(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
2023 年 6 月 15 日 (15.06.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/103697 A1

(51) 国际专利分类号:
G06F 9/54 (2006.01)

(21) 国际申请号: PCT/CN2022/130846

(22) 国际申请日: 2022 年 11 月 9 日 (09.11.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202111507637.6 2021年12月10日 (10.12.2021) 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: 朱少峰 (**ZHU, Shaofeng**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 章庆隆 (**ZHANG, Qinglong**); 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: 广州三环专利商标代理有限公司 (**SCIHEAD IP LAW FIRM**); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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, 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,

WO 2023/103697 A1

(54) **Title:** COMMUNICATION METHOD IN COMPUTER SYSTEM, AND RELATED PRODUCT

(54) 发明名称: 一种计算机系统中的通信方法及相关产品

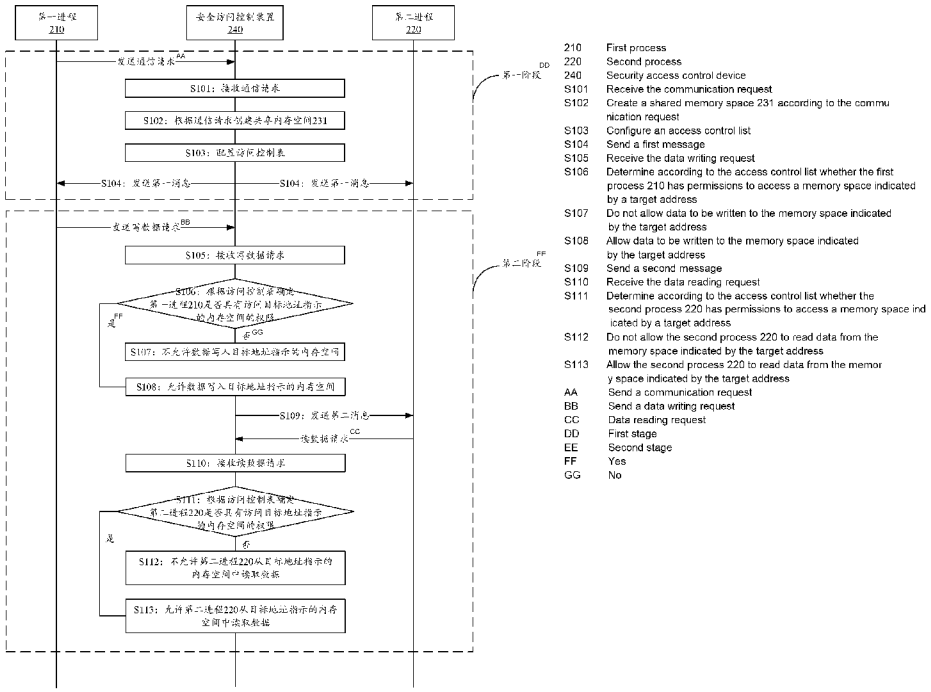

图 4

(57) **Abstract:** A communication method in a computer system and a related product, capable of reducing loss caused by processes, running in different enclaves of the system, during communication. Specifically, the method above comprises the following steps: receiving a communication request from a first process (S101); and then creating a shared memory space according to the communication request (S102), wherein the first process and a second process have permissions to access the shared memory space, the first process is a process running in a first enclave, and the second process is a process running in a second enclave. The first process and the second

[见续页]

LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, CV, 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, 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))。

process can access the shared memory space, so that the first process and the second process can perform read and write operations on the shared memory space, and thus can implement communication on the basis of the shared memory space. When communication is implemented on the basis of the shared memory space, data copying and data encryption are not needed in the procedure, and thus, the procedure will cause less loss.

(57) 摘要：一种计算机系统中的通信方法及相关产品，能够减少运行在该系统的不同enclave中的进程在通信过程中造成的损耗。具体地，上述方法包括以下步骤：接收来自第一进程的通信请求（S101），然后根据上述通信请求创建共享内存空间（S102），其中，第一进程和第二进程具有访问上述共享内存空间的权限，第一进程是第一enclave中运行的进程，第二进程是第二enclave中运行的进程。由于第一进程和第二进程可以访问共享内存空间，因此第一进程和第二进程可以对共享内存空间进行读写操作，也就可以基于共享内存空间实现通信。在基于共享内存空间实现通信时，由于这一过程无需数据拷贝，也无需数据加密，因此这一过程会带来更少的损耗。

一种计算机系统中的通信方法及相关产品

本申请要求于2021年12月10日提交中国专利局、申请号为202111507637.6、申请名称为“一种计算机系统中的通信方法及相关产品”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

本申请实施例涉及数据安全领域，尤其涉及一种计算机系统中的通信方法及相关产品。

背景技术

近年来，为了提高计算平台上数据的安全性，计算平台上一般部署有可信执行环境（trusted execution environment, TEE）系统。用户通过将需要保护的程序以飞地（enclave）的形式部署在TEE系统上，可以保证上述程序的完整性和相关数据的机密性。在实际应用中，用户可以在TEE系统中部署多个enclave，并且运行在不同enclave上的进程之间可能存在通信的需求。

目前，不同enclave在通信时，通常需要利用不可信进程（如部署在不可信环境中的应用程序和操作系统（operating system, OS））进行数据的转发，以运行在enclave A上的进程A向运行在enclave B上的进程B发送数据为例：进程A先将数据发送至不可信进程，再由不可信进程将数据转发至进程B。这一过程涉及到了数据的拷贝。而且，由于数据经由了不可信进程的转发，这可能导致数据的泄漏，因此为了保证数据的安全性，进程A在将数据发送至不可信进程之前，还需对数据进行加密，相应地，进程B在接收到不可信进程转发的数据后，还需对数据进行解密。也就是说，上述通信过程会带来较大的资源损耗。

因此，如何减少运行在不同enclave上的进程在通信时带来的损耗，仍然是数据安全领域中的一个急需解决的问题。

发明内容

本申请实施例提供了一种计算机系统中的通信方法及相关产品，能够创建出一个共享内存空间，该共享内存空间支持运行在不同enclave上的多个可信进程访问，这样，基于共享内存空间可以使得上述多个可信进程间的通信无需拷贝、且无需加密，从而减少上述多个可信进程在通信时带来的损耗。

第一方面，本申请实施例提供了一种计算机系统中的通信方法，该系统包括第一enclave和第二enclave，该方法包括如下步骤：接收来自第一进程的通信请求，然后根据上述通信请求创建共享内存空间，其中，第一进程和第二进程具有访问上述共享内存空间的权限，第一进程是第一enclave中运行的进程，第二进程是第二enclave中运行的进程。由于第一进程和第二进程可以访问共享内存空间，因此第一进程和第二进程可以对共享内存空间进行读写操作，也就可以基于共享内存空间实现通信。在基于共享内存空间实现通信时，由于这一过程无需数据拷贝，也无需数据加密，因此这一过程会带来更少的损耗。

在第一方面的一种可能的实现方式中，上述通信请求携带了多个进程的标识，上述多个进程具有访问共享内存空间的权限，其中，上述多个进程包括第一进程和第二进程。如此，可以保证共享内存空间的安全性，从而提高第一进程和第二进程之间的通信的安全性。

在第一方面的一种可能的实现方式中，不可信进程不具有访问共享内存空间的权限。其中，不可信进程包括运行在不可信执行环境中的进程、以及通信请求中未指明的进程中的至少一个进程。由上述实现方式可知，通信请求写到了多个进程的标识，因此，通信请求中未指明的进程是指除上述多个进程之外的进程。如此，也可以保证共享内存空间的安全性，从而提高第一进程和第二进程之间的通信的安全性。

在第一方面的一种可能的实现方式中，上述通信请求包括共享内存空间的大小，共享内存空间为计算机系统的内存中一段满足上述大小要求的内存空间。如此，可以使得共享内存空间的创建更加灵活，更能有效的利用计算机系统中的内存资源。

在第一方面的一种可能的实现方式中，在根据通信请求创建共享内存空间之后，上述方法还包括：配置访问控制表，其中，访问控制表用于指示第一进程和第二进程具有访问共享内存空间的权限。

在第一方面的一种可能的实现方式中，上述方法还包括：接收来自第一进程的写数据请求，其中，写数据请求包括待写入的数据和目标地址，共享内存空间包括目标地址指示的内存空间。然后，根据访问控制表确定第一进程具有访问目标地址指示的内存空间的权限，之后，允许数据写入目标地址指示的内存空间。然后，向第二进程发送通知消息，其中，通知消息包括上述目标地址，通信消息用于指示第二进程从目标地址指示的内存空间中读取上述数据。

在第一方面的一种可能的实现方式中，在向第二进程发送通知消息之后，上述方法还包括：接收来自第二进程的读数据请求，其中，读数据请求包括上述目标地址。然后，根据所述访问控制表确定第二进程具有访问目标地址指示的内存空间的权限，之后，允许第二进程从目标地址指示的内存空间中读取数据。

上述实现方式中，基于访问控制表可以确定具有访问共享内存空间权限的进程，以及不具有访问共享内存空间权限的进程，只有具有访问共享内存空间权限的进程才能够向共享内存空间进行读写操作，从而保证了共享内存空间的安全性，提高了第一进程和第二进程之间的通信的安全性。

第二方面，本申请实施例提供了一种安全访问控制装置，该装置应用于计算机系统，该系统包括第一 enclave 和第二 enclave。该装置包括通信管理模块和内存管理模块。其中，通信管理模块用于接收来自第一进程的通信请求，第一进程是第一 enclave 中运行的进程。内存管理模块用于根据上述通信请求创建共享内存空间，其中，第二进程是第二 enclave 中运行的进程，第一进程和第二进程具有访问上述共享内存空间的权限。

