

CLAIMS

1. An encryption method, comprising:

calculating a second random matrix (B) using a first random matrix (A)
and a secret key (s) ;

5 generating a ciphertext corresponding to a message using the second
random matrix (B),

wherein the generating the ciphertext comprising :

performing a rounding process for sending the generated ciphertext to
a smaller modulus area,

10 wherein the generating the ciphertext comprises calculating a first value
which is obtained by calculating the first random matrix and a random vector,
and calculating 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.

15

2. The encryption method as claimed in claim 1, wherein the
generating the ciphertext comprises performing message encryption without
Gaussian sampling.

20

3. The encryption method as claimed in claim 1, the generating the
ciphertext further comprises performing a rounding process for the first

value, and performing a rounding process for the result value obtained by calculating the second random matrix and the random vector.

4. The encryption method as claimed in claim 1, further comprising :
- 5 calculating the first random matrix (A) including randomly-determined values;
- calculating the secret key (s);
- calculating a public key using the second random matrix (B).

- 10 5. The encryption method as claimed in claim 4, wherein the calculating the secret key comprises 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.

6. The encryption method as claimed in claim 4, further comprising :
- 15 extracting an error (E) from a discrete Gaussian distribution or a distribution that is within a short statistical distance to the discrete Gaussian distribution, wherein a size of the error is determined by an error parameter which is greater than zero and less than one.

7. A calculation device, comprising:

a memory configured to store a second random matrix (B) obtained by calculating a first random matrix (A) and a secret key (s) ; and

5 a processor configured to generate a ciphertext corresponding to a message using the second random matrix (B),

wherein the processor performs a rounding process for sending the generated ciphertext to a smaller modulus area,

wherein the processor is configured to:

10 calculate a first value which is obtained by calculating the first random matrix and a random vector, and

calculate 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.

15 8. The calculation device as claimed in claim 7, wherein the processor performs message encryption without Gaussian sampling.

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

perform a rounding process for the first value, and

perform a rounding process for the result value obtained by calculating
5 the second random matrix and the random vector.

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

calculate the first random matrix (A) including randomly-determined values;

10 calculate the secret key (s);

calculate a public key using the second random matrix (B).

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

15 calculate 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.

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

extract an error (E) from a discrete Gaussian distribution or a distribution that is within a short statistical distance to the discrete Gaussian distribution,

wherein a size of the error is determined by an error parameter which is greater than zero and less than one.

13. A recording medium on which a program code is stored, the program code sequentially performing the steps for:

calculating a second random matrix (B) using a first random matrix (A) and a secret key (s) ;

generating a ciphertext corresponding to a message using the second random matrix (B),

wherein the generating the ciphertext comprising :

performing a rounding process for sending the generated ciphertext to a smaller modulus area,

wherein the generating the ciphertext comprises calculating a first value which is obtained by calculating the first random matrix and a random vector, and calculating 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.