

(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
2020 年 9 月 17 日 (17.09.2020)



(10) 国际公布号
WO 2020/181933 A1

(51) 国际专利分类号:
G06F 21/64 (2013.01)

(21) 国际申请号: PCT/CN2020/073818

(22) 国际申请日: 2020 年 1 月 22 日 (22.01.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910185759.4 2019 年 3 月 12 日 (12.03.2019) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: 林文珍 (LIN, Wenzhen); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。殷山 (YIN, Shan); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

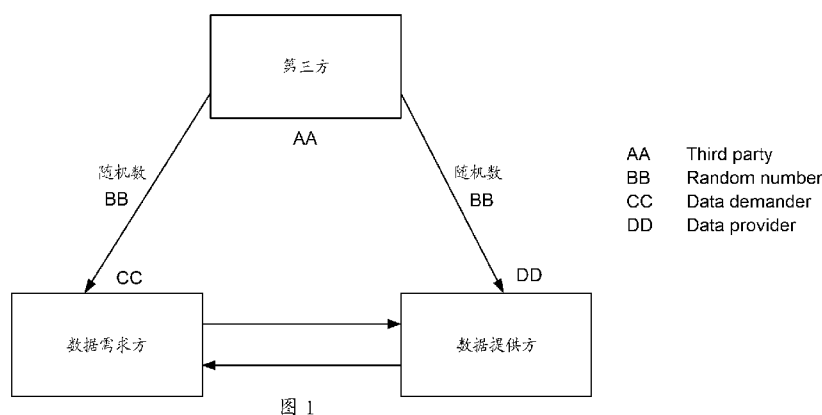
(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (CN)。

(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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,

(54) Title: SECURE MODEL PREDICTION METHOD AND DEVICE EMPLOYING SECRET SHARING TECHNIQUE

(54) 发明名称: 基于秘密分享的安全模型预测方法和装置



(57) Abstract: A secure model prediction method and device employing a secret sharing technique, the method comprising: receiving a first random number set from a third party; using the first random number set, a model coefficient vector, and a vector from a data provider to generate a shared calculation prediction result; and performing model prediction using the shared calculation prediction result. The method can protect private data of respective parties from leaking out, and ensure calculation accuracy.

(57) 摘要: 一种基于秘密分享的安全模型预测方法, 包括: 接收来自第三方的第一随机数集合; 使用所述第一随机数集合、模型系数向量和来自数据提供方的向量来生成共享计算预测结果; 以及使用所述共享计算预测结果进行模型预测。该方法能保护各方的私有数据不泄漏, 并且确保了计算的准确性。

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, 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))。

基于秘密分享的安全模型预测方法和装置

技术领域

[01] 本发明主要涉及多方数据合作，尤其涉及多方数据合作中的数据安全和模型安全。

背景技术

5 [02] 在数据分析、数据挖掘、经济预测等领域，模型可被用来分析、发现潜在的数据价值。但模型方所拥有的数据往往是不健全的，由此难以准确地刻画目标。为了得到更好的模型预测结果，通常模型方会与数据方进行数据合作，结合不同的数据或特征标签共同完成模型计算。

10 [03] 在多方数据合作过程中，涉及到数据安全和模型安全等问题。一方面，数据方不想输出自己的价值数据给模型方，泄漏私有数据；另一方面，模型中包含的特征标签（也称为模型系数）等信息也是模型方的私有数据，具有重要的商业价值，因此也要保证数据合作中的模型安全问题。

[04] 在现有技术中，存在三种多方数据合作的技术方案。第一种方案是数据方和模型方都将数据和模型放置在可信第三方，由第三方进行模型预测。但是其缺点是完全可信第
15 三方难以实现，并且在数据和模型的传输过程中存在安全风险。第二种方案是模型方对模型系数进行同态加密，将经加密的模型部署到数据方，数据方使用私有数据进行模型预测，然后将计算结果返回模型方。但这种方案由于同态加密的计算限制，对于计算的类型有限制，并且同态加密比较复杂，计算时间较长。第三种方案是使用 SGX (Software Guard Extension) 硬件结合机器学习和密码学，使用差分隐私技术对训练好的模型作系
20 数模糊。但使用差分隐私技术做模型系数模糊，模糊程度难以把握。对于需要得到精确计算结果的模型来说，会影响结果准确性。

[05] 因此，在多方数据合作中期望一种既保护数据和模型安全、又能得到精确计算结果的秘密分享方案。

发明内容

25 [06] 为解决上述技术问题，本发明提供了一种基于秘密分享的安全模型预测方法，包括：

[07] 接收来自第三方的第一随机数集合；

[08]使用所述第一随机数集合、模型系数向量和来自数据提供方的向量来生成共享计算预测结果；以及

[09]使用所述共享计算预测结果进行模型预测。

[10]可选地，所述生成共享计算预测结果包括：

5 [11]使用所述模型系数向量和所述第一随机数集合来生成中间模型向量；

[12]将所述中间模型向量发送给所述数据提供方并接收来自所述数据提供方的中间数据向量；

[13]使用来自所述数据提供方的所述中间数据向量和所述第一随机数集合来生成中间数据值；

10 [14]接收来自所述数据提供方的中间模型值；以及

[15]使用所述中间模型值和所述中间数据值来生成所述共享计算预测结果。

[16]可选地，所述共享计算预测结果是所述中间模型值和所述中间数据值的乘积。

[17]可选地，所述方法进一步包括：

[18]使用所述模型系数向量和本地存储的附加数据向量来生成第二共享计算预测结果；

15 以及

[19]使用所述共享计算预测结果和所述第二共享计算预测结果来进行模型预测。

[20]可选地，所述方法进一步包括：

[21]使用所述第一随机数集合、所述模型系数向量和来自第二数据提供方的向量来生成第二共享计算预测结果；以及

20 [22]使用所述共享计算预测结果和所述第二共享计算预测结果来进行模型预测。

[23]可选地，所述模型预测使用逻辑回归模型和/或线性回归模型。

[24]本申请的实施例还提供了一种基于秘密分享的安全模型预测方法，包括：

[25]接收来自第三方的第二随机数集合；

[26]使用所述第二随机数集合和数据向量来生成中间数据向量；

25 [27]将所述中间数据向量发送给数据需求方并接收来自所述数据需求方的中间模型向量；

[28]使用所述中间模型向量和所述第二随机数集合来生成中间数据值；以及

[29]将所述中间数据值提供给所述数据需求方以用于模型预测。

[30]本申请的实施例进一步提供了一种用于基于秘密分享的安全模型预测的装置,包括:

[31]接收模块,其被配置成接收来自第三方的第一随机数集合;

[32]预测向量生成模块,其被配置成使用所述第一随机数集合、模型系数向量和来自数据提供方的向量来生成共享计算预测结果; 以及

[33]模型预测模块,其被配置成使用所述共享计算预测结果进行模型预测。

[34]可选地,所述接收模块被进一步配置成接收来自所述数据提供方的中间数据向量和中间模型值;

[35]所述预测向量生成模块被进一步配置成:

10 [36]使用所述模型系数向量和所述第一随机数集合来生成中间模型向量;

[37]使用中间数据向量和所述第一随机数集合来生成中间数据值; 以及

[38]使用所述中间模型值和所述中间数据值来生成所述共享计算预测结果;

[39]所述装置进一步包括传送模块,其被配置成将所述中间模型向量发送给所述数据提供方。

15 [40]可选地,所述共享计算预测结果是所述中间模型值和所述中间数据值的乘积。

[41]可选地,所述预测向量生成模块被进一步配置成:

[42]使用所述模型系数向量和本地存储的附加数据向量来生成第二共享计算预测结果; 以及

[43]使用所述共享计算预测结果和所述第二共享计算预测结果来进行模型预测。

20 [44]可选地,所述预测向量生成模块被进一步配置成:

[45]使用所述第一随机数集合、所述模型系数向量和来自第二数据提供方的向量来生成第二共享计算预测结果; 以及

[46]使用所述共享计算预测结果和所述第二共享计算预测结果来进行模型预测。

[47]可选地,所述模型预测使用逻辑回归模型和/或线性回归模型。

25 [48]本申请的实施例还提供了一种用于基于秘密分享的安全模型预测的装置,包括:

[49]接收模块,其被配置成接收来自第三方的第二随机数集合,以及接收来自数据需求

方的中间模型向量;

