(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2024 年 12 月 19 日 (19.12.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/255640 A1

(51) 国际专利分类号:
G06F 9/455 (2018.01)

(21) 国际申请号: PCT/CN2024/097172

(22) 国际申请日: 2024 年 6 月 4 日 (04.06.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310712879.1 2023年6月15日 (15.06.2023) CN

(71) 申请人: 海光信息技术股份有限公司 (**HYGON INFORMATION TECHNOLOGY CO., LTD.**) [CN/CN]; 中国天津市滨海新区华苑产业区海泰西路18号北2-204工业孵化-3-8, Tianjin 300392 (CN)。

(72) 发明人:刘子行(**LIU, Zixing**); 中国天津市滨海新区华苑产业区海泰西路18号北2-204工业孵化-3-8, Tianjin 300392 (CN)。 应志伟(**YING, Zhiwei**); 中国天津市滨海新区华苑产业区海泰西路18号北2-204工业孵化-3-8, Tianjin 300392 (CN)。 杨葛(**YANG, Ge**); 中国天津市滨海新区华苑产业区海泰西路18号北2-204工业孵化-3-8, Tianjin 300392 (CN)。

(74) 代理人:北京市柳沈律师事务所(**LIU , SHEN & ASSOCIATES**); 中国北京市海淀区彩和坊路10号1号楼10层, Beijing 100080 (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, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD,

(54) **Title:** METHOD FOR CONFIGURING CRYPTOGRAPHIC HARDWARE, CONFIDENTIAL COMPUTING METHOD FOR DATA, AND RELATED DEVICE

(54) 发明名称: 加密硬件的配置方法、数据机密计算方法及相关设备

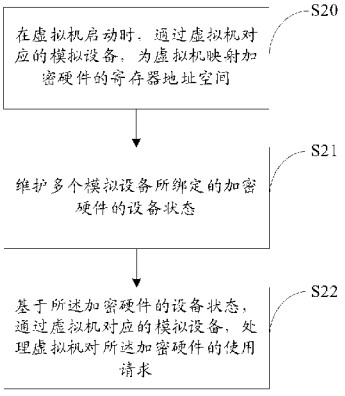

图 9

(57) **Abstract:** Provided in the embodiments of the present disclosure are a method for configuring cryptographic hardware, a confidential computing method for data, and a related device. The method for configuring cryptographic hardware comprises: maintaining a device state of cryptographic hardware bound to a plurality of simulation devices, which device state is an idle state or a busy state, wherein one simulation device corresponds to one virtual machine, and a plurality of simulation devices are bound to the cryptographic hardware, such that the plurality of virtual machines share the cryptographic hardware by means of the corresponding simulation devices; and on the basis of the device state of the cryptographic hardware, processing a use request of a virtual machine for the cryptographic hardware by means of the simulation device corresponding to the virtual machine, such that the virtual machine uses the cryptographic hardware, wherein the virtual machine is any one of the plurality of virtual machines. The embodiments of the present disclosure can improve the utilization rate of cryptographic hardware by virtual machines.

WO 2024/255640 A1

[见续页]

SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

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

本国际公布:
— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本公开的实施例提供一种加密硬件的配置方法、数据机密计算方法及相关设备，加密硬件的配置方法包括：维护多个模拟设备所绑定的加密硬件的设备状态，设备状态包括空闲状态和忙碌状态；其中，一个模拟设备对应一个虚拟机，并且多个模拟设备与加密硬件相绑定，以使得多个虚拟机通过对应的模拟设备共享加密硬件；基于加密硬件的设备状态，通过虚拟机对应的模拟设备，处理虚拟机对加密硬件的使用请求，以使得虚拟机使用加密硬件，虚拟机为多个虚拟机中的任一个虚拟机。本公开的实施例能够提升虚拟机对于加密硬件的利用率。

加密硬件的配置方法、数据机密计算方法及相关设备

本申请要求于 2023 年 6 月 15 日递交的中国专利申请第 202310712879.1 号的优先权，在此全文引用上述中国专利申请公开的内容以作为本申请的一部分。

技术领域

本公开实施例涉及一种加密硬件的配置方法、数据机密计算方法及相关设备。

背景技术

通过虚拟化技术（Virtualization），计算机可虚拟化出多台虚拟机（Virtual Machine，VM），从而高效利用计算机的硬件资源。虚拟机在进行数据的密码计算时，涉及到利用计算机中的加密硬件进行密码计算。在此背景下，如何提供技术方案，以提升虚拟机对于加密硬件的利用率，成为了本领域技术人员亟需解决的技术问题。

发明内容

有鉴于此，本公开实施例提供一种加密硬件的配置方法、数据机密计算方法及相关设备，以实现提升虚拟机对于加密硬件的利用率，提高虚拟机数据处理性能。

第一方面，本公开实施例提供一种加密硬件的配置方法，包括：

维护多个模拟设备所绑定的加密硬件的设备状态，所述设备状态包括空闲状态和忙碌状态；其中，一个模拟设备对应一个虚拟机，并且多个模拟设备与加密硬件相绑定，以使得多个虚拟机通过对应的模拟设备共享加密硬件；

基于所述加密硬件器的设备状态，通过虚拟机对应的模拟设备，处理所述虚拟机对所述加密硬件器的使用请求，以使得虚拟机使用所述加密硬件，所述虚拟机为多个虚拟机中的任一个虚拟机。

第二方面，本公开实施例提供一种加密硬件的配置装置，包括：

状态维护逻辑，用于维护多个模拟设备所绑定的加密硬件的设备状态，所述设备状态包括空闲状态和忙碌状态；其中，一个模拟设备对应一个虚拟机，并且多个模拟设备与加密硬件相绑定，以使得多个虚拟机通过对应的模拟设备共享加密硬件；

请求处理逻辑，用于基于所述加密硬件器的设备状态，通过虚拟机对应的模拟设备，处理所述虚拟机对所述加密硬件器的使用请求，以使得虚拟机使用所述加密硬件，所述虚拟机为多个虚拟机中的任一个虚拟机。

第三方面，本公开实施例提供一种数据机密计算方法，包括：

获取虚拟机发送的对于模拟设备的机密计算命令，模拟设备用于模拟安全密码协处理器的程序，所述安全密码协处理器为根据如上述所述的加密硬件的配置方法配置得到的加密硬件；

获取所述安全密码协处理器的使用权限，以使得根据所述机密计算命令，得到所述安全密码协处理器的机密计算结果，并将所述机密计算结果返回至虚拟机。

第四方面，本公开实施例提供一种数据机密计算装置，包括：

命令获取逻辑，用于获取虚拟机发送的对于模拟设备的机密计算命令，模拟设备用于模拟安全密码协处理器的程序，所述安全密码协处理器为根据如上述所述的加密硬件的配置方法配置得到的加密硬件；

硬件使用逻辑，用于获取所述安全密码协处理器的使用权限，以使得根据所述机密计算命令，得到所述安全密码协处理器的机密计算结果，并将所述机密计算结果返回至虚拟机。

第五方面，本公开实施例提供一种计算机系统，包括：虚拟机监视器、多个虚拟机，以及加密硬件；所述虚拟机监视器包括如上述所述的加密硬件的配置装置，或者，如上述所述的数据机密计算装置。

第六方面，本公开实施例提供一种电子设备，包括存储器和处理器，所述存储器上存储有可由所述处理器运行的计算机程序，所述处理器运行所述计算机程序时执行如上述所述的加密硬件的配置方法，或者，如上述所述的数据机密计算方法中的步骤。

第七方面，本公开实施例提供一种存储介质，所述存储介质存储一条或多条计算机可执行指令，所述一条或多条计算机可执行指令被执行时，实现

如上述所述的加密硬件的配置方法，和/或，如上述所述的数据机密计算方法。

本公开实施例所提供的加密硬件的配置方法中，通过维护多个模拟设备所绑定的密码协处理器的设备状态，所述设备状态包括空闲状态和忙碌状态，其中，一个模拟设备对应一个虚拟机，并且多个模拟设备与加密硬件相绑定，以使得多个虚拟机通过对应的模拟设备共享加密硬件；进而，基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理所述虚拟机对所述加密硬件的使用请求，以使得所述虚拟机使用所述加密硬件，所述虚拟机为多个虚拟机中的任一个虚拟机。

可见，本公开实施例通过多个模拟设备对加密硬件的设备状态维护，从而多个虚拟机能够共享加密硬件，在加密硬件为空闲状态时，多个虚拟机中的任一个虚拟机能够使用加密硬件进行计算处理，进而基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理虚拟机对所述加密硬件的使用请求，保障加密硬件在一个时刻被一个虚拟机使用，实现多个虚拟机共享加密硬件进行数据的密码计算处理，提升虚拟机对于加密硬件的利用率，提高虚拟机的数据处理性能。

附图说明

为了更清楚地说明本公开实施例的技术方案，下面将对实施例所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本公开的实施例，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，还可以根据提供的附图获得其他的附图。

图 1 是计算机系统的可选架构示意图；

图 2 是计算机系统的另一可选架构示意图；

图 3 是计算机系统的又一可选架构示意图；

图 4 是加密硬件的可选架构示意图；

图 5 是加密硬件的可选配置方法；

图 6 是本公开实施例提供的加密硬件的配置方法的可选流程图；

图 7 是本公开实施例提供的多个虚拟机对加密硬件的访问示意图；

图 8 是本公开实施例提供的虚拟机访问加密硬件的交互示意图；

图 9 是本公开实施例提供的加密硬件的配置方法的另一可选流程图；

图 10 是本公开实施例提供的虚拟机访问加密硬件的地址映射示意图；

图 11 是本公开实施例提供的虚拟机通过模拟设备同步访问共享内存空间的交互示意图；

图 12 是本公开实施例提供的加密硬件访问内存的地址转换示意图；

图 13 是本公开实施例提供的多个虚拟机共享加密硬件的计算时序图；

图 14 是本公开实施例提供的加密硬件的配置装置的可选框图；

图 15 是本公开实施例提供的数据机密计算方法的可选流程图；

图 16 是本公开实施例提供的多个虚拟机同步访问安全密码协处理器的交互示意图；以及

图 17 是本公开实施例提供的数据机密计算装置的可选框图。

具体实施方式

下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本公开一部分实施例，而不是全部的实施例。基于本公开中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本公开保护的范围。

作为一种可选示例，图 1 示出了计算机系统的可选架构示意图，如图 1 所示，计算机系统的架构可以包括：CPU（Central Processing Unit，中央处理器）核心 1，加密硬件 2，内存 3。

其中，CPU 核心 1 可通过软件形式配置虚拟机监视器（Virtual Machine Monitor，VMM）11，并通过虚拟化技术虚拟化出多个虚拟机（Virtual Machine，VM）12，该多个虚拟机 12 可由虚拟机监视器 11 进行管理。

加密硬件 2 是进行密码计算处理的硬件设备，例如密码协处理器，利用加密硬件 2 能够优化密码学计算中频繁的数据操作，节省计算时间，提高计算速度，提升对数据的密码学计算性能。

在一个示例中，加密硬件 2 可以用于对虚拟机的虚拟机数据进行密码计算。当加密硬件被某一虚拟机调用时，加密硬件 2 可以获取该虚拟机的数据计算命令，从而根据该数据计算命令的地址信息，从内存中得到对应的数据，并进行数据的密码运算，所述密码运算可以是加密计算、解密计算或哈希计算等。其中，加密硬件的调用可以是通过加密硬件的驱动程序，来驱动加密

硬件工作。

需要说明的是，加密硬件在图 1 所述系统架构的运行环境为普通计算环境时，能够实现基础的密码计算功能。但是，由于普通计算环境下，加密硬件的硬件资源可以被虚拟机直接访问，并且，加密硬件不存在封闭的执行环境，导致其并不具备对数据的机密计算能力。

