(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114282257 B
(45)授权公告日 2022.07.15

(21)申请号 202210218430.5
(22)申请日 2022.03.08
(65)同一申请的已公布的文献号
申请公布号 CN 114282257 A
(43)申请公布日 2022.04.05
(73)专利权人 富算科技(上海)有限公司
地址 200120 上海市浦东新区中国(上海)自由贸易试验区浦东大道1200号2层A区
(72)发明人 卞阳 尤志强 赵东 朱崇炳
(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 唐正瑜
(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)
G06F 8/30(2018.01)
G06F 8/41(2018.01)
(56)对比文件
CN 113472538 A,2021.10.01
CN 113516256 A,2021.10.19
EP 1770587 A1,2007.04.04
张伟娜等.人工智能与区块链技术融合发展研究.《电子技术应用》.2021,第47卷(第10期),全文.
朱建明等.基于区块链的隐私保护可信联邦学习模型.《计算机学报》.2021,第44卷(第12期),全文.
Brunno F. Goldstein等.Preventing DNN Model IP Theft via Hardware Obfuscation.《IEEE Journal on Emerging and Selected Topics in Circuits and Systems》.2021,第11卷(第2期),全文.
审查员 张亚芳

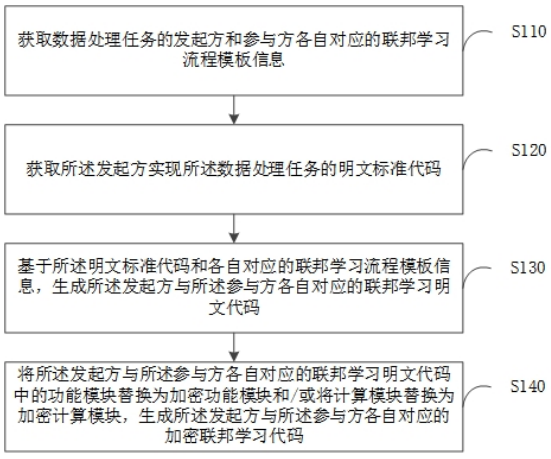
权利要求书2页 说明书14页 附图9页

(54)发明名称

联邦学习代码生成方法、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代码生成方法、装置、电子设备及存储介质，涉及计算机技术领域。该方法通过获取数据处理任务的发起方与参与方各自对应的联邦学习流程模板信息，该联邦学习流程模板信息是由预先配置的功能框架模块和/或计算框架模块构成的，这样可以针对不同的数据处理任务的发起方和参与方灵活配置联邦学习流程模板信息，从而可以针对不同的数据处理任务快速开发出对应的联邦学习代码，能够应对更多的数据处理任务，并且，算法的安全性由加密功能模块和加密计算模块来保证，整体代码无需关心数据加密的问题，进而可以降低联邦学习代码的开发难度以及提高联邦学习代码的开发效率。



CN 114282257 B

1.一种联邦学习代码生成方法,其特征在于,所述方法包括:

获取数据处理任务的发起方与参与方各自对应的联邦学习流程模板信息,其中,所述联邦学习流程模板信息用于表征对所述数据处理任务进行联邦学习的数据处理逻辑,所述联邦学习流程模板信息包括功能框架模块和/或计算框架模块,所述功能框架模块是指用于实现所述数据处理任务的通用功能的框架程序,所述计算框架模块是指用于实现所述数据处理任务的特定算法的框架程序;

获取所述发起方实现所述数据处理任务的明文标准代码;

基于所述明文标准代码和各自对应的联邦学习流程模板信息,生成所述发起方与所述参与方各自对应的联邦学习明文代码,其中,所述联邦学习明文代码包括功能模块和/或计算模块,所述功能模块是利用所述明文标准代码中的通用功能代码和所述功能框架模块生成的,所述计算模块是利用所述明文标准代码中的特定算法代码和所述计算框架模块生成的;

将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块替换为加密功能模块和/或将计算模块替换为加密计算模块,生成所述发起方与所述参与方各自对应的加密联邦学习代码。

2.根据权利要求1所述的方法,其特征在于,所述将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块替换为加密功能模块和/或将计算模块替换为加密计算模块,包括:

将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块采用预设加密算法进行加密,获得加密功能模块;和/或,获取所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块对应的预先加密的加密计算模块;

将功能模块替换为对应的加密功能模块,和/或,将计算模块替换为对应的加密计算模块。

3.根据权利要求2所述的方法,其特征在于,所述获取所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块对应的预先加密的加密计算模块,包括:

对所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块进行解析,获得计算模块对应的多个基础算子;

获取每个基础算子对应的预先加密的加密算子,加密计算模块包括多个加密算子。

4.根据权利要求1所述的方法,其特征在于,所述将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块替换为加密功能模块和/或将计算模块替换为加密计算模块,包括:

将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块采用预设加密算法进行加密,获得加密功能模块;和/或,将所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块采用预设加密算法进行加密,获得加密计算模块;

将功能模块替换为对应的加密功能模块,和/或,将计算模块替换为对应的加密计算模块。

5.根据权利要求2-4任一所述的方法,其特征在于,所述预设加密算法为全同态加密算法或多方安全计算。

6.根据权利要求1所述的方法,其特征在于,所述获取数据处理任务的发起方与参与方

各自对应的联邦学习流程模板信息之前，还包括：

配置不同角色方对应的角色配置信息；

根据所述角色配置信息配置发起方或参与方。

7.根据权利要求1所述的方法，其特征在于，功能框架模块为预先针对不同的数据处理任务的发起方或参与方所配置的，计算框架模块为预先针对不同的数据处理任务的发起方或参与方所配置的，所述联邦学习流程模板信息包含实现所述数据处理任务对应的功能框架模块和/或计算框架模块。

8.一种联邦学习代码生成装置，其特征在于，所述装置包括：

模板信息获取模块，用于获取数据处理任务的发起方与参与方各自对应的联邦学习流程模板信息，其中，所述联邦学习流程模板信息用于表征对所述数据处理任务进行联邦学习的数据处理逻辑，所述联邦学习流程模板信息包括功能框架模块和/或计算框架模块，所述功能框架模块是指用于实现所述数据处理任务的通用功能的框架程序，所述计算框架模块是指用于实现所述数据处理任务的特定算法的框架程序；

明文代码获取模块，用于获取所述发起方实现所述数据处理任务的明文标准代码；

明文代码生成模块，用于基于所述明文标准代码和各自对应的联邦学习流程模板信息，生成所述发起方与所述参与方各自对应的联邦学习明文代码，其中，所述联邦学习明文代码包括功能模块和/或计算模块，所述功能模块是利用所述明文标准代码中的通用功能代码和所述功能框架模块生成的，所述计算模块是利用所述明文标准代码中的特定算法代码和所述计算框架模块生成的；

加密代码生成模块，用于将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块替换为加密功能模块和/或将计算模块替换为加密计算模块，生成所述发起方与所述参与方各自对应的加密联邦学习代码。

9.一种电子设备，其特征在于，包括处理器以及存储器，所述存储器存储有计算机可读取指令，当所述计算机可读取指令由所述处理器执行时，运行如权利要求1-7任一所述的方法。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时运行如权利要求1-7任一所述的方法。

联邦学习代码生成方法、装置、电子设备及存储介质

技术领域

[0001] 本申请涉及计算机技术领域，具体而言，涉及一种联邦学习代码生成方法、装置、电子设备及存储介质。

背景技术

[0002] 联邦学习是指一种机器学习框架，能有效帮助多个节点在满足数据隐私保护的要求下，联合训练模型。联邦学习代码需要基于各参与方的数据计算、参数训练、各方的交互等，而目前针对不同的业务需要分别开发一套联邦学习代码，所以使得需要更多的时间来开发和维护联邦学习代码，开发难度大且开发效率低。

发明内容

[0003] 本申请实施例的目的在于提供一种联邦学习代码生成方法、装置、电子设备及存储介质，用以改善现有技术中联邦学习代码开发难度大且开发效率低的问题。

[0004] 第一方面，本申请实施例提供了一种联邦学习代码生成方法，所述方法包括：

[0005] 获取数据处理任务的发起方与参与方各自对应的联邦学习流程模板信息，其中，所述联邦学习流程模板信息用于表征对所述数据处理任务进行联邦学习的数据处理逻辑，所述联邦学习流程模板信息包括功能框架模块和/或计算框架模块，所述功能框架模块是指用于实现所述数据处理任务的通用功能的框架程序，所述计算框架模块是指用于实现所述数据处理任务的特定算法的框架程序；

[0006] 获取所述发起方实现所述数据处理任务的明文标准代码；

[0007] 基于所述明文标准代码和各自对应的联邦学习流程模板信息，生成所述发起方与所述参与方各自对应的联邦学习明文代码，其中，所述联邦学习明文代码包括功能模块和/或计算模块，所述功能模块是利用所述明文标准代码中的通用功能代码和所述功能框架模块生成的，所述计算模块是利用所述明文标准代码中的特定算法代码和所述计算框架模块生成的；

[0008] 将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块替换为加密功能模块和/或将计算模块替换为加密计算模块，生成所述发起方与所述参与方各自对应的加密联邦学习代码。

[0009] 在上述实现过程中，通过获取数据处理任务的发起方与参与方各自对应的联邦学习流程模板信息，该联邦学习流程模板信息是由预先配置的功能框架模块和/或计算框架模块构成的，然后可利用联邦学习流程模板信息将发起方的明文标准代码转换为联邦学习代码，这样可以针对不同的数据处理任务的发起方和参与方灵活配置联邦学习流程模板信息，从而可以针对不同的数据处理任务快速开发出对应的联邦学习代码，能够应对更多的数据处理任务，并且，算法的安全性由加密功能模块和加密计算模块来保证，整体代码无需关心数据加密的问题，进而可以降低联邦学习代码的开发难度以及提高联邦学习代码的开发效率。

[0010] 可选地，所述将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块替换为加密功能模块和/或将计算模块替换为加密计算模块，包括：

[0011] 将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块采用预设加密算法进行加密，获得加密功能模块；和/或，获取所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块对应的预先加密的加密计算模块；

[0012] 将功能模块替换为对应的加密功能模块，和/或，将计算模块替换为对应的加密计算模块。

[0013] 在上述实现过程中，通过对功能模块采用预设加密算法进行加密可以提高算法的安全性，而加密计算模块进行预先加密，在对计算模块进行加密时，可以直接调用即可，可以提高代码的开发效率。

