(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117579310 A
(43)申请公布日 2024.02.20

(21)申请号 202311427990.2

(22)申请日 2023.10.31

(71)申请人 杭州富算科技有限公司
地址 310051 浙江省杭州市滨江区西兴街道缤纷街615号4楼401室

(72)发明人 尤志强 卞阳 赵东 赵华宇 张伟奇

(74)专利代理机构 北京慧加伦知识产权代理有限公司 16035
专利代理师 李永敏

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/08(2006.01)
H04L 67/12(2022.01)

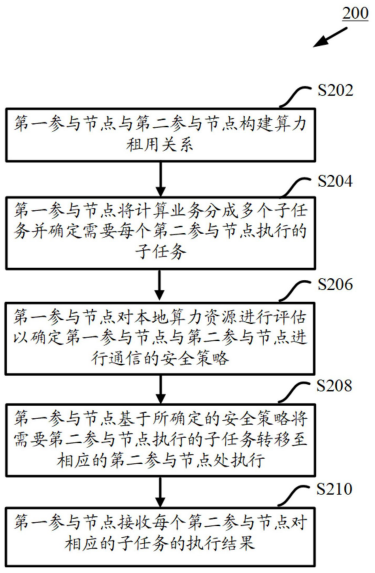
权利要求书2页 说明书7页 附图3页

(54)发明名称

利用数联网中的分布式算力执行计算业务的方法

(57)摘要

本公开的实施例提供一种利用数联网中的分布式算力执行计算业务的方法。数联网包括多个子网。每个子网包括枢纽节点和与枢纽节点直接连接的多个参与节点。该方法包括:作为算力租用方的第一参与节点与作为算力出租方的至少一个第二参与节点构建算力租用关系;第一参与节点将计算业务分成多个子任务并确定需要每个第二参与节点执行的子任务;第一参与节点对本地算力资源进行评估以确定第一参与节点与该至少一个第二参与节点进行通信的安全策略;第一参与节点基于所确定的安全策略将需要该至少一个第二参与节点执行的子任务转移至相应的第二参与节点处执行;第一参与节点接收每个第二参与节点对相应的子任务的执行结果。



CN 117579310 A

1.一种利用数联网中的分布式算力执行计算业务的方法,其特征在于,所述数联网包括多个子网,每个子网包括枢纽节点和与所述枢纽节点直接连接的多个参与节点,所述多个子网中的枢纽节点相互直接连接,所述方法包括:

作为算力租用方的第一参与节点与作为算力出租方的至少一个第二参与节点构建算力租用关系;

所述第一参与节点将计算业务分成多个子任务并确定需要每个第二参与节点执行的子任务;

所述第一参与节点对本地算力资源进行评估以确定所述第一参与节点与所述至少一个第二参与节点进行通信的安全策略;

所述第一参与节点基于所确定的安全策略将需要所述至少一个第二参与节点执行的子任务转移至相应的第二参与节点处执行;以及

所述第一参与节点接收每个第二参与节点对相应的子任务的执行结果。

2.根据权利要求1所述的方法,其特征在于,所述第一参与节点对本地算力资源进行评估以确定所述第一参与节点与所述至少一个第二参与节点进行通信的安全策略包括:

确定所述第一参与节点的本地算力资源是否足够支持对目标数据执行同态加密,所述目标数据是需要所述至少一个第二参与节点执行的子任务所涉及的所有数据;以及

响应于所述第一参与节点的本地算力资源不足够支持对所述目标数据执行同态加密,所述第一参与节点确定使用对称加密的方式与所述至少一个第二参与节点进行数据传输。

3.根据权利要求2所述的方法,其特征在于,所述第一参与节点基于所确定的安全策略将需要所述至少一个第二参与节点执行的子任务转移至相应的第二参与节点处执行包括,响应于所述第一参与节点的本地算力资源不足够支持对所述目标数据执行同态加密:

所述第一参与节点通过用于密钥协商的可信执行环境与每个第二参与节点分别协商得到相应的共享密钥;

所述第一参与节点使用相应的共享密钥对所述目标数据中的相应数据执行对称加密;

所述第一参与节点向每个第二参与节点发送相应的子任务所涉及的指令和经对称加密的数据;

每个第二参与节点在飞地对所述经对称加密的数据进行解密;以及

每个第二参与节点在所述飞地根据所接收的指令和经解密的数据来执行相应的子任务。

4.根据权利要求2所述的方法,其特征在于,所述第一参与节点基于所确定的安全策略将需要所述至少一个第二参与节点执行的子任务转移至相应的第二参与节点处执行包括,响应于所述第一参与节点的本地算力资源不足够支持对所述目标数据执行同态加密:

所述第一参与节点通过用于密钥协商的可信执行环境与每个第二参与节点分别协商得到相应的共享密钥;

所述第一参与节点向每个第二参与节点发送用于同态加密的公钥;

所述第一参与节点使用相应的共享密钥对所述目标数据中的相应数据执行对称加密;

所述第一参与节点向每个第二参与节点发送相应的子任务所涉及的指令和经对称加密的数据;

每个第二参与节点在飞地对所述经对称加密的数据进行解密;

每个第二参与节点在所述飞地根据所接收的指令和经解密的数据来执行相应的子任务;以及

每个第二参与节点使用所述公钥在所述飞地对相应的子任务的执行结果进行同态加密。

5.根据权利要求4所述的方法,其特征在于,所述方法还包括:所述第一参与节点对每个第二参与节点的执行结果进行同态解密。

6.根据权利要求4所述的方法,其特征在于,在所述第一参与节点与第三参与节点执行联合计算任务的情况下:

所述第一参与节点向所述第三参与节点发送所述公钥;

所述第三参与节点接收每个第二参与节点的经同态加密的执行结果;

