

(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 10 月 10 日 (10.10.2024)



(10) 国际公布号
WO 2024/208271 A1

- (51) 国际专利分类号:
G06F 21/57 (2013.01)
- (21) 国际申请号: PCT/CN2024/085826
- (22) 国际申请日: 2024 年 4 月 3 日 (03.04.2024)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202310377569.9 2023年4月6日 (06.04.2023) CN
- (71) 申请人: 支付宝(杭州)信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。
- (72) 发明人: 刘双 (LIU, Shuang); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。 陈洲 (CHEN, Zhou); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11,

Zhejiang 310000 (CN)。 闫守孟 (YAN, Shoumeng); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(74) 代理人: 北京亿腾知识产权代理事务所(普通合伙) (E-TONE INTELLECTUAL PROPERTY FIRM (GENERAL PARTNERSHIP)); 中国北京市海淀区中关村紫金数码园 3 号楼 707, Beijing 100190 (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, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(54) Title: METHOD AND APPARATUS FOR MEMORY PAGE MANAGEMENT

(54) 发明名称: 内存页面管理方法及装置

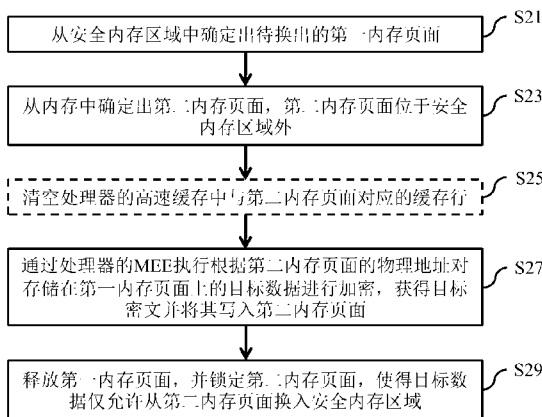


图 2

- S21 Determine a first memory page to be paged out from a secure memory region
- S23 Determine a second memory page from a memory, the second memory page being outside a secure memory region
- S25 Clear a cache line corresponding to a second memory page from the cache of a processor
- S27 By means of the MEE of a processor, encrypt the target data stored on the first memory page according to a physical address of a second memory page, so as to give a target ciphertext and write same into the second memory page
- S29 Release the first memory page and lock the second memory page, such that the target data is only permitted to be paged into the secure memory region from the second memory page

(57) Abstract: Provided are a method and apparatus for memory page management. A computing device for executing the method comprises a processor and a memory. The processor comprises a memory encryption engine (MEE), and the memory comprises a secure memory region. After a first memory page to be paged out is determined from a secure memory region, a second memory page can be determined from a common memory outside the secure memory region. By means of the MEE, the target data stored on the first memory page is encrypted according to a physical address of the first memory page, so as to give a target ciphertext and write same into the second memory page. The first memory page is then released and the second memory page is locked, such that the target data is only permitted to be paged into the secure memory region from the second memory page.

(57) 摘要: 一种内存页面管理方法及装置。执行该方法的计算设备包括处理器和内存, 该处理器包括内存加密引擎 MEE, 该内存中包括安全内存区域。在从安全内存区域中确定出待换出的第一内存页面后, 可以从安全内存区域外的普通内存中确定出第二内存页面; 然后通过 MEE 实现根据第一内存页面的物理地址对存储在第二内存页面上的目标数据进行加密, 获得目标密文并将其写入第二内存页面; 进而释放该第一内存页面并锁定第二内存页面, 使得该目标数据仅允许从第二内存页面换入安全内存区域。

(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))。

内存页面管理方法及装置

本申请要求于 2023 年 04 月 06 日提交中国国家知识产权局、申请号为 202310377569.9、
5 申请名称为“内存页面管理方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本说明书一个或多个实施例涉及计算机领域，尤其涉及一种内存页面管理方法及装置。

10

背景技术

基于硬件的可信执行环境（trusted execution environment，TEE）解决方案中，通常需要在计算设备的内存中预留属于 TEE 的安全内存区域。计算设备运行过程中，可能因安全内存区域中剩余安全内存不足而启用内存换页机制，将属于安全内存区域的某些安全内存
15 页面换出到安全内存区域外，即将存储在某些安全内存页面上的目标数据换出到普通内存。
希望有一种新的技术方案，以期能够更为快速的完成换出安全内存页面。

发明内容

本说明书一个或多个实施例中提供了一种内存页面管理方法及装置。

20 第一方面，提供了一种内存页面管理方法，所述方法由计算设备执行，所述计算设备包括处理器和内存，所述处理器包括内存加解密引擎（memory encryption engine，MEE），所述内存中包括安全内存区域。其中，所述方法包括：从所述安全内存区域中确定出待换出的第一内存页面；从所述内存中确定出第二内存页面，所述第二内存页面位于所述安全内存区域外；通过所述 MEE，根据所述第二内存页面的物理地址对存储在所述第一内存页
25 面上的目标数据进行加密，获得目标密文并将其写入所述第二内存页面；释放所述第一内存页面，并锁定所述第二内存页面，使得所述目标数据仅允许从所述第二内存页面换入所述安全内存区域。

在一种可能的实施方式中，其中，所述方法还包括：当允许访问所述目标数据的安全应用请求访问所述目标数据而发生缺页错误时，从所述内存中确定出用于存储所述目标数
30 据的第二内存页面；从所述安全内存区域中确定出第三内存页面；通过所述 MEE，根据所述第二内存页面的物理地址对写入所述第二内存页面的所述目标密文进行解密，获得

