

(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 2020/119263 A1

(43) 国际公布日
2020年6月18日 (18.06.2020)

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2019/112645

(22) 国际申请日: 2019年10月23日 (23.10.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811521029.9 2018年12月12日 (12.12.2018) 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)。

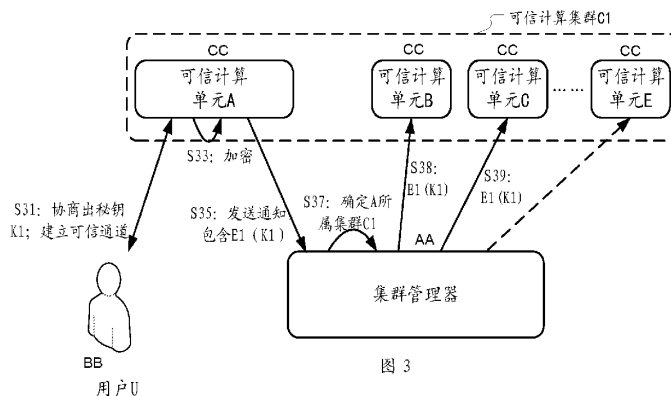
(72) 发明人: 周爱辉 (ZHOU, Aihui); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团

法务部, Zhejiang 311121 (CN)。黄群山 (HUANG, Qunshan); 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)。余超凡 (YU, Chaofan); 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)。蔡伟文 (CAI, Weiwen); 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)。王磊 (WANG, Lei); 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: METHOD AND APPARATUS FOR ESTABLISHING TRUSTED CHANNEL BETWEEN USER AND TRUSTED COMPUTING CLUSTER

(54) 发明名称: 在用户和可信计算集群之间建立可信通道的方法及装置



(57) Abstract: Provided are a method and apparatus for establishing a trusted channel between a user and a trusted computing cluster. According to the method, when a user wants to establish a trusted channel with a trusted computing cluster, the user only needs to negotiate a session key with any first trusted computing unit in the cluster to establish the trusted channel; then, the first trusted computing unit uses a common cluster key of the trusted computing cluster where the first trusted computing unit belongs to encrypt the session key, and sends same to a cluster manager; and the cluster manager distributes the encrypted session key in the trusted computing cluster so that the other trusted computing units in the cluster acquire the session key to participate in the trusted channel. Thus, the user establishes the trusted channel with the entire trusted computing cluster.

[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))。

(57) 摘要: 本说明书实施例提供一种在用户与可信计算集群之间建立可信通道的方法和装置。根据以上方法, 当用户想要与可信计算集群建立可信通道时, 用户仅需要与该集群中的任意的第一可信计算单元协商出会话密钥, 建立可信通道。然后, 第一可信计算单元利用所属的可信计算集群共同的集群密钥, 对该会话密钥进行加密, 并发送给集群管理器。集群管理器将加密的会话密钥在可信计算集群中传播, 从而使得集群中的其他可信计算单元获取到会话密钥, 加入到该可信通道。于是, 用户与整个可信计算集群建立起可信通道。