(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년10월01일
(11) 등록번호 10-2005946
(24) 등록일자 2019년07월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2006.01) *H04L 9/06* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/008 (2013.01)
H04L 9/0662 (2013.01)
(21) 출원번호 10-2018-0138600
(22) 출원일자 2018년11월13일
심사청구일자 2018년11월13일
(56) 선행기술조사문헌
KR101045804 B1*
KR101832861 B1*
F. Armknecht 외 6명, A Guide to Fully Homomorphic Encryption, Cryptology ePrint Archive, Report: 2015/192 (2015.)*
KR101472507 B1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
신지선
서울특별시 송파구 올림픽로 435, 311동 2001호 (신천동, 파크리오)
(74) 대리인
두호특허법인

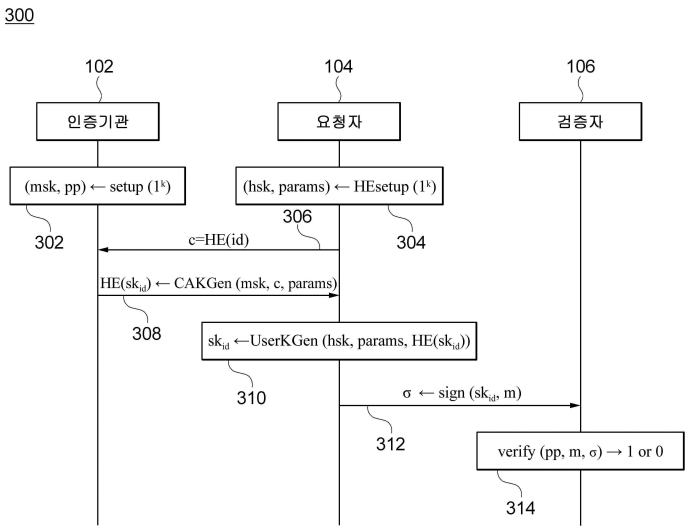
전체 청구항 수 : 총 8 항 심사관 : 양종필

(54) 발명의 명칭 **동형암호를 이용한 익명 아이디 기반 서명 시스템 및 방법**

(57) 요 약

동형암호를 이용한 익명 아이디 기반 서명 시스템 및 방법이 개시된다. 일 실시예에 따른 방법은, 인증 요청자 단말에서, 상기 인증 요청자 단말의 대칭형 동형암호 비밀키(hsk)를 이용하여, 상기 인증 요청자 단말의 아이디(id)에 대응되는 제1 동형 암호문(c=HE(id))을 생성하는 단계; 인증 기관 서버에서, 상기 인증 요청자 단말로부터 수신되는 상기 제1 동형 암호문(c)을 이용하여, 상기 아이디(id)에 대응되는 비밀키(sk_{id})에 대한 제2 동형 암호문($C=HE(sk_{id})$)을 생성하는 단계; 및 상기 인증 요청자 단말에서, 상기 제2 동형 암호문(C)을 수신하고, 수신된 상기 제2 동형 암호문(C)으로부터 상기 비밀키(sk_{id})를 획득하는 단계를 포함한다.

대 표 도



(52) CPC특허분류
H04L 9/321 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711075702
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신기술인력양성(정보화)
연구과제명 지능형 비행로봇 융합기술 연구
기 여 율 1/1
주관기관 세종대학교 산학협력단
연구기간 2018.06.01 ~ 2019.02.28

명 세 서

청구범위

청구항 1

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 단말 장치에서 수행되는 방법으로서,

인증 요청자 단말에서, 상기 인증 요청자 단말의 대칭형 동형암호 비밀키(hsk)를 이용하여, 상기 인증 요청자 단말의 아이디(id)에 대응되는 제1 동형 암호문(c=HE(id))을 생성하는 단계;

인증 기관 서버에서, 상기 인증 요청자 단말로부터 수신되는 상기 제1 동형 암호문(c)을 이용하여, 상기 아이디(id)에 대응되는 비밀키(sk_{id})에 대한 제2 동형 암호문($C=HE(sk_{id})$)을 생성하는 단계; 및

상기 인증 요청자 단말에서, 상기 제2 동형 암호문(C)을 수신하고, 수신된 상기 제2 동형 암호문(C)으로부터 상기 비밀키(sk_{id})를 획득하는 단계를 포함하며,

상기 제1 동형 암호문(c)을 생성하는 단계는,

상기 비밀키 생성을 위한 랜덤값(random)을 생성하는 단계; 및

상기 대칭형 동형암호 비밀키(hsk)를 이용하여, 생성된 상기 랜덤값(random)에 대응되는 제3 동형 암호문(HE(random))을 생성하는 단계를 더 포함하는, 방법.

