(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111885079 B
(45)授权公告日 2022.04.12

(21)申请号 202010763176.8
(22)申请日 2020.07.31
(65)同一申请的已公布的文献号
申请公布号 CN 111885079 A
(43)申请公布日 2020.11.03
(73)专利权人 支付宝(杭州)信息技术有限公司
地址 310000 浙江省杭州市西湖区西溪路556号8层B段801-11
专利权人 香港理工大学
(72)发明人 区文浩 薛海洋 杨如鹏 宫博睿 刘宏发
(74)专利代理机构 北京亿腾知识产权代理事务所(普通合伙) 11309
代理人 陈霁 周良玉
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/00(2022.01)
H04L 9/32(2006.01)

(56)对比文件
CN 110830232 A,2020.02.21
CN 109787743 A,2019.05.21
CN 107919965 A,2018.04.17
US 2015135329 A1,2015.05.14
贾福春 等.《机器学习算法在同态加密数据集上的应用》.《清华大学学报(自然科学版)》.2020,全文.

审查员 申杨

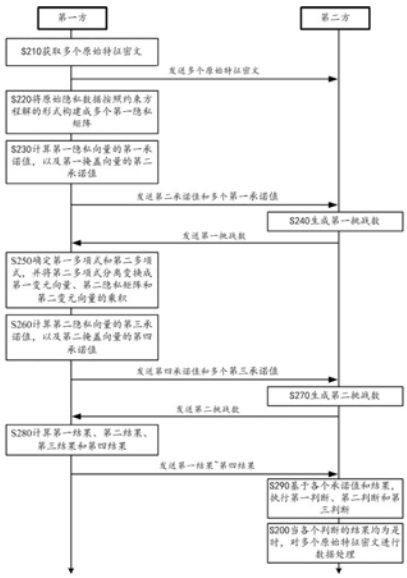
权利要求书6页 说明书24页 附图4页

(54)发明名称

保护数据隐私的多方联合处理数据的方法及装置

(57)摘要

本说明书实施例提供了保护数据隐私的多方联合处理数据的方法及装置。在该方法中,第一方将经过同态加密的多个原始特征密文发送至第二方之后,还将原始隐私数据按照约束方程解的形式,构建成多个第一隐私矩阵,分别计算其中多个第一隐私向量的承诺值和第一掩盖向量的承诺值。在接收到第二方的第一挑战数时,基于构建的第二多项式和分离变换后的第二多项式,计算多个第二隐私向量的承诺值和第二掩盖向量的承诺值。在接收到第二方的第二挑战数时,基于构建的第一多项式和分离变换后的第二多项式分别计算多个结果。第一方将确定的多个承诺值和多个结果均发送至第二方,使得第二方对原始特征密文进行验证,验证通过后对原始特征密文进行数据处理。



CN 111885079 B

1.一种保护数据隐私的多方联合处理数据的方法，多方包括第一方和第二方，所述第一方存储有原始隐私数据，其中包括多个业务对象的原始特征向量m_i，每个原始特征向量m_i具有第一约定数据格式，所述方法通过所述第一方执行，包括：

获取多个原始特征密文c_i，并将其发送至所述第二方；其中，多个原始特征密文c_i通过约定同态加密过程对对应的原始特征向量m_i加密得到；

将所述原始隐私数据，按照预先构建的多个约束方程解的形式构建成多个第一隐私矩阵，其中包括多个第一隐私向量$a_\tau b_\tau c_\tau$；所述多个约束方程基于所述约定同态加密过程和第一约定数据格式构建；

利用预设承诺算法和多个第一掩盖随机数，分别计算对应的第一隐私向量$a_\tau b_\tau c_\tau$的第一承诺值$A_\tau B_\tau C_\tau$，以及第一掩盖向量d的第二承诺值D；

将所述第二承诺值D和多个第一承诺值$A_\tau B_\tau C_\tau$发送至所述第二方；

接收所述第二方发送的第一挑战数y；

将所述第一挑战数y作为第二子变元Y的取值，确定基于所述多个约束方程、多个第一隐私向量$a_\tau b_\tau c_\tau$、所述第一掩盖向量d、第一子变元X和所述第二子变元Y，构建的第一多项式Lr和第二多项式tX，并将所述第二多项式tX分离变换成第一变元向量Z、第二隐私矩阵T和第二变元向量F的乘积；所述第二隐私矩阵T包括第二掩盖向量u和多个第二隐私向量t′；

利用所述预设承诺算法和多个第二掩盖随机数，分别计算对应的第二隐私向量t′的第三承诺值$T'_\eta T''_\psi$，以及所述第二掩盖向量u的第四承诺值U；

将所述第四承诺值U和多个第三承诺值$T'_\eta T''_\psi$发送至所述第二方；

接收所述第二方发送的第二挑战数x；

将所述第二挑战数x作为所述第一子变元X的取值，基于分离变换后的第二多项式，确定与所述第二隐私矩阵T对应的第一结果$\bar{t}$，以及与多个第二掩盖随机数对应的第二结果$\bar{\gamma}$；以及，基于所述第一多项式Lr，确定与所述第一隐私矩阵对应的第三结果lr，和与多个第一掩盖随机数对应的第四结果ρ；

将所述第一结果$\bar{t}$、第二结果$\bar{\gamma}$、第三结果lr和第四结果ρ发送至所述第二方，以使所述第二方在基于接收的结果和承诺值进行验证并通过之后，对所述多个原始特征密文c_i进行数据处理。

2.根据权利要求1所述的方法，其中，所述第一多项式Lr为所述第二多项式tX的因式；所述第一多项式Lr的各项基于不同幂次的变元分别与多个第一隐私向量$a_\tau b_\tau c_\tau$或所述第一掩盖向量d的乘积得到，所述变元包括所述第一子变元X和/或第二子变元Y；

所述第一变元向量Z和第二变元向量F包含不同幂次的第一子变元X。

3.根据权利要求2所述的方法，所述基于分离变换后的第二多项式，确定与所述第二隐私矩阵T对应的第一结果$\bar{t}$，以及与多个第二掩盖随机数对应的第二结果$\bar{\gamma}$的步骤，包括：

计算所述第一变元向量Z与所述第二隐私矩阵T的乘积，得到第一结果$\bar{t}$；

计算所述第一变元向量Z与由多个第二掩盖随机数构成的第三掩盖向量γ的乘积，得到第二结果$\bar{\gamma}$。

4.根据权利要求2所述的方法，所述基于所述第一多项式Lr，确定与所述第一隐私矩阵对应的第三结果lr，和与多个第一掩盖随机数对应的第四结果ρ的步骤，包括：

将所述第二挑战数x、多个第一隐私向量$a_\tau b_\tau c_\tau$、所述第一掩盖向量d均代入所述第一多

项式Lr中，得到第一结果lr；所述第二挑战数x作为所述第一子变元X的取值；

将多个第一掩盖随机数分别替换所述第一多项式Lr中对应的第一隐私向量和第一掩盖向量，得到第二结果ρ。

5.根据权利要求1所述的方法，其中，每个原始特征向量m_i具有以下第一约定数据格式：其包括第一数量sn个属性块，每个属性块包括位于第一位置的第二数量个预设0值和位于第二位置的该属性块的特征值b_{sn}^i，特征值b_{sn}^i的取值或0或1。

6.根据权利要求1或5所述的方法，其中，多个原始特征密文c_i通过以下约定同态加密过程加密得到：使用第一公钥N和多个第一加密随机数r_i，采用第一同态加密算法，分别对多个原始特征向量m_i进行同态加密后得到。

7.根据权利要求6所述的方法，其中，所述多个约束方程具体基于以下内容构建：多个原始特征密文c_i的同态加密过程、多个辅助特征密文c_s^*的同态加密过程、所述第一约定数据格式和多个辅助特征向量m_s^*的第二约定数据格式；所述第一约定数据格式包括特征值b_{sn}^i的取值范围；

所述多个辅助特征密文c_s^*，通过以下同态加密过程加密得到：使用所述第一公钥N和多个第二加密随机数r_s^*，采用所述第一同态加密算法，分别对多个辅助特征向量m_s^*进行同态加密后得到；

所述多个辅助特征向量m_s^*，通过以第三数量个业务对象为单位，对按照约定排列顺序排练的多个业务对象进行分组，并将任意分组中多个原始特征向量的特征值b_{sn}^i进行拼接得到。

8.根据权利要求7所述的方法，所述多个约束方程包括：

通过将同态加密过程中的原始隐私数据采用变量标识，将同态加密过程转换得到的多个乘法约束方程和多个加法约束方程；

通过将特征值b_{sn}^i、原始特征向量m_i采用变量标识，将每个原始特征向量m_i表示为第一数量sn个特征值b_{sn}^i分别与相应系数相乘后的和值，得到的加法约束方程，所述系数基于第一数量sn和第二数量确定；

通过将特征值b_{sn}^i采用变量标识，将特征值b_{sn}^i的取值范围采用乘法约束方程或加法约束方程表示时得到的约束方程。

9.根据权利要求8所述的方法，其中，所述原始隐私数据还包括：多个第一加密随机数r_i、多个辅助特征向量m_s^*、多个第二加密随机数r_s^*和多个特征值b_{sn}^i。

10.根据权利要求8所述的方法，当特征值b_{sn}^i的取值或0或1时，针对特征值b_{sn}^i取值范围的约束方程包括，特征值b_{sn}^i减去1的差值与该特征值b_{sn}^i的乘积等于0；

所述方法还包括：

在小于第一巨数值的整数范围内，随机生成第四数量个挑选随机数R'_j；

获取所述第二方随机生成的第四数量个第一随机数$l_{i,sn}^j$的集合，每个集合中的第一随机数$l_{i,sn}^j$的数量与多个原始特征向量m_i中的特征值b_{sn}^i总数相等，第一随机数$l_{i,sn}^j$的取值或0

或1；

针对每个集合，将该集合中的各个第一随机数$l_{i,sn}^{j}$分别与对应位置的特征值b_{sn}^{i}相乘，再与对应位置的挑选随机数R′$_j$相加，得到对应的第一验证数L′$_j$；

将得到的多个第一验证数L′$_j$发送至所述第二方；

当接收到所述第二方发送的表示初步验证通过的第一通知时，执行将所述原始隐私数据，按照预先构建的多个约束方程解的形式构建成多个第一隐私矩阵；其中，所述第一通知在确定多个第一验证数L′$_j$小于所述第一巨数值时发送。

11.根据权利要求10所述的方法，多个约束方程还包括：

通过将特征值b_{sn}^{i}、多个挑选随机数R′$_j$采用变量标识，基于所述第一验证数L′$_j$的计算过程构建得到的加法约束方程。

12.根据权利要求1所述的方法，其中，所述预设承诺算法包括佩德森承诺算法。

13.根据权利要求1所述的方法，所述第一多项式Lr和第二多项式tX基于劳伦特多项式构建。

14.根据权利要求6所述的方法，所述第一同态加密算法包括Paillier加密算法。

15.根据权利要求1所述的方法，所述第一方和所述第二方之间共享所述多个约束方程，以及第一多项式的变量表达形式、第二多项式的变量表达形式和分离变换后的第二多项式的变量表达形式，在变量表达形式中原始隐私数据采用变量标识。

16.根据权利要求1所述的方法，所述业务对象包括：用户、商品、商户或事件。

17.一种保护数据隐私的多方联合处理数据的方法，多方包括第一方和第二方，所述第一方存储有原始隐私数据，其中包括多个业务对象的原始特征向量m$_i$，每个原始特征向量m$_i$具有第一约定数据格式，所述方法通过所述第二方执行，包括：

接收所述第一方发送的多个原始特征密文c$_i$，其通过约定同态加密过程对对应的原始特征向量m$_i$加密得到；

接收所述第一方发送的第二承诺值D和多个第一承诺值$A_\tau B_\tau C_\tau$；

生成第一挑战数y，并将其发送至所述第一方；

接收所述第一方发送的第四承诺值U和多个第三承诺值T′$_\eta$T″$_\psi$；

生成第二挑战数x，并将其发送至所述第一方；

接收所述第一方发送的第一结果$\bar{t}$、第二结果$\bar{\gamma}$、第三结果lr和第四结果ρ；

利用预设承诺算法和所述第二结果$\bar{\gamma}$计算所述第一结果$\bar{t}$的第五承诺值；基于所述第二挑战数x、所述第四承诺值U和多个第三承诺值T′$_\eta$T″$_\psi$，以及分离变换后的第二多项式tX的变量表达形式，计算所述第一结果$\bar{t}$的第六承诺值；执行所述第五承诺值与第六承诺值是否相等的第一判断；

基于所述第二挑战数x、所述第一结果$\bar{t}$以及分离变换后的第二多项式tX的变量表达形式，计算第二多项式tX的第一取值；至少基于所述第三结果lr以及第二多项式tX的变量表达形式，计算第二多项式tX的第二取值；执行所述第一取值与所述第二取值是否相等的第二判断；

利用所述预设承诺算法和所述第四结果ρ计算所述第三结果lr的第七承诺值；基于所述第一挑战数y、第二挑战数x、第二承诺值D和多个第一承诺值$A_\tau B_\tau C_\tau$，以及第一多项式Lr的

变量表达形式，计算所述第三结果lr的第八承诺值；执行所述第七承诺值与第八承诺值是否相等的第三判断；

当各个判断的结果均为是时，确定对所述约定同态加密过程和所述第一约定数据格式的零知识证明验证通过；

基于所述第一约定数据格式，对多个原始特征密文c_i进行数据处理，得到数据处理结果。

18.根据权利要求17所述的方法，其中，在变量表达形式中，所述第一多项式Lr为所述第二多项式tX的因式，所述第一多项式Lr的各项基于不同幂次的变元分别与多个第一隐私向量$a_\tau b_\tau c_\tau$或第一掩盖向量d的乘积得到，所述变元包括第一子变元X和/或第二子变元Y；

在变量表达形式中，分离变换后的第二多项式tX等于第一变元向量Z、第二隐私矩阵T和第二变元向量F的乘积，所述第一变元向量Z和第二变元向量F包含不同幂次的第一子变元X。

19.根据权利要求18所述的方法，所述计算所述第一结果$\bar{t}$的第六承诺值的步骤，包括：

将所述第二挑战数x作为所述第一子变元X的取值，计算所述第一变元向量Z中的每一元素，并将每一元素作为对应的第三承诺值$T'_\eta T''_\psi$和第四承诺值U的指数，计算各幂之间的连乘，得到所述第一结果$\bar{t}$的第六承诺值。

