



(12) 发明专利申请

(10) 申请公布号 CN 102270153 A

(43) 申请公布日 2011. 12. 07

(21) 申请号 201110230959. 0

(22) 申请日 2011. 08. 12

(71) 申请人 曙光信息产业(北京)有限公司
地址 100084 北京市海淀区水磨西街 64 号

(72) 发明人 唐焕焕 石旭 叶丞

(74) 专利代理机构 北京安博达知识产权代理有限公司 11271

代理人 徐国文

(51) Int. Cl.

G06F 9/455(2006. 01)

G06F 21/22(2006. 01)

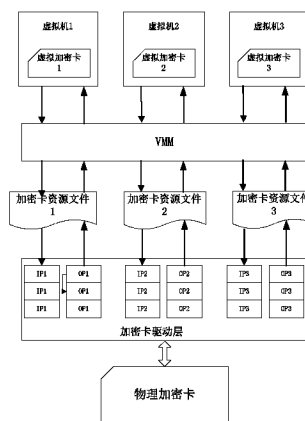
权利要求书 1 页 说明书 2 页 附图 3 页

(54) 发明名称

一种虚拟环境下加密卡共享的方法和装置

(57) 摘要

本发明提供了一种虚拟环境下加密卡共享的方法, 将一个硬件加密卡映射成独立的加密卡资源文件; 为每个资源文件建立处理队列并调度处理请求。本发明通过将同一块加密卡映射为多个不同的资源文件, 就可以将多个不同的加密卡资源分配给各虚拟机使用, 但各虚拟机在物理层面上使用的仍是同一块加密卡, 极大的提高了加密卡的使用效率。



1. 一种虚拟环境下加密卡共享的方法,其特征在于:
将一个硬件加密卡映射成独立的加密卡资源文件;
为每个资源文件建立处理队列并调度处理请求。
2. 如权利要求 1 所述的方法,其特征在于:所述处理队列包括输入队列和输出队列;
所述输入队列存放的是对加密卡的请求操作命令和数据;
所述输出队列存放的是加密卡响应请求后返回的响应结果。
3. 如权利要求 1 所述的方法,其特征在于:所述加密卡资源文件的数量至少为一个。
4. 如权利要求 1 所述的方法,其特征在于:所述调度处理请求采用先到先服务算法。
5. 如权利要求 2 所述的方法,其特征在于:请求在被加密卡处理后,该请求会在输入队列中被删除,请求完成后把处理结果返回到输出队列。
6. 一种虚拟环境下加密卡共享的装置,其特征在于:包括,
资源映射模块,用于将一个硬件加密卡映射成独立的加密卡资源文件;
队列管理模块,用于为每个资源文件建立处理队列并调度处理请求。
7. 如权利要求 6 所述的装置,其特征在于:所述处理队列包括输入队列和输出队列;
所述输入队列存放的是对加密卡的请求操作命令和数据;
所述输出队列存放的是加密卡响应请求后返回的响应结果。
8. 如权利要求 6 所述的装置,其特征在于:所述加密卡资源文件的数量至少为一个。
9. 如权利要求 6 所述的装置,其特征在于:所述调度处理请求采用先到先服务算法。
10. 如权利要求 7 所述的装置,其特征在于:请求在被加密卡处理后,该请求会在输入队列中被删除,请求完成后把处理结果返回到输出队列。

一种虚拟环境下加密卡共享的方法和装置

技术领域

[0001] 本发明涉及硬件共享,具体来讲,涉及一种在虚拟机环境下对加密卡进行共享的方法和装置。

背景技术

[0002] 近年来随着云应用模式的迅速发展,云安全成为广大用户最为关注的问题。目前,加密卡普遍应用于信息安全领域,用于认证用户身份和保障用户数据安全,所以使用加密卡保证云环境的安全成为了首选。在云环境中普遍使用虚拟化技术,而当前的虚拟化技术导致虚拟机对加密卡是独占性质的,即如果虚拟机 A 使用了加密卡,其他虚拟机就无法使用该加密卡,直到 A 释放加密卡资源。

