

(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
2023 年 9 月 14 日 (14.09.2023)



(10) 国际公布号
WO 2023/169079 A1

- (51) 国际专利分类号:
H04L 9/40 (2022.01) **H04L 9/08 (2006.01)**
- (21) 国际申请号: PCT/CN2023/071505
- (22) 国际申请日: 2023 年 1 月 10 日 (10.01.2023)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202210227401.5 2022年3月8日 (08.03.2022) CN
- (71) 申请人: 支付宝(杭州)信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。
- (72) 发明人: 钱中天(QIAN, Zhongtian); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。 潘无穷(PAN, Wuqiong); 中国浙

江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。 韦韬(WEI, Tao); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。 李婷婷(LI, Tingting); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。 卫振强(WEI, Zhenqiang); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。 李天一(LI, Tianyi); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (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,

(54) Title: DATA PROCESSING

(54) 发明名称: 数据处理

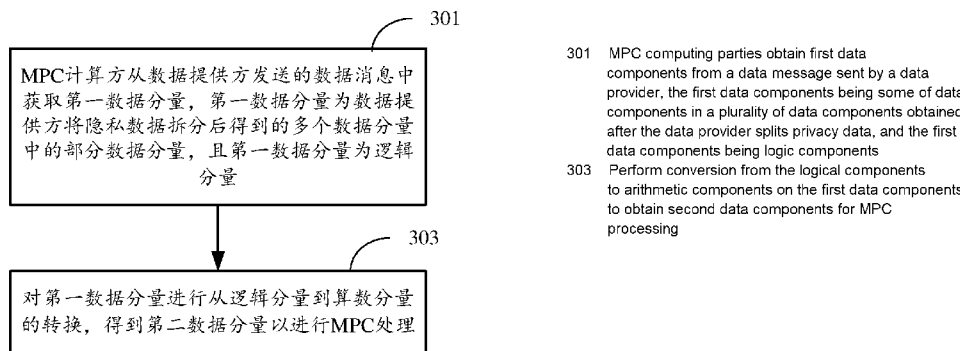


图 3

(57) Abstract: Embodiments of the present description provide a data processing method and apparatus, which are applied to a system comprising a data provider and N secure multi-party computation (MPC) computing parties, N being an integer greater than 3. According to the method of the embodiments, firstly, the MPC computing parties obtain first data components from a data message sent by the data provider, the first data components being some of data components in a plurality of data components obtained after the data provider splits privacy data, and the first data components being logic components; and then conversion from the logical components to arithmetic components is performed on the first data components to obtain second data components for MPC processing.

(57) 摘要: 本说明书实施例提供了一种数据处理方法和装置, 应用于包括数据提供方和N个多方安全计算MPC计算方的系统, 所述N为3以上的整数。根据该实施例的方法, 首先各MPC计算方从所述数据提供方发送的数据消息中获取第一数据分量, 所述第一数据分量为所述数据提供方将隐私数据拆分后得到的多个数据分量中的部分数据分量, 且所述第一数据分量为逻辑分量; 然后对所述第一数据分量进行从逻辑分量到算数分量的转换, 得到第二数据分量用以进行MPC处理。

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, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, 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))。

数据处理

技术领域

[01]本说明书一个或多个实施例涉及计算机技术领域,尤其涉及数据处理的方法和装置。

背景技术

[02]众所周知,数据往往包含大量的隐私和机密信息,统称为隐私数据,很多企业、医院等机构都会对隐私数据进行保护。在密码学中如何在不泄露隐私的情况下,保密地使用互联网实现数据共享是一个重要的问题。在这种背景下,MPC (Secure Multi-Party Computation, 安全多方计算)应运而生。MPC 指的是一组互相不信任的参与者在保护隐私的同时,还可以进行协同计算。其中,上述的参与者称为 MPC 计算方。

[03]数据提供方将隐私数据随机拆分成多个数据分量,将数据分量通过数据提供者与 MPC 计算方之间建立的安全信道提供给 MPC 计算方。数据提供者提供给各 MPC 计算方数据分量的原则在于,每个 MPC 计算方只获得其中一部分数据分量而非原始数据全部,并且至少 2 个以上的 MPC 计算方之间交互数据分量后能还原出原始数据。这样能够保证每个 MPC 计算方都只接触过数据分量,即便攻击者攻破一个 MPC 计算方,并且长期窃取或修改它,也不能获得有效信息。

[04]由于数据提供者与 MPC 计算方之间是通过公网传输的,因此亟需一种数据处理方式能够降低数据提供者与 MPC 计算方之间数据分量传输对公网传输造成的压力。

发明内容

[05]本说明书一个或多个实施例描述了一种数据处理方法,以便于降低数据分量传输对公网传输造成的压力。

[06]根据第一方面,提供了一种数据处理方法,应用于包括数据提供方和 N 个多方安全计算 MPC 计算方的系统,所述 N 为 3 以上的整数,所述方法包括:各 MPC 计算方从所述数据提供方发送的数据消息中获取第一数据分量,所述第一数据分量为所述数据提供方将隐私数据拆分后得到的多个数据分量中的部分数据分量,且所述第一数据分量为逻辑分量;对所述第一数据分量进行从逻辑分量到算数分量的转换,得到第二数据分量用以进行 MPC 处理。

[07]根据本申请实施例中一可实现的方式,所述 N 个 MPC 计算方包括第一 MPC 计算方、第二 MPC 计算方和第三 MPC 计算方;对所述逻辑分量进行转换得到算数分量包括:各

MPC 计算方进行零共享处理，得到第三数据分量，所述第三数据分量为算数分量；第一 MPC 计算方利用本地持有的逻辑分量进行算数值的第一转换和第二转换后，得到两个选择项，所述两个选择项为算数分量；第一 MPC 计算方利用所述两个选择项向第三 MPC 计算方进行不经意传输；各 MPC 计算方将本地得到的算数分量作为待分享数据进行算数共享处理，得到所述第二数据分量。

[08]根据本申请实施例中的一可实现的方式，所述零共享处理包括：各 MPC 计算方利用本地持有的第一零共享密钥生成第一派生值，以及本地持有的第二零共享密钥生成第二派生值；利用所述第一派生值与所述第二派生值的差值，得到第三数据分量。

[09]根据本申请实施例中的一可实现的方式，所述逻辑分量包括第一逻辑分量和第二逻辑分量；所述第一 MPC 计算方利用本地持有的逻辑分量进行算数值的第一转换和第二转换包括：所述第一 MPC 计算方利用交互密钥生成随机值；利用本地持有的第一逻辑分量、第二逻辑分量、所述随机值以及所述 MPC 处理所采用定点数的小数位数进行所述第一转换和第二转换，得到两个选择项；该方法还包括：所述第二 MPC 计算方利用所述交互密钥生成所述随机值。

[10]根据本申请实施例中的一可实现的方式，所述第一转换和所述第二转换分别采用如下公式得到选择项 m_0 和 m_1 ：

$$m_0 = (0 \wedge u_1 \wedge u_2) \times (1 \ll B) - \text{rnd};$$

$$m_1 = (1 \wedge u_1 \wedge u_2) \times (1 \ll B) - \text{rnd}$$

[11]其中， $\wedge$ 为异或运算符， $\ll$ 为左移运算符， u_1 和 u_2 分别为第一逻辑分量和第二逻辑分量， rnd 为所述随机值， B 为所述 MPC 处理所采用定点数的小数位数。

