(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111382445 B
(45)授权公告日 2023.04.07

(21)申请号 202010140483.0

(22)申请日 2020.03.03

(65)同一申请的已公布的文献号
申请公布号 CN 111382445 A

(43)申请公布日 2020.07.07

(73)专利权人 首都师范大学
地址 100048 北京市海淀区西三环北路105号

(72)发明人 张倩颖 冀东旭 施智平 关永 李晓娟 王瑞 王国辉 邵振洲

(74)专利代理机构 北京智信四方知识产权代理有限公司 11519
专利代理师 钟文芳 宋海龙

(51)Int.Cl.
G06F 21/57(2013.01)
G06F 21/60(2013.01)
G06F 21/74(2013.01)

(56)对比文件
US 2015199507 A1,2015.07.16
US 2016254904 A1,2016.09.01
CN 107682159 A,2018.02.09
CN 108595950 A,2018.09.28
CN 109522754 A,2019.03.26
CN 110011801 A,2019.07.12
US 2019340393 A1,2019.11.07
郑显义 等;.系统安全隔离技术研究综述.计算机学报.2016,40(05),第1057-1079页.
石元兵;.基于可信计算的可信应用研究.信息安全与通信保密.2010,(12),第92-94页.

审查员 余佳佳

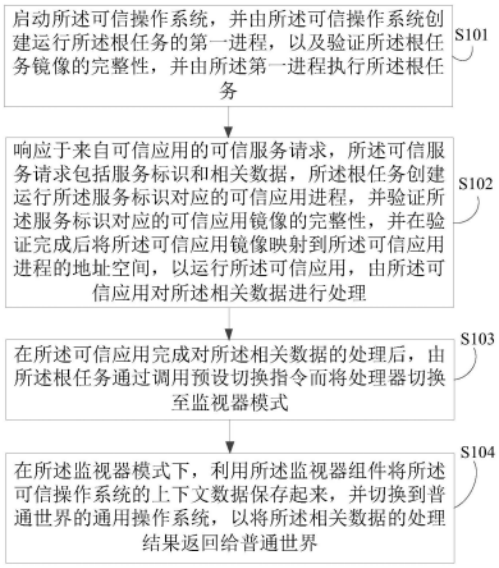
权利要求书2页 说明书10页 附图3页

(54)发明名称

利用可信执行环境系统提供可信服务的方法

(57)摘要

本公开实施例公开了一种利用基于微内核架构的可信执行环境系统提供可信服务的方法，该方法包括：启动可信操作系统，由可信操作系统创建运行根任务的第一进程，以及验证根任务镜像的完整性，由第一进程执行根任务；响应于来自普通世界的服务请求，根任务创建运行服务标识对应的可信应用进程，并验证服务标识对应的可信应用镜像的完整性，并在验证完成后基于可信应用镜像创建可信应用进程；在可信应用完成对相关数据的处理后，由根任务通过调用预设切换指令而将处理器切换至监视器模式；在监视器模式下，利用监视器组件将可信操作系统的上下文数据保存起来，并切换到普通世界的通用操作系统。



CN 111382445 B

1.一种利用基于微内核架构的可信执行环境系统提供可信服务的方法,其特征在于,所述可信执行环境系统中运行有可信操作系统、可信服务组件、监视器组件以及根任务,所述可信操作系统基于微内核构建,并由微内核提供核心服务;所述可信服务组件用于提供可信计算服务,所述可信计算服务包括:完整性度量与验证、数据封装/解封装、远程证明;所述监视器组件用于负责安全世界和普通世界之间的切换;根任务为在所述可信执行环境系统的用户层第一个运行的应用程序,用于接管可信执行环境系统中未用资源、并负责创建和管理其他应用程序;所述方法包括:

启动所述可信操作系统,并由所述可信操作系统创建运行所述根任务的第一进程,以及验证所述根任务镜像的完整性,并由所述第一进程执行所述根任务;

响应于来自普通世界的服务请求,所述服务请求包括服务标识和相关数据,所述根任务创建运行所述服务标识对应的可信应用进程,并验证所述服务标识对应的可信应用镜像的完整性,并在验证完成后基于所述可信应用镜像映射到新建可信应用进程的地址空间,以运行所述可信应用,由所述可信应用对所述相关数据进行处理;

在所述可信应用完成对所述相关数据的处理后,由所述根任务通过调用预设切换指令而将处理器切换至监视器模式;

在所述监视器模式下,利用所述监视器组件将所述可信操作系统的上下文数据保存起来,并切换到普通世界的通用操作系统,以将所述相关数据的处理结果返回给普通世界;

其中,所述根任务创建运行所述服务标识对应的可信应用进程,并验证所述服务标识对应的可信应用镜像的完整性,并在验证完成后将所述可信应用镜像映射到新建可信应用进程的地址空间,以运行所述可信应用,包括:

运行可信应用时,所述根任务创建所述可信应用进程并配置相关信息;

利用所述根任务验证可信应用镜像文件的数字签名证书;所述数字签名证书由应用开发者附在可信应用镜像末端,包含可信应用镜像的标准完整性值;其中,可信应用的完整性值可以用密码学中的单向哈希算法计算得到;

利用所述根任务计算可信应用镜像的完整性值并与数字证书中的标准值进行对比,若完整性值对比一致,则将镜像文件映射到新建可信应用进程的地址空间中;否则可信应用进程创建失败,并返回错误值;

所述方法还包括:

响应于所述可信应用发送的封装请求,利用所述根任务将代表所述可信应用身份的完整性值以及待封装数据发送给可信服务组件,所述封装请求中包括所述待封装数据;

利用所述可信服务组件根据所述完整性值和设备的根对称加密密钥派生出封装密钥,然后使用所述封装密钥对所述待封装数据进行加密,并将封装结果返回给所述根任务;

响应于所述可信应用发送的解封请求,利用所述根任务将待解封的封装结果和可信应用的完整性值发送给所述可信服务组件;

利用所述可信服务组件进行密钥派生和解密操作并将解封结果返回给所述根任务,并利用所述根任务将解封后的原始数据返回给所述可信应用;

所述方法还包括:

响应于远程可信实体作为验证者而发送的验证请求,所述验证请求中包含待验证的服务标识和随机数;利用所述根任务将对应于所述服务标识的所述可信应用的完整性值和随

机数发送给可信服务组件;并利用所述可信服务组件使用证明密钥对所述完整性值和随机数进行签名,并把签名结果返回给所述根任务;

利用所述根任务将签名结果返回给所述验证者,以便由所述验证者根据所述签名结果决定所述服务标识对应的所述可信应用的当前状态是否可信。

2.根据权利要求1所述的方法,其特征在于,还包括:

获取运行可信执行环境系统的设备提供的根对称加密密钥和设备根密钥;并利用所述对称加密密钥和设备根密钥对数据进行保护,设备根密钥为设备厂商颁发的非对称密钥,代表所述设备的身份。

3.根据权利要求1或2所述的方法,其特征在于,所述可信操作系统基于微内核构建,利用微内核提供的隔离机制为上层可信应用提供隔离保证;所述可信操作系统提供实现可信应用的创建、管理以及销毁的接口服务,用于对可信应用实现全生命周期管理;所述可信应用之间的消息传递通过调用微内核提供的进程间通信接口实现;所述可信操作系统提供中断处理功能,包括中断在内核中注册以及中断触发后发送通知信号到对应的中断处理程序进行处理。

4.根据权利要求1或2所述的方法,其特征在于,所述监视器组件用于负责普通世界和安全世界的上下文切换:当普通世界或者安全世界调用预设切换指令时,触发处理器切换到监视器模式,在监视器模式下,监视器根据所述监视器模式下的向量基地址寄存器中存储的异常向量表跳转到对应的预设异常处理程序执行,所述预设异常处理程序对当前世界的处理器上下文进行保存,然后加载另外一个世界的处理器上下文。

5.根据权利要求1或2所述的方法,其特征在于,所述根任务为微内核创建的第一个用户层应用程序;所述根任务的镜像的完整性在启动前由微内核负责检查验证;所述微内核启动后将所有系统未用资源交由根任务管理;所述根任务拥有最高优先级,并负责创建和管理其他应用;当接收到来自普通世界的服务请求时,所述根任务根据服务请求中的服务ID将服务请求数据转发到对应的可信应用进行处理;当可信应用处理完成后,由所述根任务通过调用预设切换指令将处理结果返回给普通世界。

6.根据权利要求1或2所述的方法,其特征在于,所述可信执行环境系统中还运行有可信服务组件;所述可信服务组件为根任务创建的一个服务组件,所述可信服务组件是唯一与存储根对称加密密钥和设备根密钥进行交互的可信应用;可信计算服务由可信服务组件完成,以保证可信计算服务所需要的机密信息不会离开可信服务组件。

7.根据权利要求1所述的方法,其特征在于,所述证明密钥为由设备产生并通过厂商的签名密钥签发的非对称密钥。

利用可信执行环境系统提供可信服务的方法

技术领域

[0001] 本公开涉及计算机技术技术领域,具体涉及一种利用基于微内核架构的可信执行环境系统提供可信服务的方法。

背景技术

[0002] 随机计算机技术的快速发展和网络技术的日新月异,移动设备已经应用到社会的各个领域中,如智能家居、消费电子、网络设备和医疗仪器等。移动设备中处理的数据越来越重要,因此成为了被攻击的目标。如今移动设备在网上支付,电子银行等方面的应用飞速发展,一旦用户数据被泄露或用户设备被攻击者利用,将直接造成用户的财产损失。因此,移动设备安全的重要性不言而喻。针对上述情况Global Platform(GP)提出了可信执行环境(Trusted Execution Environment,TEE)的概念,TEE用来进行数字版权管理、移动支付和敏感数据保护。TEE是与设备上运行Android,Linux等操作系统(Operation System,OS)的通用执行环境(Rich ExecutionEnvironment,REE)并存的,并且为REE提供安全服务。

[0003] ARM TrustZone技术作为TEE的一种具体方案,将系统隔离为两个世界。它将TEE和REE分别称为安全世界(Secure World)和普通世界(NormalWorld)。对于安全性要求较高的操作,如指纹对比,私钥签名等,需要在安全世界完成。可信应用(Trusted Application,TA)是运行在安全世界中的应用。在TrustZone中,安全世界的软硬件资源是与普通世界隔离的,并且安全世界可以访问两个世界的资源,而普通世界只能访问自己的资源。TrustZone如今广泛用于各个主流设备供应商的产品中,如华为,三星等。

[0004] 自ARM TrustZone技术提出以来,很多学者和研究机构专注于基于TrustZone的可信执行环境的实现方案,目前已经有多个开源项目和方案可供研究。

[0005] OP-TEE是由Linaro开发的一个开源TEE项目,主要由三个组件构成:普通世界用户层客户端(optee_client),Linux内核TEE驱动程序(optee_linuxdriver)以及安全世界的TEE OS(optee_os)。Optee_client是运行在普通世界用户空间的客户端API。该API允许用户使用标准API调用可信应用程序。Optee_linuxdriver是用于控制普通世界用户空间和安全世界通信的设备驱动。Optee_os是运行在安全世界的可信操作系统。

[0006] ANDIX OS是格兰茨技术大学的Andreas等人基于TrustZone技术开发的一款TEE OS,它是一款支持多任务、非抢占式的操作系统。ANDIX OS利用TrustZone实现了安全任务与REE OS之间的隔离。ANDIX OS的整体架构与OP-TEE类似,区别在与安全世界中的核心组件是ANDIX安全内核。ANDIX内核是一个宏内核,提供进程隔离,调度和通信等功能。

[0007] Open-TEE是赫尔辛基大学设计实现的独立于硬件的TEE。Open-TEE被设计作为用户层的守护进程。它从执行Base开始,Base是一个将TEE功能封装为一个整体的进程。Base完成初始化后,它将创建两个独立但相关的进程,Manager和Launcher。Manager负责可信应用程序之间的通信并监视其状态,并提供安全存储和控制共享内存等类似于OS的功能。Launcher的唯一目的是使TA的创建更有效率。

[0008] 除此之外还有高通的QSEE以及华为的TrustedCore等商用TEE系统。

[0009] 上述方案中的TEE OS大部分采用的是宏内核架构，普遍缺乏对特权的隔离。内核服务都以特权模式在内核的地址空间中运行。各个软件组件具有高度紧密性，服务之间可以直接通过函数调用。倘若某个组件存在漏洞，可能会导致整个系统的崩溃。因此与TEE和TA相关的漏洞也不断在被发现，例如VE-2016-0825,CVE-2017-0518/0519,CVE-2016-2431/2432,CVE-2015-6639/6647以及CVE-2016-8762/8763/8764。而在Open-TEE中，它不是一个真正的OS，并不能提供完整OS的功能。此外，在OP-TEE中，安全世界执行TA前会对其完整性进行验证，但未提及关于数据封装和远程证明的服务；在ANDIX和Open-TEE中均未提及可信计算相关的功能。而上述缺点直接影响到TEE系统的安全性。

发明内容

[0010] 本公开实施例提供一种利用基于微内核架构的可信执行环境系统提供可信服务的方法，所述可信执行环境系统中运行有可信操作系统、可信服务组件、监视器组件以及根任务，所述可信操作系统基于微内核构建，并由微内核提供核心服务；所述可信服务组件用于提供可信计算服务；所述监视器组件用于负责安全世界和普通世界之间的切换；根任务为在所述可信执行环境系统的用户层第一个运行的应用程序，用于接管可信执行环境系统中未用资源、并负责创建和管理其他应用程序；所述方法包括：

