

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; 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; 其中, 所述计算节点对接了可信随机源; 所述方法包括:
 - 5 从所述可信随机源获取可信随机数;
 - 基于获取到的可信随机数对持有的隐私数据进行运算得到运算结果;
 - 至少将所述可信随机数作为计算参数, 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。
- 10 2. 根据权利要求 1 所述的方法, 还包括:
 - 创建与本计算节点发送至所述其它计算节点的所述可信随机数对应的审计日志; 其中, 所述审计日志记录了与所述可信随机数相关的描述信息。
3. 根据权利要求 2 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; 其中, 该计算参数至少
 - 15 包括由其它各计算节点发送的随机数;
 - 基于收集到的计算参数执行多方安全计算; 以及,
 - 创建与所述其它各计算节点发送的随机数对应的审计日志; 其中, 所述审计日志包括与所述随机数相关的描述信息。
4. 根据权利要求 2 或 3 所述的方法, 还包括:
 - 20 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作为计算参数的随机数进行隐私审计, 确认所述计算节点发送的作为计算参数的随机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作为计算参数的随机数进行隐私审计, 确认所述计算节点发送的作为计算参数的随机数是否存在隐私泄露风险。
- 25 5. 根据权利要求 4 所述的方法, 与所述可信随机数相关的描述信息, 包括: 与所述可信随机数对应的随机数生成规则;
 - 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作为计算参数的随机数进行隐私审计, 确认所述计算节点发送的作为计算参数的随机数是否存在隐私泄露风险, 包括:
- 30 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匹配来自所述可信随机源的可信随机数;

如果是, 确认所述计算节点发送的作为计算参数的随机数存在隐私泄露风险;

如果否, 确认所述计算节点发送的作为计算参数的随机数不存在隐私泄露风险。

6. 根据权利要求 1 所述的方法, 所述从所述可信随机源获取可信随机数, 包括以下中的任一:

5 获取由所述可信随机源生成的随机数作为所述可信随机数;

获取由所述可信随机源生成的随机数, 将由所述可信随机源生成的随机数, 与本计算节点生成的随机数进一步进行运算得到的结果, 作为所述可信随机数;

获取由所述可信随机源生成的随机数, 将所述随机数输入密钥生成函数计算得到的随机数作为所述可信随机数;

10 获取由所述可信随机源生成的随机数, 将所述随机数输入密钥生成函数计算得到的随机数, 与本计算节点生成的随机数进一步进行运算得到的结果, 作为所述可信随机数。

7. 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; 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; 其中, 所述计算节点对接了可信随机源; 所述装置包括:

15 获取模块, 从所述可信随机源获取可信随机数;

运算模块, 基于获取到的可信随机数对持有的隐私数据进行运算得到运算结果;

发送模块, 至少将所述可信随机数作为计算参数, 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 8. 根据权利要求 7 所述的装置, 还包括:

创建模块, 创建与本计算节点发送至所述其它计算节点的所述可信随机数对应的审计日志; 其中, 所述审计日志记录了与所述可信随机数相关的描述信息。

9. 根据权利要求 8 所述的方法, 还包括:

25 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; 其中, 该计算参数至少包括由其它各计算节点发送的随机数;

基于收集到的计算参数执行多方安全计算; 以及,

创建与所述其它各计算节点发送的随机数对应的审计日志; 其中, 所述审计日志包括与所述随机数相关的描述信息。

10. 根据权利要求 8 或 9 所述的装置, 还包括:

30 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作为计算参数的随机数进行隐私审计, 确认所述计算节点发送的作为计算参数的随机数是否存在隐私

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作为计算参数的随机数进行隐私审计, 确认所述计算节点发送的作为计算参数的随机数是否存在隐私泄露风险。

- 5 11. 根据权利要求 10 所述的装置, 与所述可信随机数相关的描述信息, 包括: 与所述可信随机数对应的随机数生成规则;

所述审计模块进一步:

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匹配来自所述可信随机源的可信随机数;

- 10 如果是, 确认所述计算节点发送的作为计算参数的随机数存在隐私泄露风险;
如果否, 确认所述计算节点发送的作为计算参数的随机数不存在隐私泄露风险。

12. 根据权利要求 7 所述的装置, 所述从所述可信随机源获取可信随机数, 包括以下中的任一:

获取由所述可信随机源生成的随机数作为所述可信随机数;

- 15 获取由所述可信随机源生成的随机数, 将由所述可信随机源生成的随机数, 与本计算节点生成的随机数进一步进行运算得到的结果, 作为所述可信随机数;

获取由所述可信随机源生成的随机数, 将所述随机数输入密钥生成函数计算得到的随机数作为所述可信随机数;

- 20 获取由所述可信随机源生成的随机数, 将所述随机数输入密钥生成函数计算得到的随机数, 与本计算节点生成的随机数进一步进行运算得到的结果, 作为所述可信随机数。

13. 一种电子设备, 包括:

处理器;

用于存储机器可执行指令的存储器;

- 25 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:

从所述可信随机源获取可信随机数;

基于获取到的可信随机数对持有的隐私数据进行运算得到运算结果;

- 30 至少将所述可信随机数作为计算参数, 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。