[0003] 在 Linux 系统下,正常加密卡的驱动程序会将加密卡映射为具有唯一资源标识号的资源文件,所有应用程序通过该资源标识号使用该资源文件,并通过驱动程序使用物理加密卡。虚拟化技术使用 VMM(Virtual Machine Monitor,虚拟机监视器)对硬件进行调度,如图 1 所以。当前的虚拟化技术 VMM 分配方案是:为一台虚拟机分配了加密卡硬件资源后,其他虚拟机就无法申请该硬件资源。

[0004] 这种对加密卡的使用模式极大的浪费了加密卡资源,所以我们需要找到一种使得加密卡可以被多虚拟机共享使用方法,提高加密卡的使用效率。

发明内容

[0005] 为了解决上述问题,本发明提出了一种虚拟环境下加密卡的共享方法,即改变现有加密卡驱动程序将一块加密卡映射为一个资源文件的单一模式,而是将同一块加密卡映射为多个不同的资源文件,这样从 VMM 的角度来看就是有多个物理加密卡存在,VMM 就可以将多个不同的加密卡资源分配给各虚拟机使用,但各虚拟机在物理层面上使用的仍是同一块加密卡。

[0006] 一种虚拟环境下加密卡共享的方法,

[0007] 将一个硬件加密卡映射成独立的加密卡资源文件;

[0008] 为每个资源文件建立处理队列并调度处理请求。

[0009] 优选的,所述处理队列包括输入队列和输出队列;

[0010] 所述输入队列存放的是对加密卡的请求操作命令和数据;

[0011] 所述输出队列存放的是加密卡响应请求后返回的响应结果。

[0012] 优选的,所述加密卡资源文件的数量至少为一个。

[0013] 优选的,所述调度处理请求采用先到先服务算法。

[0014] 优选的,请求在被加密卡处理后,该请求会在输入队列中被删除,请求完成后把处理结果返回到输出队列。

[0015] 一种虚拟环境下加密卡共享的装置,包括,

[0016] 资源映射模块,用于将一个硬件加密卡映射成独立的加密卡资源文件;

- [0017] 队列管理模块,用于为每个资源文件建立处理队列并调度处理请求。
- [0018] 优选的,所述处理队列包括输入队列和输出队列;
- [0019] 所述输入队列存放的是对加密卡的请求操作命令和数据;
- [0020] 所述输出队列存放的是加密卡响应请求后返回的响应结果。
- [0021] 优选的,所述加密卡资源文件的数量至少为一个。
- [0022] 优选的,所述调度处理请求采用先到先服务算法。
- [0023] 优选的,请求在被加密卡处理后,该请求会在输入队列中被删除,请求完成后把处理结果返回到输出队列。
- [0024] 本发明通过将同一块加密卡映射为多个不同的资源文件,就可以将多个不同的加密卡资源分配给各虚拟机使用,但各虚拟机在物理层面上使用的仍是同一块加密卡,极大的提高了加密卡的使用效率。

附图说明

- [0025] 图 1 是虚拟机独占加密卡示意图。
- [0026] 图 2 是多虚拟机共享加密卡示意图。
- [0027] 图 3 是多虚拟机共享加密卡通信示意图。

具体实施方式

- [0028] 下面结合附图和具体实施方式对本发明进行说明。
- [0029] 为了实现虚拟环境下多虚拟机共享加密卡,需要在现有普通加密卡驱动基础上加入资源映射模块和队列处理模块。
- [0030] 资源映射模块的主要作用就是将一个加密卡硬件映射成为多个独立的加密卡资源文件,如图 3 所示一块物理加密卡被映射为三个独立的资源文件,但各资源文件最终访问的是一块物理加密卡。所以需要在驱动内对不同资源文件的请求进行管理。为了解决上面的问题引入了队列管理模块。
- [0031] 队列管理模块的主要作用是为每个资源文件建立两个处理队列,一个是输入队列,如图 3 所示的 IP1、IP2 和 IP3;一个是输出队列,如图 3 所示的 OP1、OP2 和 OP3。输入队列存放的是对加密卡的请求操作命令和数据,输出队列存放的是加密卡响应请求后,返回的响应结果。队列管理模块的另一个重要作用是分派请求。队列管理模块按照各队列中请求的时间先后顺序分派请求,即先到先服务原则。一旦一个请求被对列管理模块选中,将要交给加密卡处理,该请求会被从输入队列中删除;一旦一个请求被加密卡处理完成,队列管理模块会将加密卡返回的处理结果放入输出队列,同样按照先到先服务原则,返回给对应的资源文件,最终返回给对应的虚拟机。

