

多方安全计算方法及装置、电子设备

技术领域

[01] 本说明书一个或多个实施例涉及分布式计算领域，尤其涉及一种多方安全计算方法及装置、电子设备。

5 背景技术

[02] 多方安全计算是一种密码学技术，参与计算的多方可以通过执行一个多方安全计算算法，基于各自持有的输入数据来共同进行安全计算，得到出一个计算结果，而不向其它各方泄露持有的输入数据。

- 10 [03] 多方安全计算算法，虽然能保护隐私数据，但不正确甚至恶意的算法实现，仍然可能会泄露隐私数据。最理想情况下，各方可以自行开发自己的多方安全计算软件，并各自利用各自开发的多方安全计算软件来参与多方安全计算。然而，在实际应用中，各方通常使用的可能是一个提供商提供的多方安全计算软件；因此，对于提供商而言，则需要证明其提供的多方安全计算软件是可信的，没有泄露隐私数据。

发明内容

- 15 [04] 本说明书提出一种多方安全计算方法，应用于分布式网络中部署的任一计算节点；其中，所述分布式网络部署了多个计算节点，所述多个计算节点基于各自持有的隐私数据共同参与多方安全计算，所述方法包括：

[05] 基于多方安全计算算法生成与持有的隐私数据相关的计算参数；

- 20 [06] 将所述计算参数发送至参与多方安全计算的其它计算节点，以由所述其它计算节点基于收集到的由参与多方安全计算的各计算节点发送的计算参数执行多方安全计算；以及，

[07] 创建对应于所述计算参数的审计日志；其中，所述审计日志记录了与所述计算参数相关的描述信息。

[08] 可选的，还包括：

- 25 [09] 收集参与多方安全计算的其它各计算节点发送的计算参数，基于收集到的由其它各计算节点发送的计算参数执行多方安全计算；以及，

- [10]创建对应于由所述其它各计算节点发送的计算参数的审计日志，并存储所述审计日志；其中，所述审计日志记录了与所述计算参数相关的描述信息。
- [11]可选的，所述计算参数，包括：
- [12]参与多方安全计算的随机数；和/或，
- 5 [13]参与多方安全计算的密文数据。
- [14]可选的，与所述计算参数相关的描述信息，包括：
- [15]与参与多方安全计算的随机数对应的随机数生成规则；和/或，
- [16]与参与多方安全计算的密文数据对应的密钥。
- [17]可选的，还包括：
- 10 [18]基于所述审计日志对参与多方安全计算的计算节点发送的计算参数进行隐私审计，确认所述计算节点发送的计算参数是否存在隐私泄露风险；或者，将所述审计日志发送至第三方的审计节点，以由所述审计节点对参与多方安全计算的计算节点发送的计算参数进行隐私审计，确认所述计算节点发送的计算参数是否存在隐私泄露风险。
- [19]可选的，所述基于所述审计日志对参与多方安全计算的计算节点发送的计算参数进行
- 15 行隐私审计，确认所述计算节点发送的计算参数是否存在隐私泄露风险，包括：
- [20]基于所述审计日志中记录的，与参与多方安全计算的计算节点发送的随机数对应的随机数生成规则，校验所述随机数是否为基于其它各计算节点持有的隐私数据构建的随机数；
- [21]如果是，确认所述计算节点发送的计算参数存在隐私泄露风险；
- 20 [22]如果否，确认所述计算节点发送的计算参数不存在隐私泄露风险。
- [23]可选的，所述基于所述审计日志对参与多方安全计算的计算节点发送的计算参数进行隐私审计，确认所述计算节点发送的计算参数是否存在隐私泄露风险，包括：
- [24]基于所述审计日志中记录的，参与多方安全计算的计算节点发送的密文数据对应的密钥，校验所述所述密钥是否为其它各计算节点持有的已知密钥；
- 25 [25]如果是，确认所述计算节点发送的计算参数存在隐私泄露风险；
- [26]如果否，确认所述计算节点发送的计算参数不存在隐私泄露风险。
- [27]本说明书还提出一种多方安全计算装置，应用于分布式网络中部署的任一计算节点；

其中,所述分布式网络部署了多个计算节点,所述多个计算节点基于各自持有的隐私数据共同参与多方安全计算,所述装置包括:

[28]生成模块,基于多方安全计算算法生成与持有的隐私数据相关的计算参数;

- 5 [29]发送模块,将所述计算参数发送至参与多方安全计算的其它计算节点,以由所述其它计算节点基于收集到的由参与多方安全计算的各计算节点发送的计算参数执行多方安全计算;

[30]创建模块,创建对应于所述计算参数的审计日志;其中,所述审计日志记录了与所述计算参数相关的描述信息。

[31]可选的,还包括:

- 10 [32]收集模块,收集参与多方安全计算的其它各计算节点发送的计算参数,基于收集到的由其它各计算节点发送的计算参数执行多方安全计算;

[33]所述创建模块进一步:

[34]创建对应于由所述其它各计算节点发送的计算参数的审计日志,并存储所述审计日志;其中,所述审计日志记录了与所述计算参数相关的描述信息。

- 15 [35]可选的,所述计算参数,包括:

[36]参与多方安全计算的随机数;和/或,

[37]参与多方安全计算的密文数据。

[38]可选的,与所述计算参数相关的描述信息,包括:

[39]与参与多方安全计算的随机数对应的随机数生成规则;和/或,

- 20 [40]与参与多方安全计算的密文数据对应的密钥。

[41]可选的,还包括:

- [42]审计模块,基于所述审计日志对参与多方安全计算的计算节点发送的计算参数进行隐私审计,确认所述计算节点发送的计算参数是否存在隐私泄露风险;或者,将所述审计日志发送至第三方的审计节点,以由所述审计节点对参与多方安全计算的计算节点发送的计算参数进行隐私审计,确认所述计算节点发送的计算参数是否存在隐私泄露风险。
- 25

[43]可选的,所述审计模块进一步:

[44]基于所述审计日志中记录的,与参与多方安全计算的计算节点发送的随机数对应的

随机数生成规则,校验所述随机数是否为基于其它各计算节点持有的隐私数据构建的随机数;

[45]如果是,确认所述计算节点发送的计算参数存在隐私泄露风险;

[46]如果否,确认所述计算节点发送的计算参数不存在隐私泄露风险。

5 [47]可选的,所述审计模块进一步:

[48]基于所述审计日志中记录的,参与多方安全计算的计算节点发送的密文数据对应的密钥,校验所述所述密钥是否为其它各计算节点持有的已知密钥;

[49]如果是,确认所述计算节点发送的计算参数存在隐私泄露风险;

[50]如果否,确认所述计算节点发送的计算参数不存在隐私泄露风险。

10 [51]本说明书还提出一种电子设备,应用于分布式网络;其中,所述分布式网络部署了多个计算节点,所述多个计算节点基于各自持有的隐私数据共同参与多方安全计算,包括:

[52]处理器;

[53]用于存储机器可执行指令的存储器;

15 [54]其中,通过读取并执行所述存储器存储的与多方安全计算的控制逻辑对应的机器可执行指令,所述处理器被促使:

[55]基于多方安全计算算法生成与持有的隐私数据相关的计算参数;

[56]将所述计算参数发送至参与多方安全计算的其它计算节点,以由所述其它计算节点基于收集到的由参与多方安全计算的各计算节点发送的计算参数执行多方安全计算;以

20 及,

[57]创建对应于所述计算参数的审计日志;其中,所述审计日志记录了与所述计算参数相关的描述信息。

[58]通过以上技术方案,由于参与多方安全计算的各计算节点,在基于搭载的多方安全计算算法生成了计算参数之后,还可以创建并存储与计算参数对应的审计日志,并在审

25 计日志中记录与所述计算参数相关的描述信息,使得各计算节点的管理用户可以通过查看审计日志,就可以了解到多方安全计算算法生成的计算参数的详细信息,因此对于多方安全计算算法的使用方而言,可以获得更加便于对算法进行审计的审计信息;而对于

多方安全计算算法的提供方而言，可以在不公开多方安全计算算法的源代码的前提下，使得上述多方安全计算算法变得透明可审计。

附图说明

[59]图 1 是一示例性实施例提供的一种多方安全计算方法的流程图。

5 [60]图 2 是一示例性实施例提供的一种电子设备的结构示意图。

[61]图 3 是一示例性实施例提供的一种多方安全计算装置的框图。

具体实施方式

[62]在实际应用中，出于隐私保护的目，多方安全计算算法通常为黑盒算法，搭载多方安全计算算法的各个计算节点之间的数据传输行为很不透明；

10 [63]例如，对于搭载诸如秘密分享、同态加密、混淆电路等多方安全计算算法的计算节点之间，通常传输携带大量的密文和/或随机数的交互消息，即便对于多方安全计算算法的使用者而言，也很难理解以上交互消息中携带的密文和/或随机数的具体含义。

[64]因此，对于多方安全计算算法的提供方而言，为证明其所提供的多方安全计算算法透明可信，则不得不需要将其所提供的多方安全计算算法的源代码向使用者或者中立机

15 构进行公开，以完成针对算法的审计。

[65]基于此，本说明书中则旨在提出一种，多方安全计算算法的提供方可以在不公开算法的源代码的前提下，向算法使用者提供更加便于对算法进行审计的审计信息的技术方案。

20 [66]在实现时，分布式网络中的计算节点，可以基于搭载的多方安全计算算法生成与持有的隐私数据相关的计算参数；例如，在实际应用中，生成的计算参数可以包括，参与多方安全计算的随机数；和/或，参与多方安全计算的密文数据。

[67]一方面，当生成了上述计算参数后，上述计算节点可以将生成的计算参数，发送至分布式网络中参与多方安全计算的其它各计算节点，由其它计算节点基于收集到的由参与多方安全计算的各计算节点发送的计算参数来执行多方安全计算。

25 [68]另一方面，上述计算节点还可以创建对应于上述计算参数的审计日志，在审计日志中记录与上述计算参数相关的描述信息，并存储创建完成的审计日志；

[69]例如,生成的计算参数包括,参与多方安全计算的随机数;和/或,参与多方安全计算的密文数据为例,与上述计算参数相关的描述信息,则可以包括与参与多方安全计算的随机数对应的随机数生成规则;和/或,与参与多方安全计算的密文数据对应的密钥信息。

- 5 [70]通过以上技术方案,由于参与多方安全计算的各计算节点,在基于搭载的多方安全计算算法生成了计算参数之后,还可以创建并存储与计算参数对应的审计日志,并在审计日志中记录与所述计算参数相关的描述信息,使得各计算节点的管理用户可以通过查看审计日志,就可以了解到多方安全计算算法生成的计算参数的详细信息,因此对于多方安全计算算法的使用方而言,可以获得更加便于对算法进行审计的审计信息;而对于
- 10 多方安全计算算法的提供方而言,可以在不公开多方安全计算算法的源代码的前提下,使得上述多方安全计算算法变得透明可审计。

[71]下面通过具体实施例并结合具体的应用场景对本说明书进行描述。

- [72]请参考图 1,图 1 是本说明书一实施例提供的一种多方安全计算方法,应用于分布式网络中部署的任一计算节点;其中,上述分布式网络部署了多个计算节点,上述多个
- 15 计算节点基于各自持有的隐私数据共同参与多方安全计;所述多方安全计算方法执行以下步骤:

[73]步骤 102,基于多方安全计算算法生成与持有的隐私数据相关的计算参数;

- [74]步骤 104,将所述计算参数发送至参与多方安全计算的其它计算节点,以由所述其它计算节点基于收集到的由参与多方安全计算的各计算节点发送的计算参数执行多方
- 20 安全计算;

[75]步骤 106,创建对应于所述计算参数的审计日志;其中,所述审计日志记录了与所述计算参数相关的描述信息。

[76]上述分布式网络,可以包括能够支撑多方安全计算,且采用了分布式架构的任意形态的数据网络;

- 25 [77]例如,在一种场景下,上述分布式网络可以是由若干台计算设备组成的设备集群(比如服务器集群)搭建的多方安全计算平台;

[78]又如,在另一种场景下,上述分布式网络也可以是由若干台节点设备组成的区块链网络;在该区块链网络中可以部署需要由多台节点设备基于持有的隐私数据共同参与多方安全计算,且需要保证持有的隐私数据不公开给其它节点设备的在线业务。其中,上

述在线业务的具体类型，在本说明书中不进行特别限定。

[79]上述计算节点，具体可以包括上述分布式网络中，能够搭载上述多方安全计算算法的节点设备。

5 [80]上述多方安全计算算法，具体可以包括由各计算节点独立开发，或者由提供方统一提供的多方安全计算算法；比如，在实际应用中，上述多方安全计算算法，具体可以对应由各计算节点独立开发，或者由提供方统一提供的多方安全计算软件。

