

CLAIMS

1. An encryption method, comprising:

setting a secret key, and generating a public key using the secret key

and an error; and

- 5 applying the public key to a message, and then performing a rounding

process and encrypting the message,

wherein the secret key is a random combination from among -1, 0 and

1, and

wherein a size of the error is determined by an error parameter which

- 10 is greater than zero and less than one.

2. The encryption method as claimed in claim 1, wherein the generating

the public key comprises:

calculating a first random matrix (A) including randomly-

- 15 determined values;

calculating the secret key (s) by randomly combining a column
vector of which each component has one value from among -1,
0 and 1 in a matrix form;
extracting the error (E) from a discrete Gaussian distribution or
5 a distribution that is within a short statistical distance to the
discrete Gaussian distribution;
calculating a second random matrix (B) by modulating the first
random matrix, the secret key and the error;
calculating the public key including the first random matrix and
10 the second random matrix.

3. The encryption method as claimed in claim 2, wherein the encrypting
the message comprises:

setting a random vector of which each component has a value of
15 -1, 0 and 1;
respectively calculating a first value which is obtained by
calculating the first random matrix and the random vector, and a

second value which is obtained by adding a value obtained by
encoding the message to a result value obtained by calculating
the second random matrix and the random vector; and
performing a rounding process to remove a predetermined
5 number of lower bits for each of the first and second values, and
calculating a ciphertext corresponding to the message.

4. The encryption method as claimed in claim 1, wherein the generating
the public key comprises:

10 setting a ring which is a set of polynomials with a predetermined
coefficient;
calculating the secret key from the ring;
calculating a first random polynomial from the ring;
extracting the error from a discrete Gaussian distribution or a
15 distribution that is within a short statistical distance to the
discrete Gaussian distribution;

calculating a second random polynomial by modulating the error
in the first random polynomial and the secret key; and
setting the public key including the first random polynomial and
the second random polynomial.

5

5. The encryption method as claimed in claim 4, wherein the encrypting
the message comprises:

randomly extracting a polynomial of which each coefficient has
one value from among -1, 0 and 1;

10

respectively calculating a first value which is obtained by
calculating the first random polynomial and the polynomial, and
a second value which is obtained by adding a value obtained by
encoding the message to a result value obtained by calculating
the second random polynomial and the polynomial; and

15

performing a rounding process to remove a predetermined
number of lower bits for each of the first and second values,

and calculating a ciphertext polynomial corresponding to the message.

6. The encryption method as claimed in any one of claims 1 to 5, further comprising:

based on another message encrypted by the public key being received, decrypting the received another message to the secret key.

7. A calculation device, comprising:

a memory; and

a processor configured to:

set a secret key;

generate a public key using the secret key and an error; and

store the secret key and the public key in the memory,

wherein the processor is further configured to apply the public key to a message to be encrypted, and then perform a rounding process and encrypt the message,

wherein the secret key is a random combination from among -1, 0

and 1, and

wherein a size of the error is determined by an error parameter

which is greater than zero and less than one.

5

8. The calculation device as claimed in claim 7, wherein the processor is configured to:

calculate a first random matrix (A) including randomly-determined vectors;

10

calculate the error (E) from a discrete Gaussian distribution or a distribution that is within a short statistical distance to the discrete Gaussian distribution;

calculate a second random matrix (B) by modulating the first random matrix, the secret key and the error; and

15

set the public key including the first random matrix and the second random matrix.

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

set a random vector of which each component has a value of -1,
0 and 1;

5 respectively calculate a first value which is obtained by
calculating the first random matrix and the random vector, and a
second value which is obtained by adding a value obtained by
encoding the message to a result value obtained by calculating
the second random matrix and the random vector; and
10 perform a rounding process to remove a predetermined number
of lower bits for each of the first and second values, and
calculating a ciphertext corresponding to the message.

10. The calculation device as claimed in claim 9, wherein the processor
15 is configured to:

set a ring which is a set of polynomials with a predetermined
coefficient;

calculate the secret key from the ring;

calculate a first random polynomial from the ring;

extract the error from a discrete Gaussian distribution or a distribution that is within a short statistical distance to the

5 discrete Gaussian distribution; and

calculate a second random polynomial by modulating the error in the first random polynomial and the secret key, and set the public key including the first random polynomial and the second random polynomial.

10

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

randomly extract a polynomial of which each coefficient has one value from among -1, 0 and 1;

15 respectively calculate a first value which is obtained by calculating the first random polynomial and the polynomial, and a second value which is obtained by adding a value

obtained by encoding the message to a result value obtained by
calculating the second random polynomial and the polynomial;
and
perform a rounding process to remove a predetermined number
5 of lower bits for each of the first and second values, and
calculating a ciphertext polynomial corresponding to the
message.

12. The calculation device as claimed in any one of claims 7 to 11, further
10 comprising:

a communicator for broadcasting the public key stored in the
memory,
wherein the processor is configured to, based on another message
encrypted by the public key being received, decrypt the received
15 another message to the secret key.

13. A recording medium on which a program code is stored, the

program code sequentially performing the steps for:

calculating a first random matrix (A) including randomly-determined values;

calculating a secret key (s) by randomly combining a column

5 vector of which each component has one value from among -1,

0 and 1 in a matrix form;

calculating an error from a discrete Gaussian distribution or a

distribution that is within a short statistical distance to the

discrete Gaussian distribution;

10 calculating a second random matrix (B) by modulating the first

random matrix, the secret key and the error; and

setting a public key including the first random matrix and the

second random matrix.

15 14. The recording medium as claimed in claim 13, wherein the program

code further performs the steps for:

setting a random vector of which each component has a value of
-1, 0 and 1;
respectively calculating a first value which is obtained by
calculating the first random matrix and the random vector, and a
5 second value which is obtained by adding a value obtained by
encoding a message to a result value obtained by calculating the
second random matrix and the random vector; and
performing a rounding process to remove a predetermined number
of lower bits for each of the first and second values, and calculating
10 a ciphertext corresponding to the message.