



(51) International Patent Classification:

G06F 7/60 (2006.01) H04L 9/00 (2022.01)
G06F 7/38 (2006.01) H04L 9/14 (2006.01)
G06F 15/16 (2006.01) G06F 21/60 (2013.01)

(21) International Application Number:

PCT/US2024/033316

(22) International Filing Date:

10 June 2024 (10.06.2024)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/471,940 08 June 2023 (08.06.2023) US

(71) Applicant: ALGEMETRIC, INC. [US/US]; 5555 Tech Center Dr #100, Colorado Springs, Colorado 80919 (US).

(72) Inventors: HONORIO ARAUJO DA SILVA, David W.; 7860 Interlaken Drive, Colorado Springs, Colorado 80920 (US). HARMON, Luke E.; 1709 Sherman Street, Colorado Springs, Colorado 80909 (US). DELAVIGNETTE, Gaetan; 3603 Leeds Lane, Colorado Springs, Colorado 80907 (US).

(74) Agent: COCHRAN, William et al.; 2026 Caribou Drive, #201, Fort Collins, Colorado 80525 (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.

(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).

(54) Title: METHODS AND SYSTEMS FOR ADDITION, MULTIPLICATION, SUBTRACTION, AND DIVISION OF RATIONAL NUMBERS ENCODED IN THE DOMAIN OF FAREY RATIONALS FOR MPC SYSTEMS

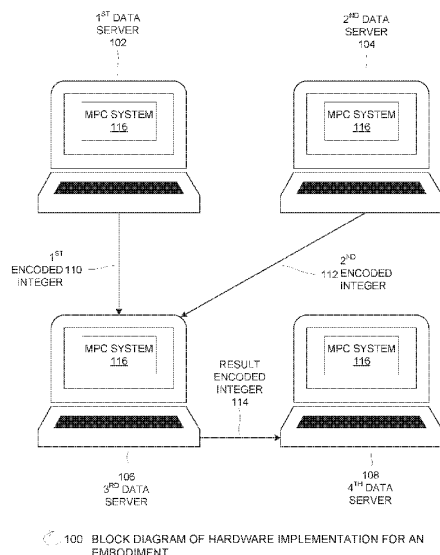


FIG. 1

(57) Abstract: Disclosed are methods and systems to provide encoding and decoding using of p-adic arithmetic, and inverse p-adic arithmetic, in the domain of Farey rationals that is induced by a ring isomorphism, such that said encoded integers preserve inverses, and additive and multiplicative homomorphic properties. This encoding permits MPC systems to perform arithmetic more efficiently and accurately, particularly for division.

Published:

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

(88) Date of publication of the international search report:

13 February 2025 (13.02.2025)