



(12) 发明专利

(10) 授权公告号 CN 101493870 B

(45) 授权公告日 2010. 10. 27

(21) 申请号 200810236866. 7

(56) 对比文件

(22) 申请日 2008. 12. 17

WO 2007127018 A1, 2007. 11. 08, 全文.

(73) 专利权人 武汉大学

US 20080046898 A1, 2008. 02. 21, 全文.

地址 430072 湖北省武汉市武昌区八一路
299 号

审查员 苏珊娜

(72) 发明人 张焕国 严飞 徐士伟 傅建明
李小菲 汤梅 向爽

(74) 专利代理机构 湖北武汉永嘉专利代理有限
公司 42102

代理人 王守仁

(51) Int. Cl.

G06F 21/00 (2006. 01)

G06F 11/36 (2006. 01)

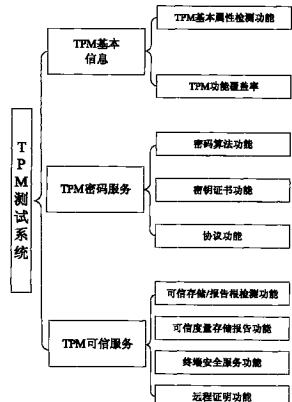
权利要求书 3 页 说明书 11 页 附图 8 页

(54) 发明名称

可信平台模块测试方法

(57) 摘要

本发明提供了一种可信平台模块测试装置，包括：基本信息测试系统，用于测试不同可信平台模块的基本信息，所述可信平台模块的基本信息包括基本属性检测功能和功能覆盖率；密码服务测试系统，用于测试可信平台模块作为安全芯片的基本密码功能，所述基本密码功能包括密码算法功能、密钥证书功能和协议功能；可信服务测试系统，用于测试可信平台模块的可信特征，所述可信特征包括可信存储 / 报告根检测功能，可信度量存储报告功能，终端安全服务功能，以及远程证明功能；上述各测试系统安装在可信计算系统上，所述可信计算系统内装有作为硬件芯片的可信平台模块。使用该装置能对 TPM 进行规范符合性测试，可以高效覆盖待测试 TPM 的可信功能。



1. 可信平台模块测试方法,其特征在于 :

其通过可信平台模块实现,可信平台模块包括 :

基本信息测试系统,用于测试不同可信平台模块的基本信息,所述可信平台模块的基本信息包括基本属性检测功能和功能覆盖率;

密码服务测试系统,用于测试可信平台模块作为安全芯片的基本密码功能,所述基本密码功能包括密码算法功能、密钥证书功能和协议功能;

可信服务测试系统,用于测试可信平台模块的可信特征,所述可信特征包括可信存贮 / 报告根检测功能,可信度量存储报告功能,终端安全服务功能,以及远程证明功能;

上述各测试系统安装在可信计算系统上,所述可信计算系统内装有作为硬件芯片的可信平台模块;

所述基本属性检测功能的测试方法,是通过获取所述可信平台模块基本属性的操作,检测可信平台模块的基本属性返回值,所述返回值包括:可信平台模块的版本信息和厂商信息;可信平台模块支持哪些命令、算法和协议;可信平台模块能够支持的平台配置寄存器的数量、能够提供的最大会话数;以及固定标志位 pFlags 和可变标志位 vFlags;

所述功能覆盖率的测试方法包括 :

301) 对同一功能代入不同错误参数,根据返回不同的错误代码,获知所述可信平台模块对同一功能的处理流程;

302) 根据所述处理流程,对可信平台模块的每个功能进行覆盖验证,即:输入包含正确参数的功能测试命令,以及输入包含错误参数的功能测试命令;若前者的返回值为正确代码,且后者的返回值为错误代码,则该功能被覆盖,否则不被覆盖;

303) 统计可信平台模块所有功能的覆盖情况,得出功能覆盖率;

所述密码算法功能的测试方法是 :

对所述可信平台模块的加解密算法、签名算法、随机数生成算法、散列函数进行测试,同时提供可选的性能测试;对于没有提供标准测试接口的功能,采用可信平台模块开发厂家提供的开发硬件进行二次开发;其步骤包括 :

401) 向可信平台模块发送相关密码算法命令及原始数据;

402) 接受可信平台模块返回的计算值;

403) 根据 401) 的算法命令及原始数据和 402) 的计算值判断可信平台模块是否符合规范要求;

所述密钥证书功能的测试方法包括 :

501) 向可信平台模块发送生成密钥指令,根据其返回的操作结果判断是否能完成创建密钥的功能,若为“是”,则进入下一步,否则停止测试;

502) 向可信平台模块发送装载密钥指令,根据其返回的操作结果判断是否能完成装载密钥的功能,若为“是”,则进入下一步,否则停止测试;

503) 向可信平台模块发送使用密钥指令,根据其返回的操作结果及密钥属性判断是否能完成使用密钥的功能;若为“是”,则密钥证书功能符合规范,否则不符合规范;

所述协议功能的测试方法包括 :

601) 向可信平台模块建立授权会话,根据其返回结果判断是否能够获取授权信息,若为“是”,则进入下一步,否则停止测试;

602) 根据正确的授权信息,向可信平台模块发送操作敏感数据命令,判断其是否返回操作成功的信息;

603) 根据错误的授权信息,向可信平台模块发送操作敏感数据命令,判断其是否返回操作失败的信息。

604) 验证 602) 和 603) 返回的信息是否符合规范;

所述可信存储 / 报告根检测功能的测试方法包括:

701) 验证可信平台模块上的可信存储 / 报告根是否存在,若存在则销毁可信存储 / 报告根,然后进入下一步;否则直接进入下一步;

702) 创建可信存储 / 报告根,记录可信平台模块的返回值;

703) 读取可信平台模块上的可信存储 / 报告根,记录其返回值;

704) 验证步骤 702) 和 703) 的返回值是否符合规范;

所述可信度量存储报告功能的测试方法包括:

801) 向可信平台模块注入度量值;

802) 向可信平台模块发出计算度量值的指令;

803) 记录可信平台模块返回的计算后的度量值;

804) 验证 803) 计算后度量值是否满足规范;

805) 向可信平台模块发出读取指定平台配置寄存器的指令;

806) 将度量值写入指定的平台配置寄存器;

807) 向可信平台模块发出读取指定平台配置寄存器内容的指令;

808) 记录可信平台模块返回的指定平台配置寄存器的内容;

809) 计算 808) 的返回值,并与规范相比较;

所述终端安全服务功能的测试方法包括:

901) 将原始数据,通过可信平台模块进行平台无关加密;

902) 将 901) 加密后的数据,通过可信平台模块进行平台无关解密;

903) 若解密成功,记录可信平台模块返回的平台无关解密数据;若解密不成功则停止测试过程;

904) 将原始数据,通过可信平台模块进行平台相关加密;

905) 将平台配置信息设置成与 904) 相符的状态,然后对 904) 的加密数据进行平台相关解密;

906) 若解密成功,记录可信平台模块返回的平台相关解密数据;若解密不成功,则停止测试过程;

907) 将原始数据,通过可信平台配置模块进行平台相关加密;

908) 将平台配置信息设置成与 907) 不符的状态,然后对 907) 的加密数据进行平台相关解密;

909) 记录可信平台模块返回的解密状态信息,其应该为不成功,否则不符合规范;

910) 将 903) 的平台无关解密数据和 906) 的平台相关解密数据,与 901) 的原始数据进行比较;若比较结果一致,则终端安全服务功能符合规范,否则不符合规范;

所述远程证明功能测试方法包括:

1001) 向可信平台模块发出读取相关事件信息的指令;

- 1002) 向可信平台模块发出读取指定平台配置寄存器签名的指令；
- 1003) 向可信平台模块发出读取指定平台配置寄存器内容的指令；
- 1004) 分别记录 1001)、1002)、1003) 返回的相关事件、指定平台配置寄存器的签名、指定平台配置寄存器的内容；
- 1005) 根据 1004) 获得的相关事件和指定平台配置寄存器的内容，计算指定平台配置寄存器的签名，并与 1004) 获得的指定平台配置寄存器的签名相比较。

可信平台模块测试方法

技术领域

[0001] 本发明涉及计算机信息安全技术领域,特别是涉及一种基于功能划分的可信平台模块 (TPM) 测试装置,用于对不同厂商不同版本的 TPM 进行测试。

背景技术

[0002] 可信计算组织 (TCG, Trusted Computing Group) 是由来自工业和学术的组件提供商、软件开发商、系统开发商、网络与体系公司组成的大型组织,它致力于研究和开发能够适用于多平台的、公开的工业规范。

