



(21) 申请号 201980042114.3

(22) 申请日 2019.06.27

(65) 同一申请的已公布的文献号
申请公布号 CN 112400295 A

(43) 申请公布日 2021.02.23

(30) 优先权数据
18183913.5 2018.07.17 EP

(85) PCT国际申请进入国家阶段日
2020.12.22

(86) PCT国际申请的申请数据
PCT/EP2019/067151 2019.06.27

(87) PCT国际申请的公布数据
W02020/015974 EN 2020.01.23

(73) 专利权人 亚萨合莱有限公司
地址 瑞典斯德哥尔摩

(72) 发明人 哈坎·奥尔松 弗兰斯·伦德贝里

(74) 专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 唐京桥 侯艳超

(51) Int.Cl.
H04L 9/08 (2006.01)
H04L 9/40 (2022.01)
H04L 9/32 (2006.01)

(56) 对比文件
CN 101430751 A, 2009.05.13
CN 105577383 A, 2016.05.11
US 2013205379 A1, 2013.08.08
US 8437474 B2, 2013.05.07
W0 2018125989 A2, 2018.07.05

审查员 万林青

权利要求书3页 说明书6页 附图3页

(54) 发明名称

管理与单个公共密钥相关联的多个用户设备的中央私密密钥

(57) 摘要

提供了用于管理与单个公共密钥相关联的多个用户设备的中央私密密钥的方法。该方法在密钥管理器中被执行并且包括以下步骤：从第一用户设备接收转换数据和第二用户设备的标识符；获得与第一用户设备相关联的第一中央私密密钥；通过将转换数据应用于第一中央私密密钥来生成第二中央私密密钥，其中，以与第一用户设备将转换数据应用于第一用户设备的设备私密密钥的方式相反的方式应用相同的转换数据；以及存储与第二用户设备相关联的第二中央私密密钥。



1. 一种用于管理与单个公共密钥相关联的多个用户设备 (2a至2c) 的中央私密密钥的方法,所述方法在密钥管理器 (1) 中执行并且包括以下步骤:

从第一用户设备 (2a) 接收 (40) 转换数据和第二用户设备 (2b) 的标识符;

获得 (42) 与和所述公共密钥相关联的所述第一用户设备 (2a) 相关联的第一中央私密密钥;

通过将所述转换数据应用于所述第一中央私密密钥来生成 (44) 第二中央私密密钥,其中,以与所述第一用户设备 (2a) 将所述转换数据应用于所述第一用户设备 (2a) 的设备私密密钥的方式相反的方式应用相同的转换数据以生成第二设备私密密钥,以确保所述第二中央私密密钥和所述第二设备私密密钥也与所述公共密钥相关联;

存储 (46) 与所述第二用户设备 (2b) 相关联的所述第二中央私密密钥;以及

使用所述密钥管理器与所述第二用户设备之间的安全通信,再次执行所述密钥管理器与所述第二用户设备之间的生成 (44),从而产生演进的所述第二设备私密密钥和演进的所述第二中央私密密钥,所述演进的所述第二设备私密密钥和所述演进的所述第二中央私密密钥二者也与所述公共密钥相关联。

2. 根据权利要求1所述的方法,其中,生成 (44) 所述第二中央私密密钥的步骤包括:将所述转换数据作为数值偏移应用于现有的中央私密密钥。

3. 根据权利要求1或2所述的方法,还包括以下步骤:

接收 (48) 对所述多个用户设备 (2a至2c) 中的一个用户设备执行密码动作的请求,所述请求与所述多个用户设备 (2a至2c) 中的特定的一个用户设备相关联;

选择 (50) 与和所述请求相关联的用户设备相对应的中央私密密钥,从而产生选择的私密密钥;以及

与和所述请求相关联的用户设备协作 (52),使得所述选择的中央私密密钥由所述密钥管理器 (1) 应用以及和所述请求相关联的用户设备的设备私密密钥由和所述请求相关联的用户设备应用,由此执行所述密码动作。

4. 根据权利要求3所述的方法,其中,与和所述请求相关联的用户设备协作 (52) 的步骤包括以下子步骤:

将所述选择的中央私密密钥应用于 (52a) 数据集,从而产生所得到的数据;以及
发送 (52b) 所述所得到的数据。

5. 根据权利要求3所述的方法,其中,所述密码动作是对数据集进行解密。

6. 根据权利要求3所述的方法,其中,所述密码动作是对数据集进行签名。

7. 根据权利要求1或2的方法,其中,所述转换数据包括数值。

8. 一种用于管理与单个公共密钥相关联的多个用户设备 (2a至2c) 的中央私密密钥的密钥管理器 (1),所述密钥管理器 (1) 包括:

处理器 (60);以及

存储指令 (67) 的存储器 (64),所述指令 (67) 在由所述处理器执行时使所述密钥管理器 (1) 进行以下操作:

从第一用户设备 (2a) 接收转换数据和与所述公共密钥相关联的第二用户设备 (2b) 的标识符;

获得与所述第一用户设备 (2a) 相关联的第一中央私密密钥;

通过将所述转换数据应用于所述第一中央私密密钥来生成第二中央私密密钥,其中,以与所述第一用户设备(2a)将所述转换数据应用于所述第一用户设备(2a)的设备私密密钥的方式相反的方式应用相同的转换数据以生成第二设备私密密钥,以确保所述第二中央私密密钥和所述第二设备私密密钥也与所述公共密钥相关联;

存储与所述第二用户设备(2b)相关联的所述第二中央私密密钥;以及

使用所述密钥管理器与所述第二用户设备之间的安全通信,再次执行所述密钥管理器与所述第二用户设备之间的生成,从而产生演进的所述第二设备私密密钥和演进的所述第二中央私密密钥,所述演进的所述第二设备私密密钥和所述演进的所述第二中央私密密钥二者也与所述公共密钥相关联。

9. 根据权利要求8所述的密钥管理器(1),其中,用于生成所述第二中央私密密钥的指令包括在由所述处理器执行时使所述密钥管理器(1)将所述转换数据作为数值偏移应用于现有的中央私密密钥的指令(67)。

10. 根据权利要求8或9所述的密钥管理器(1),还包括在由所述处理器执行时使所述密钥管理器(1)进行以下操作的指令(67):

接收对所述多个用户设备(2a至2c)中的一个用户设备执行密码动作的请求,所述请求与所述多个用户设备(2a至2c)中的特定的一个用户设备相关联;

选择与和所述请求相关联的用户设备相对应的中央私密密钥,从而产生选择的私密密钥;以及

与和所述请求相关联的用户设备协作,使得所述选择的中央私密密钥由所述密钥管理器(1)应用以及和所述请求相关联的用户设备的设备私密密钥由和所述请求相关联的用户设备应用,由此执行所述密码动作。

11. 根据权利要求10所述的密钥管理器(1),其中,用于与和所述请求相关联的用户设备协作的指令包括在由所述处理器执行时使所述密钥管理器(1)进行以下操作的指令(67):

将所述选择的中央私密密钥应用于数据集,从而产生所得到的数据;以及
发送所述所得到的数据。

12. 根据权利要求10所述的密钥管理器(1),其中,所述密码动作是对数据集进行解密。

13. 根据权利要求10所述的密钥管理器(1),其中,所述密码动作是对数据集进行签名。

14. 根据权利要求8或9所述的密钥管理器(1),其中,所述转换数据包括数值。

15. 一种计算机可读装置,其上存储有用于管理与单个公共密钥相关联的多个用户设备(2a至2c)的中央私密密钥的计算机程序(67,91),所述计算机程序包括计算机程序代码,所述计算机程序代码当在密钥管理器(1)上运行时使所述密钥管理器进行以下操作:

从第一用户设备(2a)接收转换数据和第二用户设备(2b)的标识符;

获得与和所述公共密钥相关联的所述第一用户设备(2a)相关联的第一中央私密密钥;

通过将所述转换数据应用于所述第一中央私密密钥来生成第二中央私密密钥,其中,以与所述第一用户设备(2a)将所述转换数据应用于所述第一用户设备(2a)的设备私密密钥的方式相反的方式应用相同的转换数据以生成第二设备私密密钥,以确保所述第二中央私密密钥和所述第二设备私密密钥也与所述公共密钥相关联;

存储与所述第二用户设备(2b)相关联的所述第二中央私密密钥;以及

使用所述密钥管理器与所述第二用户设备之间的安全通信,再次执行所述密钥管理器与所述第二用户设备之间的生成,从而产生演进的第二设备私密密钥和演进的第二中央私密密钥,所述演进的第二设备私密密钥和所述演进的第二中央私密密钥二者也与所述公共密钥相关联。

管理与单个公共密钥相关联的多个用户设备的中央私密密钥

技术领域

[0001] 本发明涉及用于管理与单个公共密钥相关联的多个用户设备的中央私密密钥的方法、密钥管理器、计算机程序和计算机程序产品。

背景技术

[0002] 密码密钥对被越来越多地例如用于数字数据的加密和签名。密码密钥对由公共密钥和私密密钥(也称为私有密钥)组成。对于对数字内容进行签名,用户使用私密密钥对数据进行签名,之后任何人都可以使用公共密钥来验证签名。对于加密,任何人都可以使用公共密钥为用户加密数据,之后只能使用私密密钥进行解密。

[0003] 因此,最重要的是将私密密钥保持为秘密的。一种解决方案是私密密钥永远不离开用户的用户设备。然而,用户可能具有多个设备,例如电话、计算机、平板计算机等。此外,有多名员工的公司可能希望规定所有员工来代表该公司,从而需要分发公司的私密密钥。理想地,一个公共密钥应适用于这些不同的设备中的所有设备。

[0004] 可以在设备之间复制私密密钥,但这会造成安全风险。设备中的一个设备可能丢失或被盗,从而危及私密密钥的所有副本的完整性。

发明内容

[0005] 一个目的是改善如何管理密码密钥对的私密密钥。

[0006] 根据第一方面,提供了用于管理与单个公共密钥相关联的多个用户设备的中央私密密钥的方法。该方法在密钥管理器中被执行并且包括以下步骤:从第一用户设备接收转换数据和第二用户设备的标识符;获得与第一用户设备相关联的第一中央私密密钥;通过将转换数据应用于第一中央私密密钥来生成第二中央私密密钥,其中,以与第一用户设备将转换数据应用于第一用户设备的设备私密密钥的方式相反的方式应用相同的转换数据;以及存储与第二用户设备相关联的第二中央私密密钥。

[0007] 生成第二中央私密密钥的步骤可以包括:将转换数据作为数值偏移应用于现有的中央私密密钥。

[0008] 该方法还可以包括以下步骤:接收对用户设备中的一个用户设备执行密码动作的请求,该请求与用户设备中的特定的一个用户设备相关联;选择与请求的用户设备相对应的中央私密密钥,从而产生选择的私密密钥;以及与请求的用户设备协作,使得选择的中央私密密钥由密钥管理器应用以及请求的用户设备的设备私密密钥由请求的用户设备应用,由此执行密码动作。