[0014] 可选地，所述获取所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块对应的预先加密的加密计算模块，包括：

[0015] 对所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块进行解析，获得计算模块对应的多个基础算子；

[0016] 获取每个基础算子对应的预先加密的加密算子，加密计算模块包括多个加密算子。

[0017] 在上述实现过程中，对计算模块进行解析，获得多个基础算子，然后将基础算子替换为加密算子，如此可以预先对基础算子进行加密获得加密算子，提高开发效率。

[0018] 可选地，所述将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块替换为加密功能模块和/或将计算模块替换为加密计算模块，包括：

[0019] 将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块采用预设加密算法进行加密，获得加密功能模块；和/或，将所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块采用预设加密算法进行加密，获得加密计算模块；

[0020] 将功能模块替换为对应的加密功能模块，和/或，将计算模块替换为对应的加密计算模块。

[0021] 在上述实现过程中，也可以对功能模块和计算模块进行实时加密，这样避免提前加密一些使用效率不高的模块，浪费加密资源的问题。

[0022] 可选地，所述预设加密算法为全同态加密算法或多方安全计算。如此可确保算法的安全性。

[0023] 可选地，所述获取数据处理任务的发起方与参与方各自对应的联邦学习流程模板信息之前，还包括：

[0024] 配置不同角色方对应的角色配置信息；

[0025] 根据所述角色配置信息配置发起方或参与方。

[0026] 在上述实现过程中，预先配置角色配置信息，从而可以预先根据角色配置信息配置不同的角色，以便于可以快速针对不同的角色开发对应的联邦学习代码。

[0027] 可选地，功能框架模块为预先针对不同的数据处理任务的发起方或参与方所配置的，计算框架模块为预先针对不同的数据处理任务的发起方或参与方所配置的，所述联邦学习流程模板信息包含实现所述数据处理任务对应的功能框架模块和/或计算框架模块。预先配置功能框架模块和计算框架模块，这样可以在配置联邦学习流程模板信息时，调用

功能框架模块和/或计算框架模块进行组合即可，配置效率更高。

[0028] 第二方面，本申请实施例提供了一种联邦学习代码生成装置，所述装置包括：

[0029] 模板信息获取模块，用于获取数据处理任务的发起方与参与方各自对应的联邦学习流程模板信息，其中，所述联邦学习流程模板信息用于表征对所述数据处理任务进行联邦学习的数据处理逻辑，所述联邦学习流程模板信息包括功能框架模块和/或计算框架模块，所述功能框架模块是指用于实现所述数据处理任务的通用功能的框架程序，所述计算框架模块是指用于实现所述数据处理任务的特定算法的框架程序；

[0030] 明文代码获取模块，用于获取所述发起方实现所述数据处理任务的明文标准代码；

[0031] 明文代码生成模块，用于基于所述明文标准代码和各自对应的联邦学习流程模板信息，生成所述发起方与所述参与方各自对应的联邦学习明文代码，其中，所述联邦学习明文代码包括功能模块和/或计算模块，所述功能模块是利用所述明文标准代码中的通用功能代码和所述功能框架模块生成的，所述计算模块是利用所述明文标准代码中的特定算法代码和所述计算框架模块生成的；

[0032] 加密代码生成模块，用于将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块替换为加密功能模块和/或将计算模块替换为加密计算模块，生成所述发起方与所述参与方各自对应的加密联邦学习代码。

[0033] 可选地，所述加密代码生成模块，用于将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块采用预设加密算法进行加密，获得加密功能模块；和/或，获取所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块对应的预先加密的加密计算模块；将功能模块替换为对应的加密功能模块，和/或，将计算模块替换为对应的加密计算模块。

[0034] 可选地，所述加密代码生成模块，用于对所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块进行解析，获得计算模块对应的多个基础算子；获取每个基础算子对应的预先加密的加密算子，加密计算模块包括多个加密算子。

[0035] 可选地，所述加密代码生成模块，用于将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块采用预设加密算法进行加密，获得加密功能模块；和/或，将所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块采用预设加密算法进行加密，获得加密计算模块；将功能模块替换为对应的加密功能模块，和/或，将计算模块替换为对应的加密计算模块。

[0036] 可选地，所述预设加密算法为全同态加密算法或多方安全计算。

[0037] 可选地，所述装置还包括：

[0038] 配置模块，用于配置不同角色方对应的角色配置信息；根据所述角色配置信息配置发起方或参与方。

[0039] 可选地，功能框架模块为预先针对不同的数据处理任务的发起方或参与方所配置的，计算框架模块为预先针对不同的数据处理任务的发起方或参与方所配置的，所述联邦学习流程模板信息包含实现所述数据处理任务对应的功能框架模块和/或计算框架模块。

[0040] 第三方面，本申请实施例提供一种电子设备，包括处理器以及存储器，所述存储器存储有计算机可读取指令，当所述计算机可读取指令由所述处理器执行时，运行如上述第

一方面提供的所述方法中的步骤。

[0041] 第四方面，本申请实施例提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时运行如上述第一方面提供的所述方法中的步骤。

[0042] 本申请的其他特征和优点将在随后的说明书阐述，并且，部分地从说明书中变得显而易见，或者通过实施本申请实施例了解。本申请的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

[0043] 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。

[0044] 图1为本申请实施例提供的一种联邦学习代码生成方法的流程图；

[0045] 图2为本申请实施例提供的一种功能框架模块的示意图；

[0046] 图3为本申请实施例提供的一种基础算子的示意图；

[0047] 图4为本申请实施例提供的一种基础算子加密为加密算子的示意图；

[0048] 图5为本申请实施例提供的一种多方安全计算的实现过程示意图；

[0049] 图6为本申请实施例提供的一种全同态加密算法的实现过程示意图；

[0050] 图7为本申请实施例提供的一种加法算子的加密示意图；

[0051] 图8为本申请实施例提供的另一种加法算子的加密示意图；

[0052] 图9为本申请实施例提供的一种明文代码转换为联邦学习代码的示意图；

[0053] 图10为本申请实施例提供的一种在模型训练场景下实现联邦学习的过程示意图；

[0054] 图11为本申请实施例提供的一种在数据统计场景下实现联邦学习的过程示意图；

[0055] 图12为本申请实施例提供的一种联邦学习代码生成装置的结构框图；

[0056] 图13为本申请实施例提供的一种用于执行联邦学习代码生成方法的电子设备的结构示意图。

具体实施方式

[0057] 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。

[0058] 需要说明的是，本发明实施例中的术语“系统”和“网络”可被互换使用。“多个”是指两个或两个以上，鉴于此，本发明实施例中也可以将“多个”理解为“至少两个”。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，字符“/”，如无特殊说明，一般表示前后关联对象是一种“或”的关系。

[0059] 本申请实施例提供一种联邦学习代码生成方法，该方法通过获取数据处理任务的发起方与参与方各自对应的联邦学习流程模板信息，该联邦学习流程模板信息是由预先配置的功能框架模块和/或计算框架模块构成的，然后可利用联邦学习流程模板信息将发起方的明文标准代码转换为联邦学习代码，这样可以针对不同的数据处理任务的发起方和参

与方灵活配置联邦学习流程模板信息，从而可以针对不同的数据处理任务快速开发出对应的联邦学习代码，能够应对更多的数据处理任务，并且，算法的安全性由加密功能模块和加密计算模块来保证，整体代码无需关心数据加密的问题，进而可以降低联邦学习代码的开发难度以及提高联邦学习代码的开发效率。

[0060] 下面先对联邦学习做简单介绍。

[0061] 联邦学习旨在建立一个基于分布数据集的联邦学习模型，其本质上是一种分布式机器学习技术，或机器学习框架。联邦学习的目标是在保证数据隐私安全及合法合规的基础上，实现共同建模，提升AI模型的效果。

[0062] 若把每个参与共同建模的企业称为参与方，根据多参与方之间数据分别的不同，把联邦学习分为三类：横向联邦学习、纵向联邦学习和联邦迁移学习。

[0063] 横向联邦学习的本质是样本的联合，适用于参与者间业务相同但触达客户不同，即特征重叠多，用户重叠少时的场景，比如不同地区的银行间，他们的业务相似(特征相似)，但用户不同(样本不同)，在横向联邦学习中，可以看作是基于样本的分布式模型训练，分发全部数据到不同的机器，每台机器从服务器下载模型，然后利用本地数据训练模型，之后返回给服务器需要更新的参数，服务器聚合各机器上的返回的参数，更新模型，再把最新的模型反馈到每台机器。在这个过程中，每台机器下都是相同且完整的模型，且机器之间不交流不依赖，在预测时每台机器也可以独立预测，可以把这个过程看作成基于样本的分布式训练模型。

[0064] 纵向联邦学习的本质是特征的联合，适用于用户重叠多，特征重叠少的场景，比如同一地区的商超和银行，他们触达的用户都为该地区的居民(样本相同)，但业务不同(特征不同)。纵向联邦学习的本质是交叉用户在不同业态下的特征联合，比如商超A和银行B，在传统的机器学习建模过程中，需要将两部分数据集中到一个数据中心，然后再将每个用户的特征合并成一条数据用来训练模型，所以就需要双方有用户交集，并有一方存在标签。在整个过程中参与方都不知道另一方的数据和特征，且训练结束后参与方只得到自己侧的模型参数。

[0065] 联邦迁移学习：当参与者间特征和样本重叠都很少时可以考虑使用联邦迁移学习，如不同地区的银行和商超间的联合。主要适用于以深度神经网络为基模型的场景。

[0066] 迁移学习，是指利用数据、任务、或模型之间的相似性，将在源领域学习过的模型，应用于目标领域的一种学习过程。迁移学习的核心是，找到源领域和目标领域之间的相似性。

[0067] 本申请生成的联邦学习代码可以应用于上述的纵向联邦学习场景和迁移联邦学习场景，下面详细介绍本申请的联邦学习代码生成方法。

[0068] 请参照图1，图1为本申请实施例提供的一种联邦学习代码生成方法的流程图，该方法包括如下步骤：

[0069] 步骤S110：获取数据处理任务的发起方和参与方各自对应的联邦学习流程模板信息。

[0070] 本申请实施例的联邦学习代码生成方法的执行主体可以是联邦学习平台，联邦学习平台可以部署于发起方和参与方的终端设备上，发起方可以在联邦学习平台上触发对数据处理任务的处理。也就是说，在联邦学习平台上触发数据处理任务的用户可以称为发起