청구항 2

청구항 1에 있어서,

상기 아이디(id)는, 상기 인증 요청자 단말이 생성한 가상 아이디(pseudonym)인, 방법.

청구항 3

청구항 1에 있어서,

상기 제2 동형 암호문을 생성하는 단계는, 대칭형 동형암호의 eval 알고리즘을 이용하여 상기 제1 동형 암호문(c)으로부터 상기 제2 동형 암호문(C)을 생성하는, 방법.

청구항 4

삭제

청구항 5

청구항 1에 있어서,

상기 제2 동형 암호문(C)을 생성하는 단계는, 상기 인증 요청자 단말로부터 수신되는 상기 제3 동형 암호문을 추가적으로 고려하여 상기 제2 동형 암호문($C=HE(sk_{id})$)을 생성하도록 구성되는, 방법.

청구항 6

자신의 대칭형 동형암호 비밀키(hsk)를 이용하여, 인증 요청자 단말의 아이디(id)에 대응되는 제1 동형 암호문

(c=HE(id))을 생성하는 인증 요청자 단말; 및

상기 인증 요청자 단말로부터 수신되는 상기 제1 동형 암호문(c)을 이용하여, 상기 아이디(id)에 대응되는 비밀키(sk_{id})에 대한 제2 동형 암호문(C=HE(sk_{id}))을 생성하는 인증 기관 서버를 포함하며,

상기 인증 요청자 단말은, 상기 비밀키 생성을 위한 랜덤값(random)을 생성하고, 상기 대칭형 동형암호 비밀키(hsk)를 이용하여 생성된 상기 랜덤값(random)에 대응되는 제3 동형 암호문(HE(random))을 생성하며, 상기 인증 기관 서버로부터 상기 제2 동형 암호문(C)을 수신하고, 수신된 상기 제2 동형 암호문(C)으로부터 상기 비밀키(sk_{id})를 획득하는, 아이디 기반 서명 시스템.

청구항 7

청구항 6에 있어서,

상기 아이디(id)는, 상기 인증 요청자 단말이 생성한 가상 아이디 (pseudonym)인, 아이디 기반 서명 시스템.

청구항 8

청구항 6에 있어서,

상기 인증 기관 서버는,

대칭형 동형암호의 eval 알고리즘을 이용하여 상기 제1 동형 암호문(c)으로부터 상기 제2 동형 암호문(C)을 생성하는, 아이디 기반 서명 시스템.

청구항 9

삭제

청구항 10

청구항 6에 있어서,

상기 인증 기관 서버는,

상기 인증 요청자 단말로부터 수신되는 상기 제3 동형 암호문을 추가적으로 고려하여 상기 제2 동형 암호문(C=HE(sk_{id}))을 생성하는, 아이디 기반 서명 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 아이디 기반의 서명 기술과 관련된다.

배 경 기 술

[0003] 아이디 기반 서명(IDentity Based Signature)란 공개 키 서명 방식의 일종으로 사용자의 정보(Identity)를 공개키로 사용한다. 이때 공개키로 사용할 수 있는 정보는 사용자의 이메일 주소나 전화번호 등 그 사용자에게만 해당하는 유일한 정보여야 한다. 공개 키 암호 방식의 장점은 이전에 서로 만나서 키를 나누어가지지 않은 사용자라도 안전하게 통신할 수 있다는 점이다. 다만, 이때 상대방이 공개 키가 정말로 그 사용자의 공개 열쇠인지 확인할 수 있는 방법이 반드시 필요하다. 아이디 기반 서명 기법은 상대방의 신원을 공개키로 사용하므로 이런 과정이 불필요하다는 장점이 있다.

[0004] 아이디 기반 서명 기법에서는 사용자의 아이디에 해당하는 비밀키를 부여하는 비밀키 생성자(key generator)가

필요하며, 일반적으로 신뢰할 수 있는 인증 기관(CA; Certified Authority)가 이를 수행한다. 그러나 이 과정에서 인증 기관은 각 사용자의 아이디 및 비밀키 정보를 모두 알게 되므로, 기존의 공개키 방식의 암호 시스템과 비교하여 비밀 정보가 중앙에 집중되는 문제가 발생한다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 등록특허공보 제10-1865703호 (2018. 06. 01)

발명의 내용

해결하려는 과제

[0007] 개시되는 실시예들은 대칭형 동형암호 기술을 응용하여 사용자의 아이디 정보 및 비밀키 정보를 인증 기관 등의 비밀키 생성자로부터 보호하기 위한 기술적인 수단을 제공하기 위한 것이다.

과제의 해결 수단

[0009] 예시적인 실시예에 따르면, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 단말 장치에서 수행되는 방법으로서, 인증 요청자 단말에서, 상기 인증 요청자 단말의 대칭형 동형암호 비밀키(hsk)를 이용하여, 상기 인증 요청자 단말의 아이디(id)에 대응되는 제1 동형 암호문(c=HE(id))을 생성하는 단계; 인증 기관 서버에서, 상기 인증 요청자 단말로부터 수신되는 상기 제1 동형 암호문(c)을 이용하여, 상기 아이디(id)에 대응되는 비밀키(sk_{id})에 대한 제2 동형 암호문(C=HE(sk_{id}))을 생성하는 단계; 및 상기 인증 요청자 단말에서, 상기 제2 동형 암호문(C)을 수신하고, 수신된 상기 제2 동형 암호문(C)으로부터 상기 비밀키(sk_{id})를 획득하는 단계를 포함하는, 방법이 제공된다.

[0010] 상기 아이디(id)는, 상기 인증 요청자 단말이 임의로 생성한 가상 아이디(pseudonym)일 수 있다.

[0011] 상기 제2 동형 암호문을 생성하는 단계는, 대칭형 동형암호의 eval 알고리즘을 이용하여 상기 제1 동형 암호문(c)으로부터 상기 제2 동형 암호문(C)을 생성하도록 구성될 수 있다.

[0012] 상기 제1 동형 암호문(c)을 생성하는 단계는, 상기 비밀키 생성을 위한 랜덤값(random)을 생성하는 단계; 및 상기 대칭형 동형암호 비밀키(hsk)를 이용하여, 생성된 상기 랜덤값(random)에 대응되는 제3 동형 암호문(HE(random))을 생성하는 단계를 더 포함할 수 있다.

[0013] 상기 제2 동형 암호문(C)을 생성하는 단계는, 상기 인증 요청자 단말로부터 수신되는 상기 제3 동형 암호문을 추가적으로 고려하여 상기 제2 동형 암호문(C=HE(sk_{id}))을 생성하도록 구성될 수 있다.

[0014] 다른 예시적인 실시예에 따르면, 자신의 대칭형 동형암호 비밀키(hsk)를 이용하여, 상기 인증 요청자 단말의 아이디(id)에 대응되는 제1 동형 암호문(c=HE(id))을 생성하는 인증 요청자 단말; 및 상기 인증 요청자 단말로부터 수신되는 상기 제1 동형 암호문(c)을 이용하여, 상기 아이디(id)에 대응되는 비밀키(sk_{id})에 대한 제2 동형 암호문(C=HE(sk_{id}))을 생성하는 인증 기관 서버를 포함하며, 상기 인증 요청자 단말은, 상기 인증 기관 서버로부터 상기 제2 동형 암호문(C)을 수신하고, 수신된 상기 제2 동형 암호문(C)으로부터 상기 비밀키(sk_{id})를 획득하는, 아이디 기반 서명 시스템이 제공된다.

[0015] 상기 아이디(id)는, 상기 인증 요청자 단말이 임의로 생성한 가상 아이디(pseudonym)일 수 있다.

[0016] 상기 인증 기관 서버는, 대칭형 동형암호의 eval 알고리즘을 이용하여 상기 제1 동형 암호문(c)으로부터 상기 제2 동형 암호문(C)을 생성할 수 있다.

[0017] 상기 인증 요청자 단말은, 상기 비밀키 생성을 위한 랜덤값(random)을 생성하고, 상기 대칭형 동형암호 비밀키(hsk)를 이용하여 생성된 상기 랜덤값(random)에 대응되는 제3 동형 암호문(HE(random))을 생성할 수 있다.

[0018] 상기 인증 기관 서버는, 상기 인증 요청자 단말로부터 수신되는 상기 제3 동형 암호문을 추가적으로 고려하여

상기 제2 동형 암호문($C=HE(sk_{id})$)을 생성할 수 있다.

발명의 효과

[0020] 개시되는 실시예들에 따르면, 아이디 기반의 서명을 위한 키 발급 과정에서 인증 기관 등의 키 생성자에게 아이디 및 이에 대응되는 비밀키가 노출되는 것을 방지할 수 있어 아이디 기반 서명의 보안성을 한층 더 높일 수 있다.

