

可信状态证明的方法和相关设备

本申请要求于2019年12月31日提交中国国家知识产权局、申请号为201911422163.8、发明名称为“可信状态证明的方法和相关设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5 **技术领域**

本申请涉及网络安全技术领域，具体涉及一种可信状态证明的方法和相关设备。

背景技术

为解决当前网络安全的问题，可信计算组（trusted computing group, TCG）提出了可信计算的方法。通过该可信计算的方法能够证明网络设备是否被非法篡改和破坏。

10 但是，随着组网的日益复杂，证明服务器连接大量的网络设备。大量的网络设备的可信状态的证明均需要依赖于证明服务器。从而增加了证明服务器进行可信状态证明的过程中需要处理的信息量以及证明服务器的负担。若证明服务器被非法篡改，会导致网络设备无法抵御非法篡改和破坏。

发明内容

15 本申请提供了一种可信状态证明的方法和相关设备。其用于解决如何降低证明服务器进行可信状态证明的过程中需要处理的信息量的技术问题。

第一方面，本发明实施例提供了一种可信状态证明的方法，该方法用于网络设备。该网络设备连接于上游设备和下游网络设备之间，该上游设备为该网络设备的上游网络设备或证明服务器，该方法包括：首先，对该网络设备的第一可信证明代理进行度量以获取第一代理度量值，该第一代理度量值用于证明该第一可信证明代理的可信状态；随后，向该上游设备发送该第一代理度量值；最后，接收来自该上游设备的至少一个基线值，该至少一个基线值中的至少部分基线值用于证明该下游网络设备的可信状态。

在该实施方式中，使用处于可信状态的第一可信证明代理承担对下游网络设备的可信状态的证明，有效地降低了证明服务器处理的信息量。此外，该方法在证明服务器出现被非法篡改和破坏的情况下，该第一可信证明代理会独立的实现对下游网络设备的可信状态的证明，提高了可靠性。

在一种可选的实现方式中，该网络设备包括与该第一可信证明代理连接的至少一个第一待证明对象，该方法还包括：获取该至少一个第一待证明对象中每个第一待证明对象的第一度量值，该第一度量值用于证明该第一待证明对象的可信状态；该至少一个基线值包括与该第一待证明对象对应的第一基线值，该接收来自该上游设备的至少一个基线值之后，该方法还包括：根据该第一待证明对象对应的该第一基线值和该第一度量值，证明该第一待证明对象的可信状态。

在该实施方式中，由第一可信证明代理负责对第一待证明对象的可信状态进行证明。因各第一待证明对象的可信状态的证明均无需依赖于证明服务器，有效地降低了证明服务器所处理的信息量。而且在证明服务器出现被攻击的情况下，第一可信证明代理能够独立的实现对第一待证明对象的可信状态的证明，提高了可靠性。

在一种可选的实现方式中，该获取该第一待证明对象的第一度量值之后，该方法还包

-2-

括：将该第一度量值向该上游设备发送。在该实施方式中，处于可信状态的第一可信证明代理，将第一度量值向上游设备发送。由上游设备负责对第一待证明对象的证明，有效地降低了第一可信证明代理所处理的信息量以及该第一待证明对象的负担。

5 在一种可选的实现方式中，该至少一个基线值包括第二基线值，该第二基线值与该下游网络设备的第二可信证明代理对应，该接收来自该上游设备的至少一个基线值之后，该方法还包括：接收来自该下游网络设备的第二代理度量值，该第二代理度量值用于证明该第二可信证明代理的可信状态；根据该第二基线值和该第二代理度量值，证明该第二可信证明代理的可信状态。

10 在该实施方式中，由第一可信证明代理负责对第二可信证明代理的证明，有效地降低了证明服务器所处理的信息量以及证明服务器的负担。

在一种可选的实现方式中，该方法还包括：接收来自该下游网络设备的第二代理度量值，该第二代理度量值用于证明该第二可信证明代理的可信状态；将该第二代理度量值向该上游设备发送。在该实施方式中，由上游设备负责对第二可信证明代理的证明，有效地降低了第一可信证明代理所处理的信息量以及证明服务器的负担。

15 在一种可选的实现方式中，该方法还包括：该至少一个基线值包括第三基线值，该第三基线值与该下游网络设备的第二待证明对象对应，该接收来自该上游设备的至少一个基线值之后，该方法还包括：接收来自该下游网络设备的第二度量值，该第二度量值用于证明该第二待证明对象的可信状态；根据该第二待证明对象对应的该第三基线值和该第二度量值，证明该第二待证明对象的可信状态。

20 在该实施方式中，由处于可信状态的第一可信证明代理承担对第二待证明对象的可信状态的证明，有效地降低了证明服务器处理的信息量以及证明服务器的负担。而且有效地提高了对第二待证明对象进行证明的效率。避免了在证明服务器被非法篡改的情况下，进而篡改第二待证明对象的风险。