10 [81]上述计算参数，具体是指由参与多方安全计算的各计算节点，基于搭载的多方安全计算算法生成的，与各计算节点持有的隐私数据相关计算参数；各计算节点需要计算节点之间通过交互消息互相传输生成的计算参数，并基于收集到的各计算节点生成的计算参数来执行多方安全计算。

[82]在实际应用中，上述计算参数通常可以包括：需要参与多方安全计算的随机数；和/或，需要参与多方安全计算的密文数据。

15 [83]其中，需要说明的是，在实际应用中，上述多方安全计算算法，通常包括诸如秘密分享、同态加密、混淆电路等多方安全计算算法。而上述计算参数所包含的具体内容，通常取决于各计算节点所搭载的多方安全计算算法的具体算法类型。当各节点设备搭载以上列举出的不同算法时，上述计算参数所包含的内容，也会存在一定的差异。

[84]例如，基于秘密分享算法，上述计算参数，通常包括各计算节点将持有的隐私数据拆分出的 N 个随机数；其中，上述 N 个随机数包括 $N-1$ 个独立生成的随机数、和将上述 $N-1$ 个随机数与持有的隐私数据一起进行运算得到的运算结果（即第 N 个随机数）。

20 [85]基于同态加密算法，上述计算参数，通常包括基于持有的密钥对隐私数据进行加密后得到的密文数据。

[86]基于混淆电路算法，上述计算参数，通常包括用于对混淆电路的输入值（即参与计算的输入数据）和输出值分别进行替换的随机数（也称之为输入值和输出值的混淆值），以及将输入值的混淆值作为密钥，对输出数据的混淆值进行加密后得到的密文数据。

25 [87]在本说明书中，可以在分布式网络中，部署多个计算节点，各个计算节点作为多方安全计算的参与方，可以通过共同搭载同一种多方安全计算算法，在不泄露各自持有的隐私数据的前提下，来参与多方安全计算。

[88]例如，各个计算节点可以共同搭载由多方安全计算算法的提供商提供的多方安全计

算软件,通过该多方安全计算软件进行消息交互,在各个计算节点之间传输参与多方安全计算的随机数、和/或密文数据,来参与多方安全计算。

[89]上述分布式网络中部署的各个计算节点,除了需要共同搭载上同一种多方安全计算算法以外,还可以分别部署独立的数据源,结果存储系统、以及日志存储系统。

5 [90]其中,上述数据源,用于存储和维护各个数据节点持有的隐私数据。

[91]上述结果存储系统,用于存储和维护各个数据节点参与多方安全计算最终得到的计算结果。

[92]需要说明的是,在一些仅有少量数据参与的安全多方计算中,各个节点设备也可以不需要部署独立的数据源和结果存储系统。在这种情况下,各个计算节点,可以直接获取用户通过操作界面输入的数据作为数据源,并将最终的多方安全计算的计算结果,通过该操作界面向用户输出即可。上述日志存储系统,用于存储和维护由各个数据节点创建的与计算参数相关的审计日志。

10

[93]需要说明的是,对于创建的审计日志,也可以存储在第三方的存储设备或者存储系统中,在这种情况下,各个计算节点本地则不需要部署独立的日志存储系统;也即,在实际应用中,审计日志的生成节点和存储节点,可以相同也可以不同,在本说明书中不进行特别限定。

15

[94]对于参与多方安全计算的任一目标计算节点而言,在与其它各计算节点共同完成多方安全计算时,首先可以从部署的数据源中读取需要参与多方安全计算的隐私数据;

[95]然后,可以基于搭载的多方安全计算算法,对读取到的隐私数据进行计算,生成与持有的隐私数据相关的随机数、和/或密文数据。

20

[96]进一步,上述目标计算节点可以基于搭载的多方安全计算算法现有的消息交互机制,来构建交互消息,将生成的随机数、和/或密文数据作为计算参数,发送至参与多方安全计算的其它计算节点。

[97]而其它计算节点可以收集由参与多方安全计算的各计算节点通过交互消息发送的计算参数,并基于收集到的计算参数,来执行多方安全计算,然后将计算结果在本地部署的上述结果存储系统中进行存储。

25

[98]相应的,上述目标计算节点也可以收集由参与多方安全计算的各计算节点,通过交互消息发送的计算参数,并基于收集到的计算参数,来执行多方安全计算,然后将计算

结果在本地部署的上述结果存储系统中进行存储。

[99] 其中，需要说明的是，参与多方安全计算的各计算节点，在基于收集到的计算参数执行多方安全计算的计算过程，通常取决于各计算节点所搭载的多方安全计算算法的具体算法类型，不同类型的多方安全计算算法所涉及的计算过程通常会存在一定的差异。

- 5 [100] 以下分别以各计算节点搭载的多方安全计算算法为秘密分享算法、同态加密算法、混淆电路算法为例，对以上列举出的各种算法的算法逻辑进行简要描述。

[101] 1) 秘密分享 (secret sharing) 算法

- [102] 秘密分享(secret sharing)算法也称为秘密分割算法、秘密共享算法。它的基本原理是将秘密 (比如密钥) 拆分成多个分片(share)，分别交给不同人保管。只有收集到的
10 share 的数量超过门限数量时，才能恢复秘密；而如果收集到的 share 的数量少于门限数量，则基于 share 无法恢复秘密的任何信息。其中，秘密分享算法应用在多方安全计算中时，上述门限数量通常与分布式网络中部署的需要参与多方计算的计算节点的数量相同。

- [103] 当秘密分享算法用于多方安全计算时，各计算节点会将输入数据分别拆分成
15 share，并互相交换 share；然后，各计算节点会分别对本地收集到的多个 share 进行运算，得到与多方安全计算最终的计算结果对应的 share (即最终运算结果的一个分片)；最后，各计算节点合并生成的所有与最终的计算结果对应的 share，得到最终的计算结果，完成多方安全计算。

- [104] 如果上述分布式网络中部署的各计算节点，所搭载的多方安全计算算法为秘密
20 分享算法，上述目标计算节点在从部署的数据源中读取到需要参与多方安全计算的隐私数据 S 之后，首先可以按照秘密分享算法，将上述隐私数据分割为 d 个 share(随机数)。

[105] 具体地，基于秘密分享算法，可以在预设的随机数取值空间 P 中，采用随机抽取的方式，生成 d-1 个独立的随机数作为前 d-1 个 share，记为 $S_1, S_2, S_3, \dots, S_{d-1}$ 。