在第二方面的一种可能的实现方式中，上述通信请求携带了多个进程的标识，上述多个进程具有访问共享内存空间的权限，其中，上述多个进程包括第一进程和第二进程。

在第二方面的一种可能的实现方式中，不可信进程不具有访问共享内存空间的权限。其中，不可信进程包括运行在不可信执行环境中的进程、以及通信请求中未指明的进程中的至少一个进程。由上述实现方式可知，通信请求写到了多个进程的标识，因此，通信请求中未指明的进程是指除上述多个进程之外的进程。

在第二方面的一种可能的实现方式中，上述通信请求包括共享内存空间的大小，共享内存空间为计算机系统的内存中一段满足上述大小要求的内存空间。

在第二方面的一种可能的实现方式中，上述装置还包括访问控制模块，访问控制模块用于配置访问控制表，其中，访问控制表用于指示第一进程和第二进程具有访问共享内存空间的权限。

在第二方面的一种可能的实现方式中，上述通信管理模块还用于接收来自第一进程的写数据请求，其中，写数据请求包括待写入的数据和目标地址，共享内存空间包括目标地址指示的内存空间。上述访问控制模块用于根据访问控制表确定第一进程具有访问目标地址指示的内存空间的权限，并允许数据写入目标地址指示的内存空间。上述通信管理模块还用于向第二进程发送通知消息，其中，通知消息包括上述目标地址，通信消息用于指示第二进程从目标地址指示的内存空间中读取上述数据。

在第二方面的一种可能的实现方式中，上述通信管理模块还用于接收来自第二进程的读数据请求，其中，读数据请求包括上述目标地址。上述访问控制模块用于根据所述访问控制表确定第二进程具有访问目标地址指示的内存空间的权限，并允许第二进程从目标地址指示的内存空间中读取数据。

第三方面，本申请实施例提供了一种计算设备，该设备应用于计算机系统，该系统包括第一 enclave 和第二 enclave。该设备包括处理器和访问控制器。处理器用于接收来自第一进程的通信请求，并根据上述通信请求创建共享内存空间，其中，第一进程是第一 enclave 中运行的进程，第二进程是第二 enclave 中运行的进程，第一进程和第二进程具有访问上述共享内存空间的权限。处理器还用于配置访问控制表到访问控制器。访问控制器用于根据访问控制表确定第一进程和第二进程具有访问共享内存空间的权限，以使第一进程和第二进程基于共享内存空间实现通信。

在第三方面的一种可能的实现方式中，上述通信请求携带了多个进程的标识，上述多个进程具有访问共享内存空间的权限，其中，上述多个进程包括第一进程和第二进程。

在第三方面的一种可能的实现方式中，不可信进程不具有访问共享内存空间的权限。其中，不可信进程包括运行在不可信执行环境中的进程、以及通信请求中未指明的进程中的至少一个进程。由上述实现方式可知，通信请求写到了多个进程的标识，因此，通信请求中未指明的进程是指除上述多个进程之外的进程。

在第三方面的一种可能的实现方式中，上述通信请求包括共享内存空间的大小，共享内存空间为计算机系统的内存中一段满足上述大小要求的内存空间。

在第三方面的一种可能的实现方式中，上述处理器还用于接收来自第一进程的写数据请求，其中，写数据请求包括待写入的数据和目标地址，共享内存空间包括目标地址指示的内存空间。上述访问控制器用于根据访问控制表确定第一进程具有访问目标地址指示的内存空间的权限，并允许数据写入目标地址指示的内存空间。上述处理器还用于向第二进程发送通知消息，其中，通知消息包括上述目标地址，通信消息用于指示第二进程从目标地址指示的内存空间中读取上述数据。

在第三方面的一种可能的实现方式中，上述处理器还用于接收来自第二进程的读数据请求，其中，读数据请求包括上述目标地址。上述访问控制器用于根据所述访问控制表确定第二进程具有访问目标地址指示的内存空间的权限，并允许第二进程从目标地址指示的内存空间中读取数据。

第四方面，本申请实施例提供了一种计算机可读存储介质，该计算机可读存储介质存储有计算机指令，当计算机指令被计算设备执行时，计算设备执行前述第一方面或第一方面的任意一种实现方式所描述的方法。

附图说明

图 1 是本申请实施例提供的一种 TEE 系统的结构示意图；

图 2 是本申请实施例提供的一种内存隔离机制的示意图；

图 3 是本申请实施例提供的一种计算系统的结构示意图；

图 4 是本申请实施例提供的一种通信方法的流程示意图；

图 5 是本申请实施例提供的一种安全访问控制装置的结构示意图；

图 6 是本申请实施例提供的一种计算设备的结构示意图；

图 7 是本申请实施例提供的一种访问控制器的部署示意图；

图 8 是本申请实施例提供的另一种访问控制器的部署示意图；

图 9 是本申请实施例提供的又一种访问控制器的部署示意图；

图 10 是本申请实施例提供的另一种访问控制器的部署示意图。

具体实施方式

为了使本申请实施例的方案更清晰，在具体描述本申请实施例的方案之前，首先对本申请实施例涉及到的相关术语进行解释。

在大数据和人工智能的时代，人们能够更方便并且更高效地获取到各种数据。但与此同时，人们访问数据的行为也被记录、被学习以及被使用。如果在这一过程中不注重隐私保护，个人信息就可能被泄漏。为此，对用户数据进行保护是至关重要的。

近年来，在智能终端、边缘计算、云计算等领域，计算平台通常采用 TEE 系统来提高用户数据的安全性。图 1 示例性的展示了 TEE 系统的结构示意图。如图 1 所示，TEE 系统 100 包括不可信应用程序 110、不可信操作系统（operating system, OS）120、enclave 130、可信计算基（trusted computing base, TCB）140 和系统资源 150。下面简要描述 TEE 系统的各个部分。

不可信应用程序 110：是指用户部署的普通应用程序，这里的普通应用程序是指用户部署的、不需要受到额外的安全性保护的程序，区别于 enclave 130 中的程序。不可信应用程序 110 具体可以包括主机应用程序（host application）。

不可信 OS 120：通常由服务提供商部署，用于为不可信应用程序 110 提供运行环境和相关服务。不可信操作系统可以包括富操作系统（rich operating system, Rich OS）。

enclave 130：是运行在计算设备中、具有独立资源（包括内存资源、网络资源以及计算资源等）的一个安全可信的执行环境，能够保证运行在其中的程序的完整性，以及上述程序在运行过程产生的数据的机密性。本申请实施例中，enclave 130 包括程序和一段内存空间，其中，enclave 130 中的程序是指用户部署的、需要受到保护的程序，具体可以包括应用程序、应用程序和可信操作系统、虚拟机（virtual machine, VM）、容器（container）或沙盒（sandbox）等。需要说明的是，上述可信操作系统为用户部署的、用于为 enclave 130 中的应用程序提供运行环境和相关服务。enclave 130 中的内存空间（以下称为 enclave 内存空间）是 TEE 系统 100 拥有的内存中的一段连续的内存空间，用于存储 enclave 130 中的程序以及该程序在运行过程中产生的数据（以下称为运行态数据）。

TCB 140：对于 TEE 系统 100 来说，TCB 140 是实现系统内数据安全的所有安全保护机制（如内存隔离机制、数字签名机制、远程证明机制等）的集合，用于保证 enclave 130 中的程序的完整性以及运行态数据的机密性，防止其受到不可信进程的篡改或非法访问。其中，不可信进程包括不可信应用程序 110 和不可信 OS 120 等可以主动攻击 enclave 130 或作为攻

击 enclave 130 的跳板的进程。

本申请实施例中，TCB 140 包括可信硬件 141 和 TCB 高特权级软件 142。其中，可信硬件 141 是由计算平台提供者部署的硬件资源，用于为 enclave 130 的创建、管理（如中断管理）以及保护(如内存保护)等提供硬件支持。可信硬件 141 可以包括中央处理器(central processing unit, CPU）内核、硬件可信根（如符合可信赖平台模块（trusted platform module, TPM）标准的安全芯片、eFuse）以及其他硬件特性（如内存总线）。TCB 高特权级软件 142 是由计算平台提供者部署的、运行在可信硬件 141 上的软件资源，用于为 enclave 130 的创建、管理以及保护等提供功能支持。

值得注意的是，上述术语“TCB 高特权级软件”可以具有不同的名称，例如，不同标准、同一标准的不同版本、不同厂商对术语“TCB 高特权级软件”可以具有不同的称呼，例如，“TCB 软件”、“安全监视器”、“security monitor”等。

系统资源 150：包括内存资源和外设资源。内存资源包括与 TEE 系统 100 中的处理器（如运行不可信应用程序 110、不可信 OS 120 的处理器，以及运行 enclave 130 中的程序的处理器）直接交换数据的内部存储器，可用于随时读写数据，而且读写数据的速度很快。内存资源可以包括多种存储器，例如，只读存储器（read only memory, ROM）、随机存取存储器（random access memory, RAM）。外设资源是指连接在计算设备主机之外的硬件设备，用于传输和存储数据，例如，硬盘（solid state drive, SSD）、网卡。

还需说明的是，上述关于 TEE 系统 100 的介绍中涉及到“用户”、“服务提供商”和“计算平台提供者”，下面对上述几种概念进行区分：“计算平台提供者”是指部署基础设施，即部署计算资源（如服务器）、部署存储资源（如存储器）以及部署网络资源（如网卡），从而搭建出计算平台的厂商；“服务提供商”是指利用上述计算平台给“用户”提供服务的厂商，例如，允许用户在计算平台上部署和运行软件、允许用户访问运行在计算平台上的应用程序等；“用户”是指上述服务的使用者。

从图 1 可以看出，TEE 系统 100 中形成了两个互相隔离的环境：一个是可信环境（也称安全环境，即 secure world），一个是不可信环境（也称非安全环境，即 non-secure world）。其中，不可信应用程序 110、不可信 OS 120 以及一部分系统资源 150 属于不可信环境，enclave 130、TCB 140 以及一部分系统资源 150 属于可信环境。

