(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113515778 B
(45)授权公告日 2022.12.16

(21)申请号 202110769349.1

(22)申请日 2021.07.07

(65)同一申请的已公布的文献号
申请公布号 CN 113515778 A

(43)申请公布日 2021.10.19

(73)专利权人 建信金融科技有限责任公司
地址 200120 上海市自由贸易试验区银城路99号12层、15层

(72)发明人 李武璐 刘春伟 霍昱光 权纯 王雪

(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 贾磊 李辉

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)
G06K 9/62(2022.01)

审查员 马兴婕

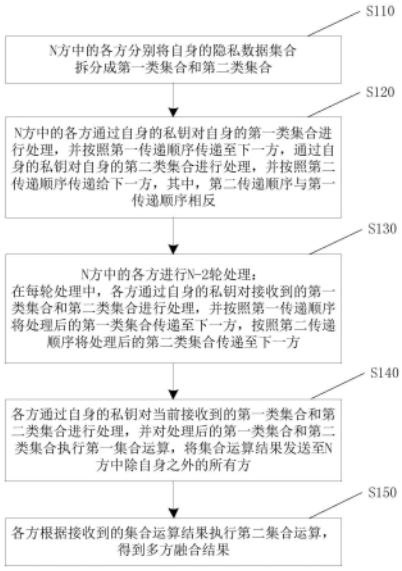
权利要求书3页 说明书14页 附图7页

(54)发明名称

多方隐私数据融合方法、装置及电子设备

(57)摘要

本说明书公开了多方隐私数据融合方法、装置及电子设备，涉及数据安全技术领域，其中，各方将隐私数据集合随机拆分为两类集合，先采用自身私钥对自身的两类集合进行处理，然后将处理后的第一类集合正序传递给下一方，将第二类集合逆序传递给下一方；各方还进行N-2轮数据交互，在每轮交互中，各方通过自身私钥对接收到的两类集合进行处理，再将第一类集合正序传递给下一方，将第二类集合逆序传递给下一方；各方再通过自身私钥对接收到的两类集合进行处理，进而对处理后的这两类集合执行集合运算，将运算结果发送给其余各方；各方根据接收到的集合运算结果执行再执行集合运算，得到多方融合结果。本方案中各方无法获取任意两方的交集或并集信息。



CN 113515778 B

1.一种多方隐私数据融合方法,其特征在于,隐私数据融合的参与方个数为N,N为大于等于3的整数,所述方法包括:

N方中的各方分别将自身的隐私数据集合中的原始数据随机打乱,并拆分成第一类集合和第二类集合;

所述N方中的各方通过自身的私钥对自身的第一类集合进行处理,并按照第一传递顺序传递至下一方,通过自身的私钥对自身的第二类集合进行处理,并按照第二传递顺序传递给下一方,其中,所述第二传递顺序与第一传递顺序相反;

所述N方中的各方进行N-2轮数据交互:在每轮处理中,各方通过自身的私钥对接收到的第一类集合和第二类集合进行处理,并按照第一传递顺序将处理后的第一类集合传递至下一方,按照第二传递顺序将处理后的第二类集合传递至下一方;

各方通过自身的私钥对当前接收到的第一类集合和第二类集合进行处理,并对处理后的第一类集合和第二类集合执行第一集合运算,将集合运算结果发送至所述N方中除自身之外的所有方;所述第一集合运算为取并集运算;

各方根据接收到的集合运算结果执行第二集合运算,得到多方融合结果;所述第二集合运算为取并集运算。

2.根据权利要求1所述的方法,其特征在于,在所述各方根据接收到的集合运算结果执行第二集合运算,得到多方融合结果之后,还包括:

各方识别自身执行第一集合运算时的第一类集合和第二类集合中的元素在所述多方融合结果中对应的位置,并将第一类集合中元素的位置识别结果按照所述第一传递顺序传递至下一方,将第二类集合中元素的位置识别结果按照所述第二传递顺序传递至下一方;

各方根据接收到的第一类集合和第二类集合中元素的位置识别结果,标记自身的隐私数据集合在所述多方融合结果中对应的位置。

3.根据权利要求1所述的方法,其特征在于,所述N方中的各方分别将自身的隐私数据集合拆分成第一类集合和第二类集合之前,还包括:

各方获取自身的目标数据集合;

各方对所述目标数据集合中的数据,进行乱序处理;

各方将乱序处理后的目标数据集合转换为隐私数据集合。

4.根据权利要求3所述的方法,其特征在于,所述各方将乱序处理后的目标数据集合转换为隐私数据集合,包括:

所述N方商定椭圆曲线和随机点生成函数;

各方采用所述椭圆曲线和所述随机点生成函数将自身的原始数据集合转换为隐私数据集合。

5.根据权利要求3所述的方法,其特征在于,所述各方将乱序处理后的目标数据集合转换为隐私数据集合,包括:

所述N方共同确定共享密钥;

各方通过所述共享密钥,将所述目标数据集合转换为隐私数据集合。

6.一种多方隐私数据融合方法,其特征在于,包括:

将自身的隐私数据集合中的原始数据随机打乱,并拆分成第一类集合和第二类集合;

通过自身的私钥对自身的第一类集合进行处理,并按照第一传递顺序传递至下一方,

通过自身的私钥对自身的第二类集合进行处理，并按照第二传递顺序传递至下一方，其中，所述第二传递顺序与第一传递顺序相反；

进行N-2轮数据交互：在每轮处理中，各方通过自身的私钥对接收到的第一类集合和第二类集合进行处理，并按照第一传递顺序将处理后的第一类集合传递至下一方，按照第二传递顺序将处理后的第二类集合传递至下一方；隐私数据融合的参与方个数为N，N为大于等于3的整数；

通过自身的私钥对当前接收到的第一类集合和第二类集合进行处理，并对处理后的第一类集合和第二类集合执行第一集合运算，将集合运算结果发送至所述N方中除自身之外的所有方；所述第一集合运算为取并集运算；

根据接收到的集合运算结果执行第二集合运算，得到多方融合结果；所述第二集合运算为取并集运算。

7.根据权利要求6所述的方法，其特征在于，在根据接收到的集合运算结果执行第二集合运算，得到多方融合结果之后，还包括：

识别自身执行第一集合运算时的第一类集合和第二类集合中的元素在所述多方融合结果中对应的位置，并将第一类集合中元素的位置识别结果按照所述第一传递顺序传递至下一方，将第二类集合中元素的位置识别结果按照所述第二传递顺序传递至下一方；

根据接收到的第一类集合和第二类集合中元素的位置识别结果，标记自身的隐私数据集合在所述多方融合结果中对应的位置。

8.根据权利要求6所述的方法，其特征在于，所述将自身的隐私数据集合拆分成第一类集合和第二类集合之前，还包括：

获取目标数据集合；

对所述目标数据集合中的数据，进行乱序处理；

将乱序处理后的目标数据集合转换为隐私数据集合。

9.根据权利要求8所述的方法，其特征在于，所述将乱序处理后的目标数据集合转换为隐私数据集合，包括：

与所述N方中的其余各方商定椭圆曲线和随机点生成函数；

采用所述椭圆曲线和所述随机点生成函数将原始数据集合转换为隐私数据集合。

10.根据权利要求8所述的方法，其特征在于，所述将乱序处理后的目标数据集合转换为隐私数据集合，包括：

获取共享密钥，其中，所述共享密钥由进行隐私数据融合的N参与方共同确定；

通过所述共享密钥，将所述目标数据集合转换为隐私数据集合。

11.一种多方隐私数据融合装置，其特征在于，包括：

拆分单元，用于将自身的隐私数据集合中的原始数据随机打乱，并拆分成第一类集合和第二类集合；

第一交互单元，用于通过自身的私钥对自身的第一类集合进行处理，并按照第一传递顺序传递至下一方，通过自身的私钥对自身的第二类集合进行处理，并按照第二传递顺序传递给下一方，其中，所述第二传递顺序与第一传递顺序相反；

第二交互单元，用于进行N-2轮数据交互：在每轮处理中，各方通过自身的私钥对接收到的第一类集合和第二类集合进行处理，并按照第一传递顺序将处理后的第一类集合传递

至下一方，按照第二传递顺序将处理后的第二类集合传递至下一方；隐私数据融合的参与方个数为N，N为大于等于3的整数；

第三交互单元，用于通过自身的私钥对当前接收到的第一类集合和第二类集合进行处理，并对处理后的第一类集合和第二类集合执行第一集合运算，将集合运算结果发送至所述N方中除自身之外的所有方；所述第一集合运算为取并集运算；

融合单元，用于根据接收到的集合运算结果执行第二集合运算，得到多方融合结果；所述第二集合运算为取并集运算。

12.根据权利要求11所述的装置，其特征在于，还包括：

识别单元，用于识别自身执行第一集合运算时的第一类集合和第二类集合中的元素在所述多方融合结果中对应的位置，并将第一类集合中元素的位置识别结果按照所述第一传递顺序传递至下一方，将第二类集合中元素的位置识别结果按照所述第二传递顺序传递至下一方；

标记单元，用于根据接收到的第一类集合和第二类集合中元素的位置识别结果，标记自身的隐私数据集合在所述多方融合结果中对应的位置。

13.根据权利要求11所述的装置，其特征在于，还包括：

第一获取单元，用于获取目标数据集合；

乱序单元，用于对所述目标数据集合中的数据，进行乱序处理；

转换单元，用于将乱序处理后的目标数据集合转换为隐私数据集合。

14.根据权利要求13所述的装置，其特征在于，所述转换单元包括：

商定单元，用于与所述N方中的其余各方商定椭圆曲线和随机点生成函数；

第一转换子单元，用于采用所述椭圆曲线和所述随机点生成函数将原始数据集合转换为隐私数据集合。

15.根据权利要求13所述的装置，其特征在于，所述转换单元包括：

第二获取子单元，用于获取共享密钥，其中，所述共享密钥由进行隐私数据融合的N参与方共同确定；

第二转换子单元，还用于通过所述共享密钥，将所述目标数据集合转换为隐私数据集合。

16.一种电子设备，其特征在于，包括：

通信模块、存储器和处理器，所述通信模块、所述处理器和所述存储器之间互相通信连接，所述存储器中存储有计算机指令，所述处理器通过执行所述计算机指令，从而实现权利要求6至10任一项所述方法的步骤。

17.一种计算机存储介质，其特征在于，所述计算机存储介质存储有计算机程序指令，所述计算机程序指令被执行时实现权利要求6至10任一项所述方法的步骤。

多方隐私数据融合方法、装置及电子设备

技术领域

[0001] 本申请涉及数据安全技术领域，特别涉及多方隐私数据融合方法、装置及电子设备。

背景技术

[0002] 数据规模和能力是商业机构的主要竞争力之一。各家机构都在扩充自身的数据量，以提升数据覆盖度和全面性的应用需求。目前机构向其他机构共享用户信息(ID、手机号、设备号等)时，需要征得相应用户的授权作为必要条件。在实际场景中，用户授权过程会带来时效性和用户体验等负面影响，并且造成潜在的合规性风险(例如：授权条款存在不严谨或者误导性，容易受到用户投诉或负面评价)。因此，需要在技术层面探索真正保护各方隐私(需求方隐私+提供方隐私)的数据共享与融合方案，在最大程度上保护各方的隐私与利益，同时避免业务的合规性出现隐患。

[0003] 然而现有技术在解决多方数据隐私融合的同时，会造成交集规模和并集规模等额外信息的泄露，例如A、B、C分别为甲、乙、丙三方的隐私数据集合，甲方能够获取|B∪C|和|B∩C|的元素数量信息，相当于乙丙双方的隐私数据集合(交集、并集)的元素数量信息公开给了其他机构，对于乙、丙双方而言形成了隐私泄露，虽然不涉及原始数据的安全性，但是仍存在一定的风险。

发明内容

[0004] 本申请实施方式的目的是提供多方隐私数据融合方法、装置及电子设备，以解决多方的交集或并集信息容易泄露的问题。

[0005] 为解决上述技术问题，本说明书实施方式提供一种多方隐私数据融合方法包括：N方中的各方分别将自身的隐私数据集合拆分成第一类集合和第二类集合；所述N方中的各方通过自身的私钥对自身的第一类集合进行处理，并按照第一传递顺序传递至下一方，通过自身的私钥对自身的第二类集合进行处理，并按照第二传递顺序传递给下一方，其中，所述第二传递顺序与第一传递顺序相反；所述N方中的各方进行N-2轮数据交互：在每轮处理中，各方通过自身的私钥对接收到的第一类集合和第二类集合进行处理，并按照第一传递顺序将处理后的第一类集合传递至下一方，按照第二传递顺序将处理后的第二类集合传递至下一方；各方通过自身的私钥对当前接收到的第一类集合和第二类集合进行处理，并对处理后的第一类集合和第二类集合执行第一集合运算，将集合运算结果发送至所述N方中除自身之外的所有方；各方根据接收到的集合运算结果执行第二集合运算，得到多方融合结果。

[0006] 本说明书实施例所提供的多方隐私数据融合方法，各方将自身的隐私数据集合随机拆分为两类集合，各方先采用自身的私钥对自身的两类集合进行处理，然后将处理后的第一类集合按照正序传递给下一方，将第二类集合逆序传递给下一方；各方还进行N-2轮数据交互，在每轮交互中，各方通过自身的私钥对接收到的两类集合进行处理，再将第一类集

合按照正序传递给下一方，将第二类集合按照逆序传递给下一方；各方将再通过自身的私钥对接收到的两类集合进行处理，进而对处理后的这两类集合执行集合运算，将运算结果发送给其余各方；各方根据接收到的集合运算结果执行再执行集合运算，得到多方融合结果。本方案过程中，各方无法获取任意两方的交集或并集信息，从而提高了隐私数据融合的安全性。

附图说明

[0007] 为了更清楚地说明本申请实施方式或现有技术中的技术方案，下面将对实施方式或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施方式，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0008] 图1示出了根据本说明书实施例的一种多方隐私数据融合方法的流程图；

[0009] 图2A示出了三方所形成的逻辑闭合环形示意图；

[0010] 图2B示出了四方所形成的逻辑闭合环形示意图；

[0011] 图3示出了根据本说明书实施例的另一种多方隐私数据融合方法的流程图；

[0012] 图4示出了根据本说明书实施例的一种多方隐私数据融合方法的流程图；

[0013] 图5A示出了根据本说明书实施例的一种多方隐私数据融合装置的原理框图；

[0014] 图5B示出了根据本说明书实施例的另一种多方隐私数据融合装置的原理框图；

[0015] 图6示出了根据本说明书实施例的一种电子设备的原理框图。

具体实施方式

[0016] 为了使本技术领域的人员更好地理解本申请中的技术方案，下面将结合本申请实施方式中的附图，对本申请实施方式中的技术方案进行清楚、完整地描述，显然，所描述的实施方式仅仅是本申请一部分实施方式，而不是全部的实施方式。基于本申请中的实施方式，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施方式，都应当属于本申请保护的范围。

[0017] 本说明书实施例提供了多方隐私数据融合方法。下面先以甲、乙、丙三方为例，对多方隐私数据融合方法做具体介绍。

[0018] 首先，在开始融合之前，对甲乙丙三方的数据做预处理。具体可以为以下步骤(1)-(5)。

[0019] (1)甲乙丙三方通过协商确定椭圆曲线$(\mathbb{G},q)$和随机点生成函数$H_p(\bullet)$，并确定一个椭圆曲线生成元$g \in \mathbb{G}$。在本说明书中，椭圆曲线的倍点运算以幂运算的形式表示，当然也可以以其他形式表示。

[0020] (2)甲乙丙三方各自生成自身的私钥$sk_1, sk_2, sk_3 \in \mathbb{Z}_q^*$，其中$sk_1$是甲方的私钥，$sk_2$是乙方的私钥，$sk_3$是丙方的私钥，各方各自计算自身的公钥$pk_1 = g^{sk_1}, pk_2 = g^{sk_2}, pk_3 = g^{sk_3}$并公开；

[0021] (3)甲乙丙三方从自身的数据库中提取待融合隐私数据的原始数据，并随机打乱顺序分别得到集合$A=\{a_1,\cdots,a_l\}$、$B=\{b_1,\cdots,b_m\}$以及$C=\{c_1,\cdots,c_n\}$。

[0022] (4)甲乙丙三方根据三方的密钥协商机制,计算本次隐私数据融合任务的共享密钥K,$K = g^{sk_1 \cdot sk_2 \cdot sk_3}$。

[0023] (5)甲方对集合A进行随机化拆分,得到两个拆分集合$\overline{\mathrm{A}} = \{a_{i_1}, \cdots, a_{i_{l_1}}\}$以及$\overline{\mathrm{A}}^* = \{a^*_{i_1}, \cdots, a^*_{i_{l_2}}\}$,满足$\overline{\mathrm{A}} \cup \overline{\mathrm{A}}^* = \mathrm{A}$且$l_1 + l_2 = l$,然后计算得到自身的隐私数据集合$\overline{\overline{\mathrm{A}}} = \left\{H_p(a_{i_1}, K), \cdots, H_p\left(a_{i_{l_1}}, K\right)\right\} = \{\bar{a}_1, \cdots, \bar{a}_{l_1}\}$以及$\overline{\overline{\mathrm{A}}}^* = \left\{H_p(a^*_{i_1}, K), \cdots, H_p\left(a^*_{i_{l_2}}, K\right)\right\} = \{\bar{a}^*_1, \cdots, \bar{a}^*_{l_2}\}$。

[0024] 乙方对集合B进行随机化拆分,得到两个拆分集合$\overline{\mathrm{B}} = \{b_{j_1}, \cdots, b_{j_{m_1}}\}$以及$\overline{\mathrm{B}}^* = \{b^*_{j_1}, \cdots, b^*_{j_{m_2}}\}$,满足$\overline{\mathrm{B}} \cup \overline{\mathrm{B}}^* = \mathrm{B}$且$m_1 + m_2 = m$,然后计算得到自身的隐私数据集合$\overline{\overline{\mathrm{B}}} = \{H_p(b_{j_1}, K), \cdots, H_p(b_{j_{m_1}}, K)\} = \{\bar{b}_1, \cdots, \bar{b}_{m_1}\}$以及$\overline{\overline{\mathrm{B}}}^* = \{H_p(b^*_{j_1}, K), \cdots, H_p(b^*_{j_{m_2}}, K)\} = \{\bar{b}^*_1, \cdots, \bar{b}^*_{m_2}\}$。

[0025] 丙方对集合C进行随机化拆分,得到两个拆分集合$\overline{\mathrm{C}} = \{c_{k_1}, \cdots, c_{k_{n_1}}\}$以及$\overline{\mathrm{C}}^* = \{c^*_{k_1}, \cdots, c^*_{k_{n_2}}\}$,满足$\overline{\mathrm{C}} \cup \overline{\mathrm{C}}^* = \mathrm{C}$且$n_1 + n_2 = n$,然后计算得到自身的隐私数据集合$\overline{\overline{\mathrm{C}}} = \{H_p(c_{k_1}, K), \cdots, H_p(c_{k_{n_1}}, K)\} = \{\bar{c}_1, \cdots, \bar{c}_{n_1}\}$以及$\overline{\overline{\mathrm{C}}}^* = \{H_p(c^*_{k_1}, K), \cdots, H_p(c^*_{k_{n_2}}, K)\} = \{\bar{c}^*_1, \cdots, \bar{c}^*_{n_2}\}$。

