(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106997438 B
(45)授权公告日 2019.11.12

(21)申请号 201710196512.3
(22)申请日 2017.03.29
(65)同一申请的已公布的文献号
申请公布号 CN 106997438 A
(43)申请公布日 2017.08.01
(73)专利权人 山东英特力数据技术有限公司
地址 272000 山东省济宁市高新区崇文大道431号英特力工业园
(72)发明人 江涛 卢飞 程归鹏 韩应得
(74)专利代理机构 济宁汇景知识产权代理事务所(普通合伙) 37254
代理人 葛东升
(51)Int.Cl.
G06F 21/57(2013.01)

审查员 郭瑞

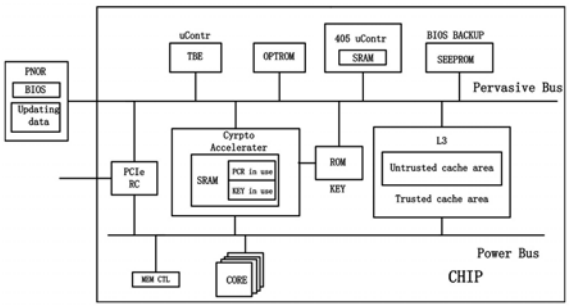
权利要求书2页 说明书5页 附图3页

(54)发明名称

一种可信服务器CPU设计方法

(57)摘要

本发明公开了一种可信服务器CPU设计方法,包括:在CPU内部中设置加解密加速器;在CPU内部中设计Trusted boot engine,用于执行代码,度量BIOS,传递可信链;在CPU内部设计微控制器,用于执行计算,管理和控制外设接口与密码资源;在CPU内部设计多个ROM存储;利用片内加解密加速器、微控制器、PervasiveBus、ROM等资源设计信任根的传递流程与异常处理;本发明在片内设计Trusted compute module功能,不可能使用外部手段获取片内信息,操作系统正常启动之后可信服务器CPU仍然能对计算环境提供可信密码保护,可解决片外方案带来的安全性问题。



CN 106997438 B

1.一种可信服务器CPU设计方法,其特征在于:所述设计方法包括如下步骤:

S1,在CPU内部中设计加解密加速器,用于可信度量和密码加速;

S2,在CPU内部中设计Trusted boot engine,用于执行代码,操作系统上电时初始化及各种加载判断流程、并度量BIOS,传递可信链;

S3,在CPU内部设计微控制器,用于执行计算,管理和控制外设接口与密码资源;

S4,在CPU内部设计多个ROM存储,用于保存可信计算各级度量过程中的密钥、证书及度量值;

S5,利用片内加解密加速器、微控制器、PervasiveBus、ROM资源设计信任根的传递流程与异常处理。

2.根据权利要求1所述的设计方法,其特征在于:所述可信服务器CPU的芯片包括基于PowerBus互连的SoC系统、基于PervasiveBus的带外管理系统。

3.根据权利要求1所述的设计方法,其特征在于:所述可信服务器CPU的内部包括能彻底解决可信根的安全性问题的Trusted compute module结构;所述的Trusted compute module结构属于Pervasive manage system系统,包括Trusted boot engine、微控制器、OTPROM、SEEPROM、加解密加速器、ROM;所述的Trusted boot engine、微控制器、OTPROM、SEEPROM、加解密加速器、ROM分别连接在PervasiveBus上,所述的加解密加速器也同时连接在Power bus上。

4.根据权利要求3所述的设计方法,其特征在于:所述Trusted compute module结构的各组件的协同工作包括:

所述Trusted boot engine负责芯片的初始化,以及将BIOS代码从片外存储器PNOR拷贝到片内L3缓存,并交由加解密加速器对BIOS代码进行完整性验证;所述的片外存储器PNOR存储有包括BIOS代码和需要被更新的加密证书信息;

所述的OTPROM是一个只能写入一次的存储器,存储了Trusted boot engine引擎的执行指令,一旦写入将不可更改;

所述的SEEPROM中存储经过验证的备份BIOS,当PNOR中的BIOS未通过验证时,从SEEPROM中加载保证操作系统可以正常启动,当操作系统更新BIOS时,经过加解密加速器验证后的新BIOS将会被拷贝至SEEPROM中;

