(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114595483 B
(45)授权公告日 2022.08.02

(21)申请号 202210500489.3

(22)申请日 2022.05.10

(65)同一申请的已公布的文献号
申请公布号 CN 114595483 A

(43)申请公布日 2022.06.07

(73)专利权人 富算科技(上海)有限公司
地址 200135 上海市浦东新区中国(上海)自由贸易试验区浦东大道1200号2层A区

(72)发明人 孙小超 陈立峰 卞阳 尤志强

(74)专利代理机构 北京超凡宏宇专利代理事务所(特殊普通合伙) 11463
专利代理师 唐正瑜

(51)Int.Cl.
G06F 21/62(2013.01)

(56)对比文件
CN 110941854 A,2020.03.31
CN 113472538 A,2021.10.01
CN 111444526 A,2020.07.24
CN 113849806 A,2021.12.28
CN 114386038 A,2022.04.22
US 2015007258 A1,2015.01.01
仲红.安全多方计算的关键技术分析.《安徽农业大学学报》.2007,第34卷(第02期),全文.
李书缘等.面向多方安全的数据联邦系统.《软件学报》.2022,第33卷(第03期),全文.
Riza Arda Kirmizioglu等.Multi-Party WebRTC Services Using Delay and Bandwidth Aware SDN-Assisted IP Multicasting of Scalable Video Over 5G Networks.《IEEE Transactions on Multimedia》.2019,第22卷(第04期),全文.

审查员 张亚芳

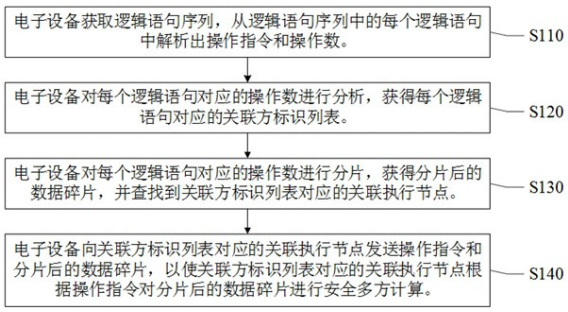
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种安全多方计算方法、装置、电子设备及存储介质

(57)摘要

本申请提供一种安全多方计算方法、装置、电子设备及存储介质,用于改善整个安全多方计算的总资源消耗较高的问题。该方法包括:获取逻辑语句序列,从逻辑语句序列中的每个逻辑语句中解析出操作指令和操作数;对每个逻辑语句对应的操作数进行分析,获得每个逻辑语句对应的关联方标识列表;对每个逻辑语句对应的操作数进行分片,获得分片后的数据碎片,并查找到关联方标识列表对应的关联执行节点;向关联方标识列表对应的关联执行节点发送操作指令和分片后的数据碎片,以使关联方标识列表对应的关联执行节点根据操作指令对分片后的数据碎片进行安全多方计算。



CN 114595483 B

1.一种安全多方计算方法,其特征在于,包括:

获取逻辑语句序列,从所述逻辑语句序列中的每个逻辑语句中解析出操作指令和操作数;

对所述每个逻辑语句对应的操作数进行分析,获得所述每个逻辑语句对应的关联方标识列表;

对所述每个逻辑语句对应的操作数进行分片,获得分片后的数据碎片,并查找到所述关联方标识列表对应的关联执行节点;

向所述关联方标识列表对应的关联执行节点发送所述操作指令和所述分片后的数据碎片,以使所述关联方标识列表对应的关联执行节点根据所述操作指令对所述分片后的数据碎片进行安全多方计算;

其中,所述操作数包括:输入数据和中间数据;所述对所述每个逻辑语句对应的操作数进行分析,获得所述每个逻辑语句对应的关联方标识列表,包括:获取所述输入数据的关联方标识和所述中间数据的历史数据关联方标识;将所述输入数据的关联方标识和所述中间数据的历史数据关联方标识进行合并,获得所述每个逻辑语句对应的关联方标识列表;

所述对所述每个逻辑语句对应的操作数进行分片,获得分片后的数据碎片,包括:对所述输入数据进行分片,获得所述输入数据的数据碎片;对所述中间数据进行重新分片,获得所述中间数据的数据碎片;将所述输入数据的数据碎片与所述中间数据的数据碎片进行合并,获得所述分片后的数据碎片。

2.根据权利要求1所述的方法,其特征在于,所述获取逻辑语句序列,包括:

获取源代码,对所述源代码进行编译,获得所述逻辑语句序列。

3.根据权利要求1所述的方法,其特征在于,所述查找到所述关联方标识列表对应的关联执行节点,包括:

在数据库中查找所述关联方标识列表中的每个关联方标识对应的至少一个服务器标识,获得多个服务器标识,所述数据库中存储有所述关联方标识与所述服务器标识的对应关系;

将所述多个服务器标识对应的服务器节点确定为所述关联执行节点。

4.一种安全多方计算装置,其特征在于,包括:

语句序列获取模块,用于获取逻辑语句序列,从所述逻辑语句序列中的每个逻辑语句中解析出操作指令和操作数;

关联列表获取模块,用于对所述每个逻辑语句对应的操作数进行分析,获得所述每个逻辑语句对应的关联方标识列表;

数据碎片获得模块,用于对所述每个逻辑语句对应的操作数进行分片,获得分片后的数据碎片,并查找到所述关联方标识列表对应的关联执行节点;

