

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

15 providing the 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

20 wherein the access permission information is information about a calculation 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:

25 obtaining authorization information about the first plaintext data;

 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 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 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.~~

~~4. The method according to claim 3, 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.~~

~~5.3.~~ The method according to claim 41 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 calculation result.

~~6.4.~~ The method according to claim 41 or 2, wherein the access permission information is null information.

~~7.5.~~ 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 a-the at least one program for data use authorization is installed and is running in the first trusted execution environment.

~~8.6.~~ The method according to claim 1 or 2, wherein the secure transmission is encrypted transmission.

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

receiving, from a data provider, a verification request;

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

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

10 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,

15 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 result of the at least one program, and storing at least one piece of encrypted data, at least one first key and at least one piece of authorization information corresponding to the at least one first key being stored in the first trusted execution environment, the at least one first key being used to decrypt the at least one piece of encrypted data to obtain at least one piece of plaintext data, the at least one piece of authorization information corresponding to the at least one piece of plaintext data, and the authorization information being information about at least one program allowed to use corresponding plaintext data, the method comprising:

25 receiving a data request from a data user, the data request being used to request to use the at least one piece of plaintext data, and the data user including a second trusted execution environment;

30 receiving authentication information from the data user, the authentication information being generated by the second trusted execution environment;

performing verification for each piece of authorization information based on the authentication information and the authorization information in the first trusted execution environment; and

~~for each piece of authorization information, when the verification succeeds, securely transmitting a first key corresponding to the authorization information to the second trusted execution environment by using the first trusted execution environment, and providing corresponding encrypted data to the data user.~~

5

~~10. A data processing method, wherein the method is performed by a data manager, the data manager including a first trusted execution environment, at least one piece of plaintext data and at least one piece of authorization information corresponding to the at least one piece of plaintext data being stored in the first trusted execution environment, and the authorization information being information about at least one program allowed to use corresponding plaintext data, the method comprising:~~

10

~~receiving a data request from a data user, the data request being used to request to use the at least one piece of plaintext data, and the data user including a second trusted execution environment;~~

15

~~receiving authentication information from the data user, the authentication information being generated by the second trusted execution environment;~~

~~performing verification for each piece of authorization information based on the authentication information and the authorization information in the first trusted execution environment; and~~

20

~~for each piece of authorization information, when the verification succeeds, securely transmitting plaintext data corresponding to the authorization information to the second trusted execution environment by using the first trusted execution environment.~~

25

~~11.8.~~ The method according to claim ~~9 or 10~~7, wherein the first trusted execution environment and the second trusted execution environment are located on one platform or different platforms.

30

~~12.9.~~ The method according to claim ~~9 or 10~~7, wherein the receiving the authentication information from the data user includes: receiving, by using the first trusted execution environment, the authentication information securely transmitted from the second trusted execution environment.

~~13.10.~~ The method according to claim ~~97~~, wherein the authentication information includes a first code hash value of a first program that is installed and running in the second trusted execution environment, each piece of authorization information including at least one code hash value of at least one program; and the performing
5 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 included in the authorization information.

10 ~~14.11.~~ The method according to claim ~~13.10~~, 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 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
15 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.

~~15.12.~~ The method according to claim ~~97~~, wherein the data manager further
20 includes a data storage module, the at least one piece of encrypted data being stored in the data storage module.

~~16. A data processing method, wherein the method is performed by a data user, the data user including a second trusted execution environment, a first program
25 running in the second trusted execution environment, and the method comprising:
sending a data request to a data manager to request to use at least one piece of plaintext data corresponding to at least one piece of encrypted data stored in the data manager, the data manager including a first trusted execution environment, at least one first key and at least one piece of authorization information corresponding to the
30 at least one first key being stored in the first trusted execution environment, the at least one first key being used to decrypt the at least one piece of encrypted data to obtain the at least one piece of plaintext data, the at least one piece of authorization information corresponding to the at least one piece of plaintext data, and the~~

~~authorization information being information about at least one program allowed to use corresponding plaintext data;~~

~~sending authentication information to the data manager, so that the first trusted execution environment performs verification for each piece of authorization information based on the authentication information and the authorization information, the authentication information being generated by the second trusted execution environment;~~

~~for each piece of authorization information, when the verification succeeds, receiving, by using the second trusted execution environment, a first key that corresponds to the authorization information and that is securely transmitted from the first trusted execution environment, obtaining encrypted data corresponding to the authorization information from the data manager, and decrypting the encrypted data by using the first key in the second trusted execution environment to obtain corresponding plaintext data; and~~

~~performing calculation based on the at least one piece of plaintext data by using the first program in the second trusted execution environment to obtain a calculation result.~~

17. A data processing method, wherein the method is performed by a data user, the data user including a second trusted execution environment and a first program running in the second trusted execution environment, the method comprising:

~~sending a data request to a data manager to request to use at least one piece of plaintext data stored in the data manager, the data manager including a first trusted execution environment, the at least one piece of plaintext data and at least one piece of authorization information respectively corresponding to the at least one piece of plaintext data being stored in the first trusted execution environment, and the authorization information being information about at least one program allowed to use corresponding plaintext data;~~

~~sending authentication information to the data manager, so that the first trusted execution environment performs verification for each piece of authorization information based on the authentication information and the authorization information, the authentication information being generated by the second trusted execution environment;~~

for each piece of authorization information, when the verification succeeds, receiving, by using the second trusted execution environment, plaintext data that corresponds to the authorization information and that is securely transmitted from the first trusted execution environment; and

- 5 performing calculation based on the at least one piece of plaintext data by using the first program in the second trusted execution environment to obtain a calculation result.

18. The method according to claim 16 or 17, wherein the first program has a first code hash value, each piece of authorization information including a first code hash value and a second key corresponding to the first code hash value, and the second key being used to encrypt a calculation result of the first program and being provided by a calculation result user corresponding to the calculation result, the method further comprising:

- 15 for each piece of authorization information, when the verification succeeds, receiving, by using the second trusted execution environment, the second key that corresponds to the authorization information and that is securely transmitted from the first trusted execution environment;

after the calculation result is obtained, determining, in the second trusted execution environment, whether at least one second key corresponding to the at least one piece of authorization information is consistent; and

- 20 when the at least one second key is consistent, encrypting the calculation result by using the second key in the second trusted execution environment to obtain an encrypted calculation result.

25

19. The method according to claim 18, further comprising: sending the encrypted calculation result to the calculation result user after the encrypted calculation result is obtained.

- 30 20. The method according to claim 16, wherein the obtaining the encrypted data corresponding to the authorization information from the data manager includes: reading the encrypted data corresponding to the authorization information from the data manager.

~~21.13.~~ 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 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;

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;

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 result of the at least one program.

~~22.14.~~ 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 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 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 result of the at least one program.

23.15. The apparatus according to claim 21-or-2213 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.

24.16. The apparatus according to claim 2315, 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 2416, 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.

26.18. The apparatus according to claim 2416, wherein the access permission information is null information.

27.19. The apparatus according to claim 21-or-2213 or 14, wherein the verification unit is further configured to verify, based on the authentication information, whether a-the at least one program for data use authorization is installed and is running in the first trusted execution environment.

28.20. The apparatus according to claim 21-or-2213 or 14, wherein the secure transmission is an encrypted transmission.

29. A data processing apparatus, wherein the apparatus is implemented by a data manager, the data manager including a first trusted execution environment and storing

at least one piece of encrypted data, at least one first key and at least one piece of authorization information corresponding to the at least one first key being stored in the first trusted execution environment, the at least one first key being used to decrypt the at least one piece of encrypted data to respectively obtain at least one piece of plaintext data, the at least one piece of authorization information corresponding to the at least one piece of plaintext data, and the authorization information being information about at least one program allowed to use corresponding plaintext data, the apparatus comprising:

a first receiving unit, configured to receive a data request from a data user, the data request being used to request to use the at least one piece of plaintext data, and the data user including a second trusted execution environment;

a second receiving unit, configured to receive authentication information from the data user, the authentication information being generated by the second trusted execution environment;

a verification unit, configured to perform verification for each piece of authorization information based on the authentication information and the authorization information in the first trusted execution environment; and

a first secure transmission unit for each piece of authorization information, configured to: when the verification succeeds, securely transmit a first key corresponding to the authorization information to the second trusted execution environment by using the first trusted execution environment, and a providing unit for each piece of authorization information, configured to provide corresponding encrypted data to the data user.

30. A data processing apparatus, wherein the apparatus is implemented by a data manager, the data manager including a first trusted execution environment, at least one piece of plaintext data and at least one piece of authorization information respectively corresponding to the at least one piece of plaintext data being stored in the first trusted execution environment, the authorization information being information about at least one program allowed to use corresponding plaintext data, and the apparatus comprising:

a first receiving unit, configured to receive a data request from a data user, the data request being used to request to use the at least one piece of plaintext data, and the data user including a second trusted execution environment;

~~a second receiving unit, configured to receive authentication information from the data user, the authentication information being generated by the second trusted execution environment;~~
~~a verification unit, configured to perform verification for each piece of authorization information based on the authentication information and the authorization information in the first trusted execution environment; and~~
~~a secure transmission unit for each piece of authorization information, configured to: when the verification succeeds, securely transmit plaintext data corresponding to the authorization information to the second trusted execution environment by using the first trusted execution environment.~~

~~31. The apparatus according to claim 29 or 30, wherein the first trusted execution environment and the second trusted execution environment are located on one platform or different platforms.~~

~~32. The apparatus according to claim 29 or 30, wherein the verification unit is further configured to receive, by using the first trusted execution environment, the authentication information securely transmitted from the second trusted execution environment.~~

~~33. The apparatus according to claim 29, wherein the authentication information includes a first code hash value of a first program that is installed and running in the second trusted execution environment, each piece of authorization information including at least one code hash value of at least one program; and the verification unit is further configured to verify, for each piece of authorization information, whether the first code hash value is a code hash value included in the authorization information.~~

~~34. The apparatus according to claim 33, 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 first program and being provided by a calculation result user corresponding to the calculation result; and the apparatus further comprises a second secure transmission unit, configured to: for each piece of authorization information, when the verification~~

succeeds, further securely transmit the second security key to the second trusted execution environment by using the first trusted execution environment.

