云虚拟化平台可信证明技术研究综述

涂碧波[1,2]，程杰[1,2]，夏豪骏[1,2]，张坤[1,2]，孙瑞娜[1,2,3]

（1. 中国科学院信息工程研究所，北京 100093；2. 中国科学院大学网络空间安全学院，北京 100049；
3. 新疆财经大学信息管理学院，新疆 乌鲁木齐 830012）

摘 要：伴随云计算的飞速发展，云平台的安全问题也备受关注。可信计算是云安全体系中重要支撑技术，可信证明是可信计算的一个重要特性，用于验证云虚拟化平台是否具有可信性，为保证云平台安全提供基础。现基于可信证明的定义，系统梳理虚拟化平台的可信根虚拟化、平台身份证明、平台状态证明、虚拟机的可信证明框架等关键技术的研究进展，分析并对比典型方案，探讨现有的工作的局限性，最后指出未来的研究趋势。

关键词：云平台；可信证明；证书链扩展；完整性度量；远程证明

中图分类号：TP309

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021213

Overview of research on trusted attestation technology of cloud virtualization platform

TU Bibo[1,2], CHENG Jie[1,2], XIA Haojun[1,2], ZHANG Kun[1,2], SUN Ruina[1,2,3]

1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
3. China School of Information Management, Xinjiang University of Finance and Economics, Urumqi 830012, China

Abstract: With the rapid development of cloud computing, the security issues of cloud platforms have also attracted much attention. Trusted computing is an essential supporting technology in the cloud computing security system. Trusted attestation is an important feature in trusted computing. The use of trusted attestation technology verifies whether the cloud virtualization platform is trustworthy, thereby providing a foundation for ensuring the security of the cloud platform. Now based on the definition of trusted attestation, the research progress of key technologies such as the root of trust virtualization, platform identity authentication, platform status certification, and trusted attestation framework for virtual machines were systematically sorted out, typical schemes were analyzed and compared. Furthermore, the limitations of existing work were discussed. Finally, the future research trend of this area were pointed out.

Keywords: cloud platform, trusted attestation, certificate chain extension, integrity measurement, remote attestation

1 引言

随着互联网的普及和业务数据的激增，云计算[1]因其高性能、低成本的优势得到飞速发展。Amazon、Google、阿里、华为等国内外知名的大型互联网公司都拥有独立的云计算平台及云计算推进战略规划，政府部门、事业单位也将部分业务迁移到云上。Gartner 数据显示，截至 2019 年，全球云计算市场规模已达到 1 883 亿美元，增速为 20.86%。2020 年，线上办公、线上会议等应用爆发式增长，催生了“云经济”，不少企业加快数字化转型的进程。除此之外，新基建提出的“加快 5G 网络、数据中心等基

收稿日期：2021−07−28；**修回日期**：2021−11−03

通信作者：张坤，zhangkun@iie.ac.cn

基金项目：广东省重点领域研发计划基金资助项目（No.2019B010137002）

Foundation Item: Guangdong Province Key Area Research and Development Program (No.2019B010137002)

础设施建设”为云计算的发展奠定了政策基调。目前，我国的云计算发展已经进入了一个跃升的阶段。

云计算飞速发展的同时，云安全问题也日益突出。在云计算环境下，用户失去了对计算和数据的完全控制[2]能力，造成了信任缺失，虚拟化技术扩展了软件栈、增加了新的攻击面，底层资源的共享可能引发同驻攻击，解决云安全问题迫在眉睫。然而，传统的被动防护策略难以抵御新的漏洞和攻击，同时安全产品自身的安全性也相当脆弱，容易被攻击者利用而成为新的攻击面。

可信计算是一种前瞻性的安全技术，它将防护前置以主动的方式弥补被动防护的不足。目前，用“可信计算构筑网络安全”已成为一种共识，基于可信计算技术构建新一代的安全结构也成为国际的主流。同时，可信计算作为云安全体系的重要技术之一，是解决云安全问题的有效手段[3]。对我国来说，安全市场对可信的需求也在不断攀升，2019 年发布和实施的等级保护 2.0[4]的云安全的相关标准中，强化了可信计算技术的使用，从一级到四级都提出了可信验证的防护要求。

可信证明是可信计算的重要的技术特征之一。随着云虚拟化平台下可信计算的发展，对可信证明技术的研究也在不断深入。本文对云虚拟化平台可信证明的关键技术进行分析和总结，以期为研究人员对此研究进展有个总体把握，对未来研究提供借鉴。

2　背景

2.1　云计算

云计算是目前互联网时代信息基础设施与应用服务模式的重要形态，它依托于虚拟化技术，为信息系统的软硬件资源提供按需共享的应用方式。云计算提供了多样的服务模式，包括基础设施即服务（IaaS, infrastructure as a service）、平台即服务（PaaS, platform as a service）、软件即服务（SaaS, software as a service），甚至 X 即服务（XaaS, X as a service）。其中，IaaS 具有高度虚拟化、动态伸缩性和庞大规模的技术特征，是其他服务模式的基础，也是整个云平台建设的基石。本文的研究重点也在 IaaS 云。

2.2　可信证明的定义

不同的组织对可信有不同的定义。其中，可信计算组（TCG, trusted computing group）的定义得到了普遍的认可。TCG 认为，若实体是可信的，则它的行为总是以预期的方式朝着预期的目标发展。即若一个实体可信，则其行为、能力符合预期并且可验证其符合预期。

对于证明，TCG 规范中的定义是证明是一种报告机制，证明方将其平台的身份以及软硬件配置信息报告给挑战方。挑战方验证成功后，相信证明方提供的身份信息和报告是正确、可靠的。美国国家安全局对证明的定义[5]则是证明是证明方向挑战方提供证据而表明其具备某些特性的行为。文献[6]在这 2 个定义的基础上重新定义证明，并给出形式化描述。其认为证明是证明方通过提供证据和（或）逻辑推理向挑战方表明自己具有某种属性的过程。形式化表示为

$$S \xrightarrow{<E(S)\ \vee\ R(S,r)>} \text{evidence}$$

$$C \xrightarrow{I(\text{evidence})} P$$

其中，S 表示证明方，C 表示挑战方；$E(S)$表示获取证明信息的操作，$R(S,r)$表示逻辑推理的操作；evidence 表示证据的结果，I(evidence)表示验证证据结果的操作，P 表示证明方具有的属性。

结合可信和证明的定义，可信证明的定义如定义 1 所示。

定义 1　可信证明是证明方向挑战方提供可信相关的证据，挑战方验证可信证据是否符合预期来判断证明方是否可信的过程。

根据可信证明的定义，可信证明应包括 2 个基本步骤：一是证明方提供与可信相关的可信证据，这些可信证据包括证明方的平台身份信息、证明方平台软硬件配置的完整性信息等；二是挑战方收到可信证据后，验证其是否符合预期，并根据验证结果推理证明方是否具备可信性。

3　云虚拟化平台可信证明

本节首先介绍物理平台可信证明的关键技术，并在此基础上，分析将可信证明技术应用到虚拟平台时面临的问题和解决思路。

3.1　物理平台可信证明

根据可信证明的定义，可信证明的过程分为可信凭证的获取和可信凭证的验证。根据可信凭证类型的不同，将可信证明分为平台身份证明和平台状态证明。

平台身份证明是通过提供与平台相关的身份

证书来验证平台是一个可信的实体。在物理平台，作为可信根的可信平台模块（TPM, trusted platform module）中都有一个唯一的背书密钥（EK, endorsement key）来标识平台的身份。若直接采用 EK 来进行平台身份证明，会暴露平台的真实身份。对此，在 TPM v1.1 规范中提出了基于隐私 CA（PCA, privacy CA）的平台身份证明方案。该方案引入一个可信第三方（PCA），通过验证 TPM 内 EK 的正确性来为证明方颁发身份密钥（AIK, attestation identity key）证书；当证明方向挑战方请求验证平台身份的可信性时，证明方提供 AIK 证书作为平台的身份信息，挑战方验证 AIK 证书的正确性来确定平台身份的可信性。该方案虽然在一定程度上避免了身份的泄露，但是 AIK 证书的请求和验证都需要 PCA 的参与，PCA 的安全性和性能可能成为该方案的瓶颈。TPM v1.2 提出的直接匿名证明（DAA, direct anonymous attestation）的平台身份证明方案[7]采用群签名和零知识证明等密码学技术解决了平台匿名问题，提高了平台身份的隐私保护，但是该方案使用的签名技术长度过长，导致计算量过大、效率不高。对此，一些学者提出了改良的 DAA 方案[8]，如基于椭圆曲线及双线性映射对的优化的 DAA 方案，有效降低了传统 DAA 方案中长度过长和计算量大的问题，提高通信和计算性能。

