(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 116541870 B
(45)授权公告日 2023.09.05

(21)申请号 202310812593.0

(22)申请日 2023.07.04

(65)同一申请的已公布的文献号
申请公布号 CN 116541870 A

(43)申请公布日 2023.08.04

(73)专利权人 北京富算科技有限公司
地址 102699 北京市大兴区黄村东大街38号院3号楼5层505

(72)发明人 王兆凯 卞阳 尤志强 张伟奇

(74)专利代理机构 北京慧加伦知识产权代理有限公司 16035
专利代理师 李永敏

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

(56)对比文件
CN 114462626 A,2022.05.10
CN 114492850 A,2022.05.13
CN 114547643 A,2022.05.27
WO 2023092792 A1,2023.06.01

审查员 张慧娟

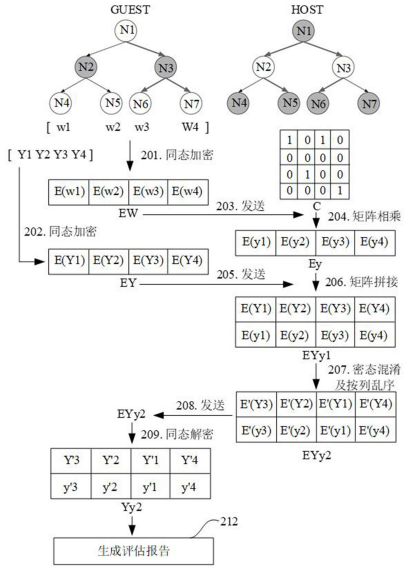
权利要求书3页 说明书15页 附图8页

(54)发明名称

用于评估联邦学习模型的方法及装置

(57)摘要

本公开的实施例提供一种用于评估联邦学习模型的方法及装置。参与联邦学习的第一参与方拥有联邦学习模型的叶子节点的权重矩阵和输入样本的样本标签矩阵。参与联邦学习的第二参与方拥有联邦学习模型根据输入样本生成的预测结果矩阵。该方法由第一参与方执行。该方法包括:对叶子节点的权重矩阵和样本标签矩阵进行同态加密;向第二参与方发送经同态加密的权重矩阵和经同态加密的样本标签矩阵;接收由第二参与方生成的第一矩阵,第一矩阵通过将预测标签矩阵与经同态加密的样本标签矩阵进行按列拼接并执行密态混淆及按列乱序操作来生成,预测标签矩阵为经同态加密的权重矩阵与预测结果矩阵的矩阵乘积;以及对第一矩阵进行同态解密以获得第二矩阵。




CN 116541870 B

1.一种用于评估联邦学习模型的方法,其特征在于,参与联邦学习的第一参与方拥有所述联邦学习模型的叶子节点的权重矩阵和输入样本的样本标签矩阵,参与所述联邦学习的第二参与方拥有所述联邦学习模型根据所述输入样本生成的预测结果矩阵,所述方法由所述第一参与方执行,所述方法包括:

对所述叶子节点的权重矩阵和所述样本标签矩阵进行同态加密;

向所述第二参与方发送经同态加密的权重矩阵和经同态加密的样本标签矩阵;

接收由所述第二参与方生成的第一矩阵,所述第一矩阵通过将预测标签矩阵与所述经同态加密的样本标签矩阵进行按列拼接并执行密态混淆及按列乱序操作来生成,所述预测标签矩阵为所述经同态加密的权重矩阵与所述预测结果矩阵的矩阵乘积;以及

对所述第一矩阵进行同态解密以获得第二矩阵,所述第二矩阵的每列包括一个样本的样本标签和与该样本相对应的预测标签;

其中,所述预测标签矩阵与所述经同态加密的样本标签矩阵被按列拼接成拼接矩阵,对所述拼接矩阵执行密态混淆操作包括:针对所述拼接矩阵中的每个元素,生成随机数并将所生成的随机数与该元素相加。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:根据所述第二矩阵来生成针对所述联邦学习模型的评估报告。

3.根据权利要求1所述的方法,其特征在于,所述方法还包括:

对所述第二矩阵执行按列乱序操作以生成第三矩阵;以及

将所述第三矩阵发送给参与所述联邦学习的另一参与方,以便由所述另一参与方根据所述第三矩阵来生成针对所述联邦学习模型的评估报告,其中,所述另一参与方包括:所述第二参与方,或者第三参与方。

4.一种用于评估联邦学习模型的装置,其特征在于,参与联邦学习的第一参与方拥有所述联邦学习模型的叶子节点的权重矩阵和输入样本的样本标签矩阵,参与所述联邦学习的第二参与方拥有所述联邦学习模型根据所述输入样本生成的预测结果矩阵,所述装置作为所述第一参与方,所述装置包括:

至少一个处理器;以及

存储有计算机程序的至少一个存储器;

其中,当所述计算机程序由所述至少一个处理器执行时,使得所述装置执行根据权利要求1至3中任一项所述的方法的步骤。

5.一种用于评估联邦学习模型的方法,其特征在于,参与联邦学习的第一参与方拥有所述联邦学习模型的叶子节点的权重矩阵和输入样本的样本标签矩阵,参与所述联邦学习的第二参与方拥有所述联邦学习模型根据所述输入样本生成的预测结果矩阵,所述方法由所述第二参与方执行,所述方法包括:

从所述第一参与方接收经同态加密的权重矩阵和经同态加密的样本标签矩阵;

将所述经同态加密的权重矩阵与所述预测结果矩阵进行矩阵相乘以获得预测标签矩阵;

将所述预测标签矩阵与所述经同态加密的样本标签矩阵进行按列拼接以生成拼接矩阵;

对所述拼接矩阵执行密态混淆及按列乱序操作以生成第一矩阵;以及

向所述第一参与方发送所述第一矩阵；

其中，对所述拼接矩阵执行密态混淆操作包括：针对所述拼接矩阵中的每个元素，生成随机数并将所生成的随机数与该元素相加。

6.根据权利要求5所述的方法，其特征在于，对所述拼接矩阵执行密态混淆操作包括：针对所述拼接矩阵中的每个元素，生成随机数并将所生成的随机数与该元素相加。

7.根据权利要求5所述的方法，其特征在于，所述方法还包括：

接收由所述第一参与方生成的第三矩阵，所述第三矩阵通过对所述第一矩阵进行同态解密并执行按列乱序操作来生成，所述第三矩阵的每列包括一个样本的样本标签和与该样本相对应的预测标签；以及

根据所述第三矩阵来生成针对所述联邦学习模型的评估报告。

8.根据权利要求5至7中任一项所述的方法，其特征在于，所述第二参与方通过以下操作来拥有所述预测结果矩阵：

从所述第一参与方接收第一样本索引，所述第一样本索引由所述第一参与方根据所述联邦学习模型的第一节点分裂条件推理获得，所述第一样本索引指示所述输入样本与所述叶子节点的第一预测关系；

根据所述联邦学习模型的第二节点分裂条件推理获得第二样本索引，所述第二样本索引指示所述输入样本与所述叶子节点的第二预测关系；

对所述第一样本索引和所述第二样本索引求交集以获得预测样本索引；以及

将所述预测样本索引转换成矩阵形式以获得所述预测结果矩阵。

9.根据权利要求5至7中任一项所述的方法，其特征在于，所述第二参与方通过以下操作来拥有所述预测结果矩阵：

获得所述第一参与方生成的第一样本索引的第一碎片矩阵，所述第一样本索引由所述第一参与方根据所述联邦学习模型的第一节点分裂条件推理获得，所述第一样本索引指示所述输入样本与所述叶子节点的第一预测关系，所述第一样本索引被转换成第一样本索引矩阵，所述第一样本索引矩阵被碎片化成所述第一碎片矩阵和第二碎片矩阵；

根据所述联邦学习模型的第二节点分裂条件推理获得第二样本索引，所述第二样本索引指示所述输入样本与所述叶子节点的第二预测关系；

将所述第二样本索引转换成矩阵形式以获得第二样本索引矩阵；

将所述第二样本索引矩阵碎片化成第三碎片矩阵和第四碎片矩阵；

获得所述第一参与方根据所述第二碎片矩阵和所述第三碎片矩阵生成的第一中间碎片矩阵和第二中间碎片矩阵，其中，所述第三碎片矩阵由所述第二参与方发送给所述第一参与方或者由所述第一参与方生成；

根据所述第一碎片矩阵和所述第四碎片矩阵生成第三中间碎片矩阵和第四中间碎片矩阵；

向所述第一参与方发送所述第三中间碎片矩阵和所述第四中间碎片矩阵；

获得所述第一参与方根据所述第一中间碎片矩阵、所述第二中间碎片矩阵、所述第三中间碎片矩阵和所述第四中间碎片矩阵生成的第一交集碎片矩阵；

根据所述第一中间碎片矩阵、所述第二中间碎片矩阵、所述第三中间碎片矩阵和所述第四中间碎片矩阵生成第二交集碎片矩阵；以及

将所述第一交集碎片矩阵与所述第二交集碎片矩阵相加以获得所述预测结果矩阵。

10.一种用于评估联邦学习模型的装置,其特征在于,参与联邦学习的第一参与方拥有所述联邦学习模型的叶子节点的权重矩阵和输入样本的样本标签矩阵,参与所述联邦学习的第二参与方拥有所述联邦学习模型根据所述输入样本生成的预测结果矩阵,所述装置作为所述第二参与方,所述装置包括:

至少一个处理器;以及

存储有计算机程序的至少一个存储器;

其中,当所述计算机程序由所述至少一个处理器执行时,使得所述装置执行根据权利要求5至9中任一项所述的方法的步骤。

# 用于评估联邦学习模型的方法及装置

## 技术领域

[0001] 本公开的实施例涉及数据处理技术领域，具体地，涉及用于评估联邦学习模型的方法及装置。

## 背景技术

[0002] 基于XGBoost的联邦学习模型(也可称为XGBoost模型)是常用隐私计算模型之一。如今在许多应用场景中XGBoost模型已被广泛使用，例如金融风控，广告营销，疾病预测等。在银行、电商等公司的应用场景中，往往会采用XGBoost模型来作为主要的机器学习模型。在使用XGBoost模型的过程中，需要对XGBoost模型的模型效果做评估。在对XGBoost模型进行评估时，不应当定位个体信息。如果不能很好保护个体信息，则难以满足合规需求。如何在不暴露个体信息的情况下，获得XGBoost模型的准确评估报告已经成为了重要的研究方向之一。

## 发明内容

[0003] 本文中描述的实施例提供了一种用于评估联邦学习模型的方法、装置以及存储有计算机程序的计算机可读存储介质。

[0004] 根据本公开的第一方面，提供了一种用于评估联邦学习模型的方法。参与联邦学习的第一参与方拥有联邦学习模型的叶子节点的权重矩阵和输入样本的样本标签矩阵。参与联邦学习的第二参与方拥有联邦学习模型根据输入样本生成的预测结果矩阵。该方法由第一参与方执行。该方法包括：对叶子节点的权重矩阵和样本标签矩阵进行同态加密；向第二参与方发送经同态加密的权重矩阵和经同态加密的样本标签矩阵；接收由第二参与方生成的第一矩阵，第一矩阵通过将预测标签矩阵与经同态加密的样本标签矩阵进行按列拼接并执行密态混淆及按列乱序操作来生成，预测标签矩阵为经同态加密的权重矩阵与预测结果矩阵的矩阵乘积；以及对第一矩阵进行同态解密以获得第二矩阵，第二矩阵的每列包括一个样本的样本标签和与该样本相对应的预测标签。