所述的加解密加速器除了包含通用加解密算法硬件模块外,主要承担可信链建立过程中的各级验证工作;

所述的ROM与加解密加速器相连,ROM内包含加解密、验证签名需要的相关密钥;

所述的微控制器能进行密钥管理、策略控制和外设控制。

5.根据权利要求1所述的设计方法,其特征在于:所述的操作系统正常启动之后,可信服务器CPU仍然对计算环境提供可信密码保护。

6.根据权利要求1所述的设计方法,其特征在于:所述的可信服务器CPU以可信服务器CPU为可信根,建立可信链的过程步骤如下:

SⅠ,操作系统上电后,触发Trusted boot engine可信启动引擎;

SⅡ,CPU执行BIOS;

SⅢ,BIOS启动,以BIOS为可信根,继续对操作系统OS内核度量,BIOS调用加解密加速器的度量接口,对操作系统内核OS的完整性进行度量;

SⅣ,度量通过,BIOS将引导操作系统OS,并将信任链传递给操作系统OS;

SⅤ,OS启动,以OS为可信根,继续对应用系统Application度量,OS调用加解密加速器的度量接口,对应用系统Application内核的完整性进行度量;

SⅥ,度量通过,OS将引导应用系统Application,完成可信链的建立。

7.根据权利要求6所述的设计方法,其特征在于:所述SI的步骤具体包括以下子步骤:

S11,Trusted boot engine执行OTPROM中的 code,初始化芯片;

S12,Trusted boot engine访问片外的存储器PNOR,把BIOS拷贝到片内的L3缓存的非安全区域;

S13,Trusted boot engine调用加解密加速器引擎度量接口对BIOS进行度量验证;

S14,加解密加速器使用杂凑算法对BIOS进行度量,并与已有的度量值进行比对;

S15,加解密加速器度量完毕,结果反馈给Trusted boot engine;

S16,验证通过则Trusted boot engine执行copy指令把安全BIOS拷贝到L3缓存的安全区域;

S17,验证不通过,则Trusted boot engine执行copy指令把SEEPROM中的经过验证的备份BIOS拷贝到L3缓存的安全区域;

S18,Trusted boot engine把控制权交给CPU。

一种可信服务器CPU设计方法

技术领域：

[0001] 本发明涉及可信服务器设计的技术领域，特别是涉及一种可信服务器CPU设计方法。

背景技术：

[0002] 21世纪是信息的时代，信息技术产业的飞速发展，特别是网络及服务器升级、推广、普及带给人们巨大的利益和便利。当今处于信息化高速发展阶段，世界各地均建立大规模数据中心，应用服务器集群，对于如何保障服务器安全以及数据信息的安全成为至关重要的问题，也面临着各种信息安全遭到危害的事件的严峻考验。目前普遍采用可信计算这种技术手段来解决该类问题。可信计算是指利用物理平台的一种装置作为可信根，可信根作为无条件百分百可信的基础，从主机上电开始，根据设计策略，可信根作为一级启动组件，对下一级启动组件进行度量验证，验证通过，则启动该组件，并以该组件作为可信基础，再对下一级度量验证，这样一级一级的度量验证，一级一级的启动，建立整个计算系统的可信环境。作为可信根的该装置安全性至关重要，一般为一种安全芯片，也称为加密卡TCM(Trusted compute module)或者TPM(Trusted platform module)，也叫作TCM卡加密卡或者TPM加密卡。

