

(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 2022/199290 A1

(43) 国际公布日
2022 年 9 月 29 日 (29.09.2022)

(51) 国际专利分类号:
G06F 21/60 (2013.01) G06F 21/62 (2013.01)
G06F 21/53 (2013.01)

(21) 国际申请号: PCT/CN2022/076771

(22) 国际申请日: 2022 年 2 月 18 日 (18.02.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110317808.2 2021年3月25日 (25.03.2021) 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

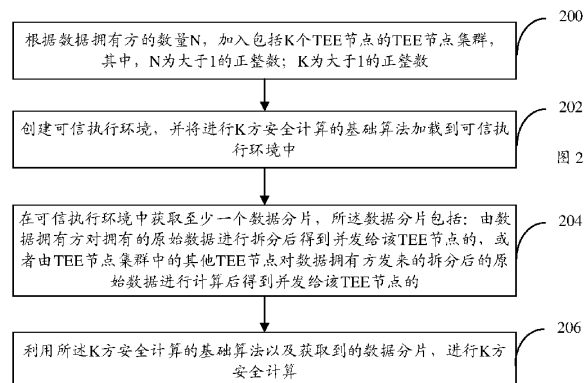
省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(72) 发明人: 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)。张煜龙 (ZHANG, Yulong); 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)。段然 (DUAN, Ran); 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)。张振飞 (ZHANG, Zhenfei); 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: SECURE MULTI-PARTY COMPUTATION

(54) 发明名称: 多方安全计算



200 Add, according to the number N of data owners, a TEE node cluster comprising K TEE nodes, wherein N is a positive integer greater than 1, and K is a positive integer greater than 1

202 Create a trusted execution environment, and load a basic algorithm for performing secure K-party computation into the trusted execution environment

204 Obtain at least one data fragment in the trusted execution environment, the data fragment being obtained after a data owner splits owned original data and being sent to a TEE node, or being obtained after other TEE nodes in the TEE node cluster calculate the split original data sent by the data owner and being sent to the TEE node

206 Perform secure K-party computation by using the basic algorithm of secure K-party computation and the obtained data fragment

(57) Abstract: Provided are a secure multi-party computation method and device. The method comprises: adding, according to the number N of data owners, a TEE node cluster comprising K TEE nodes (200); creating a trusted execution environment in the TEE nodes, and loading a basic algorithm for performing secure K-party computation into the trusted execution environment (202); obtaining at least one data fragment in the trusted execution environment; and performing secure K-party computation by using the basic algorithm of secure K-party computation and the obtained data fragment (206).

[见续页]

WO 2022/199290 A1

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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, 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))。

(57) 摘要: 提供了一种多方安全计算方法和装置。根据数据拥有方的数量N, 加入包括K个TEE节点的TEE节点集群(200); 在TEE节点中创建可信执行环境, 并将进行K方安全计算的基础算法加载到可信执行环境中(202); 在可信执行环境中获取至少一个数据分片; 利用K方安全计算的基础算法以及获取到的数据分片, 进行K方安全计算(206)。