



(12) 发明专利

(10) 授权公告号 CN 108469986 B

(45) 授权公告日 2021. 04. 09

(21) 申请号 201710100246.X

(22) 申请日 2017.02.23

(65) 同一申请的已公布的文献号
申请公布号 CN 108469986 A

(43) 申请公布日 2018.08.31

(73) 专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72) 发明人 夏虞斌 申宇 陈海波

(74) 专利代理机构 北京中博世达专利商标代理有限公司 11274

代理人 申健

(51) Int. Cl.

G06F 9/48 (2006.01)

(56) 对比文件

US 2016378688 A1, 2016.12.29

CN 106095576 A, 2016.11.09

CN 103399778 A, 2013.11.20

CN 105700945 A, 2016.06.22

CN 105956465 A, 2016.09.21

US 2015205542 A1, 2015.07.23

审查员 张也

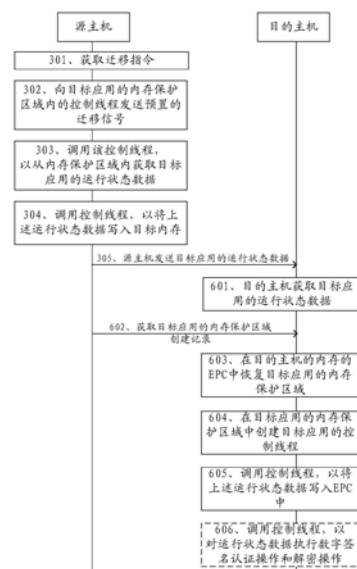
权利要求书2页 说明书10页 附图5页

(54) 发明名称

一种数据迁移方法及装置

(57) 摘要

本发明的实施例提供一种数据迁移方法及装置,涉及通信技术领域,可实现EPC内的数据迁移,以提高应用程序迁移前后的数据一致性。该方法包括:源主机获取迁移指令,所述迁移指令用于指示将创建有enclave的目标应用迁移至目的主机;所述源主机调用所述目标应用的enclave内预置的控制线程,以将EPC内所述目标应用的运行状态数据写入所述源主机的目标内存,所述目标内存为所述源主机的内存中除所述EPC之外的区域;所述源主机向目的主机发送所述目标应用在所述目标内存中的运行状态数据。



1. 一种数据迁移方法,其特征在于,包括:

源主机获取迁移指令,所述迁移指令用于指示将创建有内存保护区域enclave的目标应用迁移至目的主机;

所述源主机调用所述目标应用的enclave内预置的控制线程,以将内存保护区域内内存页缓存EPC内所述目标应用的运行状态数据写入所述源主机的目标内存,所述目标内存为所述源主机的内存中除所述EPC之外的区域;

所述源主机向所述目的主机发送所述目标应用在所述目标内存中的运行状态数据;

其中,所述源主机调用所述目标应用的enclave内预置的控制线程,以将EPC内所述目标应用的运行状态数据写入所述源主机的目标内存,包括:

所述源主机调用所述控制线程,以从所述EPC内获取所述目标应用的运行状态数据;

所述源主机调用所述控制线程,以将所述EPC内所述目标应用的运行状态数据写入所述目标内存;

所述目标应用的enclave内还包括N个工作线程, $N \geq 1$;

其中,所述源主机调用所述控制线程,以从所述EPC内获取所述目标应用的运行状态数据,包括:

当所述控制线程接收到预置的迁移信号时,所述源主机调用所述控制线程,以将所述目标应用的全局状态设置为迁移状态;

当所述全局状态为迁移状态时,所述源主机将所述N个工作线程中每个工作线程的本地状态设置为空闲状态;

当所述N个工作线程中每个工作线程的本地状态均为空闲状态时,所述源主机调用所述控制线程,以通过所述源主机的CPU访问所述EPC内所述目标应用的运行状态数据。

2. 根据权利要求1所述的方法,其特征在于,在所述源主机调用所述控制线程,以从所述EPC内获取所述目标应用的运行状态数据之后,还包括:

所述源主机调用所述控制线程,以对所述运行状态数据执行加密操作;

所述源主机调用所述控制线程,以对加密后的运行状态数据执行数字签名操作;

其中,所述源主机调用所述控制线程,以将所述EPC内所述目标应用的运行状态数据写入所述目标内存,包括:

所述源主机调用所述控制线程,以将执行所述数字签名操作后的运行状态数据写入所述目标内存。

3. 一种数据迁移方法,其特征在于,包括:

目的主机从源主机获取目标应用的运行状态数据;

所述目的主机在所述目的主机的内存保护区域内内存页缓存EPC中恢复所述目标应用的内存保护区域enclave;

所述目的主机在所述目标应用的enclave中创建所述目标应用的控制线程;

所述目的主机调用所述控制线程,以将所述运行状态数据复制到所述EPC中;

其中,所述目的主机在内存的EPC中恢复所述目标应用的enclave,包括:

所述目的主机从所述源主机获取所述目标应用的enclave创建记录,所述enclave创建记录中记录有所述目标应用的enclave的内存地址;

所述目的主机根据所述内存地址在内存的EPC中恢复所述目标应用的enclave。

4. 根据权利要求3所述的方法,其特征在于,所述目的主机调用所述控制线程,以将所述运行状态数据复制到所述EPC中,包括:

所述目的主机调用所述控制线程,以将所述运行状态数据写入所述EPC中;

所述目的主机调用所述控制线程,以对写入所述EPC中的运行状态数据执行数字签名认证操作和解密操作。

5. 一种主机,所述主机为源主机,其特征在于,包括:

获取单元,用于获取迁移指令,所述迁移指令用于指示将创建有内存保护区域enclave的目标应用迁移至目的主机;

执行单元,用于调用所述目标应用的enclave内预置的控制线程,以将内存保护区域内内存缓存EPC内所述目标应用的运行状态数据写入所述源主机的目标内存,所述目标内存为所述源主机的内存中除所述EPC之外的区域;

发送单元,用于向所述目的主机发送所述目标应用在所述目标内存中的运行状态数据;

其中,所述执行单元,具体用于:调用所述控制线程,以从所述EPC内获取所述目标应用的运行状态数据;调用所述控制线程,以将所述EPC内所述目标应用的运行状态数据写入所述目标内存;

所述目标应用的enclave内还包括N个工作线程, $N \geq 1$;