所述第三参与节点使用所述公钥对本地数据进行同态加密;

所述第三参与节点根据本地指令、经同态加密的本地数据和所接收的经同态加密的执行结果来执行本地任务;

所述第一参与节点接收所述第三参与节点执行的本地任务的执行结果;以及

所述第一参与节点对所述第三参与节点的执行结果进行同态解密。

7.根据权利要求6所述的方法,其特征在于,所述第一参与节点与所述第三参与节点之间的通信数据经由第一枢纽节点和第三枢纽节点来传递,其中,所述第一枢纽节点与所述第一参与节点直接连接,所述第三枢纽节点与所述第三参与节点直接连接。

8.根据权利要求1所述的方法,其特征在于,所述第一参与节点对本地算力资源进行评估以确定所述第一参与节点与所述至少一个第二参与节点进行通信的安全策略包括:

确定所述第一参与节点的本地算力资源是否足够支持对目标数据执行同态加密,所述目标数据是需要所述至少一个第二参与节点执行的子任务所涉及的所有数据;以及

响应于所述第一参与节点的本地算力资源足够支持对所述目标数据执行同态加密,所述第一参与节点确定使用同态加密的方式与所述至少一个第二参与节点进行数据传输。

9.根据权利要求8所述的方法,其特征在于,所述第一参与节点基于所确定的安全策略将需要所述至少一个第二参与节点执行的子任务转移至相应的第二参与节点处执行包括:

响应于所述第一参与节点的本地算力资源足够支持对所述目标数据执行同态加密,所述第一参与节点对所述目标数据执行同态加密,并向每个第二参与节点发送相应的子任务所涉及的指令和经同态加密的数据;以及

每个第二参与节点根据所接收的指令和所述经同态加密的数据来执行相应的子任务。

10.根据权利要求1至9中任一项所述的方法,其特征在于,所述第一参与节点与所述第二参与节点之间的通信数据经由第一枢纽节点和第二枢纽节点来传递,其中,所述第一枢纽节点与所述第一参与节点直接连接,所述第二枢纽节点与所述第二参与节点直接连接。

利用数联网中的分布式算力执行计算业务的方法

技术领域

[0001] 本公开的实施例涉及数联网技术领域,具体地,涉及利用数联网中的分布式算力执行计算业务的方法。

背景技术

[0002] 数据共享和数据价值的流通,对于当前推进数字化经济转型发展越来越重要。随着对数据的互通、共享、交换的需求持续升温,继个人计算机(PC)互联网、移动互联网、产业互联网、物联网之后,“数联网”也应运而生。本文所提到的新型“数联网”,是实现数据要素跨行业、跨区域、跨机构流通的基础设施,与传统的狭义数联网(仅仅用于数交所或类似场景中的数据买卖交易的互联网)显著不同。狭义数联网仅仅是“数数相连的互联网”,仅涉及数据在数联网中透明传输。应用端可以直接获取数据,产生各种基于数据的业务应用。

[0003] 在新型“数联网”中,非常关键的底层能力是算力。算力在分布上是松散的。数联网作为开放性的网络体系,可以支持海量主体通过被允许的方式接入数联网。接入数联网的主体构成数联网中的一个数据节点。该节点具备一定的算力资源。当某些节点本地的计算任务结束之后,这些节点的算力资源会存在一定的闲置,导致算力资源的浪费。如果将闲置的算力资源出租给其它节点,则可充分利用数联网的算力资源,使得参与到数联网的节点获得除数据流通之外的价值。

[0004] 在利用数联网中的分布式算力执行计算业务时,需要考虑数据安全问题。

发明内容

[0005] 本文中描述的实施例提供了一种利用数联网中的分布式算力执行计算业务的方法。该方法旨在解决数联网中出现数据泄露时导致的安全问题。

[0006] 根据本公开的第一方面,提供了一种利用数联网中的分布式算力执行计算业务的方法。数联网包括多个子网。每个子网包括枢纽节点和与枢纽节点直接连接的多个参与节点。多个子网中的枢纽节点相互直接连接。该方法包括:作为算力租用方的第一参与节点与作为算力出租方的至少一个第二参与节点构建算力租用关系;第一参与节点将计算业务分成多个子任务并确定需要每个第二参与节点执行的子任务;第一参与节点对本地算力资源进行评估以确定第一参与节点与该至少一个第二参与节点进行通信的安全策略;第一参与节点基于所确定的安全策略将需要该至少一个第二参与节点执行的子任务转移至相应的第二参与节点处执行;以及第一参与节点接收每个第二参与节点对相应的子任务的执行结果。

[0007] 在本公开的一些实施例中,第一参与节点对本地算力资源进行评估以确定第一参与节点与该至少一个第二参与节点进行通信的安全策略包括:确定第一参与节点的本地算力资源是否足够支持对目标数据执行同态加密,目标数据是需要该至少一个第二参与节点执行的子任务所涉及的所有数据;以及响应于第一参与节点的本地算力资源不足够支持对目标数据执行同态加密,第一参与节点确定使用对称加密的方式与该至少一个第二参与节

点进行数据传输。

[0008] 在本公开的一些实施例中,第一参与节点基于所确定的安全策略将需要该至少一个第二参与节点执行的子任务转移至相应的第二参与节点处执行包括,响应于第一参与节点的本地算力资源不足够支持对目标数据执行同态加密:第一参与节点通过用于密钥协商的可信执行环境与每个第二参与节点分别协商得到相应的共享密钥;第一参与节点使用相应的共享密钥对目标数据中的相应数据执行对称加密;第一参与节点向每个第二参与节点发送相应的子任务所涉及的指令和经对称加密的数据;每个第二参与节点在飞地对经对称加密的数据进行解密;以及每个第二参与节点在飞地根据所接收的指令和经解密的数据来执行相应的子任务。