[0003] 为此，人们开发研究了可信计算方法平台，如公开号为CN103973668B的中国专利公开了一种网络信息系统中服务器端的个人隐私数据保护方法，本发明公开了一种网络信息系统中服务器端的个人隐私数据保护方法，意在提供一种能支持各类常见文本查询、查询性能高、且安全性好的一种网络信息系统中服务器端的个人隐私数据保护方法。通过在网络信息系统的客户端和服务器端之间铺设一层中间软件，负责实施本发明所提供的技术方法，以完成两项功能：一是将外部用户通过系统客户端输入的个人隐私数据进行加密后，存放到系统服务器端的后台数据库中，从而确保个人隐私信息在不可信服务器端的安全性；二是为个人隐私数据建立合适的索引，以支持精确查询、相似查询、范围查询等常见文本查询，从而确保密文查询的高效性。如公开号为CN101901319A的中国专利公开了一种可信计算平台以及信任链传递验证方法，信任链是可信计算机系统的一个关键组成部分；它的存在保证了计算机系统从可信源头开始至系统启动整个过程的安全可信性；但是现有的信任传递方式为链式传递方式，由于链式传递的信任度逐层衰减的问题，造成了可信计算平台的信任链建立过程存在安全隐患；本发明通过可信平台控制模块TPCM授权CPU对可信计算平台进行链式度量，同时TPCM尾随CPU对信任链进行实时的、随机的、分块的进行度量，并在平台信任链的各部分代码中嵌入检查点，统计并比较运行总时间与预期总时间，以及各块的运行时间和预期时间，从而判断各个信任节点是否被篡改；本发明提高了对信任链建立和检查的实时性，尤其可以防御TOUTOC攻击。如公开号为CN100390701的中国专利公开了一种自举具有冗余可信平台模块的可信服务器的方法和系统，在数据处理系统内的多个可信平台模块以冗余方式被使用，这提供了可靠的机制，用于安全地将用以自举系统可信平台模块的秘密数据存储在休眠状态。管理程序请求每个可信平台模块加密秘密数据的拷

贝，由此产生加密的秘密数据值的多个版本，它们然后被存储在可信平台内的非易失性存储器内。在以后的某个时间点，加密的秘密数据值被取出，被执行先前的加密的可信平台模块解密，然后被彼此比较。如果根据比较操作，有任何解密的值不匹配值的额定数，则将用于不匹配的解密值的相应可信平台模块指定为有缺陷，因为它还不能够正确地解密它先前加密的值。

[0004] 目前，对于可信根的该装置安全芯片TCM在可信服务器CPU设计方面的应用文献比较少。现有普遍采用技术方案有二种：一种如图4所示，采用主板外接加密卡的方案，卡上有安全芯片，加密卡一般利用主板上提供的PCIE接口插槽，接入主板，和主板上CPU协同工作，建立可信计算环境；另一种如图5所示，主板上嵌入TCM卡形式还有一种直接把TCM嵌入到主板上的形式，与CPU通过PCIE总线连接。以上现有技术方案均属于在CPU外部增加安全芯片的方案，属于片外方案，有安全隐患，存在以下不足：1)容易被绕过，这样就保证不了下一级启动组件的安全性；2)容易被恶意用户定位、分析，进而容易被恶意利用、破坏和替换；3)数据传输路径长，容易被监听、篡改。面对这一安全隐患瓶颈，因此有必要提出一种新的可信服务器CPU设计方法解决上述问题。

发明内容：

[0005] 为了要解决的目前技术问题的不足，本发明提供了一种可信服务器CPU设计方法，解决了安全隐患，数据传输不易被监听、篡改，本发明解决其技术问题的技术方案为：一种可信服务器CPU设计方法，该设计方法包括如下步骤：

[0006] S1,在CPU内部中设计加解密加速器，用于可信度量和密码加速；

[0007] S2,在CPU内部中设计TBE，即Trusted boot engine，用于执行代码，操作系统上电时初始化及各种加载判断流程、并度量BIOS，传递可信链；

[0008] S3,在CPU内部设计微控制器，用于执行计算，管理和控制外设接口与密码资源；

[0009] S4,在CPU内部设计多个ROM存储，用于保存可信计算各级度量过程中的密钥、证书及度量值等；

[0010] S5,利用片内加解密加速器、微控制器、PervasiveBus、ROM等资源设计信任根的传递流程与异常处理。

[0011] 所述的可信服务器CPU芯片包括基于PowerBus互连的SoC系统即System on chip、基于PervasiveBus的带外管理系统。

[0012] 所述的可信服务器CPU内部包括能彻底解决可信根的安全性问题的TCM结构；所述的TCM结构属于PMS系统，即Pervasive manage system，包括TBE、微控制器、OTPROM、SEEPROM、加解密加速器、ROM；所述的TBE、微控制器、OTPROM、SEEPROM、加解密加速器、ROM连接在PervasiveBus上，同时所述的加解密加速器也连接在Power bus上。

[0013] 所述TCM结构的各组件的协同工作包括：所述TBE负责芯片的初始化，以及将BIOS代码从片外存储器PNOR拷贝到片内L3缓存，并交由加解密加速器对BIOS代码进行完整性验证；所述的OTPROM是一个只能写入一次的存储器，存储了TBE引擎的执行指令，一旦写入将不可更改；所述的片外存储器PNOR存储了包括BIOS代码和需要被更新的加密证书等信息；所述的SEEPROM中存储经过验证的备份BIOS，当PNOR中的BIOS未通过验证时，从SEEPROM中加载保证操作系统可以正常启动，当操作系统更新BIOS时，经过加解密加速器验证后的新

BIOS将会被拷贝至SEEPROM中;所述的加解密加速器除了包含通用加解密算法硬件模块外,主要承担可信链建立过程中的各级验证工作;所述的ROM与加解密加速器相连,ROM内包含加解密、验证签名需要的相关密钥;所述的微控制器能进行密钥管理、策略控制和外设控制。

[0014] 所述的操作系统正常启动之后,可信服务器CPU仍然对计算环境提供可信密码保护。

[0015] 所述的可信服务器CPU以可信服务器CPU为可信根,建立可信链的过程步骤如下:

[0016] SⅠ,操作系统上电后,触发TBE可信启动引擎;

[0017] SⅡ,CPU执行BIOS;

[0018] SⅢ,BIOS启动,以BIOS为可信根,继续对操作系统OS内核度量,BIOS调用加解密加速器的度量接口,对操作系统内核OS的完整性进行度量;

[0019] SⅣ,度量通过,BIOS将引导操作系统OS,并将信任链传递给操作系统OS;

[0020] SⅤ,OS启动,以OS为可信根,继续对应用系统Application度量,OS调用加解密加速器的度量接口,对应用系统Application内核的完整性进行度量;

[0021] SⅥ,度量通过,OS将引导应用系统Application,完成可信链的建立。

[0022] 所述的可信服务器CPU以可信服务器CPU为可信根,建立可信链的过程步骤中所述的步骤SI具体包括以下子步骤:

[0023] S11,TBE执行OTPROM中的code,初始化芯片;

[0024] S12,TBE访问片外的存储器PNOR,把BIOS拷贝到片内的L3缓存的非安全区域;

[0025] S13,TBE调用加解密加速器引擎度量接口对BIOS进行度量验证;

[0026] S14,加解密加速器使用杂凑算法对BIOS进行度量,并与已有的度量值进行比对;

[0027] S15,加解密加速器度量完毕,结果反馈给TBE;

[0028] S16,验证通过则TBE执行copy指令把安全BIOS拷贝到L3缓存的安全区域;

[0029] S17,验证不通过,则TBE执行copy指令把SEEPROM中的经过验证的备份BIOS拷贝到L3缓存的安全区域;

[0030] S18,TBE把控制权交给CPU。

[0031] 与现有技术相比,本发明的有益效果体现在:本发明所述一种可信服务器CPU设计方法,包括如下步骤:在CPU内部中设计加解密加速器,用于可信度量和密码加速;在CPU内部中设计TBE,用于执行代码,系统上电时初始化及各种加载判断流程、并度量BIOS,传递可信链;在CPU内部设计微控制器,用于执行计算,管理和控制外设接口与密码资源;在CPU内部设计多个ROM存储,用于保存可信计算各级度量过程中的密钥、证书及度量值等;利用片内加解密加速器、微控制器、PervasiveBus、ROM等资源设计信任根的传递流程与异常处理;可信服务器CPU芯片包括基于PowerBus互连的SoC系统、基于PervasiveBus的带外管理系统;可信服务器CPU内部包括能彻底解决可信根的安全性问题的TCM结构,包括TBE、微控制器、OTPROM、SEEPROM、加解密加速器、ROM;所述系统正常启动之后,可信服务器CPU仍然对计算环境提供可信密码保护;本发明的技术方案在片内设计TCM功能,不可能使用外部手段获取片内信息,做到彻底的安全,可解决片外方案带来的安全性问题。

