

(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 2019/128567 A1

(43) 国际公布日
2019 年 7 月 4 日 (04.07.2019)

(51) 国际专利分类号:
G06Q 40/02 (2012.01)

(21) 国际申请号: PCT/CN2018/116838

(22) 国际申请日: 2018 年 11 月 22 日 (22.11.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201711480640.7 2017 年 12 月 29 日 (29.12.2017) 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: 杜华兵 (DU, Huabing); 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, 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,

(54) Title: DATA AUDITING METHOD AND DEVICE

(54) 发明名称: 一种数据审计的方法及装置

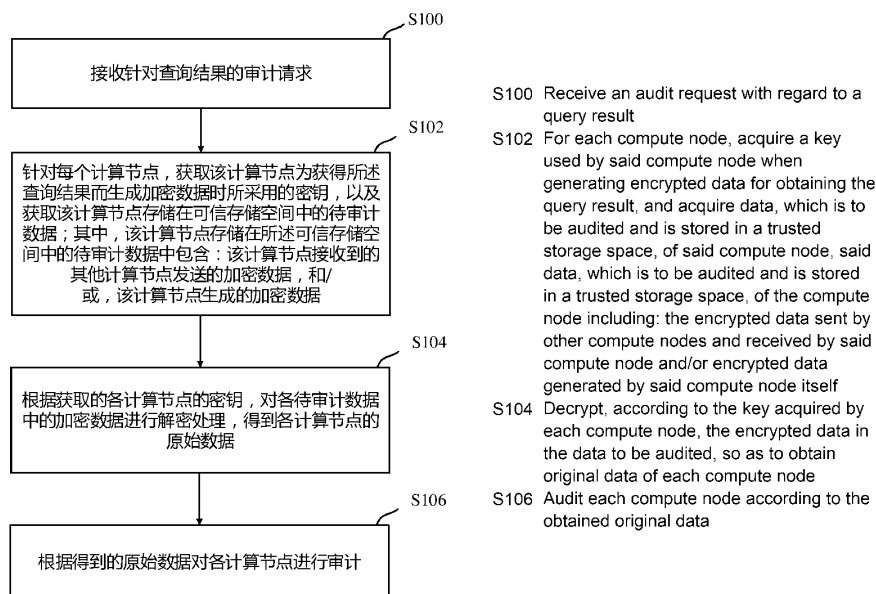


图 2

(57) Abstract: A data auditing method and device. For each compute node, when secure multi-party computation is performed according to a query request, the received encrypted data sent by other compute nodes and/or encrypted data generated by itself can be stored in a trusted storage space as data to be audited. In this way, if the agent subsequently receives an audit request with regard to a query result corresponding to the query request, the agent can decrypt, according to the key acquired from each compute node, the encrypted data which is acquired from the trusted storage space and included in the data to be audited, so as to obtain original data of each compute node, and audit each compute node according to the original data.

[见续页]

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: 一种数据审计的方法及装置, 针对每个计算节点, 在根据查询请求进行安全多方计算时, 可将接收到其他计算节点发送的加密数据和/或自身生成的加密数据, 作为待审计数据存储在可信存储空间中。使得后续若代理方接收到针对该查询请求对应的查询结果的审计请求, 可由代理方根据从各计算节点获取的密钥, 对从可信存储空间中获取的各待审计数据中包含的加密数据进行解密处理, 得到各计算节点的原始数据。并根据各原始数据对各计算节点进行审计。