

(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



(10) 国际公布号

WO 2021/027254 A1

(43) 国际公布日

2021 年 2 月 18 日 (18.02.2021)

(51) 国际专利分类号:

G06F 21/62 (2013.01)

(21) 国际申请号:

PCT/CN2020/071432

(22) 国际申请日:

2020 年 1 月 10 日 (10.01.2020)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

201910734775.4 2019 年 8 月 9 日 (09.08.2019) CN

(71) 申请人: 创新先进技术有限公司 (ADVANCED

NEW TECHNOLOGIES CO., LTD.) [—/CN]; 开曼

群岛大开曼岛乔治镇医院路 27 号开曼企业

中心, Grand Cayman KY1-9008 (KY)。

(72) 发明人: 周亚顺 (ZHOU, Yashun); 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)。 李漓春

(LI, Lichun); 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)。

王华忠 (WANG, Huazhong); 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,

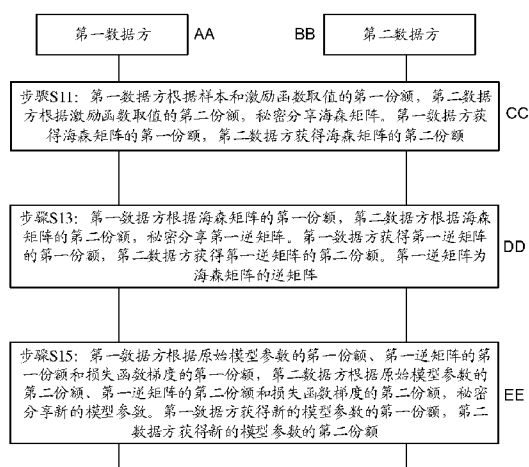
Beijing 100085 (CN)。

(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,

(54) Title: MODEL PARAMETER DETERMINATION METHOD AND APPARATUS, AND ELECTRONIC DEVICE

(54) 发明名称: 模型参数确定方法、装置和电子设备



AA First data party
BB Second data party
CC Step S11: the first data party and the second data party secretly share a Hessian matrix according to a sample and a first share of an excitation function value and according to a second share of the excitation function value respectively. The first data party obtains the first share of the Hessian matrix, and the second data party obtains the second share of the Hessian matrix
DD Step S13: the first data party and the second data party secretly share a first inverse matrix according to the first share of the Hessian matrix and according to the second share of the Hessian matrix respectively. The first data party obtains the first share of the first inverse matrix, and the second data party obtains the second share of the first inverse matrix. The first inverse matrix is an inverse matrix of the Hessian matrix
EE Step S15: the first data party and the second data party secretly share new model parameters according to the first share of original model parameters, the first share of the first inverse matrix and the first share of a loss function gradient, and according to the second share of the original model parameters, the second share of the first inverse matrix and the second share of the loss function gradient respectively. The first data party obtains the first share of the new model parameters, and the second party obtains the second share of the new model parameters

图 2

(57) Abstract: A model parameter determination method and apparatus, and an electronic device. The method comprises: secretly sharing a Hessian matrix with a partner according to feature data and the share of an excitation function value to obtain the share of the Hessian matrix; secretly sharing a first inverse matrix with the partner according to the share of the Hessian matrix to obtain the share of the first inverse matrix, the first inverse matrix being an inverse matrix of the Hessian matrix; and secretly sharing new model parameters with the partner according to the share of original model parameters, the share of the first inverse matrix and the share of a loss function gradient to obtain the share of the new model parameters.

(57) 摘要: 一种模型参数确定方法、装置和电子设备。所述方法包括: 根据特征数据和激励函数取值的份额与合作方秘密分享海森矩阵, 得到海森矩阵的份额; 根据海森矩阵的份额与合作方秘密分享第一逆矩阵, 得到第一逆矩阵的份额, 所述第一逆矩阵为海森矩阵的逆矩阵; 根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数, 得到新的模型参数的份额。

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, 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))。

模型参数确定方法、装置和电子设备

技术领域

[01]本说明书实施例涉及计算机技术领域，特别涉及一种模型参数确定方法、装置和电子设备。

5 背景技术

[02]大数据时代，存在非常多的数据孤岛。数据通常分散存于不同的企业中，企业与企业之间由于竞争关系和隐私保护的考虑，并不是完全的互相信任。在一些情况下，企业与企业之间需要进行合作安全建模，以便在充分保护企业数据隐私的前提下，利用各方的数据对数据处理模型进行协作训练。

- 10 [03]在对数据处理模型进行协作训练的过程中，可以利用模型参数优化方法对数据处理模型的模型参数进行多次优化调整。由于用于对数据处理模型进行训练的数据是分散在合作建模的各方的，因此如何在保护数据隐私的条件下，协作确定数据处理模型的模型参数，是当前亟需解决的技术问题。

发明内容

- 15 [04]本说明书实施例的目的是提供一种模型参数确定方法、装置和电子设备，以在保护数据隐私的前提下，由多方协作确定数据处理模型的模型参数。

[05]为实现上述目的，本说明书中一个或多个实施例提供的技术方案如下。

- [06]根据本说明书一个或多个实施例的第一方面，提供了一种模型参数确定方法，应用于第一数据方，包括：根据特征数据和激励函数取值的份额与合作方秘密分享海森矩阵，
20 得到海森矩阵的份额；根据海森矩阵的份额与合作方秘密分享第一逆矩阵，得到第一逆矩阵的份额，所述第一逆矩阵为海森矩阵的逆矩阵；根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数，得到新的模型参数的份额。

- [07]根据本说明书一个或多个实施例的第二方面，提供了一种模型参数确定装置，应用于
25 第一数据方，包括：第一秘密分享单元，用于根据特征数据和激励函数取值的份额与合作方秘密分享海森矩阵，得到海森矩阵的份额；第二秘密分享单元，用于根据海森矩

阵的份额与合作方秘密分享第一逆矩阵,得到第一逆矩阵的份额,所述第一逆矩阵为海森矩阵的逆矩阵;第三秘密分享单元,用于根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数,得到新的模型参数的份额。

[08]根据本说明书一个或多个实施例的第三方面,提供了一种电子设备,包括:存储器,

5 用于存储计算机指令;处理器,用于执行所述计算机指令以实现如第一方面所述的方法步骤。

[09]根据本说明书一个或多个实施例的第四方面,提供了一种模型参数确定方法,应用于第二数据方,包括:根据激励函数取值的份额与合作方秘密分享海森矩阵,得到海森矩阵的份额;根据海森矩阵的份额与合作方秘密分享第一逆矩阵,得到第一逆矩阵的份
10 额,所述第一逆矩阵为海森矩阵的逆矩阵;根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数,得到新的模型参数的份额。

[10]根据本说明书一个或多个实施例的第五方面,提供了一种模型参数确定装置,应用于第二数据方,包括:第一秘密分享单元,用于根据激励函数取值的份额与合作方秘密分享海森矩阵,得到海森矩阵的份额;第二秘密分享单元,用于根据海森矩阵的份额与合作方秘密分享第一逆矩阵,得到第一逆矩阵的份额,所述第一逆矩阵为海森矩阵的逆
15 矩阵;第三秘密分享单元,用于根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数,得到新的模型参数的份额。

[11]根据本说明书一个或多个实施例的第六方面,提供了一种电子设备,包括:存储器,用于存储计算机指令;处理器,用于执行所述计算机指令以实现如第四方面所述的方法
20 步骤。

[12]由以上本说明书实施例提供的技术方案可见,本说明书实施例中,第一数据方和第二数据方可以利用秘密分享算法,在不泄漏自身所拥有的数据的前提下,协作确定数据处理模型的模型参数。另外,由于使用了牛顿法,因而本实施例的模型参数确定方法有较快的收敛速度,可以减少模型参数优化调整的次数,提高数据处理模型的训练效率。

25 附图说明

[13]为了更清楚地说明本说明书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,下面描述中的附图仅仅是本说明书中记载的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动性

的前提下，还可以根据这些附图获得其他的附图。

[14]图 1 为本说明书实施例一种模型参数确定系统的示意图；

[15]图 2 为本说明书实施例一种模型参数确定方法的流程图；

[16]图 3 为本说明书实施例一种模型参数确定方法的流程图；

5 [17]图 4 为本说明书实施例一种模型参数确定方法的流程图；

[18]图 5 为本说明书实施例一种模型参数确定装置的示意图；

[19]图 6 为本说明书实施例一种模型参数确定装置的示意图；

[20]图 7 为本说明书实施例一种电子设备的功能结构图。

具体实施方式

10 [21]下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本说明书保护的范围。应当理解，尽管在本说明书可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些
15 术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。

[22]模型参数优化方法可以包括梯度下降法、牛顿法等等。所述牛顿法可以包括原始牛顿法以及基于原始牛顿法的各种变形方法（诸如阻尼牛顿法、正则化牛顿法等等；正则化牛顿法是指附带了正则化项的牛顿法；正则化可以降低模型的复杂度和不稳定程度，
20 从而降低过拟合的危险）。考虑到相较于梯度下降法，牛顿法有着更快的收敛速度。因此若合作建模各方通过秘密分享的方式，利用牛顿法协作确定数据处理模型的模型参数，则不仅可以保护合作建模各方的数据隐私，还可以减少模型参数优化调整的次数，提高数据处理模型的训练效率。