方，其余参与的用户可以称为参与方，参与方可以为一个，也可以为多个，可以根据实际情况而定。

[0071] 数据处理任务可以如数据统计任务、模型训练任务、模型预测任务等，由于发起方无法单独执行数据处理任务，所以需要参与方的数据(如对于模型训练任务，发起方有特征数据，而参与方有标签数据)，发起方可以在联邦学习平台上向确定的参与方发送邀请，以邀请参与方来协助完成数据处理任务。

[0072] 例如，发起方为公司A，公司A需要进行审计网络模型训练任务，但是公司A没有标签数据，则公司A可以在联邦学习平台上触发神经网络模型训练任务，公司A有样本数据，而公司B有标签数据，神经网络模型训练需要公司B的标签数据，所以，公司A可以在联邦学习平台上向公司B发送任务邀请，公司B通过联邦平台接收到任务邀请后，可对任务邀请进行确认后向公司A反馈是否同意邀请，若公司B同意，则公司B可以作为本次神经网络模型训练任务的参与方，公司A和公司B共同完成神经网络模型的训练任务。

[0073] 为了适配不同的数据处理任务，可以预先在联邦学习平台上配置不同角色对应的联邦学习流程模板信息，联邦学习流程模板信息用于表征对数据处理任务进行联邦学习的数据处理逻辑，联邦学习流程模板信息包括功能框架模块和/或计算框架模块，即联邦学习流程模板信息可以包括功能框架模块或计算框架模块，或者联邦学习流程模板信息也可以包括功能框架模块和计算框架模块，其可以是根据不同角色的需求所配置的。功能框架模块是指用于实现数据处理任务的通用功能的框架程序，计算框架模块是指用于实现数据处理任务的特定算法的框架程序。

[0074] 联邦学习流程模板信息可以是指一种通用的数据处理逻辑，所以，可以预先针对不同的数据处理任务来为不同的角色进行配置。数据处理逻辑，其可以理解：如对于模型训练任务，先进行数据输入、数据预处理、模型参数初始化、模型训练、模型评估的数据处理逻辑，即各个角色在进行联邦学习时，可以按照对应的数据处理逻辑进行处理。

[0075] 联邦学习流程模板信息是由预先配置的功能框架模块和/或计算框架模块所构成的，比如有的参与方不需要计算框架模块，只需要功能框架模块，计算由发起方来执行，此时发起方的联邦学习流程模板信息则包括功能框架模块和计算框架模块，而参与方的联邦学习流程模板信息包括功能框架模块，当然若有的参与方只参与计算，则其联邦学习流程模板信息包括计算框架模块。

[0076] 功能框架模块可以是指一些通用的框架程序，或者是针对角色需要区分使用的模块，在一些实施方式中，功能框架模块为预先针对不同的数据处理任务的发起方和参与方所配置的，计算框架模块为预先针对不同的数据处理任务的发起方或参与方所配置的，联邦学习流程模板信息则包含实现数据处理任务对应的功能框架模块和/或计算框架模块。预先配置功能框架模块和计算框架模块，这样可以在配置联邦学习流程模板信息时，调用功能框架模块和/或计算框架模块进行组合即可，配置效率更高。

[0077] 比如在模型训练过程中，需要区分标签方和特征方，如果是标签方，需要使用针对标签数据处理的数据处理模块，如果是特征参与方，需要使用仅对特征数据的数据处理模块。若还有其他角色，如模型发起方、结果获取方等，则会涉及到计算最终结果的获取模块以及相关数据统计信息的报告模块，而针对模型中上报模型结果、上报模型参数以及上报处理的数据都可以使用相对通用的模块。

[0078] 也就是说，功能框架模块是形成完整联邦算法必须的部分，主要是针对算法的非核心计算逻辑功能，比如算法所需的数据输入模块、数据预处理模块、模型报告生成模块、模型参数保存模块等。这些功能框架模块是算法核心计算逻辑的前置和后置依赖，相对于计算框架模块是独立的。比如对于数据输入，可以根据具体的角色，配置相应的功能框架模块，如标签方的数据输入形态为“样本id+特征+标签”或者是“样本id+标签”，而特征方的数据输入形态为“样本id+特征”，数据处理则是根据相应的预处理规则，在各参与方本地执行并做最终的各节点状态同步。模型报告是在标签方执行，然后将报告结果同步给发起方，模型预测值与真实标签进行相应的计算，其输入输出比较明确，且与算法核心计算逻辑相对独立。如果标签方是发起方，则可直接执行报告生成获得结果。模型参数保存模块同样可以独立于算法核心计算逻辑。

[0079] 功能框架模块可以分为角色模块和通用模块，通用模块可以是一些基础模块，角色模块可以是针对不同的角色所配置的，如图2所示。

[0080] 计算框架模块可以是针对数据处理任务所涉及到的特定算法，如针对核心计算逻辑涉及数值计算的具体操作符，如加法、乘法、矩阵乘法，或者是计算函数，如sigmoid、relu、ks、auc等函数。

[0081] 所以，只需要针对数据处理任务的各角色，抽象包装为独立的功能框架模块和计算框架模块，在配置各角色的联邦学习流程模板信息时，进行功能框架模块和/或计算框架模块的组合调用即可。

[0082] 也就是说，联邦平台在确定数据处理任务的发起方和参与方后，可自动调用获得预先为其配置的联邦学习流程模板信息。

[0083] 步骤S120:获取所述发起方实现所述数据处理任务的明文标准代码。

[0084] 其中，明文标准代码可以理解为是发起方自身为实现数据处理任务所开发的源代码，如数据处理任务为模型训练任务，明文标准代码为执行模型训练任务的源代码，发起方在对源代码进行编译后，就可以执行模型训练任务了。这里之所以称为标准代码是指代码中的函数命名等需要遵循联邦平台要求，如sigmoid函数名称必须为英文小写。

[0085] 明文标准代码可以是发起方发送给联邦学习平台的，如此联邦学习平台就可以将发起方的明文标准代码转换为发起方和参与方的联邦学习代码。

[0086] 步骤S130:基于所述明文标准代码和各自对应的联邦学习流程模板信息，生成所述发起方与所述参与方各自对应的联邦学习明文代码。

[0087] 联邦学习平台在获得明文标准代码、发起方对应的联邦学习流程模板信息以及参与方的联邦学习流程模板信息后，可以生成发起方和参与方各自的联邦学习明文代码。

[0088] 其中，联邦学习明文代码是指没有加密的代码，其包括功能模块和/或计算模块，功能模块是利用明文标准代码中的通用功能代码和功能框架模块生成的，计算模块是利用明文标准代码中的特定算法代码和计算框架模块生成的。例如，若发起方的联邦学习流程模板信息包括功能框架模块和计算框架模块，则生成的发起方的联邦学习明文代码则包括功能模块和计算模块，若参与方的联邦学习流程模板信息包括功能框架模块，则生成的参与方的联邦学习明文代码则包括功能模块。

[0089] 明文标准代码中包含了需要实现通用功能的代码段以及实现特定算法的代码段，功能框架模块为实现通用功能提供了一个框架程序，计算框架模块为实现特定算法提供了

一个框架程序，所以，可以对明文标准代码进行解析，从中解析出通用功能代码段以及算法代码段，然后可以将通用功能代码段填入功能框架模块中，如此可获得功能模块，将算法代码段填入计算框架模块中，如此可获得计算模块。例如，对于数据输入模块，明文标准代码中包含了具体的输入数据，则可以将输入数据填入数据输入模块对应的功能框架模块中，对于梯度计算模块，明文标准代码中包含了具体的计算方法，则可以将具体的计算方法填入梯度计算模块对应的计算框架模块中。

[0090] 而联邦学习流程模板信息中包含功能框架模块和/或计算框架模块，并且功能框架模块和/或计算框架模块之间按照一定的顺序组合，以形成联邦学习的数据处理逻辑。所以，对于发起方的联邦学习明文代码，可以将明文标准代码中的相关代码段填入其联邦学习流程模板信息中的模块中，如此可获得发起方的联邦学习明文代码。对于参与方的联邦学习明文代码，也可以将明文标准代码中的相关代码段填入其联邦学习流程模板信息中的模块中，如此可获得参与方的联邦学习明文代码。

[0091] 步骤S140：将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块替换为加密功能模块和/或将计算模块替换为加密计算模块，生成所述发起方与所述参与方各自对应的加密联邦学习代码。

[0092] 上述获得的联邦学习明文代码为未加密的代码，由于发起方和参与方都不想把各自的隐私数据发给对方，所以，还需要对联邦学习明文代码进行加密，获得加密联邦学习代码，以确保算法的安全性。这样发起方和参与方在进行联邦学习时，各自编译各自的加密联邦学习代码即可执行数据处理任务。

[0093] 在对联邦学习明文代码进行加密时，可以将发起方与参与方各自的联邦学习明文代码中的功能模块替换为加密功能模块，和/或将计算模块替换为加密计算模块，然后即可生成加密联邦学习代码。

[0094] 例如，发起方的联邦学习明文代码包括功能模块和计算模块时，则可将功能模块替换为加密功能模块，将计算模块替换为加密计算模块，如此可获得加密后的加密联邦学习代码。若参与方的联邦学习明文代码包括功能模块，则可将功能模块替换为加密功能模块，即可获得加密后的加密联邦学习代码。这样就可以针对发起方和参与方分别生成加密联邦学习代码，联邦学习平台可将发起方的加密联邦学习代码发送给发起方，可将参与方的联邦学习代码发送给参与方。

[0095] 在上述实现过程中，通过获取数据处理任务的发起方与参与方各自对应的联邦学习流程模板信息，该联邦学习流程模板信息是由预先配置的功能框架模块和/或计算框架模块构成的，然后可利用联邦学习流程模板信息将发起方的明文标准代码转换为联邦学习代码，这样可以针对不同的数据处理任务的发起方和参与方灵活配置联邦学习流程模板信息，从而可以针对不同的数据处理任务快速开发出对应的联邦学习代码，能够应对更多的数据处理任务，并且，算法的安全性由加密功能模块和加密计算模块来保证，整体代码无需关心数据加密的问题，进而可以降低联邦学习代码的开发难度以及提高联邦学习代码的开发效率。

[0096] 在上述实施例的基础上，为了快速获得各方的联邦学习流程模板信息，还可以预先配置不同角色对应的角色配置信息，然后可根据角色配置信息来配置发起方或参与方，从而可以预先根据角色配置信息配置不同的角色，以便于可以快速针对不同的角色开发对

