统的应用中所包含的结构化数据。

4. 根据权利要求 1 所述的方法，其中，通过预设验证方式，验证所述第一结构化数据的完整性，得到验证结果，包括：

20 对所述第一结构化数据进行哈希计算，得到第一哈希值；

将所述第一哈希值传递至运行于可信执行环境中的受信任的应用 TA；

通过 TA，将所述第一哈希值进行验证处理，获得验证结果。

5. 根据权利要求 1 所述的方法，还包括：

获取系统编译服务器下发的系统度量策略配置文件和验证 TA 策略配置文件；

25 存储所述系统度量策略配置文件和所述验证 TA 策略配置文件；

其中，所述系统度量策略配置文件用于获取所述第一结构化数据；所述系统度量策略配置文件的文件信息包括需要进行数据完整性验证的结构化数据列表和位置指示信息，所述位置指示信息用于指示需要进行数据完整性验证的结构化数据对应的文件存储位置；

30 所述验证 TA 策略配置文件用于在验证所述第一结构化数据不完整情况下，获取所述验证策略；所述验证 TA 策略配置文件的文件信息包括：需要进行数据完整性验证的结构化数据列表、需要进行数据完整性验证的结构化数据经哈希计算后得到的正确哈希值以及不同的结构化数据验证失败时对应的验证策略。

6. 一种系统合法性验证装置，包括：

35 第一获取模块，用于获取第一结构化数据，所述第一结构化数据为待加载至系统内核的结构化数据；

验证模块，用于通过预设验证方式，验证所述第一结构化数据的完整性，得到验证结果；

第一处理模块，用于在所述验证结果表征所述第一结构化数据完整的情况下，将所述第一结构化数据加载至所述系统内核；

5 第二处理模块，用于在所述验证结果表征所述第一结构化数据不完整的情况下，生成告警提示信息，并根据验证策略进行第一处理；其中，所述第一处理包括下述中的一项：

将所述第一结构化数据加载至所述系统内核；

限制对所述第一结构化数据的加载；

停止当前设备或应用的运行。

10 7. 根据权利要求 6 所述的装置，其中，所述第一获取模块包括：

第一获取单元，用于在完成安全启动和验证启动后，且在系统文件的预设存储位置检测到待验证的所述第一结构化数据的情况下，在所述预设存储位置获取所述第一结构化数据。

8. 根据权利要求 6 所述的装置，其中，所述第一结构化数据包括第二结构化数据和第三结构化数据，其中，所述第二结构化数据为上层系统中所包含的结构化数据，所述第三结构化数据为上层系统的应用中所包含的结构化数据。

9. 根据权利要求 6 所述的装置，其中，所述验证模块，包括：

第一计算单元，用于对所述第一结构化数据进行哈希计算，得到第一哈希值；

第一处理单元，用于将所述第一哈希值传递至运行于可信执行环境中的受信任的应用

20 TA；

验证单元，用于通过 TA，将所述第一哈希值进行验证处理，获得验证结果。

10. 根据权利要求 6 所述的装置，还包括：

第二获取模块，用于获取系统编译服务器下发的系统度量策略配置文件和验证 TA 策略配置文件；

25 存储模块，用于存储所述系统度量策略配置文件和所述验证 TA 策略配置文件；

其中，所述系统度量策略配置文件用于获取所述第一结构化数据；所述系统度量策略配置文件的文件信息包括需要进行数据完整性验证的结构化数据列表和位置指示信息，所述位置指示信息用于指示需要进行数据完整性验证的结构化数据对应的文件存储位置；

所述验证 TA 策略配置文件用于在验证所述第一结构化数据不完整情况下，获取所述验证策略；所述验证 TA 策略配置文件的文件信息包括：需要进行数据完整性验证的结构化数据列表、需要进行数据完整性验证的结构化数据经哈希计算后得到的正确哈希值以及不同的结构化数据验证失败时对应的验证策略。

11. 一种电子设备，包括处理器和存储器，所述存储器存储可在所述处理器上运行的程序或指令，所述程序或指令被所述处理器执行时实现如权利要求 1 至 5 任一项所述的系统合法性验证方法的步骤。

12. 一种可读存储介质，所述可读存储介质上存储程序或指令，所述程序或指令被处理器执行时实现如权利要求 1 至 5 任一项所述的系统合法性验证方法的步骤。

13. 一种芯片，包括处理器和通信接口，所述通信接口和所述处理器耦合，所述处理器用于运行程序或指令，实现如权利要求 1-5 中任一项所述的系统合法性验证方法的步骤。

