(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102726027 B
(45)授权公告日 2014.05.21

(21)申请号 201180003438.X
(22)申请日 2011.12.28
(85)PCT国际申请进入国家阶段日
2012.03.01
(86)PCT国际申请的申请数据
PCT/CN2011/084823 2011.12.28
(87)PCT国际申请的公布数据
WO2013/097117 ZH 2013.07.04
(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 刘新保
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
(56)对比文件
WO 2011156261 A,2011.12.15, 说明书第[0019]－[0033]段,图1A,1B, 图2.
US 7865712 B2,2011.01.04, 全文.
CN 102163266 A,2011.08.24, 全文.
审查员 李晓

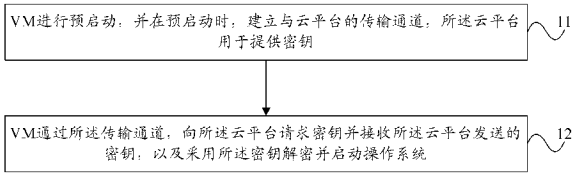
权利要求书2页 说明书9页 附图4页

(54)发明名称

虚拟机全盘加密下预启动时的密钥传输方法和设备

(57)摘要

本发明提供一种虚拟机全盘加密下预启动时的密钥传输方法和设备。该方法包括虚拟机进行预启动,所述虚拟机处于全盘加密状态;所述虚拟机在预启动时,建立与云平台的传输通道,所述云平台用于提供密钥;所述虚拟机通过所述传输通道,向所述云平台请求密钥并接收所述云平台发送的密钥;所述虚拟机采用所述密钥解密并启动操作系统。本发明实施例可以在虚拟机预启动阶段实现密钥传输,进而启动虚拟机。



CN 102726027 B

1. 一种虚拟机全盘加密下预启动时的密钥传输方法，其特征在于，包括：

虚拟机进行预启动，所述虚拟机处于全盘加密状态；

所述虚拟机在预启动时，建立与云平台的传输通道，所述云平台用于提供密钥；

所述虚拟机通过所述传输通道，向所述云平台请求密钥并接收所述云平台发送的密钥；

所述虚拟机采用所述密钥解密并启动操作系统；

其中，所述建立与云平台的传输通道，包括：

确定超级监视器内为虚拟机分配的传输通道；

通过所述超级监视器内为虚拟机分配的传输通道，得到虚拟机与云平台之间的传输通道；

或者，

设置启动加载操作系统，并在所述启动加载操作系统启动后向 DHCP 服务器申请 IP，根据所述 IP 地址建立与云平台的传输通道；

其中，当所述建立与云平台的传输通道，为确定超级监视器内为虚拟机分配的传输通道；通过所述超级监视器内为虚拟机分配的传输通道，得到虚拟机与云平台之间的传输通道时，所述向所述云平台请求密钥并接收所述云平台发送的密钥，包括：

通过所述超级监视器内的传输通道，向云平台发送密钥请求消息，所述密钥请求消息中携带虚拟机的标识信息；

接收云平台返回的密钥，所述密钥为云平台根据所述虚拟机的标识信息确定的；

当所述建立与云平台的传输通道，为设置启动加载操作系统，并在所述启动加载操作系统启动后向 DHCP 服务器申请 IP，根据所述 IP 地址建立与云平台的传输通道时，所述向所述云平台请求密钥并接收所述云平台发送的密钥，包括：

通过建立的 IP 通道，向云平台发送密钥请求消息，所述密钥请求消息中携带虚拟机的标识信息；

接收云平台返回的密钥，所述密钥为云平台根据所述虚拟机的标识信息确定的。

2. 根据权利要求 1 所述的方法，其特征在于，所述通过所述超级监视器内的传输通道，向云平台发送密钥请求消息，包括：

虚拟机通过所述超级监视器内的传输通道，向宿主机发送密钥请求消息，并经由所述宿主机和云平台间的 IP 连接通道，将所述密钥请求消息发送给云平台，所述宿主机在所述虚拟机预启动前完成启动并获取 IP 地址以及与云平台建立 IP 连接通道。

3. 根据权利要求 1 所述的方法，其特征在于，所述虚拟机进行预启动之前，所述方法还包括：

所述虚拟机在上次正常启动操作系统后，通过超级监视器内的传输通道，向云平台发送携带虚拟机的标识信息的密钥请求消息，接收所述云平台发送的根据所述虚拟机的标识信息确定的密钥，并采用所述密钥对所述虚拟机的数据进行全盘加密处理；或者，

所述虚拟机在上次正常启动操作系统后，获取 IP 地址，根据所述 IP 地址建立与云平台的 IP 连接，通过所述 IP 连接向云平台发送携带虚拟机的标识信息的密钥请求消息，接收所述云平台发送的根据所述虚拟机的标识信息确定的密钥，并采用所述密钥对所述虚拟机的数据进行全盘加密处理。

4. 一种虚拟机全盘加密下预启动时的密钥传输设备，其特征在于，包括：建立模块，用于进行处于全盘加密状态的虚拟机的预启动操作，并在预启动时，建立与云平台的传输通道，所述云平台用于提供密钥；

传输模块，用于通过所述传输通道，向所述云平台请求密钥并接收所述云平台发送的密钥；

解密模块，用于采用所述密钥解密并启动操作系统；

其中，所述建立模块为启动加载模块，所述启动加载模块用于确定超级监视器内为虚拟机分配的传输通道；通过所述超级监视器内为虚拟机分配的传输通道，得到虚拟机与云平台之间的传输通道；

或者，

所述建立模块为启动加载系统模块，所述启动加载系统模块用于在所述启动加载操作系统启动后向 DHCP 服务器申请 IP，根据所述 IP 地址建立与云平台的传输通道；

其中，当所述建立模块为启动加载模块，所述启动加载模块用于确定超级监视器内为虚拟机分配的传输通道；通过所述超级监视器内为虚拟机分配的传输通道，得到虚拟机与云平台之间的传输通道时，所述传输模块具体用于：

通过所述超级监视器内的传输通道，向云平台发送密钥请求消息，所述密钥请求消息中携带虚拟机的标识信息；

接收云平台返回的密钥，所述密钥为云平台根据所述虚拟机的标识信息确定的；

当所述建立模块为启动加载系统模块，所述启动加载系统模块用于在所述启动加载操作系统启动后向 DHCP 服务器申请 IP，根据所述 IP 地址建立与云平台的传输通道时，所述传输模块具体用于：

通过建立的 IP 通道，向云平台发送密钥请求消息，所述密钥请求消息中携带虚拟机的标识信息；

接收云平台返回的密钥，所述密钥为云平台根据所述虚拟机的标识信息确定的。

5. 根据权利要求 4 所述的设备，其特征在于，所述传输模块具体用于：通过所述超级监视器内的传输通道，向宿主机发送密钥请求消息，并经由所述宿主机和云平台间的 IP 连接通道，将所述密钥请求消息发送给云平台，所述宿主机在所述虚拟机预启动前完成启动并获取 IP 地址以及与云平台建立 IP 连接通道。