[0009] 在本公开的一些实施例中,第一参与节点基于所确定的安全策略将需要该至少一个第二参与节点执行的子任务转移至相应的第二参与节点处执行包括,响应于第一参与节点的本地算力资源不足够支持对目标数据执行同态加密:第一参与节点通过用于密钥协商的可信执行环境与每个第二参与节点分别协商得到相应的共享密钥;第一参与节点向每个第二参与节点发送用于同态加密的公钥;第一参与节点使用相应的共享密钥对目标数据中的相应数据执行对称加密;第一参与节点向每个第二参与节点发送相应的子任务所涉及的指令和经对称加密的数据;每个第二参与节点在飞地对经对称加密的数据进行解密;每个第二参与节点在飞地根据所接收的指令和经解密的数据来执行相应的子任务;以及每个第二参与节点使用公钥在飞地对相应的子任务的执行结果进行同态加密。

[0010] 在本公开的一些实施例中,方法还包括:第一参与节点对每个第二参与节点的执行结果进行同态解密。

[0011] 在本公开的一些实施例中,在第一参与节点与第三参与节点执行联合计算任务的情况下:第一参与节点向第三参与节点发送公钥;第三参与节点接收每个第二参与节点的经同态加密的执行结果;第三参与节点使用公钥对本地数据进行同态加密;第三参与节点根据本地指令、经同态加密的本地数据和所接收的经同态加密的执行结果来执行本地任务;第一参与节点接收第三参与节点执行的本地任务的执行结果;以及第一参与节点对第三参与节点的执行结果进行同态解密。

[0012] 在本公开的一些实施例中,第一参与节点与第三参与节点之间的通信数据经由第一枢纽节点和第三枢纽节点来传递。其中,第一枢纽节点与第一参与节点直接连接。第三枢纽节点与第三参与节点直接连接。

[0013] 在本公开的一些实施例中,第一参与节点对本地算力资源进行评估以确定第一参与节点与该至少一个第二参与节点进行通信的安全策略包括:确定第一参与节点的本地算力资源是否足够支持对目标数据执行同态加密,目标数据是需要该至少一个第二参与节点执行的子任务所涉及的所有数据;以及响应于第一参与节点的本地算力资源足够支持对目标数据执行同态加密,第一参与节点确定使用同态加密的方式与该至少一个第二参与节点进行数据传输。

[0014] 在本公开的一些实施例中,第一参与节点基于所确定的安全策略将需要该至少一个第二参与节点执行的子任务转移至相应的第二参与节点处执行包括:响应于第一参与节点的本地算力资源足够支持对目标数据执行同态加密,第一参与节点对目标数据执行同态加密,并向每个第二参与节点发送相应的子任务所涉及的指令和经同态加密的数据;以及

每个第二参与节点根据所接收的指令和经同态加密的数据来执行相应的子任务。

[0015] 在本公开的一些实施例中,第一参与节点与第二参与节点之间的通信数据经由第一枢纽节点和第二枢纽节点来传递。其中,第一枢纽节点与第一参与节点直接连接。第二枢纽节点与第二参与节点直接连接。

[0016] 根据本公开的第二方面,提供了一种存储有计算机程序的计算机可读存储介质,其中,计算机程序在由处理器执行时实现根据本公开的第一方面所述的方法的步骤。

附图说明

[0017] 为了更清楚地说明本公开的实施例的技术方案,下面将对实施例的附图进行简要说明,应当知道,以下描述的附图仅仅涉及本公开的一些实施例,而非对本公开的限制,其中:

[0018] 图1是数联网的示意性拓扑图;

[0019] 图2是根据本公开的实施例的利用数联网中的分布式算力执行计算业务的方法的示意性流程图;

[0020] 图3是根据本公开的实施例的在数联网中具有算力租用关系的参考节点的示意性关系图;

[0021] 图4是根据本公开的实施例的在数联网中具有互联合作关系的参考节点的示意性关系图。

[0022] 需要注意的是,附图中的元素是示意性的,没有按比例绘制。

具体实施方式

[0023] 为了使本公开的实施例的目的、技术方案和优点更加清楚,下面将结合附图,对本公开的实施例的技术方案进行清楚、完整的描述。显然,所描述的实施例是本公开的一部分实施例,而不是全部的实施例。基于所描述的本公开的实施例,本领域技术人员在无需创造性劳动的前提下所获得的所有其它实施例,也都属于本公开保护的范围。

[0024] 除非另外定义,否则在此使用的所有术语(包括技术和科学术语)具有与本公开主题所属领域的技术人员所通常理解的相同含义。进一步将理解的是,诸如在通常使用的词典中定义的那些的术语应解释为具有与说明书上下文和相关技术中它们的含义一致的含义,并且将不以理想化或过于正式的形式来解释,除非在此另外明确定义。另外,诸如“第一”和“第二”的术语仅用于将一个部件(或部件的一部分)与另一个部件(或部件的另一部分)区分开。

[0025] 图1示出数联网的示意性拓扑图。数联网可包括多个子网10。每个子网10包括枢纽节点11和与枢纽节点直接连接的多个参与节点12。该多个子网10中的枢纽节点11可相互直接连接。枢纽节点11与枢纽节点11之间可以通过专网进行互联。枢纽节点11承担对参与节点12进行信息聚合、寻址导航等功能。参与节点12可以是各类政务主体、行业主体、公司主体、机构主体等。直接连接到同一个枢纽节点11的参与节点12通过该枢纽节点11进行通信。直接连接到不同枢纽节点11的参与节点12通过它们各自直接连接的枢纽节点11进行通信。也就是说,参与节点12只与其直接连接的枢纽节点11直接通信,枢纽节点11之间可直接通信,而参与节点12之间需经由相应的枢纽节点11进行通信。

