

多方安全计算

技术领域

[01] 本说明书一个或多个实施例涉及电子信息技术, 尤其涉及多方安全计算方法和装置。

背景技术

[02] 多方安全计算能够在不泄露各数据拥有方的原始数据的前提下, 各数据拥有方分别提供各自的原始数据, 按照约定的基础算法进行计算, 并将计算的最终结果发送给数据需求方。

[03] 相关技术中, 提供原始数据的数据拥有方不管数量为几个, 数据拥有方均作为计算参与方进行多方安全计算, 该方式计算效率较低。因此, 希望提供一种能够较高计算效率的多方安全计算方案。

发明内容

[04] 本说明书一个或多个实施例描述了多方安全计算方法和装置, 以提高多方安全计算的计算效率。

[05] 根据第一方面, 提供了一种多方安全计算方法, 该方法对 N 个数据拥有方的原始数据进行计算, 应用于 TEE 节点中, 包括: 根据数据拥有方的数量 N , 加入包括 K 个 TEE 节点的 TEE 节点集群; 创建可信执行环境, 并将进行 K 方安全计算的基础算法加载到可信执行环境中; 在可信执行环境中获取至少一个数据分片, 所述数据分片包括: 由数据拥有方对拥有的原始数据进行拆分后得到并发给该 TEE 节点的, 或者由 TEE 节点集群中的其他 TEE 节点对数据拥有方发来的拆分后的原始数据进行计算后得到并发给该 TEE 节点的; 利用所述 K 方安全计算的基础算法以及获取到的数据分片, 进行 K 方安全计算; 其中, N 为大于 1 的正整数; K 为大于 1 的正整数。

[06] 在一个实施例中, 所述 K 方安全计算的基础算法的计算速度比 N 方安全计算的基础算法的计算速度更快。

[07] 在一个实施例中, TEE 节点集群中的 K 个 TEE 节点通过同一个局域网执行所述 K 方安全计算。

[08] 在一个实施例中, 在所述数据分片是由数据拥有方对拥有的原始数据进行拆分后得

到并发给该 TEE 节点时,在可信执行环境中获取至少一个数据分片之前,进一步包括:在可信执行环境中生成公私钥对;其中,该 TEE 节点生成的公私钥对与所述 TEE 节点集群中其他 TEE 节点生成的公私钥对不同;将生成的公私钥对中的公钥分别发送给数据拥有方,并接收对称密钥加密信息;该对称密钥加密信息是由数据拥有方利用该 TEE 节点发送的公钥,对生成的对称密钥进行加密后得到并发来的;在可信执行环境中获取至少一个数据分片,包括:在可信执行环境中接收数据拥有方发来的数据分片,利用生成的公私钥对中的私钥从该数据拥有方发来的对称密钥加密信息中解密出对称密钥,并利用解密出的该对称密钥对该数据拥有方发来的数据分片进行解密,得到解密后的数据分片。

[09]在一个实施例中,在 N 不小于 K 时,所述 TEE 节点集群中的 K 个 TEE 节点是从 N 个数据拥有方中选择出,并对选择出的 K 个数据拥有方加载 TEE 功能后得到的。

[10]在一个实施例中,所述 K 为 3。

[11]第二方面,本说明书实施例还提供了一种多方安全计算装置,该装置用于实现对 N 个数据拥有方的原始数据进行计算,该装置位于 TEE 节点中,包括:创建单元,被配置为根据数据拥有方的数量 N ,加入包括 K 个 TEE 节点的 TEE 节点集群;以及创建可信执行环境,并将进行 K 方安全计算的基础算法加载到可信执行环境中;数据分片获取单元,被配置为在可信执行环境中获取至少一个数据分片,所述数据分片包括:由数据拥有方对拥有的原始数据进行拆分后得到并发给该 TEE 节点的,或者由 TEE 节点集群中的其他 TEE 节点对数据拥有方发来的拆分后的原始数据进行计算后得到并发给该 TEE 节点的;计算单元,被配置为利用所述 K 方安全计算的基础算法以及获取到的数据分片,进行 K 方安全计算;其中, N 为大于 1 的正整数; K 为大于 1 的正整数。