数据碎片发送模块,用于向所述关联方标识列表对应的关联执行节点发送所述操作指令和所述分片后的数据碎片,以使所述关联方标识列表对应的关联执行节点根据所述操作指令对所述分片后的数据碎片进行安全多方计算;

其中,所述操作数包括:输入数据和中间数据;所述关联列表获取模块,包括:关联标识获取模块,用于获取所述输入数据的关联方标识和所述中间数据的历史数据关联方标识;关联标识合并模块,用于将所述输入数据的关联方标识和所述中间数据的历史数据关联方

标识进行合并，获得所述每个逻辑语句对应的关联方标识列表；

所述数据碎片获得模块，包括：输入数据分片模块，用于对所述输入数据进行分片，获得所述输入数据的数据碎片；中间数据分片模块，用于对所述中间数据进行重新分片，获得所述中间数据的数据碎片；数据碎片合并模块，用于将所述输入数据的数据碎片与所述中间数据的数据碎片进行合并，获得所述分片后的数据碎片。

5.一种电子设备，其特征在于，包括：处理器和存储器，所述存储器存储有所述处理器可执行的机器可读指令，所述机器可读指令被所述处理器执行时执行如权利要求1至3任一项所述的方法。

6.一种计算机可读存储介质，其特征在于，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器运行时执行如权利要求1至3任一项所述的方法。

一种安全多方计算方法、装置、电子设备及存储介质

技术领域

[0001] 本申请涉及隐私计算和安全多方计算的技术领域，具体而言，涉及一种安全多方计算方法、装置、电子设备及存储介质。

背景技术

[0002] 安全多方计算(Secure Multi-Party Computation,SMC)的研究主要是针对无可信第三方的情况下，如何安全地计算一个约定函数的问题。一个安全多方计算协议，如果对于拥有无限计算能力攻击者而言是安全的，则称作是信息论安全的或无条件安全的；如果对于拥有多项式计算能力的攻击者是安全的，则称为是密码学安全的或条件安全的。

[0003] 目前，基于秘密分享的安全多方计算的过程中，需要先将参与计算的操作数通过秘密分享的方式发送给各个参与方，然后，所有参与方都会参与到每一步计算逻辑语句的执行过程中。在每一步的逻辑语句计算过程中，由颗粒度较细的操作指令或者计算算子组成，例如加法、乘法或幂运算等算子，这些算子需要所有参与方都参与计算过程，即使是某一步的逻辑所处理的数据与某一方无关，也需要该无关方参与安全多方计算的过程。因此，目前整个安全多方计算的总资源消耗较高。

发明内容

[0004] 本申请实施例的目的在于提供一种安全多方计算方法、装置、电子设备及存储介质，用于改善整个安全多方计算的总资源消耗较高的问题。

[0005] 本申请实施例提供了一种安全多方计算方法，包括：获取逻辑语句序列，从逻辑语句序列中的每个逻辑语句中解析出操作指令和操作数；对每个逻辑语句对应的操作数进行分析，获得每个逻辑语句对应的关联方标识列表；对每个逻辑语句对应的操作数进行分片，获得分片后的数据碎片，并查找到关联方标识列表对应的关联执行节点；向关联方标识列表对应的关联执行节点发送操作指令和分片后的数据碎片，以使关联方标识列表对应的关联执行节点根据操作指令对分片后的数据碎片进行安全多方计算。在上述的实现过程中，通过在执行每个逻辑语句时，分析出关联方标识列表对应的关联执行节点，并只由这些关联方标识列表对应的关联执行节点来参与计算过程，避免了无关方参与安全多方计算的情况，从而有效地降低了整个安全多方计算的总资源消耗，改善了整个安全多方计算的总资源消耗高问题。进一步地，在各个参与方的计算资源不对等的情况下，使用该安全多方计算方法可以合理均衡地使用各个参与方的计算资源，从而有效提高在各方计算资源不对等情况下的资源利用率。

[0006] 可选地，在本申请实施例中，操作数包括：输入数据和中间数据；对每个逻辑语句对应的操作数进行分析，获得每个逻辑语句对应的关联方标识列表，包括：获取输入数据的关联方标识和中间数据的历史数据关联方标识；将输入数据的关联方标识和中间数据的历史数据关联方标识进行合并，获得每个逻辑语句对应的关联方标识列表。

[0007] 在上述的实现过程中，通过动态地分析出输入数据的关联方标识和中间数据的历

史数据关联方标识，并将输入数据的关联方标识和中间数据的历史数据关联方标识进行合并，避免了静态地将中间数据让所有参与方进行安全多方计算的情况，从而只由这些关联方标识列表对应的关联执行节点来参与计算过程，有效地降低了整个安全多方计算的总资源消耗。

[0008] 可选地，在本申请实施例中，对每个逻辑语句对应的操作数进行分片，获得分片后的数据碎片，包括：对输入数据进行分片，获得输入数据的数据碎片；对中间数据进行重新分片，获得中间数据的数据碎片；将输入数据的数据碎片与中间数据的数据碎片进行合并，获得分片后的数据碎片。

[0009] 在上述的实现过程中，通过动态地对输入数据和中间数据进行分片，并将输入数据的数据碎片与中间数据的数据碎片进行合并，避免了将数据碎片让所有参与方进行安全多方获知导致安全性降低的情况，从而只由这些关联方标识列表对应的关联执行节点来参与计算过程，有效地提高了整个安全多方计算的安全性。