[50]预测向量生成模块, 其被配置成使用所述第二随机数集合和数据向量来生成中间数据向量, 以及使用所述中间模型向量和所述第二随机数集合来生成中间数据值; 以及

5 [51]传送模块, 其被配置成将所述中间数据向量发送给数据需求方, 以及将所述中间数据值提供给所述数据需求方以用于模型预测。

[52]本申请的实施例进一步提供了一种基于秘密分享的安全模型预测装置, 包括:

[53]处理器; 以及

[54]被安排成存储计算机可执行指令的存储器, 所述可执行指令在被执行时使所述处理器执行以下操作:

10 [55]接收来自第三方的第一随机数集合;

[56]使用所述第一随机数集合、模型系数向量和来自数据提供方的向量来生成共享计算预测结果; 以及

[57]使用所述共享计算预测结果进行模型预测。

[58]本申请的实施例进一步提供了一种基于秘密分享的安全模型预测装置, 包括:

15 [59]处理器; 以及

[60]被安排成存储计算机可执行指令的存储器, 所述可执行指令在被执行时使所述处理器执行以下操作:

[61]接收来自第三方的第二随机数集合;

[62]使用所述第二随机数集合和数据向量来生成中间数据向量;

20 [63]将所述中间数据向量发送给数据需求方并接收来自所述数据需求方的中间模型向量;

[64]使用所述中间模型向量和所述第二随机数集合来生成中间数据值; 以及

[65]将所述中间数据值提供给所述数据需求方以用于模型预测。

[66]本发明提供了一种安全的去中心的模型预测方法, 达到了以下技术优点:

25 [67]1、数据不出各自边界, 不需要可信第三方进行数据融合, 也不需要任何一方的数据部署或引入到其他方, 即可完成模型预测。

[68]2、结合秘密分享, 保护合作各方的数据隐私。使用数据拆分的方式进行各方计算,

合作方不对另一方暴露自己的明文数据，只将各自拆分的不可识别数值做计算，得到最终的精准计算结果。

附图说明

[69]图 1 是根据本发明的各方面的基于秘密分享的多方数据合作系统的架构图。

5 [70]图 2 解说了根据本发明的各方面的一个数据需求方与一个数据提供方进行数据合作的示例。

[71]图 3 解说了根据本发明的各方面的一个数据需求方与两个数据提供方进行数据合作的示例。

10 [72]图 4 解说了根据本发明的各方面的由数据需求方执行的基于秘密分享的数据合作方法。

[73]图 5 解说了根据本发明的各方面的由数据需求方执行的基于秘密分享的数据合作方法。

[74]图 6 解说了根据本发明的各方面的由数据提供方执行的基于秘密分享的数据合作的示例方法。

15 [75]图 7 是根据本发明的各方面的数据需求方的框图。

[76]图 8 是根据本发明的各方面的数据提供方的框图。

具体实施方式

[77]为了让本发明的上述目的、特征和优点能更明显易懂，以下结合附图对本发明的具体实施方式作详细说明。

20 [78]在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是本发明还可以采用其它不同于在此描述的其它方式来实施，因此本发明不受下面公开的具体实施例的限制。

[79]图 1 是根据本发明的各方面的基于秘密分享的多方数据合作系统的架构图。

25 [80]如图 1 所示，本发明的基于秘密分享的多方数据合作系统包括数据需求方（也称为模型方）、数据提供方（也称为数据方）和第三方（公正第三方，例如，公正的司法机构或政府机关等）。

[81]数据需求方拥有模型，模型系数向量为 $W = \{\omega_1, \omega_2, \dots, \omega_n\}$ ，数据提供方拥有数据向量 $X = \{x_1, x_2, \dots, x_n\}$ ；第三方生成一系列随机数并分别分发给数据提供方和数据需求方。数据需求方使用模型系数和其获分配的随机数进行计算，数据提供方使用其拥有的数据和其获分配的随机数进行计算，数据需求方和数据提供方交换计算结果进行进一步处理，随后将结果汇总，得到模型预测结果。

[82]以下通过四个具体实施例来解说本发明的技术方案。

[83]实施例一

[84]参照图 2，解说了根据本发明的各方面的一个数据需求方与一个数据提供方进行数据合作的一个实施例。

10 [85]在步骤 201，第三方生成随机数集合 R_1 和 R_2 。

[86]例如， $R_1 = \{a, c_0\}$ ， $R_2 = \{b, c_1\}$ ，其中 a 和 b 是随机数向量， c_0 和 c_1 是随机数，并且 $c = a \times b$ ， $c = c_0 + c_1$ 。其中 $a \times b$ 是向量乘法。

[87]在步骤 202，第三方将随机数集合 R_1 和 R_2 分别发送给数据需求方和数据提供方。

15 [88]在步骤 203，数据需求方使用随机数集合 R_1 和模型系数向量 $W = \{\omega_1, \omega_2, \dots, \omega_n\}$ 进行计算，得到中间模型向量 e 。例如， $e = W - a$ 。

[89]在步骤 204，数据提供方使用随机数集合 R_2 和数据向量 $X = \{x_1, x_2, \dots, x_n\}$ 进行计算，得到中间数据向量 f 。例如， $f = X - b$ 。

[90]在步骤 205 和 206，数据需求方和数据提供方交换在步骤 203 和 204 中计算得到的结果。

20 [91]具体而言，数据需求方可在步骤 205 将计算结果 e 发送给数据提供方，并且数据提供方在步骤 206 将计算结果 f 发送给数据需求方。

[92]注意，虽然在图 2 中，步骤 205 在步骤 206 之前，但其次序可以交换，或者可以同时进行。

25 [93]在步骤 207，数据需求方使用随机数集合 R_1 和数据提供方在步骤 206 中提供的中间数据向量 f 进行计算，得到中间数据值 z_0 。例如， $z_0 = a \times f + c_0$ ，其中 $a \times f$ 是向量乘法。

[94]在步骤 208，数据提供方使用随机数集合 R_2 和数据需求方在步骤 205 中提供的中间模型向量进行计算，得到中间模型值 z_1 。例如， $z_1 = e \times X + c_1$ ，其中 $e \times X$ 是向量

乘法。

[95]在步骤 209, 数据提供方将 z_1 发送给数据需求方。

[96]在步骤 210, 数据需求方将 z_0 和 z_1 进行汇总, 得到模型系数与数据之积 $W \times X$, 其在本文也被称为共享计算预测结果。

5 [97]例如, $z = z_0 + z_1 = a \times f + c_0 + e \times X + c_1$

$$= a \times (X - b) + (W - a) \times X + c$$

$$= a \times X - a \times b + W \times X - a \times X + a \times b$$

$$= W \times X$$

[98]在步骤 211, 使用步骤 210 中得到的共享计算预测结果来进行模型预测。

10 [99]例如, 对于逻辑回归 (Logistic Regression) 模型, 计算 $\text{sigma}l = \frac{1}{1 + e^{-\omega * x + \lambda}}$, 其中 ω 、 λ 为模型系数, 由模型方提供。x 为计算所需的输入, 属于数据提供方的私有数据。

[100] 实施例二

[101] 在图 2 解说的实施例中, 数据需求方只提供了模型信息。在一些情形中, 数据需求方既具有模型信息 W , 又具有数据信息 X' 。

15 [102] 在这种情况下, 步骤 201-209 与图 2 中解说的实施例相同, 在此不再赘述。以下仅描述与图 2 的过程不同的地方。

[103] 在步骤 210, 数据需求方计算附加中间数据值 z_0' 。

$$z_0' = W \times X'.$$

[104] 在步骤 211, 数据需求方将 z_0 、 z_1 和 z_0' 汇总, 得到共享计算预测结果:

20 $z = z_0 + z_1 + z_0' = W \times X + W \times X'.$

[105] 在步骤 212, 使用 $W \times X + W \times X'$ 来进行模型预测。

[106] 实施例三

[107] 以上解说了一个数据需求方与一个数据提供方进行数据合作的实施例。在一些情形中, 数据需求方可能在模型预测中需要来自多个数据提供方的数据, 由此数据需求方需要与多个数据提供方进行数据合作。图 3 解说了一个数据需求方与两个数据提供方 (数据提供方 1 和数据提供方 2) 进行数据合作的示例。

