

CLAIMS

What is claimed is:

1. A data processing method, wherein the method is performed by a data provider, the data provider having first plaintext data, the method comprising

5 obtaining first encrypted data of the first plaintext data, a first key used to decrypt the first encrypted data, and authorization information about the first plaintext data;

 sending a verification request to a data manager, the data manager including a first trusted execution environment;

10 receiving authentication information from the data manager, and performing verification based on the authentication information, the authentication information being generated by the first trusted execution environment;

 when the verification succeeds, securely transmitting the first key and the authorization information to the first trusted execution environment; and providing the

15 first encrypted data to the data manager,

 wherein the authorization information includes at least one code hash value of at least one program allowed to use the first plaintext data and at least one piece of access permission information corresponding to the at least one code hash value, and

 wherein the access permission information is information about a calculation
20 result of the at least one program.

2. A data processing method, wherein the method is performed by a data provider, the data provider having first plaintext data, and the method comprising

 obtaining authorization information about the first plaintext data;

25 sending a verification request to a data manager, the data manager including a first trusted execution environment;

 receiving authentication information from the data manager, and performing verification based on the authentication information, the authentication information being generated by the first trusted execution environment and

30 when the verification succeeds, securely transmitting the first plaintext data and the authorization information to the first trusted execution environment.

wherein the authorization information includes at least one code hash value of at least one program allowed to use the first plaintext data and at least one piece of access permission information corresponding to the at least one code hash value, and

5 wherein the access permission information is information about a calculation result of the at least one program.

3. The method according to claim 1 or 2, wherein the access permission information is a second key, the second key being used to encrypt the corresponding calculation result and being provided by a calculation result user corresponding to the
10 calculation result.

4. The method according to claim 1 or 2, wherein the access permission information is null information.

15 5. The method according to claim 1 or 2, wherein the performing verification based on the authentication information includes: verifying, based on the authentication information, whether the at least one program for data use authorization is installed and is running in the first trusted execution environment.

20 6. The method according to claim 1 or 2, wherein the secure transmission is encrypted transmission.

7. A data processing method, wherein the method is performed by a data manager, the data manager including a first trusted execution environment, the method
25 comprising, at the data manager:

receiving, from a data provider, a verification request;

generating, by the first trusted execution environment, authentication information after receiving the verification request;

30 sending the authentication information to the data provider, wherein the authentication information is used by the data provider for performing a verification to determine whether the first trusted execution environment is a secure execution environment; and

receiving, from the data provider, a first key, authorization information about plaintext data, and first encrypted data in response to a successful verification,

wherein the first encrypted data is obtained after encryption of the plaintext data and the first key used to decrypt the first encrypted data,

wherein the authorization information includes at least one code hash value of at least one program allowed to use the first plaintext data and at least one piece of access permission information corresponding to the at least one code hash value, and
5 wherein the access permission information is information about a calculation result of the at least one program.

8. The method according to claim 7, wherein the first trusted execution
10 environment and the second trusted execution environment are located on one platform or different platforms.

9. The method according to claim 7, wherein the receiving the authentication information from the data user includes: receiving, by using the first trusted execution
15 environment, the authentication information securely transmitted from the second trusted execution environment.

10. The method according to claim 7, wherein the authentication information includes a first code hash value of a first program that is installed and running in the
20 second trusted execution environment, each piece of authorization information including at least one code hash value of at least one program; and the performing verification for each piece of authorization information based on the authentication information and the authorization information includes: verifying, for each piece of authorization information, whether the first code hash value is a code hash value
25 included in the authorization information.

11. The method according to claim 10, wherein each piece of authorization information includes a first code hash value and a second key corresponding to the first code hash value, the second key being used to encrypt a calculation result of the
30 first program and being provided by a calculation result user corresponding to the calculation result; and the method further comprises: for each piece of authorization information, when the verification succeeds, further securely transmitting the second security key to the second trusted execution environment by using the first trusted execution environment.

12. The method according to claim 7, wherein the data manager further includes a data storage module, the at least one piece of encrypted data being stored in the data storage module.

5

13. A data processing apparatus, wherein the apparatus is implemented by a data provider, the data provider having first plaintext data, the apparatus comprising:

an acquisition unit, configured to obtain first encrypted data of the first plaintext data, a first key used to decrypt the first encrypted data, and authorization information
10 about the first plaintext data;

a sending unit, configured to send a verification request to a data manager, the data manager including a first trusted execution environment;

a verification unit, configured to receive authentication information from the data manager, and perform verification based on the authentication information, the authentication information being generated by the first trusted execution environment;
15

a secure transmission unit, configured to: when the verification succeeds, securely transmit the first key and the authorization information to the first trusted execution environment; and

a providing unit, configured to provide the first encrypted data to the data manager,
20

wherein the authorization information includes at least one code hash value of at least one program allowed to use the first plaintext data and at least one piece of access permission information corresponding to the at least one code hash value, and

wherein the access permission information is information about a calculation
25 result of the at least one program.

14. A data processing apparatus, wherein the apparatus is implemented by a data provider, the data provider having first plaintext data, the apparatus comprising:

an acquisition unit, configured to obtain authorization information about the first
30 plaintext data;

a sending unit, configured to send a verification request to a data manager, the data manager including a first trusted execution environment;

a verification unit, configured to receive authentication information from the data manager, and perform verification based on the authentication information, the

authentication information being generated by the first trusted execution environment;
and

a secure transmission unit, configured to: when the verification succeeds,
securely transmit the first plaintext data and the authorization information to the first
5 trusted execution environment,

wherein the authorization information includes at least one code hash value of at
least one program allowed to use the first plaintext data and at least one piece of
access permission information corresponding to the at least one code hash value, and

wherein the access permission information is information about a calculation
10 result of the at least one program.

15 15. The apparatus according to claim 13 or 14, wherein the authorization
information includes at least one code hash value and the at least one code hash value
is at least one code hash value of at least one program allowed to use the first plaintext
data.

20 16. The apparatus according to claim 15, wherein the authorization information
includes at least one piece of access permission information corresponding to the at
least one code hash value and the access permission information is information about
a calculation result of a corresponding program.

25 17. The apparatus according to claim 16, wherein the access permission
information is a second key, the second key being used to encrypt the corresponding
calculation result and being provided by a calculation result user corresponding to the
calculation result.

18. The apparatus according to claim 16, wherein the access permission
information is null information.

30 19. The apparatus according to claim 13 or 14, wherein the verification unit is
further configured to verify, based on the authentication information, whether the at
least one program for data use authorization is installed and is running in the first
trusted execution environment.

20. The apparatus according to claim 13 or 14, wherein the secure transmission is an encrypted transmission.

21. A computing device, comprising a memory and a processor, the memory
5 storing executable code, and the processor implementing the method according to any one of claims 1 to 12 when executing the executable code.