(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 11 月 26 日 (26.11.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/233137 A1

(51) 国际专利分类号:
G06F 17/15 (2006.01)

(21) 国际申请号: PCT/CN2020/070939

(22) 国际申请日: 2020 年 1 月 8 日 (08.01.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910434666.0 2019年5月23日 (23.05.2019) CN

(71) 申请人: 创新先进技术有限公司 (**ADVANCED NEW TECHNOLOGIES CO., LTD.**) [—/CN]; 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心, Grand Cayman KY1-9008 (KY)。

(72) 发明人: 周亚顺 (**ZHOU, Yashun**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 李漓春 (**LI, Lichun**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 殷山 (**YIN, Shan**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 王华忠 (**WANG, Huazhong**); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

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

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,

(54) **Title:** METHOD AND APPARATUS FOR DETERMINING VALUE OF LOSS FUNCTION, AND ELECTRONIC DEVICE

(54) 发明名称: 损失函数取值的确定方法、装置和电子设备

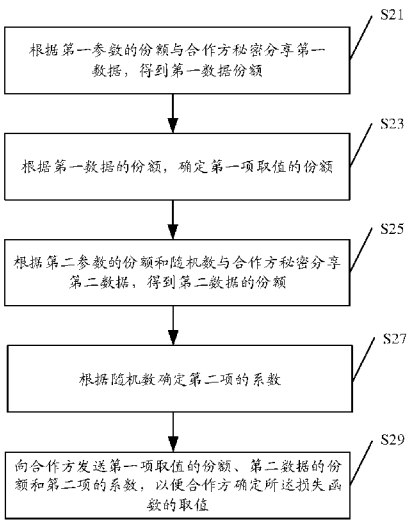


图 2

S21 Secretly share first data with a cooperating party according to a share of a first parameter to obtain a share of the first data
S23 Determine a share of a value of a first term according to the share of the first data
S25 Secretly share second data with the cooperating party according to a share of a second parameter and a random number to obtain a share of the second data
S27 Determine a coefficient of a second term according to the random number
S29 Send the share of the value of the first term, the share of the second data, and the coefficient of the second term to the cooperating party so that the cooperating party determines a value of a loss function

(57) **Abstract:** A method and apparatus for determining a value of a loss function, and an electronic device. The method is used for determining a value of a loss function. The loss function comprises a first term and a second term. The method comprises: secretly sharing first data with a cooperating party according to a share of a first parameter to obtain a share of the first data (S21); determining a share of a value of a first term according to the share of the first data (S23); secretly sharing second data with the cooperating party according to a share of a second parameter and a random number to obtain a share of the second data (S25); determining a coefficient of a second term according to the random number (S27), the coefficient of the second term and the second data being used for jointly determining a value of the second term; and sending the share of the value of the first term, the share of the second data, and the coefficient of the second term to the cooperating party so that the cooperating party determines a value of a loss function (S29).

WO 2020/233137 A1

[见续页]

BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

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

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：一种损失函数取值的确定方法、装置和电子设备。所述方法用于确定损失函数的取值。所述损失函数包括第一项和第二项。所述方法包括：根据第一参数的份额与合作方秘密分享第一数据，得到第一数据的份额（S21）；根据第一数据的份额，确定第一项取值的份额（S23）；根据第二参数的份额和随机数与合作方秘密分享第二数据，得到第二数据的份额（S25）；根据随机数确定第二项的系数（S27），第二项的系数和第二数据用于共同确定第二项的取值；向合作方发送第一项取值的份额、第二数据的份额和第二项的系数，以便合作方确定所述损失函数的取值（S29）。

损失函数取值的确定方法、装置和电子设备

技术领域

[01]本说明书实施例涉及计算机技术领域，特别涉及一种损失函数取值的确定方法、装置和电子设备。

背景技术

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

[03]在合作安全建模的场景中，需要计算数据处理模型的损失函数的值；通过损失函数的值可以衡量数据处理模型的训练效果（例如过拟合、欠拟合等），进而决定是否终止训练。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，在相关技术中，通常是将合作建模各方的数据汇总在独立的第三方，由该独立的第三方来计算损失函数的值。由于将合作建模各方的数据进行了汇总，这样容易造成企业数据的泄漏。

发明内容

[04]本说明书实施例的目的是提供一种损失函数取值的确定方法、装置和电子设备，以在保护数据隐私的前提下，由建模的各数据方协作计算出损失函数的值。

[05]为实现上述目的，本说明书中一个或多个实施例提供的技术方案如下。

[06]根据本说明书一个或多个实施例的第一方面，提供了一种损失函数取值的确定方法，所述损失函数包括第一项和第二项；所述方法包括：根据第一参数的份额与合作方秘密分享第一数据，得到第一数据的份额；根据第一数据的份额，确定第一项取值的份额；根据第二参数的份额和随机数与合作方秘密分享第二数据，得到第二数据的份额；根据随机数确定第二项的系数，第二项的系数和第二数据用于共同确定第二项的取值；向合作方发送第一项取值的份额、第二数据的份额和第二项的系数，以便合作方确定所述损失函数的取值。

[07]根据本说明书一个或多个实施例的第二方面，提供了一种损失函数取值的确定装置，

所述损失函数包括第一项和第二项；所述装置包括：第一秘密分享单元，用于根据第一参数的份额与合作方秘密分享第一数据，得到第一数据的份额；第一确定单元，用于根据第一数据的份额，确定第一项取值的份额；第二秘密分享单元，用于根据第二参数的份额和随机数与合作方秘密分享第二数据，得到第二数据的份额；确定单元，用于根据随机数确定第二项的系数，第二项的系数和第二数据用于共同确定第二项的取值；发送单元，用于向合作方发送第一项取值的份额、第二数据的份额和第二项的系数，以便合作方确定所述损失函数的取值。

[08]根据本说明书一个或多个实施例的第三方面，提供了一种电子设备，包括：存储器，用于存储计算机指令；处理器，用于执行所述计算机指令以实现如第一方面所述的方法步骤。

[09]根据本说明书一个或多个实施例的第四方面，提供了一种损失函数取值的确定方法，所述损失函数包括第一项和第二项；所述方法包括：根据第一参数的份额和标签值与合作方秘密分享第一数据，得到第一数据的份额；根据第一数据的份额，确定第一项取值的第一份额；根据第二参数的份额与合作方秘密分享第二数据，得到第二数据的第一份额；接收合作方发来的第一项取值的第二份额、第二数据的第二份额和第二项的系数，第二项的系数和第二数据用于共同确定第二项的取值；根据第一项取值的第一份额、第一项取值的第二份额、第二数据的第一份额、第二数据的第二份额和第二项的系数，确定所述损失函数的值。

[10]根据本说明书一个或多个实施例的第五方面，提供了一种损失函数取值的确定装置，所述损失函数包括第一项和第二项；所述装置包括：第一秘密分享单元，用于根据第一参数的份额和标签值与合作方秘密分享第一数据，得到第一数据的份额；第一确定单元，用于根据第一数据的份额，确定第一项取值的第一份额；第二秘密分享单元，用于根据第二参数的份额与合作方秘密分享第二数据，得到第二数据的第一份额；接收单元，用于接收合作方发来的第一项取值的第二份额、第二数据的第二份额和第二项的系数，第二项的系数和第二数据用于共同确定第二项的取值；确定单元，用于根据第一项取值的第一份额、第一项取值的第二份额、第二数据的第一份额、第二数据的第二份额和第二项的系数，确定所述损失函数的值。