在平台状态证明方面，证明方向挑战方报告平台软硬件配置的状态信息用于验证平台的可信性。基于二进制的证明是其他证明方法的基础。该方法是证明方在平台自启动时，从硬件可信根 TPM 开始，遵循“先度量，再验证，最后跳转”的思想，逐级度量启动序列上实体的完整性，并将度量结果的哈希值存储到 TPM 的平台配置寄存器（PCR, platform configuration register）内，如实地获取了系统从 BIOS 到操作系统各层次的完整性状态信息，再将这些度量信息报告给挑战方验证。在此基础上，文献[9]提出了完整性度量框架（IMA, integrity measurement architecture），该框架将完整性度量扩展到了应用层，实现应用程序加载时的完整性度量。IMA 将可信证明研究工作向前推进一大步，为实现系统的完整性度量提供了参考意义。随后，文献[10]在 IMA 的基础上提出了一种基于信息流完整性的证明方法（PRIMA, policy-reduced IMA）。该方法通过增加信息流完整性约束，简化了系统完整性证明的范围。上述基于二进制的证明方法存在易泄露平台配置信息、扩展性差、效率低、TOCTOU（time-of-check to time-of-use）等问题[11]。对此，有些学者开始基于属性证明（PBA, property-based attestation）方法的研究。PBA 是将系统的某些配置映射为具体的安全属性，然后证书中心颁发相应的安全属性证书，挑战方通过验证属性证书来判断证明方是否可信。PBA 不再直接验证配置信息的哈希值，一定程度上保护了平台的隐私和提高了可扩展性。IBM 公司提出了基于属性的证明框架[12]，随后有学者提出相应的证明方案和具体的证明协议。文献[13]提出了基于组件的属性证明方法，利用证书权威机构颁发各种组件属性证书，证明方根据配置的组件属性证书和 TPM 的完整性度量值向挑战方证明其配置的状态满足一定的安全属性，实现了细粒度的可信证明。

物理平台可信证明的框架如图 1 所示。该框架中包含 3 个实体：拥有 TPM 的证明方、挑战方以及证书颁发方。证明方负责基于 TPM 获取平台的身份或状态信息（如平台配置、软件特征、系统状态等），并将这些可信信息通过验证代理报告给挑战方。挑战方又称为验证者，负责请求证明方的可信信息，并根据相应的验证策略验证证明方的身份或平台的状态，从而判断其可信性。证书颁发方负责颁发证明方的身份证书或者属性证书，并在验证时提供证书的有效性的验证。3 个实体相互合作，共同实现物理平台的可信证明。

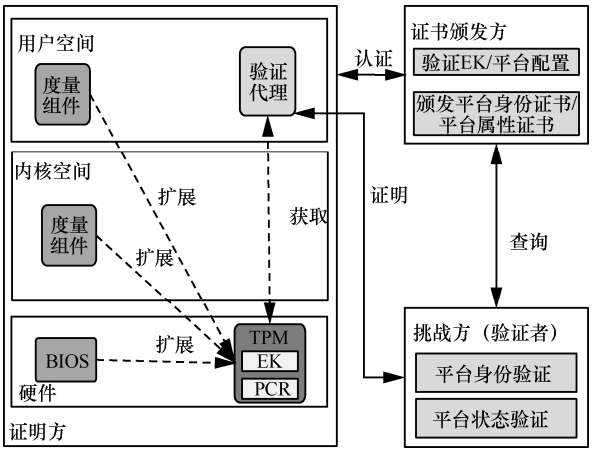


图 1 物理平台可信证明框架

3.2 虚拟平台可信证明

由于虚拟化平台高度虚拟化、动态伸缩、规模

庞大的特征，直接将物理平台的可信证明技术应用于虚拟机平台存在一些问题，一些学者对此展开了研究，如图 2 所示。

1) 可信根虚拟化技术。在物理平台下，每个证明方都拥有一个硬件防篡改的物理可信根 TPM，用于提供平台的身份信息，存储平台的可信度量值，以及远程证明等。但在虚拟化平台，由于资源的高度虚拟化，一台云服务器上可以同时部署多台虚拟机，而单个物理可信根无法同时为多台虚拟机提供可信服务，难以满足云平台可信的需求。因此需要可信根虚拟化技术，为虚拟机提供可信证明的基础。

2) 虚拟平台的身份证明技术。对于物理平台，其物理 TPM 拥有一个唯一且可信的 EK 标识平台的身份。但对于虚拟机，由于可信根虚拟化技术，无法提供一个硬件可信的虚拟 EK（vEK, virtual EK）标识虚拟机的身份。因此需要建立一条从物理 TPM 到虚拟 TPM 的证书链，将信任从物理平台扩展到虚拟机。除此之外，PCA 和 DAA 的平台身份证明方法，因为其对隐私 CA 的过度依赖或计算量过大等问题，难以适应大规模的云虚拟化环境。基于环签名的身份证明技术为解决大规模身份证明提供思路。

3) 虚拟平台的状态证明技术。物理平台从可信根开始构建信任链，通过逐级度量的方式获得平台的可信状态信息，并通过基于二进制或属性的方式进行平台的状态验证。对于虚拟平台，虚拟机的可信凭证不仅可以利用虚拟可信根通过构建信任链的方式获取，还可以利用虚拟机外度量技术。此外，对于云虚拟化平台，由于其动态的特性，进一步研究了基于行为的平台状态证明方法，以期实现对虚拟机动态、实时的可信证明。

4) 虚拟机的可信证明框架。在物理平台下，挑战方仅需与物理平台（证明方）建立可信连接以验证其可信性。但对于虚拟平台，虚拟机监视器（VMM, virtual machine monitor）和底层宿主机的可信性可能影响虚拟机的可信性。因此，在对虚拟机进行可信证明时，也需要证明底层平台的可信性。此时验证的对象发生了变化，可信证明框架也随之改变。

下一节将从这 4 个方面梳理虚拟平台可信证明的研究现状。

4　关键技术

4.1　可信根虚拟化

虚拟化技术是云计算的核心技术之一，其使一台云服务器上同时运行多台虚拟机。但是在可信证明中，单个物理可信根无法为每台虚拟机提供唯一的身份信息；并且，虚拟机的动态特性可能使通过构建信任链获取可信度量值的方案产生信任环路；此外，多台虚拟机的可信度量值的存储可能造成可信根资源访问冲突，降低可信性。为满足虚拟平台可信的需求，文献[14]提出了虚拟可信平台模块（vTPM, virtual trusted platform module）的概念，每台虚拟机都拥有独立的 vTPM。vTPM 通过模拟物理 TPM 的功能，为虚拟机提供身份凭证、存储可信度量值、保护敏感信息等，实现了多台虚拟机对 TPM 资源的共享和复用。

对于 vTPM 的实现方式，国内外展开了大量的研究，本文接下来将按照虚拟化类型和虚拟机监视器类型 2 种分类方式展开分析，并进一步介绍我国物理可信根及其虚拟化技术的研究现状。

