

WHAT IS CLAIMED IS:

1. A ciphertext comparison method using homomorphic encryption, the method being performed in a computing apparatus including one or more processors and a memory for storing one or more programs executable by the one or more processors; the ciphertext comparison method comprising:

acquiring a first ciphertext obtained by encrypting first real-number data using a homomorphic encryption algorithm and a second ciphertext obtained by encrypting second real-number data using the homomorphic encryption algorithm; and

generating a ciphertext for a result for comparison in size between the first real-number data and the second real-number data using homomorphic evaluation of the first ciphertext, the second ciphertext, and an approximation function for approximating a signum function,

wherein the generating of the ciphertext comprises:

performing homomorphic evaluation of subtraction between the first real-number data and the second real-number data using the first ciphertext and the second ciphertext in an encrypted state; and

performing homomorphic evaluation of the approximation function using a result for the homomorphic evaluation of the subtraction to generate the ciphertext for the result of the size comparison.

2. The ciphertext comparison method of claim 1, wherein the approximation function is a function of approximating the signum function to a polynomial composed of addition and multiplication.

3. The ciphertext comparison method of claim 1, wherein the homomorphic encryption algorithm is an approximate homomorphic encryption algorithm that supports homomorphic evaluation of addition, subtraction, and multiplication.

4. A ciphertext comparison apparatus using homomorphic encryption, the apparatus comprising:

one or more processors;

a memory; and

one or more programs,

wherein the one or more programs are stored in the memory and executed by the one or more processors; and

the programs comprise instructions for:

acquiring a first ciphertext obtained by encrypting first real-number data using a homomorphic encryption algorithm and a second ciphertext obtained by encrypting second real-number data using the homomorphic encryption algorithm; and

generating a ciphertext for a result for comparison in size between the first real-number data and the second real-number data using homomorphic evaluation of the first ciphertext, the second ciphertext, and an approximation function for approximating a signum function,

wherein the generating of the ciphertext comprises:

performing homomorphic evaluation of subtraction between the first real-number data and the second real-number data using the first ciphertext and the second ciphertext in an encrypted state; and

performing homomorphic evaluation of the approximation function using a result for the homomorphic evaluation of the subtraction to generate the ciphertext for the result of the size comparison.

5. The ciphertext comparison apparatus of claim 4, wherein the approximation function is a function of approximating the signum function to a polynomial composed of addition and multiplication.

6. The ciphertext comparison apparatus of claim 4, wherein the homomorphic encryption algorithm is an approximate homomorphic encryption algorithm that supports homomorphic evaluation of addition, subtraction, and multiplication.