

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
21 March 2019 (21.03.2019)



(10) International Publication Number
WO 2019/053486 A1

(51) International Patent Classification:
G06F 15/00 (2006.01) *G09C 5/00* (2006.01)
G06F 7/48 (2006.01)

(21) International Application Number:
PCT/IB2017/054919

(22) International Filing Date:
11 August 2017 (11.08.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/484,304 11 August 2017 (11.08.2017) US

(71) Applicant: **THE GOVERNING COUNCIL OF THE UNIVERSITY OF TORONTO** [CA/CA]; Banting Institute, 100 College St., Suite 413, Toronto, Ontario M5G 1L5 (CA).

(72) Inventors: **KHEDR, Alhassan**; Banting Institute, 100 College St., Suite 413, Toronto, Ontario M5G 1L5 (CA). **GU-**

LAK, Glenn; Banting Institute, 100 College St., Suite 413, Toronto, Ontario M5G 1L5 (CA).

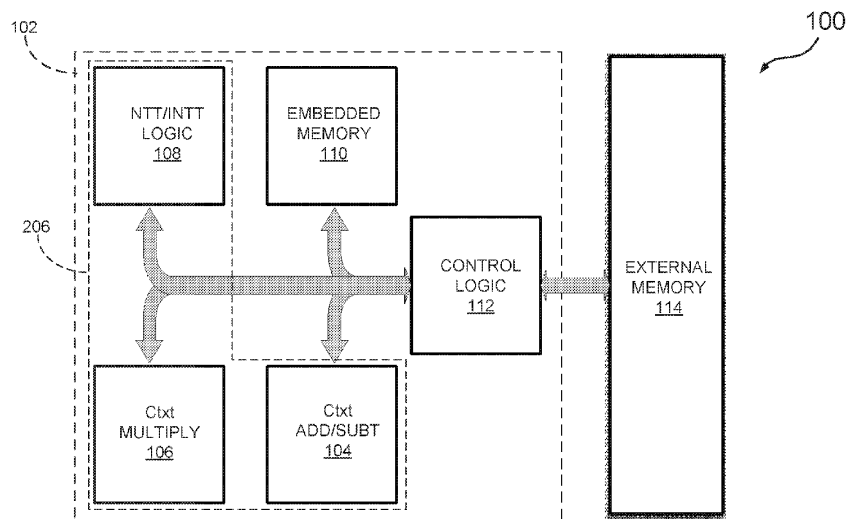
(74) Agent: **HEER, Christopher**; 36 Lombard Street, Suite 500, Toronto, Ontario M5C 2X3 (CA).

(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, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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,

(54) Title: A HOMOMORPHIC PROCESSING UNIT (HPU) FOR ACCELERATING SECURE COMPUTATIONS UNDER HOMOMORPHIC ENCRYPTION

FIG. 1A



(57) Abstract: Fully homomorphic encryption integrated circuit (IC) chips, systems and associated methods are disclosed. In one embodiment, an integrated circuit (IC) homomorphic processor chip is disclosed. The IC homomorphic processor chip includes at least one processor slice. Each processor slice includes local control circuitry, a numeric theoretic transform (NTT) butterfly unit, and on-chip memory. The NTT butterfly unit is responsive to the local control circuitry to operate in multiple modes for performing operations on encrypted data using homomorphic encryption. Each mode is associated with a different configuration of the NTT butterfly unit.

WO 2019/053486 A1

[Continued on next page]

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))*