(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2016 년 3 월 31 일 (31.03.2016)

WIPO | PCT

(10) 국제공개번호
WO 2016/048054 A2

(51) 국제특허분류:
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)

(21) 국제출원번호: PCT/KR2015/010073

(22) 국제출원일: 2015 년 9 월 24 일 (24.09.2015)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
62/054,499 2014 년 9 월 24 일 (24.09.2014) US
10-2015-0134823 2015 년 9 월 23 일 (23.09.2015) KR

(71) 출원인: **삼성전자 주식회사 (SAMSUNG ELECTRONICS CO., LTD.)** [KR/KR]; 16677 경기도 수원시 영통구 삼성로 129, Gyeonggi-do (KR).

(72) 발명자: **허미숙 (HUH, Mi-suk)**; 16709 경기도 수원시 영통구 청명북로 33 435 동 503 호, Gyeonggi-do (KR). **이희관 (LEE, Hee-kwan)**; 13556 경기도 성남시 분당구 정자일로 239 101 동 2103 호, Gyeonggi-do (KR). **최광표 (CHOI, Kwang-pyo)**; 14008 경기도 안양시 만안구 박달로 498 번길 28 106 동 1302 호, Gyeonggi-do (KR). **김찬열 (KIM, Chan-yul)**; 14442 경기도 부천시 오정구 오정로 245 102 동 506 호, Gyeonggi-do (KR). **서석충 (SEO, Seog-chung)**; 02179 서울시 중랑구 망우로 72 가길 22 B 동 301 호, Seoul (KR).

(74) 대리인: **리앤목 특허법인 (Y.P.LEE, MOCK & PARTNERS)**; 06292 서울시 강남구 언주로 30 길 13 대림아크로텔 12 층, Seoul (KR).

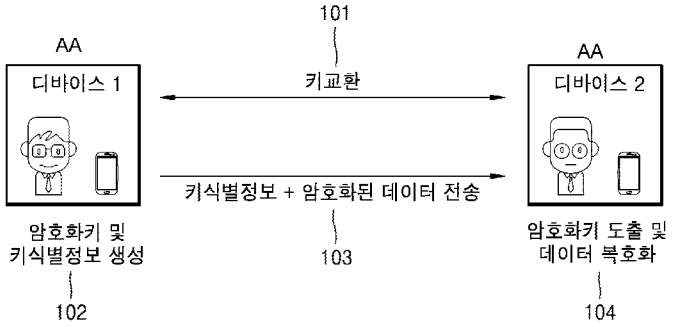
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, 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 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).

[다음 쪽 계속]

(54) **Title**: METHOD, APPARATUS AND SYSTEM FOR SECURE DATA COMMUNICATION

(54) **발명의 명칭** : 데이터 통신 보안을 위한 방법, 장치 및 시스템



101 ... Key exchange
102 ... Encryption key and key identification information generation
103 ... Key identification information and encrypted data transmission
104 ... Encryption key derivation and data decryption
AA ... Device

(57) **Abstract**: The present disclosure relates to technical matters for sensor networks, machine to machine (M2M) communication, machine type communication (MTC) and Internet of Things (IoT). The present disclosure can be used for intelligent services based on these technical matters (smart home, smart building, smart city, smart car, or connected car, healthcare, digital education, retail business, security and safety related services, and the like). A method for transmitting encrypted data from a first device to a second device that prevents identification of the transmitting and receiving devices is disclosed, the method for transmitting data is characterized by comprising the steps of: generating an encryption key for data encryption; generating key identification information using the generated encryption key and encrypting data; and transmitting to the second device a data set including the encrypted data and the key identification information.

(57) **요약서**:

[다음 쪽 계속]

WO 2016/048054 A2

공개:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

본 개시는 센서 네트워크(Sensor Network), 사물 통신(Machine to Machine, M2M), MTC(Machine Type Communication) 및 사물 인터넷(Internet of Things, IoT)을 위한 기술과 관련된 것이다. 본 개시는 상기 기술을 기반으로 하는 지능형 서비스(스마트 홈, 스마트 빌딩, 스마트 시티, 스마트 카 혹은 커넥티드 카, 헬스 케어, 디지털 교육, 소매업, 보안 및 안전 관련 서비스 등)에 활용될 수 있다. 본 개시에서는, 제 1 디바이스에서 제 2 디바이스로 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 송신하는 방법으로서, 데이터를 암호화하기 위한 암호화키를 생성하는 단계, 생성된 암호화키를 이용하여 키식별정보를 생성하고 데이터를 암호화하는 단계, 암호화된 데이터 및 키식별정보를 포함하는 데이터 세트를 제 2 디바이스로 송신하는 단계를 포함하는 것을 특징으로 하는 암호화된 데이터 전송 방법이 개시된다.

명세서

발명의 명칭: 데이터 통신 보안을 위한 방법, 장치 및 시스템

기술분야

[1] 본 개시는 데이터 통신의 보안을 유지하기 위한 방법, 장치 및 시스템에 관한 것이다.

배경기술

[2] 인터넷은 인간이 정보를 생성하고 소비하는 인간 중심의 연결 망에서, 사물 등 분산된 구성 요소들 간에 정보를 주고 받아 처리하는 IoT(Internet of Things, 사물인터넷) 망으로 진화하고 있다. 클라우드 서버 등과의 연결을 통한 빅데이터(Big data) 처리 기술 등이 IoT 기술에 결합된 IoE (Internet of Everything) 기술도 대두되고 있다. IoT를 구현하기 위해서, 센싱 기술, 유무선 통신 및 네트워크 인프라, 서비스 인터페이스 기술, 및 보안 기술과 같은 기술 요소 들이 요구되어, 최근에는 사물간의 연결을 위한 센서 네트워크(sensor network), 사물 통신(Machine to Machine, M2M), MTC(Machine Type Communication)등의 기술이 연구되고 있다.

[3] IoT 환경에서는 연결된 사물들에서 생성된 데이터를 수집, 분석하여 인간의 삶에 새로운 가치를 창출하는 지능형 IT(Internet Technology) 서비스가 제공될 수 있다. IoT는 기존의 IT(information technology)기술과 다양한 산업 간의 융합 및 복합을 통하여 스마트홈, 스마트 빌딩, 스마트 시티, 스마트 카 혹은 커넥티드 카, 스마트 그리드, 헬스 케어, 스마트 가전, 첨단의료서비스 등의 분야에 응용될 수 있다.

[4] 특히 IoT 환경에서는 디바이스들 간의 데이터 통신을 수행하는 경우가 많다. 일반적으로, 송신 디바이스 및 수신 디바이스는 암호화된 데이터를 송신 및 수신하는데, 수신 디바이스가 암호화된 데이터를 복호화 하기 위해서는 송신 디바이스에 대한 정보가 필요하다. 따라서, 데이터 통신 시에는 송신 디바이스는 IP address와 같은 송신 디바이스에 관한 정보를 수신 디바이스에게 제공한다. 정보가 노출될 수가 있다. 그러나, IP address와 같은 송신 디바이스의 정보에 기초하여 제3자는 송신 디바이스와 수신 디바이스, 송신 디바이스와 수신 디바이스간의 통신 빈도 등 많은 개인적인 정보를 획득할 수 있다.

[5] 따라서, 암호화된 데이터 자체를 통해서, 제 3 자가 아닌 수신 디바이스만이 송신 디바이스를 식별할 수 있도록 하는 기술에 대한 수요가 증가하고 있다.

[6] 뿐만 아니라, IoT 환경에서는 송신 디바이스와 수신 디바이스는 암호화된 데이터 통신을 위해 암호화 키를 생성 및 교환한다. 그러나, 송신 디바이스와 수신 디바이스가 동일한 키 데이터에 기초하여 암호화 키를 생성하는 경우가 일반적이어서, 제 3 디바이스가 송신 디바이스와 수신 디바이스 중 하나의 디바이스를 해킹함으로써, 두 디바이스 간에 송수신되는 데이터 모두를 해킹할

수 있었다.

[7] 따라서, 보다 안전한 암호화 키 생성 및 교환 기술에 대한 수요가 증가하고 있다.

발명의 상세한 설명

기술적 과제

[8] 본 발명은 안전한 암호화 키 생성 및 교환 기술을 제공하고자 한다.

과제 해결 수단

[9] 본 발명은 암호화된 데이터 교환시 송수신 디바이스의 식별을 방지하는 방법을 제공하며, 특히 인터넷 메신저와 같은 서버형 메시지 서비스에서 암호화된 데이터 교환시 송수신 디바이스의 식별을 방지하는 방법을 제공하고자 한다. 또한 본 발명은 암호화된 데이터 통신을 위한 안전한 키 생성 및 교환 방법을 제공하고자 한다.

발명의 효과

[10] 본 발명의 일 실시예에 따르면, 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 전송하거나 수신하는 방법 및 디바이스를 제공함으로써, 암호화된 데이터로 인해 송수신 디바이스의 정보가 제3자에게 노출이 되지 않으면서도 수신 디바이스는 암호화된 데이터를 복호화할 수 있다.

도면의 간단한 설명

[11] 도 1은 일부 실시예에 따른 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 제1 디바이스와 제2 디바이스 사이에서 전송하거나 수신하는 디바이스를 도시화한 것이다.

[12] 도 2는 일부 실시예에 따른 제1 디바이스에서 제2 디바이스로 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 송신하는 방법을 도시하는 흐름도이다.

[13] 도 3은 일부 실시예에 따른 제2 디바이스에서 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 제1 디바이스로부터 수신하는 방법을 도시하는 흐름도이다.

[14] 도 4는 일부 실시예에 따른 공개키 및 난수를 이용하여 암호화된 데이터를 송신하는 방법을 도시하는 흐름도이다.

[15] 도 5는 일부 실시예에 따른 공개키 및 난수를 이용하여 암호화된 데이터를 수신하는 방법을 도시하는 흐름도이다.

[16] 도 6은 일부 실시예에 따른 수신 디바이스의 공개키를 이용하여 암호화된 데이터를 송신하는 방법을 도시한 흐름도이다.

[17] 도 7은 일부 실시예에 따른 수신 공개키를 이용하여 암호화된 데이터를 수신하는 방법을 도시한 흐름도이다.

[18] 도 8은 일부 실시예에 따른 공유된 비공개키를 이용하여 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 전송하고 수신하는 방법의 흐름도이다.

[19] 도 9는 일부 실시예에 따른 디바이스를 식별할 수 있는 정수를 이용하여 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 송신하는 방법을 도시한 흐름도이다.

[20] 도 10는 일부 실시예에 따른 디바이스를 식별할 수 있는 정수를 이용하여 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 수신하는 방법을 도시한 흐름도이다.

[21] 도 11은 일부 실시예에 따른 암호화된 데이터를 저장하면서 제1 디바이스의 식별정보를 획득하는, 암호화된 데이터를 수신하는 방법을 도시하는 흐름도이다.

[22] 도 12는 일부 실시예에 따른 송신 디바이스가 소정의 디바이스의 그룹에 대하여 암호화된 데이터를 송신하는 방법을 도시하는 개념도이다.

[23] 도 13은 일부 실시예에 따른 제2 디바이스가 제1 디바이스를 포함하는 복수의 디바이스로부터 키식별정보를 수신하고 데이터를 송신한 제1 디바이스의 키를 식별하기 위한 매칭과정을 설명하기 위한 플로우를 도시한다.

[24] 도 14는 일부 실시예에 따른 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 제2 디바이스로 송신하는 제1 디바이스를 도시하는 블록도이다.

[25] 도 15는 일부 실시예에 따른 송수신 디바이스의 식별을 방지하는 암호화된 데이터 세트를 수신하는 디바이스를 도시하는 블록도이다.

[26] 도 16은 일부 실시예에 따른 디바이스를 설명하기 위한 세부 블록도이다.

[27] 도 17은 일부 실시예에 따른 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 송수신하는 시스템을 도시하는 개념도이다.

[28] 도 18은 일부 실시예에 따른 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 송신하는 방법을 도시하는 흐름도이다.

[29] 도 19은 일부 실시예에 따른 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 수신하는 방법을 도시하는 흐름도이다.

[30] 도 20 및 도 21은 일부 실시예에 따른 키 공유 방법을 도시하는 시스템 도면이다.

[31] 도 22는 일부 실시예에 따른 키 공유 방법을 도시하는 흐름도이다.

[32] 도 23은 일부 실시예에 따른 키 공유 및 암호화 키 생성 방법을 도시하는 흐름도이다.

[33] 도 24는 일부 실시예에 따른 키 공유 방법을 도시하는 흐름도이다.

[34] 도 25 및 도 26은 일부 실시예에 따른 암호화 통신을 위한 제 1 디바이스와 제 2 디바이스 간의 키 공유 방법을 도시한다.

[35] 도 27은 일부 실시예에 따른 SAS 생성 방법을 도시한다.

[36] 도 28은 일부 실시예에 따른 키 공유 디바이스의 블록도이다.

[37] 도 29은 일부 실시예에 따른 키 공유 디바이스의 세부 블록도이다.

발명의 실시를 위한 최선의 형태

[38] 상기와 같은 종래 기술의 문제를 해결하기 위한 일부 실시예는, 제1 디바이스에서 암호화된 데이터를 송신하는 방법으로써, 송신할 데이터를 암호화하기 위한 암호화키를 생성하는 단계; 상기 생성된 암호화키를 이용하여 키식별정보를 생성하는 단계; 상기 생성된 암호화 키를 이용하여 송신할 데이터를 암호화하는 단계; 및 상기 암호화된 데이터 및 상기 키식별정보를 포함하는 데이터 세트를 제2 디바이스로 송신하는 단계를 포함할 수 있다.

[39] 상기 키식별정보는 상기 제2 디바이스가 식별할 수 있는 상기 제1 디바이스의 식별정보 또는 상기 암호화키를 식별할 수 있는 정보를 포함할 수 있다.

[40] 상기 암호화키를 생성하는 단계는, 상기 제1 디바이스의 공개키 및 제1 난수를 상기 제2 디바이스로 전송하고 상기 제2 디바이스로부터 상기 제2 디바이스의 공개키 및 제2 난수를 수신하는 단계; 및 상기 제1 디바이스의 공개키 및 상기 제2 디바이스의 공개키를 이용하여 상기 암호화키를 생성하는 단계를 포함하고, 상기 키식별정보는 상기 제1 난수, 상기 제2 난수 및 상기 암호화키를 이용하여 생성되며, 상기 키식별정보는 상기 제 1 난수 또는 상기 제 2 난수에 기초하여 상기 제 1 디바이스를 식별할 수 있는 정보를 포함할 수 있다.

[41] 상기 키식별정보를 생성하는 단계는, 상기 제 2 디바이스로부터 상기 제2 디바이스의 공개키를 수신하는 단계; 및 상기 수신된 제2 디바이스의 공개키를 이용하여 상기 암호화키를 암호화하여 상기 키식별정보를 생성하는 단계를 포함할 수 있다.

[42] 상기 암호화키를 생성하는 단계는, 제2 디바이스와 비공개키를 공유하는 단계; 및 상기 비공개키 및 제1 난수를 이용하여 상기 암호화키를 생성하는 단계를 포함하고, 상기 키식별정보는 상기 제1 난수, 및 상기 제1 난수와 상기 암호화키를 조합한 값을 상기 제1 난수로 키-해싱한 값을 포함할 수 있다.

[43] 상기 암호화키는 제1 디바이스의 식별넘버(Pa) 및 제2 디바이스의 식별넘버(Pb)보다 작은 난수이고, 상기 키식별정보는 제1 디바이스의 식별넘버(Pa) 및 제2 디바이스의 식별넘버(Pb)의 곱 또는 최대공약수에 상기 난수를 더한 값일 수 있다.

[44] 상기 데이터 세트는 메시지 인증 코드(message authentication code)를 더 포함하고, 상기 메시지 인증 코드는 상기 제2 디바이스가 획득한 암호화키가 상기 제 1 디바이스가 송신한 암호화 키와 동일한 암호화 키인지 여부를 확인하기 위해 이용될 수 있다.

[45] 상기와 같은 종래 기술의 문제를 해결하기 위한 일부 실시예는, 제2 디바이스에서 암호화된 데이터를 수신하는 방법으로써, 제1 디바이스로부터 암호화된 데이터 및 키식별정보를 포함하는 데이터 세트를 수신하는 단계; 상기 키식별정보를 이용하여 제1 디바이스에 대한 암호화키를 획득하는 단계; 상기 획득된 암호화키를 이용하여 상기 암호화된 데이터를 복호화하는 단계를 포함할 수 있다.

[46] 상기 키식별정보는 제2 디바이스가 식별할 수 있는 제1 디바이스의 정보 또는

상기 암호화키를 식별할 수 있는 정보를 포함할 수 있다.

[47] 상기 방법은, 상기 제1 디바이스를 포함하는 적어도 하나의 디바이스로부터 적어도 하나의 공개키 및 적어도 하나의 난수를 각각 수신하고 상기 제2 디바이스의 공개키 및 제2 난수를 상기 적어도 하나의 디바이스로 각각 송신하는 단계를 더 포함하고, 상기 제1 디바이스에 대한 암호화키를 획득하는 단계는, 상기 수신된 적어도 하나의 공개키 및 상기 제2 디바이스의 공개키를 이용하여 상기 적어도 하나의 디바이스에 대한 적어도 하나의 암호화키를 생성하는 단계; 상기 적어도 하나의 암호화키를 이용하여 적어도 하나의 키식별정보를 생성하는 단계; 상기 생성된 적어도 하나의 키식별정보와 상기 수신된 키식별정보를 비교하여 상기 암호화된 데이터를 송신한 제1 디바이스를 식별하는 단계; 및 상기 식별된 제1 디바이스에 대한 암호화키를 획득하는 단계를 포함할 수 있다.

[48] 상기 방법은, 상기 제2 디바이스의 공개키를 상기 제1 디바이스로 송신하는 단계를 더 포함하고, 상기 제1 디바이스에 대한 암호화키를 획득하는 단계는, 상기 수신된 데이터 세트 내의 키식별정보를 상기 제2 디바이스의 공개키에 대응되는 개인키를 이용하여 복호화하여 상기 암호화키를 획득하는 단계를 포함할 수 있다.

[49] 상기 방법은, 상기 제1 디바이스를 포함하는 적어도 하나의 디바이스들과 적어도 하나의 비공개키를 공유하는 단계를 더 포함하고, 상기 데이터 세트를 수신하는 단계는 상기 적어도 하나의 디바이스 중 상기 제1 디바이스로부터 암호화된 데이터 및 키식별정보를 수신하는 단계를 포함하고, 상기 키식별정보는 상기 제1 디바이스의 제1 난수, 및 상기 제1 난수로 암호화키를 키-해싱한(key-hashed) 값을 포함하고, 상기 암호화키는 상기 제1 디바이스와 공유한 비공개키와 상기 제1난수의 조합에 의해 생성된 정보이며, 상기 제1 디바이스에 대한 암호화키를 획득하는 단계는, 수신한 상기 제1 난수를 이용하여, 상기 적어도 하나의 비공개키와 상기 제1 난수를 각각 조합한 값들을 상기 제1 난수로 각각 키-해싱하여 적어도 하나의 매칭키들을 생성하는 단계; 상기 생성된 적어도 하나의 매칭키들과 수신한 상기 제1 난수로 상기 암호화키를 키-해싱한 값을 비교하여 상기 데이터 세트를 송신한 제1 디바이스를 식별하는 단계; 및 상기 제1 디바이스의 암호화키를 획득하는 단계를 포함할 수 있다.

[50] 상기 암호화키는 상기 키식별정보를 상기 제2 디바이스의 식별 넘버로 나눈 몫 또는 나머지 중 적어도 하나에 기초하여 결정될 수 있다.

[51] 상기 데이터 세트는 메시지 인증 코드(message authentication code)를 더 포함하고, 상기 메시지 인증 코드는 상기 획득한 암호화키가 제 1 디바이스가 송신한 암호화 키와 동일한 암호화키인지를 여부를 확인하기 위해 이용될 수 있다.

[52] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로써, 본 개시의 일부

실시예는 상기 방법을 구현하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

[53] 상기와 같은 종래 기술의 문제를 해결하기 위한 일부 실시예는, 암호화된 데이터를 송신하는 제1 디바이스로써, 암호화키를 생성하고, 상기 생성된 암호화키를 이용하여 키식별정보를 생성하고 데이터를 암호화하는 제어부; 상기 암호화된 데이터 및 상기 키식별정보를 포함하는 데이터 세트를 제2 디바이스로 송신하는 송수신부를 포함할 수 있다.

[54] 상기 키식별정보는 상기 제2 디바이스가 식별 할 수 있는 상기 제1 디바이스의 정보 또는 상기 암호화키를 식별할 수 있는 정보를 포함할 수 있다.

[55] 상기 송수신부는 상기 제1 디바이스의 공개키 및 제1 난수를 제2 디바이스로 전송하고 상기 제2 디바이스로부터 상기 제2 디바이스의 공개키 및 제2 난수를 수신하고, 상기 제어부는 상기 제1 디바이스의 공개키 및 상기 제2 디바이스의 공개키를 이용하여 상기 암호화키를 생성하고, 상기 키식별정보는 상기 제1 난수, 제2 난수 및 상기 암호화키를 이용하여 생성되며, 상기 키식별정보는 상기 제 1 난수 또는 제 2 난수에 기초하여 상기 제 1 디바이스를 식별할 수 있는 정보를 포함할 수 있다.

[56] 상기 송수신부는 제 2 디바이스로부터 상기 제2 디바이스의 공개키를 수신하고, 상기 키식별정보는 상기 제2 디바이스의 공개키를 이용하여 상기 암호화키를 암호화하여 생성될 수 있다.

[57] 상기 송수신부는 상기 제2 디바이스와 비공개키를 공유하고, 상기 제어부는 상기 비공개키 및 제1 난수를 이용하여 상기 암호화키를 생성하고, 상기 키식별정보는 상기 제1 난수 및 상기 제1 난수와 상기 암호화키를 조합한 값을 상기 제1 난수로 키-해싱한 값일 수 있다.

[58] 상기 암호화키는 상기 제1 디바이스의 식별넘버 및 상기 제2 디바이스의 식별넘버보다 작은 난수를 포함하고, 상기 키식별정보는 상기 제1 디바이스의 식별넘버와 상기 제2 디바이스의 식별넘버의 곱 또는 최대 공약수에 상기 난수를 더한 값을 포함할 수 있다.

[59] 상기와 같은 종래 기술의 문제를 해결하기 위한 일부 실시예는, 암호화된 데이터를 수신하는 제2 디바이스로써, 암호화된 데이터 및 키식별정보를 포함하는 데이터 세트를 제1 디바이스로부터 수신하는 송수신부; 상기 키식별정보를 이용하여 암호화키를 획득하고, 상기 암호화키를 이용하여 상기 수신된 암호화된 데이터를 복호화하는 제어부를 포함하며, 상기 키식별정보는 상기 제2 디바이스가 식별 할 수 있는 상기 제1 디바이스의 정보 또는 상기 암호화키를 식별할 수 있는 정보를 포함할 수 있다.

[60] 상기 송수신부는 상기 제1 디바이스를 포함하는 적어도 하나의 디바이스로부터 적어도 하나의 공개키 및 적어도 하나의 난수를 각각 수신하고 상기 제2 디바이스의 공개키 및 제2 난수를 상기 적어도 하나의 디바이스로 각각 추가적으로 전송하며, 상기 제어부는 상기 수신된 적어도 하나의 공개키 및 상기

제2 디바이스의 공개키를 이용하여 상기 적어도 하나의 디바이스에 대한 적어도 하나의 암호화키를 생성하고, 상기 적어도 하나의 암호화키를 이용하여 적어도 하나의 키식별정보를 생성하고, 상기 생성된 적어도 하나의 키식별정보와 상기 수신된 키식별정보를 비교하여 상기 제1 디바이스를 식별(identify)하고, 상기 식별된 제1 디바이스에 대한 암호화키를 획득할 수 있다.

[61] 상기 송수신부는 상기 제2 디바이스의 공개키를 상기 제1 디바이스로 추가적으로 전송하고, 상기 제어부는 상기 키식별정보를 상기 제2 디바이스의 공개키에 대응되는 개인키를 이용하여 복호화하여 암호화키를 획득할 수 있다.

[62] 상기 송수신부는 제1 디바이스를 포함하는 적어도 하나의 디바이스들로부터 적어도 하나의 비공개키를 추가적으로 공유하고, 상기 적어도 하나의 디바이스 중 제1 디바이스로부터 암호화된 데이터 및 키식별정보를 수신하며, 상기 키식별정보는 상기 제1 디바이스로부터 수신한 제1 난수 및 상기 제1 난수로 암호화키를 키-해싱한(key-hashed) 값을 포함하고, 상기 암호화키는 상기 제1 디바이스의 비공개키와 상기 제1난수의 조합이에 의해 생성된 정보이며, 상기 제어부는 수신한 상기 제1 난수를 이용하여, 상기 적어도 하나의 비공개키와 상기 제1 난수를 각각 조합한 값들을 상기 제1 난수로 각각 키-해싱하여 적어도 하나의 매칭키들을 생성하고, 상기 생성된 적어도 하나의 매칭키들 중 수신한 상기 제1 난수로 상기 암호화키를 키-해싱한 값와 동일한 값을 탐색하여 상기 제1 디바이스를 식별하고, 상기 제1 디바이스와 공유한 비공개 키 및 상기 제1 난수를 이용하여 상기 암호화키를 획득할 수 있다.

[63] 상기 암호화키는 상기 키식별정보를 상기 제2 디바이스의 식별넘버로 나눈 몫에 의하여 결정될 수 있다.

[64] 상기와 같은 종래 기술의 문제를 해결하기 위한 일부 실시예는, 제1 디바이스에서 암호화된 데이터 송신을 위한 키를 공유하는 방법에 있어서, 통신 내역에 기초하여, 제 2 디바이스에게 송신한 제 1 디바이스의 제 1 공개키 및 상기 제 1 디바이스의 제 1 공개키에 대응하는 제 1 디바이스의 제 1 개인키가 저장되어 있는지 판단하는 단계; 판단 결과에 기초하여 제 1 디바이스의 제 2 공개키 및 제 1 디바이스의 제 2 개인키를 생성하는 단계; 상기 생성된 제 1 디바이스의 제 2 공개키를 상기 제 1 디바이스의 제 1 개인키로 서명하는 단계; 및 상기 서명된 제 2 공개키를 제 2 디바이스로 송신하는 단계를 포함할수 있다.

[65] 상기 방법은, 상기 제 2 디바이스로부터 상기 제 2 디바이스의 제 1 개인키로 서명된 제 2 공개키를 수신하는 단계; 통신 내역에 기초하여, 상기 제 2 디바이스의 제 1 개인키와 대응되는 상기 제 2 디바이스의 제 1 공개키를 획득하는 단계; 상기 획득한 제 2 디바이스의 제 1 공개키로 상기 서명된 제 2 공개키를 검증하는 단계; 및 상기 검증 결과에 기초하여 암호화 통신을 수행할 수 있다.

[66] 상기 제 1 디바이스의 제 1 공개키 및 상기 제 1 디바이스의 제 1 개인키는, 이전의 상기 제 1 디바이스 및 상기 제 2 디바이스 간의 통신 수행시 사용된

키들일 수 있다.

[67] 상기 제 2 디바이스의 제 1 공개키 및 상기 제 2 디바이스의 제 1 개인키는, 이전의 상기 제 1 디바이스 및 상기 제 2 디바이스 간의 통신 수행시 사용된 키들일 수 있다.

[68] 상기 검증 결과에 기초하여 암호화 통신을 수행하는 단계는, 상기 검증 결과에 기초하여 암호화 키를 생성하거나, SAS(Short Authentication String) 계산을 수행할 수 있다.

[69] 상기 방법은, 상기 제 1 디바이스의 제 1 개인키, 상기 제 1 디바이스의 제 1 공개키 및 상기 제 2 디바이스의 제 1 공개키를 삭제할 수 있다.

[70] 상기 판단하는 단계는, 상기 통신 내역에 기초하여 이전 통신 수행시 상기 제 2 디바이스에게 송신한 제 1 난수가 저장되어 있는지 판단하는 단계를 포함하고, 상기 서명하는 단계는, 상기 통신 내역에 기초하여 이전 통신 수행시 상기 제 2 디바이스로부터 수신한 제 2 난수를 상기 제 1 디바이스의 제 1 개인키로 서명하는 단계를 포함하고, 상기 송신하는 단계는, 상기 서명된 제 2 난수를 송신하는 단계를 포함할 수 있다.

[71] 상기 서명된 제 2 공개키를 수신하는 단계는, 상기 제 2 디바이스의 제 1 개인키로 서명된 제 1 난수를 수신하는 단계를 포함하고, 상기 검증하는 단계는, 상 기 획득한 제 2 디바이스의 제 1 공개키로 상기 서명된 제 1 난수를 검증하는 단계를 포함할 수 있다.

