(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114866409 B
(45)授权公告日 2024.03.26

(21)申请号 202210457729.6
(22)申请日 2022.04.27
(65)同一申请的已公布的文献号
申请公布号 CN 114866409 A
(43)申请公布日 2022.08.05
(73)专利权人 阿里巴巴(中国)有限公司
地址 311121 浙江省杭州市余杭区五常街道文一西路969号3幢5层554室
(72)发明人 丁宁
(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
专利代理师 李威
(51)Int.Cl.
H04L 41/08(2022.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 104811450 A,2015.07.29
CN 110581829 A,2019.12.17
US 2021176059 A1,2021.06.10
WO 2021227879 A1,2021.11.18
CN 111800378 A,2020.10.20
CN 106454528 A,2017.02.22
CN 111614637 A,2020.09.01
CN 113098833 A,2021.07.09
CN 113204760 A,2021.08.03

审查员 陈幂

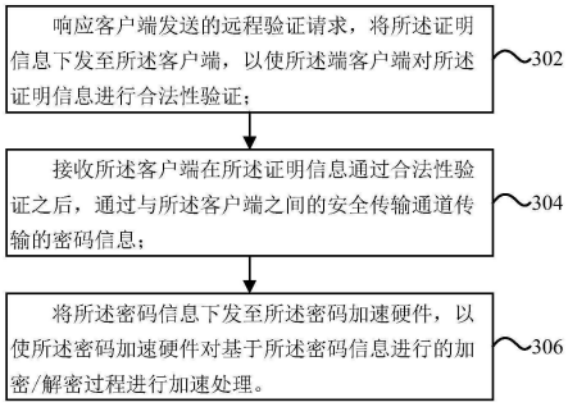
权利要求书2页 说明书8页 附图3页

(54)发明名称

基于密码加速硬件的密码加速方法及装置

(57)摘要

本说明书一个或多个实施例提供一种基于密码加速硬件的密码加速方法及装置。该方法包括:响应于客户端发送的远程验证请求,将证明信息下发至所述客户端,以使所述客户端对所述证明信息进行合法性验证;接收客户端在所述证明信息通过合法性验证之后,通过与所述客户端之间的安全传输通道传输的密码信息;将所述密码信息下发至密码加速硬件,以使密码加速硬件对基于所述密码信息进行的加密/解密过程进行加速处理。



CN 114866409 B

1.一种基于密码加速硬件的密码加速方法,应用于云服务器,所述云服务器包括密码加速硬件,所述密码加速硬件上的安全存储器存储了证明信息和所述云服务器的设备信息,所述证明信息用于证明所述云服务器的运行环境的合法性;所述设备信息用于生成所述证明信息,所述方法包括:

将所述设备信息通过与第三方证明服务器之间的安全传输通道传输至所述证明服务器,以使证明服务器基于所述设备信息生成所述证明信息;通过所述安全传输通道接收所述证明服务器传输的证明信息,并将所述证明信息下发至所述密码加速硬件上的安全存储器进行存储;

响应于客户端发送的远程验证请求,将所述证明信息下发至所述客户端,以使所述客户端将所述证明信息发送至第三方证明服务器,以由第三方证明服务器对所述证明信息进行合法性验证;

接收所述客户端在所述证明信息通过合法性验证之后,通过与所述客户端之间的安全传输通道传输的密码信息;

将所述密码信息下发至所述密码加速硬件,以使所述密码加速硬件对基于所述密码信息进行的加密/解密过程进行加速处理。

2.根据权利要求1所述的方法,所述密码加速硬件包括密码协处理器。

3.根据权利要求2所述的方法,所述密码协处理器为集成在所述云服务器搭载的处理器上的密码协处理器;或者,所述密码协处理器为与所述云服务器搭载的处理器对接的密码协处理器外设。

4.根据权利要求1所述的方法,所述安全存储器包括限制除了所述密码加速硬件以外的硬件和/或软件进行访问的可编程存储器。

5.根据权利要求1所述的方法,所述安全存储器包括被加密保护的安全内存。

6.根据权利要求1所述的方法,所述方法还包括:

基于所述设备信息在本地生成所述证明信息,并将生成的所述证明信息在所述密码加速硬件上的安全存储器进行存储。

7.根据权利要求1所述的方法,所述设备信息包括所述云服务器的唯一特征码。

8.根据权利要求1所述的方法,所述方法还包括:

与所述客户端协商用于建立安全通道的协商密钥;

基于所述协商密钥建立与所述客户端之间的安全传输通道。

9.根据权利要求8所述的方法,所述安全存储器还存储了用于生成协商密钥对的种子密钥;所述协商密钥对包括协商公钥和协商私钥;

与所述客户端协商用于建立安全通道的协商密钥,包括:

根据所述协商公钥生成第一协商证书,将所述第一协商证书发送至所述客户端,以使所述客户端发送其本地生成的第二协商证书;

根据所述第一协商证书和所述第二协商证书计算用于建立安全通道的协商密钥。

10.根据权利要求1所述的方法,所述证明信息包括基于所述设备信息创建的密钥对中的公钥生成的证明证书。

11.根据权利要求1-10任一所述的方法,所述云服务器包括裸金属服务器。

12.一种基于密码加速硬件的密码加速装置,应用于云服务器,所述云服务器包括密码

加速硬件,所述密码加速硬件上的安全存储器存储了证明信息和所述云服务器的设备信息,所述证明信息用于证明所述云服务器的运行环境的合法性;所述设备信息用于生成所述证明信息,所述装置包括:

证明信息生成单元:用于将所述设备信息通过与第三方证明服务器之间的安全传输通道传输至所述证明服务器,以使证明服务器基于所述设备信息生成所述证明信息;

证明信息传输单元:用于通过所述安全传输通道接收所述证明服务器传输的证明信息,并将所述证明信息下发至所述密码加速硬件上的安全存储器进行存储;

数据下发单元:用于响应于客户端发送的远程验证请求,将所述证明信息下发至所述客户端,以使所述客户端将所述证明信息发送至第三方证明服务器,以由第三方证明服务器对所述证明信息进行合法性验证;

信息传输单元:用于接收所述客户端在所述证明信息通过合法性验证之后,通过与所述客户端之间的安全传输通道传输的密码信息;

加速处理单元:用于将所述密码信息下发至所述密码加速硬件,以使所述密码加速硬件对基于所述密码信息进行的加密/解密过程进行加速处理。

13.一种密码协处理器,包括:

处理器;

用于存储处理器可执行指令的存储器;

其中,所述处理器通过运行所述可执行指令以实现如权利要求1-11中任一项所述的方法。

14.一种计算机可读存储介质,其上存储有计算机指令,该指令被处理器执行时实现如权利要求1-11中任一项所述方法的步骤。

基于密码加速硬件的密码加速方法及装置

技术领域

[0001] 本说明书一个或多个实施例涉及计算机技术领域,尤其涉及一种基于密码加速硬件的密码加速方法及装置。

背景技术

[0002] 云服务器是一种简单高效、安全可靠、处理能力可弹性伸缩的计算服务器。其管理方式比物理服务器更简单高效。用户无需提前购买硬件,即可迅速创建或释放任意多台云服务器。在云服务的场景下,为了提高安全性,往往需要对网络传输链路上的数据进行加密保护。为了提高云服务器解密数据的效率,云服务器往往搭载了密码加速硬件用于对数据的加密/解密处理。而利用云服务器提供的密码加速硬件加密/解密数据时,数据安全问题尤为重要。

发明内容

[0003] 有鉴于此,本说明书一个或多个实施例提供一种基于密码加速硬件的密码加速方法及装置,以解决相关技术中存在的问题。

[0004] 为实现上述目的,本说明书一个或多个实施例提供技术方案如下:

[0005] 根据本说明书一个或多个实施例的第一方面,提出了一种基于密码加速硬件的密码加速方法,应用于云服务器,云服务器包括密码加速硬件,所述密码加速硬件上的安全存储器存储证明信息,所述证明信息用于证明所述云服务器的运行环境的合法性;所述方法包括:

[0006] 响应于客户端发送的远程验证请求,将所述证明信息下发至所述客户端,以使所述客户端对所述证明信息进行合法性验证;

[0007] 接收所述客户端在所述证明信息通过合法性验证之后,通过与所述客户端之间的安全传输通道传输的密码信息;

[0008] 将所述密码信息下发至所述密码加速硬件,以使所述密码加速硬件对基于所述密码信息进行的加密/解密过程进行加速处理。

[0009] 根据本说明书一个或多个实施例的第二方面,提出了一种基于密码加速硬件的密码加速装置,包括:

[0010] 数据下发单元:用于响应于客户端发送的远程验证请求,将所述证明信息下发至所述客户端,以使所述客户端对所述证明信息进行合法性验证;

[0011] 信息传输单元:用于接收所述客户端在所述证明信息通过合法性验证之后,通过与所述客户端之间的安全传输通道传输的密码信息;

[0012] 加速处理单元:用于将所述密码信息下发至所述密码加速硬件,以使所述密码加速硬件对基于所述密码信息进行的加密/解密过程进行加速处理。

[0013] 根据本说明书一个或多个实施例的第三方面,提出了一种密码协处理,包括:

[0014] 处理器;

[0015] 用于存储处理器可执行指令的存储器；

[0016] 其中，所述处理器通过运行所述可执行指令以实现如第一方面所述的方法。

[0017] 根据本说明书一个或多个实施例的第四方面，提出了一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如第一方面所述方法的步骤。

[0018] 本申请的有益效果：

[0019] 本申请通过为搭载密码加速硬件的云服务器引入针对云服务器的运行环境的合法性进行远程验证的机制，在用户将密码信息远程下发至云服务器的密码加速硬件之前，可以提前发起针对云服务器的运行环境的合法性进行远程证明。在证明合法性后，再通过安全传输通道传输待加密/解密的密码信息，避免密码泄露，可以有效解决云服务场景下数据安全问题。