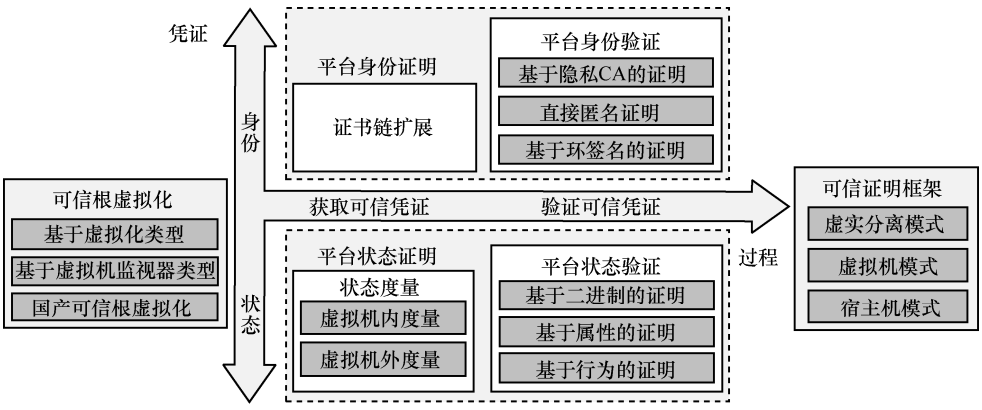
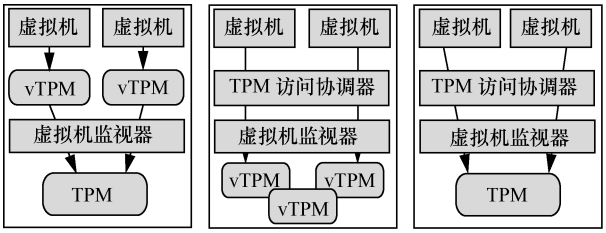


图 2　虚拟平台可信证明关键技术概括

4.1.1 基于虚拟化类型的 vTPM

根据虚拟化类型，vTPM 的实现方式可以分为软件 vTPM、硬件 vTPM 和半虚拟化 vTPM。图 3 显示了 Xen 平台下的这 3 种实现方式。



(a) 软件vTPM (b) 硬件vTPM (c) 半虚拟化vTPM

图 3 Xen 平台下 vTPM 实现方式

软件 vTPM 是通过软件模拟的方式为每台虚拟机提供一个与物理 TPM 相同功能的 vTPM 实例，如图 3(a)所示。文献[14]首次提出了基于 Xen 平台的软件 vTPM 实现方案，并介绍了在通用 TPM 和 IBM 的 PCIXCC 外部卡 2 种情况下的 vTPM 实现框架。该方案是由 Dom0 中的 TPM 管理器为每台虚拟机创建一个 vTPM 实例，并利用 Xen 平台的通信机制和隔离特性使虚拟机能够使用对应的 vTPM 实例构建自身的可信环境。同时，底层的物理平台利用物理 TPM 构建可信的运行环境，vTPM 与 TPM 协同保证这个平台的可信。此外，文献[15]提出了一个云租户可配置的软件的 vTPM 实现方案。该方案接收用户的安全策略，并根据策略为用户的虚拟机提供一个 μTPM，确保云服务提供商可以为用户提供一个满足其安全需求的可信虚拟机。

软件 vTPM 的实现方案可同时为多台虚拟机提供虚拟可信根，可用性较高。但是也存在一些明显的问题：首先，软件模拟的方式导致存储的敏感信息不再受硬件保护，并且软件 vTPM 的安全性也无法保证；其次，由于 vTPM 实例运行在 Dom0 中，利用内存泄露等方式便可窃取 vTPM 实例中的数据，增加了新的攻击面；再者，vTPM 与虚拟机间的绑定关系是明文配置，攻击者可以据此获得敏感的数据。

为了提高软件 vTPM 的安全性，文献[16]提出将 vTPM 置于 CPU 的系统管理模式（SMM, system management mode）中运行，实现了强隔离，保证了 vTPM 的安全。然而进入 SMM 模式需要挂起其他所有的 CPU 内核，性能开销大。文献[17]基于 Intel SGX 技术的隔离特性设计了一个新的可信安全组件 eTPM（enclave TPM），通过将 eTPM 的代码数据放在 SGX（software guard extensions）的隔离区域 enclave 中运行，确保 eTPM 运行时的安全。

硬件 vTPM 是通过修改物理 TPM，使之可以运行多个 vTPM 实例，从而为每台虚拟机提供独立的 vTPM，如图 3(b)所示。

文献[18]基于 Intel VT-x 技术提出了一个硬件辅助 vTPM 方案。该方案中扩展了 TPM 命令集，为每台 VM 提供一个 TPM 控制结构（TPMCS, TPM control structure），并为每台 VM 保存和加载单独的 vTPM 上下文，并且利用基于硬件保护的保护环隔离 vTPM 的上下文。当特定 VM 使用其 vTPM 时，vTPM 的前端驱动调用 TPM 命令加载到 TPM 对应的 TPMCS 中，实现了多台 VM 共用物理 TPM 的资源。该方案允许每台 VM 使用完整的 TPM 的功能，好像每台 VM 都拥有属于自己的 TPM，并且由硬件保护虚拟机的敏感信息，可信性和安全性高。但是该方案需要硬件辅助虚拟化的支持，并且需要修改物理 TPM，对于已经部署 TPM 的环境改动较大。此外，该方案无法支持多台虚拟机的并发访问，可用性不高，无法不适用于大规模的云虚拟化平台。

半虚拟化 vTPM 是在虚拟机监视器中添加对物理 TPM 的调度机制以及提供某些接口，为虚拟机提供中介访问物理 TPM，如图 3(c)所示。

文献[19]在虚拟机监视器中增加了半虚拟化模块来实现 VM 对 TPM 的访问，尽可能地保证所有 VM 之间公平的共享一个物理 TPM。该半虚拟化模块通过一个超级调用接口来允许 VM 直接调用虚拟机监视器，并对 TPM 的某些部分（如 PCR 和计数器）进行了复制和分区。模块内的上下文管理器维护了虚拟机与 vTPM 的关联，隔离不同的 VM 的 TPM 上下文。此外，该半虚拟化模块还包含了调度程序和命令过滤器等。该方案克服了软件 vTPM 局限性和对硬件辅助虚拟化的需求；实现了对物理 TPM 的多路复用。但是同一时间内仅允许一台虚拟机访问 TPM，无法支持多虚拟机的并发访问，可用性差，也尚未解决虚拟机身份密钥的分配和管理的问题。

4.1.2 基于虚拟机监视器类型的 vTPM

基于虚拟机监视器类型 vTPM 的实现方式，主要分为 Xen 和 KVM（Kernel-based VM）2 种架构，前文已分析了 Xen 架构下 vTPM 的实现方式，本节将对 KVM 中 vTPM 的实现方式展开介绍。

KVM 架构下 vTPM 的实现方式主要分为以下 3 类：TPM passthrough、基于函数库模拟和 CUSE TPM。

TPM passthrough 是一种基于硬件的 vTPM 实现方式。它利用 I/O 虚拟化技术使虚拟机直接使用物理 TPM 来实现 vTPM 的所有计算和存储操作。该方式将虚拟机和物理 TPM 直接绑定，可信性强；但也存在物理 TPM 单一时刻仅能被单台 VM 独占的问题，制约了可用性。

基于函数库模拟和 CUSE TPM 都是软件 vTPM 的实现。区别在于，基于函数库模拟是在 Qemu 内部使用 libtpms 函数库模拟物理 TPM，从而为每台 VM 提供 vTPM 实例。CUSE TPM 是在 QEMU 外部使用 libtpms 函数库模拟物理 TPM，再通过宿主机提供的 IOCTL 接口访问 vTPM 实例。这 2 种方式具有软件 vTPM 支持虚拟机并发访问、高可用性的优点；但同样存在 vTPM 自身的安全性，以及存储的敏感信息缺少安全防护的问题。基于 Intel SGX 技术的物理安全隔离特性和密封功能，可以实现对 KVM 架构下的软件 vTPM 运行时的安全保护[20]。

4.1.3　国产可信根虚拟化

我国也高度重视对可信计算领域的研究与发展，目前已经形成了基于使用国产密码算法的可信密码模块（TCM, trusted cryptography module）的可信计算体系，制定了一系列相关的标准。TCM 目前已得到广泛的应用，多种设备等已普遍集成 TCM，可支持基于 TCM 的安全启动和信任链的构建。

针对 TCM 虚拟化的研究也受到了广泛的关注。文献[21]提出了基于单根设备虚拟化技术的硬件 vTCM 实现方案。在该方案中，vTCM 是基于硬件实现，与 VM 一一对应，绕过了 VMM，直接为 VM 提供可信密码服务。这不仅提高了安全性，也进一步提高了效率，满足高安全可信虚拟环境的需求。随后，文献[22]也提出了一种 vTCM 方案，该方案是在底层宿主机的物理环境中增加少量的 vTCM，保证物理 TCM 和 vTCM 可以同时运行。在 vTCM 的调度模块和管理模块的相互配合下实现在 vTCM 有限的情况下多个 vTCM 的调度切换，如此一来，不仅支持为每台虚拟机分配一个绑定的 vTCM 实例，而且保证这些实例轮流在物理 vTCM 场景中运行，确保了安全要求和成本之间的平衡。

