(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 9 月 10 日 (10.09.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/177392 A1

(51) 国际专利分类号:
G06N 20/00 (2019.01) *G06F 21/60* (2013.01)

(21) 国际申请号: PCT/CN2019/119227

(22) 国际申请日: 2019 年 11 月 18 日 (18.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910158538.8 2019年3月1日 (01.03.2019) CN

(71) 申请人: 深圳前海微众银行股份有限公司 (WEBANK CO., LTD) [CN/CN]; 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518000 (CN)。

(72) 发明人: 刘洋 (LIU, Yang); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518000 (CN)。 陈天健 (CHEN, Tianjian); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518000 (CN)。 杨强 (YANG, Qiang); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518000 (CN)。

(74) 代理人: 深圳市世纪恒程知识产权代理事务所 (CENFO INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市南山区粤海街道高新技术产业园北区松坪山路3号奥特讯电力大厦201, Guangdong 518057 (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:** FEDERATED LEARNING-BASED MODEL PARAMETER TRAINING METHOD, APPARATUS AND DEVICE, AND MEDIUM

(54) **发明名称**: 基于联邦学习的模型参数训练方法、装置、设备及介质

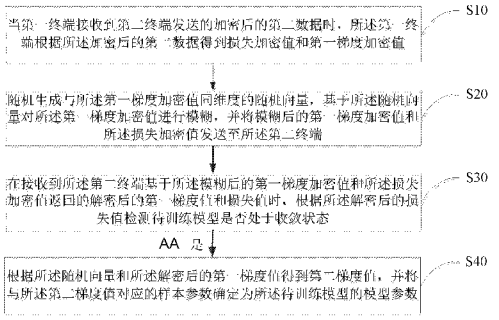


图 2

S10 When a first terminal receives encrypted second data sent by a second terminal, the first terminal obtains a loss encryption value and a first gradient encryption value according to the encrypted second data

S20 Randomly generate a random vector having the same dimension as the first gradient encryption value, perform fuzzing on the first gradient encryption value on the basis of the random vector, and send the fuzzed first gradient encryption value and the loss encryption value to the second terminal

S30 When the decrypted first gradient value and loss value returned by the second terminal on the basis of the fuzzed first gradient encryption value and the loss encryption value are received, detect whether a model to be trained is in a convergence state according to the decrypted loss value

S40 Obtain a second gradient value according to the random vector and the decrypted first gradient value, and determine a sample parameter corresponding to the second gradient value as a model parameter of the model to be trained

AA Yes

(57) **Abstract:** Disclosed in the present application are a federated learning-based model parameter training method, apparatus and device, and a medium. The method comprises: when a first terminal receives encrypted second data sent by a second terminal, obtaining a corresponding loss encryption value and a first gradient encryption value; randomly generating a random vector having the same dimension as the first gradient encryption value, performing fuzzing on the first gradient encryption value on the basis of the random vector, and sending the fuzzed first gradient encryption value and the loss encryption value to the second terminal; when the decrypted first gradient value and loss value returned by the second terminal are received, detecting whether a model to be trained is in a convergence state according to the decrypted loss value; and if yes, obtaining a second gradient value according to the random vector and the decrypted first gradient value, and determining a sample parameter corresponding to the second gradient value as a model parameter.

(57) **摘要**: 本申请公开了一种基于联邦学习的模型参数训练方法、装置、设备及介质。该方法包括: 当第一终端接收到第二终端发送的加密后的第二数据时，获取对应的损失加密值和第一梯度加密值; 随机生成与第一梯度加密值同维度的随机向量，基于随机向量对第一梯度加密值进行模糊，并将模糊后的第一梯度加密值和损失加密值发送至第二终端; 在接收到第二终端返回的解密后的第一梯度值和损失值时，根据解密后的损失值检测待训练模型是否处于收敛状态; 若是，则根据随机向量和解密后的第一梯度值得到第二梯度值，并将与第二梯度值对应的样本参数确定为模型参数。

WO 2020/177392 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))。

基于联邦学习的模型参数训练方法、装置、设备及介质

本申请要求于2019年3月1日提交中国专利局、申请号为201910158538.8、发明名称为“基于联邦学习的模型参数训练方法、装置、设备及介质”的中国专利申请的优先权，其全部内容通过引用结合在申请中。

技术领域

本申请涉及数据处理技术领域，尤其涉及一种基于联邦学习的模型参数训练方法、装置、设备及介质。

背景技术

“机器学习”是人工智能的核心研究领域之一，而如何在保护数据隐私、满足合法合规要求的前提下继续进行机器学习，是机器学习领域现在关注的一个趋势，在此背景下，人们研究提出了“联邦学习”的概念。

联邦学习利用技术算法加密建造的模型，联邦双方在不用给出己方数据的情况下，也可进行模型训练得到模型参数，联邦学习通过加密机制下的参数交换方式保护用户数据隐私，数据和模型本身不会进行传输，也不能反猜对方数据，因此在数据层面不存在泄露的可能，也不违反更严格的数据保护法案如GDPR（General Data Protection Regulation，《通用数据保护条例》）等，能够在较高程度保持数据完整性的同时，保障数据隐私。然而，目前的联邦学习技术都必须依靠可信第三方，以通过第三方来对联邦双方的数据进行聚合后建模，从而使得联邦学习在一些场景下应用有限。

发明内容

本申请的主要目的在于提供一种基于联邦学习的模型参数训练方法、装置、设备及存储介质，旨在实现无需可信第三方而仅用联邦双方数据就可以进行模型训练，以避免应用受限。

为实现上述目的，本申请提供一种基于联邦学习的模型参数训练方法，所述基于联邦学习的模型参数训练方法包括：

当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端根

据所述加密后的第二数据得到损失加密值和第一梯度加密值；

随机生成与所述第一梯度加密值同维度的随机向量，基于所述随机向量对所述第一梯度加密值进行模糊，并将模糊后的第一梯度加密值和所述损失加密值发送至所述第二终端；

在接收到所述第二终端基于所述模糊后的第一梯度加密值和所述损失加密值返回的解密后的第一梯度值和损失值时，根据所述解密后的损失值检测待训练模型是否处于收敛状态；

若检测到所述待训练模型处于收敛状态，则根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，并将与所述第二梯度值对应的样本参数确定为所述待训练模型的模型参数。

此外，为实现上述目的，本申请还提供一种基于联邦学习的模型参数训练装置，所述基于联邦学习的模型参数训练装置包括：

数据获取模块，用于当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端根据所述加密后的第二数据得到损失加密值和第一梯度加密值；

第一发送模块，用于随机生成与所述第一梯度加密值同维度的随机向量，基于所述随机向量对所述第一梯度加密值进行模糊，并将模糊后的第一梯度加密值和所述损失加密值发送至所述第二终端；

模型检测模块，用于在接收到所述第二终端基于所述模糊后的第一梯度加密值和所述损失加密值返回的解密后的第一梯度值和损失值时，根据所述解密后的损失值检测待训练模型是否处于收敛状态；

参数确定模块，用于若检测到所述待训练模型处于收敛状态，则根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，并将与所述第二梯度值对应的样本参数确定为所述待训练模型的模型参数。

此外，为实现上述目的，本申请还提供一种基于联邦学习的模型参数训练设备，所述基于联邦学习的模型参数训练设备包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被所述处理器执行时实现如上所述的基于联邦学习的模型参数训练方法的步骤。

此外，为实现上述目的，本申请还提供一种存储介质，所述存储介质上存储有基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程

序被处理器执行时实现如上所述的基于联邦学习的模型参数训练方法的步骤。

本申请提供一种基于联邦学习的模型参数训练方法、装置、设备及介质，当第一终端接收到第二终端发送的加密后的第二数据时，第一终端根据该加密后的第二数据得到损失加密值和第一梯度加密值；随机生成与该第一梯度加密值同维度的随机向量，基于该随机向量对该第一梯度加密值进行模糊，将模糊后的第一梯度加密值和该损失加密值发送至第二终端；在接收到第二终端基于该模糊后的第一梯度加密值和该损失加密值返回的解密后的第一梯度值和损失值时，根据该解密后的损失值检测待训练模型是否处于收敛状态；若检测到待训练模型处于收敛状态，第一终端则根据该随机向量和解密后的第一梯度值得到第二梯度值，即去掉该解密后的第一梯度值中的随机向量，以还原真实梯度值，得到第二梯度值，然后将与该第二梯度值对应的样本参数确定为待训练模型的模型参数。本申请仅通过第一终端和第二终端之间的数据传输与计算，最终得到损失值，进而确定待训练模型中的模型参数，可无需可靠第三方而仅用两方数据就可以进行模型训练，以避免应用受限，同时，本申请中第一终端接收到的第二数据是模型中间结果的加密数据，第一终端和第二终端通信过程中的数据通过加密和模糊处理，因此本申请不会泄露原始特征数据，可达到同样级别的安全保证，保障终端样本数据的隐私性和安全性。

