

保护数据隐私的多方数据查询方法及装置

5 本申请要求于 2021 年 12 月 28 日提交中国国家知识产权局、申请号为 202111621978.6、申请名称为“保护数据隐私的多方数据查询方法及装置”的中国专利申请
申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

10 本说明书涉及数据安全技术领域，尤其涉及一种保护数据隐私的多方数据查询方法
及装置。

背景技术

在大数据背景下，常常需要将不同数据方的业务数据进行综合处理。例如，在对
用户信息进行分析场景中，A 方持有用户的身高、体重等各身体状态数据，B 方持有
用户的工资数据，C 方持有用户的借贷数据。在对多方数据进行联合处理的过程中，
15 数据隐私的保护和安全性成为值得关注的问题。

在数据处理过程中，难免存在对数据进行联合排序的情况，例如，A 方需要查询
工资处于前 N 位的用户的工资总和，或者，需要查询工资处于前 N 位的用户的借贷情
况，或者，需要查询身高处于前 M 位的用户的工资总和，等等。以上情况中，需要对
A、B 和 C 三方所持有的数据进行联合排序，进而基于相应的排序结果得到数据查询
20 结果。如果 A、B 和 C 多方将其持有的用户的隐私数据直接以明文的形式上传至一个
第三方，第三方将数据进行汇总成表格之后，对表格中的相应数据进行排序，以基于
排序结果得到各方所需的数据查询结果，该过程有可能会泄露各方的用户的隐私数据。

那么，如何提供一种在保护数据隐私的前提下，实现多方数据查询方法成为亟待
解决的问题。

25 **发明内容**

本说明书一个或多个实施例提供了一种保护数据隐私的多方数据查询方法及装置，
以实现对方隐私数据的保护。

根据第一方面，提供一种保护数据隐私的多方数据查询方法，所述多方包括多个
数据拥有方，其各自持有 N 个目标对象的若干属性值的属性值，所述方法通过所述多
30 方之外的中间方执行，所述方法包括：

获得各数据拥有方发送的 N 个目标对象的属性值密文，以得到密文表格，其中，

所述密文表格的一行对应于一个目标对象，一列对应于一个属性项；

以行为单位对所述密文表格进行乱序，得到乱序表格；

响应于针对目标属性项查询排序相关数据的查询指令，对所述乱序表格中所述目标属性项对应的属性值密文进行排序，得到目标排序表格，基于所述目标排序表格，

5 得到所述排序相关数据作为查询结果。

在一种可选实施方式中，所述中间方为密态计算系统，其中包括 M 个执行方；

所述获得各数据拥有方发送的 N 个目标对象的属性值密文，包括：

所述 M 个执行方中的各执行方，分别获得各数据拥有方发送的一份属性值分片作为属性值密文，其中，每份属性值分片是，各数据拥有方将其持有的属性值划分成 M
10 份而确定的；

所述以行为单位对所述密文表格进行乱序，包括：

所述各执行方基于本方所持有的属性值密文，通过多方安全计算 MPC 方案，与其他 M-1 个执行方联合以行为单位对所述密文表格进行乱序。

在一种可选实施方式中，所述排序相关数据为，对所述目标属性项对应的排序序
15 列中指定 X 位的属性值密文进行指定计算的计算结果；

所述得到所述排序相关数据作为查询结果，包括：

从所述目标排序表格中得到所述指定 X 位的目标属性值密文；

对所述目标属性值密文进行所述指定计算。

在一种可选实施方式中，所述以行为单位对所述密文表格进行乱序，包括：

20 通过至少一个乱序流程对所述密文表格进行乱序，其中，任一当前乱序流程包括：

针对所述密文表格的各目标子表格，从该目标子表格中确定至少一对置换行；

针对各对置换行，以一定概率执行位置置换，以得到该目标子表格对应的乱序子表格，基于所述乱序子表格确定本轮乱序流程的输出表格，用于形成所述乱序表格。

在一种可选实施方式中，所述一定概率根据针对该对置换行生成的随机数确定。

25 在一种可选实施方式中，所述当前乱序流程为首次乱序流程时，所述目标子表格为所述密文表格；所述当前乱序流程为非首次乱序流程时，所述目标子表格为上一乱

序流程对应的输出表格中行数不小于 2 的表格。

在一种可选实施方式中，所述从该目标子表格中确定至少一对置换行，包括：

基于该目标子表格的行数，确定循环阈值；

- 迭代执行多次循环过程，每次循环过程包括，至少基于当前的循环次数，从该目标子表格中选出至少一对置换行；直到达到与所述循环阈值相关的循环结束条件。

在一种可选实施方式中，所述至少基于当前的循环次数，从该目标子表格中选出至少一对置换行，包括：

从该目标子表格中，分别选择所对应行标号等于当前的循环次数的行，以及所对应行标号等于当前的循环次数与所述循环阈值之和的行，作为一对置换行。

- 在一种可选实施方式中，所述基于所述乱序子表格确定本轮乱序流程的输出表格，包括：

利用所述循环阈值，划分所述乱序子表格，以确定出本轮乱序流程的输出表格。

在一种可选实施方式中，所述循环阈值形式为 2^m ，其中 m 与该目标子表格的行数 n 满足如下条件： $2^m < n \leq 2^{m+1}$ 。

- 在一种可选实施方式中，所述密文表格中各行对应的行标号通过二进制表示；

至少基于当前的循环次数，从该目标子表格中选出至少一对置换行，包括：

从该目标子表格中选择所对应行标号除第 i 位外其他位均相同的两行，作为一对置换行，其中，所述 i 等于所述当前的循环次数，所述目标子表格为所述密文表格自身。

- 在一种可选实施方式中，所述对所述乱序表格中所述目标属性项对应的属性值密文进行排序，包括：

迭代执行多个排序流程，其中，任意一个排序流程，包括：

针对所述乱序表格中当前待排序的各表格部分，从该表格部分包含的目标属性项对应的属性值密文中，确定出基准密文；

- 基于所述基准密文，对该表格部分包含的目标属性项对应的其他属性值密文进行分组，以得到大于所述基准密文的第一行集合，小于所述基准密文的第二行集合；

将各表格部分对应的第一行集合和第二行集合中行数大于 1 的集合，作为下一排序流程对应的待排序的表格部分；直至得到目标排序表格。

在一种可选实施方式中，所述分组还得到等于所述基准密文的第三行集合。

- 5 在一种可选实施方式中，所述任意一个排序流程还包括，将各表格部分对应的第一行集合、第二行集合和第三行集合进行排列放置，使得第一行集合放置于第三行集合的下部，第二行集合放置于第三行集合的上部。

在一种可选实施方式中，所述以行为单位对所述密文表格进行乱序，包括：

判断所述密文表格的总行数是否满足预设乱序条件，其中，所述预设乱序条件包括：总行数等于预设数值的整数次幂；

- 10 若判断不满足所述预设乱序条件，使用特定行填充所述密文表格，得到填充表格，所述填充表格的总行数满足所述预设乱序条件；

以行为单位对所述填充表格进行乱序，以得到乱序表格。

在一种可选实施方式中，所述得到目标排序表格，包括：

对所述乱序表格中所述目标属性项对应的属性值密文进行排序，得到排序后表格；

- 15 将排序后表格中所填充的特定行移除，得到所述目标排序表格。

根据第二方面，提供一种保护数据隐私的多方数据查询装置，所述多方包括多个数据拥有方，其各自持有 N 个目标对象的若干属性值的属性值，所述装置部署在所述多方之外的中间方，所述装置包括：