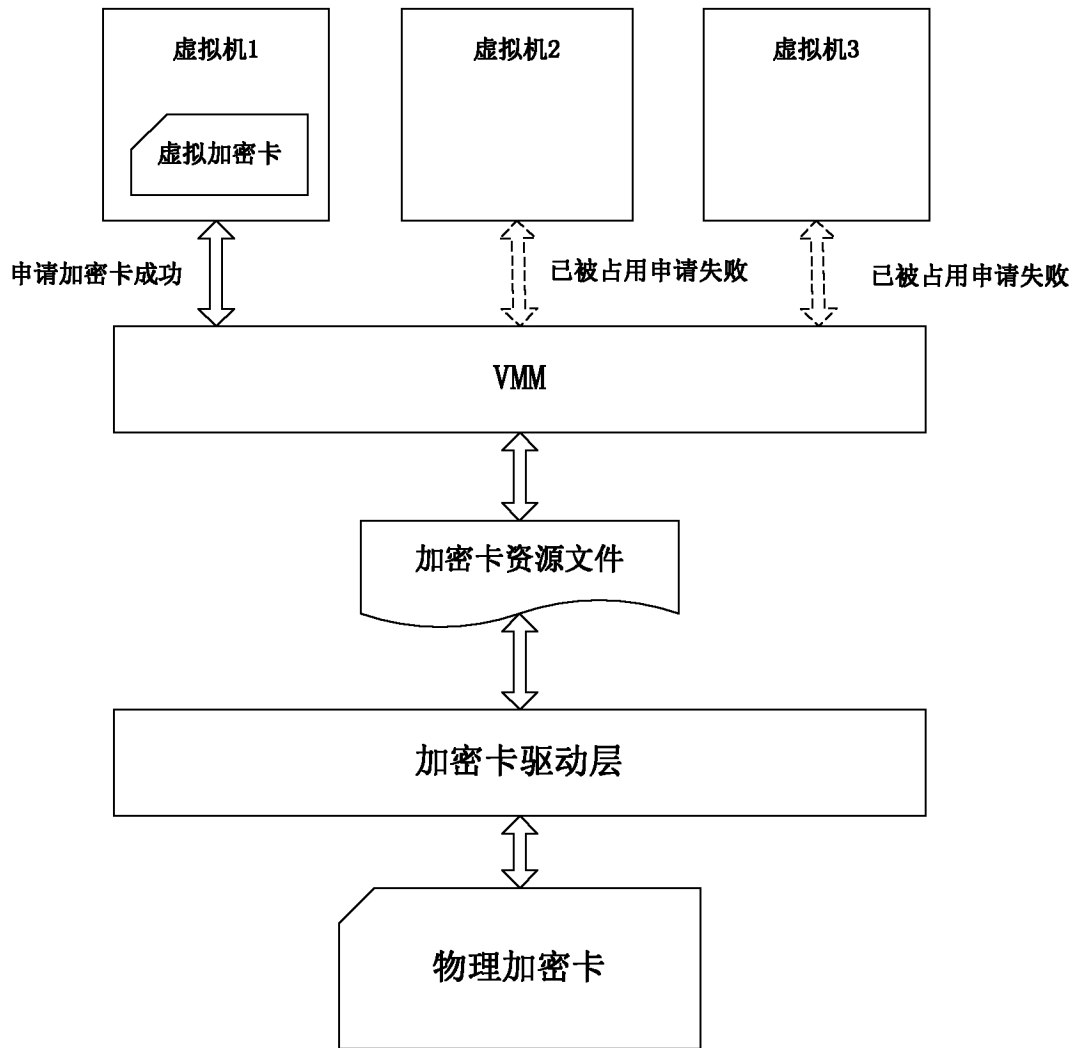


图 1