所述目标数据并将其存储至所述第三内存页面；根据所述第三内存页面更新所述安全应用对应的页表。

在一种可能的实施方式中，所述方法还包括：在所述从所述内存中确定出第二内存页面之后，清空所述处理器的高速缓存中与所述第二内存页面对应的缓存行。

5 在一种可能的实施方式中，所述安全内存区域属于基于硬件的 TEE。

第二方面，提供了一种内存页面管理装置，部署在计算设备中，所述计算设备包括处理器和内存，所述处理器包括 MEE，所述内存中包括安全内存区域。所述装置包括：换页驱动模块，配置为从所述安全内存区域中确定出待换出的第一内存页面；所述换页驱动模块，还配置为从所述内存中确定出第二内存页面，所述第二内存页面位于所述安全内存区域外；安全换页模块，配置为通过所述 MEE，根据所述第二内存页面的物理地址对存储在所述第一内存页面上的目标数据进行加密，获得目标密文并将其写入所述第二内存页面；所述换页驱动模块，配置为释放所述第一内存页面，并锁定所述第二内存页面，使得所述目标数据仅允许从所述第二内存页面换入所述安全内存区域。

在一种可能的实施方式中，所述换页驱动模块，还配置为当允许访问所述目标数据的安全应用请求访问所述目标数据而发生缺页错误时，从所述内存中确定出用于存储所述目标数据的所述第二内存页面；所述换页驱动模块，还配置为从所述安全内存区域中确定出第三内存页面；所述安全换页模块，还配置为通过所述 MEE，根据所述第二内存页面的物理地址对写入所述第二内存页面的所述目标密文进行解密，获得所述目标数据并将其存储至所述第三内存页面；所述换页驱动模块，还配置为根据所述第三内存页面更新所述安全应用对应的页表。

在一种可能的实施方式中，所述安全换页模块，还配置为在从所述内存中确定出第二内存页面之后，清空所述处理器的高速缓存中与所述第二内存页面对应的缓存行。

在一种可能的实施方式中，所述安全内存区域属于基于硬件的 TEE。

第三方面，提供了一种计算设备，包括内存和处理器，所述处理器包括处理核心和内存加解密引擎，所述内存包括安全内存区域，所述内存中存储有位于所述安全内存区域外的可执行代码/指令，所述处理器的处理核心执行所述可执行代码/指令时，实现第一方面中任一项所述的方法。

第四方面，提供了一种计算机可读存储介质，其上存储有计算机程序/指令，所述计算机程序/指令在计算设备中执行时，计算设备实现第一方面中任一项所述的方法。

30 通过本说明书一个或多个实施例中提供的方法及装置，计算设备在从安全内存区域中

确定出待换出的第一内存页面之后，可以从安全内存区域外的普通内存确定出第二内存页面；然后通过 MEE 实现根据第二内存页面的物理地址对存储在第一内存页面上的目标数据进行加密，获得目标密文并将其写入第二内存页面，进而释放第一内存页面并锁定第二内存页面，使得目标数据仅允许从第二内存页面换入安全内存区域。如此，计算设备在换出属于安全内存区域的安全内存页面的过程中，通过复用处理器中的 MEE 来完成对存储在安全内存页面上的目标数据进行加密，可以更为快速的完成换出安全内存页面。

附图说明

为了更清楚地说明本说明书实施例的技术方案，下面将对实施例描述中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发明的一些实施例，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它的附图。

图 1 为示例性提供的一种支持基于硬件的 TEE 的计算设备的结构示意图；

图 2 为本说明书实施例中提供的一种内存页面管理方法的流程图之一；

图 3 为本说明书实施例中提供的一种内存页面管理方法的流程图之二；

图 4 为本说明书实施例中提供的一种内存页面管理装置的结构示意图。

具体实施方式

下面结合附图，对本说明书所提供的各个非限制性实施例进行详细描述。

目前工业界十分关注 TEE 技术的解决方案，几乎所有主流的芯片和软件联盟都有自己独立的 TEE 解决方案，比如 Intel SGX (Software Guard Extensions, 软件保护扩展) 以及 ARM Trust zone (信任区) 等基于硬件的 TEE。其中，TEE 可以起到黑箱作用，在 TEE 中的代码和数据即便是操作系统层都无法偷窥，只有通过代码中预先定义的接口才能对其进行操作。在效率方面，由于 TEE 的黑箱性质，在 TEE 中进行运算的是明文数据，而不是同态加密中复杂的密码学运算，计算过程效率几乎没有损失。

图 1 为示例性提供的一种支持基于硬件的 TEE 的计算设备的结构示意图。参见图 1 所示，该计算设备可以包括处理器和内存。处理器包括一个或多个处理核心，处理核心包括但不限于用于提取指令的预取逻辑、用于解码指令的解码逻辑和用于执行指令的执行逻辑等等。该处理器还可以包括用于缓存指令和/或数据的高速缓存，例如可以包括但不限于级别为 L1、L2 和 LLC 等多个级别的高速缓存。除此之外，处理器中还可以包括配置有 MEE 的系统代理，其中该 MEE 的功能在下文中详细描述。

该计算设备还可以包括其它功能模块，例如还可以包括用于支持处理器访问内存的内存控制器。内存控制器可以耦合到包含 MEE 的系统代理，也可以独立于处理器和内存。

基于硬件的 TEE 解决方案中，需要在计算设备的内存中预留安全内存区域，例如预留预定数量的物理内存页面作为安全内存区域。下面以 Intel SGX 技术的安全内存区域为例进行说明：计算设备可以基于 SGX 技术创建 enclave（围圈或飞地），以作为用于执行特定应用程序（安全应用）的 TEE。计算设备可以利用处理器中新增的处理器指令，在内存中分配部分区域 EPC（Enclave Page Cache，围圈页面缓存或飞地页面缓存），以用于驻留上述的 Enclave，前述的 EPC 所对应的内存区域即为属于 TEE 的安全内存/安全内存区域。

