

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
09 April 2020 (09.04.2020)



(10) International Publication Number
WO 2020/072476 A1

(51) International Patent Classification:

G06F 9/00 (2018.01) H04W 12/06 (2009.01)
H04L 9/32 (2006.01)

Grove, IL 60047 (US). **PRINCE, Ian**; 6 The Lodge, Glade Mews, Guilford, Surrey GU1 2EZ (GB). **LUTZ, Wayne**; 902 Lira Drive, Fort Washington, MD 20744 (US).

(21) International Application Number:

PCT/US2019/054039

(74) Agent: **KASNEVICH, Andrew, D.** et al.; Hunton Andrews Kurth LLP, 2200 Pennsylvania Ave, NW, Washington, DC 20037 (US).

(22) International Filing Date:

01 October 2019 (01.10.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/740,352 02 October 2018 (02.10.2018) US
16/205,119 29 November 2018 (29.11.2018) US

(71) Applicant: **CAPITAL ONE SERVICES, LLC** [US/US];
1680 Capital One Drive, Mclean, VA 22102 (US).

(72) Inventors: **OSBORN, Kevin**; 49 Hillside Road, Newton Highlands, MA 02461 (US). **RULE, Jeffrey**; 3906 Laird Place, Chevy Chase, MD 20815 (US). **MORETON, Paul**; 11916 Brookmeade Court, Glen Allen, VA 23059 (US). **DUANE, William**; 4 Howard Road, Westford, MA 01886 (US). **HART, Colin**; 2604 S Adams Street, Arlington, VA 22206 (US). **NEWMAN, Kaitlin**; 1717 Lamont Street NW, Washington, DC 20010 (US). **MOSSLER, Lara**; 113 Appomattox Street, Farmville, VA 23901 (US). **HERRINGTON, Daniel**; 8 Spruce Street, #48D, New York, NY 10038 (US). **CHIGURUPATI, Srinivasa**; 5804 Teal Court, Long

(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).

(54) Title: SYSTEMS AND METHODS FOR CRYPTOGRAPHIC AUTHENTICATION OF CONTACTLESS CARDS

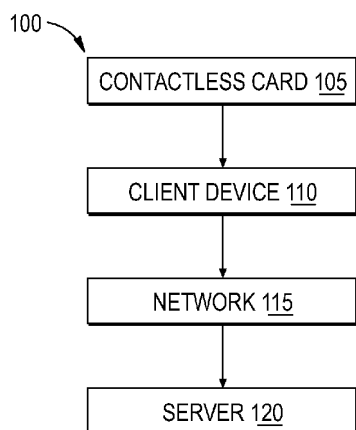


FIG. 1A

(57) Abstract: Example embodiments of systems and methods for data transmission between transmitting and receiving devices are provided. In an embodiment, a method comprises generating a card key using the master key and the identification number, generating a first session key using the card key and a first portion of the counter and a second session key using the card key and a second portion of the counter, generating a cryptographic result including the counter using one or more cryptographic algorithms and the card key, generating a cryptogram using the first session key, the cryptogram including the cryptographic result and the identification number, encrypting the cryptogram using the second session key, and transmitting the encrypted cryptogram and the cryptographic result.

[Continued on next page]

Published:

— with international search report (Art. 21(3))