为提升数据的机密性和完整性，以及计算过程的机密性，计算机系统中还可以设置机密计算环境，图 2 示出了计算机系统的另一可选架构示意图，其中，纵向虚线用于区分机密计算环境和普通计算环境，实线框是机密计算环境的组件，虚线框是普通计算环境的组件。

如图 2 所示，计算机系统可以包括硬件层、系统软件层、服务层、应用层和跨层管理五个部分。其中，硬件层基于硬件隔离实现受保护的资源不被开放系统访问，并基于硬件安全功能为机密计算提供受信任的硬件基础；系统软件层为机密计算提供基于软件的隔离机制、必要的硬件资源和基础服务；服务层为上层应用程序提供统一的机密计算服务接口及安全服务，安全服务是由底层的系统软件和硬件以及管理模块交互形成，机密计算统一服务接口用以屏蔽底层硬件架构和软件的开发接口差异；应用层是直接面向结果需求方的应用程序，结果需求方通过应用程序执行计算操作；跨层管理为执行机密计算业务提供必要的管理模块。

在一个示例中，机密计算环境中的硬件层的组件可以主要包括可信执行控制单元、隔离内存空间、可信固件、硬件密码引擎、设备唯一密钥、随机数生成器、信任根；系统软件层的组件可以主要包括机密计算操作系统、机密计算虚拟化软件；服务层的组件可以主要包括机密计算统一服务接口、隔离计算、安全启动、远程证明、安全信道、密钥派生、存储保护、密码运算、数据封装；应用层的组件可以主要包括机密计算应用程序；跨层管理的组件可以主要包括密钥管理、日志管理、白名单管理、 资源管理。

需要说明的是，在机密计算环境的硬件层的组件中，可信固件可以例如安全处理器。在以虚拟机为实现方式的可信执行环境中，图 3 示例性的示出了计算机系统的又一可选架构示意图。对应图 1，结合图 3 所示，系统架构还可以包括：安全处理器 4，安全处理器 4 是专门设置的负责处理与虚拟机的机密计算相关操作的处理器。例如，安全处理器 4 可进行内存加解密等操

作，从而避免物理主机、虚拟机监视器 11 对虚拟机的数据访问和篡改，保障虚拟机的数据安全。

图 3 所示系统架构的运行环境可以包括机密计算环境，安全处理器具有封闭的可执行环境，虚拟机监视器 11 可配置与安全处理器 4 相通信的 API 接口，实现虚拟机监视器 11 与安全处理器 4 的数据交互。

为进一步从硬件的角度保障虚拟机的数据安全，提升数据的机密性和完整性，在计算机系统包括机密计算环境和普通计算环境的情况下，可以对应存在不同的加密硬件。如图 4 所示加密硬件的可选架构示意图，可以进一步将加密硬件设置为相隔离的普通密码协处理器和安全密码协处理器。

所述普通密码协处理器也可以称为高性能密码协处理器，为针对虚拟机进行基础密码计算的硬件，普通密码协处理器的硬件资源能够被 CPU 核心直接访问，应用于普通计算环境下；安全密码协处理器为针对虚拟机进行机密计算的硬件，并且，安全密码协处理器与安全处理器能够使用封闭的执行环境，从而安全密码协处理器的硬件资源不能被虚拟机直接访问，其可以由安全处理器进行配置，能够在虚拟机进行安全等级要求高的机密计算任务时使用，实现虚拟机数据的机密计算，保证机密数据不被外泄。

需要说明的是，参考图 3 所示，CPU 核心 1 中的虚拟机 12 可以包括虚拟机 121 和虚拟机 122。其中，虚拟机 121 为在普通计算环境下，未使用安全保护机制的虚拟机，如使用普通内存的普通虚拟机；虚拟机 122 为在机密计算环境下，使用安全保护机制的虚拟机，如使用安全内存的安全虚拟机。并且，安全虚拟机的安全性可高于普通虚拟机，安全处理器 4 可为安全虚拟机分配安全内存，并维护安全虚拟机的嵌套页表，避免主机操作系统、虚拟机监视器等获取安全内存的使用情况，降低虚拟机被攻击的风险。

可以理解的是，通过虚拟化技术，计算机可虚拟化出多台虚拟机，而在以虚拟机为实现方式的可信执行环境（Trusted Execution Environment，TEE），即普通计算环境、机密计算环境，虽然加密硬件可以包括普通密码协处理器、安全密码协处理器，但是，加密硬件的硬件数量远远小于虚拟出的虚拟机数量，并且，多个虚拟机同时使用加密硬件将导致加密硬件的硬件资源冲突。

因此，为实现虚拟机利用加密硬件进行密码计算或机密计算，作为一种可选实现，如图 5 所示，可以将加密硬件直通给多个虚拟机中的任一虚拟机

使用，例如：在普通计算环境下，将一普通密码协处理器直通给一普通虚拟机使用，或者，在机密计算环境下，将安全密码协处理器直通给一安全虚拟机使用。直通给虚拟机的加密硬件获取并执行虚拟机发送的数据计算任务，并且，在计算结束后通过中断通知直通的虚拟机，从而节省 CPU 的计算带宽。

但是，在数据处理过程中，发明人发现：加密硬件只能由直通的虚拟机使用，其他虚拟机或主机操作系统无法使用，这将导致虚拟机无法高效利用加密硬件实现计算功能，降低了虚拟机的数据处理性能。

可见，如何实现提升虚拟机对于加密硬件的利用率，显得尤为重要。基于此，本公开实施例通过改进的技术方案，利用虚拟机监视器的多个模拟设备对加密硬件进行设备状态维护，从而多个虚拟机能够共享加密硬件，并且，基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理虚拟机对所述加密硬件的使用请求，以使得多个虚拟机中的任一个虚拟机使用所述加密硬件进行密码计算，实现提升虚拟机对于加密硬件的利用率，提高虚拟机的数据处理性能。

基于上述思路，图 6 示例性的示出了本公开实施例提供的加密硬件的配置方法的可选流程图，该方法流程可由虚拟机监视器实现。其中，虚拟机监视器可以通过模拟设备层，在虚拟机启动时创建多个模拟设备，所述模拟设备用于模拟加密硬件的配置，一个模拟设备对应一个虚拟机，虚拟机对加密硬件的使用需要通过对应的模拟设备建立使用关系，并且，虚拟机监视器能够指定模拟设备绑定的加密硬件。参照图 6，该方法流程可以包括如下步骤。

步骤 S21，维护多个模拟设备所绑定的加密硬件的设备状态。

本公开实施例中的虚拟机监视器增加了一层模拟设备层，通过模拟设备层实现多个虚拟机对密码协处理器的共享，使得多个虚拟机能够并发访问加密硬件，进行数据处理，避免采用直通的方式，将加密硬件直通给单个虚拟机。

基于所述模拟设备层，设置多个模拟设备，所述模拟设备可以是模拟加密硬件的配置，一个模拟设备对应一个虚拟机，多个模拟设备与加密硬件相绑定，从而虚拟机不再直接访问加密硬件，而是访问对应的模拟设备，使得多个虚拟机通过对应的模拟设备共享加密硬件。

其中，图 7 示例性的示出了本公开实施例中多个虚拟机对加密硬件的访问示意图。如图 7 所示，多个虚拟机访问对应的模拟设备，通过对应的模拟设备共享加密硬件。图 7 中，多个模拟设备之间相互同步操作，控制虚拟机对加密硬件的访问，当一虚拟机通过模拟设备对加密硬件进行使用时，另一虚拟机需等待加密硬件的执行完成。

在一些实施例中，虚拟机监视器可以对应有共享内存空间，其中，所述共享内存空间可以配置为允许多个模拟设备进行读写，则多个模拟设备可以将所绑定的加密硬件的设备状态存储在共享内存空间中，从而在共享内存空间中可以记录多个模拟设备所绑定的加密硬件的设备状态，而且，多个模拟设备可以基于对共享内存空间的访问，共享加密硬件的设备状态。

所述设备状态可以包括加密硬件的空闲状态和忙碌状态，其中，加密硬件处于空闲状态时，表示加密硬件未执行密码计算处理，可以被任一虚拟机使用；加密硬件处于忙碌状态时，表示加密硬件当前被某一虚拟机占用，正在执行密码计算处理，不能被除当前使用的虚拟机之外的其他虚拟机使用。基于虚拟机对加密硬件的使用需要通过对应的模拟设备，因此，通过维护多个模拟设备所绑定的加密硬件的设备状态，能够使得多个虚拟机通过对应的模拟设备共享加密硬件。

步骤 S22，基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理虚拟机对所述加密硬件的使用请求。

基于加密硬件的设备状态包括空闲状态和忙碌状态，当多个虚拟机中的任一个虚拟机，具有使用加密硬件进行密码计算的需求时，虚拟监视器可以通过虚拟机对应的模拟设备，处理所述虚拟机对加密硬件的使用请求。

作为一种可选实现，虚拟机可以基于对应的模拟设备查询加密硬件的设备状态，从而确定对加密硬件的使用请求的发送时机。在一个示例中，如果模拟设备查询到所述加密硬件的设备状态为空闲状态，则可以通过虚拟机对应的模拟设备，获取虚拟机请求使用所述加密硬件的使用请求，进而通过虚拟机对应的模拟设备响应该使用请求，以使得所述虚拟机使用所述加密硬件，实现虚拟机对加密硬件的使用。

可以理解的是，在虚拟化技术中，加密硬件用于对虚拟机的虚拟机数据进行密码计算处理，由于虚拟机数据对应虚拟机地址空间内的虚拟机物理地

址（Guest Physical Address，GPA），而加密硬件处理的虚拟机数据对应的是内存地址空间的主机物理地址（Host Physical Address，HPA），加密硬件需要根据主机物理地址在内存中查找到对应数据。因此，在加密硬件获取虚拟机的计算命令前，需要得到虚拟机地址空间的虚拟机物理地址到内存地址空间的主机物理地址的映射关系，而该映射关系主要通过输入输出（I/O）页表进行记录。

需要说明的是，本公开实施例中的模拟设备可以维护，记录有虚拟机地址空间的虚拟机物理地址，到内存地址空间的主机物理地址的映射关系的I/O 页表。从而，可以通过所述第一模拟设备响应所述使用请求，以使得第一虚拟机使用所述加密硬件。

在一个可选实现中，第一模拟设备对第一虚拟机的使用请求的响应可以是将第一虚拟机的 I/O 页表设置给输入输出内存管理单元（I/O Memory Management Unit，IOMMU），使得加密硬件能够获取虚拟机发送的计算命令。其中，所述计算命令可以携带虚拟机物理地址，加密硬件在获取所述计算命令后，通过 IOMMU，能够将所述计算命令中的虚拟机物理地址翻译成主机物理地址，在内存中得到对应目标数据进行计算。

其中，图 8 示例性的示出了本公开实施例中虚拟机访问加密硬件的交互示意图。如图 8 所示，虚拟机 01 和 02 分别通过对应的模拟设备 01'和 02'，访问共享内存空间中记录的加密硬件的设备状态；当模拟设备 01'在共享内存空间中获取加密硬件的设备状态为“空闲状态”时，将共享内存空间中记录的加密硬件设备状态调整为“忙碌状态”并使用加密硬件，模拟设备 02'需等待加密硬件的执行完成。进而，虚拟机 01 通过模拟设备 01'对共享内存空间中记录的设备状态调整，能够实现对加密硬件的使用；模拟设备 01'将 I/O 页表设置至 IOMMU，加密硬件基于 IOMMU 将虚拟机物理地址翻译成主机物理地址，在内存中得到对应的数据，并进行计算。

可以看出，本公开实施例通过多个模拟设备对加密硬件的设备状态维护，从而多个虚拟机能够共享加密硬件，进而基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理虚拟机对所述加密硬件的使用请求，保障加密硬件在一个时刻被一个虚拟机使用，实现多个虚拟机共享加密硬件进行数据的密码计算处理，提升虚拟机对于加密硬件的利用率，提高虚拟机的数据