TEE 系统 100 支持内存隔离机制，内存隔离机制使得运行在不可信环境中的进程无法访问可信环境中的内存空间，以及可信环境中的 enclave 内存空间仅能被运行在该 enclave 中的进程访问，不能被运行在其他 enclave 中的进程访问，从而达到保护 enclave 内存空间中程序以及运行态数据的目的。图 2 示例性的展示了内存隔离机制，如图 2 所示，运行在不可信环境中的进程包括不可信应用程序 110 和不可信 OS 120，运行在可信环境中的进程包括运行在 enclave A 中的进程和运行在 enclave B 中的进程，可信环境中的内存空间包括 enclave A 中的内存空间和 enclave B 中的内存空间。基于内存隔离机制，enclave A 中的内存空间能够被运行在 enclave A 中的进程访问，但不能被不可信应用程序 110、不可信 OS 120 以及运行在 enclave B 中的进程访问；enclave B 中的内存空间能够被运行在 enclave B 中的进程访问，但不能被不可信应用程序 110、不可信 OS 120 以及运行在 enclave A 中的进程访问。

下面结合图 2 介绍内存隔离机制的实现原理，以 enclave A 中的内存空间为例：

首先，enclave A 中的内存空间的创建过程如下：将 enclave A 中的程序加载至 TEE 系统 100，之后，enclave A 中的程序调用不可信 OS 120 来为其分配一段连续的内存空间 A，并根据内存空间 A 来配置对应的页表。然后，不可信 OS 120 调用 TCB 高特权级软件 142 检查上

述页表，判断内存空间 A 是否可用。在内存空间 A 可用的情况下，将内存空间 A 作为 enclave A 中的内存空间，之后再记录内存空间 A 的地址范围，以用于确定仅有运行在 enclave A 中的进程能够访问内存空间 A，从而完成 enclave A 的创建。

接下来，当 TEE 系统 100 中的某个进程向内存空间 A 发起访问时，TCB 高特权级软件 142 首先判断该进程是否具有访问内存空间 A 的权限，如果有，则允许该进程访问内存空间 A；如果没有，则不允许该进程访问内存空间 A。不难理解，在上述不可信应用程序 110、不可信 OS 120、运行在 enclave A 中的进程以及运行在 enclave B 中的进程中，只有运行在 enclave A 中的进程能够访问内存空间 A，而不可信应用程序 110、不可信 OS 120 以及运行在 enclave B 中的进程均不能够访问内存空间 A，因此实现了内存空间 A 中程序以及运行态数据的安全性。

应理解，在实际应用中，TEE 系统 100 中可能部署有多个 enclave，运行在不同 enclave 中的进程之间可能存在通信的需求。仍以图 2 为例，假设 TEE 系统 100 可以实现人脸识别模型的训练，其中，enclave A 包括实现样本数据（如人脸图像）的收集以及对收集到的样本数据进行预处理的程序，enclave B 包括获取上述预处理后的样本数据，并根据这些样品数据进行人脸识别模型的训练的程序。因此，运行在 enclave A 中的进程与运行在 enclave B 中的进程之间需要进行通信。但内存隔离机制的存在使得运行在 enclave B 中的进程无法直接从 enclave A 中的内存空间中读取上述预处理后的样本数据，运行在 enclave A 中的进程也无法直接向 enclave B 中的内存空间中写入上述预处理后的样本数据。不仅如此，上述预处理后的样品数据还涉及到隐私安全问题，也就是说，还要保证运行在 enclave A 中的进程与运行在 enclave B 中的进程之间的通信是安全的。

针对上述问题，本申请实施例提供了一种通信方法，不仅能够使得运行在不同 enclave 中的进程相互通信，还能够保证整个通信过程的安全性。该方法可以应用于计算机系统，该系统可以是前文描述的 TEE 系统，图 3 示例性的展示了本申请实施例提供的一种可能的计算机系统的结构示意图。如图 3 所示，计算机系统 200 包括第一进程 210、第二进程 220、内存 230 以及安全访问控制装置 240。下面对计算机系统 200 中的各个部分进行简单描述。

第一进程 210 是运行在第一 enclave 中的进程，第二进程 220 是运行在第二 enclave 中的进程，第一 enclave 和第二 enclave 是不同的 enclave。其中，第一 enclave 包括第一程序和第一内存空间，第一程序运行于第一 enclave 中，第一程序的运行过程即为第一进程 210，第一内存空间是内存 230 上的一段连续的内存空间，用于存储第一程序以及第一程序运行过程中产生的数据；第二 enclave 包括第二程序和第二内存空间，第二程序运行于第二 enclave 中，第二程序的运行过程即为第二进程 220，第二内存空间是内存 230 上的一段连续的、与第一内存空间不重叠的内存空间，用于存储第二程序以及第二程序运行过程中产生的数据。需要说明的是，第一 enclave 和第二 enclave 的详细说明可参见图 1 中关于 enclave 130 的描述，为了简便，此处不再展开额外的叙述。

内存 230 包括上述第一内存空间、第二内存空间以及共享内存空间 231。可选的，计算机系统 200 还可以包括运行在不可信环境中的进程，例如，不可信 OS、不可信应用程序对应的进程，因此，内存 230 还可以包括相应的内存空间，例如，不可信 OS 对应的进程能够访问的内存空间，以及不可信应用程序对应的进程能够访问的内存空间。而且，除了第一 enclave 和第二 enclave，计算机系统 200 还可以包括其他的 enclave，因此，内存 230 还可以包括其他 enclave 中的内存空间。

安全访问控制装置240用于创建共享内存空间231，其中，共享内存空间231是内存230中的一段连续的内存空间，支持第一进程210和第二进程220访问，换句话说，第一进程210和第二进程220具有访问共享内存空间231的权限，本申请实施例中，上述第一进程210和第二进程220具有访问共享内存空间231的权限是指：第一进程210和第二进程220可以向向共享内存空间231读写数据，那么第一进程210和第二进程220也就可以基于共享内存空间231实现通信。在一些实施例中，为了提高第一进程210和第二进程220之间的通信的安全性，共享内存空间231可以仅支持可信进程访问，其中，可信进程包括第一进程210和第二进程220。这样，第一进程210和第二进程220之间的通信就可以无需经由不可信进程对数据进行转发，也就无需拷贝数据以及加密数据，从而减小通信过程中的损耗。

可选的，安全访问控制装置240还用于配置访问控制表，其中，访问控制表用于表明具有访问共享内存空间231权限的进程（包括第一进程210和第二进程220）。这样，安全访问控制装置240便可以基于访问控制表确定第一进程210和第二进程220能够访问共享内存空间231，从而允许第一进程210和第二进程220向共享内存空间231写入数据，或从共享内存空间231中读取数据，进而实现第一进程210和第二进程220之间的通信。

下面以第一进程210向第二进程220发送数据为例，描述本申请实施例提供的通信方法，该方法由安全访问控制装置240执行，也就是说通过下文还可以进一步描述安全访问控制装置240的功能。如图4所示，整个通信过程可以分为两个阶段：第一阶段是共享内存空间231的创建阶段（S101-S104），第二阶段是通信阶段（S105-S113）。

S101：安全访问控制装置240接收来自第一进程210的通信请求。

其中，通信请求包括共享内存空间231的大小和多个进程220的标识。多个进程220包括第一进程210和第二进程220，可选的，第一进程210的标识可以是第一进程210的ID、第一enclave的ID、或存储有第一程序的内存空间的物理地址等，类似的，第二进程220的标识可以是第二进程220的ID、第二enclave的ID、或存储有第二程序的内存空间的物理地址等，本申请实施例不作限定。

应理解，当第一进程210想要向第二进程220发送数据时，第一进程210可以确定自身的标识、第二进程220的标识以及待发送数据的大小。因此，第一进程210可以根据待发送数据的大小确定共享内存空间231的大小，从而得到上述通信请求，并向安全访问控制装置240发送上述通信请求。

S102：安全访问控制装置240根据上述通信请求创建共享内存空间231。

其中，共享内存空间231是内存230中一段满足上述大小要求的内存空间。具体地，安全访问控制装置240接收到上述通信请求后，对通信请求进行解析，获得共享内存空间231的大小，然后，根据共享内存空间231的大小，从内存230中选取一段连续的、满足上述大小要求的内存空间。之后，安全访问控制装置240判断上述选取的内存空间是否可用，当上述选取的内存空间可用时，将上述选取的内存空间作为共享内存空间231；当上述选取的内存空间不可用时，安全访问控制装置240重复上述从内存230中选取内存空间的步骤，直至选取到可用的内存空间。

在一种可能的实现方式中，安全访问控制装置240判断上述选取的内存空间是否可用，包括如下步骤：安全访问控制装置240记录上述选取的内存空间的地址范围，然后根据记录的地址范围确定这一段内存空间与内存230中已使用的内存空间（包括第一内存空间和第二内存空间）是否重叠。当上述选取的内存空间的地址范围与上述已使用的内存空间的地址范

围不重叠时，确定上述选取的内存空间可用，相反的，当上述选取的内存空间的地址范围与上述已使用的内存空间的地址范围有重叠时，确定上述选取的内存空间不可用。

S103：安全访问控制装置 240 配置访问控制表。

其中，访问控制表用于表明具有访问共享内存空间 231 权限的进程，包括第一进程 210 和第二进程 220。

可选的，为了保证第一进程 210 和第二进程 220 之间通信的安全性，访问控制表可以配置为：可信进程具有访问共享内存空间 231 的权限，此处的可信进程可以包括通信请求指定的进程，即，通信请求中包括的多个进程的标识所对应的多个进程是可信进程。另外，考虑到计算机系统 200 中可能还包括多个比第一进程 210 和第二进程 220 的权限更高的进程，这一部分进程也可以是可信进程。

可选的，访问控制表还可以配置为：不可信进程不具有访问共享内存空间 231 的权限，此处的不可信进程包括运行在不可信执行环境中的进程，其中，不可信环境的描述可参见上述图 1 的相关叙述。