[12]在一个实施例中,所述 K 方安全计算的基础算法的计算速度比 N 方安全计算的基础算法的计算速度更快。

[13]在一个实施例中,TEE 节点集群中的 K 个 TEE 节点通过同一个局域网执行所述 K 方安全计算。

[14]在一个实施例中,进一步包括:公私钥对生成单元,被配置为在所述数据分片是由数据拥有方对拥有的原始数据进行拆分后得到并发给该 TEE 节点时,在可信执行环境中生成公私钥对;其中,该 TEE 节点生成的公私钥对与所述 TEE 节点集群中其他 TEE 节点生成的公私钥对不同;将生成的公私钥对中的公钥分别发送给数据拥有方,并接收

对称密钥加密信息;该对称密钥加密信息是由数据拥有方利用该 TEE 节点发送的公钥,对生成的对称密钥进行加密后得到并发来的;所述数据分片获取单元,被配置为在可信执行环境中接收数据拥有方发来的数据分片,利用生成的公私钥对中的私钥从该数据拥有方发来的对称密钥加密信息中解密出对称密钥,并利用解密出的该对称密钥对该数据拥有方发来的数据分片进行解密,得到解密后的数据分片。

[15]在一个实施例中,在 N 不小于 K 时,所述 TEE 节点集群中的 K 个 TEE 节点是从 N 个数据拥有方中选择出,并对选择出的 K 个数据拥有方加载 TEE 功能后得到的。

[16]在一个实施例中,所述 K 为 3。

[17]根据第三方面,提供了一种计算设备,包括存储器和处理器,所述存储器中存储有可执行代码,所述处理器执行所述可执行代码时,实现本说明书任一实施例所述的方法。

[18]在本说明书实施例提供的多方安全计算方法和装置,根据数据拥有方的数量 N ,加入包括 K 个 TEE 节点的 TEE 节点集群,TEE 节点集群中的 TEE 节点创建可信执行环境,并将进行 K 方安全计算的基础算法加载到可信执行环境中,TEE 节点集群中的 TEE 节点在可信执行环境中获取至少一个数据分片,TEE 节点集群利用 K 方安全计算的基础算法以及获取到的数据分片,进行 K 方安全计算。由于基础算法和数据分片均是在 TEE 节点的可信执行环境中的,因此,可以确保 TEE 节点可信, N 个数据拥有方可以放心由该 K 个 TEE 节点对 N 个数据拥有方的原始数据进行多方安全计算。另外,由于 TEE 节点集群中 TEE 节点的数量是可控的,使得在数据拥有方的数量 N 是固定时,可以选择效率更高的基础算法进行多方安全计算,从而提高进行多方安全计算的计算效率。

附图说明

[19]为了更清楚地说明本说明书实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图是本说明书的一些实施例,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的附图。

[20]图 1 是本说明书一个实施例提供的系统架构的示意图;

[21]图 2 是本说明书一个实施例提供的多方安全计算方法的流程图;

[22]图 3 是本说明书一个实施例中多方安全计算装置的示意图;

[23]图 4 是本说明书另一个实施例中多方安全计算装置的示意图。

具体实施方式

[24]下面结合附图，对本说明书提供的方案进行描述。

[25]相关技术中，在进行多方安全计算的数据拥有方数量不同时，进行多方安全计算的基础算法会不同，使用不同的基础算法进行多方安全计算时对应的计算效率也会不同。在需要进行多方安全计算的数据拥有方的数量 N 确定之后，可以根据数据拥有方的数量 N 确定所需使用的进行 N 方安全计算的基础算法，并利用该 N 方安全计算的基础算法对 N 个数据拥有方的原始数据进行 N 方安全计算。由于数据拥有方的数量 N 是固定的，那么对应的基础算法也是确定的。如果该数据拥有方的数量 N 所对应的基础算法非常复杂，在利用该基础算法进行 N 方安全计算时计算效率较低，那么必定会影响得到 N 方安全计算结果的效率。

[26]为了提高对 N 个数据拥有方的原始数据进行多方安全计算的计算效率，可以考虑变换进行多方安全计算的计算参与方的数量，而对于变换后计算参与方的数量是多少，可以根据基础算法所对应的计算效率来确定计算参与方的数量，例如，选择效率更高的基础算法，该效率更高的基础算法对应的计算参与方的数量为 3，那么变换后计算参与方的数量为 3，即利用 3 个计算参与方对 N 个数据拥有方的原始数据进行三方安全计算。

