

在用户和可信计算集群之间建立可信通道的方法及装置

技术领域

[01] 本说明书一个或多个实施例涉及安全计算领域，尤其与可信计算集群建立可信通道的方法和装置。

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。其中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内部的运行时内存等秘密。

[03] 在用户设备与可信计算单元交换要处理的数据之前，通常首先通过协商得到一个共同的加密密钥，该密钥除了通信的双方，其他任何人都不可能破解。双方之间的数据发送均通过该协商得出的密钥来进行加密，如此，我们称为，用户设备与可信计算单元建立了可信通道，可以在该可信通道上安全传输保密数据。

[04] 在许多情况下，用户设备需要与可信计算平台中的多个可信计算单元进行通信。为此，用户设备往往需要与这些可信计算单元分别进行密钥协商，分别单独建立可信通道。当可信平台中的可信计算单元数目增多，数量庞大时，用户接入会变得复杂繁琐，成本高昂。

[05] 因此，希望能有改进的方案，安全有效，且快速便捷地在用户与可信计算平台之间建立可信通道。

发明内容

[06] 本说明书一个或多个实施例描述了建立和重建可信通道的方法及装置，从而使得用户可以与整个可信计算集群，简单又安全地建立可信通道。

[07] 根据第一方面，提供了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：

- [08] 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；
- [09] 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；
- [10] 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
5 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。
- [11] 根据一个实施例，通过以下方式与用户协商出第一会话密钥：
- [12] 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。
- 10 [13] 在一个实施例中，在向所述集群管理器发出第一通知之前，方法还包括：
- [14] 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；
- [15] 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；
- [16] 将所述第一会话标识包含在所述第一通知中。
- [17] 根据第二方面，提供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
15 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：
- [18] 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；
- 20 [19] 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；
- [20] 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。
- 25 [21] 根据一种实施方式，上述方法还包括：
- [22] 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；

[23] 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。

[24] 在一个实施例中，所述第一通知还包括第一会话标识，并且，所述方法还包括：
5 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。

[25] 根据一种事实方式，集群管理器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。

[26] 在一个实施例中，集群管理器还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
10 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。

[27] 根据第三方面，提供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
15 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：

[28] 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
20 输的数据进行加密；

[29] 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；

[30] 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。

25 [31] 根据第四方面，提供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：

[32] 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;

- 5 [33] 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;

[34] 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;

- 10 [35] 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。

- [36] 在一个实施例中, 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。

- [37] 根据第五方面, 提供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:

[38] 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;

[39] 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;

- 25 [40] 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。

[41] 根据第六方面, 提供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:

[42] 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;

[43] 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;

[44] 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。

[45] 根据第七方面, 提供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:

[46] 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;

[47] 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;

[48] 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。

[49] 根据第八方面, 提供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:

[50] 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
- 5 密钥是针对所述第二可信通道的更新密钥；
- [51] 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；
- [52] 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
- 10 信计算单元列表中移除；
- [53] 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。
- 15 [54] 根据第九方面，提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行第一方面到第四方面的方法。
- [55] 根据第十方面，提供了一种计算设备，包括存储器和处理器，其特征在于，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，实现第一方面到第四
- 20 [56] 通过本说明书实施例提供的方法和装置，当用户想要与可信计算集群建立可信通道时，用户仅需要与该集群中的任意一个可信计算单元协商出会话密钥，建立可信通道。接着，集群管理器会将加密的会话密钥在可信计算集群中传播，从而使得集群中的其他可信计算单元获取到会话密钥，加入到该可信通道。于是，用户与整个可信计算集群建立起可信通道。在这个过程中，用户不需要依次单独与各个可信计算单元协商和通信，
- 25 也不需要关注可信计算集群的集群细节，对用户来说，建立可信通道的过程变得非常简单和清晰。

附图说明

[57] 为了更清楚地说明本申请实施例的技术方案，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申请的一些实施例，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。

- 5 [58] 图 1 示出根据本说明书一个实施例的可信计算单元、会话、会话节点的关系示意图；
- [59] 图 2 为本说明书披露的一个实施例中可信通道的整个生命周期；
- [60] 图 3 示出根据一个实施例的在用户与可信计算集群之间建立可信通道的示意图；
- [61] 图 4 示出根据一个实施例的在用户与可信计算集群之间重建可信通道的流程图；
- [62] 图 5 示出根据一个实施例的在用户与可信计算集群之间重建可信通道的流程图；
- 10 [63] 图 6 示出根据一个实施例的用于建立可信通道的建立装置的示意性框图；
- [64] 图 7 示出根据一个实施例的用于建立可信通道的建立装置的示意性框图；
- [65] 图 8 示出根据一个实施例的用于重建可信通道的重建装置的示意性框图；
- [66] 图 9 示出根据一个实施例的用于重建可信通道的重建装置的示意性框图。

