

(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 2021/027598 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)

G06N 3/02 (2006.01)

(21) 国际申请号:

PCT/CN2020/106254

(22) 国际申请日:

2020 年 7 月 31 日 (31.07.2020)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

201910735439.1 2019年8月9日 (09.08.2019) CN

201910734784.3 2019年8月9日 (09.08.2019) CN

201910735442.3 2019年8月9日 (09.08.2019) CN

201910735421.1 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.); 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: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL

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

(54) 发明名称: 模型参数确定方法、装置和电子设备

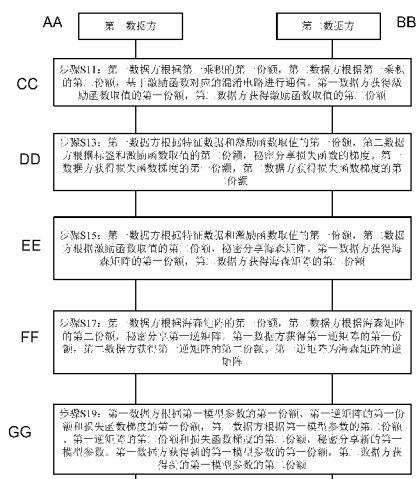


图 3

AA FIRST DATA PARTY
BB SECOND DATA PARTY
CC STEP S11: A FIRST DATA PARTY, ACCORDING TO A FIRST SHARE OF A FIRST PRODUCT, AND A SECOND DATA PARTY, ACCORDING TO A SECOND SHARE OF THE FIRST PRODUCT, COMMUNICATE WITH EACH OTHER ON THE BASIS OF A GARBLED CIRCUIT CORRESPONDING TO AN ACTIVATION FUNCTION; THE FIRST DATA PARTY OBTAINS A FIRST SHARE OF A VALUE OF THE ACTIVATION FUNCTION AND THE SECOND DATA PARTY OBTAINS A SECOND SHARE OF THE VALUE OF THE ACTIVATION FUNCTION
DD STEP S13: THE FIRST DATA PARTY, ACCORDING TO FEATURE DATA AND THE FIRST SHARE OF THE VALUE OF THE ACTIVATION FUNCTION, AND THE SECOND DATA PARTY, ACCORDING TO A TAG AND THE SECOND SHARE OF THE VALUE OF THE ACTIVATION FUNCTION, SECRETLY SHARE A GRADIENT OF A LOSS FUNCTION; THE FIRST DATA PARTY OBTAINS A FIRST SHARE OF THE GRADIENT OF THE LOSS FUNCTION AND THE SECOND DATA PARTY OBTAINS A SECOND SHARE OF THE GRADIENT OF THE LOSS FUNCTION
EE STEP S15: THE FIRST DATA PARTY, ACCORDING TO THE FEATURE DATA AND THE FIRST SHARE OF THE VALUE OF THE ACTIVATION FUNCTION, AND THE SECOND DATA PARTY, ACCORDING TO THE SECOND SHARE OF THE VALUE OF THE ACTIVATION FUNCTION, SECRETLY SHARE A HESSIAN MATRIX; THE FIRST DATA PARTY OBTAINS A FIRST SHARE OF THE HESSIAN MATRIX AND THE SECOND DATA PARTY OBTAINS A SECOND SHARE OF THE HESSIAN MATRIX
FF STEP S17: THE FIRST DATA PARTY, ACCORDING TO THE FIRST SHARE OF THE HESSIAN MATRIX, AND THE SECOND DATA PARTY, ACCORDING TO THE SECOND SHARE OF THE HESSIAN MATRIX, SECRETLY SHARE A FIRST INVERSE MATRIX; THE FIRST DATA PARTY OBTAINS A FIRST SHARE OF THE FIRST INVERSE MATRIX AND THE SECOND DATA PARTY OBTAINS A SECOND SHARE OF THE FIRST INVERSE MATRIX, WHEREIN THE FIRST INVERSE MATRIX IS AN INVERSE MATRIX OF THE HESSIAN MATRIX
GG STEP S19: THE FIRST DATA PARTY, ACCORDING TO A FIRST SHARE OF A FIRST MODEL PARAMETER, THE FIRST SHARE OF THE FIRST INVERSE MATRIX, AND THE FIRST SHARE OF THE GRADIENT OF THE LOSS FUNCTION, AND THE SECOND DATA PARTY, ACCORDING TO A SECOND SHARE OF THE FIRST MODEL PARAMETER, THE SECOND SHARE OF THE FIRST INVERSE MATRIX, AND THE SECOND SHARE OF THE GRADIENT OF THE LOSS FUNCTION, SECRETLY SHARE A NEW FIRST MODEL PARAMETER; THE FIRST DATA PARTY OBTAINS A FIRST SHARE OF THE NEW FIRST MODEL PARAMETER AND THE SECOND DATA PARTY OBTAINS A SECOND SHARE OF THE NEW FIRST MODEL PARAMETER

(57) Abstract: A method and apparatus for determining a model parameter, and an electronic device. The method comprises: communicating with a cooperation party according to a share of a first product and a garbled circuit corresponding to an activation function to obtain a share of a value of the activation function; secretly sharing a gradient of a loss function with the cooperation party according to feature data and the share of the value of the activation function to obtain a share of the gradient of the loss function; secretly sharing a Hessian matrix with the cooperation party according to the feature data and the share of the value of the activation function to obtain

PROPERTY AGENCY LTD.; 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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, IT, 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))。

a share of the Hessian matrix; secretly sharing a first inverse matrix with the cooperation party according to the share of the Hessian matrix to obtain a share of the first inverse matrix; and secretly sharing a new first model parameter with the cooperation party according to a share of a first model parameter, the share of the first inverse matrix, and the share of the gradient of the loss function to obtain a share of the new first model parameter. A model parameter of a data processing model can be determined by the collaboration of multiple parties on the premise of protecting data privacy.

(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: 根据第一乘积的份额和激励函数对应的混淆电路与合作方进行通信, 得到激励函数取值的份额; 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; 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; 根据第一模型参数的份额、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第一模型参数, 得到新的第一模型参数的份额。可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。

模型参数确定方法、装置和电子设备

本申请要求 2019 年 08 月 09 日递交的申请号为 201910735439.1、发明名称为“模型参数确定方法、装置和电子设备”的中国专利申请的优先权，2019 年 08 月 09 日递交的申请号为 201910734784.3、发明名称为“模型参数确定方法、装置和电子设备”的中国
5 专利申请的优先权，2019 年 08 月 09 日递交的申请号为 201910735442.3、发明名称为“模型参数确定方法、装置和电子设备”的中国专利申请的优先权，以及 2019 年 08 月 09 日递交的申请号为 201910735421.1、发明名称为“模型参数确定方法、装置和电子设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

10 技术领域

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。

背景技术

15 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，使用各方的数据对数据处理模型进行协作训练。

在对数据处理模型进行协作训练的过程中，可以使用模型参数优化方法对数据处理
20 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

25 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。

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。

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：根据第一乘积的份额和激励函数对应的混淆电路与合作方进行通
30 信，得到激励函数取值的份额，所述第一乘积为特征数据和第一模型参数的乘积；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；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；根据第一模型参数的份额、第一逆矩阵的份额和
5 损失函数梯度的份额与合作方秘密分享新的第一模型参数，得到新的第一模型参数的份额。

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方法，应用于第二数据方，包括：根据第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到激励函数取值的份额，所述第一乘积为特征数据和第一模型参数的乘积；根据
10 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；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额，所述第一逆矩阵为海森矩阵的逆矩阵；根据第一模型参数的份额、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第一模型参数，得到新的第一模型参数的份额。

15 根据本说明书一个或多个实施例的第三方面，提供了一种模型参数确定方法，应用于第一数据方，包括：根据特征数据和第一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，所述第一乘积为特征数据和第一模型参数的乘积；根据第一乘积的份额与合作方秘密分享激励函数的取值，得到激励函数取值的份额；根据特征数据和激励函数取值的份额与合作方分别秘密分享损失函数的梯度和海森矩阵，得到损失函数
20 梯度的份额和海森矩阵的份额；根据随机正交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正交矩阵和海森矩阵之间的乘积；在第二乘积的条件数满足预设条件时，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；根据第一逆矩阵的份额、损失函数梯度的份额和第一模型参数的份额与合作方秘密分享新的第一
25 模型参数，得到新的第一模型参数的份额；迭代执行所述秘密分享第一乘积的步骤，得到新的第一乘积的份额，根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到新的激励函数取值的份额，迭代执行所述秘密分享损失函数的梯度和海森矩阵的步骤，得到新的损失函数梯度的份额和新的海森矩阵的份额，迭代执行所述秘密分享第二乘积的步骤，得到新的第二乘积的份额；在新的第二乘积的条件数不满足所
30 述预设条件时，根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长，

计算第二模型参数的份额。

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：根据第一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，所述第一乘积为特征数据和第一模型参数的乘积；根据第一乘积的份额与合作方秘密分享激励函数的取值，得到激励函数取值的份额；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；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；根据随机正交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正交矩阵和海森矩阵之间的乘积；在第二乘积的条件数满足预设条件时，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；根据第一逆矩阵的份额、损失函数梯度的份额和第一模型参数的份额与合作方秘密分享新的第一模型参数，得到新的第一模型参数的份额；迭代执行所述秘密分享第一乘积的步骤，得到新的第一乘积的份额，根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到新的激励函数取值的份额；迭代执行所述秘密分享损失函数的梯度的步骤，得到新的损失函数梯度的份额，迭代执行所述秘密分享海森矩阵的步骤，得到新的海森矩阵的份额，迭代执行所述秘密分享第二乘积的步骤，得到新的第二乘积的份额；在新的第二乘积的条件数不满足所述预设条件时，根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

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，应用于第一数据方，包括：激励函数取值份额获取单元，用于根据第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到激励函数取值的份额，所述第一乘积为特征数据和第一模型参数的乘积；损失函数梯度份额获取单元，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损失函数的梯度，得到损失函数梯度的份额；海森矩阵份额获取单元，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；第一逆矩阵份额获取单元，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；模型参数份额获取单元，用于根据第一模型参数的份额、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第一模型参数，得到新的第一模型参数的份额。

根据本说明书一个或多个实施例的第六方面，提供了一种模型参数确定装置，应用于第二数据方，包括：激励函数取值份额获取单元，用于根据第一乘积的份额和激励函

数对应的混淆电路与合作方进行通信，得到激励函数取值的份额，所述第一乘积为特征数据和第一模型参数的乘积；损失函数梯度份额获取单元，用于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；海森矩阵份额获取单元，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
5 份额；第一逆矩阵份额获取单元，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；模型参数份额获取单元，用于根据第一模型参数的份额、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第一模型参数，得到新的第一模型参数的份额。

根据本说明书一个或多个实施例的第七方面，提供了一种模型参数确定装置，应用于
10 于第一数据方，包括：第一秘密分享单元，用于根据特征数据和第一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，所述第一乘积为特征数据和第一模型参数的乘积；第二秘密分享单元，用于根据第一乘积的份额与合作方秘密分享激励函数的取值，得到激励函数取值的份额；第三秘密分享单元，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损失函数的梯度和海森矩阵，分别得到损失函数梯度的份
15 额和海森矩阵的份额；第四秘密分享单元，用于根据随机正交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正交矩阵和海森矩阵之间的乘积；第五秘密分享单元，用于在第二乘积的条件数满足预设条件时，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；第六秘密分享单元，用于根据第一逆矩阵的份额、损失函
20 数梯度的份额和第一模型参数的份额与合作方秘密分享新的第一模型参数，得到新的第一模型参数的份额；迭代单元，用于迭代执行所述秘密分享第一乘积的步骤，得到新的第一乘积的份额，根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到新的激励函数取值的份额，迭代执行所述秘密分享损失函数的梯度和海森矩阵的步骤，得到新的损失函数梯度的份额和新的海森矩阵的份额，迭代执行所述秘密分享
25 第二乘积的步骤，得到新的第二乘积的份额；在新的第二乘积的条件数不满足所述预设条件时，根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

根据本说明书一个或多个实施例的第八方面，提供了一种模型参数确定装置，应用于
30 第二数据方，包括：第一秘密分享单元，用于根据第一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，所述第一乘积为特征数据和第一模型参数的乘积；

第二秘密分享单元，用于根据第一乘积的份额与合作方秘密分享激励函数的取值，得到激励函数取值的份额；第三秘密分享单元，用于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；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；第四秘密分享单元，用于根据随机正交

5 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正交矩阵和海森矩阵之间的乘积；第五秘密分享单元，用于在第二乘积的条件数满足预设条件时，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；第六秘密分享单元，用于根据第一逆矩阵的份额、损失函数梯度的份额和第一模型参数的份额与合作方秘密分享新的

10 第一模型参数，得到新的第一模型参数的份额；迭代单元，用于迭代执行所述秘密分享第一乘积的步骤，得到新的第一乘积的份额，根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到新的激励函数取值的份额；迭代执行所述秘密分享损失函数的梯度的步骤，得到新的损失函数梯度的份额，迭代执行所述秘密分享海森矩阵的步骤，得到新的海森矩阵的份额，迭代执行所述秘密分享第二乘积的步骤，得到新的第二乘积的份额；在新的第二乘积的条件数不满足所述预设条件时，根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

15

根据本说明书一个或多个实施例的第九方面，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一方面、第二方面、第三方面或第四方面所述的方法步骤。

20 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在不泄漏自身所持有数据的前提下，协作确定数据处理模型的模型参数。

附图说明

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，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。

25

图 1 为本说明书实施例一种逻辑电路的示意图；

图 2 为本说明书实施例一种模型参数确定系统的示意图；

30 图 3 为本说明书实施例一种模型参数确定方法的流程图；

图 4 为本说明书实施例一种基于混淆电路进行计算的示意图；

图 5 为本说明书实施例一种模型参数确定方法的流程图；

图 6 为本说明书实施例一种模型参数确定方法的流程图；

图 7 为本说明书实施例一种模型参数确定装置的功能结构示意图；

5 图 8 为本说明书实施例一种模型参数确定装置的功能结构示意图；

图 9 为本说明书实施例一种模型参数确定方法的流程图；

图 10 为本说明书实施例一种模型参数确定方法的流程图；

图 11 为本说明书实施例一种模型参数确定方法的流程图；

图 12 为本说明书实施例一种模型参数确定装置的功能结构示意图；

10 图 13 为本说明书实施例一种模型参数确定装置的功能结构示意图；

图 14 为本说明书实施例一种电子设备的功能结构示意图。

具体实施方式

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、
15 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。

多方安全计算（Secure Muti-Party Computation，MPC）是一种保护数据隐私安全的
20 算法。多方安全计算能让参与计算的多个数据方在不暴露自身数据的前提下进行协作计

秘密分享（SS，Secret Sharing）是一种保护数据隐私安全的算法，可以用于实现多
方安全计算。具体地，多个数据方可以在不泄露自身数据的前提下，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
25 持有数据 x_1 ，数据方 P_2 持有数据 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 。

混淆电路（Garbled Circuit）是一种保护数据隐私的安全计算协议，可以用于实现多
方安全计算。具体地，可以将给定的计算任务（例如函数）转换为逻辑电路，所述逻辑
30 电路可以由至少一个运算门构成，所述运算门可以包括与门、或门、异或门等等。所述

逻辑电路可以包括至少两个输入线和至少一个输出线，通过对所述逻辑电路的输入线和/或输出线进行加密便可以得到混淆电路。多个数据方可以在不泄漏自身数据的前提下，使用所述混淆电路进行协作计算，得到所述计算任务的执行结果。

不经意传输 (Oblivious Transfer, OT), 又称为茫然传输, 是一种可以保护隐私的双方通信协议, 能够使通信双方以一种选择模糊化的方式传递数据。发送方可以具有多个数据。经由不经意传输接收方能够获得所述多个数据中的一个或多个数据。在此过程中, 发送方不知晓接收方接收的是哪些数据; 而接收方不能够获得其所接收数据之外的其它任何数据。不经意传输协议是混淆电路的基础协议。在使用混淆电路进行协作计算的过程中, 通常会使用到不经意传输协议。

10 以下介绍混淆电路的一个应用场景示例。

数据方 P_1 持有数据 x_1 和数据 x_3 , 数据方 P_2 持有数据 x_2 。函数 $y = f(x_1, x_2, x_3) = x_1 x_2 x_3$ 可以表示为如图1所示的逻辑电路。所述逻辑电路由与门1和与门2构成。所述逻辑电路可以包括输入线 a 、输入线 b 、输入线 d 、输出线 c 和输出线 s 。

以下介绍数据方 P_1 生成与门1的混淆真值表的过程。

15 与门1对应的真值表可以如表1所示。

表1

a	b	c
0	0	0
0	1	0
1	0	0
1	1	1

数据方 P_1 可以生成两个随机数 k_a^0 和 k_a^1 , 分别对应输入线 a 的两个输入值0和1; 可以生成两个随机数 k_b^0 和 k_b^1 , 分别对应输入线 b 的两个输入值0和1; 可以生成两个随机数 k_c^0 和 k_c^1 , 分别对应输出线 c 的两个输出值0和1。由此可以得到如表2所示的随机化真值表。

20

表2

a	b	c
k_a^0	k_b^0	k_c^0
k_a^0	k_b^1	k_c^0
k_a^1	k_b^0	k_c^0

k_a^1	k_b^1	k_c^1
---------	---------	---------

数据方 P_1 可以分别将随机数 k_a^0 和 k_b^0 作为密钥,对随机数 k_c^0 进行加密,得到随机数密文 $E_{k_a^0}(E_{k_b^0}(k_c^0))$;可以分别将随机数 k_a^0 和 k_b^1 作为密钥,对随机数 k_c^0 进行加密,得到随机数密文 $E_{k_a^0}(E_{k_b^1}(k_c^0))$;可以分别将随机数 k_a^1 和 k_b^0 作为密钥,对随机数 k_c^0 进行加密,得到随机数密文 $E_{k_a^1}(E_{k_b^0}(k_c^0))$;可以分别将随机数 k_a^1 和 k_b^1 作为密钥,对随机数 k_c^1 进行加密,得到随机数密文 $E_{k_a^1}(E_{k_b^1}(k_c^1))$ 。由此可以得到如表3所示的加密的随机化真值表。

表3

A	b	c
k_a^0	k_b^0	$E_{k_a^0}(E_{k_b^0}(k_c^0))$
k_a^0	k_b^1	$E_{k_a^0}(E_{k_b^1}(k_c^0))$
k_a^1	k_b^0	$E_{k_a^1}(E_{k_b^0}(k_c^0))$
k_a^1	k_b^1	$E_{k_a^1}(E_{k_b^1}(k_c^1))$

