(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114996772 A
(43)申请公布日 2022.09.02

(21)申请号 202210693204.2

(22)申请日 2022.06.17

(71)申请人 上海富数科技有限公司广州分公司
地址 510640 广东省广州市天河区岑村圣堂大街工业区38号二层C区741房

(72)发明人 陈立峰 卞阳 李腾飞

(74)专利代理机构 北京超凡宏宇专利代理事务所(特殊普通合伙) 11463
专利代理师 赵兴

(51)Int.Cl.
G06F 21/71(2013.01)
G06F 21/60(2013.01)
G06N 20/00(2019.01)

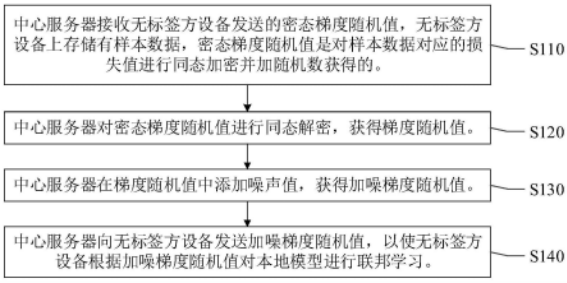
权利要求书2页 说明书10页 附图5页

(54)发明名称

一种联邦学习方法、装置、电子设备及存储介质

(57)摘要

本申请提供一种联邦学习方法、装置、电子设备及存储介质，用于改善目前联邦学习过程的安全性较低的问题。该方法包括：接收无标签方设备发送的密态梯度随机值，无标签方设备上存储有样本数据，密态梯度随机值是对样本数据对应的损失值进行同态加密并加随机数获得的；对密态梯度随机值进行同态解密，获得梯度随机值；在梯度随机值中添加噪声值，获得加噪梯度随机值；向无标签方设备发送加噪梯度随机值，以使无标签方设备根据加噪梯度随机值对本地模型进行联邦学习。



CN 114996772 A

1.一种联邦学习方法,其特征在于,包括:

接收无标签方设备发送的密态梯度随机值,所述无标签方设备上存储有样本数据,所述密态梯度随机值是对所述样本数据对应的损失值进行同态加密并加随机数获得的;

对所述密态梯度随机值进行同态解密,获得梯度随机值;

在所述梯度随机值中添加噪声值,获得加噪梯度随机值;

向无标签方设备发送所述加噪梯度随机值,以使所述无标签方设备根据所述加噪梯度随机值对本地模型进行联邦学习。

2.根据权利要求1所述的方法,其特征在于,所述在所述梯度随机值中添加噪声值,包括:

使用局部差分隐私算法生成所述噪声值,并在所述梯度随机值中添加所述噪声值。

3.根据权利要求1-2任一所述的方法,其特征在于,在所述接收无标签方设备发送的密态梯度随机值之前,还包括:

获取密态损失值,所述密态损失值是有标签方设备计算出来的,所述有标签方设备是存储有所述样本数据对应的样本标签的设备;

向所述无标签方设备发送所述密态损失值,以使所述无标签方设备根据所述密态损失值计算密态梯度值,并将所述密态梯度值加上生成的随机数,获得并返回所述密态梯度随机值。

4.根据权利要求3所述的方法,其特征在于,所述获取密态损失值,包括:

向所述有标签方设备发送公钥,以使所述有标签方设备使用所述公钥对获得的损失值进行同态加密,获得并返回所述密态损失值;

接收所述有标签方设备发送的所述密态损失值。

5.一种联邦学习方法,其特征在于,应用于无标签方设备,包括:

获取密态损失值,根据所述密态损失值和所述无标签方设备上存储的样本数据计算出密态梯度值,所述密态损失值是同态加密获得的;

将所述密态梯度值加上生成的随机数,获得密态梯度随机值;

向中心服务器发送所述密态梯度随机值,以使所述中心服务器从所述密态梯度随机值使用解密出梯度随机值,并在所述梯度随机值中添加噪声值,获得并返回加噪梯度随机值;

接收所述中心服务器发送的所述加噪梯度随机值,并将所述加噪梯度随机值减去所述随机数,获得加噪梯度值,所述加噪梯度值用于对本地模型进行联邦学习。

6.根据权利要求5所述的方法,其特征在于,所述获取密态损失值,包括:

获取所述本地模型的模型参数和所述样本数据,并计算所述模型参数和所述样本数据之间的内积结果;

向有标签方设备发送所述内积结果,以使所述有标签方设备计算所述内积结果对应的预测标签,并计算所述预测标签与所述内积结果对应的样本标签之间的损失值,然后,使用所述中心服务器的公钥对所述损失值进行同态加密,获得并返回密态损失值;

接收所述有标签方设备发送的所述密态损失值。

7.一种联邦学习装置,其特征在于,应用于中心服务器,包括:

密态梯度接收模块,用于接收无标签方设备发送的密态梯度随机值,所述无标签方设备上存储有样本数据,所述密态梯度随机值是对所述样本数据对应的损失值进行同态加密

并加随机数获得的；

密态梯度解密模块，用于对所述密态梯度随机值进行同态解密，获得梯度随机值；

梯度随机加噪模块，用于在所述梯度随机值中添加噪声值，获得加噪梯度随机值；

加噪梯度发送模块，用于向无标签方设备发送所述加噪梯度随机值，以使所述无标签方设备根据所述加噪梯度随机值对本地模型进行联邦学习。

8.根据权利要求7所述的装置，其特征在于，所述梯度随机加噪模块，包括：

差分隐私生成模块，用于使用局部差分隐私算法生成所述噪声值，并在所述梯度随机值中添加所述噪声值。

9.一种电子设备，其特征在于，包括：处理器和存储器，所述存储器存储有所述处理器可执行的机器可读指令，所述机器可读指令被所述处理器执行时执行如权利要求1至6任一项所述的方法。

10.一种计算机可读存储介质，其特征在于，该计算机可读存储介质上存储有计算机程序，该计算机程序被处理器运行时执行如权利要求1至6任一项所述的方法。

一种联邦学习方法、装置、电子设备及存储介质

技术领域

[0001] 本申请涉及机器学习和联邦学习的技术领域，具体而言，涉及一种联邦学习方法、装置、电子设备及存储介质。

背景技术

[0002] 联邦机器学习(Federated Machine Learning，FML)，又被称为联邦学习(Federated Learning)、联合学习或者联盟学习，是一种机器学习技术，具体来说就是人们在多个拥有本地数据样本的分散式边缘设备或服务器上训练算法；这种方法与传统的集中式机器学习技术有显著不同，传统的集中式机器学习技术将所有的本地数据集上传到一个服务器上，而更经典的分散式方法则通常假设本地数据样本都是相同分布的。联邦机器学习是一个机器学习框架，能有效帮助多个机构在满足用户隐私保护、数据安全和法律法规的要求下，进行数据使用和机器学习建模。

[0003] 在目前的联邦学习过程中，有标签方设备和无标签方设备可以相互通信；无标签方设备是指存储有用于训练模型的样本数据的设备，而有标签方设备是指存储有该样本数据对应样本标签的设备。有标签方设备需要在无需获知无标签设备上明文存储的样本数据的情况下，计算出样本数据对应预测标签与样本标签的损失值，并将损失值发送给无标签方设备，以使无标签方设备根据损失值计算出梯度值，使用梯度值对本地模型进行训练。在具体的实践过程中发现，目前联邦学习过程的安全性较低。