[0005] 在本公开的一些实施例中，该方法还包括：根据第二矩阵来生成针对联邦学习模型的评估报告。

[0006] 在本公开的一些实施例中，该方法还包括：对第二矩阵执行按列乱序操作以生成第三矩阵；以及将第三矩阵发送给第二参与方，以便由第二参与方根据第三矩阵来生成针对联邦学习模型的评估报告。

[0007] 在本公开的一些实施例中，该方法还包括：对第二矩阵执行按列乱序操作以生成第三矩阵；以及将第三矩阵发送给参与联邦学习的第三参与方，以便由第三参与方根据第三矩阵来生成针对联邦学习模型的评估报告。

[0008] 根据本公开的第二方面，提供了一种用于评估联邦学习模型的装置。参与联邦学习的第一参与方拥有联邦学习模型的叶子节点的权重矩阵和输入样本的样本标签矩阵。参与联邦学习的第二参与方拥有联邦学习模型根据输入样本生成的预测结果矩阵。该装置作

为第一参与方。该装置包括至少一个处理器;以及存储有计算机程序的至少一个存储器。当计算机程序由至少一个处理器执行时,使得装置:对叶子节点的权重矩阵和样本标签矩阵进行同态加密;向第二参与方发送经同态加密的权重矩阵和经同态加密的样本标签矩阵;接收由第二参与方生成的第一矩阵,第一矩阵通过将预测标签矩阵与经同态加密的样本标签矩阵进行按列拼接并执行密态混淆及按列乱序操作来生成,预测标签矩阵为经同态加密的权重矩阵与预测结果矩阵的矩阵乘积;以及对第一矩阵进行同态解密以获得第二矩阵,第二矩阵的每列包括一个样本的样本标签和与该样本相对应的预测标签。

[0009] 在本公开的一些实施例中,计算机程序在由至少一个处理器执行时使得装置还:根据第二矩阵来生成针对联邦学习模型的评估报告。

[0010] 在本公开的一些实施例中,计算机程序在由至少一个处理器执行时使得装置还:对第二矩阵执行按列乱序操作以生成第三矩阵;以及将第三矩阵发送给第二参与方,以便由第二参与方根据第三矩阵来生成针对联邦学习模型的评估报告。

[0011] 在本公开的一些实施例中,计算机程序在由至少一个处理器执行时使得装置还:对第二矩阵执行按列乱序操作以生成第三矩阵;以及将第三矩阵发送给参与联邦学习的第三参与方,以便由第三参与方根据第三矩阵来生成针对联邦学习模型的评估报告。

[0012] 根据本公开的第三方面,提供了一种存储有计算机程序的计算机可读存储介质,其中,计算机程序在由处理器执行时实现根据本公开的第一方面所述的方法的步骤。

[0013] 根据本公开的第四方面,提供了一种用于评估联邦学习模型的方法。参与联邦学习的第一参与方拥有联邦学习模型的叶子节点的权重矩阵和输入样本的样本标签矩阵。参与联邦学习的第二参与方拥有联邦学习模型根据输入样本生成的预测结果矩阵。该方法由第二参与方执行。该方法包括:从第一参与方接收经同态加密的权重矩阵和经同态加密的样本标签矩阵;将经同态加密的权重矩阵与预测结果矩阵进行矩阵相乘以获得预测标签矩阵;将预测标签矩阵与经同态加密的样本标签矩阵进行按列拼接以生成拼接矩阵;对拼接矩阵执行密态混淆及按列乱序操作以生成第一矩阵;以及向第一参与方发送第一矩阵。

[0014] 在本公开的一些实施例中,对拼接矩阵执行密态混淆操作包括:针对拼接矩阵中的每个元素,生成随机数并将所生成的随机数与该元素相加。

[0015] 在本公开的一些实施例中,该方法还包括:接收由第一参与方生成的第三矩阵,第三矩阵通过对第一矩阵进行同态解密并执行按列乱序操作来生成,第三矩阵的每列包括一个样本的样本标签和与该样本相对应的预测标签;以及根据第三矩阵来生成针对联邦学习模型的评估报告。

[0016] 在本公开的一些实施例中,第二参与方通过以下操作来拥有预测结果矩阵:从第一参与方接收第一样本索引,第一样本索引由第一参与方根据联邦学习模型的第一节点分裂条件推理获得,第一样本索引指示输入样本与叶子节点的第一预测关系;根据联邦学习模型的第二节点分裂条件推理获得第二样本索引,第二样本索引指示输入样本与叶子节点的第二预测关系;对第一样本索引和第二样本索引求交集以获得预测样本索引;以及将预测样本索引转换成矩阵形式以获得预测结果矩阵。

[0017] 在本公开的一些实施例中,第二参与方通过以下操作来拥有预测结果矩阵:获得第一参与方生成的第一样本索引的第一碎片矩阵,第一样本索引由第一参与方根据联邦学习模型的第一节点分裂条件推理获得,第一样本索引指示输入样本与叶子节点的第一预测

关系，第一样本索引被转换成第一样本索引矩阵，第一样本索引矩阵被碎片化成第一碎片矩阵和第二碎片矩阵；根据联邦学习模型的第二节点分裂条件推理获得第二样本索引，第二样本索引指示输入样本与叶子节点的第二预测关系；将第二样本索引转换成矩阵形式以获得第二样本索引矩阵；将第二样本索引矩阵碎片化成第三碎片矩阵和第四碎片矩阵；获得第一参与方根据第二碎片矩阵和第三碎片矩阵生成的第一中间碎片矩阵和第二中间碎片矩阵，其中，第三碎片矩阵由第二参与方发送给第一参与方；根据第一碎片矩阵和第四碎片矩阵生成第三中间碎片矩阵和第四中间碎片矩阵；向第一参与方发送第三中间碎片矩阵和第四中间碎片矩阵；获得第一参与方根据第一中间碎片矩阵、第二中间碎片矩阵、第三中间碎片矩阵和第四中间碎片矩阵生成的第一交集碎片矩阵；根据第一中间碎片矩阵、第二中间碎片矩阵、第三中间碎片矩阵和第四中间碎片矩阵生成第二交集碎片矩阵；以及将第一交集碎片矩阵与第二交集碎片矩阵相加以获得预测结果矩阵。

[0018] 在本公开的一些实施例中，第二参与方通过以下操作来拥有预测结果矩阵：获得第一参与方生成的第一样本索引的第一碎片矩阵，第一样本索引由第一参与方根据联邦学习模型的第一节点分裂条件推理获得，第一样本索引指示输入样本与叶子节点的第一预测关系，第一样本索引被转换成第一样本索引矩阵，第一样本索引矩阵被碎片化成第一碎片矩阵和第二碎片矩阵；根据联邦学习模型的第二节点分裂条件推理获得第二样本索引，第二样本索引指示输入样本与叶子节点的第二预测关系；将第二样本索引转换成矩阵形式以获得第二样本索引矩阵；将第二样本索引矩阵碎片化成第三碎片矩阵和第四碎片矩阵；获得第一参与方根据第二碎片矩阵和第三碎片矩阵生成的第一中间碎片矩阵和第二中间碎片矩阵，其中，第三碎片矩阵由第一参与方生成；根据第一碎片矩阵和第四碎片矩阵生成第三中间碎片矩阵和第四中间碎片矩阵；向第一参与方发送第三中间碎片矩阵和第四中间碎片矩阵；获得第一参与方根据第一中间碎片矩阵、第二中间碎片矩阵、第三中间碎片矩阵和第四中间碎片矩阵生成的第一交集碎片矩阵；根据第一中间碎片矩阵、第二中间碎片矩阵、第三中间碎片矩阵和第四中间碎片矩阵生成第二交集碎片矩阵；以及将第一交集碎片矩阵与第二交集碎片矩阵相加以获得预测结果矩阵。

[0019] 根据本公开的第五方面，提供了一种用于评估联邦学习模型的装置。参与联邦学习的第一参与方拥有联邦学习模型的叶子节点的权重矩阵和输入样本的样本标签矩阵。参与联邦学习的第二参与方拥有联邦学习模型根据输入样本生成的预测结果矩阵。该装置作为第二参与方。该装置包括至少一个处理器；以及存储有计算机程序的至少一个存储器。当计算机程序由至少一个处理器执行时，使得装置：从第一参与方接收经同态加密的权重矩阵和经同态加密的样本标签矩阵；将经同态加密的权重矩阵与预测结果矩阵进行矩阵相乘以获得预测标签矩阵；将预测标签矩阵与经同态加密的样本标签矩阵进行按列拼接以生成拼接矩阵；对拼接矩阵执行密态混淆及按列乱序操作以生成第一矩阵；以及向第一参与方发送第一矩阵。

[0020] 在本公开的一些实施例中，计算机程序在由至少一个处理器执行时使得装置通过以下操作来对拼接矩阵执行密态混淆操作：针对拼接矩阵中的每个元素，生成随机数并将所生成的随机数与该元素相加。

[0021] 在本公开的一些实施例中，计算机程序在由至少一个处理器执行时使得装置还：接收由第一参与方生成的第三矩阵，第三矩阵通过对第一矩阵进行同态解密并执行按列乱

序操作来生成，第三矩阵的每列包括一个样本的样本标签和与该样本相对应的预测标签；以及根据第三矩阵来生成针对联邦学习模型的评估报告。

[0022] 在本公开的一些实施例中，计算机程序在由至少一个处理器执行时使得装置通过以下操作来拥有预测结果矩阵：从第一参与方接收第一样本索引，第一样本索引由第一参与方根据联邦学习模型的第一节点分裂条件推理获得，第一样本索引指示输入样本与叶子节点的第一预测关系；根据联邦学习模型的第二节点分裂条件推理获得第二样本索引，第二样本索引指示输入样本与叶子节点的第二预测关系；对第一样本索引和第二样本索引求交集以获得预测样本索引；以及将预测样本索引转换成矩阵形式以获得预测结果矩阵。

[0023] 在本公开的一些实施例中，计算机程序在由至少一个处理器执行时使得装置通过以下操作来拥有预测结果矩阵：获得第一参与方生成的第一样本索引的第一碎片矩阵，第一样本索引由第一参与方根据联邦学习模型的第一节点分裂条件推理获得，第一样本索引指示输入样本与叶子节点的第一预测关系，第一样本索引被转换成第一样本索引矩阵，第一样本索引矩阵被碎片化成第一碎片矩阵和第二碎片矩阵；根据联邦学习模型的第二节点分裂条件推理获得第二样本索引，第二样本索引指示输入样本与叶子节点的第二预测关系；将第二样本索引转换成矩阵形式以获得第二样本索引矩阵；将第二样本索引矩阵碎片化成第三碎片矩阵和第四碎片矩阵；获得第一参与方根据第二碎片矩阵和第三碎片矩阵生成的第一中间碎片矩阵和第二中间碎片矩阵，其中，第三碎片矩阵由第二参与方发送给第一参与方；根据第一碎片矩阵和第四碎片矩阵生成第三中间碎片矩阵和第四中间碎片矩阵；向第一参与方发送第三中间碎片矩阵和第四中间碎片矩阵；获得第一参与方根据第一中间碎片矩阵、第二中间碎片矩阵、第三中间碎片矩阵和第四中间碎片矩阵生成的第一交集碎片矩阵；根据第一中间碎片矩阵、第二中间碎片矩阵、第三中间碎片矩阵和第四中间碎片矩阵生成第二交集碎片矩阵；以及将第一交集碎片矩阵与第二交集碎片矩阵相加以获得预测结果矩阵。