- 20 获得模块，配置为获得各数据拥有方发送的 N 个目标对象的属性值密文，以得到密文表格，其中，所述密文表格中一行对应于一个目标对象，一列对应于一个属性项；

乱序模块，配置为以行为单位对所述密文表格进行乱序，得到乱序表格；

排序模块，配置为响应于针对目标属性项查询排序相关数据的查询指令，对所述乱序表格中所述目标属性项对应的属性值密文进行排序，得到目标排序表格；

查询模块，配置为基于所述目标排序表格，得到所述排序相关数据作为查询结果。

- 25 在一种可选实施方式中，所述中间方为密态计算系统，其中包括 M 个执行方；

所述获得模块，具体配置为所述 M 个执行方中的各执行方，分别获得各数据拥有

方发送的一份属性值分片作为属性值密文，其中，每份属性值分片是，各数据拥有方将其持有的属性值划分成 M 份而确定的；

所述乱序模块，具体配置为所述各执行方基于本方所持有的属性值密文，通过多方安全计算 MPC 方案，与其他 M-1 个执行方联合以行为单位对所述密文表格进行乱序。

在一种可选实施方式中，所述排序相关数据为，对所述目标属性项对应的排序序列中指定 X 位的属性值密文进行指定计算的计算结果；

所述查询模块，具体配置为从所述目标排序表格中得到所述指定 X 位的目标属性值密文；

10 对所述目标属性值密文进行所述指定计算。

在一种可选实施方式中，所述乱序模块，被具体配置为通过至少一个乱序流程对所述密文表格进行乱序，其中，所述乱序模块通过如下单元实现任一当前乱序流程的执行：

15 第一确定单元，配置为针对所述密文表格的各目标子表格，从该目标子表格中确定至少一对置换行；

位置置换单元，配置为针对各对置换行，以一定概率执行位置置换，以得到该目标子表格对应的乱序子表格；

第二确定单元，配置为基于所述乱序子表格确定本轮乱序流程的输出表格，用于形成所述乱序表格。

20 在一种可选实施方式中，所述一定概率根据针对该对置换行生成的随机数确定。

在一种可选实施方式中，所述当前乱序流程为首次乱序流程时，所述目标子表格为所述密文表格；所述当前乱序流程为非首次乱序流程时，所述目标子表格为上一乱序流程对应的输出表格中行数不小于 2 的表格。

25 在一种可选实施方式中，所述第一确定单元，具体配置为基于该目标子表格的行数，确定循环阈值；

迭代执行多次循环过程，每次循环过程包括，至少基于当前的循环次数，从该目标子表格中选出至少一对置换行；直到达到与所述循环阈值相关的循环结束条件。

在一种可选实施方式中，所述第一确定单元，具体配置为从该目标子表格中，分别选择所对应行标号等于当前的循环次数的行，以及所对应行标号等于当前的循环次数与所述循环阈值之和的行，作为一对置换行。

在一种可选实施方式中，所述第二确定单元，具体配置为利用所述循环阈值，划分所述乱序子表格，以确定出本轮乱序流程的输出表格。

在一种可选实施方式中，所述循环阈值形式为 2^m ，其中 m 与该目标子表格的行数 n 满足如下条件： $2^m < n \leq 2^{m+1}$ 。

在一种可选实施方式中，所述密文表格中各行对应的行标号通过二进制表示；

所述第一确定单元，具体配置为从该目标子表格中选择所对应行标号除第 i 位外其他位均相同的两行，作为一对置换行，其中，所述 i 等于所述当前的循环次数，所述目标子表格为所述密文表格自身。

在一种可选实施方式中，所述排序模块，具体配置为迭代执行多个排序流程，其中，任意一个排序流程，包括：

针对所述乱序表格中当前待排序的各表格部分，从该表格部分包含的目标属性项对应的属性值密文中，确定出基准密文；

基于所述基准密文，对该表格部分包含的目标属性项对应的其他属性值密文进行分组，以得到大于所述基准密文的第一行集合，小于所述基准密文的第二行集合；

将各表格部分对应的第一行集合和第二行集合中行数大于 1 的集合，作为下一排序流程对应的待排序的表格部分；直至得到目标排序表格。

在一种可选实施方式中，所述分组还得到等于所述基准密文的第三行集合。

在一种可选实施方式中，所述排序模块，还具体配置为将各表格部分对应的第一行集合、第二行集合和第三行集合进行排列放置，使得第一行集合放置于第三行集合的下部，第二行集合放置于第三行集合的上部。

在一种可选实施方式中，所述乱序模块，包括：

判断单元，配置为判断所述密文表格的总行数是否满足预设乱序条件，其中，所述预设乱序条件包括：总行数等于预设数值的整数次幂；

填充单元，配置为若判断不满足所述预设乱序条件，使用特定行填充所述密文表

格，得到填充表格，所述填充表格的总行数满足所述预设乱序条件；

乱序单元，配置为以行为单位对所述填充表格进行乱序，以得到乱序表格。

在一种可选实施方式中，所述排序模块，具体配置为：

对所述乱序表格中所述目标属性项对应的属性值密文进行排序，得到排序后表格；

5 将排序后表格中所填充的特定行移除，得到所述目标排序表格。

根据第三方面，提供一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行第一方面所述的方法。

根据第四方面，提供一种计算设备，包括存储器和处理器，其中，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现第一方面所述的方法。

10 根据本说明书实施例提供的方法及装置，各数据拥有方发送属性值密文至中间方，可以避免属性值的泄露。并且，中间方在获得由各数据拥有方发送的属性值密文构建的密文表格之后，首先以行为单位对密文表格进行乱序，以打乱密文表格中各行的前后顺序关系，得到乱序表格。进而对乱序表格中目标属性项对应的属性值密文进行排序。即使对该密文表格中的多个目标属性项对应的属性值密文进行排序，由于在针对
15 任一目标属性项进行排序之前，需要打乱表格中行的前后顺序关系，使得每次排序时，表格中前后行的位置不能追踪，避免了表格中各行在排序列上的顺序关系（例如处于第一属性项排序列第a位的目标对象，即为处于第二属性项排序列第b位的目标对象）的暴露。

附图说明

20 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单的介绍。显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1A 为本说明书披露的一个实施例的实施框架示意图；

25 图 1B 为本说明书披露的一个实施例的实施框架示意图；

图 2 为实施例提供的保护数据隐私的多方数据查询方法的一种流程示意图；

图 3 为实施例提供的一个乱序流程的过程示意图；

图 4 为实施例提供的一个乱序流程的过程示意图；

图 5 为实施例提供的乱序的一种场景示意图；

图 6 为实施例提供的保护数据隐私的多方数据查询装置的一种示意性框图。

5 **具体实施方式**

下面将结合附图，详细描述本说明书实施例的技术方案。

如前所述，在多方联合进行数据处理过程中，数据隐私安全成为目前备受关注的
问题。在具体的数据处理过程中，难免存在对数据进行联合排序的情况。例如，在对
用户信息进行分析场景中，A 方持有用户的身高、体重等各身体状态属性的属性值，B
10 方持有用户的工资属性的属性值（具体的工资数额），C 方持有用户的借贷属性的属
性值（具体的借贷数额）。在 A 方需要查询工资处于前 N 位的用户的工资总和，或者，
需要查询工资处于前 N 位的用户的借贷情况，或者，需要查询身高处于前 M 位的用户
的工资总和与体重处于前 M 位的用户的工资总和的大小等查询需求的情况下，需要对
15 A、B 和 C 三方所持有的数据发送至一个第三方，第三方基于 A、B 和 C 三方所发送
的数据，进行联合排序，进而基于相应的排序结果得到数据查询结果。

第三方在进行数据查询过程中，对 A、B 和 C 三方所发送的数据进行联合排序时，
可以采用目前存在的一种基于类似保序加密方式的排序方式。该排序方式中，第三方
获得各方（A、B 和 C）上传的属性值密文，以获得待排序的表格，该表格中用户标识
和各属性项的属性值是密文的（例如，表格中一行存储一个用户针对多个属性项的属
20 性值密文，一行存储各用户针对一个属性项的属性值密文），但是各行之间的顺序关
系是明文的。后续的，第三方基于指示对目标属性项进行排序的查询请求，直接对该
表格中目标属性项的属性值密文进行排序。

上述数据查询过程中，第三方在使用上述排序方式对数据进行排序的过程中，在
对表格的多列（多个目标属性项）的属性值密文进行排序时，会出现表格中各行在排
25 序列上的顺序关系暴露的情况，例如：目标属性项包括用户的体重属性项和工资属性
项，第三方分别针对表格中体重属性项和工资属性项的属性值密文进行排序后，第三
方可能会得到个人隐私信息如体重第 5 名的人，工资是第 1 名的信息，这在隐私数据
保密情况下是不允许的。