[0003] TCG 已经发布了多个应用领域的数个文档与规范,其中最主要的规范是 TPM(TrustedPlatform Module) 规范。关于 TPM 的规范有两个版本,分别为 1.1b 和 1.2。

[0004] 版本 1.1b 可参考 :

[0005] [1]TCPA Main Specification, Version 1.1b,

[0006] https://www.trustedcomputinggroup.org/specs/TPM/TCPA_Main_TCG_Architecture_v1_1b.pdf, February 2002。

[0007] 版本 1.2 可参考 :

[0008] [2]Trusted Computing Group (TCG), TPM Main Specification-Part 1 : DesignPrinciples,

[0009] https://www.trustedcomputinggroup.org/specs/TPM/Main_Part1_Rev94.zip, March2006 ;

[0010] [3]Trusted Computing Group (TCG), TPM Main Specification-Part 2 : TPMStructures,

[0011] https://www.trustedcomputinggroup.org/specs/TPM/Main_Part2_Rev94.zip, March2006 ;

[0012] [4]Trusted Computing Group (TCG), TPM Main Specification-Part 3 : Commands,

[0013] https://www.trustedcomputinggroup.org/specs/TPM/Main_Part3_Rev94.zip, March2006。

[0014] 上述规范对 TPM 的设计原理、体系结构、数据结构、功能、命令和基本参数都进行了说明和规定。

[0015] TPM 主要由与密码相关的功能组件和一些存储区域组成,是一个含有密码运算部件和存储部件的小型片上系统 (SOC)。它是计算平台中的集成专用硬件模块,利用密码机制建立信任链,构建可信赖的计算环境,是可信计算平台的信任根源。

[0016] 近来,国内市场上已经出现越来越多装配有 TPM 的机器。鉴于以上两个规范的复杂性,以及对市场上的 TPM 产品的调研结果得知,并不是所有厂商生产的 TPM 芯片均是能够符合规范的。事实上,在规范定义与产品实现之间,很多厂商为了市场的需要,并考虑到成本和实际使用,研制出来的 TPM 产品和规范之间是存在很多差异的。虽然许多厂商声称他

们生产的 TPM 芯片是符合 TCG 规范的,但事实上,对于使用者来说,他们没有一个行之有效的方法对该说法进行验证,也就无法得知产品的真实性和有效性。并且,国内对于 TPM 的测试还是一项空白,尚没有任何公司、高校或研究所提出了对 TPM 进行有效测试的方法。

[0017] 综上所述,研究出一种能够测试不同型号 TPM 的方法,以便能够方便地对 TPM 进行规范符合性测试就显得非常必要了。

发明内容

[0018] 本发明所要解决的技术问题是:提供一种可信平台模块测试方法,使用该方法能对 TPM 进行规范符合性测试,可以高效覆盖待测试 TPM 的可信功能。

[0019] 本发明所采用的技术方案是:可信平台模块测试方法通过可信平台模块实现,可信平台模块包括:

[0020] 基本信息测试系统,用于测试不同可信平台模块的基本信息,所述可信平台模块的基本信息包括基本属性检测功能和功能覆盖率;

[0021] 密码服务测试系统,用于测试可信平台模块作为安全芯片的基本密码功能,所述基本密码功能包括密码算法功能、密钥证书功能和协议功能;

[0022] 可信服务测试系统,用于测试可信平台模块的可信特征,所述可信特征包括可信存贮/报告根检测功能,可信度量存储报告功能,终端安全服务功能,以及远程证明功能;

[0023] 上述各测试系统安装在可信计算系统上,所述可信计算系统内装有作为硬件芯片的可信平台模块;

[0024] 所述基本属性检测功能的测试方法,是通过获取所述可信平台模块基本属性的操作,检测可信平台模块的基本属性返回值,所述返回值包括:可信平台模块的版本信息和厂商信息;可信平台模块支持哪些命令、算法和协议;可信平台模块能够支持的平台配置寄存器的数量、能够提供的最大会话数;以及固定标志位 pFlags 和可变标志位 vFlags;

[0025] 所述功能覆盖率的测试方法包括:

[0026] 301) 对同一功能代入不同错误参数,根据返回不同的错误代码,获知所述可信平台模块对同一功能的处理流程;

[0027] 302) 根据所述处理流程,对可信平台模块的每个功能进行覆盖验证,即:输入包含正确参数的功能测试命令,以及输入包含错误参数的功能测试命令;若前者的返回值为正确代码,且后者的返回值为错误代码,则该功能被覆盖,否则不被覆盖;

[0028] 303) 统计可信平台模块所有功能的覆盖情况,得出功能覆盖率;

[0029] 所述密码算法功能的测试方法是:

[0030] 对所述可信平台模块的加解密算法、签名算法、随机数生成算法、散列函数进行测试,同时提供可选的性能测试;对于没有提供标准测试接口的功能,采用可信平台模块开发厂家提供的开发硬件进行二次开发;其步骤包括:

[0031] 401) 向可信平台模块发送相关密码算法命令及原始数据;

[0032] 402) 接受可信平台模块返回的计算值;

[0033] 403) 根据 401) 的算法命令及原始数据和 402) 的计算值判断可信平台模块是否符合规范要求;

[0034] 所述密钥证书功能的测试方法包括:

- [0035] 501) 向可信平台模块发送生成密钥指令,根据其返回的操作结果判断是否能完成创建密钥的功能,若为“是”,则进入下一步,否则停止测试;
- [0036] 502) 向可信平台模块发送装载密钥指令,根据其返回的操作结果判断是否能完成装载密钥的功能,若为“是”,则进入下一步,否则停止测试;
- [0037] 503) 向可信平台模块发送使用密钥指令,根据其返回的操作结果及密钥属性判断是否能完成使用密钥的功能;若为“是”,则密钥证书功能符合规范,否则不符合规范;
- [0038] 所述协议功能的测试方法包括:
- [0039] 601) 向可信平台模块建立授权会话,根据其返回结果判断是否能够获取授权信息,若为“是”,则进入下一步,否则停止测试;
- [0040] 602) 根据正确的授权信息,向可信平台模块发送操作敏感数据命令,判断其是否返回操作成功的信息;
- [0041] 603) 根据错误的授权信息,向可信平台模块发送操作敏感数据命令,判断其是否返回操作失败的信息。
- [0042] 604) 验证 602) 和 603) 返回的信息是否符合规范;
- [0043] 所述可信存储 / 报告根检测功能的测试方法包括:
- [0044] 701) 验证可信平台模块上的可信存储 / 报告根是否存在,若存在则销毁可信存储 / 报告根,然后进入下一步;否则直接进入下一步;
- [0045] 702) 创建可信存储 / 报告根,记录可信平台模块的返回值;
- [0046] 703) 读取可信平台模块上的可信存储 / 报告根,记录其返回值;
- [0047] 704) 验证步骤 702) 和 703) 的返回值是否符合规范;
- [0048] 所述可信度量存储报告功能的测试方法包括:
- [0049] 801) 向可信平台模块注入度量值;
- [0050] 802) 向可信平台模块发出计算度量值的指令;
- [0051] 803) 记录可信平台模块返回的计算后的度量值;
- [0052] 804) 验证 803) 计算后度量值是否满足规范;
- [0053] 805) 向可信平台模块发出读取指定平台配置寄存器的指令;
- [0054] 806) 将度量值写入指定的平台配置寄存器;
- [0055] 807) 向可信平台模块发出读取指定平台配置寄存器内容的指令;
- [0056] 808) 记录可信平台模块返回的指定平台配置寄存器的内容;
- [0057] 809) 计算 808) 的返回值,并与规范相比较;
- [0058] 所述终端安全服务功能的测试方法包括:
- [0059] 901) 将原始数据,通过可信平台模块进行平台无关加密;
- [0060] 902) 将 901) 加密后的数据,通过可信平台模块进行平台无关解密;
- [0061] 903) 若解密成功,记录可信平台模块返回的平台无关解密数据;若解密不成功则停止测试过程;
- [0062] 904) 将原始数据,通过可信平台模块进行平台相关加密;
- [0063] 905) 将平台配置信息设置成与 904) 相符的状态,然后对 904) 的加密数据进行平台相关解密;
- [0064] 906) 若解密成功,记录可信平台模块返回的平台相关解密数据;若解密不成功,

