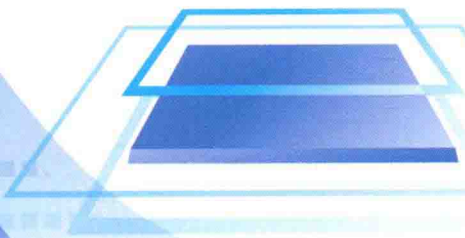
可信平台模块虚拟化与证明

Trusted Platform Module Virtualization and Attestation

谭 良 著



科学出版社

可信平台模块虚拟化与证明
Trusted Platform Module Virtualization and Attestation

谭 良 著

科学出版社
北京

内 容 简 介

本书系统化地介绍 TPM 虚拟化、可信虚拟平台及虚拟域(或终端)的证明。TPM 虚拟化是可信云环境的核心，本书详细介绍可信虚拟平台具有瀑布特征的信任链模型及理论、可信虚拟平台新的证书信任扩展方法、基于影子页表+的软件型 vTPM 密钥保护方案、可信虚拟平台 vTPM 动态迁移方法，从理论和实践两方面系统回答 TPM 虚拟化所涉及的所有问题。虚拟平台及虚拟域(或终端)的可信证明是云计算进一步延展和广泛应用的基础，详细介绍可信虚拟平台的远程证明方案、可信终端的远程证明方案、一种优化的直接匿名证言协议方案、可信终端动态运行环境的可信证据收集机制、直接匿名证言协议的性能估算新方法、可信终端动态运行环境的可信证据收集代理、一种新的可信终端运行环境远程证明方案，从理论和实践两方面给出虚拟平台及虚拟域(或终端)的可信证明所涉及的各种问题，具有一定的理论和实践意义。

本书可供可信计算、可信云计算，以及对可信云计算感兴趣的信息安全、计算机及其他领域的学者和工程技术人员参考使用。

图书在版编目 (CIP) 数据

可信平台模块虚拟化与证明/谭良著. —北京：科学出版社，2018.8
ISBN 978-7-03-055769-8

Ⅰ. ①可… Ⅱ. ①谭… Ⅲ. ①计算机网络－网络安全－研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 298656 号

责任编辑：闫 悦 王迎春 / 责任校对：王萌萌
责任印制：张克忠 / 封面设计：迷底书装

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

河北鹏润印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2018 年 8 月第 一 版 开本：720×1 000 1/16
2018 年 8 月第一次印刷 印张：17 1/4
字数：323 000

定价：108.00 元

(如有印装质量问题，我社负责调换)

序

可信计算是一种信息系统安全新技术，包括可信硬件、可信软件、可信网络和可信计算应用等诸多方面。迄今已有 35 年的发展历史，1983 年美国国防部制定了世界上第一个可信计算机系统评价准则(trusted computer system evaluation criteria, TCSEC)，在 TCSEC 中第一次提出可信计算机(trusted computer)和可信计算基(trusted computing base，TCB)的概念，并把 TCB 作为系统安全的基础。之后，美国国防部又相继推出了可信网络解释(trusted network interpretation，TNI)和可信数据库解释(trusted database interpretation，TDI)，从而形成了最早的一套可信计算技术文件。1999 年，IBM、HP、Intel 和微软等著名 IT 企业发起成立了可信计算平台联盟(Trusted Computing Platform Alliance，TCPA)。TCPA 的成立标志着可信计算高级阶段的形成。2003 年 TCPA 改名为可信计算组织(Trusted Computing Group，TCG)，标志着可信计算技术和应用领域的进一步扩大。TCPA 和 TCG 的出现形成了可信计算的新高潮。TCG 是一个非营利组织，旨在研究制定可信计算的工业标准。目前 TCG 已经制定了一系列的可信计算技术规范，如可信 PC、可信平台模块(trusted platform module，TPM)、可信软件栈(trusted software stack，TSS)、可信网络连接(trusted network connection，TNC)、可信手机模块等，并且不断地对这些技术规范进行修改完善和版本升级。