为此，本说明书实施例提供的处理方法，主要针对持有隐私数据（N 个目标对象

的若干属性项的属性值)的多方数据查询的场景而设计。

图 1A 为本说明书披露的一个实施例的实施场景示意图。在该实施场景中，示意性示出了多个数据拥有方，例如，A 方、B 方和 C 方，以及中间方 D，其中，该中间方 D 可以采用密态计算系统实现。各个数据拥有方和中间方各自具体可以体现为：具有计算、处理能力的设备、平台、服务器或设备集群。其中，各数据拥有方持有其方的隐私数据，即 N 个目标对象的若干属性项的属性值，中间方 D 用于接收各数据拥有方(即 A 方、B 方和 C 方)，分别发送的 N 个目标对象的属性值密文，组成密文表格，继而执行后续的数据查询流程。各数据拥有方均不希望其各自持有的数据(N 个目标对象的若干属性项的属性值)泄露，且不希望各行(各目标对象的属性值)在排序列上的顺序关系暴露。

为此，根据本说明书的实施例，各数据拥有方对各自持有的 N 个目标对象的若干属性项的属性值，按照中间方 D 的数据上传要求进行相应处理，得到各属性值的属性值密文；之后，各数据拥有方将其各自的属性值密文，上传至中间方 D。中间方 D 获得各数据拥有方发送的 N 个目标对象的属性值密文，以得到密文表格，该密文表格的一行对应于一个目标对象，一列对应于一个属性项，即该密文表格中一行存储一个目标对象针对多个属性项的属性值密文，一列存储各目标对象针对一个属性项的属性值密文，密文表格可以如下表 1 所示。

表 1

	属性项 1	属性项 2	属性项 3	属性项 4		属性项 V
目标对象 1 的标识 (密文)	属性值密文 11	属性值密文 12	属性值密文 13	属性值密文 14		属性值密文 1V
.....						
目标对象 N 的标识 (密文)	属性值密文 N1	属性值密文 N2	属性值密文 N3	属性值密文 N4		属性值密文 NV

中间方 D 以行为单位对该密文表格进行乱序，即对密文表格进行行乱序，以打乱密文表格中行与行之间的前后顺序关系，使得密文表格中前后行的位置不能追踪，得

到乱序之后的表格，即乱序表格。

中间方 D 响应于针对目标属性项查询排序相关数据的查询指令，对乱序表格中目标属性项对应的属性值密文进行排序，得到目标排序表格，其中，该目标排序表格中各行可以以目标属性项对应的属性值密文的从大到小（或者从小到大）的顺序排序。

- 5 基于目标排序表格，得到排序相关数据作为查询结果。之后将查询结果反馈至查询指令发起方。

可以理解的是，中间方 D 响应于查询指令，对乱序表格中目标属性项对应的属性值密文进行排序，可以作为确定查询指令对应的查询结果的中间流程。此种情况下，排序所得的目标排序表格，一般不会被反馈至查询指令发起方处。

- 10 在一种实现方式中，中间方 D 可以通过密态计算系统实现，其中包括 M 个执行方，该 M 个执行方可以在可信执行环境 TEE 中运行，一个执行方可以通过一个 TEE 实现，此时可以称执行方为可信执行方。另一种情况，该 M 个执行方也可以在普通执行环境中运行。如图 1B 所示，执行方的个数 M 可以设置为 3，各数据拥有方将其持有的每一属性值划分为 3 份，得到每一属性值对应的 3 份属性值分片，各数据拥有方将其持有的每一属性值对应的每份属性值分片分别发送至每一执行方。3 个执行方中的各执行方，分别获得各数据拥有方发送的一份属性值分片作为属性值密文，基于本方所持有的属性值密文，通过多方安全计算 MPC 方案，与其他 2 个执行方联合以行为单位对密文表格进行乱序。

- 20 其中，每一执行方均获得属性值的一部分（属性值分片），每一执行方均无法获得属性值明文，可以避免属性值明文在每一执行方的泄露。且若某一或指定数量以下的执行方被攻击成功，由于该执行方仅获得了属性值的一部分，攻击者也无法通过其攻击成功的执行方，获得各数据拥有方的属性值明文。

并且，各执行方在可信执行环境 TEE 中运行的情况下，该密态计算系统对其数据的保护程度会更高，防攻击能力更好。

- 25 本实施例中，由于在针对任一目标属性项进行排序之前，需要打乱表格中行的前后顺序关系，使得每次排序时，表格中前后行的位置不能追踪，避免了表格中各行在排序列上的顺序关系（例如处于第一属性项排序列第 a 位的目标对象，即为处于第二属性项排序列第 b 位的目标对象）的暴露。

下面结合具体实施例，对本说明书提供的保护数据隐私的多方数据查询方法进行

详细阐述。

图 2 示出了本说明书一个实施例中保护数据隐私的多方数据查询方法的流程图。多方包括多个数据拥有方，多个数据拥有方各自持有 N 个目标对象的若干属性项的属性值，该方法通过多个数据拥有方之外的中间方执行。所述方法包括如下步骤 S210-

5 S240:

S210: 获得各数据拥有方发送的 N 个目标对象的属性值密文，以得到密文表格。其中，密文表格的一行对应于一个目标对象，一列对应于一个属性项，即该密文表格中一行存储一个目标对象针对多个属性项的属性值密文，一列存储各目标对象针对一个属性项的属性值密文。

10 在一种实现方式中，该多个数据拥有方 A_i 在将其所持有的 N 个目标对象的属性值，按照中间方的数据上传要求，发送至该中间方之前，为了保证中间方侧数据查询流程的有效进行，该多个数据拥有方 A_i 之间需要对齐 N 个目标对象的属性值。其中，该对齐可以是，多个数据拥有方 A_i 均按照预设的目标对象排列顺序，排列目标对象的各属性项的属性值，例如，目标对象 1 的所有属性项的属性值处于第一行，目标对象
15 2 的所有属性项的属性值处于第二行，以此类推，目标对象 N 的所有属性项的属性值处于第 N 行。一种实现中，该目标对象可以是如下之一：用户、物品。

可以理解的是，各数据拥有方 A_i 将对齐后的 N 个目标对象的若干属性项的属性值密文发送至中间方时，还需要将相应的 N 个目标对象的对象标识密文发送至中间方。

S220: 以行为单位对密文表格进行乱序，得到乱序表格。中间方可以基于预设乱
20 序方案或以随机的方式，以行为单位对密文表格进行乱序，即打乱密文表格中行与行之间的前后顺序关系，得到乱序表格。在该乱序表格中，无法获知各行具体存储有哪个目标对象的针对多个属性项的属性值密文；在乱序表格中的每一行，目标对象及其对应的各属性项的属性值密文之间的对应关系未改变。

S230: 响应于针对目标属性项查询排序相关数据的查询指令，对乱序表格中目标
25 属性项对应的属性值密文进行排序，得到目标排序表格。其中，该查询指令可以是任一数据拥有方发起的，也可以是使用上述多个数据拥有方所共同提供服务的用户发起的，其中该服务与多个数据拥有方所持有的目标对象的属性值相关。该查询指令中至少包含有指示针对目标属性项的属性值密文进行排序的信息。即该查询指令对应的查询结果即排序相关数据，需要利用针对目标属性项对应的属性值密文的排序结果确定。

排序后，所得到的目标排序表格中，各行以目标属性项对应的属性值密文的从大到小（或者从小到大）的顺序排序。例如：目标排序表格中，目标属性项对应的最大的属性值密文所在行，位于第 1 行；目标属性项对应的次大的属性值密文所在行，位于第 2 行，以此类推，目标属性项对应的最小的属性值密文所在行，位于第 N 行。反之，目标排序表格中，目标属性项对应的最小的属性值密文所在行，位于第 1 行；目标属性项对应的次小的属性值密文所在行，位于第 2 行，以此类推，目标属性项对应的最大的属性值密文所在行，位于第 N 行。

