

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
20 August 2020 (20.08.2020)



(10) International Publication Number
WO 2020/165335 A1

- (51) International Patent Classification:
H04L 9/30 (2006.01)
- (21) International Application Number:
PCT/EP2020/053743
- (22) International Filing Date:
13 February 2020 (13.02.2020)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
16/276,689 15 February 2019 (15.02.2019) US
- (71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).
- (71) Applicant (for MG only): **IBM UNITED KINGDOM LIMITED** [GB/GB]; PO Box 41, North Harbour, Portsmouth Hampshire PO6 3AU (GB).
- (72) Inventors: **SCHWARZ, Eric, Mark**; IBM Corporation, 2455 South Road, Poughkeepsie, New York 12601-5400

(US). **BRADBURY, Jonathan**; IBM Corporation, 2455 South Road, Poughkeepsie, New York 12601-5400 (US). **MALLEY, Edward, Thomas**; IBM Corporation, 2455 South Road, Poughkeepsie, New York 12601-5400 (US). **JACOBI, Christian**; IBM Corporation, 2455 South Road, Poughkeepsie, New York 12601-5400 (US).

(74) Agent: **GRAHAM, Timothy**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester Hampshire SO21 2JN (GB).

(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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) Title: PERFORM CRYPTOGRAPHIC COMPUTATION SCALAR MULTIPLY INSTRUCTION

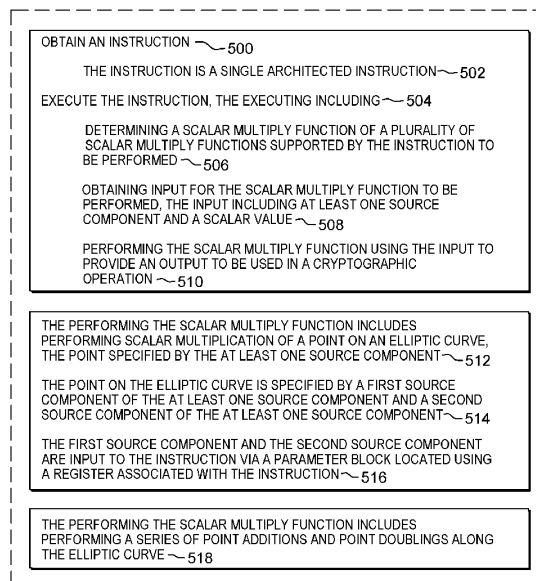


FIG. 5A

(57) Abstract: A single architected instruction to perform scalar multiplication for cryptographic operations is obtained. The instruction is executed, and the executing includes determining a scalar multiply function of a plurality of scalar multiply functions supported by the instruction to be performed. Input for the scalar multiply function is obtained, and the input includes at least one source component and a scalar value. The scalar multiply function is performed using the input to provide an output to be used in a cryptographic operation.

[Continued on next page]



WO 2020/165335 A1

(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).

Published:

- with international search report (Art. 21(3))
- with amended claims (Art. 19(1))