

(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



(10) 国际公布号  
**WO 2023/124400 A1**

(43) 国际公布日  
2023 年 7 月 6 日 (06.07.2023)

(51) 国际专利分类号:  
*G06F 21/62* (2013.01)

(21) 国际申请号: PCT/CN2022/125462

(22) 国际申请日: 2022 年 10 月 14 日 (14.10.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:  
202111621978.6 2021 年 12 月 28 日 (28.12.2021) CN

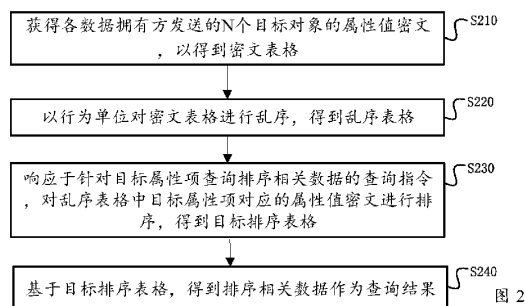
(71) 申请人: 支付宝 (杭州) 信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(72) 发明人: 潘无穷 (PAN, WuQiong); 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)。 韦韬 (WEI, Tao); 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)。 李婷婷 (LI, TingTing); 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)。 李天一 (LI, TianYi); 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)); 中国北京市海淀区中关村紫金数码园 3 号楼 707, Beijing 100190 (CN)。

(54) Title: MULTI-PARTY DATA QUERY METHOD AND APPARATUS FOR PROTECTING DATA PRIVACY

(54) 发明名称: 保护数据隐私的多方数据查询方法及装置



S210 Obtain attribute value ciphertext of N target objects sent by each data holder so as to obtain a ciphertext table  
S220 Perform out-of-order processing on the ciphertext table in rows to obtain an out-of-order table  
S230 In response to a query instruction for querying sorting-related data in respect of a target attribute item, sort the attribute value ciphertext corresponding to the target attribute item in the out-of-order table to obtain a target sorting table  
S240 On the basis of the target sorting table, obtain sorting-related data as a query result

图 2

(57) Abstract: A multi-party data query method and apparatus for protecting data privacy. Multiple parties comprise a plurality of data holders which respectively hold attribute values of a plurality of attribute items of N target objects. The method is executed by means of an intermediate party except the multiple parties. The method comprises: obtaining attribute value ciphertext of N target objects sent by each data holder so as to obtain a ciphertext table (S210), wherein one row of the ciphertext table corresponds to one target object, and one column corresponds to one attribute item; performing out-of-order processing on the ciphertext table in rows to obtain

[见续页]

WO 2023/124400 A1

(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, 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, CV, 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, ME, 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))。

an out-of-order table (S220); in response to a query instruction for querying sorting-related data in respect of a target attribute item, sorting the attribute value ciphertext corresponding to the target attribute item in the out-of-order table to obtain a target sorting table (S230); and on the basis of the target sorting table, obtaining sorting-related data as a query result (S240).

(57) 摘要: 一种保护数据隐私的多方数据查询方法及装置, 多方包括多个数据拥有方, 其各自持有N个目标对象的若干属性项的属性值, 方法通过多方之外的中间方执行, 方法包括: 获得各数据拥有方发送的N个目标对象的属性值密文, 以得到密文表格 (S210), 其中, 密文表格的一行对应于一个目标对象, 一列对应于一个属性项; 以行为单位对密文表格进行乱序, 得到乱序表格 (S220); 响应于针对目标属性项查询排序相关数据的查询指令, 对乱序表格中目标属性项对应的属性值密文进行排序, 得到目标排序表格 (S230); 基于目标排序表格, 得到排序相关数据作为查询结果 (S240)。