处理器中的 MEE 用于对处理器和安全内存区域间交换的数据进行加解密。与安全应用相关的数据（enclave 中的代码和数据）从处理器到安全内存区域时，可以被处理器内部的 MEE 加密以获得对应的密文，密文可以通过内存控制器写入到安全内存区域；安全内存区域中的密文只有 MEE 能够解密。由此，enclave 的安全边界只包含其自身和处理器，无论是特权软件或非特权软件都无法访问 Enclave，即便是操作系统管理员和虚拟机监控器（virtual machine monitor, VMM；或称为 hypervisor）也无法影响 enclave 中的代码和数据。

计算设备运行期间，可能因安全内存区域的可用物理内存不足而启用内存换页机制。区别于普通内存页面的换页过程，为了保证安全内存区域存储的数据的安全性，换出属于安全内存区域的安全内存页面前，需要加密其存储的目标数据以获得目标密文，此外还可能生成用于保证新鲜性的 Nonce 和/或用于验证完整性的信息验证码(message authentication code, MAC)等等，然后再将目标密文存储到安全内存区域外的普通内存页面；可以理解，从普通内存页面将目标密文换入安全内存页面前，需要对应的执行解密操作。对安全内存页面执行换页机制的过程中，通常采用软件的方式完成对数据的加解密操作，耗时较长。

本说明书实施例中至少提供了一种内存页面管理方法和装置。执行该方法的计算设备包括处理器和内存，处理器中包括 MEE，内存中包括安全内存区域。计算设备在从安全内存区域中确定出待换出的第一内存页面之后，可以从安全内存区域外的普通内存确定出第二内存页面；然后通过 MEE 实现根据第二内存页面的物理地址对存储在第一内存页面上的目标数据进行加密，获得目标密文并将其写入第二内存页面，进而释放第一内存页面并锁定第二内存页面，使得目标数据仅允许从第二内存页面换入安全内存区域。如此，计算设备在换出属于安全内存区域的安全内存页面的过程中，通过复用处理器中的 MEE 来完成对存储在安全内存页面上的目标数据进行加密，可以更为快速的完成换出安全内存页面，以利支持依赖安全内存页面运行的安全应用更加高效的运行。

下面结合图 1 示例的计算设备详细描述本说明书实施例中提供的技术方案。

图 2 为本说明书实施例中提供的一种内存页面管理方法的流程图之一。该方法可以由计算设备执行，该计算设备包括处理器和内存，该处理器包括 MEE，该内存中包括安全内存区域，该安全内存区域属于基于硬件的 TEE，此外该处理器还可以包括一个或多个处理核心。该方法示例性的描述了换出属于安全内存区域的安全内存页面的过程。

参见图 2 所示，该方法可以包括但不限于如下步骤 S21~步骤 S29 中的部分或全部。

步骤 S21，从安全内存区域中确定出待换出的第一内存页面。

计算设备部署的操作系统（operating system，OS）可以配置换页驱动模块，通过换页驱动模块监控内存的使用情况，例如监控安全内存区域的使用情况。当换页驱动模块监控到安全内存区域的可用物理内存不足时，该换页驱动模块可以触发对安全内存页面的换页过程，按照基于访问频次和/或访问时间等预先配置的决策规则，从属于安全内存区域的多个安全内存页面中确定出待换出的第一内存页面。就硬件层面而言，计算设备的处理器可以通过其处理核心执行换页驱动模块所对应的部分指令，使得计算设备实现前述步骤 S21。

步骤 S23，从内存中确定出第二内存页面，第二内存页面位于安全内存区域外。

换页驱动模块例如还可以监控内存中除安全内存区域外的普通内存区域的使用情况。换页驱动模块决策出待换出的第一内存页面后，可以接着从普通内存区域中确定出第二内存页面。就硬件层面而言，计算设备的处理器可以通过其处理核心执行换页驱动模块所对应的部分指令，使得计算设备实现前述步骤 S23。

当第二内存页面是处于空闲态的内存页面的情况下，即第二内存页面的物理内存地址上并未存储相关数据的情况下，可以直接接着执行如下步骤 S27。当第二内存页面并非处于空闲态的内存页面的情况下，例如第二内存页面上存储有可供 TEE 外的应用程序访问的业务数据的情况下，可以依次执行如下步骤 S25 和步骤 S27。

步骤 S25，清空处理器的高速缓存中与第二内存页面对应的缓存行。

计算设备中部署的 OS 或者虚拟机监控器可以配置安全换页模块。换页驱动模块可以向安全换页模块提供第一内存页面和第二内存页面的物理内存地址，由安全换页模块实现根据第二内存页面的物理地址，清空处理器的高速缓存中与第二内存页面对应的缓存行（cache line），保证第二内存页面的物理地址和其对应处理器的高速缓存中的数据具有一致性，避免后续过程中发生处理器的高速缓存中对相同物理内存地址同时存在明文数据和目标密文等两个不同的副本。就硬件层面而言，计算设备的处理器可以通过其处理核心执行安全换页模块所对应的部分指令，使得计算设备实现前述步骤 S25。

步骤 S27, 通过处理器的 MEE 执行根据第二内存页面的物理地址对存储在第一内存页面上的目标数据进行加密, 获得目标密文并将其写入第二内存页面。

安全换页模块可以向 MEE 提供第一页面管理请求, 其中至少包括第一内存页面和第二内存页面的物理内存地址, 还可以包括用于指示 MEE 需要执行的页面管理操作是换出安全内存页面的指示信息, 从而触发 MEE 实现步骤 S27 中所述的功能。就硬件层面而言, 计算设备的处理器可以通过其处理核心执行安全换页模块所对应的部分指令, 完成由处理核心向 MEE 提供前述的第一页面管理请求, 进而触发 MEE 执行对应的页面管理操作。

