

WHAT IS CLAIMED IS:

1. An apparatus for performing machine learning by using data to be exchanged, comprises at least one computing device and at least one storage device storing instructions, wherein the instructions, when executed by the at least one computing device, cause the at least one computing device to perform the following steps:

receiving first primary encryption result data from a first data provider and receiving second primary encryption result data from a second data provider;

transmitting the first primary encryption result data to the second data provider and transmitting the second primary encryption result data to the first data provider;

receiving second secondary encryption result data from the first data provider and receiving first secondary encryption result data from the second data provider; and

obtaining machine learning samples by concatenating the first secondary encryption result data and the second secondary encryption result data, and performing machine learning based on the machine learning samples.

2. The apparatus of claim 1, wherein,

the first primary encryption result data is obtained by the first data provider encrypting first data to be exchanged by using a first encryption function, and the second primary encryption result data is obtained by the second data provider encrypting second data to be exchanged by using a second encryption function, wherein the first data to be exchanged at least partially corresponds to the second data to be exchanged;

the first secondary encryption result data is obtained by the second data provider encrypting the first primary encryption result data by using the second encryption function, and the second secondary encryption result data is obtained by the first data provider encrypting the second primary encryption result data by using the first encryption function.

3. The apparatus of claim 2, wherein each first data record to be exchanged among the first data to be exchanged includes at least identification information and attribute information, and each second data record to be exchanged among the second data to be exchanged includes at least identification information and label information about a machine learning target.

4. The apparatus of claim 2, wherein the first encryption function is a private function of

the first data provider, the second encryption function is a private function of the second data provider, and the first encryption function and the second encryption function constitute one-way commutative private functions.

5. The apparatus of claim 2, wherein the first encryption function is a first power function with a first private big prime number, and the second encryption function is a second power function with a second private big prime number.

6. The apparatus of claim 1, wherein the machine learning samples are machine learning training samples, machine learning test samples, or machine learning prediction samples, and a machine learning executing unit trains a machine learning model, tests the machine learning model, or predicts using the machine learning model based on the machine learning samples.

7. A method for performing machine learning by a computing device using data to be exchanged, comprising:

receiving first primary encryption result data from a first data provider and receiving second primary encryption result data from a second data provider;

transmitting the first primary encryption result data to the second data provider and transmitting the second primary encryption result data to the first data provider;

receiving second secondary encryption result data from the first data provider and receiving first secondary encryption result data from the second data provider; and

obtaining machine learning samples by concatenating the first secondary encryption result data and the second secondary encryption result data, and performing machine learning based on the machine learning samples.

8. The method of claim 7, wherein,

the first primary encryption result data is obtained by the first data provider encrypting first data to be exchanged by using a first encryption function, and the second primary encryption result data is obtained by the second data provider encrypting second data to be exchanged by using a second encryption function, wherein the first data to be exchanged at least partially corresponds to the second data to be exchanged;

the first secondary encryption result data is obtained by the second data provider encrypting the first primary encryption result data by using the second encryption function, and the second secondary encryption result data is obtained by the first data provider

encrypting the second primary encryption result data by using the first encryption function.

9. The method of claim 8, wherein each first data record to be exchanged among the first data to be exchanged includes at least identification information and attribute information, and each second data record to be exchanged among the second data to be exchanged includes at least identification information and label information about a machine learning target.

10. The method of claim 8, wherein the first encryption function is a private function of the first data provider, the second encryption function is a private function of the second data provider, and the first encryption function and the second encryption function constitute one-way commutative private functions.

11. The method of claim 8, wherein the first encryption function is a first power function with a first private big prime number, and the second encryption function is a second power function with a second private big prime number.

12. The method of claim 7, wherein the machine learning samples are machine learning training samples, machine learning test samples, or machine learning prediction samples, and the performing machine learning based on the machine learning samples comprises: training a machine learning model, testing the machine learning model, or predicting using the machine learning model based on the machine learning samples.

13. A data providing apparatus, comprising at least one computing device and at least one storage device storing instructions, wherein the instructions, when executed by the at least one computing device, cause the at least one computing device to perform the following steps:

encrypting first data to be exchanged by using a first encryption function to obtain first primary encryption result data, transmitting the first primary encryption result data to a machine learning executing apparatus, receiving second primary encryption result data from the machine learning executing apparatus, encrypting the second primary encryption result data by using the first encryption function to obtain second secondary encryption result data, and transmitting the second secondary encryption result data to the machine learning executing apparatus;

or, encrypting second data to be exchanged by using a second encryption function to

obtain the second primary encryption result data, transmitting the second primary encryption result data to the machine learning executing apparatus, receiving the first primary encryption result data from the machine learning executing apparatus, encrypting the first primary encryption result data by using the second encryption function to obtain first secondary encryption result data, and transmitting the first secondary encryption result data to the machine learning executing apparatus.

14. The data providing apparatus of claim 13, wherein,
each first data record to be exchanged among the first data to be exchanged includes at least identification information and attribute information;

each second data record to be exchanged among the second data to be exchanged includes at least identification information and label information about a machine learning target.

15. The data providing apparatus of claim 13, wherein the first encryption function is a private function of a first data provider, the second encryption function is a private function of a second data provider, and the first encryption function and the second encryption function constitute one-way commutative private functions.

