

CLAIMS

WHAT IS CLAIMED IS:

1. A homomorphic encryption device, comprising:

a recryption parameter generating circuit configured to, based on an arithmetic scenario comprising information about an arithmetic schedule between a plurality of ciphertexts, generate a recryption parameter comprising a plurality of recryption levels respectively for the plurality of ciphertexts, and in response to a situation where a sum of a level consumption quantities of at least one operation performed on a corresponding ciphertext is greater than a maximum recryption level, divide the sum into a plurality of levels that are divided such that each of the plurality of levels is less than or equal to the maximum recryption level, and schedule a plurality of recryptions between the at least one operation performed on the corresponding ciphertext, the plurality of recryptions corresponding to the plurality of levels that are divided;

a recryption circuit configured to generate a plurality of recrypted ciphertexts by recrypting each of the plurality of ciphertexts to a corresponding recryption level, based on the recryption parameter; and

an arithmetic circuit configured to output an arithmetic result by performing operations by using the plurality of recrypted ciphertexts, according to the arithmetic scenario.

2. The homomorphic encryption device of claim 1, wherein at least two of the plurality of recryption levels respectively corresponding to the plurality of ciphertexts are different from each other.

3. The homomorphic encryption device of claim 1 or claim 2, wherein the recryption parameter generating circuit is further configured to:

determine level consumption quantities of at least one operation comprised in the arithmetic scenario; and

generate the recryption parameter based on the determined level consumption quantities of the at least one operation.

4. The homomorphic encryption device of claim 3, wherein the recryption

parameter generating circuit is further configured to, for each of the plurality of ciphertexts, determine the sum of the level consumption quantities of the at least one operation performed on the corresponding ciphertext, as a decryption level of the corresponding ciphertext.

5. The homomorphic encryption device of claim 4, wherein a number of levels corresponds to a value obtained by adding "1" to a quotient when the sum is divided by the maximum decryption level.

6. The homomorphic encryption device of claim 5, wherein the arithmetic circuit is further configured to, in response to the situation where the sum of the level consumption quantities of the at least one operation performed on the corresponding ciphertext is greater than the maximum decryption level, provide an intermediate result value to the decryption circuit while performing the arithmetic scenario, and

the decryption circuit is further configured to decrypt the intermediate result value while performing the arithmetic scenario.

7. The homomorphic encryption device of claim 3, wherein the decryption parameter generating circuit is further configured to, based on the determined level consumption quantities of the at least one operation, generate the decryption parameter such that a level of the arithmetic result is minimized.

8. The homomorphic encryption device of claim 7, wherein the decryption parameter generating circuit is further configured to generate the decryption parameter such that the level of the arithmetic result is "0".

9. A ciphertext arithmetic method performed by a homomorphic encryption device, the ciphertext arithmetic method comprising:

determining a plurality of decryption levels for a plurality of ciphertexts, based on an arithmetic scenario comprising information about an arithmetic schedule for the plurality of ciphertexts;

decrypting each of the plurality of ciphertexts to a corresponding decryption level from among the plurality of decryption levels; and

outputting an arithmetic result by performing operations comprising at least one multiplication operation by using the plurality of reencrypted ciphertexts,

wherein at least two of the plurality of reencryption levels are different from each other,

wherein a remaining number of possible arithmetic operations of the reencrypted ciphertexts is larger than a remaining number of possible arithmetic operations of the plurality of ciphertexts,

wherein the determining of the plurality of reencryption levels comprises:

determining a level consumption quantity for each of at least one operation comprised in the arithmetic scenario; and

for each of the plurality of ciphertexts, determining a corresponding reencryption level, based on the determined level consumption quantities of the at least one operation, and

wherein the determining of the corresponding reencryption level comprises:

in response to a situation where a sum of level consumption quantities of at least one operation performed on a corresponding ciphertext from among the plurality of ciphertexts is greater than a maximum reencryption level, by dividing the sum into a plurality of levels that are divided such that each of the plurality of levels is less than or equal to the maximum reencryption level, scheduling a plurality of reencryptions, which correspond to the plurality of levels that are divided, between the at least one operation performed on the corresponding ciphertext.

10. The ciphertext arithmetic method of claim 9, wherein the determining of the plurality of reencryption levels comprises:

obtaining a parameter mapping table comprising a plurality of reencryption parameters that correspond to a plurality of operation combinations; and

based on comparing the parameter mapping table with an operation combination comprised in the arithmetic scenario, determining the plurality of reencryption levels according to a reencryption parameter corresponding to the operation combination.

11. The ciphertext arithmetic method of claim 9, wherein the determining of the corresponding reencryption level comprises determining the sum, as a reencryption level that corresponds to the corresponding ciphertext.

12. The ciphertext arithmetic method of claim 9, wherein the determining of the corresponding decryption level comprises:

in response to a situation where the sum is less than or equal to the maximum decryption level, determining the sum as a decryption level of the corresponding ciphertext.

13. The ciphertext arithmetic method of claim 9, wherein the determining of the plurality of decryption levels comprises, based on the level consumption quantity for each of at least one operation comprised in the arithmetic scenario, determining, as the plurality of decryption levels, levels optimized such that a level of the arithmetic result is minimized.

14. The ciphertext arithmetic method of claim 13, wherein the determining of the plurality of decryption levels comprises determining, as the plurality of decryption levels, levels optimized such that the level of the arithmetic result is "0."

15. The ciphertext arithmetic method of claim 9, wherein the determining of the plurality of decryption levels comprises, by comparing a parameter mapping table, which comprises a plurality of decryption parameters corresponding to a plurality of operation combinations stored in the homomorphic encryption device, with an operation combination comprised in the arithmetic scenario, determining, as the plurality of decryption levels, levels comprised in a decryption parameter corresponding to the operation combination comprised in the arithmetic scenario.

16. A ciphertext arithmetic method performed by a homomorphic encryption device, the ciphertext arithmetic method comprising:

receiving a plurality of ciphertexts from outside the homomorphic encryption device;

receiving a parameter mapping table that comprises a plurality of decryption parameters corresponding to a plurality of operation combinations; and

by comparing the parameter mapping table with an operation combination comprised in an arithmetic scenario, outputting a decryption parameter corresponding to the operation combination comprised in the arithmetic scenario;

based on types and orders of operations required between the plurality of

ciphertexts, reencrypting the plurality of ciphertexts as a plurality of reencrypted ciphertexts to a plurality of reencryption levels respectively corresponding to the plurality of reencrypted ciphertexts such that an arithmetic result comprises no preliminary text; and

outputting the arithmetic result comprising no preliminary text by performing operations comprising at least one multiplication operation by using the plurality of reencrypted ciphertexts,

wherein the reencrypting of the plurality of ciphertexts comprises:

for each of the plurality of ciphertexts, determining a sum of level consumption quantities of at least one operation performed on a corresponding ciphertext, as a reencryption level that corresponds to the corresponding ciphertext; and

for each of the plurality of ciphertexts, reencrypting the corresponding ciphertext to the reencryption level, and

wherein the determining of the sum of the level consumption quantities of the at least one operation as the reencryption level that corresponds to the corresponding ciphertext comprises, in response to a situation where the sum is greater than a maximum reencryption level, by dividing the sum into a plurality of levels, scheduling a plurality of reencryptions, which correspond to the plurality of levels that are divided, between the at least one operation performed on the corresponding ciphertext.

17. The ciphertext arithmetic method of claim 16, wherein at least two of the plurality of reencryption levels respectively corresponding to the plurality of reencrypted ciphertexts are different from each other.

18. The ciphertext arithmetic method of claim 16, wherein each of the plurality of reencryption parameters in the parameter mapping table comprises information about levels optimized such that a level of the arithmetic result is minimized according to a corresponding operation combination from among the plurality of operation combinations.

19. The ciphertext arithmetic method of claim 16, wherein the determining of the sum of the level consumption quantities of the at least one operation as the reencryption level that corresponds to the corresponding ciphertext comprises, in response to a situation where the sum is less than or equal to the maximum reencryption level, determining the sum as the reencryption level of the corresponding ciphertext.