附图说明

[0020] 图1是一示例性实施例提供的一种基于密码加速硬件的密码加速方法的系统架构示意图。

[0021] 图2是一示例性实施例提供的一种密码加速硬件的原理图。

[0022] 图3是一示例性实施例提供的一种基于密码加速硬件的密码加速方法的流程图。

[0023] 图4是一示例性实施例提供的一种基于密码加速硬件的密码加速方法的流程示意图。

[0024] 图5是一示例性实施例提供的一种云服务器的示意结构图。

[0025] 图6是一示例性实施例提供的一种基于密码加速硬件的密码加速装置的框图。

具体实施方式

[0026] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[0027] 需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[0028] 传统的弹性云服务器，用户通常要向服务商租用计算资源，而这些计算资源通常不是物理资源，而是虚拟资源。由于是虚拟资源，因此对于一些性能要求较高的任务(例如高性能运算)，对计算资源进行虚拟化往往会带来性能上延迟。而且，如果发生密集的输入输出操作，也会存在性能损失。同时，由于传统的弹性云服务器的计算资源通常会分配给多个租户，导致有租户突发高负荷时，其他组合仍会受到影响，因此，对于性能和稳定性要求很高的应用，传统的弹性云服务器是无法满足需求的。

[0029] 而裸金属服务器，就是一种兼具弹性云服务器的优势，同时又具有物理机般的高

性能的服务器。对于裸金属服务器来说，服务商大多只提供单租户服务，由单个租户独享物理服务器的资源，同时可以与用户已有的虚拟化服务器进行互通和协同。因此，由于裸金属服务器具有独占计算资源的特性，非常适合对安全隔离要求较高的场景；例如，非常适合部署银行、金融、证券等行业相关的任务。而且，也非常适合对云服务器性能有着高要求的场景；例如超级计算、航空航天等科学研究场景。

[0030] 由于用户通常需要远程处理密钥、密码等敏感信息，因此在云服务的裸金属场景下，数据安全变得尤为重要。出于安全考虑，通常需要对内存、硬盘等存储介质中以及网络传输链路上的数据进行加密保护。除此之外，云服务器上通常还会搭载密码加速硬件(比如可以是一个密码协处理器)，该密码加速硬件可以用于对数据进行加解密的过程进行加速，提升加解密数据的效率和速度。

[0031] 而在实际应用中，用户在远程访问云服务器时，利用云服务器提供的密码加速硬件对加解密的过程进行加速处理，往往需要将用于对数据进行加密的密钥远程下发到云服务器。在这个过程中，使得密钥等机密信息存在泄漏的风险。

[0032] 有鉴于此，本说明提出一种为搭载密码加速硬件的云服务器引入远程证明机制，远程验证云服务器运行环境的合法性后，再对密码进行传输和处理的技术方案。

[0033] 在实现时，云服务器搭载了密码加速硬件，其中，密码加速硬件具有安全存储器，安全存储器用于存储证明信息，证明信息用于证明所述云服务器的运行环境的合法性。云服务器响应于客户端发送的远程验证请求，将证明信息下发至客户端，以使客户端对证明信息进行合法性验证；客户端对证明信息进行合法性验证后，云服务器通过安全传输通道接收密码信息；然后云服务器通过密码加速硬件对密码信息进行的加密/解密过程进行加速处理。

[0034] 图1是一示例性实施例提供的一种基于密码加速硬件的密码加速方法的系统架构示意图。如图1所示，该系统可以包括云服务器102，第三方证明服务器104，客户端106，网络108。

[0035] 云服务器102可以包括弹性云服务器或裸金属服务器，云服务器搭载了用于对密码信息加密/解密过程进行加速的密码加速硬件。第三发证明服务器104可以包括用于颁发数字证书的证书服务器。客户端106可以包括笔记本电脑，手机，平板设备等电子设备提供的客户端，本发明对此不作限定。网络108可以包括多种类型的有线或无线网络。

[0036] 在一实施例中，以云服务器为裸金属服务器，第三方证明服务器为证书服务器，客户端为用户使用的笔记本电脑提供的客户端为例。用户可以通过客户端远程访问裸金属服务器，然后基于本说明书提供的基于密码加速硬件的密码加速方法，通过证书服务器远程证明裸金属服务器运行环境的合法性，然后接收客户端通过安全传输通道传输的密码信息，将上述密码信息下发至密码加速硬件，然后完成针对密码信息进行的加密/解密过程进行加速处理。

[0037] 请参见图2，图2是一示例性实施例提供的一种密码加速硬件的原理图。

[0038] 如图2所示，上述密码加速硬件具体可以包括安全存储器，运算单元，证明信息管理子系统，密钥管理子系统。其中，安全存储器，运算单元作为硬件单元在图中用实线标识，证明信息管理子系统及密钥管理子系统作为软件单元在图中用虚线标识。需要说明的是，上述密码加速硬件中可以具有证明信息管理子系统和/或密钥管理子系统中的一个或多