在一些实施例中，访问控制表包括多个标识以及共享内存空间 231 的地址范围，其中，多个标识中的每个标识对应一个进程，多个标识包括第一进程 210 的标识和第二进程 220 的标识。访问控制表用于指示多个标识对应的多个进程具有访问共享内存空间 231 的权限。共享内存空间 231 的地址范围可以通过共享内存空间 231 的基地址以及偏移量，或者共享内存空间 231 的基地址以及末地址等多种方式来表示，此处不作具体限定。

S104：安全访问控制装置 240 分别向第一进程 210 和第二进程 220 发送第一消息，以告知第一进程 210 和第二进程 220 已完成共享内存空间 231 的创建。

其中，第一消息包括共享内存空间 231 的地址范围。具体地，安全访问控制装置 240 根据访问控制表获得第一进程 210 的标识、第二进程 220 的标识以及共享内存空间 231 的地址范围，然后，根据共享内存空间 231 的地址范围得到第一消息，根据第一进程 210 的标识向第一进程 210 发送第一消息，根据第二进程 220 的标识向第二进程 220 发送第一消息。

S105：安全访问控制装置 240 接收来自第一进程 210 的写数据请求。

其中，写数据请求包括第一进程 210 的标识、待写入的数据以及目标地址，共享内存空间 231 包括上述目标地址指示的内存空间。具体地，第一进程 210 接收到第一消息后，通过解析第一消息获得共享内存空间 231 的地址范围，然后根据共享内存空间 231 的地址范围确定目标地址，从而得到写数据请求，并向安全访问控制装置 240 发送上述写数据请求。

S106：安全访问控制装置 240 根据访问控制表确定第一进程 210 是否具有访问目标地址指示的内存空间的权限。如果第一进程 210 不具有访问目标地址指示的内存空间的权限，则执行 S107；如果第一进程 210 具有访问目标地址指示的内存空间的权限，则执行 S108-S113。

具体地，安全访问控制装置 240 接收到上述写数据请求后，通过解析写数据请求获得第一进程 210 的标识，然后将第一进程 210 的标识与访问控制表中的多个标识进行匹配。如果第一进程 210 的标识与访问控制表中的所有标识均不同，则确定第一进程 210 不具有访问共享内存空间 231 的权限，安全访问控制装置 240 将执行 S107；如果第一进程 210 的标识与访问控制表中的任一个标识相同，则确定第一进程 210 具有访问共享内存空间 231 的权限，安全访问控制装置 240 将执行 S108-S113。

为了进一步提高共享内存空间 231 的安全性，可选的，安全访问控制装置 240 在确定第一进程 210 的标识与访问控制表中的某一个标识相同后，还执行以下步骤：判断目标地址是否在共享内存空间 231 的地址范围内，如果不在，则执行 S107；如果在，则执行 S108-S113。

S107：安全访问控制装置240不允许上述数据写入目标地址指示的内存空间。

可选的，安全访问控制装置240还可以发出告警信息，以用于说明此时共享内存空间231的访问出现异常。应理解，当出现这种内存访问异常的情况时，意味着此时的共享内存空间231可能出现异常，因此，可选的，安全访问控制装置240还可以执行以下一个或多个步骤：（1）清空共享内存空间231；（2）释放共享内存空间231；（3）删除访问控制表。如此，不仅可以节省计算机系统200中的内存资源，还可以保证第一进程210和第二进程220之间的通信的准确性。

S108：安全访问控制装置240允许上述数据写入目标地址指示的内存空间。

S109：安全访问控制装置240向第二进程220发送第二消息，以告知第二进程220从目标地址指示的内存空间中读取数据。

具体地，安全访问控制装置240根据访问控制表获得第二进程220的标识，然后根据第二进程220的标识向第二进程220发送第二消息。其中，第二消息包括目标地址。

S110：安全访问控制装置240接收来自第二进程220的读数据请求。

其中，读数据请求包括第二进程220的标识和目标地址。具体地，第二进程220接收到上述第二消息后，通过解析第二消息获得目标地址，从而得到读数据请求，并向安全访问控制装置240发送上述读数据请求。

S111：安全访问控制装置240根据访问控制表确定第二进程220是否具有访问目标地址指示的内存空间的权限。如果第二进程220不具有访问目标地址指示的内存空间的权限，则执行S112；如果第二进程220具有访问目标地址指示的内存空间的权限，则执行S113。

具体地，安全访问控制装置240接收到上述读数据请求后，通过解析读数据请求获得第二进程220的标识，然后将第二进程220的标识与访问控制表中的多个进程的标识进行匹配。如果第二进程220的标识与访问控制表中的所有标识均不同，则确定第二进程220不具有访问共享内存空间231的权限，安全访问控制装置240将执行S112；如果第二进程220的标识与访问控制表中的任一个标识相同，则确定第二进程220具有访问共享内存空间231的权限，安全访问控制装置240将执行S113。

与上述S106类似的，为了进一步提高共享内存空间231的安全性，可选的，安全访问控制装置240在确定第二进程220的标识与访问控制表中的某一个标识相同后，还执行以下步骤：判断目标地址是否在共享内存空间231的地址范围内，如果不在，则执行S112；如果在，则执行S113。

S112：安全访问控制装置240不允许第二进程220从目标地址指示的内存空间中读取第一进程210写入的数据。

可选的，安全访问控制装置240还可以发出告警信息，以用于说明此时共享内存空间231的访问出现异常。应理解，当出现这种内存访问异常的情况时，意味着此时的共享内存空间231可能出现异常，因此，可选的，安全访问控制装置240还可以执行以下一个或多个步骤：（1）清空共享内存空间231；（2）释放共享内存空间231；（3）删除访问控制表。如此，不仅可以节省计算机系统200中的内存资源，还可以保证第一进程210和第二进程220之间的通信的准确性。

S113：安全访问控制装置240允许第二进程220从目标地址指示的内存空间中读取第一进程210写入的数据。

可选的，第二进程220从目标地址指示的内存空间中读取到上述数据后，安全访问控制装置240还可以执行以下一个或多个步骤：（1）清空共享内存空间231；（2）释放共享内存

空间 231；（3）删除访问控制表。如此，可以节省计算机系统 200 的内存资源。

上述实施例仅仅描述了第一进程 210 向第二进程 220 发送数据的过程，应理解，第二进程 220 向第一进程 210 发送数据的过程与上述实施例描述的过程类似，为了简便，本申请中不再展开描述。还应理解，在实际应用中，第一进程 210 可以向运行在不同 enclave 中的多个进程发送数据，例如：第一进程 210 想要向第二进程 220 以及运行在第三 enclave 中的第三进程发送数据，在这种情况下，安全访问控制装置 240 仍然可以基于上述实施例的构思实现第一进程 210 与第二进程 220 以及第三进程的通信。具体实现中，与上述实施例不同的是：通信请求除了包括第一进程 210 的标识和第二进程 220 的标识，还包括第三进程的标识；访问控制表中除了包括第一进程 210 的标识和第二进程 220 的标识，还包括第三进程的标识。这样，第二进程 220 和第三进程均可以从共享内存空间 231 中读取到第一进程 210 写入的数据。

总的来说，通过实施本申请实施例提供的通信方法，可以实现运行在不同 enclave 中的进程之间的安全通信，而且由于上述通信过程无需拷贝数据，也无需加密数据，因此还可以减少整个通信过程带来的损耗。

上文结合图 1-图 4，详细描述了本申请实施例提供的通信方法，接下来将结合图 5-图 7，描述能够执行上述方法的安全访问控制装置 240 以及计算设备。

请参见图 5，图 5 示出了本申请实施例提供的一种安全访问控制装置 240 的结构示意图。如图 5 所示，安全访问控制装置 240 包括通信管理模块 241、内存管理模块 242 以及访问控制模块 243。通信管理模块 241、内存管理模块 242 以及访问控制模块 243 协同工作，以实现上述方法实施例中安全访问控制装置 240 执行的步骤。具体地，通信管理模块 241 用于执行上述 S101、S104-S105、S109-S110；内存管理模块 242 用于执行上述 S102；访问控制模块 243 用于执行上述 S103、S106-S108、S111-S113。在第二进程 220 从目标地址指示的内存空间中读取到第一进程 210 写入的数据后，或者出现如上述 S107 或 S112 所述的共享内存空间 231 的访问异常时，可选的，内存管理模块 242 还可以执行清空共享内存空间 231，以及释放共享内存空间 231 的步骤；访问控制模块 243 还可以执行删除访问控制表的步骤。

应理解，图 5 所示的仅仅是根据功能对上述安全访问控制装置 240 的一种示例性的结构划分方式，本申请实施例并不对安全访问控制装置 240 的结构的具体划分方式进行限定。还应理解，安全访问控制装置 240 内部的各个模块可以是软件模块，也可以是硬件模块，也可以部分是软件模块部分是硬件模块。例如，通信管理模块 241 和内存管理模块 242 是软件模块，访问控制模块 243 是硬件模块。

请参见图 6，图 6 是本申请实施例提供的一种计算设备的结构示意图。该电子设备可以是上文中的安全访问控制装置 240。如图 6 所示，计算设备 300 包括存储器 310、处理器 320、访问控制器 330、通信接口 340 以及总线 350。其中，存储器 310、处理器 320、访问控制器 330、通信接口 340 通过总线 350 实现彼此之间的通信连接。

存储器 310 可以是只读存储器（read only memory, ROM）、静态存储设备、动态存储设备或者随机存取存储器（random access memory, RAM）等。存储器 310 可以存储计算机指令，例如，通信管理模块 241 中的计算机指令、内存管理模块 242 中的计算机指令以及访问控制模块 243 的计算机指令等。存储器 310 中存储的计算机指令可以被处理器 320 以及访问控制器 330 执行，当处理器 320 以及访问控制器 330 执行上述计算机指令时，可以实现安全访问控制装置 240 的部分或全部功能。存储器 310 还可以存储数据，例如：处理器 320 和访问控