도면의 간단한 설명

[0022] 도 1은 일 실시예에 따른 아이디 기반 서명 시스템을 설명하기 위한 블록도

도 2는 일반적인 아이디 기반 서명 방법을 설명하기 위한 흐름도

도 3은 일 실시예에 따른 아이디 기반 서명 방법을 설명하기 위한 흐름도

도 6은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0023] 이하, 도면을 참조하여 본 발명의 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 본 발명은 이에 제한되지 않는다.

[0024] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 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 본 발명의 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.

[0026] 도 1은 일 실시예에 따른 아이디 기반 서명 시스템(100)을 설명하기 위한 블록도이다. 도시된 바와 같이, 일 실시예에 따른 아이디 기반 서명 시스템(100)은 인증 기관(Certified Authority)(102), 인증 요청자(104) 및 검증자(106)를 포함한다.

[0027] 인증 기관(102)은 요청자(104)의 아이디(id)를 수신하고, 이로부터 비밀키(sk_{id})를 생성하는 키 생성(key generation) 서버이다. 상기 아이디는 요청자(104)의 이메일 주소 또는 전화번호 등 그 사용자에게만 해당하는 유일한 정보이다.

[0028] 요청자(104)는 인증 기관(102)으로부터 수신되는 비밀키(sk_{id})를 이용하여 메시지(m)에 대한 서명값(σ)을 생성하는 단말이다. 이후 요청자(104)는 상기 서명값(σ)을 검증자(106)에게 송신하여 인증을 요청한다.

[0029] 마지막으로, 검증자(106)는 요청자(104)로부터 수신된 서명값(σ)을 검증함으로써 요청자(104)에 대한 인증을 수행하는 단말이다.

[0031] 도 2는 일반적인 아이디 기반 서명 방법(200)을 설명하기 위한 흐름도이다. 아이디 기반 서명은 setup, keygen, sign, verify를 포함하는 네 개의 알고리즘으로 구성된다.

[0032] 단계 202에서, 인증 기관(102)은 setup 알고리즘을 이용하여 시큐리티 파라미터 k로부터 마스터 비밀키(msk) 및 이에 대응되는 공개키(pp)를 생성한다. 이를 수식으로 나타내면 다음과 같다.

[0033] $(msk, pp) \leftarrow setup\ (1^k)$

[0034] 단계 204에서, 요청자(104)는 자신의 아이디(id)를 인증 기관으로 송신한다.

[0035] 단계 206에서, 인증 기관(102)은 요청자(104)의 아이디(id)로부터 이에 대응되는 비밀키(sk_{id})를 생성한다. 구체적으로 인증 기관(102)은 아이디(id)와 마스터 비밀키(msk)를 keygen 알고리즘에 입력하여 id에 대응되는 비밀키를 생성한다. 이를 수식으로 나타내면 다음과 같다.

[0036] $sk_{id} \leftarrow keygen\ (msk,\ id)$

[0037] 단계 208에서, 요청자(104)는 인증 기관(102)으로부터 발급받은 비밀키(sk_{id}) 및 sign 알고리즘을 이용하여 메시지(m)를 서명하여 서명값(σ)을 생성한다. 이를 수식으로 나타내면 다음과 같다.

[0038] $\sigma \leftarrow sign\ (sk_{id},\ m)$

[0039] 단계 210에서, 검증자(106)는 요청자(104)로부터 수신되는 서명값(σ)을 검증한다. 구체적으로 검증자(106)는 인증 기관(102)의 공개키(pp), 원본 메시지(m) 및 서명값(σ) verify 알고리즘에 입력하여 검증 결과를 출하게 된다. 예를 들어 검증자(106)는 서명이 유효한 경우 1, 그렇지 않은 경우 0을 검증 결과로서 반환할 수 있다. 이를 수식으로 나타내면 다음과 같다.

[0040] $verify\ (pp,\ m,\ \sigma) \rightarrow 1\ or\ 0$

[0042] 상기 흐름도에서 알 수 있는 바와 같이, 아이디 기반 서명 방법은 인증 기관(102)을 통하여 아이디에 대응되는 비밀키를 생성하는 과정을 수반한다. 이 과정에서 인증 기관(102)은 아이디 기반 서명을 이용하는 모든 사용자의 아이디 및 이에 대응되는 비밀키 쌍에 대한 정보를 알 수 있게 되는 바, 민감한 개인정보가 중앙의 인증 기관(102)에 집중되는 문제가 발생한다. 이를 해결하기 위하여 본 발명의 실시예에서는 대칭형 동형암호 기법을 사용한다.

