1. 可信计算
   1. 可信计算概述
      1. 概念

目前可信计算中的可信存在多种不同定义．ＩＳＯ?ＩＥＣ将可信定义为［２］：参与计算的组件操作或过程在任意的条件下是可预测的，并能够抵御病毒和一定程度的物理干扰．ＩＥＥＥ 给出的可信定义为：计算机系统所提供服务的可信赖性是可论证的．ＴＣＧ（Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ）将可信定义为［４］：一个实体是可信的，如果它的行为总是以预期的方式，朝着预期的目标．ＴＣＧ的可信计算技术思路是通过在硬件平台上引入可信平台模块ＴＰＭ（ｔｒｕｓｔｅｄ　ｐｌａｔｆｏｒｍ　ｍｏｄｕｌｅ）来提高计算机系统的安全性，这种技术思路目前得到了产业界的普遍认同．我们的思路与ＴＣＧ类似，认为可信是指以安全芯片为基础，建立可信的计算环境，确保系统实体按照预期的行为执行．

* + 1. 国内外发展现状

早在２０世纪９０年代中期，国外一些计算机厂商就开始提出可信计算技术方案，通过在硬件层嵌入一个安全模块，基于密码技术建立可信根安全存储和信任链机制，实现可信计算安全目标．该技术思路于１９９９年逐步被ＩＴ产业界接受和认可，并形成可信计算平台联盟（Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　ＰｌａｔｆｏｒｍＡｌｌｉａｎｃｅ，ＴＣＰＡ）．同时，于２００１年提出了ＴＰＭ１．１技术标准．之后，一些国际ＩＴ技术主导厂商推出了相关可信计算产品，得到用户和产业界的普遍认可，至此可信计算成为ＩＴ 产业发展趋势．到２００３年，ＴＣＰＡ已发展成员近２００个，几乎包括所有的国际ＩＴ主流厂商，随后ＴＣＰＡ改名为ＴＣＧ，并逐步建立起ＴＣＧ　ＴＰＭ１．２技术规范体系，其触角延伸到ＩＴ技术的每个领域．２００９年该规范体系的４个核心标准成为ＩＳＯ国际标准．在产业发展上，Ｉｎｔｅｌ微软在其核心产品中装配可信计算技术，到２０１０年，ＴＰＭ基本成为笔记本和台式机的标配部件．

* + 1. 国内发展

是 我国一直高度重视可信计算技术，承载着核心技术自主创新信息安全自主掌控的信念，大致经历了３个发展阶段：

第１个阶段为２００１年至２００５年，是消化吸收ＴＣＧ技术理念阶段．联想兆日基于ＴＣＧ技术体系开发出相关产品，瑞达也提出了一套ＰＣ安全技术路线．全国信息安全标准化技术委员会（ＴＣ２６０）成立了可信计算标准工作小组，推进中国可信计算标准的研究．

第２个阶段为２００６年至２００７年，建立自主技术理论和标准体系阶段．我国有关管理部门意识到可信计算给中国ＩＴ产业自主创新带来发展机遇，专门组织学术界和企事业单位，开展基于中国密码算法的可信计算技术方案研究，提出《可信计算密码应用方案》，之后组建了可信计算密码应用技术体系研究专项工作组（后改名为中国可信计算工作组（Ｃｈｉｎａ　ＴＣＭ　Ｕｎｉｏｎ，ＴＣＭＵ），国科学院软件所、同方、兆日、瑞达等１１家单位加入该工作组，制定出以ＴＣＭ（ｔｒｕｓｔｅｄ　ｃｒｙｐｔｏｇｒａｐｈｙｍｏｄｕｌｅ）为核心的《可信计算密码支撑平台技术规范》系列标准［５］，并于２００７年１２月颁布《可信计算密码支撑平台功能与接口技术规范》，同时，国民技术、联想、同方,方正,长城,瑞达等均开发出基于此标准的产品．

第３个阶段为２００８年以后，推动产业发展阶段．ＴＣＭ 产品开始规模上市，获得政府,军工,国计民生领域用户高度认可．中国可信计算工作组目前有国民技术,联想,同方,中国科学院软件所,方正,卫士通等２９个成员单位，由企业牵头，政府支持，大力推进中国可信计算产业的发展．到２０１０年，在ＴＣＭＵ全体成员共同努力下，已建立起可信计算芯片.可信计算机.可信网络和应用.可信计算产品测评的基本完整的产业体系

* 1. 可信计算发展
     1. 可信1.0容错计算
     2. 可信2.0 被动可信体系
     3. 可信3.0主动免疫体系
  2. 组成结构

可信计算的基本思想是

1、首先计算机系统建立一个信任根，信任根的可信性由物理安全、技术安全、和管理安全共同确保。

2、再建立一条信任链，从根开始到硬件平台, 到操系统,到软件系统，到应用体系，到可信网络，逐步建立信任级, 把信任扩展到整个计算机系统, 从而确保整个计算机系统的可信，信任链如图所示