所述执行单元,具体用于:当所述控制线程接收到预置的迁移信号时,调用所述控制线程,以将所述目标应用的全局状态设置为迁移状态;当所述全局状态为迁移状态时,将所述N个工作线程中每个工作线程的本地状态设置为空闲状态;当所述N个工作线程中每个工作线程的本地状态均为空闲状态时,调用所述控制线程,以通过所述源主机的CPU访问所述EPC内所述目标应用的运行状态数据。

6. 根据权利要求5所述的主机,其特征在于,所述主机还包括:

加密单元,用于调用所述控制线程对所述运行状态数据执行加密操作;调用所述控制线程对加密后的运行状态数据执行数字签名操作;

所述执行单元,具体用于:调用所述控制线程,以将执行所述数字签名操作后的运行状态数据写入所述目标内存。

7. 一种主机,所述主机为目的主机,其特征在于,包括:

获取单元,用于从源主机获取目标应用的运行状态数据;

恢复单元,用于在所述目的主机的内存保护区域内存缓存EPC中恢复所述目标应用的内存保护区域enclave;

创建单元,用于在所述目标应用的enclave中创建所述目标应用的控制线程;

复制单元,用于调用所述控制线程,以将所述运行状态数据复制到所述EPC中;

其中,所述恢复单元,具体用于:从所述源主机获取所述目标应用的enclave创建记录,所述enclave创建记录中记录有所述目标应用的enclave的内存地址;根据所述内存地址在内存的EPC中恢复所述目标应用的enclave。

8. 根据权利要求7所述的主机,其特征在于,

所述复制单元,具体用于:调用所述控制线程,以将所述运行状态数据写入所述EPC中;调用所述控制线程,以对所述运行状态数据执行数字签名认证操作和解密操作。

一种数据迁移方法及装置

技术领域

[0001] 本发明实施例涉及通信技术领域,尤其涉及一种数据迁移方法及装置。

背景技术

[0002] 为了提高应用程序在物理主机上运行时的安全性,可在物理主机的内存中划分出一个特定的保护区域,即EPC (Enclave Page Cache, enclave内存页缓存),在EPC内专门运行各个应用程序的enclave (内存保护区域) 代码。以应用A为例,应用A的enclave是指在应用A的地址空间 (address space) 中创建的一个可信执行环境,该enclave内可运行应用A的部分或全部代码,而在该enclave内运行的代码可称为enclave代码。

[0003] 应用A的enclave代码在运行过程中产生的运行状态数据,例如,SSA (State Save Area, 线程运行状态信息) 等,一般存储在应用A的enclave所在的EPC内。该EPC内的数据只允许应用A的enclave代码访问,而运行在该物理主机上的操作系统或虚拟机监控器都不允许访问EPC内的数据。

[0004] 而在云计算应用场景下,可能需要将应用程序在两台不同的物理主机之间迁移。在迁移过程中,一般由源主机上的操作系统或虚拟机监控器访问内存中的数据,并将内存中的数据,例如,应用程序的代码和运行状态数据等,发送到目标物理主机内,但是,内存中EPC内的数据只允许各个应用的enclave代码访问,无法被源主机上的操作系统或虚拟机监控器访问,因此,EPC中存储的数据无法迁移至目标物理主机,导致迁移前后应用程序的相关数据不一致。

发明内容

[0005] 本发明的实施例提供一种数据迁移方法及装置,可实现EPC内的数据迁移,以提高应用程序迁移前后的数据一致性。

[0006] 为达到上述目的,本发明的实施例采用如下技术方案:

[0007] 第一方面,本发明的实施例提供一种数据迁移方法,包括:源主机获取用于指示将创建有enclave的目标应用迁移至目的主机的迁移指令;源主机调用该目标应用的enclave内预置的控制线程,由于该控制线程位于目标应用的enclave内,因此,该控制线程可访问EPC内目标应用的运行状态数据,从而由该控制线程将EPC内该目标应用的运行状态数据写入源主机的目标内存,该目标内存为源主机的内存中除该EPC之外的区域,由于目标内存中的数据是允许源主机的操作系统访问的,因此,源主机可以向目的主机发送该目标应用在目标内存中的运行状态数据,从而实现EPC内的数据迁移,使得目标应用在迁移前后的运行状态等数据保持一致。

[0008] 在一种可能的设计方法中,源主机调用该目标应用的enclave内预置的控制线程,以将EPC内该目标应用的运行状态数据写入源主机的目标内存,包括:源主机调用该控制线程,以从该EPC内获取该目标应用的运行状态数据;源主机调用该控制线程,以将该运行状态数据写入该目标内存。

[0009] 在一种可能的设计方法中,该目标应用的enclave内还包括N个工作线程, $N \geq 1$;其中,源主机调用该控制线程,以从该EPC内获取该目标应用的运行状态数据,包括:当所述控制线程接收到预置的迁移信号时,源主机调用该控制线程,以将该目标应用的全局状态设置为迁移状态;当全局状态为迁移状态时,源主机将N个工作线程中每个工作线程的本地状态设置为空闲状态;当N个工作线程中每个工作线程的本地状态均为空闲状态时,源主机调用该控制线程,以通过源主机的CPU访问EPC内所述目标应用的运行状态数据。

[0010] 由于工作线程在运行的过程中可能会修改EPC内目标应用的运行状态数据,那么,如果N个工作线程中的任意工作线程的本地状态为忙碌状态,则说明该工作线程有可能正在修改EPC内目标应用的运行状态数据,此时,控制线程需要等待该工作线程的本地状态转变为空闲状态,直到控制线程确定上述N个工作线程的本地状态都为空闲状态后,触发EPC内的数据迁移过程,这样可以避免目标应用在迁移的过程中,enclave内的任意工作线程执行时修改了EPC内目标应用的运行状态数据,从而导致目标应用在迁移前后的运行状态不一致的问题。

[0011] 在一种可能的设计方法中,在源主机调用该控制线程,以从EPC内获取该目标应用的运行状态数据之后,还包括:源主机调用该控制线程,以对该运行状态数据执行加密操作;源主机调用该控制线程,以对加密后的运行状态数据执行数字签名操作;其中,源主机调用控制线程,以将EPC内目标应用的运行状态数据写入目标内存,包括:源主机调用控制线程,以将执行了数字签名操作后的运行状态数据写入目标内存。