S240：基于目标排序表格，得到排序相关数据作为查询结果。中间方得到目标排序表格之后，可以得到目标属性项对应的属性值密文之间的排序顺序，在该排序顺序的基础上，基于查询指令进行一系列逻辑分析，得到排序相关数据，即查询指令对应的查询结果。将该查询结果发送至查询指令发起方。

在本说明书的一种实现方式中，该排序相关数据为，对目标属性项对应的排序序列中指定 X 位的属性值密文进行指定计算的计算结果；

所述 S240，可以包括如下步骤 01：从目标排序表格中得到指定 X 位的目标属性值密文；步骤 02：对目标属性值密文进行指定计算。

其中，该指定计算包括但不限于求和、求均值、求连乘以及比较大小等计算。

该种情况下，发起该查询指令的数据持有方可以为，未持有目标属性项的数据持有方。

举例而言，多个数据拥有方分别为 A、B、C 三方，目标对象分别为用户 1-N。其中，A 方持有用户 1-N 的身高、体重、年龄各身体状态属性项的属性值，B 方持有用户 1-N 的工资属性项的属性值（具体的工资数额）以及工作年限属性项的属性值（具体的年限数），C 方持有用户 1-N 的借贷属性项的属性值（具体的借贷数额）。

该查询指令为 A 方发送的，用于查询工资属性项的处于前 10 位的工资总和，相应的，排序相关数据为：对工资属性项对应的排序序列中前 10 位的属性值密文（工资数额密文）进行求和计算的计算结果。中间方获得 A、B、C 三方各自上传的用户 1-N 的属性值密文，以得到密文表格；以行为单位对密文表格进行乱序，得到乱序表格；对乱序表格中工资属性项对应的属性值密文进行排序，得到目标排序表格。从目标排序表格中工资属性项对应的属性值密文中，确定出处于前 10 位的属性值密文，即处于前 10 位的工资数额密文，作为目标属性值密文；对目标属性值密文进行密态求和，得

到工资总和密文，即查询结果。后续的，将查询结果发送至 A 方。

在另一种实现方式中，该排序相关数据为，对目标属性项对应的排序序列中指定 h 位目标对象的指定属性项所对应属性值密文进行指定计算的计算结果，该指定属性项为不同于目标属性项的属性项；该种情况下，发起该查询指令的数据持有方可以为，
5 未持有指定属性项和/或目标属性项的数据持有方。

该实现方式中，中间方从目标排序表格中的指定属性项对应的属性值密文中，确定出指定 Y 位的属性值密文，对该指定 Y 位的属性值密文进行指定计算，得到计算结果，作为查询结果。承接上述例子，A 方需要查询工资处于前 Y 位的用户的借贷总和，相应的，查询指令为 A 方发送的，用于查询工资属性项的处于前 10 位的用户的借贷
10 属性项对应的属性值密文总和（即借贷数额总和），也就是说，该查询指令用于查询工资属性项对应的排序表格（目标排序表格）中，工资属性项对应的排序序列中前 10 位用户的借贷属性项的属性值密文之和。

相应的，中间方对乱序表格中工资属性项对应的属性值密文进行排序，得到工资属性项对应的排序表格，即目标排序表格，从目标排序表格中，确定出工资属性项对
15 应的排序序列中处于前 10 位的用户，作为目标用户，并确定该目标用户对应的借贷属性项的属性值密文，进而对所确定出的借贷属性项的属性值密文进行求和，得到求和结果，作为查询结果。

在另一种实现方式中，该查询指令还可以用于，查询第一计算值和第二计算值的比较结果，其中，第一计算值基于第一属性项对应的排序表格中指定属性项对应的指
20 定 h 位的属性值密文和第一计算方式而确定；第二计算值基于第二属性项对应的排序表格中指定属性项对应的指定 h 位的属性值密文和第一计算方式而确定，即该排序相关数据为，对第一属性项对应的排序序列中指定 h 位的目标对象的指定属性项所对应属性值密文，和第二属性项对应的排序序列中指定 h 位的目标对象的指定属性项所对应属性值密文，进行指定计算的计算结果。其中，上述第一属性项和第二属性项均作
25 为目标属性项。

其中，第一属性项、第二属性项和指定属性项各不相同。该种情况下，发起该查询指令的数据持有方可以为，未持有指定属性项、第一属性项和/或第二属性项的任一数据持有方。

在上述情况中，中间方针对各目标属性项（即第一属性项或第二属性项）进行排

序之前，均需要先对待排序的表格（例如密文表格或者前一排序的表格）进行乱序。
具体的可以是：中间方首先针对作为目标属性项的第一属性项进行排序，即对乱序表格中第一属性项对应的属性值密文进行排序，得到第一目标排序表格，从第一目标排序表格中，确定出第一属性项对应的排序序列中指定 h 位的目标对象，作为第一组对象，从第一目标排序表格中确定出第一组对象的指定属性项所对应属性值密文，作为第一组属性值密文；基于第一组属性值密文以及第一计算方式，得到第一计算值。

之后，针对作为目标属性项的第二属性项进行排序，即重新对密文表格（或者第一目标排序表格）以行为单位进行乱序，得到乱序后的第一表格，响应于前述查询指令，对第一表格中第二属性项对应的属性值密文进行排序，得到第二目标排序表格。
10 然后，从第二目标排序表格中，确定出第二属性项对应的排序序列中指定 h 位的目标对象，作为第二组对象，从第二目标排序表格中确定出第二组对象的指定属性项所对应属性值密文，作为第二组属性值密文；基于第二组属性值密文以及第一计算方式，得到第二计算值。

比较第一计算值和第二计算值的大小，得到比较结果（即排序相关数据），作为
15 查询结果。将该查询结果反馈至查询指令发起方。

承接上述例子，查询结果表征，A 方需要查询身高（第一属性项）对应的排序序列中前 10 位用户的工资总和，与体重（第二属性项）对应的排序序列中前 10 位用户的工资总和的大小，其中，身高属性项和体重属性项均为目标属性项。也就是说，查询结果表征需要分别针对身高属性项和体重属性项排序，该排序相关数据为，对身高
20 属性项对应的排序序列中身高处于前 10 位用户的工资总和，和体重属性项对应的排序序列中体重处于前 10 位用户的工资总和进行比较的结果。

相应的，中间方对乱序表格中身高属性项对应的属性值密文进行排序，得到身高属性项对应的排序表格，即第一目标排序表格，从第一目标排序表格中，确定出身高处于前 10 位用户的工资属性项对应的属性值密文，作为第一组属性值密文，进而对第一
25 组属性值密文进行密态求和，第一和值。之后，中间方对密文表格（或者第一目标排序表格），以行为单位进行乱序，得到乱序后的第一表格；响应于查询指令，对第一表格中体重属性项对应的属性值密文进行排序，得到第二目标排序表格；从二目标排序表格中，确定出体重处于前 10 位用户的工资属性项对应的属性值密文，作为第二组属性值密文，进而对第二组属性值密文进行密态进行求和，得到第二和值；比较第

一和值与第二和值的大小，得到查询结果（即排序相关数据）。

本实施例，由于在针对任一目标属性项进行排序之前，需要打乱表格中行的前后顺序关系，使得每次排序时，表格中前后行的位置不能追踪，避免了表格中各行在排序序列上的顺序关系（例如处于第一属性项排序列第 a 位的目标对象，即为处于第二属性项排序列第 b 位的目标对象）的暴露。相应的，作为第三方的中间方，其在无法得到各属性值明文的同时，也不会得到表格中各行在排序序列上的顺序关系。

在本说明书的另一实施例中，考虑到对各数据拥有方的隐私数据（属性值）的保护，中间方为密态计算系统，其中包括 M 个执行方。其中，该执行方可以在可信执行环境 TEE（Trusted Execution Environment）中运行相应的，该密态计算系统为可信密态计算（TrustEd Cryptographic Computing，TECC）系统；或者该执行方也可以在普通执行环境中运行。