则停止测试过程；

[0065] 907) 将原始数据,通过可信平台配置模块进行平台相关加密；

[0066] 908) 将平台配置信息设置成与 907) 不符的状态,然后对 907) 的加密数据进行平台相关解密；

[0067] 909) 记录可信平台模块返回的解密状态信息,其应该为不成功,否则不符合规范；

[0068] 910) 将 903) 的平台无关解密数据和 906) 的平台相关解密数据,与 901) 的原始数据进行比较;若比较结果一致,则终端安全服务功能符合规范,否则不符合规范；

[0069] 所述远程证明功能测试方法包括：

[0070] 1001) 向可信平台模块发出读取相关事件信息的指令；

[0071] 1002) 向可信平台模块发出读取指定平台配置寄存器签名的指令；

[0072] 1003) 向可信平台模块发出读取指定平台配置寄存器内容的指令；

[0073] 1004) 分别记录 1001)、1002)、1003) 返回的相关事件、指定平台配置寄存器的签名、指定平台配置寄存器的内容；

[0074] 1005) 根据 1004) 获得的相关事件和指定平台配置寄存器的内容,计算指定平台配置寄存器的签名,并与 1004) 获得的指定平台配置寄存器的签名相比较。

[0075] 本发明提供的方法是国内首次设计并实现 TPM 测试系统,具有以下优点：

[0076] 第一,对规范进行了分析与总结,得到了 TPM 最小功能集和 TPM 功能划分,从而得到了具体的 TPM 功能依赖关系,使得能够高效覆盖待测试 TPM 功能。

[0077] 第二,根据上述分析与总结的结果,设计并实现了基于功能划分的 TPM 测试系统,有效解决了 TPM 规范符合性测试问题。

附图说明

[0078] 图 1 :TPM 测试系统功能划分。

[0079] 图 2 :TPM 最小功能集。

[0080] 图 3 :基于功能划分的 TPM 测试系统结构示意图。

[0081] 图 4 :TPM 基本属性检测功能的测试方法。

[0082] 图 5 :TPM 功能覆盖率测试方法。

[0083] 图 6 :TPM 密钥证书功能测试方法。

[0084] 图 7 :TPM 协议功能测试方法。

[0085] 图 8 :可信存储 / 报告根检测功能的测试方法。

[0086] 图 9 :可信度量存储报告的测试方法。

[0087] 图 10 :终端安全服务功能的测试方法。

[0088] 图 11 :远程证明功能的测试方法。

[0089] 图 12 :TPM 密码算法功能测试方法。

具体实施方式

[0090] 由于目前的可信计算平台模块 TPM 规范主要以体系结构和技术性描述为主,其中所描述的功能存在密不可分的关系,功能之间彼此依赖,有些功能必须基于其它功能的基

础上才能够运行。因此,对 TPM 测试,首先需要对 TPM 规范中的可信功能进行抽取、划分与总结。

[0091] 本发明通过对 TPM 规范进行抽取,得到了 TPM 的功能划分。同时分析得到了 TPM 最小功能集,被划分的 TPM 功能都可以映射到 TPM 最小功能集的不同层次上,从而得到具体的功能依赖关系,并基于此设计了测试系统对 TPM 进行测试,使得能够高效覆盖待测试 TPM 功能,对 TPM 进行规范符合性测试。

[0092] 具体而言,本发明的思路是:

[0093] 1. 抽取 TPM 功能划分:

[0094] 根据对 TPM 规范进行分析、归纳与总结,可知 TPM 在向平台所提供密码算法、密钥管理、授权协议等功能的同时,还为平台本身的完整性、数据安全性提供了密码功能支持。因此,如图 1 所示,将 TPM 功能测试划分为三个部分:

[0095] ①基本信息

[0096] 本部分主要是测试不同厂家生产的 TPM 的基本信息,让用户对被测试的 TPM 有基本了解。

[0097] ②密码服务

[0098] 本部分主要测试 TPM 作为安全芯片的基本密码功能,是可信服务测试的基础。测试内容包括密码算法、密钥使用以及协议。

[0099] ③可信服务

[0100] 本部分用于测试 TPM 的可信特征,体现了 TPM 作为平台信任根,对平台完整性的保障和对用户数据秘密性的保护机制。

[0101] 2. 提炼 TPM 最小功能集

[0102] 同时,根据进一步对规范的分析,归纳与总结,得到 TPM 最小功能集,这个最小功能集包含了 TPM 最基本的功能。如图 2 所示,TPM 内部的随机数产生功能 (TPM_GetRandom、TPM_StirRandom) 和哈希功能 (TPM_SHA1Start、TPM_SHA1Update、TPM_SHA1Complete、TPM_SHA1CompleteExtend) 是最底层功能,所有其它都依赖于它们的正确实现;协议功能 (TPM_OSAP 和 TPM_OIAP) 相关功能是保证 TPM 内部密钥使用真实性与完整性的手段,处于次底层的位置,其依赖哈希功能和随机数产生功能;PCR(平台配置寄存器)读写功能 (TPM_Extend、TPM_PCRRead) 依赖哈希功能和随机数产生功能;TPM 的安全存储功能是利用一种树形密钥结构实现的,其树的根节点是永远贮存在 TPM 中存储根密钥 (Storage RootKey, SRK),而获取 TPM 所有权 (TPM_TakeOwnership(I)) 功能能够产生 SRK,所有密钥相关操作都依赖于它,其依赖协议功能和读取基本属性功能 (TPM_GetCapability);产生密钥功能 (TPM_CreateWrapKey(s)) 功能和装载密钥 (TPM_LoadKey) 功能是利用 TPM 产生普通密钥的重要功能,保证了 TPM 所有密码相关功能,产生密钥功能依赖获取 TPM 所有权功能,装载密钥功能依赖产生密钥功能;清除 TPM 所有权功能 (TPM_OwnerClear(I)) 依赖获取 TPM 所有权功能;最后签名功能 (TPM_Sign(S) 和 TPM_Quote(S))、封装与解封功能 (TPM_Seal(s) 和 TPM_Unseal(S))、解除绑定功能 (TPM_UnBind(I))、卸载密钥功能 (TPM_EvictKey) 等相关功能是出于最高层次的应用,它们的正常运行依赖于之前所有功能的正确实现。上述功能表达式中 S 表示使用了 TPM_OSAP 协议, I 表示使用了 TPM_OIAP 协议。

[0103] 3. 将 TPM 的功能划分分别映射到 TPM 最小功能集的不同层次上

[0104] TPM 最小功能集涵盖了对 TPM 所有功能划分的测试, 被划分的 TPM 功能可以分别映射到最小功能集的不同层次, 结合图 1 和图 2 :

[0105] 基本信息功能是最基本的功能, 其依赖层次最低, 在最小功能集中包括 : 读取基本属性功能 ;

[0106] 密码服务包含密码算法功能、密钥证书功能、协议功能等功能, 其依赖层次居中, 为 TPM 可信服务提供基础, 在最小功能集中包括 : 哈希功能、随机数产功能、协议功能、获取 TPM 所有权功能、清除 TPM 所有权功能、产生密钥功能和装载密钥功能 ;

[0107] 可信服务, 在最小功能集中其依赖层次最高, 它为平台提供完整性的保障, 同时为用户提供数据秘密性的保护机制, 在最小功能集中包括 : PCR 读写功能、签名功能、封装与解封功能、解除绑定功能和卸载密钥功能。

[0108] 如图 1 所示, 以上 TPM 功能三大部分的划分又可进行更细致的划分。基本信息又分为 : 基本属性检测功能和功能覆盖率两个方面 ; 密码服务又分为 : 密码算法功能、密钥证书功能和协议功能三个方面 ; 可信服务又可分为 : 可信存储 / 报告根检测功能、可信度量存储报告功能、终端安全服务功能和远程证明功能的测试。

[0109] 因此, 可信平台模块测试装置包括 :

[0110] 基本信息测试系统, 用于测试不同可信平台模块的基本信息, 所述可信平台模块的基本信息包括基本属性检测功能和功能覆盖率 ;

[0111] 密码服务测试系统, 用于测试可信平台模块作为安全芯片的基本密码功能, 所述基本密码功能包括密码算法功能、密钥证书功能和协议功能 ;

