



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0074791
(43) 공개일자 2014년06월18일

(51) 국제특허분류(Int. Cl.)
G06F 21/00 (2006.01) G06F 21/30 (2013.01)
G06F 15/16 (2006.01)
(21) 출원번호 10-2013-0011575
(22) 출원일자 2013년02월01일
심사청구일자 2013년02월01일
(30) 우선권주장
1020120142991 2012년12월10일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
정익래
서울 광진구 긴고랑로4길 53, 203호 (중곡동, 호동아파트)
김기성
경기 부천시 원미구 상일로 72, 1842동 805호 (상동, 반달마을아파트)
홍준희
서울 중구 다산로 32, 27동 201호 (신당동, 남산타운아파트)
(74) 대리인
특허법인엠에이피에스

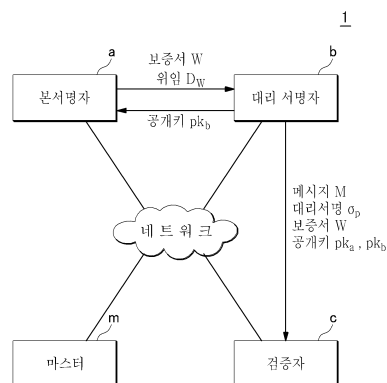
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 대리 서명 시스템 및 방법

(57) 요약

본 발명은 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 개체;를 포함하되, 상기 사용자 개체는 자신의 사용자 비밀키, 대리 서명자 개체의 사용자 공개키, 및 보증서를 사용하여 위임을 생성하여 대리 서명자 개체에게 전송하는 본 서명자 개체; 자신의 사용자 비밀키, 메시지, 및 상기 본 서명자 개체로부터 수신한 위임 및 보증서를 사용하여 대리 서명을 생성하여 검증자 개체에게 전송하는 대리 서명자 개체; 및 상기 대리 서명자 개체로부터 수신한 본 서명자 개체의 사용자 공개키, 대리 서명자 개체의 사용자 공개키, 메시지, 및 보증서를 사용하여 상기 대리 서명을 검증하는 검증자 개체;를 포함하는 시스템을 제공한다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	1415123237
부처명	지식경제부
연구사업명	정보통신기술인력양성
연구과제명	스마트 그리드 기술연구
기 여 율	1/1
주관기관	고려대학교 산학협력단
연구기간	2012.01.01 ~ 2012.12.31

특허청구의 범위

청구항 1

대리 서명 시스템에 있어서,

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 개체;를 포함하되,

상기 사용자 개체는

자신의 사용자 비밀키, 대리 서명자 개체의 사용자 공개키, 및 보증서를 사용하여 위임을 생성하여 대리 서명자 개체에게 전송하는 본 서명자 개체;

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

상기 대리 서명자 개체로부터 수신한 본 서명자 개체의 사용자 공개키, 대리 서명자 개체의 사용자 공개키, 메시지, 및 보증서를 사용하여 상기 대리 서명을 검증하는 검증자 개체;를 포함하는 대리 서명 시스템.

청구항 2

제 1 항에 있어서,

상기 대리 서명 시스템은

상기 일반 서명 기능 제공부와 기능적으로 연결되어 있고, 상기 일반 서명 기능 제공부를 사용하여 상기 사용자 개체의 사용자 공개키 및 사용자 비밀키를 생성하는 마스터 개체;를 더 포함하는 대리 서명 시스템.

청구항 3

제 1 항에 있어서,

상기 일반 서명 기능 제공부는 ID 기반 서명 기법(ID-based signature scheme)을 사용하는 대리 서명 시스템.

청구항 4

제 2 항에 있어서,

상기 일반 서명 기능 제공부는 안전성 레벨 파라미터에 기초하여 시스템 파라미터를 출력하는 시스템 설정 기능 제공부를 포함하며,

상기 마스터 개체는 상기 시스템 설정 기능 제공부를 사용하여 시스템 파라미터를 출력하는 대리 서명 시스템.