发明内容

[0004] 本申请实施例的目的在于提供一种联邦学习方法、装置、电子设备及存储介质，用于改善目前联邦学习过程的安全性较低的问题。

[0005] 本申请实施例提供了一种联邦学习方法，包括：接收无标签方设备发送的密态梯度随机值，无标签方设备上存储有样本数据，密态梯度随机值是对样本数据对应的损失值进行同态加密并加随机数获得的；对密态梯度随机值进行同态解密，获得梯度随机值；在梯度随机值中添加噪声值，获得加噪梯度随机值；向无标签方设备发送加噪梯度随机值，以使无标签方设备根据加噪梯度随机值对本地模型进行联邦学习。在上述的实现过程中，通过在获得的梯度随机值中添加噪声值，获得加噪梯度随机值；向无标签方设备发送加噪梯度随机值，使得无标签方设备难以使用梯度值、预测标签和样本数据破解出有标签设备上存储的样本标签，从而有效地提高了联邦学习的安全性。

[0006] 可选地，在本申请实施例中，在梯度随机值中添加噪声值，包括：使用局部差分隐私算法生成噪声值，并在梯度随机值中添加噪声值。在上述的实现过程中，通过使用局部差分隐私算法生成噪声值，由于局部差分隐私算法只考虑本地数据集的统计学特性，从而让多方联邦学习或者多方安全计算的过程中，更好地避免了本地数据泄露到其他设备的风险，从而有效地提高了联邦学习的安全性。

[0007] 可选地，在本申请实施例中，在接收无标签方设备发送的密态梯度随机值之前，还

包括:获取密态损失值,密态损失值是有标签方设备计算出来的,有标签方设备是存储有样本数据对应的样本标签的设备;向无标签方设备发送密态损失值,以使无标签方设备根据密态损失值计算密态梯度值,并将密态梯度值加上生成的随机数,获得并返回密态梯度随机值。在上述的实现过程中,通过向无标签方设备发送密态损失值,以使无标签方设备根据密态损失值计算密态梯度值,并将密态梯度值加上生成的随机数,获得并返回密态梯度随机值,从而避免了梯度值在明文状态下泄露给无标签方设备的问题,从而有效地提高了联邦学习的安全性。

[0008] 可选地,在本申请实施例中,获取密态损失值,包括:向有标签方设备发送中心服务器的公钥,以使有标签方设备使用公钥对获得的损失值进行同态加密,获得并返回密态损失值;接收有标签方设备发送的密态损失值。

[0009] 本申请实施例还提供了一种联邦学习方法,应用于无标签方设备,包括:获取密态损失值,根据密态损失值和无标签方设备上存储的样本数据计算出密态梯度值,密态损失值是同态加密获得的;将密态梯度值加上生成的随机数,获得密态梯度随机值;向中心服务器发送密态梯度随机值,以使中心服务器从密态梯度随机值使用解密出梯度随机值,并在梯度随机值中添加噪声值,获得并返回加噪梯度随机值;接收中心服务器发送的加噪梯度随机值,并将加噪梯度随机值减去随机数,获得加噪梯度值,加噪梯度值用于对本地模型进行联邦学习。在上述的实现过程中,通过在获得的梯度随机值中添加噪声值,获得加噪梯度随机值;向无标签方设备发送加噪梯度随机值,使得无标签方设备难以使用梯度值、预测标签和样本数据破解出有标签设备上存储的样本标签,从而有效地提高了联邦学习的安全性。

[0010] 可选地,在本申请实施例中,获取密态损失值,包括:获取本地模型的模型参数和样本数据,并计算模型参数和样本数据之间的内积结果;向有标签方设备发送内积结果,以使有标签方设备计算内积结果对应的预测标签,并计算预测标签与内积结果对应的样本标签之间的损失值,然后,使用中心服务器的公钥对损失值进行同态加密,获得并返回密态损失值;接收有标签方设备发送的密态损失值。在上述的实现过程中,通过获取本地模型的模型参数和样本数据,并计算模型参数和样本数据之间的内积结果;向有标签方设备发送内积结果,从而避免了直接将样本数据明文泄露给有标签方设备的问题,而是只泄露模型参数和样本数据之间的内积结果给有标签方式设备,从而有效地提高了联邦学习的安全性。

[0011] 本申请实施例还提供了一种联邦学习装置,应用于中心服务器,包括:密态梯度接收模块,用于接收无标签方设备发送的密态梯度随机值,无标签方设备上存储有样本数据,密态梯度随机值是对样本数据对应的损失值进行同态加密并加随机数获得的;密态梯度解密模块,用于对密态梯度随机值进行同态解密,获得梯度随机值;梯度随机加噪模块,用于在梯度随机值中添加噪声值,获得加噪梯度随机值;加噪梯度发送模块,用于向无标签方设备发送加噪梯度随机值,以使无标签方设备根据加噪梯度随机值对本地模型进行联邦学习。

[0012] 可选地,在本申请实施例中,梯度随机加噪模块,包括:差分隐私生成模块,用于使用局部差分隐私算法生成噪声值,并在梯度随机值中添加噪声值。

[0013] 可选地,在本申请实施例中,联邦学习装置,还包括:密态损失获取模块,用于获取密态损失值,密态损失值是有标签方设备计算出来的,有标签方设备是存储有样本数据对

应的样本标签的设备;密态损失发送模块,用于向无标签方设备发送密态损失值,以使无标签方设备根据密态损失值计算密态梯度值,并将密态梯度值加上生成的随机数,获得并返回密态梯度随机值。

[0014] 可选地,在本申请实施例中,密态损失获取模块,包括:公钥同态加密模块,用于向有标签方设备发送中心服务器的公钥,以使有标签方设备使用公钥对获得的损失值进行同态加密,获得并返回密态损失值;密态损失接收模块,用于接收有标签方设备发送的密态损失值。

[0015] 本申请实施例还提供了一种联邦学习装置,应用于无标签方设备,包括:密态梯度计算模块,用于获取密态损失值,根据密态损失值和无标签方设备上存储的样本数据计算出密态梯度值,密态损失值是同态加密获得的;密态梯度随机模块,用于将密态梯度值加上生成的随机数,获得密态梯度随机值;密态梯度发送模块,用于向中心服务器发送密态梯度随机值,以使中心服务器从密态梯度随机值使用解密出梯度随机值,并在梯度随机值中添加噪声值,获得并返回加噪梯度随机值;加噪梯度接收模块,用于接收中心服务器发送的加噪梯度随机值,并将加噪梯度随机值减去随机数,获得加噪梯度值,加噪梯度值用于对本地模型进行联邦学习。

[0016] 可选地,在本申请实施例中,密态梯度计算模块,包括:内积结果计算模块,用于获取本地模型的模型参数和样本数据,并计算模型参数和样本数据之间的内积结果;内积结果发送模块,用于向有标签方设备发送内积结果,以使有标签方设备计算内积结果对应的预测标签,并计算预测标签与内积结果对应的样本标签之间的损失值,然后,使用中心服务器的公钥对损失值进行同态加密,获得并返回密态损失值;第一损失接收模块,用于接收有标签方设备发送的密态损失值。

