(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2024 년 5 월 16 일 (16.05.2024)

WIPO | PCT

(10) 국제공개번호
WO 2024/101511 A1

(51) 국제특허분류:
H04L 9/32 (2006.01) *H04W 4/44* (2018.01)
H04L 9/30 (2006.01) *H04W 4/46* (2018.01)
H04W 12/06 (2009.01)

(21) 국제출원번호: PCT/KR2022/018928

(22) 국제출원일: 2022 년 11 월 28 일 (28.11.2022)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2022-0149004 2022 년 11 월 9 일 (09.11.2022) KR

(71) 출원인: 주식회사 시옷 **(CIOT CO., INC.)** [KR/KR]; 06626 서울특별시 서초구 서초대로74길 45, 14층, Seoul (KR).

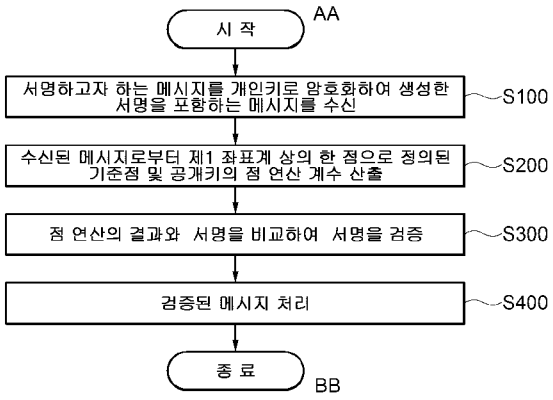
(72) 발명자: 박한나 **(PARK, Han Na)**; 02455 서울특별시 동대문구 회기로 85, 200동 207호, Seoul (KR). 정해일 **(JUNG, Hae Il)**; 06990 서울특별시 동작구 동작대로 29길 119, 106동 803호, Seoul (KR). 조성민 **(CHO, Sung Min)**; 05090 서울특별시 광진구 능동로4길 41, 704동 1703호, Seoul (KR).

(74) 대리인: 이장훈 **(LEE, Jang Hoon)**; 06173 서울특별시 강남구 테헤란로 623 6층 (삼성동,삼성빌딩), 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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD,

(54) Title: METHOD FOR VERIFYING SIGNATURE OF MESSAGE IN V2X COMMUNICATION ENVIRONMENT AND COMPUTING DEVICE FOR PERFORMING SAME

(54) 발명의 명칭: V2X 통신 환경에서 메시지의 서명 검증 방법 및 이를 수행하는 컴퓨팅 장치



S100 ... Receive message including signature generated by encrypting message, which is to be signed, with private key
S200 ... Obtain, from received message, reference point defined as point on first coordinate system and point operation coefficient of public key
S300 ... Verify signature by comparing result of point operation with signature
S400 ... Process verified message
AA ... Start
BB ... End

(57) Abstract: The present invention relates to a method for verifying a signature during transmission and reception of a message between computing devices. A method for verifying the signature of a message in a V2X communication environment, according to the present invention, comprises the steps of: receiving the message including a signature generated by encrypting the message to be signed with a private key; obtaining, from the received message, a reference point defined as a point on a first coordinate system and a point operation coefficient of a public key; and verifying the signature by comparing the result of a point operation according to the obtained coefficient with the signature. It is preferable that the signature is one value of signatures according to a message protocol,

WO 2024/101511 A1

[다음 쪽 계속]

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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))

which has been replaced with an inverse element. According to the present invention, accurate information can be quickly provided due to an improved verification speed even in a restricted environment.

(57) 요약서: 본 발명은 컴퓨팅 장치간 메시지 송수신 과정에서 서명을 검증하는 방법에 관한 것이다. 본 발명에 따른 V2X 통신 환경에서 메시지의 서명 검증 방법은 서명하고자 하는 상기 메시지를 개인키로 암호화하여 생성한 서명을 포함하는 상기 메시지를 수신하는 단계; 상기 수신된 메시지로부터 제1 좌표계 상의 한 점으로 정의된 기준점 및 공개키의 점 연산 계수를 산출하는 단계; 및 상기 산출된 계수에 따른 점 연산의 결과와 상기 서명을 비교하여 상기 서명을 검증하는 단계를 포함하고, 상기 서명은 메시지 프로토콜에 따른 서명 중 일 값을 역원으로 대체한 것이 바람직하다. 본 발명에 따르면, 보다 향상된 검증 속도를 통해 제약된 환경에서도 정확한 정보를 신속하게 제공받을 수 있다.

명세서

발명의 명칭: V2X 통신 환경에서 메시지의 서명 검증 방법 및 이를 수행하는 컴퓨팅 장치

기술분야

[1] 본 발명은 컴퓨팅 장치간 메시지 송수신 과정에서 서명을 검증하는 방법에 관한 것이다. 바람직하게는 차량 내 컴퓨터 장치와의 메시지 내 서명의 검증 방법에 관한 것이다.

배경기술

[2] IEEE 1609.2 는 WAVE (Wireless Access in Vehicular Environment) 기반의 차량간(V2V, Vehicle-to-Vehicle) 또는 차량과 인프라간(V2I, Vehicle-to-Infrastructure) 통신 상의 메시지를 보호하기 위한 프로토콜들을 정의하며 ECDSA 전자 서명 기법을 사용한다.

[3] ECDSA(Elliptic Curve Digital Signature Algorithm)는 타원곡선 이론에 기반한 공개 키 암호 방식으로 타원곡선 암호(elliptic curve cryptography; ECC)는 RSA 과 같은 기존 공개 키 암호 방식에 비하여 비교적 짧은 키를 사용하면서도 그와 비슷한 수준의 안전성을 제공한다는 장점이 있다.

[4] 따라서, 타원곡선 암호는 IoT(Internet of Thing) 장치와 같이 전송량과 리소스가 제한된 상황이나 고속 주행 중인 차량 통신 환경에 적합한 장점이 있으며, 이러한 이유로 RSA를 대체할 차세대 공개키 암호기술로 부상하고 있다.

[5] 즉, RSA 등의 기존의 공개키 암호 방식 (public key cryptosystem)에 비해 짧은 키 길이를 이용한 타원곡선 암호를 통한 디지털 서명 및 검증 방식은 자율주행을 위한 통신 프로토콜의 제한 내에서 상호 통신을 위한 과정에 응용되고 있다.

[6] 다만, 유한체에서 정의되는 타원곡선에 의한 서명/검증 방식은 일반적인 실수체의 연산에 비하여 높은 연산량을 요구하므로 이에 따라 보다 효율적인 검증 방법을 제공할 필요가 있다.

발명의 상세한 설명

기술적 과제

[7] 본 발명은 보다 향상된 검증 속도를 갖는 타원곡선 기반의 암호화 방법을 제안하는 것을 목적으로 한다.

[8] 또한, 본 발명은 환경에 따라 적합한 파라미터를 제공하는 암호화 방법을 제안하는 것을 목적으로 한다.

[9] 또한, 본 발명은 환경에 따라 보다 빠른 좌표계 변환 방법을 제안하는 것을 목적으로 한다.

[10] 또한, 본 발명은 자율주행 환경에서 표준 통신 프로토콜을 고려한 파라미터를 제공하는 암호화 방법을 제안하는 것을 목적으로 한다.

과제 해결 수단

[11] 상기 기술적 과제를 해결하기 위한 본 발명에 따른 V2X 통신 환경에서 메시지의 서명 검증 방법은 서명하고자 하는 상기 메시지를 개인키로 암호화하여 생성한 서명을 포함하는 상기 메시지를 수신하는 단계; 상기 수신된 메시지로부터 제1 좌표계 상의 한 점으로 정의된 기준점 및 공개키의 점 연산 계수를 산출하는 단계; 및 상기 산출된 계수에 따른 점 연산의 결과와 상기 서명을 비교하여 상기 서명을 검증하는 단계를 포함하고, 상기 서명은 메시지 프로토콜에 따른 서명 중 일 값을 역원으로 대체한 것이 바람직하다.

[12] 상기 메시지는 상기 일 값의 역원 대체 여부에 대한 식별자를 더 포함하는 것이 바람직하다.

[13] 상기 서명은 기준점의 점 연산 계수의 산출을 위한 일 값을 역원으로 대체한 것이 바람직하다.

[14] 상기 수신하는 단계는 상기 공개키에 대한 적어도 하나 이상의 스칼라 곱의 연산 결과를 수신하고, 상기 점 연산하는 단계는 상기 산출된 계수에 따라 점 연산 결과 또는, 상기 점 연산을 구성하는 하위 연산 중 적어도 일부를 미리 저장한 연산 테이블 내 값을 참조하여 연산을 수행하는 것이 바람직하다.

[15] 상기 연산 테이블은 제1 좌표계로 수신된 상기 공개키의 스칼라 곱의 연산 결과를 제2 좌표계로 변환하여 상기 연산 결과 리스트를 생성하고, 상기 연산 결과 리스트를 제1 좌표계로 변환하여 저장한 것이 바람직하다.

[16] 상기 서명은 임의의 난수에 따라 상기 제1 좌표계 상의 임의의 기준점을 스칼라 곱함으로써 생성되고, 상기 점 연산하는 단계는 상기 기준점과 상기 공개키를 상기 산출된 계수에 따라 점 연산하는 것이 바람직하다.

[17] 상기 기준점에 대한 스칼라 곱 결과 리스트는 미리 생성된 것이 바람직하다.