[0010] 可选地，在本申请实施例中，获取逻辑语句序列，包括：获取源代码，对源代码进行编译，获得逻辑语句序列。

[0011] 可选地，在本申请实施例中，查找到关联方标识列表对应的关联执行节点，包括：在数据库中查找关联方标识列表中的每个关联方标识对应的至少一个服务器标识，获得多个服务器标识，数据库中存储有关联方标识与服务器标识的对应关系；将多个服务器标识对应的服务器节点确定为关联执行节点。

[0012] 本申请实施例还提供了一种安全多方计算装置，包括：语句序列获取模块，用于获取逻辑语句序列，从逻辑语句序列中的每个逻辑语句中解析出操作指令和操作数；关联列表获取模块，用于对每个逻辑语句对应的操作数进行分析，获得每个逻辑语句对应的关联方标识列表；数据碎片获得模块，用于对每个逻辑语句对应的操作数进行分片，获得分片后的数据碎片，并查找到关联方标识列表对应的关联执行节点；数据碎片发送模块，用于向关联方标识列表对应的关联执行节点发送操作指令和分片后的数据碎片，以使关联方标识列表对应的关联执行节点根据操作指令对分片后的数据碎片进行安全多方计算。

[0013] 在上述的实现过程中，通过对每个逻辑语句对应的操作数进行分片，获得分片后的数据碎片，并查找到关联方标识列表对应的关联执行节点；然后，向关联方标识列表对应的关联执行节点发送操作指令和分片后的数据碎片，以使关联方标识列表对应的关联执行节点根据操作指令对分片后的数据碎片进行安全多方计算。也就是说，通过在执行每个逻辑语句时，分析出关联方标识列表对应的关联执行节点，并只由这些关联方标识列表对应的关联执行节点来参与计算过程，避免了无关方参与安全多方计算的情况，从而有效地降低了整个安全多方计算的总资源消耗。

[0014] 可选地，在本申请实施例中，操作数包括：输入数据和中间数据；关联列表获取模块，包括：关联标识获取模块，用于获取输入数据的关联方标识和中间数据的历史数据关联方标识；关联标识合并模块，用于将输入数据的关联方标识和中间数据的历史数据关联方标识进行合并，获得每个逻辑语句对应的关联方标识列表。

[0015] 可选地，在本申请实施例中，数据碎片获得模块，包括：输入数据分片模块，用于对输入数据进行分片，获得输入数据的数据碎片；中间数据分片模块，用于对中间数据进行重新分片，获得中间数据的数据碎片；数据碎片合并模块，用于将输入数据的数据碎片与中间

数据的数据碎片进行合并，获得分片后的数据碎片。

[0016] 可选地，在本申请实施例中，语句序列获取模块，包括：源代码编译模块，用于获取源代码，对源代码进行编译，获得逻辑语句序列。

[0017] 可选地，在本申请实施例中，数据碎片获得模块，还包括：服务器标识查找模块，用于在数据库中查找关联方标识列表中的每个关联方标识对应的至少一个服务器标识，获得多个服务器标识，数据库中存储有关联方标识与服务器标识的对应关系；执行节点确定模块，用于将多个服务器标识对应的服务器节点确定为关联执行节点。

[0018] 本申请实施例还提供了一种电子设备，包括：处理器和存储器，存储器存储有处理器可执行的机器可读指令，机器可读指令被处理器执行时执行如上面描述的方法。

[0019] 本申请实施例还提供了一种计算机可读存储介质，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器运行时执行如上面描述的方法。

附图说明

[0020] 为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本申请实施例中的某些实施例，因此不应被看作是对范围的限定，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他相关的附图。

[0021] 图1示出的本申请实施例提供的安全多方计算方法的流程示意图；

[0022] 图2示出的本申请实施例提供的逻辑语句的处理过程示意图；

[0023] 图3示出的本申请实施例提供的安全多方计算装置的结构示意图；

[0024] 图4示出的本申请实施例提供的电子设备的结构示意图。

具体实施方式

[0025] 下面将结合本申请实施例中附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请实施例中的一部分实施例，而不是全部的实施例。通常在此处附图中描述和示出的本申请实施例的组件可以以各种不同的配置来布置和设计。因此，以下对在附图中提供的本申请实施例的详细描述并非旨在限制要求保护的本申请实施例的范围，而是仅仅表示本申请实施例中的选定实施例。基于本申请实施例，本领域技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本申请实施例保护的范围。

[0026] 在介绍本申请实施例提供的安全多方计算方法之前，先介绍本申请实施例中所涉及的一些概念：

[0027] 同态加密(Homomorphic encryption)是一种加密形式，同态加密允许人们对密文进行特定形式的代数运算得到仍然是加密的结果，将其解密所得到的结果与对明文进行同样的运算结果一样。换言之，这项技术令人们可以在加密的数据中进行诸如检索、比较等操作，得出正确的结果，而在整个处理过程中无需对数据进行解密。

[0028] 计算机集群(computer cluster)，又被简称为集群，是指一组松散或紧密连接在一起工作的计算机，这些计算机需要被安装操作系统和协同工作的软件后才能在一起协同工作，此处协同工作的计算机又可以被称为集群节点或者服务器节点。由于这些计算机协

