

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2019년 6월 20일 (20.06.2019)



(10) 국제공개번호
WO 2019/117694 A1

- (51) 국제특허분류:
H04L 9/00 (2006.01) **H04L 9/06** (2006.01)
- (21) 국제출원번호: PCT/KR2018/016060
- (22) 국제출원일: 2018년 12월 17일 (17.12.2018)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2017-0173608 2017년 12월 15일 (15.12.2017) KR
10-2018-0129749 2018년 10월 29일 (29.10.2018) KR
- (71) 출원인: 서울대학교산학협력단 (SEOUL NATIONAL UNIVERSITY R&DB FOUNDATION) [KR/KR]; 08826 서울시 관악구 관악로 1, Seoul (KR). 주식회사 크립토크랩 (CRYPTO LAB INC.) [KR/KR]; 08826 서울시 관악구 관악로 1, 27동 404호, Seoul (KR).
- (72) 발명자: 천정희 (CHEON, Jung Hee); 08826 서울시 관악구 관악로 1, Seoul (KR). 김두형 (KIM, Duhyeong); 08826 서울시 관악구 관악로 1, Seoul (KR). 송용수 (SONG, Yongsoo); 92122 캘리포니아주 샌디에고 7520 살먼트 디알 아파트 1014, California (US). 한규형 (HAN,

Kyoohyung); 10250 경기도 고양시 일산동구 푸르메마음길 75, A-4호, Gyeonggi-do (KR).

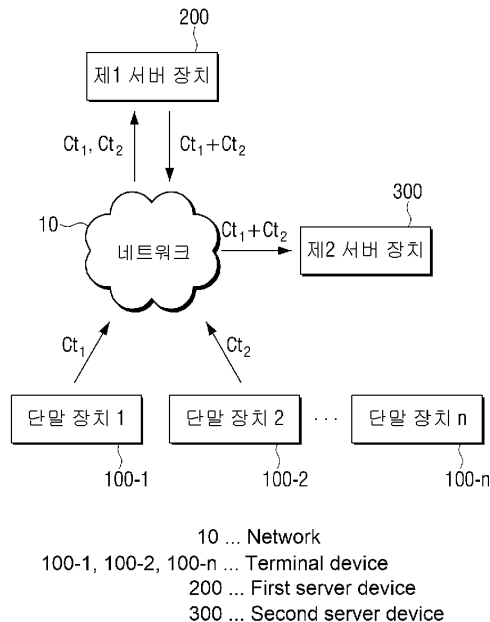
(74) 대리인: 김태현 (KIM, Tae-hun); 06626 서울시 서초구 강남대로 343 신덕빌딩 9층, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 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 국내 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), 유럽 (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

(54) Title: TERMINAL DEVICE FOR PERFORMING HOMOMORPHIC ENCRYPTION, SERVER DEVICE FOR PROCESSING CIPHER TEXT THEREOF, AND METHODS THEREFOR

(54) 발명의 명칭: 동형 암호화를 수행하는 단말 장치와 그 암호문을 처리하는 서버 장치 및 그 방법들



(57) Abstract: Disclosed is an encryption method. According to the present method, a homomorphic cipher text can be generated by using a public key after reflecting a scaling factor to a message. The generated cipher text is generated in the form in which a result value is restored when decrypted, wherein the result value is a value in which an error value is added to a value in which the scaling factor is reflected to the message. Accordingly, it is possible to effectively generate a homomorphic cipher text which can be operated in an encrypted state.

(57) 요약서: 암호화 방법이 개시된다. 본 방법에 따르면, 메시지에 스케일링 팩터를 반영한 후 공개 키를 이용하여 동형 암호문을 생성할 수 있다. 생성된 암호문은, 복호화하였을 때 메시지에 스케일링 팩터를 반영한 값에 에러 값을 가산한 결과값이 복원되는 형태로 생성된다. 이에 따라, 암호문 상태로 연산이 가능한 동형 암호문을 효과적으로 생성할 수 있다.

WO 2019/117694 A1

[다음 쪽 계속]

(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML,
MR, NE, SN, TD, TG).

규칙 4.17에 의한 선언서:

- 신규성을 해치지 아니하는 개시 또는 신규성 상실의 예
외에 관한 선언 (규칙 4.17(v))

공개:

- 국제조사보고서와 함께 (조약 제21조(3))