(54) 发明名称
基于VTPM对虚拟机进行安全保护的方法及系统

(57) 摘要
本发明公开了一种基于VTPM对虚拟机进行安全保护的方法及系统，属于互联网技术领域。该方法包括：物理主机接收虚拟机发送的基础种子获取请求，此基础种子获取请求中至少携带UUID；物理主机将UUID发送至KMC，以便KMC根据UUID生成基础种子；物理主机接收KMC反馈的基础种子，将基础种子发送至虚拟机，以便虚拟机根据基础种子创建VTPM的根密钥，该根密钥用于VTPM为虚拟机创建密钥以保护虚拟机的安全。本发明不依赖于任一物理主机，通过第三方设备为虚拟机派发基础种子，从而在虚拟机从一个物理主机迁移到另一个物理主机上时，通过基础种子即可生成出相同的根密钥，不仅降低了操作复杂度、节省了资源，而且不会破坏虚拟机中的密钥层次。
1. 一种基于VTPM对虚拟机进行安全保护的方法，其特征在于，所述方法包括：
物理主机接收虚拟机发送的基础种子获取请求，所述基础种子获取请求中至少携带通用唯一标识码UUID；
所述物理主机将所述UUID发送至密钥管理中心KMC，以便所述KMC根据所述UUID生成基础种子；
所述物理主机接收所述KMC反馈的基础种子，所述基础种子发送至所述虚拟机，
以便所述虚拟机根据所述基础种子创建虚拟可信平台模块VTPM的根密钥，所述根密钥用于
所述VTPM为虚拟机创建密钥以保护虚拟机的安全。

2. 根据权利要求1所述的方法，其特征在于，所述物理主机将所述UUID发送至KMC之前，
所述方法还包括：
所述物理主机基于预先配置的KMC地址，向所述KMC地址指定的所述KMC发送密钥保护请求，
使得所述KMC在接收到所述密钥保护请求时获取非对称密钥，所述非对称密钥包括公钥和私钥，所述KMC存储所述私钥；
所述物理主机接收所述KMC反馈的所述公钥，使用所述公钥对待发送至所述KMC的所述UUID进行加密，
以便所述KMC使用所述私钥解密出所述UUID。

3. 根据权利要求2所述的方法，其特征在于，所述方法还包括：
所述物理主机向对应的第一可信平台模块TPM加载所述公钥，以便使用所述第一TPM中的
所述公钥对待发送至所述KMC的所述UUID进行加密。

4. 根据权利要求2所述的方法，其特征在于，所述方法还包括：
所述KMC使用所述私钥加密向所述物理主机反馈的基础种子；
所述物理主机将所述基础种子发送至所述虚拟机之前，所述方法还包括：
所述物理主机使用所述公钥解密出所述KMC反馈的基础种子。

5. 根据权利要求2所述的方法，其特征在于，所述KMC根据所述UUID生成基础种子，具体为：
所述KMC根据对应的第一TPM生成对称密钥，将所述UUID和所述对称密钥作为随机数发生器的参数，
使得所述随机数发生器基于所述参数生成所述基础种子。

6. 根据权利要求1所述的方法，其特征在于，所述方法还包括：
所述KMC备份所述基础种子和所述UUID，以便所述虚拟机再次从所述KMC请求到所述基础种子，
使得所述虚拟机基于所述基础种子恢复出相同的所述根密钥。

7. 一种基于VTPM对虚拟机进行安全保护的系统，其特征在于，所述系统包括：虚拟机、
物理主机、密钥管理中心KMC；
所述物理主机，用于接收虚拟机发送的基础种子获取请求，所述基础种子获取请求中至少携带通用唯一标识码UUID；
所述物理主机，还用于将所述UUID发送至所述KMC；
所述KMC，用于根据所述UUID生成基础种子，并将所述基础种子发送至所述物理主机；
所述物理主机，还用于接收所述KMC反馈的基础种子，将所述基础种子发送至所述虚拟机；
所述虚拟机，用于根据所述基础种子创建虚拟可信平台模块VTPM的根密钥，所述根密钥用于
所述VTPM为虚拟机创建密钥以保护虚拟机的安全。
8. 根据权利要求7所述的系统，其特征在于，所述物理主机，还用于基于预先配置的KMC地址，向所述KMC地址指定的所述KMC发送密钥保护请求；
所述KMC，还用于接收到所述密钥保护请求时获取非对称密钥，所述非对称密钥包括公钥和私钥；
所述KMC，还用于存储所述私钥，并将所述公钥发送至所述物理主机；
所述物理主机，还用于接收所述KMC反馈的所述公钥，使用所述公钥对待发送至所述KMC的所述UUID进行加密；
所述KMC，还用于使用所述私钥解密出所述UUID。