处理性能。

在一些实施例中，基于虚拟机不再直接访问加密硬件，而是访问对应的模拟设备，则虚拟机对加密硬件的使用可以通过对应的模拟设备实现。以多个虚拟机中的任一个虚拟机（例如：第一虚拟机）为例，在第一虚拟机得到对应的第一模拟设备查询到加密硬件的设备状态为空闲状态后，第一虚拟机能够向对应的第一模拟设备发送请求使用所述加密硬件的使用请求，进而能够通过第一虚拟机对应的第一模拟设备，获取第一虚拟机请求使用所述加密硬件的使用请求，并且，通过所述第一模拟设备响应所述使用请求，以使得第一虚拟机使用所述加密硬件。

进一步的，在一些实施例中，基于模拟设备对所绑定的加密硬件的设备状态的维护，当第一虚拟机使用加密硬件时，可以通过所述第一虚拟机对应的第一模拟设备，将所述加密硬件的设备状态调整为忙碌状态，以使得第二虚拟机停止发送使用请求，直至所述加密硬件的设备状态调整为空闲状态。其中，所述第二虚拟机可以为所述多个虚拟机中不同于所述第一虚拟机的虚拟机。

可以理解的是，第一模拟设备在响应第一虚拟机对加密硬件的使用请求后，第一虚拟机能够使用加密硬件进行数据的密码计算处理，为避免其他虚拟机同时使用加密硬件，而造成加密硬件的硬件资源冲突，可以通过第一模拟设备将处于空闲状态的加密硬件的设备状态调整为忙碌状态。进而，在第一虚拟机使用所述加密硬件时，其他虚拟机对应的模拟设备查询到的加密硬件的设备状态为忙碌状态，使得其他虚拟机停止向对应的模拟设备发送所述加密硬件的使用请求，直至第一虚拟机使用完毕。在第一虚拟机对加密硬件使用完毕时，可以通过第一虚拟机对应的第一模拟设备将所述加密硬件的设备状态调整为空闲状态，其他虚拟机在通过对应模拟设备查询到加密硬件为空闲状态时，才可以向对应的模拟设备发送对所述加密硬件的使用请求，从而在保障加密硬件在一个时刻被一个虚拟机使用的情况下，通过任一虚拟机在加密硬件为空闲状态时，使用加密硬件的方式，来实现多个虚拟机共享加密硬件进行数据的密码计算处理。

在一些实施例中，通过多个模拟设备对所绑定的加密硬件的设备状态的读写，多个模拟设备所绑定的加密硬件的设备状态的维护可以基于共享内存

空间实现。在共享内存空间中可以记录多个模拟设备所绑定的加密硬件的设备状态，从而多个虚拟机可以通过对应的模拟设备对共享内存空间的访问，共享加密硬件的设备状态，进而实现共享加密硬件，进行数据的密码计算处理。

基于所述共享内存空间，作为一种可选实现，通过第一虚拟机对应的第一模拟设备，将所述加密硬件的设备状态调整为忙碌状态可以是通过第一虚拟机对应的第一模拟设备，将所述共享内存空间中记录的加密硬件的设备状态，调整为忙碌状态，从而其他虚拟机能够停止发送对加密硬件的使用请求，避免其它虚拟机对加密硬件的无效使用请求的发送和资源冲突。

作为另一种可选实现，在第一虚拟机结束使用加密硬件时，通过所述第一虚拟机对应的第一模拟设备，可以将所述共享内存空间中记录的加密硬件的设备状态，调整为空闲状态，使得其他虚拟机能够发送对加密硬件的使用请求，利用加密硬件执行数据的密码计算处理。

在一些实施例中，为实现多个虚拟机对加密硬件的使用，需要将多个虚拟机的虚拟机物理地址映射至加密硬件的寄存器空间，因此，需要建立虚拟机在加密硬件的地址空间中的映射关系。其中，图 9 示例性的示出了本公开实施例中加密硬件的配置方法的另一可选流程图。如图 9 所示，在步骤 S21 之前，还可以包括:

步骤 S20，在虚拟机启动时，通过虚拟机对应的模拟设备，为虚拟机映射加密硬件的寄存器地址空间。

可以理解的是，基于虚拟机不再直接访问密码协处理器，而是访问模拟设备，则可以通过虚拟机对应的模拟设备，为虚拟机映射加密硬件的寄存器地址空间。并且，由于模拟设备是虚拟机监视器在虚拟机启动时创建，则通过虚拟机对应的模拟设备，为虚拟机映射加密硬件的寄存器地址空间的时机也可以发生在虚拟机启动时，即在虚拟机启动时，通过虚拟机对应的模拟设备，为虚拟机映射加密硬件的寄存器地址空间。

作为一种可选实现，基于虚拟机不再直接访问加密硬件，而是访问模拟设备，虚拟机可以在启动时，向模拟设备发送加密硬件的寄存器地址查询请求，即，在虚拟机启动时，通过虚拟机对应的模拟设备，获取虚拟机对于加密硬件的寄存器地址空间的查询请求。进而，通过对应的模拟设备查询所述

寄存器地址空间的地址信息，以及，根据查询的所述寄存器地址空间的地址信息，为虚拟机映射加密硬件的寄存器地址空间。

进一步的在一个示例中，根据查询的所述寄存器地址空间的地址信息，为虚拟机映射加密硬件的寄存器地址空间，可以是根据所述寄存器地址空间的地址信息建立嵌套页表，所述嵌套页表用于记录虚拟机的虚拟机物理地址到密码协处理器的地址空间的映射。

需要说明的是，一虚拟机通过对应的模拟设备创建嵌套页表，以在虚拟机使用所述加密硬件前，根据所述嵌套页表，得到虚拟机物理地址在加密硬件的地址空间内对应的物理地址，进而虚拟机通过模拟设备能够在共享内存空间中查询加密硬件对应的设备状态，并使用加密硬件。其中，图 10 示例性的示出了虚拟机访问加密硬件的地址映射示意图。如图 10 所示，虚拟机监视器创建嵌套页表，将虚拟机的虚拟机物理地址映射到加密硬件的寄存器空间，从而虚拟机可以利用嵌套页表，查询虚拟机物理地址在加密硬件的寄存器空间中的物理地址，从而实现对加密硬件的访问。

基于创建的嵌套页表，图 11 示例性的示出了虚拟机通过模拟设备同步访问共享内存空间的交互示意图。如图 11 所示，虚拟机 01 和 02 分别查询对应的嵌套页表中记录的虚拟机的虚拟机物理地址到加密硬件的地址空间的映射关系，从而向对应的模拟设备 01'和 02'发送设备状态查询请求；通过对应的模拟设备 01'和 02'，在共享内存空间中查询加密硬件的设备状态；当对应的模拟设备 01'或 02'查询到加密硬件的当前设备状态为"空闲状态"时，根据对应的嵌套页表 01"或 02"中记录的虚拟机的虚拟机物理地址到加密硬件的地址空间的映射关系，通过对应的模拟设备 01'或 02'将共享内存空间中的设备状态调整为“忙碌状态”，从而对应的虚拟机 01 或 02 能够使用加密硬件。

在一些实施例中，虚拟机使用加密硬件执行数据的计算时，加密硬件需要通过输入输出内存管理单元获取虚拟机的虚拟机物理地址对应的主机物理地址。因此，基于输入输出页表可以记录虚拟机的虚拟机物理地址到主机物理地址的映射关系，可以通过所述第一模拟设备将第一虚拟机的输入输出页表，写入输入输出内存管理单元，所述输入输出页表记录有虚拟机物理地址到主机物理地址的地址映射关系，以使得第一虚拟机在使用密码协处理器

进行计算时，根据所述输入输出页表，查询到主机物理地址，从而在内存中获取待处理的目标数据，并进行计算，将计算结果返回至第一虚拟机。

需要说明的是，虚拟机监视器可以开启 IOMMU 功能，为加密硬件建立 I/O 页表，提供虚拟机物理地址到主机物理地址的映射关系，从而加密硬件能够通过 I/O 页表访问主机物理内存。其中，图 12 示例性的示出了加密硬件访问内存的地址转换示意图。如图 12 所示，在虚拟机使用加密硬件启动计算时，由于加密硬件能够获取虚拟机发送的数据的虚拟机物理地址（GPA），从而加密硬件能够通过 IOMMU 查询 I/O 页表，将 GPA 翻译成主机物理地址(HPA)，并访问内存数据。

为便于理解上述内容，图 13 示例性的示出了本公开实施例提供的多个虚拟机共享加密硬件的计算时序图。如图 13 所示，虚拟机启动时，执行步骤 S310，向模拟设备发送对加密硬件的寄存器地址空间的查询请求；模拟设备获取虚拟机的查询请求，进而执行步骤 S311，模拟设备向加密硬件查询寄存器地址空间，在一可选示例中，模拟设备在查询到加密硬件的寄存器地址空间后，可以向虚拟机反馈地址信息，以使虚拟机得到加密硬件的寄存器地址空间；模拟设备执行步骤 S312，为虚拟机映射加密硬件的寄存器地址空间，完成虚拟机与加密硬件的寄存器地址空间的映射。在虚拟机运行时，虚拟机执行步骤 S313，虚拟机向模拟设备查询加密硬件的设备状态；模拟设备获取该查询请求，执行步骤 S314，模拟设备在共享内存空间中查询并调整加密硬件的设备状态，在一可选示例中，模拟设备在查询到加密硬件的设备状态后，能够向虚拟机反馈加密硬件的设备状态（图中虚线箭头所示步骤）；当模拟设备查询到加密硬件的设备状态为空闲状态时，模拟设备执行步骤 S315，向 IOMMU 设置记录有 GPA 到 HPA 的映射关系的 I/O 页表，使得虚拟机能够执行步骤 S316，向加密硬件发送计算命令，其中计算命令中携带 GPA；加密硬件获取所述计算命令，并执行步骤 S317，向 IOMMU 查询 GPA 对应的 HPA；基于对应的 HPA，能够执行步骤 S318，向内存请求目标数据；进而执行步骤 S319，内存向加密硬件返回对应 HPA 的目标数据；加密硬件获取目标数据，并执行步骤 S320，对目标数据进行计算处理；进而在得到计算结果后，执行步骤 S321，加密硬件向虚拟机发送计算结果。

在一些实施例中，基于图 2 所示计算机系统架构的普通计算环境和机密

计算环境，所述加密硬件可以包括普通密码协处理器和/或安全密码协处理器。其中，所述普通密码协处理器用于执行在普通计算环境下的普通计算任务；所述安全密码协处理器用于执行在机密计算环境下的机密计算任务。

作为一种可选实现，所述普通计算环境可以与所述机密计算环境相隔离，所述普通计算环境用于执行普通计算任务，所述机密计算环境用于执行机密计算任务。

需要说明的是，本公开实施例的加密硬件的配置方法适用于普通密码协处理器，也适用于机密计算环境下具有一个或多个安全密码协处理器的情况；其中，在适用安全密码协处理器时，基于数据的安全性，需要通过安全处理器向安全密码协处理器进行消息的转达。

可以看出，本公开实施例通过多个模拟设备对加密硬件的设备状态维护，从而多个虚拟机能够共享加密硬件，在加密硬件为空闲状态时，多个虚拟机中的任一个虚拟机能够使用加密硬件进行计算处理，进而基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理虚拟机对所述加密硬件的使用请求，保障密码协处理器在一个时刻被一个虚拟机使用，实现多个虚拟机共享加密硬件进行数据的密码计算处理，提升虚拟机对于加密硬件的利用率，提高虚拟机的数据处理性能。

下面对本公开实施例提供的加密硬件的配置装置进行介绍，下文描述的装置内容可以认为是虚拟机监视器为实现本公开实施例提供的加密硬件的配置方法，所需设置的功能模块。下文描述的内容可与上文描述内容相互对应参照。