[23]秘密分享（SS，Secret Sharing）是一种保护数据隐私安全的算法。多个数据方可以在不泄漏自身数据的前提下，使用秘密分享算法进行协作计算，得到秘密信息。每个数据方可以获得该秘密信息的一份份额。单个数据方无法恢复该秘密信息。只有多个数据方一同协作才能恢复该秘密信息。例如数据方 P_1 拥有数据 x_1 ，数据方 P_2 拥有数据 x_2 。

采用秘密分享算法，数据方 P_1 和数据方 P_2 可以进行协作计算，得到秘密信息 $y = y_1 + y_2 = x_1 x_2$ 。数据方 P_1 在计算后可以获得秘密信息 y 的份额 y_1 ，数据方 P_2 在计算后可以获得秘密信息 y 的份额 y_2 。

5 [24]在合作安全建模的场景中，出于保护数据隐私的考虑，多个数据方可以在不泄漏自身所拥有的数据的前提下，基于自身拥有的数据，对数据处理模型进行协作训练。所述数据处理模型包括但不限于逻辑回归模型和神经网络模型等。在对数据处理模型进行训练的过程中，可以利用模型参数优化方法对数据处理模型的模型参数进行优化调整。考虑到在合作安全建模的场景中，用于对数据处理模型进行训练的数据分散在合作建模的各数据方。因此在合作安全建模的场景中，所述模型参数优化方法可以采用秘密分享算
10 法来实现。

[25]损失函数（Loss Function）可以用于衡量数据处理模型的预测值与真实值之间不一致的程度。损失函数的值越小，表示数据处理模型的鲁棒性越好。所述损失函数包括但不限于对数损失函数（Logarithmic Loss Function）、平方损失函数（Square Loss）等。

15 [26]海森矩阵（Hessian Matrix），又称为黑塞矩阵、海瑟矩阵或海塞矩阵等，是损失函数的二阶偏导数所构成的方阵，用于表示损失函数的局部曲率。

[27]激励函数（Activation Function），又称为激活函数，可以用于构建数据处理模型。激励函数定义了给定输入下的输出。通过激励函数可以在数据处理模型中加入非线性因素，提高数据处理模型的表达能力。所述激励函数例如可以包括 Sigmoid 函数、Tanh 函数和 ReLU 函数等等。

20 [28]本说明书提供一种模型参数确定系统的实施例。

[29]请参阅图 1。在该实施例中，所述模型参数确定系统可以包括第一数据方、第二数据方和可信任的第三方（TTP, Trusted Third Party）。

[30]所述第三方可以为一个服务器；或者，还可以为包括多个服务器的服务器集群。所述第三方可以用于向所述第一数据方和所述第二数据方提供随机数。具体地，所述第三
25 方可以生成随机数矩阵，可以将所述随机数矩阵中的各个随机数拆分为两个份额，可以将其中一个份额作为第一份额，将其中另一个份额作为第二份额。所述第三方可以将所述随机数矩阵中各个随机数的第一份额形成的矩阵作为所述随机数矩阵的第一份额，将所述随机数矩阵中各个随机数的第二份额形成的矩阵作为所述随机数矩阵的第二份额；可以向所述第一数据方发送所述随机数矩阵的第一份额，可以向所述第二数据方发送所

述随机数矩阵的第二份额。其中，所述随机数矩阵的第一份额和所述随机数矩阵的第二份额的和等于所述随机数矩阵。

[31] 所述第一数据方和所述第二数据方分别为合作安全建模的双方。所述第一数据方可以为不拥有标签的数据方，所述第二数据方可以为拥有标签的数据方。例如，所述第一数据方可以拥有完整的特征数据，所述第二数据方可以拥有特征数据的标签。或者，所述
5 第一数据方可以拥有特征数据的一部分数据项，所述第二数据方可以拥有特征数据的另一部分数据项和标签。具体地，例如，特征数据可以包括用户的储蓄金额和借贷金额。所述第一数据方可以拥有用户的储蓄金额，所述第二数据方可以拥有用户的借贷金额和特征数据的标签。所述标签可以用于区分不同类型的特征数据，具体数值例如可以取自
10 0 和 1。这里的数据方可以为电子设备。所述电子设备可以包括个人计算机、服务器、手持设备、便携式设备、平板型设备、多处理器装置；或者，还可以包括由以上任何多个装置或设备所构成的集群等。另外，特征数据及其对应的标签共同构成了样本数据，样本数据可以用于对数据处理模型进行训练。

[32] 在合作安全建模的场景中，所述第一数据方和所述第二数据方可以分别获得原始模型参数的一份份额。这里可以将所述第一数据方获得份额作为原始模型参数的第一份额，
15 可以将所述第二数据方获得份额作为原始模型参数的第二份额。原始模型参数的第一份额和原始模型参数的第二份额的和等于原始模型参数。

[33] 所述第一数据方可以接收随机数矩阵的第一份额。所述第二数据方可以接收随机数矩阵的第二份额。所述第一数据方可以基于原始模型参数的第一份额、特征数据和随机
20 数矩阵的第一份额，所述第二数据方可以基于原始模型参数的第二份额、标签和随机数矩阵的第二份额，采用秘密分享的方式，协作确定新的模型参数。所述第一数据方和所述第二数据方可以分别获得新的模型参数的一份份额。具体过程可以参见后面的模型参数确定方法实施例。

[34] 本说明书还提供一种模型参数确定方法的实施例。

[35] 该实施例可以利用牛顿法来确定模型参数。请参阅图 2。该实施例可以包括以下步骤。
25

[36] 步骤 S11：第一数据方根据特征数据和激励函数取值的第一份额，第二数据方根据激励函数取值的第二份额，秘密分享海森矩阵。第一数据方获得海森矩阵的第一份额，第二数据方获得海森矩阵的第二份额。

[37]步骤 S13: 第一数据方根据海森矩阵的第一份额, 第二数据方根据海森矩阵的第二份额, 秘密分享第一逆矩阵。第一数据方获得第一逆矩阵的第一份额, 第二数据方获得第一逆矩阵的第二份额。第一逆矩阵为海森矩阵的逆矩阵。

[38]步骤 S15: 第一数据方根据原始模型参数的第一份额、第一逆矩阵的第一份额和损失函数梯度的第一份额, 第二数据方根据原始模型参数的第二份额、第一逆矩阵的第二份额和损失函数梯度的第二份额, 秘密分享新的模型参数。第一数据方获得新的模型参数的第一份额, 第二数据方获得新的模型参数的第二份额。

[39]下面介绍在实施例中涉及的一些术语。

[40] (一)、第一乘积、第二乘积和第三乘积。所述第一乘积可以为原始模型参数和特征数据之间的乘积。所述第二乘积可以为随机数矩阵和海森矩阵之间的乘积。所述第三乘积可以为海森矩阵的逆矩阵和损失函数梯度之间的乘积。

[41]在一些场景示例中, 所述第一乘积可以表示为 XW ; 其中, W 表示原始模型参数, 具体为原始模型参数构成的向量; X 表示特征数据, 具体为特征数据构成的矩阵。

[42]所述第二乘积可以表示为 HR , 其中, H 表示海森矩阵, R 表示随机数矩阵。

[43]所述第三乘积可以表示为 $H^{-1}dW$, 其中, H^{-1} 表示海森矩阵的逆矩阵, dW 表示损失函数的梯度, dW 为向量。

[44] (二)、第一逆矩阵和第二逆矩阵。鉴于海森矩阵为方阵, 因而可以对海森矩阵进行求逆处理, 可以将海森矩阵的逆矩阵作为第一逆矩阵。所述第二乘积可以为方阵, 因而可以对所述第二乘积进行求逆处理, 可以将所述第二乘积的逆矩阵作为第二逆矩阵。

[45]延续前面的场景示例, 所述第一逆矩阵可以表示为 H^{-1} , 所述第二逆矩阵可以表示为 $(HR)^{-1}$ 。

[46]在一些实施例中, 在步骤 S11 之前, 所述第一数据方可以根据特征数据和拥有的原始模型参数的第一份额, 所述第二数据方可以根据拥有的原始模型参数的第二份额, 秘密分享第一乘积。所述第一数据方和所述第二数据方可以分别获得所述第一乘积的一份份额。为了便于描述, 可以将所述第一数据方获得的份额作为第一乘积的第一份额, 可以将所述第二数据方获得的份额作为第一乘积的第二份额。第一乘积的第一份额和第一乘积的第二份额的和等于第一乘积。

[47]延续前面的场景示例，原始模型参数的第一份额可以表示为 $\langle W \rangle_0$ ，原始模型参数的第二份额可以表示为 $\langle W \rangle_1$ ， $\langle W \rangle_0 + \langle W \rangle_1 = W$ 。所述第一数据方可以根据 X 和 $\langle W \rangle_0$ ，所述第二数据方可以根据 $\langle W \rangle_1$ ，秘密分享第一乘积 XW 。所述第一数据方可以获得第一乘积的第一份额 $\langle XW \rangle_0$ ，所述第二数据方可以获得第一乘积的第二份额 $\langle XW \rangle_1$ 。 $\langle XW \rangle_0 + \langle XW \rangle_1 = XW$ 。

[48]进一步地，所述第一数据方还可以根据第一乘积的第一份额，所述第二数据方还可以根据第一乘积的第二份额，秘密分享多项式的取值。所述第一数据方和所述第二数据方可以分别获得所述多项式取值的一份份额。所述多项式可以用于拟合所述数据处理模型的激励函数。如此可以将所述第一数据方获得的份额作为激励函数取值的第一份额，可以将所述第二数据方获得的份额作为激励函数取值的第二份额。激励函数取值的第一份额和激励函数取值的第二份额的和等于激励函数的取值。当然，本说明书并不限于上述采用多项式拟合的方式实现对激励函数取值的秘密分享，还可以采用其它方式实现对激励函数取值的秘密分享。

