

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2020년 6월 11일 (11.06.2020)



(10) 국제공개번호
WO 2020/116807 A1

- (51) 국제특허분류:
H04L 9/00 (2006.01) **H04L 9/30** (2006.01)
- (21) 국제출원번호: PCT/KR2019/015410
- (22) 국제출원일: 2019년 11월 13일 (13.11.2019)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
62/776,883 2018년 12월 7일 (07.12.2018) US
10-2019-0128403 2019년 10월 16일 (16.10.2019) KR
- (71) 출원인: 주식회사 크립토허 (**CRYPTO LAB INC.**) [KR/
KR]; 08826 서울시 관악구 관악로 1, 27동 404호, Seoul
(KR).
- (72) 발명자: 천정희 (**CHEON, Jung Hee**); 08826 서울시 관
악구 관악로 1, Seoul (KR). 김동우 (**KIM, Dong Woo**);
08826 서울시 관악구 관악로 1, 27동 441호, Seoul (KR).
김두형 (**KIM, Du Hyeong**); 08826 서울시 관악구 관악
로 1, Seoul (KR).
- (74) 대리인: 김태현 (**KIM, Tac-hun**); 06626 서울시 서초구
강남대로343 신덕빌딩 9층, Seoul (KR).
- (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국
내 권리의 보호를 위하여): 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, 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.

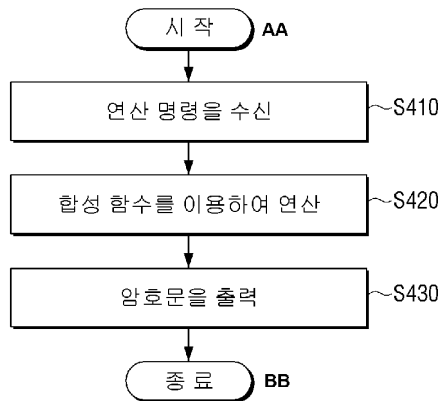
- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역
내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE,
LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM,
ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유
럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK,
MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML,
MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

(54) Title: APPARATUS AND METHOD FOR PERFORMING NON-POLYNOMIAL CALCULATION ON CRYPTOGRAM

(54) 발명의 명칭: 암호문에 대한 비다항식 연산을 수행하는 장치 및 방법



S410 ... Receive calculation command
S420 ... Perform calculation by using synthesis function
S430 ... Output cryptogram
AA ... Start
BB ... End

(57) Abstract: Disclosed is a cryptogram calculation method. The cryptogram calculation method comprises the steps of: receiving a comparative calculation command for a plurality of cryptograms of the same type; performing a calculation by reflecting the plurality of cryptograms of the same type on a synthesis function corresponding to the comparative calculation command; and outputting the calculated cryptograms of the same type.

(57) 요약서: 암호문 연산 방법이 개시된다. 본 암호문 연산 방법은 복수의 동형 암호문에 대한 비교 연산 명령을 입력받는 단계, 비교 연산 명령에 대응되는 합성 함수에 복수의 동형 암호문을 반영하여 연산하는 단계, 및 연산된 동형 암호문을 출력하는 단계를 포함한다.

WO 2020/116807 A1