[72] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로써, 본 개시의 일부 실시예는 상기 방법을 구현하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

[73] 상기와 같은 종래 기술의 문제를 해결하기 위한 일부 실시예는, 암호화된 데이터 송신을 위한 키를 공유하는 제 1 디바이스 있어서, 통신 내역에 기초하여, 제 2 디바이스에게 송신한 제 1 디바이스의 제 1 공개키 및 상기 제 1 디바이스의 제 1 공개키에 대응하는 제 1 디바이스의 제 1 개인키가 저장되어 있는지 판단하는 제어부; 판단 결과에 기초하여 제 1 디바이스의 제 2 공개키 및 제 1 디바이스의 제 2 개인키를 생성하고, 상기 생성된 제 1 디바이스의 제 2 공개키를 상기 제 1 디바이스의 제 1 개인키로 서명하는 암호화부; 및 상기 서명된 제 2 공개키를 제 2 디바이스로 송신하는 통신부를 포함할 수 있다.

[74] 상기 통신부는, 상기 제 2 디바이스로부터 상기 제 2 디바이스의 제 1 개인키로 서명된 제 2 공개키를 수신하고, 상기 암호화부는, 통신 내역에 기초하여, 상기 제 2 디바이스의 제 1 개인키와 대응되는 상기 제 2 디바이스의 제 1 공개키를 획득하고, 상기 획득한 제 2 디바이스의 제 1 공개키로 상기 서명된 제 2 공개키를 검증하고, 상기 제어부는, 상기 검증 결과에 기초하여 암호화 통신을 수행할 지 여부를 결정할 수 있다.

[75] 상기 제 1 디바이스의 제 1 공개키 및 상기 제 1 디바이스의 제 1 개인키는, 이전의 상기 제 1 디바이스 및 상기 제 2 디바이스 간의 통신 수행시 사용된

키들일 수 있다.

[76] 상기 제 2 디바이스의 제 1 공개키 및 상기 제 2 디바이스의 제 1 개인키는, 이전의 상기 제 1 디바이스 및 상기 제 2 디바이스 간의 통신 수행시 사용된 키들일 수 있다.

[77] 상기 암호화부는, 상기 검증 결과에 기초하여 암호화 키를 생성하거나, SAS(Short Authentication String) 계산을 수행할 수 있다.

[78] 상기 암호화부는, 상기 제 1 디바이스의 제 1 개인키, 상기 제 1 디바이스의 제 1 공개키 및 상기 제 2 디바이스의 제 1 공개키를 삭제할 수 있다.

[79] 상기 제어부는, 상기 통신 내역에 기초하여 이전 통신 수행시 상기 제 2 디바이스에게 송신한 제 1 난수가 저장되어 있는지 판단하고, 상기 암호화부는, 상기 통신 내역에 기초하여 이전 통신 수행시 상기 제 2 디바이스로부터 수신한 제 2 난수를 상기 제 1 디바이스의 제 1 개인키로 서명하며, 상기 통신부는, 상기 서명된 제 2 난수를 송신할 수 있다.

[80] 상기 통신부는, 상기 제 2 디바이스의 제 1 개인키로 서명된 제 1 난수를 수신하고, 상기 암호화부는, 상기 획득한 제 2 디바이스의 제 1 공개키로 상기 서명된 제 1 난수를 검증할 수 있다.

발명의 실시를 위한 형태

[81] 본 발명에서 사용되는 용어는 본 발명에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도 또는 판례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 발명의 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 발명에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 발명의 전반에 걸친 내용을 토대로 정의되어야 한다.

[82] 본 명세서에서, 어떤 부분이 다른 부분과 연결되어 있다고 할 때, 이는 직접적으로 연결되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 전기적으로 연결되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 포함한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어 또는 소프트웨어로 구현되거나 하드웨어와 소프트웨어의 결합으로 구현될 수 있다.

[83] 본 명세서에서 디바이스라 함은, 퍼스널 컴퓨터(Personal Computer), 휴대폰(Cellular Phone), 스마트 폰, TV, 타블렛, 노트북, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 네비게이션, MP3 플레이어, 디지털 카메라 등의 디바이스를 포함할 수 있고, 상기 예시에 제한되지 않으며, 다양한 디바이스를 포함할 수 있다.

[84] 본 명세서에서, 디바이스 키라 함은 공개키(비대칭키)를 포함할 수 있으며, 추가적으로 비밀키(대칭키)를 포함할 수 있다. 디바이스 키는 디바이스 간 암호화 통신을 위해 사용되는 데이터를 의미할 수 있다. 디바이스 키는 디바이스 내에 저장된 키 연산 알고리즘을 통해 생성될 수 있다. 키 연산 알고리즘은 AES, MD5, ECDH 등 다양한 알고리즘을 포함할 수 있으며, 상기 예시에 제한되지 않는다. 또한 키 연산 알고리즘은 당업자에게 자명하므로, 자세한 설명은 생략한다.

[85] 본 명세서에서 키의 교환이라 함은, 제 1 디바이스와 제 2 디바이스가 제 1 디바이스 키 또는 제 2 디바이스 키 중 적어도 하나를 송신 및 수신하는 절차를 의미할 수 있다. 즉, 두 디바이스 간에 두 디바이스의 키를 송수신하는 과정을 의미할 수 있다.

[86] 본 명세서에서 키의 공유라 함은, 제 1 디바이스가 제 2 디바이스가 제 1 디바이스 키 및 제 2 디바이스 키뿐만 아니라 제 3 디바이스 키 또한 송수신하는 과정을 의미할 수 있다. 즉, 두 디바이스 이외의 다른 디바이스의 키를 송수신하는 과정을 의미할 수 있다. 물론 키 공유는 키 교환을 포함하는 개념일 수도 있다. 나아가, 키의 공유는 키를 협의하여 결정하는 것, 협의된 키를 전송하는 것, 협의된 키를 수신하는 것을 포함할 수 있으나, 이에 제한되는 것은 아니다.

[87] 본 명세서에서 근거리 통신 방식이라 함은, 두 디바이스가 소정의 범위 내에 있을 때에만 통신이 가능한 통신 방식을 의미할 수 있으며, 예를 들어, 블루투스, NFC 등을 포함할 수 있다. 물론 상기 예시에 제한되는 것은 아니다.

[88] 본 명세서에서 원거리 통신 방식이라 함은, 두 디바이스가 거리와 관계 없이 통신이 가능한 통신 방식을 의미할 수 있으며, SMS, 전화와 같은 셀룰러 네트워크를 이용한 통신 방식을 포함할 수 있다. 물론 상기 예시에 제한되는 것은 아니다.

[89] 본 명세서에서, 난수는 함수에 의해 출력되는 값을 다르기 위해서 함수에 입력되는 값에 추가되는 임의의 값을 의미할 수 있다. 예를 들어, 해시 함수에 입력되는 값이 동일할 경우 출력되는 값은 항상 동일하므로, 출력 값을 다르게 하기 위해 입력 값에 난수를 추가하여 해시함수의 값을 구할 수 있다.

[90] 본 명세서에서, 제1 디바이스의 난수를 제1 난수라 하고, 제2 디바이스의 난수를 제2 난수라 할 수 있다. 예를 들어, 제1 디바이스가 공개키를 전송하면서 생성한 임의의 값을 제1 난수라 할 수 있고, 제2 디바이스가 공개키를 전송하면서 생성한 임의의 값을 제2 난수라 할 수 있다.

[91] 본 명세서에서, 공개키(public key)란 제3자에게 배포될 수 있는 값으로서, 이 공개키로부터 생성된 개인키(private key)와 쌍을 이룰 수 있다. 또한 공개키와 개인키는 비대칭키 방식일 수 있다. 즉, 개인키란 제3자에게 배포되지 않는 값으로서, 공개키로 암호화된 데이터는 개인키에 의해서만 복호화될 수 있다.

[92] 본 명세서에서, 비공개키란 제3자에게 노출되지 않고, 송수신 디바이스, 즉

송신 디바이스와 수신 디바이스 사이에서 공유되는 값으로서, 대칭키의 의미를 가질 수 있다.

[93] 본 명세서에서, 데이터 세트는 데이터 제공자에 의해서 제공되어 특정 시간에 제작된 특정 데이터의 묶음을 의미할 수 있다.

[94] 본 명세서에서, 해시 함수(hashing function)는 어떤 입력 값에 대한 테이블 주소(table address)를 계산하기 위한 방법으로서, 주어진 입력 값으로부터 레코드가 저장되어 있는 주소를 산출해 낼 수 있는 수식을 의미할 수 있다. 해쉬함수는 동일한 입력에 대해서는 언제나 동일한 값을 출력한다. 해시함수의 특징은 입력값을 이용하여 출력값을 획득하는 것은 쉽지만, 출력값으로부터 입력값을 거꾸로 유추하는 것은 거의 불가능하다는 점이다.

[95] 본 명세서에서, 키를 갖는 해시함수(keyed hash)는 기본 입력 값 외에도 키를 추가적으로 필요로 하는 함수를 의미할 수 있다. 키가 없는 해시 함수의 경우 주어진 입력 값을 아는 누구라도 해시 값을 계산할 수 있는 반면, 키를 갖는 해시 함수의 경우는 주어진 입력 값을 알더라도 키가 있는 사람만이 그 해시 값을 계산할 수 있다. 본 명세서에서, k라는 키를 갖는 해시함수는 $f_k(x)$는 f(k,x)로 표현될 수도 있다. 또한, 본 명세서에서 $f_k(x)$는 x를 k로 키-해싱한다(keyed hash)고 표현될 수도 있다. 또한 키를 갖는 해시 함수는 해시 함수 범위에 포함될 수 있다.

[96] 본 개시에서, 암호화키는 데이터를 암호화하기 위한 정보를 포함할 수 있따. 로서, 예를 들어 암호화 키는, 이미지를 암호화하기 위한 스크램블키 등을 포함할 수 있으나 상기 예시에 제한되지 않는다. 암호화키는 랜덤하게 생성될 수 있고, 데이터를 송신하는 디바이스나 수신하는 디바이스의 공개키나 비밀키를 이용하여 생성될 수도 있다. 예를 들어, 제1 디바이스와 제2 디바이스의 키 교환과정에서 디피-헬만(D-H) 방식에 의해 생성되는 키를 이용하여 암호화키가 생성될 수 있다. 물론 상기 예시에 제한되지 않는다.

[97] 본 명세서에서, 키식별정보는 암호화된 데이터를 송신하는 송신 디바이스와 수신 디바이스 간에서만 식별가능한 정보로서, 수신 디바이스는 키식별정보를 이용하여 송신 디바이스를 파악하여 암호화된 데이터를 복호화할 수 있다. 다만, 제3자는 키식별정보로부터 송신 디바이스 또는 수신 디바이스의 정보를 획득할 수 없다. 따라서, 본 발명의 일 실시예에 따르면, 송수신 디바이스의 프라이버시가 보장되는 효과를 가질 수 있다.

[98] 상용 인터넷 메신저(IM)의 경우 IM에서 사용하는 ID는 전화번호나 이름이 아닌 다른 것을 사용하며 이를 IM서버에서 매핑시켜 수신 디바이스에게 데이터를 전달하게 된다. 그러므로 송신 디바이스와 수신 디바이스가 아닌 제3자가 공중(air)에서 패킷(packet)을 캡쳐하더라도, 일반적으로는 송/수신자의 정보를 알기 어렵다.

[99] 다만, IM을 이용한 통신 방식에서도 모든 통신 과정이 서버에서 수행되는 것은 아니다. 수신 디바이스가 수신한 패킷 내의 암호화 되지 않는 데이터(예를 들면,

메시지 정보)는 별도의 절차를 수행하지 않고도 확인이 가능하지만, 암호화된 데이터를 확인하기 위해서는 수신 디바이스가 복호화를 수행해야 한다. 따라서, IM을 이용한 통신 방식에서도 송신 디바이스는 복호화를 위해 송신 디바이스의 정보를 삽입하여 제공하게 된다. 따라서, 제3자가 패킷을 캡쳐하는 경우에는, 암호화된 데이터를 복호화할 수는 없지만 송수신 디바이스의 정보를 획득할 가능성을 배제할 수 없다. 띠리사. 일부 실시예에 따르면, 프라이버시 정보의 식별을 방지하기 위해 송수신 디바이스는 각 디바이스의 정보를 제3자가 알기 어렵도록 변환하거나, 대체하여 송신할 수 있다

[100] 도 1은 일부 실시예에 따른 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 제1 디바이스와 제2 디바이스 사이에서 전송하거나 수신하는 디바이스를 도시화한 것이다.

[101] 일부 실시예에 따르면, 제 1 디바이스 및 제 2 디바이스는 각각 송신 디바이스 및 수신 디바이스일 수 있으며, 제 1 디바이스와 제 2 디바이스는 키식별정보를 사용함으로써, 제 3 자가 송신 디바이스 또는 수신 디바이스에 대한 정보를 식별할 수 없도록 한다.

[102] 단계 101에서, 데이터를 송신하는 제1 디바이스와 데이터를 수신하는 제2 디바이스는 서로의 키를 교환한다. 즉, 제1 디바이스는 제2 디바이스로부터 제2 디바이스의 키를 수신하고, 제1 디바이스의 키를 전송할 수 있다. 제 1 디바이스의 키 및 제 2 디바이스의 키는 공개키 또는 비밀키(비공개키)를 포함할 수 있다. 또한 제 1 디바이스와 제 2 디바이스는 각각의 디바이스에서 생성된 소정의 값(예를 들면, 난수)을 키와 함께 교환할 수 있다.

[103] 단계 102에서, 일부 실시예에 다르면, 제1 디바이스는 암호화키를 생성할 수 있다. 암호화키는 제2 디바이스와 미리 교환한 공개키 또는 비밀키를 이용하여 생성될 수 있으나, 랜덤하게 생성될 수도 있다. 일부 실시예에 따르면, 암호화키는 제 1 디바이스와 제 2 디바이스 간에 송신되는 데이터를 암호화 하는데 사용되는 키 데이터를 포함할 수 있다.

[104] 또한 단계 102에서, 제1 디바이스는 암호화키를 이용하여 송신할 데이터를 암호화할 수 있다. 또한 제 1 디바이스는 키식별정보를 생성할 수 있다. 일부 실시예에 따른키식별정보의 생성은 데이터의 암호화보다 먼저 수행되거나 후에 수행될 수도 있다.

[105] 단계 103에서, 제 1 디바이스는 단계 102에서 생성한 키식별정보와 암호화된 데이터를 송신할 수 있다. 일부 실시예에 따르면, 제 1 디바이스는 생성된 키식별정보와 암호화된 데이터를 한꺼번에 또는 각각 별도로 송신할 수 있다.

[106] 단계 104에서, 제 2 디바이스는 수신된 키식별정보를 이용하여, 송신한 제1 디바이스를 식별할 수 있다. 또한 제 2 디바이스는 키식별정보에 기초하여 암호화키를 도출해 내거나, 그러나 제 1 디바이스 또는 제 2 디바이스 이외의 다른 디바이스(예를 들면, 제3자)는 키식별정보만으로는 송신디바이스나 수신 디바이스를 식별할 수 없다.

[107] 일부 실시예에 따르면, 키식별정보는 제2 디바이스가 식별할 수 있는 제1 디바이스의 식별정보(예를 들어, 아이디, 이름, 전화번호, 디바이스의 키 등)를 제2 디바이스가 알아볼 수 있는 형태로 암호화한 것일 수 있다. 또한 일부 실시예에 따르면, 키식별정보는 단계 101에서 교환된 제 1 디바이스의 키, 제 2 디바이스의 키, 각각의 디바이스에서 생성된 소정의 값, 암호화키 중 적어도 하나에 기초하여 생성될 수 있다.

[108] 도 2는 일부 실시예에 따른 제1 디바이스에서 제2 디바이스로 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 송신하는 방법을 도시하는 흐름도이다.

[109] 단계 201에서, 제1 디바이스는 암호화키를 생성한다. 암호화키는 제2 디바이스에게 송신한 제 1 디바이스의 키 또는 제 2 디바이스로부터 수신된 제 2 디바이스 키에 기초하여 생성될 수도 있고, 난수에 기초하여 생성될 수도 있다.

[110] 또한 일부 실시예에 따르면, 제1 디바이스는 제2 디바이스와 디바이스 키를 교환할 수도 있다. 교환되는 디바이스 키는 공개키 또는 비밀키를 포함할 수 있다. 또한 제 1 디바이스 및 제 2 디바이스는 난수를 생성하고 생성된 난수를 각 디바이스의 키와 함께 교환할 수도 있다.

[111] 일부 실시예에 따르면, 암호화키의 생성은 제 1 디바이스와 제 2 디바이스 간의 디바이스의 키 교환 이전 또는 이후에 수행될 수 있다. 암호화키는 교환된 디바이스의 키 또는 교환된 난수에 기초하여 생성될 수 있다.

[112] 단계 203에서, 제1 디바이스는 생성된 암호화키를 이용하여 키식별정보를 생성하고 암호화된 데이터를 생성할 수 있다.

[113] 일부 실시예에 따르면, 키식별정보는 제2 디바이스가 제 1 디바이스를 식별할 수 있게 한다. 다시 말해서, 제 2 디바이스 또한 제 1 디바이스와 교환한 디바이스 키 및 난수에 기초하여 키식별정보를 생성할 수 있으므로, 제 2 디바이스는 제 1 디바이스를 식별할 수 있다. 제 2 디바이스는 키식별정보에 기초하여 암호화키를 획득할 수 있다. 암호화키일부 실시예에 따르면, 제 1 디바이스와 제 2 디바이스는 디바이스의 키를 교환하지 않을 수도 있다. 즉, 제 1 디바이스는 디바이스의 키 교환 없이 암호화키 제 1 디바이스의 식별 정보와 제 2 디바이스의 식별 정보에 기초하여 키식별정보를 생성할 수도 있다.

[114] 또한 일부 실시예에 따르면, 제 1 디바이스는 제 1 디바이스와 제 2 디바이스가 사용하는 어플리케이션의 정보에 기초하여 키식별정보를 생성할 수도 있다. 예를 들면, 제 1 디바이스는 제 2 디바이스와 사용하는 소정의 메신저 어플리케이션의 정보에 기초하여 키식별정보를 생성할 수도 있다.

[115] 암호화키제 2 디바이스는 키식별정보 및 제 2 디바이스의 식별 정보를 이용해서, 암호화키를 획득할 수 있다. 예를 들면, 디바이스의 식별정보는 디바이스의 전화번호, MAC 주소, IP 주소, 디바이스 제조번호 등을 포함할 수 있으며, 상기 예시에 제한되지 않는다. 일부 실시예에 따르면, 제 1 디바이스가 암호화키를 이용하여 데이터를 암호화하여 암호화된 데이터를 생성하는 단계는

공지된 여러 방법에 의해 구현될 수 있다. 예를 들어 제 1 디바이스는 데이터를 보호하기 위해 소정의 양식에 따라서 데이터를 혼합하거나 또는 무질서하게 재배열(암호화)하여 소정의 키에 의해서만 복호화될 수 있도록 데이터를 처리할 수 있다.

[116] 또한 일부 실시예에 따르면, 제 1 디바이스는 데이터를 전송할 때 데이터를 스크램블링함으로써, 특정한 키를 가지고 있는 자만이 원 데이터를 복원할 수 있도록 데이터를 처리할 수 있다..

[117] 또한 일부 실시예에 따르면, 일부 실시예에 따른제 1 디바이스의 키식별정보의 생성 단계와 암호화된 데이터의 생성 단계의 순서는 구현 예에 따라 변경될 수 있다.

[118] 단계 205에서, 제1 디바이스는 생성된 키식별정보 및 암호화된 데이터를 포함하는 데이터 세트를 제2 디바이스로 송신할 수 있다. 또한 제 1 디바이스가 송신하는 데이터가 이미지 데이터인 경우, 키식별정보는 이미지 데이터 내에 삽입될 수도 있다.

[119] 일부 실시예에 따르면, 제 1 디바이스는 암호화키를 제 1 디바이스의 키 또는 제 2 디바이스의 키로 암호화 하여 송신할 수도 있다. 예를 들면, 제 1 디바이스는 제 1 디바이스의 공유 키를 이용하여 암호화키를 암호화하여 제 2 디바이스에게 제공할 수 있다. 제 2 디바이스는 키식별정보에 기초하여 제 1 디바이스를 식별하고, 제 1 디바이스의 공유 키를 이용하여 제 1 디바이스의 공유 키로 암호화된 암호화키를 복호화할 수 있다.

[120] 일부 실시예에 따르면, 제 1 디바이스는 제 2 디바이스를 포함한 복수의 디바이스에게 데이터 세트를 송신할 수도 있다. 제 1 디바이스는 제 2 디바이스를 포함한 복수의 디바이스 각각의 디바이스 키로 암호화 키를 암호화하고, 키식별 정보와 함께 제 2 디바이스를 포함한 복수의 디바이스 각각에게 송신할 수 있다.

[121] 또한 일부 실시예에 따르면, 제 1 디바이스는 제 2 디바이스의 디바이스 키를 이용하여 암호화키를 암호화하여 제 2 디바이스에게 제공할 수 있다. 제 2 디바이스는 제 2 디바이스의 키를 이용하여 암호화된 암호화키를 복호화할 수 있다.

[122] 도 3은 일부 실시예에 따른 제2 디바이스에서 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 제1 디바이스로부터 수신하는 방법을 도시하는 흐름도이다.

[123] 단계 301에서, 제2 디바이스는 제1 디바이스를 포함하는 적어도 하나의 디바이스와 디바이스 키를 교환할 수 있다. 일부 실시예에 따르면 디바이스 키는 디바이스의 공개키 또는 디바이스의 비공개키를 포함할 수 있다. 또한 일부 실시예에 따르면, 디바이스 키의 교환이란 각자의 키를 서로 전송하고 수신하는 것 중 적어도 하나를 의미할 수 있다. 예를 들어, 제1 디바이스가 제1 디바이스의 디바이스 키를 제2 디바이스로 전송하고 제2 디바이스로부터 제2 디바이스의

디바이스 키를 수신하는 것을 키의 교환이라고 할 수 있다. 또한, 제1 디바이스가 자신의 키를 전송할 필요가 없다면, 제2 디바이스의 디바이스 키를 제 2 디바이스로부터 수신하는 것을 키의 교환이라고 할 수 있다.

[124] 또한 일부 실시예에 따르면, 제 2 디바이스는 제 1 디바이스와 난수와 같은 소정의 값을 교환할 수도 있다.

[125] 단계 303에서, 제2 디바이스는 제1 디바이스로부터 암호화된 데이터 및 키식별정보를 포함하는 데이터 세트를 수신할 수 있다. 제 2 디바이스는 데이터 세트에 포함된 키식별정보에 기초하여 수신한 데이터 세트가 제 1 디바이스가 송신 및 암호화한 데이터 세트임을 확인할 수 있다. 다만 다른 디바이스(제3자)는 제 1 디바이스와 디바이스 키 또는 소정의 값을 교환한 바 없으므로, 데이터 세트 내에 포함된 키 식별 정보를 획득하더라도, 데이터 세트의 송신 디바이스에 관한 정보를 획득할 수 없다.

[126] 일부 실시예에 따르면, 데이터 세트는 메시지 인증 코드(MAC: message authentication code)를 더 포함할 수 있다. 메시지 인증 코드는 데이터를 수신한 제2 디바이스에서 획득한 암호화키가 올바른 암호화키인지를 판단하기 위해 이용될 수 있다

[127] 단계 305에서, 제2 디바이스는 키식별정보를 이용하여 암호화키를 획득할 수 있다. 예를 들어, 제 2 디바이스는 키식별정보를 통하여 데이터를 송신한 제1 디바이스를 식별하고, 제 1 디바이스와의 약속에 기초하여 생성된 암호화키를 획득할 수 있다.

[128] 일부 실시예에 따르면, 제 2 디바이스는 제1 디바이스의 디바이스 키 및 제2 디바이스의 디바이스 키에 기초하여 암호화키를 생성할 수 있다. 또한, 일부 실시예에 따르면, 암호화키가 제 2 디바이스의 디바이스 키로 암호화되어 있는 경우에는, 제2 디바이스는 제 2 디바이스 자신의 디바이스 키만으로 를 생성할 수도 있다. 또한, 암호화키 생성을 위해 키 교환과정에서 서로 교환된 소정의 값이필요할 수 있다.

[129] 단계 307에서, 제2 디바이스는 암호화키를 이용하여 암호화된 데이터를 복호화할 수 있다. 제 1 디바이스는 데이터를 보호하기 위해 소정의 양식에 따라서 데이터를 혼합 또는 무질서하게 재배열(암호화)하여 특정한 키에 의해서만 복호화될 수 있는 암호화된 데이터가 송신하였으며, 제 2 디바이스는 단계 305에서 획득한 암호화키를 이용하여 데이터를 복호화 할 수 있다.

[130] 도 4는 일부 실시예에 따른 공개키 및 난수를 이용하여 암호화된 데이터를 송신하는 방법을 도시하는 흐름도이다.

[131] 단계 401에서, 제1 디바이스는 제1 디바이스의 공개키 및 제1 난수를 제2 디바이스로 전송하고 제2 디바이스로부터 상기 제2 디바이스의 공개키 및 제2 난수를 수신한다. 제1 디바이스와 제2 디바이스의 공개키는 암호화키를 생성하기 위해 사용되며, 제1 난수와 제2 난수는 암호화키를 이용하여 키식별정보를 생성하기 위해 사용될 수 있다.

[132] 단계 403에서, 제1 디바이스는 제1 디바이스의 공개키 및 제2 디바이스의 공개키를 이용하여 암호화키(k_{ab})를 생성한다. 일부 실시예에 따른 암호화키는 디피-헬만(D-H) 방식에 의해 제1 디바이스와 제2 디바이스의 공개키를 이용하여 생성될 수 있으며 상기 예시에 제한되지 않는다.

[133] 단계 405에서, 제1 디바이스는 생성된 암호화키를 이용하여 데이터를 암호화한다.

[134] 단계 407에서, 제1 디바이스는 암호화키(k_{ab}) 및 상기 제1 난수, 제2 난수를 이용하여 키식별정보(k_{id})를 생성한다. 키식별정보(k_{id})는 제1 난수와 제2 난수를 조합한 값을 암호화키로 해싱한 값일 수 있다. 예를 들면, 키식별정보는 k_{id} =lnonce_allnonce_bl k_{ab} 로 표현될 수 있으며, 상기 예시에 제한되지 않는다.

[135] 단계 409에서, 제1 디바이스는 키식별정보 및 암호화된 데이터를 제2 디바이스로 송신한다.

[136] 도 5는 일부 실시예에 따른 공개키 및 난수를 이용하여 암호화된 데이터를 수신하는 방법을 도시하는 흐름도이다.

[137] 단계 501에서, 제2 디바이스는 제1 디바이스를 포함하는 복수의 외부 디바이스들과 공개키 및 난수를 각각 교환한다. 또한 암호화된 데이터의 송신이 예상되는 디바이스가 제1 디바이스뿐인 경우, 제2 디바이스는 제1 디바이스와의 사이에서만 공개키 및 난수를 교환할 수 있다.

[138] 단계 503에서, 제2 디바이스는 수신된 복수의 공개키를 이용하여 복수의 디바이스에 대한 복수의 암호화키를 생성한다. 예를 들어, 복수의 암호화키는 제1 디바이스의 공개키를 이용한 암호화키를 포함할 수 있다. 제1 디바이스의 공개키를 이용한 암호화키는 제1 디바이스로부터 수신된 암호화된 데이터를 복호화할 때 사용될 수 있다.

[139] 단계 505에서, 생성된 복수의 암호화키를 이용하여 복수의 키식별정보를 각각 생성한다.

[140] 단계 507에서, 제2 디바이스는 생성된 복수의 키식별정보와 수신된 키식별정보를 비교하여 데이터를 송신한 제1 디바이스 키를 식별(identify)한다.

[141] 일부 실시예에 따르면, 키의 식별이라 함은 제2 디바이스가 키식별정보에 기초하여 단계 501에서 제 1 디바이스를 포함하는 복수의 디바이스와 교환한 복수의 공개키 중에 제1 디바이스의 공개키를 선택하거나, 제 1 디바이스의 공개키를 이용한 암호화키가 어떤 것인지를 선택하는 동작을 포함할 수 있다.

[142] 단계 509에서, 제 2 디바이스는 식별된 제 1 디바이스에 대응하는 암호화키를 획득할 수 있다. 다시 말해서, 제 2 디바이스는 단계 507에서의 제 1 디바이스 키를 식별하고, 식별 결과에 기초하여 제 1 디바이스에 대응하는 암호화 키를 선택 또는 획득할 수 있다.

[143] 단계 511에서, 제2 디바이스는 식별된 제1 디바이스에 대한 암호화키를 이용하여 제 1 디바이스가 송신한 암호화된 데이터를 복호화한다.

[144] 도 6은 일부 실시예에 따른 제1 디바이스가 제2 디바이스의 공개키를 이용하여

암호화키를 송신하는 방법을 도시한 흐름도이다.