应的联邦学习代码。

[0097] 其中，角色配置信息可以包括数据层面、参数层面、任务层面等方面的信息，如数据层面包含标签信息(如是否包含标签，标签所在列索引等)、支持的数据类型(如int、float)和样本数据拆分(如拆分形式、拆分比例等)，参数层面包含联邦学习类型(如纵向或迁移)和加密类型(多方安全计算、全同态加密算法等)，任务层面包含任务类型(如训练、预测、评估等)以及输入输出类型(数据集、模型、报告)。

[0098] 角色配置信息可以是管理员在联邦平台上输入的，根据角色配置信息可以在联邦平台上配置不同的角色，如发起方和参与方，这样就可以针对不同角色配置对应的联邦学习流程模板信息。

[0099] 在上述实施例的基础上，在将功能模块替换为加密功能模块，和/或将计算模块替换为加密计算模块的过程中，可以将发起方和参与方各自对应的联邦学习明文代码中的功能模块采用预设加密算法进行加密，获得加密功能模块，和/或，获取发起方和参与方各自对应的联邦学习明文代码中的计算模块对应的预先加密的加密计算模块，然后可将功能模块替换为对应的加密功能模块，和/或将计算模块替换为对应的加密计算模块。

[0100] 例如，发起方的联邦学习明文代码包括功能模块和计算模块，此时可以对功能模块采用预设加密算法进行加密，由于计算模块是由一些算子构成，所以加密计算模块可以是预先加密好存储在联邦学习平台上的，如联邦学习平台上存储有计算模块和对应的加密计算模块的映射关系，所以联邦平台可以根据映射关系获得计算模块对应的加密计算模块。若参与方的联邦学习明文代码包括功能模块，则可以直接将功能模块采用预设加密算法进行加密，获得加密功能模块后，将参与方的联邦学习明文代码中的功能模块替换为加密功能模块，即可获得加密联邦学习代码。

[0101] 其中，预设加密算法可以为全同态加密算法、多方安全计算或差分隐私加密技术等加密算法，而预设的加密计算模块也可以是采用这些加密算法进行加密的。

[0102] 在上述实现过程中，通过对功能模块采用预设加密算法进行加密可以提高算法的安全性，而加密计算模块进行预先加密，在对计算模块进行加密时，可以直接调用即可，可以提高代码的开发效率。

[0103] 在上述实施例的基础上，由于计算模块一般是由一些算子构成的，所以，可以预先对算子进行加密，然后在获得加密联邦学习代码的过程中，可以先对发起方和参与方各自对应的联邦学习明文代码中的计算模块进行解析，获得计算模块对应的多个基础算子，然后获取每个基础算子对应的预先加密的加密算子，加密计算模块则包含多个加密算子，也就是说，将联邦学习明文代码中的计算模块的多个基础算子替换为对应的加密算子，即可获得加密联邦学习代码。

[0104] 如图3所示，可以预先针对不同的数据处理任务，抽象出一些基础算子，如联合统计、机器学习、深度学习，抽取通用的基本计算算子，形成两层基本算子结构。图3中，针对不同的业务中涉及的不同数据处理技术，通过细粒度化抽取，可以形成基础算子，基础算子包括第一基础算子和第二基础算子，第二基础算子可以由第一基础算子形成，第二基础算子可以构建出不同的数据处理技术。

[0105] 然后可以通过预设加密算法(如全同态加密算法或多方安全计算)，对第一基础算子和第二基础算子进行加密，获得加密算子(包括第一加密算子和第二加密算子)，如图4所

示。

[0106] 下面针对全同态加密算法和多方安全计算，获得加密算子的过程进行详细介绍。以加法算子为例，来分别介绍两种加密算法的实现过程。

[0107] 假设A、B两方分别输入数据X、Y，对输入数据进行求和计算，A作为发起方来协调整体执行逻辑，B作为参与方。采用多方安全计算进行加密的过程如图5所示，多方安全计算(MPC)实现安全的加法计算，原始数据全程都以碎片形式公开，不存在暴露风险。

[0108] 计算过程如下：

[0109] (1)发起方方A、参与方B分别针对各自持有的数据X，Y进行碎片化；这里的碎片化是指将原始数据拆分，在方案场景下，即X拆分为Xa、Xb，其中X = Xa + Xb。同理，Y拆分为Ya、Yb。

[0110] (2)分发部分碎片，发起方A将碎片Xb发送给参与方B，参与方B将碎片Ya发送给参与方A。

[0111] (3)发起方A持有碎片Xa、Ya；参与方B持有碎片Xb、Yb。

[0112] (4)各方分别在各自本地执行碎片加法，即A方执行SUMa = Xa + Ya；B方执行SUMb = Xb + Yb。这样就得到了碎片状态的加法结果。

[0113] 采用全同态加密算法(FHE)的过程如图6所示，全同态加密算法能够支持任意次的加法和乘法运算，采用的是同态加密实现安全的加法计算，原始数据全程都以密态形式公开，不存在暴露风险。执行过程如下：

[0114] (1)发起方A首先生成同态加密的公私钥，并且将公钥发送给参与方B。

[0115] (2)参与方B本地生成随机数R，并对持有的原始数据Y进行混淆，也就是计算Y-R。

[0116] (3)各方执行同态加密，发起方A对自身持有的数据进行同态加密，参与方B对混淆数据Y-R以及随机数R进行同态加密，得到密态数据，以[]表示。

[0117] (4)发起方A执行密态加法计算，得到[X+Y-R]，这样就得到了密态的加法结果，而由于随机数是存在于参与方B本地，发起方A在没有授权[R]信息的情况下，也无法解密。

[0118] 同理对于其他基础算子，也可以按照同样的加密算法，获得加密算子。

[0119] 所以，在进行基础算子替换时，先对计算模块进行编译解析，得到每一个计算模块中的操作算子符、依赖参数以及输出。比如明文中的计算指令：y=x*w，则将被解析成“*,x|w,y”，解析结果格式为：运算符、依赖参数、输出。这些运算符即称为基础算子。然后可通过基础算子与加密算子的映射关系，将其替换为加密算子，如乘法算子“*”替换为多方安全计算的加密算子mpc.mul()或者全同态加密的加密算子fhe.mul()，如图7和图8所示。本方案中涉及的基础算子包括两种，一种是最细粒度的算子，如乘法、加法、比较，另一类为基础函数算子，如sigmoid、relu、max、median等。

[0120] 在上述实现过程中，对计算模块进行解析，获得多个基础算子，然后将基础算子替换为加密算子，如此可以预先对基础算子进行加密获得加密算子，提高开发效率。

[0121] 在上述实施例的基础上，在获得加密联邦学习代码时，还可以实时对计算模块进行加密，如可以将发起方和参与方各自对应的联邦学习明文代码中的功能模块采用预设加密算法进行加密，获得加密功能模块，和/或，将发起方与参与方各自对应的联邦学习明文代码中的计算模块采用预设加密算法进行加密，获得加密计算模块，然后将功能模块替换为对应的加密功能模块，和/或，将计算模块替换为对应的加密计算模块。

[0122] 例如，如果发起方的联邦学习明文代码包括功能模块和计算模块，而参与方的联邦学习明文代码包括功能模块，则对于发起方，则可对功能模块采用预设加密算法（如多方安全计算或全同态加密算法）进行加密，获得加密功能模块，以及对计算模块采用预设加密算法（如多方安全计算或全同态加密算法）进行加密，获得加密计算模块，然后将功能模块替换为加密功能模块，以及将计算模块替换为加密计算模块，如此可获得发起方的加密联邦学习代码。对于参与方，则可对功能模块采用预设加密算法（如多方安全计算或全同态加密算法）进行加密，获得加密功能模块，然后将功能模块替换为加密功能模块，如此可获得参与方的加密联邦学习代码。

[0123] 需要说明的是，对于计算模块的加密，和上述对基础算子的加密方式类似，如可以对计算模块进行编译解析，获得操作运输符（即基础算子），然后可采用多方安全计算或全同态加密算法对操作运输符进行加密，获得加密算子，加密算子即可构成加密计算模块，具体过程可参照上述实施例的描述，在此不再重复赘述。同理，对功能模块，可以采用多方安全计算或全同态加密算法进行整体加密。

[0124] 在上述实现过程中，也可以对功能模块和计算模块进行实时加密，这样避免提前加密一些使用效率不高的模块，浪费加密资源的问题。

[0125] 本申请中，可以将发起方的明文标准代码进行编译转换，快速转换为发起方和参与方的加密联邦学习代码，如图9所示。本方案只需要维护功能框架模块和计算框架模块，或者加密算子即可，就可以应对新的不同数据处理任务的加密联邦学习代码的开发。

[0126] 开发人员只需要开发功能框架模块、计算框架模块以及基础算子即可，由于不同算法都存在相通的功能或者计算都那样，所以可通过组合功能框架模块和计算框架模块，如此能够应有的更多不同算法的联邦学习代码的开发。而且对功能框架模块进行抽象，可以形成针对不同角色以及通用的功能框架模块，在代码生成过程中可以以模块复用的形式添加到整体代码逻辑中，可快速实现代码的开发，保证算法的完整性。算法的安全性由加密算子、加密模块来保证，整体代码无需关心数据加密的问题，可有效提高代码的开发效率。

[0127] 并且，本方案可以应用于数据统计、模型训练等场景，如图10所示的模型训练场景下发起方和参与方之间的联邦学习过程，以及如图11所示的数据统计场景下发起方和参与方之间的联邦学习过程，这样可快速扩展到广告计算、个性化推荐、金融风控等不同的场景。所以，本申请可以提供一种相对通用的方式，快速生成联邦学习代码，解决不同企业不同业务涉及到的数据处理算法需要快速生成联邦学习代码的问题，以较低的成本代价赋能传统企业或者互联网企业开发出针对自身业务的联邦学习代码，降低联邦学习代码的开发难度，明显提升联邦学习代码的开发效率。

[0128] 请参照图12，图12为本申请实施例提供的一种联邦学习代码生成装置200的结构框图，该装置200可以是电子设备上的模块、程序段或代码。应理解，该装置200与上述图1方法实施例对应，能够执行图1方法实施例涉及的各个步骤，该装置200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。

[0129] 可选地，所述装置200包括：

[0130] 模板信息获取模块210，用于获取数据处理任务的发起方与参与方各自对应的联邦学习流程模板信息，其中，所述联邦学习流程模板信息用于表征对所述数据处理任务进行联邦学习的数据处理逻辑，所述联邦学习流程模板信息包括功能框架模块和/或计算框

