

CLAIMS

WHAT IS CLAIMED IS:

1. A non-transitory computer readable medium storing program code that, when is executed by a processor, causes the processor to:
 - calculate a message, based on a first cipher text, a second cipher text, and a private key;
 - compare coefficients of the message with a reference value to generate a comparison result, the reference value being based on a prime number;
 - generate, based on the message, a modified message by selectively modifying a respective one of the coefficients of the message, in response to the comparison result indicating that the respective one of the coefficients of the message is greater than the reference value; and
 - decrypt the modified message.
2. The non-transitory computer readable medium of claim 1, wherein the program code, when executed, causes the processor to generate the modified message by,
 - maintaining the respective one of the coefficients of the message, in response to the respective one of the coefficients of the message being less than the reference value.
3. The non-transitory computer readable medium of claim 2, wherein the program code, when executed, causes the processor to selectively modify the coefficients of the message by,
 - setting the respective one of the coefficients in the modified message to a first value, in response to the respective one of the coefficients of the message being greater than the reference value and the respective one of the coefficients of the message is even, and

setting the respective one of the coefficients in the modified message to a second value, in response to the respective one of the coefficients of the message being greater than the reference value and the respective one of the coefficients of the message is odd.

4. The non-transitory computer readable medium of any one of claims 1 to 3, wherein the program code, when executed, causes the processor to calculate the reference value by a division operation on the prime number and one of a round operation, a floor operation, and a ceil operation on a result of the division operation of divisor 2.

5. The non-transitory computer readable medium of any one of claims 1 to 4, wherein the program code, when executed, causes the processor to calculate the message by, executing a multiplication operation on the second cipher text and the private key to generate a multiplication result; and executing an addition operation on the multiplication result and the first cipher text.

6. The non-transitory computer readable medium of any one of claims 1 to 5, wherein the program code, when executed, causes the processor to decrypt the modified message by executing a modulo operation on the modified message.

7. The non-transitory computer readable medium of claim 6, wherein a divisor of the modulo operation is “2”.

8. A decryption device comprising:
processing circuitry configured to,

calculate a message based on a first cipher text, a second cipher text, and a private key,

compare coefficients of the message with a reference value to generate a comparison result, the reference value being based on a prime number,

generate, based on the message, a modified message by selectively modifying a respective one of the coefficients, in response to the comparison result indicating that the respective one of the coefficients of the message is greater than the reference value, and decrypt the modified message.

9. The decryption device of claim 8, wherein the processing circuitry is configured to generate the modified message by,

maintaining the respective one of the coefficients of the message, in response to the respective one of the coefficients of the message being less than the reference value.

10. The decryption device of claim 9, wherein the processing circuitry is configured to selectively modify the coefficients of the message by,

setting the respective one of the coefficients in the modified message to a first value, in response to the respective one of the coefficients of the message being greater than the reference value and the respective one of the coefficients of the message is even, and

setting the respective one of the coefficients in the modified message to a second value, in response to the respective one of the coefficients of the message being greater than the reference value and the respective one of the coefficients of the message is odd.

11. The decryption device of any one of claims 8 to 10, wherein the processing

circuitry is configured to calculate the reference value by a division operation on the prime number and one of a round operation, a floor operation, and a ceil operation on a result of the division operation of divisor “2”.

12. The decryption device of any one of claims 8 to 11, wherein the processing circuitry is configured to calculate the message by,

executing a multiplication operation on the second cipher text and the private key to generate a multiplication result; and

executing an addition operation on the multiplication result and the first cipher text.

13. The decryption device of any one of claims 8 to 12, wherein the processing circuitry is configured to decrypt the modified message by executing a modulo operation on the modified message.

14. The decryption device of claim 13, wherein a divisor of the modulo operation is “2”.

15. A communication system comprising:

an encryption device configured to,

calculate a first cipher text based on a first public key, and

calculate a second cipher text based on a second public key and a plain text message; and

a decryption device configured to,

sample a private key based on a first normal distribution,

sample the first public key from a polynomial ring,
calculate the second public key based on the private key and the first public key,
receive the first cipher text and the second cipher text from the encryption device
in response to transmitting the first public key and the second public key thereto,
generate a transmission message based on the first cipher text, the second cipher
text, and the private key,
compare coefficients of the transmission message with a reference value to
generate a comparison result, the reference value being based on a prime number,
generate, based on the transmission message, a modified transmission message
by selectively modifying a respective one of the coefficients of the transmission message,
in response to the comparison result indicating that the respective one of the coefficients
of the message is greater than the reference value, and
decrypt the modified transmission message.

16. The communication system of claim 15, wherein the decryption device is
configured to generate the modified transmission message by,

setting the respective one of the coefficients in the modified transmission message to a
first value, in response to the respective one of the coefficients of the transmission message being
greater than the reference value and the respective one of the coefficients of the transmission
message is even,

setting the respective one of the coefficients in the modified transmission message to a
second value, in response to the respective one of the coefficients of the transmission message
being greater than the reference value and the respective one of the coefficients of the transmission
message is odd, and

maintaining the respective one of the coefficients of the transmission message, in response to the respective one of the coefficients of the transmission message being less than the reference value.

17. The communication system of claim 15 or claim 16, wherein the decryption device is further configured to calculate the second public key, by executing a first multiplication operation on the private key and the first public key, and executing a first addition operation on a result of the first multiplication operation and a first error sampled from the first normal distribution.

18. The communication system of claim 17, wherein the encryption device is further configured to:

calculate the first cipher text by executing a second multiplication operation on the first public key and a second error sampled from a second normal distribution, executing a third multiplication operation on a third error sampled from the second normal distribution and a parameter, and executing a second addition operation on multiplication results of the second and third multiplication operations; and

calculate the second cipher text by executing a fourth multiplication operation on the second public key and the second error, executing a fifth multiplication operation on a fourth error sampled from the second normal distribution and the parameter, and executing a third addition operation on multiplication results of the fourth and fifth multiplication operations and the plain text message.

19. The communication system of claim 18, wherein the decryption device is further

configured to calculate the transmission message by executing a sixth multiplication operation on the first cipher text and the private key, and executing a fourth addition operation on a multiplication result of the sixth multiplication operation and the second cipher text.

20. The communication system of any one of claims 15 to 19, wherein the decryption device is configured to restore the plain text message by executing a modulo operation on the modified transmission message.