[145] 단계 601에서, 제1 디바이스가 제2 디바이스의 공개키를 수신한다. 물론, 제1 디바이스도 제 1 디바이스의 공개키를 제2 디바이스로 전송할 수 있다. 단계 602에서, 제1 디바이스가 데이터를 암호화하기 위한 암호화키를 생성한다. 암호화키는 랜덤하게 생성될 수 있다. 또한, 암호화키는 제1 디바이스 및 제2 디바이스 중 적어도 하나의 공개키에 기초하여 생성될 수 있다.

[146] 단계 603에서, 제1 디바이스가 제2 디바이스의 공개키(Pr2)를 이용하여 암호화키(g)를 암호화하여 키식별정보(k_{id})를 생성한다. 일부 실시예에 따르면, 키식별정보라 함은, 암호화키를 암호화하여 생성된 정보일 수 있다. 예를 들면, 키식별정보는 k_{id}=E_Pr2(g)로 표현될 수 있다. 또한, 일부 실시예에 따르면, 키식별정보는 입력을 암호화키로 하고 해시함수 키를 제 2 디바이스의 공개키로 하는, 키를 갖는 해시함수(keyed hash)의 결과값일 수 있다. 예를 들면, $k_{id}=f_{pr2}(g)$로 표현될 수 있다.

[147] 단계 605에서, 제1 디바이스는 생성된 키식별정보 및 암호화키에 의해 암호화된 데이터를 제2 디바이스로 송신한다.

[148] 도 7은 일부 실시예에 따른 제2 디바이스가 제2 디바이스의 공개키를 이용하여 암호화된 데이터를 수신하는 방법을 도시한 흐름도이다.

[149] 단계 701에서, 제2 디바이스는 제1 디바이스와 키를 교환한다. 예를 들어, 제2 디바이스는 제2 디바이스의 공개키를 제1 디바이스로 전송할 수 있다.

[150] 단계 703에서, 제2 디바이스는 제1 디바이스로부터 키식별정보 및 암호화된 데이터를 수신한다.

[151] 단계 705에서, 제2 디바이스는 수신된 키식별정보로부터 데이터를 복호화하기 위한 암호화키를 획득한다. 키식별정보는 제1 디바이스가 제2 디바이스의 공개키를 이용하여 암호화키를 암호화한 데이터 일 수 있다. 제2 디바이스는 키식별정보를 제2 디바이스의 공개키(public key)에 대응하는 제2 디바이스의 개인키(private key)를 이용하여 복호화하여 암호화키를 획득할 수 있다.

[152] 단계 707에서, 제2 디바이스는 단계 705에서 획득한 암호화키를 이용하여 수신된 암호화된 데이터를 복호화한다.

[153] 도 8은 일부 실시예에 따른 공유된 비공개키를 이용하여 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 전송하고 수신하는 방법의 흐름도이다.

[154] 단계 801에서, 제1 디바이스와 제2 디바이스가 동일한 비공개키를 공유한다. 비공개키는 대칭키로서, 제1 디바이스와 제2 디바이스 사이에서만 공유되는 데이터이며, 제 1 디바이스 및 제 2 디바이스를 제외한 다른 디바이스에게 노출되지 않는 데이터일 수 있다.

[155] 일부 실시예에 따르면, 비공개키의 공유라 함은 비공개키를 서로 전송하는 절차뿐만 아니라, 소정의 절차에 의해 비공개키를 서로 결정, 선택 또는 생성하는 절차를 더 포함할 수도 있다.

[156] 단계 802에서, 제1 디바이스는 비공개키와 제1 난수를 이용하여 암호화키(S)를

생성한다. 일부 실시예에 따르면, 비공개키는 마스터키(Masterkey)포함할 수 있다. 일부 실시예에 따르면 암호화 키는 마스터키 및 넌스(nonce)와 같은 소정의 값에 의해 생성될 수 있으며, 상기 예시에 제한되지 않는다.(암호화키(S) = 마스터키(Masterkey)+소정의 값(nonceA))

[157] 단계 803에서, 제1 디바이스에서는 제1 난수로 암호화키를 키-해싱한 값(세션키)을 제1 난수 및 암호화된 데이터와 함께 제2 디바이스로 송신한다. 즉, 제 1 디바이스가 전송하는 데이터는 ①제1 난수, ②세션키, ③암호화된 데이터를 포함할 수 있다.

[158] 또한 일부 실시예에 따르면, 제1 디바이스는 생성된 암호화키를 이용하여 데이터를 암호화할 수 있다.

[159] 단계 805에서, 제2 디바이스는 제1 난수, 세션키, 암호화된 데이터를 수신한다. 세션키는 전술한 메시지 인증 코드(MAC)을 포함할 수 있다.

[160] 단계 807에서, 제2 디바이스는 수신한 제1 난수를 이용하여, 기존에 공유한 제 1 디바이스를 포함한 모든 송신 디바이스의 비공개키(MK1~MKn)와 제1 난수를 조합한 복수의 후보 암호화키들(S1~Sn)을 생성한다.

[161] 단계 809에서, 제2 디바이스는 생성된 복수의 후보 암호화키들(S1~Sn) 를 제1 난수로 각각 키-해싱하여 복수의 후보 매칭키들(SS1~SSn)을 생성한다. 복수의 후보 매칭키들은 수식으로서 $f_{nonceA}(S1)$, $f_{nonceA}(S2)$, ..., $f_{nonceA}(Sn)$과 같이 표현될 수 있다. 일부 실시예에 따르면 넌스(nonce)는 소정의 값으로써, 제 1 디바이스 또는 제 2 디바이스가 생성하는 난수(Random Number)를 포함할 수 있다.

[162] 단계 811에서, 제2 디바이스는 생성한 복수의 후보 매칭키들(SS1~SSn)과 수신한 세션키를 비교하여, 세션키를 송신한 제1 디바이스의 세션키를 식별할 수 있다. 또한 일부 실시예에 따르면, 제 2 디바이스는 제1 디바이스와 공유한 비공개키를 식별할 수 있다.

[163] 단계 813에서, 제2 디바이스는 데이터를 송신한 제1 디바이스와 공유한 비공개키와 제1 난수의 조합에 의한 암호화키를 획득할 수 있다.. 또한 일부 실시예에 따르면, 제1 디바이스와 대응하는 암호화키는 제 2 디바이스가 단계 809에서 생성한 n개의 암호화키들 중 1개에 해당하므로, 제2 디바이스는 세션키에 기초하여 제 2 디바이스가 생성한 후보 암호화키들(S1~Sn) 중 하나를 선택할 수도 있다. 단계 815에서, 제2 디바이스는 획득한 암호화키에 의해 암호화된 데이터를 복호화한다.

[164] 도 9는 일부 실시예에 따른 디바이스의 식별넘버를 이용하여 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 송신하는 방법을 도시한 흐름도이다.

[165] 단계 901에서, 제1 디바이스는 암호화키를 생성한다. 일부 실시예에 따르면, 암호화키는 제1 디바이스의 식별넘버(Pa) 및 제2 디바이스의 식별넘버(Pb)보다 작은 난수를 포함할 수 있다.

[166] 일부 실시예에 따르면, 식별넘버는 전화번호 또는 아이디 등을 포함할 수

있으며, 식별넘버 또는 암호화키가 정수가 아닌 경우 소정의 테이블에 의해 정수로 변환되어 도 9의 절차에서 사용될 수 있다. 또한 일부 실시예에 따르면, 식별넘버는 식별키일 수 있다. 단계 903에서, 제1 디바이스는 암호화키를 이용하여 데이터를 암호화한다.

[167] 단계 905에서, 제1 디바이스는 암호화키를 이용하여 제1 디바이스의 식별넘버(Pa) 및 제2 디바이스의 식별넘버(Pb)의 곱 또는 최대 공약수에 암호화키(R)를 더한 값을 포함하는 키식별정보(k_{id})를 생성한다. 예를 들면, 키식별정보는 k_{id}=pa*pb+r의 수식에 의해 생성될 수 있으며, 다만 상기 예시에 제한되지 않는다.

[168] 단계 907에서, 제1 디바이스는 암호화된 데이터 및 키식별정보를 포함하는 데이터 세트를 제2 디바이스로 송신한다. 데이터 세트를 수신 받은 제2 디바이스의 동작은 도 10과 관련하여 자세히 설명한다.

[169] 도 10는 일부 실시예에 따른 디바이스를 식별할 수 있는 정수를 이용하여 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 수신하는 방법을 도시한 흐름도이다.

[170] 단계 1001에서, 제2 디바이스는 키식별정보(Pa*Pb+R) 및 암호화된 데이터를 수신한다.

[171] 단계 1003에서, 제2 디바이스는 키식별정보(Pa*Pb+R) 를 제2 디바이스의 식별넘버로 나누고 남는 R을 획득한다. 여기에서 R은 제1 디바이스가 데이터를 암호화한 암호화키일 수 있다.

[172] 단계 1005에서, 제2 디바이스는 암호화키 R을 이용하여 수신된 암호화된 데이터를 복호화한다.

[173] 도 11은 일부 실시예에 따른 암호화된 데이터를 저장하면서 제1 디바이스의 식별정보를 획득하는, 암호화된 데이터를 수신하는 방법을 도시하는 흐름도이다.

[174] 단계 1101에서, 제2 디바이스는 수신된 암호화된 데이터를 저장하는 과정에서 제1 디바이스의 식별정보를 획득한다. 식별정보를 획득하는 과정은 예를 들어 수신 디바이스가 소정의 리스트에 기재된 디바이스들 중 송신 디바이스를 선택하고, 선택한 송신 디바이스의 식별정보를 암호화된 데이터에 부가하여 저장하는 과정을 포함할 수 있다.

[175] 일부 실시예에 따르면, 제 2 디바이스가 제 1 디바이스의 식별정보를 획득하는 방법은 앞선 도 1 내지 도 10에서 설명한 바와 같이 다양한 파라미터(예를 들면, 난수, 비공개키, 등)에 의해 생성될 수 있다.

[176] 또한, 본 발명의 일 실시예에 따르면, 제2 디바이스는 수신된 데이터를 저장하면서 데이터를 송신한 제1 디바이스를 식별하는 식별정보를 생성할 수 있다.

[177] 일부 실시예에 따르면, 제 2 디바이스는 제 1 디바이스를 포함하는 복수의 디바이스와 비공개키를 공유할 수 있다.

[178] 단계 1103에서, 제2 디바이스는 획득된 제1 디바이스의 식별정보를 이용하여 제1 디바이스의 비공개키를 획득한다. 즉, 제 2 디바이스는 단계 1101에서 생성된 식별정보에 기초하여 송신 디바이스인 제 1 디바이스의 비공개키를 획득할 수 있다.

[179] 단계 1105에서, 제2 디바이스는 제1 디바이스의 비공개키를 이용하여 암호화키를 생성한다. 일부 실시예에 따르면, 제 1 디바이스의 비공개키는 제 1 디바이스가 데이터를 암호화할 때 사용한 암호화키와 동일할 수 있다.

[180] 단계 1107에서, 제2 디바이스는 암호화키를 이용하여 암호화된 데이터를 복호화한다.

[181] 일부 실시예에 따르면, 제 2 디바이스는 암호화 키를 이용하여 암호화 키와 대응하는 복호화 키를 생성하고, 생성된 복호화 키를 이용하여 암호화된 데이터를 복호화할 수 있으며, 암호화 키를 이용하여 복호화를 수행할 수도 있다.

[182] 도 12는 일부 실시예에 따른 송신 디바이스가 소정의 디바이스의 그룹에 대하여 암호화된 데이터를 송신하는 방법을 도시하는 개념도이다.

[183] 도 12(a)는 수신 디바이스가 하나인 경우에 송신 디바이스가 생성하는 데이터 세트를 도시한다. 도 12(a)의 데이터 세트는 공개키를 이용하여 생성된 암호화키와 키식별정보를 포함할 수 있다.

[184] 도 12(b)는 수신 디바이스가 복수의 디바이스를 포함하는 그룹인 경우 송신 디바이스가 생성하는 데이터 세트를 도시한다. 도 12(b)의 데이터 세트는 도 12(a)와는 상이하게, 복수의 키식별정보를 포함하는 데이터 세트의 구조를 도시한다. 수신 디바이스 각각에 대하여 키식별정보가 생성되므로, 도 12(b)의 데이터 세트는 수신 디바이스의 수에 대응하는 키식별정보가 포함될 수 있다.

[185] 도 12(c)는 수신 디바이스가 하나인 경우 송신 디바이스가 암호화키(g)를 수신하는 디바이스의 공개키로 암호화하여, 암호화된 공개키와 암호화된 데이터를 포함하는 데이터 세트의 구조를 도시한 것이다. 도 12(c)의 데이터 세트에는 키식별정보 대신 수신 디바이스의 공개키로 암호화된 암호화키가 포함될 수 있다.

[186] 도 12(d)는 수신 디바이스가 복수의 디바이스를 포함하는 그룹일 경우 송신 디바이스가 송신하는 데이터 세트를 도시한다. 도 12(c)와는 상이하게, 도 12(d)의 데이터 세트는 복수의 디바이스의 공개키로 각각 암호화키를 암호화한, 복수의 암호화키가 포함될 수 있다.. 예를 들면, E_Pr1(g)는 암호화키(g)를 제1 수신 디바이스의 공개키로 암호화한 것을 의미하고, E_Pr2(g)는 암호화키(g)를 제2 수신 디바이스의 공개키로 암호화한 것을 의미할 수 있다. c는 난수를 의미할 수 있다. 다만 상기 예시에 제한되지 않는다.

[187] 일부 실시예에 따르면, 데이터 세트는 메시지 인증 코드(MAC: message authentication code)를 포함할 수 있다. 메시지 인증 코드는 수신 디바이스에서 획득한 암호화키가 올바른 암호화키인지를 판단하기 위해 이용될 수 있다. 예를

들어, 도 12(d)의 hash(gllc)는 그룹을 위한 여러 개의 키식별정보 중 어느 것이 데이터 세트를 수신한 디바이스를 위한 키식별정보인지 파악하기 위한 값일 수 있다.

[188] 예를 들어, 데이터 세트를 수신한 수신 디바이스가 E_Pr1(g) 값을 자신의 개인키로 복호화하면 g값을 획득할 수 있다. 수신 디바이스는 획득한 g값과 데이터 세트 내의 c 값을 해시하고, 해시한 값이 수신한 데이터 세트 내의 hash(gllc)와 동일한지 판단할 수 있다. 수신 디바이스는 판단 결과에 따라, E_Pr1(g)값이 수신 디바이스를 위한 키식별정보인지를 파악할 수 있다. 동일하지 않다면, 수신 디바이스는 E_Pr2(g), E_Pr3(g) 등에 대하여 동일한 과정을 반복하여, 수신 디바이스를 위한 키식별정보를 식별할 수 있다.

[189] 도 12(e)는 수신 디바이스가 하나인 경우 식별넘버를 이용하여 암호화된 데이터를 송신하는 방법의 데이터 세트의 구조를 도시한 것이다. 앞서 설명한 바와 같이 식별넘버는 전화번호와 같은 소정의 정수로 이루어진 데이터를 포함할 수 있다.

[190] 일부 실시예에 따르면, 도 12(e)에서의 Pa는 제1 디바이스의 전화번호이고, Pb는 제2 디바이스의 전화번호이며, R은 제1 디바이스의 전화번호(Pa) 및 제2 디바이스의 전화번호(Pb)보다 작은 랜덤한 정수일 수 있다. 또한, R이 정수가 아니라 문자나 소수인 경우에도 테이블 등에 의하여 정수로 변환하여 상술한 방법에 적용할 수 있다.

[191] 도 12(f)는 수신 디바이스가 복수의 디바이스를 포함하는 그룹인 경우 전화번호 등의 식별넘버를 이용하여 암호화된 데이터를 송신하는 방법의 데이터 세트의 구조를 도시한 것이다. 도 12(e)와는 상이하게, 도 12(f)의 데이터 세트에서는 Pa(송신 디바이스의 전화번호)*Pb1(수신자1의 전화번호)* Pb2(수신자2의 전화번호)* Pb3(수신자3의 전화번호)+R(암호화키)에 의해 생성된 키 식별정보를 포함할 수 있다.

[192] 일부 실시예에 따르면, 복수의 디바이스 중 도 12(f)의 데이터 세트를 수신한 수신 디바이스는 다른 디바이스의 전화번호와 관계없이 자신의 전화번호로 키식별정보를 나누면 나머지인 R(암호화키)를 획득할 수 있다.

[193] 또한, 복수의 디바이스 중 도 12(f)의 데이터 세트를 수신한 수신 디바이스는 MAC을 이용하여, 획득한 암호화키가 올바른 암호화키인지를 확인할 수 있다. 예를 들어, 데이터 세트는 난수, 키 식별정보, MAC을 포함할 수 있으며, 수신 디바이스는 키식별정보를 이용하여 암호화키 R을 획득하고 R을 키로 하여 난수 값을 키 해싱(keyed hash)한 값이 MAC과 동일한지 확인함으로써, 획득한 암호화키가 올바른 암호화키인지를 확인할 수 있다.

[194] 일부 실시예에 따르면, MAC은 데이터 세트에 포함된 기타정보에 포함될 수 있다.

[195] 도 13은 일부 실시예에 따른 제2 디바이스가 제1 디바이스를 포함하는 복수의 디바이스로부터 키식별정보를 수신하고 데이터를 송신한 제1 디바이스의 키를

식별하기 위한 매칭과정을 설명하기 위한 플로우를 도시한다.

[196] 일부 실시예에 따르면. 매칭과정이란 제 2 디바이스가 수신한 값과 제 2 디바이스(또는 서버)에 저장된 복수의 값을 비교하여 일치하는 동일한 값을 찾는 과정을 의미할 수 있다.

[197] 단계 1301에서, 제2 디바이스는 제1 디바이스를 포함하는 복수의 디바이스와 키를 교환한다. 일부 실시예에 따르면, 도 13의 키라 함은, 공개키, 비공개키 등을 포함할 수 있으며, 상기 예시에 제한되지 않는다.

[198] 단계 1303에서, 제2 디바이스는 복수의 디바이스 각각과 교환한 키를 이용하여 암호화키를 각각 생성하고, 복수의 디바이스 각각에 대한 복수의 매칭키를 생성한다. 일부 실시예에 따르면, 매칭키 또한 키를 식별하기 위한 키식별정보일 수 있다. 또한 제 2 디바이스는 복수의 디바이스 각각과 교환한 키, 암호화키 및 매칭키 중 적어도 하나를 저장할 수 있다.

[199] 단계 1305에서, 제2 디바이스는 암호화된 데이터 및 키식별정보를 수신한다. 일부 실시예에 따르면, 제 2 디바이스는 암호화된 데이터 및 키식별정보를 포함하는 데이터 세트를 수신할 수 있다.

[200] 단계 1307에서, 제2 디바이스는 수신한 키식별정보를 미리 생성한 복수의 매칭키와 비교한다. 일부 실시예에 따르면, 제 2 디바이스는 저장된 매칭키와 수신된 키식별정보를 비교할 수 있다.

[201] 단계 1309에서, 제2 디바이스는 암호화된 데이터를 송신한 디바이스를 식별한다. 즉, 제 2 디바이스는 단계 1307의 비교 결과에 기초하여 송신 디바이스를 식별할 수 있다.

[202] 단계 1311에서, 제2 디바이스는 데이터를 송신한 디바이스의 암호화키를 도출해낸다.

[203] 단계 1313에서, 제2 디바이스는 암호화키를 이용하여 암호화된 데이터를 복호화할 수 있다.

[204] 도 14는 일부 실시예에 따른 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 제2 디바이스로 송신하는 제1 디바이스를 도시하는 블록도이다.

[205] 일부 실시예에 따르면, 제1 디바이스(1400)는 제어부(1401) 및 송수신부(1402)를 포함한다.

[206] 일부 실시예에 따르면, 제어부(1401)은 암호화키를 생성하고, 생성된 암호화키를 이용하여 키식별정보를 생성하고 데이터를 암호화한다.

[207] 일부 실시예에 따르면, 송수신부(1402)는 암호화된 데이터 및 키식별정보를 포함하는 데이터 세트를 제2 디바이스로 송신한다. 여기에서 키식별정보는 수신 디바이스만이 식별 할 수 있는 송신 디바이스의 정보를 암호화된 형태로 포함할 수 있다. 제어부(1410)는 암호화키뿐만 아니라, 제 2 디바이스의 공개키, 식별넘버, 제 2 디바이스의 비공개키 중 적어도 하나를 이용하여 키식별정보를 생성할 수 있다. 키식별정보를 생성하는 방법은 도 1내지 도 13에서 설명한 바와 같으므로, 자세한 설명은 생략한다.

[208] 도 15는 본발명의 일 실시예에 따른, 송수신 디바이스의 식별을 방지하는 암호화된 데이터 세트를 수신하는 제2 디바이스를 도시하는 블록도이다.

[209] 일부 실시예에 따르면, 제2 디바이스(1500)는 제어부(1510)와 송수신부(1520)을 포함한다.

[210] 일부 실시예에 따르면, 송수신부(1520)는 제1 디바이스로부터 암호화된 데이터 및 키식별정보를 포함하는 데이터 세트를 수신한다. 키식별정보는 수신 디바이스가 식별 할 수 있는 송신 디바이스의 정보를 암호화된 형태로 포함할 수 있다.

[211] 일부 실시예에 따르면, 제어부(1510)는 키식별정보를 이용하여 암호화키를 획득하고, 암호화키를 이용하여 암호화된 데이터를 복호화할 수 있다. 예를 들어, 제어부(1510)는 송수신부(1520)에서 수신한 데이터 세트 내에 포함된 키식별정보에 기초하여 송신 디바이스를 식별하고, 식별 결과에 기초하여 암호화키를 획득 또는 선택할 수 있다. 제어부(1510)는 암호화키를 이용하여 암호화된 데이터를 복호화할 수 있다. 암호화키를 획득하는 제어부(1510)의 동작은 앞선 도 1 내지 도 10에서 설명한 바와 대응된다.

[212] 도 16은 일부 실시예에 따른 디바이스를 설명하기 위한 세부 블록도이다.

[213] 본 발명의 일 실시예에 따르면, 제2 디바이스는 제1 디바이스를 포함하는 적어도 하나의 디바이스들과 적어도 하나의 비공개키를 공유하는 송수신부, 및 제1 디바이스로부터 암호화된 데이터를 수신하고, 암호화된 데이터를 수신하는 동안 암호화된 데이터를 송신한 제1 디바이스를 식별하고, 식별된 제1 디바이스의 식별정보를 암호화된 데이터에 부가하거나 저장하고, 제1 디바이스의 식별정보를 이용하여 제1 디바이스와 공유한 비공개키를 식별하고, 비공개키를 이용하여 암호화키를 생성하고, 암호화키를 이용하여 암호화된 데이터를 복호화하는 제어부를 포함할 수 있다.

[214] 또한, 본 발명의 일 실시예에 따르면, 수신 디바이스가 데이터를 수신하는 중에 송신 디바이스를 식별할 수 있는 소정의 방법에 의하여 송신 디바이스를 식별하는 식별정보를 생성하고, 송신 디바이스의 식별정보를 이용하여 암호화된 데이터에 대한 암호화키를 획득할 수 있다. 키식별정보는 제 2 디바이스와 교환한 난수, 공개키, 비공개키, 식별넘버, 사용하는 어플리케이션 중 적어도 하나의 정보에 기초하여 생성될 수 있으며, 제어부(1670)가 키식별정보를 생성하는 방법은 앞서 설명한 바와 대응되므로 자세한 설명은 생략한다.

[215] 일부 실시예에 따르면, 제어부는 RAM(1671), CPU(1673), ROM(1672), GPU(1674) 및 BUS(1675) 중 적어도 하나를 포함할 수 있으며, 제어부에 포함된 RAM(1671) 또는 ROM(1672)는 메모리(1620)과 동일 또는 별도의 저장부를 의미할 수 있다.

[216] 본 발명의 일 실시예에 따르면 제 1 디바이스는 핸드폰, 스마트폰, PMP, 태블릿, MP3 플레이어, 네비게이션과 같은 모바일 디바이스 또는 퍼스널 컴퓨터, 랩탑

컴퓨터, TV, 모니터, 냉장고 등 홈 디바이스일 수 있으며, 상기 예시에 제한되지 않는다.

[217] 본 발명의 일 실시예에 따르면, 사용자 입력부(1645)는 사용자로부터 입력을 수신을 수신하며, 예를 들어, 키보드, 터치패드, 터치스크린, 마우스, 트랙볼, 전자펜, 등을 포함할 수 있으며, 상기 예시에 제한되지 않는다. 일부 실시예에 따르면, 사용자 입력부(1645)는 키(1646), 터치패널(1647) 및 펜 인식 패널(1648) 중 적어도 하나를 포함할 수 있따.

[218] 본 발명의 일 실시예에 따르면 움직임 감지부(1665)는 GPS, 가속도 센서, 근접도 센서, 압력 센서, 조도 센서 등과 같은 다양한 센서를 포함할 수 있다. 뿐만 아니라 움직임 감지부(1665)는 서버와 같은 외부 디바이스에서 수신하는 정보에 기초하여 제 1 디바이스의 상태 및 제 1 디바이스에서 발생하는 이벤트를 감지할 수 있다.

[219] 본 발명의 일 실시예에 따르면 송수신부(1630)은 와이파이 칩(1631), 블루투스 칩(1632), 무선통신 칩(1633), NFC 칩(1634)를 포함할 수 있다. 송수신부(1630)은 제어부(1670)의 제어에 따라 다른 디바이스와 통신을 수행하는 구성부를 의미할 수 있다.

[220] 본 발명의 일 실시예에 따르면 메모리(1620)는 램(RAM), 플래시 메모리(Flash Memory), 하드 디스크, SSD와 같이 디바이스 내에 내장된 주 기억디바이스 또는 보조 기억디바이스로써 역할을 수행하는 모든 종류의 메모리를 포함할 수 있다.

[221] 또한 일부 실시예에 따르면, 제 1 디바이스(1600)는 GPS칩(1625), 오디오 프로세서(1640), 비디오 프로세서(1630), 마이크부(1650), 촬상부(1655), 스피커(1660) 및 표시 패널(1611)을 포함하는 디스플레이부(161)을 포함할 수 있다.

[222] 또한 제 1 디바이스(1600)는 도 14의 제 1 디바이스(1400)과 동일한 디바이스일 수 있다. 또한 도 16에 도시된 구성 요소가 모두 제 1 디바이스(1600)의 필수 구성 요소인 것은 아니다. 도 16에 도시된 구성 요소보다 많은 구성 요소에 의해 제 1 디바이스(1600)가 구현될 수도 있고, 도 16에 도시된 구성 요소보다 적은 구성 요소에 의해 제 1 디바이스(1600)가 구현될 수도 있다. 또한 일부 실시예에 따르면, 앞서 설명한 제 2 디바이스(1500) 또한 제 1 디바이스(1600)와 동일한 구성을 포함할 수 있다.

[223] 본 발명에 따른 디바이스는 프로세서, 프로그램 데이터를 저장하고 실행하는 메모리, 디스크 드라이브와 같은 영구 저장부(permanent storage), 외부 디바이스와 통신하는 통신 포트, 터치 패널, 키(key), 버튼 등과 같은 사용자 인터페이스 디바이스 등을 포함할 수 있다. 소프트웨어 모듈 또는 알고리즘으로 구현되는 방법들은 상기 프로세서상에서 실행 가능한 컴퓨터가 읽을 수 있는 코드들 또는 프로그램 명령들로서 컴퓨터가 읽을 수 있는 기록 매체 상에 저장될 수 있다. 여기서 컴퓨터가 읽을 수 있는 기록 매체로 마그네틱 저장 매체(예컨대, ROM(read-only memory), RAM(random-access memory), 플로피 디스크, 하드

디스크 등) 및 광학적 판독 매체(예컨대, 시디롬(CD-ROM), 디브이디(DVD: Digital Versatile Disc)) 등이 있다. 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템들에 분산되어, 분산 방식으로 컴퓨터가 판독 가능한 코드가 저장되고 실행될 수 있다. 매체는 컴퓨터에 의해 판독가능하며, 메모리에 저장되고, 프로세서에서 실행될 수 있다.

[224] 도 17은 일부 실시예에 따른 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 송수신하는 시스템을 도시하는 개념도이다.

[225] 일부 실시예에 따른 시스템은 암호화된 데이터를 송신하는 제1 디바이스 및 암호화된 데이터를 수신하는 제2 디바이스를 포함할 수 있다.

[226] 제1 디바이스는 암호화키를 생성하고, 생성된 암호화키를 이용하여 데이터를 암호화하며, 암호화된 데이터 및 키식별정보를 포함하는 데이터 세트를 제2 디바이스로 전송할 수 있다.

[227] 또한, 제2 디바이스는 데이터 세트를 수신하고, 수신된 데이터 세트의 키식별정보를 이용하여 암호화키를 획득하고, 획득된 암호화키를 이용하여 암호화된 데이터를 복호화할 수 있다.

