(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2024 年 12 月 12 日 (12.12.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/251098 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2024/097142

(22) 国际申请日: 2024 年 6 月 3 日 (03.06.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310666563.3 2023年6月6日 (06.06.2023) CN

(71) 申请人: 北京火山引擎科技有限公司 (**BEIJING VOLCANO ENGINE TECHNOLOGY CO., LTD.**) [CN/CN]; 中国北京市海淀区紫金数码园4号楼13层1309, Beijing 100190 (CN)。

(72) 发明人:林宇(**LIN, Yu**); 中国北京市朝阳区七圣中街12号院融中心B1小邮局, Beijing 100028 (CN)。蔡权伟(**CAI, Quanwei**); 中国北京市朝阳区七圣中街12号院融中心B1小邮局, Beijing 100028 (CN)。吴烨(**WU, Ye**); 中国北京市朝阳区七圣中街12号院融中心B1小邮局, Beijing 100028 (CN)。

(74) 代理人:北京世辉律师事务所(**SHIHUI PARTNERS**); 中国北京市朝阳区建国门外大街2号北京银泰中心C座42层, Beijing 100022 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ,

WO 2024/251098 A1

(54) **Title:** DATA PROCESSING METHOD AND ELECTRONIC DEVICE

(54) 发明名称: 数据处理方法和电子设备

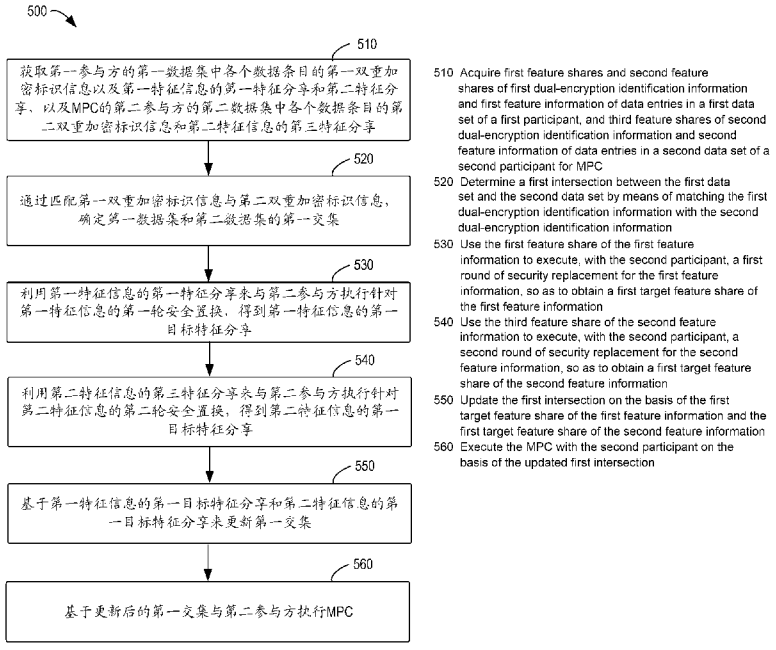

图 5

(57) **Abstract:** Provided in the embodiments of the present disclosure are a data processing method and an electronic device. The method comprises: a first participant acquiring first feature shares and second feature shares of first dual-encryption identification information and first feature information of a first data set of the first participant, and first feature shares of second dual-encryption identification information and second feature information of a second data set of a second participant; determining a first intersection between the first data set and the second data set by means of matching the first dual-encryption identification information with the

[见续页]

LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第21条(3))。

second dual-encryption identification information; using the first feature share of the first feature information to execute a first round of security replacement with the second participant, so as to obtain a first target feature share of the first feature information; using the first feature share of the second feature information to execute a second round of security replacement with the second participant, so as to obtain a first target feature share of the second feature information; and updating the first intersection, and executing MPC with the second participant on the basis of the updated first intersection.

(57) 摘要: 本公开的实施例提供了数据处理方法和电子设备。该方法包括：第一参与方获取第一参与方的第一数据集的第一双重加密标识信息、第一特征信息的第一特征分享和第二特征分享，以及第二参与方的第二数据集的第二双重加密标识信息和第二特征信息的第一特征分享；通过匹配第一双重加密标识信息与第二双重加密标识信息，确定第一数据集和第二数据集的第一交集；利用第一特征信息的第一特征分享与第二参与执行第一轮安全置换，得到第一特征信息的第一目标特征分享；并利用第二特征信息的第一特征分享与第二参与执行第二轮安全置换，得到第二特征信息的第一目标特征分享。更新第一交集并基于更新后的第一交集与第二参与方执行MPC。

数据处理方法和电子设备

本申请要求 2023 年 06 月 06 日递交的、标题为“数据处理方法和电子设备”、申请号为 202310666563.3 的中国发明专利申请的优先权，该申请的全部内容通过引用结合在本申请中。

技术领域

本公开的示例实施例总体涉及计算机领域，特别地涉及用于数据处理的方法、装置、设备和计算机可读存储介质。

背景技术

近年来，由于用户隐私、数据安全、合法合规、商业竞争等因素，很难合法和合规的将分散的数据源整合到一起进行计算、分析和学习。在这样的背景下，基于多方安全计算（Secure Multi-party Computation，MPC）的解决方案迅速发展起来，在不需要将分散数据源集中在一起的情况下就可以联合多个分散的数据源进行联合计算、联合数据分析和联合机器学习。MPC 旨在解决一组互不信任的参与方在保护数据安全的情况下执行协同计算的问题，为数据需求方提供不泄露原始数据前提下的多方协同计算能力。多方安全计算可以用于支持安全的数据合作和融合应用，在数据不出域、合法合规的前提下联合多方数据源进行计算和分析。

发明内容

在本公开的第一方面，提供了一种数据处理方法。该方法被实现在多方安全计算 MPC 的第一参与方，该方法包括：获取第一参与方的第一数据集中各个数据条目的第一双重加密标识信息以及第一特征信息的第一特征分享和第二特征分享，以及 MPC 的第二参与方的

第二数据集中各个数据条目的第二双重加密标识信息和第二特征信息的第三特征分享；通过匹配第一双重加密标识信息与第二双重加密标识信息，确定第一数据集和第二数据集的第一交集，第一交集中的数据条目包括相匹配的标识信息以及标识信息所标识的第一特征信息的第二特征分享和第二特征信息的第三特征分享；利用第一特征信息的第一特征分享来与第二参与方执行针对第一特征信息的第一轮安全置换，得到第一特征信息的第一目标特征分享；利用第二特征信息的第三特征分享来与第二参与方执行针对第二特征信息的第二轮安全置换，得到第二特征信息的第一目标特征分享；基于第一特征信息的第一目标特征分享和第二特征信息的第一目标特征分享来更新第一交集；以及基于更新后的第一交集与第二参与方执行 MPC。

在本公开的第二方面，提供了一种数据处理方法。该方法被实现在多方安全计算 MPC 的第二参与方，该方法包括：获取 MPC 的第一参与方的第一数据集中各个数据条目的第一特征信息的第四特征分享和针对第一数据集的第一置换信息，以及第二参与方的第二数据集中各个数据条目的第二特征信息的第一特征分享；利用第一特征信息的第四特征分享和第一置换信息来与第一参与方执行针对第一特征信息的第一轮安全置换，得到第一特征信息的第二目标特征分享；利用第二特征信息的第一特征分享来与第一参与方执行针对第二特征信息的第二轮安全置换，得到第二特征信息的第二目标特征分享；基于第一特征信息的第二目标特征分享和第二特征信息的第一目标特征分享来生成针对第一数据集和第二数据集的第二交集；以及基于第二交集与第一参与方执行 MPC。

在本公开的第三方面，提供了一种数据处理装置。该装置被实现在多方安全计算 MPC 的第一参与方，该装置包括：信息获取模块，被配置为获取第一参与方的第一数据集中各个数据条目的第一双重加密标识信息以及第一特征信息的第一特征分享和第二特征分享，以及 MPC 的第二参与方的第二数据集中各个数据条目的第二双重加密标识信息和第二特征信息的第三特征分享；第一交集确定模块，被配

置为通过匹配第一双重加密标识信息与第二双重加密标识信息，确定第一数据集和第二数据集的第一交集，第一交集中的数据条目包括相匹配的标识信息以及标识信息所标识的第一特征信息的第二特征分享和第二特征信息的第三特征分享；第一安全置换模块，被配置为利用第一特征信息的第一特征分享来与第二参与方执行针对第一特征信息的第一轮安全置换，得到第一特征信息的第一目标特征分享；第二安全置换模块，被配置为利用第二特征信息的第三特征分享来与第二参与方执行针对第二特征信息的第二轮安全置换，得到第二特征信息的第一目标特征分享；交集更新模块，被配置为基于第一特征信息的第一目标特征分享和第二特征信息的第一目标特征分享来更新第一交集；以及 MPC 执行模块，被配置为基于更新后的第一交集与第二参与方执行 MPC。

在本公开的第四方面，提供了一种数据处理装置。该装置被实现在多方安全计算 MPC 的第二参与方，该装置包括：信息获取模块，被配置为获取 MPC 的第一参与方的第一数据集中各个数据条目的第一特征信息的第四特征分享和针对第一数据集的第一置换信息，以及第二参与方的第二数据集中各个数据条目的第二特征信息的第一特征分享；第一安全置换模块，被配置为利用第一特征信息的第四特征分享和第一置换信息来与第一参与方执行针对第一特征信息的第一轮安全置换，得到第一特征信息的第二目标特征分享；第二安全置换模块，被配置为利用第二特征信息的第一特征分享来与第一参与方执行针对第二特征信息的第二轮安全置换，得到第二特征信息的第二目标特征分享；第二交集生成模块，被配置为基于第一特征信息的第二目标特征分享和第二特征信息的第一目标特征分享来生成针对第一数据集和第二数据集的第二交集；以及 MPC 执行模块，被配置为基于第二交集与第一参与方执行 MPC。

在本公开的第五方面，提供了一种电子设备。该设备包括至少一个处理单元；以及至少一个存储器，至少一个存储器被耦合到至少一个处理单元并且存储用于由至少一个处理单元执行的指令。指令在由

至少一个处理单元执行时使电子设备执行第一方面的方法。

在本公开的第六方面，提供了一种电子设备。该设备包括至少一个处理单元；以及至少一个存储器，至少一个存储器被耦合到至少一个处理单元并且存储用于由至少一个处理单元执行的指令。指令在由至少一个处理单元执行时使电子设备执行第二方面的方法。

在本公开的第七方面，提供了一种计算机可读存储介质。该计算机可读存储介质上存储有计算机程序，计算机程序可由处理器执行以实现第一方面的方法。

在本公开的第八方面，提供了一种计算机可读存储介质。该计算机可读存储介质上存储有计算机程序，计算机程序可由处理器执行以实现第二方面的方法。

应当理解，该部分中所描述的内容并非旨在限定本公开的实施例的关键特征或重要特征，也不用于限制本公开的范围。本公开的其他特征将通过以下的描述而变得容易理解。

附图说明

结合附图并参考以下详细说明，本公开各实施例的上述和其他特征、优点及方面将变得更加明显。在附图中，相同或相似的附图标记表示相同或相似的元素，其中：

图 1 示出了能够在其中实现本公开的实施例的示例环境的示意图；

图 2 示出了根据本公开的一些实施例的用于数据处理的多方信令流的流程图；

图 3 示出了根据本公开的一些实施例的安全置换的示例的示意图；

图 4 示出了根据本公开的一些实施例的基于示例数据集的数据处理信令流的流程图；

图 5 示出了根据本公开的一些实施例的在第一参与方处实现的数据处理方法的流程图；

图 6 示出了根据本公开的一些实施例的在第二参与方处实现的数据处理方法的流程图；

图 7 示出了根据本公开的一些实施例的在第一参与方处实现的数据处理装置的示意性结构框图；

图 8 示出了根据本公开的一些实施例的在第二参与方处实现的数据处理装置的示意性结构框图；以及

图 9 示出了可以实施本公开的一个或多个实施例的电子设备的框图。

具体实施方式

下面将参照附图更详细地描述本公开的实施例。虽然附图中示出了本公开的某些实施例，然而应当理解的是，本公开可以通过各种形式来实现，而且不应该被解释为限于这里阐述的实施例，相反，提供这些实施例是为了更加透彻和完整地理解本公开。应当理解的是，本公开的附图及实施例仅用于示例性作用，并非用于限制本公开的保护范围。

在本公开的实施例的描述中，术语“包括”及其类似用语应当理解为开放性包含，即“包括但不限于”。术语“基于”应当理解为“至少部分地基于”。术语“一个实施例”或“该实施例”应当理解为“至少一个实施例”。术语“一些实施例”应当理解为“至少一些实施例”。下文还可能包括其他明确的和隐含的定义。

在本文中，除非明确说明，“响应于 A”执行一个步骤并不意味着在“A”之后立即执行该步骤，而是可以包括一个或多个中间步骤。

可以理解的是，本技术方案所涉及的数据（包括但不限于数据本身、数据的获得、使用、存储或删除）应当遵循相应法律法规及相关规定的要求。

首先对本公开的实施例中涉及的名词进行简要介绍。

秘密分享（secret share）：通过某种运算将一个数据值拆分为多份的加密方式。例如，加法秘密分享可以将数据值x拆分为$x = x_1 + x_2$两个秘密分享值。

多方安全计算（MPC）：指的是存在 N 个参与方 P1, P2, …, PN,

其中参与方 Pi 拥有输入数据 Xi，在不向任何其他参与方泄露自己的输入数据的前提下，N 个参与方共同计算一个函数 f(X1, X2, …, XN)。在运算中通过应用密码学（如同态加密）、秘密分享、差分隐私等安全机制，可以确保输入数据的安全性。例如，多个参与方输入数据的秘密分享值，可以计算指定算术运算、逻辑运算，输出的运算结果仍为秘密分享的形式。

椭圆曲线密钥交换（Elliptic Curve Diffie–Hellman key Exchange，ECDH）：两个参与方通过椭圆曲线加密算法实现密钥交换。

同态加密（Homomorphic Encryption，HE）：是实现多方安全计算的方法之一。同态加密允许对密文进行特定形式的代数运算得到仍然是密文空间里的运算结果。经过加密后的数据，可以通过同态加法、乘法运算等，在不解密数据的情况下计算得到新的密文，新密文解密后可以得到经过相应同态运算的数据。也就是说，在密文空间的运算等价于在明文空间里的运算。因此，利用同态加密技术，可以在加密的数据上进行运算，而在整个运算过程中无需对数据进行解密。

