

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
02 January 2026 (02.01.2026)



(10) International Publication Number
WO 2026/002791 A1

(51) International Patent Classification:
H04L 9/06 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/EP2025/067277

(22) International Filing Date:
19 June 2025 (19.06.2025)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
18/756,603 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). **SLEGEL, Timothy**; IBM CORPORATION, 2455 South Road, Poughkeepsie, New York 12601-5400 (US). **KILINÇ, Görkem**; IBM Deutschland Road GmbH, Schoenaicher Street 220, BW 71032 Boeblingen (DE). **GOMES, Louis**; IBM CORPORATION, 2455 SOUTH ROAD, POUGHKEEPSIE, New York 12601-5400 (US).

(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, 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

(54) Title: INSTRUCTION TO ACCELERATE HASH PROCESSING

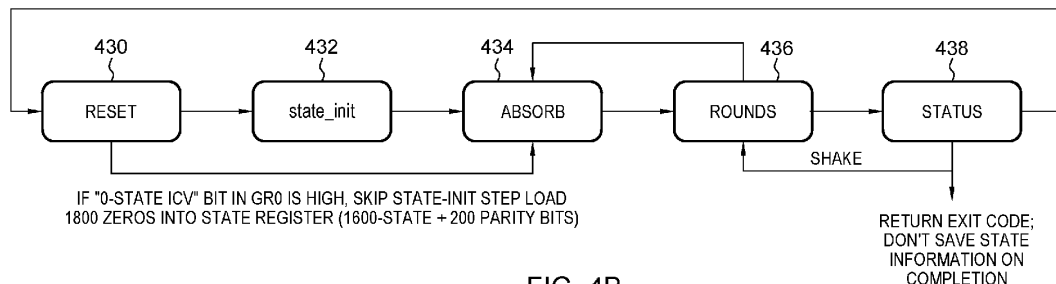


FIG. 4B

(57) Abstract: An instruction is executed to generate a message digest for a message. The message digest is to be used in authentication of the message. Executing the instruction includes obtaining from the instruction a control indicator and determining, based on the control indicator, an initial chaining value to be used to generate the message digest. The message digest is generated using the initial chaining value and the message digest is provided to be used in the authentication of the message.

WO 2026/002791 A1