(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 113826352 A
(43)申请公布日 2021.12.21

(21)申请号 202080035909.4

(22)申请日 2020.06.10

(30)优先权数据
16/449,904 2019.06.24 US

(85)PCT国际申请进入国家阶段日
2021.11.15

(86)PCT国际申请的申请数据
PCT/EP2020/066133 2020.06.10

(87)PCT国际申请的公布数据
WO2020/260026 EN 2020.12.30

(71)申请人 国际商业机器公司
地址 美国纽约

(72)发明人 E·罗德里格茨 P·卡尔纳蒂 K·博吉雷迪

(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
代理人 吴信刚

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

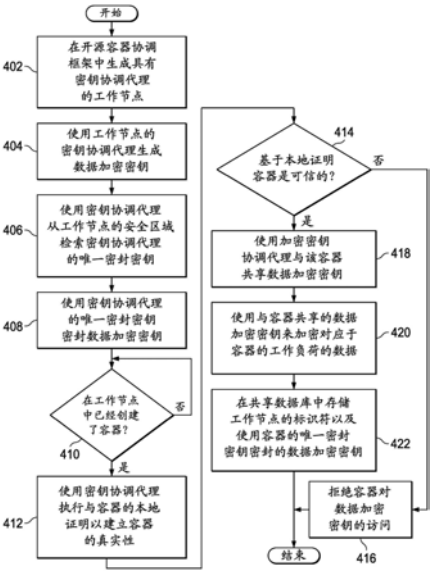
权利要求书5页 说明书12页 附图8页

(54)发明名称

多节点集群中的可信容器之间的密码密钥协调

(57)摘要

提供了访问管理容器环境中的共享敏感信息。多个工作节点中的每个工作节点能够使用数据加密密钥来访问位于多个工作节点内的安全区域中的共享的敏感应用程序数据。所述多个工作节点中的每个工作节点使用密封密钥来保护每个相应的工作节点的数据加密密钥,所述密封密钥对于相应的工作节点上的安全区域是唯一的。




CN 113826352 A

1.一种用于在管理的容器环境中访问共享的敏感信息的方法,所述方法包括:

由多个工作节点中的每个工作节点使用数据加密密钥来访问位于所述多个工作节点内的安全区域中的共享的敏感应用程序数据;以及

由所述多个工作节点中的每个工作节点使用密封密钥来保护每个相应的工作节点的所述数据加密密钥,所述密封密钥对于相应的工作节点上的所述安全区域是唯一的。

2.如权利要求1所述的方法,进一步包括:

在集群中建立第一工作节点;

由所述第一工作节点生成所述数据加密密钥;

由所述第一工作节点生成对于所述第一工作节点上的所述安全区域唯一的用于保护所述数据加密密钥的第一密封密钥,

响应于在所述集群中创建第二工作节点,由所述第一工作节点执行与所述集群中的所述第二工作节点的远程证明;以及

一旦成功执行所述远程证明,由所述第一工作节点将所述数据加密密钥的副本提供至所述第二工作节点。

3.如权利要求2所述的方法,进一步包括:

由所述第二工作节点通过使用所述第二密封密钥加密所述数据加密密钥来生成对于所述第二工作节点上的所述安全区域唯一的用于保护所述数据加密密钥的第二密封密钥。

4.一种用于在管理的容器环境中访问共享的敏感信息的系统,所述系统包括:

多个工作节点,其中:

所述多个工作节点中的每个工作节点使用数据加密密钥来访问位于所述多个工作节点内的安全区域中的共享的敏感应用程序数据;以及

所述多个工作节点中的每个工作节点使用密封密钥来保护每个相应的工作节点的所述数据加密密钥,所述密封密钥对于相应的工作节点上的所述安全区域是唯一的。

5.如权利要求4所述的系统,其中:

在集群中建立第一工作节点;

所述第一工作节点生成所述数据加密密钥;

所述第一工作节点生成对于所述第一工作节点上的所述安全区域唯一的用于保护所述数据加密密钥的第一密封密钥;

响应于在所述集群中创建第二工作节点,所述第一工作节点执行与所述集群中的所述第二工作节点的远程证明;以及

一旦成功执行所述远程证明,所述第一工作节点将所述数据加密密钥的副本提供给所述第二工作节点。

6.如权利要求5所述的系统,其中:

所述第二工作节点通过使用所述第二密封密钥加密所述数据加密密钥来生成对于所述第二工作节点上的所述安全区域唯一的用于保护所述数据加密密钥的第二密封密钥。

7.一种用于在管理的容器环境中访问共享的敏感信息的计算机程序产品,所述计算机程序产品包括计算机可读存储介质,所述计算机可读存储介质具有随其体现的程序指令,所述程序指令可由一组处理器执行以使该组处理器执行一种方法,所述方法包括:

由多个工作节点中的每个工作节点使用数据加密密钥来访问位于所述多个工作节点

内的安全区域中的共享的敏感应用程序数据;以及

由所述多个工作节点中的每个工作节点使用密封密钥来保护每个相应的工作节点的所述数据加密密钥,所述密封密钥对于相应的工作节点上的所述安全区域是唯一的。

8.如权利要求7所述的计算机程序产品,进一步包括:

在集群中建立第一工作节点;

由所述第一工作节点生成所述数据加密密钥;

由所述第一工作节点生成对于所述第一工作节点上的所述安全区域唯一的用于保护所述数据加密密钥的第一密封密钥;

响应于在所述集群中创建第二工作节点,由所述第一工作节点执行与所述集群中的所述第二工作节点的远程证明;以及

一旦成功执行所述远程证明,由所述第一工作节点将所述数据加密密钥的副本提供至所述第二工作节点。

9.如权利要求8所述的计算机程序产品,进一步包括:

由所述第二工作节点通过使用所述第二密封密钥加密所述数据加密密钥来生成对于所述第二工作节点上的所述安全区域唯一的用于保护所述数据加密密钥的第二密封密钥。

10.一种用于密码密钥协调的计算机实现方法,所述计算机实现方法包括:

在开源容器协调框架的集群中生成具有第一密钥协调代理的第一工作节点;

使用所述第一工作节点的所述第一密钥协调代理生成数据加密密钥;

使用所述第一密钥协调代理从所述第一工作节点的安全区域检索所述第一密钥协调代理的密封密钥;以及

使用所述第一密钥协调代理的所述密封密钥密封所述数据加密密钥。

11.如权利要求10所述的计算机实现方法,进一步包括:

确定是否已在所述第一工作节点中创建容器;以及

响应于确定已在所述第一工作节点中创建容器,使用所述第一密钥协调代理执行与所述容器的本地证明以建立所述容器的真实性。

12.如权利要求11所述的计算机实现方法,进一步包括:

基于所述本地证明来确定所述容器是否可信;以及

响应于基于所述本地证明确定所述容器是不可信的,拒绝所述容器对所述数据加密密钥的访问。

13.如权利要求12所述的计算机实现方法,进一步包括:

响应于基于所述本地证明确定所述容器是可信的,使用所述第一密钥协调代理与所述容器共享所述数据加密密钥;

使用与所述容器共享的所述数据加密密钥来加密对应于所述容器的工作负荷的数据;以及

在共享数据库中存储所述第一工作节点的标识符以及使用所述容器的唯一密封密钥密封的所述数据加密密钥。

14.如权利要求10所述的计算机实现方法,进一步包括:

在所述集群内生成具有第二密钥协调代理的第二工作节点;以及

使用所述第二工作节点的所述第二密钥协调代理执行与所述第一工作节点的所述第

一密钥协调代理的远程证明以建立所述第二密钥协调代理的真实性。

15.如权利要求14所述的计算机实现方法,进一步包括:

基于所述远程证明来判定所述第二密钥协调代理是否可信;以及

响应于基于所述远程证明确定所述第二密钥协调代理是不可信的,拒绝所述第二密钥协调代理对所述第一密钥协调代理的所述数据加密密钥的访问。

16.如权利要求15所述的计算机实现方法,进一步包括:

响应于基于所述远程证明确定所述第二密钥协调代理是可信的,使用所述第一工作节点的所述第一密钥协调代理将所述第一密钥协调代理的所述数据加密密钥与所述第二密钥协调代理共享;

使用所述第二密钥协调代理从所述第二工作节点的安全区域检索所述第二密钥协调代理的唯一密封密钥;以及

使用所述第二密钥协调代理的所述唯一密封密钥密封所述数据加密密钥。

17.如权利要求10所述的计算机实现方法,其中,即使当容器在所述集群内移动时,敏感应用程序数据也仅在可信的容器之间共享。

18.如权利要求17所述的计算机实现方法,其中,在任何形式的存储器内保护所述敏感应用程序数据。

19.一种用于密码密钥协调的计算机程序产品,所述计算机程序产品包括计算机可读存储介质,所述计算机可读存储介质具有随其体现的程序指令,所述程序指令可由一组处理器执行以使该组处理器执行一种方法,所述方法包括:

在开源容器协调框架的集群中生成具有第一密钥协调代理的第一工作节点;

使用所述第一工作节点的所述第一密钥协调代理生成数据加密密钥;

使用所述第一密钥协调代理从所述第一工作节点的安全区域检索所述第一密钥协调代理的密封密钥;以及

使用所述第一密钥协调代理的所述密封密钥密封所述数据加密密钥。

20.如权利要求19所述的计算机程序产品,进一步包括:

确定是否已在所述第一工作节点中创建容器;以及

响应于确定已在所述第一工作节点中创建容器,使用所述第一密钥协调代理执行与所述容器的本地证明以建立所述容器的真实性。

21.如权利要求20所述的计算机程序产品,进一步包括:

基于所述本地证明来判定所述容器是否可信;以及

响应于基于所述本地证明确定所述容器是不可信的,拒绝所述容器对所述数据加密密钥的访问。

22.如权利要求21所述的计算机程序产品,进一步包括:

响应于基于所述本地证明确定所述容器是可信的,使用所述第一密钥协调代理与所述容器共享所述数据加密密钥;

使用与所述容器共享的所述数据加密密钥来加密对应于所述容器的工作负荷的数据;以及

在共享数据库中存储所述第一工作节点的标识符以及用所述容器的唯一密封密钥密封的所述数据加密密钥。

23.如权利要求19所述的计算机程序产品,进一步包括:

在所述集群内生成具有第二密钥协调代理的第二工作节点;以及

使用所述第二工作节点的所述第二密钥协调代理执行与所述第一工作节点的所述第一密钥协调代理的远程证明以建立所述第二密钥协调代理的真实性。

24.如权利要求23所述的计算机程序产品,进一步包括:

基于所述远程证明来判定所述第二密钥协调代理是否可信;以及

响应于基于所述远程证明确定所述第二密钥协调代理是不可信的,拒绝所述第二密钥协调代理对所述第一密钥协调代理的所述数据加密密钥的访问。

25.如权利要求24所述的计算机程序产品,进一步包括:

响应于基于所述远程证明确定所述第二密钥协调代理是可信的,使用所述第一工作节点的所述第一密钥协调代理将所述第一密钥协调代理的所述数据加密密钥与所述第二密钥协调代理共享;