[0024] 在本公开的一些实施例中，计算机程序在由至少一个处理器执行时使得装置通过以下操作来拥有预测结果矩阵：获得第一参与方生成的第一样本索引的第一碎片矩阵，第一样本索引由第一参与方根据联邦学习模型的第一节点分裂条件推理获得，第一样本索引指示输入样本与叶子节点的第一预测关系，第一样本索引被转换成第一样本索引矩阵，第一样本索引矩阵被碎片化成第一碎片矩阵和第二碎片矩阵；根据联邦学习模型的第二节点分裂条件推理获得第二样本索引，第二样本索引指示输入样本与叶子节点的第二预测关系；将第二样本索引转换成矩阵形式以获得第二样本索引矩阵；将第二样本索引矩阵碎片化成第三碎片矩阵和第四碎片矩阵；获得第一参与方根据第二碎片矩阵和第三碎片矩阵生成的第一中间碎片矩阵和第二中间碎片矩阵，其中，第三碎片矩阵由第一参与方生成；根据第一碎片矩阵和第四碎片矩阵生成第三中间碎片矩阵和第四中间碎片矩阵；向第一参与方发送第三中间碎片矩阵和第四中间碎片矩阵；获得第一参与方根据第一中间碎片矩阵、第二中间碎片矩阵、第三中间碎片矩阵和第四中间碎片矩阵生成的第一交集碎片矩阵；根据第一中间碎片矩阵、第二中间碎片矩阵、第三中间碎片矩阵和第四中间碎片矩阵生成第二交集碎片矩阵；以及将第一交集碎片矩阵与第二交集碎片矩阵相加以获得预测结果矩阵。

[0025] 根据本公开的第六方面，提供了一种存储有计算机程序的计算机可读存储介质，其中，计算机程序在由处理器执行时实现根据本公开的第四方面所述的方法的步骤。

## 附图说明

[0026] 为了更清楚地说明本公开的实施例的技术方案,下面将对实施例的附图进行简要说明,应当知道,以下描述的附图仅仅涉及本公开的一些实施例,而非对本公开的限制,其中:

[0027] 图1是根据本公开的实施例的联邦学习模型在第一参与方与第二参与方处的示例性存储结构图;

[0028] 图2是根据本公开的实施例的评估联邦学习模型的过程的示意性组合流程图和信令方案;

[0029] 图3是根据本公开的实施例的评估联邦学习模型的过程的另一示意性组合流程图和信令方案;

[0030] 图4是根据本公开的实施例的生成预测结果矩阵的示意性组合流程图和信令方案;

[0031] 图5是根据本公开的实施例的生成预测结果矩阵的另一示意性组合流程图和信令方案;

[0032] 图6是根据本公开的实施例的由第一参与方执行的用于评估联邦学习模型的方法的示意性流程图;

[0033] 图7是根据本公开的实施例的由第二参与方执行的用于评估联邦学习模型的方法的示意性流程图;

[0034] 图8是根据本公开的实施例的作为第一参与方的用于评估联邦学习模型的装置的示意性框图;以及

[0035] 图9是根据本公开的实施例的作为第二参与方的用于评估联邦学习模型的装置的示意性框图。

[0036] 需要注意的是,附图中的元素是示意性的,没有按比例绘制。

## 具体实施方式

[0037] 为了使本公开的实施例的目的、技术方案和优点更加清楚,下面将结合附图,对本公开的实施例的技术方案进行清楚、完整的描述。显然,所描述的实施例是本公开的一部分实施例,而不是全部的实施例。基于所描述的本公开的实施例,本领域技术人员在无需创造性劳动的前提下所获得的所有其它实施例,也都属于本公开保护的范围。

[0038] 除非另外定义,否则在此使用的所有术语(包括技术和科学术语)具有与本公开主题所属领域的技术人员所通常理解的相同含义。进一步将理解的是,诸如在通常使用的词典中定义的那些的术语应解释为具有与说明书上下文和相关技术中它们的含义一致的含义,并且将不以理想化或过于正式的形式来解释,除非在此另外明确定义。另外,诸如“第一”和“第二”的术语仅用于将一个部件(或部件的一部分)与另一个部件(或部件的另一部分)区分开。

[0039] 图1示出根据本公开的实施例的联邦学习模型在第一参与方与第二参与方处的示例性存储结构图。在图1的示例中,第一参与方GUEST为标签拥有方,第二参与方HOST为数据合作方。一般而言,联邦学习中数据合作方的数量可以有多个,但标签拥有方的数量为一个。在图1中以两个参与方为例来进行说明。图1中的第一参与方GUEST和第二参与方HOST拥

有完整的模型节点关系结构。第一参与方GUEST拥有非叶子节点N1和所有叶子节点N4、N5、N6和N7的信息，不拥有非叶子节点N2和N3的信息。第二参与方HOST拥有非叶子节点N2和N3的信息，不拥有非叶子节点N1和任何叶子节点N4、N5、N6和N7的信息。

[0040] 假设有四个输入样本a、b、c和d。四个输入样本a、b、c和d被分别输入第一参与方GUEST的树模型和第二参与方HOST的树模型，并在每个树模型上都进行了路径推理。在图1的示例中，第一参与方GUEST的预测结果是：叶子节点N4有输入样本a和c，叶子节点N5有输入样本a和c，叶子节点N6有输入样本b和d，叶子节点N7有输入样本b和d。第二参与方HOST的预测结果是：叶子节点N4有输入样本a、b、c和d，叶子节点N5没有输入样本，叶子节点N6有输入样本a和b，叶子节点N7有输入样本c和d。

[0041] 第一参与方GUEST拥有的叶子节点N4、N5、N6和N7的信息包括：叶子节点N4、N5、N6和N7的权重。叶子节点N4、N5、N6和N7的权重可按照叶子节点的编号顺序来组成权重矩阵。第一参与方GUEST还拥有输入样本的样本标签。输入样本的样本标签可按照输入样本的输入顺序组成样本标签矩阵。第二参与方HOST拥有联邦学习模型根据输入样本生成的预测结果矩阵。预测结果矩阵根据第一参与方GUEST的预测结果与第二参与方HOST的预测结果的交集来生成。在本公开的实施例中，预测结果矩阵的每一行对应一个叶子节点，预测结果矩阵的每一列对应一个样本。

[0042] 在本文中以XGBoost模型为例来进行说明。本领域技术人员应理解图1中的存储结构只是示例性的，本公开的实施例不限制联邦学习模型在各参与方处的存储结构。

[0043] 图2示出根据本公开的实施例的评估联邦学习模型的过程的示意性组合流程图和信令方案。在图2的示例中，由第一参与方GUEST来生成针对联邦学习模型的评估报告。

[0044] 第一参与方GUEST拥有叶子节点的权重矩阵[w1 w2 w3 w4]。其中，w1表示叶子节点N4的权重。w2表示叶子节点N5的权重。w3表示叶子节点N6的权重。w4表示叶子节点N7的权重。第二参与方HOST拥有预测结果矩阵C。输入样本a、b、c和d的样本标签矩阵被表示为[Y1 Y2 Y3 Y4]。其中，Y1表示输入样本a的样本标签。Y2表示输入样本b的样本标签。Y3表示输入样本c的样本标签。Y4表示输入样本d的样本标签。

[0045] 第一参与方GUEST在动作201处对叶子节点的权重矩阵[w1 w2 w3 w4]进行同态加密，以获得经同态加密的权重矩阵EW =[E(w1)E(w2) E(w3) E(w4)]。第一参与方GUEST在动作202处对样本标签矩阵[Y1 Y2 Y3 Y4]进行同态加密，以获得经同态加密的样本标签矩阵EY=[E(Y1) E(Y2) E(Y3) E(Y4)]。动作202可与动作201并行地执行，也可以先于动作201执行。

[0046] 第一参与方GUEST在动作203处向第二参与方HOST发送经同态加密的权重矩阵EW。然后，第二参与方HOST在动作204处将经同态加密的权重矩阵EW与预测结果矩阵C进行矩阵相乘以获得预测标签矩阵Ey=EW×C=[E(y1) E(y2) E(y3) E(y4)]。其中，y1表示输入样本a的预测标签。y2表示输入样本b的预测标签。y3表示输入样本c的预测标签。y4表示输入样本d的预测标签。“预测标签”表示联邦学习模型对输入样本进行预测获得的标签。

[0047] 第一参与方GUEST在动作205处向第二参与方HOST发送经同态加密的样本标签矩阵EY。动作205可与动作203并行地执行，也可以先于动作203执行。动作205还可以在动作203之后且在动作204之前执行。

[0048] 第二参与方HOST在动作206处将预测标签矩阵Ey与经同态加密的样本标签矩阵EY

进行按列拼接以生成拼接矩阵EYy1：

[0049] $$EYy1=\begin{bmatrix}E(Y1) & E(Y2) & E(Y3) & E(Y4)\\ E(y1) & E(y2) & E(y3) & E(y4)\end{bmatrix}。$$

[0050] 其中，拼接矩阵的每列包括一个样本的经同态加密的样本标签和与该样本相对应的经同态加密的预测标签。

[0051] 为了使得个体预测结果不被泄露，第二参与方HOST在动作207处对拼接矩阵EYy1执行密态混淆及按列乱序(Shuffle)操作以生成第一矩阵EYy2：

[0052] $$EYy2=\begin{bmatrix}E'(Y3) & E'(Y2) & E'(Y1) & E'(Y4)\\ E'(y3) & E'(y2) & E'(y1) & E'(y4)\end{bmatrix}。$$

[0053] 在对拼接矩阵EYy1执行密态混淆操作的过程中，针对拼接矩阵中的每个元素，生成随机数并将所生成的随机数与该元素相加。在本公开的一些实施例中，随机数远小于拼接矩阵中的元素。随机数的量级例如是$1e^{-10}$，因此不会影响预测标签和样本标签的数据准确性。对拼接矩阵EYy1执行密态混淆的目的是在拼接矩阵EYy1上加入随机扰动以消除密文对应关系，以免第一参与方GUEST根据密文对应关系推测出样本顺序。

[0054] 经过乱序处理的第一矩阵的每列仍然包括一个样本的经同态加密的样本标签和与该样本相对应的经同态加密的预测标签，只是不能够根据列号来确定该列对应哪个样本。

[0055] 第二参与方HOST在动作208处向第一参与方GUEST发送第一矩阵EYy2。第一参与方GUEST在动作209处对第一矩阵EYy2进行同态解密以获得第二矩阵Yy2：

[0056] $$Yy2=\begin{bmatrix}Y'3 & Y'2 & Y'1 & Y'4\\ y'3 & y'2 & y'1 & y'4\end{bmatrix}。$$

[0057] 由于在拼接矩阵EYy1中的每个元素上增加的随机数非常小，因此可以认为

$$Yy2=\begin{bmatrix}Y3 & Y2 & Y1 & Y4\\ y3 & y2 & y1 & y4\end{bmatrix}。$$

[0058] 第二矩阵Yy2的每列包括一个样本的样本标签和与该样本相对应的预测标签。这样，第一参与方GUEST知道每个样本的样本标签和与该样本相对应的预测标签，但是不知道哪个样本标签对应哪个样本，也不知道预测结果矩阵C(即不知道第一参与方GUEST的预测结果与第二参与方HOST的预测结果的交集)，因此可避免个体预测结果泄露。第二参与方HOST不知道样本标签和预测标签的值，仅仅只能获得加密状态的标签信息(加密状态的样本标签矩阵EY和加密状态的预测标签矩阵C)。由于第二参与方HOST无法对加密状态的标签信息进行解密，所以无法定位个体预测结果，进而保护了预测标签信息和样本标签信息。

