(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112703702 A
(43)申请公布日 2021.04.23

(21)申请号 201980050813.2

(22)申请日 2019.05.31

(30)优先权数据
1809887.1 2018.06.15 GB

(85)PCT国际申请进入国家阶段日
2021.01.29

(86)PCT国际申请的申请数据
PCT/GB2019/051524 2019.05.31

(87)PCT国际申请的公布数据
WO2019/239108 EN 2019.12.19

(71)申请人 艾欧特可有限公司
地址 英国埃塞克斯郡

(72)发明人 C·P·奥特里 A·W·罗斯科 M·梅格尔

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 王小东 黄纶伟

(51)Int.Cl.
H04L 9/00(2006.01)
H04L 9/32(2006.01)

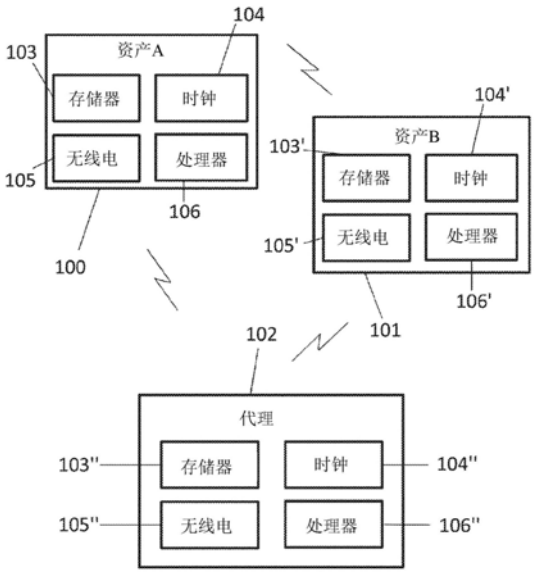
权利要求书4页 说明书16页 附图10页

(54)发明名称

分散式认证

(57)摘要

第一装置和第二装置(100、101)存储相应的装置数据和私钥。所述第一装置数据另外由所述第二装置和代理(102)存储;并且所述第二装置数据另外由所述第一装置和所述代理(102)存储。在承诺阶段(6)中,所述第一装置(100)使用其装置数据、私钥和第一随机nonce来生成一次性第一装置承诺值,并将其发送给所述代理(102)。所述第二装置(101)使用其装置数据、私钥和第二随机nonce来生成一次性第二装置承诺值,并将其发送给所述代理(102)。在检查阶段(8、10)中,所述装置(100、101)将密钥信息传递给所述代理(102),所述代理验证所述接收到的一次性承诺值。在摘要阶段(12)中,所述代理(102)计算一次性摘要,将其发送给所述第二装置(101)。然后,所述第二装置(101)验证所述接收到的一次性摘要以认证所述第一装置(100)。



CN 112703702 A

1.一种用于使用代理向第二装置认证第一装置的方法,其中:

所述第一装置存储第一装置数据和第一装置私钥;

所述第二装置存储第二装置数据和第二装置私钥;

所述第一装置数据另外由所述第二装置和所述代理存储;并且

所述第二装置数据另外由所述第一装置和所述代理存储,

所述方法包括,在承诺阶段中:

所述第一装置使用所述第一装置数据和第一装置私钥信息生成一次性第一装置承诺值,所述第一装置私钥信息包括所述第一装置私钥和第一随机nonce,或从二者中导出;

所述第一装置将所述一次性第一装置承诺值发送给所述代理;

所述第二装置使用所述第二装置数据和第二装置密钥信息生成一次性第二装置承诺值,所述第二装置密钥信息包括所述第二装置私钥和第二随机nonce,或从二者中导出;

所述第二装置将所述一次性第二装置承诺值发送给所述代理,

所述方法进一步包括,在所述承诺阶段之后执行的检查阶段中:

所述第一装置将所述第一装置密钥信息传递给所述代理;

所述第二装置将所述第二装置密钥信息传递给所述代理;

所述代理使用由所述代理存储的所述第一装置数据以及从所述第一装置接收的所述第一装置密钥信息来验证从所述第一装置接收的所述一次性第一装置承诺值;并且

所述代理使用由所述代理存储的所述第二装置数据以及从所述第二装置接收的所述第二装置密钥信息来验证从所述第二装置接收的所述一次性第二装置承诺值;

所述方法进一步包括,在所述承诺阶段中成功验证所述一次性第一装置承诺值和所述一次性第二装置承诺值之后执行的摘要阶段中:

所述代理根据以下各项计算一次性摘要:i)由所述代理存储的所述第一装置数据;ii)由所述代理存储的所述第二装置数据;iii)从所述第一装置接收的所述第一装置密钥信息;以及iv)从所述第二装置接收的所述第二装置密钥信息;

所述代理将所述一次性摘要发送给所述第二装置;并且

所述第二装置通过至少使用以下各项对所述第一装置进行认证:i)由所述第二装置存储的所述第一装置数据;ii)由所述第二装置存储的所述第二装置数据;iii)从所述第一装置接收的所述第一装置密钥信息;以及iv)所述第二装置密钥信息,从而验证从所述代理接收的所述一次性摘要。

2.根据权利要求1所述的方法,其中所述方法进一步包括:所述代理将所述一次性摘要发送给所述第一装置,并且所述第一装置通过至少使用以下各项对所述第二装置进行认证:i)由所述第一装置存储的所述第一装置数据;ii)由所述第一装置存储的所述第二装置数据;iii)所述第一装置密钥信息;以及iv)从所述第二装置接收的所述第二装置密钥信息,从而验证从所述代理接收的所述一次性摘要。

3.根据权利要求1或2所述的方法,其中除了由所述代理执行的对所述一次性第一装置和第二装置承诺值的验证之外,所述第一装置和所述第二装置验证一个或多个一次性承诺值。

4.根据前述权利要求中任一项所述的方法,其中所述代理存储代理数据和代理装置私钥,并且其中所述方法进一步包括:所述代理使用所述代理数据和代理装置密钥信息来生

成一次性代理装置承诺值，所述代理装置密钥信息包括所述代理装置私钥第三随机nonce，或从二者中导出。

5.根据权利要求4所述的方法，其中所述第二装置存储所述代理数据和所述代理装置私钥，所述方法进一步包括：

所述代理将所述一次性代理装置承诺值发送给所述第二装置；

所述代理将所述代理装置密钥信息传递给所述第二装置；并且

所述第二装置使用存储在所述第二装置中的所述代理数据以及从所述代理装置接收的所述代理装置密钥信息来验证从所述代理装置接收的所述一次性代理装置承诺值。

6.根据权利要求5所述的方法，其包括：

所述代理另外使用所述代理数据和所述代理装置密钥信息来计算所述一次性摘要值；并且

当对所述第一装置进行认证时，所述第二装置另外使用由所述第二装置存储的所述代理数据以及从所述代理装置接收的所述代理装置密钥信息来验证从所述代理接收的所述一次性摘要。

7.根据权利要求4到6中任一项所述的方法，其中所述第一装置存储所述代理数据和所述代理装置私钥，所述方法进一步包括：

所述代理将所述一次性代理装置承诺值发送给所述第一装置；

所述代理将所述代理装置密钥信息传递给所述第一装置；并且

所述第一装置使用存储在所述第一装置中的所述代理数据以及从所述代理装置接收的所述代理装置密钥信息来验证从所述代理装置接收的所述一次性代理装置承诺值。

8.根据权利要求7所述的方法，其包括：

所述代理另外使用所述代理数据和所述代理装置密钥信息来计算所述一次性摘要值；并且

当对所述第二装置进行认证时，所述第一装置另外使用由所述第一装置存储的所述代理数据以及从所述代理装置接收的所述代理装置密钥信息来验证从所述代理接收的所述一次性摘要。

9.一种通信系统，其包括：

第一装置；

第二装置；以及

代理装置，

其中：

所述第一装置存储第一装置数据和第一装置私钥；

所述第二装置存储第二装置数据和第二装置私钥；

所述第一装置数据另外由所述第二装置和所述代理装置存储；并且

所述第二装置数据另外由所述第一装置和所述代理装置存储，

其中，所述第一装置在承诺阶段中被配置成：

使用所述第一装置数据和第一装置私钥信息生成一次性第一装置承诺值，所述第一装置私钥信息包括所述第一装置私钥和第一随机nonce，或从二者中导出；并且

将所述一次性第一装置承诺值发送给所述代理装置，

其中所述第二装置在所述承诺阶段中被配置成：

使用所述第二装置数据和第二装置密钥信息生成一次性第二装置承诺值，所述第二装置密钥信息包括所述第二装置私钥和第二随机nonce，或从二者中导出；并且

将所述一次性第二装置承诺值发送给所述代理装置，

其中：

所述第一装置在所述承诺阶段之后执行的检查阶段将所述第一装置密钥信息传递给所述代理装置；

所述第二装置在所述检查阶段中被配置成将所述第二装置密钥信息传递给所述代理装置；

所述代理装置在所述检查阶段中被配置成使用由所述代理装置存储的所述第一装置数据以及从所述第一装置接收的所述第一装置密钥信息来验证从所述第一装置接收的所述一次性第一装置承诺值；并且

所述代理装置在所述检查阶段中被进一步配置成使用由所述代理装置存储的所述第二装置数据以及从所述第二装置接收的所述第二装置密钥信息来验证从所述第二装置接收的所述一次性第二装置承诺值；

并且其中：

所述代理装置被配置成响应于在所述承诺阶段中对所述一次性第一装置承诺值和所述一次性第二装置承诺值的成功验证而进入摘要阶段；

当处于摘要阶段时，所述代理装置被配置成根据以下各项计算一次性摘要：i)由所述代理装置存储的所述第一装置数据；ii)由所述代理装置存储的所述第二装置数据；iii)从所述第一装置接收的所述第一装置密钥信息；以及iv)从所述第二装置接收的所述第二装置密钥信息，并将所述一次性摘要发送给所述第二装置；并且

所述第二装置被配置成通过至少使用以下各项对所述第一装置进行认证：i)由所述第二装置存储的所述第一装置数据；ii)由所述第二装置存储的所述第二装置数据；iii)从所述第一装置接收的所述第一装置密钥信息；以及iv)所述第二装置密钥信息，从而验证从所述代理装置接收的所述一次性摘要。

10.根据权利要求9所述的通信系统，其中所述第一装置、所述第二装置和所述代理装置中的至少一个是传感器或传感器集线器。

11.根据权利要求9或10所述的通信系统，其中所述代理装置被进一步配置成将所述一次性摘要发送给所述第一装置，并且所述第一装置被配置成通过至少使用以下各项对所述第二装置进行认证：i)由所述第一装置存储的所述第一装置数据；ii)由所述第一装置存储的所述第二装置数据；iii)所述第一装置密钥信息；以及iv)从所述第二装置接收的所述第二装置密钥信息，从而验证从所述代理装置接收的所述一次性摘要。

12.根据权利要求9到11中任一项所述的通信系统，其中所述代理装置存储代理数据和代理装置私钥，并且其中所述代理装置在承诺阶段中被配置成使用所述代理数据和代理装置密钥信息来生成一次性代理装置承诺值，所述代理装置密钥信息包括所述代理装置私钥第三随机nonce，或从二者中导出。

13.根据权利要求9到12中任一项所述的通信系统，其中所述第二装置存储所述代理数据和所述代理装置私钥，所述代理装置被配置成将所述一次性代理装置承诺值发送给所述

第二装置并将所述代理装置密钥信息传递给所述第二装置，并且其中所述第二装置被配置成使用存储在所述第二装置中的所述代理数据以及从所述代理装置接收的所述代理装置密钥信息来验证从所述代理装置接收的所述一次性代理装置承诺值。

14.根据权利要求13所述的通信系统，其中：

所述代理被配置成另外使用所述代理数据和所述代理装置密钥信息来计算所述一次性摘要值；并且

当对所述第一装置进行认证时，所述第二装置被配置成另外使用由所述第二装置存储的所述代理数据以及从所述代理装置接收的所述代理装置密钥信息来验证从所述代理接收的所述一次性摘要。

15.根据权利要求12到14中任一项所述的通信系统，其中所述第一装置存储所述代理数据和所述代理装置私钥，所述代理装置被配置成将所述一次性代理装置承诺值发送给所述第一装置并将所述代理装置密钥信息传递给所述第一装置，并且其中所述第一装置被配置成使用存储在所述第一装置中的所述代理数据以及从所述代理装置接收的所述代理装置密钥信息来验证从所述代理装置接收的所述一次性代理装置承诺值。

16.根据权利要求15所述的通信系统，其中：

所述代理被配置成另外使用所述代理数据和所述代理装置密钥信息来计算所述一次性摘要值；并且

当对所述第二装置进行认证时，所述第一装置被配置成另外使用由所述第一装置存储的所述代理数据以及从所述代理装置接收的所述代理装置密钥信息来验证从所述代理接收的所述一次性摘要。

17.根据权利要求9到16中任一项所述的通信系统，其中所述第一装置数据包括标识所述第一装置的第一标识数据，并且所述第二装置数据包括标识所述第二装置的第二标识数据。

18.根据权利要求9到17中任一项所述的通信系统，其中所述第一装置、第二装置和代理装置包括无线电，并且被配置成通过无线电进行通信。

19.根据权利要求9到17中任一项所述的通信系统，其中所述第一装置、第二装置和代理装置被配置成通过一个或多个有线链路进行通信。

分散式认证

背景技术

[0001] 本发明涉及用于对装置进行认证的方法和系统。

[0002] 认证过程是密码系统的核心概念。认证在希望交换信息的两方之间建立信任。认证可以确定一方是否是谁或声称的身份。认证与授权不同;授权确定允许一方执行的操作,如可能与所述方通信或不通信的其它各方。