我国在可信计算领域起步不晚、水平不低、成果可喜。2006 年在国家密码管理局的主持下，我国制定了《可信计算平台密码技术方案》和《可信计算密码支撑平台功能与接口规范》。2007 年，在全国信息安全标准化技术委员会的主持下，我国制定了一系列可信计算标准，包括芯片、主板、软件、可信网络连接等标准。这些成果的取得与学术界对相关问题的关注、参与和研究密切相关。而我国可信计算技术逐步推广和应用，更与学术界的研究有极大的关系。自从可信计算概念提出以来，学术界对各种相关问题作了比较全面的研究，取得了丰硕的研究成果。就以发表在国内的学术成果来说，截至 2017 年 12 月，根据中国知网的记录，单以可信计算为篇名的有 614 篇，其中核心期刊以上 190 篇；以可信计算为关键字的有 1743 篇，其中核心期刊以上 651 篇；以可信计算为篇名的硕士论文 93 篇，以可信计算为关键字的硕士论文 388 篇；以可信计算为篇名的博士论文 21 篇，以可信计算为关键字的博士论文 86 篇。这些数据说明学术界关于可信计算的研究非常广泛。

可信计算的基本思想是在通用计算平台上嵌入一个防篡改的硬件可信安全芯片，利用芯片的安全特性保证系统按照预期的行为执行，从根本上提高终端的安全

性。四川师范大学谭良教授用了数年的时间撰写了本书。本书关于可信平台模块虚拟化及证明方面的研究有一定的创新，具有以下特点。

(1)选题新颖，有研究意义。本书加强了我国可信计算中可信计算平台证明及TPM虚拟化问题的研究。谭良教授对TPM虚拟化及可信计算平台证明进行了非常系统、深入、全面的研究。例如，在可信计算平台证明方面，包括《TCG架构下的证明问题研究及进展》《一种可信终端运行环境远程证明方案》《可信终端动态运行环境的可信证据收集机制》《直接匿名证言协议的性能估算新方法》《一种优化的直接匿名证言协议方案》等；在可信平台模块虚拟化方面，包括《TPM虚拟化及其进展》《虚拟平台上一种新的证书信任扩展方法》《虚拟平台环境中一种新的vTPM迁移方法》《一种基于影子页表+的软件型vTPM密钥保护方案》《云环境中可信虚拟平台的远程证明方案研究》等，以上选题都具有创新感。对解决可信计算平台证明及TPM虚拟化问题具有较大的研究意义。

(2)分析全面，发现问题准确。谭良教授在对可信计算平台证明及TPM虚拟化的研究过程中，分析全面，发现问题准确。例如，在可信计算平台证明方面，他在综述论文《TCG架构下的证明问题研究及进展》中就全面分析了TCG架构下的证明研究进展，总结出了三方面的问题。①对于平台身份证明，直接匿名证明(direct anonymous attestation，DAA)方案采用基于零知识证明的群签名技术，每次证明(包括DAA证书的颁发和验证)至少需要运行3次零知识证明协议，在实现上复杂度仍然较大，不仅效率低，性能差，只支持单信任域，而且群签名技术不够完善，隐私泄露问题仍然存在。因此，一个满足基本要求而简单、高效、易于实现的平台身份证明实用算法是最为重要的关键问题之一。②对于平台配置证明，二进制证明方法不仅暴露了本地平台(包括硬件和软件)的配置信息，而且不能解决平台系统更新和备份问题。尽管基于属性的证明方法是一种更加有效且灵活的远程证明解决方案，但仍然复杂性高、难以实现。基于自动信任协商的远程证明方法属性证书和环签名方案代替平台配置信息有效防止隐私泄露，满足了系统升级和备份过程的可信检测要求。但在实现该证明方案时，仍然需要TPM宿主的参与辅助，安全隐患仍然存在。因此，一个满足基本要求而又简单、高效、易于实现的平台配置证明算法是解决问题的关键。③对于平台动态环境状态(运行时环境状态)证明，待解决的问题包括应用程序的完整性度量框架、收集平台运行环境中的关键信息建立信任模型，以及如何收集、收集什么、采用什么方式建立信任模型等。