[0059] 第一参与方GUEST在动作212处根据第二矩阵Yy2来生成针对联邦学习模型的评估报告。

[0060] 在本公开的一些实施例中，对于二分类场景，针对联邦学习模型的评估报告可包括：评估指标KS(Kolmogorov-Smirnov)和AUC(Area Under the Curve)。

[0061] KS被计算为：

[0062] $$KS = MAX(\frac{TP}{TP+FN} - \frac{FP}{FP+TN}) \quad (1)$$

[0063] 将样本预测值(预测标签对应的值)逐一作为阈值,计算TP、FP、FN和TN,最终求最大值得到KS值。其中,TP表示被联邦学习模型预测为正类的正样本,TN表示被联邦学习模型预测为负类的负样本,FP表示被联邦学习模型预测为正类的负样本,FN表示被联邦学习模型预测为负类的正样本。

[0064] AUC被计算为:

[0065] $$AUC = \frac{\sum_{i \in PositiveClass} rank_i - \frac{M*(1+M)}{2}}{M*N} \quad (2)$$

[0066] 其中,$rank_i$为正样本按照概率排序后的位置值,M为正样本个数,N为负样本个数。

[0067] 在本公开的一些实施例中,对于多分类场景,针对联邦学习模型的评估报告可包括:评估指标F1, Accuracy, Precision, Recall。

[0068] 先计算单个类别的评估指标F1、Accuracy、Precision和Recall,其中i为类别序号, n为类别个数。

[0069] $$Precision_i = \frac{TP_i}{TP_i + FP_i} \quad (3)$$

[0070] $$Recall_i = \frac{TP_i}{TP_i + FN_i} \quad (4)$$

[0071] $$F1_i = 2 * \frac{Precision_i * Recall_i}{Precision_i + Recall_i} \quad (5)$$

[0072] $$Accuracy_i = \frac{TP_i + TN_i}{TP_i + TN_i + FP_i + FN_i} \quad (6)$$

[0073] 多分类指标计算还区分macro,micro,weighted。假设评估报告取macro 公式进行计算,多个类别汇总的macro公式被表示为:

[0074] $$macroPrecision = \frac{\sum_{n=i} Precision_i}{n} \quad (7)$$

[0075] $$macroPrecision = \frac{\sum_{n=i} Precision_i}{n} \quad (8)$$

[0076] $$macroRecall = \frac{\sum_{n=i} Recall_i}{n} \quad (9)$$

[0077] $$macroF1 = \frac{\sum_{n=i} F1_i}{n} \quad (10)$$

[0078] 在图2的示例的替代实施例中，可由第二参与方HOST来生成针对联邦学习模型的评估报告。图3示出这种情况下的评估联邦学习模型的过程的示意性组合流程图和信令方案。在图2的示例的基础上，第一参与方GUEST在动作209处对第一矩阵EYy2进行同态解密以获得第二矩阵Yy2后，第一参与方GUEST在动作310处对第二矩阵Yy2进行按列乱序操作以生成第三矩阵Yy3：

[0079] $$Yy3=\begin{bmatrix} Y4 & Y2 & Y1 & Y3 \\ y4 & y2 & y1 & y3 \end{bmatrix}。$$

[0080] 第一参与方GUEST在动作311处将第三矩阵Yy3发送给第二参与方HOST。第二参与方HOST在动作312处根据第三矩阵Yy3来生成针对联邦学习模型的评估报告。第三矩阵Yy3包括一个样本的样本标签和与该样本相对应的预测标签。这样，第二参与方HOST知道每个样本的样本标签和与该样本相对应的预测标签，但是不知道哪个样本标签对应哪个样本，因此可避免个体预测结果泄露。

[0081] 在图2和图3的示例的替代实施例中，如果联邦学习中数据合作方的数量有多个，则也可由参与联邦学习的第三参与方(未示出)来生成针对联邦学习模型的评估报告。第三参与方是数据合作方，但不是交集聚合方。在该替代实施例中，在图3的基础上，第一参与方GUEST可将第三矩阵Yy3发送给参与联邦学习的第三参与方，以便由第三参与方根据第三矩阵Yy3来生成针对联邦学习模型的评估报告。这样，第三参与方知道每个样本的样本标签和与该样本相对应的预测标签，但是不知道哪个样本标签对应哪个样本，也不知道预测结果矩阵C(即不知道第一参与方GUEST的预测结果与第二参与方HOST的预测结果的交集)，因此可避免个体预测结果泄露。由于第二参与方HOST也不知道哪个样本标签对应哪个样本，因此向第三参与方发送经过按列乱序操作的第三矩阵Yy3而非第二矩阵Yy2能够避免第三参与方与第二参与方HOST合谋来确定个体预测结果。

[0082] 本公开的实施例能够分别在基于低带宽和基于MPC(Multi-Party Computation)高带宽的应用场景下使用联邦学习模型来进行联合预测。基于低带宽的预测方案有较高的计算性能，在半诚实场景下，可安全运行。基于MPC高带宽的预测方案则有更强的安全性保障。图4示出基于低带宽的预测方案。图5示出基于MPC高带宽的预测方案。

[0083] 在图4的示例中，第一参与方GUEST在动作441处根据联邦学习模型的第一节点分裂条件推理生成第一样本索引[[a, c][a, c] [b, d][b, d] ]。第一样本索引指示输入样

本a、b、c和d与叶子节点N4、N5、N6和N7的第一预测关系。在图4的示例中，第一节点分裂条件由非叶子节点N1和所有叶子节点N4、N5、N6和N7的节点分裂条件来组成。第一预测关系指示：叶子节点N4有输入样本a和c，叶子节点N5有输入样本a和c，叶子节点N6有输入样本b和d，叶子节点N7有输入样本b和d。

[0084] 第一参与方GUEST在动作442处向第二参与方HOST发送第一样本索引[[a, c] [a, c][b, d][b, d] ]。

[0085] 第二参与方HOST在动作443处根据联邦学习模型的第二节点分裂条件推理获得第二样本索引[[a, b, c, d] [ ][a, b] [c, d]]。第二样本索引指示输入样本a、b、c和d与叶子节点N4、N5、N6和N7的第二预测关系。在图4的示例中，第二节点分裂条件由非叶子节点N2和N3的节点分裂条件来组成。第二预测关系指示：叶子节点N4有输入样本a、b、c和d，叶子节点N5没有输入样本，叶子节点N6有输入样本a和b，叶子节点N7有输入样本c和d。

[0086] 动作443可与动作441或动作442并行地执行，也可以在动作441或动作442之前执行。

[0087] 第二参与方HOST在动作444处对第一样本索引和第二样本索引求交集以获得预测样本索引[[a, c] [ ][b] [d]]。然后，第二参与方HOST在动作445处将预测样本索引[[a, c][ ] [b][d] ]转换成矩阵形式以获得预测结果矩阵C。在本公开的实施例中，预测结果矩阵C的每一行对应一个叶子节点，预测结果矩阵的每一列对应一个样本标签。在图4的示例中，预测结果矩阵C表示：叶子节点N4有输入样本a和c(第一行对应叶子节点N4，第一行的第一列和第三列为1，其余列为0)，叶子节点N5没有输入样本(第二行对应叶子节点N5，第二行的每列都为0)，叶子节点N6有输入样本b(第三行对应叶子节点N6，第三行的第二列为1，其余列为0)，叶子节点N7有输入样本d(第四行对应叶子节点N7，第四行的第四列为1，其余列为0)。

[0088] 在图5的示例中，第一参与方GUEST根据联邦学习模型的第一节点分裂条件推理生成第一样本索引[[a, c] [a, c][b, d] [b, d]]并在动作551处将第一样本索引[[a, c] [a, c][b, d] [b, d]]转换成矩阵形式，以获得第一样本索引矩阵P。

[0089] 第二参与方HOST根据联邦学习模型的第二节点分裂条件推理生成第二样本索引[[a, b, c, d][ ] [a, b][c, d] ]并在动作552处将第二样本索引[[a, b, c, d] [ ][a, b] [c, d]]转换成矩阵形式，以获得第二样本索引矩阵Q。

[0090] 第一参与方GUEST在动作553处将第一样本索引矩阵P碎片化成第一碎片矩阵p2和第二碎片矩阵p1。例如，可随机生成第一碎片矩阵p2，然后根据p1=P-p2来计算p1。

[0091] 第二参与方HOST在动作554处将第二样本索引矩阵Q碎片化成第三碎片矩阵q1和第四碎片矩阵q2。例如，可随机生成第三碎片矩阵q1，然后根据q2=Q-q1来计算q2。

[0092] 动作553可与动作552或动作554并行地执行，也可以在动作552或动作554之前执行。动作554可与动作551或动作553并行地执行，也可以在动作551或动作553之前执行。

[0093] 在动作555处，第一参与方GUEST与第二参与方HOST共享第一碎片矩阵p2，第二参与方HOST与第一参与方GUEST共享第三碎片矩阵q1。

[0094] 第一参与方GUEST在动作556处根据第二碎片矩阵p1和第三碎片矩阵q1生成第一中间碎片矩阵f1和第二中间碎片矩阵e1。在本公开的一些实施例中，第一参与方GUEST可预先生成三元组碎片矩阵<a1, b1, c1>。第一参与方GUEST可根据第二碎片矩阵p1、第三碎片

矩阵q1和三元组碎片矩阵<a1, b1, c1>来生成第一中间碎片矩阵f1和第二中间碎片矩阵e1。其中,f1= p1-a1,e1=q1-b1。

[0095] 第二参与方HOST在动作557处根据第一碎片矩阵p2和第四碎片矩阵q2生成第三中间碎片矩阵f2和第四中间碎片矩阵e2。在本公开的一些实施例中,第二参与方HOST可预先生成三元组碎片矩阵<a2, b2, c2>。第二参与方HOST可根据第一碎片矩阵p2、第四碎片矩阵q2和三元组碎片矩阵<a2, b2, c2>来生成第三中间碎片矩阵f2和第四中间碎片矩阵e2。其中,f2= p2-a2,e2=q2-b2。(a1 + a2) × (b1 + b2) = (c1 + c2)。

[0096] 在动作558处,第一参与方GUEST与第二参与方HOST共享(向第二参与方HOST发送)第一中间碎片矩阵f1和第二中间碎片矩阵e1,第二参与方HOST与第一参与方GUEST(向第一参与方GUEST发送)共享第三中间碎片矩阵f2和第四中间碎片矩阵e2。

[0097] 第一参与方GUEST在动作559处根据第一中间碎片矩阵f1、第二中间碎片矩阵e1、第三中间碎片矩阵f2和第四中间碎片矩阵e2生成第一交集碎片矩阵z1。在一个示例中,z1= e×f+a1×f+b1×e+c1,其中,f=f1+f2,e=e1+e2。

[0098] 第二参与方HOST在动作560处根据第一中间碎片矩阵f1、第二中间碎片矩阵e1、第三中间碎片矩阵f2和第四中间碎片矩阵e2生成第二交集碎片矩阵z2。在一个示例中,z2= a2×f+b2×e+c2,其中,f=f1+f2,e=e1+e2。

[0099] 第一参与方GUEST在动作561处向第二参与方HOST发送第一交集碎片矩阵z1。第二参与方HOST在动作562处将第一交集碎片矩阵z1与第二交集碎片矩阵z2相加以获得预测结果矩阵C。

[0100] 通过对第一参与方GUEST和第二参与方HOST的预测结果执行碎片化操作,并只共享预测结果的一部分(碎片),第一参与方GUEST和第二参与方HOST都不知道对方的预测结果,因此有更强的安全性保障。

