



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2015년06월22일

(11) 등록번호 10-1522731

(24) 등록일자 2015년05월18일

(51) 국제특허분류(Int. Cl.)

H04L 9/32 (2006.01) H04L 9/30 (2006.01)

(21) 출원번호 10-2014-0022552

(22) 출원일자 2014년02월26일

심사청구일자 2014년02월26일

(56) 선행기술조사문헌

KR1020030062402 A*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

정익래

서울특별시 광진구 김고량로4길 53, 203호(중곡1동, 호동아파트)

김기성

서울특별시 성북구 안암로 145, 로봇융합관 404호 (안암동5가)

(74) 대리인

심경식, 홍성욱, 한승범, 유병욱

전체 청구항 수 : 총 14 항

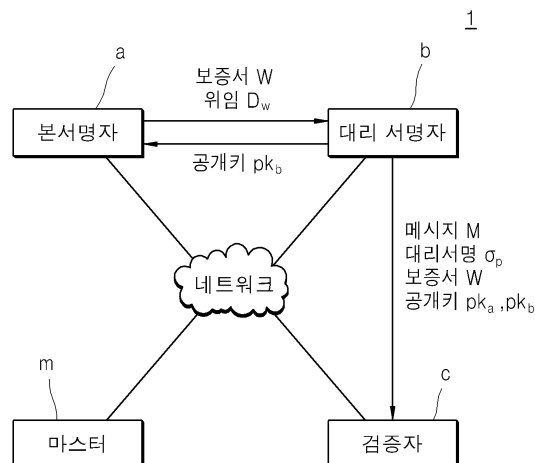
심사관 : 하정훈

(54) 발명의 명칭 대리 서명 시스템 및 방법

(57) 요약

본 발명의 일 실시예에 따른 대리 서명 시스템은 전자 서명을 생성하고 검증하는 수단을 제공하는 일반 서명 기능 제공부; 및 상기 일반 서명 기능 제공부와 기능적으로 연결되어 있고, 상기 일반 서명 기능 제공부를 사용하여 대리 서명을 생성하고 검증하는 하나 이상의 사용자 개체를 포함하고, 상기 사용자 개체는 본 서명자 개체의 비밀키, 대리 서명자 개체의 공개키, 및 보증서를 사용하여 위임 권한을 생성하여 상기 대리 서명자 개체에게 전송하는 상기 본 서명자 개체; 상기 대리 서명자 개체의 비밀키, 메시지 및 상기 본 서명자 개체로부터 수신한 위임 권한 및 보증서를 사용하여 대리 서명을 생성하여 검증자 개체에게 전송하는 상기 대리 서명자 개체; 및 상기 대리 서명자 개체로부터 수신한, 상기 본 서명자 개체의 공개키, 상기 대리 서명자 개체의 공개키, 메시지, 및 보증서를 사용하여 상기 대리 서명을 검증하는 검증자 개체를 포함한다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호 ITAH0301130330070001000100100

부처명 미래창조과학부

연구관리전문기관 정보통신산업진흥원

연구사업명 대학IT연구센터육성지원사업

연구과제명 스마트그리드 기술 연구

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2013.01.01 ~ 2013.12.31

명세서

청구범위

청구항 1

전자 서명을 생성하고 검증하는 수단을 제공하는 일반 서명 기능 제공부; 및

상기 일반 서명 기능 제공부와 기능적으로 연결되어 있고, 상기 일반 서명 기능 제공부를 사용하여 대리 서명을 생성하고 검증하는 하나 이상의 사용자 개체를 포함하고,

상기 사용자 개체는

본 서명자 개체의 비밀키, 대리 서명자 개체의 공개키, 및 보증서를 사용하여 위임 권한을 생성하여 상기 대리 서명자 개체에게 전송하는 상기 본 서명자 개체;

상기 대리 서명자 개체의 비밀키, 메시지 및 상기 본 서명자 개체로부터 수신한 위임 권한 및 보증서를 사용하여 대리 서명을 생성하여 검증자 개체에게 전송하는 상기 대리 서명자 개체; 및

상기 대리 서명자 개체로부터 수신한, 상기 본 서명자 개체의 공개키, 상기 대리 서명자 개체의 공개키, 메시지, 및 보증서를 사용하여 상기 대리 서명을 검증하는 검증자 개체를 포함하며,

상기 대리 서명자 개체는

상기 일반 서명 기능 제공부에 의해 출력되는 아이디를 기반으로 하는 Sign 알고리즘을 사용하여 제1 대리 서명을 생성하고, 상기 제1 대리 서명을 포함하는 아이디를 기반으로 하는 Extract 알고리즘을 사용하여 위임 권한을 출력하며, 상기 위임 권한 및 상기 제1 대리 서명을 포함하는 아이디를 기반으로 하는 Sign 알고리즘을 사용하여 제2 대리 서명을 생성하고, 상기 제1 및 제2 대리 서명을 최종 대리 서명으로서 출력하는 것을 특징으로 하는 대리 서명 시스템.

청구항 2

제1항에 있어서,

상기 본 서명자 개체는

상기 일반 서명 기능 제공부에 의해 출력되는 시스템 파라미터, 아이디, 마스터 키를 입력 파라미터로 하는 아이디(ID) 기반 서명 기법의 Extract 알고리즘을 사용하여 상기 위임 권한을 생성하되, 상기 아이디 부분에는 상기 본 서명자 개체의 공개키, 상기 대리 서명자 개체의 공개키 및 상기 보증서가 입력되고, 상기 마스터 키 부분에는 상기 본 서명자 개체의 비밀키가 입력되는 것을 특징으로 하는 대리 서명 시스템.

청구항 3

제1항에 있어서,

상기 Sign 알고리즘은

상기 제1 대리 서명의 생성 시, 상기 일반 서명 기능 제공부에 의해 출력되는 시스템 파라미터, 상기 아이디, 상기 위임 권한, 및 상기 메시지를 입력 파라미터로 하고,

상기 제2 대리 서명의 생성 시, 상기 시스템 파라미터, 상기 제1 대리 서명을 포함하는 아이디, 상기 위임 권한, 및 상기 메시지를 입력 파라미터로 하며,

상기 Extract 알고리즘은

상기 위임 권한의 출력 시, 상기 시스템 파라미터, 상기 제1 대리 서명을 포함하는 아이디, 및 상기 대리 서명자 개체의 비밀키를 입력 파라미터로 하는 것을 특징으로 하는 대리 서명 시스템.

청구항 4

제1항에 있어서,

상기 일반 서명 기능 제공부와 기능적으로 연결되어 있고, 상기 일반 서명 기능 제공부를 사용하여 상기 사용자 개체의 공개키 및 비밀키를 생성하는 마스터 개체

를 더 포함하는 것을 특징으로 하는 대리 서명 시스템.

청구항 5

제4항에 있어서,

상기 일반 서명 기능 제공부는

안전성 레벨 파라미터에 기초하여 시스템 파라미터를 출력하는 시스템 설정 기능 제공부를 포함하고,

상기 마스터 개체는

상기 시스템 설정 기능 제공부를 사용하여 상기 시스템 파라미터를 출력하는 것을 특징으로 하는 대리 서명 시스템.

청구항 6

제4항에 있어서,

상기 일반 서명 기능 제공부는

마스터 공개키 및 마스터 비밀키를 생성하는 마스터 키 생성 기능 제공부를 포함하고,

상기 마스터 개체는

상기 마스터 키 생성 기능 제공부를 사용하여 상기 사용자 개체의 공개키 및 비밀키를 생성하는 것을 특징으로 하는 대리 서명 시스템.

청구항 7

제1항에 있어서,

상기 일반 서명 기능 제공부는

아이디 기반 서명 기법(ID-based signature scheme)을 사용하는 것을 특징으로 하는 대리 서명 시스템.

청구항 8

제1항에 있어서,

상기 일반 서명 기능 제공부는

공개키에 대응하는 비밀키를 생성하는 사용자 비밀키 생성 기능 제공부를 포함하고,

상기 본 서명자 개체는

상기 사용자 비밀키 생성 기능 제공부를 사용하여 상기 위임 권한을 생성하는 것을 특징으로 하는 대리 서명 시스템.