[27]下面描述以上构思的具体实现方式。

[28]为了方便对本说明书的理解，首先对本说明书所应用的系统架构进行描述。如图 1 中所示，该系统架构主要包括： N 个数据拥有方和由 K 个 TEE 节点组成的 TEE 节点集群。其中， N 、 K 均为大于 1 的正整数。

[29]数据拥有方是提供原始数据的一方。在 N 个数据拥有方需要提供原始数据用于进行多方安全计算，将 N 个数据拥有方提供的原始数据转嫁到 TEE 节点集群中的 TEE 节点上，由 K 个 TEE 节点利用 N 个数据拥有方提供的原始数据进行 K 方安全计算。

[30]下面描述该多方安全计算方法的具体实现过程。

[31]图 2 示出根据一个实施例的多方安全计算方法的流程图。可以理解，该方法可以通过任何具有计算、处理能力的装置、设备、平台、设备集群来执行。参见图 2，该方法对 N 个数据拥有方的原始数据进行计算，应用于 TEE 节点中；此后，具体的实现包括：步骤 200：根据数据拥有方的数量 N ，加入包括 K 个 TEE 节点的 TEE 节点集群；其中， N 为大于 1 的正整数； K 为大于 1 的正整数。

[32] 步骤 202: 创建可信执行环境, 并将进行 K 方安全计算的基础算法加载到可信执行环境中。

[33] 步骤 204: 在可信执行环境中获取至少一个数据分片, 所述数据分片包括: 由数据拥有方对拥有的原始数据进行拆分后得到并发给该 TEE 节点的, 或者由 TEE 节点集群中的其他 TEE 节点对数据拥有方发来的拆分后的原始数据进行计算后得到并发给该 TEE 节点的。

[34] 步骤 206: 利用所述 K 方安全计算的基础算法以及获取到的数据分片, 进行 K 方安全计算。

[35] 在图 2 所示的多方安全计算方法中, 由于基础算法和数据分片均是在 TEE 节点的可信执行环境中的, 因此, 可以确保 TEE 节点可信, N 个数据拥有方可以放心由该 K 个 TEE 节点对 N 个数据拥有方的原始数据进行多方安全计算, 且对 TEE 集群进行 K 方安全计算得到的计算结果是信任的。另外, 由于 TEE 节点集群中 TEE 节点的数量是可控的, 使得在数据拥有方的数量 N 是固定时, 可以选择效率更高的基础算法进行多方安全计算, 从而提高进行多方安全计算的计算效率。

[36] 下面描述各步骤的实现过程。

[37] 在步骤 200 中, 根据数据拥有方的数量 N, 加入包括 K 个 TEE 节点的 TEE 节点集群。其中, N 为大于 1 的正整数; K 为大于 1 的正整数。

[38] 如果只需要一个数据拥有方提供原始数据进行计算, 那么就不需要使用多方安全计算方法, 因此, 需要使用多方安全计算方法进行计算时, 对应的数据拥有方的数量 N 肯定为大于 1 的正整数。

[39] TEE 节点是具有 TEE 功能的服务器, 该 TEE 功能的服务器可以保证数据是保密且不可篡改的, 但是如果攻击者对 TEE 节点进行物理拆卸, 在攻击者付出足够大的成本的情况下, 依然可以截取到该需要保密的数据。存在单个 TEE 节点被攻破的情况, 但两个 TEE 节点被同时攻破的概率极低, 因此, 进行 K 方安全计算的 TEE 节点的数量 K 也需要是大于 1 的正整数。

[40] 数据拥有方是提供原始数据的一方。该原始数据可以是参与计算的数据, 也可以是参与计算的模型。且各数据拥有方均不希望自己拥有的数据或模型被其他数据拥有方获知到。例如, 在进行某些数据的预测时, 需要利用五个数据拥有方分别拥有的原始数据, 才能够得到预测结果, 其中, 一个数据拥有方提供预测模型, 另外四个数据拥有方提供

用于输入到预测模型中的数据，而预测模型以及数据都属于数据拥有方各自的隐私数据，各数据拥有方不希望其他数据拥有方获知到自己的预测模型或者自己的数据。因此，可以利用多方安全计算来实现结果的预测，而不会泄露各数据拥有方各自拥有的原始数据。

[41]在本说明书实施例中，TEE 节点集群中 TEE 节点的数量 K 可以根据数据拥有方的数量 N 来确定。依据可以是 K 方安全计算的基础算法的计算速度比 N 方安全计算的基础算法的计算速度更快。

