



- (51) **International Patent Classification:**
G06F 17/10 (2006.01) *G06F 21/64* (2013.01)
G06F 9/38 (2018.01)
- (21) **International Application Number:**
PCT/SG2021/050723
- (22) **International Filing Date:**
24 November 2021 (24.11.2021)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
10202011663Q 24 November 2020 (24.11.2020) SG
- (71) **Applicant: AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH** [SG/SG]; 1 Fusionopolis Way, #20-10 Connexis North Tower, Singapore 138632 (SG).
- (72) **Inventors: YANG, Hong;** c/o Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis South Tower, Singapore 138632 (SG). **KANG, Dee Meng;** c/o Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis South Tower, Singapore 138632 (SG). **AL BADAWI, Ahmad Qaisar Ahmad;** 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,

(54) **Title:** DEVICE FOR PROCESSING HOMOMORPHICALLY ENCRYPTED DATA

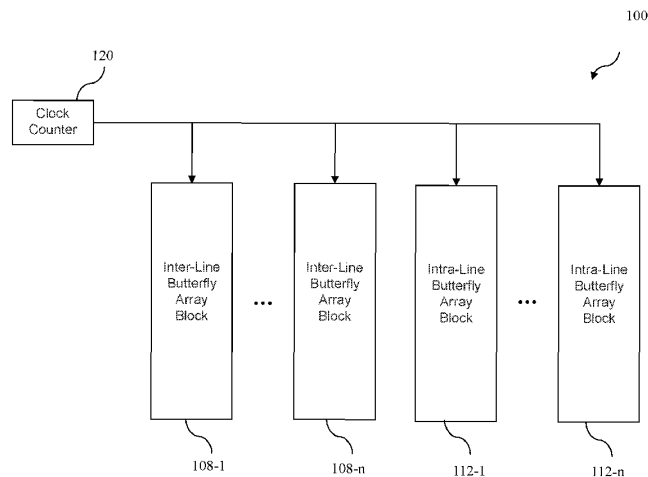


FIG. 1

(57) **Abstract:** There is provided a device for processing homomorphically encrypted data. The device includes: inter-line butterfly array blocks, each inter-line butterfly array block including inter-line modulus butterfly units, each inter-line modulus butterfly unit being configured to perform a modulus butterfly operation based on a computation pair of data points received corresponding to a pair of input data points at a same row of a matrix of input data points; intra-line butterfly array blocks, each intra-line butterfly array block including intra-line modulus butterfly units, each intra-line modulus butterfly unit being configured to perform a modulus butterfly operation based on a computation pair of data points received corresponding to a pair of input data points at a same column of the matrix of input data points; and a clock counter communicatively coupled to each inter-line butterfly array block and each intra-line butterfly array block, and configured to output a counter signal for controlling each inter-line butterfly array block and each intra-line butterfly array block to operate with single cycle initiation interval. The matrix of input data points includes columns of input data points, whereby parallel input data points derived from the homomorphically encrypted data are arranged into the columns of input data points. Furthermore, the inter-line butterfly array blocks and the intra-line butterfly array blocks are arranged in series to form a pipeline for processing the matrix of input data points.

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.

(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
-