

as being limited to the described embodiments and/or the drawings. In addition, it should be understood that the disclosure includes various improvements, modifications and changes of the embodiments of the claims which are obvious to those skilled in the art are included in the scope of rights of the disclosure.

【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.
2. The encryption method as claimed in claim 1, wherein a modulus of the homomorphic ciphertext is set as an exponentiation of one scaling factor.
3. The encryption method as claimed in claim 1, 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.
4. 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.

5. 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.

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

7. The ciphertext processing method as claimed in claim 6, 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.

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

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

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

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

10. 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.

11. The terminal device as claimed in claim 10, 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.

12. The terminal device as claimed in claim 10, wherein the processor is configured to set a modulus of the homomorphic ciphertext as an exponentiation of the scaling factor, and store the set modulus of the homomorphic ciphertext in the memory.

13. The terminal device as claimed in claim 10, wherein the processor is configured 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.

14. The terminal device as claimed in claim 10, 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.

15. The terminal device as claimed in claim 10, 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.

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

setting a ring which is a set including elements between which addition and multiplication are defined, the ring including a plaintext space that is a real number from among sets that are closed to addition and multiplication;

calculating a secret key from the ring;

calculating a public key corresponding to the calculated secret key; and

applying the public key to a message and generating a homomorphic ciphertext.

17. The encryption method as claimed in claim 16, wherein the ring satisfies the following equation:

$$a(X) = a(X^{-1}) \text{ where } a(X) \in R, X^{-1} := -X^{n-1}$$

wherein $a(X)$ is a polynomial corresponding to the ring, and the R is a ring including a real space that is a complex number.

18. The encryption method as claimed in claim 16, wherein the homomorphic ciphertext has a complexity of $O(n \log n)$ with respect to an addition or multiplication computation.

19. The encryption method as claimed in claim 16, further comprising:

calculating a first random polynomial from the ring;

extracting an error; and

modulating the error in the first random polynomial and the secret key, and

calculating a second random polynomial,

wherein the calculating the public key comprises:

calculating the public key using the first and second random polynomials.

20. The encryption method as claimed in claim 16, wherein the generating the homomorphic ciphertext comprises:

calculating the message as a polynomial corresponding to the ring, and

applying the public key to the calculated polynomial and generating a

homomorphic ciphertext.

21. The encryption method as claimed in claim 16, further comprising:

performing at least one computation from among addition or multiplication

with respect to the generated homomorphic ciphertext and a pre-generated

homomorphic ciphertext,

wherein the performing the computation comprises:

performing a first function process with respect to each of the

generated homomorphic ciphertext and the pre-generated homomorphic

ciphertext;

performing a computation between the homomorphic ciphertext for which the first function process is performed; and
performing a second function process, which is an inverse function of the first function, with respect to a homomorphic ciphertext for which the computation is performed.

22. The encryption method as claimed in claim 21, wherein the first function is a Number Theoretic Transform (NTT) function.

23. The encryption method as claimed in claim 16, 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 the message is restored.