

用于构建可信执行环境的方法、装置及设备

技术领域

[01]本说明书涉及计算机技术领域，尤其涉及一种可信执行环境的构建方法、装置及设备。

背景技术

[02]可信执行环境作为一项安全技术已经广泛应用于各类金融等场景中。当前，很多监管部门也对可信执行环境提出了多项标准。但是，如何让具体产品完备且一致的满足监管要求，一直是一项技术难题。特别是在当前国产化进程的大趋势下，如何将现有的可信执行环境实例（如 SGX 或 Trustzone 等）在满足监管要求的前提下向如 RISC-V 等指令集迁移，也是一项挑战。为此，需要提供一种可实现可信执行环境的性质传递和功能迁移的可行执行环境的构建方案。

发明内容

[03]本说明书实施例的目的是提供一种可实现可信执行环境的性质传递和功能迁移的可行执行环境的构建方案。

[04]为了实现上述技术方案，本说明书实施例是这样实现的：本说明书实施例提供一种可信执行环境的构建方法，所述方法包括：获取可信执行环境的监管要求信息。对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息。对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，并基于所述可信执行环境的安全方案的公理生成所述可信执行环境的安全方案对应的测试用例。基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境。

[05]本说明书实施例提供一种可信执行环境的构建装置，所述装置包括：监管要求获取模块，获取可信执行环境的监管要求信息。监管要求解析模块，对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息。处理模块，对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，并基于所述可信执行环境的安全方案的公理生成所述可信执行环境的安全方案对应的测试用例。可信环境构建模块，基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境。

[06]本说明书实施例提供一种可信执行环境的构建设备，所述可信执行环境的构建设备包括：处理器；以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：获取可信执行环境的监管要求信息。对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息。对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，并基于所述可信执行环境的安全方案的公理生成所述可信执行环境的安全方案对应的测试用例。基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境。

[07]本说明书实施例还提供了一种存储介质，其中，所述存储介质用于存储计算机可执行指令，所述可执行指令在被执行时实现以下流程：获取可信执行环境的监管要求信息。对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息。对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，并基于所述可信执行环境的安全方案的公理生成所述可信执行环境的安全方案对应的测试用例。基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境。

附图说明

[08]为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[09]图 1 为本说明书一种可信执行环境的构建方法实施例；

[10]图 2 为本说明书另一种可信执行环境的构建方法实施例；

[11]图 3 为本说明书一种可信执行环境的构建过程的示意图；

[12]图 4 为本说明书一种可信执行环境的构建装置实施例；

[13]图 5 为本说明书一种可信执行环境的构建设备实施例。

具体实施方式

[14]本说明书实施例提供一种可信执行环境的构建方法、装置及设备。

[15]为了使本技术领域的人员更好地理解本说明书中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本说明书保护的范围。

实施例一

[16]如图 1 所示，本说明书实施例提供一种可信执行环境的构建方法，该方法的执行主体可以为服务器或终端设备，其中，该终端设备可以如笔记本电脑或台式电脑等计算机设备，还可以如手机或平板电脑等移动终端设备。该服务器可以是某项业务（如进行交易的业务或金融业务等）或需要为某设备（如物联网设备、云端设备、移动终端设备等）构建可执行环境的服务器，具体如，该服务器可以是支付业务的服务器，也可以是与金融或即时通讯等相关业务的服务器等。本实施例中的执行主体以服务器为例进行说明，对于执行主体为终端设备的情况，可以参见下述相关内容，在此不再赘述。该方法具体可以包括以下步骤：

[17]在步骤 S102 中，获取可信执行环境的监管要求信息。

[18]其中，可信执行环境可以是 TEE（Trusted Execution Environment），该可信执行环境可以为进行数据处理的安全运行环境，该可信执行环境可以通过预定的编程语言编写的程序来实现（即可以是以软件的形式实现），也可以是通过指定的实体部件和编写的程序来实现（即可以是硬件+软件的形式实现），本说明书实施例并不限定可信执行环

境通过上述哪一种形式实现，而且具体通过何种形式实现可以根据实际情况设定。可信执行环境可以是安全并与其它环境相隔离的数据处理环境，即在可信执行环境中执行的处理，以及数据处理的过程中产生的数据等无法被可执行环境外的其它执行环境或应用程序所访问。可信执行环境可以通过创建一个可以在可信区域（如 TrustZone 等）中独立运行的小型操作系统实现，可信执行环境可以以系统调用（如由 TrustZone 内核直接处理）的方式直接提供的服务。终端设备中可以包括 REE（富执行环境）和 TEE（即可信执行环境），REE 下可以运行终端设备安装的操作系统，如 Android 操作系统、iOS 操作系统、Windows 操作系统、Linux 操作系统等，REE 可以为上层应用程序提供终端设备的所有功能，比如摄像功能，触控功能等，但是，REE 中存在很多安全隐患，例如，操作系统可以获得某应用程序的所有数据，但很难验证该操作系统或该应用程序是否被篡改，如果被篡改，则用户的信息将存在很大的安全隐患，针对于此，就需要终端设备中的可信执行环境进行处理。可信执行环境具有其自身的执行空间，也即是在可信执行环境下也存在一个操作系统，可信执行环境比 REE 的安全级别更高，可信执行环境所能访问的终端设备中的软件和硬件资源是与 REE 分离的，但可信执行环境可以直接获取 REE 的信息，而 REE 不能获取可信执行环境的信息。可信执行环境可以通过提供的接口来进行验证等处理，从而保证用户信息（如支付信息、用户隐私信息等）不会被篡改、密码不会被劫持、指纹或面部等信息不会被盗用。监管要求信息可以是对可信执行环境的构建方式、需要采用的安全处理机制、可信执行环境的架构、生命周期、口令输入和修改方式、消息输出机制、身份鉴别功能、时钟功能等进行限定和监管的相关信息，具体如，监管要求信息可以包括可信服务中的相关事务，需要保证原子性、一致性、隔离性和持久性，限制未被授权的 TA 访问该可信执行环境中的可信服务等，除了上述方式外，还可以包括多种监管要求信息，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[19]在实施中，可信执行环境作为一项安全技术已经广泛应用于各类金融等场景中。当前，很多监管部门也对可信执行环境提出了多项标准。但是，如何让具体产品完备且一致的满足监管要求，一直是一项技术难题。特别是在当前国产化进程的大趋势下，如何将现有的可信执行环境实例（如 SGX 或 Trustzone 等）在满足监管要求的前提下向如 RISC-V 等指令集迁移，也是一项挑战。为此，需要提供一种可实现可信执行环境的性质传递和功能迁移的可行执行环境的构建方案。