[0011] 启动所述可信操作系统，并由所述可信操作系统创建运行所述根任务的第一进程，以及验证所述根任务镜像的完整性，并由所述第一进程执行所述根任务；

[0012] 响应于来自普通世界的服务请求，所述服务请求包括服务标识和相关数据，所述根任务创建运行所述服务标识对应的可信应用进程，并验证所述服务标识对应的可信应用镜像的完整性，并在验证完成后将所述可信应用镜像映射到新建可信应用进程的地址空间，以运行所述可信应用，由所述可信应用对所述相关数据进行处理；

[0013] 在所述可信应用完成对所述相关数据的处理后，由所述根任务通过调用预设切换指令而将处理器切换至监视器模式；

[0014] 在所述监视器模式下，利用所述监视器组件将所述可信操作系统的上下文数据保存起来，并切换到普通世界的通用操作系统，以将所述相关数据的处理结果返回给普通世界。

[0015] 进一步地，还包括：

[0016] 获取运行可信执行环境系统的设备提供的根对称加密密钥和设备根密钥；并利用所述对称加密密钥和设备根密钥对数据进行保护，设备根密钥为设备厂商颁发的非对称密钥，代表所述设备的身份。

[0017] 进一步地，所述可信操作系统基于微内核构建，利用微内核提供的隔离机制为上层可信应用提供隔离保证；所述可信操作系统提供实现可信应用的创建、管理以及销毁的接口服务，用于对可信应用实现全生命周期管理；所述可信应用之间的消息传递通过调用微内核提供的进程间通信接口实现；所述可信操作系统提供中断处理功能，包括中断在内核中注册以及中断触发后发送通知信号到对应的中断处理程序进行处理。

[0018] 进一步地，所述监视器组件用于负责普通世界和安全世界的上下文切换：当普通世界或者安全世界调用预设切换指令时，触发处理器切换到监视器模式，在监视器模式下，监视器根据所述监视器模式下的向量基地址寄存器中存储的异常向量表跳转到对应的预

设异常处理程序执行，所述预设异常处理程序对当前世界的处理器上下文进行保存，然后加载另外一个世界的处理器上下文。

[0019] 进一步地，所述根任务为微内核创建的第一个用户层应用程序；所述根任务的镜像的完整性在启动前由微内核负责检查验证；所述微内核启动后将所有系统未用资源交由根任务管理；所述根任务拥有最高优先级，并负责创建和管理其他应用；当接收到来自普通世界的服务请求时，所述根任务根据请求中的服务ID将服务请求数据转发到对应的可信应用进行处理；当可信应用处理完成后，由所述根任务通过调用预设切换指令将处理结果返回给普通世界。

[0020] 进一步地，所述可信执行环境系统中还运行有可信服务组件；所述可信服务组件为根任务创建的一个服务组件，所述可信服务组件是唯一与存储根对称加密密钥和设备根密钥进行交互的可信应用可信计算服务由可信服务组件完成，以保证可信计算服务所需要的机密信息不会离开可信服务组件。

[0021] 进一步地，所述根任务创建运行所述服务标识对应的可信应用进程，并验证所述服务标识对应的可信应用镜像的完整性，并在验证完成后将所述可信应用镜像映射到所述可信应用进程的地址空间，以运行所述可信应用，包括：

[0022] 运行可信应用时，利用所述根任务创建所述可信应用进程并配置相关信息；

[0023] 利用所述根任务验证可信应用镜像文件的数字签名证书；所述数字签名证书由应用开发者附在可信应用镜像末端，包含可信应用镜像的标准完整性值；其中，可信应用的完整性值可以用密码学中的单向哈希算法计算得到；

[0024] 利用所述根任务计算可信应用镜像的完整性值并与数字证书中的标准值进行对比，若完整性值对比一致，则将镜像文件映射到进程的地址空间中；否则进程创建失败，并返回错误值。

[0025] 进一步地，所述方法还包括：

[0026] 响应于所述可信应用发送的封装请求，利用所述根任务将代表所述可信应用身份的完整性值以及待封装数据发送给可信服务组件，所述封装请求中包括所述待封装数据；

[0027] 利用所述可信服务组件根据所述完整性值和设备的根对称加密密钥派生出封装密钥，然后使用所述封装密钥对所述待封装数据进行加密，并将封装结果返回给所述根任务；

[0028] 响应于所述可信应用发送的解封请求，利用所述根任务将待解封的封装结果和可信应用的完整性值发送给所述可信服务组件；

[0029] 利用所述可信服务组件进行密钥派生和解密操作并将解封结果返回给所述根任务，并利用所述根任务将解封后的原始数据返回给所述可信应用。

[0030] 进一步地，所述方法还包括：

[0031] 响应于远程可信实体作为验证者而发送的验证请求，所述验证请求中包含待验证的服务标识和随机数；利用所述根任务将对应于所述服务标识的所述可信应用的完整性值和随机数发送给可信服务组件；并利用所述可信服务组件使用证明密钥对所述完整性值和随机数进行签名，并把签名结果返回给所述根任务；

[0032] 利用所述根任务将签名结果返回给所述验证者，以便由所述验证者根据所述签名结果决定所述服务标识对应的所述可信应用的当前状态是否可信。

[0033] 第二方面，本公开实施例提供了一种电子设备，包括存储器和处理器；其中，所述存储器用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令被所述处理器执行以实现上述任一方面所述的方法。

[0034] 第三方面，本公开实施例提供了一种计算机可读存储介质，用于存储实现上述方法所用的计算机指令，其包含用于执行上述任一方面所述方法所涉及的计算机指令。

[0035] 本公开实施例提供的技术方案可以包括以下有益效果：

[0036] 1、本公开优点一在于基于微内核架构构建TEE系统。本公开利用微内核提供的隔离机制为上层可信应用提供隔离，从而使得TEE OS的组件之间，以及可信应用之间都被安全隔离，因此即使某一组件出现问题也不会而导致整个系统崩溃，即使某个组件被攻击者利用也不会影响其他组件的安全性。

[0037] 2、本公开优点二在于为上述TEE系统的用户层提供了可信计算服务。本公开在用户层添加了完整性度量和验证、数据封装/解封装和远程证明等核心可信计算功能。完整性度量和验证在可信应用执行前对其镜像进行检查，确保镜像身份的合法性和完整性；数据封装将敏感数据绑定到特定可信应用，从而保证数据的机密性；远程证明可以向远程可信实体证明特定应用的运行状态。本公开提供的核心可信计算功能可以进一步提高系统的安全性。

[0038] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

[0039] 结合附图，通过以下非限制性实施方式的详细描述，本公开的其它特征、目的和优点将变得更加明显。在附图中：

[0040] 图1示出根据本公开一实施方式的利用基于微内核架构的可信执行环境系统提供可信服务的方法的流程图；

[0041] 图2示出根据本公开一实施方式的可信执行环境系统的软件架构示意图；

[0042] 图3示出根据本公开一实施方式的可信应用响应普通世界服务请求过程的流程图；

[0043] 图4示出根据本公开一实施方式的完整性度量和验证过程的流程图；

[0044] 图5示出根据本公开一实施方式的数据封装过程的流程图；

[0045] 图6示出根据本公开一实施方式的远程证明过程的流程图。

具体实施方式

[0046] 下文中，将参考附图详细描述本公开的示例性实施方式，以使本领域技术人员可容易地实现它们。此外，为了清楚起见，在附图中省略了与描述示例性实施方式无关的部分。

[0047] 在本公开中，应理解，诸如“包括”或“具有”等的术语旨在指示本说明书中所公开的特征、数字、步骤、行为、部件、部分或其组合的存在，并且不欲排除一个或多个其他特征、数字、步骤、行为、部件、部分或其组合存在或被添加的可能性。

[0048] 另外还需要说明的是，在不冲突的情况下，本公开中的实施例及实施例中的特征

可以相互组合。下面将参考附图并结合实施例来详细说明本公开。

[0049] 针对上述TEE方案采用宏内核架构实现而存在的不足，本公开提出了一种利用基于微内核架构的可信执行环境系统提供可信服务的方法，基于微内核架构实现了TEE(可信执行环境，Trusted Execution Environment)系统，为普通操作系统提供可信服务，并基于微内核的隔离机制为可信服务提供隔离，同时提供了完整性度量与验证、数据封装/解封装和远程证明等可信计算服务。本公开构建的TEE系统主要包括TEE OS(OperatingSystem)，监视器(Monitor)，根任务(Root Task)，Trusted Service以及可信应用等。TEE OS是基于微内核构建，由微内核提供核心服务。监视器是TrustZone中负责安全世界和普通世界之间切换的组件。根任务是用户层运行的第一个应用程序，接管所有系统未用资源并负责其他应用的创建和管理。Trusted Service提供数据封装/解封装和远程证明等可信计算服务。可信应用主要是一些安全敏感的操作，负责为普通世界提供安全服务。

[0050] 为了实现本公开的目的之一，提供一种基于微内核架构的TEE系统，采用的技术方案包含TEE OS、监视器和根任务等三个组件。

[0051] 所述TEE OS的技术方案如下：

[0052] 1)TEE OS基于微内核构建，利用微内核提供的隔离机制为上层应用提供隔离保证。

[0053] 2)TEE OS提供进程管理功能，负责可信应用的创建、管理以及销毁服务，实现对可信应用全生命周期管理。

[0054] 3)TEE OS提供了进程间通信(Inter Process Communication，IPC)服务。IPC机制可以用于可信应用之间的通信和消息传递。

[0055] 4)中断处理服务需要在内核中进行中断注册。当有中断触发后，中断通知信号会通过内核发送到对应的用户层中断处理程序进行处理。

[0056] 所述监视器负责ARM TrustZone中的安全世界和普通世界的上下文切换。当普通世界或安全世界调用切换指令(Secure Monitor Call，SMC)时，处理器切换到监视器模式。由对应的SMC处理程序完成相应世界上下文保存和恢复以及传递相关参数的操作。

[0057] 所述根任务是用户层运行的第一个应用程序，由内核负责创建，检查其镜像完整性并提供启动环境。微内核启动后将所有系统未用资源交由根任务接管。根任务拥有最高优先级并负责创建和管理其他应用。当接收到来自普通世界的服务请求时，根任务将根据请求ID负责将请求数据转发到对应的可信应用进行处理。完成处理请求后根任务通过调用SMC指令将处理结果返回给普通世界。

[0058] 为了实现本公开的另一目的，提供完整性度量和验证、数据封装/解封装以及远程证明等核心可信计算服务。可信计算服务，采用的技术方案包括提供基本密码学算法的用户层密码学库以及提供可信计算功能的TrustService。

[0059] 所述密码学库在用户层添加并提供基本的密码学算法，至少需要包含对称加密算法、非对称加密算法以及哈希算法。

[0060] 所述Trust Service是一个优先级仅低于根任务的可信应用。TrustService可信计算服务需要设备提供基本的硬件密钥支持，包括一个根对称加密密钥和一个设备根密钥，对称加密密钥负责对平台的数据进行保护，设备根密钥是厂商颁发的一个非对称密钥，代表设备的身份。Trust Service基于上述硬件密钥提供数据封装/解封装和远程证明等可

信计算服务。

[0061] 所述完整性度量和验证具体方案如下：

[0062] 1)当可信应用需要运行时，根任务创建一个新进程并进行配置。

[0063] 2)根任务验证可信应用镜像的数字签名证书。数字签名证书由应用开发者附在镜像末端，其中包含可信应用镜像的标准完整性值。

[0064] 3)计算可信应用程序镜像的完整性值，并与数字证书中的标准值进行对比。若一致，则验证成功；否则进程创建失败，返回错误值。计算得到的完整性值由根任务保存，可用于数据封装/解封装和远程证明。

[0065] 4)验证成功后，可信应用镜像映射到新进程的地址空间。

[0066] 所述数据封装/解封装具体方案如下：

[0067] 1)可信应用向根任务发送数据封装请求，包含了要封装的原始数据。

[0068] 2)根任务将代表可信应用身份的完整性值和待封装数据发送到Trusted Service。

[0069] 3)Trusted Service根据可信应用的完整性值和根对称加密密钥派生出封装密钥。封装密钥的派生使用了设备根对称加密密钥和可信应用的完整性值，因此能够保证使用该封装密钥保护的数据只能由该设备的对应可信应用使用。

[0070] 4)利用派生密钥实现待封装数据的对称加密操作，得到封装结果。

[0071] 5)封装结果返回给根任务保存。

[0072] 6)解封装为封装的逆过程。可信应用向根任务发送解封装请求。由根任务将封装结果和完整性值发送给Trusted Service进行解封操作，其中涉及密钥派生和对称解密等操作。最后将解封装结果即原始数据返回给可信应用。

[0073] 所述远程证明具体方案如下：

[0074] 1)远程可信实体作为验证者向证明者发送验证请求，请求中包含要验证的服务ID和随机数nonce。

[0075] 2)证明者接收到验证请求后，根任务将对应ID的可信应用的完整性值和随机数nonce发送给Trusted Service。

[0076] 3)Trust Service使用证明密钥对完整性值和随机数nonce进行签名，并将签名结果返回根任务。其中证明密钥由设备产生并由厂商的签名密钥签发。