各数据拥有方将其持有的每一属性值划分为 M 份，得到每一属性值对应的 M 份属性值分片，各数据拥有方将其持有的每一属性值对应的每份属性值分片，分别发送至每一执行方。相应的，所述 S210，被设置为：M 个执行方中的各执行方，分别获得各数据拥有方发送的一份属性值分片作为属性值密文，其中，每份属性值分片是，各数据拥有方将其持有的属性值划分成 M 份而确定的。

进一步的，所述 S220，被设置为：各执行方基于本方所持有的属性值密文，通过多方安全计算 MPC 方案，与其他 M-1 个执行方联合以行为单位对密文表格进行乱序。

本实施例中，每一执行方均获得属性值的一部分（属性值分片），每一执行方均无法获得属性值明文，可以避免属性值明文在每一执行方的泄露。

中间方在对密文表格以行为单位进行乱序时，可以利用相关技术中任一可以实现对表格进行乱序的方式。也可以利用本说明所提供的后续的乱序方式进行乱序，下面对密文表格的乱序方式进行详细阐述。

在本说明书的一个实施例中，所述 S220，可以包括如下步骤：通过至少一个乱序流程对密文表格进行乱序，其中，任一当前乱序流程，可以包括如下步骤 11-13：

步骤 11：针对密文表格的各目标子表格，从该目标子表格中确定至少一对置换行。

步骤 12：针对各对置换行，以一定概率执行位置置换，以得到该目标子表格对应的乱序子表格。

步骤 13: 基于该乱序子表格确定本轮乱序流程的输出表格, 用于形成乱序表格。

其中, 一种实现中, 该一定概率根据针对该对置换行生成的随机数确定。即中间方在确定出目标子表格中的至少一对置换行之后, 针对各对置换行, 生成随机数, 基于该随机数进行位置置换。一种情况, 该随机数可以为第一值或第二值, 第一值可以为 1, 表示置换所对应置换行的位置; 第二值可以为 0, 表示不置换所对应置换行的位置。另一种情况, 该随机数可以 0-1 的值, 其中, 随机数值越大表示置换所对应置换行的位置的概率越大。可以理解的是, 本说明书中所提到的置换所对应置换行的位置指的是, 置换各对置换行中所存储的目标对象的属性值密文, 例如确定需要置换第一行和第四行的位置, 即将第一行所存储的目标对象的属性值密文, 存储至第四行, 将第四行所存储的目标对象的属性值密文存储至第一行。

一种情况中, 中间方通过密态计算系统实现, 其中包括 M 个执行方, 上述针对各对置换行生成的随机数, 是由 M 个执行方中的每一执行方基于其生成的随机数分片, 通过 MPC 方案, 与其他 M-1 联合确定的。这样, 每一执行方仅生成了该随机数的分片, 无法获知随机数, 相应的, 各对置换行是否真正的置换了位置, 各个执行方也无法获知。

在一种实现中, 中间方可以预存有乱序流程阈值, 相应的, 在首次乱序流程中, 密态计算系统可以直接将密文表格作为目标子表格。或者也可以从密文表格, 确定出至少一个目标子表格, 其中, 每一目标子表格包括连续的至少两行。

后续的, 中间方针对每一目标子表格, 从该目标子表格中确定出至少一对置换行, 针对各对置换行, 以一定概率执行位置置换, 以得到该目标子表格对应的乱序子表格。之后, 中间方获得本轮乱序流程的所有目标子表格对应的乱序子表格, 基于所有目标子表格对应的乱序子表格, 确定本轮乱序流程的输出表格。

在乱序流程执行个数未达到乱序流程阈值的情况下, 一种情况, 可以直接将本轮乱序流程的输出表格 (部分行乱序之后的密文表格), 作为一个目标子表格, 循环执行后续的流程 (即步骤 11-13), 直至乱序流程执行个数达到乱序流程阈值, 得到乱序表格。另一种情况, 确定出目标子表格对应的乱序子表格之后, 基于所确定的至少一对置换行中的一对置换行, 对乱序之后所得的表格进行划分, 得到多个子表格, 将该多个子表格作为本轮乱序流程对应的输出表格, 其中每一输出表格即为后一乱序流程的目标子表格, 进而执行后续流程, 直至乱序流程执行个数达到乱序流程阈值, 得到

乱序表格。

在另一种实现方式中，任一当前乱序流程，如图 3 所示，可以包括如下步骤：

S310: 针对密文表格的各目标子表格，基于该目标子表格的行数，确定循环阈值。
一种情况中，该循环阈值形式为 2^m ，其中 m 与该目标子表格的行数 n 可以满足如下条件： $2^m < n \leq 2^{m+1}$ 。中间方针对每一目标子表格，可以将该目标子表格作为一个单独的
5 需要乱序的表格，针对该目标子表格中所包含的各行，重新为其配置新的行标号。例如，重新将目标子表格中的第一行的行标号设置为 0（或者 1），之后的行的行标号依次递增 1。

S320: 至少基于当前的循环次数，从该目标子表格中选出一对置换行。

10 S330: 针对该对置换行，以一定概率执行位置置换。

S340: 更新循环次数，基于更新后的循环次数，判断是否达到与循环阈值相关的循环结束条件。若判断未达到与循环阈值相关的循环结束条件，返回执行 S320；

S350: 若判断达到与循环阈值相关的循环结束条件，得到该目标子表格对应的乱序子表格，并基于所有目标子表格对应的乱序子表格，确定本轮乱序流程的输出表格，
15 用于形成乱序表格。

其中，判断是否达到与循环阈值相关的循环结束条件，可以是，循环次数的初始值为 0，更新一次循环次数为针对当前的循环次数加一，相应的，加一后的循环次数达到循环阈值，即达到与循环阈值相关的循环结束条件。也可以是，循环次数的初始值为循环阈值，更新一次循环次数为针对当前的循环次数减一，相应的，减一后的循环次数为 0，即达到与循环阈值相关的循环结束条件。
20

在一种实现中，中间方可以基于当前的循环次数和循环阈值，从该目标子表格中选出至少一对置换行。具体的，可以是：从该目标子表格中，分别选择所对应行标号等于当前的循环次数的行，以及所对应行标号等于当前的循环次数与循环阈值之和的行，作为一对置换行。

25 在一种实现方式中，前述 S350，可以被设置为，利用循环阈值，划分乱序子表格，以确定出本轮乱序流程的输出表格。其中，可以直接将目标子表格对应的乱序子表格中所对应行标号为循环阈值的行，作为划分基准行，将该乱序子表格中该划分基准行及其之前的行作为一个新的表格，该划分基准行之后的行作为一个新的表格，作为本

轮乱序流程的输出表格。

在当前乱序流程中，针对所有的目标子表格执行上述 S310-S350，以得到本轮乱序流程的所有输出表格。可以理解的是，在当前乱序流程，在对各目标子表格的乱序子表格进行划分之后，出现划分之后所得的所有新的表格的行数均小于 2，即本轮乱序流程的输出表格的行数均小于 2 的情况，则直接基于本轮乱序流程的输出表格，生成乱序表格。

一种实现中，在上述乱序过程中，中间方可以记录密文表格与各目标子表格之间的位置关系，并且记录各目标子表格对应的乱序子表格与其划分后的新的子表格之间的位置关系，相应的，中间方可以基于上述位置关系，确定出每一轮乱序流程的输出表格之间的位置关系。在一轮乱序流程的输出表格的行数均小于 2 之后，直接基于本轮乱序流程的输出表格之间的位置关系，生成乱序表格。

其中，为了提高乱序速度，可以在任意乱序流程中，并行化执行对各目标子表格的乱序步骤。

举例而言，密文表格（表格 1）包含 4 行，行标号分别 0-3，每行分别表示为 X[0]-X[3]，其中，X[0]存储于目标对象 1 的所有属性项的属性项密文，X[1]存储于目标对象 2 的所有属性项的属性项密文，X[2]存储于目标对象 3 的所有属性项的属性项密文，X[3]存储于目标对象 4 的所有属性项的属性项密文。

