

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
26 December 2025 (26.12.2025)



(10) International Publication Number
WO 2025/261643 A1

(51) International Patent Classification:

G06F 21/60 (2013.01) G06F 21/78 (2013.01)
G06F 21/62 (2013.01) H04L 9/06 (2006.01)
G06F 21/72 (2013.01)

(21) International Application Number:

PCT/EP2025/061493

(22) International Filing Date:

28 April 2025 (28.04.2025)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

18/749,865 21 June 2024 (21.06.2024) US
18/749,928 21 June 2024 (21.06.2024) US

(71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).

(71) Applicant (for MG only): **IBM DEUTSCHLAND GMBH** [DE/DE]; Schönaicher Str. 220, 71032 Böblingen (DE).

(72) Inventors: **RAO, Rajat**; c/o IBM India Pvt Ltd, Outer Ring Road, Embassy Manyatha B B119, 1F, Building MD3, Bangalore 560045 (IN). **BRADBURY, Jonathan**; c/o IBM Corp., 2455 South Road, Poughkeepsie, New York 12601 (US). **GOMES, Louis**; c/o IBM Corp., 2455 South Road, Poughkeepsie, New York 12601 (US). **BUENDGEN, Reinhard**; c/o IBM Deutschland Research & Development GmbH, Schoenaicher Strasse 220, 71032 Boeblingen (DE). **S R, Soujanya**; c/o IBM India Pvt Ltd, Block 3, Chokkanahalli Village, Thanisandra Main Road, Bangalore 560064 (IN).

(74) Agent: **HAEMMERLING, Jens**; c/o IBM Deutschland GmbH, Patentwesen und Urheberrecht, Schönaicher Str. 220, 71032 Böblingen (DE).

(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,

(54) Title: INSTRUCTION TO ACCELERATE CRYPTOGRAPHIC PROCESSING

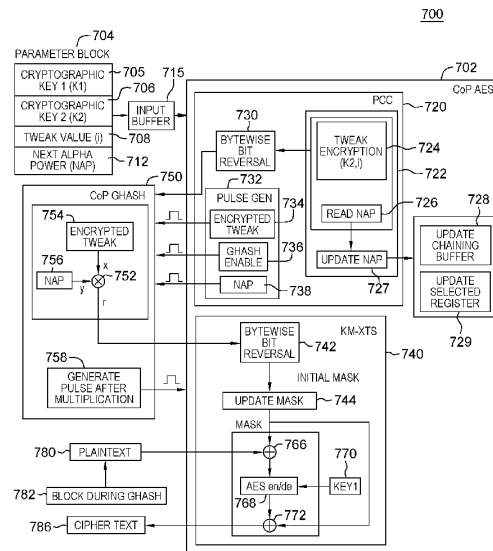


FIG. 7

(57) Abstract: A cipher instruction is executed. The executing the cipher instruction includes encrypting a confidential value to provide an encrypted confidential value and generating a mask value using the encrypted confidential value. A cipher operation is performed on at least a portion of a message specified by the cipher instruction. The performing the cipher operation on the at least the portion of the message uses the mask value. A result of the cipher operation is provided.

[Continued on next page]

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))*