



(51) International Patent Classification:

G06N 20/00 (2019.01) G06N 99/00 (2019.01)
H04L 9/00 (2006.01) G06N 3/02 (2006.01)

(21) International Application Number:

PCT/SG2021/050015

(22) International Filing Date:

08 January 2021 (08.01.2021)

(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: **JIN, Chao**; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis South

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

(54) Title: METHOD AND SYSTEM FOR PRIVACY-PRESERVING LOGISTIC REGRESSION TRAINING BASED ON HOMOMORPHICALLY ENCRYPTED CIPHERTEXTS

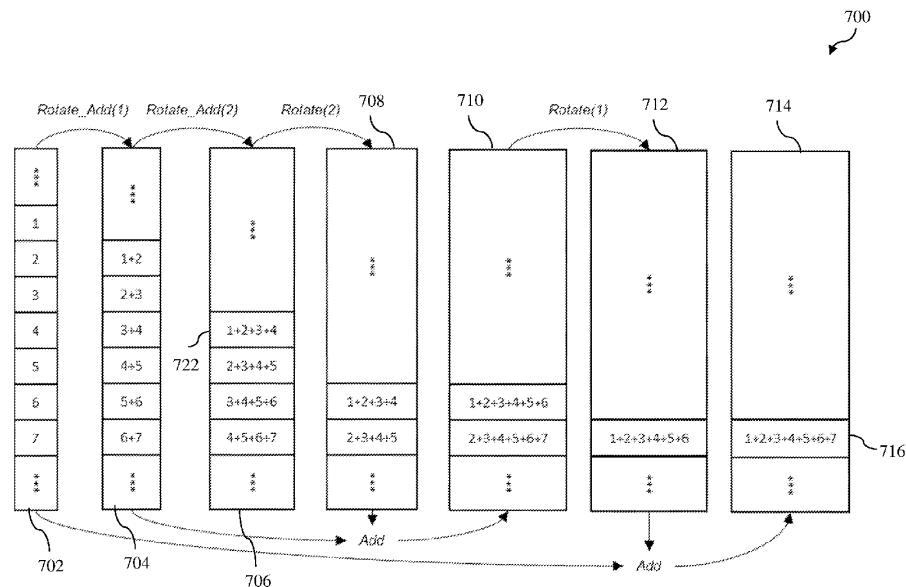


FIG. 7

(57) Abstract: There is provided a method of privacy-preserving logistic regression training based on homomorphically encrypted ciphertexts. The method includes: obtaining a first packed ciphertext comprising at least a portion of a first training data sample packed into a first vector of slots thereof for training a privacy-preserving logistic regression model; obtaining a second packed ciphertext comprising a plurality of weights of the privacy-preserving logistic regression model packed into a first vector of slots thereof; determining at least a first output probability of the privacy-preserving logistic regression model based on the first packed ciphertext and the second packed ciphertext; and updating the plurality of weights based on the first output probability. There is also provided a corresponding system for privacy-preserving logistic regression training based on homomorphically encrypted data.

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).

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*
-