

WHAT IS CLAIMED IS:

1. An encryption method performed by a computing apparatus (12,110, 120, 130) including one or more processors (14) and a memory (16) for storing one or more programs (20) executed by the one or more processors, the encryption method comprising:

generating (201, 204, 207) a public key share of a user;

receiving (202, 203, 205,206, 208, 209) public key shares of one or more other users from terminals of the one or more other users;

generating (210, 211, 212) a public key using the public key share of the user and the public key shares of the one or more other users;

encrypting a first plaintext using the public key, thereby generating a first ciphertext;

obtaining a second ciphertext resulting from encrypting a second plaintext using the public key; and

performing homomorphic evaluation on the first and the second ciphertext by adding the first and the second ciphertext, thereby generating a third ciphertext corresponding to the sum of the first and the second plaintext.

2. The encryption method of claim 1, wherein the generating of the public key share comprises:

generating a private key share of the user; and

generating a public key share of the user using the private key share of the user; and/or

wherein the public key shares of the one or more other users are generated using private key shares of the one or more other users.

3. The encryption method of claim 1 or 2, further comprising providing the generated public key share to the terminals of the one or more other users.

4. An encryption apparatus comprising:

one or more processors (14);

a memory (16); and

one or more programs (20),

wherein,

the one or more programs are stored in the memory and executed by the one or more

processors; and

the programs comprise instructions for:

generating (201, 204, 207) a public key share of a user;

receiving (202, 203, 205, 206, 208, 209) public key shares of one or more other users from terminals of the one or more other users;

generating (210, 211, 212) a public key using the public key share of the user and the public key shares of the one or more other users; and

encrypting a first plaintext using the public key, thereby generating a first ciphertext;

obtaining a second ciphertext resulting from encrypting a second plaintext using the public key; and

performing homomorphic evaluation on the first and the second ciphertext by adding the first and the second ciphertext, thereby generating a third ciphertext corresponding to the sum of the first and the second plaintext.

5. The encryption apparatus of claim 4, wherein the generating of the public key share comprises:

generating a private key share of the user; and

generating a public key share of the user using the private key share of the user; and/or

wherein the public key shares of the one or more other users are generated using private key shares of the one or more other users.

6. The encryption apparatus of claim 4, wherein the programs further include instructions for providing the generated public key share to the terminals of the one or more other users.

7. A decryption method performed by a computing apparatus (12, 110, 120, 130) including one or more processors (14) and a memory (16) for storing one or more programs (20) executed by the one or more processors, the decryption method comprising:

generating (301, 304, 305) a partial decryption result for a ciphertext encrypted with a public key by using a private key share of a user, wherein the ciphertext is generated by adding a plurality of ciphertexts encrypted with the public key in an encrypted state as defined in claim 1;

requesting (302, 303) terminals of one or more other users to perform partial decryption of the ciphertext;

receiving (306, 307) partial decryption results for the ciphertext using private key shares of the one or more other users from the one or more other user terminals; and

generating plaintext for the ciphertext using the generated partial decryption result and the partial decryption results received from the one or more other users, wherein the plaintext is a result of adding plaintexts for the plurality of ciphertexts.

8. The decryption method of claim 7, wherein the public key is generated using a public key share of the user and public key shares of the one or more other users; and/or

wherein,

the public key share of the user is generated using the private key share of the user, and

the public key shares of the one or more other users are generated using the private key shares of the one or more other users.

9. The decryption method of claim 7, wherein the generating of the plaintext comprises generating plaintext for the ciphertext by adding the generated partial decryption result and the partial decryption results received from the one or more other users.

10. A decryption apparatus comprising:

one or more processors (14);

a memory (16); and

one or more programs (20),

wherein,

the one or more programs are stored in the memory and executed by the one or more processors; and

the program comprises instructions for:

generating (301, 304, 305) a partial decryption result for a ciphertext encrypted with a public key by using a private key share of a user, wherein the ciphertext is generated by adding a plurality of ciphertexts encrypted with the public key in an encrypted state as defined in claim 4;

requesting (302, 303) terminals of one or more other users to perform partial decryption of the ciphertext;

receiving (306, 307) partial decryption results for the ciphertext using private key shares of the one or more other users from the one or more other user terminals; and

generating plaintext for the ciphertext using the generated partial decryption result and the partial decryption results received from the one or more other users,

wherein the plaintext is a result of adding plaintexts for the plurality of ciphertexts.

11. The decryption apparatus of claim 10, wherein the public key is generated using a public key share of the user and public key shares of the one or more other users.

12. The decryption apparatus of claim 11, wherein,
the public key share of the user is generated using the private key share of the user;
and

the public key shares of the one or more other users are generated using the private key shares of the one or more other users.

13. The decryption apparatus of claim 11, wherein the generating of the plaintext comprises generating plaintext for the ciphertext by adding the generated partial decryption result and the partial decryption results received from the one or more other users.