

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
26 October 2023 (26.10.2023)



(10) International Publication Number
WO 2023/204534 A1

(51) International Patent Classification:

H04L 9/00 (2006.01) *G06F 11/14* (2006.01)
G06F 17/11 (2006.01) *G06F 5/01* (2006.01)
G06F 7/50 (2006.01) *H04L 9/08* (2006.01)
G06F 7/523 (2006.01)

(21) International Application Number:

PCT/KR2023/005107

(22) International Filing Date:

14 April 2023 (14.04.2023)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

10-2022-0048850	20 April 2022 (20.04.2022)	KR
10-2022-0131799	13 October 2022 (13.10.2022)	KR
10-2022-0137739	24 October 2022 (24.10.2022)	KR
10-2022-0166511	02 December 2022 (02.12.2022)	KR

(71) Applicant: **CRYPTO LAB INC.** [KR/KR]; 27-404, 1, Gwanak-ro, Gwanak-gu, Seoul 08826 (KR).

(72) Inventors: **CHEON, Jung Hee**; 1, Gwanak-ro, Gwanak-gu, Seoul 08826 (KR). **BAE, Youngjin**; 1, Gwanak-ro, Gwanak-gu, Seoul 08826 (KR). **KIM, Jaehyung**; 104-302, 20, Noryangjin-ro 23ga-gil, Dongjak-gu, Seoul 06902 (KR).

(74) Agent: **KIM, Tae-hun**; 9th Floor, Shinduk Bldg., 343, Gangnam-daero, Seocho-gu, Seoul 06626 (KR).

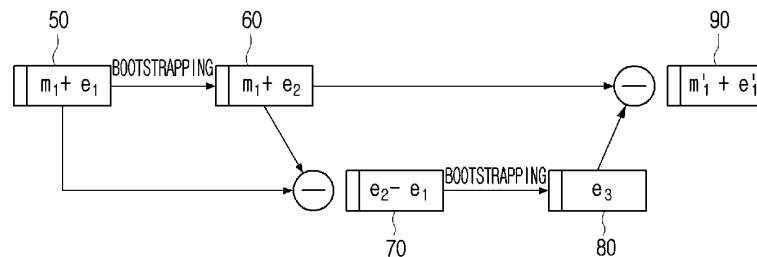
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, 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, 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, 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))

(54) Title: APPARATUS FOR BOOTSTRAP PROCESSING HOMOMORPHIC ENCRYPTED MESSAGE AND METHOD THEREOF



(57) Abstract: Disclosed is a method of processing an encrypted message. The method of processing an encrypted message includes: performing calculation on a homomorphic encrypted message on an approximate message including an error, and when a proportion of the approximate message in a calculation result encrypted message acquired by the calculation exceeds a threshold value, extending a plain text space of the calculation result encrypted message, in which the extending of the plain text space includes, generating a first intermediate encrypted message by applying a preset bootstrapping calculation to the calculation result encrypted message, generating a second intermediate encrypted message by applying the preset bootstrapping calculation to a subtraction calculation result between the calculation result encrypted message and the first intermediate encrypted message, and generating a homomorphic encrypted message having an extended plain text space by performing a subtraction calculation of the second intermediate encrypted message on the first intermediate encrypted message.



WO 2023/204534 A1