9. 根据权利要求8所述的系统，其特征在于，所述物理主机，还用于向对应的第一可信平台模块TPM加载所述公钥，以便使用所述第一TPM中的所述公钥对待发送至所述KMC的所述UUID进行加密。

10. 根据权利要求8所述的系统，其特征在于，所述KMC，还用于使用所述私钥加密向所述物理主机反馈的所述基础种子；
所述物理主机，还用于使用所述公钥解密出所述KMC反馈的所述基础种子。

11. 根据权利要求8所述的系统，其特征在于，所述KMC，还用于根据对应的第二TPM生成对称密钥，将所述UUID和所述对称密钥作为随机数发生器的参数，使得所述随机数发生器基于所述参数生成所述基础种子。

12. 根据权利要求8所述的系统，其特征在于，所述KMC，还用于备份所述基础种子和所述UUID，以便所述虚拟机再次从所述KMC请求到所述基础种子，使得所述虚拟机基于所述基础种子恢复出相同的所述根密钥。

13. 一种计算机设备，其特征在于，包括：存储器、处理器和总线，其中，所述存储器和所述处理器通过所述总线直连；
所述存储器用于存放计算机指令，所述处理器用于执行所述存储器存储的计算机指令；当所述计算机设备运行时，所述处理器运行计算机指令，使得所述计算机设备执行权利要求1至6任一项所述的基于VTPM对虚拟机进行安全保护的方法。
基于VTPM对虚拟机进行安全保护的方法及系统

技术领域
[0001] 本发明涉及互联网技术领域，特别涉及一种基于VTPM对虚拟机进行安全保护的方法及系统。

背景技术
[0002] 在现代生活中，互联网为用户的生活带来了极大的便利，同时也滋生了很多欺诈和犯罪行为，加上互联网上客观存在的各种各样的漏洞，就衍生出一系列信息安全问题。随着互联网日益深入到政治、军事、经济、文化、生活的方方面面，信息安全已成为影响国家安全、社会稳定、经济发展的重大问题，必须采取有力措施保障信息安全。
[0003] 以对虚拟机的安全进行保护为例，当前主要通过物理主机中的TPM为虚拟机中的VTPM(Virtualizing the Trusted Platform Module, 虚拟可信平台模块)创建根密钥，VTPM利用该根密钥为虚拟机创建密钥保护体系，以保护虚拟机的敏感信息、存储虚拟环境度量值、为虚拟机提供远程证明等。对于VTPM对虚拟机进行安全保护的过程如下：
[0004] TPM为物理主机创建AIK(Attestation Identity Key，证明身份密钥)、隐私CA(Certification Authority，证书)对所创建的AIK进行签名后，TPM将签名后的AIK及Quote(引用)命令发送至物理主机上的任一VTPM，该VTPM通过采用签名后的AIK及Quote命令，为虚拟机创建EK，并基于EK为虚拟机创建AIK，进而基于所创建的EK和AIK对虚拟机的安全进行保护。
[0005] 在实现本发明的过程中，发明人发现现有技术至少存在以下问题：
[0006] 在上述过程中，VTPM得以对虚拟机进行安全保护主要依赖于TPM所创建的AIK，而当虚拟机从一个物理主机迁移到另一个物理主机上时，VTPM为虚拟机创建的密钥保护体系将不再适用，此时需要在新的物理主机上为虚拟机重新创建新的密钥保护体系，该过程不仅操作复杂、资源消耗较大，且破坏了虚拟机中的密钥层次。

发明内容
[0007] 为了解决相关技术的问题，本发明实施例提供了一种基于VTPM对虚拟机进行安全保护的方法及系统。
[0008] 一方面，本发明实施例提供了一种基于VTPM对虚拟机的安全进行保护的方法，该方法包括：当虚拟机在虚拟平台上初次运行时，虚拟机向物理主机发送基础种子获取请求，该基础种子获取请求中携带UUID(Universally Unique Identifier，通用唯一标识码)等信息。物理主机接收虚拟机发送的基础种子获取请求，并将基础种子获取请求中所携带的UUID发送至KMC(Key Management Center，密钥管理中心)。KMC基于该UUID生成基础种子，并将所生成的基础种子发送至虚拟机。当接收机到KMC发送的基础种子，虚拟机根据基础种子为VTPM创建根密钥，进而创建密钥保护体系。由于该基础种子并不依赖于物理主机，而是由KMC进行派发，因而在一个物理主机上迁移至另一个物理主机时，虚拟机可根据该基础种子重新为VTPM创建密钥保护体系，以保护虚拟机中数据安全。
在一个可能的设计中，物理主机可根据预先配置的KMC地址，有针对性地向该KMC地址所指向的KMC发送密钥请求。当接收到物理主机发送的密钥请求时，KMC从密钥数据库中随机获取一个非对称密钥，存储该非对称密钥的私钥，同时将该非对称密钥中的公钥发送至物理主机。物理主机接收KMC发送的公钥，并采用该公钥对UUID及其他信息（例如创建者、物理地址等）进行加密后，发送至KMC。物理主机通过采用公钥对待发送至KMC的UUID及其他信息进行加密，避免了UUID及其他信息在发送至KMC的过程中被其他用户截获，提高了虚拟机的信息安全。