[0003] 通常使用公钥基础结构(PKI)进行验证,在所述公钥基础结构中,被称为证书颁发机构(CA)的集中受信任的第三方(TTP)会仔细检查一方的身份,然后证实所述方的公钥(非对称密钥对中的公钥)。当第二方看到此证书时,第二方便知道如何生成仅第一方可以解密的消息,或者第二方可以验证签名,所述签名证明第一方确实是加密签名文档的作者。

[0004] 然而,PKI并不适合所有情况。PKI设计用于集中式客户端-服务器模型,在所述模型中,希望进行认证各方必须通过某个集中式网络(通常是公共因特网)进行通信,以完成交易。各方必须依靠TTP来持有可能成本高昂的证书。PKI的复杂性使其不太适合物联网(IoT),在这种情况下,需要从数十亿个节点中提供认证,其中许多节点是可移动的,并且可能缺乏任何普遍理解的身份感,至少从整个世界的角度来看。即使节点确实具有有意义的身份(例如,凭借其所有权或物理位置),在此规模下创建和维护有效PKI的成本也将非常高。PKI越大且结构化越多,通常需要更多的CA层。由于PKI认证需要复杂的数学计算,因此这可能会对装置(可能是简单的电池供电的传感器)施加无法接受的计算机电源和电力需求。此外,在复杂的IoT系统中,许多资产通常需要在短暂的一次性突发中与许多其它资产进行实时通信。

[0005] 已经尝试通过在网关级别使用PKI认证为大型IoT网络提供认证。然而,依赖网关认证会使传感器和传感器集线器容易受到各种攻击,如蛮力攻击、中间人攻击和量子后暴露。如果网关是公开的,则依赖所述网关进行连接的所有组件、路由和功能也将公开。

[0006] 本发明旨在提供一种替代性认证方法,所述方法克服常规的集中式PKI认证方法中存在的这些缺点中的至少一些缺点。

发明内容

[0007] 根据第一方面,本发明提供了一种用于使用代理向第二装置认证第一装置的方法,其中:

[0008] 所述第一装置存储第一装置数据和第一装置私钥;

[0009] 所述第二装置存储第二装置数据和第二装置私钥;

[0010] 所述第一装置数据另外由所述第二装置和所述代理存储;并且

[0011] 所述第二装置数据另外由所述第一装置和所述代理存储,

[0012] 所述方法包括,在承诺阶段中:

[0013] 所述第一装置使用所述第一装置数据和第一装置私钥信息生成一次性第一装置承诺值,所述第一装置私钥信息包括所述第一装置私钥和第一随机nonce,或从二者中导出;

[0014] 所述第一装置将所述一次性第一装置承诺值发送给所述代理；

[0015] 所述第二装置使用所述第二装置数据和第二装置密钥信息生成一次性第二装置承诺值，所述第二装置密钥信息包括所述第二装置私钥和第二随机nonce，或从二者中导出；

[0016] 所述第二装置将所述一次性第二装置承诺值发送给所述代理，

[0017] 所述方法进一步包括，在所述承诺阶段之后执行的检查阶段中：

[0018] 所述第一装置将所述第一装置密钥信息传递给所述代理；

[0019] 所述第二装置将所述第二装置密钥信息传递给所述代理；

[0020] 所述代理使用由所述代理存储的所述第一装置数据以及从所述第一装置接收的所述第一装置密钥信息来验证从所述第一装置接收的所述一次性第一装置承诺值；并且

[0021] 所述代理使用由所述代理存储的所述第二装置数据以及从所述第二装置接收的所述第二装置密钥信息来验证从所述第二装置接收的所述一次性第二装置承诺值；

[0022] 所述方法进一步包括，在所述承诺阶段中成功验证所述一次性第一装置承诺值和所述一次性第二装置承诺值之后执行的摘要阶段中：

[0023] 所述代理根据以下各项计算一次性摘要：i)由所述代理存储的所述第一装置数据；ii)由所述代理存储的所述第二装置数据；iii)从所述第一装置接收的所述第一装置密钥信息；以及iv)从所述第二装置接收的所述第二装置密钥信息；

[0024] 所述代理将所述一次性摘要发送给所述第二装置；并且

[0025] 所述第二装置通过至少使用以下各项对所述第一装置进行认证：i)由所述第二装置存储的所述第一装置数据；ii)由所述第二装置存储的所述第二装置数据；iii)从所述第一装置接收的所述第一装置密钥信息；以及iv)所述第二装置密钥信息，从而验证从所述代理接收的所述一次性摘要。

[0026] 根据第二方面，本发明提供了一种通信系统，其包括：

[0027] 第一装置；

[0028] 第二装置；以及

[0029] 代理装置，

[0030] 其中：

[0031] 所述第一装置存储第一装置数据和第一装置私钥；

[0032] 所述第二装置存储第二装置数据和第二装置私钥；

[0033] 所述第一装置数据另外由所述第二装置和所述代理装置存储；并且

[0034] 所述第二装置数据另外由所述第一装置和所述代理装置存储，

[0035] 其中，所述第一装置在承诺阶段中被配置成：

[0036] 使用所述第一装置数据和第一装置私钥信息生成一次性第一装置承诺值，所述第一装置私钥信息包括所述第一装置私钥和第一随机nonce，或从二者中导出；并且

[0037] 将所述一次性第一装置承诺值发送给所述代理装置，

[0038] 其中所述第二装置在所述承诺阶段中被配置成：

[0039] 使用所述第二装置数据和第二装置密钥信息生成一次性第二装置承诺值，所述第二装置密钥信息包括所述第二装置私钥和第二随机nonce，或从二者中导出；并且

[0040] 将所述一次性第二装置承诺值发送给所述代理装置，

[0041] 其中：

[0042] 所述第一装置在所述承诺阶段之后执行的检查阶段将所述第一装置密钥信息传递给所述代理装置；

[0043] 所述第二装置在所述检查阶段中被配置成将所述第二装置密钥信息传递给所述代理装置；

[0044] 所述代理装置在所述检查阶段中被配置成使用由所述代理装置存储的所述第一装置数据以及从所述第一装置接收的所述第一装置密钥信息来验证从所述第一装置接收的所述一次性第一装置承诺值；并且

[0045] 所述代理装置在所述检查阶段中被进一步配置成使用由所述代理装置存储的所述第二装置数据以及从所述第二装置接收的所述第二装置密钥信息来验证从所述第二装置接收的所述一次性第二装置承诺值；

[0046] 并且其中：

[0047] 所述代理装置被配置成响应于在所述承诺阶段中对所述一次性第一装置承诺值和所述一次性第二装置承诺值的成功验证而进入摘要阶段；

[0048] 当处于摘要阶段时，所述代理装置被配置成根据以下各项计算一次性摘要：i)由所述代理装置存储的所述第一装置数据；ii)由所述代理装置存储的所述第二装置数据；iii)从所述第一装置接收的所述第一装置密钥信息；以及iv)从所述第二装置接收的所述第二装置密钥信息，并将所述一次性摘要发送给所述第二装置；并且

[0049] 所述第二装置被配置成通过至少使用以下各项对所述第一装置进行认证：i)由所述第二装置存储的所述第一装置数据；ii)由所述第二装置存储的所述第二装置数据；iii)从所述第一装置接收的所述第一装置密钥信息；以及iv)所述第二装置密钥信息，从而验证从所述代理装置接收的所述一次性摘要。

[0050] 根据另一方面，本发明提供一种装置，所述装置被配置用于实施由所述第一装置执行的本文公开的方法步骤。根据另一方面，本发明提供一种装置，所述装置被配置用于实施由所述第二装置执行的本文公开的方法步骤。根据另一方面，本发明提供了一种代理装置，所述代理装置被配置用于实施由所述代理装置执行的本文公开的方法步骤。

[0051] 因此，将看到，根据本发明，可以使用代理来向所述第二装置提供经纪、独立数据验证和置信度，即第一装置的身份或其所声称的是什么—即，所述第一装置实际上是由所述第一装置数据标识的装置。所述第一装置和所述第二装置都在承诺阶段中将从相应装置数据中导出的相应一次性承诺值传输给所述代理，优选地，所述一次性承诺值对于所述装置是唯一的。然后，仅在两个装置以及任选的代理都提交了各自的承诺值之后，所述第一装置和所述第二装置以及任选的所述代理才揭示允许所述代理以及任选的所述第一装置和/或所述第二装置验证所述承诺值的密钥信息。所述代理使用其存储的第一装置数据和第二装置数据向所述代理认证所述第一装置和所述第二装置。假设此验证成功，则所述代理计算摘要并将所述摘要传输给所述第二装置。此摘要向所述第二装置确认所述第一装置的真实性。与在不涉及所述代理的情况下仅所述第二装置尝试直接对所述第一装置进行认证的情况相比，通过使所述代理以这种方式证明所述第一装置的真实性，所述第二装置可以以更大的置信度对所述第一装置进行认证。所述装置可以是简单的装置，如物联网传感器或传感器集线器，或者可以是更复杂的装置，如例如路由器。

[0052] 所述装置数据(第一装置数据、第二装置数据和任何代理装置数据)优选地是装置特异性数据。所述装置数据可以包括预置数据。所述装置数据可以包括标识数据。

[0053] 所述代理可以是受信任的装置。具体地说,例如由于在此方法之前发生的数据交换,所述第二装置(以及任选的所述第一装置)可以信任所述代理。在一些实施例中,所述第二装置(以及任选的所述第一装置)可以通过本文公开的步骤中的至少一些步骤来建立对所述代理的信任。

[0054] 所述代理可以存储代理数据和代理装置私钥。任选地,所述代理数据也由所述第二装置存储,并且任选地由所述第一装置存储。

[0055] 在一些实施例中,所述代理装置可以使用所述代理数据和代理装置密钥信息来生成一次性代理装置承诺值,所述代理装置密钥信息包括所述代理装置私钥第三随机nonce,或从二者中导出。在优选实施例中,所述代理可以将所述一次性代理装置承诺值发送给所述第二装置。其可以将所述一次性代理装置承诺值发送给所述第一装置。

[0056] 所述第一随机nonce可以由所述第一装置生成。所述第二随机nonce可以由所述第二装置生成。所述第三随机nonce可以由所述代理装置生成。每个随机nonce可以从真随机源中生成,或通过伪随机数生成器生成。

[0057] 在一些实施例中,在所述检查阶段中,所述代理装置将所述代理装置密钥信息传递给所述第二装置。其还可以将所述代理装置密钥信息传递给所述第一装置。

[0058] 在一些实施例中,所述第二装置使用由所述第二装置存储的所述代理数据以及从所述代理装置接收的所述代理装置密钥信息来验证从所述代理装置接收的所述一次性代理装置承诺值。在一些实施例中,所述第一装置使用由所述第一装置存储的所述代理数据以及从所述代理装置接收的所述代理装置密钥信息来验证从所述代理装置接收的所述一次性代理装置承诺值。

[0059] 在一些实施例中,所述代理被配置成仅在所述承诺阶段中由所述第二装置成功验证所述一次性第一装置承诺值和所述一次性代理装置承诺值之后才进入所述摘要阶段。在一些实施例中,所述代理被配置成仅在所述承诺阶段中由所述第一装置成功验证所述一次性第二装置承诺值和所述一次性代理装置承诺值之后才进入所述摘要阶段。所述第一和/或第二装置可以将成功的验证传递给所述代理装置。所述第一和/或第二装置可以将由所述第一和/或第二装置分别计算的一个或多个重新计算的承诺值发送给所述代理装置。除了成功验证所述一次性第一装置承诺值和所述一次性第二装置承诺值之外,仅在由所述第一装置和所述第二装置之一或两者成功验证所述一次性代理装置承诺值之后,所述代理才能进入所述摘要阶段。

[0060] 在一些实施例中,所述代理另外使用所述代理数据和所述代理装置密钥信息来计算所述一次性摘要值。

[0061] 所述第二装置(以及任选的所述第一装置)可以通过另外使用所述代理数据和所述代理装置密钥信息来验证从所述代理接收的所述一次性摘要,从而对所述第一装置进行认证。

[0062] 所述第一装置和/或所述第二装置可以是任何电子装置。所述装置可能是无线装置。所述装置可能是路由器和/或服务器。所述装置可能是便携式装置。所述装置可能是电池供电的。在实施例的优选集合中,所述装置是无线传感器装置。所述装置可以使用

IEEE802.1X协议(例如802.11(WiFi))相互通信和/或与代理通信。所述装置可以通过无线电相互通信和/或与代理通信,例如,使用如ZigBee™等IEEE 802.15协议和/或使用WiFi或蓝牙或任何其它短距离、中距离或长距离无线电协议。然而,这不是必需的,并且所述装置可以使用一个或多个无线光信道、微波链路、如802.3x(以太网)等有线链路、电线、光纤电缆等进行通信。所述第一和/或第二装置可以包括互联网接口;所述装置可能具有相应的IP地址,也可能没有IP地址;所述装置可能是IoT装置。

[0063] 代理可以是任何装置。所述代理可以具有所述第一和/或第二装置的任何特征。具体地说,所述代理可以是另一传感器装置。在一些实施例中,所述代理是传感器集线器或网关。

[0064] 所述第一装置、所述第二装置和代理可以全部彼此靠近,例如,在小于1公里、或小于100米或小于10米的范围内,或者它们可以分布在更大的距离上,甚至可以分布在整个区域内。

[0065] 在一些实施例中,所述第一装置或所述第二装置可以另外充当所述代理,即一个物理装置可以既是所述第一装置又是所述代理,或者可以既是所述第二装置又是所述代理。然而,在其它实施例中,所述代理不同于所述第一装置和所述第二装置。

[0066] 在一些实施例中,所述方法可以用于为第二多个装置或第二组装置认证第一多个装置或第一组装置。

[0067] 在一些实施例中,所述方法可以用于向第二多个装置或第二组装置相互地认证第一多个装置或第一组装置。

[0068] 所述方法可以进一步包括,在所述摘要阶段中,所述代理将所述一次性摘要发送给所述第一装置。所述第一装置可以通过至少使用以下各项对所述第二装置进行认证:i)由所述第一装置存储的所述第一装置数据;ii)由所述第一装置存储的所述第二装置数据;iii)所述第一装置密钥信息;以及iv)从所述第二装置接收的所述第二装置密钥信息,从而验证从所述代理接收的所述一次性摘要。以这种方式,所述方法可以实现所述第一装置和所述第二装置的相互认证。

[0069] 当认证所述第一装置时,所述第二装置可以另外使用由所述第二装置存储的所述代理装置数据以及从所述代理装置接收的所述代理装置密钥信息来验证从所述代理接收的所述一次性摘要。当认证所述第二装置时,所述第一装置可以另外使用由所述第一装置存储的所述代理装置数据以及从所述代理装置接收的所述代理装置密钥信息来验证从所述代理接收的所述一次性摘要。

[0070] 在一些实施例中,除了由所述代理执行的验证之外,所述第一装置和/或所述第二装置还可以验证一个或多个承诺值。这可以提高协议抵抗攻击的鲁棒性。具体地说,在所述承诺阶段中,一些实施例可以包括:所述第一装置另外将所述一次性第一装置承诺值发送给所述第二装置。所述实施例可以包括:所述第二装置另外将所述一次性第二装置承诺值发送给所述第一装置。一些实施例可以包括,在所述检查阶段中,所述第一装置另外将所述第一装置密钥信息传递给所述第二装置。然后,所述第二装置可以使用由所述第二装置存储的所述第一装置数据以及所述接收到的第一装置密钥信息来验证从所述第一装置接收的所述一次性第一装置承诺值。一些实施例可以包括:所述第二装置将所述第二装置密钥信息传递给所述第一装置。然后,所述第一装置可以使用由所述第一装置存储的所述第二

装置数据以及所述接收到的第二装置密钥信息来验证从所述第二装置接收的所述一次性第二装置承诺值。

[0071] 所述第一装置和第二装置优选地被配置成不与集中式证书颁发机构通信。所述装置不需要含有任何用于执行公钥加密的机制。与使用PKI认证协议相比，这可以简化装置的设计并降低处理要求和功耗。

[0072] 一些实施例可以使用如SHA函数等散列操作来生成相应的承诺值。与执行非对称密钥操作相比，这通常给装置带来更少的计算负担。

[0073] 所述方法可以包括握手阶段，在所述握手阶段中，所述第一装置、所述第二装置和所述代理装置中的一个或多个由所述第一装置、所述第二装置和所述代理装置中的一个或多个其它装置标识。可以在没有强认证的情况下执行此标识。所述标识可以包括交换可以从所述装置中的一个或多个装置的装置数据中导出的一个或多个相对较短的散列值(例如，20位散列值)。每个散列值可以包含相应的随机nonce作为散列的输入，使得所述散列值是一次性值。每个散列值可以包含相应的时间戳作为散列的输入。每个随机nonce可以由相应的装置传递给所述其它装置中的至少一个装置。握手可以包括：所述第一装置通过基于由所述第一装置存储的所述第二装置数据和从所述第二装置接收的随机nonce重新计算散列值来确定所述第二装置的身份。所述第一装置可以将所述重新计算的散列值与从所述第二装置接收的散列值进行比较，并在散列值匹配时标识所述第二装置。类似地，握手可以包括：所述第二装置通过基于由所述第一装置存储的所述第一装置数据和从所述第一装置接收的随机nonce重新计算散列值来确定所述第一装置的身份。所述第二装置可以将所述重新计算的散列值与从所述第一装置接收的散列值进行比较，并在散列值匹配时标识所述第一装置。

[0074] 所述方法可以另外包括预先部署的握手阶段，用于向所述第二装置和所述代理提供所述第一装置数据，以及用于向所述第一装置和所述代理提供所述第二装置数据。

[0075] 所述代理计算的所述一次性摘要可以进一步取决于来自所述装置中的一个或多个装置的时间戳信息。所述第二装置和/或所述第一装置可以使用所述时间戳信息来验证所述一次性摘要的新鲜度。这可以帮助防止重放攻击。

[0076] 由所述第一装置或所述第二装置分别生成的所述第一装置承诺值或所述第二装置承诺值可以另外取决于来自相应装置的内部时钟的时间戳信息。接收承诺值的装置(例如，代理)可以检查所述承诺值满足新鲜度条件(例如，根据验证代理的时钟，距离当前时间不超过0.1秒)作为验证所述承诺值的一部分。

[0077] 所述第一装置可以执行里程碑检查，在所述里程碑检查中，所述第一装置检查所述第一装置已经执行了协议的阶段集合。所述阶段集合可以包含所述承诺阶段和/或所述检查阶段和/或所述摘要阶段。所述阶段集合可能进一步包含握手阶段。所述检查阶段可以提供密钥交换里程碑和单独的检查里程碑。如果里程碑检查失败，则所述第一装置可以退出所述认证方法。所述第一装置可以被配置成向代理证明其已经执行了里程碑阶段集合。所述第二装置可以类似地被配置成执行这些里程碑操作中的一些或全部。

[0078] 所述装置之间的通信可以在两个或更多个不同的信道上进行划分，如在两个不同的无线电协议上进行划分，或者在有线信道和无线信道上进行划分。这可以提供更大的安全性。

[0079] 所述装置可以共享一个加密密钥(例如AES密钥),所述密钥可以用来加密装置之间的数据通信中的一些或全部。然而,认证的完整性优选地不依赖于这种AES密钥的安全性。

[0080] 所述代理和/或所述第一或第二装置可以被配置成例如在区块链中记录成功的认证。

[0081] 优选地,所述系统被配置成使得每次执行认证协议时在所述装置之间交换不同的数据。如本文所公开的,这可以通过使用nonce来实现。以这种方式,每次都可能从头开始认证,这可以防止攻击者对密钥或证书进行解密。实施例可以提供量子电阻。

[0082] 优选地,所述装置之间不存在永久认证。认证可以仅在需要的基础上进行。在一些情况下,经认证的状态可能仅持续一个通信会话,所述通信会话可能仅持续几秒钟或更短。这在所述装置是移动的并且可能彼此相邻(例如,在短距离无线电范围内)仅几秒钟的情况下尤其合适。

[0083] 可以由相同的第一装置和第二装置多次执行承诺、检查和摘要阶段,优选地使用不同的随机nonce。所述第一装置和第二装置可以被配置成每当满足条件时,如每当(重新)建立所述装置之间的通信链路(如无线信道)时,执行这些阶段(即,重新认证)。

[0084] 在一组实施例中,所述第一装置是第一网关(例如,路由器或允许数据进出连接所述第一装置和所述第二装置的局域网的其它装置)。在一些此类实施例中,所述第二装置可以是第二网关,其可以与与所述第一装置相同的外部网络接口,或与不同的外部网络接口。

[0085] 所述第一网关和第二网关可以是静态装置(即不是移动装置)。所述网关之间可能具有持久的通信信道,如有线链接。然而,即使在通信信道持久存在的情况下,也可能需要间隔地执行承诺、检查和摘要阶段。所述装置可以以每秒一次的频率进行重新认证,或者甚至更频繁地进行重新认证,例如每秒五十次或更多次。通过确保蛮力破解安全性所需的时间比任何一次认证会话的持续时间要长得多,这可以提供针对潜在攻击者的更大的安全性,从而甚至可以抵抗基于量子计算的攻击。

[0086] 在一些实施例中,所述系统可以在所述第一装置和所述第二装置之间提供两个通信信道,其可以是公用介质(如一根以太网电缆)上的两个多路复用信道,或者是可以使用不同的相应介质(如一对以太网电缆)的两个多路复用信道。所述系统可以被配置成使得在任何时间点,所述两个信道中的至多一个信道提供经认证的信道,所述信道已被用于执行本文所公开的承诺、检查和摘要阶段,而另一个信道断开(即不用于任何数据通信)或仅用于不敏感的通信。所述经认证的信道可以用于敏感通信。所述装置可以以规则间隔交替改变所述两个信道中的哪个信道是经认证的信道。每当经认证的信道的身份改变时,都可以执行重新认证。这种交替可能每秒发生一次,或者甚至更频繁地发生,例如每秒五十次或更多次。通过确保蛮力破解安全性所需的时间比任何一个经认证的信道的持续时间要长得多,这可以提供针对潜在攻击者的更大的安全性,从而甚至可以抵抗基于量子计算的攻击。当然,可能存在三个或更多个信道,其子集是在任何特定时间的认证。

[0087] 装置数据可以包括一个或多个属性,如特定于特定装置或装置类别的型号、唯一ID、类别、所有者等。通过选择和/或组合适当的属性,可以定义对于网络内的每个装置唯一的装置数据。私钥可以使用装置属性生成。私钥可能是在每个装置的启动期间生成的。

[0088] 可以规定装置彼此通信。预置通常不同于认证。在启动认证协议之前可能需要将

装置预置为相互通信。

[0089] 每个装置可以包括用于由处理器执行，用于实施本文公开的一个或多个步骤的软件指令。所述软件可以存储在装置的存储器中。每个装置可以包括以下一项或多项：CPU、DSP、GPU、FPGA、ASIC、易失性存储器、非易失性存储器、输入、输出、显示器、网络连接、电源、无线电、时钟以及任何其它适当的组件。所述装置可以被配置成存储或显示或输出认证的结果。

[0090] 本文所述的任何方面或实施例的特征可以在适当的情况下应用于本文所述的任何其它方面或实施例。在参考不同的实施例或实施例组时，应当理解，这些不一定是不同的而是可以重叠。

附图说明

[0091] 现在将参考附图仅通过举例的方式来描述本发明的某些优选实施例，在附图中：

[0092] 图1是示出两个资产和代理的示意图，所述资产和代理被配置成参与体现本发明的认证协议；

[0093] 图2是流程图，其示出了体现本发明的认证协议的主要阶段；

[0094] 图3是流程图，其提供了在资产的初始部署期间实施的认证协议的“握手”阶段的更详细视图；

[0095] 图4a是流程图，其提供了在初始部署资产后对资产进行认证时实施的认证协议的“握手”阶段的第一部分的更详细视图；

[0096] 图4b是流程图，其提供了认证协议的该部署后“握手”阶段的第二部分的更详细视图；

[0097] 图5是提供了认证协议的“承诺”阶段的更详细视图的流程图；

[0098] 图6是提供了认证协议的“检查”阶段的更详细视图的流程图，在所述检查阶段中检查承诺值；

[0099] 图7是提供了认证协议的“最终摘要”阶段的更详细视图的流程图，在所述最终摘要阶段中生成并共享最终摘要值；并且

[0100] 图8是提供了认证协议的最终“里程碑”阶段的更详细视图的流程图，在所述里程碑阶段中，检查每个资产是否已通过每个必需的里程碑。

具体实施方式

[0101] 图1示出了无线传感器网络的组件，所述无线传感器网络包括资产A 100、资产B 101和被称为代理102或资产P的第三资产，所述资产和代理被配置成参与体现本发明的认证协议。所述网络可能含有比这更多的资产。这些资产中的每一个资产均含有相应的存储器103、时钟104、无线电105和处理器106。存储器103可以存储软件，所述软件包括用于在相应处理器106上执行的指令，以便执行本文所述的步骤中的一些或全部步骤。可替代地，资产100、101、102可以含有专用硬件，如密码加速器(未示出)，其用于执行至少一些步骤。资产100、101、102可以含有电池、用户界面、传感器等。这些资产通过无线电彼此通信。

[0102] 这些资产可以是例如物联网传感器或传感器集线器。例如，资产A 100可以是位于灯柱上的传感器，资产B 101可以是位于车辆上的传感器，并且代理102可以是嵌入在靠近

灯柱的道路中的传感器。在短暂的时间窗口内，车辆通过无线电接近灯柱和道路传感器，车辆传感器B可能希望先与灯柱传感器A进行认证，然后再交换来自灯柱传感器A的传感器数据。如下面更详细描述的，通过与道路传感器102进行额外的通信，保障了认证。在一些实施例中，资产A 100和资产B 101之一或两者可以是网关装置，其在两个不同的网络(如局域网和因特网)之间接口。

[0103] 图2示出了作为本发明的实施例的认证协议的概述。所述认证协议可以在图1的传感器网络或其它网络中实施。

[0104] 该协议以资产(例如，资产A 100)或资产组(将被称为资产A)向另一资产(例如，资产B 101)或资产组(将被称为资产B)发出认证信号为开始。资产B在收到此认证信号后，会向被称为“代理”或资产P的第三资产(例如，代理102)发出认证请求。然后，此代理向资产A和资产B发出进一步的请求，并且一旦每个资产成功从代理接收到此请求，认证就会继续进行。所有这些都在图2流程图的“请求”步骤2处进行。图3和图4中更详细地示出了此步骤。

[0105] 每次需要认证时都会发出一个请求，并且资产的认证将在需要认证的特定通信停止时立即停止。结果，除了故意使用认证之外，认证始终处于“关闭”状态，因此对于任何资产都没有永久认证；换句话说，认证仅在需要的基础上发生，从而提高了协议的安全性。