制器 330 在执行上述计算机指令时产生的中间数据和结果数据，例如，共享内存空间 231 的地址范围、第一进程 210 的标识、第二进程 220 的标识等。

处理器 320 可以采用 CPU、微处理器（如片上系统（system on chip, SoC））、专用集成电路（application specific integrated circuit, ASIC）、图形处理器（graphics processing unit, GPU）或者一个或多个集成电路。处理器 320 还可以是一种集成电路芯片，具有信号的处理能力，在实现过程中，上述安全访问控制装置 240 的部分功能，即通信管理模块 241 以及内存管理模块 242 的部分或全部功能，可通过处理器 320 中的硬件的集成逻辑电路或者软件形式的指令完成。处理器 320 还可以是通用处理器、数据信号处理器（digital signal process, DSP）、现场可编程逻辑门阵列（field programmable gate array, FPGA）或者其他可编程逻辑器件，分立门或者晶体管逻辑器件，分立硬件组件。通用处理器可以是微处理器，也可以是任何常规的处理器，结合本申请实施例所公开的方法的步骤（例如上述 S101-S105、S109-S110 等）可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器、闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器 310，处理器 320 读取存储器 310 中的信息，结合其硬件完成上述安全访问控制装置 240 中的通信管理模块 241 以及内存管理模块 242 的部分或全部功能。

在一些实施例中，处理器 320 可以执行上述 S101-S105、S109-S110、以及清空共享内存空间 231、释放共享内存空间 231、删除访问控制表中的部分或全部步骤，当处理器 320 执行上述步骤时，可以实现上述安全访问控制装置 240 中的通信管理模块 241 和内存管理模块 242 的部分或全部功能。

访问控制器 330 可以包括至少一个寄存器，至少一个寄存器包括位图（bitmap）寄存器，位图寄存器用于存储具有访问共享内存空间 231 权限的进程的信息。具体实现中，假设位图寄存器的位数为 N（N 为大于 0 的整数），那么位图寄存器可以通过以下方式来存储具有访问共享内存空间 231 权限的进程的信息：位图寄存器的每一个位对应一个进程，当位图寄存器的第 M 位为 1 时，表明该进程具有访问共享内存空间 231 的权限，相反的，当位图寄存器的第 M 位为 0 时，表明该进程不具有访问共享内存空间 231 的权限。其中，选用的位图寄存器可以由计算机系统 200 中、运行在不同 enclave 中的进程的个数确定，例如，计算机系统 200 中通常会运行 10 个进程，这 10 个进程分别运行在 10 个 enclave 中，那么可以选择位数为 10 的位图寄存器。

可选的，上述至少一个寄存器还包括地址寄存器，用于存储共享内存空间的地址范围，其中，地址寄存器的个数可以是两个，如图 6 示出的地址寄存器 1 和地址寄存器 2。其中，地址寄存器 1 用于存储共享内存空间 231 的基地址，地址寄存器 2 用于存储共享内存空间 231 的偏移量。

需要说明的是，上述位图寄存器、地址寄存器 1 以及地址寄存器 2 所起的作用相当于上述方法实施例中的访问控制表，那么，处理器 320 执行配置访问控制表的操作（即 S103）相当于处理器 320 配置上述位图寄存器、地址寄存器 1 以及地址寄存器 2，从而将访问控制表配置到访问控制器 330 中。

在一些实施例中，访问控制器 330 可以执行上述 S106-S108、S111-S113 所描述的部分或全部步骤，当访问控制器 330 执行上述步骤时，可以实现上述安全访问控制装置 240 中的访问控制模块 243 的部分或全部功能。

通信接口 340 使用例如但不限于收发器一类的收发模块，来实现计算设备 300 与其他设

备或通信网络之间的通信。

总线 350 可以包括在计算设备 300 中的各个部件（例如，存储器 310、处理器 320、访问控制器 330、通信接口 340）之间传送信息的通路。

示例性地，上述方法实施例中的第一 enclave 和第二 enclave 部署在计算设备 300 上，存储器 310 还包括上述共享内存空间 231，处理器 320 还用于运行上述第一进程 210 和第二进程 220，在这种场景下，访问控制器 330 的部署是灵活的，具体可以部署在处理器 320（即第一进程 210 和第二进程 220）访问共享内存空间 231 时对应的访问路径上，该条路径可以是：处理器 320→内存总线→内存总线端口→内存仲裁器→内存控制器→共享内存空间 231，其中，内存仲裁器和内存控制器可以是存储器 310 中的部件。在一些实施例中，处理器 320（如 SoC）中集成有内存仲裁器和内存控制器，在这种情况下，上述访问路径可以是：CPU→内存总线→内存总线端口→内存仲裁器→内存控制器→共享内存空间 231。因此，访问控制器 330 可以部署在内存总线、内存总线端口、内存仲裁器以及内存控制器上。

图 7 和图 8 示出了访问控制器 330 部署在内存控制器上的情况，其中，图 7 示出的是访问控制器 330 部署在存储器 310 中的内存控制器上的示意图，图 8 示出的是访问控制器 330 部署在处理器 320 中的内存控制器上的示意图。当访问控制器 330 部署在内存控制器上，如果访问控制器 330 确定第一进程 210 具有访问共享内存空间 231 的权限，则直接将数据写入目标地址指示的内存空间；如果访问控制器 330 确定第一进程 210 不具有访问共享内存空间 231 的权限，则丢弃数据。类似的，如果访问控制器 330 确定第二进程 220 具有访问共享内存空间 231 的权限，则直接从目标地址指示的内存空间中读取数据，并将读取到的数据返回给第二进程 220；如果访问控制器 330 确定第二进程 220 不具有访问共享内存空间 231 的权限，则不会从目标地址指示的共享内存空间 231 中读取数据。

图 9 和图 10 示出了访问控制器 330 部署在内存仲裁器上的情况，其中，图 9 示出的是访问控制器 330 部署在存储器 310 中的内存仲裁器上的示意图，图 10 示出的是访问控制器 330 部署在处理器 320 中的内存仲裁器上的示意图。当访问控制器 330 部署在内存仲裁器上时，如果访问控制器 330 确定第一进程 210 具有访问共享内存空间 231 的权限，则将第一进程 210 发送的写数据请求转发给内存控制器，从而使得第一进程 210 能够将数据写入目标地址指示的内存空间；如果访问控制器 330 确定第一进程 210 不具有访问共享内存空间 231 的权限，则不会将上述写数据请求转发给内存控制器，那么第一进程 210 也不能将数据写入目标地址指示的内存空间。类似的，如果访问控制器 330 确定第二进程 220 具有访问共享内存空间 231 的权限，则将第二进程 220 发送的读数据请求转发给内存控制器，从而使得第二进程 220 能够从目标地址指示的内存空间中读取到数据；如果访问控制器 330 确定第二进程 220 不具有访问共享内存空间 231 的权限，则不会将上述读数据请求转发给内存控制器，那么第二进程 220 也不会从目标地址指示的共享内存空间 231 中读取到数据。

应理解，访问控制器 330 还可以部署内存总线或内存总线端口等处，当访问控制器 330 部署内存总线或内存总线端口处时，访问控制器 330 执行的步骤与上述访问控制器 330 部署在内存仲裁器上时执行的步骤的思路是一致的，为了简便，本申请实施例不再展开叙述。

还应理解，上述实施例仅描述了安全访问控制装置 240 部署在一个计算设备（如计算设备 300）上的场景，在实际应用中，安全访问控制装置 240 的各个模块还可以分别部署在不同计算设备中，例如，通信管理模块 241 和内存管理模块 242 部署在一个计算设备上，访问控制模块 243 部署在另一个计算设备上，本申请实施例对此并不限定。

上述各个附图对应的流程的描述各有侧重，某个流程中没有详细描述的部分，可以参见其他流程的相关描述。

在上述实施例中，可以全部或部分地通过软件、硬件或者其组合来实现。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，其中，该计算机程序产品包括一个或多个由上述安全访问控制装置 240 执行的计算机指令，在计算设备上加载和执行这些计算机指令时，可以全部或部分地实现本申请实施例所述的流程或功能。

上述计算设备可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。上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，上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、双绞线或无线（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。上述计算机可读存储介质存储有一个或多个由上述安全访问控制装置 240 执行的计算机指令。该计算机可读存储介质可以是计算设备能够存取的任何可用介质或者是包含一个或多个介质集成的服务器、数据中心等数据存储设备。上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，光盘）、或者半导体介质（例如，固态硬盘（solid state disk, SSD））。

权 利 要 求 书

1. 一种计算机系统中的通信方法，其特征在于，所述计算机系统包括第一飞地 enclave 和第二 enclave，所述方法包括：

接收来自第一进程的通信请求，其中，所述第一进程是所述第一 enclave 中运行的进程；

根据所述通信请求创建共享内存空间，其中，所述第一进程和第二进程具有访问所述共享内存空间的权限，所述第二进程是所述第二 enclave 中运行的进程。

2. 根据权利要求 1 所述的方法，其特征在于，所述通信请求携带了多个进程的标识，所述多个进程具有访问所述共享内存空间的权限，其中，所述多个进程包括所述第一进程和所述第二进程。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，所述通信请求包括所述共享内存空间的大小，所述共享内存空间为所述计算机系统的内存中一段满足所述大小要求的内存空间。

