【CLAIMS】

1. An encryption method of a terminal device, the method comprising:

   setting a scaling factor; and

   reflecting the scaling factor in a message to be encrypted, and performing encryption using a public key to generate a homomorphic ciphertext,

   wherein the homomorphic encryption is, based on a decryption being performed, in a form that a result value obtained by adding an error value to a value obtained by reflecting the scaling factor in the message is restored,

   wherein a modulus of the homomorphic ciphertext is a value obtained by multiplying a plurality of different scaling factors by each other, and the plurality of different scaling factors are set as values which are disjoint from each other within a similar range.

2. The encryption method as claimed in claim 1, wherein the generating the homomorphic ciphertext comprises:

calculating an error from a discrete Gaussian distribution or a distribution that is within a short statistical distance to the discrete Gaussian distribution; and

multiplying the message by the scaling factor and adding the error to the multiplied message, and performing encryption using the public key to generate the homomorphic ciphertext.

3. The encryption method as claimed in claim 1, further comprising:

based on the message being a plurality of message vectors, converting the plurality of message vectors into a polynomial in a form capable of being encrypted in parallel,

wherein the generating the homomorphic ciphertext comprises multiplying the polynomial by the scaling factor, and performing homomorphic encryption using the public key.

4. A ciphertext processing method of a server device, the ciphertext processing method comprising:

receiving a plurality of homomorphic ciphertext that are individually encrypted;

performing a predetermined computation with respect to the plurality of homomorphic ciphertext; and

eliminating a noise domain from a result ciphertext calculated by the computation and extracting data of a valid domain,

wherein each of the plurality of homomorphic ciphertext is a ciphertext generated by multiplying a message by a scaling factor, and performing encryption of the multiplied message,

wherein the noise domain is determined to correspond to a size of the scaling factor, and

wherein a modulus of the homomorphic ciphertext is a value obtained by multiplying a plurality of different scaling factors by each other, and the plurality of different scaling factors are set as values which are disjoint from each other within a similar range.

5. The ciphertext processing method as claimed in claim 4, further comprising:

based on each of the plurality of homomorphic ciphertext is a ciphertext generated by packing a plurality of message vectors, performing a computation process in parallel of message vectors included in each of the plurality of homomorphic ciphertext.

6. The ciphertext processing method as claimed in claim 5, further comprising:

rotating an order of each of message vectors included in the plurality of homomorphic ciphertext.

7. The ciphertext processing method as claimed in claim 5, further comprising:

based on the message being a complex number, performing a conjugation computation for the plurality of homomorphic ciphertext.

8. A terminal device, comprising:

a memory configured to store a scaling factor and a public key;

a processor configured to reflect the scaling factor in a message to be encrypted, and then perform encryption using the public key, and generate a homomorphic ciphertext; and

a communicator configured to transmit the homomorphic ciphertext to an external device,

wherein the homomorphic ciphertext is, based on a decryption being performed, in a form that a result value obtained by adding an error value to a value obtained by reflecting the scaling factor in the message is restored,

wherein the processor is configure to set a modulus of the homomorphic ciphertext as a value obtained by multiplying a plurality of different scaling factors by each other, and store the set modulus of the homomorphic ciphertext in the memory, and

wherein the plurality of different scaling factors are set as values which are disjoint from each other within a similar range.

9. The terminal device as claimed in claim 8, further comprising:

an input interface configured to receive input of the message and the scaling factor,

wherein the processor is configured to store, in the memory, the message input through the input interface and the scaling factor.

10. The terminal device as claimed in claim 8, wherein the processor is configured to:

calculate an error from a discrete Gaussian distribution or a distribution that is within a short statistical distance to the discrete Gaussian distribution; and

multiply the message by the scaling factor and add the error to the multiplied message, and then perform encryption using the public key.

11. The terminal device as claimed in claim 8, wherein the processor is configured to:

based on the message being a plurality of message vectors, convert the plurality of message vectors into a polynomial in a form capable of being encrypted in parallel; and

multiply the polynomial by the scaling factor, and then perform homomorphic encryption using the public key.