

权 利 要 求 书

1、一种使用待交换数据来执行机器学习的设备，包括至少一个计算装置和至少一个存储指令的存储装置，其中，所述指令在被所述至少一个计算装置运行时，促使所述至少一个计算装置执行以下步骤：

从第一数据提供方接收第一初次加密结果数据和从第二数据提供方接收第二初次加密结果数据；

将第一初次加密结果数据发送到第二数据提供方和将第二初次加密结果数据发送到第一数据提供方；

从第一数据提供方接收第二再次加密结果数据和从第二数据提供方接收第一再次加密结果数据；以及

通过将第一再次加密结果数据与第二再次加密结果数据进行拼接来获取机器学习样本，并基于机器学习样本来执行机器学习。

2、如权利要求1所述的设备，其中，

第一初次加密结果数据由第一数据提供方通过使用第一加密函数对第一待交换数据进行加密而得，第二初次加密结果数据由第二数据提供方通过使用第二加密函数对第二待交换数据进行加密而得，其中，第一待交换数据与第二待交换数据至少部分对应；

第一再次加密结果数据由第二数据提供方通过使用第二加密函数对第一初次加密结果数据进行加密而得，第二再次加密结果数据由第一数据提供方通过使用第一加密函数对第二初次加密结果数据进行加密而得。

3、如权利要求2所述的设备，其中，第一待交换数据之中的每条第一待交换数据记录至少包括标识信息和属性信息，第二待交换数据之中的每条第二待交换数据记录至少包括标识信息和关于机器学习目标的标记信息。

4、如权利要求2所述的设备，其中，第一加密函数为第一数据提供方的私有函数，第二加密函数为第二数据提供方的私有函数，并且，第一加密函数和第二加密函数之间构成单向可交换私有函数。

5、如权利要求2所述的设备，其中，第一加密函数为具有第一私有大素数的第一幂函数，第二加密函数为具有第二私有大素数的第二幂函数。

6、如权利要求1所述的设备，其中，机器学习样本为机器学习训练样本、机器学习测试样本或机器学习预测样本，并且，机器学习执行单元基于机器学习样本来训练机器学习模型、测试机器学习模型或使用机器学习模型来进行预测。

7、一种由计算装置使用待交换数据来执行机器学习的方法，包括：

从第一数据提供方接收第一初次加密结果数据和从第二数据提供方接收

第二初次加密结果数据；

将第一初次加密结果数据发送到第二数据提供方和将第二初次加密结果数据发送到第一数据提供方；

5 从第一数据提供方接收第二再次加密结果数据和从第二数据提供方接收第一再次加密结果数据；以及

通过将第一再次加密结果数据与第二再次加密结果数据进行拼接来获取机器学习样本，并基于机器学习样本来执行机器学习。

8、如权利要求7所述的方法，其中，

10 第一初次加密结果数据由第一数据提供方通过使用第一加密函数对第一待交换数据进行加密而得，第二初次加密结果数据由第二数据提供方通过使用第二加密函数对第二待交换数据进行加密而得，其中，第一待交换数据与第二待交换数据至少部分对应；

15 第一再次加密结果数据由第二数据提供方通过使用第二加密函数对第一初次加密结果数据进行加密而得，第二再次加密结果数据由第一数据提供方通过使用第一加密函数对第二初次加密结果数据进行加密而得。

9、如权利要求8所述的方法，其中，第一待交换数据之中的每条第一待交换数据记录至少包括标识信息和属性信息，第二待交换数据之中的每条第二待交换数据记录至少包括标识信息和关于机器学习目标的标记信息。

20 10、如权利要求8所述的方法，其中，第一加密函数为第一数据提供方的私有函数，第二加密函数为第二数据提供方的私有函数，并且，第一加密函数和第二加密函数之间构成单向可交换私有函数。

11、如权利要求8所述的方法，其中，第一加密函数为具有第一私有素数的第一幂函数，第二加密函数为具有第二私有素数的第二幂函数。

25 12、如权利要求7所述的方法，其中，机器学习样本为机器学习训练样本、机器学习测试样本或机器学习预测样本，并且，所述基于机器学习样本来执行机器学习为基于机器学习样本来训练机器学习模型、测试机器学习模型或使用机器学习模型来进行预测。

30 13、一种数据提供设备，包括至少一个计算装置和至少一个存储指令的存储装置，其中，所述指令在被所述至少一个计算装置运行时，促使所述至少一个计算装置执行以下步骤：

35 使用第一加密函数对第一待交换数据进行加密而得到第一初次加密结果数据，将第一初次加密结果数据发送到机器学习执行设备，从机器学习执行设备接收第二初次加密结果数据，通过使用第一加密函数对第二初次加密结果数据进行加密而得到第二再次加密结果数据，将第二再次加密结果数据发送给机器学习执行设备；

或者，使用第二加密函数对第二待交换数据进行加密而得到第二初次加

密结果数据，将第二初次加密结果数据发送到机器学习执行设备，从机器学习执行设备接收第一初次加密结果数据，通过使用第二加密函数对第一初次加密结果数据进行加密而得到第一再次加密结果数据，将第一再次加密结果数据发送给机器学习执行设备。

- 5 14、如权利要求 13 所述的数据提供设备，其中，
 第一待交换数据之中的每条第一待交换数据记录至少包括标识信息和属性信息；

 第二待交换数据之中的每条第二待交换数据记录至少包括标识信息和关于机器学习目标的标记信息。

- 10 15、如权利要求 13 所述的数据提供设备，其中，第一加密函数为第一数据提供方的私有函数，第二加密函数为第二数据提供方的私有函数，并且，第一加密函数和第二加密函数之间构成单向可交换私有函数。

