

权利要求书

1. 一种在用户和可信计算集群之间建立可信通道的方法,所述方法通过第一可信计算单元执行,所述第一可信计算单元归属于预先建立的第一可信计算集群,所述第一可信计算集群中的每个可信计算单元均维护有共同的第一集群密钥,所述第一可信计算单元预先向集群管理器注册有所归属的所述第一可信计算集群的信息,所述方法包括:
- 5 与用户协商出第一会话密钥,并建立与所述用户的第一可信通道,所述第一会话密钥用于对通过所述第一可信通道传输的数据进行加密;
- 利用所述第一集群密钥对所述第一会话密钥进行加密,得到第一加密密钥;
- 向所述集群管理器发出第一通知,其中包含所述第一加密密钥,以使得所述集群管
- 10 理器将所述第一加密密钥传递给所述第一可信计算集群中的其他可信计算单元。
2. 根据权利要求1所述的方法,其中与用户协商出第一会话密钥包括:
- 将本地的第一公钥和第一私钥所构成的密钥对中的第一公钥发送给所述用户,并获取用户提供的用户公钥;
- 基于所述第一公钥,第一私钥和所述用户公钥,生成第一会话密钥。
- 15 3. 根据权利要求1所述的方法,在向所述集群管理器发出第一通知之前,所述方法还包括:
- 向所述集群管理器发送针对第一可信通道的标识请求消息;
- 获取所述集群管理器为所述第一可信通道分配的第一会话标识;
- 将所述第一会话标识包含在所述第一通知中。
- 20 4. 一种在用户和可信计算集群之间建立可信通道的方法,所述方法通过集群管理器执行,所述集群管理器用于管理至少一个预先建立的可信计算集群,所述方法包括:
- 从第一可信计算单元接收第一通知,所述第一通知中包括第一加密密钥,所述第一加密密钥是利用第一集群密钥对第一会话密钥进行加密而得到,所述第一会话密钥是所述第一可信计算单元与用户建立的第一可信通道所对应的数据加密密钥;
- 25 确定所述第一可信计算单元所属的第一可信计算集群,所述第一可信计算集群中的每个可信计算单元均维护有所述第一集群密钥;
- 将所述第一加密密钥传递给所述第一可信计算集群中的第二可信计算单元,以使得所述第二可信计算单元根据其维持的第一集群密钥对所述第一加密密钥进行解密以得到所述第一会话密钥,从而基于所述第一会话密钥而加入到所述第一可信通道中。
- 30 5. 根据权利要求4所述的方法,还包括,
- 响应于所述第一可信计算单元针对所述第一可信通道的标识请求消息,为所述第一

可信通道分配第一会话标识;

将所述第一可信计算单元添加到与所述第一会话标识对应的第一可信计算单元列表。

5 6. 根据权利要求 5 所述的方法, 其中所述第一通知还包括所述第一会话标识, 所述方法还包括:

将所述第一会话标识传递给所述第二可信计算单元; 以及

将所述第二可信计算单元添加到所述第一可信计算单元列表中。

7. 根据权利要求 4 所述的方法, 其中确定所述第一可信计算单元所属的第一可信计算集群包括,

10 利用维护的集群信息表, 确定所述第一可信计算单元所属的第一可信计算集群, 以及所述第一可信计算集群中包含的各个可信计算单元。

8. 根据权利要求 4 所述的方法, 还包括:

将所述第一加密密钥传递给所述第一可信计算集群中的第三可信计算单元, 以使得所述第三可信计算单元根据其维持的第一集群密钥对所述第一加密密钥进行解密以得
15 到所述第一会话密钥, 从而基于所述第一会话密钥而加入到所述第一可信通道中。

9. 一种在用户和可信计算集群之间重建可信通道的方法, 所述方法通过第四可信计算单元执行, 所述第四可信计算单元已与用户建立第二可信通道, 所述第四可信计算单元归属于预先建立的第二可信计算集群, 所述第二可信计算集群中的每个可信计算单元均维护有共同的第二集群密钥, 且所述第四可信计算单元预先向集群管理器注册有所归属的所述第二可信计算集群的信息, 并从所述集群管理器获取有与所述第二可信通道对应的第二会话标识, 所述方法包括:

响应于针对第二可信通道的密钥更新请求, 与所述用户协商出针对所述第二可信通道的第二会话密钥, 所述第二会话密钥用于替代所述第二可信通道的原有密钥, 对传输的数据进行加密;