[12]根据本申请实施例中的一可实现的方式，各 MPC 计算方利用本地得到的算数分量进行算数共享处理，得到所述第二数据分量包括：各 MPC 计算方将本地的待分享数据进行加密后分享给下一 MPC 计算方，并接收上一 MPC 计算方分享来的数据并进行解密；将解密后的数据与本地的待分享数据合并，得到所述第二数据分量；其中各 MPC 计算方按照环状次序进行所述分享处理。

[13]根据第二方面，提供了一种数据处理方法，应用于包括数据提供方和 N 个 MPC 计算方的系统，所述 N 为 3 以上的整数，所述方法包括：所述数据提供方将隐私数据拆分为多个数据分量；将所述多个数据分量通过数据消息分发给所述 N 个 MPC 计算方，以使得各 MPC 计算方接收到所述多个数据分量中的部分数据分量作为第一数据分量，所

述第一数据分量为逻辑分量。

[14]根据本申请实施例中一可实现的方式，所述多个数据分量为N个数据分量；将所述多个数据分量通过数据消息分发给所述N个MPC计算方包括：向各MPC计算方分别发送两个数据分量，且向其中任一个MPC计算方发送的第一个数据分量与向该MPC计算方的上一个MPC计算方发送的第二个数据分量相同；各MPC计算方按环状排序。

[15]根据第三方面，提供了一种数据处理装置，应用于包括数据提供方和N个多方安全计算MPC计算方的系统，所述N为3以上的整数；所述装置设置于所述MPC计算方，包括：数据获取单元，被配置为从所述数据提供方获取第一数据分量，所述第一数据分量为所述数据提供方将隐私数据拆分后得到的多个数据分量中的部分数据分量，且所述第一数据分量为逻辑分量；算数转换单元，被配置为对所述第一数据分量进行从逻辑分量到算数分量的转换，得到第二数据分量用以进行MPC处理。

[16]根据第四方面，提供了一种数据处理装置，应用于包括数据提供方和N个多方安全计算MPC计算方的系统，所述N为3以上的整数；所述装置设置于所述数据提供方，包括：数据拆分单元，被配置为将隐私数据拆分为多个数据分量；数据发送单元，被配置为将所述多个数据分量通过数据消息分发给所述N个MPC计算方，以使得各MPC计算方接收到所述多个数据分量中的部分数据分量作为第一数据分量，所述第一数据分量为逻辑分量。

[17]根据第五方面，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，实现第一方面或第二方面的方法。

[18]根据本说明书实施例提供的方法和装置，数据提供方仅需要向各MPC计算方传输逻辑分量；由各MPC计算方利用接收到的逻辑分量转换得到算数分量，从而降低公网传输的数据量。

附图说明

[19]为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例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。

[20]图1为本申请实施例适用的系统架构图；

[21]图2示出根据一个实施例的数据处理方法的流程图；

[22]图 3 示出根据另一个实施例的数据处理方法的流程图；

[23]图 4 为本申请实施例提供的一种数据传输的实例图；

[24]图 5 为本申请实施例提供的另一种数据传输的实例图；

[25]图 6 为本申请实施例提供的逻辑分量转换算数分量的方法流程图；

[26]图 7 示出根据一个实施例的数据处理装置的示意性框图；

[27]图 8 示出根据另一个实施例的数据处理装置的示意性框图。

具体实施方式

[28]在本发明实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本发明。在本发明实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。

[29]应当理解，本文中使用的术语“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[30]取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”或“响应于检测”。类似地，取决于语境，短语“如果确定”或“如果检测（陈述的条件或事件）”可以被解释成为“当确定时”或“响应于确定”或“当检测（陈述的条件或事件）时”或“响应于检测（陈述的条件或事件）”。

[31]图 1 为本申请实施例适用的系统架构图，如图 1 中所示，该系统包括数据提供方和 N 个 MPC 计算方，N 为 3 以上的整数，在图 1 中 N 以 3 为例。TECC（可信密态计算）基于 MPC（Secure Multi-Party Computation，安全多方计算）算法，是一种安全高效的密态计算方法。在 TECC 应用场景下，上述的 MPC 计算方可以为各 TEE（Trusted Execution Environment，可信执行环境）。

[32]目前已有的数据分量传输方式是，数据提供方由于数据提供方与 MPC 计算方之间是通过公网传输的，这种传输方式下，每个数据提供方都需要传输 $(N-1)*N$ 份数据分量。

[33]以图 1 中为例，数据提供者 1 将数据 u 拆分成 u1、u2 和 u3。然后将 u1、u2 提供给 MPC 计算方 A，将 u2、u3 提供给 MPC 计算方 B，将 u3、u1 提供给 MPC 计算方 C。

[34]在诸如机器学习等模型训练或预测场景下，数据提供方提供的隐私数据为样本特征数据的 one hot（独热）编码数据。相应地，数据提供方传输的第一数据分量为由 one hot

编码数据随机拆分的逻辑分量，由于一些应用场景的需要，同时会传输逻辑分量对应的算数分量。其中逻辑分量指的是各元素为二进制值的数据分量，算数分量指的是各元素为整型数据值的数据分量。例如，对于特征数量为 d ，分桶为 b ，样本数量为 n 的数据集，可以使用 $X[d][b][n]$ 来表示样本特征数据的 one hot 编码， $X[d][b][n]$ 中各元素的取值为 0 或 1。每个元素占用 1bit，将其拆分为逻辑分量，每个逻辑分量的大小与 $X[d][b][n]$ 一致。同时，数据提供方需要提供上述逻辑分量对应的数据分量，即 $X[d][b][n]$ 的每个元素都用一个整数表示，占用 32bit。这种方式显然也会造成公网的传输压力过大，以 $d=200$ ， $b=13$ ， $n=100w$ 为例，全量发送 6 个数据分量大小约为 60GB，这是难以接受的。本申请则致力于在降低公网传输的数据量的基础上，仍保证各 MPC 计算方能够获取逻辑分量以及对应的算数分量。

[35]下面结合附图，对本说明书提供的方案进行描述。

[36]图 2 示出根据一个实施例的数据处理方法的流程图。该方法由图 1 所示系统中的数据提供者执行。如图 2 所示，该方法包括以下步骤：步骤 201：数据提供方将隐私数据拆分为多个数据分量。

[37]步骤 203：将多个数据分量通过数据消息分发给 N 个 MPC 计算方，以使得各 MPC 计算方接收到上述多个数据分量中的部分数据分量作为第一数据分量，第一数据分量为逻辑分量。

[38]图 3 示出根据另一个实施例的数据处理方法的流程图，该方法由图 1 所示系统中的各 MPC 计算方执行。如图 3 中所示，该方法包括以下步骤：

[39]步骤 301：MPC 计算方从数据提供方发送的数据消息中获取第一数据分量，第一数据分量为数据提供方将隐私数据拆分后得到的多个数据分量中的部分数据分量，且第一数据分量为逻辑分量。

[40]步骤 303：对第一数据分量进行从逻辑分量到算数分量的转换，得到第二数据分量用以进行 MPC 处理。

[41]通过图 2 和图 3 所示数据处理方法，数据提供方将原本需要同时向 MPC 计算方传输逻辑分量和算数分量，替换为仅传输逻辑分量；由各 MPC 计算方利用接收到的逻辑分量转换得到算数分量，从而降低公网传输的数据量。