具体实施方式

- 15 [67] 下面结合附图，对本说明书提供的方案进行描述。
- [68] 根据本说明书实施例的方案，可以在用户与可信计算集群之间，安全而快速便捷地建立可信通道。上述可信计算集群可以是预先建立的集群，其中包括多个可信计算单元。可信计算单元可以是具有一定隔离能力从而保证计算安全性的计算模块或计算设备，例如是可信的计算容器 enclave，比如采用 SGX 或 Trust Zone 等技术而实现。
- 20 [69] 多个可信计算单元通过互相认证身份，可以形成一个可信计算集群。在建立可信计算集群的过程中，各个可信计算单元会通过密钥协商等方式，而维护一个共同的集群密钥，这是本方案实施的前提和要求。
- [70] 根据本说明书中的实施例，希望统一建立和维护用户与整个可信集群之间的可信通道，如此避免用户与各个可信计算单元之间单独建立通道的繁琐。
- 25 [71] 如果用户与可信计算集群建立起可信通道，则意味着用户与可信计算集群建立了可信关系。为了更清楚的进行描述，引入“会话（session）”的概念，来表示这种可信

关系。也就是说,在本文中,会话可以认为是用户与可信计算集群建立的可信通道关系。

[72] 一个可信计算集群可以与多个用户建立多个可信关系,那就意味着该可信计算集群可以对应多个可信通道,即多个会话。

[73] 如前所述,为了在用户和可信计算集群之间进行安全数据传输,通信双方会协商
5 交换一个加密密钥,本文中将该密钥称为会话密钥。会话密钥与可信通道相对应,用于对通过该可信通道传输的数据进行加解密。

[74] 在以上会话的概念的基础上,结合会话密钥,可以引申出会话节点的概念,用来表示可信计算集群中的可信计算单元在每个会话内对应的实体。由于一个可信计算集群可以有多个会话,因此每个可信计算单元可以对应多个会话节点。

10 [75] 从会话的角度来说,一个会话可以对应一个或者多个会话节点。会话节点 N 是否加入了某个会话 S 的判断标准是,该会话节点 N 是否拥有会话 S 对应的正确的会话密钥 k。若会话节点 N 拥有正确的会话密钥 k,则认为会话节点 N 加入了会话 S;若会话节点 N 没有正确的会话密钥 k,则认为会话节点 N 尚未加入会话 S。

[76] 图 1 示出根据本说明书一个实施例的可信计算单元、会话、会话节点的关系示意图。
15 在图 1 中,假定某个可信计算集群包括 5 个可信计算单元,分别记为 A, B, C, D, E。另外,该可信计算集群具有 3 个会话,分别对应于与用户 U1, U2 和 U3 建立的可信通道 1, 通道 2 和通道 3。

[77] 在图 1 中,纵向示出各个可信计算单元与会话节点的关系。例如,可信计算单元 A
20 包括分别与会话 1,2,3 对应的会话节点 A-1, A-2 和 A-3;可信计算单元 B 包括分别与会话 1,2,3 对应的会话节点 B-1, B-2 和 B-3。

[78] 图 1 的横向示出各个会话与会话节点的关系。例如,会话 1 包括分别与计算单元 A, B, C, D, E 对应的会话节点 A-1, B-1, C-1, D-1, E-1。但是,这些节点是否加入了对应会话,取决于该节点是否具有正确的会话密钥。例如,在图 1 中,会话节点 A-3 由于不具有正确的会话密钥,而没有加入到会话 3。

25 [79] 以上描述了针对用户与可信计算集群的可信通道(或会话)的总体管理架构和构思。在这样的管理架构的基础上,可以安全快速地建立或重建用户与可信计算集群的可信通道。

[80] 图 2 为本说明书披露的一个实施例中可信通道的整个生命周期。如图 2 所示,首先,用户与可信计算集群中的某个可信计算单元(例如单元 A)建立可信通道,即创建

了一个会话。然后，对该会话进行扩张，使得集群中各个对应的会话节点（例如图 1 所示的会话节点）加入到该会话中。这个过程涉及将对应的会话密钥在整个可信计算集群中传播。如此，可信计算集群中各个可信计算单元均得到了会话密钥，于是，各个可信计算单元均加入到会话中，用户就与整个可信计算集群建立了可信通道。