在一个可能的设计中，物理主机中设置有第一TPM，该第一TPM用于存储物理主机内不同层次的密钥，在物理主机与KMC的交互中，物理主机可从该第一TPM中读取KMC所发送的公钥，对读取至KMC的数据进行加密，并对KMC发送的数据进行解密，从而保证与KMC之间交互的数据安全。

在一个可能的设计中，KMC采用存储的私钥对生成的基础种子进行加密，并将加密后的基础种子发送至物理主机。当接收到KMC采用私钥加密后基础种子，物理主机从第一TPM中读取公钥，并使用公钥对该加密后的基础种子进行解密，得到基础种子。通过计算得到的基础种子进行加密，有效地保证了基础种子的安全。

在一个可能的设计中，KMC中设置有第二TPM，当接收到物理主机发送的UUID时，KMC生成对称密钥，从OpenSSL库中调用随机数生成函数，并以UUID和对称私钥作为随机数生成函数的参数，生成基础种子。

在一个可能的设计中，KMC将所生成的基础种子及UUID存储到数据库中（如备份数据库中），在使用过程中，即便物理平台的第一TPM或主板损坏，虚拟机仍然可从KMC中获取到基础种子，进而根据基础种子恢复出相同的根密钥，创建相同的密钥体系，从而有效地防止了虚拟机中的数据丢失。

另一方面，本发明实施例提供了一种基于VTTPM对虚拟机的安全保护的体系，该体系包括：虚拟机、物理主机、KMC。其中，物理主机内设置有第一TSS和第一TPM，第一TSS可为外部设备（如虚拟机、KMC等）访问TPM提供接口；虚拟机内安装有多个应用模块，可触发虚拟机执行不同的操作，虚拟机内设置有第二TSS和VTTPM等，第二TSS可为外部设备访问VTTPM提供接口，KMC内设置有备份数据库、密钥数据库等多个数据库。

当虚拟机在虚拟平台上初始化时，虚拟机向物理主机发送基础种子获取请求，该基础种子获取请求中携带UUID等信息。物理主机接收虚拟机发送的基础种子获取请求，并将基础种子获取请求中所携带的UUID发送至KMC。KMC基于该UUID生成基础种子，并将所生成的基础种子发送至虚拟机。当接收机到KMC发送的基础种子，虚拟机根据基础种子为VTTPM创建根密钥，进而创建密钥保护体系。由于该基础种子并不依赖于物理主机，而是由KMC进行派发，因而当虚拟机从一个物理主机上迁移到另一个物理主机时，虚拟机可根据该基础种子重新为VTTPM创建密钥保护体系，以保护虚拟机中数据安全。

在一个可能的设计中，物理主机可根据预先配置的KMC地址，有针对性地向该KMC地址所指向的KMC发送密钥请求。当接收到物理主机发送的密钥请求时，KMC从密钥数据库中随机获取一个非对称密钥，存储该非对称密钥中的私钥，同时将该非对称密钥中的公钥发送至物理主机。物理主机接收KMC发送的公钥，并采用该公钥对UUID及其他信息（例如创建者、物理地址等）进行加密后，发送至KMC。物理主机通过采用公钥对待发送至KMC
的UUID及其他信息进行加密，避免了UUID及其他信息在发送至KMC的过程中被其他用户截获，提高了虚拟机的信息安全。

[0017] 在一个可能的设计中，物理主机中设置有第一TPM，该第一TPM用于存储物理主机内不同层次的密钥，在物理主机与KMC的交互中，物理主机可从该第一TPM中调用KMC所发送的公钥，对待发送至KMC的数据进行加密，并对KMC发送的数据进行解密，从而保证与KMC之间交互的数据安全。

[0018] 在一个可能的设计中，KMC采用存储的私钥对生成的基础种子进行加密，并将加解密后的基础种子发送至物理主机。当接收到KMC采用私钥加密后的基础种子，物理主机从第一TPM中调用公钥，并使用公钥对该加解密后的基础种子进行解密，得到基础种子。通过对基础种子进行加密，有效地保证了基础种子的安全。

[0019] 在一个可能的设计中，KMC中设置有第二TPM，当接收到物理主机发送的UUID时，KMC生成一对对称密钥，从OpenSSL库中借用随机数生成函数，并以UUID和对称密钥作为随机数生成函数的参数，生成基础种子。

