CLAIMS

What is claimed is:

1. A method for multi-party collaborative model updating for privacy protection, wherein the multi-party comprises a server and n participants, the method comprises a plurality of rounds of iterations, and any t^{th} round of iteration comprises:

determining, by each participant i, a corresponding local gradient vector based on a local sample set and current model parameters;

performing, by each participant i, random binarization processing on elements in the local gradient vector by using a randomized algorithm that satisfies differential privacy, to obtain a perturbed gradient vector;

sending, by each participant i, the determined perturbed gradient vector to the server;

aggregating, by the server, n perturbed gradient vectors sent by the n participants, and performing binary representation on elements in a current aggregation result based on plus or minus signs of the elements, to obtain a target gradient vector;

receiving, by each participant i, the target gradient vector from the server, and updating the current model parameters based on the target gradient vector for a next round of iteration; and

after the plurality of rounds of iterations, using, by each participant i, the current model parameters obtained by the participant i as a service prediction model that is updated by the participant i in collaboration with other participants, wherein

the performing binary representation on elements in a current aggregation result based on plus or minus signs of the elements comprises:

superimposing a current error compensation vector on the current aggregation result to obtain a superimposition result; and

performing binary representation on elements in the superimposition result based on plus or minus signs of the elements by using a sign function, wherein

the current error compensation vector is obtained by superimposing, on an error compensation vector in a previous round, a difference between an aggregation result in the previous round and a binary representation result corresponding to the aggregation result in the previous round.

2. The method according to claim 1, wherein the local gradient vector comprises

a first element, and the performing, by each participant i, random binarization processing on elements in the local gradient vector by using a randomized algorithm that satisfies differential privacy comprises:

determining a first probability based on a value of the first element, wherein the first probability is positively correlated with the value of the first element; and

converting the value of the first element to 1 by using the first probability, and converting the value of the first element to −1 by using a second probability, wherein a sum of the first probability and the second probability is 1.

3. The method according to claim 2, wherein the determining a first probability based on a value of the first element comprises:

adding a noise value to the value of the first element; and

determining the first probability based on the value of the first element obtained after the noise value is added and by using a cumulative distribution function with Gaussian distribution.

4. The method according to claim 3, wherein the noise value is obtained through random sampling from Gaussian distribution whose expected value is 0 and variance is σ^2, and σ is determined at least based on products of global sensitivity and proportions of two differential privacy parameters.

5. The method according to claim 4, wherein the two differential privacy parameters are a privacy budget ε and a relaxation term δ.

6. The method according to claim 3, wherein the noise value is obtained through random sampling from Gaussian distribution whose expected value is 0 and variance is σ^2, and σ satisfies the following constraint condition:

a third probability calculated by using the cumulative distribution function for a maximum boundary value of the function determined based on at least σ is close to a fourth probability calculated by using the cumulative distribution function for a minimum boundary value of the function determined based on at least σ.

7. The method according to claim 6, wherein the maximum boundary value of the function is a difference between a first proportion determined based on global sensitivity and σ and a second proportion determined based on a product of a privacy budget ε and σ and the global sensitivity, and the minimum boundary value of the function is a difference between an opposite number of the first proportion and the second proportion.

8. The method according to claim 1, wherein

samples in the local sample set of any participant i are pictures, and the service prediction model is a picture recognition model; or

samples in the local sample set of any participant i are audio, and the service prediction model is an audio recognition model; or

samples in the local sample set of any participant i are text, and the service prediction model is a text recognition model.

9. A method for multi-party collaborative model updating for privacy protection, wherein the multi-party comprises a server and n participants, the method is performed by any participant i in the n participants, the method comprises a plurality of rounds of iterations, and any t^{th} round of iteration comprises:

determining a corresponding local gradient vector based on a local sample set and current model parameters;

performing random binarization processing on elements in the local gradient vector by using a randomized algorithm that satisfies differential privacy, to obtain a perturbed gradient vector;

sending the perturbed gradient vector to the server;

receiving a target gradient vector from the server, wherein the target gradient vector is obtained after the server aggregates n perturbed gradient vectors sent by the n participants, and then performs binary representation on elements in a current aggregation result based on plus or minus signs of the elements;

updating the current model parameters based on the target gradient vector for a next round of iteration; and

after the plurality of rounds of iterations, using the current model parameters obtained by the participant i as a service prediction model that is updated by the participant i in collaboration with other participants, wherein

the performing binary representation on elements in a current aggregation result based on plus or minus signs of the elements comprises:

superimposing a current error compensation vector on the current aggregation result to obtain a superimposition result; and

performing binary representation on elements in the superimposition result based on plus or minus signs of the elements by using a sign function, wherein

the current error compensation vector is obtained by superimposing, on an error compensation vector in a previous round, a difference between an aggregation result in

the previous round and a binary representation result corresponding to the aggregation result in the previous round.