首次乱序流程，表格 1 作为目标子表格，基于表格 1 的行数，确定循环阈值 2 ($2^1 < 8 \leq 2^2$)；从表格 1 中分别选择所对应行标号等于当前的循环次数 0 的行(X[0])，以及所对应行标号等于当前的循环次数 0 与循环阈值 2 之和的行(X[2])，作为一对置换行；以一定概率针对 X[0]和 X[2]两行执行位置置换，X[0]和 X[2]两行是否真实的执置换位置的概率是随机的。其中，若置换 X[0]和 X[2]，即将目标对象 3 的所有属性项的属性项密文存储至 X[0]，将目标对象 1 的所有属性项的属性项密文存储至 X[2])。

接着，循环次数加一，从表格 1 中分别选择所对应行标号等于当前的循环次数 1 的行(X[1])，以及所对应行标号等于当前的循环次数 1 与循环阈值 2 之和的行(X[3])，作为一对置换行，以一定概率针对 X[1]和 X[3]两行执行位置置换，是否真实的进行位置置换随机。循环次数加一（为 2），达到了循环结束条件 ($2=2$)，得到表格 1 的乱序子表格（表格 2），其中，表格 2 中的，X[0]、X[1]、X[2]以及 X[3]存储的是哪个目标对象的所有属性项的属性值是不确定的。

基于循环阈值2划分表格2,得到两个新的子表格分别为表格3(包括X[0]和X[1])和表格4(包括X[2]和X[3]),作为第一轮乱序流程的输出表格。针对表格4(表格3)重新设置其行的行标号X[0]'和X[1]',其中,X[0]'对应X[2],X[1]'对应X[3]。

- 5 第二轮乱序流程,将表格3和表格4分别作为目标子表格,针对表格3(表格4),基于其行数2,确定循环阈值为0;从表格3(表格4)中,分别选择所对应行标号等于当前的循环次数0的行X[0](X[0]'),以及所对应行标号等于当前的循环次数与所述循环阈值之和的行X[1](X[1]'),作为一对置换行。以一定概率针对X[0](X[0]')和X[1](X[1]')执行位置置换,得到表格3对应的乱序子表格即表格5(表格4对应的乱序子表格,即表格6)。基于循环阈值0划分表格5(表格6),得到两个新的子表格,分别为表格7和表格8(表格9和表格10),作为第二轮乱序流程的输出表格,其中,第二轮乱序流程的输出表格的行数均为1,小于2,则基于第二轮乱序流程的输出表格,生成乱序表格。

在另一种实现方式中,任一当前乱序流程,如图4所示,可以包括如下步骤S410-S450:

- 15 S410: 基于密文表格的行数,确定循环阈值。一种情况中,该循环阈值的形式为m,该m与该目标子表格的行数n可以满足如下条件: $2^m < n \leq 2^{m+1}$ 。

S420: 从密文表格中,选择所对应行标号除第i位外其他位均相同的两行,作为一对置换行对,以得到至少一对置换行,其中,i等于当前的循环次数。

- 20 S430: 针对各对置换行,以一定概率执行位置置换。其中,该一定概率根据针对所对应置换行生成的随机数确定。

S440: 更新循环次数,基于更新后的循环次数,判断是否达到与循环阈值相关的循环结束条件。若判断未达到,返回执行S420;

S450: 若判断达到,得到本轮乱序流程的输出表格,并基于该输出表格生成乱序表格。

- 25 本实施例中,密文表格中各行的行标号通过二进制表示,具体的二进制的位数可以根据实际情况进行设置,例如4位,8位等。在4位的情况下,可以例如第一行X[0],对应的行标号表示为0000,第二行X[1],对应的行标号表示为0001,以此类推。

在确定出循环阈值之后,可以设置循环次数i的取值范围为[0, m-1]中的整数。i

可以从 0 开始取，相应的，更新循环次数为在当前的循环次数加一，达到与循环阈值相关的循环结束条件为更新后的循环次数达到循环阈值。另一种情况，i 也可以从 m-1 开始取，此时，更新循环次数为在当前的循环次数减一，达到与循环阈值相关的循环结束条件为更新后的循环次数为 0。

- 5 一种实现中，为了提高乱序速度，可以在任意乱序流程中，并行化执行对各对置换行的位置置换步骤。

如图 5 所示，以密文表格（目标子表格）中包含 4 行为例说明，4 行对应的行标号分别表示为：第一行 X[0]对应的行标号为 0000，第二行 X[1]对应的行标号为 0001，第三行 X[2]对应的行标号为 0010，第四行 X[3]对应的行标号为 0011。其中，循环阈值为 2，相应的，i 可以取值 0,1。i 等于 0 时，从该密文表格中选择所对应行标号除第 0 位外其他位均相同的两行，作为一对置换行对，以得到至少一对置换行，具体为：第一行 X[0]和第二行 X[1]为一对置换行，第三行 X[2]和第四行 X[3] 为一对置换行。

针对第一行 X[0]和第二行 X[1]，以一定概率进行位置置换，并针对第三行 X[2]和第四行 X[3]，以一定概率进行位置置换，得到中间排序表格。其中，各行之间的位置关系被重排。

更新 i，更新后的 i 等于 1，从该中间排序表格（前一次循环的结果）中选择所对应行标号除第 1 位外其他位均相同的两行，作为一对置换行对，以得到至少一对置换行，具体为：第一行 X[0]和第三行 X[2]为一对置换行，第二行 X[1]和第四行 X[3] 为一对置换行。针对第一行 X[0]和第三行 X[2]，以一定概率进行位置置换，并针对第二行 X[1]和第四行 X[3]，以一定概率进行位置置换。

更新 i，更新后的 i 等于 2，达到循环结束条件，得到乱序表格。

本实施例可以通过一个乱序流程实现对密文表格的乱序，打乱表格中行的前后顺序关系，使得每次排序时，表格中前后行的位置不能追踪，避免了表格中各行在排序列上的顺序关系（例如处于第一属性项排序列第 a 位的目标对象，即为处于第二属性项排序列第 b 位的目标对象）的暴露。

在本说明书的一种实现方式中，为了实现密文表格的乱序效果更好，所述 S220，可以包括如下步骤 21-22：

步骤 21：判断密文表格的总行数是否满足预设乱序条件，其中，预设乱序条件包

括：总行数等于预设数值的整数次幂。其中，该预设数值可以根据实际情况设置，一种情况，该预设数值为 2。

步骤 22：若判断满足预设乱序条件，以行为单位对密文表格进行乱序。其中，在密文表格的总行数满足预设乱序条件下，在一定程度上可以使得密文表格中各行被确定为 5 一对置换行中的一行的概率均等，避免出现某些行被执行位置置换的概率很小，在一定程度上影响乱序效果。例如，密文表格中包括 5 行，利用前述图 3 所示的乱序流程，会出现第 5 行未参与乱序的情况，这在一定程度上存在第 5 行所存储的目标对象的某些隐私数据被泄露的隐患。为了降低上述情况的发生，提高乱序效果，中间方在判断密文表格满足不预设乱序条件的情况下，所述 S220，还可以包括步骤 23-24：

10 步骤 23，使用特定行填充密文表格，得到填充表格，填充表格的总行数满足预设乱序条件；步骤 24，以行为单位对填充表格进行乱序，以得到乱序表格。该特定行对应的行标号不同于密文表格中各行的行标号，该特定行中可以包含指定类数据的密文。

后续的，在对填充特定行的填充表格进行乱序，得到其对应的乱序表格之后，响应于针对目标属性项查询排序相关数据的查询指令，对乱序表格中目标属性项对应的 15 属性值密文进行排序，得到排序后表格，并将排序后表格中所填充的特定行移除，得到目标排序表格。

在另一实现方式中，在判断密文表格不满足预设乱序条件的情况下，还可以在针对乱序表格以行为单位进行乱序之后，确定出其中参加乱序流程次数较少的行（例如：所对应行标号大于 2^m 的行），将该类行以随机方式进行乱序，例如，该类行之间进 20 行随机行乱序，或者将该类行随机插入其他行（例如：该类行随机插入表格中所对应行标号不大于 2^m 的行）。以更好的打乱该类行的前后行的位置顺序关系。