25

[108] 在该实施例中，数据需求方具有模型 $W_A = \{\omega_{A1}, \omega_{A2}, \dots, \omega_{An}\}$ 和 $W_B = \{\omega_{B1}, \omega_{B2}, \dots, \omega_{Bn}\}$ ，数据提供方 1 具有数据 $X_A = \{x_{A1}, x_{A2}, \dots, x_{An}\}$ ，并且数据提供方 2 具有数据 $X_B = \{x_{B1}, x_{B2}, \dots, x_{Bn}\}$ 。在模型预测中需要共享计算预测结果 $W_A \times X_A$ 和 $W_B \times X_B$ 。

5 [109] 在步骤 301，第三方生成第一组随机数 $\{R_1, R_2\}$ 和第二组随机数 $\{R_1', R_2'\}$ ，其中第一组随机数用于数据需求方与数据提供方 1 的数据合作，而第二组随机数用于数据需求方与数据提供方 2 的数据合作。

[110] 具体而言， $R_1 = \{a, c0\}$ ， $R_2 = \{b, c1\}$ ，其中 $c = a \times b$ ， $c = c0 + c1$ ； $R_1' = \{a', c0'\}$ ， $R_2 = \{b', c1'\}$ ，其中 a, b 和 a', b' 是随机数向量， $c0, c1$ 和 $c0', c1'$ 是随机数，
10 并且 $c' = a' \times b'$ ， $c' = c0' + c1'$ 。请注意， $a \times b$ 和 $a' \times b'$ 是向量乘法。

[111] 在步骤 302，第三方将随机数集合 R_1 和 R_1' 提供给数据需求方，将 R_2 提供给数据提供方 1，将 R_2' 提供给数据提供方 2。

[112] 在步骤 303，数据需求方计算 e 和 e' 。

[113] 具体而言， $e = W_A - a$ ， $e' = W_B - a'$ 。

15 [114] 在步骤 304 和 305，数据提供方 1 和数据提供方 2 分别计算 $f = X_A - b$ 和 $f' = X_B - b'$ 。

[115] 在步骤 306-308，数据需求方和数据提供方 1、数据提供方 2 交换在步骤 303 - 305 中计算得到的结果。

[116] 具体而言，数据需求方在步骤 306 将计算结果 e 发送给数据提供方 1，在步骤
20 307 将计算结果 e' 发送给数据提供方 2。

[117] 数据提供方 1 在步骤 308 将计算结果 f 发送给数据需求方，在步骤 309 将计算结果 f' 发送给数据需求方。

[118] 注意，图 3 中示出了步骤 306-308 的特定次序，但这些步骤的次序可以交换，或者可以同时进行。

25 [119] 在步骤 310，数据需求方使用随机数集合 R_1 和数据提供方 1 在步骤 308 中提供的结算结果 f 进行计算，得到第一中间数据值 $z0$ 。例如， $z0 = a \times f + c0$ 。

[120] 数据需求方还使用随机数集合 R_1' 和数据提供方 2 在步骤 309 中提供的结算结果 f' 进行计算，得到第二中间数据值 $z0'$ 。例如， $z0' = a' \times f' + c0'$ 。

[121] 在步骤 311, 数据提供方 1 使用随机数集合 R_2 和数据需求方在步骤 306 中提供的计算结果 e 进行计算, 得到第一中间模型值 $z1$ 。例如, $z1 = e \times X_A + c1$ 。

[122] 在步骤 312, 数据提供方 2 使用随机数集合 R_2' 和数据需求方在步骤 307 中提供的计算结果 e' 进行计算, 得到第二中间模型值 $z1'$ 。例如, $z1' = e' \times X_B + c1'$ 。

5 [123] 在步骤 313 和 314, 数据提供方 1 将 $z1$ 发送给数据需求方, 数据提供方 2 将 $z1'$ 发送给数据需求方。

[124] 在步骤 315, 数据需求方将 $z0$ 和 $z1$ 进行汇总, 得到模型系数与数据之积 $W_A \times X$, 并且将 $z0'$ 和 $z1'$ 进行汇总, 得到模型系数与数据之积 $W_B \times X$ 。

[125] 例如, $z = z0 + z1 = a \times f + c0 + e \times X_A + c1$

$$\begin{aligned} 10 \quad &= a \times (X_A - b) + (W_A - a) \times X_A + c \\ &= a \times X_A - a \times b + W_A \times X_A - a \times X_A + a \times b \\ &= W_A \times X_A \end{aligned}$$

$$z' = z0' + z1' = a' \times f + c0' + e' \times X_B + c1'$$

$$\begin{aligned} &= a' \times (X_B - b) + (W_B - a') \times X_B + c' \\ 15 \quad &= a' \times X_B - a' \times b + W_B \times X_B - a' \times X_B + a' \times b \\ &= W_B \times X_B \end{aligned}$$

[126] 在步骤 316, 使用步骤 315 和 316 中的结果 (也称为共享计算预测结果) 来进行模型预测。

20 [127] 在一种实施例, 模型 W_A 和 W_B 可以是相同的, 换言之, 数据需求方使用一个模型 $W = W_A = W_B$ 和来自两个数据提供方的数据进行模型预测。

[128] 请注意, 图 3 中按照特定次序描述了一个数据需求方和两个数据提供方进行数据合作的过程, 但是步骤的其它次序也是可能的。数据需求方和数据提供方 1 之间的数据合作的各步骤与数据需求方和数据提供方 2 之间的数据合作的各步骤是独立的, 可以分别在不同时间完成。例如, 数据需求方和数据提供方 1 之间的数据合作的步骤可以在数据需求方和数据提供方 2 之间的数据合作之前或之后完成, 或者两个过程中的一些步骤可以是在时间上是交叉的。并且一些步骤可以进行拆分, 例如步骤 303 中的计算 e 和 e' 可以分开进行。

[129] 以上解说了一个数据需求方和两个数据提供方之间的数据合作, 该过程也可适

用于一个数据需求方和两个以上数据提供方之间的数据合作，其操作类似于图 3 中解说
的过程。

[130] 请注意，虽然本发明是以逻辑回归模型为例进行解说，但其它模型也可适用于
本发明，诸如线性回归模型， $y = \omega \times x + e$ ，等等。进一步，以上描述了两种具体的随
5 机数生成方法，但其它随机数生成方法也在本发明的范围内，本领域普通技术人员能够
根据实际需要构想出合适的随机数生成方法。

[131] 图 4 解说了根据本发明的各方面的由数据需求方执行的基于秘密分享的数据合
作方法的一个示例。

[132] 参见图 4，在步骤 401，接收来自第三方的第一随机数集合。

10 [133] 该步骤可以对应于以上参照图 2 描述的步骤 201、202，和/或参照图 3 描述的步
骤 301、302。

[134] 在步骤 402，使用所述第一随机数集合、模型系数向量和来自数据提供方的向量
来生成共享计算预测结果。

15 [135] 该步骤可以对应于以上参照图 2 描述的步骤 203 - 210，和/或参照图 3 描述的步
骤 303 - 315。

[136] 在步骤 403，使用共享计算预测结果进行模型预测。

[137] 该步骤可以对应于以上参照图 2 描述的步骤 211，和/或参照图 3 描述的步骤 303
- 316。

20 [138] 图 5 解说了根据本发明的各方面的由数据需求方执行的基于秘密分享的数据合
作方法的一个示例。

[139] 参见图 5，在步骤 501，接收来自第三方的第一随机数集合 R_1 。

[140] 具体而言，第三方可以生成随机数集合 $R = \{a, b, c_0, c_1\}$ ，其中 $c = a \times b$ ， $c = c_0$
+ c_1 ，其中所述第一随机数集合 R_1 为 $\{a, c_0\}$ ，而 $R_2 = \{b, c_1\}$ 被提供给数据提供方。

25 [141] 在另一示例中，第三方可以生成随机数集合 $R = \{a, b, c_0, c_1\}$ ，其中 $c = a_0 + a_1$ ，
 $c = b_0 + b_1$ ，其中第一随机数集合 $R_1 = \{a, c_0\}$ ，而 $R_2 = \{b, c_1\}$ 可被提供给数据提供方。

