

(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
2021 年 10 月 7 日 (07.10.2021)



(10) 国际公布号
WO 2021/197040 A1

- (51) 国际专利分类号:
G06F 21/57 (2013.01) **G06F 21/51** (2013.01)
- (21) 国际申请号: PCT/CN2021/080810
- (22) 国际申请日: 2021 年 3 月 15 日 (15.03.2021)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202010246265.5 2020 年 3 月 31 日 (31.03.2020) CN
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 何达(HE, Da); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。齐杰(QI, Jie); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (74) 代理人: 北京润泽恒知识产权代理有限公司 (BEIJING RUN ZEHENG INTELLECTUAL

PROPERTY LAW FIRM); 中国北京市海淀区中关村南大街 31 号神舟大厦 702, Beijing 100081 (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, 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,

(54) Title: TRUSTED MEASUREMENT METHOD AND RELATED APPARATUS

(54) 发明名称: 可信度量方法及相关装置

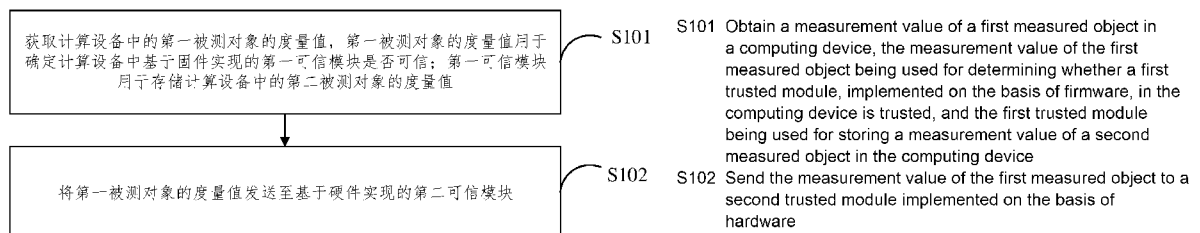


图 1

(57) Abstract: A trusted measurement method and a related apparatus. The trusted measurement method comprises: obtaining a measurement value of a first measured object in a computing device, the measurement value of the first measured object being used for determining whether a first trusted module, implemented on the basis of firmware, in the computing device is trusted, and the first trusted module being used for storing a measurement value of a second measured object in the computing device (S101); and sending the measurement value of the first measured object to a second trusted module implemented on the basis of hardware (S102). The method can improve the security of the computing device.

(57) 摘要: 一种可信度量方法及相关装置, 所述可信度量方法包括: 获取计算设备中的第一被测对象的度量值, 第一被测对象的度量值用于确定计算设备中基于固件实现的第一可信模块是否可信; 第一可信模块用于存储计算设备中的第二被测对象的度量值 (S101); 将第一被测对象的度量值发送至基于硬件实现的第二可信模块 (S102)。该方法能够提高计算设备的安全性。

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))。

可信度量方法及相关装置

本申请要求于 2020 年 3 月 31 日提交中国国家知识产权局、申请号为 202010246265.5、发明名称为“可信度量方法及相关装置”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

本申请涉及信息技术领域，特别涉及一种可信度量方法及相关装置。

背景技术

随着信息技术的飞速发展，计算设备的安全性的重要性日益提升。

计算设备的安全性可以通过对计算设备上运行的代码以及计算设备中存储的数据的完整性的度量结果确定。当计算设备上运行的代码是可信的代码，计算设备中存储的数据是可信的数据时，计算设备是可信的。计算设备上运行的代码可以从计算设备中存储的数据中读取并加载至计算设备中运行的。若计算设备中存储的数据或者计算设备中运行的代码被篡改，即计算设备上运行的代码和计算设备中存储的数据的完整性被破坏，则计算设备是不可信的。

目前，计算设备的安全性需要提升。

发明内容

本申请提供了一种可信度量方法及相关装置，用于提高计算设备的安全性。

第一方面，本申请提供一种可信度量方法。所述方法包括：获取计算设备中的第一被测对象的度量值，所述第一被测对象的度量值用于确定所述计算设备中基于固件实现的第一可信模块是否可信；所述第一可信模块用于存储所述计算设备中的第二被测对象的度量值；将所述第一被测对象的度量值发送至基于硬件实现的第二可信模块。

在采用上述方法时，通过将用于确定第一可信模块是否可信的第一被测对象的度量值发送给基于硬件实现的第二可信模块，第二可信模块可存储接收到的第一被测对象的度量值。由于基于硬件实现的第二可信模块中对内部数据的安全保护等级高于基于固件实现的第一可信模块的安全防护等级，其中利用第二可信模块存储的第一被测对象的度量值来确定第一可信模块是否可信将更为安全和准确。从而可以提升计算设备的安全性。

在一种可能的实现方式中，所述第一被测对象包括以下至少一种：所述第一可信模块或所述第一可信模块中的数据。

在一示例中，所述第一可信模块中的数据可以包括以下至少一种：所述第一可信模块自身的数据，所述第二被测对象的度量值等。

在一示例中，第一被测对象可以仅包括第一可信模块中存储的第二被测对象的度量值。

在一种可能的实现方式中，所述第二被测对象的度量值为采用扩展操作的方式存储于所述第一可信模块的第一寄存器中的；所述第一被测对象的度量值为采用扩展操作的方式存储于所述第二可信模块的第二寄存器中的。

在一种可能的实现方式中，所述第二可信模块还用于存储第三被测对象的度量值；所述第三被测对象为在所述第一可信模块启动前所述计算设备中的被测对象；所述第二被测对象

为在所述第一可信模块启动后所述计算设备中的被测对象。

在一种可能的实现方式中，所述第一可信模块为基于所述计算设备上的可信操作系统运行的；所述第三被测对象，包括以下至少一项：BIOS 代码，所述计算设备的引导加载程序和所述可信操作系统的启动代码。

5 在一种可能的实现方式中，所述第三被测对象的度量值为采用扩展操作的方式存储于所述第二可信模块的第三寄存器中的。

在一种可能的实现方式中，所述第一可信模块为基于固件的可信平台模块 fTPM，所述第二被测对象的度量值存储于所述第一可信模块的平台配置寄存器 PCR；和/或，所述第二可信模块为离散可信平台模块 dTPM 或集成可信平台模块，所述第一被测对象的度量值存储于所述
10 第二可信模块的 PCR。

在一种可能的实现方式中，所述第一被测对象包括所述第二被测对象的度量值；在所述获取计算设备中的第一被测对象的度量值之前，所述方法还包括：获取所述第二被测对象的度量值；其中，所述第二被测对象包括以下至少一种：所述计算设备中的 APP、进程、程序、日志、数据库、文件、数据；将所述第二被测对象的度量值发送至所述第一可信模块。

15 在一种可能的实现方式中，在所述获取计算设备中的第一被测对象的度量值之前，包括：检测到所述第一被测对象发生变更。

在一种可能的实现方式中，在所述获取计算设备中的第一被测对象的度量值之前，包括：接收定期触发的状态监测指示。

在一种可能的实现方式中，所述获取计算设备中的第一被测对象的度量值，包括：获取
20 至少两个第一被测对象对应的一个度量值。

第二方面，本申请提供一种可信度量装置。所述装置包括：获取模块，用于获取计算设备中的第一被测对象的度量值，所述第一被测对象的度量值用于确定所述计算设备中基于固件实现的第一可信模块是否可信；所述第一可信模块用于存储所述计算设备中的第二被测对象的度量值；发送模块，用于将所述第一被测对象的度量值发送至基于硬件实现的第二可信
25 模块。

在一种可能的实现方式中，所述第一被测对象包括以下至少一种：所述第一可信模块或所述第一可信模块中的数据。

在一种可能的实现方式中，所述第二被测对象的度量值为采用扩展操作的方式存储于所述第一可信模块的第一寄存器中的；其中，扩展操作后所述第一寄存器中的数据为根据扩展
30 操作前所述第一寄存器中的数据和所述第二被测对象的度量值生成的；所述第一被测对象的度量值为采用扩展操作的方式存储于所述第二可信模块的第二寄存器中的；其中，扩展操作后所述第二寄存器中的数据为根据扩展操作前所述第二寄存器中的数据和所述第一被测对象的度量值生成的。

在一种可能的实现方式中，所述第一可信模块为基于固件的可信平台模块 fTPM，所述第二被测对象的度量值存储于所述第一可信模块的平台配置寄存器 PCR；和/或，所述第二可信模块为离散可信平台模块 dTPM，或，集成可信平台模块 iTPM，所述第一被测对象的度量值存储于所述第二可信模块的 PCR。

在一种可能的实现方式中，所述获取模块，还用于在所述获取计算设备中的第一被测对象的度量值之前，获取所述第二被测对象的度量值；其中，所述第一被测对象包括所述第二
40 被测对象的度量值；所述第二被测对象包括以下至少一种：所述计算设备中的 APP、进程、程

序、日志、数据库、文件、数据；所述发送模块，还用于将所述第二被测对象的度量值发送至所述第一可信模块。

在一种可能的实现方式中，所述获取模块，还用于在检测到所述第一被测对象发生变更后，执行所述获取计算设备中的第一被测对象的度量值的步骤。

5 在一种可能的实现方式中，所述获取模块，还用于在接收定期触发的状态监测指示后，执行所述获取计算设备中的第一被测对象的度量值的步骤。

在一种可能的实现方式中，所述获取模块，具体用于获取至少两个第一被测对象对应的一个度量值。

第三方面，本申请提供一种计算设备，所述计算设备包括：基于所述计算设备的固件实现的10 第一可信模块，基于硬件实现的第二可信模块和第二方面任一所述的可信度量装置；其中，所述第一可信模块用于存储计算设备中的第二被测对象的度量值；所述第二可信模块用于存储所述第一被测对象的度量值。

在一种可能的实现方式中，所述计算设备还包括：验证装置，用于从所述第二可信模块15 中获取所述第一被测对象的度量值，根据所述第一被测对象的度量值确定所述第一被测对象是否可信。