청구항 5

제 2 항에 있어서,

상기 일반 서명 기능 제공부는 마스터 공개키 및 마스터 비밀키를 생성하는 마스터 키 생성 기능 제공부를 포함하며,

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

청구항 6

제 1 항에 있어서,

상기 일반 서명 기능 제공부는 사용자 공개키에 대응하는 사용자 비밀키를 생성하는 사용자 비밀키 생성 기능 제공부를 포함하며,

상기 본 서명자 개체는 상기 사용자 비밀키 생성 기능 제공부를 사용하여 상기 위임을 생성하는 대리 서명 시스템.

청구항 7

제 1 항에 있어서,

상기 일반 서명 기능 제공부는 메시지에 대한 전자 서명을 생성하는 서명 생성 기능 제공부를 포함하며,

상기 대리 서명자 개체는 상기 서명 생성 기능 제공부를 사용하여 상기 대리 서명을 생성하는 대리 서명 시스템.

청구항 8

제 1 항에 있어서,

상기 일반 서명 기능 제공부는 서명이 유효한지 검증하는 서명 검증 기능 제공부를 포함하며,

상기 대리 서명자 개체는 상기 서명 검증 기능 제공부를 사용하여 상기 대리 서명을 검증하는 대리 서명 시스템.

청구항 9

제 1 항에 있어서,

상기 일반 서명 기능 제공부는 기지정된 길이의 결과값을 출력하는 해시 함수를 제공하며,

상기 메시지 및 상기 보증서의 길이는 상기 해시 함수가 출력하는 결과값의 길이와 동일한 대리 서명 시스템.

청구항 10

대리 서명 시스템을 사용하는 대리 서명 방법에 있어서,

본 서명자 개체가 자신의 사용자 비밀키, 대리 서명자 개체의 사용자 공개키, 보증서, 및 자신과 기능적으로 연결되어 있는 일반 서명 기능 제공부의 사용자 비밀키 생성 기능 제공부를 사용하여 위임을 생성하는 단계;

대리 서명자 개체가 자신의 사용자 비밀키, 메시지, 상기 본 서명자 개체로부터 수신한 위임 및 보증서, 및 자신과 기능적으로 연결되어 있는 일반 서명 기능 제공부의 서명 생성 기능 제공부를 사용하여 대리 서명을 생성하는 단계; 및

검증자 개체가 상기 대리 서명자 개체로부터 수신한 본 서명자 개체의 사용자 공개키, 대리 서명자 개체의 사용자 공개키, 메시지, 보증서, 및 자신과 기능적으로 연결되어 있는 일반 서명 기능 제공부의 서명 검증 기능 제공부를 사용하여 대리 서명을 검증하는 단계;를 포함하는 대리 서명 방법.

청구항 11

제 10 항에 있어서,

마스터 개체가 자신과 기능적으로 연결되어 있는 일반 서명 기능 제공부의 시스템 설정 기능 제공부를 사용하여 시스템 파라미터를 출력하는 단계; 및

상기 마스터 개체가 상기 일반 서명 기능 제공부의 마스터 키 생성 기능 제공부를 사용하여 사용자 공개키 및 사용자 비밀키를 생성하는 단계;를 더 포함하는 대리 서명 방법.

청구항 12

제 10 항에 있어서,

상기 일반 서명 기능 제공부는 ID 기반 서명 기법(ID-based signature scheme)을 사용하는 대리 서명 방법.

청구항 13

제 10 항에 있어서,

상기 일반 서명 기능 제공부는 기지정된 길이의 결과값을 출력하는 해시 함수를 제공하며,
상기 메시지 및 상기 보증서의 길이는 상기 해시 함수가 출력하는 결과값의 길이와 동일한 대리 서명 방법.

명세서

기술분야

[0001] 본 발명은 대리 서명 시스템 및 방법에 관한 것이다.