[228] 또한 일부 실시예에 따르면, 제 1 디바이스는 제 2 디바이스를 포함하는 복수의 디바이스 그룹(제 2 디바이스 내지 제 n 디바이스)에게 데이터 세트를 송신할 수도 있다. 이는 앞서 설명한 바와 대응되므로, 자세한 설명은 생략한다.

[229] 도 18은 일부 실시예에 따른 따른 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 송신하는 방법을 도시하는 흐름도이다.

[230] 단계 1810에서, 제1 디바이스는 제2 디바이스와 키를 공유한다. 일부 실시예에 따르면, 공유되는 키는 공개키 또는 비공개키를 포함할 수 있다. 또한 일부 실시예에 따르면, 제 2 디바이스는 제 1 디바이스와 공유키, 난수 등을 교환할 수도 있으며, 이는 앞서 설명한 바와 대응되므로 자세한 설명은 생략한다.

[231] 단계 1820에서, 제1 디바이스는 데이터를 암호화하기 위한 암호화키를 생성한다. 암호화키는 단계 1810에서 공유된 키에 기초하여 생성될 수 있으나, 공유되는 키와 무관하게 생성될 수도 있다. 또한, 일부 실시예에 따르면, 암호화키는 제1 디바이스와 제2 디바이스가 키를 교환하는 과정에서 생성될 수도 있다.

[232] 또한 일부 실시예에 따르면, 암호화키는 제1 디바이스에 의해 생성되지 않을 수도 있다. 예를 들어, 제2 디바이스에 의해 생성된 암호화키가 키의 공유 과정에서 제1 디바이스에게 전달될 수도 있다.

[233] 단계 1830에서, 제1 디바이스는 생성된 암호화키를 이용하여 데이터를 암호화하고, 제2 디바이스와 공유한 키를 이용하여 암호화키를 암호화한다. 예를 들어, 제2 디바이스와 공유한 키가 공개키인 경우, 제2 디바이스의 공개키를 이용하여 암호화키를 암호화할 수 있다. 이때, 제2 디바이스는 암호화된 암호화키를 자신의 비밀키로 복호화할 수 있다.

[234] 단계 1840에서, 제1 디바이스는 암호화된 데이터, 암호화된 암호화키 및 메시지

인증 코드(Message Authentication Code)를 포함하는 데이터 세트를 제2 디바이스로 송신한다. 메시지 인증 코드는 제2 디바이스에서 복호화한 암호화키가 제 1 디바이스가 송신한 암호화키와 동일한지 여부를 확인하기 위해 사용될 수 있다.

[235] 도 19은 본 발명의 다른 실시예에 따른 송수신 디바이스의 식별을 방지하는 암호화된 데이터를 수신하는 방법을 도시하는 흐름도이다.

[236] 단계 1910에서, 제2 디바이스는 제1 디바이스와 키를 공유한다. 일부 실시예에 따르면, 공유되는 키는 공개키 또는 비공개키를 포함할 수 있다. 또한 일부 실시예에 따르면, 제 2 디바이스는 제 1 디바이스와 공유키, 난수 등을 교환할 수도 있으며, 이는 앞서 설명한 바와 대응되므로 자세한 설명은 생략한다.

[237] 단계 1920에서, 제2 디바이스는 암호화된 데이터, 적어도 하나의 암호화된 암호화키 및 메시지 인증 코드(Message Authentication Code)를 포함하는 데이터 세트를 제1 디바이스로부터 수신한다. 암호화된 데이터를 수신하는 디바이스가 복수인 경우, 제 2 디바이스가 수신한 데이터 세트 내에는 복수의 암호화된 암호화키가 포함될 수 있다.

[238] 단계 1930에서, 제2 디바이스는 적어도 하나의 암호화된 암호화키를 이용하여 적어도 하나의 암호화키를 획득한다. 예를 들면, 제 2 디바이스는 수신된 데이터 세트 내의 암호화된 암호화키를 키식별정보에 기초하여 선택된 키(예를 들면, 단계 1910에서 공유된 공개키, 비공개키, 공유키, 난수, 식별넘버 중 적어도 하나)를 이용하여 복호화할 수 있다.

[239] 일부 실시예에 따르면, 암호화된 데이터를 수신하는 디바이스가 복수인 경우, 제2 디바이스는 복수의 암호화된 암호화키를 이용하여 복수의 암호화키를 획득할 수 있다.

[240] 단계 1940에서, 제2 디바이스는 획득한 복수의 암호화키 중에서 올바른 암호화키를 메시지 인증 코드를 이용하여 판단한다. 예를 들어, 제2 디바이스는 획득한 복수의 암호화키 각각을 이용하여 메시지 인증 코드를 생성하고 생성된 메시지 인증 코드와 수신된 데이터 세트 내에 포함된 메시지 인증 코드와 비교할 수 있다. 제 2 디바이스는 수신된 데이터 세트 내에 포함된 메시지 인증 코드와 일치하는 생성된 메시지 인증 코드와 대응하는암호화 키를 선택할 수 있다.

[241] 단계 1950에서, 제2 디바이스는 단계 1940에서 선택한 암호화키를 이용하여 암호화된 데이터를 복호화한다.

[242] 도 20 및 도 21은 일부 실시예에 따른 키 공유 방법을 도시하는 시스템 도면이다.

[243] 도 20을 참조하면, 일부 실시예에 따르면, 제 1 디바이스(101)와 제 2 디바이스(102)는 첫번째 통신을 수행할 수 있다. 첫번째 통신을 위해 제 1 디바이스(101)와 제 2 디바이스(102)는 각각 공개키 및 개인키를 생성하고, 생성한 공개키를 공유할 수 있다. 제 1 디바이스(101)와 제 2 디바이스(102)는 공유한 공개키 및 생성한 개인키에 기초하여 송수신되는 데이터를

암호화하는데 사용되는 암호화 키를 생성할 수 있다.

[244] 일부 실시예에 따르면, 제 1 디바이스(101)와 제 2 디바이스(102)간의 첫번째 통신 시에는 암호화 키를 생성하기 위해 인증 과정을 수행할 수 있다. 예를 들면, 제 1 디바이스(101) 및 제 2 디바이스(102)는 SAS(Short Authentication String)을 생성 및 확인함으로써, 상호간을(즉, 제 1 디바이스가 제 2 디바이스를, 제 2 디바이스가 제 1 디바이스를) 식별하고, 암호화 키를 생성할 수 있다.

[245] 일부 실시예에 다르면, 제 1 디바이스(101)와 제 2 디바이스(102)는 두번째 통신을 수행할 수 있다. 즉, 제 1 디바이스(101)와 제 2 디바이스(102)는 첫번째 통신 이후, 두번째 통신을 수행할 수 있다. 일부 실시예에 따르면, 제 1 디바이스(101)와 제 2 디바이스(102)는 두번째 통신 수행시에는 SAS를 생성 및 확인하지 않고, 첫번째 통신 시 사용하였던 공통의 키 정보에 기초하여 상호간을 식별하고, 암호화 키를 생성할 수 있다. SAS를 생성 및 확인 단계를 생략하는 경우, 사용자의 번거로움 없이 안전하게 키를 교환할 수 있다.

[246] 제 1 디바이스(101)와 제 2 디바이스(102)는 두번째 통신 시, 공통 키 정보에 기초하여 암호화 통신을 수행할 수 있다. 더 자세히는, 제 1 디바이스(101)와 제 2 디바이스(102)는 공통 키 정보에 기초하여 각각 암호화 키를 생성할 수 있다. 제 1 디바이스(101)와 제 2 디바이스(102)는 생성한 암호화 키를 비교함으로써, 암호화 키를 확인하고, 확인된 암호화 키에 기초하여 암호화 통신을 수행할 수 있다.

[247] 암호화 통신 이후, 제 1 디바이스(101)와 제 2 디바이스(102)는 생성한 공개키 및 개인키를 모두 삭제할 수 있으며, 다만 생성된 암호화 키에 관한 정보는 다음 통신을 대비하여 저장해놓을 수 있다. 생성된 암호화 키에 관한 정보는 제 1 디바이스(101)와 제 2 디바이스(102) 간의 세번째 통신에서의 공통 키 정보로 사용 될 수 있다.

[248] 다만, 도 21을 참조하면, 제 1 디바이스(101)와 제 2 디바이스(102)가 동일한 공통 키 정보를 저장하고, 동일한 공통 키 정보에 기초하여 암호화 된 통신을 수행하므로, 제 3 자(103)가 제 1 디바이스(101) 또는 제 2 디바이스(102) 중 하나를 해킹하는 경우에는, 제 3 자의 중간자 공격(MITM)이 가능할 수도 있다. 참고적으로, 본 개시에서 첫번째 통신 및 두번째 통신은 통신 순서의 선, 후를 구분하기 위함일 뿐, 최초의 통신을 의미하는 것은 아니다.

[249] 도 22는 일부 실시예에 따른 키 공유 방법을 도시하는 흐름도이다.

[250] 단계 2201에서, 제 1 디바이스는 제 2 디바이스에게 송신한 제 1 디바이스의 제 1 공개키 및 제 1 디바이스의 제 1 개인키 저장되어 있는지 판단할 수 있다.

[251] 일부 실시예에 따르면, 제 1 디바이스는 제 2 디바이스 또는 서버로부터 통신 시작 요청을 수신하고, 통신 내역에 기초하여 통신 시작 요청 수신 이전에 제 2 디바이스와 통신을 수행한 적이 있는지 여부를 판단할 수 있다. 또한 제 2 디바이스와 이전에 통신을 수행한 적이 있는 경우, 제 1 디바이스는 제 2 디바이스에게 송신한 제 1 디바이스의 제 1 공개키 및 제 1 디바이스의 제 1

공개키에 대응하는 제 1 디바이스의 제 1 개인키가 저장되어 있는지 판단할 수 있다.

[252] 일부 실시예에 따르면, 제 1 디바이스의 제 1 공개키 및 제 1 디바이스의 제 1 개인키는 통신 시작 요청 수신 이전에 수행되었던 통신(이전 통신)에서 사용된 키일 수 있다. 즉, 제 1 디바이스는 이전의 통신 종료시, 제 1 디바이스의 제 1 공개키 및 제 1 디바이스의 제 1 개인키를 저장할 수 있다.

[253] 만약 제 1 디바이스와 이전에 통신을 수행한 적이 없는 경우, 제 1 디바이스는 SAS 생성 및 추가적인 인증 절차를 수행할 수도 있다.

[254] 단계 2203에서, 제 1 디바이스는 판단 결과에 기초하여, 제 1 디바이스의 제 2 공개키 및 제 1 디바이스의 제 2 개인키를 생성할 수 있다.

[255] 단계 2205에서, 제 1 디바이스는 생성된 제 1 디바이스의 제 2 공개키를 제 1 디바이스의 제 1 개인키로 서명할 수 있다.

[256] 일부 실시예에 따르면, 서명이라함은 검증 절차를 통해 출처를 확인할 수 있도록 데이터를 처리하는 방식을 의미할 수 있다. 예를 들면, 제 1 디바이스가 공개키로 데이터를 암호화 하면, 제 2 디바이스가 공개키와 대응하는 개인키로 암호화된 데이터를 복호화하는 동작과 유사한 방식으로, 제 1 디바이스가 개인키로 데이터에 서명하면, 제 2 디바이스는 개인키와 대응되는 공개키로 해당 데이터를 송신한 디바이스를 식별할 수 있다. 물론 상기 예시에 제한되지 않으며, 본 개시의 서명은 출처를 표시하는 모든 방법을 포함할 수 있다.

[257] 단계 2207에서, 제 1 디바이스는 서명된 제 2 공개키를 제 2 디바이스로 송신할 수 있다. 일부 실시예에 따르면 제 1 디바이스는 서명된 제 2 공개키와 함께 서명되지 않은 제 2 공개키를 송신할 수도 있다. 제 2 디바이스는 서명된 제 2 공개키를 검증하고, 서명되지 않는 제 2 공개키와 비교할 수도 있다.

[258] 도 23은 일부 실시예에 따른 키 공유 및 암호화 키 생성 방법을 도시하는 흐름도이다.

[259] 단계 2301에서, 제 1 디바이스는 제 2 디바이스로부터 제 2 디바이스의 제 1 개인키로 서명된 제 2 공개키를 수신할 수 있다. 일부 실시예에 따르면, 제 2 디바이스의 제 1 공개키 및 제 2 디바이스의 제 1 개인키는 통신 시작 요청 수신 이전에 수행되었던 통신(이전 통신)에서 사용된 키일 수 있다.

[260] 단계 2303에서, 제 1 디바이스는 통신 내역에 기초하여 제 2 디바이스의 제 1 개인키와 대응되는 제 2 디바이스의 제 1 공개키를 획득할 수 있다. 일부 실시예에 따르면, 제 1 디바이스는 제 1 디바이스 내에 저장된 제 2 디바이스의 제 1 공개키를 획득할 수 있다. 즉, 제 1 디바이스는 이전의 통신 종료 시, 제 2 디바이스의 제 1 공개키를 저장할 수 있다.

[261] 단계 2305에서, 제 1 디바이스는 획득한 제 2 디바이스의 제 1 공개키로 서명된 제 2 공개키를 검증할 수 있다. 일부 실시예에 따르면, 제 1 디바이스는 서명된 제 2 공개키를 검증함으로써, 제 2 디바이스를 인증 또는 식별할 수 있다.

[262] 단계 2307에서, 제 1 디바이스는 검증 결과에 기초하여 암호화 통신 수행할 수

있다. 일부 실시예에 따르면, 제 1 디바이스는 검증 결과에 기초하여 암호화 키를 생성할 수 있다.

[263] 예를 들면, 검증 결과, 제 2 디바이스가 인증되는 경우에는, 제 1 디바이스는 제 1 디바이스의 제 2 개인키 및 제 2 디바이스의 제 2 공개키에 기초하여 암호화 키를 생성할 수 있다.

[264] 일부 실시예에 따르면, 암호화 키는 다양한 방식에 의해 생성될 수 있다, 예를 들면, 제 1 디바이스의 제 2 개인키 및 제 2 디바이스의 제 2 공개키를 연산함으로써, 소정의 값을 획득하고, 획득한 소정의 값을 키 유도 함수에 입력함으로써, 통신 암호화용 데이터를 획득할 수 있다. 제 1 디바이스는 통신 암호화용 데이터 중 일부를 암호화 키로 사용할 수 있고, 통신 암호화용 데이터 중 암호화 키로 사용하지 않는 나머지 일부의 데이터 MAC(Message Authentication Code) 또는 키 확인 데이터로 사용할 수 있다. 물론 상기 예시에 제한되지 않으며, 암호화 키는 다양한 파라미터 또는 다양한 방식에 의해 생성될 수 있다.

[265] 또한 일부 실시예에 따르면, 검증 결과, 제 2 디바이스가 인증되지 않는 경우에는, 제 1 디바이스는 SAS(Short Authentication String) 계산을 수행할 수 있다. 즉, 제 1 디바이스는 제 2 디바이스를 인증하기 위해 추가적인 프로세스를 수행할 수 있다.

[266] 예를 들면, 제 1 디바이스는 제 1 디바이스의 제 2 공개키, 제 2 디바이스의 제 2 공개키를 이용하여 해시 연산을 수행하고, 해시 연산 결과에 기초하여 소정의 단어로 변환하고, 변환된 단어를 사운드 데이터(예를 들면, 보이스 데이터) 로 변경하여 제 1 디바이스와 제 2 디바이스에게 제공할 수 있다.

[267] 제 1 디바이스와 제 2 디바이스는 제공된 사운드 데이터를 출력하고, 제 1 디바이스와 제 2 디바이스의 사용자는 제 1 디바이스와 제 2 디바이스에서 출력된 사운드 데이터에 기초하여 제 1 디바이스와 제 2 디바이스간의 인증을 위한 소정의 절차를 수행할 수 있다. 물론 제 1 디바이스가 생성하는 SAS는 꼭 사운드 데이터로 변환될 필요는 없으며, 텍스트 데이터인 경우, 제 1 디바이스와 제 2 디바이스는 디스플레이부를 통해 제공된 텍스트 데이터를 출력할 수도 있다. 즉, SAS를 통한 추가적인 인증 방법에는 제한이 없다.

[268] 또한 일부 실시예에 따르면, 현재 수행중인 통신이 종료되면, 제 1 디바이스는 제 1 디바이스의 제 1 공개키, 제 1 디바이스의 제 1 개인키 및 제 2 디바이스의 제 1 공개키를 삭제하고, 제 1 디바이스의 제 2 공개키, 제 1 디바이스의 제 2 개인키 및 제 2 디바이스의 제 2 공개키를 저장할 수 있다. 저장된 제 1 제 1 디바이스의 제 2 공개키, 제 1 디바이스의 제 2 개인키 및 제 2 디바이스의 제 2 공개키는 다음 통신 시 사용될 수 있다.

[269] 도 24는 일부 실시예에 따른 키 공유 방법을 도시하는 흐름도이다.

[270] 단계 2401에서, 제 1 디바이스는 이전 통신 수행시 제 2 디바이스에게 송신한 제 1 난수가 저장되어 있는지 판단할 수 있다. 일부 실시예에 따르면, 제 1 난수는

현재 통신의 시작 요청 이전에 제 1 디바이스와 제 2 디바이스 간에 수행되었던 통신에서 사용되었던 난수를 포함할 수 있다. 또한 제 1 난수는 제 1 디바이스가 생성하여 제 2 디바이스에게 송신한 난수를 포함할 수 있다.

[271] 단계 2403에서, 제 1 디바이스는 판단 결과에 기초하여, 제 1 디바이스의 제 2 공개키 및 제 1 디바이스의 제 2 개인키를 생성할 수 있다. 이는 도 22 내지 도 23에서 설명한 바와 대응된다.

[272] 단계 2405에서, 제 1 디바이스는 이전 통신 수행시 제 2 디바이스로부터 수신한 제 2 난수를 제 1 디바이스의 제 1 개인키로 서명 할 수 있다. 즉, 제 1 디바이스는 이전 통신 수행시 제 2 디바이스로부터 수신한 제 2 난수를 이전 통신 수행시 사용했던 제 1 디바이스의 제 1 개인키로 서명할 수 있다.

[273] 단계 2407에서, 제 1 디바이스는 서명된 제 2 난수를 제 2 디바이스로 송신 할 수 있다.

[274] 또한 일부 실시예에 따르면 제 1 디바이스는 서명된 제 2 난수와 함께, 제 1 디바이스의 제 2 공개키 및 제 1 디바이스의 제 2 공개키, 서명된 제 2 난수에 기초한 해시 값 중 적어도 하나를 제 2 디바이스에게 송신할 수 있다.

[275] 또한 일부 실시예에 따르면, 제 1 디바이스는 제 2 디바이스의 제 1 개인키로 서명된 제 1 난수를 수신할 수 있다. 제 1 디바이스는 제 2 디바이스의 제 1 개인키로 서명된 제 1 난수를 제 2 디바이스의 제 1 공개키로 검증할 수 있다. 즉, 제 1 디바이스와 제 2 디바이스는 이전 단계에서 사용된 개인키를 대신 난수를 사용함으로써 도 22 내지 도 23에서 수행한 키공유 방식을 수행할 수 있다.

[276] 일부 실시예에 따르면, 제 1 디바이스는 검증 결과에 기초하여 암호화된 통신을 수행할 수 있다. 이는 도 22 내지 도 23에서 설명한 바와 대응되므로, 자세한 설명은 생략한다.

[277] 또한 일부 실시예에 따르면, 제 1 디바이스와 제 2 디바이스는 현재 수행중인 통신의 종료 이전에 다음 통신 시 사용하기 위한 제 3 난수 및 제 4 난수를 각각 생성하고, 제 1 디바이스 및 제 2 디바이스와 교환 할 수 있다. 제 1 디바이스 및 제 2 디바이스는 교환된 난수를 이용하여 다음 통신 수행시 키 공유를 수행할 수 있다.

[278] 일부 실시예에 따르면, 제 1 디바이스는 제 2 디바이스로부터 수신된 제 4 난수를 제 2 개인키로 서명하여 저장할 수 있다. 또한 제 1 디바이스는 서명 이후, 제 1 디바이스의 제 2 개인키를 삭제할 수 있다. 즉, 제 1 디바이스는 개인키를 저장하지 않을 수 있다.

[279] 도 25 및 도 26은 일부 실시예에 따른 암호화 통신을 위한 제 1 디바이스와 제 2 디바이스 간의 키 공유 방법을 도시한다.

[280] 도 25를 참조하면, 단계 2501에서, 제 1 디바이스는 제 1 디바이스의 제 1 공개키, 제 1 디바이스의 제 1 개인키 및 제 2 디바이스의 제 1 공개키를 저장할 수 있다.

[281] 또한 일부 실시예에 따르면, 단계 2501의 이전 통신 단계라 함은 도 20에서

설명한 첫번째 통신에 서 수행되는 단계일 수 있다. 또한 일부 실시예에 따르면, 제 1 디바이스는 제 1 디바이스의 제 1 공개키, 제 1 디바이스의 제 1 개인키 및 제 2 디바이스의 제 1 공개키를 저장한 이후, 제 2 디바이스 또는 서버로부터 두번째 통신의 시작을 요청하는 통신 시작 요청을 수신할 수 있다.

[282] 단계 2503에서, 제 2 디바이스는 제 1 디바이스의 공개키, 제 2 디바이스의 제 1 개인키 및 제 1 디바이스의 제 1 공개키를 저장할 수 있다. 일부 실시예에 따르면, 단계 2503 또한 도 20에서 설명한 첫번째 통신 시 수행되는 단계일 수 있다. 또한 일부 실시예에 따르면, 제 2 디바이스는 제 1 디바이스의 공개키, 제 2 디바이스의 제 1 개인키 및 제 1 디바이스의 제 1 공개키를 저장한 이후, 제 1 디바이스 또는 서버에게 두번째 통신의 시작을 요청하는 통신 시작 요청을 송신할 수 있다.

[283] 단계 2505에서, 제 1 디바이스는 제 1 디바이스의 제 2 공개키 및 제 1 디바이스의 제 2 개인키를 생성할 수 있다.

[284] 단계 2507에서, 제 2 디바이스는, 제 2 디바이스의 제 2 공개키 및 제 2디바이스의 제 2 개인키를 생성할 수 있다.

[285] 단계 2509에서, 제 1 디바이스는 제 1 디바이스의 제 1 개인키로 제 1 디바이스의 제 2 공개키를 서명할 수 있다.

[286] 단계 2511에서, 제 2 디바이스는 제 2 디바이스의 제 1 개인키로 제 2 디바이스의 제 2 공개키를 서명할 수 있다. 단계 2505 내지 단계 2511은 앞선 도 22 내지 도 23에서 설명한 바와 대응되므로 자세한 설명은 생략한다.

[287] 단계 2513에서, 제 1 디바이스는 서명된 제 1 디바이스의 제 2 공개키 및 제 1 디바이스의 제 2 공개키를 제 2 디바이스에게 송신할 수 있다.

[288] 단계 2515에서, 제 2 디바이스는 서명된 제 2 디바이스의 제 2 공개키 및 제 2 디바이스의 제 2 공개키를 제 2 디바이스에게 송신할 수 있다.

[289] 단계 2517에서, 제 1 디바이스는 제 2 디바이스의 제 1 개인키로 서명된 제 2 디바이스의 제 2 공개키를 검증할 수 있다. 일부 실시예에 따르면, 개인키와 공개키는 대응되며, 공개키로 암호화한 데이터는 개인키로 복호화 할 수 있고, 개인키로 서명한 데이터는 공개키로 검증할 수 있다.

[290] 일부 실시예에 다르면 제 1 디바이스는 단계 2501에서 저장된 제 2 디바이스의 제 1 공개키를 이용하여 서명된 제 2 디바이스의 제 2 공개키를 검증할 수 있다. 또한 제 1 디바이스는 검증된 제 2 디바이스의 제 2 공개키를 수신된 제 2 디바이스의 제 2 공개키와 비교할 수도 있다.

[291] 단계 2519에서, 제 2 디바이스는 제 1 디바이스의 제 1 공개키로 서명된 제 1 디바이스의 제 1 공개키를 검증할 수 있다. 일부 실시예에 다르면 제 2 디바이스는 단계 2503에서 저장된 제 1 디바이스의 제 1 공개키를 이용하여 서명된 제 1 디바이스의 제 2 공개키를 검증할 수 있다. 또한 제 2 디바이스는 검증된 제 1 디바이스의 제 2 공개키를 수신된 제 1 디바이스의 제 2 공개키와 비교할 수도 있다.

[292] 단계 2521에서, 제 1 디바이스와 제 2 디바이스는 검증 결과에 기초하여 암호화 키를 생성 및 교환할 수 있다. 암호화 키 생성 및 교환은 앞서 설명한 바와 대응되므로 자세한 설명은 생략한다.

[293] 도 26을 참조하면 단계 2601에서, 제 1 디바이스는 제 2 디바이스에게 송신한 제 1 난수, 제 1 디바이스의 제 1 공개키로 서명된 제 2 난수 및 제 2 디바이스의 제 1 공개키를 저장할 수 있다. 일부 실시예에 따르면, 제 2 난수는 제 1 디바이스가 제 2 디바이스로부터 이전의 통신 단계에서 수신한 난수를 포함할 수 있다.

[294] 단계 2601의 이전 통신 단계라 함은 도 20에서 설명한 첫번째 통신에 서 수행되는 단계일 수 있다. 또한 일부 실시예에 따르면, 제 1 디바이스는 제 2 디바이스에게 송신한 제 1 난수, 제 1 디바이스의 제 1 공개키로 서명된 제 2 난수 및 제 2 디바이스의 제 1 공개키를 저장한 이 후, 제 2 디바이스 또는 서버로부터 두번째 통신의 시작을 요청하는 통신 시작 요청을 수신할 수 있다.

[295] 단계 2603에서, 제 2 디바이스는 제 2 디바이스의 제 1 공개키로 서명된 제 1 난수, 제 1 디바이스에게 송신한 제 2 난수 및 제 1 디바이스의 제 1 공개키를 저장할 수 있다.

[296] 단계 2603의 이전 통신 단계라 함은 도 20에서 설명한 첫번째 통신에 서 수행되는 단계일 수 있다. 또한 일부 실시예에 따르면, 제 2 디바이스는 제 1 디바이스에게 송신한 제 2 난수, 제 2 디바이스의 제 1 공개키로 서명된 제 1 난수 및 제 1 디바이스의 제 1 공개키를 저장한 이 후, 제 1 디바이스 또는 서버에게 두번째 통신의 시작을 요청하는 통신 시작 요청을 송신할 수 있다.

[297] 단계 2605에서, 제 1 디바이스는 제 1 디바이스의 제 2 공개키 및 제 1 디바이스의 제 2 개인키를 생성할 수 있다.

[298] 단계 2607에서, 제 2 디바이스는, 제 2 디바이스의 제 2 공개키 및 제 2 디바이스의 제 2 개인키를 생성할 수 있다.

[299] 단계 2609에서, 제 1 디바이스는 서명된 제 2 난수, 제 1 디바이스의 제 2 공개키 및 서명된 제 2 난수와 제 1 디바이스의 제 2 공개키에 기초하여 생성된 해시 값을 제 2 디바이스에게 송신할 수 있다.

[300] 일부 실시예에 따르면, 제 1 디바이스가 송신한 해시 값은 제 2 디바이스가 제 1 디바이스를 검증하기 위해 사용될 수 있다. 추가적으로 제 1 디바이스는 제 1 디바이스의 핀 넘버를 추가적으로 고려함으로써 생성할 수도 있다.

[301] 단계 2611에서, 제 2 디바이스는 서명된 제 1 난수, 제 2 디바이스의 제 2 공개키 및 서명된 제 1 난수와 제 2 디바이스의 제 2 공개키에 기초하여 생성된 해시 값을 제 1 디바이스에게 송신할 수 있다.

[302] 일부 실시예에 따르면, 제 2 디바이스가 송신한 해시 값은 제 1 디바이스가 제 2 디바이스를 검증하기 위해 사용될 수 있다. 추가적으로 제 2 디바이스는 제 2 디바이스의 핀 넘버를 추가적으로 고려함으로써 생성할 수도 있다.

[303] 단계 2613에서, 제 1 디바이스는 제 2 디바이스의 제 1 공개키로 서명된 제 1 난수를 검증할 수 있다.

[304] 단계 2615에서, 제 2 디바이스는 제 1 디바이스의 제 1 공개키로 서명된 제 2 난수를 검증할 수 있다.

[305] 단계 2617에서, 제 1 디바이스와 제 2 디바이스는 검증 결과에 기초하여 암호화 키를 생성 및 교환할 수 있다. 단계 2613 내지 단계 2617은 앞서 설명한 내용과 대응되므로 자세한 설명은 생략한다.

[306] 도 27은 일부 실시예에 따른 SAS 생성 방법을 도시한다.

