(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
2020 年 10 月 1 日 (01.10.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/192287 A1

(51) 国际专利分类号:
G06F 21/57 (2013.01)

(21) 国际申请号: PCT/CN2020/074980

(22) 国际申请日: 2020 年 2 月 13 日 (13.02.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910224103.9 2019年3月22日 (22.03.2019) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (**ALIBABA GROUP HOLDING LIMITED**) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: 潘无穷 (**PAN, Wuqiong**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (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, 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 COMPUTING METHOD, AND SERVER

(54) 发明名称: 一种可信计算方法及服务器

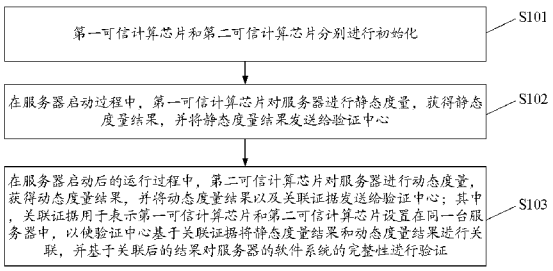

图 1

S101 A first trusted computing chip and a second trusted computing chip perform initialization separately

S102 During a startup process of a server, a first trusted computing chip performs a static measurement on the server, acquires a static measurement result, and sends the static measurement result to a verification center

S103 During an operation process after startup of the server, the second trusted computing chip performs a dynamic measurement on the server, acquires a dynamic measurement result, and sends the dynamic measurement result and association evidence to the verification center, wherein the association evidence indicates that the first trusted computing chip and the second trusted computing chip are provided within the same server, such that the verification center associates the static measurement result and the dynamic measurement result on the basis of the association evidence, and verifies the integrity of a software system of the server on the basis of the associated results

(57) **Abstract:** Disclosed in an embodiment of the present disclosure is a trusted computing method, applicable in a server. The server is provided with a first and second trusted computing chip. The method comprises: during a startup process of the server, the first trusted computing chip performing a static measurement on the server, acquiring a static measurement result, and sending the same to a verification center; and during an operation process after startup of the server, the second trusted computing chip performing a dynamic measurement on the server, acquiring a dynamic measurement result, and sending the same along with association evidence to the verification center, wherein the association evidence indicates that the first trusted computing chip and the second trusted computing chip are provided within the same server, such that the verification center associates the two measurement results, and then verifies the integrity of a software system of the server. In this way, the invention conducts both a static measurement and a dynamic measurement, and improves reliability of trusted computing, thereby achieving a technical effect of meeting requirements of high-security scenarios. Further disclosed is a server.

WO 2020/192287 A1

[见续页]

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: 本说明书实施例公开了一种可信计算方法，应用于服务器中，服务器中设置有第一和第二可信计算芯片，该方法包括：在服务器启动过程中，第一可信计算芯片对服务器进行静态度量，获得静态度量结果，并将其发送给验证中心；在服务器启动后的运行过程中，第二可信计算芯片对服务器进行动态度量，获得动态度量结果，并将其与关联证据一起发送给验证中心；关联证据表示第一可信计算芯片和第二可信计算芯片设置在同一台服务器中，以使验证中心将两个度量结果进行关联，再对服务器的软件系统的完整性进行验证。如此，实现了同时进行静态度量和动态度量，提高了可信计算的可靠性，从而满足高安全场景的需求的技术效果。同时，本发明还公开了一种服务器。

一种可信计算方法及服务器

技术领域

[01] 本说明书实施例涉及互联网技术领域，尤其涉及一种可信计算方法及服务器。

背景技术

[02] 可信计算技术主要用于保障系统软件不被攻击者篡改，目前实施的主要是静态度量，静态度量主要是保障系统启动过程中软件的完整性，并不能保证系统运行过程中的软件的完整性。动态度量主要是保障系统运行过程中软件的完整性，但动态度量并没有被真正使用，导致可信计算的结果的可靠性较低，难以满足一些高安全场景（比如：金融公司的数据中心）的需求。

发明内容

[03] 本说明书实施例通过提供一种可信计算方法及服务器，解决了现有技术中在对服务器进行可信计算时，其计算结果的可靠性较低的技术问题，实现了同时进行静态度量和动态度量，提高了可信计算的可靠性，从而满足高安全场景的需求的技术效果。

[04] 一方面，本说明书通过本说明书的一实施例提供如下技术方案：

[05] 一种可信计算方法，应用于服务器中，所述服务器中设置有第一可信计算芯片和第二可信计算芯片，所述方法包括：

[06] 在所述服务器启动过程中，所述第一可信计算芯片对所述服务器进行静态度量，获得静态度量结果，并将所述静态度量结果发送给验证中心；

[07] 在所述服务器启动后的运行过程中，所述第二可信计算芯片对所述服务器进行动态度量，获得动态度量结果，并将所述动态度量结果以及关联证据发送给所述验证中心；其中，所述关联证据用于表示所述第一可信计算芯片和所述第二可信计算芯片设置在同一台服务器中，以使所述验证中心基于所述关联证据将所述静态度量结果和所述动态度量结果进行关联，并基于关联后的结果对所述服务器的软件系统的完整性进行验证。

[08] 优选地，所述第一可信计算芯片插在所述服务器上的串行外设接口 SPI 接口或低引脚数目 LPC 接口，所述第二可信计算芯片插在所述服务器上的总线和接口标准 PCIE 接口或串行高级技术附件 SATA 接口或通用串行总线 USB 接口。

[09] 优选地，在所述第一可信计算芯片对所述服务器进行静态度量之前，还包括:

[10] 所述第一可信计算芯片接收证书颁发机构签发的第一设备证书，以及所述第二可信计算芯片接收所述证书颁发机构签发的第二设备证书;

[11] 其中，在所述第一可信计算芯片将所述静态度量结果发送给验证中心时，所述第一可信计算芯片还将所述第一设备证书发给所述验证中心，以使所述验证中心对所述第一设备证书进行验证;

[12] 在所述第二可信计算芯片将所述动态度量结果发送给验证中心时，所述第二可信计算芯片还将所述第二设备证书发给所述验证中心，以使所述验证中心对所述第二设备证书进行验证。

[13] 优选地，在所述第一可信计算芯片对所述服务器进行静态度量之前，还包括:

[14] 所述第二可信计算芯片接收所述证书颁发机构签署的所述关联证据。

[15] 优选地，所述关联证据，包括:

[16] 所述第一可信计算芯片的标识信息;

[17] 所述第二可信计算芯片的标识信息;

[18] 所述证书颁发机构的签名。

[19] 优选地，所述第一可信计算芯片对所述服务器进行静态度量，获得静态度量结果，包括:

[20] 所述第一可信计算芯片采集所述服务器中的基本输入/输出系统 BIOS 的程序代码、引导程序 Bootloader 的程序代码、操作系统 OS 的程序代码;

[21] 所述第一可信计算芯片基于所述 BIOS 的程序代码、所述 Bootloader 的程序代码、以及所述 OS 的程序代码，生成所述静态度量结果。

[22] 优选地，所述第二可信计算芯片对所述服务器进行动态度量，获得动态度量结果，包括:

[23] 所述第二可信计算芯片采集应用程序的静态可执行性程序代码、以及所述应用程序运行时在内存中的程序代码，所述应用程序安装在所述服务器上;

[24] 所述第二可信计算芯片基于所述应用程序的静态可执行性程序代码、以及所述应用程序运行时在内存中的程序代码，生成所述动态度量结果。

[25] 优选地，在所述第二可信计算芯片将所述动态度量结果以及关联证据发送给所述验证中心之后，还包括:

[26] 所述第一可信计算芯片接收所述验证中心反馈的第一验证结果，所述第一验证结果与所述静态度量对应;

[27] 所述第二可信计算芯片接收所述验证中心反馈的第二验证结果，所述第二验证结果与所述动态度量对应，所述第二验证结果中携带有所述关联证据。

[28] 另一方面，本说明书通过本说明书的一实施例，提供如下技术方案:

[29] 一种服务器，包括:

[30] 主板;

[31] 第一可信计算芯片，设置在所述主板上，用于在所述服务器启动过程中，对所述服务器进行静态度量，获得静态度量结果，并将所述静态度量结果发送给验证中心;

[32] 第二可信计算芯片，设置在所述主板上，用于在所述服务器启动后的运行过程中，对所述服务器进行动态度量，获得动态度量结果，并将所述动态度量结果以及关联证据发送给所述验证中心;

[33] 其中，所述关联证据用于表示所述第一可信计算芯片和所述第二可信计算芯片设置在同一台服务器中，以使所述验证中心基于所述关联证据将所述静态度量结果和所述动态度量结果进行关联，并基于关联后的结果对所述服务器的软件系统的完整性进行验证。

[34] 优选地，所述第一可信计算芯片插在所述服务器上的串行外设接口 SPI 接口或低引脚数目 LPC 接口，所述第二可信计算芯片插在所述服务器上的总线和接口标准 PCIE 接口或串行高级技术附件 SATA 接口或通用串行总线 USB 接口。

[35] 优选地，所述第一可信计算芯片，还用于:

[36] 在对所述服务器进行静态度量之前，接收证书颁发机构签发的第一设备证书；在将所述静态度量结果发送给验证中心时，还将所述第一设备证书发给所述验证中心，以使所述验证中心对所述第一设备证书进行验证;

[37] 所述第二可信计算芯片，还用于:

[38] 在所述第一可信计算芯片对所述服务器进行静态度量之前，接收所述证书颁发机构签发的第二设备证书；在将所述动态度量结果发送给验证中心时，还将所述第二设备

证书发给所述验证中心，以使所述验证中心对所述第二设备证书进行验证。

[39] 优选地，所述第二可信计算芯片，还用于：

[40] 在所述第一可信计算芯片对所述服务器进行静态度量之前，接收所述证书颁发机构签署的所述关联证据。

[41] 优选地，所述关联证据，包括：

[42] 所述第一可信计算芯片的标识信息；

[43] 所述第二可信计算芯片的标识信息；

[44] 所述证书颁发机构的签名。

[45] 优选地，所述第一可信计算芯片，具体用于：

[46] 采集所述服务器中的基本输入/输出系统 BIOS 的程序代码、引导程序 Bootloader 的程序代码、操作系统 OS 的程序代码；基于所述 BIOS 的程序代码、所述 Bootloader 的程序代码、以及所述 OS 的程序代码，生成所述静态度量结果。

[47] 优选地，所述第二可信计算芯片，具体用于：

[48] 采集应用程序的静态可执行性程序代码、以及所述应用程序运行时在内存中的程序代码，所述应用程序安装在所述服务器上；基于所述应用程序的静态可执行性程序代码、以及所述应用程序运行时在内存中的程序代码，生成所述动态度量结果。

[49] 优选地，所述第一可信计算芯片，还用于：接收所述验证中心反馈的第一验证结果，所述第一验证结果与所述静态度量对应；

[50] 所述第二可信计算芯片，还用于：接收所述验证中心反馈的第二验证结果，所述第二验证结果与所述动态度量对应，所述第二验证结果中携带有所述关联证据。

[51] 本说明书实施例中提供的一个或多个技术方案，至少具有如下技术效果或优点：

[52] 在本说明书实施例中，公开了一种可信计算方法，应用于服务器中，所述服务器中设置有第一可信计算芯片和第二可信计算芯片，所述方法包括：在所述服务器启动过程中，所述第一可信计算芯片对所述服务器进行静态度量，获得静态度量结果，并将所述静态度量结果发送给验证中心；在所述服务器启动后的运行过程中，所述第二可信计算芯片对所述服务器进行动态度量，获得动态度量结果，并将所述动态度量结果、以及关联证据发送给验证中心；其中，所述关联证据用于表示所述第一可信计算芯片和所述

第二可信计算芯片设置在同一台服务器中，以使所述验证中心用于基于所述关联证据将所述静态度量结果和所述动态度量结果进行关联，并基于关联后的结果对所述服务器的软件系统的完整性进行验证。由于在服务器中设置了两个相关联的可信计算芯片，其中，第一可信计算芯片用于对所述服务器进行静态度量，第二可信计算芯片用于对服务器进行动态度量，并将静态度量结果和动态度量结果同时发给验证中心，以使得验证中心可以基于静态度量结果和动态度量结果一起对业务服务器的软件系统的完成性进行验证。如此，解决了现有技术中在对服务器进行可信计算时，其计算结果的可靠性较低的技术问题，实现了同时进行静态度量和动态度量，提高了可信计算的可靠性，从而满足高安全场景的需求的技术效果。

