CLAIMS

What is claimed is:

1. A secure multi-party computation method, applicable to any one computing node deployed in a distributed network, a plurality of computing nodes being deployed in the distributed network, and the plurality of computing nodes jointly participating in a secure multi-party computation based on respectively held private data, the computing node being connected to a trusted random source, the method comprising:

obtaining a trusted random number from the trusted random source;

performing an operation on the held private data based on the obtained trusted random number to obtain an operation result, wherein the operation result includes an operation result obtained by performing an irreversible operation on the trusted random number and the held private data, and wherein the held private data cannot be restored by performing an inverse operation on the operation result; and

transmitting at least the trusted random number as a computing parameter to other computing nodes participating in the secure multi-party computation for the other computing nodes to perform the secure multi-party computation based on collected computing parameters transmitted by the computing nodes participating in the secure multi-party computation.

2. The method according to claim 1, further comprising:

creating an audit log corresponding to the trusted random number transmitted by the computing node to the other computing nodes, the audit log recording description information related to the trusted random number.

3. The method according to claim 2, further comprising:

collecting computing parameters transmitted by the other computing nodes participating in the secure multi-party computation, the computing parameters at least comprising random numbers transmitted by the other computing nodes;

performing the secure multi-party computation based on the collected computing parameters; and

creating an audit log corresponding to the random numbers transmitted by the other computing nodes, the audit log comprising description information related to the random numbers.

4. The method according to claim 2 or 3, further comprising:

performing, based on the audit log, a privacy audit on the random number transmitted as a computing parameter by the computing node participating in the secure multi-party computation, to determine whether the random number transmitted as a computing parameter by the computing node is at a risk of privacy leakage; or

transmitting the audit log to a third-party audit node for the audit node to perform a privacy audit on the random number transmitted as a computing parameter by the computing node participating in the secure multi-party computation, to determine whether the random number transmitted as a computing parameter by the computing node is at a risk of privacy leakage.

5. The method according to claim 4, wherein the description information related to the trusted random number comprises a random number generation rule corresponding to the trusted random number; and

the performing, based on the audit log, a privacy audit on the random number transmitted as a computing parameter by the computing node participating in the secure multi-party computation, to determine whether the random number transmitted as a computing parameter by the computing node is at a risk of privacy leakage comprises:

verifying, based on the random number generation rule that is recorded in the audit log and corresponds to the random number transmitted by the computing node participating in the secure multi-party computation, whether the random number matches the trusted random number from the trusted random source; and

if it does, determining that the random number transmitted as the computing parameter by the computing node is at the risk of privacy leakage; or

if it does not, determining that the random number transmitted as the computing parameter by the computing node is not at the risk of privacy leakage.

6. The method according to claim 1, wherein the obtaining a trusted random number from the trusted random source comprises any one of the following:

obtaining a random number generated by the trusted random source as the trusted random number;

obtaining a random number generated by the trusted random source, and using a result obtained by further performing an operation on the random number generated by the trusted random source and a random number generated by the computing node as the trusted random number;

obtaining a random number generated by the trusted random source, and using a random number computed by inputting the random number generated by the trusted random source into a key generation function as the trusted random number; and

obtaining a random number generated by the trusted random source, and using a result obtained by further performing an operation on a random number computed by inputting the random number generated by the trusted random source into a key generation function and a random number generated by the computing node as the trusted random number.

7. A secure multi-party computation apparatus, applicable to any one computing node deployed in a distributed network, a plurality of computing nodes being deployed in the distributed network, and the plurality of computing nodes jointly participating in a secure multi-party computation based on respectively held private data, the computing node being connected to a trusted random source, the apparatus comprising:

an obtaining module, configured to obtain a trusted random number from the trusted random source;

an operation module, configured to perform an operation on the held private data based on the obtained trusted random number to obtain an operation result, wherein the operation result includes an operation result obtained by performing an irreversible operation on the trusted random number and the held private data, and wherein the held private data cannot be restored by performing an inverse operation on the operation result; and

a transmission module, configured to transmit at least the trusted random number as a computing parameter to other computing nodes participating in the secure multi-party computation for the other computing nodes to perform the secure multi-party computation based on collected computing parameters transmitted by the computing nodes participating in the secure multi-party computation.

8. The apparatus according to claim 7, further comprising:

a creation module, configured to create an audit log corresponding to the trusted random number transmitted by the computing node to the other computing nodes, the audit log recording description information related to the trusted random number.

9. The apparatus according to claim 8, further comprising:

a collection module, configured to collect computing parameters transmitted by the other computing nodes participating in the secure multi-party computation, the computing

parameters at least comprising random numbers transmitted by the other computing nodes;

perform the secure multi-party computation based on the collected computing parameters; and

create an audit log corresponding to the random numbers transmitted by the other computing nodes, the audit log comprising description information related to the random numbers.

10. The apparatus according to claim 8 or 9, further comprising:

an audit module, configured to perform, based on the audit log, a privacy audit on the random number transmitted as a computing parameter by the computing node participating in the secure multi-party computation, to determine whether the random number transmitted as a computing parameter by the computing node is at a risk of privacy leakage; or

transmit the audit log to a third-party audit node for the audit node to perform a privacy audit on the random number transmitted as a computing parameter by the computing node participating in the secure multi-party computation, to determine whether the random number transmitted as a computing parameter by the computing node is at a risk of privacy leakage.

11. The apparatus according to claim 10, wherein the description information related to the trusted random number comprises a random number generation rule corresponding to the trusted random number; and

the audit module is further configured to:

verify, based on the random number generation rule that is recorded in the audit log and corresponds to the random number transmitted by the computing node participating in the secure multi-party computation, whether the random number matches the trusted random number from the trusted random source; and

if it does, determine that the random number transmitted as the computing parameter by the computing node is at the risk of privacy leakage; or

if it does not, determine that the random number transmitted as the computing parameter by the computing node is not at the risk of privacy leakage.

12. The apparatus according to claim 7, wherein the obtaining a trusted random number from the trusted random source comprises any one of the following:

obtaining a random number generated by the trusted random source as the trusted random number;

obtaining a random number generated by the trusted random source, and using a result obtained by further performing an operation on the random number generated by the trusted

random source and a random number generated by the computing node as the trusted random number;

obtaining a random number generated by the trusted random source, and using a random number computed by inputting the random number generated by the trusted random source into a key generation function as the trusted random number; and

obtaining a random number generated by the trusted random source, and using a result obtained by further performing an operation on a random number computed by inputting the random number generated by the trusted random source into a key generation function and a random number generated by the computing node as the trusted random number.

13. An electronic device, comprising:

a processor; and

a memory configured to store machine-executable instructions, wherein

by reading and executing the machine-executable instructions stored in the memory and corresponding to control logic of secure multi-party computation, the processor is configured to perform the method according to any one of claims 1-6.