在一种可能的实现方式中，所述计算设备还包括：度量执行装置，用于获取所述第一被20 测对象的完整性参数，向所述度量执行装置发送所述第一被测对象的完整性参数；以及，接收所述度量执行装置发送的所述第一被测对象的度量值；所述度量执行装置，用于接收所述第一被测对象的完整性参数，根据所述第一被测对象的完整性参数生成所述第一被测对象的度量值。

第四方面，本申请提供一种可信度量程序，所述可信度量程序被执行时用于实现第一方面任一所述的可信度量方法。

第五方面，本申请提供一种可信度量系统，所述系统包括：基于计算设备的固件实现的25 第一可信模块、基于硬件实现的第二可信模块和第二方面任一所述的可信度量装置；所述第一可信模块，用于存储计算设备中的第二被测对象的度量值；所述第二可信模块，用于存储所述第一被测对象的度量值。

在一种可能的实现方式中，所述可信度量系统还包括：验证装置，用于从所述第二可信30 模块中获取所述第一被测对象的度量值，根据所述第一被测对象的度量值确定所述第一被测对象是否可信。

在一种可能的实现方式中，所述可信度量系统还包括：度量执行装置，用于获取所述第35 一被测对象的完整性参数，向所述度量执行装置发送所述第一被测对象的完整性参数；以及，接收所述度量执行装置发送的所述第一被测对象的度量值；所述度量执行装置，用于接收所述第一被测对象的完整性参数，根据所述第一被测对象的完整性参数生成所述第一被测对象的度量值。

第六方面，本申请提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有40 指令，所述指令可以由处理电路上的一个或多个处理器执行。当其在计算机上运行时，使得计算机执行上述第一方面中任意可能的实现方式中的方法。

附图说明

40 图1为本申请实施例提供的一种可信度量方法的流程示意图一；

图 2 为本申请实施例提供的可信度量方法的计算设备的系统架构示意图；

图 3 为本申请提供的可信度量方法的处理流程示意图一；

图 4 为本申请提供的可信度量方法的处理流程示意图二；

图 5 为本申请实施例提供的可信度量方法的处理流程示意图三；

5 图 6 为本申请实施例提供的可信度量装置的结构示意图一；

图 7 为本申请实施例提供的可信度量装置的结构示意图二；

图 8 为本申请实施例提供的一种计算设备的结构示意图。

具体实施方式

10 本申请的实施方式部分使用的术语仅用于对本申请的具体实施例进行解释，而非旨在限定本申请。

本申请提供用于确定计算设备的安全性的可信度量方法。采用本申请提供的方法获得计算设备上的各种对象的度量结果，之后可以根据度量结果与预期度量结果进行比较来确定计算设备上的各种对象是否被篡改，进而能够帮助计算设备使用者在发现计算设备的系统环境
15 被篡改时作出正确的判断和处理。

图 1 为本申请实施例提供的一种可信度量方法的流程示意图一。本申请实施例的执行主体可以是可信度量装置。在一示例中，可信度量装置可以是可运行于计算设备中的应用（Application，APP）程序。如图 1 所示，本申请实施例的步骤可以包括：

S101，获取计算设备中的第一被测对象的度量值，所述第一被测对象的度量值用于确定
20 所述计算设备中基于固件实现的第一可信模块是否可信；所述第一可信模块用于存储所述计算设备中的第二被测对象的度量值。

S102，将所述第一被测对象的度量值发送至基于硬件实现的第二可信模块。

在本申请实施例中，计算设备上部署有第一可信模块和第二可信模块，第一可信模块和第二可信模块均用于存储计算设备中的被测对象的度量值。其中，计算设备中的各种被度量的对象称为被测对象。示例性地，被测对象是 APP、进程、程序、文件、日志、数据库或数据
25 等。被测对象的度量值可以是根据被测对象的完整性参数确定的，被测对象的完整性参数可以是被测对象的哈希值或签名等。

第一可信模块和第二可信模块有多种写入数据的方法。在一示例中，第一可信模块和第二可信模块支持允许直接写入数据或者以扩展操作的方式写入数据。在实际应用中，以扩展操作的方式写入的数据在被篡改时可被检测到，从而实现快速地确定被测对象是否可信。在
30 另一示例中，第一可信模块和第二可信模块支持通过加密存储、加密读写、仅允许具有密钥的对象写入数据和读取数据等方式来保证数据的安全性。

第一可信模块和第二可信模块可用于存储各类被测对象的度量值。在一示例中，第二可信模块接收可信度量装置发送待存储的度量值。之后，可以允许验证装置读取第一可信模块、
35 第二可信模块中的各个被测对象的度量值，将读取到的度量值与预期度量值比较，来确定被测对象是否可信，从而能够通过计算设备上的被测对象是否可信确定计算设备是否可信。

在本申请实施例中，第一可信模块用于存储第二被测对象的度量值，第二可信模块用于存储第一被测对象的度量值。表 1 为被测对象的度量值与存储位置对应关系的一种示意。

表1

被测对象	被测对象对应的度量值	存储位置
第二被测对象	第二被测对象的度量值	第一可信模块
第一被测对象	第一被测对象的度量值	第二可信模块

举例来说，第二被测对象可以是计算设备上的各种被测对象。在实际应用中，第二被测对象可以是在第一可信模块启动后计算设备上的被测对象。示例性地，第二被测对象可以是APP代码、APP的启动日志、APP的操作日志、数据库、数据库操作日志等。第一被测对象可以用于确定第一可信模块是否可信的被测对象。示例性地，第一被测对象可以包括以下至少一种：第一可信模块或第一可信模块中的数据。

在本申请实施例中，基于固件实现的第一可信模块的存储容量能够基于计算设备的硬件能力配置，从而使得第一可信模块支持存储数量较多的被测对象的度量值。

在本申请实施例中，第一可信模块是基于固件实现的，第一可信模块中的代码和数据实际可存储在内存中。需要说明的是，即使存储于可信执行环境的安全内存中，第一可信模块中存储的数据有可能被篡改，即第一可信模块中存储的度量值有可能被篡改。为了提高第一可信模块以及第一可信模块中的数据的安全性，本申请实施例中将第一被测对象的度量值发送给基于硬件实现的第二可信模块，第二可信模块存储接收到的第一被测对象的度量值。

在基于硬件实现的第二可信模块中，用于保护内部数据和代码等信息的处理模块可以是基于硬件实现的，因而能够保证内部数据的安全。第二可信模块中存储的数据在被篡改时能够被验证装置发现。与第二可信模块相比，在基于固件实现的第一可信模块中，用于保护内部数据和代码等信息的处理模块可以是基于固件实现的，因而可能被修改。当基于固件的处理模块被修改时，可能导致第一可信模块或者第一可信模块中的数据在被篡改时不能被发现。由此可见，基于硬件实现的第二可信模块的安全性高于基于固件实现的第一可信模块。基于此，利用第二可信模块存储的第一被测对象的度量值来确定第一可信模块以及第一可信模块中的数据是否可信更为安全和准确。

在本申请实施例中，举例来说，第一被测对象可以包括作为一个完整整体的第一可信模块以及各种存储于第一可信模块中的数据。示例性地，第一可信模块可以为作为一个完整整体实现的第一可信模块对应的APP、程序、进程。第一可信模块中的数据可以为第一可信模块启动或运行时需要启动或者加载的进程、程序、代码、数据，以及，存储于第一可信模块的寄存器中的数据等。为了提高第一可信模块和第一可信模块中的数据的安全性，可以分别将第一可信模块的度量值，以及，第一可信模块中的数据的度量值，扩展至第二可信模块的寄存器。之后，验证装置就能够分别根据存储于第二可信模块的寄存器中的数据进行验证，并综合验证结果对第一可信模块是否可信作出判断。

在本申请实施例中，各种被测对象的度量值可以采用扩展操作的方式存储于第一可信模块或者第二可信模块的寄存器中。扩展操作后寄存器中的数据为根据扩展操作前寄存器中的数据和待存储的被测对象的度量值生成的。在一示例中，第二被测对象的度量值为采用扩展操作的方式存储于第一可信模块的第一寄存器中的；其中，扩展操作后第一寄存器中的数据为根据扩展操作前的第一寄存器中的数据和第二被测对象的度量值生成的。在另一示例中，可将第一被测对象的度量值扩展至第二可信模块的第二寄存器中；其中，扩展操作后第二寄存器中的数据为根据扩展操作前第二寄存器中的数据和第一被测对象的度量值生成的。由于扩展操作的结果是不可逆的，当采用扩展操作的方式存储于第一可信模块或第二可信模块中的数据被篡改时，能够被验证装置快速发现。从而能够进一步提升计算设备的安全性。

在本申请实施例中，第一被测对象可以包括以下至少一种：第一可信模块或第一可信模块中的数据。其中，第一可信模块的度量值，可用于确定计算设备上当前运行的第一可信模块本身的代码是否可信。在一种实施方式中，第一可信模块中的数据包括第二被测对象的度量值等。第二被测对象的度量值是确定第二被测对象是否可信的依据，第一可信模块中的数据
5 的度量值可用于确定第二被测对象的度量值是否可信，即依据是否可信。

在本申请实施例中，第二可信模块还可以用于存储第三被测对象的度量值。

在一种实施方式中，第三被测对象为在第一可信模块启动前计算设备中的被测对象；第二被测对象为在第一可信模块启动后计算设备中的被测对象。从计算设备整体的角度来看，第三被测对象的度量值能够用于确定在启用第一可信模块之前计算设备中的运行环境是否可信。运行环境可包括操作系统中处于已进入运行状态的代码、全局变量、计算设备的存储器
10 中存储的数据等。示例性地，对启动过程的被测对象的度量采用静态度量的方式，即在代码被加载执行前对代码进行度量，对运行过程的被测对象的度量采用动态度量的方式，即在运行过程中的代码的运行状态发生变化时，或者，周期性地对运行过程中的代码进行度量。