[0009] 与请求的用户设备协作的步骤可以包括以下子步骤:将选择的中央私密密钥应用于数据集,从而产生所得到的数据;以及发送所得到的数据。

[0010] 密码动作可以是对数据集进行解密。

[0011] 密码动作可以是对数据集进行签名。

[0012] 转换数据可以包括数值。在一个实施方式中,转换数据是数值。

[0013] 根据第二方面,提供了用于管理与单个公共密钥相关联的多个用户设备的中央私密密钥的密钥管理器。密钥管理器包括:处理器;以及存储指令的存储器,所述指令在由处理器执行时使密钥管理器进行以下操作:从第一用户设备接收转换数据和第二用户设备的标识符;获得与第一用户设备相关联的第一中央私密密钥;通过将转换数据应用于第一中央私密密钥来生成第二中央私密密钥,其中,以与第一用户设备将转换数据应用于第一用户设备的设备私密密钥的方式相反的方式应用相同的转换数据;以及存储与第二用户设备相关联的第二中央私密密钥。

[0014] 用于生成第二中央私密密钥的指令可以包括在由处理器执行时使密钥管理器将转换数据作为数值偏移应用于现有的中央私密密钥的指令。

[0015] 密钥管理器还可以包括在由处理器执行时使密钥管理器进行以下操作的指令:接收对用户设备中的一个用户设备执行密码动作的请求,该请求与用户设备中的特定的一个用户设备相关联;选择与请求的用户设备相对应的中央私密密钥,从而产生选择的私密密钥;以及与所述请求的用户设备协作,使得选择的中央私密密钥由密钥管理器应用以及请求的用户设备的设备私密密钥由请求的用户设备应用,由此执行密码动作。

[0016] 用于与请求的用户设备协作的指令可以包括在由处理器执行时使密钥管理器进行以下操作的指令:将选择的中央私密密钥应用于数据集,从而产生所得到的数据;以及发送所得到的数据。

[0017] 密码动作可以是对数据集进行解密。

[0018] 密码动作可以是对数据集进行签名。

[0019] 转换数据可以包括数值。在一个实施方式中,转换数据是数值。

[0020] 根据第三方面,提供了用于管理与单个公共密钥相关联的多个用户设备的中央私密密钥的计算机程序。该计算机程序包括计算机程序代码,所述计算机程序代码当在密钥管理器上运行时使密钥管理器进行以下操作:从第一用户设备接收转换数据和第二用户设备的标识符;获得与第一用户设备相关联的第一中央私密密钥;通过将转换数据应用于第一中央私密密钥来生成第二中央私密密钥,其中,以与第一用户设备将转换数据应用于第一用户设备的设备私密密钥的方式相反的方式应用相同的转换数据;以及存储与第二用户设备相关联的第二中央私密密钥。

[0021] 根据第四方面,提供了计算机程序产品,其包括根据第三方面的计算机程序和其上存储有计算机程序的计算机可读装置。

[0022] 通常,除非本文中另外明确定义,否则权利要求中使用的所有术语应根据其在技术领域中的普通含义进行解释。除非另外明确指出,否则对“一/一个/该元件、设备、部件、装置、步骤等”的所有引用应被公开解释为是指元件、设备、部件、装置、步骤等的至少一种实例。除非明确说明,否则本文中公开的任何方法的步骤不必以所公开的确切顺序来执行。

附图说明

[0023] 现在参照附图通过示例的方式描述本发明,在附图中:

[0024] 图1是示出可以应用本文提出的实施方式的环境的示意图;

[0025] 图2A至图2B是示出用于管理与单个公共密钥相关联的多个用户设备的中央私密密钥的方法的实施方式的流程图;

[0026] 图3是示出根据一个实施方式的图1的密钥管理器的部件的示意图;以及
[0027] 图4示出了包括计算机可读装置的计算机程序产品的一个示例。

具体实施方式

[0028] 现在将在下文中参照附图更全面地描述本发明,在附图中示出了本发明的某些实施方式。然而,本发明可以以许多不同的形式来实施,并且不应被解释为限于本文中阐述的实施方式;而是,这些实施方式通过示例的方式被提供,使得本公开内容将是透彻和完整的,并且将本发明的范围充分地传达给本领域技术人员。在整个说明书中,相同的附图标记指代相同的元件。