[49]延续前面的场景示例，所述激励函数可以为 Sigmoid 函数。所述激励函数的取值可以表示为 $a = \text{sigmoid}(XW)$ 。所述激励函数取值的第一份额可以表示为 $\langle a \rangle_0$ ，所述激励函数取值的第二份额可以表示为 $\langle a \rangle_1$ 。其中， $\langle a \rangle_0 + \langle a \rangle_1 = a$ 。 $\langle a \rangle_0$ 、 $\langle a \rangle_1$ 和 a 分别为向量。

[50]进一步地，所述第一数据方还可以根据特征数据和激励函数取值的第一份额，所述第二数据方还可以根据标签和激励函数取值的第二份额，秘密分享损失函数的梯度。所述第一数据方和所述第二数据方可以分别获得所述损失函数梯度的一份份额。为了便于描述，可以将所述第一数据方获得的份额作为损失函数梯度的第一份额，可以将所述第二数据方获得的份额作为损失函数梯度的第二份额。损失函数梯度的第一份额和损失函数梯度的第二份额的和等于损失函数的梯度。

[51]延续前面的场景示例，所述第一数据方可以根据 X 和 $\langle a \rangle_0$ ，所述第二数据方可以根据标签 Y 和 $\langle a \rangle_1$ ，秘密分享损失函数的梯度 dW （具体为向量）。所述第一数据方可以获得损失函数梯度的第一份额 $\langle dW \rangle_0$ ，所述第二数据方可以获得损失函数梯度的第二份额 $\langle dW \rangle_1$ 。

[52]下面介绍所述第一数据方和所述第二数据方秘密分享损失函数 dW 的详细过程。

[53]所述第一数据方可以根据 X ，所述第二数据方可以根据 $\langle a \rangle_1$ ，秘密分享 $X^T \langle a \rangle_1$ 。

所述第一数据方可以获得 $\langle [X^T \langle a \rangle_1] \rangle_0$ ，所述第二数据方可以获得 $\langle [X^T \langle a \rangle_1] \rangle_1$ 。

$\langle [X^T \langle a \rangle_1] \rangle_0 + \langle [X^T \langle a \rangle_1] \rangle_1 = X^T \langle a \rangle_1$ 。

- 5 [54]所述第一数据方还可以根据 X ，所述第二数据方还可以根据标签 Y （具体为标签构成的向量），秘密分享 $X^T Y$ 。所述第一数据方可以获得 $\langle X^T Y \rangle_0$ ，所述第二数据方可以获得 $\langle X^T Y \rangle_1$ 。 $\langle X^T Y \rangle_0 + \langle X^T Y \rangle_1 = X^T Y$ 。

[55]所述第一数据方可以计算 $X^T \langle a \rangle_0$ ；可以计算 $X^T \langle a \rangle_0 + \langle [X^T \langle a \rangle_1] \rangle_0 - \langle X^T Y \rangle_0$ 作为损失函数梯度 dW 的第一份额 $\langle dW \rangle_0$ 。所述

- 10 第二数据方可以计算 $\langle [X^T \langle a \rangle_1] \rangle_1 - \langle X^T Y \rangle_1$ 作为损失函数梯度 dW 的第二份额 $\langle dW \rangle_1$ 。

$$\begin{aligned}
 dW &= \langle dW \rangle_0 + \langle dW \rangle_1 \\
 &= X^T \langle a \rangle_0 + \langle [X^T \langle a \rangle_1] \rangle_0 - \langle X^T Y \rangle_0 + \langle [X^T \langle a \rangle_1] \rangle_1 - \langle X^T Y \rangle_1 \\
 &= X^T \langle a \rangle_0 + X^T \langle a \rangle_1 - X^T Y \\
 &= X^T a - X^T Y \\
 &= X^T (a - Y)
 \end{aligned}$$

[56]在一些实施例，在步骤 S11 中，所述第一数据方可以根据特征数据和激励函数取值的第一份额，所述第二数据方可以根据激励函数取值的第二份额，秘密分享海森矩阵。

- 15 所述第一数据方和所述第二数据方可以分别获得所述海森矩阵的一份份额。为了便于描述，可以将所述第一数据方获得的份额作为所述海森矩阵的第一份额，可以将所述第二数据方获得的份额作为所述海森矩阵的第二份额。海森矩阵的第一份额和海森矩阵的第二份额的和等于海森矩阵。

- [57]具体地，所述第一数据方可以根据激励函数取值的第一份额，所述第二数据方可以根据激励函数取值的第二份额，秘密分享对角矩阵。所述第一数据方和所述第二数据方可以分别获得所述对角矩阵的一份份额。为了便于描述，可以将所述第一数据方获得的份额作为所述对角矩阵的第一份额，可以将所述第二数据方获得的份额作为所述对角矩阵的第二份额。对角矩阵的第一份额和对角矩阵的第二份额的和等于对角矩阵。如此所
- 20

述第一数据方可以根据特征数据和所述对角矩阵的第一份额,所述第二数据方可以根据所述对角矩阵的第二份额,秘密分享海森矩阵。所述第一数据方可以获得所述海森矩阵的第一份额,所述第二数据方可以获得所述海森矩阵的第二份额。

[58]延续前面的场景示例,所述第一数据方可以根据 $\langle a \rangle_0$,所述第二数据方可以根据

5 $\langle a \rangle_1$,秘密分享对角矩阵 RNN 。所述第一数据方可以获得对角矩阵的第一份额 RNN_0 ,所述第二数据方可以获得对角矩阵的第二份额 RNN_1 。

[59]下面介绍所述第一数据方和所述第二数据方秘密分享对角矩阵 RNN 的详细过程。

[60]所述第一数据方可以根据 $\langle a \rangle_0$,所述第二数据方可以根据 $\langle a \rangle_1$,秘密分享 $\langle a \rangle_0 \bullet \langle a \rangle_1$ 。所述第一数据方可以获得 $\langle [\langle a \rangle_0 \bullet \langle a \rangle_1] \rangle_0$,所述第二数据方可以获

10 得 $\langle [\langle a \rangle_0 \bullet \langle a \rangle_1] \rangle_1$ 。 $\langle [\langle a \rangle_0 \bullet \langle a \rangle_1] \rangle_0 + \langle [\langle a \rangle_0 \bullet \langle a \rangle_1] \rangle_1 = \langle a \rangle_0 \bullet \langle a \rangle_1$ 。其中,
•表示按位相乘运算。例如,向量 $m = (m_1, m_2, m_3)$,向量 $n = (n_1, n_2, n_3)$ 。那么,
 $m \bullet n = (m_1 n_1, m_2 n_2, m_3 n_3)$ 。

[61]所述第一数据方可以计算 $\langle r \rangle_0 = \langle a \rangle_0 - \langle [\langle a \rangle_0 \bullet \langle a \rangle_1] \rangle_0 - \langle a \rangle_0 \bullet \langle a \rangle_0$,所述第二数据方可以计算 $\langle r \rangle_1 = \langle a \rangle_1 - \langle [\langle a \rangle_0 \bullet \langle a \rangle_1] \rangle_0 - \langle a \rangle_1 \bullet \langle a \rangle_1$ 。

$$\begin{aligned} r &= \langle r \rangle_0 + \langle r \rangle_1 \\ &= \langle a \rangle_0 - \langle [\langle a \rangle_0 \bullet \langle a \rangle_1] \rangle_0 - \langle a \rangle_0 \bullet \langle a \rangle_0 + \langle a \rangle_1 - \langle [\langle a \rangle_0 \bullet \langle a \rangle_1] \rangle_0 - \langle a \rangle_1 \bullet \langle a \rangle_1 \\ &= \{ \langle a \rangle_0 + \langle a \rangle_1 \} \{ 1 - \langle a \rangle_0 - \langle a \rangle_1 \} \\ &= a(1-a) \end{aligned}$$

15

[62] $\langle r \rangle_0$ 、 $\langle r \rangle_1$ 和 r 分别为向量。因而所述第一数据方可以根据 $\langle r \rangle_0$ 生成对角矩阵 $RNN = \text{diag}(r)$ 的第一份额 $RNN_0 = \text{diag}(\langle r \rangle_0)$,所述第二数据方可以根据 $\langle r \rangle_1$ 生成对

角矩阵 $RNN = \text{diag}(r)$ 的第二份额 $RNN_1 = \text{diag}(\langle r \rangle_1)$ 。 $RNN_0 + RNN_1 = RNN$ 。其中,对

角矩阵 RNN 的第一份额 RNN_0 和第二份额 RNN_1 均可以为一个对角矩阵。在实际处理过

20

程中,所述第一数据方可以将 $\langle r \rangle_0$ 中的数据元素作为 RNN_0 主对角线上的数据元素,这样便实现了根据 $\langle r \rangle_0$ 生成 RNN_0 ;可以将 $\langle r \rangle_1$ 中的数据元素作为 RNN_1 主对角线上的数据元素,这样便实现了根据 $\langle r \rangle_1$ 生成 RNN_1 。

[63]所述第一数据方可以根据 X 和 RNN_0 ,所述第二数据方可以根据 RNN_1 ,秘密分享海

森矩阵 H 。所述第一数据方可以获得海森矩阵的第一份额 $\langle H \rangle_0$ ，所述第二数据方可以获得海森矩阵的第二份额 $\langle H \rangle_1$ 。