[142] 在步骤 502，使用模型系数向量 W 和第一随机数集合 R_1 来生成中间模型向量 e 。
例如， $e = W - a$ 。

[143] 在步骤 503, 将中间模型向量 e 发送给数据提供方并接收来自数据提供方的中间数据向量 f 。

[144] 在步骤 504, 使用中间数据向量 f 和所述第一随机数集合 R_1 来生成中间数据值 z_0 。

5 [145] 在步骤 505, 接收来自数据提供方的中间模型值 z_1 。

[146] 在步骤 506, 使用中间模型值 z_1 和中间数据值 z_0 来生成共享计算预测结果。

[147] 在步骤 507, 使用共享计算预测结果进行模型预测。

[148] 图 6 解说了根据本发明的各方面的由数据提供方执行的基于秘密分享的数据合作的示例方法。

10 [149] 在步骤 601, 接收来自第三方的第二随机数集合 R_2 。

[150] 在步骤 602, 使用第二随机数集合 R_2 和数据向量 X 来生成中间数据向量 f 。

[151] 在步骤 603, 将中间数据向量 f 发送给数据需求方并接收来自数据需求方的中间模型向量 e 。

[152] 在步骤 604, 使用中间模型向量 e 和第二随机数集合 R_2 来生成中间数据值 z_1 。

15 [153] 在步骤 605, 将中间数据值 z_1 提供给所述数据需求方以用于模型预测。

[154] 图 7 解说了根据本发明的各方面的数据需求方的框图。

[155] 具体而言, 数据需求方(模型方)可包括接收模块 701、预测向量生成模块 702、模型预测模块 703、传送模块 704、以及存储器 705。其中存储器 705 存储模型系数。

20 [156] 接收模块 701 可被配置成接收来自第三方的第一随机数集合, 接收来自所述数据提供方的中间数据向量和/或中间模型值。

[157] 预测向量生成模块 702 可被配置成使用所述第一随机数集合、模型系数向量和来自数据提供方的向量来生成共享计算预测结果。

25 [158] 具体而言, 预测向量生成模块 702 可被配置成使用所述模型系数向量和第一随机数集合来生成中间模型向量; 使用中间数据向量和第一随机数集合来生成中间数据值; 以及使用中间模型值和中间数据值来生成共享计算预测结果。

[159] 预测向量生成模块 702 还可被配置成使用模型系数向量和第一随机数集合来生成中间模型向量; 使用来自数据提供方的中间数据向量和中间模型向量来生成共享计算

预测结果。

[160] 模型预测模块 703 可被配置成使用共享计算预测结果进行模型预测。

[161] 传送模块 704 可被配置成将所述中间模型向量发送给所述数据提供方。

[162] 图 8 解说了根据本发明的各方面的数据提供方的框图。

5 [163] 具体而言，数据提供方可包括：接收模块 801、预测向量生成模块 802、传送模块 803 以及存储器 804。其中存储器 804 可存储私有数据。

[164] 接收模块 801 可被配置成接收来自第三方的第二随机数集合，以及接收来自数据需求方的中间模型向量。

10 [165] 预测向量生成模块 802 可被配置成使用所述第二随机数集合和数据向量来生成中间数据向量，以及使用所述中间模型向量和所述第二随机数集合来生成中间数据值。

[166] 传送模块 803 可被配置成将所述中间数据向量发送给数据需求方，以及将所述中间数据值提供给所述数据需求方以用于模型预测。

[167] 与现有技术相比，本发明具有以下优点：

15 [168] 1) 能够保护各方的私有数据不泄漏。各方持有的数据不出自己的计算边界，各方在本地通过加密方式的交互，完成计算。虽然有公正第三方参与，但第三方只提供随机数的分发，不参与具体的计算过程。

[169] 2) 对接成本不高。纯软件方案，除基本的服务器等，没有其他额外的硬件要求，不会引入其他硬件安全漏洞，可在线完成计算。

[170] 3) 计算完全无损，不影响结果准确性。

20 [171] 4) 算法本身不受限。计算结果实时返回，可支持加、减、乘、除等四则运算，及其混合计算，不因算法而受限制。

[172] 5) 秘密分享的安全多方计算算法，不需要保留密钥等信息，即可通过中间拆分、转换、结果汇总等方式，得到最终结果。而在分发随机数的第三方公正的前提下，计算过程中的中间值无法回推出原始明文。

25 [173] 本文结合附图阐述的说明描述了示例配置而不代表可被实现或者落在权利要求的范围内的所有示例。本文所使用的术语“示例性”意指“用作示例、实例或解说”，而并不意指“优于”或“胜过其他示例”。本详细描述包括具体细节以提供对所描述的

技术的理解。然而，可以在没有这些具体细节的情况下实践这些技术。在一些实例中，众所周知的结构和设备以框图形式示出以避免模糊所描述的示例的概念。

[174] 在附图中，类似组件或特征可具有相同的附图标记。此外，相同类型的各个组件可通过在附图标记后跟随短划线以及在类似组件之间进行区分的第二标记来加以区分。如果在说明书中仅使用第一附图标记，则该描述可应用于具有相同的第一附图标记的类似组件中的任何一个组件而不论第二附图标记如何。

[175] 结合本文中的公开描述的各种解说性框以及模块可以用设计成执行本文中描述的功能的通用处理器、DSP、ASIC、FPGA 或其他可编程逻辑器件、分立的门或晶体管逻辑、分立的硬件组件、或其任何组合来实现或执行。通用处理器可以是微处理器，但在替换方案中，处理器可以是任何常规的处理器、控制器、微控制器、或状态机。处理器还可被实现为计算设备的组合（例如，DSP 与微处理器的组合、多个微处理器、与 DSP 核心协同的一个或多个微处理器，或者任何其他此类配置）。

[176] 本文中所描述的功能可以在硬件、由处理器执行的软件、固件、或其任何组合中实现。如果在由处理器执行的软件中实现，则各功能可以作为一条或多条指令或代码存储在计算机可读介质上或藉其进行传送。其他示例和实现落在本公开及所附权利要求的范围内。例如，由于软件的本质，以上描述的功能可使用由处理器执行的软件、硬件、固件、硬连线或其任何组合来实现。实现功能的特征也可物理地位于各种位置，包括被分布以使得功能的各部分在不同的物理位置处实现。另外，如本文（包括权利要求中）所使用的，在项目列举（例如，以附有诸如“中的至少一个”或“中的一个或多个”之类的措辞的项目列举）中使用的“或”指示包含性列举，以使得例如 A、B 或 C 中的至少一个的列举意指 A 或 B 或 C 或 AB 或 AC 或 BC 或 ABC（即，A 和 B 和 C）。同样，如本文所使用的，短语“基于”不应被解读为引述封闭条件集。例如，被描述为“基于条件 A”的示例性步骤可基于条件 A 和条件 B 两者而不脱离本公开的范围。换言之，如本文所使用的，短语“基于”应当以与短语“至少部分地基于”相同的方式来解读。

[177] 计算机可读介质包括非瞬态计算机存储介质和通信介质两者，其包括促成计算机程序从一地向另一地转移的任何介质。非瞬态存储介质可以是能被通用或专用计算机访问的任何可用介质。作为示例而非限定，非瞬态计算机可读介质可包括 RAM、ROM、电可擦除可编程只读存储器（EEPROM）、压缩盘（CD）ROM 或其他光盘存储、磁盘存储或其他磁存储设备、或能被用来携带或存储指令或数据结构形式的期望程序代码手段且能被通用或专用计算机、或者通用或专用处理器访问的任何其他非瞬态介质。任何

连接也被正当地称为计算机可读介质。例如，如果软件是使用同轴电缆、光纤电缆、双绞线、数字订户线（DSL）、或诸如红外、无线电、以及微波之类的无线技术从 web 网站、服务器、或其它远程源传送而来的，则该同轴电缆、光纤电缆、双绞线、数字订户线（DSL）、或诸如红外、无线电、以及微波之类的无线技术就被包括在介质的定义之中。如本文所使用的盘（disk）和碟（disc）包括 CD、激光碟、光碟、数字通用碟（DVD）、软盘和蓝光碟，其中盘常常磁性地再现数据而碟用激光来光学地再现数据。以上介质的组合也被包括在计算机可读介质的范围内。

[178] 提供本文的描述是为了使得本领域技术人员能够制作或使用本公开。对本公开的各种修改对于本领域技术人员将是显而易见的，并且本文中定义的普适原理可被应用于其他变形而不会脱离本公开的范围。由此，本公开并非被限定于本文所描述的示例和设计，而是应被授予与本文所公开的原理和新颖特征相一致的最广范围。

权利要求书

1. 一种基于秘密分享的安全模型预测方法, 包括:

接收来自第三方的第一随机数集合;

使用所述第一随机数集合、模型系数向量和来自数据提供方的向量来生成共享计算

5 预测结果; 以及

使用所述共享计算预测结果进行模型预测。

2. 如权利要求 1 所述的方法, 其特征在于, 所述生成共享计算预测结果包括:

使用所述模型系数向量和所述第一随机数集合来生成中间模型向量;

将所述中间模型向量发送给所述数据提供方并接收来自所述数据提供方的中间数

10 据向量;

使用来自所述数据提供方的所述中间数据向量和所述第一随机数集合来生成中间数据值;

接收来自所述数据提供方的中间模型值; 以及

使用所述中间模型值和所述中间数据值来生成所述共享计算预测结果, 其中所述共

15 享计算预测结果是所述中间模型值和所述经处理中间数据值的乘积。

3. 如权利要求 2 所述的方法, 其特征在于, 进一步包括:

使用所述模型系数向量和本地存储的附加数据向量来生成第二共享计算预测结果;

以及

使用所述共享计算预测结果和所述第二共享计算预测结果来进行模型预测。

20 4. 如权利要求 2 所述的方法, 其特征在于, 进一步包括:

使用所述第一随机数集合、所述模型系数向量和来自第二数据提供方的向量来生成第二共享计算预测结果; 以及

使用所述共享计算预测结果和所述第二共享计算预测结果来进行模型预测。

25 5. 如权利要求 1 所述的方法, 其特征在于, 所述模型预测使用逻辑回归模型和/或线性回归模型。

6. 一种基于秘密分享的安全模型预测方法, 包括:

接收来自第三方的第二随机数集合;

使用所述第二随机数集合和数据向量来生成中间数据向量;

将所述中间数据向量发送给数据需求方并接收来自所述数据需求方的中间模型向

30 量;