[0077] 4)根任务将签名结果返回给验证者，由验证者根据验签结果决定该服务是否可信。

[0078] 下面通过具体实施例详细介绍本公开实施例的细节。

[0079] 图1示出根据本公开一实施方式的利用基于微内核架构的可信执行环境系统提供可信服务的方法的流程图。所述可信执行环境系统中运行有可信操作系统、可信服务组件、监视器组件以及根任务，所述可信操作系统基于微内核构建，并由微内核提供核心服务；所述可信服务组件用于提供可信计算服务；所述监视器组件用于负责安全世界和普通世界之间的切换；根任务为在所述可信执行环境系统的用户层第一个运行的应用程序，用于接管可信执行环境系统中未用资源、并负责创建和管理其他应用程序；如图1所示，所述利用基于微内核架构的可信执行环境系统提供可信服务的方法包括以下步骤：

[0080] 在步骤S101中，启动所述可信操作系统，并由所述可信操作系统创建运行所述根

任务的第一进程,以及验证所述根任务镜像的完整性,并由所述第一进程执行所述根任务;

[0081] 在步骤S102中,响应于来自普通世界的服务请求,所述服务请求包括服务标识和相关数据,所述根任务创建运行所述服务标识对应的可信应用进程,并验证所述服务标识对应的可信应用镜像的完整性,并在验证完成后将所述可信应用镜像映射到新建可信应用进程的地址空间,以运行所述可信应用,由所述可信应用对所述相关数据进行处理;

[0082] 在步骤S103中,在所述可信应用完成对所述相关数据的处理后,由所述根任务通过调用预设切换指令而将处理器切换至监视器模式;

[0083] 在步骤S104中,在所述监视器模式下,利用所述监视器组件将所述可信操作系统的上下文数据保存起来,并切换到普通世界的通用操作系统,以将所述相关数据的处理结果返回给普通世界。

[0084] 本实施例中,可信执行环境系统使用ARM TrustZone技术提供两个运行环境:安全世界和普通世界;其中普通世界运行通用操作系统;安全世界运行可信执行环境,可信执行环境内运行可信应用,为普通世界提供安全服务。

[0085] 在本实施例的一个可选实现方式中,该方法还包括:

[0086] 获取运行可信执行环境系统的设备提供的根对称加密密钥和设备根密钥;并利用所述对称加密密钥和设备根密钥对数据进行保护,设备根密钥为设备厂商颁发的非对称密钥,代表所述设备的身份。

[0087] 在本实施例的一个可选实现方式中,所述可信操作系统基于微内核构建,利用微内核提供的隔离机制为上层可信应用提供隔离保证;所述可信操作系统提供实现可信应用的创建、管理以及销毁的接口服务,用于对可信应用实现全生命周期管理;所述可信应用之间的消息传递通过调用微内核提供的进程间通信接口实现;所述可信操作系统提供中断处理功能,包括中断在内核中注册以及中断触发后发送通知信号到对应的中断处理程序进行处理。

[0088] 在本实施例的一个可选实现方式中,所述监视器组件用于负责普通世界和安全世界的上下文切换:当普通世界或者安全世界调用预设切换指令时,触发处理器切换到监视器模式,在监视器模式下,监视器根据所述监视器模式下的向量基地址寄存器中存储的异常向量表跳转到对应的预设异常处理程序执行,所述预设异常处理程序对当前世界的处理器上下文进行保存,然后加载另外一个世界的处理器上下文。

[0089] 在本实施例的一个可选实现方式中,所述可信执行环境系统中还运行有可信服务组件;所述可信服务组件为根任务创建的一个服务组件,所述可信服务组件是唯一与存储根对称加密密钥和设备根密钥进行交互的可信应用可信计算服务由可信服务组件完成,以保证可信计算服务所需要的机密信息不会离开可信服务组件。

[0090] 图2示出根据本公开一实施方式的可信执行环境系统的软件架构示意图。如图2所示,本公开基于微内核架构的可信执行环境系统主要包括以下组件:TEE OS(MicroTEE,可信操作系统),监视器(Monitor)组件,根任务(Root Task)组件,可信服务组件(Trusted Service)以及可信应用(TA)。TEE OS基于微内核构建并提供进程管理、进程间通信以及地址空间管理等核心服务。监视器负责安全世界和普通世界之间的切换。根任务作为用户层运行的第一个应用程序,接管所有系统未用资源并负责创建和管理其他可信应用。Trusted Service负责管理平台密钥,并提供可信计算服务。可信应用为普通世界提供安全服务。

[0091] 1、TEE OS基于微内核构建并为上层可信应用提供核心服务接口。可信应用需要执行时，可以通过进程创建接口服务创建新进程并分配指定大小的内存空间。可信应用之间需要通信进行消息交换时，通过调用TEE OS提供的发送和接收消息的IPC接口服务实现。上层可信应用之间的相互隔离由微内核的隔离机制提供保证。TEE OS用户层提供密码学库，用于为可信应用提供基本的密码学算法，至少包含对称加密算法，非对称加密算法以及哈希算法。密码学库可以作为静态库链接到可执行文件中。

[0092] 2、监视器负责安全世界和普通世界之间的切换。SMC指令触发处理器切换进入监视器模式。关于监视器设置和功能如下：

[0093] 1)监视器的配置操作在平台初始化时完成，包括设置监视器模式的栈顶指针以及将向量表基地址写入向量表基地址寄存器(Monitor VectorBase Address Register，MVBAR)。

[0094] 2)SMC指令需要在特权模式下执行，所以需要添加一个系统调用。用户层可信应用可以通过该系统调用进入特权模式并执行SMC指令。

[0095] 3)监视器模式可以通过物理寄存器r0，r1等来传递参数和数据。当数据较大时，需要通过两个世界之间的共享内存来传递。

[0096] 4)当调用SMC指令触发处理器进入监视器模式后，可以通过向量表跳转到对应的SMC处理程序。该处理程序需要完成保存当前世界上下文并恢复另一世界上下文以及更改NS位的操作。NS位保存在安全配置寄存器(Secure Configuration Register，SCR)中。

[0097] 3、根任务可以实现为初始进程，是内核启动后运行的第一个用户层应用。它由内核创建并在加载其他可信应用时验证镜像的完整性。当内核完成启动后，将所有未用系统资源交由根任务管理。因此，根任务在用户层拥有最高的优先级。根任务负责管理其他可信应用，包括创建、配置和销毁等整个生命周期的管理。当普通世界发来服务请求时，根任务根据请求中的服务ID将数据转发到对应的可信应用进行处理。当处理完成后，根任务执行SMC指令实现将结果返回给普通世界。