作为可选实现，图 14 示例性的示出了本公开实施例提供的加密硬件的配置装置的可选框图，该装置可应用于虚拟机监视器，参照图 14，该装置可以包括：状态维护逻辑 101 和请求处理逻辑 102。

其中，所述状态维护逻辑 101，用于维护多个模拟设备所绑定的加密硬件的设备状态，所述设备状态包括空闲状态和忙碌状态；其中，一个模拟设备对应一个虚拟机，并且多个模拟设备与加密硬件相绑定，以使得多个虚拟机通过对应的模拟设备共享加密硬件；

所述请求处理逻辑 102，用于基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理所述虚拟机对所述加密硬件的使用请求，以使得虚

拟机使用所述加密硬件，所述虚拟机为多个虚拟机中的任一个虚拟机。

可选的，所述请求处理逻辑 102，用于基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理所述虚拟机对所述加密硬件的使用请求的步骤包括:

如果所述加密硬件的设备状态为空闲状态，通过第一虚拟机对应的第一模拟设备，获取第一虚拟机请求使用所述加密硬件的使用请求；所述第一虚拟机为多个虚拟机中的任一个虚拟机;

通过所述第一模拟设备响应所述使用请求，以使得所述第一虚拟机使用所述加密硬件。

可选的，还包括：通过所述第一模拟设备，将所述加密硬件的设备状态调整为忙碌状态，以使得第二虚拟机停止发送使用请求，直至所述加密硬件的设备状态调整为空闲状态；其中，所述第二虚拟机为所述多个虚拟机中不同于第一虚拟机的虚拟机。

具体的，所述状态维护逻辑 101 用于执行前述的加密硬件的配置方法。

进一步的，对应前述的加密硬件的配置方法，加密硬件的配置装置还可进一步设置地址映射逻辑 100，用于在虚拟机启动时，通过虚拟机对应的模拟设备，为虚拟机映射加密硬件的寄存器地址空间。

可选的，所述状态维护逻辑 101 中，维护多个模拟设备所绑定的加密硬件的设备状态的步骤包括:

在共享内存空间中记录多个模拟设备所绑定的加密硬件的设备状态，所述共享内存空间配置为允许所述多个模拟设备进行读写。

可选的，所述状态维护逻辑 101，通过第一虚拟机对应的第一模拟设备，将加密硬件的设备状态调整为忙碌状态的步骤包括:

通过所述第一虚拟机对应的第一模拟设备，将所述共享内存空间中记录的加密硬件的设备状态，调整为忙碌状态。

可选的，所述状态维护逻辑 101，还用于在所述第一虚拟机结束使用加密硬件时，通过所述第一虚拟机对应的第一模拟设备，将所述共享内存空间中记录的加密硬件的设备状态，调整为空闲状态。

可选的，所述地址映射逻辑 100，用于在虚拟机启动时，通过虚拟机对应的模拟设备，为虚拟机映射加密硬件的寄存器地址空间的步骤可以包括;

通在虚拟机启动时，通过虚拟机对应的模拟设备，获取虚拟机对于加密硬件的寄存器地址空间的查询请求；

通过虚拟机对应的模拟设备查询所述寄存器地址空间的地址信息，以及，根据查询的所述寄存器地址空间的地址信息，为虚拟机映射加密硬件的寄存器地址空间。

可选的，所述根据查询的所述寄存器地址空间的地址信息，为虚拟机映射加密硬件的寄存器地址空间的步骤可以包括：

根据所述寄存器地址空间的地址信息建立嵌套页表，所述嵌套页表用于记录虚拟机的虚拟机物理地址到加密硬件的地址空间的映射。

可选的，所述状态维护逻辑 101，通过所述第一模拟设备响应所述使用请求，以使得所述第一虚拟机使用所述加密硬件的步骤可以包括：

通过所述第一模拟设备将所述第一虚拟机的输入输出页表，写入输入输出内存管理单元，所述输入输出页表记录有虚拟机物理地址到主机物理地址的地址映射关系。

本公开实施例在机密计算环境下，还提出一种数据机密计算方法，其中，该机密计算环境下的安全密码协处理器可以是根据上述所述加密硬件的配置方法配置得到的加密硬件，出于本公开的技术思路，图 15 示出了本公开实施例提供的数据机密计算方法的可选流程图，该方法流程可由虚拟机监视器实现。如图 15 所示，该方法流程可以包括如下步骤。

步骤 S41，获取虚拟机发送的对于模拟设备的机密计算命令。

本公开实施例中的虚拟机监视器增加了一层模拟设备层，通过模拟设备层创建用于模拟安全密码协处理器对应配置的模拟设备，所述安全密码协处理器可以是根据前述加密硬件的配置方法配置得到的加密硬件。从而，虚拟机能够将机密计算命令直接发送至模拟设备，避免采用直通的方式，将安全密码协处理器直通给虚拟机，则虚拟机监视器能够获取虚拟机发送的对于模拟设备的机密计算命令。

所述机密计算命令用于指示安全密码协处理器对数据进行机密计算。

步骤 S42，获取安全密码协处理器的使用权限，以使得根据所述机密计算命令，得到所述安全密码协处理器的机密计算结果，并将所述机密计算结果返回至虚拟机。

本公开实施例中，不同虚拟机的虚拟机监视器可以同步协商对安全密码协处理器的使用。在一个示例中，虚拟机监视器具有内存空间，虚拟机监视器的同步可以是一虚拟机监视器对应查找另一虚拟机监视器的内存空间中，记录的安全密码协处理器的设备状态标志位，若所述设备状态标志位指示未使用安全密码协处理器，则安全密码协处理器当前为空闲状态，从而能够获取安全密码协处理器的使用权限，则虚拟机监视器能够向安全密码协处理器发送用于进行机密计算的机密计算命令；安全密码协处理器在获得用于进行机密计算的机密计算命令后，能够对数据进行机密计算，并将机密计算结果发送至虚拟机监视器，从而虚拟机监视器能够得到所述安全密码协处理器的机密计算结果，并将所述机密计算结果返回至虚拟机，完成虚拟机的机密计算。

可以看出，本公开实施例的数据机密计算方法能够实现多个虚拟机对安全密码协处理器的使用，提升了虚拟机对于安全密码协处理器的利用率，提高了虚拟机的数据处理性能。

在一些实施例中，基于不同虚拟机的虚拟机监视器可以同步协商对安全密码协处理器的使用，以及模拟设备模拟安全密码协处理器的配置，则可以通过访问不同的模拟设备对应安全密码协处理器的设备状态，在不同的模拟设备对应安全密码协处理器的设备状态均为空闲状态时，获取安全密码协处理器的使用权限，并将对应的模拟设备模拟的安全密码协处理器的设备状态，调整为忙碌状态，从而获取安全密码协处理器的使用权限，避免采用直通的方式，将安全密码协处理器直通给多个虚拟机中的任一个虚拟机。

需要说明的是，不同的模拟设备对应的安全密码协处理器可以是唯一的，即安全密码协处理器的数量是 1。从而，当不同的模拟设备对应安全密码协处理器的设备状态均为空闲状态时，当前安全密码协处理器未使用，可以获取安全密码协处理器的使用权限。

在一些实施例中，虚拟机发送的机密计算命令中可以携带有命令 ID 和命令地址参数，所述命令 ID 对应于需执行的机密计算类型，例如：加密运算、解密运算、哈希运算等；所述命令地址参数可以包括数据的虚拟机物理地址（GPA）。

需要说明的是，在机密计算环境下，安全密码协处理器能够访问机密资

源，例如：虚拟机的密文、安全存储（用于存储高度机密的密钥）。但是，在访问内存时，安全处理器、安全密码协处理器并不使用 IOMMU 进行地址翻译，只处理对应于内存地址空间的主机物理地址（HPA）。因此，需要将机密计算命令中命令地址参数的虚拟机物理地址转换为主机物理地址。

命令地址参数中包括虚拟机物理地址，为获取进行机密计算的目标数据，需要得到数据对应于内存地址空间的主机物理地址。作为一种可选实现，虚拟机监视器在通过模拟设备获取机密计算命令后，能够根据所述机密计算命令，将虚拟机物理地址转换为主机物理地址，从而得到处理后的机密计算命令，以在内存中获取待计算的目标数据。进而，虚拟机监视器能够向安全密码协处理器发送所述处理后的机密计算命令，并获取安全密码协处理器的机密计算结果。

在一些实施例中，虚拟机监视器可以创建嵌套页表，所述嵌套页表可以记录有虚拟机物理地址到主机物理地址的地址映射关系，从而根据所述机密计算命令，将所述虚拟机物理地址转换为主机物理地址，可以具体为，根据所述命令地址参数，查询嵌套页表，将所述虚拟机物理地址转换为主机物理地址。

需要说明的是，在一个可选示例中，嵌套页表可以记录虚拟机物理地址在加密硬件的寄存器空间中的地址映射关系，在另一个可选示例中，嵌套页表可以记录虚拟机物理地址在内存地址空间中的地址映射关系。本公开实施例中，基于安全处理器、安全密码协处理器不使用 IOMMU 做地址翻译，只处理主机物理地址（HPA）。因此，虚拟机监视器可以查询记录有虚拟机物理地址在内存地址空间中的地址映射关系的嵌套页表，从而将机密计算命令中命令地址参数的虚拟机物理地址转换为主机物理地址，该主机物理地址即虚拟机物理地址对应于内存地址空间的主机物理地址，以实现安全密码协处理器根据该主机物理地址在内存中获取数据并进行机密计算。其中，记录有虚拟机物理地址在内存地址空间中的地址映射关系的嵌套页表可以是通过安全处理器向内存发送地址查询命令，获取内存的地址空间；进而基于获取的内存地址空间，建立虚拟机物理地址与内存地址空间的主机物理地址映射关系。

需要进一步说明的是，基于虚拟机监视器通过模拟设备模拟安全密码协

处理器的配置，虚拟机向模拟设备发送机密计算命令，并且，通过虚拟机监视器得到返回的机密计算结果后，能够进入虚拟机退出模式。

其中，图 16 示例性的示出了本公开实施例中多个虚拟机访问安全密码协处理器的交互示意图。如图 16 所示，虚拟机 A 和 B 分别对应虚拟机监视器 a 和 b，并且，虚拟机监视器 a 的模拟设备层设置有模拟安全密码协处理器配置的模拟设备 A'，虚拟机监视器 b 的模拟设备层设置有模拟安全密码协处理器配置的模拟设备 B'；虚拟机监视器 a 对应查找嵌套页表 A"，虚拟机监视器 b 对应查找嵌套页表 B"。并且，虚拟机 A 和 B 可以是安全虚拟机。其中，嵌套页表 A"和嵌套页表 B"记录有对应虚拟机的虚拟机物理地址（GPA）到内存地址空间内的主机物理地址（HPA）的地址映射关系。

基于模拟设备 A'和 B'对安全密码协处理器的配置模拟，虚拟机 A 和 B 可以向对应的模拟设备 A'和 B'发送数据机密计算命令。进而，虚拟机监视器 a 和 b 能够获取对应的虚拟机对于模拟设备发送的数据机密计算命令，并查询对应的嵌套页表，将数据机密计算命令中的虚拟机物理地址转换为主机物理地址。进一步，虚拟机监视器 a 和 b 可以相互同步对安全密码协处理器的使用权限，例如：当虚拟机监视器 a 同步访问虚拟机监视器 b 时，得到虚拟机监视器 b 未使用安全密码协处理器的结果，则虚拟机监视器 a 将安全密码协处理器的设备状态记录为对应虚拟机 A 使用的“忙碌状态”；进而，虚拟机监视器 a 能够通过安全处理器向安全密码协处理器发送包含有主机物理地址的数据机密计算命令，使得安全密码协处理器能够根据主机物理地址在内存中获取目标数据，对目标数据进行机密计算，并将机密计算结果通过安全处理器发送给虚拟机监视器 a；最后，虚拟机监视器 a 向虚拟机 A 返回该机密计算结果。