[42]作为其中一种可实现的方式，数据提供方仍可以采用现有的传输方式，将隐私数据拆分成多个数据分量。然后向各 MPC 计算方分别发送两个数据分量，且向其中任一个 MPC 计算方发送的第一个数据分量与向该 MPC 计算方的上一个 MPC 计算方发送的第二个数据分量相同。

[43]以图 1 中为例，数据提供者 1 将数据 u 拆分成 u_1 、 u_2 和 u_3 。然后将 u_1 、 u_2 提供给 MPC 计算方 A，将 u_2 、 u_3 提供给 MPC 计算方 B，将 u_3 、 u_1 提供给 MPC 计算方 C。即在步骤 301 中，MPC 计算方 A 获取到的第一数据分量为 u_1 和 u_2 ，由于 u_1 和 u_2 均为逻辑分量，因此将 u_1 和 u_2 分别称为第一逻辑分量和第二逻辑分量。相应地，MPC 计算方 B 获取到的第一数据分量中包含的第一逻辑分量和第二逻辑分量分别为 u_2 和 u_3 ，MPC 计算方 C 获取到的第一数据分量中包含的第一逻辑分量和第二逻辑分量分别为 u_3 和 u_1 。

[44]作为另一种可实现的方式，数据提供方可以将 N 个数据分量分别发送给 N 个 MPC 计算方，即每个 MPC 计算方接收到其中一个数据分量且每个 MPC 计算方接收到的数据分量不同。

[45]这种情况下，在上述步骤 301 中，MPC 计算方接收到数据分量后，利用接收到的数据分量进行算数共享（sharing）处理即可获取到第一数据分量。

[46]所谓算数共享处理指的是：将本地的待分享数据进行加密后分享给下一 MPC 计算方，并接收上一 MPC 计算方分享来的数据并进行解密。然后将接收到的解密后的数据与本地的待分享数据合并，得到第一数据分量。也就是说，算数共享处理是各 MPC 计算方按照环状次序进行数据分享的过程。另外，MPC 计算方进行加密时采用的密钥与下一 MPC 计算方解密所采用的密钥相同，该密钥是预先配置或约定好的。

[47]以图 1 所示的 3 个 MPC 计算方为例对这种实现方式进行描述。如图 4 所示，首先，数据提供方依然将原始数据拆分成三个数据分量 u_1 、 u_2 和 u_3 。然后将 u_1 传输给 MPC 计算方 A，将 u_2 传输给 MPC 计算方 B，将 u_3 传输给 MPC 计算方 C。

[48]MPC 计算方 A、MPC 计算方 B 和 MPC 计算方 C 共同执行一次算数共享处理。其中，每个 MPC 计算方预先约定好交互密钥使得每个 MPC 计算方本地均存在交互密钥对（share_rng_d, share_rng_u）。MPC 计算方 A 的 share_rng_d 与 MPC 计算方 C 的 share_rng_u 相同，MPC 计算方 B 的 share_rng_d 与 MPC 计算方 A 的 share_rng_u 相同，MPC 计算方 C 的 share_rng_d 与 MPC 计算方 B 的 share_rng_u 相同。

[49]在进行算数共享处理时，MPC 计算方 A 利用 share_rng_d 对 u_1 进行加密后传输给 MPC 计算方 C，MPC 计算方 C 利用 share_rng_u 进行解密得到 u_1 。

[50]MPC 计算方 B 利用 share_rng_d 对 u_2 进行加密后传输给 MPC 计算方 A，MPC 计算方 A 利用 share_rng_u 进行解密得到 u_2 。

[51]MPC 计算方 C 利用 share_rng_d 对 u_3 进行加密后传输给 MPC 计算方 B，MPC 计算方 B 利用 share_rng_u 进行解密得到 u_3 。

[52]进行算数共享处理之后，MPC 计算方 A 本地存在 u_1 和 u_2 ，MPC 计算方 B 本地存在 u_2 和 u_3 ，MPC 计算方 C 本地存在 u_3 和 u_1 。但公网仅需要传输 3 份数据分量(逻辑分量)，即从原本需要传输 6 份数据分量减少到 3 份。而在 MPC 计算方之间进行算数共享时，由于是在高速网内部因此对于网络传输的压力很小。

[53]作为再一种可实现的方式，数据提供方拆分得到的数据分量数量小于 N ，仅向其中部分 MPC 计算方传输一个数据分量，其他 MPC 获取 0 个数据分量。即有部分 MPC 计算方分别接收到其中一个数据分量且每个 MPC 计算方接收到的数据分量不同，另一部分 MPC 计算方接收到 0 个数据分量。

[54]这种情况下，在上述步骤 301 中，MPC 计算方从数据消息中获取到数据分量（1 个或 0 个）后，可以首先进行零共享（zero sharing）处理，得到第四数据分量；然后将得到的第四数据分量和从数据消息中获取的数据分量进行合并后得到第五数据分量；再将第五数据分量作为待分享数据进行算数共享处理，得到第一数据分量。

[55]零共享处理指的是各 MPC 计算方各自生成数据分量并且各 MPC 计算方生成的数据分量的和为 0。具体地，零共享处理包括：MPC 计算方利用本地持有的第一零共享密钥生成第一派生值，以及本地持有的第二零共享密钥生成第二派生值；利用所述第一派生值与所述第二派生值的差值，得到上述的第四数据分量。其中每个 MPC 计算方预先约定好零共享密钥使得每个 MPC 计算方本地均存在由第一零共享密钥和第二零共享密钥构成的密钥对（ $prng, prngu$ ）。MPC 计算方 A 的 $prng$ 与 MPC 计算方 C 的 $prngu$ 相同，MPC 计算方 B 的 $prng$ 与 MPC 计算方 A 的 $prngu$ 相同，MPC 计算方 C 的 $prng$ 与 MPC 计算方 B 的 $prngu$ 相同。

[56]以图 1 所示的 3 个 MPC 计算方为例对这种实现方式进行描述。如图 5 所示，首先，数据提供方依然将原始数据拆分成两个数据分量 y_1 和 y_2 。然后将 y_1 传输给 MPC 计算方 A，将 y_2 传输给 MPC 计算方 B，MPC 计算方 C 得到 0 个数据分量。

[57]MPC 计算方 A、MPC 计算方 B 和 MPC 计算方 C 共同执行一次零共享处理，分别获得 0 的三个分量 x_1 、 x_2 和 x_3 。具体地，各 MPC 计算方各自使用 $prng$ 生成第一派生值 buf_1 ，使用 $prngu$ 生成第二派生值 buf_2 ，将 $buf_1 - buf_2$ 的值作为零共享处理得到的第四数据分量。

[58]MPC 计算方 A 将零共享处理的结果 x_1 与 y_1 合并后得到第五数据分量 $x_1 + y_1$ ，MPC 计算方 B 将零共享处理的结果 x_2 与 y_2 合并后得到第五数据分量 $x_2 + y_2$ ，MPC 计算方 C 将零共享处理的结果 x_3 与接收到的 0 个数据分量合并后得到第五数据分量 x_3 。

[59]然后 MPC 计算方 A、MPC 计算方 B 和 MPC 计算方 C 共同执行一次算数共享处理。

[60]在进行算数共享处理时，MPC 计算方 A 利用 share_rng_d 对 x_1+y_1 进行加密后传输给 MPC 计算方 C，MPC 计算方 C 利用 share_rng_u 进行解密得到 x_1+y_1 。

