

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
24 July 2025 (24.07.2025)



(10) International Publication Number
WO 2025/154060 A1

(51) International Patent Classification:
H04L 9/00 (2022.01) *G06F 21/60* (2013.01)

(21) International Application Number:
PCT/IL2025/050047

(22) International Filing Date:
14 January 2025 (14.01.2025)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/621,206 16 January 2024 (16.01.2024) US
63/701,629 01 October 2024 (01.10.2024) US

(71) Applicant: **DWALLET LABS LTD.** [IL/IL]; 2 Har-Sinai St., 6581602 Tel - Aviv (IL).

(72) Inventors: **BRAKERSKI, Zvika**; 4 Simtat Gur Arye Street, 6451521 Tel Aviv (IL). **FRIEDMAN, Offir Mordechai**; 97 Rothschild Boulevard, 6523510 Tel Aviv (IL). **MARMOR, Avichai**; 14 Har Adir St., 4448322 Kfar-

Saba (IL). **MUTZARI, Dolev**; 9 Ha-Khelmonit St, 7542009 Rishon-LeZion (IL). **COHEN SCALY, Yehonatan Ezra**; 19 Levontin Street, 6511208 Tel Aviv (IL). **SPIIZER, Yuval**; 108 Sderot Yerushalayim, 5236373 Ramat - Gan (IL).

(74) Agent: **MANDIN, Jeff**; REINHOLD COHN GROUP, 26A Habarzel St., 6971037 Tel Aviv (IL).

(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, MU, 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, UY, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) Title: FULLY HOMOMORPHIC ENCRYPTION BASED ON NON-CYCLOTOMIC RINGS

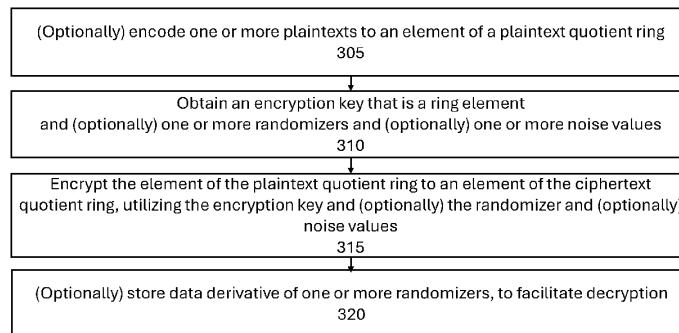


Fig. 3

(57) Abstract: A processor-based method of fully homomorphic encryption, comprising: encrypting an element of a first non-cyclotomic ring to an element of a second non-cyclotomic ring; wherein the first non-cyclotomic ring is a quotient of: a third non-cyclotomic ring that is derivative of an irreducible non-cyclotomic polynomial, and a first non-trivial ideal of the third non-cyclotomic ring, and wherein the second non-cyclotomic ring is a quotient of: the third non-cyclotomic ring, and a second ideal of the third non-cyclotomic ring, wherein the second ideal is not the first ideal.

[Continued on next page]



WO 2025/154060 A1

(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))