附图说明

图1为本申请实施例方案涉及的硬件运行环境的设备结构示意图；

图2为本申请基于联邦学习的模型参数训练方法第一实施例的流程示意图；

图3为本申请第一实施例中步骤S10的细化流程示意图；

图4为本申请基于联邦学习的模型参数训练方法第二实施例的流程示意图；

图5为本申请基于联邦学习的模型参数训练方法第三实施例的流程示意图；

图6为本申请基于联邦学习的模型参数训练装置第一实施例的功能模块示意图。

本申请目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定

本申请。

参照图 1，图 1 为本申请实施例方案涉及的硬件运行环境的设备结构示意图。

本申请实施例基于联邦学习的模型参数训练设备可以是智能手机、PC（Personal Computer，个人计算机）、平板电脑、便携计算机和服务器等终端设备。

如图 1 所示，该基于联邦学习的模型参数训练设备可以包括：处理器 1001，例如 CPU，通信总线 1002，用户接口 1003，网络接口 1004，存储器 1005。其中，通信总线 1002 用于实现这些组件之间的连接通信。用户接口 1003 可以包括显示屏（Display）、输入单元比如键盘（Keyboard），可选用户接口 1003 还可以包括标准的有线接口、无线接口。网络接口 1004 可选的可以包括标准的有线接口、无线接口（如 Wi-Fi 接口）。存储器 1005 可以是高速 RAM 存储器，也可以是稳定的存储器（non-volatile memory），例如磁盘存储器。存储器 1005 可选的还可以是独立于前述处理器 1001 的存储装置。

本领域技术人员可以理解，图1中示出的基于联邦学习的模型参数训练设备结构并不构成对基于联邦学习的模型参数训练设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

如图1所示，作为一种计算机存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及基于联邦学习的模型参数训练程序。

在图 1 所示的终端中，网络接口 1004 主要用于连接后台服务器，与后台服务器进行数据通信；用户接口 1003 主要用于连接客户端，与客户端进行数据通信；而处理器 1001 可以用于调用存储器 1005 中存储的基于联邦学习的模型参数训练程序，并执行以下基于联邦学习的模型参数训练方法的各个步骤。

基于上述硬件结构，提出本申请基于联邦学习的模型参数训练方法的各实施例。

本申请提供一种基于联邦学习的模型参数训练方法。

参照图 2，图 2 为本申请基于联邦学习的模型参数训练方法第一实施例的流程示意图。

在本实施例中，该基于联邦学习的模型参数训练方法包括：

步骤 S10，当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端根据所述加密后的第二数据得到损失加密值和第一梯度加密值；

在本实施例中，当第一终端接收到第二终端发送的加密后的第二数据时，第一终端根据该加密后的第二数据得到损失加密值和第一梯度加密值。其中，第一终端和第二终端可以为智能手机、个人计算机、平板电脑、便携计算机和和服务器等终端设备，第二数据为第二终端根据其样本数据和对应的样本参数计算得到的，为模型中间结果，然后第二终端对第二数据进行加密，可通过密钥对生成软件生成公钥和私钥，然后采用该生成的公钥，通过同态加密算法对第二数据进行加密，得到加密后的第二数据，以保障传输数据的隐私性和安全性。此外，损失加密值和第一梯度加密值的获取方法为：当第一终端接收到第二终端发送的第二数据后，第一终端获取与该第二数据对应的第一数据，及与该第一数据对应的标本标签；然后基于第一数据、加密后的第二数据、样本标签和预设损失函数计算损失值，采用第二终端的公钥（第二终端会将其公钥发送至第一终端），通过同态加密算法加密各个计算损失值的计算因子，以得到加密后的损失值，记作损失加密值；然后根据预设损失函数得到梯度函数，并根据该梯度函数计算得到第一梯度值，并采用第二终端的公钥，通过同态加密算法加密该第一梯度值，得到加密的第一梯度值，记作第一梯度加密值。具体的获取过程可参照下述实施例，此处不作赘述。

步骤 S20，随机生成与所述第一梯度加密值同维度的随机向量，基于所述随机向量对所述第一梯度加密值进行模糊，并将模糊后的第一梯度加密值和所述损失加密值发送至所述第二终端；

第一终端在得到损失加密值和第一梯度加密值后，随机生成与该第一梯度加密值同维度的随机向量，基于该随机向量对该第一梯度加密值进行模糊，即若第一梯度加密值为[[g]]，随机向量为 R，则模糊后的第一梯度加密值为[[g+R]]，然后将模糊后的第一梯度加密值和该损失加密值发送至第二终端。对应的，第二终端在接收到该第一梯度加密值和损失加密值时，通过第二终端的私钥对该第一梯度加密值和损失加密值进行解密，得到解密后的第一梯度值和损失值。

步骤 S30，在接收到所述第二终端基于所述模糊后的第一梯度加密值和所述损失加密值返回的解密后的第一梯度值和损失值时，根据所述解密后的损失值检测待训练模型是否处于收敛状态；

第一终端在接收到第二终端基于该模糊后的第一梯度加密值和该损失加密值返回的解密后的第一梯度值和损失值时，根据该解密后的损失值检测待训

练模型是否处于收敛状态。具体的，步骤“根据所述解密后的损失值检测待训练模型是否处于收敛状态”包括：

步骤 a1，获取所述第一终端前一次获取到的第一损失值，并将所述解密后的损失值记作第二损失值；

当第一终端得到解密后的损失值后，第一终端获取第一终端前一次获取到的第一损失值，并将解密后的损失值记为第二损失值。需要说明的是，当待训练模型未处于收敛状态时，第一终端会持续根据第二终端发送的加密后的第二数据得到损失加密值，然后将损失加密值发送给第二终端进行解密，进而接收第二终端返回的解密后的损失值，直到待训练模型处于收敛状态。第一损失值也是第二终端解密后的损失值。可以理解的是，第一损失值是第二终端前一次发送的解密后的损失值，第二损失值是第二终端当前发送的解密后的损失值。

步骤 a2，计算所述第一损失值与所述第二损失值之间的差值，并判断所述差值是否小于或者等于预设阈值；

当第一终端获取到第一损失值和第二损失值后，第一终端计算第一损失值与第二损失值之间的差值，并判断该差值是否小于或者等于预设阈值。其中，该预设阈值的具体数值可预先根据具体需要进行设置，在本实施例中对预设阈值对应的数值不做具体限制。

步骤 a3，当所述差值小于或者等于预设阈值时，则判定所述待训练模型处于收敛状态；

步骤 a4，当所述差值大于预设阈值时，则判定所述待训练模型未处于收敛状态。

当该差值小于或者等于预设阈值时，第一终端则判定待训练模型处于收敛状态；当确定该差值大于预设阈值时，第一终端则判定待训练模型未处于收敛状态。

步骤 S40，若检测到所述待训练模型处于收敛状态，则根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，并将与所述第二梯度值对应的样本参数确定为所述待训练模型的模型参数。

若检测到待训练模型处于收敛状态，第一终端则根据该随机向量和解密后的第一梯度值得到第二梯度值，即去掉该解密后的第一梯度值中的随机向量，以还原真实梯度值，得到第二梯度值，然后将与该第二梯度值对应的样本参数确定为该待训练模型的模型参数。

本申请实施例提供一种基于联邦学习的模型参数训练方法，当第一终端接收到第二终端发送的加密后的第二数据时，第一终端根据该加密后的第二数据得到损失加密值和第一梯度加密值；随机生成与该第一梯度加密值同维度的随机向量，基于该随机向量对该第一梯度加密值进行模糊，将模糊后的第一梯度加密值和该损失加密值发送至第二终端；在接收到第二终端基于该模糊后的第一梯度加密值和该损失加密值返回的解密后的第一梯度值和损失值时，根据该解密后的损失值检测待训练模型是否处于收敛状态；若检测到待训练模型处于收敛状态，第一终端则根据该随机向量和解密后的第一梯度值得到第二梯度值，即去掉该解密后的第一梯度值中的随机向量，以还原真实梯度值，得到第二梯度值，然后将与该第二梯度值对应的样本参数确定为待训练模型的模型参数。本申请仅通过第一终端和第二终端之间的数据传输与计算，最终得到损失值，进而确定待训练模型中的模型参数，可无需可靠第三方而仅用两方数据就可以进行模型训练，以避免应用受限，同时，本申请中第一终端接收到的第二数据是模型中间结果的加密数据，第一终端和第二终端通信过程中的数据通过加密和模糊处理，因此本申请不会泄露原始特征数据，可达到同样级别的安全保证，保障终端样本数据的隐私性和安全性。