附图说明

[0032] 图1为本发明的可信服务器CPU架构图。

[0033] 图2为本发明的CPU内部设计TCM结构图。

[0034] 图3为本发明以可信服务器CPU为可信根的建立可信链过程图。

[0035] 图4为现有技术方案的主板外接TCM结构图。

[0036] 图5为现有技术方案的主板内嵌TCM结构图。

具体实施方式

[0037] 结合附图1至图3对本发明进一步详细描述,以便公众更好地掌握本发明的实施方法,本发明具体的实施方案为:

[0038] 如图1、图2所示,本发明所述的一种可信服务器CPU设计方法,该设计方法包括如下步骤:

[0039] S1,在CPU内部中设计加解密加速器,用于可信度量和密码加速;

[0040] S2,在CPU内部中设计TBE,用于执行代码,操作系统上电时初始化及各种加载判断流程、并度量BIOS,传递可信链;

[0041] S3,在CPU内部设计微控制器,用于执行计算,管理和控制外设接口与密码资源;

[0042] S4,在CPU内部设计多个ROM存储,用于保存可信计算各级度量过程中的密钥、证书及度量值等;

[0043] S5,利用片内加解密加速器、微控制器、PervasiveBus、ROM等资源设计信任根的传递流程与异常处理。

[0044] 优选的,可信服务器CPU芯片包括基于PowerBus互连的SoC系统、基于PervasiveBus的带外管理系统。

[0045] 优选的,可信服务器CPU内部包括能彻底解决可信根的安全性问题的TCM结构;所述的TCM结构属于PMS系统,包括TBE即启动引擎、PPC405微控制器即405uContr、OTPROM、SEEPROM、加解密加速器即Crypto Accelerator、ROM;所述的TBE、PPC405微控制器、OTPROM、SEEPROM、加解密加速器、ROM连接在PervasiveBus上,同时所述的加解密加速器也连接在Power bus上。

[0046] 所述TCM结构的各组件的协同工作包括:

[0047] 所述TBE负责芯片的初始化,以及将BIOS代码从片外存储器PNOR拷贝到片内L3缓存,并交由加解密加速器对BIOS代码进行完整性验证;

[0048] 所述的OTPROM是一个只能写入一次的存储器,存储了TBE引擎的执行指令,一旦写入将不可更改;

[0049] 所述的片外存储器PNOR存储了包括BIOS代码和需要被更新的加密证书等信息;

[0050] 所述的SEEPROM中存储经过验证的备份BIOS,当PNOR中的BIOS未通过验证时,从SEEPROM中加载保证操作系统可以正常启动,当操作系统更新BIOS时,经过加解密加速器验证后的新BIOS将会被拷贝至SEEPROM中;

[0051] 所述的加解密加速器除了包含通用加解密算法硬件模块外,主要承担可信链建立过程中的各级验证工作;

[0052] 所述的ROM与加解密加速器相连,ROM内包含加解密、验证签名需要的相关密钥;

[0053] 所述的PPC405微控制器主要负责密钥管理、策略控制和外设控制。

[0054] 所述的系统正常启动之后，可信服务器CPU仍然对计算环境提供可信密码保护。

[0055] 实施例1

[0056] 如图3所示，作为优选最佳实施方式，所述的可信服务器CPU以可信服务器CPU为可信根，建立可信链的过程步骤如下：

[0057] SⅠ，操作系统上电后，触发TBE可信启动引擎；

[0058] SⅡ，CPU执行BIOS；

[0059] SⅢ，BIOS启动，以BIOS为可信根，继续对操作系统OS内核度量，BIOS调用加解密加速器的度量接口，对操作系统内核OS的完整性进行度量；

[0060] SⅣ，度量通过，BIOS将引导操作系统OS，并将信任链传递给操作系统OS；

[0061] SⅤ，OS启动，以OS为可信根，继续对应用系统Application度量，OS调用加解密加速器的度量接口，对应用系统Application内核的完整性进行度量；