25 在一种可选的实现方式中，该至少一个基线值包括第三基线值，该第三基线值与该下游网络设备的第二待证明对象对应，该接收来自该上游设备的至少一个基线值之后，该方法还包括：向该下游网络设备发送该第三基线值。

在该实施方式中，由下游网络设备负责承担对第二待证明对象的可信状态的证明，有效地降低了第一可信证明代理处理的信息量以及负担。此外，该实施方式避免了在第一可信证明代理被非法篡改的情况下，进而篡改下游网络设备的风险。

30 在一种可选的实现方式中，该第一待证明对象和该第一可信证明代理为两个板卡；或，该第一待证明对象和该第一可信证明代理为两个虚拟机；或，该第一待证明对象和该第一可信证明代理为虚拟机、网络功能虚拟化管理和编排系统或网络功能虚拟化基础设施层中的任意两个。

35 第二方面，本发明实施例提供了一种可信状态证明的方法，该方法用于上游设备。对上游设备的说明，参见第一方面所示，不做赘述。该方法包括：首先，接收来自该网络设备的第一代理度量值，该第一代理度量值用于证明该网络设备的第一可信证明代理的可信状态；随后，根据该第一代理度量值证明该第一可信证明代理处于可信状态；最后，向该

网络设备发送至少一个基线值，该至少一个基线值中的至少部分基线值用于证明该下游网络设备的可信状态。

本方面所示的过程以及有益效果的具体说明，参见第一方面所示，不做赘述。

5 在一种可选的实现方式中，该至少一个基线值包括与该网络设备的第一待证明对象对应的第一基线值。

在一种可选的实现方式中，该方法还包括：接收来自该网络设备的第一度量值，该第一度量值用于证明该网络设备的第一待证明对象的可信状态；根据该第一待证明对象对应的第一基线值和该第一度量值，证明该第一待证明对象的可信状态。

10 在一种可选的实现方式中，该至少一个基线值包括第二基线值，该第二基线值与该下游网络设备的第二可信证明代理对应。

在一种可选的实现方式中，该方法还包括：接收来自该网络设备的第二代理度量值，该第二代理度量值用于证明该下游网络设备的第二可信证明代理的可信状态；根据该第二可信证明代理对应的第二基线值和该第二代理度量值，证明该第二可信证明代理的可信状态。

15 在一种可选的实现方式中，该至少一个基线值包括第三基线值，该第三基线值与该下游网络设备的第二待证明对象对应。

第三方面，本发明实施例提供了一种网络设备，该网络设备包括第一可信证明代理，该第一可信证明代理用于执行上述第一方面所示的可信状态证明的方法，具体执行过程以及有益效果的说明，参见第一方面所示。

20 第四方面，本发明实施例提供了一种上游网络设备，该上游网络设备包括可信证明代理，该上游网络设备包括可信证明代理用于执行上述第二方面所示的可信状态证明的方法，具体执行过程以及有益效果的说明，参见第二方面所示。

第五方面，本发明实施例提供了一种证明服务器，该证明服务器、网络设备和下游网络设备依次连接，该证明服务器包括处理器、存储器以及光收发器，其中，该处理器通过
25 线路分别与该存储器以及该光收发器通过线路互联；该光收发器用于执行第二方面所示的收发相关操作，该处理器用于执行第二方面所示的处理相关操作，具体执行过程以及有益效果的说明，参见第二方面所示。

第六方面，本发明实施例提供了一种通信系统。该通信系统包括上游设备、网络设备和下游网络设备。该上游设备如第四方面或第五方面所示，该网络设备如第三方面所示，
30 不做赘述。

第七方面，本发明实施例提供了一种计算机可读存储介质，包括指令，当该指令在计算机上运行时，使得该计算机执行上述第一方面或其任意具体实现方式所示的方法，不做赘述。

第八方面，本发明实施例提供了一种包含指令的计算机程序产品，当该计算机程序产品在计算机上运行时，使得该计算机执行上述第一方面或其任意具体实现方式所示的方法，
35 不做赘述。

附图说明

—4—

图 1 为可信状态证明应用的通信架构第一种示意图；

图 2 为本发明所提供的网络设备的第一种实施例结构示例图；

图 3 为本发明所提供的网络设备的第二种实施例结构示例图；

图 4 为本发明所提供的可信状态证明方法的第一种实施例步骤流程图；

5 图 5 为本发明所提供的可信状态证明方法的第二种实施例步骤流程图；

图 6 为可信状态证明应用的通信架构第二种示意图；

图 7 为本发明所提供的第一待证明对象的系统架构示例性；

图 8 为本发明所提供的可信状态证明方法的第三种实施例步骤流程图；

图 9 为本发明所提供的可信状态证明方法的第四种实施例步骤流程图；

10 图 10 为本发明所提供的证明服务器的一种实施例结构图。

具体实施方式

首先，对本申请所提供的可信状态证明的方法所应用的通信系统的架构进行说明。图 1 为可信状态证明方法应用的通信架构示意图。如图 1 所示，该通信系统包括证明服务器 101 和网络设备集群 102。其中，网络设备集群 102 内包括多个网络设备。证明服务器 101 与 15 各网络设备连接。相互连接的证明服务器 101 与网络设备进行信息交互，以实现对各网络设备的可信状态的证明。以下结合具体示例对证明服务器 101 与各网络设备之间的连接方式进行说明。

