(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년06월04일
(11) 등록번호 10-2118956
(24) 등록일자 2020년05월29일

(51) 국제특허분류(Int. Cl.)
G06F 21/44 (2013.01) *G06F 21/33* (2013.01)
H04L 9/30 (2006.01)
(52) CPC특허분류
G06F 21/44 (2013.01)
G06F 21/33 (2013.01)
(21) 출원번호 10-2019-0106668
(22) 출원일자 2019년08월29일
심사청구일자 2019년08월29일
(56) 선행기술조사문헌
KR101800737 B1*
KR1020190063193 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
부산대학교 산학협력단
부산광역시 금정구 부산대학로63번길 2 (장전동, 부산대학교)
(72) 발명자
신지선
서울특별시 광진구 능동로 209, 광개토관 823호
남일구
서울특별시 송파구 올림픽로 435 파크리오아파트 311동 2001호
(74) 대리인
두호특허법인

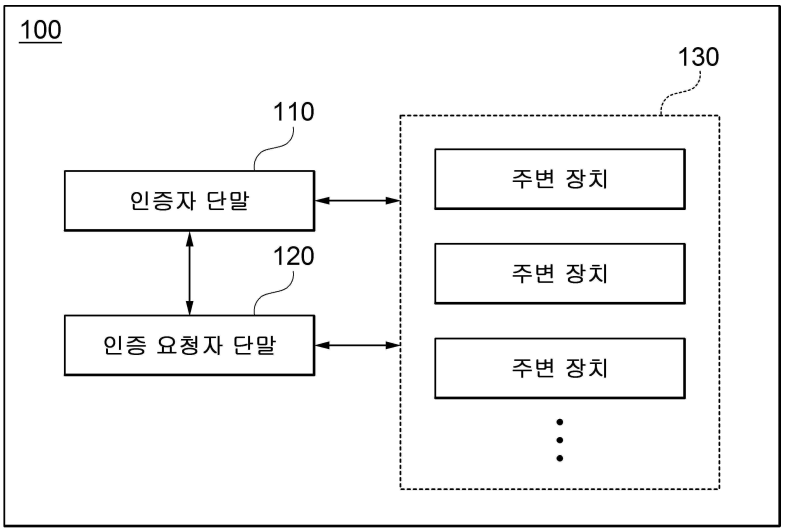
전체 청구항 수 : 총 15 항 심사관 : 문남두

(54) 발명의 명칭 **인증 시스템 및 방법**

(57) 요 약

인증 시스템 및 방법이 개시된다. 개시되는 일 실시예에 따른 인증 시스템은 하나 이상의 주변 장치 각각에 인증을 위한 비밀키를 발급하는 인증 요청자 단말 및 상기 인증 요청자 단말로부터 인증 요청을 수신하는 경우, 상기 하나 이상의 주변 장치로 상기 인증 요청자 단말에 대한 인증 확인 요청을 송신하고, 상기 하나 이상의 주변 장치로부터 수신하는 인증 확인 응답을 검증함으로써 상기 인증 요청자 단말을 인증하는 인증자 단말을 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/30 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711075702
부처명 과학기술정보통신부
연구관리전문기관 정보통신기획평가원
연구사업명 대학ICT연구센터지원사업
연구과제명 지능형 비행로봇 융합기술 연구
기 여 율 60/100
주관기관 세종대학교 산학협력단
연구기간 2018.06.01 ~ 2021.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711070434
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 대학ICT연구센터육성지원사업
연구과제명 자가충전형 초소형 전국단위 위치추적 시스템 원천기술 개발
기 여 율 40/100
주관기관 울산과학기술원
연구기간 2017.06.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

하나 이상의 주변 장치 각각에 인증을 위한 비밀키를 발급하는 인증 요청자 단말; 및

상기 인증 요청자 단말로부터 인증 요청을 수신하는 경우, 상기 하나 이상의 주변 장치로 상기 인증 요청자 단말에 대한 인증 확인 요청을 송신하고, 상기 하나 이상의 주변 장치로부터 수신하는 인증 확인 응답을 검증함으로써 상기 인증 요청자 단말을 인증하는 인증자 단말을 포함하며,

상기 주변 장치는, 상기 비밀키를 이용하여 상기 인증 확인 요청으로부터 상기 인증 확인 응답을 생성하고,

상기 인증 요청자 단말은, 상기 하나 이상의 주변 장치 각각으로부터 수신하는 식별 정보를 자신의 마스터 비밀키로 서명함으로써 상기 하나 이상의 주변 장치별 상기 비밀키를 생성하는, 인증 시스템.

청구항 2

삭제

청구항 3

청구항 1에 있어서,

상기 인증 확인 요청을 수신한 특정 주변 장치는, 상기 인증 확인 요청에 포함된 식별 정보 및 난수를 자신의 상기 비밀키로 서명하여 상기 인증 확인 응답을 생성하는, 인증 시스템.

청구항 4

청구항 3에 있어서,

상기 인증 확인 응답을 수신한 인증자 단말은, 기 저장된 마스터 공개키 및 상기 식별 정보를 이용하여 상기 인증 확인 응답이 상기 특정 주변 장치로부터 송신된 것인지를 검증하는, 인증 시스템.

청구항 5

청구항 1에 있어서,

상기 인증 확인 요청은, 상기 하나 이상의 주변 장치 각각으로부터 수신하는 식별 정보에 기초하여 생성된 제1 키를 은닉화(encapsulation)한 제2 키인, 인증 시스템.

청구항 6

청구항 5에 있어서,

상기 인증 확인 요청을 수신한 특정 주변 장치는, 기 저장된 마스터 공개키, 상기 식별 정보 및 자신의 상기 비밀키를 이용하여 상기 제2 키로부터 제3 키를 복원하고, 상기 제3 키에 기초하여 상기 인증 확인 응답을 생성하는, 인증 시스템.

청구항 7

청구항 6에 있어서,

상기 인증 확인 응답을 수신한 인증자 단말은, 상기 제1 키에 기초하여 계산된 결과 값과 상기 인증 확인 응답이 일치하는지 검증하여 상기 인증 요청자 단말을 인증하는, 인증 시스템.

청구항 8

청구항 1에 있어서,

상기 인증자 단말은, n(이때, n은 1 이상의 자연수)개 이상의 상기 주변 장치의 식별 정보를 상기 인증 요청자 단말로부터 수신하여 상기 인증 확인 요청을 송신하고,

상기 인증 확인 요청을 송신한 주변 장치로부터 수신한 인증 확인 응답 중 k(이때, $1 \leq k \leq n$)개 이상에 대한 검증에 성공하는 경우, 상기 인증 요청자 단말이 인증된 것으로 판단하는, 인증 시스템.

청구항 9

인증 요청자 단말이 하나 이상의 주변 장치 각각에 인증을 위한 비밀키를 발급하는 단계;

상기 인증 요청자 단말로부터 인증 요청을 수신하는 경우, 인증자 단말이 상기 하나 이상의 주변 장치로 상기 인증 요청자 단말에 대한 인증 확인 요청을 송신하는 단계; 및

상기 인증자 단말이 상기 하나 이상의 주변 장치로부터 수신하는 인증 확인 응답을 검증함으로써 상기 인증 요청자 단말을 인증하는 단계를 포함하며,

상기 주변 장치는, 상기 비밀키를 이용하여 상기 인증 확인 요청으로부터 상기 인증 확인 응답을 생성하고,

상기 인증 요청자 단말은, 상기 하나 이상의 주변 장치 각각으로부터 수신하는 식별 정보를 자신의 마스터 비밀키로 서명함으로써 상기 하나 이상의 주변 장치 별 상기 비밀키를 생성하는, 인증 방법.

