

MULTI-PARTY DATA QUERY METHODS AND APPARATUSES FOR DATA PRIVACY PROTECTION

ABSTRACT

Embodiments of this specification provide multi-party data query methods and
5 apparatuses for data privacy protection. The multi-party includes a plurality of data
owners, and each of the plurality of data owners holds attribute values of several
attribute items of N target objects, and the method is performed by an intermediate party
other than the multi-party. The method includes following: Attribute value ciphertexts
of the N target objects sent by each data owner are obtained to obtain a ciphertext table,
10 where one row in the ciphertext table corresponds to one target object, and one column
corresponds to one attribute item; the ciphertext table is disordered in units of rows to
obtain a disordered table; 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 are sorted to obtain a target sorted table; and the
15 sorting-related data are obtained as a query result based on the target sorted table.

[FIG. 2]