例如，该网络设备集群 102 所包括的网络设备 1021 与证明服务器 101 直接连接。具体地，该网络设备 1021 直接与证明服务器 1021 创建传输控制协议 20 (transmission control protocol, TCP) 连接。或者证明服务器 101 与网络设备 1021 之间还可创建网际互连协议 (internet protocol, IP) 等其他连接。对此，本申请不做限定。

又如，该网络设备集群 102 所包括的网络设备 1022 与证明服务器 101 间接连接。其中，间接连接的该证明服务器 101 与该网络设备 1022 之间，间隔有一个或多个其他网络设备。 25 具体地，该网络设备 1022 经由网络设备 1021 与该证明服务器 101 间接连接。对网络设备集群 102 所包括的其他网络设备与证明服务器 101 的连接关系的说明，参见网络设备 1021 或网络设备 1022 的说明，不做赘述。

以下对各网络设备内部的结构进行说明：

该网络设备包括至少一个待证明对象。本申请以网络设备包括多个待证明对象为例。

30 其中，多个待证明对象在网络设备内分别独立启动或运行。且不同的待证明对象在网络设备内可通过背板总线、进程间通信等方式进行信息交互。为更好的理解，以下对待证明对象可能的实现方式进行示例性说明。

方式 1：图 2 为本发明所提供的网络设备的第一种实施例结构示例图。如图 2 所示，网络设备 200 包括多个业务板卡（如业务板卡 2011、业务板卡 2012 至业务板卡 201N）。图 35 2 所示对业务板卡的数量不做限定。业务板卡 2011、业务板卡 2012 至业务板卡 201N 分别通过背板总线 204 连接系统控制板卡 202 和系统时钟板卡 203。图 2 所示对系统控制板卡 202 和系统时钟板卡 203 的数量的说明为可选地示例，不做限定。

-5-

该系统时钟板卡 203 用于进行时钟同步。该系统控制板卡 202 用于对业务板卡进行控制。控制方式包括但不限于软件的升降级、业务数据配置、告警的收集和上报等。业务板卡用于对业务数据进行处理。处理方式包括但不限于汇聚、传输、路由或交换等。其中，该待证明对象可为所有业务板卡、系统控制板卡 202 和系统时钟板卡 203 中的全部或部分。

5 方式 2：图 3 为本发明所提供的网络设备的第二种实施例结构示意图。如图 3 所示，网络设备 300 采用网络功能虚拟化（network function virtualization, NFV）技术。通过 NFV 实现网络设备 300 的应用与硬件之间的解耦。该网络设备 300 包括 NFV 管理和编排系统（NFV management and orchestration, NFV MANO）301、NFV 基础设施层（NFV Infrastructure, NFVI）302 和多个虚拟机 303。该 NFV MANO301 分别与 NFVI302 以及各虚拟机 303 连接。其中，NFV MANO301 用于执行对虚拟机 303 和 NFVI302 的管理。NFVI302 通过其包括的硬件资源、软件资源或两者的组合来完成虚拟化资源的部署。该 NFVI302 向虚拟机 303 提供虚拟化资源。其中，该待证明对象可为所有虚拟机 303、NFV MANO301 以及 NFVI302 中的全部或部分。

15 图 4 为本发明所提供的可信状态证明方法的第一种实施例步骤流程图。以下结合图 4 所示对本申请所提供的可信状态证明方法的具体执行过程进行说明。

步骤 401、第一可信证明代理获取第一代理度量值。

本实施例所示的第一可信证明代理位于目标网络设备内。该第一可信证明代理用于执行可信状态的证明。以下首先对目标网络设备在通信网络中的连接位置进行说明：

20 本实施例所示的目标网络设备连接于上游设备和下游网络设备之间。其中，该上游设备可为连接于目标网络设备和证明服务器之间的一个或多个网络设备中的任一个。该上游设备还可为证明服务器。如图 1 所示，目标网络设备 1023 的上游设备可为网络设备 1022、网络设备 1201 以及证明服务器 101 中的任一个。

25 该下游网络设备为需要经由该目标网络设备与证明服务器间接连接的一个或多个网络设备中的任一个。对间接连接的说明，详见图 1 所示，不做赘述。又如，目标网络设备 1023 的下游网络设备为网络设备 1024。

30 在一种具体的实现方式中，该第一可信证明代理可为图 2 所示的业务板卡。且该第一可信证明代理与待证明对象为互不相同的业务板卡。例如，待证明对象为业务板卡 2011、业务板卡 2012，而该第一可信证明代理为业务板卡 201N。此种示例下，该待证明对象还可为系统控制板卡 202 以及系统时钟板卡 203。