청구항 9

제1항에 있어서,
 상기 일반 서명 기능 제공부는
 메시지에 대한 전자 서명을 생성하는 서명 생성 기능 제공부를 포함하고,
 상기 대리 서명자 개체는
 상기 서명 생성 기능 제공부를 사용하여 상기 대리 서명을 생성하는 것을 특징으로 하는 대리 서명 시스템.

청구항 10

제1항에 있어서,
 상기 일반 서명 기능 제공부는
 서명이 유효한지 검증하는 서명 검증 기능 제공부를 포함하고,
 상기 대리 서명자 개체는
 상기 서명 검증 기능 제공부를 사용하여 상기 대리 서명을 검증하는 것을 특징으로 하는 대리 서명 시스템.

청구항 11

제1항에 있어서,
 상기 일반 서명 기능 제공부는
 기 지정된 길이의 결과값을 출력하는 해시 함수를 제공하고,
 상기 해시 함수는
 상기 메시지 및 상기 보증서의 길이와 동일한 길이의 결과값을 출력하는 것을 특징으로 하는 대리 서명 시스템.

청구항 12

대리 서명 시스템을 사용한 대리 서명 방법에 있어서,
 본 서명자 개체에서, 상기 본 서명자 개체의 비밀키, 대리 서명자 개체의 공개키, 보증서, 및 상기 본 서명자 개체와 기능적으로 연결되어 있는 일반 서명 기능 제공부의 사용자 비밀키 생성 기능 제공부를 사용하여 위임 권한을 생성하는 단계;
 상기 대리 서명자 개체에서, 상기 대리 서명자 개체의 비밀키, 메시지, 상기 본 서명자 개체로부터 수신한 위임 권한과 보증서, 및 상기 대리 서명자 개체와 기능적으로 연결되어 있는 일반 서명 기능 제공부의 서명 생성 기능 제공부를 사용하여 대리 서명을 생성하는 단계; 및
 검증자 개체에서, 상기 대리 서명자 개체로부터 수신한, 상기 본 서명자 개체의 공개키, 상기 대리 서명자 개체의 공개키, 메시지, 보증서, 및 상기 검증자 개체와 기능적으로 연결되어 있는 일반 서명 기능 제공부의 서명 검증 기능 제공부를 사용하여 상기 대리 서명을 검증하는 단계를 포함하고,
 상기 대리 서명자 개체는
 상기 일반 서명 기능 제공부에 의해 출력되는 아이디를 기반으로 하는 Sign 알고리즘을 사용하여 제1 대리 서명을 생성하고, 상기 제1 대리 서명을 포함하는 아이디를 기반으로 하는 Extract 알고리즘을 사용하여 위임 권한을 출력하며, 상기 위임 권한 및 상기 제1 대리 서명을 포함하는 아이디를 기반으로 하는 Sign 알고리즘을 사용하여 제2 대리 서명을 생성하고, 상기 제1 및 제2 대리 서명을 최종 대리 서명으로서 출력하는 것을 특징으로 하는 대리 서명 방법.

청구항 13

제12항에 있어서,

상기 위임 권한을 생성하는 단계는

상기 일반 서명 기능 제공부에 의해 출력되는 시스템 파라미터, 아이디, 마스터 키를 입력 파라미터로 하는 ID 기반 서명 기법의 Extract 알고리즘을 사용하여 상기 위임 권한을 생성하는 단계

를 포함하고,

상기 아이디 부분에는 상기 본 서명자 개체의 공개키, 상기 대리 서명자 개체의 공개키 및 상기 보증서가 입력되고, 상기 마스터 키 부분에는 상기 본 서명자 개체의 비밀키가 입력되는 것을 특징으로 하는 대리 서명 방법.

청구항 14

제12항에 있어서,

상기 Sign 알고리즘은

상기 제1 대리 서명의 생성 시, 상기 일반 서명 기능 제공부에 의해 출력되는 시스템 파라미터, 상기 아이디, 상기 위임 권한, 및 상기 메시지를 입력 파라미터로 하고,

상기 제2 대리 서명의 생성 시, 상기 시스템 파라미터, 상기 제1 대리 서명을 포함하는 아이디, 상기 위임 권한, 및 상기 메시지를 입력 파라미터로 하며,

상기 Extract 알고리즘은

상기 위임 권한의 출력 시, 상기 시스템 파라미터, 상기 제1 대리 서명을 포함하는 아이디, 및 상기 대리 서명자 개체의 비밀키를 입력 파라미터로 하는 것을 특징으로 하는 대리 서명 방법.

발명의 설명

기술 분야

[0001] 본 발명의 실시예들은 대리 서명 시스템 및 방법에 관한 것이다.

[0002]

배경 기술

[0003]

대리 서명 기법은 본 서명자의 서명 권한을 특정 개체(대리 서명자)에게 위임하여 본 서명자를 대신해 서명을 할 수 있는 기법을 말한다. 주로 위임이 빈번하게 발생하는 분산 컴퓨팅(Distributed Computing) 환경에서 사용되며, 그리드 컴퓨팅(Grid Computing) 및 모바일 통신에서 활용된다. 최근에는 이러한 환경들이 복합적으로 존재하는 스마트그리드 환경이 또 다른 응용환경으로 각광받고 있다.

[0004]

대리 서명 기법을 가장 잘 표현할 수 있는 예는, 어느 회사의 간부(본 서명자)가 출장으로 장기간 자리를 비울 경우 업무의 효율성을 위해 자신의 서명 권한을 자신의 비서(대리 서명자)에 위임하는 예이다. 이러한 대리 서명기법은 다음과 같은 성질을 만족해야 한다.

[0005]

첫째, 본 서명자는 자신이 본 서명자 임에도 불구하고 대리 서명을 생성할 수 없어야 한다. 이러한 개념은 대리 서명자의 프라이버시를 보호함은 물론이고 추후 분쟁의 여지를 없애주는 중요한 성질이다. 둘째, 서명 확인자는 본 서명자의 동의하에 대리 서명이 대리 서명자에 의해 생성되었음을 확인할 수 있어야 한다. 셋째, 서명을 확인하는 사람은 대리 서명자의 신원을 확인할 수 있어야 한다. 넷째, 대리 서명자는 자신의 서명에 대해 부인할 수 없어야 한다. 이러한 4가지 성질은 대리 서명이 반드시 만족해야 할 중요한 성질이다.

[0006]

ID 기반 서명 기법이란 각 개인을 식별할 수 있는 ID 자체가 서명 확인키로 쓰이며, 각 개인은 자신의 ID에 대한 서명키를 KGC(Key Generation Center)를 통해 발급받는 환경이다. 이러한 ID 기반의 환경은 기존의 공개키

환경에 비해 공인 인증서 발급 과정이 없이 ID 만으로 서명 생성 및 확인이 가능하여 일반 서명에 비해 효율적이며 자유롭다.

[0007] 관련 선행기술로는 한국 등록특허공보 제10-0732233호(발명의 명칭: 접선형 함수를 사용한 대리서명능력 제한성을 가지는 개인식별정보 기반 대리서명 장치 및 그 방법, 등록일자: 2007년 06월 19일)가 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명의 일 실시예는 아이디(ID) 기반 서명 기법을 사용하여 대리 서명을 생성하고 검증하는 알고리즘을 제공함으로써 특정 환경에서의 서명 위조를 방지하여 안전한 대리 서명을 생성할 수 있으며, 이를 통해 대리 서명 시스템의 안전성 및 효율성을 향상시킬 수 있는 대리 서명 시스템 및 방법을 제공한다.