使用所述第二密钥协调代理从所述第二工作节点的安全区域检索所述第二密钥协调代理的唯一密封密钥;以及

使用所述第二密钥协调代理的所述唯一密封密钥密封所述数据加密密钥。

26.一种包括程序代码装置的计算机程序,当所述程序在计算机上运行时,所述程序代码装置适于执行如权利要求1至3或权利要求10至18中任一项所述的方法。

27.一种用于密码密钥协调的系统,所述系统可操作为:

在开源容器协调框架的集群中生成具有第一密钥协调代理的第一工作节点;

使用所述第一工作节点的所述第一密钥协调代理生成数据加密密钥;

使用所述第一密钥协调代理从所述第一工作节点的安全区域检索所述第一密钥协调代理的密封密钥;以及

使用所述第一密钥协调代理的所述密封密钥密封所述数据加密密钥。

28.如权利要求27所述的系统,其中,所述系统可操作为:

确定是否已在所述第一工作节点中创建容器;以及

响应于确定已在所述第一工作节点中创建容器,使用所述第一密钥协调代理执行与所述容器的本地证明以建立所述容器的真实性。

29.如权利要求28所述的计算机实现方法,其中,所述系统可操作为:

基于所述本地证明来判定所述容器是否可信;以及

响应于基于所述本地证明确定所述容器是不可信的,拒绝所述容器对所述数据加密密钥的访问。

30.如权利要求29所述的系统,其中,所述系统可操作为:

响应于基于所述本地证明确定所述容器是可信的,使用所述第一密钥协调代理与所述容器共享所述数据加密密钥;

使用与所述容器共享的所述数据加密密钥来加密对应于所述容器的工作负荷的数据;以及

在共享数据库中存储所述第一工作节点的标识符以及使用所述容器的唯一密封密钥密封的所述数据加密密钥。

31.如权利要求27所述的系统,其中,所述系统可操作为:

在所述集群内生成具有第二密钥协调代理的第二工作节点;以及

使用所述第二工作节点的所述第二密钥协调代理执与所述第一工作节点的所述第一密钥协调代理行远程证明以建立所述第二密钥协调代理的真实性。

32.如权利要求31所述的系统,其中,所述系统可操作为:

基于所述远程证明来判定所述第二密钥协调代理是否可信;以及

响应于基于所述远程证明确定所述第二密钥协调代理是不可信的,拒绝由所述第二密钥协调代理对所述第一密钥协调代理的所述数据加密密钥的访问。

33.如权利要求32所述的系统,其中,所述系统可操作为:

响应于基于所述远程证明确定所述第二密钥协调代理是可信的,使用所述第一工作节点的所述第一密钥协调代理将所述第一密钥协调代理的所述数据加密密钥与所述第二密钥协调代理共享;

使用所述第二密钥协调代理从所述第二工作节点的安全区域检索所述第二密钥协调代理的唯一密封密钥;以及

使用所述第二密钥协调代理的所述唯一密封密钥密封所述数据加密密钥。

34.如权利要求27所述的系统,其中,即使当容器在所述集群内移动时,敏感应用程序数据也仅在可信的容器之间共享。

35.如权利要求34所述的系统,其中,在任何形式的存储器内保护所述敏感应用程序数据。

# 多节点集群中的可信容器之间的密码密钥协调

## 技术领域

[0001] 本公开总体上涉及开源容器协调(orchestration)框架,并且更具体地涉及在开源容器协调框架的多节点集群内的可信节点与容器之间提供密码密钥协调。

## 背景技术

[0002] 例如,开源容器协调框架(诸如Kubernetes)是互连的物理和/或虚拟计算节点(即,机器)的集群,其提供容器化应用程序的自动部署、扩展和管理。开源容器协调框架代表应用程序工作负荷协调计算、联网和存储基础设施。这提供了平台即服务(PaaS)的大部分简单性,具有基础设施即服务(IaaS)的灵活性,并且使得能够跨基础设施提供商移植。

[0003] 节点集群包含两种类型的节点,主节点和工作节点。主节点负责管理集群中的工作节点。主节点是从例如应用程序编程接口、用户接口或命令行接口接收的将在集群中执行的所有操作的入口点。工作节点负责运行一个或多个工作负荷和具有在集群中的其他工作节点上运行的不同工作负荷的联网。开源容器协调框架的特征可以包括例如快速应用程序部署、自动恢复和自我修复和无缝应用程序更新。

[0004] 工作节点中的基本调度单元是容器,例如,pod。容器可共同位于工作节点上并共享资源。在开源容器协调框架中的每个容器被分配工作节点的集群内的唯一容器互联网协议地址,这允许应用程序使用端口而没有冲突的风险。目前,容器可在主机上彼此引用,但是位于一个工作节点上的容器无法直接寻址另一个工作节点内的另一个容器,其将必须使用容器的唯一互联网协议地址。容器可定义卷,诸如,例如,本地磁盘目录或网络磁盘,并且将卷暴露给工作节点中的其他容器。服务是一起工作的一组容器,诸如多层应用程序的一个层。

[0005] 然而,在包含多个工作节点的集群中,访问在集群上运行的应用程序之间的敏感数据目前是不可能的。尤其当敏感应用程序数据由工作节点上的安全区域密封时更是这样。安全区域是存储器的隔离和可信区域,其中,保护应用程序功能的关键方面,这帮助保持敏感应用程序数据机密且未修改。换言之,安全区域是主存储器的经加密的部分。通过基于处理器的安全机制来硬化安全区域。虽然向从给定机器的硬件(例如,工作节点的处理器芯片)将安全性标记到密封加密密钥是高度安全的,但是这目前使得在动态、分布式开源容器协调框架(诸如Kubernetes)中共享敏感的应用程序数据,这更加具有挑战性(如果不是不可能的话)。

## 发明内容

[0006] 根据一个说明性实施例,提供了一种用于在管理的容器环境中访问共享的敏感信息的方法。多个工作节点中的每个工作节点使用数据加密密钥来访问位于多个工作节点内的安全区域中的共享的敏感应用程序数据。所述多个工作节点中的每个工作节点使用密封密钥来保护每个相应的工作节点的数据加密密钥,所述密封密钥对于相应的工作节点上的安全区域是唯一的。进一步,所述方法在群集中建立第一工作节点。所述第一工作节点生成

所述数据加密密钥和所述第一工作节点上的对所述安全区域唯一的用于保护所述数据加密密钥的第一密封密钥。响应于集群中的第二工作节点的创建，第一工作节点与集群中的第二工作节点执行远程证明。当成功执行远程证明时，第一工作节点将数据加密密钥的副本提供至第二工作节点。此外，第二工作节点通过使用第二密封密钥加密数据加密密钥来生成第二工作节点上的安全区域唯一的用于保护数据加密密钥的第二密封密钥。根据其他说明性实施例，提供了一种用于访问管理容器环境中的共享敏感信息的系统和计算机程序产品。

[0007] 根据又一说明性实施例，提供一种用于密码密钥协调的计算机实现方法。一组处理器在开源容器协调框架的集群中生成具有密钥协调代理的工作节点。该组处理器使用工作节点的密钥协调代理生成数据加密密钥。该组处理器使用所述密钥协调代理从所述工作节点的安全区域检索所述第一密钥协调代理的密封密钥。该组处理器使用所述第一密钥协调代理的所述密封密钥密封所述数据加密密钥。进一步，该组处理器确定是否已在工作节点中创建容器。响应于该组处理器确定在所述工作节点中已创建容器，该组处理器使用所述第一密钥协调代理执行与所述容器的本地证明以建立所述容器的真实性。然后，该组处理器基于该本地证明来确定该容器是否是可信的。响应于该组处理器基于所述本地证明确定所述容器是不可信的，该组处理器拒绝所述容器对所述数据加密密钥的访问。响应于该组处理器基于所述本地证明确定所述容器是可信的，该组处理器使用所述密钥协调代理与所述容器共享所述数据加密密钥，使用与所述容器共享的所述数据加密密钥来加密对应于所述容器的工作负荷的数据，并且将所述工作节点的标识符和用所述容器的唯一密封密钥密封的所述数据加密密钥存储在共享数据库中。根据又一说明性实施例，提供一种用于密码密钥协调的计算机程序产品。

[0008] 因此，说明性实施例能够在集群内的可信容器之间提供加密密钥协调。此外，说明性实施例通过使用利用唯一密封密钥密封的数据加密密钥，使在集群内的不同工作节点上运行分布式应用程序的不同容器能够在不同容器之间共享敏感应用程序数据。

[0009] 根据一个方面，提供了一种用于在管理的容器环境中访问共享的敏感信息的方法，所述方法包括：由多个工作节点中的每个工作节点使用数据加密密钥来访问位于所述多个工作节点内的安全区域中的共享的敏感应用程序数据；以及由所述多个工作节点中的每个工作节点使用密封密钥来保护每个相应的工作节点的所述数据加密密钥，所述密封密钥对于相应的工作节点上的所述安全区域是唯一的。

[0010] 根据另一方面，提供了一种用于访问管理容器环境中的共享敏感信息的系统，所述系统包括：多个工作节点，其中：所述多个工作节点中的每个工作节点使用数据加密密钥来访问位于所述多个工作节点内的安全区域中的共享敏感应用程序数据；以及所述多个工作节点中的每个工作节点使用密封密钥来保护每个相应的工作节点的所述数据加密密钥，所述密封密钥对于相应的工作节点上的所述安全区域是唯一的。

[0011] 根据另一方面，提供了一种用于在管理的容器环境中访问共享的敏感信息的计算机程序产品，所述计算机程序产品包括计算机可读存储介质，所述计算机可读存储介质具有随其体现的程序指令，所述程序指令可由一组处理器执行以使该组处理器执行一种方法，所述方法包括：由多个工作节点中的每个工作节点使用数据加密密钥来访问位于所述多个工作节点内的安全区域中的共享的敏感应用程序数据；以及由所述多个工作节点中的

每个工作节点使用密封密钥来保护每个相应的工作节点的所述数据加密密钥，所述密封密钥对于相应的工作节点上的所述安全区域是唯一的。

[0012] 根据另一个方面，提供了一种用于密码密钥协调的计算机实现方法，所述计算机实现方法包括：在开源容器协调框架的集群中生成具有第一密钥协调代理的第一工作节点；使用所述第一工作节点的所述第一密钥协调代理生成数据加密密钥；使用所述第一密钥协调代理从所述第一工作节点的安全区域检索所述第一密钥协调代理的密封密钥；以及使用所述第一密钥协调代理的密封密钥密封所述数据加密密钥。

[0013] 根据另一方面，提供一种用于密码密钥协调的计算机程序产品，所述计算机程序产品包括计算机可读存储介质，所述计算机可读存储介质具有随其体现的程序指令，所述程序指令可由一组处理器执行以致使该组处理器执行一种方法，所述方法包括：在开源容器协调框架的集群中生成具有第一密钥协调代理的第一工作节点；使用所述第一工作节点的所述第一密钥协调代理生成数据加密密钥；使用所述第一密钥协调代理从所述第一工作节点的安全区域检索所述第一密钥协调代理的密封密钥；以及使用所述第一密钥协调代理的密封密钥密封所述数据加密密钥。

