



(51) International Patent Classification:

G06Q 20/38 (2012.01) G06Q 20/34 (2012.01)
G06Q 20/32 (2012.01) G06Q 20/36 (2012.01)

(21) International Application Number:

PCT/US2022/050885

(22) International Filing Date:

23 November 2022 (23.11.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

17/551,670 15 December 2021 (15.12.2021) US

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

(72) Inventors: **OSBORN, Kevin**; c/o Capital One Services,
LLC, 1680 Capital One Drive, McLean, Virginia 22102
(US). **PRASAD, Jaikishan**; c/o Capital One Services, LLC,

1680 Capital One Drive, McLean, Virginia 22102 (US).
CATALA CASTELLAR, Jose; c/o Capital One Services,
LLC, 1680 Capital One Drive, McLean, Virginia 22102
(US).

(74) Agent: **CARR, Nick et al.**; KDB Firm PLLC, 2601 Weston
Parkway, Suite 103, Cary, North Carolina 27513 (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, 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, 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.

(54) Title: KEY RECOVERY BASED ON CONTACTLESS CARD AUTHENTICATION

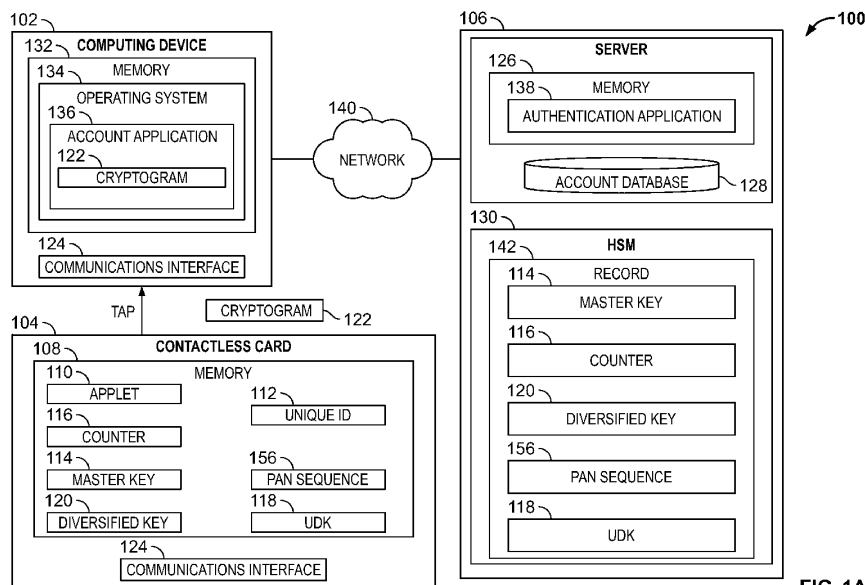


FIG. 1A

(57) Abstract: Systems, methods, apparatuses, and computer-readable media for key recovery based on contactless card cryptograms. A server may receive, from an application, a request to recover a private key for a digital wallet, the request includes a first cryptogram generated by a contactless card. The server may decrypt the first cryptogram based on a key for the contactless card. The server may determine, based on the decryption, a unique identifier of the contactless card and a diversification factor associated with the digital wallet. The server may generate the private key based on the unique identifier and the diversification factor. The server may transmit the private key to the application via a network.

[Continued on next page]

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, CV, 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, 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))