[42]例如，在 N 为 10 时，由于多方安全计算在计算过程中存在计算参与方之间频繁的数据交互，在进行多方安全计算的计算参与方的数量越多，交互过程就越多，那么通信开销就越大，计算速度也就越慢。因此，可以选择数量比 N 少的 TEE 节点来进行多方安全计算，比如， K 为 7， K 为 4 等，通过降低通信开销，提高多方安全计算的计算速度。

[43]随着对多方安全计算的基础算法的研究，在进行多方安全计算的计算参与方的数量为一些特殊数量时，可以使用计算速度更快的基础算法，比如，在进行多方安全计算的计算参与方的数量为 3 时，三方安全计算的基础算法速度更快。那么，优选地， K 等于 3。

[44]在本说明书实施例中，当数量 K 的选择为计算速度更快的基础算法所对应的数量时，例如，该数量 K 等于 3，那么 N 与 K 之间包括如下两种关系：关系一、 N 不等于 K ；关系二、 N 等于 K 。

[45]在 N 与 K 之间为关系一时，数据拥有方的数量 N 无论为多少时，例如， N 等于 2，再如， N 等于 5，都可以将 N 个数据拥有方的原始数据转嫁到三个 TEE 节点中进行三方安全计算。由于三方安全计算的基础算法的计算速度是相对于其他数量的多方安全计算的基础算法的计算速度更快，因此，通过将创建三个 TEE 节点的 TEE 节点集群，以进行三方安全计算，从而可以相对于 N 方安全计算的计算速度更快。

[46]在 N 与 K 之间为关系二时，即 $N=K=3$ ，此时，为了提高三方安全计算的计算速度，在本说明书实施例中，可以将 TEE 节点集群中的三个 TEE 节点设置在同一个局域网中，以提高计算速度。

[47]可以理解， N 个数据拥有方一般属于不同的机构组织，这些机构组织之间通过公网进行数据交互，而通过公网进行数据交互时，交互速度较慢，一般通过公网交互一次数据可能需要几百毫秒的时长。而进行多方安全计算时，需要多个计算参与方之间进行频

繁的数据交互，导致多方安全计算的计算速度较慢。在本说明书实施例中，通过局域网进行数据交互时，交互一次数据可能只需要几毫秒的时长，多个计算参与方在进行频繁的数据交互过程中，可以提高多方安全计算的计算速度。

[48]优选地，无论N与K之间的关系对应何种关系，在本说明书实施例中，TEE节点集群中的K个TEE节点通过同一个局域网进行K方安全计算。

[49]其中，在实现将K个TEE节点通过同一个局域网进行K方安全计算时，可以通过云平台的方式来实现。即利用云平台提供多个TEE节点的租用，在根据数量N确定了TEE节点的数量K之后，从云平台上租用K个TEE节点，由于该云平台上的多个TEE节点均位于同一个局域网中，因此，租用的K个TEE节点位于同一个局域网中，从而可以通过同一个局域网进行K方安全计算。

[50]在本说明书一个实施例中，在N不小于K时，所述TEE节点集群中的K个TEE节点是从N个数据拥有方中选择出，并对选择出的K个数据拥有方加载TEE功能后得到的。例如，数据拥有方的数量为5个，TEE节点的数量K为3个，那么可以从5个数据拥有方中选择3个数据拥有方，在该3个数据拥有方中加载TEE功能后将其作为TEE节点集群中的3个TEE节点。其中，需要保证选择的K个数据拥有方被N个数据拥有方信任。

[51]在步骤202中，创建可信执行环境，并将进行K方安全计算的基础算法加载到可信执行环境中。

[52]TEE基于可信硬件，是CPU上的一块独立的安全区域，它运行在一个独立的环境中且与操作系统并行运行。CPU确保TEE中数据和基础算法的机密性和完整性都得到保护。通过同时使用硬件和软件来保护数据和基础算法，TEE比操作系统更加安全。在TEE中运行的受信任应用程序可以访问设备主处理器和内存的全部功能，而硬件隔离保护这些组件不受主操作系统中运行的用户安装应用程序的影响。总结来说，运行在TEE中的数据 and 基础算法，是保密且不可篡改的。

[53]在本说明书一个实施例中，可信执行环境可以基于英特尔的SGX技术来实现。在实现时，每一个TEE节点可以基于SGX技术创建enclave(围圈或飞地)容器，创建的enclave容器驻留在一个被保护的物理内存区域EPC(enclave page cache)中，该enclave容器即为创建的可信执行环境。

[54]在本说明书实施例中，TEE节点在创建了可信执行环境之后，需要针对该可信执行

环境向第三方的 TEE 认证服务器进行远程认证。

[55]在 TEE 节点进行远程认证时, TEE 节点会根据创建的可信执行环境进行度量, 并根据度量结果产生一个远程认证请求发送给 TEE 认证服务器, TEE 认证服务器根据该远程认证请求, 对该 TEE 节点的可信执行环境进行验证, 以验证该可信执行环境是否合理可信。若验证合理可信, 则确定认证通过, 否则确定认证不通过。此时会生成一个认证报告, 该认证报告中包括是否通过的认证结果。另外, TEE 认证服务器对该认证报告进行签名以防止 TEE 节点对认证报告进行篡改, 并将签名后的认证报告发送给 TEE 节点。

[56]进一步地, TEE 节点在接收到该签名后的认证报告后, 将该签名的认证报告发送给每一个数据拥有方, 以使数据拥有方根据该签名的认证报告中的认证结果确定该 TEE 节点是否可信。其中, K 个 TEE 节点分别向 TEE 认证服务器进行认证, 得到 K 个认证报告。只有在 K 个认证报告的认证结果均为认证通过时, 数据拥有方才确认该 K 个 TEE 节点组成的 TEE 节点集群可信, 才会确认使用该 K 个 TEE 节点对自身拥有的原始数据进行 K 方安全计算。

[57]在本说明书实施例中, K 方安全计算的基础算法的获取方式至少可以包括以下三种:

[58]第一种, 由云平台的拥有者提供。

[59]第二种, 由数据拥有方提供。

[60]第三种, 从可信第三方处抓取。

[61]其中, 该基础算法由代码来实现, TEE 节点集群中的 TEE 节点将进行 K 方安全计算的基础算法加载到可信执行环境中之后, 在进行多方安全计算时, 需要按照基础算法执行计算过程。并且, 在基础算法记载到可信执行环境中之后, 该基础算法不能被篡改, 从而可以保证 TEE 节点是按照加载的基础算法进行多方安全计算的, 使得数据拥有方对 TEE 节点的可信, 以及对计算结果的信任。

[62]N 个数据拥有方在根据认证报告确定 TEE 节点的可信执行环境是可信的之后, 还需要对每个 TEE 节点加载到可信执行环境中的基础算法进行验证。该验证方式可以是由每一个 TEE 节点针对自身加载的基础算法计算出一个哈希值, 将计算出的哈希值发送给每一个数据拥有方, 数据拥有方根据哈希值确定该 TEE 节点加载的基础算法是否为所需的基础算法, 如果是, 则对基础算法的验证通过。

[63]在步骤 204 中, 在可信执行环境中获取至少一个数据分片, 该数据分片包括: 由数

据拥有方对拥有的原始数据进行拆分后得到并发给该 TEE 节点的，或者由 TEE 节点集群中的其他 TEE 节点对数据拥有方发来的拆分后的原始数据进行计算后得到并发给该 TEE 节点的。

[64]在本说明书实施例中，每一个 TEE 节点在可信执行环境中获取到的至少一个数据分片，可以由数据拥有方对拥有的原始数据进行拆分后得到并直接发给该 TEE 节点的，也可以是由 TEE 节点集群中的其他 TEE 节点对数据拥有方发来的拆分后的原始数据进行计算后得到并发给该 TEE 节点的。

[65]例如，数据拥有方的数量 N 等于 4，即数据拥有方 A、B、C 和 D，TEE 节点的数量 K 等于 3，即 TEE 节点 E、F 和 G。数据拥有方 A 将自身的原始数据拆分成两份数据分片，分别发送给 TEE 节点 E、F，TEE 节点 E、F 在对数据分片进行中间计算后，将中间计算结果发送给 TEE 节点 G。

