

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
08 August 2024 (08.08.2024)



(10) International Publication Number
WO 2024/163410 A1

(51) International Patent Classification:

G06F 21/57 (2013.01) G06F 11/36 (2006.01)
G06F 9/30 (2018.01) G06F 21/12 (2013.01)
G06F 9/448 (2018.01)

(21) International Application Number:

PCT/US2024/013463

(22) International Filing Date:

30 January 2024 (30.01.2024)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/442,226 31 January 2023 (31.01.2023) US

(71) Applicant: **CARNEGIE MELLON UNIVERSITY**
[US/US]; 5000 Forbes Avenue, Pittsburgh, Pennsylvania
15213 (US).

(72) Inventors: **VASUDEVAN, Amit**; c/o Carnegie Mellon
University, 5000 Forbes Avenue, Pittsburgh, Pennsylv-
ania 15213 (US). **DERAKHSHAN, Farzaneh**; c/o Carnegie
Mellon University, 5000 Forbes Avenue, Pittsburgh, Penn-

sylvania 15213 (US). **ZHANG, Zichao**; c/o Carnegie Mel-
lon University, 5000 Forbes Avenue, Pittsburgh, Penn-
sylvania 15213 (US). **JIA, Limin**; c/o Carnegie Mellon
University, 5000 Forbes Avenue, Pittsburgh, Pennsylvania
15213 (US).

(74) Agent: **CARLETON, Dennis** et al.; 2601 Weston Park-
way, Suite 103, Cary, North Carolina 27513 (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,
TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS,
ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, CV,

(54) Title: END-TO-END VERIFIED TRUSTED EXECUTION ENVIRONMENTS

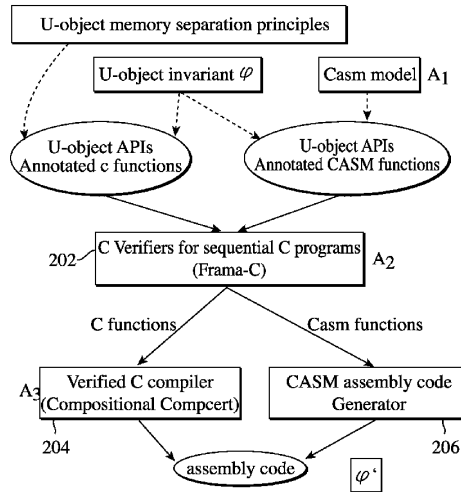


FIG. 2

(57) Abstract: Disclosed herein is a formalized programming framework using memory compartmentalization and other properties of certified compilers to provide that security guarantees verified at the source level also hold on the compiled code. A trusted execution environment formulated as a collection of objects that access separate memory locations and conform to a public interface.

[Continued on next page]

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))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))