[0026] 在数据预处理结束后,各方分别将自身数据库中待融合的原始数据转化为了隐私数据,接下来可以开始数据融合的过程。

[0027] 对于三方数据融合而言,该数据融合的过程包括四轮数据交互和一次集合运算的过程。具体如下。

[0028] 在第一轮交互时,各方均不改变集合内的元素顺序,甲乙丙三方将各自的两个隐私数据集合使用正向与反向双循环的方式分别发送给其它两方。具体步骤如下。

[0029] (1)对于$i = 1, \cdots, l_1$,甲方计算$a'_i = \bar{a}_i^{sk_1}$,得到甲方的隐私数据集合$\mathrm{A}_1 = \{a'_1, \cdots, a'_{l_1}\}$,然后将隐私数据集合$\mathrm{A}_1$发送给乙方;对于$i = 1, \cdots, l_2$,甲方计算$a^{*\prime}_i = (\bar{a}^*_i)^{sk_1}$,得到甲方的隐私数据集合$\mathrm{A}^*_1 = \{a^{*\prime}_1, \cdots, a^{*\prime}_{l_2}\}$,然后将隐私数据集合$\mathrm{A}^*_1$发送给丙方。

[0030] (2)对于$j = 1, \cdots, m_1$,乙方计算$b'_j = \bar{b}_j^{sk_2}$,得到乙方的隐私数据集合$\mathrm{B}_1 = \{b'_1, \cdots, b'_{m_1}\}$,然后将隐私数据集合$\mathrm{B}_1$发送给丙方;对于$j = 1, \cdots, m_1$,乙方计算$b^{*\prime}_j = (\bar{b}^*_j)^{sk_2}$,得到乙方的隐私数据集合$\mathrm{B}^*_1 = \{b^{*\prime}_1, \cdots, b^{*\prime}_{m_2}\}$,然后将隐私数据集合$\mathrm{B}^*_1$发送给甲方。

[0031] (3)对于$k = 1, \cdots, n_1$,丙方计算$c'_k = \bar{c}_k^{sk_3}$,得到丙方的隐私数据集合$\mathrm{C}_1 = \{c'_1, \cdots, c'_{n_1}\}$,然后将隐私数据集合$\mathrm{C}_1$发送给甲方;对于$k = 1, \cdots, n_2$,丙方计算$c^{*\prime}_k = (\bar{c}^*_k)^{sk_3}$,得到丙方的隐私数据集合$\mathrm{C}^*_1 = \{c^{*\prime}_1, \cdots, c^{*\prime}_{n_2}\}$,然后将隐私数据集合$\mathrm{C}^*_1$发送给乙方。

[0032] 在第二轮交互时,各方均不改变集合内的元素顺序,甲乙丙三方将各自的两个隐私数据集合使用正向与反向双循环的方式分别发送给其它两方。具体步骤如下。

[0033] (1)甲方对于上一轮收到的隐私数据集合$\mathrm{B}^*_1 = \{b^{*\prime}_1, \cdots, b^{*\prime}_{m_2}\}$以及$\mathrm{C}_1 = \{c'_1, \cdots, c'_{n_1}\}$($\mathrm{B}^*_1$来自乙方,$\mathrm{C}_1$来自丙方),对两个集合中的全部元素计算$b^{*\prime\prime}_j = (b^{*\prime}_j)^{sk_1}$以及$c''_k = (c'_k)^{sk_1}$,分别

得到两个新隐私数据集合$B_2^* = \{b_1^{*''}, \cdots, b_{m_2}^{*''}\}$以及$C_2 = \{c_1'', \cdots, c_{n_1}''\}$，然后将隐私数据集合$B_2^*$发送给丙方，并将$C_2$发送给乙方。

[0034] (2)乙方对于上一轮收到的隐私数据集合$A_1 = \{a_1', \cdots, a_{l_1}'\}$以及$C_1^* = \{c_1^{*'}, \cdots, c_{n_2}^{*'}\}$（$C_1^*$来自丙方，$A_1$来自甲方），对两个集合中的全部元素计算$a_i'' = (a_i')^{sk_2}$以及$c_k^{*''} = (c_k^{*'})^{sk_2}$，分别得到两个新隐私数据集合$A_2 = \{a_1'', \cdots, a_{l_1}''\}$以及$C_2^* = \{c_1^{*''}, \cdots, c_{n_2}^{*''}\}$，然后将隐私数据集合$A_2$发送给丙方，并将隐私数据集合$C_2^*$发送给甲方。

[0035] (3)丙方对于上一轮收到的隐私数据集合$A_1^* = \{a_1^{*'}, \cdots, a_{l_2}^{*'}\}$以及$B_1 = \{b_1', \cdots, b_{m_1}'\}$（$A_1^*$来自甲方，$B_1$来自乙方），对两个集合中的全部元素计算$a_i^{*''} = (a_i^{*'})^{sk_3}$以及$b_j'' = (b_j')^{sk_3}$，分别得到两个新隐私数据集合$A_2^* = \{a_1^{*''}, \cdots, a_{l_2}^{*''}\}$以及$B_2 = \{b_1'', \cdots, b_{m_1}''\}$，然后将隐私数据集合$A_2^*$发送给乙方，并将隐私数据集合$B_2$发送给甲方。

[0036] 在第三轮交互时，各方均不改变集合内的元素顺序，执行以下步骤。

[0037] (1)甲方对于上一轮收到的隐私数据集合$B_2 = \{b_1'', \cdots, b_{m_1}''\}$以及$C_2^* = \{c_1^{*''}, \cdots, c_{n_2}^{*''}\}$（$B_2$来自丙方，$C_2^*$来自乙方），对两个集合中的全部元素计算$b_j''' = (b_j'')^{sk_1}$以及$c_k^{*'''} = (c_k^{*''})^{sk_1}$，分别得到两个新隐私数据集合$B_3 = \{b_1''', \cdots, b_{m_1}'''\}$以及$C_3^* = \{c_1^{*'''}, \cdots, c_{n_2}^{*'''}\}$，计算二者的并集并打乱元素顺序，得到$X_A = B_3 \cup C_3^*$，并将$X_A$分别发送给乙方和丙方；

[0038] (2)乙方对于上一轮收到的隐私数据集合$A_2^* = \{a_1^{*''}, \cdots, a_{l_2}^{*''}\}$以及$C_2 = \{c_1'', \cdots, c_{n_1}''\}$（$A_2^*$来自丙方，$C_2$来自甲方），对两个集合中的全部元素计算$a_i^{*'''} = (a_i^{*''})^{sk_2}$以及$c_k''' = (c_k'')^{sk_2}$，分别得到两个新隐私数据集合$A_3^* = \{a_1^{*'''}, \cdots, a_{l_2}^{*'''}\}$以及$C_3 = \{c_1''', \cdots, c_{n_1}'''\}$，计算二者的并集并打乱元素顺序，得到$X_B = A_3^* \cup C_3$，并将$X_B$分别发送给甲方和丙方；

[0039] (3)丙方对于上一轮收到的隐私数据集合$A_2 = \{a_1'', \cdots, a_{l_1}''\}$以及$B_2^* = \{b_1^{*''}, \cdots, b_{m_2}^{*''}\}$（$A_2$来自乙方，$B_2^*$来自甲方），对两个集合中的全部元素计算$a_i''' = (a_i'')^{sk_3}$以及$b_j^{*'''} = (b_j^{*''})^{sk_3}$，分别得到两个新隐私数据集合$A_3 = \{a_1''', \cdots, a_{l_1}'''\}$以及$B_3^* = \{b_1^{*'''}, \cdots, b_{m_2}^{*'''}\}$，计算二者的并集并打乱元素顺序，得到$X_C = A_3 \cup B_3^*$，并将$X_C$分别发送给甲方和乙方。

[0040] 经过上述三轮数据交互后，执行一次集合运算。具体可以包括以下两个步骤：

[0041] (1)对于甲乙丙三方而言，在上一轮通信中分享了X_A，X_B，X_C，各方计算并集$X_{ABC} = X_A \cup X_B \cup X_C$。并集$X_{ABC}$中的元素顺序，需要遵循事先约定好的排序规则，以确保各方获取集合相同并且元素顺序相同。

[0042] (2)记录并集X_{ABC}的集合规模，$|X_{ABC}| = \alpha_{ABC}$.

[0043] 然后执行第四轮数据交互，以确保各方知道自身的元素在并集中的什么位置。第四轮数据交互可以包括以下步骤。

[0044] (1)甲方根据隐私数据集合$B_3 = \{b_1''', \cdots, b_{m_1}'''\}$以及$C_3^* = \{c_1^{*'''}, \cdots, c_{n_2}^{*'''}\}$，对于每个集合，分别按顺序对每一个元素，在并集$X_{ABC}$中寻找其位置信息，即计算$\{j_1, \cdots, j_{m_1}\}$和$\{k_1^*, \cdots, k_{n_2}^*\}$，分别对应$\{b_1''', \cdots, b_{m_1}'''\}$以及$\{c_1^{*'''}, \cdots, c_{n_2}^{*'''}\}$在$X_{ABC}$的位置信息，然后将$\{j_1, \cdots, j_{m_1}\}$发送给乙方，将

$\{k_1^*,\cdots,k_{n_2}^*\}$发送给丙方。

[0045] (2)乙方根据隐私数据集合$A_3^*=\{a_1^{*'''},\cdots,a_{l_2}^{*'''}\}$以及$C_3=\{c_1^{'''},\cdots,c_{n_1}^{'''}\}$，对于每个集合，分别按顺序对每一个元素，在并集$X_{ABC}$中寻找其位置信息，即计算$\{i_1^*,\cdots,i_{l_2}^*\}$和$\{k_1,\cdots,k_{n_1}\}$，分别对应$\{a_1^{*'''},\cdots,a_{l_2}^{*'''}\}$以及$\{c_1^{'''},\cdots,c_{n_1}^{'''}\}$在$X_{ABC}$的位置信息，然后将$\{i_1^*,\cdots,i_{l_2}^*\}$发送给甲方，将$\{k_1,\cdots,k_{n_1}\}$发送给丙方。

[0046] (3)丙方根据隐私数据集合$A_3=\{a_1^{'''},\cdots,a_{l_1}^{'''}\}$以及$B_3^*=\{b_1^{*'''},\cdots,b_{m_2}^{*'''}\}$，对于每个集合，分别按顺序对每一个元素，在并集$X_{ABC}$中寻找其位置信息，即计算$\{i_1,\cdots,i_{l_1}\}$和$\{j_1^*,\cdots,j_{m_2}^*\}$，分别对应$\{a_1^{'''},\cdots,a_{l_1}^{'''}\}$以及$\{b_1^{*'''},\cdots,b_{m_2}^{*'''}\}$在$X_{ABC}$的位置信息，然后将$\{i_1,\cdots,i_{l_1}\}$发送给甲方，将$\{j_1^*,\cdots,j_{m_2}^*\}$发送给乙方。

