

(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 2024/060853 A1

(43) 国际公布日
2024 年 3 月 28 日 (28.03.2024)

- (51) 国际专利分类号:
G06F 21/74 (2013.01) **G06F 21/62** (2013.01)
- (21) 国际申请号: PCT/CN2023/110872
- (22) 国际申请日: 2023 年 8 月 2 日 (02.08.2023)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202211168325.1 2022 年 9 月 23 日 (23.09.2022) 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: 张璇 (**ZHANG, Xuan**); 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)。吴超 (**WU, Chao**); 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)。辛知 (**XIN, Zhi**); 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, 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, MU, 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。

(54) **Title:** METHOD, DEVICE AND APPARATUS FOR DYNAMICALLY CONFIGURING SECURE MEMORY, AND STORAGE MEDIUM

(54) 发明名称: 一种动态配置安全内存的方法、设备、装置及存储介质

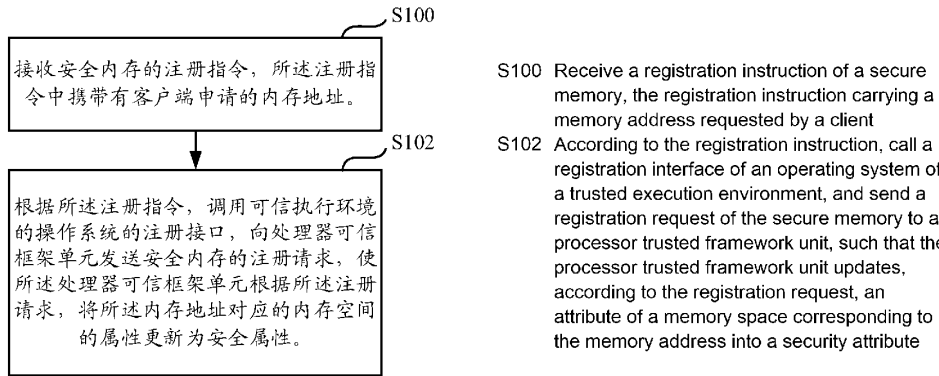


图 1

(57) **Abstract:** Disclosed in the present description are a method, device and apparatus for dynamically configuring a secure memory, and a storage medium. A client in a general execution environment sends a registration instruction of a secure memory to a trusted application in a trusted execution environment, the registration instruction carrying a memory address; and according to the registration instruction, the trusted application calls a registration interface of an operating system of the trusted execution environment, and sends a registration request of the secure memory to a processor trusted framework unit, such that the processor trusted framework unit updates, according to the registration request, an attribute of a memory space corresponding to the memory address into a security attribute. By dynamically configuring the secure memory, the present method not only meets the security requirement for privacy protection, but also reduces the waste of memory resources.

[见续页]

(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, SC, 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:
— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本说明书公开了一种动态配置安全内存的方法、设备、装置及存储介质。通用执行环境中的客户端向可信执行环境中的可信应用发送安全内存的注册指令, 注册指令中携带内存地址, 可信应用根据该注册指令, 调用可信执行环境的操作系统的注册接口, 向处理器可信框架单元发送安全内存的注册请求, 使处理器可信框架单元根据注册请求, 将内存地址对应的内存空间的属性更新为安全属性, 本方法通过动态配置安全内存既满足了隐私保护方面的安全要求, 又减少了内存资源的浪费。