[20]在实际应用中，通用信息安全标准（Common Criteria, CC）提出了一种可执行环境的构建方案，即从 PP（Protection Profile, 保护配置文件）出发，将具体的构建后的可执行环境拆分成不同的安全功能需求（即 SFR），并对安全功能需求进行与具体场景绑定的详细设计，最终得到该场景下的可执行环境。然而，上述可执行环境的构建方案中，并没有涉及到不同具体场景之间安全要求的迁移，也不涉及到对该迁移的完备性与一致性检测，因此，上述可执行环境的构建方案的复用性差，即每当需要针对某一场景构建相应的可信执行环境时，需要重新执行上述完整的过程，而且还会使得可信执行环境的构建效率低下。本说明书实施例提供一种可实现的可行执行环境的构建方案没具体可以包括以下内容：在实际应用中，最终构建出的任意场景下的可信执行环境需要满足可信执行环境的监管要求，该监管要求可以是指定的机构或部门提供的构建可行执行环境需要满足的基本条件等相关信息，该监管要求可以是第三方权威机构（如某国家的监管部门等）发布的监管要求，也可以是业务提供方在第三方权威机构发布的监管要求的基础上，结合自身的需求而设定的监管要求，该设定的监管要求可以满足第三方权威机构发布的监管要求。此外，在实际应用中，不同场景下的可信执行环境对应的监管要求可以不同，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[21]基于上述内容，为了构建满足监管要求的可信执行环境，可以获取相应的监管要求

信息,该监管要求信息对应的监管要求可以是针对某一场景的监管要求,也可以是通用的监管要求(即针对任意场景的监管要求)等,具体可以根据实际情况获取相应的监管要求信息,本说明书实施例对此不做限定。

[22]在步骤 S104 中,对上述监管要求信息进行解析,得到应用于可信执行环境且原子化的安全功能信息。

[23]其中,原子化可以是基于某信息或数据的用途或作用等,将该信息或数据以精细颗粒化的方式进行拆分和分解而得到的相对较小的单元(或者可以是该信息或数据的使用或作用的过程中的最小单元)的处理方式,例如,监管要求信息往往是文本类型的信息,即监管要求信息包括较为宏观的针对可信执行环境的监管要求的信息,为了将监管要求信息中较为宏观的内容转换为较为直观的精细颗粒化的信息,可以对监管要求信息进行原子化处理。安全功能信息可以通过通用信息安全标准(Common Criteria)中的安全功能要求 SFR 确定,或者,也可以通过其它规则确定,具体可以根据实际情况设定,本说明书实施例对此不做限定。

[24]在实施中,通过上述步骤 S102 的处理得到可信执行环境的监管要求信息后,可以基于通用信息安全标准,从保护配置文件出发,将组成可信执行环境的安全方案的安全功能进行拆分处理,具体地,由于通用信息安全标准是一个框架,计算机的可信执行环境或具有可信执行环境的对象的开发者可以根据保护配置文件中的安全功能要求(SFR)开发相应的可信执行环境,以此来满足可信执行环境的监管要求,基于此,可以结合组成可信执行环境的安全方案的安全功能,对上述监管要求信息进行解析和分解,得到原子化的安全功能信息(或原子化的安全功能需求 SFR)。

[25]在步骤 S106 中,对上述安全功能信息进行形式化解析处理,得到可证明其满足上述监管要求信息的可信执行环境的安全方案,并基于可信执行环境的安全方案的公理生成可信执行环境的安全方案对应的测试用例。

[26]其中,形式化解析处理可以包括多种可实现方式,例如可以通过形式语义翻译 Formal Semantics Translation 机制实现等,其中的形式语义翻译 Formal Semantics Translation 可以通过代数结构对待处理对象进行形式化描述,此外,还可以通过其它多种方式实现上述形式化解析处理,具体可以根据实际情况设定,本说明书实施例对此不做限定。

[27]在实施中,通过上述方式得到原子化的安全功能信息后,可以基于形式语义翻译 Formal Semantics Translation 机制对经过原子化拆分的监管要求信息进行形式化解释,得到相应的可信执行环境的安全方案,其中,得到的可信执行环境的安全方案可以是可信执行环境的通用安全方案,通用安全方案可以是不同场景下可信执行环境的安全方案的基础。此外,通过上述方式得到的可信执行环境的通用安全方案可以通过证明的方式确定该通用安全方案满足上述的监管要求信息。

[28]另外,还可以通过可信执行环境的安全方案生成可信执行环境的安全方案对应的测试用例,具体地,可以通过公理化变换 Axiomatisation Transformation 机制对通用安全方案中包含的内容进行公理化,从而形成通用安全方案的公理,然后,可以以通用安全方案的公理确定可信执行环境的安全方案对应的测试用例,其中得到的测试用例可以为通用测试用例,该通用测试用例可以是不同场景下可信执行环境的测试用例的基础。公理化变换 Axiomatisation Transformation 机制可以是基于形式公理规则确定,也可以是基于实质公理规则确定,具体可以根据实际情况设定,本说明书实施例对此不做限定。

[29]需要说明的是,上述可信执行环境的安全方案可以如上所述为通用安全方案,在实际应用中,上述可信执行环境的安全方案不仅可以包括通用安全方案,还可以包括不同场景下可信执行环境的安全方案(可以称为子安全方案),相应的,上述可信执行环境