[0047] (4)各方根据自身数据预处理中的拆分与随机乱序操作，集合本轮收到的位置信息，反推出自身元素在多方并集中的位置，并进行标记，完成多方数据融合。

[0048] 下表一示意了上述三方隐私数据融合的过程，其中，甲的隐私数据集合为A，乙的隐私数据集合为B。各方的隐私数据集合拆分为2个集合。A_1表示有一方采用自身的私钥对集合A中的数据进行了处理，C_2*表示有两方采用自身的私钥对集合C*中的数据进行了处理，以此类推，理解表格中其他同样格式的符号所表示的内容。

[0049] 表一

[0050]

三方的代号		甲		乙		丙	
拆分出的隐私数据集合		A	A*	B	B*	C	C*
第一轮	计算得到	A_1	A_1*	B_1	B_1*	C_1	C_1*
	传递后	C_1	B_1*	A_1	C_1*	B_1	A_1*
第二轮	计算得到	C_2	B_2*	A_2	C_2*	B_2	A_2*
	传递后	B_2	C_2*	C_2	A_2*	A_2	B_2*
第三轮	计算得到	B_3	C_3*	C_3	A_3*	A_3	B_3*
	计算交集或并集	B_3C_3*		A_3* C_3		A_3B_3*	
	传递后得到集合	A_3B_3*，A_3* C_3		B_3C_3*，A_3B_3*		A_3* C_3，B_3C_3*	
计算交集或并集		A_3A_3*B_3B_3* $B_3C_3C_3$*（融合结果）					
第四轮		识别出首次计算交集或并集时的集合中元素在融合结果中对应的位置，并发给其余各方					
各方找出自身的隐私数据集合中的元素在融合结果中对应的位置							

[0051] 下表二示出了另一种三方隐私数据融合的过程，其中，甲的隐私数据集合为A，乙的隐私数据集合为B，丙的隐私数据集合为C。各方的隐私数据集合拆分为3个集合。A1$^{(1)}$表示有一方采用自身的私钥对集合A1中的数据进行了处理，C3$^{(3)}$表示有三方采用自身的私钥对集合C3中的数据进行了处理，以此类推，理解表格中其他同样格式的符号所表示的内容。

[0052] 表二

[0053]

		甲			乙			丙		
拆分出的集合		A1	A2	A3	B1	B2	B3	C1	C2	C3
第一轮	计算得到	$A1^{(1)}$	$A2^{(1)}$	$A3^{(1)}$	$B1^{(1)}$	$B2^{(1)}$	$B3^{(1)}$	$C1^{(1)}$	$C2^{(1)}$	$C3^{(1)}$
	传递后	$C1^{(1)}$	$B2^{(1)}$	$C3^{(1)}$	$A1^{(1)}$	$C2^{(1)}$	$A3^{(1)}$	$B1^{(1)}$	$A2^{(1)}$	$B3^{(1)}$
第二轮	计算得到	$C1^{(2)}$	$B2^{(2)}$	$C3^{(2)}$	$A1^{(2)}$	$C2^{(2)}$	$A3^{(2)}$	$B1^{(2)}$	$A2^{(2)}$	$B3^{(2)}$
	传递后	$B1^{(2)}$	$C2^{(2)}$	$B3^{(2)}$	$C1^{(2)}$	$A2^{(2)}$	$C3^{(2)}$	$A1^{(2)}$	$B2^{(2)}$	$A3^{(2)}$
第三轮	计算得到	$B1^{(3)}$	$C2^{(3)}$	$B3^{(3)}$	$C1^{(3)}$	$A2^{(3)}$	$C3^{(3)}$	$A1^{(3)}$	$B2^{(3)}$	$A3^{(3)}$
	计算交集或并集	$B1^{(3)}$ $B3^{(3)}C2^{(3)}$			$A2^{(3)}$ $C1^{(3)}$ $C3^{(3)}$			$A1^{(3)}$ $A3^{(3)}B2^{(3)}$		
	传递后得到集合	$A2^{(3)}$ $C1^{(3)}$ $C3^{(3)}$ $A1^{(3)}$ $A3^{(3)}$ $B2^{(3)}$			$B1^{(3)}$ $B3^{(3)}$ $C2^{(3)}$ $A1^{(3)}$ $A3^{(3)}B2^{(3)}$			$B1^{(3)}$ $B3^{(3)}$ $C2^{(3)}$ $A2^{(3)}$ $C1^{(3)}$ $C3^{(3)}$		

[0054]

计算交集或并集	$A1^{(3)}A2^{(3)}$ $A3^{(3)}$ $B1^{(3)}B2^{(3)}$ $B3^{(3)}C1^{(3)}$ $C2^{(3)}C3^{(3)}$ （融合结果）
第四轮	识别出首次计算交集或并集时的集合中元素在融合结果中对应的位置，并发给其余各方
各方找出自身的隐私数据集合中的元素在融合结果中对应的位置	

[0055] 下表三示出了四方隐私数据融合的过程，其中，甲的隐私数据集合为A，乙的隐私数据集合为B，丙的隐私数据集合为C，丁的隐私数据集合为D。各方的隐私数据集合拆分为2个集合。$A1^{(1)}$表示有一方采用自身的私钥对集合A1中的数据进行了处理，$C3^{(3)}$表示有三方采用自身的私钥对集合C3中的数据进行了处理，以此类推，理解表格中其他同样格式的符号所表示的内容。

[0056] 表三

[0057]

四方的代号		甲		乙		丙		丁	
拆分出的隐私数据集合		A1	A2	B1	B2	C1	C2	D1	D2
第一轮	计算得到	$A1^{(1)}$	$A2^{(1)}$	$B1^{(1)}$	$B2^{(1)}$	$C1^{(1)}$	$C2^{(1)}$	$D1^{(1)}$	$D2^{(1)}$
	传递后	$D1^{(1)}$	$B2^{(1)}$	$A1^{(1)}$	$C2^{(1)}$	$B1^{(1)}$	$D2^{(1)}$	$C1^{(1)}$	$A2^{(1)}$
第二轮	计算得到	$D1^{(2)}$	$B2^{(2)}$	$A1^{(2)}$	$C2^{(2)}$	$B1^{(2)}$	$D2^{(2)}$	$C1^{(2)}$	$A2^{(2)}$
	传递后	$C1^{(2)}$	$C2^{(2)}$	$D1^{(2)}$	$D2^{(2)}$	$A1^{(2)}$	$A2^{(2)}$	$B1^{(2)}$	$B2^{(2)}$
第三轮	计算得到	$C1^{(3)}$	$C2^{(3)}$	$D1^{(3)}$	$D2^{(3)}$	$A1^{(3)}$	$A2^{(3)}$	$B1^{(3)}$	$B2^{(3)}$
	传递后	$B1^{(3)}$	$D2^{(3)}$	$C1^{(3)}$	$A2^{(3)}$	$D1^{(3)}$	$B2^{(3)}$	$A1^{(3)}$	$C2^{(3)}$
第四轮	计算得到	$B1^{(4)}$	$D2^{(4)}$	$C1^{(4)}$	$A2^{(4)}$	$D1^{(4)}$	$B2^{(4)}$	$A1^{(4)}$	$C2^{(4)}$
	计算交集或并集	$B1^{(4)}$ $D2^{(4)}$		$A2^{(4)}$ $C1^{(4)}$		$B2^{(4)}$ $D1^{(4)}$		$A1^{(4)}$ $C2^{(4)}$	
	传递后得到集合	$A2^{(4)}$ $C1^{(4)}$ $B2^{(4)}$ $D1^{(4)}$ $A1^{(4)}$ $C2^{(4)}$		$B1^{(4)}$ $D2^{(4)}$ $B2^{(4)}$ $D1^{(4)}$ $A1^{(4)}$ $C2^{(4)}$		$A2^{(4)}$ $C1^{(4)}$ $A2^{(4)}$ $C1^{(4)}$ $A1^{(4)}$ $C2^{(4)}$		$B2^{(4)}$ $D1^{(4)}$ $A2^{(4)}$ $C1^{(4)}$ $B2^{(4)}$ $D1^{(4)}$	
求交集或并集		$A1^{(4)}$ $A2^{(4)}$ $B1^{(4)}$ $B2^{(4)}$ $C1^{(4)}$ $C2^{(4)}$ $D1^{(4)}$ $D2^{(4)}$ （融合结果）							
第五轮		识别出首次计算交集或并集时的集合中元素在融合结果中对应的位置，并发给其余各方							
各方找出自身的隐私数据集合中的元素在融合结果中对应的位置									

[0058] 上述三方隐私数据融合方法体现了本说明书实施例提供的一种多方隐私数据融合方法的过程。下面介绍本说明书实施例提供的多方隐私数据融合方法。该方法中隐私数据融合的参与方个数为N,N为大于等于3的整数。如图1所示,该方法包括如下步骤。

[0059] S110:N方中的各方分别将自身的隐私数据集合拆分成第一类集合和第二类集合。

[0060] 该步骤对应表一所示意具体实施例中的数据预处理步骤,具体对应其中的随机化拆分步骤。

[0061] 第一类集合为至少一个,第二类集合为至少一个。第一类集合和第二类集合仅用于后续区分数据传输的方向不同,并无其他限定意义。也即,各方将自身的隐私数据集合拆分成M个集合,其中M为大于等于2的整数,并将M个集合中的至少一个集合归为第一类集合,再将M个集合中的其余集合归为第二类集合,且第二类集合包括至少一个集合。

[0062] 各方所拆分出的第一类集合的数量相等,但是第一类集合中每个集合元素的数量可以不同。各方所拆分出的第二类集合的数量相等,但是第二类集合中每个集合元素的数量可以不相同。