- 5
- [81] 在用户使用该可信通道与可信计算集群通信一段时间后，在一定情况下，可能需要更换会话密钥。这时，需要对该会话进行收缩，将不具有最新会话密钥的会话节点移除该会话，然后再次扩张会话，将最新的会话密钥再次传播到整个集群。于是，用户与整个可信计算集群重建了可信通道。这个过程可以持续进行，直到需要销毁会话。
- [82] 下面具体描述通过会话扩张建立可信通道的过程，以及通过会话收缩再扩张重建可信通道的过程。
- 10

- [83] 图 3 示出根据一个实施例的在用户与可信计算集群之间建立可信通道的示意图。具体地，在图 3 的示例中，示出了在用户 U 与可信计算集群 C1 之间建立可信通道的过程，其中用户 U 代表用户所使用的计算设备或终端，可信计算集群 C1 是预先建立的一个可信计算集群，其中包括多个可信计算单元。在图 3 的示例中，沿用图 1 的例子，假定可信计算集群 C1 包括可信计算单元 A, B, C, D, E。但是可以理解，在其他例子中，可信计算集群可以包括任意数量的可信计算单元。
- 15

- [84] 一般地，通过集群管理器来管理建立的可信计算集群。在一个实施例中，集群管理器维护有集群信息表，其中记录有各个集群中包含的各个可信计算单元的信息。通常来说，在多个可信计算单元成功构建成一个可信计算集群之后，会向集群管理器进行注册，通知集群管理器该可信计算集群的建立。如此，集群管理器根据接收到的注册信息，维护和更新上述集群信息表。表 1 示出集群信息表的一个具体示例。
- 20

表 1: 集群信息表

集群标识	计算单元
C1	A,B,C,D,E
C2	G,H,I,M,N,P
C3	X,Y,Z
.....	

- [85] 需要说明的是，在构建可信计算集群的过程中，各个可信计算单元之间会互相验

证身份, 并进行密钥协商, 最终维护一个共同的集群密钥。这是本方案的前提条件。因此, 在以下说明中, 当提及已经建立的可信计算集群, 就意味着, 该可信计算集群中每个可信计算单元均维护有该集群专有的集群密钥。

[86] 当用户 U 想要与可信计算集群 C1 建立可信通道时, 根据本说明书的实施例, 用户
5 U 可以首先与集群 C1 中的任一个可信计算单元建立可信通道。为了描述简单, 将首先与用户建立可信通道的任一可信计算单元称为第一可信计算单元。在一个具体例子中, 第一可信计算单元例如是可信计算单元 A。

[87] 为此, 在图 3 的步骤 31, 可信计算单元 A 与用户 U 协商出会话密钥 K1, 并建立
10 与用户 U 的可信通道。为了描述的简单, 下文将此可信通道称为第一可信通道。可以理解, 上述会话密钥 K1 针对或对应于第一可信通道, 用于对通过第一可信通道进行传输的数据进行加解密。需要理解, 本文中的“第一”, “第二”等描述, 仅仅为了描述的简单而对相似概念进行区分, 并不具有其他限定作用。

[88] 具体地, 可信计算单元 A 与用户 U 可以通过多种方式进行密钥协商, 从而得到上述会话密钥 K1。

15 [89] 在一个具体例子中, 可信计算单元 A 本地维持有非对称的公钥私钥对(KA-Pub, KA-Pri), 用户 U 也维持有自己的非对称公钥私钥对(KU-Pub, KU-Pri)。为了协商出共同的会话密钥, 可信计算单元 A 与用户 U 彼此交换自己的公钥。也就是, 可信计算单元 A 将其本地的公钥私钥对中的公钥 KA-Pub 发送给用户 U, 并从用户 U 接收到用户的公钥 KU-Pub。

20 [90] 接着, 可信计算单元 A 利用预定的加密算法 SE, 基于本地的公钥私钥对 KA-Pub, KA-Pri, 以及接收到的用户 U 的公钥 KU-Pub, 可以计算得到会话密钥 K1, 即:

[91] $K1 = SE(KA-Pub, KA-Pri, KU-Pub)$

[92] 根据一种实施方式, 用户 U 也利用上述加密算法, 基于用户 U 的公钥私钥对 KU-Pub, KU-Pri, 以及接收到的可信计算单元 A 的公钥 KA-Pub, 计算出一个会话密钥 K1', 即:

25 $K1' = SE(KU-Pub, KU-Pri, KA-Pub)$

[93] 加密算法 SE 可以被设计为, 使得 $SE(KA-Pub, KA-Pri, KU-Pub) = SE(KU-Pub, KU-Pri, KA-Pub)$ 。于是, 可信计算单元 A 将其计算得到的 K1 与用户 U 计算得到的 K1' 互相交换, 在确认 K1 与 K1' 相等的情况下, 完成密钥协商。