进一步的，参照图 3，图 3 为本申请第一实施例中步骤 S10 的细化流程示例图。

具体的，步骤 S10 包括：

步骤 S11，当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端获取对应的第一数据，及与所述第一数据对应的样本标签；

在本实施例中，当第一终端接收到第二终端发送的第二数据后，第一终端获取对应的第一数据，及与该第一数据对应的标本标签。其中，第一数据和第二数据均为模型中间结果，第一数据是第一终端根据其样本数据和对应的样本参数计算得到的，第二数据是第二终端根据其样本数据和对应的样本参数计算得到的。具体的，第二数据可以为第二终端中样本参数与第二终端交集样本数据中特征变量对应变量值乘积之和，以及该乘积之和的平方。原始第二数据对应的计算公式可以为：$u_A = w_A^T x_A = w_1 x_{i1} + w_2 x_{i2} \cdots w_n x_{in}$，乘积之和的平方表示为：$u_A^2$，其中，$w_1, w_2 \cdots w_n$ 表示第二终端对应的样本参数，第二终端中特征变量对应变量值的个数与第二终端对应样本参数的个数相等，即一个变量值对应一个样本参数，x 表示特征变量的特征值，1,2…n 表示对应变量值和样本参数

的个数。如当第二终端交集样本数据中的每个特征变量存在三个变量值，则 $u_A = w_A^T x_A = w_1 x_{i1} + w_2 x_{i2} + w_3 x_{i3}$。需要说明的是，第二终端发送给第一终端的第二数据是加密后的第二数据，当第二终端计算得到第二数据后，采用第二终端的公钥，通过同态加密算法加密第二数据，得到加密后的第二数据，并将加密后的第一数据发送给第二终端。其中，发送给第一终端的第二数据，即加密后的第二数据可表示为$[[u_A]]$和$[[u_A^2]]$。

第一终端计算第一数据的过程与第二终端计算第二数据的过程类似，如计算第一终端中样本参数与第一终端交集样本数据中特征变量对应变量值乘积之和的公式为：$u_B = w_B^T x_B = w_1 x_{i1} + w_2 x_{i2} \cdots w_n x_{in}$，其中，$w_1, w_2 \cdots w_n$表示第一终端中各个样本数据特征变量对应特征值的样本参数。

步骤S12，基于所述第一数据、所述加密后的第二数据、所述样本标签和预设损失函数计算损失值，并采用同态加密算法加密所述损失值，得到加密的损失值，记作损失加密值；

第一终端在接收到加密后的第二数据，并获取到对应的第一数据及其对应的样本标签后，基于第一数据、加密后的第二数据、样本标签和预设损失函数计算损失值，并采用同态加密算法加密所述损失值，得到加密的损失值，记作损失加密值。

具体的，将损失值表示为$loss$，$loss = \log 2 - \frac{1}{2} y w^T x + \frac{1}{8}(w^T x)^2$，其中，$u = w^T x = w_A^T x_A + w_B^T x_B$，$(w^T x)^2 = u^2 = (u_A + u_B)^2 = u_A^2 + u_B^2 + 2u_A u_B$，y表示第一数据对应样本标签的标签值，样本标签对应的标签值的数值可根据具体需要而设置，如在本实施例中，如可用“0”和“1”表示不同样本标签对应的标签值。当第一终端计算得到损失值后，第一终端采用第二终端的公钥（第二终端会将其公钥发送至第一终端），通过同态加密算法加密各个计算损失值的计算因子，以得到加密后的损失值。将加密后的损失值（即损失加密值）表示为$[[loss]]$，$\log 2$、$yw^T x$和$(w^T x)^2$为计算损失值的计算因子，$[[loss]] = [[\log 2]] + \left(-\frac{1}{2}\right) * [[yw^T x]] + \frac{1}{8}[[(w^T x)^2]]$，其中，$[[u]] = [[u_A + u_B]] = [[u_A]] + [[u_B]]$，$[[(w^T x)^2]] = [[(u)^2]] = [[u_A{}^2]] + [[u_B{}^2]] + [[2u_A u_B]] = [[u_A{}^2]] + [[u_B{}^2]] + 2u_B[[u_A]]$。

步骤S13，根据所述预设损失函数得到梯度函数，并根据所述梯度函数计算得到第一梯度值，并采用同态加密算法加密所述第一梯度值，得到加密的第一梯度值，记作第一梯度加密值。

然后根据预设损失函数得到梯度函数，并根据该梯度函数计算得到第一梯度值，并采用第二终端的公钥，通过同态加密算法加密该第一梯度值，得到加密的第一梯度值，记作第一梯度加密值。

具体的，第一终端计算其对应梯度值（即第一梯度值）的公式为：$g=\sum\left(\frac{1}{2}yw^{T}x-1\right)\frac{1}{2}yx$，在计算得到第一梯度值后，第一终端采用其第二终端的公钥，通过同态加密算法对该第一梯度值进行加密，以得到加密后的损失值（即第一梯度加密值），对应的，第一梯度加密值的公式为：$[[g]]=\sum[[d]]x$，其中，$[[d]]=\left[\left[\left(\frac{1}{2}yw^{T}x-1\right)\frac{1}{2}y\right]\right]=\left(\frac{1}{2}[[yw^{T}x]]+[[-1]]\right)\frac{1}{2}y$。

需要说明的是，在本实施例中，采用参数服务器的方式，第一终端和第二终端都拥有独立的参数服务器，用于各自样本数据的聚合更新同步，同时避免各自样本数据的泄露，且第一终端和第二终端对应的样本参数，即模型参数都是各自存储的，提高了第一终端和第二终端数据的安全性。

本实施例通过根据接收到的来源于第二终端的加密后的第二数据、第一终端的第一数据以及第一数据对应的样本标签计算损失值，并采用同态加密算法加密对损失值进行加密，得到损失加密值，使第一终端在计算损失值过程中，并不能获取第二终端的具体样本数据，实现了第一终端在联合第二终端样本数据计算模型参数过程中，可在不暴露第二终端样本数据的基础上计算出计算模型参数所需的损失值，提高了计算模型参数过程中第二终端样本数据的隐私性。

基于上述各实施方式，提出本申请基于联邦学习的模型参数训练方法的第二实施例。

参照图 4，在本实施例中，所述基于联邦学习的模型参数训练方法还包括：

步骤 S50，根据所述加密后的第二数据和所述第一数据计算得到加密中间结果，通过预设公钥对所述加密中间结果进行加密，得到双重加密中间结果；

作为第二终端的梯度值的其中一种获取方式，在本实施例中，第一终端可根据加密后的第二数据和上述获取到的第一数据计算得到加密中间结果，然后通过预设公钥对该加密中间结果进行加密，得到双重加密中间结果。其中，该预设公钥是第一终端根据密钥对生成软件生成的公钥，是第一终端的公钥。

步骤 S60，将所述双重加密中间结果发送至所述第二终端，以使得所述第二终端基于所述双重加密中间结果计算得到双重加密梯度值；

然后，将该双重加密中间结果发送至第二终端，以使得第二终端基于该双

重加密中间结果计算得到双重加密梯度值，进而第二终端将该双重加密梯度值发送至第一终端。

步骤 S70，在接收到所述第二终端返回的所述双重加密梯度值时，通过与所述预设公钥对应的私钥对所述双重加密梯度值进行解密，并将解密后的双重加密梯度值发送至所述第二终端，以使得所述第二终端对所述解密后的双重加密梯度值进行解密，得到所述第二终端的梯度值。

第一终端在接收到第二终端返回的双重加密梯度值时，通过与该预设公钥对应的私钥（即第一终端的私钥）对双重加密梯度值进行一次解密，并将解密后的双重加密梯度值发送至第二终端，以使得第二终端采用其私钥（即第二终端的私钥）对该解密后的双重加密梯度值进行二次解密，得到第二终端的梯度值，进而第二终端可根据该第二终端的梯度值来更新模型参数。