[64]下面介绍所述第一数据方和所述第二数据方秘密分享海森矩阵 H 的详细过程。

[65]所述第一数据方可以根据 X ，所述第二数据方可以根据 RNN_1 ，秘密分享 $X^T RNN_1$ 。

5 所述所述第一数据方可以获得 $\langle X^T RNN_1 \rangle_0$ ，所述第二数据方可以获得 $\langle X^T RNN_1 \rangle_1$ 。
 $\langle X^T RNN_1 \rangle_0 + \langle X^T RNN_1 \rangle_1 = X^T RNN_1$ 。

[66]所述第一数据方还可以根据 X ，所述第二数据方还可以根据 $\langle X^T RNN_1 \rangle_1$ ，秘密分享 $\langle X^T RNN_1 \rangle_1 X$ 。所述第一数据方可以获得 $\langle [\langle X^T RNN_1 \rangle_1 X] \rangle_0$ ，所述第二数据方可以获得 $\langle [\langle X^T RNN_1 \rangle_1 X] \rangle_1$ 。
 $\langle [\langle X^T RNN_1 \rangle_1 X] \rangle_0 + \langle [\langle X^T RNN_1 \rangle_1 X] \rangle_1 = \langle X^T RNN_1 \rangle_1 X$ 。

10 [67]所述第一数据方可以计算 $X^T RNN_0 X + \langle X^T RNN_1 \rangle_0 X + \langle [\langle X^T RNN_1 \rangle_1 X] \rangle_0$ 作为海森矩阵 H 的第一份额 $\langle H \rangle_0$ 。所述第二数据方可以将 $\langle [\langle X^T RNN_1 \rangle_1 X] \rangle_1$ 作为海森矩阵 H 的第二份额 $\langle H \rangle_1$ 。

$$\begin{aligned} H &= \langle H \rangle_0 + \langle H \rangle_1 \\ &= X^T RNN_0 X + \langle X^T RNN_1 \rangle_0 X + \langle [\langle X^T RNN_1 \rangle_1 X] \rangle_0 + \langle [\langle X^T RNN_1 \rangle_1 X] \rangle_1 \\ &= X^T RNN_0 X + \langle X^T RNN_1 \rangle_0 X + \langle X^T RNN_1 \rangle_1 X \\ &= X^T RNN_0 X + X^T RNN_1 X \\ &= X^T RNN X \end{aligned}$$

[68]在一些实施例中，第三方可以向第一数据方下发随机数矩阵的第一份额；可以向第二数据方下发随机数矩阵的第二份额。随机数矩阵的第一份额和随机数矩阵的第二份额的和等于随机数矩阵。所述第一数据方可以接收随机数矩阵的第一份额，所述第二数据方可以接收随机数矩阵的第二份额。如此在步骤 S13 中，所述第一数据方可以根据随机数矩阵的第一份额和海森矩阵的第一份额，所述第二数据方可以根据随机数矩阵的第二份额和海森矩阵的第二份额，秘密分享第二乘积。所述第一数据方和所述第二数据方可以分别获得所述第二乘积的一份份额。为了便于描述，可以将所述第一数据方获得的份额作为第二乘积的第一份额，可以将所述第二数据方获得的份额作为第二乘积的第二份额。第二乘积的第一份额和第二乘积的第二份额的和等于第二乘积。

15

20

[69]在本实施例的一些实施方式中，可以由所述第二数据方对所述第二乘积进行求逆处

理。具体地，所述第一数据方可以向所述第二数据方发送第二乘积的第一份额。所述第二数据方可以接收第二乘积的第一份额；可以将第二乘积的第一份额与自身拥有的第二乘积的第二份额相加，得到第二乘积。鉴于所述第二乘积为方阵，因而所述第二数据方可以对所述第二乘积进行求逆处理，得到所述第二乘积的逆矩阵作为第二逆矩阵；可以向所述第一数据方发送所述第二逆矩阵。所述第一数据方可以接收所述第二逆矩阵。或者，在本实施例的另一些实施方式中，还可以由所述第一数据方对所述第二乘积进行求逆处理。具体地，所述第二数据方可以向所述第一数据方发送第二乘积的第二份额。所述第一数据方可以接收第二乘积的第二份额；可以将第二乘积的第二份额与自身拥有的第二乘积的第一份额相加，得到第二乘积。鉴于所述第二乘积为方阵，因而所述第一数据方可以对所述第二乘积进行求逆处理，得到所述第二乘积的逆矩阵作为第二逆矩阵；可以向所述第二数据方发送所述第二逆矩阵。所述第二数据方可以接收所述第二逆矩阵。

[70]所述第一数据方可以将随机数矩阵的第一份额与所述第二逆矩阵相乘，得到第一逆矩阵的第一份额。所述第二数据方可以将随机数矩阵的第二份额与所述第二逆矩阵相乘，得到第一逆矩阵的第二份额。第一逆矩阵的第一份额和第一逆矩阵的第二份额的和等于第一逆矩阵。

[71]延续前面的场景示例，随机数矩阵的第一份额可以表示为 $\langle R \rangle_0$ ，随机数矩阵的第二份额可以表示为 $\langle R \rangle_1$ ， $\langle R \rangle_0 + \langle R \rangle_1 = R$ 。所述第一数据方可以根据 $\langle R \rangle_0$ 和 $\langle H \rangle_0$ ，所述第二数据方可以根据 $\langle R \rangle_1$ 和 $\langle H \rangle_1$ ，秘密分享第二乘积 HR 。所述第一数据方可以获得第二乘积的第一份额 $\langle HR \rangle_0$ ，所述第二数据方可以获得第二乘积第二份额 $\langle HR \rangle_1$ 。

[72]下面介绍所述第一数据方和所述第二数据方秘密分享第二乘积 HR 的详细过程。

[73]所述第一数据方可以根据 $\langle H \rangle_0$ ，所述第二数据方可以根据 $\langle R \rangle_1$ ，秘密分享 $\langle H \rangle_0 \langle R \rangle_1$ 。所述第一数据方可以获得 $\langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_0$ ，所述第二数据方可以获得 $\langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_1$ 。 $\langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_0 + \langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_1 = \langle H \rangle_0 \langle R \rangle_1$ 。

[74]所述第一数据方还可以根据 $\langle R \rangle_0$ ，所述第二数据方还可以根据 $\langle H \rangle_1$ ，秘密分享 $\langle H \rangle_1 \langle R \rangle_0$ 。所述第一数据方可以获得 $\langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_0$ ，所述第二数据方可以获得 $\langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_1$ 。 $\langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_0 + \langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_1 = \langle H \rangle_1 \langle R \rangle_0$ 。

[75]所述第一数据方可以计算 $\langle H \rangle_0 \langle R \rangle_0 + \langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_0 + \langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_0$ 作为第二乘积的第一份额 $\langle HR \rangle_0$ 。所述第二数据方可以计算 $\langle H \rangle_1 \langle R \rangle_1 + \langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_1 + \langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_1$ 作为第二乘积的第二份额 $\langle HR \rangle_1$ 。

$$\begin{aligned} HR &= \langle HR \rangle_0 + \langle HR \rangle_1 \\ &= \langle H \rangle_0 \langle R \rangle_0 + \langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_0 + \langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_0 + \\ &\quad \langle H \rangle_1 \langle R \rangle_1 + \langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_1 + \langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_1 \\ &= \langle H \rangle_0 \langle R \rangle_0 + \langle H \rangle_0 \langle R \rangle_1 + \langle H \rangle_1 \langle R \rangle_0 + \langle H \rangle_1 \langle R \rangle_1 \\ &= (\langle H \rangle_0 + \langle H \rangle_1)(\langle R \rangle_0 + \langle R \rangle_1) \end{aligned}$$

- 5 [76]这里由所述第二数据方对第二乘积 HR 进行求逆处理。具体地，所述第一数据方可以向所述第二数据方发送第二乘积的第一份额 $\langle HR \rangle_0$ 。所述第二数据方可以接收第二乘积的第一份额 $\langle HR \rangle_0$ ；可以将第二乘积的第一份额 $\langle HR \rangle_0$ 与自身拥有的第二乘积的第二份额 $\langle HR \rangle_1$ 相加，得到第二乘积 HR ；可以对第二乘积 HR 进行求逆处理，得到第二逆矩阵 $(HR)^{-1}$ ；可以向所述第一数据方发送第二逆矩阵 $(HR)^{-1}$ 。所述第一数据方可以接收第二逆矩阵 $(HR)^{-1}$ 。

[77]所述第一数据方可以将第二逆矩阵 $(HR)^{-1}$ 与随机数矩阵的第一份额 $\langle R \rangle_0$ 相乘，得到第一逆矩阵 H^{-1} 的第一份额 $\langle H^{-1} \rangle_0$ 。所述第二数据方可以将第二逆矩阵 $(HR)^{-1}$ 与随机数矩阵的第二份额 $\langle R \rangle_1$ 相乘，得到第一逆矩阵 H^{-1} 的第一份额 $\langle H^{-1} \rangle_1$ 。
 $H^{-1} = \langle H^{-1} \rangle_0 + \langle H^{-1} \rangle_1 = \langle R \rangle_0 (HR)^{-1} + \langle R \rangle_1 (HR)^{-1} = R \times (HR)^{-1}$ 。