배경기술

- [0002] 전자 거래 등 사용자의 신원이 위조되면 곤란한 온라인 활동이 활성화됨에 따라 전자 서명의 중요성이 점점 커지고 있다. 이에 따라, 생성된 서명을 수신한 검증자는 서명자 개체가 해당 서명을 생성하였음을 확인할 수 있어야 한다는 기본적인 요건 뿐 아니라, 제 3 자가 서명을 위조하기 어려워야 하고 서명자 개체는 자신이 서명하였음을 부인하기 어려워야 한다는 등의 안전성 및 신뢰성을 위한 여러 필요 요건을 갖추되, 계산 부하는 되도록 낮은 전자 서명을 생성하고 검증하는 방법에 대한 연구가 활발하게 진행되어오고 있다.
- [0003] 예를 들어, 이미 널리 사용되고 있는 공개키 기반 환경(Public Key Infrastructure: PKI)에서의 서명 기법은 사용자의 ID 등 공개된 식별 정보를 사용자의 공개키로 사용하는 ID 기반 서명 기법(ID-based signature scheme)으로 발전하고 있다. 이는 종래의 공개키 기반 서명 기법과 달리, 공인 인증서 발급 과정이 필요없으므로 효율적이며 자유롭다는 장점이 있다.
- [0004] 더 나아가, 서명 권한을 위임하여 다른 개체가 대신 서명하게 하는 대리 서명 기법(proxy signature scheme)이 개발되어 사용되고 있다. 이는 현실 세계에서 어떤 회사의 간부(본 서명자 개체)가 출장으로 장기간 자리를 비울 경우 업무의 효율성을 위해 자신의 서명 권한을 자신의 비서(대리 서명자 개체)에 위임하는 것에 비유할 수 있다. 본 서명자 개체가 특정 개체를 대리 서명자 개체로 지정하여 위임을 주면, 대리 서명자 개체가 본 서명자 개체를 대신하여 대리 서명을 생성하는 것이다.
- [0005] 이러한 대리 서명 기법은 점점 더 많은 응용에 사용되고 있다. 예를 들어, 위임이 빈번하게 발생하는 분산 컴퓨팅(Distributed Computing) 환경, 그리드 컴퓨팅(Grid Computing), 및 모바일 통신에서 활용된다. 최근에는 이러한 환경들이 복합적으로 존재하는 스마트 그리드 환경이 또 다른 응용 환경으로 각광받고 있다.
- [0006] 예를 들어, 대리 서명과 관련하여 한국공개특허 제10-2009-0061383호("대리 서명을 이용한 도메인 관리 장치 및 방법")에는 콘텐츠 라이선스에 대리 서명을 활용하는 구성이 개시되어 있다.
- [0007] 또한, 한국등록특허 제10-1057650호("사회적 커뮤니티 생성 권한 위임 방법")에는 존 마스터가 대리 서명을 생성하여 커뮤니티 멤버들에게 발급하는 구성이 개시되어 있다.
- [0008] 이러한 대리 서명 기법은 다음과 같은 4가지 성질을 만족해야 한다. 이는 대리 서명이 반드시 만족해야 할 중요한 성질이다.
- [0009] 첫째, 본 서명자 개체는 자신이 본 서명자 개체임에도 불구하고 대리 서명을 생성할 수 없어야 한다. 이러한 개념은 대리 서명자 개체의 프라이버시를 보호함은 물론이고 추후 분쟁의 여지를 없애주는 중요한 성질이다.
- [0010] 둘째, 서명을 확인하는 검증자는 대리 서명이 본 서명자 개체의 동의하에 대리 서명자 개체에 의해 생성되었음을 확인할 수 있어야 한다.
- [0011] 셋째, 검증자는 대리 서명자 개체의 신원을 확인할 수 있어야 한다.
- [0012] 넷째, 대리 서명자 개체는 자신의 서명에 대해 부인할 수 없어야 한다.
- [0013] 대리 서명 시스템은 일반적인 전자 서명에서의 본 서명자 개체와 검증자라는 두 개체 이외에 대리 서명자 개체라는 또다른 개체가 더 필요하므로, 일반 서명보다 구조가 복잡하다. 따라서 대리 서명 시스템을 일반 전자 서명 기법을 활용하여 구축한다면, 대리 서명 생성 시스템을 위한 별개의 방법을 개발하는 것보다 효율적일 것이다. 대리 서명 시스템을 일반 전자 서명 시스템과 연계하여 개발하면, 기반이 되는 일반 전자 서명 기법의 안전성 및 효율성이 향상되면 대리 서명 시스템의 안전성 및 효율성 또한 향상되는 효과 또한 기대할 수 있을 것이다.