20.根据权利要求18所述的方法，所述计算第二多项式tX的第一取值的步骤，包括：

将所述第二挑战数x作为所述第一变元X的取值，基于所述第一结果$\bar{t}$与所述第二变元向量F的乘积，确定第二多项式tX的第一取值。

21.根据权利要求18所述的方法，所述计算所述第三结果lr的第八承诺值的步骤，包括：

基于所述第一挑战数y、第二挑战数x计算第一多项式Lr的变量表达式中不同幂次的变元的第三取值，将多个第三取值分别作为对应的第二承诺值D和第一承诺值$A_\tau B_\tau C_\tau$的指数，计算各幂之间的连乘，得到所述第三结果lr的第八承诺值。

22.根据权利要求17所述的方法，所述第二判断在所述第一判断的结果为是时执行，所述第三判断在所述第一判断和第二判断的结果均为是时执行。

23.根据权利要求17所述的方法，其中，每个原始特征向量m_i具有以下第一约定数据格式：其包括第一数量sn个属性块，每个属性块包括位于第一位置的第二数量个预设0值和位于第二位置的该属性块的特征值b_{sn}^i，特征值b_{sn}^i的取值或0或1；所述方法还包括：

接收所述第一方发送的多个第一验证数L'_j；

在确定多个第一验证数L'_j小于第一巨数值时，向所述第一方发送表示初步验证通过的第一通知。

24.根据权利要求23所述的方法，多个业务对象的原始特征密文c_i之间纵向排列；所述对多个原始特征密文c_i进行数据处理的步骤，包括：

基于所述第一约定数据格式，对多个原始特征密文c_i中的属性块进行纵向统计求和。

25.一种保护数据隐私的多方联合处理数据的装置，多方包括第一方和第二方，所述第一方存储有原始隐私数据，其中包括多个业务对象的原始特征向量m_i，每个原始特征向量m_i具有第一约定数据格式，所述装置部署在所述第一方中，包括：

第一获取模块，配置为，获取多个原始特征密文c_i，并将其发送至所述第二方；其中，多

个原始特征密文c_i通过约定同态加密过程对对应的原始特征向量m_i加密得到；

第一构建模块，配置为，将所述原始隐私数据，按照预先构建的多个约束方程解的形式构建成多个第一隐私矩阵，其中包括多个第一隐私向量$a_\tau b_\tau c_\tau$；所述多个约束方程基于所述约定同态加密过程和第一约定数据格式构建；

第一承诺模块，配置为，利用预设承诺算法和多个第一掩盖随机数，分别计算对应的第一隐私向量$a_\tau b_\tau c_\tau$的第一承诺值$A_\tau B_\tau C_\tau$，以及第一掩盖向量d的第二承诺值D；

第一发送模块，配置为，将所述第二承诺值D和多个第一承诺值$A_\tau B_\tau C_\tau$发送至所述第二方；

第一接收模块，配置为，接收所述第二方发送的第一挑战数y；

第二构建模块，配置为，将所述第一挑战数y作为第二子变元Y的取值，确定基于所述多个约束方程、多个第一隐私向量$a_\tau b_\tau c_\tau$、所述第一掩盖向量d、第一子变元X和所述第二子变元Y，构建的第一多项式Lr和第二多项式tX，并将所述第二多项式tX分离变换成第一变元向量Z、第二隐私矩阵T和第二变元向量F的乘积；所述第二隐私矩阵T包括第二掩盖向量u和多个第二隐私向量t′；

第二承诺模块，配置为，利用所述预设承诺算法和多个第二掩盖随机数，分别计算对应的第二隐私向量t′的第三承诺值$T'_\eta T''_\psi$，以及所述第二掩盖向量u的第四承诺值U；

第二发送模块，配置为，将所述第四承诺值U和多个第三承诺值$T'_\eta T''_\psi$发送至所述第二方；

第二接收模块，配置为，接收所述第二方发送的第二挑战数x；

第一确定模块，配置为，将所述第二挑战数x作为所述第一子变元X的取值，基于分离变换后的第二多项式，确定与所述第二隐私矩阵T对应的第一结果$\bar{t}$，以及与多个第二掩盖随机数对应的第二结果$\bar{\gamma}$；以及，基于所述第一多项式Lr，确定与所述第一隐私矩阵对应的第三结果lr，和与多个第一掩盖随机数对应的第四结果ρ；

第三发送模块，配置为，将所述第一结果$\bar{t}$、第二结果$\bar{\gamma}$、第三结果lr和第四结果ρ发送至所述第二方，以使所述第二方在基于接收的结果和承诺值进行验证并通过之后，对所述多个原始特征密文c_i进行数据处理。

26.一种保护数据隐私的多方联合处理数据的装置，多方包括第一方和第二方，所述第一方存储有原始隐私数据，其中包括多个业务对象的原始特征向量m_i，每个原始特征向量m_i具有第一约定数据格式，所述装置部署在所述第二方中，包括：

第三接收模块，配置为，接收所述第一方发送的多个原始特征密文c_i，其通过约定同态加密过程对对应的原始特征向量m_i加密得到；

第四接收模块，配置为，接收所述第一方发送的第二承诺值D和多个第一承诺值$A_\tau B_\tau C_\tau$；

第四发送模块，配置为，生成第一挑战数y，并将其发送至所述第一方；

第五接收模块，配置为，接收所述第一方发送的第四承诺值U和多个第三承诺值$T'_\eta T''_\psi$；

第五发送模块，配置为，生成第二挑战数x，并将其发送至所述第一方；

第六接收模块，配置为，接收所述第一方发送的第一结果$\bar{t}$、第二结果$\bar{\gamma}$、第三结果lr和第四结果ρ；

第一判断模块，配置为，利用预设承诺算法和所述第二结果$\bar{\gamma}$计算所述第一结果$\bar{t}$的第五承诺值；基于所述第二挑战数x、所述第四承诺值U和多个第三承诺值$T'_\eta T''_\psi$，以及分离变

换后的第二多项式tX的变量表达形式，计算所述第一结果$\bar{t}$的第六承诺值；执行所述第五承诺值与第六承诺值是否相等的第一判断；

第二判断模块，配置为，基于所述第二挑战数x、所述第一结果$\bar{t}$以及分离变换后的第二多项式tX的变量表达形式，计算第二多项式tX的第一取值；至少基于所述第三结果lr以及第二多项式tX的变量表达形式，计算第二多项式tX的第二取值；执行所述第一取值与所述第二取值是否相等的第二判断；

第三判断模块，配置为，利用所述预设承诺算法和所述第四结果ρ计算所述第三结果lr的第七承诺值；基于所述第一挑战数y、第二挑战数x、第二承诺值D和多个第一承诺值$A_\tau B_\tau C_\tau$，以及第一多项式Lr的变量表达形式，计算所述第三结果lr的第八承诺值；执行所述第七承诺值与第八承诺值是否相等的第三判断；

第二确定模块，配置为，当各个判断的结果均为是时，确定所述约定同态加密过程和所述第一约定数据格式的零知识证明验证通过；

第一处理模块，配置为，基于所述第一约定数据格式，对多个原始特征密文c_i进行数据处理，得到数据处理结果。

27.一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行权利要求1-24中任一项所述的方法。

28.一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求1-24中任一项所述的方法。

保护数据隐私的多方联合处理数据的方法及装置

技术领域

[0001] 本说明书一个或多个实施例涉及数据处理和数据安全领域，尤其涉及一种保护数据隐私的多方联合处理数据的方法及装置。

背景技术

[0002] 随着计算机技术的发展，数据交互处理的需求越来越大，如何在数据交互处理的过程中保证数据的安全和隐私性，成为重要问题。例如，在一种场景中，第一方和第二方均存储有大量用户数据，需要将两方的数据进行融合统计，并将统计结果在两方之间共享。但是，第一方或者第二方的用户数据均属于隐私数据，不能明文发送至对方。在这种情况下，如何实现对两方中隐私数据的联合处理，并且保证隐私数据的安全性，是数据处理和数据安全领域需要考虑的问题。

[0003] 因此，希望能有改进的方案，在多方联合处理数据的过程中，保护各方隐私数据的安全。

发明内容

[0004] 本说明书一个或多个实施例描述了保护数据隐私的多方联合处理数据的方法及装置，以在多方联合处理数据的过程中，保护各方隐私数据的安全。具体的技术方案如下。

[0005] 第一方面，实施例提供了一种保护数据隐私的多方联合处理数据的方法，多方包括第一方和第二方，所述第一方存储有原始隐私数据，其中包括多个业务对象的原始特征向量m_i，每个原始特征向量m_i具有第一约定数据格式，所述方法通过所述第一方执行，包括：

[0006] 获取多个原始特征密文c_i，并将其发送至所述第二方；其中，多个原始特征密文c_i通过约定同态加密过程对对应的原始特征向量 m_i加密得到；

[0007] 将所述原始隐私数据，按照预先构建的多个约束方程解的形式构建成多个第一隐私矩阵，其中包括多个第一隐私向量 $a_\tau b_\tau c_\tau$；所述多个约束方程基于所述约定同态加密过程和第一约定数据格式构建；

[0008] 利用预设承诺算法和多个第一掩盖随机数，分别计算对应的第一隐私向量$a_\tau b_\tau c_\tau$的第一承诺值$A_\tau B_\tau C_\tau$，以及第一掩盖向量d的第二承诺值D；

[0009] 将所述第二承诺值D和多个第一承诺值 $A_\tau B_\tau C_\tau$发送至所述第二方；

[0010] 接收所述第二方发送的第一挑战数y；

[0011] 将所述第一挑战数y作为第二子变元Y的取值，确定基于所述多个约束方程、多个第一隐私向量$a_\tau b_\tau c_\tau$、所述第一掩盖向量d、第一子变元X和所述第二子变元Y，构建的第一多项式Lr和第二多项式tX，并将所述第二多项式tX分离变换成第一变元向量Z、第二隐私矩阵T和第二变元向量F的乘积；所述第二隐私矩阵T包括第二掩盖向量u和多个第二隐私向量 t'；

[0012] 利用所述预设承诺算法和多个第二掩盖随机数，分别计算对应的第二隐私向量t'

的第三承诺值$T'_{\eta}T''_{\psi}$，以及所述第二掩盖向量u的第四承诺值U；

[0013] 将所述第四承诺值U和多个第三承诺值$T'_{\eta}T''_{\psi}$发送至所述第二方；

[0014] 接收所述第二方发送的第二挑战数x；

[0015] 将所述第二挑战数x作为所述第一子变元X的取值，基于分离变换后的第二多项式，确定与所述第二隐私矩阵T对应的第一结果$\bar{t}$，以及与多个第二掩盖随机数对应的第二结果$\bar{\gamma}$；以及，基于所述第一多项式Lr，确定与所述第一隐私矩阵对应的第三结果lr，和与多个第一掩盖随机数对应的第四结果ρ；

[0016] 将所述第一结果 $\bar{t}$、第二结果 $\bar{\gamma}$、第三结果lr和第四结果 ρ发送至所述第二方，以使所述第二方在基于接收的结果和承诺值进行验证并通过之后，对所述多个原始特征密文C_i进行数据处理。

[0017] 第二方面，实施例提供了一种保护数据隐私的多方联合处理数据的方法，多方包括第一方和第二方，所述第一方存储有原始隐私数据，其中包括多个业务对象的原始特征向量 m_i，每个原始特征向量m_i具有第一约定数据格式，所述方法通过所述第二方执行，包括：

[0018] 接收所述第一方发送的多个原始特征密文C_i，其通过约定同态加密过程对对应的原始特征向量m_i加密得到；

[0019] 接收所述第一方发送的第二承诺值D和多个第一承诺值$A_{\tau}B_{\tau}C_{\tau}$；

[0020] 生成第一挑战数y，并将其发送至所述第一方；

[0021] 接收所述第一方发送的第四承诺值U和多个第三承诺值 $T'_{\eta}T''_{\psi}$；

[0022] 生成第二挑战数x，并将其发送至所述第一方；

[0023] 接收所述第一方发送的第一结果$\bar{t}$、第二结果 $\bar{\gamma}$、第三结果lr和第四结果ρ；

[0024] 利用预设承诺算法和所述第二结果 $\bar{\gamma}$计算所述第一结果 $\bar{t}$的第五承诺值；基于所述第二挑战数x、所述第四承诺值U和多个第三承诺值$T'_{\eta}T''_{\psi}$，以及分离变换后的第二多项式tX的变量表达形式，计算所述第一结果 $\bar{t}$的第六承诺值；执行所述第五承诺值与第六承诺值是否相等的第一判断；

[0025] 基于所述第二挑战数x、所述第一结果$\bar{t}$以及分离变换后的第二多项式tX的变量表达形式，计算第二多项式tX的第一取值；至少基于所述第三结果lr以及第二多项式tX的变量表达形式，计算第二多项式tX的第二取值；执行所述第一取值与所述第二取值是否相等的第二判断；

[0026] 利用所述预设承诺算法和所述第四结果 ρ计算所述第三结果lr的第七承诺值；基于所述第一挑战数y、第二挑战数x、第二承诺值D和多个第一承诺值$A_{\tau}B_{\tau}C_{\tau}$，以及第一多项式Lr的变量表达形式，计算所述第三结果lr的第八承诺值；执行所述第七承诺值与第八承诺值是否相等的第三判断；

[0027] 当各个判断的结果均为是时，确定对所述约定同态加密过程和所述第一约定数据格式的零知识证明验证通过；

[0028] 基于所述第一约定数据格式，对多个原始特征密文c_i进行数据处理，得到数据处理结果。

[0029] 第三方面，实施例提供了一种保护数据隐私的多方联合处理数据的装置，多方包括第一方和第二方，所述第一方存储有原始隐私数据，其中包括多个业务对象的原始特征向量 m_i，每个原始特征向量m_i具有第一约定数据格式，所述装置部署在所述第一方中，包括：

[0030] 第一获取模块，配置为，获取多个原始特征密文c_i，并将其发送至所述第二方；其中，多个原始特征密文c_i通过约定同态加密过程对对应的原始特征向量m_i加密得到；

[0031] 第一构建模块，配置为，将所述原始隐私数据，按照预先构建的多个约束方程解的形式构建成多个第一隐私矩阵，其中包括多个第一隐私向量 $a_\tau b_\tau c_\tau$；所述多个约束方程基于所述约定同态加密过程和第一约定数据格式构建；

[0032] 第一承诺模块，配置为，利用预设承诺算法和多个第一掩盖随机数，分别计算对应的第一隐私向量$a_\tau b_\tau c_\tau$的第一承诺值$A_\tau B_\tau C_\tau$，以及第一掩盖向量d的第二承诺值D；