[0009] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제(들)로 제한되지 않으며, 언급되지 않은 또 다른 과제(들)는 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

[0010]

과제의 해결 수단

[0011] 본 발명의 일 실시예에 따른 대리 서명 시스템은 전자 서명을 생성하고 검증하는 수단을 제공하는 일반 서명 기능 제공부; 및 상기 일반 서명 기능 제공부와 기능적으로 연결되어 있고, 상기 일반 서명 기능 제공부를 사용하여 대리 서명을 생성하고 검증하는 하나 이상의 사용자 개체를 포함하고, 상기 사용자 개체는 본 서명자 개체의 비밀키, 대리 서명자 개체의 공개키, 및 보증서를 사용하여 위임 권한을 생성하여 상기 대리 서명자 개체에게 전송하는 상기 본 서명자 개체; 상기 대리 서명자 개체의 비밀키, 메시지 및 상기 본 서명자 개체로부터 수신한 위임 권한 및 보증서를 사용하여 대리 서명을 생성하여 검증자 개체에게 전송하는 상기 대리 서명자 개체; 및 상기 대리 서명자 개체로부터 수신한, 상기 본 서명자 개체의 공개키, 상기 대리 서명자 개체의 공개키, 메시지, 및 보증서를 사용하여 상기 대리 서명을 검증하는 검증자 개체를 포함한다.

[0012] 상기 본 서명자 개체는 상기 일반 서명 기능 제공부에 의해 출력되는 시스템 파라미터, 아이디, 마스터 키를 입력 파라미터로 하는 아이디(ID) 기반 서명 기법의 Extract 알고리즘을 사용하여 상기 위임 권한을 생성하되, 상기 아이디 부분에는 상기 본 서명자 개체의 공개키, 상기 대리 서명자 개체의 공개키 및 상기 보증서가 입력되고, 상기 마스터 키 부분에는 상기 본 서명자 개체의 비밀키가 입력될 수 있다.

[0013] 상기 대리 서명자 개체는 상기 시스템 파라미터, 상기 아이디, 상기 위임 권한, 및 메시지를 입력 파라미터로 하는 상기 아이디 기반 서명 기법의 Sign 알고리즘을 사용하여 제1 대리 서명을 생성하고, 상기 시스템 파라미터, 상기 제1 대리 서명을 포함하는 아이디, 및 상기 대리 서명자 개체의 비밀키를 입력 파라미터로 하는 Extract 알고리즘을 사용하여 위임 권한을 출력하며, 상기 시스템 파라미터, 상기 제1 대리 서명을 포함하는 아이디, 상기 위임 권한, 및 상기 메시지를 입력 파라미터로 하는 Sign 알고리즘을 사용하여 제2 대리 서명을 생성하고, 상기 제1 대리 서명 및 상기 제2 대리 서명을 최종 대리 서명으로서 출력할 수 있다.

[0014] 본 발명의 일 실시예에 따른 대리 서명 시스템은 상기 일반 서명 기능 제공부와 기능적으로 연결되어 있고, 상기 일반 서명 기능 제공부를 사용하여 상기 사용자 개체의 공개키 및 비밀키를 생성하는 마스터 개체를 더 포함할 수 있다.

[0015] 상기 일반 서명 기능 제공부는 안전성 레벨 파라미터에 기초하여 시스템 파라미터를 출력하는 시스템 설정 기능 제공부를 포함하고, 상기 마스터 개체는 상기 시스템 설정 기능 제공부를 사용하여 상기 시스템 파라미터를 출력할 수 있다.

[0016] 상기 일반 서명 기능 제공부는 마스터 공개키 및 마스터 비밀키를 생성하는 마스터 키 생성 기능 제공부를 포함하고, 상기 마스터 개체는 상기 마스터 키 생성 기능 제공부를 사용하여 상기 사용자 개체의 공개키 및 비밀키를 생성할 수 있다.

[0017] 상기 일반 서명 기능 제공부는 아이디 기반 서명 기법(ID-based signature scheme)을 사용할 수 있다.

- [0018] 상기 일반 서명 기능 제공부는 공개키에 대응하는 비밀키를 생성하는 사용자 비밀키 생성 기능 제공부를 포함하고, 상기 본 서명자 개체는 상기 사용자 비밀키 생성 기능 제공부를 사용하여 상기 위임 권한을 생성할 수 있다.
- [0019] 상기 일반 서명 기능 제공부는 메시지에 대한 전자 서명을 생성하는 서명 생성 기능 제공부를 포함하고, 상기 대리 서명자 개체는 상기 서명 생성 기능 제공부를 사용하여 상기 대리 서명을 생성할 수 있다.
- [0020] 상기 일반 서명 기능 제공부는 서명이 유효한지 검증하는 서명 검증 기능 제공부를 포함하고, 상기 대리 서명자 개체는 상기 서명 검증 기능 제공부를 사용하여 상기 대리 서명을 검증할 수 있다.
- [0021] 상기 일반 서명 기능 제공부는 기 기정된 길이의 결과값을 출력하는 해시 함수를 제공하고, 상기 해시 함수는 상기 메시지 및 상기 보증서의 길이와 동일한 길이의 결과값을 출력할 수 있다.
- [0022] 본 발명의 일 실시예에 따른 대리 서명 방법은 본 서명자 개체에서, 상기 본 서명자 개체의 비밀키, 대리 서명자 개체의 공개키, 보증서, 및 상기 본 서명자 개체와 기능적으로 연결되어 있는 일반 서명 기능 제공부의 사용자 비밀키 생성 기능 제공부를 사용하여 위임 권한을 생성하는 단계; 상기 대리 서명자 개체에서, 상기 대리 서명자 개체의 비밀키, 메시지, 상기 본 서명자 개체로부터 수신한 위임 권한과 보증서, 및 상기 대리 서명자 개체와 기능적으로 연결되어 있는 일반 서명 기능 제공부의 서명 생성 기능 제공부를 사용하여 대리 서명을 생성하는 단계; 및 상기 검증자 개체에서, 상기 대리 서명자 개체로부터 수신한, 상기 본 서명자 개체의 공개키, 상기 대리 서명자 개체의 공개키, 메시지, 보증서, 및 상기 검증자 개체와 기능적으로 연결되어 있는 일반 서명 기능 제공부의 서명 검증 기능 제공부를 사용하여 상기 대리 서명을 검증하는 단계를 포함한다.
- [0023] 상기 위임 권한을 생성하는 단계는 상기 일반 서명 기능 제공부에 의해 출력되는 시스템 파라미터, 아이디, 마스터 키를 입력 파라미터로 하는 ID 기반 서명 기법의 Extract 알고리즘을 사용하여 상기 위임 권한을 생성하는 단계를 포함하고, 상기 아이디 부분에는 상기 본 서명자 개체의 공개키, 상기 대리 서명자 개체의 공개키 및 상기 보증서가 입력되고, 상기 마스터 키 부분에는 상기 본 서명자 개체의 비밀키가 입력될 수 있다.
- [0024] 상기 대리 서명을 생성하는 단계는 상기 시스템 파라미터, 상기 아이디, 상기 위임 권한, 및 메시지를 입력 파라미터로 하는 상기 아이디 기반 서명 기법의 Sign 알고리즘을 사용하여 제1 대리 서명을 생성하는 단계; 상기 시스템 파라미터, 상기 제1 대리 서명을 포함하는 아이디, 및 상기 대리 서명자 개체의 비밀키를 입력 파라미터로 하는 Extract 알고리즘을 사용하여 위임 권한을 출력하는 단계; 상기 시스템 파라미터, 상기 제1 대리 서명을 포함하는 아이디, 상기 위임 권한, 및 상기 메시지를 입력 파라미터로 하는 Sign 알고리즘을 사용하여 제2 대리 서명을 생성하는 단계; 및 상기 제1 대리 서명 및 상기 제2 대리 서명을 최종 대리 서명으로서 출력하는 단계를 포함할 수 있다.
- [0025] 기타 실시예들의 구체적인 사항들은 상세한 설명 및 첨부 도면들에 포함되어 있다.
- [0026]

발명의 효과

- [0027] 본 발명의 일 실시예에 따르면, 아이디(ID) 기반 서명 기법을 사용하여 대리 서명을 생성하고 검증하는 알고리즘을 제공함으로써 특정 환경에서의 서명 위조를 방지하여 안전한 대리 서명을 생성할 수 있으며, 이를 통해 대리 서명 시스템의 안전성 및 효율성을 향상시킬 수 있다.

