

权利要求书

1. 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：
 - 5 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；
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，
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
10 相关的描述信息。
 2. 根据权利要求1所述的方法，还包括：
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，
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
15 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。
 3. 根据权利要求1或2所述的方法，所述计算参数，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。
 4. 根据权利要求3所述的方法，与所述计算参数相关的描述信息，包括：
20 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。
 5. 根据权利要求4所述的方法，还包括：
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；
25 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。
 6. 根据权利要求5所述的方法，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
30 泄露风险，包括：
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;

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;

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 7. 根据权利要求5所述的方法,

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:

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;

10 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;

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。

8. 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:

15 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;

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;

20 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。

9. 根据权利要求8所述的装置,还包括:

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;

所述创建模块进一步:

25 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. 根据权利要求8或9所述的装置,所述计算参数,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。

30 11. 根据权利要求10所述的装置,与所述计算参数相关的描述信息,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。

12. 根据权利要求 11 所述的装置，还包括：

5 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。

13. 根据权利要求 12 所述的装置，所述审计模块进一步：

10 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；

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；

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。

14. 根据权利要求 12 所述的装置，所述审计模块进一步：

15 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；

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；

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。

15. 一种电子设备，包括：

处理器；

20 用于存储机器可执行指令的存储器；

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：

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；

25 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，

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。