[0020] 在一个可能的设计中，KMC将所生成的基础种子及UUID存储到数据库中（如加密备份数据文件中），在使用过程中，即便物理平台的CPU或主板损坏，虚拟机仍然可从KMC中获取到基础种子，进而根据基础种子恢复出相同的根密钥，创建相同的密钥体系，从而有效地防止了虚拟机中的数据丢失。

[0021] 第三方面，本发明实施例提供了一种计算设备，其包括计算机，计算机包括存储器、处理器和总线，其中，所述存储器和所述处理器通过总线相连。

[0022] 所述存储器用于存放计算机指令，所述处理器用于执行所述存储器存储的计算机指令；当所述计算机设备运行时，所述处理器运行计算机指令，使得所述计算机设备执行上述第一方面所述的基于VTPM对虚拟机进行安全保护的方法。

[0023] 本发明实施例提供的技术方案带来的有益效果是：

[0024] 物理主机接收虚拟机发送的至少携带UUID的基础种子获取请求，并将UUID发送至KMC，由KMC根据UUID生成基础种子，当接收到KMC反馈的基础种子，物理主机将基础种子发送至虚拟机，虚拟机根据基础种子创建VTPM的根密钥，VTPM使用该根密钥为虚拟机创建密钥，以保护虚拟机的安全。本发明不依赖于单一物理主机，通过第三方设备为虚拟机派发基础种子，从而在虚拟机从一个物理主机迁移到另一个物理主机上时，通过基础种子即可创建出相同的根密钥，不仅降低了操作复杂度、节省了资源，而且不会破坏虚拟机中的密钥层次。

附图说明

[0025] 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他的附图。

[0026] 图1是本发明一个实施例提供的基于VTPM对虚拟机的安全进行保护的方法所涉及到的实施环境的示意图；

[0027] 图2是本发明另一个实施例提供的一种基于VTPM对虚拟机的安全进行保护的方法
流程图：

[0028] 图3是本发明另一个实施例提供的一种基础种子派发的流程图；
[0029] 图4是本发明另一个实施例提供的一种根密钥创建流程图；
[0030] 图5是本发明另一个实施例提供的一种基于TPM的虚拟机的安全进行保护的系统的结构示意图；
[0031] 图6是本发明另一个实施例提供的一种计算机设备的结构示意图。

具体实施方式

[0032] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0033] 图1为本发明提供的基于VTPM对虚拟机进行安全保护的方法所涉及到的实施环境的示意图，参见图1，该实施环境包括物理主机、虚拟机和KMC。

[0034] 其中，物理主机包括物理平台、虚拟平台、主机操作系统及由CPU、硬盘等组成的各种功能组件。物理平台为主机所在的平台，物理平台内存储有机主机的第一TPM，该第一TPM具有保护物理主机、防止非法用户访问等功能。主机操作系统为物理主机运行的操作系统，包括第一个TSS(Trusted Software Stack，可信软件栈)和Libvirt，其中，第一个TSS为物理平台外部设备访问第一TPM的接口，可从物理平台的第一TPM中获取保护密钥；Libvirt为一种实现Linux虚拟化功能的Linux API(Application Programming Interface，应用程序编程接口)。虚拟平台上存储有机主机的VTPM。VTPM通过第一个TSS可获取第一TPM的保护密钥，例如获得VTPM为物理主机创建的AIK、DK等。主机操作系统使用Libvirt，在虚拟平台创建配置有机主机的虚拟机。该虚拟机包括客户端操作系统、各种功能组件、例如虚拟CPU、硬盘等，该客户端操作系统为虚拟平台管理的虚拟机所运行的操作系统，该客户端操作系统可以为Linux操作系统。

[0035] KMC具有备份功能，生成基础种子等功能，包括种子备份数据库、种子生成服务器及第二TPM等。第一TPM通过向KMC中的种子生成服务器发送基础种子生成请求，可触发种子生成服务器生成基础种子。

[0036] 在一个实施例中，虚拟平台运行在物理平台之上，主机操作系统和客户端操作系统运行在虚拟平台之上。

[0037] 在另一个实施例中，主机操作系统运行在物理平台之上，虚拟平台集成在主机操作系统之内，客户端操作系统运行在虚拟平台之上。

[0038] 上述物理主机与KMC及虚拟机之间可通过有线或无线网络进行通信。

[0039] 基于上述图1所示的基于VTPM对虚拟机进行安全保护的方法所涉及的实施环境，本发明实施例提供了一种基于VTPM对虚拟机进行安全保护的方法，参见图1，本实施例提供的一种方法流程包括：