[0033] 第一发送模块，配置为，将所述第二承诺值D和多个第一承诺值$A_\tau B_\tau C_\tau$发送至所述第二方；

[0034] 第一接收模块，配置为，接收所述第二方发送的第一挑战数y；

[0035] 第二构建模块，配置为，将所述第一挑战数y作为第二子变元Y的取值，确定基于所述多个约束方程、多个第一隐私向量$a_\tau b_\tau c_\tau$、所述第一掩盖向量d、第一子变元X和所述第二子变元Y，构建的第一多项式Lr和第二多项式tX，并将所述第二多项式tX分离变换成第一变元向量Z、第二隐私矩阵T和第二变元向量F的乘积；所述第二隐私矩阵T包括第二掩盖向量u和多个第二隐私向量 t'；

[0036] 第二承诺模块，配置为，利用所述预设承诺算法和多个第二掩盖随机数，分别计算对应的第二隐私向量t'的第三承诺值$T'_\eta T''_\psi$，以及所述第二掩盖向量u的第四承诺值U；

[0037] 第二发送模块，配置为，将所述第四承诺值U和多个第三承诺值$T'_\eta T''_\psi$发送至所述第二方；

[0038] 第二接收模块，配置为，接收所述第二方发送的第二挑战数x；

[0039] 第一确定模块，配置为，将所述第二挑战数x作为所述第一子变元X的取值，基于分离变换后的第二多项式，确定与所述第二隐私矩阵T对应的第一结果 $\bar{t}$，以及与多个第二掩盖随机数对应的第二结果 $\bar{\gamma}$；以及，基于所述第一多项式Lr，确定与所述第一隐私矩阵对应的第三结果lr，和与多个第一掩盖随机数对应的第四结果ρ；

[0040] 第三发送模块，配置为，将所述第一结果$\bar{t}$、第二结果$\bar{\gamma}$、第三结果lr和第四结果ρ发送至所述第二方，以使所述第二方在基于接收的结果和承诺值进行验证并通过之后，对所述多个原始特征密文c_i进行数据处理。

[0041] 第四方面，实施例提供了一种保护数据隐私的多方联合处理数据的装置，多方包括第一方和第二方，所述第一方存储有原始隐私数据，其中包括多个业务对象的原始特征向量 m_i，每个原始特征向量m_i具有第一约定数据格式，所述装置部署在所述第二方中，包括：

[0042] 第三接收模块，配置为，接收所述第一方发送的多个原始特征密文 C_i，其通过约定同态加密过程对对应的原始特征向量m_i加密得到；

[0043] 第四接收模块，配置为，接收所述第一方发送的第二承诺值D和多个第一承诺值$A_\tau B_\tau C_\tau$；

[0044] 第四发送模块，配置为，生成第一挑战数y，并将其发送至所述第一方；

[0045] 第五接收模块，配置为，接收所述第一方发送的第四承诺值U和多个第三承诺值$T'_\eta T''_\psi$；

[0046] 第五发送模块，配置为，生成第二挑战数x，并将其发送至所述第一方；

[0047] 第六接收模块，配置为，接收所述第一方发送的第一结果$\bar{t}$、第二结果$\bar{\gamma}$、第三结果lr和第四结果 ρ；

[0048] 第一判断模块，配置为，利用预设承诺算法和所述第二结果 $\bar{\gamma}$计算所述第一结果$\bar{t}$的第五承诺值；基于所述第二挑战数x、所述第四承诺值U和多个第三承诺值$T'_\eta T''_\psi$，以及分离变换后的第二多项式tX的变量表达形式，计算所述第一结果$\bar{t}$的第六承诺值；执行所述第五承诺值与第六承诺值是否相等的第一判断；

[0049] 第二判断模块，配置为，基于所述第二挑战数x、所述第一结果$\bar{t}$以及分离变换后的第二多项式tX的变量表达形式，计算第二多项式tX的第一取值；至少基于所述第三结果lr以及第二多项式tX的变量表达形式，计算第二多项式tX的第二取值；执行所述第一取值与所述第二取值是否相等的第二判断；

[0050] 第三判断模块，配置为，利用所述预设承诺算法和所述第四结果 ρ计算所述第三结果lr的第七承诺值；基于所述第一挑战数y、第二挑战数x、第二承诺值D和多个第一承诺值 $A_\tau B_\tau C_\tau$，以及第一多项式Lr的变量表达形式，计算所述第三结果lr的第八承诺值；执行所述第七承诺值与第八承诺值是否相等的第三判断；

[0051] 第二确定模块，配置为，当各个判断的结果均为是时，确定所述约定同态加密过程和所述第一约定数据格式的零知识证明验证通过；

[0052] 第一处理模块，配置为，基于所述第一约定数据格式，对多个原始特征密文 C_i进行数据处理，得到数据处理结果。

[0053] 第五方面，实施例提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行第一方面至第二方面中任一项所述的方法。

[0054] 第六方面，实施例提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现第一方面至第二方面中任一项所述的方法。

[0055] 根据本说明书实施例提供的方法及装置，在多方联合处理数据的过程中，第一方将经过同态加密的原始特征密文发送至第二方，预先基于约定同态加密过程和第一约定数据格式构建约束方程，在此基础上，通过与第二方的多次交互，向第二方针对约定同态加密过程和第一约定数据格式进行零知识证明，以证明第一方所发送的原始特征密文是按照约定同态加密过程进行的加密，且其对应的明文符合第一约定数据格式，第二方在对第一方验证通过之后，对原始特征密文进行数据处理。上述零知识证明的过程可以一次性对多个密文及其明文的合法性进行验证，而不会泄露任何相关明文信息，从而能够确保在多方联

合处理数据过程中各方隐私数据的安全。

附图说明

[0056] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单的介绍。显而易见地，下面描述中的附图仅仅是本发明的一些实施例，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的附图。

[0057] 图1为本说明书披露的一个实施例的实施场景示意图；

[0058] 图2为实施例提供的保护数据隐私的多方联合处理数据的一种方法流程示意图；

[0059] 图3为实施例提供的一种保护数据隐私的多方联合处理数据的装置的示意性框图；

[0060] 图4为实施例提供的一种保护数据隐私的多方联合处理数据的装置的示意性框图。

具体实施方式

[0061] 下面结合附图，对本说明书提供的方案进行描述。

[0062] 图1为本说明书披露的一个实施例的实施场景示意图。在该实施场景中，示意性地示出了2个参与方，其中第一方是隐私数据拥有方，第二方是需要结合第一方中的隐私数据进行数据处理的数据处理方。

[0063] 第一方存储的隐私数据，可以是图像、文本、音频等数据，也可以是业务对象的特征数据，例如，业务对象可以包括用户、商品、商户或事件等，其特征数据可以是用户数据、商品数据、商户数据或事件数据等。

[0064] 第二方对隐私数据的数据处理，可以是利用第一方的隐私数据进行模型训练，也可以是进行数据融合、数据统计等处理。当进行模型训练时，所训练的业务预测模型可以是分类模型或者是回归模型。

[0065] 在一种应用场景中，第一方存储有多个业务对象的第一特征数据，第一特征数据包括多个第一属性。第二方也存储有这多个业务对象的第二特征数据，该第二特征数据包括多个第二属性，即第二方存储有相同业务对象的不同属性的特征数据。特征数据可以采用特征向量的形式表示。第一方和第二方可以联合对这多个业务对象的特征数据进行处理。例如，第一方存储有100万个用户的健康数据，其中的健康项目包括，是否患有高血压、是否患有心脏病、是否患有糖尿病等，第二方存储有同样的这100万个用户的属性数据，其中包括用户年龄、用户性别、用户所处地区等等。第一方和第二方可以联合对这100万个用户的健康数据和属性数据进行数据统计，例如可以统计这100万个用户中女性患有高血压的比例，或者男性患有高血压的比例，或者统计某个地区患有某种疾病的用户比例等等。

[0066] 在第一方和第二方联合进行数据处理的情况下，出于保护隐私数据的目的，第一方不能直接将隐私数据发送至第二方，以免泄露隐私数据。在这种情况下，第一方可以将存储的隐私数据经过同态加密之后发送至第二方，第二方接收第一方发送的同态加密后的密文，并基于该密文进行数据处理。

[0067] 例如，当第一方存储的隐私数据为多个业务对象的原始特征向量时，第一方可以

采用Paillier加密算法，并基于该加密算法的第一公钥N，对每一个业务对象的原始特征向量m_i进行如下的同态加密，得到原始特征密文c_i：

[0068] $$c_i = \mathrm{Enc}(N, m_i; r_i) = (1+N)^{m_i} \cdot r_i^N \bmod N^2$$

[0069] 其中，mod为取模符号，r_i为同态加密时使用的随机数。通过上述同态加密，多个业务对象的原始特征向量加密之后，得到的密文互不相同。

[0070] 这样，当第二方接收到多个原始特征密文c_i时，可以利用同态加密算法具有的特殊性质对原始特征密文c_i进行数据处理，其处理结果与对明文处理后再加密，是等价的。因为同态加密算法具有这样的一种特殊性质，对明文进行运算后再加密，与加密后对密文进行相应的运算，结果是等价的。例如，用同样的第一公钥N加密v_1和v_2得到$\mathrm{E}_N(\mathrm{v}_1)$和$\mathrm{E}_N(\mathrm{v}_2)$，如果满足$\mathrm{E}_N(\mathrm{v}_1+\mathrm{v}_2)=\mathrm{E}_N(\mathrm{v}_1)\cdot\mathrm{E}_N(\mathrm{v}_2)$，那么则认为，该加密算法满足加法同态，相应的，$\mathrm{E}_{\mathrm{PK}}(\mathrm{v}_1)\cdot\mathrm{E}_{\mathrm{PK}}(\mathrm{v}_2)$为对应的同态加和操作。

[0071] 然而，上述过程是理想化过程。在一种场景中，恶意者可能不按照约定同态加密过程进行同态加密，而是将精心构造的恶意字符串作为原始特征密文发送至第二方。如果第二方仍然采用相应的数据处理方式对恶意字符串进行操作，并将结果返回给恶意者，那么恶意者可能借助于精心构造的恶意字符串的特点，根据第二方返回的结果反推出第二方中的隐私数据。

[0072] 考虑到以上风险，参见图1，在本说明书实施例中，预先基于要证明的约定同态加密过程和约定数据格式构建多个约束方程，其中的隐私数据采用变量标识，并在第一方和第二方之间共享构建的约束方程。第一方在向第二方发送多个原始特征密文c_i之后，与第二方之间进行基于隐私数据和约束方程的数据交互，以进行零知识证明。也就是，第一方向第二方提供针对约定同态加密过程和约定数据格式的零知识证明，证明所发送的原始特征密文c_i是通过约定同态加密过程进行加密的，并且其对应的明文符合约定数据格式，而不是恶意构造的字符串。其所交互的数据是对隐私数据进行变换后的数据。第二方在对第一方的零知识证明验证通过之后，再基于多个原始特征密文c_i进行数据处理，从而避免隐私数据泄露的风险。下面详细说明上述实施例的具体实施过程。

[0073] 图2为实施例提供的保护数据隐私的多方联合处理数据的一种方法流程示意图。其中，多方包括第一方和第二方，第一方存储有原始隐私数据，其中包括多个业务对象的原始特征向量m_i，每个原始特征向量m_i具有第一约定数据格式。例如，多个业务对象的数量为100万个，则i的取值范围可以为[1,100万]中的整数。

[0074] 原始隐私数据还可以包括其他的隐私数据。在本实施例之前提到的隐私数据，可以理解为通用意义上的隐私数据，其没有特指哪些数据。而本实施例中提到的原始隐私数据，具有确定的含义，其包含的数据比较明确，两者并不矛盾。每个业务对象具有一个原始特征向量，每个原始特征向量可以包含多个属性的特征值。第一约定数据格式可以包括属性的排列顺序、特征值的取值范围等格式。第一方可以预先将多个原始特征向量处理成具有第一约定数据格式的形式，第一约定数据格式的作用，可以理解为使得原始特征向量更适用于进行后续的数据处理。

[0075] 本实施例的方法具体包括以下步骤，步骤S210，第一方获取多个原始特征密文，发送多个原始特征密文至第二方；步骤S220，将原始隐私数据按照约束方程解的形式构建成

多个第一隐私矩阵；步骤S230，计算第一隐私向量的第一承诺值，以及第一掩盖向量的第二承诺值，发送第二承诺值和多个第一承诺值至第二方；步骤S240，第二方生成第一挑战数，发送第一挑战数至第一方；步骤S250，第一方确定第一多项式和第二多项式，并将第二多项式分离变换成第一变元向量、第二隐私矩阵和第二变元向量的乘积；步骤S260，第一方计算第二隐私向量的第三承诺值，以及第二掩盖向量的第四承诺值，发送第四承诺值和多个第三承诺值至第二方；步骤S270，第二方生成第二挑战数，发送第二挑战数至第一方；步骤S280，计算第一结果、第二结果、第三结果和第四结果，发送第一结果~第四结果至第二方；步骤S290，第二方基于各个承诺值和结果，执行第一判断、第二判断和第三判断；步骤S200，当各个判断的结果均为是时，对多个原始特征密文进行数据处理。下面详细对每个步骤进行说明。

[0076] 步骤S210，第一方获取多个原始特征密文c_i，并将其发送至第二方，第二方可以接收第一方发送的多个原始特征密文c_i。其中，多个原始特征密文c_i通过约定同态加密过程对对应的原始特征向量m_i加密得到。在获取多个原始特征密文c_i时，第一方可以直接通过约定同态加密过程，对对应的原始特征向量m_i进行加密得到；也可以是，获取预先通过约定同态加密过程加密得到的多个原始特征密文c_i。

[0077] 针对多个原始特征密文c_i的约定同态加密过程可以包括：使用第一公钥*N*和多个第一加密随机数r_i，采用第一同态加密算法，分别对多个原始特征向量m_i进行同态加密后得到。其中，第一公钥*N*可以是预先生成或者直接生成的，多个第一加密随机数r_i可以是在对对应的多个原始特征向量m_i时随机生成。

[0078] 步骤S220，第一方将原始隐私数据，按照预先构建的多个约束方程解的形式构建成多个第一隐私矩阵，例如包括3个第一隐私矩阵，分别采用矩阵*A*、*B*、*C*表示。多个第一隐私矩阵中包括多个第一隐私向量$a_\tau b_\tau c_\tau$，其可以是行向量，也可以是列向量。例如，矩阵*A*、*B*、*C*均为$rn \times cn$维的矩阵，则第一隐私向量的数量为3$rn \times cn$个，*rn*和*cn*分别表示矩阵的行数和列数，均为整数。