- [106] 例如，若隐私数据 S 是一个 64bit 的整型数据，则 $P=2^{64}$ ；最终生成的 d-1 个独立
25 的随机数，则均为从 $[0, 2^{64}-1]$ 的取值空间中随机抽取的一个取值。

[107] 进一步的，可以将上述 d-1 个随机数与隐私数据 S 一起进行运算，并将运算得到的运算结果，作为第 d 个 share，记为 S_d 。

[108] 其中，将上述 d-1 个随机数与隐私数据 S 一起进行运算的运算规则，通常取决

于具体的秘密分享算法;

[109] 例如,以秘密分享算法中最常用的 trivial additive secret sharing 算法为例,通常要求对隐私数据分割得到的 d 个 share 要满足以下表达时:

$$S = S_1 + S_2 + S_3 + \dots + S_d \% P$$

5 [110] 其中, % 为取模运算符。

[111] 基于以上表达式, $S_d = S - (S_1 + S_2 + S_3 + \dots + S_{d-1}) \% P$ 。在这种算法下,可以通过将隐私数据 S , 与前 $d-1$ 个 share 的和与取值空间 P 的取模计算结果进行相减得到 S_d 。

[112] 当基于秘密分享算法完成对隐私数据 S 的数据分割后,上述目标计算节点可以在本地保留一个 share,然后基于秘密分享算法现有的消息交互机制,来构建交互消息,

10 将剩下的 share, 分别发送给其它参与多方安全计算的各计算节点。

[113] 其中,上述目标计算节点可以在本地保留第 N 个 share,也可以保留前 $d-1$ 个 share 中的任意一个;也即,当上述目标计算节点在本地保留第 N 个 share 时,最终仅会将作为前 $d-1$ 个 share 的随机作为计算参数;而如果在本地保留前 $d-1$ 个 share 中的任意一个,最终会将作为前 $d-1$ 个 share 的剩余随机,和上述 $N-1$ 个随机数与隐私数据 S 的预算结果作为计算参数。

15

[114] 一方面,其它各计算节点,可以收集各计算节点发送的 share,按照各计算节点约定好的运算逻辑对收集到的 share 进行计算,得到一个与最终的计算结果对应的 share,并将计算结果向其它各计算节点进行广播;而上述目标计算节点可以收集其它各计算节点广播的计算结果,再按照约定好的运算逻辑对收集到的计算结果再次进行计算,得到对各个计算节点各自持有的隐私数据进行多方安全计算的最终计算结果,然后将上述最终计算结果在本地部署的结果存储系统中进行存储;

20

[115] 另一方面,上述目标计算节点,也可以收集其它各计算节点发送的 share,按照约定好的运算逻辑对收集到的 share 进行计算,得到一个与最终的计算结果对应的 share,并将计算结果向其它各计算节点进行广播;而其它各计算结果可以收集各计算节点广播的计算结果,再按照约定好的运算逻辑对收集到的计算结果再次进行计算,得到对持有的隐私数据 S 进行多方安全计算的最终结果;

25

[116] 其中,各计算节点约定好的运算逻辑,通常取决于实际的多方安全计算需求,在本说明书中不进行特别限定。

[117] 2) 同态加密算法

[118] 同态加密(homomorphic encryption)算法, 是一类能在密文状态下进行数据运算的加密算法。在不解密也不需使用解密密钥情况下, 对密文进行计算, 也可以得到基于明文进行计算得到的计算结果的密文。

5 [119] 例如, 对 a 的同态加密密文 $E(a)$ 和 b 的同态加密密文 $E(b)$ 进行运算, 可以得到 $a+b$ 的密文 $E(a+b)$, 且操作过程中不会泄露 a 、 b 或 $a+b$, 也不需要使用解密的密钥对密文进行解密。

[120] 如果上述分布式网络中部署的各计算节点, 所搭载的多方安全计算算法为同态加密算法, 上述目标计算节点在从部署的数据源中读取到需要参与多方安全计算的隐私数据 S 之后, 首先可以按照同态加密算法, 生成一对同态加密的加密密钥 PK 和解密密钥 SK , 并基于生成的加密密钥 PK 对上述隐私数据进行加密生成密文数据, 然后基于同态加密算法现有的消息交互机制, 来构建交互消息, 将生成的上述密文数据, 分别发送给其它参与多方安全计算的各计算节点。

10

[121] 一方面, 其它各计算节点, 也可以采用相同的方式, 按照同态加密算法, 生成一对同态加密的加密密钥 PK 和解密密钥 SK , 基于加密密钥 PK 对从本地部署的数据源中读取的隐私数据进行加密得到密文数据, 并收集各计算节点发送的对各自持有的隐私数据进行加密后得到的密文数据, 然后将收集到的由其它各计算节点发送的密文数据, 和本地生成的密文数据一起按照约定好的运算逻辑进行计算, 得到对各个计算节点各自持有的隐私数据进行多方安全计算的最终计算结果对应的密文数据(上述其它各计算节点无法在其本地解密该密文数据)。

15

20

[122] 当得到与最终计算结果对应的密文数据后, 其它各计算节点可以将与最终计算结果对应的密文数据, 向各节点设备进行广播。而当上述目标计算节点在收到与最终计算结果对应的密文数据后, 可以基于上述解密密钥 SK 对收到的与最终计算结果对应的密文数据进行解密, 得到最终计算结果的明文数据, 然后将上述最终计算结果的明文数据在本地部署的结果存储系统中进行存储。

25

[123] 另一方面, 上述目标计算节点, 也可以收集其它各计算节点发送的对各自持有的隐私数据进行加密后得到的密文数据, 然后将收集到的由其它各计算节点发送的密文数据, 和本地生成的密文数据一起按照约定好的运算逻辑进行计算, 得到对各个计算节点各自持有的隐私数据进行多方安全计算的最终计算结果对应的密文数据(上述目标计

算节点无法在其本地解密该密文数据)。

- [124] 当得到与最终计算结果对应的密文数据后,上述目标计算节点可以将与最终计算结果对应的密文数据,向其它各计算节点进行广播。而当其它各计算节点在收到与最终计算结果对应的密文数据后,可以基于上述解密密钥 SK 对收到的与最终计算结果对应的密文数据进行解密,得到最终计算结果的明文数据,然后将上述最终计算结果的明文数据在本地部署的结果存储系统中进行存储。