(3)方法得当，富有启发。谭良教授在解决可信计算平台证明及TPM虚拟化的问题时，研究方法得当，取得了一定的学术成果，对未来的研究具有一定的启发。例如，在可信计算平台证明方法的性能估算方面，谭良教授在分析已有研究成果的基础之上，提出了以机器周期为基本性能单位的性能负荷分布测量方法——归一化统计法(normalized statistics，NS)，该定量方法需要首先分析DAA协议中的各种复

杂运算，针对不同的运算选用当前性能较好的算法，然后统计各个算法中大整数单精度乘法、单精度加法、读内存、写内存等基本运算的数目，最后通过汇总并转换得出 DAA 协议中各实体以机器周期为单位的性能负荷分布和总性能负荷。比较分析表明，该方法不仅能相对准确、精细、有效地定量计算出 DAA 协议中各实体的性能负荷和总的性能负荷，而且测出的性能负荷具有平台无关性。又如，在 TPM 虚拟化方面，针对云环境中如何证明虚拟平台的可信问题，就 TCG 发布的*Virtualized Trusted Platform Architecture Specification* 中可信虚拟平台的远程证明方案仅仅是个框架，并没有具体实施方案，谭良教授提出了一种自顶向下的可信虚拟平台远程证明实施方案——TVP-PCA，该方案是在虚拟机中设置一个认证代理，在虚拟机管理器中新增一个认证服务，挑战方首先通过顶层的认证代理证明虚拟机环境可信，然后通过底层的认证服务证明运行于物理平台上的虚拟机管理器可信，顶层和底层证明合起来确保了整个虚拟平台的可信，有效地解决了顶层证明和底层证明的同一性问题。

总之，在学校平台、科研环境等条件限制下，谭良教授总结自己的科研成果并写成本书，我由衷地感到高兴。在此向谭良教授表示祝贺，并预祝他在今后的研究中再创佳绩。

可信计算领域值得研究的问题还很多，我希望今后能有更多的学者投入这一领域的研究，相信可信计算的明天一定会更加灿烂辉煌。

周明天

2017 年 12 月 5 日

前　言

可信计算技术的基本思想是以可信平台模块(trusted platform module，TPM)为信任根建立计算平台的信任，并以密码技术为用户提供计算平台系统资源完整、数据安全存储和平台远程证明等功能。可信计算平台的证明问题是可信计算的基本问题之一。尤其是近年来，云计算这一新兴的计算服务方式，以其宽带互连、资源池共享、弹性配置、按需服务和按量收费等独特优势，在各行各业应用中快速兴起。用户通过将计算任务和数据委托给云服务商，大大减轻了用户计算和存储的负担。但值得注意的是，云计算提供给用户的运行环境是以虚拟机作为载体的，用户的运行环境和数据都存放在云端，从而失去了对物理环境的直接控制，如何为用户提供安全的云计算服务是亟待解决的问题。国内外可信计算方面的学者敏捷地意识到可以通过可信计算来增强云计算环境的可信性，其中通过 TPM 虚拟化来构建虚拟机可信环境是解决此问题的有效方法之一。

1. 本书的研究内容

本书研究内容包括两个方面。其一是可信平台模块的虚拟化及证明，主要分为以下四点：①虚拟环境下信任链的传递；②虚拟环境下证书信任扩展；③虚拟环境下虚拟 TPM 的密钥保护；④虚拟环境下可信虚拟终端的远程证明方案。其二是终端可信计算平台的证明，主要分为三点：①平台身份证明，平台身份证明是用于向远程验证方证明可信计算平台的身份，是建立平台间信任的基础；②平台配置证明，平台配置证明是用于向远程验证方证明可信计算平台的软件配置结构，即经过度量的应用程序；③平台动态环境状态(运行时环境状态)证明。

