

(51) International Patent Classification:
H04L 29/06 (2006.01)(21) International Application Number:
PCT/IB2021/051287(22) International Filing Date:
16 February 2021 (16.02.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/801,319 26 February 2020 (26.02.2020) US(71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York, 10504 (US).(71) Applicants (for MG only): **IBM UNITED KINGDOM LIMITED** [GB/GB]; PO Box 41, North Harbour, Portsmouth Hampshire PO6 3AU (GB). **IBM (CHINA) INVESTMENT COMPANY LIMITED** [CN/CN]; 25/F, Pangu Plaza, No. 27, Central North 4th Ring Road, Chaoyang District, Beijing 100101 (CN).(72) Inventors: **ZEE, Mooheng**; IBM Corporation, 2455 South Road, Poughkeepsie, New York 12601-5400 (US). **SCZEP CZENSKI, Richard, Mark**; IBM Corporation,2455 South Road, Poughkeepsie, New York 12601-5400 (US). **FLANAGAN, John**; IBM Corporation, C/o Intellectual Property Law, 2455 South Road, Poughkeepsie, New York 12601-5400 (US). **COLONNA, Christopher**; IBM Corporation, 2455 South Road, Poughkeepsie, New York 12601-5400 (US).(74) Agent: **LITHERLAND, David**; 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, 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, IT, 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.

(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,

(54) Title: SECURE KEY EXCHANGE IN A COMPUTING ENVIRONMENT

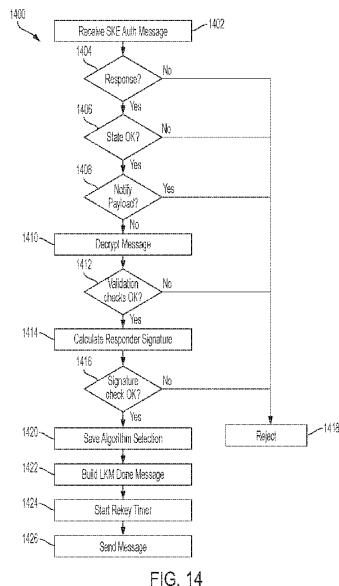


FIG. 14

(57) Abstract: A computer-implemented method includes receiving an authentication response message at an initiator channel on an initiator node from a responder channel on a responder node to establish a secure communication, the receiving at a local key manager (LKM) executing on the initiator node. A state check is performed based on a security association of the initiator node and the responder node. A validation of the authentication response message is performed. An identifier of a selected encryption algorithm is extracted from the authentication response message. The initiator channel requests to communicate with the responder channel based at least in part on a successful state check, a successful validation, and the selected encryption algorithm.

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))*