4. 根据权利要求 3 所述的方法，其特征在于，在所述根据所述通信请求创建共享内存空间之后，所述方法还包括：

配置访问控制表，其中，所述访问控制表用于指示所述第一进程和所述第二进程具有访问所述共享内存空间的权限。

5. 根据权利要求 4 所述的方法，其特征在于，所述方法还包括：

接收来自所述第一进程的写数据请求，其中，所述写数据请求包括待写入的数据和目标地址，所述共享内存空间包括所述目标地址指示的内存空间；

根据所述访问控制表确定所述第一进程具有访问所述目标地址指示的内存空间的权限，允许所述数据写入所述目标地址指示的内存空间；

向所述第二进程发送通知消息，其中，所述通知消息包括所述目标地址，所述通信消息用于指示所述第二进程从所述目标地址指示的内存空间中读取所述数据。

6. 根据权利要求 5 所述的方法，其特征在于，在所述向所述第二进程发送通知消息之后，所述方法还包括：

接收来自所述第二进程的读数据请求，其中，所述读数据请求包括所述目标地址；

根据所述访问控制表确定所述第二进程具有访问所述目标地址指示的内存空间的权限，允许所述第二进程从所述目标地址指示的内存空间中读取所述数据。

7. 一种安全访问控制装置，其特征在于，应用于计算机系统，所述计算机系统包括第一飞地 enclave 和第二 enclave，所述装置包括：

通信管理模块，用于接收来自第一进程的通信请求，其中，所述第一进程是所述第一 enclave 中运行的进程；

内存管理模块，用于根据所述通信请求创建共享内存空间，其中，所述第一进程和第二进程具有访问所述共享内存空间的权限，所述第二进程是所述第二 enclave 中运行的进程。

8. 根据权利要求 7 所述的装置，其特征在于，所述通信请求携带了多个进程的标识，所述多个进程具有访问所述共享内存空间的权限，其中，所述多个进程包括所述第一进程和所述第二进程。

9. 根据权利要求 7 或 8 所述的装置，其特征在于，所述通信请求包括所述共享内存空间的大小，所述共享内存空间为所述计算机系统的内存中一段满足所述大小要求的内存空间。

10. 根据权利要求 9 所述的装置，其特征在于，所述装置还包括访问控制模块，

所述访问控制模块，用于配置访问控制表，其中，所述访问控制表用于指示所述第一进

程和所述第二进程具有访问所述共享内存空间的权限。

11. 根据权利要求 10 所述的装置，其特征在于，

所述通信管理模块，还用于接收来自所述第一进程的写数据请求，其中，所述写数据请求包括待写入的数据和目标地址，所述共享内存空间包括所述目标地址指示的内存空间；

所述访问控制模块，用于根据所述访问控制表确定所述第一进程具有访问所述目标地址指示的内存空间的权限，允许所述数据写入所述目标地址指示的内存空间；

所述通信管理模块，还用于向所述第二进程发送通知消息，其中，所述通知消息包括所述目标地址，所述通信消息用于指示所述第二进程从所述目标地址指示的内存空间中读取所述数据。

12. 根据权利要求 11 所述的装置，其特征在于，

所述通信管理模块，还用于接收来自所述第二进程的读数据请求，其中，所述读数据请求包括所述目标地址；

所述访问控制模块，用于根据所述访问控制表确定所述第二进程具有访问所述目标地址指示的内存空间的权限，允许所述第二进程从所述目标地址指示的内存空间中读取所述数据。

13. 一种计算设备，其特征在于，应用于计算机系统，所述计算机系统包括第一飞地 enclave 和第二 enclave，所述设备包括：

处理器，用于接收来自第一进程的通信请求，并根据所述通信请求创建共享内存空间，其中，所述第一进程是所述第一 enclave 中运行的进程，所述第二进程是所述第二 enclave 中运行的进程，所述第一进程和所述第二进程具有访问所述共享内存空间的权限；配置访问控制表到访问控制器；

所述访问控制器，用于根据所述访问控制表确定所述第一进程和所述第二进程具有访问所述共享内存空间的权限，以使所述第一进程和所述第二进程基于所述共享内存空间实现通信。

14. 根据权利要求 13 所述的设备，其特征在于，所述通信请求携带了多个进程的标识，所述多个进程具有访问所述共享内存空间的权限，其中，所述多个进程包括所述第一进程和所述第二进程。

15. 根据权利要求 13 或 14 所述的设备，其特征在于，所述通信请求包括所述共享内存空间的大小，所述共享内存空间为所述计算机系统的内存中一段满足所述大小要求的内存空间。

16. 根据权利要求 15 所述的设备，其特征在于，

所述处理器，还用于接收来自所述第一进程的写数据请求，其中，所述写数据请求包括待写入的数据和目标地址，所述共享内存空间包括所述目标地址指示的内存空间；

所述访问控制器，用于根据所述访问控制表确定所述第一进程具有访问所述目标地址指示的内存空间的权限，允许所述数据写入所述目标地址指示的内存空间；

所述处理器，还用于向所述第二进程发送通知消息，其中，所述通知消息包括所述目标地址，所述通信消息用于指示所述第二进程从所述目标地址指示的内存空间中读取所述数据。

17. 根据权利要求 16 所述的设备，其特征在于，

所述处理器，还用于接收来自所述第二进程的读数据请求，其中，所述读数据请求包括所述目标地址；

所述访问控制器，用于根据所述访问控制表确定所述第二进程具有访问所述目标地址指示的内存空间的权限，允许所述第二进程从所述目标地址指示的内存空间中读取所述数据。

18. 一种计算机可读存储介质，其特征在于，存储有计算机指令，当所述计算机指令被计算设备执行时，所述计算设备执行前述权利要求 1-6 任一项所述的方法。

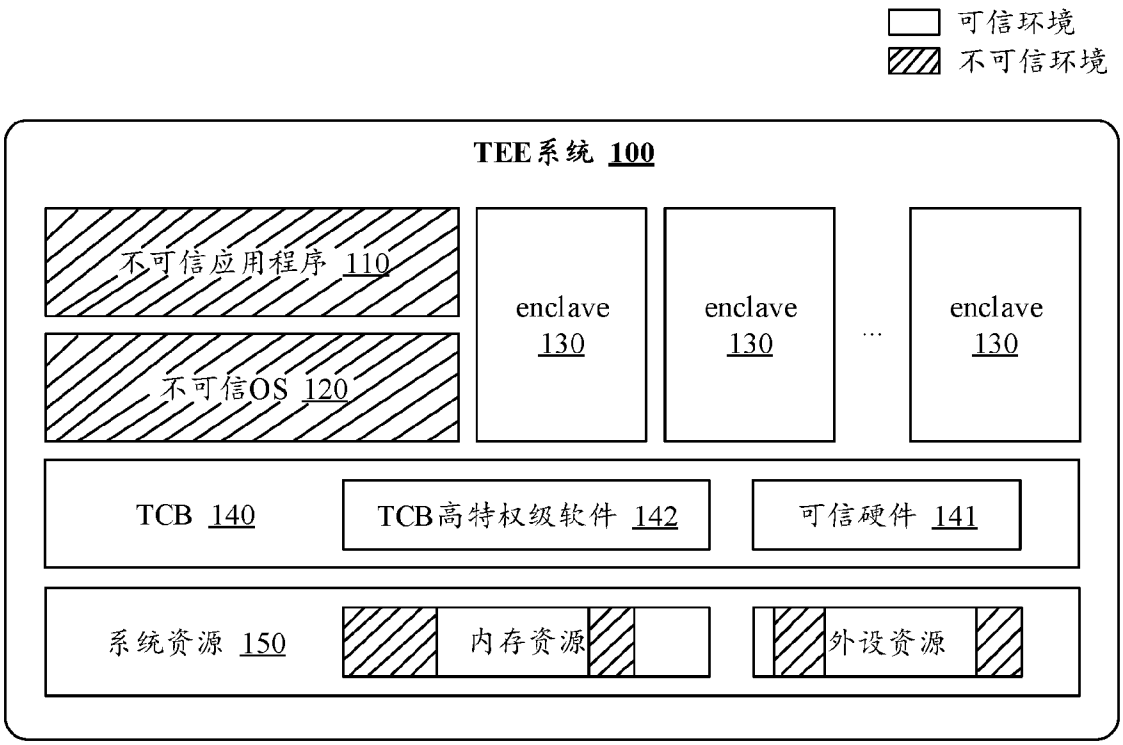
可信环境
不可信环境
TEE系统 100
不可信应用程序 110
不可信OS 120
enclave 130
enclave 130
...
enclave 130
TCB 140
TCB高特权级软件 142
可信硬件 141
系统资源 150
内存资源
外设资源

图 1

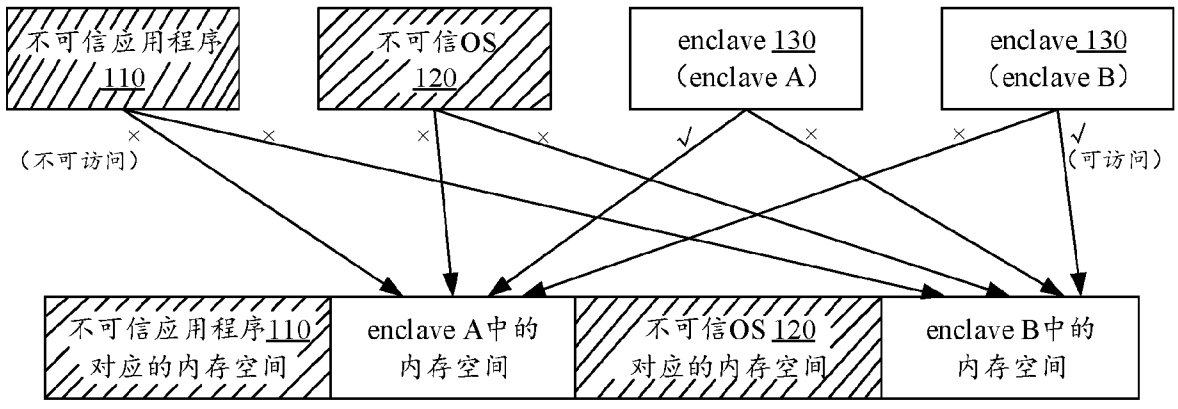
不可信应用程序 110
不可信OS 120
enclave 130 (enclave A)
enclave 130 (enclave B)
×
(不可访问)
√
(可访问)
不可信应用程序110 对应的内存空间
enclave A中的 内存空间
不可信OS 120 对应的内存空间
enclave B中的 内存空间