[0106] 所有请求均在第一通信频带(被称为频带1)上发出，所述频带可以是802.15.x信道。

[0107] 更一般地，可以在单个通信频带(频带1)上传输所有通信的情况下执行所述协议。然而，在优选实施例中，在协议期间，使用两个不同的通信频带来在不同点处传输数据。这些通信频带可以是例如任何类型的WiFi连接、蓝牙或有线连接—例如，频带1可以是802.11.x无线信道，而频带2可以是802.15.x无线信道。

[0108] 为了使资产A与资产B和代理进行认证，此特定示例实施例要求所有资产必须具有相同的预置特性，这意味着必须允许所述资产全部与所有相同的资产进行通信。资产必须具有相同的自然属性NP，其中这些自然属性可以包括字母数字字符、实数、日期、时间或组标识的任意组合。其它实施例可能没有此要求。

[0109] 认证协议的下一个阶段被称为“握手”，如图2的步骤4所示。存在两个替代性“握手”阶段。图3中详细示出的第一个4a仅在资产组的初始部署期间发生，例如，当在工厂中配置了所有资产时。第二个替代性“握手”阶段4b发生在“部署之后”(例如，从工厂进行初始部署之后)进行的任何认证期间，例如，当传感器已被安装在其它装置中时；此阶段4b在图4a和图4b中详细示出。

[0110] 如图3的阶段4a所示，当在资产的初始部署期间发生握手时，每个资产或资产组会压缩某些属性、加密这些属性并与其它资产共享。这些属性可以包含唯一ID“UID”(其是资产的硬件ID、虚拟ID和客户ID的串联)，以及“INFOx”(其是代表资产x唯一属性的数据集合)，加上基于特定资产内部时钟的时间戳记值，以及“PSx”，其是资产具有的临时规范或权限(例如，权限时间开|关、一次性工作时间、工作间隔、条件、例外、隐含、是/不是、更多/更少、至少……)。传感器的内部时钟可以使用已知的同步方法在初始设置阶段期间进行同步和/或在所述初始设置阶段后以一定间隔进行同步。硬件ID是资产制造时烘烤的唯一ID。虚拟ID是在资产首次启动期间创建的资产名称空间值的随机SHA-3散列值。客户ID是资产所属客户的唯一客户ID，并且是在初始协议部署期间创建的。然后，每个资产都使用AES密钥

(由客户或制造商预先安装在所有资产上的密钥)对这些属性进行加密。然后,这些压缩和加密的属性将通过通信频带1与参与认证过程的所有资产共享。然后,每个资产都等待所有其它资产确认接收到该属性,然后重新提交这些属性,直到接收到该确认或超时为止。所有这些共享属性由每个资产永久存储在每个资产的存储器103中。

[0111] 每个资产的预设值包含:硬件ID、型号名称、型号ID、序列号等。启动时,每个资产都会生成其唯一ID=Hardware_ID,Virtual_ID,Customer_ID。

[0112] 在认证开始之前,每个资产(包含受信任的代理)也应定义以下值:

[0113] -用于参与认证的INFO数据(不包括时间戳,所述时间戳在认证过程中添加);

[0114] -用于参与认证的临时规范数据;

[0115] -通用的AES-128加密密钥,其用于开始在资产之间共享加密的数据;

[0116] -握手超时;

[0117] -承诺交换超时;以及

[0118] -密钥交换超时。

[0119] 如图4a和图4b的阶段4b所示,当在最初部署资产后进行握手时,资产的任何属性都不会直接共享,从而提高了协议的安全性。相反,每个资产(包含代理)都会在阶段30处生成一个20位的nonce(仅使用一次的随机数)。然后,在阶段31处,每个资产都会生成时间戳并将所述时间戳写入其相应的INFO阵列。然后,在阶段32处,每个资产根据其自身属性(UID、INFO、PS)的串联来计算20位SHA-3散列值,PH(属性散列)。然后,在阶段34处,每个资产都根据阶段30的nonce的串联以及阶段32的属性散列值,进一步计算SHA-3散列值,NPH(nonced属性散列)。然后,每个资产将其NPH散列值和nonce值同时提交给频带1上的所有其它资产,并继续共享这些值,直到收到确认或超时为止,如图4b中的阶段36所示。

[0120] 如果在任何阶段资产都未收到正在传输给其它参与资产的详细信息的接收确认,并且达到了超时限制,则该资产将停止参与认证会话,如流程图中的黑色圆圈符号16所示。如果达到这种状态的是代理,则代理将停止整个认证会话(而不仅是其自身的参与)。

[0121] 如步骤38所示,一旦从其它资产接收到NPH和nonce值,每个资产将使用在部署阶段4a中获得的存储记录,通过重新计算接收到的NPH值来表示参与资产的属性。

[0122] 这些资产中的每一个都将这些替代性“握手”步骤4a或4b中的任何一个的完成记录为第一“里程碑”。在授予资产经认证状态之前,每个资产必须通过认证协议中的五个里程碑步骤,如图2所示,以及该协议的最终阶段。因此,资产需要记录(例如,将标志存储在存储器中)其已经通过了五个必需里程碑中的每一个里程碑。稍后将参考图8给出对此检查方式的解释。

[0123] 在“握手”之后,资产进入“承诺”阶段6,在图2中简要示出,并在图5中更详细地示出。在此阶段6中,每个参与资产首先在步骤40处生成204位nonce。然后,每个资产都获取其自身的私钥(所述私钥是每个资产的20位密钥,是在资产的操作系统引导期间根据资产的UID创建的,基于资产的UID并且从未共享),并且将所述私钥与在步骤40处生成的nonce串联在一起,以在步骤42处生成一次性的224位密钥。由于此密钥包含nonce,因此密钥在每个认证会话期间都是不同的,并且对于每个会话都是唯一的。

[0124] 然后在步骤44处,每个资产计算相应的承诺值,C_x。将承诺值计算为SHA-3散列函数,

[0125] C_x＝散列$_{Sx}$(UID_x、$INFO_x$、PS_x)

[0126] 其中S_x是在步骤42处生成的资产x的密钥，UID_x是资产X的硬件ID、虚拟ID和客户ID的串联，并且INFOx是描述资产X的数据集合(即，资产X的唯一属性)。此INFOx值包含时间戳，使得此INFO值特定于特定的认证会话并受时间限制。时间戳基于每个资产的内部时钟，并且这些时钟在初始设置过程中同步。PSx是资产X的临时规范或权限。因此，这些承诺值在每个认证会话中都是不同的，并且对于每个会话都是唯一的。由于在每次认证尝试中资产之间都会生成唯一的密钥，因此不存在可能被攻击者入侵的永久的密钥或证书。

[0127] 然后，在步骤46处，每个资产都使用公用AES密钥对其自身的承诺值进行加密，并通过第二通信信道(频带2)将其加密的承诺值提交给所有其它参与资产。(使用第二频带可以提供额外的安全性；然而，在一些实施例中，仅使用一个频带，即频带1。)然后，每个资产解密并存储从所有其它参与资产接收的承诺值。每个资产将继续重新提交加密的承诺值，直到收到确认或达到承诺交换超时为止。一旦资产(例如资产A)收到确认(即，所有其它资产均已收到资产A发送的承诺值的确认)，则资产A被视为已达到第二个里程碑M2。

[0128] 然后，每个资产都使用由所有资产存储的AES密钥对其一次性密钥进行加密，并将此密钥通过通信频带1提交给所有其它参与资产，如图5的阶段48和图2的阶段8所示。与承诺值一样，每个资产都重新提交此密钥值，直到从接收密钥的所有其它资产收到确认为止，或者直到达到超时限制为止，在这种情况下，已达到超时限制的特定资产停止参与认证协议，如符号16所示。一旦从所有其它资产收到确认(已收到资产密钥值)，则所述资产被视为已达到第三个里程碑M3。在特定认证会话的持续时间内，每个资产针对所述特定会话存储其它资产的已接收的密钥。

[0129] 认证协议的下一个阶段是针对每个资产，在图2的阶段10中所示的“检查承诺值”阶段中，检查所有其它资产提交的承诺值，并在图6中更详细地示出。在此阶段，每个资产都使用其自身对其它认证资产的属性的记录(这些记录在初始部署前握手阶段4a期间存储，并在握手阶段4b期间进行标识)以及上一阶段之后存储的密钥值，计算每个其它参与资产的承诺值的期望值，如阶段50所示。

[0130] 例如，资产A在阶段4b中确定哪些存储的UID、PS和INFO值对应于资产B。资产A然后使用这些值(在INFO值中，根据资产A的内部时钟包含当前时间戳)并使用先前在通信频带1上提交给资产A的资产B的密钥，计算以上给出的承诺值散列函数。

[0131] 然后，在阶段52处，每个资产检查每个它他资产最初提交的承诺值与重新计算的承诺值之间是否匹配。如果所述承诺值不匹配，则资产停止参与认证过程。如果所述承诺值确实与特定资产(例如资产A)匹配，则认为该资产已达到认证过程的第四个里程碑M4。如果所述承诺值匹配，则每个资产在阶段54处将这些重新计算的承诺值提交给代理102，并且代理检查其它资产(例如，资产A和资产B)最初提交的承诺值与从这些其它资产接收到的重新计算的承诺值是否匹配。如果值不匹配，则承诺值不匹配的资产停止参与认证过程。在一些实施例中，直到代理已经执行了这种进一步检查，才达到每个资产的第四里程碑M4。

[0132] 然后，所述过程进入“最终摘要”阶段，如图2的阶段12所示，并在图7中更详细地示出。然后，在此阶段，代理会根据其具有的其它参与资产的属性的存储记录，生成一个Ω值(也被称为最终摘要值)，如阶段60所示。具体来说，此Ω值由下式给出：

[0133] Ω＝散列$_k$(INFOS)，

[0134] 其中

[0135] $k = S_A \oplus S_B \oplus S_P$

[0136] 其中Sx是资产x的密钥，并且其中⊕表示按位XOR。

[0137] INFOS是参与认证协议的每个资产的信息的串联，在串联之前按字母顺序排序：$(UID_A、INFO_A、PS_A)$ $(UID_B、INFO_B、PS_B)$ $(UID_P、INFO_P、PS_P)$。

[0138] 尽管已经针对两个资产和代理资产举例说明了认证协议，但是应当理解，资产可以扩展到任意数量的资产。在这种情况下，INFOS将是所有参与资产的信息的串联，而k将是所有参与资产的密钥的按位XOR。

[0139] 然后，在阶段62处，通过通信频带2将此Ω值从代理发送给每个资产。然后，在阶段62处，每个资产使用其自身存储的有关所有其它认证资产的数据重新计算Ω值，然后指示这些值是否匹配。一旦资产(例如资产A)确认其重新计算的Ω值与代理提交的Ω值匹配，则该特定资产被视为已达到第五个里程碑M5。重新计算并验证此Ω值的每个资产由此确定此值已由从一开始就参与认证会话的真正代理提供。

[0140] 代理的作用是充当拥有一定信任级别的独立第三方(因为其已通过认证，并被授权扮演代理的角色，用于使用特定频带等对指定类型的装置进行认证)，以确保独立促进认证会话，验证资产A、资产B和其它参与资产(如果有的话)的承诺并在资产无法更改的认证资产中传播最终摘要值Ω。然而，资产会接收并重新计算值Ω，从而消除了欺骗代理的可能性。

[0141] 然后，认证协议的最终阶段是检查每个资产是否都通过了所有必需的里程碑，如图2的阶段14所示，并在图8中更详细地示出。此阶段可确保在认证协议期间恶意资产不能“潜入”。

[0142] 为了检查特定资产(例如资产A)是否经历了所有五个必需的里程碑，执行步骤70，在所述步骤中，资产X生成224位长度的字符串：

[0143] M＝散列$(H_P、C_P、C_X、\Omega)$

[0144] 如上文参考图6所述，其中H_P是代理的压缩AES加密属性，C_P是代理的承诺值，C_X是资产本身的承诺值，并且Ω是最终摘要值。这些属性中的每一个属性都是由资产X在所需里程碑中的相应一个里程碑之前计算或接收的，因此对应于特定里程碑。因此，正确生成此值可确认特定资产已通过所有里程碑。

[0145] 尽管在图8中未明确示出，但是在检查步骤70中，该生成的值随后被发送给代理，所述代理使用其自身对所需值的记录来重新计算值M。如果这些值匹配，则代理将生成一个224位但唯一的认证号码(UAN)，其中

[0146] UAN＝散列(M)

[0147] 并将此UAN号提交给参与认证协议的所有资产。收到此编号后，每个资产(例如资产A)接收代理和所有其它参与资产的“经认证”状态，如图8中的“是(Yes)”分支所示，这些分支指向相应的“经认证”框。相同的过程将应用于参与认证过程的所有其它资产。如果需要的话，可以记录和存储这些UAN号，例如可以将其记录到区块链中。

[0148] 在资产被认证之后，每个资产的预置可以允许具有特定权限的资产通过特定端口将特定类型的数据传递给特定资产和/或访问特定数据源。例如，如果预置了PSx数据，则成功的初始协议部署会自动授权参与资产完成PSx中定义的特定操作。随后对资产运行的每

一次成功的认证(使用部署后握手)都会自动授权资产完成相同的操作,而无需再次为资产提供授权以执行相同的操作。

[0149] 尽管在本说明书中的某些地方已使用资产A作为实例,但应当理解,该描述同样适用于资产B,以及所述资产之一或两者实际上包括资产组的情况,以及除了代理外还有三个或更多个相互认证的资产的情况。该协议允许同时认证任意数量的资产。

[0150] 在上述实例中,使用了两个通信频带,频带1和频带2,其中频带2用于共享承诺值和最终Ω值,而频带1用于认证会话期间的所有其它数据交换。如果只有一个通信频带可用,则认证协议可以继续进行,所有通信都在单个频带(频带1或频带2)上传输。