2. 本书的结构

第一部分为可信平台模块虚拟化，包括可信平台模块及其虚拟化产生的背景、研究现状、信任链及密钥相关问题。

第 1 章介绍可信平台模块虚拟化研究及进展。本书认为，云计算与可信计算相结合是构建可信云环境的重要方法，其最为关键的问题是对 TPM 的虚拟化。但就当前的研究成果来看，TPM 虚拟化不仅存在部分不符合 TCG 规范的现象，而且存在诸多安全问题，正成为云计算和可信计算融合构建可信云环境的瓶颈。本章介绍 TPM 虚拟化的基本概念、类型和基本要求，提出 TPM 虚拟化的技术分类模型，详细阐述 TPM 虚拟化的系统架构、密钥管理、证书信任扩展以及迁移等关

键技术的主要研究工作进展，并以时间为线索展现相关关键技术演进的全景视图。最后结合已有的研究成果，探讨 TCG 架构下 TPM 虚拟化的研究方向及其面临的挑战。

第 2 章介绍具有瀑布特征的可信虚拟平台信任链模型。本书认为，目前大部分研究成果采用了在虚拟平台上扩展传统信任链的构建方法，模型过粗且逻辑不完全合理，同时存在底层虚拟化平台和顶层用户虚拟机两条分离的信任链问题。为此，本章提出一种具有瀑布特征的信任链模型——TVP-QT，该模型以硬件 TPM 为起点，在底层虚拟化平台和顶层用户虚拟机信任链之间加入可信衔接点。当信任链从底层虚拟化平台传递到可信衔接点时，由可信衔接点负责对用户虚拟机的 vTPM 进行度量，之后将控制权交给 vTPM，由 vTPM 负责对用户虚拟机启动的组件及应用进行度量。该模型中可信衔接点具有承上启下的瀑布特征，能满足虚拟化环境的层次性和动态性特征，保证了整个可信虚拟平台的可信性。不仅从理论上证明了该模型的正确性，而且对实例系统的分析和讨论也表明了该模型的通用性与可行性，并在 Xen 中对该模型进行了仿真实验，实验结果表明，本信任链传递理论可以保证可信虚拟化环境在整个运行过程中是安全可信的。

第 3 章介绍虚拟平台环境中一种新的可信证书链扩展方法。本书认为，利用可信计算技术构建可信虚拟平台环境时，如何合理地将底层物理 TPM 的证书信任扩展延伸到虚拟机环境是值得关注的问题。目前已有的证书信任扩展方案均不完善，要么存在违背 TCG 规范的情况，要么增加了密钥冗余和 Privacy CA 性能负担，有的方案甚至不能进行证书信任扩展。为此，本章提出一种新的可信证书链扩展方法。首先，在 TPM 中新增一类证书——VMEK(virtual machine extension key)，并构建对 VMEK 的管理机制，该证书的主要特点是其密钥不可迁移，且可对 TPM 内和外的数据进行签名和加密；其次，利用证书 VMEK 对 vTPM 的 vEK 签名来构建底层 TPM 和虚拟机 vTPM 的证书信任关系，实现可信证书链在虚拟机中的延伸；最后，在 Xen 中实现 VMEK 证书及其管理机制和基于 VMEK 的证书信任扩展，测试结果表明，本方案可以有效地实现虚拟平台的远程证明功能。

