



(51) International Patent Classification:
H04L 9/14 (2006.01) *H04L 9/08* (2006.01)
H04L 9/30 (2006.01)

(21) International Application Number:
PCT/US2023/064655

(22) International Filing Date:
17 March 2023 (17.03.2023)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/322,091 21 March 2022 (21.03.2022) US

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; PO BOX 8999, San Francisco, CA 94128 (US).

(72) Inventors: **BADRINARAYANAN, Saikrishna**; PO BOX 8999, San Francisco, CA 94128 (US). **MUKHERJEE, Pratyay**; PO BOX 8999, San Francisco, CA 94128 (US). **PATRANABIS, Sikhar**; PO BOX 8999, San Francisco, CA 94128 (US).

(74) Agent: **RACZKOWSKI, David, B.** et al.; Kilpatrick, Townsend & Stockton LLP, 1100 Peachtree Street Suite 2800, Atlanta, GA 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, 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, MU, 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,

(54) Title: THRESHOLD SEARCHABLE SYMMETRIC ENCRYPTION



WO 2023/183760 A1

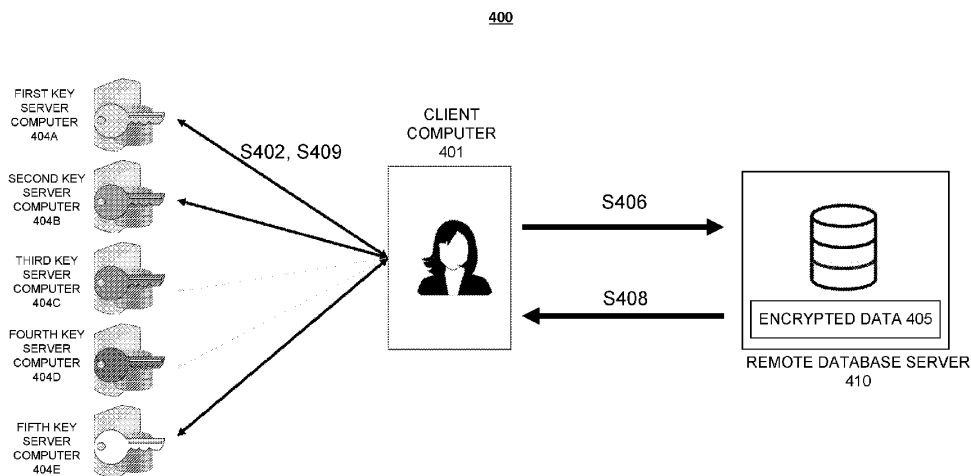


FIG. 4

(57) Abstract: A data owner can provide shares of a cryptographic key to N key servers. The N key servers can store the shares of a cryptographic key from the data owner such that T shares of the cryptographic key can be used to reconstruct the cryptographic key. A client computer can send a blinded query to T key servers of the N key servers, wherein the T key servers can encrypt a blinded query of a client computer using the share of the cryptographic key to determine a partial encryption. The client computer can receive T partial encryptions, assemble T partial encryptions to form an encrypted blinded query, and deblind the encrypted blinded query. The client computer can then use the encrypted query to perform a search on encrypted data of a remote database server using a searchable symmetric encryption scheme.

[Continued on next page]

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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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).

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))*