个,也可以不具有上述子系统,本发明对此不作限定。

[0039] 其中,上述安全存储器可以用于存储设备信息,证明信息,安全密钥等信息。上述安全存储器可以包括限制除了所述密码加速硬件以外的硬件和/或软件进行访问的可编程存储器,还可以包括被加密保护的安全内存。上述密码加速硬件中证明信息管理子系统可以用于管理第三方证明服务器下发的证明信息,支持证明信息的导入、导出等功能。上述密钥管理子系统可以用于管理远程证明过程中产生的安全密钥。上述运算单元可以由密码算法加速引擎、DMA等模块组成,用于加速针对密码信息进行的加密/解密过程。

[0040] 在一实施例中,上述密码加速硬件具体可以是密码协处理器。其中,密码协处理器具体可以是集成在上述云服务器搭载的处理器上的密码协处理器,也可以是与上述云服务器搭载的处理器对接的密码协处理器外设,本发明对此不作限定。

[0041] 下面结合附图对本说明书的基于密码加速硬件的密码加速方法进行详细说明。

[0042] 图3是一示例性实施例提供的一种基于密码加速硬件的密码加速方法的流程图。如图2所示,该方法可以应用于搭载了如图2所述的密码加速硬件的云服务器,所述方法可以包括如下的执行步骤:

[0043] 步骤302,响应于客户端发送的远程证明请求,将所述证明信息下发至所述客户端,以使所述客户端对所述证明信息进行合法性验证;

[0044] 在本实施例中,图2示出的密码加速硬件中的安全存储器存储有用于验证云服务器运行环境合法性的证明信息,其中,证明信息的具体形式在本说明书中不作特别限定。例如,可以是数字证书的形式,也可以是数字证书以外的其他形式,比如用于验证合法性的口令,电子凭证,等等。

[0045] 在示出的一种实施方式中,可以由第三方证明服务器生成证明信息。其中,第三方证明服务器可以提供为证明信息进行数字签名的服务,还可以提供验证证明信息的合法性的服务。第三方证明服务器基于云服务器的设备信息生成证明信息,并通过安全传输通道接收将上述证明信息下发至所述密码加速硬件搭载的安全存储器进行存储。其中,云服务器的设备信息具体可以是云服务器的唯一特征码,也可以是其他用于表示云服务器的特征信息,比如云服务器的序列号,出厂信息等。

[0046] 例如,以证明信息为证书为例,上述第三方证明服务器可以预先接收云服务器发送的唯一特征码,证明服务器根据唯一特征识别码生成证明密钥,其中,证明密钥对包括证明公钥和证明私钥。上述证明服务器根据证明公钥和设备信息生成用于验证运行环境合法性的证明证书并下发至上述云服务器,以由上述云服务搭载的密码加速硬件存储至安全存储器,并由密码加速硬件的证明信息管理子系统进行管理。

[0047] 为了进一步确保安全性,上述证明服务器还可以对证明证书进一步加密。上述证明服务器还具有种子密钥,用于生成根密钥,其中根密钥包括私钥和公钥。上述证明服务器在生成上述证明证书后,还可以用私钥对上述证明证书进行数字签名。后续可以基于该私钥对应的公钥对该数据签名进行验证,来完成针对该证明证书的合法性验证。

[0048] 在示出的另一种实施方式中,还可以由云服务器在本地生成证明信息。例如,以证明信息为证书为例,上述云服务搭载的密码加速硬件的安全存储器存储了云服务器的唯一特征码,密码加速硬件的密钥管理子系统可以根据上述唯一特征码生成证明密钥,其中,证明密钥对包括证明公钥和证明私钥。上述云服务器的证明信息管理子系统可以根据证明公

钥和设备信息生成用于验证运行环境合法性的证明证书,并下发至安全存储器,由证明信息管理子系统进行管理。

[0049] 为了进一步确保安全性,上述云服务器还可以对证明证书进一步加密。上述云服务器还具有种子密钥,用于生成根密钥,其中根密钥包括私钥和公钥。上述云服务器在生成上述证明证书后,还可以用私钥对上述证明证书进行数字签名。后续可以基于该私钥对应的公钥对该数据签名进行验证,来完成针对该证明证书的合法性验证。

[0050] 在本实施例中,用户可以通过客户端,将个人持有的密码信息,下发到云服务器搭载的密码加速硬件,由该密码加速硬件对基于该密码信息进行的加密/解密过程进行加速处理。而为了避免该密码信息造成泄露,在该客户端上,可以引入针对上述云服务器的运行环境的合法性进行远程验证的机制,使得用户在通过客户端,将用户密码远程下发至云服务器的密码加速硬件之前,可以通过客户端提前发起针对云服务器的运行环境的合法性进行远程证明。

[0051] 例如,客户端上可以提供远程证明的选项,比如可以是远程证明的按钮;用户可以通过点击等操作来触发这个选项。而客户端在监听到用户针对这个选项的触发操作后,发起针对云服务器运行环境合法性的远程证明。

[0052] 用户通过客户端发起了针对云服务器运行环境合法性的远程证明之后,客户端可以向云服务器发送一个远程验证请求。而云服务器在收到该远程验证请求后,可以响应于客户端该远程证明请求,通过密码加速硬件搭载的证明信息管理子系统,将上述安全存储硬件中存储证明信息下发至客户端。而客户端收到证明信息之后,可以发起针对证明信息的合法性验证。

[0053] 其中,发起针对证明信息的合法性验证的过程,通常与上述证明信息的生成过程对应。可以通过与第三方证明服务器进行远程证明交互来完成针对证明信息的远程验证,也可以在本地完成针对证明信息的合法性验证。

[0054] 在一实施例中,如果证明信息由第三方服务器生成,证明客户端可以将上述证明信息发送至第三方证明服务器进行验证。以证明信息为证书为例,如果上述证明证书携带数字签名,第三方服务器可以使用根密钥中的公钥对上述证明证书的签名验证,如果数字签名验证成功则证明证书合法。

[0055] 在另一实施例中,如果证明信息由云服务器本地生成,证明客户端可以将上述证明信息发送至云服务器进行验证。以证明信息为证书为例,如果上述证明证书携带数字签名,云服务器可以使用根密钥中的公钥对上述证明证书的签名验证,如果数字签名验证成功则证明证书合法。

[0056] 步骤304,接收所述客户端在所述证明信息通过合法性验证之后,通过与所述客户端之间的安全传输通道传输的密码信息;

[0057] 上述客户端接收证明服务器针对证明信息的验证结果,如果证明信息验证通过,则上述云服务器通过与客户端的安全传输通道传输密码信息。上述安全传输通道用于传输安全密钥以及用于密码加速硬件进行加速的密码信息等。上述安全传输通道可以预先建立,也可以在证明信息通过合法性验证后再建立,本发明对此不作限定。

[0058] 在一实施例中,上述云服务端与上述客户端可以预先协商用于建立安全通道的协商密钥,然后基于协商密钥建立与上述客户端之间的安全通道。

[0059] 具体的,上述密码加速硬件的安全存储器中还可以存储用于生成协商密钥的种子密钥,上述密码加速硬件的密钥管理子系统可以根据该种子密钥生成协商密钥,其中,协商密钥对可以包括协商公钥和协商私钥。上述云服务端可以根据协商密钥对中的协商公钥,生成第一协商证书,用于与客户端协商密钥。上述云服务端生成第一协商证书后,发送至客户端;以由客户端本地根据种子密钥生成用于协商的协商密钥对,生成第二协商证书并发送至云服务器。云服务端根据本地第一协商证书以及客户端发送的第二协商证书计算用于建立安全传输通道协商密钥,相应的,客户端根据本地的第二协商证书以及本地的第一协商证书计算协商密钥。客户端和云服务器可以使用协商密钥进行加密数据传输,以此确保加密的数据传输,避免密码等敏感信息泄露。

[0060] 步骤306,将所述密码信息下发至所述密码加速硬件,以使所述密码加速硬件对基于所述密码信息进行的加密/解密过程进行加速处理。

[0061] 上述针对云服务器的证明信息合法性验证通过后,客户端可以将密码信息通过安全传输通道下发至密码加速硬件进行加密/解密过程的加速处理。

[0062] 上述密码加速硬件对密码信息进行加密/解密的过程,可以参考相关密码加速硬件针对密码信息处理的相关技术,本发明不再赘述。

[0063] 下面结合图4,通过一个具体实施例进一步解释上述基于密码加速硬件的密码加速方法。

[0064] 图4是一示例性实施例提供的一种基于密码加速硬件的密码加速方法的流程示意图。如图4所示,云服务器搭载了密码加速硬件,密码加速硬件具有安全存储器,安全存储器用于存储证明信息、密钥信息以及设备信息。云服务器可以预先将设备信息发送至证明服务器,以由证明服务器基于设备信息预先生成证明信息,并将证明信息下发至云服务器(402),云服务器还可以在本地生成基于设备信息生成证信息。云服务器可以将证明信息存储至密码加速硬件的安全存储器进行安全存储,并由相应的证明信息管理子系统进行管理。证明服务器可以预先生成证明信息并下发至云服务器(402),其中,证明信息可以是基于云服务器的硬件唯一特征识别码生成的证明证书,云服务器可以将证明信息存储至云服务器搭载的密码加速硬件中的安全存储器中。当客户端需要证明云服务器运行环境的合法性时,可以向云服务器发起远程证明请求(404),云服务器收到远程证明请求后,可以将证明信息下发至客户端,以由客户端对证明信息进行验证(406),客户端接收证明信息,可以向证明服务器发起对证明信息的验证(408),也可以向云服务器发起对证明信息的验证。当客户端向证明服务器发起针对证明信息的验证时,证明服务器可以针对证明信息进行验证,并下发证明结果至客户端。当客户端向云服务器发起针对证明信息的验证时,云可以针对证明信息进行验证,并下发证明结果至客户端在证明信息通过合法性验证后,客户端可以通过安全传输通道传输相应的密码信息进行加密/解密处理(410)。

