

WHAT IS CLAIMED IS:

1. An electronic device, comprising:

a memory configured to store at least one instruction, and store a plurality of homomorphic ciphertexts, each of the plurality of homomorphic ciphertexts storing a plurality of variable data in an encrypted state; and

a processor configured to execute the at least one instruction,

wherein the processor is configured to generate, by executing the at least one instruction, a bin mask corresponding to a variable combination and having different variable data of the plurality of variable data classified for each of the plurality of homomorphic ciphertexts, and to generate number data corresponding to the variable combination by using the bin mask and the stored plurality of variable data based on a received instruction to perform an operation instruction on the plurality of homomorphic ciphertexts being received.

2. The electronic device of claim 1, wherein each of the plurality of homomorphic ciphertexts comprises a plurality of slots, and

each of the plurality of slots comprises one variable data.

3. The electronic device of claim 1, wherein the bin mask comprises a plurality of slots,

wherein each of the plurality of slots comprises data on whether one variable value is present,

wherein the processor is configured to generate a bin mask for each of the plurality

of variable data comprised in each of the plurality of homomorphic ciphertexts, select bin masks corresponding to the variable combination from among the plurality of generated bin masks, and generate number data with the variable combination by using multiplication between the selected bin masks.

4. The electronic device of claim 1, wherein the bin mask comprises a plurality of slots, and

each of the plurality of slots comprises a plurality of sub slots comprising data on whether one variable value is present,

wherein the processor is configured to generate one bin mask on each of the homomorphic ciphertexts, and generate number data with the variable combination by using sub slots in the bin mask which correspond to the variable combination from among the generated bin masks.

5. The electronic device of claim 4, wherein the plurality of sub slots is configured to be disposed in one slot with a preset bit distance.

6. The electronic device of claim 1, wherein the processor is configured to join a first homomorphic ciphertext and a second homomorphic ciphertext into one homomorphic ciphertext, wherein the first homomorphic ciphertext and the second homomorphic ciphertext each comprises a plurality of data on a same feature.

7. The electronic device of claim 6, wherein the processor is configured to use a first position data in the first homomorphic ciphertext and a second position data in the

second homomorphic ciphertext on common data in the first homomorphic ciphertext and the second homomorphic ciphertext to join the first homomorphic ciphertext and the second homomorphic ciphertext into one homomorphic ciphertext.

8. The electronic device of claim 7, wherein the processor is configured to compare, based on the plurality of data comprised in the first and second homomorphic ciphertexts, wherein the plurality of data of each ciphertext is encrypted with a one-direction encryption scheme using a preset common key, and position data in a homomorphic ciphertext on the encrypted data being input, encrypted data on the first homomorphic ciphertext with encrypted data on the second homomorphic ciphertext, and check the first position data and the second position data which comprise common data between the two homomorphic ciphertexts.

9. A method of processing ciphertext on a homomorphic ciphertext, the method comprising:

storing a plurality of homomorphic ciphertexts, wherein each of the plurality of homomorphic ciphertexts stores a plurality of variable data in an encrypted state;

receiving an instruction to perform an operation on the plurality of homomorphic ciphertexts;

generating a bin mask corresponding to a variable combination and having different variable data classified for each of the plurality of homomorphic ciphertexts;

generating an encrypted number data corresponding to the variable combination by using the generated bin mask and the stored plurality of variable data; and

outputting the encrypted number data.

10. The method of claim 9, wherein each of the plurality of homomorphic ciphertexts comprises a plurality of slots, and

each of the plurality of slots comprises one variable data.

11. The method of claim 9, wherein the bin mask comprises a plurality of slots, and

each of the plurality of slots comprises data on whether one variable value is present,

wherein generating the bin mask comprises generating a plurality of bin masks for each variable data comprised in the homomorphic ciphertext with respect to each homomorphic ciphertext,

wherein generating the encrypted number data comprises selecting bin masks corresponding to the variable combination from among the plurality of generated bin masks, and using multiplication between the selected bin masks to generate number data with the variable combination.

12. The method of claim 9, wherein the bin mask comprises a plurality of slots, and

each of the plurality of slots comprises a plurality of sub slots comprising data on whether one variable value is present,

wherein generating the bin mask comprises generating one bin mask with respect to each of the homomorphic ciphertexts, and

wherein generating the encrypted number data comprises using sub slots in the bin mask corresponding to the variable combination from among the generated bin masks to

generate number data with the variable combination.

13. The method of claim 12, wherein the plurality of sub slots is configured to be disposed in one slot with a preset bit distance.

14. The method of claim 9, further comprising:

joining a first homomorphic ciphertext and a second homomorphic ciphertext into one homomorphic ciphertext, wherein the first homomorphic ciphertext and the second homomorphic ciphertext each comprises a plurality of data on a same feature.

15. The method of claim 14, wherein the joining comprises using a first position data in the first homomorphic ciphertext and a second position data in the second homomorphic ciphertext on common data in the first homomorphic ciphertext and the second homomorphic ciphertext, and joining the first homomorphic ciphertext and the second homomorphic ciphertext into one homomorphic ciphertext.

16. The method of claim 15, wherein the joining comprises comparing, based on the plurality of data comprised in the first and second homomorphic ciphertexts, wherein the plurality of data of each ciphertext is encrypted with a one-direction encryption scheme using a preset common key, and position data in a homomorphic ciphertext on the encrypted data being input, encrypted data on the first homomorphic ciphertext with encrypted data on the second homomorphic ciphertext, and checking the first position data and the second position data which comprise common data between the two homomorphic

ciphertexts.

17. A computer readable recording medium comprising a program for executing a ciphertext processing method, the method comprising:

storing a plurality of homomorphic ciphertexts, wherein each of the plurality of homomorphic ciphertexts stores a plurality of variable data in an encrypted state;

receiving an instruction to perform an operation on the plurality of homomorphic ciphertexts;

generating a bin mask corresponding to a variable combination and having different variable data classified for each of the plurality of homomorphic ciphertexts;

generating an encrypted number data corresponding to the variable combination by using the bin mask; and

outputting the encrypted number data.