[125] 其中,需要说明的是,各计算节点约定好的运算逻辑,仍然取决于实际的多方安全计算需求,在本说明书中不进行特别限定。但基于同态加密算法,任何运算逻辑,都可以分解为加法同态加密、乘法同态加密等基础的运算。

10 [126] 3) 混淆电路算法

[127] 混淆电路算法,原理是通过用计算机模拟 ASIC 集成电路,来实现多方安全计算。任何多方安全计算任务,都可以用为其设计的 ASIC 集成电路来实现。即可以按照多方安全计算任务对应的运算逻辑,利用多个运算门(与门、异或门等基础运算门)连接起来,模拟出与上述运算逻辑对应的门电路,然后使用门电路来进行运算。

- 15 [128] 基于混淆电路算法,通常将多方安全计算任务对应的运算逻辑表示为门电路,并对上述门电路的每条运算线路进行加密,加密后的上述门电路称为混淆电路。最终通过用计算机来执行混淆电路的运算,来实现多方安全计算。

[129] 在基于混淆电路算法来实现多方安全计算时,参与多方安全计算的计算节点,通常会被划分为混淆电路生成方,和混淆电路的执行方两种角色。

- 20 [130] 例如,在一个由 K 个计算节点参与的多方安全计算中,通常会由其中的 K-1 个计算节点作为电路生成方,来生成混淆电路,而剩余的一个计算节点作为混淆电路的执行方,来执行混淆电路的运算,来得到最终的计算结果。

[131] 如果上述分布式网络中部署的各计算节点,所搭载的多方安全计算算法为混淆电路算法,首先可以将与多方安全计算任务对应的运算逻辑,表示为门电路;

- 25 [132] 其中,由于该运算逻辑需要由多个计算节点基于各自持有的隐私数据来共同参数,对于每一个计算节点而言,可能仅能够对应上述门电路中的一个或者其中几个运算门,其持有的隐私数据可能仅能够作为上述门电路中的一个或者其中几个运算门的输入数据。

[133] 进一步的,上述目标计算节点在从部署的数据源中读取到需要参与多方安全计算的隐私数据 S 之后,可以将读取到的隐私数据 S,作为该目标计算节点在上述门电路中对应的运算门的输入值,在上述运算门中进行运算,得到上述运算门的输出值。

[134] 其中,在实际应用中,上述门电路中每个运算门的运算逻辑,都可以用

5 [135] 真值表来表示和执行。一张真值表用于记录该运算门的输入线路取任何输入值时,输出线路得到的输出值。真值表中的每一行对应输入线路的一种输入值组合。而为了在门电路的运算中隐藏该运算门中各运算线路的真实值:

[136] 一方面,上述目标计算节点,可以基于混淆电路算法搭载的随机函数生成随机数,对上述运算门的真值表中的输入值和输出值分别进行替换;其中,替换后的随机数
10 称之为混淆值。

[137] 另一方面,上述目标计算节点,还可以将上述运算门的输入值对应的混淆值作为密钥,对上述运算门的真值表中的输出值的混淆值进行加密得到密文数据,并基于该密文数据对原来真值表中的输出值的混淆值进行替换,得到一张混淆真值表;或者,也可以基于该密文数据单独创建一张混淆真值表(即混淆真值表中仅包括该密文数据)。

15 [138] 第三方面,上述目标计算节点,还可以打乱上述混淆真值表中的每一行的顺序。

[139] 当上述目标计算节点完成以上三方面的针对上述门电路中对应的运算门的真值表的混淆替换后,此时上述混淆电路生成完毕,上述目标计算节点可以基于混淆电路现有的消息交互机制,来构建交互消息,上述目标计算节点在上述门电路中对应的运算门的输入值对应的混淆值,以及将上述运算门的输入值对应的混淆值作为密钥,对上述运
20 算门的真值表中的输出值的混淆值进行加密得到的密文数据作为计算参数,发送给作为混淆电路执行方的计算节点。

[140] 例如,在实际应用中,在基于混淆电路算法来实现多方安全计算时,通常会将混淆电路算法与不经意传输技术进行结合,上述目标计算节点在向作为作为混淆电路执行方的计算节点发送计算参数时,一方面,可以通常可以将上述混淆真值表采用明文发
25 送的形式,直接发送给作为混淆电路执行方的计算节点;另一方面,可以采用不经意传输技术,将上述目标计算节点在上述门电路中对应的运算门的输入值对应的混淆值,通过模糊化的传送方式,发送给作为混淆电路执行方的计算节点;其中,基于不经意传输技术向作为混淆电路执行方的计算节点传输数据的具体实施过程,在本说明书中不再进行详述,本领域技术人员在将本说明书的技术方案付诸实现时,可以参考相关技术中的

记载。

[141] 而作为混淆电路执行方的计算节点，在收到各计算节点发送的计算参数后，可以根据各计算节点在上述门电路中对应的运算门的输入值对应的混淆值，对与各计算节点在上述门电路中对应的运算门的混淆真值表中记录的密文数据进行解密，得到各计算节点在上述门电路中对应的运算门的输出值的混淆值。

[142] 最后，作为混淆电路执行方的计算节点，可以基于最终解密出的上述门电路中的各个运算门的输出值的混淆值后，可以逐级进行运算，得到上述门电路最终的输出值对应的混淆值，然后将将该混淆值作为最终的计算结果，发送给其它的计算节点。

[143] 上述目标计算节点在收到与门电路最终的输出值对应的混淆值后，可以查询真值表，基于混淆值与真正的输出值之间的对应关系，得到与该混淆值对应的输出值，并将该输出值作为多方安全计算的最终计算结果的原始值，在本地部署的结果存储系统中进行存储。

[144] 对于上述分布式网络中部署的各计算节点而言，当完成了以上示出的多方安全计算过程，还可以将存储在上述结果存储系统中的计算结果，向计算节点的管理用户进行可视化输出。

[145] 在本说明书中，对于搭载诸如秘密分享、同态加密、混淆电路等多方安全计算算法的计算节点之间，通常传输携带大量的密文和/或随机数的交互消息，而即便对于多方安全计算算法的使用者而言，通常也很难理解以上交互消息中携带的密文和/或随机数的具体含义

[146] 基于此，在本说明书中，当上述目标节点设备在基于搭载的多方安全计算算法的现有的消息交互机制，通过构建交互消息，将生成的计算参数发送给参与多方安全计算的各计算节点时，还可以在本地创建与发送的计算参数相关的审计日志，并将创建的审计日志，在本地部署的日志存储系统中进行存储。