[0098] 4、Trusted Service可以实现为一个可信应用，由根任务创建且优先级仅低于根任务。Trusted Service可以与平台的根对称加密密钥和设备根密钥进行交互，并提供数据封装/解封装和远程证明等可信计算服务。

[0099] 5、可信应用为普通世界提供安全服务。可信应用响应普通世界服务请求的过程如图3所示。

[0100] 1)普通世界通过SMC指令将服务请求传递到安全世界，包括服务ID以及相关数据。

[0101] 2)根任务根据服务ID将请求数据转发到对应的可信应用。

[0102] 3)可信应用处理完成请求后，将结果返回给根任务。

[0103] 4)根任务通过SMC调用进行世界切换，将结果返回给普通世界。

[0104] 在本实施例的一个可选实现方式中，步骤S202中，所述根任务创建运行所述服务标识对应的可信应用进程，并验证所述服务标识对应的可信应用镜像的完整性，并在验证完成后将所述可信应用镜像映射到所述可信应用进程的地址空间，以运行所述可信应用的步骤，进一步包括：

[0105] 运行可信应用时，利用所述根任务创建所述可信应用进程并配置相关信息；

[0106] 利用所述根任务验证可信应用镜像文件的数字签名证书；所述数字签名证书由应

用开发者附在可信应用镜像末端，包含可信应用镜像的标准完整性值；其中，可信应用的完整性值可以用密码学中的单向哈希算法计算得到；

[0107] 利用所述根任务计算可信应用镜像的完整性值并与数字证书中的标准值进行对比，若完整性值对比一致，则将镜像文件映射到进程的地址空间中；否则进程创建失败，并返回错误值。

[0108] 在本实施例的一个可选实现方式中，所述方法还包括：

[0109] 响应于所述可信应用发送的封装请求，利用所述根任务将代表所述可信应用身份的完整性值以及待封装数据发送给可信服务组件，所述封装请求中包括所述待封装数据；

[0110] 利用所述可信服务组件根据所述完整性值和设备的根对称加密密钥派生出封装密钥，然后使用所述封装密钥对所述待封装数据进行加密，并将封装结果返回给所述根任务；

[0111] 响应于所述可信应用发送的解封请求，利用所述根任务将待解封的封装结果和可信应用的完整性值发送给所述可信服务组件；

[0112] 利用所述可信服务组件进行密钥派生和解密操作并将解封结果返回给所述根任务，并利用所述根任务将解封后的原始数据返回给所述可信应用。

[0113] 在本实施例的一个可选实现方式中，所述方法还包括：

[0114] 响应于远程可信实体作为验证者而发送的验证请求，所述验证请求中包含待验证的服务标识和随机数；利用所述根任务将对应于所述服务标识的所述可信应用的完整性值和随机数发送给可信服务组件；并利用所述可信服务组件使用证明密钥对所述完整性值和随机数进行签名，并把签名结果返回给所述根任务；

[0115] 利用所述根任务将签名结果返回给所述验证者，以便由所述验证者根据所述签名结果决定所述服务标识对应的所述可信应用的当前状态是否可信。

[0116] 在一些实施例中，可信服务组件用于实现可信计算服务。

[0117] 所述可信计算服务实施步骤如下：

[0118] 1、完整性度量和验证是在可信应用程序运行前，对其镜像的完整性和数字证书签名进行验证。其过程如图4所示：

[0119] 1)由根任务为可信应用创建一个新进程，并配置地址空间、进程间通信等相关信息。

[0120] 2)可信应用镜像包括两部分：原始镜像和镜像末端的数字证书。验证数字证书的签名以确保其来自合法开发者；然后计算原始镜像的完整性值并与数字证书中的标准值进行对比，计算得到的完整性值由根任务保存。

[0121] 3)若完整性验证通过则将可信应用镜像映射到新进程的地址空间；否则进程创建失败，并返回错误值。

[0122] 2、数据封装是将数据绑定到指定可信应用，从而保证数据的机密性。其过程如图5所示。

[0123] 1)当某个可信应用需要封装机密数据时，可以向根任务发送封装请求，请求中包含了待封装数据。

[0124] 2)根任务收到可信应用的封装请求后，将待封装数据和代表可信应用身份的完整性值发送给Trusted Service。

[0125] 3)Trusted Service根据可信应用的完整性值和根对称加密密钥派生出封装密钥,使用该封装密钥对待封装数据进行加密。

[0126] 4)封装结果返回给根任务保存。

[0127] 5)解封装为封装的逆过程。根任务接收到可信应用的解封装请求后,将封装结果和可信应用的完整性值发送给Trusted Service,然后TrustedService进行密钥派生和解密操作并将解封装结果返回给根任务,最后将原始数据返回到可信应用。

[0128] 3、远程证明可以向远程可信实体证明指定可信应用的当前状态。其过程如图6所示。

[0129] 1)远程可信实体作为验证者向证明者发送验证请求,请求中包含要验证的服务ID和随机数nonce。

[0130] 2)证明者接收到验证请求后,由根任务将对应ID的可信应用的完整性值和随机数nonce发送给Trusted Service。

[0131] 3)Trusted Service使用证明密钥对完整性值和随机数nonce进行签名,并将签名结果返回给根任务。其中证明密钥由设备产生并由设备厂商的签名密钥签发。

[0132] 4)根任务将签名结果返回给验证者,由验证者根据签名结果决定该服务的当前状态是否可信。

[0133] 作为另一方面,本公开还提供了一种计算机可读存储介质,该计算机可读存储介质可以是上述实施方式中所述装置中所包含的计算机可读存储介质;也可以是单独存在,未装配入设备中的计算机可读存储介质。计算机可读存储介质存储有一个或者一个以上程序,所述程序被一个或者一个以上的处理器用来执行描述于本公开的方法。

[0134] 以上描述仅为本公开的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解,本公开中所涉及的发明范围,并不限于上述技术特征的特定组合而成的技术方案,同时也应涵盖在不脱离所述发明构思的情况下,由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本公开中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

