(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2022 년 7 월 21 일 (21.07.2022)

WIPO | PCT

(10) 국제공개번호
WO 2022/154241 A1

(51) 국제특허분류:
H04L 9/00 (2006.01)

(21) 국제출원번호: PCT/KR2021/017080

(22) 국제출원일: 2021 년 11 월 19 일 (19.11.2021)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2021-0006962 2021 년 1 월 18 일 (18.01.2021) KR

(71) 출원인: 서울대학교산학협력단 (**SEOUL NATIONAL UNIVERSITY R&DB FOUNDATION**) [KR/KR]; 08826 서울시 관악구 관악로 1, Seoul (KR).

(72) 발명자: 김준수 (**KIM, Junsoo**); 08826 서울시 관악구 관악로 1, Seoul (KR). 심형보 (**SHIM, Hyungbo**); 08826 서울시 관악구 관악로 1, Seoul (KR).

(74) 대리인: 백도현 (**BACK, Doehyun**); 07997 서울시 양천구 목동동로 293, 3103호(목동, 현대41타워), 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, 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.

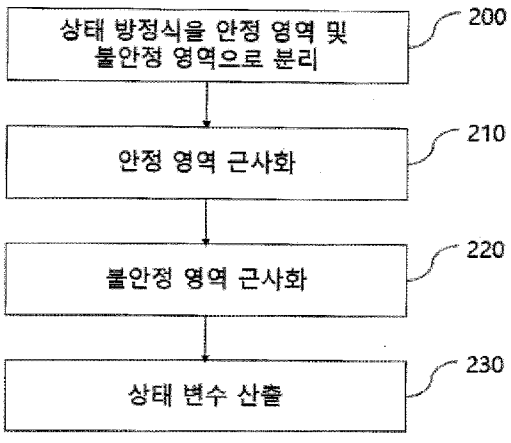
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, 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:** HOMOMORPHIC-ENCRYPTION-BASED DYNAMIC DATA PROCESSING METHOD CAPABLE OF INFINITE COMPUTATION WITHOUT REQUIRING REBOOTING AND CONTROL SIGNAL RE-ENCRYPTION

(54) **발명의 명칭:** 재부팅 및 제어신호의 재암호화가 필요없으며 무한 연산이 가능한 동형암호화기반의 동적 데이터 처리 방법



200 ... Divide state equation into stable region and unstable region
210 ... Approximate stable region
220 ... Approximate unstable region
230 ... Calculate state variables

(57) **Abstract:** The present invention relates to a homomorphic-encryption-based dynamic control data processing method and, more particularly, to a homomorphic-encryption-based dynamic data processing method capable of infinite computation without rebooting and control data re-encryption. The dynamic data processing method according to the present invention comprises: a first step of dividing a state equation into a Schur stable region ($z_s(t+1)=F_sz_s(t)+G_sy(t)$) and an unstable region ($z_u(t+1)=F_uz_u(t)+G_uy(t)$); a second step of approximating the Schur stable region; and a third step of approximating the unstable region. The third step is a step of approximating same to $z_u(t+1)\fallingdotseq F_0z_u(t)+G_uy(t)$.

(57) **요약서:** 본 발명은 동형 암호 기반의 동적 제어 데이터 처리 방법에 대한 것으로서, 좀 더 자세하게는 재부팅과 제어 데이터의 재암호화 과정 없이 무한 연산이 가능한 동형 암호 기반의 동적 데이터 처리 방법에 대한 것이다. 본 발명에 의한 동적 데이터 처리 방법은, 상기 상태 방정식을 슈어 안정(Schur stable) 영역($z_s(t+1)$ = $F_sz_s(t)$ + $G_sy(t)$)와 불안정 영역($z_u(t+1)$ = $F_uz_u(t)$ + $G_uy(t)$)로 분리하는 제1 단계와; 상기 슈어 안정 영역을 근사화하는 제2 단계와; 상기 불안정 영역을 근사화하는 제3 단계를 포함한다. 제3 단계는, $z_u(t+1)$ ≒ $F_0z_u(t)$ + $G_uy(t)$로 근사화하는 단계이다.

WO 2022/154241 A1

명세서

발명의 명칭: 재부팅 및 제어신호의 재암호화가 필요없으며 무한 연산이 가능한 동형암호화기반의 동적 데이터 처리 방법

기술분야

[1] 본 발명은 동형 암호 기반의 동적 제어 데이터 처리 방법에 대한 것으로서, 좀 더 자세하게는 재부팅과 제어 데이터의 재암호화 과정 없이 무한 연산이 가능한 동형 암호 기반의 동적 데이터 처리 방법에 대한 것이다.

배경기술

[2] 네트워크 통신으로 컴퓨터에 물리적 시스템이 연결될수록 실제 제어 시스템이 해커의 목표가 될 가능성이 높아진다. 일반적으로 연산부(computation; 사이버 부분), 물리적 시스템(물리적 부분)와 통신부(사이버 파트와 물리적 부분간의 링크)를 통칭하여 사이버-물리 시스템(cyber-physical system)이라고 한다.

[3] 사이버-물리 시스템의 개방성 및 연결성으로 인해 악성 공격에 취약할 수 밖에 없는데, 산업 플랜트 등이 악성 해커의 공격에 노출된다면 대규모 사고를 초래할 수도 있고 작게는 개별 플랜트 등이 오작동할 수 있다.

[4] 그러한 문제를 예방하기 위하여 제어 신호를 암호화하여 사용하는 방법이 채택될 수 있는데, 암호화된 데이터를 제어기가 연산을 하기 위해서는 복호화 과정이 필요하다.

[5] 복호화를 위해서는 제어기가 비밀키를 소유하고 있어야 하는데 그러한 환경에서는 비밀키가 해커에 의해서 탈취될 가능성이 있기 때문에 보안상 취약점이 존재한다.

[6] 이러한 문제를 해결하기 위하여 제어 데이터를 동형 암호화하고, 암호화된 제어 데이터를 연산하는 기술적 사상이 2013년 12월 25일에 공개된 유럽특허출원공개 EP 2 677 680 A1에 기재되어 있다. 그런데 동형 암호문은 연산을 거듭할수록 내부 노이즈가 증가하고, 실수를 정수화하는 과정에서 포함되는 스케일링 팩터(비례 정수)가 누적되는 등의 한계로 인해 나중에는 더 이상의 연산이 불가능하게 된다. 그러한 경우 제어기를 부트스트래핑(재부팅)해야 하는데, 부트스트래핑을 하는 동안은 제어기가 암호화된 상태 변수를 업데이트하지 못하므로 제어기 동작이 멈추는 문제가 있었다.