使用所述中间模型向量和所述第二随机数集合来生成中间数据值; 以及

将所述中间数据值提供给所述数据需求方以用于模型预测。

7. 一种用于基于秘密分享的安全模型预测的装置，包括：

接收模块，其被配置成接收来自第三方的第一随机数集合；

预测向量生成模块，其被配置成使用所述第一随机数集合、模型系数向量和来自数

5 据提供方的向量来生成共享计算预测结果；以及

模型预测模块，其被配置成使用所述共享计算预测结果进行模型预测。

8. 如权利要求 7 所述的装置，其特征在于，所述接收模块被进一步配置成接收来自
所述数据提供方的中间数据向量和中间模型值；

所述预测向量生成模块被进一步配置成：

10 使用所述模型系数向量和所述第一随机数集合来生成中间模型向量；

使用中间数据向量和所述第一随机数集合来生成中间数据值；以及

使用所述中间模型值和所述中间数据值来生成所述共享计算预测结果，其中所述共
享计算预测结果是所述中间模型值和所述中间数据值的乘积；

15 所述装置进一步包括传送模块，其被配置成将所述中间模型向量发送给所述数据提
供方。

9. 如权利要求 7 所述的装置，其特征在于，所述预测向量生成模块被进一步配置成：

使用所述模型系数向量和本地存储的附加数据向量来生成第二共享计算预测结果；

以及

使用所述共享计算预测结果和所述第二共享计算预测结果来进行模型预测。

20 10. 如权利要求 7 所述的装置，其特征在于，所述预测向量生成模块被进一步配置
成：

使用所述第一随机数集合、所述模型系数向量和来自第二数据提供方的向量来生成
第二共享计算预测结果；以及

使用所述共享计算预测结果和所述第二共享计算预测结果来进行模型预测。

25 11. 如权利要求 7 所述的装置，其特征在于，所述模型预测使用逻辑回归模型和/
或线性回归模型。

12. 一种用于基于秘密分享的安全模型预测的装置，包括：

接收模块，其被配置成接收来自第三方的第二随机数集合，以及接收来自数据需求
方的中间模型向量；

30 预测向量生成模块，其被配置成使用所述第二随机数集合和数据向量来生成中间数
据向量，以及使用所述中间模型向量和所述第二随机数集合来生成中间数据值；以及

传送模块，其被配置成将所述中间数据向量发送给数据需求方，以及将所述中间数据值提供给所述数据需求方以用于模型预测。

13. 一种基于秘密分享的安全模型预测装置，包括：

处理器；以及

5 被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

接收来自第三方的第一随机数集合；

使用所述第一随机数集合、模型系数向量和来自数据提供方的向量来生成共享计算预测结果；以及

10 使用所述共享计算预测结果进行模型预测。

14. 一种基于秘密分享的安全模型预测装置，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

15 接收来自第三方的第二随机数集合；

使用所述第二随机数集合和数据向量来生成中间数据向量；

将所述中间数据向量发送给数据需求方并接收来自所述数据需求方的中间模型向量；

使用所述中间模型向量和所述第二随机数集合来生成中间数据值；以及

20 将所述中间数据值提供给所述数据需求方以用于模型预测。

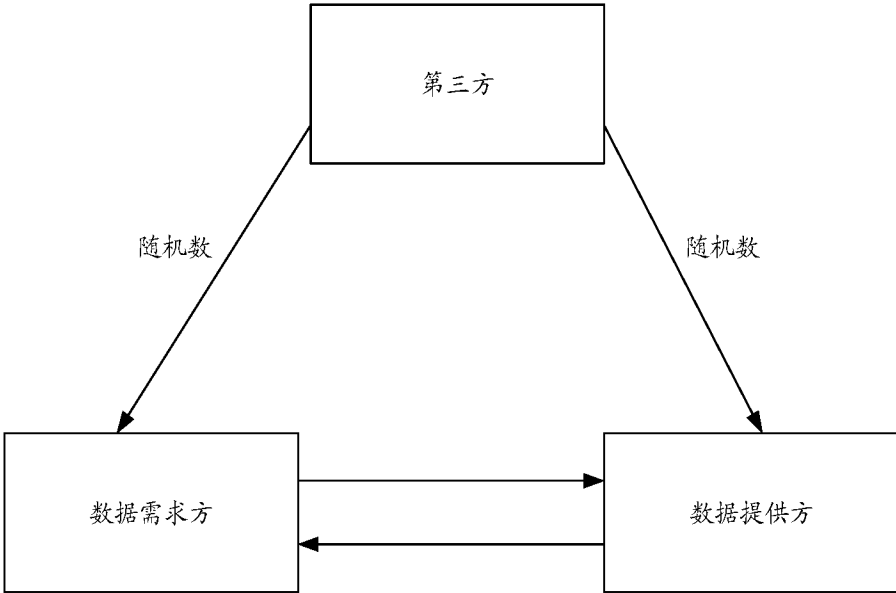


图 1

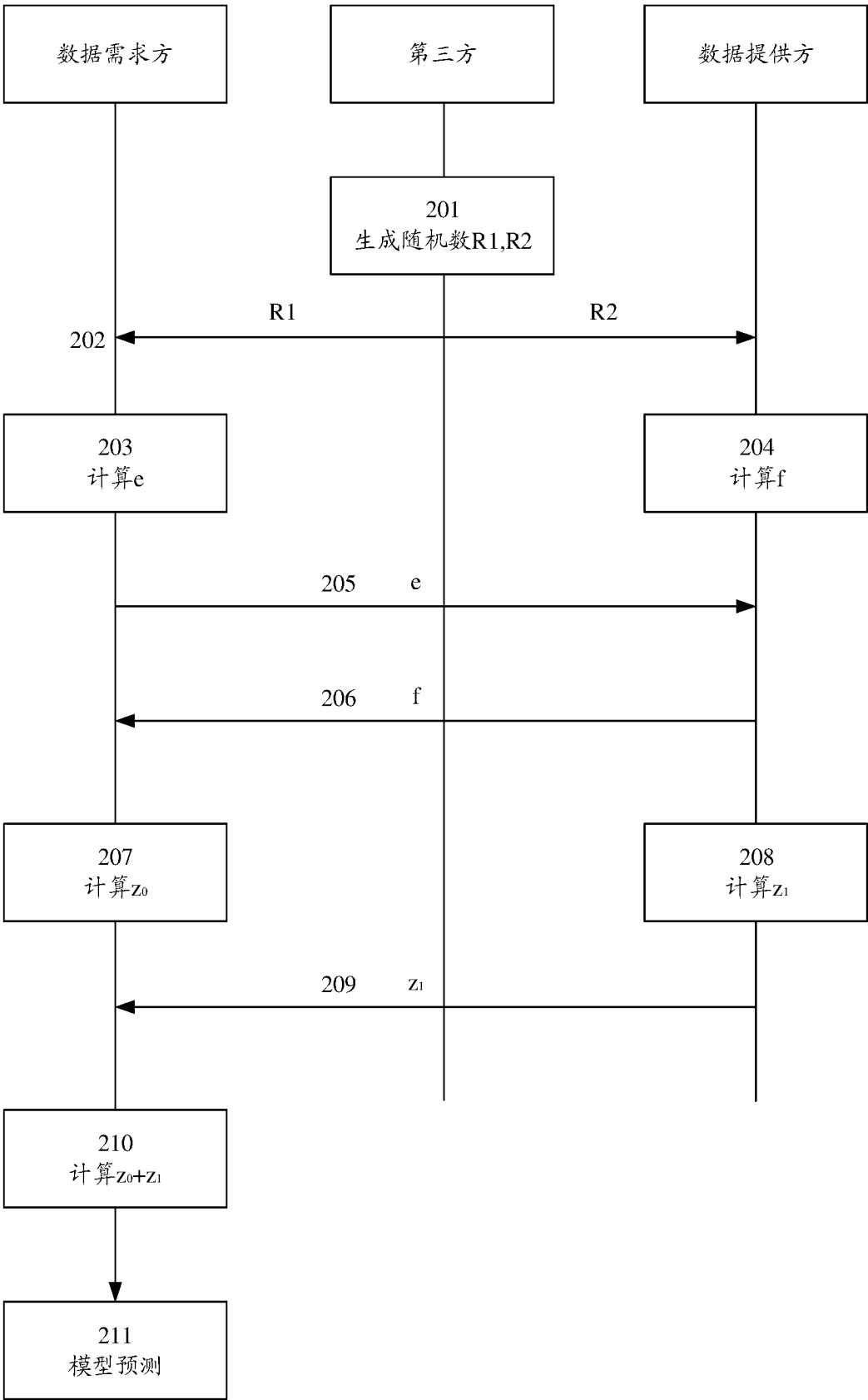


图 2

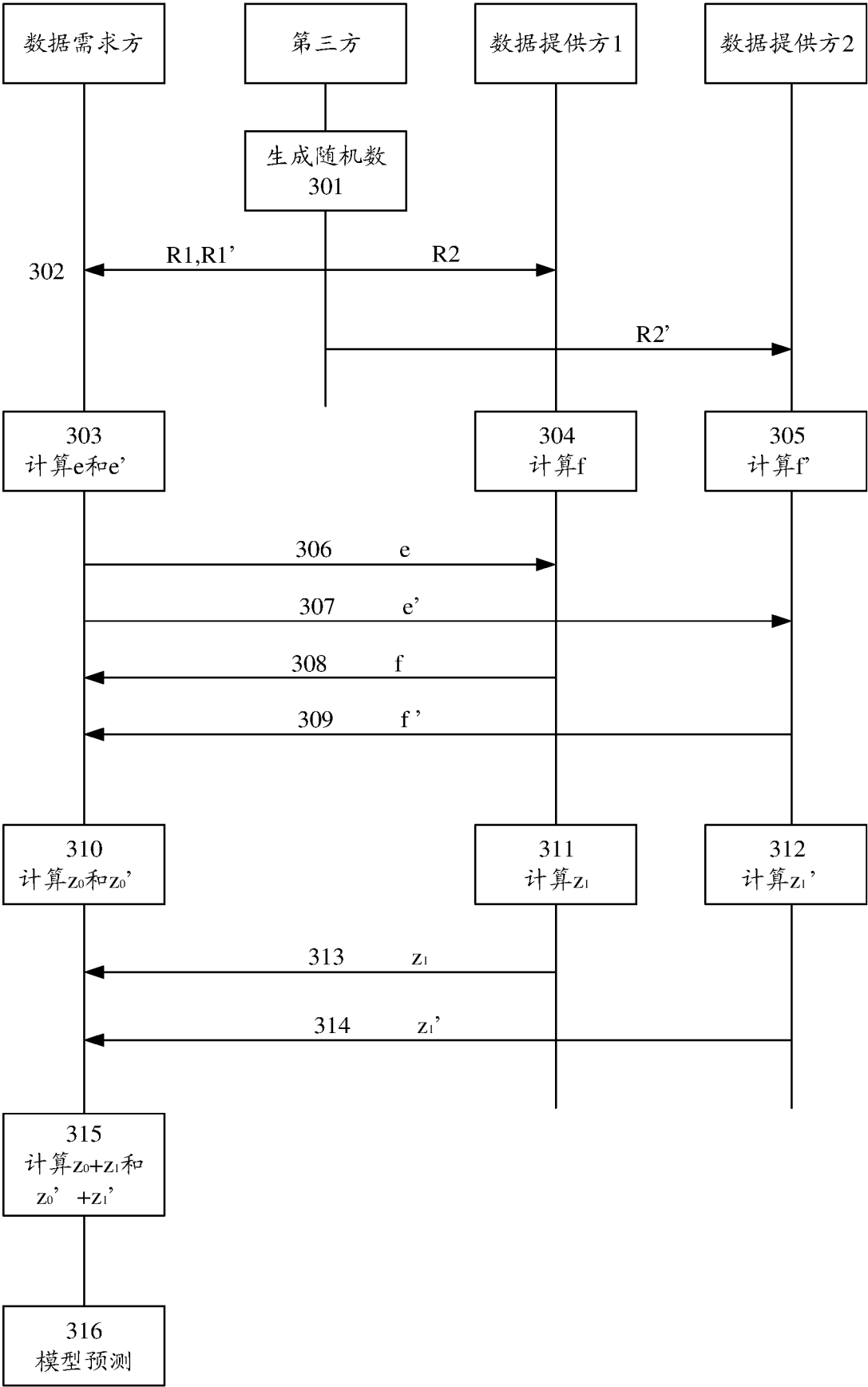


图 3

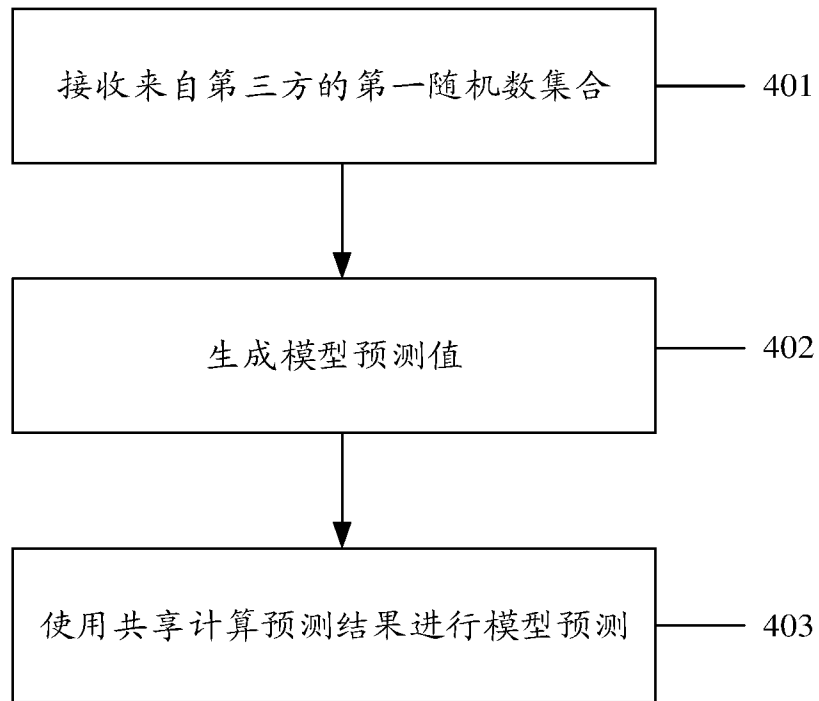


图 4

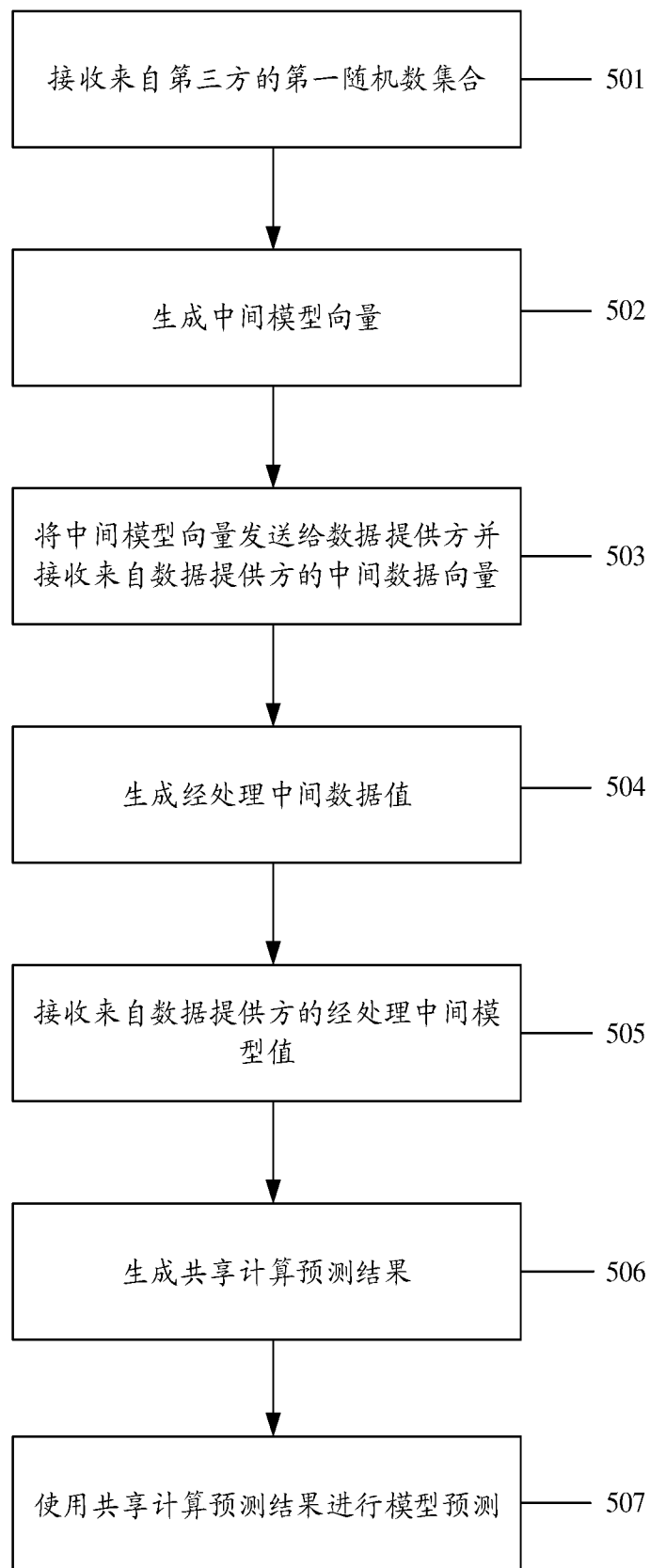


图 5

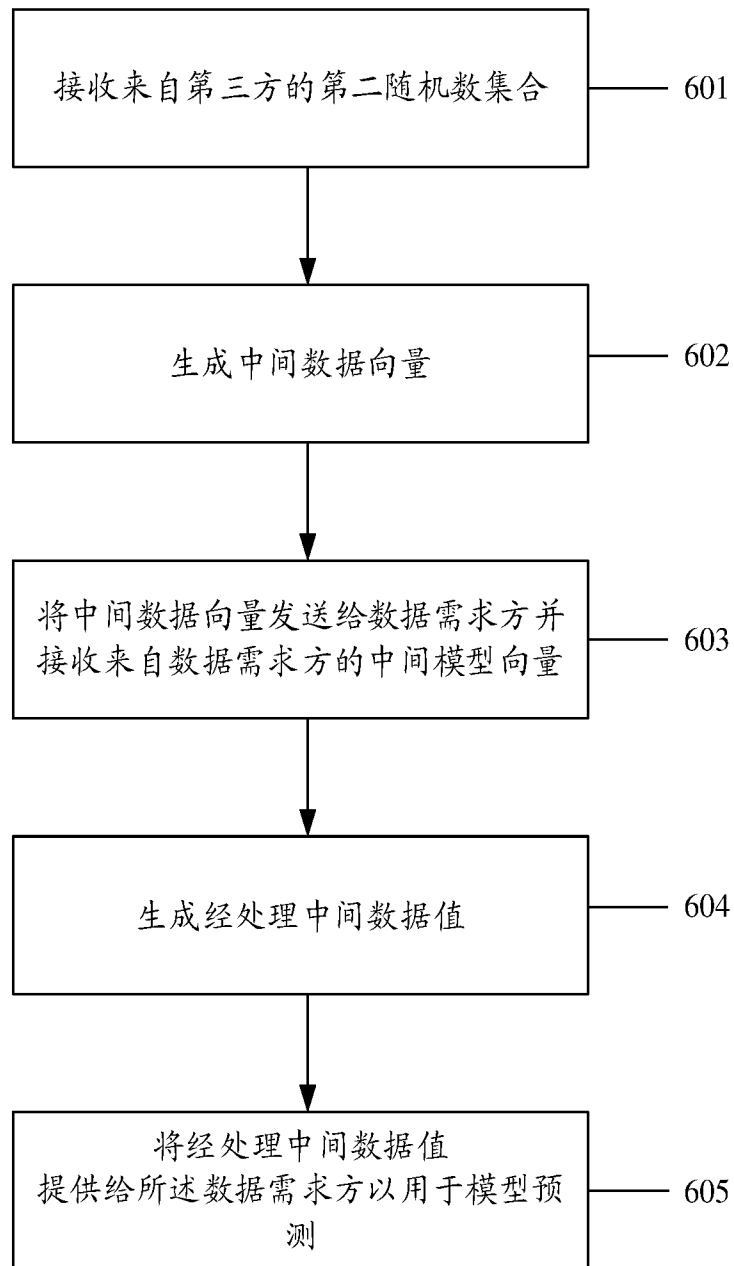


图 6

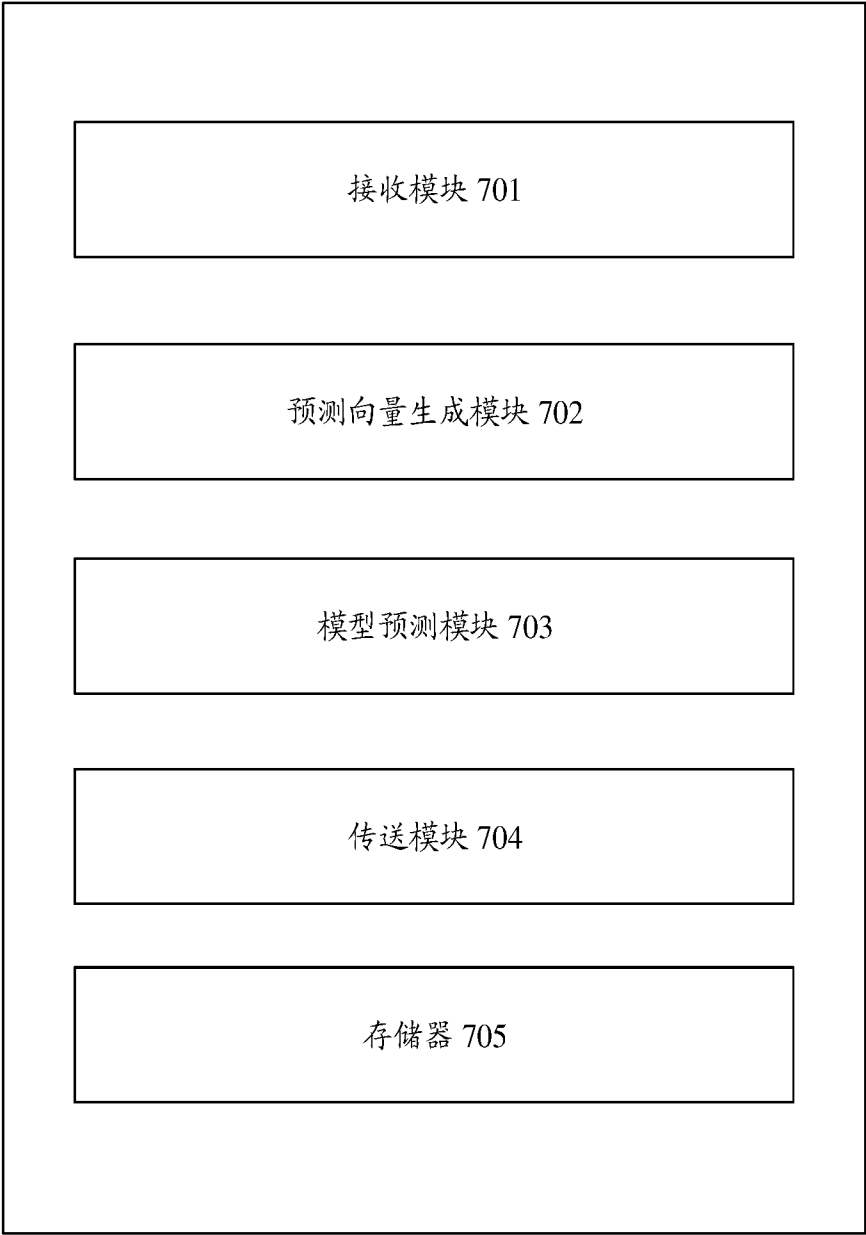


图 7

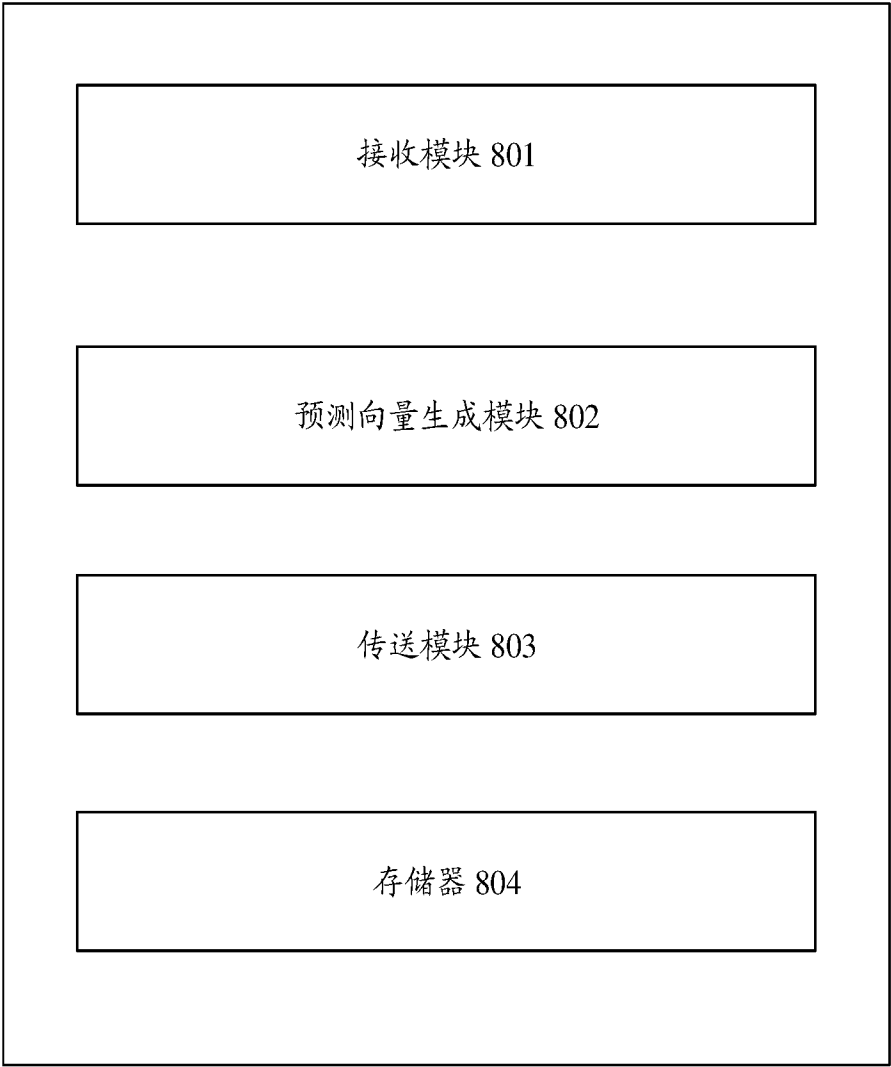


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/073818

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/64(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)

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)