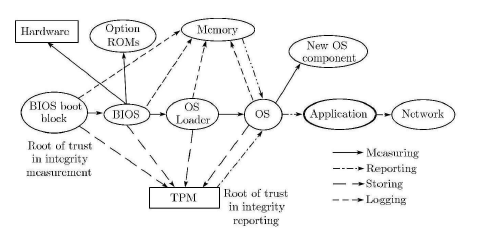


Figure 1 信任链

* + 1. 可信根和可信链

可信根是可信计算的基础，为保证可信，必须先建立一个最初的可信根。

可信根应该满足几个要求：

1. 可信根应该具有密码服务功能。
2. 可信根具备对系统启动过程的度量能力。
3. 可信根具备对系统启动过程的控制能力
4. 可信根优先于其他部分启动。

可信2.0框架由可信平台模块（TPM）以及度量代码段（CRTM）组成。其结构如图所示。

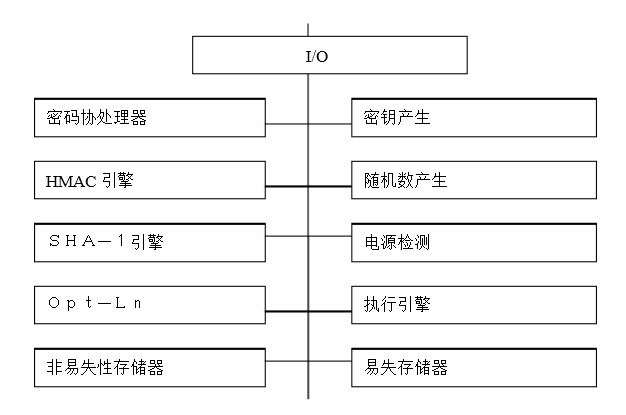


Figure 2TPM结构

可信3.0提出以可信平台控制模块(TPCM)作为系统可信根。由可信密码模块（TCM）和平台控制机制组成。

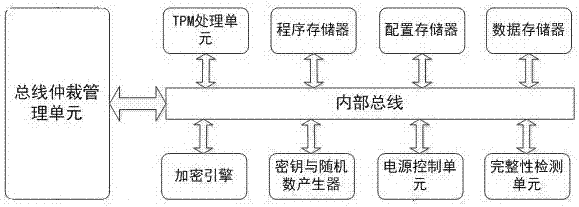


Figure 3 可信平台控制模块（TPCM）示意图

TPMCM先于 CPU启动，通过平台控制功能获取系统的控制权，并对系统进行可信度量，只有度量通过后，将控制权开发给系统。

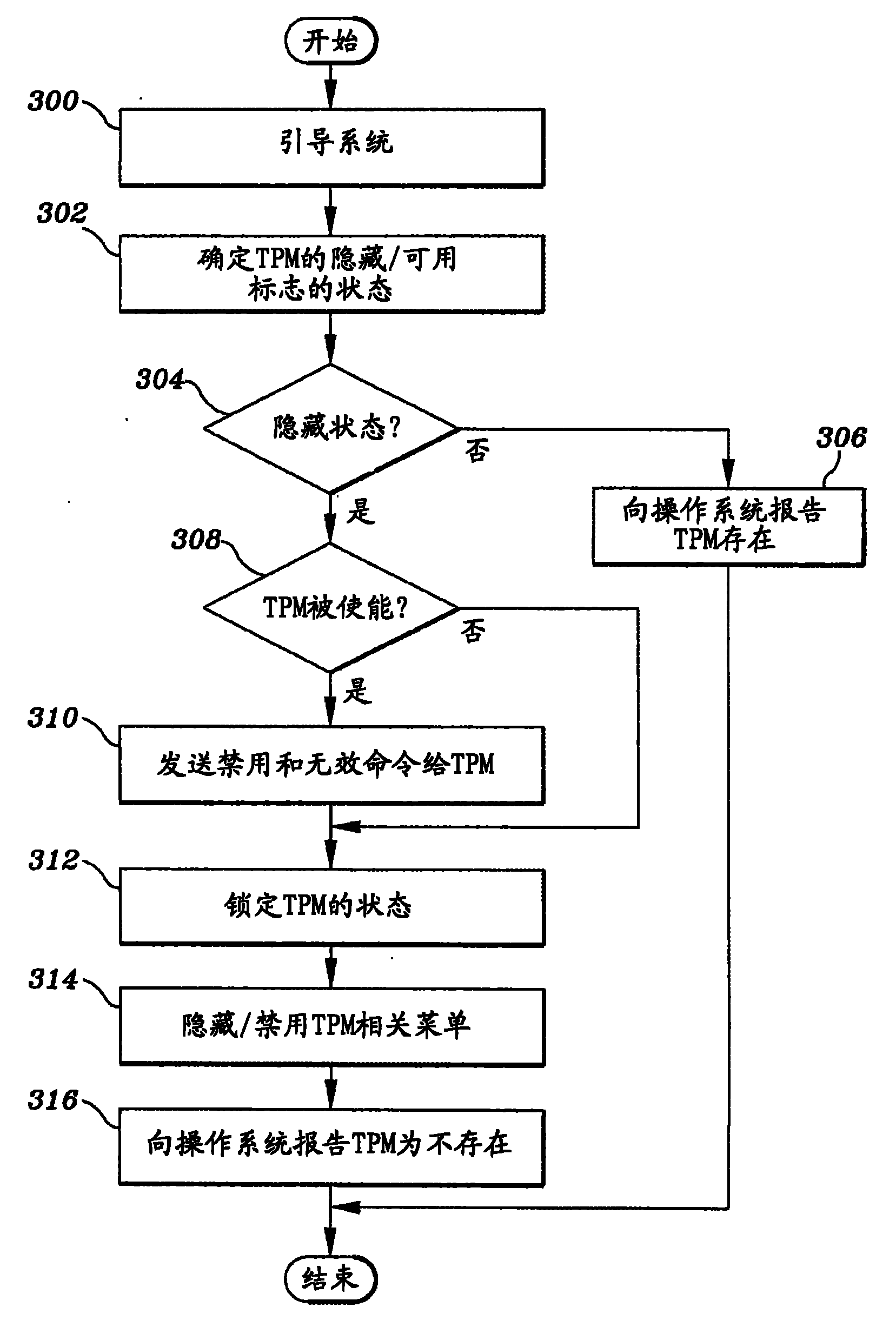


Figure 4系统启动示意图

* + 1. 可信密码服务
       1. 可信存储
          1. 可信存储TCG规范

通过密码机制实现数据的保密存储或完成性保护。

TCG于2007年5月推出了TCG的存储体系结构核心规范。技术来源于细节DriveTrust技术。

DriveTrust 技术利用硬盘的封闭计算环境，定义基于硬件安全功能的硬盘级平台。该技术认为虽然操作系统专门设计用来支持各种应用程序，但硬盘是运行专用代码(固件)管理硬盘功能的封闭存储环境。因为其内部操作与计算系统的其他组件相隔离，故硬盘是实现数据安全功能的理想位置。该技术认为DriveTrust 平台不仅仅能够保护磁盘上存储的数据，该平台还在主机与硬盘之间建立对所发送数据的信任，并使硬盘能够对应用程序进行验证、分配安全存储分区、处理数字签名并提供多种其他安全功能

Drive Trust 技术包含四个元素：

（1）增强型固件和硬件：固件是在硬盘内部计算机中运行的软件；通常，固件用于管理极为复杂的硬盘功能，如移动读取/写入磁头、跟踪磁盘上的坏扇区以及存储数据位置的位图。DriveTrust 技术添加优化硬盘存储资源的其他安全代码，扩展了硬盘的功能。DriveTrust 技术在硬盘中实现加密服务，它提供加密、散列、安全存储、解密、数字签名和随机数字生成等功能。

（2）可信发送/接收命令集：可信存储需要安全的通信基础架构。Drive Trust通信通过可信发送/接收（出/入）命令集发送。该命令集用于协调定义 ATA 和SCSI 接口的标准组织。ATA 和 SCSI 接口协议中包括安全消息传递的内容，以支持包括 DriveTrust 技术在内的安全技术支持。

（3）安全分区：200GB 的硬盘保留约 200MB 不可寻址空间，用于内部系统内存。Drive Trust 技术使用此空间创建安全分区，该分区在逻辑上和物理上均与硬盘存储的其余部分相独立，使用有效的条件访问控制，所以该安全分区也是存储加密密钥的最佳位置。如果硬盘采用 DriveTrust 技术，则只有提供正确凭证的应用程序能够访问上述安全分区，并在其中存储应用程序代码、其他内容或数据。ISV（Independent Software Vendors 的英文缩写，意为“独立软件开发商）可利用该功能构建具有其他功能的应用程序，如增强的身份验证、时间戳、对比日志记录或事务数据。

（4）隔离协议：软件应用程序、基本输入/输出系统和其他程序均可通过严格控制的通信渠道与应用 DriveTrust 技术的硬盘互操作。ISV 和其他开发商可以编写应用程序，并通过隔离协议将它们分配给硬盘中的安全分区。如果应用程序尝试访问这些安全分区，则必须向硬盘的管理员功能模块提供根据管理协议分配的凭证。管理员功能模块对应用程序进行验证，激活相应的安全分区，从而允许该应用程序通过可信发送/接收命令集与安全分区交互。

可信存储的可信源头来源于可信根中的存储根密钥（SRK）。它存放于内部，永远不对外暴露。

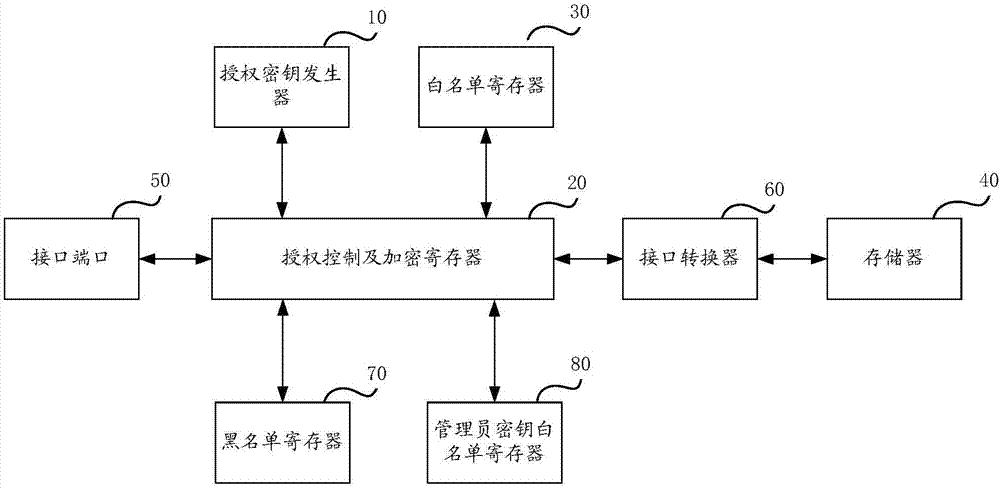


Figure 5 密钥可信存储示意图

* + - * 1. 不依赖于加密的可信存储

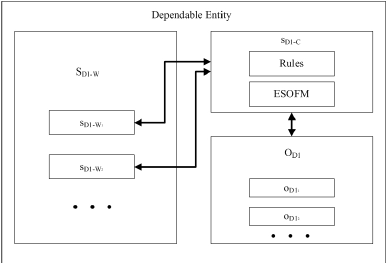


Figure 6可信主机实体体系结构

可信存储模型及体系结构中用 EID 来唯一标识一个实体，但是在实际设计系统时选择什么来唯一表示可信主机或可信移动存储设备的 EID，这是首先需要考虑的问题，下面我们仅给出几种可供选择的方案。

（1）由存储设备生产厂商来定义移动存储设备或主机硬盘的唯一序列号作为 EID。

（2）用主机硬盘的唯一序列号+网卡的 MAC 地址作为 EID

（3）用可信平台模块的背书密钥 EK（endorsement key）的公钥部分作为可信主机的 EID，即 EID=TPM\_Read Pubek。

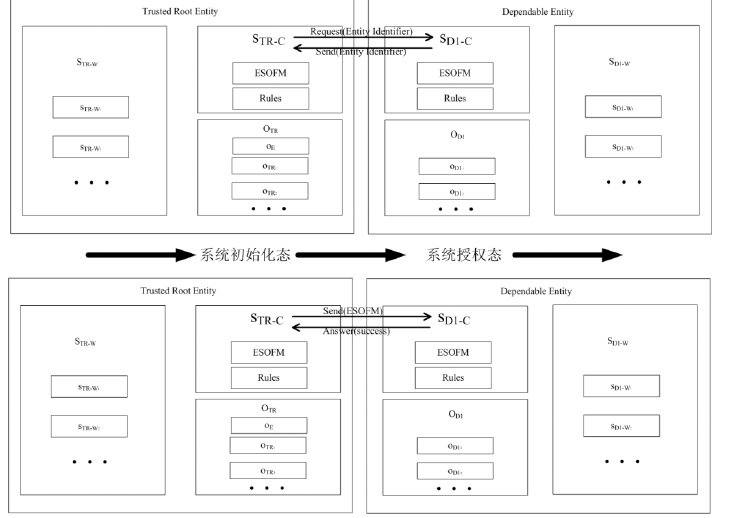


Figure 7 不使用身份签名的通信过程

在非对称密钥体制下：

（1）Request(Entity Identifier)：

sTR-C——> sD1-C：EID（TR），ESKTR（N1）其中 N1 为一随机数，TR 用自己的私钥加密 N1；

sD1-C：首先判断 EID=TR，然后 DPKTR（ESKTR（N1））=N1。

（2）Send(Entity Identifier)：

sD1-C——> sTR-C：EPKTR（EID（D1），PKD1，N1）；

sTR-C：首先 DSKTR（EPKTR（EID（D1），PKD1，N1））=EID（D1），PKD1，N1，然后判断 N1=N1，最后得到 EID（D1）和 D1 的公钥 PKD

1。

（3）依次进入系统中间态、系统初始化态、系统授权态。

（4）Send(ESOFM)：本条中的 D1 可看做可信域中的任何可信主机

sTR-C——> sD1-C：EPKD1（EID（TR），ESOFM，N2）； sD1-C：DSKD1（EPKD1（EID（TR），ESOFM，N2））= EID（TR），ESOFM，N2，判断 EID=TR，得到 ESOFM、N2，然后用新的 ESOFM 替换旧的 ESOFM。

