

(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 2020/034755 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 16/18 (2019.01) *H04L 9/08* (2006.01)
- (21) 国际申请号: PCT/CN2019/092340
- (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:
201810925187.4 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: MULTIPARTY SECURE COMPUTING METHOD, DEVICE, AND ELECTRONIC DEVICE

(54) 发明名称: 多方安全计算方法及装置、电子设备

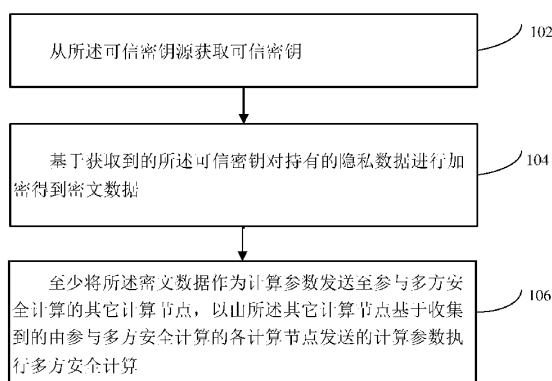


图 1

- 102 Acquire a trusted key from the trusted key source
- 104 Encrypt owned privacy data on the basis of the acquired trusted key to produce ciphertext data
- 106 At least transmit the ciphertext data as a computing parameter to other computing nodes participating in multiparty secure computing, thus allowing the other computing nodes to execute multiparty secure computing on the basis of collected computing parameters transmitted by the computing nodes participating in multiparty secure computing

(57) Abstract: A multiparty secure computing method, applicable in any computing node deployed in a distributed network. Multiple computing nodes are deployed in the distributed network. The multiple computing nodes jointly participate in multiparty secure computing on the basis of privacy data owned by each. The computing nodes are docked to a trusted key source. The method comprises: acquiring a trusted key from the trusted key source; encrypting, on the basis of the acquired trusted key, the owned privacy data to produce ciphertext data; at least transmitting the ciphertext data as a computing parameter to the other computing nodes participating

[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))。

in multiparty secure computing, thus allowing the other computing nodes to execute multiparty secure computing on the basis of the collected computing parameters transmitted by the computing nodes participating in multiparty secure computing.

(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密钥源; 所述方法包括: 从所述可信密钥源获取可信密钥; 基于获取到的所述可信密钥对持有的隐私数据进行加密得到密文数据; 至少将所述密文数据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。