[0040] 201、虚拟机向物理主机发送的基础种子获取请求，该基础种子获取请求中至少携带UUID。

[0041] 当虚拟机在虚拟平台上初次运行时，VTPM还未为虚拟机创建密钥保护体系。为了保护虚拟机中存储的信息安全，虚拟机可调用API向物理主机的第一TSS发送基础种子获取请求，以通过物理主机将UUID发送至KMC，并根据KMC派发的基础种子为虚拟机创建密钥保
护体系。其中，基础种子获取请求中至少携带虚拟机的UUID等。

0042 当接收到虚拟机发送的基础种子获取请求，物理主机将UUID发送至KMC。

0043 当物理主机上的第一TSS接收到虚拟机发送的基础种子获取请求，物理主机上的第一TSS基于预先配置的KMC地址，向KMC发送密钥保护请求。当接收到密钥保护请求时，KMC根据第二TPM生成一个非对称密钥，该非对称密钥包括公钥和私钥。KMC存储非对称密钥中的私钥，并将非对称密钥中的公钥发送至物理主机上的第一TSS。在物理主机与KMC的交互过程中，物理主机使用KMC反馈的公钥对接收到的KMC的数据进行加密，对KMC发送的数据进行解密；KMC使用私钥对接收到的物理主机的数据进行加密，对物理主机发送的数据进行解密。在本实施例中，物理主机发送至KMC的数据包括UUID及其他信息如物理主机的地址、创建者等。

0044 在第一TSS接收到KMC发送的公钥之后，物理主机将该公钥存储至第一TPM，由物理主机的第一TPM负责存储物理主机的加密信息。

0045 将UUID发送至KMC之前，物理主机上的第一TSS还将向对应的第二TPM加载该公钥，以便在后续与KMC进行交互的过程中，可使用第一TPM中的公钥对接收到的KMC的数据进行加密。具体加载时第一TSS可调用TPM_Load命令加载非对称密钥中的公钥，如果公钥加载失败，则本次VTMP为虚拟机创建密钥保护体系的流程结束。如果公钥加载成功，第一TSS通过调用TPM2_RSA_Encrypt命令，对UUID及其他信息进行加密，得到加密信息，进而通过互联网将第一加密信息发送至KMC。

0046 203、KMC根据UUID生成基础种子。

0047 当接收到基础种子派发请求（包括第一加密信息），KMC根据本地所存储的私钥，对基础种子派发请求中的密文进行解密，得到第一加密信息，包括UUID及其他信息。KMC使用第二TPM，生成一对非对称密钥；之后，KMC调用OpenSSL库中的随机数生成函数，以UUID及该对称密钥作为随机数发生器的参数，并基于该参数生成基础种子。

0048 当基础种子生成之后，KMC备份基础种子和UUID，以防止物理主机上的第一TPM或主板损坏时，虚拟机可再次从KMC中请求到基础种子，从而根据该基础种子恢复出与相同的根密钥，创建相同的密钥保护体系。

0049 204、KMC将基础种子发送至物理主机。

0050 KMC采用非对称密钥中的私钥对基础种子和其他信息进行加密，得到第二加密信息，并通过互联网将第二加密信息发送至物理主机。

0051 205、当接收到KMC反馈的基础种子，物理主机将基础种子发送至虚拟机。

0052 当接收到KMC发送的第二加密信息，第一TSS通过调用TPM2_RSA_Decrypt命令，从第一TPM中获取非对称密钥中的公钥，并采用该公钥对第二加密信息进行解密，得到基础种子及其他信息，进而将基础种子发送至虚拟机。

0053 至此，通过上述步骤201至205完成了基础种子的派发，该过程中KMC根据虚拟机的UUID为对应的虚拟机派发基础种子，即便虚拟机迁移到新的物理主机上，由于该虚拟机的UUID不会改变，虚拟机从KMC中获取到的基础种子也不会改变，因而避免了基础种子的重建。且虚拟机请求派发基础种子的过程和KMC派发基础种子的过程均由物理主机上的第一TPM进行加密，因而间接实现了VTMP和第一TPM之间的绑定关系，有效地保护了VTMP的安全。

0054 对于上述基础种子的派发过程，为了便于理解，下面将引用图3为例进行说明。
[0055] 参见图2，虚拟机在虚拟平台上初次启动后，虚拟机调用API向物理主机发送基础种子获取请求，该基础种子获取请求中至少携带虚拟机的UUID。当接收到基础种子获取请求，物理主机的第一TSS根据配置的KMC地址向KMC发送密钥请求报文，接收密钥请求之后，KMC根据第二TPM生成一个非对称密钥，KMC保存非对称密钥中的公钥，并将非对称密钥中的公钥发送至物理主机的第一TSS。物理主机的第一TSS加载非对称密钥中的公钥，如果公钥加载成功，第一TSS通过调用TPM2_RSA_Encrypt命令，采用公钥对UUID及其他信息进行加密，得到第一加密信息，进而将第一加密信息发送至KMC。当接收到第一加密信息时，KMC根据本地所存储的私钥，对第一加密信息进行解密，得到UUID。同时KMC根据第二TPM，生成一对对称密钥，并将UUID及对称密钥生成随机数发生器的参数生成基础种子。KMC备份基础种子及UUID，并采用私钥对基础种子加密，得到第二加密信息，进而将第二加密信息发送至物理主机的第一TSS，由第一TSS根据第一TSS中读取的公钥对第二加密信息进行解密，得到基础种子，进而将基础种子发送至虚拟机。

