

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 method comprising:

generating a computing parameter related to held private data based on a secure multi-party computation algorithm, wherein the computing parameter comprises ciphertext data participating in the secure multi-party computation;

transmitting the 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; ~~and~~

creating an audit log corresponding to the computing parameter, the audit log recording description information related to the computing parameter, wherein the description information comprises a key corresponding to the ciphertext data participating in the secure multi-party computation; and

transmitting the audit log to a third-party audit node for the audit node to perform a privacy audit on the computing parameter transmitted by the computing node participating in the secure multi-party computation, to determine whether the computing parameter transmitted by the computing node contains a risk of privacy leakage by:

verifying, based on the 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 and without decrypting the ciphertext data, whether the key is a known key held by the other computing nodes; and

if yes, determining that the computing parameter transmitted by the computing node contains the risk of privacy leakage; or

if no, determining that the computing parameter transmitted by the computing node does not contain the risk of privacy leakage.

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

collecting computing parameters transmitted by the other computing nodes participating in the secure multi-party computation, and performing the secure multi-party computation

based on the collected computing parameters transmitted by the other computing nodes; and
creating an audit log corresponding to the computing parameters transmitted by the other computing nodes, and storing the audit log, the audit log recording description information related to the computing parameters.

3. The method according to claim 1 or 2, wherein the computing parameter comprises:

a random number participating in the secure multi-party computation; ~~and/or~~
~~ciphertext data participating in the secure multi-party computation.~~

4. The method according to claim 3, wherein the description information related to the computing parameter comprises:

a random number generation rule corresponding to the random number participating in the secure multi-party computation; ~~and/or~~
~~a key corresponding to the ciphertext data participating in the secure multi-party computation.~~

5. The method according to claim 4, further comprising:

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

6. The method according to claim 5, wherein the performing, based on the audit log, a privacy audit on the computing parameter transmitted by the computing node participating in the secure multi-party computation, to determine whether the computing parameter transmitted by the computing node contains 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 is a random number constructed based on the private data held by the other computing nodes; and

if yes, determining that the computing parameter transmitted by the computing node contains the risk of privacy leakage; or

if no, determining that the computing parameter transmitted by the computing node does not contain the risk of privacy leakage.

~~7. The method according to claim 5, wherein~~

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

~~verifying, based on the 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, whether the key is a known key held by the other computing nodes; and~~

~~if yes, determining that the computing parameter transmitted by the computing node contains the risk of privacy leakage; or~~

~~if no, determining that the computing parameter transmitted by the computing node does not contain the risk of privacy leakage.~~

87. 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 apparatus comprising:

a generation module, configured to generate a computing parameter related to held private data based on a secure multi-party computation algorithm, wherein the computing parameter comprises ciphertext data participating in the secure multi-party computation;

a transmission module, configured to transmit the 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; ~~and~~

a creation module, configured to create an audit log corresponding to the computing parameter, the audit log recording description information related to the computing parameter, wherein the description information comprises a key corresponding to the ciphertext data participating in the secure multi-party computation; and

an audit module, configured to: transmit the audit log to a third-party audit node for the

audit node to perform a privacy audit on the computing parameter transmitted by the computing node participating in the secure multi-party computation, to determine whether the computing parameter transmitted by the computing node contains a risk of privacy leakage by:

verifying, based on the 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 and without decrypting the ciphertext data, whether the key is a known key held by the other computing nodes; and

if yes, determining that the computing parameter transmitted by the computing node contains the risk of privacy leakage; or

if no, determining that the computing parameter transmitted by the computing node does not contain the risk of privacy leakage.

~~98~~. The apparatus according to claim ~~87~~, further comprising:

a collection module, configured to: collect computing parameters transmitted by the other computing nodes participating in the secure multi-party computation, and perform the secure multi-party computation based on the collected computing parameters transmitted by the other computing nodes;

the creation module being further configured to:

create an audit log corresponding to the computing parameters transmitted by the other computing nodes, and store the audit log, the audit log recording description information related to the computing parameters.

~~109~~. The apparatus according to claim ~~8-7~~ or ~~98~~, wherein the computing parameter comprises:

a random number participating in the secure multi-party computation; ~~and/or~~
~~ciphertext data participating in the secure multi-party computation.~~

~~110~~. The apparatus according to claim ~~109~~, wherein the description information related to the computing parameter comprises:

a random number generation rule corresponding to the random number participating in the secure multi-party computation; ~~and/or~~

~~a key corresponding to the ciphertext data participating in the secure multi-party computation.~~

~~1211~~. The apparatus according to claim ~~11~~10, further comprising:

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

~~1312~~. The apparatus according to claim ~~12~~11, wherein 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 is a random number constructed based on the private data held by the other computing nodes; and

if yes, determine that the computing parameter transmitted by the computing node contains the risk of privacy leakage;

if no, determine that the computing parameter transmitted by the computing node does not contain the risk of privacy leakage.

~~14~~. ~~The apparatus according to claim 12, wherein the audit module is further configured to:~~

~~verify, based on the 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, whether the key is a known key held by the other computing nodes; and~~

~~if yes, determine that the computing parameter transmitted by the computing node contains the risk of privacy leakage; or~~

~~if no, determine that the computing parameter transmitted by the computing node does not contain the risk of privacy leakage.~~

~~1513~~. An electronic device, comprising:

a processor; and

a memory configured to store machine-executable instructions, wherein

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

~~generate a computing parameter related to held private data based on a secure multi party computation algorithm;~~

~~transmit the 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; and~~

~~create an audit log corresponding to the computing parameter, the audit log recording description information related to the computing parameter.~~