[0029] 本文提出的实施方式基于在密钥管理器与用户设备之间的协作中应用的私密密钥。两个实体都需要应用其相应的私密密钥,以使密码动作(例如签名或解密)发生。相应的公共密钥对应于两个私密密钥的组合动作。可以生成另外的私密密钥集,当所述另外的私密密钥集都被应用时,它们仍对应于公共密钥。

[0030] 图1是示出可以应用本文提出的实施方式的环境的示意图。

[0031] 存在多个不同的用户设备2a至2c。在该示例中,存在三个用户设备2a至2c,但是可以提供更多或更少的用户设备,只要存在至少两个用户设备即可。

[0032] 每个用户设备2a至2c被实现为具有处理和通信能力的任何合适的设备。例如,用户设备2a至2c可以被实现为具有无线连接性的可穿戴设备、移动电话、智能电话或平板/膝上型计算机。

[0033] 提供密钥管理器1以在密码密钥对方面与用户设备2a至2c协作。密钥管理器1可以被实现为形成服务器的一部分。

[0034] 提供用户设备2a至2c之一可能希望与之交互的第三方设备7。在与第三方设备7的交互中,用户设备需要执行涉及密码对的私密密钥的使用的密码动作。密码动作可以例如是对数据进行解密或对数据进行签名。

[0035] 提供通信网络6以允许不同实体彼此进行通信。通信网络6可以基于任意数目的合适的有线和/或无线协议,例如以太网、蓝牙或低功耗蓝牙(BLE)、ZigBee、任何IEEE 802.11x标准(也称为WiFi)、任何蜂窝网络等。

[0036] 图2A至图2B是示出用于管理与单个公共密钥相关联的多个用户设备(2a至2c)的中央私密密钥的方法的实施方式的流程图。该方法在密钥管理器中执行。

[0037] 在接收转换数据步骤50中,密钥管理器从第一用户设备接收转换数据和第二用户设备的标识符。该动作的原因可以是:第一用户设备的用户想要为第二用户设备生成相应的私密密钥集。

[0038] 转换数据包括(或是)数值。为了应用转换数据,使用操作以及隐式或显式的反向操作。在一个示例中,操作是加法,而隐式或显式的反向操作是减法(或者操作是减法,而隐式或显式的反向操作是加法)。然后,该操作起到偏移的作用。在另一示例中,操作是乘法,而隐式或显式的反向操作是除法(或者操作是除法,而隐式或显示的反向操作是乘法)。可以预先配置操作和反向操作,并且在该步骤中仅接收转换数据的数值。可替代地,在该步骤中还接收操作和(隐式或显式的)反向操作。

[0039] 在获得第一中央私密密钥步骤42中,密钥管理器获得与第一用户设备相关联的第

一中央私密密钥。第一中央私密密钥可以从数据存储器(见图3的66)中获得。

[0040] 在生成第二中央私密密钥步骤44中,密钥管理器通过将转换数据应用于第一中央私密密钥来生成第二中央私密密钥。与第一用户设备将转换数据应用于第一用户设备的设备私密密钥的方式相比,在此反向应用相同的转换数据。例如,可以将转换数据作为数值偏移应用于第一中央私密密钥。第一用户设备和密钥管理器中的一个将数值偏移添加至其第一私密密钥,而第一用户设备和密钥管理器中的另一个从其第一私密密钥中减去数值偏移。可替代地,可以使用乘法或除法将转换数据应用于第一中央私密密钥。在这样的情况下,第一用户设备和密钥管理器中的一个将其第一私密密钥乘以转换数据,而第一用户设备和密钥管理器中的另一个将其第一私密密钥除以转换数据。

[0041] 第一用户设备还创建了到第二用户设备的安全且经认证的信道(例如,使用特定于第二用户设备的公共密钥),并且将第二设备私密密钥传送给第二用户设备。然后,第一用户设备删除第二设备私密密钥和转换数据。