[0056] 206、虚拟机根据基础种子创建VTMP的根密钥。

[0057] 当接收到物理主机发送的基础种子，虚拟机将基础种子加载到虚拟平台上的第二TSS中，由第二TSS将基础种子加载到VTMP中，进而根据该基础种子为VTMP创建根密钥。在本次实施例中，基础种子包括背书基础种子、存储基础种子及平台基础种子，三种基础种子为由VTMP生成的随机数，用于基础对象的派生。针对基础种子的三种类型，虚拟机根据基础种子中背书基础种子为VTMP创建的根密钥也有三种类型。例如，如果基础种子为背书基础种子，虚拟机根据背书基础种子为VTMP创建的根密钥为背书密钥；如果基础种子为存储基础种子，虚拟机根据存储基础种子为VTMP创建的根密钥为存储根密钥。其中，背书密钥用于产生背书密钥证书，存储根密钥用于产生多种密钥加密算法。

[0058] 在本次实施例中，虚拟机根据基础种子为VTMP创建根密钥的过程，可参见下述步骤2061～2066。

[0059] 2061、当虚拟机中指定应用程序运行时，指定应用程序预先为待创建的根密钥指定期信息。

[0060] 在为待创建的根密钥指定期信息时，指定应用程序可调用第二TSS中的API为待创建的根密钥指定期信息。其中，密钥信息包括指定期算法类型、密钥参数和密钥描述等。

[0061] 2062、虚拟机判断本地是否已为VTMP创建虚拟背书密钥，如果已为VTMP创建虚拟背书密钥，则执行步骤2063；如果未为VTMP创建虚拟背书密钥，虚拟机根据背书基础种子，为VTMP创建虚拟背书密钥。

[0062] 在本次实施例中，虚拟背书密钥用于对属主发送的数据进行加密，其中，属主为虚拟机的拥有者。虚拟机根据背书基础种子，创建虚拟背书密钥时，第二TSS通过调用TPM2_CreatePrimary命令，从VTMP中获取背书基础种子，并基于该背书基础种子为VTMP创建虚拟背书密钥。在该过程中，如果第二TSS接收到来自VTMP返回的句柄，则说明虚拟背书密钥创建成功，第二TSS将虚拟背书密钥持久到VTMP中，并执行步骤2063，如果第二TSS未接收到来自VTMP返回的句柄，则说明虚拟背书密钥创建失败，流程结束。

[0063] 2063、虚拟机判断是否已为VTMP创建了属主，如果已为VTMP创建了属主，则执行步骤2064，如果未为VTMP创建属主，虚拟机根据存储基础种子，为VTMP创建属主。

[0064] 当判断出未为VTMP创建属主，虚拟机根据基础种子创建一个指定会话，该指定
会话为由一个第二TSS到VTPM的会话。虚拟机通过修改指定会话的存储控制域(Storage Hierarchy)的授权数据(Auth value)为VTPM创建属主。在该过程中，虚拟机还为属主权限设置了属主权限，规定属主可以控制VTPM资源的分配，例如属主可控制存储控制域的开启和关闭、创建根密钥，将密钥对象持久化保存到TPM的非易失性存储介质等，但属主不能直接访问密钥，因此，需要由第二TSS管理属主口令，该属主口令可以为随机值或特定值。如果属主口令为一个随机值，则由第二TSS生成保存；如果属主口令为一个特定值，则该特定值可以为第二TSS代码固定值等。

0065  2064. 虚拟机根据属主授权数据及预先指定的密钥参数，创建存储根密钥。

0066  第二TSS使用属主授权数据和指定应用程序预先指定的密钥参数，通过调用TPM2_CreatePrimary命令，在VTPM中为VTPM创建存储根密钥，在创建存储根密钥的过程中，如果第二TSS接收到存储根密钥句柄，则说明在VTPM中已成功创建了存储根密钥。当然，除了接收到存储根密钥句柄外，第二TSS还将接收到保存密钥blob等。