[94] 如此,可信计算单元 A 与用户 U 会计算得到相同的会话密钥 K1,从而实现密钥协商。

[95] 在其他实施例中,也可以使用本领域中已知或将来采用的其他密钥协商方式。例如,通信双方交换一些设备信息,根据双方设备信息和约定算法,生成会话密钥;或者, 5 约定其中的一方根据任意方式生成会话密钥,然后通知给另一方,等等。

[96] 在可信计算单元 A 与用户 U 协商得到第一会话密钥 K1 的基础上,在步骤 33,可信计算单元 A 利用所属的可信计算集群 Ci 的集群密钥,以下称为第一集群密钥 E1,对上述第一会话密钥 K1 进行加密,得到一个加密密钥 E1(K1)。如前所述,一个已经构建好的可信计算集群中,每个可信计算单元均维护有该集群专有的集群密钥。对于可信集 10 群集群 C1 来说,其中的每个可信计算单元 A-E,均维护有集群密钥 E1。因此,可信计算单元 A 可以利用其维护的集群密钥 E1,采用预定加密算法,计算得到加密密钥 E1(K1)。

[97] 之后,在步骤 35,可信计算单元 A 向集群管理器发送一个通知,下文称为第一通知,该第一通知中包含上述用集群密钥 E1 加密得到的加密密钥 E1(K1)。

[98] 集群管理器从可信计算单元 A 接收到上述通知后,在步骤 S37,首先确定可信计 15 算单元 A 所归属的可信计算集群的信息。如前所述,在各个可信计算集群建立时,会向集群管理器进行注册,因此集群管理器维护有各个可信计算集群的信息。例如,通过表 1 的集群信息表维护集群的信息。

[99] 在步骤 37,集群管理器可以通过查询维护的集群信息表,确定可信计算单元 A 所 20 归属的可信计算集群,称为第一可信计算集群,还可以确定出该第一可信计算集群中所包含的其他可信计算单元。

[100] 例如,通过查询表 1 的集群信息表,集群管理器可以确定,可信计算单元 A 归属于可信计算集群 C1,该可信计算集群中还包含可信计算单元 B,C,D,E。

[101] 于是,接下来,在步骤 S38,集群管理器将步骤 S35 中收到的第一通知中的加密密 25 钥 E1(K1),传递给上述第一可信计算集群中的其他可信计算单元,在此将上述其他可信计算单元中的任意一个,称为第二可信计算单元,例如,传递给可信计算单元 B。

[102] 如前所述,第一可信计算集群 C1 中的每个可信计算单元,均维护有共同的集群密钥 E1。因此,第二可信计算单元(例如单元 B)接收到加密密钥 E1(K1)后,就可以利用其维护的集群密钥 E1,从加密密钥 E1(K1)中解密得到会话密钥 K1。一旦拥有了正确的会话密钥 K1,第二可信计算单元就可以加入到与用户 U 通信的第一可信通道中。

[103]可以理解,在步骤 S38 之后,或者与步骤 S38 并行地,集群管理器可以将上述加密密钥 E1(K1)逐个传递给第一可信计算集群(C1)中的各个可信计算单元。例如集群管理器还在步骤 S39 将加密密钥 E1(K1)传递给第三可信计算单元,例如单元 C,于是该可信计算单元 C 也加入到第一可信通道中;类似的,可信计算单元 D, E 也可以在接收
5 到集群管理器传递的 E1(K1),进而解密获取到 K1 后加入到第一可信通道中。

[104]在一个实施例中,集群管理器可以将上述加密密钥传递给第一可信计算集群中的所有可信计算单元,以使得每个可信计算单元均加入到第一可信通道中。在另一实施例中,集群管理器也可以根据预先设定的规则,或者根据需要,将上述加密密钥传递给第一可信计算集群中的部分可信计算单元。例如,如果某个可信计算单元出现故障,或者
10 处理性能出现严重下降,或者处理能力不足,集群管理器可以避免将上述加密密钥传递给这样的可信计算单元。其中,可信计算单元的处理状态可以由可信计算单元定期向集群管理器进行报告,也可以由集群管理器统一评估和管理。