无论是 TPM 还是 TCM 都是被动设备，其功能的实现依赖于上层应用的调用。对此，我国提出了的可信平台控制模块（TPCM, trusted platform control module）的概念[23]，将对称密码和非对称密码相结合，以 TPCM 为根对整个平台进行主动控制和可信度量，增强了可信芯片的运算能力和控制能力，提高了平台的安全性和效率。TPCM 不再从属于 CPU，可以进行独立的设计，因此，其拥有比 TPM 更好的性能；并且 TPCM 的主动控制能力可以对云虚拟化平台实施动态的监控，保证运行环境实时的可信。因此，TPCM 将来很有可能成为实现云虚拟化平台可信根虚拟化的一个发展方向。

4.1.4　小结

本节首先从虚拟化类型和虚拟机监视器类型 2 个角度介绍了现有的 vTPM 的实现方式，方案对比如表 1 所示。进一步地，介绍了国内可信根 TCM 和 TPCM 以及它们的虚拟化研究现状。

目前来说，可信根虚拟化技术存在一些问题。首先，软件的 vTPM 实现方式通过软件模拟 TPM 的功能，违背了可信计算使用硬件保护敏感信息的初衷，无法保证软件 vTPM 自身的安全性以及其保

表 1　　**vTPM 类型对比**

虚拟机监视器类型	虚拟化方式	方案	并发访问支持	与物理 TPM 关系	性能	安全性
Xen	软件模拟	软件 vTPM[14]	多虚拟机并发	绑定	中	低
		基于 SMM 保护[16]	多虚拟机并发	绑定	差	高
		eTPM[17]	多虚拟机并发	绑定	好	高
	半虚拟化	半虚拟化 vTPM[19]	单虚拟机独占	直接访问	受限	中
	硬件	硬件辅助 vTPM[18]	单虚拟机独占	直接访问	受限	高
Qemu-KVM	软件模拟	基于函数库模拟	多虚拟机并发	完全脱离	较好	低
		CUSE TPM	多虚拟机并发	完全脱离	较好	低
		SvTPM[20]	多虚拟机并发	绑定	较好	高
	硬件	TPM passthrough	单虚拟机独占	直接访问	受限	高

护的敏感信息的可信性。现有的解决方案也存在引入额外性能开销的问题。其次，硬件和半虚拟化的vTPM实现方式，在某一时刻，物理TPM仅能被单台虚拟机独占，严重影响了可用性。面对动态化、大规模、分布式的云虚拟化平台，现有的可信根虚拟化方案无法满足云平台的大量的可信度量的需求。具有主动控制能力的TPCM在实现可信计算虚拟化技术中更具有优势，但目前TPCM的相关技术并不成熟，未来还需进一步的研究和探索。

4.2 平台身份证明

平台身份证明是证明方向挑战方提供平台的身份证书来证明其是可以被信任的实体。虚拟机的平台身份证明将从证书链的扩展和平台身份验证2个方面进行归纳、分析和总结。

4.2.1 证书链的扩展

每个物理TPM都拥有一个唯一的EK标识平台的身份，但出于安全和隐私保护的目的，平台身份证明过程并不直接使用EK，而是采用EK的别名AIK。由于EK是物理可信的，根据信任传递特性，则AIK也是可信的，从而可以利用AIK验证平台身份的可信。vTPM的实现方式中，软件vTPM通过软件模拟的方式为虚拟机提供类似物理TPM的接口和功能，被广泛应用。但软件vTPM没有硬件保护，无法提供一个可信的vEK，进而无法生成可信的虚拟AIK（vAIK, virtual AIK）。对此，虚拟机平台身份证明时，需要将证书链从物理TPM扩展到vTPM。

为了实现证书链的扩展，文献[14]提出了EK→AIK→vEK→vAIK的证书链方案。该方案中vEK和vAIK均由vTPM产生，利用物理TPM中的AIK签名来绑定vEK的可信，通过PCA验证vEK的可信并颁发vAIK证书用于虚拟机的身份证明。该方案直接将信任扩展到虚拟机，TPM和vTPM的证书结构一致，现有的物理平台身份证明协议可以直接应用于虚拟机，易于部署和实现。然而，AIK的时效很短，AIK的失效会导致vEK签名的失效，最终导致vAIK的失效，因此需要频繁地向PCA申请AIK证书、vAIK证书，增加PCA的负担；并且，此方案需要使用AIK对vEK签名，违背了TCG规范中AIK只能对TPM内部数据签名的要求。

为了解决AIK时效短的问题，文献[24]提出了EK→vEK→vAIK的证书链方案。该方案用TPM的EK替代AIK对vEK进行签名绑定。由于EK唯一且一直存在，因此解决了AIK时效短的问题。但根据TCG的规范，EK证书同样不能用于外部签名。

为了减少PCA的负担，文献[25]提出了EK→AIK→vAIK的证书链方案。该方案中vAIK证书直接由AIK签发，从而减少了PCA的使用。但同样存在不符合TCG规范的问题。

为了符合TCG规范，文献[26]提出了EK→AIK→SK→vAIK的证书链方案。该方案在TPM内引入签名密钥（SK, signature key），并以此为中介实现AIK对vAIK的间接签名。但该方案需要vAIK和SK一一绑定，产生大量的密钥冗余，并且vAIK的重构需要生成新的SK，也带来新的性能压力。文献[27]在TPM内增加一类证书——VMEK（virtual machine extension key），并提出了VMEK→vEK→vAIK的证书链方案。VMEK的密钥不可迁移，且可对TPM内外的数据签名和加密。由VMEK对vEK签名，实现了证书链的扩展，解决了违背TCG规范、增加密钥冗余和PCA性能负担等问题。

上述的证书链扩展方案中，vAIK证书的申请都需要TPM的支持，虚拟机状态切换频繁，将增加系统的负担。对此，文献[28]提出了EK→tEK→vEK→vAIK的证书链方案。该方案是在Xen平台下新增一个DomainT域，该域拥有一个身份密钥tEK。首先CA验证DomainT的完整性向其签发tEK证书；再由DomainT签发vEK证书，进而保证vAIK证书的合法性。vAIK证书的生成由DomainT参与，减少了对TPM的访问，减轻了系统负担。

综上所述，现有的虚拟机证书链扩展方案对比如表2所示，证书链的扩展方案正在向符合TCG规范，减少密钥冗余，降低PCA负担，以及vAIK证书的申请避免TPM的参与来不断优化和完善。

表2 虚拟机证书链扩展方案对比

方案	遵守规范	增加密钥冗余	增加隐私CA负担	依赖TPM
EK→AIK→vEK→vAIK	否	否	是	是
EK→vEK→vAIK	否	否	否	是
EK→AIK→vAIK	否	否	是	是
EK→AIK→SK→vAIK	是	是（多）	否	是
VMEK→vEK→vAIK	是	是（1）	否	是
EK→tEK→vEK→vAIK	是	否	否	否

4.2.2 平台身份验证

虚拟机的平台身份证明中，先通过证书链扩展获取虚拟机的可信身份证书，进一步需进行平台身份验证。在物理平台中，典型的方案为 PCA 方案和 DAA 方案。vTPM 的设计和实现使这些方案可以直接应用于虚拟机的身份验证，但是在实际应用中面临一些问题。首先，PCA 方案中，证明过程的各个操作都需要 PCA 的参与，PCA 的安全性和性能可能成为平台身份证明的瓶颈。在云虚拟化环境，虚拟机的数量显著增加，更加剧了 PCA 的负担。其次，DAA 方案虽然克服了 PCA 方案中 PCA 瓶颈局限性，但其复杂的计算量使其无法适用于大规模的云虚拟化平台。为此，一些学者将研究聚焦于基于环签名[29]的平台身份证明。