[61]MPC 计算方 B 利用 share_rng_d 对 x_2+y_2 进行加密后传输给 MPC 计算方 A，MPC 计算方 A 利用 share_rng_u 进行解密得到 x_2+y_2 。

[62]MPC 计算方 C 利用 share_rng_d 对 x_3 进行加密后传输给 MPC 计算方 B，MPC 计算方 B 利用 share_rng_u 进行解密得到 x_3 。

[63]进行算数共享处理之后，MPC 计算方 A 本地存在 $u_1=x_1+y_1$ ， $u_2=x_2+y_2$ ，MPC 计算方 B 本地存在 $u_2=x_2+y_2$ ， $u_3=x_3$ ，MPC 计算方 C 本地存在 $u_3=x_3$ ， $u_1=x_1+y_1$ 。但公网仅需要传输 2 份数据分量，即从原本需要传输 6 份数据分量减少到 2 份。而在 MPC 计算方之间进行算数共享时，由于是在高速网内部因此对于网络传输的压力很小。

[64]通过上面实施例中的所述的方式可以将数据分量(逻辑分量)从 6 个缩小为 3 个或 2 个。

[65]下面结合实施例对上述步骤 303 即“对第一数据分量进行从逻辑分量到算数分量的转换，得到第二数据分量用以进行 MPC 处理”进行详细描述。

[66]图 6 为本申请实施例提供的一种从逻辑分量到算数分量的转换方法流程图，在该流程中，系统中包括第一 MPC 计算方、第二 MPC 计算方和第三 MPC 计算方。如图 6 中所示，包括以下步骤：步骤 601：各 MPC 计算方进行零共享处理，得到第三数据分量。

[67]在进行零共享处理时，各 MPC 计算方利用本地持有的第一零共享密钥生成第一派生值，以及本地持有的第二零共享密钥生成第二派生值；然后利用第一派生值与第二派生值的差值，得到第三数据分量。经过零共享处理得到的第三数据分量为算数分量。具体将在后续实施例中举例说明。

[68]步骤 603：第一 MPC 计算方利用本地持有的逻辑分量进行算数值的第一转换和第二转换后，得到两个选择项，所述两个选择项为算数分量。

[69]作为一种可实现的方式，第一 MPC 计算方可以利用交互密钥生成随机值；利用本地持有的第一逻辑分量、第二逻辑分量、随机值以及所采用定点数的小数位数进行第一转换和第二转换，得到两个选择项。另外，第二 MPC 计算方也可以利用交互密钥生成上述的随机值。

[70]其中可以利用如下公式分别得到两个选择项 m_0 和 m_1 ：

$$m_0=(0^{\wedge}u_1^{\wedge}u_2)\times(1<<B)-\text{rnd}$$

$$m_1=(1^{\wedge}u_1^{\wedge}u_2)\times(1<<B)-\text{rnd}$$

[71]其中， $\wedge$ 为异或运算符， $<<$ 为左移运算符。B 为 MPC 处理所采用定点数的小数位数。

MPC 算法中使用的是定点数，所谓定点数一般指的是定点小数。计算机处理的数值数

据多数带有小数,小数点一般隐含在某个固定的位置上,称为定点表示法,简称定点数。

rnd 为随机值,可以利用本地持有的交互密钥 share_rng_u 生成。

[72]步骤 605: 第一 MPC 计算方利用所述两个选择项向第三 MPC 计算方进行不经意传输。

[73]不经意传输(OT, oblivious transfer)是一个密码学协议,目前被广泛的应用于 MPC。

目的是 MPC 计算方将 m0 和 m1 发送给另一个 MPC 计算方,该另一个 MPC 计算方只能获取 m0 和 m1 中的一个,并且发送 m0 和 m1 的 MPC 计算方也无法获知另一个 MPC 计算方获取的是 m0 和 m1 中的哪一个。

[74]作为其中一种可实现的方式,本步骤中的不经意传输可以是三方不经意传输,第一 MPC 计算方作为不经意传输的发送(send)方,第二 MPC 计算方作为协助(help)方,第三 MPC 计算方作为接收(receive)方。第一 MPC 计算方以 m0 和 m1 作为两个选择项,第二 MPC 计算方和第三 MPC 计算方本地持有的 u3 作为选择,执行一次不经意传输。具体将在后续实施例中举例描述。

[75]步骤 607: 各 MPC 计算方将本地得到的算数分量作为待分享数据进行算数共享处理,得到所述第二数据分量。

[76]具体地,在进行算数共享处理时,各 MPC 计算方将本地的待分享数据进行加密后分享给下一 MPC 计算方,并接收上一 MPC 计算方分享来的数据并进行解密;将解密后的数据与本地的待分享数据合并,得到第二数据分量;其中各 MPC 计算方按照环状次序进行上述的分享处理。

[77]以图 1 所示的 3 个 MPC 计算方为例对这种实现方式进行描述。假设 MPC 计算方 A、MPC 计算方 B 和 MPC 计算方 C 分别获取到了第一数据分量(u1,u2), (u2,u3), 和(u3,u1)。

[78]MPC 计算方 A、MPC 计算方 B 和 MPC 计算方 C 共同执行一次零共享处理,分别得到各自的第三数据分量 r1, r2 和 r3。r1, r2 和 r3 均为算数分量。

[79]MPC 计算方 A 使用本地的 share_rng_u 生成随机值 rnd, 确定

$$m0=(0^{u1^{u2}}) \times (1 \ll B)-rnd,$$

$$m1=(1^{u1^{u2}}) \times (1 \ll B)-rnd。$$

[80]其中, “ $1 \ll B$ ” 是一个转算数分量的处理, 即将 $(1^x.b^x.bu)$ 转成算数值。

[81]MPC 计算方 B 使用本地的 share_rng_d 生成随机值 rnd, 该值与 MPC 计算方 A 生成的随机值相同。此时 MPC 计算方 B 本地持有 r2', $r2' = r2 + rnd$ 。

[82]MPC 计算方 A 作为不经意传输的 send 方, MPC 计算方 B 作为 help 方, MPC 计算方 C 作为 receive 方。MPC 计算方 A 以 m0 和 m1 作为两个选择项, MPC 计算方 B 和

MPC 计算方 C 本地持有的 u_3 作为选择, 执行一次不经意传输。

[83]具体地, MPC 计算方 A 和 MPC 计算方 B 进行交互产生共有的随机值 W_0 和 W_1 。MPC 计算方 A 发送 $m_0^{W_0}$, $m_1^{W_1}$ 给 MPC 计算方 C。MPC 计算方 B 利用 u_3 将 W_c 发送给 MPC 计算方 C, 其中 W_c 为 W_0 或 W_1 。MPC 计算方 C 利用 W_c 分别对 $m_0^{W_0}$, $m_1^{W_1}$ 进行解密, 解密其中一个, 得到 m_i , m_i 为 m_0 和 m_1 中的一个值。不经意传输后, MPC 计算方 C 本地持有 r_3' , $r_3' = r_3 + m_i$ 。

[84]MPC 计算方 A 将 r_1 作为待分享数据, MPC 计算方 B 将 r_2' 作为待分享数据, MPC 计算方 C 将 r_3' 作为待分享数据, 执行一次算数共享处理, 得到各自的算数分量。即 MPC 计算方 A 得到算数分量 $r_1 + r_2'$, MPC 计算方 B 得到算数分量 $r_2 + r_3'$, MPC 计算方 C 得到算数分量 $r_1 + r_3'$ 。

[85]下面论证上述过程是否得到算数分量: 由于 u_3 的取值是 0 或者 1,

[86]当 u_3 为 0 时:

$$\begin{aligned} r_1 + r_2' + r_3' &= r_1 + r_2 + \text{rnd} + r_3 + (0^{u_1 u_2}) * (1 \ll B) - \text{rnd} \\ &= (0^{u_1 u_2}) * (1 \ll B) = (u_3^{u_1 u_2}) * (1 \ll B) \end{aligned}$$

[87]当 u_3 为 1 时:

$$\begin{aligned} r_1 + r_2' + r_3' &= r_1 + r_2 + \text{rnd} + r_3 + (1^{u_1 u_2}) * (1 \ll B) - \text{rnd} \\ &= (1^{u_1 u_2}) * (1 \ll B) = (u_3^{u_1 u_2}) * (1 \ll B) \end{aligned}$$

[88]其中, $(1 \ll B)$ 实际上是将逻辑值转为算数值的处理, 也就是说, $r_1 + r_2' + r_3'$ 经过上述处理后相当于逻辑量的和 $(u_3^{u_1 u_2})$ 再转算数值。将 r_1 、 r_2' 和 r_3' 进行一次算数 sharing, 三个 MPC 计算方就各自拥有了算数分量。

[89]在该例子中, 数据提供方只需要发送样本的逻辑分量, 而不需要发送算数分量, 相比较需要同时传输逻辑分量和算数分量数据传输量降低为 1/33。

[90]上述对本说明书特定实施例进行了描述。其它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求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。

[91]根据另一方面的实施例, 提供了一种数据处理装置。图 7 示出根据一个实施例的数据处理装置的示意性框图。可以理解, 该装置可以设置于图 1 所示系统中的 MPC 计算方, 可以体现为应用程序, 或者应用程序中的插件或软件开发工具包 (Software Development Kit, SDK) 等功能单元的形式。如图 7 所示, 该装置 700 包括: 数据获取

单元 701 和算数转换单元 702。其中各组成单元的主要功能如下：数据获取单元 701，被配置为从数据提供方获取第一数据分量，第一数据分量为数据提供方将隐私数据拆分后得到的多个数据分量中的部分数据分量，且第一数据分量为逻辑分量。

[92]算数转换单元 702，被配置为对第一数据分量进行从逻辑分量到算数分量的转换，得到第二数据分量用以进行 MPC 处理。

[93]作为其中一种可实现的方式，算数转换单元 702 可以具体被配置为：进行零共享处理，得到第三数据分量，所述第三数据分量为算数分量；若该装置位于第一 MPC 计算方，则算数转换单元 702 利用本地持有的逻辑分量进行算数值的第一转换和第二转换后，得到两个选择项，该两个选择项为算数分量；利用两个选择项向第三 MPC 计算方进行不经意传输。

[94]若该装置位于第三 MPC 计算方，则算数转换单元 702 获取第一 MPC 计算方不经意传输来的选择项。

[95]算数转换单元 702 进一步被配置为将本地得到的算数分量作为待分享数据进行算数共享处理，得到第二数据分量。

[96]作为其中一种可实现的方式，算数转换单元 702 在进行零共享处理时，可以利用本地持有的第一零共享密钥生成第一派生值，以及本地持有的第二零共享密钥生成第二派生值；利用第一派生值与第二派生值的差值，得到第三数据分量。

[97]作为其中一种可实现的方式，算数转换单元 702 在利用本地持有的逻辑分量进行算数值的第一转换和第二转换时，可以具体利用交互密钥生成随机值；利用本地持有的第一逻辑分量、第二逻辑分量、随机值以及所采用定点数的小数位数进行第一转换和第二转换，得到两个选择项。

[98]若该装置位于第二 MPC 计算方，则算数转换单元 702 利用交互密钥也生成上述的随机值。

[99]其中，上述的第一转换和第二转换分别采用如下公式得到选择项 m0 和 m1：

$$m0=(0^{\wedge}u1^{\wedge}u2)\times(1<<B)-rnd$$

$$m1=(1^{\wedge}u1^{\wedge}u2)\times(1<<B)-rnd$$

[100]其中， $\wedge$ 为异或运算符， $<<$ 为左移运算符，u1 和 u2 分别为第一逻辑分量和第二逻辑分量，rnd 为随机值，B 为所采用定点数的小数位数。

[101]作为其中一种可实现的方式，算数转换单元 702 利用本地得到的算数分量进行算数共享处理时，可以具体将本地的待分享数据进行加密后分享给下一 MPC 计算方，并接收上一 MPC 计算方分享来的数据并进行解密；将解密后的数据与本地的待分享数据合

并，得到第二数据分量；其中各 MPC 计算方按照环状次序进行上述的分享处理。

[102]根据另一方面的实施例，提供了一种数据处理装置。图 8 示出根据一个实施例的数据处理装置的示意性框图。可以理解，该装置可以设置于图 1 所示系统中的数据提供方，可以体现为应用程序，或者应用程序中的插件或软件开发工具包（Software Development Kit, SDK）等功能单元的形式。如图 8 所示，该装置 800 包括：数据拆分单元 801 和数据发送单元 802。其中各组成单元的主要功能如下：数据拆分单元 801，被配置为将隐私数据拆分为多个数据分量。

[103]数据发送单元 802，被配置为将多个数据分量通过数据消息分发给 N 个 MPC 计算方，以使得各 MPC 计算方接收到多个数据分量中的部分数据分量作为第一数据分量，该第一数据分量为逻辑分量。

[104]作为一种可实现的方式，上述多个数据分量为 N 个数据分量。数据发送单元 802 可以向各 MPC 计算方分别发送两个数据分量，且向其中任一个 MPC 计算方发送的第一个数据分量与向该 MPC 计算方的上一个 MPC 计算方发送的第二个数据分量相同；各 MPC 计算方按环状排序。

[105]需要说明的是，本公开中涉及的“第一”、“第二”、“第三”等限定并不具备大小、顺序和数量等方面的限制，仅仅用以在名称上加以区分，例如“第一数据分量”、“第二数据分量”、“第三数据分量”等用以在名称上区分各数据分量。

[106]根据另一方面的实施例，还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，令计算机执行结合图 2、图 3 或图 6 所描述的方法。

[107]根据再一方面的实施例，还提供一种计算设备，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，实现结合图 2、图 3 或图 6 所述的方法。

[108]随着时间、技术的发展，计算机可读存储介质含义越来越广泛，计算机程序的传播途径不再受限于有形介质，还可以直接从网络下载等。可以采用一个或多个计算机可读存储介质的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子（非穷举的列表）包括：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（EPROM 或闪存）、光纤、便携式紧凑磁盘只读存储器（CD-ROM）、光存储器件、磁存储器件、或者上述的任意合适的组合。在本说明书中，计算机可读存储介质可以是任

何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[109]上述的处理器可包括一个或多个单核处理器或多核处理器。处理器可包括任何一般用途处理器或专用处理器（如图像处理器、应用处理器基带处理器等）的组合。