[105]通过以上过程可以看到,当用户 U 想要与可信计算集群 C1 建立可信通道时,用户 U 仅需要与集群 C1 中的任意一个可信计算单元(例如单元 A)协商出会话密钥 K1,建
15 立第一可信通道。接着,集群管理器会将加密的会话密钥 E1(K1)在可信计算集群 C1 中传播,从而使得集群中的其他可信计算单元获取到会话密钥,加入到该第一可信通道。于是,可以认为,用户 U 与整个可信计算集群建立了上述第一可信通道。在这个过程中,用户 U 不需要依次单独与各个可信计算单元协商和通信,也不需要关注可信计算集群 C1 的集群细节,对用户来说,建立可信通道的过程变得非常简单和清晰。

20 [106]此外,在集群管理器传播密钥时,传播的是利用集群密钥 E1 进行加密的加密密钥 E1(K1),而该集群密钥 E1 仅仅由对应的可信计算集群中的成员保有和维持。即使在传播过程中,加密密钥 E1(K1)被其他计算设备获取,但是该计算设备由于不具有对应的集群密钥 E1,仍然无法解密获知会话密钥 K1,从而无法加入到第一可信通道的会话中。如此,确保了可信通道建立的安全性。

25 [107]进一步地,在一个实施例中,集群管理器不仅维护建立的集群信息,还以会话的形式管理和维护各个可信通道的状态,也即维护各个会话的状态。下面描述在以上建立第一可信通道的过程中,集群管理器对该第一可信通道对应的会话的管理。

[108]在一种实施方式中,在可信计算单元 A 与用户 U 成功建立上述第一可信通道之后,可信计算单元 A 会向集群管理器发送一个消息,用以通知集群管理器,已新建一个可信
30 通道,请求为该可信通道分配会话标识。

[109] 于是，在前述步骤 31 之后，步骤 35 之前，集群管理器为该第一可信通道分配一个会话标识，在此称为第一会话标识。在具体例子中，会话标识可以体现为会话 id 的形式，例如记为 SID1。

5 [110] 在一个实施例中，集群管理器在分配上述第一会话标识之后，还针对该新建的第一会话标识，建立对应的可信计算单元列表，在此称为第一可信计算单元列表，用于记录加入到对应会话的可信计算单元。

[111] 由于针对第一可信通道的请求消息来自于第一可信计算单元 A，说明该第一可信通道通过可信计算单元 A 创建，可信计算单元 A 已经加入该会话，因此，在一个具体例子中，集群管理器在创建上述第一可信计算单元列表时，就将第一可信计算单元 A 的
10 单元标识添加到该第一可信计算单元列表中。

[112] 然后，集群管理器将该第一会话标识返回给可信计算单元 A。于是，在一个实施例中，可信计算单元 A 还将以上获得的第一会话标识 SID1，包含在上述第一通知中。此时，上述第一通知中包含针对第一可信通道的加密密钥 E1(K1)，以及该第一可信通道对应的会话标识 SID1，两者互相对应关联。

15 [113] 在另一具体例子中，集群管理器在接收到上述第一通知，确认第一可信计算单元 A 已获得针对第一可信通道的会话密钥后，将第一可信计算单元 A 的单元标识添加与第一会话标识对应的第一可信计算单元列表中。

[114] 例如，此时该第一可信计算单元列表可以表示为：

SID1: <A>

20 [115] 接着，在步骤 S38，集群管理器将加密密钥 E1(K1)传递给了第二可信计算单元，例如，可信计算单元 B。在一个实施例中，集群管理器还将该第一会话标识 SID1 也传递给第二可信计算单元，使其知晓所加入的可信通道的会话标识。并且，集群管理器还将第二可信计算单元对应的单元标识添加到上述第一会话标识对应的第一可信计算单元列表中。此时，该第一可信计算单元列表可以表示为：

25 SID1: <A,B>

[116] 在后续集群管理器将加密密钥 E1(K1)又传递给了可信计算单元 C, D, E 之后，类似的，会将这些可信计算单元的单元标识也添加到上述第一可信计算单元列表中。此时，该列表可以表示为：

SID1: <A,B,C,D,E>

[117] 如此，通过会话标识和对应的可信计算单元列表，记录和管理与第一可信通道对应的会话的状态。

[118] 可以理解，与上述与第一可信通道对应的第一会话类似的，集群管理器记录和管理与各个可信通道对应的各个会话的状态。在一个具体例子中，集群管理器通过会话状态表记录各个会话的状态，会话状态表中记录各个会话标识对应的可信计算单元列表。表 2 示出在一个具体例子中的会话状态表。

表 2: 会话状态表

会话标识	可信计算单元列表
SID1	A,B,C,D,E
SID2	A,B,C,D
SID3	G,H,I,M,N,P
.....	