的安全方案对应的测试用例不仅可以包括通用测试用例，还可以包括不同场景下可信执行环境的测试用例（可以称为子测试用例）等。

[30]在步骤 S108 中，基于可信执行环境的安全方案和可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与该安全方案和该测试用例在预设性质项目上具备相同性质信息的可信执行环境。

[31]其中，性质迁移机制可以是已经过验证或认证的对象性质或性质迁移至与该对象存在指定关联关系的另一对象的处理机制，例如，针对可信执行环境的通用安全方案，如果通用安全方案经过验证，该通用安全方案满足上述监管要求信息，当通过该通用安全方案生成某场景下的可信执行环境的子安全方案时，可以通过性质迁移机制，将该通用安全方案具备的满足上述监管要求信息等性质迁移到场景下的可信执行环境的子安全方案，此时，该子安全方案也满足上述监管要求信息。预设性质项目可以包括一个性质项目，也可以包括多个性质项目，其中的性质项目可以如“是否满足监管要求信息”、“通用安全方案与子安全方案对应的技术方案是否一致”、“通用安全方案与子安全方案对应的技术方案是否完备”等，具体可以根据实际情况设定，本说明书实施例对此不做限定。性质信息可以是性质项目对应的内容信息，例如，性质项目为“是否满足监管要求信息”，相应的性质信息可以为“满足监管要求信息”等。目标场景可以是任意场景，例如终端设备场景或物联网场景等，此外，目标场景可以包括一个场景，也可以包括多个不同的场景，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[32]在实施中，通过上述方式得到可信执行环境的安全方案（即通用安全方案）和可信执行环境的安全方案对应的测试用例（即通用测试用例）后，可以基于通用安全方案，通过预设的性质迁移机制构建目标场景下可信执行环境的子安全方案，同样的，可以基于通用测试用例，通过预设的性质迁移机制构建目标场景下可信执行环境的子测试用例。然后，可以获取目标场景下可信执行环境的子安全方案中包括如资源占用限制等在内的受限信息或完备信息，可以结合得到的受限信息或完备信息，基于目标场景下可信执行环境的子测试用例构建目标场景下的可信执行环境，同时，还可以通过性质迁移机制将子测试用例的相关性质迁移至目标场景下的可信执行环境，以使得生成的目标场景下的可信执行环境可以满足上述监管要求信息。

[33]本说明书实施例提供一种可信执行环境的构建方法，通过对获取的可信执行环境的监管要求信息进行解析，得到应用于可信执行环境且原子化的安全功能信息，然后，通过对安全功能信息进行形式化解析处理，得到可证明其满足监管要求信息的可信执行环境的安全方案，并基于可信执行环境的安全方案的公理生成可信执行环境的安全方案对应的测试用例，进而基于可信执行环境的安全方案和可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与该安全方案和该测试用例在预设性质项目上具备相同性质信息的可信执行环境，这样，基于形式化、公理化的形式构建可信执行环境的通用安全方案和通用测试用例等，并在此基础上描述监管要求，使得监管要求和通用安全方案和通用测试用例等技术方案一致且完备，而且，通过本实施例提供的技术方案，可以将监管要求完备且一致的传递或迁移到具体的目标场景下可信执行环境的具体实现中，从而避免不同场景下对监管要求的重复认证，提高了可信执行环境的构建效率。

实施例二

[34]如图 2 所示，本说明书实施例提供一种可信执行环境的构建方法，该方法的执行主体可以为服务器或终端设备，其中，该终端设备可以如笔记本电脑或台式电脑等计算机设备，还可以如手机或平板电脑等移动终端设备。该服务器可以是为某项业务（如进行交易的业务或金融业务等）或需要为某设备（如物联网设备、云端设备、移动终端设备

等)构建可执行环境的服务器,具体如,该服务器可以是支付业务的服务器,也可以是与金融或即时通讯等相关业务的服务器等。本实施例中的执行主体以服务器为例进行说明,对于执行主体为终端设备的情况,可以参见下述相关内容,在此不再赘述。该方法具体可以包括以下步骤:在步骤 S202 中,获取可信执行环境的监管要求信息。

[35]其中,可信执行环境 TEE 可以包括多种不同的实现方式,例如,可信执行环境可以包括通过 SGX 和预设的第一应用程序构建的可信执行环境、通过 Trustzone 和预设的第二应用程序构建的可信执行环境和通过预设的第三应用程序构建的可信执行环境中的一种或多种,也即是:本实施例中的可信执行环境并不限于是通过软件的方式构建的可信执行环境,也不限于是通过硬件+软件的方式构建的可信执行环境,不论哪种方式构建的可信执行环境均可以应用于本说明书实施例中。

[36]在步骤 S204 中,获取组成安全方案的安全功能信息。

[37]在实施中,如图 3 所示,针对可信执行环境的安全方案(即通用安全方案),可以对该可信执行环境的安全方案的内容进行分析,确定该安全方案中所包含的安全功能,然后,可以从该安全方案中获取组成安全方案的安全功能,并可以获取组成安全方案的安全功能的信息,从而得到组成安全方案的安全功能信息。

[38]需要说明的是,组成通用安全方案的安全功能的描述与具体应用场景和可信执行环境的实现无关。

[39]在步骤 S206 中,通过通用信息安全标准 CC,基于获取的组成安全方案的安全功能信息对上述监管要求信息进行拆解处理,得到应用于可信执行环境且原子化的安全功能信息。

[40]其中,原子化的安全功能信息对应的安全功能中,不同的安全功能之间满足相互独立且完全穷尽 MECE (Mutually Exclusive Collectively Exhaustive) 规则,即组成安全方案的安全功能之间相互独立,当前得到的安全功能相对于安全方案来说已完全穷尽。

[41]在步骤 S208 中,对上述安全功能信息进行形式化解析处理,得到可信执行环境的预选安全方案。

[42]如图 3 所示,上述步骤 S208 的具体处理可以参见上述实施例一中步骤 S106 中的相关内容,在此不再赘述。

[43]通过上述方式得到可信执行环境的预选安全方案后,可以证明可信执行环境的预选安全方案能够满足可信执行环境的监管要求信息,具体可以参见下述步骤 S210 和步骤 S212 的处理。