[0012] 这样,将经过加密和签名的运行状态数据写入目标内存后,没有加密密钥和签名密钥的用户无法读取和修改该运行状态数据,从而提高了数据迁移过程中enclave内产生的运行状态数据的保密性和完整性。

[0013] 第二方面,本发明的实施例提供一种数据迁移方法,包括:目的主机从源主机获取目标应用的运行状态数据;目的主机在目的主机的内存的EPC中恢复该目标应用的enclave;目的主机在该目标应用的enclave中创建该目标应用的控制线程;目的主机调用该控制线程,以将该运行状态数据复制到该EPC中。

[0014] 在一种可能的设计方法中,目的主机在内存的EPC中恢复该目标应用的enclave,包括:目的主机从源主机获取该目标应用的enclave创建记录,该enclave创建记录中记录有该目标应用的enclave的内存地址;目的主机根据该内存地址在内存的EPC中恢复该目标应用的enclave。

[0015] 在一种可能的设计方法中,目的主机调用该控制线程,以将该运行状态数据复制到该EPC中,包括:目的主机调用该控制线程,以将该运行状态数据写入该EPC中;目的主机调用该控制线程,以对写入EPC中的运行状态数据执行数字签名认证操作和解密操作。

[0016] 第三方面,本发明的实施例提供一种源主机,包括:获取单元,用于获取迁移指令,该迁移指令用于指示将创建有enclave的目标应用迁移至目的主机;执行单元,用于调用该目标应用的enclave内预置的控制线程,以将EPC内该目标应用的运行状态数据写入源主机的目标内存,该目标内存为源主机的内存中除该EPC之外的区域;发送单元,用于向目的主机发送目标应用在该目标内存中的运行状态数据。

[0017] 在一种可能的设计方法中,该执行单元,具体用于:调用该控制线程,以从该EPC内获取该目标应用的运行状态数据;调用该控制线程,以将EPC内的该运行状态数据写入该目

标内存。

[0018] 在一种可能的设计方法中,该目标应用的enclave内还包括N个工作线程, $N \geq 1$;该执行单元,具体用于:当所述控制线程接收到预置的迁移信号时,调用所述控制线程,以将所述目标应用的全局状态设置为迁移状态;当所述全局状态为迁移状态时,将所述N个工作线程中每个工作线程的本地状态设置为空闲状态;当所述N个工作线程中每个工作线程的本地状态均为空闲状态时,调用所述控制线程,以通过所述源主机的CPU访问所述EPC内所述目标应用的运行状态数据。

[0019] 在一种可能的设计方法中,该物理主机还包括:加密单元,用于调用该控制线程,以对该运行状态数据执行加密操作;调用该控制线程,以对加密后的运行状态数据执行数字签名操作;执行单元,具体用于:调用控制线程,以将执行数字签名操作后的运行状态数据写入目标内存。

[0020] 第四方面,本发明的实施例提供一种目的主机,包括:获取单元,用于从源主机获取目标应用的运行状态数据;恢复单元,用于在目的主机的内存的EPC中恢复该目标应用的enclave;创建单元,用于在该目标应用的enclave中创建该目标应用的控制线程;复制单元,用于调用该控制线程,以将该运行状态数据复制到该EPC中。

[0021] 在一种可能的设计方法中,该恢复单元,具体用于:从源主机获取该目标应用的enclave创建记录,该enclave创建记录中记录有该目标应用的enclave的内存地址;根据该内存地址在内存的EPC中恢复该目标应用的enclave。

[0022] 在一种可能的设计方法中,该复制单元,具体用于:调用该控制线程,以将该运行状态数据写入该EPC中;调用该控制线程,以对该运行状态数据执行数字签名认证操作和解密操作。

[0023] 第五方面,本发明的实施例提供一种源主机,包括:处理器、存储器、总线和通信接口;该存储器用于存储计算机执行指令,该处理器与该存储器通过该总线连接,当源主机运行时,该处理器执行该存储器存储的该计算机执行指令,以使源主机执行上述第一方面中的任一项数据迁移方法。

[0024] 第六方面,本发明的实施例提供一种目的主机,包括:处理器、存储器、总线和通信接口;该存储器用于存储计算机执行指令,该处理器与该存储器通过该总线连接,当目的主机运行时,该处理器执行该存储器存储的该计算机执行指令,以使目的主机执行上述第二方面中的任一项数据迁移方法。

[0025] 第七方面,本发明的实施例提供一种数据迁移系统,包括第三方面中任一项的源主机,以及第四方面中任一项的目的主机。

[0026] 第八方面,本发明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中存储有指令,当其在上述源主机和/或目的主机上运行时,使得上述源主机和/或目的主机执行上述各方面的数据迁移方法。

[0027] 第九方面,本发明实施例提供了一种包含指令的计算机程序产品,当其在上述源主机和/或目的主机上运行时,使得上述源主机和/或目的主机执行上述各方面的数据迁移方法。

[0028] 本发明的实施例中,上述源主机和目的主机的名字对设备本身不构成限定,在实际实现中,这些设备可以以其他名称出现。只要各个设备的功能和本发明的实施例类似,即

属于本发明权利要求及其等同技术的范围之内。

[0029] 另外,第二方面至第九方面中任一种设计方式所带来的技术效果可参见上述第一方面中不同设计方法所带来的技术效果,此处不再赘述。

附图说明

[0030] 图1为本发明实施中虚拟机的运行环境的架构示意图;

[0031] 图2为本发明实施例提供的一种数据迁移系统的架构示意图;

[0032] 图3为本发明实施例提供的一种数据迁移方法的交互示意图;

[0033] 图4为本发明实施例提供的一种数据迁移方法的应用场景示意图;

[0034] 图5为本发明实施例提供的一种数据迁移方法的流程示意图;

[0035] 图6为本发明实施例提供的一种源主机的结构示意图;

[0036] 图7为本发明实施例提供的一种目的主机的结构示意图;

[0037] 图8为本发明实施例提供的一种源主机(或目的主机)的硬件结构示意图。

具体实施方式

[0038] 以下,术语“第一”、“第二”仅用于描述目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”的特征可以明示或者隐含地包括一个或者更多个该特征。在本发明实施例的描述中,除非另有说明,“多个”的含义是两个或两个以上。