数据方 P_1 可以打乱表3中各行的排列顺序,得到如表4所示的混淆真值表。

表4

a	b	c
k_a^1	k_b^0	$E_{k_a^1}(E_{k_b^0}(k_c^0))$
k_a^0	k_b^1	$E_{k_a^0}(E_{k_b^1}(k_c^0))$
k_a^1	k_b^1	$E_{k_a^1}(E_{k_b^1}(k_c^1))$
k_a^0	k_b^0	$E_{k_a^0}(E_{k_b^0}(k_c^0))$

数据方 P_1 还可以生成与门2的混淆真值表,具体过程与生成与门1的混淆真值表的过程相类似,在此不再详述。

数据方 P_1 可以分别将与门1的混淆真值表和与门2的混淆真值表发送给数据方 P_2 。数据方 P_2 可以接收与门1的混淆真值表和与门2的混淆真值表。

数据方 P_1 可以将数据 x_1 的各个比特(bit)在输入线a对应的随机数发送给数据方 P_2 ;可以将数据 x_3 的各个比特(bit)在输入线d对应的随机数发送给数据方 P_2 。数据方 P_2 可以接收数据 x_1 和数据 x_3 的各个比特对应的随机数。例如,数据

$x_1 = b_0 \times 2^0 + b_1 \times 2^1 + \dots + b_i \times 2^i + \dots$ 。对于数据 x_1 的第 i 个比特 b_i ，当 b_i 的值为0时，数据方 P_1 可以将 b_i 在输入线 a 对应的随机数 k_a^0 发送给数据方 P_2 ；当 b_i 的值为1时，数据方 P_1 可以将 b_i 在输入线 a 对应的随机数 k_a^1 发送给数据方 P_2 。

数据方 P_1 可以以随机数 k_a^0 和 k_a^1 作为输入，数据方 P_2 可以以数据 x_2 的各个比特作为输入，二者进行不经意传输。数据方 P_2 可以获得数据 x_2 的各个比特对应的随机数。具体地，数据方 P_1 可以生成两个随机数 k_a^0 和 k_a^1 ，分别对应输入线 d 的两个输入值0和1。如此针对数据 x_2 的每个比特，数据方 P_1 可以以随机数 k_a^0 和 k_a^1 作为在不经意传输过程中输入的秘密信息，数据方 P_2 可以以该比特作为在不经意传输过程中输入的选择信息，进行不经意传输。通过不经意传输，数据方 P_2 可以获得该比特在输入线 d 对应的随机数。具体地，当该比特的值为0时，数据方 P_2 可以获得随机数 k_a^1 ；当该比特的值为1时，数据方 P_2 可以获得随机数 k_a^0 。根据不经意传输的特性，数据方 P_1 并不知晓数据方 P_2 具体选择的是哪个随机数，数据方 P_2 也不能够知晓除了所选择的随机数以外的其它随机数。

通过以上过程，数据方 P_2 获得了数据 x_1 、数据 x_2 和数据 x_3 的各个比特对应的随机数。如此数据方 P_2 可以使用数据 x_1 的每个比特在输入线 a 对应的随机数、以及数据 x_2 的相应比特在输入线 b 对应的随机数，尝试对与门1的混淆真值表中的4个随机数密文进行解密；数据方 P_2 仅能够成功解密其中的一个随机数密文，从而得到输出线 c 的一个随机数。接下来，数据方 P_2 可以使用数据 x_3 的相应比特在输入线 d 对应的随机数、以及解密出的输出线 c 的随机数，尝试对与门2的混淆真值表中的4个随机数密文进行解密；数据方 P_2 仅能够成功解密其中的一个随机数密文，得到输出线 s 的一个随机数。数据方 P_2 可以将解密出的输出线 s 的随机数发送给数据方 P_1 。数据方 P_1 可以接收输出线 s 的随机数；可以根据输出线 s 的随机数、以及随机数和输出值的对应关系，获得输出线 s 的输出值。

输出线 s 的每个输出值可以视作函数 $y = f(x_1, x_2, x_3) = x_1 x_2 x_3$ 取值的一个比特。如此数据方 P_1 可以根据输出线 s 的多个输出值，确定出函数 $y = f(x_1, x_2, x_3) = x_1 x_2 x_3$ 的取值。

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。

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。

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。激励函数通常为非线性函数。通过激励函数可以在所述数据处理模型中加入非线性因素，提高所述数据处理模型的表达能力。所述激励函数可以包括 Sigmoid 函数、Tanh 函数和 ReLU 函数等。所述数据处理模型可以包括逻辑回归模型和神经网络模型等。

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持有的数据的前提下，基于自身持有的数据，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，可以使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。模型参数优化方法可以包括梯度下降法、牛顿法等等。其中，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，从而降低过拟合的危险）。所述模型参数优化方法可以仅采用秘密分享的方式来实现；或者，还可以采用秘密分享和混淆电路相结合的方式来实现。

本说明书提供模型参数确定系统的一个实施例。

请参阅图2。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）。

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，所述第三方可以生成随机正交矩阵，可以将所述随机正交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正交矩阵中各个随机数的第一份额形成的矩阵作为所述随机正交矩阵的第一份额，将所述随机正交矩阵中各个随机数的第二份额形成的矩阵作为所述随机正交矩阵的第二份额；可以向所述第一数据方发送所述随机正交矩阵的第一份额，可以向所述第二数据方发送所述随机正交矩阵的第二份额。其中，所述随机正交矩阵的第一份额和所述随机正交矩阵的第二份额的和等于所述随机正交矩阵。另外，一方面所述随机正交矩阵可以由随机数构成的随机数矩阵；另一方面所述随机正交矩阵还可以为正交矩阵。一

个方阵与一个正交矩阵相乘后可以得到一个新的矩阵，该新的矩阵与该方阵具有相同的条件数。这样便于第一数据方和第二数据方在不泄漏自身持有的海森矩阵的份额的条件下，协作计算得到海森矩阵的条件数；进而便于根据条件数来度量海森矩阵的病态程度。具体过程详见后面的实施例。

- 5 鉴于所述第一数据方和所述第二数据方在基于混淆电路进行计算的过程中涉及到不经意传输，所述第三方还可以生成第一OT随机数和第二OT随机数；可以向所述第一数据方发送所述第一OT随机数；可以向所述第二数据方发送所述第二OT随机数。OT随机数可以为在不经意传输过程中所使用到的随机数。

10 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持有特征数据的数据方，所述第二数据方可以为持有标签的数据方。例如，所述第一数据方可以持有完整的特征数据，所述第二数据方可以持有特征数据的标签。或者，所述第一数据方可以持有特征数据的一部分数据项，所述第二数据方可以持有特征数据的另一部分数据项和特征数据的标签。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持有用户的储蓄金额，所述第二数据方可以持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0和1。值得说明的是，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。

- 15 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第一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第一模型参数的第一份额，可以将所述第二数据方获得份额作为第一模型参数的第二份额。第一模型参数的第一份额和第一模型参数的第二份额的和等于第一模型参数。

20 所述第一数据方可以接收随机正交矩阵的第一份额和第一OT随机数。所述第二数据方可以接收随机正交矩阵的第二份额和第二OT随机数。如此所述第一数据方可以基于第一模型参数的第一份额、特征数据、随机正交矩阵的第一份额和第一OT随机数，所述第二数据方可以基于第一模型参数的第二份额、标签值、随机正交矩阵的第二份额和第二OT随机数，协作确定新的第一模型参数。所述第一数据方和所述第二数据方可以分别获得新的第一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。

- 25 基于上述模型参数确定系统实施例，下面将结合图3，详细描述本说明书模型参数确

定方法的一个实施例。该实施例可以包括以下步骤。

步骤S11: 第一数据方根据第一乘积的第一份额, 第二数据方根据第一乘积的第二份额, 基于激励函数对应的混淆电路进行通信。第一数据方获得激励函数取值的第一份额, 第二数据方获得激励函数取值的第二份额。

5 步骤S13: 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。第一数据方获得损失函数梯度的第一份额, 第二数据方获得损失函数梯度的第二份额。

步骤S15: 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。

步骤S17: 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。

15 步骤S19: 第一数据方根据第一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, 第二数据方根据第一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, 秘密分享新的第一模型参数。第一数据方获得新的第一模型参数的第一份额, 第二数据方获得新的第一模型参数的第二份额。

下面介绍在实施例中涉及的一些术语。

20 (一)、第一乘积、第二乘积、第三乘积、第四乘积和第五乘积。所述第一乘积可以为第一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正交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。所述第四乘积可以为损失函数梯度的第一份额与预设步长的乘积。所述第五乘积可以为损失函数梯度的第二份额与预设步长的乘积。

25 在一些场景示例中, 所述第一乘积可以表示为 XW ; 其中, W 表示第一模型参数, 具体为第一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。

所述第二乘积可以表示为 HR , 其中, H 表示海森矩阵, R 表示随机正交矩阵。

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。

所述第四乘积可以表示为 $G < dW >_0$, 所述第五乘积可以表示为 $G < dW >_1$ 。其中, G

表示预设步长, $\langle dW \rangle_0$ 表示损失函数梯度的第一份额, $\langle dW \rangle_1$ 表示损失函数梯度的第二份额, $\langle dW \rangle_0 + \langle dW \rangle_1 = dW$ 。

(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。

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 $(HR)^{-1}$ 。

在一些实施例中, 在步骤S11之前, 所述第一数据方可以根据持有的特征数据和第一模型参数的第一份额, 所述第二数据方可以根据持有的第一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。

延续前面的场景示例, 第一模型参数的第一份额可以表示为 $\langle W \rangle_0$, 第一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 $\langle XW \rangle_1$ 。 $\langle XW \rangle_0 + \langle XW \rangle_1 = XW$ 。

20

在一些实施例中, 可以根据所述激励函数构建相应的逻辑电路。所述逻辑电路可以由所述第一数据方构建; 或者, 也可以由所述第二数据方构建; 又或者, 还可以由其它设备 (例如可信任的第三方) 构建。所述逻辑电路可以由至少一个运算门构成, 所述运算门可以包括与门、或门、异或门等等。所述逻辑电路可以包括至少两个输入线和至少一个输出线, 通过对所述逻辑电路的输入线和/或输出线进行加密便可以得到混淆电路。所述混淆电路可以包括所述逻辑电路中各个运算门的混淆真值表。值得说明的是, 这里可以直接根据激励函数构建逻辑电路; 或者, 也可以对激励函数进行各种适当的变形, 可以根据变形后的激励函数构建逻辑电路; 又或者, 还可以以所述激励函数为基础生成其它函数, 可以根据其它函数构建逻辑电路。相应地, 这里激励函数与混淆电路相对应

25

可以理解为：混淆电路是根据激励函数的逻辑电路生成的，或者，混淆电路是根据变形后的激励函数的混淆电路生成的，又或者，混淆电路是根据其它函数的逻辑电路生成的。

所述第一数据方和所述第二数据方均可以持有激励函数对应的混淆电路。在一些实施方式中，所述混淆电路可以由所述第一数据方生成。所述第一数据方可以将生成的混淆电路发送给所述第二数据方。所述第二数据方可以接收所述混淆电路。在另一些实施方式中，所述混淆电路也可以由所述第二数据方生成。所述第二数据方可以将生成的混淆电路发送给所述第一数据方。所述第一数据方可以接收所述混淆电路。

在步骤S11中，第一数据方可以根据第一乘积的第一份额，第二数据方可以根据第一乘积的第二份额，基于激励函数对应的混淆电路进行通信。所述第一数据方和所述第二数据方可以分别获得激励函数取值的一份份额。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。

请参阅图4。以下介绍第一数据方和第二数据方基于混淆电路进行计算的一个场景示例。

可以根据激励函数 $f(x_1, x_2)$ 构建函数 $y = f_1(x_1, x_2, x_3) = f(x_1, x_2) - x_3$ 。其中， x_1 用于表示第一乘积的第一份额， x_2 用于表示第一乘积的第二份额， x_3 用于表示激励函数取值的一份份额（以下称为激励函数取值的第二份额）， $f_1(x_1, x_2, x_3)$ 的取值用于表示激励函数取值的另一份份额（以下称为激励函数取值的第一份额）。

可以构建与函数 $f_1(x_1, x_2, x_3) = f(x_1, x_2) - x_3$ 相对应的逻辑电路，通过对该逻辑电路的输入线和/或输出线进行加密便可以得到混淆电路。所述第一数据方和所述第二数据方均可以持有该混淆电路。值得说明的是，函数 $y = f_1(x_1, x_2, x_3) = f(x_1, x_2) - x_3$ 及其对应的逻辑电路可以由所述第一数据方构建；或者，也可以由所述第二数据方构建；又或者，还可以由其它设备（例如可信任的第三方）构建。

所述第二数据方可以生成激励函数取值的一份份额作为第二份额。如此所述第一数据方可以以第一乘积的第一份额作为该混淆电路的输入，所述第二数据方可以以第一乘积的第二份额以及激励函数取值的第二份额作为该混淆电路的输入，进行通信。所述第一数据方可以基于该混淆电路计算得到激励函数取值的另一份份额作为第一份额。具体的计算过程可以参见前面有关介绍混淆电路的场景示例，在此不再详述。

在一些实施方式中, 为了降低混淆电路的复杂程度, 还可以使用分段线性函数拟合所述激励函数。这样便可以根据所述分段线性函数构建相应的逻辑电路, 通过对该逻辑电路的输入线和/或输出线进行加密便可以得到混淆电路。所述第一数据方和所述第二数据方均可以持有该混淆电路。例如, 所述激励函数可以为Sigmoid函数, 所述分段线性函

$$5 \quad \text{数可以为 } y = f(x) = \begin{cases} 1 & x \geq \frac{0.5}{k} \\ kx + 0.5 & -\frac{0.5}{k} < x < \frac{0.5}{k} \\ 0 & x \leq -\frac{0.5}{k} \end{cases}, \quad k \text{ 表示分段线性函数的系数。}$$

第一数据方可以根据第一乘积的第一份额, 第二数据方可以根据第一乘积的第二份额, 基于该混淆电路进行通信。所述第一数据方和所述第二数据方可以分别获得分段线性函数取值的一份份额。为了便于描述, 可以将所述第一数据方获得的份额作为分段线性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分段线性函数取值的第二份额。分段线性函数取值的第一份额和分段线性函数取值的第二份额的和等于分段线性函数的取值。如此所述第一数据方可以将分段线性函数取值的第一份额作为激励函数取值的第一份额。所述第二数据方可以将分段线性函数取值的第二份额作为激励函数取值的第二份额。

15 在一些实施例中, 在步骤S13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。

20 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 $\langle dW \rangle_1$ 。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。

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

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

5 获得 $\langle X^T Y \rangle_1$ 。 $\langle X^T Y \rangle_0 + \langle X^T Y \rangle_1 = X^T Y$ 。

所述第一数据方可以计算 $X^T < a \rangle_0$ ；可以计算
 $X^T < a \rangle_0 + \langle [X^T < a \rangle_1] \rangle_0 - \langle X^T Y \rangle_0$ 作为损失函数梯度 dW 的第一份额 $\langle dW \rangle_0$ 。所述
 第二数据方可以计算 $\langle [X^T < a \rangle_1] \rangle_1 - \langle X^T Y \rangle_1$ 作为损失函数梯度 dW 的第二份额
 $\langle dW \rangle_1$ 。

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

在一些实施例中，在步骤S15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。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。

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。如此所述
 所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
 25 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。

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 $\langle a \rangle_1$ ，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 。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。

- 5 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， $\bullet$ 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，
 $m \bullet n = (m_1 n_1, m_2 n_2, m_3 n_3)$ 。

- 10 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 $\langle r \rangle_1 = \langle a \rangle_1 - \langle [\langle a \rangle_0 \bullet \langle a \rangle_1] \rangle_1 - \langle a \rangle_1 \bullet \langle a \rangle_1$ 。

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

- $\langle r \rangle_0$ 、 $\langle r \rangle_1$ 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
15 $RNN = \text{diag}(r)$ 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 。
20

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 $\langle H \rangle_1$ 。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。

- 25 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 $X^T RNN_1$ 。

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 $\langle X^T RNN_1 \rangle_1$ 。

$$\langle X^T RNN_1 \rangle_0 + \langle X^T RNN_1 \rangle_1 = X^T RNN_1。$$

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

5 以获得 $\langle [\langle X^T RNN_1 \rangle_1 X] \rangle_1$ 。

$$\langle [\langle X^T RNN_1 \rangle_1 X] \rangle_0 + \langle [\langle X^T RNN_1 \rangle_1 X] \rangle_1 = \langle X^T RNN_1 \rangle_1 X。$$

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 $\langle H \rangle_1$ 。

$$\begin{aligned} H &= \langle H \rangle_0 + \langle H \rangle_1 \\ &= X^T RNN_0 X + \langle X^T RNN_1 \rangle_0 X + \langle [\langle X^T RNN_1 \rangle_1 X] \rangle_0 + \langle [\langle X^T RNN_1 \rangle_1 X] \rangle_1 \\ 10 \quad &= X^T RNN_0 X + \langle X^T RNN_1 \rangle_0 X + \langle X^T RNN_1 \rangle_1 X \\ &= X^T RNN_0 X + X^T RNN_1 X \\ &= X^T RNN X \end{aligned}$$

在一些实施例中，第三方可以向第一数据方下发随机正交矩阵的第一份额；可以向第二数据方下发随机正交矩阵的第二份额。随机正交矩阵的第一份额和随机正交矩阵的第二份额的和等于随机正交矩阵。所述第一数据方可以接收随机正交矩阵的第一份额，

15 所述第二数据方可以接收随机正交矩阵的第二份额。如此在步骤S17中，所述第一数据方可以根据随机正交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正交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

20 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。

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持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

25 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持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。

所述第一数据方可以将随机正交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正交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。

延续前面的场景示例，随机正交矩阵的第一份额可以表示为 $\langle R \rangle_0$ ，随机正交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 $\langle HR \rangle_1$ 。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。

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 $\langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_1$ 。 $\langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_0 + \langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_1 = \langle H \rangle_0 \langle R \rangle_1$ 。

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 $\langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_1$ 。 $\langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_0 + \langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_1 = \langle H \rangle_1 \langle R \rangle_0$ 。

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 $\langle HR \rangle_1$ 。

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

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 $\langle HR \rangle_0$ 与自身持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 $(HR)^{-1}$ 。