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

[12]由以上本说明书实施例提供的技术方案可见，本说明书实施例中，第一数据方和第二数据方可以利用秘密分享算法，在不泄漏自身所拥有的数据的前提下，协作计算出损失函数的值；从而便于根据损失函数的值，来衡量数据处理模型的训练效果，进而决定是否终止训练。

附图说明

[13]为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[14]图 1 为本说明书实施例一种损失函数取值的确定方法的流程图；

[15]图 2 为本说明书实施例一种损失函数取值的确定方法的流程图；

[16]图 3 为本说明书实施例一种损失函数取值的确定方法的流程图；

[17]图 4 为本说明书实施例一种损失函数取值的确定装置的功能结构图；

[18]图 5 为本说明书实施例一种损失函数取值的确定装置的功能结构图；

[19]图 6 为本说明书实施例一种电子设备的功能结构图。

具体实施方式

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

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

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

[22]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。在对数据处理模型进行训练的过程中，可以通过计算损失函数的值，来衡量数据处理模型的训练效果（例如过拟合、欠拟合等），进而决定是否终止训练。所述数据处理模型包括但不限于逻辑回归模型、线性回归模型、神经网络模型等。不同的数据处理模型可以采用不同的损失函数来衡量。例如，逻辑回归模型可以采用对数损失函数（Logarithmic Loss Function）来衡量，线性回归模型可以采用平方损失函数（Square Loss）来衡量。

[23]在合作安全建模的场景中，出于保护数据隐私的考虑，多个数据方可以在不泄漏自身所拥有的数据的前提下，基于自身拥有的数据，对数据处理模型进行协作训练。在一些场景示例中，进行合作安全建模的数据方的数量为两个。其中一个数据方可以拥有完整的样本数据，另一个数据方可以拥有样本数据的标签值；或者，其中一个数据方可以拥有样本数据中的一部分数据项，另一个数据方可以拥有样本数据的另一部分数据项和样本数据的标签值。具体地，例如，样本数据包括用户的储蓄金额和借贷金额。其中一个数据方可以拥有用户的储蓄金额，另一个数据方可以拥有用户的借贷金额和样本数据的标签值。

[24]所述多个数据方需要协作计算损失函数的值，以决定是否终止训练。考虑到用于对数据处理模型进行训练的数据分散在合作建模的各数据方，若采用秘密分享算法，则合作建模的各数据方可以在不泄漏自身所拥有的数据的前提下，基于自身拥有的数据，协作计算出损失函数的值。

[25]本说明书提供一种损失函数取值的确定方法的实施例。

[26]请参阅图 1，该实施例可以包括以下步骤。

[27]步骤 S101：第一数据方根据第一参数的第一份额，第二数据方根据第一参数的第二份额和标签值，秘密分享第一数据。第一数据方获得第一数据的第一份额，第二数据方获得第一数据的第二份额。

[28]步骤 S103：第一数据方根据第一数据的第一份额，确定第一项取值的第一份额。

[29]步骤 S105：第二数据方根据第一数据的第二份额，确定第一项取值的第二份额。

[30]步骤 S107：第一数据方根据第二参数的第一份额和随机数，第二数据方根据第二参数的第二份额，秘密分享第二数据。第一数据方获得第二数据的第一份额，第二数据方获得第二数据的第二份额。

[31]步骤 S109：第一数据方根据随机数确定第二项的系数。

[32]步骤 S111：第一数据方向第二数据方发送第一项取值的第一份额、第二数据的第一份额和第二项的系数。

[33]步骤 S113：第二数据方接收第一项取值的第一份额、第二数据的第一份额和第二项的系数。

[34]步骤 S115：第二数据方根据第一项取值的第一份额、第一项取值的第二份额、第二数据的第一份额、第二数据的第二份额和第二项的系数，确定所述损失函数的值。

[35]下面介绍在实施例中涉及的一些术语。

[36]（一）、第一项和第二项。所述第一项和所述第二项分别为所述损失函数中的函数项。

[37]在一些场景示例中，所述损失函数可以为对数损失函数 $L(\theta)=-\frac{1}{m}\sum_{i=1}^{m}[y_i\log h_\theta(x_i)+(1-y_i)\log(1-h_\theta(x_i))]$。$m$ 表示样本数据的数量；x_i 表示第 i 个样本数据；y_i 表示样本数据 x_i 的标签值；θ 表示数据处理模型的模型参数；$h_\theta(x_i)$ 表示数据处理模型的激励函数的取值，$h_\theta(x_i)=\frac{1}{1+e^{-\theta x_i}}$。

$$
\begin{aligned}
L(\theta)&=-\frac{1}{m}\sum_{i=1}^{m}[y_i(\log h_\theta(x_i)+(1-y_i)\log(1-h_\theta(x_i))]\\
&=-\frac{1}{m}\sum_{i=1}^{m}[y_i\log\frac{1}{1+e^{-\theta x_i}}+(1-y_i)\log\frac{e^{-\theta x_i}}{1+e^{-\theta x_i}}]\\
&=-\frac{1}{m}\sum_{i=1}^{m}[y_i\log\frac{1}{1+e^{-\theta x_i}}+(1-y_i)(-\theta x_i+\log\frac{1}{1+e^{-\theta x_i}}]\\
&=-\frac{1}{m}\sum_{i=1}^{m}[\log h_\theta(x_i)+(1-y_i)(-\theta x_i)]\\
&=-\frac{1}{m}\sum_{i=1}^{m}\log h_\theta(x_i)+\frac{1}{m}\sum_{i=1}^{m}(1-y_i)\theta x_i\\
&=-\frac{1}{m}\log\prod_{i=1}^{m}h_\theta(x_i)+\frac{1}{m}\sum_{i=1}^{m}(1-y_i)\theta x_i\\
&=-\frac{1}{m}\log\prod_{i=1}^{m}h_\theta(x_i)r_i/\prod_{i=1}^{m}r_i+\frac{1}{m}\sum_{i=1}^{m}(1-y_i)\theta x_i
\end{aligned}
$$

，r_i 表示第 i 个随机数。

[38]那么，所述第一项可以为$\frac{1}{m}\sum_{i=1}^{m}(1-y_i)\theta x_i$，所述第二项可以为$-\frac{1}{m}\log\prod_{i=1}^{m}h_\theta(x_i)r_i/\prod_{i=1}^{m}r_i$。

[39]（二）、第一数据方和第二数据方。所述第一数据方和所述第二数据方分别为合作安全建模的双方。所述第一数据方可以为不拥有标签值的数据方，所述第二数据方可以为拥有标签值的数据方。例如，所述第一数据方可以拥有完整的样本数据，所述第二数据方可以拥有样本数据的标签值。或者，所述第一数据方可以拥有样本数据的一部分数据项，所述第二数据方可以拥有样本数据的另一部分数据项和标签值。所述标签值可以用于区分不同类型的样本数据，具体数值例如可以取自0和1。其中，所述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。

[40]（三）、第一参数和第二参数。所述第一参数和所述第二参数分别为所述第一数据方和所述第二数据方在合作安全建模过程中获得的中间结果。所述第一参数和所述第二参数不同。例如，所述第一参数可以为样本数据与数据处理模型的模型参数之间的乘积，所述第二参数可以为数据处理模型的激励函数的值。