图 1 示出了本公开的实施例能够在其中实现的示例环境 100 的示意图。环境 100 涉及基于 MPC 协议的安全计算。出于示例性目的，示出了参与方 110（在本文中有时称为第一参与方、参与方 C、或 C 方）和参与方 120（也称为第二参与方、参与方 P、或 P 方）。参与方 110 具有自己的数据集 112，参与方 120 具有自己的数据集 122。在 MPC 运算中，两个参与方期望在确保各自数据集的数据安全的情况下进行指定运算。

数据集 112 和数据集 122 中的每个数据集可以包括一个或多个数据条目，每个数据条目包括标识信息和特征信息。每个数据条目的标识信息可以包括一个或多个标识类型对应的标识符（ID），特征信息可以包括一个或多个特征类型对应的特征。标识信息部分用于标识或区分特征信息部分。举例而言，对于记录广告投放情况的数据集，标识信息的类型可以包括广告投放平台标识和广告投放用户标识，特征信息的类型可以包括广告是否被点击、广告被观看时长、广告是否被

收藏等。

在一些实现中，数据集 112 和数据集 122 的标识信息可以包括一个或多个相同标识类型，例如都包括广告投放平台标识和广告投放用户标识。在一些实现中，数据集 112 和数据集 122 的特征信息可以包括一个或多个相同特征类型，或者可以包括完全不同的特征类型。

在图 1 中，参与方 110 或参与方 120 均可以对应于任意类型的具有计算能力的一个或多个电子设备，包括终端设备或服务端设备。终端设备可以是任意类型的移动终端、固定终端或便携式终端，包括移动手机、台式计算机、膝上型计算机、笔记本计算机、上网本计算机、平板计算机、媒体计算机、多媒体平板、个人通信系统（PCS）设备、个人导航设备、个人数字助理（PDA）、音频/视频播放器、数码相机/摄像机、定位设备、电视接收器、无线电广播接收器、电子书设备、游戏设备或者前述各项的任意组合，包括这些设备的配件和外设或者其任意组合。服务端设备例如可以包括计算系统/服务器，诸如大型机、边缘计算节点、云环境中的计算设备，等等。

应当理解，仅出于示例性的目的描述环境 100 的结构和功能，而不暗示对于本公开的范围的任何限制。例如，虽然图 1 为示出，在一些情况下，MPC 运算还可以涉及更多参与方，每个参与方可以具有各自的数据集。

在 MPC 运算中，有时需要确定多个参与方的数据集之间的交集匹配。举例来说，多个参与方各输入一个数据集，在不泄漏双方交集的条件下，确定多个数据集的交集。这里的交集指的是两个数据集中标识信息相匹配的数据条目。在一些实现中，通过交集匹配，可以确定合并两个数据集中由相同标识符所索引的不同特征信息。在一些实现中，在获得匹配标识信息的情况下，还可以生成交集中的数据条目的特征信息的密码分享，用于后续的 MPC 运算。

在一些交集匹配方案中，基于双重椭圆曲线密钥交换（ECDH）技术来生成双方并集的匿名标识（ID），其中双方的交集部分会被映射为相同的匿名 ID。之后，双方通过匿名 ID 执行 MPC 协议完成后

续计算。然而这类协议所生成的结果是双方的并集，当双方数据量不平衡时，并集的规模很大，而实际有意义的交集部分很少，导致后续MPC计算协议会产生很大的额外开销。

另一些方案基于MPC协议，以秘密分享的形式匹配出双方的交集ID，并同时生成双方特征的秘密分享。然而，这类方案对通信条件要求比较高，且难以实现多ID的匹配。而且，当某个数据集中包含重复ID时，计算开销较大。

当前，期望能够提供通信和计算方面高效，且能确保交集信息的安全性的交集匹配方案。

根据本公开的示例实施例，提供了一种用于数据处理的改进方案。该方案基于安全置换（secure permutation）协议，也称为不经意置换协议。根据该方案，对于MPC中具有第一数据集的第一参与方和具有第二数据集的第二参与方，第一参与方获取第一参与方的第一数据集中各个数据条目的第一双重加密标识信息以及第一特征信息的第一特征分享和第二特征分享，以及第二参与方的第二数据集中各个数据条目的第二双重加密标识信息和第二特征信息的第一特征分享。第一参与方通过匹配第一双重加密标识信息与第二双重加密标识信息，确定第一数据集和第二数据集的第一交集，第一交集中的数据条目包括相匹配的标识信息以及标识信息所标识的第一特征信息的第二特征分享和第二特征信息的第一特征分享。然后，第一参与方利用第一特征信息的第一特征分享来与第二参与方执行针对第一特征信息的第一轮安全置换，得到第一特征信息的第一目标特征分享；并且利用第二特征信息的第一特征分享来与第二参与方执行针对第二特征信息的第二轮安全置换，得到第二特征信息的第一目标特征分享。第一参与方基于第一特征信息的第一目标特征分享和第二特征信息的第一目标特征分享来更新第一交集；并且基于更新后的第一交集与第二参与方执行MPC。

根据本公开的实施例，通过安全置换技术，在不暴露交集的情况下生成了双方数据交集特征的特征分享（即，秘密分享）。该方案显

著提高了交集匹配的效率。

以下将继续参考附图描述本公开的一些示例实施例。

图 2 示出了根据本公开的一些实施例的用于数据处理的多方信令流 200 的流程图。为便于讨论，将参考图 1 的环境 100 来信令流 200。信令流 200 涉及参与方 110 和参与方 120，其中参与方 110 具有数据集 112，参与方 120 具有数据集 122。

假设数据集 112 和数据集 122 的数据条目均包括一个或多个类型的标识信息；数据集 112 包括n_c个数据条目，每个数据条目包括m_c个特征；数据集 122 包括n_p个数据条目，每个数据条目包括m_p个特征。数据集 112 可以被表示为$\{(Cid_i, u_{i,0}, \ldots, u_{i,m_c})\}_{i\in[n_c]}$（在此使用$[n_c]$的形式表示范围$[0, n_c)$，下同），其中$Cid_i$指的是第 i 个数据条目的标识信息，$u_{i,0}$指的是第 i 个数据条目的特征 0，$u_{i,m_c}$指的是第 i 个数据条目的特征$m_c$。类似的，数据集 122 可以被表示为$\{(Pid_i, v_{i,0}, \ldots, v_{i,m_p})\}_{i\in[n_p]}$。

在信令流 200 中，参与方 110 和参与方 120 各自获取后续用于安全置换需要的信息。特别地，参与方 110 获取数据集 112 中各个数据条目的双重加密标识信息$\widetilde{Cid}_i$以及特征信息$u_{i,j}$的第一特征分享$[u_{i,j}]_0$和第二特征分享$u''_{i,j}$，以及参与方 120 的数据集 122 中各个数据条目的双重加密标识信息$\widetilde{Pid}_i$和特征信息$v_{i,j}$的第一特征分享$v'_{i,j}$。参与方 120 获取参与方 110 的数据集 112 中各个数据条目的第一特征信息$u_{i,j}$的第四特征分享$[u_{i,j}]_1$和针对数据集 112 的第一置换信息π_1，以及参与方 120 的数据集 122 中各个数据条目的特征信息$v_{i,j}$的第一特征分享$[v_{i,j}]_0$。

在一些实施例中，参与方 110 初始地具有自己的原始数据集 112，而参与方 120 初始地具有自己的原始数据集 122。参与方 110 和参与方 120 可以通过对标识信息加密和生成特征信息的秘密分享，来进行信息交换。考虑到加密需要，在初始化阶段，参与方 110 和参与方 120 可以各自确定要使用的加密方式以及密钥。

在一些实施例中，数据集 112 和 122 中的标识信息可以基于椭圆曲线加密算法来实现，并且参与方 110 和 120 可以通过椭圆曲线密钥交换来实现密钥交换。举例来说，参与方 110 可以随机选择椭圆曲线加密密钥r_c；并且参与方 120 可以随机选择椭圆曲线加密密钥r_p。在其他实施例中，对标识信息的加密还可以基于其他任何适当的加密算法，只要参与方 110 和 120 各自选择用于对标识信息进行加密的密钥。

在一些实施例中，参与方 110 和参与方 120 可以首先同步数据集 112 和数据集 122 的数据量。如果数据集 112 的数据条目数量和数据集 122 的数据条目数量不相等（即，$n_c \neq n_p$），则参与方 110 和/或参与方 120 需要对数据集进行填充。这是因为后续要使用到安全置换协议，而安全置换协议不能改变数据量，因此在初始阶段要求双方数据量相同。在一些实施例中，参与方 110 和/或参与方 120 可以使用随机标识信息，并使用 0 作为特征信息来填充数据集 112 和/或数据集 122。在一些实施例中，填充的随机标识信息可以与数据集 112 或数据集 122 中的真实标识信息不相同。例如，可以从一个很大范围内选择随机标识信息，以保证出现相同标识信息的概率可忽略。在一些实施例中，在填充后，可以使数据集 112 和数据集 122 均包含$max(n_c, n_p)$个数据条目。为便于讨论，在后续步骤中，假设$n_c = n_p = max(n_c, n_p)$的情况。

在上述初始化阶段和加密方式确定后，参与方 110 和 120 可以执行各自数据集的标识信息加密和特征信息的特征分享生成以及交换。参与方 110 可以对自己数据集 112 中各个数据条目的标识信息执行一次加密以及生成特征信息的特征分享（210），得到加密标识信息和特征信息的第三特征分享（在图 2 中分别被标记为“加密标识信息 1”和“特征分享 1-3”）。参与方 120 可以对自己数据集 122 中各个数据条目的标识执行一次加密以及生成特征信息的特征分享（212），得到加密标识信息和特征信息的第三特征分享（在图 2 中分别被标记为“加密标识信息 2”和“特征分享 2-3”）。

在一些实施例中，标识信息加密和特征信息的特征分享生成可以由任一方触发。在一些实施例中，如果参与方 120 是可多次调用的客户端，而参与方 110 是服务器侧，可以由参与方 120 先发起请求。在一些实施例中，在接收到请求后，参与方 110 可以根据客户端 120 的数据集 122 的大小（即其中的数据条目的数目）来确定是否需要在数据集 112 中填充伪数据条目。应当理解，参与方 110 和参与方 120 在不同应用场景中可能对应于不同实体，两者的交集匹配可以基于任意原因、由任一方或由双方协商来触发。

在一些实施例中，在加密之前，参与方 110 可以对数据集 112 中的各个数据条目进行乱序处理。可选地或附加地，参与方 120 可以对数据集 122 中的各个数据条目进行乱序处理。

在一些实施例中，在加密标识信息时，参与方 110 可以使用第一加密密钥，例如椭圆曲线加密密钥r_c来对数据集 112 中各个数据条目的标识信息Cid_i进行加密，得到数据集 112 的加密标识信息，即$Cid'_i = r_c \cdot H(Cid_i)$。这样，数据集 112 中各个数据条目的标识信息被随机化，以避免向其他方透露真实标识信息。类似的，参与方 120 可以使用第二加密密钥，例如椭圆曲线加密密钥r_p来对数据集 122 中各个数据条目的标识信息Pid_i进行加密，得到数据集 122 的加密标识信息，即$Pid'_i = r_p \cdot H(Pid_i)$。这样，数据集 122 中各个数据条目的标识信息被随机化，以避免向其他方透露真实标识信息。在加密过程中，$H: \{0,1\}^* \to \mathbb{G}$，是将任意输入映射为椭圆曲线点的哈希函数。当然，如上文提及的，对标识信息的加密还可以基于任何其他适当加密算法。

在生成特征信息的特征分享（也称为秘密分享）时，参与方 110 可以随机生成本方数据集 112 的特征信息$u_{i,j}$的第一特征分享$\left\{[u_{i,j}]_0\right\}_{i\in[n_c],j\in[m_c]}$。参与方 110 基于第一特征分享来生成特征信息$u_{i,j}$的第三特征分享$u'_{i,j}$。举例来说，参与方 110 将数据集 112 的特征信息$u_{i,j}$减去第一特征分享$[u_{i,j}]_0$，得到第三特征分享，即$u'_{i,j} = u_{i,j} - [u_{i,j}]_0$。

类似地，参与方 120 可以随机生成本方数据集 122 的特征信息$v_{i,j}$的第一特征分享$\left\{\left[v_{i,j}\right]_0\right\}_{i\in[n_p],j\in[m_p]}$。参与方 110 基于第一特征分享来生成特征信息$v_{i,j}$的第三特征分享$v'_{i,j}$。举例来说，参与方 120 将数据集 122 的特征信息$v_{i,j}$减去第一特征分享$\left[v_{i,j}\right]_0$，得到第三特征分享，即$v'_{i,j} = v_{i,j} - \left[v_{i,j}\right]_0$。

参与方 110 将数据集 112 的加密标识信息和特征信息的第三特征分享$\left\{\left(Cid'_i, u'_{i,j}\right)\right\}_{i\in[n_c],j\in[m_c]}$发送（220）给参与方 120。参与方 120 将数据集 122 的加密标识信息和特征信息的第三特征分享$\left\{\left(Pid'_i, v'_{i,j}\right)\right\}_{i\in[n_p],j\in[m_p]}$发送（222）给参与方 110。

接下来，参与方 110 和参与方 120 再次加密接收到的对方加密标识信息，得到双重加密标识信息。

在一些实施例中，在接收到数据集 122 的加密标识信息和特征信息的第三特征分享$\left\{\left(Pid'_i, v'_{i,j}\right)\right\}_{i\in[n_p],j\in[m_p]}$后，参与方 110 对接收到的数据集 122 的加密标识信息Pid'_i执行二次加密（230）。在一些实施例中，在对加密标识信息Pid'_i执行二次加密时，参与方 110 可以再次使用第一加密密钥（例如，用于对数据集 112 中的标识信息执行一次加密的椭圆曲线加密密钥r_c）来对数据集 122 中的加密标识信息Pid'_i执行二次加密，得到数据集 122 的双重加密标识信息$\widetilde{Pid}_i = r_c r_p \cdot H(Pid_i)$。

类似地，参与方 120 对接收到的数据集 112 的加密标识信息Cid'_i执行二次加密和特征分享生成（232）。在一些实施例中，在对加密标识信息Cid'_i执行二次加密时，参与方 120 可以再次使用第二加密密钥（例如，用于对数据集 122 中的标识信息执行一次加密的椭圆曲线加密密钥r_p）来对数据集 112 中的加密标识信息Cid'_i执行二次加密，得到数据集 122 的双重加密标识信息$\widetilde{Cid}_i = r_P r_c \cdot H(Cid_i)$。

