

(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 2020/034754 A1

(43) 国际公布日
2020年2月20日 (20.02.2020)

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2019/092266

(22) 国际申请日: 2019年6月21日 (21.06.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810924482.8 2018年8月14日 (14.08.2018) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层847号邮箱, Grand Cayman (KY)。

(72) 发明人: 李漓春 (LI, Lichun); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。殷山 (YIN, Shan); 中

国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。王华忠 (WANG, Huazhong); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。林文珍 (LIN, Wenzhen); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (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,

(54) Title: SECURE MULTI-PARTY COMPUTATION METHOD AND APPARATUS, AND ELECTRONIC DEVICE

(54) 发明名称: 多方安全计算方法及装置、电子设备

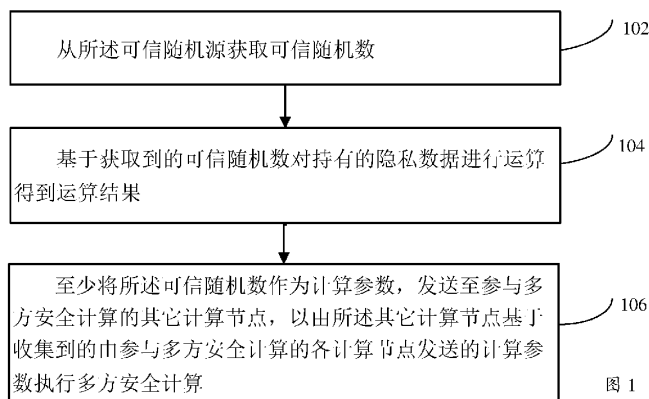


图 1

102 Obtain a trusted random number from a trusted random source
104 Perform an operation on held private data on the basis of the obtained trusted random number to obtain an operation result
106 Transmit at least the trusted random number as a computing parameter to other computing nodes participating in secure multi-party computation, so that the other computing nodes perform secure multi-party computation on the basis of collected computing parameters transmitted by the computing nodes participating in the secure multi-party computation

(57) Abstract: A secure multi-party computation method, applied to any computing node deployed in a distributed network. Multiple computing nodes are deployed in the distributed network, the multiple computing nodes jointly participate in secure multi-party computation on the basis of private data held by the computing nodes, and the computing node is connected to a trusted random source. The method comprises: obtaining a trusted random number from the trusted random source; performing an operation on the held private data on the basis of the obtained trusted random number to obtain an operation result; and transmitting at least the trusted random number as a computing parameter to other computing nodes participating in secure multi-party computation, so that the other computing nodes perform secure multi-party computation on the basis of collected computing parameters transmitted by the computing nodes participating in the secure multi-party computation.

[见续页]



WO 2020/034754 A1

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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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: 一种多方安全计算方法, 应用于分布式网络中部署的任一计算节点; 所述分布式网络部署了多个计算节点, 所述多个计算节点基于各自持有的隐私数据共同参与多方安全计算; 其中, 所述计算节点对接了可信随机源; 所述方法包括: 从所述可信随机源获取可信随机数; 基于获取到的可信随机数对持有的隐私数据进行运算得到运算结果; 至少将所述可信随机数作为计算参数, 发送至参与多方安全计算的其它计算节点, 以由所述其它计算节点基于收集到的由参与多方安全计算的各计算节点发送的计算参数执行多方安全计算。