[41]在合作安全建模的过程中，所述第一数据方和所述第二数据方分别获得所述第一参数的一份份额。为了便于描述，可以将所述第一数据方获得的份额作为第一参数的第一份额，可以将所述第二数据方获得的份额作为第一参数的第二份额。第一参数的第一份额和第一参数的第二份额的和即为第一参数。此外，所述第一参数的数量可以为多个。如此所述第一数据方可以拥有多个第一参数的第一份额，所述第二数据方可以拥有多个第一参数的第二份额。

[42]延续前面的场景示例，第一参数可以表示为θx_i，第一参数的第一份额可以表示为$<\theta x_i>_0$，第一参数的第二份额可以表示为$<\theta x_i>_1$。其中$<\theta x_i>_0+<\theta x_i>_1=\theta x_i$。

[43]在合作安全建模的过程中，所述第一数据方和所述第二数据方分别获得所述第二参数的一份份额。为了便于描述，可以将所述第一数据方获得的份额作为第二参数的第一份额，可以将所述第二数据方获得的份额作为第二参数的第二份额。第二参数的第一份额和第二参数的第二份额的和即为第二参数。此外，所述第二参数的数量可以为多个。如此所述第一数据方可以拥有多个第二参数的第一份额，所述第二数据方可以拥有多个第二参数的第二份额。

[44]延续前面的场景示例，第二参数可以表示为 $h_\theta(x_i)=\frac{1}{1+e^{-\theta x_i}}$，第二参数的第一份额可以表示为 $<h_\theta(x_i)>_0$，第二参数的第二份额可以表示为 $<h_\theta(x_i)>_1$。其中 $<h_\theta(x_i)>_0+<h_\theta(x_i)>_1=h_\theta(x_i)$。

[45]（四）、第一数据和第二数据。所述第一数据和所述第二数据分别由所述第一数据方和所述第二数据方通过秘密分享算法计算得到。所述第一数据用于确定第一项的取值。所述第二数据与所述第二项的系数相结合能够确定出第二项的取值。

[46]延续前面的场景示例，第一数据可以表示为 $(1-y_i)\theta x_i$，第二数据可以表示为 $r_i h_\theta(x_i)$，第二项的系数可以表示为 $\prod_{i=1}^{m} r_i$。

[47]（五）、第三数据和第四数据。所述第三数据和所述第四数据分别由所述第一数据方和所述第二数据方通过秘密分享算法计算得到。根据第三数据的份额能够确定出第一数据的份额。根据第四数据的份额能够确定出第二数据的份额。

[48]延续前面的场景示例，第三数据可以表示为 $(1-y_i)<\theta x_i>_0$，第四数据可以表示为 $r_i<h_\theta(x_i)>_1$。

[49]在一些实施例中，在步骤 S101 中，所述第一数据方可以根据第一参数的第一份额，所述第二数据方可以根据第一参数的第二份额和标签值，秘密分享第一数据。所述第一数据方和所述第二数据方可以分别获得第一数据的一份份额。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数据的第一份额，可以将所述第二数据方获得的份额作为第一数据的第二份额。第一数据的第一份额和第一数据的第二份额的和即为第一数据。

[50]如前面所述，所述第一数据方可以拥有多个第一参数的第一份额，所述第二数据方可以拥有多个第一参数的第二份额。如此所述第一数据方可以根据每个第一参数的第一份额，所述第二数据方可以根据该第一参数的第二份额和与该第一参数相对应的标签值，秘密分享一个第一数据。所述第一数据方可以获得该第一数据的第一份额，所述第二数据方可以获得该第一数据的第二份额。值得说明的是，第一参数与标签值相对应可以理解为：标签值所对应的样本数据与用于计算第一参数的样本数据为同一样本数据。

[51]进一步地，所述第一数据方可以根据每个第一参数的第一份额，所述第二数据方可以根据与该第一参数相对应的标签值，秘密分享一个第三数据。所述第一数据方和所述

第二数据方可以分别获得该第三数据的一份份额。为了便于描述，可以将所述第一数据方获得的份额作为该第三数据的第一份额，可以将所述第二数据方获得的份额作为该第三数据的第二份额。该第三数据的第一份额和该第三数据的第二份额的和即为该第三数据。如此所述第一数据方可以直接将该第三数据的第一份额作为第一数据的第一份额。所述第二数据方可以将该第一参数的第二份额与与该第一参数相对应的标签值按照预设运算规则进行运算；可以将运算结果与该第三数据的第二份额相加，可以将相加结果作为第一数据的第二份额。

[52]延续前面的场景示例，所述第一数据方可以根据$<\theta x_i>_0$，所述第二数据方可以根据$1-y_i$，秘密分享第三数据$(1-y_i)<\theta x_i>_0$。所述第一数据方可以获得第三数据的第一份额$<[(1-y_i)<\theta x_i>_0]>_0$。所述第二数据方可以获得第三数据的第二份额$<[(1-y_i)<\theta x_i>_0]>_1$。其中，$<[(1-y_i)<\theta x_i>_0]>_0+<[(1-y_i)<\theta x_i>_0]>_1=(1-y_i)<\theta x_i>_0$。

[53]所述第一数据方可以直接将第三数据的第一份额$<[(1-y_i)<\theta x_i>_0]>_0$作为第一数据$(1-y_i)\theta x_i$的第一份额$<(1-y_i)\theta x_i>_0$。所述第二数据方可以根据$<\theta x_i>_1$和$y_i$计算得到$(1-y_i)<\theta x_i>_1$；可以将计算结果$(1-y_i)<\theta x_i>_1$与第三数据的第二份额$<[(1-y_i)<\theta x_i>_0]>_1$相加；可以将相加结果作为第一数据$(1-y_i)\theta x_i$的第二份额$<(1-y_i)\theta x_i>_1$。其中，

$$\begin{aligned}&<(1-y_i)\theta x_i>_0+<(1-y_i)\theta x_i>_1\\=&<[(1-y_i)<\theta x_i>_0]>_0+<[(1-y_i)<\theta x_i>_0]>_1+(1-y_i)<\theta x_i>_1。\\=&(1-y_i)\theta x_i\end{aligned}$$

[54]在一些实施例中，经过步骤S101，所述第一数据方可以获得多个第一数据的第一份额。如此在步骤S103中，所述第一数据方可以对多个第一数据的第一份额进行累加；可以根据累加结果确定第一项取值的第一份额。具体地，所述第一数据方可以将累加结果与第一数据的数量（也即第一参数的数量）相除，得到第一项取值的第一份额。

[55]延续前面的场景示例，所述第一数据方可以计算$\frac{1}{m}\sum_{i=1}^{m}<(1-y_i)\theta x_i>_0$作为第一项取值的第一份额。

[56]在一些实施例中，经过步骤S101，所述第二数据方可以获得多个第一数据的第二份额。如此在步骤S105中，所述第二数据方可以对多个第一数据的第二份额进行累加；可以根据累加结果确定第一项取值的第二份额。具体地，所述第一数据方可以将累加结果与第一数据的数量（也即第一参数的数量）相除，得到第一项取值的第二份额。第一

项取值的第一份额和第一项取值的第二份额的和即为第一项的取值。

[57]延续前面的场景示例，所述第二数据方可以计算$\frac{1}{m}\sum_{i=1}^{m}<(1-y_i)\theta x_i>_1$作为第一项取值的第二份额。其中，$\frac{1}{m}\sum_{i=1}^{m}<(1-y_i)\theta x_i>_0+\frac{1}{m}\sum_{i=1}^{m}<(1-y_i)\theta x_i>_1=\frac{1}{m}\sum_{i=1}^{m}(1-y_i)\theta x_i$。