[66]需要说明的是，每一个数据拥有方对各自原始数据进行拆分的份数可以相同，也可以不相同。但每一个数据拥有方对各自原始数据进行拆分的份数至少为两份。

[67]在本说明书实施例中，为了提高数据分片在由数据拥有方发送给 TEE 节点时传输过程中的安全性，在所述数据分片是由数据拥有方对拥有的原始数据进行拆分后得到并发给该 TEE 节点时，在步骤 204 之前，可以进一步包括：在可信执行环境中生成公私钥对；其中，该 TEE 节点生成的公私钥对与所述 TEE 节点集群中其他 TEE 节点生成的公私钥对不同；将生成的公私钥对中的公钥分别发送给数据拥有方，并接收对称密钥加密信息；该对称密钥加密信息是由数据拥有方利用该 TEE 节点发送的公钥，对生成的对称密钥进行加密后得到并发来的。

[68]那么相应地，在步骤 204 中，包括：在可信执行环境中接收数据拥有方发来的数据分片，利用生成的公私钥对中的私钥从该数据拥有方发来的对称密钥加密信息中解密出对称密钥，并利用解密出的该对称密钥对该数据拥有方发来的数据分片进行解密，得到解密后的数据分片。

[69]在本说明书一个实施例中，TEE 节点可以与数据拥有方之间可以建立长连接，以在建立了长连接之后 TEE 节点与数据拥有方在进行数据传输时，以加密方式进行数据的传输，从而可以保障数据在传输过程中的安全性。

[70]以数据拥有方的数量为 4 个，TEE 节点的数量为 3 个为例，对本步骤进行说明。

[71]数据拥有方分别为 A、B、C 和 D，TEE 节点分别为 E、F 和 G。各 TEE 节点分别

对应公钥 e、f、g，TEE 节点 E 将公钥 e 发送给数据拥有方 A、B、C 和 D，TEE 节点 F 将公钥 f 发送给数据拥有方 A、B、C 和 D，TEE 节点 G 将公钥 g 发送给数据拥有方 A、B、C 和 D。

[72] 数据拥有方 A 将原始数据拆分成数据分片 A1 和 A2，其中，A1 用于发送给 TEE 节点 E，A2 用于发送给 TEE 节点 F。数据拥有方 A 生成分别对应于 TEE 节点 E、F 的对称密钥 a1、a2，利用 TEE 节点 E 对应的公钥 e 对对称密钥 a1 进行加密，得到对称密钥加密信息 a10，利用 TEE 节点 F 对应的公钥 f 对对称密钥 a2 进行加密，得到对称密钥加密信息 a20；并将对称密钥加密信息 a10、对称密钥加密信息 a20 分别发送给 TEE 节点 E、F。

[73] 数据拥有方 A 利用对称密钥 a1 对数据分片 A1 进行加密，利用对称密钥 a2 对数据分片 A2 进行加密，并将加密后的数据分片 A1、A2，分别发送给 TEE 节点 E、F。

[74] 相应地，TEE 节点 E 接收到数据拥有方 A 发来的加密后的数据分片 A1 和对称密钥加密信息 a10。TEE 节点 E 利用公私钥对中的私钥解密出对称密钥 a1，并利用对称密钥 a1 解密出数据分片 A1。其他加密解密过程与该加密解密过程同理，在此不再赘述。

[75] 其中，该对称密钥可以是生成的随机数。

[76] 在本说明书一个实施例中，接收到的该数据分片为密文数据，可以是数据拥有方使用秘密共享、混淆电路等技术生成的，该数据分片可以是密码学分片，也可以是随机数分片。由于该数据分片是密文数据，因此，TEE 节点均无法根据数据拥有方发送的数据分片获知到原始数据，从而可以进一步保障数据的隐私性。

[77] 在步骤 206 中，利用所述 K 方安全计算的基础算法以及获取到的数据分片，进行 K 方安全计算。

[78] 在本说明书实施例中，该 TEE 节点可以是一个服务器，也可以是服务器组。在 TEE 节点是服务器组时，TEE 节点在获取到数据分片之后，可以将数据分片分配给服务器组内的其他服务器，服务器组对获取到的数据分片进行并计算，可以提高数据处理的吞吐量，从而在整体上提高计算速度。

[79] TEE 节点集群中的各 TEE 节点按照各自加载的基础算法执行计算过程，且在计算过程中，各 TEE 节点之间需要频繁的交互中间结算结果。

[80] 为了得到最终的计算结果，在本说明书实施例中，可以根据指定一个 TEE 节点或两个以上的 TEE 节点完成最终结果的提取。例如，在指定一个 TEE 节点完成最终结果的