（5）Answer(success)：本条中的 D1 可看做可信域中的任何可信主机 sD1-C——> sTR-C：EPKTR（EID（D1），N2）； sTR-C：首先 DSKTR（EPKTR（EID（D1），N2））=EID（D1），N2，然后判断EID=D1、N2=N2，证明成功传送 ESOFM，最后结束会话。

在对称密钥体制下：

（1）Request(Entity Identifier)：本条也可看做与可信域中除 D1 外的其他可信主机传输会话密钥的过程（传输会话密钥的三次握手过程，但在传输密钥的过程中存在伪造威胁）。 sTR-C——> sD1-C：EID（TR），OPID（EK），EKTR（KS，N1）其中 OPID（EK）表示要求接收者用自己的秘密密钥进行加密操作，KS为会话密钥，TR 用自己的秘密密钥加密（KS，N1）； sD1-C：首先判断 EID=TR、OPID=EK，然后 D1 用自己的秘密密钥加密（EKTR（KS，N1））； sD1-C——> sTR-C：OPID（DK），EKD1（EKTR（KS，N1））其中 OPID（DK）表示要求接收者用自己的秘密密钥进行解密操作；

sTR-C：首先判断 OPID=DK，然后 DKTR（EKD1（EKTR（KS，N1））） KD1（KS，N1），本步存在安全威胁，因为 sTR-C无法判断信息流是来自 sD1-C； sTR-C——> sD1-C：EID（TR），OPID（DK），EKD1（KS，1）； sD1-C：首先判断 EID=TR、OPID=DK，然后 DKD1（EKD1（KS，1））= KS，N1 得到会话密钥 KS和 N1 随机数。 （2）Send(Entity dentifier)： sD1-C——> sTR-C：OPID（DKS），EKS（EID（D1），N1）中 OPID（DKS）表示要求用会话密钥进行解密操作； sTR-C：首先判 PID=DKS，然后 DKS（EKS（EID（D1），N1））=EID（D1），N1，然后断 N1=N1，最后得到 EID（D1）。 （3）依次进入系统中间态、系统始化态、系统授权态。 （4）Send(ESOFM)：本条中的 D1 可看做可域中的任何可信主机，即向可信域中其他主机下发 ESOFM sTR-C——> D1-C：OPID（DKS），EKS（EID（TR），ESOFM，N2）； sD1-C：首先判 PID=DKS，然后 DKS（EKS（EID（TR），ESOFM，N2））=EID（TR），ESOFM，2，判断 EID=TR，得到 ESOFM、N2，然后用新的 ESOFM替换旧的 SOFM。 （5）Answer(success)：本条中的 D1 可看做可信域中的任可信主机 sD1-C——> sTR-C：OPID（DKS），EKS（EID（D1），N2）； sTR-C：先判断 OPID=DKS，然后 DKS（EKS（EID（D1），N2））=EID（D1），N2，然后判断 EID=D1、N2=N2，证明成功传送 ESOFM，最后结束会。

* + - * 1. 基于区块链的可信存储技术

在不同的应用场景或设计体系中，区块链技术根据准入机制一般被分为公有链、私有链和联盟链。公有链节点可以自由地进入或退出区块链网络，并且读取或写入链上的数据。私有链节点的准入与写入操作受内部权限控制，读操作可选择性地对外开放，仍具有区块链分布式存储架构。联盟链不同于公有链、私有链，它采用多中心的方式，通过预先设置参与节点和权限控制，成为介于公有链和私有链之间的“中间态”产品。联盟链因节点数量相对有限且有组织构成，具有弱中心化、强可控性、强拓展性、交易速度较快等特性，主要适用于特定组织或公司进行搭建。

基于区块链的可信存储，在论文[25]中提出。先简述如下：包括几个方面的工作：

身份认证：

Hyperledger Fabric 的成员身份认证基于标准的X.509 证书，采用PKI（public key infrastructure）体系为每个成员生成数字证书以标识用户身份。MSP（membership service provider）是Hyperledger Fabric 的一个组件，它将证书发布、用户认证、后台加密机制和协议进行抽象，提供身份到组织的映射，利用PKI 体系发布数据证书，结合MSP 进行身份认证和权限控制。通过信任背书签发证书，从根CA 证书的私钥签名生成的证书还可以签发新证书，中间CA 证书可由其他CA证书签发，也可利用自身私钥签发新证书由此可形成一个证书信任链；Fabric CA 是超级账本的数字证书认证中心模块，Fabric CA 服务端提供用户登录和注册的数字证书管理功能，提供了RESTful 接口供客户端访问，数据存储在MySQL 中。通过MSP 标识检查身份证书有效性、证书路径检查是否存在用户证书到根CA证书的有效路径及CRL检查证书是否被吊销完成身份认证。

数据上传

电能量数据采集节点先发送数据给附近数据采集基站，第i 个数采集节点i N 向数据采集基站中第j 个数据采集基站j DC 传输的数据格式为数据IPFS存储Record E Data CertSig timestamp (1)= ( || ) Ni Ni i E PK N Data E ata imestamp (2)( ) Ni Ni Ni sign SK E Sig  Sign Data (3)其中，DCj PK 为实体j DC 的公钥，DCj PK E 为利DCj PK 加密信息，Ni PK 为实体i N 的公钥，Ni PK E为利用Ni PK 加密信息，Ni Data 为利用数据集节点i N 采集到的原始数据， timestamp 为时间戳，Ni SK 为实体i N 的私钥，SKNi Sign 为用实体i N 的私钥对Ni E Data 哈希运算后进行的签名数据。

数据IPFS存储

数据采集基站收集上传数据后对上传*Record* 进行验证，如利用身私钥解密*DCi SK* 得到字段如式(4)所示。( )( || || || )*DCj i j SK N DC D RecordData ert Sig timestamp* (4)提取其中的*Cert* 字段，对其进行身份验证确定据来源为*i N* ，并计算出*i N* 的公钥*Ni PK* ，对提取出的*Sig* 字段进行密，得到( ) *Ni PK D Sig* ，再对*Data* 进行哈希加密得到哈希数值，与发节点发送来的数字签名解密得到的哈希数值( ) *Ni PK D Sig* 进行校验，若同则通过校验，验证数据正确。如果数据来源安全且完整有效，数据集节点客户端向IPFS 请求将信息存储到IPFS 中，IPFS作为基于内寻址的分布式存储网络，采用分布式哈希表（DHT）索引结构及Merkle 向无环图数据结构，服务器位置及文件存储名称或路径都不被作为索条件。客户端提交数据存储请求至IPFS 节点，IPFS 将会根据文件容计算得到的哈希值返回给数据采集基站客户端。

数据区块链上传

数据采集基站节点向区块链网络发送上传请求，调用智能合约stub.PutState 并将哈希值和信息类型等参数传入区块链网络；区块链节点收到请求首先验证用户身份，通过后执行智能合将哈希值、客户端ID、数据采集节点ID、查询数据类型（表码表）、数据收集时间绑定并播该请求给其他节点执行相同的操作；然后在节点间达成共识后将智能合约执行结果写入区账本，反馈给收集节点客户端信息保存情况。电能量数据上传流程如图 所示。

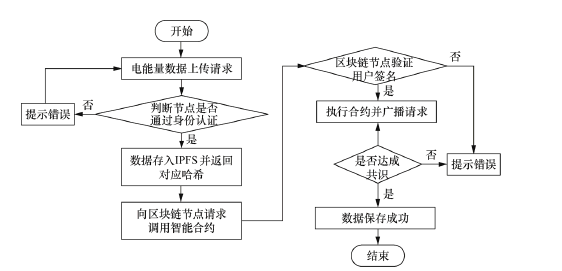


Figure 8数据上传流程

数据访问验证

若客户端节点*m DC* 提交访问请求*n DC* 数据采集器所采集的*Nj* 据采集节点数据。首先，客户端节点*m DC* 应向数据采集器节点*n DC* 出感知数据共享请求， *n DC* 节点查验身份后，将请求转发给数据采节点*Nj*；采集节点*Nj*制定访问约束条件（如数据共享范围、时效、问次数等）授权访问，并将访问约束条件及访问数据的加密私钥*j SK* 送给数据采集器节点*n DC* ，数据采集器节点*n DC* 将访问条件、加密钥*j SK* 等用客户端节点*m DC* 公钥*DCm PK* 加密发送给客户端节点*m C* 。其次，数据采集器节点*DCm* 通过自身私钥解密数据，并向智能合约出访问请求，访问过程图3 所示，根据访问条件及访问身份调用智合约解锁脚本，智能合约分析访问请求，提取信息类别后向区块链节请求调用stub.GetState 将查询条件作为参数传入，区块链节点执行智合约，从区块链账本中检索出查询信息对应的哈希记录并反馈给客户密信息，若据哈希记录在IPFS 中检索不出文件或检索出文件不符合访问条件，则证明数据被篡改。最，户端节点m DC 利用从区块链上访问数据及n DC 发送的加密私钥j SK 后，利用加密私钥j SK 密访问数据，完成数据访问过程。端节点DCm；客户端DCm 根据哈希记录向PFS 节点发起请求查询出对应的加