35. The apparatus according to claim 29, 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.

36. A data processing apparatus, wherein the apparatus is implemented by a data user, the data user including a second trusted execution environment, and a first program running in the second trusted execution environment, the apparatus comprising:
a first sending unit, configured to send a data request to a data manager to request to use at least one piece of plaintext data corresponding to at least one piece of encrypted data stored in the data manager, the data manager including a first trusted execution environment, at least one first key and at least one piece of authorization information corresponding to the at least one first key being stored in the first trusted execution environment, the at least one first key being used to decrypt the at least one piece of encrypted data to obtain the at least one piece of plaintext data, the at least one piece of authorization information corresponding to the at least one piece of plaintext data, and the authorization information being information about at least one program allowed to use corresponding plaintext data;
a second sending unit, configured to send authentication information to the data manager, so that the first trusted execution environment performs verification for each piece of authorization information based on the authentication information and the authorization information, the authentication information being generated by the second trusted execution environment;
a first receiving unit for each piece of authorization information, configured to: when the verification succeeds, receive, by using the second trusted execution environment, a first key that corresponds to the authorization information and that is securely transmitted from the first trusted execution environment, an acquisition unit for each piece of authorization information, configured to obtain encrypted data corresponding to the authorization information from the data manager, and a decryption unit for each piece of authorization information, configured to decrypt the encrypted data by using the first key in the second trusted execution environment to obtain corresponding plaintext data; and

~~a calculation unit, configured to perform calculation based on the at least one piece of plaintext data by using the first program in the second trusted execution environment to obtain a calculation result.~~

- 5 ~~37. A data processing apparatus, wherein the apparatus is implemented by a data user, the data user including a second trusted execution environment, and a first program running in the second trusted execution environment, the apparatus comprising:~~
- 10 ~~a first sending unit, configured to send a data request to a data manager to request to use at least one piece of plaintext data stored in the data manager, the data manager including a first trusted execution environment, the at least one piece of plaintext data and at least one piece of authorization information respectively corresponding to the at least one piece of plaintext data being stored in the first trusted execution environment, and the authorization information being information about at least one program allowed to use corresponding plaintext data;~~
- 15 ~~a second sending unit, configured to send authentication information to the data manager, so that the first trusted execution environment performs verification for each piece of authorization information based on the authentication information and the authorization information, the authentication information being generated by the second trusted execution environment;~~
- 20 ~~a first receiving unit for each piece of authorization information, configured to: for each piece of authorization information, when the verification succeeds, receive, by using the second trusted execution environment, plaintext data that corresponds to the authorization information and that is securely transmitted from the first trusted execution environment; and~~
- 25 ~~a calculation unit, configured to perform calculation based on the at least one piece of plaintext data by using the first program in the second trusted execution environment to obtain a calculation result.~~

- 30 ~~38. The apparatus according to claim 36 or 37, wherein the first program has a first code hash value, each piece of authorization information including 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 first program and being provided by a calculation result user corresponding to the calculation result, and the apparatus further comprising:~~

~~a second receiving unit for each piece of authorization information, configured to: when the verification succeeds, receive, by using the second trusted execution environment, the second key that corresponds to the authorization information and that is securely transmitted from the first trusted execution environment;~~

5 ~~a determining unit, configured to: after the calculation result is obtained, determine, in the second trusted execution environment, whether at least one second key respectively corresponding to the at least one piece of authorization information is consistent; and~~

~~an encryption unit, configured to: when the at least one second key is consistent,~~
10 ~~encrypt the calculation result by using the second key in the second trusted execution environment to obtain an encrypted calculation result.~~

~~39. The apparatus according to claim 38, further comprising a third sending unit,~~
15 ~~configured to send the encrypted calculation result to the calculation result user after the encrypted calculation result is obtained.~~

~~40. The apparatus according to claim 36, wherein the acquisition unit is further~~
~~configured to read the encrypted data corresponding to the authorization information~~
~~from the data manager.~~

20

~~41. 21.~~ A computing device, comprising a memory and a processor, the memory storing executable code, and the processor implementing the method according to any one of claims 1 to ~~20-12~~ when executing the executable code.