[0042] 在存储第二中央私密密钥步骤46中,密钥管理器存储与第二用户设备相关联的第二中央私密密钥。

[0043] 现在,第二用户设备可以与密钥管理器协作,以使用第二设备私密密钥和第二中央私密密钥来执行密码动作。对应于与用于第一设备私密密钥和第一中央私密密钥的组合相同的公共密钥来执行密码动作。然而,第二用户设备和密钥管理器可能不确定第一用户设备实际上删除了第二设备私密密钥。解决这个的一种方式是使用密钥管理器与第二用户设备之间的安全通信再次执行步骤44,从而生成演进的第二设备私密密钥和演进的第二中央私密密钥。由于可以利用特定于第二用户设备的密钥对来建立安全通信,因此第一用户设备不能生成相同的第二演进的设备私密密钥。

[0044] 一旦第二中央私密密钥被存储,就可以在要利用用于用户设备之一的中央私密密钥时执行以下步骤。这些步骤可以在与前述步骤完全不同的时间点处执行。

[0045] 在接收请求步骤48中,密钥管理器接收对用户设备之一执行密码动作的请求。该请求与用户设备中的特定的一个用户设备相关联。实际上,可以从该特定的用户设备接收该请求。密码动作是例如对数据集进行解密或对数据集进行签名。为了使密钥管理器信任发送请求的用户设备,每个用户设备可选地具有传统的密码密钥对作为标识符,该密钥对特定于该用户设备。因此,在这样的实施方式中,仅当用户设备通过安全信道联系密钥管理器并使用其自己的密钥对来对其自身进行标识时,服务器才将执行该请求的密码动作。

[0046] 在选择中央私密密钥步骤50中,密钥管理器选择与请求的用户设备相对应的中央私密密钥,从而产生选择的私密密钥。例如,如果第一设备在请求中请求密码动作,则密钥管理器选择第一中央私密密钥。

[0047] 在协作步骤52中,密钥管理器与请求的用户设备协作,使得选择的中央私密密钥由密钥管理器应用以及请求的用户设备的设备私密密钥由请求的用户设备应用。这导致密码动作被执行。密码动作可以例如是对数据集进行解密或对数据集进行签名。

[0048] 要注意的是,对于第二用户设备,当两个(中央私密密钥和设备私密密钥二者)第二私密密钥被应用时,结果仍然对应于原始公共密钥。换言之,可以生成任意数目的新密钥集,所述新密钥集(在应用于中央私密密钥和设备私密密钥的相应对中时)全部对应于同一公共密钥。以这种方式,可以获得多个私密密钥集,其中每个私密密钥集被应用于不同的用

户设备,其中一个私密密钥由密钥管理器存储并且一个私密密钥由用户设备存储。

[0049] 此外,可以在不影响关于同一公共密钥的任何其他中央私密密钥和设备私密密钥集的情况下由密钥管理器或用户设备来阻碍中央私密密钥和设备私密密钥的任意组合。如果例如用户设备丢失或被盗并且用户设备的私密密钥需要被阻碍,这是非常有用的。另外,由于中央私密密钥本身不足以执行密码动作,因此黑客不能仅通过对密钥管理器进行黑客操作来访问完整的私密密钥。

[0050] 现在看向图2B,其示出了图2A的协作步骤52的可选子步骤。

[0051] 在可选的应用中央密钥子步骤52a中,密钥管理器将选择的中央私密密钥应用于数据集,从而产生所得到的数据。

[0052] 当密码动作正在解密时,所得到的数据包括已经使用所讨论的用户设备的中央私密密钥进行解密的数据集。当密码动作正在签名时,所得到的数据包括使用所讨论的用户设备的中央私密密钥应用的电子签名。

[0053] 用户设备还需要执行相应的密码动作,该密码动作可以在该步骤之前或该步骤之后发生。换言之,对于要应用的签名,用户设备和密钥管理器二者需要执行密码签名。类似地,为了使解密发生,用户设备和密钥管理器二者需要执行密码解密。在一个实施方式中,当密钥管理器应用于解密时,该密钥管理器在用户设备之前执行其解密动作。以这种方式,仅密钥设备访问解密的数据。