청구항 10

삭제

청구항 11

청구항 9에 있어서,

상기 인증 확인 요청을 수신한 특정 주변 장치는, 상기 인증 확인 요청에 포함된 식별 정보 및 난수를 자신의 상기 비밀키로 서명하여 상기 인증 확인 응답을 생성하는, 인증 방법.

청구항 12

청구항 11에 있어서,

상기 인증 확인 응답을 수신한 인증자 단말은, 기 저장된 마스터 공개키 및 상기 식별 정보를 이용하여 상기 인증 확인 응답이 상기 특정 주변 장치로부터 송신된 것인지를 검증하는, 인증 방법.

청구항 13

청구항 9에 있어서,

상기 인증 확인 요청은, 상기 하나 이상의 주변 장치 각각으로부터 수신하는 식별 정보에 기초하여 생성된 제1 키를 은닉화(encapsulation)한 제2 키인, 인증 방법.

청구항 14

청구항 13에 있어서,

상기 인증 확인 요청을 수신한 특정 주변 장치는, 기 저장된 마스터 공개키, 상기 식별 정보 및 자신의 상기 비밀키를 이용하여 상기 제2 키로부터 제3 키를 복원하고, 상기 제3 키에 기초하여 상기 인증 확인 응답을 생성하는, 인증 방법.

청구항 15

청구항 14에 있어서,

상기 인증 확인 응답을 수신한 인증자 단말은, 상기 제1 키에 기초하여 계산된 결과 값과 상기 인증 확인 응답이 일치하는지 검증하여 상기 인증 요청자 단말을 인증하는, 인증 방법.

청구항 16

청구항 9에 있어서,

상기 인증자 단말은, n(이때, n은 1 이상의 자연수)개 이상의 상기 주변 장치의 식별 정보를 상기 인증 요청자 단말로부터 수신하여 상기 인증 확인 요청을 송신하고,

상기 인증 확인 요청을 송신한 주변 장치로부터 수신한 인증 확인 응답 중 k(이때, $1 \leq k \leq n$)개 이상에 대한 검증에 성공하는 경우, 상기 인증 요청자 단말이 인증된 것으로 판단하는, 인증 방법.

청구항 17

비일시적 컴퓨터 판독 가능한 저장매체(non-transitory computer readable storage medium)에 저장된 컴퓨터 프로그램으로서,

상기 컴퓨터 프로그램은 하나 이상의 명령어들을 포함하고, 상기 명령어들은 하나 이상의 프로세서들을 갖는 컴퓨팅 장치에 의해 실행될 때, 상기 컴퓨팅 장치로 하여금,

인증 요청자 단말이 하나 이상의 주변 장치 각각에 인증을 위한 비밀키를 발급하고,

인증자 단말이 상기 인증 요청자 단말로부터 인증 요청을 수신하는 경우, 상기 하나 이상의 주변 장치로 상기 인증 요청자 단말에 대한 인증 확인 요청을 송신하고, 상기 하나 이상의 주변 장치로부터 수신하는 인증 확인 응답을 검증함으로써 상기 인증 요청자 단말을 인증하도록 하되,

상기 주변 장치는, 상기 비밀키를 이용하여 상기 인증 확인 요청으로부터 상기 인증 확인 응답을 생성하고,

상기 인증 요청자 단말은, 상기 하나 이상의 주변 장치 각각으로부터 수신하는 식별 정보를 자신의 마스터 비밀키로 서명함으로써 상기 하나 이상의 주변 장치 별 상기 비밀키를 생성하는, 비일시적 컴퓨터 판독 가능한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 개시되는 실시예들은 네트워크 상에서의 단말 장치간의 인증 기술과 관련된다.

배 경 기 술

[0002] 최근 정보 기술이 발달함에 따라, 서버(server)나 특정 디바이스(device)에 접근하는 사용자 또는 디바이스가 접근 권한이 있는지 검증할 필요성이 높아지고 있다.

[0003] 이를 위해, 서버나 특정 디바이스에 접근하는 사용자 또는 디바이스에 대해 1차적인 인증 수단을 마련하여 인증을 요하고 있으나, 인증 과정의 편의성(usability)을 잃지 않기 위해 보안성이 낮은 인증 수단을 사용하는 경우가 많다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 대한민국 공개특허공보 제10-2011-0071366호(2011.06.29.)

발명의 내용

해결하려는 과제

[0005] 개시되는 실시예들은 인증 과정의 편의성을 유지하면서, 보안성이 높은 인증 수단을 제공하기 위한 것이다.

과제의 해결 수단

[0006] 일 실시예에 따른 인증 시스템은, 하나 이상의 주변 장치 각각에 인증을 위한 비밀키를 발급하는 인증 요청자

단말 및 상기 인증 요청자 단말로부터 인증 요청을 수신하는 경우, 상기 하나 이상의 주변 장치로 상기 인증 요청자 단말에 대한 인증 확인 요청을 송신하고, 상기 하나 이상의 주변 장치로부터 수신하는 인증 확인 응답을 검증함으로써 상기 인증 요청자 단말을 인증하는 인증자 단말을 포함하며, 상기 주변 장치는, 상기 비밀키를 이용하여 상기 인증 확인 요청으로부터 상기 인증 확인 응답을 생성한다.

[0007] 상기 인증 요청자 단말은, 상기 하나 이상의 주변 장치 각각으로부터 수신하는 식별 정보를 자신의 마스터 비밀키로 서명함으로써 상기 하나 이상의 주변 장치 별 상기 비밀키를 생성할 수 있다.

[0008] 상기 인증 확인 요청을 수신한 특정 주변 장치는, 상기 인증 확인 요청에 포함된 식별 정보 및 난수를 자신의 상기 비밀키로 서명하여 상기 인증 확인 응답을 생성할 수 있다.

[0009] 상기 인증 확인 응답을 수신한 인증자 단말은, 기 저장된 마스터 공개키 및 상기 식별 정보를 이용하여 상기 인증 확인 응답이 상기 특정 주변 장치로부터 송신된 것인지를 검증할 수 있다.

[0010] 상기 인증 확인 요청은, 상기 하나 이상의 주변 장치 각각으로부터 수신하는 식별 정보에 기초하여 생성된 제1 키를 은닉화(encapsulation)한 제2 키일 수 있다.

[0011] 상기 인증 확인 요청을 수신한 특정 주변 장치는, 기 저장된 마스터 공개키, 상기 식별 정보 및 자신의 상기 비밀키를 이용하여 상기 제2 키로부터 제3 키를 복원하고, 상기 제3 키에 기초하여 상기 인증 확인 응답을 생성할 수 있다.

[0012] 상기 인증 확인 응답을 수신한 인증자 단말은, 상기 제1 키에 기초하여 계산된 결과 값과 상기 인증 확인 응답이 일치하는지 검증하여 상기 인증 요청자 단말을 인증할 수 있다.