30 该第一可信证明代理可为运行在系统控制板卡 202 内的代码段。该待证明对象为该目标网络设备 200 所包括的所有业务板卡以及系统时钟板卡 203。或者，该第一可信证明代理可为运行在系统时钟板卡 203 内的代码段。该待证明对象为该目标网络设备 200 所包括的所有业务板卡以及系统控制板卡 202。

35 在另一种具体的实现方式中，该第一可信证明代理可为图 3 所示的虚拟机。且该第一可信证明代理与待证明对象为互不相同的虚拟机。该第一可信证明代理可为运行在 NFV MANO301 内的代码段。该待证明对象为目标网络设备 300 所包括的所有虚拟机以及 NFVI302。或者，该第一可信证明代理可为运行在 NFVI302 内的代码段。该待证明对象为目标网络设

备 300 所包括的所有虚拟机以及 NFV MANO301。

该第一可信证明代理用于对下游网络设备进行可信状态的证明。为保障可信状态证明的准确性和安全性，需要获取第一代理度量值。该第一代理度量值用于证明该第一可信证明代理的可信状态。以下对获取该第一代理度量值的过程进行说明：

5 该第一可信证明代理对其自身进行度量以获取该第一代理度量值。具体地，以第一可信证明代理为代码段为例。该第一可信证明代理对整个第一可信证明代理的代码段进行密码学运算以获取该第一代理度量值。本实施例对密码学运算的具体算法类型不做限定。例如，密码学运算可为哈希、对称加密（SM1）或非对称加密（SM2）等。若第一可信证明代理为系统控制板卡或 NFV MANO301，则对整个第一可信证明代理进行静态度量或动态度量以获取该第一代理度量值。

10 步骤 402、第一可信证明代理向上游设备发送第一代理度量值。

本实施以第一可信证明代理直接向上游设备发送该第一代理度量值为例进行说明。在其他示例中，还可由第一可信证明代理经由该目标网络设备内的其他对象（例如，网络设备内的路由板卡）间接的向上游设备发送该第一代理度量值。具体在本实施例中不做限定。

15 步骤 403、上游设备接收第一代理度量值。

上游设备根据该第一代理度量值证明该第一可信证明代理是否处于可信状态。具体地，该上游设备可预先存储有第一代理基线值。上游设备判断该第一代理度量值与该第一代理基线值是否一致。

20 若否，则上游设备确定该第一可信证明代理处于不可信的状态。一种示例，该上游设备可向该第一可信证明代理发送重证明信息。重证明信息用于指示该第一可信证明代理重新执行上述步骤 401。另一种示例，该上游设备可生成结果指示信息，该结果指示信息用于指示该第一可信证明代理处于不可信的状态。基于该指示信息以实现对该第一可信证明代理的分析处理。若是，则该上游设备确定该第一可信证明代理处于可信状态。进而触发步骤 404 的执行。

25 步骤 404、上游设备向第一可信证明代理发送至少一个基线值。

本实施例所示的至少一个基线值中至少部分基线值用于证明下游网络设备的可信状态。具体地，该至少一个基线值包括与下游网络设备的第二可信证明代理对应的基线值。和/或，该至少一个基线值包括与下游网络设备的待证明对象对应的基线值。对第二可信证明代理的具体说明，可参见步骤 401 所示的对第一可信证明代理的说明，不做赘述。

30 步骤 405、第一可信证明代理接收该至少一个基线值。

该第一可信证明代理根据该至少一个基线值确定其处于可信状态。

步骤 406、第一可信证明代理对下游网络设备的可信状态进行证明。

35 处于可信状态的第一可信证明代理对下游网络设备的可信状态进行证明。具体地，该第一可信证明代理根据该至少一个基线值证明该第二可信证明代理的可信状态。和/或，该第一可信证明代理根据该至少一个基线值证明下游网络设备的待证明对象的可信状态。

采用本实施例所示的方法，由处于可信状态的第一可信证明代理承担对下游网络设备的可信状态的证明，有效地降低了证明服务器处理的信息量。在证明服务器出现被非法篡

改和破坏的情况下,该第一可信证明代理会独立的实现对下游网络设备的可信状态的证明,有效地提高了下游网络设备的可靠性以及对下游网络设备的可信状态证明的准确性。此外,该方法避免了在证明服务器被非法篡改的情况下,进而篡改下游网络设备的风险,有效提升了下游网络设备的可靠性。

5 图 5 为本发明所提供的可信状态证明方法的第二种实施例步骤流程图。以下结合图 5 所示,对目标网络设备的待证明对象的可信状态的证明过程进行示例性说明。本实施例所示由第一可信证明代理负责对目标网络设备的待证明对象的可信状态进行证明。

步骤 501、第一可信证明代理与上游设备创建第一安全通道。

10 对上游设备的说明,参见图 4 所示,不做赘述。图 6 为可信状态证明应用的通信架构第二种示意图。以图 6 所示为例,该第一可信证明代理为所属于目标网络设备 64 的可信证明代理 641。该可信证明代理 641 与所属于上游网络设备 62 的可信证明代理 621 创建第一安全通道。又如,该第一可信证明代理为所属于目标网络设备 62 的可信证明代理 621。该可信证明代理 621 与证明服务器 61 创建第一安全通道。