可以看出，本公开实施例的数据机密计算方法能够实现多个虚拟机对安全密码协处理器的使用，提升了虚拟机对于安全密码协处理器的利用率，提高了虚拟机的数据处理性能。

在一些实施例中，由于机密计算环境下，安全密码协处理器处理的是机密计算任务，虚拟机需要对机密计算命令的传输进行验证，以确定信息交互的安全性。并且，基于数据的安全性考虑，需要通过安全处理器向安全密码协处理器进行消息的转达。在一个示例中，利用安全处理器可以进行密钥协

商生成密钥对，得到芯片私钥和芯片公钥，并且，安全处理器能够将芯片公钥传输给虚拟机，由虚拟机对芯片公钥进行保存。因此，作为一种可选实现，所述机密计算命令还可以携带签名文件，所述签名文件用于通过向安全密码协处理器转发所述机密计算命令的安全处理器，利用芯片私钥对所述签名文件进行签名，例如：安全处理器对所述签名文件利用芯片私钥进行加密，以使虚拟机利用与所述芯片私钥相匹配的芯片公钥，对所述机密计算结果中的签名文件进行验签，以确定机密计算命令为通过安全处理器转达至安全密码协处理器进行执行处理。

可以看出，本公开实施例的数据机密计算方法能够实现多个虚拟机对安全密码协处理器的使用，提升了虚拟机对于安全密码协处理器的利用率，提高了虚拟机的数据处理性能。

下面对本公开实施例提供的数据机密计算装置进行介绍，下文描述的装置内容可以认为是虚拟机对应的虚拟机监视器为实现本公开实施例提供的数据机密计算方法，所需设置的功能模块。下文描述的内容可与上文描述内容相互对应参照。

作为可选实现，图 17 示例性的示出了本公开实施例提供的数据机密计算装置的可选框图，该装置可应用于虚拟机监视器，参照图 17，该装置可以包括：命令获取逻辑 110 和硬件使用逻辑 120。

其中，所述命令获取逻辑 110，用于获取虚拟机发送的对于模拟设备的机密计算命令，模拟设备用于模拟安全密码协处理器的程序，所述安全密码协处理器为根据如上述的加密硬件的配置方法配置得到的加密硬件；

所述硬件使用逻辑 120，用于获取所述安全密码协处理器的使用权限，以使得根据所述机密计算命令，得到所述安全密码协处理器的机密计算结果，并将所述机密计算结果返回至虚拟机。

可选的，所述硬件使用逻辑 120 用于获取安全密码协处理器的使用权限的步骤，包括：

通过访问不同模拟设备模拟的安全密码协处理器的设备状态，在不同模拟设备模拟的安全密码协处理器的设备状态为空闲状态时，获取安全密码协处理器的使用权限，并将对应的模拟设备模拟的安全密码协处理器的设备状态，调整为忙碌状态。

可选的，所述机密计算命令携带有命令 ID 和命令地址参数，所述命令 ID 对应于需执行的机密计算类型，所述命令地址参数包括虚拟机物理地址；

所述硬件使用逻辑 120 中，根据所述机密计算命令，得到所述加密硬件的机密计算结果的步骤，包括：

根据所述机密计算命令，将所述虚拟机物理地址转换为主机物理地址，得到处理后的机密计算命令；

向安全密码协处理器发送所述处理后的机密计算命令，并获取安全密码协处理器的机密计算结果。

可选的，所述根据所述机密计算命令，将所述虚拟机物理地址转换为主机物理地址，可以具体为，根据所述命令地址参数，查询嵌套页表，将所述虚拟机物理地址转换为主机物理地址；所述嵌套页表记录有虚拟机物理地址到主机物理地址的地址映射关系。

本公开实施例还提供一种计算机系统，所述计算机系统可以包括：虚拟机监视器、多个虚拟机，以及加密硬件，所述虚拟机监视器包括如上述所述的加密硬件的配置装置，或者，如上述所述的数据机密计算装置。

可选的，所述虚拟机监视器设置有模拟设备层，所述模拟设备层设置有如上述加密硬件的配置方法中所述的模拟设备，或者，如上述所述数据机密计算方法中所述的模拟设备。

本公开实施例还提供一种电子设备，所述电子设备可以包括存储器和处理器，所述存储器上存储有可由所述处理器运行的计算机程序，所述处理器运行所述计算机程序时执行如上述所述的加密硬件的配置方法，或者，如上述所述的数据机密计算方法中的步骤。

本公开实施例还提供一种存储介质，所述存储介质存储一条或多条计算机可执行指令，所述一条或多条计算机可执行指令被执行时，实现如本公开实施例的加密硬件的配置方法和/或数据机密计算方法。

上文描述了本公开实施例提供的多个实施例方案，各实施例方案介绍的各可选方式可在不冲突的情况下相互结合、交叉引用，从而延伸出多种可能的实施例方案，这些均可认为是本公开实施例披露、公开的实施例方案。

虽然本公开实施例披露如上，但本公开并非限定于此。任何本领域技术人员，在不脱离本公开的精神和范围内，均可作各种更动与修改，因此本公

开的保护范围应当以权利要求所限定的范围为准。

权利要求书

1.一种加密硬件的配置方法，包括:

维护多个模拟设备所绑定的加密硬件的设备状态，所述设备状态包括空闲状态和忙碌状态；其中，一个模拟设备对应一个虚拟机，并且多个模拟设备与加密硬件相绑定，以使得多个虚拟机通过对应的模拟设备共享加密硬件；以及

基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理所述虚拟机对所述加密硬件的使用请求，以使得所述虚拟机使用所述加密硬件，所述虚拟机为所述多个虚拟机中的任一个虚拟机。

2.根据权利要求 1 所述的加密硬件的配置方法，其中，所述基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理所述虚拟机对所述加密硬件的使用请求，包括:

如果所述加密硬件的设备状态为空闲状态，通过第一虚拟机对应的第一模拟设备，获取所述第一虚拟机请求使用所述加密硬件的使用请求；所述第一虚拟机为所述多个虚拟机中的任一个虚拟机；以及

通过所述第一模拟设备响应所述使用请求，以使得所述第一虚拟机使用所述加密硬件。

3.根据权利要求 2 所述的加密硬件的配置方法，还包括:

通过所述第一模拟设备，将所述加密硬件的设备状态调整为忙碌状态，以使得第二虚拟机停止发送使用请求，直至所述加密硬件的设备状态调整为空闲状态；其中，所述第二虚拟机为所述多个虚拟机中，不同于所述第一虚拟机的虚拟机。

4.根据权利要求 1-3 任一项所述的加密硬件的配置方法，其中，所述维护多个模拟设备所绑定的加密硬件的设备状态包括:

在共享内存空间中记录多个模拟设备所绑定的加密硬件的设备状态，所述共享内存空间配置为允许所述多个模拟设备进行读写。

5.根据权利要求 4 所述的加密硬件的配置方法，其中，通过第一虚拟机对应的第一模拟设备，将所述加密硬件的设备状态调整为忙碌状态包括:

通过所述第一虚拟机对应的第一模拟设备，将所述共享内存空间中记录

的加密硬件的设备状态，调整为忙碌状态。

6.根据权利要求 5 所述的加密硬件的配置方法，还包括:

在所述第一虚拟机结束使用加密硬件时，通过所述第一虚拟机对应的第一模拟设备，将所述共享内存空间中记录的加密硬件的设备状态，调整为空闲状态。

7.根据权利要求 1-6 任一项所述的加密硬件的配置方法，还包括:

在所述虚拟机启动时，通过所述虚拟机对应的模拟设备，为所述虚拟机映射加密硬件的寄存器地址空间。

8.根据权利要求 7 所述的加密硬件的配置方法，其中，所述在所述虚拟机启动时，通过所述虚拟机对应的模拟设备，为所述虚拟机映射加密硬件的寄存器地址空间包括:

在所述虚拟机启动时，通过所述虚拟机对应的模拟设备，获取所述虚拟机对于加密硬件的寄存器地址空间的查询请求；以及

通过所述虚拟机对应的模拟设备查询所述寄存器地址空间的地址信息，以及，根据查询的所述寄存器地址空间的地址信息，为所述虚拟机映射加密硬件的寄存器地址空间。

9.根据权利要求 8 所述的加密硬件的配置方法，其中，所述根据查询的所述寄存器地址空间的地址信息，为所述虚拟机映射加密硬件的寄存器地址空间，包括:

根据所述寄存器地址空间的地址信息建立嵌套页表，所述嵌套页表被配置为记录所述虚拟机的虚拟机物理地址到加密硬件的地址空间的映射。

10.根据权利要求 2-6 任一项所述的加密硬件的配置方法，其中，所述通过所述第一模拟设备响应所述使用请求，以使得所述第一虚拟机使用所述加密硬件包括:

通过所述第一模拟设备将所述第一虚拟机的输入输出页表，写入输入输出内存管理单元，所述输入输出页表记录有虚拟机物理地址到主机物理地址的地址映射关系。

11.根据权利要求 1-10 任一项所述的加密硬件的配置方法，其中，所述加密硬件包括普通密码协处理器和/或安全密码协处理器；其中，所述普通密码协处理器被配置为执行在普通计算环境下的普通计算任务；所述安全密码

协处理器被配置为执行在机密计算环境下的机密计算任务。

12.根据权利要求 11 所述的加密硬件的配置方法，其中，所述普通计算环境与所述机密计算环境相隔离，所述普通计算环境被配置为执行普通计算任务，所述机密计算环境被配置为执行机密计算任务。

13.一种加密硬件的配置装置，包括:

状态维护逻辑，被配置为维护多个模拟设备所绑定的加密硬件的设备状态，所述设备状态包括空闲状态和忙碌状态；其中，一个模拟设备对应一个虚拟机，并且所述多个模拟设备与加密硬件相绑定，以使得多个虚拟机通过对应的模拟设备共享加密硬件；以及

请求处理逻辑，被配置为基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理所述虚拟机对所述加密硬件的使用请求，以使得所述虚拟机使用所述加密硬件，所述虚拟机为所述多个虚拟机中的任一个虚拟机。

14.根据权利要求 13 所述的加密硬件的配置装置，还包括:

地址映射逻辑，被配置为在所述虚拟机启动时，通过所述虚拟机对应的模拟设备，为所述虚拟机映射加密硬件的寄存器地址空间。

15.一种数据机密计算方法，包括:

获取虚拟机发送的对于模拟设备的机密计算命令，所述模拟设备被配置为模拟安全密码协处理器的配置，所述安全密码协处理器为根据如权利要求 1 所述的加密硬件的配置方法配置得到的加密硬件；以及

获取所述安全密码协处理器的使用权限，以使得根据所述机密计算命令，得到所述安全密码协处理器的机密计算结果，并将所述机密计算结果返回至所述虚拟机。

16.根据权利要求 15 所述的数据机密计算方法，其中，所述获取所述安全密码协处理器的使用权限，包括:

通过访问不同模拟设备模拟的安全密码协处理器的设备状态，在不同模拟设备模拟的安全密码协处理器的设备状态均为空闲状态时，获取安全密码协处理器的使用权限，并将对应的模拟设备模拟的安全密码协处理器的设备状态，调整为忙碌状态。

17.根据权利要求 15 或 16 所述的数据机密计算方法，其中，所述机密计算命令携带有命令 ID 和命令地址参数，所述命令 ID 对应于需执行的机密计

算类型，所述命令地址参数包括虚拟机物理地址；

所述根据所述机密计算命令，得到所述安全密码协处理器的机密计算结果，包括：

根据所述机密计算命令，将所述虚拟机物理地址转换为主机物理地址，得到处理后的机密计算命令；以及

向所述安全密码协处理器发送所述处理后的机密计算命令，并获取所述安全密码协处理器的机密计算结果。

18.根据权利要求 17 所述的数据机密计算方法，其中，所述根据所述机密计算命令，将所述虚拟机物理地址转换为主机物理地址，包括：根据所述命令地址参数，查询嵌套页表，将所述虚拟机物理地址转换为所述主机物理地址；所述嵌套页表记录有所述虚拟机物理地址到所述主机物理地址的地址映射关系。