[0013] 상기 인증자 단말은, n(이때, n은 1 이상의 자연수)개 이상의 상기 주변 장치의 식별 정보를 상기 인증 요청자 단말로부터 수신하여 상기 인증 확인 요청을 송신하고, 상기 인증 확인 요청을 송신한 주변 장치로부터 수신한 인증 확인 응답 중 k(이때, $1 \leq k \leq n$)개 이상에 대한 검증에 성공하는 경우, 상기 인증 요청자 단말이 인증된 것으로 판단할 수 있다.

[0014] 일 실시예에 따른 인증 방법은, 인증 요청자 단말이 하나 이상의 주변 장치 각각에 인증을 위한 비밀키를 발급하는 단계, 상기 인증 요청자 단말로부터 인증 요청을 수신하는 경우, 인증자 단말이 상기 하나 이상의 주변 장치로 상기 인증 요청자 단말에 대한 인증 확인 요청을 송신하는 단계 및 상기 인증자 단말이 상기 하나 이상의 주변 장치로부터 수신하는 인증 확인 응답을 검증함으로써 상기 인증 요청자 단말을 인증하는 단계를 포함하며, 상기 주변 장치는, 상기 비밀키를 이용하여 상기 인증 확인 요청으로부터 상기 인증 확인 응답을 생성한다.

[0015] 상기 인증 요청자 단말은, 상기 하나 이상의 주변 장치 각각으로부터 수신하는 식별 정보를 자신의 마스터 비밀키로 서명함으로써 상기 하나 이상의 주변 장치 별 상기 비밀키를 생성할 수 있다.

[0016] 상기 인증 확인 요청을 수신한 특정 주변 장치는, 상기 인증 확인 요청에 포함된 식별 정보 및 난수를 자신의 상기 비밀키로 서명하여 상기 인증 확인 응답을 생성할 수 있다.

[0017] 상기 인증 확인 응답을 수신한 인증자 단말은, 기 저장된 마스터 공개키 및 상기 식별 정보를 이용하여 상기 인증 확인 응답이 상기 특정 주변 장치로부터 송신된 것인지를 검증할 수 있다.

[0018] 상기 인증 확인 요청은, 상기 하나 이상의 주변 장치 각각으로부터 수신하는 식별 정보에 기초하여 생성된 제1 키를 은닉화(encapsulation)한 제2 키일 수 있다.

[0019] 상기 인증 확인 요청을 수신한 특정 주변 장치는, 기 저장된 마스터 공개키, 상기 식별 정보 및 자신의 상기 비밀키를 이용하여 상기 제2 키로부터 제3 키를 복원하고, 상기 제3 키에 기초하여 상기 인증 확인 응답을 생성할 수 있다.

[0020] 상기 인증 확인 응답을 수신한 인증자 단말은, 상기 제1 키에 기초하여 계산된 결과 값과 상기 인증 확인 응답이 일치하는지 검증하여 상기 인증 요청자 단말을 인증할 수 있다.

[0021] 상기 인증자 단말은, n(이때, n은 1 이상의 자연수)개 이상의 상기 주변 장치의 식별 정보를 상기 인증 요청자 단말로부터 수신하여 상기 인증 확인 요청을 송신하고, 상기 인증 확인 요청을 송신한 주변 장치로부터 수신한 인증 확인 응답 중 k(이때, $1 \leq k \leq n$)개 이상에 대한 검증에 성공하는 경우, 상기 인증 요청자 단말이 인증된 것으로 판단할 수 있다.

발명의 효과

[0022] 개시되는 실시예들에 따르면, 하나 이상의 주변 장치를 통해 인증 요청자 단말을 복합적으로 인증함으로써, 사용자에게 편의성을 제공하면서도 다양한 인증 수단을 통한 인증의 보안성을 제고할 수 있다.

[0023] 또한 개시되는 실시예들에 따르면, 다양한 주변 기기와 신호를 주고 받을 수 있는 사물인터넷(IoT) 기기에 쉽게 적용됨으로써, 향후 다양한 분야의 기기 인증을 위해 사용될 수 있다.

도면의 간단한 설명

[0024] 도 1은 일 실시예에 따른 인증 시스템을 설명하기 위한 블록도

도 2는 일 실시예에 따른 인증 방법의 설정(setup) 단계를 설명하기 위한 순서도

도 3은 일 실시예에 따른 인증 방법의 인증(authentication) 단계를 설명하기 위한 순서도

도 4는 다른 실시예에 따른 인증 방법의 인증 단계를 설명하기 위한 순서도

도 5는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0025] 이하, 도면을 참조하여 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 개시되는 실시예들은 이에 제한되지 않는다.

[0026] 실시예들을 설명함에 있어서, 관련된 공지기술에 대한 구체적인 설명이 개시되는 실시예들의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 개시되는 실시예들에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0027] 한편, 개시되는 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램, 및 상기 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나, 또는 컴퓨터 소프트웨어 분야에서 통상적으로 사용 가능한 것일 수 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 프로그램의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0028] 본 발명의 실시예들에서 사용되는 알고리즘은 다음과 같다.

[0029] 먼저, 아이디 기반의 암호화 알고리즘은 다음과 같이 구성된다.

[0030] ① setup(1^k): 보안 파라미터 k($k \in N$)를 입력받고, 이로부터 마스터 공개키(mpk) 및 마스터 비밀키(msk)를 생성한다.

[0031] ② extract(mpk, msk, ID): ID를 입력받는 경우 그에 해당하는 비밀키 d를 생성한다. 이때 사용자의 ID는 공개키, d는 비밀키가 된다.

[0032] 두번째로, 전자 서명(digital signature) 알고리즘은 다음과 같이 구성된다.

[0033] ① sign(d, m): 비밀키 d와 메시지 m을 입력 받아 서명 sig를 생성한다.

[0034] ② verify(mpk, ID, m, sig): 공개키 ID, 메시지 m, 서명 sig를 입력으로 받아 sig이 올바른 서명이면 1을, 아니면 0을 출력한다.

[0035] 세번째로, 키 은닉 메커니즘(Key Encapsulation Mechanism, KEM)은 다음과 같이 구성된다.

[0036] ① encap(mpk, ID): 공개키 ID를 입력 받아 (k, c)를 생성한다. 이때, k는와 k를 키이며 c는 k를 은닉화(캡슐화)한 값을 나타낸다.

[0037] ② decap(mpk, ID, d, c): 공개키 ID 및 은닉화된 키 c를 입력 받아 복원에 성공하면 k를, 실패하면 모순(⊥)을 출력한다.

[0038] 도 1은 일 실시예에 따른 인증 시스템(100)의 블록도이다.

[0039] 도 1을 참조하면, 일 실시예에 따른 인증 시스템(100)은 인증자 단말(110), 인증 요청자 단말(120) 및 주변 장치(130)를 포함한다.

[0040] 인증자 단말(110)은 인증을 요청하는 인증 요청자 단말(120)에 기 약속된 권한이 있는지 검증하는 기기(device)이다. 또한, 인증 요청자 단말(120)은 인증자 단말(110)에 접근하여 사용하려는 기기이다. 아울러, 주변 장치(130)는 인증자 단말(110)의 주변 또는 인증 요청자 단말(120)의 주변에 존재하는 하나 이상의 기기이다.