同工作,在许多方面它们可以被视为单个系统;计算机集群与网格计算机不同,计算机集群将每个节点设置为执行相同的任务,由软件控制和调度。

[0029] 应用程序(application program),又被称为应用软件(application software),有时简称应用(app),是电脑软件的主要分类之一,是指为针对用户的某种特殊应用目的所撰写的计算机程序,具体例如:文本处理器、表格、浏览器、媒体播放器和图像编辑器等。

[0030] 需要说明的是,本申请实施例提供的安全多方计算方法可以被电子设备执行,这里的电子设备是指具有执行计算机程序功能的设备终端或者服务器,设备终端例如:智能手机、个人电脑、平板电脑、个人数字助理或者移动上网设备等。服务器是指通过网络提供计算服务的设备,服务器例如:x86服务器以及非x86服务器,非x86服务器包括:大型机、小型机和UNIX服务器。

[0031] 下面介绍该安全多方计算方法适用的应用场景,这里的应用场景包括但不限于:使用该安全多方计算方法对基于秘密分享的安全多方计算的过程进行改进,具体例如:在基于秘密分享的安全多方计算的过程中,分析出每个逻辑语句的关联方标识列表对应的关联执行节点,并只由这些关联方标识列表对应的关联执行节点来参与计算过程,避免了无关方参与安全多方计算的情况,有效地降低了整个安全多方计算的总资源消耗,同时也减少了逻辑语句被泄露的风险,从而增加了基于秘密分享的安全多方计算的安全性等。

[0032] 请参见图1示出的本申请实施例提供的安全多方计算方法的流程示意图;该安全多方计算方法的主要思路是,通过对每个逻辑语句对应的操作数进行分片,获得分片后的数据碎片,并查找到关联方标识列表对应的关联执行节点;然后,向关联方标识列表对应的关联执行节点发送操作指令和分片后的数据碎片,以使关联方标识列表对应的关联执行节点根据操作指令对分片后的数据碎片进行安全多方计算。也就是说,通过在执行每个逻辑语句时,分析出关联方标识列表对应的关联执行节点,并只由这些关联方标识列表对应的关联执行节点来参与计算过程,避免了无关方参与安全多方计算的情况,从而有效地降低了整个安全多方计算的总资源消耗。上述安全多方计算方案具体可以包括:

[0033] 步骤S110:电子设备获取逻辑语句序列,从逻辑语句序列中的每个逻辑语句中解析出操作指令和操作数。

[0034] 其中,上面的逻辑语句序列包括:多个逻辑语句,每个逻辑语句中包括操作指令和操作数,操作数可以包括:输入数据和中间数据,具体的例子将在下面详细地说明。

[0035] 上述步骤S110的实施方式可以包括:获取源代码,使用预设编译器对源代码进行编译,获得逻辑语句序列,并从逻辑语句序列中的每个逻辑语句中解析出操作指令和操作数;上述的预设编译器可以采用专为SMC场景而设计的编译器,即将SMC的源代码编译为逻辑语句序列的编译器;具体例如:假设源代码中的核心逻辑是$y:=(a+b+c+d)^2\times d$,其中,y表示待计算的SMC计算结果,:=表示待赋值后计算,a、b、c和d分别是Alice、Bob、Charlie和David四个参与方提供的输入数据,那么可以将该源代码编译为逻辑语句序列,逻辑语句序列包括多个逻辑语句,编译后的多个逻辑语句例如:$t_1:= a+b$、$t_2:= c+d$、$t_3:= t_1+t_2$、$t_4= t_3^2$、和$y:= t_3\times d$;其中,y表示待计算的SMC计算结果,:=表示待赋值后计算,a、b、c和d分别是Alice、Bob、Charlie和David四个参与方提供的输入数据,t_1代表第一条逻辑语句计算出来的中间数据,t_2代表第二条逻辑语句计算出来的中间数据,t_3代表第三条逻辑语句计算出来的中间数据,t_4代表第四条逻辑语句计算出来的中间数据,上面的加号和乘号等运算符

代表操作指令。

[0036] 在步骤S110之后，执行步骤S120：电子设备对每个逻辑语句对应的操作数进行分析，获得每个逻辑语句对应的关联方标识列表。

[0037] 请参见图2示出的本申请实施例提供的逻辑语句的处理过程示意图；上述步骤S120的实施方式具体可以包括：

[0038] 步骤S121：获取输入数据的关联方标识和中间数据的历史数据关联方标识。

[0039] 上述步骤S121的实施方式例如：假设编译后的多个逻辑语句是t_1:= a+b、t_2:= c+d、t_3:= t_1+t_2、t_4= t_3^2、和y:= t_3×d；且当前已经执行到第5个逻辑语句(即y:= t_3×d)，那么第5个逻辑语句的输入数据是d，使用输入数据关联执行方分析器分析出d的关联方标识是David，此处的输入数据关联执行方分析器是指用于分析出输入数据的关联方的应用程序。如果第5个逻辑语句的中间数据是t_3，那么可以使用中间数据关联执行方分析器分析出t_3的历史数据关联方标识包括：Alice、Bob、Charlie和David，此处的中间数据关联执行方分析器是指用于分析出中间数据的关联方的应用程序；当然，此处的t_3的历史数据关联方标识也可以使用元祖列表表示，具体例如：由t_3的历史数据关联方标识构成的元祖列表(可以理解为键值对数据库)为<a，Alice>、<b，Bob>、<c，Charlie>和<d，David>。

