

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
31 August 2023 (31.08.2023)



(10) International Publication Number
WO 2023/163652 A3

(51) International Patent Classification:

H04L 41/14 (2022.01) *H04L 9/00* (2022.01)
G06F 21/60 (2013.01) *H04W 12/02* (2009.01)
G06N 3/02 (2006.01)

(21) International Application Number:

PCT/SG2023/050085

(22) International Filing Date:

15 February 2023 (15.02.2023)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

10202201824W	24 February 2022 (24.02.2022)	SG
10202205037W	13 May 2022 (13.05.2022)	SG

(71) Applicant: **NANYANG TECHNOLOGICAL UNIVERSITY** [SG/SG]; 50 Nanyang Avenue, Singapore 639798 (SG).

(72) Inventors: **LAM, Kwok Yan**; c/o Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798 (SG). **WANG, Huaxiong**; c/o Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798 (SG). **LU, Xi-anhui**; c/o Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798 (SG). **ZHANG, Linru**; c/o Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798 (SG). **WANG, Xiangning**; c/o Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798 (SG).

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

(54) Title: PRIVACY-PRESERVING NEURAL NETWORK MODEL AND PRIVACY-PRESERVING PREDICTION USING THE PRIVACY-PRESERVING NEURAL NETWORK MODEL

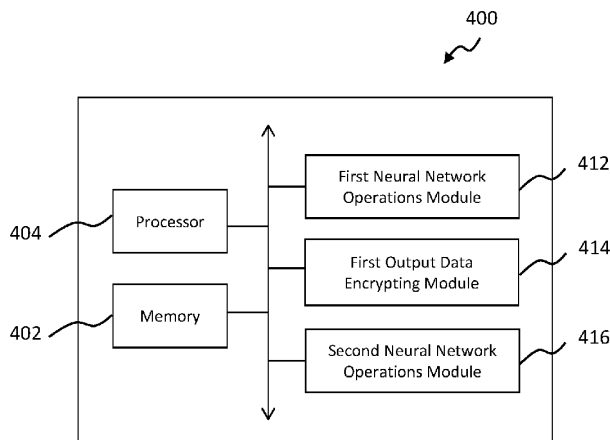


FIG. 4

(57) Abstract: A method of building a privacy-preserving neural network model is provided. The method includes: performing first neural network operations using a non-private neural network of the privacy-preserving neural network model based on first input data in plaintext to produce first output data in plaintext, whereby the non-private neural network is pre-trained and learnable parameters of the non-private neural network are fixed while performing the first neural network operations; encrypting the first output data from the non-private neural network using a homomorphic encryption method to produce first encrypted data; and performing second neural network operations homomorphically using a private neural network of the privacy-preserving neural network model based on the first encrypted data to produce second encrypted data, whereby learnable parameters of the private neural network are trained while performing the second neural network operations. There is also provided a corresponding system for building a privacy-preserving neural network model, as well as method and system for performing privacy-preserving prediction using the privacy-preserving neural network model built.

[Continued on next page]

(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, 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).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

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

05 October 2023 (05.10.2023)