CLAIMS

What is claimed is:

1. A data encryption method, comprising:

determining source data requested to be encrypted by an application in an untrusted execution environment;

generating reference data corresponding to the source data in the untrusted execution environment, wherein the reference data is data for one-time use in encrypting the source data;

reading a primary key generated for the application in a trusted execution environment;

acquiring security data by encrypting the reference data using the primary key in the trusted execution environment; and

acquiring target data by encrypting the source data using the security data in the untrusted execution environment;

wherein acquiring the security data by encrypting the reference data using the primary key in the trusted execution environment comprises:

acquiring a target array by combining the reference data and a predetermined label in the trusted execution environment, wherein the predetermined label is defined to indicate a type of the security data;

acquiring candidate data by encrypting the target array using the primary key in the trusted execution environment; and

regulating the candidate data into data with a specified length in the trusted execution environment, and determining the data with the specified length as security data matching the predetermined label.

2. The method according to claim 1, wherein generating the reference data corresponding to the source data in the untrusted execution environment comprises:

randomly generating a value as the reference data in the untrusted execution environment; and/or

reading a current timestamp as the reference data in the untrusted execution environment.

3. The method according to claim 1, wherein the security data comprises a secondary key, or a secondary key and a vector; and

regulating the candidate data into the data with the specified length in the trusted execution environment, and determining the data with the specified length as the security data matching the predetermined label comprise:

computing, in response to the predetermined label being a first value, digest data with a first specified length for the candidate data in the trusted execution environment, and determining the digest data with the first specified length as the secondary key and the vector; or

computing, in response to the predetermined label being a second value, digest data with a second specified length for the candidate data in the trusted execution environment, and determining the digest data with the second specified length as the secondary key.

4. The method according to claim 1, wherein the security data comprises a secondary key, or a secondary key and a vector; and

acquiring the target data by encrypting the source data using the security data in the untrusted execution environment comprises:

encrypting the source data as the target data in the untrusted execution environment by calling an advanced encryption standard (AES) algorithm in a symmetric key algorithm and using the vector, as an initialization vector, the secondary key; or

encrypting the source data as the target data in the untrusted execution environment by calling a non-AES algorithm in the symmetric key algorithm and using the secondary key.

5. The method according to any one of claims 1 to 4, further comprising:

associatively storing the target data and the reference data in the untrusted execution environment;

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

detecting a second operation of deleting the target data; and

deleting, in response to the second operation, the target data and the reference data from the untrusted execution environment.

7. The method according to any one of claims 1 to 4, further comprising:

detecting a third operation of unloading the application;

deleting, in response to the third operation, the primary key generated for the application from the trusted execution environment; and

deleting, in response to the third operation, the target data and the reference data from the untrusted execution environment.

8. A data decryption method, comprising:

determining target data requested to be encrypted by an application in an untrusted execution environment;

reading reference data associated with the target data in the untrusted execution environment, wherein the reference data is data for one-time use in decrypting the target data;

reading a primary key generated for the application in a trusted execution environment;

acquiring security data by encrypting the reference data using the primary key in the trusted execution environment; and

acquiring source data by decrypting the target data using the security data in the untrusted execution environment;

wherein acquiring the security data by encrypting the reference data using the primary key in the trusted execution environment comprises:

acquiring a target array by combining the reference data and a predetermined label in the trusted execution environment, wherein the predetermined label is defined to indicate a type of the security data;

acquiring candidate data by encrypting the target array using the primary key in the trusted execution environment; and

regulating the candidate data into data with a specified length in the trusted execution environment, and determining the data with the specified length as security data matching the predetermined label.

9. The method according to claim 8, further comprising:

associatively storing the target data and the reference data in the untrusted execution environment.

10. The method according to claim 9, further comprising:

detecting a second operation of deleting the target data; and

deleting, in response to the second operation, the target data and the reference data from the untrusted execution environment.

11. A data encryption apparatus, comprising:

a source data determining module, configured to determine source data requested to be encrypted by an application in an untrusted execution environment;

a reference data generating module, configured to generate reference data corresponding to the source data in the untrusted execution environment, wherein the reference data is data for one-time use in encrypting the source data;

a primary key reading module, configured to read a primary key generated for the application in a trusted execution environment;

a security data generating module, configured to acquire security data by encrypting the reference data using the primary key in the trusted execution environment; and

a source data encrypting module, configured to acquire target data by encrypting the source data using the security data in the untrusted execution environment;

the security data generating module includes:

a target array combining sub-module, configured to acquire a target array by combining the reference data and a predetermined label in the trusted execution environment, wherein the label is defined to indicate a type of the security data;

a candidate data generating sub-module, configured to acquire candidate data by encrypting the target array using the primary key; and

a candidate data regulating sub-module, configured to regulate the candidate data into data with a specified length as security data matching the label.

12. The apparatus according to claim 11, wherein the reference data generating module comprises:

a random value generating sub-module, configured to randomly generate a value as the reference data in the untrusted execution environment; and/or

a timestamp reading sub-module, configured to read a current timestamp as the reference data in the untrusted execution environment.

13. A data decryption apparatus, comprising:

a target data determining module, configured to determine target data requested to be encrypted by an application in an untrusted execution environment;

a reference data reading module, configured to read reference data associated with the target data in the untrusted execution environment, wherein the reference data is data for one-time use in decrypting the target data;

a primary key reading module, configured to read a primary key generated for the application in a trusted execution environment;

a security data generating module, configured to acquire security data by encrypting the reference data using the primary key in the trusted execution environment; and

a target data decrypting module, configured to acquire source data by decrypting the target data using the security data in the untrusted execution environment;

the security data generating module comprises:

a target array combining sub-module, configured to acquire a target array by combining the reference data and a predetermined label in the trusted execution environment, wherein the predetermined label is defined to indicate a type of the security data;

a candidate data generating sub-module, configured to acquire candidate data by encrypting the target array using the primary key; and

a candidate data regulating sub-module, configured to regulate the candidate data into data with a specified length, and determine the data with the specified length as security data matching the predetermined label.

14. A mobile terminal, comprising:

one or more processors; and

a memory configured to store one or more programs; wherein

the one or more processors, when loading and running the one or more programs, are caused

to perform the data encryption method according to any one of claims 1 to 7 or the data decryption method according to any one of claims 8 to 10.

15. A computer-readable storage medium, storing a computer program thereon, wherein the computer program, when loaded and run by a processor, causes the processor to perform the data encryption method according to any one of claims 1 to 7 or the data decryption method according to any one of claims 8 to 10.