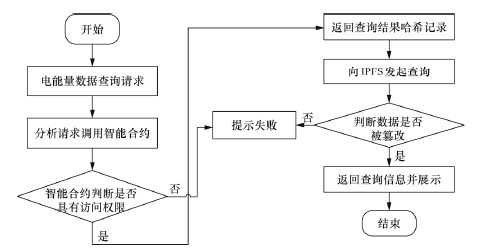


Figure 9 数据访问流程

* + - 1. 可信度量

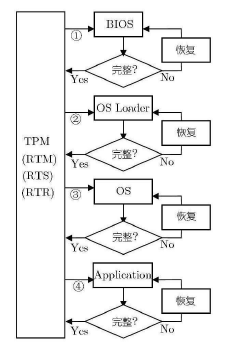


Figure 10简单的度量模型

信任链的起点是信任根，信任链的传递则是依靠可信度量技术来实现。在信任链的理论中，无论是最底层的 BIOS 启动模块还是到最上层的应用，在得到信任以运行之前，都需要经过度量，即一个测量者认证的过程。数据完整性度量技术通过消息认证码 MAC（Message uthentication Code）的一致性校验来实现度量的功能。这是现在主的度量技术方法。对于 MAC 的产生，可以利用强的分组密码或者利 ASH 函数来实现。TPM 中提供了满足单向性、抗碰撞性的安全 HASH 数 SHA-1 引擎，可以为度量的实现提供保证。 同时 TPM 还提供安存储以及内部的平台配置寄存器 PCR（Platform Configuration egister），样配合 TPM 的内部接口函数就可以把信任链传递下去。可信度量的新以及实际应用都是以平台配置寄存器 PCR 作为载体的。

一个平台中可能会有大量的完整性度量，一个特殊的完整性度量需要实时地存储更新的值。一个完整性度量的新值不允许简单地覆盖现存的值。因为这样难以鉴别完整性度量的度量来源，而且攻击者可能擦除或者替换一个正确值。如果完整性度量值个别地存储，更新值也要个别地存储，那么就难以定位存储空间的大小。作为可信度量存储载体的 PCR 就是在寄存器中支持无限的度量数量。它通过使用密码学的哈希算法对更新的 PCR 做哈希（消息摘要）。伪代码如下：

PCRi New = HASH ( PCRi Old value || value to add)

新的 PCR 值产生过程中对两部分进行了哈希，一是旧的 PCR 值，一是所增加的新数据。这样更新 PCR 的顺序是不可交换的，例如度量从 A 到 B，并不等于从 B 到 A 的度量。哈希值的另外一个特性是单向的。这意味着对于攻击者要确定输入给 PCR 的值在计算上不可行。此后更新 PCR 若没有前一个 PCR 值作为基础将不能进行。或者在重启之后，如果所有提供给 PCR 寄存器的信息缺失，后续的更新 PCR 也不能进行。 另外，在使用一个 PCR 过程中，对于 TCG 平台规范明确规定忽略的事件，度量值便不用更新。如果 PCR 已经度量过最少一个某种类型的事件，那么该类事件也可以忽略。这样就可以避免频繁记录某些重复的状态（如睡眠状态），以便延长 TPM 的使用寿命。软件数据完整性是信息安全的重要部分，但是，软件数据完整性还不能保证动态的安全性。所以上层应用软件的度量除了完整性检测度量之外，还需要借鉴其他一些度量方法。

随着现代软件的功能越来越完善，软件代码的规模也越来越庞大，度量的数据量也超乎寻常，需要对软件程序有所选取地进行度量。通过层次分析法，尽可能多地列举多种可能的度量方面，并计算出每个方面的权重值，以确定最重要的度量点。 其次对应用软件进行可信级划分，对于基本不可信以及可信程度低的软件，则不能通过度量。外因为软件的模糊性，需要引入专家评估系统，对应用软件的等级进认定。只有通过完整性检验并且等级被认定为可信的软件才能得到操作系统的授权运行。

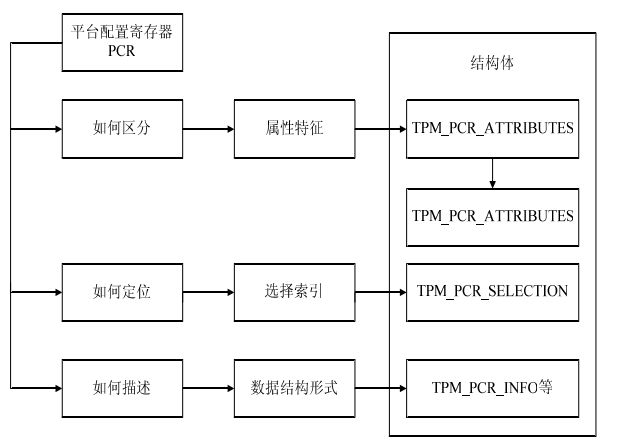


Figure 11可信度量存储体系

* + - 1. 可信报告和可信认证

可信平台度量得以广泛应用的基本功能就是完整性度量和完整性检验[28]。

完整性是可信计算的核心概念。它在可信计算技术中被广泛地应用，一般用作表示一个组件的本质状态，可由组件的设计者或者制造者发布。无论是制造完成不久或者经过长时间的日常使用，这种状态都需要一直保持。状态的任何改动都要及时地检测并报告。 完整性理的内容则是通过完整性以及实时完整性来管理组件信息。包括装载间和运行时间所作的度量。但是完整性管理不保证组件的正确性，因可信平台允许检测易变组件，这种组件的合法变更与非法篡改之间难以确定界限。

平台的可信性不单面对用户和自我管理，在外部实体评价某特定平台状态的时候也意义重大。完整性管理的基本目标在于以下可信平台功能：

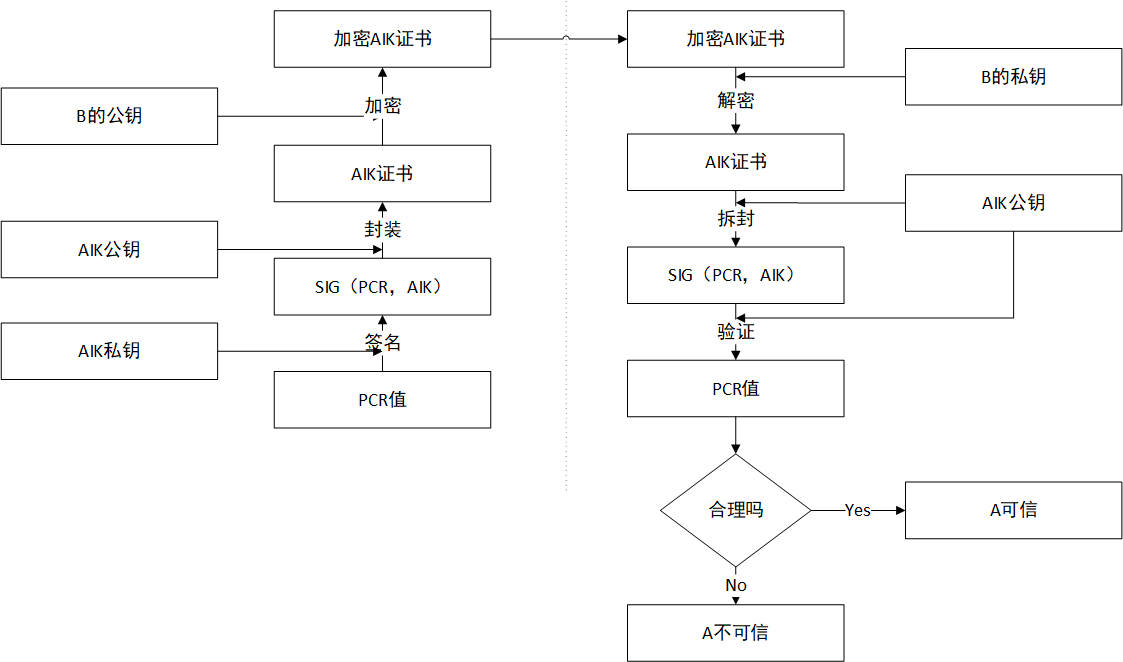


Figure 12可信计算度量机制

（1）完整性度量

它允许一个平台做自身的完整性度量。完整性度量是可信计算理念的重要概念。一个可信平台不但要装备足够的工具组建一个可信计算环境，并且要能测量其达到的可信层次。因此关键的度量信任根是可信计算平台的核心部件。度量有着双重的含义，首先是实时度量，涉及平台对软件组件进行的哈希扩展操作。其次是度量参考，涉及硬件组件或者软件组件的相关信息，一般是由制造者提供。

（2）完整性报告

它允许度量能向外提供报告。可信平台建立一个值得信赖的环境并且以预定的方式进行了度量的同时，也要以一定的方式向外界提供这些度量的报告。把自身完整性状态的报告作为证明握手协议的一部分，大大增强了当前基于信任链的证明机制。因此报告方面的信任根也是可信计算的一个关键概念。 应用两者作为完整性模型的核心，请求方与校验方之间的基本交互方式遵循完整性度量和报告的一般性应用模型。

* + 1. 可信部件
       1. 可信密码模块（TCM）

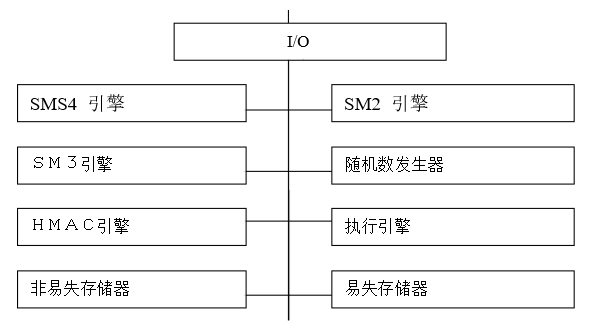


Figure 13 TCM结构

平台结构主要分为TCM 和TSM（TCM service module）。TCM 是可信计算密码支撑平台必备的关键基础部件，提供独立的密码算法支撑。TCM 定义了一个具有存储保护和执行保护的子系统，该子系统将为计算平台建立信任根基，并且其独立的计算资源将建立严格受限的安全保护机制。为防止TCM 成为计算平台的性能瓶颈，将子系统中需执行保护的函数与无需执行保护的函数分开，将无需执行保护的功能函数由计算平台主处理器执行，这些功能函数构成TSM。

TCM 结构如图13所示，各部件功能如下：

I/O：TCM 的输入输出硬件接口；

SMS4 引擎：执行SMS4 对称密码运算；

SM2 引擎：产生SM2 密钥对，执行SM2 加/解密、签名

运算；

SM3 引擎：执行杂凑运算；

随机数产生器：生成随机数；

HMAC 引擎：基于SM3 引擎，计算消息认证码；

执行引擎：TCM 的运算执行部件；

非易失性存储器：存储永久数据的存储部件；

易失性存储器：TCM 运行时的临时数据存储部件。

可信计算密码支撑平台涉及密码算法包括：SM2 椭圆曲线密码算法、SMS4 对称密码算法、SM3 密码杂凑算法、HMAC 消息认证码算法、RNG（随机数发生器）。SM2 椭圆曲线密码算法，密钥长256 位，包括：系统参数、密钥对生成和三个子算法，三个子算法分别是：数字签名算法(SM2-1)、密钥交换协议(SM2-2)、加密算法(SM2-3)。SMS4 是对称密码算法，分组长度为128bit，密钥长度为12bit，加密算法和密钥扩展算法都采用32 轮非线性迭代结构，加、解密算法的结构相同，只是轮密钥的使用顺序相反。规范要求采用CBC 模式，Ⅳ由用户自定义，数据的最末分组(128bit/16byte)需填充，如果最末数据分组长度为16byte，则在其后填充16 个内容为16 的byte，否则按最末数据分组不足16byte 所缺少的字节个数d，填充d 个内容为d 的byte。

SM3 密码杂凑算法，对给定的长度为k(k<264)的消息，经填充、迭代压缩和选裁，生成杂凑值，迭代压缩时，输入为预处理的消息分组64byte，输出摘要为32byte。HMAC 消息认证码算法，利用密码杂凑算法SM3，对给定的消息和验证双方共享的密码信息产生长度为t(16≦t≦32)个字节的消息验证码，计算公式：HMAC＝SM3((K0⊕opad) || SM3((K0⊕ipad) || text))[2]，TCG 规范对TPM 要求

HMAC 消息认证码算法使用支持20byte 的SHA-1 算法[3,4]。RNG，规范不限定随机数生成的算法，算法由TCM 制造商设计实现，要求所生成的随机数必须为真随机数，并满足国家商用密码随机数检测要求。

* + - 1. 可信平台控制芯片

TCG认为：在可信PC 中以核心BIOS(boot block BIOS)作为初始的信任根，即核心可信度量根CRTM，计算机平台启动时，先加载核心BIOS，由核心BIOS 度量其本身和BIOS 其它模块，如果通过则将控制权交给其它BIOS，由其它BIOS 度量去度量下一步要加载的程序，直至将制权交给操作系统，从而将硬件、BIOS、操作系统等各个部分通过信任链传递联系起来，构建一个可信的运行环境，提供可信度量、可信报告、保护存储、证明等功能。

。但是TCG 在构建可信平台的时候遵循通用、廉价、易用、标准等原则，为适应现有的计算机体系，放弃了一些安全特性，导致这个平台存在着一些缺陷，难以满足高可信安全环境的需求：

在TCG 可信平台中，可信根由三大信任根组成：可信储根RTS、可信报告根RTR 和可信度量根RTM。RTM 的初始点是核心可信度量根CRTM，在TCG 可信平台，CRTM并不明确，大多数的实际实现均以BIOS 的Boot Block 或整个BIOS作为核心可信度量根CRTM，在其运行之前并不进行完整性验证，而是由其自身保证完整性。由于CRTM并未集成到TPM中，也就无法受到TPM物理上的保护。随着攻击手段的发展，作为连接软件硬件桥梁的BIOS 比硬件更容易受到诸如BIOS Rootkit等方式的攻击，因而很有可能会被纂改、替换，造

成信任根的不可信，导致无法进行度量或度量失效，降低系统的安全性和可信性保障；

为了适用于现有的计算机体系，TPM通过LPC 总线挂接到南桥，但是LPC 总线的数据地址线较少，协议简单，因此容易采集总线上的数据进行分析，降低了模块的安全性；

出于安全考虑，TCG 规范中避免使用对称密钥。对称密钥和非对称密钥各有各的优缺点，需要在应用中互相结合使用才能发挥更好的安全作用。因此不设置对称密钥给实际使用造成了一定的困难。此外TCG 规范中采用多级树形结构管理密钥，使得对密钥的访问过于繁琐，降低了系统的效率；

在一些高可信安全的应用中，往往希望能在TPM中进行高速的加解密运算，但是目前的TPM对外的总线LPC 总线只有33MHz 频率、4 根地址数据复用线，在该总线上还连接了Super I/O 等设备，通信速度有限，难以满足高速加解密运算的需求。

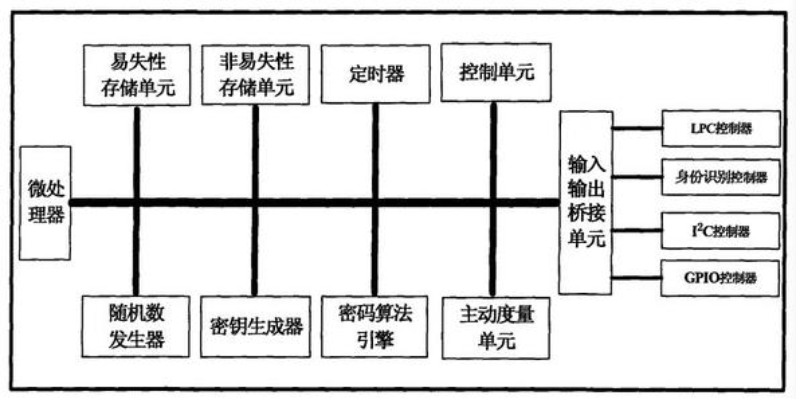


Figure 14TPCM结构示意图

在可信3.0中提出了TPCM来改进这些缺点。有论文提出了基于国产芯片的可信硬件平台。

可信硬件平台由全增强的BIOS、集成在主板上的可信平台控制模块(trusted platformcontrol module，TPCM)以及CPU 和存储器等设备组成，其结构如图所示。平台的可信安全核心是由安全控制模块(securitycontrol module，SCM)、易失性存储器、非易失性存储器、安

BIOS 和可信密码芯片等组成的可信平台控制模块(TPCM)。

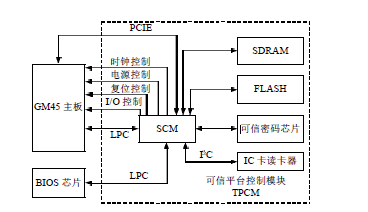


Figure 15可信平台TPCM

TPCM 中的SCM 模块采用SOPC 方式实现，集成有通过内部Avalon 总线相连的主板控制模块、密码芯片控制器、FLASH控制器、SDRAM 控制器、LPC 控制器、PCIE 控制器、I2C 控制器，并与外部的密码芯片、FLASH 芯片、SDRAM和BIOS 芯片互联。可信密码芯片主要完成数字签名、密钥生成、杂凑算法、高速对称加解密运算等功能。易失性存储器为128MB 的SDRAM，为SCM 提供扩展内存。非易失性存储器为4GB 的NAND FLASH，用于存储审计日志、BIOS 映像、操作系统内核映像等，并只能由SCM 平台控制模块访问。在该平台中，可信平台控制模块TPCM 实现了TPM 的基本功能，结合其它模块可以实现身份认证、认证启动、I/O端口物理控制、完整性度量、BIOS 保护和恢复、系统内核恢复、审计日志等多种安全功能。

一个性能比较完善的TPCM芯片对于从根本上为我国信息安全提供自主可控能力有重要的意义。

* + - 1. 可信主板

主板在整个计算机体系中处于一个承上启下的地位，为上层的软件提供运行的平台。为达到可信标准制定的目标，可信平台主板应能实现以 TPCM 为信任根的静态信任链的建立、从开机到操作系统内核加载前的信任链传递。《可信平台主板功能接口》标准在三个方面对可信平台的主板进行了约束：主板的组成结构，规定TPCM 与主板的绑定关系、主动度量的实现要求、芯片对外部设备硬件级别的访问控制；信任链构建流程，规定如何进行度量以及度量日志的存储；功能接口定义了主板对外的功能接口，即BIOS的功能接口。可信平台主板是由可信平台控制模块和其它通用部件组成，实现从开机到操作系统内核加载前的平台可信引导功能。通用部件主要包括：中央处理器、随机存取存储器（RAM）、输入输出接口、Boot ROM 固件等。

（1）必须确保可信平台主板和 TPCM 一对一的绑定关系。

（2）支持 TPCM 对输入输出接口的控制，TPCM 最少但不限于

控制以下输入输出接口的开启或关 闭：USB、PS/2、PCIE、PCI、

SATA、串口、并口、网络接口。

（3）在 CPU 执行 Boot ROM 代码 前，TPCM 先 启 动，TPCM 中 的RTM 对 Boot ROM 中的 Boot Block 进行完整性度量和度量结果的存储。

（4）EMM 作为 RTM 度量根的扩展度量模块，实现对执行部件的完整性度量，实现信任链传递。

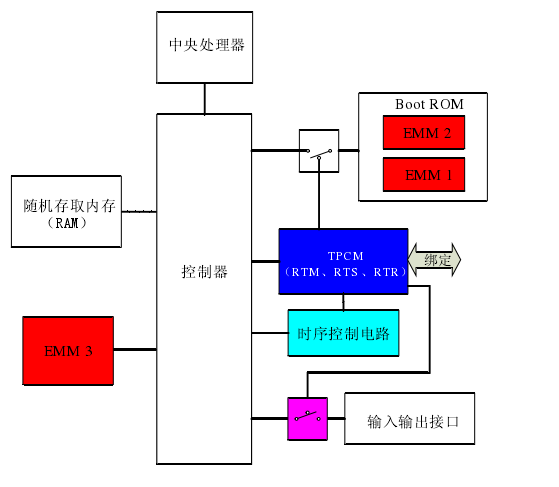


Figure 16可信平台主板结构

* + - 1. 可信软件

TCG组织提出的可信软件栈TSS(TCG Software Stack)是与TPM进行交互的核心软件部件，其作用主要是为操作系统和应用程序提供使用TPM的接口，并提供增强TPM功能的函数，是TPM与上层应用之间的桥梁。

TSS的主要功能如下：

1）为应用程序提供到TPM功能服务的单入口点。

2）按标准构建字节流隐藏应用程序锁构建的复杂命令流格式。

3）提供对TPM的同步访问控制。

4）对TPM的资源进行管理。

TSS由四个层次组成，由上向下分别为：TSS服务提供者TSP(TCG Service Provider)，TSS核心服务TCS(TCG Core Services)，TCG设备驱动库TDDL(TCG Device Driver Library)，以及TPM设备驱动TDD(TPM Device Driver)。TSP为应用程序直接提供接口函数，TCS向上为TSP提供通用服务，TDDL提供TSS用户模式与内核模式的接口函数，TDD直接驱动TPM芯片。

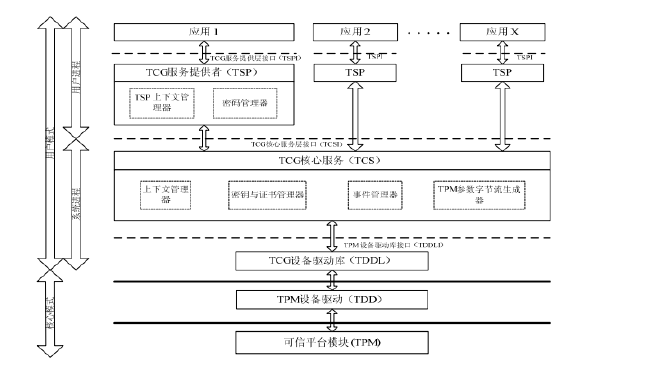
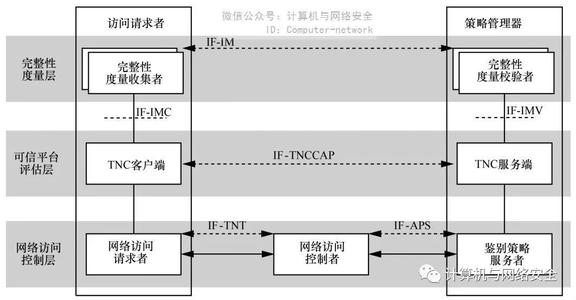


Figure 17TCG可信计算结构框架

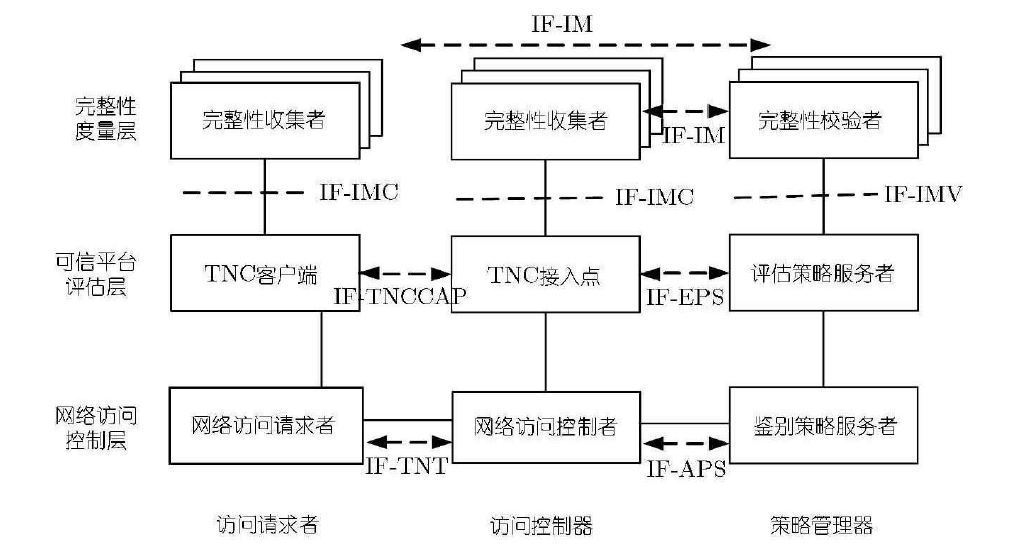
* + - 1. 可信网络连接
         1. 可信连接机制TNC

可信网络连接（Ｔｒｕｓｔｅｄｎｅｔｗｏｒｋｃｏｎｎｅｃｔｉｏｎ，ＴＮＣ）是通过对信任链的建立，然后将可信计算平台的可信性延伸到网络环境来实现整个网络可信的网络连接。可信网络连接的核心思想是：通过对请求连接的终端平台的可信性进行验证，根据其可信性对终端的接入进行控制，来确保网络连接环境的可信。可信网络连接的基础架构如图３．５所示，架构对网络终端接入的过程、连接的方式、通讯协议等进行了整合，同时与传统的信息安全防御设备、网络行为控制等设施进行了交互。在可信网络连接架构下，终端可信平台不再是孤立可信任点，相应的网络控制设施的加入更是对可信网络信任链的建立提供了有力的保障，使整个信任链处在安全的环境中

可信网络连接框架由５个实体、３层结构以及多个对象接口组成，５个实体分别是访问请求者ＡＲ、策略执行点ＰＥＰ、策略决定点ＰＤＰ、元数据存取点ＭＡＰ和网络行为控制和监控点。

ＴＮＣ接入策略为：访问请求者发出接入请求，报告其可信完整性给策略决定点，请求接入，策略决定点通过安全策略对访问请求者的接入访问进行判别，然后根据访问请求者的报告信息决定其接入控制，再由策略执行点对其接入进行决策。而元数据服务器作为可信网络连接的接入终端连接完整性、策略信息等存储中心，对申请接入的终端的连接信息进行储存；网络行为控制和监控点作为可信网络连接的控制终端，对可信网络接入点的完整性、接入策略等信息向元数据存取点进行报告，同时根据元数据存储点中存储的相关信息对接入终端的连接进行管理。

* + - * 1. 三元可信连接机制



访问请求者访问请求者主要用于发起网络访问请求、通过可信第三方实现与访问控制器的双向身份鉴别；同时对接入终端的完整性进行收集，生成完整性度量报告，完成与访问请求者访问控制器的双向平台鉴别；同时，对应用行为进行收集，生成相应度量报告，发送到策略管理器。 访问请求者包括以下功能模块：行为收集者，完整性度量收集者,TNC 客户端，网络访问请求者。

（2）访问控制器

访问控制器主要功能包括：实现与访问请求者的双向身份鉴别和可信评估；完成对服务端接入点的行为收集；将接收到的接入终端的完整性度量值发送到可信认证中心；收集接入点行为信息，生成评估报告发送到策略管理中心。 访问控制器主要包括以下模块：行为收集者，完整性度量收集者,TNC 接入点，网络访问控制者。

（3）策略管理器

依靠策略管理器，访问请求者和访问控制器可以完成双向身份鉴别，在此过程中可信第三方对双方证书的有效性进行验证。策略管理器对 TNC 客户端和TNC 接入点的平台完整性和网络行为可信性进行校验评估，形成度量报告。 策略管理器主要包括以下模块：行为校验者，完整性度量校验者，评估策略服务者，鉴别策略服务者。

* + 1. 可信体系架构

可信计算机结构以国产密码体系为基础，以可信平台控制模块为可信根，以可信主板为平台，以可信软件为核心，以可信网络连接为纽带，整合各种可信应用形成可信计算体系，为通用计算体系提供主动度量控制等服务。形成可信的双体系结构，保障信息系统和网络环境的整体安全。



Figure 18可信体系结构基本原理

1. 参考文献

［１］ Ｃｈｉｎａ　Ｉｎｔｅｒｎｅｔ　Ｎｅｔｗｏｒｋ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｃｅｎｔｅｒ．２００５Ｓｕｒｖａｙ

ｒｅｐｏｒｔ　ｏｆ　Ｃｈｉｎｅｓｅ　ｉｎｔｅｒｎｅｔ　ｓｅｃｕｒｉｔｙ［ＥＢ?ＯＬ］．２００５．［２０１１－

０１－２５］．ｈｔｔｐ：??ｗｗｗ．ｃｎｎｉｃ．ｎｅｔ．ｃｎ

［２］ Ｃｏｍｍｏｎ　Ｃｒｉｔｅｒｉａ　Ｐｒｏｊｅｃｔ　Ｓｐｏｎｓｏｒｉｎｇ　Ｏｒｇａｎｉｓａｔｉｏｎ．Ｃｏｍｍｏｎ

ｃｒｉｔｅｒｉａ　ｆｏｒ　ｉｎｆｏｒｍａｔｉｏｎ　ｔｅｃｈｎｏｌｏｇｙ　ｓｅｃｕｒｉｔｙ　ｅｖａｌｕａｔｉｏｎ．ＩＳＯ?