[18] 상기 기술적 과제를 해결하기 위한 본 발명에 따른 V2X 통신 환경에서 기본 안전 메시지의 서명 검증 을 수행하는 컴퓨팅 장치는 프로세서; 상기 프로세서에 의해 실행되는 컴퓨터 프로그램을 로드하는 메모리; 및

[19] 상기 컴퓨터 프로그램을 저장하는 스토리지를 포함하되, 상기 컴퓨터 프로그램은, 서명하고자 하는 상기 메시지를 개인키로 암호화하여 생성한 서명을 포함하는 상기 메시지를 수신하는 동작, 상기 수신된 메시지로부터 제1 좌표계 상의 한 점으로 정의된 기준점 및 공개키의 점 연산 계수를 산출하는 동작, 및 상기 산출된 계수에 따른 점 연산의 결과와 상기 서명을 비교하여 상기 서명을 검증하는 동작을 포함하고, 상기 서명은 메시지 프로토콜에 따른 서명 중 일 값을 역원으로 대체한 것이 바람직하다.

[20] 상기 메시지는 상기 일 값의 역원 대체 여부에 대한 식별자를 더 포함하는 것이 바람직하다.

[21] 상기 서명은 기준점의 점 연산 계수의 산출을 위한 일 값을 역원으로 대체한 것이 바람직하다.

[22] 상기 수신하는 동작은 상기 공개키에 대한 적어도 하나 이상의 스칼라 곱의 연산 결과를 수신하고, 상기 점 연산하는 동작은 상기 산출된 계수에 따라 점

연산 결과 또는, 상기 점 연산을 구성하는 하위 연산 중 적어도 일부를 미리 저장한 연산 테이블 내 값을 참조하여 연산을 수행하는 것이 바람직하다.

[23] 상기 연산 테이블은 제1 좌표계로 수신된 상기 공개키의 스칼라 곱의 연산 결과를 제2 좌표계로 변환하여 상기 연산 결과 리스트를 생성하고, 상기 연산 결과 리스트를 제1 좌표계로 변환하여 저장한 것이 바람직하다.

[24] 상기 서명은 임의의 난수에 따라 상기 제1 좌표계 상의 임의의 기준점을 스칼라 곱함으로써 생성되고, 상기 점 연산하는 동작은 상기 기준점과 상기 공개키를 상기 산출된 계수에 따라 점 연산하는 것이 바람직하다.

[25] 상기 기준점에 대한 스칼라 곱 결과 리스트는 미리 생성된 것이 바람직하다.

발명의 효과

[26] 본 발명에 따르면, 보다 향상된 검증 속도를 통해 제약된 환경에서도 정확한 정보를 신속하게 제공받을 수 있다.

[27] 또한, 본 발명은 환경에 따라 최적화된 파라미터를 통해 보다 안정성 높은 정보의 송수신이 가능하다.

[28] 또한, 본 발명은 표준 통신 프로토콜 내에서 제공되는 정보를 통해 향상된 연산을 수행하고 이종 환경의 인프라나 다른 사용자들과도 메시지를 안전하게 송수신 할 수 있도록 한다.

도면의 간단한 설명

[29] 도 1은 본 발명의 일 실시예에 따른 V2X 통신 환경에서 수행되는 서명 검증 방법이 적용되는 환경을 나타낸 예시도이다.

[30] 도 2는 본 발명의 일 실시예에 따른 V2X 통신 환경에서 수행되는 인증서 기반의 서명 검증 방법을 나타내는 예시도이다.

[31] 도 3은 본 발명의 일 실시예에 따른 V2X 통신 환경에서 타원곡선 기반의 디지털 서명의 생성을 위한 수도 코드를 나타낸 예시도이다.

[32] 도 4은 본 발명의 일 실시예에 따른 V2X 통신 환경에서 수행되는 서명 검증 방법을 나타내는 흐름도이다.

[33] 도 5는 본 발명의 일 실시예에 따른 V2X 통신 환경에서 수행되는 서명 검증 방법의 세부 과정을 나타낸 흐름도이다.

[34] 도 6은 본 발명의 일 실시예에 따른 V2X 통신 환경에서 수행되는 서명의 검증을 위한 수도 코드를 나타낸 예시도이다.

[35] 도 7은 본 발명의 일 실시예에 따른 V2X 통신 환경에서 수행되는 서명 데이터의 구성을 나타내는 예시도이다.

[36] 도 8은 본 발명의 일 실시예에 따른 V2X 통신 환경에서 수행되는 서명 검증 방법의 연산 테이블 생성 예를 나타낸 예시도이다.

[37] 도 9는 본 발명의 일 실시예에 따른 V2X 통신 환경에서 수행되는 메시지의 송수신예를 나타낸 예시도이다.

[38] 도 10은 본 발명의 일 실시예들에 따른 서명 검증 방법을 수행하는 컴퓨팅 장치

형태의 구현을 나타낸 예시도이다.

발명의 실시를 위한 형태

[39] 이하의 내용은 단지 발명의 원리를 예시한다. 그러므로 당업자는 비록 본 명세서에 명확히 설명되거나 도시 되지 않았지만 발명의 원리를 구현하고 발명의 개념과 범위에 포함된 다양한 장치를 발명할 수 있는 것이다. 또한, 본 명세서에 열거된 모든 조건부 용어 및 실시 예들은 원칙적으로, 발명의 개념이 이해되도록 하기 위한 목적으로만 명백히 의도되고, 이외같이 특별히 열거된 실시 예들 및 상태들에 제한적이지 않는 것으로 이해되어야 한다.

[40] 상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해질 것이며, 그에 따라 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다.

[41] 또한, 발명을 설명함에 있어서 발명과 관련된 공지 기술에 대한 구체적인 설명이 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하에는 첨부한 도면을 참조하여 본 발명의 바람직한 실시 예에 대해 상세하게 설명한다.

[42] 도 1은 본 발명의 일 실시예에 따른 고속 서명 검증 방법이 수행되는 환경을 예시하는 예시도이다.

[43] 도 1을 참고하면, 일 실시예에서 본 발명에 따른 고속 서명 검증 방법은 주행중인 차량(200)을 중심으로 차량(200)이 다른 차량(200) 또는 노변 인프라 RSU(Road Side Unit)(400)와 통신을 수행하는 환경에 적용될 수 있다.

[44] 각 수신 주체는 내부의 컴퓨팅 장치(300) 예를 들어 차량의 OBU(On-Board Unit)를 통해 표준 규약된 통신 프로토콜 상에서 수신되는 정보 내에서 파라미터를 추출하고 디지털 서명으로 암호화된 메시지를 검증함으로써 해당 메시지에 대한 처리를 수행한다.

[45] 와이파이 기반의 웨이브(WAVE, Wireless Access in Vehicle Environments)에서 정의된 표준 프로토콜을 통해 고속으로 주행하는 차량(200)은 복잡한 교통상황에서 정보를 교환할 수 있으며, 외부의 클라우드 서버(300)로부터 기지국(30)을 통해 다양한 실시간 정보를 수집하여 주행에 활용할 수 있도록 한다.

[46] IEEE 1609.2 는 WAVE (Wireless Access in Vehicular Environment) 기반의 차량간(V2V, Vehicle-to-Vehicle) 또는 차량과 인프라간(V2I, Vehicle-to-Infrastructure) 통신 상의 메시지를 보호하기 위한 프로토콜들을 정의하며 타원곡선 암호 방식을 사용할 수 있다.

[47] IEEE 1609.2 에서 이용되는 기본 안전 메시지(BSM, Basic Safety Message)(500)는 SAE J2735에서 정의된다. 도 1과 같이 특정 노변 장치(400)로 초당 10개의 메시지가 송신되는 경우 메시지의 서명의 검증을 위해서는 적어도 초당 50개 이상의 검증속도가 필요할 수 있으며 고속도로 환경이나 보다 넓은 다

차로 환경에서는 더욱 빠른 검증속도가 필요할 수 있다.

[48] 이를 위해, IEEE 1609.2 는 WAVE 기반의 통신 환경을 위해 암호화를 위해서 이용되는 키의 길이가 상대적으로 짧은 타원곡선 암호 방식을 적용할 수 있다. 즉, 타원곡선을 통한 디지털 서명 및 검증 방식이 자율주행 환경에서 메시지를 송수신 하는 데 이용될 수 있다.

[49] 도 2를 참고하면, 본 실시예에 따른 서명의 검증 과정은 서명 데이터(510)로부터 추출되는 서명자(Signer) ID(512)와 서명(Signature)(514)을 통해 검증을 수행할 수 있다.

[50] 서명 데이터(510) 내 서명자 ID(512)는 대응되는 인증서(520-N)로부터 서명에 이용된 해시 함수 등의 알고리즘을 식별할 수 있도록 하며, 인증서(520-N)의 공개키(524)를 통해 메시지로부터 복호화된 정보와 서명을 비교함으로써 검증을 수행할 수 있다.

[51] 나아가, 본 실시예에서 인증서(520-1…520-N)들은 계층적인 구조를 가질 수 있으며 하위 인증서는 발행자(Issuer) 식별자(522)를 통해 상위 인증서를 식별하고 상위 인증서의 공개키를 통해 자신의 서명을 검증하는 과정을 최상위 인증서 까지 연쇄적으로 수행할 수 있다.

[52] 이때, 서명의 검증 과정에서 효율적인 연산을 위해서 IEEE 1609.2 는 타원곡선 암호 방식을 적용하고 있으며 검증에 필요한 타원곡선을 정의하는 도메인 파라미터 들은 서명 데이터(510) 내에 포함될 수 있다.

[53] 타원곡선 암호화를 통한 서명과 검증과정에 대하여 먼저 설명하면, 타원곡선을 통한 디지털 서명 알고리즘 ECDSA(Elliptic Curve Digital Signature Algorithm)는 디지털 서명의 한 방법으로 타원 곡선을 이용하여 디지털 기반의 서명을 수행하는 알고리즘이다.