[0041] 개시되는 인증 과정에 있어서, 인증자 단말(110)은 인증 요청자 단말(120)로부터 인증 요청을 수신하고, 하나 이상의 주변 장치(130)로 위 인증 요청자 단말(120)에 대한 인증 확인 요청을 송신할 수 있다. 이때 인증 확인 요청을 수신한 주변 장치(130)와 인증자 단말(110) 간의 인증은 다양한 방법을 통해 수행될 수 있다. 예를 들어, 위 인증은 전자 서명(digital signature) 알고리즘 또는 키 은닉 메커니즘(key encapsulation mechanism, KEM)을 통해 이루어질 수 있다.

[0042] KEM은 비대칭(공개키) 알고리즘을 사용한 전송에 있어서 대칭 암호화 키 자료를 보호하기 위해 고안된 암호화 메커니즘이다. 즉, 인증자 단말(110)에서 생성된 특정 키를 곧바로 주변 장치(130)에서 알 수 없도록, 특정 키를 은닉한 새로운 키를 주변 장치(130)에 제공하는 메커니즘을 의미한다.

[0043] 이하에서는 위 두 가지 방법에 의해 이루어지는 인증 과정을 상세히 설명한다.

[0044] 인증자 단말(110)은 인증 요청자 단말(120)로부터 인증 요청을 수신하고, 하나 이상의 주변 장치(130)로 인증 요청자 단말(120)에 대한 인증 확인 요청을 송신한다. 이후 인증자 단말(110)은 상기 인증 확인 요청에 따라 주변 장치(130)로부터 수신하는 인증 확인 응답을 검증함으로써 인증 요청자 단말(120)을 인증한다.

[0045] 일 실시예에서, 인증자 단말(110)은, n(이때, n은 1 이상의 자연수)개 이상의 주변 장치(130)의 식별 정보를 인증 요청자 단말(120)로부터 수신하여 인증 확인 요청을 송신하고, 인증 확인 요청을 송신한 주변 장치(130)로부터 수신한 인증 확인 응답 중 k(이때, $1 \leq k \leq n$)개 이상에 대한 검증에 성공하는 경우, 인증 요청자 단말(120)이 인증된 것으로 판단할 수 있다.

[0046] 또한 일 실시예에 따르면, 인증자 단말(110)은 인증자 단말(110)로부터 기 설정된 반경 내에 존재하는 하나 이상의 주변 장치(130)를 감지하여, 감지된 주변 장치의 개수를 k로 설정할 수 있다. 예를 들어, 인증 요청자 단말(120)에 등록되어 인증자 단말(110)로 식별 정보가 송신된 주변 장치(130)의 개수가 5개인 경우, 위 5개의 주변 장치 중 인증자 단말(110)로부터 20m 반경 내에 존재하는 주변 장치가 있는지 탐색하여 해당하는 주변 장치의 개수를 인증 요청자 단말(120)의 인증에 필요한 주변 장치의 개수 k로 설정할 수 있다.

[0047] 상술한 전자 서명 알고리즘에 기반한 일 실시예에 따르면, 인증자 단말(110)이 송신하는 인증 확인 요청은 식별 정보 및 난수 이외의 다양한 요소로 구성될 수도 있다. 뿐만 아니라, 식별 정보 및 난수에 송신 시간 등의 요소가 부가된 구성일 수도 있다. 특정 주변 장치(130)에서 수신한 인증 확인 요청을 자신의 비밀키로 서명하여 인증자 단말(110)로 송신하고, 인증자 단말(110)에서 수신한 인증 확인 응답을 확인하여 올바른 서명인지 판단할 수 있는 한, 개시되는 실시예들에서 인증 확인 요청에 포함되는 요소들은 특정한 종류의 것으로 제한되지 않는다.

[0048] 또한 일 실시예에 따르면, 인증 확인 응답을 수신한 인증자 단말(110)은, 기 저장된 마스터 공개키(mpk) 및 식별 정보를 이용하여 인증 확인 응답이 특정 주변 장치(130)로부터 송신된 것인지를 검증할 수 있다.

[0049] 구체적으로, 인증자 단말(110)은 임의의 암호화 난수값(nonce)을 선택하여, 인증 확인 요청으로서 위 값을 각 주변 장치(130)의 식별 정보와 함께 주변 장치(130)에 송신할 수 있다.

[0050] 또한 일 실시예에 따르면, 인증자 단말(110)은 마스터 공개키, 식별 정보, 메시지 m 및 sig를 verify 함수의 입력으로 받아 위 sig가 식별 정보(공개키)에 대응되는 비밀키에 의해 서명된 것이 맞는지 판별하여, 맞다면 해당 비밀키를 가지고 있는 주변 장치(130)에 대해 verify 함수의 결과 값으로 1을 출력할 수 있다. 만약 서명이 올바르지 않다면, 인증자 단말(110)은 위 verify 함수의 결과 값으로 0을 출력할 수 있다.

[0051] 상술한 KEM에 기반한 일 실시예에 따르면, 인증자 단말(110)이 송신하는 인증 확인 요청은 하나 이상의 주변 장치(130) 각각으로부터 수신하는 식별 정보에 기초하여 생성된 제1 키를 은닉화(encapsulation)한 제2 키일 수 있다.

[0052] 구체적으로, 인증자 단말(110)은 마스터 공개키 및 주변 장치의 식별 정보를 encap 함수의 입력으로 받아 제1 키를 생성하고, 이 제1 키를 주변 장치(130)가 곧바로 알 수 없도록 은닉화한 제2 키를 인증 확인 요청으로서 주변 장치(130)에 송신할 수 있다.

[0053] 일 실시예에 따르면, 인증 확인 응답을 수신한 인증자 단말(110)은, 제1 키에 기초하여 계산된 결과 값과 인증 확인 응답이 일치하는지 검증하여 인증 요청자 단말을 인증할 수 있다.

[0054] 구체적으로, 인증 확인 응답을 수신한 인증자 단말(110)은, 제1 키 및 메시지 m을 MAC 알고리즘의 입력으로 하여 계산된 결과 값이 인증 확인 응답과 일치하는지 검증하여 일치하는 경우 해당 주변 장치(130)에 대해 인증 요청자 단말(120)이 인증되었다고 판단할 수 있다.

[0055] 인증 요청자 단말(120)은 하나 이상의 주변 장치 각각에 인증을 위한 비밀키를 발급한다.

[0056] 일 실시예에 따르면, 인증 요청자 단말(120)은 하나 이상의 주변 장치(130) 각각으로부터 수신하는 식별 정보를 자신의 마스터 비밀키(msk)로 서명함으로써 하나 이상의 주변 장치 별 비밀키를 생성할 수 있다.

[0057] 구체적으로, 하나 이상의 주변 장치(130)로부터 수신하는 식별 정보는 주변 장치 각각에 일 대 일로 대응되는 ID(identification)일 수 있다. 이에 따라, 인증 시스템(100)은 ID 기반의 암호 체계일 수 있으며, 이때 주변 장치(130) 각각의 ID는 주변 장치 별 비밀키(secret key)에 대응되는 공개키(public key)의 역할을 수행할 수 있다.