在一示例中，第三被测对象包括用于启动第一可信模块的被测对象。举例来说，在实际
15 应用中，若第一可信模块为基于计算设备上的操作系统运行的；则计算设备中用于启动第一可信模块的被测对象，包括以下至少一项：BIOS代码、计算设备的引导加载程序或操作系统的启动代码。举例来说，操作系统的启动代码为用于启动操作系统的基本功能的代码，如Linux操作系统的内核（kernel）代码。需要说明的是，其他类型的操作系统启动前加载执行的代码及加载执行的顺序还可以有其他实现方式，本申请实施例对此不作限制。在本申请实施例中，第三被测对象的度量值也可以为采用扩展操作的方式存储于第二可信模块的寄存器中的。
20

在本申请实施例中，步骤S101获取计算设备中的第一被测对象的度量值有多种实施方式。

在一种实施方式中，上述步骤可以包括：可信度量装置接收由度量执行装置根据第一被测对象的完整性参数确定的第一被测对象的度量值。其中，示例性地，度量执行装置为本地
度量模块，或者，度量服务器。在一示例中，本地度量模块为计算设备中的APP或者进程。
25

在另一种实施方式中，上述步骤可以包括：可信度量装置获取第一被测对象的完整性参数，根据第一被测对象的完整性参数确定第一被测对象的度量值。在一示例中，在第一被测对象包括第一可信模块时，度量执行装置获取第一可信模块的完整性参数。例如，获取第一可信模块的数字签名作为第一可信模块的度量值。在另一示例中，在第一被测对象包括第一可信模块中的数据时，度量执行装置获取第一可信模块中的数据的哈希值，将该哈希值作为
30 该数据对应的度量值。本申请对此不作限制。

在本申请实施例中，第一被测对象的数量为一个或多个。当为多个时，步骤S101-S102还可以采用另一组实施方式。在一种可选的实施方式中，上述步骤包括：分别获取各个第一被测对象的度量值，并分别将各个第一被测对象的度量值发送至第二可信模块，之后，第二可信模块分别存储各个第一被测对象的度量值。在另一种可选的实施方式中，上述步骤包括：
35 对于多个第一被测对象中的任意至少两个第一被测对象，获取至少两个第一被测对象对应的一个度量值；将该一个度量值发送至第二可信模块；之后，第二可信模块使用一个寄存器存储该度量值。采用这种方式，利用第二可信模块的一个存储空间，来存储用于确定多个第一被测对象是否可信的度量值，能够节约第二可信模块的存储空间。

举例来说，第一被测对象的数量为N个，N为大于或者等于2的整数。在一示例中，可信度量装置获取N个第一被测对象对应的1个度量值。示例性地，获取N个第一被测对象对应的N个
40

完整性参数，再获取N个完整性参数的完整性参数，然后，根据N个完整性参数的完整性参数来确定N个第一被测对象对应的1个度量值。在另一示例中，上述N个第一被测对象包括：APP1的代码、APP1的操作日志、APP2的代码、APP2的操作日志、允许被APP1和APP2读写的文件1等。可信度量装置分别获取与APP1有关的第一被测对象对应的1个度量值，以及，与APP2有关的第一被测对象对应的1个度量值。即获取APP1的代码、APP1的操作日志、文件1对应的1个度量值A，以及，获取APP2的代码、APP2的操作日志、文件1对应的1个度量值B，之后，分别将度量值A和B发送至第二可信模块。采用这种方式，能够在节约第二可信模块的存储空间的基础上，实现快速确定计算设备中的关键APP是否可信。

在本申请实施例中，上述步骤S101-S102支持在多种触发条件时执行。

在一示例中，可信度量装置在检测到第一被测对象发生变更时执行步骤S101-S102。举例来说，第一被测对象包括第一可信模块的APP、进程、程序、日志、数据库、文件或者第一可信模块中的数据等中的至少一种被测对象。示例性地，第一可信模块中的数据可以包括存储于第一可信模块中的寄存器中第二被测对象的度量值等。在检测到第一可信模块中的数据发生变更时，或者，在检测到第一可信模块的APP的启动请求，或者，在检测到第一可信模块的任一进程的创建请求，或者，在检测到第一可信模块的任一程序的加载请求或者动态检查请求，或者，在检测到第一可信模块的日志发生变更；或者，在检测到第一可信模块的数据库发生变更时，执行步骤S101-S102。采用这种方式能够实现第一可信模块的启动阶段的度量以及第二被测对象的度量值发生变更时的度量。

在另一示例中，可信度量装置在接收到定期触发的状态监测指示时，执行步骤S101-S102。举例来说，可信度量装置接收按照预先设置的检测周期，定期生成的状态监测指示，并在接收到状态监测指示后，执行步骤S101-S102。采用这种方式能够实现对计算设备的动态度量，即定期对运行过程中的被测对象进行度量。

在本申请实施例中，第一可信模块中的第二被测对象的度量值的获取方式有多种。例如，第二被测对象的度量值为在检测到第二被测对象发生变更时获取到的，或者，在接收定期触发的状态监测指示时获取到的。举例来说，第二被测对象是计算设备上的任意被测对象。在一示例中，第二被测对象是除第一可信模块和第一可信模块中的数据之外的其他被测对象。

在一种可选的实施方式中，在步骤S101之前，第二被测对象的度量值是由可信度量装置发送至第一可信模块中的。示例性地，可信度量装置在检测到第二被测对象发生变更时，获取第二被测对象的度量值，并发送至第一可信模块。

在另一种可选的实施方式中，计算设备支持配置至少两个可信度量装置；例如，第一和第二可信度量装置。其中，第二被测对象的度量值是由第一可信度量装置获取并发送至第一可信模块的；第一被测对象的度量值是由第二可信度量装置获取并发送至第二可信模块的。其中，第一被测对象中可包括第一可信模块中的数据，例如第二被测对象的度量值。

在上述任一实施方式的基础上，在本申请实施例中，第一可信模块可以为基于固件实现的可信平台模块（Trust Platform Module，TPM）或者基于固件实现的可信密码模块（Trust Cryptography Module，TCM）。在一示例中，第一可信模块为基于固件的可信平台模块（firmware TPM，fTPM）。相应的，第二被测对象的度量值可以存储于第一可信模块的平台配置寄存器PCR。举例来说，基于硬件实现的TPM或者TCM可被设置于计算设备与外部IO设备通信的总线中，以获悉实际被加载至内存中待由CPU中执行的代码和要使用的数据，从而可以确保被测对象的真实性。

在本申请实施例中，第二可信模块可以为基于硬件实现的TPM或者基于硬件实现的TCM。在一示例中，第二可信模块为离散可信平台模块（Discrete TPM，dTPM）或集成可信平台模块（Integrated TPM）。相应地，第一被测对象的度量值可以存储于第二可信模块的PCR。举例来说，基于固件实现的TPM或者基于固件实现的TCM运行于支持Trustzone的计算设备。

5 在本申请实施例，利用fTPM和dTPM结合的方式，能够在提升PCR数量的基础上提升安全性。一方面，由于fTPM中支持扩展定义配置寄存器，因此，能够提供较大数量的PCR。例如，fTPM支持配置超过24个PCR。另一方面，在dTPM中保存fTPM程序的度量值，用以定时对fTPM模块进行验证，能够确保运行的fTPM固件程序合法。

10 举例来说，对fTPM中所有PCR的值通过哈希Hash算法计算出摘要值，然后扩展到dTPM的特定PCR；在检测到fTPM的PCR的值发生变化时，重新计算所有PCR的值对应的摘要值并同步扩展至dTPM的特定PCR。之后，dTPM或者验证装置定时验证特定PCR中存储的fTPM的PCR的摘要值，并在验证结果为与预期不一致时上报告警。采用这种方式能够确保fTPM中的数据 and 安全性。

15 下面以第一可信模块为fTPM，第二可信模块为dTPM为例，对本申请提供的可信度量方法进行示例性说明。其中，计算设备中支持部署普通操作系统和可信操作系统。示例性地，普通操作系统可以为Linux或Windows操作系统。fTPM为基于可信操作系统运行的可信应用（Trusted Application，TA）。

图2为本申请实施例提供的应用可信度量方法的计算设备的系统架构示意图。如图2所示，计算设备包括硬件（Hardware）和软件（Software）两部分。

20 计算设备的硬件部分可以包括：片上芯片（System on Chip，SOC），SOC中包括：dTPM，ARM CPU Core，业务处理引擎，以及，安全区（Trustzone）、加解密引擎、硬件随机数、电子熔丝（eFuse）、硬件唯一密钥（HardwareUniqueKey，HUK）等。其中，Trustzone、加解密引擎、硬件随机数、eFuse、HUK可用于实现代码和数据的安全隔离。需要说明的是，Trustzone技术是通过硬件隔离实现的。示例性地，安全世界和非安全世界的操作系统分别运行于相互隔离的硬件。

25 计算设备的软件部分可以包括：非安全世界（Non-Secure world）和安全世界（Secure-world），安全世界和非安全世界通过安全监控器（Secure Monitor）实现通信。安全世界中的操作系统称为可信执行环境（Trust Execute Environment，TEE）的操作系统（TEE OS），下面简称为可信操作系统。非安全世界的操作系统称为普通操作系统。在非安全世界中，普通的用户应用（User App）基于普通操作系统运行，在安全世界中，可信执行环境的应用（TEE App）基于TEE OS运行。

30 示例性地，安全世界中的TEE App包括：TA（fTPM）、TA（KMC）、TA（DIM）、全球平台可信执行环境内部接口（GlobalPlatform TEE internal API）。其中，TA（fTPM）为前述实施例中的第一可信模块的一种实现方式。TA（fTPM）可以包括：平台配置寄存器（Platform Configuration Registers，PCR）、TPM 命令（TPM COMMAND）、X509/RS、安全散列算法（Secure Hash Algorithm，SHA）、高级加密标准（Advanced Encryption Standard，AES）、子系统Sub System等。TA（DIM）是动态完整性度量（Dynamic Integrity Measurement，DIM）的TA。