[0043] 대칭형 동형암호(Homomorphic Encryption, HE)는 KGen, Enc, Dec, Eval을 포함하는 네 개의 알고리즘을 포함한다.

[0044] KGen 알고리즘은 시큐리티 파라미터 k를 받아서 비밀키(sk)와 퍼블릭 파라미터(params)를 생성하기 위한 알고리즘이다. 이 중 비밀키(sk)는 송신자(Encryptor)와 수신자(Decryptor)가 비밀로 공유하여 보관하고, 퍼블릭 파라미터(params)는 공개된다. 이를 수식으로 나타내면 다음과 같다.

[0045] $(sk,\ params) \leftarrow KGen\ (1^k)$

[0046] Enc(sk, m) 알고리즘은 송신자(Encryptor)가 실행하는 알고리즘으로, 비밀키(나)와 암호화하려는 메시지(m)을 입력받고, m에 대한 암호문(c)를 출력한다.

[0047] Dec(sk, c) 알고리즘은 수신자(Decryptor)가 실행하는 알고리즘으로, 비밀키(나)와 암호문(c)을 입력받아 복호화된 평문 메시지(m)을 출력한다.

[0048] Eval(f, params, c_1, ..., c_n): f라는 함수를 암호문 c_1, ..., c_n에 적용하여 암호문 C를 아웃풋한다. 만약, c_1, ..., c_n이 m_1, ..., m_n의 암호문이라고 가정할 때, C는 $f(m_1, ..., m_n)$의 암호문이 된다.

[0050] 도 3은 일 실시예에 따른 아이디 기반 서명 방법(300)을 설명하기 위한 흐름도이다. 도시된 흐름도는 전술한, 인증 기관(Certified Authority)(102), 인증 요청자(104) 및 검증자(106)에 의하여 수행될 수 있다. 도시된 흐름도에서는 상기 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.

[0051] 도 3에 도시된 아이디 기반 서명 방법(300)은 동형암호를 이용한 익명(anonymous ID, 또는 pseudonym) 기반의 서명 방법(HE-IBS)으로서, setup, HESetup, CAKGen, UserKGen, sign, verify를 포함하는 여섯 개의 알고리즘으로 구성된다.

[0052] 단계 302에서, 인증 기관(102)은 setup 알고리즘을 이용하여 시큐리티 파라미터 k로부터 마스터 비밀키(msk) 및 이에 대응되는 공개키(pp)를 생성한다. 이를 수식으로 나타내면 다음과 같다.

[0053] $(msk,\ pp) \leftarrow setup\ (1^k)$

[0054] 단계 304에서, 요청자(104)는 HESetup 알고리즘을 이용하여 시큐리티 파라미터 k로부터 자신의 동형암호 비밀키

hsk와 공개 파라미터 params를 생성한다. 즉, 상기 HESetup 알고리즘은 대칭형 동형암호 기법의 KGen 알고리즘과 동일하다. 이를 수식으로 나타내면 다음과 같다.

[0055] $(hsk, params) \leftarrow HEsetup(1^k)$

[0056] 단계 306에서, 요청자(104)는 상기 304 단계에서 생성된 동형암호 비밀키(hsk) 및 대칭형 동형암호 기법의 Enc 알고리즘을 이용하여, 자신의 아이디(id)에 대응되는 제1 동형 암호문(c=HE(id))을 생성한다. 이를 수식으로 나타내면 다음과 같다.

[0057] $C = HE(id) \leftarrow Enc(hsk, id)$

[0058] 일 실시예에서, 요청자(104)의 아이디(id)는 이메일 주소, 또는 전화번호 등의 그 자체로 신원을 알 수 있는 정보가 아닌, 상기 인증 요청자 단말이 생성한 랜덤값인 가상 아이디(pseudonym)일 수 있다. 이에 따라 인증 기관(102)은 암호화되지 않은 아이디를 획득하더라도 해당 아이디에 대응되는 요청자(104)를 식별하는 것이 불가능하게 된다.

[0059] 단계 308에서, 인증 기관(102)은 요청자(104)로부터 수신되는 상기 제1 동형 암호문(c) 및 CAKGen 알고리즘을 이용하여, 상기 아이디(id)에 대응되는 비밀키(sk_{id})에 대한 제2 동형 암호문($C=HE(sk_{id})$)을 생성한다. 이를 수식으로 나타내면 다음과 같다.

