



(51) International Patent Classification:

H04L 9/32 (2006.01) **G06F 9/46** (2006.01)
G06F 9/38 (2018.01)

(21) International Application Number:

PCT/EP2025/067274

(22) International Filing Date:

19 June 2025 (19.06.2025)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

18/756,414 27 June 2024 (27.06.2024) 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]; Building C, IBM Hursley Office, Hursley Park Road, Winchester Hampshire SO21 2JN (GB).

(72) Inventors: **RAO, Rajat**; IBM INDIA PVT LIMITED, Block 3, Chokkanahalli Village, Thanisandra Main Road, Karnataka, Bangalore 560064 (IN). **BRADBURY, Jonathan**; IBM CORPORATION, 2455 South Road,

Poughkeepsie, New York 12601-5400 (US). **GOMES, Louis**; IBM CORPORATION, 2455 South Road, Poughkeepsie, New York 12601-5400 (US). **BUENDGEN, Reinhard, Theodor**; IBM Deutschland RD GmbH, Schoenaicher Street 220, BW 71032 Boeblingen (DE). **SANDEEP, Gunturi**; IBM CORPORATION, Intellectual Property Law, 1101 Kitchawan Road, Route 134, P.O. Box 218, Yorktown, New York 10598-0218 (US). **BHATTACHARJEE, Deepankar**; IBM INDIA PVT LIMITED, Block 3, Chokkanahalli Village, Thanisandra Main Road, Karnataka, Bangalore 560064 (IN).

(74) Agent: **PYECROFT, Justine**; IBM UNITED KINGDOM LIMITED, Intellectual Property Law, Hursley Park, Hursley, 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, 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,

(54) Title: INSTRUCTION TO ACCELERATE HASH-BASED MESSAGE AUTHENTICATION CODE PROCESSING

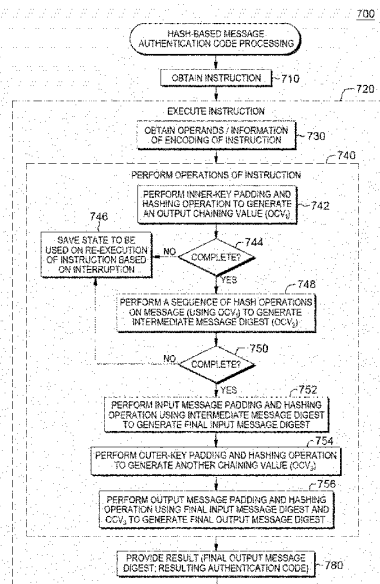


FIG. 7

(57) Abstract: An instruction is executed to generate an authentication code. Executing the instruction includes performing a plurality of operations of the instruction to generate the authentication code. The plurality of operations includes performing a sequence of hash operations on a message to generate an intermediate message digest, and performing an outer-key padding and hashing operation using the cryptographic key to generate another output chaining value to be used in generating a final output message digest based on a final input message digest produced using the intermediate message digest. The final output message digest being a resulting authentication code. The performing the sequence of hash operations and the outer-key padding and hashing operation are performed as part of a single invocation of the instruction.

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))
- in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE