

【CLAIMS】

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

5 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;

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

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

 generating a homomorphic ciphertext by applying the public
15 key to a message

 the generating the homomorphic ciphertext comprises:

 multiplying the message by a scaling factor and
 adding the error to the multiplied message, and
 performing encryption using the public key to

20 generate the homomorphic ciphertext,

 wherein the homomorphic ciphertext is in a form
 that a result value obtained by adding the error to a
 value obtained by reflecting the scaling factor in the

message,

wherein a modulus of the homomorphic ciphertext
is set as an exponentiation of one scaling factor.

- 5 2. The encryption method as claimed in claim 1, wherein the ring
satisfies the following equation:

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

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

3. The encryption method as claimed in claim 1, wherein the homomorphic
ciphertext has a complexity of $o(n \log n)$ (here, n is a natural number)
with respect to an addition or multiplication computation.

15

4. The encryption method as claimed in claim 1, further comprising:
calculating a first random polynomial from the ring; and
calculating a second random polynomial by modulating the error
in the first random polynomial and the secret key,
20 wherein the calculating the public key comprises:

calculating the public key using the first and second random

polynomials.

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

5 calculating the message as a polynomial corresponding to the
ring, and
applying the public key to the calculated polynomial and
generating a homomorphic ciphertext.

10 6. The encryption method as claimed in claim 1, 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,

15 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
20 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.

7. The encryption method as claimed in claim 6, wherein the first function is a
5 Number Theoretic Transform (NTT) function.

8. A terminal device, comprising:

a memory configured to store a message; and

a processor configured to:

10 set 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,

calculate a secret key from the ring,

15 calculate a public key corresponding to the calculated secret key,

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

multiply the message stored in the memory by a scaling factor and

20 adding the error to the multiplied message, and

generate a homomorphic ciphertext by applying the
public key to the error added message,

wherein the homomorphic ciphertext is in a form that a

result value obtained by adding the error to a value
obtained by reflecting the scaling factor in the message,
wherein a modulus of the homomorphic ciphertext is
set as an exponentiation of one scaling factor.

5

9. The terminal device as claimed in claim 8, wherein the ring satisfies
the following equation:

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

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

10. The terminal device as claimed in claim 8, wherein the
homomorphic ciphertext has a complexity of $o(n \log n)$ (here, n is a
15 natural number) with respect to an addition or multiplication
computation.

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

20 calculate a first random polynomial from the ring,
calculate a second random polynomial by modulating the error

in the first random polynomial and the secret key, and
calculate the public key using the first and second random polynomials.

12. The terminal device as claimed in claim 8, wherein the processor is
5 configured to calculate the message as a polynomial corresponding
to the ring, and generating a homomorphic ciphertext by apply the
public key to the calculated polynomial.

13. The terminal device as claimed in claim 8, wherein the processor
10 is configured to:
perform a first function process with respect to each of the
generated homomorphic ciphertext and a pre-generated
homomorphic ciphertext,
perform at least one computation from among addition or multiplication
15 with respect to the homomorphic ciphertexts 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.

20

14. The terminal device as claimed in claim 13, wherein the
first function is a Number Theoretic Transform (NTT) function.