[0014] 根据另一个方面，提供了一种用于密码密钥协调的系统，所述系统可操作为：在开源容器协调框架的集群中生成具有第一密钥协调代理的第一工作节点；使用所述第一工作节点的所述第一密钥协调代理生成数据加密密钥；使用所述第一密钥协调代理从所述第一工作节点的安全区域检索所述第一密钥协调代理的密封密钥；以及使用所述第一密钥协调代理的密封密钥密封所述数据加密密钥。

## 附图说明

[0015] 现在将参考附图仅通过举例来描述本发明的实施例，在附图中：

[0016] 图1是可以实现说明性实施例的数据处理系统的网络的图示；

[0017] 图2是可以实现说明性实施例的数据处理系统的图；

[0018] 图3是示出根据说明性实施例的密码密钥协调系统的实例的图；

[0019] 图4是示出根据说明性实施例的用于在工作者节点与在工作者节点上创建的容器之间进行密码密钥协调的过程的流程图；

[0020] 图5A-5B是示出根据说明性实施例的用于群集内的现有工作节点与新生成的工作节点之间的密码密钥协调的过程的流程图；

[0021] 图6是示出根据说明性实施例的用于保护工作节点的数据加密密钥的过程的流程图；以及

[0022] 图7是示出根据说明性实施例的用于在集群中的工作节点之间共享数据加密密钥的过程的流程图。

## 具体实施方式

[0023] 本发明可以是任何可能的集成技术细节水平的系统、方法和/或计算机程序产品。所述计算机程序产品可包含上面具有计算机可读程序指令的计算机可读存储介质(或多个介质)，所述计算机可读程序指令用于致使处理器执行本发明的各方面。

[0024] 计算机可读存储介质可以是可以保留和存储指令以供指令执行设备使用的有形

设备。计算机可读存储介质可以是例如但不限于电子存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备或前述各项的任何合适的组合。计算机可读存储介质的更具体示例的非穷举列表包括以下：便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或闪存)、静态随机存取存储器(SRAM)、便携式紧凑盘只读存储器(CD-ROM)、数字通用盘(DVD)、记忆棒、软盘、诸如穿孔卡或具有记录在其上的指令的凹槽中的凸起结构的机械编码设备、以及前述的任意合适组合。如本文中所使用的计算机可读存储介质不应被解释为瞬态信号本身，诸如无线电波或其他自由传播的电磁波、通过波导或其他传输介质传播的电磁波(例如，通过光纤电缆的光脉冲)、或通过导线传输的电信号。

[0025] 本文所描述的计算机可读程序指令可以从计算机可读存储介质下载到相应的计算/处理设备或经由网络(例如，互联网、局域网、广域网和/或无线网络)下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光传输光纤、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配器卡或网络接口从网络接收计算机可读程序指令，并转发计算机可读程序指令以存储在相应计算/处理设备内的计算机可读存储介质中。

[0026] 用于执行本发明的操作的计算机可读程序指令可以是汇编器指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、集成电路的配置数据、或以一种或多种编程语言(包括面向对象的编程语言(如Salltalk、C++等)和过程式编程语言(如“C”编程语言或类似的编程语言))的任何组合编写的源代码或目标代码。计算机可读程序指令可完全在用户的计算机上执行、部分在用户的计算机上执行、作为独立软件包执行、部分在用户的计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在后一种情形中，远程计算机可以通过任何类型的网络(包括局域网(LAN)或广域网(WAN))连接到用户的计算机，或者可以连接到外部计算机(例如，通过使用互联网服务提供商的互联网)。在一些实施例中，电子电路(包括例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA))可以通过利用计算机可读程序指令的状态信息来执行计算机可读程序指令以使电子电路个性化，以便执行本发明的各方面。

[0027] 本文参照根据本发明的实施例的方法、装置(系统)和计算机程序产品的流程图展示和/或框图描述本发明的各方面。应当理解，流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合，都可以由计算机可读程序指令来实现。

[0028] 这些计算机可读程序指令可以被提供给计算机或其他可编程数据处理装置的处理器以产生机器，使得经由计算机或其他可编程数据处理装置的处理器执行的指令创建用于实现在流程图和/或框图的一个或多个框中指定的功能/动作的装置。这些计算机可读程序指令还可以存储在计算机可读存储介质中，所述计算机可读存储介质可以指引计算机、可编程数据处理装置和/或其他设备以特定方式工作，使得具有存储在其中的指令的计算机可读存储介质包括制品，所述制品包括实现流程图和/或框图中的一个或多个方框中规定的功能/动作的各方面的指令。

[0029] 计算机可读程序指令还可以加载到计算机、其他可编程数据处理装置、或其他设备上，以使一系列操作步骤在计算机、其他可编程装置或其他设备上执行以产生计算机实现的过程，从而使得在计算机、其他可编程装置、或其他设备上执行的指令实现流程图和/

或框图的一个或多个框中所指定的功能/动作。

[0030] 附图中的流程图和框图示出了根据本发明的不同实施例的系统、方法和计算机程序产品的可能实现方式的架构、功能和操作。对此，流程图或框图中的每个方框可以代表模块、段或指令的一部分，其包括用于实现规定的逻辑功能的一个或多个可执行指令。在一些替代实施例中，框中所标注的功能可以不以图中所标注的次序发生。例如，取决于所涉及的功能，连续示出的两个框实际上可以作为一个步骤完成、同时执行、基本同时地、以部分或全部时间上重叠的方式执行，或者这些框有时可以以相反的顺序执行。还将注意的是，框图和/或流程图中的每个框、以及框图和/或流程图中的框的组合可以由基于专用硬件的系统来实现，所述基于专用硬件的系统执行指定的功能或动作或执行专用硬件与计算机指令的组合。

[0031] 现在参考附图，并且具体地参见图1-3，提供了可以实现说明性实施例的数据处理环境的图。应了解，图1-3仅意在作为示例，且无意断言或暗示关于其中可实施不同实施例的环境的任何限制。可以对所描绘的环境进行许多修改。

[0032] 图1描绘了可以实现说明性实施例的数据处理系统的网络的图形表示。网络数据处理系统100是可以在其中实现说明性实施例的计算机、数据处理系统和其他设备的网络。网络数据处理系统100包含网络102，网络102是用于提供在网络数据处理系统100内连接在一起的计算机、数据处理系统和其他设备之间的通信链路的介质。网络102可包括连接，诸如例如有线通信链路、无线通信链路和光纤电缆。

[0033] 在所描绘的实例中，服务器104和服务器106与存储装置108一起连接到网络102。服务器104和服务器106可以是例如开源容器协调框架112的集群110内的工作节点。开放源容器协调框架112可以是例如Kubernetes管理的容器环境。服务器104和服务器106可以表示物理服务器或虚拟服务器。此外，服务器104和服务器106可以具有与网络102的高速连接，并且使用一个或多个分布式多层应用程序向客户端设备提供一组服务，例如，事件监测服务、金融服务、银行服务、政府服务、教育服务、预订服务、数据服务等。同样，应当注意，服务器104和服务器106可各自表示一个或多个云环境中的计算节点群集。或者，服务器104和服务器106可各自表示一个或多个数据中心中的服务器群集。

[0034] 客户端114、客户端116和客户端118也连接到网络102。客户端114、116和118是服务器104和服务器106的客户端。在该示例中，客户端114、116和118被示为具有到网络102的有线通信链路的台式或个人计算机。然而，应当注意，客户端114、116和118仅是示例，并且可以表示其他类型的数据处理系统，诸如例如网络计算机、膝上型计算机、手持计算机、智能电话、智能手表、智能电视、智能电器、游戏设备、自助服务机等。客户端114、116和118的用户可以利用客户端114、116和118来访问和利用由服务器104和服务器106提供的服务。

[0035] 存储器108是能够以结构化格式或非结构化格式存储任何类型的数据的网络存储设备。此外，存储器108可以表示多个网络存储设备。进一步，存储装置108可以存储多个服务器的标识符和网络地址、加密密钥、加密数据等。此外，存储装置108可以存储其他类型的数据，诸如可以包括例如与系统管理员和用户相关联的用户名、密码和生物特征数据的认证或证书数据。

[0036] 此外，应当注意，网络数据处理系统100可以包括任何数量的附加服务器、客户端、存储设备和未示出的其他设备。位于网络数据处理系统100中的程序代码可以被存储在计

算机可读存储介质上并且被下载到计算机或其他数据处理设备以供使用。例如，程序代码可以存储在服务器104上的计算机可读存储介质上，并且通过网络102下载到客户端114以便在客户端114上使用。

[0037] 在所描绘的实例中，网络数据处理系统100可以被实施为许多不同类型的通信网络，例如像互联网、内联网、局域网(LAN)、广域网(WAN)、电信网络或其任何组合。图1仅旨在作为实例，而不旨在作为不同说明性实施例的体系结构限制。

[0038] 现在参见图2，描绘了根据说明性实施例的数据处理系统的图。数据处理系统200是诸如图1中的服务器104和服务器106的计算机的示例，实现说明性实施例的处理的计算机可读程序代码或指令可以位于该计算机中。数据处理系统200可以是，例如，开源容器协调框架(诸如Kubernetes)的工作节点的集群内的工作节点。数据处理系统200包含并控制可供数据处理系统200使用的一组资源。在这个说明性示例中，数据处理系统200包括通信结构202，其提供处理器单元204、存储器206、持久存储装置208、通信单元210、输入/输出(I/O)单元212和显示器214之间的通信。然而，应当注意，数据处理系统200仅旨在作为示例并且可以包含比所示出的更多或更少的组件。

[0039] 处理器单元204用于执行可加载到存储器206中的软件应用程序和程序的指令。处理器单元204可为一组一个或一个以上硬件处理器装置，或可为多核处理器，这取决于特定实施例。

[0040] 存储器206和永久性存储器208是存储设备的示例。计算机可读存储设备是能够存储信息的任何硬件，所述信息诸如例如但不限于，数据、功能形式的计算机可读程序代码、和/或在瞬态基础上和/或在持久基础上的其他合适的信息。进一步，计算机可读存储设备不包括传播介质。在这些示例中，存储器206可以是例如随机存取存储器(RAM)或任何其他合适的易失性或非易失性存储设备。永久性存储器208可以采取不同形式，这取决于特定的实现方式。例如，永久存储器208可以包含一个或多个设备。例如，永久性存储器208可以是硬盘驱动器、固态驱动器、闪存、可重写光盘、可重写磁带或上述的某种组合。永久存储器208使用的介质可以是可移除的。例如，可移动硬盘驱动器可以用于持久存储装置208。

[0041] 密钥协调代理218控制为数据处理系统200生成密码密钥(如数据加密密钥220、密封密钥222和密封密钥226)的过程。数据加密密钥220是用于加密和解密应用程序228的敏感应用程序数据232的密码密钥。密封密钥222对于密钥协调代理218是唯一的，并且密封密钥226对于容器224是唯一的。每个密封密钥可以基于例如数据处理系统200的硬件，诸如处理器单元204。密封密钥222和226是密钥加密密钥。换言之，密钥协调代理218使用密封密钥222来密封或加密数据加密密钥220，以便安全和保护数据加密密钥220。