[44]在步骤 S210 中,基于可信执行环境的预选安全方案和可信执行环境的监管要求信息,对可信执行环境的预选安全方案是否满足可信执行环境的监管要求信息进行验证处理,得到相应的验证结果。

[45]在实施中,由于上述已对经过原子化拆分的监管要求信息进行了形式化解释,因此,经过形式化解释的监管要求信息也必然满足监管要求信息,而通过形式化解释得到的预选安全方案也必然满足监管要求信息。

[46]在步骤 S212 中,如果上述验证结果指示预选安全方案满足可信执行环境的监管要求信息,则将预选安全方案作为可信执行环境的安全方案。

[47]在步骤 S214 中,基于可信执行环境的安全方案的公理生成可信执行环境的安全方案对应的测试用例。

[48]如图 3 所示,上述步骤 S214 的具体处理可以参见上述实施例一中步骤 S106 中的相

关内容，在此不再赘述。

[49]在步骤 S216 中，基于可信执行环境的安全方案，通过同态映射构建目标场景下的可信执行环境的子安全方案。

[50]其中，目标场景可以包括物联网场景、云端场景和终端设备场景中的一种或多种。此外，目标场景还可以包括任意需要构建可信执行环境的应用场景，具体可以根据实际情况设定，本说明书实施例对此不做限定。同态映射(即 Homomorphism Interpretation)：设 $V1 = (G, \#)$ 和 $V2 = (S, o)$ 是两个代数系统， $\#$ 和 o 分别是 G 和 S 上的二元运算，设 f 是从 G 到 S 上的一个映射，且对 $\forall a, b \in G$ 有 $f(a \# b) = f(a) o f(b)$ ，则称 f 为 $V1$ 到 $V2$ 的一个同态映射。

[51]在实施中，如图 3 所示，通过上述方式得到可信执行环境的通用安全方案后，可以通过同态映射的方式将可信执行环境的通用安全方案的性质纵向的迁移(或传递)至后续生成的具体场景下的安全方案，即目标场景下的可信执行环境的子安全方案，从而使通用安全方案具备的满足上述监管要求信息的性质迁移到目标场景下的可信执行环境的子安全方案中，使得目标场景下的可信执行环境的子安全方案也具备满足上述监管要求信息的性质。

[52]此外，如果目标场景包括多个不同的场景，例如，目标场景可以包括物联网场景、云端场景和终端设备场景等，不同场景下的可信执行环境的子安全方案之间通过自然变换的方式进行可信执行环境的子安全方案性质的迁移。

[53]其中，在数学的范畴论中，自然变换(Natural Transformation)可以是将一个函子变为另一个函子，使相关范畴的内在结构(就是态射间的复合)得以保持，因此可以将自然变换视为“函子间的态射”，相应的，通过自然变换可以将某一场景下具备的相关性质迁移到另一个场景下，使得该场景下的相关性质迁移到另一个场景下而得到保持。

[54]在实施中，如图 3 所示，通过上述方式得到不同场景下的可信执行环境的子安全方案后，可以通过自然变换的方式将已验证的某场景下的可信执行环境的子安全方案的性质横向的迁移(或传递)至另一个场景下的可信执行环境的子安全方案中，从而使同一通用安全方案下，某一场景下的子安全方案具备的满足上述监管要求信息的性质迁移到另一场景下的子安全方案中，使得另一场景下的子安全方案也具备满足上述监管要求信息的性质，这样，可以将已经满足合规要求的安全能力向新场景或新的平台迁移，避免进行重复认证。

[55]在步骤 S218 中，获取目标场景下可信执行环境的约束信息；结合该约束信息，并基于可信执行环境的安全方案对应的测试用例，通过同态映射构建目标场景下的可信执行环境的子测试用例。

[56]其中，约束(Constraint Inputs)信息可以包括多种，例如资源占用相关的约束信息、设备属性要求(如设备 CPU 的工作频率要求、设备的内存要求等)等，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[57]如图 3 所示，上述步骤 S218 的具体处理可以参考上述步骤 S216 的相关内容执行，在此不再赘述。通过上述方式，可以将通用测试用例已经满足监管要求信息的性质纵向迁移，从而形成配套的完备的子测试用例。

[58]在实际应用中，目标场景可以包括多个不同的场景，不同场景下的可信执行环境的子测试用例之间通过自然变换的方式进行可信执行环境的子测试用例性质的迁移。

[59]上述具体处理可以参考上述步骤 S216 的相关内容执行，在此不再赘述。通过上述方式，可以将已经满足监管要求信息的子测试用例性质向新场景或新的平台迁移，避免进

行重复认证。

[60]如图 3 所示，基于上述内容，通用安全方案与不同场景下的安全方案之间的关系为同态映射，通用测试用例与不同场景下的子测试用例之间的关系为同态映射，此外，基于同一通用安全方案的不同场景下的子安全方案之间满足的关系为自然变换，基于同一通用测试用例的不同场景下的子测试用例之间满足的关系为自然变换。

[61]在步骤 S220 中，基于目标场景下的可信执行环境的子测试用例，通过修正判定条件 MC/DC 覆盖生成目标场景下的可信执行环境。

[62]其中，修正判定条件 MC/DC 覆盖（Modified Condition and Decision Coverage）可以具有 100%覆盖率，可以用于工程化验证具体实现与技术规范同构。MC/DC 覆盖要求在一个程序中每一种输入输出至少需要出现一次，在程序中的每一个条件必须产生所有可能的输出结果至少一次，并且每一个判定中的每一个条件必须能够独立影响一个判定的输出，即在其他条件不变的前提下仅改变该条件的值，而使判定结果改变，即每个条件都要独立影响判定结果。以示例对上述内容进行说明：MC/DC 覆盖首先要求实现条件覆盖、判定覆盖，在此基础上，对于每一个条件 C，要求存在符合以下条件的两次计算：1) 条件 C 所在判定内的所有条件，除条件 C 外，其他条件的取值完全相同；2) 条件 C 的取值相反；3) 判定的计算结果相反。

[63]在实施中，如图 3 所示，可以基于上述 MC/DC 覆盖的定义和示例，可以对目标场景下的可信执行环境的子测试用例进行相应的计算，MC/DC 覆盖得到相应的输出结果，该输出结果即为目标场景下的可信执行环境（即目标场景下的可信执行环境的具体实现）。

[64]本说明书实施例提供一种可信执行环境的构建方法，通过对获取的可信执行环境的监管要求信息进行解析，得到应用于可信执行环境且原子化的安全功能信息，然后，通过对安全功能信息进行形式化解析处理，得到可证明其满足监管要求信息的可信执行环境的安全方案，并基于可信执行环境的安全方案的公理生成可信执行环境的安全方案对应的测试用例，进而基于可信执行环境的安全方案和可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与该安全方案和该测试用例在预设性质项目上具备相同性质信息的可信执行环境，这样，基于形式化、公理化的形式构建可信执行环境的通用安全方案和通用测试用例等，并在此基础上描述监管要求，使得监管要求和通用安全方案和通用测试用例等技术方案一致且完备，而且，通过本实施例提供的技术方案，可以将监管要求完备且一致的传递或迁移到具体的目标场景下可信执行环境的具体实现中，从而避免不同场景下对监管要求的重复认证，提高了可信执行环境的构建效率。

[65]此外，基于形式化以公理化约束的形式构建可信执行环境通用技术方案，并在此基础上描述监管要求，使得监管要求和通用技术方案一致且完备，另外，通过构建通用技术方案与具体场景下的技术方案之间的同态关系，使得监管要求与具体场景下的技术方案一致且完备，而且，通过构建不同场景下的技术方案之间的自然变换关系，使得监管要求在不同场景之间传递。另外，还基于公理化约束，形成相对于监管要求一致且完备的通用测试用例，以及通过构建通用测试用例与具体场景下的子测试用例之间的同态关系，保持具体场景下的子测试用例相对于监管要求一致且完备，而且，通过构建不同具体场景下的子测试用例之间的自然变换关系，保持不同场景之间的子测试用例相对于监管要求一致且完备。

实施例三

[66]以上为本说明书实施例提供的可信执行环境的构建方法，基于同样的思路，本说明

书实施例还提供一种可信执行环境的构建装置，如图 4 所示。

[67]该可信执行环境的构建装置包括：监管要求获取模块 401、监管要求解析模块 402、处理模块 403 和可信环境构建模块 404，其中：监管要求获取模块 401，获取可信执行环境的监管要求信息；监管要求解析模块 402，对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息；处理模块 403，对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，并基于所述可信执行环境的安全方案的公理生成所述可信执行环境的安全方案对应的测试用例；可信环境构建模块 404，基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境。

[68]本说明书实施例中，所述可信环境构建模块 404，包括：子方案构建单元，基于所述可信执行环境的安全方案，通过同态映射构建所述目标场景下的所述可信执行环境的子安全方案；子用例构建单元，获取所述目标场景下所述可信执行环境的约束信息；结合所述约束信息，并基于所述可信执行环境的安全方案对应的测试用例，通过同态映射构建所述目标场景下的所述可信执行环境的子测试用例；可信环境构建单元，基于所述目标场景下的所述可信执行环境的子测试用例，通过修正判定条件 MC/DC 覆盖生成所述目标场景下的可信执行环境。

[69]本说明书实施例中，所述目标场景包括物联网场景、云端场景和终端设备场景中的一种或多种。

[70]本说明书实施例中，所述目标场景包括多个不同的场景，不同场景下的所述可信执行环境的子安全方案之间通过自然变换的方式进行所述可信执行环境的子安全方案性质的迁移。

[71]本说明书实施例中，所述目标场景包括多个不同的场景，不同场景下的所述可信执行环境的子测试用例之间通过自然变换的方式进行所述可信执行环境的子测试用例性质的迁移。

[72]本说明书实施例中，所述监管要求解析模块 402，包括：安全功能信息获取单元，获取组成所述安全方案的安全功能信息；监管要求解析单元，通过通用信息安全标准 CC，基于获取的组成所述安全方案的安全功能信息对所述监管要求信息进行拆解处理，得到应用于所述可信执行环境且原子化的安全功能信息。

[73]本说明书实施例中，所述原子化的安全功能信息对应的安全功能中不同的安全功能之间满足相互独立且完全穷尽 MECE 规则。

[74]本说明书实施例中，所述处理模块 403，包括：形式化处理单元，对所述安全功能信息进行形式化解析处理，得到所述可信执行环境的预选安全方案；验证单元，基于所述可信执行环境的预选安全方案和所述可信执行环境的监管要求信息，对所述可信执行环境的预选安全方案是否满足所述可信执行环境的监管要求信息进行验证处理，得到相应的验证结果；安全方案确定单元，如果所述验证结果指示所述预选安全方案满足所述可信执行环境的监管要求信息，则将所述预选安全方案作为所述可信执行环境的安全方案。

[75]本说明书实施例中，所述可信执行环境包括通过 SGX 和预设的第一应用程序构建的可信执行环境、通过 Trustzone 和预设的第二应用程序构建的可信执行环境和通过预设的第三应用程序构建的可信执行环境中的一种或多种。

[76]本说明书实施例提供一种可信执行环境的构建装置，通过对获取的可信执行环境的

监管要求信息进行解析,得到应用于可信执行环境且原子化的安全功能信息,然后,通过对安全功能信息进行形式化解析处理,得到可证明其满足监管要求信息的可信执行环境的安全方案,并基于可信执行环境的安全方案的公理生成可信执行环境的安全方案对应的测试用例,进而基于可信执行环境的安全方案和可信执行环境的安全方案对应的测试用例,通过预设的性质迁移机制构建目标场景下与该安全方案和该测试用例在预设性质项目上具备相同性质信息的可信执行环境,这样,基于形式化、公理化的形式构建可信执行环境的通用安全方案和通用测试用例等,并在此基础上描述监管要求,使得监管要求和通用安全方案和通用测试用例等技术方案一致且完备,而且,通过本实施例提供的技术方案,可以将监管要求完备且一致的传递或迁移到具体的目标场景下可信执行环境的具体实现中,从而避免不同场景下对监管要求的重复认证,提高了可信执行环境的构建效率。