[119] 通过这样的方式，可以在后续会话进行收缩和再次扩张时，持续管理会话状态。下面描述通过会话的收缩和再次扩张，在用户和可信计算集群之间重建可信通道的过程。

[120] 如前所述，用户可以通过与可信计算集群中的任意一个可信计算单元建立可信通道，而与整个可信计算集群建立可信通道，然后通过该可信通道与可信计算集群进行数据通信。在实际操作中，出于安全等原因，在一定条件满足的情况下，例如，满足了预设的密钥更新时间间隔，或者已经使用该可信通道传输了预定量的数据等等，用户需要更换与可信计算集群之间的会话密钥。这个过程我们称为可信通道的重建。

[121] 假定用户已与某个可信计算集群之间建立了可信通道。为了描述的简单，将此处的某个可信计算集群称为第二可信计算集群，建立的可信通道称为第二可信通道。可以理解，此处的第二可信计算集群与前述的第一可信计算集群（例如集群 C1）可以是相同的集群，也可以是不同的集群。相应的，第二可信通道与前述的第一可信通道可以相同，也可以不同。

[122] 当用户想要更换针对第二可信通道的会话密钥时，根据本说明书的一个或多个实施例，用户仅需要通过第二可信计算集群中的任意一个可信计算单元进行会话密钥的更新。为了描述的简单，将该任意一个可信计算单元称为第四可信计算单元。

[123] 图 4 示出根据一个实施例的在用户与可信计算集群之间重建可信通道的流程图，该方法通过上述第四可信计算单元执行。该第四可信计算单元归属于预先建立的第二可信计算集群，第二可信计算集群已与用户建立第二可信通道。

[124] 下面结合具体例子进行说明。假定第二可信计算集群为表 1 所示的集群 C2，其中包含有可信计算单元 G,H,I,M,N,P。第二可信计算集群的信息已预先在集群管理器进行注册。另外，用户已通过与图 3 类似的方式与该可信计算集群 C2 建立有可信通道，该可信通道在本实施例中被称为第二可信通道。可以理解，在建立上述第二可信通道的过程中，集群管理器为该第二可信通道分配有第二会话标识，例如 SID3，并通过例如表 2 的会话状况表，记录有该第二会话标识对应的可信计算单元列表。并且，集群管理器还将该第二会话标识返回给加入到该会话的各个可信计算单元，因此，可信计算单元 G,H,I,M,N,P 均获取有第二可信通道对应的第二会话标识。

[125] 现在假定用户通过其中的任意一个可信计算单元 H，进行会话密钥的更新。为此，通过第四可信计算单元 H，执行以下过程。

[126] 在步骤 41，响应于针对第二可信通道的密钥更新请求，与用户协商出针对该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第二可信通道的原有密钥，对传输的数据进行加密。

[127] 在一个实施例中，上述密钥更新请求由用户发起。例如，用户可以根据自身需要，发出密钥更新请求。

[128] 在另一实施例中，上述密钥更新请求也可以由集群管理器根据预定的管理规则而发起，例如每隔预定时间间隔，要求各个可信通道更新会话密钥。

[129] 响应于针对第二可信通道的密钥更新请求，第四可信计算单元，例如单元 H，与用户协商出针对该可信通道的新的会话密钥，在此称为第二会话密钥，记为 K2。密钥协商的方式与建立可信通道时的方式相类似，不再赘述。可以理解，第二会话密钥用于替代该第二可信通道的原有密钥，对传输的数据进行加密。

[130] 接着，在步骤 43，第四可信计算单元利用所属的第二计算集群的集群密钥，即第二集群密钥，对第二会话密钥进行加密，得到第二加密密钥。

[131] 例如，在第四可信计算单元为单元 H 的情况下，可信计算单元 H 由于归属于第二计算集群 C2，因此维护有 C2 专属的第二集群密钥 E2。于是，可以利用第二集群密钥 E2 对第二会话密钥 K2 加密，得到第二加密密钥 E2(K2)。

[132] 另一方面，如前所述，在第四可信计算单元 H 预先建立或加入第二可信通道时，会从集群管理器获取有与第二可信通道对应的第二会话标识，例如 SID3。因此，在步骤 45，第四可信计算单元可以向集群管理器发出第二通知，其中包含第二加密密钥 E2(K2)和第二会话标识，以使得集群管理器将第二加密密钥传递给与第二会话标识相关的其他可信计算单元。

[133] 接下来有关第二可信通道的会话收缩和再扩张的过程由集群管理器执行。

[134] 图 5 示出根据一个实施例的在用户与可信计算集群之间重建可信通道的流程图，该方法通过集群管理器执行。

[135] 如图 5 所示，在步骤 51，集群管理器从第四可信计算单元接收到第二通知，其中包含第二加密密钥和第二会话标识。其中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，第二加密密钥是利用第二集群密钥对更新得到的第二会话密钥进行加密而得到。例如，与图 4 的步骤 45 对应的，集群管理器从可信计算单元 H 接收到第二通知，其中包含第二加密密钥 E2(K2)和第二会话标识 SID3。