[54] ECDSA는 문자 그대로 타원 곡선에 기반하여 디지털 서명을 수행한다. 타원곡선은 $y2 = x3 + ax + b$ 형태의 비교적 간단한 형태의 방정식으로 정의될 수 있으나, 타원 곡선을 사용하는 암호화 기술은 실수체와 달리 소수체의 유한체(Finite Field)를 이용하므로 일방향성을 가질 수 있다.

[55] 유한체에서 정의된 타원 곡선 상의 한 시작점(base point)에서 반복적인 곱셈 연산을 수행했을 때 곱셈의 결과에 따른 종료점은 쉽게 구할 수 있지만, 시작점과 종료점 만을 아는 상태에서 시작점에서 얼마 횟수의 곱셈 연산을 수행해야 하는지는 역으로 유추하기 어렵다는 일방향성을 디지털 서명에 이용한다.

[56] 즉 ECDSA 역시 비대칭키로 개인키(private key)와 공개키(public key)를 상술한 유한체 상에서 쌍으로 생성하며, 개인키를 통해 암호화된 메시지와 서명을 수신측에서 수신하면 메시지를 공개키를 통해 복호화하고 서명과 복호화된 값을 비교함으로써 서명의 진위 여부를 검증한다.

[57] 구체적으로 본 실시예에 따른 ECDSA의 서명 생성 과정을 도 3에서 예시된 수도 코드(Pseudo Code)를 참고하여 설명하면 ECDSA는 도메인 파라미터 D는

타원곡선을 정의하는 계수 a,b 및 생성자로 기준점 P와 위수 n으로 구성될 수 있다.

[58] 먼저, 위수 n 을 사용하여 1 ~ n-1 까지의 정수 중 랜덤하게 발생된 난수 k를 선택하는 것으로 서명 과정은 수행된다(Step1). ECDSA의 공개키(Q)는 난수 k를 유한체 상의 기준점(P)와 곱하는 형태로 Q = k*P 를 통해 생성되며, Q의 x축 좌료 값 x1은 정수로 변환될 수 있다.(Step2).

[59] 이때, Q = k*P 는 일반적인 실수계 연산과 달리 점 가산 (point addition; PA) 및 점 두배 (point doubling; PD) 연산의 반복으로 계산될 수 있으며 유한 좌표계 상에서 점 가산과 점 두배의 연산에는 연산 소요 사이클이 비교적 큰 역원 연산이 포함될 수 있다.

[60] 다만 이러한 연산의 부하는 반복적인 서명을 수행하는 송신 측에 비하여 서명을 수신하여 제공된 공개키를 통해 검증하는 측에서 영향이 더 크게 나타나므로 본 실시예에 따른 고속 서명 검증 방법은 이를 해결하기 위한 방법을 제안한다.

[61] 이어서, Q의 유한체 상의 좌표는 모듈로 연산을 통해서 도메인 파라미터 n 내에 정의될 수 있다(Step3). 이때, 모듈로 연산의 결과는 디지털 서명의 값 r로 이용된다.

[62] 다음, 암호화하여 보내고자 하는 메시지 m은 해시함수 H()를 통해 생성된 해시값 e로 생성되며(Step 4) 디지털 서명의 다른 값 s^{-1}는 해시값 e, 개인키 d, 산출된 r, 및 난수 k의 연산에 대한 모듈로 값으로 생성될 수 있다(Step5).

[63] 이때, s^{-1}는 서명의 검증 과정에서 기준점 p의 스칼라 곱 계수를 결정하는데 이용되며 구체적으로 IEEE 1609.2 에서 정의된 서명 중 요소 s에 대한 역원 s^{-1}을 검증하는 측에서 산출하여 계수를 결정할 때의 부하를 줄이기 위해 역원으로 미리 계산하여 제공하도록 한다.

[64] 생성된 서명 r 및 s의 역원 s^{-1}를 리턴하는 것으로 디지털 서명 과정은 종료된다(Step6).

[65] 이어서, 서명과 메시지를 수신한 측에서는 수신된 메시지를 복호화함으로써 서명의 진위 여부를 검증한다.

[66] 이에 대해서는 도 4를 참고하여 설명한다.

[67] 도 4를 참고하면, 본 실시예에 따른 고속 서명 검증 방법을 수행하는 수신측의 컴퓨팅 장치(300)는 서명하고자 하는 메시지를 개인키로 암호화하여 생성한 서명과 상기 메시지를 수신한다(S100).

[68] 이때, 도 5를 참고하면 본 실시예에 따른 컴퓨팅 장치(300)는 메시지 프로토콜에 따른 서명 중 일 값을 역원을 대체한 값 수신할 수 있다(S110)

[69] 다음, 수신된 메시지를 이용하여 수신된 메시지로부터 제1 좌표계 상의 한 점으로 정의된 기준점 및 공개키의 점 연산 계수 산출하되(S200), 본 실시예에 따른 컴퓨팅 장치(300) 는 역원 s^{-1}를 포함하는 서명을 통해 점 연산, 바람직하게는 스칼라 곱의 횟수를 정의하는 계수를 보다 효율적으로 산출할 수

있다(S210).

[70] 도 6에 따른 수도 코드를 통해 보다 상세하게 설명하면, 서명 검증은 메시지(m)와 서명(r, s^{-1})를 받아들여 공개키(Q)로 복호화 함으로써 수행된다.

[71] 먼저, 컴퓨팅 장치(300)는 서명을 유효성을 검증한다(Step1.) 구체적으로 r, s^{-1}의 범위가 $0 < r < n$, $0 < s^{-1} < n$ 인지 체크한다.

[72] 유효한 서명인 경우 서명 생성 과정에서 해싱한 것과 마찬가지로 메시지를 해시함수 H()를 통해 해싱하여 해시 값 e를 생성한다(Step2.) 이때 이용된 해시함수에 대한 식별은 상술한 도 2의 서명자 ID를 통해 식별할 수 있다.

[73] 이어서, 검증을 위한 계수의 산출을 위한 매개 값으로 서명 내 일 값 s의 역원에 대한 모듈로 값으로 $w(w = s^{-1} \bmod n)$를 계산한다(Step 3.).

[74] 본 실시예에서는 서명의 요소 중 s를 역원 s^{-1}로 대체하여 수신하였으므로 부가적인 역원 연산 없이 w를 산출할 수 있다.

[75] 다음 구체적인 계수로 두 점 기준점 P에 대한 계수 $u1(u1 = e*w \bmod n)$과 공개키 Q에 대한 계수 $u2(u2 = r*w \bmod n)$를 각각 해시 값 e과 매개 값 w 및 서명 값 중 r을 이용하여 생성한다(Step4).

[76] 서명의 검증을 위해서는 산출된 계수에 따라 각 기준점의 스칼라 곱 연산과 산출된 결과의 가산 연산을 수행한다(Step5.)

[77] 추출된 P와 Q의 계수에 대한 스칼라 곱 결과를 가산함으로써 검증을 위한 $X(X(x1, y1) = (u1*P + u2*Q))$를 산출할 수 있다(Step5.).

[78] 추가적으로 X의 유효성을 검증하기 위해 산출된 (x1, y1)가 무한원점(O)이면 잘못된 서명이므로 거절(“Reject Signature”)하되(Step6.), 유효한 경우 추가적인 모듈로 연산을 통해 최종 피 검증값 $v(v = x1 \bmod n)$를 생성한다(Step 7.).

[79] 최종 검증은 산출된 피 검증값 v와 서명의 r을 비교하여 v와 r이 동일하면 서명의 검증을 완료(“Accept Signature”)하고 그렇지 않은 경우 거절한다(Step 8.)

[80] 이때, 본 실시예에 따른 서명 데이터는 타원곡선을 통해 생성된 서명 (r,s) 중 s를 역원으로 대체하므로 이에 대한 식별자 정보를 포함할 수 있다.

[81] 도 7을 참조하면, 서명 데이터(510)는 도 2에서 상술한 서명자 ID(512) 및 서명(514)외에 해시 함수에 대한 식별자를 해시 ID(513)로 포함할 수 있다.

[82] 서명의 대상이 되는 대상 데이터(515)는 시퀀스 형태의 메시지 구조로써, 서명 값을 생성 또는 검증할 때 이용되는 해시되는 데이터를 포함할 수 있다. 나아가 대상 데이터(515)에는 선택적으로 확장 가능한 데이터 필드가 추가될 수 있으며 부가 데이터로 본 실시예에 따른 서명 요소 중 s가 역원으로 대체되었음을 식별자 플래그로 포함할 수 있다.

[83] 따라서, 서명(514)은 구체적으로 ECDSA 에 따른 서명으로 r 및 대체된 s^{-1}를 포함한다.

[84] 나아가 본 실시예에는 산출된 계수에 따른 점 연산의 효율적인 연산을 위해 점 연산 결과 또는, 상기 점 연산을 구성하는 하위 연산 중 적어도 일부를 미리 저장한 연산 테이블 내 값을 참조하여 연산을 수행할 수 있다.

[85] 상술한 바와 같이 유한체로 정의된 제1 좌표계 상의 점 연산은 일반적인 실수계 연산과 달리 수행되며, 따라서 보다 복잡한 연산 과정을 요하게 된다.

[86] 따라서, 본 실시예에 따른 컴퓨팅 장치(300)는 산출된 계수에 따라 점 연산 결과 또는, 상기 점 연산을 구성하는 하위 연산 중 적어도 일부를 미리 저장한 연산 테이블 내 값을 참조하여 연산을 수행함으로써 일부 연산 과정을 생략하고 보다 빠른 연산을 수행할 수 있다.