[307] 일부 실시예에 따르면, 제 1 디바이스는 제 1 디바이스의 공개키(2701) 및 제 2 디바이스의 공개키(2703)을 해시함수에 입력함으로써, 해시값(2705)을 생성할 수 있다. 일부 실시예에 따르면, 제 2 디바이스 또한 제 1 디바이스와 동일한 방식으로 해시 값을 생성할 수 있다.

[308] 일부 실시예에 따르면, 제 1 디바이스는 해시 값(2703)을 생성하고, 생성한 해시 값을 소정의 단어(2707)로 변환할 수 있다. 제 1 디바이스는 소정의 단어(2707)를 제 2 디바이스에게 송신할 수 있다.

[309] 일부 실시예에 따르면, 제 1 디바이스는 제 1 디바이스의 사용자에게, 제 2 디바이스는 제 2 디바이스의 사용자에게 소정의 단어(2707)를 출력하고, 출력된 소정의 단어(2707)에 기초하여 사용자 입력을 수신함으로서, 제 1 디바이스와 제 2 디바이스는 상호간의 인증 절차를 수행할 수 있다.

[310] 도 28은 일부 실시예에 따른 키 공유 디바이스의 블록도이다.

[311] 도 28에 도시된 바와 같이 일부 실시예에 따른 워터마크 데이터를 삽입하는 디바이스인 제 1 디바이스(101)는 제어부(2801), 통신부(2803) 및 제어부(2805)를 포함할 수 있다. 그러나 도 28에 도시된 구성 요소가 모두 제 1 디바이스(101)의 필수 구성 요소인 것은 아니다. 도 28에 도시된 구성 요소보다 많은 구성 요소에 의해 제 1 디바이스(101)가 구현될 수도 있고, 도 28에 도시된 구성 요소보다 적은 구성 요소에 의해 제 1 디바이스(101)가 구현될 수도 있다. 또한 일부 실시예에 따르면, 제 2 디바이스 또한 제 1 디바이스(101)와 동일한 구성을 포함할 수 있다.

[312] 일부 실시예에 따르면, 제어부(2801)는 통상적으로 제 1 디바이스(101)의 전반적인 동작을 제어한다. 예를 들어, 제어부(2801)는 제 1 디바이스(101)에 저장된 프로그램을 실행함으로써, 제 1 디바이스(101)가 포함하는 구성요소들을 전반적으로 제어할 수 있다. 또한 제어부(2801) 적어도 하나의 프로세서를 포함할 수 있다.

[313] 일부 실시예에 따르면, 제어부(2801)는 통신 내역에 기초하여 제 1 디바이스 내에 공개키, 개인키, 난수 등이 저장되어 있는지 판단할 수 있다. 즉, 제어부(2801)는 이전 통신 단계에서 사용된 후, 다음 통신 단계를 위해 저장된 공개키, 개인키, 난수 등이 저장되어 있는지 여부 및 현재 통신 중인 디바이스와의 이전 통신 내역이 존재하는지를 판단할 수 있다.

[314] 일부 실시예에 따르면, 제어부(2801)는 통신 내역에 기초하여, 제 2 디바이스에게 송신한 제 1 디바이스의 제 1 공개키 및 제 1 디바이스의 제 1 공개키에 대응하는 제 1 디바이스의 제 1 개인키가 저장되어 있는지 판단할 수

있다. 공개키, 개인키, 난수에 대한 설명은 앞서 설명한 바와 대응되므로, 자세한 설명은 생략한다.

[315] 또한 일부 실시예에 따르면, 제어부(2801)는 암호화부(2805)의 검증 결과에 따라 암호화 통신을 수행할지 여부를 결정할 수 있다. 일부 실시예에 따르면, 제어부(2801)는 암호화 키를 생성할지 또는 SAS 계산을 수행할 지 여부를 결정할 수 있다.

[316] 일부 실시예에 따르면, 통신부(2803)는 제 2 디바이스에게 공개키, 난수, 서명된 공개키 등을 송신할 수 있다. 또한 통신부(2803)는 생성된 암호화 키 교환을 위한 키 확인 데이터 또는 MAC(Message Authentication Code)를 송신할 수도 있다.

[317] 일부 실시예에 따르면, 통신부(2803)는 서명된 제 2 공개키를 제 2 디바이스로 송신할 수 있고, 제 2 디바이스로부터 제 2 디바이스의 제 1 개인키로 서명된 제 2 공개키를 수신할 수도 있다. 통신부(2803)가 송신 및 수신하는 공개키, 난수, 서명된 공개키 등에 대한 설명은 앞서 설명한 바와 대응되므로 자세한 설명은 생략한다.

[318] 또한 일부 실시예에 따르면, 통신부(2803)는 통신 시작 요청을 송신 및 수신할 수 있다. 앞서 설명한 바와 같이 공유, 교환이라 함은 수신 및 송신 동작을 모두 포함할 수 있다.

[319] 일부 실시예에 따르면, 암호화부(2805)는 공개키와 같은 소정의 데이터를 서명, 검증, 암호화 및 복호화 할 수 있다. 일부 실시예에 따르면, 암호화부(2805)는 제 1 디바이스의 제 2 공개키 및 제 1 디바이스의 제 2 개인키를 생성하고, 생성된 제 1 디바이스의 제 2 공개키를 제 1 디바이스의 제 1 개인키로 서명할 수 있다. 또한 암호화부(2805)는, 통신 내역에 기초하여, 제 2 디바이스의 제 1 개인키와 대응되는 제 2 디바이스의 제 1 공개키를 획득하고, 획득한 제 2 디바이스의 제 1 공개키로 서명된 제 2 공개키를 검증할 수 있다. 암호화부(2805)가 서명, 검증, 암호화 및 복호화 하는 동작은 앞서 설명한 바와 대응되므로, 자세한 설명은 생략한다.

[320] 일부 실시예에 따르면, 암호화부(2805)는, 현재 수행중인 통신이 종료되면, 이전 통신의 수행 후 저장되었던 데이터를 삭제할 수 있다. 예를 들면, 암호화부(2805)는 이전 통신에서 사용되었던, 제 1 디바이스의 제 1 개인키, 제 1 디바이스의 제 1 공개키 및 제 2 디바이스의 제 1 공개키를 삭제할 수 있다. 이는 앞서 설명한 내용과 대응된다.

[321] 또한 일부 실시예에 따르면, 검증 결과에 따른 제어부(2801)의 제어에 따라 암호화부(2805)는 암호화 키를 생성하거나, SAS 계산을 수행할 수 있다. 암호화 키의 생성 및 SAS 계산은 앞서 설명한 동작과 대응된다.

[322] 도 28은 일부 실시예에 따른 키 공유 디바이스의 세부 블록도이다.

[323] 도 29에 도시된 바와 같이 일부 실시예에 따른 키 공유 디바이스인 제 1 디바이스(101)는, 제어부(2801), 통신부(2803), 암호화부(2805) 외에도 사용자 입력부(2900), 출력부(2910), 센서부(2920), A/V 입력부(2950) 및 저장부(2960)을

더 포함할 수도 있다.

[324] 통신부(2803)는, 제 1 디바이스(101)와 제 2 디바이스(102) 또는 외부 서버 간의 통신을 하게 하는 하나 이상의 구성요소를 포함할 수 있다. 예를 들어, 통신부(2803)는, 근거리 통신부(2941), 이동통신부(2943), 방송 수신부(2945)를 포함할 수 있다.

[325] 일부 실시예에 따르면 근거리 통신부(2941)는, 블루투스 통신부, BLE(Bluetooth Low Energy) 통신부, 근거리 자기장 통신부(Near Field Communication), WLAN(와이파이) 통신부, 지그비(Zigbee) 통신부, 적외선(IrDA, infrared Data Association) 통신부, WFD(Wi-Fi Direct) 통신부, UWB(ultra wideband) 통신부, Ant+ 통신부 등을 포함할 수 있으나, 이에 한정되는 것은 아니다.

[326] 일부 실시예에 따르면, Ant+ 통신부는 블루투스와 같이 소정의 규격을 가진 ANT라는 무선 네트워크 프로토콜을 이용한 무선 통신을 수행하는 통신부로써, 저전력 기술 기반의 프로토콜이다. ANT 프로토콜은 신체 정보 등의 다양한 데이터를 프로파일로 저장하여 다른 디바이스에 전송할 수 있는 프로토콜로써, 당업자에게 자명하므로, 자세한 설명은 생략한다.이동 통신부(2943)는, 이동 통신망 상에서 기지국, 외부의 단말, 서버 중 적어도 하나와 무선 신호를 송수신한다. 여기에서, 무선 신호는, 음성 호 신호, 화상 통화 호 신호 또는 문자/멀티미디어 메시지 송수신에 따른 다양한 형태의 데이터를 포함할 수 있다.

[327] 방송 수신부(2945)는, 방송 채널을 통하여 외부로부터 방송 신호 및/또는 방송 관련된 정보를 수신한다. 방송 채널은 위성 채널, 지상파 채널을 포함할 수 있다. 구현 예에 따라서 제 1 디바이스(101)는 방송 수신부(2945)를 포함하지 않을 수도 있다.

[328] 저장부(메모리)(2960)는, 제어부(2801)의 처리 및 제어를 위한 프로그램을 저장할 수 있고, 제 1 디바이스(101)로 입력되거나 제 1디바이스(101)로부터 출력되는 데이터를 저장할 수도 있다. 또한 일부 실시예에 따르면, 저장부(2960)는 공개키, 개인키, 난수 등을 저장할 수 있다.

[329] 저장부(메모리)(2960)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(RAM, Random Access Memory) SRAM(Static Random Access Memory), 롬(ROM, Read-Only Memory), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다.

[330] 저장부(메모리)(2960)에 저장된 프로그램들은 그 기능에 따라 복수 개의 모듈들로 분류할 수 있는데, 예를 들어, UI 모듈(2961), 터치 스크린 모듈(2962), 알림 모듈(2963) 등으로 분류될 수 있다.

[331] UI 모듈(2961)은, 제 1 디바이스(101)와 연동되는 특화된 UI, GUI 등을 제공할 수 있다. 예를 들어, UI 모듈(2961)는 제 1 디바이스(101)가 제 2 디바이스(102)와

통신을 수행하기 위한 절차를 진행하고 있는지 확인할 수 있는 UI 또는 GUI를 제공할 수 있다.

[332] 터치 스크린 모듈(2962)은 사용자의 터치 스크린 상의 터치 제스처를 감지하고, 터치 제스처에 관한 정보를 제어부(2801)로 전달할 수 있다. 일부 실시예에 따른 터치 스크린 모듈(2962)은 터치 코드를 인식하고 분석할 수 있다. 터치 스크린 모듈(2962)은 컨트롤러를 포함하는 별도의 하드웨어로 구성될 수도 있다.

[333] 터치스크린의 터치 또는 근접 터치를 감지하기 위해 터치스크린의 내부 또는 근처에 다양한 센서가 구비될 수 있다. 터치스크린의 터치를 감지하기 위한 센서의 일례로 촉각 센서가 있다. 촉각 센서는 사람이 느끼는 정도로 또는 그 이상으로 특정 물체의 접촉을 감지하는 센서를 말한다. 촉각 센서는 접촉면의 거칠기, 접촉 물체의 단단함, 접촉 지점의 온도 등의 다양한 정보를 감지할 수 있다.

[334] 또한, 터치스크린의 터치를 감지하기 위한 센서의 일례로 근접 센서가 있다.

[335] 근접 센서는 소정의 검출면에 접근하는 물체, 혹은 근방에 존재하는 물체의 유무를 전자계의 힘 또는 적외선을 이용하여 기계적 접촉이 없이 검출하는 센서를 말한다. 근접 센서의 예로는 투과형 광전 센서, 직접 반사형 광전 센서, 미러 반사형 광전 센서, 고주파 발진형 근접 센서, 정전용량형 근접 센서, 자기형 근접 센서, 적외선 근접 센서 등이 있다. 일부 실시예에 따르면, 제 1 디바이스(101)는 근접 센서를 통해 제 2 디바이스와의 거리 정보를 획득할 수도 있다.

[336] 사용자의 터치 제스처에는 탭, 터치&홀드, 더블 탭, 드래그, 패닝, 플릭, 드래그 앤드 드롭, 스와이프 등이 있을 수 있다.

[337] 알림 모듈(2963)은 제 1 디바이스(101)의 이벤트 발생을 알리기 위한 신호를 발생할 수 있다. 제 1 디바이스(101)에서 발생되는 이벤트의 예로는 호 신호 수신, 메시지 수신, 키 신호 입력, 일정 알림 등이 있다. 알림 모듈(2963)은 디스플레이부(2911)를 통해 비디오 신호 형태로 알림 신호를 출력할 수도 있고, 음향 출력부(2912)를 통해 오디오 신호 형태로 알림 신호를 출력할 수도 있고, 진동 모터(2913)를 통해 진동 신호 형태로 알림 신호를 출력할 수도 있다. 저장부(메모리)(2960)가 수행하는 동작은 앞서 설명한 내용과 대응되므로 자세한 설명은 생략한다.

[338] 제어부(2801)는 제 1 디바이스(101)의 전반적인 동작을 제어한다. 이는 앞서 설명한 바와 대응되므로, 자세한 설명은 생략한다.

[339] 사용자 입력 수신부(2900)는, 사용자가 제 1 디바이스(101)를 제어하기 위한 데이터를 입력하는 수단을 의미한다. 예를 들어, 사용자 입력부(2900)에는 키 패드(key pad), 돔 스위치 (dome switch), 터치 패드(접촉식 정전 용량 방식, 압력식 저항막 방식, 적외선 감지 방식, 표면 초음파 전도 방식, 적분식 장력 측정 방식, 피에조 효과 방식 등), 조그 휠, 조그 스위치 등이 있을 수 있으나 이에 한정되는 것은 아니다.

[340] 출력부(2910)는, 오디오 신호 또는 비디오 신호 또는 진동 신호를 출력할 수 있으며, 출력부(2910)는 디스플레이부(2911), 음향 출력부(2912), 및 진동 모터(2913)를 포함할 수 있다.

[341] 디스플레이부(2911)는 제 1 디바이스(101)에서 처리되는 정보를 표시 출력한다.

[342] 한편, 디스플레이부(2911)와 터치패드가 레이어 구조를 이루어 터치 스크린으로 구성되는 경우, 디스플레이부(2911)는 출력 장치 이외에 입력 장치로도 사용될 수 있다. 디스플레이부(2911)는 액정 디스플레이(liquid crystal display), 박막 트랜지스터 액정 디스플레이(thin film transistor-liquid crystal display), 유기 발광 다이오드(organic light-emitting diode), 플렉시블 디스플레이(flexible display), 3차원 디스플레이(3D display), 전기영동 디스플레이(electrophoretic display) 중에서 적어도 하나를 포함할 수 있다. 그리고 제 1 디바이스(101)의 구현 형태에 따라 제 1 디바이스(101)는 디스플레이부(2911)를 2개 이상 포함할 수도 있다. 이때, 2개 이상의 디스플레이부(2911)는 힌지(hinge)를 이용하여 마주보게 배치될 수 있다.

[343] 음향 출력부(2912)는 통신부(2100)로부터 수신되거나 저장부(메모리)(2940)에 저장된 오디오 데이터를 출력한다. 또한, 음향 출력부(2912)는 디바이스(101)에서 수행되는 기능(예를 들어, 호신호 수신음, 메시지 수신음, 알림음)과 관련된 음향 신호를 출력한다. 이러한 음향 출력부(6222)에는 스피커(speaker), 버저(Buzzer) 등이 포함될 수 있다.

[344] 진동 모터(2913)는 진동 신호를 출력할 수 있다. 예를 들어, 진동 모터(6229)는 오디오 데이터 또는 비디오 데이터(예컨대, 호신호 수신음, 메시지 수신음 등)의 출력에 대응하는 진동 신호를 출력할 수 있다. 또한, 진동 모터(2913)는 터치스크린에 터치가 입력되는 경우 진동 신호를 출력할 수도 있다.

[345] 센서부(2920)는, 제 1 디바이스(101)의 상태 또는 제 1 디바이스(101) 주변의 상태를 감지하고, 감지된 정보를 제어부(2801)로 전달할 수 있다.

[346] 센서부(2920)는, 지자기 센서(Magnetic sensor)(2921), 가속도 센서(Acceleration sensor)(2922), 온/습도 센서(2923), 적외선 센서(2924), 자이로스코프 센서(2925), 위치 센서(예컨대, GPS)(2926), 기압 센서(2927), 근접 센서(2928), 및 RGB 센서(광센서)(illuminance sensor)(2929) 중 적어도 하나를 포함할 수 있으나, 이에 한정되는 것은 아니다. 각 센서들의 기능은 그 명칭으로부터 당업자가 직관적으로 추론할 수 있으므로, 구체적인 설명은 생략하기로 한다.

[347] 신호 획득부(A/V(Audio/Video)입력부)(2930)는 오디오 신호 또는 비디오 신호 입력을 위한 것으로, 이에는 카메라(2951)와 음향 입력부(2952) 등이 포함될 수 있다. 카메라(2951)은 화상 통화모드 또는 촬영 모드에서 이미지 센서를 통해 정지영상 또는 동영상 등의 화상 프레임을 얻을 수 있다. 이미지 센서를 통해 캡쳐된 이미지는 제어부(2801) 또는 별도의 이미지 처리부(미도시)를 통해 처리될 수 있다.

[348] 카메라(2951)에서 처리된 화상 프레임은 저장부(메모리)(2960)에 저장되거나 통신부(2803)를 통하여 외부로 송신될 수 있다. 카메라(2951)는 단말기의 구성 태양에 따라 2개 이상이 구비될 수도 있다.

[349] 음향 입력부(2952)는, 외부의 음향 신호를 입력 받아 전기적인 음성 데이터로 처리한다. 일부 실시예에 따르면, 음향 입력부(2952)는 마이크로폰일 수 있으며, 상기 예시에 제한되지 않는다. 음향 입력부(2952)은 외부 디바이스, 서버 또는 사용자로부터 음향 신호를 수신할 수 있다. 또한 음향 입력부(2952)는 외부의 음향 신호를 입력받는 과정에서 발생 되는 잡음(noise)를 제거하기 위한 다양한 잡음 제거 알고리즘을 이용할 수 있다.

[350] 본 발명에 따른 장치는 프로세서, 프로그램 데이터를 저장하고 실행하는 메모리, 디스크 드라이브와 같은 영구 저장부(permanent storage), 외부 장치와 통신하는 통신 포트, 터치 패널, 키(key), 버튼 등과 같은 사용자 인터페이스 장치 등을 포함할 수 있다. 소프트웨어 모듈 또는 알고리즘으로 구현되는 방법들은 상기 프로세서상에서 실행 가능한 컴퓨터가 읽을 수 있는 코드들 또는 프로그램 명령들로서 컴퓨터가 읽을 수 있는 기록 매체상에 저장될 수 있다. 여기서 컴퓨터가 읽을 수 있는 기록 매체로 마그네틱 저장 매체(예컨대, ROM(read-only memory), RAM(random-access memory), 플로피 디스크, 하드 디스크 등) 및 광학적 판독 매체(예컨대, 시디롬(CD-ROM), 디브이디(DVD: Digital Versatile Disc)) 등이 있다. 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템들에 분산되어, 분산 방식으로 컴퓨터가 판독 가능한 코드가 저장되고 실행될 수 있다. 매체는 컴퓨터에 의해 판독가능하며, 메모리에 저장되고, 프로세서에서 실행될 수 있다.

[351] 본 발명에서 인용하는 공개 문헌, 특허 출원, 특허 등을 포함하는 모든 문헌들은 각 인용 문헌이 개별적으로 및 구체적으로 병합하여 나타내는 것 또는 본 발명에서 전체적으로 병합하여 나타낸 것과 동일하게 본 발명에 병합될 수 있다.

[352] 본 발명의 이해를 위하여, 도면에 도시된 바람직한 실시 예들에서 참조 부호를 기재하였으며, 본 발명의 실시 예들을 설명하기 위하여 특정 용어들을 사용하였으나, 특정 용어에 의해 본 발명이 한정되는 것은 아니며, 본 발명은 당업자에 있어서 통상적으로 생각할 수 있는 모든 구성 요소들을 포함할 수 있다.

[353] 본 발명은 기능적인 블록 구성들 및 다양한 처리 단계들로 나타내어질 수 있다. 이러한 기능 블록들은 특정 기능들을 실행하는 다양한 개수의 하드웨어 또는/및 소프트웨어 구성들로 구현될 수 있다. 예를 들어, 본 발명은 하나 이상의 마이크로프로세서들의 제어 또는 다른 제어 디바이스들에 의해서 다양한 기능들을 실행할 수 있는, 메모리, 프로세싱, 로직(logic), 룩업 테이블(look-up table) 등과 같은 직접 회로 구성들을 채용할 수 있다. 본 발명에의 구성 요소들이 소프트웨어 프로그래밍 또는 소프트웨어 요소들로 실행될 수 있는 것과 유사하게, 본 발명은 데이터 구조, 프로세스들, 루틴들 또는 다른 프로그래밍

구성들의 조합으로 구현되는 다양한 알고리즘을 포함하여, C, C++, 자바(Java), 어셈블러(assembler) 등과 같은 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 기능적인 측면들은 하나 이상의 프로세서들에서 실행되는 알고리즘으로 구현될 수 있다. 또한, 본 발명은 전자적인 환경 설정, 신호 처리, 및/또는 데이터 처리 등을 위하여 종래 기술을 채용할 수 있다. '매커니즘', '요소', '수단', '구성'과 같은 용어는 넓게 사용될 수 있으며, 기계적이고 물리적인 구성들로서 한정되는 것은 아니다. 상기 용어는 프로세서 등과 연계하여 소프트웨어의 일련의 처리들(routines)의 의미를 포함할 수 있다.

[354] 본 발명에서 설명하는 특정 실행들은 일 실시 예들로서, 어떠한 방법으로도 본 발명의 범위를 한정하는 것은 아니다. 명세서의 간결함을 위하여, 종래 전자적인 구성들, 제어 시스템들, 소프트웨어, 상기 시스템들의 다른 기능적인 측면들의 기재는 생략될 수 있다. 또한, 도면에 도시된 구성 요소들 간의 선들의 연결 또는 연결 부재들은 기능적인 연결 및/또는 물리적 또는 회로적 연결들을 예시적으로 나타낸 것으로서, 실제 디바이스에서는 대체 가능하거나 추가의 다양한 기능적인 연결, 물리적인 연결, 또는 회로 연결들로서 나타내어질 수 있다. 또한, '필수적인', '중요하게' 등과 같이 구체적인 언급이 없다면 본 발명의 적용을 위하여 반드시 필요한 구성 요소가 아닐 수 있다.

[355] 본 발명의 명세서(특히 특허청구범위에서)에서 '상기'의 용어 및 이와 유사한 지시 용어의 사용은 단수 및 복수 모두에 해당하는 것일 수 있다. 또한, 본 발명에서 범위(range)를 기재한 경우 상기 범위에 속하는 개별적인 값을 적용한 발명을 포함하는 것으로서(이에 반하는 기재가 없다면), 발명의 상세한 설명에 상기 범위를 구성하는 각 개별적인 값을 기재한 것과 같다. 마지막으로, 본 발명에 따른 방법을 구성하는 단계들에 대하여 명백하게 순서를 기재하거나 반하는 기재가 없다면, 상기 단계들은 적당한 순서로 행해질 수 있다. 반드시 상기 단계들의 기재 순서에 따라 본 발명이 한정되는 것은 아니다. 본 발명에서 모든 예들 또는 예시적인 용어(예들 들어, 등등)의 사용은 단순히 본 발명을 상세히 설명하기 위한 것으로서 특허청구범위에 의해 한정되지 않는 이상 상기 예들 또는 예시적인 용어로 인해 본 발명의 범위가 한정되는 것은 아니다. 또한, 당업자는 다양한 수정, 조합 및 변경이 부가된 특허청구범위 또는 그 균등물의 범주 내에서 설계 조건 및 팩터에 따라 구성될 수 있음을 알 수 있다.

청구범위

[청구항 1] 제1 디바이스에서 암호화된 데이터를 송신하는 방법으로써,
송신할 데이터를 암호화하기 위한 암호화키를 생성하는 단계;
상기 생성된 암호화키를 이용하여 키식별정보를 생성하는 단계;
상기 생성된 암호화 키를 이용하여 송신할 데이터를 암호화하는 단계; 및
상기 암호화된 데이터 및 상기 키식별정보를 포함하는 데이터 세트를 제2 디바이스로 송신하는 단계를 포함하고,
상기 키식별정보는 상기 제2 디바이스가 식별할 수 있는 상기 제1 디바이스의 식별정보 또는 상기 암호화키를 식별할 수 있는 정보를 포함하는, 데이터를 송신하는 방법.

[청구항 2] 제 1항에 있어서,
상기 암호화키를 생성하는 단계는,
상기 제1 디바이스의 공개키 및 제1 난수를 상기 제2 디바이스로 전송하고 상기 제2 디바이스로부터 상기 제2 디바이스의 공개키 및 제2 난수를 수신하는 단계; 및
상기 제1 디바이스의 공개키 및 상기 제2 디바이스의 공개키를 이용하여 상기 암호화키를 생성하는 단계를 포함하고,
상기 키식별정보는 상기 제1 난수, 상기 제2 난수 및 상기 암호화키를 이용하여 생성되며,
상기 키식별정보는 상기 제 1 난수 또는 상기 제 2 난수에 기초하여 상기 제 1 디바이스를 식별할 수 있는 정보를 포함하는 것을 특징으로 하는,
암호화된 데이터를 송신하는 방법.

[청구항 3] 제 1항에 있어서,
상기 키식별정보를 생성하는 단계는,
상기 제 2 디바이스로부터 상기 제2 디바이스의 공개키를 수신하는 단계; 및
상기 수신된 제2 디바이스의 공개키를 이용하여 상기 암호화키를 암호화하여 상기 키식별정보를 생성하는 단계를 포함하는,
암호화된 데이터를 송신하는 방법.

[청구항 4] 제 1항에 있어서,
상기 암호화키를 생성하는 단계는
제2 디바이스와 비공개키를 공유하는 단계; 및
상기 비공개키 및 제1 난수를 이용하여 상기 암호화키를 생성하는 단계를 포함하고,
상기 키식별정보는 상기 제1 난수, 및 상기 제1 난수와 상기

암호화키를 조합한 값을 상기 제1 난수로 키-해싱한 값을 포함하는, 암호화된 데이터를 송신하는 방법.

[청구항 5] 제2 디바이스에서 암호화된 데이터를 수신하는 방법으로써,
제1 디바이스로부터 암호화된 데이터 및 키식별정보를 포함하는 데이터 세트를 수신하는 단계;
상기 키식별정보를 이용하여 제1 디바이스에 대한 암호화키를 획득하는 단계;
상기 획득된 암호화키를 이용하여 상기 암호화된 데이터를 복호화하는 단계를 포함하며,
상기 키식별정보는 제2 디바이스가 식별할 수 있는 제1 디바이스의 정보 또는 상기 암호화키를 식별할 수 있는 정보를 포함하는, 암호화된 데이터를 수신하는 방법.

[청구항 6] 제 5항에 있어서,
상기 방법은,
상기 제1 디바이스를 포함하는 적어도 하나의 디바이스로부터 적어도 하나의 공개키 및 적어도 하나의 난수를 각각 수신하고
상기 제2 디바이스의 공개키 및 제2 난수를 상기 적어도 하나의 디바이스로 각각 송신하는 단계를 더 포함하고,
상기 제1 디바이스에 대한 암호화키를 획득하는 단계는,
상기 수신된 적어도 하나의 공개키 및 상기 제2 디바이스의 공개키를 이용하여 상기 적어도 하나의 디바이스에 대한 적어도 하나의 암호화키를 생성하는 단계;
상기 적어도 하나의 암호화키를 이용하여 적어도 하나의 키식별정보를 생성하는 단계;
상기 생성된 적어도 하나의 키식별정보와 상기 수신된 키식별정보를 비교하여 상기 암호화된 데이터를 송신한 제1 디바이스를 식별하는 단계; 및
상기 식별된 제1 디바이스에 대한 암호화키를 획득하는 단계를 포함하는, 암호화된 데이터를 수신하는 방법.