[0017] 本申请实施例还提供了一种电子设备,包括:处理器和存储器,存储器存储有处理器可执行的机器可读指令,机器可读指令被处理器执行时执行如上面描述的方法。

[0018] 本申请实施例还提供了一种计算机可读存储介质,该计算机可读存储介质上存储有计算机程序,该计算机程序被处理器运行时执行如上面描述的方法。

附图说明

[0019] 为了更清楚地说明本申请实施例的技术方案,下面将对本申请实施例中所需要使用的附图作简单地介绍,应当理解,以下附图仅示出了本申请实施例中的某些实施例,因此不应被看作是对范围的限定,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他相关的附图。

[0020] 图1示出的本申请实施例提供的联邦学习方法的流程示意图;

[0021] 图2示出的本申请实施例提供的三方执行联邦学习方法的交互时序图;

[0022] 图3示出的本申请实施例提供的两方执行联邦学习方法的交互时序图;

[0023] 图4示出的本申请实施例提供的无标签方设备执行的联邦学习方法的流程示意图;

[0024] 图5示出的本申请实施例提供的联邦学习装置的结构示意图;

[0025] 图6示出的本申请实施例提供的电子设备的结构示意图。

具体实施方式

[0026] 下面将结合本申请实施例中附图，对本申请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申请实施例中的一部分实施例，而不是全部的实施例。通常在此处附图中描述和示出的本申请实施例的组件可以以各种不同的配置来布置和设计。因此，以下对在附图中提供的本申请实施例的详细描述并非旨在限制要求保护的本申请实施例的范围，而是仅仅表示本申请实施例中的选定实施例。基于本申请实施例，本领域技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本申请实施例保护的范围。

[0027] 在介绍本申请实施例提供的联邦学习方法之前，先介绍本申请实施例中所涉及的一些概念：

[0028] 机器学习(Machine Learning,ML)，是指人工智能领域中研究人类学习行为的一个分支；借鉴认知科学、生物学、哲学、统计学、信息论、控制论、计算复杂性等学科或理论的观点，通过归纳、一般化、特殊化、类比等基本方法探索人类的认识规律和学习过程，建立各种能通过经验自动改进的算法，使计算机系统能够具有自动学习特定知识和技能的能力。

[0029] 同态加密(Homomorphic encryption)是一种加密形式，同态加密允许人们对密文进行特定形式的代数运算得到仍然是加密的结果，将其解密所得到的结果与对明文进行同样的运算结果一样。换言之，这项技术令人们可以在加密的数据中进行诸如检索、比较等操作，得出正确的结果，而在整个处理过程中无需对数据进行解密。

[0030] 差分隐私(Differential Privacy)是一个数据共享手段，可以实现仅仅分享用于描述数据库的一些统计特征、而不公开具体到个人的信息。差分隐私背后的直观想法是：如果随机修改数据库中的一个记录造成的影响足够小，求得的统计特征就不能被用来反推出单一记录的内容；这一特性可以被用来保护隐私。从另一个角度来理解差分隐私，可以将其视为用于公开统计数据库统计特征的算法的一个约束条件。该约束条件要求数据库各记录中的隐私信息不被公开。

[0031] 需要说明的是，本申请实施例提供的联邦学习方法可以被电子设备执行，此处的电子设备包括但不限于：有标签方设备、无标签方设备和/或中心服务器。其中，有标签方设备是指有用于训练模型的样本标签的电子设备，有标签方式设备上可以有样本标签对应的样本数据，也可以没有样本标签对应的样本数据。无标签方设备是指有用于训练模型的样本数据的电子设备，但是该无标签设备上没有样本数据对应的样本标签，因此，需要联合无标签设备上的样本数据和有标签设备上的样本标签一起训练机器学习模型。可选地，无标签设备和有标签设备可以选择一个中心服务器，中心服务器就是用于来协调一起训练机器学习模型的过程，且保证在训练机器学习的过程中，不让无标签设备上的样本数据泄露给有标签设备和中心服务器，也不让有标签设备上的样本标签泄露给无标签设备和中心服务器，也就是说，样本数据和样本标签均不能明文泄露除设备自己以外的其它设备中，中心服务器也并不知道明文状态下的样本数据和样本标签。

[0032] 上述的有标签方设备、无标签方设备和中心服务器均是指具有执行计算机程序功能的设备终端或者服务器，设备终端例如：智能手机、个人电脑、平板电脑、个人数字助理或者移动上网设备等。服务器是指通过网络提供计算服务的设备，服务器例如：x86服务器以及非x86服务器，非x86服务器包括：大型机、小型机和UNIX服务器。可以理解的是，上述的有

标签方设备对应的用户和无标签方设备对应的用户均是联邦学习的参与方，因此，上述的有标签方设备和无标签方设备又可以均被称为参与方设备。

[0033] 下面介绍该联邦学习方法适用的应用场景，这里的应用场景包括但不限于：在联邦学习的过程中，无标签设备获得的梯度值可以使用公式表示为$\frac{dL}{d\theta^{(2)}} = [y - h(\theta^{(2)})]x^{(2)}$；其中，$\frac{dL}{d\theta^{(2)}}$表示梯度值，y表示样本标签，$h(\theta^{(2)})$表示预测标签，$x^{(2)}$表示样本数据。由于无标签设备已经存储有样本数据，且在模型多次迭代后能够获取到准确的预测标签，即$h(\theta^{(2)})$和$x^{(2)}$是已知的。随着训练次数加深最后得到准确的梯度值，且y是离散值0或1，导致无标签方设备容易使用梯度值、预测标签和样本数据破解出有标签设备上存储的样本标签，具体的破解思路可以将上面的公式简化看待为一个子集和(Subset Sum)问题，子集和问题在小规模计算或是稀疏搜索域的情况下是存在快速解法的。因此，根据梯度值、预测标签和样本数据容易破解出有标签设备上存储的样本标签，导致联邦学习的安全性较低。在这种场景中，可以使用该联邦学习方法来向获得的梯度随机值中添加噪声值，使得无标签方设备难以使用梯度值、预测标签和样本数据破解出有标签设备上存储的样本标签，从而有效地提高了联邦学习的安全性。

[0034] 请参见图1示出的本申请实施例提供的联邦学习方法的流程示意图；在三方(包括：有标签方设备、无标签方设备和中心服务器)执行的联邦学习场景中，该联邦学习方法可以应用于中心服务器，即该联邦学习方法可以被中心服务器执行，当然也可以被两方执行的联邦学习方法中的有标签方设备执行，后面将详细地介绍这种方式。上述联邦学习方法的主要思路是，通过在获得的梯度随机值中添加噪声值，获得加噪梯度随机值；向无标签方设备发送加噪梯度随机值，使得无标签方设备难以使用梯度值、预测标签和样本数据破解出有标签设备上存储的样本标签，从而有效地提高了联邦学习的安全性。上述的联邦学习方法具体可以包括：

[0035] 步骤S110：中心服务器接收无标签方设备发送的密态梯度随机值，无标签方设备上存储有样本数据，密态梯度随机值是对样本数据对应的损失值进行同态加密并加随机数获得的。

[0036] 请参见图2示出的本申请实施例提供的三方执行联邦学习方法的交互时序图；上述步骤S110的实施方式例如：中心服务器可以事先使用非对称加密算法生成一对公钥(public key，pk)和私钥(secret key)，然后向无标签方设备发送中心服务器上生成的公钥。无标签方设备在接收到中心服务器发送的公钥pk之后，先获取本地存储的样本数据和模型参数，此处的样本数据可以表示为x，模型参数可以表示为θ；然后，计算样本数据和模型参数之间的内积结果，并向有标签方设备发送该内积结果，其中，此处的内积结果可以表示为u，那么u可以对x和θ进行内积计算获得的。有标签方设备在接收到无标签方设备发送的内积结果之后，先计算出该内积结果对应的预测标签，将该内积结果输入机器学习模型，即可获得预测标签，此处的预测标签具体可以表示为h(θ)，并计算出该预测标签与内积结果对应的样本标签之间的损失值，该损失值可以表示为y-h(θ)，其中此处的y表示样本标签，然后，使用中心服务器的公钥对损失值进行同态加密，获得的密态损失值可以表示为[L]＝[y-h(θ)]，并向无标签方设备发送该密态损失值[L]。无标签方设备在接收到有标签方设备发送的密态损失值之后，根据该密态损失值计算出密态梯度，该密态梯度可以表示

为$[\frac{dL}{d\theta}] = [y - h(\theta)]x$;然后,将密态梯度值加上生成的随机数,获得密态梯度随机值$[\frac{dL}{d\theta} + R]$,此处的R代表生成的随机数,最后,向中心服务器发送该密态梯度随机值$[\frac{dL}{d\theta} + R]$。中心服务器就可以接收无标签方设备发送的密态梯度随机值$[\frac{dL}{d\theta} + R]$。

[0037] 在步骤S110之后,执行步骤S120:中心服务器对密态梯度随机值进行同态解密,获得梯度随机值。

[0038] 上述步骤S120的实施方式例如:中心服务器对密态梯度随机值$[\frac{dL}{d\theta} + R]$进行同态解密,获得的梯度随机值可以表示为$\frac{dL}{d\theta} + R$。

[0039] 在步骤S120之后,执行步骤S130:中心服务器在梯度随机值中添加噪声值,获得加噪梯度随机值。

[0040] 上述步骤S130的实施方式例如:中心服务器使用局部差分隐私(Local Differential Privacy,LDP)算法生成噪声值,并在梯度随机值中添加噪声值,获得加噪梯度随机值;其中,此处的局部差分隐私算法又被称为本地化差分隐私算法。由于局部差分隐私算法只考虑本地数据集的统计学特性,从而让多方联邦学习或者多方安全计算的过程中,更好地避免了本地数据泄露到其他设备的风险,从而有效地提高了联邦学习的安全性。上述的噪声值也可以采用全局差分隐私(Global Differential Privacy,GDP)算法来生成,由于全局差分隐私算法考虑全部数据集的统计学特性,从而让多方联邦学习或者多方安全计算的过程中,更快地加速模型训练和收敛过程。当然,在具体的实践过程中,上述的噪声值也可以采用拉普拉斯(Laplace)噪声,或者采用CH噪声。

[0041] 在步骤S130之后,执行步骤S140:中心服务器向无标签方设备发送加噪梯度随机值,以使无标签方设备根据加噪梯度随机值对本地模型进行联邦学习。

[0042] 上述步骤S140的实施方式例如:中心服务器通过传输控制协议(Transmission Control Protocol,TCP)或者用户数据报协议(User Datagram Protocol,UDP)向无标签方设备发送加噪梯度随机值。无标签方设备在接收到中心服务器发送的加噪梯度随机值之后,可以将加噪梯度随机值减去随机数,即可获得加噪梯度值,然后使用加噪梯度值更新本地模型的权重值;此处的本地模型包括但不限于:机器学习算法中的逻辑回归算法模型。在上面的过程中,仅描述了一轮数据交互的过程,在具体实践时需要重复上述步骤S110至步骤S140,直到本地模型的损失函数收敛,具体例如:本地模型的损失值小于预设比例或者迭代次数(epoch)数量大于预设阈值时,即可获得训练后的本地模型。其中,上述的预设比例可以根据具体情况设置,例如设置为5%或者10%等;上述的预设阈值也可以根据具体情况进行设置,例如设置为100或者1000等等。

[0043] 在上述的实现过程中,首先,接收无标签方设备发送的密态梯度随机值,然后对密态梯度随机值进行同态解密,获得梯度随机值,再向梯度随机值中添加噪声值,最后向无标签方设备发送加噪声后的梯度随机值,使得无标签方设备难以根据接收到的梯度随机值破解出样本标签,因为接收到的梯度随机值是添加噪声后的数值。也就是说,通过在获得的梯度随机值中添加噪声值,获得加噪梯度随机值;向无标签方设备发送加噪梯度随机值,使得

无标签方设备难以使用梯度值、预测标签和样本数据破解出有标签设备上存储的样本标签，从而有效地提高了联邦学习的安全性。

[0044] 请参见图3示出的本申请实施例提供的两方执行联邦学习方法的交互时序图；该联邦学习方法具体可以包括：

[0045] 步骤S210：有标签方设备接收无标签方设备发送的密态梯度随机值，无标签方设备上存储有样本数据，密态梯度随机值是对样本数据对应的损失值进行同态加密并加随机数获得的。

[0046] 上述步骤S210的实施方式例如：无标签方设备获取样本数据和模型参数，并计算样本数据和模型参数之间的内积结果，然后向有标签方设备发送内积结果。有标签方式设备在接收到无标签方设备发送的内积结果之后，先计算内积结果对应的预测标签，并计算预测标签与内积结果对应的样本标签之间的损失值，然后，对损失值进行同态加密，获得密态损失值，最后向无标签方设备发送密态损失值。无标签方设备在接收到有标签方设备发送的密态损失值之后，根据接收到的密态损失值计算出密态梯度，并将密态梯度加上随机生成的随机数，获得密态梯度随机值，然后向有标签方设备发送密态梯度随机值。有标签方设备就可以接收无标签方设备发送的密态梯度随机值了。

[0047] 在步骤S210之后，执行步骤S220：有标签方设备对密态梯度随机值进行同态解密，获得梯度随机值。

[0048] 在步骤S220之后，执行步骤S230：有标签方设备在梯度随机值中添加噪声值，获得加噪梯度随机值。

[0049] 在步骤S230之后，执行步骤S240：有标签方设备向无标签方设备发送加噪梯度随机值，以使无标签方设备根据加噪梯度随机值对本地模型进行联邦学习。

[0050] 其中，上述步骤S220至步骤S240的实施原理和实施方式与步骤S120至步骤S140的实施原理和实施方式是类似的，因此，这里不再说明其实施原理和实施方式，如有不清楚的地方，可以参考对步骤S120至步骤S140的描述。