[0026] 在实践中,数联网中可能存在海量的子网10。单个子网10中可能存在海量的参与节点12。因此,数联网中的参与节点12的数量可能是非常庞大的。图1只示意性地示出了数联网中的一部分子网10。当某些参与节点12本地的计算任务结束之后,这些参与节点12的算力资源会存在一定的闲置,导致算力资源的浪费。如果这些参与节点12将闲置的算力资源出租给需要额外算力的参与节点12,那么需要额外算力的参与节点12就不必购买额外的硬件设备,只需要租用数联网中闲置的算力资源就可完成计算任务,这样数联网的整体算力资源可被很好地整合和利用。

[0027] 在某个参与节点需要租用算力的情况下,由于该参与节点(作为算力租用方)的计算业务中的一部分需要发送至算力出租方处来执行,因此,需要考虑出现数据泄露时导致的安全问题。

[0028] 本公开提出了一种利用数联网中的分布式算力执行计算业务的方法。该方法旨在解决数联网中出现数据泄露时导致的安全问题。图2示出根据本公开的实施例的利用数联网中的分布式算力执行计算业务的方法200的示意性流程图。

[0029] 在图2的框S202处,作为算力租用方的第一参与节点与作为算力出租方的至少一个第二参与节点构建算力租用关系。参考图3所示的在数联网中具有算力租用关系的参考节点的示意性关系图,第一参与节点A12经由路径1直接连接第一枢纽节点A11,第二参与节点B12经由路径3直接连接第二枢纽节点B11,第一枢纽节点A11经由路径2直接连接第二枢纽节点B11。第一参与节点A12可向第一枢纽节点A11发布算力资源买单。第一枢纽节点A11可根据其接收的算力资源卖单来确定与第一参与节点A12发布的算力资源买单相匹配的算力资源。算力资源卖单可来自直接连接第一枢纽节点A11的参与节点(未示出),也可以来自它枢纽节点。在图3的示例中,与第一参与节点A12发布的算力资源买单相匹配的算力资源来自至少一个第二参与节点B12。尽管在图3中示出了多个第二参与节点B12,但是本公开的实施例也支持只有一个第二参与节点B12的情况。第一枢纽节点A11可与第二枢纽节点B11通过签约的方式构建算力租用关系。这样,作为算力租用方的第一参与节点A12与作为算力出租方的第二参与节点B12构建了算力租用关系。

[0030] 在这里,“第二参与节点”指的是作为算力出租方的参与节点。本领域技术人员应理解,并不是直接连接到第二枢纽节点B11的全部参与节点都是“第二参与节点”。为了避免不重要的细节模糊本公开的重点,在图3中未示出直接连接到第二枢纽节点B11的全部参与节点。类似的,“第一参与节点”指的是作为算力租用方的参与节点。本领域技术人员应理解,并不是直接连接到第一枢纽节点A11的全部参与节点都是“第一参与节点”。为了避免不重要的细节模糊本公开的重点,在图3中未示出直接连接到第一枢纽节点A11的全部参与节点。

[0031] 在框S204处,第一参与节点A12将计算业务分成多个子任务并确定需要每个第二参与节点B12执行的子任务。第一参与节点A12可根据其本地算力资源以及匹配的算力资源卖单来确定将计算业务分成几个子任务。这样,除了第一参与节点A12本地执行的子任务,每个算力资源卖单可对应一个子任务。也就是说,每个第二参与节点B12执行一个子任务。

[0032] 在框S206处,第一参与节点A12对本地算力资源进行评估以确定第一参与节点A12与该至少一个第二参与节点B12进行通信的安全策略。在本公开的一些实施例中,第一参与节点A12确定第一参与节点A12的本地算力资源是否足够支持对目标数据执行同态加密。目

标数据是需要该至少一个第二参与节点B12执行的子任务所涉及的所有数据(这些子任务的输入数据)。同态加密(属于非对称加密)相对于对称加密更复杂,因此同态加密需要的算力资源比对称加密需要的算力资源更大,但是同态加密相对于对称加密更安全。如果第一参与节点A12的本地算力资源不足够支持对目标数据执行同态加密,则第一参与节点A12确定使用对称加密的方式与该至少一个第二参与节点B12进行数据传输。如果第一参与节点A12的本地算力资源足够支持对目标数据执行同态加密,则第一参与节点A12确定使用同态加密的方式与该至少一个第二参与节点B12进行数据传输。

[0033] 在框S208处,第一参与节点A12基于所确定的安全策略将需要该至少一个第二参与节点B12执行的子任务转移至相应的第二参与节点B12处执行。在框S210处,第一参与节点A12接收每个第二参与节点B12对相应的子任务的执行结果。

[0034] 下面针对第一参与节点A12的本地算力资源不足够支持对目标数据执行同态加密以及第一参与节点A12的本地算力资源足够支持对目标数据执行同态加密两种情况分别描述在框S208和框S210处执行的具体操作。

[0035] 在本公开的一些实施例中,如果第一参与节点A12的本地算力资源不足够支持对目标数据执行同态加密,则第一参与节点A12通过用于密钥协商的可信执行环境(Trusted Execution Environment,TEE)与每个第二参与节点B12分别协商得到相应的共享密钥。也就是说,每个第二参与节点B12得到的共享密钥是不同的。在这里第一参与节点A12作为可信执行环境中的客户端,第二参与节点B12作为可信执行环境中的服务端。应注意,在第一参与节点A12通过可信执行环境与每个第二参与节点B12进行通信的过程中,第一参与节点A12依次经由路径1、第一枢纽节点A11、路径2、第二枢纽节点B11和路径3与第二参与节点B12进行通信。

[0036] 然后,第一参与节点A12使用相应的共享密钥对目标数据中的相应数据执行对称加密。例如,第一参与节点A12使用第一共享密钥对第一子任务所涉及的数据执行对称加密,使用第二共享密钥对第二子任务所涉及的数据执行对称加密,以此类推。由于每个第二参与节点B12得到的共享密钥是不同的,因此即使经对称加密的数据在数据传输过程中发生泄漏,获得该数据的节点也无法对该数据进行解密。

[0037] 接着,第一参与节点A12(依次经由路径1、第一枢纽节点A11、路径2、第二枢纽节点B11和路径3)向每个第二参与节点B12发送相应的子任务所涉及的指令和经对称加密的数据。

[0038] 每个第二参与节点B12在接收到指令和经对称加密的数据之后,在其本地的飞地(enclave)对经对称加密的数据进行解密。飞地的安全级别很高,无论是特权或非特权软件都无法访问飞地,即便是操作系统管理员和虚拟机监视器(virtual machine monitor,VMM)也无法影响飞地中的代码和数据,因而飞地具有极高的安全性。

[0039] 每个第二参与节点B12在飞地根据所接收的指令和经解密的数据来执行相应的子任务。如上所述,飞地具有极高的安全性,因此即使经解密的数据作为明文参与子任务的执行,第二参与节点B12中的明文也不会泄露。此外,由于在第二参与节点B12中使用明文进行计算,计算效率更高,计算时间更短。

[0040] 在本公开的另一些实施例中,如果第一参与节点A12的本地算力资源不足够支持对目标数据执行同态加密,可通过第二参与节点B12对子任务的执行结果进行同态加密以

获得经同态加密的中间数据。具体地,第一参与节点A12通过用于密钥协商的可信执行环境与每个第二参与节点B12分别协商得到相应的共享密钥。并行地或者先后地,第一参与节点A12向每个第二参与节点B12发送用于同态加密的公钥。并行地或者先后地,第一参与节点A12使用相应的共享密钥对目标数据中的相应数据执行对称加密。然后,第一参与节点A12向每个第二参与节点B12发送相应的子任务所涉及的指令和经对称加密的数据。每个第二参与节点B12在飞地对经对称加密的数据进行解密。每个第二参与节点B12在飞地根据所接收的指令和经解密的数据来执行相应的子任务。然后,每个第二参与节点B12使用用于同态加密的公钥在飞地对相应的子任务的执行结果进行同态加密。

[0041] 在本公开的一些示例中,第二参与节点B12可依次经由路径3、第二枢纽节点B11、路径2、第一枢纽节点A11和路径1向第一参与节点A12发送经同态加密的执行结果,然后,第一参与节点A12可对每个第二参与节点B12的执行结果进行同态解密。经同态解密的执行结果可以是计算业务的最终结果,也可以作为第一参与节点A12的本地任务的输入数据,然后在第一参与节点A12执行完本地任务之后获得计算业务的最终结果。

[0042] 在本公开的一些实施例中,第一参与节点A12可与第三参与节点C12执行联合计算任务。图4示出这种情况下数联网中的一些参考节点的示意性关系图。在这种情况下,第一参与节点A12可依次经由路径1、第一枢纽节点A11、路径4、第三枢纽节点C11和路径5向第三参与节点C12发送用于同态加密的公钥。该公钥与第一参与节点A12发送给第二参与节点B12的公钥相同。在第二参与节点B12执行的子任务的执行结果作为第三参与节点C12执行的联合计算任务的输入的情况下,第二参与节点B12可依次经由路径3、第二枢纽节点B11、路径2、第一枢纽节点A11、路径4、第三枢纽节点C11和路径5向第三参与节点C12发送第二参与节点B12的经同态加密的执行结果。第三参与节点C12接收每个第二参与节点B12的经同态加密的执行结果。第三参与节点C12使用用于同态加密的公钥对本地数据进行同态加密。然后,第三参与节点C12根据本地指令、经同态加密的本地数据和所接收的经同态加密的执行结果来执行本地任务。由于第三参与节点C12的经同态加密的本地数据和所接收的经同态加密的执行结果使用了相同的公钥进行同态加密,因此密态下的二者(经同态加密的本地数据和所接收的经同态加密的执行结果)能够正常参与指令的计算,且第三参与节点C12执行本地任务的结果依然是同态加密的。第三参与节点C12在执行完本地任务之后可依次经由路径5、第三枢纽节点C11、路径4、第一枢纽节点A11和路径1向第一参与节点A12发送其执行结果。第一参与节点A12接收第三参与节点C12执行的本地任务的执行结果。然后,第一参与节点A12对第三参与节点C12的执行结果进行同态解密。

[0043] 在上述实施例的进一步的实施例中,第一参与节点A12可在对第三参与节点C12的执行结果进行同态解密以获得明文数据之后,对所获得的明文数据进行对称加密,并将经对称加密的数据发送给第二参与节点B12。

[0044] 第一参与节点A12、第二参与节点B12和第三参与节点C12可重复上述交互过程,直至执行完联合计算任务。这样,尽管第一参与节点A12与第二参与节点B12采用对称加密的方式来通信,也不影响第一参与节点A12与第三参与节点C12采用同态加密的方式来执行联合计算任务。

[0045] 可替代的,在本公开的另一些实施例中,如果第一参与节点A12的本地算力资源足够支持对目标数据执行同态加密,则第一参与节点A12对目标数据执行同态加密,并(依次

经由路径1、第一枢纽节点A11、路径2、第二枢纽节点B11和路径3)向每个第二参与节点B12发送相应的子任务所涉及的指令和经同态加密的数据。每个第二参与节点B12根据所接收的指令和经同态加密的数据来执行相应的子任务。然后,第一参与节点A12可对每个第二参与节点B12的执行结果进行同态解密。经同态解密的执行结果可以是计算业务的最终结果,也可以作为第一参与节点A12的本地任务的输入数据,然后在第一参与节点A12执行完本地任务之后获得计算业务的最终结果。