附图说明

[53] 为了更清楚地说明本说明书实施例中的技术方案，下面将对实施例描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本说明书实施例的一些实施例，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。

[54] 图 1 为本说明书实施例中一种可信计算方法的流程图；

[55] 图 2 为本说明书实施例中一种可信计算方法的动态展示图；

[56] 图 3 为本说明书实施例中一种服务器的结构图。

具体实施方式

[57] 在正式介绍本方法之前，先对现有技术进行如下介绍：

[58] 可信计算芯片，是可信计算信任的基础，与上层验证软件一同完成可信计算的功能。国外一般称为 TPM(Trusted Platform Module)，国内一般称为 TPCM(Trusted Platform Control Module ）。

[59] 可信计算技术主要用于保障系统软件不被攻击者篡改，目前实施的主要是静态度量，静态度量主要是保障系统启动过程中软件的完整性，并不能保证系统运行过程中的软件的完整性。动态度量主要是保障系统运行过程中软件的完整性，但动态度量并没有被真正使用。

[60] 其中一个原因是：动态度量对性能要求很高，动态度量通常是周期性进行的，并

且每次都对所有软件进行度量。而现有的 TPM/TPCM 芯片都是低价、低性能的密码芯片，不能满足动态度量的要求。

[61] 另一个原因是：现有 TPM/TPCM 都是采用 SPI 接口，这个接口传输性能非常低，之所以采用这个接口是因为只有这个接口在系统早期的时候能够使用，而 TPM/TPCM 又要求在系统早期的时候运行以验证 BIOS 的完整性。但针对一些高安全场景（比如：金融公司的数据中心），则需要进行动态度量，这就需要一个高速传输接口，而 SPI 接口又无法满足这样的需求。

[62] 综上原因，导致现有技术中在对服务器进行可信计算时，其计算结果的可靠性较低，难以满足一些高安全场景（比如：金融公司的数据中心）的需求。

[63] 本说明书实施例通过提供一种可信计算方法及服务器，解决了在对服务器进行可信计算时，其计算结果的可靠性较低的技术问题。实现了同时进行静态度量和动态度量，提高了可信计算的可靠性，从而满足高安全场景的需求的技术效果。

[64] 本说明书实施例的技术方案为解决上述技术问题，总体思路如下：

[65] 一种可信计算方法，应用于服务器中，所述服务器中设置有第一可信计算芯片和第二可信计算芯片，所述方法包括：在所述服务器启动过程中，所述第一可信计算芯片对所述服务器进行静态度量，获得静态度量结果，并将所述静态度量结果发送给验证中心；在所述服务器启动后的运行过程中，所述第二可信计算芯片对所述服务器进行动态度量，获得动态度量结果，并将所述动态度量结果以及关联证据发送给所述验证中心；其中，所述关联证据用于表示所述第一可信计算芯片和所述第二可信计算芯片设置在同一台服务器中，以使所述验证中心用于基于所述关联证据将所述静态度量结果和所述动态度量结果进行关联，并基于关联后的结果对所述服务器的软件系统的完整性进行验证。

[66] 为了更好的理解上述技术方案，下面将结合说明书附图以及具体的实施方式对上述技术方案进行详细的说明。

实施例一

[67] 本实施例提供了一种可信计算方法，应用于服务器中，该服务器中同时设置有第一可信计算芯片和第二可信计算芯片（即：具有双信任根）。其中，第一可信计算芯片插在服务器主板上的 SPI（Serial Peripheral Interface，串行外设接口）接口上，第二可信计算芯片插在服务器主板上的 PCIE（Peripheral Component Interface Express，总线和接口标准）接口上，第二可信计算芯片的性能高于第一可信计算芯片。

[68] SPI 接口属于低速接口，其在服务器启动过程中就能使用（具体来讲，在主板上电时即可使用），第一可信计算芯片插在 SPI 接口上，可用于对服务器进行静态度量。其中，由于在服务器启动过程中（也可以理解成在服务器的 OS 启动过程中），其软件环境比较简单，使得静态度量需要的运算量较小，因此，第一可信计算芯片采用 TPM/TPCM 芯片即可。一般来讲，TPM/TPCM 可以满足静态度量的需求，且一般价格较低，有利于节约成本。

[69] 在具体实施过程中，也可以将第一可信计算芯片插在服务器主板上的 LPC（Low Pin Count，低引脚数目）接口上，LPC 接口与 SPI 接口类似，在服务器动过程中就能使用（即：在主板上电时时即可使用）。

[70] PCIE 接口属于高速接口，其只能在服务器启动完成后使用（即：在服务器运行过程中才能使用）。由于在服务器启动后的运行过程中，OS 上的应用程序较多，且功能复杂，导致动态度量所需的运算量较大，因此，第二可信计算芯片采用高性能安全芯片（一般价格较高），其性能远高于第一可信计算芯片，且配合 PCIE 高速接口，可以满足动态度量的需求。

[71] 在具体实施过程中，也可以将第二可信计算芯片插在服务器主板上的 SATA（Serial Advanced Technology Attachment，串行高级技术附件）接口上或 USB（Universal Serial Bus，通用串行总线）接口，SATA 接口也属于高速接口，可以满足高速的数据传输的需求。

[72] 如图 1 所示，所述可信计算方法，包括：

[73] 步骤 S101：第一可信计算芯片和第二可信计算芯片分别进行初始化。

[74] 具体来讲，在第一可信计算芯片初始化时，第一可信计算芯片可以接收到 CA（Certificate Authority，证书颁发机构）签发的第一设备证书。

[75] 在具体实施过程中，如图 2 所示，第一可信计算芯片在初始化前，其中可能没有设备证书，也有可能在出厂前带有设备证书，出于安全考虑，无论第一可信计算芯片内原先有没有设备证书，在进行初始化时，都由证书颁发机构重新签发一个新的设备证书（即：第一设备证书），并将原来的设备证书作废。其中，第一设备证书中存储有与第一可信计算芯片的私钥对应的公钥。证书颁发机构向第一可信计算芯片签发第一设备证书，则代表证书颁发机构认可第一可信计算芯片的身份合法。