[0063] 第一类集合和第二类集合中,任意两个集合的交集可以为空,也可以为不为空,但是第一类集合和第二类集合中所有集合的并集应为隐私数据集合。

[0064] 任意两个或两个以上的集合的交集为空的情形,可以参阅表一所示意的具体实施例。

[0065] 两个集合的交集不为空的情形,例如甲方的隐私数据集合中有a1、a2、a3、a4、a5五个元素,则可以提取数据a1、a2作为集合A1,提取数据a2、a3作为集合A2,提取数据a3、a4、a5作为集合A3,也即从甲的隐私数据集合中提取出3个集合。

[0066] 在一些实施例中，第一类集合和第二类集合中，还可以有两个或两个以上的集合中的元素相同。

[0067] 在一些实施例中，第一类集合和第二类集合中，各类集合的数量可以是预先设置好的。例如，在表一所示意的具体实施例中，各类集合的数量均为1。各类集合的数量可以与隐私数据融合的参与方的数量无关，也可以与各方所提供用于融合的数据量的大小无关。

[0068] 而在一些实施例中，在执行步骤S110之前，多方可以约定第一类集合和第二类集合中各类集合的数量。例如，可以根据数据融合的参与方的个数确定各类集合的数量，或者根据提供用于融合的数据量最多的一方所提供的数据量来确定各类集合的数量，或者也可以根据其他情况确定各类集合的数量，本说明书不再一一列举。

[0069] 本说明书中所述的“隐私数据”可以是各方数据库中存储的不对其他机构公开的原始数据。例如，一方机构的数据库中可能存储以后关于用户的多个字段信息，每一条用户记录都有这些字段的内容，原始数据可以是其中一个字段中多个记录的取值，如多个用户的设备号，或者多个用户的身份证号，或者多个用户的手机号，或者多个用户的工商注册号等。

[0070] 本说明书中所述的“隐私数据”也可以是在这些原始数据的基础上采用加密算法得到的数据，加密后的数据可以对其他机构公开。这里所指的加密算法，可以如表一所示意的具体实施方式那样采用随机点生成函数将原始数据映射为椭圆曲线上的点，也可以采用RSA、DES、MD5等加密算法，本说明书不再一一列举。

[0071] 在一些实施例中，在各方原始数据集合中的数据转换为隐私数据之前，还将各方原始数据集合中数据的顺序随机打乱，以使得即使隐私数据被获取也无法直接获知对应的原始数据，从而进一步提高原始数据的安全性。

[0072] S120：N方中的各方通过自身的私钥对自身的第一类集合进行处理，并按照第一传递顺序传递至下一方，通过自身的私钥对自身的第二类集合进行处理，并按照第二传递顺序传递给下一方，其中，第二传递顺序与第一传递顺序相反。

[0073] 该步骤对应表一所示意具体实施例中的第一轮交互操作。

[0074] S130：N方中的各方进行N-2轮处理：在每轮处理中，各方通过自身的私钥对接收到的第一类集合和第二类集合进行处理，并按照第一传递顺序将处理后的第一类集合传递至下一方，按照第二传递顺序将处理后的第二类集合传递至下一方。

[0075] 该步骤对应表一所示意具体实施例中的第二轮交互操作。

[0076] 在步骤S130“各方通过自身的私钥对接收到的第一类集合和第二类集合进行处理”中，“接收到的第一类集合和第二类集合”应为步骤S120中传递操作之后接收到的第一类集合和第二类集合，或者为上一轮传递操作后接收到的第一类集合和第二类集合。

[0077] 第一传递顺序和第二传递顺序是指集合在N方所形成的逻辑闭合环形上的传递顺序，传递顺序可以为顺时针或者逆时针，第一传递顺序为其中一者，第二传递顺序为其中另一者。

[0078] 例如，当数据融合的参与方为三个时，上述步骤S130执行1轮传递，三方所形成的逻辑闭合环形如图2A所示；当数据融合的参与方为四个时，上述步骤S130执行2轮传递，四方所形成的逻辑闭合环形可以如图2B所示。

[0079] 上述步骤S102中的第一传递方向可以为顺时针方向，第二传递方向可以为逆时针

方向。当然，第一传递方向也可以为逆时针方向，第二传递方向也可以为顺时针方向。

[0080] 在一些实施例中，在步骤S120和S130将集合传递至下一方时，各方均不打乱集合中数据的顺序。

[0081] 步骤S120、S130以及下述S140中“通过自身的私钥”对集合进行处理，即对集合中的数据进行处理。在一些实施例方式中，该处理方式可以是幂运算，其中私钥对应的数字作为幂，集合中的数据对应的数字作为底数。在一些对数据的安全性要求较高的场合，该处理方式还可以为椭圆曲线的倍点运算。无论是幂运算还是椭圆曲线的倍点运算，其都有以下特点：各方私钥对于数据的处理顺序对多轮传递后得到的结果没有影响。

[0082] S140：各方通过自身的私钥对当前接收到的第一类集合和第二类集合进行处理，并对处理后的第一类集合和第二类集合执行第一集合运算，将集合运算结果发送至N方中除自身之外的所有方。

[0083] 该步骤对应表一所示意具体实施例中的第三轮交互操作。

[0084] 在经历了步骤S120、S130和S140之后，每一方均接收到第一类集合和第二类集合。在步骤S130对这些集合进行处理后，第一类集合和第二类集合中的每一个集合都经过了多方私钥的处理。

[0085] S150：各方根据接收到的集合运算结果执行第二集合运算，得到多方融合结果。

[0086] 该步骤对应表一所示意具体实施例中三轮交互操作之后的第一次集合运算。

[0087] 步骤S140中的第一集合运算、步骤S150中的第二集合运算，可以是交集运算，也可以是并集运算，具体根据实际需求而定。

[0088] 步骤S140各方将集合运算结果发送至N方中除自身之外的所有方之后，每一方均接收到来自N-1方的M个集合(第一类集合和第二类集合的数量之和为M)的运算结果，步骤S150再结合自身执行第一集合运算时的第一类集合和第二类集合，每一方均能够知道N×M个集合的运算结果，即得到了多方数据的融合结果。

[0089] 多方数据融合后的集合可以提供给专门的机构，由专门的机构给需要这些数据信息的用户提供数据服务。该专门的机构可以具有权限获得各方的私钥，进而可以从融合后的集合中解析出各方的数据。

[0090] 本说明书实施例所提供的多方隐私数据融合方法，各方将自身的隐私数据集合随机拆分为两类集合，各方先采用自身的私钥对自身的两类集合进行处理，然后将处理后的第一类集合按照正序传递给下一方，将第二类集合逆序传递给下一方；各方还进行N-2轮数据交互，在每轮交互中，各方通过自身的私钥对接收到的两类集合进行处理，再将第一类集合按照正序传递给下一方，将第二类集合按照逆序传递给下一方；各方将再通过自身的私钥对接收到的两类集合进行处理，进而对处理后的这两类集合执行集合运算，将运算结果发送给其余各方；各方根据接收到的集合运算结果执行再执行集合运算，得到多方融合结果。本方案过程中，各方无法获取任意两方的交集或并集信息，从而提高了隐私数据融合的安全性。

[0091] 在一些实施例中，多方数据融合过程除了需要提供融合后的数据集合之外，还需要提供各方的隐私数据在融合后的数据集合中对应的位置。为此，如图3所示，可以执行以下步骤：

[0092] S160：各方识别自身执行第一集合运算时的第一类集合和第二类集合中的元素在

多方融合结果中对应的位置，并将第一类集合中元素的位置识别结果按照第一传递顺序传递至下一方，将第二类集合中元素的位置识别结果按照第二传递顺序传递至下一方。

[0093] 该方法对应表一所示意具体实施例中的第四轮交互操作。

[0094] 例如在表一所示意的具体实施方式中，甲在第三轮时对B_3和C_3*执行集合运算，该步骤S160中的“自身执行第一集合运算时的第一类集合和第二类集合中的元素”即是指集合B_3和C_3*中的元素。

[0095] 该步骤中的“识别”操作仅仅是查看是否相同。例如，集合B_3中有元素b_1''',…,b_{m_1}'''，分别识别这些元素在融合结果中对应的位置。

[0096] S170：各方根据接收到的第一类集合和第二类集合中元素的位置识别结果，标记自身的隐私数据集合在多方融合结果中对应的位置。

[0097] 该步骤对应表一所示意具体实施例中三轮交互操作之后的第一次集合运算。

[0098] 在一些实施例中，在执行步骤S110之前，各方将自身原始数据集合中的数据转换为隐私数据，从而得到隐私数据集合。具体方法可以为：获取目标数据集合，即原始数据集合；对目标数据集合中的数据，进行乱序处理；将乱序处理后的目标数据集合转换为隐私数据集合。可以与N方中的其余各方商定椭圆曲线和随机点生成函数，再采用椭圆曲线和随机点生成函数将原始数据集合转换为隐私数据集合。

[0099] 该具体方法可以参阅表一对应的具体实施例理解，不再赘述。

[0100] 在一些实施例中，为防止同一方的同一数据在每一次数据融合任务时转换得到的隐私数据为同一内容从而使得该数据容易泄露，各方在将自身原始数据集合中的数据转换为隐私数据之前，可以先获取共享密钥，其中，共享密钥由进行隐私数据融合的N参与方共同确定；通过共享密钥，将目标数据集合转换为隐私数据集合。

[0101] 例如，在一些实施例中，共享密钥可以为各方私钥的乘积，或者各方私钥的求和结果，或者也可以是数据融合参与方的个数执行1024次方。共享密钥的商定方式可以多种多样，本说明书对此不做限定。

[0102] 下面从N方中的一方视角为例，介绍本说明书所提供的多方隐私数据融合方法。该方法各步骤的描述及有益效果可以参阅图1所示意的实施例进行理解，下文不再赘述。

[0103] 如图4所示，该方法包括如下步骤。

[0104] S410：将自身的隐私数据集合拆分成第一类集合和第二类集合。

[0105] S420：通过自身的私钥对自身的第一类集合进行处理，并按照第一传递顺序传递至下一方，通过自身的私钥对自身的第二类集合进行处理，并按照第二传递顺序传递至下一方，其中，第二传递顺序与第一传递顺序相反。

[0106] S430：进行N-2轮数据交互：在每轮处理中，各方通过自身的私钥对接收到的第一类集合和第二类集合进行处理，并按照第一传递顺序将处理后的第一类集合传递至下一方，按照第二传递顺序将处理后的第二类集合传递至下一方。

[0107] S440：通过自身的私钥对当前接收到的第一类集合和第二类集合进行处理，并对处理后的第一类集合和第二类集合执行第一集合运算，将集合运算结果发送至N方中除自身之外的所有方。

[0108] S450：根据接收到的集合运算结果执行第二集合运算，得到多方融合结果。

[0109] 在一些实施例中，如图4所示还包括以下步骤。

[0110] S460:识别自身执行第一集合运算时的第一类集合和第二类集合中的元素在多方融合结果中对应的位置,并将第一类集合中元素的位置识别结果按照第一传递顺序传递至下一方,将第二类集合中元素的位置识别结果按照第二传递顺序传递至下一方。

[0111] S470:根据接收到的第一类集合和第二类集合中元素的位置识别结果,标记自身的隐私数据集合在多方融合结果中对应的位置。

[0112] 在一些实施例中,在步骤S410之前,还可以先获取目标数据集合;对目标数据集合中的数据,进行乱序处理;将乱序处理后的目标数据集合转换为隐私数据集合。

[0113] 在一些实施例中,“将乱序处理后的目标数据集合转换为隐私数据集合”可以为:与N方中的其余各方商定椭圆曲线和随机点生成函数;采用椭圆曲线和随机点生成函数将原始数据集合转换为隐私数据集合。

[0114] 在一些实施例中,“将乱序处理后的目标数据集合转换为隐私数据集合”可以为:获取共享密钥,其中,共享密钥由进行隐私数据融合的N参与方共同确定;通过共享密钥,将目标数据集合转换为隐私数据集合。

[0115] 本说明书实施例还提供了一种多方隐私数据融合装置,可以用于实现图4所示的多方隐私数据融合方法。该装置的具体描述及有益效果可以参阅图1所示意的实施例进行理解,下文不再赘述。如图5A所示,该装置包括拆分单元501、第一交互单元502、第二交互单元503、第三交互单元504和融合单元505。

[0116] 拆分单元501用于将自身的隐私数据集合拆分成第一类集合和第二类集合。

[0117] 第一交互单元502用于通过自身的私钥对自身的第一类集合进行处理,并按照第一传递顺序传递至下一方,通过自身的私钥对自身的第二类集合进行处理,并按照第二传递顺序传递至下一方,其中,所述第二传递顺序与第一传递顺序相反。

[0118] 第二交互单元503用于进行N-2轮数据交互:在每轮处理中,各方通过自身的私钥对接收到的第一类集合和第二类集合进行处理,并按照第一传递顺序将处理后的第一类集合传递至下一方,按照第二传递顺序将处理后的第二类集合传递至下一方。

[0119] 第三交互单元504用于通过自身的私钥对当前接收到的第一类集合和第二类集合进行处理,并对处理后的第一类集合和第二类集合执行第一集合运算,将集合运算结果发送至所述N方中除自身之外的所有方。

[0120] 融合单元505用于根据接收到的集合运算结果执行第二集合运算,得到多方融合结果。

[0121] 在一些实施例中,如图5B所示,该多方隐私数据融合装置还包括识别单元506和标记单元507。

[0122] 识别单元506用于识别自身执行第一集合运算时的第一类集合和第二类集合中的元素在所述多方融合结果中对应的位置,并将第一类集合中元素的位置识别结果按照所述第一传递顺序传递至下一方,将第二类集合中元素的位置识别结果按照所述第二传递顺序传递至下一方。

[0123] 标记单元507用于根据接收到的第一类集合和第二类集合中元素的位置识别结果,标记自身的隐私数据集合在所述多方融合结果中对应的位置。

[0124] 在一些实施例中,如图5B所示,该多方隐私数据融合装置还包括第一获取单元508、乱序单元509和转换单元510。

[0125] 第一获取单元508用于获取目标数据集合。乱序单元509用于对所述目标数据集合中的数据，进行乱序处理。转换单元510用于将乱序处理后的目标数据集合转换为隐私数据集合。

[0126] 在一些实施例中，如图5B所示，所述转换单元510包括商定单元511和第一转换子单元512。

[0127] 商定单元511用于与所述N方中的其余各方商定椭圆曲线和随机点生成函数。第一转换子单元512用于采用所述椭圆曲线和所述随机点生成函数将原始数据集合转换为隐私数据集合。

[0128] 在一些实施例中，如图5B所示，所述转换单元510包括第二获取子单元513和第二转换子单元514。

[0129] 第二获取子单元513用于获取共享密钥，其中，所述共享密钥由进行隐私数据融合的N参与方共同确定。第二转换子单元514还用于通过所述共享密钥，将所述目标数据集合转换为隐私数据集合。

[0130] 本发明实施例还提供了一种电子设备，如图6所示，该电子设备可以包括处理器61和存储器62，还包括通信模块63。其中处理器61和存储器62可以通过总线或者其他方式连接，图6中以通过总线连接为例。

[0131] 处理器61可以为中央处理器(Central Processing Unit,CPU)。处理器61还可以为其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等芯片，或者上述各类芯片的组合。

[0132] 存储器62作为一种非暂态计算机可读存储介质，可用于存储非暂态软件程序、非暂态计算机可执行程序以及模块，如本发明实施例中的多方隐私数据融合方法对应的程序指令/模块(例如，图5A所示的拆分单元501、第一交互单元502、第二交互单元503、第三交互单元504和融合单元505)。处理器61通过运行存储在存储器62中的非暂态软件程序、指令以及模块，从而执行处理器的各种功能应用以及数据处理，即实现上述方法实施例中的多方隐私数据融合方法。

[0133] 存储器62可以包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需要的应用程序；存储数据区可存储处理器61所创建的数据等。此外，存储器62可以包括高速随机存取存储器，还可以包括非暂态存储器，例如至少一个磁盘存储器件、闪存器件、或其他非暂态固态存储器件。在一些实施例中，存储器62可选包括相对于处理器61远程设置的存储器，这些远程存储器可以通过网络连接至处理器61。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0134] 所述一个或者多个模块存储在所述存储器62中，当被所述处理器61执行时，执行如图4所示实施例中的多方隐私数据融合方法。

[0135] 上述电子设备具体细节可以对应参阅图4的实施例中对应的相关描述和效果进行理解，此处不再赘述。

[0136] 本领域技术人员可以理解，实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质

中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,所述存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory,ROM)、随机存储记忆体(Random Access Memory,RAM)、快闪存储器(Flash Memory)、硬盘(Hard Disk Drive,缩写:HDD)或固态硬盘(Solid-State Drive,SSD)等;所述存储介质还可以包括上述种类的存储器的组合。

[0137] 在20世纪90年代,对于一个技术的改进可以很明显地区分是硬件上的改进(例如,对二极管、晶体管、开关等电路结构的改进)还是软件上的改进(对于方法流程的改进)。然而,随着技术的发展,当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此,不能说一个方法流程的改进就不能用硬件实体模块来实现。例如,可编程逻辑器件(Programmable Logic Device,PLD)(例如现场可编程门阵列(Field Programmable Gate Array,FPGA))就是这样一种集成电路,其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片PLD上,而不需要请芯片制造厂商来设计和制作专用的集成电路芯片2。而且,如今,取代手工地制作集成电路芯片,这种编程也多半改用“逻辑编译器(logic compiler)”软件来实现,它与程序开发撰写时所用的软件编译器相类似,而要编译之前的原始代码也得用特定的编程语言来撰写,此称之为硬件描述语言(Hardware Description Language,HDL),而HDL也并非仅有一种,而是有许多种,如ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDL(Ruby Hardware Description Language)等,目前最普遍使用的是VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)与Verilog2。本领域技术人员也应该清楚,只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中,就可以很容易得到实现该逻辑方法流程的硬件电路。

[0138] 本说明书中的各个实施方式均采用递进的方式描述,各个实施方式之间相同相似的部分互相参见即可,每个实施方式重点说明的都是与其他实施方式的不同之处。

[0139] 上述实施方式阐明的系统、装置、模块或单元,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。

[0140] 为了描述的方便,描述以上装置时以功能分为各种单元分别描述。当然,在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0141] 通过以上的实施方式的描述可知,本领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品可以存储在存储介质中,如ROM/RAM、磁碟、光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本申请各个实施方式的某些部分的方法。

[0142] 本申请可用于众多通用或专用的计算机系统环境或配置中。例如:个人计算机、服务器计算机、手持设备或便携式设备、平板型设备、多处理器系统、基于微处理器的系统、置顶盒、可编程的消费电子设备、网络PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境等等。

[0143] 本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0144] 虽然通过实施方式描绘了本申请，本领域普通技术人员知道，本申请有许多变形和变化而不脱离本申请的精神，希望所附的权利要求包括这些变形和变化而不脱离本申请的精神。