도면의 간단한 설명

- [0028] 도 1은 본 발명의 일 실시예에 따른 대리 서명 시스템의 구조를 도시한 도면이다.
- 도 2는 종래의 공개키 기반 서명 시스템에서 교환되는 정보의 간략한 흐름을 도시한 도면이다.
- 도 3은 종래의 ID 기반 서명 시스템의 동작 흐름을 각 개체의 동작에 사용되는 알고리즘의 입력값 및 출력값을 포함하는 명세와 함께 도시한 도면이다.
- 도 4는 종래의 대리 서명 시스템의 동작 흐름을 각 개체의 동작에 사용되는 알고리즘의 입력값 및 출력값을 포

함하는 명세와 함께 도시한 도면이다.

도 5는 본 발명의 일 실시예에 따른 일반 서명 기능 제공부를 도시한 도면이다.

도 6은 본 발명의 일 실시예에 따른 마스터 개체를 도시한 도면이다.

도 7은 본 발명의 일 실시예에 따른 사용자 개체를 도시한 도면이다.

도 8은 본 발명의 일 실시예에 따른 대리 서명 방법을 설명하기 위해 도시한 도면이다.

도 9는 본 발명의 일 실시예에 따라 대리 서명을 생성하는 과정을 상세히 설명하기 위해 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0029] 본 발명의 이점 및/또는 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성요소를 지칭한다.
- [0030] 도 1은 본 발명의 일 실시예에 따른 대리 서명 시스템의 구조를 도시한 도면이다.
- [0031] 도 1을 참조하면, 상기 대리 서명 시스템(1)에는 네트워크를 통해 연결된 본 서명자(a), 대리 서명자(b), 및 검증자(c)를 포함하는 사용자 개체(entity)가 참여한다.
- [0032] 사용자 중, 본 서명자(a)는 자신의 서명 권한을 대리 서명자(b)에게 위임하는 개체이며, 대리 서명자(b)는 본 서명자(a)로부터 수신한 위임(delegation)에 따라 본 서명자(a)를 대신하여 대리 서명을 생성하는 개체이고, 검증자(c)는 대리 서명을 검증, 즉 수신한 서명이 본 서명자(a)의 정당한 위임을 받은 대리 서명자(b)에 의해 생성된, 유효한 서명임을 확인하는 개체이다.
- [0033] 도면에는 각각 하나의 본 서명자(a), 대리 서명자(b), 및 검증자(c) 개체만이 도시되어 있고, 이들이 서로 다른 개체인 것처럼 도시되어 있다. 그러나 본 서명자(a), 대리 서명자(b), 및 검증자(c)는 모두 사용자 개체로서, 이들의 역할은 고정적이지 않을 수 있으며, 대리 서명 시스템(1)에 참여하는 사용자 개체의 수에도 제한이 없을 것임을 쉽게 이해할 수 있을 것이다. 또한, 이들 각 사용자 개체는 사용자가 사용하는 기기, 단말, 서버나 소프트웨어 등의 실체를 의미할 수 있다. 이는 통용되는 개념이므로 본 명세서에서 이에 대한 명시적 기재는 생략한다. 예를 들어, 이하 기술에서 사용자라 함은 본 서명자(a), 대리 서명자(b), 및 검증자(c) 등의 사용자 개체를 나타낼 수 있다.
- [0034] 본 발명의 일 실시예에 따른 대리 서명 시스템(1)은 공개키 기반 환경(Public Key Infrastructure: PKI)에서 구현될 수 있으며, 각 사용자의 공개키 및 비밀키를 생성하여 해당 사용자에게 배포하는 마스터(m) 개체가 상기 대리 서명 시스템(1)에 더 참여할 수 있다. 여기에서 마스터(m)는 키 생성 기관(Key Generation Center), 인증 기관(Certification Authority) 등 다양한 이름으로 불릴 수 있으며, 대리 서명 시스템(1)이 원활하게 운영되도록 관리하는 기관들을 통칭하는 개념으로 사용되었다.
- [0035] 본 서명자(a)는 자신의 비밀키, 대리 서명자(b)의 공개키, 및 보증서를 사용하여 위임 권한을 생성하고, 대리 서명자(b)는 자신의 비밀키, 메시지, 본 서명자(a)로부터 수신한 위임 권한 및 보증서를 사용하여 대리 서명을 생성하며, 검증자(c)는 대리 서명자(b)로부터 수신한 본 서명자(a)의 공개키, 대리 서명자(b)의 공개키, 메시지, 및 보증서를 사용하여 대리 서명을 검증한다.
- [0036] 따라서, 도면에 도시되어 있는 바와 같이, 각 사용자 개체는 보증서, 위임 권한, 메시지 및 대리 서명 등을 주고 받을 수 있으며, 각 사용자 개체의 공개키를 더 주고 받을 수 있다. 또는 일 실시예에서 공개키는 미리 공개되어, 각 사용자 개체가 자신의 공개키를 상대방 개체에게 전송하는 과정 없이 접근될 수 있다. 또한, 도시되어 있지 않지만, 마스터(m)가 각 사용자의 공개키 및 비밀키를 생성하여 각 사용자에게 전송할 수 있다.
- [0037] 전술한 바와 같이, 본 발명의 일 실시예에 따른 대리 서명 시스템(1)은 일반 전자 서명 기법을 사용하여 대리 서명을 생성하고 검증한다. 바람직한 실시예에서 대리 서명 시스템(1)은 ID 기반 서명 기법(ID-based

signature scheme)을 기반으로 하는 일반 전자 서명 기법을 사용한다.

- [0038] ID 기반 서명 기법은 ID, 이메일 등의 이미 공개되어 있는 사용자 식별정보를 사용자의 공개키로 사용하여, 마스터(m)가 각 사용자에게 공인 인증서, 즉 공개키 인증서(public key certificate)를 발급할 필요를 없앤 일반 전자 서명 기법이다. 사용자의 공개키가 해당 사용자의 것임을 보증하기 위해, 인증기관이 자신의 마스터 비밀키로 각 사용자의 공개키에 서명하는 과정이 필요 없으므로, 종래의 공개키 기반 전자 서명 기법보다 효율성 및 안전성이 높다.
- [0039] 이에 대해서는 도 5 내지 도 7을 통해 뒤에서 자세히 기술할 것이며, 먼저 도 2 내지 도 4를 통해 종래의 일반 전자 서명 및 대리 서명 시스템에서의 메시지 및 동작의 흐름을 설명한다.
- [0040] 도 2는 종래의 공개키 기반 서명 시스템에서 교환되는 정보의 간략한 흐름을 도시하고 있다.
- [0041] 먼저, 마스터(m)가 공개키, 비밀키, 공개키가 해당 사용자의 것임을 보증하는 인증서를 각 사용자에게 배포한다(S210). 도면에는 본 서명자(a)에게 전송하는 동작만 도시되어 있으나, 검증자(c)를 포함하는 다른 사용자에게도 해당 사용자에 대해 생성된 공개키, 비밀키 및 인증서가 전송된다.
- [0042] 다음, 본 서명자(a)가 메시지에 서명하여 자신의 공개키 및 인증서와 함께 검증자(c)에게 전송한다(S220).
- [0043] 서명을 생성하고 검증하는 등의 각 개체의 동작의 흐름은 도 3과 유사하므로 도시하지 않았다. 도 2와 도 3의 정보 흐름을 비교해보면, 전송한 바와 같이, ID 기반 서명 기법에서는 인증서가 필요 없으며, 공개키 대신 사용자의 아이디가 사용됨을 알 수 있다.
- [0044] 도 3은 종래의 ID 기반 서명 시스템의 동작 흐름을 각 개체의 동작에 사용되는 알고리즘의 입력값 및 출력값을 포함하는 명세와 함께 도시하고 있다. 당업자는 이러한 알고리즘 명세를 쉽게 이해할 수 있을 것이므로, 명세에 대한 자세한 설명은 생략한다.
- [0045] 먼저, 마스터(m)가 시스템을 설정한다(S310). 시스템 설정 단계(310)에 대해 도시되어 있는 알고리즘 명세는 안전성 레벨 파라미터를 입력하면 시스템 파라미터가 출력됨을 보여주고 있다. 즉, 안전성 레벨 파라미터를 통해 ID 기반 서명 시스템 및 방법의 안전성을 설정할 수 있다. 이 단계는 ID 기반 서명 기법 뿐 아니라 다양한 전자 서명 기법에 포함될 수 있으며, 공지의 기술이므로 설명을 생략한다.
- [0046] 다음으로, 마스터(m)는 설정된 시스템 파라미터를 사용하여 마스터 공개키 및 마스터 비밀키를 생성한다(S320). 예를 들어, 마스터(m)는 상기 시스템 설정 단계(310)에서 설정된 시스템 파라미터에 의해 행의 수 및 열의 수가 결정되는 트랩 도어(trapdoor) 행렬을 생성함으로써 이를 수행할 수 있다. 이때, 전송한 바와 같이 기반이 되는 수학적 난제를 변경하면 전체 전자 서명 시스템의 안전성 또는 효율성이 향상될 수 있다.
- [0047] 도시되어 있지 않지만, 상기 단계들(S310, S320)에서 출력된 시스템 파라미터 및 마스터 공개키는 시스템의 모든 사용자 개체에게 공개된다.
- [0048] 다음으로, 마스터(m)는 사용자로부터 ID를 수신하여(S330), 자신의 마스터 비밀키를 사용하여 해당 ID에 대응하는 사용자 비밀키를 생성하여(S340), 해당 사용자에게 전송한다(S350). 도면에는 본 서명자(a)에 대하여 수행하는 것만 도시되어 있으나, 각 사용자에 대해 상기 단계들을 수행한다.
- [0049] 다음으로, 본 서명자(a)가 자신의 비밀키로 메시지에 서명하여(S360), 서명된 메시지를 자신의 ID와 함께 검증자(c)에게 전송한다(S370).
- [0050] 다음으로, 검증자(c)가 마스터 공개키, 본 서명자(a)의 ID를 사용하여 메시지와 함께 수신된 본 서명자(a)의 서명을 검증한다(S380). 즉, 자신이 수신한 서명이 본 서명자(a)가 생성한 정당한 서명임이 확인되면 1을, 아니면 0을 출력한다. 이때, 1 또는 0은 설명을 위한 실시예일 뿐으로, 검증 결과를 나타내기 위한 다양한 조합이 사용될 수 있다.
- [0051] 도 4는 종래의 대리 서명 시스템의 동작 흐름을 각 개체의 동작에 사용되는 알고리즘의 입력값 및 출력값을 포함하는 명세와 함께 도시하고 있다.
- [0052] 먼저, 마스터(m)가 시스템을 설정하고(S410), 사용자 공개키 및 비밀키를 생성하여(S420), 사용자에게 전송한다(S430). 도면에는 본 서명자(a)에 대하여 수행하는 것만 도시되어 있으나, 각 사용자에 대해 상기 단계들을 수행한다. 또한, 도면에는 마스터(m)가 상기 단계들(S410, S420, S430)을 수행하는 것으로 도시되어 있으나, 대리 서명 시스템에서는 마스터(m)가 포함되지 않을 수 있으며, 그럴 경우에는 각 사용자가 자신의 공개키 및 비

