

一种建立可信计算集群的方法和装置

技术领域

[01] 本说明书实施例涉及可信计算集群领域，具体地，涉及一种建立可信计算集群的方法和装置。

5 背景技术

[02] 为了计算和数据传输的安全，常常使用可信计算单元进行可信计算和数据处理。可信计算单元可以保证其中的代码执行是安全的，外界（包括操作系统或驱动等）都无法获取其内部运行时内存等秘密。初始状态，每个可信计算单元并不可信，无法保证各可信计算单元之间传播的信息不被泄露。为保证信息传输的安全性，构建可信计算集群，

10 即各个可信计算单元建立信任关系，并协商得到一个共同的加密密钥。当多个可信计算单元拥有相同的密钥时，认为该多个可信计算单元构成了一个逻辑上的可信计算集群；其中，密钥除了通信的双方，其他任何可信计算单元无法破解。

[03] 当所要建立的可信计算集群中涉及的可信计算单元的数目庞大时，采用传统方式建立可信计算集群的耗时会很长，因此需要寻找新的方法来建立可信计算集群。

15 发明内容

[04] 本申请提供了一种建立可信计算集群的方法和装置，缩短了建立可信计算集群的时间。

[05] 第一方面，提供了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；该方法包括：

20 [06] 将 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；

[07] 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他可信计算单元进行单元间信任认证；

25 [08] 在多个分组之间，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；

[09]在经过信任认证的 N 个可信计算单元中,传播秘密信息,使得 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]在一个实施例中,单元间信任认证包括:

[11]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:

5 [12]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;

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

[14]在一个实施例中,在多个分组之间,同时并行进行组间信任认证,包括:

10 [15]在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分组序列中的相邻分组进行组间信任认证。

[16]在一个实施例中,在多个分组之间,同时并行进行组间信任认证,包括:

[17]在多个分组中,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。

[18]在一个实施例中,组间信任认证包括:

15 [19]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。

[20]在一个实施例中,在经过信任认证的 N 个可信计算单元中传播秘密信息,包括:

20 [21]在 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 H。

[22]在一个实施例中,在经过信任认证的 N 个可信计算单元中传播秘密信息,包括:

[23]使得具有秘密信息的多个可信计算单元中的每个可信计算单元,同时分别向不具有秘密信息的多个可信计算单元发送秘密信息。

[24]在一个实施例中,秘密信息是集群秘钥。

25 [25]第二方面,提供了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;该装置包括:

[26]分组单元,用于将 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；

[27] 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；

- 5 [28] 第二认证单元，用于在多个分组之间，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；

[29] 传输单元，用于在经过信任认证的 N 个可信计算单元中，传播秘密信息，使得 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。

[30] 在一个实施例中，单元间信任认证包括：

- 10 [31] 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：

[32] 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；

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

[34] 在一个实施例中，第二认证单元具体用于：

- 15 [35] 在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分组序列中的相邻分
组进行组间信任认证。

[36] 在一个实施例中，第二认证单元具体用于：

[37] 在多个分组中，使得至少一个分组同时与其它至多 K 个分组进行组间信任认证。

[38] 在一个实施例中，组间信任认证包括：

- 20 [39] 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。

[40] 在一个实施例中，传输单元具体用于：

[41] 在 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秘
25 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 H 。

[42] 在一个实施例中，传输单元具体用于：

[43]使得具有秘密信息的多个可信计算单元中的每个可信计算单元，同时分别向不具有秘密信息的多个可信计算单元发送秘密信息。

[44]在一个实施例中，秘密信息是集群秘钥。

[45]第三方面，提供了一种计算机可读存储介质，其上存储有计算机程序，当计算机程序在计算机中执行时，令计算机第一方面的的方法。

[46]第四方面，提供了一种计算设备，包括存储器和处理器，其特征在于，存储器中存储有可执行代码，处理器执行可执行代码时，实现第一方面的方法。

[47]基于本说明书实施例提供的建立可信集群的方法和装置，首先，通过将N个可信计算单元划分为多个分组，每个分组包括的可信计算单元的数量不大于K+1；每个分组中指定的一个第一可信计算单元，使得各分组中的各个第一可信计算单元同时并行地与同分组中的其他可信计算单元进行单元间的信任认证；然后多个分组之间同时并行的进行组间信任认证，从而获得经过信任认证的N个可信计算单元；最后，在经过信任认证的N个可信计算单元中传播秘密信息，使得N个可信计算单元获得相同的秘密信息，以形成N个可信计算单元的可信集群。如此，缩短了建立可信集群的时间，提高了建立可信集群的效率。