[7] 2018년 11월 19일에 등록공고된 한국특허 제10-1919940호는, 부트스트래핑을 하는 동안에 상태 변수 업데이트 문제를 해결하기 위한 방법을 제안하고 있다. 이 특허는 다중 제어기를 도입하여 어느 하나의 제어기가 부트 스트래핑을 하는 동안에 다른 제어기가 상태 변수를 업데이트하는 방법을 제안하고 있다. 그러나 이 방법은 제어기를 여러 개 사용하므로 비용 문제와 복잡도 상승으로 인해 실제 적용에 어려움이 있고, 제어기가 여전히 재부팅을 해야 하는 한계를 가지고 있기

때문에 소요 연산 시간을 짧게 하기도 어려운 문제가 있었다.

[8] 본 출원인은 상기 문제를 해결하기 위해 2019년 10월 10일에 상태 행렬을 정수화함으로써 무한 연산이 가능한 발명에 대해 특허출원을 하고 특허등록을 받은 바 있다(특허 제10-2306635호; 2021년 9월 28일 등록공고).

[9] 그러나 이 발명에 따르면 제어 신호의 재암호화 과정이 필요한 한계가 있어서 예를 들어 제어 알고리즘을 분산하여 여러 제어기가 처리하는 시스템에서는 문제가 생길 수 있다.

발명의 상세한 설명

기술적 과제

[10] 본 발명은 전술한 종래 기술의 문제를 해결함으로써 재부팅 과정 및 제어 신호의 재암호화 과정이 필요없으면서도, 동형암호기반 동적 데이터의 무한 연산이 가능한 동적 제어 데이터의 처리 방법을 제공하는 것을 목적으로 한다.

과제 해결 수단

[11] 본 발명에 의한 동적 데이터 처리 방법은, 피제어부와, 제어기와, 제어기로부터 수신한 제어 신호를 복호화하는 모듈과, 복호화 모듈로부터 복호화된 제어 신호를 수신하여 작동하는 액츄에이터와, 피제어부의 출력을 검지하는 센서와, 센서의 신호를 동형 암호화하는 동형 암호화 모듈을 포함하는 환경에서 실행되며,상기 제어기의 상태 방정식은, $\boldsymbol{x(t+1) = Fx(t) + Gy(t)}$ 이다.

[12] 본 발명에 의한 동적 데이터 처리 방법은, 상기 상태 방정식을 슈어 안정(Schur stable) 영역($\boldsymbol{z_s(t+1) = F_s z_s(t) + G_s y(t)}$)과 불안정 영역($\boldsymbol{z_u(t+1) = F_u z_u(t) + G_u y(t)}$)으로 분리하는 제1 단계와; 상기 슈어 안정 영역을 근사화하는 제2 단계와; 상기 불안정 영역을 근사화하는 제3 단계를 포함한다.

[13] 제2 단계는, $\begin{bmatrix} z_{s,1}(t+1) \\ z_{s,2}(t+1) \\ \vdots \\ z_{s,k_1}(t+1) \end{bmatrix} \approx \begin{bmatrix} z_{s,2}(t) \\ \vdots \\ z_{s,k_1}(t) \\ 0 \end{bmatrix} + \begin{bmatrix} G_s \\ F_s G_s \\ \vdots \\ F_s^{k_1-1} G_s \end{bmatrix} y(t)$ 로 근사화하는 단계이다.

[14] 제3 단계는, $\boldsymbol{z_u(t+1) \approx F_0 z_u(t) + G_u y(t)}$ 로 근사화하는 단계로서, 제어 신호 생성을 위한 상태 변수 연산식은,

[15] $\xi(k_2 t+1) = \xi(k_2 t) + T_2 F_0^{-1} G_u y(t)$

[16] $\xi(k_2 t+2) = \xi(k_2 t+1) + T_2 F_0^{-2} G_u y(t)$

[17] ⋮

[18] $\xi(k_2 t+k_2-1) = \xi(k_2 t+k_2-2) + T_2 F_0^{-(k_2-1)} G_u y(t)$

[19] $\xi(k_2 t+k_2) = T_2 F_0^{k_2} T_2^{-1} \xi(k_2 t+k_2-1) + T_2 G_u y(t)$

[20] 이다.

[21] F_s는 모든 고유값(eigenvalue)의 절대값은 1보다 작으며, F_u의 모든 고유값의

절대값은 1보다 크거나 같으며, k_1은 $F_s^{k_1}$가 0에 수렴하는 충분히 큰 자연수이다.

[22] k_2는 $\|F_u - F_0\| < \varepsilon$ (ε는 0보다 큰 충분히 작은 수)이고

[23] $TF_0^{k_2}T^{-1} \in \mathbb{Z}^{n\times n}$ ($F_0 \in \mathbb{R}^{n\times n}$이고, $T_2 \in \mathbb{R}^{n\times n}$)인 조건을 만족시키는 자연수이다.

[24] $\begin{bmatrix} z_{s,2}(t) \\ \vdots \\ z_{s,k_1}(t) \\ 0 \end{bmatrix} = A \begin{bmatrix} z_{s,1}(t) \\ z_{s,2}(t) \\ \vdots \\ z_{s,k_1}(t) \end{bmatrix}$ 이며, A는 대각 원소 바로 위의 원소가 모두 1이며, 나머지 원소는 0인 행렬이다.

[25] k_1과 k_2는 같은 값이 될 수 있다.

[26] 본 발명에 의한 동적 데이터 처리 방법은, 컴퓨터 판독 가능 기록 매체에 기록된 컴퓨터 프로그램에 의해 실행될 수 있다.

[27]

발명의 효과

[28] 본 발명에 의한 동형 암호 기반의 동적 데이터를 처리함에 있어서 재부팅 및 제어 신호의 재암호화 과정이 필요없이도 무한 연산이 가능한 동적 데이터의 처리 방법이 제공되는 효과가 있다.

도면의 간단한 설명

[29] 도 1은 본 발명에 의한 동적 제어 데이터의 처리 방법이 수행되는 환경의 예시적인 블록도.

[30] 도 2는 본 발명에 의한 동적 데이터의 처리 방법의 흐름도.

[31] 도 3은 본 발명에 의한 동적 데이터 처리 방법을 실행하는 전자적 연산 장치의 예시적인 블록도.

