

WHAT IS CLAIMED IS:

1. A ciphertext computation method comprising:

receiving an input of a comparison computation command for a plurality of homomorphic ciphertexts;

performing computation by reflecting the plurality of homomorphic ciphertexts to a composite function corresponding to the comparison computation command; and

outputting the computed homomorphic ciphertext,

wherein the comparison computation is maximum value calculation or minimum value calculation, and

wherein the performing the computation comprises performing computation of the maximum value calculation or the minimum value calculation by using a composite function corresponding to square root computation.

2. The ciphertext computation method according to claim 1, wherein the composite function has a complexity $\theta(\alpha)$ or $\theta(\alpha \log \alpha)$ in response to an accuracy $2^{-\alpha}$.

~~3. The ciphertext computation method according to claim 1, wherein the comparison computation is maximum value calculation or minimum value calculation, and~~

~~wherein the performing the computation comprises performing computation of the maximum value calculation or the minimum value calculation by using a composite function corresponding to square root computation.~~

34. The ciphertext computation method according to claim 13, wherein the composite function corresponding to the square root computation is a function that

repeatedly performs computation of a first function including a first variable having an input value as an initial value and a second variable having a value obtained by subtracting 1 from the input value as an initial value, and a second function including the second variable predetermined number of times.

45. The ciphertext computation method according to claim 34, wherein the predetermined number of times is a number of times corresponding to an error rate of the square root computation.

~~6. The ciphertext computation method according to claim 1, wherein the comparison computation is computation of outputting a predetermined value according to size comparison, and~~

~~wherein the performing the computation comprises repeatedly performing computation of a composite function including function computation corresponding to inverse computation predetermined number of times.~~

~~7. The ciphertext computation method according to claim 1, wherein the comparison computation is computation of outputting a predetermined value according to size comparison, and~~

~~wherein the performing the computation comprises repeatedly performing computation by using a composite function corresponding to a sign function predetermined number of times.~~

~~8. The ciphertext computation method according to claim 7, wherein the composite function corresponding to the sign function is a composite function that~~

obtains an output value closer to 1 for an input value larger than 0 and obtains an output value closer to -1 for an input value smaller than 0.

~~9. The ciphertext computation method according to claim 7, wherein the performing the computation comprises performing the comparison computation by using two or more different composite functions which are approximate functions corresponding to the sign function.~~

540. A computation apparatus comprising:

a memory storing at least one instruction; and

a processor configured to execute the at least one instruction,

wherein the processor, by executing the at least one instruction, is configured to,

based on an input of a comparison computation command for a plurality of

homomorphic ciphertexts being received, perform computation by reflecting the

plurality of homomorphic ciphertexts to a composite function corresponding to the

comparison computation command, and output the computed homomorphic ciphertext,

wherein the comparison computation is maximum value calculation or

minimum value calculation, and

wherein the processor is configured to perform computation of the maximum

value calculation or the minimum value calculation by using a composite function

corresponding to square root computation.

~~11. The computation apparatus according to claim 10, wherein the comparison computation is maximum value calculation or minimum value calculation, and~~

~~wherein the processor is configured to perform computation of the maximum~~

value calculation or the minimum value calculation by using a composite function corresponding to square root computation.

12. The computation apparatus according to claim 10, wherein the comparison computation is computation of outputting a predetermined value according to size comparison, and

wherein the processor is configured to repeatedly perform computation of a composite function including function computation corresponding to inverse computation predetermined number of times.

13. The computation apparatus according to claim 10, wherein the comparison computation is computation of outputting a predetermined value according to size comparison, and

wherein the processor is configured to repeatedly perform computation by using a composite function corresponding to a sign function predetermined number of times.

14. The computation apparatus according to claim 13, wherein the composite function corresponding to the sign function is a composite function that obtains an output value closer to 1 for an input value larger than 0 and obtains an output value closer to -1 for an input value smaller than 0.

15. The computation apparatus according to claim 13, wherein the processor is configured to perform the comparison computation by using two or more different composite functions which are approximate functions corresponding to the sign

~~function.~~