

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密钥源;所述方法包括:
- 5 从所述可信密钥源获取可信密钥;
- 基于获取到的所述可信密钥对持有的隐私数据进行加密得到密文数据;
- 至少将所述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,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其它计算节点的密文数据对应的审计日志;其中,所述审计日志记录了与所述密文数据相关的描述信息。
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对持有的隐私数据进行加密得到的密文数据;
- 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密文数据对应的审计日志;其中,所述审计日志包括与加密后的隐私数据相关的描述信息。
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密文数据进行隐私审计,确认所述计算节点发送的作为计算参数的密文数据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密文数据进行隐私审计,确认所述计算节点发送的作为计算参数的密文数据是否存在隐私泄露风险。
- 25 5. 根据权利要求4所述的方法,与所述密文数据相关的描述信息,包括:与所述密文数据对应的加密密钥;
- 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密文数据进行隐私审计,确认所述计算节点发送的作为计算参数的密文数据是否存在隐私泄露风险,包括:
- 校验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密文数据对应
- 30 的加密密钥,是否匹配来自所述可信密钥源的可信密钥;
- 如果是,确认所述计算节点发送的作为计算参数的密文数据不存在隐私泄露风险;

如果否, 确认所述计算节点发送的作为计算参数的密文数据存在隐私泄露风险。

6. 根据权利要求 5 所述的方法, 其中, 与本计算节点发送至所述其它计算节点的密文数据对应的审计日志中, 还记录了与密文数据对应的解密密钥、以及与所述密文数据对应的明文数据;

5 所述方法还包括:

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密文数据对应的解密密钥, 对所述密文数据进行解密得到明文数据;

校验解密后的明文数据与所述审计日志中记录的与所述密文数据对应的明文数据是否匹配;

10 如果是, 确认所述计算节点发送的作为计算参数的密文数据不存在隐私泄露风险; 如果否, 确认所述计算节点发送的作为计算参数的密文数据存在隐私泄露风险。

7. 根据权利要求 1 所述的方法, 所述可信密钥为随机数;

从所述可信密钥源获取可信密钥, 包括以下中的任一:

获取由所述可信密钥源生成的随机数作为所述可信密钥;

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

获取由所述可信密钥源生成的随机数, 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密钥;

20 获取由所述可信密钥源生成的随机数, 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, 作为所述可信密钥。

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; 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密钥源; 所述方法包括:

获取模块, 从所述可信密钥源获取可信密钥;

25 加密模块, 基于获取到的所述可信密钥对持有的隐私数据进行加密得到密文数据;

发送模块, 至少将所述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, 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。

9. 根据权利要求 8 所述的装置, 还包括:

30 创建模块, 创建与本计算节点发送至其它计算节点的密文数据对应的审计日志; 其中, 所述审计日志记录了与所述密文数据相关的描述信息。

10. 根据权利要求 9 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; 其中, 该计算参数至少包括由其它各计算节点对持有的隐私数据进行加密得到的密文数据;

计算模块, 基于收集到的计算参数执行多方安全计算;

5 所述创建模块进一步:

创建与所述其它各计算节点发送的密文数据对应的审计日志; 其中, 所述审计日志包括与加密后的隐私数据相关的描述信息。

11. 根据权利要求 10 所述的装置, 还包括:

10 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密文数据进行隐私审计, 确认所述计算节点发送的作为计算参数的密文数据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密文数据进行隐私审计, 确认所述计算节点发送的作为计算参数的密文数据是否存在隐私泄露风险。

12. 根据权利要求 10 或 11 所述的装置, 与所述密文数据相关的描述信息, 包括:
15 与所述密文数据对应的加密密钥;

所述审计模块进一步:

校验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密文数据对应的加密密钥, 是否匹配来自所述可信密钥源的可信密钥;

如果是, 确认所述计算节点发送的作为计算参数的密文数据不存在隐私泄露风险;

20 如果否, 确认所述计算节点发送的作为计算参数的密文数据存在隐私泄露风险。

13. 根据权利要求 12 所述的装置, 其中, 与本计算节点发送至所述其它计算节点的密文数据对应的审计日志中, 还记录了与密文数据对应的解密密钥、以及与所述密文数据对应的明文数据;

所述审计模块进一步:

25 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密文数据对应的解密密钥, 对所述密文数据进行解密得到明文数据;

校验解密后的明文数据与所述审计日志中记录的与所述密文数据对应的明文数据是否匹配;

如果是, 确认所述计算节点发送的作为计算参数的密文数据不存在隐私泄露风险;

30 如果否, 确认所述计算节点发送的作为计算参数的密文数据存在隐私泄露风险。

14. 根据权利要求 8 所述的装置, 所述可信密钥为随机数;

从所述可信密钥源获取可信密钥，包括以下中的任一：

获取由所述可信密钥源生成的随机数作为所述可信密钥；

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

- 5 获取由所述可信密钥源生成的随机数，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密钥；

获取由所述可信密钥源生成的随机数，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，作为所述可信密钥。

15. 一种电子设备，包括：

- 10 处理器；

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：

从所述可信密钥源获取可信密钥；

- 15 基于获取到的所述可信密钥对持有的隐私数据进行加密得到密文数据；

至少将所述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，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。