0067  2065. 当存储根密钥创建成功之后，虚拟平台上的TSS将存储根密钥持久化到VTPM的非易失性存储介质中。

0068  当存储根密钥创建成功之后，第二TSS向VTPM发送TPM2EvictControl命令，VTPM通过执行TPM2EvictControl命令，将存储根密钥持久化到非易失性存储介质中。通过将存储根密钥持久化到非易失性存储介质中，当客户端操作系统重新启动时，虚拟机无需重新加载存储根密钥，且存储根密钥不会被其他对象替换出虚拟机的内存。

0069  2066. 虚拟机生成存储根密钥的密钥索引，并返回给指定应用程序。

0070  第二TSS保存存储根密钥句柄及保存密钥blob，例如将该存储根密钥句柄及保存密钥blob保存在易失性存储介质中，同时，第二TSS还将根据存储根密钥生成存储根密钥索引，并将该存储根密钥索引发送至指定应用程序。

0071  对于虚拟机根据基础种子为VTPM创建根密钥的过程，下面将通过图2为例进行详述。

0072  2072. （1）虚拟机中的指定应用程序调用第二TSS中的API为待创建的根密钥指定属性信息。

0073  （2）虚拟机判断本地是否已为VTPM创建虚拟背书密钥，如果未为VTPM创建虚拟背书密钥，第二TSS通过调用TPM2CreatePrimary命令，在VTPM中获取背书基础种子，并基于该背书基础种子为VTPM创建虚拟背书密钥。在该过程中，如果第二TSS接收到VTPM返回的句柄，则说明虚拟背书密钥创建成功。

0074  （3）虚拟机判断是否已为VTPM创建了属主，如果未为VTPM创建属主，虚拟机根据存储基础种子创建一个指定会话，该指定会话为一个由第二TSS到VTPM的会话，虚拟机通过修改指定会话的存储控制域(Storage Hierarchy)的授权数据(Auth value)为VTPM创建属主。

0075  （4）第二TSS使用属主授权数据和指定应用程序预先指定的密钥参数，通过调用TPM2CreatePrimary命令，在VTPM中为VTPM创建存储根密钥，在创建存储根密钥的过程中，如果第二TSS接收到存储根密钥句柄，则说明在VTPM中已成功创建了存储根密钥。当然，除了接收到存储根密钥句柄外，第二TSS还将接收到保存密钥blob等。

0076  （5）第二TSS向VTPM发送TPM2EvictControl命令，VTPM通过执行该TPM2EvictControl命令，将存储根密钥持久化到非易失性存储介质中。
本发明实施例提供的方法，物理主机接收虚拟机发送的至少携带UUID的基础种子获取请求，并向UUID发送至KMC，由KMC根据UUID生成基础种子，当接收到KMC反馈的基础种子，物理主机将基础种子发送至虚拟机，虚拟机根据基础种子创建VTPM的根密钥，VTPM使用该根密钥为虚拟机创建密钥，以保护虚拟机的安全。本发明不依赖于任一物理主机，通过第三方设备为虚拟机派发基础种子，从而在虚拟机从一个物理主机迁移到另一个物理主机上时，通过基础种子即可创建出相同的根密钥，不仅降低了操作复杂度，节省了资源，而且不会破坏虚拟机中的密钥层次。

参见图5，本发明实施例提供了一种基于VTPM对虚拟机进行安全保护的系统，该系统包括：虚拟机501、物理主机502、密钥管理中心KMC503；物理主机502，用于接收虚拟机501发送的基础种子获取请求，基础种子获取请求中至少携带通用唯一标识码UUID；物理主机502，还用于将UUID发送至KMC503；KMC503，用于根据UUID生成基础种子，并将基础种子发送至物理主机502；物理主机502，还用于接收KMC503反馈的基础种子，将基础种子发送至虚拟机501；虚拟机501，用于根据基础种子创建虚拟可信平台模块VTPM的根密钥，该根密钥用于VTPM为虚拟机创建密钥以保护虚拟机的安全。

在本发明的另一个实施例中，物理主机502，还用于基于预先配置的KMC地址，向KMC地址指定的KMC503发送密钥保护请求；KMC503，还用于在接收到密钥保护请求时获取非对称密钥，该非对称密钥包括公钥和私钥；物理主机502，还用于接收KMC503反馈的公钥，使用公钥对待发送至KMC的UUID进行加密；KMC503，还用于使用私钥解密出UUID。

在本发明的另一个实施例中，物理主机502，还用于向对应的第一可信平台模块TPM加载公钥，以便使用第一TPM中的公钥对待发送至KMC503的UUID进行加密。

在本发明的另一个实施例中，KMC503，还用于使用私钥加密向物理主机502反馈的基础种子；物理主机502，还用于使用公钥解密出KMC503反馈的基础种子。

在本发明的另一个实施例中，KMC503，还用于根据对应的第二TPM生成对称密钥，将UUID和对称密钥作为随机数发生器的参数，使得随机数发生器基于参数生成基础种子。