[76] 同理，在第二可信计算芯片初始化时，第二可信计算芯片可以接收到证书颁发机

构签发的第二设备证书。

[77] 在具体实施过程中，第二可信计算芯片在初始化前，其中可能没有设备证书，也有可能在出厂前带有设备证书，出于安全考虑，无论第二可信计算芯片内原先有没有设备证书，都由证书颁发机构重新签发一个新的设备证书（即：第二设备证书），并将原来的设备证书作废。其中，第二设备证书存储有与第二可信计算芯片的私钥对应的公钥。证书颁发机构向第二可信计算芯片签发第二设备证书，则代表证书颁发机构认可第二可信计算芯片的身份合法。

[78] 在具体实施过程中，证书颁发机构可以为一台服务器，或者为一组服务器集群。

[79] 作为一种可选的实施例，在第一可信计算芯片和第二可信计算芯片需要进行初始化时，第二可信计算芯片还会接收到证书颁发机构签署的关联证据。该关联证据用于表示第一可信计算芯片和第二可信计算芯片设置在同一台服务器中，用于将同一台服务器内的第一可信计算芯片和第二可信计算进行绑定。此处，关联证据的使用，可以避免攻击者使用不同主机的度量结果拼凑出一个合法的度量结果。

[80] 在具体实施过程中，所述关联证据，主要包括：第一可信计算芯片的标识信息（例如：ID 号）、第二可信计算芯片的标识信息（例如：ID 号）、以及证书颁发机构的签名。

[81] 举例来讲，证书颁发机构可以基于其私钥（即：证书颁发机构的私钥）对第一可信计算芯片的 ID 号和第二可信计算芯片的 ID 号进行签名（即：私钥加密），获得所述关联证据。

[82] 在第一可信计算芯片和第二可信计算芯片完成初始化后，即可执行步骤 S102。

[83] 步骤 S102：在服务器启动过程中，第一可信计算芯片对服务器进行静态度量，获得静态度量结果，并将静态度量结果发送给验证中心。

[84] 静态度量：静态度量发生在开机的过程中，能够保证系统刚开机的时候的安全性。其主要是指对 BIOS、Bootloader、OS 等代码进行度量，检测其是否被篡改。该度量过程是伴随着系统启动过程完成的，每部分软件在运行前由调用它的软件进行度量，

[85] 在具体实施过程中，第一可信计算芯片主要负责采集静态度量所需的数据，并生成静态度量结果。

[86] 具体来讲，第一可信计算芯片可以采集服务器中的 BIOS 的程序代码（Basic Input /

Output System，基本输入/输出系统）、OPROM（拓展只读存储器）中的程序代码、Bootloader（引导程序）的程序代码、OS（Operating System，操作系统）的程序代码；并基于 BIOS 的程序代码、OPROM（拓展只读存储器）中的程序代码、Bootloader 的程序代码、以及 OS 的程序代码，生成静态度量结果（其中即包含第一可信计算芯片采集到的这些程序代码）。

[87] 步骤 S103：在服务器启动后的运行过程中，第二可信计算芯片对服务器进行动态度量，获得动态度量结果，并将动态度量结果以及关联证据发送给验证中心；其中，关联证据用于表示第一可信计算芯片和第二可信计算芯片设置在同一台服务器中，以使验证中心基于关联证据将静态度量结果和动态度量结果进行关联，并基于关联后的结果对服务器的软件系统的完整性进行验证。

[88] 动态度量：动态度量主要是保证系统开机之后（运行过程中）的软件（或应用程序）的安全性，这些软件安装在 OS 上。通过监控系统调用、周期性校验代码完整性等方式，检测系统的完整性。

[89] 在具体实施过程中，第二可信计算芯片主要负责采集动态度量所需的数据，并生成动态度量结果。

[90] 具体来讲，第二可信计算芯片可以采集应用程序的静态可执行性程序代码、以及应用程序运行时在内存中的程序代码，（此处的“应用程序”是：指服务器中的全部应用程序或部分指定的应用程序，安装在 OS 之上）；并基于应用程序的静态可执行性程序代码、以及应用程序运行时在内存中的程序代码，生成动态度量结果（其中即包含第二可信计算芯片采集到的这些程序代码）。

[91] 在具体实施过程中，第二可信计算芯片可以基于一预设频率对服务器进行动态度量。例如，1 小时 1 次、或 2 小时 1 次，或 6 小时 1 次、等等。所述预设频率可以根据实际需求自由调整，此处不做具体限定。

[92] 在具体实施过程中，验证中心可以为一台服务器，或者为一组服务器集群，用于对可信计算芯片发来的度量结果（即：第一可信计算芯片发来的静态度量结果，以及第二可信计算芯片发来的动态度量结果）进行验证，判断其软件的安全性（即：程序是否完整，是否被篡改）。

[93] 在具体实施过程中，第一可信计算芯片在获得静态度量结果后，即可将静态度量结果发送给验证中心，以供给验证中心进行验证。

[94] 具体来讲，第一可信计算芯片可以将静态度量结果、以及第一设备证书一起发送给验证中心，以供给验证中心进行安全验证；其中，第一设备证书用于表示第一可信计算芯片是由证书颁发机构认可的可信任的芯片。在验证中心对第一设备证书、以及静态度量结果依次验证完成后，会将验证结果（即：第一验证结果）发送给第一可信计算芯片，从而告知第一可信计算芯片 BIOS、OPROM 、Bootloader、OS 等程序代码是否安全（即：是否完整，是否被篡改）。

[95] 同理，第二可信计算芯片在每次获得动态度量结果后，即可将动态度量结果发送给验证中心，以供给验证中心进行验证。

[96] 具体来讲，第二可信计算芯片可以将动态度量结果、第二设备证书、以及关联证据一起发送给验证中心，以供给验证中心进行安全验证。其中，第二设备证书用于表示第二可信计算芯片是由证书颁发机构认可的可信任的芯片，关联证据用于表示第一可信计算芯片和第二可信计算芯片位于同一台服务器上（即：这里的动态度量结果和前面的静态度量结果来自于同一台服务器）。在验证中心对第二设备证书、关联证据、以及动态度量结果依次验证完成后，会将验证结果（即：第二验证结果）发送给第二可信计算芯片，从而告知第二可信计算芯片服务器上的应用程序是否安全（例如：程序是否完整，或程序是否被篡改）。