6. 根据权利要求 4 所述的设备，其特征在于，还包括：

加密模块，用于在上次正常启动操作系统后，通过超级监视器内的传输通道，向云平台发送携带虚拟机的标识信息的密钥请求消息，接收所述云平台发送的根据所述虚拟机的标识信息确定的密钥，并采用所述密钥对所述虚拟机的数据进行全盘加密处理；或者，在上次正常启动操作系统后，获取 IP 地址，根据所述 IP 地址建立与云平台的 IP 连接，通过所述 IP 连接向云平台发送携带虚拟机的标识信息的密钥请求消息，接收所述云平台发送的根据所述虚拟机的标识信息确定的密钥，并采用所述密钥对所述虚拟机的数据进行全盘加密处理。

虚拟机全盘加密下预启动时的密钥传输方法和设备

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种虚拟机(Virtual Machine,VM)全盘加密下预启动时的密钥传输方法和设备。

背景技术

[0002] 云计算场景下，虚拟机(Virtual Machine，VM)的磁盘数据，包括系统盘和数据盘的数据会存在安全风险。如果能对VM的数据进行全盘加密，并且密钥能掌握在用户自己手中的话，非授权人员就不能获得用户的数据，这样就会极大程度上保护用户在云中的敏感数据。

[0003] 传统的全盘加密技术作为终端安全的一种解决方案，技术已经成熟，传统技术中，可以在启动操作系统前，也就是预启动(Pre-boot)阶段，由启动加载(boot loader)程序根据用户输入的密码生成密钥，并用密钥解密磁盘上的数据，解密的数据中包括操作系统(Operation System,OS)，在操作系统解密后可以启动操作系统。

[0004] 上述的传统全盘加密技术中，用户是在单一终端上执行的操作，boot loader程序可以获取密钥。但是，云应用场景下，VM所需的密钥需要从外界的云平台处获取，而在VM的操作系统未启动前，VM没有IP地址，无法与外界通信，也就不能获取到密钥，使得VM的操作系统不能被启动，造成VM停留在预启动阶段。

发明内容

[0005] 本发明提供一种虚拟机全盘加密下预启动时的密钥传输方法和设备，实现VM内的boot loader程序可以在预启动阶段获取密钥，进而启动VM的操作系统。

[0006] 本发明提供了一种虚拟机全盘加密下预启动时的密钥传输方法，包括：

[0007] 虚拟机进行预启动，所述虚拟机处于全盘加密状态；

[0008] 所述虚拟机在预启动时，建立与云平台的传输通道，所述云平台用于提供密钥；

[0009] 所述虚拟机通过所述传输通道，向所述云平台请求密钥并接收所述云平台发送的密钥；

[0010] 所述虚拟机采用所述密钥解密并启动操作系统。

[0011] 本发明提供了一种虚拟机全盘加密下预启动时的密钥传输设备，包括：

[0012] 建立模块，用于进行处于全盘加密状态的虚拟机的预启动操作，并在预启动时，建立与云平台的传输通道，所述云平台用于提供密钥；

[0013] 传输模块，用于通过所述传输通道，向所述云平台请求密钥并接收所述云平台发送的密钥；

[0014] 解密模块，用于采用所述密钥解密并启动操作系统。

[0015] 由上述技术方案可知，本发明实施例通过虚拟机在预启动阶段建立与提供密钥的云平台之间的传输通道，可以实现预启动阶段密钥的传输，能够使得虚拟机获取密钥，进而可以解密虚拟机的操作系统，并实现虚拟机的操作系统的启动，避免由于不能获取密钥而

停留在预启动阶段。

附图说明

[0016] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0017] 图 1 为本发明虚拟机全盘加密下预启动时的密钥传输方法的一实施例的流程示意图；

[0018] 图 2 为本发明虚拟机全盘加密下预启动时的密钥传输方法的另一实施例的流程示意图；

[0019] 图 3 为图 2 对应的系统结构示意图；

[0020] 图 4 为本发明虚拟机全盘加密下预启动时的密钥传输方法的另一实施例的流程示意图；

[0021] 图 5 为图 4 对应的系统结构示意图；

[0022] 图 6 为本发明中加密方法的一实施例的流程示意图；

[0023] 图 7 为本发明中加密方法的另一实施例的流程示意图；

[0024] 图 8 为本发明虚拟机全盘加密下预启动时的密钥传输设备的结构示意图。

具体实施方式

[0025] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，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，都属于本发明保护的范围。

[0026] 图 1 为本发明虚拟机全盘加密下预启动时的密钥传输方法的一实施例的流程示意图，包括：

[0027] 步骤 11 :VM 进行预启动，并在预启动时，建立与云平台的传输通道，所述云平台用于提供密钥；

[0028] 其中，VM 在预启动时处于全盘加密状态，即 VM 的操作系统处于加密状态，需要解密出 VM 的操作系统才能完成 VM 的启动，否则将如现有技术停留在预启动状态。

[0029] 该 VM 是指能够被用户使用的虚拟机，例如，对于 XEN 场景下，VM 是指 domain U，另外，在 XEN 场景下，还存在一种特殊的虚拟机 :宿主机 (Domain 0)，该宿主机并不是被用户使用的虚拟机，而是管理各 Domain U 的虚拟机。因此，在 XEN 场景下，上述的 VM 是指 Domain U。可以理解的是，对于其他虚拟化平台，不区分 Domain 0、Domain U 的场景，例如，VMware ESXi 场景下，Domain 0 的功能可以是由 hypervisor 执行，而由 Domain U 执行的操作可以是由 hypervisor 上的虚拟机执行。

[0030] 通常来讲，Domain 0 的操作系统是不加密的，因此当云平台向 Domain 0 下发启动虚拟机指令后，Domain 0 的操作系统就会启动，而 Domain U 的系统盘，即操作系统所在的盘是加密的，需要解密后才会启动。每个 Domain U 的密钥可以保存在云平台内。

[0031] 云平台中与 VM 磁盘加密相关的模块可以进一步细分为密钥管理模块和加密管理模块。其中，密钥管理模块用于对各 Domain U 的密钥进行管理，例如，生成每个 Domain U 对应的密钥，更新密钥、存储密钥、备份密钥、恢复密钥等。加密管理模块用于确定管理策略，例如，配置需要加密的 Domain U 的信息，配置 Domain U 上需要加密的卷的信息等。另外，加密管理模块还负责将密钥管理模块中的密钥传递给 Domain U。

[0032] 另外，上述的传输通道可以是通过超级监视器 (hypervisor) 的传输通道，或者是采用 IP 地址直接与云平台建立的传输通道。具体内容可以参见后续实施例。