此外，参与方 120 还随机生成数据集 112 的特征信息$u_{i,j}$的第四特征分享$\left\{\left[u_{i,j}\right]_1\right\}_{i\in[n_c],j\in[m_c]}$，并且基于接收到的数据集 112 的特征信息的第三特征分享$\left\{u'_{i,j}\right\}_{i\in[n_c],j\in[m_c]}$和所生成的第四特征分享

$\left\{\left[u_{i,j}\right]_1\right\}_{i\in[n_c],j\in[m_c]}$，生成数据集 112 的特征信息$u_{i,j}$的第二特征分享（$u''_{i,j}$），例如将$u'_{i,j}$减去特征分享$\left[u_{i,j}\right]_1$，得到第二特征分享$u''_{i,j} = u'_{i,j} - \left[u_{i,j}\right]_1$。参与方 120 随机生成第一置换信息$\pi_1$，其可以是$[0, n_c)$范围内的随机置换向量，用于扰乱数据集 112 的双重加密标识信息$\widetilde{Cid}_i$与第二特征分享$u''_{i,j}$之间的对应关系，即$\pi_1\left(\left\{\left(\widetilde{Cid}_i, u''_{i,j}\right)\right\}_{i\in[n_c],j\in[m_c]}\right)$。这样，数据集 112 的双重加密标识信息$\widetilde{Cid}_i$与第二特征分享$u''_{i,j}$之间的对应关系被置换。参与方 112 将置换后的数据集 112 的双重加密标识信息$\widetilde{Cid}_i$与第二特征分享$u''_{i,j}$（在图中被表示为<双重加密标识信息 1，特征分享 1-2>）发送（234）给参与方 110。

这样，参与方 110 获得数据集 112 的双重加密标识信息$\widetilde{Cid}_i$以及数据集 122 的双重加密标识信息$\widetilde{Pid}_i$。接下来，参与方 110 根据双方数据的双重加密标识信息进行交集匹配，得到将双方数据集对齐（即交集数据条目都处于相同的位置）所需要的置换。举例来说，参与方 110 通过匹配数据集 112 的双重加密标识信息$\widetilde{Cid}_i$和数据集 122 的双重加密标识信息$\widetilde{Pid}_i$，确定（240）数据集 112 与数据集 122 的第一交集。在本公开的实施例中，两个数据集的交集指的是找出两个数据集中标识信息相匹配（或相同）的数据条目。第一交集中的数据条目包括相匹配的标识信息以及标识信息所标识的特征信息$u_{i,j}$的第二特征分享（$u''_{i,j}$）和特征信息$v_{i,j}$的第三特征分享$v'_{i,j}$。

参与方 110 基于数据集 112 的双重加密标识信息$\left\{\widetilde{Cid}_i\right\}_{i\in[n_c]}$与数据集 122 的双重加密标识信息$\left\{\widetilde{Pid}_i\right\}_{i\in[n_p]}$之间的匹配结果，确定数据集 112 和数据集 122 中的哪些数据条目的标识信息相匹配。如前文所述，数据集 112 的双重加密标识信息$\widetilde{Cid}_i$分别由参与方 110 使用第一加密密钥r_c和参与方 120 使用第二加密密钥r_p进行加密，即$\widetilde{Cid}_i = r_p\, r_c \cdot H(Cid_i)$，而数据集 122 的双重加密标识信息$\widetilde{Pid}_i$分别由参与方 120 使用第二加密密钥$r_p$和参与方 110 使用第一加密密钥$r_c$进行加密，即$\widetilde{Pid}_i = r_c r_p \cdot H(Pid_i)$。如果数据集 112 中的某个数据条目的标识信

息与数据集 122 中某个数据条目的标识信息相匹配，那么经两个密钥r_c和r_p加密后，这两个数据条目的标识信息仍然相匹配。因此，可以在不透露实际标识信息的基础上，由参与方 110 执行标识信息的匹配与否的判断。

注意，虽然第一交集中的数据条目包括相匹配的标识信息以及标识信息所标识的特征信息$u_{i,j}$的第二特征分享（$u''_{i,j}$）和特征信息$v_{i,j}$的第三特征分享$v'_{i,j}$，但考虑到参与方 120 在将数据集 112 的双重加密标识信息$\widetilde{cid}_i$与第二特征分享$u''_{i,j}$发送给参与方 110 之前执行过一次扰乱，因此第二特征分享$u''_{i,j}$与标识信息的对应关系可能是不准确的。因此，参与方 110 和参与方 120 将调用安全置换协议来调整数据集 112 的特征分享和数据集 122 的特征分享。

在此，为便于理解，先参考图 3 来简单介绍安全置换协议的基本概念和实现方法。安全置换协议的主要功能 300 如下图所示，P0 方输入置换π和数据集的一个分享$[x]_0$，P1 方输入数据集的另一个分享$[x]_1$。输出结果为置换后数据集的分享$[y]_0$和$[y]_1$，满足$\pi([x]_0 + [x]_1) = [y]_0 + [y]_1$。安全置换协议有多种实现方式，在本公开中以一个典型的三方实现为例。三个参与方 P0、P1 和 P2 不合谋地执行以下步骤：

初始化阶段：假设数据长度为n，第三方 P2 首先生成长度为n的随机向量$\tilde{x}, u_0, u_1$和一个$[0, n)$范围的随机置换信息$\tilde{\pi}$，满足$\tilde{\pi}(\tilde{x}) = u_0 + u_1$。P2 将$\tilde{\pi}, u_0$发送给 P0，将$\tilde{x}, u_1$发送给 P1。

在线执行阶段：P0 输入 π，$[x]_0$，P1 输入$[x]_1$；

P0 计算$\pi \circ \tilde{\pi}^{-1}$并发送给 P1；P1 计算$[x]_1 - \tilde{x}$，并发送给 P0；

P0 计算得到$[y]_0 = \left(\pi([x]_1 - \tilde{x}) + \pi \circ \tilde{\pi}^{-1}(u_0)\right) + \pi([x]_0)$；

P1 计算得到$[y]_1 = \pi \circ \tilde{\pi}^{-1}(u_1)$。

以上过程可以验证正确性，即 $[y]_0 + [y]_1 = \pi([x]_0 + [x]_1)$。

除了上述实现方式之外，例如可以使用同态加密技术实现两方的安全置换协议：

P1 使用同态加密技术加密$\widetilde{[x]}_1 = Enc([x]_1)$，并发送给 P0；

P0 使用同态加法计算得到$\tilde{x} = Add(\widetilde{[x]}_1, [x]_0)$；

P0 使用置换信息π处理$\tilde{x}$得到$\tilde{y} = \pi(\tilde{x})$;

P0 生成随机特征分享$[y]_0$，计算$[\widetilde{y}]_1 = Add(\tilde{y}, -[y]_0)$，并发送给P1;

P1 解密得到$[y]_1 = Dec([\widetilde{y}]_1)$。

接下来返回参考图 2，参与方 110 与参与方 120 执行针对数据集 112 的特征信息的第一轮安全置换（250）。在第一轮安全置换中，参与方 110 拥有数据集 112 的特征信息$u_{i,j}$的第一特征分享$\{[u_{i,j}]_0\}_{i\in[n_c],j\in[m_c]}$，参与方 120 拥有数据集 112 的特征信息$u_{i,j}$的第四特征分享$\{[u_{i,j}]_1\}_{i\in[n_c],j\in[m_c]}$和第一置换信息$\pi_1$。在第一轮安全置换中，参与方 110 相当于安全置换协议中的 P1，参与方 120 相当于安全置换协议中的 P0。通过调用第一轮安全置换协议，可以调整第一交集中数据集 112 的特征分享，以获得与交集顺序对齐的数据集 112 的特征分享。

在一些实施例中，在第三方 P2 的协助下，或者通过使用同态加密技术，参与方 110 输入$\{[u_{i,j}]_0\}_{i\in[n_c],j\in[m_c]}$，参与方 120 输入$\{[u_{i,j}]_1\}_{i\in[n_c],j\in[m_c]}$和$\pi_1$。经过安全置换，参与方 110 得到数据集 112 的特征信息$u_{i,j}$的第一目标特征分享$\{[\delta_{i,j}]_0\}_{i\in[n_c],j\in[m_c]}$；参与方 120 得到数据集 112 的特征信息$u_{i,j}$的第二目标特征分享$\{[\delta_{i,j}]_1\}_{i\in[n_c],j\in[m_c]}$。特征信息$u_{i,j}$的第一目标特征分享和第二目标特征分享满足：$\pi_1\left(\{[u_{i,j}]_0 + [u_{i,j}]_1\}_{i\in[n_c],j\in[m_c]}\right) = \{[\delta_{i,j}]_0 + \delta_{i,j}]_1\}_{i\in[n_c],j\in[m_c]}$。

然后，参与方 110 可以使用特征信息$u_{i,j}$的第一目标特征分享$\{[\delta_{i,j}]_0\}_{i\in[n_c],j\in[m_c]}$和从参与方 120 接收到的特征信息$u_{i,j}$的第二特征分享$\{u''_{i,j}\}_{i\in[n_c],j\in[m_c]}$，计算$[\delta_{i,j}]_2 = [\delta_{i,j}]_0 + u''_{i,j}$。可以证明，$[\delta_{i,j}]_1 + [\delta_{i,j}]_2$等于数据集 112 中真实数据条目对应的特征信息。

进一步地，参与方 110 与参与方 120 执行针对数据集 122 的特征信息的第二轮安全置换（260）。在第二轮安全置换中，参与方 110 拥

有数据集 122 的特征信息$v_{i,j}$的第三特征分享$\{v'_{i,j}\}_{i\in[n_p],j\in[m_p]}$，参与方 120 拥有数据集 122 的特征信息$v_{i,j}$的第一特征分享$\{[v_{i,j}]_0\}_{i\in[n_p],j\in[m_p]}$。

在一些实施例中，参与方 110 还通过匹配数据集 112 的双重加密标识信息$\widetilde{Cid}_i$与数据集 122 的双重加密标识信息$\widetilde{Pid}_i$，来生成得到将双方数据集对齐（即交集数据条目都处于相同的位置）所需要的第二置换信息π_0。首先，参与方 110 持有数据集 112 的双重加密标识信息$\{\widetilde{Cid}_i\}_{i\in[n_c]}$与数据集 122 的双重加密标识信息$\{\widetilde{Pid}_i\}_{i\in[n_p]}$。参与方 110 使用双重加密标识信息$\{\widetilde{Pid}_i\}_{i\in[n_p]}$匹配$\{\widetilde{Cid}_i\}_{i\in[n_c]}$，以生成针对参与方 120 的加密标识信息$Pid'_i$对应的第二置换信息$\pi_0$。

在一些实施例中，首先，参与方 110 初始化n_p长度的置换向量$\pi_0 = \{-1\}^{n_p}$，$\varphi = \{0, 1, \ldots, n_p - 1\}$。参与方 110 遍历双重加密标识信息$\{\widetilde{Pid}_i\}_{i\in[n_p]}$。如果基于通过匹配确定数据集 112 中的第一数据条目和数据集 122 中的第二数据条目的标识信息（即，双重加密标识信息）相匹配，则生成的第二置换信息（π_0）包括对第一数据条目或第二数据条目的位置的索引。如果基于通过匹配确定第一数据条目和第二数据条目的标识信息不匹配，则生成第二置换信息（π_0）以包括伪索引。例如，对于每个$\widetilde{Pid}_i$，若存在$\widetilde{Cid}_k = \widetilde{Pid}_i$，则令$\pi_0[i] = k$，并将$k$从$\varphi$中删除$\varphi = \varphi - \{k\}$。否则，参与方 110 从$\varphi$中随机选取一个元素$k'$，令$\pi_0[i] = k'$，并$\varphi = \varphi - \{k'\}$。在这个过程中，参与方 110 会记录哪些位置是真实交集，用于在后续步骤中设置真实交集标识列。经过遍历，参与方 110 生成第二置换信息π_0。

这样，在第二轮安全置换中，参与方 110 拥有数据集 122 的特征信息$v_{i,j}$的第三特征分享$\{v'_{i,j}\}_{i\in[n_p],j\in[m_p]}$和第二置换信息$\pi_0$。在第二轮安全置换中，参与方 110 相当于安全置换协议中的 P0，参与方 120 相当于安全置换协议中的 P2。通过调用第二轮安全置换协议，可以调整第一交集中数据集 122 的特征分享，以获得与交集顺序对齐的数据集 122 的特征分享。

在一些实施例中，在第三方 P2 的协助下，或者通过使用同态加密技术，参与方 120 输入$\{v'_{i,j}\}_{i\in[n_p],j\in[m_p]}$和$\pi_0$，参与方 120 输入$\{[v_{i,j}]_0\}_{i\in[n_p],j\in[m_p]}$。经过安全置换，参与方 110 得到数据集 122 的特征信息$v_{i,j}$的第一目标特征分享$\{[\gamma_{i,j}]_0\}_{i\in[n_p],j\in[m_p]}$；参与方 120 得到数据集 122 的特征信息$v_{i,j}$的第二目标特征分享$\{[\gamma_{i,j}]_1\}_{i\in[n_p],j\in[m_p]}$。特征信息$v_{i,j}$的第一目标特征分享和第二目标特征分享满足：$\pi_0\left(\{v'_{i,j}+[v_{i,j}]_0\}_{i\in[n_p],j\in[m_p]}\right)=\{[\gamma_{i,j}]_0+\gamma_{i,j}]_1\}_{i\in[n_p],j\in[m_p]}$。可以证明，$[\gamma_{i,j}]_0+[\gamma_{i,j}]_1$等于数据集 122 中真实数据条目对应的特征信息。

在第一轮安全置换和第二轮安全置换后，参与方 110 基于所得到的数据集 112 的特征信息$u_{i,j}$的第一目标特征分享$[\delta_{i,j}]_0$和数据集 122 的特征信息$v_{i,j}$的第一目标特征分享$[\gamma_{i,j}]_0$来更新（270）第一交集。在一些实施例中，在更新后的第一交集中，数据集 112 的特征信息$u_{i,j}$的第二特征分享$u''_{i,j}$被更新为特征信息$u_{i,j}$的第二特征分享$u''_{i,j}$和第一目标特征分享$[\delta_{i,j}]_0$之和，即$[\delta_{i,j}]_2=[\delta_{i,j}]_0+u''_{i,j}$。在更新后的第一交集中，数据集 122 的特征信息$v_{i,j}$的第三特征分享$v'_{i,j}$被更新为特征信息$v_{i,j}$的第一目标特征分享$[\gamma_{i,j}]_0$。参与方 110 可以按行拼接$[\delta_{i,j}]_2$和$[\gamma_{i,j}]_0$，得到更新后的第一交集。

