CLAIMS

What is claimed is:

1. A method for data processing in an equity incentive system, applied in a first device in the equity incentive system, the method comprising:

obtaining a mapping relation that comprises a correspondence between at least one data type and at least one encryption scheme;

determining, based on the mapping relation, a first encryption scheme corresponding to a first data type of first data;

encrypting the first data in accordance with the first encryption scheme to obtain a first cipher text;

generating a first data packet based on the first cipher text and the first encryption scheme; and

transmitting the first data packet to a second device in the equity incentive system,

wherein the first encryption scheme is a random padding encryption scheme, a non-random encryption scheme, or a long text encryption scheme,

wherein a data type corresponding to the random padding encryption scheme is a field, which is not involved in the query, of the share-holding incentive information; a data type corresponding to the non-random encryption scheme is a field of the share-holding incentive information related to the index or the query; and a data type corresponding to the long text encryption scheme is a text or file, which has a length greater than a predetermined threshold, of the share-holding incentive information.

2. The method according to claim 1, wherein

the first encryption scheme is the long text encryption scheme,

said encrypting the first data in accordance with the first encryption scheme to obtain the first cipher text comprises:

encrypting the first data using a first secret key to obtain the first cipher text, wherein the first secret key is a secret key corresponding to the first data; and

encrypting the first secret key to obtain a second cipher text; and

said generating the first data packet based on the first cipher text and the first encryption scheme comprises:

generating the first data packet based on the first cipher text, the first encryption scheme, and the second cipher text.

3. The method according to claim 1, wherein

the first encryption scheme is the random padding encryption scheme,

said encrypting the first data in accordance with the first encryption scheme to obtain the first cipher text comprises:

encrypting the first data using a first secret key to obtain the first cipher text, wherein the first secret key is a random secret key; and

said generating the first data packet based on the first cipher text and the first encryption scheme comprises:

generating the first data packet based on the first cipher text and the first encryption scheme.

4. The method according to claim 1, wherein

the first encryption scheme is the non-random padding encryption scheme;

said encrypting the first data in accordance with the first encryption scheme to obtain the first cipher text comprises:

encrypting the first data using a first secret key to obtain the first cipher text, wherein the first secret key is a fixed secret key; and

said generating the first data packet based on the first cipher text and the first encryption scheme comprises:

generating the first data packet based on the first cipher text and the first encryption scheme.

5. The method according to claim 2, wherein said encrypting the first secret key to obtain the second cipher text comprises:

encrypting the first secret key using a second secret key to obtain the second cipher text, wherein the second secret key is a secret key agreed between the first device and the second device.

6. The method according to claim 2, wherein said encrypting the first secret key to obtain the second cipher text comprises:

encrypting the first secret key using a second secret key to obtain the second cipher text, wherein the second secret key is a public key corresponding to a private key in the second device.

7. The method according to claim 2, further comprising, prior to transmitting, by the first device, the first data packet to the second device:

splicing, by the first device, the first cipher text and the second cipher text to obtain the first data packet.

8. The method according to any one of claims 1 to 7, wherein said generating the first data packet based on the first cipher text and the first encryption scheme comprises:

generating the first data packet by using an encryption identifier corresponding to the first encryption scheme as a prefix.

9. An apparatus for data processing, comprising modules configured to perform the method according to any one of claims 1 to 8.

10. An apparatus for data processing, comprising:

a memory having instructions stored thereon; and

a processor,

wherein the processor, when executing the instructions, causes the apparatus to perform the method according to any one of claims 1 to 8.

11. A non-transitory computer-readable storage medium, having a computer program or instruction stored thereon, wherein the computer program or instruction, when executed, performs the method according to any one of claims 1 to 8.

12. A non-transitory computer program product, comprising computer program codes, wherein the computer program codes, when executed by a communication device, cause the communication device to perform the method according to any one of claims 1 to 8.