

(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 2020/034751 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/CN2019/092217

(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:
201810925182.1 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)。

(54) Title: MULTI-PARTY SECURITY COMPUTING 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

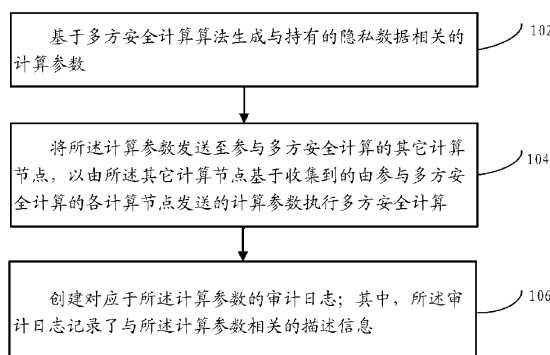


图 1

- 102 Generate computing parameters related to the held privacy data on the basis of a multi-party security computing algorithm
- 104 Send the computing parameters to other computing nodes participating in multi-party security computation so as to execute multi-party security computation by means of the other computing nodes on the basis of the acquired computing parameters sent by each computing node participating in multi-party security computation
- 106 Create an audit log corresponding to the computing parameters, wherein the audit log records description information related to the computing parameters

(57) Abstract: A multi-party security computing method, that is applied to any computing node deployed in a distributed network; the distributed network deploys multiple computing nodes, the multiple computing nodes jointly participating in multi-party security computation on the basis of respectively held privacy data; the method comprises: generating computing parameters related to the held privacy data on the basis of a multi-party security computing algorithm; sending the computing parameters to other computing nodes participating in multi-party security computation so as to execute multi-party security computation by means of the other computing

[见续页]

(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, 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))。

nodes on the basis of the acquired computing parameters sent by each computing node participating in multi-party security computation; and creating an audit log corresponding to the computing parameters, wherein the audit log records description information related to the computing parameters.

(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; 其中, 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, 所述方法包括: 基于多方安全计算算法生成与持有的隐私数据相关的计算参数; 将所述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; 以及, 创建对应于所述计算参数的审计日志; 其中, 所述审计日志记录了与所述计算参数相关的描述信息。