在一些实施例中，参与方 110 还设置针对更新后的第一交集中各个数据条目的匹配标记，其中双重加密标识信息匹配的数据条目的匹配标记被设置为第一值并且指示标识信息的真实匹配，双重加密标识信息不匹配的数据条目的匹配标记被设置为第二值并且指示标识信息的伪匹配。匹配标记的设置可以基于在生成第二置换信息π_0时所记录的匹配情况。在一些实施例中，第一值可以被设置为 1，第二值可以被设置为 0。

例如，参与方 110 可以在更新后的第一交集中额外设置匹配标记列，其中记录对应数据条目的匹配标记（也称为 is_real 标志位），用

于标识该数据条目是真实交集还是虚假填充的交集。参与方 110 会根据填充的实际情况将真实匹配交集的 is_real 标志位设置为 1，虚假匹配交集的 is_real 标志位设置为 0。

在参与方 120 侧，在第一轮安全置换和第二轮安全置换后，参与方 120 基于数据集 112 的特征信息$u_{i,j}$的第二目标特征分享$[\delta_{i,j}]_1$和数据集 122 的特征信息$v_{i,j}$的第一目标特征分享$[\gamma_{i,j}]_0$来生成（272）针对数据集 112 和数据集 122 的第二交集。例如，参与方 120 按行拼接$[\delta_{i,j}]_1$和$[\gamma_{i,j}]_1$，得到第二交集。第二交集中的数据条目不包括标识信息，并且特征信息$u_{i,j}$的第二目标特征分享$[\delta_{i,j}]_1$和特征信息$v_{i,j}$的第一目标特征分享$[\gamma_{i,j}]_0$按数据条目的粒度顺序对应。

在参与方 120 处，参与方 120 也类似设置第二交集的匹配标记。由于参与方 120 不能确定第二交集中数据条目的标识信息是否匹配，参与方 120 可以将所有数据条目的匹配标记设置为指示标识信息的伪匹配，即 is_real 标志位均设置为指示不相匹配，例如均设置为 0。

然后，参与方 110 基于更新后的第一交集，并且参与方 120 基于第二交集，执行（280）数据集 112 和数据集 122 的 MPC。

由于第一交集和第二交集中的数据条目还包括标识信息不匹配的数据条目，利用第一交集和第二交集来执行 MPC 后可以得到候选计算结果。参与方 110 可以基于所确定的第一交集中每对数据条目的候选计算结果和针对第一交集的匹配标记来确定 MPC 的目标计算结果。例如，如果第一交集的匹配标记中真索引对应的数据条目的匹配标志位被设置为 1，伪索引对应的数据条目的匹配标志位被设置为 0，参与方 110 可以基于第一交集中数据条目的候选计算结果与第一交集中该数据条目的匹配标记的相乘运算，生成目标计算结果。

类似地，参与方 120 可以基于所确定的第二交集中数据条目的候选计算结果和针对第二交集的匹配标记来确定 MPC 的目标计算结果。如果第二交集中数据条目的匹配标记被设置为 0，参与方 120 可以基于第二交集中数据条目的候选计算结果与第二交集中数据条目的匹配标记的相乘运算，生成目标计算结果。

因此，虽然第一交集和第二交集均不是真实交集结果，但在 MPC 运算后，通过调用 MPC 乘法将输出的候选计算结果与 is_real 标记位相乘，即可保留真实交集运算结果。

为更便于理解，图 4 示出了根据本公开的一些实施例的基于示例数据集的数据处理信令流 400 的流程图。图 4 的信令流 400 可以被认为是图 2 的信令流的一个示例。在图 4 中，给出了数据集 112 和 122 的具体示例，以参考该具体示例来描述各个加密阶段以及求交阶段。在图 4 的示例中，假设数据集 112 具有 5 条数据条目，数据集 122 具有 4 条数据条目。为了对齐数据条目数量，数据集 122 中填充有伪数据条目，由#表示。

如图 4 所示，在一次加密阶段，参与方 120 对数据集 122 中的标识信息进行随机化，即，使用第二加密密钥 rp 对标识信息执行一次加密；以及生成特征信息的第一特征分享和第三特征分享。参与方 120 在消息 1 中将数据集 122 的加密标识信息和第三特征分享（<[rp]ID, Enc(特征 2)>）402 发送给参与方 110。可以看出，在消息 1 中，数据集 122 中标识信息和特征信息被加密。参与方 120 保留数据集 122 的特征信息的第一特征分享 405。

类似地，在一次加密阶段，参与方 110 对数据集 112 中的标识信息进行随机化，即，使用第一加密密钥 rc 对标识信息执行一次加密；以及生成特征信息的第一特征分享和第三特征分享。参与方 110 在消息 2 中将数据集 112 的加密标识信息和第三特征分享(<[rp]ID, Enc(特征 1)>）414 发送给参与方 120。可以看出，在消息 2 中，数据集 112 中标识信息和特征信息被加密。参与方 110 保留数据集 112 的特征信息的第一特征分享 410，且参与方 110 知道自身数据集中这些第一特征分享 410 与标识信息 412 之间的对应关系。

在二次加密阶段，参与方 120 执行操作 420，包括对接收到的参与方 110 的数据集 112 的加密标识信息和第三特征分享（<[rc]ID, Enc(特征 1)>）执行乱序处理；利用第二加密密钥 rp 对加密标识信息[rc]ID 执行二次加密，得到双重加密标识信息[rp] [rc]ID；以及对第三

特征分享 Enc(特征 1) $u'_{i,j}$执行秘密拆分，得到第四特征分享$[u_{i,j}]_1$和第二特征分享$u''_{i,j}$，即$u''_{i,j} = u'_{i,j} - [u_{i,j}]_1$。参与方 120 使用第一置换信息$\pi_1$ 434 来扰乱数据集 112 的双重加密标识信息和第四特征分享$u''_{i,j}$组成的集合，得到扰乱后的集合 430。参与方 120 在扰乱后的集合 430 中计算第二特征分享$u''_{i,j}$，并在消息 3 中将集合 435 发送给参与方 110。集合 435 包括数据集 112 的双重加密标识信息和第二特征分享$u''_{i,j}$。

类似的，在二次加密阶段，参与方 110 执行操作 415，包括对接收到的参与方 120 的数据集 122 的加密标识信息和第三特征分享（<[rp]ID, Enc(特征 2)>）执行乱序处理；利用第一加密密钥 rc 对加密标识信息[rp]ID 执行二次加密，得到双重加密标识信息[rc] [rp]ID。这样，参与方 110 接收到的集合 402 称为集合 422，包括数据集 122 的双重加密标识信息[rc] [rp]ID 和第三特征分享。

参与方 110 通过匹配数据集 112 的双重加密标识信息[rp] [rc]ID 和数据集 122 的双重加密标识信息[rc] [rp]ID，确定第二置换信息π_0 424。参与方 110 还可以确定第一交集 426。在确定第一交集 426 时，交集中数据条目的顺序保持与消息 3 一致。

参与方 110 与参与方 120 执行第一轮安全置换 450，以同步参与方 110 的数据集 112 的特征信息。在第一轮安全置换 450 中，参与方 110 输入数据集 112 的第一特征分享 410（其对齐到标识信息 412）；参与方 120 输入数据集 112 的第四特征分享 438 和第一置换信息π_1 434，第四特征分享 438 是未被第一置换信息π_1 434 扰乱的特征分享。为执行第一轮安全置换 450，参与方 120 还可以获得置换信息 432，例如可以从第三方 P2 获得。

经过第一轮安全置换 450，参与方 110 得到数据集 112 的特征信息的第一目标特征分享$[\delta_{i,j}]_0$ 452，参与方 120 得到数据集 112 的特征信息的第二目标特征分享$[\delta_{i,j}]_1$ 454。参与方 110 可以确定数据集 112 的特征信息的第一目标特征分享$[\delta_{i,j}]_0$ 452 与标识信息 456 的对应关系。

接着，参与方 110 与参与方 120 执行第一轮安全置换 460，以同步参与方 120 的数据集 122 的特征信息。在第一轮安全置换 460 中，参与方 110 输入数据集 122 的第三特征分享 462 和第二置换信息π_0 424；参与方 120 输入数据集 122 的第一特征分享 405。参与方 110 可以获知数据集 122 的第三特征分享 462 与第一交集中的标识信息 464 的对应关系。为执行第二轮安全置换 460，参与方 110 还可以获得置换信息 425，例如可以从第三方 P2 获得。

经过第二轮安全置换 460，参与方 110 得到数据集 122 的特征信息的第一目标特征分享$[\gamma_{i,j}]_0$ 466，参与方 120 得到数据集 122 的特征信息的第二目标特征分享$[\gamma_{i,j}]_1$ 468。参与方 110 可以确定数据集 122 的特征信息的第一目标特征分享$[\gamma_{i,j}]_0$ 466 与标识信息 472 的对应关系。

基于数据集 112 的特征信息的第一目标特征分享$[\delta_{i,j}]_0$ 452 和数据集 122 的特征信息的第一目标特征分享$[\gamma_{i,j}]_0$ 466，参与方 110 更新第一交集 426，得到更新后的第一交集 474。基于数据集 112 的特征信息的第二目标特征分享$[\delta_{i,j}]_1$ 454 和数据集 122 的特征信息的第二目标特征分享$[\gamma_{i,j}]_1$ 468，参与方 120 生成第二交集 476。

此外，参与方 110 还可以设置第一交集 474 中各个数据条目的匹配标记（is_real 标记位）。参与方 120 也可以设置第二交集 476 的匹配标记（is_real 标记位）。参与方 110 可以根据双重标识信息匹配的实际情况将真实交集的 is_real 标记位设置为 1，虚假交集的 is_real 标记位设置为 0。而参与方 120 则将所有的 is_real 标记位均设置为 0。在基于第一交集和第二交集执行 MPC 运算时，可以调用 MPC 乘法将 MPC 运算的候选结果与 is_real 标记位相乘，即可保留真实交集运算结果。

根据本公开的实施例，可以支持在不暴露双方数据集的真实信息情况下，支持获得 MPC 协议所需的特征分享，以进行 MPC 运算。通过采用安全置换技术，特征分享和交集匹配的效率提高，双方需要缓存的数据量减小。在一些实施例中，使用 ECDH 和安全置换协议，计

算、通信高效。而且，在整个交互过程中，可以不向其中一个参与方泄露交集的规模，确保数据安全性。

图 5 示出了根据本公开的一些实施例的在第一参与方处实现的数据处理方法 500 的流程图。方法 500 例如可以被实现 MPC 的第一参与方，例如图 1 的参与方 110。为便于讨论，将参考图 1 的环境 100 来描述方法 500。

在框 510，参与方 110 获取第一参与方的第一数据集中各个数据条目的第一双重加密标识信息以及第一特征信息的第一特征分享和第二特征分享，以及 MPC 的第二参与方的第二数据集中各个数据条目的第二双重加密标识信息和第二特征信息的第三特征分享。

在框 520，参与方 110 通过匹配第一双重加密标识信息与第二双重加密标识信息，确定第一数据集和第二数据集的第一交集，第一交集中的数据条目包括相匹配的标识信息以及标识信息所标识的第一特征信息的第二特征分享和第二特征信息的第三特征分享。

在框 530，参与方 110 利用第一特征信息的第一特征分享来与第二参与方执行针对第一特征信息的第一轮安全置换，得到第一特征信息的第一目标特征分享。

在框 540，参与方 110 利用第二特征信息的第三特征分享来与第二参与方执行针对第二特征信息的第二轮安全置换，得到第二特征信息的第一目标特征分享。

在框 550，参与方 110 基于第一特征信息的第一目标特征分享和第二特征信息的第一目标特征分享来更新第一交集。

在框 560，参与方 110 基于更新后的第一交集与第二参与方执行 MPC。

在一些实施例中，在获取第一双重加密标识信息以及第一特征信息的第一特征分享之前，方法 500 还包括：对第一数据集中各个数据条目的第一标识信息进行加密，得到第一加密标识信息；基于第一特征信息的第一特征分享，生成第一特征信息的第三特征分享；以及向第二参与方发送第一加密标识信息和第一特征信息的第三特征分享，

以用于第二参与方生成和向第一参与方发送第一双重加密标识信息以及第一特征信息的第一特征分享。

在一些实施例中，对第一标识信息进行加密包括：利用第一加密密钥对第一数据集中各个数据条目的第一标识信息进行加密，得到第一加密标识信息。第一双重加密标识信息由第二参与方利用第二加密密钥对第一标识信息加密后得到。

在一些实施例中，获取第二双重加密标识信息包括：从第二参与方接收第二参与方的第二数据集中各个数据条目的第二加密标识信息和第二特征信息的第三特征分享，第二加密标识信息由第二参与方利用第二加密密钥加密得到；以及利用第一加密密钥对第二加密标识信息执行二次加密，得到第二双重加密标识信息。

在一些实施例中，获取第一双重加密标识信息和第一特征信息的第二特征分享包括：从第二参与方接收第一双重加密标识信息和第一特征信息的第二特征分享，第一双重加密标识信息与第一特征信息的第二特征分享之间的对应关系由第二参与方基于第一置换信息置换。

在一些实施例中，在第一轮安全置换中第二参与方至少使用第一置换信息。

在一些实施例中，与第二参与方执行第二轮安全置换包括：基于第一双重加密标识信息与第二双重加密标识信息之间的匹配，来生成针对第二参与方的第二加密标识信息对应的第二置换信息；以及利用第二特征信息的第三特征分享和第二置换信息来与第二参与方执行第二轮安全置换。

在一些实施例中，生成第二置换信息包括：如果基于匹配确定第一数据集中的第一数据条目和第二数据集中的第二数据条目的双重加密标识信息相匹配，则生成第二置换信息以包括对第一数据条目或第二数据条目的位置的索引；以及如果基于匹配确定第一数据条目和第二数据条目的双重加密标识信息不匹配，则生成第二置换信息以包括伪索引。

在一些实施例中，更新第一交集包括：更新第一交集，在更新后

的第一交集中第一特征信息的第二特征分享被更新为第一特征信息的第二特征分享和第一目标特征分享之和，并且第二特征信息的第三特征分享被更新为第二特征信息的第一目标特征分享。

在一些实施例中，在第一轮安全置换之前，方法 500 还包括：如果第一数据集的数据条目数量和第二数据集的数据条目数量不相等，则通过填充伪数据条目来使第一数据集的数据条目数目等于第二数据集的数据条目数量。