所述第一数据方可以将第二逆矩阵 $(HR)^{-1}$ 与随机正交矩阵的第一份额 $\langle R \rangle_0$ 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 $(HR)^{-1}$ 与随机正交矩阵的第二份额 $\langle R \rangle_1$ 相乘，得到第一逆矩阵 H^{-1} 的第一份额 $\langle H^{-1} \rangle_1$ 。

$$H^{-1} = \langle H^{-1} \rangle_0 + \langle H^{-1} \rangle_1 = \langle R \rangle_0 (HR)^{-1} + \langle R \rangle_1 (HR)^{-1} = R \times (HR)^{-1}.$$

在一些实施例中，在步骤S19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。

所述第一数据方可以将第一模型参数的第一份额与第三乘积的第一份额相减，得到新的第一模型参数的第一份额。所述第二数据方可以将第一模型参数的第二份额与第三乘积的第二份额相减，得到新的第一模型参数的第二份额。

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 $\langle H^{-1} \times dW \rangle_1$ 。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。

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 $\langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_1$ 。

$$5 \quad \langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_0 + \langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_1 = \langle H^{-1} \rangle_0 \langle dW \rangle_1。$$

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 $\langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_1$ 。

$$\langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_0 + \langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_1 = \langle H^{-1} \rangle_1 \langle dW \rangle_0。$$

10 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 $\langle H^{-1} \times dW \rangle_1$ 。

$$\begin{aligned} H^{-1} \times dW &= \langle H^{-1} \times dW \rangle_0 + \langle H^{-1} \times dW \rangle_1 \\ &= \langle H^{-1} \rangle_0 \langle dW \rangle_0 + \langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_0 + \langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_0 + \\ 15 \quad &\langle H^{-1} \rangle_1 \langle dW \rangle_1 + \langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_1 + \langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_1 \\ &= \langle H^{-1} \rangle_0 \langle dW \rangle_0 + \langle H^{-1} \rangle_0 \langle dW \rangle_1 + \langle H^{-1} \rangle_1 \langle dW \rangle_0 + \langle H^{-1} \rangle_1 \langle dW \rangle_1 \\ &= (\langle H^{-1} \rangle_0 + \langle H^{-1} \rangle_1)(\langle dW \rangle_0 + \langle dW \rangle_1) \end{aligned}$$

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 $\langle W' \rangle_1 = \langle W \rangle_1 - \langle H^{-1} \times dW \rangle_1$ ， $\langle W' \rangle_0$ 表示新的第一模型参数的第一份额， $\langle W' \rangle_1$ 表示新的第一模型参数的第二份额， W' 表示新的第一模型参数。

$$20 \quad W' = \langle W' \rangle_0 + \langle W' \rangle_1 = \langle W \rangle_0 - \langle H^{-1} \times dW \rangle_0 + \langle W \rangle_1 - \langle H^{-1} \times dW \rangle_1 = W - H^{-1} \times dW。$$

牛顿法有着较快的收敛速度。步骤S11-步骤S19的模型参数确定方法，由于使用了牛顿法，不仅可以保护合作建模各方（第一数据方和第二数据方）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。

另外，由于数据处理模型中的激励函数通常为非线性函数，涉及的运算为非线性运

算，导致其取值无法直接使用秘密分享算法进行计算。因此若仅通过秘密分享，使用牛顿法协作确定数据处理模型的模型参数，则需要使用多项式来拟合所述激励函数。使用多项式来拟合激励函数存在越界的问题（多项式的输入超过一定范围时，其输出会变得很大或者很小），有可能造成数据处理模型无法完成训练。而混淆电路的复杂程度较高，

5 因此若仅通过混淆电路，使用牛顿法协作确定数据处理模型的模型参数，会造成数据处理模型的训练过程变得复杂。步骤S11-步骤S19的模型参数确定方法，通过秘密分享和混淆电路相结合的方式，不仅可以避免越界的问题，还可以降低数据处理模型训练过程的复杂程度。

10 在一些实施例中，在步骤S17之前，第一数据方可以根据随机正交矩阵的第一份额和海森矩阵的第一份额，第二数据方可以根据随机正交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。第一数据方可以获得第二乘积的第一份额，第二数据方可以获得第二乘积的第二份额。所述第二乘积为随机正交矩阵和海森矩阵之间的乘积。关于秘密分享第二乘积的具体过程可以参见上文中的有关描述。

15 如此在步骤S17中，在第二乘积的条件数满足预设条件时，第一数据方可以根据海森矩阵的第一份额，第二数据方可以根据海森矩阵的第二份额，秘密分享第一逆矩阵。第一数据方可以获得第一逆矩阵的第一份额，第二数据方可以获得第一逆矩阵的第二份额。

所述预设条件可以包括：条件数小于或等于预设阈值。所述预设阈值可以为经验值，或者，还可以采用其它方式（例如机器学习的方式）获得。

20 所述第一数据方和所述第二数据方均可以持有所述预设条件。进而，所述第一数据方和所述第二数据方可以分别判断第二乘积的条件数是否满足所述预设条件。在一些实施方式中，可以由第一数据方计算第二乘积的条件数。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持有的第二乘积的第一份额相加，得到第二乘积；

25 可以计算第二乘积的条件数；可以判断第二乘积的条件数是否满足所述预设条件；可以向所述第二数据方发送第二乘积的条件数。所述第二数据方可以接收第二乘积的条件数；可以判断第二乘积的条件数是否满足所述预设条件。在另一些实施方式中，还可以由第二数据方计算第二乘积的条件数。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持有的第二乘积的第二份额相加，得到第二乘积；可以计算第二乘积

30

的条件数；可以判断第二乘积的条件数是否满足所述预设条件；可以向所述第一数据方发送第二乘积的条件数。所述第一数据方可以接收第二乘积的条件数；可以判断第二乘积的条件数是否满足所述预设条件。

或者，可以仅由第一数据方持有所述预设条件，进而仅由第一数据方判断第二乘积的条件数是否满足所述预设条件。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持有的第二乘积的第一份额相加，得到第二乘积；可以计算第二乘积的条件数；可以判断第二乘积的条件数是否满足所述预设条件；可以向所述第二数据方发送判断结果信息。所述第二数据方可以接收判断结果信息。

又或者，可以仅由第二数据方持有所述预设条件，进而仅由第二数据方判断第二乘积的条件数是否满足所述预设条件。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持有的第二乘积的第二份额相加，得到第二乘积；可以计算第二乘积的条件数；可以判断第二乘积的条件数是否满足所述预设条件；可以向所述第一数据方发送判断结果信息。所述第一数据方可以接收判断结果信息。

如前面所述，一个方阵与一个正交矩阵相乘后可以得到一个新的矩阵，该新的矩阵与该方阵具有相同的条件数。鉴于海森矩阵为方阵，因而第二乘积的条件数等于海森矩阵的条件数。这样便实现了第一数据方和第二数据方在不泄漏自身持有的海森矩阵的份额的条件下，协作计算得到海森矩阵的条件数。

第二乘积的条件数满足所述预设条件，表明第二乘积的病态程度较小，即表明海森矩阵的病态程度较小，因而可以使用牛顿法确定模型参数。

第二乘积的条件数不满足所述预设条件，表明第二乘积的病态程度较大，即表明海森矩阵的病态程度较大，无法使用牛顿法确定模型参数，因而可以使用梯度下降法代替牛顿法确定模型参数。具体地，所述第一数据方可以根据第一模型参数的第一份额、损失函数梯度的第一份额和预设步长，计算新的第一模型参数的第一份额。所述第二数据方可以根据第一模型参数的第二份额、损失函数梯度的第二份额和预设步长，计算新的第一模型参数的第二份额。

所述预设步长可以用于控制梯度下降法的迭代速度。所述预设步长可以为任意适当正实数。例如，当预设步长过大时，迭代速度会过快，导致有可能无法获得最优模型参数。当预设步长过小时，导致迭代速度会过慢，导致花费的时间较长。所述预设步长具

体可以为经验值；或者，也可以采用机器学习的方式得到。当然，所述预设步长还可以采用其它方式得到。所述第一数据方和所述第二数据方均可以持有所述预设步长。

所述第一数据方可以将损失函数梯度的第一份额与预设步长相乘，得到第四乘积；可以将第一模型参数的第一份额与第四乘积相减，得到新的第一模型参数的第一份额。

- 5 所述第二数据方可以将损失函数梯度的第二份额与预设步长相乘，得到第五乘积；可以将第一模型参数的第二份额与第五乘积相减，得到新的第一模型参数的第二份额。新的第一模型参数的第一份额和新的第一模型参数的第二份额的和等于新的第一模型参数。

- 延续前面的场景示例，所述第一数据方可以将损失函数梯度的第一份额 $\langle dW \rangle_0$ （具体为向量）与预设步长 G 相乘（具体为向量的数乘），得到第四乘积 $G \langle dW \rangle_0$ ；可以将
10 第一模型参数的第一份额 $\langle W \rangle_0$ 与第四乘积 $G \langle dW \rangle_0$ 相减，得到新的第一模型参数的第一份额 $\langle W' \rangle_0 = \langle W \rangle_0 - G \langle dW \rangle_0$ 。

- 所述第二数据方可以将损失函数梯度的第二份额 $\langle dW \rangle_1$ （具体为向量）与预设步长 G 相乘（具体为向量的数乘），得到第五乘积 $G \langle dW \rangle_1$ ；可以将第一模型参数的第二份额 $\langle W \rangle_1$ 与第五乘积 $G \langle dW \rangle_1$ 相减，得到新的第一模型参数的第二份额
15 $\langle W' \rangle_1 = \langle W \rangle_1 - G \langle dW \rangle_1$ 。其中， $\langle W' \rangle_0 + \langle W' \rangle_1 = W'$ ， W' 表示新的第一模型参数。

这样通过条件数和预设条件，本实施例可以避免在使用牛顿法确定模型参数的过程中由于出现病态矩阵所导致的不收敛问题。

- 在本实施例的一些实施方式中，还可以包括对数据处理模型的模型参数进行迭代优化调整的过程。具体地，可以重复执行秘密分享第一乘积的步骤，所述第一数据方可以获得新的第一乘积的第一份额，所述第二数据方可以获得新的第一乘积的第二份额。新的第一乘积为特征数据和新的第一模型参数的乘积。可以重复执行步骤S11，所述第一数据方可以获得新的激励函数取值的第一份额，所述第二数据方可以获得新的激励函数取值的第二份额。可以重复执行步骤S13，所述第一数据方可以获得新的损失函数梯度的第一份额，所述第二数据方可以获得新的损失函数梯度的第二份额。可以重复执行步骤S15，
20 所述第一数据方可以获得新的海森矩阵的第一份额，所述第二数据方可以获得新的海森矩阵的第二份额。可以重复执行秘密分享第二乘积的步骤，所述第一数据方可以获得新的第二乘积的第一份额，所述第二数据方可以获得新的第二乘积的第二份额。新的第二乘积为随机正交矩阵和新的海森矩阵之间的乘积。

在新的第二乘积的条件数满足预设条件时，表明在该轮迭代过程中可以继续使用牛顿法确定模型参数。可以重复执行步骤S17，所述第一数据方可以获得新的第一逆矩阵的第一份额，所述第二数据方可以获得新的第一逆矩阵的第二份额。新的第一逆矩阵为新的海森矩阵的逆矩阵。所述第一数据方可以根据新的第一模型参数的第一份额、新的第一逆矩阵的第一份额和新的损失函数梯度的第一份额，所述第二数据方可以根据新的第一模型参数的第二份额、新的第一逆矩阵的第二份额和新的损失函数梯度的第二份额，秘密分享第二模型参数。所述第一数据方可以获得第二模型参数的第一份额，所述第二数据方可以获得第二模型参数的第二份额。第二模型参数的第一份额和第二模型参数的第二份额的和等于第二模型参数。这样可以通过秘密分享和混淆电路相结合的方式实现迭代过程。通过秘密分享和混淆电路相结合的方式，不仅可以避免越界的问题，还可以降低数据处理模型训练过程的复杂程度。另外在迭代的过程中，由于使用了牛顿法，不仅可以保护合作建模各方（第一数据方和第二数据方）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。

在新的第二乘积的条件数不满足预设条件时，表明在该轮迭代过程中无法继续使用牛顿法确定模型参数，因而可以使用梯度下降法代替牛顿法确定模型参数。所述第一数据方可以根据新的第一模型参数的第一份额、新的损失函数梯度的第一份额和预设步长，计算第二模型参数的第一份额。具体计算过程与根据第一模型参数的第一份额、损失函数梯度的第一份额和预设步长，计算新的第一模型参数的第一份额的过程相类似。所述第二数据方可以根据新的第一模型参数的第二份额、新的损失函数梯度的第二份额和预设步长，计算第二模型参数的第二份额。具体计算过程与根据第一模型参数的第二份额、损失函数梯度的第二份额和预设步长，计算新的第一模型参数的第二份额的过程相类似。这样可以通过秘密分享和混淆电路相结合的方式实现迭代过程。通过秘密分享和混淆电路相结合的方式，不仅可以避免越界的问题，还可以降低数据处理模型训练过程的复杂程度。另外在迭代的过程中，使用了梯度下降法。

在本实施例的另一些实施方式中，还可以包括对数据处理模型的模型参数进行迭代优化调整的过程。具体地，可以重复执行秘密分享第一乘积的步骤，所述第一数据方可以获得新的第一乘积的第一份额，所述第二数据方可以获得新的第一乘积的第二份额。新的第一乘积为特征数据和新的第一模型参数的乘积。所述第一数据方可以根据新的第一乘积的第一份额，所述第二数据方可以根据新的第一乘积的第二份额，秘密分享新的

激励函数的取值。所述第一数据方可以获得新的激励函数取值的第一份额，所述第二数据方可以获得新的激励函数取值的第二份额。可以重复执行步骤S13，所述第一数据方可以获得新的损失函数梯度的第一份额，所述第二数据方可以获得新的损失函数梯度的第二份额。可以重复执行步骤S15，所述第一数据方可以获得新的海森矩阵的第一份额，所述
5 所述第二数据方可以获得新的海森矩阵的第二份额。可以重复执行秘密分享第二乘积的步骤，所述第一数据方可以获得新的第二乘积的第一份额，所述第二数据方可以获得新的第二乘积的第二份额。新的第二乘积为随机正交矩阵和新的海森矩阵之间的乘积。

在新的第二乘积的条件数满足预设条件时，表明在该轮迭代过程中可以继续使用牛顿法确定模型参数。可以重复执行步骤S17，所述第一数据方可以获得新的第一逆矩阵的
10 第一份额，所述第二数据方可以获得新的第一逆矩阵的第二份额。新的第一逆矩阵为新的海森矩阵的逆矩阵。所述第一数据方可以根据新的第一模型参数的第一份额、新的第一逆矩阵的第一份额和新的损失函数梯度的第一份额，所述第二数据方根据新的第一模型参数的第二份额、新的第一逆矩阵的第二份额和新的损失函数梯度的第二份额，秘密分享第二模型参数。所述第一数据方可以获得第二模型参数的第一份额，所述第二数据
15 方可以获得第二模型参数的第二份额。第二模型参数的第一份额和第二模型参数的第二份额的和等于第二模型参数。这样可以通过秘密分享的方式实现迭代过程。另外在迭代的过程中，由于使用了牛顿法，不仅可以保护合作建模各方（第一数据方和第二数据方）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。

在新的第二乘积的条件数不满足预设条件时，表明在该轮迭代过程中无法继续使用
20 牛顿法确定模型参数，因而可以使用梯度下降法代替牛顿法确定模型参数。所述第一数据方可以根据新的第一模型参数的第一份额、新的损失函数梯度的第一份额和预设步长，计算第二模型参数的第一份额。具体计算过程与根据第一模型参数的第一份额、损失函数梯度的第一份额和预设步长，计算新的第一模型参数的第一份额的过程相类似。所述
25 第二数据方可以根据新的第一模型参数的第二份额、新的损失函数梯度的第二份额和预设步长，计算第二模型参数的第二份额。具体计算过程与根据第一模型参数的第二份额、损失函数梯度的第二份额和预设步长，计算新的第一模型参数的第二份额的过程相类似。这样可以通过秘密分享的方式实现迭代过程。另外在迭代的过程中，使用了梯度下降法。

以下介绍所述第一数据方根据新的第一乘积的第一份额，所述第二数据方根据新的第一乘积的第二份额，秘密分享新的激励函数的取值的过程。

30 所述第一数据方可以根据新的第一乘积的第一份额，所述第二数据方可以根据新的

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新的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新的激励函数取值的第二份额。新的激励函数取值

5 的第一份额和新的激励函数取值的第二份额的和等于新的激励函数的取值。

本实施例的模型参数确定方法，第一数据方和第二数据方可以在不泄漏自身所持有的数据的前提下，协作确定数据处理模型的模型参数。

10 上文中结合图3，详细描述本说明书模型参数确定方法的一个实施例。上文中第一数据方执行的方法步骤，可以单独实现为第一数据方侧的模型参数确定方法；第二数据方执行的方法步骤，可以单独实现为第二数据方侧的模型参数确定方法。下面将结合图5和图6，详细描述本说明书实施例中第一数据方侧的模型参数确定方法、以及第二数据方侧的模型参数确定方法。

15 本说明书还提供模型参数确定方法的另一个实施例。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第一模型参数的份额。请参阅图5。该实施例可以包括以下步骤。

步骤 S21：根据第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到激励函数取值的份额，所述第一乘积为特征数据和第一模型参数的乘积。

20 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。具体地，所述第一数据方可以根据特征数据和第一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；可以根据第一乘积的份额和激励函数对应的混淆电路与合作方通信，得到激励函数取值的份额。具体过程可以参见前面步骤 S11 的相关描述，在此不再赘述。

25 步骤 S23：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。

在一些实施例中，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数的梯度，得到损失函数梯度的份额。具体过程可以参见前面步骤 S13 的相关描述，在此不再赘述。

30 步骤 S25：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。

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 S15 的相关描述，在此不再赘述。

步骤 S27：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。

在一些实施例中，所述第一数据方可以根据随机正交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正交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正交矩阵的份额相乘，得到第一逆矩阵的份额。具体过程可以参见前面步骤 S17 的相关描述，在此不再赘述。

或者，在另一些实施例中，所述第一数据方可以根据随机正交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正交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正交矩阵的份额相乘，得到第一逆矩阵的份额。具体过程可以参见前面步骤 S17 的相关描述，在此不再赘述。

步骤 S29：根据第一模型参数的份额、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第一模型参数，得到新的第一模型参数的份额。

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和损失函数梯度之间的乘积。所述第一数据方可以将第一模型参数的份额与第三乘积的份额相减，得到新的第一模型参数的份额。具体过程可以参见前面步骤 S19 的相关描述，在此不再赘述。

在一些实施例中，所述第一数据方可以根据随机正交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正交矩阵和海森矩阵之间的乘积。