在本实施例中，第一终端和第二终端两方进行通信的第一数据和第二数据都是模型中间结果的加密数据，不存在泄露原始特征数据，且其他数据传输过程中也进行了加密，可在保障终端数据隐私性和安全性的同时，对第二终端的模型参数进行训练，确定第二终端的模型参数。

基于上述各实施方式，提出本申请基于联邦学习的模型参数训练方法的第三实施例。

参照图 5，在本实施例中，所述基于联邦学习的模型参数训练方法还包括：

步骤 S80，接收所述第二终端发送的加密样本数据，根据所述加密样本数据和所述第一数据得到所述第二终端的第一部分梯度值，并采用同态加密算法加密所述第一部分梯度值，得到加密的第一部分梯度值，记作第二梯度加密值；

作为第二终端的梯度值的又一种获取方式，在本实施例中，第二终端可以发送加密样本数据至第一终端，使得第一终端根据该加密样本数据计算第二终端的部分梯度值。具体的，第一终端接收第二终端发送的加密样本数据，然后根据加密样本数据和上述根据加密后的第二数据获取到的第一数据，得到第二终端的第一部分梯度值，并采用第二终端的公钥通过同态加密算法加密该第一部分梯度值，得到加密的第一部分梯度值，将其记作第二梯度加密值。

步骤 S90，将所述第二梯度加密值发送至所述第二终端，以使得所述第二终端基于所述第二梯度加密值和根据所述第二数据计算得到的第二部分梯度值，得到所述第二终端的梯度值。

然后，将该第二梯度加密值发送至第二终端，以使得第二终端基于该第二

梯度加密值和根据第二数据计算得到的第二部分梯度值，得到第二终端的梯度值。具体的，第二终端根据第二数据计算得到的第二部分梯度值，同时对接收到的第二梯度加密值进行解密，得到第一部分梯度值，然后，将第一部分梯度值和第二部分梯度值这两部分梯度值结合可得到该第二终端的梯度值，进而第二终端可根据该第二终端的梯度值来更新模型参数。

在本实施例中，第一终端通过接收到的第二终端发送的加密样本数据，得到第二终端梯度的一部分（即第一部分梯度值），然后将加密后的第一部分梯度值（即第二梯度加密值）发送至第二终端，使得第二终端解密后，得到第一部分梯度值，进而结合该第一部分梯度值和第二部分梯度值（第二终端本地计算得到的）这两部分梯度值，得到该第二终端的梯度值，进而根据该第二终端的梯度值来更新模型参数。通过上述方式，本实施例对第二终端的模型参数进行训练，确定出第二终端的模型参数，同时，由于第一终端和第二终端两方进行通信的数据均进行了加密，可保障终端数据的隐私性和安全性。

此外，需要说明的是，作为第二终端的梯度值的另一种获取方式，可采用与第一实施例中相同的方法来计算第二终端的梯度值。具体的，第一终端将加密后的第一数据发送到第二终端，第二终端在接收到第一终端发送的加密后的第一数据时，第二终端根据该加密后的第一数据得到第二终端的损失加密值和梯度加密值；随机生成与该第二终端的梯度加密值同维度的随机向量，基于该随机向量对该第二终端的梯度加密值进行模糊，将模糊后的第二终端的梯度加密值和该第二终端的损失加密值发送至第一终端；在接收到第一终端基于该模糊后的第二终端的梯度加密值和该第二终端的损失加密值返回的解密后的第二终端的梯度值和损失值时，根据该解密后的第二终端的损失值检测待训练模型是否处于收敛状态；若检测到待训练模型处于收敛状态，第二终端则根据该随机向量和解密后的第二终端的梯度值得到第二终端的梯度值，即去掉该解密后的第二终端的梯度值中的随机向量，以还原真实梯度值，得到第二终端的梯度值，然后将与该第二终端的梯度值对应的样本参数确定为待训练模型的模型参数。此过程与上述第一实施例中基本相似，可参照上述第一实施例，此处不作赘述。

进一步的，基于上述各实施方式，提出本申请基于联邦学习的模型参数训练方法的第四实施例。在本实施例中，在步骤S30之后，所述基于联邦学习的

模型参数训练方法还包括：

若检测到所述待训练模型未处于收敛状态，则执行步骤A：根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，更新所述第二梯度值，并根据更新后的第二梯度值，对应更新样本参数；

在本实施例中，若检测到待训练模型未处于收敛状态，即差值大于预设阈值时，第一终端则根据该随机向量和解密后的第一梯度值得到第二梯度值，即去掉该解密后的第一梯度值中的随机向量，以还原真实梯度值，得到第二梯度值，进而更新第二梯度值，并根据更新后的第二梯度值，对应更新样本参数。

其中，样本参数的更新方法为：计算更新后的第二梯度值与预设系数之间的乘积，将样本参数减去该乘积，以得到更新后的样本参数。具体的，第一终端根据更新后的梯度值更新其对应样本参数所用公式为：$w=w_0-\eta g$，其中，w表示更新后的样本参数，w_0表示更新前的样本参数；η为一个系数，是预先设置好的，即预设系数，其对应的数值可根据具体需要而设置；g为更新后的梯度值。

步骤B，生成对应的梯度值更新指令，并发送至所述第二终端，以使得所述第二终端根据所述梯度值更新指令更新所述第二终端的梯度值，并根据更新后的第二终端的梯度值更新对应的样本参数。

第一终端生成对应的梯度值更新指令，并发送至第二终端，以使得第二终端根据该梯度值更新指令更新第二终端的梯度值，并根据更新后的第二终端的梯度值更新对应的样本参数。其中，第二终端的样本参数的更新方法与第一终端梯度值的更新方法基本相同，此处不作赘述。

需要说明的是，步骤B与步骤A的执行顺序不分先后。

进一步的，基于上述各实施方式，提出本申请基于联邦学习的模型参数训练方法的第五实施例。在本实施例中，在步骤S30之后，所述基于联邦学习的模型参数训练方法还包括：

步骤C，当所述第一终端确定模型参数，且接收到执行请求后，所述第一终端将所述执行请求发送给所述第二终端，以使得所述第二终端在接收到所述执行请求后，根据对应的模型参数和与所述执行请求对应特征变量的变量值返回第一预测分数给所述第一终端；

在本实施例中，当第一终端确定模型参数后，第一终端检测是否接收到执行请求。当第一终端接收到执行请求后，第一终端将该执行请求发送给第二终

端。当第二终端接收到执行请求后，第二终端获取其对应的模型参数，以及获取与该执行请求对应特征变量的变量值，并根据该模型参数和变量值计算得到第一预测分数，并将该第一预测分数发送给第一终端。可以理解的是，第一终端计算第一预测分数的公式为：$w_A^T x_A = w_1 x_{i1} + w_2 x_{i2} \cdots w_n x_{in}$。

步骤D，当接收到所述第一预测分数后，根据确定的所述模型参数和与所述执行请求对应特征变量的变量值，计算第二预测分数；

当第一终端接收到第二终端发送的第一预测分数后，第一终端根据其所确定的模型参数和与该执行请求对应特征变量的变量值计算第二预测分数。其中，第一终端计算第二预测分数的公式为：$w_B^T x_B = w_1 x_{i1} + w_2 x_{i2} \cdots w_n x_{in}$。

步骤E，将所述第一预测分数和所述第二预测分数相加，得到预测分数总和，并根据所述预测分数总和输入所述待训练模型中，得到模型分数，并根据所述模型分数确定是否执行所述执行请求。

当第一终端得到第一预测分数和第二预测分数后，第一终端将第一预测分数和第二预测分数相加，得到预测分数总和，并将该预测分数总和输入待训练模型中，得到模型分数。其中，预测分数总和的表达式为：$w^T x = w_A^T x_A + w_B^T x_B$，待训练模型的表达式为：

$$P(y=1|x) = \frac{1}{1+\exp(-w^T x)}。$$

当得到模型分数后，第一终端可根据该模型分数判断是否执行该执行请求。如当该待训练模型为欺诈模型，该执行请求为贷款请求时，若计算所得的模型分数大于或者等于预设分数，第一终端则确定该贷款请求为欺诈请求，拒绝执行该贷款请求；若计算所得的模型分数小于预设分数，第一终端则确定该贷款请求为真实的贷款请求，执行该贷款请求。

本实施例通过第一终端接收到执行请求后，通过待训练模型分析该执行请求，以确定是否执行该执行请求，提高了第一终端执行请求过程中的安全性。

本申请还提供一种基于联邦学习的模型参数训练装置。

参照图6，图6为本申请基于联邦学习的模型参数训练装置第一实施例的功能模块示意图。

所述基于联邦学习的模型参数训练装置包括：

数据获取模块10，用于当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端根据所述加密后的第二数据得到损失加密值和第一梯度加密值；

第一发送模块20，用于随机生成与所述第一梯度加密值同维度的随机向量，基于所述随机向量对所述第一梯度加密值进行模糊，并将模糊后的第一梯度加密值和所述损失加密值发送至所述第二终端；

模型检测模块30，用于在接收到所述第二终端基于所述模糊后的第一梯度加密值和所述损失加密值返回的解密后的第一梯度值和损失值时，根据所述解密后的损失值检测待训练模型是否处于收敛状态；

参数确定模块40，用于若检测到所述待训练模型处于收敛状态，则根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，并将与所述第二梯度值对应的样本参数确定为所述待训练模型的模型参数。

进一步的，所述数据获取模块10包括：

第一获取单元，用于当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端获取对应的第一数据，及与所述第一数据对应的样本标签；

第一加密单元，用于基于所述第一数据、所述加密后的第二数据、所述样本标签和预设损失函数计算损失值，并采用同态加密算法加密所述损失值，得到加密的损失值，记作损失加密值；

第二加密单元，用于根据所述预设损失函数得到梯度函数，并根据所述梯度函数计算得到第一梯度值，并采用同态加密算法加密所述第一梯度值，得到加密的第一梯度值，记作第一梯度加密值。

进一步的，所述基于联邦学习的模型参数训练装置还包括：

第一加密模块，用于根据所述加密后的第二数据和所述第一数据计算得到加密中间结果，通过预设公钥对所述加密中间结果进行加密，得到双重加密中间结果；

第一计算模块，用于将所述双重加密中间结果发送至所述第二终端，以使得所述第二终端基于所述双重加密中间结果计算得到双重加密梯度值；

第二解密模块，用于在接收到所述第二终端返回的所述双重加密梯度值时，通过与所述预设公钥对应的私钥对所述双重加密梯度值进行解密，并将解密后的双重加密梯度值发送至所述第二终端，以使得所述第二终端对所述解密后的双重加密梯度值进行解密，得到所述第二终端的梯度值。

进一步的，所述基于联邦学习的模型参数训练装置还包括：

第二加密模块，用于接收所述第二终端发送的加密样本数据，根据所述加密样本数据和所述第一数据得到所述第二终端的第一部分梯度值，并采用同态

加密算法加密所述第一部分梯度值，得到加密的第一部分梯度值，记作第二梯度加密值；

第二发送模块，用于将所述第二梯度加密值发送至所述第二终端，以使得所述第二终端基于所述第二梯度加密值和根据所述第二数据计算得到的第二部分梯度值，得到所述第二终端的梯度值。

进一步的，所述基于联邦学习的模型参数训练装置还包括：

参数更新模块，用于若检测到所述待训练模型未处于收敛状态，则根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，更新所述第二梯度值，并根据更新后的第二梯度值，对应更新样本参数；

指令发送模块，用于生成对应的梯度值更新指令，并发送至所述第二终端，以使得所述第二终端根据所述梯度值更新指令更新所述第二终端的梯度值，并根据更新后的第二终端的梯度值更新对应的样本参数。

进一步的，所述基于联邦学习的模型参数训练装置还包括：

第三发送模块，用于当所述第一终端确定模型参数，且接收到执行请求后，所述第一终端将所述执行请求发送给所述第二终端，以使得所述第二终端在接收到所述执行请求后，根据对应的模型参数和与所述执行请求对应特征变量的变量值返回第一预测分数给所述第一终端；

第二计算模块，用于当接收到所述第一预测分数后，根据确定的所述模型参数和与所述执行请求对应特征变量的变量值，计算第二预测分数；

分数获取模块，用于将所述第一预测分数和所述第二预测分数相加，得到预测分数总和，并根据所述预测分数总和输入所述待训练模型中，得到模型分数，并根据所述模型分数确定是否执行所述执行请求。

进一步的，所述模型检测模块 30 包括：

第二获取单元，用于获取所述第一终端前一次获取到的第一损失值，并将所述解密后的损失值记作第二损失值；

差值判断单元，用于计算所述第一损失值与所述第二损失值之间的差值，并判断所述差值是否小于或者等于预设阈值；

第一判定单元，用于当所述差值小于或者等于预设阈值时，则判定所述待训练模型处于收敛状态；

第二判定单元，用于当所述差值大于预设阈值时，则判定所述待训练模型未处于收敛状态。

其中，上述基于联邦学习的模型参数训练装置中各个模块的功能实现与上述基于联邦学习的模型参数训练方法实施例中各步骤相对应，其功能和实现过程在此处不再一一赘述。

本申请还提供一种存储介质，该存储介质上存储有基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被处理器执行时实现如以上任一项实施例所述的基于联邦学习的模型参数训练方法的步骤。

本申请存储介质的具体实施例与上述基于联邦学习的模型参数训练方法各实施例基本相同，在此不作赘述。

需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请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，该计算机软件产品存储在如上所述的一个存储介质(如 ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本申请各个实施例所述的方法。

以上仅为本申请的优选实施例，并非因此限制本申请的专利范围，凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本申请的专利保护范围内。

权 利 要 求 书

1、一种基于联邦学习的模型参数训练方法，其中，所述基于联邦学习的模型参数训练方法包括：

当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端根据所述加密后的第二数据得到损失加密值和第一梯度加密值；

随机生成与所述第一梯度加密值同维度的随机向量，基于所述随机向量对所述第一梯度加密值进行模糊，并将模糊后的第一梯度加密值和所述损失加密值发送至所述第二终端；

在接收到所述第二终端基于所述模糊后的第一梯度加密值和所述损失加密值返回的解密后的第一梯度值和损失值时，根据所述解密后的损失值检测待训练模型是否处于收敛状态；

若检测到所述待训练模型处于收敛状态，则根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，并将与所述第二梯度值对应的样本参数确定为所述待训练模型的模型参数。

2、如权利要求 1 所述的基于联邦学习的模型参数训练方法，其中，所述当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端根据所述加密后的第二数据得到损失加密值和第一梯度加密值的步骤包括：

当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端获取对应的第一数据，及与所述第一数据对应的样本标签；

基于所述第一数据、所述加密后的第二数据、所述样本标签和预设损失函数计算损失值，并采用同态加密算法加密所述损失值，得到加密的损失值，记作损失加密值；

根据所述预设损失函数得到梯度函数，并根据所述梯度函数计算得到第一梯度值，并采用同态加密算法加密所述第一梯度值，得到加密的第一梯度值，记作第一梯度加密值。

3、如权利要求 2 所述的基于联邦学习的模型参数训练方法，其中，所述基于联邦学习的模型参数训练方法还包括：

根据所述加密后的第二数据和所述第一数据计算得到加密中间结果，通过预设公钥对所述加密中间结果进行加密，得到双重加密中间结果；

将所述双重加密中间结果发送至所述第二终端，以使得所述第二终端基于所述双重加密中间结果计算得到双重加密梯度值；

在接收到所述第二终端返回的所述双重加密梯度值时，通过与所述预设公钥对应的私钥对所述双重加密梯度值进行解密，并将解密后的双重加密梯度值发送至所述第二终端，以使得所述第二终端对所述解密后的双重加密梯度值进行解密，得到所述第二终端的梯度值。

4、如权利要求 2 所述的基于联邦学习的模型参数训练方法，其中，所述基于联邦学习的模型参数训练方法还包括：

接收所述第二终端发送的加密样本数据，根据所述加密样本数据和所述第一数据得到所述第二终端的第一部分梯度值，并采用同态加密算法加密所述第一部分梯度值，得到加密的第一部分梯度值，记作第二梯度加密值；

将所述第二梯度加密值发送至所述第二终端，以使得所述第二终端基于所述第二梯度加密值和根据所述第二数据计算得到的第二部分梯度值，得到所述第二终端的梯度值。

5、如权利要求 3 所述的基于联邦学习的模型参数训练方法，其中，所述根据所述解密后的损失值检测待训练模型是否处于收敛状态的步骤之后，还包括：

若检测到所述待训练模型未处于收敛状态，则根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，更新所述第二梯度值，并根据更新后的第二梯度值，对应更新样本参数；