[0042] 密钥协调代理218还控制协调数据加密密钥220与数据处理系统200内创建的容器224的分配的过程。容器224表示运行对应于应用程序228的一个或多个工作负荷的集合的一个或多个容器(诸如pod)的集合。密钥协调代理218在与容器224共享数据加密密钥220之前执行本地证明过程以确保容器224是经认证的可信容器。在接收数据加密密钥220之后，容器224用对容器224唯一的密封密钥226密封或加密数据加密密钥220。容器224利用数据加密密钥220来加密和解密对应于应用程序228的敏感应用程序数据232。

[0043] 密钥协调代理218进一步控制协调数据加密密钥220与一组一个或多个其他数据处理系统(即，集群内的一组其他工作节点)的分布的过程。密钥协调代理218执行远程证明

过程以确保在与集群中的相应工作节点共享数据加密密钥220之前，一组其他工作节点中的每个工作节点是经认证的可信工作节点。

[0044] 应用程序228可以表示在数据处理系统200上的容器(如容器224)的集合上运行的分布式多层应用程序。应用程序228可表示任何类型的软件应用程序，例如银行应用程序、金融应用程序、医疗应用程序、保险应用程序、商业应用程序、娱乐应用程序、游戏应用程序、流式数据应用程序等，其执行用于请求客户端装置的服务。

[0045] 安全区域230是存储器206的加密区段，其中，保护应用程序228的功能的各方面，保持敏感应用程序数据232是机密的和未修改的。敏感应用程序数据232表示对应于应用程序228的任何类型的私人信息，诸如个人用户信息、医疗记录、银行余额、信用卡号、社会保障号、财务记录等。安全区域230还存储密封密钥234。密封密钥234表示密封密钥222和密封密钥226。密钥协调代理218和容器224在需要时分别从安全区域230检索密封密钥222和密封密钥226以密封数据加密密钥220。

[0046] 因此，数据处理系统200作为专用计算机系统操作，其中数据处理系统200中的密钥协调代理218使得能够与数据处理系统200内的可信容器以及与集群(诸如图1中的集群110)中的其他可信工作节点进行密钥协调。特别地，与不具有密钥协调代理218的当前可用的通用计算机系统相比，密钥协调代理218将数据处理系统200转换成专用计算机系统。

[0047] 本文实例中，通信单元210经由网络(例如，图1中的网络102)提供与其他计算机、数据处理系统和装置的通信。通信单元210可通过使用物理和无线通信链路两者来提供通信。物理通信链路可以利用例如导线、电缆、通用串行总线、或任何其他物理技术来为数据处理系统200建立物理通信链路。无线通信链路可利用例如短波、高频、超高频、微波、无线保真(Wi-Fi)、Bluetooth®技术、全球移动通信系统(GSM)、码分多址(CDMA)、第二代(2G)、第三代(3G)、第四代(4G)、4G长期演进(LTE)、高级LTE、第五代(5G)或任何其他无线通信技术或标准来建立数据处理系统200的无线通信链路。

[0048] 输入/输出单元212允许与可以连接至数据处理系统200的其他设备进行数据的输入和输出。例如，输入/输出单元212可以通过小键盘、键盘、鼠标、麦克风和/或一些其他合适的输入设备为用户输入提供连接。显示器214提供向用户显示信息的机制，并且可以包括触摸屏能力以允许用户通过例如用户界面或输入数据做出屏幕上选择。

[0049] 用于操作系统、应用程序和/或程序的指令可以位于存储器206和持久存储装置208中，存储器206和持久存储装置208通过通信结构202与处理器单元204通信。在这个说明性示例中，指令在永久存储器208上呈功能形式。这些指令可以被加载到存储器206中以便由处理器单元204运行。不同实施例的过程可由处理器单元204使用计算机实现的指令来执行，这些指令可位于存储器(诸如存储器206)中。这些程序指令被称为可由处理器单元204中的处理器读取和运行的程序代码、计算机可用程序代码或计算机可读程序代码。在不同的实施例中，程序指令可以体现在不同的物理计算机可读存储设备上，诸如存储器206或持久存储装置208。

[0050] 程序代码236以功能形式位于计算机可读介质238上，所述计算机可读介质238可选择性地移除并且可以加载到或转移到数据处理系统200上以由处理器单元204运行。程序代码236和计算机可读介质238形成计算机程序产品240。在一个示例中，计算机可读介质238可以是计算机可读存储介质242或计算机可读信号介质244。计算机可读存储介质242可

以包括例如光盘或磁盘，该光盘或磁盘被插入或放置到作为永久性存储器208的一部分的驱动器或其他设备中，以便转移到作为永久性存储器208的一部分的存储设备(诸如硬盘驱动器)上。计算机可读存储介质242还可以采取永久性存储器的形式，诸如连接到数据处理系统200的硬盘驱动器、拇指驱动器或闪存。在一些实例中，计算机可读存储介质242可以不是从数据处理系统200可移除的。

[0051] 或者，可使用计算机可读信号介质244将程序代码236传送到数据处理系统200。计算机可读信号介质244可以是例如包含程序代码236的传播数据信号。例如，计算机可读信号介质244可以是电磁信号、光信号和/或任何其他合适类型的信号。这些信号可通过通信链路传输，例如无线通信链路、光纤电缆、同轴电缆、电线和/或任何其他合适类型的通信链路。换言之，在说明性实例中，通信链路和/或连接可以是物理的或无线的。计算机可读介质还可以采取非有形介质的形式，诸如包含程序代码的通信链路或无线传输。

[0052] 在一些说明性实施例中，程序代码236可以通过计算机可读信号介质244从另一设备或数据处理系统通过网络下载到永久存储器208，以便在数据处理系统200内使用。例如，存储在数据处理系统中的计算机可读存储介质中的程序代码可以通过网络从数据处理系统下载到数据处理系统200。提供程序代码236的数据处理系统可以是服务器计算机、客户端计算机或能够存储和传输程序代码236的一些其他设备。

[0053] 数据处理系统200所示的不同组件并不意味着对可实施不同实施例的方式提供架构限制。可以在数据处理系统中实现不同的说明性实施例，该数据处理系统包括除了数据处理系统200所示出的那些组件之外的组件，或者代替数据处理系统200所示出的那些组件的组件。图2中所示的其他部件可以不同于所示的说明性实例。不同的实施例可以使用能够执行程序代码的任何硬件设备或系统来实现。作为一个实例，数据处理系统200可以包括与无机部件集成的有机部件和/或可以完全由排除人类的有机部件组成。例如，存储装置可包括有机半导体。

[0054] 作为另一示例，数据处理系统200中的计算机可读存储设备是可存储数据的任何硬件装置。存储器206、持久存储装置208和计算机可读存储介质242是有形形式的物理存储装置的示例。

[0055] 在另一个示例中，总线系统可以用于实现通信结构202并且可以由一个或多个总线(如系统总线或输入/输出总线)组成。当然，总线系统可以使用任何合适类型的架构来实现，所述架构在附接到总线系统的不同组件或设备之间提供数据传输。另外，通信单元可包括用于发送和接收数据的一个或多个设备，诸如调制解调器或网络适配器。进一步，存储器可以是例如存储器206或例如在可存在于通信结构202中的接口和存储器控制器集线器中找到的高速缓存。

[0056] 说明性实施例解决了在动态、分布式开源容器协调框架中使用可信容器与开源容器协调框架的基础设施中的工作节点之间的密码密钥协调过程来共享敏感应用程序数据的挑战。当具有在开源容器协调框架中具有“n”个工作节点的集群时，说明性实施例通过使用数据加密密钥对敏感应用程序数据进行加密和解密，使得集群中的每个工作节点能够访问安全区域内部的敏感应用程序数据。说明性实施例在受信任的(即，证明的)工作者节点之间共享数据加密密钥。每个工作节点通过用密封密钥加密数据加密密钥来保护其数据加密密钥，所述密封密钥对于给定工作节点上的安全区域是唯一的。通过利用该机制，说明性

实施例为硬件(即,工作节点的处理器)标记安全性,同时还提供可信工作节点之间的密钥协调机制。

[0057] 当在集群中创建工作节点时,工作节点生成用于对在工作节点的安全区域中运行的敏感应用程序数据进行加密的数据加密密钥。当工作节点是集群中仅有的工作节点时,密钥协调软件代理(例如,位于工作节点中的一组守护进程中的“密钥协调守护进程”)生成数据加密密钥。守护进程组确保特定容器的实例在集群中的所有工作节点或者选择的工作节点上运行。守护进程组在每个添加的工作节点上创建容器,并且当工作节点从集群移除时,创建垃圾收集容器。守护进程组可以包括其他守护进程,例如,集群存储守护进程、日志收集器守护进程、监视守护进程等。

[0058] 工作节点使用数据加密密钥来保护在安全区域中运行的敏感应用程序数据。此外,工作节点使用从工作节点的处理器导出的其密封密钥密封数据加密密钥,使得密封密钥对于工作节点是唯一的。应注意,安全区域可仅在同一工作节点上检索密封密钥。换言之,不同工作节点上的相同安全区域将具有不同的密封密钥。

[0059] 当在集群中创建新的工作节点时,新的工作节点的软件代理(例如,密钥协调守护进程)执行与集群中的现有工作节点的远程证明。证明是演示软件可执行文件已经在平台上被适当地实例化的过程。证明允许远程方获得预期软件正在Intel®SGX使能的平台上的安全区域内安全运行的置信度。证明在断言中传达以下信息:1)被证明的软件的身份;2)未测量状态(例如,模式软件正在运行)的细节;以及3)软件与其自身相关联的数据。在成功证明时,新工作节点从集群中的现有工作节点接收数据加密密钥的副本。在接收数据加密密钥之后,新的工作节点利用其自身的唯一密封密钥密封数据加密密钥。说明性实施例还可以利用包含数据加密密钥和加密数据的共享数据库或数据存储。仅可信的(即,证明的)工作节点可访问共享数据库。

[0060] 因此,说明性实施例通过使用利用密封密钥加密的数据加密密钥使在集群内的不同工作节点上运行分布式应用程序的不同容器能够在不同容器之间共享敏感应用程序数据。每个容器和每个密钥协调代理具有其自己的唯一密封密钥。每个密钥协调代理执行证明过程。因此,说明性实施例确保即使当容器在工作者节点的群集内移动(例如,创建、删除等)时,敏感应用程序数据仅在可信(即,验证)容器之间共享。此外,说明性实施例可以保护任何形式的存储中的敏感应用程序数据,例如,在硬盘上、在文件存储中等。

[0061] 因此,说明性实施例提供了克服在开源容器协调框架内的容器之间共享敏感应用程序数据的技术问题的一个或多个技术方案。从而这些一个或多个技术方案在数据安全领域具有技术效果和实际应用。