架模块，所述功能框架模块是指用于实现所述数据处理任务的通用功能的框架程序，所述计算框架模块是指用于实现所述数据处理任务的特定算法的框架程序；

[0131] 明文代码获取模块220，用于获取所述发起方实现所述数据处理任务的明文标准代码；

[0132] 明文代码生成模块230，用于基于所述明文标准代码和各自对应的联邦学习流程模板信息，生成所述发起方与所述参与方各自对应的联邦学习明文代码，其中，所述联邦学习明文代码包括功能模块和/或计算模块，所述功能模块是利用所述明文标准代码中的通用功能代码和所述功能框架模块生成的，所述计算模块是利用所述明文标准代码中的特定算法代码和所述计算框架模块生成的；

[0133] 加密代码生成模块240，用于将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块替换为加密功能模块和/或将计算模块替换为加密计算模块，生成所述发起方与所述参与方各自对应的加密联邦学习代码。

[0134] 可选地，所述加密代码生成模块240，用于将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块采用预设加密算法进行加密，获得加密功能模块；和/或，获取所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块对应的预先加密的加密计算模块；将功能模块替换为对应的加密功能模块，和/或，将计算模块替换为对应的加密计算模块。

[0135] 可选地，所述加密代码生成模块240，用于对所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块进行解析，获得计算模块对应的多个基础算子；获取每个基础算子对应的预先加密的加密算子，加密计算模块包括多个加密算子。

[0136] 可选地，所述加密代码生成模块240，用于将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块采用预设加密算法进行加密，获得加密功能模块；和/或，将所述发起方与所述参与方各自对应的联邦学习明文代码中的计算模块采用预设加密算法进行加密，获得加密计算模块；将功能模块替换为对应的加密功能模块，和/或，将计算模块替换为对应的加密计算模块。

[0137] 可选地，所述预设加密算法为全同态加密算法或多方安全计算。

[0138] 可选地，所述装置200还包括：

[0139] 配置模块，用于配置不同角色方对应的角色配置信息；根据所述角色配置信息配置发起方或参与方。

[0140] 可选地，功能框架模块为预先针对不同的数据处理任务的发起方或参与方所配置的，计算框架模块为预先针对不同的数据处理任务的发起方或参与方所配置的，所述联邦学习流程模板信息包含实现所述数据处理任务对应的功能框架模块和/或计算框架模块。

[0141] 需要说明的是，本领域技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的装置的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再重复描述。

[0142] 请参照图13，图13为本申请实施例提供的一种用于执行联邦学习代码生成方法的电子设备的结构示意图，所述电子设备可以包括：至少一个处理器310，例如CPU，至少一个通信接口320，至少一个存储器330和至少一个通信总线340。其中，通信总线340用于实现这些组件直接的连接通信。其中，本申请实施例中设备的通信接口320用于与其他节点设备进行信令或数据的通信。存储器330可以是高速RAM存储器，也可以是非易失性的存储器(non-

volatile memory)，例如至少一个磁盘存储器。存储器330可选的还可以是至少一个位于远离前述处理器的存储装置。存储器330中存储有计算机可读取指令，当所述计算机可读取指令由所述处理器310执行时，电子设备执行上述图1所示方法过程。

[0143] 可以理解，图13所示的结构仅为示意，所述电子设备还可包括比图13中所示更多或者更少的组件，或者具有与图13所示不同的配置。图13中所示的各组件可以采用硬件、软件或其组合实现。

[0144] 本申请实施例提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时，执行如图1所示方法实施例中电子设备所执行的方法过程。

[0145] 本实施例公开一种计算机程序产品，所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算机程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，计算机能够执行上述各方法实施例所提供的方法，例如，包括：

[0146] 获取数据处理任务的发起方与参与方各自对应的联邦学习流程模板信息，其中，所述联邦学习流程模板信息用于表征对所述数据处理任务进行联邦学习的数据处理逻辑，所述联邦学习流程模板信息包括功能框架模块和/或计算框架模块，所述功能框架模块是指用于实现所述数据处理任务的通用功能的框架程序，所述计算框架模块是指用于实现所述数据处理任务的特定算法的框架程序；

[0147] 获取所述发起方实现所述数据处理任务的明文标准代码；

[0148] 基于所述明文标准代码和各自对应的联邦学习流程模板信息，生成所述发起方与所述参与方各自对应的联邦学习明文代码，其中，所述联邦学习明文代码包括功能模块和/或计算模块，所述功能模块是利用所述明文标准代码中的通用功能代码和所述功能框架模块生成的，所述计算模块是利用所述明文标准代码中的特定算法代码和所述计算框架模块生成的；

[0149] 将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块替换为加密功能模块和/或将计算模块替换为加密计算模块，生成所述发起方与所述参与方各自对应的加密联邦学习代码。

[0150] 综上所述，本申请实施例提供一种联邦学习代码生成方法、装置、电子设备及存储介质，该方法通过获取数据处理任务的发起方与参与方各自对应的联邦学习流程模板信息，该联邦学习流程模板信息是由预先配置的功能框架模块和/或计算框架模块构成的，然后可利用联邦学习流程模板信息将发起方的明文标准代码转换为联邦学习代码，这样可以针对不同的数据处理任务的发起方和参与方灵活配置联邦学习流程模板信息，从而可以针对不同的数据处理任务快速开发出对应的联邦学习代码，能够应对更多的数据处理任务，并且，算法的安全性由加密功能模块和加密计算模块来保证，整体代码无需关心数据加密的问题，进而可以降低联邦学习代码的开发难度以及提高联邦学习代码的开发效率。

[0151] 在本申请所提供的实施例中，应该理解到，所揭露装置和方法，可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，又例如，多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些通信接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0152] 另外，作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0153] 再者，在本申请各个实施例中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。

[0154] 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。

[0155] 以上所述仅为本申请的实施例而已，并不用于限制本申请的保护范围，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

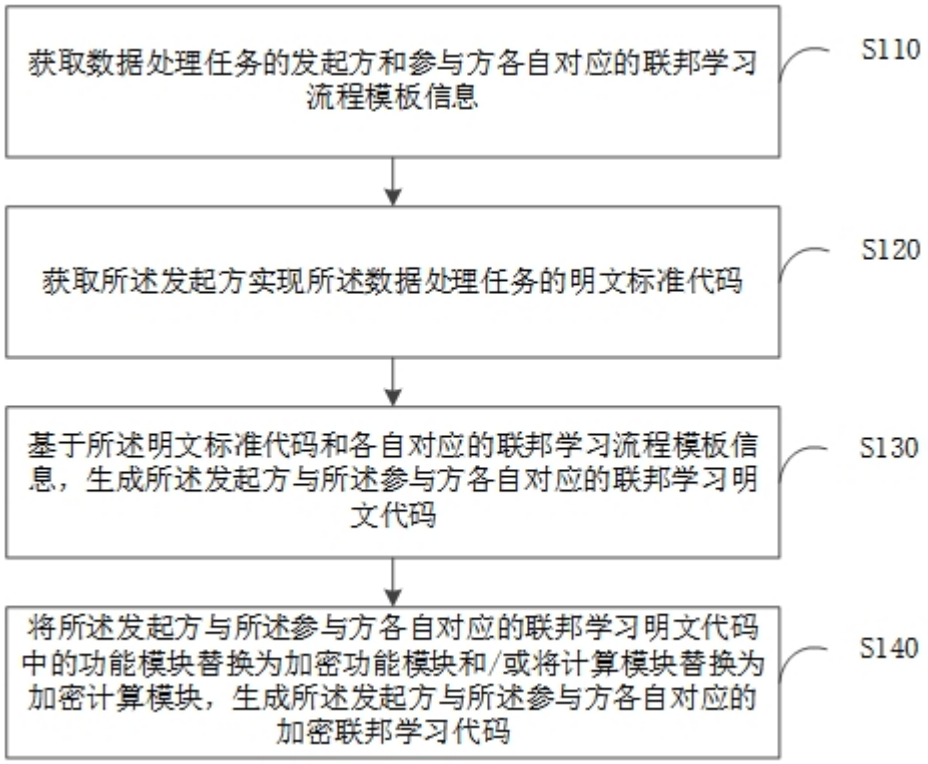

获取数据处理任务的发起方和参与方各自对应的联邦学习流程模板信息
S110
获取所述发起方实现所述数据处理任务的明文标准代码
S120
基于所述明文标准代码和各自对应的联邦学习流程模板信息，生成所述发起方与所述参与方各自对应的联邦学习明文代码
S130
将所述发起方与所述参与方各自对应的联邦学习明文代码中的功能模块替换为加密功能模块和/或将计算模块替换为加密计算模块，生成所述发起方与所述参与方各自对应的加密联邦学习代码
S140

图1


标签方
特征方
角色模块
Label_datahandler
Feature_datahandler
通用模块
report
Data_saver

图2

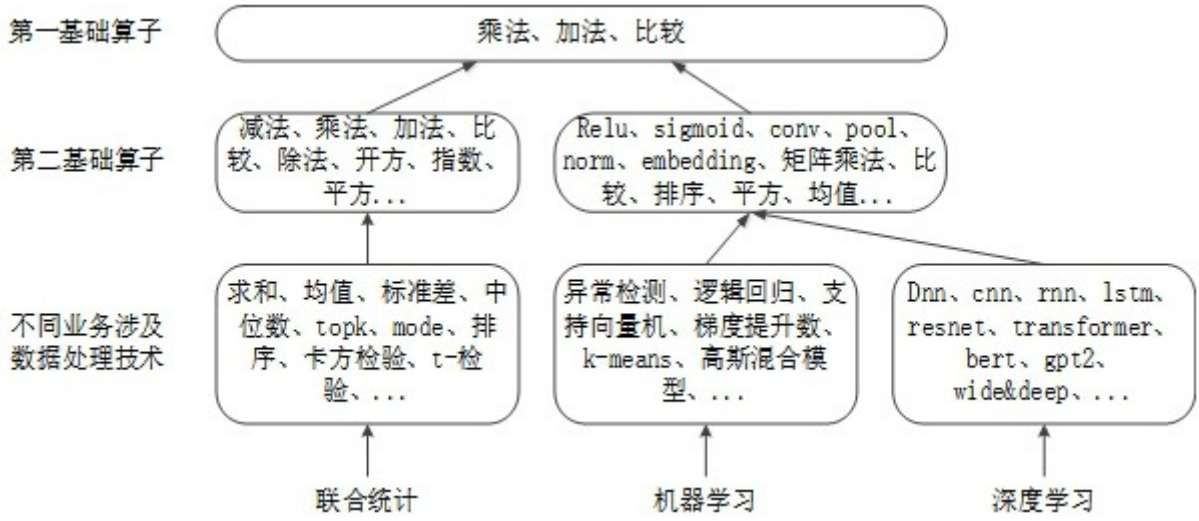

第一基础算子
乘法、加法、比较
第二基础算子
减法、乘法、加法、比较、除法、开方、指数、平方...
Relu、sigmoid、conv、pool、norm、embedding、矩阵乘法、比较、排序、平方、均值...
不同业务涉及数据处理技术
求和、均值、标准差、中位数、topk、mode、排序、卡方检验、t-检验、...
异常检测、逻辑回归、支持向量机、梯度提升数、k-means、高斯混合模型、...
Dnn、cnn、rnn、lstm、resnet、transformer、bert、gpt2、wide&deep、...
联合统计
机器学习
深度学习