[0040] 步骤S122：将输入数据的关联方标识和中间数据的历史数据关联方标识进行合并，获得每个逻辑语句对应的关联方标识列表。

[0041] 上述步骤S122的实施方式例如：假设第5个逻辑语句的输入数据的关联方标识是David，且第5个逻辑语句的中间数据t_3的历史数据关联方标识包括：Alice、Bob、Charlie和David，可以使用关联方合并器将输入数据的关联方标识和中间数据的历史数据关联方标识进行合并，获得每个逻辑语句对应的(去重后的)关联方标识列表是Alice、Bob、Charlie和David。

[0042] 在步骤S120之后，执行步骤S130：电子设备对每个逻辑语句对应的操作数进行分片，获得分片后的数据碎片，并查找到关联方标识列表对应的关联执行节点。

[0043] 上述步骤S130中的对每个逻辑语句对应的操作数进行分片的实施方式具体可以包括：首先，使用输入数据分片器对输入数据进行同态加密，获得同态加密后的数据，并使用同态加密算法对同态加密后的数据进行分片，获得输入数据的数据碎片。然后，使用中间数据重分片器对中间数据进行重新分片，获得中间数据的数据碎片。最后，将输入数据的数据碎片与中间数据的数据碎片进行合并，获得分片后的数据碎片。

[0044] 上述步骤S130中的查找到关联方标识列表对应的关联执行节点的实施方式具体可以包括：在数据库中查找关联方标识列表中的每个关联方标识对应的至少一个服务器标识，获得多个服务器标识；其中，数据库中存储有关联方标识与服务器标识的对应关系，此处的数据库包括：关系型数据库和非关系型数据库；可以使用的关系型数据库例如：Mysql、PostgreSQL、Oracle和SQLSever等，可以使用的非关系型数据库包括：grakn数据库、Neo4j图数据库、Hadoop子系统HBase、MongoDB和CouchDB等。将多个服务器标识对应的服务器节点确定为关联执行节点，此处的服务器节点是指集群中的服务器节点。

[0045] 在步骤S130之后，执行步骤S140：电子设备向关联方标识列表对应的关联执行节点发送操作指令和分片后的数据碎片，以使关联方标识列表对应的关联执行节点根据操作指令对分片后的数据碎片进行安全多方计算。

[0046] 上述步骤S140的实施方式例如:电子设备通过传输控制协议(Transmission Control Protocol,TCP)或者用户数据报协议(User Datagram Protocol,UDP)向关联方标识列表对应的关联执行节点发送操作指令和分片后的数据碎片,以使关联方标识列表对应的关联执行节点根据操作指令对分片后的数据碎片进行安全多方计算。关联执行节点在接收到电子设备发送的操作指令和分片后的数据碎片之后,根据操作指令对分片后的数据碎片进行安全多方计算。

[0047] 在具体的实践过程中,还可以对源代码进行编译的过程进行优化,获得优化后的多个逻辑语句,有些编译过程优化可以减少某个参与方执行逻辑语句的数量。相比于,编译后的多个逻辑语句是$t_1:=a+b$、$t_2:=t_1+c$、$t_3:=t_2+d$、$t_4=t_3^2$、和$y:=t_3\times d$;Alice需要参与全部五个逻辑语句的安全多方计算过程。然而,假设编译后的多个逻辑语句是$t_1:=a+b$、$t_2:=c+d$、$t_3:=t_1+t_2$、$t_4=t_3^2$、和$y:=t_3\times d$;Alice只需要参与$t_1:=a+b$、$t_3:=t_1+t_2$、$t_4=t_3^2$、和$y:=t_3\times d$这四个逻辑语句的安全多方计算过程即可。两者相对比,可以得出结论,分析出关联方标识列表对应的关联执行节点,并只由这些关联方标识列表对应的关联执行节点来参与计算,可以有效降低整个安全多方计算的总资源消耗。可以理解的是,当然有些编译过程优化可以减少所有参与方执行的逻辑语句的总次数,可以表示为“参与方*逻辑语句”的总次数最少,例如循环执行、迭代执行或者递归调用的逻辑语句等等。

[0048] 在上述的实现过程中,通过对每个逻辑语句对应的操作数进行分片,获得分片后的数据碎片,并查找到关联方标识列表对应的关联执行节点;然后,向关联方标识列表对应的关联执行节点发送操作指令和分片后的数据碎片,以使关联方标识列表对应的关联执行节点根据操作指令对分片后的数据碎片进行安全多方计算。也就是说,通过在执行每个逻辑语句时,分析出关联方标识列表对应的关联执行节点,并只由这些关联方标识列表对应的关联执行节点来参与计算过程,避免了无关方参与安全多方计算的情况,从而有效地降低了整个安全多方计算的总资源消耗,改善了整个安全多方计算的总资源消耗高问题。进一步地,在各个参与方的计算资源不对等的情况下,使用该安全多方计算方法可以合理均衡地使用各个参与方的计算资源,从而有效提高在各方计算资源不对等情况下的资源利用率。

[0049] 请参见图3示出的本申请实施例提供的安全多方计算装置的结构示意图;本申请实施例提供了一种安全多方计算装置200,包括:

[0050] 语句序列获取模块210,用于获取逻辑语句序列,从逻辑语句序列中的每个逻辑语句中解析出操作指令和操作数。

[0051] 关联列表获取模块220,用于对每个逻辑语句对应的操作数进行分析,获得每个逻辑语句对应的关联方标识列表。

[0052] 数据碎片获得模块230,用于对每个逻辑语句对应的操作数进行分片,获得分片后的数据碎片,并查找到关联方标识列表对应的关联执行节点。

[0053] 数据碎片发送模块240,用于向关联方标识列表对应的关联执行节点发送操作指令和分片后的数据碎片,以使关联方标识列表对应的关联执行节点根据操作指令对分片后的数据碎片进行安全多方计算。

[0054] 可选地,在本申请实施例中,操作数包括:输入数据和中间数据;关联列表获取模块,包括:

[0055] 关联标识获取模块，用于获取输入数据的关联方标识和中间数据的历史数据关联方标识。

[0056] 关联标识合并模块，用于将输入数据的关联方标识和中间数据的历史数据关联方标识进行合并，获得每个逻辑语句对应的关联方标识列表。

[0057] 可选地，在本申请实施例中，数据碎片获得模块，包括：

[0058] 输入数据分片模块，用于对输入数据进行分片，获得输入数据的数据碎片。

[0059] 中间数据分片模块，用于对中间数据进行重新分片，获得中间数据的数据碎片。

[0060] 数据碎片合并模块，用于将输入数据的数据碎片与中间数据的数据碎片进行合并，获得分片后的数据碎片。

[0061] 可选地，在本申请实施例中，语句序列获取模块，包括：

[0062] 源代码编译模块，用于获取源代码，对源代码进行编译，获得逻辑语句序列。

[0063] 可选地，在本申请实施例中，数据碎片获得模块，还包括：

[0064] 服务器标识查找模块，用于在数据库中查找关联方标识列表中的每个关联方标识对应的至少一个服务器标识，获得多个服务器标识，数据库中存储有关联方标识与服务器标识的对应关系。

[0065] 执行节点确定模块，用于将多个服务器标识对应的服务器节点确定为关联执行节点。

[0066] 应理解的是，该装置与上述的安全多方计算方法实施例对应，能够执行上述方法实施例涉及的各个步骤，该装置具体的功能可以参见上文中的描述，为避免重复，此处适当省略详细描述。该装置包括至少一个能以软件或固件(firmware)的形式存储于存储器中或固化在装置的操作系统(operating system,OS)中的软件功能模块。

[0067] 请参见图4示出的本申请实施例提供的电子设备的结构示意图。本申请实施例提供的一种电子设备300，包括：处理器310和存储器320，存储器320存储有处理器310可执行的机器可读指令，机器可读指令被处理器310执行时执行如上的方法。

[0068] 本申请实施例还提供了一种计算机可读存储介质330，该计算机可读存储介质330上存储有计算机程序，该计算机程序被处理器310运行时执行如上的方法。

[0069] 其中，计算机可读存储介质330可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器(Static Random Access Memory, 简称SRAM)，电可擦除可编程只读存储器(Electrically Erasable Programmable Read-Only Memory, 简称EEPROM)，可擦除可编程只读存储器(Erasable Programmable Read Only Memory, 简称EPROM)，可编程只读存储器(Programmable Read-Only Memory, 简称PROM)，只读存储器(Read-Only Memory, 简称ROM)，磁存储器，快闪存储器，磁盘或光盘。

[0070] 本申请实施例提供的几个实施例中，应该理解到，所揭露的装置和方法，也可以通过其他的方式实现。以上所描述的装置实施例仅是示意性的，例如，附图中的流程图和框图显示了根据本申请实施例的多个实施例的装置、方法和计算机程序产品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、程序段或代码的一部分，模块、程序段或代码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。也应当注意，在有些作为替换的实现方式中，方框中所标注的功能也可以和附图中所标注的发生顺序不同。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，这主要根据所涉及的功能而定。

[0071] 另外，在本申请实施例中的各个实施例的各功能模块可以集成在一起形成一个独立的部分，也可以是各个模块单独存在，也可以两个或两个以上模块集成形成一个独立的部分。此外，在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本申请实施例的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0072] 在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。

[0073] 以上的描述，仅为本申请实施例的可选实施方式，但本申请实施例的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请实施例揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请实施例的保护范围之内。

