

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
05 October 2023 (05.10.2023)



(10) International Publication Number
WO 2023/192071 A1

- (51) International Patent Classification:
H04L 9/40 (2022.01) *H04L 9/06* (2006.01)
- (21) International Application Number:
PCT/US2023/015815
- (22) International Filing Date:
21 March 2023 (21.03.2023)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
63/324,498 28 March 2022 (28.03.2022) US
- (71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).
- (72) Inventors: **BADRINARAYANAN, Saikrishna**; P.O. Box 8999, San Francisco, California 94128 (US). **DAS, Sourav**; P.O. Box 8999, San Francisco, California 94128 (US). **GARIMELLA, Gayathri Annapurna**; P.O. Box 8999,

San Francisco, California 94128 (US). **RAGHURAMAN, Srinivasan**; P.O. Box 8999, San Francisco, California 94128 (US). **RINDAL, Peter Byerley**; P.O. Box 8999, San Francisco, California 94128 (US).

(74) Agent: **CRETSINGER, Cathy E.** et al.; 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, 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, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) Title: PRIVATE-SET INTERSECTION OF UNBALANCED DATASETS

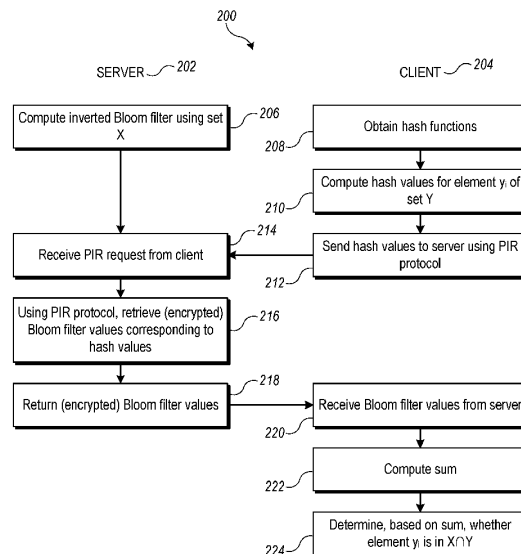


FIG. 2

(57) Abstract: Private set intersection (PSI) protocols can be efficiently performed for sets of disparate sizes. A server can compute an array, such as an inverted Bloom filter or cuckoo hash table, that represents the content of the server set. A client can query the array, e.g., using a private information retrieval (PIR) protocol, to obtain information that enables the client to determine whether a particular element of the client's set is also in the server's set. By repeating the query for each element of the client's set, the client can learn the intersection.

[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, 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))*