15 基于该第一安全通道实现第一可信证明代理和上游设备之间所交互的信息的安全。具体地,第一可信证明代理和上游设备之间基于安全传输层(transport layer security, TLS)、互联网安全协议(internet protocol security, IPsec)或共享密钥等方式,互相进行身份认证以及协商密钥。在经过身份认证和密码协商后,该第一安全通道创建成功。可见,该第一安全通道为加密的安全通道。

步骤 502、第一可信证明代理通过第一安全通道接收来自上游设备的度量代理请求。

20 该度量代理请求用于指示该第一可信证明代理对其自身进行度量以获取代理度量值。例如,若目标网络设备为网络设备 61,则第一可信证明代理 621 经由第一安全通道接收来自证明服务器 61 的度量代理请求。又如,若目标网络设备为网络设备 64,则第一可信证明代理 641 经由第一安全通道接收来自可信证明代理 621 的度量代理请求。其中,该第一可信证明代理 621 用于将来自证明服务器 61 的该度量代理请求向可信证明代理 641 转发。

25 步骤 503、第一可信证明代理根据度量代理请求获取第一代理度量值。

步骤 504、第一可信证明代理通过第一安全通道向上游设备发送第一代理度量值。

步骤 505、上游设备通过第一安全通道接收第一代理度量值。

步骤 503 至 505 的说明,详见图 4 所示的步骤 401 至 403 的描述,不做赘述。

步骤 506、上游设备通过第一安全通道向第一可信证明代理发送至少一个基线值。

30 其中,该至少一个基线值包括与第一待证明对象对应的第一基线值。该第一待证明对象为目标网络设备所包括的待证明对象。具体地,该目标网络设备内的第一可信证明代理分别与多个第一待证明对象连接。

步骤 507、第一可信证明代理通过第一安全通道接收该至少一个基线值。

步骤 508、第一可信证明代理对下游网络设备的可信状态进行证明。

35 步骤 507 至步骤 508 的说明,详见图 4 所示的步骤 405 至步骤 406 的描述,不做赘述。

步骤 509、第一可信证明代理向第一待证明对象发送度量请求。

在第一可信证明代理处于可信状态下,该第一可信证明代理通过该度量请求获取各第

一待证明对象的第一度量值。该第一可信证明代理可周期性向第一待证明对象发送该度量请求。以实现周期性的对第一待证明对象的可信状态的证明。或者，该第一可信证明代理也可基于触发事件向第一待证明对象发送该度量请求。该触发事件可为第一待证明对象复位、初始上电或者基于网管人员输入的命令。

5 本实施例所示的步骤 508 和步骤 509 之间，并无执行时序上的前后限定。

步骤 510、第一待证明对象根据该度量请求生成第一度量值。

为实现对各第一待证明对象的可信状态的证明，则需要每个第一待证明对象生成第一度量值。本实施例对第一待证明对象所生成的第一度量值的具体数量不做限定。具体地，该第一待证明对象可包括有多个子对象。第一待证明对象针对各子对象生成对应的第一度量值。其中，各子对象对应的第一度量值用于证明该子对象的可信状态。可见，本实施例
10 通过对各子对象的可信状态的证明，以完成对第一待证明对象的可信状态的证明。

具体地，通过对第一待证明对象在系统启动阶段中进行静态度量以证明可信状态。其中，该第一待证明对象所包括的子对象可为基本输入输出系统(basic input output system, BIOS)、操作系统加载器(operator system loader, OSLoader)、操作系统(operating system, OS)以及该 OS 所启动的应用等。
15

在经由静态度量以证明该第一待证明对象在系统启动阶段处于可信状态。随后对第一待证明对象在系统运行阶段进行动态度量。该第一待证明对象所包括子对象为第一待证明对象上正在运行的进程。

图 7 为本发明所提供的第一待证明对象的系统架构示例性。以下结合图 7 所示对第一待证明对象进行静态度量的过程进行说明：
20

该第一待证明对象包括可信度量核心根(core root of trust for measurement, CRTM) 701。该 CRTM701 无需进行度量即可确定其处于可信状态。该 CRTM701 作为证明第一待证明对象的可信状态的信任链的起点。本实施例对 CRTM701 的具体形态不做限定。例如，若第一待证明对象为业务板卡，则 CRTM701 为设置在第一待证明对象内的独立芯片。该 CRTM701 为信任的根源(root of trust, RoT)。又如，该 CRTM701 可为运行在第一待证明对象上的受硬件保护的一段代码。
25

首先，该第一待证明对象上电后，运行该 CRTM701。已运行的 CRTM701 对作为子对象的 BIOS702 进行度量以获取 BIOS702 的第一度量值。该 CRTM701 将 BIOS702 的第一度量值存储至可信平台模块(trusted platform module, TPM) 703。本实施例所示的 TPM703 可为第一待证明对象所包括的独立的 TPM 芯片、基于固件的 TPM 模块(firmware TPM, fTPM)或基于虚拟可信平台模块(virtual TPM, vTPM)等。且该 TPM703 包括独立的存储空间。该存储空间可为平台配置寄存器(platform configuration register, PCR)。
30