[58]在一些实施例中，在步骤 S107 中，所述第一数据方可以根据第二参数的第一份额和随机数，所述第二数据方可以根据第二参数的第二份额，秘密分享第二数据。所述第一数据方和所述第二数据方可以分别获得第二数据的一份份额。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数据的第一份额，可以将所述第二数据方获得的份额作为第二数据的第二份额。第二数据的第一份额和第二数据的第二份额的和即为第二数据。

[59]如前面所述，第二参数的数量可以为多个。所述第一数据方可以生成多个随机数，每个随机数可以对应一个第二参数（或第二参数的第一份额）。随机数可以用于掩盖第二参数，以进行隐私保护，从而防止第二数据方获得具体的第二参数。这样在后续的步骤 S115 中，即使第二数据方获得了来自第一数据方的第二数据的第一份额，进而将第二数据的第一份额与自身拥有的第二数据的第二份额相加，获得的也是第二参数与随机数的乘积，而无法获得具体的第二参数。相关场景示例可以参见后续的步骤 S115。如此所述第一数据方可以根据每个第二参数的第一份额和与该第二参数相对应的随机数，所述第二数据方可以根据该第二参数的第二份额，秘密分享一个第二数据。所述第一数据方可以获得该第二数据的第一份额，所述第二数据方可以获得该第二数据的第二份额。

[60]进一步地，所述第一数据方可以根据每个随机数，所述第二数据方可以根据与该随机数相对应的第二参数的第二份额，秘密分享一个第四数据。所述第一数据方和所述第二数据方可以分别获得该第四数据的一份份额。为了便于描述，可以将所述第一数据方获得的份额作为该第四数据的第一份额，可以将所述第二数据方获得的份额作为该第四数据的第二份额。该第四数据的第一份额和该第四数据的第二份额的和即为该第四数据。如此所述第一数据方可以将该第二参数的第一份额与该随机数相乘；可以将乘积结果与该第四数据的第一份额相加；可以将相加结果作为第二数据的第一份额。所述第二数据方可以直接将该第四数据的第二份额作为第二数据的第二份额。

[61]延续前面的场景示例，所述第一数据方可以根据r_i，所述第二数据方可以根据$<h_\theta(x_i)>_1$，秘密分享第四数据$r_i<h_\theta(x_i)>_1$。所述第一数据方可以获得第四数据的第一

份额 $<[r_i<h_\theta(x_i)>_1]>_0$，所述第二数据方可以获得第四数据的第二份额 $<[r_i<h_\theta(x_i)>_1]>_1$。其中，$<[r_i<h_\theta(x_i)>_1]>_0+<[r_i<h_\theta(x_i)>_1]>_1=r_i<h_\theta(x_i)>_1$。

[62]所述第一数据方可以将 $<h_\theta(x_i)>_0$ 与 r_i 相乘；可以将乘积结果 $r_i<h_\theta(x_i)>_0$ 与第四数据的第一份额 $<[r_i<h_\theta(x_i)>_1]>_0$ 相加；可以将相加结果作为第一数据 $r_ih_\theta(x_i)$ 的第一份额 $<r_ih_\theta(x_i)>_0$。所述第二数据方可以直接将第四数据的第二份额 $<[r_i<h_\theta(x_i)>_1]>_1$ 作为第一数据 $r_ih_\theta(x_i)$ 的第二份额 $<r_ih_\theta(x_i)>_1$。其中，

$$
\begin{aligned}
&<r_ih_\theta(x_i)>_0+<r_ih_\theta(x_i)>_1\\
&=r_i<h_\theta(x_i)>_0+<[r_i<h_\theta(x_i)>_1]>_0+<[r_i<h_\theta(x_i)>_1]>_1。\\
&=r_ih_\theta(x_i)
\end{aligned}
$$

[63]在一些实施例中，在步骤 S109 中，所述第一数据方可以将多个随机数进行累乘，得到第二项的系数。延续前面的场景示例，所述第一数据方可以计算 $\prod_{i=1}^{m}r_i$ 作为第二项的系数。

[64]在一些实施例中，在步骤 S111 中，所述第一数据方可以向所述第二数据方发送第一项取值的第一份额、多个第二数据的第一份额和第二项的系数。在步骤 S113 中，所述第二数据方可以接收第一项取值的第一份额、多个第二数据的第一份额和第二项的系数。

[65]在一些实施例中，在步骤 S115 中，所述第二数据方可以将第一项取值的第一份额和第一项取值的第二份额相加，得到第一项的取值；可以将第二数据的第一份额和第二数据的第二份额相加，得到第二数据；可以根据第二数据和第二项的系数，确定第二项的取值。所述第二数据方可以将第一项的取值和第二项的取值相加，得到所述损失函数的值。其中，所述第二数据方可以将每个第二数据的第一份额和该第二数据的第二份额相加，得到第二数据；可以将多个第二数据进行累乘；可以根据累乘结果与第二项的系数，确定第二项的取值。

[66]延续前面的场景示例，所述第二数据方可以将第一项取值的第一份额 $\frac{1}{m}\sum_{i=1}^{m}<(1-y_i\ \theta x_i>_0$ 和第一项取值的第二份额 $\frac{1}{m}\sum_{i=1}^{m}<(1-y_i)\theta x_i>_1$ 相加，得到第一项的取值 $\frac{1}{m}\sum_{i=1}^{m}(1-y_i)\theta x_i$。

[67]所述第二数据方可以将第二数据的第一份额 $<r_ih_\theta(x_i)>_0$ 和第二数据的第二份额相加，

得到第二数据 $r_i h_\theta(x_i)$；可以计算 $-\frac{1}{m}\log\prod_{i=1}^{m} h_\theta(x_i)r_i / \prod_{i=1}^{m} r_i$，得到第二项的取值。值得说明的是，由于使用了随机数，所述第二数据方即使将第二数据的第一份额和第二数据的第二份额相加，获得的也是第二参数 $h_\theta(x_i)$ 与随机数 r_i 的乘积 $r_i h_\theta(x_i)$，而无法获得具体的第二参数 $h_\theta(x_i)$，从而实现了对第二参数 $h_\theta(x_i)$ 的掩盖。

[68]所述第二数据方可以将第一项的取值 $\frac{1}{m}\sum_{i=1}^{m}(1-y_i)\theta x_i$ 和第二项的取值 $-\frac{1}{m}\log\prod_{i=1}^{m} h_\theta(x_i)r_i / \prod_{i=1}^{m} r_i$ 相加，得到对数损失函数 $L(\theta = -\frac{1}{m}\sum_{i=1}^{m}$ i y [+ h − o x g T θ (y 的取值。

[69]在本实施例中，第一数据方和第二数据方可以利用秘密分享算法，在不泄漏自身所拥有的数据的前提下，协作计算出损失函数的值；从而便于根据损失函数的值，来衡量数据处理模型的训练效果，进而决定是否终止训练。例如，第二数据方可以将损失函数的值发送给可信任的第三方（TTP，Trusted Third Party），由可信任的第三方来决定是否终止训练。