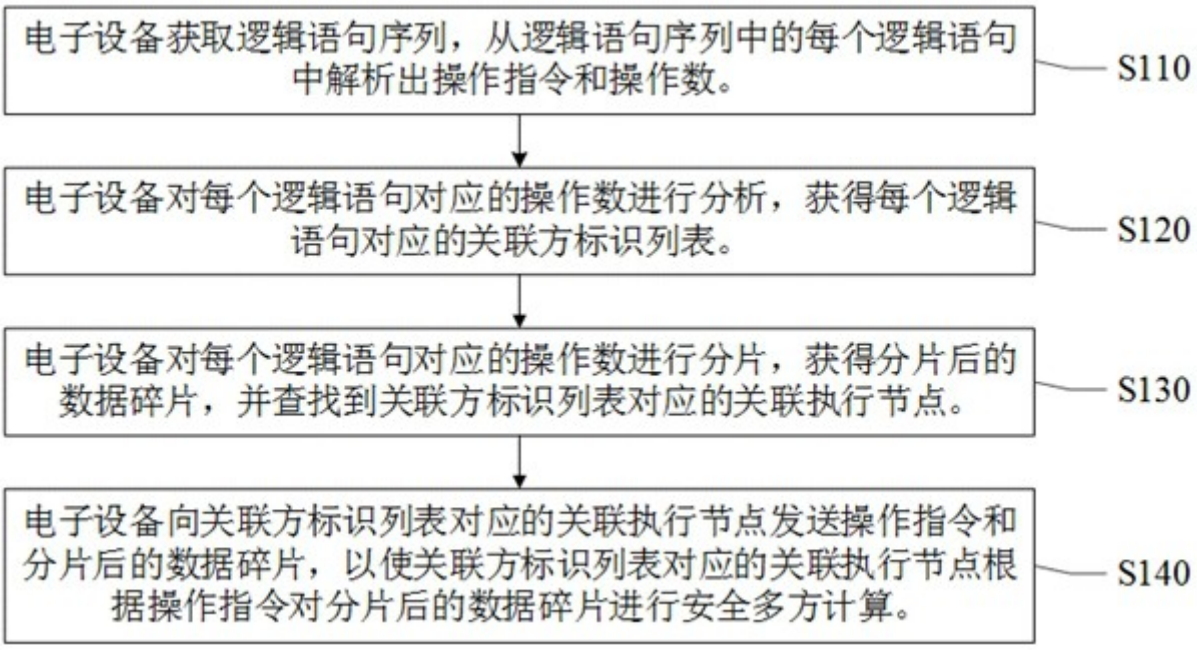

电子设备获取逻辑语句序列，从逻辑语句序列中的每个逻辑语句中解析出操作指令和操作数。
S110
电子设备对每个逻辑语句对应的操作数进行分析，获得每个逻辑语句对应的关联方标识列表。
S120
电子设备对每个逻辑语句对应的操作数进行分片，获得分片后的数据碎片，并查找到关联方标识列表对应的关联执行节点。
S130
电子设备向关联方标识列表对应的关联执行节点发送操作指令和分片后的数据碎片，以使关联方标识列表对应的关联执行节点根据操作指令对分片后的数据碎片进行安全多方计算。
S140