[0079] 多个约束方程基于上述约定同态加密过程和第一约定数据格式构建，并且第一方和第二方共享多个约束方程的变量表达形式，在变量表达形式中原始隐私数据采用变量标识。具体的，一方可以预先构建多个约束方程，将其发送至另一方。

[0080] 多个约束方程可以包括非线性约束方程(例如采用乘法约束方程表示)和线性约束方程(例如采用加法约束方程表示)。乘法约束方程的形式可以表示为$a \cdot b = c$，定义a为该乘法约束方程的左因子，b为右因子，*c*为该乘法约束方程的积。根据该乘法约束方程的形式可以将所有的原始隐私数据构建成*A*、*B*、*C*三个矩阵，用*MC*表示所有乘法约束方程的数量，则*A*、*B*、*C*三个矩阵的维数$rn \times cn$可以满足$rn \approx cn \approx \sqrt{MC}$，这样能够尽可能降低通信量。且*A*、*B*、*C*三个矩阵之间满足以下关系：

[0081] $$A \circ B = C$$

[0082] 其中，$\circ$符号表示哈达玛乘积，即三个矩阵满足：它们相同位置处的元素分别是同一个乘法约束方程的左因子、右因子和积。相同位置可以理解为相同行和相同列。

[0083] 加法约束方程也可以采用*A*、*B*、*C*三个矩阵来表示。例如，采用以下第一隐私向量表示*A*、*B*、*C*三个矩阵中的各个行，$\tau \in [1, rn]$：

[0084] $a_\tau=(a_{\tau,1},\dots,a_{\tau,cn}),b_\tau=(b_{\tau,1},\dots,b_{\tau,cn}),c_\tau=(c_{\tau,1},\dots,c_{\tau,cn})$

[0085] 所有加法约束方程可以包括LC条，$LC<2MC$，表示如下：

[0086] $$\sum_{\tau=1}^{rn} a_\tau \cdot w_{\pi,a,\tau} + \sum_{\tau=1}^{rn} b_\tau \cdot w_{\pi,b,\tau} + \sum_{\tau=1}^{rn} c_\tau \cdot w_{\pi,c,\tau} = K_\pi, \pi \in [1,LC]$$

[0087] 其中，$w_{\pi,a,\tau}$、$w_{\pi,b,\tau}$和$w_{\pi,c,\tau}$为常数向量，K_π为标量，下标π表示加法约束方程的编号，$w_{\pi,a,\tau}$表示在第π条加法约束方程中属于第一隐私向量a_τ的常数向量，$w_{\pi,b,\tau}$表示在第π条加法约束方程中属于第一隐私向量b_τ的常数向量，$w_{\pi,c,\tau}$表示在第π条加法约束方程中属于第一隐私向量c_τ的常数向量。上述$w_{\pi,a,\tau}$、$w_{\pi,b,\tau}$、$w_{\pi,c,\tau}$和K_π均是第一方和第二方之间的共享数据，不属于隐私数据。

[0088] 为了更详细地说明如何将乘法约束方程转换为矩阵，以及将加法约束方程转换成等式，这里给出一个例子。假设只考虑一组约束，其中涉及的隐私变量包括x_1,x_2,x_3,x_p,x_q，其满足的约束为：

[0089] $$x_1 \cdot x_2 = x_3, \quad x_p \cdot x_3 = x_q, \quad 2x_1 + 3x_2 - 2x_q = 6$$

[0090] 那么，变量x_1、x_p可以为矩阵A的$a_{1,1}$及$a_{1,2}$项，变量x_2、x_3以及变量x_3、x_q可以分别是矩阵B的$b_{1,1}$、$b_{1,2}$项，以及矩阵C的$c_{1,1}$、$c_{1,2}$项。用矩阵中的项描述上述加法约束方程而得到的常数向量分别为，$w_{1,a,1}=(2,0,\dots,0)$, $w_{1,b,1}=(3,0,\dots,0)$, $w_{1,c,1}=(0,-2,\dots,0)$，对应的标量为$K_1=6$。这里需要注意的是，除了上述显性的加法约束方程外，其还应满足第一个乘法约束方程的积等于第二个乘法约束方程的右因子，因此，另一加法约束方程应为，$c_{1,1}=b_{1,2}$。其对应的常数向量分别为，$w_{2,a,1}=(0,\dots,0)$, $w_{2,b,1}=(0,-1,\dots,0)$, $w_{2,c,1}=(1,0,\dots,0)$，其相应的标量为，$K_2=0$。上述仅仅是一种可行的实施方式，根据上述转换方式，还可以得到其他的ABC矩阵形式，例如将变量x_1、x_p作为矩阵A的$a_{1,1}$及$a_{2,1}$项，x_1、x_p的先后顺序还可以不同。因此，可以存在很多种ABC的矩阵形式。在具体实施时，选择一种形式即可。

[0091] 步骤S230，第一方利用预设承诺算法和多个第一掩盖随机数，分别计算对应的第一隐私向量$a_\tau b_\tau c_\tau$的第一承诺值$A_\tau B_\tau C_\tau$，以及第一掩盖向量d的第二承诺值D，将第二承诺值D和多个第一承诺值$a_\tau b_\tau c_\tau$发送至第二方，第二方接收第一方发送的第二承诺值D和多个第一承诺值$a_\tau b_\tau c_\tau$。第一方在发送第二承诺值D和多个第一承诺值$A_\tau B_\tau C_\tau$时，可以分别发送，也可以打包一起发送，本说明书对该发送方式不做限定。

[0092] 其中，第一掩盖向量d的维度与多个第一隐私向量$a_\tau b_\tau c_\tau$的维度相同，用于对多个第一隐私向量$a_\tau b_\tau c_\tau$进行掩盖，防止隐私泄露。第一承诺值和第二承诺值可以用于后续对关于多个第一隐私矩阵的相关验证。

[0093] 预设承诺算法可以包括佩德森承诺算法(Pedersen commitment)和其他的承诺算法。例如，当第一隐私矩阵包括3个，且分别采用矩阵A、B、C表示时，多个第一掩盖随机数可以采用$\alpha_1,\ \beta_1,\ \gamma_1,\dots,\ \alpha_{rn},\ \beta_{rn},\ \gamma_{rn},\ \delta$表示，每个第一隐私向量对应一个第一掩盖随机数，第一掩盖向量d也对应有一个第一掩盖随机数δ。通过预设承诺算法和多个第一掩盖随机数，可以将多个第一隐私向量和第一掩盖向量承诺并隐藏起来。

[0094] 多个第一掩盖随机数可以是在预设范围内随机生成的。cn维的第一掩盖向量d中的每一维数据可以是在$[0,N^2)$的整数空间中随机选取的。多个第一掩盖随机数也可以是在$[0,N^2)$的整数空间中随机选取得到。N为第一公钥。

[0095] 下面以佩德森承诺算法为例说明承诺值的计算过程。将第一承诺值$A_\tau B_\tau C_\tau$和第二承诺值D分别采用以下公式表示：

[0096] $$A_\tau = Com_{ck}(a_\tau,\alpha_\tau), B_\tau = Com_{ck}(b_\tau,\beta_\tau), C_\tau = Com_{ck}(c_\tau,\gamma_\tau),$$
$$D = Com_{ck}(d,\delta)$$

[0097] 其中，$\tau \in [1,rn]$，$A_\tau = Com_{ck}(a_\tau,\alpha_\tau)$表示利用$\alpha_\tau$计算得到$a_\tau$的承诺值为$A_\tau$，其余三个公式的含义与此类似，不再赘述。以$A_\tau$为例，采用以下步骤说明第一承诺值$A_\tau$的计算方法，其他承诺值的计算方法类似，不再赘述。

[0098] 步骤1a，针对第一隐私向量$a_\tau = (a_{\tau,1},\dots,a_{\tau,cn})$，确定一个阶为$N^2$的群$Q$；

[0099] 步骤2a，在群Q中随机确定cn+1个生成元$g, g_1,\dots,g_{cn}$，则ck可以表示为$ck = (Q,N^2,g,g_1,\dots,g_{cn})$；

[0100] 步骤3a，采用以下公式计算得到第一隐私向量a_τ的第一承诺值：

[0101] $$A_\tau = Com_{ck}(a_\tau,\alpha_\tau) = g^{\alpha_\tau}\prod_{k=1}^{cn} g_k^{a_{\tau,k}}$$

[0102] 其中，$\prod$为连乘符号。

[0103] 本实施例的所有承诺值均可以参照步骤1a-3a进行计算，只需要对其中的参量进行相应替换即可。在后续说明中的承诺值的计算过程也可以参照此处的说明。

[0104] 步骤S240，第二方生成第一挑战数y，并将其发送至第一方，第一方接收第二方发送的第一挑战数y。第二方可以在接收到第一方发送的第二承诺值D和多个第一承诺值$A_\tau B_\tau C_\tau$之后，生成第一挑战数y，并将其发送至第一方。在生成第一挑战数y时，可以在预设的整数范围内随机生成。

[0105] 步骤S250，第一方将第一挑战数y作为第二子变元Y的取值，确定基于多个约束方程、多个第一隐私向量$a_\tau b_\tau c_\tau$、第一掩盖向量d、第一子变元X和第二子变元Y，构建的第一多项式Lr和第二多项式tX，并将第二多项式tX分离变换成第一变元向量Z、第二隐私矩阵T和第二变元向量F的乘积。第一变元向量Z和第二变元向量F均是关于第一子变元X的向量。第二隐私矩阵T包括第二掩盖向量u和多个第二隐私向量t'。

[0106] 其中，第一方或者第二方，可以预先基于多个约束方程构建第一多项式Lr和第二多项式tX的变量表达形式，或者由一方预先构建，然后分享至另一方。

[0107] 第一方可以直接将第一挑战数y、多个第一隐私向量$a_\tau b_\tau c_\tau$、第一掩盖向量d代入变量表达形式的第一多项式Lr和第二多项式tX中，然后再对第二多项式tX进行分离变换，这样能够提高处理的效率。

[0108] 针对于得到分离变量形式的第二多项式tX，在另一种可行的实施方式中，第一方或者第二方可以预先对第二多项式tX的变量表达形式进行分离变换，或者由一方预先进行该分离变换，然后分享至另一方。第二方在得到变量表达形式且分离变换后的第二多项式

tX时，即在得到变量表达形式的第一变元向量Z、第二隐私矩阵T和第二变元向量F的乘积时，可以直接将第一挑战数y、多个第一隐私向量$a_\tau b_\tau c_\tau$、第一掩盖向量d代入。

[0109] 上述提及的多项式可以有多种形式。第一多项式Lr可以为第二多项式tX的因式，第一多项式Lr的各项基于不同幂次的变元分别与多个第一隐私向量$a_\tau b_\tau c_\tau$或第一掩盖向量d的乘积得到，该变元包括第一子变元X和/或第二子变元Y；第一变元向量Z和第二变元向量F包含不同幂次的第一子变元X。例如，第一多项式Lr和第二多项式tX可以基于劳伦特(Laurent)多项式构建。

[0110] 以劳伦特多项式为例，针对所有约束方程，可以构建以下多个多项式：

[0111] $$Lr = \sum_{\tau=1}^{rn} a_\tau Y^\tau X^\tau + \sum_{\tau=1}^{rn} b_\tau X^{-\tau} + X^{rn}\sum_{\tau=1}^{rn} c_\tau X^\tau + dX^{2rn+1} \quad (1)$$

[0112] $$Ls = \sum_{\tau=1}^{rn} w_{a,\tau} Y^{-\tau} X^{-\tau} + \sum_{i=1}^{rn} w_{b,\tau} X^\tau + \sum_{\tau=1}^{rn} w_{c,\tau} X^{-\tau}$$

[0113] $$Lr' = Lr \circ Y' + 2Ls$$

[0114] $$tX = Lr \cdot Lr' - 2K = \sum_{k=-3rn}^{4rn+2} t_k X^k \quad (2)$$

[0115] $$K = \sum_{\pi=1}^{LC} K_\pi Y^{MC+rn+\pi}$$

[0116] 其中，Y'是向量$(Y^{rn}, \ldots, Y^{rn\cdot cn})$，各个符号的含义与步骤S220中的定义相同，此处不再赘述。当将第一挑战数y作为第二子变元Y的取值，将多个第一隐私向量$a_\tau b_\tau c_\tau$、第一掩盖向量d代入上述多个多项式中时，可以得到第一多项式Lr和第二多项式tX的具体表达形式，其为关于第一子变元X的多项式。

[0117] 上述的第一多项式Lr和第二多项式tX的形式仅是一种实施方式，还可以在这种形式的基础上进行一定的变换，例如，可以将Y^τ增加或者转移至b_τ所在的项中，或者增加或者转移至c_τ所在的项中，等等，这些都是可行。所有变换形式的第一多项式Lr和第二多项式tX均属于本说明书的保护范围内。

[0118] 在得到第二多项式tX的具体表达形式时，可以对其进行分离变换，将其分离成第一变元向量Z、第二隐私矩阵T和第二变元向量F的乘积，即$tX=ZTF$的形式。由于第一变元向量Z和第二变元向量F均是关于第一子变元X的向量，这样的分离变换将所有的隐私数据均转移至第二隐私矩阵T中，更便于对隐私数据的变换处理。

[0119] 下面介绍一种对第二多项式tX进行分离变换的实施方式。

[0120] 在$[0,N^2)$整数空间中随机选取n'-1个用于掩藏隐私数据的随机数$\mu_1, \mu_2, \ldots, \mu_{n'-1}$。$n'$可以预先设定。令$m_1'$及$m_2'$为预先设定的两个正数，且满足$3\cdot rn \le n'\cdot m_1'$及$4\cdot rn+2 \le n'\cdot m_2'$。则第二多项式$tX$可变换成另外两个度分别为$(3rn-1)$和$(4rn+1)$的多项式$t^1(X)$和$t^2(X)$的组合，$tX = X^{-m_1'\cdot n'} t^1(X) + X t^2(X)$，这两个多项式$t^1(X)$和$t^2(X)$的系数处于$[0,N^2)$所表示的整数空间内。将$t^1(X)$和$t^2(X)$的系数写在一个$(m_1'+m_2')\times n'$维的第二隐私矩阵$T$中，并且加入已选取的$(n'$-1)个随机数$\mu_1, \mu_2, \ldots, \mu_{n'-1}$，即得到了第二隐私矩阵$T$的构造，其构造如下：