[0039] 为了方便理解本发明实施例,首先在此介绍本发明实施例描述中会引入的几个术语;

[0040] 虚拟机(VM):通过虚拟机软件可以在一台物理主机上模拟出一台或者多台虚拟的计算机,而这些虚拟机就像真正的计算机那样工作,虚拟机上可以安装操作系统和应用程序,虚拟机还可访问网络资源。对于在虚拟机中运行的应用程序而言,虚拟机就像是在真正的计算机中工作。

[0041] 硬件层:虚拟化环境运行的硬件平台。其中,如图1所示,硬件层可包括多种硬件,例如,某物理主机的硬件层可包括CPU、内存、网卡、存储器、高速/低速输入/输出(I/O, Input/Output)设备,及具有特定处理功能的其它设备。

[0042] 宿主机(Host):作为管理层,用以完成硬件资源的管理、分配;为虚拟机呈现虚拟硬件平台;实现虚拟机的调度和隔离。例如,如图1所示,Host内可设置虚拟机监控器(VMM)。其中,虚拟硬件平台对其上运行的各个虚拟机提供各种硬件资源,如提供虚拟处理器(VCPU, virtual CPU)、虚拟内存、虚拟磁盘、虚拟网卡等等。

[0043] 可以理解的是,本发明实施例可以应用于xen、KVM(Kernel-based Virtual Machine,基于内核的虚拟机)等虚拟机平台中,本发明实施例对此不作限制。

[0044] 本发明的实施例提供一种数据迁移方法,可应用于图2所示的数据迁移系统,该系统包括源主机21和目的主机22。

[0045] 其中,源主机21内运行有应用A,该应用A为创建有enclave(内存保护区)的任意应用,也就是说,应用A中的enclave代码是在源主机21的EPC中运行的,运行过程中产生的运行状态数据存储存储在EPC中。

[0046] 那么,当需要将应用A迁移至目的主机22时,通常是由源主机21的操作系统访问源主机21的内存,将内存中存储的应用A的代码以及运行状态数据等数据发送至目的主机22。而内存中EPC内存存储的上述运行状态数据只允许应用A的enclave代码通过调用源主机21的CPU才能访问,因此,该EPC内的数据无法发送至目的主机22,那么,目的主机22根据源主机21发送的数据恢复出的应用A的运行状态,与源主机21内运行的应用A的运行状态可能不同。

[0047] 对此,在本发明实施例提供的数据迁移方法中,在每一个创建有enclave的目标应用的enclave内,例如,图2中的应用A,预先创建一个控制线程,由于该控制线程位于应用A的enclave内,即控制线程的代码也是应用A的enclave代码,因此,该控制线程可访问EPC内应用A的运行状态数据,并将该运行状态数据写入除EPC之外的目标内存中,即可以由源主机21的操作系统访问的内存中。并且,当上述运行状态数据迁移至目的主机后,该控制线程还可以用于将迁移来的运行状态数据恢复至目的主机内应用A的enclave所在的EPC中。

[0048] 这样,当源主机21获取到迁移指令(该迁移指令用于指示将创建有enclave的目标应用,例如,应用A,迁移至目的主机22)后,由于应用A的enclave内的控制线程具有访问EPC的访问权限,因此,源主机21可以调用该控制线程,将EPC内应用A的运行状态数据写入源主机21的目标内存;由于目标内存中的数据是允许源主机21的操作系统访问的,因此,后续源主机21便可以沿用现有的数据迁移方法,将已写入目标内存中的上述运行状态数据,以及原本就存储在目标内存中的应用A的代码等相关数据发送给目的主机22。

[0049] 目的主机22接收到上述源主机21发送的应用A的相关数据后,可以先为应用A在目的主机22的EPC中恢复应用A的enclave,进而在该enclave内创建应用A的控制线程,由于该控制线程具有访问EPC的访问权限,因此,可由创建出的控制线程将上述运行状态数据复制到应用A的enclave所在的EPC中,从而恢复应用A中enclave内的运行状态。

[0050] 这样,通过上述方法可以在应用迁移的过程中实现EPC内的数据迁移,使得应用在迁移前后的运行状态等数据保持一致。

[0051] 当然,上述控制线程还可以对EPC目标应用的运行状态数据执行加密操作和数字签名操作等保密措施,从而保证迁移过程中运行状态数据的机密性和合法性,后续实施例中将对对此详细阐述,故此处不再赘述。

[0052] 另外,本发明实施例提供的数据迁移方法不仅适用于云虚拟化环境下虚拟机的迁移过程中,还适用于任意两台物理主机之间对含有enclave的应用的迁移过程,本发明实施例对此不作任何限制,后续实施例中以虚拟机的迁移过程为例,举例说明本发明实施例提供的数据迁移方法。

[0053] 如图3所示,为本发明实施例提供的一种数据迁移方法的交互示意图,该方法包括:

[0054] 301、源主机获取迁移指令,该迁移指令用于指示源主机将创建有enclave的目标应用迁移至目的主机。

[0055] 以虚拟机迁移为例,源主机上运行有Host,Host上运行有至少一个虚拟机,而每个虚拟机内可运行至少一个应用。那么,将目标虚拟机(目标虚拟机为上述至少一个虚拟机中的一个)迁移至目的主机时,需要将目标虚拟机内的应用也迁移至目的主机,目标虚拟机内的应用中可能包括创建有enclave的目标应用。

[0056] 此时,如图4所示,Host内的VMM可以向目标虚拟机发送迁移指令,以指示目标虚拟机:源主机准备将目标应用,例如应用A,迁移至目的主机。

[0057] 或者,目标虚拟机也可以通过轮询监测的方式,定时的从VMM中查询VMM是否生成迁移指令,如果生成上述迁移指令,则从VMM中获取该迁移指令,本发明实施例对此不作任何限定。

[0058] 302、源主机调用enclave驱动,向目标应用的enclave内的控制线程发送预置的迁移信号。

[0059] 目标虚拟机获取到上述迁移指令后,检查目标虚拟机内是否创建了包含enclave的应用,对于包含enclave的应用,例如图4中的应用A,该应用A一般在其enclave内需要运行 $N(N \geq 1)$ 个工作线程,而在本发明实施例中,在应用A的enclave内预先设置了一个控制线程,该控制线程专门用于对该enclave所在的EPC区域内的数据执行数据迁移。