图1

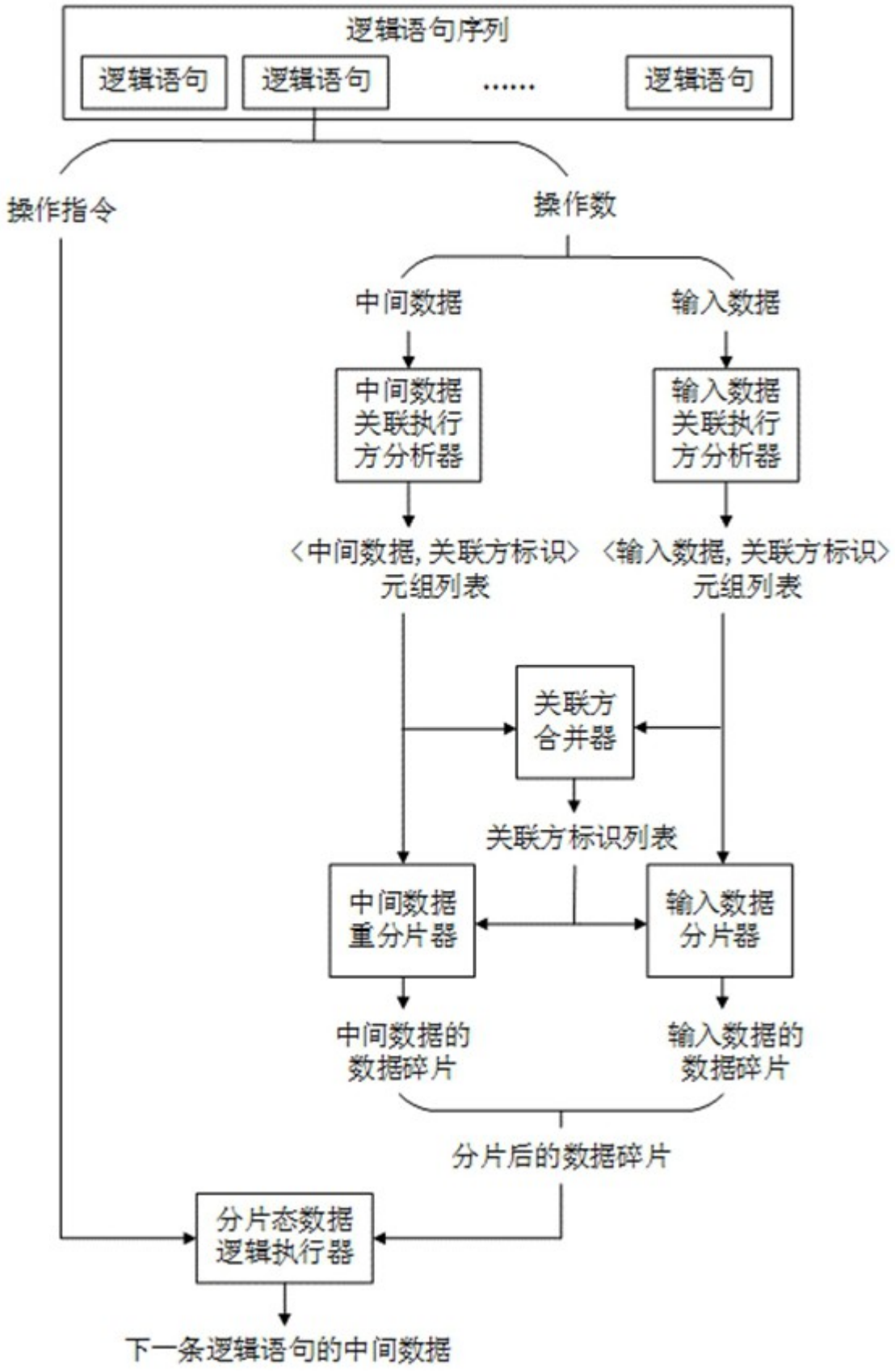

逻辑语句序列
逻辑语句
逻辑语句
.....
逻辑语句
操作指令
操作数
中间数据
输入数据
中间数据关联执行方分析器
输入数据关联执行方分析器
〈中间数据,关联方标识〉元组列表
〈输入数据,关联方标识〉元组列表
关联方合并器
关联方标识列表
中间数据重分片器
输入数据分片器
中间数据的数据碎片
输入数据的数据碎片
分片后的数据碎片
分片态数据逻辑执行器
下一条逻辑语句的中间数据

图2

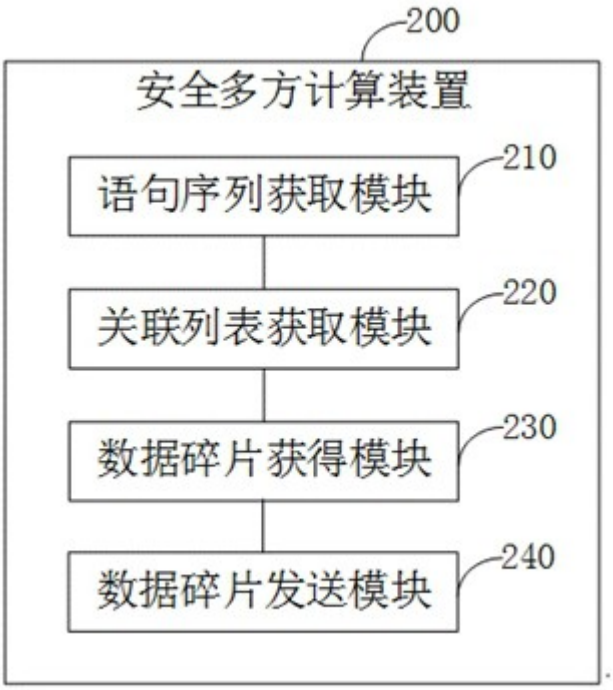

200
安全多方计算装置
语句序列获取模块
210
关联列表获取模块
220
数据碎片获得模块
230
数据碎片发送模块
240

图3

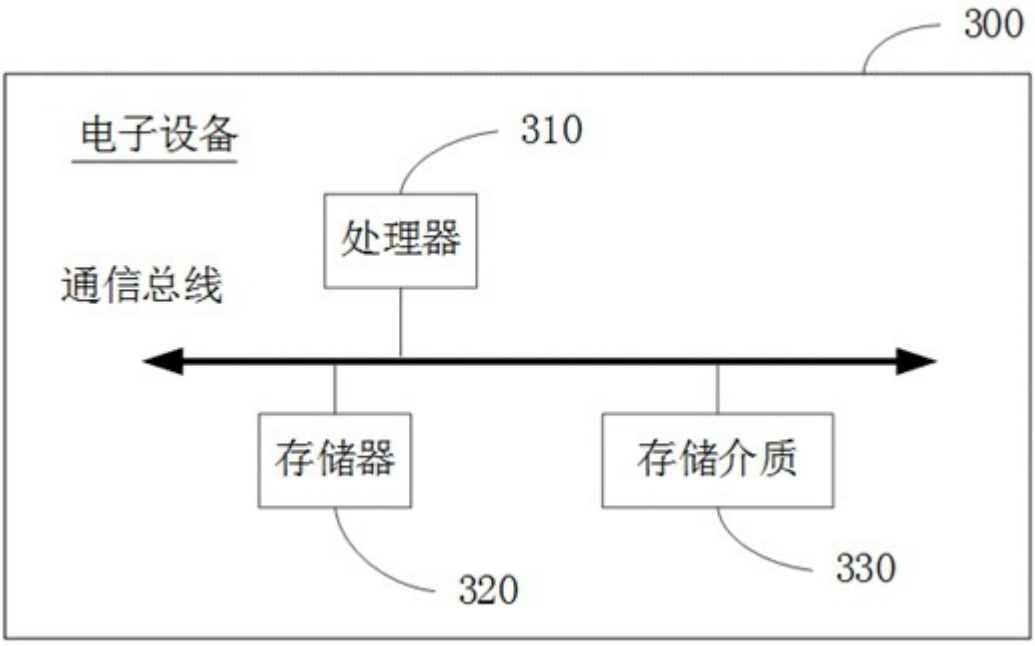

300
电子设备
310
处理器
通信总线
存储器
存储介质
320
330

图4