[110]在一个实施例中，处理器中的至少一个可以与用于系统控制逻辑的一个或多个控制器的逻辑一起封装。在一个实施例中，处理器中的至少一个可以与用于系统控制逻辑的一个或多个控制器的逻辑一起封装以形成系统级封装。在一个实施例中，处理器中的至少一个可以与用于系统控制逻辑的一个或多个控制器的逻辑集成在相同的管芯上。在一个实施例中，处理器中的至少一个可以与用于系统控制逻辑的一个或多个控制器的逻辑集成在相同的管芯上以形成系统芯片。

[111]可以以一种或多种程序设计语言或其组合来编写用于执行本发明操作的计算机程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如 Java、Smalltalk、C++，还包括常规的过程式程序设计语言—诸如“C”语言或类似的设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)连接到用户计算机，或者，可以连接到外部计算机（例如利用因特网服务提供商来通过因特网连接）。

[112]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，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[113]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。

[114]以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明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。

权利要求书

1、一种数据处理方法，应用于包括数据提供方和 N 个多方安全计算 MPC 计算方的系统，所述 N 为 3 以上的整数，所述方法包括：

各 MPC 计算方从所述数据提供方发送的数据消息中获取第一数据分量，所述第一数据分量为所述数据提供方将隐私数据拆分后得到的多个数据分量中的部分数据分量，且所述第一数据分量为逻辑分量；

对所述第一数据分量进行从逻辑分量到算数分量的转换，得到第二数据分量用以进行 MPC 处理。

2、根据权利要求 1 所述的方法，其中，所述 N 个 MPC 计算方包括第一 MPC 计算方、第二 MPC 计算方和第三 MPC 计算方；

对所述逻辑分量进行转换得到算数分量包括：

各 MPC 计算方进行零共享处理，得到第三数据分量，所述第三数据分量为算数分量；

第一 MPC 计算方利用本地持有的逻辑分量进行算数值的第一转换和第二转换后，得到两个选择项，所述两个选择项为算数分量；

第一 MPC 计算方利用所述两个选择项向第三 MPC 计算方进行不经意传输；

各 MPC 计算方将本地得到的算数分量作为待分享数据进行算数共享处理，得到所述第二数据分量。

3、根据权利要求 2 所述的方法，其中，所述零共享处理包括：

各 MPC 计算方利用本地持有的第一零共享密钥生成第一派生值，以及本地持有的第二零共享密钥生成第二派生值；

利用所述第一派生值与所述第二派生值的差值，得到第三数据分量。

4、根据权利要求 2 所述的方法，其中，所述逻辑分量包括第一逻辑分量和第二逻辑分量；

所述第一 MPC 计算方利用本地持有的逻辑分量进行算数值的第一转换和第二转换包括：所述第一 MPC 计算方利用交互密钥生成随机值；利用本地持有的第一逻辑分量、第二逻辑分量、所述随机值以及所述 MPC 处理所采用定点数的小数位数进行所述第一转换和第二转换，得到两个选择项；

该方法还包括：所述第二 MPC 计算方利用所述交互密钥生成所述随机值。

5、根据权利要求 4 所述的方法，其中，所述第一转换和所述第二转换分别采用如下公式得到选择项 m_0 和 m_1 ：

$$m0=(0^{\wedge}u1^{\wedge}u2)\times(1<<B)-rnd$$

$$m1=(1^{\wedge}u1^{\wedge}u2)\times(1<<B)-rnd$$

其中, $\wedge$ 为异或运算符,

$<<$ 为左移运算符,

$u1$ 和 $u2$ 分别为第一逻辑分量和第二逻辑分量,

rnd 为所述随机值,

B 为所述 MPC 处理所采用定点数的小数位。

6、根据权利要求 2 所述的方法, 其中, 各 MPC 计算方利用本地得到的算数分量进行算数共享处理, 得到所述第二数据分量包括:

各 MPC 计算方将本地的待分享数据进行加密后分享给下一 MPC 计算方, 并接收上一 MPC 计算方分享来的数据并进行解密;

将解密后的数据与本地的待分享数据合并, 得到所述第二数据分量;

其中各 MPC 计算方按照环状次序进行所述分享处理。

7、一种数据处理方法, 应用于包括数据提供方和 N 个 MPC 计算方的系统, 所述 N 为 3 以上的整数, 所述方法包括:

所述数据提供方将隐私数据拆分为多个数据分量;

将所述多个数据分量通过数据消息分发给所述 N 个 MPC 计算方, 以使得各 MPC 计算方接收到所述多个数据分量中的部分数据分量作为第一数据分量, 所述第一数据分量为逻辑分量。

8、根据权利要求 7 所述的方法, 其中, 所述多个数据分量为 N 个数据分量;

将所述多个数据分量通过数据消息分发给所述 N 个 MPC 计算方包括: 向各 MPC 计算方分别发送两个数据分量, 且向其中任一个 MPC 计算方发送的第一个数据分量与向该 MPC 计算方的上一个 MPC 计算方发送的第二个数据分量相同;

各 MPC 计算方按环状排序。

9、一种数据处理装置, 应用于包括数据提供方和 N 个多方安全计算 MPC 计算方的系统, 所述 N 为 3 以上的整数; 所述装置设置于所述 MPC 计算方, 包括:

数据获取单元, 被配置为从所述数据提供方获取第一数据分量, 所述第一数据分量为所述数据提供方将隐私数据拆分后得到的多个数据分量中的部分数据分量, 且所述第一数据分量为逻辑分量;

算数转换单元, 被配置为对所述第一数据分量进行从逻辑分量到算数分量的转换, 得到第二数据分量用以进行 MPC 处理。

10、一种数据处理装置，应用于包括数据提供方和 N 个多方安全计算 MPC 计算方的系统，所述 N 为 3 以上的整数；所述装置设置于所述数据提供方，包括：

数据拆分单元，被配置为将隐私数据拆分为多个数据分量；

数据发送单元，被配置为将所述多个数据分量通过数据消息分发给所述 N 个 MPC 计算方，以使得各 MPC 计算方接收到所述多个数据分量中的部分数据分量作为第一数据分量，所述第一数据分量为逻辑分量。

11、一种计算设备，包括存储器和处理器，其特征在于，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 至 8 中任一项所述的方法。

