

(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
2020 年 7 月 2 日 (02.07.2020)



(10) 国际公布号
WO 2020/134632 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/116252

(22) 国际申请日: 2019 年 11 月 7 日 (07.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811631728.9 2018 年 12 月 29 日 (29.12.2018) 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: 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)。 陈星宇 (CHEN,

Xingyu); 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)。 解岭 (XIE, Ling); 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)。

(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,

(54) Title: METHOD AND DEVICE FOR ESTABLISHING TRUSTED COMPUTING CLUSTER

(54) 发明名称: 一种建立可信计算集群的方法和装置

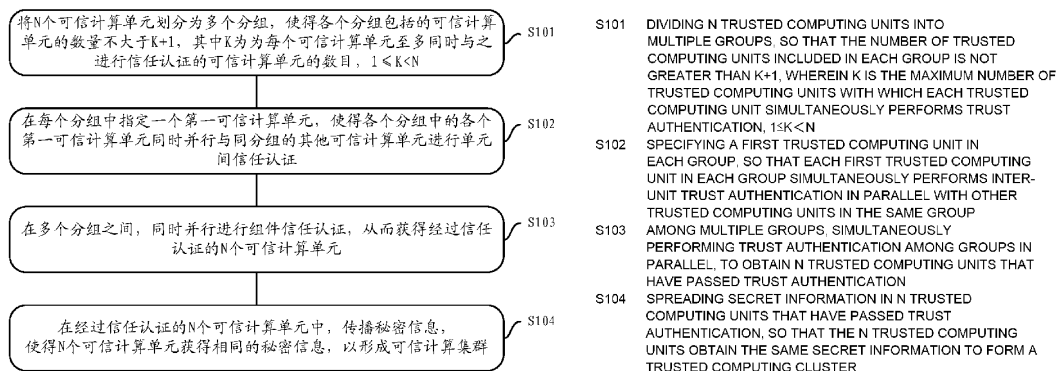


图 3

(57) Abstract: The embodiment provides a method and a device for establishing trusted cluster, which is used to form a trusted computing cluster with N trusted computing units, the method comprises: dividing N trusted computing units into multiple groups, so that the number of trusted computing units included in each group is not greater than K+1, K is the maximum number of trusted computing units with which each trusted computing unit simultaneously performs trust authentication; specifying a first trusted computing unit in each group, so that each first trusted computing unit in each group simultaneously performs inter-unit trust authentication in parallel with other trusted computing units in the same group; among multiple groups, simultaneously performing trust authentication among groups in parallel, to obtain N trusted computing units that have passed trust authentication; spreading secret information in N trusted computing units that have passed trust authentication, so that the N trusted computing units obtain the same secret information to form a trusted computing cluster.

[见续页]

WO 2020/134632 A1

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: 本实施例提供了一种建立可信集群的方法和装置, 用于将N个可信计算单元形成可信计算集群, 方法包括, 将N个可信计算单元划分为多个分组, 使得各个分组包括的可信计算单元的数量不大于K+1, K为每个可信计算单元至多同时与之进行信任认证的可信计算单元的数目; 在每个分组中指定一个第一可信计算单元, 使得各个分组中的各个第一可信计算单元同时并行地与同分组的其它可信计算单元进行单元间信任认证; 在多个分组之间, 同时并行进行组间信任认证, 从而获得经过信任认证的N个可信计算单元; 在经过信任认证的N个可信计算单元中, 传播秘密信息, 使得N个可信计算单元获得相同的秘密信息, 以形成可信计算集群。