[147] 其中，上述审计日志，具体可以用于记录向参与多方安全计算的各计算节点发送的计算参数相关的描述信息；

[148] 在示出的一种实施方式中，计算节点需要向其它参与多方安全计算的计算节点发送的计算参数，通常是携带在该计算节点所构建的交互消息中的消息字段中，因此可以在审计日志中记录计算节点所构建的交互消息中，每一个字段的具体含义，以及与每一个字段相关的描述信息，以供审计使用。

- [149] 相应的, 当上述目标节点设备在接收到由其它各计算节点通过构建的交互消息发送的计算参数时, 也可以在本地创建与其它各计算节点发送的计算参数相关的审计日志, 并将创建的审计日志, 在本地部署的日志存储系统中进行存储。
- [150] 例如, 对于部署在上述分布式网络中的各计算节点而言, 通常搭载了同一多方安全计算算法, 因此各计算节点构建的交互消息通常遵循相同的消息格式; 因此, 上述目标计算节点在收到其它各计算节点发送的交互消息后, 可以按照标准的消息格式对该交互消息进行解析, 生成相应的审计日志, 并在审计日志中记录该交互消息中的每一个字段的具体含义。
- [151] 在本说明书中, 上述审计日志中记录的与上述计算参数相关的描述信息, 可以与上述计算参数所包含的内容相对应。
- [152] 各计算节点通过交互消息向其它计算节点发送的计算参数, 通常包括参与多方安全计算的随机数; 和/或, 参与多方安全计算的密文数据; 相应的, 最终生成的审计日志中记录的与上述计算参数相关的描述信息, 则可以包括与参与多方安全计算的随机数对应的描述信息; 和/或, 与参与多方安全计算的密文数据对应的描述信息。
- [153] 其中, 上述描述信息的具体内容, 在本说明书中不进行特别限定; 在实际应用中, 可以基于计算节点的管理用户对计算节点搭载的多方安全计算算法的具体审计需求。
- [154] 在示出的一种实施方式中, 最终生成的审计日志中记录的与上述计算参数相关的描述信息, 可以包括与参与多方安全计算的随机数对应的随机数生成规则; 和/或, 与参与多方安全计算的密文数据对应的密钥;
- [155] 其中, 上述随机数生成规则, 具体可以涵盖与上述随机数的生成方式相关的任意形式的描述信息;
- [156] 例如, 上述随机数在计算节点本地随机生成、由计算节点将本地生成的随机数和其它数据通过某运算得到、从其它计算节点或者可信的随机源接收到的随机数、从其它计算节点或者可信的随机源接收到的随机数和其它数据通过某运算得到、由计算节点将在本地生成的随机数和接收到的随机数通过某运算得到, 等等, 在本说明书中不再进行一一列举。
- [157] 而与参与多方安全计算的密文数据对应的密钥, 具体可以包括对该密文数据进行加密时所使用的加密密钥;
- [158] 其中, 在一些场景下, 除了加密密钥以外, 还可以携带对上述密文数据进行解

密的解密密钥；甚至，在上述审计日志中，还可以携带上述密文数据的明文数据。

[159] 例如，在一种实现方式中，计算节点创建的与本地发送给其它各计算节点的计算参数相关的审计日志，和计算节点创建的与接收到的其它各计算节点发送的计算参数相关的审计日志，所记录的与计算参数相关的描述信息，可以存在一定的差异。

- 5 [160] 由于多方安全计算节点，各个计算节点采用的输入数据，通常需要向其它参与多方安全计算的计算节点严格保密；因此，计算节点创建的与它各计算节点发送的计算参数相关的审计日志中，如果需要记录与密文数据对应的密钥时，可以仅记录与该密文数据相关的加密密钥。而对于计算节点创建的与本地发送给其它各计算节点的计算参数相关的审计日志中，则除了可以记录该密文数据的加密密钥，还可以记录该密文数据的解密密钥，以及该密文数据的明文数据。
- 10

- [161] 通过这种方式，使得计算节点的管理用户，可以基于审计日志记录的解密密钥，对该计算节点在本地生成的作为计算参数的密文数据进行解密后，来进一步校验解密后的计算参数的明文数据，与审计日志中记录的计算参数的明文数据是否一致，来审计该计算节点搭载的多方安全计算算法，是否在用户不知情的情况下，在传输的计算参数中恶意添加了隐私数据，以此来提升算法的可审计性。
- 15

[162] 在本说明书中，对于上述分布式网络中部署的各计算节点而言，可能共同使用由多方安全计算算法的提供方所提供的多方安全算法，虽然多方安全算法本身是用于保护隐私数据的算法，但不正确甚至恶意的算法实现，仍然可能会存在隐私数据泄露的风险。

- 20 [163] 例如，在一种场景下，恶意的多方安全计算算法，可能并不会按照算法设计使用随机生成的随机数作为密钥，来加密需要向其它各计算节点传输的隐私数据，而是会在用户使用用户不知情的情况下，选择使用其它参与方已知的密钥来加密需要向其它各计算节点传输的隐私数据，使得接收方可以通过已知的密钥解密数据，获得其它计算节点持有的隐私数据；

- 25 [164] 又如，在另一种场景下，恶意的多方安全计算算法，可能会在使用用户不知情的情况下，基于计算节点持有的隐私数据来构造假随机数，然后利用假随机数向其它计算节点发送隐私数据。

[165] 在本说明书中，对于上述分布式网络中部署的各计算节点而言，可以基于上述日志存储系统中存储的审计日志，对各计算节点搭载的多方安全算法进行隐私审计（也

可以仅对本节点搭载的多方安全算法，或者各计算节点中某一指定的计算节点搭载的多方安全算法进行隐私审计)，来确定各计算节点发送的计算参数，是否存在隐私泄露的风险。

[166] 当然，在实际应用中，对各计算节点搭载的多方安全算法进行隐私审计，也可以由第三方的审计节点来完成；在这种情况下，上述分布式网络中部署的各计算节点，可以将上述日志存储系统中所述审计日志，发送给上述审计节点（比如可以主动发送审计日志，也可以由审计节点来主动调用审计日志），由上述第三方的审计节点基于接收到的审计日志，对各计算节点搭载的多方安全算法进行隐私审计，来确定各计算节点发送的计算参数，是否存在隐私泄露的风险。

10 [167] 例如，在一种场景下，各计算节点搭载由提供商提供的多方安全计算算法，并由各计算节点的运营方，来独立的部署审计节点，用于对提供商提供的多方安全计算算法进行隐私审计。