本说明书实施例中，中间方可以通过多种排序算法，对乱序表格的目标属性项的属性值密文进行排序，例如：merge 排序算法、堆排序算法等。本说明书实施例提供了一种排序方式，具体的，所述 S240，可以包括：迭代执行多个排序流程，其中，任 25 意一个排序流程，包括如下步骤 31-33：

步骤 31：针对乱序表格中当前待排序的各表格部分，从该表格部分包含的目标属性项对应的属性值密文中，确定出基准密文。

步骤 32：基于基准密文，对该表格部分包含的其他属性值密文进行分组，以得到大于基准密文的第一行集合，小于基准密文的第二行集合。

步骤 33：将各表格部分对应的第一行集合和第二行集合中行数大于 1 的集合，作为下一排序流程对应的待排序的表格部分；直至得到目标排序表格。一种情况，可以是在各待排序的表格部分对应的第一行集合和第二行集合中行数均不大于 1 的情况下，得到目标排序表格。

- 5 一种实现中，中间方得到乱序表格后，响应于查询指令，对乱序表格迭代执行多个排序流程。其中，在首个排序流程中，乱序表格作为当前待排序的表格部分，从该表格部分包含的目标属性项对应的属性值密文中，确定出一个属性值密文作为基准密文。将该基准密文与目标属性项对象的其他属性值密文进行比较，得到比较结果；进而基于比较结果，对该表格部分包含的目标属性项对应的其他属性值密文进行分组，
- 10 以得到大于基准密文的第一行集合，小于基准密文的第二行集合。其中，第一行集合包括：该表格部分中大于基准密文的目标属性项对象的其他属性值密文所在行，第二行集合包括：该表格部分中小于基准密文的目标属性项对象的其他属性值密文所在行。

- 将该表格部分对应的第一行集合和第二行集合中行数大于 1 的集合，作为下一排序流程对应的待排序的表格部分，返回执行上述步骤 31-33；直至各待排序的表格部分
- 15 对应的第一行集合和第二行集合中行数均不大于 1，得到目标排序表格。

一种情况中，该分组还得到等于基准密文的第三行集合。该第三行集合包括：该表格部分中等于基准密文的目标属性项对象的其他属性值密文所在行。该第三行集合中的行无需再针对目标属性项进行排序。

- 在本说明书的一种实现方式中，该任意一个排序流程还可以包括，将各表格部分
- 20 对应的第一行集合、第二行集合和第三行集合进行排列放置，使得第一行集合放置于第三行集合的下部，第二行集合放置于第三行集合的上部。各表格部分对应的第一行集合、第二行集合和第三行集合按照该种排列放置，可以实现将乱序表格中各行，按照目标属性项对应的属性值密文从小到大的顺序排序。在另一种实现方式中，该任意一个排序流程还可以包括，将各表格部分对应的第一行集合、第二行集合和第三行集
- 25 合进行排列放置，第一行集合放置于第三行集合的上部，第二行集合放置于第三行集合的下部，以实现将乱序表格中各行，按照目标属性项对应的属性值密文从大到小的顺序排序。

其中，为了提高排序速度，可以在任意排序流程中，并行化执行对各表格部分的排序。

上述内容对本说明书的特定实施例进行了描述，其他实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行，并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要按照示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的，或者可能是有利的。

相应于上述方法实施例，本说明书实施例，提供了一种的保护数据隐私的多方数据查询装置 600，所述多方包括多个数据拥有方，其各自持有 N 个目标对象的若干属性值的属性值，所述装置部署在多方之外的中间方，其示意性框图如图 6 所示，包括：

获得模块 610，配置为获得各数据拥有方发送的 N 个目标对象的属性值密文，以得到密文表格，其中，所述密文表格中一行对应于一个目标对象，一列对应于一个属性项；

乱序模块 620，配置为以行为单位对所述密文表格进行乱序，得到乱序表格；

排序模块 630，配置为响应于针对目标属性项查询排序相关数据的查询指令，对所述乱序表格中所述目标属性项对应的属性值密文进行排序，得到目标排序表格；

查询模块 640，配置为基于所述目标排序表格，得到所述排序相关数据作为查询结果。

在一种可选实施方式中，所述中间方为密态计算系统，其中包括 M 个执行方；

所述获得模块 610，具体配置为所述 M 个执行方中的各执行方，分别获得各数据拥有方发送的一份属性值分片作为属性值密文，其中，每份属性值分片是，各数据拥有方将其持有的属性值划分成 M 份而确定的；

所述乱序模块 620，具体配置为所述各执行方基于本方所持有的属性值密文，通过多方安全计算 MPC 方案，与其他 M-1 个执行方联合以行为单位对所述密文表格进行乱序。

在一种可选实施方式中，所述排序相关数据为，对所述目标属性项对应的排序序列中指定 X 位的属性值密文进行指定计算的计算结果；

所述查询模块 640，具体配置为从所述目标排序表格中得到所述指定 X 位的目标属性值密文；

对所述目标属性值密文进行所述指定计算。

在一种可选实施方式中，所述乱序模块 620，被具体配置为通过至少一个乱序流程对所述密文表格进行乱序，其中，所述乱序模块 620 通过如下单元实现任一当前乱序流程的执行：

第一确定单元（图中未示出），配置为针对所述密文表格的各目标子表格，从该
5 目标子表格中确定至少一对置换行；

位置置换单元（图中未示出），配置为针对各对置换行，以一定概率执行位置置换，以得到该目标子表格对应的乱序子表格；

第二确定单元（图中未示出），配置为基于所述乱序子表格确定本轮乱序流程的输出表格，用于形成所述乱序表格。

10 在一种可选实施方式中，所述一定概率根据针对该对置换行生成的随机数确定。

在一种可选实施方式中，所述当前乱序流程为首次乱序流程时，所述目标子表格为所述密文表格；所述当前乱序流程为非首次乱序流程时，所述目标子表格为上一乱序流程对应的输出表格中行数不小于 2 的表格。

在一种可选实施方式中，所述第一确定单元，具体配置为基于该目标子表格的行
15 数，确定循环阈值；

迭代执行多次循环过程，每次循环过程包括，至少基于当前的循环次数，从该目标子表格中选出至少一对置换行；直到达到与所述循环阈值相关的循环结束条件。

在一种可选实施方式中，所述第一确定单元，具体配置为从该目标子表格中，分别选择所对应行标号等于当前的循环次数的行，以及所对应行标号等于当前的循环次数
20 与所述循环阈值之和的行，作为一对置换行。

在一种可选实施方式中，所述第二确定单元，具体配置为利用所述循环阈值，划分所述乱序子表格，以确定出本轮乱序流程的输出表格。

在一种可选实施方式中，所述循环阈值形式为 2^m ，其中 m 与该目标子表格的行数 n 满足如下条件： $2^m < n \leq 2^{m+1}$ 。

25 在一种可选实施方式中，所述密文表格中各行对应的行标号通过二进制表示；

所述第一确定单元，具体配置为从该目标子表格中选择所对应行标号除第 i 位外其他位均相同的两行，作为一对置换行，其中，所述 i 等于所述当前的循环次数，所

述目标子表格为所述密文表格自身。

在一种可选实施方式中，所述排序模块 630，具体配置为迭代执行多个排序流程，其中，任意一个排序流程，包括：

- 5 针对所述乱序表格中当前待排序的各表格部分，从该表格部分包含的目标属性项对应的属性值密文中，确定出基准密文；

基于所述基准密文，对该表格部分包含的目标属性项对应的其他属性值密文进行分组，以得到大于所述基准密文的第一行集合，小于所述基准密文的第二行集合；

将各表格部分对应的第一行集合和第二行集合中行数大于 1 的集合，作为下一排序流程对应的待排序的表格部分；直至得到目标排序表格。

- 10 在一种可选实施方式中，所述分组还得到等于所述基准密文的第三行集合。

在一种可选实施方式中，所述排序模块 630，还具体配置为将各表格部分对应的第一行集合、第二行集合和第三行集合进行排列放置，使得第一行集合放置于第三行集合的下部，第二行集合放置于第三行集合的上部。