如此在步骤 S27 中，所述第一数据方可以在第二乘积的条件数满足预设条件时，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。其中，第二乘积的条件数可以由第一数据方和/或合作方来计算。第二乘积的条件数等于海森矩阵的条件数。

第二乘积的条件数满足所述预设条件，表明第二乘积的病态程度较小，可以使用牛
5 顿法确定模型参数。

第二乘积的条件数不满足所述预设条件，表明第二乘积的病态程度较大，无法使用
牛顿法确定模型参数，因而可以使用梯度下降法代替牛顿法确定模型参数。所述第一数
据方可以根据第一模型参数的份额、损失函数梯度的份额和预设步长，计算新的第一模
型参数的份额。所述第一数据方具体可以将损失函数梯度的份额与预设步长相乘，得到
10 第四乘积；可以将第一模型参数的份额与第四乘积相减，得到新的第一模型参数的份额。

在本实施例的一些实施方式中，还可以包括对数据处理模型的模型参数进行迭代优
化调整的过程。具体地，所述第一数据方可以重复执行秘密分享第一乘积的步骤，得到
新的第一乘积的份额；可以重复执行步骤S21，得到新的激励函数取值的份额；可以重复
执行步骤S23，得到新的损失函数梯度的份额；可以重复执行步骤S25，得到新的海森矩
15 阵的份额；可以重复执行秘密分享第二乘积的步骤，得到新的第二乘积的份额。新的第
二乘积为随机正交矩阵和新的海森矩阵之间的乘积。

在新的第二乘积的条件数满足预设条件时，表明可以继续使用牛顿法确定模型参数。
所述第一数据方可以重复执行步骤S27，得到新的第一逆矩阵的份额。新的第一逆矩阵为
新的海森矩阵的逆矩阵。所述第一数据方进而可以根据新的第一逆矩阵的份额、新的损
20 失函数梯度的份额和新的第一模型参数的份额与合作方秘密分享第二模型参数，得到第
二模型参数的份额。

在新的第二乘积的条件数不满足预设条件时，表明需要使用梯度下降法代替牛顿法
确定模型参数。所述第一数据方可以根据新的第一模型参数的份额、新的损失函数梯度
的份额和预设步长，计算第二模型参数的份额。

25 在本实施例的另一些实施方式中，还可以包括对数据处理模型的模型参数进行迭代
优化调整的过程。具体地，所述第一数据方可以重复执行秘密分享第一乘积的步骤，得
到新的第一乘积的份额。所述第一数据方可以根据新的第一乘积的份额与合作方秘密分
享激励函数的取值，得到新的激励函数取值的份额。所述第一数据方可以重复执行步骤
S23，得到新的损失函数梯度的份额；可以重复执行步骤S25，得到新的海森矩阵的份额；
30 可以重复执行秘密分享第二乘积的步骤，得到新的第二乘积的份额。新的第二乘积为随

机正交矩阵和新的海森矩阵之间的乘积。

在新的第二乘积的条件数满足预设条件时，表明可以继续使用牛顿法确定模型参数。所述第一数据方可以重复执行步骤S27，所述第一数据方可以获得新的第一逆矩阵的份额。新的第一逆矩阵为新的海森矩阵的逆矩阵。所述第一数据方进而可以根据新的第一逆矩阵的份额、新的损失函数梯度的份额和新的第一模型参数的份额与合作方秘密分享第二模型参数，得到第二模型参数的份额。

在新的第二乘积的条件数不满足预设条件时，表明需要使用梯度下降法代替牛顿法确定模型参数。所述第一数据方可以根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

10 本实施例的模型参数确定方法，第一数据方可以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，得到新的第一模型参数的份额。

本说明书还提供模型参数确定方法的另一个实施例。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第一模型参数的份额。请参阅图6。该实施例可以包括以下步骤。

15 步骤 S31：根据第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到激励函数取值的份额，所述第一乘积为特征数据和第一模型参数的乘积。

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。具体地，所述第二数据方可以根据第一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；可以根据第一乘积的份额和激励函数对应的混淆电路与合作方通信，得到激励函数取值的份额。具体过程可以参见前面步骤 S11 的相关描述，在此不再赘述。

步骤 S33：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。

25 在一些实施例中，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。具体过程可以参见前面步骤 S13 的相关描述，在此不再赘述。

步骤 S35：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。

30 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 S15 的相关描述，在此不再赘述。

步骤 S37：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。

在一些实施例中，所述第二数据方可以根据随机正交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正交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正交矩阵的份额相乘，得到第一逆矩阵的份额。具体过程可以参见前面步骤 S17 的相关描述，在此不再赘述。

或者，在另一些实施例中，所述第二数据方可以根据随机正交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正交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正交矩阵的份额相乘，得到第一逆矩阵的份额。具体过程可以参见前面步骤 S17 的相关描述，在此不再赘述。

步骤 S39：根据第一模型参数的份额、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第一模型参数，得到新的第一模型参数的份额。

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第一模型参数的份额与第三乘积的份额相减，得到新的第一模型参数的份额。具体过程可以参见前面步骤 S19 的相关描述，在此不再赘述。

在一些实施例中，所述第二数据方可以根据随机正交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正交矩阵和海森矩阵之间的乘积。

如此在步骤 S37 中，所述第二数据方可以在第二乘积的条件数满足预设条件时，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。其中，第二乘积的条件数可以由第二数据方和/或合作方来计算。第二乘积的条件数等于海森矩阵的条件数。

第二乘积的条件数满足所述预设条件，表明第二乘积的病态程度较小，可以使用牛

顿法确定模型参数。

第二乘积的条件数不满足所述预设条件，表明第二乘积的病态程度较大，无法使用牛顿法确定模型参数，因而可以使用梯度下降法代替牛顿法确定模型参数。所述第二数据方可以根据第一模型参数的份额、损失函数梯度的份额和预设步长，计算新的第一模型参数的份额。所述第二数据方具体可以将损失函数梯度的份额与预设步长相乘，得到第四乘积；可以将第一模型参数的份额与第四乘积相减，得到新的第一模型参数的份额。

在本实施例的一些实施方式中，还可以包括对数据处理模型的模型参数进行迭代优化调整的过程。具体地，所述第二数据方可以重复执行秘密分享第一乘积的步骤，得到新的第一乘积的份额；可以重复执行步骤S31，得到新的激励函数取值的份额；可以重复执行步骤S33，得到新的损失函数梯度的份额；可以重复执行步骤S35，得到新的海森矩阵的份额；可以重复执行秘密分享第二乘积的步骤，得到新的第二乘积的份额。新的第二乘积为随机正交矩阵和新的海森矩阵之间的乘积。

在新的第二乘积的条件数满足预设条件时，表明可以继续使用牛顿法确定模型参数。所述第二数据方可以重复执行步骤S37，得到新的第一逆矩阵的份额。新的第一逆矩阵为新的海森矩阵的逆矩阵。所述第二数据方进而可以根据新的第一逆矩阵的份额、新的损失函数梯度的份额和新的第一模型参数的份额与合作方秘密分享第二模型参数，得到第二模型参数的份额。

在新的第二乘积的条件数不满足预设条件时，表明需要使用梯度下降法代替牛顿法确定模型参数。所述第二数据方可以根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

在本实施例的另一些实施方式中，还可以包括对数据处理模型的模型参数进行迭代优化调整的过程。具体地，所述第二数据方可以重复执行秘密分享第一乘积的步骤，得到新的第一乘积的份额。所述第二数据方可以根据新的第一乘积的份额与合作方秘密分享激励函数的取值，得到新的激励函数取值的份额。所述第二数据方可以重复执行步骤S33，得到新的损失函数梯度的份额；可以重复执行步骤S35，得到新的海森矩阵的份额；可以重复执行秘密分享第二乘积的步骤，得到新的第二乘积的份额。新的第二乘积为随机正交矩阵和新的海森矩阵之间的乘积。

在新的第二乘积的条件数满足预设条件时，表明可以继续使用牛顿法确定模型参数。所述第二数据方可以重复执行步骤S37，得到新的第一逆矩阵的份额。新的第一逆矩阵为新的海森矩阵的逆矩阵。所述第二数据方进而可以根据新的第一逆矩阵的份额、新的损

失函数梯度的份额和新的第一模型参数的份额与合作方秘密分享第二模型参数，得到第二模型参数的份额。

在新的第二乘积的条件数不满足预设条件时，表明需要使用梯度下降法代替牛顿法确定模型参数。所述第二数据方可以根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

本实施例的模型参数确定方法，第二数据方可以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，得到新的第一模型参数的份额。

下面将结合图7和图8，详细描述本说明书实施例中的模型参数确定装置。

本说明书还提供模型参数确定装置的一个实施例。请参阅图7。该实施例可以应用于第一数据方，可以包括以下单元。

激励函数取值份额获取单元 41，用于根据第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到激励函数取值的份额，所述第一乘积为特征数据和第一模型参数的乘积；

损失函数梯度份额获取单元 43，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损失函数的梯度，得到损失函数梯度的份额；

海森矩阵份额获取单元 45，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；

第一逆矩阵份额获取单元 47，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；

模型参数份额获取单元 49，用于根据第一模型参数的份额、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第一模型参数，得到新的第一模型参数的份额。

本说明书还提供模型参数确定装置的另一个实施例。请参阅图8。该实施例可以应用于第二数据方，可以包括以下单元。

激励函数取值份额获取单元 51，用于根据第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到激励函数取值的份额，所述第一乘积为特征数据和第一模型参数的乘积；

损失函数梯度份额获取单元 53，用于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；

海森矩阵份额获取单元 55，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；

第一逆矩阵份额获取单元 57，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；

模型参数份额获取单元 59，用于根据第一模型参数的份额、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第一模型参数，得到新的第一模型参数的份额。

请参阅图2，本说明书还提供模型参数确定系统的另一个实施例。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。

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，所述第三方可以生成随机正交矩阵，可以将所述随机正交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正交矩阵中各个随机数的第一份额形成的矩阵作为所述随机正交矩阵的第一份额，将所述随机正交矩阵中各个随机数的第二份额形成的矩阵作为所述随机正交矩阵的第二份额；可以向所述第一数据方发送所述随机正交矩阵的第一份额，可以向所述第二数据方发送所述随机正交矩阵的第二份额。其中，所述随机正交矩阵的第一份额和所述随机正交矩阵的第二份额的和等于所述随机正交矩阵。另外，一方面所述随机正交矩阵可以由随机数构成的随机数矩阵；另一方面所述随机正交矩阵还可以为正交矩阵。一个方阵与一个正交矩阵相乘后可以得到一个新的矩阵，该新的矩阵与该方阵具有相同的条件数。这样便于第一数据方和第二数据方在不泄漏自身持有的海森矩阵的份额的条件下，协作计算得到海森矩阵的条件数；进而便于根据条件数来度量海森矩阵的病态程度。具体过程详见后面的实施例。

鉴于所述第一数据方和所述第二数据方在基于混淆电路进行计算的过程中涉及到不经意传输，所述第三方还可以生成第一OT随机数和第二OT随机数；可以向所述第一数据方发送所述第一OT随机数；可以向所述第二数据方发送所述第二OT随机数。OT随机数可以为在不经意传输过程中所使用到的随机数。

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持有特征数据的数据方，所述第二数据方可以为持有标签的数据方。例如，所述第一数据方可以持有完整的特征数据，所述第二数据方可以持有特征数据的标签。或者，所述

的另一部分数据项和特征数据的标签。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持有用户的储蓄金额，所述第二数据方可以持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0和1。值得说明的是，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。

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第一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第一模型参数的第一份额，可以将所述第二数据方获得份额作为第一模型参数的第二份额。第一模型参数的第一份额和第一模型参数的第二份额的和等于第一模型参数。

所述第一数据方可以接收随机正交矩阵的第一份额和第一OT随机数。所述第二数据方可以接收随机正交矩阵的第二份额和第二OT随机数。如此所述第一数据方可以基于第一模型参数的第一份额、特征数据、随机正交矩阵的第一份额和第一OT随机数，所述第二数据方可以基于第一模型参数的第二份额、标签、随机正交矩阵的第二份额和第二OT随机数，协作确定第二模型参数。例如，所述第一数据方和所述第二数据方可以采用秘密分享的方式，使用牛顿法协作确定新的第一模型参数；进而，可以采用秘密分享和混淆电路相结合的方式，使用梯度下降法协作确定第二模型参数。

基于上述模型参数确定系统实施例，下面将结合图9，详细描述本说明书模型参数确定方法的另一个实施例。该实施例可以包括以下步骤。

步骤S601：第一数据方根据特征数据和第一模型参数的第一份额，第二数据方根据第一模型参数的第二份额，秘密分享第一乘积。第一数据方获得第一乘积的第一份额，第二数据方获得第一乘积的第二份额。所述第一乘积为特征数据和第一模型参数的乘积。

步骤S603：第一数据方根据第一乘积的第一份额，第二数据方根据第一乘积的第二份额，秘密分享激励函数的取值。第一数据方获得激励函数取值的第一份额，第二数据方获得激励函数取值的第二份额。

步骤S605：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。第一数据方获得损失函数梯度的第一份额，第二数据方获得损失函数梯度的第二份额。

步骤S607：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。

步骤S609：第一数据方根据随机正交矩阵的第一份额和海森矩阵的第一份额，第二数据方根据随机正交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。第一数据方获得第二乘积的第一份额，第二数据方获得第二乘积的第二份额。所述第二乘积为随机正交矩阵和海森矩阵之间的乘积。

步骤S611：在第二乘积的条件数满足预设条件时，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。

步骤S613：第一数据方根据第一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，第二数据方根据第一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，秘密分享新的第一模型参数。第一数据方获得新的第一模型参数的第一份额，第二数据方获得新的第一模型参数的第二份额。

下面介绍在实施例中涉及的一些术语。

(一)、第一乘积、第二乘积、第三乘积、第四乘积和第五乘积。所述第一乘积可以为第一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正交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。所述第四乘积可以为损失函数梯度的第一份额与预设步长的乘积。所述第五乘积可以为损失函数梯度的第二份额与预设步长的乘积。

在一些场景示例中，所述第一乘积可以表示为 XW ；其中， W 表示第一模型参数，具体为第一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。

所述第二乘积可以表示为 HR ，其中， H 表示海森矩阵， R 表示随机正交矩阵。

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。

所述第四乘积可以表示为 $G \langle dW \rangle_0$ ，所述第五乘积可以表示为 $G \langle dW \rangle_1$ 。其中， G 表示预设步长， $\langle dW \rangle_0$ 表示损失函数梯度的第一份额， $\langle dW \rangle_1$ 表示损失函数梯度的第二份额， $\langle dW \rangle_0 + \langle dW \rangle_1 = dW$ 。

(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。

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 $(HR)^{-1}$ 。

5

在一些实施例中, 在步骤S601中, 所述第一数据方可以根据特征数据和第一模型参数的第一份额, 所述第二数据方可以根据第一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。

10

延续前面的场景示例, 第一模型参数的第一份额可以表示为 $\langle W \rangle_0$, 第一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 $\langle XW \rangle_1$ 。 $\langle XW \rangle_0 + \langle XW \rangle_1 = XW$ 。

15

在一些实施例中, 在步骤S603中, 所述第一数据方可以根据第一乘积的第一份额, 所述第二数据方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。

20

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。

25

在一些实施例中, 在步骤S605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

5 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。

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 $\langle dW \rangle_1$ 。

10 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。

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

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 $\langle X^T Y \rangle_1$ 。
 $\langle X^T Y \rangle_0 + \langle X^T Y \rangle_1 = X^T Y$ 。

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

20 $\langle dW \rangle_1$ 。

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

在一些实施例中, 在步骤S607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。

25 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。

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。如此所述所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。

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 $\langle a \rangle_1$, 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 。

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。

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, $\bullet$ 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,

$m \bullet n = (m_1 n_1, m_2 n_2, m_3 n_3)$ 。

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 $\langle r \rangle_1 = \langle a \rangle_1 - \langle [\langle a \rangle_0 \bullet \langle a \rangle_1] \rangle_1 - \langle a \rangle_1 \bullet \langle a \rangle_1$ 。

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

$\langle r \rangle_0$ 、 $\langle r \rangle_1$ 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 。

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 $\langle H \rangle_1$ 。

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。

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 $X^T RNN_1$ 。
 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 $\langle X^T RNN_1 \rangle_1$ 。
 $\langle X^T RNN_1 \rangle_0 + \langle X^T RNN_1 \rangle_1 = X^T RNN_1$ 。

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 $\langle [\langle X^T RNN_1 \rangle_1 X] \rangle_1$ 。

$$\langle [\langle X^T RNN_1 \rangle_1 X] \rangle_0 + \langle [\langle X^T RNN_1 \rangle_1 X] \rangle_1 = \langle X^T RNN_1 \rangle_1 X。$$

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 $\langle H \rangle_1$ 。

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

在一些实施例中，第三方可以向第一数据方下发随机正交矩阵的第一份额；可以向第二数据方下发随机正交矩阵的第二份额。随机正交矩阵的第一份额和随机正交矩阵的第二份额的和等于随机正交矩阵。所述第一数据方可以接收随机正交矩阵的第一份额，

所述第二数据方可以接收随机正交矩阵的第二份额。如此在步骤S609中, 所述第一数据方可以根据随机正交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正交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

5 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。

延续前面的场景示例, 随机正交矩阵的第一份额可以表示为 $\langle R \rangle_0$, 随机正交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

10 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 $\langle HR \rangle_1$ 。

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。

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

15 $\langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_1$ 。 $\langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_0 + \langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_1 = \langle H \rangle_0 \langle R \rangle_1$ 。

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 $\langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_1$ 。 $\langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_0 + \langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_1 = \langle H \rangle_1 \langle R \rangle_0$ 。

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

20 $\langle H \rangle_1 \langle R \rangle_1 + \langle [\langle H \rangle_0 \langle R \rangle_1] \rangle_1 + \langle [\langle H \rangle_1 \langle R \rangle_0] \rangle_1$ 作为第二乘积的第二份额 $\langle HR \rangle_1$ 。