[168] 其中，对各计算节点搭载的多方安全算法进行隐私审计的审计逻辑，取决于上述审计日志中记录的与计算参数相关的描述信息的具体内容；

15 [169] 在示出的一种实施方式中，以上述计算参数为参与多方安全计算的随机数；以及，与上述计算参数相关的描述信息为，与参与多方安全计算的随机数对应的随机数生成规则为例：

[170] 在这种场景下，计算节点可以从本地部署的日志存储系统中，读取参与多方安全计算的各计算节点发送的作为计算参数的随机数对应的审计日志，并基于读取到的审计日志中记录的，与上述随机数对应的随机数生成规则，来校验该随机数是否为基于其它各计算节点持有的隐私数据构建的随机数；

20 [171] 例如，在实际应用中，可以计算上述随机数生成规则中记录的，在生成上述随机数时所使用的数据的摘要值（比如 hash 值），将计算得到的摘要与其它各计算节点持有的隐私数据的摘要值进行比较，来确定上述随机数是否为基于其它各计算节点持有的隐私数据构建的假随机数。

25 [172] 如果经过校验确认，上述随机数为基于其它各计算节点持有的隐私数据构建的随机数，作为计算参数的该随机数则存在隐私泄露的风险；反之，如果经过校验确认，生成上述随机数的数据源为合法数据源，上述随机数并不是基于其它各计算节点持有的隐私数据构建的随机数，作为计算参数的该随机数则并不存在隐私泄露的风险。

[173] 通过这种方式，使得计算节点通过对本地部署的日志存储系统中的审计日志进行简易的审计，就可以确认作为计算参数的随机数是否为基于其它各计算节点持有的隐私数据构建的假随机数，从而可以及时发现隐私泄露的风险。

[174] 在示出的另一种实施方式中，以上述计算参数为参与多方安全计算的密文数据；
5 以及，与所述计算参数相关的描述信息为，与参与多方安全计算的密文数据对应的密钥为例：

[175] 在这种场景下，计算节点可以从本地部署的日志存储系统中，读取参与多方安全计算的各计算节点发送的作为计算参数的密文数据对应的审计日志，并基于读取到的审计日志中记录的，与上述密文数据对应的密钥，来校验该密钥是否为其它各计算节点
10 持有的已知密钥；

[176] 例如，在实际应用中，可以将上述审计日志中记录的与上述密文数据对应的密钥，与其它各计算节点持有的已知密钥进行比较，来确定上述密文数据对应的密钥是否为其它各计算节点持有的已知密钥。

[177] 如果经过校验确认，上述密文数据对应的密钥为其它各计算节点持有的已知密
15 钥，作为计算参数的该随机数则存在隐私泄露的风险；反之，如果经过校验确认，上述密文数据对应的密钥并不匹配其它各计算节点持有的已知密钥，作为计算参数的该随机数则并不存在隐私泄露的风险。

[178] 通过这种方式，使得计算节点通过对本地部署的日志存储系统中的审计日志进行简易的审计，就可以确认作为计算参数的密文数据对应的密钥，是否为其它各计算节点
20 持有的已知密钥，从而可以及时发现隐私泄露的风险。

[179] 当然，在一些场景下，如果上述审计日志中，除了携带加密密钥以外，还携带了对上述密文数据进行解密的解密密钥，以及上述密文数据的明文数据，此时计算节点还可以基于读取到的审计日志中记录的，与上述密文数据对应的解密密钥，以及上述密文数据的明文数据，进一步对上述密文数据进行安全校验，来确认上述密文数据是否被
25 搭载的多方安全计算算法，恶意添加了隐私数据；

[180] 例如，在实际应用中，可以基于审计日志记录的解密密钥，对该计算节点在本地生成的作为计算参数的密文数据进行解密后，来进一步校验解密后的计算参数的明文数据，是否与审计日志中记录的计算参数的明文数据是否一致，来审计该计算节点搭载的多方安全计算算法，是否在用户不知情的情况下，在传输的作为计算参数的密文数据

中恶意添加了隐私数据；如果一致，表明该计算节点搭载的由提供商提供的多方安全计算算法的实现逻辑，与该多方安全计算算法的设计一致，上述密文数据不存在隐私泄露的风险；如果不一致，表明该计算节点搭载的由算法提供方提供的多方安全计算算法，可能在用户不知情的情况下，在传输的计算参数中恶意添加了隐私数据，此时上述密文数据存在隐私泄露的风险。

[181] 通过这种方式，使得计算节点通过对本地部署的日志存储系统中的审计日志进行简易的审计，就可以确认作为计算参数的密文数据中，是否被搭载的多方安全算法恶意添加了隐私数据，从而可以及时发现隐私泄露的风险。

[182] 通过以上技术方案，由于参与多方安全计算的各计算节点，在基于搭载的多方安全计算算法生成了计算参数之后，还可以创建并存储与计算参数对应的审计日志，并在审计日志中记录与所述计算参数相关的描述信息，使得各计算节点的管理用户可以通过查看审计日志，就可以了解到多方安全计算算法生成的计算参数的详细信息，因此对于多方安全计算算法的使用方而言，可以获得更加便于对算法进行审计的审计信息；而对于多方安全计算算法的提供方而言，可以在不公开多方安全计算算法的源代码的前提下，使得上述多方安全计算算法变得透明可审计。

[183] 与上述方法实施例相对应，本说明书还提供了一种多方安全计算装置的实施例。本说明书的多方安全计算装置的实施例可以应用在电子设备上。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在电子设备的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图 2 所示，为本说明书的多方安全计算装置所在电子设备的一种硬件结构图，除了图 2 所示的处理器、内存、网络接口、以及非易失性存储器之外，实施例中装置所在的电子设备通常根据该电子设备的实际功能，还可以包括其他硬件，对此不再赘述。

[184] 图 3 是本说明书一示例性实施例示出的一种多方安全计算装置的框图。

[185] 请参考图 3，所述多方安全计算装置 30 可以应用在前述图 2 所示的电子设备中，包括有：生成模块 301、发送模块 302、和创建模块 303。

[186] 生成模块 301，基于多方安全计算算法生成与持有的隐私数据相关的计算参数；

[187] 发送模块 302，将所述计算参数发送至参与多方安全计算的其它计算节点，以由所述其它计算节点基于收集到的由参与多方安全计算的各计算节点发送的计算参数执

行多方安全计算;