밀키를 생성할 수 있다.

- [0053] 다음으로, 본 서명자(a)가 대리 서명자(b)로부터 수신한(S440) 대리 서명자(b)의 공개키 및 자신의 비밀키를 사용하여 보증서로부터 위임을 생성하고(S450), 생성된 위임을 보증서와 함께 대리 서명자(b)에게 전송한다(S460).
- [0054] 보증서는 위임 기간, 서명할 수 있는 메시지 집합 등 위임 권한에 대한 정보를 포함하고 있다. 이러한 보증서에 기초하여 생성된 위임은 안전한 채널로 대리 서명자(b)에게 전달되며, 해당 위임을 가진 대리 서명자(b)만이 본 서명자(a)의 대리 서명을 생성할 수 있다.
- [0055] 다음으로, 대리 서명자(b)가 수신한 보증서 및 위임을 기초로 자신의 비밀키를 사용하여 메시지에 서명하여(S470), 검증자(c)에게 본 서명자(a)의 공개키 및 자신의 공개키와 함께 전송한다(S480).
- [0056] 다음으로, 검증자(c)가 수신한 정보들을 사용하여 대리 서명자(b)의 서명을 검증한다(S380). 즉, 자신이 수신한 서명이 본 서명자(a)의 위임을 받은 대리 서명자(b)가 생성한 정당한 서명임이 확인되면 1을, 아니면 0을 출력한다. 이때, 1 또는 0은 설명을 위한 실시예일 뿐으로, 검증 결과를 나타내기 위한 다양한 조합이 사용될 수 있다.
- [0057] 전술한 바와 같이, 이러한 대리 설명 기법을 일반 서명 기법과 별도로 개발하는 것보다 일반 서명 기법을 기초로 하여 서명 기법을 개발하는 것이 훨씬 효율적이며, 이러한 본 발명의 목적을 달성하기 위해 본 발명의 일 실시예에 따른 대리 서명 시스템(1)은 기법이 되는 일반 전자 서명 기법으로 ID 기반 서명 기법을 사용한다.
- [0058] 도 5 내지 도 7을 통해 이를 설명한다.
- [0059] 도 5에 도시되어 있는 일반 서명 기능 제공부(10)는 도 6 및 도 7에 도시되어 있는 바와 같이 대리 서명 시스템(1)에 참여하는 각 개체와 기능적으로 연결되어 각 개체에 의해 사용된다. 일 실시예에서 일반 서명 기능 제공부(10)는 각 개체에 의해 호출되는 모듈 라이브러리의 형태로 제공될 수 있으므로, 설명의 편의를 위해 일반 서명 기능 제공부(10)가 제공하는 알고리즘은 앞에 라이브러리를 뜻하는 L.을, 각 개체에 의해 사용되는 알고리즘은 앞에 대리 서명을 뜻하는 PS.를 붙여 구분하였다.
- [0060] 본 발명의 일 실시예에 따른 대리 설명 시스템(1)은 안전한 해시(hash) 함수가 존재한다고 가정하고 이를 사용하는데, 해시 함수는 임의의 길이의 데이터를 입력으로 하여 일정한 길이의 해시값을 출력한다. 또한, 설계의 편의성을 위해 일 실시예에서 메시지와 보증서의 길이는 해시 함수가 출력하는 해시값의 길이와 동일할 수 있다. 본 명세서에서 해시 함수는 H()로 도시하였다.
- [0061] 도 5에서는 일반 서명 기능 제공부(10)를 도시하고 있다. 상기 일반 서명 기능 제공부(10)는 ID 기반 서명 기법을 사용하므로, 일반 서명 기능 제공부(10)가 포함하는 시스템 설정 기능 제공부(11), 마스터 키 생성 기능 제공부(13), 사용자 비밀키 생성 기능 제공부(15), 서명 생성 기능 제공부(17), 및 서명 검증 기능 제공부(19)는 도 3에 도시되어 있는 알고리즘을 사용할 수 있다.
- [0062] 이를 보다 자세히 살펴보면, 시스템 설정 기능 제공부(11)는 시스템을 설정하는 L.Setup을 제공한다. 즉, 시스템 설정 기능 제공부(11)는 안전성 레벨 파라미터를 입력받고, 이를 기초로 시스템 파라미터를 출력한다.
- [0063] 마스터 키 생성 기능 제공부(13)는 마스터 공개키 및 마스터 비밀키를 생성하는 L.KeyGen을 제공한다. 즉, 마스터 키 생성 기능 제공부(13)는 시스템 파라미터를 입력받고, 이를 기초로 마스터 공개키 및 마스터 비밀키를 출력한다. 도 3에서 설명한 바와 같이, 마스터 공개키는 공개된다.
- [0064] 사용자 비밀키 생성 기능 제공부(15)는 마스터 비밀키로 사용자의 ID에 대응하는 비밀키를 발급하는 L.Extract를 제공한다. 즉, 사용자 비밀키 생성 기능 제공부(15)는 시스템 파라미터, 사용자의 ID, 마스터 비밀키를 입력받아, ID에 대응하는 비밀키를 출력한다.
- [0065] 서명 생성 기능 제공부(17)는 사용자 비밀키를 사용하여 메시지에 서명하는 L.Sign를 제공한다. 즉, 서명 생성 기능 제공부(17)는 시스템 파라미터, 본 서명자의 ID, ID에 대응하는 비밀키, 메시지를 입력받아 메시지에 대한 서명을 출력한다.
- [0066] 서명 검증 기능 제공부(19)는 사용자 ID를 사용해 서명을 검증하는 L.Verify를 제공한다. 즉, 서명 검증 기능 제공부(19)는 시스템 파라미터, 본 서명자의 ID, 메시지, 메시지에 대한 서명을 입력받아 정당한 서명이면 1을 출력하고, 아니면 0을 출력한다.