[0060] 其中,上述控制线程执行的具体代码是预先编写在应用A的enclave中的,这部分代码专门用于迁移EPC内在该enclave中产生的运行状态数据,那么,当源主机获取到上述迁移指令后,可创建一个新的线程专门执行上述预先编写的代码,此时该新的线程即为上述工作线程,该工作线程接收到上述迁移信号后执行对应的代码,以完成下述步骤303-304的数据迁移过程,直至该数据迁移过程结束时,上述工作线程结束运行。

[0061] 那么,如果目标虚拟机内创建了包含enclave的应用,例如,应用A,则如图4所示,目标虚拟机可调用目标虚拟机操作系统内的enclave驱动,向上述应用A的enclave内的控制线程发送预置的迁移信号,以触发上述控制线程执行上述数据迁移过程。

[0062] 示例性的,该迁移信号可以为本领域技术人员根据实际经验预先定义的信号,本发明实施例对此不作任何限定。

[0063] 303、源主机调用该控制线程,以从EPC内获取目标应用的运行状态数据。

[0064] 其中,运行状态数据具体可以为目标应用的enclave代码在其enclave内运行时产生的栈数据、堆数据和SSA数据等,本发明实施例对此不作任何限制。

[0065] 具体的,上述应用A的enclave内的控制线程接收到迁移信号后,如图5所示,可执行下述步骤501-506,访问该enclave所在的EPC内应用A的运行状态数据。

[0066] 501、源主机调用控制线程,以将目标应用的全局状态设置为迁移状态。

[0067] 具体的,应用A的enclave内可以设置一个全局标识,该全局标识用于指示应用A的全局状态,这个全局标识是上述 N 个工作线程都可以查询到的。那么,上述enclave内的控制线程接收到迁移信号后,控制线程可将应用A的全局状态设置为迁移状态,例如,将全局标识设置为1,即指示当前需要对上述enclave所在的EPC内应用A的运行状态数据执行数据迁移。

[0068] 502、源主机根据全局状态,将 N 个工作线程中每个工作线程的本地状态设置为空闲状态。

[0069] 对于 N 个工作线程中的每个工作线程,源主机都预先设置有一个本地标识,该本地标识用于指示该工作线程的本地状态。当该工作线程启动时,该工作线程会将自身的本地状态置为忙碌状态(busy),即指示该工作线程正在运行,而工作线程在运行的过程中可能会修改EPC内应用A的运行状态数据。

[0070] 因此,为了保证应用A在迁移前后的运行状态一致,在本发明实施例中,当该工作

线程启动时,该工作线程会将自身的本地状态置为忙碌状态,进而,该工作线程会查询当前的全局标识,若全局标识为1(即全局状态为迁移状态),则该工作线程可以将与其对应的本地状态设置为空闲状态(free),当该工作线程的本地状态设置为空闲状态时,停止执行该工作线程,这样可以避免应用A在迁移的过程中,enclave内的任意工作线程运行时修改了EPC内应用A的运行状态数据,从而导致应用A在迁移前后的运行状态不一致的问题。

[0071] 503、源主机调用控制线程,以确定N个工作线程中每个工作线程的本地状态均为空闲状态。

[0072] 对于enclave内的控制线程,当控制线程将应用A的全局状态设置为迁移状态后,监测上述N个工作线程的本地状态。如果N个工作线程中的任意工作线程的本地状态为忙碌状态,则说明该工作线程有可能正在修改EPC内应用A的运行状态数据,此时,控制线程需要等待该工作线程的本地状态转变为空闲状态,直到控制线程确定上述N个工作线程的本地状态都为空闲状态时,可继续执行下述步骤504-506。

[0073] 504、源主机调用控制线程,以通过源主机的CPU访问EPC内目标应用的运行状态数据。

[0074] 由于控制线程位于应用A的enclave内,因此,该控制线程具有访问该enclave所在的EPC的权限,那么,控制线程可以通过源主机的CPU,访问该enclave所在的EPC内应用A的运行状态数据,进而复制该应用A的运行状态数据。

[0075] 505、源主机内的控制线程对上述运行状态数据执行加密操作。

[0076] 506、源主机内的控制线程对加密后的运行状态数据执行数字签名操作。

[0077] 在步骤505和506中,源主机可以通过enclave的remote attestation(远程认证)技术,从预置的存储位置获取加密密钥和签名密钥,然后,使用加密密钥对上述应用A的运行状态数据执行加密操作,再使用签名密钥对加密后应用A的运行状态数据执行数字签名操作。

[0078] 后续将经过加密和签名的运行状态数据写入目标内存后,没有加密密钥和签名密钥的用户无法读取和修改该运行状态数据,从而提高了数据迁移过程中enclave内产生的运行状态数据的保密性和完整性。

[0079] 至此,通过执行步骤501-506,控制线程通过调用源主机的CPU,访问EPC内目标应用的运行状态数据。

[0080] 304、源主机调用控制线程,以将上述运行状态数据写入目标内存。

[0081] 其中,本发明实施例中涉及的目标内存,是指源主机的内存中除上述EPC之外的区域,该区域可由源主机的操作系统访问。

[0082] 具体的,控制线程将经过加密和数字签名的运行状态数据写入目标内存,这样,运行状态数据虽在被写入可以由操作系统访问的目标内存中,但是,由于该运行状态数据已经被加密和数字签名,因此,可提高位于目标内存中的运行状态数据的安全性。

[0083] 305、源主机将目标应用的运行状态数据发送至目的主机。

[0084] 在源主机的目标内存中,还存储有应用A的代码以及应用A的enclave创建记录(该enclave创建记录中记录有应用A内创建的enclave的内存地址)等相关数据。在步骤305中,源主机可以将这些数据、目标应用的运行状态数据以及目标虚拟机的相关数据一同发送至目的主机,由目的主机恢复上述目标虚拟机,并在目标虚拟机内恢复应用A,以实现应用A的

迁移过程。

[0085] 仍如图3所示,为本发明实施例提供一种数据迁移方法,该方法包括:

[0086] 601、目的主机从源主机获取目标应用的运行状态数据。

[0087] 602、目的主机从源主机获取目标应用的enclave创建记录,该enclave创建记录中记录有目标应用的enclave的内存地址。

[0088] 具体的,源主机可以将目标虚拟机内目标应用的代码(包括在enclave内运行的enclave代码以及在enclave外运行的代码)、运行状态数据和enclave创建记录等目标虚拟机的相关信息同时发给目的主机,目的主机同时获取到上述运行状态数据和enclave创建记录,其中,上述运行状态数据为加密状态的。

[0089] 603、目的主机根据上述内存地址在目的主机的内存的EPC中恢复目标应用的enclave。

[0090] 604、目的主机在目标应用的enclave中创建目标应用的控制线程。

[0091] 605、目的主机调用控制线程,以将上述运行状态数据写入EPC中。

[0092] 目的主机接收到上述目标虚拟机的相关信息后,可以先在目的主机的host上创建目标虚拟机,进而,根据接收到的目标应用的代码在新创建的目标虚拟机中创建一个初始目标应用,此时的目标应用的运行状态可以为一个预设的初始值。

[0093] 另外,由于目标应用中可能有一部分代码是并不是运行在目标应用的enclave内的,因此,目的主机的操作系统对这部分代码运行时产生的运行状态数据是具有访问权限的,那么,目的主机可以调用其操作系统在初始目标应用中先恢复这部分运行状态数据。

[0094] 而对于运行在目标应用的enclave内的enclave代码产生的运行状态数据,由于只有位于目标应用的enclave内的enclave代码对其具有访问权限,因此,目的主机可以先在自身内存的EPC中为目标应用创建其enclave,即目标应用的enclave。

[0095] 具体的,在步骤603中,目的主机可以根据目标应用的enclave创建记录中记载的内存地址,在目的主机的EPC中创建一个新的enclave,并将目标应用的enclave代码加载到这个新的enclave中,作为恢复后该目标应用的enclave。

[0096] 但是,该目标应用的enclave的运行状态还未恢复,因此,在步骤604中,目的主机在上述目标应用的enclave中为目标应用创建一个控制线程。进而,在步骤605中,由该控制线程将步骤601中获取到的enclave代码产生的运行状态数据写入该enclave所在的EPC中,从而恢复整个目标应用的运行状态。

[0097] 606、目的主机调用控制线程,以对上述运行状态数据执行数字签名认证操作和解密操作。

[0098] 可选的,如果源主机在发送上述enclave代码产生的运行状态数据时已经对该运行状态数据执行了加密和数字签名操作,那么,目的主机为了恢复目标应用的运行状态,还需要获取加密时使用的密密钥和数字签名时使用的签名密钥,进而,由于上述控制线程使用加密密钥对目标应用的运行状态数据执行解密操作,再使用签名密钥对目标应用的运行状态数据执行签名认证操作,从而恢复出目标应用的enclave内的运行状态,使得目的主机上运行的目标应用的运行状态与迁移之前源主机上运行的目标应用的运行状态相同。

[0099] 可以理解的是,上述源主机、目的主机等为了实现上述功能,其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到,结合本文中所公开

的实施例描述的各示例的单元及算法步骤,本发明实施例能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本发明实施例的范围。

[0100] 本发明实施例可以根据上述方法示例对上述源主机、目的主机等进行功能模块的划分,例如,可以对应各个功能划分各个功能模块,也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现,也可以采用软件功能模块的形式实现。需要说明的是,本发明实施例中对模块的划分是示意性的,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式。

[0101] 在采用对应各个功能划分各个功能模块的情况下,图6示出了上述实施例中所涉及的源主机的一种可能的结构示意图,该源主机包括:获取单元71,执行单元72,发送单元73和加密单元74。

[0102] 获取单元71用于支持源主机执行图3中的过程301;执行单元72用于支持源主机执行图3中的过程303-304,以及图5中的过程501-504;发送单元73用于支持源主机执行图3中的过程302和305;加密单元74用于支持源主机执行图5中的过程505-506。其中,上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述,在此不再赘述。

[0103] 在采用对应各个功能划分各个功能模块的情况下,图7示出了上述实施例中所涉及的目的主机的一种可能的结构示意图,该目的主机包括:获取单元81,恢复单元82,创建单元83和复制单元84。

[0104] 获取单元81用于支持目的主机执行图6中的过程601;恢复单元82用于支持目的主机执行图6中的过程602-603;创建单元83用于支持目的主机执行图6中的过程604;复制单元84用于支持目的主机执行图6中的过程605-606。其中,上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述,在此不再赘述。

[0105] 在采用集成的单元的情况下,图8示出了上述实施例中所涉及的源主机(或目的主机)的一种可能的结构示意图。源主机(或目的主机)包括:处理模块1302和通信模块1303。处理模块1302用于对源主机(或目的主机)的动作进行控制管理。通信模块1303用于支持源主机(或目的主机)与其他网络实体的通信。源主机(或目的主机)还可以包括存储模块1301,用于存储源主机(或目的主机)的程序代码和数据。

[0106] 其中,处理模块1302可以是处理器或控制器,例如可以是中央处理器(Central Processing Unit,CPU),通用处理器,数字信号处理器(Digital Signal Processor,DSP),专用集成电路(Application-Specific Integrated Circuit,ASIC),现场可编程门阵列(Field Programmable Gate Array,FPGA)或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本发明实施例公开内容所描述的各种示例性的逻辑方框,模块和电路。所述处理器也可以是实现计算功能的组合,例如包含一个或多个微处理器组合,DSP和微处理器的组合等等。通信模块1303可以是收发器、收发电路或通信接口等。存储模块1301可以是存储器。

[0107] 当源主机(或目的主机)内运行有虚拟机时,源主机(或目的主机)的架构示意图如图1所示。

[0108] 进一步地,本发明实施例还提供一种数据迁移系统,该系统包括如图2所示的源主机21和目的主机22。

[0109] 在上述实施例中,可以全部或部分的通过软件,硬件,固件或者其任意组合来实现。当使用软件程序实现时,可以全部或部分地以计算机程序产品的形式出现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时,全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))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、服务器或数据中心传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。该可用介质可以是磁性介质,(例如,软盘、硬盘、磁带)、光介质(例如,DVD)或者半导体介质(例如固态硬盘 Solid State Disk(SSD))等。

[0110] 以上所述,仅为本申请的具体实施方式,但本申请的保护范围并不局限于此,任何在本申请揭露的技术范围内的变化或替换,都应涵盖在本申请的保护范围之内。因此,本申请的保护范围应以所述权利要求的保护范围为准。