[97] 在具体实施过程中，验证中心可以基于关联证据将来自于同一台服务器的静态度量结果和动态度量结果进行关联，再基于关联后的结果对该服务器的软件系统的完整性进行验证。

[98] 其中，验证中心可以针对静态度量结果生成第一验证结果，并返回给第一可信计算芯片；并且，验证中心可以针对动态度量结果生成第二验证结果，并在第二验证结果中添加关联证据，再返回给第二可信计算芯片。此处，由于添加了关联证据，可以证明第一验证结果和第二验证结果是针对同一台服务器进行验证所获得的结果。

[99] 在具体实施过程中，若服务器发现第一验证结果表明 BIOS、OPROM 、Bootloader、OS 等程序代码中存在不安全因素（例如：程序是否完整，或程序被篡改），则输出第一提示信息，以提示技术人员对服务器进行安全排查。

[100] 同理，若服务器发现第二验证结果表明服务器上的应用程序存在不安全因素（例如：程序是否完整，或程序被篡改），则输出第二提示信息，以提示技术人员对服务器进行安全排查。

[101] 进一步，服务器还可以向远程主机进行远程证明。其中，远程主机是指与服务器存在业务往来的设备。

[102] 具体来讲，服务器在向远程主机进行远程证明时，可以使用第一可信计算芯片的私钥对第一验证结果进行签名（即：私钥加密），同时，使用第二可信计算芯片的私钥对第二验证结果进行签名（即：私钥加密），并将第一验证结果、第一设备证书、以及第二验证结果、第二设备证书打包一起发给远程主机，远程主机在验证过设备证书和签名的有效性后，即可相信验证结果。

[103] 在具体实施过程中，若远程主机对设备证书和签名验证后，发现设备证书或签名无效，则可以不相信验证结果，并拒绝向服务器提供任何服务。或者，在发现验证结果表明服务器的软件环境不安全（即：程序不完整，或程序被篡改）时，也可以拒绝向服务器提供任何服务。

[104] 上述本说明书实施例中的技术方案，至少具有如下的技术效果或优点：

[105] 在本说明书实施例中，公开了一种可信计算方法，应用于服务器中，所述服务器中设置有第一可信计算芯片和第二可信计算芯片，所述方法包括：在所述服务器启动过程中，所述第一可信计算芯片对所述服务器进行静态度量，获得静态度量结果，并将所述静态度量结果发送给验证中心；在所述服务器启动后的运行过程中，所述第二可信计算芯片对所述服务器进行动态度量，获得动态度量结果，并将所述动态度量结果、以及关联证据发送给验证中心；其中，所述关联证据用于表示所述第一可信计算芯片和所述第二可信计算芯片设置在同一台服务器中，以使所述验证中心用于基于所述关联证据将所述静态度量结果和所述动态度量结果进行关联，并基于关联后的结果对所述服务器的软件系统的完整性进行验证。由于在服务器中设置了两个相关联的可信计算芯片，其中，第一可信计算芯片用于对所述服务器进行静态度量，第二可信计算芯片用于对服务器进行动态度量，并将静态度量结果和动态度量结果同时发给验证中心，以使得验证中心可以基于静态度量结果和动态度量结果一起对业务服务器的软件系统的完成性进行验证。如此，解决了现有技术中在对服务器进行可信计算时，其计算结果的可靠性较低的技术问题，实现了同时进行静态度量和动态度量，提高了可信计算的可靠性，从而满足高安全场景的需求的技术效果。

实施例二

[106] 基于同一发明构思，如图 3 所示，本实施例提供了一种服务器 200，包括：

[107] 主板 210;

[108] 第一可信计算芯片 201，设置在所述主板上，用于在所述服务器启动过程中，对所述服务器进行静态度量，获得静态度量结果，并将所述静态度量结果发送给验证中心;

[109] 第二可信计算芯片 202，设置在所述主板上，用于在所述服务器启动后的运行过程中，对所述服务器进行动态度量，获得动态度量结果，并将所述动态度量结果以及关联证据发送给所述验证中心;

[110] 其中，关联证据用于表示第一可信计算芯片 201 和第二可信计算芯片 202 设置在同一台服务器中，以使验证中心基于关联证据将静态度量结果和动态度量结果进行关联，并基于关联后的结果对服务器的软件系统的完整性进行验证。

[111] 作为一种可选的实施例，所述第一可信计算芯片 201 插在所述服务器上的串行外设接口 SPI 接口或低引脚数目 LPC 接口，所述第二可信计算芯片 202 插在所述服务器上的总线和接口标准 PCIE 接口或串行高级技术附件 SATA 接口或通用串行总线 USB 接口。

[112] 作为一种可选的实施例，第一可信计算芯片 201，还用于:

[113] 进行初始化，并接收证书颁发机构签发的第一设备证书。

[114] 作为一种可选的实施例，第一可信计算芯片 201，还用于:

[115] 在所述将所述静态度量结果发送给验证中心时，还将所述第一设备证书一起发给所述验证中心，以使所述验证中心对所述第一设备证书进行验证。

[116] 作为一种可选的实施例，第二可信计算芯片 202，还用于:

[117] 进行初始化，并接收所述证书颁发机构签发的第二设备证书。

[118] 作为一种可选的实施例，第二可信计算芯片 202，还用于:

[119] 在将所述静态度量结果发送给验证中心时，还将所述第一设备证书一起发给所述验证中心，以使所述验证中心对所述第一设备证书进行验证。

[120] 作为一种可选的实施例，第二可信计算芯片 202，还用于:

[121] 在所述第一可信计算芯片 201 对所述服务器进行静态度量之前，接收所述证书颁发机构签署的关联证据；其中，所述关联证据用于表示所述第一可信计算芯片 201 和所述第二可信计算芯片 202 设置在同一台服务器中。

[122] 作为一种可选的实施例，所述关联证据，包括:

[123] 第一可信计算芯片 201 的标识信息;

[124] 第二可信计算芯片 202 的标识信息;

[125] 证书颁发机构的签名。

[126] 作为一种可选的实施例，第一可信计算芯片 201，具体用于:

[127] 采集所述服务器中的基本输入/输出系统 BIOS 的程序代码、引导程序 Bootloader 的程序代码、操作系统 OS 的程序代码；基于所述 BIOS 的程序代码、所述 Bootloader 的程序代码、以及所述 OS 的程序代码，生成所述静态度量结果。