[청구항 7] 제 5 항에 있어서,
상기 방법은,
상기 제1 디바이스를 포함하는 적어도 하나의 디바이스들과 적어도 하나의 비공개키를 공유하는 단계를 더 포함하고,
상기 데이터 세트를 수신하는 단계는
상기 적어도 하나의 디바이스 중 상기 제1 디바이스로부터 암호화된 데이터 및 키식별정보를 수신하는 단계를 포함하고,
상기 키식별정보는 상기 제1 디바이스의 제 1 난수, 및 상기 제 1 난수로 암호화키를 키-해싱한(key-hashed) 값을 포함하고,

상기 암호화키는 상기 제 1 디바이스와 공유한 비공개키와 상기 제 1난수의 조합에 의해 생성된 정보이며,
상기 제 1 디바이스에 대한 암호화키를 획득하는 단계는,
수신한 상기 제 1 난수를 이용하여, 상기 적어도 하나의 비공개키와 상기 제1 난수를 각각 조합한 값들을 상기 제1 난수로 각각 키-해싱하여 적어도 하나의 매칭키들을 생성하는 단계;
상기 생성된 적어도 하나의 매칭키들과 수신한 상기 제1 난수로 상기 암호화키를 키-해싱한 값을 비교하여 상기 데이터 세트를 송신한 제 1 디바이스를 식별하는 단계; 및
상기 제 1 디바이스의 암호화키를 획득하는 단계를 포함하는,
암호화된 데이터를 수신하는 방법.

[청구항 8] 암호화된 데이터를 송신하는 제1 디바이스로써,
암호화키를 생성하고, 상기 생성된 암호화키를 이용하여 키식별정보를 생성하고 데이터를 암호화하는 제어부;
상기 암호화된 데이터 및 상기 키식별정보를 포함하는 데이터 세트를 제2 디바이스로 송신하는 송수신부를 포함하며,
상기 키식별정보는 상기 제2 디바이스가 식별 할 수 있는 상기 제1 디바이스의 정보 또는 상기 암호화키를 식별할 수 있는 정보를 포함하는 것을 특징으로 하는제1 디바이스.

[청구항 9] 제 8 항에 있어서,
상기 송수신부는 상기 제1 디바이스의 공개키 및 제1 난수를 제2 디바이스로 전송하고 상기 제2 디바이스로부터 상기 제2 디바이스의 공개키 및 제2 난수를 수신하고,
상기 제어부는 상기 제1 디바이스의 공개키 및 상기 제2 디바이스의 공개키를 이용하여 상기 암호화키를 생성하고,
상기 키식별정보는 상기 제1 난수, 제2 난수 및 상기 암호화키를 이용하여 생성되며,
상기 키식별정보는 상기 제 1 난수 또는 제 2 난수에 기초하여 상기 제 1 디바이스를 식별할 수 있는 정보를 포함하는 것을 특징으로 하는, 제1 디바이스.

[청구항 10] 제 8 항에 있어서,
상기 송수신부는 제 2 디바이스로부터 상기 제 2 디바이스의 공개키를 수신하고,
상기 키식별정보는 상기 제 2 디바이스의 공개키를 이용하여 상기 암호화키를 암호화하여 생성되는 것을 특징으로 하는, 제1 디바이스.

[청구항 11] 암호화된 데이터를 수신하는 제 2 디바이스로서,
암호화된 데이터 및 키식별정보를 포함하는 데이터 세트를 제1

디바이스로부터 수신하는 송수신부;
상기 키식별정보를 이용하여 암호화키를 획득하고, 상기 암호화키를 이용하여 상기 수신된 암호화된 데이터를 복호화하는 제어부를 포함하며,
상기 키식별정보는 상기 제2 디바이스가 식별 할 수 있는 상기 제1 디바이스의 정보 또는 상기 암호화키를 식별할 수 있는 정보를 포함하는 것을 특징으로 하는, 제2 디바이스.

[청구항 12] 제 11 항에 있어서,
상기 송수신부는 상기 제2 디바이스의 공개키를 상기 제1 디바이스로 추가적으로 전송하고,
상기 제어부는 상기 키식별정보를 상기 제2 디바이스의 공개키에 대응되는 개인키를 이용하여 복호화하여 암호화키를 획득하는 것을 특징으로 하는, 제2 디바이스.

[청구항 13] 제 1 디바이스에서 암호화된 데이터 송신을 위한 키를 공유하는 방법에 있어서,
통신 내역에 기초하여, 제 2 디바이스에게 송신한 제 1 디바이스의 제 1 공개키 및 상기 제 1 디바이스의 제 1 공개키에 대응하는 제 1 디바이스의 제 1 개인키가 저장되어 있는지 판단하는 단계;
판단 결과에 기초하여 제 1 디바이스의 제 2 공개키 및 제 1 디바이스의 제 2 개인키를 생성하는 단계;
상기 생성된 제 1 디바이스의 제 2 공개키를 상기 제 1 디바이스의 제 1 개인키로 서명하는 단계; 및
상기 서명된 제 2 공개키를 제 2 디바이스로 송신하는 단계를 포함하는 키 공유 방법.

[청구항 14] 제 13 항에 있어서,
상기 방법은,
상기 제 2 디바이스로부터 상기 제 2 디바이스의 제 1 개인키로 서명된 제 2 공개키를 수신하는 단계;
통신 내역에 기초하여, 상기 제 2 디바이스의 제 1 개인키와 대응되는 상기 제 2 디바이스의 제 1 공개키를 획득하는 단계;
상기 획득한 제 2 디바이스의 제 1 공개키로 상기 서명된 제 2 공개키를 검증하는 단계; 및
상기 검증 결과에 기초하여 암호화 통신을 수행하는 단계를 포함하는 방법.

[청구항 15] 제 13 항에 있어서,
상기 제 1 디바이스의 제 1 공개키 및 상기 제 1 디바이스의 제 1 개인키는, 이전의 상기 제 1 디바이스 및 상기 제 2 디바이스 간의 통신 수행시 사용된 키들인 것을 특징으로 하는 방법.

[청구항 16] 제 13 항에 있어서,
상기 판단하는 단계는,
상기 통신 내역에 기초하여 이전 통신 수행시 상기 제 2 디바이스에게 송신한 제 1 난수가 저장되어 있는지 판단하는 단계를 포함하고,
상기 서명하는 단계는,
상기 통신 내역에 기초하여 이전 통신 수행시 상기 제 2 디바이스로부터 수신한 제 2 난수를 상기 제 1 디바이스의 제 1 개인키로 서명하는 단계를 포함하고,
상기 송신하는 단계는,
상기 서명된 제 2 난수를 송신하는 단계를 포함하는 방법.

[청구항 17] 암호화된 데이터 송신을 위한 키를 공유하는 제 1 디바이스 있어서,
통신 내역에 기초하여, 제 2 디바이스에게 송신한 제 1 디바이스의 제 1 공개키 및 상기 제 1 디바이스의 제 1 공개키에 대응하는 제 1 디바이스의 제 1 개인키가 저장되어 있는지 판단하는 제어부;
판단 결과에 기초하여 제 1 디바이스의 제 2 공개키 및 제 1 디바이스의 제 2 개인키를 생성하고, 상기 생성된 제 1 디바이스의 제 2 공개키를 상기 제 1 디바이스의 제 1 개인키로 서명하는 암호화부; 및
상기 서명된 제 2 공개키를 제 2 디바이스로 송신하는 통신부를 포함하는 디바이스.

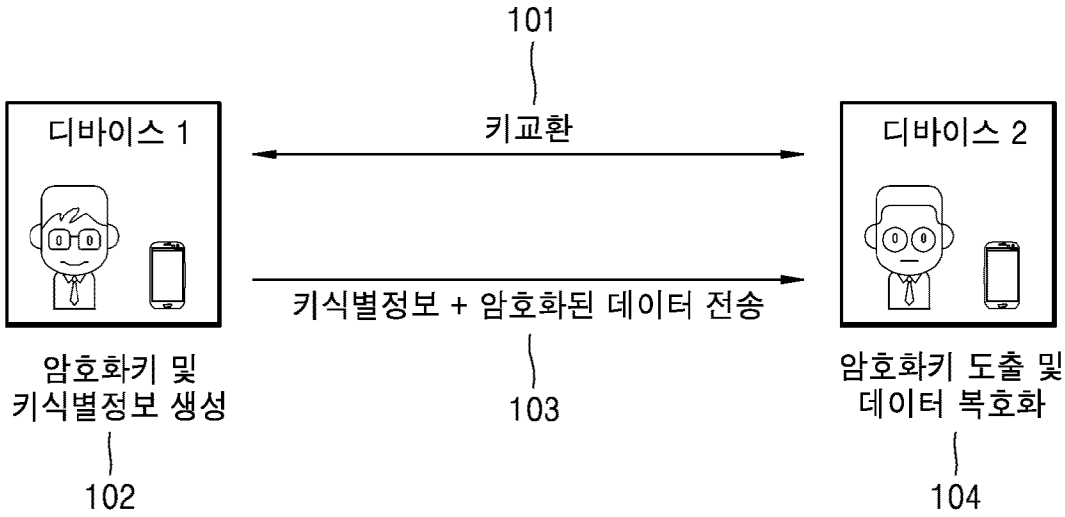
[청구항 18] 제 17 항에 있어서,
상기 통신부는, 상기 제 2 디바이스로부터 상기 제 2 디바이스의 제 1 개인키로 서명된 제 2 공개키를 수신하고,
상기 암호화부는, 통신 내역에 기초하여, 상기 제 2 디바이스의 제 1 개인키와 대응되는 상기 제 2 디바이스의 제 1 공개키를 획득하고, 상기 획득한 제 2 디바이스의 제 1 공개키로 상기 서명된 제 2 공개키를 검증하고,
상기 제어부는, 상기 검증 결과에 기초하여 암호화 통신을 수행할지 여부를 결정하는 것을 특징으로 하는 디바이스.

[청구항 19] 제 17 항에 있어서,
상기 제어부는,
상기 통신 내역에 기초하여 이전 통신 수행시 상기 제 2 디바이스에게 송신한 제 1 난수가 저장되어 있는지 판단하고,
상기 암호화부는,
상기 통신 내역에 기초하여 이전 통신 수행시 상기 제 2 디바이스로부터 수신한 제 2 난수를 상기 제 1 디바이스의 제 1

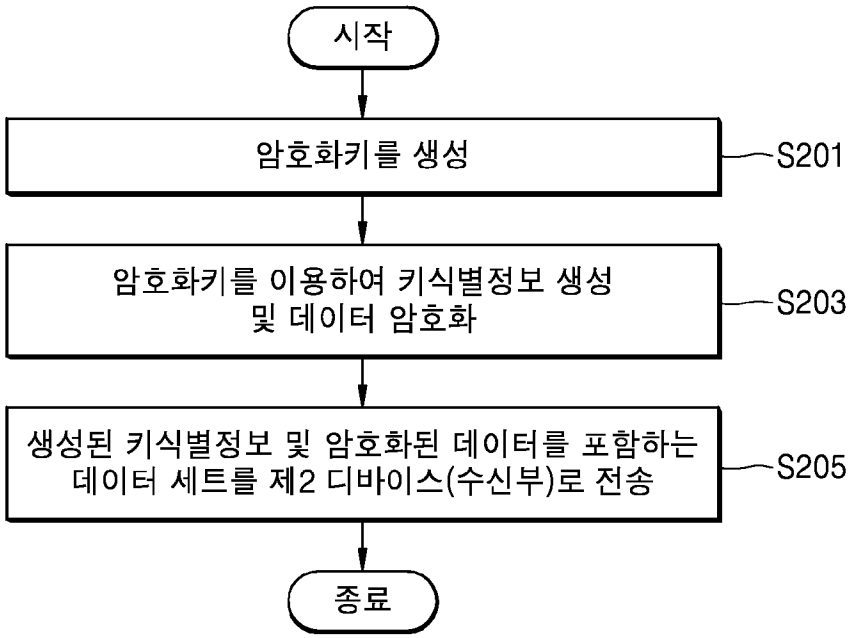
개인키로 서명하며,
상기 통신부는,
상기 서명된 제 2 난수를 송신하는 디바이스.

[청구항 20] 제1항 또는 제13항의 방법 중 어느 한 항의 방법을 컴퓨터에서 실행시키는 프로그램을 기록한, 컴퓨터로 판독가능한 기록매체.

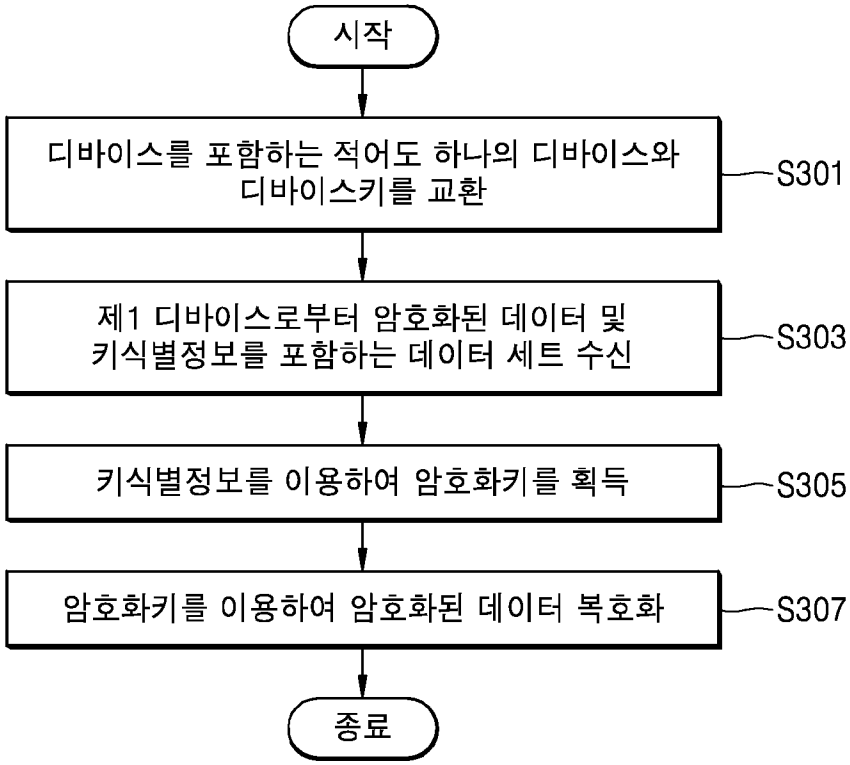
[Fig. 1]


101
디바이스 1
키교환
디바이스 2
키식별정보 + 암호화된 데이터 전송
암호화키 및
키식별정보 생성
103
암호화키 도출 및
데이터 복호화
102
104

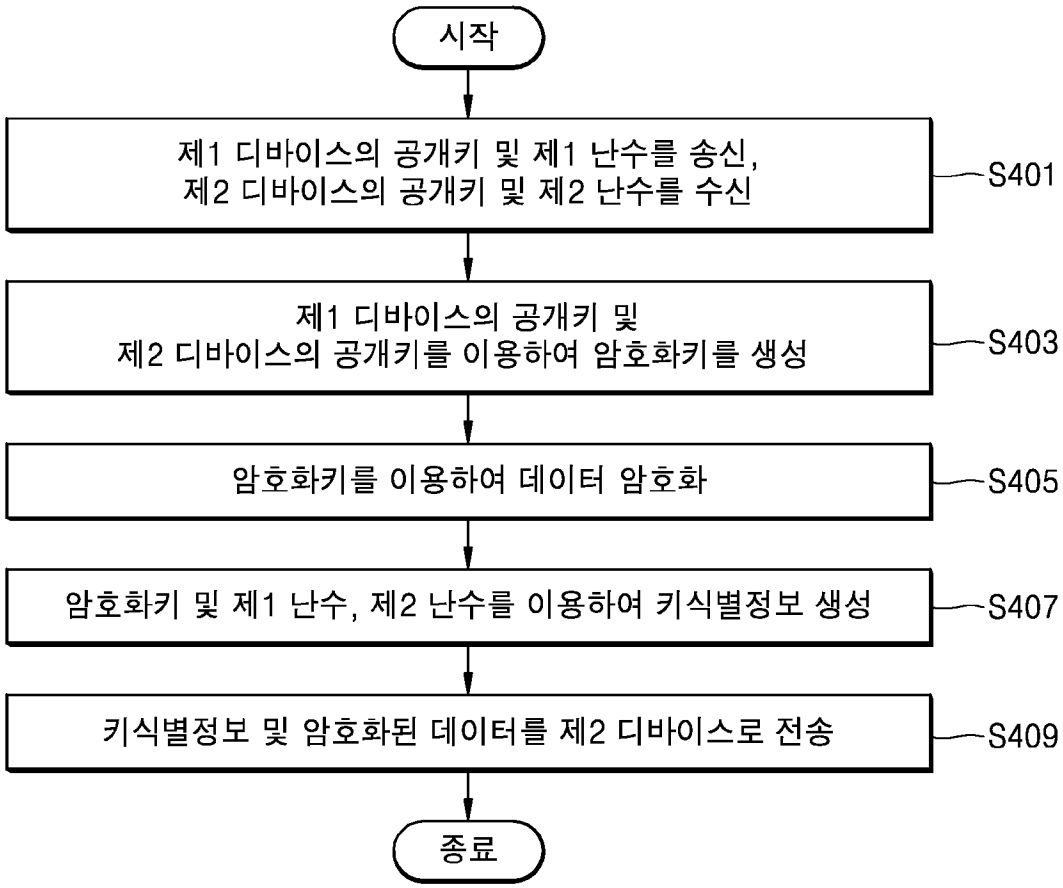
[Fig. 2]


시작
암호화키를 생성
S201
암호화키를 이용하여 키식별정보 생성
및 데이터 암호화
S203
생성된 키식별정보 및 암호화된 데이터를 포함하는
데이터 세트를 제2 디바이스(수신부)로 전송
S205
종료

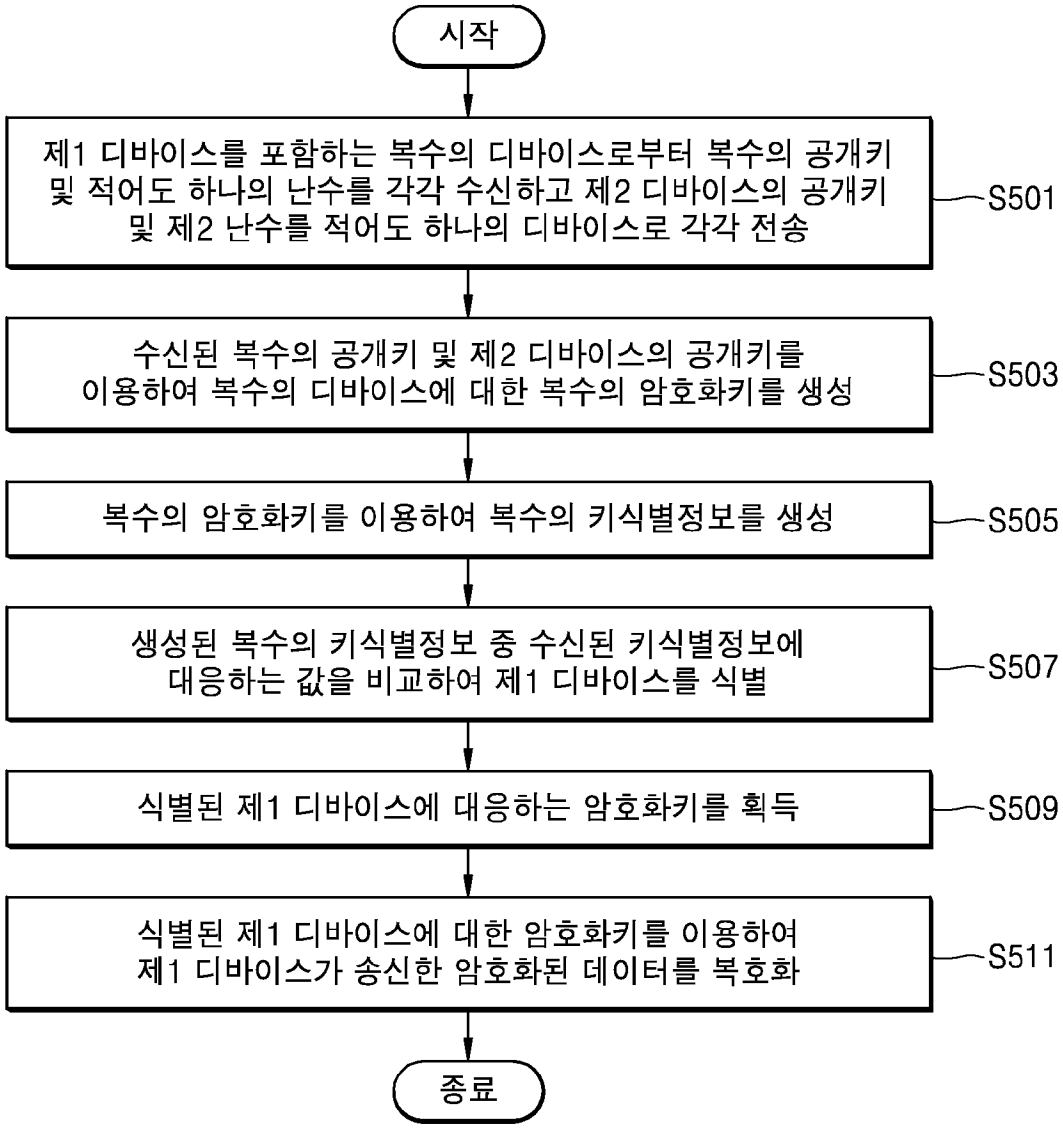
[Fig. 3]


시작
디바이스를 포함하는 적어도 하나의 디바이스와 디바이스키를 교환
S301
제1 디바이스로부터 암호화된 데이터 및 키식별정보를 포함하는 데이터 세트 수신
S303
키식별정보를 이용하여 암호화키를 획득
S305
암호화키를 이용하여 암호화된 데이터 복호화
S307
종료

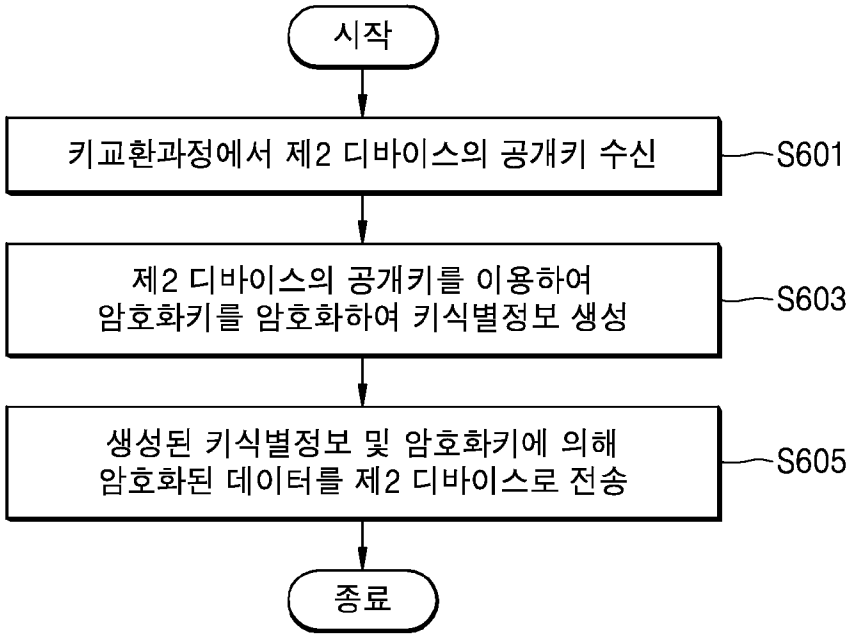
[Fig. 4]


시작
제1 디바이스의 공개키 및 제1 난수를 송신, 제2 디바이스의 공개키 및 제2 난수를 수신
S401
제1 디바이스의 공개키 및 제2 디바이스의 공개키를 이용하여 암호화키를 생성
S403
암호화키를 이용하여 데이터 암호화
S405
암호화키 및 제1 난수, 제2 난수를 이용하여 키식별정보 생성
S407
키식별정보 및 암호화된 데이터를 제2 디바이스로 전송
S409
종료

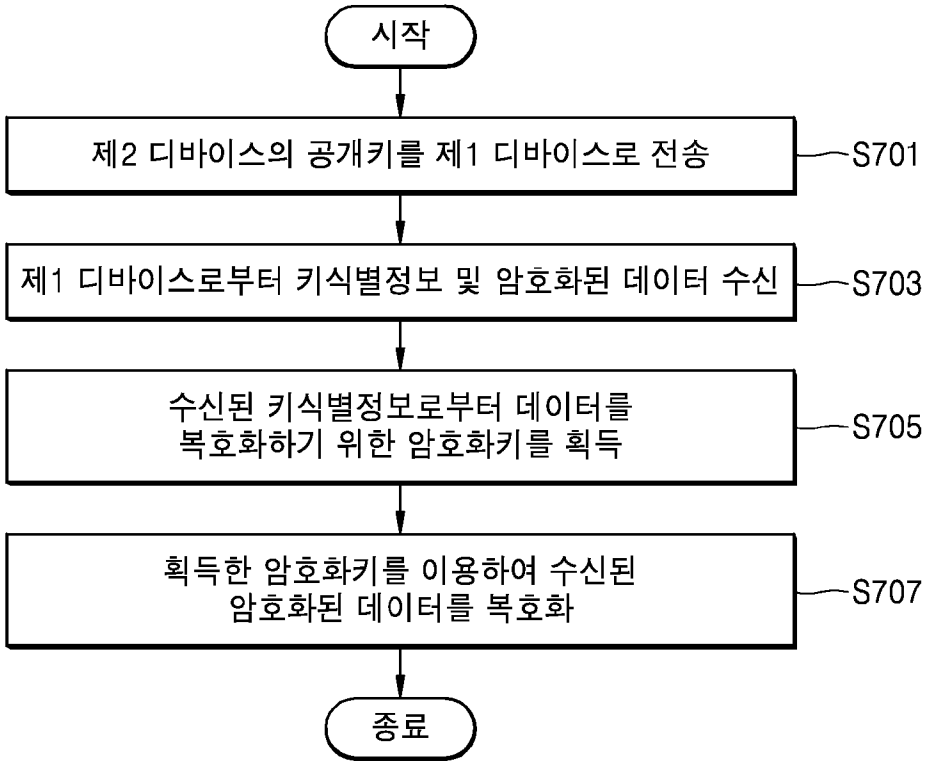
[Fig. 5]


시작
제1 디바이스를 포함하는 복수의 디바이스로부터 복수의 공개키 및 적어도 하나의 난수를 각각 수신하고 제2 디바이스의 공개키 및 제2 난수를 적어도 하나의 디바이스로 각각 전송
S501
수신된 복수의 공개키 및 제2 디바이스의 공개키를 이용하여 복수의 디바이스에 대한 복수의 암호화키를 생성
S503
복수의 암호화키를 이용하여 복수의 키식별정보를 생성
S505
생성된 복수의 키식별정보 중 수신된 키식별정보에 대응하는 값을 비교하여 제1 디바이스를 식별
S507
식별된 제1 디바이스에 대응하는 암호화키를 획득
S509
식별된 제1 디바이스에 대한 암호화키를 이용하여 제1 디바이스가 송신한 암호화된 데이터를 복호화
S511
종료

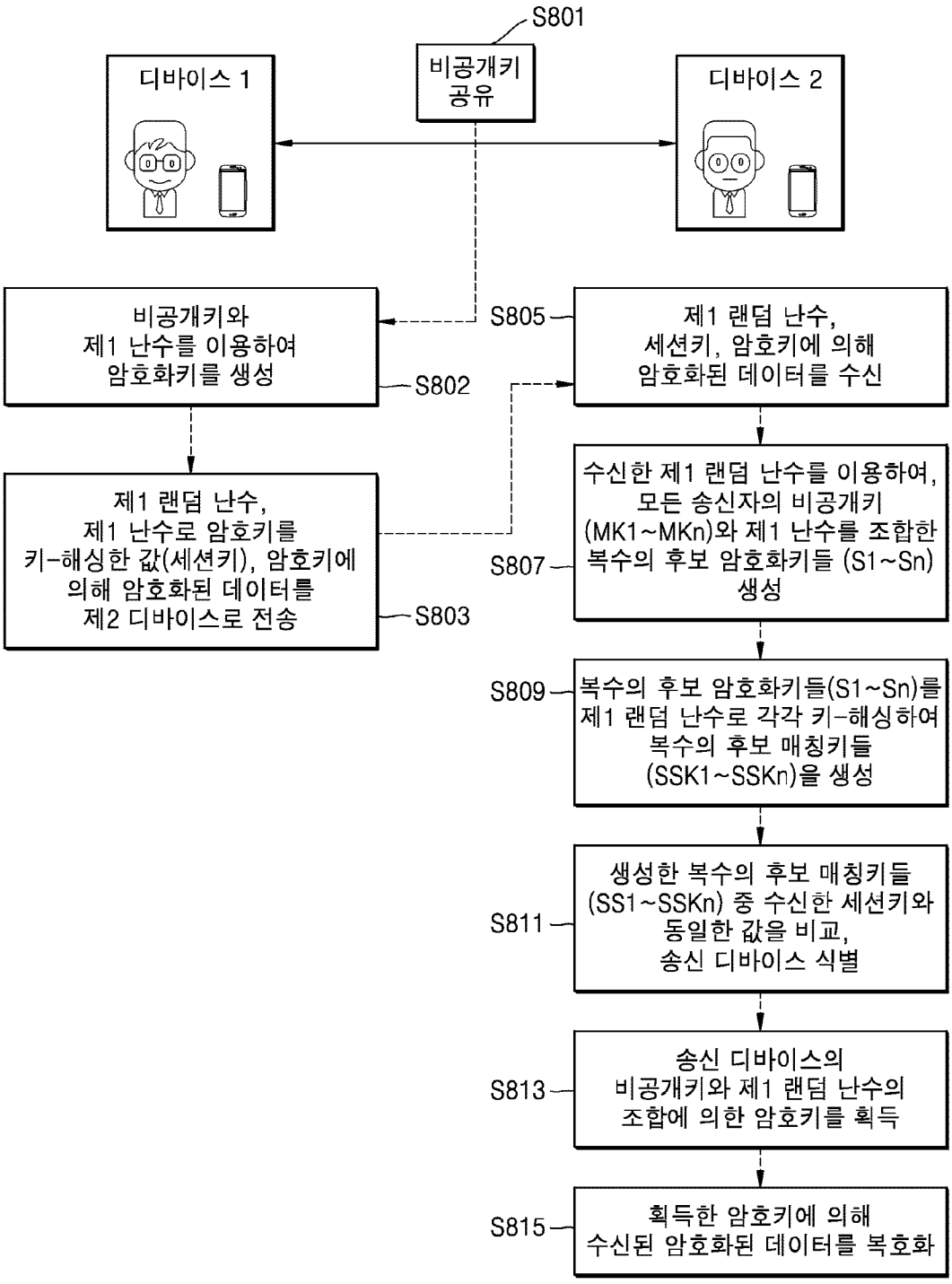
[Fig. 6]