40 非安全世界中的User App包括：本地应用（Native App）、密钥管理系统（Key Manager Center，KMC）、度量启动模块、全球平台可信执行环境客户端接口（Global Platform TEE Client API）等。其中，GlobalPlatform TEE internal API和Global Platform TEE Client API用于实现User APP与各个TA之间建立通信连接，度量启动模块可以用于获取被测对象的度

量值, 需要说明的是, 度量启动模块可以为基于普通操作系统运行的用户应用, 也可以为普通操作系统中的系统应用、系统进程, 还可以是安全世界中的TA。

安全世界的TEE OS中支持运行: TEE Core、TEE功能(Func)/数据库(Libs)、加密函数(Crypt)、硬件抽象层(Hardware Abstraction Layer, HAL)等。

5 普通操作系统中支持运行: TPM驱动(TPM Drv)、TEE驱动(TEE Drv)。其中, TEE驱动(TEE Drv)用于实现普通操作系统与TEE OS之间的通信连接, TPM Drv用于实现度量启动APP与安全世界的TA(fTPM)之间的通信连接。

在本申请实施例中, 第一被测对象的度量值可以存储于dTPM的PCR中, 第二被测对象的度量值可以存储于fTPM的PCR中。

10 需要说明的是, 为了防止PCR中存储的度量值被恶意代码篡改或伪造, 上述各种TPM预先定义需限制对PCR执行的操作。其中包括: 一方面, 不允许采用对普通字符设备的寄存器进行读写时所采用的通过端口映射的方式随意对PCR进行读写; 另一方面, 将PCR被设置于各种TPM的内部, 以保护内部存储的数据; 又一方面, 只允许两种操作来修改PCR的值: 其中, 重置操作(Reset)和扩展操作(Extend), 重置操作可发生在机器断电或者重新启动之后, PCR的值
15 自动重新清零。

在系统运行过程中, 只能通过扩展操作来改变PCR的内容。示例性地, 扩展操作的定义如下:

$$\text{PCR}[n] = \text{HASH}\{\text{PCR}[n-1] \parallel \text{newMeasurement}\}。$$

其中, PCR[n-1]代表第n-1时刻PCR中存储的数据, PCR[n]代表第n时刻PCR中存储的数据, newMeasurement代表第n时刻获得的被测对象的度量值。扩展操作可以是不可逆的, 举例来说, 先将度量值A扩展至PCR, 再将度量值B扩展至PCR, 得到的PCR值, 与先将度量值B扩展至PCR, 再将度量值A扩展至PCR得到的PCR值是不同的。通过扩展操作, PCR能够记录一个无限长的度量值序列, 这一系列度量值组成的序列能够反映系统状态的变迁, 如果这个扩展序列中的某一个度量值改变, 之后的度量序列都会受到影响, 即PCR中的数值与验证装置记录的期望数值
25 不符。

在本申请实施例中, 在上述步骤S102中将第一被测对象的度量值发送至第二可信模块后, 该度量值以扩展的方式写入PCR中, 即将第一被测对象的度量值扩展至第二可信模块的PCR中。类似的, 第二被测对象的度量值也可以是以扩展的方式写入第一可信模块的PCR中的。

需要说明的是, 对计算设备的完整性度量可以利用信任传递机制。信任传递机制中定义, 30 在确认当前环节可信的前提下, 由当前环节度量下一环节的安全性, 在确定下一环节可信后, 将控制权转交给下一环节, 然后, 依次向后推进。基于这种信任传递机制, 当根据计算设备上的某一时刻的运行环境为可信时, 若下一时刻需要运行的被测对象为可信的, 则认为在运行下一时刻要运行的被测对象之后的运行环境是可信的。

采用以扩展操作的方式存储度量值能够实现信任链的传递。举例来说, 计算设备中的一些被测对象的加载顺序或者调用顺序是固定的, 例如, 计算设备的启动阶段加载或者执行的
35 多个程序。这些加载顺序或者调用顺序为固定的被测对象可组成一个被测对象序列, 称为定序被测对象序列。对于任一定序被测对象序列, 将该序列中的被测对象对应的度量值以扩展方式写入一个PCR中。对于该PCR来说, 当PCR中的数据被验证为可信时, 该PCR对应的在先被调用的多个被测对象均是可信的, 多个被测对象可组成一条信任链。每个可信的被测对象还可以作为一个新的信任链的起点。当一个新的被测对象是基于一个可信的被测对象执行时,
40

只要确认该新的被测对象的代码和数据是可信的，则加载该新的被测对象的代码和数据执行后的系统运行环境也是可信的。对于部署有两个操作系统的计算设备来说，计算设备在加载并执行代码时，允许通过切换时间片的方式，逐个加载和执行各个操作系统上的代码，以实现被测对象的依次加载或执行，从而实现信任链的传递。

5 示例性地，对于图2所示计算设备来说，计算设备的启动阶段加载和执行的代码包括：BIOS代码、操作系统引导程序、操作系统启动代码。在一示例中，计算设备在启动阶段的度量过程包括：获取BIOS代码的度量值1，将度量值1扩展至第二可信模块的PCR1，获取操作系统引导程序代码的度量值2，将度量值2扩展至PCR1，获取操作系统启动代码的度量值3，将度量值3扩展至PCR1。用于校验被测对象是否可信的验证装置在每次扩展操作后读取PCR1中的数据，
10 将其与期望值进行比较，以确定各个代码是否可信。

需要说明的是，由于第一可信模块通常是在操作系统的启动代码执行后启动的，第一可信模块无法存储在其自身启动前被加载和执行的代码的度量值，因此，将启动阶段的被测对象的度量值以扩展方式存储于第二可信模块，能够实现以对第一可信模块启动前的运行环境是否可信进行度量。

15 在实际应用中，对当前被测对象的度量必须由在当前被测对象之前加载或调用的其他对象执行，即度量过程需要早于调度执行过程，以保障度量过程中的度量对象的真实性。对度量结果的验证过程可以晚于调度执行过程，也可以与调度执行过程同时进行。在一示例中，遵循先度量再执行的原则，在验证待加载执行的被测对象不可信时，停止加载不可信的被测对象，从而帮助用户快速确认计算设备的安全性，在另一示例中，当验证过程晚于调度执行
20 过程时，将验证为不可信的被测对象记录在日志中，以供用户查看。

在本申请实施例中，利用 fTPM 定义大量 PCR，能够支持对计算设备中多个维度的被测对象进行度量。示例性地，支持按照被测对象的类型和调用顺序规划的多个度量链路的度量。下面采用具体的例子对本申请实施例提供的可信度量方法进行示例性说明。

在本申请实施例的应用场景中，对于复杂系统，例如，一个操作系统中可能存在多个进
25 程，这些进程可能分别基于不同的应用场景运行，各个进程的功能相对独立，进程存在独立启动、动态加载的需求，例如，以非预期的执行顺序加载执行或者中断执行。该场景无法直接使用TPM的信任链传递的方式来度量整个系统。此时，考虑按照进程所基于的应用场景规划度量链路。需要说明的是，对于归属于一条度量链路的被测对象可以采用一个PCR记录其对应的度量值。

30 图3为本申请提供的可信度量方法的处理流程示意图一。如图3所示，在本申请实施例中，对于复杂系统可以考虑分为两个度量链路：基础系统进程和系统扩展功能进程。其中，基础系统进程用于负责完成操作系统的框架的启动。

将启动阶段加载执行的基础系统进程的度量值存储至dTPM的PCR中。需要说明的是，基础系统进程可以通过dTPM的信任链传递方式进行启动，即启动阶段的信任链中可包括启动阶段
35 需要加载执行的一个或多个基础系统进程。示例性地，将用于获取基础系统进程的度量值并将其扩展至dTPM中的这部分代码也可以添加到启动阶段的信任链中。其中，在操作系统的框架启动阶段，被加载执行的这部分代码可以仅实现前述实施例中的可信度量装置的部分功能，以确保系统的框架运行安全。

系统扩展功能进程的度量值存储到fTPM的PCR中。示例性地，系统扩展功能进程为满足以下至少一个条件的进程：对应一个独立的功能，支持独立的启动、退出，或者，即使发生异
40

常也不会扩展影响操作系统框架或其他的系统扩展功能进程。在实际应用中，对每个系统扩展功能进程分别采用一个PCR记录其对应的度量值。在一些场景中，系统扩展功能进程可以随基础系统进程一起启动，也可以在需要时启动，本申请对此不作限制。

基于上述两条度量链路的划分，对于计算设备的整体安全性度量方案可以包括如下步骤：

第一方面，在操作系统的框架启动阶段，获取基础系统进程的度量值，并将度量值扩展至dTPM。第二方面，获取系统扩展功能进程的度量值并扩展至fTPM。第三方面，在第二方面的基础上，当检测到fTPM中存储的系统扩展功能进程的度量值发生变化时，获取fTPM中所有PCR存储数据的度量值，并将fTPM中所有PCR存储数据的度量值扩展至dTPM中。示例性地，第二方面和第三方面的步骤可以由第一可信度量装置执行，第三方面的步骤可以由第一可信度量装置执行。通过第一方面的步骤能够实现对基础系统进程进行度量，通过第二方面和第三方面能够实现对扩展系统进程进程的度量。从而可以从基础系统进程和扩展系统进程两个方面综合确认计算设备是否可信。