[0062] 现在参见图3,描绘了根据说明性实施例示出密钥协调系统的示例的示图。密码密钥协调系统300可以在诸如图1中的网络数据处理系统100的数据处理系统的网络中实现。密码密钥协调系统300是用于在开源容器协调框架的多节点集群内的可信容器和节点之间提供密码密钥协调的硬件和软件组件的系统。

[0063] 在该实例中,密码密钥协调系统300包括开源容器协调框架302、集群304和数据库306。开源容器协调框架302、集群304和数据库306可以是例如图1中的开源容器协调框架112、集群110和存储器108。然而,应注意,在替代说明性实施例中,数据库306可位于开源容器协调框架302的远程外部。在另一个替代的说明性实施例中,数据库306是可选的。

[0064] 在这个实例中，群集304包括工作节点A 308和工作节点B 310，例如，图1中的服务器104和服务器106。然而，应注意，群集304可包含任何数量的工作节点。工作节点A308和工作节点B310经由网络312(诸如图1中的网络102)彼此通信。

[0065] 工作节点A308包括代理A 314和容器1 316。类似地，工作节点B 310包括代理B 318和容器2 320。代理A 314和代理B 318类似于图2中的密钥协调代理218。同样，容器1 316和容器2 320类似于图2中的容器224。

[0066] 代理A 314包含密封密钥A(SK-A)322和数据加密密钥(DEK)324。密封密钥A 322和数据加密密钥324可以是例如图2中的密封密钥222和数据加密密钥220。密封密钥A 322对于代理A 314是唯一的。代理A 314使用密封密钥A 322密封数据加密密钥324。

[0067] 容器1316包含数据加密密钥(DEK)326和密封密钥1(SK-1)328。密封密钥1 328对于容器1316是唯一的。容器1 316使用密封密钥1 328密封数据加密密钥326。应当注意，容器1 316中的数据加密密钥326与代理A 314中的数据加密密钥324相同。在基于本地证明330确定容器1 316是可信容器之后，代理A 314与容器1 316共享数据加密密钥324的副本。本地证明330提供在工作节点A 308上运行的安全区域之间的断言。换言之，工作节点A 308上的安全区域使用它们的报告向彼此提供认证。对于本地和远程证明两者，应用程序的受保护部分被加载到安全区域中，该安全区域测量应用程序的代码和数据并随后生成报告。在建立了真实性之后，安全区域经由安全信道交换信息。

[0068] 代理B 318包含密封密钥B(SK-B)332。应当注意，代理A 314中的数据加密密钥324与代理B 318中的数据加密密钥334相同。在基于远程证明342确定代理B 318是可信密钥协调代理之后，代理A314与代理B318共享数据加密密钥324的副本。远程证明342提供从代理A 314到代理B 318的断言。在远程证明中，代理A 314上的安全区域向代理B 318发送引用。代理B 318然后执行关于可信处理器是否生成引用的验证。在验证时，代理B 318信任代理A314上的安全区域的真实性。在接收到数据加密密钥334之后，代理B 318使用对代理B 318唯一的密封密钥B 332密封数据加密密钥334。

[0069] 容器2 320包含数据加密密钥(DEK)336和密封密钥2(SK-2)338。密封密钥2 338对于容器2 320是唯一的。容器2 320使用密封密钥2 338密封数据加密密钥336。应当注意，容器2 320中的数据加密密钥336与代理B 318中的数据加密密钥334相同。在基于本地证明340确定容器2 320是可信容器之后，代理B 318与容器2 320共享数据加密密钥334的副本。本地证明340是与本地证明330类似的本地证明过程。

[0070] 容器1 316和容器2 320利用它们各自的数据加密密钥来解密和加密对应于与容器1 316和容器2 320上运行的分布式应用程序相关联的工作负荷的敏感应用程序数据。开源容器协调框架302利用数据库306来存储例如加密的数据和加密密钥。数据库306是共享数据库。

[0071] 现在参见图4，示出了根据说明性实施例的用于在工作节点与在工作节点上创建的容器之间进行密码密钥协调的过程的流程图。图4中所示的过程可以在开源容器协调框架(例如，图1中的开源容器协调框架112或图3中的开源容器协调框架302)中实现。

[0072] 当开源容器协调框架中的一组一个或多个处理器在开源容器协调框架中生成具有密钥协调代理的工作节点(步骤402)时，该过程开始。所述一组一个或多个处理器可以位于开源容器协调框架的一个或多个节点中。此外，该组处理器使用工作节点的密钥协调代

理生成数据加密密钥(步骤404)。进一步,该组处理器使用密钥协调代理从工作节点的安全区域检索密钥协调代理的唯一密封密钥(步骤406)。使用密钥协调代理的唯一密封密钥,该组处理器密封数据加密密钥(步骤408)。

[0073] 该组处理器确定在工作节点中是否已经创建了容器(步骤410)。如果该组处理器确定在工作节点中尚未创建容器,那么步骤410输出否,则过程返回到步骤410,其中该组处理器等待在工作节点中创建容器。如果该组处理器确定在工作节点中创建了容器,则步骤410输出是,那么该组处理器使用密钥协调代理执行与容器的本地证明以建立容器的真实性(步骤412)。

[0074] 该组处理器基于本地证明来做出关于容器是否是可信的确定(步骤414)。如果该组处理器基于本地证明确定容器是不可信的,则步骤414输出否,该组处理器拒绝容器对数据加密密钥的访问(步骤416)。之后,处理结束。

[0075] 如果该组处理器基于本地证明确定该容器是可信的,步骤414输出是,则该组处理器使用密钥协调代理与该容器共享数据加密密钥(步骤418)。进一步,该组处理器使用与容器共享的数据加密密钥来加密对应于容器的工作负荷的数据(步骤420)。此外,该组处理器在共享数据库中存储工作节点的标识符以及使用容器的唯一密封密钥密封的数据加密密钥(步骤422)。之后,处理结束。

[0076] 现在参见图5A-5B,示出根据说明性实施例的用于群集内的现有工作节点与新产生的工作节点之间的密码密钥协调的过程的流程图。图5A-5B中所示的过程可以在开源容器协调框架(例如,图1中的开源容器协调框架112或图3中的开源容器协调框架302)中实现。

[0077] 当开源容器协调框架中的一组一个或多个处理器在所述该组处理器已在所述集群中生成具有第一密钥协调代理的第一工作节点之后在所述开源容器协调框架的节点集群内生成具有第二密钥协调代理的第二工作节点(步骤502)时,所述过程开始。该组处理器使用第二工作节点的第二密钥协调代理执行与第一工作节点的第一密钥协调代理的远程证明以建立第二密钥协调代理的真实性(步骤504)。

[0078] 该组处理器基于所述远程证明来做出关于所述第二密钥协调代理是否可信的判定(步骤506)。如果该组处理器基于所述远程证明确定所述第二密钥协调代理是不可信的,步骤506输出否,则该组处理器拒绝所述第二密钥协调代理对所述第一密钥协调代理的数据加密密钥的访问(步骤508)。之后,处理结束。

[0079] 如果该处理器基于远程证明确定第二密钥协调代理是可信的,步骤506输出是,那么该组处理器使用第一工作节点的第一密钥协调代理与第二密钥协调代理共享第一密钥协调代理的数据加密密钥(步骤510)。进一步,该组处理器使用第二密钥协调代理从第二工作节点的安全区域检索第二密钥协调代理的唯一密封密钥(步骤512)。此外,该组处理器使用第二密钥协调代理的唯一密封密钥密封数据加密密钥(步骤514)。

[0080] 该处理器确定在第二工作节点中是否已经创建了容器(步骤516)。如果该组处理器确定在第二工作节点中尚未创建容器,步骤516输出否,那么所述过程返回到步骤516,其中该组处理器等待在第二工作节点中创建容器。如果该组处理器确定在第二工作节点中已创建容器,步骤516输出是,那么该处理器使用第二密钥协调代理执行与第二工作节点的容器的本地证明以建立容器的真实性(步骤518)。

[0081] 该组处理器基于本地证明来做出关于第二工作节点的容器是否是可信的确定(步骤520)。如果该组处理器基于本地证明确定第二工作节点的容器是不可信的,步骤520输出否,那么该组处理器拒绝由第二工作节点的容器访问第二密钥协调代理的数据加密密钥(步骤522)。之后,处理结束。

[0082] 如果该组处理器基于本地证明确定第二工作节点的容器是可信的,步骤520输出是,那么该组处理器使用第二密钥协调代理与第二工作节点的容器共享数据加密密钥(步骤524)。此外,该组处理器使用与第二工作节点的容器共享的数据加密密钥,对对应于第一工作节点上的另一容器的工作负荷的数据解密,以便对数据执行一组一个或多个操作(步骤526)。该组操作可包括例如创建、读取、更新和删除操作中的一个或多个。随后,在执行所述一组操作之后,该组处理器使用与第二工作节点的容器共享的数据加密密钥加密数据(步骤528)。此外,该组处理器将第二工作节点的标识符以及使用第二工作节点上的容器的唯一密封密钥密封的数据加密密钥存储在共享数据库中(步骤530)。之后,处理结束。

[0083] 现在参见图6,示出根据说明性实施例的用于保护工作节点的数据加密密钥的过程的流程图。图6中示出的过程可以在开源容器协调框架(例如,图1中的开源容器协调框架112或图3中的开源容器协调框架302)中实现。

[0084] 当开源容器协调框架的多个工作节点中的每个工作节点使用数据加密密钥访问位于多个工作节点内的安全区域中的共享敏感应用程序数据(步骤602)时,过程开始。此外,多个工作节点中的每个工作节点使用对相应工作节点上的安全区域唯一的密封密钥来保护每个相应工作节点的数据加密密钥(步骤604)。之后,处理结束。

[0085] 现在参见图7,示出了根据说明性实施例的用于在集群中的工作节点之间共享数据加密密钥的过程的流程图。图7中所示的过程可以在开源容器协调框架(例如,图1中的开源容器协调框架112或图3中的开源容器协调框架302)中实现。

[0086] 当开源容器协调框架在开源容器协调框架的集群中建立第一工作节点(步骤702)时,该过程开始。第一工作节点生成数据加密密钥(步骤704)。此外,第一工作节点基于第一工作节点的硬件生成对于第一工作节点上的安全区域唯一的第一密封密钥,用于通过使用第一密封密钥加密数据加密密钥来保护数据加密密钥(步骤706)。

[0087] 随后,响应于集群中的第二工作节点的创建,第一工作节点与集群中的第二工作节点执行远程证明(步骤708)。当成功执行远程证明时,第一工作节点将数据加密密钥的副本提供至第二工作节点(步骤710)。第二工作节点基于第二工作节点的硬件生成对于第二工作节点上的安全区域唯一的第二密封密钥,用于通过使用第二密封密钥加密数据加密密钥来保护数据加密密钥(步骤712)。之后,处理结束。

[0088] 因此,本发明的示例性实施例提供了一种用于在开源容器协调框架的多节点集群内的可信节点与容器之间提供加密密钥协调的计算机实现的方法、计算机系统和计算机程序产品。已经出于说明的目的呈现了本发明的不同实施例的描述,但并不旨在是穷尽性的或局限于所公开的实施例。在不背离所描述的实施例的范围和精神的情况下,许多修改和变化对本领域的普通技术人员而言将是显而易见的。选择本文使用的术语以最佳地解释实施例的原理、实际应用程序或在市场上找到的技术上的技术改进,或使得本领域普通技术人员能够理解本文公开的实施例。