图3

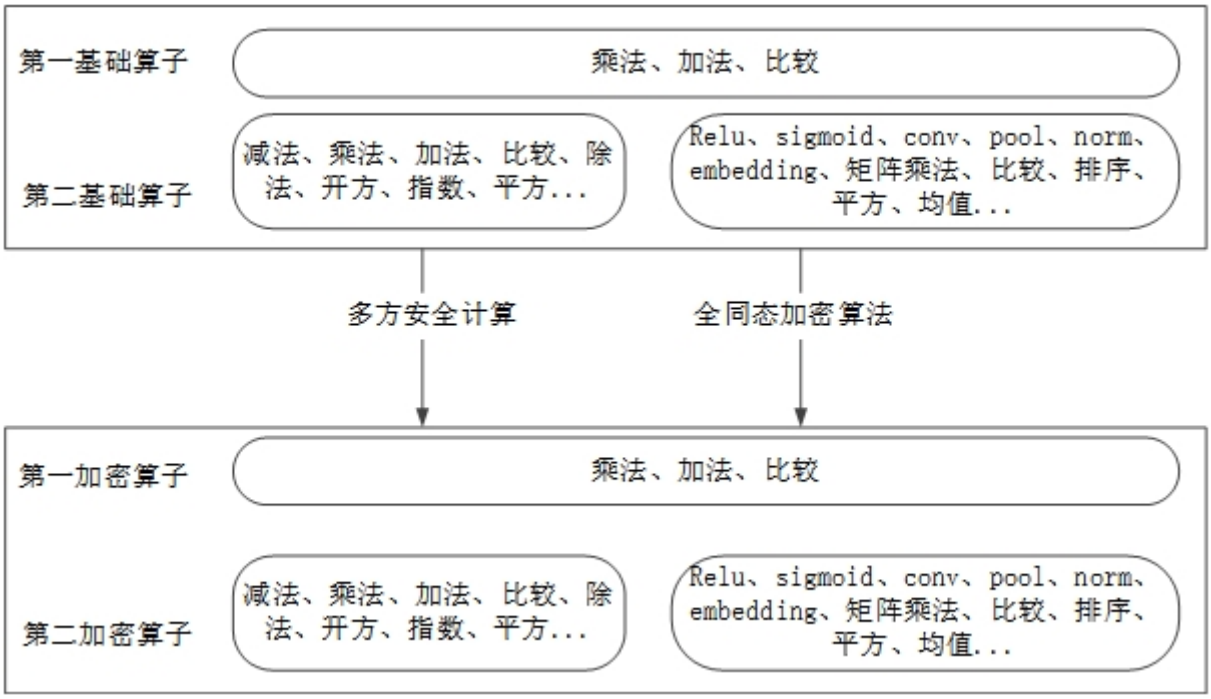

第一基础算子
乘法、加法、比较
第二基础算子
减法、乘法、加法、比较、除法、开方、指数、平方...
Relu、sigmoid、conv、pool、norm、embedding、矩阵乘法、比较、排序、平方、均值...
多方安全计算
全同态加密算法
第一加密算子
乘法、加法、比较
第二加密算子
减法、乘法、加法、比较、除法、开方、指数、平方...
Relu、sigmoid、conv、pool、norm、embedding、矩阵乘法、比较、排序、平方、均值...

图4

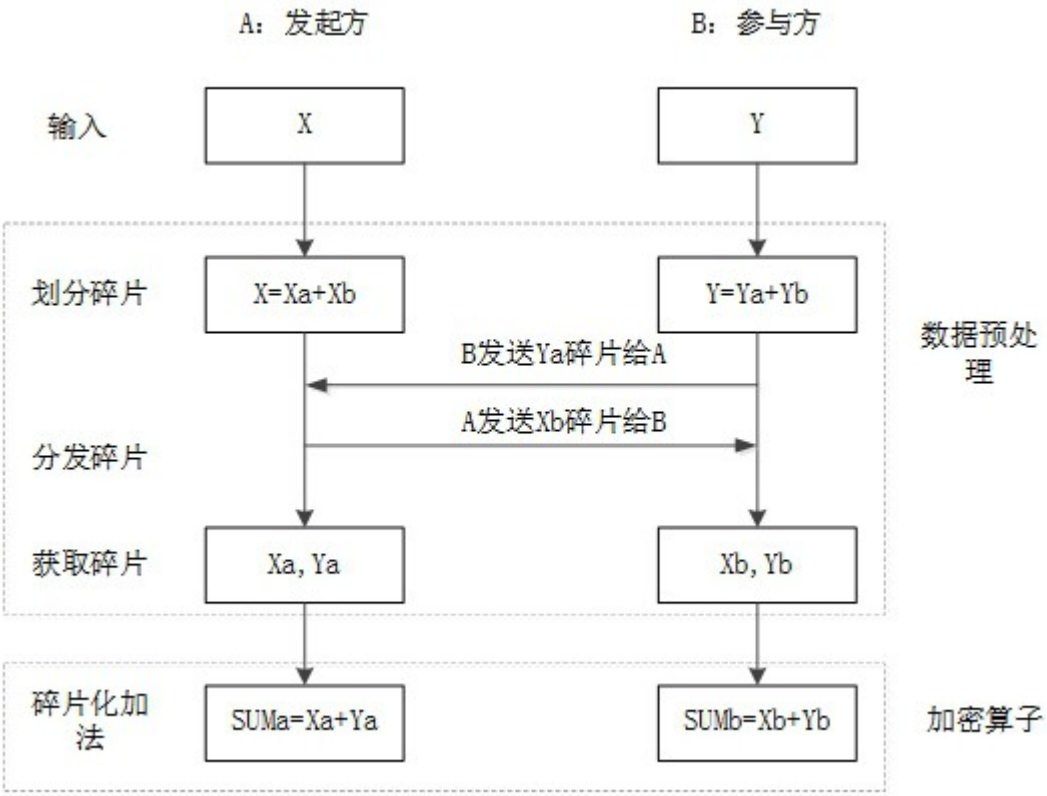

A：发起方
B：参与方
输入
X
Y
划分碎片
X=Xa+Xb
Y=Ya+Yb
数据预处理
B发送Ya碎片给A
A发送Xb碎片给B
分发碎片
获取碎片
Xa,Ya
Xb,Yb
碎片化加法
SUMa=Xa+Ya
SUMb=Xb+Yb
加密算子

图5

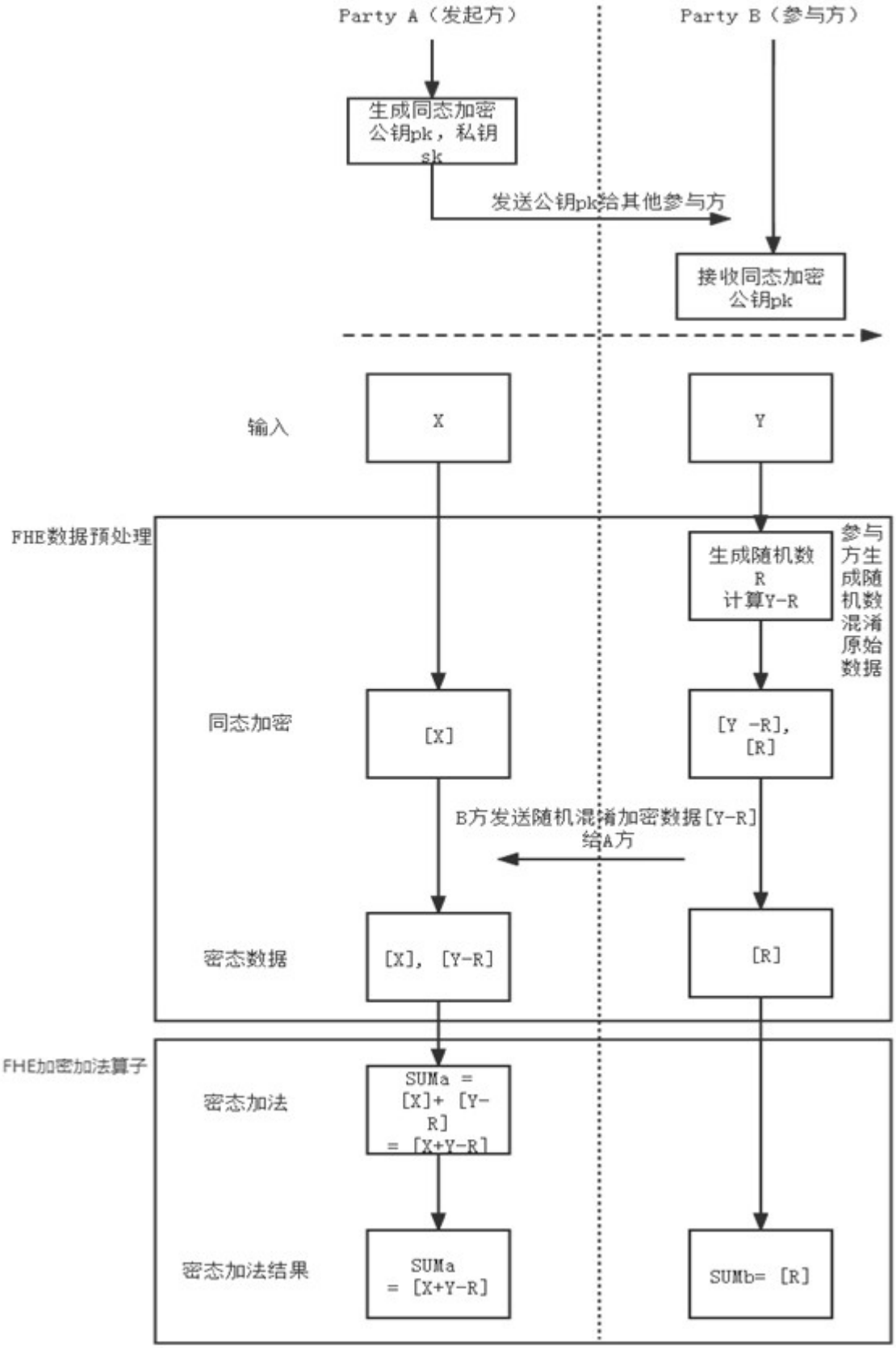

Party A（发起方）
Party B（参与方）
生成同态加密公钥pk，私钥sk
发送公钥pk给其他参与方
接收同态加密公钥pk
输入
X
Y
FHE数据预处理
生成随机数R
计算Y-R
参与方生成随机数混淆原始数据
同态加密
[X]
[Y -R], [R]
B方发送随机混淆加密数据[Y-R]给A方
密态数据
[X], [Y-R]
[R]
FHE加密加法算子
密态加法
SUMa = [X]+ [Y-R] = [X+Y-R]
密态加法结果
SUMa = [X+Y-R]
SUMb= [R]