在一种可选实施方式中，所述乱序模块 620，包括：

- 15 判断单元（图中未示出），配置为判断所述密文表格的总行数是否满足预设乱序条件，其中，所述预设乱序条件包括：总行数等于预设数值的整数次幂；

填充单元（图中未示出），配置为若判断不满足所述预设乱序条件，使用特定行填充所述密文表格，得到填充表格，所述填充表格的总行数满足所述预设乱序条件；

- 20 乱序单元（图中未示出），配置为以行为单位对所述填充表格进行乱序，以得到乱序表格。

在一种可选实施方式中，所述排序模块 630，具体配置为：

对所述乱序表格中所述目标属性项对应的属性值密文进行排序，得到排序后表格；

将排序后表格中所填充的特定行移除，得到所述目标排序表格。

- 25 上述装置实施例与方法实施例相对应，具体说明可以参见方法实施例部分的描述，此处不再赘述。装置实施例是基于对应的方法实施例得到，与对应的方法实施例具有同样的技术效果，具体说明可参见对应的方法实施例。

本说明书实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，当

所述计算机程序在计算机中执行时，令计算机执行本说明书所提供的所述保护数据隐私的多方数据查询方法。

本说明书实施例还提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现本说明书所提供的所述保护数据隐私的多方数据查询方法。

本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于存储介质和计算设备实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。

10 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明实施例所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

15 以上所述的具体实施方式，对本发明实施例的目的、技术方案和有益效果进行了进一步的详细说明。所应理解的是，以上所述仅为本发明实施例的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

20

权 利 要 求 书

1、一种保护数据隐私的多方数据查询方法，所述多方包括多个数据拥有方，其各自持有 N 个目标对象的若干属性值的属性值，所述方法通过所述多方之外的中间方执行，所述方法包括：

获得各数据拥有方发送的 N 个目标对象的属性值密文，以得到密文表格，其中，所述密文表格的一行对应于一个目标对象，一列对应于一个属性项；

以行为单位对所述密文表格进行乱序，得到乱序表格；

响应于针对目标属性项查询排序相关数据的查询指令，对所述乱序表格中所述目标属性项对应的属性值密文进行排序，得到目标排序表格，基于所述目标排序表格，得到所述排序相关数据作为查询结果。

2、根据权利要求 1 所述的方法，其中，所述中间方为密态计算系统，其中包括 M 个执行方；

所述获得各数据拥有方发送的 N 个目标对象的属性值密文，包括：

所述 M 个执行方中的各执行方，分别获得各数据拥有方发送的一份属性值分片作为属性值密文，其中，每份属性值分片是，各数据拥有方将其持有的属性值划分成 M 份而确定的；

所述以行为单位对所述密文表格进行乱序，包括：

所述各执行方基于本方所持有的属性值密文，通过多方安全计算 MPC 方案，与其他 $M-1$ 个执行方联合以行为单位对所述密文表格进行乱序。

3、根据权利要求 1 所述的方法，其中，所述排序相关数据为，对所述目标属性项对应的排序序列中指定 X 位的属性值密文进行指定计算的计算结果；

所述得到所述排序相关数据作为查询结果，包括：

从所述目标排序表格中得到所述指定 X 位的目标属性值密文；

对所述目标属性值密文进行所述指定计算。

4、根据权利要求 1 所述的方法，其中，所述以行为单位对所述密文表格进行乱序，包括：

通过至少一个乱序流程对所述密文表格进行乱序,其中,任一当前乱序流程包括:

针对所述密文表格的各目标子表格,从该目标子表格中确定至少一对置换行;

针对各对置换行,以一定概率执行位置置换,以得到该目标子表格对应的乱序子表格,基于所述乱序子表格确定本轮乱序流程的输出表格,用于形成所述乱序表格。

5、根据权利要求4所述的方法,其中,所述一定概率根据针对该对置换行生成的随机数确定。

6、根据权利要求4所述的方法,其中,所述当前乱序流程为首次乱序流程时,所述目标子表格为所述密文表格;所述当前乱序流程为非首次乱序流程时,所述目标子表格为上一乱序流程对应的输出表格中行数不小于2的表格。

7、根据权利要求4所述的方法,其中,所述从该目标子表格中确定至少一对置换行,包括:

基于该目标子表格的行数,确定循环阈值;

迭代执行多次循环过程,每次循环过程包括,至少基于当前的循环次数,从该目标子表格中选出至少一对置换行;直到达到与所述循环阈值相关的循环结束条件。

8、根据权利要求7所述的方法,其中,所述至少基于当前的循环次数,从该目标子表格中选出至少一对置换行,包括:

从该目标子表格中,分别选择所对应行标号等于当前的循环次数的行,以及所对应行标号等于当前的循环次数与所述循环阈值之和的行,作为一对置换行。

9、根据权利要求7所述的方法,其中,所述基于所述乱序子表格确定本轮乱序流程的输出表格,包括:

利用所述循环阈值,划分所述乱序子表格,以确定出本轮乱序流程的输出表格。

10、根据权利要求7所述的方法,其中,所述循环阈值形式为 2^m ,其中 m 与该目标子表格的行数 n 满足如下条件: $2^m < n \leq 2^{m+1}$ 。

11、根据权利要求7所述的方法,其中,所述密文表格中各行对应的行标号通过二进制表示;

至少基于当前的循环次数,从该目标子表格中选出至少一对置换行,包括:

从该目标子表格中选择所对应行标号除第 i 位外其他位均相同的两行,作为一对

置换行，其中，所述 i 等于所述当前的循环次数，所述目标子表格为所述密文表格自身。

12、根据权利要求 1-11 任一项所述的方法，其中，所述对所述乱序表格中所述目标属性项对应的属性值密文进行排序，包括：

迭代执行多个排序流程，其中，任意一个排序流程，包括：

针对所述乱序表格中当前待排序的各表格部分，从该表格部分包含的目标属性项对应的属性值密文中，确定出基准密文；

基于所述基准密文，对该表格部分包含的目标属性项对应的其他属性值密文进行分组，以得到大于所述基准密文的第一行集合，小于所述基准密文的第二行集合；

将各表格部分对应的第一行集合和第二行集合中行数大于 1 的集合，作为下一排序流程对应的待排序的表格部分；直至得到目标排序表格。

13、根据权利要求 12 所述的方法，其中，所述分组还得到等于所述基准密文的第三行集合。

14、根据权利要求 13 所述的方法，其中，所述任意一个排序流程还包括，将各表格部分对应的第一行集合、第二行集合和第三行集合进行排列放置，使得第一行集合放置于第三行集合的下部，第二行集合放置于第三行集合的上部。

15、根据权利要求 1-11 任一项所述的方法，其中，所述以行为单位对所述密文表格进行乱序，包括：

判断所述密文表格的总行数是否满足预设乱序条件，其中，所述预设乱序条件包括：总行数等于预设数值的整数次幂；

若判断不满足所述预设乱序条件，使用特定行填充所述密文表格，得到填充表格，所述填充表格的总行数满足所述预设乱序条件；

以行为单位对所述填充表格进行乱序，以得到乱序表格。

16、根据权利要求 15 所述的方法，所述得到目标排序表格，包括：

对所述乱序表格中所述目标属性项对应的属性值密文进行排序，得到排序后表格；

将排序后表格中所填充的特定行移除，得到所述目标排序表格。

17、一种保护数据隐私的多方数据查询装置，所述多方包括多个数据拥有方，其

各自持有 N 个目标对象的若干属性项的属性值，所述装置部署在所述多方之外的中间方，所述装置包括：

获得模块，配置为获得各数据拥有方发送的 N 个目标对象的属性值密文，以得到密文表格，其中，所述密文表格中一行对应于一个目标对象，一列对应于一个属性项；

乱序模块，配置为以行为单位对所述密文表格进行乱序，得到乱序表格；

排序模块，配置为响应于针对目标属性项查询排序相关数据的查询指令，对所述乱序表格中所述目标属性项对应的属性值密文进行排序，得到目标排序表格；

查询模块，配置为基于所述目标排序表格，得到所述排序相关数据作为查询结果。

18、一种计算设备，包括存储器和处理器，其中，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-16 中任一项所述的方法。