[0151] 拒信,上述认证协议实施例提供了一种点对点量子抗性认证的方法,所述方法允许任何两个数字资产或资产组彼此安全地进行认证,而无需第三方证书或公钥基础结构。此外,资产或资产组不需要互联网连接、集中式通信手段或第三方数据库来完成认证过程,从而允许去中心化实时、从头开始、始终关闭、按需的认证。在图3的初始部署"握手"阶段之后,在认证会话运行期间在参与资产之间交换的所有数据值都是随机化、一次性、单向、从不相同(在SHA-3功能内)的值,这意味着证明是零知识,因为每个资产向其它参与资产证明了自己的身份,而没有通过通信频带明确揭示任何身份数据。这带来了协议的量子抵抗力,并且没有理由重播或窃听。与仅使用共享AES密钥进行认证相比,这具有优势,所述密钥被多次使用并且是对称分组密码。如果攻击者知道AES密钥,则认证过程会受到威胁。相反,在上述认证协议实施例中,没有什么可以妥协的,因为在资产之间共享的承诺值和密钥都是都是一次性值,其对于每个会话都是特定的和唯一的。

[0152] 为了进一步说明上述认证协议实施例的优点,下面是一些可能针对该协议部署的恶意攻击的实例。对于每种可能的攻击,将提供一种解释,说明该协议如何应对这些攻击。这些陈述仅涉及参考附图公开的示例实施例;它们不一定全部均等地适用于本发明的每个实施例。

[0153] 窃听攻击

[0154] 攻击者监听有线或无线传播的信息,并将其用于未来目的。这是一种重放攻击。其可能是网络窃听或离线窃听。

[0155] 在此协议的运行期间,没有任何理由进行窃听,因为在部署后认证会话期间,所有交换的数据值都是随机的一次性单向(不可逆)值。由于资产攻击者未参与初步协议部署会(在本实施例中,所述会话对于首次运行该协议的资产是必需的),因此其对资产A(以及代理和组中的其它资产)的真实属性(UID、INFO、PS)没有初步了解,因此,资产攻击者将无法在协议的"检查承诺值"阶段中重新计算其它参与资产的正确承诺值以证明匹配,如图6所示。

[0156] 资产攻击者必须提交其它资产做出的承诺的重新计算值(不仅是指示匹配的逻辑TRUE或FALSE信号),并且代理检查其它资产最初提供的其它资产的承诺值是否匹配资产攻击者提供的代表经窃听资产的承诺值。如果代理未发现匹配,则重新计算不匹配的承诺值(即资产攻击者)的资产将被拒绝并举报。

[0157] 如果重放,当前会话中窃听的数据将无法用于下一个会话,因为在握手阶段(如图4a和图4b所示),资产攻击者将无法从接收到的散列值中导出其它参与资产和代理的真实属性,因为其缺乏有关其它参与资产和代理的真实属性(UID、INFO、PS)的初步了解。这将导

致资产攻击者无法在“检查承诺值”阶段中重新计算其它参与资产和代理的正确承诺值，如图6所示。同样，如果代理没有证明匹配，则重新计算不匹配的承诺值(即资产攻击者)的资产将被拒绝并举报。

[0158] 尽管在初始部署期间，资产共享UID、INFO、PS的AES加密值，但在图3的握手阶段中，该初始部署仅发生一次，并且此共享数据在以后的任何部署后认证会话中将一文不值。

[0159] 中间人攻击

[0160] MITM是一种窃听者攻击。攻击者进入两个资产(或资产和代理)之间，并且它们之间的所有通信仅通过攻击者进行。因此，攻击者冒充了双方，并且可以复制、更改或删除双方之间的部分数据流量，即攻击相互认证。这可以是被动攻击或主动攻击。

[0161] 为了防止MITM攻击，资产和代理在一次性初始协议部署期间通过相互之间共享其AES加密的真实属性(UID、INFO、PS)进行相互认证。假定MITM冒充了经认证的资产，因为MITM并未经过初始协议部署阶段，并且其对已被认证的资产和代理的真实属性没有任何初步了解。MITM将无法在图6的“检查承诺值”阶段中重新计算经认证的资产和代理的正确承诺值，并且不会被认证(即不受信任)以代表其可能相冒充的任何资产执行特定操作。

[0162] 伪造的资产

[0163] 在此攻击中，资产攻击者充当合法资产(例如，其已被烧毁)的副本(克隆)，并且攻击者试图通过向代理发出认证请求来尝试与其它资产进行认证会话，就像合法资产由于某种原因断开连接后所做的那样。

[0164] 即使知道AES加密密钥，伪造的资产也将无法成功通过图6的“检查承诺值”阶段。部署后协议数据交换是零知识证明，即资产和/或代理仅将其身份数据(UID、INFO、PS)的散列值共享给其它参与资产，而无需向其它资产明确透露其真实身份数据资产。

[0165] 即使伪造的资产是真正资产的完整克隆，因此知道INFO和PS数据，但仍将在图6的“检查承诺值”阶段中拒绝并举报所述伪造的资产，因为其具有NULL或不同的随机唯一ID UID＝HID.VID.CID，所述ID用于计算承诺值和最终摘要值，如上所述。

[0166] 如果资产攻击者能够在第一个一次性协议初始部署阶段(在此阶段中，资产共享其属性)期间以某种方式潜入资产组，则此操作将失败，因为非法资产将需要安装新的AES加密密钥。此AES密钥仅在合法资产通过上述协议的初始部署版本之前预先安装在所述合法资产上。

[0167] 伪造的代理

[0168] 在此攻击中，攻击者充当促进其它资产的认证过程的合法代理，并对合法资产的认证挑战(请求)做出响应。

[0169] 由于该协议实现了双向认证方法，因此所有资产也会检查代理的承诺。由于此功能，伪造的代理案例与上述伪造的资产案例相似。区别仅在于代理将被拒绝并举报的时间。在图6的“检查承诺值”阶段，代理检查并确定资产是否将继续进行认证过程的下一个阶段，真正的认证资产在此阶段将无法识别伪造的代理。然而，在图7的“最终摘要”阶段，在资产重新计算伪造的代理所宣布的最终摘要值并将所述摘要值与他们根据对真正代理属性的了解而计算出的摘要值进行比较之后，真正的资产将检测到不匹配、将代理举报为不合法并将自身从认证会话中删除。

[0170] 如果伪造的代理在第一次一次性初始部署协议期间以某种方式潜入进行认证的

资产组，则伪造的代理也将失败，因为所述代理必须安装新的AES加密密钥才能解密其它资产的属性，并了解所述其它资产的UID、INFO和PS。AES密钥仅在合法资产通过初始部署协议之前预先安装在所述合法资产上。

[0171] 重播攻击(在下一个部署后会话中)

[0172] 在此攻击中，攻击者尝试在下一个会话中重播特定资产的认证会话值(在先前的会话中窃听的)，从而试图使代理和其它资产认为攻击者是合法资产之一，以便经过认证。

[0173] 由于攻击者没有经历如图3所示的初始协议部署会话，因此其对资产A(以及代理和组中的其它资产)的真实属性(UID、INFO、PS)没有任何初步了解，因此无法仅根据接收到的散列数据值来解析其它资产属性。因此，当代理检查匹配时，攻击者将无法重新计算代理和其它资产的正确承诺值以证明这种匹配。此外，所有资产的INFO属性还包含时间戳。因此，在不同的(时间+x秒的时间段)，INFO属性值将不同，因此，所有其它会话的经计算的承诺值和最终摘要值都将不同。由于此功能，可以有效防止将来的认证会话中发生重放攻击。

[0174] 假设在协议的“检查承诺值”阶段中，在图6中，当真正资产必须提交其计算出的承诺值时，攻击者不计算新的承诺，而只是简单地提交较早(在先前的会话中)被窃听的被攻击的真正资产(例如资产B)的承诺值。被窃听的资产B的承诺值似乎与资产B的当前承诺值不同，后者是由代理根据其对资产B的真实属性(UID、INFO、PS)的初步了解以及当前时间戳值重新计算的。结果，代理将拒绝并举报Asset-B-Eve。

[0175] 重播攻击(在当前的部署后会话内)

[0176] 在此攻击中，攻击者尝试在当前会话中重播目标资产的认证会话值，以使代理和其它资产认为攻击者是合法资产，以便经过认证。

[0177] 由于攻击者没有经历图3的初始协议部署会话，因此其对资产A(以及代理和组中的其它资产)的真实属性(UID、INFO、PS)没有任何初步了解，因此无法根据接收到的散列数据值来解析其它资产属性。因此，当代理检查此匹配项时，攻击者将无法计算其“自身的”承诺值或重新计算代理和其它资产的正确的当前承诺值以证明这种匹配。

[0178] 在部署后握手阶段(图4a和图4b)期间传输的每个新的随机散列值和nonce在被资产接收者接收后立即变得无效(从资产接收者的角度来看)。攻击者至少需要一次性数据传输事件才能窃听数据。如果攻击者想在同一会话中传输窃听的数据，则这些相同的数据将被接收者拒绝，因为接收者已经从真正资产B接收了一次性值，然后接收者从窃听资产B接收了所述一次性值。在这种情况下，攻击者将被拒绝并举报。

[0179] 注入攻击

[0180] 通过重播攻击后可以引入此攻击。在此攻击中，攻击者尝试将虚假数据注入经认证的资产的组中。为此必须经过认证。

[0181] 由于上述协议实施例防止了重放攻击，所以也可以防止注入攻击。

[0182] 会话劫持攻击

[0183] 在此攻击中，攻击者试图通过替换代理或在会话中间偷偷进入作为代理来控制认证会话。

[0184] 由于该协议阻止了使用伪造的代理进行认证的可能性(请参见上文)，并且在每个会话结束时，都存在最终的检查里程碑阶段(图8)，如果资产未经过认证协议的所有必需里程碑，则所述阶段消除了对任何一个或多个资产进行认证的可能性，因此攻击者不可能通

过劫持会话来成功完成认证会话。

[0185] 蛮力

[0186] 蛮力攻击是一种反复试验的方法,用于获取认证会话期间资产交换的数据值。在蛮力攻击中,使用自动化软件来生成有关所需数据值的大量连续猜测。

[0187] 在此协议实施例中,使用随机的单向SHA-3散列函数对资产属性进行散列处理,并且根据散列值对该属性数据进行逆向工程化的可能性非常高。此外,会话持续时间非常短(通常少于0.01秒,具体取决于认证资产的数量);对于会话中的每个参与资产,SHA-3散列资产承诺值都不同,并且在每个新的认证会话中,SHA-3散列资产最终摘要值都不同。因此,在这样一个非常短的会话中猜测所有交换的认证值的正确组合实际上是不可能的,也是不可行的,从而将蛮力攻击的风险降至最低。

[0188] 本领域的技术人员应当理解,本发明已经通过描述其一个或多个具体实施例来说明并且不限于这些实施例;在所附权利要求的范围内,许多变化和修改是可能的。

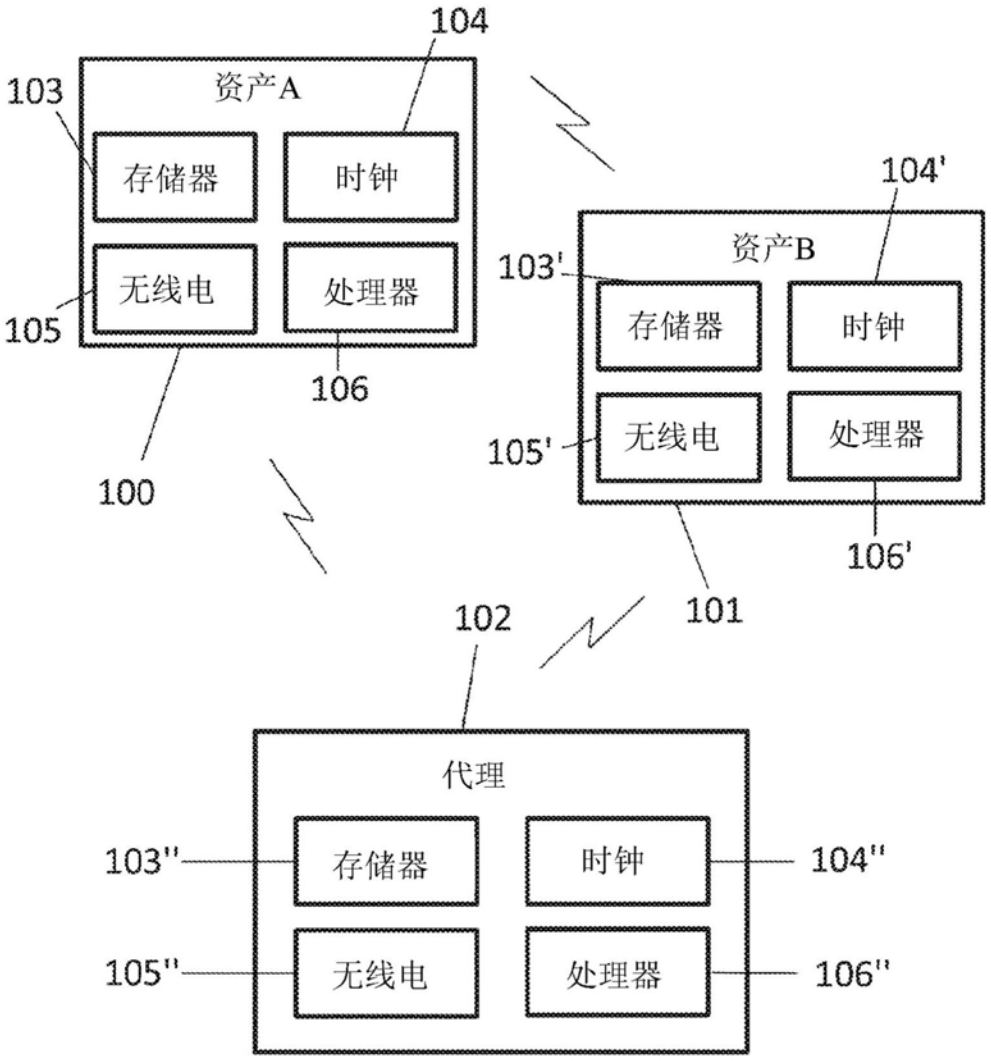

104
资产A
103
存储器
时钟
无线电
处理器
105
106
100
104'
资产B
103'
存储器
时钟
105'
无线电
处理器
106'
101
102
代理
103''
存储器
时钟
104''
105''
无线电
处理器
106''

