



(51) International Patent Classification:

G09C 5/00 (2006.01) G06F 21/62 (2013.01)
G06F 7/72 (2006.01) H04L 9/00 (2022.01)

(21) International Application Number:

PCT/CA2022/051827

(22) International Filing Date:

15 December 2022 (15.12.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/289,783 15 December 2021 (15.12.2021) US
18/081,078 14 December 2022 (14.12.2022) US

(71) Applicant: THE GOVERNING COUNCIL OF THE
UNIVERSITY OF TORONTO [CA/CA]; Banting In-

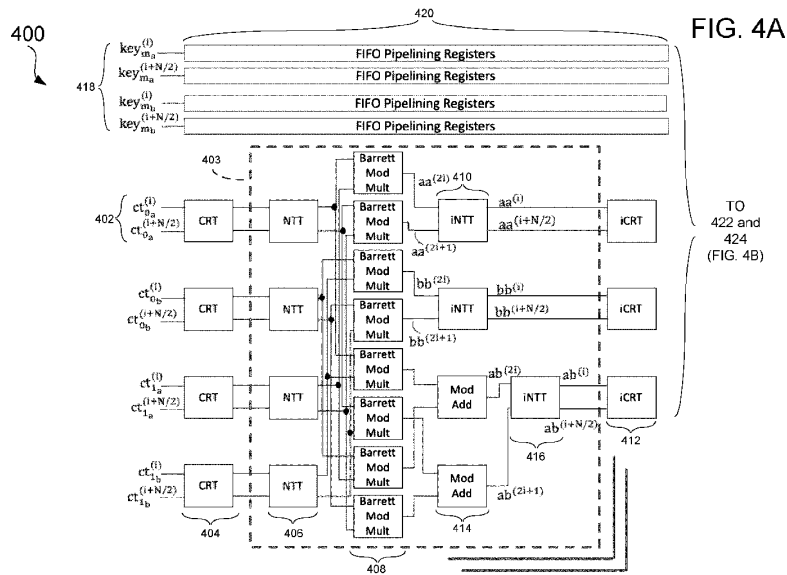
stitute, Heritage Building, 100 College Street, Suite 413,
Toronto, Ontario M5G1L5 (CA).

(72) Inventors: **BAJPEYI, Shaveer**; Banting Institute, 100
College Street, Suite 413, Toronto, Ontario M5G 1L5 (CA).
GULAK, Glenn; Banting Institute, 100 College Street,
Suite 413, Toronto, Ontario M5G 1L5 (CA).

(74) Agent: **BHOLE IP LAW**; 130 Queens Quay East, Suite
1214, Toronto, Ontario M5A0P6 (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, 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,

(54) Title: CRYPTOGRAPHIC PROCESSOR FOR FULLY HOMOMORPHIC ENCRYPTION (FHE) APPLICATIONS



(57) Abstract: Cryptographic processor chips, systems and associated methods are disclosed. In one embodiment, a cryptographic processor is disclosed. The cryptographic processor includes a first cryptographic processing module to perform a first logic operation. The first cryptographic processing module includes first input circuitry to receive ciphertext input symbols. A first pipeline stage performs a first operation on the ciphertext input symbols and generates a first stage output. On-chip memory temporarily stores the first stage output and feeds the first stage output to a second pipeline stage in a pipelined manner. The second pipeline stage is configured to perform a second operation on the first stage output in a pipelined manner with respect to the first pipeline stage.

[Continued on next page]

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