[32]

발명의 실시를 위한 형태

[33] 이하에서는 첨부 도면을 참조하여 본 발명에 대해서 자세하게 설명한다.

[34] 본 명세서에서 수행되는 정보(데이터) 전송 과정은 필요에 따라서 암호화/복호화가 적용될 수 있으며, 본 명세서 및 특허청구범위에서 정보(데이터) 전송 과정을 설명하는 표현은 별도로 언급되지 않더라도 모두 암호화/복호화하는 경우도 포함하는 것으로 해석되어야 한다. 본 명세서에서 "A로부터 B로 전송(전달)" 또는 "A가 B로부터 수신"과 같은 형태의 표현은 중간에 다른 매개체가 포함되어 전송(전달) 또는 수신되는 것도 포함하며, A로부터 B까지 직접 전송(전달) 또는 수신되는 것만을 표현하는 것은 아니다. 본 발명의 설명에 있어서 각 단계의 순서는 선행 단계가 논리적 및 시간적으로 반드시 후행 단계에 앞서서 수행되어야 하는 경우가 아니라면 각 단계의 순서는 비제한적으로 이해되어야 한다. 즉 위와 같은 예외적인 경우를 제외하고는 후행 단계로 설명된 과정이 선행 단계로 설명된 과정보다 앞서서 수행되더라도 발명의 본질에는 영향이 없으며 권리범위 역시 단계의 순서에 관계없이 정의되어야 한다. 그리고 본 명세서에서 “A 또는 B”는 A와 B 중 어느 하나를

선택적으로 가리키는 것 뿐만 아니라 A와 B 모두를 포함하는 것도 의미하는 것으로 정의된다. 또한, 본 명세서에서 "포함"이라는 용어는 포함하는 것으로 나열된 요소 이외에 추가로 다른 구성요소를 더 포함하는 것도 포괄하는 의미를 가진다.

[35] 본 명세서에서 "모듈" 또는 "유니트"라 함은 범용적 또는 개별적으로 적용되는 하드웨어와 그 기능을 수행하는 소프트웨어의 논리적 결합을 의미한다.

[36] 본 명세서에서는 본 발명의 설명에 필요한 필수적인 구성요소만을 설명하며, 본 발명의 본질과 관계가 없는 구성요소는 언급하지 아니한다. 그리고 언급되는 구성요소만을 포함하는 배타적인 의미로 해석되어서는 아니되며 다른 구성요소도 포함할 수 있는 비배타적인 의미로 해석되어야 한다.

[37] 본 명세서에서 "동적 제어 데이터"라고 함은, 일정 시간 내에 처리되지 않으면 무의미해지거나 그 가치가 현저히 떨어져서 사실상 효용성이 사라지는 제어 데이터로 정의되며, "동적 제어기"라고 함은 동적 시스템으로 만들어진 제어기라는 뜻으로 제어기 내부에 상태 변수를 유지하여 매 연산시간마다 상태변수가 갱신되는 형태의 제어기를 포함한다.

[38] 본 발명은 전자적 연산이 가능한 컴퓨터 등의 전자적 연산 장치에 의해서 수행되며, 후술하는 본 발명의 각 단계의 수학적 연산 및 산출은 해당 연산 또는 산출을 하기 위해 공지되어 있는 코딩 방법 및/또는 본 발명에 적합하게 고안된 코딩에 의해서 컴퓨터 연산으로 구현될 수 있다.

[39] 본 발명에 의한 방법은 컴퓨터, 태블릿 PC, 모바일폰, 휴대용 연산 장치, 고정식 연산 장치 등의 전자적 연산장치에 의해서 실행될 수 있다. 또한, 본 발명의 하나 또는 그 이상의 방법 또는 형태가 적어도 하나의 프로세서에 의해 실행될 수 있다는 점이 이해되어야 한다. 프로세서는, 컴퓨터, 태블릿PC, 모바일 장치, 휴대용 연산장치 등에 설치될 수 있다. 컴퓨터 프로그램 명령을 저장하도록 되어 있는 메모리가 그러한 장치에 설치되어서 프로그램이 저장된 프로그램 명령을 프로세서가 실행하도록 특별히 프로그램되어 하나 또는 그 이상의, 본 명세서에 기재된 기재된 바와 같은 프로세스를 실행할 수 있다. 또한, 본 명세서에 기재된 정보 및 방법 등은,하나 또는 그 이상의 추가적인 구성요소와 프로세서를 포함하는 컴퓨터, 태블릿PC, 모바일 장치, 휴대용 연산 장치 등에 의해서 실행될 수 있다는 점이 이해되어야 한다. 또한, 제어 로직은, 프로세서, 제어부/제어 유니트 등에 의해 실행가능한 프로그램 명령을 포함하는 비휘발성 컴퓨터 판독 가능 매체로 구현될 수 있다. 컴퓨터판독 가능 매체의 예로는, ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 플래시 드라이브, 스마트 카드, 광학 데이터 저장 장치 등이 있지만 그에 제한되는 것은 아니다. 또한, 컴퓨터 판독 가능 기록 매체는 네트워크로 연결된 컴퓨터에 분산되어, 컴퓨터 판독 가능 매체가 분산된 방식 예를 들어 원격 서버 또는 CAN(Controller Area Network)에 의해 분산된 방식으로 저장되고 실행될 수도 있다.

[40] 본 발명의 각 단계를 수행하는 전자적 연산 장치의 일례가 도 3에 도시되어

있다. 도 3에 도시된 바와 같이 전자적 연산 장치(309)는 프로세서(예를 들어 중앙 처리 유니트(CPU; 310)와, 메모리(320)와, 유선 또는 무선 통신 유니트(330)와, 적어도 하나의 입력 유니트(340), 및 적어도 하나의 출력 유니트(350)를 포함하지만, 포함하는 구성요소는 열거된 구성요소에 제한되지 않는다. 도 3에 도시된 구조는 단지 설명의 목적으로 단순화되어 제공되는 것이라는 점이 이해되어야 한다. 전자적 연산 장치(309)의 구조는 후술하는 특허청구범위에 따라서 당업자에 의해 적절한 방식으로 변경될 수 있다. 또한, 전자적 연산 장치(309)의 각 구성요소 역시 후술하는 특허청구범위에 따라서 당업자에 의해 적절한 방식으로 변경될 수 있다. 그러므로, 도 3에 도시된 장치의 구조는 단지 예시적이며 본 발명의 권리범위를 제한하는 것으로 해석되어서는 아니된다.