在一些实施例中，方法 500 还包括：设置针对更新后的第一交集中各个数据条目的匹配标记，其中双重加密标识信息匹配的数据条目的匹配标记被设置为第一值并且指示标识信息的真实匹配，双重加密标识信息不匹配的数据条目的匹配标记被设置为第二值并且指示标识信息的伪匹配。

在一些实施例中，执行 MPC 包括：基于更新后的第一交集来与第二参与方执行 MPC，得到针对更新后的第一交集中各个数据条目的候选计算结果；以及基于候选计算结果与更新后的第一交集中各个数据条目的匹配标记确定 MPC 的目标计算结果。

在一些实施例中，第一值被设置为 1，第二值被设置为 0。确定目标计算结果包括：至少基于候选计算结果与更新后的第一交集中各个数据条目的匹配标记的相乘运算，生成 MPC 的目标计算结果。

图 6 示出了根据本公开的一些实施例的在第二参与方处实现的数据处理方法的流程图。方法 600 例如可以被实现图 1 的参与方 120。为便于讨论，将参考图 1 的环境 100 来描述方法 600。

在框 610，参与方 120 获取 MPC 的第一参与方的第一数据集中各个数据条目的第一特征信息的第四特征分享和针对第一数据集的第一置换信息，以及第二参与方的第二数据集中各个数据条目的第二特征信息的第一特征分享。

在框 620，参与方 120 利用第一特征信息的第四特征分享和第一置换信息来与第一参与方执行针对第一特征信息的第一轮安全置换，得到第一特征信息的第二目标特征分享。

在框 630，参与方 120 利用第二特征信息的第一特征分享来与第一参与方执行针对第二特征信息的第二轮安全置换，得到第二特征信息的第二目标特征分享。

在框 640，参与方 120 基于第一特征信息的第二目标特征分享和第二特征信息的第一目标特征分享来生成针对第一数据集和第二数据集的第二交集。

在框 650，参与方 120 基于第二交集与第一参与方执行 MPC。

在一些实施例中，方法 600 还包括：对第二数据集中各个数据条目的第二标识信息进行加密，得到第二加密标识信息；基于第二特征信息的第一特征分享，生成第二特征信息的第三特征分享；以及向第一参与方发送第二加密标识信息和第二特征信息的第三特征分享，以用于第一参与方确定和向第二参与方发送第二特征信息的第一特征分享。

在一些实施例中，在执行第一轮安全置换之前，方法 600 还包括：从第一参与方接收第一加密标识信息和第一特征信息的第三特征分享；对第一加密标识信息执行二次加密，得到第一双重加密标识信息；基于第一特征信息的第三特征分享和第四特征分享，生成第一特征信息的第二特征分享；通过利用第一置换信息来置换第一双重加密标识信息与第一特征信息的第二特征分享之间的对应关系；以及将置换后的第一双重加密标识信息和第一特征信息的第二特征分享发送给第一参与方。

在一些实施例中，第一加密标识信息由第一参与方利用第一加密密钥进行加密，并且其中执行二次加密包括：利用第二加密密钥对第一标识信息进行加密，得到第一双重加密标识信息。

在一些实施例中，第二交集中的数据条目不包括标识信息，并且第一特征信息的第二目标特征分享和第二特征信息的第一目标特征分享按数据条目的粒度顺序对应。

在一些实施例中，执行 MPC 包括：设置针对第二交集中各个数据条目的匹配标记，匹配标记被设置为指示标识信息的伪匹配；基于

第二交集来与第一参与方执行 MPC，得到针对第二交集中各个数据条目的候选计算结果；以及基于候选计算结果与第二交集中各个数据条目的匹配标记来确定 MPC 的目标计算结果。

在一些实施例中，针对第二交集中各个数据条目的匹配标记被设置为 0。确定目标计算结果包括：至少基于候选计算结果与针对第二交集中各个数据条目的匹配标记的相乘运算，生成 MPC 的目标计算结果。

图 7 示出了根据本公开的一些实施例的在第一参与方处实现的数据处理装置 700 的示意性结构框图。装置 700 可以被实现为或者被包括在参与方 110 中。装置 700 中的各个模块/组件可以由硬件、软件、固件或者它们的任意组合来实现。

如图所示，装置 700 包括信息获取模块 710，被配置为获取第一参与方的第一数据集中各个数据条目的第一双重加密标识信息以及第一特征信息的第一特征分享和第二特征分享，以及 MPC 的第二参与方的第二数据集中各个数据条目的第二双重加密标识信息和第二特征信息的第三特征分享。装置 700 还包括第一交集确定模块 720，被配置为通过匹配第一双重加密标识信息与第二双重加密标识信息，确定第一数据集和第二数据集的第一交集，第一交集中的数据条目包括相匹配的标识信息以及标识信息所标识的第一特征信息的第二特征分享和第二特征信息的第三特征分享。装置 700 还包括第一安全置换模块 730，被配置为利用第一特征信息的第一特征分享来与第二参与方执行针对第一特征信息的第一轮安全置换，得到第一特征信息的第一目标特征分享。装置 700 还包括第二安全置换模块 740，被配置为利用第二特征信息的第三特征分享来与第二参与方执行针对第二特征信息的第二轮安全置换，得到第二特征信息的第一目标特征分享。

装置 700 还包括交集更新模块 750，被配置为基于第一特征信息的第一目标特征分享和第二特征信息的第一目标特征分享来更新第一交集；以及 MPC 执行模块 760，被配置为基于更新后的第一交集与第二参与方执行 MPC。

在一些实施例中，装置 700 还包括：一次加密模块，被配置为在获取第一双重加密标识信息以及第一特征信息的第一特征分享之前，对第一数据集中各个数据条目的第一标识信息进行加密，得到第一加密标识信息；特征分享生成模块，被配置为基于第一特征信息的第一特征分享，生成第一特征信息的第三特征分享；以及特征分享发送模块，被配置为向第二参与方发送第一加密标识信息和第一特征信息的第三特征分享，以用于第二参与方生成和向第一参与方发送第一双重加密标识信息以及第一特征信息的第一特征分享。

在一些实施例中，一次加密模块被配置为：利用第一加密密钥对第一数据集中各个数据条目的第一标识信息进行加密，得到第一加密标识信息。第一双重加密标识信息由第二参与方利用第二加密密钥对第一标识信息加密后得到。

在一些实施例中，信息获取模块 710 包括：第一信息接收模块，被配置为从第二参与方接收第二参与方的第二数据集中各个数据条目的第二加密标识信息和第二特征信息的第三特征分享，第二加密标识信息由第二参与方利用第二加密密钥加密得到；以及二次加密模块，被配置为利用第一加密密钥对第二加密标识信息执行二次加密，得到第二双重加密标识信息。

在一些实施例中信息获取模块 710 包括：第二信息接收模块，被配置为从第二参与方接收第一双重加密标识信息和第一特征信息的第二特征分享，第一双重加密标识信息与第一特征信息的第二特征分享之间的对应关系由第二参与方基于第一置换信息置换。

在一些实施例中，在第一轮安全置换中第二参与方至少使用第一置换信息。

在一些实施例中，第二安全置换模块 740 包括：置换信息生成模块，被配置为基于第一双重加密标识信息与第二双重加密标识信息之间的匹配，来生成针对第二参与方的第二加密标识信息对应的第二置换信息；以及安全执行模块，被配置为利用第二特征信息的第三特征分享和第二置换信息来与第二参与方执行第二轮安全置换。

在一些实施例中，置换信息生成模块被配置为：如果基于匹配确定第一数据集中的第一数据条目和第二数据集中的第二数据条目的双重加密标识信息相匹配，则生成第二置换信息以包括对第一数据条目或第二数据条目的位置的索引；以及如果基于匹配确定第一数据条目和第二数据条目的双重加密标识信息不匹配，则生成第二置换信息以包括伪索引。

在一些实施例中，交集更新模块 750 被配置为：更新第一交集，在更新后的第一交集中第一特征信息的第二特征分享被更新为第一特征信息的第二特征分享和第一目标特征分享之和，并且第二特征信息的第三特征分享被更新为第二特征信息的第一目标特征分享。

在一些实施例中，在第一轮安全置换之前，装置 700 还包括：填充模块，被配置为如果第一数据集的数据条目数量和第二数据集的数据条目数量不相等，则通过填充伪数据条目来使第一数据集的数据条目数目等于第二数据集的数据条目数量。

在一些实施例中，装置 700 还包括：标记设置模块，被配置为设置针对更新后的第一交集中各个数据条目的匹配标记，其中双重加密标识信息匹配的数据条目的匹配标记被设置为第一值并且指示标识信息的真实匹配，双重加密标识信息不匹配的数据条目的匹配标记被设置为第二值并且指示标识信息的伪匹配。

在一些实施例中，MPC 执行模块 760 包括：候选结果确定模块，被配置为基于更新后的第一交集来与第二参与方执行 MPC，得到针对更新后的第一交集中各个数据条目的候选计算结果；以及目标结果确定模块，被配置为基于候选计算结果与更新后的第一交集中各个数据条目的匹配标记确定 MPC 的目标计算结果。

在一些实施例中，第一值被设置为 1，第二值被设置为 0。目标结果确定模块被配置为：至少基于候选计算结果与更新后的第一交集中各个数据条目的匹配标记的相乘运算，生成 MPC 的目标计算结果。

图 8 示出了根据本公开的一些实施例的在第二参与方处实现的数据处理装置 800 的示意性结构框图。装置 800 可以被实现为或者被包

括在参与方 120 中。装置 800 中的各个模块/组件可以由硬件、软件、固件或者它们的任意组合来实现。

如图所示，装置 800 包括信息获取模块 810，被配置为获取 MPC 的第一参与方的第一数据集中各个数据条目的第一特征信息的第四特征分享和针对第一数据集的第一置换信息，以及第二参与方的第二数据集中各个数据条目的第二特征信息的第一特征分享。

装置 800 还包括第一安全置换模块 820，被配置为利用第一特征信息的第四特征分享和第一置换信息来与第一参与方执行针对第一特征信息的第一轮安全置换，得到第一特征信息的第二目标特征分享。

装置 800 还包括第二安全置换模块 830，被配置为利用第二特征信息的第一特征分享来与第一参与方执行针对第二特征信息的第二轮安全置换，得到第二特征信息的第二目标特征分享。

装置 800 还包括第二交集生成模块 840，被配置为基于第一特征信息的第二目标特征分享和第二特征信息的第一目标特征分享来生成针对第一数据集和第二数据集的第二交集。装置 800 还包括 MPC 执行模块 850，被配置为基于第二交集与第一参与方执行 MPC。

在一些实施例中，装置 800 还包括：一次加密模块，被配置为对第二数据集中各个数据条目的第二标识信息进行加密，得到第二加密标识信息；第一特征分享生成模块，被配置为基于第二特征信息的第一特征分享，生成第二特征信息的第三特征分享；以及特征分享发送模块，被配置为向第一参与方发送第二加密标识信息和第二特征信息的第三特征分享，以用于第一参与方确定和向第二参与方发送第二特征信息的第一特征分享。

在一些实施例中，装置 800 还包括：特征分享接收模块，被配置为在执行第一轮安全置换之前，从第一参与方接收第一加密标识信息和第一特征信息的第三特征分享；二次加密模块，被配置为对第一加密标识信息执行二次加密，得到第一双重加密标识信息；第一特征分享生成模块，被配置为基于第一特征信息的第三特征分享和第四特征分享，生成第一特征信息的第二特征分享；置换模块，被配置为通过

利用第一置换信息来置换第一双重加密标识信息与第一特征信息的第二特征分享之间的对应关系；以及信息发送模块，被配置为将置换后的第一双重加密标识信息和第一特征信息的第二特征分享发送给第一参与方。

在一些实施例中，第一加密标识信息由第一参与方利用第一加密密钥进行加密，并且二次加密模块被配置为：利用第二加密密钥对第一标识信息进行加密，得到第一双重加密标识信息。

在一些实施例中，第二交集中的数据条目不包括标识信息，并且第一特征信息的第二目标特征分享和第二特征信息的第一目标特征分享按数据条目的粒度顺序对应。

在一些实施例中，MPC 执行模块 850 包括：标记设置模块，被配置为设置针对第二交集中各个数据条目的匹配标记，匹配标记被设置为指示标识信息的伪匹配；候选结果确定模块，被配置为基于第二交集来与第一参与方执行 MPC，得到针对第二交集中各个数据条目的候选计算结果；以及目标结果确定模块，被配置为基于候选计算结果与第二交集中各个数据条目的匹配标记来确定 MPC 的目标计算结果。

在一些实施例中，针对第二交集中各个数据条目的匹配标记被设置为 0。目标结果确定模块被配置为：至少基于候选计算结果与针对第二交集中各个数据条目的匹配标记的相乘运算，生成 MPC 的目标计算结果。

图 9 示出了可以实施本公开的一个或多个实施例的电子设备 900 的框图。应当理解，图 9 所示出的电子设备 900 仅仅是示例性的，而不应当构成对本文所描述的实施例的功能和范围的任何限制。图 9 所示出的电子设备 900 可以用于实现图 1 的参与方 110 或参与方 120，图 7 所述的装置 700，或图 8 所述的装置 800。

如图 9 所示，电子设备 900 是通用计算设备的形式。电子设备 900 的组件可以包括但不限于一个或多个处理器或处理单元 910、存储器 920、存储设备 930、一个或多个通信单元 940、一个或多个输入设备 950 以及一个或多个输出设备 960。处理单元 910 可以是实际或虚拟

处理器并且能够根据存储器 920 中存储的程序来执行各种处理。在多处理器系统中，多个处理单元并行执行计算机可执行指令，以提高电子设备 900 的并行处理能力。

电子设备 900 通常包括多个计算机存储介质。这样的介质可以是电子设备 900 可访问的任何可以获得的介质，包括但不限于易失性和非易失性介质、可拆卸和不可拆卸介质。存储器 920 可以是易失性存储器（例如寄存器、高速缓存、随机访问存储器（RAM））、非易失性存储器（例如，只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、闪存）或它们的某种组合。存储设备 930 可以是可拆卸或不可拆卸的介质，并且可以包括机器可读介质，诸如闪存驱动、磁盘或者任何其他介质，其可以能够用于存储信息和/或数据（例如用于训练的训练数据）并且可以在电子设备 900 内被访问。