附图说明

[48]为了更清楚地说明本说明书披露的多个实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书披露的多个实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图。

[49]图1是本说明书实施例提供的一种场景示意图；

[50]图2(a)是一种可信计算单元建立信任认证的认证过程示意图；

[51]图2(b)是一种可信计算单元传输秘钥的传输过程示意图；

[52]图3是实施例提供的一种建立可信计算集群的方法流程示意图；

[53]图4(a)是实施例提供的一种可信计算单元建立信任认证过程的示意图；

[54]图4(b)是实施例提供的另一种可信计算单元建立信任认证过程的示意图；

[55]图5是实施例提供的一种两个可信计算单元之间建立信任认证的流程示意图；

[56]图 6(a)是实施例提供的一种分组之间建立信任认证的过程示意图;

[57]图 6(b)是实施例提供的另一种分组之间建立信任认证的过程示意图;

[58]图 7(a)是实施例提供的另一种分组之间建立信任认证的过程示意图;

[59]图 7(b)是实施例提供的另一种分组之间建立信任认证的过程示意图;

5 [60]图 8(a)是实施例提供的一种可信计算单元传输密钥的过程示意图;

[61]图 8(b)是实施例提供的另一种可信计算单元传输密钥的过程示意图;

[62]图 9 是实施例提供的一种建立可信计算集群的装置结构示意图。

具体实施方式

[63]下面结合附图对本说明书实施例的方案进行描述。

10 [64]图 1 是本申请实施例提供的一种场景示意图。如图 1 所示,将多个可信计算单元(N1、N2、N3...Nn) 构建成一个可信计算集群 Rc, 并使得可信计算单元 N1、N2、N3...Nn 均维护着一个相同的密钥 Ec, 将该密钥 Ec 作为可信计算集群 Rc 的集群密钥, 以便于后续各个可信计算单元之间的秘密数据的传输。可信计算单元之间的数据传输均通过该集群密钥 Ec 来进行加密, 提高了秘密数据传输的安全性。其中, 可信计算集群 Rc 由集
15 群管理器统一管理。

[65]为了将多个可信计算单元形成图 1 所示的可信计算集群, 至少需要以下过程: 首先, 多个可信计算单元之间需要彼此进行信任认证, 确认对方是可信的计算单元, 然后, 需要在可信计算单元之间传播密钥, 从而使得, 彼此经过信任认证的多个可信计算单元维护共同的密钥, 如此形成可信计算集群。

20 [66]根据一种方案, 通过串行方式实现可信计算集群的形成。图 2(a)和图 2(b)示出一种建立可信计算集群的方法过程示意图。图 2(a)和图 2(b)所示的是由中心可信计算单元串行完成可信计算集群的建立。如前所述, 建立可信集群分为两个过程; 在串行建立可信计算集群的方案中, 第一个过程如图 2(a)所示, n 个可信计算单元之间串行建立信任认证; 第二个过程是图 2(b), 在图 2(a)完成 n 个可信计算单元的认证之后, 在 n 个可信计
25 算单元之间串行传播密钥, 以使所有的可信计算单元拥有共同的密钥, 以此构成了一个逻辑上的可信计算集群。

[67]可以理解, 建立可信计算集群的耗时也分为两个部分:

[68]1、可信计算单元之间建立信任认证的耗时；

[69]2、可信计算单元之间传输密钥的耗时。

[70]假设 n 个可信计算单元中任意两个可信计算单元之间完成相互信任认证需要时间 t_1 ，一个可信计算单元可以同时最多与 K 个可信计算单元并行建立信任认证；完成信任认证后，一个可信计算单元将密钥发送至另一个可信计算单元需要时间 t_2 ，一个可信计算单元可以同时最多与 H 个节点并行传输密钥。

[71]那么，如图 2(a)所示，以 $K=1$ 为例进行说明， n 个可信计算单元由中心可信计算单元 N_1 串行与其他可信计算单元完成信任认证，即中心可信计算单元 N_1 与可信计算单元 N_2 建立信任认证，然后再由可信计算单元 N_2 与可信计算单元 N_3 建立信任认证，依次串行建立信任关系，直至 n 个可信计算单元完成信任认证，需要的时间 $T_1=(n-1)*t_1$ 。那么，如果一个可信计算单元同时与 K 个可信计算单元建立可信认证， n 个可信计算单元完成信任认证需要耗时 $T_1=t_1*(n-1)/K$ 。