生成对应的梯度值更新指令，并发送至所述第二终端，以使得所述第二终端根据所述梯度值更新指令更新所述第二终端的梯度值，并根据更新后的第二终端的梯度值更新对应的样本参数。

6、如权利要求 1 所述的基于联邦学习的模型参数训练方法，其中，所述根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，并将与所述第二梯度值对应的样本参数确定为所述待训练模型的模型参数的步骤之后，还包括：

当所述第一终端确定模型参数，且接收到执行请求后，所述第一终端将所述执行请求发送给所述第二终端，以使得所述第二终端在接收到所述执行请求后，根据对应的模型参数和与所述执行请求对应特征变量的变量值返回第一预测分数给所述第一终端；

当接收到所述第一预测分数后，根据确定的所述模型参数和与所述执行请求对应特征变量的变量值，计算第二预测分数；

将所述第一预测分数和所述第二预测分数相加，得到预测分数总和，并根据所述预测分数总和输入所述待训练模型中，得到模型分数，并根据所述模型分数确定是否执行所述执行请求。

7、如权利要求 1 所述的基于联邦学习的模型参数训练方法，其中，所述根据所述解密后的损失值检测待训练模型是否处于收敛状态的步骤包括：

获取所述第一终端前一次获取到的第一损失值，并将所述解密后的损失值记作第二损失值；

计算所述第一损失值与所述第二损失值之间的差值，并判断所述差值是否小于或者等于预设阈值；

当所述差值小于或者等于预设阈值时，则判定所述待训练模型处于收敛状态；

当所述差值大于预设阈值时，则判定所述待训练模型未处于收敛状态。

8、一种基于联邦学习的模型参数训练装置，其中，所述基于联邦学习的模型参数训练装置包括：

数据获取模块，用于当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端根据所述加密后的第二数据得到损失加密值和第一梯度加密值；

第一发送模块，用于随机生成与所述第一梯度加密值同维度的随机向量，基于所述随机向量对所述第一梯度加密值进行模糊，并将模糊后的第一梯度加密值和所述损失加密值发送至所述第二终端；

模型检测模块，用于在接收到所述第二终端基于所述模糊后的第一梯度加密值和所述损失加密值返回的解密后的第一梯度值和损失值时，根据所述解密后的损失值检测待训练模型是否处于收敛状态；

参数确定模块，用于若检测到所述待训练模型处于收敛状态，则根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，并将与所述第二梯度值对应的样本参数确定为所述待训练模型的模型参数。

9、如权利要求 8 所述的基于联邦学习的模型参数训练装置，其中，所述数据获取模块包括：

第一获取单元，用于当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端获取对应的第一数据，及与所述第一数据对应的样本标签；

第一加密单元，用于基于所述第一数据、所述加密后的第二数据、所述样

本标签和预设损失函数计算损失值，并采用同态加密算法加密所述损失值，得到加密的损失值，记作损失加密值；

第二加密单元，用于根据所述预设损失函数得到梯度函数，并根据所述梯度函数计算得到第一梯度值，并采用同态加密算法加密所述第一梯度值，得到加密的第一梯度值，记作第一梯度加密值。

10、如权利要求 9 所述的基于联邦学习的模型参数训练装置，其中，所述基于联邦学习的模型参数训练装置还包括：

第一加密模块，用于根据所述加密后的第二数据和所述第一数据计算得到加密中间结果，通过预设公钥对所述加密中间结果进行加密，得到双重加密中间结果；

第一计算模块，用于将所述双重加密中间结果发送至所述第二终端，以使得所述第二终端基于所述双重加密中间结果计算得到双重加密梯度值；

第二解密模块，用于在接收到所述第二终端返回的所述双重加密梯度值时，通过与所述预设公钥对应的私钥对所述双重加密梯度值进行解密，并将解密后的双重加密梯度值发送至所述第二终端，以使得所述第二终端对所述解密后的双重加密梯度值进行解密，得到所述第二终端的梯度值。

11、如权利要求 9 所述的基于联邦学习的模型参数训练装置，其中，所述基于联邦学习的模型参数训练装置还包括：

第二加密模块，用于接收所述第二终端发送的加密样本数据，根据所述加密样本数据和所述第一数据得到所述第二终端的第一部分梯度值，并采用同态加密算法加密所述第一部分梯度值，得到加密的第一部分梯度值，记作第二梯度加密值；

第二发送模块，用于将所述第二梯度加密值发送至所述第二终端，以使得所述第二终端基于所述第二梯度加密值和根据所述第二数据计算得到的第二部分梯度值，得到所述第二终端的梯度值。

12、如权利要求 10 所述的基于联邦学习的模型参数训练装置，其中，所述基于联邦学习的模型参数训练装置还包括：

参数更新模块，用于若检测到所述待训练模型未处于收敛状态，则根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，更新所述第二梯度值，并根据更新后的第二梯度值，对应更新样本参数；

指令发送模块，用于生成对应的梯度值更新指令，并发送至所述第二终端，

以使得所述第二终端根据所述梯度值更新指令更新所述第二终端的梯度值，并根据更新后的第二终端的梯度值更新对应的样本参数。

13、如权利要求 8 所述的基于联邦学习的模型参数训练装置，其中，所述基于联邦学习的模型参数训练装置还包括：

第三发送模块，用于当所述第一终端确定模型参数，且接收到执行请求后，所述第一终端将所述执行请求发送给所述第二终端，以使得所述第二终端在接收到所述执行请求后，根据对应的模型参数和与所述执行请求对应特征变量的变量值返回第一预测分数给所述第一终端；

第二计算模块，用于当接收到所述第一预测分数后，根据确定的所述模型参数和与所述执行请求对应特征变量的变量值，计算第二预测分数；

分数获取模块，用于将所述第一预测分数和所述第二预测分数相加，得到预测分数总和，并根据所述预测分数总和输入所述待训练模型中，得到模型分数，并根据所述模型分数确定是否执行所述执行请求。

14、如权利要求 8 所述的基于联邦学习的模型参数训练装置，其中，所述模型检测模块包括：

第二获取单元，用于获取所述第一终端前一次获取到的第一损失值，并将所述解密后的损失值记作第二损失值；

差值判断单元，用于计算所述第一损失值与所述第二损失值之间的差值，并判断所述差值是否小于或者等于预设阈值；

第一判定单元，用于当所述差值小于或者等于预设阈值时，则判定所述待训练模型处于收敛状态；

第二判定单元，用于当所述差值大于预设阈值时，则判定所述待训练模型未处于收敛状态。

15、一种基于联邦学习的模型参数训练设备，其中，所述基于联邦学习的模型参数训练设备包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被所述处理器执行时实现如下步骤：

当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端根据所述加密后的第二数据得到损失加密值和第一梯度加密值；

随机生成与所述第一梯度加密值同维度的随机向量，基于所述随机向量对

所述第一梯度加密值进行模糊，并将模糊后的第一梯度加密值和所述损失加密值发送至所述第二终端；

在接收到所述第二终端基于所述模糊后的第一梯度加密值和所述损失加密值返回的解密后的第一梯度值和损失值时，根据所述解密后的损失值检测待训练模型是否处于收敛状态；

若检测到所述待训练模型处于收敛状态，则根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，并将与所述第二梯度值对应的样本参数确定为所述待训练模型的模型参数。

16、如权利要求 15 所述的基于联邦学习的模型参数训练设备，其中，所述基于联邦学习的模型参数训练程序被所述处理器执行时还实现如下步骤：

当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端获取对应的第一数据，及与所述第一数据对应的样本标签；

基于所述第一数据、所述加密后的第二数据、所述样本标签和预设损失函数计算损失值，并采用同态加密算法加密所述损失值，得到加密的损失值，记作损失加密值；

根据所述预设损失函数得到梯度函数，并根据所述梯度函数计算得到第一梯度值，并采用同态加密算法加密所述第一梯度值，得到加密的第一梯度值，记作第一梯度加密值。

17、如权利要求 16 所述的基于联邦学习的模型参数训练设备，其中，所述基于联邦学习的模型参数训练程序被所述处理器执行时还实现如下步骤：

根据所述加密后的第二数据和所述第一数据计算得到加密中间结果，通过预设公钥对所述加密中间结果进行加密，得到双重加密中间结果；

将所述双重加密中间结果发送至所述第二终端，以使得所述第二终端基于所述双重加密中间结果计算得到双重加密梯度值；

在接收到所述第二终端返回的所述双重加密梯度值时，通过与所述预设公钥对应的私钥对所述双重加密梯度值进行解密，并将解密后的双重加密梯度值发送至所述第二终端，以使得所述第二终端对所述解密后的双重加密梯度值进行解密，得到所述第二终端的梯度值。

