(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 September 2025 (18.09.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/193638 A1

(51) International Patent Classification:
G06F 21/53 (2013.01) *G06F 21/60* (2013.01)
G06F 21/57 (2013.01)

(21) International Application Number:
PCT/US2025/019261

(22) International Filing Date:
11 March 2025 (11.03.2025)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/563,951 11 March 2024 (11.03.2024) US
18/666,801 16 May 2024 (16.05.2024) US

(71) Applicant: **TENSTORRENT USA, INC.** [US/US]; 7717 Southwest Pkwy, Building #3, Suite 200, Austin, Texas 78735 (US).

(72) Inventors: **CHEN, Zhimin**; 6653 Mount Holly Dr., San Jose, California 95120 (US). **DOCKSER, Kenneth**; 9500 Palmbrook Dr., Austin, Texas 78717 (US). **ISHII, Yasuo**; 580 Arastradero Rd. #307, Palo Alto, California 94306 (US). **OUSHEROVITCH, Alex**; 7717 Southwest Pkwy, Building #3, Suite 200, Austin, Texas 78735 (US).

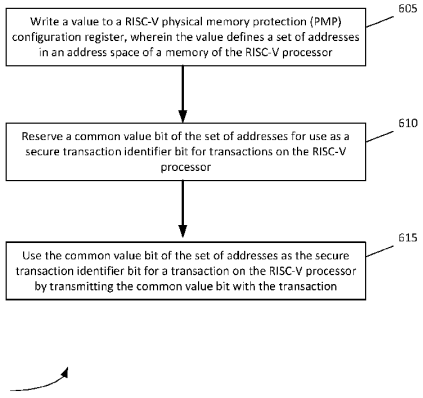
(74) Agent: **SCHEUERLEIN, Eric**; 3790 El Camino Real, Unit #531, Palo Alto, California 94306 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: 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,

WO 2025/193638 A1

(54) Title: STATIC TRUSTED EXECUTION ENVIRONMENT FOR INTER-ARCHITECTURE PROCESSOR PROGRAM COMPATIBILITY

FIG. 6



(57) Abstract: Computer-implemented methods and associated hardware for static trusted execution environment for inter-architecture processor program compatibility are disclosed herein. A device (e.g., RISC-V), may emulate a static trusted execution environment (e.g., ARM TrustZone) using physical memory protection (PMP). A regular world may have access to only a portion of an address space of the device, while a secure world may have access to the full address space. A secure world identifier (SWID) may be a configuration status register (CSR) only accessible by a mode (e.g., machine mode). When an entry is added to a translation lookaside buffer (TLB), the SWID may be added as part of a tag to differentiate secure world entries from regular world entries.

[Continued on next page]

TJ, TM, TN, TR, TT, TZ, UA, UG, US, UY, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (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).

Published:
— *with international search report (Art. 21(3))*