[41] 프로세서(310)는 전자적 연산 장치(309)의 작동을 제어할 수 있다. 더 자세하게는 프로세서(310)는 도 3에 도시된 바와 같은 전자적 연산 장치(309)에 설치된 여러 구성요소를 제어하고 상호작용하도록 작동될 수 있다. 예를 들어, 메모리(320)는 프로세서(310)에 의해 실행되는 프로그램 명령이나 데이터를 저장할 수 있다. 본 명세서에서 설명하는 프로세스(단계)는 프로세서(310)의 실행을 위해 메모리(320)에 프로그램 명령어의 형태로 저장될 수 있다. 통신 유니트(330)는 전자적 연산 장치(309)가 통신 네트워크를 통해서 적어도 하나의 외부 장치로 데이터를 전송하거나 적어도 하나의 외부 장치로부터 데이터를 수신하도록 할 수 있다. 입력 유니트(340)는 전자적 연산 장치(309)가 오디오/비디오 입력, 사용자 입력, 데이터 입력 등의 다양한 형태의 입력을 수신하도록 할 수 있다. 이러한 목적을 위해 입력 유니트(340)는 다양한 형태의 입력을 받아들이기 위해서 예를 들어, 적어도 하나의 카메라(342, 즉 "이미지 획득 유니티")와, 터치 패널(344)과, 마이크로폰(도시되지 않음), 센서(346), 키보드, 마우스, 적어도 하나의 버튼이나 스위치(도시되지 않음) 등과 같은 다양한 입력 장치를 포함할 수 있다. 본 명세서에서 사용되는 "이미지 획득 유니트"라는 용어는 카메라(342)를 가리킬 수 있지만 그것에 제한되는 것은 아니다. 출력 유니트(1350)는, 사용자가 볼 수 있도록 디스플레이 스크린(1352)에 정보를 표시할 수 있다. 디스플레이 스크린(1352)은 공지되어 있는 다양한 메커니즘을 통해서 사용자 태핑(tapping)이나 스크린(1352)을 누르는 것과 같은 적어도 하나의 입력을 받아들이도록 구성될 수 있다. 출력 유니트(1350)는, 광원(1354)을 더 포함할 수 있다. 전자적 연산 장치(1309)는, 단일 장치로 도시되어 있지만, 사용되는 동안 서로 연결되고 상호작용할 수 있는 다중의 분리된 장치로 구성될 수도 있다.

[42] 본 명세서에서 "값"이라 함은 스칼라값 뿐만 아니라 행렬, 벡터 또는 다항식도 포함하는 개념으로 정의된다.

[43] 본 명세서에서 특정값에 대해 암호화 또는 해쉬 등과 같은 연산을 하여 소정의 값을 획득한다는 의미는 해당 특정값 뿐만 아니라 해당 특정값의 변형값(예를

들어, 특정값에 소정의 값을 추가로 연산하거나 소정의 규칙에 따라서 해당 특정값을 변화시키는 등의 과정을 통해서 산출된 다른 값)에 대한 암호화 또는 해쉬 등의 연산도 포함하는 것으로 정의된다.

[44] 본 명세서에서 설명하는 예시적인 실시예는 본 명세서에 개시(開示)되는 장치의 구조, 기능, 제작 및 용도와 방법의 원리에 대한 전반적인 이해를 제공한다. 이러한 하나 이상의 실시예가 첨부 도면에 도시되어 있다. 당업자라면 여기에 구체적으로 기재되고 첨부 도면에 도시되어 있는 장치 및 방법이 비제한적이고 예시적인 실시예이며 본 발명의 권리범위는 특허청구범위에 의해서 정의된다는 점을 이해할 것이다. 하나의 예시적인 실시예와 관련되어 도시되고 설명되는 특징은 다른 실시예의 특징과도 결합될 수 있다. 그러한 수정(modification) 또는 변경(variation)은 본 발명의 권리범위에 포함되도록 의도된다.

[45] |*| 는 *의 반올림 값을 의미한다.

[46] 본 명세서에서는 설명의 편의를 위해 제어기(10)가 이산시간 선형 시불변 제어기(discrete-time linear time-invariant controller)인 것으로 가정한다. 그러나 본 발명의 기술적 사상을 이해한, 제어 분야에서 통상의 지식을 가지는 사람이라면, 다른 형태의 선형 제어기 또는 시변 제어기에도 본 발명을 별다른 어려움 없이 적용할 수 있다.

[47] 도 1에는 본 발명에 의한 동적 제어 데이터 처리를 수행하는 제어 환경의 일례가 도시되어 있다.

[48] 이 환경은, 제어기(10)와, 액츄에이터(20)와, 복호화 모듈(25)과, 피제어부(30)와, 센서(40)와, 암호화 모듈(45)을 포함한다.

[49] 액츄에이터(20)와 복호화 모듈(25)은 별도의 구성요소로 도 1에 도시되어 있지만, 액츄에이터(20)와 복호화 모듈(25)은 일체로 구성될 수도 있다. 센서(40)와 암호화 모듈(45)도 별도의 구성요소로 도 1에 도시되어 있지만, 센서(40)와 암호화 모듈(45)은 일체로 구성될 수도 있다. 복호화 모듈(25)과 암호화 모듈(45) 중 적어도 어느 하나는 제어기(10)와 일체로 구성될 수도 있다.

[50] 복호화와 암호화는 대칭키 방식을 사용할 수도 있고, 공개키 암호화 방식을 사용할 수도 있다. 대칭키 방식인 경우에는, 복호화 모듈(25)과 암호화 모듈(45)이 동일한 키를 가지고 있으며, 공개키 암호화 방식인 경우에는 복호화 모듈(25)은 비밀키를, 암호화 모듈(45)은 공개키를 가질 수 있다.

[51] 액츄에이터(20)는 제어기(10)의 제어 명령 u(t)에 따라서 피제어부(30)를 제어한다. 센서(40)는 피제어부(30)의 출력을 감지한다. 암호화 모듈(45)은 센서(40)가 감지한 신호를 동형 암호화한 값인 $\bar{y}(t)$를 제어기 입력값으로서 제어기(10)로 입력한다. 복호화 모듈(25)은 제어기(10)의 출력인 암호화된 제어기 출력 신호값인 $\bar{u}(t)$를 복호화하여 액츄에이터(20)에 제공한다.