[0062] SⅥ，度量通过，OS将引导应用系统Application，完成可信链的建立。

[0063] 如图3所示，作为优选最佳实施方式，所述的步骤SI具体包括以下子步骤：

[0064] S11，TBE执行OTPROM中的code，初始化芯片；

[0065] S12，TBE访问片外的存储器PNOR，把BIOS拷贝到片内的L3缓存的非安全区域；

[0066] S13，TBE调用加解密加速器引擎度量接口对BIOS进行度量验证；

[0067] S14，加解密加速器使用杂凑算法对BIOS进行度量，并与已有的度量值进行比对；

[0068] S15，加解密加速器度量完毕，结果反馈给TBE；

[0069] S16，验证通过则TBE执行copy指令把安全BIOS拷贝到L3缓存的安全区域；

[0070] S17，验证不通过，则TBE执行copy指令把SEEPROM中的经过验证的备份BIOS拷贝到L3缓存的安全区域；

[0071] S18，TBE把控制权交给CPU。

[0072] 与现有技术相比，本发明的有益效果体现在：本发明所述一种可信服务器CPU设计方法，包括如下步骤：在CPU内部中设计加解密加速器，用于可信度量和密码加速；在CPU内部中设计TBE，用于执行代码，系统上电时初始化及各种加载判断流程、并度量BIOS，传递可信链；在CPU内部设计微控制器，用于执行计算，管理和控制外设接口与密码资源；在CPU内部设计多个ROM存储，用于保存可信计算各级度量过程中的密钥、证书及度量值等；利用片内加解密加速器、微控制器、PervasiveBus、ROM等资源设计信任根的传递流程与异常处理；可信服务器CPU芯片包括基于PowerBus互连的SoC系统、基于PervasiveBus的带外管理系统；可信服务器CPU内部包括能彻底解决可信根的安全性问题的TCM结构，包括TBE、微控制器、OTPROM、SEEPROM、加解密加速器、ROM；所述系统正常启动之后，可信服务器CPU仍然对计算环境提供可信密码保护；本发明的技术方案在片内设计TCM功能，不可能使用外部手段获取片内信息，做到彻底的安全，可解决片外方案带来的安全性问题。

[0073] 以上所述仅为本发明的较佳实施例而已，但本发明的保护范围并不限制于本发明的具体实施方式，凡在本发明的精神和原则、揭露技术范围之内，所作的任何修改、等同替换、改进、改型等，均应包含在本发明的保护范围之内。

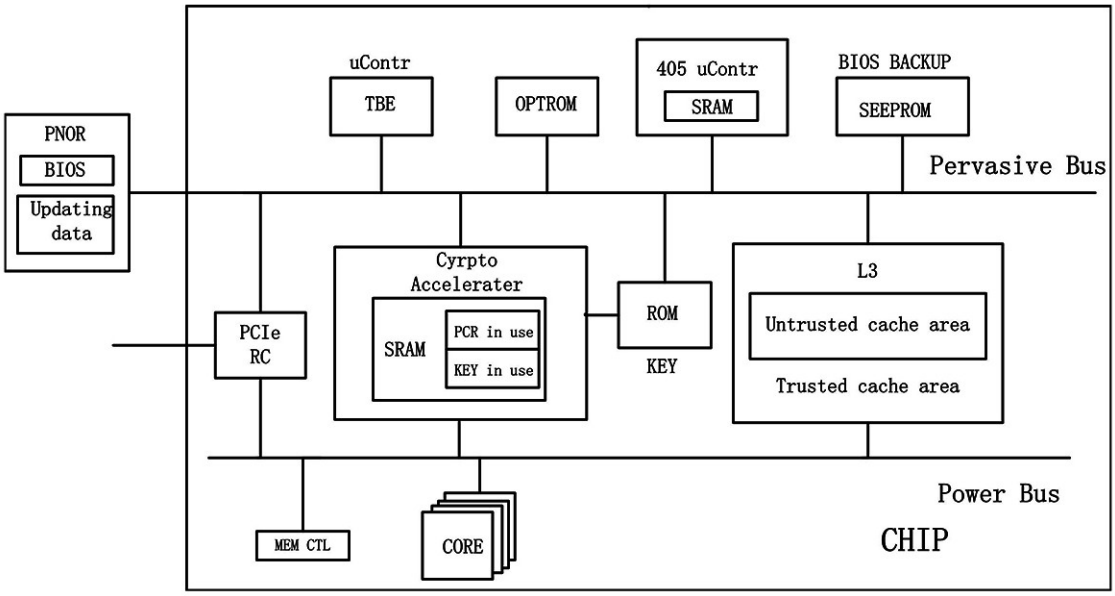

uContr
TBE
OPTROM
405 uContr
SRAM
BIOS BACKUP
SEEPROM
PNOR
BIOS
Updating data
Pervasive Bus
Cyrpto Accelerater
SRAM
PCR in use
KEY in use
ROM
KEY
L3
Untrusted cache area
Trusted cache area
PCIe RC
Power Bus
MEM CTL
CORE
CHIP