[0121] $$T=\begin{bmatrix} t'_{0,0} & t'_{0,1} & \cdots & t'_{0,n'-1} \\ t'_{1,0} & t'_{1,1} & \cdots & t'_{1,n'-1} \\ \vdots & \vdots & & \vdots \\ t'_{m'_1-1,0} & t'_{m'_1-1,1} & \cdots & t'_{m'_1-1,n'-1} \\ t''_{0,0} & t''_{0,1} & \cdots & t''_{0,n'-1} \\ t''_{1,0} & t''_{1,1} & \cdots & t''_{1,n'-1} \\ \vdots & \vdots & & \vdots \\ t''_{m'_2-1,0} & t''_{m'_2-1,1} & \cdots & t''_{m'_2-1,n'-1} \\ \mu_1 & \mu_2 & \cdots & 0 \end{bmatrix}=\begin{bmatrix} t'_0 \\ t'_1 \\ \vdots \\ t'_{m'_1-1} \\ t''_0 \\ t''_1 \\ \vdots \\ t''_{m'_2-1} \\ u \end{bmatrix} \quad (3)$$

[0122] 其中，第二隐私矩阵T包括多个第二隐私向量t'和第二掩盖向量u，第二隐私向量t'具体包括$t'_0, t'_1, \ldots, t'_{m'_1-1}, t''_0, \ldots, t''_{m'_2-1}$。第一变元向量$Z$和第二变元向量$F$的形式为：

[0123] $$Z=(X^{-m'_1n'}, X^{-(m'_1-1)n'}, \ldots, X^{-n'}, X, X^{n'+1}, \ldots, X^{(m'_2-1)n'+1}, X^2) \quad (4)$$

[0124] $$F=\begin{pmatrix} 1 \\ X \\ \vdots \\ X^{n'-1} \end{pmatrix} \quad (5)$$

[0125] 上述第二隐私矩阵T的具体形式与所选定的n'、m'_1及m'_2有关，也与第二多项式tX的具体形式有关，当n'、m'_1及m'_2改变时，或者第二多项式tX的具体形式改变时，第二隐私矩阵T的具体形式也会发生变化。第一方和第二方共享除隐私数据之外的选定参数以及多项式的表达形式，在此基础上，第一方和第二方均可以基于共享的非隐私数据，实现本实施例中的零知识证明。

[0126] 步骤S260，第一方利用预设承诺算法和多个第二掩盖随机数，分别计算对应的第二隐私向量t'的第三承诺值$T'_\eta T''_\psi$，以及第二掩盖向量u的第四承诺值U，将第四承诺值U和多个第三承诺值$T'_\eta T''_\psi$发送至第二方，第二方可以接收第一方发送的第四承诺值U和多个第三承诺值$T'_\eta T''_\psi$。第二掩盖向量u的维度与第二隐私向量的维度相同，用于对多个第二隐私向量t'进行掩盖，防治隐私泄露。其中，第三承诺值和第四承诺值可以用于后续对关于第二隐私矩阵的相关验证。第一方在发送第四承诺值U和多个第三承诺值$T'_\eta T''_\psi$时，可以分别发送，也可以打包一起发送，本说明书对该发送方式不做限定。

[0127] 多个第二掩盖随机数可以是在预设范围内随机生成的，例如可以是在$[0, N^2)$的整数空间中随机选取得到。每个第二隐私向量对应一个第二掩盖随机数，第二掩盖向量也对应有一个第二掩盖随机数。通过预设承诺算法和多个第二掩盖随机数，可以将多个第二隐私向量和第二掩盖向量承诺并隐藏起来。

[0128] 例如，多个第二掩盖随机数可以表示为$\gamma'_0, \ldots, \gamma'_{m'_1-1}, \gamma''_0, \ldots, \gamma''_{m'_2-1}, \gamma_u$，当第二隐

私向量t'具体包括$t'_0, t'_1, \ldots, t'_{m'_1-1}, t''_0, \ldots, t''_{m'_2-1}$时，每个向量对应的承诺值如下：

[0129] $$T'_\eta = Com_{ck}(t'_\eta; \gamma'_\eta), T''_\psi = Com_{ck}(t''_\psi; \gamma'_\psi{}'), U = Com_{ck}(u; \gamma_u) \quad (6)$$

[0130] 其中，$\eta \in [0, m'_1 - 1], \psi \in [0, m'_2 - 1]$。每个承诺值的计算可以参见步骤S230中的说明，此处不再赘述。

[0131] 步骤S270，第二方生成第二挑战数x，并将其发送至第一方。第一方接收第二方发送的第二挑战数x。第二方可以在接收到第一方发送的第四承诺值U和多个第三承诺值$T'_\eta T''_\psi$之后，生成第二挑战数x，并将其发送至第一方。在生成第二挑战数x时，可以在预设的整数范围内随机生成。

[0132] 步骤S280，第一方将第二挑战数x作为第一子变元X的取值，基于分离变换后的第二多项式，确定与第二隐私矩阵T对应的第一结果$\bar{t}$，以及与多个第二掩盖随机数对应的第二结果$\bar{\gamma}$；以及，基于第一多项式Lr，确定与第一隐私矩阵对应的第三结果lr，和与多个第一掩盖随机数对应的第四结果ρ。其中，第一结果和第二结果可以用于后续对关于第二隐私矩阵的相关验证，第三结果和第四结果可以用于后续对关于多个第一隐私矩阵的相关验证。

[0133] 第一方将第一结果$\bar{t}$、第二结果$\bar{\gamma}$、第三结果lr和第四结果ρ发送至第二方，第二方接收第一方发送的第一结果$\bar{t}$、第二结果$\bar{\gamma}$、第三结果lr和第四结果ρ。第一方在发送各个结果时，可以一一进行发送，也可以将各个结果进行打包后发送，本说明书对具体的发送方式不做限定。

[0134] 在一种实施方式中，第一多项式Lr可以为第二多项式tX的因式，且第一多项式Lr的各项基于不同幂次的变元分别与多个第一隐私向量$a_\tau b_\tau c_\tau$或第一掩盖向量d的乘积得到，分离变换后的第二多项式为第一变元向量Z、第二隐私矩阵T和第二变元向量F的乘积，且第一变元向量Z和第二变元向量F包含不同幂次的第一子变元X。

[0135] 在步骤S280中，基于分离变换后的第二多项式，确定与第二隐私矩阵T对应的第一结果$\bar{t}$，以及与多个第二掩盖随机数对应的第二结果$\bar{\gamma}$的步骤，包括：

[0136] 将第二挑战数x作为第一子变元X的取值，计算第一变元向量Z与第二隐私矩阵T的乘积，得到第一结果$\bar{t}$；计算第一变元向量Z与由多个第二掩盖随机数构成的第三掩盖向量γ的乘积，得到第二结果$\bar{\gamma}$。第一结果$\bar{t}$和第二结果$\bar{\gamma}$的计算过程可以采用以下公式表示：

[0137] $$\bar{t} = Z(x)T, \quad \bar{\gamma} = Z(x) \cdot \gamma \quad (7)$$

[0138] 以上仅仅是计算第一结果$\bar{t}$和第二结果$\bar{\gamma}$的一种方式，还可以基于第二隐私矩阵T与第二变元向量F的乘积，得到第一结果，基于第二变元向量F与第三掩盖向量γ的乘积计算第二结果。这些实施方式都能起到将ZTF进行分离而得到第一结果的目的，方便后续第二方对第二隐私矩阵T进行验证。

[0139] 在步骤S280中，基于第一多项式Lr，确定与第一隐私矩阵对应的第三结果lr，和与多个第一掩盖随机数对应的第四结果ρ的步骤，包括：

[0140] 将第二挑战数x、多个第一隐私向量$a_\tau b_\tau c_\tau$、第一掩盖向量d均代入第一多项式Lr中，得到第一结果lr；将多个第一掩盖随机数分别替换第一多项式Lr中对应的第一隐私向量和第一掩盖向量，得到第二结果ρ。其中，第二挑战数x作为第一子变元X的取值。

[0141] 例如，当第一多项式采用以下形式表示时，

[0142] $$Lr = \sum_{\tau=1}^{rn} a_\tau Y^\tau X^\tau + \sum_{\tau=1}^{rn} b_\tau X^{-\tau} + X^{rn} \sum_{\tau=1}^{rn} c_\tau X^\tau + dX^{2rn+1}$$

[0143] 将第二挑战数x、第一挑战数y、多个第一隐私向量$a_\tau b_\tau c_\tau$、第一掩盖向量d均代入上式Lr，可以得到以下第一结果lr：

[0144] $$lr = \sum_{\tau=1}^{rn} a_\tau x^\tau y^\tau + \sum_{\tau=1}^{rn} b_\tau x^{-\tau} + x^{rn} \sum_{\tau=1}^{rn} c_\tau x^\tau + dx^{2rn+1} \quad (8)$$

[0145] 将多个第一掩盖随机数α_τ, β_τ, γ_τ, δ分别替换上式lr中对应的第一隐私向量和第一掩盖向量，得到第二结果ρ：

[0146] $$\rho = \sum_{\tau=1}^{rn} \alpha_\tau x^\tau y^\tau + \sum_{\tau=1}^{rn} \beta_\tau x^{-\tau} + x^{rn} \sum_{\tau=1}^{rn} \gamma_\tau x^\tau + \delta x^{2rn+1} \quad (9)$$

[0147] 步骤S290，第二方基于各个承诺值和结果，执行以下第一判断、第二判断和第三判断。

[0148] 第一判断，利用预设承诺算法和第二结果$\bar{\gamma}$计算第一结果$\bar{t}$的第五承诺值；基于第二挑战数x、第四承诺值U和多个第三承诺值$T'_\eta T''_\psi$，以及分离变换后的第二多项式tX的变量表达形式，计算第一结果$\bar{t}$的第六承诺值；执行第五承诺值与第六承诺值是否相等的第一判断。

[0149] 第二判断，基于第二挑战数x、第一结果$\bar{t}$以及分离变换后的第二多项式tX的变量表达形式，计算第二多项式tX的第一取值；至少基于第三结果lr以及第二多项式tX的变量表达形式，计算第二多项式tX的第二取值；执行第一取值与第二取值是否相等的第二判断。

[0150] 第三判断，利用预设承诺算法和第四结果ρ计算第三结果lr的第七承诺值；基于第一挑战数y、第二挑战数x、第二承诺值D和多个第一承诺值$A_\tau B_\tau C_\tau$，以及第一多项式Lr的变量表达形式，计算第三结果lr的第八承诺值；执行第七承诺值与第八承诺值是否相等的第三判断。

[0151] 其中，上述三个判断的执行顺序可以有多种形式，本说明书并不限定上述三个判断的执行顺序。例如，第二判断可以在第一判断的结果为是时执行，第三判断可以在第一判断和第二判断的结果均为是时执行。

[0152] 当各个判断的结果均为是时，确定对约定同态加密过程和第一约定数据格式的零知识证明验证通过，当其中至少有一个判断的结果为否时，确定验证不通过，可以不再继续执行后续步骤。

[0153] 本实施例在进行验证之前有一个假设，即假设第一方按照约定同态加密过程对隐私数据进行了同态加密，且假设原始特征向量按照第一约定数据格式进行了处理，如果上述假设均成立，则上述三个判断过程的判断结果应均为是，如果三个判断过程的判断结果均为是，则上述假设成立，即确定第一方确实按照约定同态加密过程对隐私数据进行了加密，且原始特征向量确实符合第一约定数据格式。

[0154] 上述验证过程的一个前提是，所有约束方程都是基于约定同态加密过程和第一约定数据格式构建的。上述验证过程还根据了承诺值所满足的一定性质，即原数值的承诺值相乘的结果，等于原数值相加之后再计算承诺值，对原数值的承诺值进行求幂并相乘的结果，等于该原数值乘以对应的幂相加之后再计算承诺值，采用公式可以表示为

[0155] $$T' \cdot T'' = Com(t') \cdot Com(t'') = Com(t' + t'') \quad (10)$$

[0156] $$(T')^{x_1}\cdot(T'')^{x_2}=[Com(t')]^{x_1}\cdot[Com(t'')]^{x_2}=Com(x_1t'+x_2t'') \quad (11)$$

[0157] 其中，$T'=Com(t'),T''=Com(t'')$，T'为原数值t'的承诺值，T''为原数值t''的承诺值。$Com(t')$表示计算t'的承诺值，$Com(t'')$表示计算t''的承诺值，其中省略了所用到的随机数。

[0158] 在一种实施方式中，在变量表达形式中，第一多项式Lr为第二多项式tX的因式，且第一多项式Lr的各项基于不同幂次的变元分别与多个第一隐私向量 $a_\tau b_\tau c_\tau$或第一掩盖向量d的乘积得到。在变量表达形式中，分离变换后的第二多项式tX等于第一变元向量Z、第二隐私矩阵T和第二变元向量F的乘积。在本实施方式中，各个判断中的各项计算可以按照以下方式进行。

[0159] 在第一判断中，计算第一结果 $\bar{t}$的第六承诺值时，可以将第二挑战数x作为第一子变元X的取值，计算第一变元向量Z中的每一元素，并将每一元素作为对应的第三承诺值 $T'_\eta T''_\psi$和第四承诺值U的指数，计算各幂之间的连乘，得到第一结果$\bar{t}$的第六承诺值。

[0160] 在利用预设承诺算法和第二结果$\bar{\gamma}$计算第一结果$\bar{t}$的第五承诺值时，可以以第二结果 $\bar{\gamma}$为随机数，依据步骤S230中计算承诺值的方法计算第五承诺值。

[0161] 在第二判断中，计算第二多项式tX的第一取值时，可以将第二挑战数x作为第一变元X的取值，基于第一结果$\bar{t}$与第二变元向量F的乘积，确定第二多项式tX的第一取值。

[0162] 在第三判断中，计算第三结果lr的第八承诺值时，可以基于第一挑战数y、第二挑战数x计算第一多项式Lr的变量表达式中不同幂次的变元的第三取值，将多个第三取值分别作为对应的第二承诺值D和第一承诺值$A_\tau B_\tau C_\tau$的指数，计算各幂之间的连乘，得到第三结果lr的第八承诺值。

[0163] 在利用预设承诺算法和第四结果ρ计算第三结果lr的第七承诺值时，可以以第四结果 ρ为随机数，依据步骤S230中计算承诺值的方法计算第七承诺值。

[0164] 在另一实施方式中，当分离变换后的第二多项式tX的变量表达形式为 $tX=ZTF$时，且在式(7)中$\bar{t}=Z(x)T,\ \bar{\gamma}=Z(x)\cdot\gamma$，则第一结果$\bar{t}$可以表示为式(3)和式(4)的乘积，即