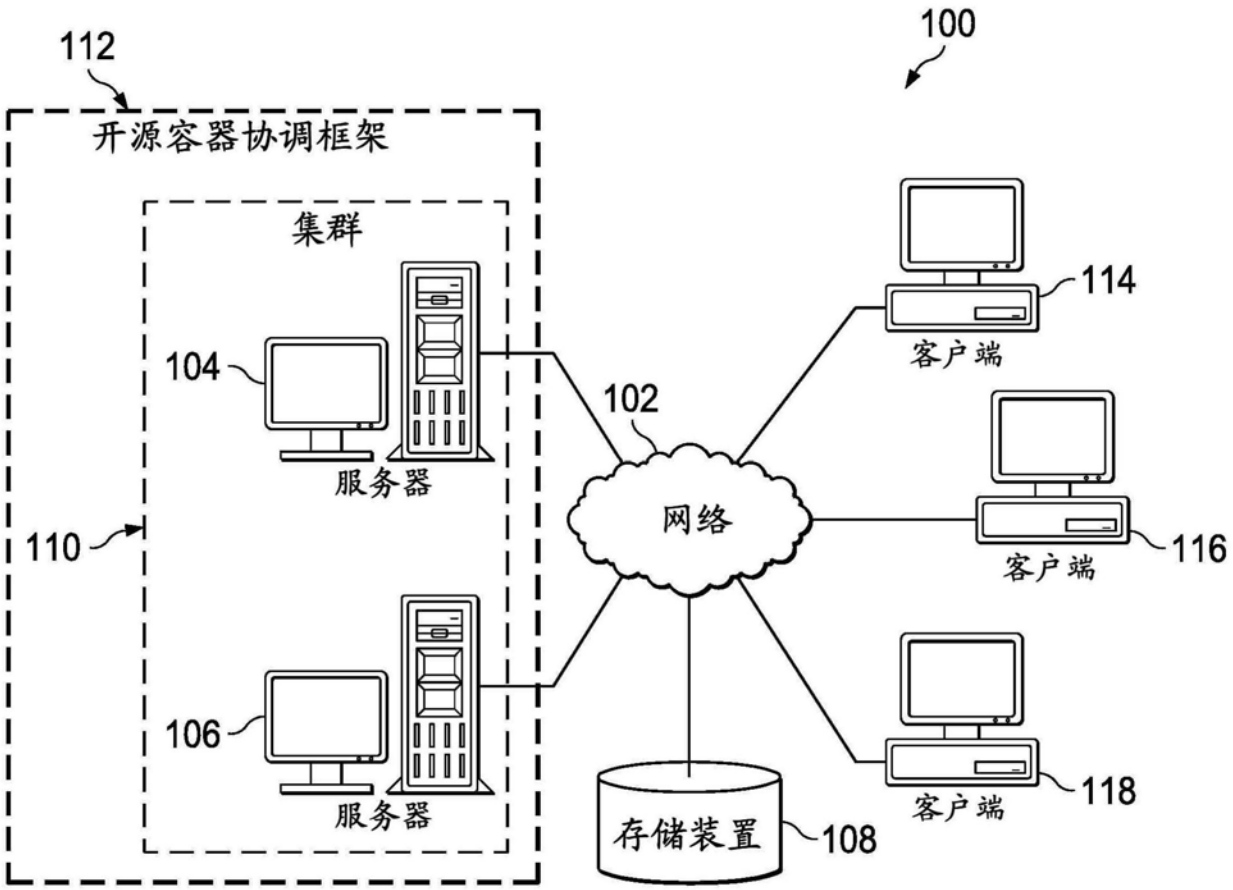

100
112
开源容器协调框架
集群
104
服务器
106
服务器
110
102
网络
114
客户端
116
客户端
118
客户端
存储装置
108

图1

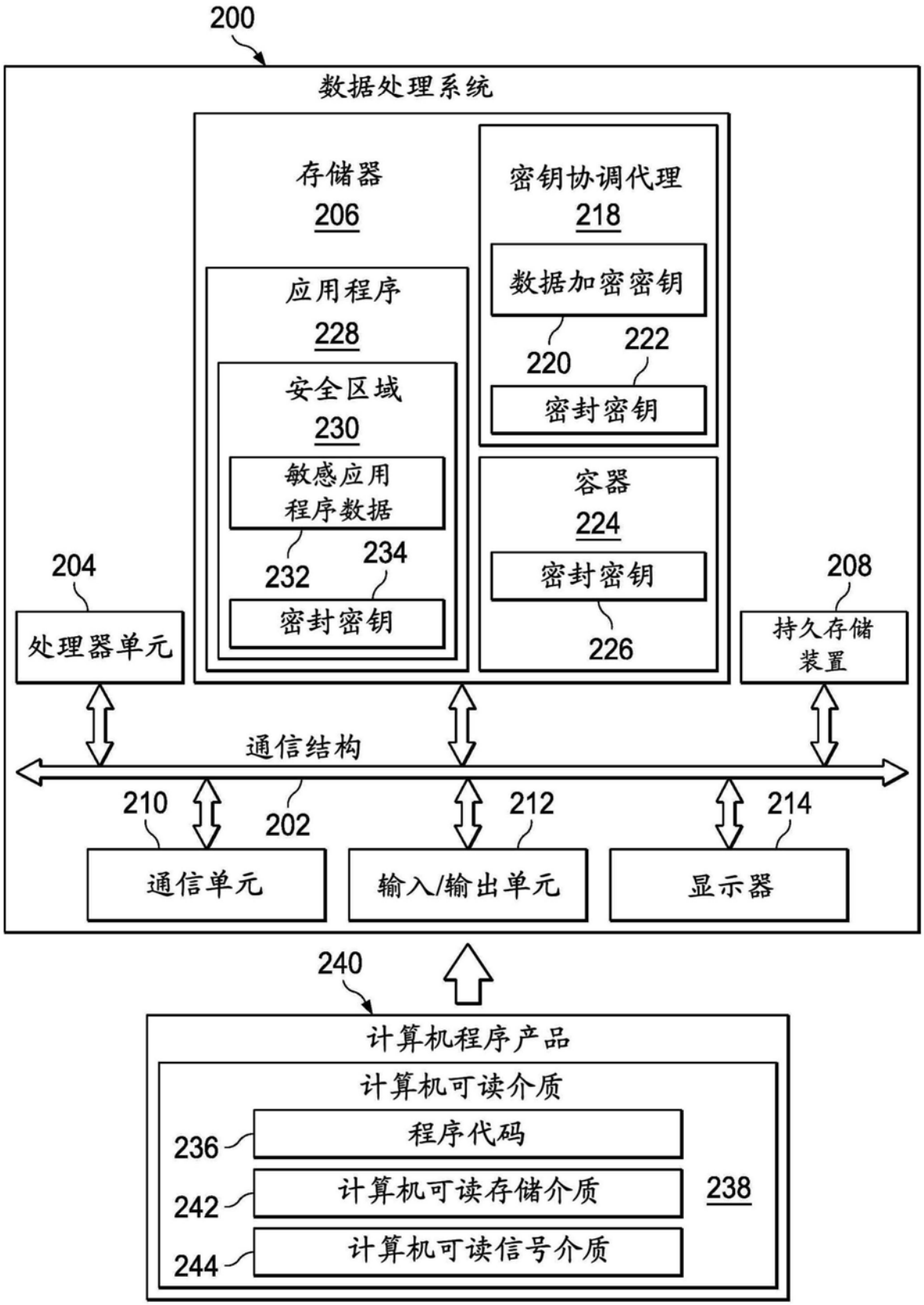

200
数据处理系统
存储器
206
应用程序
228
安全区域
230
敏感应用
程序数据
232
234
密封密钥
密钥协调代理
218
数据加密密钥
220
222
密封密钥
容器
224
密封密钥
226
204
处理器单元
208
持久存储
装置
通信结构
210
202
212
214
通信单元
输入/输出单元
显示器
240
计算机程序产品
计算机可读介质
236
程序代码
242
计算机可读存储介质
238
244
计算机可读信号介质

图2

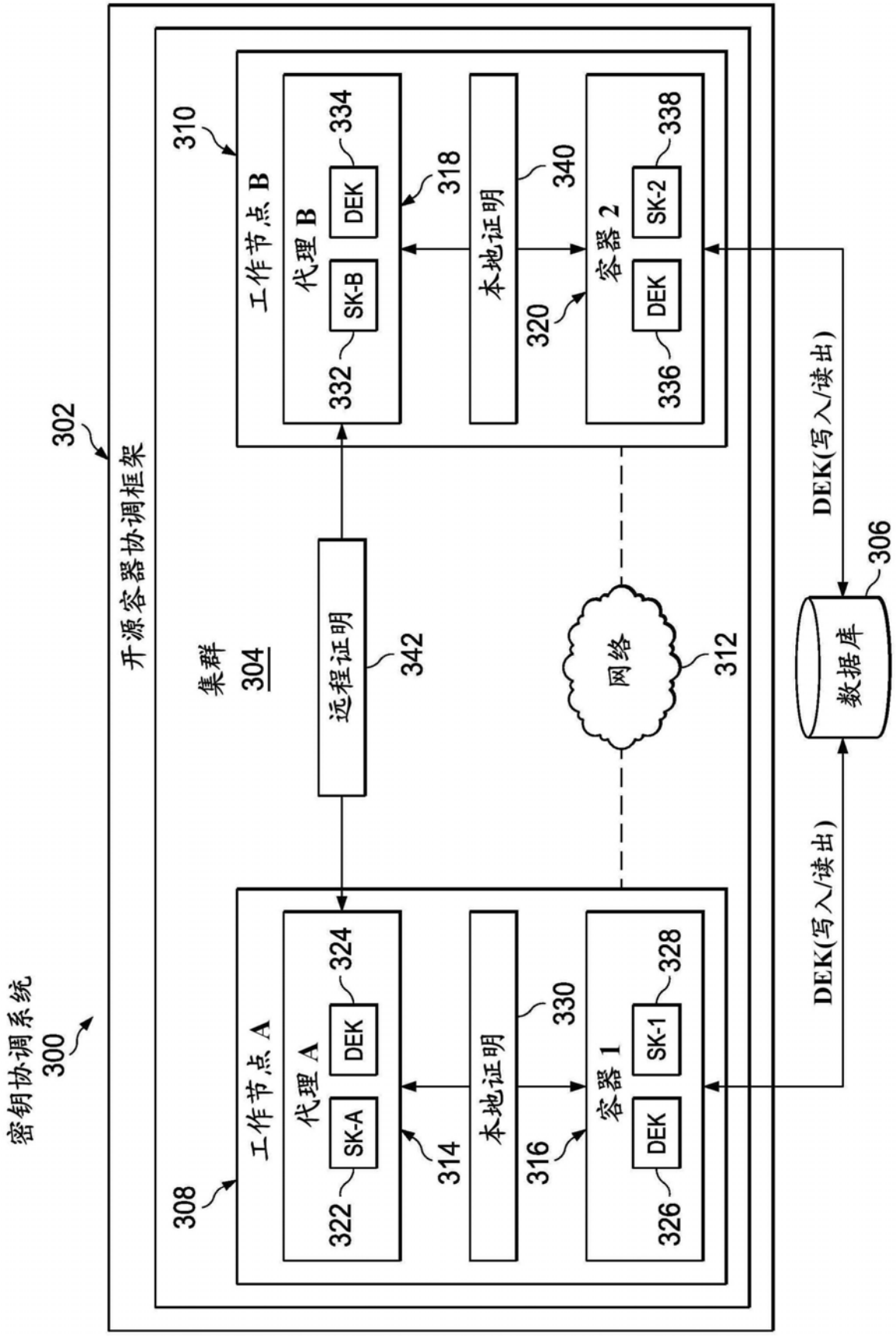

密钥协调系统
300
302
开源容器协调框架
集群
304
工作节点 A
308
代理 A
SK-A
322
DEK
324
314
本地证明
316
330
容器 1
DEK
326
SK-1
328
工作节点 B
310
代理 B
SK-B
332
DEK
334
318
本地证明
320
340
容器 2
DEK
336
SK-2
338
远程证明
342
网络
312
数据库
306
DEK(写入/读出)
DEK(写入/读出)

