

权利要求书

- 1、一种建立可信计算集群的方法，用于将 N 个可信计算单元形成可信计算集群；
所述方法包括：
- 将所述 N 个可信计算单元划分为多个分组，使得各个分组包括的可信计算单元的数量不大于 K+1，其中，K 为每个可信计算单元至多同时与之进行信任认证的可信计算单元的数目；
- 在每个分组中指定一个第一可信计算单元，使得各个分组中的各个第一可信计算单元并行地与同分组的其他可信计算单元进行单元间信任认证；
- 在所述多个分组之间，并行进行组间信任认证，从而获得经过信任认证的 N 个可信计算单元；
- 在所述经过信任认证的可信计算单元中，传播秘密信息，使得经过信任认证的可信计算单元获得相同的秘密信息，以形成可信计算集群。
- 2、根据权利要求 1 所述的方法，其中，所述单元间信任认证包括：
- 两个可信计算单元双方均执行以下步骤，以相互进行信任认证：
- 从对方可信计算单元获取其单元认证报告，将其发送到第三方认证机构进行认证；
- 将自身的单元认证报告发送给对方可信计算单元，以供其发送到所述第三方认证机构进行认证。
- 3、根据权利要求 1 所述的方法，其中，在所述多个分组之间，并行进行组间信任认证，包括：
- 在所述多个分组形成的分组序列中，并行使得每个分组与该分组在所述分组序列中的相邻分组进行组间信任认证。
- 4、根据权利要求 1 所述的方法，其中，在所述多个分组之间，并行进行组间信任认证，包括：
- 在所述多个分组中，使得至少一个分组同时与其他至多 K 个分组进行组间信任认证。
- 5、根据权利要求 1 到 4 中任一项的方法，其中，所述组间信任认证包括：
- 在进行组间信任认证的每个分组中指定一个第二可信计算单元，使得各个第二可信计算单元之间进行单元间信任认证。
- 6、根据权利要求 1 所述的方法，其中，所述在经过信任认证的所述 N 个可信计算单元中传播秘密信息，包括：
- 在所述 N 个可信计算单元中指定一个第三可信计算单元，将第三可信计算单元具有的第一数据指定为所述秘密信息，使得第三可信计算单元分别向 M 个可信计算单元发

送所述秘密信息，其中 M 不超过每个可信计算单元至多同时向其发送秘密信息的可信计算单元的数目。

7、根据权利要求 6 所述的方法，其中，所述在经过信任认证的所述 N 个可信计算单元中传播秘密信息，包括：

- 5 使得具有所述秘密信息的多个可信计算单元中的每个可信计算单元，分别向不具有所述秘密信息的多个可信计算单元发送所述秘密信息。

8、根据权利要求 1 所述的方法，其中，所述秘密信息是集群秘钥。

9、一种建立可信计算集群的装置，用于将 N 个可信计算单元形成可信计算集群；所述装置包括：

- 10 分组单元，用于将所述 N 个可信计算单元划分为多个分组，使得各个分组包括的可信计算单元的数量不大于 $K+1$ ，其中， K 为每个可信计算单元至多同时与之进行信任认证的可信计算单元的数目；

第一认证单元，用于在每个分组中指定一个第一可信计算单元，使得各个分组中的各个第一可信计算单元同时并行地与同分组的其它可信计算单元进行单元间信任认证；

- 15 第二认证单元，用于在所述多个分组之间，同时并行进行组间信任认证，从而获得经过信任认证的 N 个可信计算单元；

传输单元，用于在所述经过信任认证的 N 个可信计算单元中，传播秘密信息，使得所述 N 个可信计算单元获得相同的秘密信息，以形成可信计算集群。

10、根据权利要求 9 所述的装置，其中，所述单元间信任认证包括：

- 20 两个可信计算单元双方均执行以下步骤，以相互进行信任认证：

从对方可信计算单元获取其单元认证报告，将其发送到第三方认证机构进行认证；

将自身的单元认证报告发送给对方可信计算单元，以供其发送到所述第三方认证机构进行认证。

11、根据权利要求 9 所述的装置，其中，所述第二认证单元具体用于：

- 25 在所述多个分组形成的分组序列中，并行使得每个分组与该分组在所述分组序列中的相邻分组进行组间信任认证。

12、根据权利要求 9 所述的装置，其中，所述第二认证单元具体用于：

在所述多个分组中，使得至少一个分组同时与其他至多 K 个分组进行组间信任认证。

13、根据权利要求 9 到 12 中任一项的装置，其中，所述组间信任认证包括：

- 30 在进行组间信任认证的每个分组中指定一个第二可信计算单元，使得各个第二可信计算单元之间进行单元间信任认证。

14、根据权利要求 9 所述的装置，其中，所述传输单元具体用于：

在所述 N 个可信计算单元中指定一个第三可信计算单元，将第三可信计算单元具有的第一数据指定为所述秘密信息，使得第三可信计算单元同时分别向 M 个可信计算单元发送所述秘密信息，其中 M 不超过每个可信计算单元至多同时向其发送秘密信息的

5 可信计算单元的数目 H。

15、根据权利要求 14 所述的装置，其中，所述传输单元具体用于：

使得具有所述秘密信息的多个可信计算单元中的每个可信计算单元，同时分别向不具有所述秘密信息的多个可信计算单元发送所述秘密信息。

16、根据权利要求 9 所述的装置，其中，所述秘密信息是集群密钥。

10 17、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 至 8 中任一项的所述的方法。

18、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 至 8 中任一项所述的方法。