- 15 [78]在一些实施例，在步骤 S15 中，所述第一数据方可以根据第一逆矩阵的第一份额和损失函数梯度的第一份额，所述第二数据方可以根据第一逆矩阵的第二份额和损失函数梯度的第二份额，秘密分享第三乘积。所述第一数据方和所述第二数据方可以分别获得所述第三乘积的一份份额。为了便于描述，可以将所述第一数据方获得的份额作为第三乘积的第一份额，可以将所述第二数据方获得的份额作为第三乘积的第二份额。第三乘积的第一份额和第三乘积的第二份额的和等于第三乘积。

[79]所述第一数据方可以将原始模型参数的第一份额与第三乘积的第一份额相减，得到新的模型参数的第一份额。所述第二数据方可以将原始模型参数的第二份额与第三乘积的第二份额相减，得到新的模型参数的第二份额。

[80]值得说明的是,在实际应用中,可以将新的模型参数作为新的原始模型参数,重复执行步骤 S11、步骤 S13 和步骤 S15。通过重复执行本实施例的模型参数确定方法,可以实现对数据处理模型的模型参数进行迭代优化调整。

[81]延续前面的场景示例,所述第一数据方可以根据 $\langle H^{-1} \rangle_0$ 和 $\langle dW \rangle_0$, 所述第二数据

5 方可以根据 $\langle H^{-1} \rangle_1$ 和 $\langle dW \rangle_1$, 秘密分享第三乘积 $H^{-1} \times dW$ 。所述第一数据方可以获得第三乘积的第一份额 $\langle H^{-1} \times dW \rangle_0$, 所述第二数据方可以获得第三乘积的第二份额 $\langle H^{-1} \times dW \rangle_1$ 。

[82]下面介绍所述第一数据方和所述第二数据方秘密分享第三乘积 $H^{-1} \times dW$ 的详细过程。

10 [83] 所述第一数据方可以根据 $\langle H^{-1} \rangle_0$, 所述第二数据方可以根据 $\langle dW \rangle_1$, 秘密分享 $\langle H^{-1} \rangle_0 \langle dW \rangle_1$ 。所述第一数据方可以获得 $\langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_0$, 所述第二数据方可以获得 $\langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_1$ 。 $\langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_0 + \langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_1 = \langle H^{-1} \rangle_0 \langle dW \rangle_1$ 。

[84] 所述第一数据方还可以根据 $\langle dW \rangle_0$, 所述第二数据方还可以根据 $\langle H^{-1} \rangle_1$, 秘密分享 $\langle H^{-1} \rangle_1 \langle dW \rangle_0$ 。所述第一数据方可以获得 $\langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_0$, 所述第二数据方可以获得 $\langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_1$ 。 $\langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_0 + \langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_1 = \langle H^{-1} \rangle_1 \langle dW \rangle_0$ 。

[85] 所述第一数据方可以计算 $\langle H^{-1} \rangle_0 \langle dW \rangle_0 + \langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_0 + \langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_0$

作为第三乘积的第一份额 $\langle H^{-1} \times dW \rangle_0$ 。所述第二数据方可以计算 $\langle H^{-1} \rangle_1 \langle dW \rangle_1 + \langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_1 + \langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_1$ 作为第三乘积的第二份额 $\langle H^{-1} \times dW \rangle_1$ 。

$$\begin{aligned} H^{-1} \times dW &= \langle H^{-1} \times dW \rangle_0 + \langle H^{-1} \times dW \rangle_1 \\ &= \langle H^{-1} \rangle_0 \langle dW \rangle_0 + \langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_0 + \langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_0 + \\ &\quad \langle H^{-1} \rangle_1 \langle dW \rangle_1 + \langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_1 + \langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_1 \\ &= \langle H^{-1} \rangle_0 \langle dW \rangle_0 + \langle H^{-1} \rangle_0 \langle dW \rangle_1 + \langle H^{-1} \rangle_1 \langle dW \rangle_0 + \langle H^{-1} \rangle_1 \langle dW \rangle_1 \\ &= (\langle H^{-1} \rangle_0 + \langle H^{-1} \rangle_1)(\langle dW \rangle_0 + \langle dW \rangle_1) \end{aligned}$$

[86] 所述第一数据方可以计算 $\langle W' \rangle_0 = \langle W \rangle_0 - \langle H^{-1} \times dW \rangle_0$, 所述第二数据方可以计算

$\langle W' \rangle_1 = \langle W \rangle_1 - \langle H^{-1} \times dW \rangle_1$, $\langle W' \rangle_0$ 表示新的模型参数的第一份额, $\langle W' \rangle_1$ 表示新的模型参数的第二份额, W' 表示新的模型参数。

$$W' = \langle W' \rangle_0 + \langle W' \rangle_1 = \langle W \rangle_0 - \langle H^{-1} \times dW \rangle_0 + \langle W \rangle_1 - \langle H^{-1} \times dW \rangle_1 = W - H^{-1} \times dW$$

[87] 在本实施例中, 第一数据方和第二数据方可以利用秘密分享算法, 在不泄漏自身所
5 拥有的数据的前提下, 协作确定数据处理模型的模型参数。另外, 由于使用了牛顿法, 因而本实施例的模型参数确定方法有较快的收敛速度, 可以减少模型参数优化调整的次數, 提高数据处理模型的训练效率。

[88] 基于同样的发明构思, 本说明书还提供另一种模型参数确定方法的实施例。该实施例以第一数据方为执行主体, 所述第一数据方可以持有特征数据和原始模型参数的份额。

10 请参阅图 3。该实施例可以包括以下步骤。

[89] 步骤 S21: 根据特征数据和激励函数取值的份额与合作方秘密分享海森矩阵, 得到海森矩阵的份额。

[90] 在一些实施例中, 所述合作方可以理解为与所述第一数据方进行合作安全建模的数据方, 具体可以为前面的第二数据方。所述第一数据方可以根据第一乘积的份额与合作
15 方秘密分享多项式的取值, 得到多项式取值的份额作为激励函数取值的份额。所述第一乘积可以为原始模型参数和特征数据之间的乘积。所述第一数据方可以根据特征数据和原始模型参数的份额与合作方秘密分享第一乘积, 得到第一乘积的份额。所述多项式用于拟合所述激励函数。

[91] 所述第一数据方可以根据特征数据和激励函数取值的份额与合作方秘密分享损失函
20 数的梯度, 得到损失函数梯度的份额。

[92] 在一些实施例中, 所述第一数据方可以根据激励函数取值的份额与合作方秘密分享
对角矩阵, 得到对角矩阵的份额; 可以根据特征数据和对角矩阵的份额与合作方秘密分
享海森矩阵, 得到海森矩阵的份额。具体过程可以参见前面步骤 S11 中的相关描述, 在此不再赘述。

25 [93] 步骤 S23: 根据海森矩阵的份额与合作方秘密分享第一逆矩阵, 得到第一逆矩阵的
份额, 所述第一逆矩阵为海森矩阵的逆矩阵。

[94] 在一些实施例中, 所述第一数据方可以根据随机数矩阵的份额和海森矩阵的份额与
合作方秘密分享第二乘积, 得到第二乘积的份额。所述第二乘积可以为随机数矩阵和海

森矩阵之间的乘积。所述第一数据方可以向合作方发送第二乘积的份额；可以接收合作方反馈的第二逆矩阵，所述第二逆矩阵为所述第二乘积的逆矩阵；可以将第二逆矩阵与随机数矩阵的份额相乘，得到第一逆矩阵的份额。具体过程可以参见前面步骤 S13 中的相关描述，在此不再赘述。

- 5 [95]或者，在另一些实施例中，所述第一数据方可以根据随机数矩阵的份额和海森矩阵的份额与合作方秘密分享第二乘积，得到第二乘积的第一份额。所述第二乘积可以为随机数矩阵和海森矩阵之间的乘积。所述第一数据方可以接收合作方发来的第二乘积的第二份额；可以根据第二乘积的第一份额和第二乘积的第二份额确定第二逆矩阵，所述第二逆矩阵为所述第二乘积的逆矩阵；可以将第二逆矩阵与随机数矩阵的份额相乘，得到
- 10 第一逆矩阵的份额。具体过程可以参见前面步骤 S13 中的相关描述，在此不再赘述。

[96]步骤 S25：根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数，得到新的模型参数的份额。

- [97]在一些实施例中，所述第一数据方可以根据第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享第三乘积，得到第三乘积的份额。所述第三乘积可以为第一逆矩阵
- 15 和损失函数梯度之间的乘积。所述第一数据方可以将原始模型参数的份额与第三乘积的份额相减，得到新的模型参数的份额。具体过程可以参见前面步骤 S15 中的相关描述，在此不再赘述。

[98]在本实施例中，第一数据方可以利用秘密分享算法，在不泄漏自身所拥有的数据的前提下，与合作方协作确定数据处理模型的模型参数，得到新的模型参数的份额。

- 20 [99]基于同样的发明构思，本说明书还提供另一种模型参数确定方法的实施例。该实施例以第二数据方为执行主体，所述第二数据方可以持有标签和原始模型参数的份额。请参阅图 4。该实施例可以包括以下步骤。

[100] 步骤 S31：根据激励函数取值的份额与合作方秘密分享海森矩阵，得到海森矩阵的份额。

- 25 [101] 在一些实施例中，所述合作方可以理解为与所述第二数据方进行合作安全建模的数据方，具体可以为前面的第一数据方。所述第二数据方可以根据第一乘积的份额与合作方秘密分享多项式的取值，得到多项式取值的份额作为激励函数取值的份额。所述第一乘积可以为原始模型参数和特征数据之间的乘积。所述第二数据方可以根据原始模型参数的份额与合作方秘密分享第一乘积，得到第一乘积的份额。所述多项式用于拟合