[0101] 在图5的示例的替代实施例中,在动作555处,第一参与方GUEST与第二参与方HOST不共享第一碎片矩阵p2和第三碎片矩阵q1。第一参与方GUEST与第二参与方HOST可先执行DH密钥交换,然后共享随机种子。接着,第一参与方GUEST和第二参与方HOST根据共享的随机种子分别生成第三碎片矩阵q1和第一碎片矩阵p2。这样可以减少第一参与方GUEST与第二参与方HOST的数据交换量,从而节约网络资源。

[0102] 图6示出根据本公开的实施例的由第一参与方执行的用于评估联邦学习模型的方法600的示意性流程图。参与联邦学习的第一参与方拥有联邦学习模型的叶子节点的权重矩阵和输入样本的样本标签矩阵。参与联邦学习的第二参与方拥有联邦学习模型根据输入样本生成的预测结果矩阵。

[0103] 在框S602处,第一参与方对叶子节点的权重矩阵和样本标签矩阵进行同态加密。

[0104] 在框S604处,第一参与方向第二参与方发送经同态加密的权重矩阵和经同态加密的样本标签矩阵。

[0105] 在框S606处,第一参与方接收由第二参与方生成的第一矩阵。第一矩阵通过将预测标签矩阵与经同态加密的样本标签矩阵进行按列拼接并执行密态混淆及按列乱序操作来生成。预测标签矩阵为经同态加密的权重矩阵与预测结果矩阵的矩阵乘积。

[0106] 在框S608处,第一参与方对第一矩阵进行同态解密以获得第二矩阵。第二矩阵的每列包括一个样本的样本标签和与该样本相对应的预测标签。

[0107] 在本公开的一些实施例中，该第一参与方根据第二矩阵来生成针对联邦学习模型的评估报告。

[0108] 在本公开的一些替代实施例中，第一参与方对第二矩阵执行按列乱序操作以生成第三矩阵，然后将第三矩阵发送给第二参与方，以便由第二参与方根据第三矩阵来生成针对联邦学习模型的评估报告。

[0109] 在本公开的一些替代实施例中，第一参与方将第二矩阵发送给参与联邦学习的第三参与方，以便由第三参与方根据第二矩阵来生成针对联邦学习模型的评估报告。

[0110] 图7示出根据本公开的实施例的由第二参与方执行的用于评估联邦学习模型的方法700的示意性流程图。参与联邦学习的第一参与方拥有联邦学习模型的叶子节点的权重矩阵和输入样本的样本标签矩阵。参与联邦学习的第二参与方拥有联邦学习模型根据输入样本生成的预测结果矩阵。

[0111] 在框S702处，第二参与方从第一参与方接收经同态加密的权重矩阵和经同态加密的样本标签矩阵。

[0112] 在框S704处，第二参与方将经同态加密的权重矩阵与预测结果矩阵进行矩阵相乘以获得预测标签矩阵。

[0113] 在框S706处，第二参与方将预测标签矩阵与经同态加密的样本标签矩阵进行按列拼接以生成拼接矩阵。

[0114] 在框S708处，第二参与方对拼接矩阵执行密态混淆及按列乱序操作以生成第一矩阵。

[0115] 在框S710处，第二参与方向第一参与方发送第一矩阵。

[0116] 在本公开的一些实施例中，第二参与方接收由第一参与方生成的第三矩阵。第三矩阵通过对第一矩阵进行同态解密并执行按列乱序操作来生成。第三矩阵的每列包括一个样本的样本标签和与该样本相对应的预测标签。然后，第二参与方根据第三矩阵来生成针对联邦学习模型的评估报告。

[0117] 图8示出根据本公开的实施例的作为第一参与方的用于评估联邦学习模型的装置800的示意性框图。如图8所示，该装置800可包括处理器810和存储有计算机程序的存储器820。当计算机程序由处理器810执行时，使得装置800可执行如图6所示的方法600的步骤。在一个示例中，装置800可以是计算机设备或云计算节点等。装置800可对叶子节点的权重矩阵和样本标签矩阵进行同态加密。装置800可向第二参与方发送经同态加密的权重矩阵和经同态加密的样本标签矩阵。装置800可接收由第二参与方生成的第一矩阵。第一矩阵通过将预测标签矩阵与经同态加密的样本标签矩阵进行按列拼接并执行密态混淆及按列乱序操作来生成。预测标签矩阵为经同态加密的权重矩阵与预测结果矩阵的矩阵乘积。装置800可对第一矩阵进行同态解密以获得第二矩阵。第二矩阵的每列包括一个样本的样本标签和与该样本相对应的预测标签。

[0118] 在本公开的一些实施例中，装置800可根据第二矩阵来生成针对联邦学习模型的评估报告。

[0119] 在本公开的一些实施例中，装置800可对第二矩阵执行按列乱序操作以生成第三矩阵。装置800可将第三矩阵发送给第二参与方，以便由第二参与方根据第三矩阵来生成针对联邦学习模型的评估报告。

[0120] 在本公开的一些实施例中，装置800可将第二矩阵发送给参与联邦学习的第三参与方，以便由第三参与方根据第二矩阵来生成针对联邦学习模型的评估报告。

[0121] 在本公开的实施例中，处理器810可以是例如中央处理单元(CPU)、微处理器、数字信号处理器(DSP)、基于多核的处理器架构的处理器等。存储器820可以是使用数据存储技术实现的任何类型的存储器，包括但不限于随机存取存储器、只读存储器、基于半导体的存储器、闪存、磁盘存储器等。

[0122] 此外，在本公开的实施例中，装置800也可包括输入设备830，例如键盘、鼠标等，用于输入多个输入样本。另外，装置800还可包括输出设备840，例如显示器等，用于输出评估报告。

[0123] 图9示出根据本公开的实施例的作为第二参与方的用于评估联邦学习模型的装置900的示意性框图。如图9所示，该装置900可包括处理器910和存储有计算机程序的存储器920。当计算机程序由处理器910执行时，使得装置900可执行如图7所示的方法700的步骤。在一个示例中，装置900可以是计算机设备或云计算节点等。装置900可从第一参与方接收经同态加密的权重矩阵和经同态加密的样本标签矩阵。装置900可将经同态加密的权重矩阵与预测结果矩阵进行矩阵相乘以获得预测标签矩阵。装置900可将预测标签矩阵与经同态加密的样本标签矩阵进行按列拼接以生成拼接矩阵。装置900可对拼接矩阵执行密态混淆及按列乱序操作以生成第一矩阵。装置900可向第一参与方发送第一矩阵。

[0124] 在本公开的一些实施例中，装置900可接收由第一参与方生成的第三矩阵。第三矩阵通过对第一矩阵进行同态解密并执行按列乱序操作来生成。第三矩阵的每列包括一个样本的样本标签和与该样本相对应的预测标签。装置900可根据第三矩阵来生成针对联邦学习模型的评估报告。

[0125] 在本公开的一些实施例中，装置900可从第一参与方接收第一样本索引。第一样本索引由第一参与方根据联邦学习模型的第一节点分裂条件推理获得。第一样本索引指示输入样本与叶子节点的第一预测关系。装置900可根据联邦学习模型的第二节点分裂条件推理获得第二样本索引。第二样本索引指示输入样本与叶子节点的第二预测关系。装置900可对第一样本索引和第二样本索引求交集以获得预测样本索引。装置900可将预测样本索引转换成矩阵形式以获得预测结果矩阵。

[0126] 在本公开的一些实施例中，装置900可获得第一参与方生成的第一样本索引的第一碎片矩阵。第一样本索引由第一参与方根据联邦学习模型的第一节点分裂条件推理获得。第一样本索引指示输入样本与叶子节点的第一预测关系。第一样本索引被转换成第一样本索引矩阵。第一样本索引矩阵被碎片化成第一碎片矩阵和第二碎片矩阵。装置900可根据联邦学习模型的第二节点分裂条件推理获得第二样本索引。第二样本索引指示输入样本与叶子节点的第二预测关系。装置900可将第二样本索引转换成矩阵形式以获得第二样本索引矩阵。装置900可将第二样本索引矩阵碎片化成第三碎片矩阵和第四碎片矩阵。装置900可获得第一参与方根据第二碎片矩阵和第三碎片矩阵生成的第一中间碎片矩阵和第二中间碎片矩阵。其中，第三碎片矩阵由第二参与方发送给第一参与方。装置900可根据第一碎片矩阵和第四碎片矩阵生成第三中间碎片矩阵和第四中间碎片矩阵。装置900可向第一参与方发送第三中间碎片矩阵和第四中间碎片矩阵。装置900可获得第一参与方根据第一中间碎片矩阵、第二中间碎片矩阵、第三中间碎片矩阵和第四中间碎片矩阵生成的第一交

集碎片矩阵。装置900可根据第一中间碎片矩阵、第二中间碎片矩阵、第三中间碎片矩阵和第四中间碎片矩阵生成第二交集碎片矩阵。装置900可将第一交集碎片矩阵与第二交集碎片矩阵相加以获得预测结果矩阵。

[0127] 在本公开的一些实施例中，装置900可获得第一参与方生成的第一样本索引的第一碎片矩阵。第一样本索引由第一参与方根据联邦学习模型的第一节点分裂条件推理获得。第一样本索引指示输入样本与叶子节点的第一预测关系。第一样本索引被转换成第一样本索引矩阵。第一样本索引矩阵被碎片化成第一碎片矩阵和第二碎片矩阵。装置900可根据联邦学习模型的第二节点分裂条件推理获得第二样本索引。第二样本索引指示输入样本与叶子节点的第二预测关系。装置900可将第二样本索引转换成矩阵形式以获得第二样本索引矩阵。装置900可将第二样本索引矩阵碎片化成第三碎片矩阵和第四碎片矩阵。装置900可获得第一参与方根据第二碎片矩阵和第三碎片矩阵生成的第一中间碎片矩阵和第二中间碎片矩阵。其中，第三碎片矩阵由第一参与方生成。装置900可根据第一碎片矩阵和第四碎片矩阵生成第三中间碎片矩阵和第四中间碎片矩阵。装置900可向第一参与方发送第三中间碎片矩阵和第四中间碎片矩阵。装置900可获得第一参与方根据第一中间碎片矩阵、第二中间碎片矩阵、第三中间碎片矩阵和第四中间碎片矩阵生成的第一交集碎片矩阵。装置900可根据第一中间碎片矩阵、第二中间碎片矩阵、第三中间碎片矩阵和第四中间碎片矩阵生成第二交集碎片矩阵。装置900可将第一交集碎片矩阵与第二交集碎片矩阵相加以获得预测结果矩阵。

[0128] 在本公开的实施例中，处理器910可以是例如中央处理单元(CPU)、微处理器、数字信号处理器(DSP)、基于多核的处理器架构的处理器等。存储器920可以是使用数据存储技术实现的任何类型的存储器，包括但不限于随机存取存储器、只读存储器、基于半导体的存储器、闪存、磁盘存储器等。

[0129] 此外，在本公开的实施例中，装置900也可包括输入设备930，例如键盘、鼠标等，用于输入多个输入样本。另外，装置900还可包括输出设备940，例如显示器等，用于输出评估报告。

[0130] 在本公开的其它实施例中，还提供了一种存储有计算机程序的计算机可读存储介质，其中，计算机程序在由处理器执行时能够实现如图6至图7所示的方法的步骤。

[0131] 综上所述，根据本公开的实施例的用于评估联邦学习模型的方法及装置能够在对联邦学习模型进行评估的时候避免个体预测结果泄露，满足合规需求。根据本公开的实施例的用于评估联邦学习模型的方法及装置能够适用于不同带宽的应用场景。