提取时，其他 TEE 节点将中间计算结果发送给该指定的 TEE 节点，由该指定的 TEE 节点根据各 TEE 节点的中间计算结果提取出最终的结果。

[81]在本说明书实施例中，在 TEE 节点集群中的 TEE 节点获取到 K 方安全计算的结果之后，将该 K 方安全计算的结果发送给数据需求方。其中，该数据需求方可以是 N 个数据拥有方中的一个或者多个，也可以是数据拥有方以外的其他方。

[82]另一方面的实施例，还提供了一种多方安全计算装置，该装置用于实现对 N 个数据拥有方的原始数据进行计算，该装置位于 TEE 节点中。如图 3 示出一个实施例的多方安全计算装置。可以理解，该装置可以通过任何具有计算、处理能力的装置、设备、平台和设备集群来实现。如图 3 所示，该装置 30 包括：创建单元 31，被配置为根据数据拥有方的数量 N，加入包括 K 个 TEE 节点的 TEE 节点集群；以及创建可信执行环境，并将进行 K 方安全计算的基础算法加载到可信执行环境中；数据分片获取单元 32，被配置为在可信执行环境中获取至少一个数据分片，所述数据分片包括：由数据拥有方对拥有的原始数据进行拆分后得到并发给该 TEE 节点的，或者由 TEE 节点集群中的其他 TEE 节点对数据拥有方发来的拆分后的原始数据进行计算后得到并发给该 TEE 节点的；计算单元 33，被配置为利用所述 K 方安全计算的基础算法以及获取到的数据分片，进行 K 方安全计算；其中，N 为大于 1 的正整数；K 为大于 1 的正整数。

[83]一个可能的实现方式中，所述 K 方安全计算的基础算法的计算速度比 N 方安全计算的基础算法的计算速度更快。

[84]一个可能的实现方式中，TEE 节点集群中的 K 个 TEE 节点通过同一个局域网执行所述 K 方安全计算。

[85]一个可能的实现方式中，请参考图 4，该装置 30 可以进一步包括：公私钥对生成单元 34，被配置为在所述数据分片是由数据拥有方对拥有的原始数据进行拆分后得到并发给该 TEE 节点时，在可信执行环境中生成公私钥对；其中，该 TEE 节点生成的公私钥对与所述 TEE 节点集群中其他 TEE 节点生成的公私钥对不同；将生成的公私钥对中的公钥分别发送给数据拥有方，并接收对称密钥加密信息；该对称密钥加密信息是由数据拥有方利用该 TEE 节点发送的公钥，对生成的对称密钥进行加密后得到并发来的；所述数据分片获取单元 32，被配置为在可信执行环境中接收数据拥有方发来的数据分片，利用生成的公私钥对中的私钥从该数据拥有方发来的对称密钥加密信息中解密出对称密钥，并利用解密出的该对称密钥对该数据拥有方发来的数据分片进行解密，得到解密后的数据分片。

[86]一个可能的实现方式中，在 N 不小于 K 时，所述 TEE 节点集群中的 K 个 TEE 节点是从 N 个数据拥有方中选择出，并对选择出的 K 个数据拥有方加载 TEE 功能后得到的。

[87]一个可能的实现方式中，所述 K 为 3。

[88]本说明书一个实施例提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现执行说明书中任一实施例中的方法。

[89]可以理解的是，本说明书实施例示意的结构并不构成对多方安全计算装置的具体限定。在说明书的另一些实施例中，多方安全计算装置可以包括比图示更多或者更少的部件，或者组合某些部件，或者拆分某些部件，或者不同的部件布置。图示的部件可以以硬件、软件或者软件和硬件的组合来实现。

[90]上述装置、系统内的各模块之间的信息交互、执行过程等内容，由于与本说明书方法实施例基于同一构思，具体内容可参见本说明书方法实施例中的叙述，此处不再赘述。

[91]本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[92]本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、挂件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

[93]以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

权利要求书

1、多方安全计算方法，应用于 TEE 节点中，包括：

根据数据拥有方的数量 N，加入包括 K 个 TEE 节点的 TEE 节点集群；

创建可信执行环境，并将进行 K 方安全计算的基础算法加载到可信执行环境中；

在可信执行环境中获取至少一个数据分片，所述数据分片包括：由数据拥有方对拥有的原始数据进行拆分后得到并发给该 TEE 节点的，或者由 TEE 节点集群中的其他 TEE 节点对数据拥有方发来的拆分后的原始数据进行计算后得到并发给该 TEE 节点的；