5 14. 一种计算机程序产品，所述计算机程序产品被存储在非易失的存储介质中，所述计算机程序产品被至少一个处理器执行以实现如权利要求 1-5 中任一项所述的系统合法性验证方法的步骤。

15. 一种电子设备，所述电子设备被配置成执行如权利要求 1-5 中任一项所述的系统合法性验证方法的步骤。

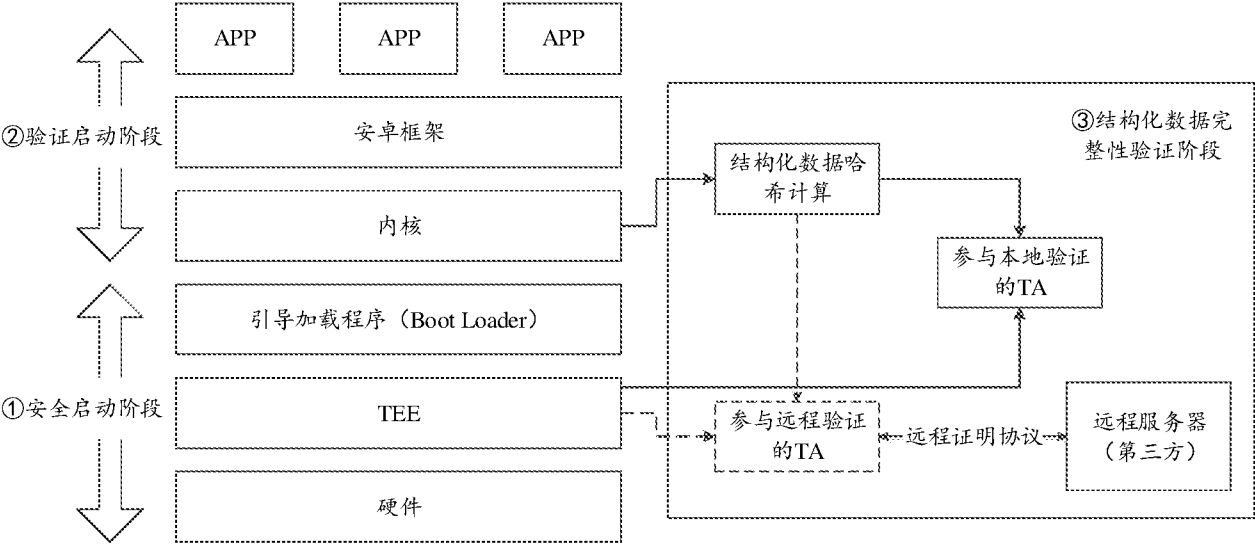


图 1

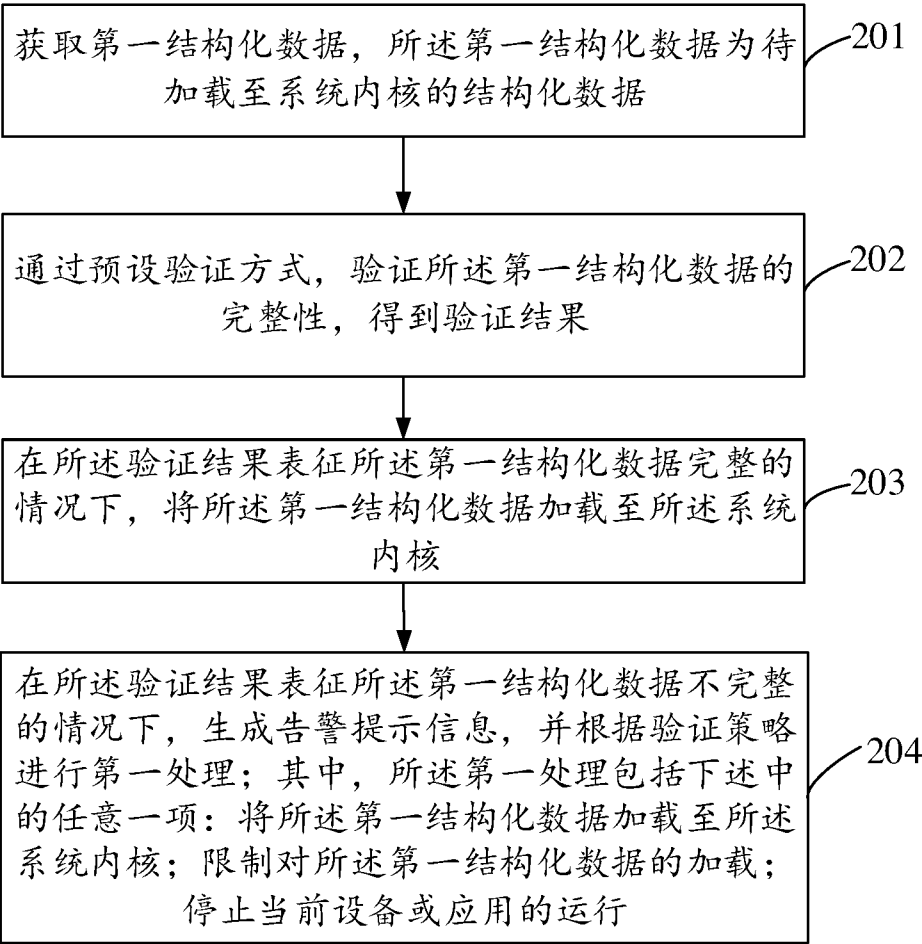


图 2

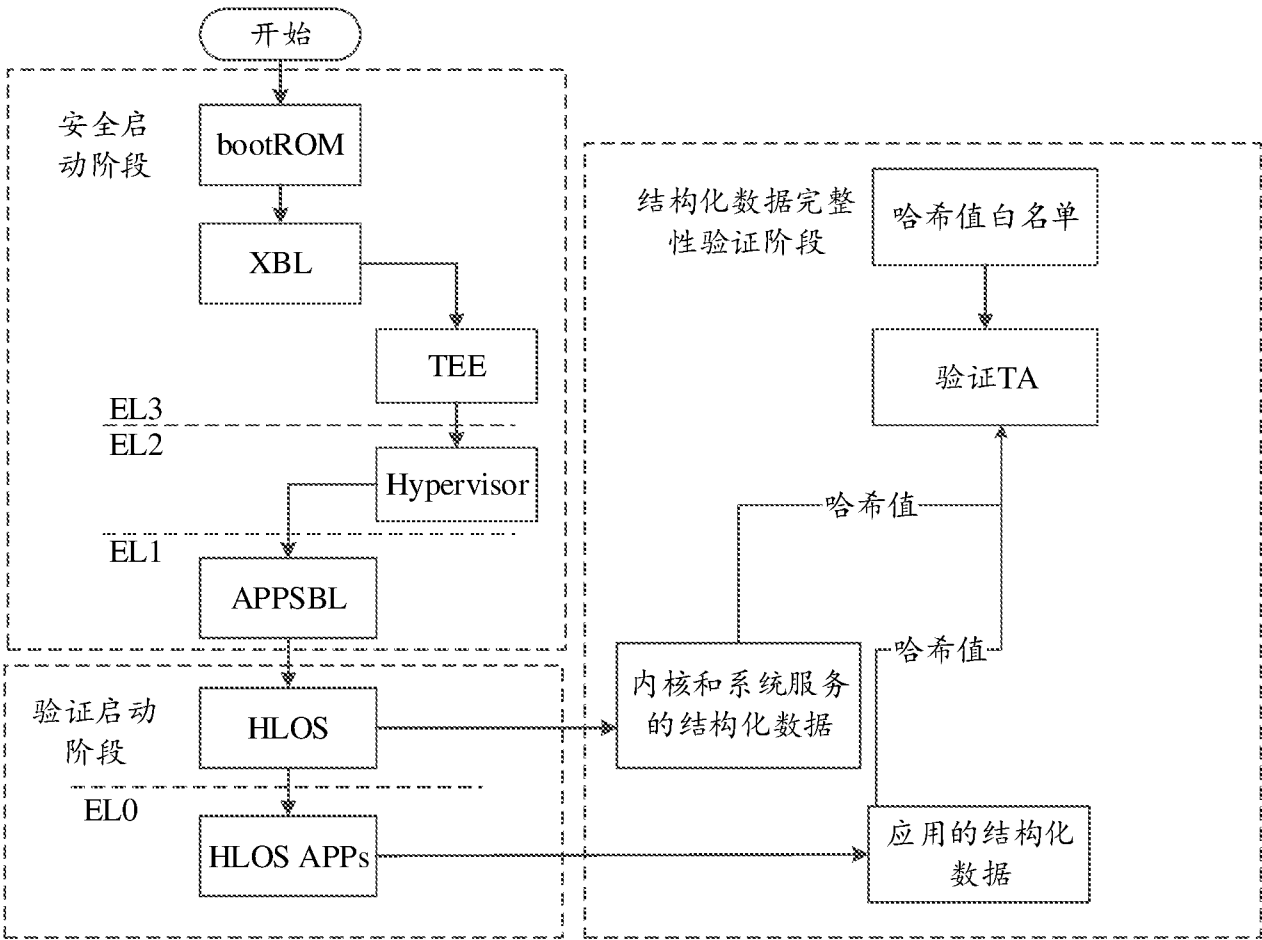


图 3

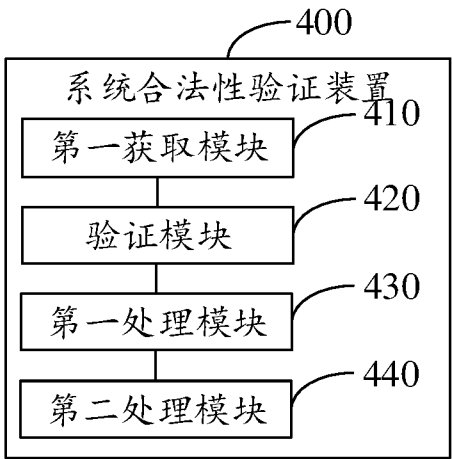


图 4

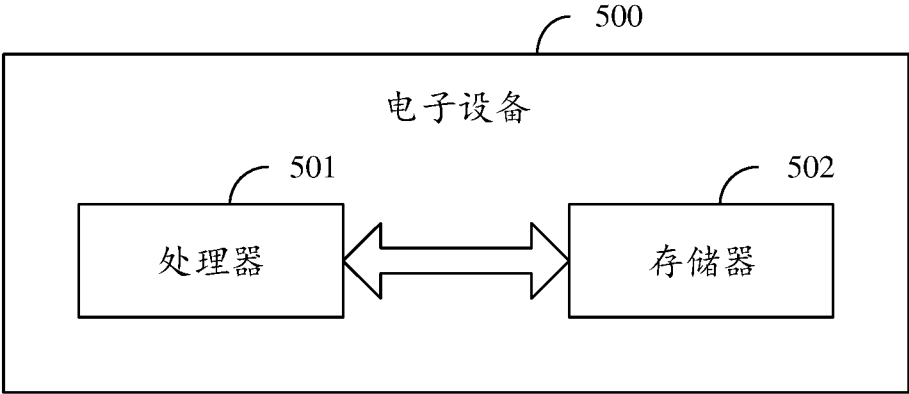


图 5

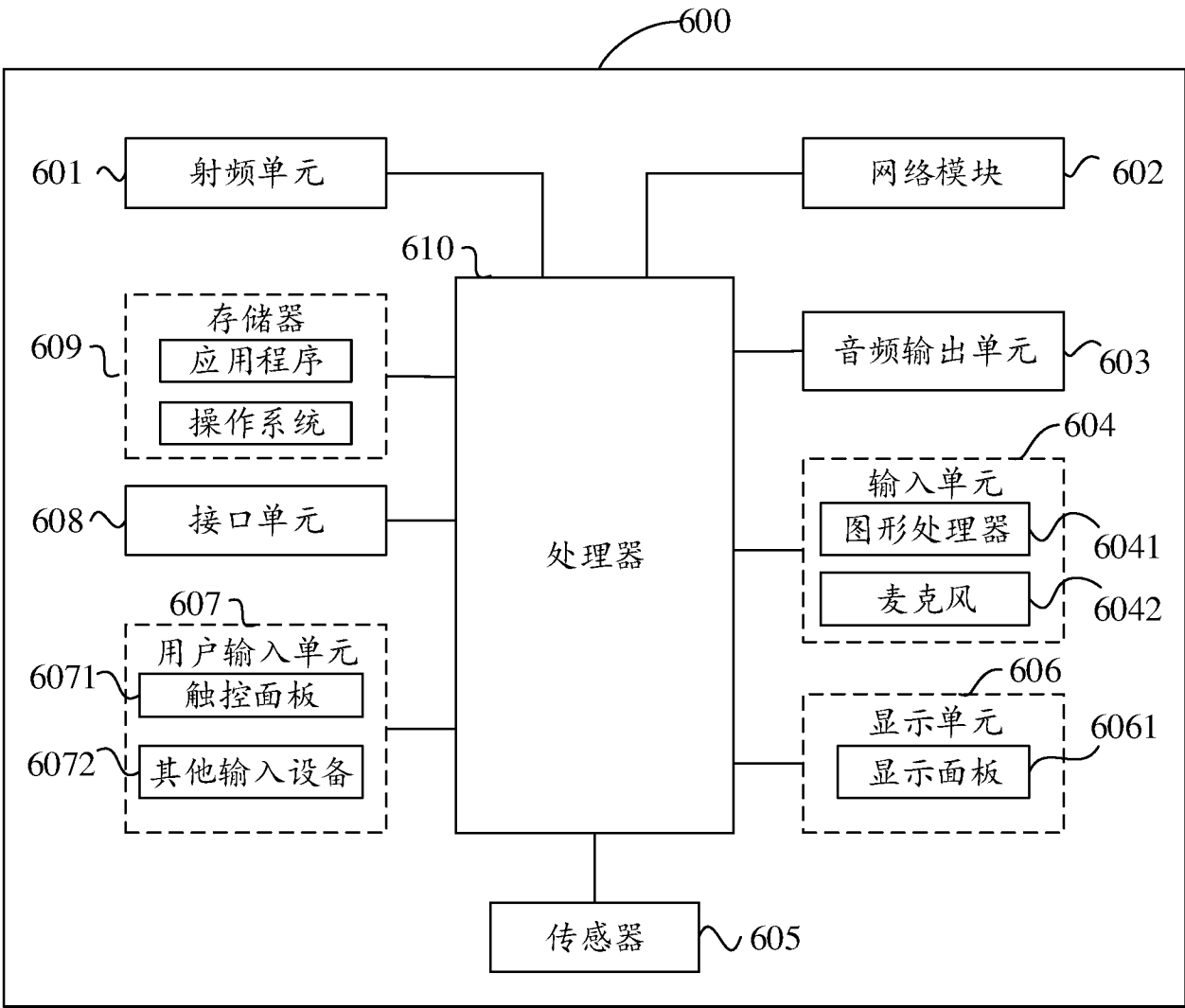


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/099283

A. CLASSIFICATION OF SUBJECT MATTER G06F 21/51(2013.01)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) IPC: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) CNABS, VEN, CNTXT, USTXT, CNKI, BAIDU: 结构化, 数据, 加载, 内核, 可信执行环境, 完整性, 合法性, TEE, structured, data, load, kernel, integrity, legitimacy		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 