[0112] 可信服务测试系统, 用于测试可信平台模块的可信特征, 所述可信特征包括可信存贮 / 报告根检测功能, 可信度量存储报告功能, 终端安全服务功能, 以及远程证明功能 ;

[0113] 上述各测试系统安装在可信计算系统上, 所述可信计算系统内装有作为硬件芯片的可信平台模块。

[0114] 基于以上分析, 将 TPM 功能可具体划分为九类 :

[0115] 1. 基本属性检测功能, 即获取 TPM 基本属性。

[0116] 2. 功能覆盖率, 即厂商提供的 TPM 对规范中所规定功能的覆盖程度。

[0117] 3. 密码算法功能, 用于检测算法实现是否符合国家或行业相应算法标准。本模块将主要提供正确性测试, 同时提供可选的性能测试。

[0118] 4. 密钥证书功能, 主要测试密钥属性是否正确以及证书是否存在并且符合规范。

[0119] 5. 协议功能, 主要测试 TPM 能否建立符合规范的认证会话。

[0120] 6. 可信存储 / 报告根检测功能, 主要测试可信存储根 (RTS) 和可信报告根 (RTR) 是否存在, 并且是否符合可信计算平台模块 TPM 规范中所定义的表现形式。

[0121] 7. 可信度量存储与报告功能, 主要测试完整性度量报告测试流程。

[0122] 8. 终端安全服务功能, 主要测试基于 TPM 的加解密功能。

[0123] 9. 远程证明功能, 主要测试 TPM 能否向远程的验证者提供指定 PCR 的签名, 为平台的真实性提供保障。

[0124] 检测者对各部分的 TPM 功能的测试具体实施方案如下 :

[0125] 一、基本信息检测, 即 TPM 硬件检测

[0126] 1. 基本属性检测功能的评测

[0127] 1.1 功能与原理

[0128] TPM 的基本属性值应该包括 :TPM 版本信息和厂商信息 ;TPM 支持哪些命令、算法和协议 ;TPM 能够支持 PCR 的数量、能够提供的最大会话数等内置参数 ; 以及 TPM 的一些内部数据, 如 : 固定标志位 pFlags 和可变标志位 vFlags 等。

[0129] 1.2 测试方法与目标

[0130] 通过获取所述 TPM 属性的操作, 检测 TPM 的基本属性返回值。基本属性不应该包括一些敏感信息, 这些敏感信息属于非基本属性, 如 :TPM 密钥的公私钥、可信存储根和可信报告根等。通过获得基本属性的操作无法获得这些敏感信息, 这些敏感信息的获得需要通过专门的操作和特定的授权。其测试方法如图 4 所示。

[0131] 2. 功能覆盖率检测

[0132] 2.1 功能与原理

[0133] 本部分测试的主要是测试 TPM 所提供的功能对 TPM 规范中所规定功能的覆盖程度。

[0134] 向 TPM 发送不同功能的命令, 无论带正确的还是错误的参数, TPM 都应该对应地返回一些值, 通过将返回值与规范中所规定的相比较, 得出 TPM 的功能是否齐全。

[0135] 2.2 测试方法与目标

[0136] 对同一功能代入不同错误参数, 根据返回不同的错误代码, 可以大概获知 TPM 对同一功能的处理流程。在大概获知功能的处理流程之后, 更有助于对功能覆盖率进行测试。其测试方法如图 5 所示, 包括 :

[0137] 301) 对同一功能代入不同错误参数, 根据返回不同的错误代码, 获知所述可信平台模块对同一功能的处理流程 ;

[0138] 302) 根据所述处理流程, 对可信平台模块的每个功能进行覆盖验证, 即 : 输入包含正确参数的功能测试命令, 以及输入包含错误参数的功能测试命令 ; 若前者的返回值为正确代码, 且后者的返回值为错误代码, 则该功能被覆盖, 否则不被覆盖 ;

[0139] 303) 统计可信平台模块所有功能的覆盖情况, 得出功能覆盖率。

[0140] 二、密码服务检测

[0141] 3. 密码算法功能测试

[0142] 3.1 功能与原理

[0143] 密码协处理器是可信计算平台模块 TPM 的重要组成部分, 负责实现 TPM 内部密码学操作, 所采用的密码算法实现都必须符合国家或行业相应算法标准。

[0144] 3.2 测试方法与目标

[0145] 本部分将进行标准 TPM 芯片的加解密算法, 签名算法, 随机数生成算法, 散列函数的正确性测试, 同时提供可选的性能测试。对于没有提供标准测试接口的功能采用 TPM 开发厂家提供的开发硬件进行二次开发。如图 12 所示, 具体包括 :

[0146] 401) 向可信平台模块发送相关密码算法命令及原始数据 ;

[0147] 402) 接受可信平台模块返回的计算值 ;

[0148] 403) 根据 401) 的算法命令及原始数据和 402) 的计算值判断可信平台模块是否符合规范要求。

[0149] 4. 密钥及证书功能测试

[0150] 4.1 功能与原理

[0151] TPM 必须有能够在内部生成不对称密钥对的功能。本方案 8 主要采用如图 6 所示的测试系统进行测试。TPM 还应具有表明自身身份的证书，本方案将基于厂商具体的实现技术规范对其进行测试 3002

[0152] 4.2 测试方法与目标

[0153] 本部分主要测试的是：密钥是否能够被创建、密钥是否能够被装载、所创建的密钥它的属性是否正确以及是否生成了密钥对应的使用授权信息、证书是否存在，是否符合相应规范要求。其测试方法如图 6 所示，包括：

[0154] 501) 向可信平台模块发送生成密钥指令，根据其返回的操作结果判断是否能完成创建密钥的功能，若为“是”，则进入下一步，否则停止测试；

[0155] 502) 向可信平台模块发送装载密钥指令，根据其返回的操作结果判断是否能完成装载密钥的功能，若为“是”，则进入下一步，否则停止测试；

[0156] 503) 向可信平台模块发送使用密钥指令，根据其返回的操作结果及密钥属性判断是否能完成使用密钥的功能；若为“是”，则密钥证书功能符合规范，否则不符合规范。

[0157] 5. 协议功能检测

[0158] 5.1 功能与原理

[0159] 授权协议是 TPM 外部实体与 TPM 之间的访问协议，实现了外部实体与 TPM 之间的授权认证、信息的完整性验证和敏感数据的机密保护。

[0160] 可信计算平台内的密钥、敏感数据及其它需要存储保护的数据必须具有相应的授权数据，并且只能通过对相应授权数据进行验证才能访问。不允许任意存取的 TPM 数据都拥有一个授权数据—共享秘密。这个共享秘密包含在 TPM 数据的内部。

[0161] 5.2 测试方法与目标

[0162] 本部分主要测试能否建立认证会话并获得授权信息、能否通过正确的授权信息获取所需数据以及能否验证出不正确的授权信息等。是否提供一定的机制对重放攻击的抵御。其方法如图 7 所示，包括：

[0163] 601) 向可信平台模块建立授权会话，根据其返回结果判断是否能够获取授权信息，若为“是”，则进入下一步，否则停止测试；

[0164] 602) 根据正确的授权信息，向可信平台模块发送操作敏感数据命令，判断其是否返回操作成功的信息；

[0165] 603) 根据错误的授权信息，向可信平台模块发送操作敏感数据命令，判断其是否返回操作失败的信息。

[0166] 604) 验证 602) 和 603) 返回的信息是否符合规范。

[0167] 值得注意的是，TPM 对字典攻击并没有很好的防范机制，TPM 应对未成功的授权尝试进行计数，以避免攻击者对同一授权进行无数次的伪造授权尝试。

[0168] 三、可信服务测试

[0169] 6. 可信存储 / 报告根检测功能的评测

[0170] 6.1 功能与原理

[0171] 本部分主要测试可信存储根 (RTS) 和可信报告根 (RTR) 是否存在，并且是否符合 TPM 规范中所定义的表现形式。

[0172] 根据 TPM 规范规定, RTR 在 TPM 中就是背书密钥 EK。而 RTS 对外部存储器件中的 TPM 所需要使用的数据进行保护,在 TPM 芯片中,SRK 充当起了 RTS 的责任。于是,对 RTR 和 RTS 的测试也就转换成了对 EK 和 SRK 的测试。