[0060] $HE(skid) \leftarrow CAKGen(msk, c, params)$

[0061] 일 실시예에서, CAKGen 알고리즘은 대칭형 동형암호 기법의 eval 알고리즘을 이용함으로써, id에 대응되는 제1 동형 암호문(c)에서 id를 추출하지 않고도 곧바로 비밀키(sk_{id})에 대한 제2 동형 암호문($C=HE(sk_{id})$)을 생성할 수 있다. 구체적으로, eval 알고리즘에서 f를 keygen 알고리즘으로 가정하면 다음과 같은 관계가 성립한다.

[0062] $Eval(keygen(msk, HE(id)), params) = HE(sk_{id})$

[0063] 이와 같이, eval 대칭형 동형암호를 이용할 경우 인증 기관(102)에서 알 수 있는 정보는 id의 동형 암호문(HE(id)) 및 비밀키의 동형 암호문($HE(sk_{id})$) 뿐으로, 인증 기관(102)은 아이디 및 비밀키의 실제 값을 알 수 없다. 따라서 본 발명의 실시예에 따를 경우, 인증 기관(102)에 아이디 및 비밀키가 노출되는 것을 차단할 수 있다.

[0064] 단계 310에서, 요청자(104)는 상기 제2 동형 암호문(C)을 수신하고, 수신된 상기 제2 동형 암호문(C)으로부터 비밀키(sk_{id})를 획득한다. 구체적으로, 요청자(104)는 UserKGen 알고리즘을 이용하여 $HE(sk_{id})$를 복호화함으로써 sk_{id}를 얻을 수 있다. 이를 수식으로 나타내면 다음과 같다.

[0065] $Sk_{id} \leftarrow UserKGen(hsk, params, C=HE(sk_{id}))$

[0066] 단계 312에서, 요청자(104)는 310 단계에서 획득한 비밀키(sk_{id}) 및 sign 알고리즘을 이용하여 메시지(m)를 서명하여 서명값(σ)을 생성한다. 이를 수식으로 나타내면 다음과 같다.

[0067] $\sigma \leftarrow sign(sk_{id}, m)$

[0068] 단계 314에서, 검증자(106)는 요청자(104)로부터 수신되는 서명값(σ)을 검증한다. 구체적으로 검증자(106)는 인증 기관(102)의 공개키(pp), 원본 메시지(m) 및 서명값(σ) verify 알고리즘에 입력하여 검증 결과(1 또는 0)를 출하게 된다. 이를 수식으로 나타내면 다음과 같다.

[0069] $verify(pp, m, \sigma) \rightarrow 1 \text{ or } 0$

[0071] 한편, 상기 방법에 따를 경우 인증 기관(102)은 수신되는 아이디의 실제 값을 알 수 없으므로 자신이 어떤 id에 대한 비밀키를 발급하였는지 알 수 없다. 그러나 인증 기관(102)은 비밀키 생성 알고리즘(keygen)을 보유하고 있으므로, 추후에 id를 알게 될 경우 해당 id에 대응되는 비밀키를 keygen 알고리즘을 이용하여 생성할 수 있다.

[0072] 이를 보완하기 위하여, 일 실시예에서 요청자(104)는 상기 비밀키 생성을 위한 랜덤값(random)을 직접 선택하고, 선택된 랜덤값(random)에 대응되는 제3 동형 암호문(HE(random))을 생성하여 이를 인증 기관(102)으로 송신할 수 있다. 그러면 이를 수신한 인증 기관(102)은 수신된 랜덤값의 동형 암호문을 추가적으로 keygen

함수에 적용하여 비밀키(sk_{id})를 생성할 수 있다. 이를 수식으로 나타내면 다음과 같다.

[0073] $Eval(keygen(msk, HE(id), HE(random)), params) = HE(sk_{id})$

[0074] 이와 같이 요청자(104)가 직접 비밀키 생성을 위한 랜덤값을 결정할 경우, 인증 기관(102)은 추후에 요청자(104)의 아이디를 획득하더라도 비밀키 생성에 사용된 랜덤값은 여전히 알 수 없으므로 아이디에 대응되는 비밀키를 생성할 수 없게 된다.

[0076] 도 4는 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 기술되지 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0077] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 본 발명의 실시예들에 따른 인증 기관(102), 인증 요청자(104) 및 검증자(106)일 수 있다. 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.

[0078] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 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.

[0079] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0080] 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.