参照前文, MEE 主要用于对处理器和安全内存区域间交换的数据进行加解密, 与安全应用相关的数据从处理器到安全内存区域时, 被 MEE 加密以获得对应的密文并通过内存控制器写入到安全内存区域。而且, MEE 对数据进行加解密的过程中, 通常会选择被处理的数据所对应的安全内存页面的物理内存地址作为输入。由此不难理解, 前述步骤 S27 中, 响应于第一页面管理请求, MEE 可以实现: 通过内存控制器实现根据第一内存页面的物理地址, 从安全内存区域中读取存储于第一内存页面的目标数据的第一密文, 根据第一内存页面的物理地址对该第一密文进行解密以获得目标数据; 进而根据第二内存页面的物理地址对该目标数据进行加密以获得目标密文, 并通过内存控制器实现根据第二内存页面的物理地址将目标数据所对应的目标密文写入第二内存页面。

在一些可能的实施方式中, 计算设备还可以通过安全换页模块生成用于保证目标数据的新鲜性的 Nonce, 和/或, 生成用于验证目标数据和/目标密文的完整性的 MAC。

步骤 S29, 释放第一内存页面, 并锁定第二内存页面, 使得目标数据仅允许从第二内存页面换入安全内存区域。

换页驱动模块可以更新允许访问第一内存页面的安全应用所对应的页表, 并清空第一内存页面上存储的目标数据的第一密文, 从而完成释放第一内存页面。例如, 前述页表中包括一个或多个页表项, 其中一个页表项包括目标数据所对应的虚拟内存页面与该第一内存页面间的映射关系, 安全应用通过该虚拟内存页面发起对通过第一内存页面存储的目标数据的访问; 换页驱动模块例如可以从该页表中删除第一内存页面所对应的页表项, 或者将第一内存页面所对应的页表项置为无效, 从而完成对相关页表的更新。

换页驱动模块可以通过锁定第二内存页面, 实现将目标数据所对应的目标密文固定在第二内存页面的物理地址上, 直到该第二内存页面中的目标密文被换入安全内存区域。换页驱动模块锁定第二内存页面后, 可以使计算设备中部署的 OS 禁止将第二内存页面换出到磁盘的交换空间并且禁止对第二内存页面进行页面迁移; 或者, 计算设备中部署的 OS

允许将第二内存页面换出到磁盘的交换空间，被换出到交换空间的目标密文被重新换入普通内存区域时，仅允许将该目标密文换入到第二内存页面的物理地址而禁止换入到普通内存区域的其它内存页面。

就硬件层面而言，计算设备的处理器可以通过其处理核心执行换页驱动模块所对应的部分指令，使得计算设备实现前述步骤 S29。

允许访问目标数据的安全应用请求访问已经被换出安全内存区域的目标数据时，因安全内存区域中原本用于存储目标数据的第一内存页面已经被释放掉，计算设备将会发生缺页错误，此种情况下需要将目标数据重新换入到安全内存区域。由此，计算设备还可以维护目标数据与第二内存页面间的对应关系，例如通过换页驱动模块维护目标数据所对应的虚拟内存页面与第二内存页面间的对应关系，以便后续过程中发生安全应用请求访问目标数据时，换页驱动模块可以根据该对应关系重新将目标数据换入到安全内存区域。

参见图 3，从安全内存区域外将目标数据换入安全内存区域的过程，可以包括但不限于如下步骤 S31~步骤 S37 中的部分或全部。

步骤 S31，当允许访问目标数据的安全应用请求访问目标数据而发生缺页错误时，从内存中确定出用于存储目标数据的第二内存页面。

安全应用例如可以通过目标数据所对应的虚拟内存页面发起对目标数据的访问，由于安全应用的页表中与该虚拟内存页面对应的页表项已经被删除或无效，因此会发生缺页错误。换页驱动模块可以处理该缺页错误，实现基于其维护的该虚拟内存页面与第二内存页面间的对应关系，确定出用于存储目标数据的内存页面是普通内存空间中的第二内存页面。

步骤 S33，从安全内存区域中确定出第三内存页面。

换页驱动模块可以从安全内存区域中确定出处于空闲态的第三内存页面。

就硬件层面而言，计算设备的处理器可以通过其处理核心执行换页驱动模块所对应的部分指令，使得计算设备实现前述步骤 S31 和步骤 S33。

步骤 S35，通过 MEE 执行根据第二内存页面的物理地址对写入第二内存页面中的目标密文进行解密，获得目标数据并将其存储至第三内存页面。

换页驱动模块可以向安全换页模块提供第二内存页面和第三内存页面的物理内存地址。安全换页模块可以向 MEE 提供第二页面管理请求，其中至少包括第二内存页面和第三内存页面的物理内存地址，还可以包括用于指示 MEE 需要执行的页面管理操作是换入安全内存页面的指示信息，从而触发 MEE 完成步骤 S35 中所述的功能。就硬件层面而言，计算设备的处理器可以通过其处理核心执行安全换页模块所对应的部分指令，完成由处理

核心向 MEE 提供前述的第二页面管理请求，触发 MEE 执行对应的页面管理操作。

与前述步骤 S27 相对应的，响应于第二页面管理请求，MEE 可以：通过内存控制器实现根据第二内存页面的物理地址，从安全内存区域外的普通内存中读取已写入第二内存页面的目标数据的目标密文，根据第二内存页面的物理地址对该目标密文进行解密以获得目标数据；进而根据第三内存页面的物理地址对该目标数据进行加密以获得第二密文，并通过内存控制器实现根据第三内存页面的物理地址将第二密文写入第三内存页面。

在一些可能的实施方式中，计算设备还可以通过安全换页模块实现根据相应的 Nonce 验证目标数据的新鲜性，以避免发生重放攻击；和/或，计算设备还可以通过安全换页模块实现根据相应的 MAC 验证目标数据和/或目标密文的完整性。可以理解的是，Nonce 验证未通过或者 MAC 验证未通过的情况下，说明可能存在入侵者发起重放攻击或者恶意更改第二内存页面中存储的目标密文，可以采用相应技术手段应对。

步骤 S37，根据第三内存页面更新安全应用对应的页表。

换页驱动模块可以在安全应用对应的页面中新增或更新一个有效的页表项，该页表项中包括用于支持安全应用访问目标数据的虚拟内存页面与第三内存页面间的对应关系。如此，对于安全应用通过目标数据所对应的虚拟内存页面发起的对目标数据的访问请求，可以根据更新后的页表中的相关页表项查询到用于存储目标数据的第三内存页面，从而具体实现对通过第三内存页面存储的目标数据进行访问。

完成将目标数据换入安全内存后，计算设备还可以对应的释放原本用于存储目标数据的第二内存页面。例如，安全驱动模块在通过 MEE 完成执行步骤 S35 后，可以向换页驱动模块返回成功完成换页操作的响应消息，触发换页驱动模块执行前述步骤 S37，并根据第二内存页面的物理内存地址从普通内存区域删除目标密文，完成释放第二内存页面。

前述各个方法实施例中，虽然结合换页驱动模块和安全换页模块来描述计算设备实现的各个方法步骤，然而可以理解的是计算设备在实现前述各个方法步骤的过程中，可能并不依赖换页驱动模块和安全换页模块来实现，例如可能依赖其它软件模块来实现。

与前述方法实施例基于相同的构思，本说明书实施例中还提供了一种内存页面管理装置 400，部署在计算设备中，所述计算设备包括处理器和内存，所述处理器包括 MEE，所述内存中包括安全内存区域。所述装置 400 包括：换页驱动模块 41，配置为从所述安全内存区域中确定出待换出的第一内存页面；所述换页驱动模块 41，还配置为从所述内存中确定出第二内存页面，所述第二内存页面位于所述安全内存区域外；安全换页模块 43，配置为通过所述 MEE 执行根据所述第二内存页面的物理地址对存储在所述第一内存页面上的

目标数据进行加密，获得目标密文并将其写入所述第二内存页面；所述换页驱动模块 41，配置为释放所述第一内存页面，并锁定所述第二内存页面，使得所述目标数据仅允许从所述第二内存页面换入所述安全内存区域。

5 在一种可能的实施方式中，所述换页驱动模块 41，还配置为当允许访问所述目标数据的安全应用请求访问所述目标数据而发生缺页错误时，从所述内存中确定出用于存储所述目标数据的所述第二内存页面；所述换页驱动模块 41，还配置为从所述安全内存区域中确定出第三内存页面；所述安全换页模块 43，还配置为通过所述 MEE 执行根据所述第二内存页面的物理地址对写入所述第二内存页面的所述目标密文进行解密，获得所述目标数据并将其存储至所述第三内存页面；所述换页驱动模块 41，还配置为根据所述第三内存页面
10 更新所述安全应用对应的页表。

在一种可能的实施方式中，所述安全换页模块 43，还配置为在从所述内存中确定出第二内存页面之后，清空所述处理器的高速缓存中与所述第二内存页面对应的缓存行。

在一种可能的实施方式中，所述安全内存区域属于基于硬件的 TEE。

本领域技术人员应该可以意识到，在上述一个或多个示例中，本说明书所描述的功能
15 可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能所对应的计算机程序存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令/代码进行传输，以便这些功能所对应的计算机程序被计算机执行时，通过计算机实现本说明书任意一个实施例中的所述的方法。

本说明书实施例中还提供了一种计算机可读存储介质，其上存储有计算机程序/指令，
20 当所述计算机程序/指令在计算设备中执行时，实现本说明书任意一个实施例中提供的内存页面管理方法。

本说明书实施例中还提供了一种计算设备，包括内存和处理器，所述处理器包括处理核心和 MEE，所述内存包括安全内存区域，所述内存中存储有位于所述安全内存区域外的可执行代码/指令，所述处理器的处理核心执行所述可执行代码/指令时，实现本说明书任
25 意一个实施例中提供的内存页面管理方法。

本说明书中的各个实施例均采用递进的方式描述，各个实施例中相同、相似的部分互相参见即可，每个实施例中重点说明的都是与其他实施例的不同之处。尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