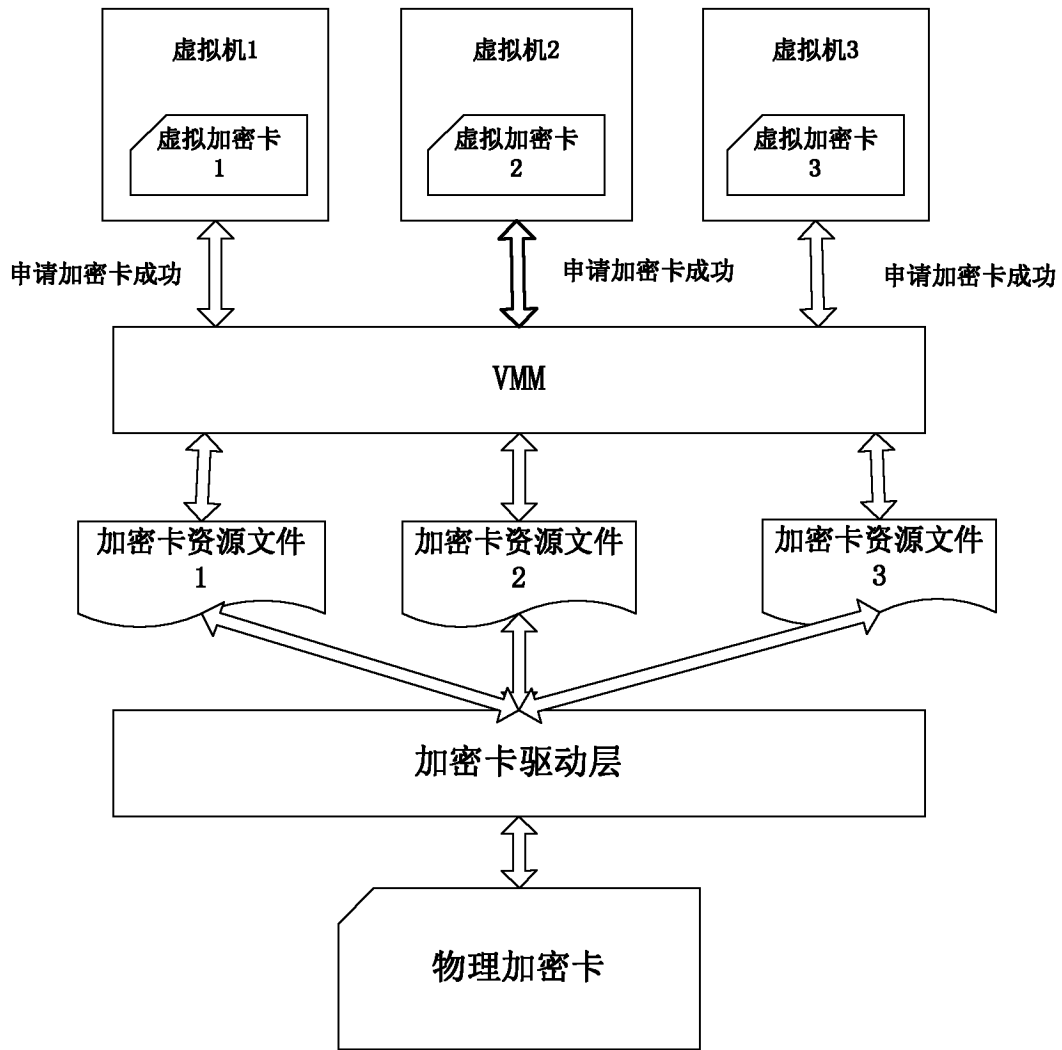


图 2