시작
키교환과정에서 제2 디바이스의 공개키 수신
S601
제2 디바이스의 공개키를 이용하여 암호화키를 암호화하여 키식별정보 생성
S603
생성된 키식별정보 및 암호화키에 의해 암호화된 데이터를 제2 디바이스로 전송
S605
종료

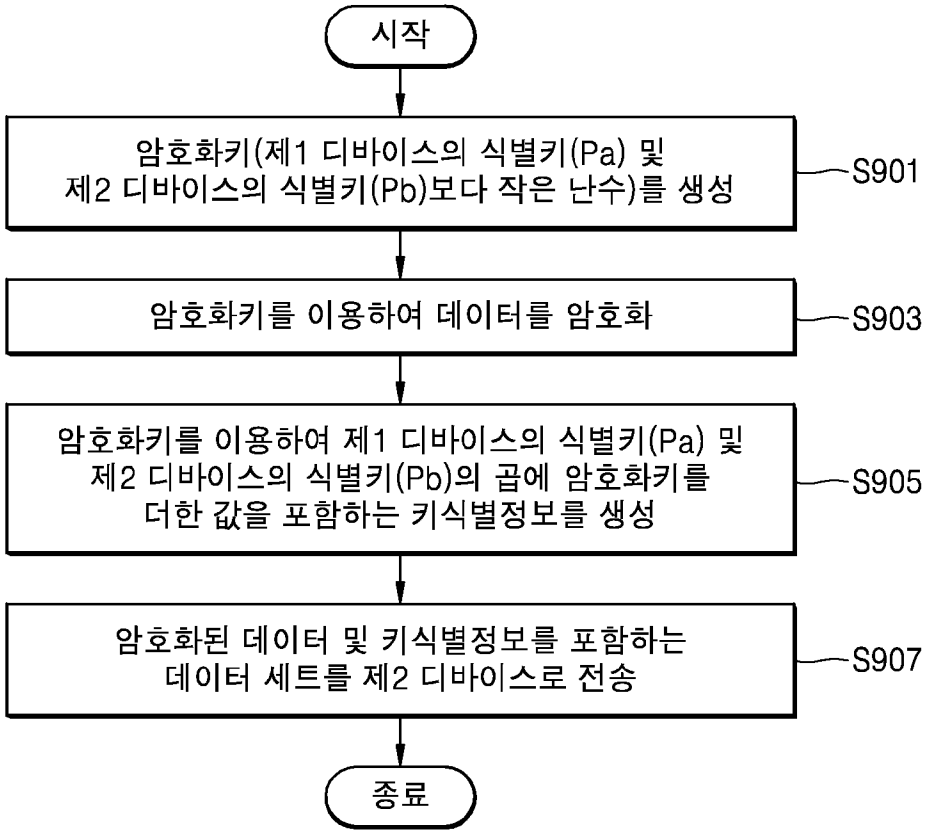
[Fig. 7]


시작
제2 디바이스의 공개키를 제1 디바이스로 전송
S701
제1 디바이스로부터 키식별정보 및 암호화된 데이터 수신
S703
수신된 키식별정보로부터 데이터를
복호화하기 위한 암호화키를 획득
S705
획득한 암호화키를 이용하여 수신된
암호화된 데이터를 복호화
S707
종료

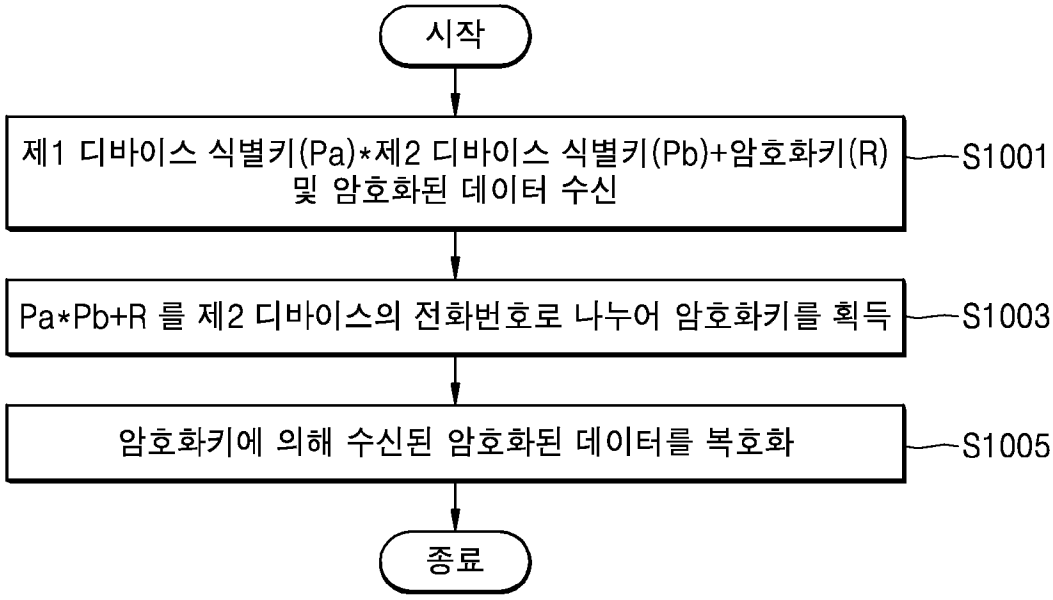
[Fig. 8]


S801
비공개키 공유
디바이스 1
디바이스 2
비공개키와 제1 난수를 이용하여 암호화키를 생성
S802
제1 랜덤 난수, 제1 난수로 암호키를 키-해싱한 값(세션키), 암호키에 의해 암호화된 데이터를 제2 디바이스로 전송
S803
S805
제1 랜덤 난수, 세션키, 암호키에 의해 암호화된 데이터를 수신
수신한 제1 랜덤 난수를 이용하여, 모든 송신자의 비공개키 (MK1~MKn)와 제1 난수를 조합한 복수의 후보 암호화키들 (S1~Sn) 생성
S807
S809
복수의 후보 암호화키들(S1~Sn)를 제1 랜덤 난수로 각각 키-해싱하여 복수의 후보 매칭키들 (SSK1~SSKn)을 생성
S811
생성한 복수의 후보 매칭키들 (SS1~SSKn) 중 수신한 세션키와 동일한 값을 비교, 송신 디바이스 식별
S813
송신 디바이스의 비공개키와 제1 랜덤 난수의 조합에 의한 암호키를 획득
S815
획득한 암호키에 의해 수신된 암호화된 데이터를 복호화

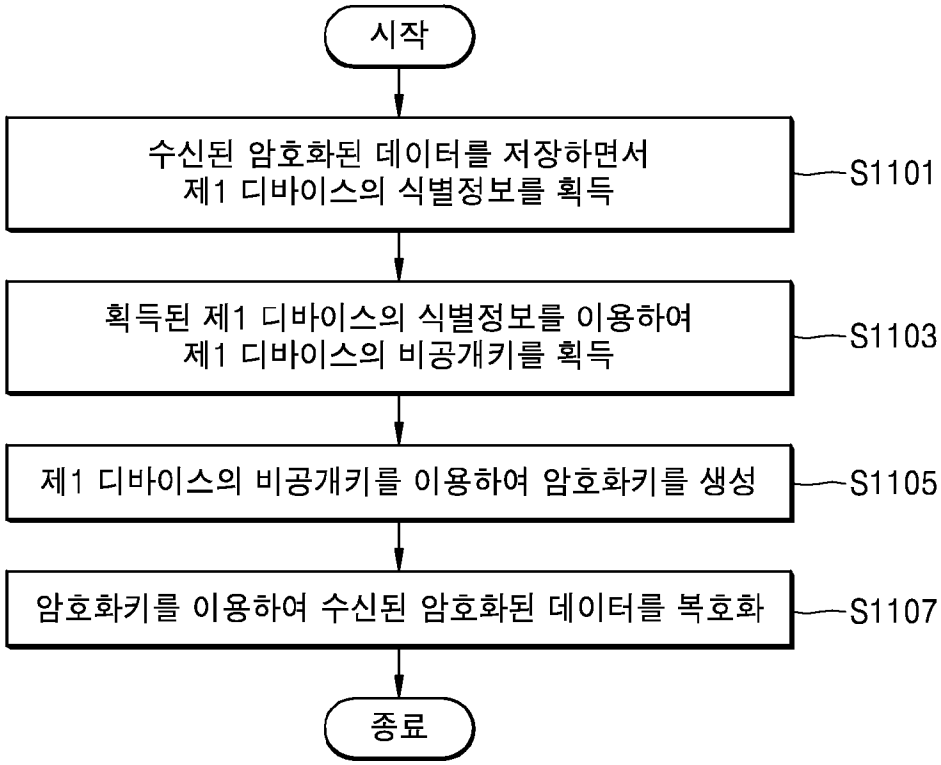
[Fig. 9]


시작
암호화키(제1 디바이스의 식별키(Pa) 및
제2 디바이스의 식별키(Pb)보다 작은 난수)를 생성
S901
암호화키를 이용하여 데이터를 암호화
S903
암호화키를 이용하여 제1 디바이스의 식별키(Pa) 및
제2 디바이스의 식별키(Pb)의 곱에 암호화키를
더한 값을 포함하는 키식별정보를 생성
S905
암호화된 데이터 및 키식별정보를 포함하는
데이터 세트를 제2 디바이스로 전송
S907
종료

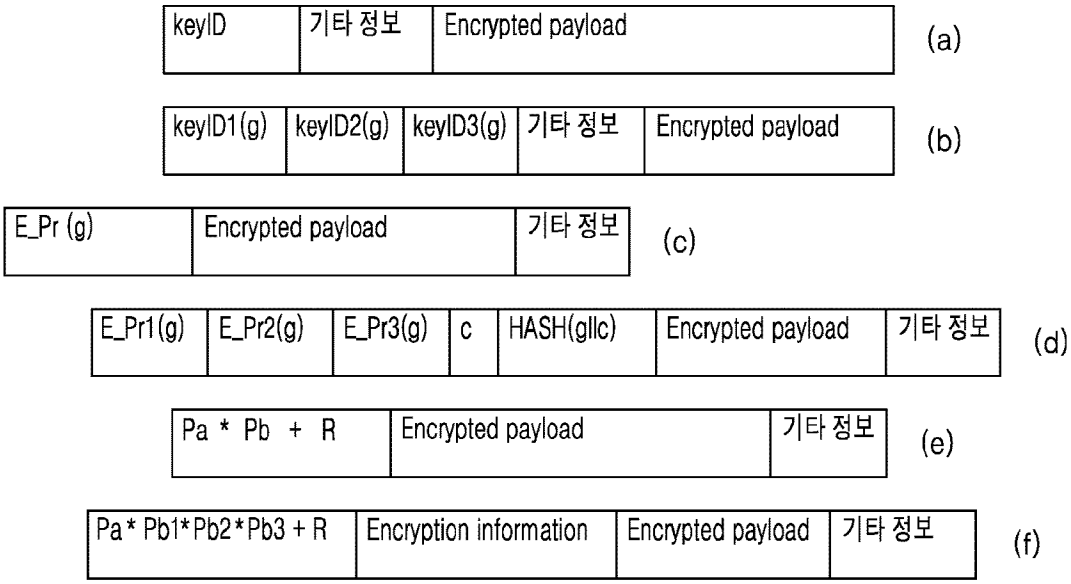
[Fig. 10]


시작
제1 디바이스 식별키(Pa)*제2 디바이스 식별키(Pb)+암호화키(R)
및 암호화된 데이터 수신
S1001
Pa*Pb+R 를 제2 디바이스의 전화번호로 나누어 암호화키를 획득
S1003
암호화키에 의해 수신된 암호화된 데이터를 복호화
S1005
종료

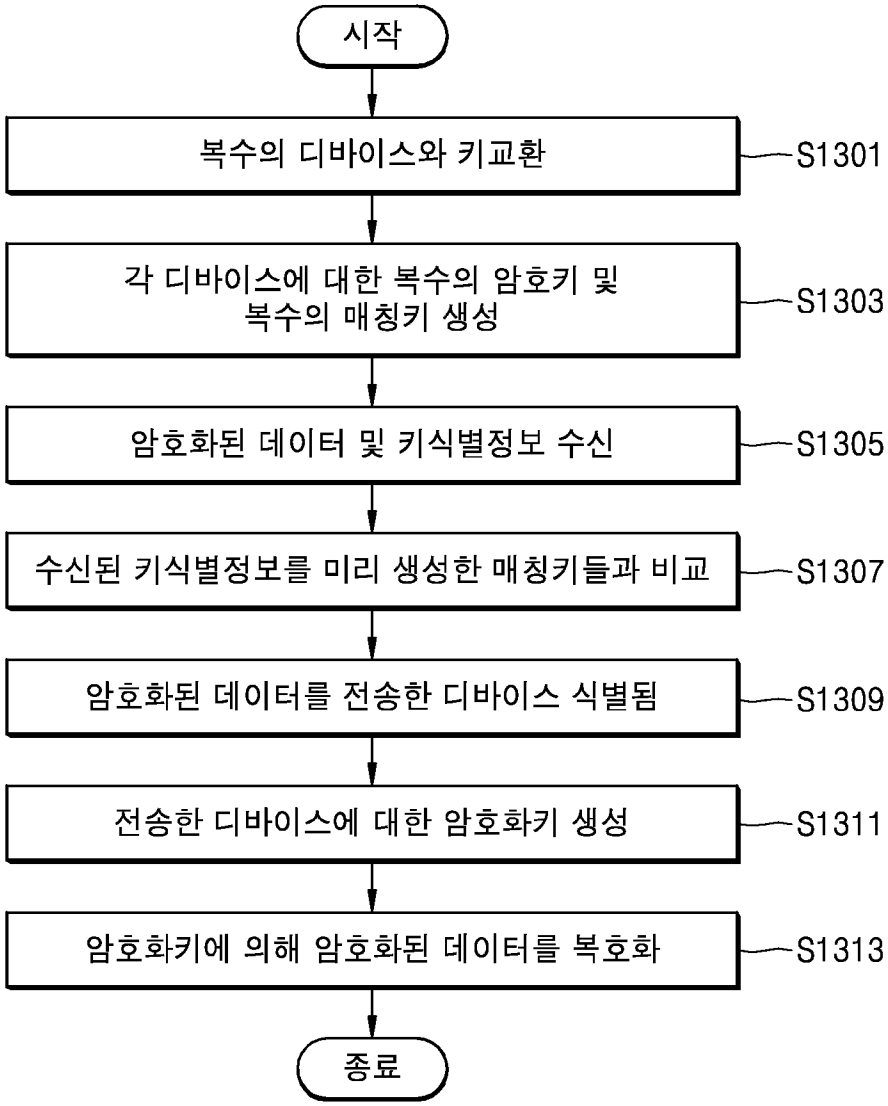
[Fig. 11]


시작
수신된 암호화된 데이터를 저장하면서 제1 디바이스의 식별정보를 획득
S1101
획득된 제1 디바이스의 식별정보를 이용하여 제1 디바이스의 비공개키를 획득
S1103
제1 디바이스의 비공개키를 이용하여 암호화키를 생성
S1105
암호화키를 이용하여 수신된 암호화된 데이터를 복호화
S1107
종료

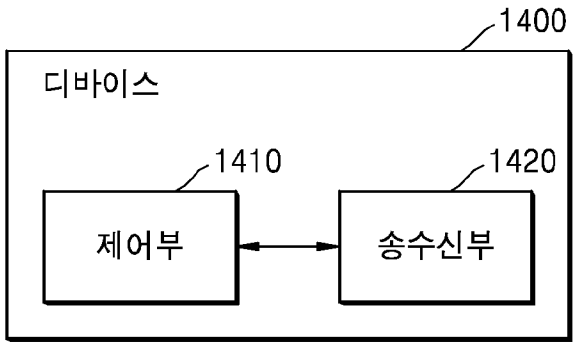
[Fig. 12]


keyID
기타 정보
Encrypted payload
(a)
keyID1(g)
keyID2(g)
keyID3(g)
기타 정보
Encrypted payload
(b)
E_Pr (g)
Encrypted payload
기타 정보
(c)
E_Pr1(g)
E_Pr2(g)
E_Pr3(g)
c
HASH(gIIc)
Encrypted payload
기타 정보
(d)
Pa * Pb + R
Encrypted payload
기타 정보
(e)
Pa* Pb1*Pb2*Pb3 + R
Encryption information
Encrypted payload
기타 정보
(f)

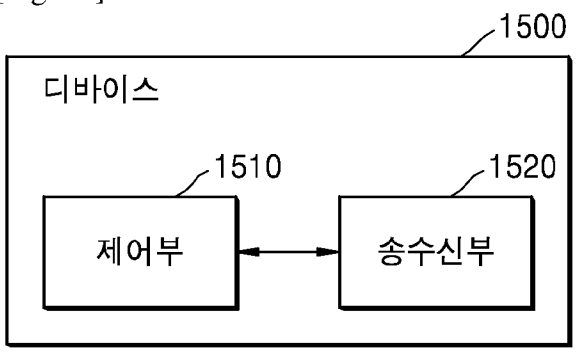
[Fig. 13]



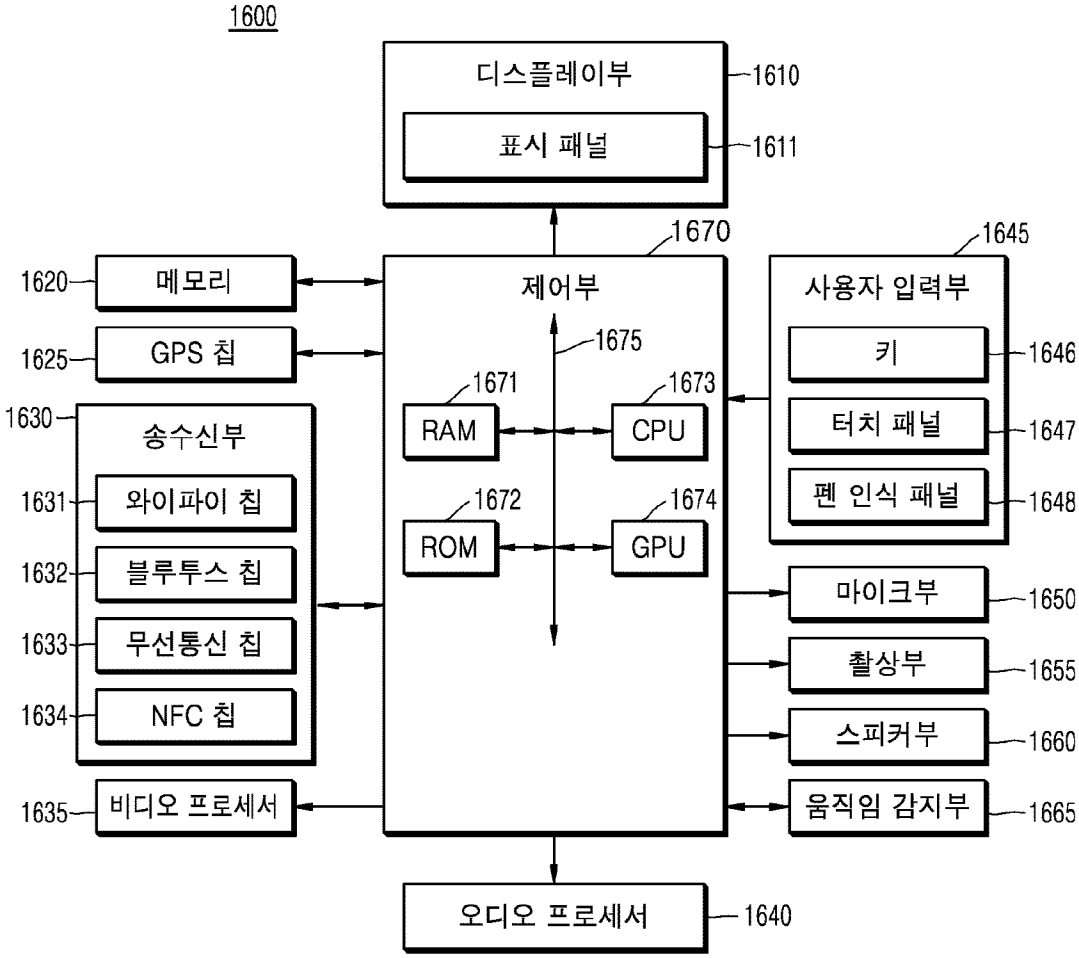
[Fig. 14]



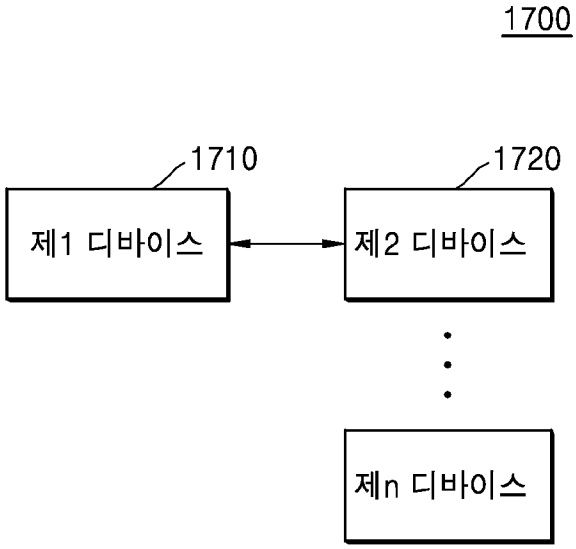
[Fig. 15]



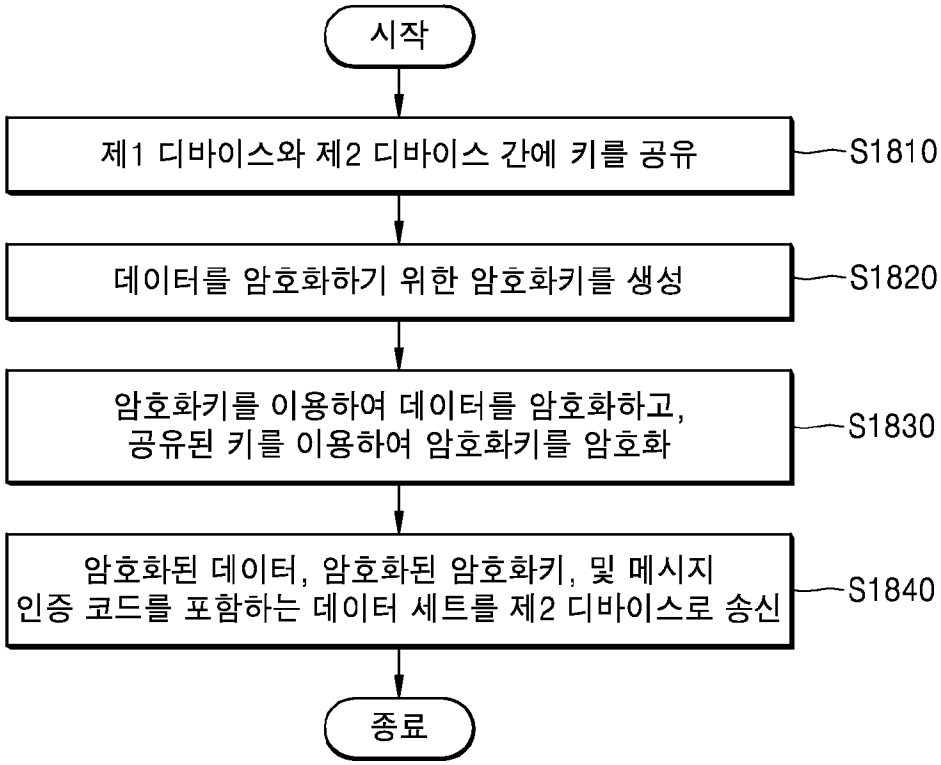
[Fig. 16]


1600
디스플레이부
1610
표시 패널
1611
1670
제어부
1675
1671
RAM
1673
CPU
1672
ROM
1674
GPU
1645
사용자 입력부
키
1646
터치 패널
1647
펜 인식 패널
1648
1620
메모리
1625
GPS 칩
1630
송수신부
1631
와이파이 칩
1632
블루투스 칩
1633
무선통신 칩
1634
NFC 칩
1635
비디오 프로세서
마이크부
1650
촬상부
1655
스피커부
1660
움직임 감지부
1665
오디오 프로세서
1640

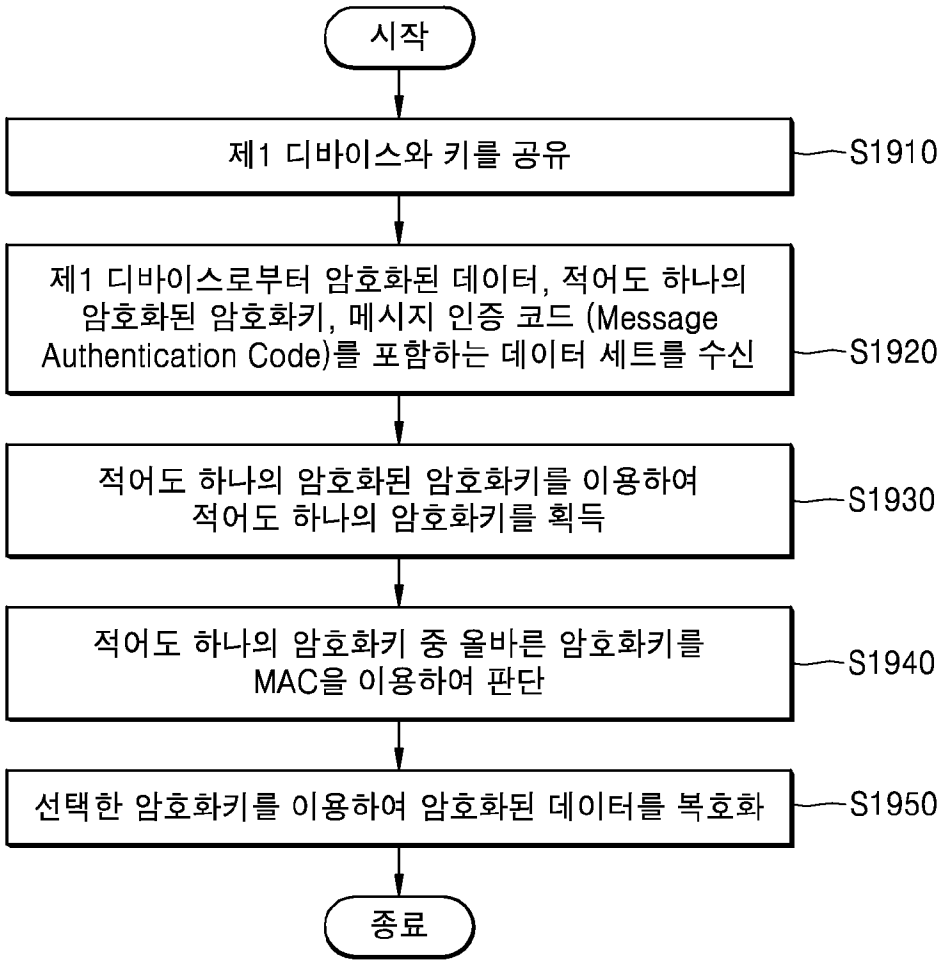
[Fig. 17]