[0173] 6.2 测试方法与目标

[0174] 此处应验证 EK 和 SRK 是否存在,然后比对 EK 和 SRK 的表现形式是否与 TPM 规范相对应,可以通过读取 EK 和 SRK,根据其属性,比对规范,确定其表现形式是否与规范相对应。其测试方法如图 8 所示,包括:

[0175] 701) 验证可信平台模块上的可信存储 / 报告根是否存在,若存在则销毁可信存储 / 报告根,然后进入下一步;否则直接进入下一步;

[0176] 702) 创建可信存储 / 报告根,记录可信平台模块的返回值;

[0177] 703) 读取可信平台模块上的可信存储 / 报告根,记录其返回值;

[0178] 704) 验证步骤 702) 和 703) 的返回值是否符合规范。

[0179] 7. 可信度量存储报告功能测试

[0180] 7.1 功能与原理

[0181] 可信度量的存储与报告实际上是完整性度量值的报告与存储。

[0182] 7.2 测试方法与目标

[0183] 本部分主要测试计算度量值的算法的种类与正确性;度量值是否记入指定 PCR 和平台是否能够向验证者提供指定的 PCR 值;度量信息是否记录到日志中和平台是否可向验证者提供指定 PCR 的相关事件日志信息。对度量值的算法一般使用的 SHA-1 算法,对其正确性进行测试,并且进行验证;测试度量值是否记录并验证;测试平台是否可以读写指定 PCR 的相关事件日志信息。其测试方法如图 9 所示,包括:

[0184] 801) 向可信平台模块注入度量值;

[0185] 802) 向可信平台模块发出计算度量值的指令;

[0186] 803) 记录可信平台模块返回的计算后的度量值;

[0187] 804) 验证 803) 计算后度量值是否满足规范;

[0188] 805) 向可信平台模块发出读取指定平台配置寄存器的指令;

[0189] 806) 将度量值写入指定的平台配置寄存器;

[0190] 807) 向可信平台模块发出读取指定平台配置寄存器内容的指令;

[0191] 808) 记录可信平台模块返回的指定平台配置寄存器的内容;

[0192] 809) 计算 808) 的返回值,并与规范相比较。

[0193] 8. 终端安全服务功能测试

[0194] 8.1 功能与原理

[0195] TPM 终端安全服务测试主要分为平台相关加解密测试和平台无关加解密测试。

[0196] 8.2 测试方法与目标

[0197] 平台无关加解密测试的是在把原始数据进行加密以后,再解密以后,能够还原成原始数据。平台相关加解密主要测试的是在把原始数据进行加密以后,再解密以后,能够还原成原始数据外,还应该测试解密时平台设置是否达到了解密的要求。其测试方法如图 10 所示,包括:

[0198] 901) 将原始数据,通过可信平台模块进行平台无关加密;

- [0199] 902) 将 901) 加密后的数据,通过可信平台模块进行平台无关解密 ;
- [0200] 903) 若解密成功,记录可信平台模块返回的平台无关解密数据;若解密不成功则停止测试过程 ;
- [0201] 904) 将原始数据,通过可信平台模块进行平台相关加密 ;
- [0202] 905) 将平台配置信息设置成与 904) 相符的状态,然后对 904) 的加密数据进行平台相关解密 ;
- [0203] 906) 若解密成功,记录可信平台模块返回的平台相关解密数据;若解密不成功,则停止测试过程 ;
- [0204] 907) 将原始数据,通过可信平台配置模块进行平台相关加密 ;
- [0205] 908) 将平台配置信息设置成与 907) 不符的状态,然后对 907) 的加密数据进行平台相关解密 ;
- [0206] 909) 记录可信平台模块返回的解密状态信息,其应该为不成功,否则不符合规范 ;
- [0207] 910) 将 903) 的平台无关解密数据和 906) 的平台相关解密数据,与 901) 的原始数据进行比较;若比较结果一致,则终端安全服务功能符合规范,否则不符合规范。
- [0208] 9. 远程证明服务功能的测试
- [0209] 9.1 功能与原理
- [0210] 向远程的验证者提供指定 PCR 的签名,为平台的真实性提供保障。
- [0211] 9.2 测试方法与目标
- [0212] 要求能验证指定 PCR 签名。其测试方法如图 11 所示。
- [0213] 1001) 向可信平台模块发出读取相关事件信息的指令 ;
- [0214] 1002) 向可信平台模块发出读取指定平台配置寄存器签名的指令 ;
- [0215] 1003) 向可信平台模块发出读取指定平台配置寄存器内容的指令 ;
- [0216] 1004) 分别记录 1001)、1002)、1003) 返回的相关事件、指定平台配置寄存器的签名、指定平台配置寄存器的内容 ;
- [0217] 1005) 根据 1004) 获得的相关事件和指定平台配置寄存器的内容,计算指定平台配置寄存器的签名,并与 1004) 获得的指定平台配置寄存器的签名相比较。
- [0218] 基于以上 TPM 测试实施方案,根据通过 TPM 最小功能集所得到的 TPM 功能的依赖关系,对 TPM 相应功能(命令)按照 1 ~ 9 的先后顺序进行测试。首先对 TPM 基本信息进行检测;其次对 TPM 密码服务相关功能进行检测;最后对 TPM 可信服务相关功能进行检测。
- [0219] 具体实现中,依据上述功能划分和最小功能集,可以得到 TPM 功能之间的依赖关系。依据得到的 TPM 功能之间的依赖关系,同时考虑到 TPM 接口 API(应用程序接口)的特殊性,即其所有输入参数都是以字节流的形式顺序连接起来发送给 TPM 的。这样就可对 TPM 测试系统进行了如图 3 的设计 :
- [0220] Java 前台接收由用户传入的测试需求(即功能调用),生成测试用例和测试流程,其中测试用例存储在数据库中。Java 部分实现与上层界面和数据库进行交互的功能;同时根据测试中功能(命令)之间的依赖关系,调用通用模块,通用模块实现了:从数据库中读取各条命令的参数值、构造与解析数据包、分析返回数据包内容和将分析结果存入数据库等功能。

[0221] Java 通过使用 JNI 技术, 调用 native 方法, 将组装好的命令(功能), 即将组合好的数据包按照依赖关系顺序发送给 C 部分, 实现与 C 交互。

[0222] C 部分主要实现与 TPM 进行交互的功能。C 后台从 Java 端接收数据包, 调用 TPM 驱动程序直接将数据包转发给 TPM ;接收 TPM 返回的数据包, 并将数据包回送给 Java 部分。

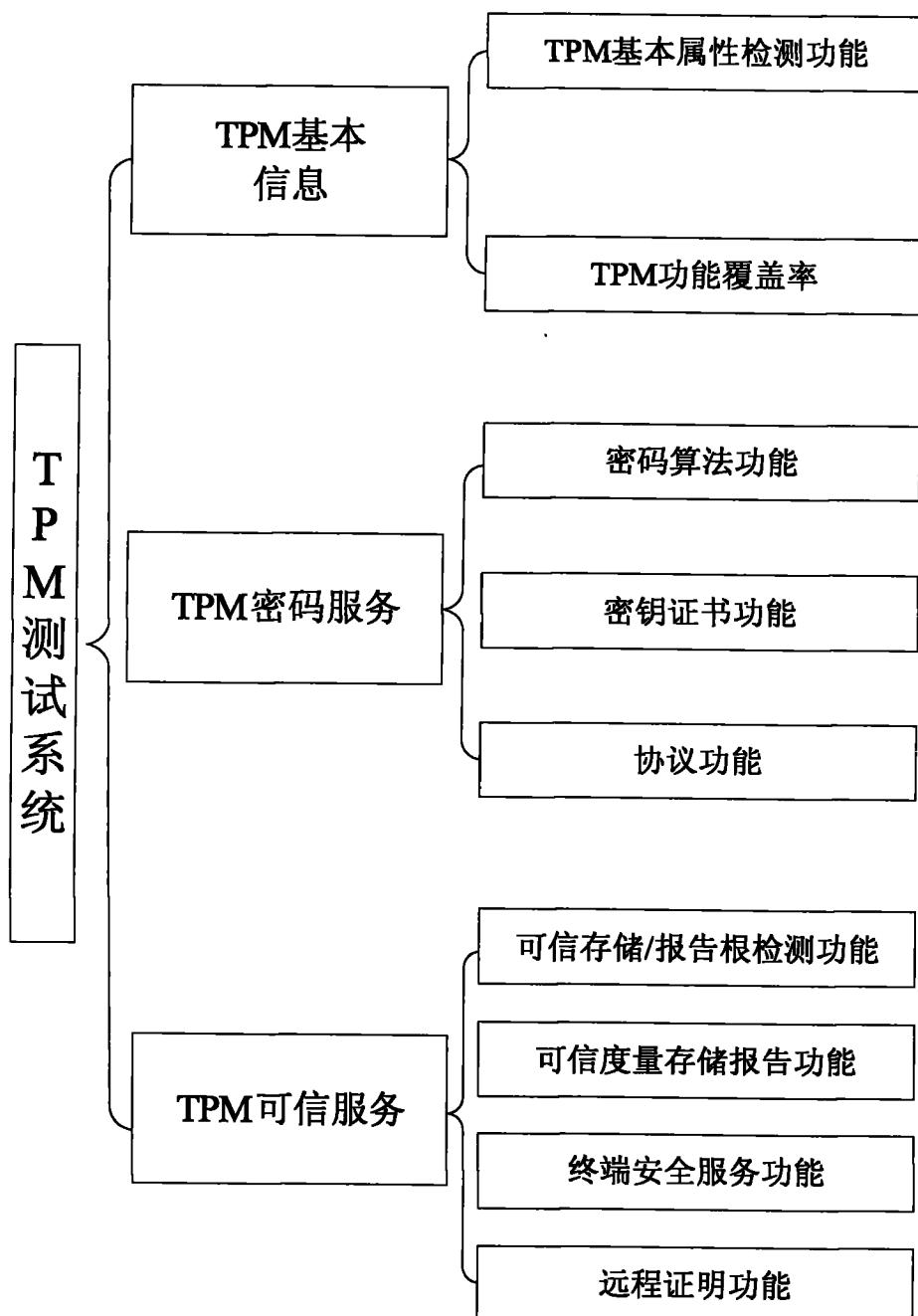


图 1

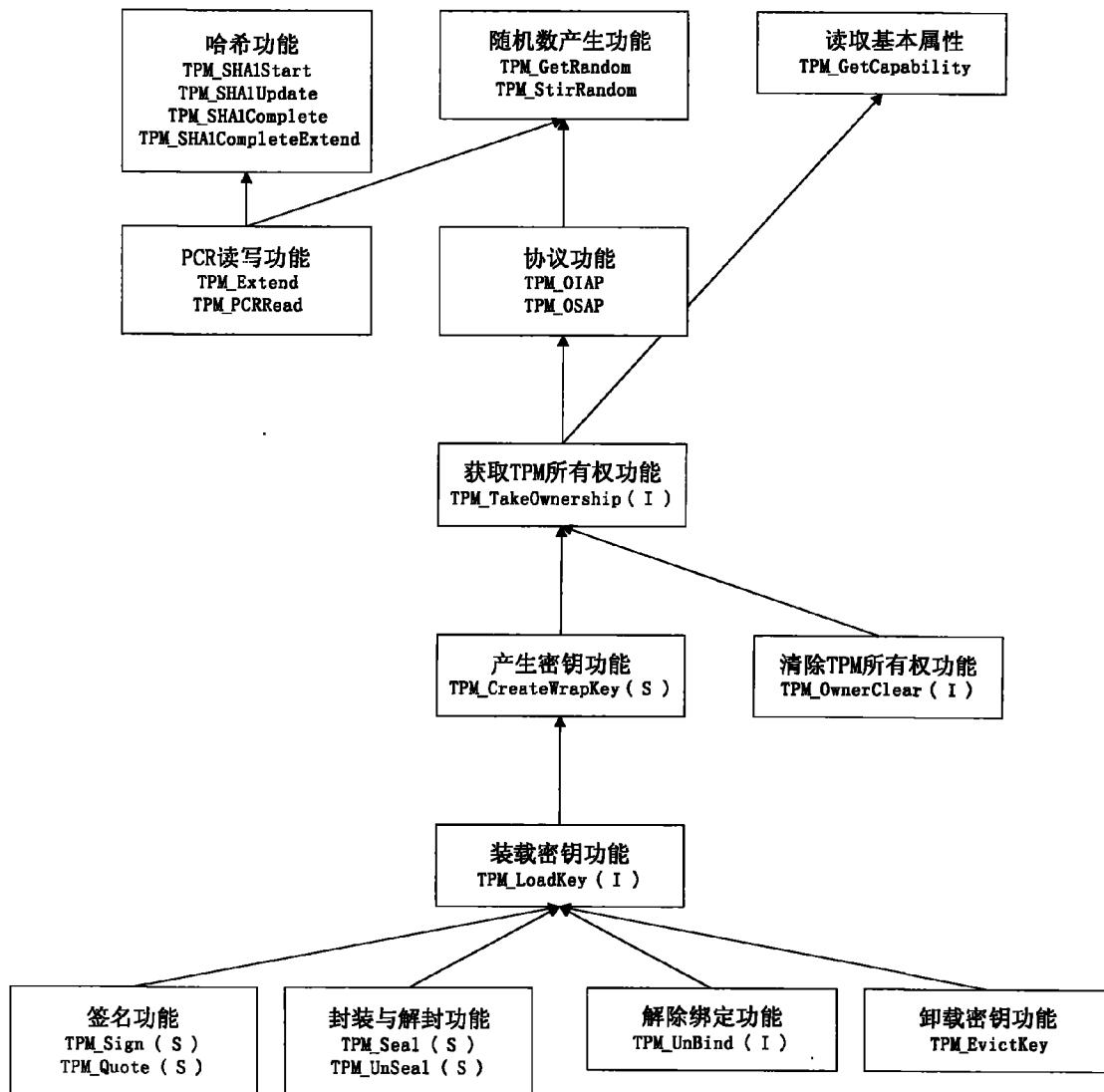


图 2

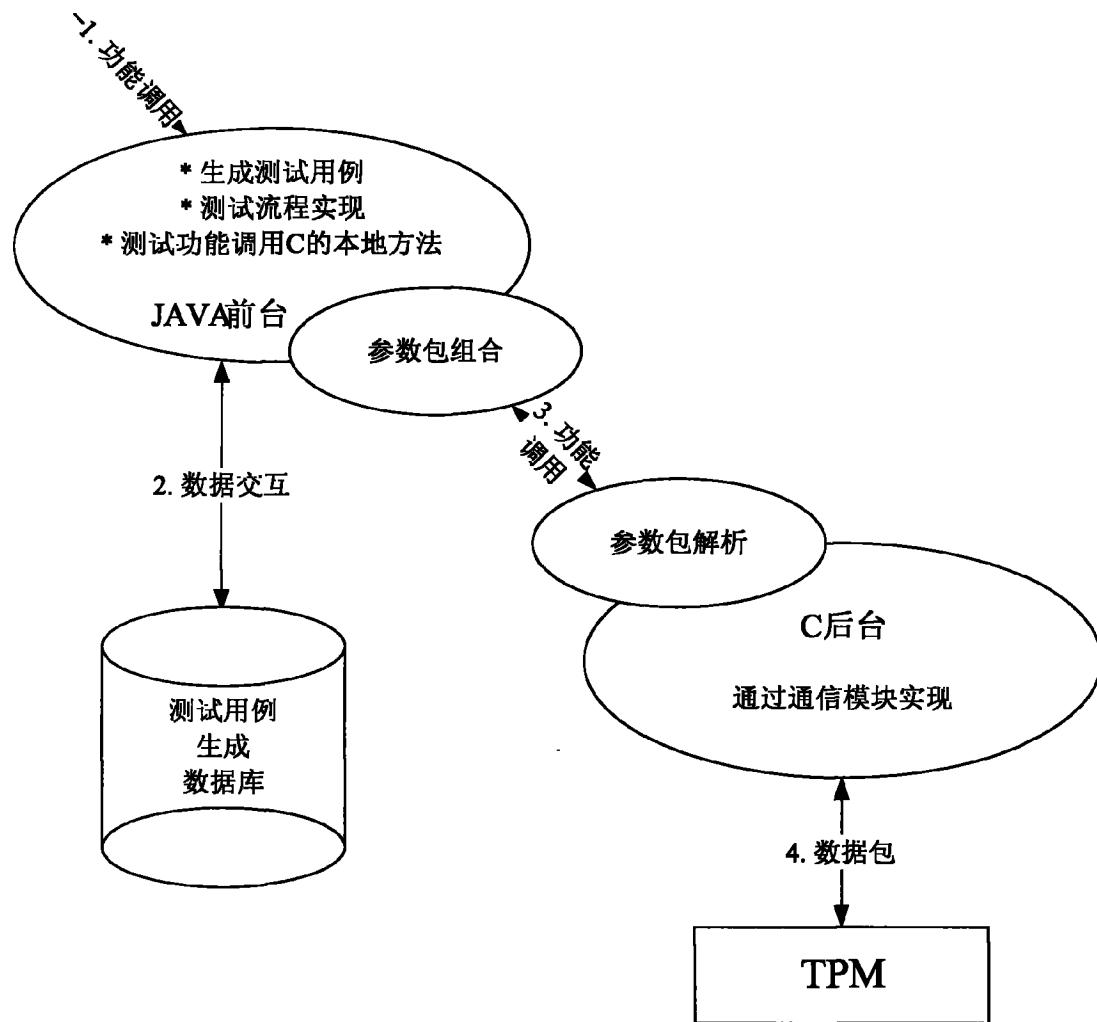


图 3

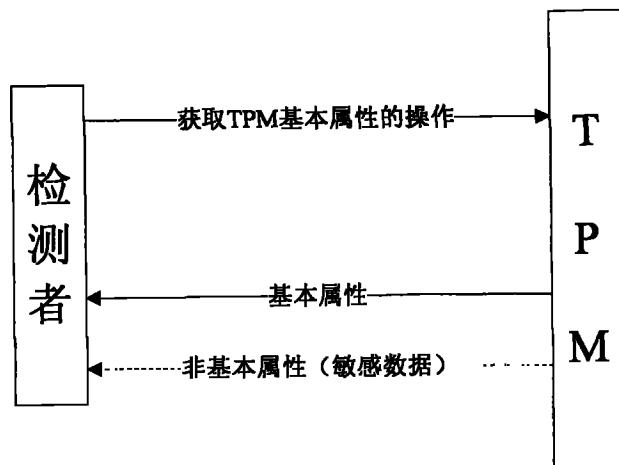


图 4