第 4 章介绍基于影子页表+的软件型 vTPM 密钥保护方案。本书认为，由于 TPM 是一块资源受限的硬件芯片，在可信虚拟平台上所有用户虚拟机都通过共享方式来实现可信计算的功能是不现实的。因此，当前不少虚拟平台在对 TPM 虚拟化时采用软件仿真方式。而现有虚拟机环境中的许多恶意攻击均能窃取和破坏此类 vTPM 运行时的密钥秘密信息，特别是在全虚拟化和硬件虚拟化平台环境中，整个虚拟机均处于 VMM 的用户空间中，vTPM 的密钥秘密信息更容易遭到攻击，这将严重影响虚拟机和 vTPM 的安全。为此，本章提出一种基于影子页表+的软件型 vTPM 密钥秘密信息保护方案，该方案主要是在全虚拟化或硬件虚拟化平台中通过新增影子页表管理模块 MMU-vTPM 来保护 vTPM 的密钥秘密信息，该管理模块通过对 vTPM

密钥私有内存页表的访问控制来阻止其他进程访问和破坏 vTPM 密钥秘密信息私有内存。而且为了防止恶意用户对 MMU-vTPM 模块进行篡改，采用 TPM 的静态度量机制和动态度量机制对该模块进行完整性保护。最后，基于 Xen 实现该方案，测试结果表明，该方案能够保证 vTPM 的 vEK 和 vSRK 等关键密钥秘密信息的安全性，而且不会带来严重的性能损失。

第 5 章介绍云环境中可信虚拟平台的远程证明方案研究。本书认为，在云环境中如何证明虚拟平台的可信是一个值得研究的问题。由于云环境中虚拟平台包括运行于物理平台上的虚拟机管理器和虚拟机，它们是不同的逻辑运行实体，具有层次性和动态性，现有的可信终端远程证明方案，包括隐私 CA(privacy certification authority，PCA)方案和直接匿名证明(direct anonymous attestation，DAA)方案，都并不能直接用于可信虚拟平台。而 TCG 发布的*Virtualized Trusted Platform Architecture Specification*中可信虚拟平台的远程证明方案仅仅是个框架，并没有具体实施方案。为此，本章提出一种自顶向下的可信虚拟平台远程证明实施方案——TVP-PCA，该方案是在虚拟机中设置一个认证代理，在虚拟机管理器中新增一个认证服务，挑战方首先通过顶层的认证代理证明虚拟机环境可信，然后通过底层的认证服务证明运行于物理平台上的虚拟机管理器可信，顶层和底层证明合起来确保了整个虚拟平台的可信，有效解决了顶层证明和底层证明的同一性问题。实验表明，本方案不仅能证明虚拟机的可信，而且能证明虚拟机管理器和物理平台的可信，因而证明了云环境中的虚拟平台是真正可信的。

第二部分为虚拟域(终端)的可信证明，主要介绍 TCG 架构下平台身份证明、终端远程证明、证据收割及匿名证明等相关研究。

第 6 章介绍 TCG 架构下的证明问题研究及进展。本书认为 TCG 架构下的证明问题解决方案由于可扩展性差、不够灵活、容易泄露平台隐私以及性能低，正在成为可信计算应用、推广和普及的瓶颈，严重地阻碍了可信计算在更广的范围内延伸和拓展。本章介绍证明的基本概念并给出形式化定义，详细阐述三元和四元证明系统的基本架构及工作机制，并指出平台身份证明采用了“推”式四元证明系统，而平台配置证明仍然采用三元证明系统。分析当前对 TCG 架构下的平台身份证明、平台环境状态配置信息证明以及平台动态环境状态(运行时环境状态)证明等三方面开展的研究工作，并对这些工作进行总结。结合已有的研究成果，探讨 TCG 架构下的证明问题的研究方向及其面临的挑战。

第 7 章介绍一种新的可信终端运行环境远程证明方案。本书针对可信终端的远程证明无论基于二进制的证明方案还是基于属性的证明方案并不能证明终端运行环境的真正可信这一问题，提出一种终端可信环境远程证明方案。针对静态环境，该方案考虑了满足可信平台规范的信任链以及相关软件配置的可信属性证明；针对动态环境，该方案考虑了终端行为的可信属性证明，并分别给出信任链、平台软件配