19.根据权利要求 17 或 18 所述的数据机密计算方法，其中，所述机密计算命令还携带签名文件，所述签名文件被配置为通过向所述安全密码协处理器转发所述机密计算命令的安全处理器，利用芯片私钥对所述签名文件进行签名，以使虚拟机利用与所述芯片私钥相匹配的芯片公钥，对所述机密计算结果中的签名文件进行验签。

20.一种数据机密计算装置，包括：

命令获取逻辑，被配置为获取虚拟机发送的对于模拟设备的机密计算命令，模拟设备被配置为模拟安全密码协处理器的程序，所述安全密码协处理器为根据如权利要求 1 所述的加密硬件的配置方法配置得到的加密硬件；以及

硬件使用逻辑，被配置为获取所述安全密码协处理器的使用权限，以使得根据所述机密计算命令，得到所述安全密码协处理器的机密计算结果，并将所述机密计算结果返回至所述虚拟机。

21.一种计算机系统，包括：虚拟机监视器、多个虚拟机，以及加密硬件，所述虚拟机监视器包括如权利要求 13 至 14 任一项所述的加密硬件的配置装置，或者，如权利要求 20 所述的数据机密计算装置。

22.根据权利要求 21 所述的计算机系统，其中，所述虚拟机监视器设置有模拟设备层，所述模拟设备层设置有如权利要求 1 至 12 任一项所述的加

密硬件的配置方法中的模拟设备，或者，如权利要求 15 至 19 任一项所述的数据机密计算方法中的模拟设备。

23.一种电子设备，包括存储器和处理器，所述存储器上存储有可由所述处理器运行的计算机程序，所述处理器运行所述计算机程序时执行如权利要求 1 至 12 任一项所述的加密硬件的配置方法，或者，如权利要求 15 至 19 任一项所述的数据机密计算方法中的步骤。

24.一种存储介质，其中，所述存储介质存储一条或多条计算机可执行指令，所述一条或多条计算机可执行指令被执行时，实现如权利要求 1 至 12 任一项所述的加密硬件的配置方法，和/或，如权利要求 15 至 19 任一项所述的数据机密计算方法。

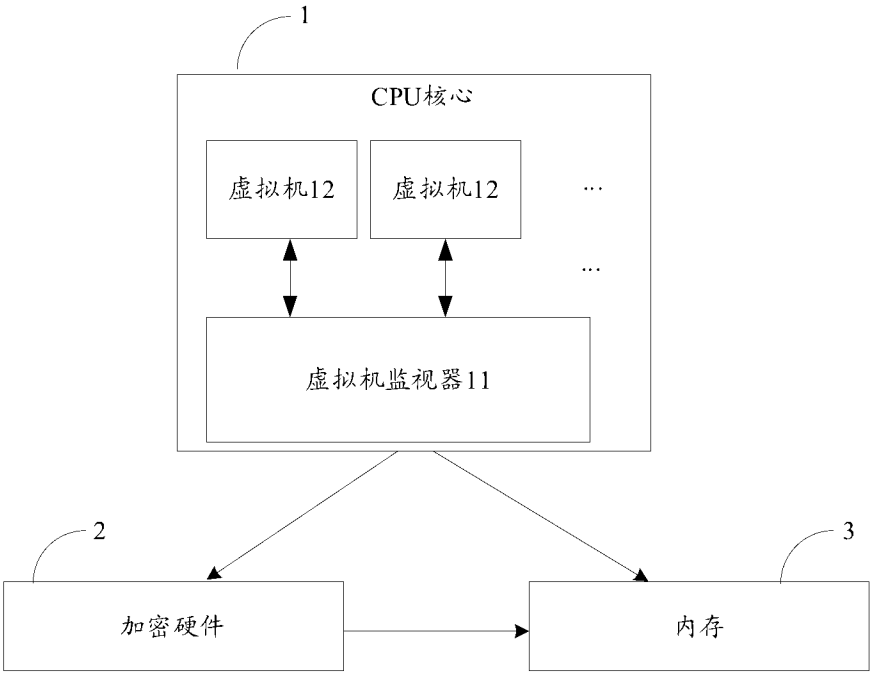

图 1

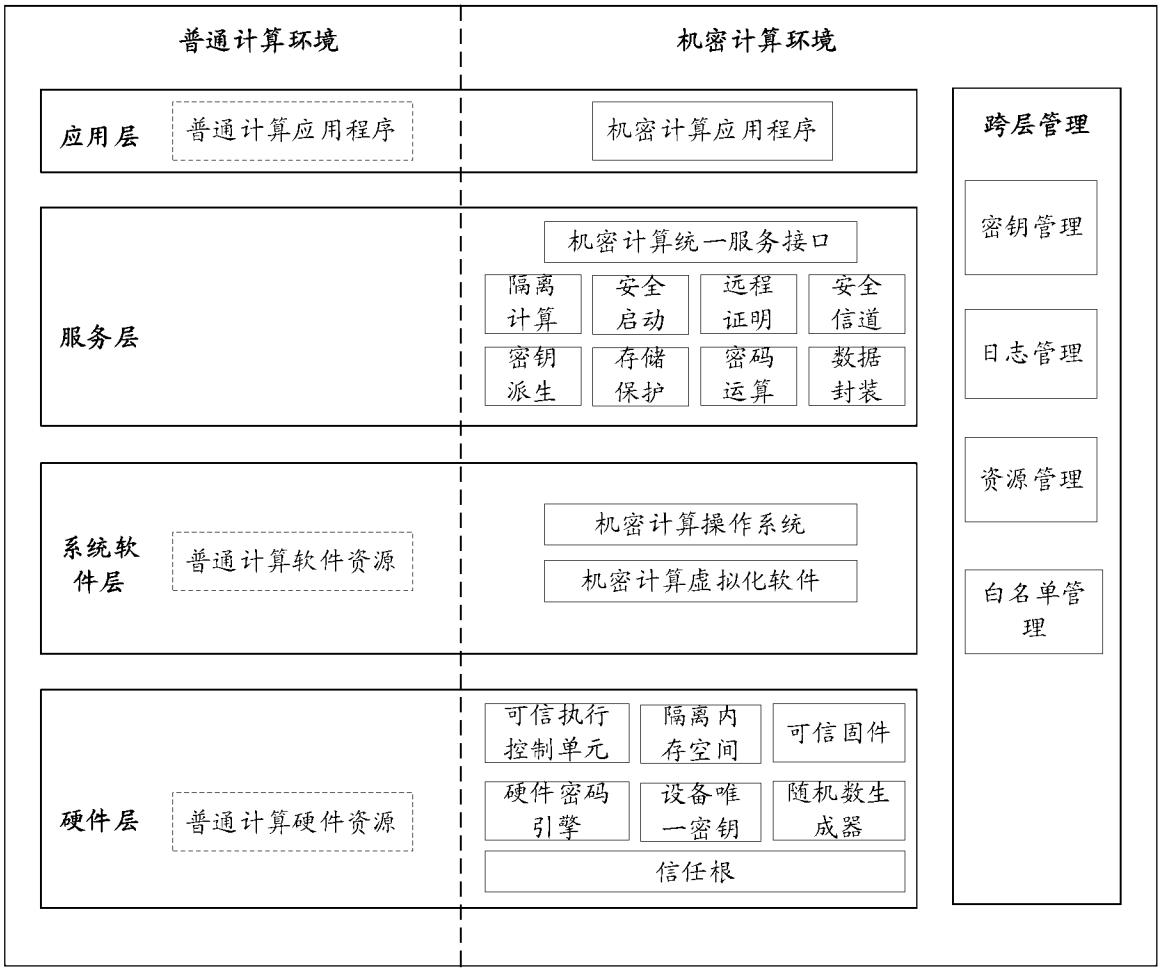
普通计算环境
机密计算环境
应用层
普通计算应用程序
机密计算应用程序
跨层管理
密钥管理
日志管理
资源管理
白名单管理
服务层
机密计算统一服务接口
隔离计算
安全启动
远程证明
安全信道
密钥派生
存储保护
密码运算
数据封装
系统软件层
普通计算软件资源
机密计算操作系统
机密计算虚拟化软件
硬件层
普通计算硬件资源
可信执行控制单元
隔离内存空间
可信固件
硬件密码引擎
设备唯一密钥
随机数生成器
信任根

图 2

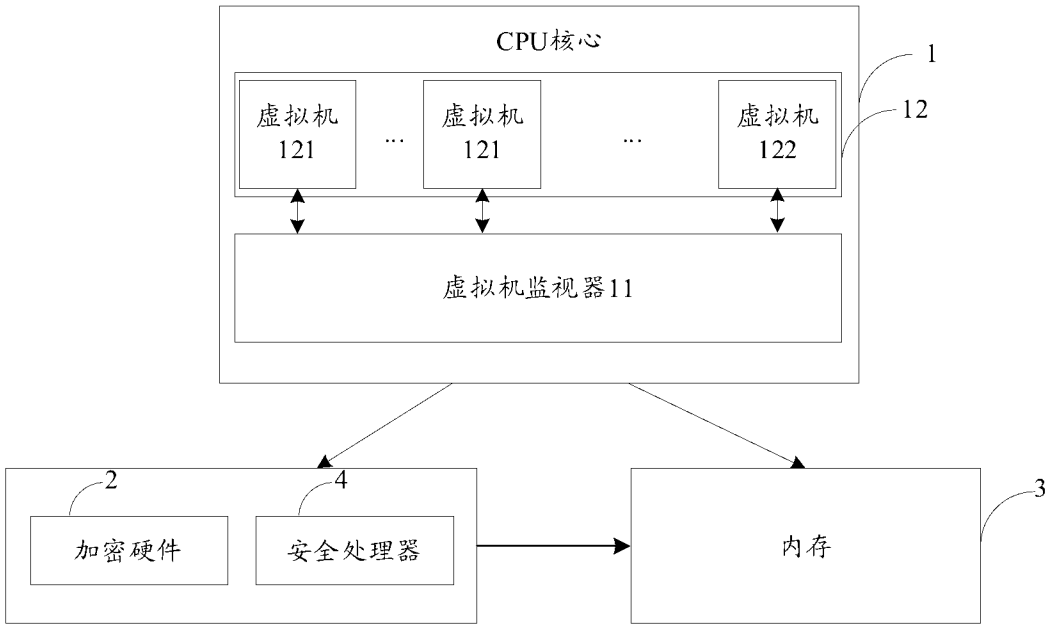
CPU核心
1
12
虚拟机
121
虚拟机
121
虚拟机
122
虚拟机监视器11
2
4
加密硬件
安全处理器
内存
3