[0065] 图5是一示例性实施例提供的一种云服务器的示意结构图。请参考图5,在硬件层面,该设备包括处理器502、内部总线504、网络接口506、内存508以及非易失性存储器510,当然还可能包括其他任务所需要的硬件。本说明书一个或多个实施例可以基于软件方式来实现,比如由处理器502从非易失性存储器510中读取对应的计算机程序到内存508中然后运行。当然,除了软件实现方式之外,本说明书一个或多个实施例并不排除其他实现方式,比如逻辑器件抑或软硬件结合的方式等等,也就是说以下处理流程的执行主体并不限定于

各个逻辑单元,也可以是硬件或逻辑器件。

[0066] 请参考图6,图6是一示例性实施例提供的一种基于密码加速硬件的密码加速装置的框图。

[0067] 数据下发单元602:用于响应于客户端发送的远程验证请求,将所述证明信息下发至所述客户端,以使所述客户端对所述证明信息进行合法性验证;

[0068] 信息传输单元604:用于接收所述客户端在所述证明信息通过合法性验证之后,通过与所述客户端之间的安全传输通道传输的密码信息;

[0069] 加速处理单元606:用于将所述密码信息下发至所述密码加速硬件,以使所述密码加速硬件对基于所述密码信息进行的加密/解密过程进行加速处理。

[0070] 可选的,所述密码加速硬件包括密码协处理器。

[0071] 可选的,所述密码协处理器为集成在所述云服务器搭载的处理器上的密码协处理器;或者,所述密码协处理器为与所述云服务器搭载的处理器对接的密码协处理器外设。

[0072] 可选的,所述安全存储器包括限制除了所述密码加速硬件以外的硬件和/或软件进行访问的可编程存储器。

[0073] 可选的,安全存储器包括被加密保护的安全内存。

[0074] 可选的,基于密码加速硬件的密码加速装置还可以具有证书生成单元,具体用于将所述设备信息通过与第三方证明服务器之间的安全传输通道传输至所述证明服务器,以使证明服务器基于所述设备信息生成所述证明信息;通过所述安全传输通道接收所述证明服务器传输的证明信息,并将所述证明信息下发至所述密码加速硬件搭载的安全存储器进行存储;或者,基于所述设备信息在本地生成所述证明信息,并将生成的所述证明信息在所述密码加速硬件搭载的安全存储器进行存储。

[0075] 可选的,所述设备信息包括所述云服务器的唯一特征码。

[0076] 可选的,基于密码加速硬件的密码加速装置还可以具有密钥协商单元,用于与所述客户端协商用于建立安全通道的协商密钥;

[0077] 基于所述协商密钥建立与所述客户端之间的安全传输通道。

[0078] 可选的,安全存储器还存储了用于生成协商密钥对的种子密钥;所述协商密钥对包括协商公钥和协商私钥;密钥协商单元进一步用于根据所述协商公钥生成第一协商证书,将所述第一协商证书发送至所述客户端,以使所述客户端发送本地生成的第二协商证书;

[0079] 根据所述第一协商证书和所述第二协商证书计算用于建立安全通道的协商密钥。

[0080] 可选的,所述证明信息包括基于所述设备信息创建的密钥对中的公钥生成的证明证书。

[0081] 可选的,所述云服务器包括裸金属服务器。

[0082] 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,计算机的具体形式可以是个人计算机、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、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[0083] 在一个典型的配置中,计算机包括一个或多个处理器(CPU)、输入/输出接口、网络

接口和内存。

[0084] 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。

[0085] 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、磁盘存储、量子存储器、基于石墨烯的存储介质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。

[0086] 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。

[0087] 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。

[0088] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。还应当理解,本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0089] 应当理解,尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息,但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如,在不脱离本说明书一个或多个实施例范围的情况下,第一信息也可以被称为第二信息,类似地,第二信息也可以被称为第一信息。取决于语境,如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0090] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已,并不用以限制本说明书一个或多个实施例,凡在本说明书一个或多个实施例的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本说明书一个或多个实施例保护的范围之内。