30 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在

一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

- 5 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

权 利 要 求 书

1. 一种内存页面管理方法，由计算设备执行，所述计算设备包括处理器和内存，所述处理器包括内存加解密引擎 MEE，所述内存中包括安全内存区域，所述方法包括：

从所述安全内存区域中确定出待换出的第一内存页面；

从所述内存中确定出第二内存页面，所述第二内存页面位于所述安全内存区域外；

通过所述 MEE，根据所述第二内存页面的物理地址对存储在所述第一内存页面上的目标数据进行加密，获得目标密文并将其写入所述第二内存页面；

释放所述第一内存页面，并锁定所述第二内存页面，使得所述目标数据仅允许从所述第二内存页面换入所述安全内存区域。

2. 根据权利要求 1 所述的方法，所述方法还包括：

当允许访问所述目标数据的安全应用请求访问所述目标数据而发生缺页错误时，从所述内存中确定出用于存储所述目标数据的所述第二内存页面；

从所述安全内存区域中确定出第三内存页面；

通过所述 MEE，根据所述第二内存页面的物理地址对写入所述第二内存页面的所述目标密文进行解密，获得所述目标数据并将其存储至所述第三内存页面；

根据所述第三内存页面更新所述安全应用对应的页表。

3. 根据权利要求 1 所述的方法，所述方法还包括：在所述从所述内存中确定出第二内存页面之后，清空所述处理器的高速缓存中与所述第二内存页面对应的缓存行。

4. 根据权利要求 1-3 中任一项所述的方法，所述安全内存区域属于基于硬件的 TEE。

5. 一种内存页面管理装置，部署在计算设备中，所述计算设备包括处理器和内存，所述处理器包括内存加解密引擎 MEE，所述内存中包括安全内存区域，所述装置包括：

换页驱动模块，配置为从所述安全内存区域中确定出待换出的第一内存页面；

所述换页驱动模块，还配置为从所述内存中确定出第二内存页面，所述第二内存页面位于所述安全内存区域外；

安全换页模块，配置为通过所述 MEE，根据所述第二内存页面的物理地址对存储在所述第一内存页面上的目标数据进行加密，获得目标密文并将其写入所述第二内存页面；

所述换页驱动模块，配置为释放所述第一内存页面，并锁定所述第二内存页面，使得所述目标数据仅允许从所述第二内存页面换入所述安全内存区域。

6. 根据权利要求 5 所述的装置，其中，

所述换页驱动模块，还配置为当允许访问所述目标数据的安全应用请求访问所述目标

数据而发生缺页错误时，从所述内存中确定出用于存储所述目标数据的所述第二内存页面；

所述换页驱动模块，还配置为从所述安全内存区域中确定出第三内存页面；

所述安全换页模块，还配置为通过所述 MEE 执行根据所述第二内存页面的物理地址对写入所述第二内存页面的所述目标密文进行解密，获得所述目标数据并将其存储至所述第三内存页面；

所述换页驱动模块，还配置为根据所述第三内存页面更新所述安全应用对应的页表。

7. 根据权利要求 5 所述的装置，所述安全换页模块，还配置为在从所述内存中确定出第二内存页面之后，清空所述处理器的高速缓存中与所述第二内存页面对应的缓存行。

8. 根据权利要求 5-7 中任一项所述的装置，所述安全内存区域属于基于硬件的 TEE。

9. 一种计算设备，包括内存和处理器，所述处理器包括处理核心和内存加解密引擎 MEE，所述内存包括安全内存区域，所述内存中存储有位于所述安全内存区域外的可执行代码，所述处理器的处理核心执行所述可执行代码时，实现权利要求 1-4 中任一项所述的方法。

10. 一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序在计算设备中执行时，计算设备实现权利要求 1-4 中任一项所述的方法。

