

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
03 June 2021 (03.06.2021)



(10) International Publication Number
WO 2021/107515 A1

(51) International Patent Classification:

H04L 9/30 (2006.01) **H04L 9/06** (2006.01)
G06F 21/60 (2013.01)

(21) International Application Number:

PCT/KR2020/016488

(22) International Filing Date:

20 November 2020 (20.11.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

10-2019-0155732 28 November 2019 (28.11.2019) KR
10-2020-0101937 13 August 2020 (13.08.2020) KR

(71) Applicant: **SEOUL NATIONAL UNIVERSITY R&DB
FOUNDATION** [KR/KR]; 1, Gwanak-ro, Gwanak-gu,
Seoul 08826 (KR).

(72) Inventors: **CHEON, Jung Hee**; 1, Gwanak-ro, Gwanak-
gu, Seoul 08826 (KR). **SON, Yongha**; 1, Gwanak-ro,
Gwanak-gu, Seoul 08826 (KR). **KIM, Duhyeong**; 1,
Gwanak-ro, Gwanak-gu, Seoul 08826 (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, 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, IT, JO, JP, KE, KG, KH, KN,
KP, 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.

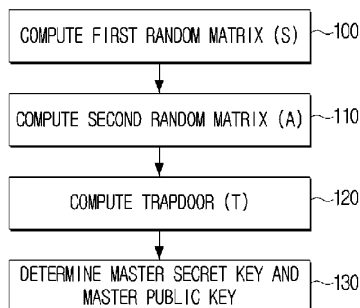
(84) Designated States (*unless otherwise indicated, for every
kind of regional protection available*): ARIPO (BW, GH,

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))

(54) Title: IDENTITY-BASED ENCRYPTION METHOD BASED ON LATTICES



(57) Abstract: A calculation device is disclosed. The calculation device includes: a memory storing at least one instruction and identity information; and a processor performing the at least one instruction, wherein the processor may randomly sample small elements, generate a function-processed output value by function-processing the stored identity information, and generate an encrypted text for a message by using a master public key computed using a ring having a dimension (d) represented by a power of 2 and an integer multiplication of 3 or more, the sampled small elements and the function-processed output value.

WO 2021/107515 A1