[128] 作为一种可选的实施例，第二可信计算芯片 202，具体用于:

[129] 采集应用程序的静态可执行性程序代码、以及所述应用程序运行时在内存中的程序代码，所述应用程序安装在所述服务器上；基于所述应用程序的静态可执行性程序代码、以及所述应用程序运行时在内存中的程序代码，生成所述动态度量结果。

[130] 作为一种可选的实施例，第一可信计算芯片 201，还用于:

[131] 接收所述验证中心反馈的第一验证结果，所述第一验证结果与所述静态度量对应。

[132] 作为一种可选的实施例，第二可信计算芯片 202，还用于:

[133] 接收所述验证中心反馈的第二验证结果，所述第二验证结果与所述动态度量对应，所述第二验证结果中携带有所述关联证据。

[134] 由于本实施例所介绍的服务器为实施本说明书实施例中可信计算方法所采用的设备，故而基于本说明书实施例中所介绍的可信计算方法，本领域所属技术人员能够了解本实施例的服务器的具体实施方式以及其各种变化形式，所以在此对于该服务器如何实现本说明书实施例中的方法不再详细介绍。只要本领域所属技术人员实施本说明书实施例中可信计算方法所采用的设备，都属于本说明书所欲保护的范围。

[135] 本领域内的技术人员应明白，本说明书实施例的实施例可提供为方法、系统、或计算机程序产品。因此，本说明书实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本说明书实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[136] 本说明书实施例是参照根据本说明书实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或

方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

[137] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

[138] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

[139] 尽管已描述了本说明书实施例的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本说明书实施例范围的所有变更和修改。

[140] 显然，本领域的技术人员可以对本说明书实施例进行各种改动和变型而不脱离本说明书实施例的精神和范围。这样，倘若本说明书实施例的这些修改和变型属于本说明书实施例权利要求及其等同技术的范围之内，则本说明书实施例也意图包含这些改动和变型在内。

权利要求书

1、一种可信计算方法，应用于服务器中，所述服务器中设置有第一可信计算芯片和第二可信计算芯片，所述方法包括:

在所述服务器启动过程中，所述第一可信计算芯片对所述服务器进行静态度量，获得静态度量结果，并将所述静态度量结果发送给验证中心;

在所述服务器启动后的运行过程中，所述第二可信计算芯片对所述服务器进行动态度量，获得动态度量结果，并将所述动态度量结果以及关联证据发送给所述验证中心;

其中，所述关联证据用于表示所述第一可信计算芯片和所述第二可信计算芯片设置在同一台服务器中，以使所述验证中心基于所述关联证据将所述静态度量结果和所述动态度量结果进行关联，并基于关联后的结果对所述服务器的软件系统的完整性进行验证。

2、如权利要求 1 所述的方法，所述第一可信计算芯片插在所述服务器上的串行外设接口 SPI 接口或低引脚数目 LPC 接口，所述第二可信计算芯片插在所述服务器上的总线和接口标准 PCIE 接口或串行高级技术附件 SATA 接口或通用串行总线 USB 接口。

3、如权利要求 1 所述的方法，在所述第一可信计算芯片对所述服务器进行静态度量之前，还包括:

所述第一可信计算芯片接收证书颁发机构签发的第一设备证书，以及所述第二可信计算芯片接收所述证书颁发机构签发的第二设备证书;

其中，在所述第一可信计算芯片将所述静态度量结果发送给验证中心时，所述第一可信计算芯片还将所述第一设备证书发给所述验证中心，以使所述验证中心对所述第一设备证书进行验证;

在所述第二可信计算芯片将所述动态度量结果发送给验证中心时，所述第二可信计算芯片还将所述第二设备证书发给所述验证中心，以使所述验证中心对所述第二设备证书进行验证。

4、如权利要求 3 所述的方法，在所述第一可信计算芯片对所述服务器进行静态度量之前，还包括:

所述第二可信计算芯片接收所述证书颁发机构签署的所述关联证据。

5、如权利要求 1 所述的方法，所述关联证据，包括:

所述第一可信计算芯片的标识信息;

所述第二可信计算芯片的标识信息;

所述证书颁发机构的签名。

6、如权利要求 1 所述的方法，所述第一可信计算芯片对所述服务器进行静态度量，

获得静态度量结果，包括:

所述第一可信计算芯片采集所述服务器中的基本输入/输出系统 BIOS 的程序代码、引导程序 Bootloader 的程序代码、操作系统 OS 的程序代码;

所述第一可信计算芯片基于所述 BIOS 的程序代码、所述 Bootloader 的程序代码、以及所述 OS 的程序代码，生成所述静态度量结果。

7、如权利要求 1 所述的方法，所述第二可信计算芯片对所述服务器进行动态度量，获得动态度量结果，包括:

所述第二可信计算芯片采集应用程序的静态可执行性程序代码、以及所述应用程序运行时在内存中的程序代码，所述应用程序安装在所述服务器上;

所述第二可信计算芯片基于所述应用程序的静态可执行性程序代码、以及所述应用程序运行时在内存中的程序代码，生成所述动态度量结果。

8、如权利要求 1~7 任一所述的方法，在所述第二可信计算芯片将所述动态度量结果以及关联证据发送给所述验证中心之后，还包括:

所述第一可信计算芯片接收所述验证中心反馈的第一验证结果，所述第一验证结果与所述静态度量对应;

所述第二可信计算芯片接收所述验证中心反馈的第二验证结果，所述第二验证结果与所述动态度量对应，所述第二验证结果中携带有所述关联证据。

9、一种服务器，包括:

主板;

第一可信计算芯片，设置在所述主板上，用于在所述服务器启动过程中，对所述服务器进行静态度量，获得静态度量结果，并将所述静态度量结果发送给验证中心;

第二可信计算芯片，设置在所述主板上，用于在所述服务器启动后的运行过程中，对所述服务器进行动态度量，获得动态度量结果，并将所述动态度量结果以及关联证据发送给所述验证中心;

其中，所述关联证据用于表示所述第一可信计算芯片和所述第二可信计算芯片设置在同一台服务器中，以使所述验证中心基于所述关联证据将所述静态度量结果和所述动态度量结果进行关联，并基于关联后的结果对所述服务器的软件系统的完整性进行验证。