举例来说，计算设备的启动阶段和运行阶段的度量流程可以包括：在计算设备上电时，首先加载运行初始度量根CRTM。需要说明的是，在实际应用中，CRTM可决定计算设备启动时先执行的代码，CRTM本身可以是一段代码，CRTM应当是可信的，其可以存储于BIOS中，CRTM可以不具有写dTPM权限。然后，CRTM获取BIOS的度量值，在确认BIOS可信时，加载BIOS；之后，由于CRTM不具有写权限，由BIOS将BIOS的度量值扩展至dTPM的PCR1；然后，BIOS获取OS基础进程的度量值，将OS基础进程的度量值扩展至dTPM的PCR1中；在确认OS基础进程可信时，加载OS基础进程。示例性地，通过安全启动流程确认BIOS、OS基础进程是否可信。在实际应用中，也可以仅执行度量步骤，而不进行是否可信的判断，度量数据将用于在启动后对启动阶段的安全性的判断。在计算设备的运行阶段，OS基础进程获取APP1的度量值，将APP1的度量值扩展至fTPM的PCR2中，然后加载APP1；同时，OS基础进程获取APP2的度量值，将APP2的度量值扩展至fTPM的PCR3中，然后加载APP2。其中，APP1和APP2是不同应用场景使用的APP，APP1与APP2的运行互不影响，例如，二者运行时所依赖的运行环境互不关联。

表2为被测对象的度量值与存储位置的对应关系的一种示意。

表2

被测对象	被测对象划分	加载阶段	应用场景	度量值的存储位置	
BIOS	第三被测对象	操作系统启动阶段	启动场景	dTPM	PCR1
OS基础进程	第三被测对象	操作系统启动阶段	启动场景	dTPM	PCR1
APP1	第二被测对象	操作系统运行阶段	画图场景	fTPM	PCR2
APP2	第二被测对象	操作系统运行阶段	计时场景	fTPM	PCR3

其中，APP1和APP2对应不同的应用场景，二者的运行互不影响。因此分别使用一个单独的PCR记录二者的度量值。

在本申请实施例，采用将系统扩展功能进程这类被测对象的度量值存储至第一可信模块中的独立PCR的方式，能使得计算设备不需要限制系统扩展功能进程与基础系统进程以固定的顺序启动。即系统扩展功能进程可以独立的启动和退出，不影响基础系统进程的度量和安全性。

在本申请实施例，根据被测对象的加载阶段、是否是第一可信模块和是否是第一可信模块中的数据、应用场景、被测对象的类型，确定被测对象的度量值的存储位置。其中，存储位置包括：存储于第一可信模块或者第二可信模块，存储于全新PCR还是已有PCR等。当需

要将任一被测对象的度量值存储于第一可信模块的全新PCR中时,利用第一可信模块的配置机制增加PCR的个数。需要说明的是,约定第一可信模块仅用来存储与第一可信模块无关的被测对象的度量值。上述步骤可以由本申请实施例的任一可信度量装置执行。

在一示例中,按照被测对象的加载阶段,将加载阶段为操作系统启动阶段的被测对象的度量值发送至第二可信模块,将加载阶段为操作系统运行阶段的被测对象的度量值发送至第二可信模块。

在另一示例中,按照被测对象的应用场景,将各个第二被测对象的度量值扩展至第一可信模块中与第二被测对象的应用场景相对应的PCR中。在一示例中,第一可信模块中的多个PCR与多个应用场景一一对应。在另一示例中,第一可信模块中的某一个PCR可用于存储一个应用场景相关的被测对象的度量值。

在又一示例中,当检测到被测对象与第一可信模块无关且被测对象的类型为APP、进程、程序、日志、数据库、文件、数据时,就确定该被测对象为第二被测对象,并将该被测对象的度量值存储于第一可信模块中。

在本申请实施例的另一应用场景中,对于操作系统在运行阶段受到破坏的情况,采用动态度量的方式来对计算设备上的被测对象进行度量。

需要说明的是,计算设备中加载的对象在初始加载或者启动时未受到攻击,这个时期获得的度量值可以确定计算设备上当前加载运行的对象是可信的。但是,计算设备上的各种对象的运行状态并不是一成不变的。计算设备上的对象在运行过程中有可能受到破坏,即对象启动时获取的度量值不能反映处于运行过程中对象是否可信。如果仍然按照启动时的标准来衡量,可能会给出错误的结果。

图4为本申请提供的可信度量方法的处理流程示意图二。如图4所示,系统度量分为系统启动度量流程和系统运行度量流程,其中,系统启动度量流程的被测对象为基础度量对象,系统允许度量流程的被测对象为扩展度量对象。在实际应用中,运行状态不变的被测对象也可以划分到启动度量流程。

具体的度量方案可以如下:一方面,将系统启动流程涉及的基础度量对象的度量值存储至dTPM。示例性地,系统启动流程包含fTPM的启动流程。另一方面,将系统运行流程涉及的扩展度量对象的度量值存储至fTPM。需要说明的是,运行状态可改变的扩展度量对象的度量值采用独立的PCR存储。此外,在系统运行过程中,若检测到扩展度量对象发生变化,例如,功能模块发生变化,则对发生变化的扩展度量对象重新获取度量值,并更新至fTPM的PCR。之后,对fTPM的所有PCR的值获取对应的度量值,并更新至dTPM。例如,计算fTPM中所有PCR值的摘要并将其扩展到dTPM的PCR中。然后,通过定时验证dTPM的PCR中的数据正确性,来确定所有运行态模块是否可信。

采用动态度量的方式,能够对运行状态可能发生改变的被测对象进行实时度量,从而能够持续地确定计算设备上的被测对象是否可信。

在本申请实施例中,采用第二可信模块存储与第一可信模块中存储的代码、数据以及第一可信模块相关的被测对象的度量值,从而能够利用第二可信模块较高的安全性来提升第一可信模块本身以及第一可信模块中存储的度量值的安全性,进而提升计算设备的安全性。

在本申请实施例的实际应用中,除图3-4所示应用方式外,第一可信模块还可以用于扩展其他应用场景的被测对象的度量值,从而能够从更多的维度衡量计算设备是否可信。

在本申请实施例中,上述第一可信模块和第二可信模块可用于存储计算设备上部署的操

作系统和用户APP等相关的各类被测对象的度量值。当以扩展方式存储被测对象的度量值时，该存储度量值的PCR所存储的数值实际上对应了一条信任链的可信状态。基于信任链的起点以及任一节点均是可信，以扩展方式存储数据能够用来确定计算设备是否始终处于可信状态。

本申请实施例中的其它技术方案细节和技术效果可参见本申请其它实施例中的描述。

5 图 5 为本申请实施例提供的可信度量方法的处理流程示意图三。本申请实施例的执行主体涉及多个进程、进程调度模块。其中，进程 1 为操作系统中正在运行的进程，进程 1 的度量值以扩展方式存储于 PCR1，基于 PCR1 中的值可确定进程 1 是可信的。如图 5 所示，本申请实施例的步骤可以包括：

S501，进程 1 检测到需要调用进程 2。

10 其中，示例性地，进程 1 需要调用进程 2。

S502，进程 1 获取进程 2 的度量值。

其中，在一种实施方式中，进程 1 获取进程 2 的代码，将进程 2 的代码发送至度量执行装置以获取进程 2 的度量值，该种实施方式中，进程 1 获取进程 2 的度量值的过程与前述实施例中可信度量装置获取被测对象的度量值类似。在另一种实施方式中，进程 1 将进程 2 的代码发送至度量执行装置，由度量执行装置获取进程 2 的度量值。其中，度量值执行装置可以为本本地度量模块或者度量服务器。

S503，进程 1 将进程 2 的度量值扩展至 fTPM 的 PCR1 中。

其中，在执行步骤 S503 之前，PCR1 中存储有进程 1 的度量值。在执行步骤 S503 后，PCR1 中存储有根据进程 1 的度量值和进程 2 的度量值拼接的度量值。

20 S504，安全验证模块对 PCR1 中的度量值进行验证。

其中，步骤 S504 为可选的步骤。该步骤可用于确定进程 2 是否可信。

S505，进程 1 通知进程调度模块调用进程 2。

S506，进程调度模块调用进程 2。

S507，进程 2 检测到需要调用进程 3。

25 S508，进程 2 获取进程 3 的度量值。

S509，进程 2 将进程 3 的度量值扩展至 fTPM 的 PCR1。

S510，安全验证模块对 PCR1 中的度量值进行验证。

其中，步骤 S510 为可选的步骤。该步骤可用于确定进程 3 是否可信。

S511，进程 2 通知进程调度模块调用进程 3。

30 S512，可信度量装置获取 fTPM 的所有 PCR1 的度量值，并扩展至 dTPM 的 PCR2 中。

S513，安全验证模块对 PCR2 中的度量值进行验证。

在本申请实施例中，上述进程 1、进程 2、进程 3 也可以为支持可信度量的 APP、应用等。即本申请实施例提供的可信度量方法可以由计算设备中支持可信度量的多个对象共同完成，以确保计算设备的安全性。

35 本申请实施例中的其它技术方案细节和技术效果可参见本申请其它实施例中的描述。

图 6 为本申请实施例提供的可信度量装置的结构示意图一。如图 6 所示，本申请提供一种可信度量装置 600，包括获取模块 601 和发送模块 602。其中，获取模块 601，用于执行前述实施例中步骤 S101；发送模块 602，用于执行前述实施例中步骤 S102。

在本申请实施例中，可信度量装置可以是 APP、程序等。

40 在本申请实施例中，可信度量装置可以是位于计算设备的 OS 中的进程或者 APP，可以在

REE 中,也可以在 TEE 中。

需要说明的是,本申请实施例提供的可信度量装置可用以执行前述实施例中提供的可信度量方法,本申请实施例提供的方法可由计算设备中的一个或多个可信度量装置相互配合实现,具体可参见前述实施例中的描述。在实际应用中,可信度量方法的步骤可以由计算设备中的多个 APP、进程等对象执行。本申请对此不作限制。

图7为本申请实施例提供的可信度量装置的结构示意图二。如图7所示,本申请实施例的可信度量装置700包括:处理器701;存储器702,用于存储一个或多个程序;当所述一个或多个程序被所述一个或多个处理器执行,使得所述一个或多个处理器实现如上述前述实施例可信度量方法中任一可信度量装置执行的步骤。示例性地,该可信度量装置可以是计算设备或者计算设备的组件。在本申请实施例中,可信度量装置700还可以包括接口703,用于与第一可信模块、第二可信模块进行通信,在一些场景中,接口703还可以与验证装置、度量执行装置进行通信。此外,服务器和还可以包括总线704,用于实现可信度量装置内部的通信。在本申请实施例中,可信度量装置还可以是芯片。