18、一种存储介质，其中，所述存储介质上存储有基于联邦学习的模型参数训练程序，所述基于联邦学习的模型参数训练程序被处理器执行时实现如下步骤：

当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端根据所述加密后的第二数据得到损失加密值和第一梯度加密值；

随机生成与所述第一梯度加密值同维度的随机向量，基于所述随机向量对所述第一梯度加密值进行模糊，并将模糊后的第一梯度加密值和所述损失加密值发送至所述第二终端；

在接收到所述第二终端基于所述模糊后的第一梯度加密值和所述损失加密值返回的解密后的第一梯度值和损失值时，根据所述解密后的损失值检测待训练模型是否处于收敛状态；

若检测到所述待训练模型处于收敛状态，则根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，并将与所述第二梯度值对应的样本参数确定为所述待训练模型的模型参数。

19、如权利要求 18 所述的存储介质，其中，所述基于联邦学习的模型参数训练程序被处理器执行时还实现如下步骤：

当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端获取对应的第一数据，及与所述第一数据对应的样本标签；

基于所述第一数据、所述加密后的第二数据、所述样本标签和预设损失函数计算损失值，并采用同态加密算法加密所述损失值，得到加密的损失值，记作损失加密值；

根据所述预设损失函数得到梯度函数，并根据所述梯度函数计算得到第一梯度值，并采用同态加密算法加密所述第一梯度值，得到加密的第一梯度值，记作第一梯度加密值。

20、如权利要求 19 所述的存储介质，其中，所述基于联邦学习的模型参数训练程序被处理器执行时还实现如下步骤：

根据所述加密后的第二数据和所述第一数据计算得到加密中间结果，通过预设公钥对所述加密中间结果进行加密，得到双重加密中间结果；

将所述双重加密中间结果发送至所述第二终端，以使得所述第二终端基于所述双重加密中间结果计算得到双重加密梯度值；

在接收到所述第二终端返回的所述双重加密梯度值时，通过与所述预设公钥对应的私钥对所述双重加密梯度值进行解密，并将解密后的双重加密梯度值发送至所述第二终端，以使得所述第二终端对所述解密后的双重加密梯度值进行解密，得到所述第二终端的梯度值。

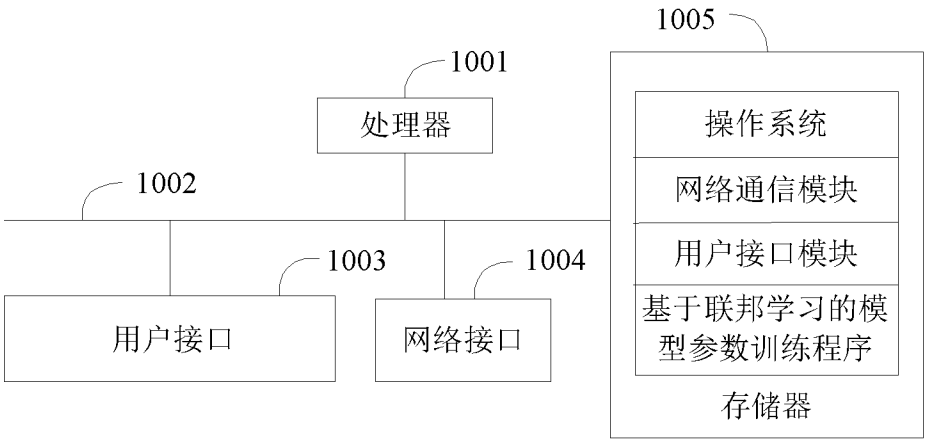

1005
1001
处理器
操作系统
网络通信模块
1002
用户接口模块
1003
1004
基于联邦学习的模型参数训练程序
用户接口
网络接口
存储器

图 1

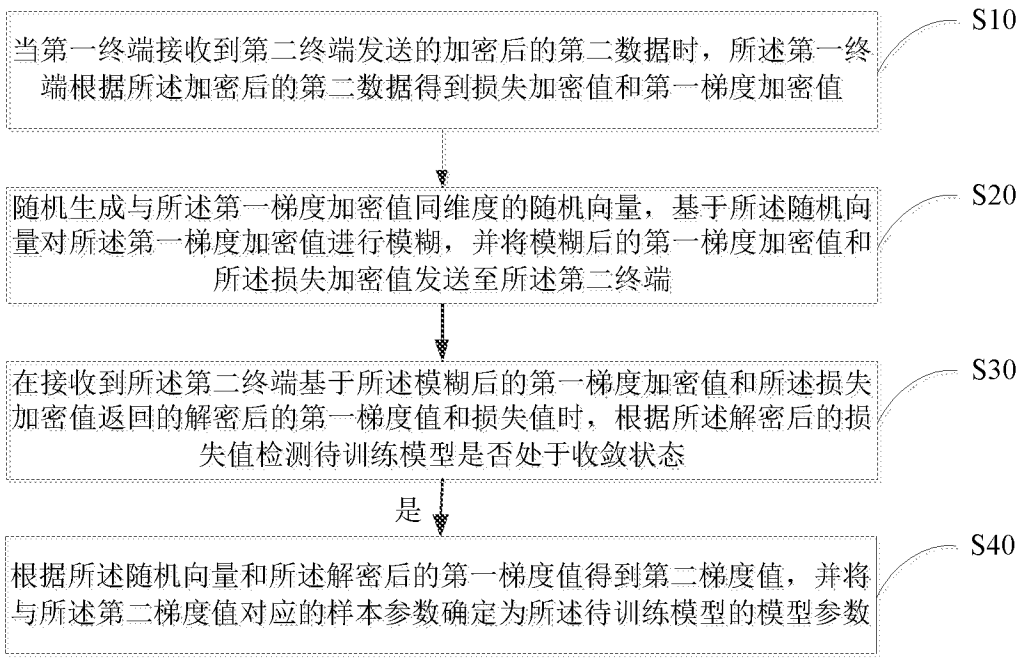

当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端根据所述加密后的第二数据得到损失加密值和第一梯度加密值
S10
随机生成与所述第一梯度加密值同维度的随机向量，基于所述随机向量对所述第一梯度加密值进行模糊，并将模糊后的第一梯度加密值和所述损失加密值发送至所述第二终端
S20
在接收到所述第二终端基于所述模糊后的第一梯度加密值和所述损失加密值返回的解密后的第一梯度值和损失值时，根据所述解密后的损失值检测待训练模型是否处于收敛状态
S30
是
根据所述随机向量和所述解密后的第一梯度值得到第二梯度值，并将与所述第二梯度值对应的样本参数确定为所述待训练模型的模型参数
S40

图 2

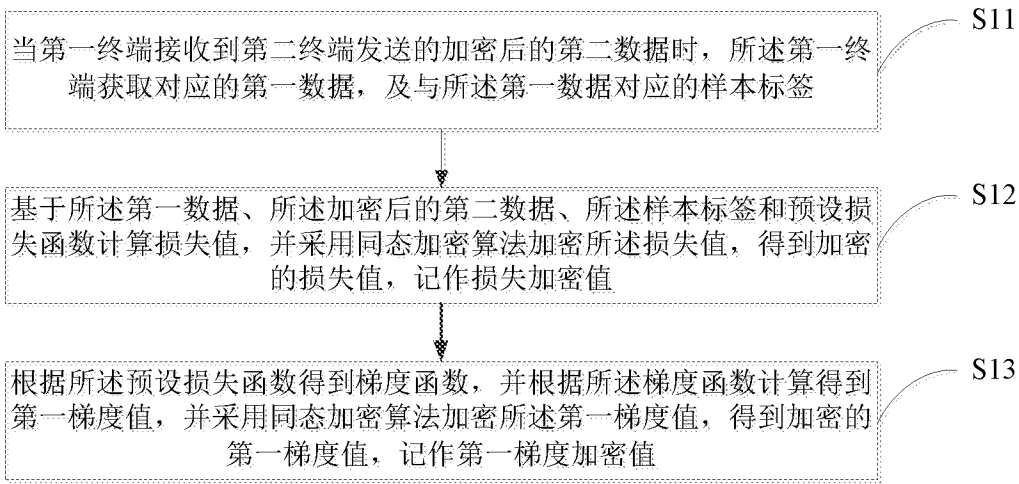

当第一终端接收到第二终端发送的加密后的第二数据时，所述第一终端获取对应的第一数据，及与所述第一数据对应的样本标签
S11
基于所述第一数据、所述加密后的第二数据、所述样本标签和预设损失函数计算损失值，并采用同态加密算法加密所述损失值，得到加密的损失值，记作损失加密值
S12
根据所述预设损失函数得到梯度函数，并根据所述梯度函数计算得到第一梯度值，并采用同态加密算法加密所述第一梯度值，得到加密的第一梯度值，记作第一梯度加密值
S13