[87] 구체적으로 점 연산의 스칼라 곱은 점 가산과 점 두배 연산의 조합으로 구성될 수 있으며 하위 연산은 점 연산을 구성하는 점 가산 연산을 기준으로 구분할 수 있다.

[88] 구체적으로 기준점 P의 순차적인 스칼라 곱의 연산 결과는 고정될 수 있으므로 미리 서명자가 생성하고 제공할 수 있다.

[89] 또한, 공개키 Q에 대해서는 지정된 범위에서 순차적인 스칼라 곱의 연산 결과를 리스트로 생성하여 테이블로 저장하며 따라서, 해당되는 계수에 대한 연산 결과를 테이블에서 직접 참조함으로써 보다 효율적으로 검증 과정을 수행할 수 있다.

[90] 바람직하게 본 실시예에서 연산 테이블은 순차적인 홀수 계수를 갖는 스칼라 곱의 연산 결과 리스트를 테이블로 생성하여 저장할 수 있다.

[91] 즉, 컴퓨팅 장치(300)가 전체 계수에 따른 테이블의 절반의 크기를 이용하되 산출된 계수에 따른 하위 연산을 홀수 계수를 갖는 스칼라 곱의 가산(감산)으로 구성함으로써 테이블을 참조한 고속 연산이 가능하도록 한다.

[92] 도 8을 참고하면, 본 실시예에서 연산 테이블에 저장되는 연산 결과 리스트 중에서 공개키 Q와 공개키 Q의 점 두배 연산 결과 2Q는 미리 수신되어 메모리에 저장될 수 있으며 따라서, 이에 대한 연산 과정은 생략될 수 있다.

[93] 3Q는 Q와 2Q의 점 가산 연산으로 구성될 수 있으며, 5Q는 앞서 산출된 3Q와 산출된 2Q의 가산으로 수행될 수 있다.

[94] 또한, 이를 위해 이용되는 2Q의 경우 도 7에 따른 서명 데이터(51) 내 대상 데이터(515)의 확장 가능한 데이터 필드가 추가될 수 있으며 부가 데이터에 포함하여 전송될 수 있다.

[95] 이상 컴퓨팅 장치(300)는 공개키의 순차적인 스칼라 곱의 연산 결과를 테이블로 생성할 수 있다. 이때 생성하고자 하는 연산 결과 리스트의 크기는 송수신되는 메시지의 특성에 따라 결정될 수 있다.

[96] 나아가 연산 결과 리스트의 보다 빠른 생성을 위하여 생성과정은 혼합 좌표계를 이용하여 수행될 수 있다.

[97] 컴퓨팅 장치(200)에서 연산을 위해 이용되는 Q는 일반적인 유한 좌표계 상의 점으로 정의되므로 연산 테이블의 생성 과정에서 보다 빠른 점 연산을 위해 유한 좌표계를 투영한 투영 좌표계를 추가적으로 이용하여 스칼라 곱 연산을 수행할 수 있다.

[98] 바람직하게는 유한 좌표계의 수신된 점 Q의 일 좌표 값 (x,y)를 (x,y,z=1)로 투영

좌표계로 변환하여 연산 결과 리스트를 생성한다.

[99] 이상의 과정으로 생성된 연산 테이블의 값들은 투영 좌표계의 값을 가지므로 검증을 위해서는 다시 유한 좌표계의 값으로 변환이 필요하다.

[100] 본 실시예에서 좌표계의 변환은 연산 테이블 내 값들의 역원을 이용하여 연산될 수 있다. 하지만, 역원 연산은 일반적으로 복잡한 연산과정에 따라 많은 리소스를 필요로 하므로 컴퓨팅 장치(300)는 생성된 연산 테이블의 좌표계 변환을 위한 역원을 추가로 제공받을 수 있다.

[101] 따라서, 본 실시예에서 컴퓨팅 장치(300)는 선택된 투영 좌표계에 따른 연산 테이블이 생성되면, 수신된 역원을 이용하여 유한 좌표계로 테이블을 변환한다.

[102] 이때, 본 실시예에서 컴퓨팅 장치(300)는 연산 테이블의 값들에 대한 전체 역원을 제공하는 대신 테이블 내 전체 값들의 곱에 따른 통합 역원을 제공하고, 통합 역원을 통한 관계식으로 각 세부 값들의 좌표계를 순차적으로 변환하도록 함으로써 좌표계 변환 과정을 효율화 할 수 있다.

[103] 이상 본 실시예에 따른 고속 서명 검증 과정은 서명 검증에 소요되는 연산의 효율화를 위해 송신측에서 제공된 서명 s의 역원과 공개키 P의 연산 결과 리스트 및 Q의 일부 연산 결과를 이용하여 순차적인 연산 결과 리스트를 연산 테이블로 생성하여 저장하는 것을 통해 연산의 효율화를 꾀할 수 있으므로, Q의 연산 테이블의 생성에 투영 좌표계(바람직하게는 자코비안(Jacobian) 좌표계)를 이용함으로써 보다 빠르게 연산 리스트를 생성할 수 있다.

[104] 이상 본 실시예에 따른 컴퓨팅 장치(300)는 점 연산을 구성하는 하위 연산을 연산 테이블을 참조하여 스칼라 곱 결과를 산출할 수 있다.

[105] 다음, 산출된 계수에 따라 상술한 서명 과정에서 개인키로부터 유한체로 정의된 제1 좌표계 상의 한 점으로 생성된 공개키와 기준점의 점 연산 결과를 참조하고 수신된 서명을 검증한다(S300).

[106] 이상의 과정을 통해 서명의 검증되면 검증된 메시지를 수신 측의 컴퓨팅 장치(300)에서 처리한다(S400). 예를 들어, 메시지에 포함된 정보를 이용하여 자율주행에 반영함으로써 보다 안전한 주행을 수행할 수행하거나 자율주행 차량에 탑승한 승객에게 부가적인 정보를 제공해 줄 수 있다.

[107] 도 9를 참조하면, 본 실시예에 따른 고속 서명 검증 방법은 자율주행 환경에 적용될 수 있다.

[108] 일 예로 클라우드 서버(300)와 차량(200) 간의 통신에서 클라우드 서버(300)는 메시지와 함께 실시간으로 대용량의 데이터들을 스트리밍 형태로 제공할 수 있으므로 메시지 #1와 함께 복수의 스칼라 곱 결과(Q,2Q)를 미리 제공함으로써 차량(200) 내에서의 검증에 드는 리소스를 줄이도록 한다. 차량(200)에서는 빈번한 통신에도 효율적으로 생성된 연산 테이블을 재사용함으로써 정보를 수신할 수 있다.

[109] 또한, 도로 인프라(400) 간 차량(200) 간의 통신의 경우 주행 도로에 인접한 각각의 노변 장치(RSU, Road Side Unit)와 통신을 지속적으로 수행하므로 생성된

연산 테이블의 재사용 가능성이 높으므로 인프라(400)에서 미리 연산된 공개키의 스칼라 곱을 복수(Q,2Q)로 포함하는 메시지 #2로 제공함으로써 차량(200)에서 연산 테이블을 효율적으로 생성하도록 하는 것도 가능하다.

[110] 이어서, 차량(200)과 차량(200)간의 통신은 예를 들어 전방 차량(200)의 이상 상태나 전방 차량(200)에서 판단한 상황을 후방 추종 차량(200)들에게 통지하기 위한 방향으로 이루어질 수 있으며, 긴급성을 요하므로 보다 가용 리소스가 작은 차량(200)에서 빠른 검증을 위해 메시지와 함께 복수의 스칼라 곱 결과(Q,2Q)와 역원 s^{-1}을 메시지 #3와 함께 제공하는 것도 가능하다. 즉, 역원을 직접 제공함으로써 검증을 보다 빠르게 수행할 수 있도록 한다.

[111] 또한, 차량(200)이 사용자의 단말(UE, User Equipment)과 통신하는 것도 가능하며 셔틀 서비스를 위해 사용자의 단말에게 차량(200)의 접근을 알리는 형태로 통신을 수행하는 것도 가능하다.

[112] 따라서 차량(200)은 차량(200)의 위치를 실시간으로 안내하기 위해 메시지 #4와 함께 공개키의 복수의 스칼라 곱 결과(Q, 2Q)와 역원 s^{-1}를 제공할 수 있으며 사용자 단말은 수신된 스칼라 곱 결과로부터 연산 테이블을 생성하여 검증을 수행할 수 있다.

[113] 또는 차량(200)이 횡단보도에 진입하는 경우와 같이 긴급성을 요하는 경우에는 추가적인 스칼라 곱 결과와 역원을 함께 보행자의 사용자 단말에 제공하는 것도 가능하며 상황에 따라 선택적으로 송신하는 파라미터를 결정할 수 있다.

[114] 이하, 본 발명의 일 실시예에 따른 고속 서명 검증을 수행하는 컴퓨팅 장치(300)의 구체적인 하드웨어 구현에 대하여 설명한다.

[115] 도 10을 참조하면, 본 발명의 몇몇 실시예들에서 컴퓨팅 장치(300)는 컴퓨팅 장치의 형태로 구현될 수 있다. 컴퓨팅 장치(300)를 구성하는 각각의 모듈 중 하나 이상은 범용 컴퓨팅 프로세서 상에서 구현되며 따라서 프로세서(processor)(308), 입출력 I/O(302), 메모리 (memory)(340), 인터페이스(interface)(306) 및 버스(314, bus)를 포함할 수 있다. 프로세서(308), 입출력 장치(302), 메모리 (340) 및/또는 인터페이스(306)는 버스(314)를 통하여 서로 결합될 수 있다. 버스(314)는 데이터들이 이동되는 통로(path)에 해당한다.