[0165] $$\bar{t}=Z(x)T=\left(x^{-m'_1n'},x^{-(m'_1-1)n'},\dots,x^{-n'},\right.$$
$$\left.x,x^{n'+1},\dots,x^{(m'_2-1)n'+1},x^2\right)\cdot(t'_0,t'_1,\dots,t'_{m'_1-1},t''_0,\dots,t''_{m'_2-1},u) \quad (12)$$

[0166] 则第一判断可以是判断以下等式(13)是否成立

[0167] $$Com_{ck}(\bar{t};\bar{\gamma})=\left(\prod_{\eta=0}^{m'_1-1}(T'_\eta)^{x^{(\eta-m_1)n'}}\right)\left(\prod_{\psi=0}^{m'_2-1}(T''_\psi)^{x^{\psi n'+1}}\right)U^{x^2} \quad (13)$$

[0168] 等式(13)是基于式(11)表示的承诺值性质而建立。在等式(13)中，等式左边为第一结果$\bar{t}$的第五承诺值，等式右边为第一结果$\bar{t}$的第六承诺值。

[0169] 第二判断可以是判断以下等式(14)是否成立

[0170] $$\bar{t}F(x)=lr\cdot lr'-2K \quad (14)$$

[0171] 其中，$lr' = lr \circ y' + 2Ls(x)$，$lr'$的计算以及$K$的取值可以参见式(1)和式(2)，$y' = (y^{rn}, \ldots, y^{rn \cdot cn})$，第二方利用第一挑战数$y$和第二挑战数$x$可以计算$Ls(x)$以及$lr'$的值。等式(14)的左边为第二多项式$tX$的第一取值，右边为第二多项式$tX$的第二取值。等式(14)是基于第二多项式，即式(2)建立。

[0172] 第三判断可以是判断以下等式(15)是否成立

[0173] $$Com_{ck}(lr;\rho) = [\prod_{\tau=1}^{rn} A_\tau{}^{x^\tau y^\tau}] * [\prod_{\tau=1}^{rn} B_\tau{}^{x^{-\tau}}] * [\prod_{\tau=1}^{rn} C_\tau{}^{x^{rn+\tau}}] D^{x^{2\cdot rn+1}} \quad (15)$$

[0174] 等式(15)是基于式(11)表示的承诺值性质而建立。在等式(15)中，等式左边为第三结果lr的第七承诺值，等式右边为第三结果lr的第八承诺值。

[0175] 步骤S200，当各个判断的结果均为是时，第二方基于第一约定数据格式，对多个原始特征密文c_i数据处理，得到数据处理结果。

[0176] 在基于第一约定数据格式，对多个原始特征密文的数据处理，可以是进行模型训练，也可以是进行数据融合或数据统计等处理。例如，第二方可以基于自身存储的多个业务对象的特征数据，以及多个原始特征密文，进行数据融合或者进行数据统计。第一方和第二方中多个业务对象均按照约定排列顺序进行排列，第一方和第二方共享该约定排列顺序。例如，第一方和第二方中共享按照一定顺序排列的业务对象标识，且第一方和第二方中的同一业务对象标识，表示同一个业务对象。例如，第一方中的业务对象1和第二方中的业务对象1均表示用户1，第一方中的业务对象20和第二方中的业务对象20均表示用户20。在具体实施方式部分的第五段中，给出了第二方联合两方的数据进行处理的一个例子。当第二方得到数据处理结果时，可以将该数据处理结果发送至第一方，实现数据处理结果的共享。

[0177] 在一种实施方式中，多个业务对象的原始特征密文c_i之间可以纵向排列。这里的纵向排列可以理解为，一个业务对象的原始特征密文占用一横行。对多个原始特征密文c_i进行数据处理时，可以基于第一约定数据格式，对多个原始特征密文c_i中的属性块进行纵向统计求和。

[0178] 在另一种实施方式中，多个业务对象的原始特征密文c_i之间可以横向排列。这里的横向排列可以理解为，一个业务对象的原始特征密文占用一竖列。对多个原始特征密文c_i进行数据处理时，可以基于第一约定数据格式，对多个原始特征密文c_i中的属性块进行横向统计求和。

[0179] 在上述实施方式中，业务对象的数量可能非常大，例如在百万级别。对原始特征密文进行统计求和时，可能产生进位。为了使得统计求和的结果不会因为进位的问题而产生错误，在一个实施例中，可以在原始特征向量中针对进位问题而增加预设0值。例如，每个原始特征向量m_i可以具有以下第一约定数据格式：其包括第一数量sn个属性块，每个属性块包括位于第一位置的第二数量个预设0值和位于第二位置的该属性块的特征值b^i_{sn}，特征值b^i_{sn}的取值或0或1。sn为整数，表示每个原始特征向量中的属性个数。第一位置可以在第二位置的左侧或者右侧。

[0180] 例如，当业务对象的总数量为100万个左右时，第二数量可以设置为31，那么31+1=32就是一个属性块占用的比特，如果第一数量为32，则一个原始特征向量即为32*32=1024比特。对每个原始特征向量进行Paillier同态加密之后的密文，即为2048比特。原始特征向量m_i可采用式(16)的形式表示

[0181] m_i=00…b_{32}…00…$b_2$00…b_1 (16)

[0182] 其中，b_1至b_{32}为原始特征向量中的32个特征值，其取值为0或1。

[0183] 当原始特征密文对应的明文采用式(16)的形式表示式，对指定的属性块进行统计求和时，该属性块中填充的0值能为统计求和中的进位提供空间，使得统计求和准确进行。

[0184] 在另一实施例中，多个约束方程具体可以基于以下内容构建：多个原始特征密文c_i的同态加密过程、多个辅助特征密文c_s^*的同态加密过程、第一约定数据格式和多个辅助特征向量m_s^*的第二约定数据格式；第一约定数据格式包括特征值b^i_{sn}的取值范围。

[0185] 其中，多个辅助特征密文c_s^*，通过以下同态加密过程加密得到：使用第一公钥N和多个第二加密随机数r_s^*，采用第一同态加密算法，分别对多个辅助特征向量m_s^*进行同态加密后得到。第二加密随机数r_s^*可以是在预设范围内随机生成的用于同态加密的随机数，针对每个待加密的明文，生成与之对应的第二加密随机数。

[0186] 多个辅助特征向量m_s^*，通过以第三数量个业务对象为单位，对按照约定排列顺序排练的多个业务对象进行分组，并将任意分组中多个原始特征向量的特征值b^i_{sn}进行拼接得到。第三数量为根据经验设定的预设值，例如可以为15。约定排列顺序是针对多个业务对象的排列顺序，第一方和第二方共享该约定排列顺序。

[0187] 基于约定同态加密过程和第一约定数据格式构建的约束方程，能对第一约定数据格式中进行验证。为了能进一步对原始特征向量中的特征值取值范围进行验证可以基于特征值构建辅助特征向量，并确定辅助特征密文。

[0188] 多个约束方程可以包括：

[0189] 方程一，通过将同态加密过程中的原始隐私数据采用变量标识，将同态加密过程转换得到的多个乘法约束方程和多个加法约束方程；

[0190] 方程二，通过将特征值b^i_{sn}、原始特征向量m_i采用变量标识，将每个原始特征向量m_i表示为第一数量sn个特征值b^i_{sn}分别与相应系数相乘后的和值，得到的加法约束方程，该系数基于第一数量sn和第二数量确定；

[0191] 方程三，通过将特征值b^i_{sn}采用变量标识，将特征值b^i_{sn}的取值范围采用乘法约束方程或加法约束方程表示时得到的约束方程。

[0192] 其中，原始隐私数据除了多个原始特征向量m_i之外，还可以包括：多个第一加密随机数r_i、多个辅助特征向量m_s^*、多个第二加密随机数r_s^*和多个特征值b^i_{sn}。在构建约束方程时，原始隐私数据采用变量标识。第一方和第二方共享所构建的约束方程。

[0193] 当特征值b^i_{sn}的取值或0或1时，针对特征值b^i_{sn}取值范围的约束方程包括：

[0194] 方程四，特征值b^i_{sn}减去1的差值与该特征值b^i_{sn}的乘积等于0。该方程可以表示为$b^i_{sn}\cdot\left(b^i_{sn}-1\right)=0$，其中$b^i_{sn}$表示第$i$个业务对象的原始特征向量的第$sn$个特征值。

[0195] 上述方程的解包含四组，0、1以及大于第一巨数值的两个解。其中，第一巨数值可以为2^{282}。为了在第一方具有的特征值的解中排除大于第一巨数值的两个解，上述方法还可以包括以下步骤1b-5b验证步骤。

[0196] 步骤1b，第一方在小于第一巨数值的整数范围内，随机生成第四数量j个挑选随机

数R_j'。其中，第四数量可以为预设数值，表示重复次数，例如可以为128或者其他数量，j可以在小于等于第四数量的正整数范围内取值。例如，第一方在 $[0,2^{282}]$整数范围内随机生成第四数量个$R_j', j \in [1,\ 128]$。

[0197] 步骤2b，第一方获取第二方随机生成的第四数量j个第一随机数$l_{i,sn}^{j}$的集合，第j个集合中的第一随机数$l_{i,sn}^{j}$的数量与多个原始特征向量m_i中的特征值b^{i}_{sn}总数相等，第一随机数$l_{i,sn}^{j}$的取值或0或1。

[0198] 第一方可以向第二方发送指示其生成第一随机数的消息，第二方在接收到该消息时，生成第一随机数。该消息可以携带第四数量以及特征值b^{i}_{sn}的总数。该特征值b^{i}_{sn}的总数是原始特征向量的总数量与每个原始特征向量中的特征值总数量的乘积。

[0199] 步骤3b，第一方，针对每个集合，将该集合中的各个第一随机数 $l_{i,sn}^{j}$分别与对应位置的特征值b^{i}_{sn}相乘，再与对应位置的挑选随机数R_j'相加，得到对应的第一验证数L_j'；第一方将得到的多个第一验证数 L_j'发送至第二方，第二方接收第一方发送的多个第一验证数 L_j'。

[0200] 本实施例中，可以采用以下式表示第一验证数的计算过程：

[0201] $$L_j' = \left(\sum_i \sum_{sn} l_{i,sn}^{j} \cdot b_{sn}^{i}\right) + R_j' \quad (17)$$

[0202] 其中，L_j'表示第j个第一验证数，$l_{i,sn}^{j}$表示第j个集合中与第i个原始特征向量中的第sn个特征值b^{i}_{sn}对应的第一随机数，R_j'表示第j个挑选随机数。

[0203] 第一方在发送多个第一验证数L_j'时，可以分别发送，也可以打包一起发送，本说明书对该发送方式不做限定。

[0204] 步骤4b，第二方在确定多个第一验证数 L_j'小于第一巨数值时，向第一方发送表示初步验证通过的第一通知。第二方可以判断每一个第一验证数L_j'是否小于第一巨数值。如果特征值的取值都为0或1，则式(17)等式右侧括号中的项会非常小，这使得每个L_j'与 R_j'的差值是可忽略的，而R_j'是在小于第一巨数值的整数范围内随机取值，若每个L_j'都小于第一巨数值，则证明第一方对特征值作弊的可能性为 $\frac{1}{2^{128}}$（例如在$j \in [1,128]$的条件下），L_j'的重复次数j越多，第一方作弊的可能性越小。而第一方在对特征值进行式(17)所示的变换之后，实际起到的作用是采用第一随机数对特征值进行随机化掩盖，这样又避免泄露第一方的隐私数据。

[0205] 步骤5b，第一方，当接收到第二方发送的表示初步验证通过的第一通知时，执行步骤S220，将原始隐私数据，按照预先构建的多个约束方程解的形式构建成多个第一隐私矩阵。其中，第一通知在确定多个第一验证数 L_j'小于第一巨数值时发送。

[0206] 采用本实施例的方式，可以预先向第二方对特征值的取值进行验证，排除所构建

的 $b_{sn}^{i}\cdot\left(b_{sn}^{i}-1\right)=0$约束方程中解为大于第一巨数值的情况。这样，后续的零知识证明过程会更加准确。

[0207] 在另一实施例中，约束方程还可以包括：

[0208] 方程五，通过将特征值b^{i}_{sn}、多个挑选随机数R_j'采用变量标识，基于第一验证数 L_j'的计算过程构建得到的加法约束方程。

[0209] 结合上述的方程一~方程五，可以构建更多的约束方程。下面对多个约束方程的具体形式进行说明。

[0210] 采用 $Const_{\{c,m,r\}}$表示一个明文m与其所对应密文c在使用随机数r进行Pallier同态加密时所满足的约束条件，其中$c=(1+N)^{m}\cdot r^{N}\bmod N^{2}$。该约束条件的生成过程可由计算 Paillier同态加密时所进行的所有步骤导出，即将幂运算过程转换为线性运算和乘法运算，得到以下多个约束方程

[0211] $$Const_{\{c,m,r\}}=\begin{cases}T^{0}=1+m\cdot N\\ R_0=r\\ R_1=R_{J_1}\cdot R_{k_1}\\ \vdots\\ R_w=R_{J_w}\cdot R_{k_w}(=r^{N})\\ c=T^{0}\cdot R_w\end{cases}\qquad(18)$$

[0212] 通过式(18)可以将同态加密过程转换为加法约束方程和多个乘法约束方程。其中，W的大小可通过如下方式确定

[0213] $$w=[\log_2 N]+h(N)-1$$

[0214] 其中，$h(N)$代表N的汉明重量，符号 [ ]代表向上取整，N为第一密钥。

[0215] 结合上述的方程一~方程五，并且将同态加密过程采用式(18)进行变换，以及，以第一数量sn取32，第二数量取31，第三数量取15为例，可以得到以下形式的多个约束方程：

[0216] ① $Const_{\{c_i,m_i,r_i\}}$

[0217] ② $\sum_{sn}2^{32sn-1}\cdot b_{sn}^{i}=m_i$

[0218] ③ $b_{sn}^{i}\cdot\left(b_{sn}^{i}-1\right)=0$

[0219] ④ $Const_{\{c_j^{'},R_j^{'},r_j^{'}\}}$

[0220] ⑤ $\left(\sum_i\sum_{sn}l_{i,sn}^{j}\cdot b_{sn}^{i}\right)+R_j^{'}=L_j^{'}$

[0221] ⑥ $2^{479}\cdot b_{sn}^{15s}+\cdots b_1^{15s-14}=m_s^{*}$

[0222] ⑦ $Const_{\{c_s^{*},m_s^{*},r_s^{*}\}}$

[0223] 其中，$Const_{\{c_j^{'},R_j^{'},r_j^{'}\}}$表示，使用第一公钥$N$和多个加密随机数$r_j$’，采用第一同态加密算法，分别对多个挑选随机数$R_j$’进行同态加密后得到密文$c_j$’。其中，多个加密随机