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

25 在一些实施例中, 所述预设条件可以包括: 条件数小于或等于预设阈值。所述预设

阈值可以为经验值，或者，还可以采用其它方式（例如机器学习的方式）获得。

所述第一数据方和所述第二数据方均可以持有所述预设条件。进而，所述第一数据方和所述第二数据方可以分别判断第二乘积的条件数是否满足所述预设条件。在一些实施方式中，可以由第一数据方计算第二乘积的条件数。具体地，所述第二数据方可以向
5 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持有的第二乘积的第一份额相加，得到第二乘积；可以计算第二乘积的条件数；可以判断第二乘积的条件数是否满足所述预设条件；可以向所述第二数据方发送第二乘积的条件数。所述第二数据方可以接收第二乘积的条件数；可以判断第二乘积的条件数是否满足所述预设条件。在另一些实施方式中，还可以由第
10 二数据方计算第二乘积的条件数。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持有的第二乘积的第二份额相加，得到第二乘积；可以计算第二乘积的条件数；可以判断第二乘积的条件数是否满足所述预设条件；可以向所述第一数据方发送第二乘积的条件数。所述第一数据方可以接收第二乘积的条件数；可以判断第二乘
15 积的条件数是否满足所述预设条件。

或者，可以仅由第一数据方持有所述预设条件，进而仅由第一数据方判断第二乘积的条件数是否满足所述预设条件。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持有的第二乘积的第一份额相加，得到第二乘积；可以计算第二乘积
20 的条件数；可以判断第二乘积的条件数是否满足所述预设条件；可以向所述第二数据方发送判断结果信息。所述第二数据方可以接收判断结果信息。

又或者，可以仅由第二数据方持有所述预设条件，进而仅由第二数据方判断第二乘积的条件数是否满足所述预设条件。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
25 积的第一份额与自身持有的第二乘积的第二份额相加，得到第二乘积；可以计算第二乘积的条件数；可以判断第二乘积的条件数是否满足所述预设条件；可以向所述第一数据方发送判断结果信息。所述第一数据方可以接收判断结果信息。

如前面所述，一个方阵与一个正交矩阵相乘后可以得到一个新的矩阵，该新的矩阵与该方阵具有相同的条件数。鉴于海森矩阵为方阵，因而第二乘积的条件数等于海森矩
30 阵的条件数。这样便实现了第一数据方和第二数据方在不泄漏自身持有的海森矩阵的份

额的条件，协作计算得到海森矩阵的条件数。

在一些实施例中，第二乘积的条件数满足所述预设条件，表明第二乘积的病态程度较小，即表明海森矩阵的病态程度较小，因而可以使用牛顿法确定模型参数。如此在步骤S611中，所述第一数据方可以根据海森矩阵的第一份额，所述第二数据方可以根据海森矩阵的第二份额，秘密分享第一逆矩阵。所述第一数据方可以获得第一逆矩阵的第一份额，所述第二数据方可以获得第一逆矩阵的第二份额。

在一些实施方式中，可以由所述第二数据方对所述第二乘积进行求逆。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。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。

所述第一数据方可以将随机正交矩阵的第一份额与第二逆矩阵相乘，得到第一逆矩阵的第一份额。所述第二数据方可以将随机正交矩阵的第二份额与第二逆矩阵相乘，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。

延续前面的场景示例，这里由第二数据方对第二乘积 HR 进行求逆。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 $(HR)^{-1}$ 。

所述第一数据方可以将第二逆矩阵 $(HR)^{-1}$ 与随机正交矩阵的第一份额 $\langle R \rangle_0$ 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 $(HR)^{-1}$ 与随机正交矩阵的第二份额 $\langle R \rangle_1$ 相乘，得到第一逆矩阵 H^{-1} 的第一份额 $\langle H^{-1} \rangle_1$ 。

$$H^{-1} = \langle H^{-1} \rangle_0 + \langle H^{-1} \rangle_1 = \langle R \rangle_0 (HR)^{-1} + \langle R \rangle_1 (HR)^{-1} = R \times (HR)^{-1}。$$

- 5 在一些实施例中，在步骤S613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
- 10 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。

所述第一数据方可以将第一模型参数的第一份额与第三乘积的第一份额相减，得到新的第一模型参数的第一份额。所述第二数据方可以将第一模型参数的第二份额与第三乘积的第二份额相减，得到新的第一模型参数的第二份额。

- 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
- 15 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 $\langle H^{-1} \times dW \rangle_1$ 。

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。

- 20 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 $\langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_1$ 。

$$\langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_0 + \langle [\langle H^{-1} \rangle_0 \langle dW \rangle_1] \rangle_1 = \langle H^{-1} \rangle_0 \langle dW \rangle_1。$$

- 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
- 25 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 $\langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_1$ 。

$$\langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_0 + \langle [\langle H^{-1} \rangle_1 \langle dW \rangle_0] \rangle_1 = \langle H^{-1} \rangle_1 \langle dW \rangle_0。$$

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 $\langle H^{-1} \times dW \rangle_1$ 。

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

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
 $\langle W' \rangle_1 = \langle W \rangle_1 - \langle H^{-1} \times dW \rangle_1$ ， $\langle W' \rangle_0$ 表示新的第一模型参数的第一份额， $\langle W' \rangle_1$ 表
 示新的第一模型参数的第二份额， W' 表示新的第一模型参数。

$$\begin{aligned}
 W' &= \langle W' \rangle_0 + \langle W' \rangle_1 = \langle W \rangle_0 - \langle H^{-1} \times dW \rangle_0 + \langle W \rangle_1 - \langle H^{-1} \times dW \rangle_1 = W - H^{-1} \times dW \\
 10 \quad &。
 \end{aligned}$$

在一些实施例中，第二乘积的条件数不满足所述预设条件，表明第二乘积的病态程
 度较大，即表明海森矩阵的病态程度较大，无法使用牛顿法确定模型参数，因而可以使
 用梯度下降法代替牛顿法确定模型参数。具体地，所述第一数据方可以根据第一模型参
 15 数的第一份额、损失函数梯度的第一份额和预设步长，计算新的第一模型参数的第一份
 额。所述第二数据方可以根据第一模型参数的第二份额、损失函数梯度的第二份额和预
 设步长，计算新的第一模型参数的第二份额。

所述预设步长可以用于控制梯度下降法的迭代速度。所述预设步长可以为任意适当
 正实数。例如，当预设步长过大时，迭代速度会过快，导致有可能无法获得最优模型参
 20 数。当预设步长过小时，导致迭代速度会过慢，导致花费的时间较长。所述预设步长具
 体可以为经验值；或者，也可以采用机器学习的方式得到。当然，所述预设步长还可以
 采用其它方式得到。所述第一数据方和所述第二数据方均可以持有所述预设步长。

所述第一数据方可以将损失函数梯度的第一份额与预设步长相乘，得到第四乘积；
 可以将第一模型参数的第一份额与第四乘积相减，得到新的第一模型参数的第一份额。
 25 所述第二数据方可以将损失函数梯度的第二份额与预设步长相乘，得到第五乘积；可以
 将第一模型参数的第二份额与第五乘积相减，得到新的第一模型参数的第二份额。新的

第一模型参数的第一份额和新的第一模型参数的第二份额的和等于新的第一模型参数。

延续前面的场景示例，所述第一数据方可以将损失函数梯度的第一份额 $\langle dW \rangle_0$ （具体为向量）与预设步长 G 相乘（具体为向量的数乘），得到第四乘积 $G \langle dW \rangle_0$ ；可以将第一模型参数的第一份额 $\langle W \rangle_0$ 与第四乘积 $G \langle dW \rangle_0$ 相减，得到新的第一模型参数的

5 第一份额 $\langle W' \rangle_0 = \langle W \rangle_0 - G \langle dW \rangle_0$ 。

所述第二数据方可以将损失函数梯度的第二份额 $\langle dW \rangle_1$ （具体为向量）与预设步长 G 相乘（具体为向量的数乘），得到第五乘积 $G \langle dW \rangle_1$ ；可以将第一模型参数的第二份额 $\langle W \rangle_1$ 与第五乘积 $G \langle dW \rangle_1$ 相减，得到新的第一模型参数的第二份额

$\langle W' \rangle_1 = \langle W \rangle_1 - G \langle dW \rangle_1$ 。其中， $\langle W' \rangle_0 + \langle W' \rangle_1 = W'$ ， W' 表示新的第一模型参数。

10 这样通过条件数和预设条件，本实施例可以避免在使用牛顿法确定模型参数的过程中由于出现病态矩阵所导致的不收敛问题。

步骤S601-步骤S613的模型参数确定方法，通过秘密分享的方式实现。另外，牛顿法有着较快的收敛速度。步骤S601-步骤S613的模型参数确定方法，由于使用了牛顿法，不仅可以保护合作建模各方（第一数据方和第二数据方）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。

15 在一些实施例中，还可以包括对数据处理模型的模型参数进行迭代优化调整的过程。

可以重复执行步骤S601，所述第一数据方可以获得新的第一乘积的第一份额，所述第二数据方可以获得新的第一乘积的第二份额。新的第一乘积为特征数据和新的第一模型参数的乘积。所述第一数据方可以根据新的第一乘积的第一份额，所述第二数据方可以根据新的第一乘积的第二份额，基于激励函数对应的混淆电路进行通信。第一数据方可以获得新的激励函数取值的第一份额，第二数据方可以获得新的激励函数取值的第二份额。可以重复执行步骤S605，所述第一数据方可以获得新的损失函数梯度的第一份额，所述第二数据方可以获得新的损失函数梯度的第二份额。可以重复执行步骤S607，所述

20 第一数据方可以获得新的海森矩阵的第一份额，所述第二数据方可以获得新的海森矩阵的第二份额。可以重复执行步骤S609，所述第一数据方可以获得新的第二乘积的第一份额，所述第二数据方可以获得新的第二乘积的第二份额。新的第二乘积为随机正交矩阵和新的海森矩阵之间的乘积。

25

在新的第二乘积的条件数满足预设条件时，表明在该轮迭代过程中可以继续使用牛

顿法确定模型参数。可以重复执行步骤S611。所述第一数据方可以获得新的第一逆矩阵的第一份额，所述第二数据方可以获得新的第一逆矩阵的第二份额。新的第一逆矩阵为新的海森矩阵的逆矩阵。所述第一数据方可以根据新的第一模型参数的第一份额、新的第一逆矩阵的第一份额和新的损失函数梯度的第一份额，所述第二数据方根据新的第一模型参数的第二份额、新的第一逆矩阵的第二份额和新的损失函数梯度的第二份额，秘密分享第二模型参数。所述第一数据方可以获得第二模型参数的第一份额，所述第二数据方可以获得第二模型参数的第二份额。第二模型参数的第一份额和第二模型参数的第二份额的和等于第二模型参数。这样可以通过秘密分享和混淆电路相结合的方式实现迭代过程。通过秘密分享和混淆电路相结合的方式，不仅可以避免越界的问题，还可以降低数据处理模型训练过程的复杂程度。另外在迭代的过程中，由于使用了牛顿法，不仅可以保护合作建模各方（第一数据方和第二数据方）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。

在新的第二乘积的条件数不满足预设条件时，表明在该轮迭代过程中无法继续使用牛顿法确定模型参数，因而可以使用梯度下降法代替牛顿法确定模型参数。所述第一数据方可以根据新的第一模型参数的第一份额、新的损失函数梯度的第一份额和预设步长，计算第二模型参数的第一份额。所述第二数据方可以根据新的第一模型参数的第二份额、新的损失函数梯度的第二份额和预设步长，计算第二模型参数的第二份额。第二模型参数的第一份额和第二模型参数的第二份额的和等于第二模型参数。这样可以通过秘密分享和混淆电路相结合的方式实现迭代过程。通过秘密分享和混淆电路相结合的方式，不仅可以避免越界的问题，还可以降低数据处理模型训练过程的复杂程度。另外在迭代的过程中，使用了梯度下降法。

以下介绍所述第一数据方根据新的第一乘积的第一份额，所述第二数据方根据新的第一乘积的第二份额，基于激励函数对应的混淆电路进行通信的过程。

可以根据所述激励函数构建相应的逻辑电路。所述逻辑电路可以由所述第一数据方构建；或者，也可以由所述第二数据方构建；又或者，还可以由其它设备（例如可信任的第三方）构建。所述逻辑电路可以由至少一个运算门构成，所述运算门可以包括与门、或门、异或门等等。所述逻辑电路可以包括至少两个输入线和至少一个输出线，通过对所述逻辑电路的输入线和/或输出线进行加密便可以得到混淆电路。所述混淆电路可以包括所述逻辑电路中各个运算门的混淆真值表。值得说明的是，这里可以直接根据激励函数构建逻辑电路；或者，也可以对激励函数进行各种适当的变形，可以根据变形后的激

励函数构建逻辑电路；又或者，还可以以所述激励函数为基础生成其它函数，可以根据其它函数构建逻辑电路。相应地，这里激励函数与混淆电路相对应可以理解为：混淆电路是根据激励函数的逻辑电路生成的，或者，混淆电路是根据变形后的激励函数的混淆电路生成的，又或者，混淆电路是根据其它函数的逻辑电路生成的。

5 所述第一数据方和所述第二数据方均可以持有激励函数对应的混淆电路。在一些实施方式中，所述混淆电路可以由所述第一数据方生成。所述第一数据方可以将生成的混淆电路发送给所述第二数据方。所述第二数据方可以接收所述混淆电路。在另一些实施方式中，所述混淆电路也可以由所述第二数据方生成。所述第二数据方可以将生成的混淆电路发送给所述第一数据方。所述第一数据方可以接收所述混淆电路。

10 如此，第一数据方可以根据新的第一乘积的第一份额，第二数据方可以根据新的第一乘积的第二份额，基于激励函数对应的混淆电路进行通信。所述第一数据方和所述第二数据方可以分别获得新的激励函数取值的一份份额。为了便于描述，可以将所述第一数据方获得的份额作为新的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新的激励函数取值的第二份额。新的激励函数取值的第一份额和新的激励函数取值的第二份额的和等于新的激励函数的取值。

15 请参阅图4。以下介绍第一数据方和第二数据方基于混淆电路进行计算的一个场景示例。

20 可以根据激励函数 $f(x_1, x_2)$ 构建函数 $y = f_1(x_1, x_2, x_3) = f(x_1, x_2) - x_3$ 。其中， x_1 用于表示新的第一乘积的第一份额， x_2 用于表示新的第一乘积的第二份额， x_3 用于表示新的激励函数取值的一份份额（以下称为新的激励函数取值的第二份额）， $f_1(x_1, x_2, x_3)$ 的取值用于表示新的激励函数取值的另一份份额（以下称为新的激励函数取值的第一份额）。

25 可以构建与函数 $f_1(x_1, x_2, x_3) = f(x_1, x_2) - x_3$ 相对应的逻辑电路，通过对该逻辑电路的输入线和/或输出线进行加密便可以得到混淆电路。所述第一数据方和所述第二数据方均可以持有该混淆电路。值得说明的是，函数 $y = f_1(x_1, x_2, x_3) = f(x_1, x_2) - x_3$ 及其对应的逻辑电路可以由所述第一数据方构建；或者，也可以由所述第二数据方构建；又或者，还可以由其它设备（例如可信任的第三方）构建。

 所述第二数据方可以生成新的激励函数取值的一份份额作为第二份额。如此所述第一数据方可以以新的第一乘积的第一份额作为该混淆电路的输入，所述第二数据方可以以新的第一乘积的第二份额以及新的激励函数取值的第二份额作为该混淆电路的输入，

进行通信。所述第一数据方可以基于该混淆电路计算得到新的激励函数取值的另一份份额作为第一份额。具体的计算过程可以参见前面有关介绍混淆电路的场景示例，在此不再详述。

在一些实施方式中，为了降低混淆电路的复杂程度，还可以使用分段线性函数拟合所述激励函数。这样便可以根据所述分段线性函数构建相应的逻辑电路，通过对该逻辑电路的输入线和/或输出线进行加密便可以得到混淆电路。所述第一数据方和所述第二数据方均可以持有该混淆电路。例如，所述激励函数可以为Sigmoid函数，所述分段线性函

$$\text{数可以为 } y = f(x) = \begin{cases} 1 & x \geq \frac{0.5}{k} \\ kx + 0.5 & -\frac{0.5}{k} < x < \frac{0.5}{k} \\ 0 & x \leq -\frac{0.5}{k} \end{cases}, \quad k \text{ 表示分段线性函数的系数。}$$

第一数据方可以根据新的第一乘积的第一份额，第二数据方可以根据新的第一乘积的第二份额，基于该混淆电路进行通信。所述第一数据方和所述第二数据方分别获得分段线性函数取值的一份份额。为了便于描述，可以将所述第一数据方获得的份额作为分段线性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分段线性函数取值的第二份额。分段线性函数取值的第一份额和分段线性函数取值的第二份额的和等于分段线性函数的取值。所述第一数据方可以将分段线性函数取值的第一份额作为新的激励函数取值的第一份额。所述第二数据方可以将分段线性函数取值的第二份额作为新的激励函数取值的第二份额。

本实施例的模型参数确定方法，第一数据方和第二数据方可以在不泄漏自身所持有的数据的前提下，协作确定数据处理模型的模型参数。

上文中结合图9，详细描述本说明书模型参数确定方法的另一个实施例。上文中第一数据方执行的方法步骤，可以单独实现为第一数据方侧的模型参数确定方法；第二数据方执行的方法步骤，可以单独实现为第二数据方侧的模型参数确定方法。下面将结合图10和图11，详细描述本说明书实施例中第一数据方侧的模型参数确定方法、以及第二数据方侧的模型参数确定方法。

本说明书还提供模型参数确定方法的另一个实施例。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第一模型参数的份额。请参阅图10。该实施例可以包括以下步骤。

步骤S701: 根据特征数据和第一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, 所述第一乘积为特征数据和第一模型参数的乘积。

5 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。

步骤S703: 根据第一乘积的份额与合作方秘密分享激励函数的取值, 得到激励函数取值的份额。

10 在一些实施例中, 所述第一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, 所述多项式用于拟合所述激励函数。

步骤S705: 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和海森矩阵, 分别得到损失函数梯度的份额和海森矩阵的份额。

15 步骤S707: 根据随机正交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正交矩阵和海森矩阵之间的乘积。

步骤S709: 在第二乘积的条件数满足预设条件时, 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。

20 在一些实施例中, 所述预设条件可以包括: 条件数小于或等于预设阈值。第二乘积的条件数可以由第一数据方和/或合作方来计算。第二乘积的条件数等于海森矩阵的条件数。

在一些实施例中, 第二乘积的条件数满足所述预设条件, 表明第二乘积的病态程度较小, 可以使用牛顿法确定模型参数。如此所述第一数据方可以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。

25 步骤S711: 根据第一逆矩阵的份额、损失函数梯度的份额和第一模型参数的份额与合作方秘密分享新的第一模型参数, 得到新的第一模型参数的份额。

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和损失函数梯度之间的乘积。所述第一数据方可以将第一模型参数的份额与第三乘积的份额相减, 得到新的第一模型参数的份额。