[116] 구체적으로, 프로세서(308)는 CPU(Central Processing Unit), MPU(Micro Processor Unit), MCU(Micro Controller Unit), GPU(Graphic Processing Unit), 마이크로프로세서, 디지털 신호 프로세스, 마이크로컨트롤러, 어플리케이션 프로세서(AP, application processor) 및 이들과 유사한 기능을 수행할 수 있는 논리 소자들 중에서 적어도 하나를 포함할 수 있다.

[117] 입출력 장치(302)는 키패드(keypad), 키보드, 터치스크린 및 디스플레이 장치 중 적어도 하나를 포함할 수 있다. 메모리 장치(340)는 데이터 및/또는 프로그램 등을 저장할 수 있다.

[118] 인터페이스(306)는 통신 네트워크로 데이터를 전송하거나 통신 네트워크로부터 데이터를 수신하는 기능을 수행할 수 있다. 인터페이스(306)는

유선 또는 무선 형태일 수 있다. 예컨대, 인터페이스(306)는 안테나 또는 유무선 트랜시버 등을 포함할 수 있다. 메모리 (340)는 프로세서(308)의 동작을 향상시키되, 개인정보의 보호를 위한 휘발성의 동작 메모리로서, 고속의 디램 및/또는 에스램 등을 더 포함할 수도 있다.

[119] 또한, 메모리(340) 내에는 여기에 설명된 일부 또는 모든 모듈의 기능을 제공하는 프로그래밍 및 데이터 구성을 저장한다. 예를 들어, 상술한 검증 방법의 선택된 양태들을 수행하도록 하는 로직을 포함할 수 있다.

[120] 메모리 (340)에 저장된 상술한 검증 방법을 수행하는 각 단계를 포함하는 명령어들의 집합으로 프로그램 또는 어플리케이션을 로드하고 프로세서가 각 단계를 수행할 수 있도록 한다. 예를 들어, 서명하고자 하는 상기 메시지를 개인키로 암호화하여 생성한 서명을 포함하는 상기 메시지를 수신하는 동작, 상기 수신된 메시지로부터 제1 좌표계 상의 한 점으로 정의된 기준점 및 공개키의 점 연산 계수를 산출하는 동작, 및 상기 산출된 계수에 따른 점 연산의 결과와 상기 서명을 비교하여 상기 서명을 검증하는 동작 등이 포함된 컴퓨터 프로그램이 프로세서에 의해 각 수행될 수 있다.

[121] 나아가, 여기에 설명되는 다양한 실시예는 예를 들어, 소프트웨어, 하드웨어 또는 이들의 조합된 것을 이용하여 컴퓨터 또는 이와 유사한 장치로 읽을 수 있는 기록매체 내에서 구현될 수 있다.

[122] 하드웨어적인 구현에 의하면, 여기에 설명되는 실시예는 ASICs (application specific integrated circuits), DSPs (digital signal processors), DSPDs (digital signal processing devices), PLDs (programmable logic devices), FPGAs (field programmable gate arrays, 프로세서(processors), 제어기(controllers), 마이크로 컨트롤러(micro-controllers), 마이크로 프로세서(microprocessors), 기타 기능 수행을 위한 전기적인 유닛 중 적어도 하나를 이용하여 구현될 수 있다. 일부의 경우에 본 명세서에서 설명되는 실시예들이 제어 모듈 자체로 구현될 수 있다.

[123] 소프트웨어적인 구현에 의하면, 본 명세서에서 설명되는 절차 및 기능과 같은 실시예들은 별도의 소프트웨어 모듈들로 구현될 수 있다. 상기 소프트웨어 모듈들 각각은 본 명세서에서 설명되는 하나 이상의 기능 및 작동을 수행할 수 있다. 적절한 프로그램 언어로 씌여진 소프트웨어 어플리케이션으로 소프트웨어 코드가 구현될 수 있다. 상기 소프트웨어 코드는 메모리 모듈에 저장되고, 제어모듈에 의해 실행될 수 있다.

[124] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위 내에서 다양한 수정, 변경 및 치환이 가능할 것이다.

[125] 따라서, 본 발명에 개시된 실시 예 및 첨부된 도면들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시 예 및 첨부된 도면에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의

보호 범위는 아래의 청구 범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리 범위에 포함되는 것으로 해석되어야 할 것이다

청구범위

[청구항 1] V2X 통신 환경에서 메시지의 서명 검증 방법에 있어서,
서명하고자 하는 상기 메시지를 개인키로 암호화하여 생성한 서명을 포함하는 상기 메시지를 수신하는 단계;
상기 수신된 메시지로부터 제1 좌표계 상의 한 점으로 정의된 기준점 및 공개키의 점 연산 계수를 산출하는 단계; 및
상기 산출된 계수에 따른 점 연산의 결과와 상기 서명을 비교하여 상기 서명을 검증하는 단계를 포함하고,
상기 서명은 메시지 프로토콜에 따른 서명 중 일 값을 역원으로 대체한 것을 특징으로 하는 서명 검증 방법.

[청구항 2] 제 1 항에 있어서,
상기 메시지는 상기 일 값의 역원 대체 여부에 대한 식별자를 더 포함하는 것을 특징으로 하는 서명 검증 방법.

[청구항 3] 제 2 항에 있어서,
상기 서명은 기준점의 점 연산 계수의 산출을 위한 일 값을 역원으로 대체한 것을 특징으로 하는 서명 검증 방법.

[청구항 4] 제 2 항에 있어서,
상기 수신하는 단계는 상기 공개키에 대한 적어도 하나 이상의 스칼라 곱의 연산 결과를 수신하고,
상기 점 연산하는 단계는 상기 산출된 계수에 따라 점 연산 결과 또는,
상기 점 연산을 구성하는 하위 연산 중 적어도 일부를 미리 저장한 연산 테이블 내 값을 참조하여 연산을 수행하는 것을 특징으로 하는 서명 검증 방법.

[청구항 5] 제 2 항에 있어서,
상기 연산 테이블은 제1 좌표계로 수신된 상기 공개키의 스칼라 곱의 연산 결과를 제2 좌표계로 변환하여 상기 연산 결과 리스트를 생성하고,
상기 연산 결과 리스트를 제1 좌표계로 변환하여 저장한 것을 특징으로 하는 서명 검증 방법.

[청구항 6] 제 5 항에 있어서,
상기 서명은 임의의 난수에 따라 상기 제1 좌표계 상의 임의의 기준점을 스칼라 곱함으로써 생성되고,
상기 점 연산하는 단계는 상기 기준점과 상기 공개키를 상기 산출된 계수에 따라 점 연산하는 것을 특징으로 하는 서명 검증 방법.

[청구항 7] 제 1 항에 있어서,
상기 기준점에 대한 스칼라 곱 결과 리스트는 미리 생성된 것을 특징으로 하는 서명 검증 방법.

[청구항 8] 프로세서;

상기 프로세서에 의해 실행되는 컴퓨터 프로그램을 로드하는 메모리; 및
상기 컴퓨터 프로그램을 저장하는 스토리지를 포함하되,
상기 컴퓨터 프로그램은,
서명하고자 하는 메시지를 개인키로 암호화하여 생성한 서명을 포함하는 상기 메시지를 수신하는 동작,
상기 수신된 메시지로부터 제1 좌표계 상의 한 점으로 정의된 기준점 및 공개키의 점 연산 계수를 산출하는 동작, 및
상기 산출된 계수에 따른 점 연산의 결과와 상기 서명을 비교하여 상기 서명을 검증하는 동작을 포함하고,
상기 서명은 메시지 프로토콜에 따른 서명 중 일 값을 역원으로 대체한 것을 특징으로 하는 컴퓨팅 장치.

[청구항 9] 제 8 항에 있어서,
상기 메시지는 상기 일 값의 역원 대체 여부에 대한 식별자를 더 포함하는 것을 특징으로 하는 컴퓨팅 장치.

[청구항 10] 제 9 항에 있어서,
상기 서명은 기준점의 점 연산 계수의 산출을 위한 일 값을 역원으로 대체한 것을 특징으로 하는 컴퓨팅 장치.

[청구항 11] 제 9 항에 있어서,
상기 수신하는 동작은 상기 공개키에 대한 적어도 하나 이상의 스칼라 곱의 연산 결과를 수신하고,
상기 점 연산하는 동작은 상기 산출된 계수에 따라 점 연산 결과 또는,
상기 점 연산을 구성하는 하위 연산 중 적어도 일부를 미리 저장한 연산 테이블 내 값을 참조하여 연산을 수행하는 것을 특징으로 하는 컴퓨팅 장치.

[청구항 12] 제 9 항에 있어서,
상기 연산 테이블은 제1 좌표계로 수신된 상기 공개키의 스칼라 곱의 연산 결과를 제2 좌표계로 변환하여 상기 연산 결과 리스트를 생성하고,
상기 연산 결과 리스트를 제1 좌표계로 변환하여 저장한 것을 특징으로 하는 컴퓨팅 장치.

[청구항 13] 제 12 항에 있어서,
상기 서명은 임의의 난수에 따라 상기 제1 좌표계 상의 임의의 기준점을 스칼라 곱함으로써 생성되고,
상기 점 연산하는 동작은 상기 기준점과 상기 공개키를 상기 산출된 계수에 따라 점 연산하는 것을 특징으로 하는 컴퓨팅 장치.