[0051] 请参见图4示出的本申请实施例提供的无标签方设备执行的联邦学习方法的流程示意图；在具体的实践过程中，上面无标签方设备还可以不根据内积结果计算密态损失值，而是根据样本数据对应的密态预测标签与密态样本标签计算出密态损失值，该实施方式具体可以包括：

[0052] 步骤S310：无标签方设备获取密态损失值，根据密态损失值和无标签方设备上存储的样本数据计算出密态梯度值，密态损失值是根据密态预测标签与有标签方设备上的密态样本标签计算获得的。

[0053] 上述步骤S310的实施方式例如：无标签方设备获取样本数据，并使用中心服务器的公钥对样本数据进行同态加密，获得密态样本数据，然后向有标签方设备发送密态样本数据。有标签方设备先计算密态样本数据对应的密态预测标签，并计算密态预测标签与有标签方设备计算出的密态样本标签之间的密态损失值，然后向无标签方设备发送密态损失值。无标签方设备接收有标签方设备发送的密态损失值。

[0054] 步骤S320：无标签方设备将密态梯度值加上生成的随机数，获得密态梯度随机值，并向中心服务器发送密态梯度随机值。

[0055] 上述步骤S320的实施方式例如：无标签方设备在接收到有标签方设备发送的密态

损失值之后，根据该密态损失值计算出密态梯度，该密态梯度可以表示为$[\frac{dL}{d\theta}] = [y - h(\theta)]x$；然后，将密态梯度值加上生成的随机数，获得密态梯度随机值$[\frac{dL}{d\theta} + R]$，此处的R代表生成的随机数，最后，向中心服务器发送该密态梯度随机值$[\frac{dL}{d\theta} + R]$。

[0056] 步骤S330：中心服务器接收无标签方设备发送的密态梯度随机值，并对密态梯度随机值进行同态解密，获得梯度随机值，然后，在梯度随机值中添加噪声值，获得加噪梯度随机值，并向无标签方设备发送加噪梯度随机值。

[0057] 可选地，中心服务器在接收无标签方设备发送的密态梯度随机值之前，还可以向无标签方设备发送密态损失值，让无标签方设备根据密态损失值计算出密态梯度随机值，该实施方式可以包括：

[0058] 步骤S331：中心服务器获取密态损失值，密态损失值是有标签方设备计算出来的，有标签方设备是存储有样本数据对应的样本标签的设备。

[0059] 上述步骤S331的实施方式例如：中心服务器通过超文本传输协议(Hyper Text Transfer Protocol，HTTP)或者超文本传输安全协议(Hyper Text Transfer Protocol Secure，HTTPS)向有标签方设备发送中心服务器的公钥。有标签方设备在通过HTTP协议或者HTTPS协议接收到中心服务器发送的公钥之后，使用公钥对获得的损失值进行同态加密，获得密态损失值。

[0060] 步骤S332：中心服务器向无标签方设备发送密态损失值，以使无标签方设备根据密态损失值计算密态梯度值，并将密态梯度值加上生成的随机数，获得并返回密态梯度随机值。

[0061] 上述步骤S332的实施方式例如：中心服务器通过HTTP协议或者HTTPS协议向无标签方设备发送密态损失值。无标签方设备在接收到中心服务器发送的密态损失值之后，根据密态损失值计算密态梯度值，并将密态梯度值加上生成的随机数，获得密态梯度随机值，最后，向中心服务器发送该密态梯度随机值。

[0062] 步骤S340：无标签方设备接收中心服务器发送的加噪梯度随机值，并将加噪梯度随机值减去随机数，获得加噪梯度值，然后，使用加噪梯度值对本地模型进行训练。

[0063] 上述步骤S340的实施方式例如：无标签方设备在接收到中心服务器发送的加噪梯度随机值之后，可以将加噪梯度随机值减去随机数，即可获得加噪梯度值，然后使用加噪梯度值对本地模型进行训练，具体地，使用加噪梯度值更新本地模型的权重值；此处的本地模型包括但不限于：机器学习算法中的逻辑回归算法模型。在上面的过程中，仅描述了一轮数据交互的过程，在具体实践时需要重复上述步骤，直到本地模型的损失函数收敛，具体例如：本地模型的损失值小于预设比例或者迭代次数(epoch)数量大于预设阈值时，即可获得训练后的本地模型。其中，上述的预设比例可以根据具体情况设置，例如设置为5％或者10％等；上述的预设阈值也可以根据具体情况进行设置，例如设置为100或者1000等等。

[0064] 请参见图5示出的本申请实施例提供的联邦学习装置的结构示意图；本申请实施例提供了一种联邦学习装置400，应用于中心服务器，包括：

[0065] 密态梯度接收模块410，用于接收无标签方设备发送的密态梯度随机值，无标签方

设备上存储有样本数据，密态梯度随机值是对样本数据对应的损失值进行同态加密并加随机数获得的。

[0066] 密态梯度解密模块420，用于对密态梯度随机值进行同态解密，获得梯度随机值。

[0067] 梯度随机加噪模块430，用于在梯度随机值中添加噪声值，获得加噪梯度随机值。

[0068] 加噪梯度发送模块440，用于向无标签方设备发送加噪梯度随机值，以使无标签方设备根据加噪梯度随机值对本地模型进行联邦学习。

[0069] 可选地，在本申请实施例中，梯度随机加噪模块，包括：

[0070] 差分隐私生成模块，用于使用局部差分隐私算法生成噪声值，并在梯度随机值中添加噪声值。

[0071] 可选地，在本申请实施例中，联邦学习装置，还包括：

[0072] 密态损失获取模块，用于获取密态损失值，密态损失值是有标签方设备计算出来的，有标签方设备是存储有样本数据对应的样本标签的设备。

[0073] 密态损失发送模块，用于向无标签方设备发送密态损失值，以使无标签方设备根据密态损失值计算密态梯度值，并将密态梯度值加上生成的随机数，获得并返回密态梯度随机值。

[0074] 可选地，在本申请实施例中，密态损失获取模块，包括：

[0075] 公钥同态加密模块，用于向有标签方设备发送中心服务器的公钥，以使有标签方设备使用公钥对获得的损失值进行同态加密，获得并返回密态损失值。

[0076] 密态损失接收模块，用于接收有标签方设备发送的密态损失值。

[0077] 本申请实施例提供了一种联邦学习装置，应用于无标签方设备，包括：

[0078] 密态梯度计算模块，用于获取密态损失值，根据密态损失值和无标签方设备上存储的样本数据计算出密态梯度值，密态损失值是同态加密获得的。

[0079] 密态梯度随机模块，用于将密态梯度值加上生成的随机数，获得密态梯度随机值。

[0080] 密态梯度发送模块，用于向中心服务器发送密态梯度随机值，以使中心服务器从密态梯度随机值使用解密出梯度随机值，并在梯度随机值中添加噪声值，获得并返回加噪梯度随机值。

[0081] 加噪梯度接收模块，用于接收中心服务器发送的加噪梯度随机值，并将加噪梯度随机值减去随机数，获得加噪梯度值，加噪梯度值用于对本地模型进行联邦学习。

[0082] 可选地，在本申请实施例中，密态梯度计算模块，包括：

[0083] 内积结果计算模块，用于获取本地模型的模型参数和样本数据，并计算模型参数和样本数据之间的内积结果。

[0084] 内积结果发送模块，用于向有标签方设备发送内积结果，以使有标签方设备计算内积结果对应的预测标签，并计算预测标签与内积结果对应的样本标签之间的损失值，然后，使用中心服务器的公钥对损失值进行同态加密，获得并返回密态损失值。