数r_j'和多个挑选随机数R_j'也属于隐私数据。密文c_j'可以共享给第二方。

[0224] 在上述多个约束方程中,①代表所有明文密文对需满足正确加密;若满足约束方程②-⑦,则说明原明文符合约定数据格式条件。其中,约束②保证了由b^i_{sn}可以构成m_i,约束③-⑦则用来保证所有特征值b^i_{sn}只能为0或1。

[0225] 在上述实施例中,第一方和第二方之间共享多个约束方程,以及第一多项式的变量表达形式、第二多项式的变量表达形式和分离变换后的第二多项式的变量表达形式,在变量表达形式中原始隐私数据采用变量标识。

[0226] 上述实施例中,可以采用Paillier同态加密技术将多个特征(例如32个特征)包装到一个明文中,可以高效地一次性加密多个特征。对于上述证明过程,实施例中引入了约束系统,将所要证明的内容转换为约束,并零知识证明这些约束。

[0227] 上述实施例中并不限定明文的长度必须小于同态加密的最小私钥长度,本实施例中引入的辅助特征向量,用每15 个明文中的特征值构造一个辅助特征向量并对其进行加密,即约束⑥⑦。由于此方法构造的辅助特征向量的长度小于最小私钥的长度,因此上述所有约束方程可以共同保证明文的正确加密且明文具有约定的特殊结构特征。此方案中,其通信量大小为乘法约束数量的平方根个群元素,通信量相对比较小,提高了通信效率。此外,由于实施例中的通信量与乘法约束数量呈平方根关系,则当被证明的信息数量越大时,每个信息的平均证明大小将会越小,实施例的高效性则越显著。

[0228] 在具体实现中,为了提高系统效率,可以在大群中求幂以及乘法运算的效率上,采用快速傅立叶变换(Fast Fourier Transform,FFT)技术、指数运算乘积(multi-exponentiation)技术以及预计算(pre-computation)技术等减少计算量,或者将其预先提前进行。具体来说,FFT技术可以降低计算两个多项式乘法时复杂度,例如在计算lr'时可以用其以提高效率;而指数运算乘积技术可以用于降低求幂运算时的计算复杂度,例如在对第一隐私矩阵A、B、C计算承诺值时可以采用此方法。此外,实施例中可以预先计算第一隐私矩阵 A、B、C中大部分项的取值,这样可以提高实际证明时的效率。

[0229] 上述内容对本说明书的特定实施例进行了描述,其他实施例在所附权利要求书的范围内。在一些情况下,在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行,并且仍然可以实现期望的结果。另外,在附图中描绘的过程不一定要按照示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中,多任务处理和并行处理也是可以的,或者可能是有利的。

[0230] 图3为实施例提供的一种保护数据隐私的多方联合处理数据的装置的示意性框图。多方包括第一方和第二方,所述第一方存储有原始隐私数据,其中包括多个业务对象的原始特征向量m_i,每个原始特征向量m_i具有第一约定数据格式,所述装置300部署在第一方中,该第一方可以通过任何具有计算、处理能力的设备、平台或设备集群来实现。该实施例与图2所示方法实施例中第一方执行的方法相对应。该装置300包括:

[0231] 第一获取模块310,配置为,获取多个原始特征密文C_i,并将其发送至所述第二方;其中,多个原始特征密文C_i通过约定同态加密过程对对应的原始特征向量m_i加密得到;

[0232] 第一构建模块320,配置为,将所述原始隐私数据,按照预先构建的多个约束方程解的形式构建成多个第一隐私矩阵,其中包括多个第一隐私向量 $a_\tau b_\tau c_\tau$;所述多个约束方

程基于所述约定同态加密过程和第一约定数据格式构建；

[0233] 第一承诺模块330，配置为，利用预设承诺算法和多个第一掩盖随机数，分别计算对应的第一隐私向量 $a_\tau b_\tau c_\tau$ 的第一承诺值 $A_\tau B_\tau C_\tau$，以及第一掩盖向量*d*的第二承诺值*D*；

[0234] 第一发送模块340，配置为，将所述第二承诺值*D*和多个第一承诺值 $A_\tau B_\tau C_\tau$ 发送至所述第二方；

[0235] 第一接收模块350，配置为，接收所述第二方发送的第一挑战数*y*；

[0236] 第二构建模块360，配置为，将所述第一挑战数*y*作为第二子变元*Y*的取值，确定基于所述多个约束方程、多个第一隐私向量 $a_\tau b_\tau c_\tau$、所述第一掩盖向量*d*、第一子变元*X*和所述第二子变元*Y*，构建的第一多项式*Lr*和第二多项式*tX*，并将所述第二多项式*tX*分离变换成第一变元向量*Z*、第二隐私矩阵*T*和第二变元向量*F*的乘积；所述第二隐私矩阵*T*包括第二掩盖向量*u*和多个第二隐私向量 t'；

[0237] 第二承诺模块370，配置为，利用所述预设承诺算法和多个第二掩盖随机数，分别计算对应的第二隐私向量 t' 的第三承诺值 $T'_\eta T''_\psi$，以及所述第二掩盖向量*u*的第四承诺值*U*；

[0238] 第二发送模块380，配置为，将所述第四承诺值*U*和多个第三承诺值 $T'_\eta T''_\psi$ 发送至所述第二方；

[0239] 第二接收模块390，配置为，接收所述第二方发送的第二挑战数*x*；

[0240] 第一确定模块311，配置为，将所述第二挑战数*x*作为所述第一子变元*X*的取值，基于分离变换后的第二多项式，确定与所述第二隐私矩阵*T*对应的第一结果 $\bar{t}$，以及与多个第二掩盖随机数对应的第二结果 $\bar{\gamma}$；以及，基于所述第一多项式*Lr*，确定与所述第一隐私矩阵对应的第三结果*lr*，和与多个第一掩盖随机数对应的第四结果 ρ；

[0241] 第三发送模块312，配置为，将所述第一结果 $\bar{t}$、第二结果 $\bar{\gamma}$、第三结果*lr*和第四结果 ρ 发送至所述第二方，以使所述第二方在基于接收的结果和承诺值进行验证并通过之后，对所述多个原始特征密文 C_i 进行数据处理。

[0242] 在一种实施方式中，所述第一多项式*Lr*为所述第二多项式*tX*的因式；所述第一多项式*Lr*的各项基于不同幂次的变元分别与多个第一隐私向量 $a_\tau b_\tau c_\tau$ 或所述第一掩盖向量*d*的乘积得到，所述变元包括所述第一子变元*X*和/或第二子变元*Y*；第一变元向量*Z*和第二变元向量*F*包含不同幂次的第一子变元*X*。

[0243] 在一种实施方式中，第一确定模块311，基于分离变换后的第二多项式，确定与所述第二隐私矩阵*T*对应的第一结果 $\bar{t}$，以及与多个第二掩盖随机数对应的第二结果 $\bar{\gamma}$ 时，包括：

[0244] 计算所述第一变元向量*Z*与所述第二隐私矩阵*T*的乘积，得到第一结果 $\bar{t}$；

[0245] 计算所述第一变元向量*Z*与由多个第二掩盖随机数构成的第三掩盖向量 γ 的乘积，得到第二结果 $\bar{\gamma}$。

[0246] 在一种实施方式中，第一确定模块311，基于所述第一多项式*Lr*，确定与所述第一

隐私矩阵对应的第三结果lr，和与多个第一掩盖随机数对应的第四结果 ρ时，包括：

[0247] 将所述第二挑战数x、多个第一隐私向量 $a_\tau b_\tau c_\tau$、所述第一掩盖向量d均代入所述第一多项式Lr中，得到第一结果lr；所述第二挑战数x作为所述第一子变元X的取值；

[0248] 将多个第一掩盖随机数分别替换所述第一多项式Lr中对应的第一隐私向量和第一掩盖向量，得到第二结果ρ。

[0249] 在一种实施方式中，每个原始特征向量m_i具有以下第一约定数据格式：其包括第一数量sn个属性块，每个属性块包括位于第一位置的第二数量个预设0值和位于第二位置的该属性块的特征值 b_{sn}^i，特征值b_{sn}^i的取值或0或1。

[0250] 在一种实施方式中，多个原始特征密文C_i通过以下约定同态加密过程加密得到：使用第一公钥N和多个第一加密随机数 r_i，采用第一同态加密算法，分别对多个原始特征向量m_i进行同态加密后得到。

[0251] 在一种实施方式中，所述多个约束方程具体基于以下内容构建：多个原始特征密文 C_i的同态加密过程、多个辅助特征密文 c_s^*的同态加密过程、所述第一约定数据格式和多个辅助特征向量m_s^*的第二约定数据格式；所述第一约定数据格式包括特征值b_{sn}^i的取值范围；

[0252] 所述多个辅助特征密文c_s^*，通过以下同态加密过程加密得到：使用所述第一公钥N和多个第二加密随机数r_s^*，采用所述第一同态加密算法，分别对多个辅助特征向量m_s^*进行同态加密后得到；

[0253] 所述多个辅助特征向量m_s^*，通过以第三数量个业务对象为单位，对按照约定排列顺序排练的多个业务对象进行分组，并将任意分组中多个原始特征向量的特征值 b_{sn}^i进行拼接得到。

[0254] 在一种实施方式中，多个约束方程包括：

[0255] 通过将同态加密过程中的原始隐私数据采用变量标识，将同态加密过程转换得到的多个乘法约束方程和多个加法约束方程；

[0256] 通过将特征值b_{sn}^i、原始特征向量m_i采用变量标识，将每个原始特征向量m_i表示为第一数量sn个特征值 b_{sn}^i分别与相应系数相乘后的和值，得到的加法约束方程，所述系数基于第一数量sn和第二数量确定；

[0257] 通过将特征值b_{sn}^i采用变量标识，将特征值 b_{sn}^i的取值范围采用乘法约束方程或加法约束方程表示时得到的约束方程。

[0258] 在一种实施方式中，所述原始隐私数据还包括：多个第一加密随机数r_i、多个辅助特征向量 m_s^*、多个第二加密随机数r_s^*和多个特征值 b_{sn}^i。

[0259] 在一种实施方式中，当特征值b_{sn}^i的取值或0或1时，针对特征值 b_{sn}^i取值范围的约束方程包括，特征值 b_{sn}^i减去1的差值与该特征值b_{sn}^i的乘积等于0；

[0260] 装置300还包括：

[0261] 随机数生成模块(图中未示出),配置为在小于第一巨数值的整数范围内,随机生成第四数量个挑选随机数 R_j';

[0262] 集合获取模块(图中未示出),配置为,获取所述第二方随机生成的第四数量个第一随机数 $l_{i,sn}^j$ 的集合,每个集合中的第一随机数 $l_{i,sn}^j$ 的数量与多个原始特征向量 m_i 中的特征值 b_{sn}^i 总数相等,第一随机数 $l_{i,sn}^j$ 的取值或0或1;

[0263] 验证数计算模块(图中未示出),配置为,针对每个集合,将该集合中的各个第一随机数 $l_{i,sn}^j$ 分别与对应位置的特征值 b_{sn}^i 相乘,再与对应位置的挑选随机数 R_j' 相加,得到对应的第一验证数 L_j';

[0264] 验证数发送模块(图中未示出),配置为,将得到的多个第一验证数 L_j' 发送至所述第二方;

[0265] 第一构建模块320,具体配置为,当接收到所述第二方发送的表示初步验证通过的第一通知时,将所述原始隐私数据,按照预先构建的多个约束方程解的形式构建成多个第一隐私矩阵;其中,所述第一通知在确定多个第一验证数 L_j' 小于所述第一巨数值时发送。

[0266] 在一种实施方式中,多个约束方程还包括:

[0267] 通过将特征值 b_{sn}^i、多个挑选随机数 R_j' 采用变量标识,基于所述第一验证数 L_j' 的计算过程构建得到的加法约束方程。

[0268] 在一种实施方式中,所述预设承诺算法包括佩德森承诺算法。

[0269] 在一种实施方式中,所述第一多项式Lr和第二多项式tX基于劳伦特多项式构建。

[0270] 在一种实施方式中,所述第一同态加密算法包括Paillier加密算法。

[0271] 在一种实施方式中,所述第一方和所述第二方之间共享所述多个约束方程,以及第一多项式的变量表达形式、第二多项式的变量表达形式和分离变换后的第二多项式的变量表达形式,在变量表达形式中原始隐私数据采用变量标识。

[0272] 在一种实施方式中,所述业务对象包括:用户、商品、商户或事件。

[0273] 图4为实施例提供的一种保护数据隐私的多方联合处理数据的装置的示意性框图。多方包括第一方和第二方,所述第一方存储有原始隐私数据,其中包括多个业务对象的原始特征向量m_i,每个原始特征向量m_i具有第一约定数据格式,所述装置400部署在第二方中,第二方可以通过任何具有计算、处理能力的设备、平台或设备集群来实现。该实施例与图2所示方法实施例中第二方执行的方法相对应。该装置400可以包括:

[0274] 第三接收模块410,配置为,接收所述第一方发送的多个原始特征密文 C_i,其通过约定同态加密过程对对应的原始特征向量m_i加密得到;

[0275] 第四接收模块420,配置为,接收所述第一方发送的第二承诺值D和多个第一承诺值 $A_\tau B_\tau C_\tau$;

[0276] 第四发送模块430,配置为,生成第一挑战数y,并将其发送至所述第一方;

[0277] 第五接收模块440,配置为,接收所述第一方发送的第四承诺值U和多个第三承诺值 $T_\eta' T_\psi''$;

[0278] 第五发送模块450，配置为，生成第二挑战数x，并将其发送至所述第一方；

[0279] 第六接收模块460，配置为，接收所述第一方发送的第一结果$\bar{t}$、第二结果$\bar{\gamma}$、第三结果lr和第四结果ρ；

[0280] 第一判断模块470，配置为，利用预设承诺算法和所述第二结果$\bar{\gamma}$计算所述第一结果$\bar{t}$的第五承诺值；基于所述第二挑战数x、所述第四承诺值U和多个第三承诺值$T_{\eta}'T_{\psi}''$，以及分离变换后的第二多项式tX的变量表达形式，计算所述第一结果$\bar{t}$的第六承诺值；执行所述第五承诺值与第六承诺值是否相等的第一判断；

[0281] 第二判断模块480，配置为，基于所述第二挑战数x、所述第一结果$\bar{t}$以及分离变换后的第二多项式tX的变量表达形式，计算第二多项式tX的第一取值；至少基于所述第三结果lr以及第二多项式tX的变量表达形式，计算第二多项式tX的第二取值；执行所述第一取值与所述第二取值是否相等的第二判断；