图1

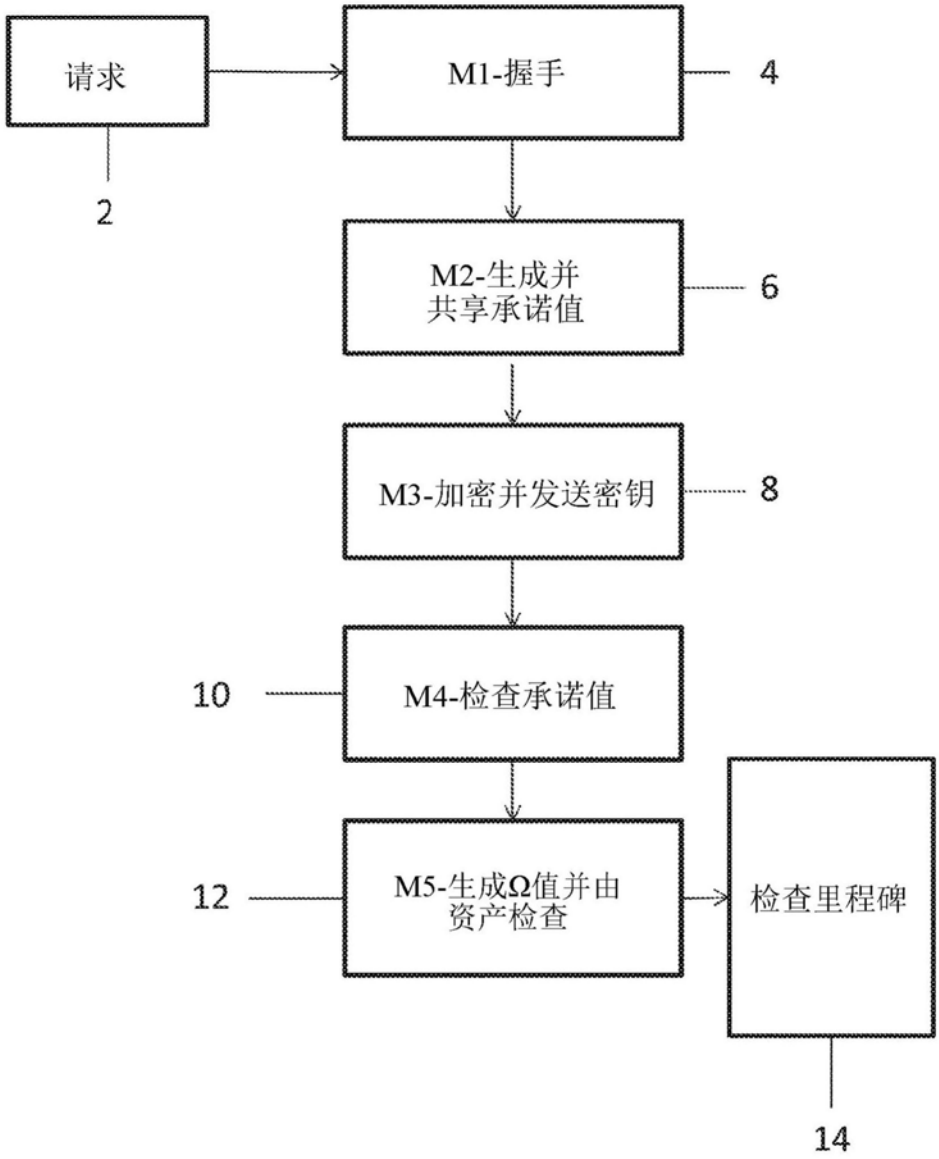

请求
2
M1-握手
4
M2-生成并
共享承诺值
6
M3-加密并发送密钥
8
10
M4-检查承诺值
12
M5-生成Ω值并由
资产检查
检查里程碑
14

图2

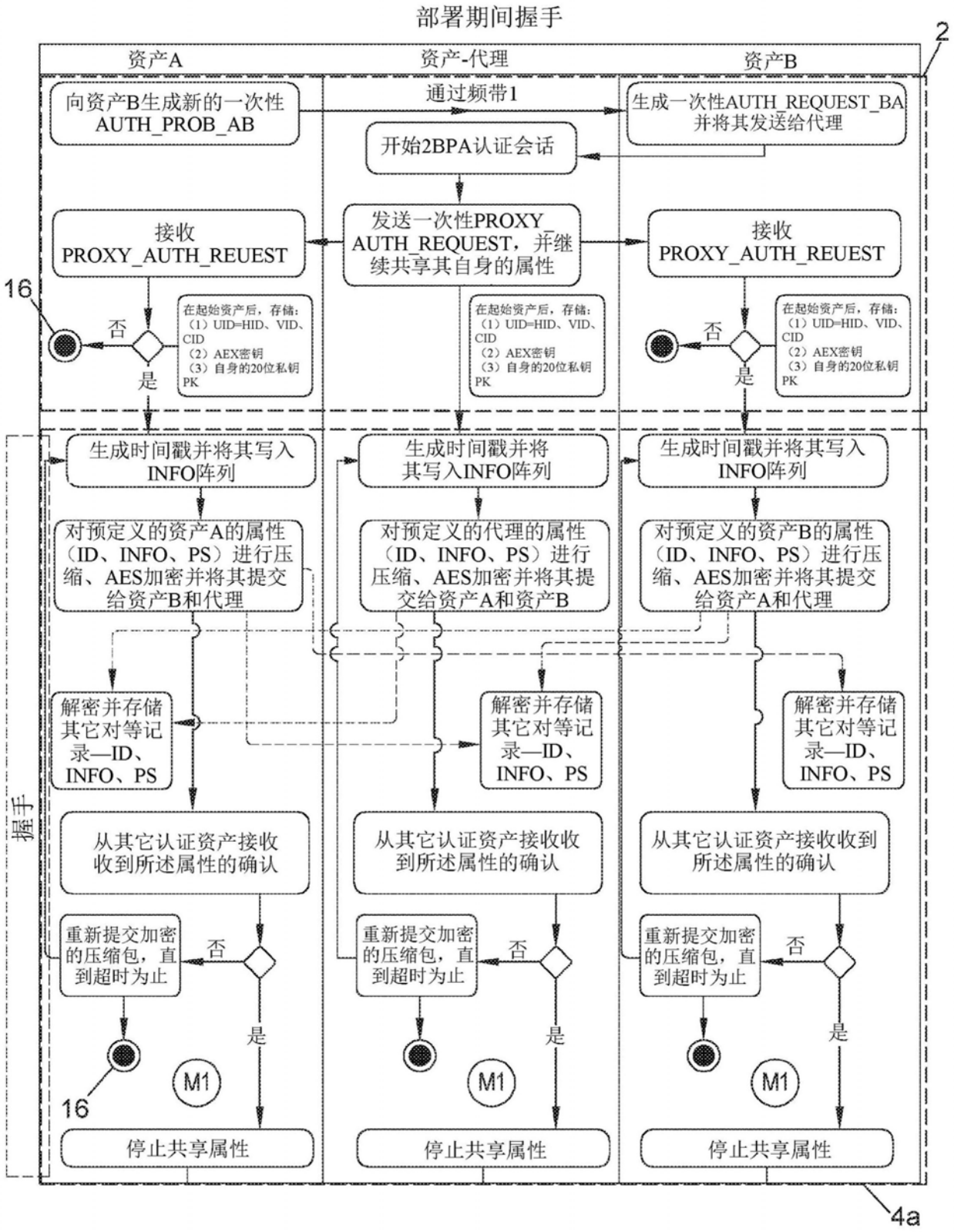

部署期间握手
2
资产A
资产-代理
资产B
向资产B生成新的一次性AUTH_PROB_AB
通过频带1
生成一次性AUTH_REQUEST_BA并将其发送给代理
开始2BPA认证会话
接收PROXY_AUTH_REUEST
发送一次性PROXY_AUTH_REQUEST，并继续共享其自身的属性
接收PROXY_AUTH_REUEST
16
否
是
在起始资产后，存储：（1）UID=HID、VID、CID（2）AEX密钥（3）自身的20位私钥PK
在起始资产后，存储：（1）UID=HID、VID、CID（2）AEX密钥（3）自身的20位私钥PK
否
是
在起始资产后，存储：（1）UID=HID、VID、CID（2）AEX密钥（3）自身的20位私钥PK
握手
生成时间戳并将其写入INFO阵列
生成时间戳并将其写入INFO阵列
生成时间戳并将其写入INFO阵列
对预定义的资产A的属性（ID、INFO、PS）进行压缩、AES加密并将其提交给资产B和代理
对预定义的代理的属性（ID、INFO、PS）进行压缩、AES加密并将其提交给资产A和资产B
对预定义的资产B的属性（ID、INFO、PS）进行压缩、AES加密并将其提交给资产A和代理
解密并存储其它对等记录—ID、INFO、PS
解密并存储其它对等记录—ID、INFO、PS
解密并存储其它对等记录—ID、INFO、PS
从其它认证资产接收收到所述属性的确认
从其它认证资产接收收到所述属性的确认
从其它认证资产接收收到所述属性的确认
重新提交加密的压缩包，直到超时为止
否
是
重新提交加密的压缩包，直到超时为止
否
是
重新提交加密的压缩包，直到超时为止
否
是
16
M1
M1
M1
停止共享属性
停止共享属性
停止共享属性
4a

图3

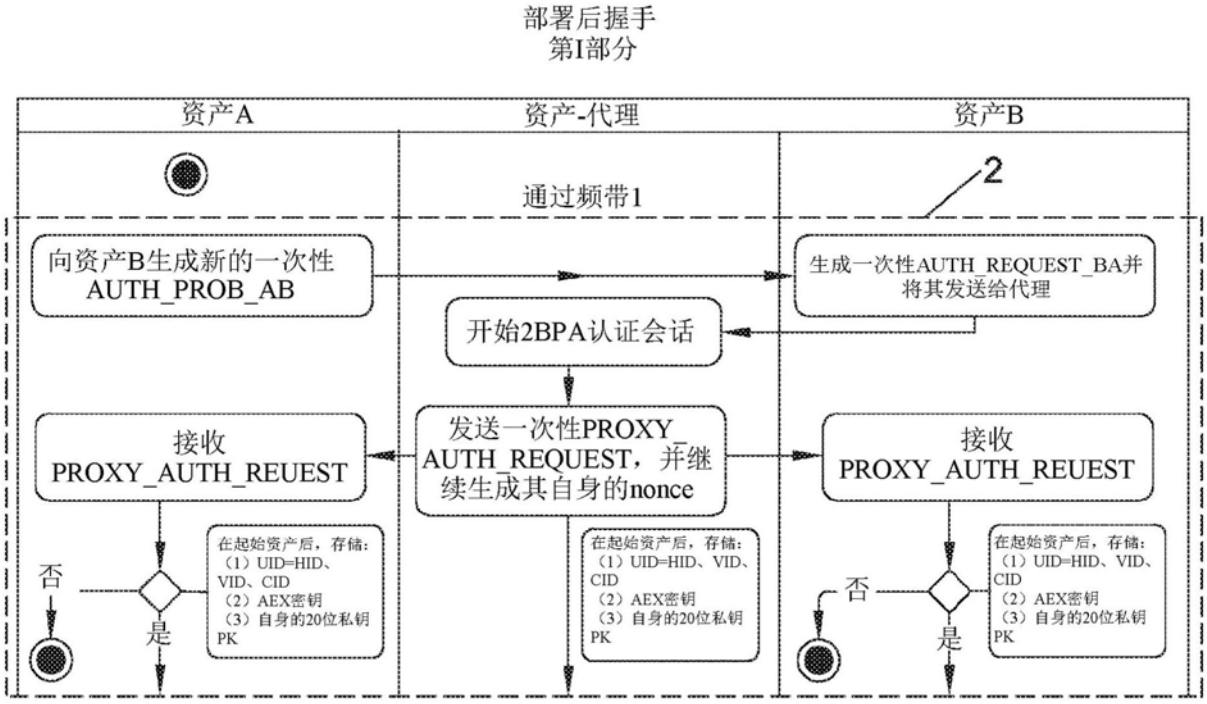

部署后握手
第I部分
资产A
资产-代理
资产B
通过频带1
2
向资产B生成新的一次性AUTH_PROB_AB
生成一次性AUTH_REQUEST_BA并将其发送给代理
开始2BPA认证会话
发送一次性PROXY_AUTH_REQUEST，并继续生成其自身的nonce
接收PROXY_AUTH_REUEST
接收PROXY_AUTH_REUEST
否
是
否
是
在起始资产后，存储：（1）UID=HID、VID、CID（2）AEX密钥（3）自身的20位私钥PK
在起始资产后，存储：（1）UID=HID、VID、CID（2）AEX密钥（3）自身的20位私钥PK
在起始资产后，存储：（1）UID=HID、VID、CID（2）AEX密钥（3）自身的20位私钥PK