[0132] 附图中的流程图和框图显示了根据本公开的多个实施例的装置和方法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、程序段或指令的一部分，所述模块、程序段或指令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。在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。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，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0133] 除非上下文中另外明确地指出，否则在本文和所附权利要求中所使用的词语的单

数形式包括复数，反之亦然。因而，当提及单数时，通常包括相应术语的复数。相似地，措辞“包含”和“包括”将解释为包含在内而不是独占性地。同样地，术语“包括”和“或”应当解释为包括在内的，除非本文中明确禁止这样的解释。在本文中使用术语“示例”之处，特别是当其位于一组术语之后时，所述“示例”仅仅是示例性的和阐述性的，且不应当被认为是独占性的或广泛性的。

[0134] 适应性的进一步的方面和范围从本文中提供的描述变得明显。应当理解，本申请的各个方面可以单独或者与一个或多个其它方面组合实施。还应当理解，本文中的描述和特定实施例旨在仅说明的目的并不旨在限制本申请的范围。

[0135] 以上对本公开的若干实施例进行了详细描述，但显然，本领域技术人员可以在不脱离本公开的精神和范围的情况下对本公开的实施例进行各种修改和变型。本公开的保护范围由所附的权利要求限定。

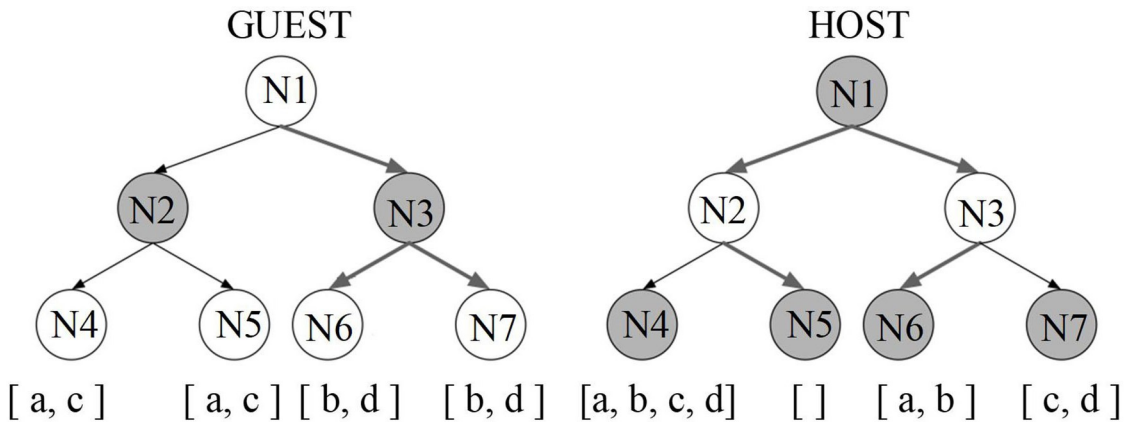



图 1

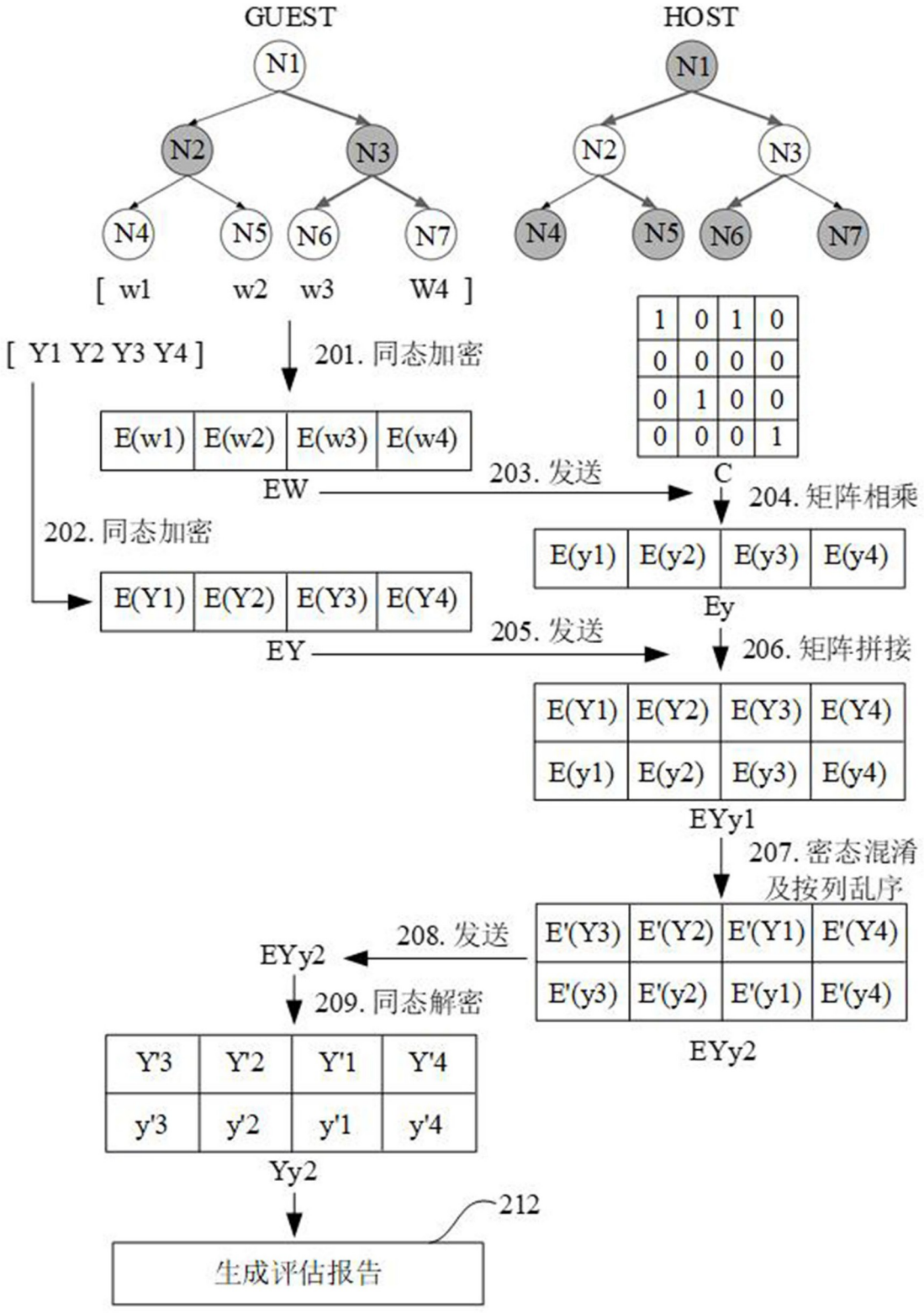

GUEST
HOST
N1
N2
N3
N4
N5
N6
N7
[ w1 w2 w3 W4 ]
[ Y1 Y2 Y3 Y4 ]
201. 同态加密
E(w1) E(w2) E(w3) E(w4)
EW
1 0 1 0
0 0 0 0
0 1 0 0
0 0 0 1
C
203. 发送
204. 矩阵相乘
E(y1) E(y2) E(y3) E(y4)
Ey
202. 同态加密
E(Y1) E(Y2) E(Y3) E(Y4)
EY
205. 发送
206. 矩阵拼接
E(Y1) E(Y2) E(Y3) E(Y4)
E(y1) E(y2) E(y3) E(y4)
EYy1
207. 密态混淆
及按列乱序
E'(Y3) E'(Y2) E'(Y1) E'(Y4)
E'(y3) E'(y2) E'(y1) E'(y4)
EYy2
208. 发送
EYy2
209. 同态解密
Y'3 Y'2 Y'1 Y'4
y'3 y'2 y'1 y'4
Yy2
212
生成评估报告

图 2

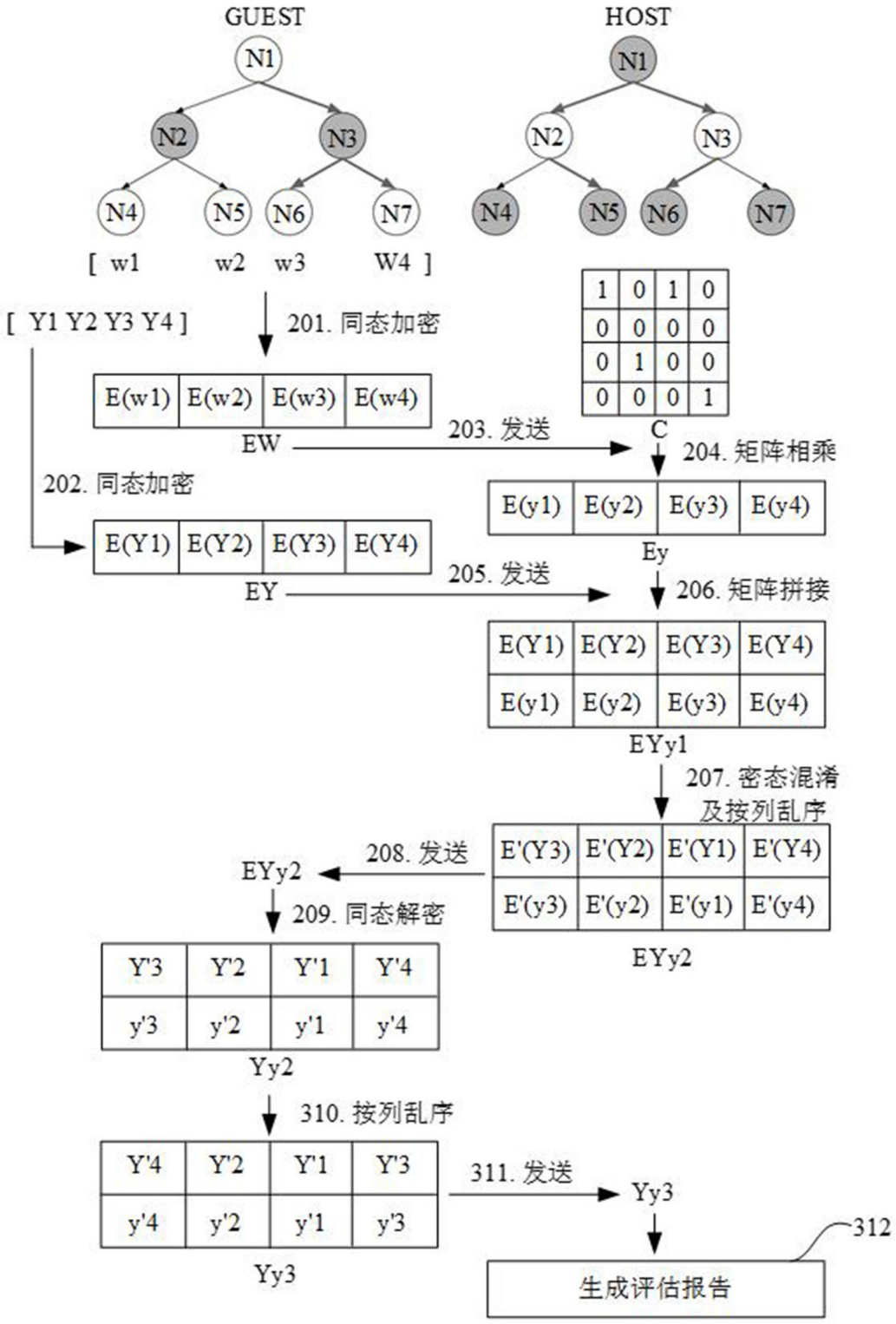

GUEST
HOST
N1
N2
N3
N4
N5
N6
N7
[ w1 w2 w3 W4 ]
[ Y1 Y2 Y3 Y4 ]
201. 同态加密
E(w1) E(w2) E(w3) E(w4)
EW
203. 发送
C
204. 矩阵相乘
E(y1) E(y2) E(y3) E(y4)
Ey
202. 同态加密
E(Y1) E(Y2) E(Y3) E(Y4)
EY
205. 发送
206. 矩阵拼接
EYy1
207. 密态混淆及按列乱序
208. 发送
EYy2
209. 同态解密
Yy2
310. 按列乱序
311. 发送
Yy3
312
生成评估报告

