



(51) International Patent Classification:

H04L 9/00 (2006.01) *G06F 21/62* (2013.01)
H04L 9/28 (2006.01)

(21) International Application Number:

PCT/SG2021/050131

(22) International Filing Date:

12 March 2021 (12.03.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: **AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH** [SG/SG]; 1 Fusionopolis Way, #20-10 Connexis North Tower, Singapore 138632 (SG).

(72) Inventors: **TAN, Hong Meng Benjamin**; c/o Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis South Tower, Singapore 138632 (SG). **YEO, Sze Ling**; c/o Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis South Tower, Singapore 138632 (SG).

AUNG, Khin Mi Mi; c/o Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis South Tower, Singapore 138632 (SG).

(74) Agent: **VIERING, JENTSCHURA & PARTNER LLP**; P.O. Box 1088, Rochor Post Office, Rochor Road, Singapore 911833 (SG).

(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, IR, IS, IT, 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.

(54) Title: ENCODING DATA FOR HOMOMORPHIC COMPUTATION AND PERFORMING HOMOMORPHIC COMPUTATION ON ENCODED DATA

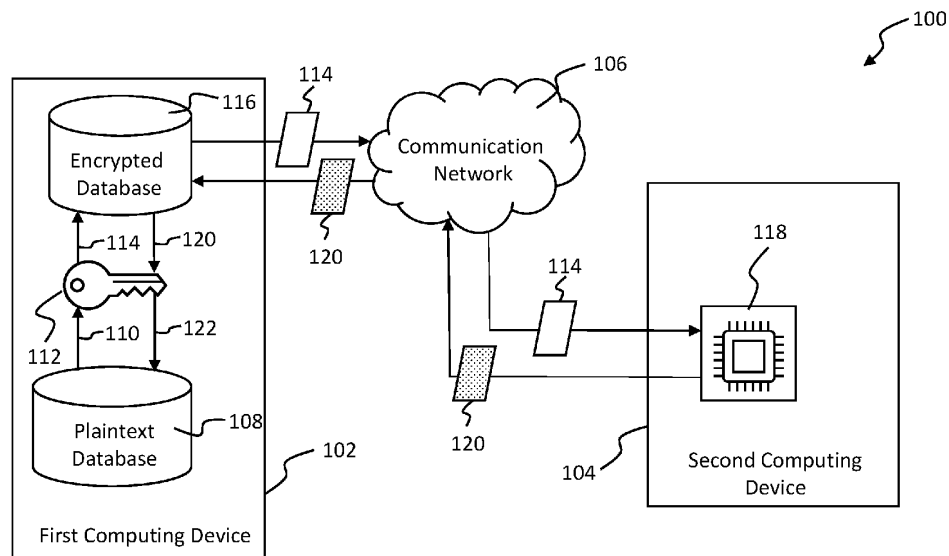


FIG. 1

(57) Abstract: In some aspects, a method for generating encoded plaintext data in a plaintext vector space includes obtaining a plurality of vectors of plaintext elements, where each plaintext element is an element of a first finite field. The method further includes encoding the plurality of vectors of plaintext elements to a vector of field elements, where each vector of plaintext elements is encoded to a respective field element of the vector of field elements, each of the field elements is an element of a second finite field, and the second finite field is a finite extension field of the first finite field. The method additionally includes encoding the vector of field elements into an element of the plaintext vector space to produce the encoded plaintext data for homomorphic encryption and computation.

[Continued on next page]

(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).

Published:

- *with international search report (Art. 21(3))*
- *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*