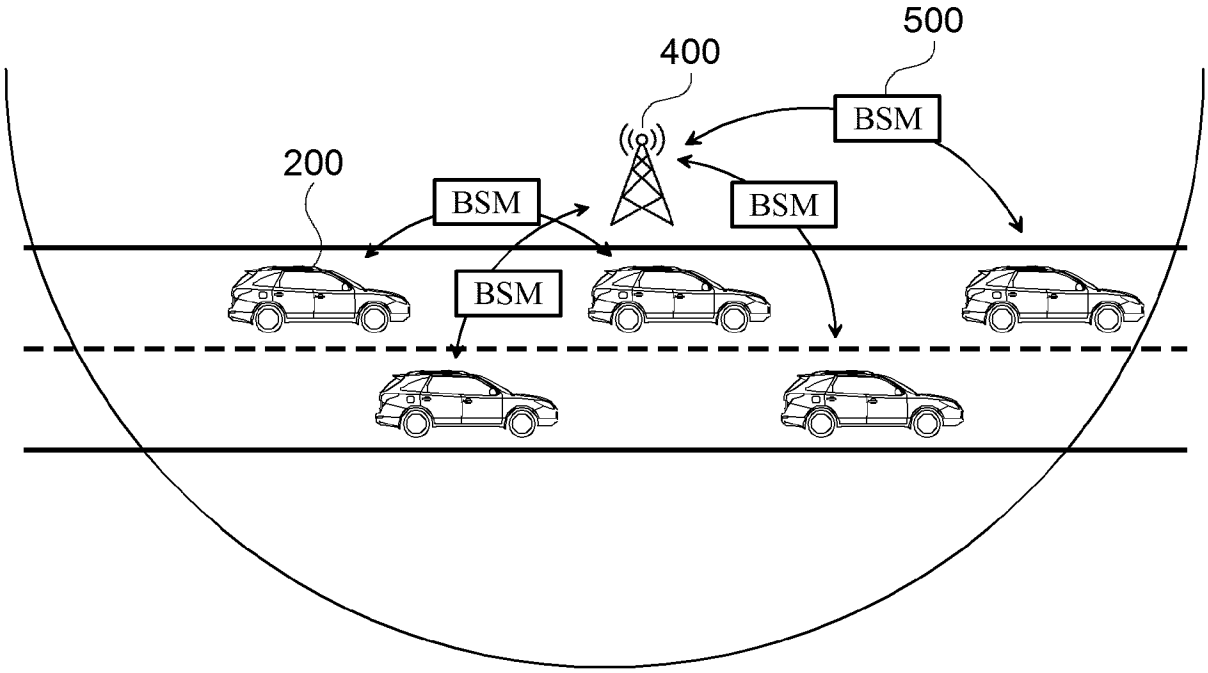
[청구항 14] 제 8 항에 있어서,
상기 기준점에 대한 스칼라 곱 결과 리스트는 미리 생성된 것을 특징으로 하는 컴퓨팅 장치.

[청구항 15] 제 1 항 내지 제 7 항 중 어느 한 항에 따른 서명 검증 방법을 컴퓨팅

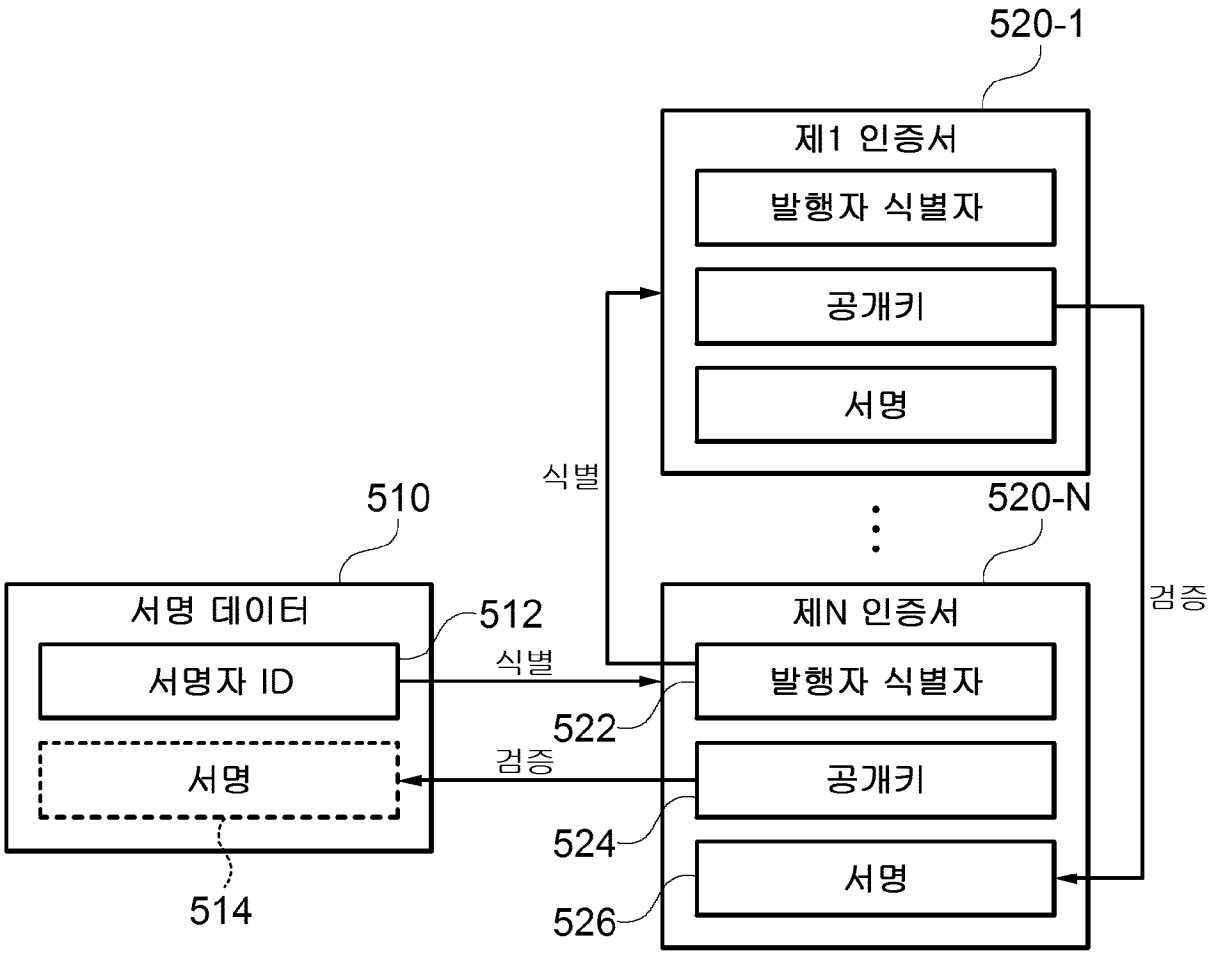
장치에서 수행하는 컴퓨터 판독 가능한 기록 매체에 저장된 프로그램.

WO 2024/101511 PCT/KR2022/018928

[도1]



[도2]



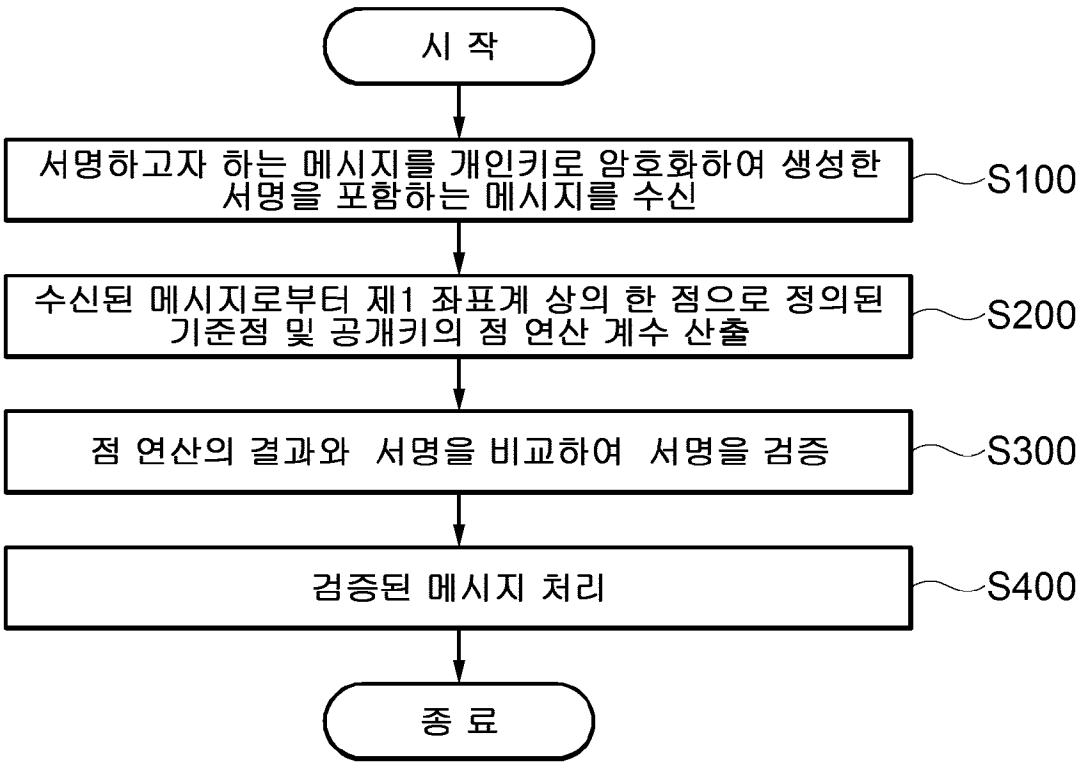
[도3]