所述激励函数。

[102] 所述第二数据方可以根据标签和激励函数取值的份额与合作方秘密分享损失函数的梯度，得到损失函数梯度的份额。

[103] 在一些实施例中，所述第二数据方可以根据激励函数取值的份额与合作方秘密分享对角矩阵，得到对角矩阵的份额；可以根据对角矩阵的份额与合作方秘密分享海森矩阵，得到海森矩阵的份额。具体过程可以参见前面步骤 S11 中的相关描述，在此不再赘述。

[104] 步骤 S33：根据海森矩阵的份额与合作方秘密分享第一逆矩阵，得到第一逆矩阵的份额，所述第一逆矩阵为海森矩阵的逆矩阵。

[105] 在一些实施例中，所述第二数据方可以根据随机数矩阵的份额和海森矩阵的份额与合作方秘密分享第二乘积，得到第二乘积的份额。所述第二乘积可以为随机数矩阵和海森矩阵之间的乘积。所述第二数据方可以向合作方发送第二乘积的份额；可以接收合作方反馈的第二逆矩阵，所述第二逆矩阵为所述第二乘积的逆矩阵；可以将第二逆矩阵与随机数矩阵的份额相乘，得到第一逆矩阵的份额。具体过程可以参见前面步骤 S13 中的相关描述，在此不再赘述。

[106] 或者，在另一些实施例中，所述第二数据方可以根据随机数矩阵的份额和海森矩阵的份额与合作方秘密分享第二乘积，得到第二乘积的第一份额。所述第二乘积可以为随机数矩阵和海森矩阵之间的乘积。所述第二数据方可以接收合作方发来的第二乘积的第二份额；可以根据第二乘积的第一份额和第二乘积的第二份额确定第二逆矩阵，所述第二逆矩阵为所述第二乘积的逆矩阵；可以将第二逆矩阵与随机数矩阵的份额相乘，得到第一逆矩阵的份额。具体过程可以参见前面步骤 S13 中的相关描述，在此不再赘述。

[107] 步骤 S35：根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数，得到新的模型参数的份额。

[108] 在一些实施例中，所述第二数据方可以根据第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享第三乘积，得到第三乘积的份额。所述第三乘积可以为第一逆矩阵和损失函数梯度之间的乘积。所述第二数据方可以将原始模型参数的份额与第三乘积的份额相减，得到新的模型参数的份额。具体过程可以参见前面步骤 S15 中的相关描述，在此不再赘述。

[109] 在本实施例中，第二数据方可以利用秘密分享算法，在不泄漏自身所拥有的数

据的前提下，与合作方协作确定数据处理模型的模型参数，得到新的模型参数的份额。

[110] 基于同样的发明构思，本说明书还提供一种模型参数确定装置的实施例。请参阅图 5。该实施例可以应用于第一数据方，可以包括以下单元。

5 [111] 第一秘密分享单元 41，用于根据特征数据和激励函数取值的份额与合作方秘密分享海森矩阵，得到海森矩阵的份额；

[112] 第二秘密分享单元 43，用于根据海森矩阵的份额与合作方秘密分享第一逆矩阵，得到第一逆矩阵的份额，所述第一逆矩阵为海森矩阵的逆矩阵；

[113] 第三秘密分享单元 45，用于根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数，得到新的模型参数的份额。

10 [114] 基于同样的发明构思，本说明书还提供一种模型参数确定装置的实施例。请参阅图 6。该实施例可以应用于第二数据方，可以包括以下单元。

[115] 第一秘密分享单元 51，用于根据激励函数取值的份额与合作方秘密分享海森矩阵，得到海森矩阵的份额；

15 [116] 第二秘密分享单元 53，用于根据海森矩阵的份额与合作方秘密分享第一逆矩阵，得到第一逆矩阵的份额，所述第一逆矩阵为海森矩阵的逆矩阵；

[117] 第三秘密分享单元 55，用于根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数，得到新的模型参数的份额。

20 [118] 下面介绍本说明书电子设备的一个实施例。图 7 是该实施例中一种电子设备的硬件结构示意图。如图 7 所示，所述电子设备可以包括一个或多个（图中仅示出一个）处理器、存储器和传输模块。当然，本领域普通技术人员可以理解，图 7 所示的硬件结构仅为示意，其并不对上述电子设备的硬件结构造成限定。在实际中所述电子设备还可以包括比图 7 所示更多或者更少的组件单元；或者，具有与图 7 所示不同的配置。

25 [119] 所述存储器可以包括高速随机存储器；或者，还可以包括非易失性存储器，例如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。当然，所述存储器还可以包括远程设置的网络存储器。所述远程设置的网络存储器可以通过诸如互联网、企业内部网、局域网、移动通信网等网络连接至所述电子设备。所述存储器可以用于存储应用程序的程序指令或模块，例如本说明书图 3 所对应实施例的程序指令或模块；和/或，本说明书图 4 所对应实施例的程序指令或模块。

[120] 所述处理器可以按任何适当的方式实现。例如，所述处理器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit, ASIC）、可编程逻辑控制器和嵌入微控制器的形式等等。所述处理器可以读取并执行所述存储器中的程序指令或模块。

[121] 所述传输模块可以用于经由网络进行数据传输，例如经由诸如互联网、企业内部网、局域网、移动通信网等网络进行数据传输。

[122] 需要说明的是，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或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它实施例的不同之处。尤其，对于装置实施例和电子设备实施例而言，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。另外，可以理解的是，本领域技术人员在阅读本说明书文件之后，可以无需创造性劳动想到将本说明书列举的部分或全部实施例进行任意组合，这些组合也在本说明书公开和保护的范围之内。

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

Language) 与 Verilog2。本领域技术人员也应该清楚,只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中,就可以很容易得到实现该逻辑方法流程的硬件电路。

[124] 上述实施例阐明的系统、装置、模块或单元,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的,计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

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

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

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

[128] 虽然通过实施例描绘了本说明书,本领域普通技术人员知道,本说明书有许多变形和变化而不脱离本说明书的精神,希望所附的权利要求包括这些变形和变化而不脱离本说明书的精神。

权利要求书

1、一种模型参数确定方法，应用于第一数据方，包括：

根据特征数据和激励函数取值的份额与合作方秘密分享海森矩阵，得到海森矩阵的份额；

5 根据海森矩阵的份额与合作方秘密分享第一逆矩阵，得到第一逆矩阵的份额，所述第一逆矩阵为海森矩阵的逆矩阵；

根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数，得到新的模型参数的份额。

2、如权利要求 1 所述的方法，所述激励函数取值的份额通过以下步骤获得：

10 根据第一乘积的份额与合作方秘密分享多项式的取值，得到多项式取值的份额作为激励函数取值的份额，所述第一乘积为原始模型参数和特征数据之间的乘积，所述多项式用于拟合所述激励函数。

3、如权利要求 2 所述的方法，所述第一乘积的份额通过以下步骤获得：

15 根据特征数据和原始模型参数的份额与合作方秘密分享第一乘积，得到第一乘积的份额。

4、如权利要求 2 所述的方法，所述损失函数梯度的份额通过以下步骤获得：

根据特征数据和激励函数取值的份额与合作方秘密分享损失函数的梯度，得到损失函数梯度的份额。

20 5、如权利要求 1 所述的方法，所述根据特征数据和激励函数取值的份额与合作方秘密分享海森矩阵，得到海森矩阵的份额，包括：

根据激励函数取值的份额与合作方秘密分享对角矩阵，得到对角矩阵的份额；

根据特征数据和对角矩阵的份额与合作方秘密分享海森矩阵，得到海森矩阵的份额。

6、如权利要求 1 所述的方法，所述根据海森矩阵的份额与合作方秘密分享第一逆矩阵，得到第一逆矩阵的份额，包括：

25 根据随机数矩阵的份额和海森矩阵的份额与合作方秘密分享第二乘积，得到第二乘积的份额，所述第二乘积为随机数矩阵和海森矩阵之间的乘积；

向合作方发送第二乘积的份额；

接收合作方反馈的第二逆矩阵，所述第二逆矩阵为所述第二乘积的逆矩阵；

将第二逆矩阵与随机数矩阵的份额相乘，得到第一逆矩阵的份额。

30 7、如权利要求 1 所述的方法，所述根据海森矩阵的份额与合作方秘密分享第一逆矩阵，得到第一逆矩阵的份额，包括：

根据随机数矩阵的份额和海森矩阵的份额与合作方秘密分享第二乘积,得到第二乘积的第一份额,所述第二乘积为随机数矩阵和海森矩阵之间的乘积;

接收合作方发来的第二乘积的第二份额;

5 根据第二乘积的第一份额和第二乘积的第二份额确定第二逆矩阵,所述第二逆矩阵为所述第二乘积的逆矩阵;

将第二逆矩阵与随机数矩阵的份额相乘,得到第一逆矩阵的份额。

8、如权利要求 1 所述的方法,所述根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数,得到新的模型参数的份额,包括:

10 根据第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享第三乘积,得到第三乘积的份额,所述第三乘积为第一逆矩阵和损失函数梯度之间的乘积;

将原始模型参数的份额与第三乘积的份额相减,得到新的模型参数的份额。

9、一种模型参数确定装置,应用于第一数据方,包括:

15 第一秘密分享单元,用于根据特征数据和激励函数取值的份额与合作方秘密分享海森矩阵,得到海森矩阵的份额;

第二秘密分享单元,用于根据海森矩阵的份额与合作方秘密分享第一逆矩阵,得到第一逆矩阵的份额,所述第一逆矩阵为海森矩阵的逆矩阵;

第三秘密分享单元,用于根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数,得到新的模型参数的份额。

20 10、一种电子设备,包括:

存储器,用于存储计算机指令;

处理器,用于执行所述计算机指令以实现如权利要求 1-8 中任一项所述的方法步骤。

11、一种模型参数确定方法,应用于第二数据方,包括:

根据激励函数取值的份额与合作方秘密分享海森矩阵,得到海森矩阵的份额;

25 根据海森矩阵的份额与合作方秘密分享第一逆矩阵,得到第一逆矩阵的份额,所述第一逆矩阵为海森矩阵的逆矩阵;

根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数,得到新的模型参数的份额。

12、如权利要求 11 所述的方法,所述激励函数取值的份额通过以下步骤获得:

30 根据第一乘积的份额与合作方秘密分享多项式的取值,得到多项式取值的份额作为激励函数取值的份额,所述第一乘积为原始模型参数和特征数据之间的乘积,所述多项

式用于拟合所述激励函数。

13、如权利要求 12 所述的方法，所述第一乘积的份额通过以下步骤获得：

根据原始模型参数的份额与合作方秘密分享第一乘积，得到第一乘积的份额。

14、如权利要求 12 所述的方法，所述损失函数梯度的份额通过以下步骤获得：

5 根据标签和激励函数取值的份额与合作方秘密分享损失函数的梯度，得到损失函数梯度的份额。

15、如权利要求 11 所述的方法，所述根据激励函数取值的份额与合作方秘密分享海森矩阵，得到海森矩阵的份额，包括：

根据激励函数取值的份额与合作方秘密分享对角矩阵，得到对角矩阵的份额；

10 根据对角矩阵的份额与合作方秘密分享海森矩阵，得到海森矩阵的份额。

16、如权利要求 11 所述的方法，所述根据海森矩阵的份额与合作方秘密分享第一逆矩阵，得到第一逆矩阵的份额，包括：

根据随机数矩阵的份额和海森矩阵的份额与合作方秘密分享第二乘积，得到第二乘积的份额，所述第二乘积为随机数矩阵和海森矩阵之间的乘积；

15 向合作方发送第二乘积的份额；

接收合作方反馈的第二逆矩阵，所述第二逆矩阵为所述第二乘积的逆矩阵；

将第二逆矩阵与随机数矩阵的份额相乘，得到第一逆矩阵的份额。

17、如权利要求 11 所述的方法，所述根据海森矩阵的份额与合作方秘密分享第一逆矩阵，得到第一逆矩阵的份额，包括：

20 根据随机数矩阵的份额和海森矩阵的份额与合作方秘密分享第二乘积，得到第二乘积的第一份额，所述第二乘积为随机数矩阵和海森矩阵之间的乘积；

接收合作方发来的第二乘积的第二份额；

根据第二乘积的第一份额和第二乘积的第二份额确定第二逆矩阵，所述第二逆矩阵为所述第二乘积的逆矩阵；

25 将第二逆矩阵与随机数矩阵的份额相乘，得到第一逆矩阵的份额。

18、如权利要求 11 所述的方法，所述根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数，得到新的模型参数的份额，包括：

根据第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享第三乘积，得到第三乘积的份额，所述第三乘积为第一逆矩阵和损失函数梯度之间的乘积；

