[0003a] This specification provides a computer-implemented method for secure collaborative computation of matrix products, the method comprising: obtaining, by one or more processors of a first party, a first matrix comprising private data of the first party; generating, by the one or more processors of the first party, a first random matrix having the same size as the first matrix; identifying, by the one or more processors of the first party, a first sub-matrix of the first random matrix and a second sub-matrix of the first random matrix, wherein the first sub-matrix of the first random matrix comprises all even columns of the first random matrix, and the second sub-matrix of the first random matrix comprises all odd columns of the first random matrix; computing, by the one or more processors of the first party, first scrambled private data of the first party based on the first matrix, the first random matrix, the first sub-matrix of the first random matrix, and the second sub-matrix of the first random matrix, wherein the private data of the first party are not derivable solely from the first scrambled private data of the first party, wherein the first scrambled private data of the first party comprises a first sum of the first matrix and the first random matrix and a second sum of the first sub-matrix of the first random matrix and the second sub-matrix of the first random matrix; receiving, by the one or more processors of the first party from a second party, second scrambled private data of the second party, wherein the private data of the second party are not derivable solely from the second scrambled private data of the second party; computing, by the one or more processors of the first party, a first addend of the matrix product of the first matrix comprising the private data of the first party and the second matrix comprising the private data of the second party; receiving, by the one or more processors of the first party from the second party, a second addend of the matrix product of the first matrix comprising the private data of the first party and the second matrix comprising the private data of the second party; and computing, by the one or more processors of the first party, the matrix product of the first matrix comprising the private data of the first party and the second matrix comprising the private data of the second party by summing the first addend and the second addend.

[0004] This specification also provides one or more non-transitory computer-readable storage media coupled to one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations in accordance with embodiments of the methods provided herein.

[0005] This specification further provides a system for implementing the methods provided herein. The system includes one or more processors, and a computer-readable

storage medium coupled to the one or more processors having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations in accordance with embodiments of the methods provided herein.

[0005a] This specification also provides an apparatus for implementing the methods provided herein. The apparatus includes multiple modules to perform operations in accordance with embodiments of the methods provided herein.

[0006] It is appreciated that methods in accordance with this specification may include any combination of the aspects and features described herein. That is, methods in accordance with this specification are not limited to the combinations of aspects and features specifically described herein, but also include any combination of the aspects and features provided.

[0007] The details of one or more embodiments of this specification are set forth in the accompanying drawings and the description below. Other features and advantages of this specification will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 is a block diagram illustrating an example system for secret sharing between platform A and platform B without a trusted initializer, according to an embodiment of this specification.

[0009] FIG. 2 is a flowchart illustrating an example secret sharing method between platform A and platform B without a trusted initializer for generating recommendations by platform A, according to an embodiment of this specification.

[0010] FIG. 3 is a flowchart illustrating an example secret sharing method between platform A and platform B for computing an element Z_{ij} of a matrix product of matrix A and matrix B using a secret sharing scheme without a trusted initializer, according to an embodiment of this specification.

[0011] FIG.4 is a flowchart illustrating an example method for generating a recommendation by an item rating and recommendation platform using a secret sharing scheme without a trusted initializer, according to an embodiment of this specification.

CLAIMS

1. A computer-implemented method for secure collaborative computation of matrix products, the method comprising:

obtaining, by one or more processors of a first party, a first matrix comprising private data of the first party;

generating, by the one or more processors of the first party, a first random matrix having the same size as the first matrix;

identifying, by the one or more processors of the first party, a first sub-matrix of the first random matrix and a second sub-matrix of the first random matrix, wherein the first sub-matrix of the first random matrix comprises all even columns of the first random matrix, and the second sub-matrix of the first random matrix comprises all odd columns of the first random matrix;

computing, by the one or more processors of the first party, first scrambled private data of the first party based on the first matrix, the first random matrix, the first sub-matrix of the first random matrix, and the second sub-matrix of the first random matrix, wherein the private data of the first party are not derivable solely from the first scrambled private data of the first party, wherein the first scrambled private data of the first party comprises a first sum of the first matrix and the first random matrix and a second sum of the first sub-matrix of the first random matrix and the second sub-matrix of the first random matrix;

receiving, by the one or more processors of the first party from a second party, second scrambled private data of the second party, wherein the private data of the second party are not derivable solely from the second scrambled private data of the second party;

computing, by the one or more processors of the first party, a first addend of the matrix product of the first matrix comprising the private data of the first party and the second matrix comprising the private data of the second party;

receiving, by the one or more processors of the first party from the second party, a second addend of the matrix product of the first matrix comprising the private data of the first party and the second matrix comprising the private data of the second party; and

computing, by the one or more processors of the first party, the matrix product of the first matrix comprising the private data of the first party and the second matrix comprising the private data of the second party by summing the first addend and the second addend.

2. The method of claim 1, further comprising:

transmitting, by the first party, the first scrambled private data of the first party to the second party.

3. The method of any preceding claim, further comprising:

determining whether the first matrix comprises an even number of columns; and

in response to determining that the first matrix comprises an odd number of columns, appending an all-zero column to the first matrix.

4. The method of any preceding claim, wherein the second scrambled private data of the second party is computed based on the second matrix, a second random matrix having the same size as the second matrix, a first sub-matrix of the second random matrix, and a second sub-matrix of the second random matrix.

5. The method of claim 4, wherein the first sub-matrix of the second random matrix comprises all even rows of the second random matrix, and the second sub-matrix of the second random matrix comprises all odd rows of the second random matrix.

6. The method of claim 4, wherein the second scrambled private data of the second party comprises a first difference between the second matrix and the second random matrix and a second difference of the first sub-matrix of the second random matrix and the second sub-matrix of the second random matrix.

7. The method of any preceding claim, wherein:

the first platform comprises an item rating and recommendation platform;

the private data of the first party comprise rating data that comprise respective ratings of multiple items with respect to multiple users;

the second platform comprises a social network platform; and

the private data of the first party comprise social network data that indicate social relationships between any two of the multiple users.

8. A system for providing data security by secret sharing between a first party and a second party without a trusted initializer, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 7.

9. An apparatus for providing data security by secret sharing between a first party and a second party without a trusted initializer, the apparatus comprising multiple modules for performing the method of any of claims 1 to 7.