[0058] 이러한 ID 기반 암호 체계 하에서, 인증 요청자 단말(120)은 셋업(setup) 알고리즘을 이용하여 마스터 공개키(mpk) 및 마스터 비밀키(msk)를 생성할 수 있다. 인증 요청자 단말(120)은 마스터 공개키를 생성한 후 인증 시스템(100) 내 모든 장치, 개체 또는 구성들이 마스터 공개키를 변조 없이 보유할 수 있도록 전송할 수 있다.

[0059] 또한, 인증 요청자 단말(120)은 추출(extract) 알고리즘을 이용하여 마스터 공개키, 마스터 비밀키 및 주변 장치(130) 각각으로부터 수신하는 식별 정보를 입력으로 받아 해당 식별 정보에 대응되는 비밀키를 생성할 수 있다.

[0060] 일 실시예에 따르면, 인증 요청자 단말(120)은 인증자 단말(110)과 이격된 거리와 무관하게, 웹 페이지 또는 어플리케이션(application)을 통해 인증자 단말(110)에 인증 요청을 송신할 수 있다. 그러나 인증 요청 수단은 이에 한정되는 것이 아니며, 인증 요청은 Wi-Fi 또는 이동 통신망을 통한 신호 전달에 의해서 이루어질 수도 있다.

[0061] 예를 들어, 드론(Drone) 및 이 드론을 제어하기 위한 컨트롤러(controller) 사이에서, 컨트롤러는 드론을 제어할 권한이 있는 컨트롤러임을 인증받기 위해 드론에 기 등록된 하나 이상의 주변 장치에 대해 인증 확인 요청을 송신할 것을 요청할 수 있다. 이때, 컨트롤러의 사용자는 드론 전용 어플리케이션 또는 웹 페이지에 접속하여 컨트롤러의 인증 요청을 송신할 수 있다.

[0062] 주변 장치(130)는 비밀키를 이용하여 인증 확인 요청으로부터 인증 확인 응답을 생성한다.

[0063] 상술한 전자 서명 알고리즘에 기반한 일 실시예에 따르면, 인증 확인 요청을 수신한 특정 주변 장치(130)는, 인증 확인 요청에 포함된 식별 정보 및 난수를 자신의 비밀키로 서명하여 인증 확인 응답을 생성할 수 있다.

[0064] 일 실시예에 따르면, 인증 확인 요청을 수신한 주변 장치(130)는 위 식별 정보 및 암호화 난수값을 메시지 m으로 설정하고, 이 메시지 m을 자신의 비밀키 d를 이용하여 서명하여 sign(d, m)을 통해 서명 sig를 생성할 수 있다.

[0065] 이어서, 주변 장치(130)는 인증자 단말(110)로 위 sig를 송신할 수 있다.

[0066] 상술한 KEM에 기반한 일 실시예에 따르면, 인증 확인 요청을 수신한 특정 주변 장치(130)는, 기 저장된 마스터

공개키, 식별 정보 및 자신의 비밀키를 이용하여 제2 키로부터 제3 키를 복원하고, 제3 키에 기초하여 인증 확인 응답을 생성할 수 있다.

[0067] 구체적으로, 인증 확인 요청을 수신한 특정 주변 장치(130)는, 마스터 공개키, 식별 정보, 자신의 비밀키 및 수신한 인증 확인 요청을 decap 함수의 입력으로 받아 제2 키(인증 확인 요청)에 대응되는 제3 키를 복원할 수 있다. 이때, 해당 주변 장치(130)가 인증자 단말(110)에 기 등록된 올바른 주변 장치(130)인 경우 제3 키와 제1 키는 동일할 수 있다.

[0068] 이어서, 주변 장치(130)는 식별 정보 및 제2 키를 메시지 m으로 설정하고, 이 m과 제3 키를 메시지 인증 코드(message authentication code, MAC) 알고리즘의 입력으로 하여 인증 확인 응답을 생성할 수 있다. MAC는 메시지의 인증에 사용되는 작은 크기의 정보를 의미하며, MAC 알고리즘은 비밀키를 입력 받고, 임의의 길이의 메시지를 인증하는 알고리즘을 의미한다.

[0069] 이때, 메시지 m은 주변 장치(130)와 인증자 단말(110) 간에 인증 요청자 단말(120)의 인증을 위해 사용될 수 있다면, 식별 정보 및 제2 키 외에도 임의의 요소로 구성될 수 있다. 예를 들어, 메시지 m은 식별 정보 및 제2 키에 임의의 암호화 임시 값이 부가된 형태일 수 있다. 아울러, MAC 알고리즘은 인증 확인 응답의 데이터 무결성(data integrity)을 보증하기 위하여 사용되는 것으로, 인증 확인 응답의 데이터 무결성을 보증할 수 있다면 주변 장치(130)는 MAC 알고리즘 대신 hash function 또는 고급 암호화 표준(Advanced Encryption Standard, AES)을 이용하여 인증 확인 응답을 생성할 수도 있다. 이하의 m 및 MAC 알고리즘을 이용하는 실시예에서도 상술한 사항은 마찬가지로 적용될 수 있다.

[0070] 도 2는 일 실시예에 따른 인증 방법의 설정(setup) 단계를 설명하기 위한 순서도이다.

[0071] 도 2에 도시된 방법은 예를 들어, 상술한 인증 시스템(100)에 의해 수행될 수 있다. 아래의 실시예에서, 도 1을 참조하여 상술한 인증 시스템(100)의 상세한 실시예들과 중복되는 내용은 생략하기로 한다. 도시된 순서도에서는 상술한 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다. 이는 이하 도 3 및 도 4에서도 마찬가지이다.

[0072] 도 2를 참조하면, 인증 요청자 단말(120)은 하나 이상의 주변 장치(130) 각각에 인증을 위한 비밀키를 발급한다(S112).

[0073] 일 실시예에 따르면, 인증 요청자 단말(120)은 셋업(setup) 알고리즘을 이용하여 마스터 공개키(mpk) 및 마스터 비밀키(msk)를 생성할 수 있다(S102).

[0074] 또한 일 실시예에 따르면, 인증 요청자 단말(120)은 마스터 공개키를 생성한 후 인증 시스템(100) 내 모든 장치, 개체 또는 구성들이 마스터 공개키를 변조 없이 보유할 수 있도록 전송할 수 있다. 예를 들어, 인증 요청자 단말(120)은 인증자 단말(110) 및 하나 이상의 주변 장치(130)에 마스터 공개키를 송신할 수 있다(S104, S106).

[0075] 뿐만 아니라, 인증 요청자 단말(120)은 추출(extract) 알고리즘을 이용하여 마스터 공개키, 마스터 비밀키 및 주변 장치(130) 각각으로부터 수신하는 식별 정보(예를 들어, ID)를 입력으로 받아(S108) 해당 식별 정보에 대응되는 비밀키를 생성할 수 있다(S110).

[0076] 아울러, 인증 요청자 단말(120)은, 하나 이상의 주변 장치(130)의 식별 정보를 인증자 단말(110)로 송신할 수 있고, 인증자 단말(110)과의 사이에서 주변 장치(130) 전체 개수 n(이때, n은 1 이상의 자연수) 및 인증 요청자 단말(120) 인증 시 필요한 주변 장치(130)의 최소 개수 k(이때, $1 \leq k \leq n$)를 설정할 수 있다(S116).