图 3

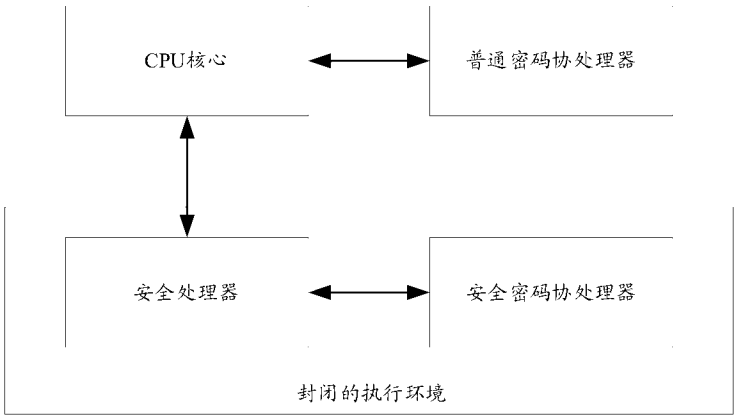
CPU核心
普通密码协处理器
安全处理器
安全密码协处理器
封闭的执行环境

图 4

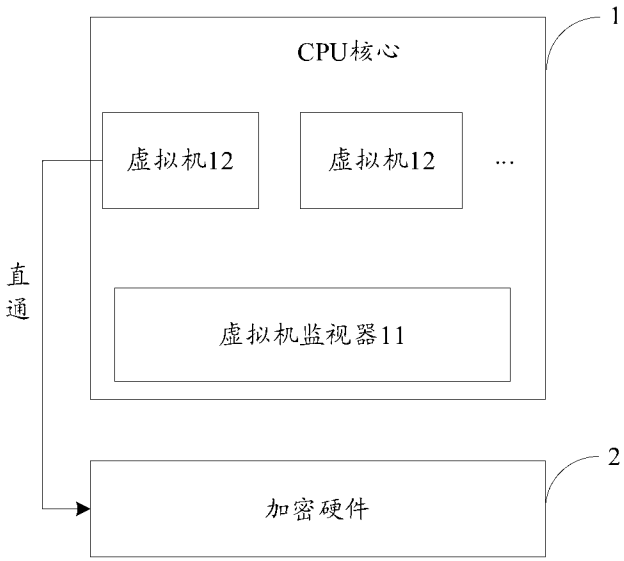
CPU核心
1
虚拟机12
虚拟机12
…
直通
虚拟机监视器11
加密硬件
2

图 5

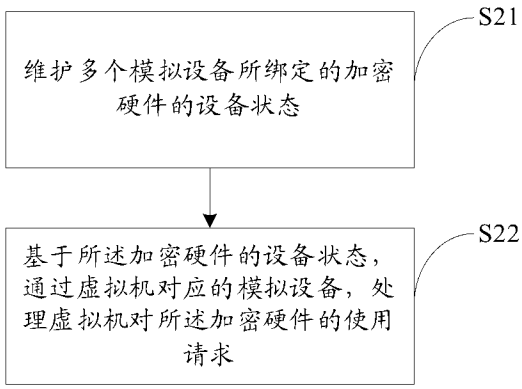
维护多个模拟设备所绑定的加密硬件的设备状态
S21
基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理虚拟机对所述加密硬件的使用请求
S22

图 6

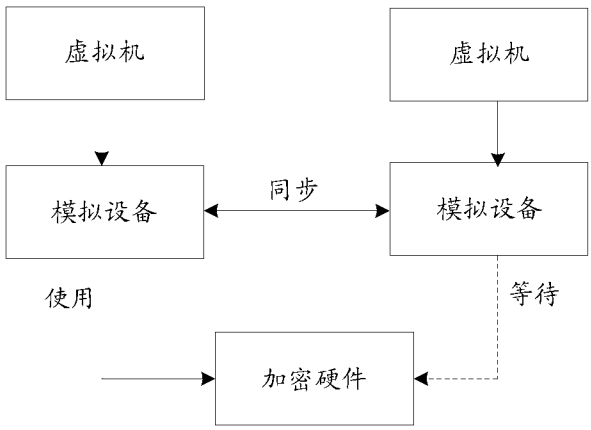
虚拟机
虚拟机
模拟设备
同步
模拟设备
使用
等待
加密硬件

图 7

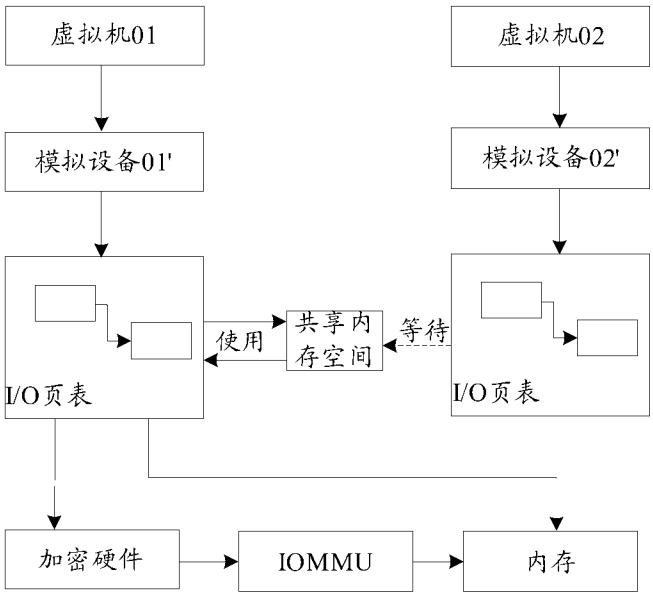
虚拟机01
虚拟机02
模拟设备01'
模拟设备02'
使用
共享内存空间
等待
I/O页表
I/O页表
加密硬件
IOMMU
内存

图 8

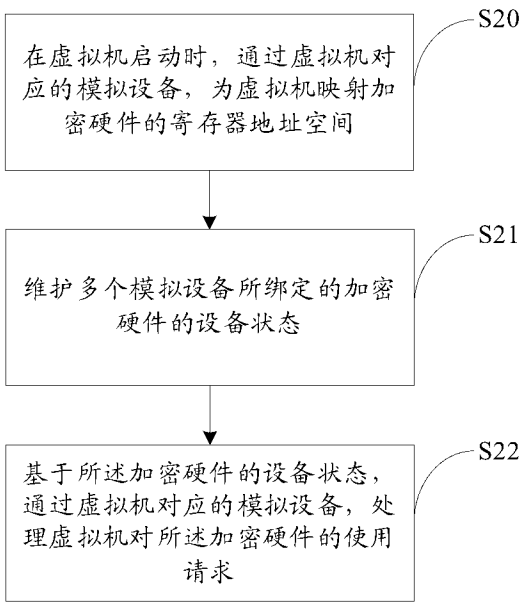
在虚拟机启动时，通过虚拟机对应的模拟设备，为虚拟机映射加密硬件的寄存器地址空间
S20
维护多个模拟设备所绑定的加密硬件的设备状态
S21
基于所述加密硬件的设备状态，通过虚拟机对应的模拟设备，处理虚拟机对所述加密硬件的使用请求
S22

图 9

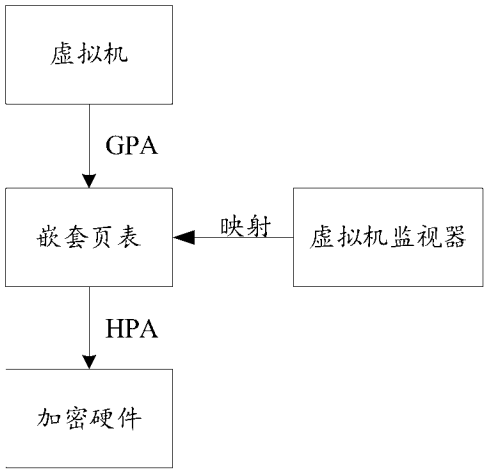
虚拟机
GPA
嵌套页表
映射
虚拟机监视器
HPA
加密硬件

图 10

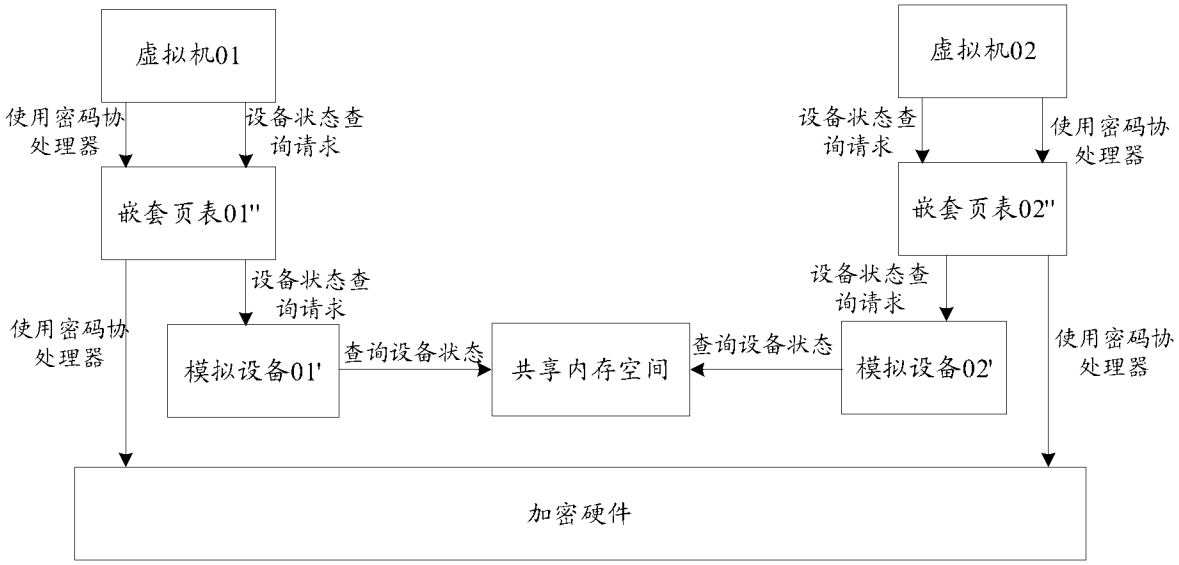
虚拟机01
使用密码协处理器
设备状态查询请求
嵌套页表01''
设备状态查询请求
使用密码协处理器
模拟设备01'
查询设备状态
共享内存空间
查询设备状态
模拟设备02'
虚拟机02
设备状态查询请求
使用密码协处理器
嵌套页表02''
设备状态查询请求
使用密码协处理器
加密硬件