ＩＥＣ　Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｓｔａｎｄａｒｄ　１５４０８ｖｅｒｓｉｏｎ　２．１［Ｓ］．Ｇｅｎｅｖｅｓｅ：

Ｃｏｍｍｏｎ　Ｃｒｉｔｅｒｉａ　Ｐｒｏｊｅｃｔ　Ｓｐｏｎｓｏｒｉｎｇ　Ｏｒｇａｎｉｓａｔｉｏｎ，１９９９

［３］ Ａｖｉｚｉｅｎｉｓ　Ａ，Ｌａｐｒｉｅ　Ｊ　Ｃ，Ｒａｎｄｅｌｌ　Ｂ，ｅｔ　ａｌ．Ｂａｓｉｃ　ｃｏｎｃｅｐｔｓ　ｏｆ

ｄｅｐｅｎｄａｂｌｅ　ａｎｄ　ｓｅｃｕｒｅ　ｃｏｍｐｕｔｉｎｇ ［Ｊ］．ＩＥＥＥ　Ｔｒａｎｓ　ｏｎ

Ｄｅｐｅｎｄａｂｌｅ　ａｎｄ　Ｓｅｃｕｒｅ　Ｃｏｍｐｕｔｉｎｇ，２００４，１（１）：１１－３３

［４］ Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ．ＴＣＧ　ｓｐｅｃｉｆｉｃａｔｉｏｎ　ａｒｃｈｉｔｅｃｔｕｒｅ

ｏｖｅｒｖｉｅｗ，ｖｅｒｓｉｏｎ　１．２ ［ＥＢ?ＯＬ］．２００３．［２０１１－０１－２５］．

ｈｔｔｐｓ：??ｗｗｗ．ｔｒｕｓｔｅｄｃｏｍｐｕｔｉｎｇｇｒｏｕｐ．ｏｒｇ

［５］ Ｃｈｉｎａ　Ｓｔａｔｅ　Ｐａｓｓｗｏｒｄ　Ａｄｍｉｎｉｓｔｒａｔｉｏｎ　Ｃｏｍｍｉｔｔｅｅ．Ｔｅｃｈｎｉｃ

ｓｐｅｃｉｆｉｃａｔｉｏｎ　ｏｆ　ｃｒｙｐｔｏｇｒａｐｈｉｃ　ｓｕｐｐｏｒｔｉｎｇ　ｐｌａｔｆｏｒｍ　ｆｏｒ　ｔｒｕｓｔｅｄ

ｃｏｍｐｕｔｉｎｇ ［ＥＢ?ＯＬ］．２００７．［２０１１－０１－２５］．ｈｔｔｐ：??ｗｗｗ．

ｏｓｃｃａ．ｇｏｖ．ｃｎ?（ｉｎ　Ｃｈｉｎｅｓｅ）

（国家密码管理局．可信密码支撑平台技术规范［ＥＢ?ＯＬ］．

２００７．［２０１１－０１－２５］．ｈｔｔｐ：??ｗｗｗ．ｏｓｃｃａ．ｇｏｖ．ｃｎ?）

［６］ Ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ．ＴＰＭ　ｍａｉｎ　ｓｐｅｃｉｆｉｃａｔｉｏｎ，ｖｅｒｓｉｏｎ

１．２ ［ＥＢ?ＯＬ］． ２００３． ［２０１１－０１－２５］． ｈｔｔｐｓ：??ｗｗｗ．

ｔｒｕｓｔｅｄｃｏｍｐｕｔｉｎｇｇｒｏｕｐ．ｏｒｇ

［７］ Ｍｉｃｒｏｓｏｆｔ．Ｓｅｃｕｒｉｔｙ　ｍｏｄｅｌ　ｆｏｒ　ｔｈｅ　ｎｅｘｔ－ｇｅｎｅｒａｔｉｏｎ　ｓｅｃｕｒｅ

ｃｏｍｐｕｔｉｎｇ　ｂａｓｅ［ＥＢ?ＯＬ］．２００２．［２０１１－０１－２５］．ｈｔｔｐ：??ｗｗｗ．

ｍｉｃｒｏｓｏｆｔ．ｃｏｍ?ｒｅｓｏｕｒｃｅｓ?ｎｇｓｃｂ?ｄｏｃｕｍｅｎｔｓ?ｎｇｓｃｂ＿ｓｅｃｕｒｉｔｙ＿

ｍｏｄｅｌ．ｄｏｃ

［８］ Ｉｎｔｅｌ．Ｔｒｕｓｔｅｄ　ｅｘｅｃｕｔｉｏｎ　ｔｅｃｈｎｏｌｏｇｙ　ａｒｃｈｉｔｅｃｔｕｒｅ　ｏｖｅｒｖｉｅｗ

［ＥＢ?ＯＬ］．２００３．［２０１１－０１－２５］．ｈｔｔｐ：??ｗｗｗ．ｉｎｔｅｌ．ｃｏｍ?

ｔｅｃｈｎｏｌｏｇｙ?ｓｅｃｕｒｉｔｙ?ａｒｃｈ－ｏｖｅｒｖｉｅｗ．ｐｄｆ

［９］ Ｐｅｔｒｏｎｉ　ＮＪｒ，Ｆｒａｓｅｒ　Ｔ，ｅｔ　ａｌ．Ｃｏｐｉｌｏｔ—Ａ　ｃｏｐｒｏｃｅｓｓｏｒ－ｂａｓｅｄ

ｋｅｒｎｅｌ　ｒｕｎｔｉｍｅ　ｉｎｔｅｇｒｉｔｙ　ｍｏｎｉｔｏｒ［Ｃ］??Ｐｒｏｃ　ｏｆ　ｔｈｅ　１３ｔｈ　Ｃｏｎｆ

ｏｎ　ＵＳＥＮＩＸ　Ｓｅｃｕｒｉｔｙ　Ｓｙｍｐｏｓｉｕｍ．Ｂｅｒｋｅｌｅｙ： ＵＳＥＮＩＸ，

２００４：１７９－１９４

［１０］ Ｓｅｓｈａｄｒｉ　Ａ，Ｌｕｋ　Ｍ，Ｓｈｉ　Ｅ，ｅｔ　ａｌ．Ｐｉｏｎｅｅｒ：Ｖｅｒｉｆｙｉｎｇ　ｃｏｄｅ

ｉｎｔｅｇｒｉｔｙ　ａｎｄ　ｅｎｆｏｒｃｉｎｇ　ｕｎｔａｍｐｅｒｅｄ　ｃｏｄｅ　ｅｘｅｃｕｔｉｏｎ　ｏｎ　ｌｅｇａｃｙ

ｓｙｓｔｅｍｓ［Ｃ］??Ｐｒｏｃ　ｏｆ　ｔｈｅ　１２ｔｈ　ＡＣＭ　Ｓｙｍｐ　ｏｎ　Ｏｐｅｒａｔｉｎｇ

Ｓｙｓｔｅｍｓ　Ｐｒｉｎｃｉｐｌｅｓ．Ｎｅｗ　Ｙｏｒｋ：ＡＣＭ，２００５：１－１６

［１１］ Ｓａｉｌｅｒ　Ｒ，Ｚｈａｎｇ　Ｘｉａｏｌａｎ，Ｊａｅｇｅｒ　Ｔ，ｅｔ　ａｌ．Ｄｅｓｉｇｎ　ａｎｄ

ｉｍｐｌｅｍｅｎｔａｔｉｏｎ　ｏｆ　ａ　ＴＣＧ－ｂａｓｅｄ　ｉｎｔｅｇｒｉｔｙ　ｍｅａｓｕｒｅｍｅｎｔ

ａｒｃｈｉｔｅｃｔｕｒｅ［Ｃ］??Ｐｒｏｃ　ｏｆ　ＵＳＥＮＩＸ　Ｓｅｃｕｒｉｔｙ０４．Ｂｅｒｋｅｌｅｙ：

ＵＳＥＮＩＸ，２００４：２２３－２３８

［１２］ Ｊａｅｇｅｒ　Ｔ，Ｓａｉｌｅｒ　Ｒ，Ｓｈａｎｋａｒ　Ｕ．ＰＲＩＭＡ：Ｐｏｌｉｃｙ－ｒｅｄｕｃｅｄ

ｉｎｔｅｇｒｉｔｙ　ｍｅａｓｕｒｅｍｅｎｔ　ａｒｃｈｉｔｅｃｔｕｒｅ ［Ｃ］??Ｐｒｏｃ　ｏｆ　ｔｈｅ　１１ｔｈ

ＡＣＭ　Ｓｙｍｐ　ｏｎ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ｍｏｄｅｌｓ　ａｎｄ　Ｔｅｃｈｎｏｌｏｇｉｅｓ．

Ｎｅｗ　Ｙｏｒｋ：ＡＣＭ，２００６：１９－２８

［１３］ Ｓｈｉ　Ｅ，Ｐｅｒｒｉｇ　Ａ，Ｄｏｏｒｎ　Ｌ　Ｖ．ＢＩＮＤ： Ａ　ｆｉｎｅ－ｇｒａｉｎｅｄ

ａｔｔｅｓｔａｔｉｏｎ　ｓｅｒｖｉｃｅ　ｆｏｒ　ｓｅｃｕｒｅ　ｄｉｓｔｒｉｂｕｔｅｄ　ｓｙｓｔｅｍｓ［Ｃ］??Ｐｒｏｃ

ｏｆ　ｔｈｅ　２００５ＩＥＥＥ　Ｓｙｍｐ　ｏｎ　Ｓｅｃｕｒｉｔｙ　ａｎｄ　Ｐｒｉｖａｃｙ．Ｌｏｓ

Ａｌａｍｉｔｏｓ，ＣＡ：ＩＥＥＥ　Ｃｏｍｐｕｔｅｒ　Ｓｏｃｉｅｔｙ，２００５：１５４－１６８

［１４］ Ｐｅｎｇ　Ｇｕｏｊｕｎ，Ｐａｎ　Ｘｕａｎｃｈｅｎ，Ｚｈａｎｇ　Ｈｕａｎｇｕｏ，ｅｔ　ａｌ．

Ｄｙｎａｍｉｃ　ｔｒｕｓｔｉｎｅｓｓ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｆｒａｍｅｗｏｒｋ　ｂａｓｅｄ　ｏｎ