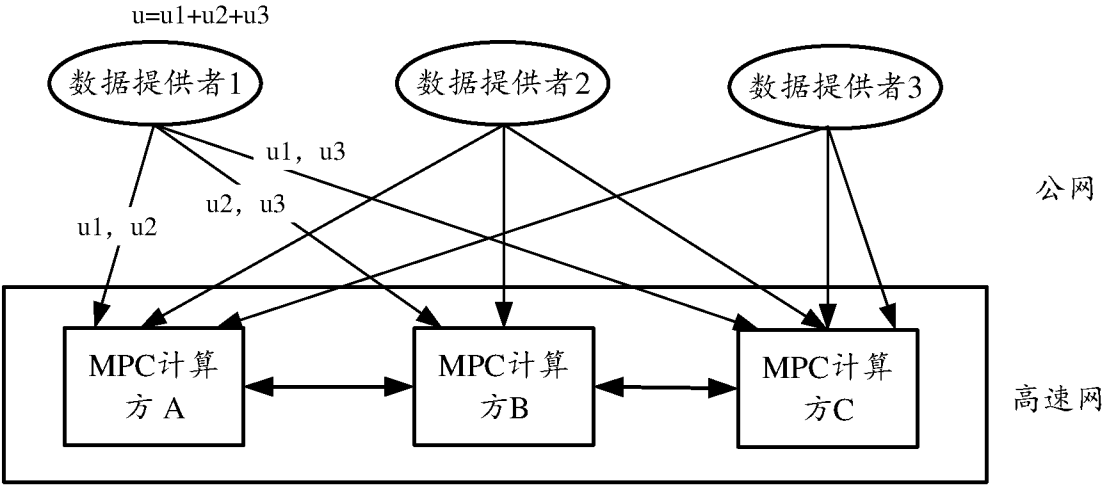


图 1

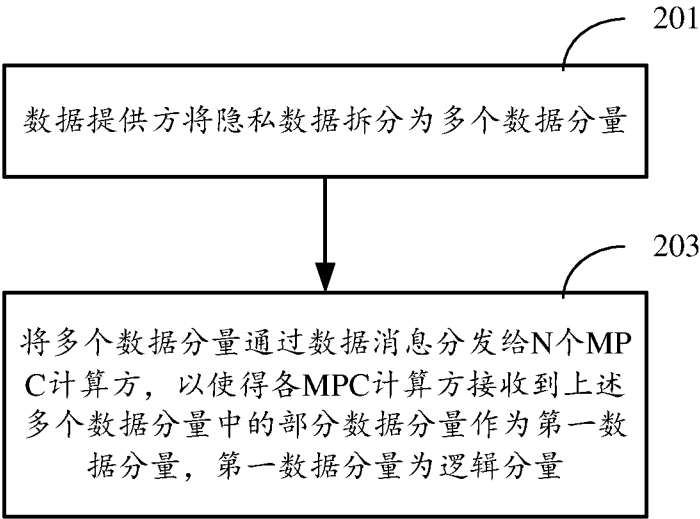


图 2

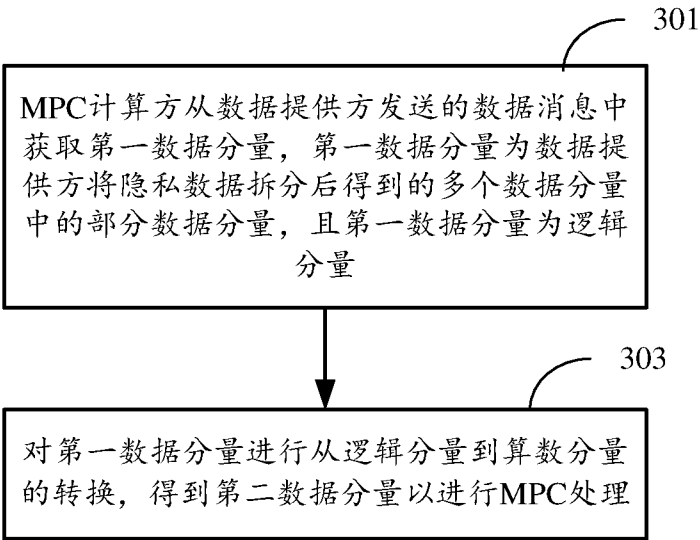


图 3

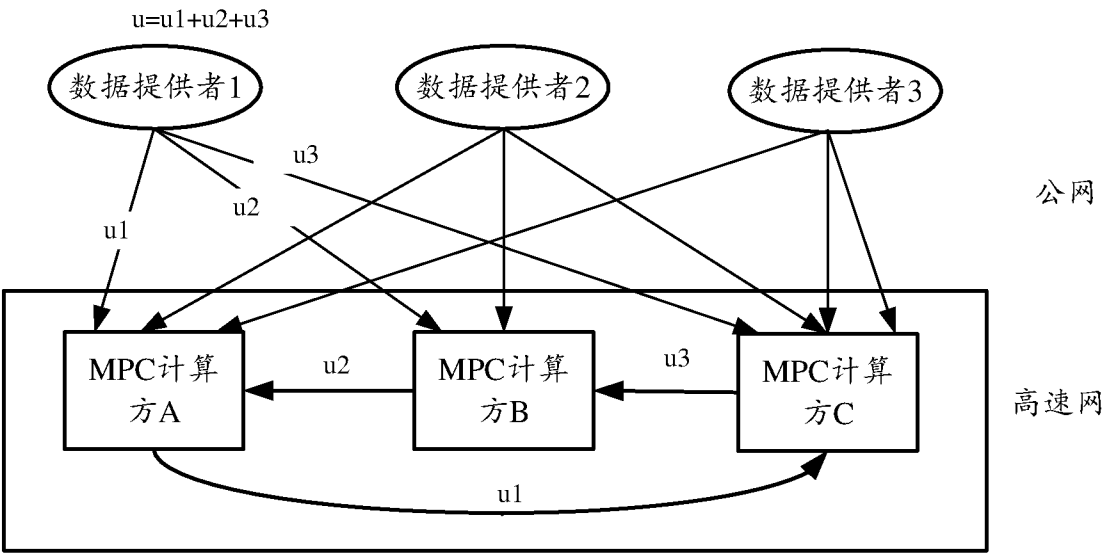


图 4

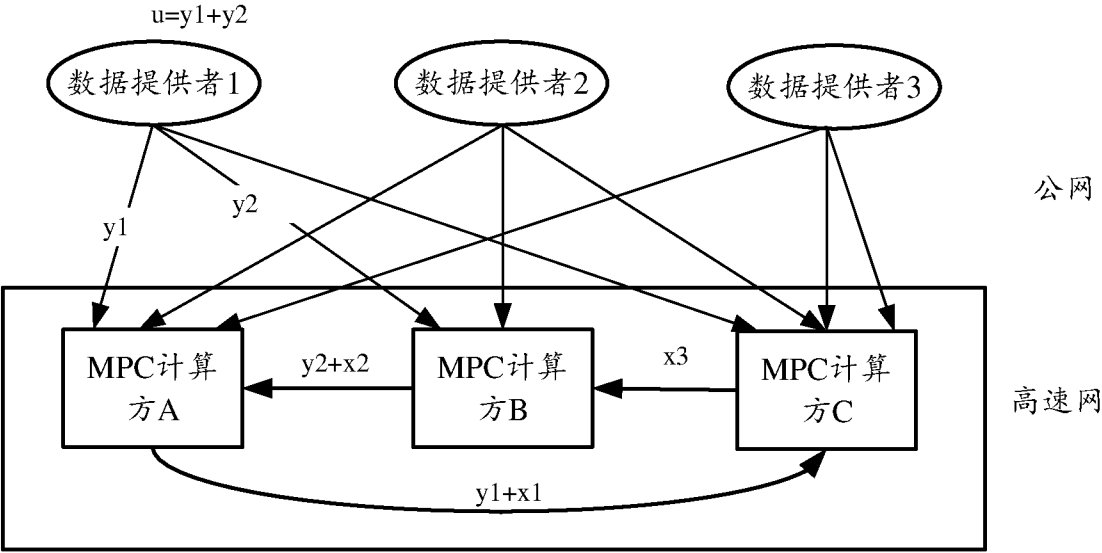


图 5

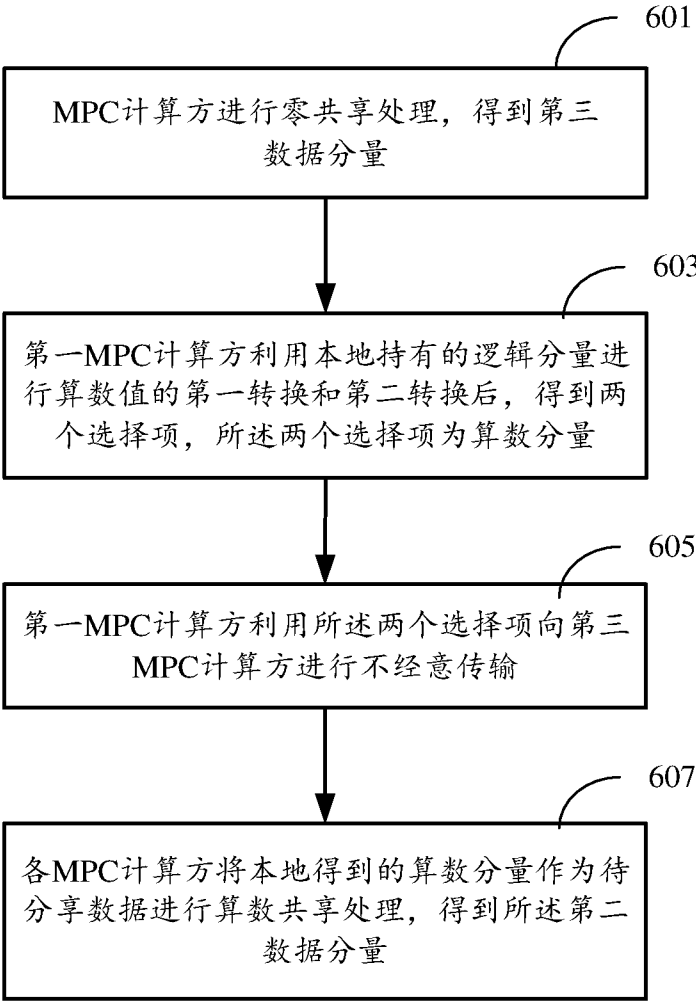


图 6

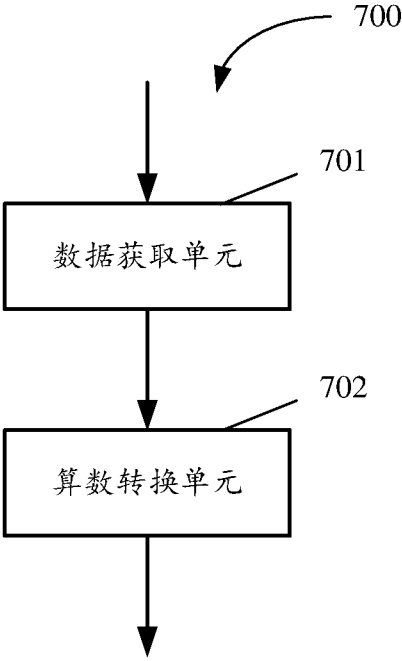


图 7

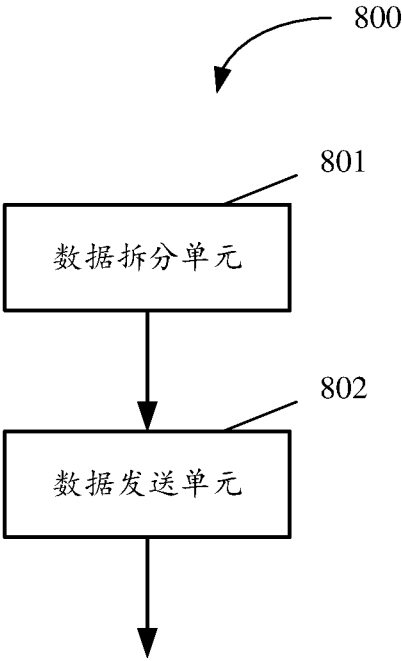


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/071505

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/40(2022.01);H04L9/08(2006.01);

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: H04L

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)

CNTXT; ENTXTC; WPABSC; VEN; ENTXT; CNKI; IEEE: 多方安全计算, 零共享, 不经意传输, 转换, 带宽, 通信量, MPC, zero sharing, Oblivious Transfer, convert, bandwidth, traffic

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 114726511 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 08 July 2022 (2022-07-08) claims 1-11, and description, paragraphs [0055]-[0146]	1-11
PX	CN 114726512 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 08 July 2022 (2022-07-08) claims 1-15, and description, paragraphs [0069]-[0231]	1-11
X	WO 2019231481 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 05 December 2019 (2019-12-05) description, paragraphs [0005]-[0470]	1, 7-11
A	CN 111049847 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 21 April 2020 (2020-04-21) entire document	1-11
A	CN 111737757 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 02 October 2020 (2020-10-02) entire document	1-11

☒ 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

11 May 2023

Date of mailing of the international search report

25 May 2023

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/071505**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 112688779 A (HUAKONG TSINGJIAO INFORMATION SCIENCE (BEIJING) CO., LTD.) 20 April 2021 (2021-04-20) entire document	1-11
