

(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 2022/213968 A1

(43) 国际公布日
2022 年 10 月 13 日 (13.10.2022)

(51) 国际专利分类号:
G06F 21/53 (2013.01)

(21) 国际申请号: PCT/CN2022/085266

(22) 国际申请日: 2022 年 4 月 6 日 (06.04.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110369397.1 2021 年 4 月 6 日 (06.04.2021) 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)。

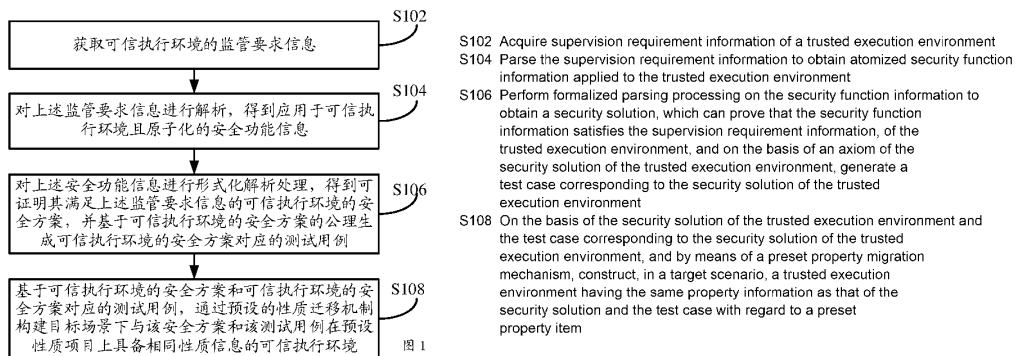
(72) 发明人: 曹爽 (CAO, Shuang); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(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, IT, JM, 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,

(54) Title: METHOD, APPARATUS AND DEVICE FOR CONSTRUCTING TRUSTED EXECUTION ENVIRONMENT

(54) 发明名称: 用于构建可信执行环境的方法、装置及设备



(57) Abstract: A method, apparatus and device for constructing a trusted execution environment. The method comprises: acquiring supervision requirement information of a trusted execution environment (S102); parsing the supervision requirement information to obtain atomized security function information applied to the trusted execution environment (S104); performing formalized parsing processing on the security function information to obtain a security solution, which can prove that the security function information satisfies the supervision requirement information, of the trusted execution environment, and on the basis of an axiom of the security solution of the trusted execution environment, generating a test case corresponding to the security solution of the trusted execution environment (S106); and on the basis of the security solution of the trusted execution environment and the test case corresponding to the security solution of the trusted execution environment, and by means of a preset property migration mechanism, constructing, in a target scenario, a trusted execution environment having the same property information as that of the security solution and the test case with regard to a preset property item (S108).

[见续页]

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, 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: 一种可信执行环境的构建方法、装置及设备, 该方法包括: 获取可信执行环境的监管要求信息 (S102); 对所述监管要求信息进行解析, 得到应用于所述可信执行环境且原子化的安全功能信息 (S104); 对所述安全功能信息进行形式化解析处理, 得到可证明其满足所述监管要求信息的所述可信执行环境的安全方案, 并基于所述可信执行环境的安全方案的公理生成所述可信执行环境的安全方案对应的测试用例 (S106); 基于所述可信执行环境的安全方案和所述可信执行环境的安全方案对应的测试用例, 通过预设的性质迁移机制构建目标场景下与所述安全方案和所述测试用例在预设性质项目上具备相同性质信息的可信执行环境 (S108)。