[0046] 在本公开的其它实施例中,还提供了一种存储有计算机程序的计算机可读存储介质,其中,计算机程序在由处理器执行时能够实现如图2所示的方法的步骤。

[0047] 综上所述,根据本公开的实施例的利用数联网中的分布式算力执行计算业务的方法能够安全地使用租用的算力来执行计算业务,不会出现数据泄露而导致的安全问题。根据本公开的实施例的方法还能够根据算力租用方的本地算力资源水平来灵活地选择与算力出租方进行通信的安全策略,以满足实际应用的需求。根据本公开的实施例的方法还能够安全地执行联合计算任务,以适应更多的应用场景。

[0048] 附图中的流程图和框图显示了根据本公开的多个实施例的装置和方法的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段或指令的一部分,所述模块、程序段或指令的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个连续的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这依所涉及的功能而定。也要注意的是,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以用执行规定的功能或动作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0049] 除非上下文中另外明确地指出,否则在本文和所附权利要求中所使用的词语的单数形式包括复数,反之亦然。因而,当提及单数时,通常包括相应术语的复数。相似地,措辞“包含”和“包括”将解释为包含在内而不是独占性地。同样地,术语“包括”和“或”应当解释为包括在内的,除非本文中明确禁止这样的解释。在本文中使用术语“示例”之处,特别是当其位于一组术语之后时,所述“示例”仅仅是示例性的和阐述性的,且不应当被认为是独占性的或广泛性的。

[0050] 适应性的进一步的方面和范围从本文中提供的描述变得明显。应当理解,本申请的各个方面可以单独或者与一个或多个其它方面组合实施。还应当理解,本文中的描述和特定实施例旨在仅说明的目的并不旨在限制本申请的范围。

[0051] 以上对本公开的若干实施例进行了详细描述,但显然,本领域技术人员可以在不脱离本公开的精神和范围的情况下对本公开的实施例进行各种修改和变型。本公开的保护范围由所附的权利要求限定。

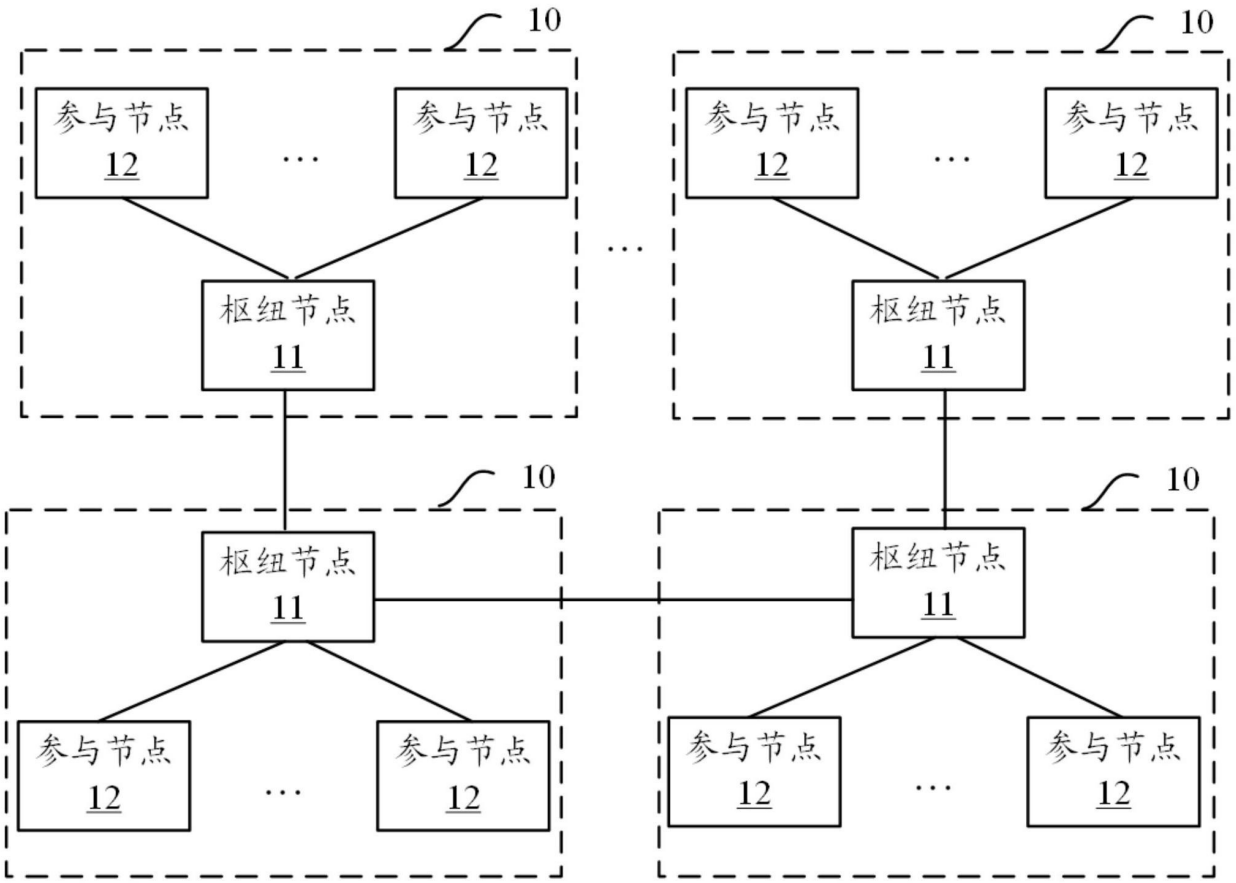

10
参与节点
12
…
参与节点
12
枢纽节点
11
10
参与节点
12
…
参与节点
12
枢纽节点
11
10
枢纽节点
11
10
枢纽节点
11
参与节点
12
…
参与节点
12
参与节点
12
…
参与节点
12