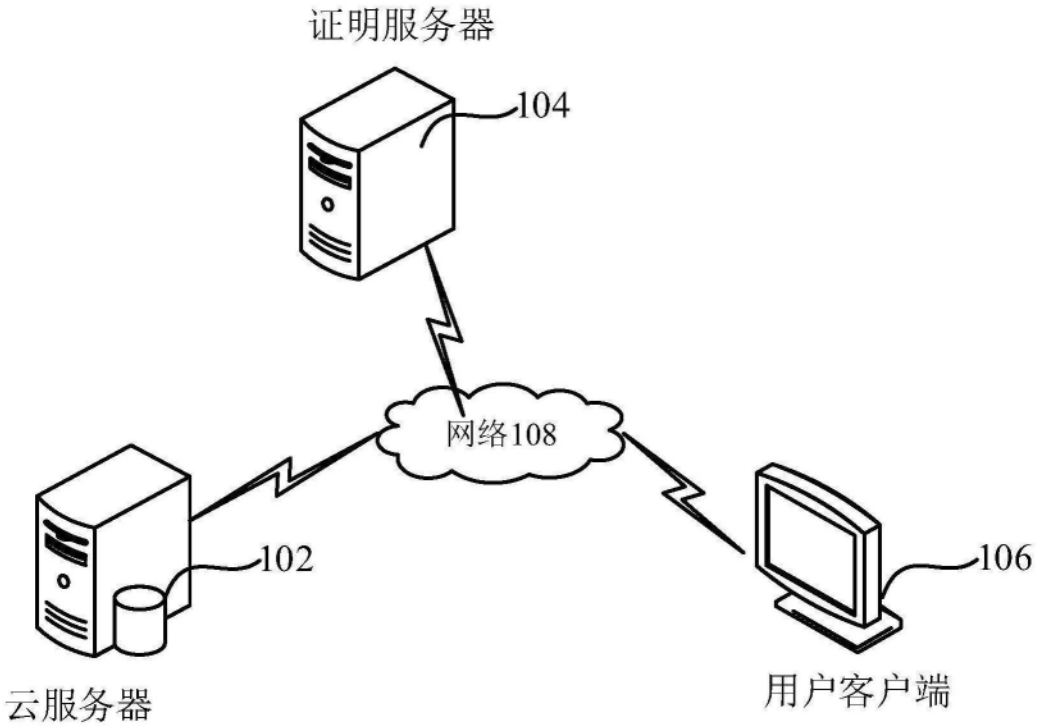

证明服务器
104
网络108
102
106
云服务器
用户客户端

图1

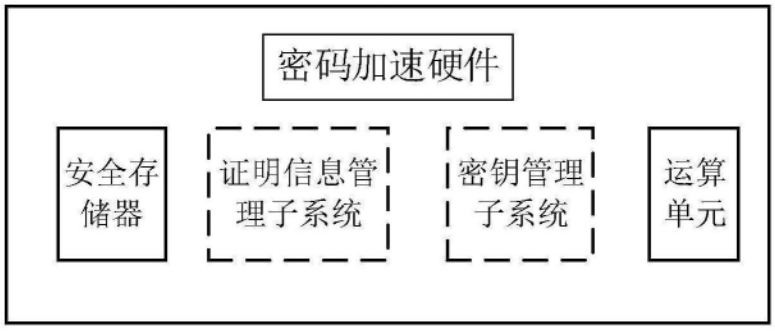

密码加速硬件
安全存储器
证明信息管理子系统
密钥管理子系统
运算单元

图2

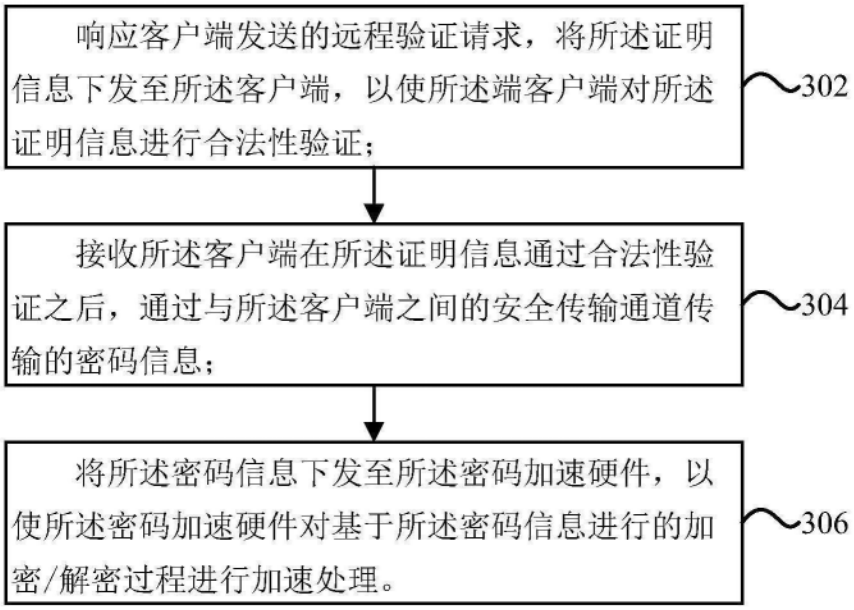

响应客户端发送的远程验证请求，将所述证明信息下发至所述客户端，以使所述端客户端对所述证明信息进行合法性验证；
302
接收所述客户端在所述证明信息通过合法性验证之后，通过与所述客户端之间的安全传输通道传输的密码信息；
304
将所述密码信息下发至所述密码加速硬件，以使所述密码加速硬件对基于所述密码信息进行的加密/解密过程进行加速处理。
306