ECDSA signature generation

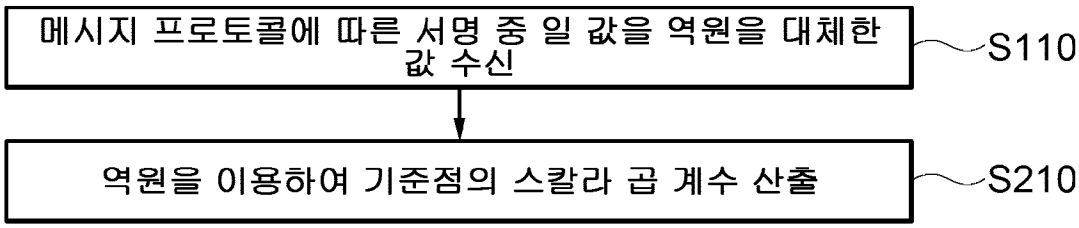
INPUT: Domain parameters $D = (a, b, P, n)$, private key d, message m.
OUTPUT: Signature (r, s^{-1})

1. Select $k \in_R [1, n-1]$.
2. Compute $kP = (x_1, y_1)$.
3. Compute $r = x_1 \bmod n$. If $r = 0$ then go to step 1.
4. Compute $e = H(m)$.
5. **Compute $s^{-1} = k(e + dr)^{-1} \bmod n$.**
6. **Return (r, s^{-1}).**

[도4]



[도5]



[도6]

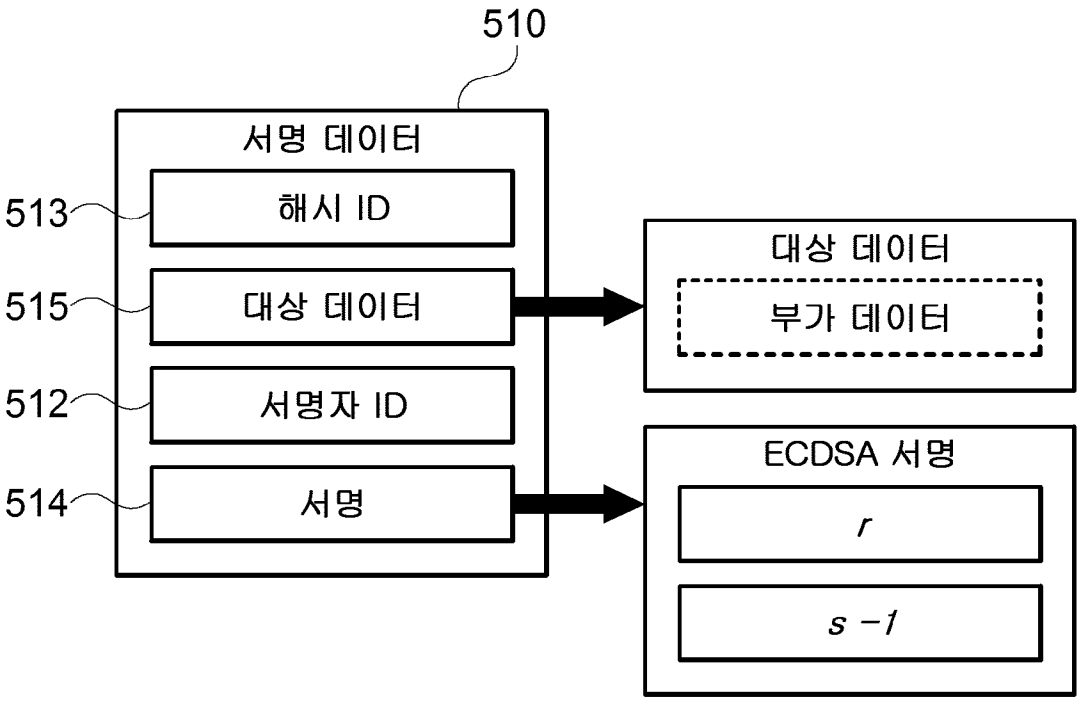
ECDSA signature verification

INPUT: Domain parameters $D = (a, b, P, n)$, public key Q, message m, signature (r, s^{-1})

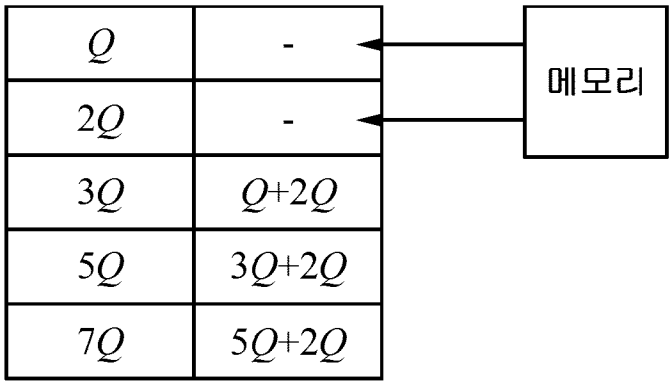
OUTPUT: Acceptance or rejection of the signature.

1. Verify that r and s are integers in the interval $[1, n-1]$. If any verification fails then return("Reject the signature").
2. Compute $e = H(m)$.
3. Compute $w = s^{-1} \bmod n$.
4. Compute $u_1 = ew \bmod n$ and $u_2 = rw \bmod n$.
5. Compute $X = u_1 P + u_2 Q$.
6. If $X = \infty$ then return("Reject the signature");
7. Compute $v = x_1 \bmod n$, x_1 of X.
8. If $v = r$ then return("Accept the signature");
   Else return("Reject the signature").

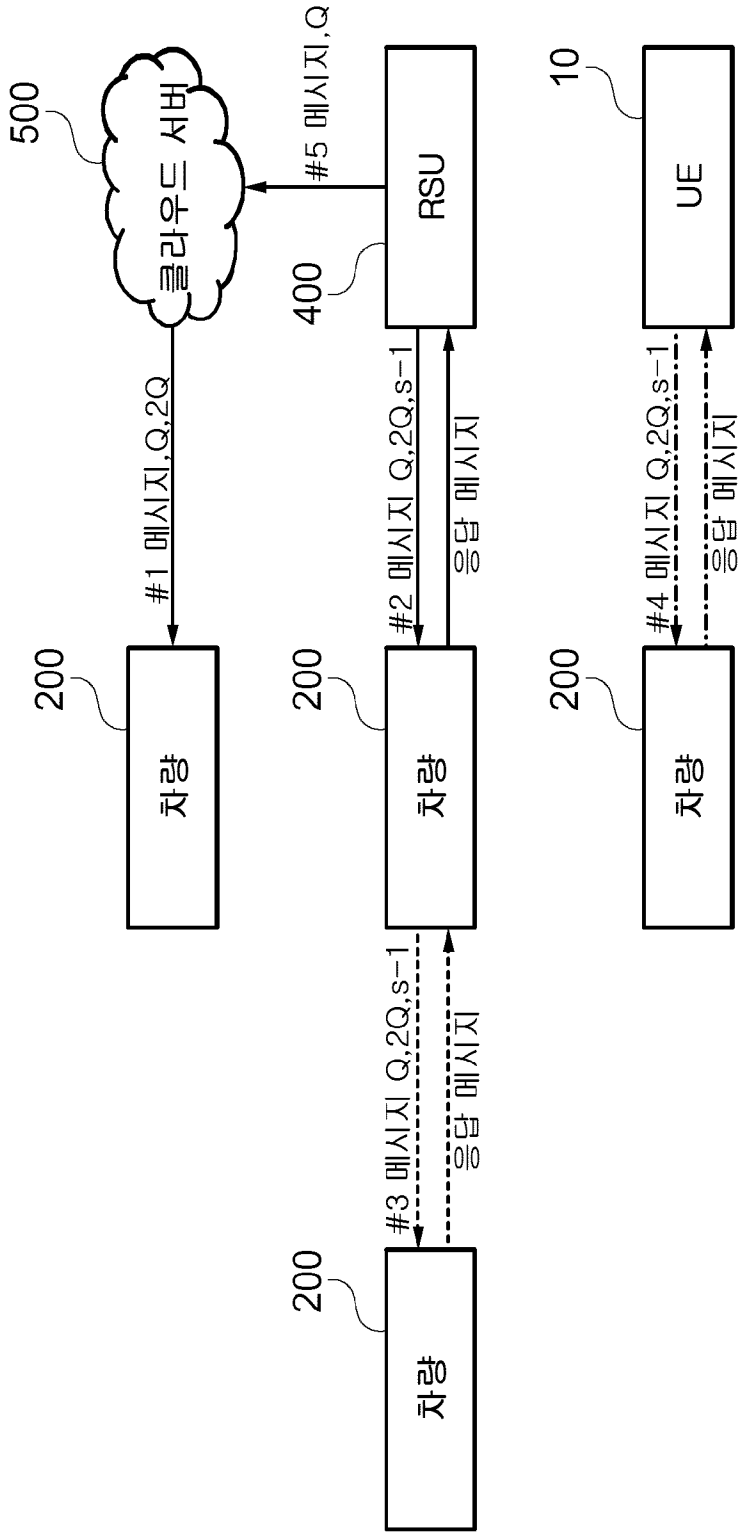
[도7]



[도8]