[0077] 도 3은 일 실시예에 따른 인증 방법의 인증(authentication) 단계를 설명하기 위한 순서도이다. 도 3에서 개시하는 인증 단계는 전자 서명 알고리즘에 기반한 일 실시예에 따른 인증 단계이다.

[0078] 도 3을 참조하면, 우선, 인증자 단말(110)은 인증 요청자 단말(120)로부터 인증 요청을 수신하는 경우(S202), 하나 이상의 주변 장치(130)로 인증 요청자 단말(120)에 대한 인증 확인 요청을 송신한다(S206).

[0079] 이때 일 실시예에 따르면, 인증자 단말(110)은 임의의 암호화 난수값(nonce)을 선택하여(S204), 인증 확인 요청으로서 위 값을 각 주변 장치(130)의 식별 정보와 함께 주변 장치(130)에 송신할 수 있다(S206). 이 경우, 인증 확인 요청을 수신하는 주변 장치(130)들은 인증자 단말(110)에 식별 정보(예를 들어, ID)가 등록된 주변 장치(130)를 의미할 수 있다.

[0080] 이후, 인증 확인 요청을 수신한 주변 장치(130)는, 비밀키를 이용하여 인증 확인 요청으로부터 인증 확인 응답을 생성한다(S212).

[0081] 구체적으로, 인증 확인 요청을 수신한 주변 장치(130)는, 위 식별 정보 및 암호화 난수값을 메시지 m으로 설정하고(S208), 이 메시지 m을 자신의 비밀키 d를 이용하여 서명하여(S210) sign(d, m) (이하, sig)을 생성할 수 있다(S212).

[0082] 이후, 인증자 단말(110)은 주변 장치(130)로부터 위 sig를 수신한다(S214).

[0083] 이후, 인증자 단말(110)은 하나 이상의 주변 장치(130)로부터 수신하는 인증 확인 응답(S214)을 검증함으로써 인증 요청자 단말(120)을 인증한다(S216).

[0084] 구체적으로, 인증자 단말(110)은 마스터 공개키, 식별 정보, 메시지 m 및 sig를 verify 함수의 입력으로 받아 위 sig가 식별 정보(공개키)에 대응되는 비밀키에 의해 서명된 것이 맞는지 판별하여, 맞다면 해당 비밀키를 가지고 있는 주변 장치(130)에 대해 verify 함수의 결과 값으로 1을 출력할 수 있다. 만약 서명이 올바르지 않다면, 인증자 단말(110)은 위 verify 함수의 결과 값으로 0을 출력할 수 있다.

[0085] 도 4는 다른 실시예에 따른 인증 방법의 인증 단계를 설명하기 위한 순서도이다.

[0086] 도 4를 참조하면, 인증자 단말(110)이 인증 요청자 단말(120)로부터 인증 요청을 수신하는 경우(S302), 하나 이상의 주변 장치(130)로 인증 요청자 단말(120)에 대한 인증 확인 요청을 송신하고(S306), 인증 확인 요청을 수신한 주변 장치(130)가 비밀키를 이용하여 인증 확인 요청으로부터 인증 확인 응답을 생성하며(S312), 이후 인증자 단말(110)에서 하나 이상의 주변 장치(130)로부터 수신하는 인증 확인 응답(S314)을 검증함으로써 인증 요청자 단말(120)을 인증하는(S316) 것은 도 3에서 상술한 바와 동일하다.

[0087] 그러나, 도 4에서 개시하는 인증 단계는 KEM에 기반한 일 실시예에 따른 인증 단계이다.

[0088] 일 실시예에 따르면, 인증 요청자 단말(120)로부터 인증 요청을 수신(S302) 이후, 인증자 단말(110)은 마스터 공개키 및 주변 장치의 식별 정보를 encap 함수의 입력으로 받아 제1 키를 생성하고, 이 제1 키를 주변 장치(130)가 곧바로 알 수 없도록 은닉화한 제2 키를 인증 확인 요청으로서 주변 장치(130)에 송신한다(S304, S306).

[0089] 이후, 인증 확인 요청을 수신한 특정 주변 장치(130)는, 마스터 공개키, 식별 정보, 자신의 비밀키 및 수신한 인증 확인 요청을 decap 함수의 입력으로 받아 제2 키(인증 확인 요청)에 대응되는 제3 키를 복원한다(S308). 이때, 해당 주변 장치(130)가 인증자 단말(110)에 기 등록된 올바른 주변 장치(130)인 경우 제3 키와 제1 키는 동일할 수 있다.

[0090] 이후, 주변 장치(130)는 식별 정보 및 제2 키를 메시지 m으로 설정하고(S310), 이 m과 제3 키를 메시지 인증 코드(message authentication code, MAC) 알고리즘의 입력으로 하여 인증 확인 응답을 생성한다(S312).

[0091] 이후, 인증 확인 응답을 수신한 인증자 단말(110)은, 제1 키 및 메시지 m을 MAC 알고리즘의 입력으로 하여 계산된 결과 값이 인증 확인 응답과 일치하는지 검증하여 일치하는 경우 해당 주변 장치(130)에 대해 인증 요청자 단말(120)이 인증되었다고 판단할 수 있다(S314, S316).

[0092] 도 5는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0093] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 인증 시스템일 수 있다.

[0094] 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0095] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다

른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0096] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0097] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(102)와 연결될 수도 있다.

[0098] 이상에서 ID 기반의 암호 체계 하에서의 인증 시스템(100) 및 인증 방법에 대해 설명하였으나, 암호 체계의 종류는 인증 서비스 제공자의 편의에 따라 취사 선택할 수 있는 사항이며, 블루투스(Bluetooth) 기반 암호 체계에도 상술한 인증 시스템(100) 및 인증 방법을 적용 가능하다. 이 경우, 일 실시예에 따른 인증 방법의 설정 단계는 페어링(pairing) 단계로, 일 실시예에 따른 인증 방법의 인증 단계는 연결(connection) 단계로 명명될 수 있다.

[0099] 상술한 대로, ID 기반의 암호 체계 및 블루투스 기반 암호 체계에서 두루 사용할 수 있는 인증 시스템(100) 및 인증 방법을 제시함으로써, 다양한 주변 기기와 신호를 주고 받을 수 있는 사물인터넷(IoT) 기기에 쉽게 될 수 있다.