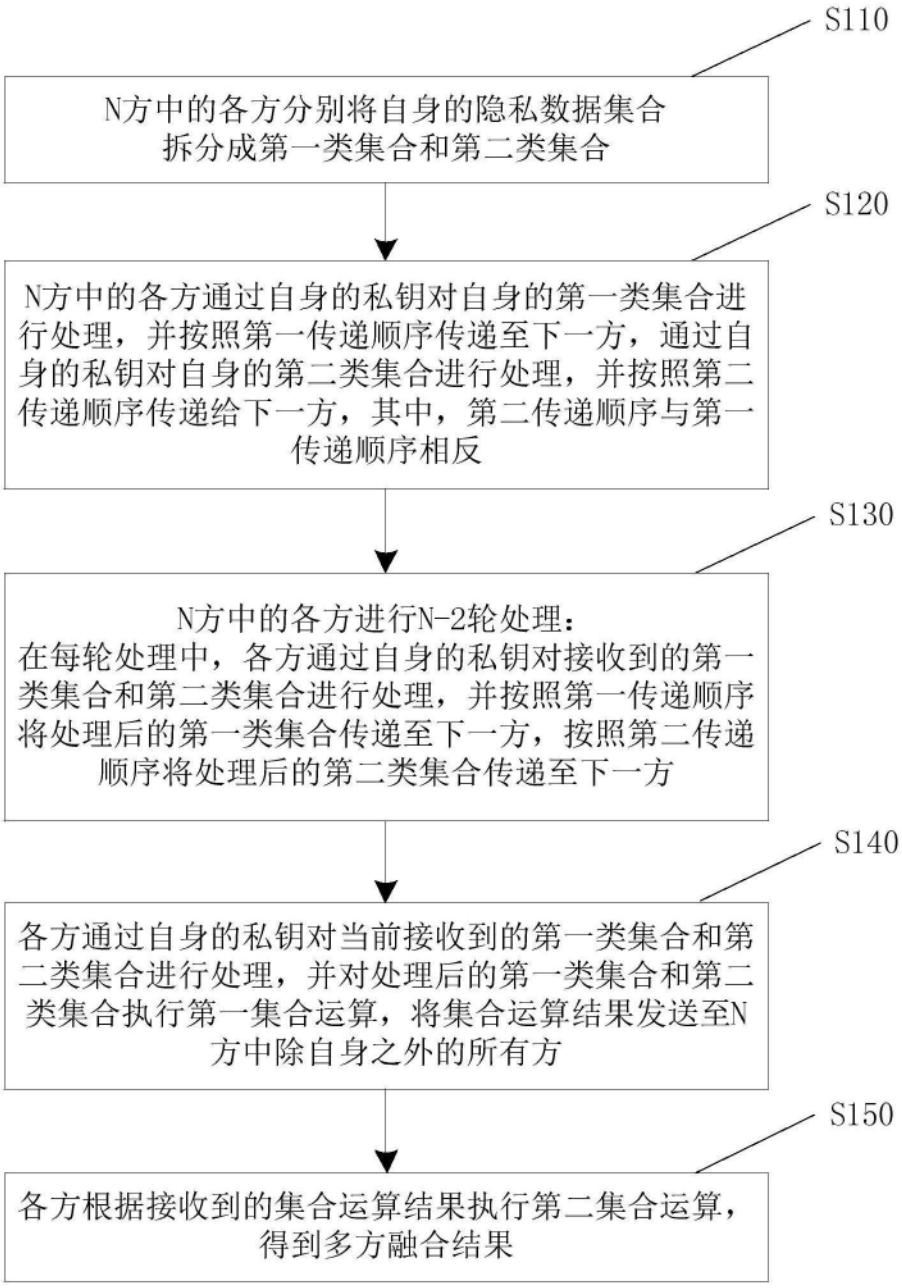

S110
N方中的各方分别将自身的隐私数据集合拆分成第一类集合和第二类集合
S120
N方中的各方通过自身的私钥对自身的第一类集合进行处理，并按照第一传递顺序传递至下一方，通过自身的私钥对自身的第二类集合进行处理，并按照第二传递顺序传递给下一方，其中，第二传递顺序与第一传递顺序相反
S130
N方中的各方进行N-2轮处理：
在每轮处理中，各方通过自身的私钥对接收到的第一类集合和第二类集合进行处理，并按照第一传递顺序将处理后的第一类集合传递至下一方，按照第二传递顺序将处理后的第二类集合传递至下一方
S140
各方通过自身的私钥对当前接收到的第一类集合和第二类集合进行处理，并对处理后的第一类集合和第二类集合执行第一集合运算，将集合运算结果发送至N方中除自身之外的所有方
S150
各方根据接收到的集合运算结果执行第二集合运算，得到多方融合结果

图1

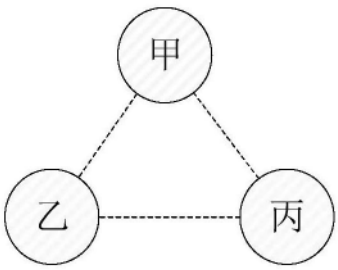

甲
乙
丙

图2A

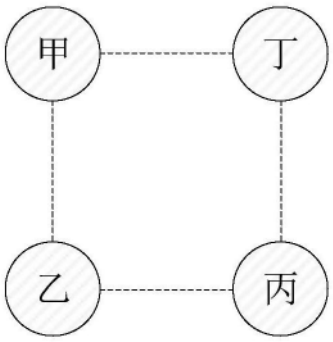


图2B

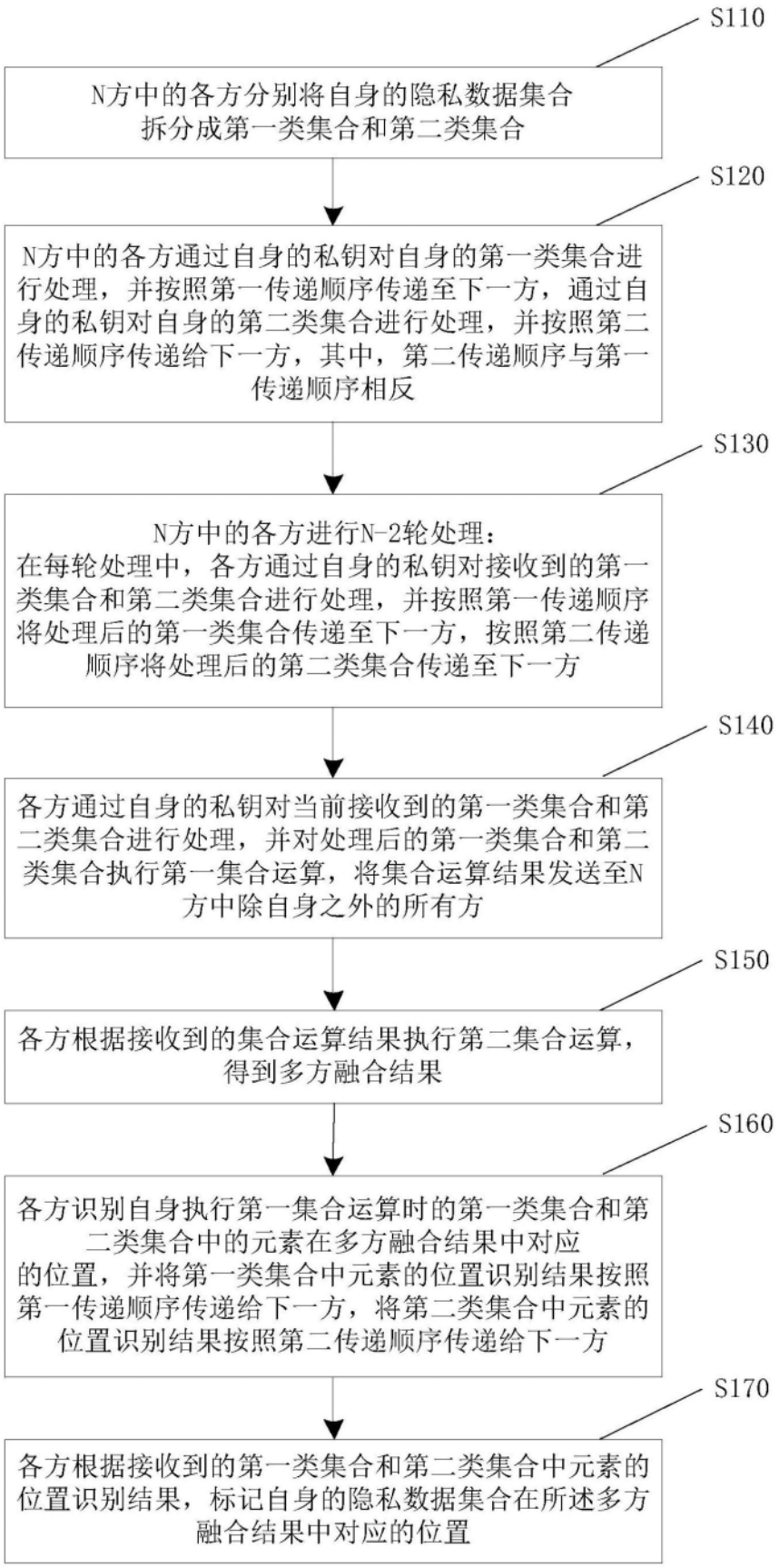

S110
N方中的各方分别将自身的隐私数据集合拆分成第一类集合和第二类集合
S120
N方中的各方通过自身的私钥对自身的第一类集合进行处理，并按照第一传递顺序传递至下一方，通过自身的私钥对自身的第二类集合进行处理，并按照第二传递顺序传递给下一方，其中，第二传递顺序与第一传递顺序相反
S130
N方中的各方进行N-2轮处理：
在每轮处理中，各方通过自身的私钥对接收到的第一类集合和第二类集合进行处理，并按照第一传递顺序将处理后的第一类集合传递至下一方，按照第二传递顺序将处理后的第二类集合传递至下一方
S140
各方通过自身的私钥对当前接收到的第一类集合和第二类集合进行处理，并对处理后的第一类集合和第二类集合执行第一集合运算，将集合运算结果发送至N方中除自身之外的所有方
S150
各方根据接收到的集合运算结果执行第二集合运算，得到多方融合结果
S160
各方识别自身执行第一集合运算时的第一类集合和第二类集合中的元素在多方融合结果中对应的位置，并将第一类集合中元素的位置识别结果按照第一传递顺序传递给下一方，将第二类集合中元素的位置识别结果按照第二传递顺序传递给下一方
S170
各方根据接收到的第一类集合和第二类集合中元素的位置识别结果，标记自身的隐私数据集合在所述多方融合结果中对应的位置