图4a

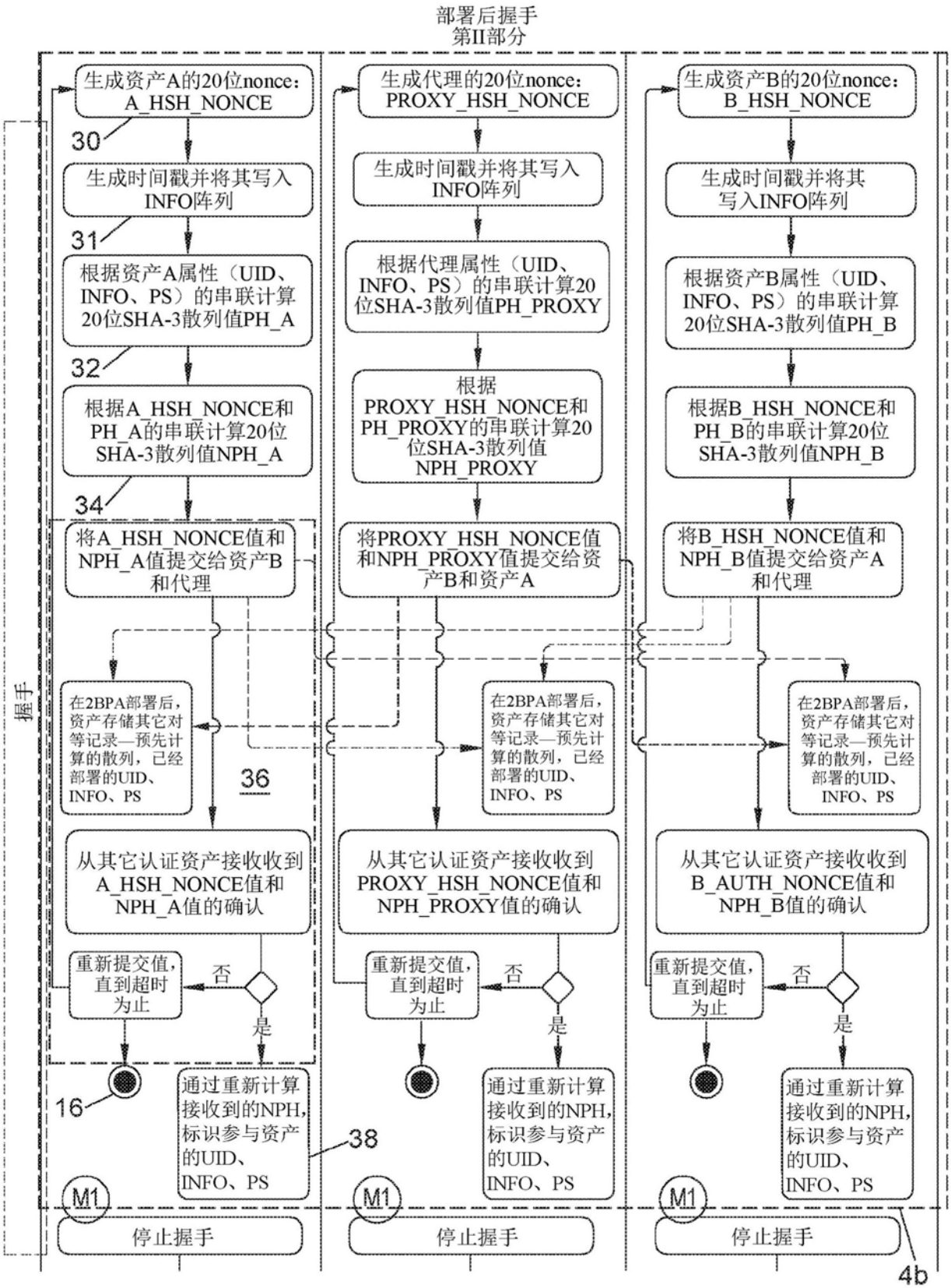

部署后握手
第II部分
握手
生成资产A的20位nonce：A_HSH_NONCE
30
生成时间戳并将其写入INFO阵列
31
根据资产A属性（UID、INFO、PS）的串联计算20位SHA-3散列值PH_A
32
根据A_HSH_NONCE和PH_A的串联计算20位SHA-3散列值NPH_A
34
将A_HSH_NONCE值和NPH_A值提交给资产B和代理
在2BPA部署后，资产存储其它对等记录—预先计算的散列，已经部署的UID、INFO、PS
36
从其它认证资产接收收到A_HSH_NONCE值和NPH_A值的确认
重新提交值，直到超时为止
否
是
16
通过重新计算接收到的NPH，标识参与资产的UID、INFO、PS
38
M1
停止握手
生成代理的20位nonce：PROXY_HSH_NONCE
生成时间戳并将其写入INFO阵列
根据代理属性（UID、INFO、PS）的串联计算20位SHA-3散列值PH_PROXY
根据PROXY_HSH_NONCE和PH_PROXY的串联计算20位SHA-3散列值NPH_PROXY
将PROXY_HSH_NONCE值和NPH_PROXY值提交给资产B和资产A
在2BPA部署后，资产存储其它对等记录—预先计算的散列，已经部署的UID、INFO、PS
从其它认证资产接收收到PROXY_HSH_NONCE值和NPH_PROXY值的确认
重新提交值，直到超时为止
否
是
通过重新计算接收到的NPH，标识参与资产的UID、INFO、PS
M1
停止握手
生成资产B的20位nonce：B_HSH_NONCE
生成时间戳并将其写入INFO阵列
根据资产B属性（UID、INFO、PS）的串联计算20位SHA-3散列值PH_B
根据B_HSH_NONCE和PH_B的串联计算20位SHA-3散列值NPH_B
将B_HSH_NONCE值和NPH_B值提交给资产A和代理
在2BPA部署后，资产存储其它对等记录—预先计算的散列，已经部署的UID、INFO、PS
从其它认证资产接收收到B_AUTH_NONCE值和NPH_B值的确认
重新提交值，直到超时为止
否
是
通过重新计算接收到的NPH，标识参与资产的UID、INFO、PS
M1
停止握手
4b

图4b

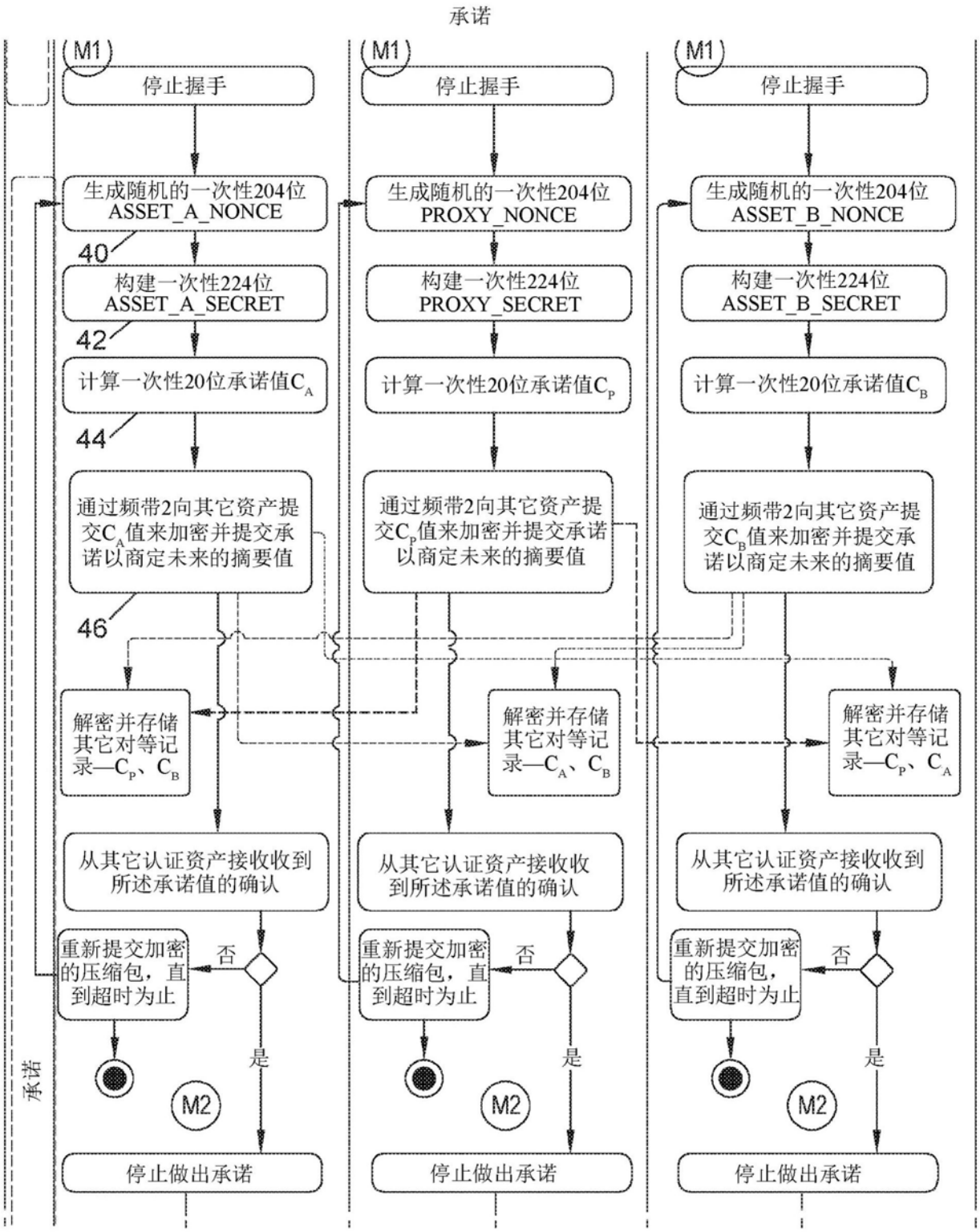

承诺
M1
停止握手
生成随机的一次性204位 ASSET_A_NONCE
40
构建一次性224位 ASSET_A_SECRET
42
计算一次性20位承诺值C_A
44
通过频带2向其它资产提交C_A值来加密并提交承诺以商定未来的摘要值
46
解密并存储其它对等记录—C_P、C_B
从其它认证资产接收收到所述承诺值的确认
重新提交加密的压缩包，直到超时为止
否
是
M2
停止做出承诺
M1
停止握手
生成随机的一次性204位 PROXY_NONCE
构建一次性224位 PROXY_SECRET
计算一次性20位承诺值C_P
通过频带2向其它资产提交C_P值来加密并提交承诺以商定未来的摘要值
解密并存储其它对等记录—C_A、C_B
从其它认证资产接收收到所述承诺值的确认
重新提交加密的压缩包，直到超时为止
否
是
M2
停止做出承诺
M1
停止握手
生成随机的一次性204位 ASSET_B_NONCE
构建一次性224位 ASSET_B_SECRET
计算一次性20位承诺值C_B
通过频带2向其它资产提交C_B值来加密并提交承诺以商定未来的摘要值
解密并存储其它对等记录—C_P、C_A
从其它认证资产接收收到所述承诺值的确认
重新提交加密的压缩包，直到超时为止
否
是
M2
停止做出承诺
承诺

