

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2021년 12월 23일 (23.12.2021) WIPO | PCT



(10) 국제공개번호
WO 2021/256843 A1

(51) 국제특허분류:
H04L 9/00 (2006.01)

(21) 국제출원번호: PCT/KR2021/007517

(22) 국제출원일: 2021년 6월 15일 (15.06.2021)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
63/039,086 2020년 6월 15일 (15.06.2020) US

(71) 출원인: 주식회사 크립토허브 (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). 이윤호 (LEE, Younho); 05507 서울시 송파구 올림픽로 435, 116-1401, Seoul (KR). 남유진 (NAM, Yujin); 08731 서울시 관악구 청림 3길 10, 612, Seoul (KR). 김승지 (KIM, Seungji); 08298 서울시 구로구 공원로 11, 1713, Seoul (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, IT, JO, JP, KE, KG, KH, KN, KP, KR, 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.

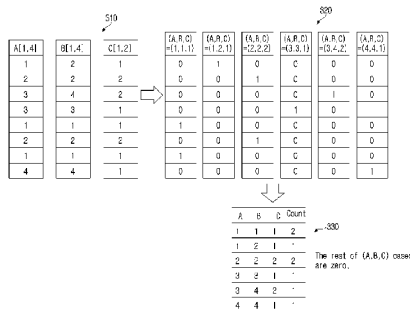
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (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: DEVICE AND METHOD FOR PERFORMING STATISTICAL CALCULATION ON HOMOMORPHIC CIPHERTEXT

(54) 발명의 명칭: 동형 암호문에 대한 통계 연산 수행하는 장치 및 방법



(57) Abstract: An electronic device is disclosed. The present electronic device comprises: a memory for storing at least one instruction and storing a plurality of homomorphic ciphertexts in which a plurality of pieces of variable information are stored in an encrypted state; and a processor for executing at least one instruction, wherein the processor executes at least one instruction to generate number information corresponding to a variable combination by using an empty mask having different pieces of variable information that are classified with respect to each homomorphic ciphertext, if a calculation command for the plurality of homomorphic ciphertexts is received.

(57) 요약서: 전자 장치가 개시된다. 본 전자 장치는 적어도 하나의 인스트럭션(instruction)을 저장하고, 복수의 변수 정보를 암호화된 상태를 저장하는 동형 암호문을 복수개 저장하는 메모리, 및 적어도 하나의 인스트럭션을 실행하는 프로세서를 포함하고, 프로세서는 적어도 하나의 인스트럭션을 실행함으로써, 복수의 동형 암호문에 대한 연산 명령이 수신되면 동형 암호문 각각에 대해서 서로 다른 변수 정보 구분하여 갖는 빈 마스크를 이용하여 변수 조합에 대응되는 개수 정보를 생성한다.

WO 2021/256843 A1