

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
01 December 2022 (01.12.2022)



(10) International Publication Number
WO 2022/251341 A1

(51) International Patent Classification:

H04L 9/08 (2006.01) *G06F 7/58* (2006.01)
G06F 21/62 (2013.01) *G06N 20/00* (2019.01)
G06F 21/60 (2013.01)

(21) International Application Number:

PCT/US2022/030896

(22) International Filing Date:

25 May 2022 (25.05.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/192,933 25 May 2021 (25.05.2021) US

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

(72) Inventors: **BADRINARAYANAN, Saikrishna**; PO BOX 8999, San Francisco, California 94128 (US). **RINDAL, Peter**; PO BOX 8999, San Francisco, California 94128 (US). **MIAO, Peihan**; PO BOX 8999, San Francisco, California 94128 (US).

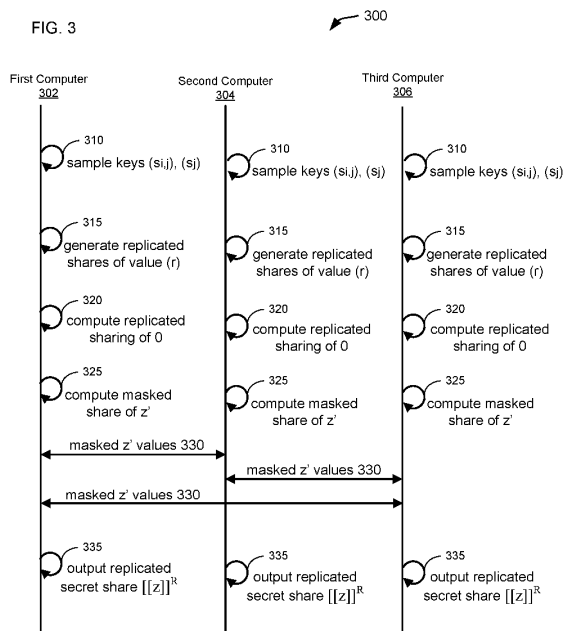
(74) Agent: **RACZKOWSKI, David B.** et al.; Kilpatrick, Townsend & Stockton LLP, 1100 Peachtree Street Suite 2800, Atlanta, Georgia 30309 (US).

(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: MULTI-PARTY COMPUTATION FOR MANY COMPUTERS

FIG. 3



(57) Abstract: Embodiments of the present disclosure are directed to methods for multi-party fixed point multiplication. The methods can include replicated methods for multi-party fixed point multiplication where the inputs and output are represented using replicated secret sharing. One replication method can require only a single round of communication in the online phase and is secure against a semi-honest adversary. Another replication method can require may include an additional key to identify any malicious communicating parties. The methods can also include a Shamir sharing fixed point multiplication method and an additive secret sharing fixed point multiplication method.

[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))*