CNPAT, CNKI, WPI, EPODOC: 随机数, 随机比特, 预测, 提供方, 模型, 需求方, 中间模型, 中间数据, random, bit, predict, forecast, provider, model, intermediate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2018359078 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC.) 13 December 2018 (2018-12-13) description, paragraphs 0015-0101, figure 3	1-14
Y	CN 108683669 A (SHENZHEN TURING SINGULARITY INTELLIGENT TECHNOLOGY CO., LTD. et al.) 19 October 2018 (2018-10-19) description, paragraphs 0138-0140	1-14
A	CN 109033854 A (ALIBABA GROUP HOLDING LIMITED) 18 December 2018 (2018-12-18) entire document	1-14
PX	CN 110032893 A (ALIBABA GROUP HOLDING LIMITED) 19 July 2019 (2019-07-19) claims 1-14	1-14



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

“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

05 April 2020

Date of mailing of the international search report

21 April 2020

Name and mailing address of the ISA/CN

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

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/073818

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2018359078	A1	13 December 2018	CN	110753926	A	04 February 2020
				WO	2018231445	A1	20 December 2018
				IN	201917049211	A	17 January 2020
CN	108683669	A	19 October 2018	None			
CN	109033854	A	18 December 2018	WO	2020015478	A1	23 January 2020
CN	110032893	A	19 July 2019	None			

国际检索报告

国际申请号

PCT/CN2020/073818

A. 主题的分类 G06F 21/64 (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) 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)) CNPAT, CNKI, WPI, EP0D0C: 随机数, 随机比特, 预测, 提供方, 模型, 需求方, 中间模型, 中间数据, random, bit, predict, forecast, provider, model, intermediate																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>Y</td> <td>US 2018359078 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC.) 2018年 12月 13日 (2018 - 12 - 13) 说明书第0015-0101段, 图3</td> <td>1-14</td> </tr> <tr> <td>Y</td> <td>CN 108683669 A (深圳市图灵奇点智能科技有限公司 等) 2018年 10月 19日 (2018 - 10 - 19) 说明书第0138-0140段</td> <td>1-14</td> </tr> <tr> <td>A</td> <td>CN 109033854 A (阿里巴巴集团控股有限公司) 2018年 12月 18日 (2018 - 12 - 18) 全文</td> <td>1-14</td> </tr> <tr> <td>PX</td> <td>CN 