图1

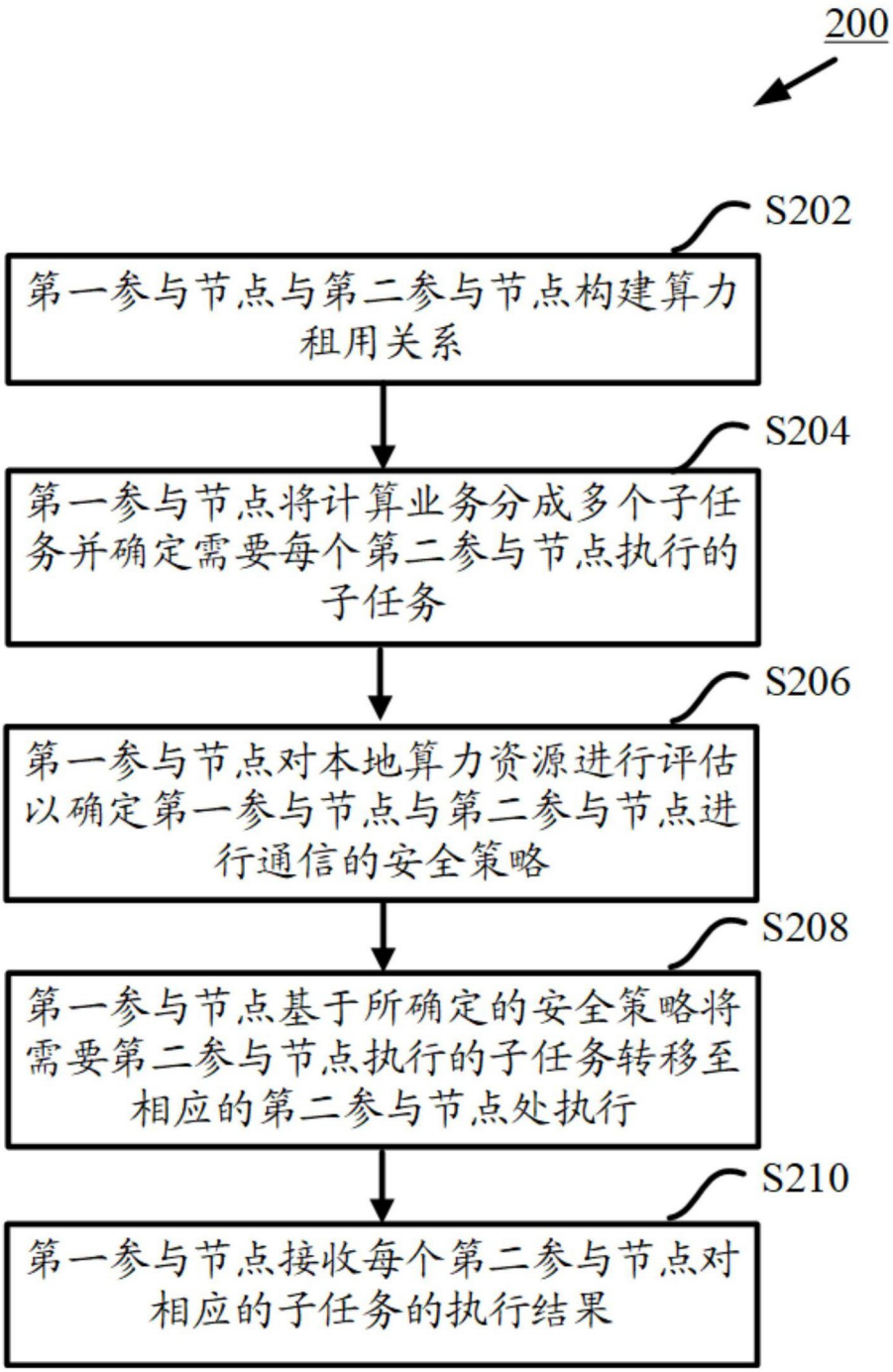

200
S202
第一参与节点与第二参与节点构建算力租用关系
S204
第一参与节点将计算业务分成多个子任务并确定需要每个第二参与节点执行的子任务
S206
第一参与节点对本地算力资源进行评估以确定第一参与节点与第二参与节点进行通信的安全策略
S208
第一参与节点基于所确定的安全策略将需要第二参与节点执行的子任务转移至相应的第二参与节点处执行
S210
第一参与节点接收每个第二参与节点对相应的子任务的执行结果