[0033] 步骤 12 ：VM 通过所述传输通道，向所述云平台请求密钥并接收所述云平台发送的密钥，以及采用所述密钥解密并启动操作系统。

[0034] 由于云平台和 VM 间已经建立了传输通道，云平台便可以通过该传输通道将密钥传输给 VM。

[0035] VM 在获取到密钥后，可以根据获取的密钥解密操作系统所在的系统盘，得到操作系统后启动操作系统，而不是如现有技术中的停留在预启动阶段。

[0036] 本实施例通过在预启动阶段建立与提供密钥的云平台之间的传输通道，可以实现预启动阶段密钥的传输，能够使得虚拟机获取密钥，进而可以解密虚拟机的操作系统，并实现虚拟机的操作系统的启动，避免由于不能获取密钥而停留在预启动阶段。

[0037] 图 2 为本发明虚拟机全盘加密下预启动时的密钥传输方法的另一实施例的流程示意图，图 3 为图 2 对应的系统结构示意图。本实施例以 XEN 场景，且通过 hypervisor 建立传输通道为例。

[0038] 参见图 3，该系统包括密钥管理模块 31、加密管理模块 32、宿主机 33、虚拟机 34 和超级监视器 (hypervisor)35。密钥管理模块 31 和加密管理模块 32 可以位于云平台内，宿主机 33、虚拟机 34 和超级监视器 35 可以位于云服务器上，一个云平台可以管理多个云服务器。其中的宿主机也就是 Domain 0，虚拟机也就是 Domain U。

[0039] 密钥管理模块用于管理每个虚拟机的密钥，包括密钥的生成、密钥更新、密钥存储、密钥备份、密钥恢复等功能。该密钥管理模块可以是云提供商设置的，也可以是用户自己设置的。例如，在一些应用场景下，如果用户不信任云提供商，要求自己手动输入对应的虚拟机的密钥，那么密钥可以由用户自己管理，此时的密钥管理模块具体可以是自助门户 (portal) 密钥输入系统。

[0040] 加密管理模块，主要是管理需要加密哪个或哪些 VM 以及加密 VM 的哪个或哪些卷，用户可以根据磁盘上数据的敏感程度来选择。同时，该模块也承担密钥的传递功能，将密钥管理模块内的密钥传递给虚拟机使用。

[0041] 宿主机上部署后端密钥传递模块，用于从云平台获取密钥并通过 hypervisor 中的传输通道传输给前端密钥传递模块。

[0042] hypervisor 是一种在虚拟环境中的“元”操作系统，可以访问云服务器上包括磁盘和内存在内的所有物理设备。当云服务器启动并执行 hypervisor 后，hypervisor 会加载所有虚拟机的操作系统同时会分配给每一台虚拟机适量的内存，CPU，网络和磁盘。具体地，hypervisor 可以为开源的 XEN。

[0043] 每个虚拟机上可以部署加密代理 (Agent) 模块，用于进行虚拟机加解密管理，例如，用户通过加密代理模块下发加密指令，根据密钥对 VM 的数据进行加密，或者对加密的

数据根据密钥解密等。本实施例中以加密代理模块中包括 boot loader 模块为例。boot loader 模块用于运行 boot loader 程序，boot loader 程序可以从虚拟机的磁盘上读取包含加密的操作系统的数据，并采用密钥对操作系统进行解密后启动操作系统。具体地，boot loader 模块可以包括前端密钥传递模块和加解密模块，前端密钥传递模块用于获取密钥，加解密模块用于根据前端密钥传递模块得到的密钥对数据进行加解密。另外，在预启动阶段，hypervisor 还可以在虚拟机上虚拟得到虚拟基本输入输出系统 (Virtual Basic Input Output System，vBIOS)。

[0044] 结合图 3 所示的系统，参见图 2，本实施例提供的方法包括：

[0045] 步骤 201：启动过程，其中包括启动加载 (boot loader) 模块运行，boot loader 模块中可以包括加解密模块和前端密钥传递模块。

[0046] 具体可以包括：云服务器启动，启动 Domain 0，并运行 hypervisor。

[0047] 其中，由于 Domain 0 是不加密的，那么云服务器启动后，Domain 0 便会启动，Domain 0 启动后会获取 IP 地址，采用该 IP 地址可以建立与云平台侧的通信连接，具体可以与加密管理模块建立连接，从而可以与云平台交互数据。

[0048] 云平台对 Domain U 进行预启动操作，预启动操作过程中启动 boot loader 模块，并在启动 Domain U 时在 hypervisor 内为每个 Domain U 分配与 Domain0 的传输通道。

[0049] 具体地，预启动操作可以包括：

[0050] 加密管理模块向 Domain 0 发送启动虚拟机指令；

[0051] Domain 0 将该启动虚拟机指令转发给 hypervisor；

[0052] Hypervisor 接收到该启动虚拟机指令后，启动 Domain U 并虚拟出 Domain0 对应的 vBIOS，并加载 Domain U 的系统卷文件，该系统卷文件中包括一部分不被加密的数据，也包括另一部分需要加密的数据，不需要加密的数据例如为 boot loader 程序、磁盘主引导区记录 (Master Boot Record，MBR) 等；需要加密的数据包括 Domain U 的操作系统，还可以包括用户需要加密的数据盘的数据等。对于不需要加密的数据，hypervisor 可以逐一启动这些程序，例如，经过加载，由于 boot loader 程序不需要加密，那么包括 boot loader 程序的 boot loader 模块经过加载后便可以启动。

[0053] 可以理解的是，上述云服务器的启动过程和预启动操作可以采用现有技术实现，具体内容可以参见现有流程。

[0054] hypervisor 可以通过共享内存等方式为 Domain 0 和 Domain U 提供传输通道。例如，在 hypervisor 内为每个 Domain U 分配约定的共享内存空间，该内存空间可以被 Domain 0 和对应的 Domain U 共同使用，使得 Domain U 和 Domain 0 通过对应的内存空间交互数据。

[0055] 步骤 202：boot loader 模块中的加解密模块向前端密钥传递模块发送密钥请求消息。

[0056] 步骤 203：boot loader 模块中的前端密钥传递模块，通过 hypervisor 提供的传输通道，向 Domain 0 的后端密钥传递模块发送密钥请求消息。

[0057] 其中，具体可以 hypervisor 在启动 MBR 后，触发 boot loader 模块发送上述的密钥请求消息。

[0058] 每个 Domain U 内的前端密钥传递模块可以通过分配的共享内存空间，向 Domain 0 发送密钥请求消息。

[0059] 步骤 204 :后端密钥传递模块在密钥请求消息中添加 Domain U 的标识信息后,发送给加密管理模块。

[0060] 其中,可以根据密钥请求消息来自的共享内存的信息确定 Domain U 的标识信息。例如,密钥请求消息来自第一内存,并且 Domain 0 在配置时已经将第一内存分配给第一 Domain U,那么可以确定 Domain U 的标识信息为第一 Domain U 的标识信息。