[72]在 n 个可信计算单元完成信任认证之后，再由中心可信计算单元 N_1 串行传播密钥，如图 2(b)所示，图 2(b)中以 $H=1$ 为例进行说明。即由可信计算单元 N_1 、 N_2 、 N_3 ... 逐个传输密钥，以使 n 个可信计算单元拥有相同的密钥，构成可信计算集群，需要的时间 $T_2=t_2*(n-1)$ 。那么，如果一个可信计算单元同时向 H 个可信计算单元传播密钥时，需要耗时 $T_2=t_2*(n-1)/H$ 。

[73]以此，由中心可信计算单元串行建立可信计算集群的总耗时为：

$$T=T_1+T_2=(n-1)/K*t_1+(n-1)/H*t_2。$$

[74]为了进一步缩短建立可信计算集群的时间，本说明书实施例进一步提供了一种建立可信计算集群的方法和装置。

[75]图 3 是本申请实施例提供的一种建立可信计算集群的方法流程示意图。该方法的执行主体是集群管理器，用于将 N 个可信计算单元形成可信计算集群。如图 3 所示，该方法可以包括以下步骤：

[76]步骤 S101，将 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， $1 \leq K \leq N$ 。

[77]需要理解，该步骤中分组的目的在于，使得每个分组内的可信计算单元之间可以在

一个认证周期 t_1 内完成彼此信任认证, 因此, 分组的依据为可信计算单元的并行认证能力, 即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数目。如果每个可信计算单元至多同时与 K 个其他可信计算单元进行信任认证, 那么, 就使得各个分组中包括的可信计算单元的数目不大于 $K+1$ 。

- 5 [78] 在一个实施例中, 可信计算单元的并行认证能力 K 依赖于其中央处理器 (central processing unit, CPU) 的计算能力。在其他可能的实施例中, 可信计算单元的并行认证能力 K 还可能依赖于其他因素, 例如网络设置, 等等。

[79] 集群管理器可以预先获知每个可信计算单元的最大信任认证数目 K , 据此对 N 个可信计算单元进行分组。

- 10 [80] 在一个实施例中, 集群管理器可以根据每个可信计算单元的唯一标识, 例如编号等, 将 N 个可信计算单元划分成多个分组。

[81] 在一个实施例中, 集群管理器划分的分组可以为均匀大小的分组, 即每个分组中包括相同数量的可信计算单元。

- 15 [82] 在另一实施例中, 集群管理器划分的分组为非均匀大小的分组, 即每个分组中包括不相同数量的可信计算单元, 例如, 一个分组中可以包括 1 个可信计算单元, 一个分组中可以包括 2 个可信计算单元, 另外一个分组中包括 4 个可信计算单元, 等等。

[83] 接着, 在步骤 S102, 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与同分组的其它可信计算单元进行单元间信任认证。

- 20 [84] 集群管理器任意指定各个分组中的一个可信计算单元为第一可信计算单元。进而, 并行执行各个分组中第一可信计算单元与同组中其他可信计算单元的单元间信任认证。

- [85] 如图 4(a) 所示, 以两个分组, 第一个分组中包括 5 个可信计算单元 (N_1 、 N_2 、 N_3 、 N_4 、 N_5), 第二个分组中包括 3 个可信计算单元 (N_6 、 N_7 、 N_8) 为例, 集群管理器指定第一分组中的 N_1 为第一可信计算单元, 指定第二分组中的 N_6 为第一可信计算单元。两个分组同时并行建立信任关系的过程是: 第一分组中的 N_1 分别同时与 N_2 、 N_3 、 N_4 、 N_5 建立信任认证, 与此同时, 第二分组中的 N_6 , 分别同时与 N_7 、 N_8 建立信任认证。由此两个分组同时并行进行上述信任认证, 因此该信任认证过程耗费的时间, 相当于两个可信计算单元建立信任认证的时间, 即一个认证周期 t_1 。

[86] 在另一个实施例中, 各分组中的任一可信计算单元可以同时并行的与同组内的其他可信计算单元分别建立信任认证, 如图 4(b) 所示。图 4(b) 以图 4(a) 中的第一个分组为例

进行说明，分组中的可信计算单元 N1、N2、N3、N4、N5 之间相互进行信任认证。

[87]在一个实施例中，任何两个可信计算单元之间的单元间信任认证，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，如图 5 所示：