발명의 내용

해결하려는 과제

[0014] 본 발명은 전술한 문제를 해결하기 위한 것으로서, 그 목적은 일반 전자 서명 기법을 사용하여 대리 서명을 생성하고 검증하는 대리 서명 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0015] 상기와 같은 목적을 달성하기 위한 본 발명의 제 1 측면에 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 개체;를 포함하되, 상기 사용자 개체는 자신의 사용자 비밀키, 대리 서명자 개체의 사용자 공개키, 및 보증서를 사용하여 위임을 생성하여 대리 서명자 개체에게 전송하는 본 서명자 개체; 자신의 사용자 비밀키, 메시지, 및 상기 본 서명자 개체로부터 수신한 위임 및 보증서를 사용하여 대리 서명을 생성하여 검증자 개체에게 전송하는 대리 서명자 개체; 및 상기 대리 서명자 개체로부터 수신한 본 서명자 개체의 사용자 공개키, 대리 서명자 개체의 사용자 공개키, 메시지, 및 보증서를 사용하여 상기 대리 서명을 검증하는 검증자 개체;를 포함하는 것을 특징으로 한다.

[0016] 상기와 같은 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 대리 서명 방법은 본 서명자 개체가 자신의 사용자 비밀키, 대리 서명자 개체의 사용자 공개키, 보증서, 및 자신과 기능적으로 연결되어 있는 일반 서명 기능 제공부의 사용자 비밀키 생성 기능 제공부를 사용하여 위임을 생성하는 단계; 대리 서명자 개체가 자신의 사용자 비밀키, 메시지, 상기 본 서명자 개체로부터 수신한 위임 및 보증서, 및 자신과 기능적으로 연결되어 있는 일반 서명 기능 제공부의 서명 생성 기능 제공부를 사용하여 대리 서명을 생성하는 단계; 및 검증자 개체가 상기 대리 서명자 개체로부터 수신한 본 서명자 개체의 사용자 공개키, 대리 서명자 개체의 사용자 공개키, 메시지, 보증서, 및 자신과 기능적으로 연결되어 있는 일반 서명 기능 제공부의 서명 검증 기능 제공부를 사용하여 대리 서명을 검증하는 단계;를 포함하는 것을 특징으로 한다.

발명의 효과

[0017] 본 발명은 전자 서명 시스템 및 방법에 있어, 일반 전자 서명 기법을 활용하여 대리 서명을 생성하고 검증하는 대리 서명 시스템 및 방법을 제공하는 효과를 얻는다.

[0018] 일반 전자 서명과 대리 서명 시스템 및 방법을 별개의 기술로 개발할 필요 없이, 기존에 존재하는 일반 전자 서명 시스템을 기초로 하여 대리 서명 시스템 및 방법을 구성할 수 있으므로 효율적이다. 특히 전자 서명은 복잡하고 어려운 수학적 난제에 기초하여 만들어지므로, 안전하면서도 계산 부하는 낮은 전자 서명 시스템 및 방법을 개발하는 것은 쉬운 일이 아니기 때문에, 일반 전자 서명 시스템보다 구성이 좀더 복잡한 대리 서명 시스템을 별도로 개발하는 것은 더욱 어려울 수 있다. 따라서 대리 서명 시스템 및 방법을 일반 전자 서명 기법이 제공하는 기능을 사용하여 구축하는 것이 효율적이다.