图1

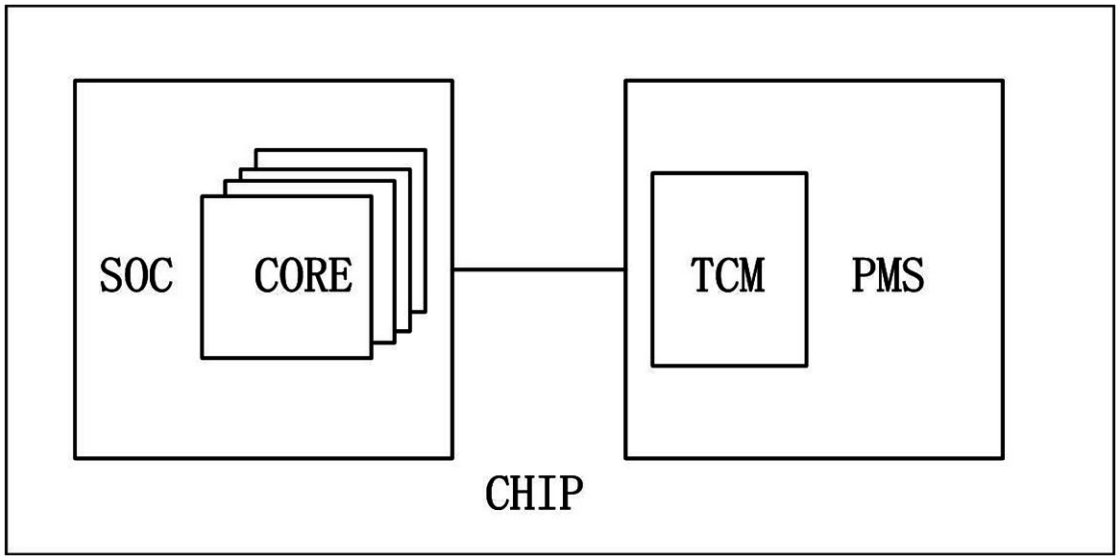

SOC
CORE
TCM
PMS
CHIP

图2

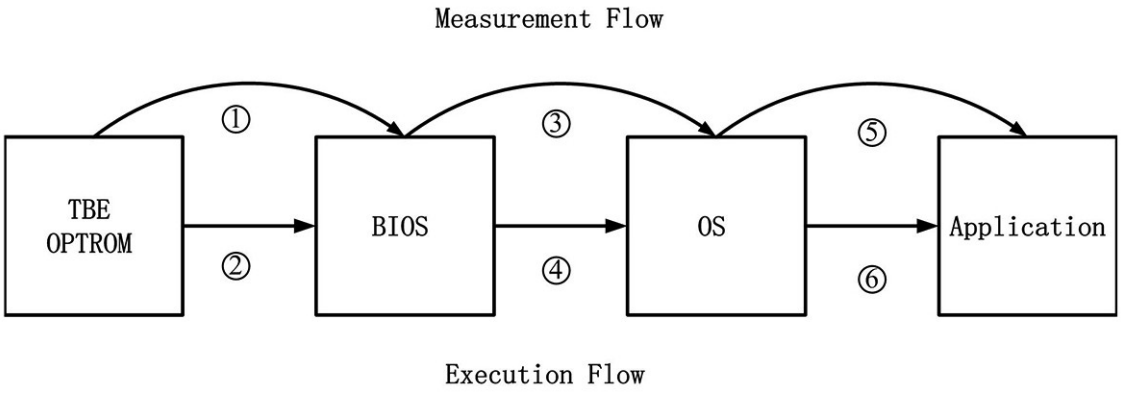

Measurement Flow
①
②
③
④
⑤
⑥
TBE
OPTROM