- [0067] 도 6은 본 발명의 일 실시예에 따른 마스터 개체를 도시하고 있다.
- [0068] 마스터(m)는 시스템 설정부(100) 및 사용자 키 생성부(200)를 포함하며, 자신과 기능적으로 연결된 일반 서명 기능 제공부(10)를 사용하여 각 사용자의 공개키 및 비밀키를 생성한다.
- [0069] 이를 보다 자세히 살펴보면, 시스템 설정부(100)의 PS.Setup는 일반 서명 기능 제공부(10)가 제공하는 L.Setup을 사용하여 시스템을 설정한다. 즉, L.Setup에 안전성 레벨 파라미터를 넘긴 후, 그 출력값으로 시스템 파라미터를 설정한다.
- [0070] 사용자 키 생성부(200)의 PS.KeyGen는 일반 서명 기능 제공부(10)의 L.KeyGen가 출력한 마스터 공개키 및 마스터 비밀키를 사용자 공개키 및 사용자 비밀키로 생성한다. 즉, 사용자 키 생성부(200)는 L.KeyGen가 출력한 결과를 본 서명자(a)를 위한 공개키 및 비밀키로 출력하고, L.KeyGen가 출력한 결과를 대리 서명자(b)를 위한 공개키 및 비밀키로 출력한다.
- [0071] 여기서는 본 서명자(a)와 대리 서명자(b)에 대해서만 기재되어 있으나, 이는 일반 서명 기능 제공부(10)가 제공하는 마스터 공개키 및 마스터 비밀키를 어떻게 각 사용자 개체의 공개키 및 비밀키로 사용하는지를 설명하기 위한 예시일 뿐으로, 다른 사용자에 대해서도 마찬가지로 수행할 수 있다.
- [0072] 도 7은 본 발명의 일 실시예에 따른 사용자 개체를 도시하고 있다. 도면에서의 사용자 개체는 본 서명자(a), 대리 서명자(b), 검증자(c), 및 기타 사용자를 포함한다.
- [0073] 사용자(a, b, c)는 위임 생성부(300), 대리 서명 생성부(400), 및 대리 서명 검증부(500)를 포함하며, 자신과 기능적으로 연결된 일반 서명 기능 제공부(10)를 사용하여 필요한 동작을 수행한다.
- [0074] 이를 보다 자세히 살펴보면, 본 서명자(a)에 의해 사용되는 위임 생성부(300)의 PS.DelGen는 일반 서명 기능 제공부(10)의 L.Extract를 사용하여 위임 권한을 생성한다. 이때, L.Extract의 ID 입력 부분에는 본 서명자(a)의 공개키, 대리 서명자(b)의 공개키, 및 보증서가 입력되고, 마스터 비밀키 입력 부분에는 본 서명자(a)의 비밀키가 입력된다.
- [0075] 대리 서명자(b)에 의해 사용되는 대리 서명 생성부(40)의 PS.ProxySign는 일반 서명 기능 제공부(10)의 L.Sign을 사용하여 대리 서명을 생성한다.
- [0076] 이를 위해, 먼저 일반 서명 기능 제공부(10)의 L.Sign은 시스템 파라미터, ID, 위임 권한, 및 메시지를 입력 받아 제1 대리 서명을 생성한다.
- [0077] 다음으로, 일반 서명 기능 제공부(10)의 L.Extract는 시스템 파라미터, 제1 대리 서명을 포함하는 ID, 및 대리 서명자의 비밀키를 입력 받아 위임 권한을 출력한다.
- [0078] 다음으로, 일반 서명 기능 제공부(10)의 L.Sign은 시스템 파라미터, 제1 대리 서명을 포함하는 ID, 위임 권한, 및 메시지를 입력 받아 제2 대리 서명을 생성한다.
- [0079] 마지막으로, 대리 서명 생성부(40)의 PS.ProxySign는 제1 대리 서명 및 제2 대리 서명을 최종 대리 서명으로서 출력한다.
- [0080] 검증자(c)에 의해 사용되는 대리 서명 검증부(500)의 PS.ProxyVerify는 일반 서명 기능 제공부(10)의 L.Verify를 사용하여 대리 서명의 정당성을 확인한다.
- [0081] 이를 위해, 먼저 제1 서명의 정당성을 L.Verify의 마스터 공개키 입력 부분에 본 서명자(a)의 공개키를, ID 입력 부분에 보증서를, 서명 입력 부분에 제1 서명을 입력하여 확인한다.
- [0082] 다음으로, 제2 서명의 정당성을 L.Verify의 마스터 공개키 입력 부분에 대리 서명자(b)의 공개키를, ID 입력 부분에 제1 보증서를, 서명 입력 r부분에 제2 서명을 입력하여 확인한다. 이때 제1 보증서는 난수와 제1 서명을 연결한 값을 해시한 것이다.
- [0083] 도 8은 본 발명의 일 실시예에 따른 대리 서명 방법을 설명하기 위해 도시한 흐름도이다.
- [0084] 도 8을 참조하면, 단계(S110)에서 마스터(m)는 자신과 기능적으로 연결된 일반 서명 기능 제공부(10)의 시스템 설정 기능 제공부(11)를 사용하여 시스템을 설정한다.
- [0085] 다음으로, 단계(S120)에서 마스터(m)는 마스터 키 생성 기능 제공부(13)를 사용하여 각 사용자의 공개키 및 비밀키를 생성한다. 이렇게 생성된 공개키 및 비밀키는 각 사용자, 즉 본 서명자(a), 대리 서명자(b) 및 검증자

(c)에게 분배된다.

[0086] 다음으로, 단계(S130)에서 본 서명자(a)는 보증서, 대리 서명자(b)의 공개키, 자신의 비밀키 및 자신과 기능적으로 연결된 일반 서명 기능 제공부(10)의 사용자 비밀키 생성 기능 제공부(15)를 사용하여 위임 권한을 생성한다. 본 서명자(a)는 이렇게 생성된 위임 권한을 대리 서명자(b)에게 전송한다.

[0087] 구체적으로, 본 서명자(a)는 ID 기반 서명 기법의 $\text{Extract}(\Gamma, ID, msk)$ 알고리즘을 다음과 같이 사용하여 위임 권한을 생성한다. $sk_{ID} = W_{a \rightarrow b} \leftarrow \text{Extract}(\Gamma, ID = pk_a || pk_b || W, msk = sk_a)$. 즉, ID 입력부에 $pk_a || pk_b || W$ 를 입력하고, 마스터 비밀키 부분에 본 서명자의 비밀키 sk_a 를 입력하고 출력되는 sk_{ID} 을 위임권한 $W_{a \rightarrow b}$ 으로 사용하는 것이다.

[0088] 다음으로, 단계(S140)에서 대리 서명자(b)는 위임 권한, 보증서, 메시지, 자신의 비밀키 및 자신과 기능적으로 연결된 일반 서명 기능 제공부(10)의 서명 생성 기능 제공부(17)를 사용하여 대리 서명을 생성한다. 대리 서명자(b)는 이렇게 생성된 대리 서명을 검증자(c)에게 전송한다.

[0089] 구체적으로, ID 기반 서명 기법의 Sign 알고리즘을 사용하여 다음과 같이 대리서명을 생성한다. $\sigma_1 \leftarrow \text{Sign}(\Gamma, ID = pk_a || pk_b || W, W_{a \rightarrow b}, M)$ 을 실행한 후, $sk_{ID} \leftarrow \text{Extract}(\Gamma, ID' = pk_a || pk_b || W || \sigma_1, sk_b)$ 를 실행한다. $\sigma_2 \leftarrow \text{Sign}(\Gamma, ID' = pk_a || pk_b || W || \sigma_1, sk_{ID}, M)$ 을 실행한 후, 최종 대리 서명은 $\sigma_p = (\sigma_1, \sigma_2)$ 된다.