[70]基于同样的发明构思，本说明书还提供另一种损失函数取值的确定方法的实施例。所述损失函数可以包括第一项和第二项。所述第一项和所述第二项分别为所述损失函数中不同的函数项。该实施例以第一数据方为执行主体。所述第一数据方可以为不拥有标签值的数据方。具体地，例如，所述第一数据方可以拥有完整的样本数据；或者，可以拥有样本数据的一部分数据项。请参阅图 2，该实施例可以包括以下步骤。

[71]步骤 S21：根据第一参数的份额与合作方秘密分享第一数据，得到第一数据份额。

[72]所述合作方可以理解为与所述第一数据方进行合作安全建模的数据方，具体可以为前面的第二数据方。所述第一数据方可以根据第一参数的份额与合作方秘密分享第一数据，得到相应的份额。具体过程可以参见前面步骤 S101 中的相关描述，在此不再赘述。

[73]步骤 S23：根据第一数据的份额，确定第一项取值的份额。

[74]所述第一数据方可以对第一数据的份额进行累加；可以根据累加结果确定第一项取值的份额。具体过程可以参见前面步骤 S103 中的相关描述，在此不再赘述。

[75]步骤 S25：根据第二参数的份额和随机数与合作方秘密分享第二数据，得到第二数据的份额。

[76]第二数据与后续第二项的系数相结合能够确定出第二项的取值。所述第一数据方可以生成与第二参数的份额相对应的随机数；可以将第二参数的份额与随机数相乘；可以根据随机数与合作方秘密分享第三数据，得到相应的份额；可以将乘积结果与第三数据的份额相加，得到第二数据的份额。具体过程可以参见前面步骤 S107 中的相关描述，在此不再赘述。

[77]步骤 S27：根据随机数确定第二项的系数。

[78]所述第一数据方可以对随机数进行累乘，得到第二项的系数。具体过程可以参见前面步骤 S109 中的相关描述，在此不再赘述。

[79]步骤 S29：向合作方发送第一项取值的份额、第二数据的份额和第二项的系数，以便合作方确定所述损失函数的取值。

[80]在本实施例中，第一数据方可以利用秘密分享算法，在不泄漏自身所拥有的数据的前提下，与合作方协作计算出第一项取值的份额、第二数据的份额和第二项的系数；可以向合作方发送第一项取值的份额、第二数据的份额和第二项的系数，以便由合作方确定出所述损失函数的取值。

[81]基于同样的发明构思，本说明书还提供另一种损失函数取值的确定方法的实施例。所述损失函数可以包括第一项和第二项。所述第一项和所述第二项分别为所述损失函数中不同的函数项。该实施例以第二数据方为执行主体。所述第二数据方可以为拥有标签值的数据方。具体地，例如，所述第二数据方可以仅拥有标签值；或者，还可以拥有样本数据的一部分数据项。请参阅图 3，该实施例可以包括以下步骤。

[82]步骤 S31：根据第一参数的份额和标签值与合作方秘密分享第一数据，得到第一数据的份额。

[83]所述合作方可以理解为与所述第二数据方进行合作安全建模的数据方，具体可以为前面的第一数据方。所述第二数据方可以将第一参数的份额与标签值按照预设运算规则进行运算；可以根据标签值与合作方秘密分享第三数据，得到相应的份额；可以将运算结果与第三数据的份额相加，得到第一数据的份额。具体过程可以参见前面步骤 S101 中的相关描述，在此不再赘述。

[84]步骤 S33：根据第一数据的份额，确定第一项取值的第一份额。

[85]所述第二数据方可以对第一数据的份额进行累加；可以根据累加结果确定第一项取值的第一份额。具体过程可以参见前面步骤 S105 中的相关描述，在此不再赘述。

[86]步骤 S35：根据第二参数的份额与合作方秘密分享第二数据，得到第二数据的第一份额。

[87]第一数据与后续第二项的系数相结合能够确定出第二项的取值。具体过程可以参见前面步骤 S107 中的相关描述，在此不再赘述。

[88]步骤 S37：接收合作方发来的第一项取值的第二份额、第二数据的第二份额和第二项的系数。

[89]步骤 S39：根据第一项取值的第一份额、第一项取值的第二份额、第二数据的第一份额、第二数据的第二份额和第二项的系数，确定所述损失函数的值。

[90]所述第二数据方可以将第一项取值的第一份额和第一项取值的第二份额相加，得到第一项的取值；可以将第二数据的第一份额和第二数据的第二份额相加，得到第二数据；可以根据第二数据和第二项的系数，确定第二项的取值；可以将第一项的取值和第二项的取值相加，得到所述损失函数的值。具体过程可以参见前面步骤 S115 中的相关描述，在此不再赘述。

[91]在本实施例中，第二数据方可以利用秘密分享算法，在不泄漏自身所拥有的数据的前提下，与合作方协作计算出第一项取值的第一份额、第二数据的第一份额。这样所述第二数据方结合来自合作方的第一项取值的第二份额、第二数据的第二份额和第二项的系数，便可以确定出损失函数的取值。

[92]基于同样的发明构思，本说明书还提供一种损失函数取值的确定装置的实施例。所述损失函数可以包括第一项和第二项。所述第一项和所述第二项分别为所述损失函数中不同的函数项。该实施例可以应用于第一数据方。所述第一数据方可以为不拥有标签值的数据方。具体地，例如，所述第一数据方可以拥有完整的样本数据；或者，可以拥有样本数据的一部分数据项。请参阅图 4，该实施例可以包括以下单元。

[93]第一秘密分享单元 41，用于根据第一参数的份额与合作方秘密分享第一数据，得到第一数据的份额；

[94]第一确定单元 43，用于根据第一数据的份额，确定第一项取值的份额；

[95]第二秘密分享单元 45，用于根据第二参数的份额和随机数与合作方秘密分享第二数据，得到第二数据的份额；

[96]第二确定单元 47，用于根据随机数确定第二项的系数，第二项的系数和第一数据用

于共同确定第二项的取值；

[97]发送单元 49，用于向合作方发送第一项取值的份额、第二数据的份额和第二项的系数，以便合作方确定所述损失函数的取值。

[98]基于同样的发明构思，本说明书还提供另一种损失函数取值的确定装置的实施例。所述损失函数可以包括第一项和第二项。所述第一项和所述第二项分别为所述损失函数中不同的函数项。该实施例可以应用于第二数据方。所述第二数据方可以为拥有标签值的数据方。具体地，例如，所述第二数据方可以仅拥有标签值；或者，还可以拥有样本数据的一部分数据项。请参阅图 5，该实施例可以包括以下单元。

[99]第一秘密分享单元 51，用于根据第一参数的份额和标签值与合作方秘密分享第一数据，得到第一数据的第一份额；

[100] 第一确定单元 53，用于根据第一数据的份额，确定第一项取值的第一份额；

[101] 第二秘密分享单元 55，用于根据第二参数的份额与合作方秘密分享第二数据，得到第二数据的第一份额；

[102] 接收单元 57，用于接收合作方发来的第一项取值的第二份额、第二数据的第二份额和第二项的系数，第二项的系数和第二数据用于共同确定第二项的取值；

[103] 第二确定单元 59，用于根据第一项取值的第一份额、第一项取值的第二份额、第二数据的第一份额、第二数据的第二份额和第二项的系数，确定所述损失函数的值。

[104] 下面介绍本说明书电子设备的一个实施例。图 6 是该实施例中一种电子设备的硬件结构示意图。如图 6 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 6 所示的硬件结构仅为示意，其并不对上述电子设备的硬件结构造成限定。在实际中所述电子设备还可以包括比图 6 所示更多或者更少的组件单元；或者，具有与图 6 所示不同的配置。

