## CLAIMS

What is claimed is:

1. A multi-party data query method for data privacy protection, wherein the multi-party comprises a plurality of data owners, each of the plurality of data owners holds attribute values of several attribute items of N target objects, the method is performed by an intermediate party other than the multi-party, and the method comprises:

obtaining attribute value ciphertexts of the N target objects sent by each data owner to obtain a ciphertext table, wherein one row in the ciphertext table corresponds to one target object, and one column corresponds to one attribute item;

disordering the ciphertext table in units of rows to obtain a disordered table;

sorting, in response to a query instruction of querying sorting-related data for a target attribute item, attribute value ciphertexts corresponding to the target attribute item in the disordered table to obtain a sorted table;

removing a predetermined row filled in the sorted table to obtain the target sorted table; and

obtaining the sorting-related data as a query result based on the target sorted table.

2. The method according to claim 1, wherein the intermediate party is a cryptographic computing system comprising M executors; and

the obtaining attribute value ciphertexts of the N target objects sent by each data owner comprises:

obtaining, by each of the M executors, one attribute value fragment sent by each data owner as an attribute value ciphertext, wherein each attribute value fragment is determined by dividing, by each data owner, an attribute value held by the data owner into M pieces; and

the disordering the ciphertext table in units of rows comprises:

disordering, by each executor in combination with the other (M−1) executors, the ciphertext table in units of rows based on the attribute value ciphertext held by the party by using a secure multi-party computation (MPC) solution.

3. The method according to claim 1, wherein the sorting-related data are a calculation result of performing specified calculation on attribute value ciphertexts at specified X locations in a sorting sequence corresponding to the target attribute item; and

the obtaining the sorting-related data as a query result comprises:

obtaining the target attribute value ciphertexts at the specified X locations from the target sorted table; and

performing the specified calculation on the target attribute value ciphertexts.

4. The method according to claim 1, wherein the disordering the ciphertext table in units of rows comprises:

disordering the ciphertext table by using at least one disordering procedure, wherein any current disordering procedure comprises:

determining, for each target subtable of the ciphertext table, at least one pair of rows to be swapped from the target subtable; and

performing location swapping on each pair of rows to be swapped with a certain probability to obtain a disordered subtable corresponding to the target subtable, and determining an output table in the current round of disordering procedure based on the disordered subtable to form the disordered table.

5. The method according to claim 4, wherein the certain probability is determined based on a random number generated for the pair of rows to be swapped.

6. The method according to claim 4, wherein when the current disordering procedure is a first disordering procedure, the target subtable is the ciphertext table; and when the current disordering procedure is not the first disordering procedure, the target subtable is a table whose quantity of rows is not less than 2 in an output table corresponding to an above-mentioned disordering procedure.

7. The method according to claim 4, wherein the determining at least one pair of rows to be swapped from the target subtable comprises:

determining an iteration threshold based on a quantity of rows in the target subtable; and

iteratively performing a plurality of iteration processes, wherein each iteration process comprises: selecting at least one pair of rows to be swapped from the target subtable based on at least a current quantity of iterations until an iteration end condition related to the iteration threshold is satisfied.

8. The method according to claim 7, wherein the selecting at least one pair of rows to be swapped from the target subtable based on at least a current quantity of iterations comprises:

respectively selecting, from the target subtable, a row whose corresponding row number is equal to the current quantity of iterations and a row whose corresponding row number is equal to a sum of the current quantity of iterations and the iteration threshold as a pair of rows to be swapped.

9. The method according to claim 7, wherein the determining an output table in the current round of disordering procedure based on the disordered subtable comprises:

dividing the disordered subtable by using the iteration threshold to determine the output table in the current round of disordering procedure.

10. The method according to claim 7, wherein a form of the iteration threshold is $2^m$, and m and the quantity n of rows in the target subtable satisfy the following condition: $2^m<n<=2^{m+1}$.

11. The method according to claim 7, wherein a row number corresponding to each row in the ciphertext table is represented in a binary way; and

the selecting at least one pair of rows to be swapped from the target subtable based on at least a current quantity of iterations comprises:

selecting, from the target subtable, two rows whose corresponding row numbers are the same in bits other than an $i^{th}$ bit as a pair of rows to be swapped, wherein i is equal to the current quantity of iterations, and the target subtable is the ciphertext table.

12. The method according to any one of claims 1 to 11, wherein the sorting attribute value ciphertexts corresponding to the target attribute item in the disordered table comprises:

iteratively performing a plurality of sorting procedures, wherein any sorting procedure comprises:

determining, for each table part currently to be sorted in the disordered table, a reference ciphertext from attribute value ciphertexts corresponding to the target attribute item comprised in the table part;

grouping, based on the reference ciphertext, other attribute value ciphertexts corresponding to the target attribute item comprised in the table part, to obtain a first row set larger than the reference ciphertext and a second row set smaller than the reference ciphertext; and

using a set whose quantity of rows is greater than 1 in the first row set and the second row set corresponding to each table part as a table part to be sorted corresponding to a next sorting procedure, until the target sorted table is obtained.

13. The method according to claim 12, wherein a third row set equal to the reference ciphertext is further obtained through the grouping.

14. The method according to claim 13, wherein the any sorting procedure further comprises: arranging the first row set, the second row set, and the third row set corresponding to each table part, so that the first row set is placed below the third row set, and the second row set is placed above of the third row set.

15. The method according to any one of claims 1 to 11, wherein the disordering the ciphertext table in units of rows comprises:

determining whether a total quantity of rows in the ciphertext table satisfies a predetermined disordering condition, wherein the predetermined disordering condition comprises: a total quantity of rows is equal to an integer power of a predetermined value;

filling the ciphertext table with the predetermined row to obtain a filled table if it is determined that the predetermined disordering condition is not satisfied, wherein a total quantity of rows in the filled table satisfies the predetermined disordering condition; and

disordering the filled table in units of rows to obtain the disordered table.

16. A multi-party data query apparatus for data privacy protection, wherein the multi-party comprises a plurality of data owners, each of the plurality of data owners holds attribute values of several attribute items of N target objects, the apparatus is deployed in an intermediate party other than the multi-party, and the apparatus comprises:

an acquisition module, configured to obtain attribute value ciphertexts of the N target objects sent by each data owner to obtain a ciphertext table, wherein one row in the ciphertext table corresponds to one target object, and one column corresponds to one attribute item;

a disordering module, configured to disorder the ciphertext table in units of rows to obtain a disordered table;

a sorting module, configured to sort, in response to a query instruction of querying sorting-related data for a target attribute item, attribute value ciphertexts corresponding to the target attribute item in the disordered table to obtain a sorted table, and remove a predetermined row filled in the sorted table to obtain the target sorted table; and

a query module, configured to obtain the sorting-related data as a query result based on the target sorted table.

17. A computing device, comprising a memory and a processor, wherein the memory stores executable code, and when executing the executable code, the processor implements the method according to any one of claims 1 to 15.