图3

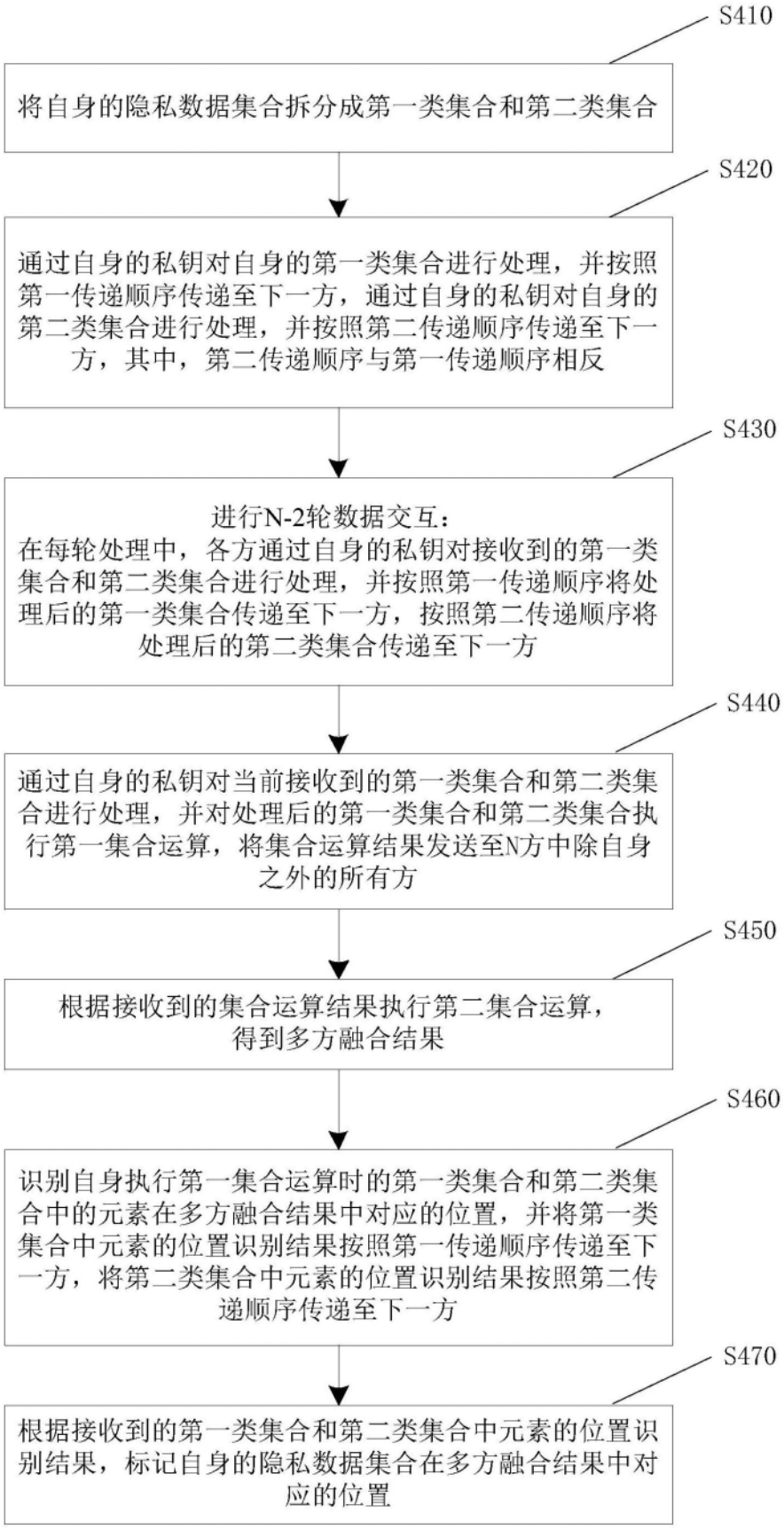

S410
将自身的隐私数据集合拆分成第一类集合和第二类集合
S420
通过自身的私钥对自身的第一类集合进行处理，并按照第一传递顺序传递至下一方，通过自身的私钥对自身的第二类集合进行处理，并按照第二传递顺序传递至下一方，其中，第二传递顺序与第一传递顺序相反
S430
进行N-2轮数据交互：
在每轮处理中，各方通过自身的私钥对接收到的第一类集合和第二类集合进行处理，并按照第一传递顺序将处理后的第一类集合传递至下一方，按照第二传递顺序将处理后的第二类集合传递至下一方
S440
通过自身的私钥对当前接收到的第一类集合和第二类集合进行处理，并对处理后的第一类集合和第二类集合执行第一集合运算，将集合运算结果发送至N方中除自身之外的所有方
S450
根据接收到的集合运算结果执行第二集合运算，得到多方融合结果
S460
识别自身执行第一集合运算时的第一类集合和第二类集合中的元素在多方融合结果中对应的位置，并将第一类集合中元素的位置识别结果按照第一传递顺序传递至下一方，将第二类集合中元素的位置识别结果按照第二传递顺序传递至下一方
S470
根据接收到的第一类集合和第二类集合中元素的位置识别结果，标记自身的隐私数据集合在多方融合结果中对应的位置

图4

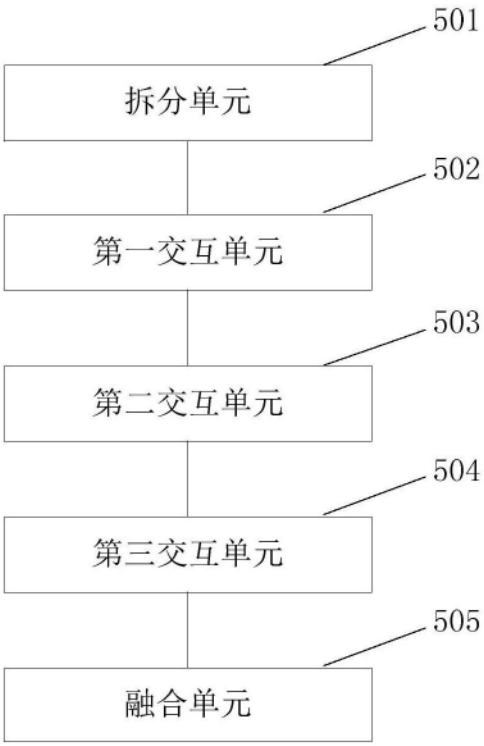


图5A

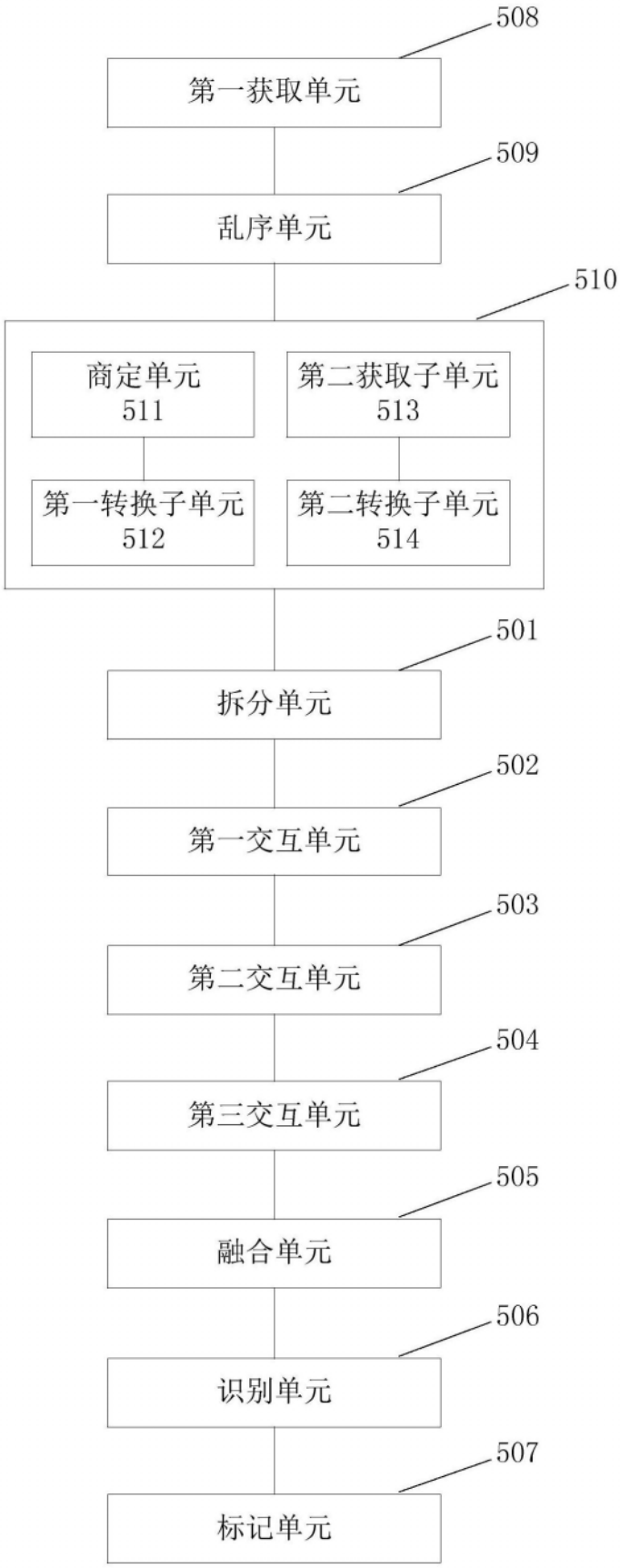

508
第一获取单元
509
乱序单元
510
商定单元
511
第二获取子单元
513
第一转换子单元
512
第二转换子单元
514
501
拆分单元
502
第一交互单元
503
第二交互单元
504
第三交互单元
505
融合单元
506
识别单元
507
标记单元

图5B

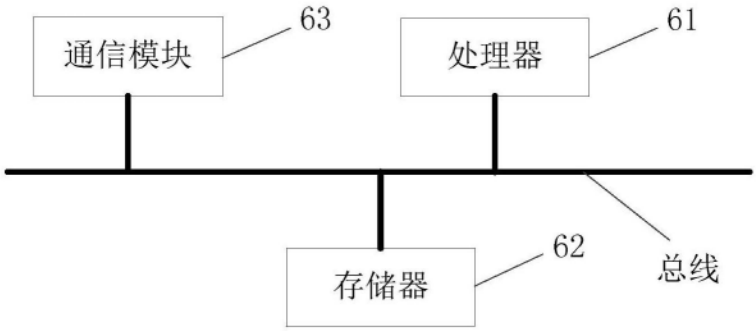


图6