本申请实施例中的其它技术方案细节和技术效果可参见本申请其它实施例中的描述。

图8为本申请实施例提供的一种计算设备的结构示意图。如图8所示,本申请提供一种计算设备800,所述计算设备包括:基于所述计算设备的固件实现的第一可信模块801,基于硬件实现的第二可信模块802和可信度量装置803;

其中,所述第一可信模块用于存储计算设备中的第二被测对象的度量值;

其中,可信度量装置803可以为图7所示实施例中的可信度量装置700。

所述第二可信模块用于存储所述第一被测对象的度量值。

在本申请实施例中,计算设备还可以包括:验证装置803。或者,计算设备可与位于计算设备之外的验证装置相连。示例性地,该独立的验证装置是远程验证服务器。

在本申请实施例中,验证装置、远程验证服务器支持执行前述实施例中验证模块执行的方法。在一示例中,验证装置用于从所述第二可信模块中获取所述第一被测对象的度量值,根据所述第一被测对象的度量值确定第一可信模块或者所述第一可信模块中的数据是否可信。在另一示例中,验证装置用于从所述第一可信模块中获取所述第二被测对象的度量值,根据所述第二被测对象的度量值确定第二被测对象是否可信。

在本申请实施例中,计算设备还可以包括度量执行装置804。示例性地,可信度量装置803,具体用于获取所述第一被测对象的完整性参数,向所述度量执行装置发送所述第一被测对象的完整性参数;以及,接收所述度量执行装置发送的所述第一被测对象的度量值。度量执行装置804,用于接收所述第一被测对象的完整性参数,根据所述第一被测对象的完整性参数生成所述第一被测对象的度量值。在本申请其他实施例中,度量执行装置804还可用于接收所述第二被测对象的完整性参数,根据所述第二被测对象的完整性参数生成所述第二被测对象的度量值。

在本申请实施例中,计算设备上可以包括一个或多个可信度量装置。在一示例中,计算设备包括第一可信度量装置和第二可信度量装置,其中,第一可信度量装置用于获取第二被测对象的度量值并将第二被测对象的度量值扩展至第一可信模块的寄存器,第二可信度量装置可以用于执行前述实施例中步骤S101-S102。具体可参看前述实施例中的描述。

在本申请实施例中,计算设备也可以是虚拟机。

在实际应用中,上述实施例中的计算设备中的第一可信模块、第二可信模块、可信度量

装置可组成一种可信度量系统。在一种可能的实现方式中,该系统还可以包括度量执行装置。在一种可能的实现方式中,该系统可以包括位于计算设备中的验证装置或者独立于计算设备之外的远程验证服务器。

本申请实施例中的其它技术方案细节和技术效果可参见本申请其它实施例中的描述。

- 5 本申请提供一种可信度量程序,所述可信度量程序被执行时用于前述实施例中任一实施例中的可信度量方法。

本申请提供一种计算机可读存储介质,所述计算机可读存储介质中存储有指令,所述指令可以由处理电路上的一个或多个处理器执行。当其在计算机上运行时,使得计算机执行上述前述实施例中任意可能的实现方式中的方法。

- 10 本申请实施例中的其它技术方案细节和技术效果可参见本申请其它实施例中的描述。

- 在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时,可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时,全部或部分地产生按照本申请所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线)或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质,(例如,软盘、硬盘、磁带)、光介质(例如,DataVData)、或者半导体介质(例如固态硬盘 Solid State Dataisk)等。
- 15
- 20

权 利 要 求

1、一种可信度量方法，其特征在于，包括：

5 获取计算设备中的第一被测对象的度量值，所述第一被测对象的度量值用于确定所述计算设备中基于固件实现的第一可信模块是否可信；所述第一可信模块用于存储所述计算设备中的第二被测对象的度量值；

将所述第一被测对象的度量值发送至基于硬件实现的第二可信模块。

2、根据权利要求1所述的方法，其特征在于，所述第一被测对象包括以下至少一种：所述
10 所述第一可信模块或所述第一可信模块中的数据。

3、根据权利要求1或2所述的方法，其特征在于，所述第二被测对象的度量值为采用扩展操作的方式存储于所述第一可信模块的第一寄存器中的；

所述所述第一被测对象的度量值为采用扩展操作的方式存储于所述第二可信模块的第二寄存器中的。

4、根据权利要求1-3任一所述的方法，其特征在于，

15 所述第一可信模块为基于固件的可信平台模块fTPM，所述第二被测对象的度量值存储于所述第一可信模块的平台配置寄存器PCR；和/或，

所述第二可信模块为离散可信平台模块dTPM或集成可信平台模块，所述第一被测对象的度量值存储于所述第二可信模块的PCR。

5、根据权利要求1-4任一所述的方法，其特征在于，所述第一被测对象包括所述第二被
20 测对象的度量值；

在所述获取计算设备中的第一被测对象的度量值之前，所述方法还包括：

获取所述第二被测对象的度量值；其中，所述第二被测对象包括以下至少一种：所述计
算设备中的APP、进程、程序、日志、数据库、文件和数据；

将所述第二被测对象的度量值发送至所述第一可信模块。

6、根据权利要求1-5任一所述的方法，其特征在于，在所述获取计算设备中的第一被测
25 对象的度量值之前，包括：检测到所述第一被测对象发生变更。

7、根据权利要求1-6所述的方法，其特征在于，所述获取计算设备中的第一被测对象的度量值，包括：获取至少两个第一被测对象对应的一个度量值。

8、一种可信度量装置，其特征在于，包括：

30 获取模块，用于获取计算设备中的第一被测对象的度量值，所述第一被测对象的度量值用于确定所述计算设备中基于固件实现的第一可信模块是否可信；所述第一可信模块用于存储所述计算设备中的第二被测对象的度量值；

发送模块，用于将所述第一被测对象的度量值发送至基于硬件实现的第二可信模块。

9、根据权利要求8所述的装置，其特征在于，所述第一被测对象包括以下至少一种：所
35 述第一可信模块或所述第一可信模块中的数据。

10、根据权利要求8或9所述的装置，其特征在于，所述第二被测对象的度量值为采用扩展操作的方式存储于所述第一可信模块的第一寄存器中的；

所述所述第一被测对象的度量值为采用扩展操作的方式存储于所述第二可信模块的第二寄存器中的。

40 11、根据权利要求8-10任一所述的装置，其特征在于，

所述第一可信模块为基于固件的可信平台模块fTPM，所述第二被测对象的度量值存储于

所述第一可信模块的平台配置寄存器PCR；和/或，

所述第二可信模块为离散可信平台模块dTPM，或，集成可信平台模块，所述第一被测对象的度量值存储于所述第二可信模块的PCR。

12、根据权利要求8-11任一所述的装置，其特征在于，

5 所述获取模块，还用于在所述获取计算设备中的第一被测对象的度量值之前，获取所述第二被测对象的度量值；其中，所述第一被测对象包括所述第二被测对象的度量值；所述第二被测对象包括以下至少一种：所述计算设备中的APP、进程、程序、日志、数据库、文件、数据；

所述发送模块，还用于将所述第二被测对象的度量值发送至所述第一可信模块。

10 13、根据权利要求8-12任一所述的装置，其特征在于，所述获取模块，还用于在检测到所述第一被测对象发生变更后，执行所述获取计算设备中的第一被测对象的度量值的步骤。

14、根据权利要求8-13任一所述的装置，其特征在于，所述获取模块，具体用于获取至少两个第一被测对象对应的一个度量值。

15 15、一种计算设备，其特征在于，所述计算设备包括：基于所述计算设备的固件实现的第一可信模块，基于硬件实现的第二可信模块和如权利要求8-14任一所述的可信度量装置；

其中，所述第一可信模块用于存储计算设备中的第二被测对象的度量值；

所述第二可信模块用于存储所述第一被测对象的度量值。

16、根据权利要求15所述的计算设备，其特征在于，所述计算设备还包括：

20 验证装置，用于从所述第二可信模块中获取所述第一被测对象的度量值，根据所述第一被测对象的度量值确定所述第一被测对象是否可信。

17、根据权利要求15或16所述的计算设备，其特征在于，所述计算设备还包括：度量执行装置；

25 所述可信度量装置，具体用于获取所述第一被测对象的完整性参数，向所述度量执行装置发送所述第一被测对象的完整性参数；以及，接收所述度量执行装置发送的所述第一被测对象的度量值；

