CLAIMS

What is claimed is:

1. A method for establishing a trusted computing cluster, the method comprising:

grouping a plurality of trusted computing units into a plurality of groups, each group of the plurality of groups including a number of trusted computing units not greater than $K+1$, K being a maximum number of trusted computing units with which a trusted computing unit of the plurality of trusted computing units performs trust authentication in parallel;

identifying a first trusted computing unit in each group, and causing first trusted computing units in the plurality of groups to each respectively perform inter-unit trust authentication with other trusted computing units in a same group in parallel;

performing inter-group trust authentication among the plurality of groups in parallel to obtain N trusted computing units on which trust authentication succeeds; and

forming the trusted computing cluster by propagating first secret information in the N trusted computing units on which trust authentication succeeds for the N trusted computing units to each obtain the first secret information.

2. The method according to claim 1, wherein the inter-unit trust authentication includes:

each trusted computing unit of two trusted computing units performing mutual trust authentication through following actions:

obtaining a unit authentication report of other trusted computing unit of the two trusted computing units from the other trusted computing unit, and sending the unit authentication report of the other trusted computing unit to a third-party authentication institution for authentication; and

sending a unit authentication report of the trusted computing unit to the other trusted computing unit for the other trusted computing unit to send the unit

authentication report of the trusted computing unit to the third-party authentication institution for authentication.

3. The method according to claim 1, wherein the performing the inter-group trust authentication among the plurality of groups in parallel includes:

identifying the plurality of groups with a group sequence of the plurality of groups; and

causing the plurality of groups to each perform inter-group trust authentication with a neighboring group in the group sequence of the plurality of groups, in parallel.

4. The method according to claim 1, wherein the performing the inter-group trust authentication among the plurality of groups in parallel includes:

causing at least one group in the plurality of groups to simultaneously perform inter-group trust authentication with a maximum of K other groups.

5. The method according to claim 1, wherein the inter-group trust authentication includes:

identifying a second trusted computing unit in each group of the inter-group trust authentication, and causing second trusted computing units of the plurality of groups to perform inter-unit trust authentication among the second trusted computing units.

6. The method according to claim 1, wherein the propagating the first secret information in the N trusted computing units includes:

identifying a third trusted computing unit in the N trusted computing units, identifying first data of the third trusted computing unit as the first secret information, and causing the third trusted computing unit to separately send the first secret information to M trusted computing units, M not exceeding a maximum number of trusted computing units to which a trusted computing unit simultaneously sends the first secret information.

7. The method according to claim 6, wherein the propagating the first secret information in the *N* trusted computing units includes:

causing each of a plurality of trusted computing units that have the first secret information to separately send the first secret information to a plurality of trusted computing units that do not have the first secret information.

8. The method according to claim 1, wherein the first secret information is a cluster key.

9. An apparatus for establishing a trusted computing cluster, the apparatus comprising:

a grouping unit, configured to group trusted plurality of trusted computing units into a plurality of groups, each group of the plurality of groups including a number of trusted computing units not greater than $K+1$, K being a maximum number of trusted computing units with which a trusted computing unit of the plurality of trusted computing units performs trust authentication in parallel;

a first authentication unit, configured to identify a first trusted computing unit in each group, and cause first trusted computing units in the plurality of groups to each respectively perform inter-unit trust authentication with other trusted computing units in a same group in parallel;

a second authentication unit, configured to perform inter-group trust authentication among the plurality of groups in parallel to obtain *N* trusted computing units on which trust authentication succeeds; and

a transmission unit, configured to form the trusted computer cluster by propagating first secret information in the *N* trusted computing units for the *N* trusted computing units to each obtain the first secret information.

10. The apparatus according to claim 9, wherein the inter-unit trust authentication includes:

each trusted computing unit of two trusted computing units performing mutual trust authentication through following actions:

obtaining a unit authentication report of other trusted computing unit of the two trusted computing units from the other trusted computing unit, and sending the unit authentication report of the other trusted computing unit to a third-party authentication institution for authentication; and

sending a unit authentication report of the trusted computing unit to the other trusted computing unit for the other trusted computing unit to send the unit authentication report of the trusted computing unit to the third-party authentication institution for authentication.

11. The apparatus according to claim 9, wherein the second authentication unit is configured to:

identify the plurality of groups with a group sequence of the plurality of groups; and

cause the plurality of groups to each perform inter-group trust authentication with a neighboring group in the group sequence of the plurality of groups, in parallel.

12. The apparatus according to claim 9, wherein the second authentication unit is configured to:

cause at least one group in the plurality of groups to simultaneously perform inter-group trust authentication with a maximum of K other groups.

13. The apparatus according to claim 9, wherein the inter-group trust authentication includes:

identifying a second trusted computing unit in each group of the inter-group trust authentication, and causing second trusted computing units of the plurality of groups to perform inter-unit trust authentication among the second trusted computing units.

14. The apparatus according to claim 9, wherein the transmission unit is configured to:

identify a third trusted computing unit in the N trusted computing units, identify first data of the third trusted computing unit as the first secret information,

and cause the third trusted computing unit to separately send the first secret information to *M* trusted computing units, *M* not exceeding a maximum number of trusted computing units to which a trusted computing unit simultaneously sends the first secret information.

15. The apparatus according to claim 14, wherein the transmission unit is configured to:

cause each of a plurality of trusted computing units that have the first secret information to separately send the first secret information to a plurality of trusted computing units that do not have the first secret information.

16. The apparatus according to claim 9, wherein the first secret information is a cluster key.

17. A computing device, comprising a memory and a processor, the memory storing executable codes, and the processor executing the executable codes to implement acts including:

grouping a plurality of trusted computing units into a plurality of groups, each group of the plurality of groups including a number of trusted computing units not greater than *K*+1, *K* being a maximum number of trusted computing units with which a trusted computing unit of the plurality of trusted computing units performs trust authentication in parallel;

identifying a first trusted computing unit in each group, and causing first trusted computing units in the plurality of groups to each respectively perform inter-unit trust authentication with other trusted computing units in a same group in parallel;

performing inter-group trust authentication among the plurality of groups in parallel to obtain *N* trusted computing units on which trust authentication succeeds; and

forming a trusted computing cluster by propagating first secret information in the *N* trusted computing units on which trust authentication succeeds for the *N* trusted computing units to each obtain the first secret information.

18. The computing device according to claim 17, wherein the inter-unit trust authentication includes:

each trusted computing unit of two trusted computing units performing mutual trust authentication through following actions:

obtaining a unit authentication report of other trusted computing unit of the two trusted computing units from the other trusted computing unit, and sending the unit authentication report of the other trusted computing unit to a third-party authentication institution for authentication; and

sending a unit authentication report of the trusted computing unit to the other trusted computing unit for the other trusted computing unit to send the unit authentication report of the trusted computing unit to the third-party authentication institution for authentication.

19. The computing device according to claim 17, wherein the performing the inter-group trust authentication among the plurality of groups in parallel includes:

identifying the plurality of groups with a group sequence of the plurality of groups; and

causing the plurality of groups to each perform inter-group trust authentication with a neighboring group in the group sequence of the plurality of groups, in parallel.

20. The computing device according to claim 17, wherein the performing the inter-group trust authentication among the plurality of groups in parallel includes:

causing at least one group in the plurality of groups to simultaneously perform inter-group trust authentication with a maximum of K other groups.