在本发明的另一个实施例中，KMC503，还用于备份基础种子和UUID，以便虚拟机501再次从KMC请求到基础种子，使得虚拟机基于基础种子恢复出相同的根密钥。

本发明实施例提供的系统，物理主机接收虚拟机发送的至少携带UUID的基础种子获取请求，并向UUID发送至KMC，由KMC根据UUID生成基础种子，当接收到KMC反馈的基础种子，物理主机将基础种子发送至虚拟机，虚拟机根据基础种子创建VTPM的根密钥，VTPM使用该根密钥为虚拟机创建密钥，以保护虚拟机的安全。本发明不依赖于任一物理主机，通过第
三方设备为虚拟机派发基础种子，从而在虚拟机一个物理主机迁移到另一个物理主机上时，通过基础种子即可创建出相同的根密钥，不仅降低了操作复杂度，节省了资源，而且不会破坏虚拟机中的密钥层次。

[0096] 参见图6，其示出了本发明的一个实施例中使用的计算设备600的说明性计算机体系结构。所述计算设备600为常规的台式计算机或者膝上型笔记本，一个或多个计算设备600可构成物理平台。所述计算设备600包括处理器601、存储器602和总线603，其中，处理器601和存储器602通过总线603连接。所述计算设备600还包括帮助计算设备内的各个部件之间传输信息的基本输入/输出系统(1/0系统)604，和用于存储操作系统、应用程序和其他程序模块的大容量存储设备605。

[0097] 所述基本输入/输出系统604包括有用于显示信息的显示器606和用于用户输入信息的诸如鼠标、键盘之类的输入设备607。其中所述显示器606和输入设备607都通过连接到总线603的输入输出控制器608连接到处理器601。所述基本输入/输出系统604还可以包括输入输出控制器608以用于接收和处理来自键盘、鼠标、或电子触控笔等其他设备的输入。类似地，输入输出控制器608还提供输出到显示屏、打印机或其他类型的输出设备。

[0098] 所述大容量存储设备605通过连接到总线603的大容量存储控制器(未示出)连接到处理器601。所述大容量存储设备605及其相关联的计算机可读介质为计算机设备600提供非易失性存储。也就是说，所述大容量存储设备605可以根据包括诸如硬盘或者CD-ROM驱动器之类的计算机可读介质(未示出)。

[0099] 不失一般性，所述计算机可读介质可以包括计算机存储介质和通信介质。计算机存储介质包括以用于存储诸如计算机可读指令、数据结构、程序模块或其他数据等信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括RAM、ROM、EPROM、EEPROM、闪存或其他固态存储其技术，CD-ROM、DVD或其他光学存储、磁带盒、磁带、磁盘存储或其他磁性存储设备。当然，本领域技术人员可知所述计算机存储介质不局限于上述几种。

[0100] 根据本发明的各种实施例，所述计算设备600还可以通过诸如因特网等网络连接到网络上的远程计算机运行。即计算设备600可以通过连接在所述总线603上的网络接口单元609连接到网络610，或者说，也可以使用网络接口单元609来连接到其他类型的网络或远程计算机系统(未示出)。

[0101] 综上，本发明实施例提供的计算设备，物理主机接收虚拟机发送的至少携带UUID的基础种子获取请求，并将UUID发送至KMC，由KMC根据UUID生成基础种子，当接收到KMC反馈的基础种子，物理主机将基础种子发送至虚拟机，虚拟机根据基础种子创建VTPM的根密钥，VTPM使用该根密钥为虚拟机创建密钥，以保护虚拟机的安全。本发明不依赖于任一物理主机，通过第三方设备为虚拟机派发基础种子，从而在虚拟机从一个物理主机迁移到另一个物理主机上时，通过基础种子即可创建出相同的根密钥，不仅降低了操作复杂度，节省了资源，而且不会破坏虚拟机中的密钥层次。

[0102] 需要说明的是：上述实施例提供的VTPM的安全保护系统在保护VTPM的安全时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将VTPM的安全保护系统的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的VTPM的安全保护系统与VTPM的
安全保护方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

【0103】本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，所述提到的存储介质可以是只读存储器，磁盘或光盘等。

【0104】以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。
图1
图2

201. 虚拟机向物理主机发送的基础种子获取请求，该基础种子获取请求中至少携带UUID

202. 当接收到虚拟机发送的基础种子获取请求，物理主机将UUID发送至KMC

203. KMC根据UUID生成基础种子

204. KMC将基础种子发送至物理主机

205. 当接收到KMC反馈的基础种子，物理主机将基础种子发送至虚拟机

206. 虚拟机根据基础种子创建VTPM的根密钥
图4