图2

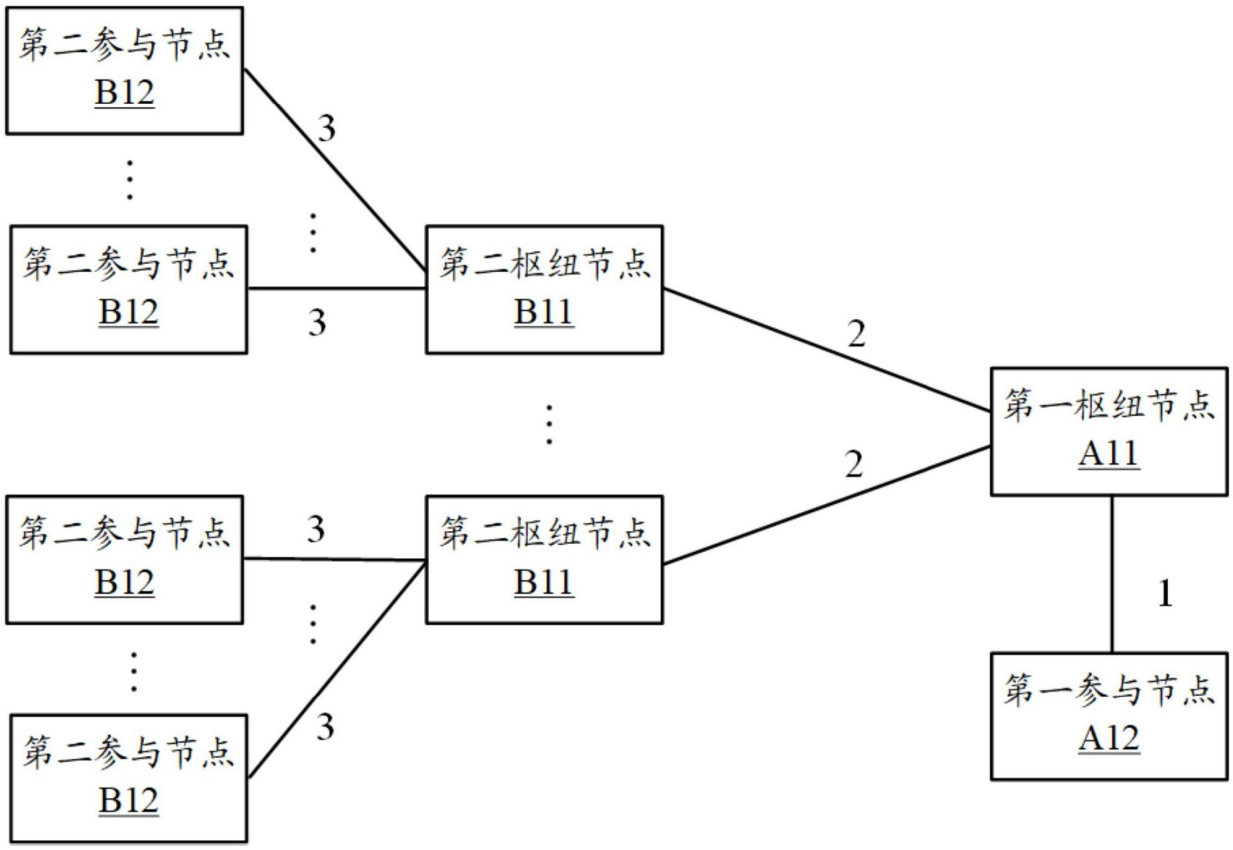

第二参与节点
B12
第二参与节点
B12
第二参与节点
B12
第二参与节点
B12
第二参与节点
B12
第二枢纽节点
B11
第二枢纽节点
B11
第一枢纽节点
A11
第一参与节点
A12
3
3
3
3
3
2
2
1

图3

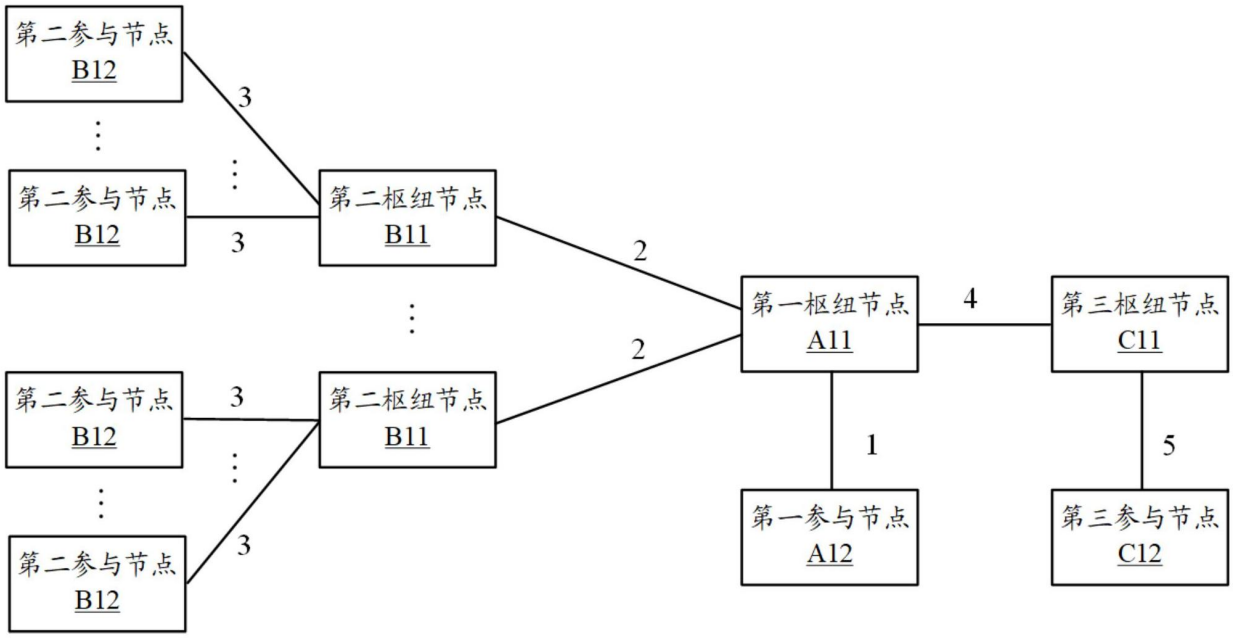

第二参与节点
B12
第二参与节点
B12
第二参与节点
B12
第二参与节点
B12
第二枢纽节点
B11
第二枢纽节点
B11
第一枢纽节点
A11
第三枢纽节点
C11
第一参与节点
A12
第三参与节点
C12
3
3
3
3
2
2
4
1
5

图4