[0085] 第一损失接收模块，用于接收有标签方设备发送的密态损失值。

[0086] 应理解的是，该装置与上述的联邦学习方法实施例对应，能够执行上述方法实施例涉及的各个步骤，该装置具体的功能可以参见上文中的描述，为避免重复，此处适当省略详细描述。该装置包括至少一个能以软件或固件(firmware)的形式存储于存储器中或固化在装置的操作系统(operating system,OS)中的软件功能模块。

[0087] 请参见图6示出的本申请实施例提供的电子设备的结构示意图。本申请实施例提供的一种电子设备500,包括:处理器510和存储器520,存储器520存储有处理器510可执行的机器可读指令,机器可读指令被处理器510执行时执行如上的方法。

[0088] 本申请实施例还提供了一种计算机可读存储介质530,该计算机可读存储介质530上存储有计算机程序,该计算机程序被处理器510运行时执行如上的方法。

[0089] 其中,计算机可读存储介质530可以由任何类型的易失性或非易失性存储设备或者它们的组合实现,如静态随机存取存储器(Static Random Access Memory,简称SRAM),电可擦除可编程只读存储器(Electrically Erasable Programmable Read-Only Memory,简称EEPROM),可擦除可编程只读存储器(Erasable Programmable Read Only Memory,简称EPROM),可编程只读存储器(Programmable Read-Only Memory,简称PROM),只读存储器(Read-Only Memory,简称ROM),磁存储器,快闪存储器,磁盘或光盘。

[0090] 本申请实施例提供的几个实施例中,应该理解到,所揭露的装置和方法,也可以通过其他的方式实现。以上所描述的装置实施例仅是示意性的,例如,附图中的流程图和框图显示了根据本申请实施例的多个实施例的装置、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分,模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意,在有些作为替换的实现方式中,方框中所标注的功能也可以和附图中所标注的发生顺序不同。例如,两个连续的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这主要根据所涉及的功能而定。

[0091] 另外,在本申请实施例中的各个实施例的各功能模块可以集成在一起形成一个独立的部分,也可以是各个模块单独存在,也可以两个或两个以上模块集成形成一个独立的部分。此外,在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本申请实施例的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外,在不相互矛盾的情况下,本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0092] 在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。

[0093] 以上的描述,仅为本申请实施例的可选实施方式,但本申请实施例的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本申请实施例揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本申请实施例的保护范围之内。

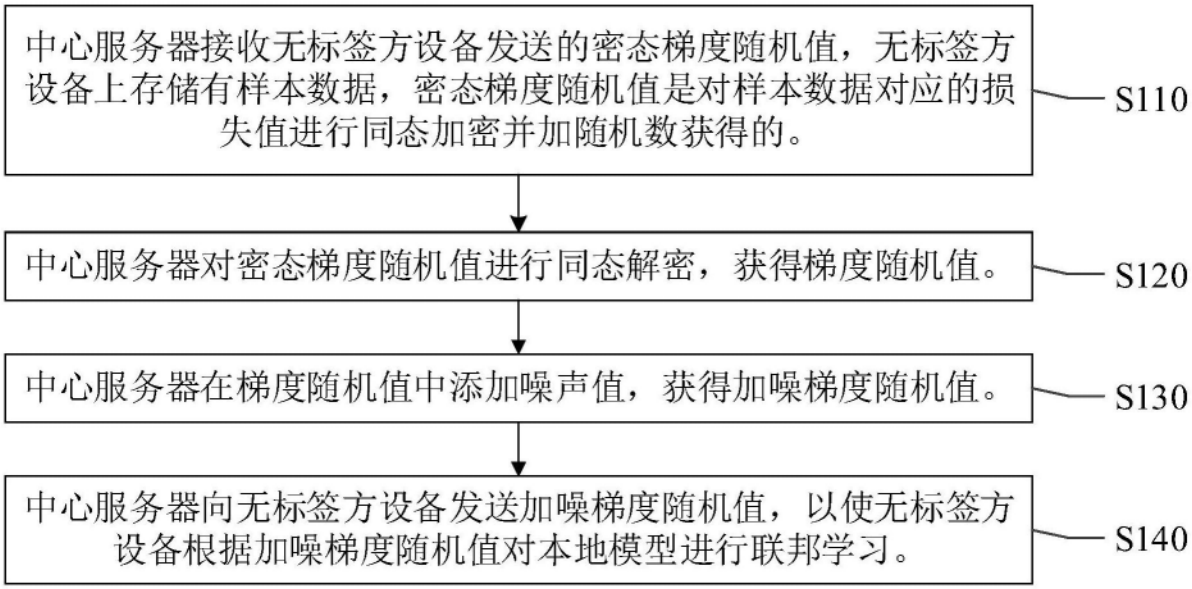

中心服务器接收无标签方设备发送的密态梯度随机值，无标签方设备上存储有样本数据，密态梯度随机值是对样本数据对应的损失值进行同态加密并加随机数获得的。
S110
中心服务器对密态梯度随机值进行同态解密，获得梯度随机值。
S120
中心服务器在梯度随机值中添加噪声值，获得加噪梯度随机值。
S130
中心服务器向无标签方设备发送加噪梯度随机值，以使无标签方设备根据加噪梯度随机值对本地模型进行联邦学习。
S140