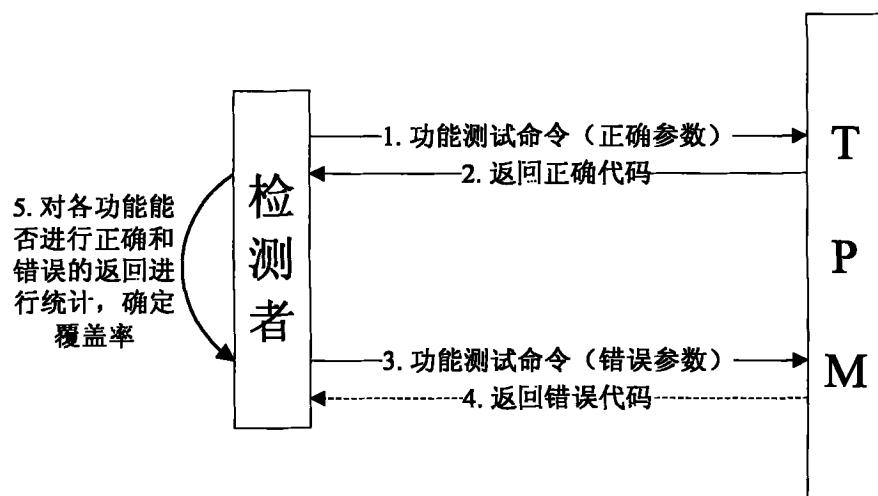


图 5

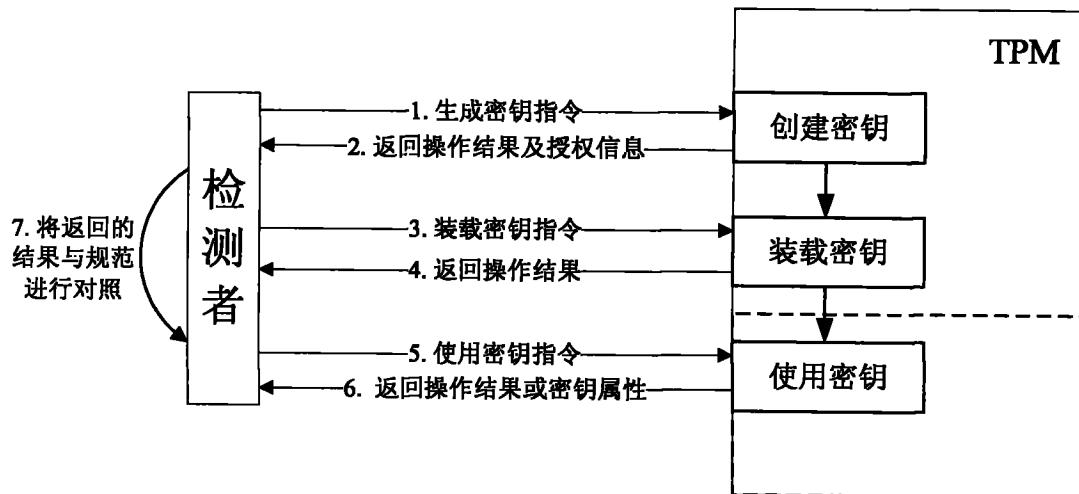


图 6

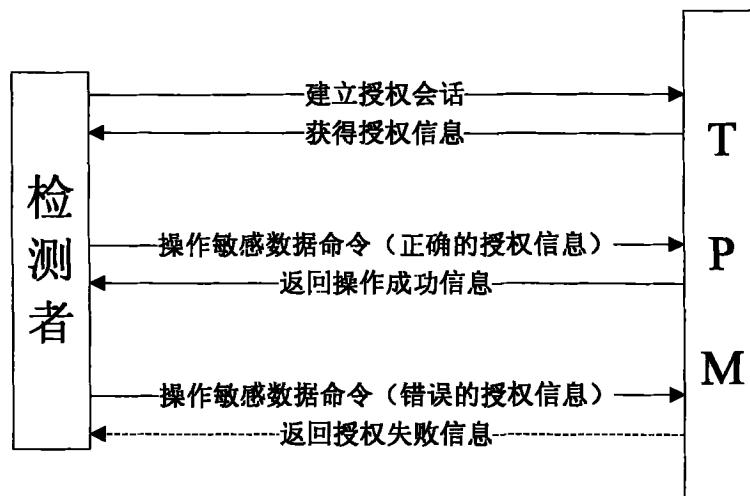


图 7

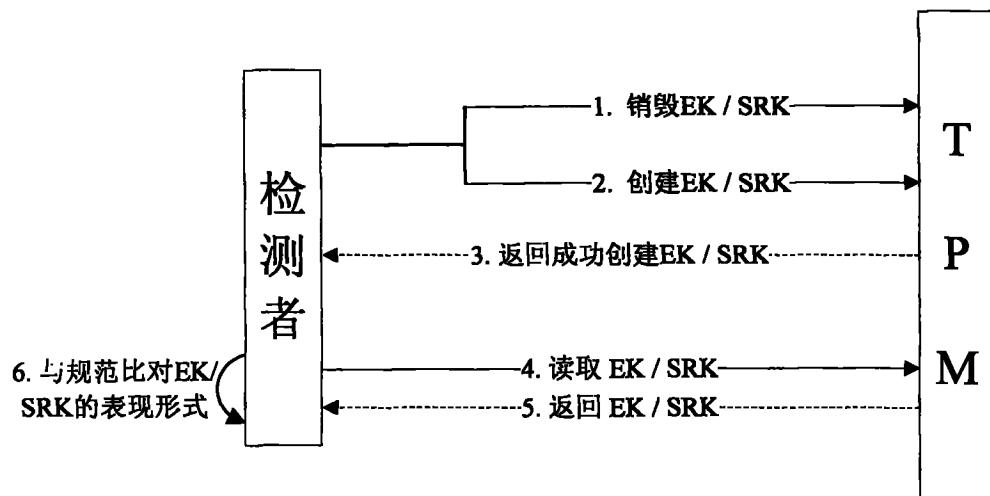


图 8