BIOS
OS
Application
Execution Flow

图3

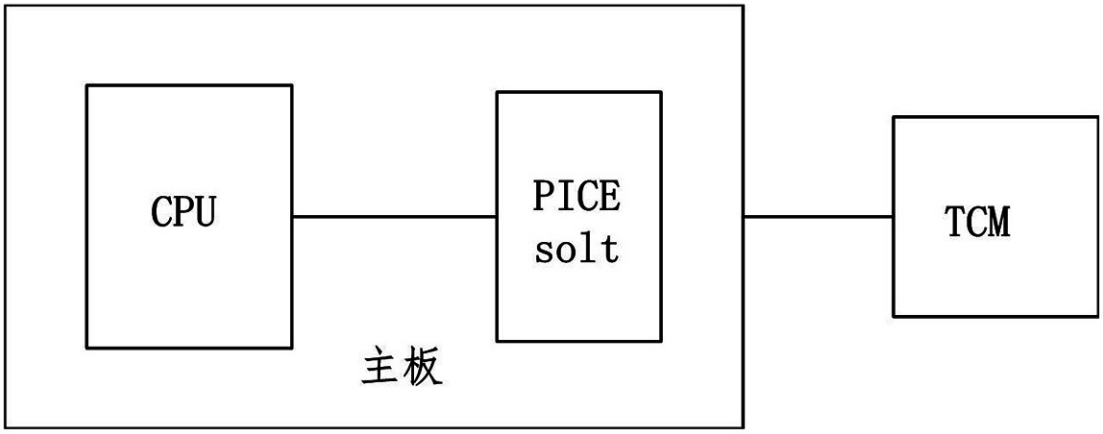

CPU
PICE
solt
TCM
主板

图4

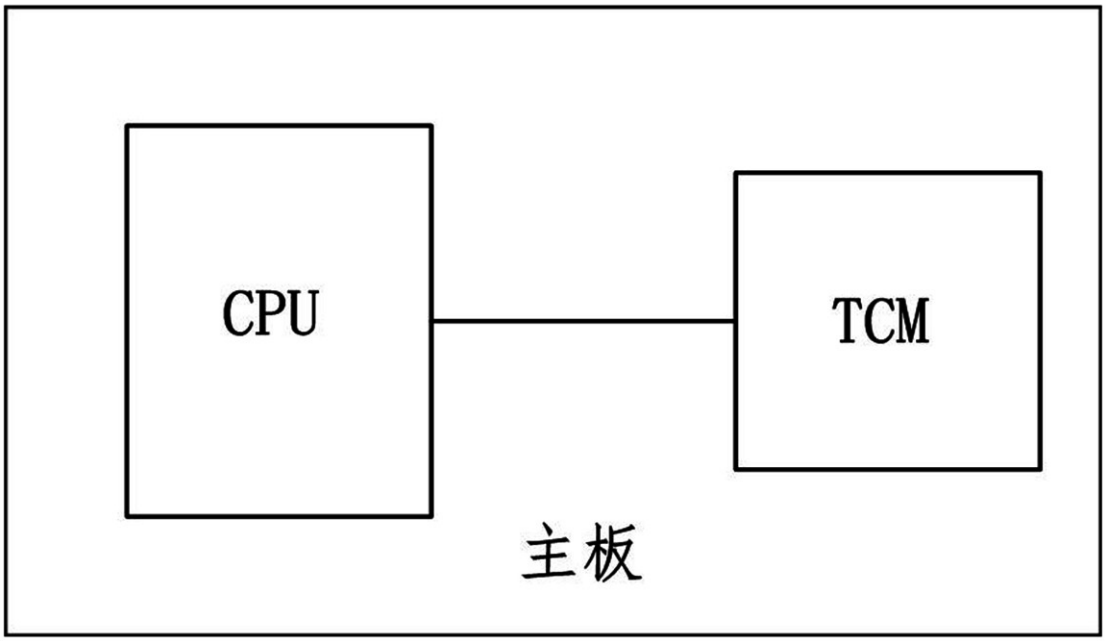


图5