

CLAIMS

What is claimed is:

1. A secure multi-party computation method, applicable to any computing node deployed in a distributed network, a plurality of computing nodes being deployed in the distributed network, 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 key source, the method comprising:

obtaining a trusted key from the trusted key source;

encrypting the held private data based on the obtained trusted key to obtain ciphertext data;

and

transmitting at least the ciphertext data 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 ciphertext data transmitted by the computing node to the other computing nodes, the audit log recording description information related to the ciphertext data.

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 comprising at least ciphertext data obtained by encrypting the private data held 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 ciphertext data transmitted by the other computing nodes, the audit log comprising description information related to the encrypted private data.

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

performing, based on the audit log, a privacy audit on the ciphertext data transmitted by the computing node participating in the secure multi-party computation, to determine whether

the ciphertext data transmitted as a computing parameter by the computing node contains 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 ciphertext data transmitted as a computing parameter by the computing node participating in the secure multi-party computation, to determine whether the ciphertext data transmitted as a computing parameter by the computing node contains a risk of privacy leakage.

5. The method according to claim 4, wherein the description information related to the ciphertext data comprises an encryption key corresponding to the ciphertext data; and

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

verifying whether the encryption key that is recorded in the audit log and corresponds to the ciphertext data transmitted by the computing node participating in the secure multi-party computation matches the trusted key from the trusted key source; and

if it does, determining that the ciphertext data transmitted as the computing parameter by the computing node does not contain the risk of privacy leakage; or

if it does not, determining that the ciphertext data transmitted as the computing parameter by the computing node contains the risk of privacy leakage.

6. The method according to claim 5, wherein a decryption key corresponding to the ciphertext data and cleartext data corresponding to the ciphertext data are further recorded in the audit log corresponding to the ciphertext data transmitted by the computing node to the other computing nodes; and

the method further comprises:

decrypting, based on the decryption key that is recorded in the audit log and corresponds to the ciphertext data transmitted by the computing node participating in the secure multi-party computation, the ciphertext data to obtain cleartext data; and

verifying whether the decrypted cleartext data matches the cleartext data that is recorded in the audit log and corresponds to the ciphertext data; and

if it does, determining that the ciphertext data transmitted as the computing parameter by the computing node does not contain the risk of privacy leakage; or

if it does not, determining that the ciphertext data transmitted as the computing parameter

by the computing node contains the risk of privacy leakage.

7. The method according to claim 1, wherein the trusted key is a random number; and the obtaining a trusted key from the trusted key source comprises any one of the following:
obtaining a random number generated by the trusted key source as the trusted key;
obtaining a random number generated by the trusted key source, and using a result obtained by further performing an operation on the random number generated by the trusted key source and a random number generated by the computing node as the trusted key;
obtaining a random number generated by the trusted key source, and using a random number calculated by inputting the random number into a key generation function as the trusted key; and
obtaining a random number generated by the trusted key source, and using a result obtained by further performing an operation on a random number calculated by inputting the random number into a key generation function and a random number generated by the computing node as the trusted key.

8. A secure multi-party computation apparatus, applicable to any computing node deployed in a distributed network, a plurality of computing nodes being deployed in the distributed network, 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 key source, the apparatus comprising:

an obtaining module, configured to obtain a trusted key from the trusted key source;
an encryption module, configured to encrypt the held private data based on the obtained trusted key to obtain ciphertext data; and
a transmission module, configured to transmit at least the ciphertext data 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.

9. The apparatus according to claim 8, further comprising:
a creation module, configured to create an audit log corresponding to the ciphertext data transmitted by the computing node to the other computing nodes, the audit log recording description information related to the ciphertext data.

10. The apparatus according to claim 9, 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 comprising at least ciphertext data obtained by encrypting the private data held by the other computing nodes; and

a computation module, configured to perform the secure multi-party computation based on the collected computing parameters, wherein

the creation module is further configured to:

create an audit log corresponding to the ciphertext data transmitted by the other computing nodes, the audit log comprising description information related to the encrypted private data.

11. The apparatus according to claim 10, further comprising:

an audit module, configured to perform, based on the audit log, a privacy audit on the ciphertext data transmitted by the computing node participating in the secure multi-party computation, to determine whether the ciphertext data transmitted as a computing parameter by the computing node contains 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 ciphertext data transmitted as a computing parameter by the computing node participating in the secure multi-party computation, to determine whether the ciphertext data transmitted as a computing parameter by the computing node contains a risk of privacy leakage.

12. The apparatus according to claim 10 or 11, wherein the description information related to the ciphertext data comprises an encryption key corresponding to the ciphertext data; and

the audit module is further configured to:

verify whether the encryption key that is recorded in the audit log and corresponds to the ciphertext data transmitted by the computing node participating in the secure multi-party computation matches the trusted key from the trusted key source; and

if it does, determine that the ciphertext data transmitted as the computing parameter by the computing node does not contain the risk of privacy leakage; or

if it does not, determine that the ciphertext data transmitted as the computing parameter by the computing node contains the risk of privacy leakage.

13. The apparatus according to claim 12, wherein a decryption key corresponding to the

ciphertext data and cleartext data corresponding to the ciphertext data are further recorded in the audit log corresponding to the ciphertext data transmitted by the computing node to the other computing nodes; and

the audit module is further configured to:

decrypt, based on the decryption key that is recorded in the audit log and corresponds to the ciphertext data transmitted by the computing node participating in the secure multi-party computation, the ciphertext data to obtain cleartext data;

verify whether the decrypted cleartext data matches the cleartext data that is recorded in the audit log and corresponds to the ciphertext data; and

if it does, determine that the ciphertext data transmitted as the computing parameter by the computing node does not contain the risk of privacy leakage; or

if it does not, determine that the ciphertext data transmitted as the computing parameter by the computing node contains the risk of privacy leakage.

14. The apparatus according to claim 8, wherein the trusted key is a random number; and the obtaining the trusted key from the trusted key source comprises any one of the following:

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

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

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

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

15. 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:

obtain a trusted key from the trusted key source;

encrypt the held private data based on the obtained trusted key to obtain ciphertext data;

and

transmit at least the ciphertext data 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.