基于环签名的平台身份证明方案[30]是选定一个临时的包含签名者（证明方）的集合，签名者利用自己的私钥和集合中其他成员的公钥独立地产生签名，挑战方通过验证签名的正确性，确定证明方身份的合法性。该方案中，挑战方无法知道具体的签名者，满足匿名性的要求；集合中的其他成员并不知道自己包含其中，成员可以动态地增减，可扩展性强；并且方案中不存在群管理员，也避免了中心节点的性能瓶颈问题。文献[31]设计了一种基于环签名的虚拟机远程证明方案。该方案引入了一个私钥生成中心（PKG, private key generation），首先云平台采用基于 PCA 的证明方案向 PKG 证明物理平台的可信性；然后 PKG 和 vTPM 管理器通过无证书算法共同生成了 vTPM 环签名密钥；最后利用环签名技术实现虚拟机的可信证明。

PCA 方案、DAA 方案以及基于环签名的身份证明方案对比如表 3 所示。对于大规模的云虚拟化环境，基于环签名的方案更具有优势。但是环签名的无条件匿名，很难追溯不可信的证明方，并且基于环签名的研究相对较少，还处于起步阶段，此方案的推广和应用还需进一步探索。

表 3　平台身份证明方案对比

方案	签名方式	匿名性	效率	实现	适用范围
PCA 方案	一次一密	差	低	容易	较小或实名认证的局域网
DAA 方案	群签名	较好	低	较难	高性能服务器之间
基于环签名的身份证明方案	环签名	好	较高	困难	较大规模云数据中心

4.3 平台状态证明

平台状态证明是挑战方验证证明方的平台状态（如软硬件配置、系统状态）的可信性的过程。本节将从状态度量和平台状态验证 2 个方面来探讨。

4.3.1 状态度量

状态度量是为了获取证明方的可信度量凭证。从技术实现角度，可以将其分为虚拟机内度量和虚拟机外度量。

1) 虚拟机内度量

虚拟机内度量是将度量软件置于虚拟机内部，通过构建信任链的方式，逐级度量来获取虚拟机的可信凭证。

基于 vTPM，传统物理平台的 IMA、PRIMA 等完整性度量方案可以直接用于虚拟机，实现虚拟机内的平台状态度量。除此之外，文献[32]在每台虚拟机内部以内核模块的形式安装感知代理，利用此代理监控虚拟机内的系统事件，并将收集到的信息存储到一个共享的内存区域，最后由中心监控软件验证这些信息和控制相应的代理。

虚拟机内度量的方式可以实时获取虚拟机软硬件配置的完整性度量值，直接且易于实现。但这种方式需要将度量软件和被度量对象放在同一区域，度量软件易受到不合法程序的攻击，安全性低；其次，这种方式只能检测虚拟机内部的安全攻击，对于虚拟机外部的同驻攻击、侧信道攻击等无能为力；再者，虚拟机内度量的方式需要云服务提供商为每台虚拟机都提供虚拟可信根（vTCM、vTPM 等）和部署远程证明代理，增加了部署的难度和造成资源的浪费。

2) 虚拟机外度量

虚拟机外度量的方式是通过在虚拟机外部拦截虚拟机事件，间接获取虚拟机的可信证据。

虚拟机外度量的方式可以通过拦截系统调用等技术实现。文献[33]提出的 Patagonix 架构就是利用虚拟机监视器控制内存管理单元，在所有程序执行前度量其二进制文件内存页的完整性，从而验证虚拟机是否发生 rootkit 攻击；文献[34]提出的 HIMA 架构是在虚拟机监视器内添加钩子，主动拦截虚拟机内调用、中断、异常等，阻止未授权的二进制文件的执行，但这对虚拟机的每次系统调用都执行相应的处理，系统开销较大；文献[35]提出了 OB-IMA 完整性度量方案，该方案也是在虚拟机外部通过拦截系统调用的方式度量虚拟机内关键文件的完整

性，不仅度量了 IMA 方案中所考虑的文件，还进一步度量了影响系统行为和完整性的系统配置文件、程序加载器和脚本解释器等文件。在此基础上，文献[36]进一步提出了虚拟机内度量和虚拟机外度量相协同的完整性度量方案，并在 Windows 虚拟机内实现了该完整性度量方案，具有可接受的性能影响。

虚拟机自省技术（VMI, virtual machine introspection）作为虚拟机外度量中最流行的一种技术，也常被用于虚拟机外的可信度量。文献[37]在虚拟机外部通过 VMI、地址转换以及内容定位等技术，度量虚拟机内部运行的进程、内核模块以及动态链接库中不变量的完整性，以此来判断程序的可信性。针对云计算环境中加密服务调用的安全性，文献[38]提出了 En-ACCI 方案，利用 VMI 技术提供的丰富的虚拟机上下文信息，更好实现了访问控制和审计。但该方案仅在加密服务调用时才验证，未对已经验证过的代码页提供任何保护，易遭受 TOCTOU 攻击。对此，文献[39]提出了一种透明且细粒度的二进制完整性验证方案（TF-BIV），该方案在进程创建时识别敏感进程，检查与进程相关的 Guest OS 内核及依赖的二进制文件的完整性，并且利用现有的 Intel EPT（extended page table）和 MTF（monitor trap flag）机制来连续监视对目标进程页和已验证物理页的更新，有效地满足了二进制验证方案需满足的隔离性、透明性、TOCTOU 攻击和细粒度的验证，且性能开销很小。

与虚拟机内度量的方式相比，虚拟机外度量的方式将度量软件与度量对象分离，度量软件不易被攻击者屏蔽，增加了安全性。但是由于无法直接获取虚拟机内的可信度量值，存在语义鸿沟等问题。

综上所述，虚拟机内度量和虚拟机外度量这 2 种方式的对比如表 4 所示。虚拟机内度量的方式可以直接度量虚拟机内的状态的度量值，获得丰富的语义信息，但是度量软件与度量对象不隔离，安全性较差；虚拟机外度量的方式是在虚拟机外获取虚拟机的可信证据，对虚拟机透明，因此安全性较高，但是语义信息空白会导致语义信息缺失。

4.3.2 平台状态验证

根据可信度量凭证的差异，可以将虚拟化平台的平台状态验证分为基于二进制的证明、基于属性的证明以及基于行为的证明。

1) 基于二进制的证明

基于二进制的证明是在平台状态证明时直接用二进制哈希值表示平台的可信凭证。

第一类是通过在服务器内部构建一个可信虚拟机监视器（TVMM, trusted virtual machine monitor），为虚拟机提供一个可信的隔离执行环境。文献[40]提出的 Terra 模型是构建了一个 TVMM，实现在一个高可靠的通用平台上为用户提供互相隔离的虚拟机底层部件，从而保护了闭盒虚拟机的隐私和完整性。文献[41]提出了可信云计算平台（TCCP, trusted cloud computing platform）模型。该模型引入了一个云外部可信实体——可信协调器（TC, trusted coordinator），基于二进制证明技术，TC 可以验证云节点的可信性并控制虚拟机只能在可信节点中启动和迁移。在 TCCP 模型中，所有的安全可信操作都需要与 TC 交互，当节点规模很大时，TC 的节点管理的时间开销也会增加，制约性能。对此，有学者提出在云平台内部选择节点充当 TC 的角色[42]，有效地将 TC 的任务分散，缓解 TC 的压力。

第二类是基于 vTPM 的实现，将传统的物理平台的二进制可信证明方案用于虚拟机。文献[43]提出了双层非平衡散列树的远程证明方案。该方案引入了层级的概念，构建了双层非平衡散列树，将单一树扩展为主树和子树，主树和子树分别对应云平台中的虚拟机和虚拟机中的度量组件，证明时仅需要提供待度量组件和认证路径，细化了证明粒度，提高了证明效率，还提供了较好的隐私保护能力。文献[44]提出了一种博弈论的方法来分析开源云的可信性，同时讨论了可信计算对云计算的有效性。开源的软件系统提高了攻击者对软件系统的了解，增加了系统遭受攻击的可能性，但云

表 4 虚拟机可信状态度量方式对比

方式	原理	安全性	透明性	语义信息	虚拟化支持
虚拟机内度量	利用操作系统的安全机制	差	不透明	丰富	不需要
虚拟机外度量	操作系统外实现的安全机制	好	透明	空白	需要