- 15 16、如权利要求 13 所述的数据提供设备，其中，第一加密函数为具有第一私有大素数的第一幂函数，第二加密函数为具有第二私有大素数的第二幂函数。

 17、一种由计算装置执行的数据提供方法，包括：

- 20 使用第一加密函数对第一待交换数据进行加密而得到第一初次加密结果数据，将第一初次加密结果数据发送到机器学习执行设备，从机器学习执行设备接收第二初次加密结果数据，使用第一加密函数对第二初次加密结果数据进行加密而得到第二再次加密结果数据，将第二再次加密结果数据发送给机器学习执行设备；

- 25 或者，使用第二加密函数对第二待交换数据进行加密而得到第二初次加密结果数据，将第二初次加密结果数据发送到机器学习执行设备，从机器学习执行设备接收第一初次加密结果数据，使用第二加密函数对第一初次加密结果数据进行加密而得到第一再次加密结果数据，将第一再次加密结果数据发送给机器学习执行设备。

- 30 18、如权利要求 17 所述的方法，其中，
 第一待交换数据之中的每条第一待交换数据记录至少包括标识信息和属性信息；

 第二待交换数据之中的每条第二待交换数据记录至少包括标识信息和关于机器学习目标的标记信息。

- 35 19、如权利要求 17 所述的方法，其中，第一加密函数为第一数据提供方的私有函数，第二加密函数为第二数据提供方的私有函数，并且，第一加密函数和第二加密函数之间构成单向可交换私有函数。

 20、如权利要求 17 所述的方法，其中，第一加密函数为具有第一私有大

素数的第一幂函数，第二加密函数为具有第二私有大素数的第二幂函数。

21、一种执行机器学习的系统，包括：

第一数据提供方设备，被配置为通过使用第一加密函数对第一待交换数据进行加密而得到第一初次加密结果数据；

- 5 第二数据提供方设备，被配置为通过使用第二加密函数对第二待交换数据进行加密而得到第二初次加密结果数据，其中，第一待交换数据与第二待交换数据至少部分对应；

10 机器学习执行设备，被配置为分别从第一数据提供方接收第一初次加密结果数据和从第二数据提供方接收第二初次加密结果数据，并分别将第一初次加密结果数据发送到第二数据提供方和将第二初次加密结果数据发送到第一数据提供方，

15 其中，第一数据提供方通过使用第一加密函数对第二初次加密结果数据进行加密而得到第二再次加密结果数据，第二数据提供方通过使用第二加密函数对第一初次加密结果数据进行加密而得到第一再次加密结果数据，并且，机器学习执行设备分别从第一数据提供方接收第二再次加密结果数据和从第二数据提供方接收第一再次加密结果数据，并通过将第一再次加密结果数据与第二再次加密结果数据进行拼接来获取机器学习样本，以基于机器学习样本来执行机器学习。

20 22、如权利要求 21 所述的系统，其中，第一待交换数据之中的每条第一待交换数据记录至少包括标识信息和属性信息，第二待交换数据之中的每条第二待交换数据记录至少包括标识信息和关于机器学习目标的标记信息。

23、如权利要求 21 所述的系统，其中，第一加密函数为第一数据提供方的私有函数，第二加密函数为第二数据提供方的私有函数，并且，第一加密函数和第二加密函数之间构成单向可交换私有函数。

25 24、如权利要求 21 所述的系统，其中，第一加密函数为具有第一私有大素数的第一幂函数，第二加密函数为具有第二私有大素数的第二幂函数。

30 25、如权利要求 21 所述的系统，其中，机器学习样本为机器学习训练样本、机器学习测试样本或机器学习预测样本，并且，机器学习执行设备基于机器学习样本来训练机器学习模型、测试机器学习模型或使用机器学习模型来进行预测。

26、一种执行机器学习的方法，包括：

由第一数据提供方通过使用第一加密函数对第一待交换数据进行加密而得到第一初次加密结果数据；

35 由第二数据提供方通过使用第二加密函数对第二待交换数据进行加密而得到第二初次加密结果数据，其中，第一待交换数据与第二待交换数据至少部分对应；

由机器学习执行设备分别从第一数据提供方接收第一初次加密结果数据和从第二数据提供方接收第二初次加密结果数据，并分别将第一初次加密结果数据发送到第二数据提供方和将第二初次加密结果数据发送到第一数据提供方；

5 由第一数据提供方通过使用第一加密函数对第二初次加密结果数据进行加密而得到第二再次加密结果数据；

 由第二数据提供方通过使用第二加密函数对第一初次加密结果数据进行加密而得到第一再次加密结果数据由；

10 由机器学习执行设备分别从第一数据提供方接收第二再次加密结果数据和从第二数据提供方接收第一再次加密结果数据；以及

 由机器学习执行设备通过将第一再次加密结果数据与第二再次加密结果数据进行拼接来获取机器学习样本，以基于机器学习样本来执行机器学习。

27、一种使用待交换数据来执行机器学习的计算机可读存储介质，其中，在所述计算机可读存储介质上记录有用于执行如权利要求 7-12 和 17-20
15 中的任一权利要求所述的方法的计算机程序。

28、一种使用待交换数据来执行机器学习的设备，包括：

 初次加密数据接收单元，被配置为从第一数据提供方接收第一初次加密结果数据和从第二数据提供方接收第二初次加密结果数据；

20 初次加密数据发送单元，被配置为将第一初次加密结果数据发送到第二数据提供方和将第二初次加密结果数据发送到第一数据提供方；

 再次加密数据接收单元，被配置为从第一数据提供方接收第二再次加密结果数据和从第二数据提供方接收第一再次加密结果数据；以及

25 机器学习执行单元，被配置为通过将第一再次加密结果数据与第二再次加密结果数据进行拼接来获取机器学习样本，并基于机器学习样本来执行机器学习。