将原始模型参数的份额与第三乘积的份额相减，得到新的模型参数的份额。

19、一种模型参数确定装置，应用于第二数据方，包括：

第一秘密分享单元，用于根据激励函数取值的份额与合作方秘密分享海森矩阵，得到海森矩阵的份额；

5 第二秘密分享单元，用于根据海森矩阵的份额与合作方秘密分享第一逆矩阵，得到第一逆矩阵的份额，所述第一逆矩阵为海森矩阵的逆矩阵；

第三秘密分享单元，用于根据原始模型参数的份额、第一逆矩阵的份额和损失函数梯度的份额与合作方秘密分享新的模型参数，得到新的模型参数的份额。

20、一种电子设备，包括：

存储器，用于存储计算机指令；

10 处理器，用于执行所述计算机指令以实现如权利要求 11-18 中任一项所述的方法步骤。

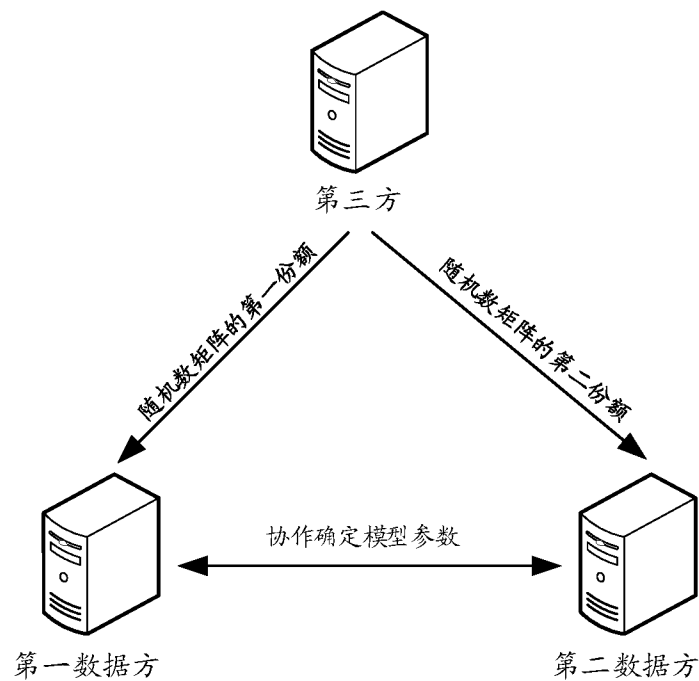


图 1

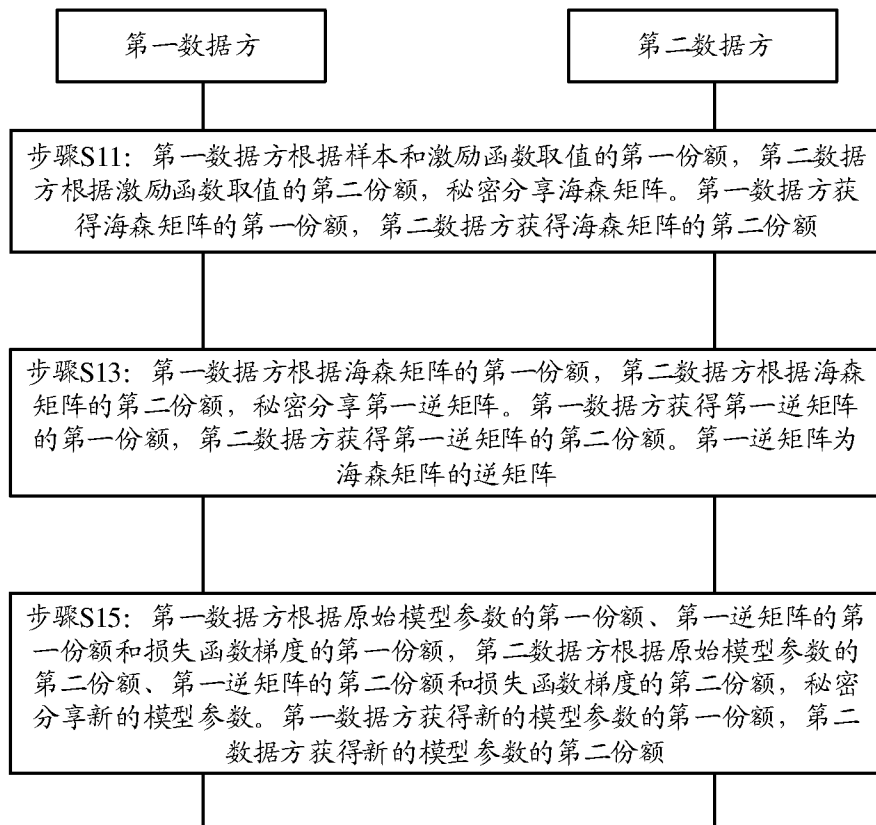


图 2

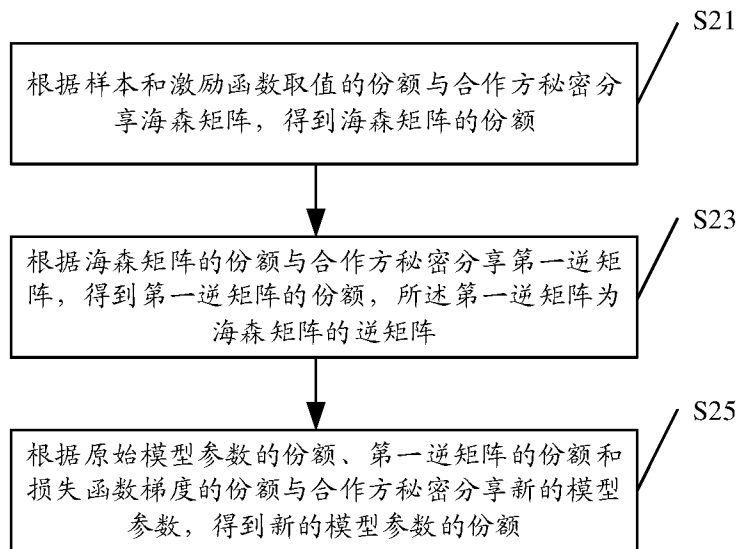


图 3

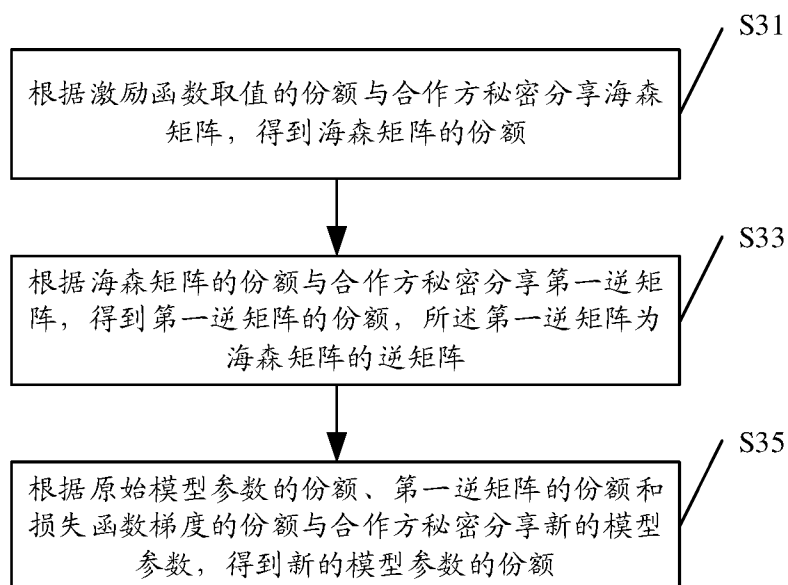


图 4

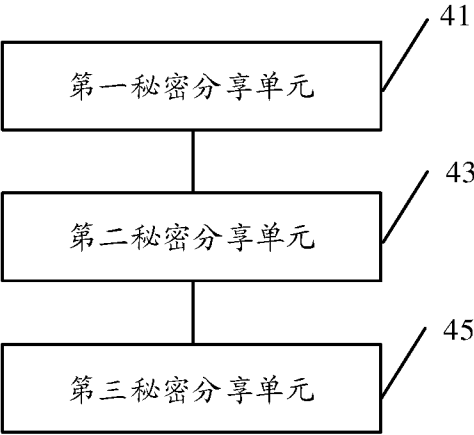


图 5

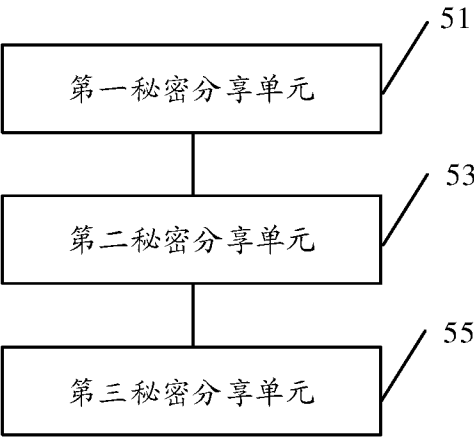


图 6

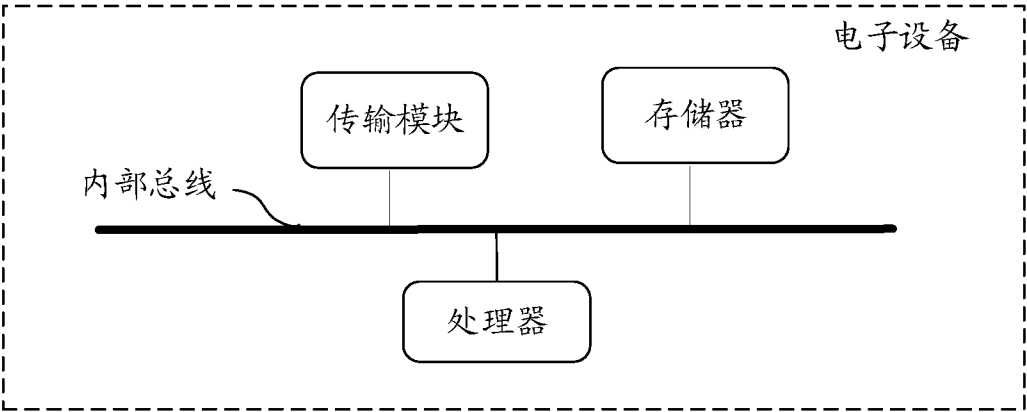


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/071432

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62(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, WPI, EPODOC, CNKI, GOOGLE: 参数, 收敛, 乘积, 相乘, 矩阵, 协作, 秘密分享, 分享, 建模, 安全, G06F21/6245, 秘密, 特征, 训练, 函数, 模型, 份额, 迭代, newton, 云存储, secret, share, iteration,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110555525 A (ALIBABA GROUP HOLDING LIMITED) 10 December 2019 (2019-12-10) claims 1-24	1-20
PX	CN 110555315 A (ALIBABA GROUP HOLDING LIMITED) 10 December 2019 (2019-12-10) claims 1-20, description, paragraphs [0036]-[0131]	1-20
PX	CN 110580410 A (ALIBABA GROUP HOLDING LIMITED) 17 December 2019 (2019-12-17) claims 1-26	1-20
PX	CN 110569228 A (ALIBABA GROUP HOLDING LIMITED) 13 December 2019 (2019-12-13) claims 1-26	1-20
PX	CN 110580409 A (ALIBABA GROUP HOLDING LIMITED) 17 December 2019 (2019-12-17) claims 1-18	1-20



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

02 April 2020

Date of mailing of the international search report

24 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

International application No.

PCT/CN2020/071432

C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110569227 A (ALIBABA GROUP HOLDING LIMITED) 13 December 2019 (2019-12-13) claims 1-10	1-20
PX	CN 110472439 A (ALIBABA GROUP HOLDING LIMITED) 19 November 2019 (2019-11-19) claims 1-24	1-20
A	CN 109977694 A (JINAN UNIVERSITY) 05 July 2019 (2019-07-05) description, paragraphs [0044]-[0070], figures 1-2	1-20
A	CN 101882992 A (CHINA AGRICULTURAL UNIVERSITY) 10 November 2010 (2010-11-10) entire document	1-20
A	US 2003112969 A1 (IBM) 19 June 2003 (2003-06-19) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/071432

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	110555525	A	10 December 2019	None	
CN	110555315	A	10 December 2019	None	
CN	110580410	A	17 December 2019	None	
CN	110569228	A	13 December 2019	None	
CN	110580409	A	17 December 2019	None	
CN	110569227	A	13 December 2019	None	
CN	110472439	A	19 November 2019	None	
CN	109977694	A	05 July 2019	None	
CN	101882992	A	10 November 2010	None	
US	2003112969	A1	19 June 2003	None	

国际检索报告

国际申请号

PCT/CN2020/071432

A. 主题的分类

G06F 21/62 (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, WPI, EPDOC, CNKI, GOOGLE: 参数, 收敛, 乘积, 相乘, 矩阵, 协作, 秘密分享, 分享, 建模, 安全, G06F21/6245, 秘密, 特征, 训练, 函数, 模型, 份额, 迭代, newton, 云存储, secret, share, iteration,

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 110555525 A (阿里巴巴集团控股有限公司) 2019年 12月 10日 (2019 - 12 - 10) 权利要求1-24	1-20
PX	CN 110555315 A (阿里巴巴集团控股有限公司) 2019年 12月 10日 (2019 - 12 - 10) 权利要求1-20, 说明书[0036]-[0131]段	1-20
PX	CN 110580410 A (阿里巴巴集团控股有限公司) 2019年 12月 17日 (2019 - 12 - 17) 权利要求1-26	1-20
PX	CN 110569228 A (阿里巴巴集团控股有限公司) 2019年 12月 13日 (2019 - 12 - 13) 权利要求1-26	1-20
PX	CN 110580409 A (阿里巴巴集团控股有限公司) 2019年 12月 17日 (2019 - 12 - 17) 权利要求1-18	1-20
PX	CN 110569227 A (阿里巴巴集团控股有限公司) 2019年 12月 13日 (2019 - 12 - 13) 权利要求1-10	1-20
PX	CN 110472439 A (阿里巴巴集团控股有限公司) 2019年 11月 19日 (2019 - 11 - 19) 权利要求1-24	1-20
A	CN 109977694 A (暨南大学) 2019年 7月 5日 (2019 - 07 - 05) 说明书第[0044]-[0070]段, 附图1-2	1-20

☒ 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

“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 2日

国际检索报告邮寄日期

2020年 4月 24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

林芳

电话号码 86-(10)-53961337

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 101882992 A (中国农业大学) 2010年 11月 10日 (2010 - 11 - 10) 全文	1-20
A	US 2003112969 A1 (IBM) 2003年 6月 19日 (2003 - 06 - 19) 全文	1-20

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/071432

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	110555525	A	2019年 12月 10日	无	
CN	110555315	A	2019年 12月 10日	无	
CN	110580410	A	2019年 12月 17日	无	
CN	110569228	A	2019年 12月 13日	无	
CN	110580409	A	2019年 12月 17日	无	
CN	110569227	A	2019年 12月 13日	无	
CN	110472439	A	2019年 11月 19日	无	
CN	109977694	A	2019年 7月 5日	无	
CN	101882992	A	2010年 11月 10日	无	
US	2003112969	A1	2003年 6月 19日	无	