图1

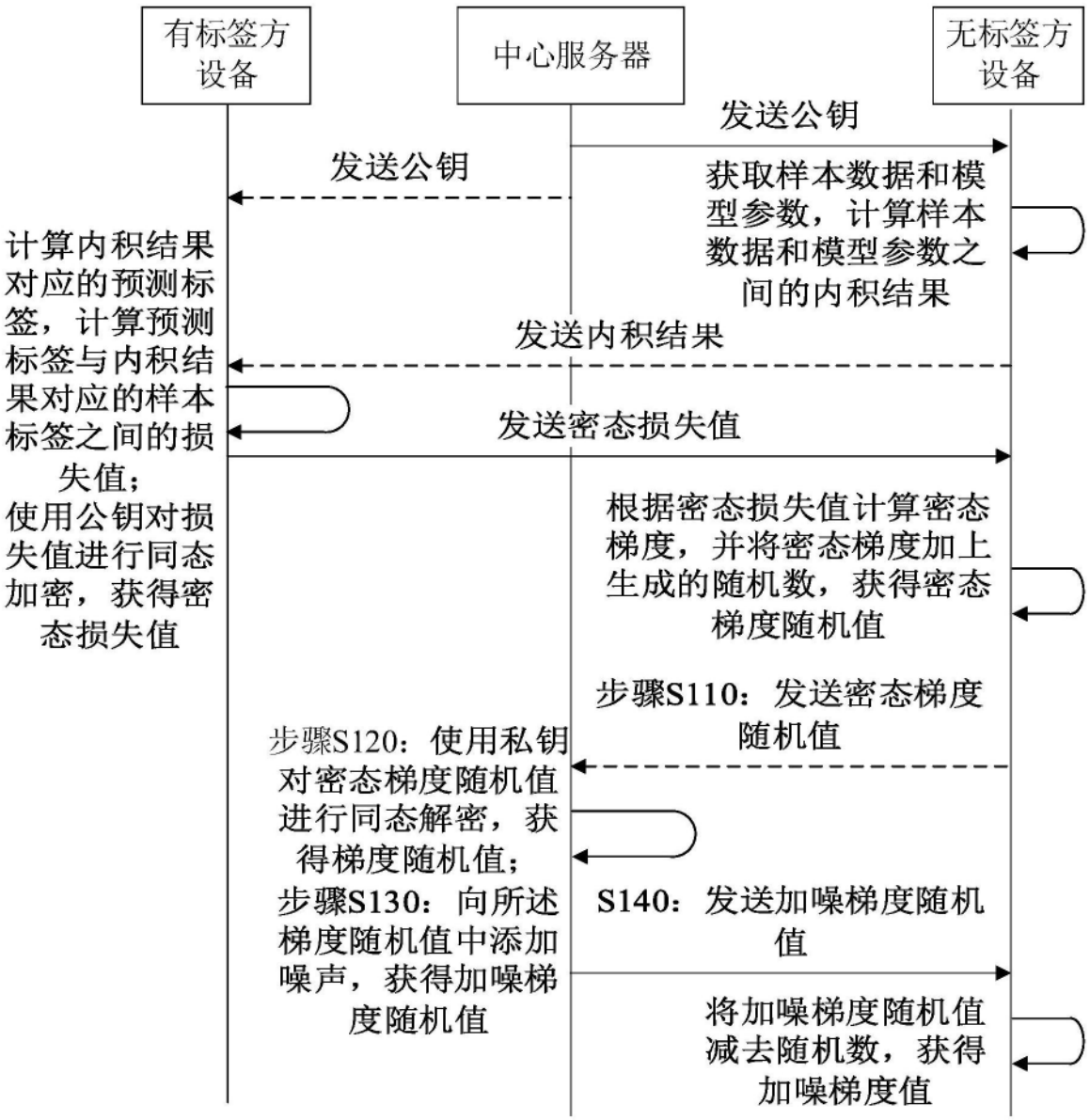

有标签方设备
中心服务器
无标签方设备
发送公钥
发送公钥
获取样本数据和模型参数，计算样本数据和模型参数之间的内积结果
计算内积结果对应的预测标签，计算预测标签与内积结果对应的样本标签之间的损失值；
使用公钥对损失值进行同态加密，获得密态损失值
发送内积结果
发送密态损失值
根据密态损失值计算密态梯度，并将密态梯度加上生成的随机数，获得密态梯度随机值
步骤S110：发送密态梯度随机值
步骤S120：使用私钥对密态梯度随机值进行同态解密，获得梯度随机值；
步骤S130：向所述梯度随机值中添加噪声，获得加噪梯度随机值
S140：发送加噪梯度随机值
将加噪梯度随机值减去随机数，获得加噪梯度值

图2

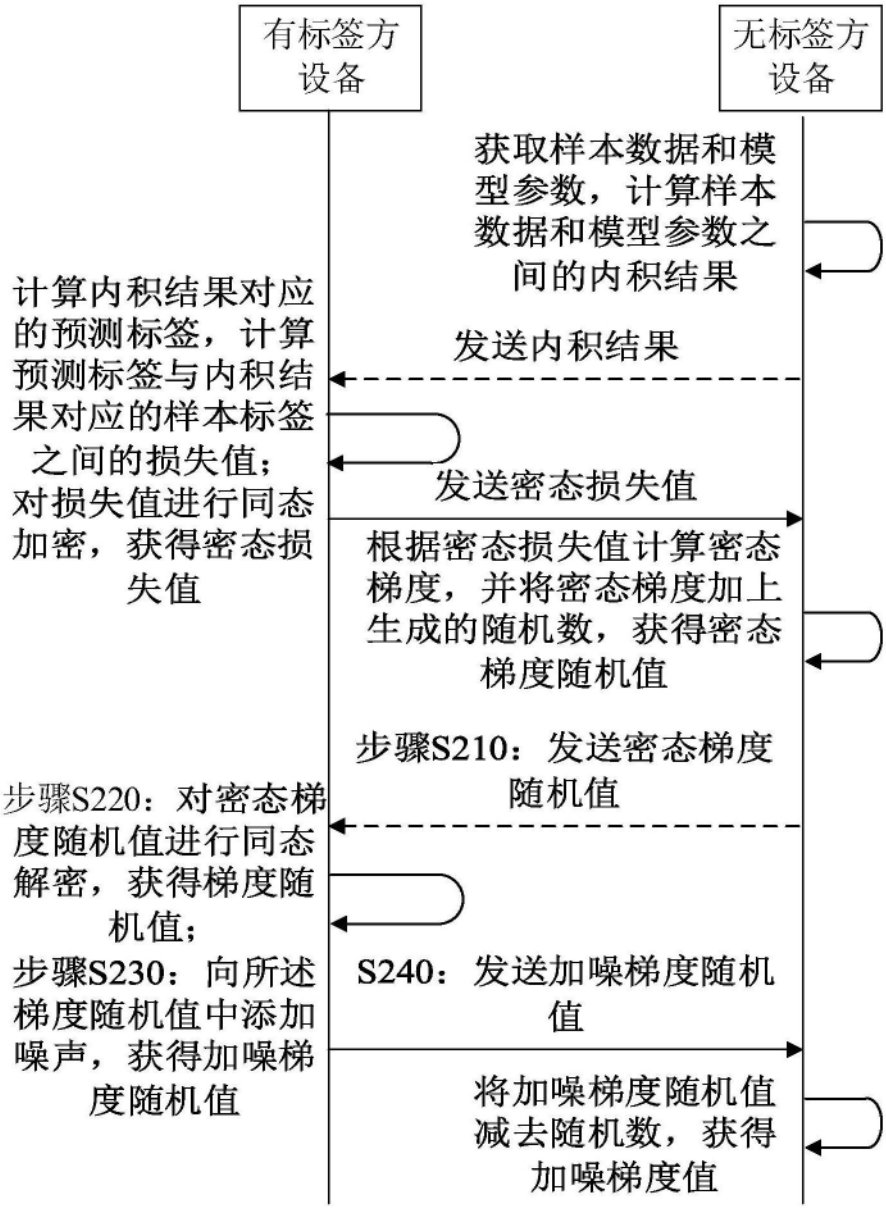

有标签方设备
无标签方设备
获取样本数据和模型参数，计算样本数据和模型参数之间的内积结果
计算内积结果对应的预测标签，计算预测标签与内积结果对应的样本标签之间的损失值；
发送内积结果
对损失值进行同态加密，获得密态损失值
发送密态损失值
根据密态损失值计算密态梯度，并将密态梯度加上生成的随机数，获得密态梯度随机值
步骤S210：发送密态梯度随机值
步骤S220：对密态梯度随机值进行同态解密，获得梯度随机值；
步骤S230：向所述梯度随机值中添加噪声，获得加噪梯度随机值
S240：发送加噪梯度随机值
将加噪梯度随机值减去随机数，获得加噪梯度值