10、如权利要求 9 所述的服务器，所述第一可信计算芯片插在所述服务器上的串行外设接口 SPI 接口或低引脚数目 LPC 接口，所述第二可信计算芯片插在所述服务器上的总线和接口标准 PCIE 接口或串行高级技术附件 SATA 接口或通用串行总线 USB 接口。

11、如权利要求 9 所述的服务器，所述第一可信计算芯片，还用于:

在对所述服务器进行静态度量之前，接收证书颁发机构签发的第一设备证书；在将所述静态度量结果发送给验证中心时，还将所述第一设备证书发给所述验证中心，以使所述验证中心对所述第一设备证书进行验证；

所述第二可信计算芯片，还用于：

在所述第一可信计算芯片对所述服务器进行静态度量之前，接收所述证书颁发机构签发的第二设备证书；在将所述动态度量结果发送给验证中心时，还将所述第二设备证书发给所述验证中心，以使所述验证中心对所述第二设备证书进行验证。

12、如权利要求 11 所述的服务器，所述第二可信计算芯片，还用于：

在所述第一可信计算芯片对所述服务器进行静态度量之前，接收所述证书颁发机构签署的所述关联证据。

13、如权利要求 9 所述的服务器，所述关联证据，包括：

所述第一可信计算芯片的标识信息；

所述第二可信计算芯片的标识信息；

所述证书颁发机构的签名。

14、如权利要求 9 所述的服务器，所述第一可信计算芯片，具体用于：

采集所述服务器中的基本输入/输出系统 BIOS 的程序代码、引导程序 Bootloader 的程序代码、操作系统 OS 的程序代码；基于所述 BIOS 的程序代码、所述 Bootloader 的程序代码、以及所述 OS 的程序代码，生成所述静态度量结果。

15、如权利要求 9 所述的服务器，所述第二可信计算芯片，具体用于：

采集应用程序的静态可执行性程序代码、以及所述应用程序运行时在内存中的程序代码，所述应用程序安装在所述服务器上；基于所述应用程序的静态可执行性程序代码、以及所述应用程序运行时在内存中的程序代码，生成所述动态度量结果。

16、如权利要求 9~15 任一所述的服务器，所述第一可信计算芯片，还用于：接收所述验证中心反馈的第一验证结果，所述第一验证结果与所述静态度量对应；

所述第二可信计算芯片，还用于：接收所述验证中心反馈的第二验证结果，所述第二验证结果与所述动态度量对应，所述第二验证结果中携带有所述关联证据。

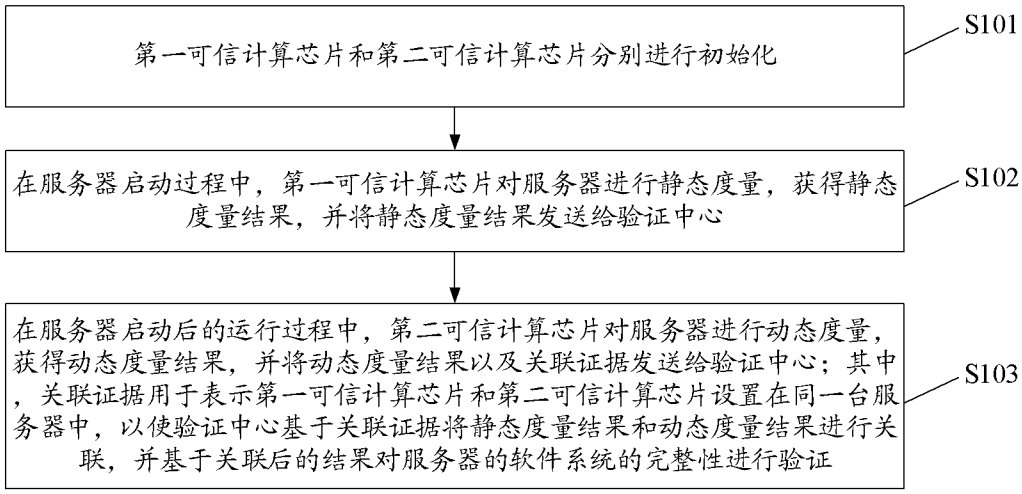
第一可信计算芯片和第二可信计算芯片分别进行初始化
S101
在服务器启动过程中，第一可信计算芯片对服务器进行静态度量，获得静态度量结果，并将静态度量结果发送给验证中心
S102
在服务器启动后的运行过程中，第二可信计算芯片对服务器进行动态度量，获得动态度量结果，并将动态度量结果以及关联证据发送给验证中心；其中，关联证据用于表示第一可信计算芯片和第二可信计算芯片设置在同一台服务器中，以使验证中心基于关联证据将静态度量结果和动态度量结果进行关联，并基于关联后的结果对服务器的软件系统的完整性进行验证
S103