图3

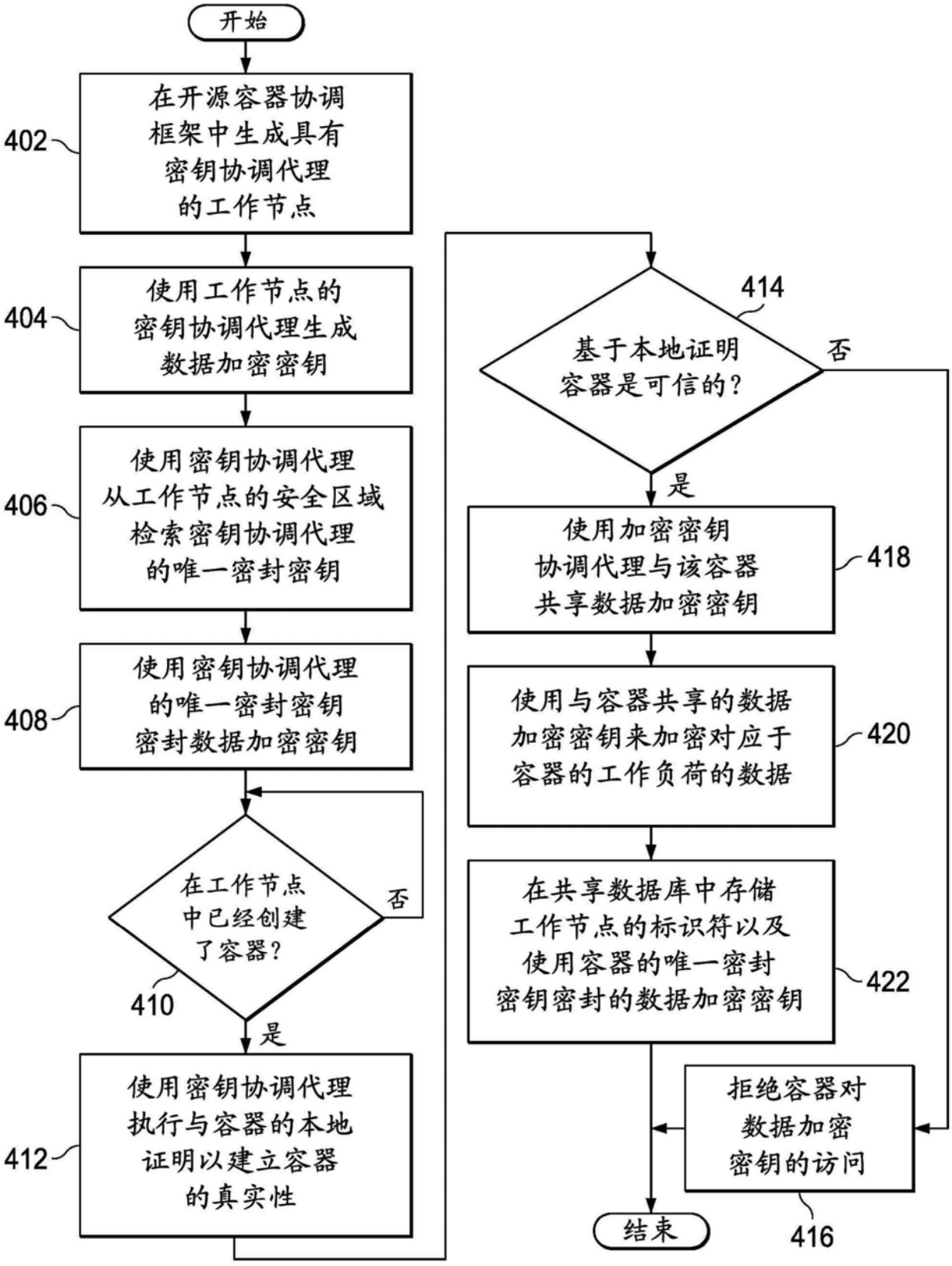

开始
在开源容器协调框架中生成具有密钥协调代理的工作节点
402
使用工作节点的密钥协调代理生成数据加密密钥
404
使用密钥协调代理从工作节点的安全区域检索密钥协调代理的唯一密封密钥
406
使用密钥协调代理的唯一密封密钥密封数据加密密钥
408
在工作节点中已经创建了容器?
否
410
是
使用密钥协调代理执行与容器的本地证明以建立容器的真实性
412
414
基于本地证明容器是可信的?
否
是
使用加密密钥协调代理与该容器共享数据加密密钥
418
使用与容器共享的数据加密密钥来加密对应于容器的工作负荷的数据
420
在共享数据库中存储工作节点的标识符以及使用容器的唯一密封密钥密封的数据加密密钥
422
拒绝容器对数据加密密钥的访问
416
结束

图4

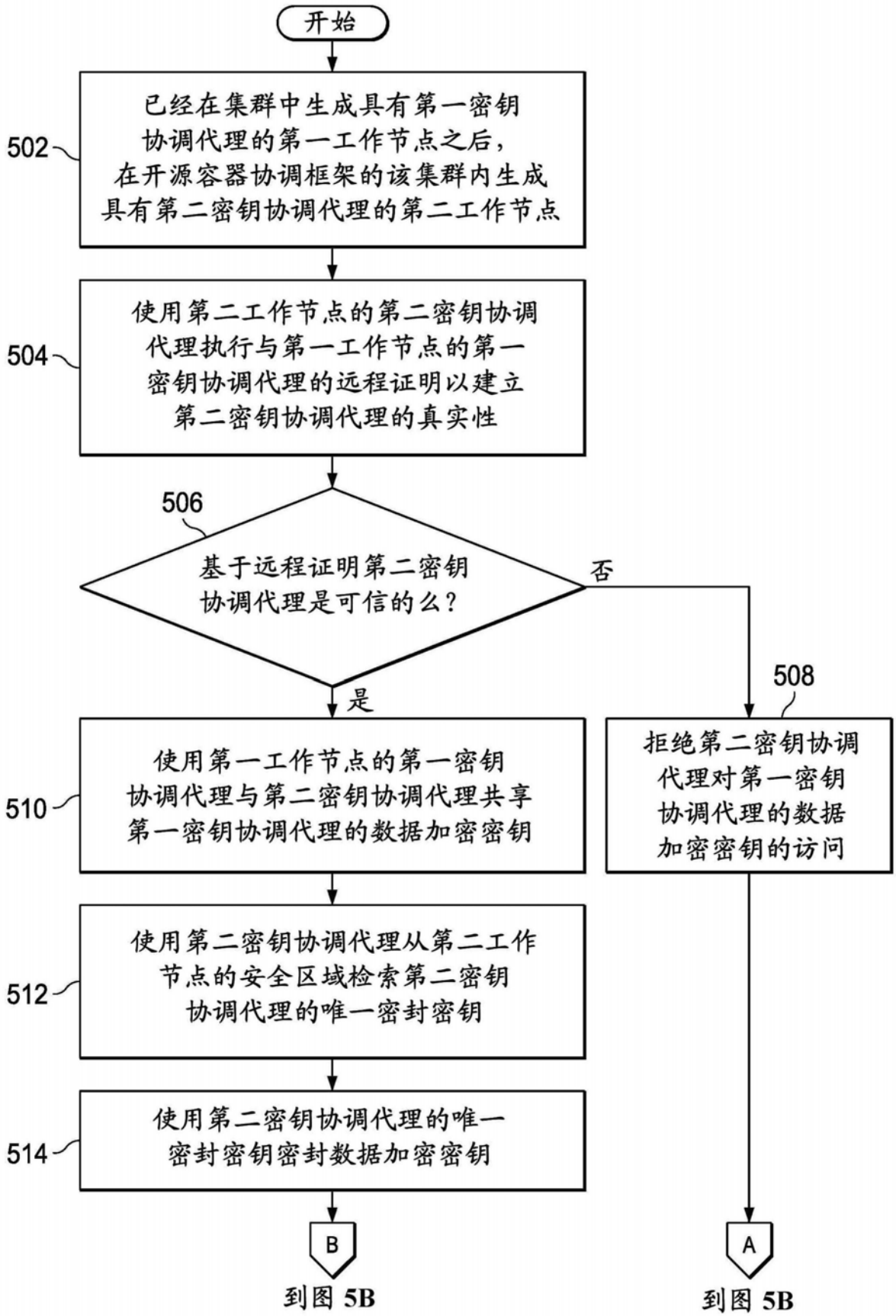

开始
已经在集群中生成具有第一密钥协调代理的第一工作节点之后，在开源容器协调框架的该集群内生成具有第二密钥协调代理的第二工作节点
502
使用第二工作节点的第二密钥协调代理执行与第一工作节点的第一密钥协调代理的远程证明以建立第二密钥协调代理的真实性
504
506
基于远程证明第二密钥协调代理是可信的么？
否
是
508
拒绝第二密钥协调代理对第一密钥协调代理的数据加密密钥的访问
使用第一工作节点的第一密钥协调代理与第二密钥协调代理共享第一密钥协调代理的数据加密密钥
510
使用第二密钥协调代理从第二工作节点的安全区域检索第二密钥协调代理的唯一密封密钥
512
使用第二密钥协调代理的唯一密封密钥密封数据加密密钥
514
B
到图 5B
A
到图 5B