5 [88]在一个实施例中，可信计算单元 X 从可信计算单元 Y 获取其单元认证报告（例如包括证书、签名信息等），将其发送到第三方认证机构进行认证，并接收第三方认证机构发送的认证结果。同时，可信计算单元 X 将自身的单元认证报告发送给可信计算单元 Y，以供可信计算单元 Y 将其发送到第三方认证机构进行认证，并接收第三方认证机构发送的认证结果。

10 [89]如果第三方认证机构认证可信计算单元 X 和可信计算单元 Y 的认证结果均为可信认证单元时，可信计算单元 X 和可信计算单元 Y 建立可信关系；如果第三方认证机构认证可信计算单元 X 和可信计算单元 Y 中任意一方的认证结果为不可信认证单元时，可信计算单元 X 和可信计算单元 Y 不建立可信关系。

[90]接着，在步骤 S103，在多个分组之间，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。

15 [91]在完成 S101 和 S102 之后，即完成将 N 个可信计算单元分组，分组内的各个可信计算单元之间同时并行的建立了信任认证之后，集群管理器并行执行分组和分组之间的信任认证。

20 [92]在一个实施例中，集群管理器在执行分组时，为每个分组设置了分组序号，在多个分组之间，同时并行进行组间信任认证时，集群管理器将多个分组构成的序列中，分组序号相邻的分组并行进行组间信任认证，如图 6(a)所示。

[93]在图 6(a)中，以 $K=1$ 为例进行说明。初始状态的 N 个可信计算单元未建立信任认证；在第一个 t_1 时间段内，将 N 个可信计算单元分成多个分组，并使各个分组中的可信计算单元建立了单元间信任认证；在第二个 t_2 时间段内，分组序列号相邻的分组之间建立组间信任认证。

25 [94]在一个实施例中，分组之间建立组间信任认证可以具体为：如图 6(b)所示，首先，集群管理器从每个分组中任意指定一个可信计算单元是第二可信计算单元，在该实施例中，各个分组中指定的第二可信计算单元可以与 S102 中指定的第一可信计算单元是同一个可信计算单元，也可以不是同一个可信计算单元，在该实施例中不作限定。

[95]然后，集群管理器使各个分组中的第二可信计算单元之间建立信任认证，如图 6(b)

所示，每个分组中的第二可信计算单元与相邻分组中的第二可信计算单元建立信任连接。在图 6(b)中以每个分组同时并行的与一个分组建立信任认证为例进行说明的。

[96]可选地，在另一个实施例中，在多个分组之间，同时并行进行组间信任认证，包括：在多个分组中，集群管理器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 换句话讲，多个分组中的某个分组同时并行与 K 个分组进行组间信任认证，如图 7(a)所示。在图 7(a)中仅以 K 为 3 进行说明。

[97]相应的，某个分组同时并行与 K 个分组进行组间信任认证，可以具体是，集群管理器为每个分组指定一个第二可信计算单元，与图 6(b)的情形相同。每个分组指定的一个第二可信计算单元与 S102 中指定的第一可信计算单元可以是同一个可信计算单元，也可以不是同一个可信计算单元，在该实施例中不作限定。在第二个 t_2 时间段内，某个分10 组中的第二可信计算单元同时与 K 个其他分组中的第二可信计算单元建立信任认证，如图 7(b)所示。在图 7(b)中，以 K 为 3 进行说明。

[98]在 S103，分组之间建立信任认证耗费的时间，相当于两个可信计算单元建立信任认证的时间 (t_1)。

15 [99]因此，在 N 个可信计算单元建立信任认证花费的总时间为 $2*t_1$ 。

[100] S104，在经过信任认证的 N 个可信计算单元中，传播秘密信息，使得 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。

[101] 在一个实施例中，集群管理器在 N 个可信计算单元中任意指定一个第三可信计算单元。第三可信计算单元可以是 S102 中集群管理器指定的某一个分组中的第一可信20 计算单元，也可以是除第一可信计算单元之外的任意分组中的任意一个可信计算单元；也可以是 S102 中，集群管理器指定的某一分组中的第二可信计算单元，也可以是除第二可信计算单元之外的任一分组中的任意一个可信计算单元。