[52] 본 발명에 의한 제어 시스템의 상태 방정식은 다음과 같이 정의된다. 평문

상태의 상태 방정식과 암호문 상태의 상태 방정식에 적용되는 동일한 연산은 동형암호의 특성상 동일한 결과를 산출하므로, 설명의 편의를 위해 본 명세서에서는 평문 상태로 설명한다.

[53] [수식1]

$$x(t+1) = Fx(t) + Gy(t)$$

[54] $$u(t) = Hx(t)$$

[55] 상태 변수를 좌표변환(

$$z(t) = T_1 x(t)$$

)을 하면 항상 다음과 같이 안정 영역(아래첨자 "s")과 불안정 영역(아래첨자 "u")으로 나눌 수 있다(단계 200).

[56] [수식2]

$$z_s(t+1) = F_s z_s(t) + G_s y(t)$$

[57] $$z_u(t+1) = F_u z_u(t) + G_u y(t)$$

[58] $$u(t) = H_s z_s(t) + H_u z_u(t) =: u_s(t) + u_s(t)$$

[59] 상기 좌표 변환 행렬 T_1은 상태 행렬 F를 Jordan Canonical Form으로 표현하는 행렬이 될 수 있다.

[60] F_s의 모든 고유값(eigenvalue

$$\lambda$$

;

$$\lambda \in \mathbb{C}$$

)의 절대값은 1보다 작다.

[61] F_u의 모든 고유값(eigenvalue

$$\lambda$$

;

$$\lambda \in \mathbb{C}$$

)의 절대값은 1보다 크거나 같다.

[62] $k_1 \to \infty$인 경우에는

$$\|F_s\|^{k_1} \to 0$$

이 된다. 충분히 큰 자연수 k_1를 선택하면 안정 영역은 다음과 같이 근사화된다(단계 210). 도 2에는 안정 영역을 먼저 근사화하고 불안정 영역을 근사화하는 것으로 도시되어 있지만 그 순서는 바뀌어도 무방하다.

[63] [수식3]

$$z_s(t+1) = F_s z_s(t) + G_s y(t) = F_s^{t+1} z_s(0) + G_s y(t) + F_s G_s y(t-1) + \cdots F_s^t G_s y(0)$$
$$\approx G_s y(t) + F_s G_s y(t-1) + \cdots + F_s^{k_1-1} G_s y(t-k_1+1)$$

[64] 여기에서 $t \geq k_1$이다.

[65] 상기 수학식 3은 다음과 같은 근사화 행렬 형태로 정리할 수 있다.

[66] [수식4]

$$\begin{bmatrix} z_{s,1}(t+1) \\ z_{s,2}(t+1) \\ \vdots \\ z_{s,k_1}(t+1) \end{bmatrix} \approx \begin{bmatrix} z_{s,2}(t) \\ \vdots \\ z_{s,k_1}(t) \\ 0 \end{bmatrix} + \begin{bmatrix} G_s \\ F_s G_s \\ \vdots \\ F_s^{k_1-1} G_s \end{bmatrix} y(t)$$

[67] $$u_s(t) = H_s z_{s,1}(t)$$

[68] 상기 수학식 4는 다음과 같이 정리할 수 있다.

[69] [수식5]

$$\begin{bmatrix} z_{s,1}(t+1) \\ z_{s,2}(t+1) \\ \vdots \\ z_{s,k_1}(t+1) \end{bmatrix} = A \begin{bmatrix} z_{s,1}(t) \\ z_{s,2}(t) \\ \vdots \\ z_{s,k_1}(t) \end{bmatrix} + \begin{bmatrix} G_s \\ F_s G_s \\ \vdots \\ F_s^{k_1-1} G_s \end{bmatrix} y(t)$$

[70] 수학식 5에서 행렬 A는 대각 원소 바로 위의 원소는 모두 "1"이며, 나머지 원소는 모두 "0"인 행렬이다.

[71] 수학식 5에서 상태 행렬 A는 정수 행렬의 형태를 취하므로, 제어 시스템의 상태 행렬이 정수 행렬이 되는 것으로 볼 수 있으며, 따라서 수학식 5는 동형 암호화된 상태에서 무한 연산이 가능해 진다.

[72] 수학식 5에 의해서 산출된 안정 영역의 상태 변수에 기초하여 z_s값을 산출한다(단계 230).

[73] 단계(200)에서는 다음과 같이 불안정 영역을 근사화한다.

[74] 먼저 다음과 같은 관계가 성립할 수 있음을 알 수 있다.

[75] $|a| \geq 1$

를 만족하는 임의의 실수 a에 대해서는,

$$\lim_{k\to\infty} (|a^k|)^{\frac{1}{k}} = a$$

가 성립한다.

[76] 그리고 0보다 큰 임의의 충분히 작은

ε

,

$|\lambda| \geq 1$

를 만족하는 복소수

λ

에 대해서,

$|\lambda - \lambda_0| < \varepsilon, \quad \lambda_0^k \in \mathbb{Z}$

를 만족하는, 자연수 k와 복소수

λ_0

가 존재한다.

[77] 상기 관계를 기초로 유도하면 다음과 같은 정리(lemma)가 성립한다.

[78] [LEMMA]

[79] 불안정한 행렬

$F_u \in \mathbb{R}^{n\times n}$

에 대해서 다음의 수학식 6을 만족하는 자연수 k_2, 행렬

$F_0 \in \mathbb{R}^{n\times n}$

, 행렬

$T_2 \in \mathbb{R}^{n\times n}$

가 존재한다.

[80] [수식6]

$$\|F_u - F_0\| < \varepsilon, \qquad T_2 F_0^{k_2} T_2^{-1} \in \mathbb{Z}^{n\times n}$$

[81] 상기 정리에 의하면, 불안정 영역의 상태 방정식은 다음과 같이 정리될 수 있다.

[82] [수식7]

$$z_u(t+1) = F_u z_u(t) + G_u y(t) \approx F_0 z_u(t) + G_u y(t)$$

[83] $$u_u(t) = H_u z_u(t)$$

[84] $$TF_0^{k_2}T^{-1} \in \mathbb{Z}^{n\times n}$$

의 관계를 만족하는 T_2를 이용하여 다음과 같은 좌표 변환을 고려한다.

