



- (51) **International Patent Classification:**
G06F 21/00 (2013.01) *G06F 21/72* (2013.01)
- (21) **International Application Number:**
PCT/US2018/066019
- (22) **International Filing Date:**
17 December 2018 (17.12.2018)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
62/607,185 18 December 2017 (18.12.2017) US
- (71) **Applicants:** **UNIVERSITY OF CENTRAL FLORIDA RESEARCH FOUNDATION, INC.** [US/US]; 12201 Research Parkway, Suite 501, Orlando, FL 32826 (US). **TRUSTEES OF BOSTON UNIVERSITY** [US/US]; One Silber Way, Boston, MA 02215 (US).
- (72) **Inventors:** **MUCCIOLO, Eduardo**; 4365 Andromeda Loop N, Orlando, FL 32816 (US). **CHAMON, Claudio**; 135 Maple Street, Lexington, MA 02420 (US).
- (74) **Agent:** **VAN DYKE, Timothy, H.** et al.; Beusse, Wolter, Sanks & Maire, PLLC, 390 N. Orange Ave., Suite 2500, Orlando, FL 32801 (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, 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, 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).

(54) **Title:** TECHNIQUES FOR SECURELY EXECUTING CODE THAT OPERATES ON ENCRYPTED DATA ON A PUBLIC COMPUTER

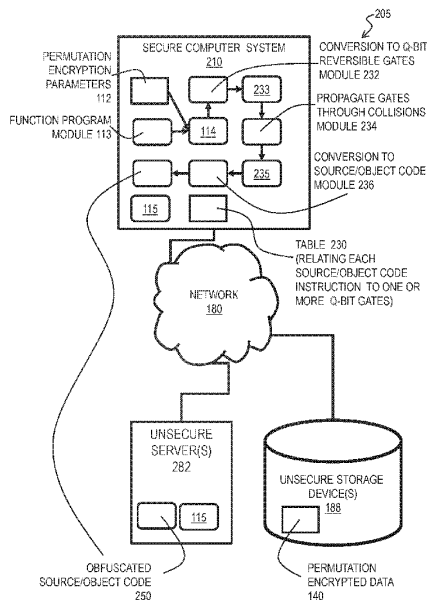


FIG. 2D

(57) **Abstract:** Techniques, for secure processing of encrypted data on public resources, include receiving first data indicating a sequence of reversible q -bit gates including a first segment for decrypting, a second segment for operating on the decrypted data, and a third segment for encrypting the resulting data. Second data indicates rules for replacing a first sequence of two gates operating on at least one shared bit of an input N -bit word with a different second sequence of one or more gates that produce the same output N -bit word. The second data is used to propagate: a gate from the first segment a distance into the second segment or beyond; and, a gate from the third segment a distance into the second segment or before. This produces an obfuscated sequence of reversible gates. Obfuscated instructions based on the obfuscated sequence of gates are sent to the public resources.

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))*