[102] 集群管理器将第三可信计算单元具有的第一数据指定为秘密信息，在一个实施例中，秘密信息可以是密钥。在其他实施例中，秘密信息可以是后续需要在可信计算集25 群中维护或传播的其他秘密数据。然后，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秘密信息，其中， M 不超过 H ， H 是每个可信计算单元至多同时向其他可信计算单元发送秘密信息的可信计算单元的最大数目。类似的，并行发送秘密信息的最大数目 H 可以依赖于例如 CPU 处理能力，或者网络设置等。

[103] 经由第三可信计算单元的首次传播，多个可信计算单元中有一部分可信计算单

元具有了上述秘密信息，另一部分还不具有上述秘密信息。在一个实施例中，在经过信任认证的 N 个可信计算单元中传播秘密信息还包括：使得具有秘密信息的多个可信计算单元中的每个可信计算单元，同时分别向不具有秘密信息的多个可信计算单元发送秘密信息，以使得 N 个可信计算单元获得相同的密钥，以形成 N 个可信计算节点的可信计算集群。

[104] 例如，假设 $H=1$ ，两个可信计算单元传输密钥耗时 t_2 ，N 个可信计算单元传输密钥的过程如图 8(a)所示。首先，密钥由可信计算单元 N1 传输给可信计算单元 N2，耗费时间 t_2 ；然后，由可信计算单元 N1 将密钥传输给可信计算单元 N3，同时并行地，由可信计算单元 N2 将密钥传输给可信计算单元 N4，耗费时间 t_2 ；进而，由可信计算单元 N1 将密钥传输给可信计算单元 N5，可信计算单元 N2 将密钥传输给可信计算单元 N6，可信计算单元 N3 将密钥传输给可信计算单元 N7，可信计算单元 N4 将密钥传输给可信计算单元 N8，耗费时间 t_2 ；……，相同的传播方式，获得密钥的各个可信计算单元分别将密钥并行传输给未获取密钥的可信计算单元，直至 N 个可信计算单元获得密钥，以形成 N 个可信计算单元的可信计算集群。

[105] 在 N 个可信计算单元中传输密钥，直至 N 个可信计算单元中的每个可信计算单元均获得密钥，需花费时间： $(\log_{(H+1)} N) * t_2$ 。

[106] 在该实施例中，K 和 H 可以是相同的值，也可以是不同的值，但考虑到每个可信计算单元的 CPU 并行计算能力，在密钥传输过程中，选择 K 和 H 中较小的值（即 $\min(H, K)$ ），作为可同时并行传输密钥的数值，换句话说讲，N 个可信计算单元中的每个可信计算单元可以分别，同时并行的向 $\min(H, K)$ 个可信计算单元发送密钥。这样的话，N 个可信计算单元中传输密钥，直至 N 个可信计算单元中的每个可信计算单元均获得密钥，需要花费时间： $(\log_{(\min(H, K)+1)} N) * t_2$ 。

[107] 由于在第一阶段进行信任认证花费的时间为 $2 * t_1$ ，因此在该实施例中，完成 N 个可信计算单元建立可信计算集群需要的总时间是：

$$T = 2 * t_1 + (\log_{(\min(H, K)+1)} N) * t_2$$

[108] 采用该建立可信计算集群的方法，缩短了建立可信计算集群的时间，提高了建立可信集群的效率。

[109] 在另一实施例中，在 N 个可信计算单元传输密钥时，N 个可信计算单元中的每

- 个节点也可以非均匀并发的向其他未获得密钥的可信计算单元传输密钥。例如：一个可信计算单元最多可以并行发送的数目 $H=4$ ，如图 8(b)所示，在第一个 t_2 时间内，可信计算单元 N1 将密钥分别，同时并行的传输给 4 个可信计算单元（N2、N3、N4 和 N5）；在第二个 t_2 时间内，可信计算单元 N1、N2、N3、N4 和 N5 可以同时并行、分别向未获得密钥的 3 个可信计算单元传输密钥，如 N1 向 N6、N7 和 N8 传输密钥，N2 向 N9、N10、N11 传输密钥，N3 向 N12、N13、N14 传输密钥，N4 向 N15、N16、N17 传输密钥，N5 向 N18、N19、N20 传输密钥，后续获得密钥的可信计算单元 N1 至 N20 可以同时并发的在第三个 t_3 时间内，分别向未获得密钥的（小于等于 4 数量）可信计算单元传输密钥，直至 N 个可信计算单元均获得密钥，构建成 N 个可信计算单元的可信计算集群。
- 10 在传播密钥的过程中，需要耗费 $Q \cdot t_2$ ，其中 $\log_{(\min(H, K)+1)} N < Q < \log_2 N$ 。在该计算建立可信计算集群中最多耗费的时间是大于 $2 \cdot t_1 + (\log_{(\min(H, K)+1)} N) \cdot t_2$ ，且小于 $2 \cdot t_1 + (\log_2 N) \cdot t_2$ 。