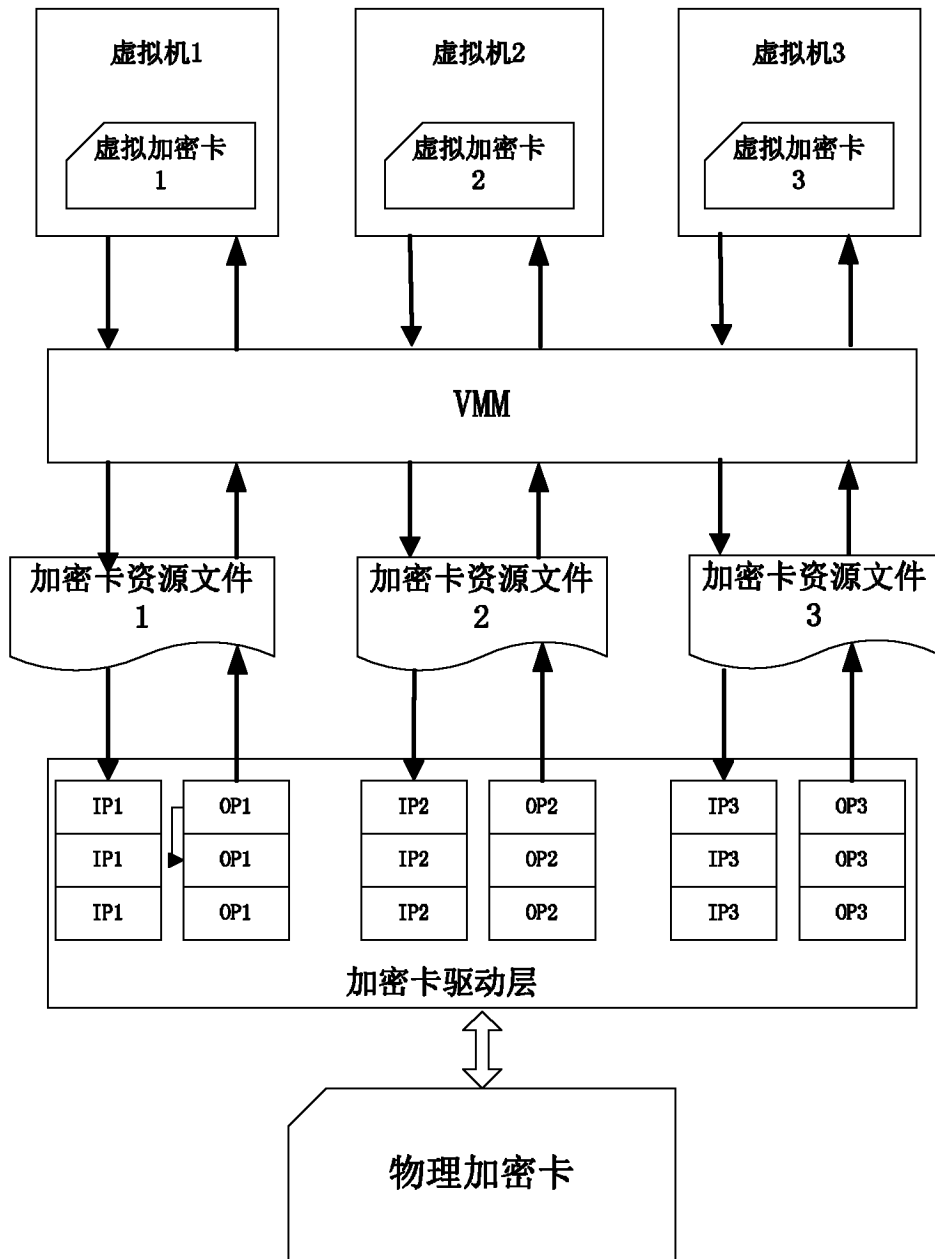


图 3