置和终端行为等属性证明的可信性判定策略和算法，以及终端运行环境远程证明的综合性判定策略和算法。

第 8 章介绍可信终端动态运行环境的可信证据收集机制。可信计算的链式度量机制不容易扩展到终端所有应用程序，可信终端要始终保证其动态运行环境的可信仍然困难，为了提供可信终端动态运行环境客观、真实、全面的可信证据，本书提出可信终端动态运行环境的可信证据收集机制。首先，在可信终端的应用层引入一个可信证据收集代理，并将该代理作为可信平台模块链式度量机制的重要一环，利用 TPM 提供的度量功能保证该代理可信；然后，通过该代理收集可信终端的内存、CPU、网络端口、磁盘文件、策略配置数据和进程等的运行时状态信息，并利用 TPM 提供的可信存储功能，保存这些状态信息作为终端运行环境的可信证据，保障可信证据本身的可信性。该可信证据收集机制具有良好的可扩展性，为支持面向不同应用的信任评估模型提供基础。

第 9 章介绍可信终端动态运行环境的可信证据收集代理。为了收集可信终端动态运行环境的可信证据，本书设计并实现了一个基于可信平台模块的终端动态运行环境可信证据收集代理。该代理的主要功能是收集可信终端内存、进程、磁盘文件、网络端口、策略数据等关键对象的状态信息和操作信息。首先，通过扩展 TPM 信任传递过程及其度量功能保证该代理的静态可信，利用可信虚拟机监视器(trusted virtual machine monitor，TVMM)提供的隔离技术保证该代理动态可信；然后，利用 TPM 的加密和签名功能保证收集的证据的来源和传输可信；最后，在 Windows 平台上实现了一个可信证据收集代理原型，并以一个开放的局域网为实验环境来分析可信证据收集代理所获取的终端动态运行环境可信证据以及可信证据收集代理在该应用实例中的性能开销。该应用实例验证了该方案的可行性。

第 10 章介绍直接匿名证言协议的性能估算新方法。性能问题是阻碍 DAA 推广和应用的首要问题。为了进一步优化该协议的性能，找出性能瓶颈，定量分析和测量 DAA 中各个实体的性能负荷分布是一项十分重要且必需的工作。本章详细分析 DAA 的协议流程，提出以机器周期为基本性能单位的性能负荷分布测量方法——归一化统计法。该方法需要首先分析 DAA 协议中的各种复杂运算，针对不同的运算选用当前性能较好的算法，然后统计各个算法中大整数单精度乘法、单精度加法、读内存、写内存等基本运算的数目，最后通过汇总并转换得出 DAA 协议中各实体以机器周期为单位的性能负荷分布和总性能负荷。比较分析表明，该方法不仅能相对准确、精细、有效地定量计算出 DAA 协议中各实体的性能负荷和总的性能负荷，而且测出的性能负荷具有平台无关性。最后为了说明该方法的有效性，将归一化统计法应用于有关可信计算匿名证明的一个典型方案的性能负荷估算。

第 11 章介绍一种优化的直接匿名证言协议方案。DAA 既解决了 PCA 的瓶颈问题，又实现了对 TPM 芯片的认证和匿名，是当前可信计算平台身份证明最好的理

论解决方案之一。但是该协议基于强 RSA 困难假设，实现过程中不仅涉及多个实体，而且涉及大量的耗时运算。突出的性能问题制约了该协议的广泛应用。本书基于普通椭圆曲线离散对数的困难性假设，提出一种较为优化的直接匿名证明方案 TMZ-DAA。该方案仅依赖普通椭圆曲线离散对数的困难性假设，涉及的主要运算是椭圆曲线的点加和标量乘，复杂性大大降低，不仅密钥长度和签名长度较短，而且在总性能方面得到较大提高，减小了 Join 协议、Sign 协议以及 Verify 算法中 TPM、Host、Issuer 以及 Verifier 等各个参与实体的计算量，为基于椭圆曲线的 TPM 提供了可行的隐私性保护解决方案。利用理想系统/现实系统模型对该方案的安全性进行分析和证明，结果表明，该方案满足不可伪造性、可变匿名性和不可关联性。

