



(51) International Patent Classification:

G06F 12/14 (2006.01) G06F 21/62 (2013.01)
G06F 21/53 (2013.01) G06F 21/64 (2013.01)

(21) International Application Number:

PCT/IL2019/050351

(22) International Filing Date:

26 March 2019 (26.03.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

258380 26 March 2018 (26.03.2018) IL

(71) Applicant: KAZUAR ADVANCED TECHNOLOGIES LTD. [IL/IL]; 126 Yigal Alon St., Tel-Aviv 6744332 (IL).

(72) Inventors: FINCHELSTEIN, Daniel Mondy; 10 Hahityashvut Street, 7583 160 Rishon Lezion (IL). PORAT, Yuval Moshe; 20 Sderot Smuts Street, 6200932 Tel Aviv-Yafo (IL). GAL-BETZER, Erez; Max Veampro Shein 1, Apartment 3, 7666601 Rehovot (IL). FENSTER, Yaacov; 58 Brande Street, 4960326 Petach Tikvah (IL).

(74) Agent: HAUSMAN, Ehud; REINHOLD COHN AND PARTNERS, P.O. Box 13239, 6113102 Tel-Aviv (IL).

(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, 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, 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,

(54) Title: METHOD OF SECURE COMMUNICATION AMONG PROTECTED CONTAINERS AND SYSTEM THEREOF

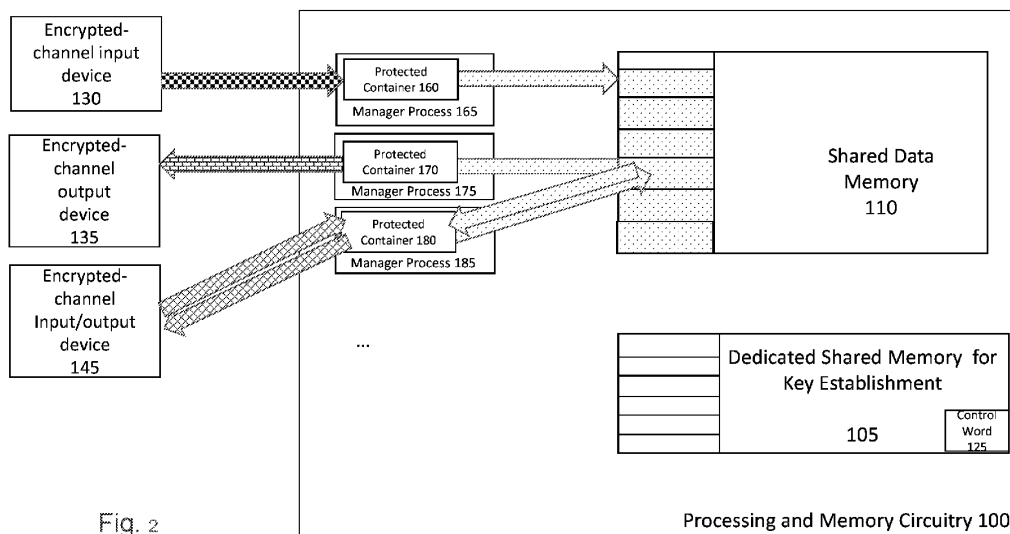


Fig. 2

(57) Abstract: There is provided a method of communication among at least two processes running on the same computer. The method comprises: generating, by at least one process of the at least two processes, a group key usable for encrypting/decrypting a data unit retrieved from/stored to shared access memory, wherein the generating utilizes, at least, a nonce provided by each of the at least two processes, and wherein the nonces are provided as encrypted integrity-protected data according to, at least, a platform-provided hiding function, wherein each process executes in a protected container, the processes are signed by a single signing authority, and the protected container infrastructure enables use of encrypted, integrity-protected data according to a platform-provided hiding function and a platform-provided revealing function; and verifying, by at least one process of the at least two processes, that a data unit read from shared access memory is successfully decrypted using the group key.

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) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, 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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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