[0061] 步骤 205 :加密管理模块转发该包含 Domain U 的标识信息的密钥请求消息给密钥管理模块。

[0062] 步骤 206 :密钥管理模块根据 Domain U 的标识信息确定出对应的密钥。

[0063] 其中,密钥管理模块是对各 Domain U 的密钥进行管理的模块,其中会保存每个 Domain U 及其对应的密钥。

[0064] 步骤 207 :密钥管理模块向加密管理模块返回密钥。

[0065] 步骤 208 :加密管理模块向后端密钥传递模块返回密钥。

[0066] 步骤 209 :后端密钥传递模块通过 hypervisor 内的传输通道,向前端密钥传递模块返回密钥。

[0067] 另外,如果是不同的 Domain U 并行进行解密处理,则上述返回密钥的消息中还可以进一步携带对应的 Domain U 的标识信息。当然,如果各 Domain U 是串行进行解密处理,则也可以不携带 Domain U 的标识信息。

[0068] 步骤 210 :前端密钥传递模块将密钥发送给加解密模块。

[0069] 步骤 211 :boot loader 模块中的加解密模块根据前端密钥传递模块接收的密钥,对 Domain U 的操作系统文件进行解密,操作系统解密后启动。

[0070] 其中,boot loader 模块可以首先从磁盘内读取加密的操作系统,之后采用获取的密钥进行解密。

[0071] 本实施例通过在 hypervisor 内建立 Domain 0 和 Domain U 之间的传输通道,可以实现 Domain U 与云平台间的通道连接,从而可以从云平台获取密钥,实现对操作系统的解密和启动。

[0072] 图 4 为本发明虚拟机全盘加密下预启动时的密钥传输方法的另一实施例的流程示意图,图 5 为图 4 对应的系统结构示意图。本实施例以 Domain U 获取 IP 地址并根据 IP 地址与云平台建立传输通道为例。

[0073] 与上一实施例不同的是,本实施例中每个Domain U的系统卷文件中包含的是启动加载系统 (boot loader OS),用以替代上一实施例中的 boot loader 程序。boot loader OS 是一种微操作系统,不仅具有 boot loader 程序的功能,还具有如下功能 :

[0074] (1) 网卡驱动 :能利用 vBIOS 虚拟出来的虚拟网卡功能 ;

[0075] (2) 动态主机配置协议 (Dynamic Host Configuration Protocol, DHCP) 客户端功能 :能向 DHCP 服务器申请分配 IP 地址 ;

[0076] (3)TCP/UDP/IP 协议栈 :能与云平台的加密管理模块建立安全的 IP 通道,例如,安全套接层 (Secure Sockets Layer, SSL) 通道,从而获取密钥。

[0077] 由于设置了上述的boot loader OS,该boot loader OS可以通过虚拟网卡从DHCP服务器申请到 IP 地址,并根据 IP 地址建立与加密管理平台的连接,因此,本实施例中不需要通过 hypervisor 建立传输通道。

[0078] 在云服务器启动后，可以启动 Domain 0。

[0079] 云平台对 Domain U 进行预启动操作，预启动操作过程中启动 boot loader OS 模块。

[0080] 类似对 boot loader 的处理，在系统卷文件中可以设置 boot loader OS，并且 boot loader OS 不加密，因此在预启动过程中可以启动 boot loader OS 模块。

[0081] 之后，参见图 4，本实施例包括：

[0082] 步骤 401：启动加载系统 (boot loader OS) 模块通过虚拟网卡向 DHCP 服务器发送 IP 地址申请消息。

[0083] 步骤 402：DHCP 服务器向 boot loader OS 模块返回分配的 IP 地址。

[0084] 步骤 403：boot loader OS 模块根据获取的 IP 地址与加密管理模块建立传输通道。

[0085] 步骤 404：boot loader OS 模块通过建立的传输通道向加密管理模块发送密钥请求消息，该密钥请求消息中携带 Domain U 的标识信息。

[0086] 步骤 405：加密管理模块向密钥管理模块发送密钥请求消息，其中携带 Domain U 的标识信息。

[0087] 步骤 406：密钥管理模块根据 Domain U 的标识信息确定出对应的密钥，并向加密管理模块返回密钥。

[0088] 步骤 407：加密管理模块通过已经建立的传输通道，向 boot loader OS 模块返回密钥。

[0089] 另外，如果是不同的 Domain U 并行进行解密处理，则上述返回密钥的消息中还可以进一步携带对应的 Domain U 的标识信息。当然，如果各 Domain U 是串行进行解密处理，则也可以不携带 Domain U 的标识信息。

[0090] 步骤 408：boot loader OS 模块采用密钥解密 Domain U 的操作系统并启动。

[0091] 由于 boot loader OS 具有 boot loader 的功能，因此，类似上一实施例中 boot loader 的处理流程可以实现操作系统的解密及启动。

[0092] 本实施例通过设置 boot loader OS，可以获取 IP 地址并建立 Domain 0 和 Domain U 之间的传输通道，可以实现 Domain U 与云平台间的通道连接，从而可以从云平台获取密钥，实现对操作系统的解密和启动。

[0093] 上述描述了解密流程，对于加密流程可以如下执行。可以理解的是，下述的加密流程可以应用在上述的解密流程之前，即虚拟机在正常启动操作系统后，可以对数据进行全盘加密，全盘加密后可以关闭虚拟机，在下次需要再次启动虚拟机时，再次启动虚拟机的预启动阶段便可以采用上述的解密流程进行处理。

[0094] 图 6 为本发明中加密方法的一实施例的流程示意图，包括：

[0095] 步骤 601：加密代理模块的加解密模块接收卷加密指令。

[0096] 步骤 602：加解密模块向加密代理模块的前端密钥传递模块发送申请密钥请求消息。

[0097] 步骤 603：加密代理模块的前端密钥传递模块通过 hypervisor 内的传输通道，向 Domain 0 内的后端密钥传递模块发送申请密钥请求消息。

[0098] 步骤 604：后端密钥传递模块在申请密钥请求消息中添加 Domain U 的标识信息

后，发送给加密管理模块。

[0099] 其中，后端密钥传递模块可以根据共享内存的信息确定 Domain U 的标识信息。

[0100] 步骤 605 ：加密管理模块转发该包含 Domain U 的标识信息的申请密钥请求消息给密钥管理模块。

[0101] 步骤 606 ：密钥管理模块根据 Domain U 的标识信息，生成对应的密钥。

[0102] 步骤 607 ：密钥管理模块向加密管理模块返回密钥。

[0103] 步骤 608 ：加密管理模块向后端密钥传递模块返回密钥。

[0104] 步骤 609 ：后端密钥传递模块通过 hypervisor 内的传输通道，向前端密钥传输模块返回密钥。

[0105] 另外，如果是不同的 Domain U 并行进行解密处理，则上述返回密钥的消息中还可以进一步携带对应的 Domain U 的标识信息。当然，如果各 Domain U 是串行进行解密处理，则也可以不携带 Domain U 的标识信息。