[85] [수식8]

$$\xi(k_2 t) = T_2 z_u(k_2 t)$$

[86] $$\xi(k_2 t+1) = T_2 F_0^{-1} z_u(k_2 t+1)$$

[87] ⋮

[88] $$\xi(k_2 t+k_2-2) = T_2 F_0^{-(k_2-2)} z_u(k_2 t+k_2-2)$$

[89] $$\xi(k_2 t+k_2-1) = T_2 F_0^{-(k_2-1)} z_u(k_2 t+k_2-1)$$

[90] 수학식 9는 다시 다음과 같이 표현할 수 있다.

[91] [수식9]

$$\xi(k_2 t+1) = \xi(k_2 t) + T_2 F_0^{-1} G_u y(t)$$

[92] $$\xi(k_2 t+2) = \xi(k_2 t+1) + T_2 F_0^{-2} G_u y(t)$$

[93] ⋮

[94] $$\xi(k_2 t+k_2-1) = \xi(k_2 t+k_2-2) + T_2 F_0^{-(k_2-1)} G_u y(t)$$

[95] $$\xi(k_2 t+k_2) = T_2 F_0^{k_2} T_2^{-1} \xi(k_2 t+k_2-1) + T_2 G_u y(t)$$

[96] 수학식 10에 의하면 좌표변환된 상태에서 불안정 영역의 상태 행렬이 정수 행렬이 되기 때문에, 동형 암호화 상태에서 불안정 영역에 대해서 무한 연산이 가능해진다.

[97] 수학식 10에 의해서 좌표변환된 상태 변수

ξ

값이 산출되면 그로부터 수학식 9에 의해서 z_u값을 산출한다(단계 230).

[98] z_s값과 z_u값이 산출되면 그로부터 상태변수 x값을 산출하고 그로부터 제어 데이터 u값을 산출하고 산출된 제어 데이터 정확하게는 제어데이터의 동형 암호화값을 액츄에이터(20)로 전송한다.

[99] k_1과 k_2는 같은 값이 될 수도 있고, 서로 다른 값이 될 수도 있다.

[100] 본 발명에 의하면, 일반적으로 실수 원소를 가지는 상태 행렬을 안정 영역과 불안정 영역으로 분리하고, 각각의 영역에 대해서 상태 방정식을 근사화한 후 상태 행렬을 정수 행렬화함으로써 동형 암호문 상태에서 무한 연산이 가능하게 할 수 있는 효과가 제공된다.

[101] 이상 첨부 도면을 참고하여 본 발명에 대해서 설명하였지만 본 발명의 권리범위는 후술하는 특허청구범위에 의해 결정되며 전술한 실시예 및/또는 도면에 제한되는 것으로 해석되어서는 아니된다. 그리고 특허청구범위에 기재된 발명의, 당업자에게 자명한 개량, 변경 및 수정도 본 발명의 권리범위에 포함된다는 점이 명백하게 이해되어야 한다.

청구범위

[청구항 1] 피제어부와, 제어기와, 제어기로부터 수신한 제어 신호를 복호화하는 모듈과, 복호화 모듈로부터 복호화된 제어 신호를 수신하여 작동하는 액츄에이터와, 피제어부의 출력을 검지하는 센서와, 센서의 신호를 동형 암호화하는 동형 암호화 모듈을 포함하는 환경에서 상기 제어기가 수행하는 동적 제어 데이터의 처리 방법에 있어서,

상기 제어기의 상태 방정식은, $x(t+1) = Fx(t) + Gy(t)$ 이며,

상기 상태 방정식을 슈어 안정(Schur stable) 영역($z_s(t+1) = F_s z_s(t) + G_s y(t)$)과 불안정 영역($z_u(t+1) = F_u z_u(t) + G_u y(t)$)으로 분리하는 제1 단계와,

상기 슈어 안정 영역을 근사화하는 제2 단계와,

상기 불안정 영역을 근사화하는 제3 단계를 포함하며,

제2 단계는,

$$\begin{bmatrix} z_{s,1}(t+1) \\ z_{s,2}(t+1) \\ \vdots \\ z_{s,k_1}(t+1) \end{bmatrix} \approx \begin{bmatrix} z_{s,2}(t) \\ \vdots \\ z_{s,k_1}(t) \\ 0 \end{bmatrix} + \begin{bmatrix} G_s \\ F_s G_s \\ \vdots \\ F_s^{k_1-1} G_s \end{bmatrix} y(t)$$

로 근사화하는 단계이며,

제3 단계는,

$z_u(t+1) \approx F_0 z_u(t) + G_u y(t)$ 로 근사화하는 단계로서,

제어 신호 생성을 위한 상태 변수 연산식은,

$$\xi(k_2 t+1) = \xi(k_2 t) + T_2 F_0^{-1} G_u y(t)$$

$$\xi(k_2 t+2) = \xi(k_2 t+1) + T_2 F_0^{-2} G_u y(t)$$

$$\vdots$$

$$\xi(k_2 t+k_2-1) = \xi(k_2 t+k_2-2) + T_2 F_0^{-(k_2-1)} G_u y(t)$$

$$\xi(k_2 t+k_2) = T_2 F_0^{k_2} T_2^{-1} \xi(k_2 t+k_2-1) + T_2 G_u y(t)$$

이며,

F_s는 모든 고유값(eigenvalue)의 절대값은 1보다 작으며, F_u의 모든 고유값의 절대값은 1보다 크거나 같으며,

k_1은 $F_s^{k_1}$가 0에 수렴하는 충분히 큰 자연수이며,

k_2는 $\|F_u - F_0\| < \varepsilon$ (ε는 0보다 큰 충분히 작은 수)이고 $TF_0^{k_2}T^{-1} \in \mathbb{Z}^{n\times n}$ ($F_0 \in \mathbb{R}^{n\times n}$이고, $T_2 \in \mathbb{R}^{n\times n}$)인 조건을 만족시키는 자연수인,

제어기가 수행하는 동적 제어 데이터의 처리 방법.

[청구항 2] 청구항 1에 있어서,

$$\begin{bmatrix} z_{s,2}(t) \\ \vdots \\ z_{s,k_1}(t) \\ 0 \end{bmatrix} = A \begin{bmatrix} z_{s,1}(t) \\ z_{s,2}(t) \\ \vdots \\ z_{s,k_1}(t) \end{bmatrix}$$

이며, A는 대각 원소 바로 위의 원소가 모두 1이며,

나머지 원소는 0인 행렬인,

제어기가 수행하는 동적 제어 데이터의 처리 방법.

