CLAIMS

1. A computer-implemented method for a first data party and a second data party to perform a secure collaborative computation of a matrix product of a first matrix comprising first private data of the first party and a second matrix comprising second private data of the second party without a trusted initializer, without the first private data being exposed to the second data party, and without the second private data being exposed to the first data party, the method comprising:

obtaining, by one or more processors of the first party, a first matrix comprising the first private data of the first party, wherein the private data represents first social relationships between any two of the plurality of users and wherein the first party comprises an item rating determined based on solving an optimization problem representing a social relationship between the plurality of users using a first predefined weight associated with the first party and a second predefined weight to prevent overfitting;

generating, by the one or more processors of the first party, a first random matrix having the same size as the first matrix, wherein the first random matrix ensures security of data included in 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 the 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 to the second 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 includes an even number of columns; and

in response to determine that the first matrix includes 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:

a 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;

a 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.