30 在一些实施例中, 第二乘积的条件数不满足所述预设条件, 表明第二乘积的病态程

度较大，无法使用牛顿法确定模型参数，因而可以使用梯度下降法代替牛顿法确定模型参数。所述第一数据方可以根据第一模型参数的份额、损失函数梯度的份额和预设步长，计算新的第一模型参数的份额。所述第一数据方具体可以将损失函数梯度的份额与预设步长相乘，得到第四乘积；可以将第一模型参数的份额与第四乘积相减，得到新的第一模型参数的份额。

在一些实施例中，还可以包括对数据处理模型的模型参数进行迭代优化调整的过程。

所述第一数据方可以重复执行步骤S701，得到新的第一乘积的份额。所述第一数据方可以根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到新的激励函数取值的份额。所述第一数据方可以重复执行步骤S705，得到新的损失函数梯度的份额和新的海森矩阵的份额；可以重复执行步骤S707，得到新的第二乘积的份额。新的第二乘积为随机正交矩阵和新的海森矩阵之间的乘积。

在新的第二乘积的条件数满足预设条件时，表明可以继续使用牛顿法确定模型参数。所述第一数据方可以重复执行步骤S709，得到新的第一逆矩阵的份额。新的第一逆矩阵为新的海森矩阵的逆矩阵。所述第一数据方进而可以根据新的第一逆矩阵的份额、新的损失函数梯度的份额和新的第一模型参数的份额与合作方秘密分享第二模型参数，得到第二模型参数的份额。

在新的第二乘积的条件数不满足预设条件时，表明需要使用梯度下降法代替牛顿法确定模型参数。所述第一数据方可以根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

本实施例的模型参数确定方法，第一数据方可以在不泄漏自身所持有的数据的前提下，与合作方协作确定数据处理模型的模型参数。

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第一模型参数的份额。请参阅图11。该实施例可以包括以下步骤。

步骤S801：根据第一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，所述第一乘积为特征数据和第一模型参数的乘积。

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。

步骤S803：根据第一乘积的份额与合作方秘密分享激励函数的取值，得到激励函数取值的份额。

在一些实施例中，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，所述多项式用于拟合所述激励函数。

步骤S805：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；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。

步骤S807：根据随机正交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正交矩阵和海森矩阵之间的乘积。

步骤S809：在第二乘积的条件数满足预设条件时，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。

在一些实施例中，所述预设条件可以包括：条件数小于或等于预设阈值。第二乘积的条件数可以由第二数据方和/或合作方来计算。第二乘积的条件数等于海森矩阵的条件数。

在一些实施例中，第二乘积的条件数满足所述预设条件，表明第二乘积的病态程度较小，可以使用牛顿法确定模型参数。如此所述第二数据方可以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。

步骤S811：根据第一逆矩阵的份额、损失函数梯度的份额和第一模型参数的份额与合作方秘密分享新的第一模型参数，得到新的第一模型参数的份额。

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第一模型参数的份额与第三乘积的份额相减，得到新的第一模型参数的份额。

在一些实施例中，第二乘积的条件数不满足所述预设条件，表明第二乘积的病态程度较大，无法使用牛顿法确定模型参数，因而可以使用梯度下降法代替牛顿法确定模型参数。所述第二数据方可以根据第一模型参数的份额、损失函数梯度的份额和预设步长，计算新的第一模型参数的份额。所述第二数据方具体可以将损失函数梯度的份额与预设步长相乘，得到第四乘积；可以将第一模型参数的份额与第四乘积相减，得到新的第一模型参数的份额。

在一些实施例中，还可以包括对数据处理模型的模型参数进行迭代优化调整的过程。所述第二数据方可以重复执行步骤S801，得到新的第一乘积的份额。所述第二数据

方可以根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到新的激励函数取值的份额。所述第二数据方可以重复执行步骤S805，得到新的损失函数梯度的份额和新的海森矩阵的份额；可以重复执行步骤S807，得到新的第二乘积的份额。新的第二乘积为随机正交矩阵和新的海森矩阵之间的乘积。

5 在新的第二乘积的条件数满足预设条件时，表明可以继续使用牛顿法确定模型参数。所述第二数据方可以重复执行步骤S809，得到新的第一逆矩阵的份额。新的第一逆矩阵为新的海森矩阵的逆矩阵。所述第二数据方进而可以根据新的第一逆矩阵的份额、新的损失函数梯度的份额和新的第一模型参数的份额与合作方秘密分享第二模型参数，得到第二模型参数的份额。

10 在新的第二乘积的条件数不满足预设条件时，表明需要使用梯度下降法代替牛顿法确定模型参数。所述第二数据方可以根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

本实施例的模型参数确定方法，第二数据方可以在不泄漏自身所持有的数据的前提下，与合作方协作确定数据处理模型的模型参数。

15

下面将结合图12和图13，详细描述本说明书实施例中的模型参数确定装置。

本说明书还提供模型参数确定装置的一个实施例。请参阅图12。该实施例可以应用于第一数据方，可以包括以下单元。

20 第一秘密分享单元 901，用于根据特征数据和第一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，所述第一乘积为特征数据和第一模型参数的乘积；

第二秘密分享单元 903，用于根据第一乘积的份额与合作方秘密分享激励函数的取值，得到激励函数取值的份额；

第三秘密分享单元 905，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损失函数的梯度和海森矩阵，分别得到损失函数梯度的份额和海森矩阵的份额；

25 第四秘密分享单元 907，用于根据随机正交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正交矩阵和海森矩阵之间的乘积；

30 第五秘密分享单元 909，用于在第二乘积的条件数满足预设条件时，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；

第六秘密分享单元911, 用于根据第一逆矩阵的份额、损失函数梯度的份额和第一模型参数的份额与合作方秘密分享新的第一模型参数, 得到新的第一模型参数的份额;

混淆电路单元 913, 用于重复执行所述秘密分享第一乘积的步骤; 根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信, 得到新的激励函数取值的份额;

5 重复执行所述秘密分享损失函数的梯度和海森矩阵的步骤、以及所述秘密分享第二乘积的步骤;

计算单元915, 用于在新的第二乘积的条件数不满足所述预设条件时, 根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长, 计算第二模型参数的份额。

本说明书还提供模型参数确定装置的另一个实施例。请参阅图13。该实施例可以应
10 用于第二数据方, 可以包括以下单元。

第一秘密分享单元 1001, 用于根据第一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, 所述第一乘积为特征数据和第一模型参数的乘积;

第二秘密分享单元 1003, 用于根据第一乘积的份额与合作方秘密分享激励函数的取值, 得到激励函数取值的份额;

15 第三秘密分享单元 1005, 用于根据激励函数取值的份额与合作方秘密分享损失函数的梯度和海森矩阵, 分别得到损失函数梯度的份额和海森矩阵的份额;

第四秘密分享单元 1007, 用于根据随机正交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正交矩阵和海森矩阵之间的乘积;

20 第五秘密分享单元 1009, 用于在第二乘积的条件数满足预设条件时, 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;

第六秘密分享单元1011, 用于根据第一逆矩阵的份额、损失函数梯度的份额和第一模型参数的份额与合作方秘密分享新的第一模型参数, 得到新的第一模型参数的份额;

25 混淆电路单元 1013, 用于重复执行所述秘密分享第一乘积的步骤; 根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信, 得到新的激励函数取值的份额; 重复执行所述秘密分享损失函数的梯度的步骤、所述秘密分享海森矩阵的步骤、以及所述秘密分享第二乘积的步骤;

30 计算单元1015, 用于在新的第二乘积的条件数不满足所述预设条件时, 根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长, 计算第二模型参数的份额。

下面介绍本说明书电子设备的一个实施例。图14是该实施例中一种电子设备的硬件结构示意图。如图14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14所示的硬件结构仅
5 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14所示更多或者更少的组件单元；或者，具有与图14所示不同的配置。

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
10 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5所对应实施例的程序指令或模块；和/或，本说明书图6所对应实施例的程序指令或模块；和/或，本说明书图10所对应实施例的程序指令或模块；和/或，本说明书图11所对应实施例的程序指令或模块。

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
15 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。

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、
20 局域网、移动通信网等网络进行数据传输。

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
25 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。

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，
30 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

5 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、RHDH（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。

10

15

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。

20

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。

25

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

30

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。

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。

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：

根据第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到激励函数取值的份额，所述第一乘积为特征数据和第一模型参数的乘积；

5 根据特征数据和激励函数取值的份额与合作方分别秘密分享损失函数的梯度和海森矩阵，得到损失函数梯度的份额和海森矩阵的份额；

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；

10 根据第一模型参数的份额、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第一模型参数，得到新的第一模型参数的份额。

2. 如权利要求 1 所述的方法，所述根据第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，包括：

15 根据第一乘积的份额和分段线性函数对应的混淆电路与合作方进行通信，得到分段线性函数取值的份额作为激励函数取值的份额，所述分段线性函数用于拟合所述激励函数。

3. 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，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；

20 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。

4. 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，包括：

25 根据随机正交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，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，将第二逆矩阵与随机正交矩阵的份额相乘，得到第一逆矩阵的份额；其中，所述第二乘积为随机正交矩阵和海森矩阵之间的乘积，所述第二逆矩阵为所述第二乘积的逆矩阵；或者，

30 根据随机正交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，接收合作方发来的第二乘积的份额，将通过秘密分享所得到的第二乘积的份额与通过接收所得到的第二乘积的份额相加，得到第二乘积，将第二乘积的逆矩阵作为第二逆矩阵，将第二逆矩阵与随机正交矩阵的份额相乘，得到第一逆矩阵的份额；其

中, 所述第二乘积为随机正交矩阵和海森矩阵之间的乘积。

5. 如权利要求 1 所述的方法, 所述根据第一模型参数的份额、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第一模型参数, 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
5 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;

将第一模型参数的份额与第三乘积的份额相减, 得到新的第一模型参数的份额。

6. 如权利要求 1 所述的方法, 还包括:

根据特征数据和第一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。

10 7. 如权利要求 6 所述的方法, 还包括:

根据随机正交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正交矩阵和海森矩阵之间的乘积;

相应地, 所述根据海森矩阵的份额与合作方秘密分享第一逆矩阵, 包括:

在第二乘积的条件数满足预设条件时, 根据海森矩阵的份额与合作方秘密分享第一
15 逆矩阵, 得到第一逆矩阵的份额。

8. 如权利要求 7 所述的方法, 还包括:

在第二乘积的条件数不满足预设条件时, 根据第一模型参数的份额、损失函数梯度
的份额和预设步长, 计算新的第一模型参数的份额。

9. 如权利要求 7 或 8 所述的方法, 还包括:

20 接收合作方发来的第二乘积的份额, 将自身的第二乘积的份额与接收的第二乘积的
份额相加, 得到第二乘积, 计算第二乘积的条件数; 或者,

向合作方发送第二乘积的份额, 以便合作方计算第二乘积的条件数。

10. 如权利要求 7 所述的方法, 还包括:

迭代执行所述秘密分享第一乘积的步骤, 得到新的第一乘积的份额, 迭代执行所述
25 与合作方进行通信的步骤, 得到新的激励函数取值的份额, 迭代执行所述秘密分享损失
函数的梯度和海森矩阵的步骤, 得到新的损失函数梯度的份额和新的海森矩阵的份额,
迭代执行所述秘密分享第二乘积的步骤, 得到新的第二乘积的份额;

在新的第二乘积的条件数满足预设条件时, 迭代执行所述秘密分享第一逆矩阵的步
骤, 得到新的第一逆矩阵的份额, 根据新的第一逆矩阵的份额、新的损失函数梯度的份
30 额和新的第一模型参数的份额与合作方秘密分享第二模型参数, 得到第二模型参数的份

额。

11. 如权利要求 7 所述的方法, 还包括:

迭代执行所述秘密分享第一乘积的步骤, 得到新的第一乘积的份额, 迭代执行所述与合作方进行通信的步骤, 得到新的激励函数取值的份额, 迭代执行所述秘密分享损失函数的梯度和海森矩阵的步骤, 得到新的损失函数梯度的份额和新的海森矩阵的份额, 迭代执行所述秘密分享第二乘积的步骤, 得到新的第二乘积的份额;

在新的第二乘积的条件数不满足所述预设条件时, 根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长, 计算第二模型参数的份额。

12. 如权利要求 7 所述的方法, 还包括:

10 迭代执行所述秘密分享第一乘积的步骤, 得到新的第一乘积的份额, 根据新的第一乘积的份额与合作方秘密分享激励函数的取值, 得到新的激励函数取值的份额, 迭代执行所述秘密分享损失函数的梯度和海森矩阵的步骤, 得到新的损失函数梯度的份额和新的海森矩阵的份额, 迭代执行所述秘密分享第二乘积的步骤, 得到新的第二乘积的份额;

15 在新的第二乘积的条件数不满足所述预设条件时, 根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长, 计算第二模型参数的份额。

13. 如权利要求 12 所述的方法, 所述根据新的第一乘积的份额与合作方秘密分享激励函数的取值, 包括:

根据新的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新的激励函数取值的份额, 所述多项式用于拟合所述激励函数。

20 14. 一种模型参数确定方法, 应用于第二数据方, 包括:

根据第一乘积的份额和激励函数对应的混淆电路与合作方进行通信, 得到激励函数取值的份额, 所述第一乘积为特征数据和第一模型参数的乘积;

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;

25 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额, 所述第一逆矩阵为海森矩阵的逆矩阵;

根据第一模型参数的份额、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第一模型参数, 得到新的第一模型参数的份额。

30 15. 如权利要求 14 所述的方法, 所述根据第一乘积的份额和激励函数对应的混淆电

路与合作方进行通信, 包括:

根据第一乘积的份额和分段线性函数对应的混淆电路与合作方进行通信, 得到分段线性函数取值的份额作为激励函数取值的份额, 所述分段线性函数用于拟合所述激励函数。

- 5 16. 如权利要求 14 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, 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。

- 10 17. 如权利要求 14 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, 包括:

根据随机正交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, 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, 将第二逆矩阵与随机正交矩阵的份额相乘, 得到第一逆矩阵的份额; 其中, 所述第二乘积为随机正交矩阵和海森矩阵之间的乘积, 所述第二逆矩阵为所述第二乘积的逆矩阵; 或者,

- 15 根据随机正交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, 接收合作方发来的第二乘积的份额, 将通过秘密分享所得到的第二乘积的份额与通过接收所得到的第二乘积的份额相加, 得到第二乘积, 将第二乘积的逆矩阵作为第二逆矩阵, 将第二逆矩阵与随机正交矩阵的份额相乘, 得到第一逆矩阵的份额; 其中, 所述第二乘积为随机正交矩阵和海森矩阵之间的乘积。

- 20 18. 如权利要求 14 所述的方法, 所述根据第一模型参数的份额、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第一模型参数, 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;

将第一模型参数的份额与第三乘积的份额相减, 得到新的第一模型参数的份额。

- 25 19. 如权利要求 14 所述的方法, 还包括:

根据第一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。

20. 如权利要求 19 所述的方法, 还包括:

根据随机正交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正交矩阵和海森矩阵之间的乘积;

- 30 相应地, 所述根据海森矩阵的份额与合作方秘密分享第一逆矩阵, 包括:

在第二乘积的条件数满足预设条件时,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。

21. 如权利要求 20 所述的方法,还包括:

在第二乘积的条件数不满足预设条件时,根据第一模型参数的份额、损失函数梯度的份额和预设步长,计算新的第一模型参数的份额。

22. 如权利要求 20 或 21 所述的方法,还包括:

接收合作方发来的第二乘积的份额,将自身的第二乘积的份额与接收的第二乘积的份额相加,得到第二乘积,计算第二乘积的条件数;或者,

向合作方发送第二乘积的份额,以便合作方计算第二乘积的条件数。

23. 如权利要求 20 所述的方法,还包括:

迭代执行所述秘密分享第一乘积的步骤,得到新的第一乘积的份额,迭代执行所述与合作方进行通信的步骤,得到新的激励函数取值的份额,迭代执行所述秘密分享损失函数的梯度的步骤,得到新的损失函数梯度的份额,迭代执行所述秘密分享海森矩阵的步骤,得到新的海森矩阵的份额,迭代执行所述秘密分享第二乘积的步骤,得到新的第二乘积的份额;

在新的第二乘积的条件数满足预设条件时,迭代执行所述秘密分享第一逆矩阵的步骤,得到新的第一逆矩阵的份额,根据新的第一逆矩阵的份额、新的损失函数梯度的份额和新的第一模型参数的份额与合作方秘密分享第二模型参数,得到第二模型参数的份额。

24. 如权利要求 20 所述的方法,还包括:

迭代执行所述秘密分享第一乘积的步骤,得到新的第一乘积的份额,迭代执行所述与合作方进行通信的步骤,得到新的激励函数取值的份额,迭代执行所述秘密分享损失函数的梯度的步骤,得到新的损失函数梯度的份额,迭代执行所述秘密分享海森矩阵的步骤,得到新的海森矩阵的份额,迭代执行所述秘密分享第二乘积的步骤,得到新的第二乘积的份额;

在新的第二乘积的条件数不满足所述预设条件时,根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长,计算第二模型参数的份额。

25. 如权利要求 20 所述的方法,还包括:

迭代执行所述秘密分享第一乘积的步骤,得到新的第一乘积的份额,根据新的第一乘积的份额与合作方秘密分享激励函数的取值,得到新的激励函数取值的份额,迭代执

行所述秘密分享损失函数的梯度的步骤，得到新的损失函数梯度的份额，迭代执行所述秘密分享海森矩阵的步骤，得到新的海森矩阵的份额，迭代执行所述秘密分享第二乘积的步骤，得到新的第二乘积的份额；

- 在新的第二乘积的条件数不满足所述预设条件时，根据新的第一模型参数的份额、
5 新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

26. 如权利要求 25 所述的方法，所述根据新的第一乘积的份额与合作方秘密分享激励函数的取值，包括：

根据新的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新的激励函数取值的份额，所述多项式用于拟合所述激励函数。

- 10 27. 一种模型参数确定方法，应用于第一数据方，包括：

根据特征数据和第一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，所述第一乘积为特征数据和第一模型参数的乘积；

根据第一乘积的份额与合作方秘密分享激励函数的取值，得到激励函数取值的份额；

- 15 根据特征数据和激励函数取值的份额与合作方分别秘密分享损失函数的梯度和海森矩阵，得到损失函数梯度的份额和海森矩阵的份额；

根据随机正交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正交矩阵和海森矩阵之间的乘积；

- 20 在第二乘积的条件数满足预设条件时，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；

根据第一逆矩阵的份额、损失函数梯度的份额和第一模型参数的份额与合作方秘密分享新的第一模型参数，得到新的第一模型参数的份额；

- 25 迭代执行所述秘密分享第一乘积的步骤，得到新的第一乘积的份额，根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到新的激励函数取值的份额，迭代执行所述秘密分享损失函数的梯度和海森矩阵的步骤，得到新的损失函数梯度的份额和新的海森矩阵的份额，迭代执行所述秘密分享第二乘积的步骤，得到新的第二乘积的份额；

