



(51) International Patent Classification:

H04L 9/30 (2006.01) *H04L 9/06* (2006.01)
H04L 9/08 (2006.01)

(21) International Application Number:

PCT/US2022/027514

(22) International Filing Date:

03 May 2022 (03.05.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/183,565 03 May 2021 (03.05.2021) US

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

(72) Inventors: **WATSON, Gaven**; P.O. Box 8999, San Francisco, California 94128 (US). **MASNY, Daniel**; P.O. Box 8999, San Francisco, California 94128 (US).

(74) Agent: **RACZKOWSKI, David B.** et al.; Kilpatrick, Townsend & Stockton LLP, 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, IQ, IR, IS, IT, JM, 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, 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: OBLIVIOUS TRANSFER FROM KEY ENCAPSULATION MECHANISMS

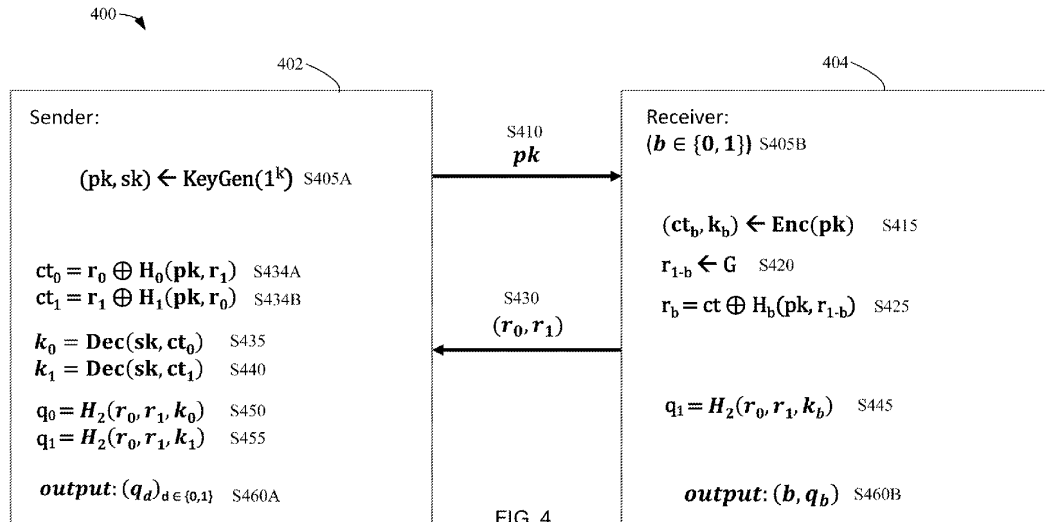


FIG. 4

(57) **Abstract:** Embodiments can perform efficient OT (oblivious transfer) protocols to efficiently establish OT correlations that could be used for an MPC protocol. The present embodiments relate to a non-interactive OT (NIOT) protocol using a key encapsulation mechanism (KEM). Two OT protocols are non-interactive OTs, in which a sender generates private, public key pair (pk, sk) that is independent of its input or generated OT correlations. The two OT protocols use a cryptographic hash function and a one-way secure dense key encapsulation mechanism (KEM).

[Continued on next page]

Declarations under Rule 4.17:

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

Published:

- *with international search report (Art. 21(3))*