图 3

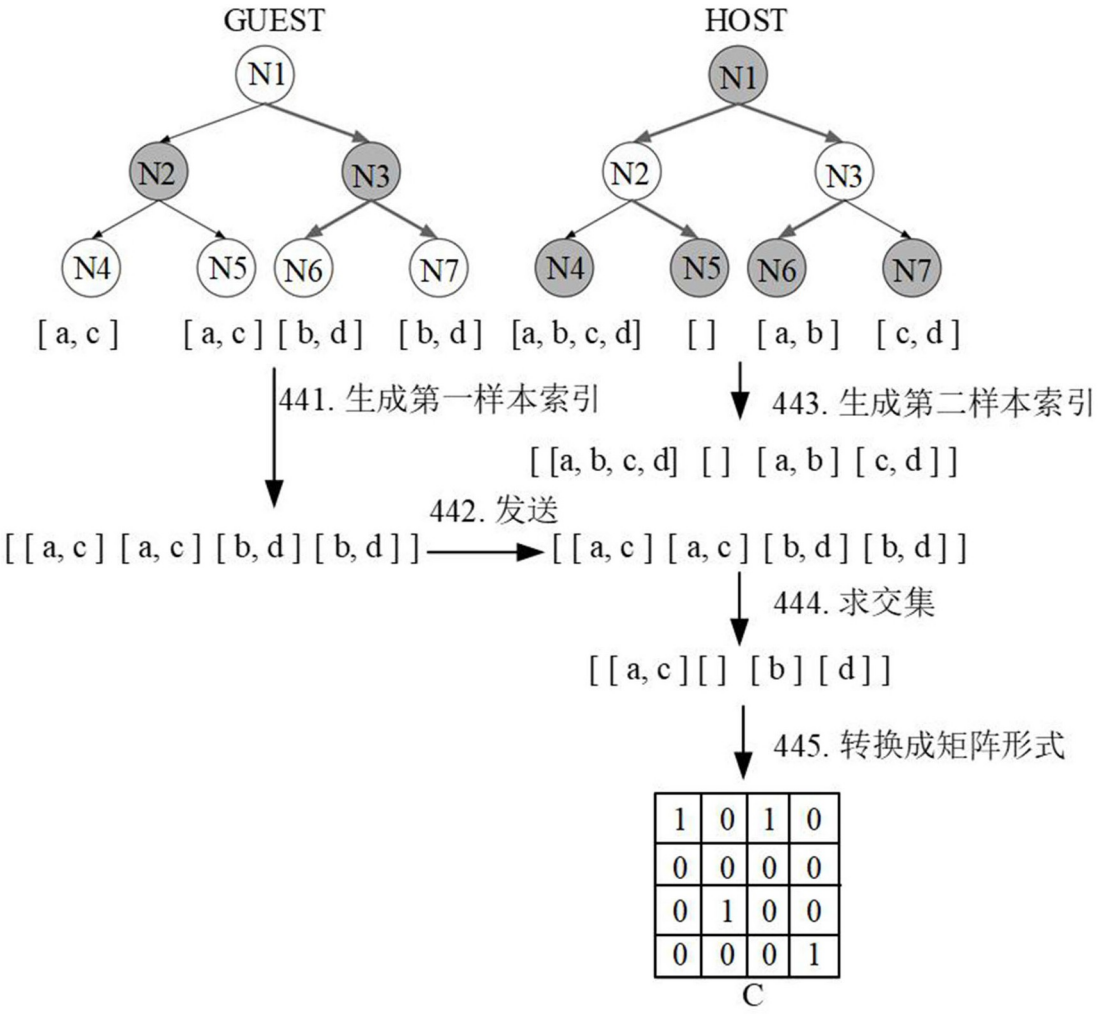

GUEST
HOST
N1
N2
N3
N4
N5
N6
N7
[ a, c ]
[ a, c ] [ b, d ]
[ b, d ]
[a, b, c, d]
[ ]
[ a, b ]
[ c, d ]
441. 生成第一样本索引
443. 生成第二样本索引
[ [a, b, c, d] [ ] [ a, b ] [ c, d ] ]
442. 发送
[ [ a, c ] [ a, c ] [ b, d ] [ b, d ] ]
[ [ a, c ] [ a, c ] [ b, d ] [ b, d ] ]
444. 求交集
[ [ a, c ] [ ] [ b ] [ d ] ]
445. 转换成矩阵形式
1 0 1 0
0 0 0 0
0 1 0 0
0 0 0 1
C

图 4

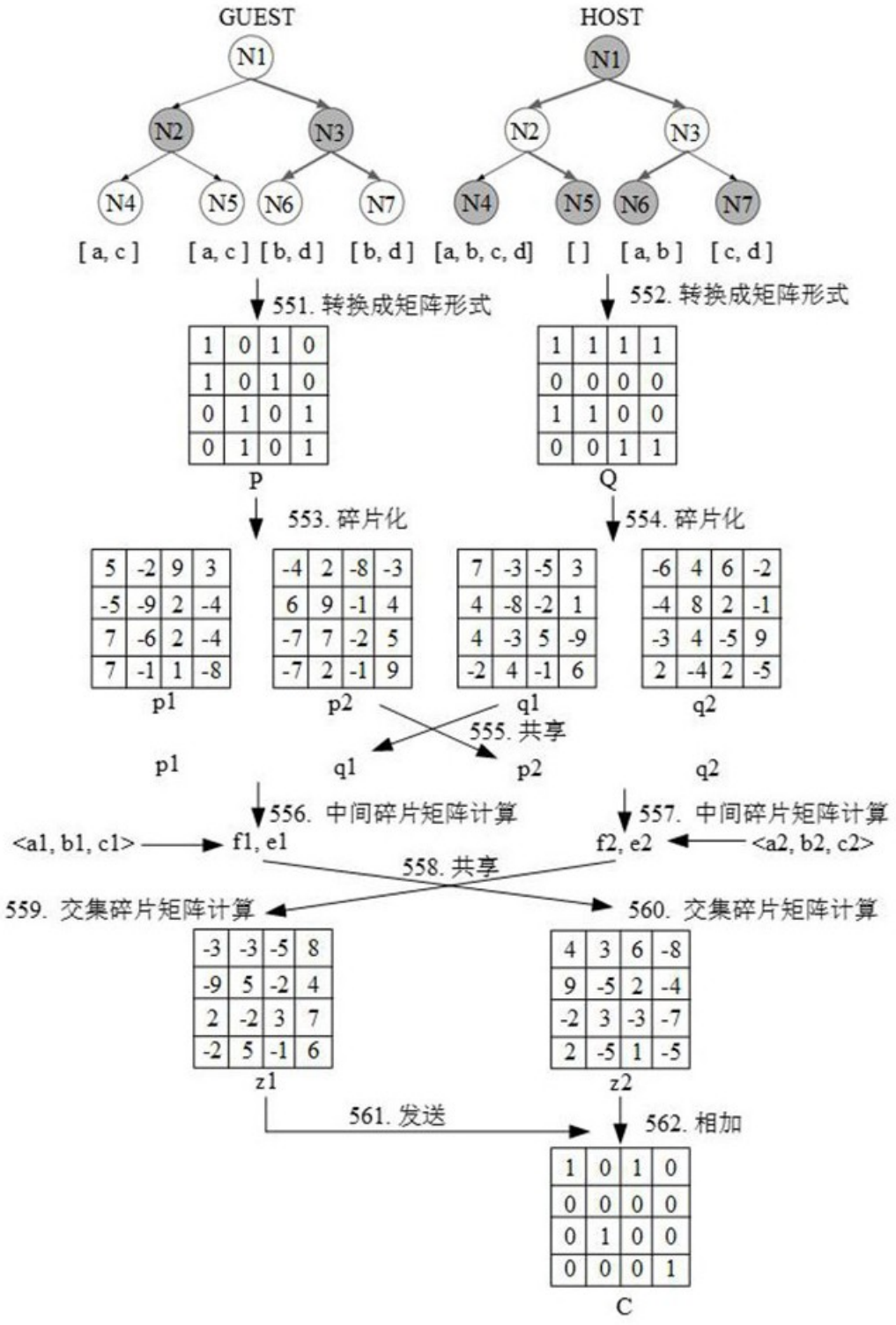

GUEST
HOST
N1
N2
N3
N4
N5
N6
N7
[a, c]
[a, c]
[b, d]
[b, d]
[a, b, c, d]
[ ]
[a, b]
[c, d]
551. 转换成矩阵形式
552. 转换成矩阵形式
P
Q
553. 碎片化
554. 碎片化
p1
p2
q1
q2
555. 共享
556. 中间碎片矩阵计算
557. 中间碎片矩阵计算
<a1, b1, c1>
f1, e1
f2, e2
<a2, b2, c2>
558. 共享
559. 交集碎片矩阵计算
560. 交集碎片矩阵计算
z1
z2
561. 发送
562. 相加
C