[0054] 在可选的发送所得到的数据子步骤52b中,密钥管理器将所得到的数据例如发送回至用户设备,该用户设备发送在步骤48中接收的请求。

[0055] 图3是示出图1的密钥管理器1的部件的示意图。使用合适的中央处理单元(CPU)、多处理器、微控制器、数字信号处理器(DSP)等中的一个或更多的任意组合来提供处理器60,处理器能够执行存储器64中存储的软件指令67,该存储器因此可以是计算机程序产品。可以可选地使用专用集成电路(ASIC)、现场可编程门阵列(FPGA)等来实现处理器60。处理器60可以被配置成执行以上参照图2A至图2B描述的方法。

[0056] 存储器64可以是随机存取存储器(RAM)和/或只读存储器(ROM)的任意组合。存储器64还包括永久性存储装置,该永久性存储装置例如可以是磁存储器、光学存储器、固态存储器或甚至远程安装的存储器中的任何单个一个或组合。

[0057] 还提供了数据存储器66,用于在处理器60中执行软件指令期间读取和/或存储数据。数据存储器66可以是RAM和/或ROM的任意组合。

[0058] 密钥管理器1还包括用于与外部实体和/或内部实体进行通信的I/O接口62。可选地,I/O接口62还包括用户接口。

[0059] 为了不使本文中提出的概念模糊,省略密钥管理器1的其他部件。

[0060] 图4示出了包括计算机可读装置的计算机程序产品90的一个示例。在该计算机可读装置上,可以存储计算机程序91,该计算机程序可以使处理器执行根据本文中描述的实施方式的方法。在该示例中,计算机程序产品是光盘,例如CD(压缩盘)或DVD(数字多功能盘)或蓝光光盘。如以上所说明的,计算机程序产品还可以以设备的存储器实施,诸如图3的计算机程序产品64。尽管计算机程序91在此被示意性地示出为所描绘的光盘上的轨道,但是可以以适合于计算机程序产品例如可移动固态存储器的任何方式例如通用串行总线(USB)驱动来存储计算机程序。

[0061] 上面主要参考一些实施方式描述了本发明。然而,如本领域技术人员容易理解的那样,在所附专利权利要求所限定的本发明的范围内,除了以上公开的实施方式以外的其他实施方式同样是可能的。