[청구항 3] 청구항 1에 있어서,

k_1과 k_2는 같은 값인,

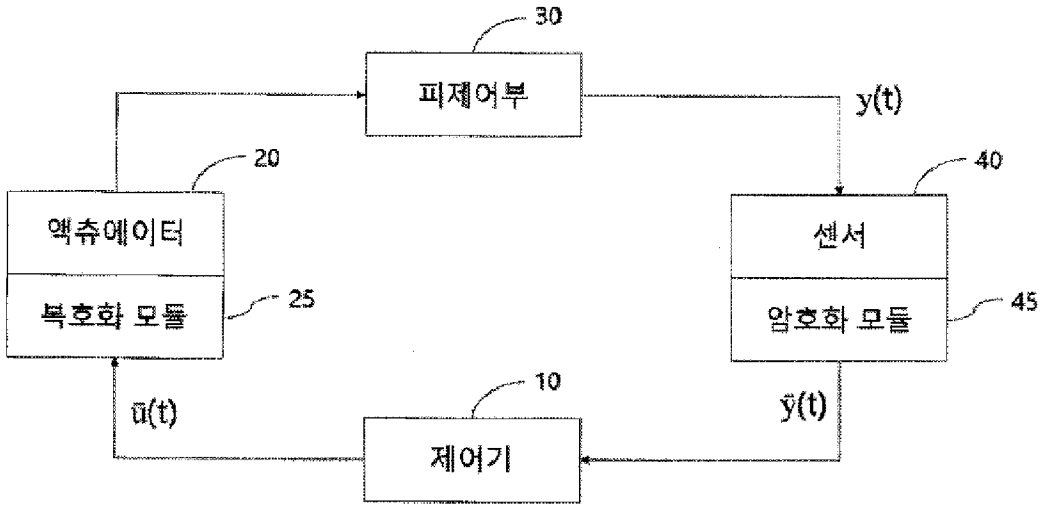
제어기가 수행하는 동적 제어 데이터의 처리 방법.

[청구항 4] 청구항 1 내지 청구항 3 중 어느 하나의 청구항에 기재된 방법의 단계를 실행하는 컴퓨터 프로그램이 기록된, 컴퓨터 판독 가능 기록 매체.

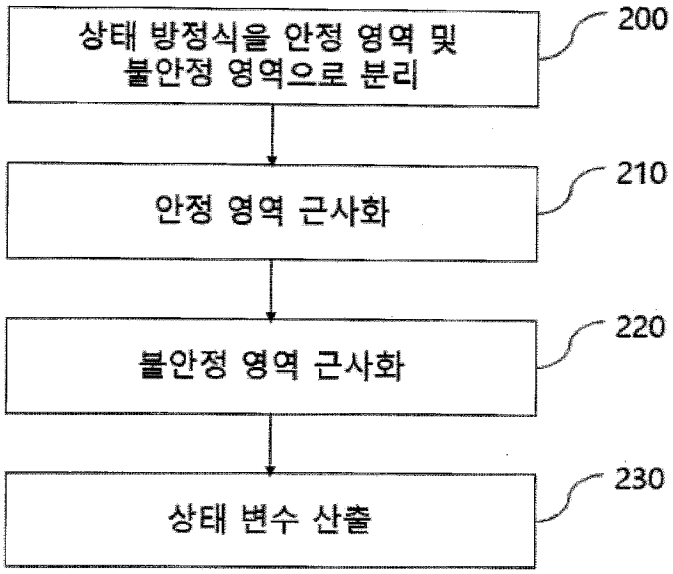
[청구항 5] 청구항 1 내지 청구항 3 중 어느 하나의 청구항에 기재된 방법의 단계를 실행하기 위해 컴퓨터 판독 가능 기록 매체에 기록된 컴퓨터 프로그램.

WO 2022/154241 PCT/KR2021/017080

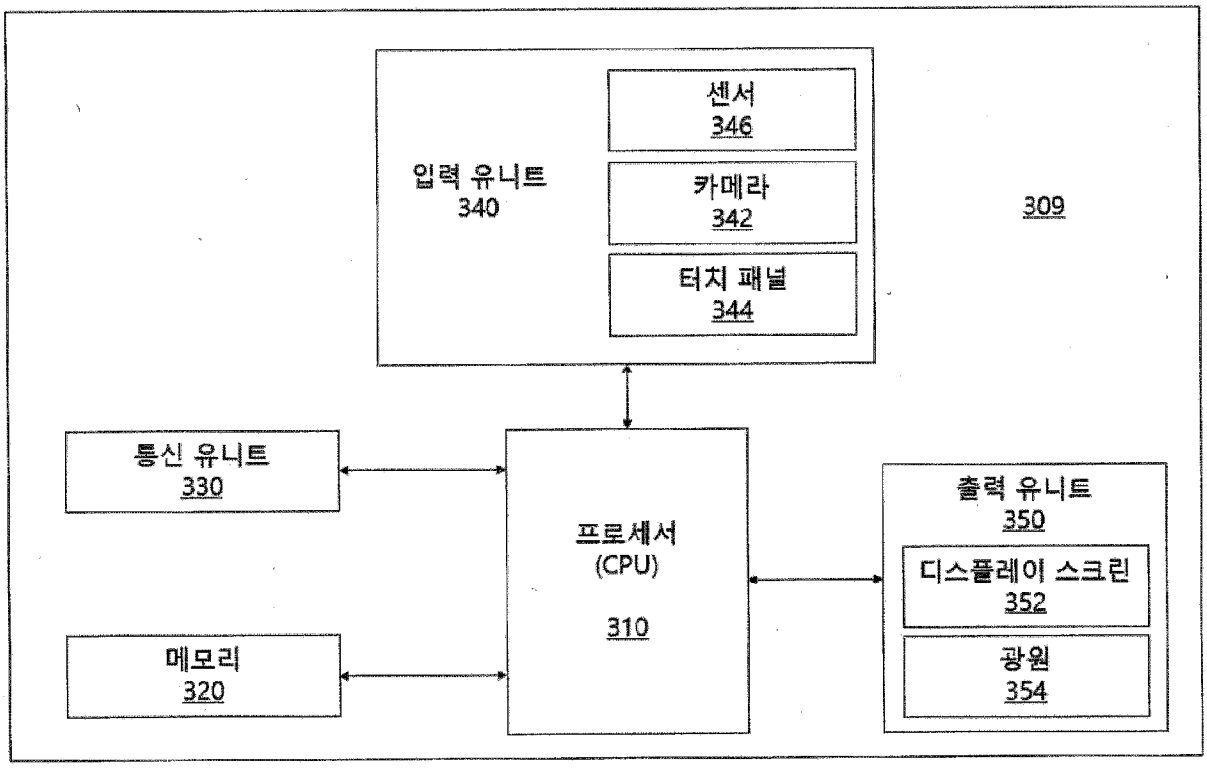
[도1]