3. 研究的目的和意义

本书研究的目的主要体现在如下两方面。

(1) 对可信计算平台中证明(attestation)问题的研究具有极其重要的意义。第一，可信基于证明，只有证明才能在不可信的环境中建立信任关系。第二，在 TCG 框架下，对平台身份的证明算法不够完善，离实际应用还有一定的距离。第三，在 TCG 框架下，对平台环境配置状态的证明还存在诸多不合理之处。例如，为了证明平台环境配置信息，TCG 规范中采用二进制证明(binary attestation)。第四，在 TCG 规范中，目前还没有涉及平台动态环境(运行时环境)的证明，而平台动态环境的可信是平台建立可信计算环境的根本要求。平台身份证明只解决平台的身份可信问题，平台配置状态证明只解决平台中的静态环境可信问题，而平台动态环境的可信问题并没有得到解决。所以，解决可信计算平台中的证明问题可以促进可信计算的应用、推广和普及。

(2) 对 TPM 虚拟化问题的研究具有重要的意义。第一，在云的虚拟化环境中 TPM 虚拟化为客户虚拟机环境提供了可信保障。TPM 虚拟化使得每个客户虚拟机在逻辑上都能拥有单个“独有”的 TPM(简称 vTPM)，就像拥有一个真实的物理 TPM 一样。客户虚拟机环境可以使用虚拟 TPM 提供的数据保护、远程证明以及完整性校验、存储和报告等功能。特别是可通过虚拟 TPM 的完整性校验功能实现客户虚拟机环境的信任链传递，通过虚拟 TPM 的数据保护功能实现客户虚拟机环境数据的密封存储，以及通过虚拟 TPM 的远程证明功能实现客户虚拟机环境的身份证明。第二，在 vTPM 体系结构中，vTPM 通过 VMM 与 TPM 和客户虚拟机绑定时，安全和效率始终是一个难以解决的两难问题。第三，在 TPM 虚拟化中，从云硬件层中的 TPM 到客户虚拟机环境的信任链传递模型和理论均不完善。建立从底层物理硬件到客户虚拟机环境完整的可信链是将可信计算融入云计算的核心，只有建立了从底层物理硬件到客户虚拟机环境完整的可信链，这样的客户虚拟机环境为云租户提供的各级服务才有了可信的基础。第四，在 TPM 虚拟化中，vTPM 在实现迁移机制

方面还存在诸多问题，特别是如何实现异构虚拟监控器平台上的迁移机制是一个公认的开问题(open problem)。vTPM 与 TPM 并不完全相同，而且 vTPM 所处的环境和 TPM 所处的环境也不完全一样，因此，原样将 TPM 远程证明已有的研究成果移植到 vTPM 是不可行的。所以，解决 TPM 虚拟化问题是将可信计算和云计算融合的关键，有力地推动云计算的广泛应用。

我们诚挚希望书中的研究成果能够促进可信计算在可信计算平台证明和可信平台模块虚拟化等方面的发展，推动可信计算在更广的范围内应用、推广和延拓，特别是在云计算中的广泛应用。但由于作者水平有限，书中不足之处在所难免，敬请广大读者批评指正。

4. 致谢

本书能够顺利出版，得益于国家自然科学基金面上项目(编号：60970113，61373162)的资助和科学出版社的支持。另外，在本书修改的过程中，得到了宋敏、舒红梅同学的大力帮助，在此表示衷心的感谢。

谭　良

2017 年 12 月

目　录

第二部分　虚拟域(终端)的可信证明