图 2

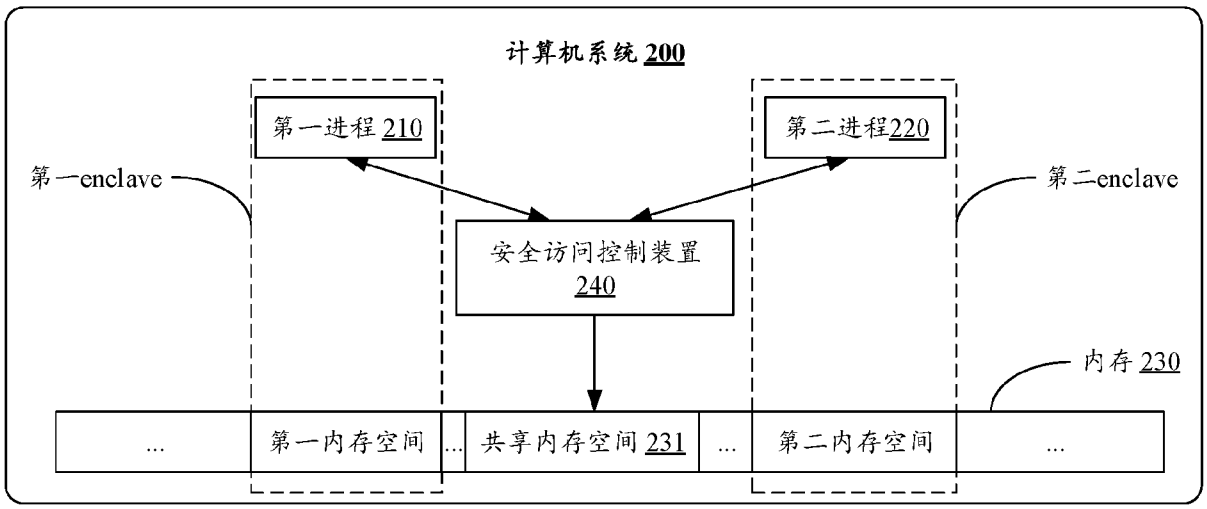
计算机系统 200
第一进程 210
第二进程220
第一enclave
第二enclave
安全访问控制装置
240
内存 230
...
第一内存空间
...
共享内存空间 231
...
第二内存空间
...

图 3

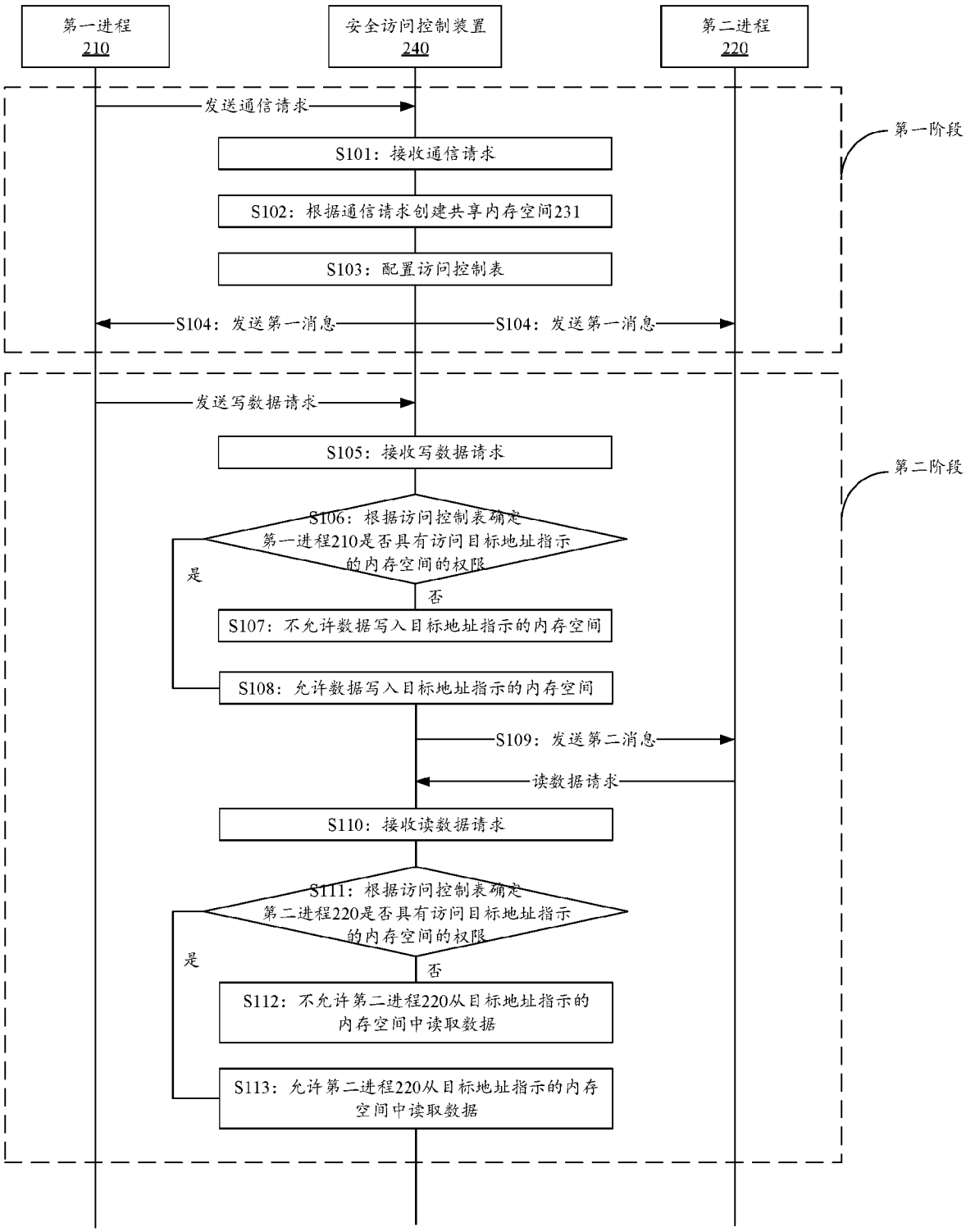
第一进程
210
安全访问控制装置
240
第二进程
220
发送通信请求
S101：接收通信请求
S102：根据通信请求创建共享内存空间231
S103：配置访问控制表
S104：发送第一消息
S104：发送第一消息
第一阶段
发送写数据请求
S105：接收写数据请求
S106：根据访问控制表确定第一进程210是否具有访问目标地址指示的内存空间的权限
是
否
S107：不允许数据写入目标地址指示的内存空间
S108：允许数据写入目标地址指示的内存空间
S109：发送第二消息
读数据请求
S110：接收读数据请求
S111：根据访问控制表确定第二进程220是否具有访问目标地址指示的内存空间的权限
是
否
S112：不允许第二进程220从目标地址指示的内存空间中读取数据
S113：允许第二进程220从目标地址指示的内存空间中读取数据
第二阶段

图 4

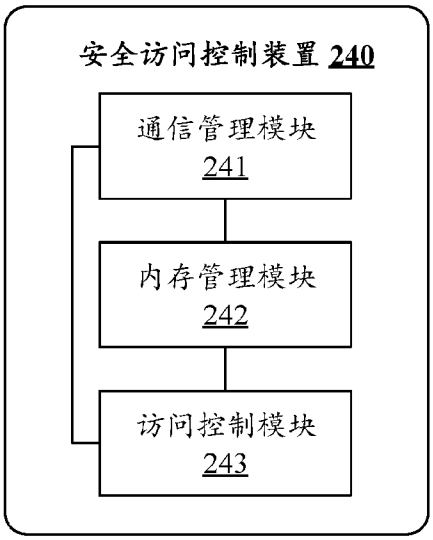
安全访问控制装置 240
通信管理模块
241
内存管理模块
242
访问控制模块
243

图 5

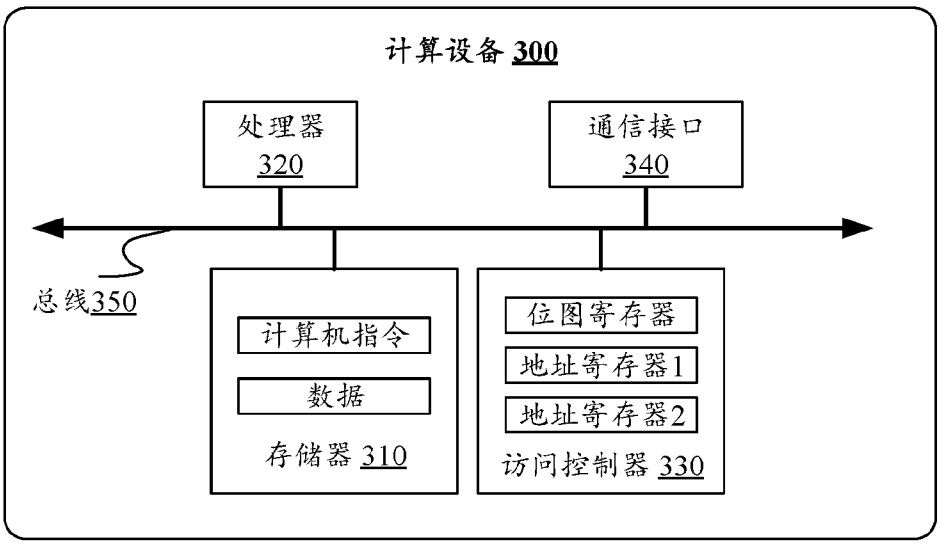
计算设备 300
处理器
320
通信接口
340
总线350
计算机指令
数据
存储器 310
位图寄存器
地址寄存器1
地址寄存器2
访问控制器 330

