(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

(43) 国际公布日
2023 年 6 月 29 日 (29.06.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/116147 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2022/125724

(22) 国际申请日: 2022 年 10 月 17 日 (17.10.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202111585885.2 2021年12月23日 (23.12.2021) CN

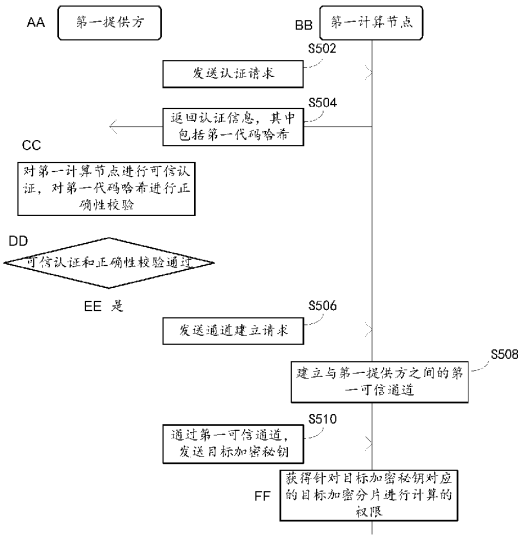
(71) 申请人: 支付宝（杭州）信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(72) 发明人: 潘无穷(PAN, Wuqiong); 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)。 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)。 李婷婷(LI, Tingting); 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)。 钱中天(QIAN, Zhongtian); 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)。 李天一(LI, Tianyi); 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)。 卫振强(WEI, Zhenqiang); 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: 北京亿腾知识产权代理事务所（普通合伙） (E-TONE INTELLECTUAL PROPERTY FIRM (GENERAL PARTNERSHIP)); 中国北京市

(54) **Title:** METHOD, APPARATUS AND SYSTEM FOR ACQUIRING DATA AUTHORIZATION

(54) 发明名称: 获取数据授权的方法、装置及系统



S502 Send an authentication request
S504 Return authentication information, which comprises a first code hash
S506 Send a channel establishment request
S508 Establish a first trusted channel between the first computing node and the first provider
S510 Send a target encryption key via the first trusted channel
AA First provider
BB First computing node
CC Perform trusted authentication on the first computing node, and perform correctness verification on the first code hash
DD Are trusted authentication and correctness verification passed?
EE Yes
FF Obtain the permission to perform computation on a target encrypted fragment corresponding to the target encryption key

图 5

(57) **Abstract:** Provided in the embodiments of the present description are a method, apparatus and system for acquiring data authorization. The method for acquiring data authorization comprises: any first computing node in a trusted computing center receiving an authentication request from a first provider; returning authentication information to the first provider, wherein the authentication information at least comprises a first code hash of a first computing logic that is run in the first computing node; receiving a channel establishment request sent by the first provider after the first provider determines that the first computing node passes trusted authentication and the first code hash passes correctness verification; establishing a first trusted channel between the first computing node and

WO 2023/116147 A1

[见续页]

海淀区中关村紫金数码园3号楼707, Beijing 100190 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, CV, 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, ME, 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:

一 包括国际检索报告(条约第21条(3))。

the first provider according to the channel establishment request; and receiving, via the first trusted channel, a target encryption key among encryption keys of several encrypted fragments that are obtained on the basis of private data of a data provider, so as to obtain the permission to perform, on the basis of the first computing logic, computation on a target encrypted fragment corresponding to the target encryption key. Therefore, the security of private data of a data provider can be ensured.

(57) 摘要：本说明书实施例提供一种获取数据授权的方法、装置及系统，在获取数据授权的方法中，可信计算中心中任意的第一计算节点，从第一提供方接收认证请求。向第一提供方返回认证信息，其中至少包括第一计算节点中运行的第一计算逻辑的第一代码哈希。接收第一提供方在确定第一计算节点通过可信认证，且第一代码哈希通过正确性验证后发送的通道建立请求。根据通道建立请求，建立与第一提供方之间的第一可信通道。通过第一可信通道，接收基于数据提供方的隐私数据获得的若干加密分片的各加密秘钥中的目标加密秘钥，从而获得基于第一计算逻辑，对目标加密秘钥对应的目标加密分片进行计算的权限。由此，可确保数据提供方的隐私数据的安全性。