租户可以利用基于二进制的证明技术验证底层平台和虚拟机的可信性，增强了对云服务提供商的信任程度。

构建 TVMM 的二进制证明方式本质上是对物理平台进行二进制证明，在可信的物理环境的基础上为虚拟机提供一个可信的隔离执行环境，保证运行在隔离环境的虚拟机不受非法的篡改，但是无法验证虚拟机自身的可信性。基于 vTPM 的二进制证明方式是通过构建信任链获取平台软硬件的完整性度量值，只能验证虚拟机的特定时刻的可信状态，是一种静态的证明方式。然而在云虚拟化环境中，虚拟机是动态的，其可信状态可能由于迁移等操作而改变，基于二进制的静态证明方式已经不足以验证虚拟机的可信状态。因此，一些学者研究云虚拟化环境下基于属性的可信证明。

2) 基于属性的证明

基于属性的证明是虽然平台运行不同的组件、拥有不同的配置，但只要能提供相同的属性，就认为其是可信的。

基于属性的证明方式可以通过一个代理将平台的完整性度量值转化为相应的属性用于平台状态证明。文献[45]根据安全属性的需求和信任策略将平台度量值转换为相应的属性，利用转换后的属性验证平台的可信性，从而有效监测和阻止对云基础设施的攻击，保障了租户虚拟机的安全。文献[46]将基于属性的证明技术和云安全监控系统 CloudPass 结合，实现对 CloudPass 系统的完整性验证和平台身份验证。

除此之外，基于属性的证明还可以直接利用虚拟机自身的安全属性来验证虚拟机的平台状态。文献[47]通过租户虚拟机流量源地址的正确性、来自租户虚拟机的流量以及租户虚拟机的状态这 3 个属性验证租户虚拟机的行为可信，对于不可信的虚拟机可以动态隔离，甚至精细到终止服务，有效减少了租户和客户之间的攻击。文献[48]提出了一种云环境下虚拟机监视和验证框架（CloudMonatt），不仅验证虚拟机在启动和运行时的完整性，还进一步验证虚拟机的机密性和可用性，完成对虚拟机全生命周期的可信验证，防止了潜在的安全漏洞。

3) 基于行为的证明

为了实现虚拟机动态证明，还有学者提出了基于行为的证明。基于行为的证明方式是通过验证系统或程序在运行时的行为变化来推理其可信性。

文献[49]通过拦截系统调用和 VMI 技术获取虚拟机内进程的上下文信息，对虚拟机的进程列表、模块列表等的一些行为进行“行为跟踪”，并利用这些行为变化特征验证虚拟机在运行时的可信性。在产业界，阿里云结合大数据分析和机器学习技术，对白名单应用的系统调用行为进行分析。搜集了用户正常行为并建立行为规则库，此后实时采集应用行为数据，对比应用行为规则库，从而验证应用行为的可信性。

在平台状态验证的研究中，根据可信度量凭证可以分为基于二进制的证明、基于属性的证明、基于行为的证明，其对比如表 5 所示。基于二进制的证明可以直接验证度量组件的可信状态信息，易于实现。但是二进制是静态的验证方式，难以应对云计算环境虚拟化和动态化的特性。基于属性证明和基于行为的证明这种方式都可以实现对虚拟机动态的平台状态验证，大大提高了证明的灵活性。但是，就目前的研究来说，存在着可信属性和行为特征的规范化定义不足，缺少理论支撑等问题。

表 5　　平台状态证明方式对比

特性	安全性	灵活性	性能	实现
二进制	中	低	很快	较易
属性	较高	高	中	难
行为	高	高	中	很难

4.4　虚拟机可信证明框架

在云虚拟化平台，虚拟机监视器负责资源的分配、虚拟机与宿主机以及管理软件的通信。恶意的虚拟机监视可能会破坏虚拟机的完整性，从而影响虚拟机的可信性。因此，在仅验证虚拟机的可信性而不验证底层平台（虚拟机监视器或宿主机）的情况下，虚拟机可信的结论是不准确的。虚拟机的可信证明需要满足同一性的需求，即虚拟机的可信证明应与底层平台的证明绑定在一起。对此，形成 3 种主要的虚拟机可信证明框架，即虚实分离模式的可信证明框架、虚拟机模式的可信证明框架和宿主机模式的可信证明框架。

虚实分离模式的可信证明框架如图 4(a)所示，该框架在虚拟机和宿主机内分别部署验证代理，通过完整性度量和可信验证技术，挑战方分别验证虚拟机和宿主机的可信性，2 个验证结果最终表示整

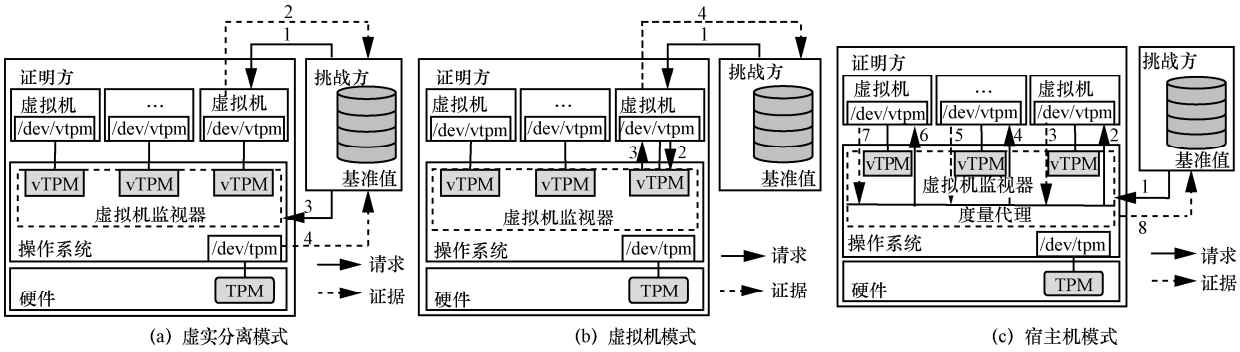


图 4　虚拟机可信证明框架

个平台的可信性。该框架直接利用物理平台成熟的可信证明技术，在实现方面改动较少；同时，对挑战方而言，虚拟机和宿主机是等价的，可以平等地验证，简化了挑战方的难度。但是，此框架需要虚拟机、虚拟机监视器以及宿主机之间相互隔离，彼此之间没有相互影响，在实际生产中无法满足此要求；再者，虚拟机和虚拟机监视器应该是绑定的，挑战方应知道它们之间的绑定关系，避免同一性问题。文献[50]利用度量联系和 MAC 地址判定解决了证明过程中的同一性问题。但在云环境中，虚拟机迁移等操作势必会破坏绑定关系，因此带来了绑定关系的一致性同步问题。

虚拟机模式的可信证明框架如图 4(b)所示，该框架是将宿主机的可信信息映射到虚拟机，并通过虚拟机与挑战方建立的可信连接一起验证虚拟机和宿主机的可信性。此框架将宿主机和虚拟机绑定，保证了同一性，避免了绑定更新的同步问题；然而，当宿主机的可信凭证无法及时映射时，无法保证可信证明时可信信息的新鲜度。

这 2 种框架每验证一台虚拟机时都需要验证其底层的宿主机，造成了验证的冗余；同时，需要频繁使用 TPM，TPM 的性能制约可信证明的效率；并且，每台虚拟机都要与挑战方交互，增加了平台身份证明的负担；再者，大量的虚拟机与挑战方连接，也造成网络的拥塞。综上，这 2 种框架更适用于有限数量的虚拟机的可信证明。

为了适用大规模的云虚拟化环境，支持更多数量的虚拟机的可信证明，有学者提出了宿主机模式可信证明框架[51]，如图 4(c)所示。此框架中，虚拟机不再直接与挑战方交互，而是在虚拟机监视器层增加一个代理，代理利用虚拟机外监控技术获取虚拟机的可信信息，并将其与宿主机的可信信息一同报告给挑战方。基于此框架，文献[52]利用 VMI 技术实现了虚拟机的可信证明，但是该方案需要对每台虚拟机都执行一个很耗时的 TPM_Qoute 操作，在大规模的云环境，会影响证明的可扩展性。

虚拟机的可信证明不仅要满足 MIRTE 提出的远程证明设计时的 5 项基本原则，还应进一步满足同一性和可扩展性的需求。现根据这 7 项要求对上述 3 种框架进行对比，如表 6 所示。其中宿主机模式的可信证明框架更为完善，但现有的研究中仍存在 TPM 性能的制约的问题，使其无法适用于大规模的云虚拟化环境。