图6

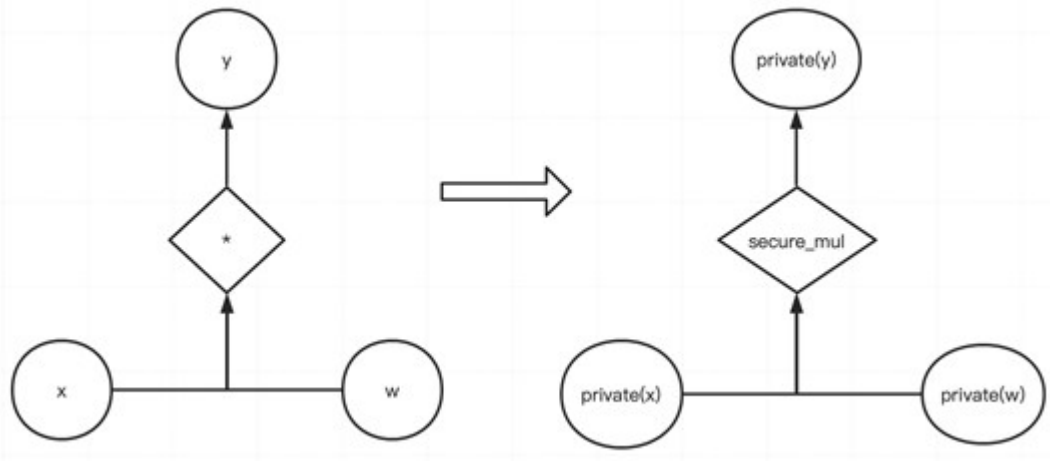

y
*
x
w
private(y)
secure_mul
private(x)
private(w)

图7

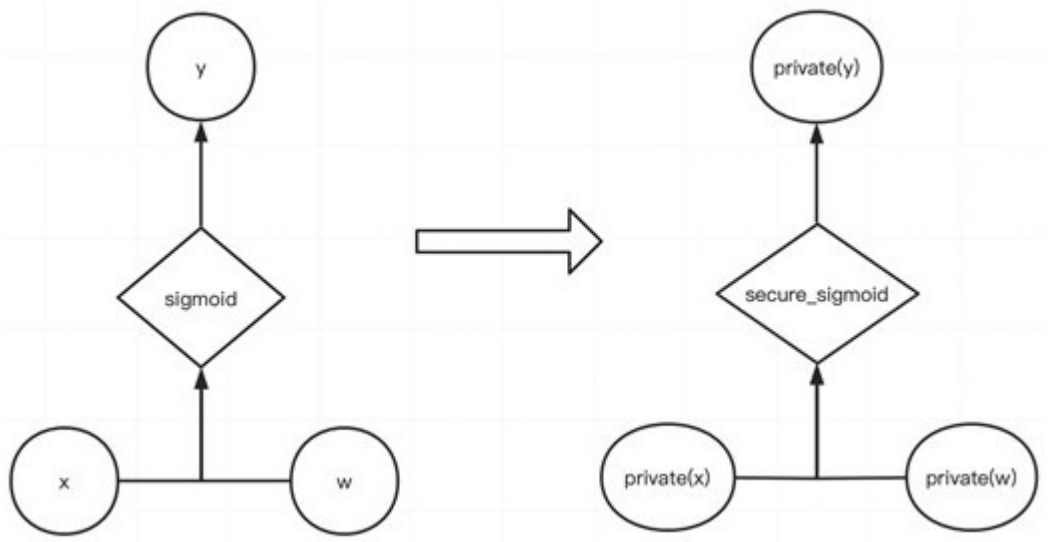

y
sigmoid
x
w
private(y)
secure_sigmoid
private(x)
private(w)

图8

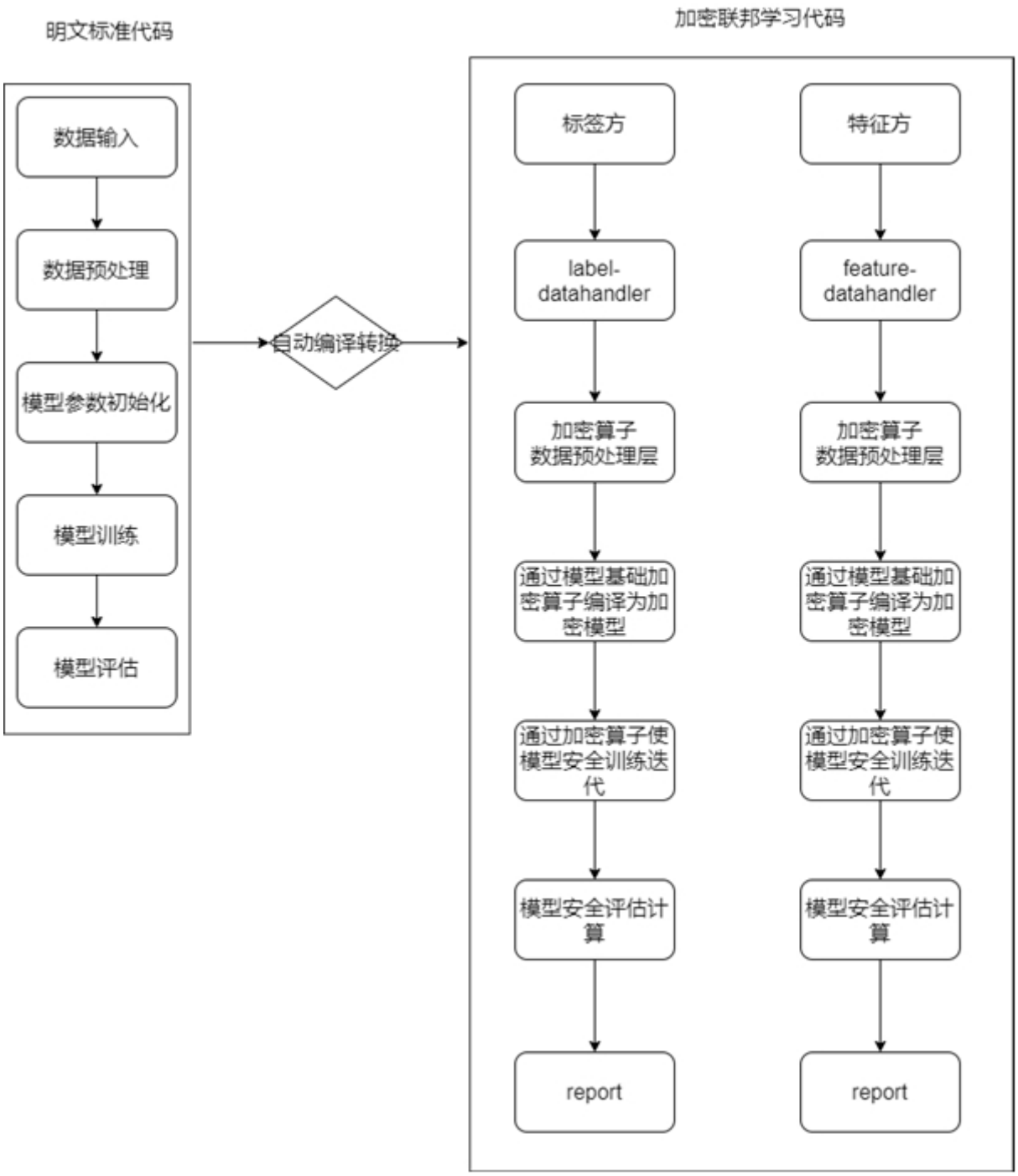

明文标准代码
数据输入
数据预处理
模型参数初始化
模型训练
模型评估
自动编译转换
加密联邦学习代码
标签方
特征方
label-datahandler
feature-datahandler
加密算子数据预处理层
加密算子数据预处理层
通过模型基础加密算子编译为加密模型
通过模型基础加密算子编译为加密模型
通过加密算子使模型安全训练迭代
通过加密算子使模型安全训练迭代
模型安全评估计算
模型安全评估计算
report
report