[0100] 이상에서 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 청구범위뿐만 아니라 이 청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0101] 10: 컴퓨팅 환경

12: 컴퓨팅 장치

14: 프로세서

16: 컴퓨터 판독 가능 저장 매체

18: 통신 버스

20: 프로그램

22: 입출력 인터페이스

24: 입출력 장치

26: 네트워크 통신 인터페이스

100: 인증 시스템

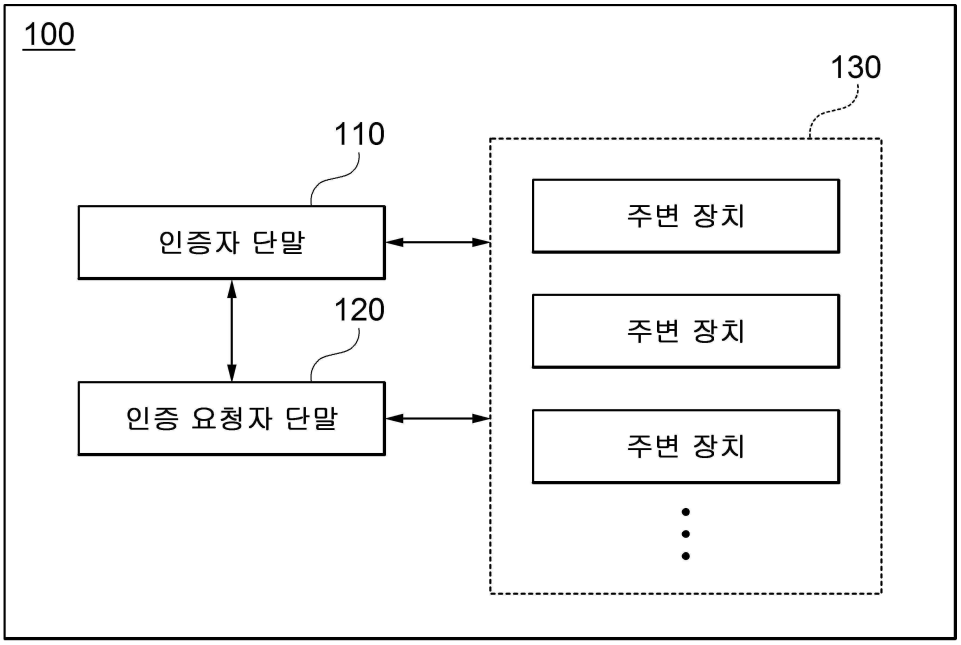
110: 인증자 단말

120: 인증 요청자 단말

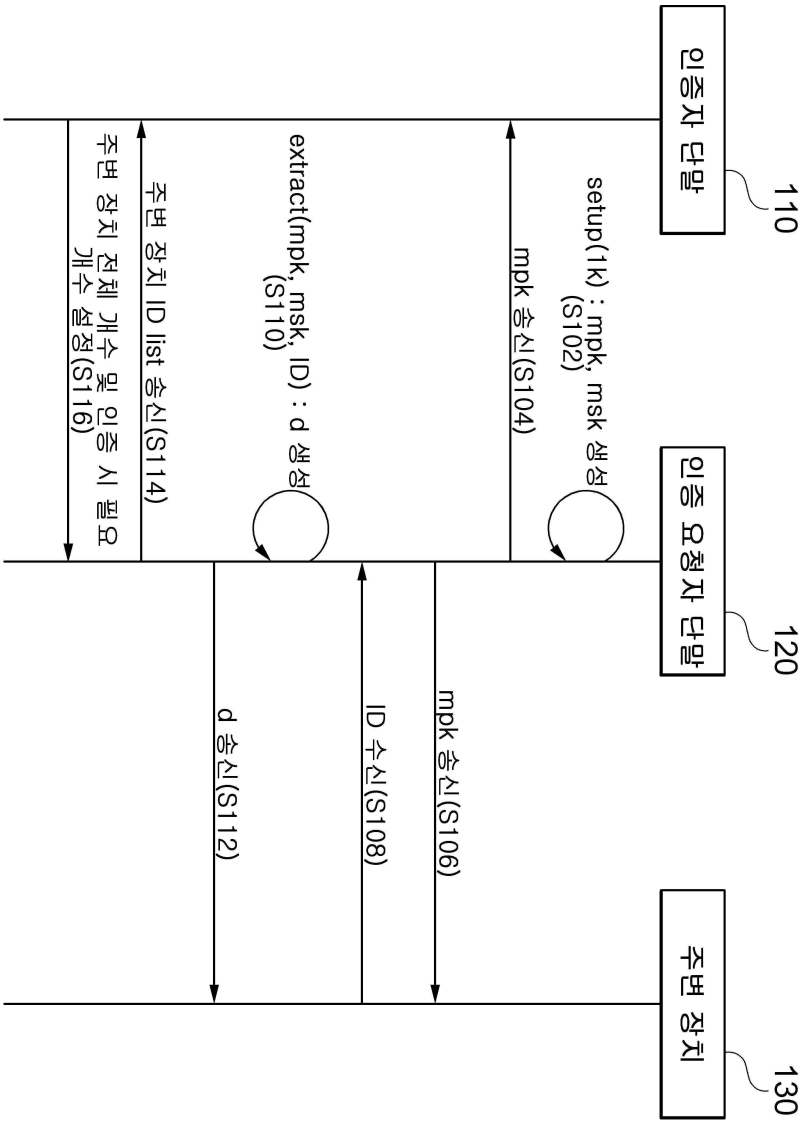
130: 주변 장치

도면

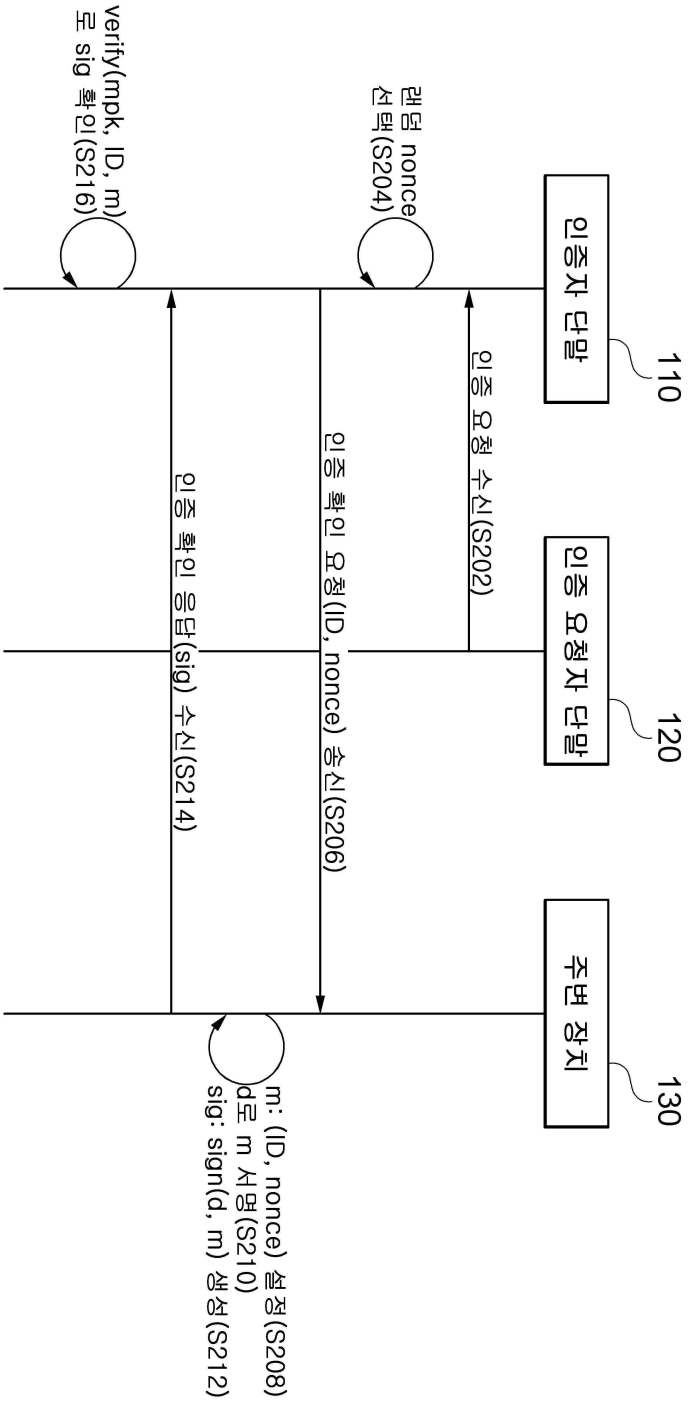
도면1



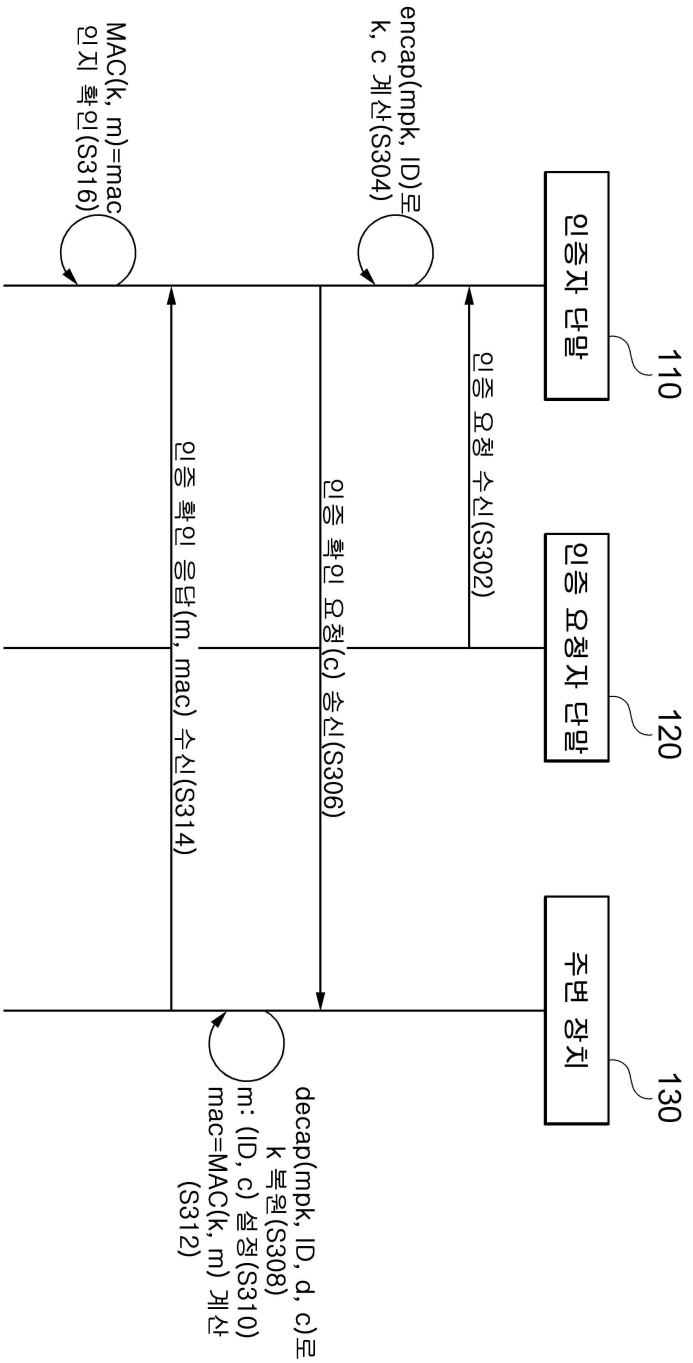
도면2


인증자 단말
110
setup(1k) : mpk, msk 생성
(S102)
mpk 송신(S104)
extract(mpk, msk, ID) : d 생성
(S110)
주변 장치 ID list 송신(S114)
주변 장치 전체 개수 및 인증 시 필요
개수 설정(S116)
인증 요청자 단말