[0019] 게다가, 대리 서명 시스템의 기반이 되는 일반 전자 서명 기법의 안전성 및 효율성을 향상시키면, 대리 서명 시스템의 안전성 및 효율성 또한 향상된다는 장점이 있다. 예를 들어, 기반이 되는 일반 전자 서명 기법을 공개키 기반에서 ID 기반으로 향상시키면, 이를 활용한 대리 서명 시스템의 안전성 및 효율성 또한 향상된다. 또한 일반 전자 서명 기법이 기초하는 수학적 난제에 대해서도, 평균적인 경우 어려운 것으로 알려져 있는 이산 대수 문제의 어려움에 기반하는 일반 전자 서명에서 최악의 경우에도 풀기 어려우면서도 계산 부하가 낮은 것으로 알려져 있는 래티스(lattice) 상에서의 SIS(small integer solution) 문제의 어려움에 기반을 두는 일반 전자 서명으로 변경한다면, 대리 서명 시스템을 다시 설계하지 않아도 대리 서명 시스템의 안전성 및 효율성이 향상된다.

도면의 간단한 설명

[0020] 도 1은 본 발명의 일실시예에 따른 대리 서명 시스템의 구조를 도시함.

도 2는 종래의 공개키 기반 서명 시스템의 동작 흐름을 도시함.

도 3은 종래의 ID 기반 서명 시스템의 동작 흐름을 도시함.

도 4는 종래의 대리 서명 시스템의 동작 흐름을 도시함.

도 5는 본 발명의 일실시예에 따른 일반 서명 기능 제공부를 도시함.

도 6은 본 발명의 일실시예에 따른 일반 서명 기능 제공부를 자세히 도시함.

도 7은 본 발명의 일실시예에 따른 마스터 개체를 도시함.

도 8은 본 발명의 일실시예에 따른 마스터 개체를 자세히 도시함.

도 9은 본 발명의 일실시예에 따른 사용자 개체를 도시함.

도 10은 본 발명의 일실시예에 따른 사용자 개체를 자세히 도시함.

도 11은 본 발명의 일실시예에 따른 대리 서명 방법의 흐름을 도시함.

발명을 실시하기 위한 구체적인 내용

- [0021] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [0022] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.
- [0023] 도 1은 본 발명의 일실시예에 따른 대리 서명 시스템의 구조를 도시하고 있다.
- [0024] 본 발명의 일실시예에 따른 대리 서명 시스템(1)에는 네트워크를 통해 연결된 본 서명자(a), 대리 서명자(b), 및 검증자(c)를 포함하는 사용자 개체(entity)가 참여한다.
- [0025] 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.
- [0026] 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 수도 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.
- [0027] 본 발명의 일실시예에 따른 대리 서명 시스템(1)은 공개키 기반 환경(Public Key Infrastructure: PKI)에서 구현될 수 있으며, 각 사용자의 사용자 공개키 및 사용자 비밀키를 생성하여 해당 사용자에게 배포하는 마스터(m) 개체가 본 발명의 일실시예에 따른 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.
- [0028] 본 서명자(a)는 자신의 사용자 비밀키, 대리 서명자(b)의 사용자 공개키, 및 보증서를 사용하여 위임을 생성하고, 대리 서명자(b)는 자신의 사용자 비밀키, 메시지, 본 서명자(a)로부터 수신한 위임 및 보증서를 사용하여 대리 서명을 생성하며, 검증자(c)는 대리 서명자(b)로부터 수신한 본 서명자(a)의 사용자 공개키, 대리 서명자(b)의 사용자 공개키, 메시지, 및 보증서를 사용하여 대리 서명을 검증한다.
- [0029] 따라서 도면에 도시되어 있는 바와 같이, 각 사용자 개체는 보증서, 위임, 메시지, 및 대리 서명 등을 주고받을 수 있으며, 각 사용자 개체의 사용자 공개키를 더 주고받을 수 있다. 또는 일실시예에서 사용자 공개키는 미리 공개되어, 각 사용자 개체가 자신의 사용자 공개키를 상대방 개체에게 전송하는 과정없이 접근될 수 있다. 또한, 도시되어 있지 않지만, 마스터(m)가 각 사용자의 사용자 공개키 및 사용자 비밀키를 생성하여 각 사용자

