

(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 2025/261644 A1

(51) International Patent Classification:

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

(21) International Application Number:

PCT/EP2025/061500

(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, Out-
er 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).
URBAN, Volker; c/o IBM Deutschland Research & Devel-
opment GmbH, Schoenaicher Strasse 220, 71032 Boeblin-
gen (DE).

(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,
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,

(54) Title: PROTECTION OF CRYPTOGRAPHIC PARAMETERS USED IN CRYPTOGRAPHIC PROCESSING

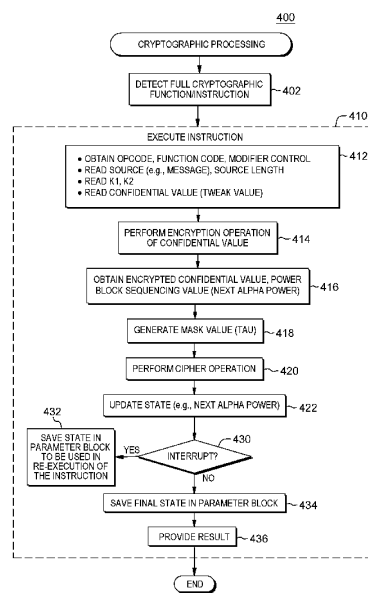


FIG. 4A

(57) Abstract: A cipher instruction is executed that includes encrypting a confidential value. A power block sequencing value is obtained as input to the cipher instruction, and a mask value is generated using the encrypted confidential value and the power block sequencing value. A cipher operation is performed on at least a portion of a message specified by the cipher instruction using the mask value. The power block sequencing value is updated, based on performing the cipher operation of the at least the portion of the message, to provide an updated power block sequencing value to be used in re-execution of the cipher instruction based on the cipher instruction being interrupted. The updated power block sequencing value is to be provided as input to the cipher instruction based on the cipher instruction being re-executed to re-generate the mask value to be used in continuing the cipher operation of the message.

WO 2025/261644 A1

[Continued on next page]

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))