[0106] 步骤 610 ：前端密钥传递模块将密钥发送给加解密模块。

[0107] 步骤 611 ：加解密模块采用密钥加密卷，也就是采用密钥对虚拟机的数据进行全盘加密。

[0108] 本实施例中 hypervisor 内传输通道的建立以及 Domain 0 对 Domain U 的标识信息的确定可以参见图 2 所示的实施例。

[0109] 图 7 为本发明中加密方法的另一实施例的流程示意图，由于加密时 Domain U 的操作系统已经启动，因此，Domain U 可以获取 IP 地址，进而可以建立与云平台侧的连接。本实施例以 Domain U 与云平台之间建立连接为例。本实施例包括 ：

[0110] 步骤 701 ：加密代理模块接收卷加密指令。

[0111] 步骤 702 ：加密代理模块通过已经建立的传输通道，向加密管理模块发送申请密钥请求消息，其中包含 Domain U 的标识信息。

[0112] 步骤 703 ：加密管理模块将包含 Domain U 的标识信息的申请密钥请求消息给密钥管理模块。

[0113] 步骤 704 ：密钥管理模块根据 Domain U 的标识信息，生成对应的密钥。

[0114] 步骤 705 ：密钥管理模块向加密管理模块返回密钥。

[0115] 步骤 706 ：加密管理模块通过建立的传输通道，向加密代理模块返回密钥。

[0116] 另外，如果是不同的 Domain U 并行进行解密处理，则上述返回密钥的消息中还可以进一步携带对应的 Domain U 的标识信息。当然，如果各 Domain U 是串行进行解密处理，则也可以不携带 Domain U 的标识信息。

[0117] 步骤 707 ：加密代理模块采用密钥加密卷，也就是采用密钥对虚拟机的数据进行全盘加密。

[0118] 另外，上述实施例中，可以采用如下方式生成 Domain U 的标识信息 ：首先在安装加密代理的时候，加密代理会根据一些信息（如 VM 的 MAC+ 一些随机数）按某种私有算法生成一个唯一的标识，这个标识在加密代理注册的时候就会给加密管理模块保持起来，并给密钥管理系统。与密钥一一对应。

[0119] 加密代理程序应该在硬盘某一个位置写上一些信息，如 MAC、随机数信息，后面 boot Loader OS 中的动态加解密模块要根据这些信息，然后根据私有的算法将这个标识计

算出来，然后再密钥申请消息中带上这个标识。图 8 为本发明虚拟机全盘加密下预启动时的密钥传输设备的结构示意图，本实施例的设备可以为 Domain U。该设备包括建立模块 81、传输模块 82 和解密模块 83；建立模块 81 用于进行处于全盘加密状态的虚拟机的预启动操作，并在预启动时，建立与云平台的传输通道，所述云平台用于提供密钥；传输模块 82 用于通过所述传输通道，向所述云平台请求密钥并接收所述云平台发送的密钥；解密模块 83 用于采用所述密钥解密并启动操作系统。

[0120] 所述建立模块为启动加载模块，所述启动加载模块用于确定超级监视器内为虚拟机分配的传输通道；通过所述超级监视器内为虚拟机分配的传输通道，得到虚拟机与云平台之间的传输通道。

[0121] 特别地，对于 XEN 场景，可以是 Domain U 内的启动加载模块通过超级监视器建立与 Domain 0 的传输通道，而 Domain 0 在启动后可以获取 IP 地址，也可以根据 IP 地址建立与云平台的传输通道，因此，Domain U 可以通过 Domain 0 建立与云平台的传输通道。

[0122] 所述传输模块具体用于：

[0123] 通过所述超级监视器内的传输通道，向云平台发送密钥请求消息，所述密钥请求消息中携带虚拟机的标识信息；接收云平台返回的密钥，所述密钥为云平台根据所述虚拟机的标识信息确定的。

[0124] 所述建立模块为启动加载系统模块，所述启动加载系统模块用于在所述启动加载操作系统启动后向 DHCP 服务器申请 IP，根据所述 IP 地址建立与云平台的传输通道。

[0125] 所述传输模块具体用于：通过建立的 IP 通道，向云平台发送密钥请求消息，所述密钥请求消息中携带虚拟机的标识信息；接收云平台返回的密钥，所述密钥为云平台根据所述虚拟机的标识信息确定的。

[0126] 所述传输模块具体用于：通过所述超级监视器内的传输通道，向宿主机发送密钥请求消息，并经由所述宿主机和云平台间的 IP 连接通道，将所述密钥请求消息发送给云平台，所述宿主机在所述虚拟机预启动前完成启动并获取 IP 地址以及与云平台建立 IP 连接通道。

[0127] 本实施例的设备还可以包括：加密模块，用于在上次正常启动操作系统后，通过超级监视器内的传输通道，向云平台发送携带虚拟机的标识信息的密钥请求消息，接收所述云平台发送的根据所述虚拟机的标识信息确定的密钥，并采用所述密钥对所述虚拟机的数据进行全盘加密处理；或者，在上次正常启动操作系统后，获取 IP 地址，根据所述 IP 地址建立与云平台的 IP 连接，通过所述 IP 连接向云平台发送携带虚拟机的标识信息的密钥请求消息，接收所述云平台发送的根据所述虚拟机的标识信息确定的密钥，并采用所述密钥对所述虚拟机的数据进行全盘加密处理。

[0128] 另外，上述的解密模块和加密模块可以同属于一个物理模块，即相当于上述方法中的加解密模块。

[0129] 本实施例通过在预启动阶段建立与提供密钥的云平台之间的传输通道，可以实现预启动阶段密钥的传输，能够使得虚拟机获取密钥，进而可以解密虚拟机的操作系统，并实现虚拟机的操作系统的启动，避免由于不能获取密钥而停留在预启动阶段。

[0130] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序

在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0131] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

