

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
23 July 2020 (23.07.2020)



(10) International Publication Number
WO 2020/149913 A2

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

(21) International Application Number:
PCT/US2019/058205

(22) International Filing Date:
25 October 2019 (25.10.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/751,068 26 October 2018 (26.10.2018) US

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).

(72) Inventors: **LUYKX, Atul**; 165 Peralta Avenue, Unit 2, San Francisco, California 94110 (US). **DAI, Wei**; c/o Visa International Service Association, P.O. Box 8999, San Francisco, California 94128 (US).

(74) Agent: **JEWIK, Patrick** et al.; Kilpatrick Townsend & Stockton LLP, Mailstop: IP Docketing – 22, 1100 Peachtree Street, Suite 2800, Atlanta, Georgia 30309 (US).

(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, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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).

Declarations under Rule 4.17:

— as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

Published:

— without international search report and to be republished upon receipt of that report (Rule 48.2(g))

(54) Title: COMPUTING KEY ROTATION PERIOD FOR BLOCK CIPHER-BASED ENCRYPTION SCHEMES SYSTEM AND METHOD

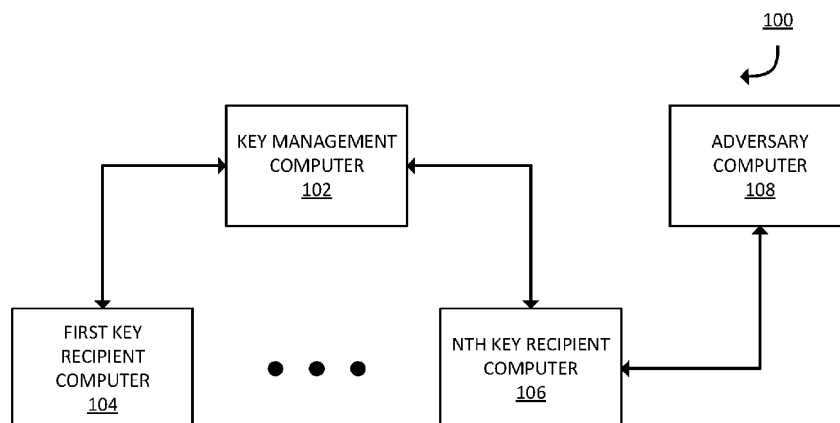


FIG. 1

(57) Abstract: A method including obtaining, by a key management computer, a key rotation period based on at least an adversarial storage limit. The key management computer can then generate a first cryptographic key. The key management computer can then generate a second cryptographic key to replace the first cryptographic key according to the key rotation period.



WO 2020/149913 A2