116776317 A (VIVO COMMUNICATION TECHNOLOGY CO., LTD.) 19 September 2023 (2023-09-19) claims 1-12, and description, paragraphs 155-163	1-15
X	CN 113190831 A (NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY OF PLA) 30 July 2021 (2021-07-30) description, paragraphs 2 and 35-60, and figures 1-5	1-15
A	CN 106096412 A (HUAWEI TECHNOLOGIES CO., LTD.) 09 November 2016 (2016-11-09) entire document	1-15
A	CN 112434306 A (INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES) 02 March 2021 (2021-03-02) entire document	1-15
A	US 2022129566 A1 (NXP B.V.) 28 April 2022 (2022-04-28) entire document	1-15
☐ 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 “D” document cited by the applicant in the international application “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 05 September 2024		Date of mailing of the international search report 11 September 2024
Name and mailing address of the ISA/CN China National Intellectual Property Administration (ISA/CN) China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/099283

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	116776317	A	19 September 2023	None	
CN	113190831	A	30 July 2021	None	
CN	106096412	A	09 November 2016	None	
CN	112434306	A	02 March 2021	None	
US	2022129566	A1	28 April 2022	None	

A. 主题的分类

G06F 21/51(2013.01)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)

IPC: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))

CNABS, VEN, CNTXT, USTXT, CNKI, BAIDU: 结构化, 数据, 加载, 内核, 可信执行环境, 完整性, 合法性, TEE, structured, data, load, kernel, integrity, legitimacy

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 116776317 A (维沃移动通信有限公司) 2023年9月19日 (2023 - 09 - 19) 权利要求1-12,说明书155-163段	1-15
X	CN 113190831 A (中国人民解放军国防科技大学) 2021年7月30日 (2021 - 07 - 30) 说明书2、35-60段, 图1-5	1-15
A	CN 106096412 A (华为技术有限公司) 2016年11月9日 (2016 - 11 - 09) 全文	1-15
A	CN 112434306 A (中国科学院信息工程研究所) 2021年3月2日 (2021 - 03 - 02) 全文	1-15
A	US 2022129566 A1 (NXP B.V.) 2022年4月28日 (2022 - 04 - 28) 全文	1-15

☐ 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

“D” 申请人在国际申请中引证的文件

“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

2024年9月5日

国际检索报告邮寄日期

2024年9月11日

ISA/CN的名称和邮寄地址

中国国家知识产权局
中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

赵天奇

电话号码 (+86) 010-53961320

PCT/ISA/210 表(第2页) (2022年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/099283

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	116776317	A	2023年9月19日	无	
CN	113190831	A	2021年7月30日	无	
CN	106096412	A	2016年11月9日	无	
CN	112434306	A	2021年3月2日	无	
US	2022129566	A1	2022年4月28日	无	