图 11

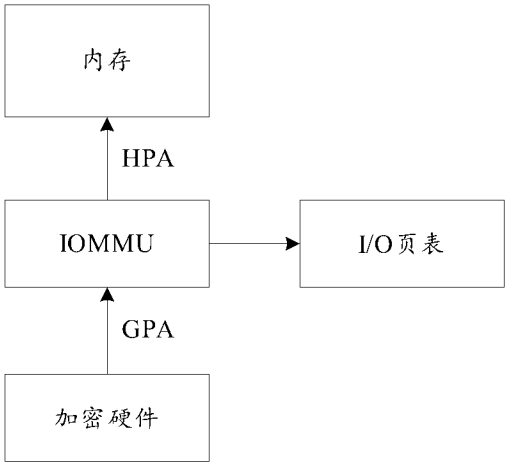
内存
HPA
IOMMU
I/O页表
GPA
加密硬件

图 12

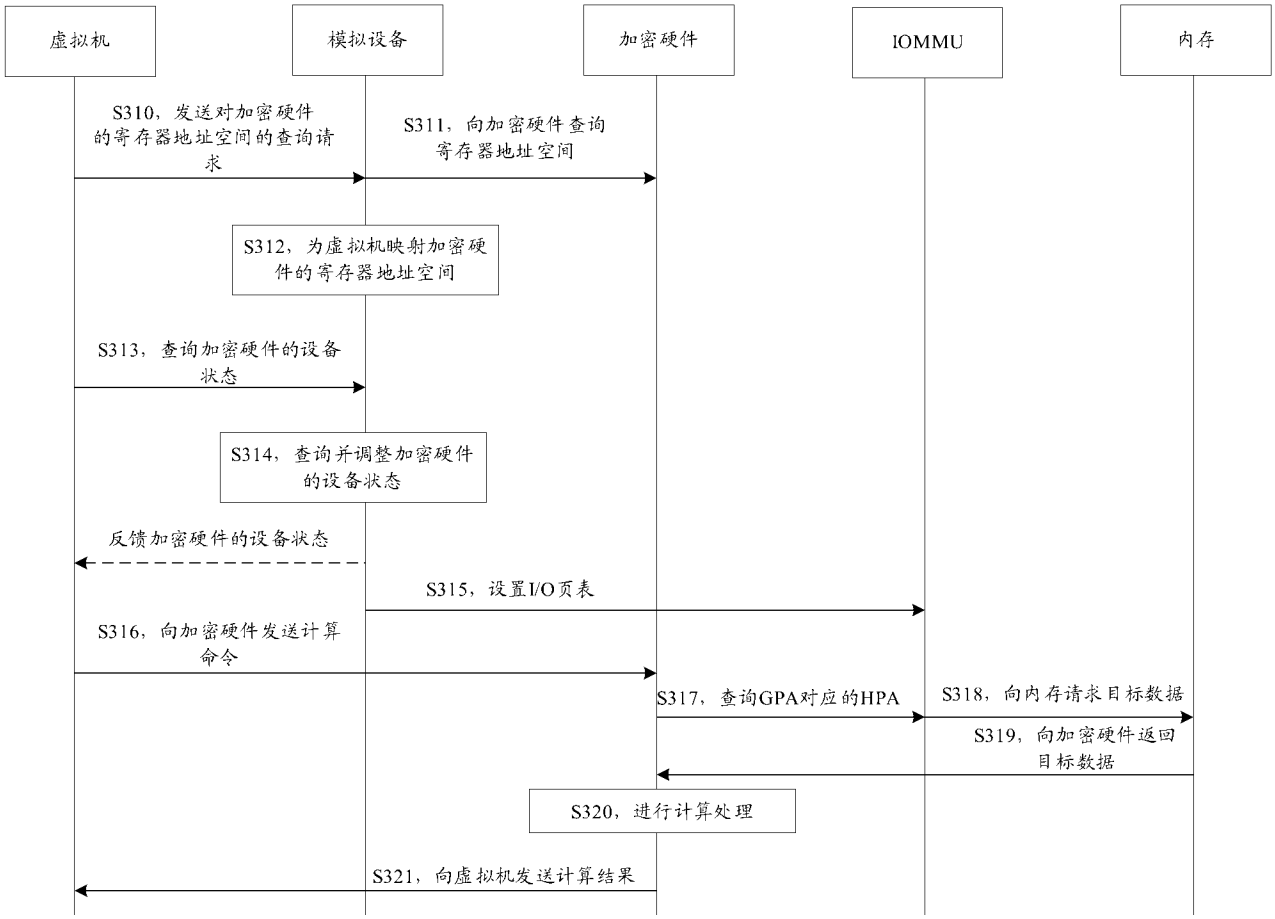
虚拟机
模拟设备
加密硬件
IOMMU
内存
S310，发送对加密硬件的寄存器地址空间的查询请求
S311，向加密硬件查询寄存器地址空间
S312，为虚拟机映射加密硬件的寄存器地址空间
S313，查询加密硬件的设备状态
S314，查询并调整加密硬件的设备状态
反馈加密硬件的设备状态
S315，设置I/O页表
S316，向加密硬件发送计算命令
S317，查询GPA对应的HPA
S318，向内存请求目标数据
S319，向加密硬件返回目标数据
S320，进行计算处理
S321，向虚拟机发送计算结果

图 13

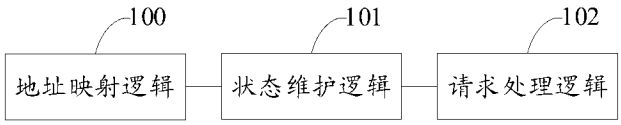
100
101
102
地址映射逻辑
状态维护逻辑
请求处理逻辑

图 14

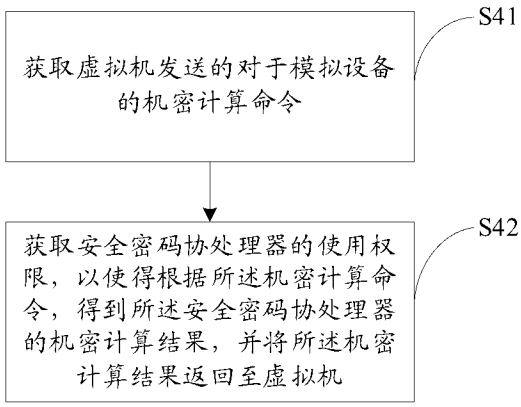
S41
获取虚拟机发送的对于模拟设备的机密计算命令
S42
获取安全密码协处理器的使用权限，以使得根据所述机密计算命令，得到所述安全密码协处理器的机密计算结果，并将所述机密计算结果返回至虚拟机

图 15

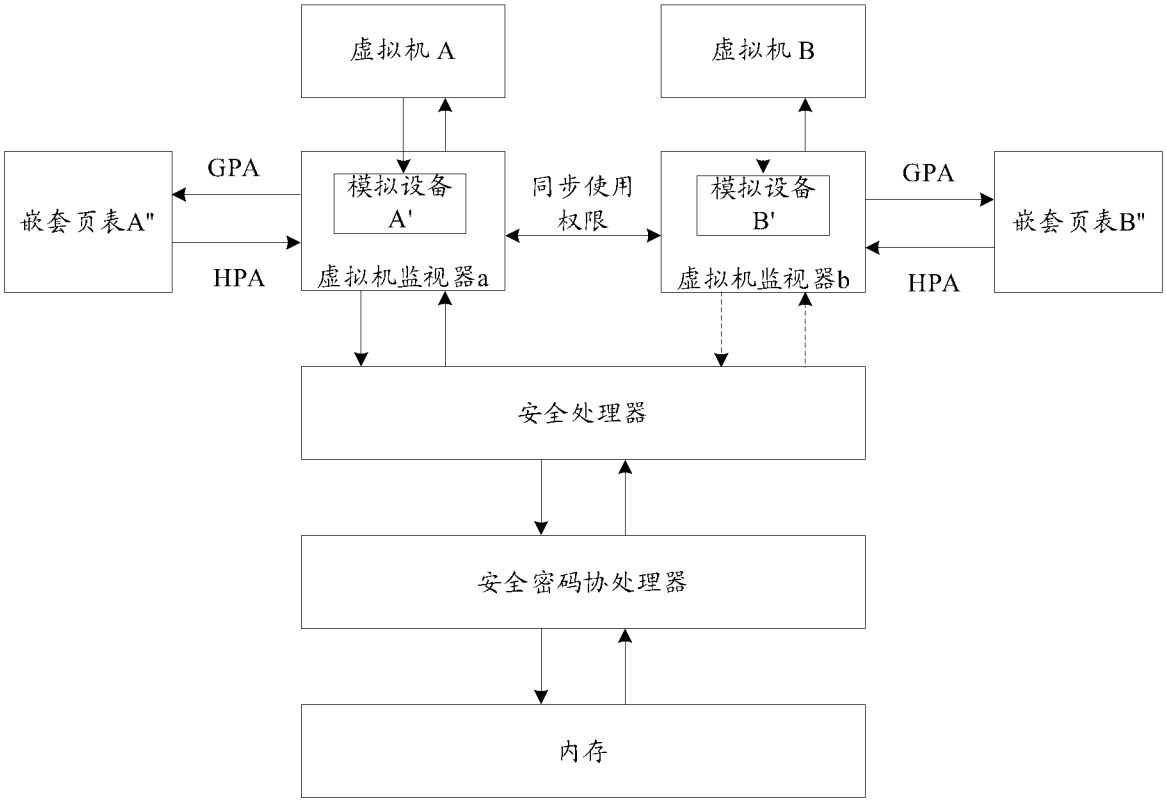
虚拟机 A
虚拟机 B
嵌套页表A"
GPA
HPA
模拟设备 A'
虚拟机监视器a
同步使用权限
模拟设备 B'
虚拟机监视器b
GPA
HPA
嵌套页表B"
安全处理器
安全密码协处理器
内存

图 16

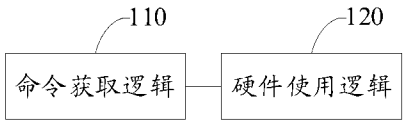
110
120
命令获取逻辑
硬件使用逻辑

图 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2024/097172

A. CLASSIFICATION OF SUBJECT MATTER

G06F9/455(2018.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F

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

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

VEN, CNABS, CNTXT, WOTXT, EPTXT, USTXT, CNKI, IEEE: 加密, 密码, 硬件, 设备, 处理器, 模拟, 仿真, 虚机, 虚拟, 共享, encryption, password, hardware, device, processor, emulation, emulation, virtual machine, virtual, shared

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 116841691 A (HYGON INFORMATION TECHNOLOGY CO., LTD.) 03 October 2023 (2023-10-03) claims 1-24	1-24
X	CN 101176100 A (INTEL CORP.) 07 May 2008 (2008-05-07) description, pages 3-27, figures 1-5, and abstract	1-24
A	CN 101267334 A (LENOVO (BEIJING) CO., LTD.) 17 September 2008 (2008-09-17) entire document	1-24
A	CN 104951688 A (NATIONAL COMPUTER NETWORK AND INFORMATION SECURITY MANAGEMENT CENTER) 30 September 2015 (2015-09-30) entire document	1-24
A	US 2006236039 A1 (INTERNATIONAL BUSINESS MACHINES CORP.) 19 October 2006 (2006-10-19) entire document	1-24
A	US 2020257547 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC) 13 August 2020 (2020-08-13) entire document	1-24

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
12 August 2024	**16 August 2024**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/097172

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 116841691 A	03 October 2023	None	
CN 101176100 A	07 May 2008	EP 1880339 A2	23 January 2008
		KR 20080008361 A	23 January 2008
		WO 2006124751 A2	23 November 2006
		JP 2008541279 A	20 November 2008
		US 2006256105 A1	16 November 2006
CN 101267334 A	17 September 2008	None	
CN 104951688 A	30 September 2015	None	
US 2006236039 A1	19 October 2006	None	
US 2020257547 A1	13 August 2020	WO 2020163122 A1	13 August 2020
		EP 3921726 A1	15 December 2021

国际检索报告

国际申请号
PCT/CN2024/097172

A. 主题的分类

G06F9/455(2018.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

VEN,CNABS,CNTXT,WOTXT,EPTXT,USTXT,CNKI,IEEE:加密，密码，硬件，设备，处理器，模拟，仿真，虚机，虚拟，共享，encryption, password, hardware, device, processor, emulation, emulation, virtual machine, virtual, shared

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 116841691 A (海光信息技术股份有限公司) 2023年10月3日 (2023 - 10 - 03) 权利要求1-24	1-24
X	CN 101176100 A (英特尔公司) 2008年5月7日 (2008 - 05 - 07) 说明书第3-27页，图1-5，摘要	1-24
A	CN 101267334 A (联想（北京）有限公司) 2008年9月17日 (2008 - 09 - 17) 全文	1-24
A	CN 104951688 A (国家计算机网络与信息安全管理中心) 2015年9月30日 (2015 - 09 - 30) 全文	1-24
A	US 2006236039 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2006年10月19日 (2006 - 10 - 19) 全文	1-24
A	US 2020257547 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC) 2020年8月13日 (2020 - 08 - 13) 全文	1-24

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“D” 申请人在国际申请中引证的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

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

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2024年8月12日	2024年8月16日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	吴媛媛 电话号码 (+86) 010-53961351

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/097172

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	116841691	A	2023年10月3日	无			
CN	101176100	A	2008年5月7日	EP	1880339	A2	2008年1月23日
				KR	20080008361	A	2008年1月23日
				WO	2006124751	A2	2006年11月23日
				JP	2008541279	A	2008年11月20日
				US	2006256105	A1	2006年11月16日
CN	101267334	A	2008年9月17日	无			
CN	104951688	A	2015年9月30日	无			
US	2006236039	A1	2006年10月19日	无			
US	2020257547	A1	2020年8月13日	WO	2020163122	A1	2020年8月13日
				EP	3921726	A1	2021年12月15日