[77]此外,基于形式化以公理化约束的形式构建可信执行环境通用技术方案,并在此基础上描述监管要求,使得监管要求和通用技术方案一致且完备,另外,通过构建通用技术方案与具体场景下的技术方案之间的同态关系,使得监管要求与具体场景下的技术方案一致且完备,而且,通过构建不同场景下的技术方案之间的自然变换关系,使得监管要求在不同场景之间传递。另外,还基于公理化约束,形成相对于监管要求一致且完备的通用测试用例,以及通过构建通用测试用例与具体场景下的子测试用例之间的同态关系,保持具体场景下的子测试用例相对于监管要求一致且完备,而且,通过构建不同具体场景下的子测试用例之间的自然变换关系,保持不同场景之间的子测试用例相对于监管要求一致且完备。

实施例四

[78]以上为本说明书实施例提供的可信执行环境的构建装置,基于同样的思路,本说明书实施例还提供一种可信执行环境的构建设备,如图5所示。

[79]所述可信执行环境的构建设备可以为上述实施例提供的服务器或终端设备等。

[80]可信执行环境的构建设备可因配置或性能不同而产生比较大的差异,可以包括一个或一个以上的处理器501和存储器502,存储器502中可以存储有一个或一个以上存储应用程序或数据。其中,存储器502可以是短暂存储或持久存储。存储在存储器502的应用程序可以包括一个或一个以上模块(图示未示出),每个模块可以包括对可信执行环境的构建设备中的一系列计算机可执行指令。更进一步地,处理器501可以设置为与存储器502通信,在可信执行环境的构建设备上执行存储器502中的一系列计算机可执行指令。可信执行环境的构建设备还可以包括一个或一个以上电源503,一个或一个以上有线或无线网络接口504,一个或一个以上输入输出接口505,一个或一个以上键盘506。

[81]具体在本实施例中,可信执行环境的构建设备包括有存储器,以及一个或一个以上的程序,其中一个或者一个以上程序存储于存储器中,且一个或者一个以上程序可以包括一个或一个以上模块,且每个模块可以包括对可信执行环境的构建设备中的一系列计算机可执行指令,且经配置以由一个或者一个以上处理器执行该一个或者一个以上程序包含用于进行以下计算机可执行指令:获取可信执行环境的监管要求信息;对所述监管要求信息进行解析,得到应用于所述可信执行环境且原子化的安全功能信息;对所述安全功能信息进行形式化解析处理,得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案,并基于所述可信执行环境的安全方案的公理生成所述可信执行环境的安全方案对应的测试用例;基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例,通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境。

[82]本说明书实施例中，所述基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境，包括：基于所述可信执行环境的安全方案，通过同态映射构建所述目标场景下的所述可信执行环境的子安全方案；获取所述目标场景下所述可信执行环境的约束信息；结合所述约束信息，并基于所述可信执行环境的安全方案对应的测试用例，通过同态映射构建所述目标场景下的所述可信执行环境的子测试用例；基于所述目标场景下的所述可信执行环境的子测试用例，通过修正判定条件 MC/DC 覆盖生成所述目标场景下的可信执行环境。

[83]本说明书实施例中，所述目标场景包括物联网场景、云端场景和终端设备场景中的一种或多种。

[84]本说明书实施例中，所述目标场景包括多个不同的场景，不同场景下的所述可信执行环境的子安全方案之间通过自然变换的方式进行所述可信执行环境的子安全方案性质的迁移。

[85]本说明书实施例中，所述目标场景包括多个不同的场景，不同场景下的所述可信执行环境的子测试用例之间通过自然变换的方式进行所述可信执行环境的子测试用例性质的迁移。

[86]本说明书实施例中，所述对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息，包括：获取组成所述安全方案的安全功能信息；通过通用信息安全标准 CC，基于获取的组成所述安全方案的安全功能信息对所述监管要求进行拆解处理，得到应用于所述可信执行环境且原子化的安全功能信息。

[87]本说明书实施例中，所述原子化的安全功能信息对应的安全功能中不同的安全功能之间满足相互独立且完全穷尽 MECE 规则。

[88]本说明书实施例中，所述对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，包括：对所述安全功能信息进行形式化解析处理，得到所述可信执行环境的预选安全方案；基于所述可信执行环境的预选安全方案和所述可信执行环境的监管要求信息，对所述可信执行环境的预选安全方案是否满足所述可信执行环境的监管要求信息进行验证处理，得到相应的验证结果；如果所述验证结果指示所述预选安全方案满足所述可信执行环境的监管要求信息，则将所述预选安全方案作为所述可信执行环境的安全方案。

[89]本说明书实施例中，所述可信执行环境包括通过 SGX 和预设的第一应用程序构建的可信执行环境、通过 Trustzone 和预设的第二应用程序构建的可信执行环境和通过预设的第三应用程序构建的可信执行环境中的一种或多种。

[90]本说明书实施例提供一种可信执行环境的构建设备，通过对获取的可信执行环境的监管要求信息进行解析，得到应用于可信执行环境且原子化的安全功能信息，然后，通过对安全功能信息进行形式化解析处理，得到可证明其满足监管要求信息的可信执行环境的安全方案，并基于可信执行环境的安全方案的公理生成可信执行环境的安全方案对应的测试用例，进而基于可信执行环境的安全方案和可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与该安全方案和该测试用例在预设性质项目上具备相同性质信息的可信执行环境，这样，基于形式化、公理化的形式构建可信执行环境的通用安全方案和通用测试用例等，并在此基础上描述监管要求，使得监管要求和通用安全方案和通用测试用例等技术方案一致且完备，而且，通过本实施例提供的技术方案，可以将监管要求完备且一致的传递或迁移到具体的目标场景下可信执行环境的具体实现中，从而避免不同场景下对监管要求的重复认证，提高了可信执行环境的