5　未来的研究展望

本文主要围绕云虚拟化平台可信证明中可信根虚拟化、平台身份证明、平台状态证明、虚拟机可信证明框架 4 个关键技术展开综述，通过分析可知，仍存在一些问题尚未解决，未来的研究工作中，可以更多地关注以下几个方面。

1) 适用于云虚拟化平台的可信根虚拟化方案。根据前文所述内容，软件 vTPM 方案存在功能缺失

表 6　　**虚拟机可信证明框架对比**

原则	新鲜信息	综合信息	约束泄露	语义明确	可信通信机制	同一性	可扩展性
虚实分离模式	好	好	好	好	好	差	差
虚拟机模式	差	好	好	好	好	好	较差
宿主机模式	好	好	好	好	好	好	好

的问题，无法保证本身的可信性；基于硬件和半虚拟化方式的 vTPM 性能不足，无法满足大规模、动态的云平台可信度量的需求；TPCM 可能成为适用于云平台可信根的发展方向，但目前来说，相关技术还不成熟，亟须展开进一步的研究。

2) 适用于虚拟机运行时动态的可信度量机制。现有虚拟机度量机制都仅度量虚拟机运行时关键不变量的完整性，片面地表示虚拟机运行时的可信状态，其虚拟机可信的结论并不十分准确。因此，需要一种新的机制，实现对虚拟机运行时整体的可信度量和验证。

3) 适用于云虚拟化平台的可信证明系统。现有的虚拟机可信证明框架都是对虚拟机逐一验证，云虚拟化平台的规模在不断扩大，逐一验证的方式易造成网络的拥塞，并且挑战方的性能也会制约可信证明的效率。因此，需要从虚拟机的平台身份证明、平台状态证明以及可信证明框架的多个方面进行系统化的设计，为大规模、动态化的云虚拟化平台提供一个高效、灵活、可扩展的可信证明系统。

6　结束语

随着云计算技术进一步成熟，随之而来的云平台的可信性问题也将成为未来信息安全领域学术界和产业界的关注焦点。本文结合可信证明的定义，在物理平台的可信证明关键技术的基础上，对虚拟机的可信证明关键技术进行梳理、分析和总结，为研究人员进行下一步的研究工作提供有益探索。

参考文献：

[1] 朱民, 涂碧波, 孟丹. 虚拟化软件栈安全研究[J]. 计算机学报, 2017, 40(2): 481-504.
ZHU M, TU B B, MENG D. The security research of virtualization software stack[J]. Chinese Journal of Computers, 2017, 40(2): 481-504.

[2] 张玉清, 王晓菲, 刘雪峰, 等. 云计算环境安全综述[J]. 软件学报, 2016, 27(6): 1328-1348.
ZHANG Y Q, WANG X F, LIU X F, et al. Survey on cloud computing security[J]. Journal of Software, 2016, 27(6): 1328-1348.

[3] 沈昌祥. 用可信计算构筑云计算安全[J]. 中国经贸导刊, 2017(16): 56-57.
SHEN C X. Constructing cloud security with trusted computing[J]. China Economic & Trade Herald, 2017(16): 56-57.

[4] 马力, 祝国邦, 陆磊. 《网络安全等级保护基本要求》(GB/T 22239-2019)标准解读[J]. 信息网络安全, 2019(2): 77-84.
MA L, ZHU G B, LU L. Baseline for classified protection of cybersecurity (GB/T 22239-2019) standard interpretation[J]. Netinfo Security, 2019(2): 77-84.

[5] COKER G, GUTTMAN J, LOSCOCCO P, et al. Attestation: evidence and trust[C]//Information and Communications Security. Berlin: Springer, 2008: 1-18.

[6] 施光源, 张建标. 可信计算领域中可信证明的研究与进展[J]. 计算机应用研究, 2011, 28(12): 4414-4419.
SHI G Y, ZHANG J B. Research and development of trustworthiness attestation in trusted computing[J]. Application Research of Computers, 2011, 28(12): 4414-4419.

[7] BRICKELL E, CAMENISCH J, CHEN L Q. Direct anonymous attestation[C]//Proceedings of the 11th ACM conference on Computer and communications security. New York: ACM Press, 2004: 132-145.

[8] CHEN L Q. A DAA scheme using batch proof and verification[C]//Proceedings of the 3rd International Conference on Trust and Trustworthy Computing. Berlin: Springer, 2010: 166-180.

[9] SAILER R, ZHANG X, JAEGER T, et al. Design and implementation of a TCG-based integrity measurement architecture[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2004: 223-238.

[10] JAEGER T, SAILER R, SHANKAR U. PRIMA: policy-reduced integrity measurement architecture[C]//Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2006: 19-28.

[11] SON J, KOO S, CHOI J, et al. Quantitative analysis of measurement overhead for integrity verification[C]//Proceedings of the Symposium on Applied Computing. New York: ACM Press, 2017: 1528-1533.

[12] PORITZ J, SCHUNTER M, VAN HERREWEGHEN E, et al. Property attestation—scalable and privacy-friendly security assessment of peer computers[R]. IBM Research, Technical Report RZ 3548, 2004.

[13] 秦宇, 冯登国. 基于组件属性的远程证明[J]. 软件学报, 2009, 20(6): 1625-1641.
QIN Y, FENG D G. Component property based remote attestation[J]. Journal of Software, 2009, 20(6): 1625-1641.

[14] BERGER S, CERES R, GOLDMAN K A, et al. vTPM: virtualizing the trusted platform module[C]//Proceedings of the 15th Usenix Security Symposium. Berkeley: USENIX Association, 2006: 305-320.

[15] HE R Y, WU S J, JIANG L. A user-specific trusted virtual environment for cloud computing[J]. Information Technology Journal, 2013, 12(10): 1905-1913.

[16] 严飞, 石翔, 李志华, 等. VirtinSpector: 一种基于 UEFI 的虚拟机动态安全度量框架设计与实现[J]. 四川大学学报(工程科学版), 2014, 46(1): 22-28.
YAN F, SHI X, LI Z H, et al. VirtinSpector: a UEFI based dynamic secure measurement framework for virtual machine[J]. Journal of Sichuan University (Engineering Science Edition), 2014, 46(1): 22-28.

[17] SUN H N, HE R Y, ZHANG Y, et al. eTPM: a trusted cloud platform enclave TPM scheme based on intel SGX technology[J]. Sensors, 2018, 18(11): 3807.

[18] STUMPF F, ECKERT C. Enhancing trusted platform modules with hardware-based virtualization techniques[C]//Proceedings of 2008 Second International Conference on Emerging Security Information, Systems and Technologies. Piscataway: IEEE Press, 2008: 1-9.

[19] ENGLAND P, LOESER J. Para-virtualized TPM sharing[C]// International Conference on Trusted Computing. Berlin: Springer, 2008: 119-132

[20] WANG J, FAN C, WANG J, et al. SvTPM: a secure and efficient vTPM in the cloud[J]. arXiv Preprint, arXiv:1905.08493, 2019.

[21] 刘明达, 曹慧渊, 拾以娟, 等. 基于 SR-IOV 的 TCM 硬件虚拟化构建可信虚拟环境[J]. 武汉大学学报(理学版), 2017, 63(2): 117-124.

LIU M D, CAO H Y, SHI Y J, et al. Building trusted virtual environment by TCM hardware virtualization based on SR-IOV[J]. Journal of Wuhan University (Natural Science Edition), 2017, 63(2): 117-124.

[22] 胡俊, 刁子朋. vTCM: 一种基于物理可信计算环境虚拟化的虚拟可信密码模块[J]. 山东大学学报(理学版), 2019, 54(7): 77-88.
HU J, DIAO Z P. vTCM: a virtualized trusted cryptography module based on the virtualization of physical trusted computing environment[J]. Journal of Shandong University (Natural Science), 2019, 54(7): 77-88.

[23] 黄坚会, 沈昌祥, 谢文录. TPCM 三阶三路安全可信平台防护架构[J]. 武汉大学学报(理学版), 2018, 64(2): 109-114.
HUANG J H, SHEN C X, XIE W L. The TPCM 3P3C defense architecture of safety and trusted platform[J]. Journal of Wuhan University (Natural Science Edition), 2018, 64(2): 109-114.

[24] GOYETTE R. A review of vTPM: virtualizing the trusted platform module[J]. Proceedings of Network Security and Cryptography, 2007: 1-17.