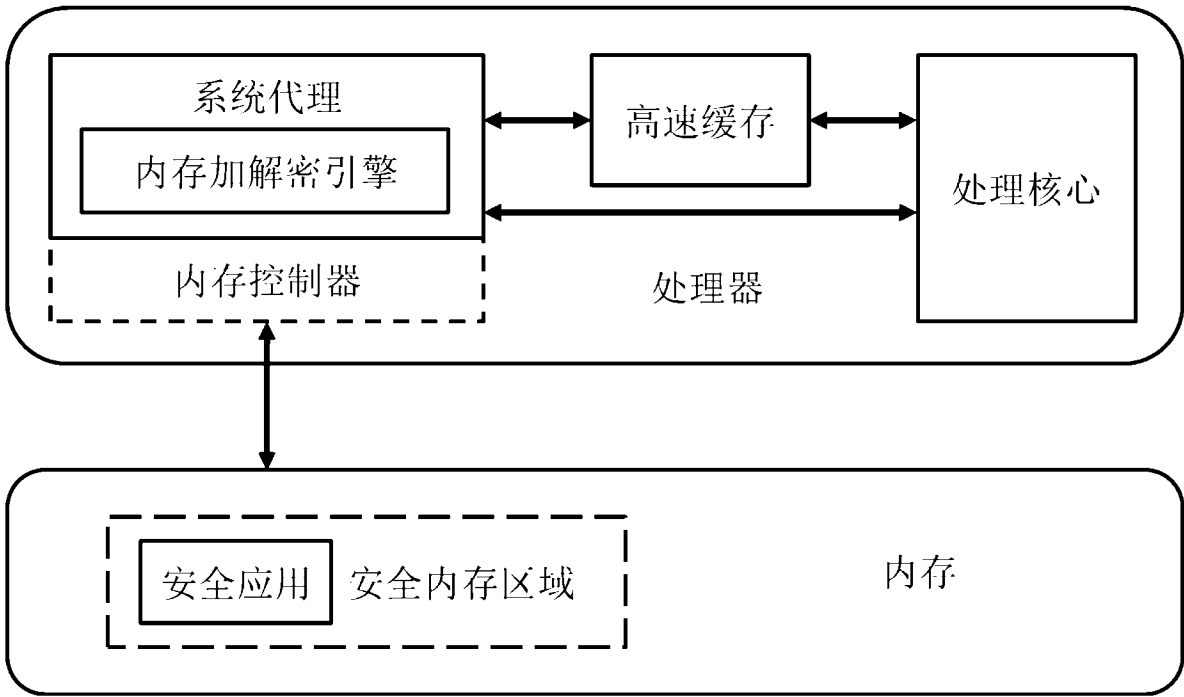


图 1

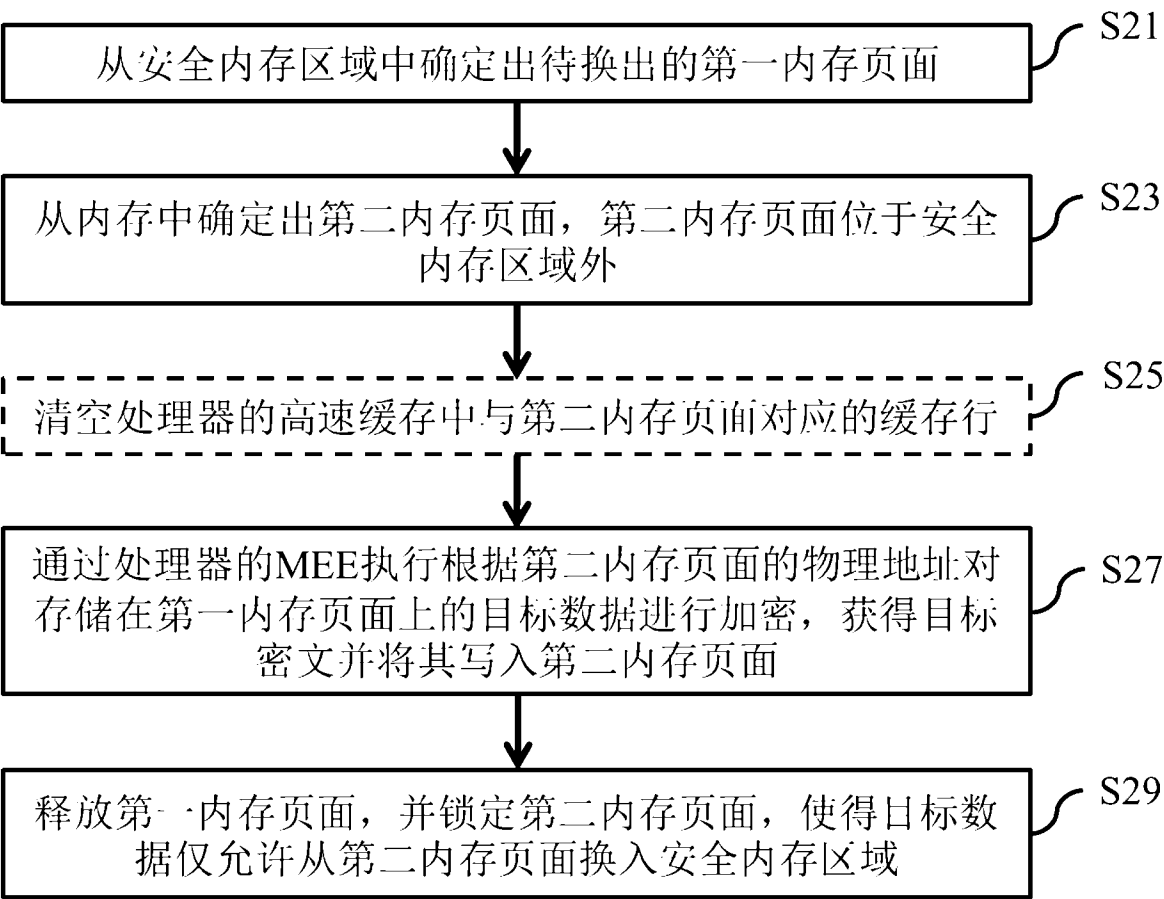


图 2

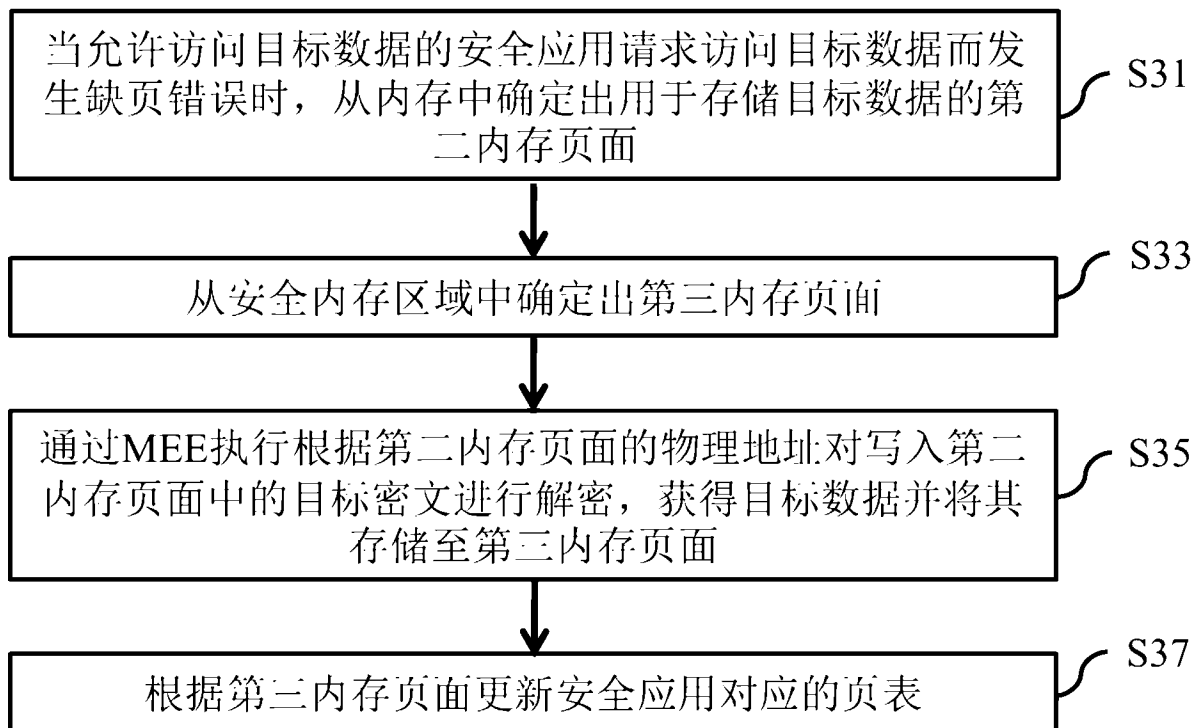


图 3

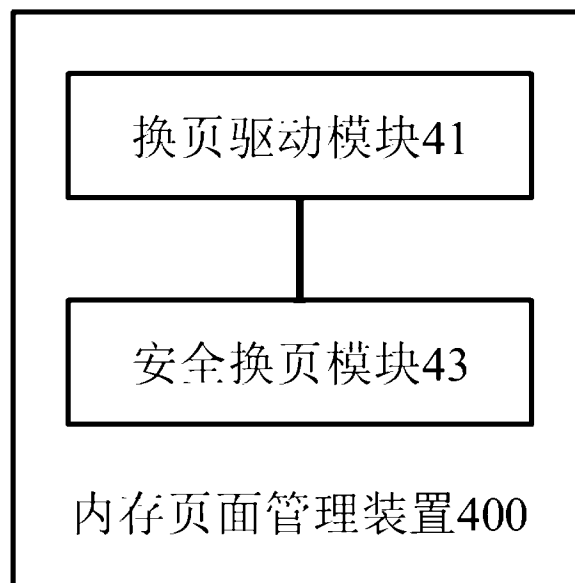


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/085826

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) 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: 飞地, 内存, 存储, 页面, 换页, 交换, 换入, 换出, 搬入, 搬出, 迁移, 安全, 可信, 内存加解密引擎, 加速, 提高, 速度, memory, storage, DRAM, enclave, page, swap, migrate, exchange, TEE, trust, secure, MEE, speed		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 116108454 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 12 May 2023 (2023-05-12) claims 1-10	1-10
A	CN 111967065 A (HAIGUANG INFORMATION TECHNOLOGY CO., LTD.) 20 November 2020 (2020-11-20) description, paragraphs [0036]-[0102], and figures 1-6	1-10
A	CN 114647487 A (ANT FINANCIAL (HANGZHOU) NETWORK TECHNOLOGY CO., LTD. et al.) 21 June 2022 (2022-06-21) entire document	1-10
A	US 2008201540 A1 (SAHITA, Ravi et al.) 21 August 2008 (2008-08-21) entire document	1-10
A	WO 2022154195 A1 (THE INDUSTRY & ACADEMIC COOPERATION IN CHUNGNAM NATIONAL UNIVERSITY et al.) 21 July 2022 (2022-07-21) entire document	1-10
☒ 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 13 June 2024		Date of mailing of the international search report 19 June 2024
Name and mailing address of the ISA/CN China National Intellectual Property Administration (ISA/ CN) China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/085826

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	李明煜 等 (LI, Mingyu et al.). "面向SGX2代新型可信执行环境的内存优化系统 (Memory Optimization System for SGXv2 Trusted Execution Environment)" 软件学报 (<i>Journal of Software</i>), Vol. 33, No. 6, 31 December 2022 (2022-12-31), 2012-2029 ISSN: 1000-9825, entire document	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/085826

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	116108454	A	12 May 2023	None			
CN	111967065	A	20 November 2020	None			