1700
1710
제1 디바이스
1720
제2 디바이스
제n 디바이스

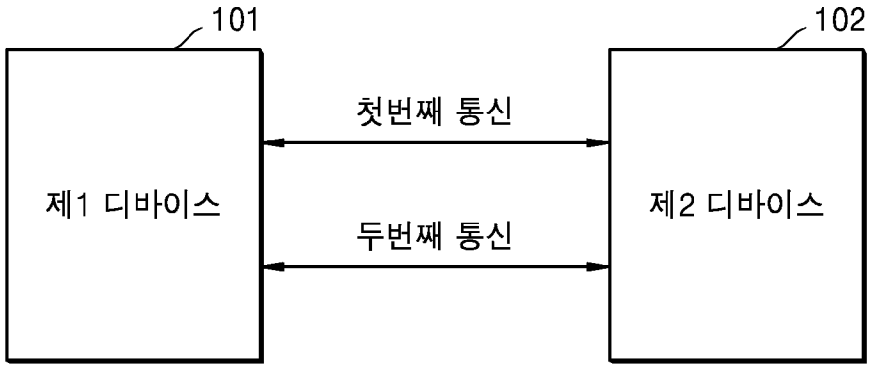
[Fig. 18]


시작
제1 디바이스와 제2 디바이스 간에 키를 공유
S1810
데이터를 암호화하기 위한 암호화키를 생성
S1820
암호화키를 이용하여 데이터를 암호화하고,
공유된 키를 이용하여 암호화키를 암호화
S1830
암호화된 데이터, 암호화된 암호화키, 및 메시지
인증 코드를 포함하는 데이터 세트를 제2 디바이스로 송신
S1840
종료

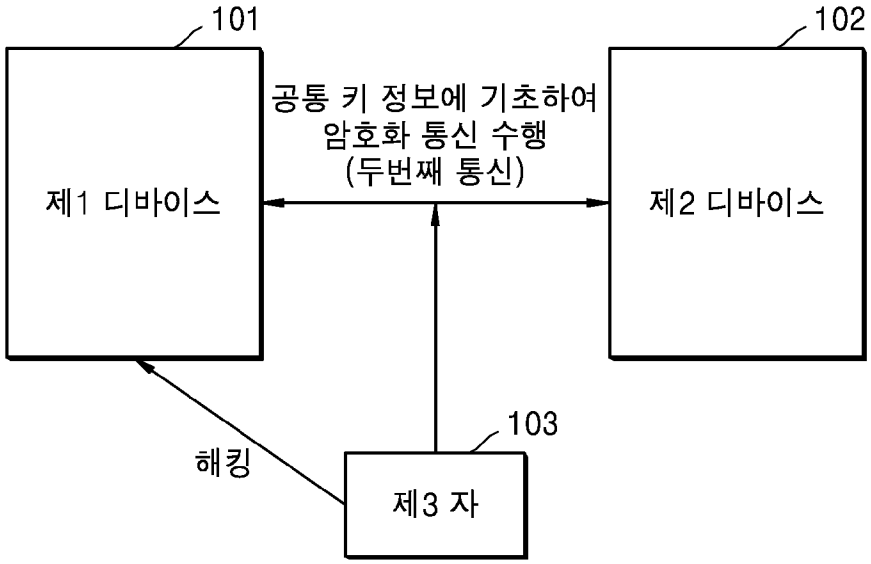
[Fig. 19]


시작
제1 디바이스와 키를 공유
S1910
제1 디바이스로부터 암호화된 데이터, 적어도 하나의
암호화된 암호화키, 메시지 인증 코드 (Message
Authentication Code)를 포함하는 데이터 세트를 수신
S1920
적어도 하나의 암호화된 암호화키를 이용하여
적어도 하나의 암호화키를 획득
S1930
적어도 하나의 암호화키 중 올바른 암호화키를
MAC을 이용하여 판단
S1940
선택한 암호화키를 이용하여 암호화된 데이터를 복호화
S1950
종료

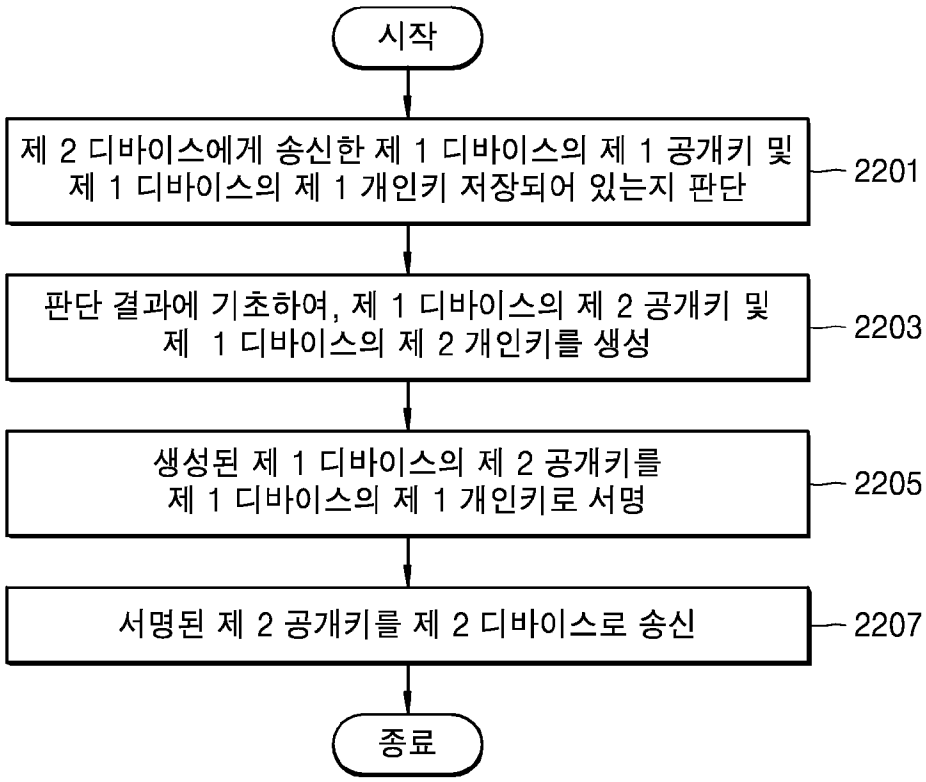
[Fig. 20]



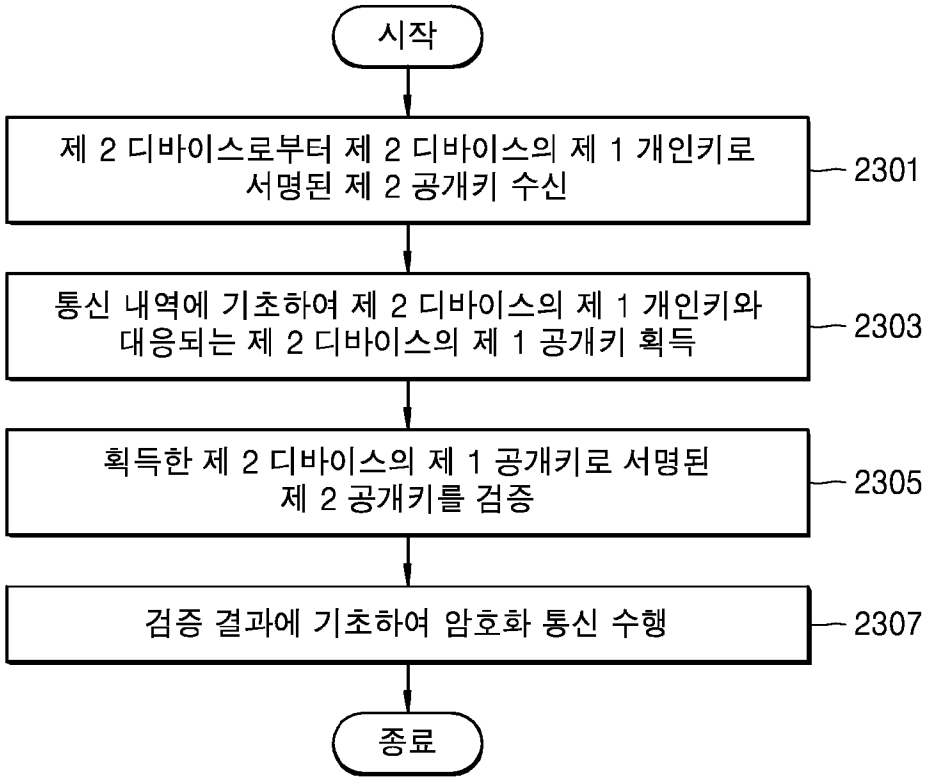
[Fig. 21]



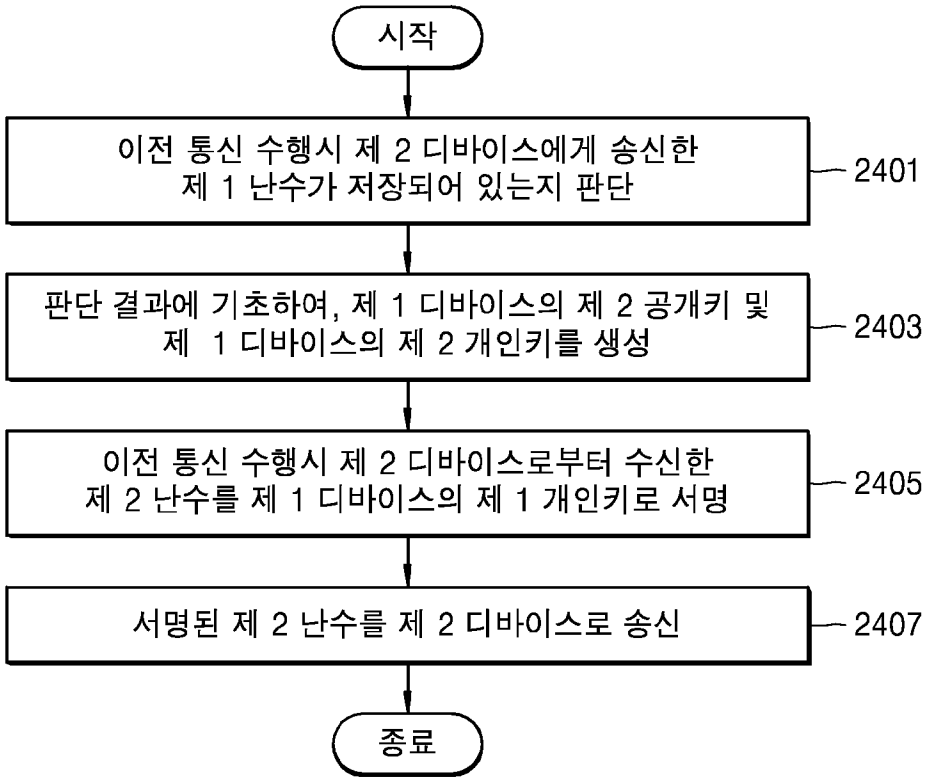
[Fig. 22]



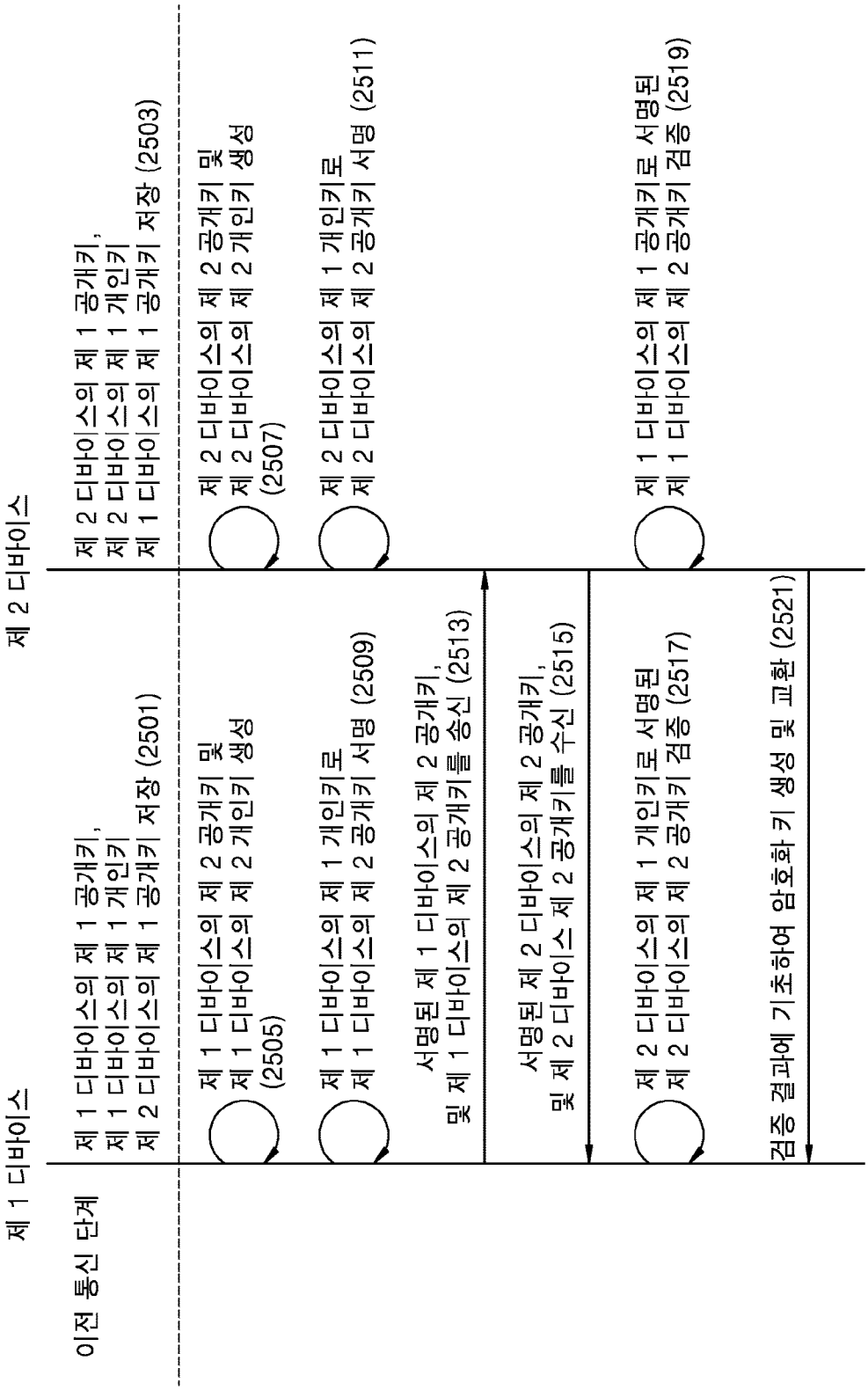
[Fig. 23]


시작
제 2 디바이스로부터 제 2 디바이스의 제 1 개인키로 서명된 제 2 공개키 수신
2301
통신 내역에 기초하여 제 2 디바이스의 제 1 개인키와 대응되는 제 2 디바이스의 제 1 공개키 획득
2303
획득한 제 2 디바이스의 제 1 공개키로 서명된 제 2 공개키를 검증
2305
검증 결과에 기초하여 암호화 통신 수행
2307
종료

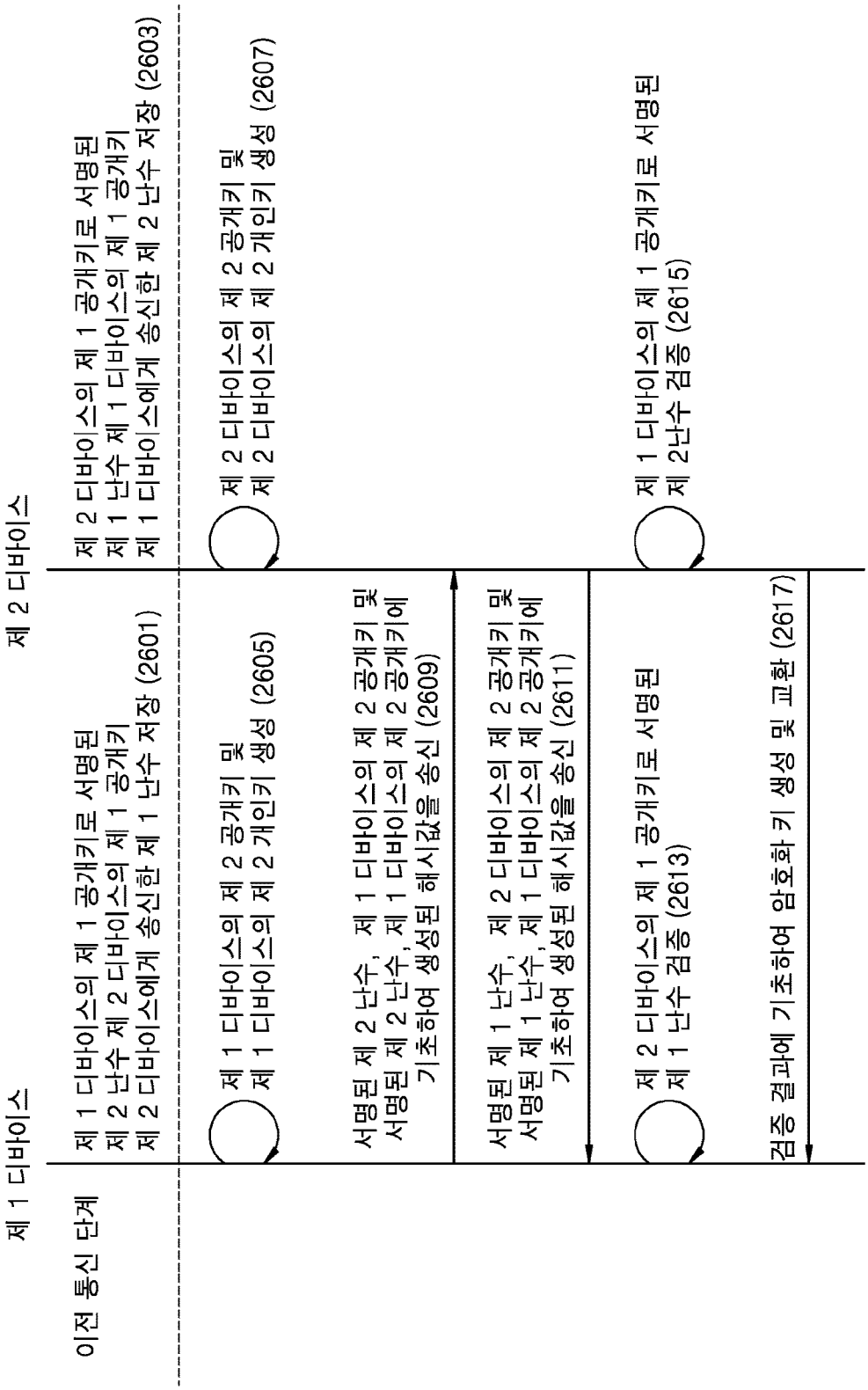
[Fig. 24]


시작
이전 통신 수행시 제 2 디바이스에게 송신한 제 1 난수가 저장되어 있는지 판단
2401
판단 결과에 기초하여, 제 1 디바이스의 제 2 공개키 및 제 1 디바이스의 제 2 개인키를 생성
2403
이전 통신 수행시 제 2 디바이스로부터 수신한 제 2 난수를 제 1 디바이스의 제 1 개인키로 서명
2405
서명된 제 2 난수를 제 2 디바이스로 송신
2407
종료

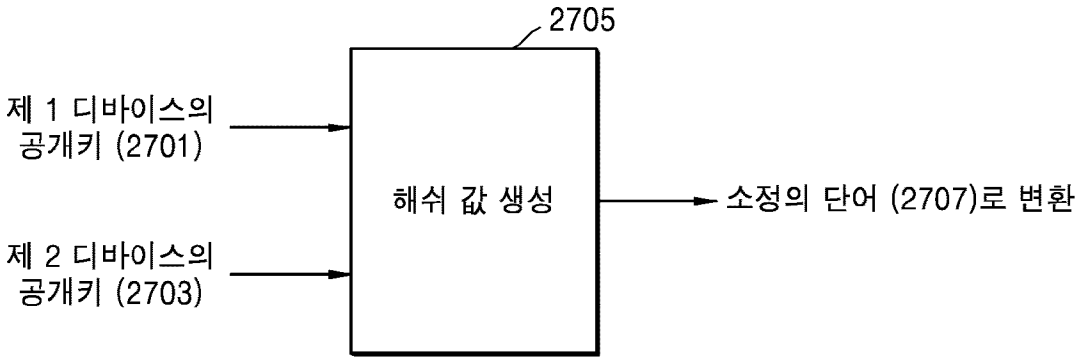
[Fig. 25]


제 1 디바이스
제 2 디바이스
이전 통신 단계
제 1 디바이스의 제 1 공개키,
제 1 디바이스의 제 1 개인키
제 2 디바이스의 제 1 공개키 저장 (2501)
제 2 디바이스의 제 1 공개키 저장 (2503)
제 1 디바이스의 제 2 공개키 및
제 1 디바이스의 제 2 개인키 생성
(2505)
제 2 디바이스의 제 2 공개키 및
제 2 디바이스의 제 2 개인키 생성
(2507)
제 1 디바이스의 제 1 개인키로
제 1 디바이스의 제 2 공개키 서명 (2509)
제 2 디바이스의 제 1 개인키로
제 2 디바이스의 제 2 공개키 서명 (2511)
서명된 제 1 디바이스의 제 2 공개키,
및 제 1 디바이스의 제 2 공개키를 송신 (2513)
서명된 제 2 디바이스의 제 2 공개키,
및 제 2 디바이스 제 2 공개키를 수신 (2515)
제 2 디바이스의 제 1 개인키로 서명된
제 2 디바이스의 제 2 공개키 검증 (2517)
제 1 디바이스의 제 1 공개키로 서명된
제 1 디바이스의 제 2 공개키 검증 (2519)
검증 결과에 기초하여 암호화 키 생성 및 교환 (2521)

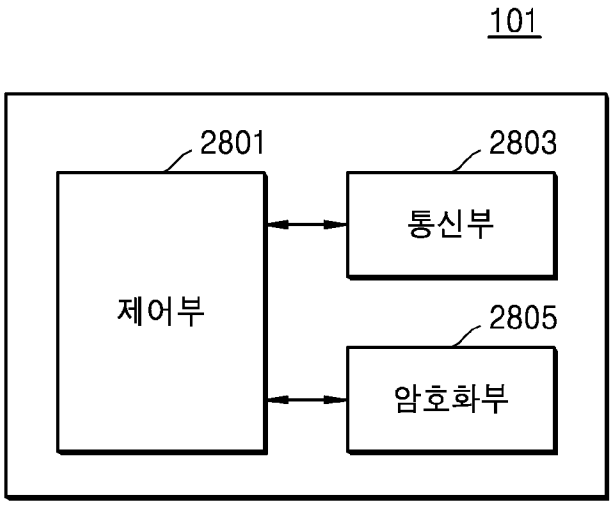
[Fig. 26]


제 1 디바이스
제 2 디바이스
이전 통신 단계
제 1 디바이스의 제 1 공개키로 서명된
제 2 난수 제 2 디바이스의 제 1 공개키
제 2 디바이스에게 송신한 제 1 난수 저장 (2601)
제 2 디바이스의 제 1 공개키로 서명된
제 1 난수 제 1 디바이스의 제 1 공개키
제 1 디바이스에게 송신한 제 2 난수 저장 (2603)
제 1 디바이스의 제 2 공개키 및
제 1 디바이스의 제 2 개인키 생성 (2605)
제 2 디바이스의 제 2 공개키 및
제 2 디바이스의 제 2 개인키 생성 (2607)
서명된 제 2 난수, 제 1 디바이스의 제 2 공개키 및
서명된 제 2 난수, 제 1 디바이스의 제 2 공개키에
기초하여 생성된 해시값을 송신 (2609)
서명된 제 1 난수, 제 2 디바이스의 제 2 공개키 및
서명된 제 1 난수, 제 1 디바이스의 제 2 공개키에
기초하여 생성된 해시값을 송신 (2611)
제 2 디바이스의 제 1 공개키로 서명된
제 1 난수 검증 (2613)
제 1 디바이스의 제 1 공개키로 서명된
제 2난수 검증 (2615)
검증 결과에 기초하여 암호화 키 생성 및 교환 (2617)

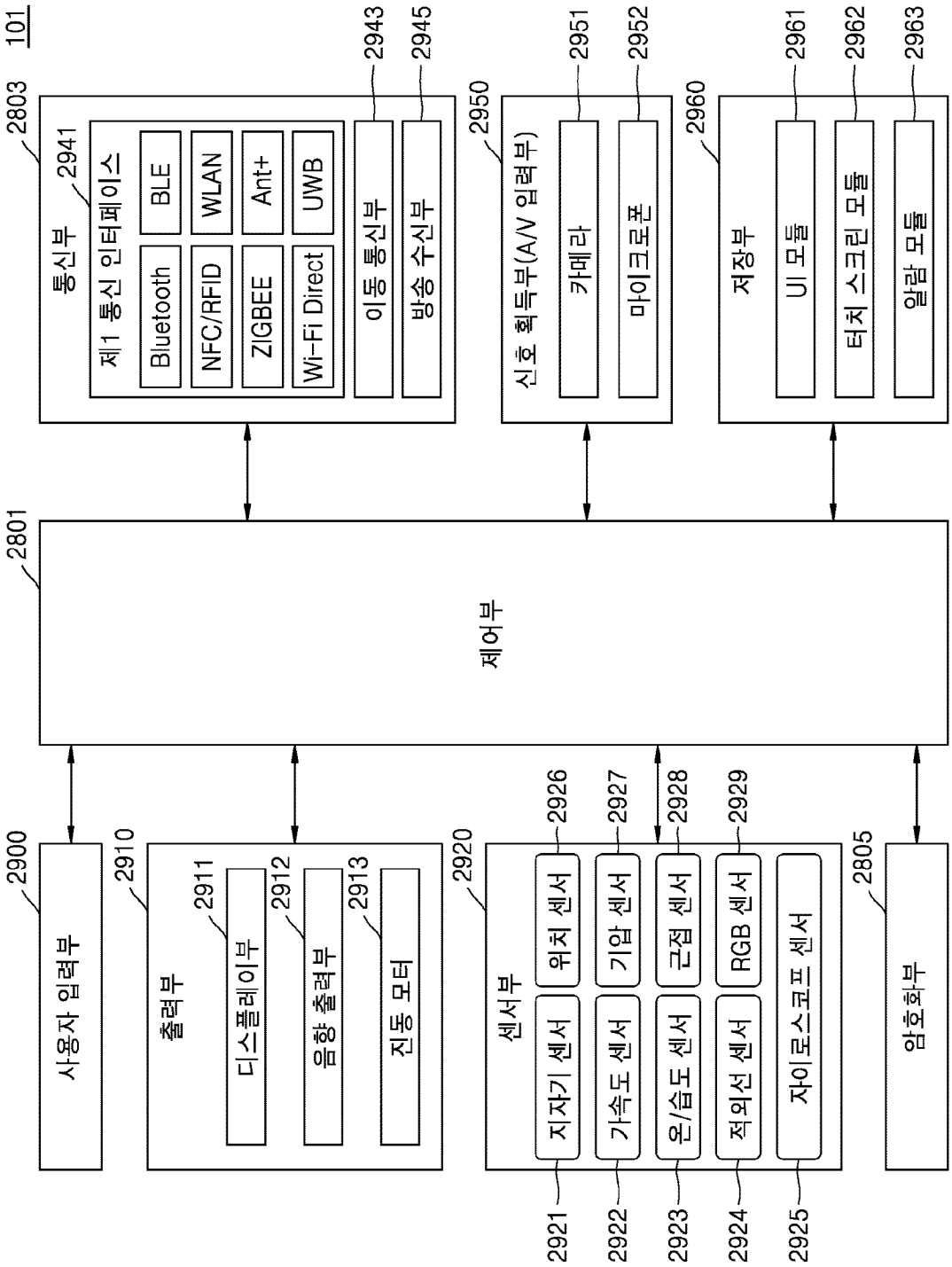
[Fig. 27]


2705
제 1 디바이스의
공개키 (2701)
제 2 디바이스의
공개키 (2703)
해쉬 값 생성
소정의 단어 (2707)로 변환

[Fig. 28]


101
2801
2803
통신부
제어부
2805
암호화부

[Fig. 29]


101
2803
통신부
2941
제1 통신 인터페이스
Bluetooth
BLE
NFC/RFID
WLAN
ZIGBEE
Ant+
Wi-Fi Direct
UWB
2943
이동 통신부
2945
방송 수신부
2950
신호 획득부(A/V 입력부)
2951
카메라
2952
마이크로폰
2960
저장부
2961
UI 모듈
2962
터치 스크린 모듈
2963
알람 모듈
2801
제어부
2900
사용자 입력부
2910
출력부
2911
디스플레이부
2912
음향 출력부
2913
진동 모터
2920
센서부
2926
위치 센서
2927
기압 센서
2928
근접 센서
2929
RGB 센서
지자기 센서
가속도 센서
온/습도 센서
적외선 센서
자이로스코프 센서
2805
암호화부
2921
2922
2923
2924
2925