构建效率。

[91]此外，基于形式化以公理化约束的形式构建可信执行环境通用技术方案，并在此基础上描述监管要求，使得监管要求和通用技术方案一致且完备，另外，通过构建通用技术方案与具体场景下的技术方案之间的同态关系，使得监管要求与具体场景下的技术方案一致且完备，而且，通过构建不同场景下的技术方案之间的自然变换关系，使得监管要求在不同场景之间传递。另外，还基于公理化约束，形成相对于监管要求一致且完备的通用测试用例，以及通过构建通用测试用例与具体场景下的子测试用例之间的同态关系，保持具体场景下的子测试用例相对于监管要求一致且完备，而且，通过构建不同具体场景下的子测试用例之间的自然变换关系，保持不同场景之间的子测试用例相对于监管要求一致且完备。

实施例五

[92]进一步地，基于上述图 1 至图 3 所示的方法，本说明书一个或多个实施例还提供了—种存储介质，用于存储计算机可执行指令信息，—种具体的实施例中，该存储介质可以为 U 盘、光盘、硬盘等，该存储介质存储的计算机可执行指令信息在被处理器执行时，能实现以下流程：获取可信执行环境的监管要求信息；对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息；对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，并基于所述可信执行环境的安全方案的公理生成所述可信执行环境的安全方案对应的测试用例；基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境。

[93]本说明书实施例中，所述基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境，包括：基于所述可信执行环境的安全方案，通过同态映射构建所述目标场景下的所述可信执行环境的子安全方案；获取所述目标场景下所述可信执行环境的约束信息；结合所述约束信息，并基于所述可信执行环境的安全方案对应的测试用例，通过同态映射构建所述目标场景下的所述可信执行环境的子测试用例；基于所述目标场景下的所述可信执行环境的子测试用例，通过修正判定条件 MC/DC 覆盖生成所述目标场景下的可信执行环境。

[94]本说明书实施例中，所述目标场景包括物联网场景、云端场景和终端设备场景中的一种或多种。

[95]本说明书实施例中，所述目标场景包括多个不同的场景，不同场景下的所述可信执行环境的子安全方案之间通过自然变换的方式进行所述可信执行环境的子安全方案性质的迁移。

[96]本说明书实施例中，所述目标场景包括多个不同的场景，不同场景下的所述可信执行环境的子测试用例之间通过自然变换的方式进行所述可信执行环境的子测试用例性质的迁移。

[97]本说明书实施例中，所述对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息，包括：获取组成所述安全方案的安全功能信息；通过通用信息安全标准 CC，基于获取的组成所述安全方案的安全功能信息对所述监管要求信息进行拆解处理，得到应用于所述可信执行环境且原子化的安全功能信息。

[98]本说明书实施例中，所述原子化的安全功能信息对应的安全功能中不同的安全功能之间满足相互独立且完全穷尽 MECE 规则。

[99]本说明书实施例中，所述对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，包括：对所述安全功能信息进行形式化解析处理，得到所述可信执行环境的预选安全方案；基于所述可信执行环境的预选安全方案和所述可信执行环境的监管要求信息，对所述可信执行环境的预选安全方案是否满足所述可信执行环境的监管要求信息进行验证处理，得到相应的验证结果；如果所述验证结果指示所述预选安全方案满足所述可信执行环境的监管要求信息，则将所述预选安全方案作为所述可信执行环境的安全方案。

[100]本说明书实施例中，所述可信执行环境包括通过 SGX 和预设的第一应用程序构建的可信执行环境、通过 Trustzone 和预设的第二应用程序构建的可信执行环境和通过预设的第三应用程序构建的可信执行环境中的一种或多种。

[101]本说明书实施例提供一种存储介质，通过对获取的可信执行环境的监管要求信息进行解析，得到应用于可信执行环境且原子化的安全功能信息，然后，通过对安全功能信息进行形式化解析处理，得到可证明其满足监管要求信息的可信执行环境的安全方案，并基于可信执行环境的安全方案的公理生成可信执行环境的安全方案对应的测试用例，进而基于可信执行环境的安全方案和可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与该安全方案和该测试用例在预设性质项目上具备相同性质信息的可信执行环境，这样，基于形式化、公理化的形式构建可信执行环境的通用安全方案和通用测试用例等，并在此基础上描述监管要求，使得监管要求和通用安全方案和通用测试用例等技术方案一致且完备，而且，通过本实施例提供的技术方案，可以将监管要求完备且一致的传递或迁移到具体的目标场景下可信执行环境的具体实现中，从而避免不同场景下对监管要求的重复认证，提高了可信执行环境的构建效率。

[102]此外，基于形式化以公理化约束的形式构建可信执行环境通用技术方案，并在此基础上描述监管要求，使得监管要求和通用技术方案一致且完备，另外，通过构建通用技术方案与具体场景下的技术方案之间的同态关系，使得监管要求与具体场景下的技术方案一致且完备，而且，通过构建不同场景下的技术方案之间的自然变换关系，使得监管要求在不同场景之间传递。另外，还基于公理化约束，形成相对于监管要求一致且完备的通用测试用例，以及通过构建通用测试用例与具体场景下的子测试用例之间的同态关系，保持具体场景下的子测试用例相对于监管要求一致且完备，而且，通过构建不同具体场景下的子测试用例之间的自然变换关系，保持不同场景之间的子测试用例相对于监管要求一致且完备。

[103]上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[104]在 20 世纪 90 年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array, FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电

