

CLAIMS

What is claimed is:

- 5 1. A method of determining an order of encrypted inputs, including a first encrypted input and a second encrypted input, using at least one processor, the first encrypted input including a first encrypted data and the second encrypted input including a second encrypted data, each of the first and second encrypted data being encrypted based on a fully homomorphic encryption scheme, the method comprising:
 - 10 generating a first series of encrypted blocks from the first encrypted data and a second series of encrypted blocks from the second encrypted data;
 - performing a first block-wise operation between the first series of encrypted blocks and the second series of encrypted blocks to obtain a first series of block-wise outputs;
 - performing a second block-wise operation between the first series of encrypted blocks
 - 15 and the second series of encrypted blocks to obtain a second series of block-wise outputs; and
 - determining an order of the first and second encrypted data based on the first series of block-wise outputs and the second series of block-wise outputs,
 - wherein said generating a first series of encrypted blocks comprises generating each encrypted block in the first series of encrypted blocks as an encrypted element of a finite field, said
 - 20 generating a second series of encrypted blocks comprises generating each encrypted block in the second series of encrypted blocks as an encrypted element of the finite field, and the first encrypted data and the second encrypted data are each a single encrypted element of the finite field.
- 25 2. The method according to claim 1, wherein each encrypted block in the first series of encrypted blocks comprises at least two bits, and each encrypted block in the second series of encrypted blocks comprises at least two bits.
3. The method according to claim 1 or 2, wherein
 - 30 the first encrypted data comprises a third series of encrypted blocks, each encrypted block thereof being a single encrypted element of the finite field, and

the second encrypted data comprises a fourth series of encrypted blocks, each encrypted block thereof being a single encrypted element of the finite field.

4. The method according to claim 3, wherein

5 said generating a first series of encrypted blocks comprises generating a plurality of first series of encrypted blocks from the first encrypted data, each first series of encrypted blocks thereof being generated from a corresponding encrypted block in the third series of encrypted blocks of the first encrypted data and each encrypted block of each first series of encrypted blocks thereof being an encrypted element of the finite field,

10 said generating a second series of encrypted blocks comprises generating a plurality of second series of encrypted blocks from the second encrypted data, each second series of encrypted blocks thereof being generated from a corresponding encrypted block in the fourth series of encrypted blocks of the second encrypted data and each encrypted block of each second series of encrypted blocks thereof being an encrypted element of the finite field,

15 said performing a first block-wise operation comprising performing, for each of the plurality of first series of encrypted blocks, the first block-wise operation between the first series of encrypted blocks and the corresponding series of encrypted blocks of the plurality of second series of encrypted blocks to obtain a corresponding first series of block-wise outputs, and

20 said performing a second block-wise operation comprising performing, for each of the plurality of first series of encrypted blocks, the second block-wise operation between the first series of encrypted blocks and the corresponding series of encrypted blocks of the plurality of second series of encrypted blocks to obtain a corresponding second series of block-wise outputs.

25 5. The method according to claim 1, wherein the first series of encrypted blocks corresponds to a vector space representation of the first encrypted data with respect to the finite field, and the second series of encrypted blocks corresponds to a vector space representation of the second encrypted data with respect to the finite field.

30 6. The method according to claim 1, wherein

the first block-wise operation is based on a less-than or greater-than block-wise comparison operation, and

the second block-wise operation is based on an equality block-wise comparison operation.

5

7. The method according to claim 1, wherein said determining the order of the first and second encrypted data comprises performing, for each block-wise output of the second series of block-wise outputs from a second block-wise output to a penultimate block-wise output, a multiplication of the block-wise output and each block-wise output subsequent to the block-wise output to produce a first series of intermediate results.

10

8. The method according to claim 7, wherein said determining the order of the first and second encrypted data further comprises performing, for each block-wise output of the first series of block-wise outputs, a multiplication of the block-wise output with the intermediate result of the first series of intermediate results corresponding to the block-wise output, to produce a second series of intermediate results.

15

9. The method according to claim 8, wherein said determining the order of the first and second encrypted data further comprises:

20

combining the second series of intermediate results to obtain a combined result; and determining the order of the first and second encrypted data based on the combined result.

10. A system for determining an order of encrypted inputs, including a first encrypted input and a second encrypted input, the first encrypted input including a first encrypted data and the second encrypted input including a second encrypted data, each of the first and second encrypted data being encrypted based on a fully homomorphic encryption scheme, the system comprising:

25

a memory; and

30

at least one processor communicatively coupled to the memory and configured to:

generate a first series of encrypted blocks from the first encrypted data and a second series of encrypted blocks from the second encrypted data;

perform a first block-wise operation between the first series of encrypted blocks and the second series of encrypted blocks to obtain a first series of block-wise outputs;

5 perform a second block-wise operation between the first series of encrypted blocks and the second series of encrypted blocks to obtain a second series of block-wise outputs; and

 determine an order of the first and second encrypted data based on the first series of block-wise outputs and the second series of block-wise outputs,

10 wherein said generate a first series of encrypted blocks comprises generating each encrypted block in the first series of encrypted blocks as an encrypted element of a finite field, said generate a second series of encrypted blocks comprises generating each encrypted block in the second series of encrypted blocks as an encrypted element of the finite field, and the first encrypted data and the second encrypted data are each a single encrypted element of the finite
15 field.

11. The system according to claim 10, wherein each encrypted block in the first series of encrypted blocks comprises at least two bits, and each encrypted block in the second series of encrypted blocks comprises at least two bits.

20

12. The system according to claim 10 or 11, wherein
 the first encrypted data comprises a third series of encrypted blocks, each encrypted block thereof being a single encrypted element of the finite field, and
 the second encrypted data comprises a fourth series of encrypted blocks, each encrypted
25 block thereof being a single encrypted element of the finite field.

13. The system according to claim 12, wherein
 said generate a first series of encrypted blocks comprises generating a plurality of first series of encrypted blocks from the first encrypted data, each first series of encrypted blocks

thereof being generated from a corresponding encrypted block in the third series of encrypted blocks of the first encrypted blocks and each encrypted block of each first series of encrypted blocks thereof being an encrypted element of the finite field,

5 said generate a second series of encrypted blocks comprises generating a plurality of second series of encrypted blocks from the second encrypted data, each second series of encrypted blocks thereof being generated from a corresponding encrypted block in the fourth series of encrypted blocks of the second encrypted blocks and each encrypted block of each second series of encrypted blocks thereof being an encrypted element of the finite field,

10 said perform a first block-wise operation comprising performing, for each of the plurality of first series of encrypted blocks, the first block-wise operation between the first series of encrypted blocks and the corresponding series of encrypted blocks of the plurality of second series of encrypted blocks to obtain a corresponding first series of block-wise outputs, and

15 said perform a second block-wise operation comprising performing, for each of the plurality of first series of encrypted blocks, the second block-wise operation between the first series of encrypted blocks and the corresponding series of encrypted blocks of the plurality of second series of encrypted blocks to obtain a corresponding second series of block-wise outputs.

14. The system according to claim 10, wherein the first series of encrypted blocks
20 corresponds to a vector space representation of the first encrypted data with respect to the finite field, and the second series of encrypted blocks corresponds to a vector space representation of the second encrypted data with respect to the finite field.

15. The system according to claim 10, wherein
25 the first block-wise operation is based on a less-than or greater-than block-wise comparison operation, and

 the second block-wise operation is based on an equality block-wise comparison operation.

16. The system according to claim 10, wherein said determine the order of the first and second encrypted data comprises performing, for each block-wise output of the second series of block-wise outputs from a second block-wise output to a penultimate block-wise output, a multiplication of the block-wise output and each block-wise output subsequent to the block-wise output to produce a first series of intermediate results.

17. The system according to claim 16, wherein said determine the order of the first and second encrypted data further comprises performing, for each block-wise output of the first series of block-wise outputs, a multiplication of the block-wise output with the intermediate result of the first series of intermediate results corresponding to the block-wise output, to produce a second series of intermediate results.

18. The system according to claim 17, wherein said determine the order of the first and second encrypted data further comprises:

combining the second series of intermediate results to obtain a combined result; and determining the order of the first and second encrypted data based on the combined result.

19. A computer program product, embodied in one or more non-transitory computer-readable storage mediums, comprising instructions executable by at least one processor to perform a method of determining an order of encrypted inputs, including a first encrypted input and a second encrypted input, the first encrypted input including a first encrypted data and the second encrypted input including a second encrypted data, each of the first and second encrypted data being encrypted based on a fully homomorphic encryption scheme, the method comprising:

generating a first series of encrypted blocks from the first encrypted data and a second series of encrypted blocks from the second encrypted data;

performing a first block-wise operation between the first series of encrypted blocks and the second series of encrypted blocks to obtain a first series of block-wise outputs;

performing a second block-wise operation between the first series of encrypted blocks and the second series of encrypted blocks to obtain a second series of block-wise outputs; and

determining an order of the first and second encrypted data based on the first series of block-wise outputs and the second series of block-wise outputs,

wherein said generating a first series of encrypted blocks comprises generating each encrypted block in the first series of encrypted blocks as an encrypted element of a finite field, said

5 generating a second series of encrypted blocks comprises generating each encrypted block in the second series of encrypted blocks as an encrypted element of the finite field, and the first encrypted data and the second encrypted data are each a single encrypted element of the finite field.

10 20. The computer program product according to claim 19, wherein each encrypted block in the first series of encrypted blocks comprises at least two bits, and each encrypted block in the second series of encrypted blocks comprises at least two bits.