[0090] 다음으로, 단계(S150)에서 검증자(c)는 보증서, 메시지, 본 서명자(a)의 공개키, 대리 서명자(b)의 공개키 및 자신과 기능적으로 연결된 일반 서명 기능 제공부(10)의 서명 검증 기능 제공부(19)를 사용하여 대리 서명을 검증한다.

[0091] 구체적으로, ID 기반 서명 기법의 Verify 알고리즘을 이용하여 $\sigma_p = (\sigma_1, \sigma_2)$ 의 정당성을 다음과 같이 확인한다. 우선 σ_1 의 정당성은 $\text{Verify}(\Gamma, pk_a, pk_a || pk_b || W, M, \sigma_1)$ 을 이용해 확인한다. 그리고 σ_2 의 정당성은 $\text{Verify}(\Gamma, pk_b, pk_a || pk_b || W || \sigma_1, M, \sigma_2)$ 을 이용해 확인한다.

[0092] 도 9는 본 발명의 일 실시예에 따라 대리 서명을 생성하는 과정을 상세히 설명하기 위해 도시한 흐름도이다.

[0093] 도 9를 참조하면, 단계(S141)에서 대리 서명자(b)는 시스템 파라미터, 아이디, 위임 권한, 및 메시지를 입력 파라미터로 하는 아이디 기반 서명 기법의 Sign 알고리즘을 사용하여 제1 대리 서명을 생성한다.

[0094] 다음으로, 단계(S143)에서 대리 서명자(b)는 시스템 파라미터, 제1 대리 서명을 포함하는 ID, 및 자신의 비밀키를 입력 파라미터로 하는 Extract 알고리즘을 사용하여 위임 권한을 출력한다.

[0095] 다음으로, 단계(S145)에서 대리 서명자(b)는 시스템 파라미터, 제1 대리 서명을 포함하는 ID, 위임 권한, 및 메시지를 입력 파라미터로 하는 Sign 알고리즘을 사용하여 제2 대리 서명을 생성한다.

[0096] 다음으로, 단계(S147)에서 대리 서명자(b)는 제1 대리 서명 및 제2 대리 서명을 최종 대리 서명으로서 출력한다.

[0097] 본 발명의 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터 판독 가능 매체를 포함한다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크와 같은 자기-광 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별

히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0098]

[0099]

지금까지 본 발명에 따른 구체적인 실시예에 관하여 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서는 여러 가지 변형이 가능함은 물론이다. 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허 청구의 범위뿐 아니라 이 특허 청구의 범위와 균등한 것들에 의해 정해져야 한다.

[0100]

이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 이는 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명 사상은 아래에 기재된 특허청구범위에 의해서만 파악되어야 하고, 이의 균등 또는 등가적 변형 모두는 본 발명 사상의 범주에 속한다고 할 것이다.

[0101]

부호의 설명

[0102]