图 3

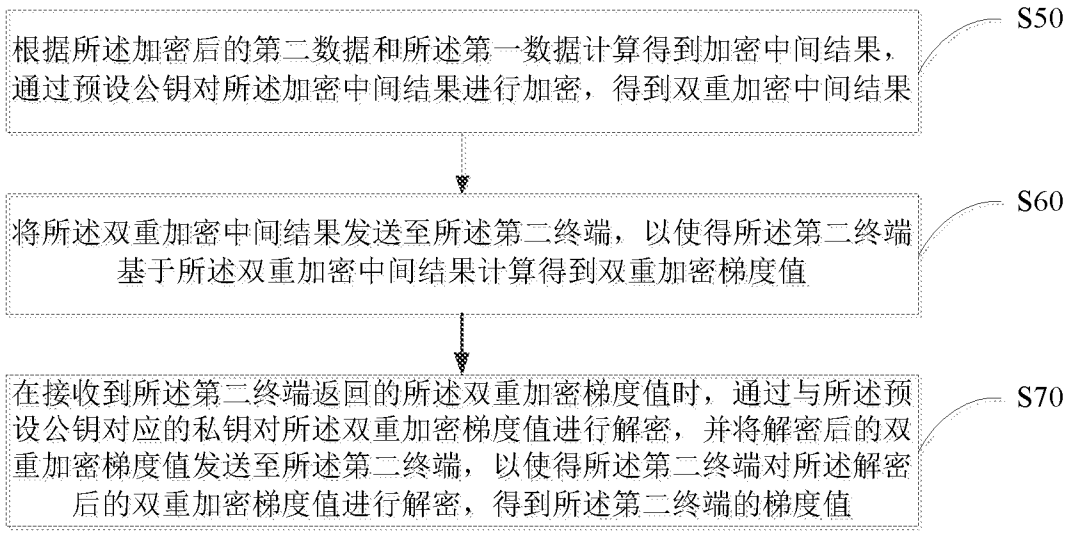

根据所述加密后的第二数据和所述第一数据计算得到加密中间结果，通过预设公钥对所述加密中间结果进行加密，得到双重加密中间结果
S50
将所述双重加密中间结果发送至所述第二终端，以使得所述第二终端基于所述双重加密中间结果计算得到双重加密梯度值
S60
在接收到所述第三终端返回的所述双重加密梯度值时，通过与所述预设公钥对应的私钥对所述双重加密梯度值进行解密，并将解密后的双重加密梯度值发送至所述第二终端，以使得所述第二终端对所述解密后的双重加密梯度值进行解密，得到所述第二终端的梯度值
S70

图 4

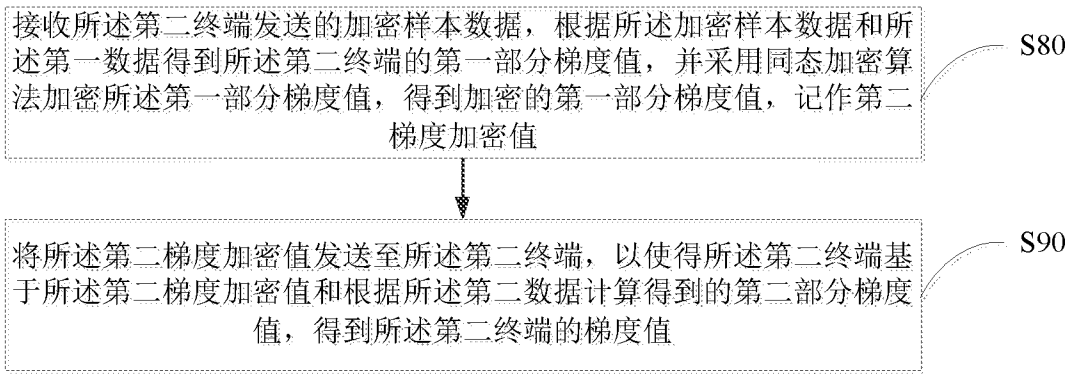

接收所述第二终端发送的加密样本数据，根据所述加密样本数据和所述第一数据得到所述第二终端的第一部分梯度值，并采用同态加密算法加密所述第一部分梯度值，得到加密的第一部分梯度值，记作第二梯度加密值
S80
将所述第二梯度加密值发送至所述第二终端，以使得所述第二终端基于所述第二梯度加密值和根据所述第二数据计算得到的第二部分梯度值，得到所述第二终端的梯度值
S90

图 5

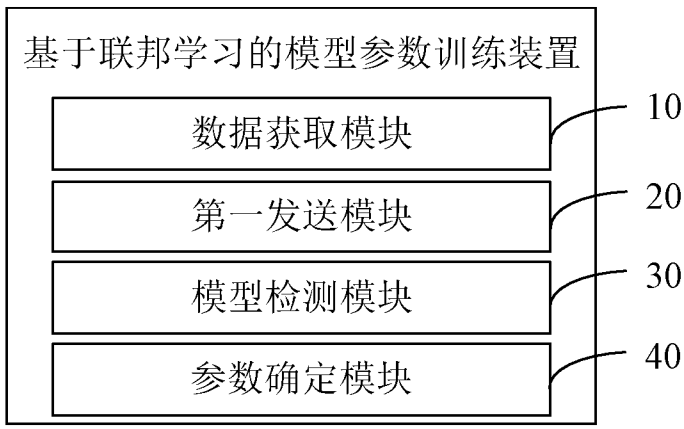

基于联邦学习的模型参数训练装置
数据获取模块
10
第一发送模块
20
模型检测模块
30
参数确定模块
40

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/119227

A. CLASSIFICATION OF SUBJECT MATTER

G06N 20/00(2019.01)i; G06F 21/60(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F, 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)

CNTXT, CNABS, SIPOABS, DWPI, CNKI: 联邦学习, 模型, 参数, 训练, 损失值, 梯度, 模糊, 向量, 加密, 解密, federated learning, model, parameter, training, loss, gradient, vague, vector, encryption, decryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109886417 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 14 June 2019 (2019-06-14) entire document	1-20
A	CN 109165515 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 08 January 2019 (2019-01-08) entire document	1-20
A	CN 109255444 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 22 January 2019 (2019-01-22) entire document	1-20
A	CN 109165725 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 08 January 2019 (2019-01-08) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 February 2020	**19 February 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/119227

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109886417 A	14 June 2019	None	
CN 109165515 A	08 January 2019	None	
CN 109255444 A	22 January 2019	None	
CN 109165725 A	08 January 2019	None	

国际检索报告

国际申请号
PCT/CN2019/119227

A. 主题的分类

G06N 20/00(2019.01)i; G06F 21/60(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F, 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）)

CNTXT, CNABS, SIPOABS, DWPI, CNKI：联邦学习，模型，参数，训练，损失值，梯度，模糊，向量，加密，解密，federated learning, model, parameter, training, loss, gradient, vague, vector, encryption, decryption

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 109886417 A (深圳前海微众银行股份有限公司) 2019年 6月 14日 (2019-06-14) 全文	1-20
A	CN 109165515 A (深圳前海微众银行股份有限公司) 2019年 1月 8日 (2019-01-08) 全文	1-20
A	CN 109255444 A (深圳前海微众银行股份有限公司) 2019年 1月 22日 (2019-01-22) 全文	1-20
A	CN 109165725 A (深圳前海微众银行股份有限公司) 2019年 1月 8日 (2019-01-08) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：
“A” 认为不特别相关的表示了现有技术一般状态的文件
“E” 在国际申请日的当天或之后公布的在先申请或专利
“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）
“O” 涉及口头公开、使用、展览或其他方式公开的文件
“P” 公布日先于国际申请日但迟于所要求的优先权日的文件
“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件
“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性
“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性
“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 2月 12日	2020年 2月 19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 程琼 电话号码 86-(10)-62411647

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/119227

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 109886417 A	2019年 6月 14日	无	
CN 109165515 A	2019年 1月 8日	无	
CN 109255444 A	2019年 1月 22日	无	
CN 109165725 A	2019年 1月 8日	无	