CN	114647487	A	21 June 2022	None			
US	2008201540	A1	21 August 2008	None			
WO	2022154195	A1	21 July 2022	US	2024078307	A1	07 March 2024
				KR	20220103253	A	22 July 2022

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)

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: 飞地, 内存, 存储, 页面, 换页, 交换, 换入, 换出, 搬入, 搬出, 迁移, 安全, 可信, 内存加解密引擎, 加速, 提高, 速度, memory, storage, DRAM, enclave, page, swap, migrate, exchange, TEE, trust, secure, MEE, speed

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 116108454 A (支付宝 (杭州) 信息技术有限公司) 2023年5月12日 (2023 - 05 - 12) 权利要求1-10	1-10
A	CN 111967065 A (海光信息技术有限公司) 2020年11月20日 (2020 - 11 - 20) 说明书第[0036]-[0102]段、图1-6	1-10
A	CN 114647487 A (蚂蚁金服 (杭州) 网络技术有限公司 等) 2022年6月21日 (2022 - 06 - 21) 全文	1-10
A	US 2008201540 A1 (SAHITA, Ravi 等) 2008年8月21日 (2008 - 08 - 21) 全文	1-10
A	WO 2022154195 A1 (THE INDUSTRY & ACADEMIC COOPERATION IN CHUNG-NAM NATIONAL UNIVERSITY 等) 2022年7月21日 (2022 - 07 - 21) 全文	1-10

☒ 其余文件在C栏的续页中列出。

☒ 见同族专利附件。

★ 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“D” 申请人在国际申请中引证的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

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

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“p” 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

“&” 同族专利的文件

国际检索实际完成的日期

2024年6月13日

国际检索报告邮寄日期

2024年6月19日

ISA/CN的名称和邮寄地址

中国国家知识产权局
中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

董洪梅

电话号码 (+86) 010-53961528

PCT/ISA/210 表(第2页) (2022年7月)

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
A	李明煜 等. "面向SGX2 代新型可信执行环境的内存优化系统" 软件学报, 第33卷, 第6期, 2022年12月31日 (2022 - 12 - 31), 2012-2029 ISSN: 1000-9825, 全文	1-10

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/085826

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	116108454	A	2023年5月12日	无	
CN	111967065	A	2020年11月20日	无	
CN	114647487	A	2022年6月21日	无	
US	2008201540	A1	2008年8月21日	无	
WO	2022154195	A1	2022年7月21日	US	2024078307 A1 2024年3月7日
				KR	20220103253 A 2022年7月22日