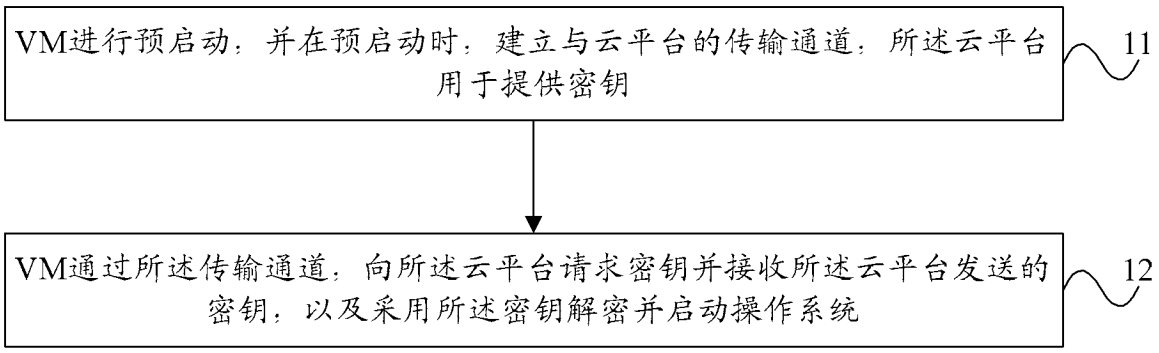

VM进行预启动，并在预启动时，建立与云平台的传输通道，所述云平台用于提供密钥
11
VM通过所述传输通道，向所述云平台请求密钥并接收所述云平台发送的密钥，以及采用所述密钥解密并启动操作系统
12

图 1

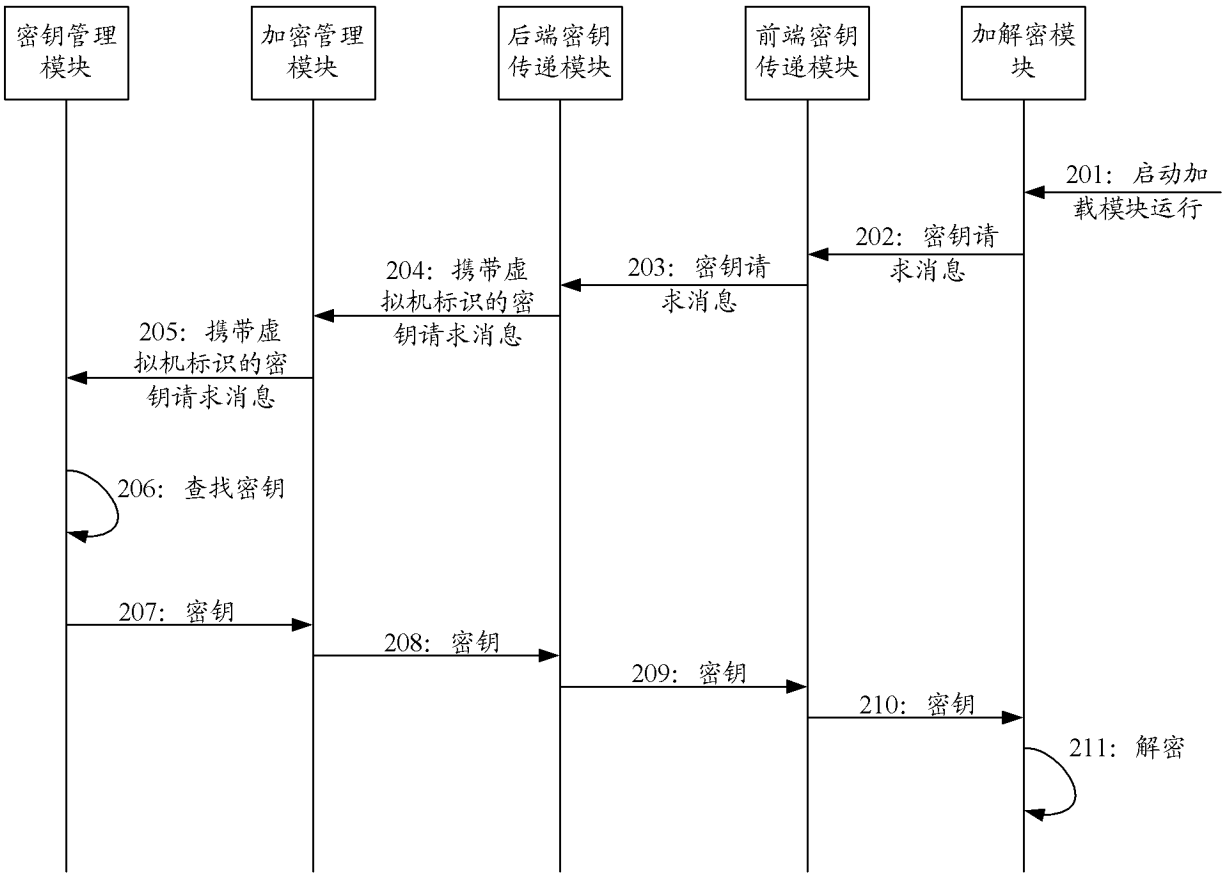

密钥管理模块
加密管理模块
后端密钥传递模块
前端密钥传递模块
加解密模块
201：启动加载模块运行
202：密钥请求消息
203：密钥请求消息
204：携带虚拟机标识的密钥请求消息
205：携带虚拟机标识的密钥请求消息
206：查找密钥
207：密钥
208：密钥
209：密钥
210：密钥
211：解密