随后，BIOS702 对作为子对象的 OSLoader704 进行度量以获取 OSLoader704 的第一度量值。该 BIOS702 将 OSLoader704 的第一度量值向 TPM703 发送。随后，OSLoader704 在加载 OS705 之前，对作为子对象的 OS705 进行度量以获取 OS705 的第一度量值。该 OSLoader704 将 OS705 的第一度量值向 TPM703 发送。OS705 启动后，由 OS705 对作为子对象的应用 706 进行度量以获取应用 706 的第一度量值。该 OS705 将应用 706 的第一度量值向 TPM703 发送。
35

该第一待证明对象将已获取的各第一度量值向第一可信证明代理发送。本实施例对具体的发送方式不做限定，例如，由应用 706 访问 TPM703，以将上述所示的各子对象的第一度量值向第一可信证明代理发送。

5 该第一待证明对象在系统启动阶段完成静态度量后，第一待证明对象即可进行对自身运行态数据的可信状态进行动态度量。具体地，该运行态数据可为第一待证明对象上正在运行的进程、内存中的代码段和/或数据段等。将运行态数据进行度量以获取该子对象的第一度量值。

需明确的是，若第一可信证明代理为独立的系统控制板卡、系统时钟板卡、业务板卡、虚拟机、NFV MANO 或 NFVI，则本实施例所示的静态度量或动态度量过程，也可适用于对第一可信证明代理的度量过程。

步骤 511、第一可信证明代理获取第一待证明对象的第一度量值。

步骤 512、第一可信证明代理证明第一待证明对象的可信状态。

15 该第一可信证明代理根据第一待证明对象对应的第一基线值和第一度量值，证明第一待证明对象的可信状态。具体地，该第一可信证明代理判断子对象对应的第一基线值与该子对象的第一度量值是否一致。若是，则第一可信证明代理确定该子对象处于可信状态。若否，则第一可信证明代理确定该子对象处于不可信状态。

以目标网络设备为网络设备 62 为例。在第一可信证明代理 621 获取到第一基线值的情况下，即可对所属于该目标网络设备 62 的第一待证明对象 622 以及第一待证明对象 623 进行可信状态证明。

20 例如，若需证明第一待证明对象 622 的 BIOS 的可信状态，第一可信证明代理 621 判断来自证明服务器 61 的 BIOS 对应的第一基线值与 BIOS 的第一度量值是否一致。若是，则第一可信证明代理 621 确定该 BIOS 处于可信状态。若否，则第一可信证明代理 621 确定该 BIOS 处于不可信状态。

25 图 5 所示的实施例中，由目标网络设备内的第一可信证明代理负责证明第一待证明对象的可信状态为例进行示例性说明。在其他示例中，也可由上游设备负责证明该第一待证明对象的可信状态。负责对第一待证明对象的可信状态进行证明的上游设备可为与目标网络设备直接或间接连接的网络设备，也可为该证明服务器，具体不做限定。

若由上游设备负责对第一待证明对象的可信状态进行证明，则该第一可信证明代理将该第一度量值转发给该上游设备。

30 所属于目标网络设备 66 的第一可信证明代理 661 将第一度量值依次经由网络设备 64 和网络设备 62 发送至证明服务器 61。由该证明服务器 61 对第一待证明对象 662 以及待证明对象 663 的可信状态进行证明。又如，该第一可信证明代理 661 可将第一度量值直接发送给可信证明代理 641。由可信证明代理 641 负责对第一待证明对象 662 以及待证明对象 663 的可信状态进行证明。

35 一种示例，第一可信证明代理可向证明服务器发送指示信息。该指示信息用于指示各第一待证明对象的可信状态。另一种示例，还可由证明服务器向第一可信证明代理发送查询请求。第一可信证明代理根据该查询请求将指示信息发送给证明服务器。从而使得证明

服务器能够查询到各第一待证明对象的可信状态。

随着组网的复杂化，目标网络设备会包括多个第一待证明对象。采用本实施例所示的方法，证明服务器无需对各第一待证明对象分别进行独立的证明。而是直接由目标网络设备的第一可信证明代理负责对第一待证明对象的可信状态进行证明。因各第一待证明对象的可信状态的证明均无需依赖于证明服务器，从而有效地降低了证明服务器所处理的信息量。而且在证明服务器出现被攻击的情况下，第一可信证明代理能够独立的实现对第一待证明对象的可信状态的证明，提高可靠性。

图 8 为本发明所提供的可信状态证明方法的第三种实施例步骤流程图。图 9 为本发明所提供的可信状态证明方法的第四种实施例步骤流程图。以下结合图 8 和图 9 所示，对下游网络设备的可信状态的证明过程进行说明。该下游网络设备包括第二可信证明代理和与该第二可信证明代理连接的一个或多个第二待证明对象。本实施例以多个第二待证明对象为例进行说明。对第二可信证明代理的说明，参见图 4 所示对第一可信证明代理的说明，不做赘述。对第二待证明对象的具体说明，参见图 4 所示对第一待证明对象的说明，不做赘述。