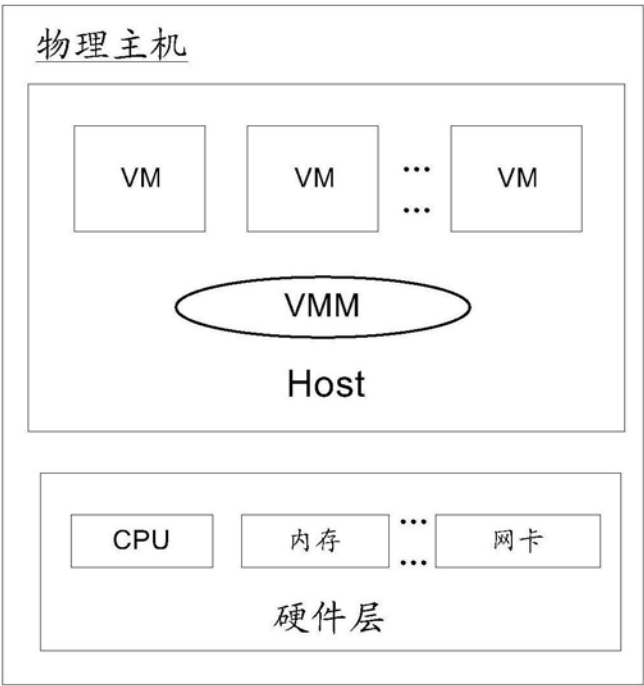


图1

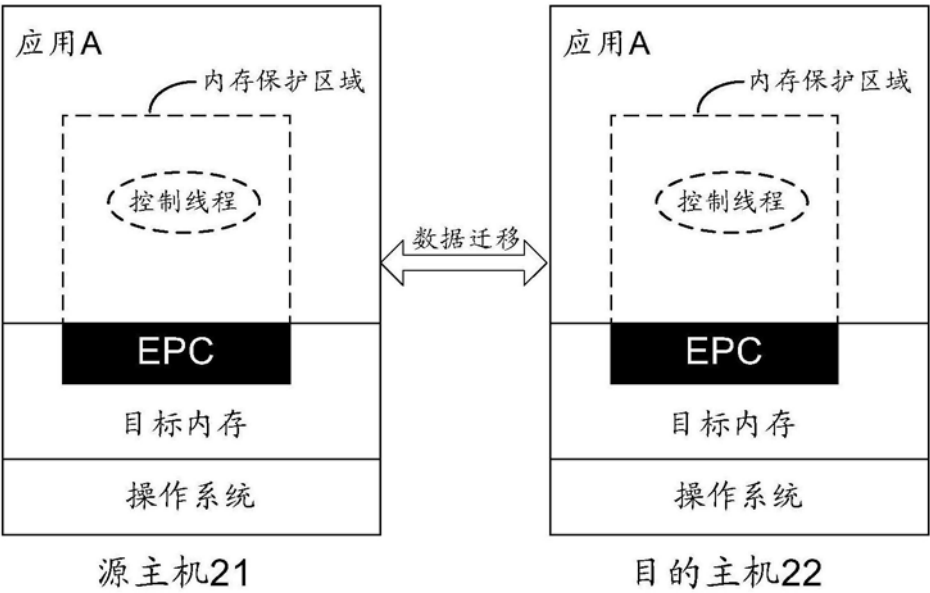


图2

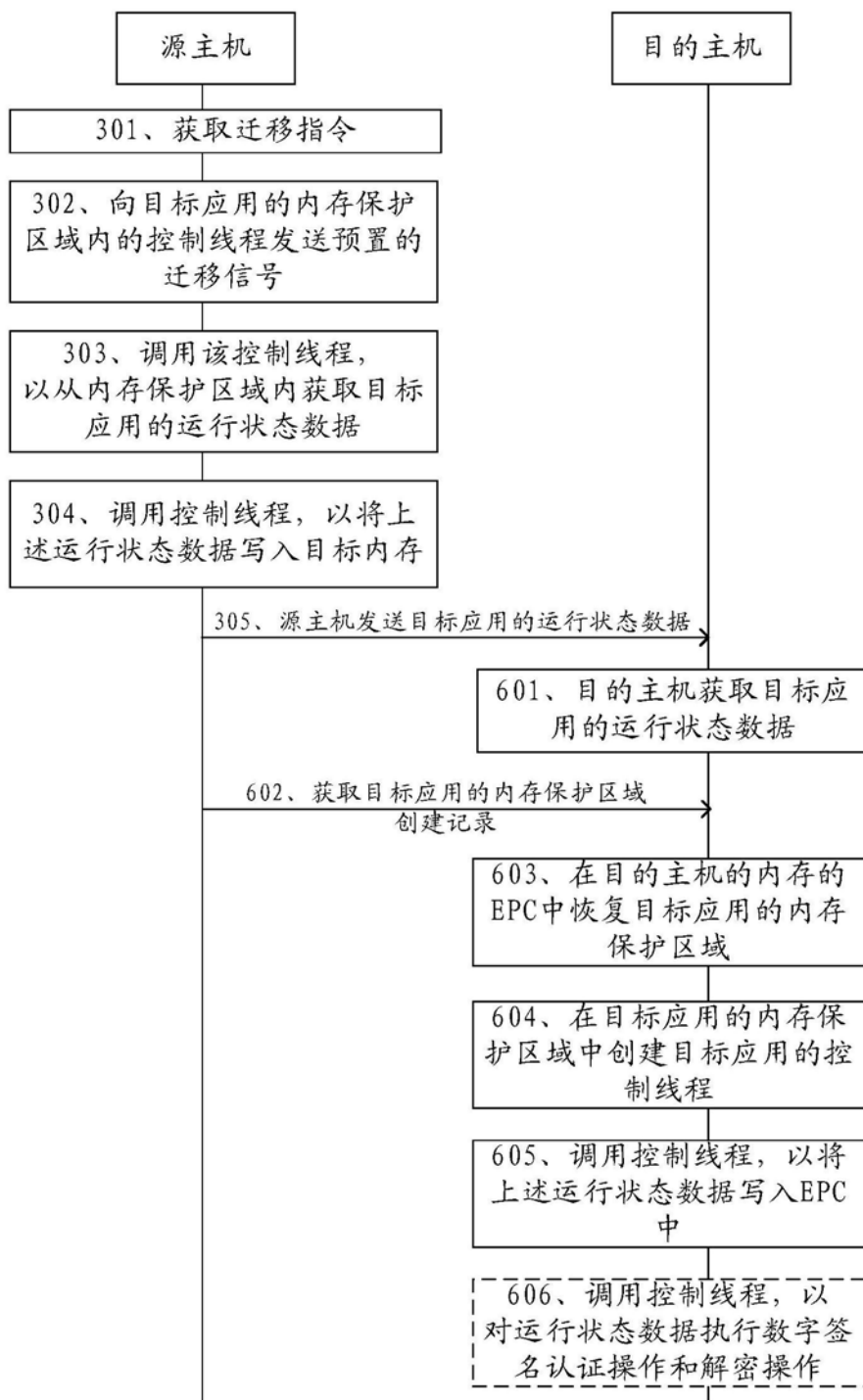


图3

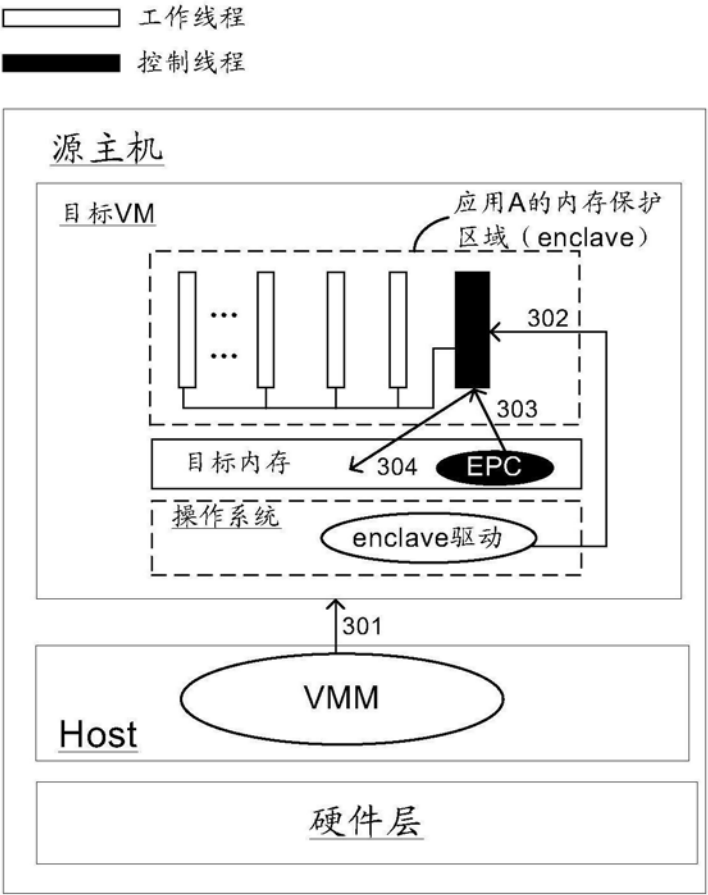


图4