图 6

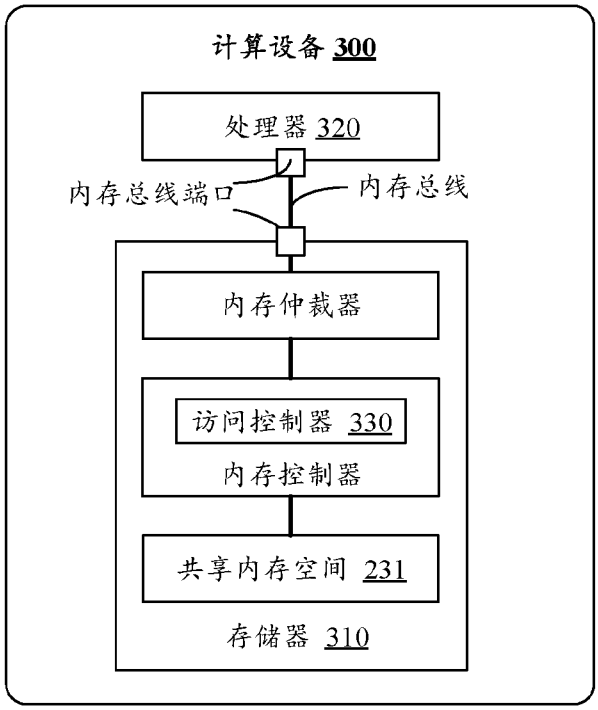
计算设备 300
处理器 320
内存总线端口
内存总线
内存仲裁器
访问控制器 330
内存控制器
共享内存空间 231
存储器 310

图 7

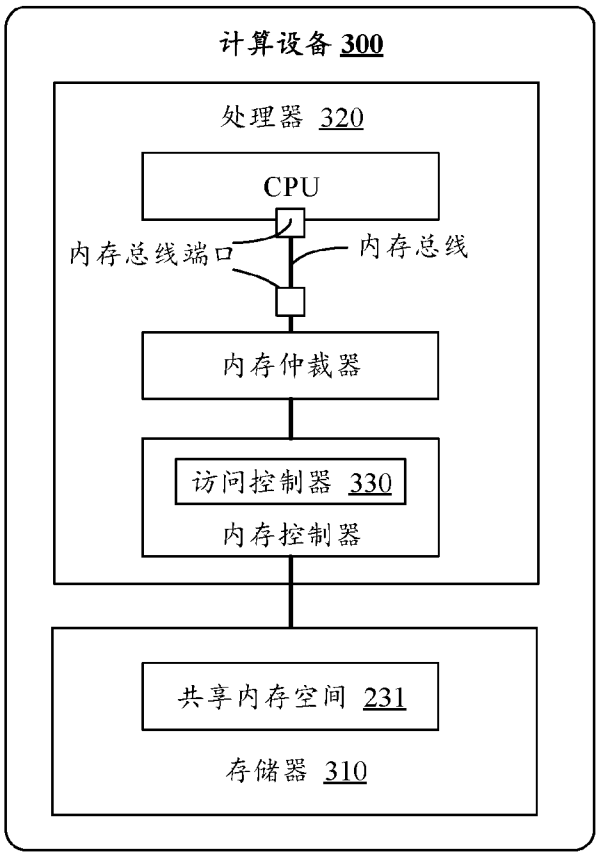
计算设备 300
处理器 320
CPU
内存总线端口
内存总线
内存仲裁器
访问控制器 330
内存控制器
共享内存空间 231
存储器 310

图 8

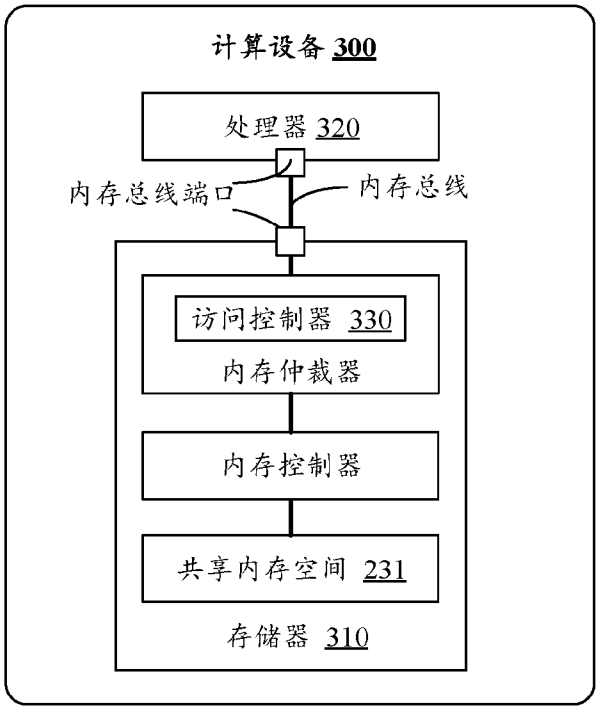
计算设备 300
处理器 320
内存总线端口
内存总线
访问控制器 330
内存仲裁器
内存控制器
共享内存空间 231
存储器 310

图 9

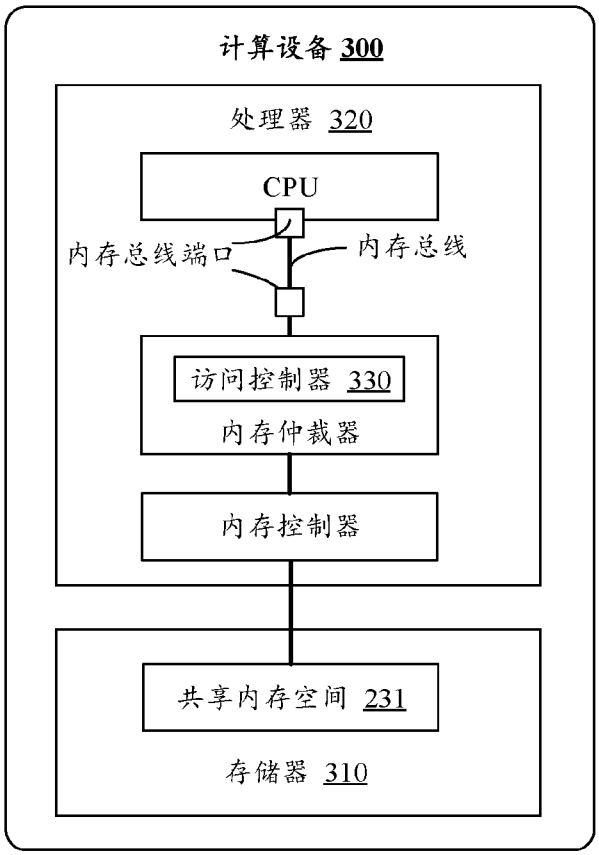
计算设备 300
处理器 320
CPU
内存总线端口
内存总线
访问控制器 330
内存仲裁器
内存控制器
共享内存空间 231
存储器 310

图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/130846

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/54(2006.01)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)

VEN; CNABS; CNTXT; WOTXT; EPTXT; USTXT; CNKI; IEEE: 飞地, 容器, 共享, 内存, 空间, 通信, enclave, shared, memory, space, communication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2019286577 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 19 September 2019 (2019-09-19) description, paragraphs [0005] and [0034]-[0040], and figure 3	1-3, 7-9, 18
X	CN 112817780 A (SHANGHAI JIAO TONG UNIVERSITY) 18 May 2021 (2021-05-18) description, paragraphs [0056]-[0071]	1-3, 7-9, 18
Y	US 2019286577 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 19 September 2019 (2019-09-19) description, paragraphs [0005] and [0034]-[0040], and figure 3	4-6, 10-17
Y	CN 112817780 A (SHANGHAI JIAO TONG UNIVERSITY) 18 May 2021 (2021-05-18) description, paragraphs [0056]-[0071]	4-6, 10-17
Y	CN 108733455 A (SHANGHAI JIAO TONG UNIVERSITY) 02 November 2018 (2018-11-02) description, paragraphs [0116]-[0119]	4-6, 10-17
A	CN 107544918 A (TANGRAM MICROELECTRONIC TECHNOLOGY (SHANGHAI) CO., LTD.) 05 January 2018 (2018-01-05) 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	Date of mailing of the international search report
16 January 2023	**28 January 2023**
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

International application No.
PCT/CN2022/130846

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 109361668 A (STATE GRID ZHEJIANG ELECTRIC POWER CO., LTD. et al.) 19 February 2019 (2019-02-19) entire document	1-18

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/130846

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2019286577 A1	19 September 2019	None	
CN 112817780 A	18 May 2021	None	
CN 108733455 A	02 November 2018	None	
CN 107544918 A	05 January 2018	None	
CN 109361668 A	19 February 2019	None	

国际检索报告

国际申请号
PCT/CN2022/130846

A. 主题的分类

G06F 9/54(2006.01)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））

VEN;CNABS;CNTXT;WOTXT;EPTXT;USTXT;CNKI;IEEE:飞地，容器，共享，内存，空间，通信，enclave, shared, memory, space, communication

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	US 2019286577 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2019年9月19日 (2019-09-19) 说明书第[0005]，[0034]-[0040]段，图3	1-3，7-9，18
X	CN 112817780 A (上海交通大学) 2021年5月18日 (2021-05-18) 说明书第[0056]-[0071]段	1-3，7-9，18
Y	US 2019286577 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2019年9月19日 (2019-09-19) 说明书第[0005]，[0034]-[0040]段，图3	4-6，10-17
Y	CN 112817780 A (上海交通大学) 2021年5月18日 (2021-05-18) 说明书第[0056]-[0071]段	4-6，10-17
Y	CN 108733455 A (上海交通大学) 2018年11月2日 (2018-11-02) 说明书第[0116]-第[0119]段	4-6，10-17
A	CN 107544918 A (致象尔微电子科技上海有限公司) 2018年1月5日 (2018-01-05) 全文	1-18
A	CN 109361668 A (国网浙江省电力有限公司 等) 2019年2月19日 (2019-02-19) 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	国际检索报告邮寄日期
2023年1月16日	2023年1月28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 刘洁 电话号码 010-53961345

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/130846

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)
US 2019286577 A1	2019年9月19日	无	
CN 112817780 A	2021年5月18日	无	
CN 108733455 A	2018年11月2日	无	
CN 107544918 A	2018年1月5日	无	
CN 109361668 A	2019年2月19日	无	