a: 본 서명자

b: 대리 서명자

c: 검증자

m: 마스터

10: 일반 서명 기능 제공부

11: 시스템 설정 기능 제공부

13: 마스터 키 생성 기능 제공부

15: 사용자 비밀키 생성 기능 제공부

17: 서명 생성 기능 제공부

19: 서명 검증 기능 제공부

100: 시스템 설정부

200: 사용자 키 생성부

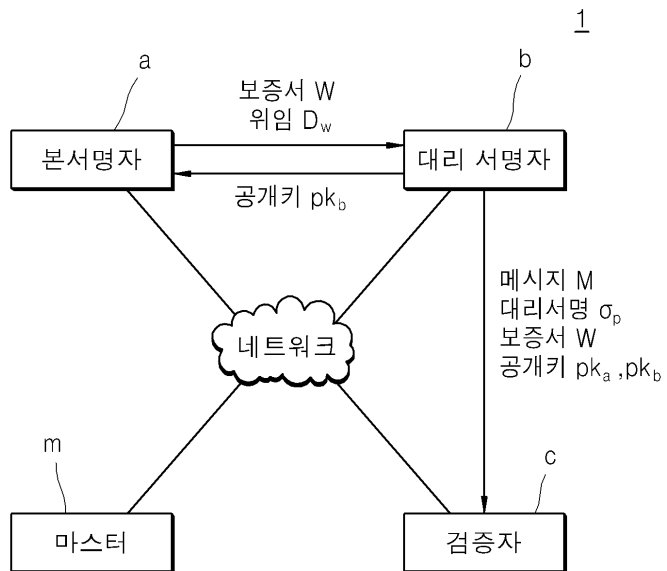
300: 위임 생성부

400: 대리 서명 생성부

500: 대리 서명 검증부

도면

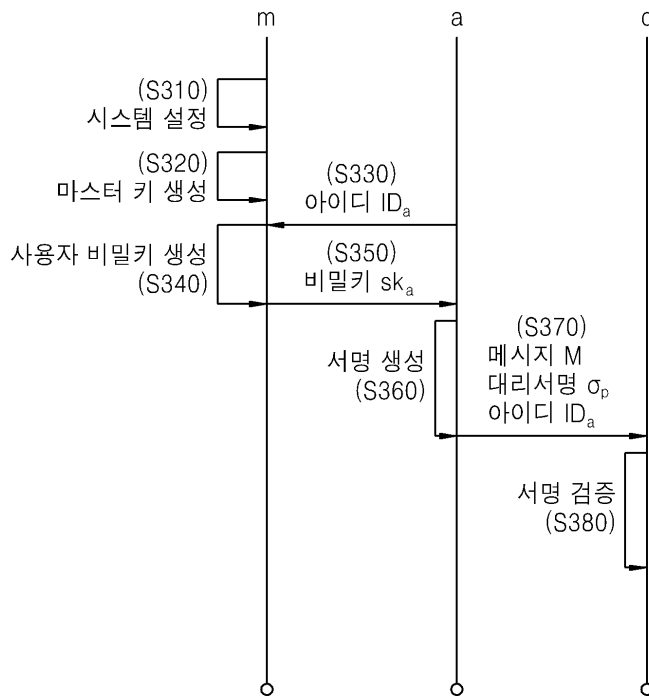
도면1



도면2

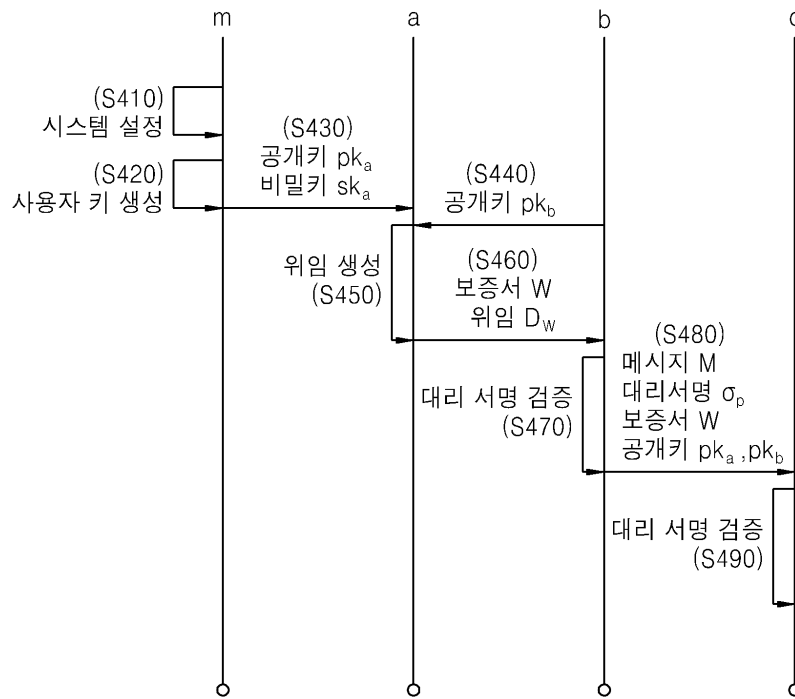


도면3



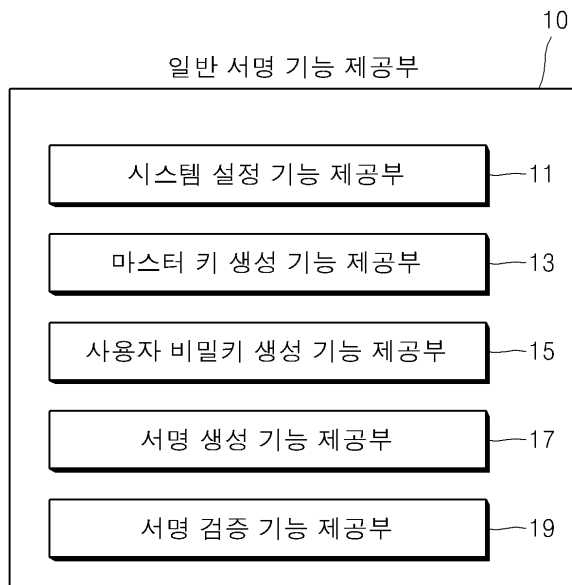
시스템 설정(S310): $\Gamma \leftarrow \text{Setup}(\lambda)$
 마스터 키 생성(S320): $(mpk, msk) \leftarrow \text{KeyGen}(\Gamma)$
 사용자 비밀키 생성(S340): $sk_{ID} \leftarrow \text{Extract}(\Gamma, ID, msk)$
 서명 생성(S360): $\sigma \leftarrow \text{Sign}(\Gamma, ID, sk_{ID}, M)$
 서명 검증(S380): 1 또는 0 $\leftarrow \text{Verify}(\Gamma, mpk, ID, M, \sigma)$

도면4

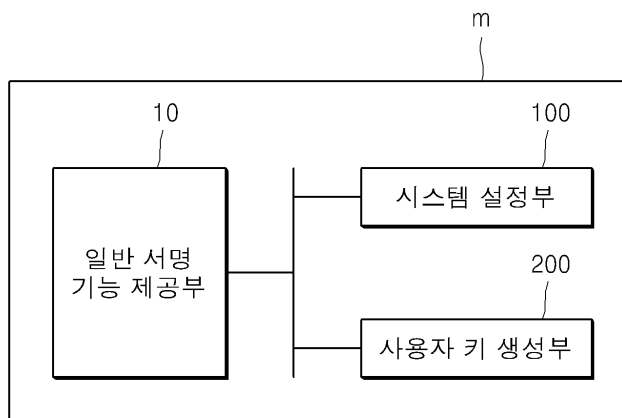


시스템 설정(S410): $\Gamma \leftarrow \text{Setup}(\lambda)$
 사용자 키 생성(S420): $(pk_a, sk_a), (pk_b, sk_b) \leftarrow \text{KeyGen}(\Gamma)$
 위임 생성(S450): $D_w \leftarrow \text{DelGen}(\Gamma, W, pk_b, sk_a)$
 대리 서명 생성(S470): $\sigma_p \leftarrow \text{ProxySign}(\Gamma, W, D_w, sk_b, M)$
 대리 서명 검증(S490): 1 또는 0 $\leftarrow \text{ProxyVerify}(\Gamma, W, M, pk_a, pk_b, \sigma_p)$

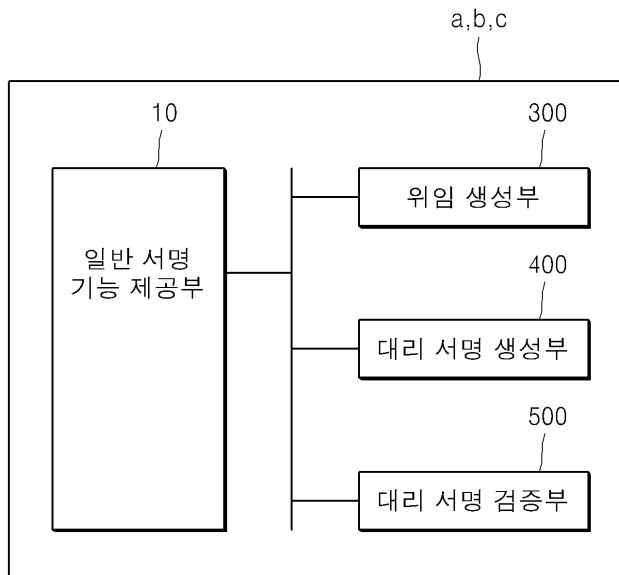
도면5



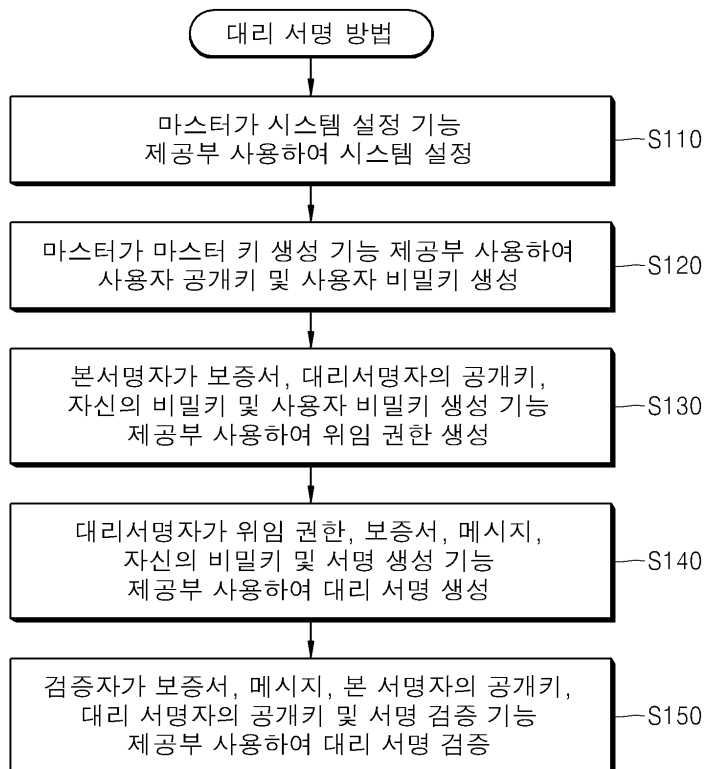
도면6



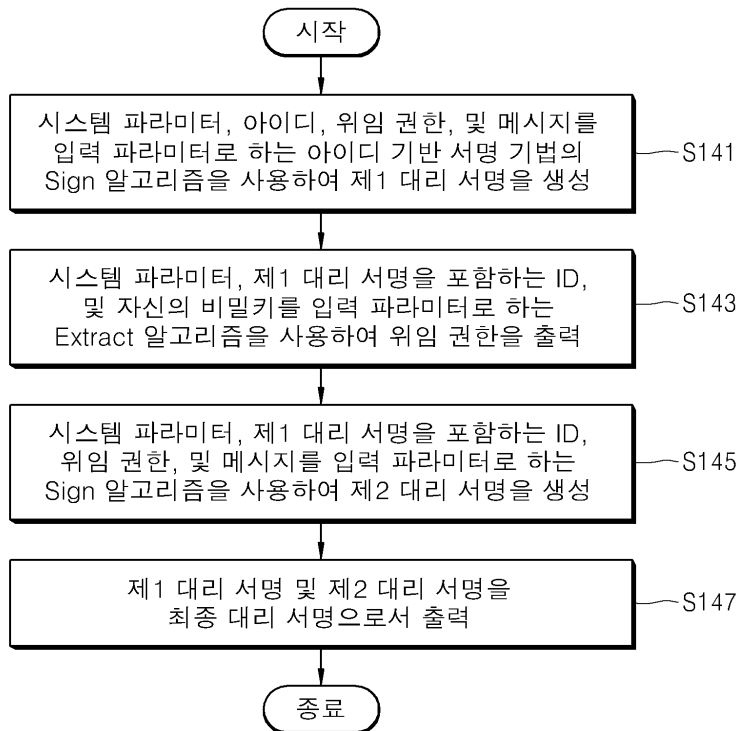
도면7



도면8



도면9



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 4항

【변경전】

상기 사용자 객체

【변경후】

상기 사용자 개체