



- (51) **International Patent Classification:**
H04L 9/06 (2006.01) *G06F 21/64* (2013.01)
- (21) **International Application Number:**
PCT/SG2020/050073
- (22) **International Filing Date:**
13 February 2020 (13.02.2020)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
10201901244X 13 February 2019 (13.02.2019) SG
- (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 Connex-

is 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, 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,

(54) **Title:** METHOD AND SYSTEM FOR DETERMINING AN ORDER OF ENCRYPTED INPUTS

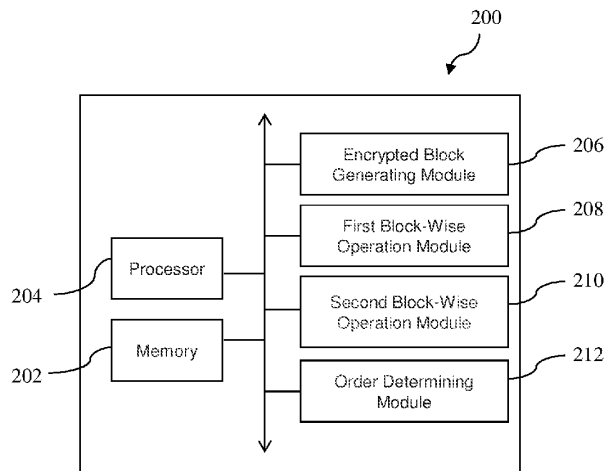


FIG. 2

(57) **Abstract:** There is provided a method of determining an order of encrypted inputs, including a first encrypted input and a second encrypted input, using at least one processor, the first encrypted input including a first encrypted data and the second encrypted input including a second encrypted data, each of the first and second encrypted data being encrypted based on a homomorphic encryption scheme, the method including: generating a first series of encrypted blocks from the first encrypted data and a second series of encrypted blocks from the second encrypted data; performing a first block-wise operation between the first series of encrypted blocks and the second series of encrypted blocks to obtain a first series of block-wise outputs; performing a second block-wise operation between the first series of encrypted blocks and the second series of encrypted blocks to obtain a second series of block-wise outputs; and determining an order of the first and second encrypted data based on the first series of block-wise outputs and the second series of block-wise outputs. There is also provided a corresponding system for determining an order of encrypted inputs.

[Continued on next page]

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))*
- *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))*
- *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*