에게 전송할 수 있다.

- [0030] 전술한 바와 같이, 본 발명의 일실시예에 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 기반이 되는 일반 전자 서명 기법으로 사용한다.
- [0031] ID 기반 서명 기법은 ID, 이메일 등의 이미 공개되어 있는 사용자 식별정보를 사용자의 공개키로 사용하여, 마스터(m)가 각 사용자에게 공인 인증서, 즉 공개 키 인증서(public key certificate)를 발급할 필요를 없앤 일반 전자 서명 기법이다. 사용자의 공개키가 해당 사용자의 것임을 보증하기 위해, 인증 기관이 자신의 마스터 비밀키로 각 사용자의 공개키에 서명하는 과정이 필요없으므로, 종래의 공개키 기반 전자 서명 기법보다 효율성 및 안전성이 높다.
- [0032] 이에 대해서는 도 5 내지 도 9를 통해 자세히 기술할 것이며, 먼저 도 2 내지 도 4를 통해 종래의 일반 전자 서명 및 대리 서명 시스템에서의 메시지 및 동작의 흐름을 설명한다.
- [0033] 도 2는 종래의 공개키 기반 서명 시스템에서 교환되는 정보의 간략한 흐름을 도시하고 있다.
- [0034] 먼저, 마스터(m)가 사용자 공개키, 사용자 비밀키, 및 사용자 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 사용자 공개키, 사용자 비밀키, 및 인증서가 전송된다.
- [0035] 다음, 본 서명자(a)가 메시지에 서명하여 자신의 사용자 공개키 및 인증서와 함께 검증자(c)에게 전송한다(S220).
- [0036] 서명을 생성하고 검증하는 등의 각 개체의 동작의 흐름은 도 3과 유사하므로 도시하지 않았다. 도2와 도 3의 정보 흐름을 비교해보면, 전술한 바와 같이, ID 기반 서명 기법에서는 인증서가 필요없으며, 사용자 공개키 대신 사용자의 아이디가 사용됨을 알 수 있다.
- [0037] 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.
- [0038] 먼저, 마스터(m)가 시스템을 설정한다(S310). 시스템 설정 단계(S310)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, 공지된 기술이므로 설명을 생략한다.
- [0039] 다음, 마스터(m)는 설정된 시스템 파라미터를 사용하여 마스터 공개키 및 마스터 비밀키를 생성한다(S320). 예를 들어, 마스터(m)는 상기 시스템 설정 단계(S310)에서 설정된 시스템 파라미터에 의해 행의 수 및 열의 수가 결정되는 트랩도어(trapdoor) 행렬을 생성함으로써 이를 수행할 수 있다. 이때 전술한 바와 같이, 기반이 되는 수학적 난제를 변경하면 전체 전자 서명 시스템의 안전성 또는 효율성이 향상될 수 있다.
- [0040] 도시되어 있지 않지만, 상기 단계들(S310, S320)에서 출력된 시스템 파라미터 및 마스터 공개키는 시스템의 모든 사용자 개체에게 공개된다.
- [0041] 다음, 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.
- [0042] 다음, 본 서명자(a)가 자신의 사용자 비밀키로 메시지에 서명하여(S360), 서명된 메시지를 자신의 ID와 함께 검증자(c)에게 전송한다(S370).
- [0043] 다음, 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.
- [0044] 도 4는 종래의 대리 서명 시스템의 동작 흐름을 각 개체의 동작에 사용되는 알고리즘의 입력값 및 출력값을 포함하는 명세와 함께 도시하고 있다.