在新的第二乘积的条件数不满足所述预设条件时，根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

- 30 28. 如权利要求 27 所述的方法，所述根据第一乘积的份额与合作方秘密分享激励

函数的取值, 包括:

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, 所述多项式用于拟合所述激励函数。

29. 如权利要求 27 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, 包括:

向合作方发送第二乘积的份额, 接收合作方发来的第二乘积的逆矩阵作为第二逆矩阵, 将第二逆矩阵与随机正交矩阵的份额相乘, 得到第一逆矩阵的份额; 或者,

接收合作方发来的第二乘积的份额, 将自身的第二乘积的份额与接收的第二乘积的份额相加, 得到第二乘积, 将第二乘积的逆矩阵作为第二逆矩阵, 将第二逆矩阵与随机正交矩阵的份额相乘, 得到第一逆矩阵的份额。

30. 如权利要求 27 所述的方法, 所述根据第一逆矩阵的份额、损失函数梯度的份额和第一模型参数的份额与合作方秘密分享新的第一模型参数, 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;

15 将第一模型参数的份额与第三乘积的份额相减, 得到新的第一模型参数的份额。

31. 如权利要求 27 所述的方法, 所述根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信, 包括:

根据新的第一乘积的份额和分段线性函数对应的混淆电路与合作方进行通信, 得到分段线性函数取值的份额作为新的激励函数取值的份额, 所述分段线性函数用于拟合所述激励函数。

32. 如权利要求 27 所述的方法, 还包括:

接收合作方发来的第二乘积的份额, 将自身的第二乘积的份额与接收的第二乘积的份额相加, 得到第二乘积, 计算第二乘积的条件数; 或者,

向合作方发送第二乘积的份额, 以便合作方计算第二乘积的条件数。

25 33. 如权利要求 27 所述的方法, 还包括:

在第二乘积的条件数不满足预设条件时, 根据第一模型参数的份额、损失函数梯度的份额和预设步长, 计算新的第一模型参数的份额。

34. 一种模型参数确定方法, 应用于第二数据方, 包括:

根据第一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, 所述第一乘积为特征数据和第一模型参数的乘积;

根据第一乘积的份额与合作方秘密分享激励函数的取值，得到激励函数取值的份额；

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；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

5 额；

根据随机正交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正交矩阵和海森矩阵之间的乘积；

在第二乘积的条件数满足预设条件时，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；

10 根据第一逆矩阵的份额、损失函数梯度的份额和第一模型参数的份额与合作方秘密分享新的第一模型参数，得到新的第一模型参数的份额；

迭代执行所述秘密分享第一乘积的步骤，得到新的第一乘积的份额，根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到新的激励函数取值的份额；迭代执行所述秘密分享损失函数的梯度的步骤，得到新的损失函数梯度的份额，迭

15 代执行所述秘密分享海森矩阵的步骤，得到新的海森矩阵的份额，迭代执行所述秘密分享第二乘积的步骤，得到新的第二乘积的份额；

在新的第二乘积的条件数不满足所述预设条件时，根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

35. 如权利要求 34 所述的方法，所述根据第一乘积的份额与合作方秘密分享激励

20 函数的取值，包括：

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，所述多项式用于拟合所述激励函数。

36. 如权利要求 34 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，包括：

25 向合作方发送第二乘积的份额，接收合作方发来的第二乘积的逆矩阵作为第二逆矩阵，将第二逆矩阵与随机正交矩阵的份额相乘，得到第一逆矩阵的份额；或者，

接收合作方发来的第二乘积的份额，将自身的第二乘积的份额与接收的第二乘积的份额相加，得到第二乘积，将第二乘积的逆矩阵作为第二逆矩阵，将第二逆矩阵与随机正交矩阵的份额相乘，得到第一逆矩阵的份额。

30 37. 如权利要求 34 所述的方法，所述根据第一逆矩阵的份额、损失函数梯度的份

额和第一模型参数的份额与合作方秘密分享新的第一模型参数，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；

将第一模型参数的份额与第三乘积的份额相减，得到新的第一模型参数的份额。

- 5 38. 如权利要求 34 所述的方法，所述根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，包括：

根据新的第一乘积的份额和分段线性函数对应的混淆电路与合作方进行通信，得到分段线性函数取值的份额作为新的激励函数取值的份额，所述分段线性函数用于拟合所述激励函数。

- 10 39. 如权利要求 34 所述的方法，还包括：

接收合作方发来的第二乘积的份额，将自身的第二乘积的份额与接收的第二乘积的份额相加，得到第二乘积，计算第二乘积的条件数；或者，

向合作方发送第二乘积的份额，以便合作方计算第二乘积的条件数。

40. 如权利要求 34 所述的方法，还包括：

- 15 在第二乘积的条件数不满足预设条件时，根据第一模型参数的份额、损失函数梯度的份额和预设步长，计算新的第一模型参数的份额。

41. 一种模型参数确定装置，应用于第一数据方，包括：

激励函数取值份额获取单元，用于根据第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到激励函数取值的份额，所述第一乘积为特征数据和第一模型参数的乘积；

- 20 损失函数梯度份额获取单元，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损失函数的梯度，得到损失函数梯度的份额；

海森矩阵份额获取单元，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；

- 25 第一逆矩阵份额获取单元，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；

模型参数份额获取单元，用于根据第一模型参数的份额、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第一模型参数，得到新的第一模型参数的份额。

42. 一种模型参数确定装置，应用于第二数据方，包括：

- 30 激励函数取值份额获取单元，用于根据第一乘积的份额和激励函数对应的混淆电路

与合作方进行通信,得到激励函数取值的份额,所述第一乘积为特征数据和第一模型参数的乘积;

损失函数梯度份额获取单元,用于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;

5 海森矩阵份额获取单元,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;

第一逆矩阵份额获取单元,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;

模型参数份额获取单元,用于根据第一模型参数的份额、第一逆矩阵的份额和损失
10 函数梯度的份额与合作方秘密分享新的第一模型参数,得到新的第一模型参数的份额。

43. 一种模型参数确定装置,应用于第一数据方,包括:

第一秘密分享单元,用于根据特征数据和第一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,所述第一乘积为特征数据和第一模型参数的乘积;

第二秘密分享单元,用于根据第一乘积的份额与合作方秘密分享激励函数的取值,
15 得到激励函数取值的份额;

第三秘密分享单元,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损失函数的梯度和海森矩阵,分别得到损失函数梯度的份额和海森矩阵的份额;

第四秘密分享单元,用于根据随机正交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正交矩阵和海森矩阵之间的
20 乘积;

第五秘密分享单元,用于在第二乘积的条件数满足预设条件时,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;

第六秘密分享单元,用于根据第一逆矩阵的份额、损失函数梯度的份额和第一模型
25 参数的份额与合作方秘密分享新的第一模型参数,得到新的第一模型参数的份额;

迭代单元,用于迭代执行所述秘密分享第一乘积的步骤,得到新的第一乘积的份额,根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信,得到新的激励函数取值的份额,迭代执行所述秘密分享损失函数的梯度和海森矩阵的步骤,得到新的损失函数梯度的份额和新的海森矩阵的份额,迭代执行所述秘密分享第二乘积的步骤,
30 得到新的第二乘积的份额;在新的第二乘积的条件数不满足所述预设条件时,根据新的

第一模型参数的份额、新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

44. 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，用于根据第一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，所述第一乘积为特征数据和第一模型参数的乘积；

5 第二秘密分享单元，用于根据第一乘积的份额与合作方秘密分享激励函数的取值，得到激励函数取值的份额；

第三秘密分享单元，用于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；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；

10 第四秘密分享单元，用于根据随机正交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正交矩阵和海森矩阵之间的乘积；

第五秘密分享单元，用于在第二乘积的条件数满足预设条件时，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；

15 第六秘密分享单元，用于根据第一逆矩阵的份额、损失函数梯度的份额和第一模型参数的份额与合作方秘密分享新的第一模型参数，得到新的第一模型参数的份额；

迭代单元，用于迭代执行所述秘密分享第一乘积的步骤，得到新的第一乘积的份额，根据新的第一乘积的份额和激励函数对应的混淆电路与合作方进行通信，得到新的激励函数取值的份额；迭代执行所述秘密分享损失函数的梯度的步骤，得到新的损失函数梯度的份额，迭代执行所述秘密分享海森矩阵的步骤，得到新的海森矩阵的份额，迭代执行所述秘密分享第二乘积的步骤，得到新的第二乘积的份额；在新的第二乘积的条件数不满足所述预设条件时，根据新的第一模型参数的份额、新的损失函数梯度的份额和预设步长，计算第二模型参数的份额。