电子设备 900 可以进一步包括另外的可拆卸/不可拆卸、易失性/非易失性存储介质。尽管未在图 9 中示出，可以提供用于从可拆卸、非易失性磁盘（例如“软盘”）进行读取或写入的磁盘驱动和用于从可拆卸、非易失性光盘进行读取或写入的光盘驱动。在这些情况中，每个驱动可以由一个或多个数据介质接口被连接至总线（未示出）。存储器 920 可以包括计算机程序产品 925，其具有一个或多个程序模块，这些程序模块被配置为执行本公开的各种实施例的各种方法或动作。

通信单元 940 实现通过通信介质与其他电子设备进行通信。附加地，电子设备 900 的组件的功能可以以单个计算集群或多个计算机器来实现，这些计算机器能够通过通信连接进行通信。因此，电子设备 900 可以使用与一个或多个其他服务器、网络个人计算机（PC）或者另一个网络节点的逻辑连接来在联网环境中进行操作。

输入设备 950 可以是一个或多个输入设备，例如鼠标、键盘、追踪球等。输出设备 960 可以是一个或多个输出设备，例如显示器、扬声器、打印机等。电子设备 900 还可以根据需要通过通信单元 940 与一个或多个外部设备（未示出）进行通信，外部设备诸如存储设备、

显示设备等，与一个或多个使得用户与电子设备900交互的设备进行通信，或者与使得电子设备900与一个或多个其他电子设备通信的任何设备（例如，网卡、调制解调器等）进行通信。这样的通信可以经由输入/输出（I/O）接口（未示出）来执行。

根据本公开的示例性实施例，提供了一种计算机可读存储介质，其上存储有计算机可执行指令，其中计算机可执行指令被处理器执行以实现上文描述的方法。根据本公开的示例性实施例，还提供了一种计算机程序产品，计算机程序产品被有形地存储在非瞬态计算机可读介质上并且包括计算机可执行指令，而计算机可执行指令被处理器执行以实现上文描述的方法。

这里参照根据本公开实现的方法、装置、设备和计算机程序产品的流程图和/或框图描述了本公开的各个方面。应当理解，流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合，都可以由计算机可读程序指令实现。

这些计算机可读程序指令可以提供给通用计算机、专用计算机或其他可编程数据处理装置的处理单元，从而生产出一种机器，使得这些指令在通过计算机或其他可编程数据处理装置的处理单元执行时，产生了实现流程图和/或框图中的一个或多个方框中规定的功能/动作的装置。也可以把这些计算机可读程序指令存储在计算机可读存储介质中，这些指令使得计算机、可编程数据处理装置和/或其他设备以特定方式工作，从而，存储有指令的计算机可读介质则包括一个制造品，其包括实现流程图和/或框图中的一个或多个方框中规定的功能/动作的各个方面的指令。

可以把计算机可读程序指令加载到计算机、其他可编程数据处理装置、或其他设备上，使得在计算机、其他可编程数据处理装置或其他设备上执行一系列操作步骤，以产生计算机实现的过程，从而使得在计算机、其他可编程数据处理装置、或其他设备上执行的指令实现流程图和/或框图中的一个或多个方框中规定的功能/动作。

附图中的流程图和框图显示了根据本公开的多个实现的系统、方

法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或指令的一部分，模块、程序段或指令的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

以上已经描述了本公开的各实现，上述说明是示例性的，并非穷尽性的，并且也不限于所公开的各实现。在不偏离所说明的各实现的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。本文中所用术语的选择，旨在最好地解释各实现的原理、实际应用或对市场中的技术的改进，或者使本技术领域的其他普通技术人员能理解本文公开的各个实施例。

权利要求书

1. 一种数据处理方法，所述方法被实现在多方安全计算 MPC 的第一参与方（C），所述方法包括:

获取所述第一参与方（C）的第一数据集中各个数据条目的第一双重加密标识信息（$\widetilde{Cid}_i$）以及第一特征信息（$u_{i,j}$）的第一特征分享（$[u_{i,j}]_0$）和第二特征分享（$u''_{i,j}$），以及所述 MPC 的第二参与方（P）的第二数据集中各个数据条目的第二双重加密标识信息（$\widetilde{Pid}_i$）和第二特征信息（$v_{i,j}$）的第三特征分享（$v'_{i,j}$）；

通过匹配所述第一双重加密标识信息（$\widetilde{Cid}_i$）与所述第二双重加密标识信息（$\widetilde{Pid}_i$），确定所述第一数据集和所述第二数据集的第一交集，所述第一交集中的数据条目包括相匹配的标识信息以及标识信息所标识的所述第一特征信息（$u_{i,j}$）的第二特征分享（$u''_{i,j}$）和所述第二特征信息（$v_{i,j}$）的第三特征分享（$v'_{i,j}$）；

利用所述第一特征信息（$u_{i,j}$）的所述第一特征分享（$[u_{i,j}]_0$）来与所述第二参与方（P）执行针对所述第一特征信息的第一轮安全置换，得到所述第一特征信息（$u_{i,j}$）的第一目标特征分享（$[\delta_{i,j}]_0$）；

利用所述第二特征信息（$v_{i,j}$）的所述第三特征分享（$v'_{i,j}$）来与所述第二参与方（P）执行针对所述第二特征信息的第二轮安全置换，得到所述第二特征信息（$v_{i,j}$）的第一目标特征分享（$[\gamma_{i,j}]_0$）；

基于所述第一特征信息（$u_{i,j}$）的第一目标特征分享（$[\delta_{i,j}]_0$）和所述第二特征信息（$v_{i,j}$）的第一目标特征分享（$[\gamma_{i,j}]_0$）来更新所述第一交集；以及

基于更新后的第一交集与所述第二参与方执行所述 MPC。

2. 根据权利要求 1 所述的方法，其中获取所述第一双重加密标识信息（$\widetilde{Cid}_i$）和所述第一特征信息（$u_{i,j}$）的所述第二特征分享（$u''_{i,j}$）包括:

从所述第二参与方（P）接收所述第一双重加密标识信息（$\widetilde{Cid}_i$）和所述第一特征信息（$u_{i,j}$）的所述第二特征分享（$u''_{i,j}$），所述第一

双重加密标识信息（$\widetilde{Cid}_i$）与所述第一特征信息（$u_{i,j}$）的所述第二特征分享（$u''_{i,j}$）之间的对应关系由所述第二参与方（P）基于第一置换信息（π_1）置换。

3. 根据权利要求 2 所述的方法，其中在所述第一轮安全置换中所述第二参与方（P）至少使用所述第一置换信息（π_1）。

4. 根据权利要求 1 所述的方法，其中与所述第二参与方（P）执行所述第二轮安全置换包括：

基于所述第一双重加密标识信息（$\widetilde{Cid}_i$）与所述第二双重加密标识信息（$\widetilde{Pid}_i$）之间的匹配，来生成针对所述第二参与方（P）的所述第二加密标识信息（Pid'_i）对应的第二置换信息（π_0）；以及

利用所述第二特征信息（$v_{i,j}$）的所述第三特征分享（$v'_{i,j}$）和所述第二置换信息（π_0）来与所述第二参与方（P）执行第二轮安全置换。

5. 根据权利要求 4 所述的方法，其中生成所述第二置换信息（π_0）包括：

如果基于所述匹配确定所述第一数据集中的第一数据条目和所述第二数据集中的第二数据条目的双重加密标识信息相匹配，则生成所述第二置换信息（π_0）以包括对所述第一数据条目或所述第二数据条目的位置的索引；以及

如果基于所述匹配确定所述第一数据条目和所述第二数据条目的双重加密标识信息不匹配，则生成所述第二置换信息（π_0）以包括伪索引。

6. 根据权利要求 1 所述的方法，其中更新所述第一交集包括：

更新所述第一交集，在更新后的第一交集中所述第一特征信息（$u_{i,j}$）的第二特征分享（$u''_{i,j}$）被更新为所述第一特征信息的所述第二特征分享（$u''_{i,j}$）和所述第一目标特征分享（$[\delta_{i,j}]_0$）之和，并且所述第二特征信息的第三特征分享（$v'_{i,j}$）被更新为所述第二特征信息（$v_{i,j}$）的第一目标特征分享（$[\gamma_{i,j}]_0$）。

7. 根据权利要求 5 所述的方法，还包括：

设置针对所述更新后的第一交集中各个数据条目的匹配标记，其中双重加密标识信息匹配的数据条目的匹配标记被设置为第一值并且指示标识信息的真实匹配，双重加密标识信息不匹配的数据条目的匹配标记被设置为第二值并且指示标识信息的伪匹配。

8. 根据权利要求 7 所述的方法，其中执行所述 MPC 包括：

基于更新后的第一交集来与所述第二参与方执行所述 MPC，得到针对所述更新后的第一交集中各个数据条目的候选计算结果；以及

基于所述候选计算结果与所述更新后的第一交集中各个数据条目的匹配标记确定所述 MPC 的目标计算结果。

9. 根据权利要求 8 所述的方法，其中所述第一值被设置为 1，所述第二值被设置为 0，并且其中确定所述目标计算结果包括：

至少基于所述候选计算结果与所述更新后的第一交集中各个数据条目的匹配标记的相乘运算，生成所述 MPC 的目标计算结果。

10. 一种用于数据处理的方法，所述方法被实现在多方安全计算 MPC 的第二参与方（P），所述方法包括：

获取所述 MPC 的第一参与方（C）的第一数据集中各个数据条目的所述第一特征信息（$u_{i,j}$）的第四特征分享（$[u_{i,j}]_1$）和针对所述第一数据集的第一置换信息（π_1），以及所述第二参与方（P）的第二数据集中各个数据条目的第二特征信息($v_{i,j}$)的第一特征分享($[v_{i,j}]_0$)；

利用所述第一特征信息（$u_{i,j}$）的第四特征分享（$[u_{i,j}]_1$）和所述第一置换信息（π_1）来与所述第一参与方（C）执行针对所述第一特征信息的第一轮安全置换，得到所述第一特征信息($u_{i,j}$)的第二目标特征分享（$[\delta_{i,j}]_1$）；

利用所述第二特征信息（$v_{i,j}$）的第一特征分享（$[v_{i,j}]_0$）来与所述第一参与方（C）执行针对所述第二特征信息的第二轮安全置换，得到所述第二特征信息（$v_{i,j}$）的第二目标特征分享（$[\gamma_{i,j}]_1$）；

基于所述第一特征信息（$u_{i,j}$）的第二目标特征分享（$[\delta_{i,j}]_1$）和所述第二特征信息（$v_{i,j}$）的第一目标特征分享（$[\gamma_{i,j}]_0$）来生成针对所述第一数据集和所述第二数据集的第二交集；以及

基于所述第二交集与所述第一参与方执行所述 MPC。

11. 根据权利要求 10 所述的方法，在执行所述第一轮安全置换之前，所述方法还包括：

从所述第一参与方（C）接收所述第一加密标识信息（$\widetilde{Cid}_i$）和所述第一特征信息（$u_{i,j}$）的第三特征分享（$u'_{i,j}$）；

对所述第一加密标识信息（$\widetilde{Cid}_i$）执行二次加密，得到所述第一双重加密标识信息（$\widetilde{Cid}_i$）；

基于所述第一特征信息（$u_{i,j}$）的第三特征分享（$u'_{i,j}$）和所述第四特征分享（$[u_{i,j}]_1$），生成所述第一特征信息（$u_{i,j}$）的所述第二特征分享（$u''_{i,j}$）；

通过利用第一置换信息（π_1）来置换所述第一双重加密标识信息（$\widetilde{Cid}_{i,j}$）与所述第一特征信息（$u_{i,j}$）的所述第二特征分享（$u''_{i,j}$）之间的对应关系；以及

将置换后的所述第一双重加密标识信息（$\widetilde{Cid}_i$）和所述第一特征信息（$u_{i,j}$）的所述第二特征分享（$u''_{i,j}$）发送给所述第一参与方（C）。

12. 根据权利要求 11 所述的方法，其中所述第二交集中的数据条目不包括标识信息，并且所述第一特征信息（$u_{i,j}$）的第二目标特征分享（$[\delta_{i,j}]_1$）和所述第二特征信息（$v_{i,j}$）的第一目标特征分享（$[\gamma_{i,j}]_0$）按数据条目的粒度顺序对应。

13. 根据权利要求 12 所述的方法，其中执行所述 MPC 包括：

设置针对所述第二交集中各个数据条目的匹配标记，所述匹配标记被设置为指示标识信息的伪匹配；

基于所述第二交集来与所述第一参与方执行所述 MPC，得到针对所述第二交集中各个数据条目的候选计算结果；以及

基于所述候选计算结果与所述第二交集中各个数据条目的匹配标记来确定所述 MPC 的目标计算结果。

14. 根据权利要求 13 所述的方法，其中针对所述第二交集中各个数据条目的匹配标记被设置为 0，并且其中确定所述目标计算结果包括：

至少基于所述候选计算结果与针对所述第二交集中各个数据条目的匹配标记的相乘运算，生成所述 MPC 的目标计算结果。

15. 一种电子设备，包括：

至少一个处理单元；以及

至少一个存储器，所述至少一个存储器被耦合到所述至少一个处理单元并且存储用于由所述至少一个处理单元执行的指令，所述指令在由所述至少一个处理单元执行时使所述电子设备执行根据权利要求 1 至 9 任一项所述的方法或根据权利要求 10 至 14 中任一项所述的方法。