[136] 接着，在步骤 53，集群管理器根据第二会话标识，获取加入到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第四可信计算单元和同属于第二可信计算集群的至少一个其他可信计算单元。

[137] 如前所述，集群管理器用于管理各个预先建立的可信计算集群，例如将其记录为表 1 所示的集群信息表。此外，集群管理器还维护与各个可信计算集群建立起的各个会话的状态。在一个实施例中，集群管理器通过表 2 的会话状态表，记录和维护与各个可信计算集群建立起的各个会话的状态。

[138] 通过上述会话状态表，集群管理器可以查询得到，与第二会话标识对应的第二可信计算单元列表，其中记录有加入到第二可信通道的可信计算单元。参考图 3 的过程，可以理解，与第四可信计算单元一起加入到第二可信通道的单元，必然同属于第二可信计算集群。因此，上述第二可信计算单元列表中包含第四可信计算单元本身，以及同属于第二可信计算集群的至少一个其他可信计算单元。

[139] 例如，对于第二通知中包含的第二会话标识 SID3，集群管理器通过例如表 2 的会话状态表，可以查询获知，与第二会话标识 SID3 对应的第二可信计算单元列表包括：

SID3: <G,H,I,M,N,P>

[140] 其中包括第四可信计算单元 H 自身，以及与单元 H 同属于第二可信计算集群 C2

的其他可信计算单元 G,I,M,N,P。

- [141]接着，在步骤 55，集群管理器将上述至少一个其他可信计算单元的每一个，均从第二可信计算单元列表中移除。也就是说，因为目前仅有第四可信计算单元获得了更新后的会话密钥，因此认为，仅有第四可信计算单元保持在与第二可信通道对应的会话中，
- 5 其他可信计算单元由于密钥未更新，而被移除了该会话。因此，将这些可信计算单元从第二可信计算单元列表中移除。

[142]继续沿用上例进行说明。在步骤 53 确定出与第二会话标识 SID3 对应的第二可信计算单元列表 <G,H,I,M,N,P>之后，在步骤 55，将该列表中除第四可信计算单元 H 之外的各个单元，均进行移除。此时，第二可信计算单元列表更新为：

10 SID3: <H>

- [143]之后，在步骤 57，集群管理器将第二加密密钥传递给上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。
- 15 [144]需要说明的是，上述第五可信计算单元是之前加入到第二可信通道中的、除第四可信计算单元之外的任意一个可信计算单元，因此第五可信计算单元必然是与第四可信计算单元同属于上述第二可信集群，因此也维持有第二集群密钥。如此，在第五可信计算单元接收到第二加密密钥后，就可以利用第二集群密钥对其解密，从而得到第二会话密钥，也就是第二可信通道的新的会话密钥。于是，第五可信计算单元就可以重新加入
- 20 到第二可信通道中。

[145]在一个实施例中，在将第二加密密钥传递给第五可信计算单元后，集群管理器将第五可信计算单元的单元标识再次添加到第二可信计算单元列表中，以表明，第五可信计算单元重新加入到第二会话中。

- [146]按照同样的方式，集群管理器可以将第二加密密钥逐个传递给之前加入到第二可信通道的各个可信计算单元，使得这些可信计算单元再次重新加入到第二可信通道。进一步地，集群管理器还可以将这些可信计算单元的单元标识也添加到第二可信计算单元列表中。
- 25

[147]沿用以上的例子进行说明。在步骤 55 中，将第二可信计算单元列表中除第四可信计算单元 H 之外的各个单元，均进行移除。也就是被移除单元包括 G,I,M,N,P。在步骤

57, 将第二加密密钥 E2(K2)传递给被移除单元中的第五可信计算单元, 例如是单元 G。于是, 可信计算单元 G 可以利用其维护的第二集群密钥 E2 对 E2(K2)进行解密, 得到针对第二可信通道的更新的会话密钥 K2, 从而再次加入该第二可信通道。

[148] 另一方面, 集群管理器还将可信计算单元 G 的单元标识, 添加回第二可信计算单元列表中, 此时, 第二可信计算单元列表更新为:

SID3: <G, H>

[149] 之后, 集群管理器还将第二加密密钥 E2(K2)传递给可信计算单元 I,M,N,P, 使得这些可信计算单元也再次加入第二可信通道。之后, 第二可信计算单元列表又更新为:

SID3: <G,H,I,M,N,P>。

10 [150] 在以上过程中, 在将第二可信计算单元列表中除第四可信计算单元之外的各个单元均进行移除时, 与第二通道对应的第二会话被收缩到最小, 仅包含第四可信计算单元。之后, 随着将第二加密密钥再次进行传播, 第二会话再次扩张。例如, 在收缩阶段, 会话 SID3 中包含的节点收缩至 <H>; 之后, 再次扩张为<G,H,I,M,N,P>。通过以上会话的收缩和再扩张过程, 实现了用户与可信计算集群之间重建可信通道的过程。

15 [151] 在以上过程中, 当用户 U 需要对已经建立的第二可信通道的会话密钥进行更换时, 用户 U 仅需要与集群中的任意一个可信计算单元协商出新的会话密钥 K2, 集群管理器会将之前加入第二可信通道的可信计算单元剔除出对应的第二会话, 然后将加密的会话密钥 E2 (K2) 在集群中再次传播, 使得这些可信计算单元重新加入到该第二会话。整个过程用户不需要依次单独与各个可信计算单元协商和通信, 也不需要关注可信计算集
20 群的集群细节, 重建的过程简单又安全。

[152] 根据另一方面的实施例, 还提供一种在用户和可信计算集群之间建立可信通道的装置。图 6 示出根据一个实施例的用于建立可信通道的建立装置的示意性框图, 且该建立装置部署在可信计算单元中。下面将该可信计算单元称为第一可信计算单元。该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
25 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。如图 6 所示, 该建立装置 600 包括:

[153] 密钥协商模块 61, 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;

[154] 第一加密模块 63, 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;

[155] 第一通知发送模块 65, 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。

5 [156] 根据一个实施例, 所述密钥协商模块 61 配置为:

[157] 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;

[158] 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。

10 [159] 在一个实施例中, 装置 600 还包括标识获取模块 (未示出), 配置为在所述第一通知发送模块 65 向所述集群管理器发出第一通知之前, 执行以下步骤:

[160] 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;

[161] 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;

[162] 将所述第一会话标识包含在所述第一通知中。

15 [163] 根据又一方面的实施例, 还提供一种在用户和可信计算集群之间建立可信通道的装置。图 7 示出根据一个实施例的用于建立可信通道的建立装置的示意性框图, 且该建立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。如图 7 所示, 该建立装置 700 包括:

20 [164] 第一通知接收模块 71, 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;

[165] 集群确定模块 73, 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;

25 [166] 第一传递模块 75, 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。

[167] 根据一个实施例, 上述建立装置 700 还包括 (未示出):

[168] 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；

[169] 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。

5 [170] 进一步的，在一个实施例中，所述第一通知还包括所述第一会话标识，

[171] 所述第一传递模块 75 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；并且，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。

[172] 根据一种实施方式，所述集群确定模块 73 配置为，利用维护的集群信息表，确定
10 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。

[173] 在一个实施例中，所述第一传递模块 75 还配置为：

[174] 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
15 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。

[175] 根据另一方面的实施例，还提供一种在用户和可信计算集群之间重建可信通道的装置。图 8 示出根据一个实施例的用于重建可信通道的重建装置的示意性框图，且该重建装置部署在可信计算单元中。下面将该可信计算单元称为第四可信计算单元。该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。在
20 以上前提下，该重建装置 800 包括：

[176] 密钥更新模块 81，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
25 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；

[177] 第二加密模块 83，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；

[178] 第二通知发送模块 85，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。

5 [179] 根据又一方面的实施例，还提供一种在用户和可信计算集群之间重建可信通道的装置。图 9 示出根据一个实施例的用于重建可信通道的重建装置的示意性框图，且该重建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。如图 9 所示，该重建装置 900 包括：

10 [180] 第二通知接收模块 91，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；

15 [181] 第二列表获取模块 93，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；

[182] 移除模块 95，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；

20 [183] 第二传递模块 97，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。

25 [184] 在一个实施例中，上述重建装置 900 还包括第二列表添加模块（未示出），配置为，在所述第二传递模块 97 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。

[185] 根据另一方面的实施例，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 到图 5 所描述的方法。

[186] 根据再一方面的实施例，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 到图 5 所述的方法。

[187] 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，本申请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
5 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。

[188] 以上所述的具体实施方式，对本申请的目的、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，以上所述仅为本申请的具体实施方式而已，并不用于限定本申请的保护范围，凡在本申请的技术方案的基础之上，所做的任何修改、等同替换、改
10 进等，均应包括在本申请的保护范围之内。