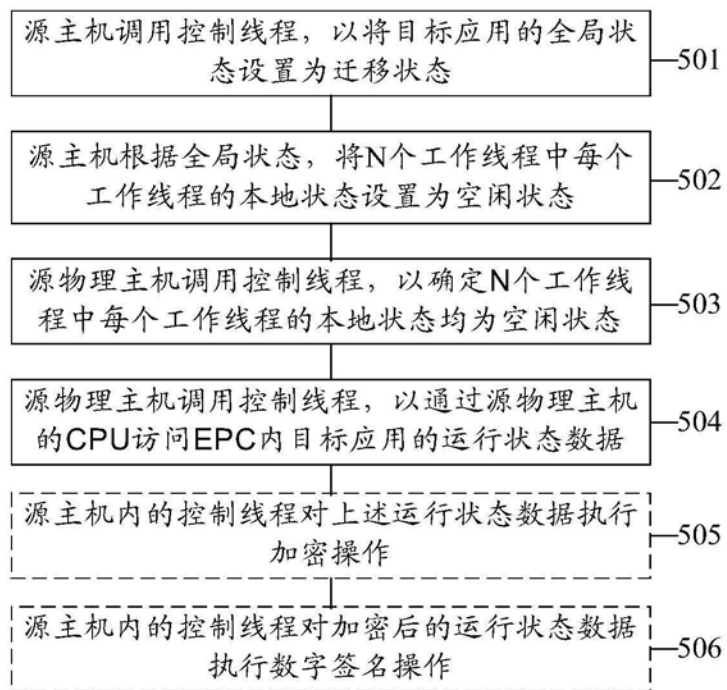


图5

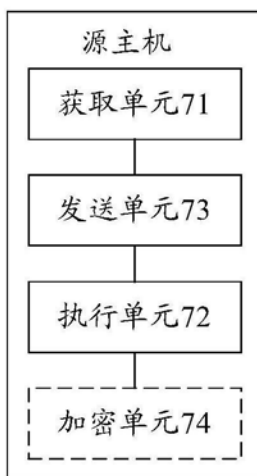


图6

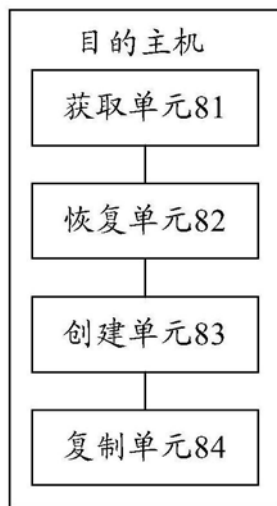


图7

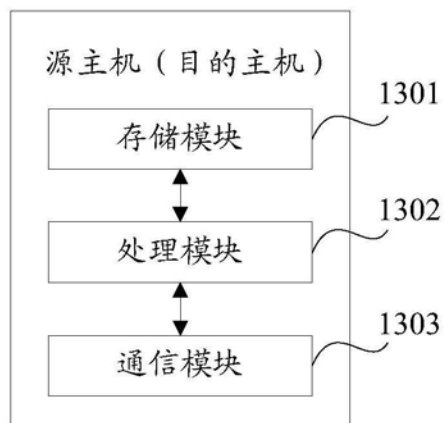


图8