[도2]



[도3]


센서
346
입력 유니트
340
카메라
342
309
터치 패널
344
통신 유니트
330
프로세서
(CPU)
310
출력 유니트
350
디스플레이 스크린
352
메모리
320
광원
354

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2021/017080

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/00(2006.01); H03M 7/30(2006.01); H04L 29/06(2006.01); H04L 9/12(2006.01); H04L 9/14(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & keywords: 동형 암호화(homomorphic encryption), 복호화(decryption), 액츄에이터(actuator), 센서(sensor), 제어기(controller), 동적 제어 데이터(dynamic control data)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2018-0092199 A (SEOUL NATIONAL UNIVERSITY R&DB FOUNDATION) 17 August 2018 (2018-08-17) See paragraphs [0063]-[0074]; and figure 2.	1-5
A	CHEON, Jung Hee et al. Need for Controllers Having Integer Coefficients in Homomorphically Encrypted Dynamic System. 2018 IEEE Conference on Decision and Control (CDC). pp. 5020-5025, 21 January 2019. See pages 5020-5023.	1-5
A	US 2019-0182216 A1 (THE GOVERNING COUNCIL OF THE UNIVERSITY OF TORONTO) 13 June 2019 (2019-06-13) See paragraphs [0145]-[0148]; and figure 2.	1-5
A	KR 10-2014-0114933 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 30 September 2014 (2014-09-30) See paragraphs [0021]-[0024]; and figure 1.	1-5

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 February 2022	**25 February 2022**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **Government Complex-Daejeon Building 4, 189 Cheongsa-ro, Seo-gu, Daejeon 35208**	
Facsimile No. **+82-42-481-8578**	Telephone No.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2014-0071605 A (SAMSUNG ELECTRONICS CO., LTD.) 12 June 2014 (2014-06-12) See paragraphs [0059]-[0076]; and figures 7-10.	1-5

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2021/017080

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
KR 10-2018-0092199 A	17 August 2018	KR 10-1919940 B1	19 November 2018
		US 10924262 B2	16 February 2021
		US 2019-0363872 A1	28 November 2019
		WO 2018-147497 A1	16 August 2018
US 2019-0182216 A1	13 June 2019	CA 3002582 A1	19 October 2017
		CN 109314641 A	05 February 2019
		EP 3443706 A1	20 February 2019
		EP 3443706 A4	25 September 2019
		JP 2019-514301 A	30 May 2019
		KR 10-2018-0127506 A	28 November 2018
		PH 12018502196 A1	16 September 2019
		SG 11201809010 TA	29 November 2018
		US 2017-0293913 A1	12 October 2017
		US 2019-0205875 A1	04 July 2019
		WO 2017-177313 A1	19 October 2017
KR 10-2014-0114933 A	30 September 2014	KR 10-1795771 B1	09 November 2017
		US 2014-0270159 A1	18 September 2014
		US 9374220 B2	21 June 2016
KR 10-2014-0071605 A	12 June 2014	CN 103856316 A	11 June 2014
		EP 2741529 A2	11 June 2014
		EP 2741529 A3	03 December 2014
		US 2014-0153724 A1	05 June 2014

국 제 조 사 보 고 서

국제출원번호
PCT/KR2021/017080

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/00(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 9/00(2006.01); H03M 7/30(2006.01); H04L 29/06(2006.01); H04L 9/12(2006.01); H04L 9/14(2006.01)

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 동형 암호화(homomorphic encryption), 복호화(decryption), 액츄에이터(actuator), 센서(sensor), 제어기(controller), 동적 제어 데이터(dynamic control data)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2018-0092199 A (서울대학교산학협력단) 2018.08.17 단락 [0063]-[0074]; 및 도면 2	1-5
A	JUNG HEE CHEON 등, `Need for Controllers Having Integer Coefficients in Homomorphically Encrypted Dynamic System', 2018 IEEE Conference on Decision and Control (CDC), 페이지 5020-5025, 2019.01.21 페이지 5020-5023	1-5
A	US 2019-0182216 A1 (THE GOVERNING COUNCIL OF THE UNIVERSITY OF TORONTO) 2019.06.13 단락 [0145]-[0148]; 및 도면 2	1-5
A	KR 10-2014-0114933 A (한국전자통신연구원) 2014.09.30 단락 [0021]-[0024]; 및 도면 1	1-5
A	KR 10-2014-0071605 A (삼성전자주식회사) 2014.06.12 단락 [0059]-[0076]; 및 도면 7-10	1-5

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☑ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"D" 본 국제출원에서 출원인이 인용한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2022년02월24일(24.02.2022)	**2022년02월25일(25.02.2022)**
ISA/KR의 명칭 및 우편주소 **대한민국 특허청** **(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)** 팩스 번호 **+82-42-481-8578**	심사관 **양정록** 전화번호 **+82-42-481-5709**

서식 PCT/ISA/210 (두 번째 용지) (2019년 7월)

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2021/017080

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2018-0092199 A	2018/08/17	KR 10-1919940 B1	2018/11/19
		US 10924262 B2	2021/02/16
		US 2019-0363872 A1	2019/11/28
		WO 2018-147497 A1	2018/08/16
US 2019-0182216 A1	2019/06/13	CA 3002582 A1	2017/10/19
		CN 109314641 A	2019/02/05
		EP 3443706 A1	2019/02/20
		EP 3443706 A4	2019/09/25
		JP 2019-514301 A	2019/05/30
		KR 10-2018-0127506 A	2018/11/28
		PH 12018502196 A1	2019/09/16
		SG 11201809010 TA	2018/11/29
		US 2017-0293913 A1	2017/10/12
		US 2019-0205875 A1	2019/07/04
		WO 2017-177313 A1	2017/10/19
KR 10-2014-0114933 A	2014/09/30	KR 10-1795771 B1	2017/11/09
		US 2014-0270159 A1	2014/09/18
		US 9374220 B2	2016/06/21
KR 10-2014-0071605 A	2014/06/12	CN 103856316 A	2014/06/11
		EP 2741529 A2	2014/06/11
		EP 2741529 A3	2014/12/03
		US 2014-0153724 A1	2014/06/05