WHAT IS CLAIMED IS:

1. A method of processing operations of a polynomial-based security algorithm, the method being performed by a computing system and comprising:

identifying a plurality of operations using secret information in the polynomial-based security algorithm;

generating a random index to be applied to the identified operations; and

performing the operations using the random index;

wherein:

the generating the random index comprises either one of:

generating a random index to be applied to the operations based on operation length or whether the same secret information is used,

generating a random index to be applied to operations having the same operation length among the operations, or

generating different random indices for the operations.

2. The method of claim 1, wherein the generating the random index comprises:

obtaining a plurality of parameters related to an operation length for secret information included in each identified operation; and

generating a random index to be applied to operations having the same length of each of the parameters among the operations.

3. The method of claim 1, wherein the generating the random index comprises generating a first random index to be applied to an operation using first secret information among the operations and generating a second random index to be applied to an operation using second secret information among the operations.

4. The method of claim 1, further comprising:

identifying a first operation group and a second operation group based on a type of operation and an order of operations; and

randomly determining an index for determining an operation order of the first operation group and the second operation group.

5. The method of claim 4, wherein the identifying the first operation group and the second operation group based on the type of operation and the order of operations comprises matching the numbers of operations of the first operation group and the second operation group by adding a first dummy operation to the first operation group.

6. The method of claim 4, wherein the identifying the first operation group and the second operation group based on the type of operation and the order of operations comprises:

identifying a first operation included in the first operation group and a second operation included in the second operation group; and

matching a length of the first operation with a length of the second operation by adding a second dummy operation to the first operation,

wherein the second operation corresponds to the first operation.

7. The method of claim 1, wherein the security algorithm comprises operations for key generation and signature generation of Dilithium using lattice-based post quantum cryptography.

8. The method of claim 1, wherein the security algorithm is a digital signature algorithm, and the secret information is information used to generate a private key.

9. An apparatus for processing operations of a polynomial-based security algorithm, the apparatus comprising:

one or more processors;

a memory which loads a computer program to be executed by the processors; and

a storage which stores the computer program,

wherein the computer program comprises instructions for performing:

an operation of identifying a plurality of operations using secret information in the polynomial-based security algorithm;

an operation of generating a random index to be applied to the identified operations; and

an operation of performing the operations using the random index;

wherein:

the operation of generating the random index comprises either one of:

an operation of generating a random index to be applied to the operations based on operation length or whether the same secret information is used,

an operation of generating a random index to be applied to operations having the same operation length among the operations, or

an operation of generating different random indices for the operations.

10. The apparatus of claim 9, wherein the operation of generating the random index comprises:

an operation of obtaining a plurality of parameters related to an operation length for secret information included in each identified operation; and

an operation of generating a random index to be applied to operations having the same length of each of the parameters among the operations.

11. The apparatus of claim 9, wherein the operation of generating the random index comprises an operation of generating a first random index to be applied to an operation using first secret information among the operations and generating a second random index to be applied to an operation using second secret information among the operations.

12. The apparatus of claim 9, further comprising:

an operation of identifying a first operation group and a second operation group based on a type of operation and an order of operations; and

an operation of randomly determining an index for determining an operation order

of the first operation group and the second operation group.

13. The apparatus of claim 12, wherein the operation of identifying the first operation group and the second operation group based on the type of operation and the order of operations comprises an operation of matching the numbers of operations of the first operation group and the second operation group by adding a first dummy operation to the first operation group.

14. The apparatus of claim 12, wherein the operation of identifying the first operation group and the second operation group based on the type of operation and the order of operations comprises:

an operation of identifying a first operation included in the first operation group and a second operation included in the second operation group; and

an operation of matching a length of the first operation with a length of the second operation by adding a second dummy operation to the first operation,

wherein the second operation corresponds to the first operation.