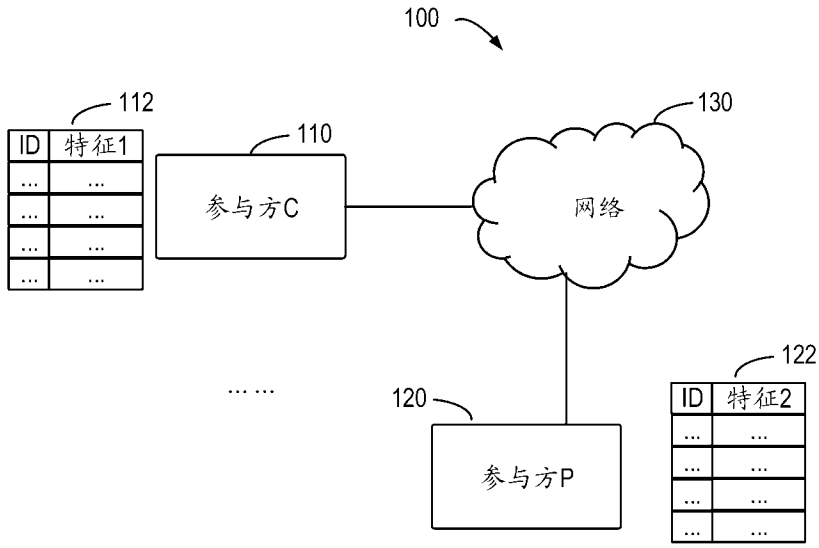

图 1

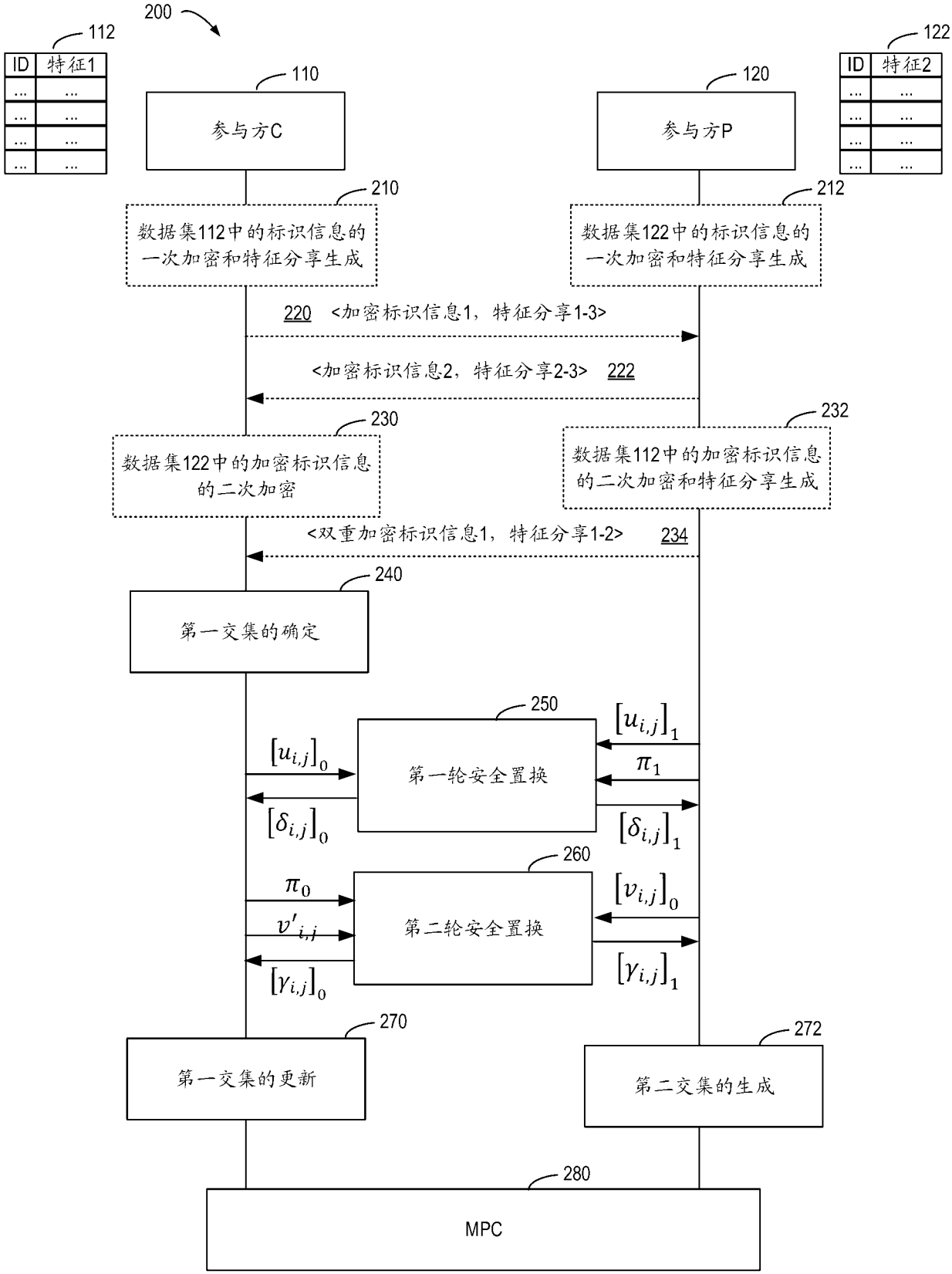
200
112
ID
特征1
122
ID
特征2
110
参与方C
120
参与方P
210
数据集112中的标识信息的一次加密和特征分享生成
212
数据集122中的标识信息的一次加密和特征分享生成
220 <加密标识信息1，特征分享1-3>
<加密标识信息2，特征分享2-3> 222
230
数据集122中的加密标识信息的二次加密
232
数据集112中的加密标识信息的二次加密和特征分享生成
<双重加密标识信息1，特征分享1-2> 234
240
第一交集的确定
250
$[u_{i,j}]_1$
$[u_{i,j}]_0$
第一轮安全置换
π_1
$[\delta_{i,j}]_0$
$[\delta_{i,j}]_1$
260
π_0
$[v_{i,j}]_0$
$v'_{i,j}$
第二轮安全置换
$[\gamma_{i,j}]_0$
$[\gamma_{i,j}]_1$
270
第一交集的更新
272
第二交集的生成
280
MPC

图 2

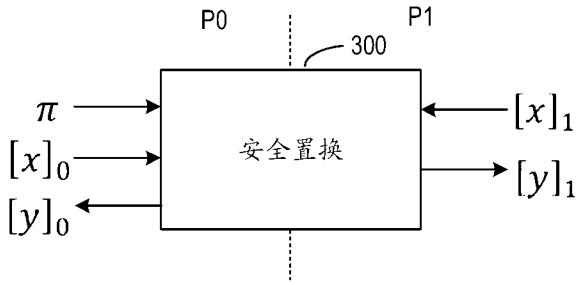

图 3

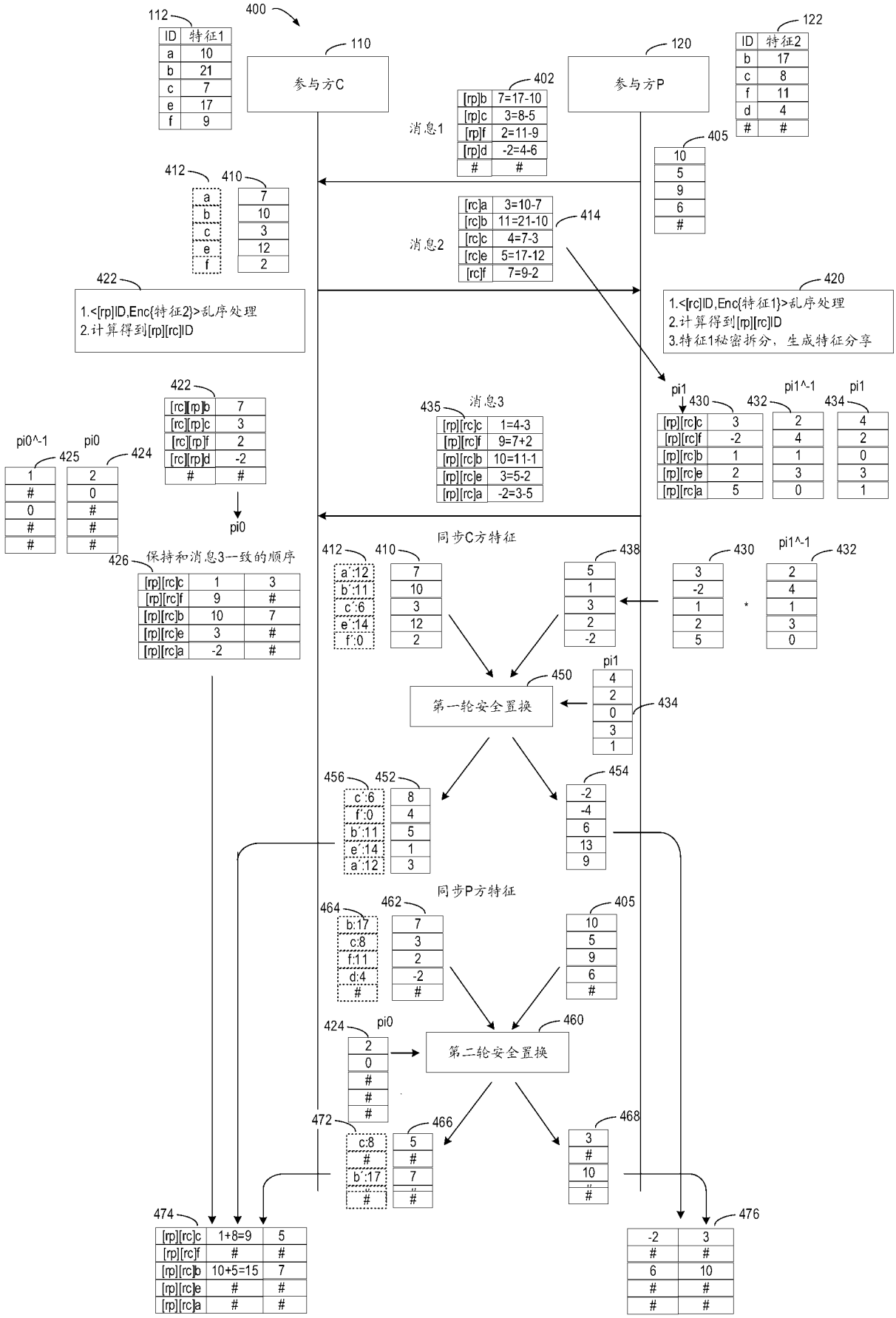
400
112
ID 特征1
a 10
b 21
c 7
e 17
f 9
110
参与方C
120
参与方P
122
ID 特征2
b 17
c 8
f 11
d 4
# #
消息1
402
[rp]b 7=17-10
[rp]c 3=8-5
[rp]f 2=11-9
[rp]d -2=4-6
# #
405
10
5
9
6
#
412
410
a
b
c
e
f
7
10
3
12
2
消息2
[rc]a 3=10-7
[rc]b 11=21-10
[rc]c 4=7-3
[rc]e 5=17-12
[rc]f 7=9-2
414
422
1.<[rp]ID,Enc{特征2}>乱序处理
2.计算得到[rp][rc]ID
420
1.<[rc]ID,Enc{特征1}>乱序处理
2.计算得到[rp][rc]ID
3.特征1秘密拆分，生成特征分享
422
[rc][rp]b 7
[rc][rp]c 3
[rc][rp]f 2
[rc][rp]d -2
# #
pi0
pi0^-1
pi0
425
424
1
#
0
#
#
2
0
#
#
#
消息3
435
[rp][rc]c 1=4-3
[rp][rc]f 9=7+2
[rp][rc]b 10=11-1
[rp][rc]e 3=5-2
[rp][rc]a -2=3-5
pi1
pi1^-1
pi1
430
432
434
[rp][rc]c 3 2 4
[rp][rc]f -2 4 2
[rp][rc]b 1 1 0
[rp][rc]e 2 3 3
[rp][rc]a 5 0 1
同步C方特征
412
410
438
a:12
b:11
c:6
e:14
f:0
7
10
3
12
2
5
1
3
2
-2
430
pi1^-1
432
3
-2
1
2
5
*
2
4
1
3
0
426
保持和消息3一致的顺序
[rp][rc]c 1 3
[rp][rc]f 9 #
[rp][rc]b 10 7
[rp][rc]e 3 #
[rp][rc]a -2 #
450
第一轮安全置换
pi1
4
2
0
3
1
434
456
452
454
c:6
f:0
b:11
e:14
a:12
8
4
5
1
3
-2
-4
6
13
9
同步P方特征
464
462
405
b:17
c:8
f:11
d:4
#
7
3
2
-2
#
10
5
9
6
#
424
pi0
460
2
0
#
#
#
第二轮安全置换
472
466
468
c:8
#
b:17
#
5
#
7
#
#
3
#
10
#
474
[rp][rc]c 1+8=9 5
[rp][rc]f # #
[rp][rc]b 10+5=15 7
[rp][rc]e # #
[rp][rc]a # #
476
-2 3
# #
6 10
# #
# #

图 4

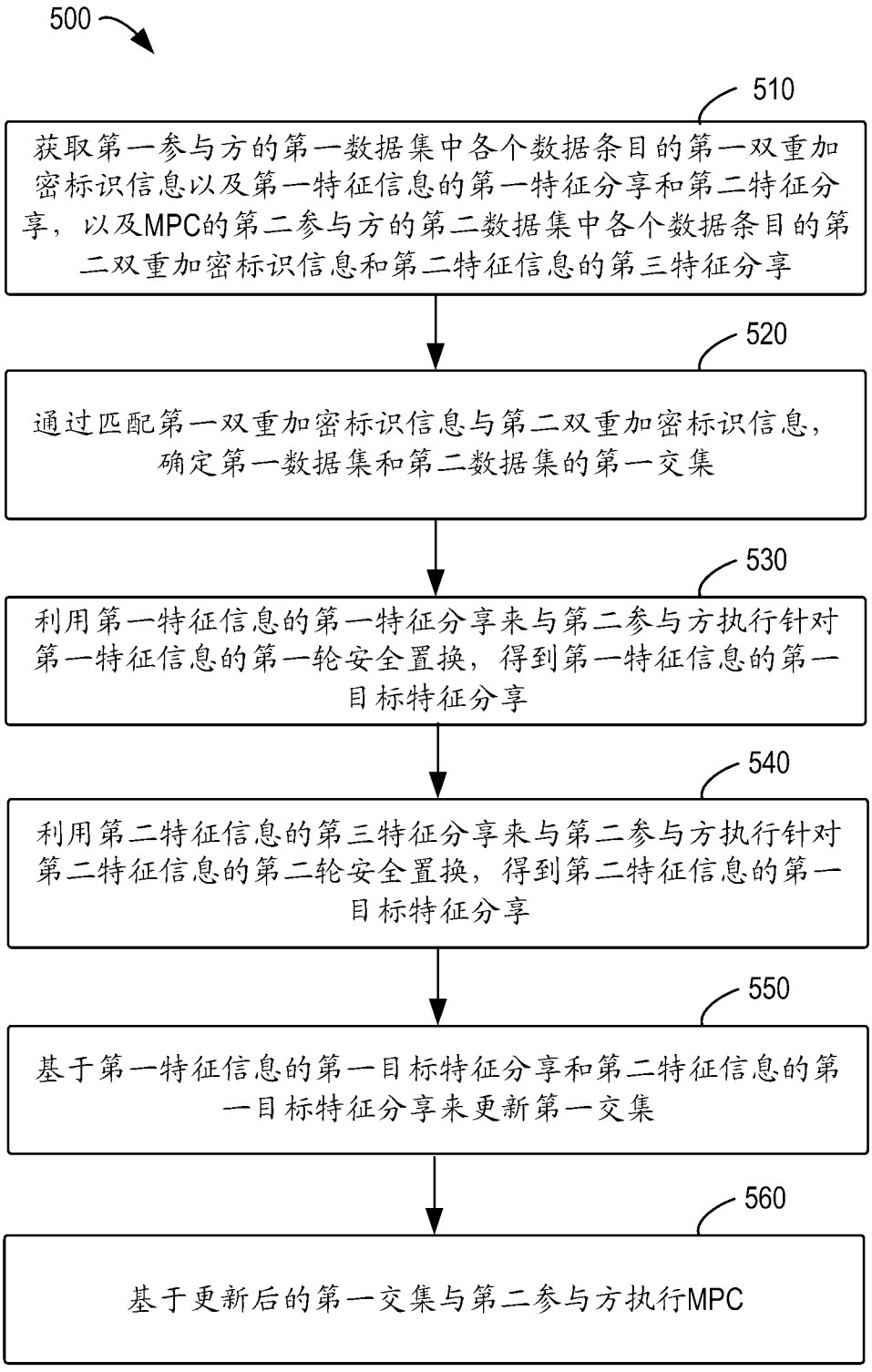
500
510
获取第一参与方的第一数据集中各个数据条目的第一双重加密标识信息以及第一特征信息的第一特征分享和第二特征分享，以及MPC的第二参与方的第二数据集中各个数据条目的第二双重加密标识信息和第二特征信息的第三特征分享
520
通过匹配第一双重加密标识信息与第二双重加密标识信息，确定第一数据集和第二数据集的第一交集
530
利用第一特征信息的第一特征分享来与第二参与方执行针对第一特征信息的第一轮安全置换，得到第一特征信息的第一目标特征分享
540
利用第二特征信息的第三特征分享来与第二参与方执行针对第二特征信息的第二轮安全置换，得到第二特征信息的第一目标特征分享
550
基于第一特征信息的第一目标特征分享和第二特征信息的第一目标特征分享来更新第一交集
560
基于更新后的第一交集与第二参与方执行MPC