图 1

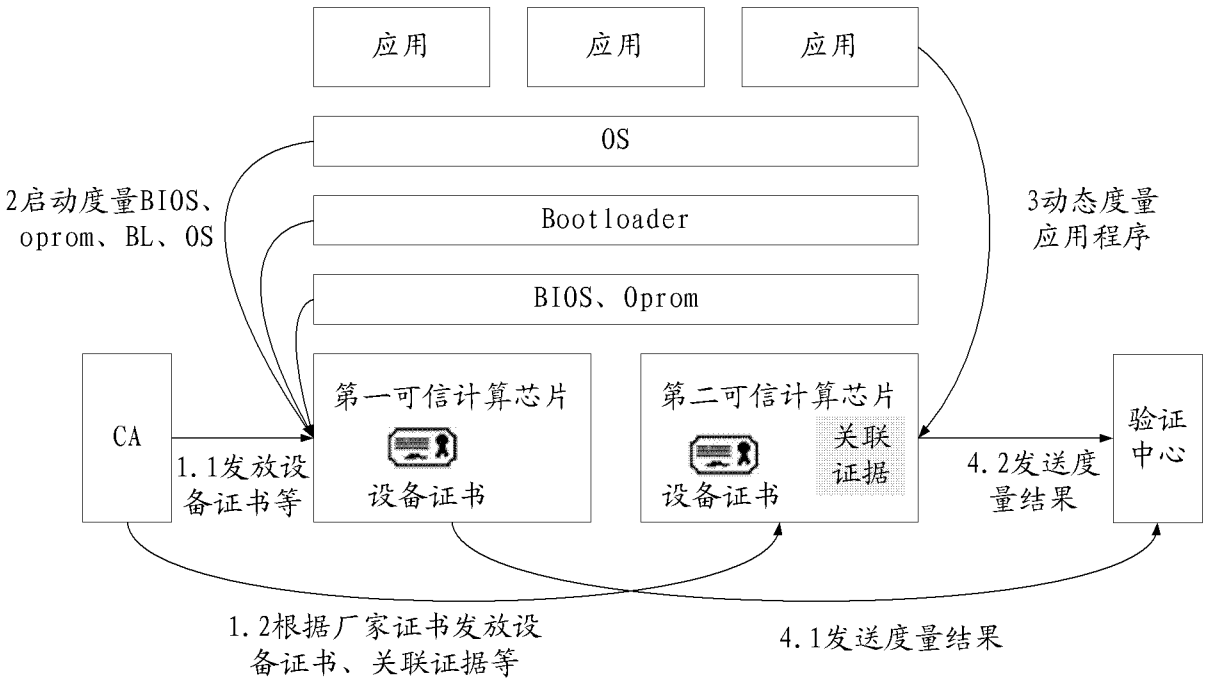
应用
应用
应用
OS
Bootloader
BIOS、Oprom
2启动度量BIOS、oprom、BL、OS
3动态度量应用程序
CA
1.1发放设备证书等
第一可信计算芯片
设备证书
第二可信计算芯片
关联证据
设备证书
4.2发送度量结果
验证中心
1.2根据厂家证书发放设备证书、关联证据等
4.1发送度量结果

图 2

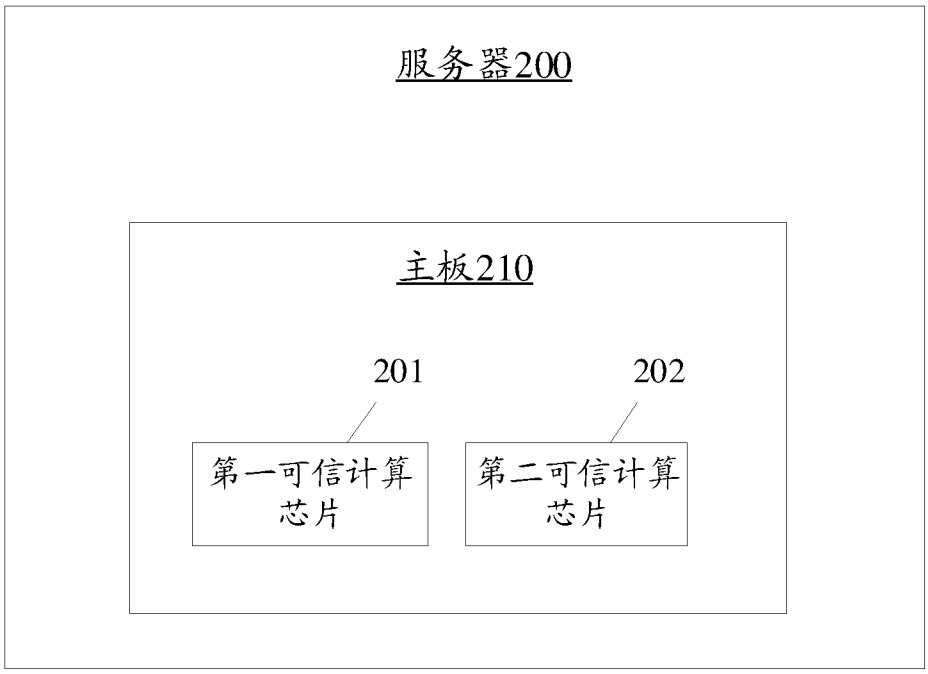

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/074980

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/57(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)

G06F21

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; CNTXT; DWPI; CNKI; SIPOABS: 可信, 安全, 芯片, 动态, 度量, 计算芯片, 服务器, 计算, 验证, credible, chip, comput+, trust, reliab+, server, verify, measur+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110096887 A (ALIBABA GROUP HOLDING LIMITED) 06 August 2019 (2019-08-06) entire document	1-16
A	CN 102436566 A (AUTOMATION RESEARCH AND DESIGN INSTITUTE OF METALLURGICAL INDUSTRY) 02 May 2012 (2012-05-02) entire document	1-16
A	CN 105227319 A (LANGCHAO ELECTRONIC INFORMATION INDUSTRY CO., LTD.) 06 January 2016 (2016-01-06) entire document	1-16
A	CN 101247410 A (LAN, Yuqing) 20 August 2008 (2008-08-20) entire document	1-16

☐ 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
30 March 2020	**20 April 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/074980

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110096887 A	06 August 2019	None	
CN 102436566 A	02 May 2012	CN 102436566 B	09 July 2014
CN 105227319 A	06 January 2016	None	
CN 101247410 A	20 August 2008	CN 101247410 B	08 June 2011

国际检索报告

国际申请号
PCT/CN2020/074980

A. 主题的分类

G06F 21/57(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)

G06F21

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;CNTXT;DWPI;CNKI;SIPOABS:可信，安全，芯片，动态，度量，计算芯片，服务器，计算，验证，credible，chip，comput+，trust，reliab+，server，verify，measur+

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 110096887 A (阿里巴巴集团控股有限公司) 2019年 8月 6日 (2019-08-06) 全文	1-16
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	1-16
A	CN 105227319 A (浪潮电子信息产业股份有限公司) 2016年 1月 6日 (2016-01-06) 全文	1-16
A	CN 101247410 A (兰雨晴) 2008年 8月 20日 (2008-08-20) 全文	1-16

☐ 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
2020年 3月 30日	2020年 4月 20日

ISA/CN的名称和邮寄地址	受权官员
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	马驰
传真号 (86-10)62019451	电话号码 62412168

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/074980

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	110096887	A	2019年 8月 6日	无			
CN	102436566	A	2012年 5月 2日	CN	102436566	B	2014年 7月 9日
CN	105227319	A	2016年 1月 6日	无			
CN	101247410	A	2008年 8月 20日	CN	101247410	B	2011年 6月 8日