利用所述 K 方安全计算的基础算法以及获取到的数据分片，进行 K 方安全计算；

其中，N 为大于 1 的正整数；K 为大于 1 的正整数。

2、根据权利要求 1 所述的方法，其中，所述 K 方安全计算的基础算法的计算速度比 N 方安全计算的基础算法的计算速度更快。

3、根据权利要求 1 所述的方法，其中，TEE 节点集群中的 K 个 TEE 节点通过同一个局域网执行所述 K 方安全计算。

4、根据权利要求 3 所述的方法，在所述数据分片是由数据拥有方对拥有的原始数据进行拆分后得到并发给该 TEE 节点时，

在可信执行环境中获取至少一个数据分片之前，进一步包括：

在可信执行环境中生成公私钥对；其中，该 TEE 节点生成的公私钥对与所述 TEE 节点集群中其他 TEE 节点生成的公私钥对不同；

将生成的公私钥对中的公钥分别发送给数据拥有方，并接收对称密钥加密信息；该对称密钥加密信息是由数据拥有方利用该 TEE 节点发送的公钥，对生成的对称密钥进行加密后得到并发来的；

在可信执行环境中获取至少一个数据分片，包括：

在可信执行环境中接收数据拥有方发来的数据分片，利用生成的公私钥对中的私钥从该数据拥有方发来的对称密钥加密信息中解密出对称密钥，并利用解密出的该对称密钥对该数据拥有方发来的数据分片进行解密，得到解密后的数据分片。

5、根据权利要求 1 所述的方法，其中，在 N 不小于 K 时，所述 TEE 节点集群中的 K 个 TEE 节点是从 N 个数据拥有方中选择出，并对选择出的 K 个数据拥有方加载 TEE 功能后得到的。

6、根据权利要求 1-5 中任一所述的方法，所述 K 为 3。

7、多方安全计算装置，该装置位于 TEE 节点中，包括：

创建单元，被配置为根据数据拥有方的数量 N，加入包括 K 个 TEE 节点的 TEE 节

点集群；以及创建可信执行环境，并将进行 K 方安全计算的基础算法加载到可信执行环境中；

数据分片获取单元，被配置为在可信执行环境中获取至少一个数据分片，所述数据分片包括：由数据拥有方对拥有的原始数据进行拆分后得到并发给该 TEE 节点的，或者由 TEE 节点集群中的其他 TEE 节点对数据拥有方发来的拆分后的原始数据进行计算后得到并发给该 TEE 节点的；

计算单元，被配置为利用所述 K 方安全计算的基础算法以及获取到的数据分片，进行 K 方安全计算；

其中，N 为大于 1 的正整数；K 为大于 1 的正整数。

8、根据权利要求 7 所述的装置，其中，所述 K 方安全计算的基础算法的计算速度比 N 方安全计算的基础算法的计算速度更快。

9、根据权利要求 7 所述的装置，其中，TEE 节点集群中的 K 个 TEE 节点通过同一个局域网执行所述 K 方安全计算。

10、根据权利要求 9 所述的装置，进一步包括：

公私钥对生成单元，被配置为在所述数据分片是由数据拥有方对拥有的原始数据进行拆分后得到并发给该 TEE 节点时，在可信执行环境中生成公私钥对；其中，该 TEE 节点生成的公私钥对与所述 TEE 节点集群中其他 TEE 节点生成的公私钥对不同；将生成的公私钥对中的公钥分别发送给数据拥有方，并接收对称密钥加密信息；该对称密钥加密信息是由数据拥有方利用该 TEE 节点发送的公钥，对生成的对称密钥进行加密后得到并发来的；

所述数据分片获取单元，被配置为在可信执行环境中接收数据拥有方发来的数据分片，利用生成的公私钥对中的私钥从该数据拥有方发来的对称密钥加密信息中解密出对称密钥，并利用解密出的该对称密钥对该数据拥有方发来的数据分片进行解密，得到解密后的数据分片。

11、根据权利要求 7 所述的装置，其中，在 N 不小于 K 时，所述 TEE 节点集群中的 K 个 TEE 节点是从 N 个数据拥有方中选择出，并对选择出的 K 个数据拥有方加载 TEE 功能后得到的。

12、根据权利要求 7 至 11 中任一所述的装置，所述 K 为 3。

13、一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-6 中任一项所述的方法。