所述度量执行装置，用于接收所述第一被测对象的完整性参数，根据所述第一被测对象的完整性参数生成所述第一被测对象的度量值。

18、一种可信度量程序，其特征在于，所述可信度量程序被执行时用于实现权利要求1-7任一所述的可信度量方法。

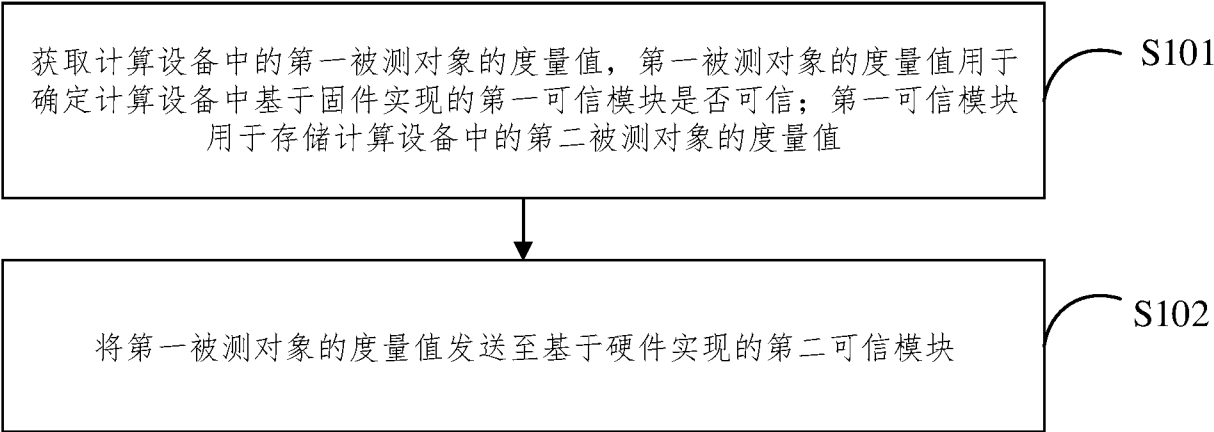


图 1

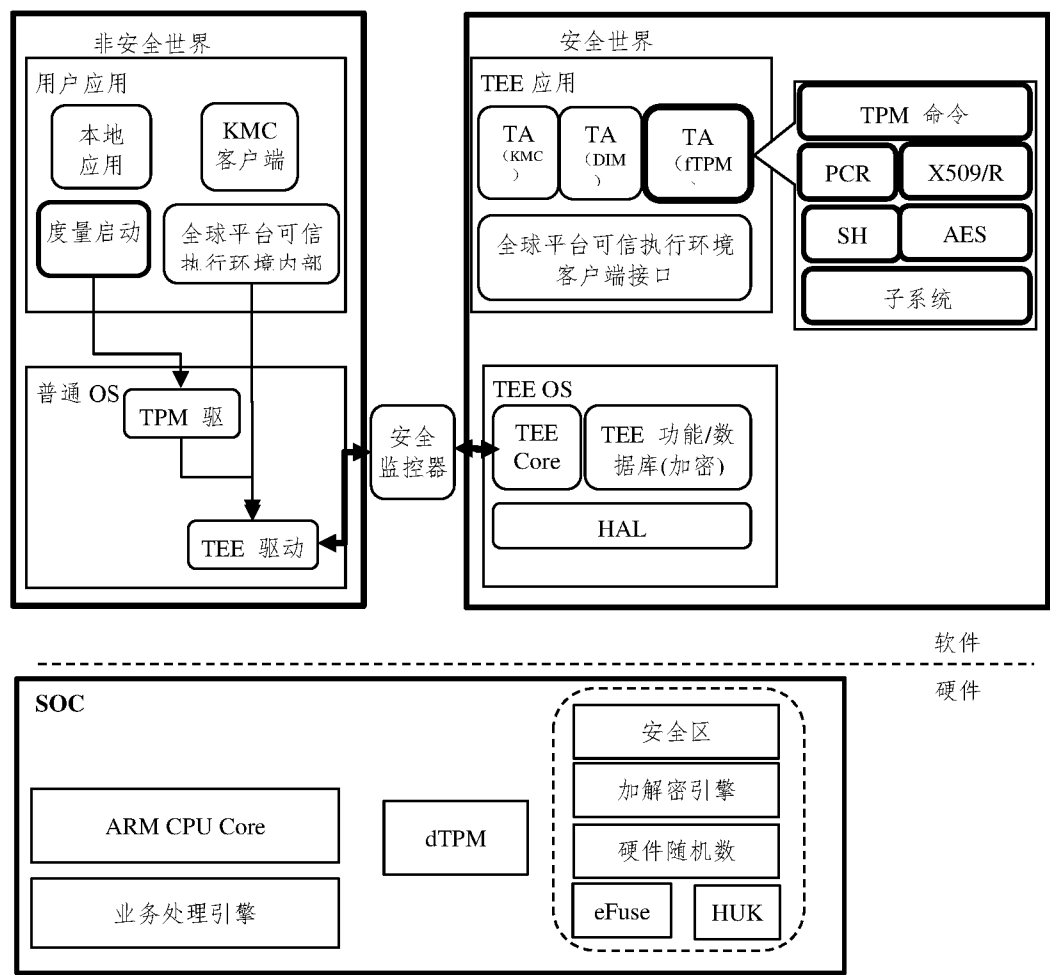


图 2

2/4

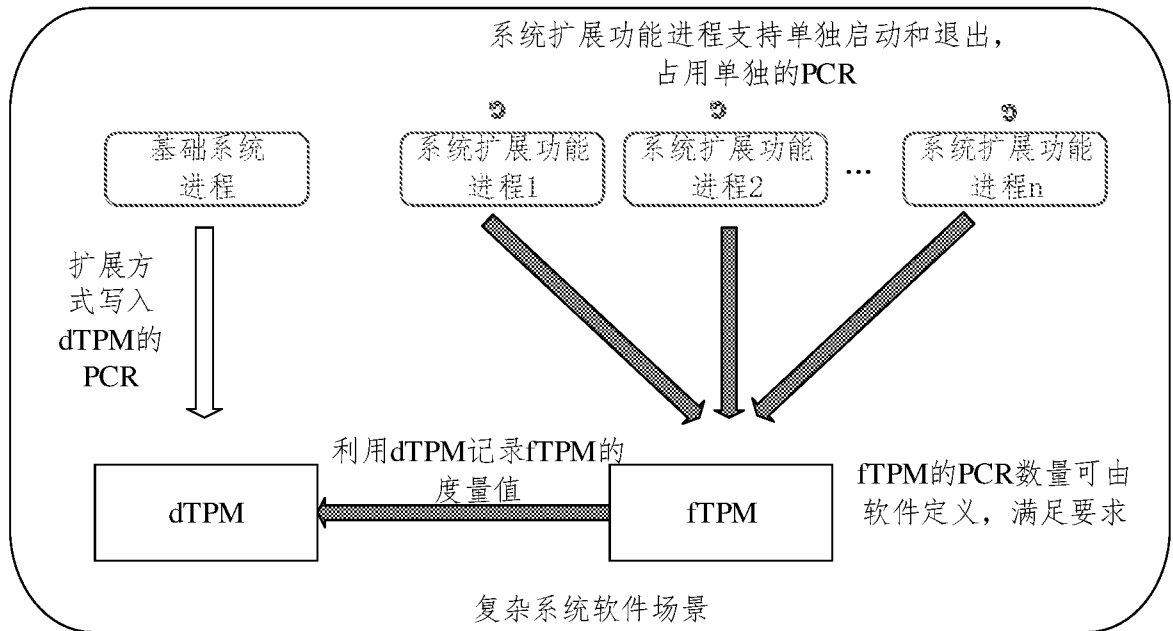


图 3

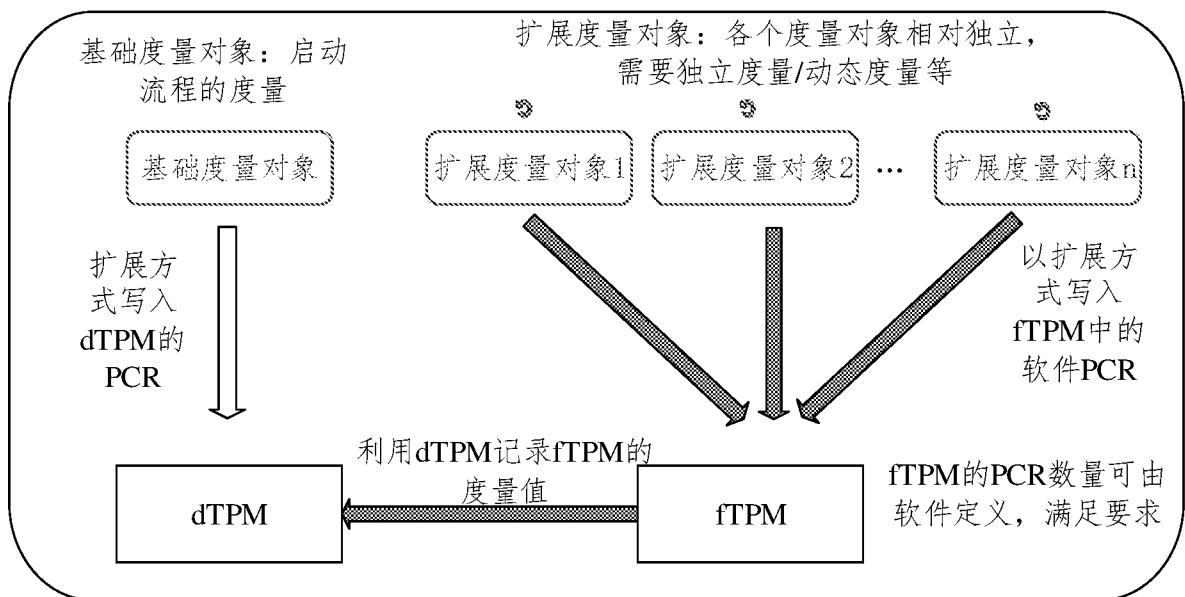


图 4

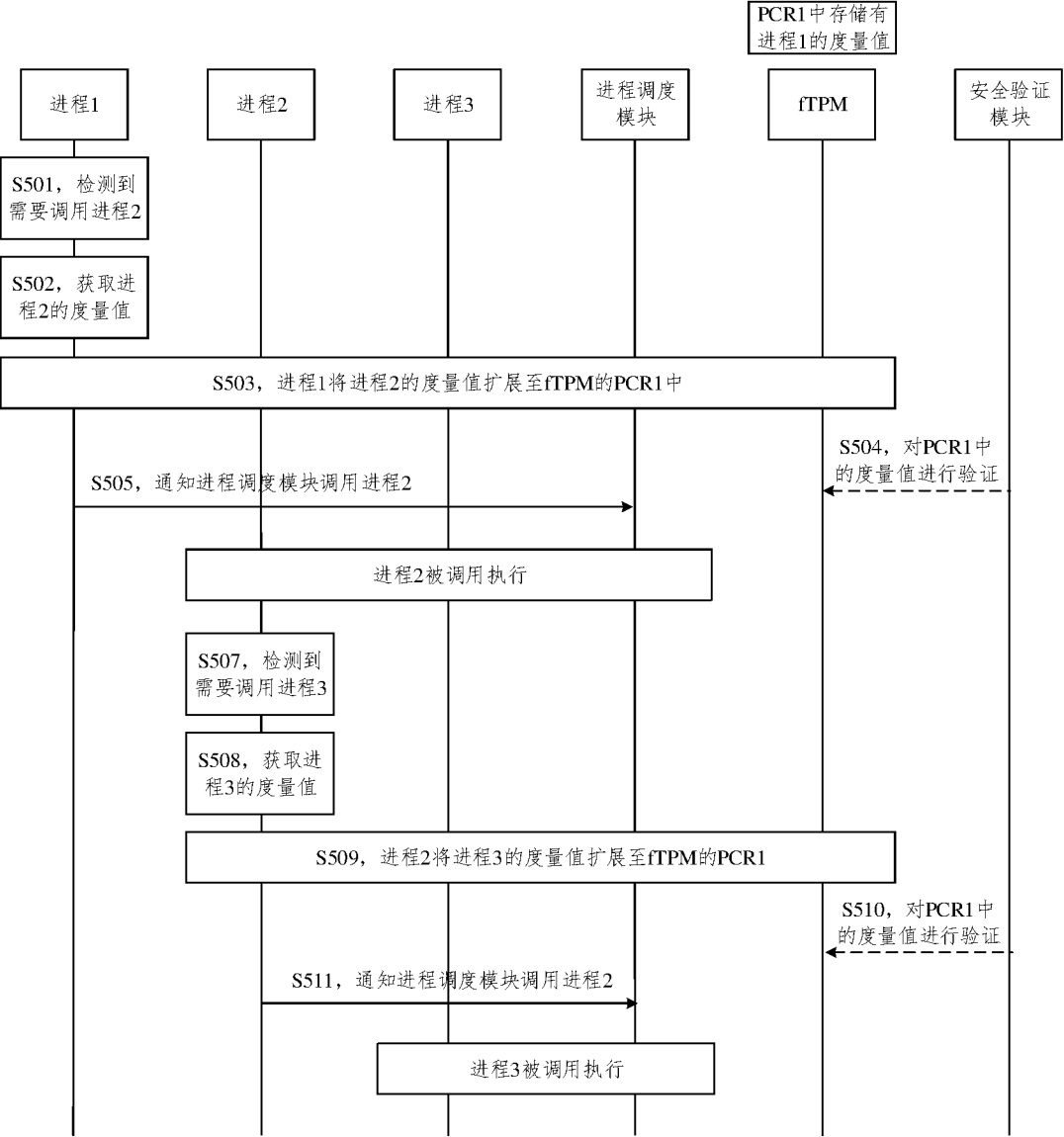


图 5

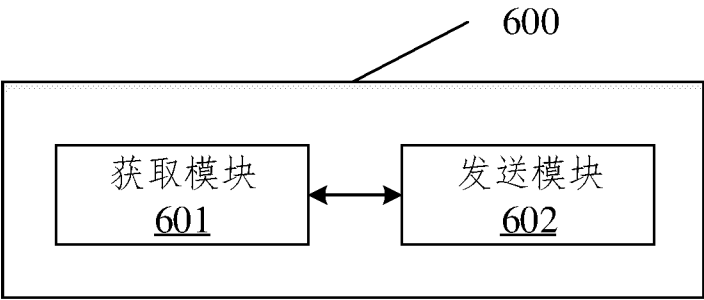


图 6

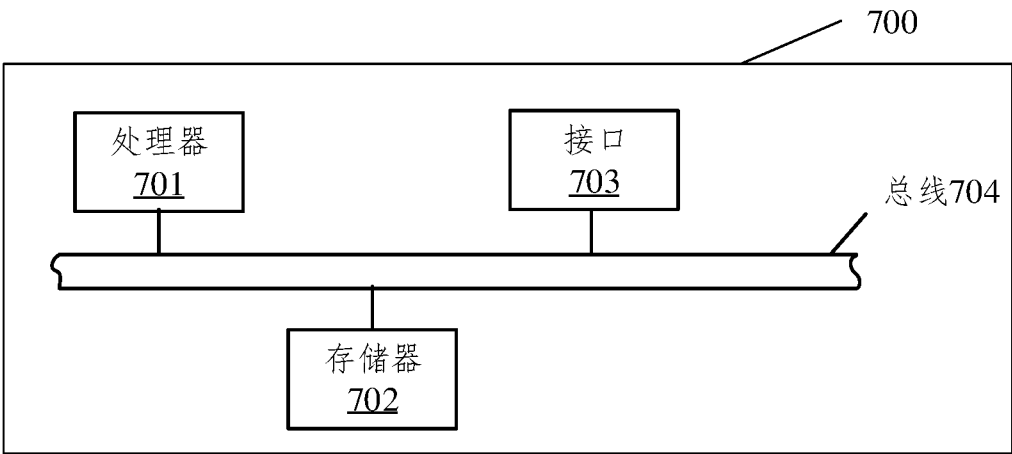


图 7

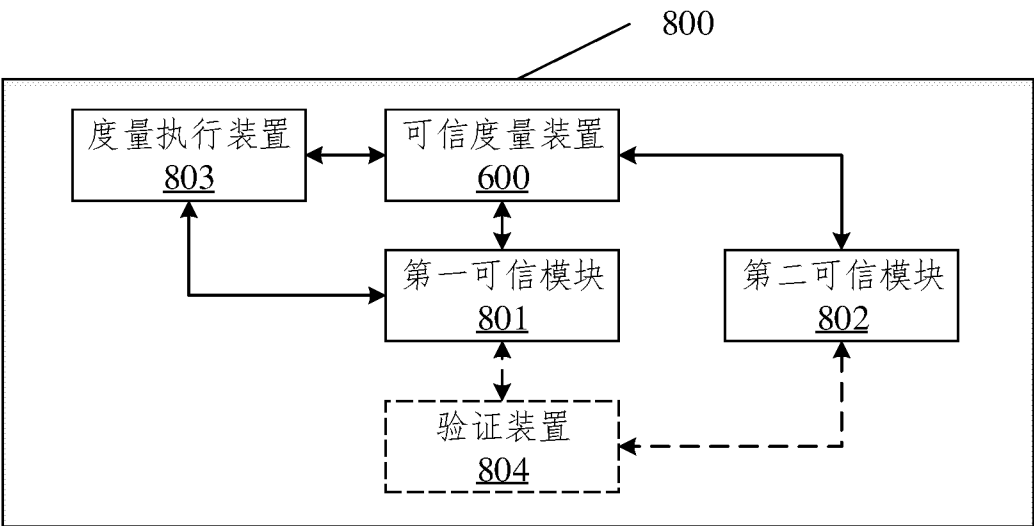


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/080810

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/57(2013.01)i; 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)

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, WPI, EPODOC, CNKI, IEEE: 可信, 度量, 第一, 第二, 扩展, 寄存器, 固件, 硬件, 离散, 进程, 应用程序, 可信平台, trust, measure, first, second, extend, register, firmware, hardware, discrete, process, application, APP, TPM

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 107451479 A (INSPUR (BEIJING) ELECTRONIC INFORMATION INDUSTRY CO., LTD.) 08 December 2017 (2017-12-08) description paragraphs 0058-0100	1-18
A	CN 105389513 A (HUAWEI TECHNOLOGIES CO., LTD.) 09 March 2016 (2016-03-09) entire document	1-18
A	CN 106127056 A (LANGCHAO ELECTRONIC INFORMATION INDUSTRY CO., LTD.) 16 November 2016 (2016-11-16) entire document	1-18
A	CN 102436566 A (AUTOMATION RESEARCH AND DESIGN INSTITUTE OF METALLURGICAL INDUSTRY) 02 May 2012 (2012-05-02) entire document	1-18
A	US 2019114431 A1 (BAIDU USA LLC.) 18 April 2019 (2019-04-18) entire document	1-18



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

02 June 2021