图5A

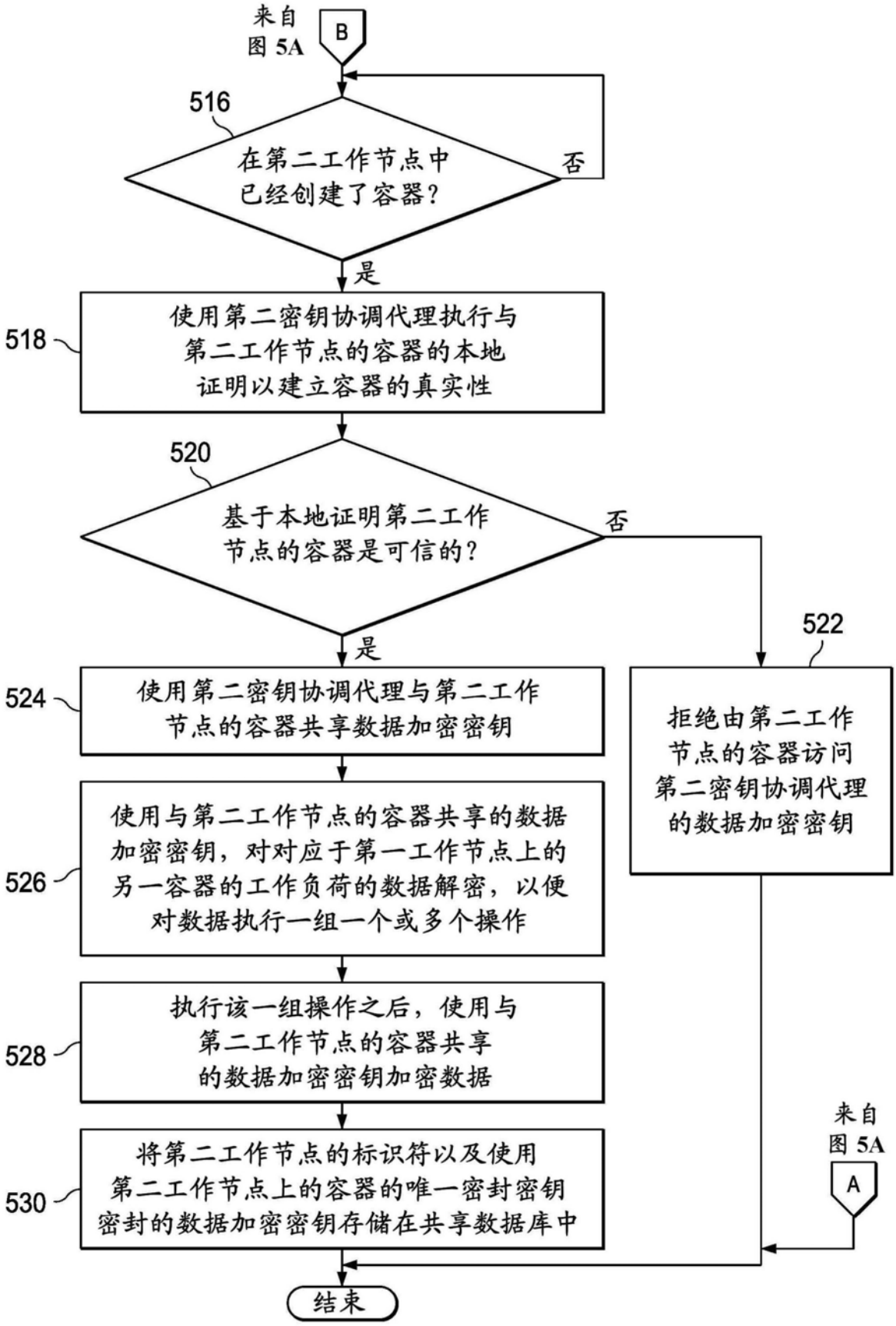

来自
图 5A
B
516
在第二工作节点中
已经创建了容器?
否
是
518
使用第二密钥协调代理执行与
第二工作节点的容器的本地
证明以建立容器的真实性
520
基于本地证明第二工作
节点的容器是可信的?
否
是
522
拒绝由第二工作
节点的容器访问
第二密钥协调代理
的数据加密密钥
524
使用第二密钥协调代理与第二工作
节点的容器共享数据加密密钥
526
使用与第二工作节点的容器共享的数据
加密密钥，对对应于第一工作节点上的
另一容器的工作负荷的数据解密，以便
对数据执行一组一个或多个操作
528
执行该一组操作之后，使用与
第二工作节点的容器共享
的数据加密密钥加密数据
530
将第二工作节点的标识符以及使用
第二工作节点上的容器的唯一密封密钥
密封的数据加密密钥存储在共享数据库中
来自
图 5A
A
结束

图5B

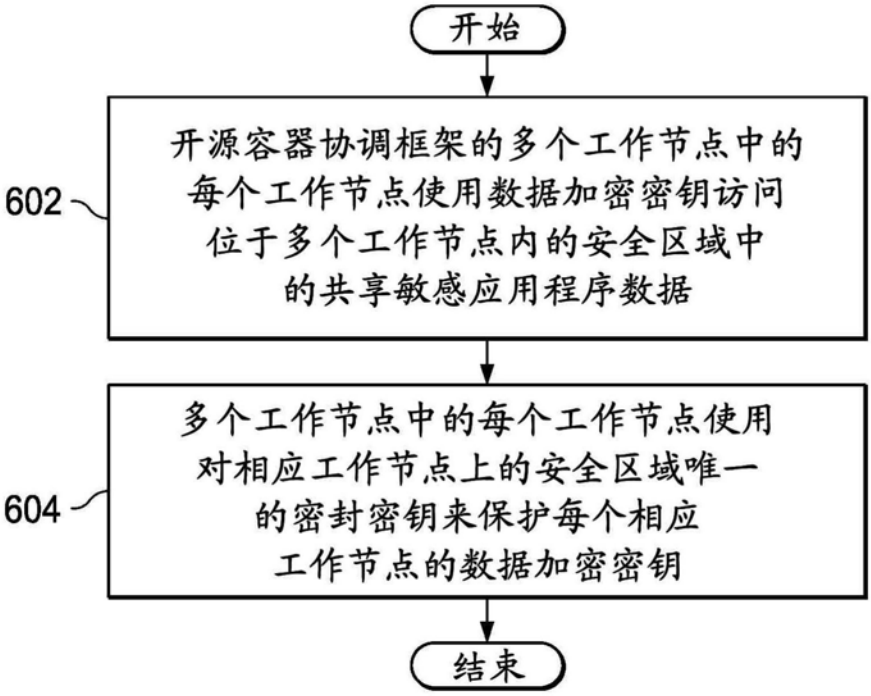

开始
开源容器协调框架的多个工作节点中的每个工作节点使用数据加密密钥访问位于多个工作节点内的安全区域中的共享敏感应用程序数据
602
多个工作节点中的每个工作节点使用对相应工作节点上的安全区域唯一的密封密钥来保护每个相应工作节点的数据加密密钥
604
结束

图6

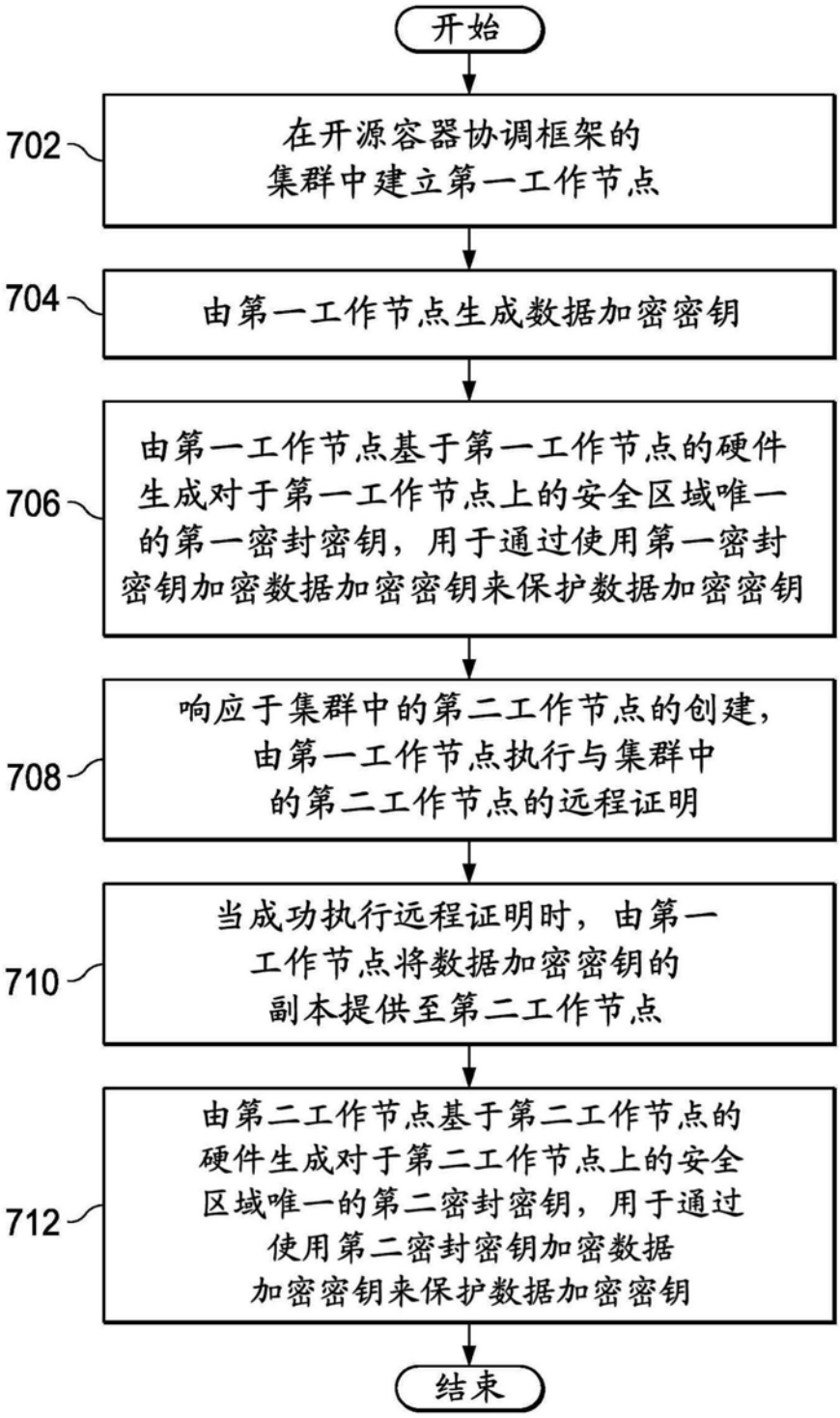

开始
702
在开源容器协调框架的集群中建立第一工作节点
704
由第一工作节点生成数据加密密钥
706
由第一工作节点基于第一工作节点的硬件生成对于第一工作节点上的安全区域唯一的第一密封密钥，用于通过使用第一密封密钥加密数据加密密钥来保护数据加密密钥
708
响应于集群中的第二工作节点的创建，由第一工作节点执行与集群中的第二工作节点的远程证明
710
当成功执行远程证明时，由第一工作节点将数据加密密钥的副本提供至第二工作节点
712
由第二工作节点基于第二工作节点的硬件生成对于第二工作节点上的安全区域唯一的第二密封密钥，用于通过使用第二密封密钥加密数据加密密钥来保护数据加密密钥
结束

图7