



(51) International Patent Classification:
H04L 9/16 (2006.01)

(21) International Application Number:
PCT/IB2021/061161

(22) International Filing Date:
01 December 2021 (01.12.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
17/121,170 14 December 2020 (14.12.2020) US

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

(71) Applicants (for MG only): **IBM ISRAEL SCIENCE AND TECHNOLOGY LTD.** [IL/IL]; Haifa University Campus, 165 Aba Khoushy Ave, Mount Carmel, 3498825 Haifa (IL). **IBM (CHINA) INVESTMENT COMPANY LTD.** [CN/CN]; 25/F, Pangu Plaza, No. 27, Central North 4th Ring Road, Chaoyang District, Beijing 100101 (CN).

(72) Inventors: **GIBLIN, Christopher**; IBM RESEARCH GMBH, SAEUMERSTRASSE 4, RUESCHLIKON, 8803 Zurich (CH). **ROONEY, John**; IBM RESEARCH GMBH, SAEUMERSTRASSE 4, RUESCHLIKON, 8803 Zurich (CH). **FROESE, Florian**; IBM RESEARCH GMBH, SAEUMERSTRASSE 4, RUESCHLIKON, 8803 Zurich (CH). **VETSCH, Pascal**; IBM RESEARCH GMBH, SAEUMERSTRASSE 4, RUESCHLIKON, 8803 Zurich (CH).

(74) Agent: **GILBOA, Eyal**; IBM ISRAEL SCIENCE AND TECHNOLOGY LTD., Haifa University Campus, 165 Aba Khoushy Ave, Mount Carmel, 3498825 Haifa (IL).

(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,

(54) Title: KEY ROTATION ON PUBLISH-SUBSCRIBE SYSTEM

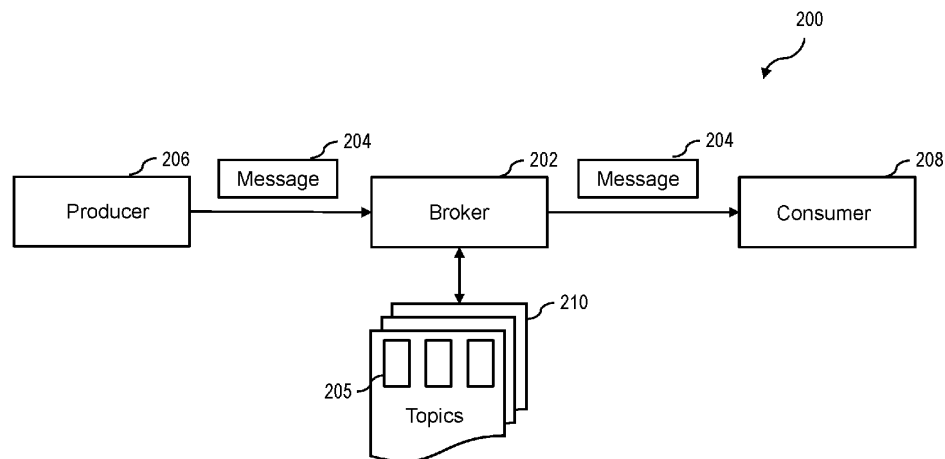


FIG. 2

(57) Abstract: A method for a cryptographic key rotation in a publish-subscribe system providing a broker (202) service for routing stored encrypted messages (204) to one or more subscribers of the topic (201) to which the routed messages(204) are assigned. The routing comprises decrypting the stored encrypted messages (204). The cryptographic key rotation comprises a re-encryption of the stored messages (204) using a cryptographic replacement key. The re-encryption is executed by an encryption module of the publish-subscribe system as a background process, while the broker (202) service is continued.

[Continued on next page]

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, 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))