路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language, HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHD（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[105]控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit, ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[106]上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[107]为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书一个或多个实施例时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[108]本领域内的技术人员应明白，本说明书的实施例可提供为方法、系统、或计算机程序产品。因此，本说明书一个或多个实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本说明书一个或多个实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[109]本说明书的实施例是参照根据本说明书实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程欺诈案例的串并设备的处理器以产生一个机器，使得通过计算机或其他可编程欺诈案例的串并设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[110]这些计算机程序指令也可存储在能引导计算机或其他可编程欺诈案例的串并设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[111]这些计算机程序指令也可装载到计算机或其他可编程欺诈案例的串并设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[112]在一个典型的配置中,计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[113]内存可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[114]计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带,磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体(transitory media),如调制的数据信号和载波。

[115]还需要说明的是,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[116]本领域技术人员应明白,本说明书的实施例可提供为方法、系统或计算机程序产品。因此,本说明书一个或多个实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且,本说明书一个或多个实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[117]本说明书一个或多个实施例可以在由计算机执行的计算机可执行指令的一般上下文中描述,例如程序模块。一般地,程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书一个或多个实施例,在这些分布式计算环境中,由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中,程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[118]本说明书中的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于系统实施例而言,由于其基本相似于方法实施例,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[119]以上所述仅为本说明书的实施例而已,并不用于限制本说明书。对于本领域技术人员来说,本说明书可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等,均应包含在本说明书的权利要求范围之内。

权利要求书

- 1、一种可信执行环境的构建方法，所述方法包括：
获取可信执行环境的监管要求信息；
对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息；
对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，并基于所述可信执行环境的安全方案的公理生成所述可信执行环境的安全方案对应的测试用例；
基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境。
- 2、根据权利要求 1 所述的方法，所述基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境，包括：
基于所述可信执行环境的安全方案，通过同态映射构建所述目标场景下的所述可信执行环境的子安全方案；
获取所述目标场景下所述可信执行环境的约束信息；结合所述约束信息，并基于所述可信执行环境的安全方案对应的测试用例，通过同态映射构建所述目标场景下的所述可信执行环境的子测试用例；
基于所述目标场景下的所述可信执行环境的子测试用例，通过修正判定条件 MC/DC 覆盖生成所述目标场景下的可信执行环境。
- 3、根据权利要求 2 所述的方法，所述目标场景包括物联网场景、云端场景和终端设备场景中的一种或多种。
- 4、根据权利要求 3 所述的方法，所述目标场景包括多个不同的场景，不同场景下的所述可信执行环境的子安全方案之间通过自然变换的方式进行所述可信执行环境的子安全方案性质的迁移。
- 5、根据权利要求 3 所述的方法，所述目标场景包括多个不同的场景，不同场景下的所述可信执行环境的子测试用例之间通过自然变换的方式进行所述可信执行环境的子测试用例性质的迁移。
- 6、根据权利要求 1 所述的方法，所述对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息，包括：
获取组成所述安全方案的安全功能信息；
通过通用信息安全标准 CC，基于获取的组成所述安全方案的安全功能信息对所述监管要求信息进行拆解处理，得到应用于所述可信执行环境且原子化的安全功能信息。
- 7、根据权利要求 6 所述的方法，所述原子化的安全功能信息对应的安全功能中不同的安全功能之间满足相互独立且完全穷尽 MECE 规则。
- 8、根据权利要求 1 所述的方法，所述对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，包括：
对所述安全功能信息进行形式化解析处理，得到所述可信执行环境的预选安全方案；
基于所述可信执行环境的预选安全方案和所述可信执行环境的监管要求信息，对所述可信执行环境的预选安全方案是否满足所述可信执行环境的监管要求信息进行验证处理，得到相应的验证结果；
如果所述验证结果指示所述预选安全方案满足所述可信执行环境的监管要求信息，则将所述预选安全方案作为所述可信执行环境的安全方案。
- 9、根据权利要求 1-8 中任一项所述的方法，所述可信执行环境包括通过 SGX 和预设的第一应用程序构建的可信执行环境、通过 Trustzone 和预设的第二应用程序构建的

可信执行环境和通过预设的第三应用程序构建的可信执行环境中的一种或多种。

10、一种可信执行环境的构建装置，所述装置包括：

监管要求获取模块，获取可信执行环境的监管要求信息；

监管要求解析模块，对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息；

处理模块，对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，并基于所述可信执行环境的安全方案的公理生成所述可信执行环境的安全方案对应的测试用例；

可信环境构建模块，基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境。

11、根据权利要求10所述的装置，所述可信环境构建模块，包括：

子方案构建单元，基于所述可信执行环境的安全方案，通过同态映射构建所述目标场景下的所述可信执行环境的子安全方案；

子用例构建单元，获取所述目标场景下所述可信执行环境的约束信息；结合所述约束信息，并基于所述可信执行环境的安全方案对应的测试用例，通过同态映射构建所述目标场景下的所述可信执行环境的子测试用例；

可信环境构建单元，基于所述目标场景下的所述可信执行环境的子测试用例，通过修正判定条件MC/DC覆盖生成所述目标场景下的可信执行环境。

12、根据权利要求11所述的装置，所述目标场景包括多个不同的场景，不同场景下的所述可信执行环境的子安全方案之间通过自然变换的方式进行所述可信执行环境的子安全方案性质的迁移。

13、根据权利要求11所述的装置，所述目标场景包括多个不同的场景，不同场景下的所述可信执行环境的子测试用例之间通过自然变换的方式进行所述可信执行环境的子测试用例性质的迁移。

14、一种可信执行环境的构建设备，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：

获取可信执行环境的监管要求信息；

对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息；

对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，并基于所述可信执行环境的安全方案的公理生成所述可信执行环境的安全方案对应的测试用例；

基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境。

15、一种存储介质，所述存储介质用于存储计算机可执行指令，所述可执行指令在被执行时实现以下流程：

获取可信执行环境的监管要求信息；

对所述监管要求信息进行解析，得到应用于所述可信执行环境且原子化的安全功能信息；

对所述安全功能信息进行形式化解析处理，得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案，并基于所述可信执行环境的安全方案的公理生成所述可信执行环境的安全方案对应的测试用例；

基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例，通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境。