A	CN 113708930 A (HANGZHOU QULIAN TECHNOLOGY CO., LTD.) 26 November 2021 (2021-11-26) entire document	1-11

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2023/071505

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	114726511	A	08 July 2022	None	
CN	114726512	A	08 July 2022	None	
WO	2019231481	A1	05 December 2019	None	
CN	111049847	A	21 April 2020	None	
CN	111737757	A	02 October 2020	None	
CN	112688779	A	20 April 2021	None	
CN	113708930	A	26 November 2021	None	

国际检索报告

国际申请号

PCT/CN2023/071505

A. 主题的分类

H04L9/40(2022.01)i;H04L9/08(2006.01)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: H04L

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))

CNTXT;ENTXTC;WPABSC;VEN;ENTXT;CNKI;IEEE:多方安全计算,零共享,不经意传输,转换,带宽,通信量,MPC, zero sharing, Oblivious Transfer, convert, bandwidth, traffic

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
PX	CN 114726511 A(支付宝(杭州)信息技术有限公司)2022年7月8日(2022-07-08) 权利要求1-11,说明书第[0055]-[0146]段	1-11
PX	CN 114726512 A(支付宝(杭州)信息技术有限公司)2022年7月8日(2022-07-08) 权利要求1-15,说明书第[0069]-[0231]段	1-11
X	WO 2019231481 A1(VISA INT SERVICE ASS)2019年12月5日(2019-12-05) 说明书第[0005]-[0470]段	1,7-11
A	CN 111049847 A(支付宝(杭州)信息技术有限公司)2020年4月21日(2020-04-21) 全文	1-11
A	CN 111737757 A(支付宝(杭州)信息技术有限公司)2020年10月2日(2020-10-02) 全文	1-11
A	CN 112688779 A(华控清交信息科技(北京)有限公司)2021年4月20日(2021-04-20) 全文	1-11
A	CN 113708930 A(杭州趣链科技有限公司)2021年11月26日(2021-11-26) 全文	1-11

☐ 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

2023年5月11日

国际检索报告邮寄日期

2023年5月25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

授权官员

张洁

电话号码(+86) 0512-88996056

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2023/071505

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	114726511	A	2022年7月8日	无	
CN	114726512	A	2022年7月8日	无	
WO	2019231481	A1	2019年12月5日	无	
CN	111049847	A	2020年4月21日	无	
CN	111737757	A	2020年10月2日	无	
CN	112688779	A	2021年4月20日	无	
CN	113708930	A	2021年11月26日	无	