[110] 其中， $(\log_2 N) \cdot t_2$ 是 N 个可信计算单元 $H=1$ 并发传播密钥所用的时间，如图 7(a)所示，N 个可信计算单元均获取到密钥所需时间是 $(\log_2 N) \cdot t_2$ 。

- 15 [111] 在一个实施例中，在 N 个可信计算单元中传输密钥时，还可以设定每个可信计算单元的并发传输密钥的 H 值不同，N 个可信计算单元均获得密钥所需要的最多时间是 $(\log_2 N) \cdot t_2$ 。建立可信计算集群的最大总耗时 $T = 2 \cdot t_1 + (\log_2 N) \cdot t_2$ 。相比传统方案，缩短了建立可信计算集群的时间。

- [112] 在另一个实施例中，如果 CPU 的计算能力足够强大时，集群管理器也可以不划分组，直接并行执行 N 个可信计算单元之间的信任认证，可以进一步缩短可信集群建立的时间。

[113] 图 2(a)、图 2(b)至图 8(a)、图 8(b)描述了建立可信计算集群的过程，下面结合图 9 描述本申请实施例提供的装置。

- 20 [114] 如图 9 所述，该装置 900 包括用于将 N 个可信计算单元形成可信计算集群；该装置 900 包括：

[115] 分组单元 901，用于将 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；

- [116] 第一认证单元 902, 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他可信计算单元进行单元间信任认证;
- [117] 第二认证单元 903, 还用于在多个分组之间, 同时并行进行组间信任认证, 从而
- 5 获得经过信任认证的 N 个可信计算单元;
- [118] 传输单元 904, 用于在经过信任认证的 N 个可信计算单元中, 传播秘密信息, 使得 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。
- [119] 可选地, 在一个实施例中, 单元间信任认证包括:
- [120] 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:
- 10 [121] 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;
- [122] 将自身的单元认证报告发送给对方可信计算单元, 以供其发送到第三方认证机构进行认证。
- [123] 在一个实施例中, 第二认证单元 903 具体用于:
- 15 [124] 在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分组序列中的相邻分组进行组间信任认证。
- [125] 可选地, 在另一个实施例中, 第二认证单元 903 具体用于:
- [126] 在多个分组中, 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。
- [127] 进一步的, 在一个实施例中, 组间信任认证包括:
- 20 [128] 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。
- [129] 在一个实施例中, 传输单元 904 具体用于:
- [130] 在 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
- 25 送秘密信息, 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 H 。
- [131] 在一个实施例中, 传输单元 904 具体用于:

[132] 使得具有秘密信息的多个可信计算单元中的每个可信计算单元，同时分别向不具有秘密信息的多个可信计算单元发送秘密信息。

[133] 可选地，在一个实施例中，秘密信息是集群秘钥。

5 [134] 通过以上装置，将N个可信计算单元形成可信计算集群。其中，这N个可信计算单元必须首先进行双向的彼此身份认证，在双方认证均通过的情况下，才进行秘钥传输，使得N个可信计算单元均拥有相同的秘钥作为集群秘钥。

10 [135] 同时，采用图3中的方法，先将N个可信计算单元分组，同时并行的建立每个分组内各个可信计算单元之间的信任认证，再同时并行的建立各个分组之间的信任认证，形成经过信任认证的N个可信计算单元；之后，再在N个可信计算单元之间传播秘密信息，以使N个可信计算单元均获得秘密信息，得到N个可信计算单元的可信计算集群，缩短了建立可信计算集群的时间。

[136] 本申请实施例还提供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，令计算机执行结合图3所描述的方法。

15 [137] 本申请实施例还提供一种计算设备，包括存储器和处理器，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，实现结合图3所述的方法。

[138] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本说明书披露的多个实施例所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

20 [139] 以上所述的具体实施方式，对本说明书披露的多个实施例的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本说明书披露的多个实施例的具体实施方式而已，并不用于限定本说明书披露的多个实施例的保护范围，凡在本说明书披露的多个实施例的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本说明书披露的多个实施例的保护范围之内。

25