120
mpk 송신(S106)
ID 수신(S108)
d 송신(S112)
주변 장치
130

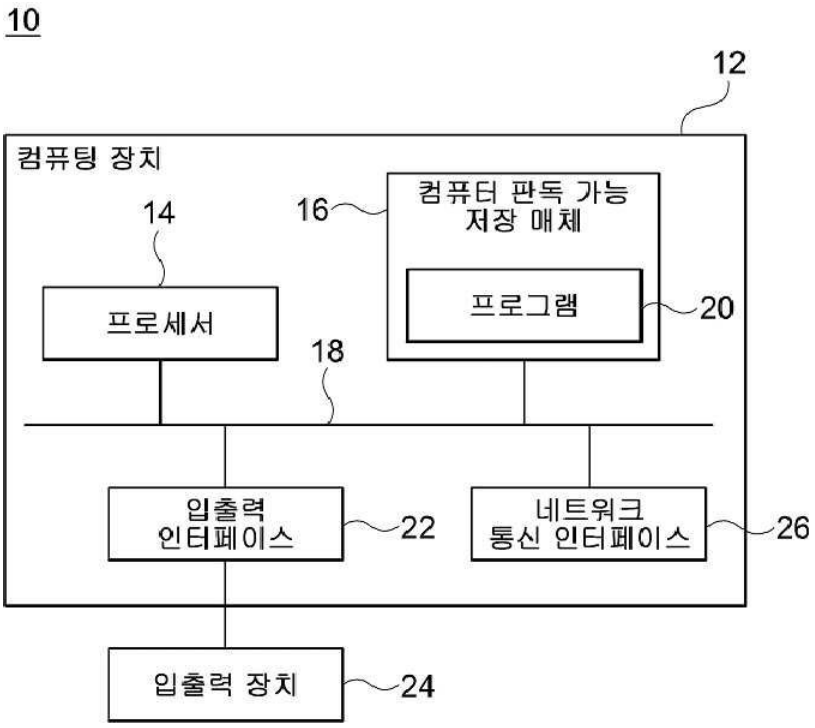
도면3


인증자 단말
110
인증 요청자 단말
120
주변 장치
130
랜덤 nonce 선택(S204)
인증 요청 수신(S202)
인증 확인 요청(ID, nonce) 송신(S206)
m: (ID, nonce) 설정(S208)
d로 m 서명(S210)
sig: sign(d, m) 생성(S212)
인증 확인 응답(sig) 수신(S214)
verify(mpk, ID, m)로 sig 확인(S216)

도면4


인증자 단말
110
인증 요청자 단말
120
주변 장치
130
encap(mpk, ID)로 k, c 계산(S304)
인증 요청 수신(S302)
인증 확인 요청(c) 송신(S306)
인증 확인 응답(m, mac) 수신(S314)
MAC(k, m)=mac 인지 확인(S316)
decap(mpk, ID, d, c)로 k 복원(S308)
m: (ID, c) 설정(S310)
mac=MAC(k, m) 계산 (S312)

도면5


10
12
컴퓨팅 장치
14
프로세서
16
컴퓨터 판독 가능
저장 매체
프로그램
20
18
입출력
인터페이스
22
네트워크
통신 인터페이스
26
입출력 장치
24