步骤 801、上游设备向第一可信证明代理发送多个基线值。

在上游设备确定第一可信证明代理处于可信状态的情况下，向该第一可信证明代理发送多个基线值。上游设备确定第一可信证明代理处于可信状态的过程的说明，详见图 5 所示的步骤 501 至步骤 505 所示，不做赘述。

本实施例中，由第一可信证明代理负责对第二可信证明代理以及第二待证明对象的可信状态的证明。该多个基线值中包括第二基线值和第三基线值。其中，该第二基线值与第二可信证明代理对应。第三基线值与第二待证明对象对应。

可选地，该上游设备根据隶属关系向第一可信证明代理发送该多个基线值。例如，如图 6 所示，该隶属关系用于指示目标网络设备 64 以及隶属该目标网络设备 64 的下游网络设备 66。此种示例下，该上游设备所生成的第二基线值与第二可信证明代理 661 对应。该第三基线值与第二待证明对象 662 以及 663 对应。

步骤 802、第一可信证明代理和第二可信证明代理创建第二安全通道。

该第一可信证明代理和第二可信证明代理创建第二安全通道的过程的说明，请参见图 5 的步骤 501 所示创建第一安全通道的过程，不做赘述。通过该第二安全通道，保障了第一可信证明代理和第二可信证明代理之间所交互的信息的安全。

步骤 801 和步骤 802 之间，并无执行时序上的前后限定。

步骤 803、第一可信证明代理通过第二安全通道向第二可信证明代理发送下游度量代理请求。

其中，该下游度量代理请求用于请求获取该第二可信证明代理的第二代理度量值。第二代理度量值用于证明第二可信证明代理的可信状态。

步骤 804、第二可信证明代理根据下游度量代理请求获取第二代理度量值。

本实施例所示的步骤 809 所示，请参见图 5 所示的步骤 503 所示，不做赘述。

步骤 805、第二可信证明代理通过第二安全通道向第一可信证明代理发送第二代理度

量值。

步骤 806、第一可信证明代理通过第二安全通道接收第二代理度量值。

步骤 807、第一可信证明代理对第二可信证明代理的可信状态进行证明。

由步骤 801 所示可知，该第一可信证明代理已接收到第二基线值，则第一可信证明代理判断该第二代理度量值是否与该第二基线值一致。

若是，则说明该第二代理度量值处于可信状态。若否，则说明该第二代理度量值处于不可信状态。该第二代理度量值处于不可信状态的说明，可见步骤 403 所示第一可信证明代理处于不可信状态的说明，不做赘述。

步骤 808、第一可信证明代理通过第二安全通道向第二可信证明代理发送第四基线值。

为了更好的理解，以下结合图 6 所示进行说明。该目标网络设备 62 的第一可信证明代理 621 从上游设备（证明服务器 61）所接收到的多个基线值中还可包括第四基线值。第四基线值用于证明从属于下游网络设备 64 的待证明对象（662 以及 663）的可信状态。

具体地，第一可信证明代理 621 确定下游网络设备 64 的第二可信证明代理 641 处于可信状态。该第一可信证明代理 621 即可将第四基线值向第二可信证明代理 641 发送。

该第二可信证明代理 641 可基于该第四基线值对从属于下游网络设备 64 的待证明对象（662 以及 663）的可信状态进行证明。或者，该第二可信证明代理还可将该第四基线值发送给从属于下游网络设备 64 的可信证明代理 661。由从属于下游网络设备 64 的可信证明代理 661 根据该第四基线值对从属于下游网络设备 641 的待证明对象（662 以及 663）进行证明。

本实施例以第一可信证明代理负责对第二可信证明代理的可信状态进行证明为例。在其他示例中，也可由上游设备负责对第二可信证明代理的可信状态进行证明。在此种示例下，该第一可信证明代理可通过第一安全通道向上游设备发送该第二代理度量值。其中，上游设备对第二可信证明代理的证明过程的说明，请参见第一可信证明代理对第二可信证明代理的证明过程，不做赘述。因由上游设备负责对第二可信证明代理进行证明，则上游设备发送至第一可信证明代理的多个基线值中，不包括该第二基线值。

步骤 809、第一可信证明代理通过第二安全通道向第二可信证明代理发送下游度量请求。

该下游度量请求用于获取各第二待证明对象的第二度量值。该第二可信证明代理将已获取的下游度量请求转发至各第二待证明对象。各第二待证明对象即可根据该下游度量请求进行度量以获取第二度量值。其中，该第二待证明对象获取第二度量值的具体过程，请参见图 5 所示的步骤 510 所示的第一待证明对象获取第一度量值的过程，不做赘述。