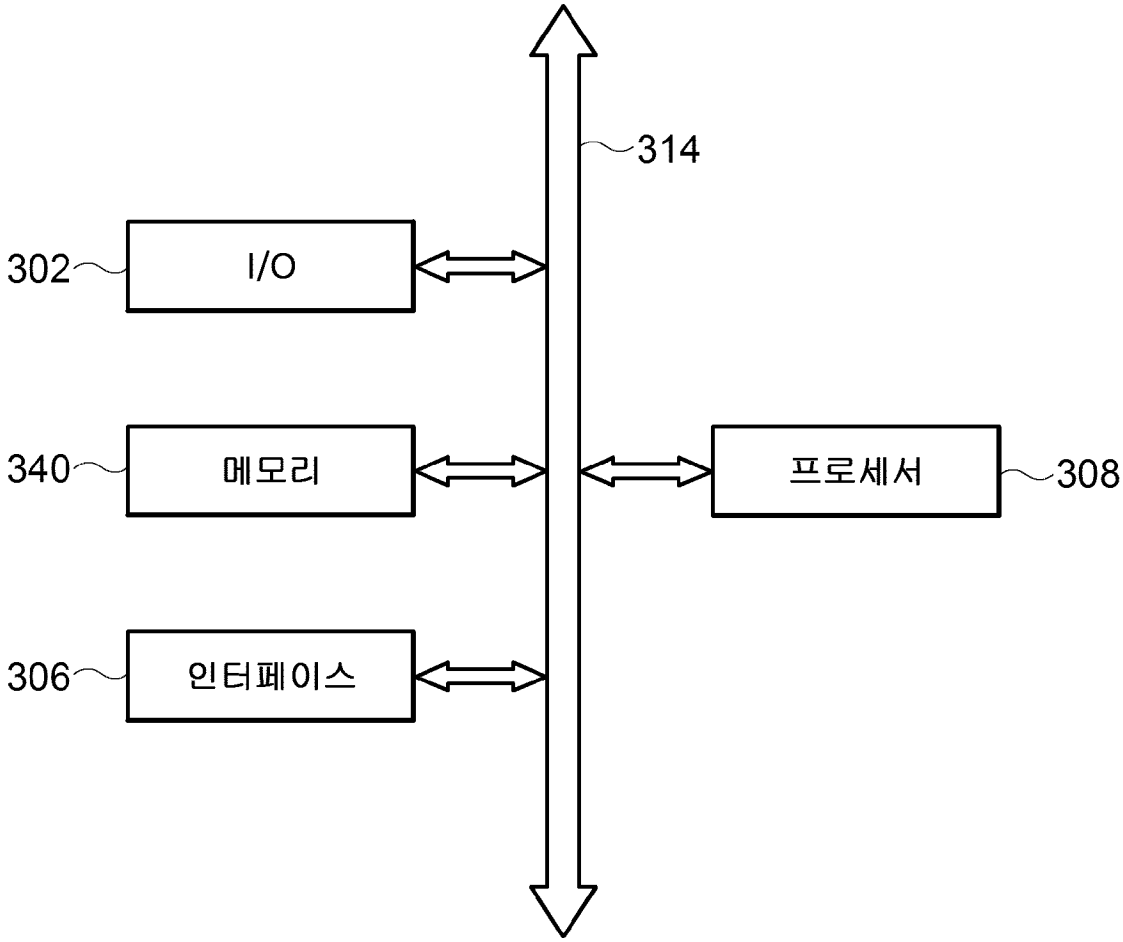


[도9]


500
클라우드 서버
#5 메시지,Q
400
RSU
10
UE
#1 메시지,Q,2Q
#2 메시지 Q,2Q,s-1
응답 메시지
#4 메시지 Q,2Q,s-1
응답 메시지
200
차량
200
차량
200
차량
#3 메시지 Q,2Q,s-1
응답 메시지
200
차량

[도10]

300



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2022/018928

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i; **H04L 9/30**(2006.01)i; **H04W 12/06**(2009.01)i; **H04W 4/44**(2018.01)i; **H04W 4/46**(2018.01)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 9/32(2006.01); G06F 7/52(2006.01); G06F 7/72(2006.01); G06F 9/44(2006.01); H04K 1/00(2006.01); H04L 9/00(2006.01); H04L 9/30(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: V2X 통신 환경(vehicle to everything communication environment), 서명(signature), 검증(verification), 기준점(base point), 점 연산(point calculation)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	양현준 등. NIST P-521 타원곡선을 지원하는 고성능 ECC 프로세서. 한국정보통신학회논문지. vol. 26, no. 4, pp. 548-555, April 2022 (YANG, Hyeon-Jun et al. A High-Performance ECC Processor Supporting NIST P-521 Elliptic Curve. Journal of the Korea Institute of Information and Communication Engineering (JKIICE)). [Retrieved on 10 July 2023]. Retrieved from <http://koreascience.or.kr/article/JAKO202212462668743.page>, <doi: https://doi.org/10.6109/jkiice.2022.26.4.548>. See page 549.	1-2,7-9,14-15
A		3-6,10-13
Y	KR 10-2022-0143557 A (SAMSUNG ELECTRONICS CO., LTD.) 25 October 2022 (2022-10-25) See paragraph [0049].	1-2,7-9,14-15
Y	KR 10-2010-0062565 A (SAMSUNG ELECTRONICS CO., LTD.) 10 June 2010 (2010-06-10) See paragraphs [0068]-[0071] and [0085]-[0120].	1-2,7-9,14-15

☑ 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 July 2023	**24 July 2023**

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.
Y	KR 10-2017-0061411 A (HANBAT NATIONAL UNIVERSITY INDUSTRY-ACADEMIC COOPERATION FOUNDATION) 05 June 2017 (2017-06-05) See paragraph [0012].	7,14
A	KR 10-2009-0005041 A (MOTOROLA INC.) 12 January 2009 (2009-01-12) See paragraphs [0023]-[0030]; and figure 1.	1-15

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2022/018928

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
KR 10-2022-0143557 A	25 October 2022	CN 115225248 A	21 October 2022
		US 2022-0337425 A1	20 October 2022
KR 10-2010-0062565 A	10 June 2010	KR 10-1548174 B1	07 September 2015
		US 2010-0138467 A1	03 June 2010
		US 2013-0198253 A1	01 August 2013
		US 8407270 B2	26 March 2013
KR 10-2017-0061411 A	05 June 2017	KR 10-1777400 B1	11 September 2017
KR 10-2009-0005041 A	12 January 2009	CN 101427500 A	06 May 2009
		CN 101427500 B	05 June 2013
		EP 2014000 A2	14 January 2009
		EP 2014000 B1	03 October 2018
		KR 10-1492644 B1	12 February 2015
		MX 2008013557 A	04 November 2008
		US 2007-0248224 A1	25 October 2007
		US 8311214 B2	13 November 2012
		WO 2007-127576 A2	08 November 2007
		WO 2007-127576 A3	17 April 2008

국 제 조 사 보 고 서

국제출원번호
PCT/KR2022/018928

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/32(2006.01)i; **H04L 9/30**(2006.01)i; **H04W 12/06**(2009.01)i; **H04W 4/44**(2018.01)i; **H04W 4/46**(2018.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 9/32(2006.01); G06F 7/52(2006.01); G06F 7/72(2006.01); G06F 9/44(2006.01); H04K 1/00(2006.01); H04L 9/00(2006.01); H04L 9/30(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: V2X 통신 환경(vehicle to everything communication environment), 서명(signature), 검증(verification), 기준점(base point), 점 연산(point calculation)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	양현준 등, NIST P-521 타원곡선을 지원하는 고성능 ECC 프로세서, 한국정보통신학회논문지, 제26권, 제4호, 페이지 548-555, 2022.04 [검색일: 2023-07-10], 출처 <http://koreascience.or.kr/article/JAKO202212462668743.page>, <doi: https://doi.org/10.6109/jkiice.2022.26.4.548> 페이지 549	1-2,7-9,14-15
A		3-6,10-13
Y	KR 10-2022-0143557 A (삼성전자주식회사) 2022.10.25 단락 [0049]	1-2,7-9,14-15
Y	KR 10-2010-0062565 A (삼성전자주식회사) 2010.06.10 단락 [0068]-[0071], [0085]-[0120]	1-2,7-9,14-15
Y	KR 10-2017-0061411 A (한밭대학교 산학협력단) 2017.06.05 단락 [0012]	7,14

☑ 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
2023년07월24일(24.07.2023)	**2023년07월24일(24.07.2023)**

ISA/KR의 명칭 및 우편주소	심사관
대한민국 특허청 **(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)**	**변성철**
팩스 번호 **+82-42-481-8578**	전화번호 **+82-42-481-8262**

국 제 조 사 보 고 서

국제출원번호
PCT/KR2022/018928

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2009-0005041 A (모토로라 인코포레이티드) 2009.01.12 단락 [0023]-[0030]; 및 도면 1	1-15

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2022/018928

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2022-0143557 A	2022/10/25	CN 115225248 A	2022/10/21
		US 2022-0337425 A1	2022/10/20
KR 10-2010-0062565 A	2010/06/10	KR 10-1548174 B1	2015/09/07
		US 2010-0138467 A1	2010/06/03
		US 2013-0198253 A1	2013/08/01
		US 8407270 B2	2013/03/26
KR 10-2017-0061411 A	2017/06/05	KR 10-1777400 B1	2017/09/11
KR 10-2009-0005041 A	2009/01/12	CN 101427500 A	2009/05/06
		CN 101427500 B	2013/06/05
		EP 2014000 A2	2009/01/14
		EP 2014000 B1	2018/10/03
		KR 10-1492644 B1	2015/02/12
		MX 2008013557 A	2008/11/04
		US 2007-0248224 A1	2007/10/25
		US 8311214 B2	2012/11/13
		WO 2007-127576 A2	2007/11/08
		WO 2007-127576 A3	2008/04/17