图3

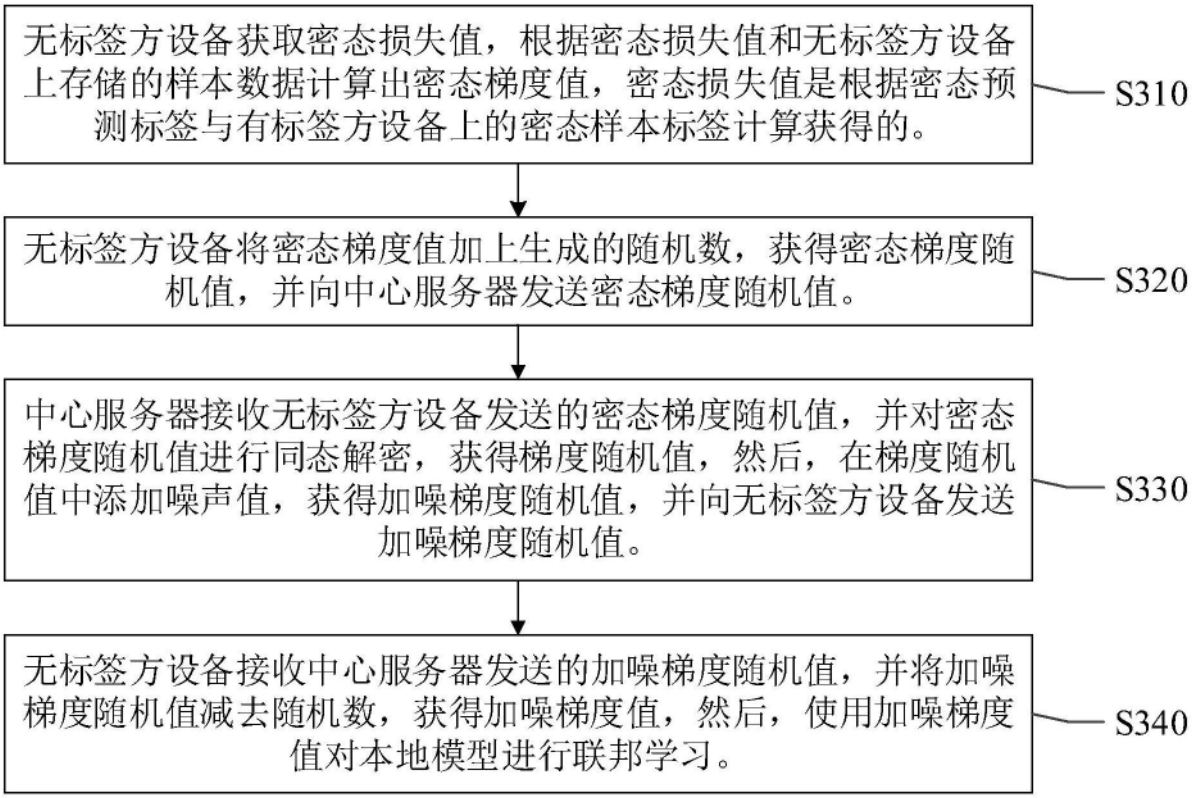

无标签方设备获取密态损失值，根据密态损失值和无标签方设备上存储的样本数据计算出密态梯度值，密态损失值是根据密态预测标签与有标签方设备上的密态样本标签计算获得的。
S310
无标签方设备将密态梯度值加上生成的随机数，获得密态梯度随机值，并向中心服务器发送密态梯度随机值。
S320
中心服务器接收无标签方设备发送的密态梯度随机值，并对密态梯度随机值进行同态解密，获得梯度随机值，然后，在梯度随机值中添加噪声值，获得加噪梯度随机值，并向无标签方设备发送加噪梯度随机值。
S330
无标签方设备接收中心服务器发送的加噪梯度随机值，并将加噪梯度随机值减去随机数，获得加噪梯度值，然后，使用加噪梯度值对本地模型进行联邦学习。
S340

图4

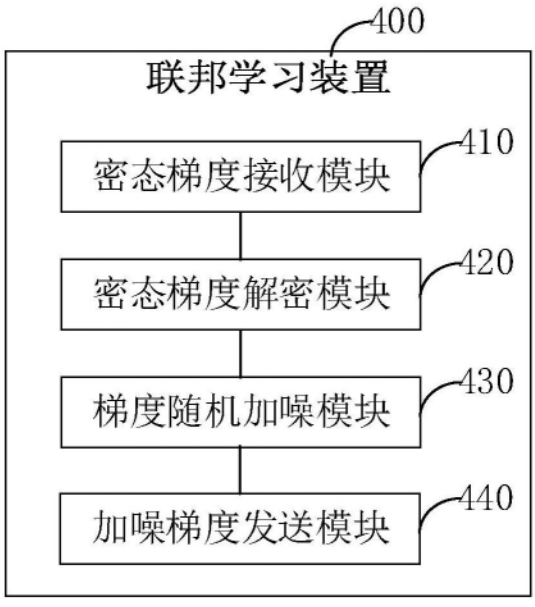

400
联邦学习装置
密态梯度接收模块
410
密态梯度解密模块
420
梯度随机加噪模块
430
加噪梯度发送模块
440

图5

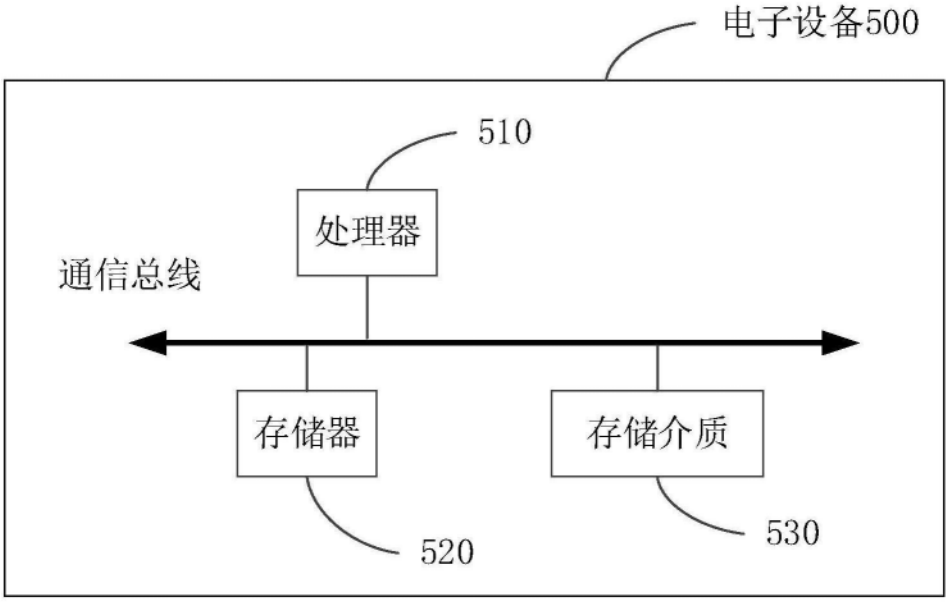


图6