图 5

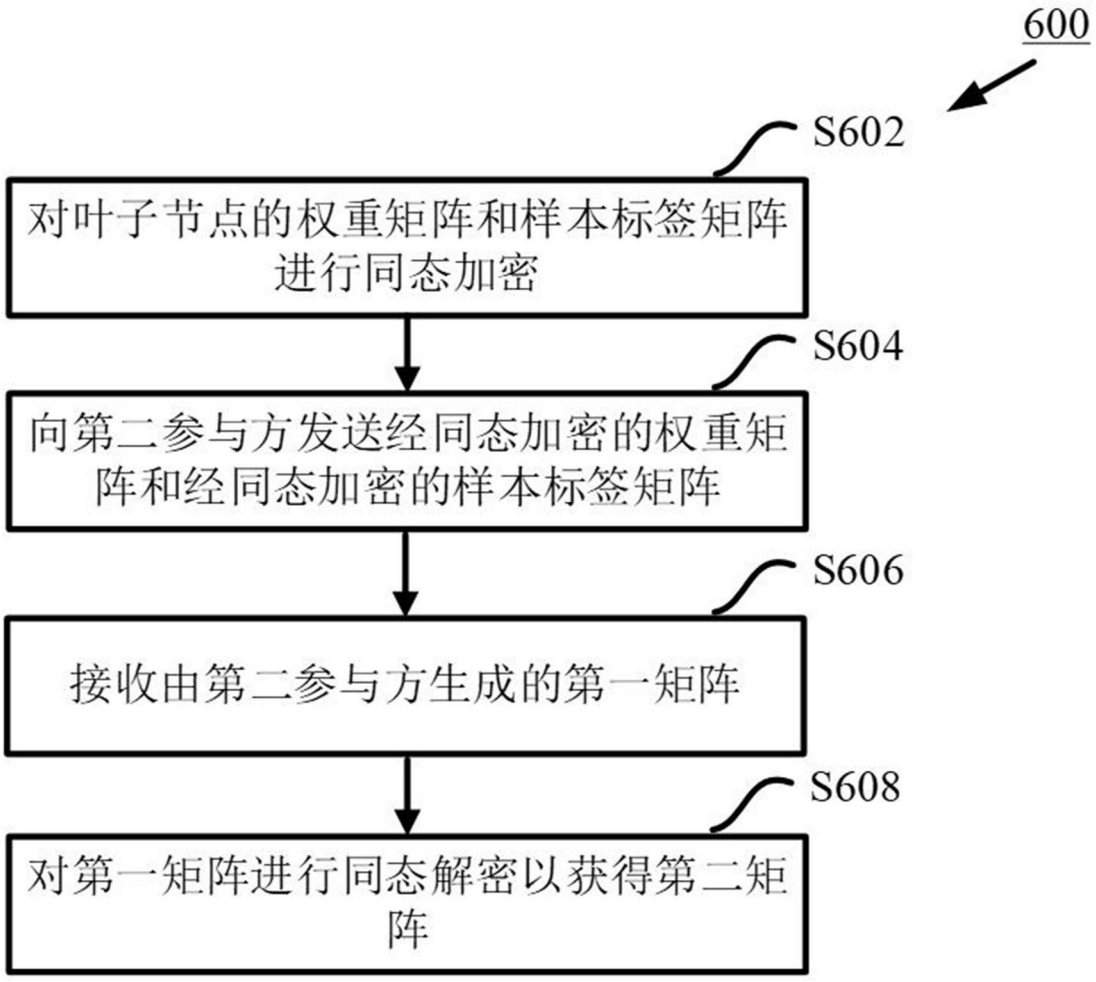

600
S602
对叶子节点的权重矩阵和样本标签矩阵进行同态加密
S604
向第二参与方发送经同态加密的权重矩阵和经同态加密的样本标签矩阵
S606
接收由第二参与方生成的第一矩阵
S608
对第一矩阵进行同态解密以获得第二矩阵

图 6

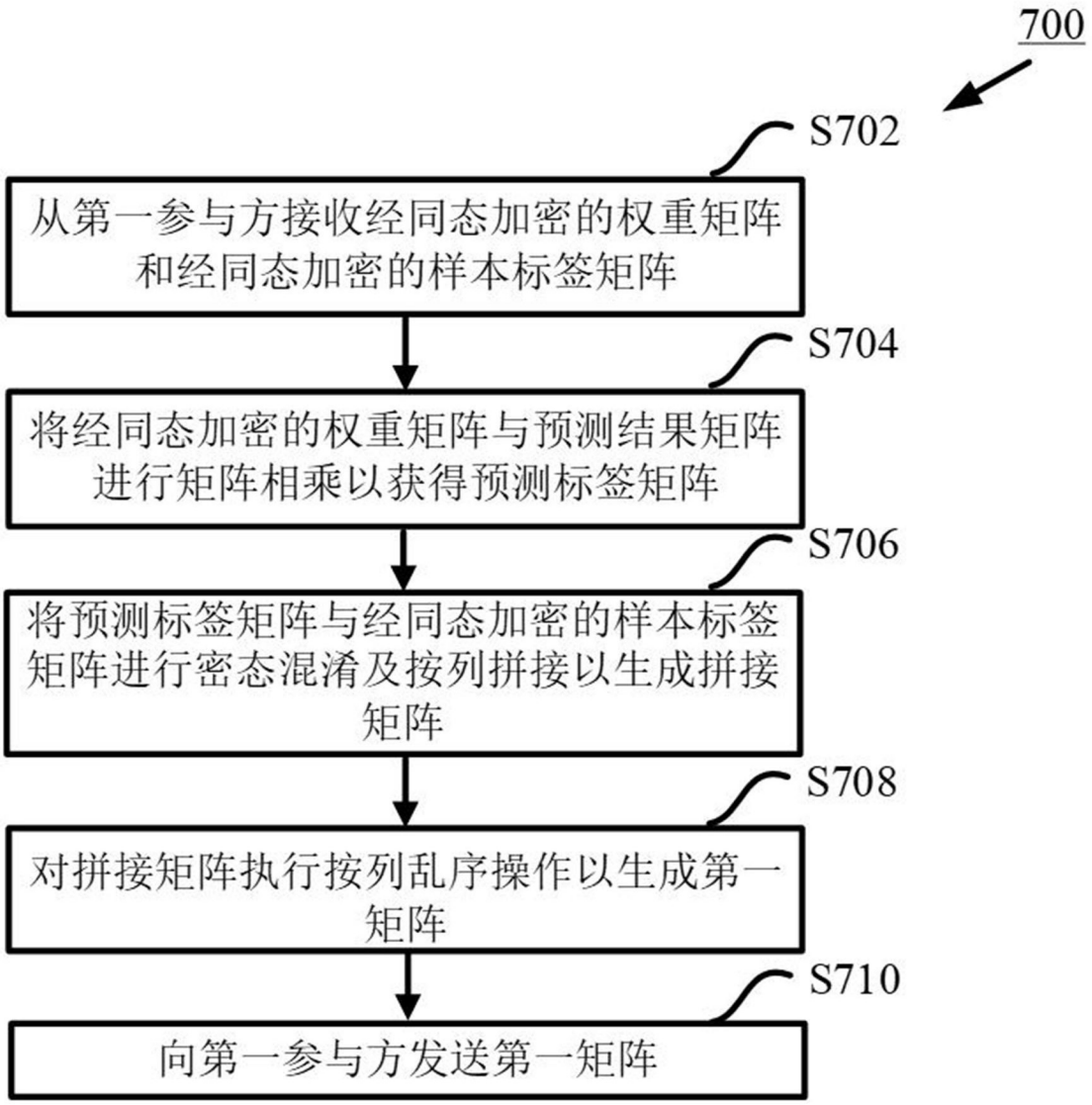

700
S702
从第一参与方接收经同态加密的权重矩阵和经同态加密的样本标签矩阵
S704
将经同态加密的权重矩阵与预测结果矩阵进行矩阵相乘以获得预测标签矩阵
S706
将预测标签矩阵与经同态加密的样本标签矩阵进行密态混淆及按列拼接以生成拼接矩阵
S708
对拼接矩阵执行按列乱序操作以生成第一矩阵
S710
向第一参与方发送第一矩阵

图 7

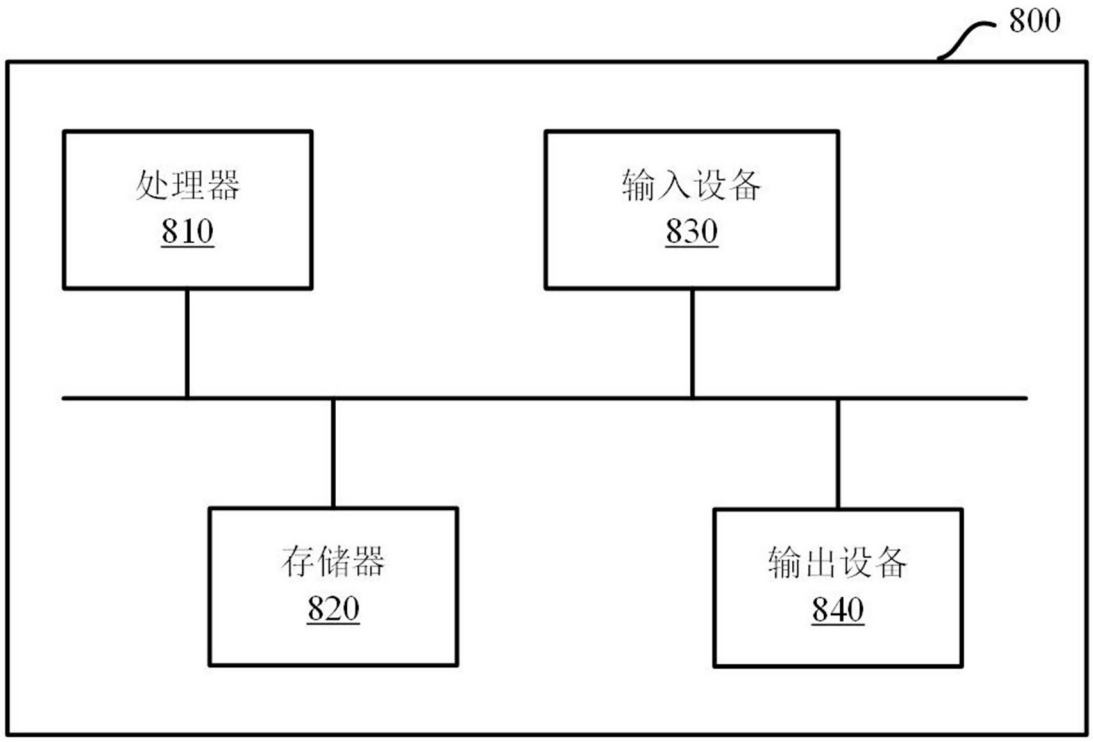

800
处理器
810
输入设备
830
存储器
820
输出设备
840

图 8

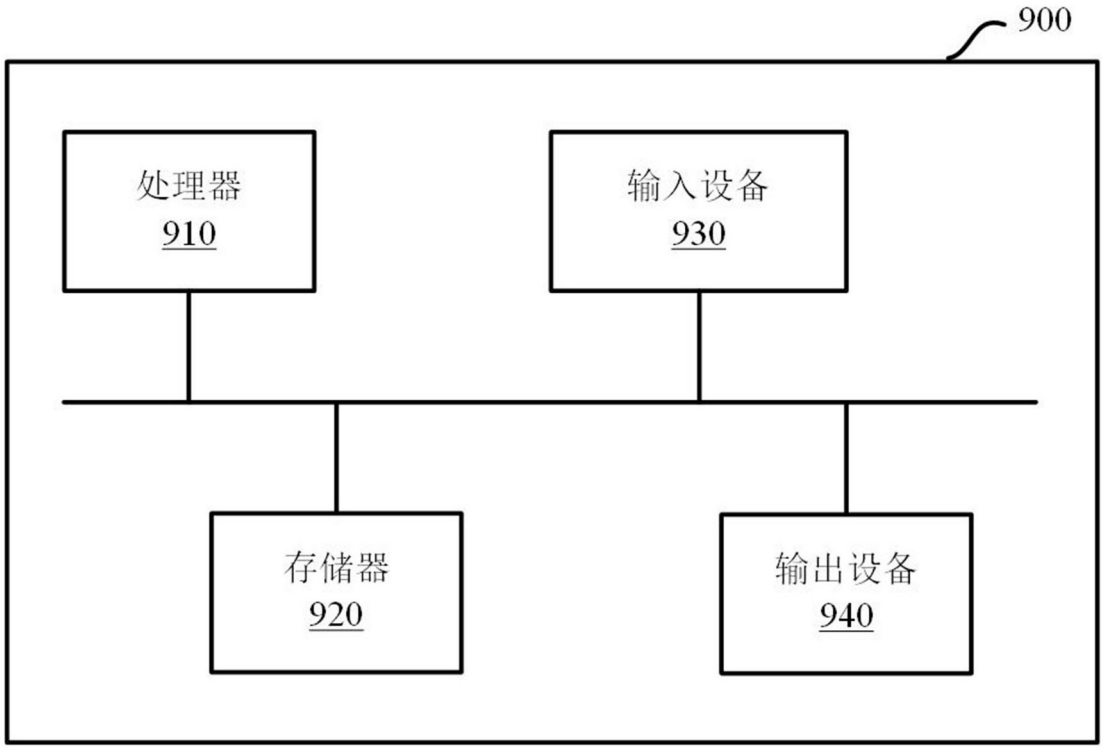

900
处理器
910
输入设备
930
存储器
920
输出设备
940

图 9