10. A system for multi-party collaborative model updating for privacy protection, comprising a server and n participants, wherein

each participant i is configured to determine a corresponding local gradient vector based on a local sample set and current model parameters;

each participant i is further configured to perform random binarization processing on elements in the local gradient vector by using a randomized algorithm that satisfies differential privacy, to obtain a perturbed gradient vector;

each participant i is further configured to send the determined perturbed gradient vector to the server;

the server is configured to aggregate n perturbed gradient vectors sent by the n participants, and perform binary representation on elements in a current aggregation result based on plus or minus signs of the elements, to obtain a target gradient vector;

each participant i is further configured to receive the target gradient vector from the server, and update the current model parameters based on the target gradient vector for a next round of iteration; and

after the plurality of rounds of iterations, each participant i is further configured to use the current model parameters obtained by the participant i as a service prediction model that is updated by the participant i in collaboration with other participants, wherein the server is further specifically configured to:

superimpose a current error compensation vector on the current aggregation result to obtain a superimposition result; and

perform binary representation on elements in the superimposition result based on plus or minus signs of the elements by using a sign function, wherein

the current error compensation vector is obtained by superimposing, on an error compensation vector in a previous round, a difference between an aggregation result in the previous round and a binary representation result corresponding to the aggregation result in the previous round.

11. The system according to claim 10, wherein the local gradient vector comprises a first element, and each participant i is specifically configured to:

determine a first probability based on a value of the first element, wherein the first probability is positively correlated with the value of the first element; and

convert the value of the first element to 1 by using the first probability, and

converting the value of the first element to −1 by using a second probability, wherein a sum of the first probability and the second probability is 1.

12. The system according to claim 11, wherein each participant i is further specifically configured to:

add a noise value to the value of the first element; and

determine the first probability based on the value of the first element obtained after the noise value is added and by using a cumulative distribution function with Gaussian distribution.

13. The system according to claim 12, wherein the noise value is obtained through random sampling from Gaussian distribution whose expected value is 0 and variance is σ^2, and σ is determined based on at least products of global sensitivity and proportions of two differential privacy parameters.

14. The system according to claim 13, wherein the two differential privacy parameters are a privacy budget ε and a relaxation term δ.

15. The system according to claim 12, wherein the noise value is obtained through random sampling from Gaussian distribution whose expected value is 0 and variance is σ^2, and σ satisfies the following constraint condition:

a third probability calculated by using the cumulative distribution function for a maximum boundary value of the function determined based on at least σ is close to a fourth probability calculated by using the cumulative distribution function for a minimum boundary value of the function determined based on at least σ.

16. The system according to claim 15, wherein the maximum boundary value of the function is a difference between a first proportion determined based on global sensitivity and σ and a second proportion determined based on a product of a privacy budget ε and σ and the global sensitivity, and the minimum boundary value of the function is a difference between an opposite number of the first proportion and the second proportion.

17. The system according to claim 10, wherein

samples in the local sample set of any participant i are pictures, and the service prediction model is a picture recognition model; or

samples in the local sample set of any participant i are audio, and the service prediction model is an audio recognition model; or

samples in the local sample set of any participant i are text, and the service prediction model is a text recognition model.

18. An apparatus for multi-party collaborative model updating for privacy protection, wherein the multi-party comprises a server and n participants, the apparatus is disposed in any participant i in the n participants and is configured to perform a plurality of rounds of iterations, and the apparatus performs any t^{th} round of iteration by using the following units comprised in the apparatus:

a determining unit, configured to determine a corresponding local gradient vector based on a local sample set and current model parameters;

a processing unit, configured to perform random binarization processing on elements in the local gradient vector by using a randomized algorithm that satisfies differential privacy, to obtain a perturbed gradient vector;

a sending unit, configured to send the perturbed gradient vector to the server;

a receiving unit, configured to receive a target gradient vector from the server, wherein the target gradient vector is obtained after the server aggregates n perturbed gradient vectors sent by the n participants, and then performs binary representation on elements in a current aggregation result based on plus or minus signs of the elements; and

an updating unit, configured to update the current model parameters based on the target gradient vector for a next round of iteration, wherein

after the plurality of rounds of iterations, the determining unit is further configured to use the current model parameters obtained by the participant i as a service prediction model that is updated by the participant i in collaboration with other participants, wherein the performing binary representation on elements in a current aggregation result based on plus or minus signs of the elements comprises:

superimposing a current error compensation vector on the current aggregation result to obtain a superimposition result; and

performing binary representation on elements in the superimposition result based on plus or minus signs of the elements by using a sign function, wherein

the current error compensation vector is obtained by superimposing, on an error compensation vector in a previous round, a difference between an aggregation result in the previous round and a binary representation result corresponding to the aggregation result in the previous round.

19. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer program, and when the computer program is executed in a computer, the computer is enabled to perform the method according to any one of

claims 1 to 9.

20. A computing device, comprising a memory and a processor, wherein the memory stores executable code, and when the processor executes the executable code, the method according to any one of claims 1 to 9 is implemented.