25 利用所述第二集群密钥对所述第二会话密钥进行加密, 得到第二加密密钥;

向所述集群管理器发出第二通知, 其中包含所述第二加密密钥和所述第二会话标识, 以使得所述集群管理器将所述第二加密密钥传递给与所述第二会话标识相关的其他可信计算单元。

10. 一种在用户和可信计算集群之间重建可信通道的方法, 所述方法通过集群管理器执行, 所述集群管理器用于管理至少一个预先建立的可信计算集群, 所述方法包括:

30 从第四可信计算单元接收第二通知, 所述第四可信计算单元归属于预先建立的第二

可信计算集群，所述第二可信计算集群中的每个可信计算单元均维护有共同的第二集群密钥，所述第二通知中包括第二会话标识和第二加密密钥，所述第二会话标识对应于所述第四可信计算单元与用户已经建立的第二可信通道，所述第二加密密钥是利用所述第二集群密钥对第二会话密钥进行加密而得到，所述第二会话密钥是针对所述第二可信通道的更新密钥；

根据所述第二会话标识，获取加入到所述第二可信通道的第二可信计算单元列表，所述第二可信计算单元列表包括所述第四可信计算单元以及同属于所述第二可信计算集群的至少一个其他可信计算单元；

将所述至少一个其他可信计算单元的每一个，均从所述第二可信计算单元列表中移除；

将所述第二加密密钥传递给所述至少一个其他可信计算单元中的第五可信计算单元，以使得所述第五可信计算单元根据其维持的第二集群密钥对所述第二加密密钥进行解密以得到所述第二会话密钥，从而基于所述第二会话密钥而重新加入到所述第二可信通道中。

11. 根据权利要求 10 所述的方法，其中在将所述第二加密密钥传递给所述至少一个其他可信计算单元中的第五可信计算单元之后，所述方法还包括，

将所述第五可信计算单元添加到所述第二可信计算单元列表中。

12. 一种在用户和可信计算集群之间建立可信通道的装置，所述装置部署在第一可信计算单元中，所述第一可信计算单元归属于预先建立的第一可信计算集群，所述第一可信计算集群中的每个可信计算单元均维护有共同的第一集群密钥，所述第一可信计算单元预先向集群管理器注册有所归属的所述第一可信计算集群的信息，所述装置包括：

密钥协商模块，配置为与用户协商出第一会话密钥，并建立与所述用户的第一可信通道，所述第一会话密钥用于对通过所述第一可信通道传输的数据进行加密；

第一加密模块，配置为利用所述第一集群密钥对所述第一会话密钥进行加密，得到第一加密密钥；

第一通知发送模块，配置为向所述集群管理器发出第一通知，其中包含所述第一加密密钥，以使得所述集群管理器将所述第一加密密钥传递给所述第一可信计算集群中的其他可信计算单元。

13. 根据权利要求 12 所述的装置，其中所述密钥协商模块配置为：

将本地的第一公钥和第一私钥所构成的密钥对中的第一公钥发送给所述用户，并获取用户提供的用户公钥；

基于所述第一公钥，第一私钥和所述用户公钥，生成第一会话密钥。

14. 根据权利要求 12 所述的装置，还包括标识获取模块，配置为在所述第一通知发送模块向所述集群管理器发出第一通知之前，执行：

向所述集群管理器发送针对第一可信通道的标识请求消息；

5 获取所述集群管理器为所述第一可信通道分配的第一会话标识；

将所述第一会话标识包含在所述第一通知中。

15. 一种在用户和可信计算集群之间建立可信通道的装置，所述装置部署在集群管理器中，所述集群管理器用于管理至少一个预先建立的可信计算集群，所述装置包括：

10 第一通知接收模块，配置为从第一可信计算单元接收第一通知，所述第一通知中包括第一加密密钥，所述第一加密密钥是利用第一集群密钥对第一会话密钥进行加密而得到，所述第一会话密钥是所述第一可信计算单元与用户建立的第一可信通道所对应的数据加密密钥；

集群确定模块，配置为确定所述第一可信计算单元所属的第一可信计算集群，所述第一可信计算集群中的每个可信计算单元均维护有所述第一集群密钥；

15 第一传递模块，配置为将所述第一加密密钥传递给所述第一可信计算集群中的第二可信计算单元，以使得所述第二可信计算单元根据其维持的第一集群密钥对所述第一加密密钥进行解密以得到所述第一会话密钥，从而基于所述第一会话密钥而加入到所述第一可信通道中。