[25] STUMPF F, BENZ M, HERMANOWSKI M, et al. An approach to a trustworthy system architecture using virtualization[C]//International Conference on Autonomic and Trusted Computing. Berlin: Springer, 2007: 191-202.

[26] 王丽娜, 高汉军, 余荣威, 等. 基于信任扩展的可信虚拟执行环境构建方法研究[J]. 通信学报, 2011, 32(9): 1-8.
WANG L N, GAO H J, YU R W, et al. Research of constructing trusted virtual execution environment based on trust extension[J]. Journal on Communications, 2011, 32(9): 1-8.

[27] 谭良, 齐能, 胡玲碧. 虚拟平台环境中一种新的可信证书链扩展方法[J]. 通信学报, 2018, 39(6): 133-145.
TAN L, QI N, HU L B. New extension method of trusted certificate chain in virtual platform environment[J]. Journal on Communications, 2018, 39(6): 133-145.

[28] 王冠, 郭一清, 陈建中. 云环境下可信系统架构与虚拟证书链生成研究[J]. 计算机科学与应用, 2018, 8(5): 738-747.
WANG G, GUO Y Q, CHEN J Z. Research on trusted system architecture and virtual certificate chain in cloud environment[J]. Computer Science and Application, 2018, 8(5): 738-747.

[29] BENDER A, KATZ J, MORSELLI R. Ring signatures: stronger definitions, and constructions without random oracles[C]//Theory of Cryptography Conference. Berlin: Springer, 2006: 60-79.

[30] LIU J Q, ZHAO J, HAN Z. A remote anonymous attestation protocol in trusted computing[C]//Proceedings of 2008 IEEE International Symposium on Parallel and Distributed Processing. Piscataway: IEEE Press, 2008: 1-6.

[31] 荣星, 赵勇. 基于无证书环签名的虚拟机可信证明方案[J]. 计算机应用, 2017, 37(2): 378-382.
RONG X, ZHAO Y. Trustworthiness attestation scheme for virtual machine based on certificateless ring signature[J]. Journal of Computer Applications, 2017, 37(2): 378-382.

[32] STELTE B, KOCH R, ULLMANN M. Towards integrity measurement in virtualized environments—a hypervisor based sensory integrity measurement architecture (SIMA)[C]//Proceedings of 2010 IEEE International Conference on Technologies for Homeland Security (HST). Piscataway: IEEE Press, 2010: 106-112.

[33] LITTY L, LAGAR-CAVILLA H A, LIE D. Hypervisor support for identifying covertly executing binaries[C]//Proceedings of the 17th USENIX Security Symposium. Berkeley: USENIX Association, 2008: 243-258.

[34] AZAB A M, NING P, SEZER E C, et al. HIMA: a hypervisor-based integrity measurement agent[C]//Proceedings of 2009 Annual Computer Security Applications Conference. Piscataway: IEEE Press, 2009: 461-470.

[35] XING B, HAN Z, CHANG X L, et al. OB-IMA: out-of-the-box integrity measurement approach for guest virtual machines[J]. Concurrency and Computation: Practice and Experience, 2015, 27(5): 1092-1109.

[36] 邢彬, 韩臻, 常晓林, 等. 基于虚拟机监控技术的可信虚拟域[J]. 信息安全学报, 2016, 1(1): 75-94.
XING B, HAN Z, CHANG X L, et al. Trusted virtual domain based on virtual machine introspection technology[J]. Journal of Cyber Security, 2016, 1(1): 75-94.

[37] 林杰, 刘川意, 方滨兴. IVirt: 基于虚拟机自省的运行环境完整性度量机制[J]. 计算机学报, 2015, 38(1): 191-203.
LIN J, LIU C Y, FANG B X. IVirt: runtime environment integrity measurement mechanism based on virtual machine introspection[J]. Chinese Journal of Computers, 2015, 38(1): 191-203.

[38] JIANG F, CAI Q, GUAN L, et al. Enforcing access controls for the cryptographic cloud service invocation based on virtual machine introspection[C]//International Conference on Information Security. Berlin: Springer, 2018: 213-230.

[39] JIANG F J, CAI Q W, LIN J Q, et al. TF-BIV: transparent and fine-grained binary integrity verification in the cloud[C]//Proceedings of the 35th Annual Computer Security Applications Conference. New York: ACM Press, 2019: 57-69.

[40] GARFINKEL T, PFAFF B, CHOW J, et al. Terra: a virtual machine-based platform for trusted computing[C]//Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles. New York: ACM Press, 2003: 193-206.

[41] SANTOS N, GUMMADI K P, RODRIGUES R. Towards trusted cloud computing[J]. HotCloud, 2009, 9(9): 3.

[42] WANG H Z, HUANG L S. An improved trusted cloud computing platform model based on DAA and privacy CA scheme[C]// Proceedings of 2010 International Conference on Computer Application and System Modeling (ICCASM 2010). Piscataway: IEEE Press, 2010: 13-33.

[43] 荣星, 沈昌祥, 江荣, 等. 基于双层非平衡散列树的云平台远程验证方案[J]. 通信学报, 2017, 38(9): 31-38.
RONG X, SHEN C X, JIANG R, et al. Remote attestation scheme for cloud platform based on double-layer unbalanced hash tree[J]. Journal on Communications, 2017, 38(9): 31-38.

[44] KAMHOUA C A, RUAN A B, MARTIN A, et al. On the feasibility of an open-implementation cloud infrastructure: a game theoretic analysis[C]//Proceedings of 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC). Piscataway: IEEE Press, 2015: 217-226.

[45] XIN S Y, ZHAO Y, LI Y. Property-based remote attestation oriented to cloud computing[C]//Proceedings of 2011 Seventh International Conference on Computational Intelligence and Security. Piscataway: IEEE Press, 2011: 1028-1032.

[46] AWAD A, KADRY S, LEE B, et al. Property based attestation for a secure cloud monitoring system[C]//Proceedings of 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing. Piscataway: IEEE Press, 2014: 934-940.

[47] VARADHARAJAN V, TUPAKULA U. Counteracting security attacks in virtual machines in the cloud using property based attestation[J].

Journal of Network and Computer Applications, 2014, 40: 31-45.

[48] ZHANG T W, LEE R B. CloudMonatt: an architecture for security health monitoring and attestation of virtual machines in cloud computing[C]//Proceedings of the 42nd Annual International Symposium on Computer Architecture. New York: ACM Press, 2015: 362-374.

[49] ZHOU Z, WU L, HONG Z, et al. DTSTM: dynamic tree style trust measurement model for cloud computing[J]. KSII Transactions on Internet and Information Systems, 2014, 8(1): 305-325.

[50] 胡玲碧, 谭良. 云环境中可信虚拟平台的远程证明方案研究[J]. 软件学报, 2018, 29(9): 2874-2895.
HU L B, TAN L. Research on trusted virtual platform remote attestation method in cloud computing[J]. Journal of Software, 2018, 29(9): 2874-2895.

[51] LAUER H, KUNTZE N. Hypervisor-based attestation of virtual environments[C]//Proceedings of 2016 IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld). Piscataway: IEEE Press, 2016: 333-340.

[52] 王伟, 陈兴蜀, 兰晓, 等. 基于 VMI 的虚拟机远程证明方案[J]. 网络与信息安全学报, 2018, 4(12): 32-43.
WANG W, CHEN X S, LAN X, et al. VMI-based virtual machine remote attestation scheme[J]. Chinese Journal of Network and Information Security, 2018, 4(12): 32-43.

[作者简介]

涂碧波（1977− ），男，湖北红安人，博士，中国科学院信息工程研究所研究员、博士生导师，主要研究方向为数据中心前沿技术与安全体系。

程杰（1994− ），女，河北秦皇岛人，中国科学院大学博士生，主要研究方向为可信计算与云计算安全。

夏豪骏（1987− ），男，湖北鄂州人，中国科学院大学博士生，中国科学院信息工程研究所工程师，主要研究方向为安全可信嵌入式系统。

张坤（1987− ），女，山东济南人，中国科学院大学博士生，中国科学院信息工程研究所高级工程师，主要研究方向为操作系统、虚拟化安全等。

孙瑞娜（1982− ），女，新疆乌鲁木齐人，中国科学院大学博士生，新疆财经大学讲师，主要研究方向为云安全、软件定义网络。