110032893 A (阿里巴巴集团控股有限公司) 2019年 7月 19日 (2019 - 07 - 19) 权利要求1-14</td> <td>1-14</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	Y	US 2018359078 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC.) 2018年 12月 13日 (2018 - 12 - 13) 说明书第0015-0101段, 图3	1-14	Y	CN 108683669 A (深圳市图灵奇点智能科技有限公司 等) 2018年 10月 19日 (2018 - 10 - 19) 说明书第0138-0140段	1-14	A	CN 109033854 A (阿里巴巴集团控股有限公司) 2018年 12月 18日 (2018 - 12 - 18) 全文	1-14	PX	CN 110032893 A (阿里巴巴集团控股有限公司) 2019年 7月 19日 (2019 - 07 - 19) 权利要求1-14	1-14
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
Y	US 2018359078 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC.) 2018年 12月 13日 (2018 - 12 - 13) 说明书第0015-0101段, 图3	1-14															
Y	CN 108683669 A (深圳市图灵奇点智能科技有限公司 等) 2018年 10月 19日 (2018 - 10 - 19) 说明书第0138-0140段	1-14															
A	CN 109033854 A (阿里巴巴集团控股有限公司) 2018年 12月 18日 (2018 - 12 - 18) 全文	1-14															
PX	CN 110032893 A (阿里巴巴集团控股有限公司) 2019年 7月 19日 (2019 - 07 - 19) 权利要求1-14	1-14															
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																	
<table border="0"> <tr> <td> * 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 “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 </td> <td> “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 </td> </tr> </table>			* 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 “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													
* 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 “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 2020年 4月 5日		国际检索报告邮寄日期 2020年 4月 21日															
ISA/CN的名称和邮寄地址 中国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 巩瑜 电话号码 86-(10)-53961382															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/073818

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)
US	2018359078	A1	2018年 12月 13日	CN	110753926	A	2020年 2月 4日
				WO	2018231445	A1	2018年 12月 20日
				IN	201917049211	A	2020年 1月 17日
CN	108683669	A	2018年 10月 19日	无			
CN	109033854	A	2018年 12月 18日	WO	2020015478	A1	2020年 1月 23日
CN	110032893	A	2019年 7月 19日	无			