(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2023 年 3 月 30 日 (30.03.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/045503 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2022/105052

(22) 国际申请日: 2022 年 7 月 12 日 (12.07.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202111133642.5 2021年9月27日 (27.09.2021) CN

(71) 申请人: 支付宝（杭州）信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路556号8层B段801-11, Zhejiang 310000 (CN)。

(72) 发明人: 杜健(DU, Jian); 中国浙江省杭州市西湖区西溪路556号8层B段801-11, Zhejiang 310000 (CN)。 段普(DUAN, Pu); 中国浙江省杭州市西湖区西溪路556号8层B段801-11, Zhejiang 310000 (CN)。 张本宇(ZHANG, Ben Yu); 中国浙江省杭州市西湖区西溪路556号8层B段801-11, Zhejiang 310000 (CN)。

(74) 代理人: 北京亿腾知识产权代理事务所（普通合伙） (E-TONE INTELLECTUAL PROPERTY FIRM (GENERAL PARTNERSHIP)); 中国北京市

(54) **Title:** FEATURE PROCESSING METHOD AND DEVICE BASED ON DIFFERENTIAL PRIVACY

(54) **发明名称:** 基于差分隐私进行特征处理的方法及装置

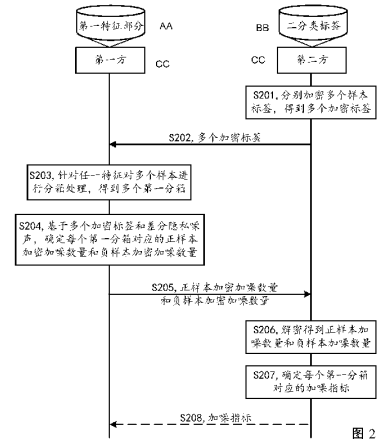


图 2

AA First feature portion
BB Binary classification label
CC First party
DD Second party
S201 Respectively encrypt the multiple binary classification labels to obtain multiple encryption labels
S202 Multiple encryption labels
S203 Obtain multiple first bins by binning multiple samples with respect to any feature
S204 Determine, on the basis of the multiple encryption labels and differential privacy noise, a positive sample encryption and noise-adding quantity and a negative sample encryption and noise-adding quantity corresponding to each of the multiple first bins
S205 Positive sample encryption and noise-adding quantity and negative sample encryption and noise-adding quantity
S206 Obtain a positive sample noise-adding quantity and a negative sample noise-adding quantity by means of encryption
S207 Determine a noise-adding indicator corresponding to each of the first bins
S208 Noise-adding indicator

(57) Abstract: Embodiments of the present description provide a feature processing method and device based on differential privacy. The method relates to a first party and a second party, where the first party stores a first feature portion of multiple samples, and the second party stores binary classification labels of the multiple samples. The method comprises: the second party respectively encrypts the multiple binary classification labels corresponding to the multiple samples so as to obtain multiple encryption labels; the first party determines, on the basis of the multiple encryption labels and differential privacy noise, a positive sample encryption and noise-adding quantity and a negative sample encryption and noise-adding quantity corresponding to each of multiple bins, where the multiple bins are obtained by binning the multiple samples with respect to any feature in the first feature portion; and the second party decrypts the positive sample encryption and noise-adding quantity and the negative sample encryption and noise-adding quantity to obtain a positive sample noise-adding quantity and a negative sample noise-adding quantity, so as to determine a noise-adding indicator of the corresponding bin.

(57) 摘要: 本说明书实施例提供一种基于差分隐私进行特征处理的方法及装置，所述方法涉及第一方和第二方，其中第一方存储多个样本的第一特征部分，第二方存储该多个样本的二分类标签；所述方法包括：第二方对多个样本对应的多个二分类标签分别进行加密，得到多个加密标签；第一方基于该多个加密标签以及差分隐私噪声，确定多个分箱中每个分箱对应的正样本加密加噪数量和负样本加密加噪数量，其中多个分箱是针对第一特征部分中的任一特征对多个样本进行分箱处理而得到；第二方对该正样本加密加噪数量和负样本加密加噪数量进行解密，得到正样本加噪数量和负样本加噪数量，从而确定出相对应分箱的加噪指标。

WO 2023/045503 A1

[见续页]

海淀区中关村紫金数码园3号楼707, Beijing 100190 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护)：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。