图9

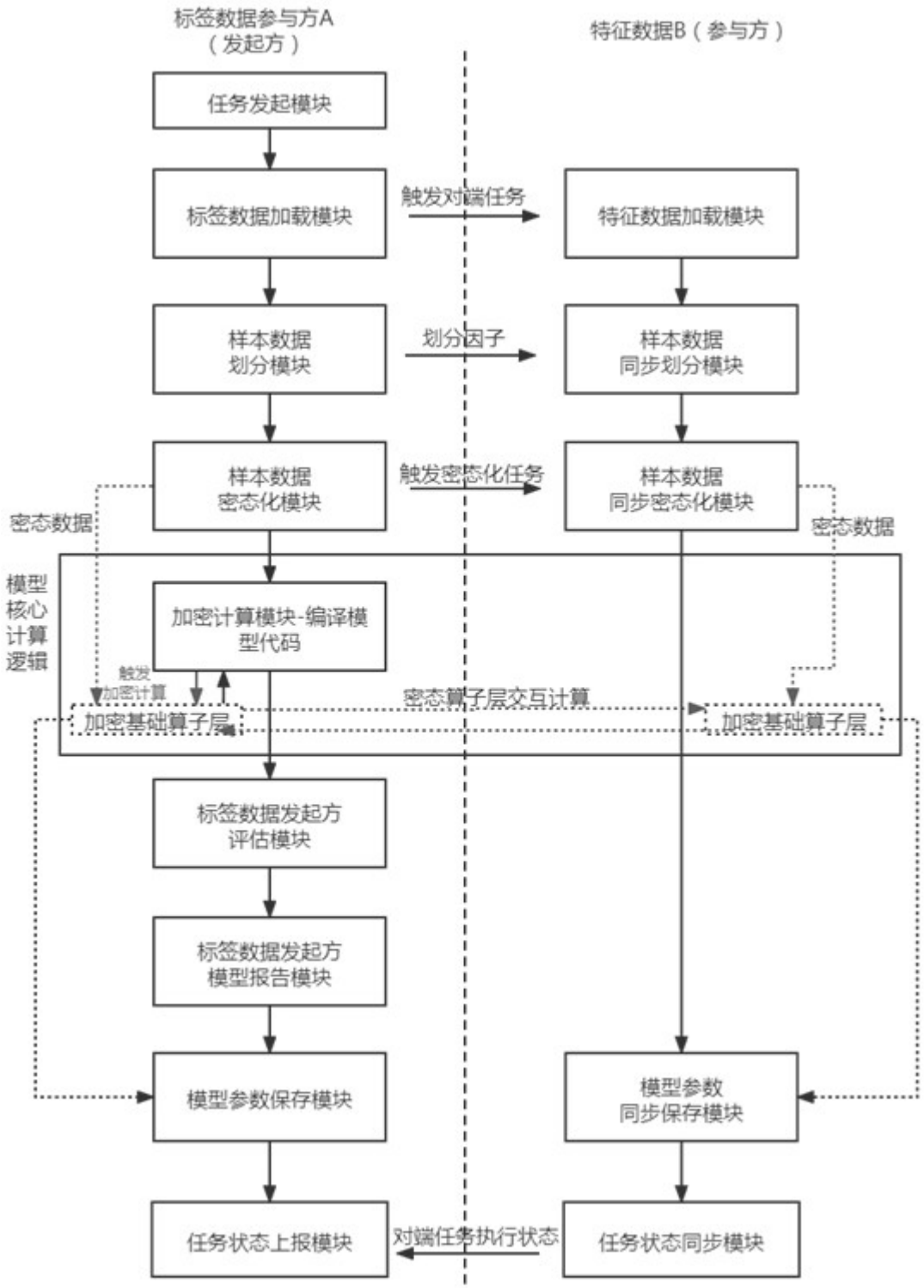

标签数据参与方A
（发起方）
特征数据B（参与方）
任务发起模块
标签数据加载模块
触发对端任务
特征数据加载模块
样本数据
划分模块
划分因子
样本数据
同步划分模块
样本数据
密态化模块
触发密态化任务
样本数据
同步密态化模块
密态数据
密态数据
模型
核心
计算
逻辑
加密计算模块-编译模型代码
触发
加密计算
密态算子层交互计算
加密基础算子层
加密基础算子层
标签数据发起方
评估模块
标签数据发起方
模型报告模块
模型参数保存模块
模型参数
同步保存模块
任务状态上报模块
对端任务执行状态
任务状态同步模块

图10

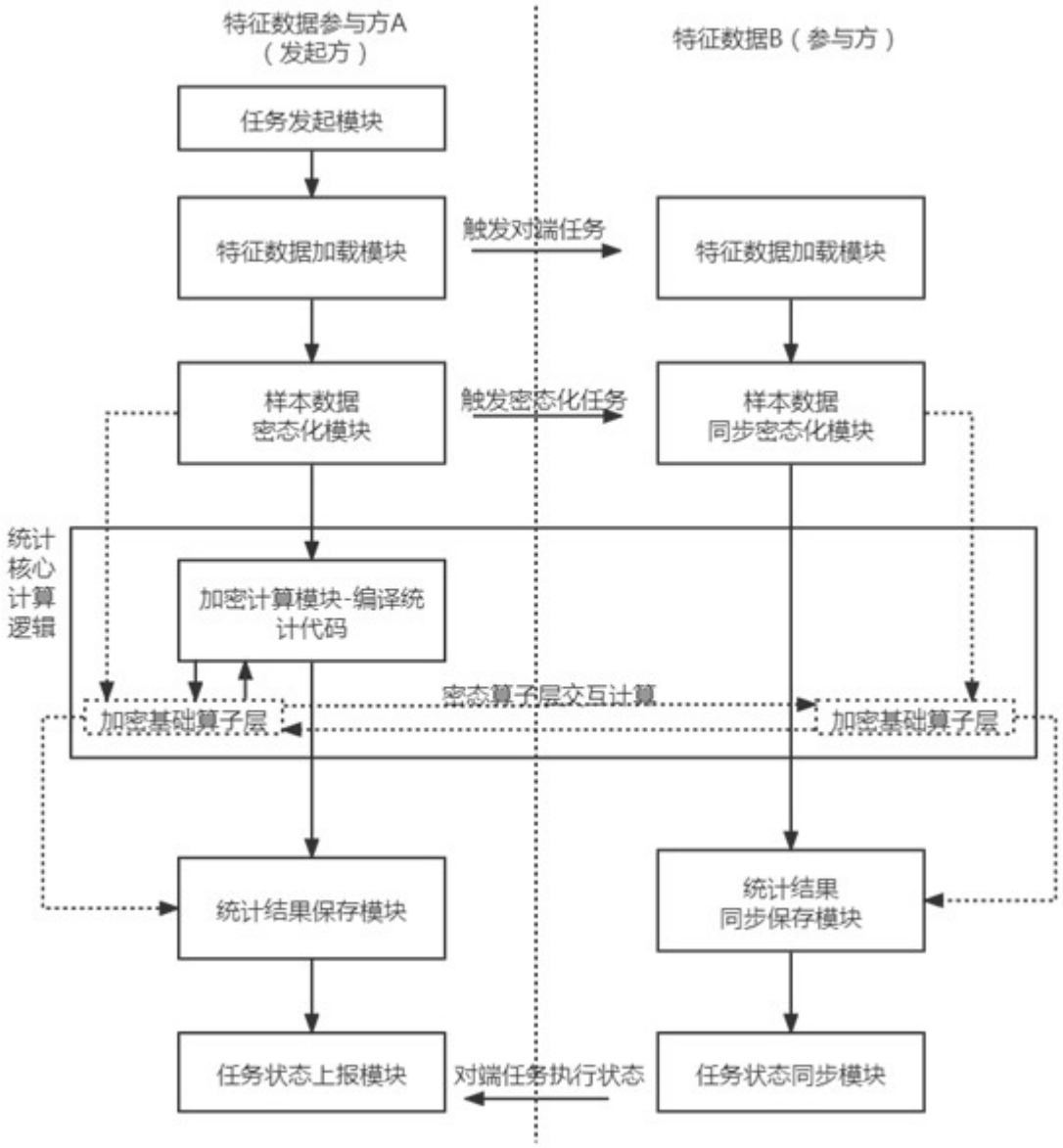

特征数据参与方A
（发起方）
特征数据B（参与方）
任务发起模块
特征数据加载模块
触发对端任务
特征数据加载模块
样本数据
密态化模块
触发密态化任务
样本数据
同步密态化模块
统计
核心
计算
逻辑
加密计算模块-编译统
计代码
密态算子层交互计算
加密基础算子层
加密基础算子层
统计结果保存模块
统计结果
同步保存模块
任务状态上报模块
对端任务执行状态
任务状态同步模块

图11

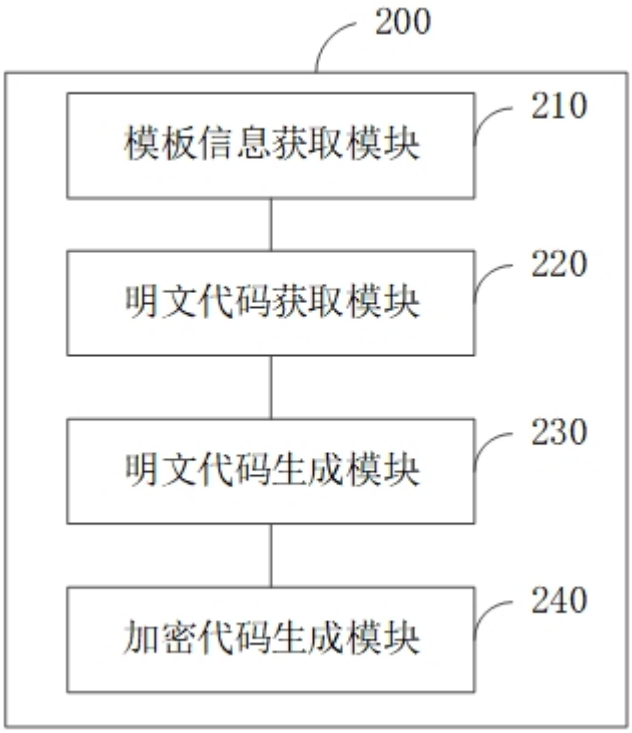

200
模板信息获取模块
210
明文代码获取模块
220
明文代码生成模块
230
加密代码生成模块
240

图12

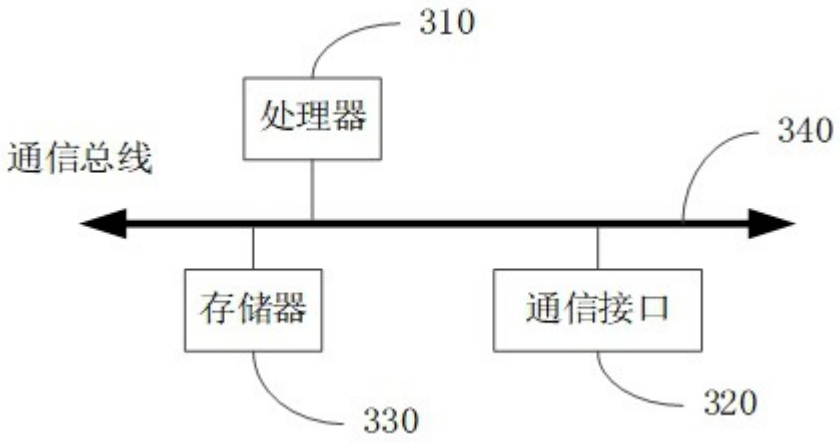

310
处理器
通信总线
340
存储器
通信接口
330
320

图13