[105] 所述存储器可以包括高速随机存储器；或者，还可以包括非易失性存储器，例如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。当然，所述存储器还可以包括远程设置的网络存储器。所述远程设置的网络存储器可以通过诸如互联网、企业内部网、局域网、移动通信网等网络连接至所述电子设备。所述存储器可以用于存储应用软件的程序指令或模块，例如本说明书图 2 所对应实施例的程序指令或模块；和/或，本说明书图 3 所对应实施例的程序指令或模块。

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

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

[108] 需要说明的是，本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同或相似的部分互相参见即可，每个实施例重点说明的都是与其它实施例的不同之处。尤其，对于装置实施例和电子设备实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。另外，可以理解的是，本领域技术人员在阅读本说明书文件之后，可以无需创造性劳动想到将本说明书列举的部分或全部实施例进行任意组合，这些组合也在本说明书公开和保护的范围内。

[109] 在20世纪90年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array，FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片PLD上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片2。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language，HDL），而HDL也并非仅有一种，而是有许多种，如ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是VHDL（Very-High-Speed Integrated Circuit Hardware Description

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

[110] 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。

[111] 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。

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

[113] 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。

[114] 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、一种损失函数取值的确定方法，所述损失函数包括第一项和第二项；所述方法包括:

根据第一参数的份额与合作方秘密分享第一数据，得到第一数据的份额;

根据第一数据的份额，确定第一项取值的份额;

根据第二参数的份额和随机数与合作方秘密分享第二数据，得到第二数据的份额;

根据随机数确定第二项的系数，第二项的系数和第二数据用于共同确定第二项的取值;

向合作方发送第一项取值的份额、第二数据的份额和第二项的系数，以便合作方确定所述损失函数的取值。

2、如权利要求 1 所述的方法，所述确定第一项取值的份额，包括:

对第一数据的份额进行累加;

根据累加结果确定第一项取值的份额。

3、如权利要求 1 所述的方法，所述方法包括:

生成与第二参数的份额相对应的随机数。

4、如权利要求 1 或 3 所述的方法，所述根据随机数确定第二项的系数，包括:

对随机数进行累乘，得到第二项的系数。

5、如权利要求 1 或 3 所述的方法，所述根据第二参数的份额和随机数与合作方秘密分享第二数据，得到第二数据的份额，包括:

将第二参数的份额与随机数相乘;

根据随机数与合作方秘密分享第三数据，得到相应的份额;

将乘积结果与第三数据的份额相加，得到第二数据的份额。

6、一种损失函数取值的确定装置，所述损失函数包括第一项和第二项；所述装置包括:

第一秘密分享单元，用于根据第一参数的份额与合作方秘密分享第一数据，得到第一数据的份额;

第一确定单元，用于根据第一数据的份额，确定第一项取值的份额;

第二秘密分享单元，用于根据第二参数的份额和随机数与合作方秘密分享第二数据，得到第二数据的份额;

第二确定单元，用于根据随机数确定第二项的系数，第二项的系数和第二数据用于共同确定第二项的取值;

发送单元，用于向合作方发送第一项取值的份额、第二数据的份额和第二项的系数，以便合作方确定所述损失函数的取值。

7、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 1-5 中任一项所述的方法步骤。

8、一种损失函数取值的确定方法，所述损失函数包括第一项和第二项；所述方法包括：

根据第一参数的份额和标签值与合作方秘密分享第一数据，得到第一数据的份额；

根据第一数据的份额，确定第一项取值的第一份额；

根据第二参数的份额与合作方秘密分享第二数据，得到第二数据的第一份额；

接收合作方发来的第一项取值的第二份额、第二数据的第二份额和第二项的系数，第二项的系数和第二数据用于共同确定第二项的取值；

根据第一项取值的第一份额、第一项取值的第二份额、第二数据的第一份额、第二数据的第二份额和第二项的系数，确定所述损失函数的值。

9、如权利要求 8 所述的方法，所述根据第一参数的份额和标签值与合作方秘密分享第一数据，得到第一数据的份额，包括：

将第一参数的份额与标签值按照预设运算规则进行运算；

根据标签值与合作方秘密分享第三数据，得到相应的份额；

将运算结果与第三数据的份额相加，得到第一数据的份额。

10、如权利要求 8 所述的方法，所述根据第一项取值的第一份额、第一项取值的第二份额、第二数据的第一份额、第二数据的第二份额和第二项的系数，确定所述损失函数的值，包括：