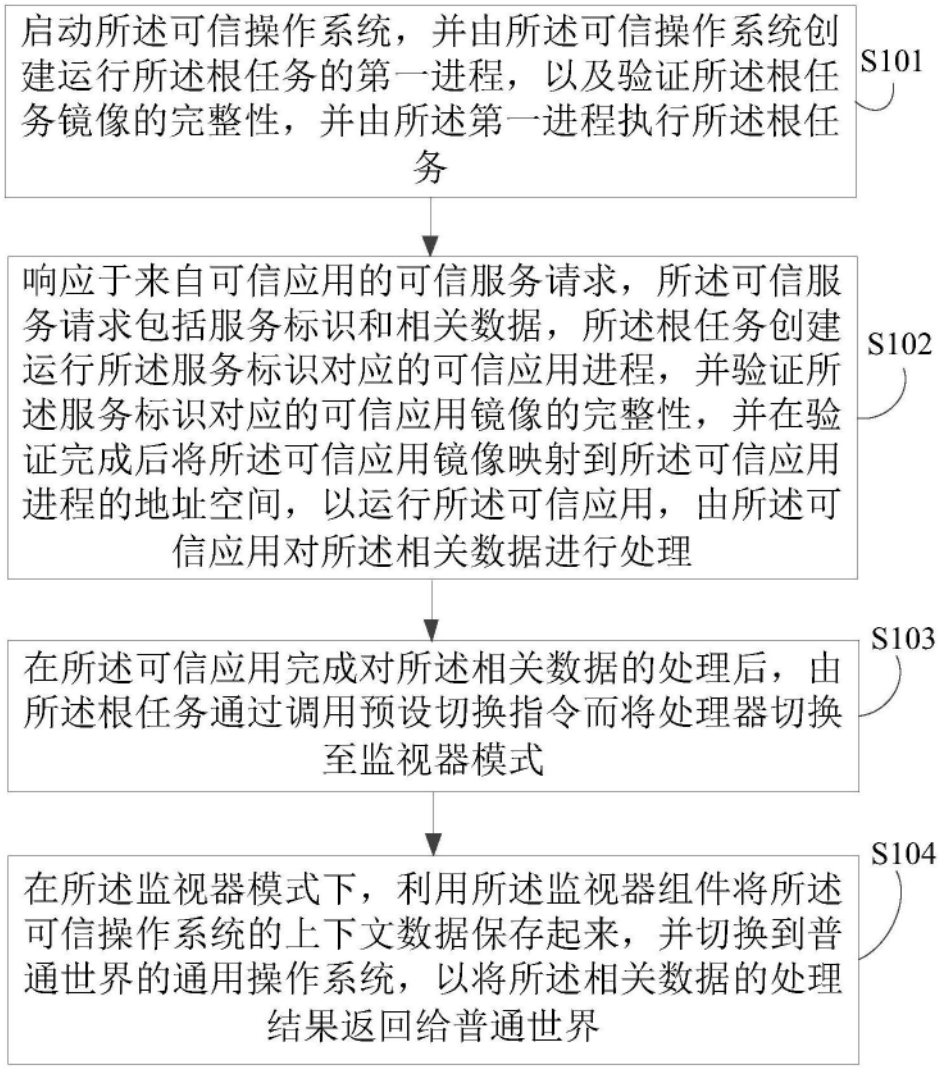

启动所述可信操作系统，并由所述可信操作系统创建运行所述根任务的第一进程，以及验证所述根任务镜像的完整性，并由所述第一进程执行所述根任务
S101
响应于来自可信应用的可信服务请求，所述可信服务请求包括服务标识和相关数据，所述根任务创建运行所述服务标识对应的可信应用进程，并验证所述服务标识对应的可信应用镜像的完整性，并在验证完成后将所述可信应用镜像映射到所述可信应用进程的地址空间，以运行所述可信应用，由所述可信应用对所述相关数据进行处理
S102
在所述可信应用完成对所述相关数据的处理后，由所述根任务通过调用预设切换指令而将处理器切换至监视器模式
S103
在所述监视器模式下，利用所述监视器组件将所述可信操作系统的上下文数据保存起来，并切换到普通世界的通用操作系统，以将所述相关数据的处理结果返回给普通世界
S104

图1

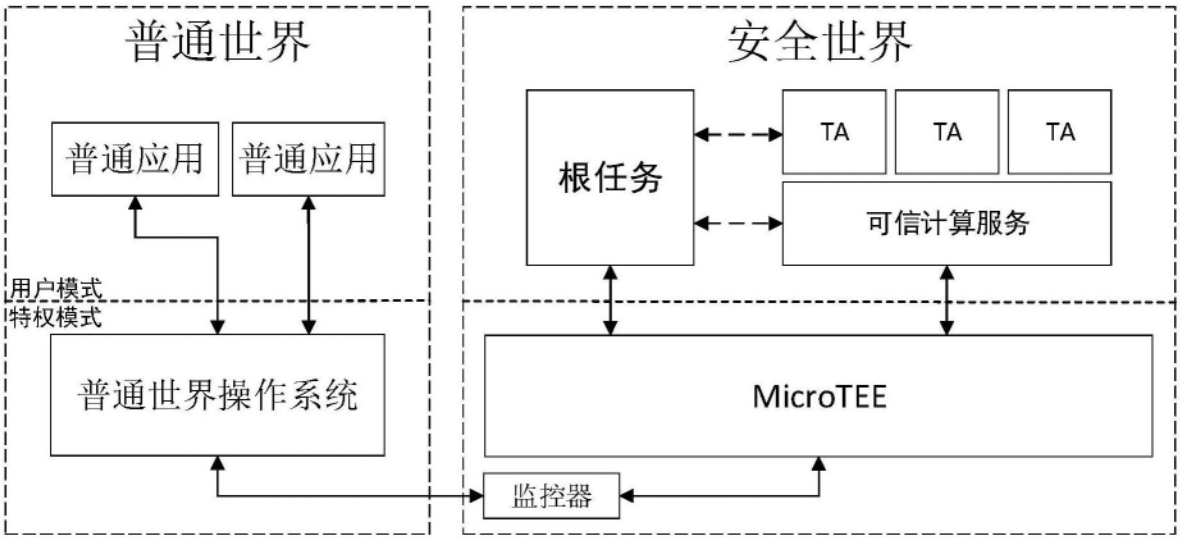

普通世界
普通应用
普通应用
用户模式
特权模式
普通世界操作系统
安全世界
根任务
TA
TA
TA
可信计算服务
MicroTEE
监控器

图2

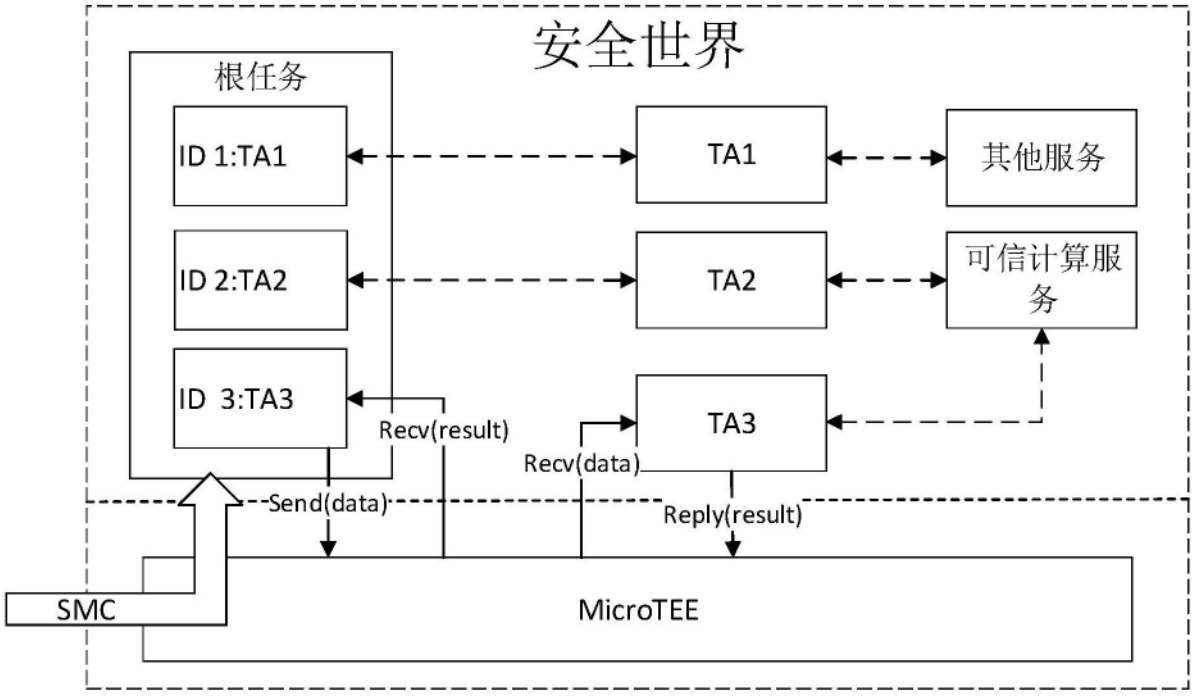

安全世界
根任务
ID 1:TA1
ID 2:TA2
ID 3:TA3
TA1
TA2
TA3
其他服务
可信计算服务
Recv(result)
Recv(data)
Send(data)
Reply(result)
SMC
MicroTEE

图3

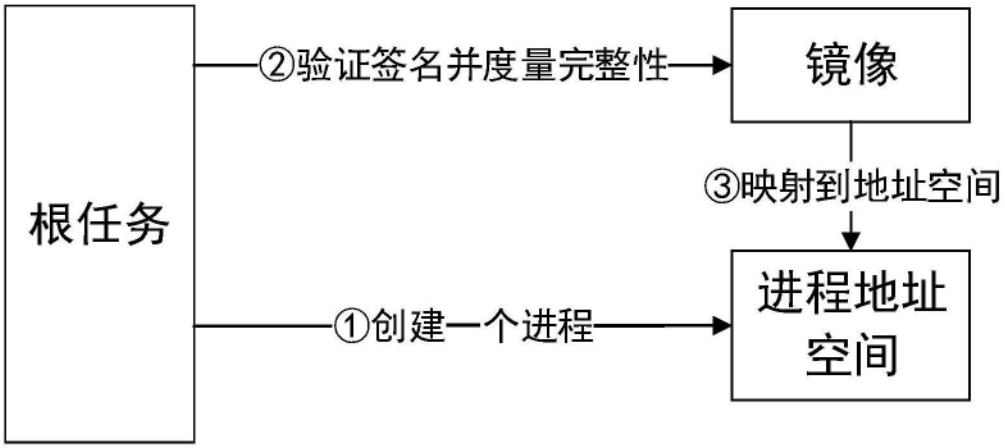

根任务
②验证签名并度量完整性
镜像
③映射到地址空间
进程地址空间
①创建一个进程

图4

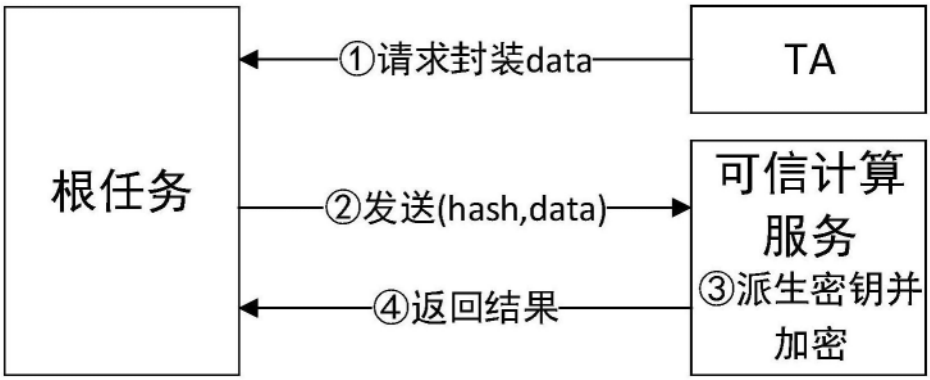

根任务
①请求封装data
TA
②发送(hash,data)
可信计算服务
③派生密钥并加密
④返回结果

图5

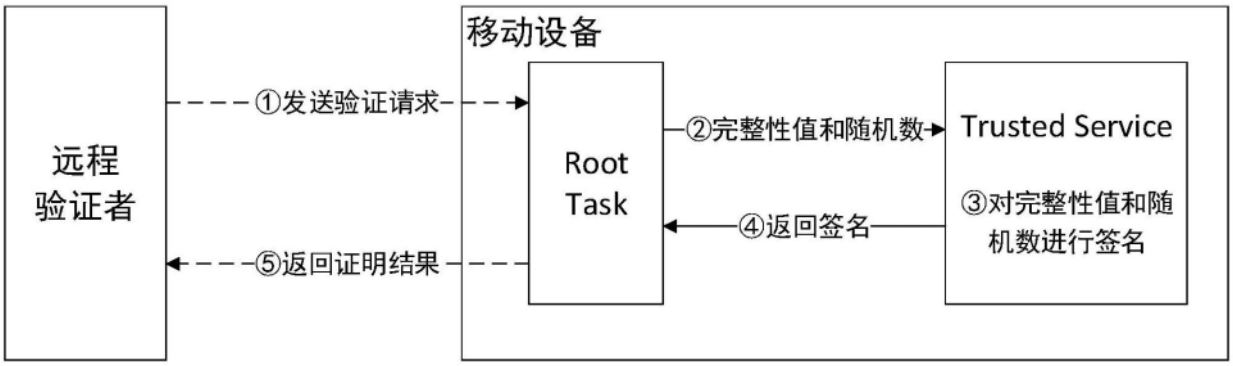

远程验证者
①发送验证请求
⑤返回证明结果
移动设备
Root Task
②完整性值和随机数
④返回签名
Trusted Service
③对完整性值和随机数进行签名

图6