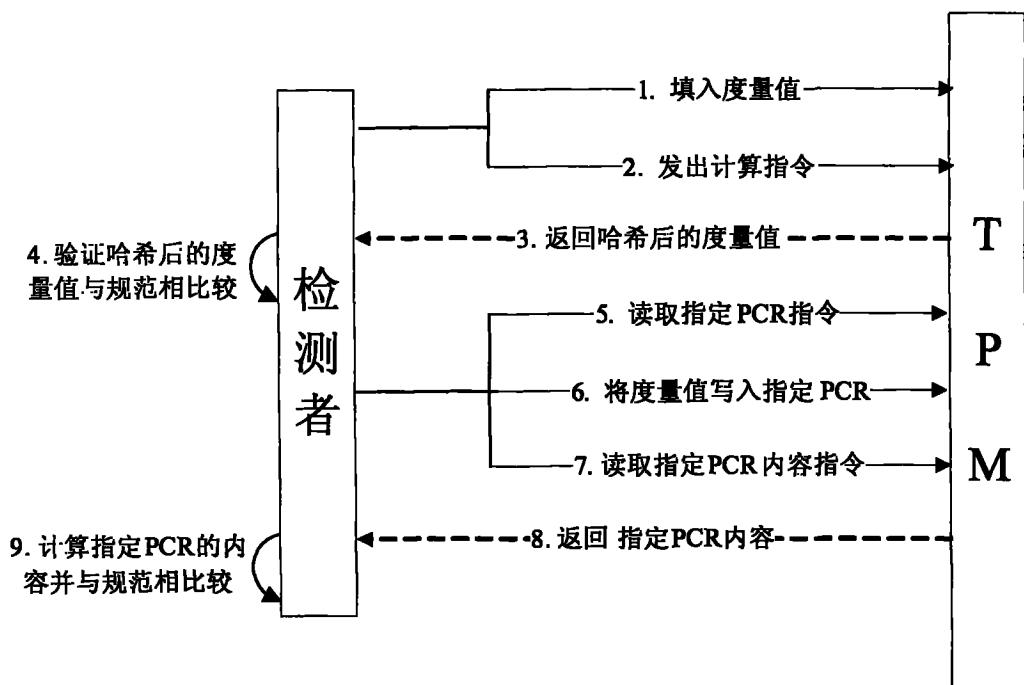


图 9

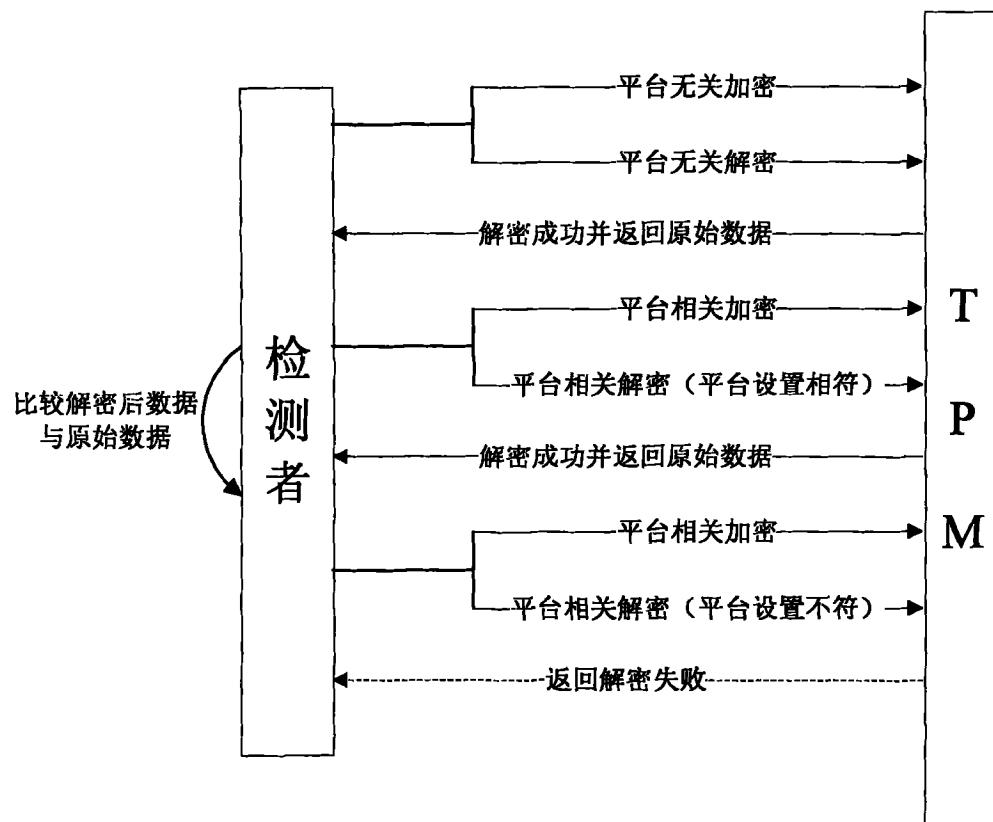


图 10

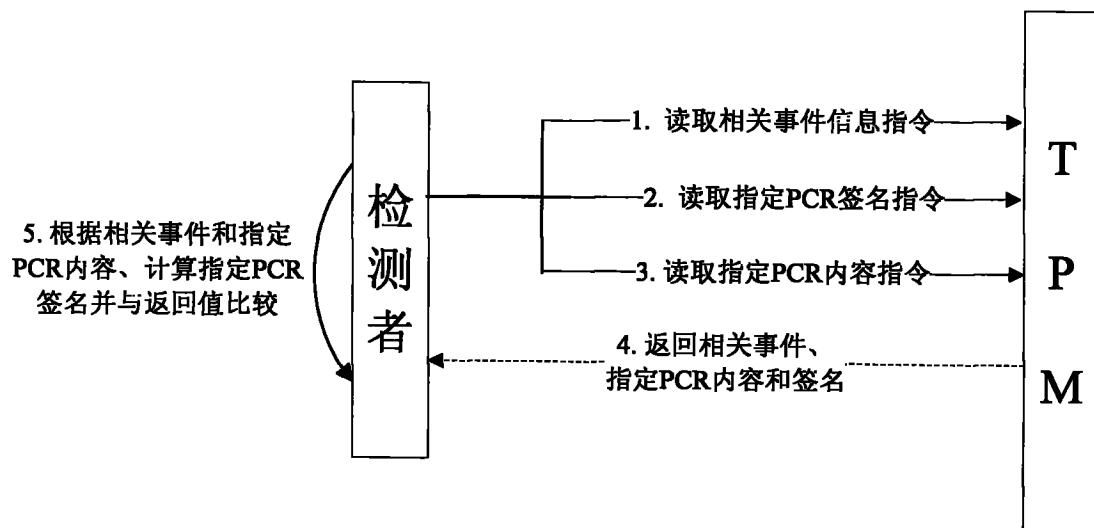


图 11

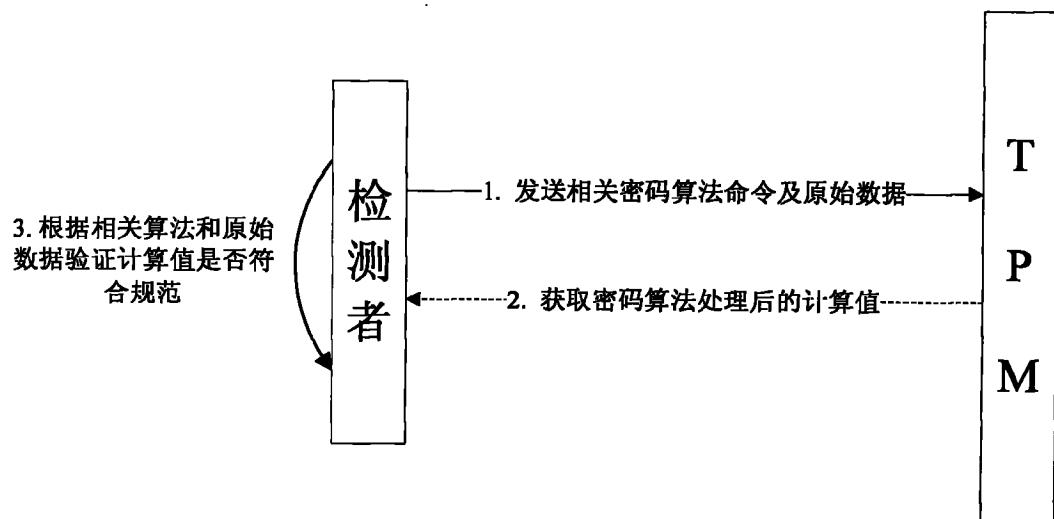


图 12