将第一项取值的第一份额和第一项取值的第二份额相加，得到第一项的取值；

将第二数据的第一份额和第二数据的第二份额相加，得到第二数据；

根据第二数据和第二项的系数，确定第二项的取值；

将第一项的取值和第二项的取值相加，得到所述损失函数的值。

11、一种损失函数取值的确定装置，所述损失函数包括第一项和第二项；所述装置包括：

第一秘密分享单元，用于根据第一参数的份额和标签值与合作方秘密分享第一数据，得到第一数据的份额；

第一确定单元，用于根据第一数据的份额，确定第一项取值的第一份额；

第二秘密分享单元，用于根据第二参数的份额与合作方秘密分享第二数据，得到第二数据的第一份额；

接收单元，用于接收合作方发来的第一项取值的第二份额、第二数据的第二份额和第二项的系数，第二项的系数和第二数据用于共同确定第二项的取值；

第二确定单元，用于根据第一项取值的第一份额、第一项取值的第二份额、第二数据的第一份额、第二数据的第二份额和第二项的系数，确定所述损失函数的值。

12、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 8-10 中任一项所述的方法步骤。

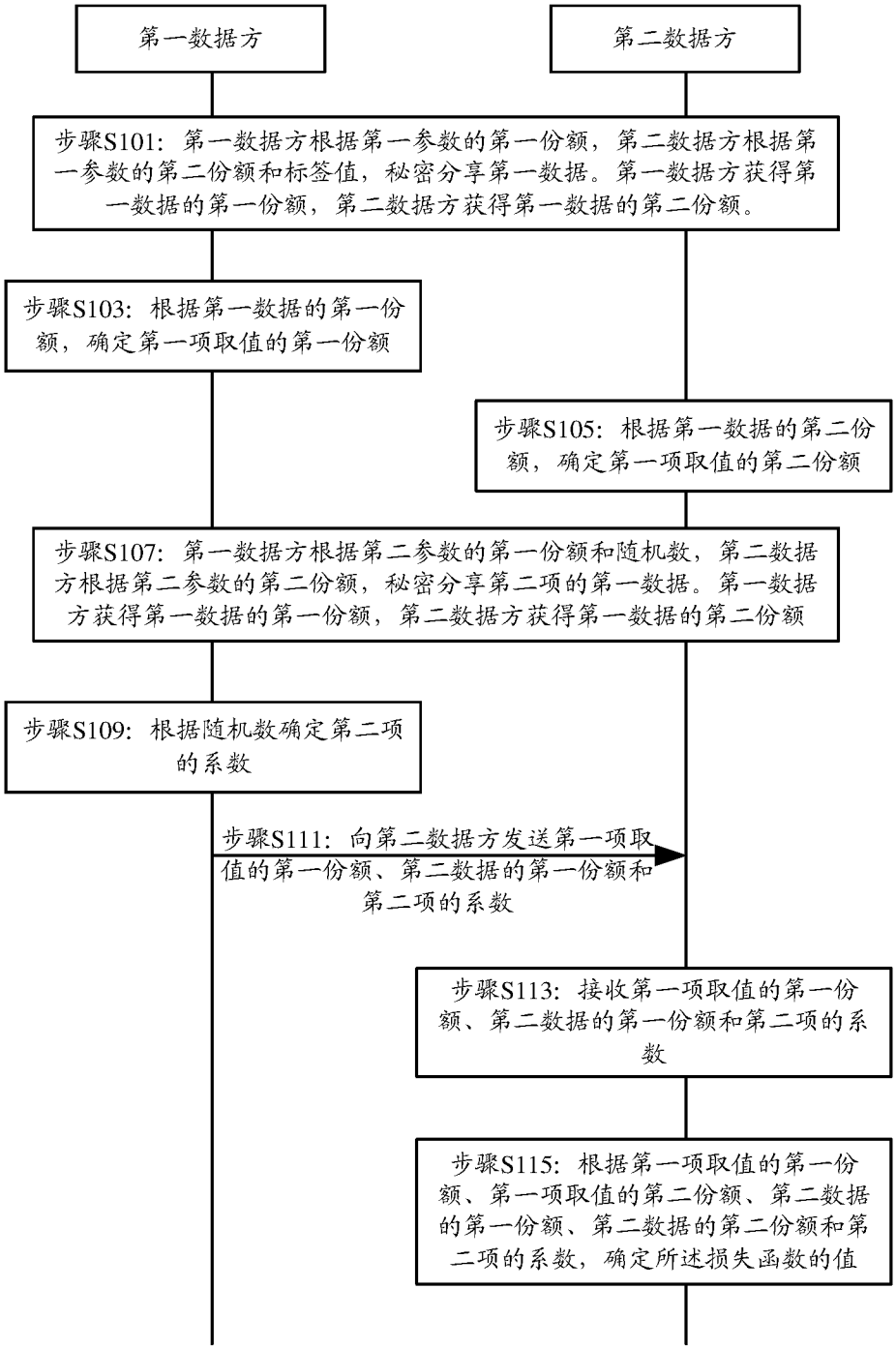

第一数据方
第二数据方
步骤S101：第一数据方根据第一参数的第一份额，第二数据方根据第一参数的第二份额和标签值，秘密分享第一数据。第一数据方获得第一数据的第一份额，第二数据方获得第一数据的第二份额。
步骤S103：根据第一数据的第一份额，确定第一项取值的第一份额
步骤S105：根据第一数据的第二份额，确定第一项取值的第二份额
步骤S107：第一数据方根据第二参数的第一份额和随机数，第二数据方根据第二参数的第二份额，秘密分享第二项的第一数据。第一数据方获得第一数据的第一份额，第二数据方获得第一数据的第二份额
步骤S109：根据随机数确定第二项的系数
步骤S111：向第二数据方发送第一项取值的第一份额、第二数据的第一份额和第二项的系数
步骤S113：接收第一项取值的第一份额、第二数据的第一份额和第二项的系数
步骤S115：根据第一项取值的第一份额、第一项取值的第二份额、第二数据的第一份额、第二数据的第二份额和第二项的系数，确定所述损失函数的值

图 1

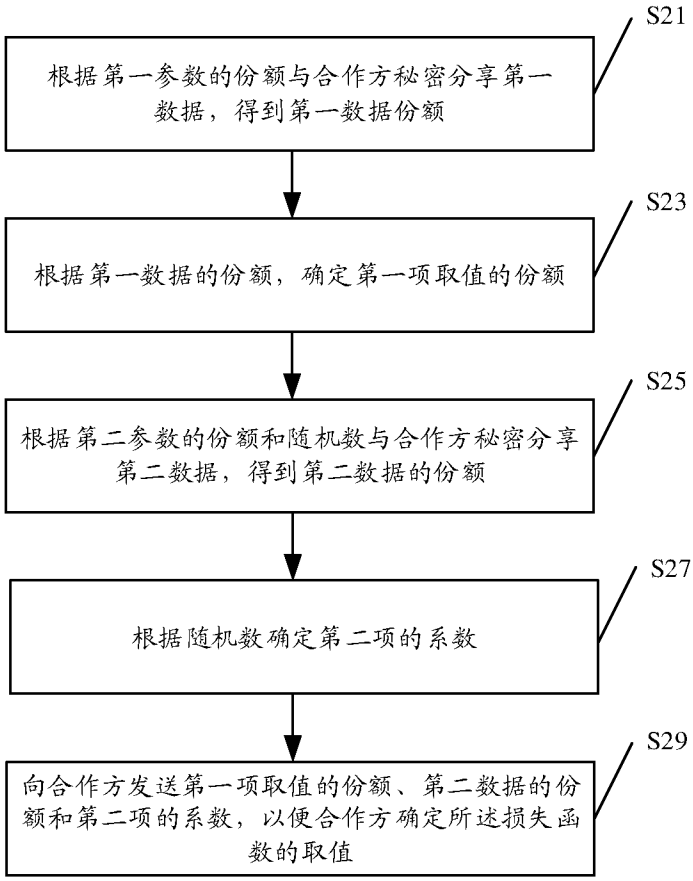

S21
根据第一参数的份额与合作方秘密分享第一数据，得到第一数据份额
S23
根据第一数据的份额，确定第一项取值的份额
S25
根据第二参数的份额和随机数与合作方秘密分享第二数据，得到第二数据的份额
S27
根据随机数确定第二项的系数
S29
向合作方发送第一项取值的份额、第二数据的份额和第二项的系数，以便合作方确定所述损失函数的取值

图 2

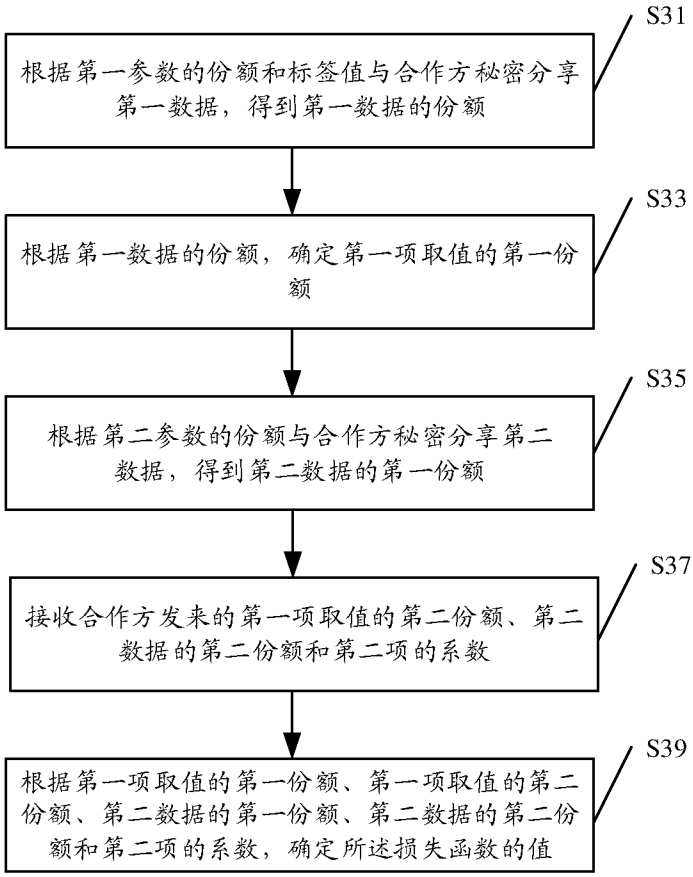

S31
根据第一参数的份额和标签值与合作方秘密分享第一数据，得到第一数据的份额
S33
根据第一数据的份额，确定第一项取值的第一份额
S35
根据第二参数的份额与合作方秘密分享第二数据，得到第二数据的第一份额
S37
接收合作方发来的第一项取值的第二份额、第二数据的第二份额和第二项的系数
S39
根据第一项取值的第一份额、第一项取值的第二份额、第二数据的第一份额、第二数据的第二份额和第二项的系数，确定所述损失函数的值