图 2

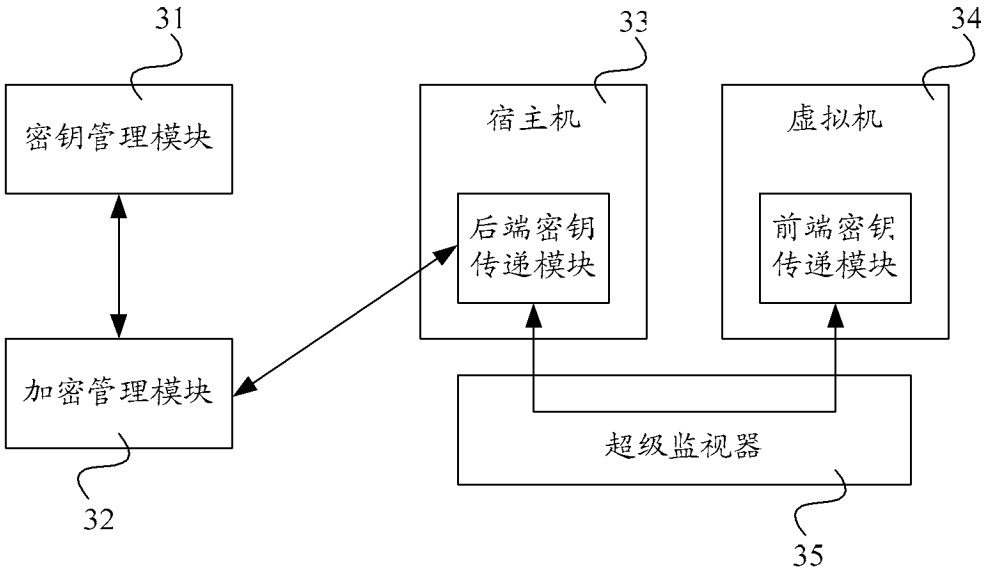

31
33
34
密钥管理模块
宿主机
虚拟机
后端密钥传递模块
前端密钥传递模块
加密管理模块
超级监视器
32
35

图 3

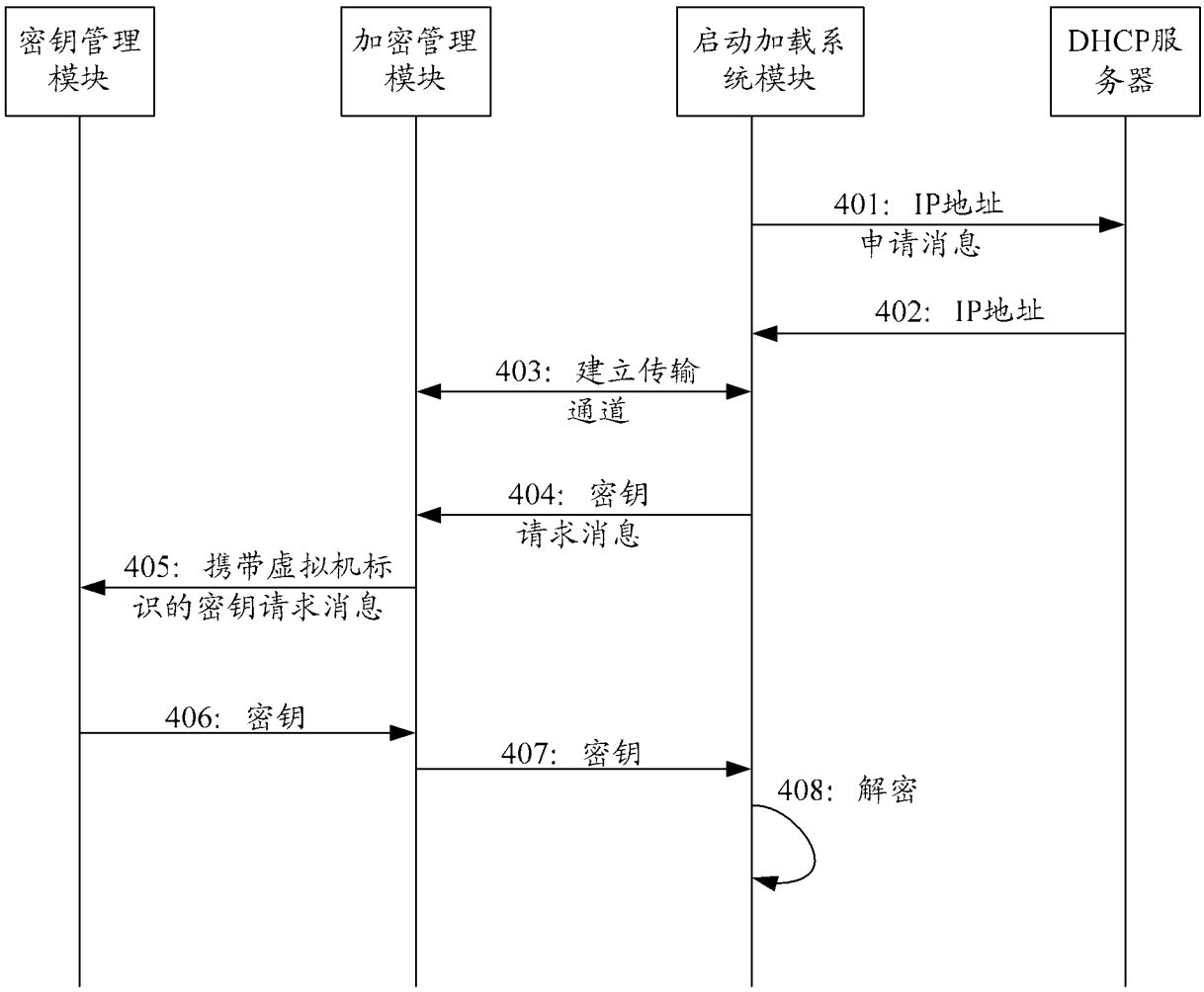

密钥管理模块
加密管理模块
启动加载系统模块
DHCP服务器
401: IP地址申请消息
402: IP地址
403: 建立传输通道
404: 密钥请求消息
405: 携带虚拟机标识的密钥请求消息
406: 密钥
407: 密钥
408: 解密