16. 根据权利要求 15 所述的装置，还包括，

20 会话标识分配模块，配置为响应于所述第一可信计算单元针对所述第一可信通道的标识请求消息，为所述第一可信通道分配第一会话标识；

第一列表添加模块，配置为将所述第一可信计算单元添加到与所述第一会话标识对应的第一可信计算单元列表。

17. 根据权利要求 16 所述的装置，其中所述第一通知还包括所述第一会话标识，

25 所述第一传递模块还配置为，将所述第一会话标识传递给所述第二可信计算单元；以及

所述第一列表添加模块还配置为，将所述第二可信计算单元添加到所述第一可信计算单元列表中。

18. 根据权利要求 15 所述的装置，其中所述集群确定模块配置为，

30 利用维护的集群信息表，确定所述第一可信计算单元所属的第一可信计算集群，以及所述第一可信计算集群中包含的各个可信计算单元。

19. 根据权利要求 15 所述的装置, 其中所述第一传递模块还配置为:

将所述第一加密密钥传递给所述第一可信计算集群中的第三可信计算单元, 以使得所述第三可信计算单元根据其维持的第一集群密钥对所述第一加密密钥进行解密以得到所述第一会话密钥, 从而基于所述第一会话密钥而加入到所述第一可信通道中。

- 5 20. 一种在用户和可信计算集群之间重建可信通道的装置, 所述装置部署在第四可信计算单元中, 所述第四可信计算单元已与用户建立第二可信通道, 所述第四可信计算单元归属于预先建立的第二可信计算集群, 所述第二可信计算集群中的每个可信计算单元均维护有共同的第二集群密钥, 且所述第四可信计算单元预先向集群管理器注册有所归属的所述第二可信计算集群的信息, 并从所述集群管理器获取有与所述第二可信通道对应的第二会话标识, 所述装置包括:

密钥更新模块, 配置为响应于针对第二可信通道的密钥更新请求, 与所述用户协商出针对所述第二可信通道的第二会话密钥, 所述第二会话密钥用于替代所述第二可信通道的原有密钥, 对传输的数据进行加密;

- 15 第二加密模块, 配置为利用所述第二集群密钥对所述第二会话密钥进行加密, 得到第二加密密钥;

第二通知发送模块, 配置为向所述集群管理器发出第二通知, 其中包含所述第二加密密钥和所述第二会话标识, 以使得所述集群管理器将所述第二加密密钥传递给与所述第二会话标识相关的其他可信计算单元。

- 20 21. 一种在用户和可信计算集群之间重建可信通道的装置, 所述装置部署在集群管理器中, 所述集群管理器用于管理至少一个预先建立的可信计算集群, 所述装置包括:

- 第二通知接收模块, 配置为从第四可信计算单元接收第二通知, 所述第四可信计算单元归属于预先建立的第二可信计算集群, 所述第二可信计算集群中的每个可信计算单元均维护有共同的第二集群密钥, 所述第二通知中包括第二会话标识和第二加密密钥, 所述第二会话标识对应于所述第四可信计算单元与用户已经建立的第二可信通道, 所述
25 第二加密密钥是利用所述第二集群密钥对第二会话密钥进行加密而得到, 所述第二会话密钥是针对所述第二可信通道的更新密钥;

第二列表获取模块, 配置为根据所述第二会话标识, 获取加入到所述第二可信通道的第二可信计算单元列表, 所述第二可信计算单元列表包括所述第四可信计算单元以及同属于所述第二可信计算集群的至少一个其他可信计算单元;

- 30 移除模块, 配置为将所述至少一个其他可信计算单元的每一个, 均从所述第二可信计算单元列表中移除;

第二传递模块，配置为将所述第二加密密钥传递给所述至少一个其他可信计算单元中的第五可信计算单元，以使得所述第五可信计算单元根据其维持的第二集群密钥对所述第二加密密钥进行解密以得到所述第二会话密钥，从而基于所述第二会话密钥而重新加入到所述第二可信通道中。

- 5 22. 根据权利要求 21 所述的装置，还包括第二列表添加模块，配置为，在所述第二传递模块将所述第二加密密钥传递给所述至少一个其他可信计算单元中的第五可信计算单元之后，将所述第五可信计算单元添加到所述第二可信计算单元列表中。

23. 一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行权利要求 1-11 中任一项的所述的方法。

- 10 24. 一种计算设备，包括存储器和处理器，其特征在于，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 1-11 中任一项所述的方法。