[188] 创建模块 303, 创建对应于所述计算参数的审计日志; 其中, 所述审计日志记录了与所述计算参数相关的描述信息。

[189] 在本实施例中, 所述装置 30 还包括:

5 [190] 收集模块 304 (图 3 中未示出), 收集参与多方安全计算的其它各计算节点发送的计算参数, 基于收集到的由其它各计算节点发送的计算参数执行多方安全计算;

[191] 所述创建模块 303 进一步:

[192] 创建对应于由所述其它各计算节点发送的计算参数的审计日志, 并存储所述审计日志; 其中, 所述审计日志记录了与所述计算参数相关的描述信息。

10 [193] 在本实施例中, 所述计算参数, 包括:

[194] 参与多方安全计算的随机数; 和/或,

[195] 参与多方安全计算的密文数据。

[196] 在本实施例中, 与所述计算参数相关的描述信息, 包括:

[197] 与参与多方安全计算的随机数对应的随机数生成规则; 和/或,

15 [198] 与参与多方安全计算的密文数据对应的密钥。

[199] 在本实施例中, 所述装置 30 还包括:

[200] 审计模块 305 (图 3 中未示出), 基于所述审计日志对参与多方安全计算的计算节点发送的计算参数进行隐私审计, 确认所述计算节点发送的计算参数是否存在隐私泄露风险;

20 [201] 或者, 将所述审计日志发送至第三方的审计节点, 以由所述审计节点对参与多方安全计算的计算节点发送的计算参数进行隐私审计, 确认所述计算节点发送的计算参数是否存在隐私泄露风险。

[202] 在本实施例中, 所述审计模块 305 进一步:

25 [203] 基于所述审计日志中记录的, 与参与多方安全计算的计算节点发送的随机数对应的随机数生成规则, 校验所述随机数是否为基于其它各计算节点持有的隐私数据构建的随机数;

[204] 如果是, 确认所述计算节点发送的计算参数存在隐私泄露风险;

- [205] 如果否, 确认所述计算节点发送的计算参数不存在隐私泄露风险。
- [206] 在本实施例中, 所述审计模块 305 进一步:
- [207] 基于所述审计日志中记录的, 参与多方安全计算的计算节点发送的密文数据对应的密钥, 校验所述所述密钥是否为其它各计算节点持有的已知密钥;
- 5 [208] 如果是, 确认所述计算节点发送的计算参数存在隐私泄露风险;
- [209] 如果否, 确认所述计算节点发送的计算参数不存在隐私泄露风险。
- [210] 上述装置中各个模块的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程, 在此不再赘述。
- [211] 对于装置实施例而言, 由于其基本对应于方法实施例, 所以相关之处参见方法
- 10 实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的, 其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的, 作为模块显示的部件可以是或者也可以不是物理模块, 即可以位于一个地方, 或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下, 即可以理解并实施。
- 15 [212] 上述实施例阐明的系统、装置、模块或模块, 具体可以由计算机芯片或实体实现, 或者由具有某种功能的产品来实现。一种典型的实现设备为计算机, 计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。
- 20 [213] 与上述方法实施例相对应, 本说明书还提供了一种电子设备的实施例。该电子设备包括: 处理器以及用于存储机器可执行指令的存储器; 其中, 处理器和存储器通常通过内部总线相互连接。在其他可能的实现方式中, 所述设备还可能包括外部接口, 以能够与其他设备或者部件进行通信。
- [214] 在本实施例中, 通过读取并执行所述存储器存储的与多方安全计算的控制逻辑
- 25 对应的机器可执行指令, 所述处理器被促使:
- [215] 基于多方安全计算算法生成与持有的隐私数据相关的计算参数;
- [216] 将所述计算参数发送至参与多方安全计算的其它计算节点, 以由所述其它计算节点基于收集到的由参与多方安全计算的各计算节点发送的计算参数执行多方安全计

算；以及，

[217] 创建对应于所述计算参数的审计日志；其中，所述审计日志记录了与所述计算参数相关的描述信息。

[218] 在本实施例中，通过读取并执行所述存储器存储的与多方安全计算的控制逻辑
5 对应的机器可执行指令，所述处理器被促使：

[219] 收集参与多方安全计算的其它各计算节点发送的计算参数，基于收集到的由其它各计算节点发送的计算参数执行多方安全计算；以及，

[220] 创建对应于由所述其它各计算节点发送的计算参数的审计日志，并存储所述审计日志；其中，所述审计日志记录了与所述计算参数相关的描述信息。

10 [221] 在本实施例中，通过读取并执行所述存储器存储的与多方安全计算的控制逻辑对应的机器可执行指令，所述处理器被促使：

[222] 基于所述审计日志对参与多方安全计算的计算节点发送的计算参数进行隐私审计，确认所述计算节点发送的计算参数是否存在隐私泄露风险；

[223] 或者，将所述审计日志发送至第三方的审计节点，以由所述审计节点对参与多
15 方安全计算的计算节点发送的计算参数进行隐私审计，确认所述计算节点发送的计算参数是否存在隐私泄露风险。

[224] 在本实施例中，通过读取并执行所述存储器存储的与多方安全计算的控制逻辑对应的机器可执行指令，所述处理器被促使：

[225] 基于所述审计日志中记录的，与参与多方安全计算的计算节点发送的随机数对
20 应的随机数生成规则，校验所述随机数是否为基于其它各计算节点持有的隐私数据构建的随机数；

[226] 如果是，确认所述计算节点发送的计算参数存在隐私泄露风险；

[227] 如果否，确认所述计算节点发送的计算参数不存在隐私泄露风险。

[228] 在本实施例中，通过读取并执行所述存储器存储的与多方安全计算的控制逻辑
25 对应的机器可执行指令，所述处理器被促使：

[229] 基于所述审计日志中记录的，参与多方安全计算的计算节点发送的密文数据对应的密钥，校验所述密文数据是否为其它各计算节点持有的已知密钥；

[230] 如果是，确认所述计算节点发送的计算参数存在隐私泄露风险；

[231] 如果否，确认所述计算节点发送的计算参数不存在隐私泄露风险。

[232] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本说明书的其它实施方案。本说明书旨在涵盖本说明书的任何变型、用途或者适应性变化，这些
5 变型、用途或者适应性变化遵循本说明书的一般性原理并包括本说明书未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本说明书的真正范围和精神由下面的权利要求指出。

[233] 应当理解的是，本说明书并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本说明书的范围仅由所附的权利要求来
10 限制。

[234] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。