ｓｏｆｔｗａｒｅ’ｓ　ｂｅｈａｖｉｏｒ　ｉｎｔｅｇｒｉｔｙ［Ｃ］??Ｐｒｏｃ　ｏｆ　ｔｈｅ　９ｔｈ　Ｉｎｔ　Ｃｏｎｆ

\_\_\_\_\_\_\_\_\_\_ｆｏｒ　Ｙｏｕｎｇ　Ｃｏｍｐｕｔｅｒ　Ｓｃｉｅｎｔｉｓｔｓ （ＩＣＹＣＳ　２００８）． Ｌｏｓ

Ａｌａｍｉｔｏｓ，ＣＡ：ＩＥＥＥ　Ｃｏｍｐｕｔｅｒ　Ｓｏｃｉｅｔｙ，２００８：２２８３－２２８８

［１５］ Ｘｕ　Ｚｉｙａｏ，Ｈｅ　Ｙｅｐｉｎｇ，Ｄｅｎｇ　Ｌｉｎｇｌｉ．Ａｎ　ｉｎｔｅｇｒｉｔｙ　ａｓｓｕｒａｎｃｅ

ｍｅｃｈａｎｉｓｍ　ｆｏｒ　ｒｕｎ－ｔｉｍｅ　ｐｒｏｇｒａｍｓ［Ｃ］??Ｐｒｏｃ　ｏｆ　Ｉｎｆｏｒｍａｔｉｏｎ

Ｓｅｃｕｒｉｔｙ　ａｎｄ　Ｃｒｙｐｔｏｌｏｇｙ．Ｂｅｒｌｉｎ：Ｓｐｒｉｎｇｅｒ，２００９：３８９－４０５

［１６］ Ｌｏｓｃｏｃｃｏ　ＰＡ，Ｗｉｌｓｏｎ　ＰＷ，Ｐｅｎｄｅｒｇｒａｓｓ　ＪＡ，ｅｔ　ａｌ．Ｌｉｎｕｘ

ｋｅｒｎｅｌ　ｉｎｔｅｇｒｉｔｙ　ｍｅａｓｕｒｅｍｅｎｔ　ｕｓｉｎｇ　ｃｏｎｔｅｘｔｕａｌ　ｉｎｓｐｅｃｔｉｏｎ

［Ｃ］??Ｐｒｏｃ　ｏｆ　ｔｈｅ　２ｎｄ　ＡＣＭ　Ｗｏｒｋｓｈｏｐ　ｏｎ　Ｓｃａｌａｂｌｅ　Ｔｒｕｓｔｅｄ

Ｃｏｍｐｕｔｉｎｇ．Ｎｅｗ　Ｙｏｒｋ：ＡＣＭ，２００７：２１－２９

［１７］ Ａｚａｂ　ＡＭ， Ｎｉｎｇ　Ｐ，Ｓｅｚｅｒ　ＥＣ，Ｚｈａｎｇ　Ｘ． ＨＩＭＡ： Ａ

ｈｙｐｅｒｖｉｓｏｒ－ｂａｓｅｄ　ｉｎｔｅｇｒｉｔｙ　ｍｅａｓｕｒｅｍｅｎｔ　ａｇｅｎｔ［Ｃ］??Ｐｒｏｃ　ｏｆ

ｔｈｅ　２００９Ａｎｎｕａｌ　Ｃｏｍｐｕｔｅｒ　Ｓｅｃｕｒｉｔｙ　Ａｐｐｌｉｃａｔｉｏｎｓ　Ｃｏｎｆ．Ｌｏｓ

Ａｌａｍｉｔｏｓ，ＣＡ：ＩＥＥＥ　Ｃｏｍｐｕｔｅｒ　Ｓｏｃｉｅｔｙ，２００９：４６１－４７０

［１８］ Ａｚａｂ　ＡＭ，Ｎｉｎｇ　Ｐｅｎｇ，Ｗａｎｇ　Ｚｈｉ，ｅｔ　ａｌ．ＨｙｐｅｒＳｅｎｔｒｙ：

Ｅｎａｂｌｉｎｇ　ｓｔｅａｌｔｈｙ　ｉｎ－ｃｏｎｔｅｘｔ　ｍｅａｓｕｒｅｍｅｎｔ　ｏｆ　ｈｙｐｅｒｖｉｓｏｒ

ｉｎｔｅｇｒｉｔｙ［Ｃ］??Ｐｒｏｃ　ｏｆ　ｔｈｅ　１７ｔｈ　ＡＣＭ　Ｃｏｎｆ　ｏｎ　Ｃｏｍｐｕｔｅｒ　ａｎｄ

Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｓｅｃｕｒｉｔｙ．Ｎｅｗ　Ｙｏｒｋ：ＡＣＭ，２０１０：３８－４９

［１９］ Ｂｅｒｇｅｒ　Ｓ，Ｃáｃｅｒｅｓ　Ｒ， Ｇｏｌｄｍａｎ　Ｋ　Ａ，ｅｔ　ａｌ．ｖＴＰＭ：

Ｖｉｒｔｕａｌｉｚｉｎｇ　ｔｈｅ　ｔｒｕｓｔｅｄ　ｐｌａｔｆｏｒｍ　ｍｏｄｕｌｅ［Ｃ］??Ｐｒｏｃ　ｏｆ　ｔｈｅ

１５ｔｈ　ＵＳＥＮＩＸ　Ｓｅｃｕｒｉｔｙ　Ｓｙｍｐｏｓｉｕｍ．Ｂｅｒｋｅｌｅｙ：ＵＳＥＮＩＸ，

２００６：３０５－３２０

［２０］ Ｓａｄｅｇｈｉ　ＡＲ，Ｓｔüｂｌｅ　Ｃ，Ｗｉｎａｎｄｙ　Ｍ．Ｐｒｏｐｅｒｔｙ－ｂａｓｅｄ　ＴＰＭ

ｖｉｒｔｕａｌｉｚａｔｉｏｎ［Ｃ］??Ｐｒｏｃ　ｏｆ　ｔｈｅ　１１ｔｈ　Ｉｎｔ　Ｃｏｎｆ　ｏｎ　Ｉｎｆｏｒｍａｔｉｏｎ

Ｓｅｃｕｒｉｔｙ．Ｂｅｒｌｉｎ：Ｓｐｒｉｎｇｅｒ，２００８：１－１６

［２１］ Ｃａｍｅｎｉｓｃｈ　Ｊ，Ｌｙｓｙａｎｓｋａｙａ　Ａ．Ａ　ｓｉｇｎａｔｕｒｅ　ｓｃｈｅｍｅ　ｗｉｔｈ

ｅｆｆｉｃｉｅｎｔ　ｐｒｏｔｏｃｏｌｓ［Ｃ］??Ｐｒｏｃ　ｏｆ　３ｒｄ　Ｉｎｔ　Ｃｏｎｆ　Ｓｅｃｕｒｉｔｙ　ｉｎ

Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｎｅｔｗｏｒｋｓ．Ｂｅｒｌｉｎ：Ｓｐｒｉｎｇｅｒ，２００３：２６８－２８９

［２２］ Ｂｒｉｃｋｅｌ　Ｅ， Ｃａｍｅｎｉｓｃｈ　Ｊ，Ｃｈｅｎ　Ｌ． Ｄｉｒｅｃｔ　ａｎｏｎｙｍｏｕｓ

ａｔｔｅｓｔａｔｉｏｎ［Ｃ］??Ｐｒｏｃ　ｏｆ　ｔｈｅ　ＡＣＭ　Ｃｏｎｆ　ｏｎ　Ｃｏｍｐｕｔｅｒ　ａｎｄ

Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｓｅｃｕｒｉｔｙ．Ｎｅｗ　Ｙｏｒｋ：ＡＣＭ，２００４：１３２－１４５

［２３］ Ｈｅ　Ｇｅ，Ｔａｔｅ　ＳＲ．Ａ　ｄｉｒｅｃｔ　ａｎｏｎｙｍｏｕｓ　ａｔｔｅｓｔａｔｉｏｎ　ｓｃｈｅｍｅ　ｆｏｒｅｍｂｅｄｄｅｄ　ｄｅｖｉｃｅｓ［Ｃ］??Ｐｒｏｃ　ｏｆ　Ｐｕｂｌｉｃ　Ｋｅｙ　Ｃｒｙｐｔｏｇｒａｐｈｙ．

Ｂｅｒｌｉｎ：Ｓｐｒｉｎｇｅｒ，２００７：１６－３０

［２４］ Ｃａｍｅｎｉｓｃｈ　Ｊ， Ｌｙｓｙａｎｓｋａｙａ　Ａ． Ｓｉｇｎａｔｕｒｅ　ｓｃｈｅｍｅｓ　ａｎｄ

ａｎｏｎｙｍｏｕｓ　ｃｒｅｄｅｎｔｉａｌｓｆｒｏｍ　ｂｉｌｉｎｅａｒ　ｍａｐｓ ［Ｃ］??Ｐｒｏｃ　ｏｆ

ＣＲＹＰＴＯ　２００４．Ｂｅｒｌｉｎ：Ｓｐｒｉｎｇｅｒ，２００４：５６－７２\_\_

[25]基于区块链的分布式电能量数据可信存储机制.李槿

[26]可信硬件平台的设计和实现 。郭灵儿