图 3

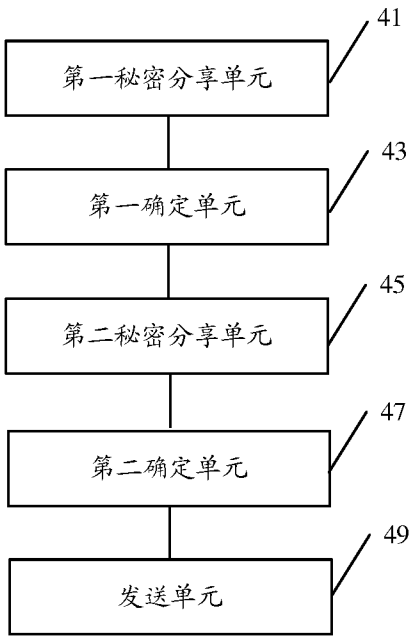

41
第一秘密分享单元
43
第一确定单元
45
第二秘密分享单元
47
第二确定单元
49
发送单元

图 4

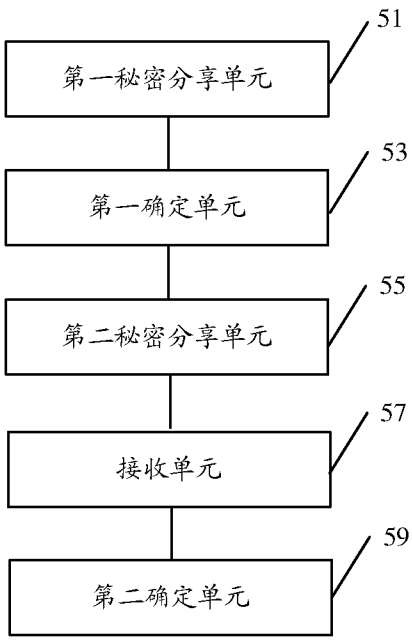

51
第一秘密分享单元
53
第一确定单元
55
第二秘密分享单元
57
接收单元
59
第二确定单元

图 5

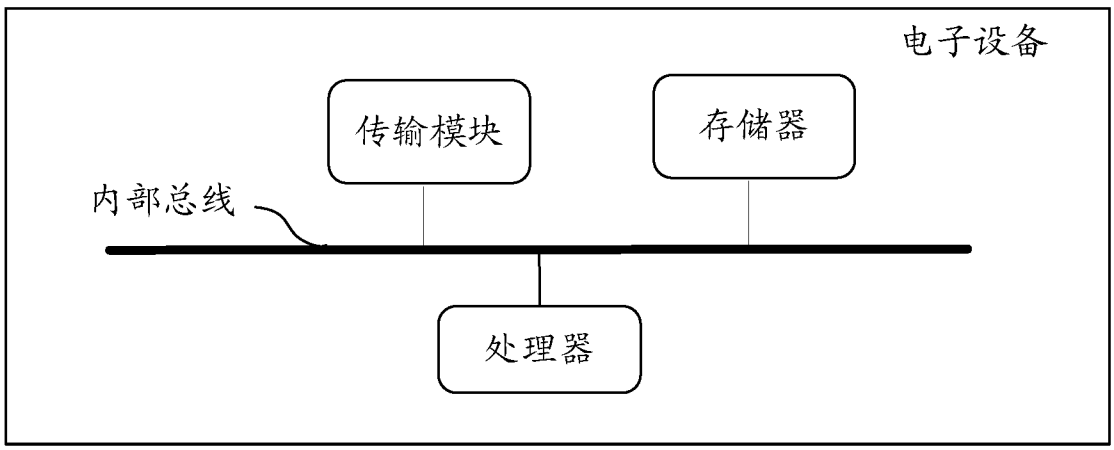

电子设备
传输模块
存储器
内部总线
处理器

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/070939

A. CLASSIFICATION OF SUBJECT MATTER

G06F 17/15(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; H04L; G06Q; 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: 损失函数, 秘密分享, 取值, 随机, 标签, loss, share, secret, value, random, tag

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110263294 A (ALIBABA GROUP HOLDING LIMITED) 20 September 2019 (2019-09-20) claims 1-12	1-12
A	CN 108764666 A (STATE GRID SHANGHAI MUNICIPAL ELECTRIC POWER COMPANY et al.) 06 November 2018 (2018-11-06) description, paragraphs [0071]-[0091]	1-12
A	CN 108418810 A (NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY) 17 August 2018 (2018-08-17) entire document	1-12
A	US 2017300811 A1 (LINKEDIN CO.) 19 October 2017 (2017-10-19) entire document	1-12
A	US 2012330867 A1 (INTERNATIONAL BUSINESS MACHINES CO.) 27 December 2012 (2012-12-27) entire document	1-12

☐ 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	Date of mailing of the international search report
25 March 2020	**08 April 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	Authorized officer
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/070939

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110263294 A	20 September 2019	None	
CN 108764666 A	06 November 2018	None	
CN 108418810 A	17 August 2018	None	
US 2017300811 A1	19 October 2017	None	
US 2012330867 A1	27 December 2012	US 2012331025 A1	27 December 2012

国际检索报告

国际申请号
PCT/CN2020/070939

A. 主题的分类

G06F 17/15(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; H04L; G06Q; 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, EPODOC: 损失函数，秘密分享，取值，随机，标签，loss, share, secret, value, random, tag

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 110263294 A (阿里巴巴集团控股有限公司) 2019年 9月 20日 (2019-09-20) 权利要求1-12	1-12
A	CN 108764666 A (国网上海市电力公司 等) 2018年 11月 6日 (2018-11-06) 说明书第[0071]-[0091]段	1-12
A	CN 108418810 A (中国人民解放军国防科技大学) 2018年 8月 17日 (2018-08-17) 全文	1-12
A	US 2017300811 A1 (LINKEDIN CO.) 2017年 10月 19日 (2017-10-19) 全文	1-12
A	US 2012330867 A1 (INTERNATIONAL BUSINESS MACHINES CO.) 2012年 12月 27日 (2012-12-27) 全文	1-12

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

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

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 3月 25日	2020年 4月 8日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 张伯 电话号码 86-(10)53961391

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/070939

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	110263294	A	2019年 9月 20日	无			
CN	108764666	A	2018年 11月 6日	无			
CN	108418810	A	2018年 8月 17日	无			
US	2017300811	A1	2017年 10月 19日	无			
US	2012330867	A1	2012年 12月 27日	US	2012331025	A1	2012年 12月 27日