[0082] 한편, 본 발명의 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 예는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0083] 이상에서 본 발명의 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 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0085] 100: 아이디 기반 서명 시스템

102: 인증 기관

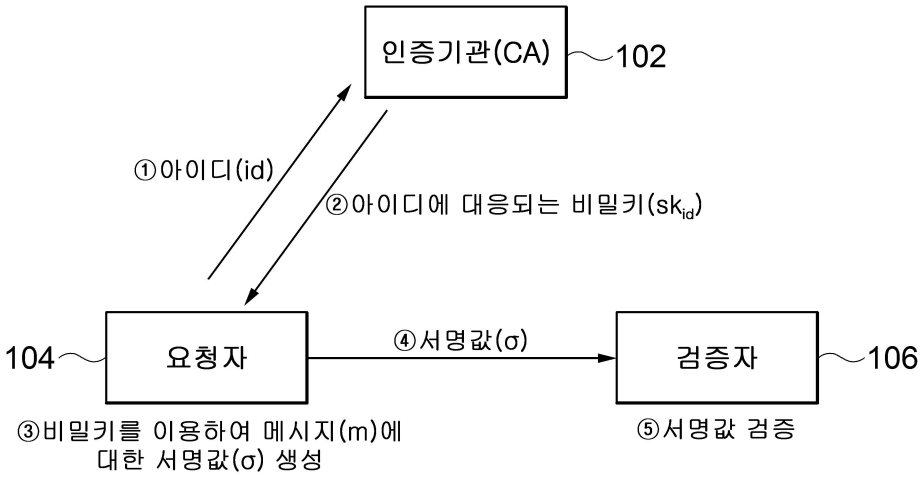
104: 인증 요청자

106: 검증자

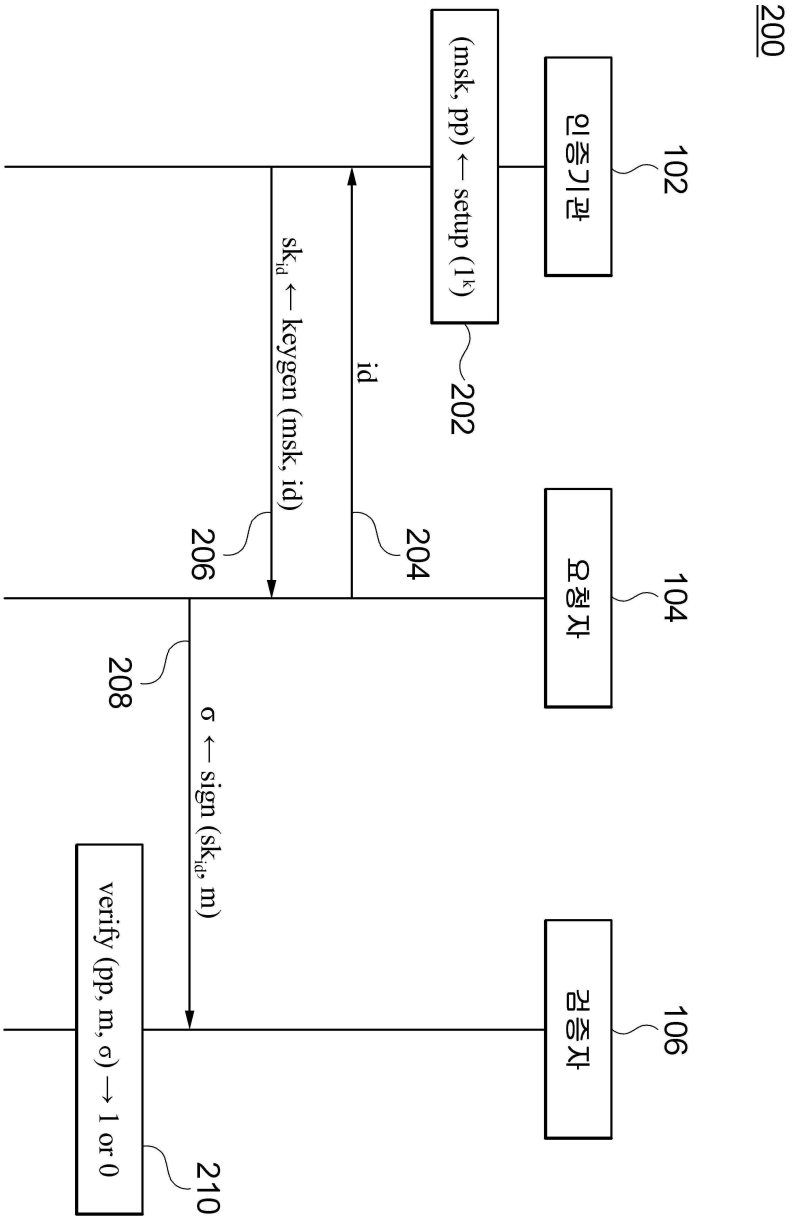
도면

도면1