图 5

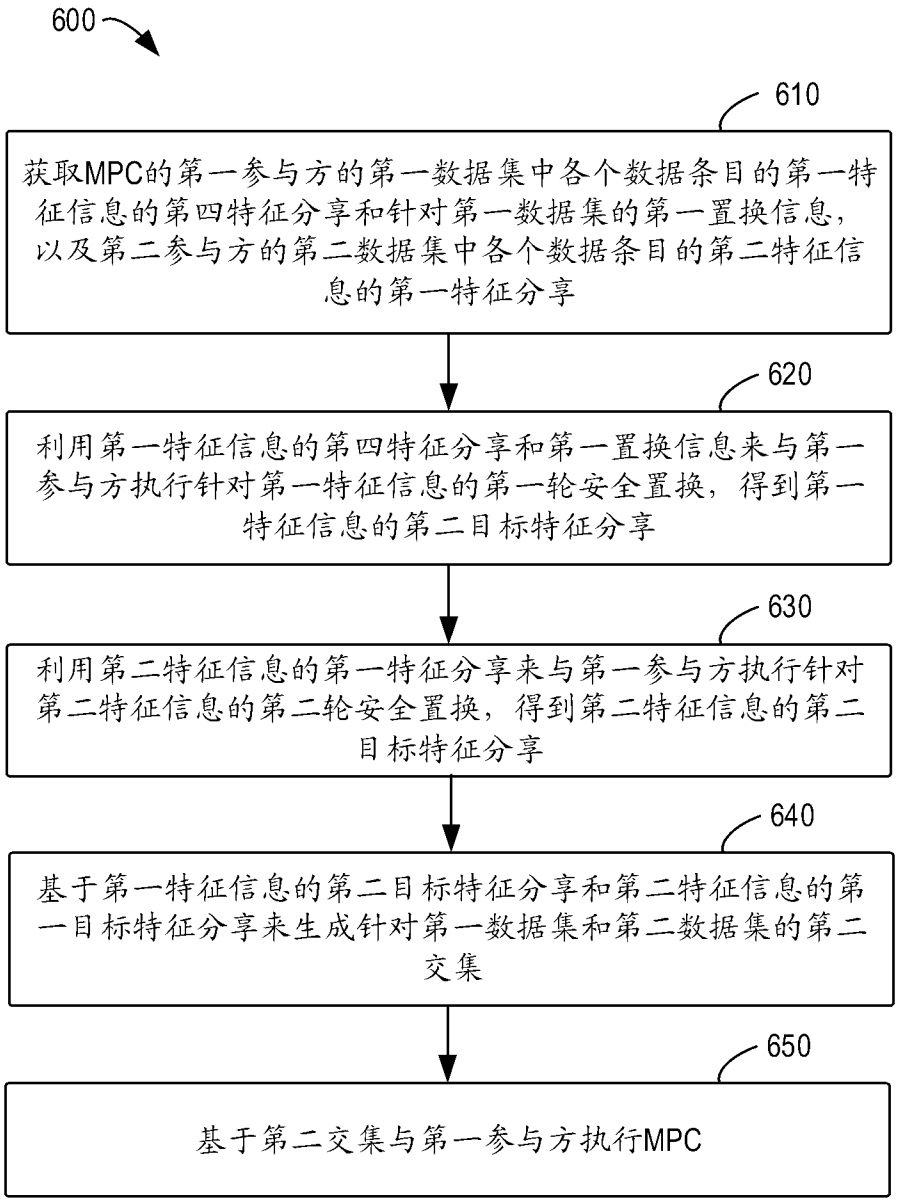
600
610
获取MPC的第一参与方的第一数据集中各个数据条目的第一特征信息的第四特征分享和针对第一数据集的第一置换信息，以及第二参与方的第二数据集中各个数据条目的第二特征信息的第一特征分享
620
利用第一特征信息的第四特征分享和第一置换信息来与第一参与方执行针对第一特征信息的第一轮安全置换，得到第一特征信息的第二目标特征分享
630
利用第二特征信息的第一特征分享来与第一参与方执行针对第二特征信息的第二轮安全置换，得到第二特征信息的第二目标特征分享
640
基于第一特征信息的第二目标特征分享和第二特征信息的第一目标特征分享来生成针对第一数据集和第二数据集的第二交集
650
基于第二交集与第一参与方执行MPC

图 6

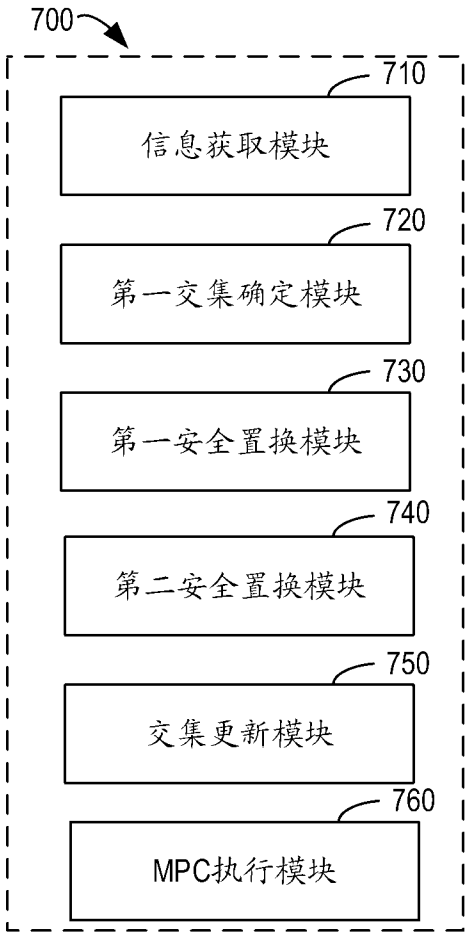
700
710
信息获取模块
720
第一交集确定模块
730
第一安全置换模块
740
第二安全置换模块
750
交集更新模块
760
MPC执行模块

图 7

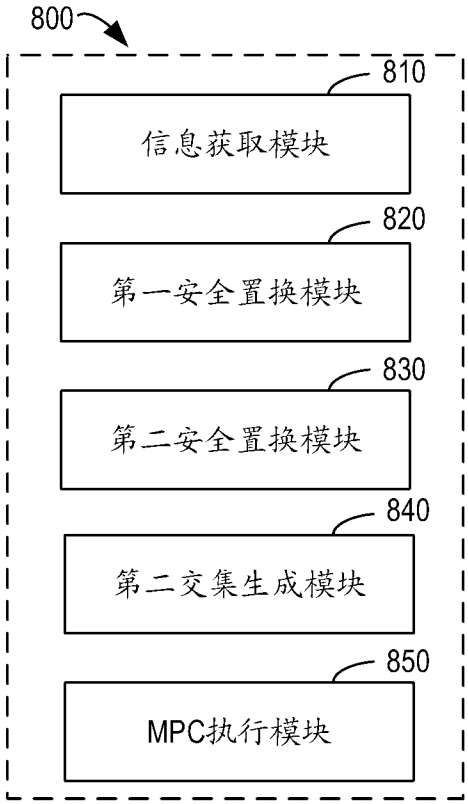
800
810
信息获取模块
820
第一安全置换模块
830
第二安全置换模块
840
第二交集生成模块
850
MPC执行模块

图 8

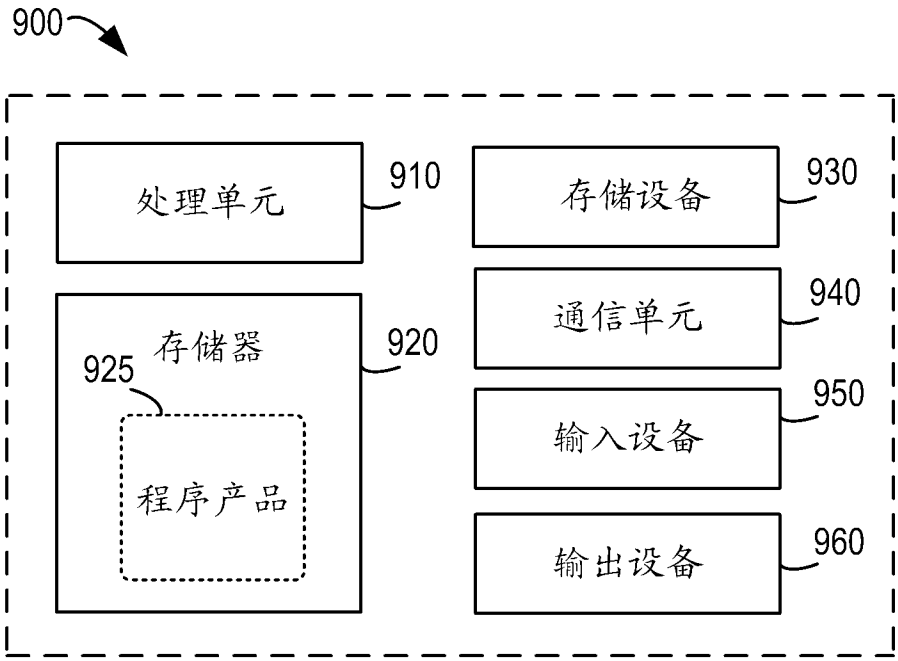
900
处理单元
910
存储器
925
920
程序产品
存储设备
930
通信单元
940
输入设备
950
输出设备
960

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2024/097142

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC:G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

VEN, CNABS, CNTXT, WOTXT, EPTXT, USTXT, CNKI, IEEE: 求交, 多方, 安全, 隐私, 分享, 秘密, multi, party, intersection, privacy, share, secret, secure, MPC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 115967491 A (HUAKONG TSINGJIAO INFORMATION SCIENCE (BEIJING) CO., LTD.) 14 April 2023 (2023-04-14) description, paragraphs 0016-0105	1-15
A	CN 115913537 A (SHENZHEN INSIGHTONE SMART TECHNOLOGY CO., LTD.) 04 April 2023 (2023-04-04) entire document	1-15
A	CN 116090002 A (CHINA MOBILE INFORMATION TECHNOLOGY CO., LTD. et al.) 09 May 2023 (2023-05-09) entire document	1-15
A	US 2015149763 A1 (MICROSOFT CORP.) 28 May 2015 (2015-05-28) entire document	1-15
PX	CN 117077156 A (BEIJING VOLCANO ENGINE TECHNOLOGY CO., LTD.) 17 November 2023 (2023-11-17) claims 1-15	1-15

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2024-08-16	**22 August 2024**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/097142

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 115967491 A	14 April 2023	None	
CN 115913537 A	04 April 2023	None	
CN 116090002 A	09 May 2023	None	
US 2015149763 A1	28 May 2015	ES 2626533 T3	25 July 2017
		EP 3075098 A1	05 October 2016
		EP 3075098 B1	01 March 2017
		US 9158925 B2	13 October 2015
		WO 2015080896 A1	04 June 2015
CN 117077156 A	17 November 2023	None	

国际检索报告

国际申请号
PCT/CN2024/097142

A. 主题的分类

G06F 21/60(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC:G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

VEN，CNABS，CNTXT，WOTXT，EPTXT，USTXT，CNKI，IEEE：求交，多方，安全，隐私，分享，秘密，multi, party, intersection, privacy, share, secret, secure, MPC

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 115967491 A (华控清交信息科技（北京）有限公司) 2023年4月14日 (2023 - 04 - 14) 说明书第0016-0105段	1-15
A	CN 115913537 A (深圳市洞见智慧科技有限公司) 2023年4月4日 (2023 - 04 - 04) 全文	1-15
A	CN 116090002 A (中移动信息技术有限公司 等) 2023年5月9日 (2023 - 05 - 09) 全文	1-15
A	US 2015149763 A1 (MICROSOFT CORP.) 2015年5月28日 (2015 - 05 - 28) 全文	1-15
PX	CN 117077156 A (北京火山引擎科技有限公司) 2023年11月17日 (2023 - 11 - 17) 权利要求1-15	1-15

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“D” 申请人在国际申请中引证的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2024-08-16	2024年8月22日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 胡丽丽 电话号码 (+86) 010-53961386

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/097142

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	115967491	A	2023年4月14日	无			
CN	115913537	A	2023年4月4日	无			
CN	116090002	A	2023年5月9日	无			
US	2015149763	A1	2015年5月28日	ES	2626533	T3	2017年7月25日
				EP	3075098	A1	2016年10月5日
				EP	3075098	B1	2017年3月1日
				US	9158925	B2	2015年10月13日
				WO	2015080896	A1	2015年6月4日
CN	117077156	A	2023年11月17日	无			