[0282] 第三判断模块490，配置为，利用所述预设承诺算法和所述第四结果ρ计算所述第三结果lr的第七承诺值；基于所述第一挑战数y、第二挑战数x、第二承诺值D和多个第一承诺值$A_{\tau}B_{\tau}C_{\tau}$，以及第一多项式Lr的变量表达形式，计算所述第三结果lr的第八承诺值；执行所述第七承诺值与第八承诺值是否相等的第三判断；

[0283] 第二确定模块411，配置为，当各个判断的结果均为是时，确定所述约定同态加密过程和所述第一约定数据格式的零知识证明验证通过；

[0284] 第一处理模块412，配置为，基于所述第一约定数据格式，对多个原始特征密文C_i进行数据处理，得到数据处理结果。

[0285] 在一种实施方式中，在变量表达形式中，所述第一多项式Lr为所述第二多项式tX的因式，所述第一多项式Lr的各项基于不同幂次的变元分别与多个第一隐私向量$a_{\tau}b_{\tau}c_{\tau}$或第一掩盖向量d的乘积得到，所述变元包括所述第一子变元X和/或第二子变元Y；

[0286] 在变量表达形式中，分离变换后的第二多项式tX等于第一变元向量Z、第二隐私矩阵T和第二变元向量F的乘积，所述第一变元向量Z和第二变元向量F包含不同幂次的第一子变元X。

[0287] 在一种实施方式中，第一判断模块470，计算所述第一结果$\bar{t}$的第六承诺值时，包括：

[0288] 将所述第二挑战数x作为所述第一子变元X的取值，计算所述第一变元向量Z中的每一元素，并将每一元素作为对应的第三承诺值$T_{\eta}'T_{\psi}''$和第四承诺值U的指数，计算各幂之间的连乘，得到所述第一结果$\bar{t}$的第六承诺值。

[0289] 在一种实施方式中，第二判断模块480，计算第二多项式tX的第一取值时，包括：

[0290] 将所述第二挑战数x作为所述第一变元X的取值，基于所述第一结果$\bar{t}$与所述第二变元向量F的乘积，确定第二多项式tX的第一取值。

[0291] 在一种实施方式中，第三判断模块490，计算第三结果lr的第八承诺值时，包括：

[0292] 基于所述第一挑战数y、第二挑战数x计算第一多项式Lr的变量表达式中不同幂次的变元的第三取值，将多个第三取值分别作为对应的第二承诺值D和第一承诺值$A_{\tau}B_{\tau}C_{\tau}$

的指数，计算各幂之间的连乘，得到所述第三结果*lr*的第八承诺值。

[0293] 在一种实施方式中，所述第二判断在所述第一判断的结果为是时执行，所述第三判断在所述第一判断和第二判断的结果均为是时执行。

[0294] 在一种实施方式中，每个原始特征向量m_i具有以下第一约定数据格式：其包括第一数量*sn*个属性块，每个属性块包括位于第一位置的第二数量个预设0值和位于第二位置的该属性块的特征值b_{sn}^{i}，特征值b_{sn}^{i}的取值或0或1；

[0295] 装置400还包括，通知发送模块(图中未示出)，配置为，接收所述第一方发送的多个第一验证数 L_j'；在确定多个第一验证数 L_j'小于第一巨数值时，向所述第一方发送表示初步验证通过的第一通知。

[0296] 在一种实施方式中，多个业务对象的原始特征密文C_i之间纵向排列；第一处理模块412，具体配置为，基于所述第一约定数据格式，对多个原始特征密文C_i中的属性块进行纵向统计求和。

[0297] 上述装置实施例与方法实施例相对应，具体说明可以参见方法实施例部分的描述，此处不再赘述。装置实施例是基于对应的方法实施例得到，与对应的方法实施例具有同样的技术效果，具体说明可参见对应的方法实施例。

[0298] 本说明书实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行图1至图2任一项所述的方法。

[0299] 本说明书实施例还提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现图1至图2任一项所述的方法。

[0300] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于存储介质和计算设备实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。

[0301] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明实施例所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

[0302] 以上所述的具体实施方式，对本发明实施例的目的、技术方案和有益效果进行了进一步的详细说明。所应理解的是，以上所述仅为本发明实施例的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

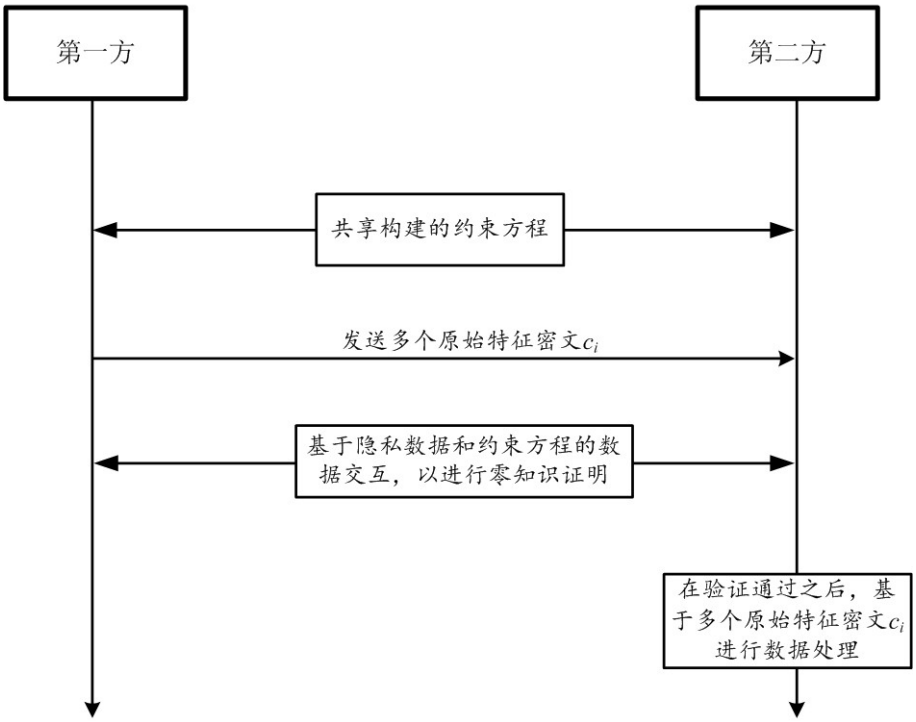

第一方
第二方
共享构建的约束方程
发送多个原始特征密文c_i
基于隐私数据和约束方程的数据交互，以进行零知识证明
在验证通过之后，基于多个原始特征密文c_i进行数据处理

图1

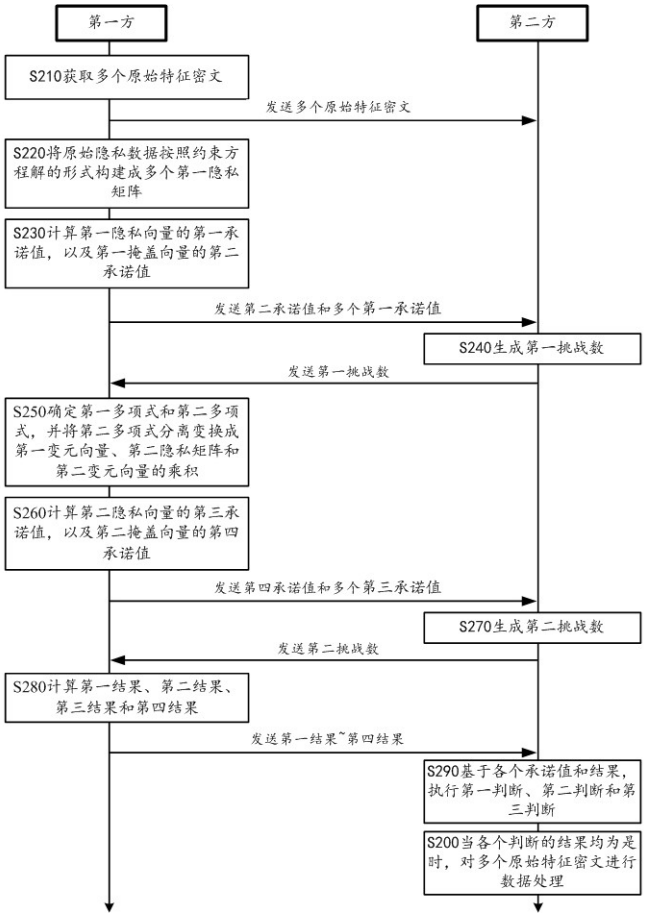

第一方
第二方
S210获取多个原始特征密文
发送多个原始特征密文
S220将原始隐私数据按照约束方程解的形式构建成多个第一隐私矩阵
S230计算第一隐私向量的第一承诺值，以及第一掩盖向量的第二承诺值
发送第二承诺值和多个第一承诺值
S240生成第一挑战数
发送第一挑战数
S250确定第一多项式和第二多项式，并将第二多项式分离变换成第一变元向量、第二隐私矩阵和第二变元向量的乘积
S260计算第二隐私向量的第三承诺值，以及第二掩盖向量的第四承诺值
发送第四承诺值和多个第三承诺值
S270生成第二挑战数
发送第二挑战数
S280计算第一结果、第二结果、第三结果和第四结果
发送第一结果~第四结果
S290基于各个承诺值和结果，执行第一判断、第二判断和第三判断
S200当各个判断的结果均为是时，对多个原始特征密文进行数据处理

图2

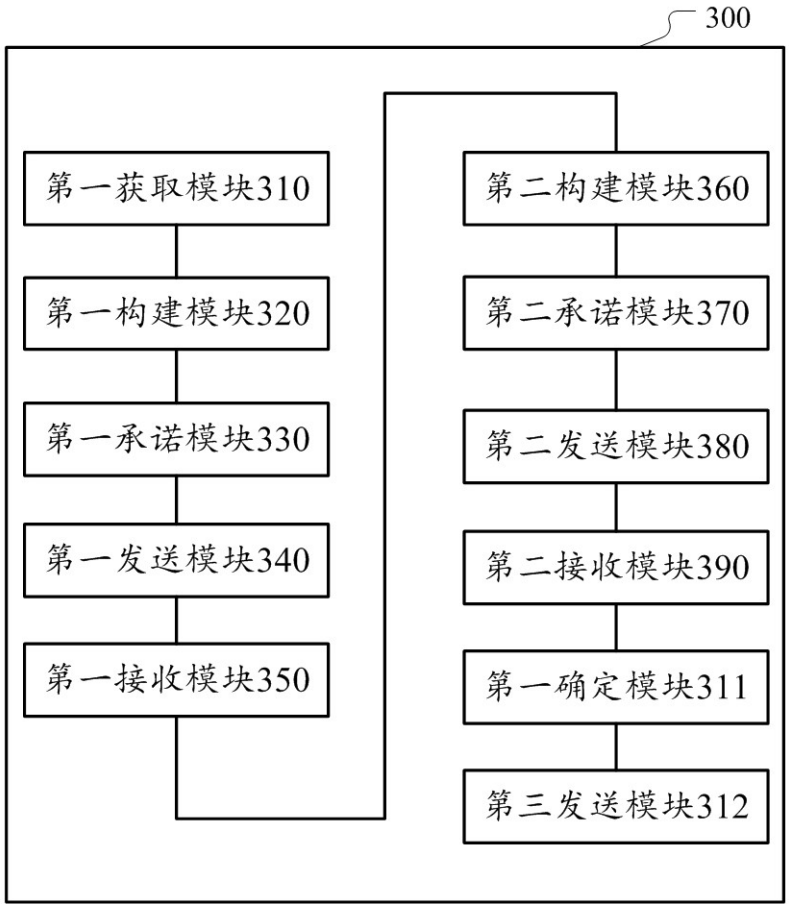

300
第一获取模块310
第一构建模块320
第一承诺模块330
第一发送模块340
第一接收模块350
第二构建模块360
第二承诺模块370
第二发送模块380
第二接收模块390
第一确定模块311
第三发送模块312

图3

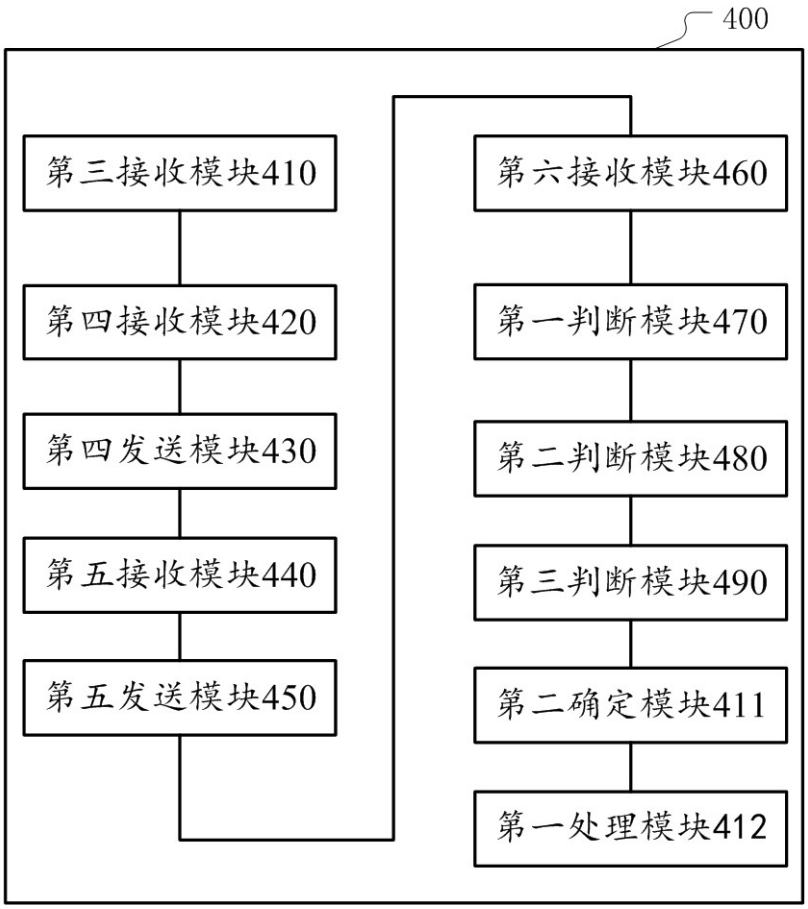

400
第三接收模块410
第四接收模块420
第四发送模块430
第五接收模块440
第五发送模块450
第六接收模块460
第一判断模块470
第二判断模块480
第三判断模块490
第二确定模块411
第一处理模块412

图4