本实施例所示的步骤 808 和步骤 809 之间并无执行时序上的前后续定。

步骤 810、第二可信证明代理获取来自第二待证明对象的第二度量值。

步骤 811、第二可信证明代理通过第二安全通道向第一可信证明代理发送第二度量值。

步骤 812、第一可信证明代理通过第二安全通道接收第二度量值。

步骤 813、第一可信证明代理证明第二待证明对象的可信状态。

该第一可信证明代理根据第二待证明对象对应的第三基线值和第二度量值，证明第二

待证明对象的可信状态。具体过程详见步骤 512 中第一待证明对象的证明过程，不做赘述。

采用本实施例所示的方法，由处于可信状态的第一可信证明代理承担对第二可信证明代理和第二待证明对象的可信状态的证明，有效地降低了证明服务器处理的信息量。而且有效地提高了对第二可信证明代理以及第二待证明对象进行证明的效率。避免了在证明服务器被非法篡改的情况下，进而篡改第二可信证明代理以及第二待证明对象的风险。

以下结合图 9 所示对下游网络设备的可信状态的证明过程的另一个实施例进行说明。

步骤 901、上游设备向第一可信证明代理发送多个基线值。

相对于图 8 所示的实施例，本实施例由第一可信证明代理负责对该第二可信证明代理的可信状态进行证明。由第二可信证明代理负责对该第二待证明对象的可信状态进行证明。此种示例下，该多个基线值包括第二基线值和第三基线值。对第二基线值和第三基线值的说明，详见步骤 801 所示，不做赘述。

步骤 901 至步骤 910 可参见图 8 所示的步骤 802 至步骤 810 的相关描述，在此不做赘述。

步骤 911、第一可信证明代理通过第二安全通道向第二可信证明代理发送第三基线值。

步骤 912、第二可信证明代理通过第二安全通道接收第三基线值。

步骤 913、第二可信证明代理证明第二待证明对象的可信状态。

第二可信证明代理根据第二待证明对象对应的第三基线值和第二度量值，证明第二待证明对象的可信状态。具体过程参见步骤 512 中第一待证明对象的证明过程，不做赘述。

采用本实施例所示的方法，由处于可信状态的第一可信证明代理承担对第二可信证明代理的证明。由第二可信证明代理负责对该第二待证明对象的可信状态的证明。有效地降低了目标网络设备处理的信息量。此外，还可以避免了在目标网络设备被非法篡改的情况下，进而篡改下游网络设备的风险。

本申请实施例提供了一种网络设备。以图 6 所示的通信系统的网络设备 64 为例。该网络设备 64 包括可信证明代理 641 以及与该可信证明代理 641 连接的一个或多个待证明对象。对可信证明代理 641 以及待证明对象的说明可参见图 1 至图 4 所示，不做赘述。

若本实施例所示的网络设备 64 为上述方法实施例所示的目标网络设备。在图 4 中，该可信证明代理 641 用于执行步骤 401、步骤 402、步骤 405 以及步骤 406。在图 5 中，该可信证明代理 641 用于执行步骤 501 至步骤 504、步骤 507 至步骤 509 以及步骤 511 至步骤 512。以待证明对象 642 为例，该待证明对象 642 用于执行步骤 510。在图 8 中，该可信证明代理 641 用于执行步骤 802 至步骤 803、步骤 806 至步骤 809 以及步骤 812 至步骤 813。在图 9 中，该可信证明代理 641 用于执行步骤 902 至步骤 903、步骤 906 至步骤 909 以及步骤 911。

若本实施例所示的网络设备 64 为上述方法实施例所示的下游网络设备。在图 8 中，该可信证明代理 641 用于执行步骤 804 至步骤 805 以及步骤 810 至步骤 811。在图 9 中，该可信证明代理 641 用于执行步骤 904 至步骤 905、步骤 910 以及步骤 912 至步骤 913。

若本实施例所示的网络设备 64 为上述方法实施例中的上游设备。此种示例下，该目标网络设备 66 还连接有一个或多个下游网络设备。在图 4 中，该上游设备 64 的可信证明代

— 13 —

理 641 用于执行步骤 403 至步骤 404。在图 5 中，该可信证明代理 641 用于执行步骤 501 以及步骤 505 至步骤 506。在图 8 中，该可信证明代理 641 用于执行步骤 801。在图 9 中，该可信证明代理 641 用于执行步骤 901。

5 本申请提供了一种证明服务器。图 10 为本发明所提供的证明服务器的一种实施例结构图。如图 10 所示，该证明服务器包括处理器 1001、存储器 1002 和光收发器 1003。该处理器 1001 通过线路与存储器 1002 和光收发器 1003 互联。

其中，该光收发器 1003 用于执行与目标网络设备之间的，如上述任一方法实施例所示的收发相关操作。存储器 1002 用于存储程序指令和数据。处理器 1001 执行该程序指令和数据以完成如上述任一方法实施例所示的处理操作。具体参见上述方法实施例，不做赘述。

10 以上实施例仅用以说明本发明的技术方案，而非对其限制。尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

15