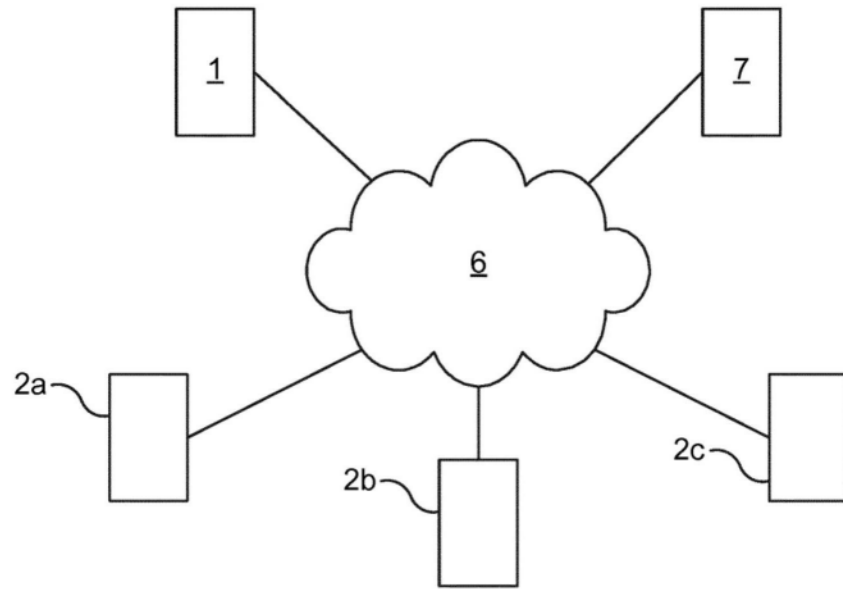


图1

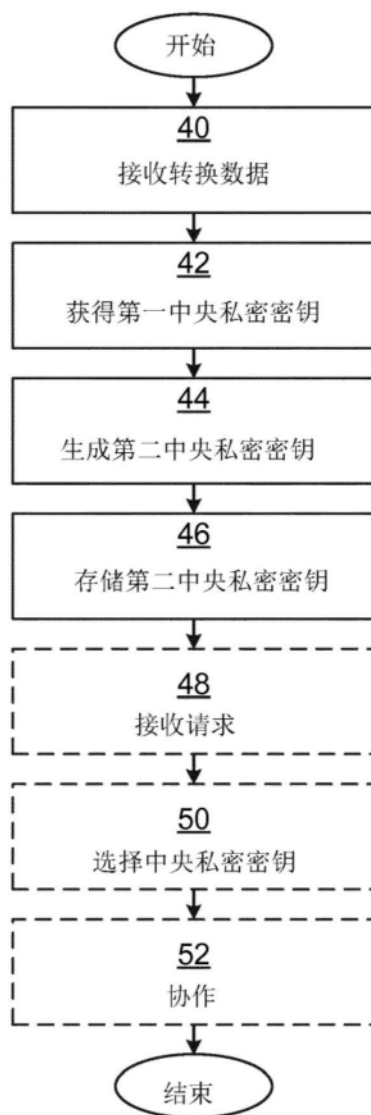


图2A

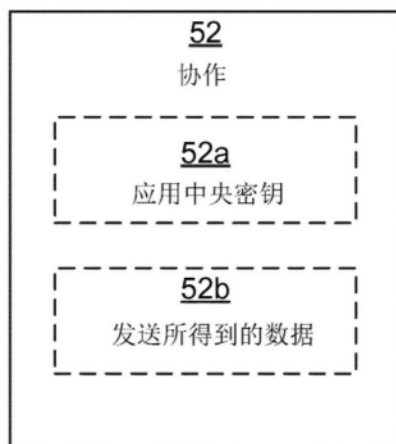


图2B

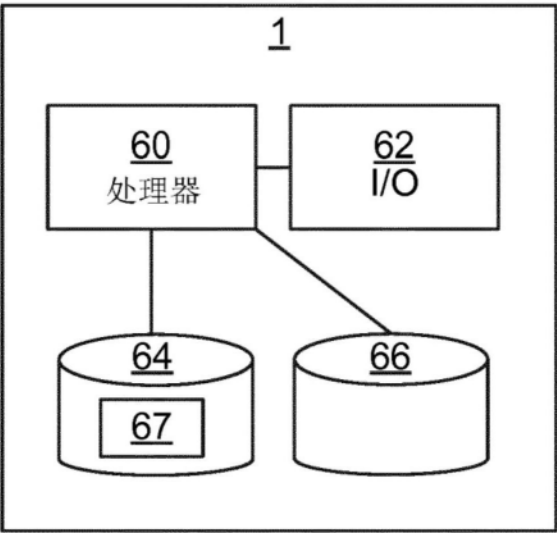


图3

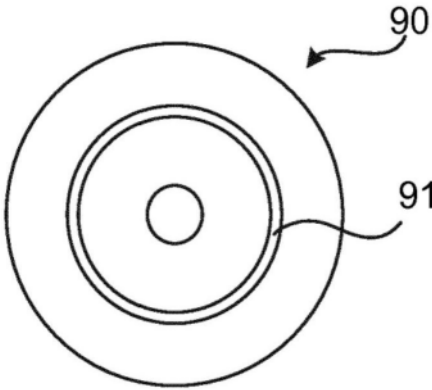


图4