25 45. 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 1-40 中任一项所述的方法步骤。

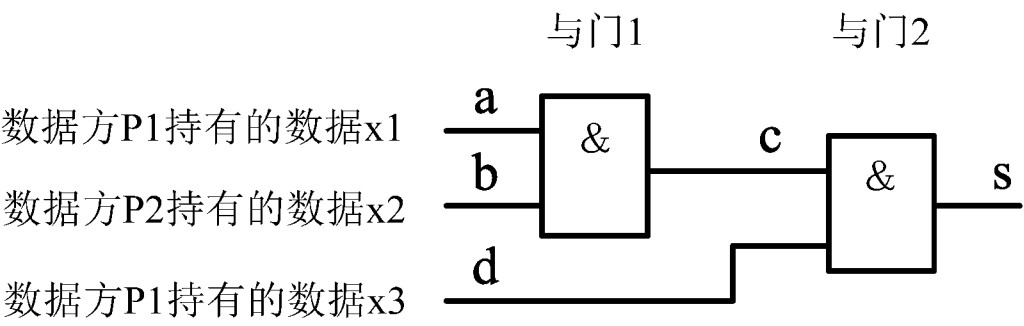


图 1

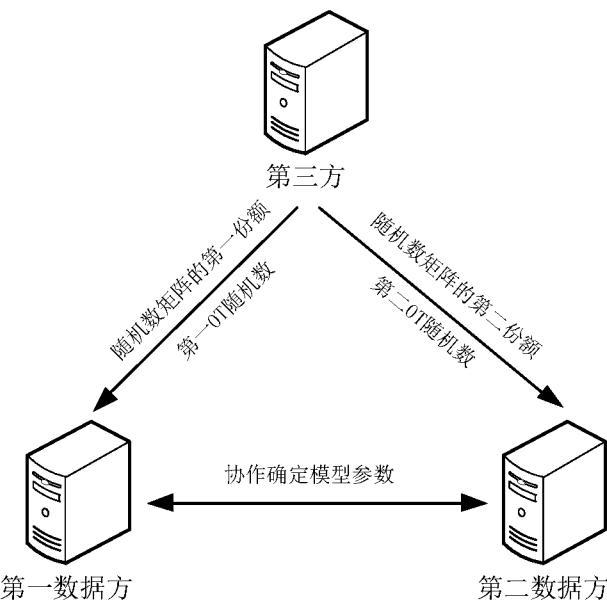


图 2

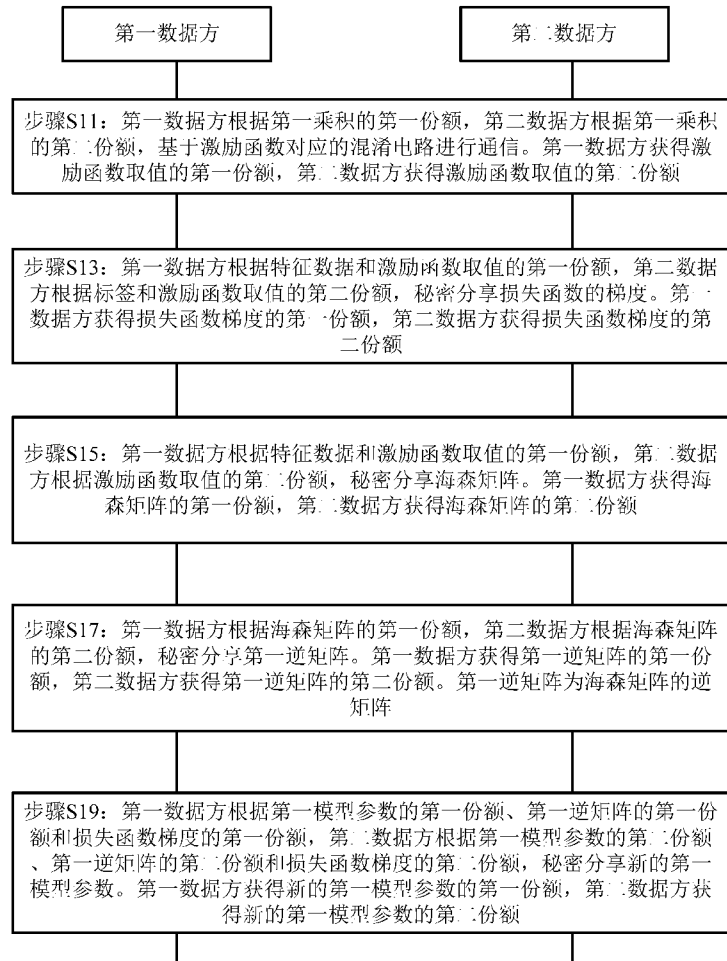


图 3

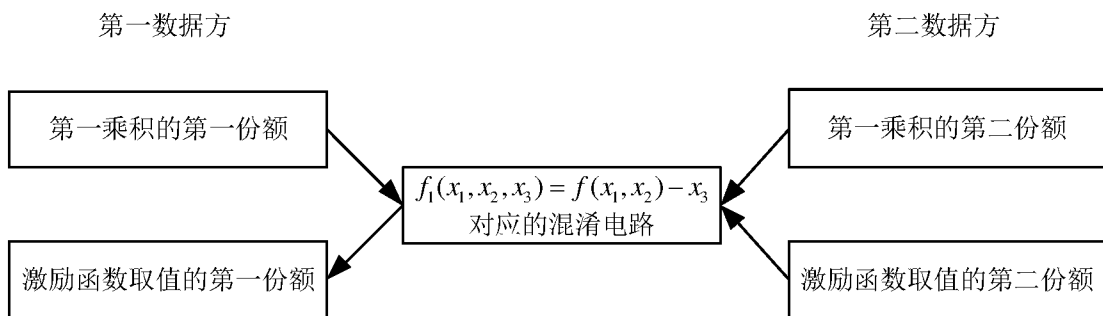


图 4

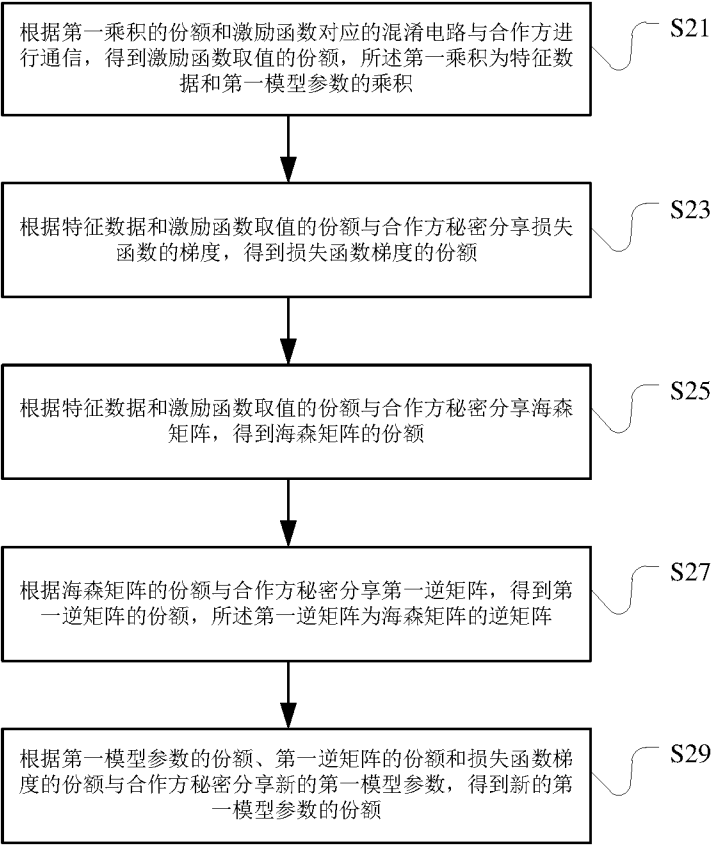


图 5

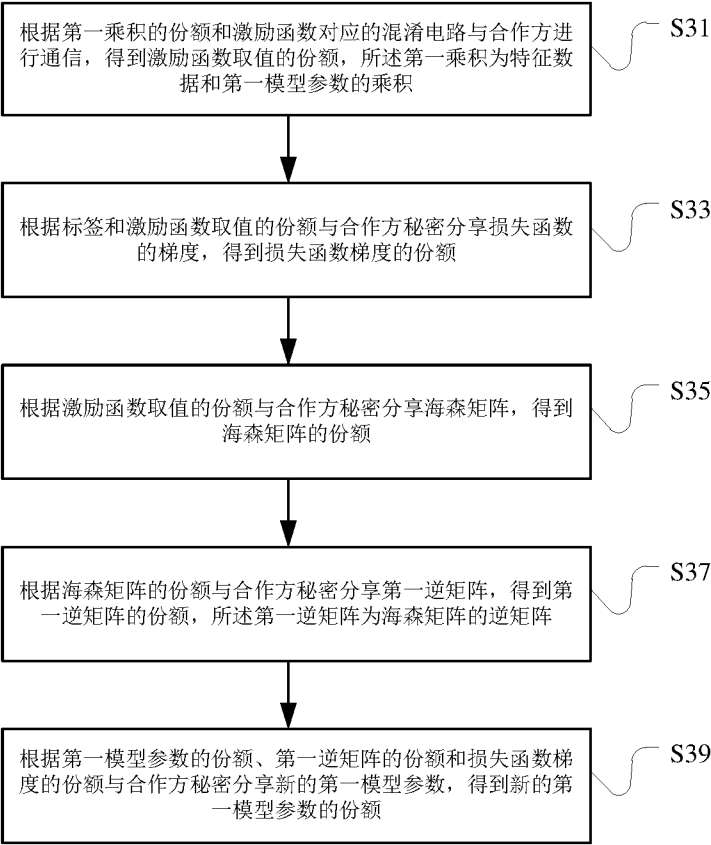


图 6

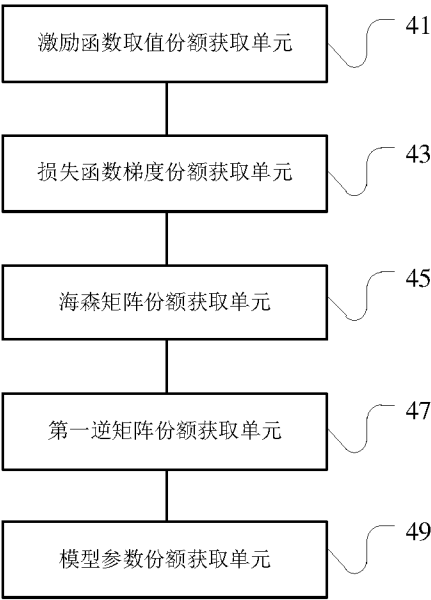


图 7

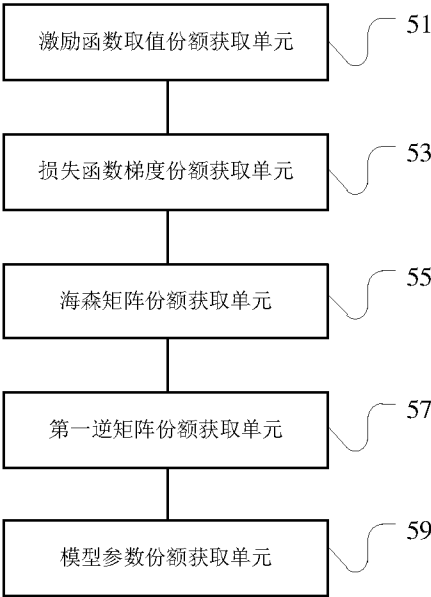


图 8

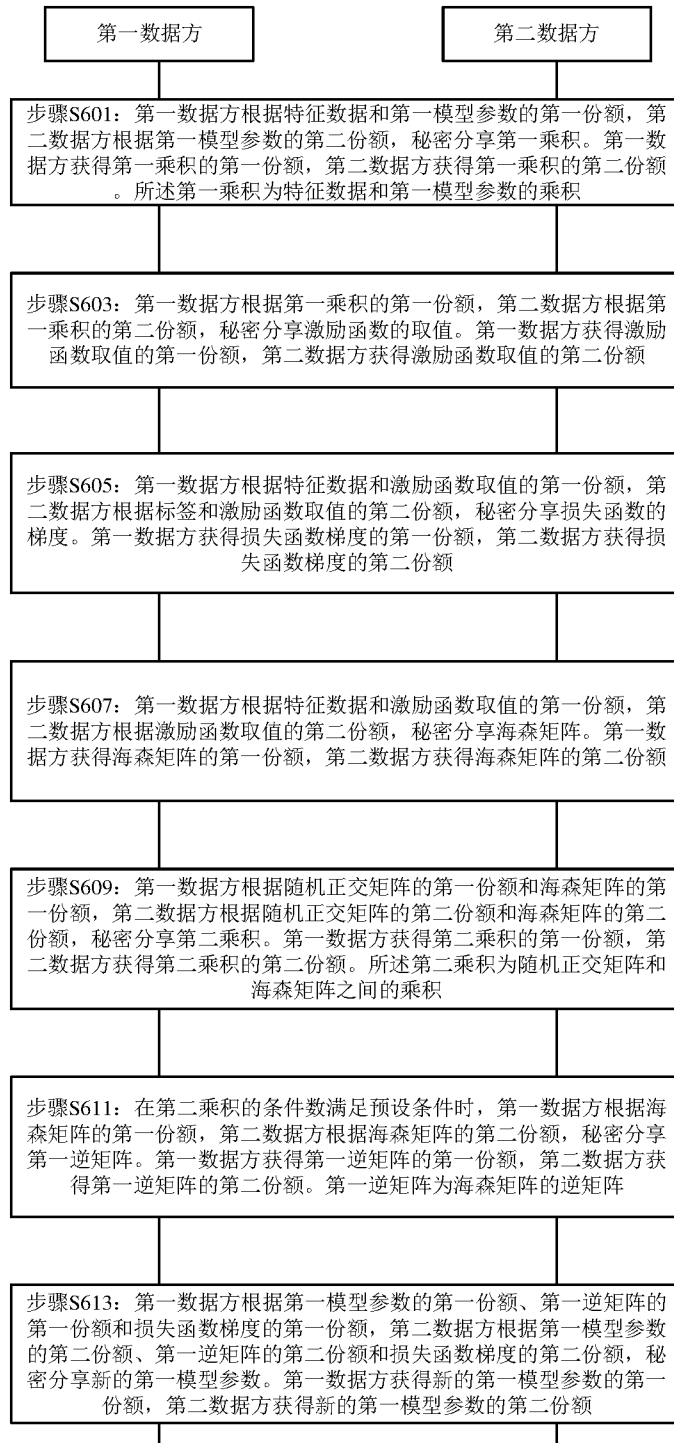


图 9

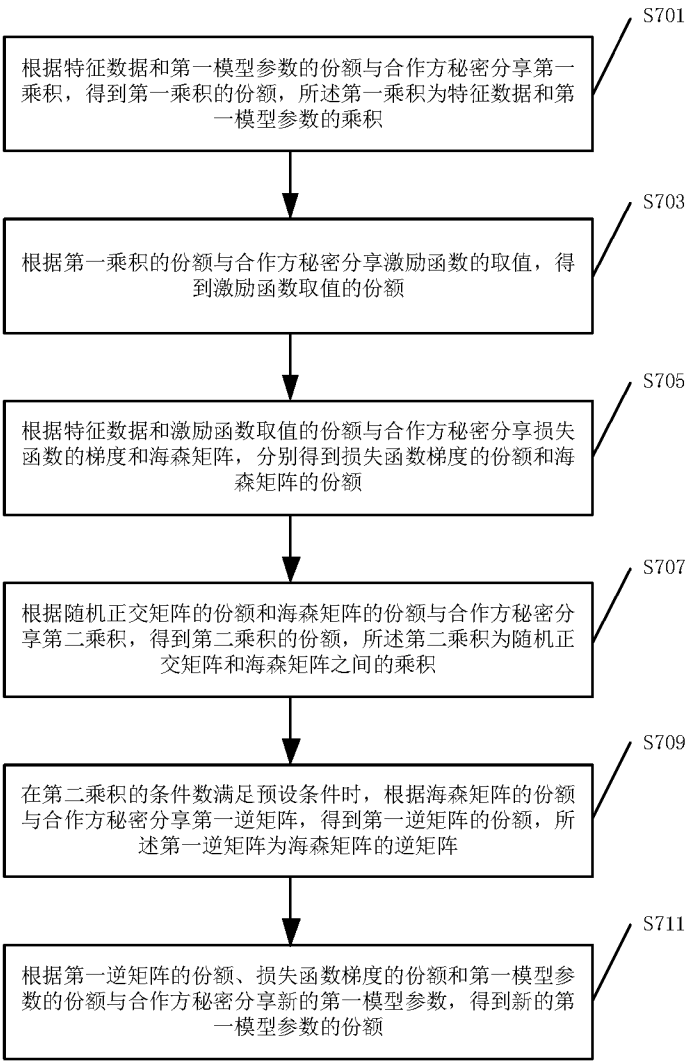


图 10

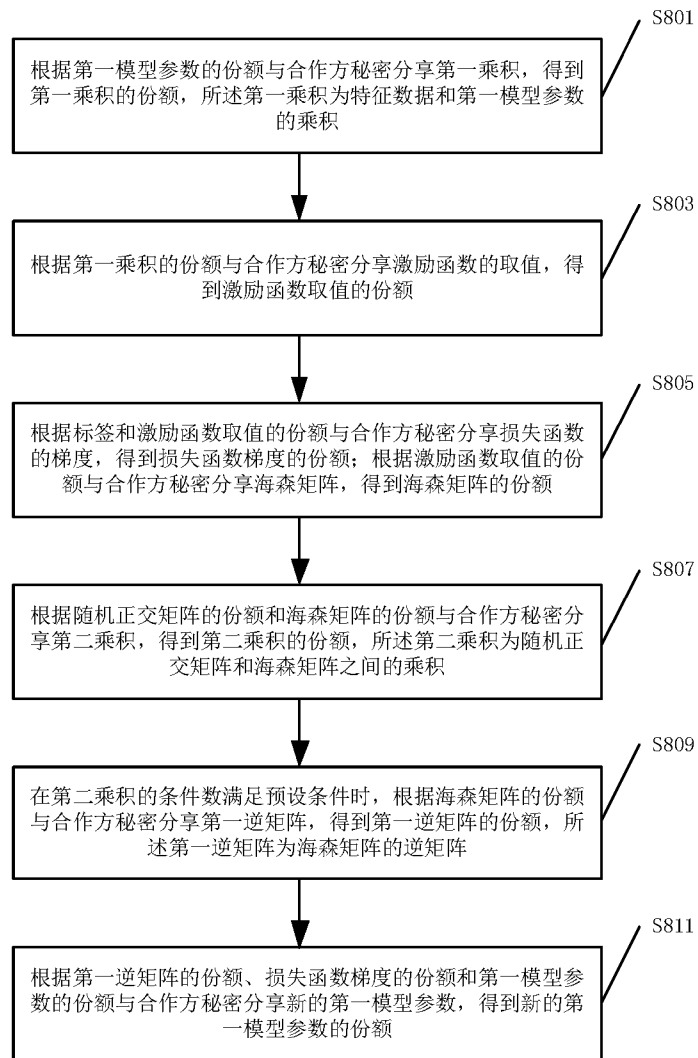


图 11

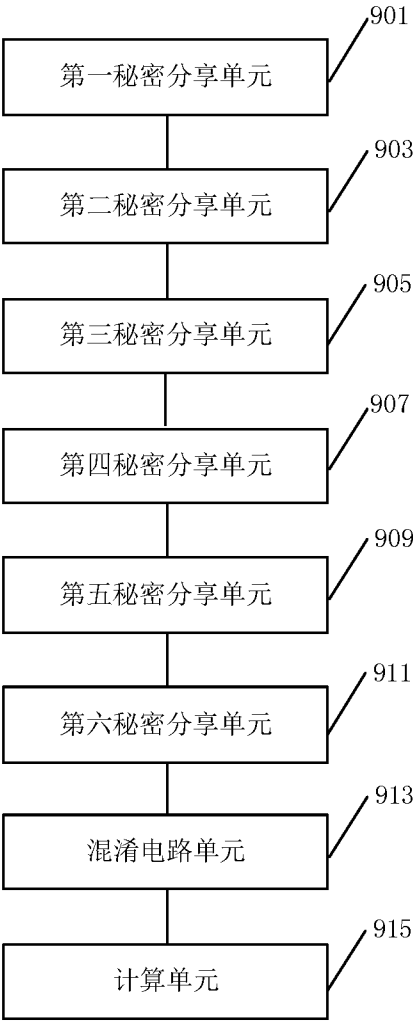


图 12

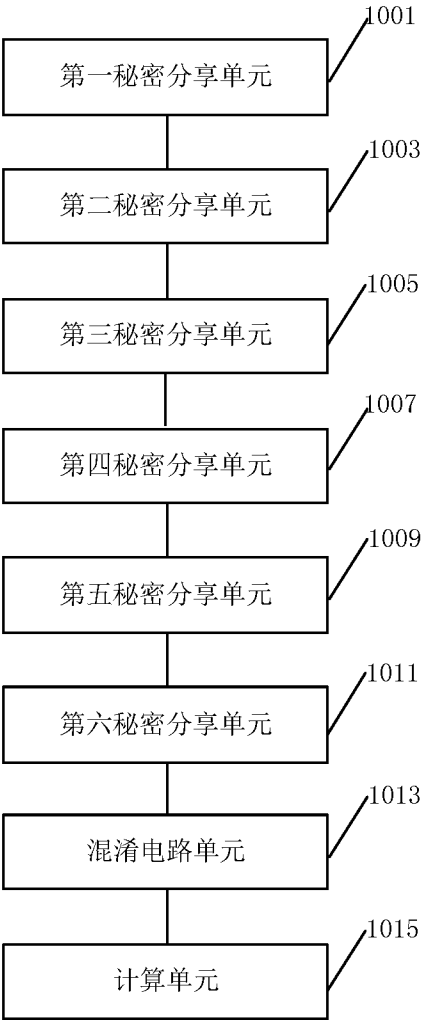


图 13

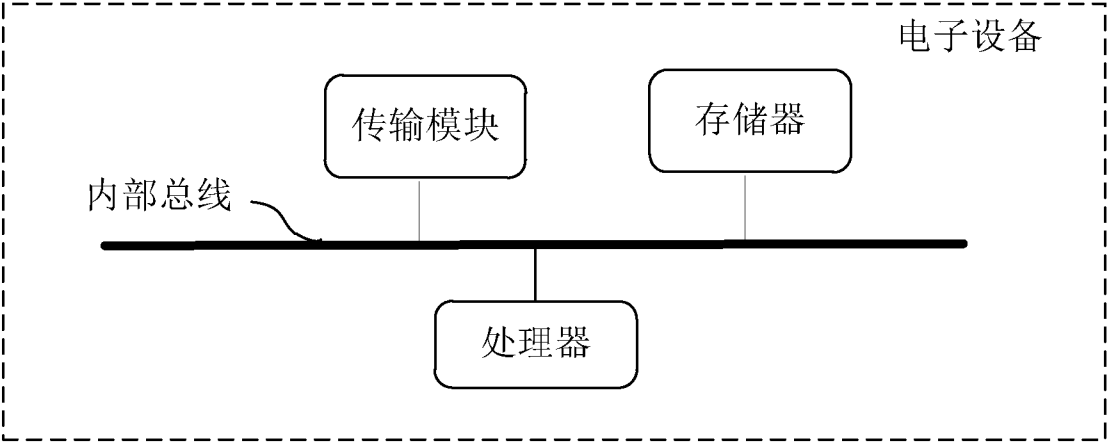


图 14

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/106254

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62(2013.01)i; G06N 3/02(2006.01)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; G06N

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: 模型, 参数, 多方安全计算, 激励函数, 激活函数, 混淆电路, 损失函数, 海森矩阵, 份额, 逆矩阵, 秘密, 密钥, 共享, model, parameter, multi-party, secure, computation, activation function, garbled circuit, loss function, hessian matrix, share, inverse matrix, secret, sharing

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110555315 A (ALIBABA GROUP HOLDING LIMITED) 10 December 2019 (2019-12-10) claims 1-20	1-45
PX	CN 110569228 A (ALIBABA GROUP HOLDING LIMITED) 13 December 2019 (2019-12-13) claims 1-26	1-45
PX	CN 110555525 A (ALIBABA GROUP HOLDING LIMITED) 10 December 2019 (2019-12-10) claims 1-24	1-45
PX	CN 110580409 A (ALIBABA GROUP HOLDING LIMITED) 17 December 2019 (2019-12-17) claims 1-18	1-45
PX	CN 110580410 A (ALIBABA GROUP HOLDING LIMITED) 17 December 2019 (2019-12-17) claims 1-26	1-45



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

19 October 2020

Date of mailing of the international search report

03 November 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/CN2020/106254**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110472439 A (ALIBABA GROUP HOLDING LIMITED) 19 November 2019 (2019-11-19) claims 1-24	1-45
A	CN 109274492 A (UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA) 25 January 2019 (2019-01-25) description, paragraphs 21-24	1-45
A	US 9449177 B1 (HRL LABORATORIES, LLC) 20 September 2016 (2016-09-20) entire document	1-45
A	US 2019149333 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 16 May 2019 (2019-05-16) entire document	1-45

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/106254

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	110555315	A	10 December 2019	None	
CN	110569228	A	13 December 2019	US 2020184081 A1	11 June 2020
CN	110555525	A	10 December 2019	None	
CN	110580409	A	17 December 2019	None	
CN	110580410	A	17 December 2019	None	
CN	110472439	A	19 November 2019	None	
CN	109274492	A	25 January 2019	None	
US	9449177	B1	20 September 2016	None	
US	2019149333	A1	16 May 2019	None	

国际检索报告

国际申请号

PCT/CN2020/106254

A. 主题的分类 G06F 21/62 (2013.01) i; G06N 3/02 (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) G06F; G06N 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, EPDOC: 模型, 参数, 多方安全计算, 激励函数, 激活函数, 混淆电路, 损失函数, 海森矩阵, 份额, 逆矩阵, 秘密, 密钥, 共享, model, parameter, multi-party, secure, computation, activation function, garbled circuit, loss function, hessian matrix, share, inverse matrix, secret, sharing																										
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>PX</td> <td>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</td> <td>1-45</td> </tr> <tr> <td>PX</td> <td>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</td> <td>1-45</td> </tr> <tr> <td>PX</td> <td>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</td> <td>1-45</td> </tr> <tr> <td>PX</td> <td>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</td> <td>1-45</td> </tr> <tr> <td>PX</td> <td>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</td> <td>1-45</td> </tr> <tr> <td>PX</td> <td>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</td> <td>1-45</td> </tr> <tr> <td>A</td> <td>CN 109274492 A (中国科学技术大学) 2019年 1月 25日 (2019 - 01 - 25) 说明书第21-24段</td> <td>1-45</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	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	1-45	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	1-45	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	1-45	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	1-45	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	1-45	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	1-45	A	CN 109274492 A (中国科学技术大学) 2019年 1月 25日 (2019 - 01 - 25) 说明书第21-24段	1-45
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																								
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	1-45																								
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	1-45																								
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	1-45																								
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	1-45																								
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	1-45																								
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	1-45																								
A	CN 109274492 A (中国科学技术大学) 2019年 1月 25日 (2019 - 01 - 25) 说明书第21-24段	1-45																								
☒ 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 10月 19日		国际检索报告邮寄日期 2020年 11月 3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		授权官员 杨春雨 电话号码 86-(10)-53961437																								

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	US 9449177 B1 (HRL LABORATORIES, LLC) 2016年 9月 20日 (2016 - 09 - 20) 全文	1-45
A	US 2019149333 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2019年 5月 16日 (2019 - 05 - 16) 全文	1-45

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/106254

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	110555315	A	2019年 12月 10日	无	
CN	110569228	A	2019年 12月 13日	US 2020184081 A1	2020年 6月 11日
CN	110555525	A	2019年 12月 10日	无	
CN	110580409	A	2019年 12月 17日	无	
CN	110580410	A	2019年 12月 17日	无	
CN	110472439	A	2019年 11月 19日	无	
CN	109274492	A	2019年 1月 25日	无	
US	9449177	B1	2016年 9月 20日	无	
US	2019149333	A1	2019年 5月 16日	无	