图3

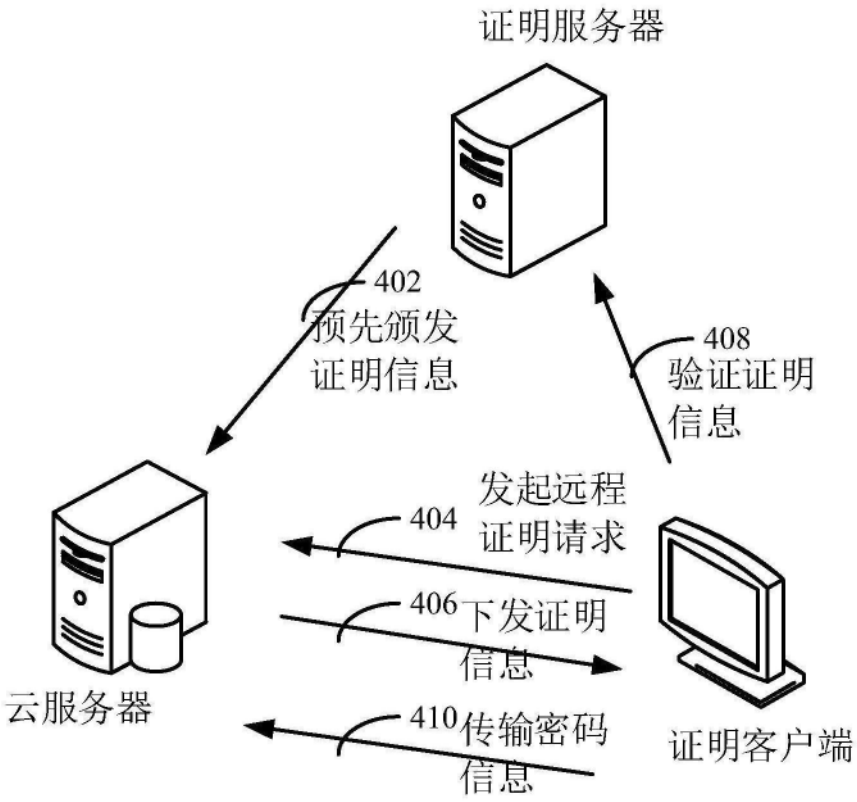

证明服务器
402
预先颁发
证明信息
408
验证证明
信息
发起远程
证明请求
404
406
下发证明
信息
410
传输密码
信息
云服务器
证明客户端

图4

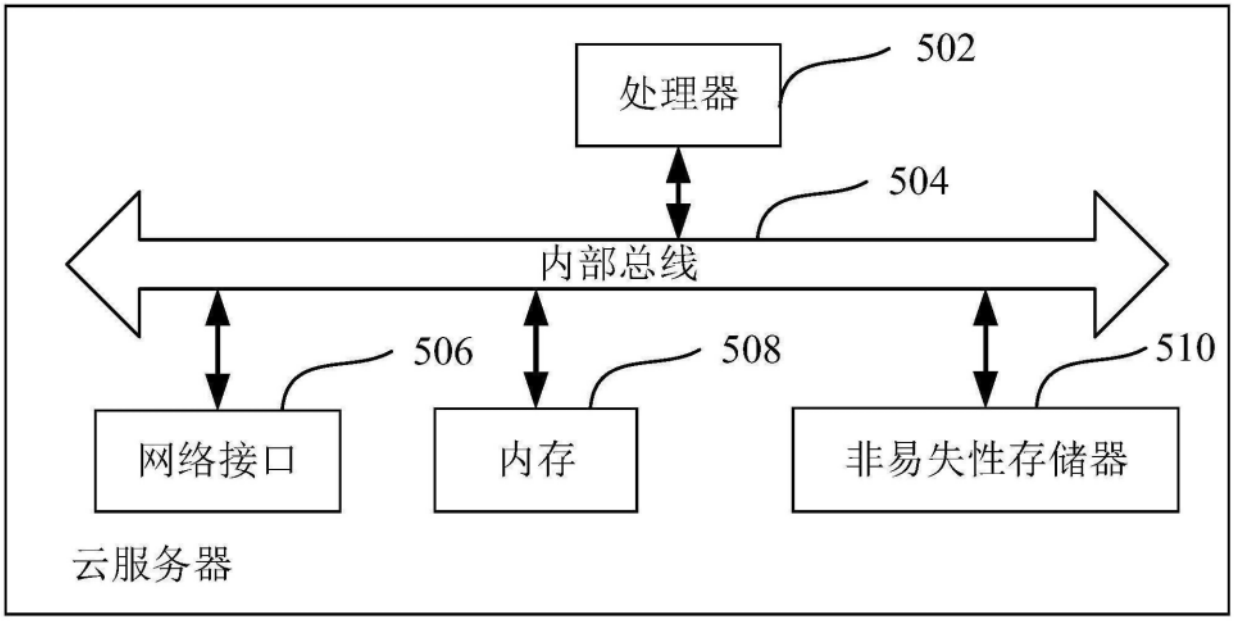

处理器
502
504
内部总线
506
508
510
网络接口
内存
非易失性存储器
云服务器

图5

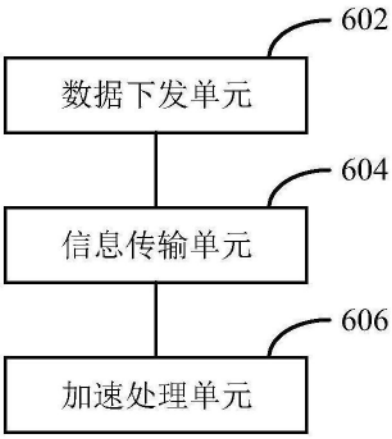

602
数据下发单元
604
信息传输单元
606
加速处理单元

图6