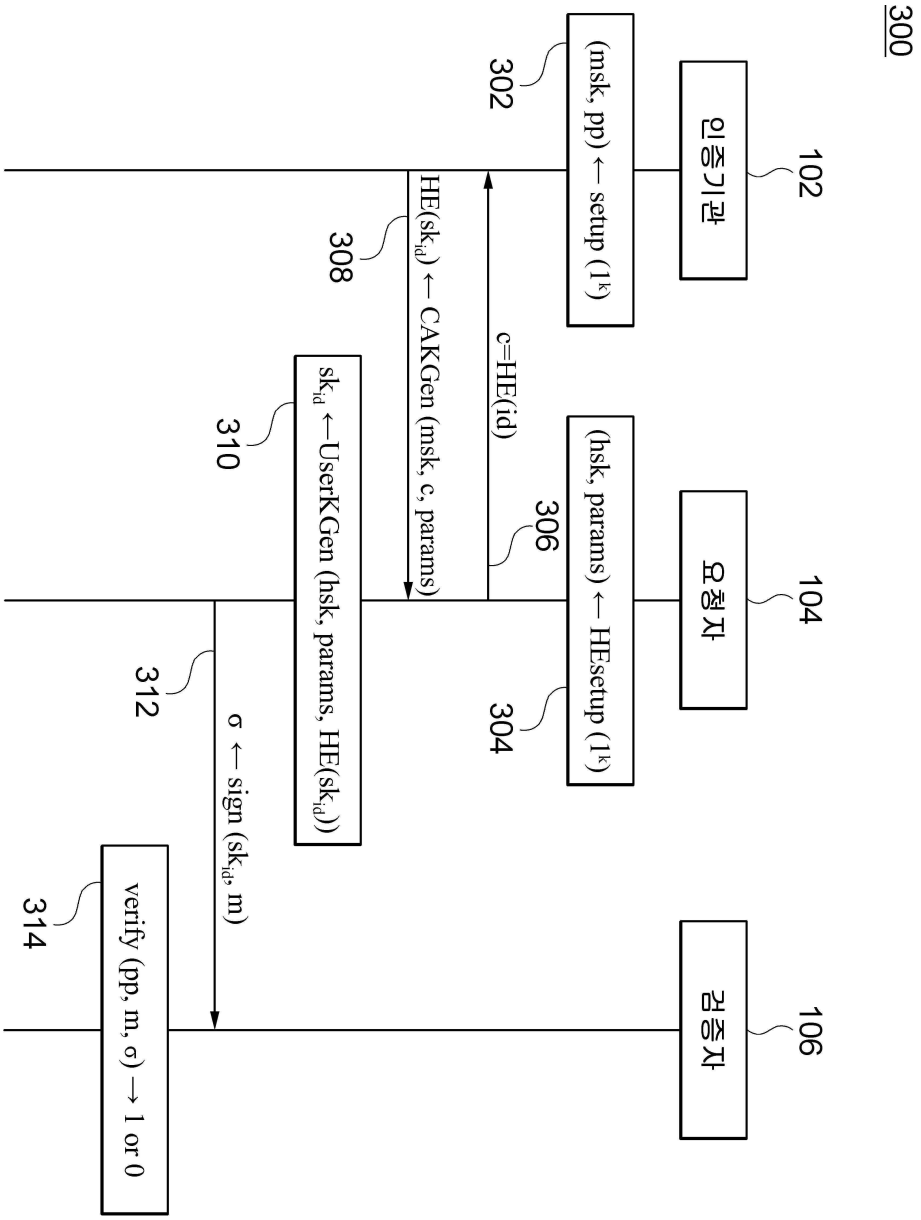
100



도면2


200
인증기관
102
(msk, pp) ← setup (1^k)
202
id
204
sk_id ← keygen (msk, id)
206
요청자
104
σ ← sign (sk_id, m)
208
검증자
106
verify (pp, m, σ) → 1 or 0
210

도면3



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제6항

【변경전】

상기 인증 요청자 단말의 아이디(id)에 대응되는 제1 동형 암호문(c=HE(id))을 생성하는 인증 요청자 단말

【변경후】

인증 요청자 단말의 아이디(id)에 대응되는 제1 동형 암호문(c=HE(id))을 생성하는 인증 요청자 단말