图5

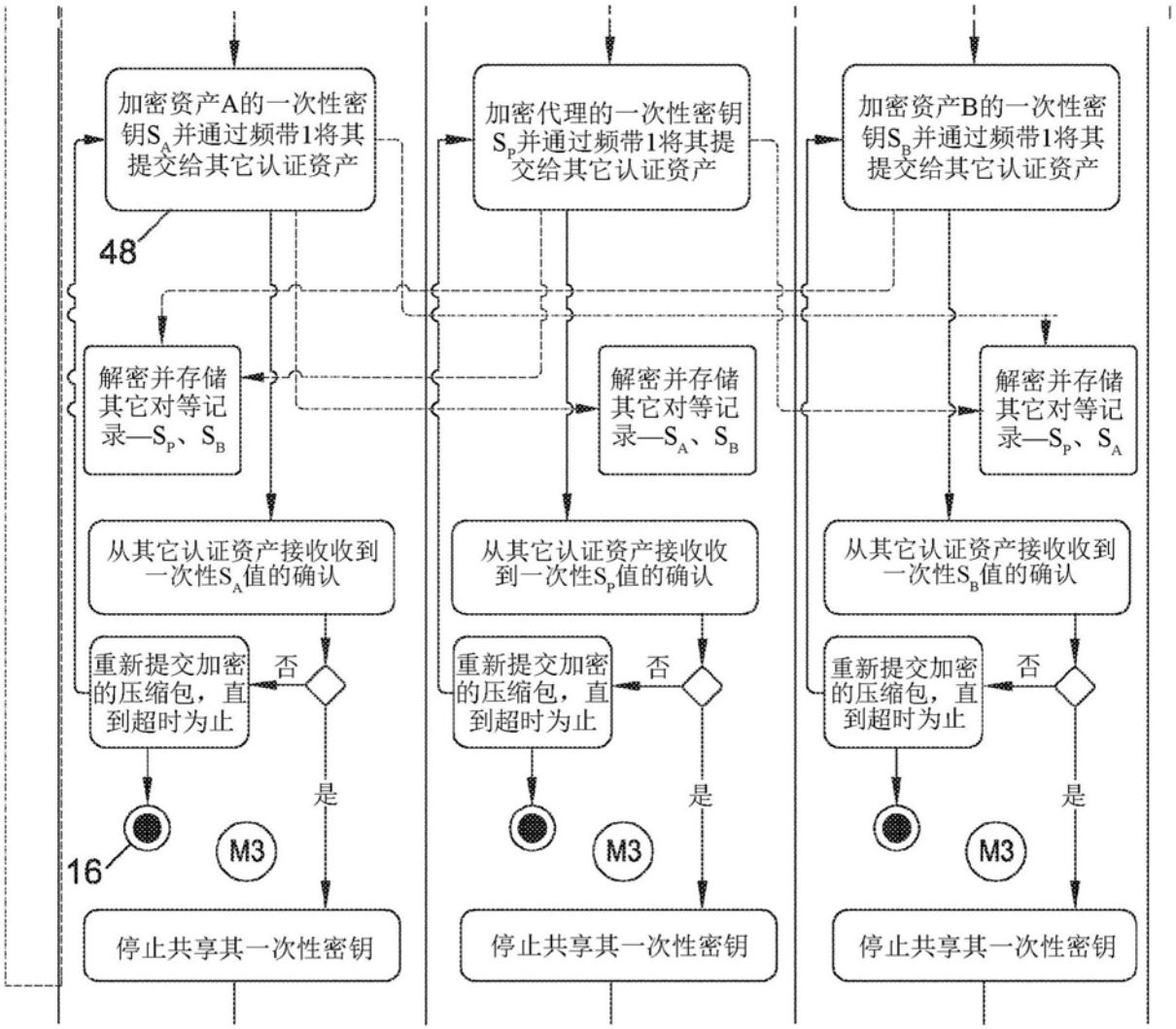

加密资产A的一次性密钥S_A并通过频带1将其提交给其它认证资产
48
解密并存储其它对等记录—S_P、S_B
从其它认证资产接收收到一次性S_A值的确认
重新提交加密的压缩包，直到超时为止
否
是
16
M3
停止共享其一次性密钥
加密代理的一次性密钥S_P并通过频带1将其提交给其它认证资产
解密并存储其它对等记录—S_A、S_B
从其它认证资产接收收到一次性S_p值的确认
重新提交加密的压缩包，直到超时为止
否
是
M3
停止共享其一次性密钥
加密资产B的一次性密钥S_B并通过频带1将其提交给其它认证资产
解密并存储其它对等记录—S_P、S_A
从其它认证资产接收收到一次性S_B值的确认
重新提交加密的压缩包，直到超时为止
否
是
M3
停止共享其一次性密钥

图5续

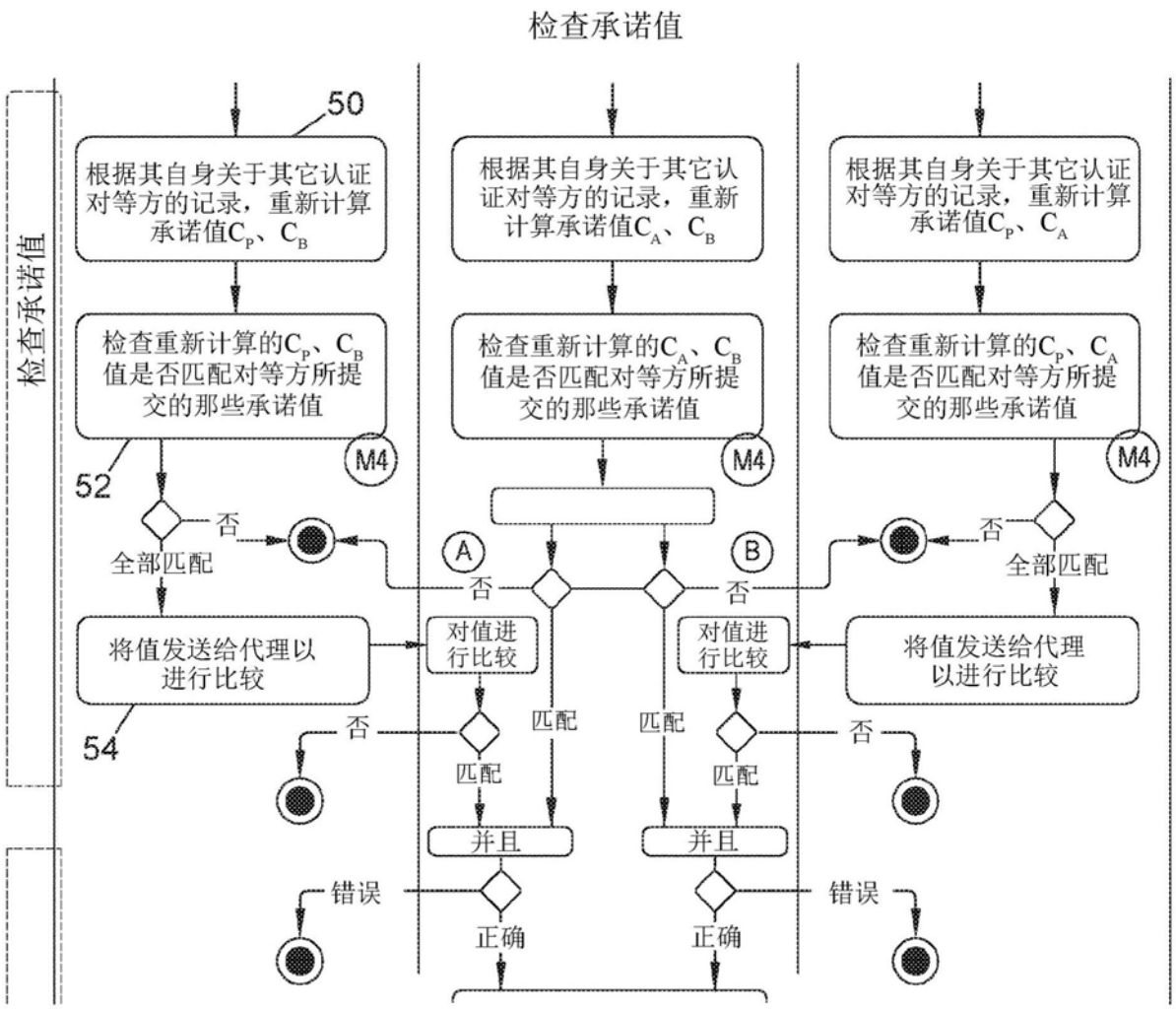

检查承诺值
检查承诺值
50
根据其自身关于其它认证对等方的记录，重新计算承诺值C_P、C_B
根据其自身关于其它认证对等方的记录，重新计算承诺值C_A、C_B
根据其自身关于其它认证对等方的记录，重新计算承诺值C_P、C_A
检查重新计算的C_P、C_B值是否匹配对等方所提交的那些承诺值
检查重新计算的C_A、C_B值是否匹配对等方所提交的那些承诺值
检查重新计算的C_P、C_A值是否匹配对等方所提交的那些承诺值
M4
M4
M4
52
否
全部匹配
A
否
B
否
否
全部匹配
将值发送给代理以进行比较
对值进行比较
对值进行比较
将值发送给代理以进行比较
54
否
匹配
匹配
匹配
否
并且
并且
错误
正确
正确
错误

图6

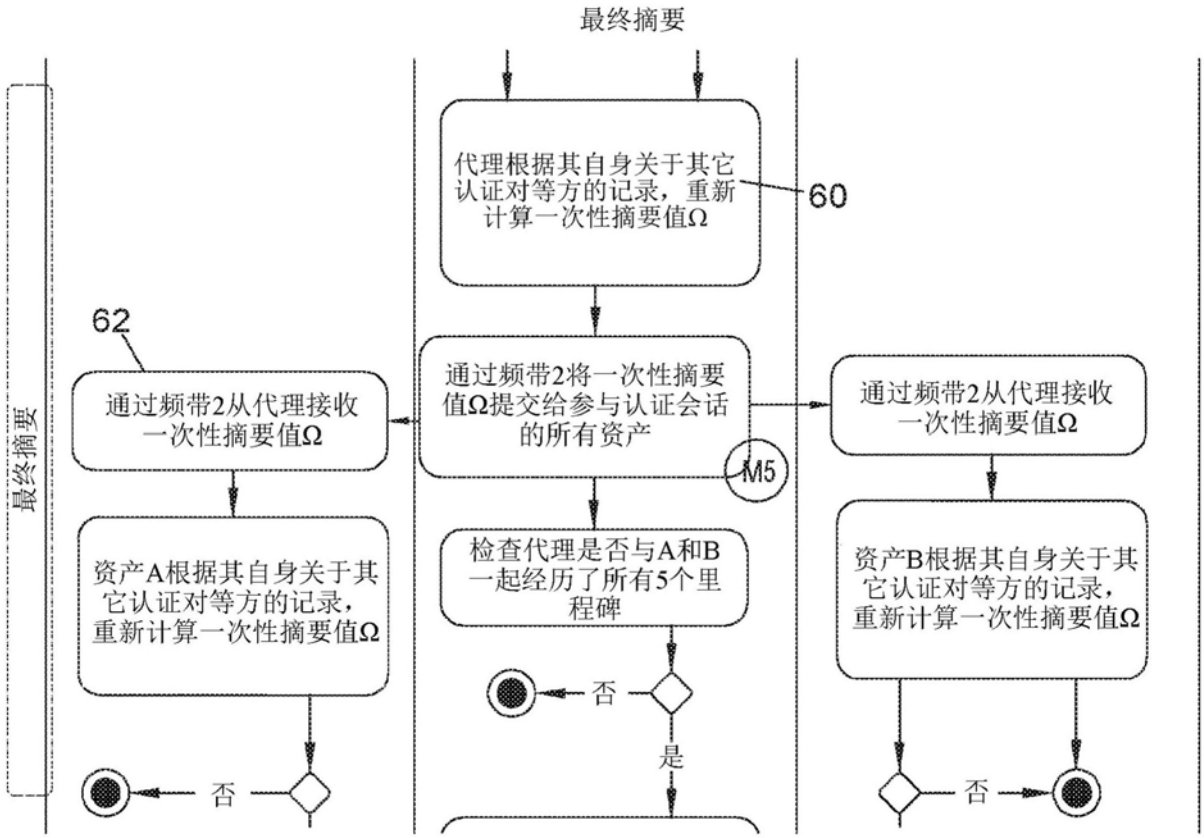

最终摘要
最终摘要
代理根据其自身关于其它认证对等方的记录，重新计算一次性摘要值Ω
60
62
通过频带2从代理接收一次性摘要值Ω
通过频带2将一次性摘要值Ω提交给参与认证会话的所有资产
M5
通过频带2从代理接收一次性摘要值Ω
资产A根据其自身关于其它认证对等方的记录，重新计算一次性摘要值Ω
检查代理是否与A和B一起经历了所有5个里程碑
资产B根据其自身关于其它认证对等方的记录，重新计算一次性摘要值Ω
否
是
否
否

图7

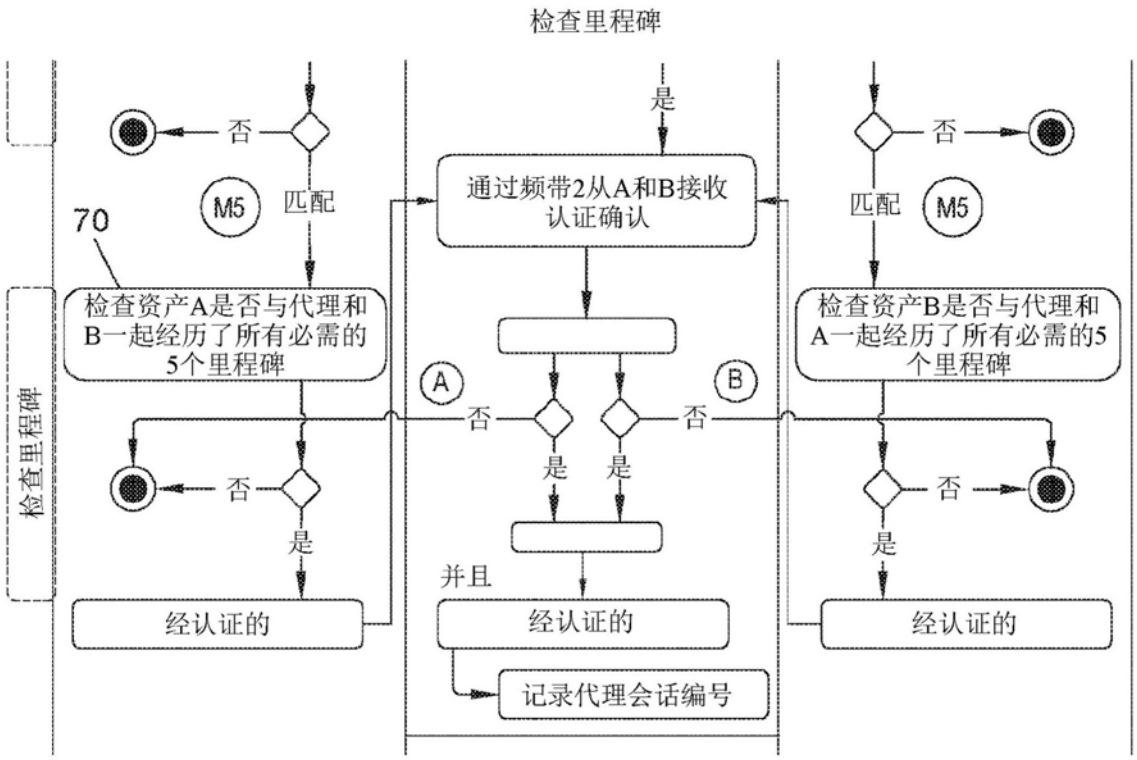

检查里程碑
检查里程碑
否
M5
匹配
70
检查资产A是否与代理和B一起经历了所有必需的5个里程碑
否
是
经认证的
是
通过频带2从A和B接收认证确认
A
否
是
并且
经认证的
记录代理会话编号
B
否
是
否
匹配
M5
检查资产B是否与代理和A一起经历了所有必需的5个里程碑
否
是
经认证的

图8