

a shared key generation module for generating a shared key based on the second private key and the first public key using a preset key-agreement algorithm;

an information encryption module for using the shared key to encrypt a seed parameter to which the data request corresponds,

5        an information sending module for sending a ciphertext obtained from encryption and the second public key to the client so that the client generates a shared key based on the first private key and the second public key using the key-agreement algorithm and uses the shared key to decrypt the ciphertext to obtain the seed parameter;

10       wherein the shared key generated based on the second private key and the first public key using the preset key-agreement algorithm is identical to the shared key generated based on the first private key and the second public key using the key-agreement algorithm.

12. A data transmission system, wherein the system comprises a data requester device and a data provider device;

15       the data requester device generating an asymmetrical key pair comprising a first public key and a first private key and sending a data request carrying the first public key to a data provider device;

the data provider device obtaining an asymmetrical key pair comprising a second public key and a second private key and generating a shared key based on the second private key and the first public key using a preset key-agreement algorithm;

20       the data provider device using the shared key to encrypt target data to which the data request corresponds and sending a ciphertext obtained from encryption and the second public key to the data requester device;

25       the data requester device generating a shared key based on the first private key and the second public key using the key-agreement algorithm and using the shared key to decrypt the ciphertext to obtain the target data.

wherein the shared key generated based on the second private key and the first public key using the preset key-agreement algorithm is identical to the shared key generated based on the first private key and the second public key using the key-agreement algorithm.

13. A data transmission method, wherein the method comprises: