

(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
2024 年 7 月 4 日 (04.07.2024)



(10) 国际公布号
WO 2024/139320 A1

(51) 国际专利分类号:
G06F 7/24 (2006.01)

(21) 国际申请号: PCT/CN2023/115347

(22) 国际申请日: 2023 年 8 月 28 日 (28.08.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202211735449.3 2022 年 12 月 31 日 (31.12.2022) 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)。冯皓楠 (FENG, Haonan); 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)。钱中天 (QIAN, Zhongtian); 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: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市

(54) Title: DATA SORTING METHOD AND APPARATUS, AND DEVICE AND READABLE STORAGE MEDIUM

(54) 发明名称: 一种数据排序方法、装置、设备及可读存储介质

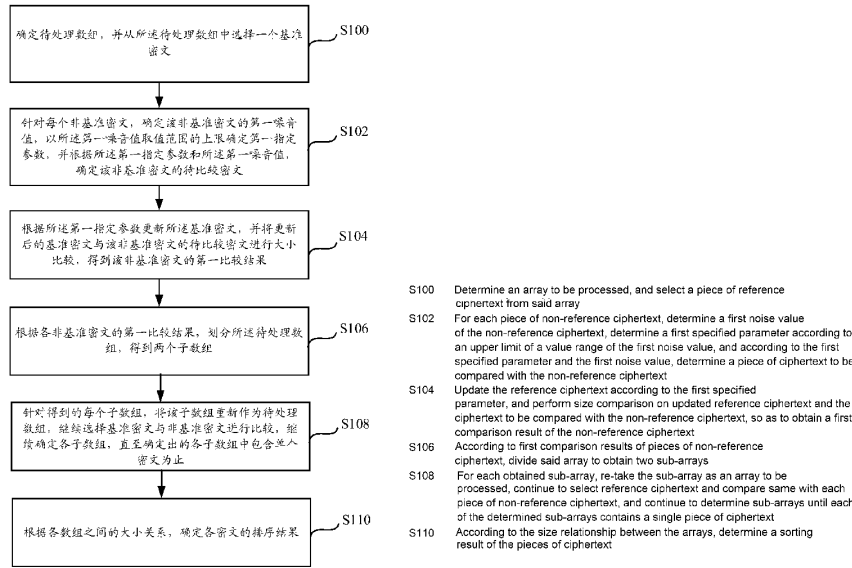


图 1

(57) Abstract: Disclosed in the present description are a data sorting method and apparatus, and a device and a readable storage medium. The data sorting method provided in the present description comprises: updating pieces of non-reference ciphertext according to first noise values corresponding to the pieces of non-reference ciphertext, and first specified parameters, and comparing each piece of non-reference ciphertext with updated reference ciphertext; and then dividing an array to be processed into a plurality of sub-arrays according to a first comparison result, respectively re-taking the sub-arrays as arrays to be processed, repeating the comparison process

[见续页]

海淀区上地三街9号嘉华大厦B座409,
Beijing 100085 (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, MG, MK, MN, MU, 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, SC, 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))。

until each of the arrays only contains a single piece of ciphertext, and determining a sorting result of the pieces of ciphertext according to the size relationship between the arrays. It can be seen that, during the sorting of pieces of ciphertext, pieces of non-reference ciphertext are updated according to noise values and first specified parameters, such that the relationship between original non-reference ciphertext and reference ciphertext is not leaked even if a comparison result is that the non-reference ciphertext is equal to the reference ciphertext, thereby improving the security and privacy protection of data during the sorting of the pieces of ciphertext.

(57) 摘要: 本说明书公开了一种数据排序方法、装置、设备及可读存储介质, 本说明书提供的排序方法中, 根据非基准密文对应的第一噪音值和第一指定参数更新非基准密文, 并将各非基准密文分别与更新后的基准密文进行比较。进而根据第一比较结果将待处理数组划分为多个子数组, 将各子数组分别重新作为待处理数组, 重复上述比较过程直至各数组只包含单一密文为止, 以各数组之间的大小关系, 确定各密文的排序结果。可见, 在对密文排序的过程中, 以噪音值和第一指定参数更新各非基准密文的方式, 即使比较结果为非基准密文与基准密文相等, 也不会泄露原始的非基准密文与基准密文之间的关系, 提高了密文排序过程中数据的安全性和隐私保护性。