Date of mailing of the international search report

16 June 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/CN2021/080810

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107451479	A	08 December 2017	None			
CN	105389513	A	09 March 2016	None			
CN	106127056	A	16 November 2016	None			
CN	102436566	A	02 May 2012	None			
US	2019114431	A1	18 April 2019	CN	109669734	A	23 April 2019

国际检索报告

国际申请号

PCT/CN2021/080810

A. 主题的分类

G06F 21/57(2013.01)i; 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)

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, WPI, EPDOC, CNKI, IEEE: 可信, 度量, 第一, 第二, 扩展, 寄存器, 固件, 硬件, 离散, 进程, 应用程序, 可信平台, trust, measure, first, second, extend, register, firmware, hardware, discrete, process, application, APP, TPM

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
X	CN 107451479 A (浪潮北京电子信息产业有限公司) 2017年 12月 8日 (2017 - 12 - 08) 说明书第0058-0100段	1-18
A	CN 105389513 A (华为技术有限公司) 2016年 3月 9日 (2016 - 03 - 09) 全文	1-18
A	CN 106127056 A (浪潮电子信息产业股份有限公司) 2016年 11月 16日 (2016 - 11 - 16) 全文	1-18
A	CN 102436566 A (冶金自动化研究设计院) 2012年 5月 2日 (2012 - 05 - 02) 全文	1-18
A	US 2019114431 A1 (BAIDU USA LLC) 2019年 4月 18日 (2019 - 04 - 18) 全文	1-18

☐ 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

2021年 6月 2日

国际检索报告邮寄日期

2021年 6月 16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

李玉坤

电话号码 86-(10)-53961358

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/080810

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	107451479	A	2017年 12月 8日	无	
CN	105389513	A	2016年 3月 9日	无	
CN	106127056	A	2016年 11月 16日	无	
CN	102436566	A	2012年 5月 2日	无	
US	2019114431	A1	2019年 4月 18日	CN 109669734 A	2019年 4月 23日