图 4

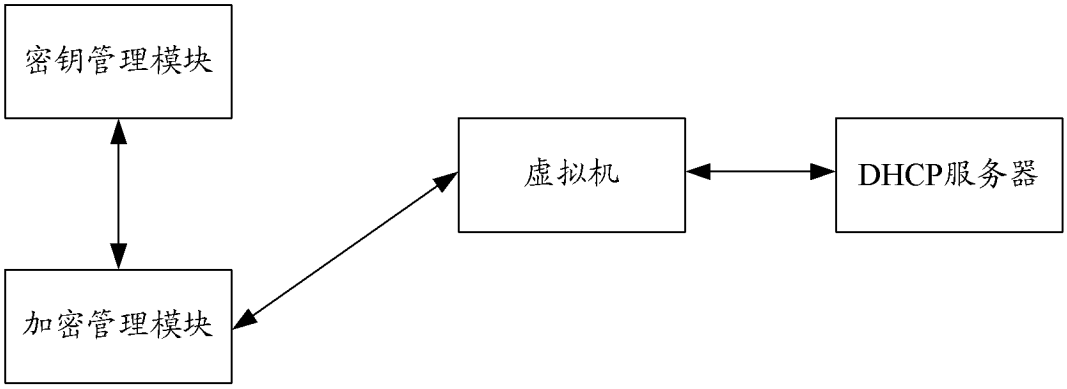

密钥管理模块
虚拟机
DHCP服务器
加密管理模块

图 5

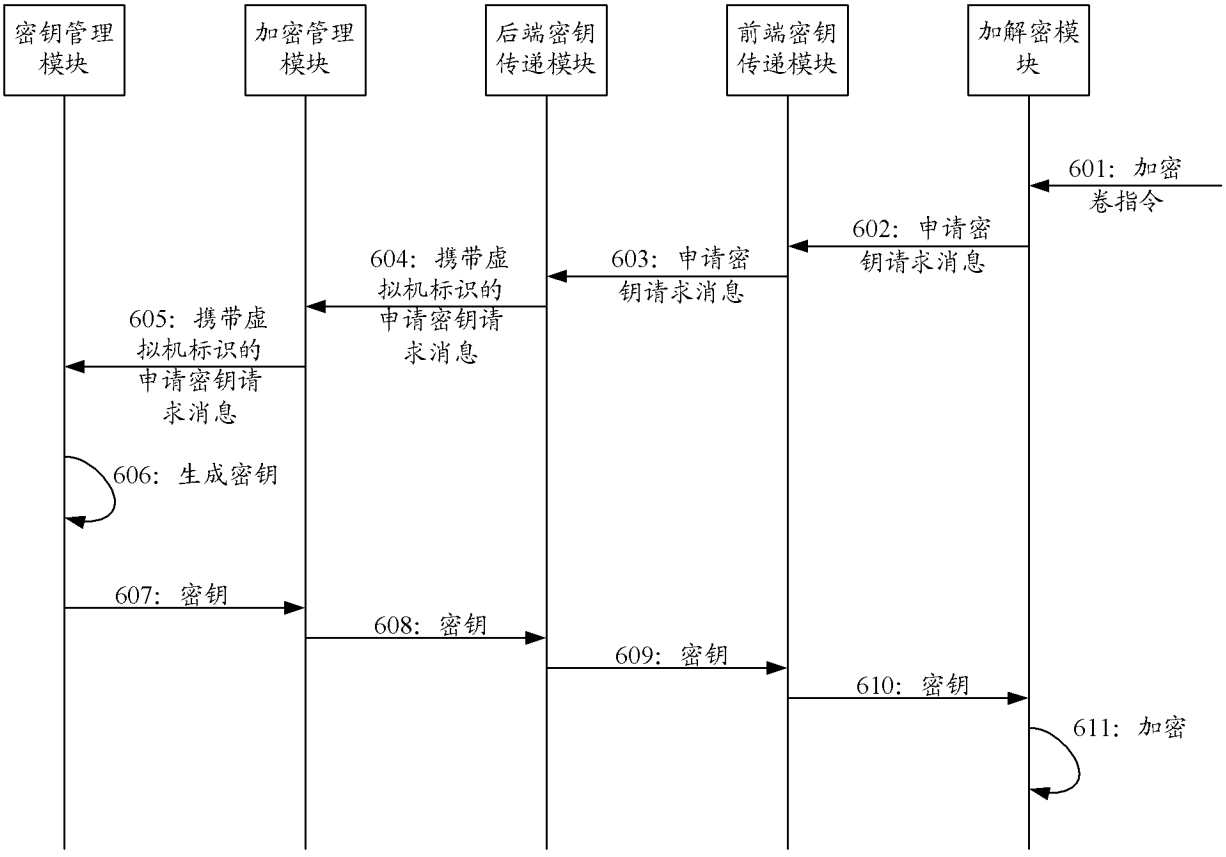

密钥管理模块
加密管理模块
后端密钥传递模块
前端密钥传递模块
加解密模块
601：加密卷指令
602：申请密钥请求消息
603：申请密钥请求消息
604：携带虚拟机标识的申请密钥请求消息
605：携带虚拟机标识的申请密钥请求消息
606：生成密钥
607：密钥
608：密钥
609：密钥
610：密钥
611：加密

图 6

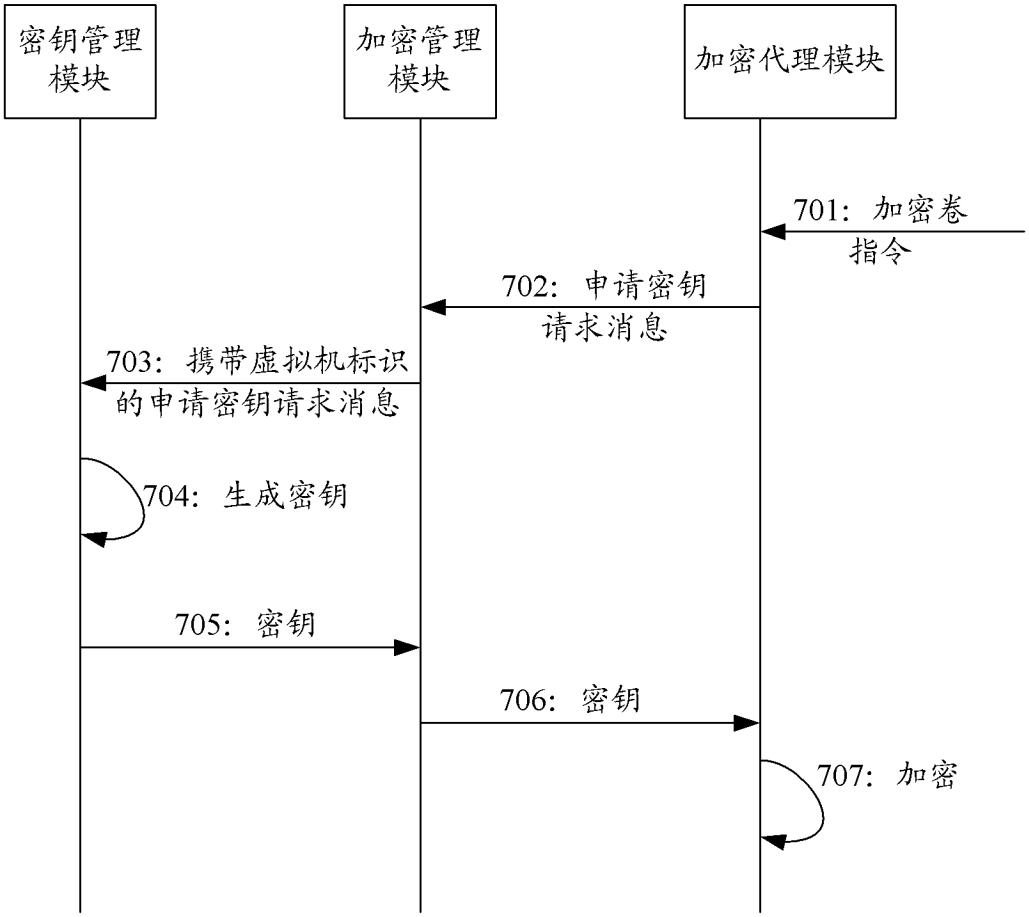

密钥管理模块
加密管理模块
加密代理模块
701：加密卷指令
702：申请密钥请求消息
703：携带虚拟机标识的申请密钥请求消息
704：生成密钥
705：密钥
706：密钥
707：加密

图 7

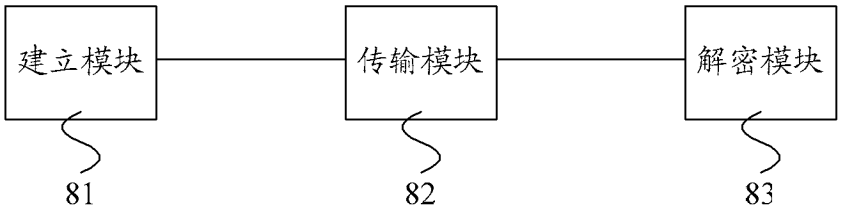

建立模块
传输模块
解密模块
81
82
83

图 8