16. The data providing apparatus of claim 13, wherein the first encryption function is a first power function with a first private big prime number, and the second encryption function is a second power function with a second private big prime number.

17. A data providing method performed by a computing device, comprising:
encrypting first data to be exchanged by using a first encryption function to obtain first primary encryption result data, transmitting the first primary encryption result data to a machine learning executing apparatus, receiving second primary encryption result data from the machine learning executing apparatus, encrypting the second primary encryption result data by using the first encryption function to obtain second secondary encryption result data, and transmitting the second secondary encryption result data to the machine learning executing apparatus;

or, encrypting second data to be exchanged by using a second encryption function to obtain the second primary encryption result data, transmitting the second primary encryption result data to the machine learning executing apparatus, receiving the first primary encryption

result data from the machine learning executing apparatus, encrypting the first primary encryption result data by using the second encryption function to obtain first secondary encryption result data, and transmitting the first secondary encryption result data to the machine learning executing apparatus.

18. The method of claim 17 wherein,

each first data record to be exchanged among the first data to be exchanged includes at least identification information and attribute information;

each second data record to be exchanged among the second data to be exchanged includes at least identification information and label information about a machine learning target.

19. The method of claim 17, wherein the first encryption function is a private function of a first data provider, the second encryption function is a private function of a second data provider, and the first encryption function and the second encryption function constitute one-way commutative private functions.

20. The method of claim 17, wherein the first encryption function is a first power function with a first private big prime number, and the second encryption function is a second power function with a second private big prime number.

21. A system for performing machine learning, comprising:

a first data provider apparatus configured to obtain first primary encryption result data by encrypting first data to be exchanged using a first encryption function;

a second data provider apparatus configured to obtain second primary encryption result data by encrypting second data to be exchanged using a second encryption function, wherein the first data to be exchanged at least partially corresponds to the second data to be exchanged;

a machine learning executing apparatus configured to receive the first primary encryption result data from the first data provider and receive the second primary encryption result data from the second data provider respectively, and transmit the first primary encryption result data to the second data provider and transmit the second primary encryption result data to the first data provider respectively,

wherein the first data provider obtains second secondary encryption result data by

encrypting the second primary encryption result data using the first encryption function, the second data provider obtains first secondary encryption result data by encrypting the first primary encryption result data using the second encryption function, and the machine learning executing apparatus receives the second secondary encryption result data from the first data provider and receives the first secondary encryption result data from the second data provider respectively, and obtains machine learning samples by concatenating the first secondary encryption result data and the second secondary encryption result data, to perform machine learning based on the machine learning samples.

22. The system of claim 21, wherein each first data record to be exchanged among the first data to be exchanged includes at least identification information and attribute information, and each second data record to be exchanged among the second data to be exchanged includes at least identification information and label information about a machine learning target.

23. The system of claim 21, wherein the first encryption function is a private function of the first data provider, the second encryption function is a private function of the second data provider, and the first encryption function and the second encryption function constitute one-way commutative private functions.

24. The system of claim 21, wherein the first encryption function is a first power function with a first private big prime number, and the second encryption function is a second power function with a second private big prime number.

25. The system of claim 21, wherein the machine learning samples are machine learning training samples, machine learning test samples, or machine learning prediction samples, and the machine learning executing apparatus trains a machine learning model, tests the machine learning model, or predicts using the machine learning model based on the machine learning samples.

26. A method for performing machine learning, comprising:
obtaining first primary encryption result data by encrypting first data to be exchanged using a first encryption function, by a first data provider;
obtaining second primary encryption result data by encrypting second data to be exchanged using a second encryption function, by a second data provider, wherein the first

data to be exchanged at least partially corresponds to the second data to be exchanged;

receiving the first primary encryption result data from the first data provider and receiving the second primary encryption result data from the second data provider respectively, and transmitting the first primary encryption result data to the second data provider and transmitting the second primary encryption result data to the first data provider respectively, by a machine learning executing apparatus;

obtaining second secondary encryption result data by encrypting the second primary encryption result data using the first encryption function, by the first data provider;

obtaining first secondary encryption result data by encrypting the first primary encryption result data using the second encryption function, by the second data provider;

receiving the second secondary encryption result data from the first data provider and receiving the first secondary encryption result data from the second data provider respectively, by the machine learning executing apparatus; and

obtaining machine learning samples by concatenating the first secondary encryption result data and the second secondary encryption result data to perform machine learning based on the machine learning samples, by the machine learning executing apparatus.

27. A computer-readable storage medium for performing machine learning by using data to be exchanged, wherein the computer-readable storage medium records computer programs for performing the method of any one of claims 7-12 and 17-20.

28. An apparatus for performing machine learning by using data to be exchanged, comprising:

a primary encryption data receiving unit configured to receive first primary encryption result data from a first data provider and receive second primary encryption result data from a second data provider;

a primary encryption data transmitting unit configured to transmit the first primary encryption result data to the second data provider and transmit the second primary encryption result data to the first data provider;

a secondary encryption data receiving unit configured to receive second secondary encryption result data from the first data provider and receive first secondary encryption result data from the second data provider; and

a machine learning executing unit configured to obtain machine learning samples by concatenating the first secondary encryption result data and the second secondary encryption result data, and perform machine learning based on the machine learning samples.