- [0045] 먼저, 마스터(m)가 시스템을 설정하고(S410), 사용자 공개키 및 사용자 비밀키를 생성하여(S420), 사용자에게 전송한다(S430). 도면에는 본 서명자(a)에 대하여 수행하는 것만 도시되어 있으나, 각 사용자에게 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 사용자 공개키 및 사용자 비밀키를 생성할 수 있다.
- [0046] 다음, 본 서명자(a)가 대리 서명자(b)로부터 수신한(S440) 대리 서명자(b)의 사용자 공개키 및 자신의 사용자 비밀키를 사용하여 보증서로부터 위임을 생성하고(S450), 생성된 위임을 보증서와 함께 대리 서명자(b)에게 전송한다(S460).
- [0047] 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.
- [0048] 다음, 대리 서명자(b)가 수신한 보증서 및 위임을 기초로 자신의 사용자 비밀키를 사용하여 메시지에 서명하여(S470), 검증자(c)에게 본 서명자(a)의 사용자 공개키 및 자신의 사용자 공개키와 함께 전송한다(S480).
- [0049] 다음, 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.
- [0050] 전술한 바와 같이, 이러한 대리 서명 기법을 일반 서명 기법과 별도로 개발하는 것보다 일반 서명 기법을 기초로 하여 대리 서명 기법을 개발하는 것이 훨씬 효율적이며, 이러한 본발명의 목적을 달성하기 위해 본 발명의 일실시예에 따른 대리 서명 시스템(1)은 기반이 되는 일반 전자 서명 기법으로 ID 기반 서명 기법을 사용한다.
- [0051] 도 5 내지 도 10을 통해 이를 설명한다.
- [0052] 도 5 내지 도 6에 도시되어 있는 일반 서명 기능 제공부(10)는 도 7 내지 도 8, 및 도 9 내지 도 10에 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 각 도면에서 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.
- [0053] 본 발명의 일실시예에 따른 대리 서명 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 일실시예에서 메시지와 보증서의 길이는 해시 함수가 출력하는 해시값의 길이와 동일할 수 있다. 본 명세서에서 해시 함수는 H()로 도시하였다.
- [0054] 도 5는 본 발명의 일실시예에 따른 일반 서명 기능 제공부를 도시하고 있다.
- [0055] 본 발명의 일실시예에 따른 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.
- [0056] 도 6을 통해 자세히 살펴보면, 시스템 설정 기능 제공부(11)는 시스템을 설정하는 L.Setup을 제공한다.
- [0057] 즉, 안전성 레벨 파라미터를 입력 받고(S11_100), 이를 기초로 시스템 파라미터를 출력한다(S11_200).
- [0058] 마스터 키 생성 기능 제공부(13)는 마스터 공개키 및 마스터 비밀키를 생성하는 L.KeyGen을 제공한다.
- [0059] 즉, 시스템 파라미터를 입력받고(S13_100), 이를 기초로 마스터 공개키 및 마스터 비밀키를 출력한다(S13_200). 도 3에서 설명한 바와 같이, 마스터 공개키는 공개된다(S13_300).
- [0060] 사용자 비밀키 생성 기능 제공부(15)는 마스터 비밀키로 사용자의 ID에 대응하는 사용자 비밀키를 발급하는 L.Extract를 제공한다.
- [0061] 즉, 시스템 파라미터, 사용자의 ID, 마스터 비밀키를 입력받아(S15_100), ID에 대응하는 사용자 비밀키를 출력한다(S15_200).

- [0062] 서명 생성 기능 제공부(17)는 사용자 비밀키를 이용해 메시지에 서명하는 L.Sign를 제공한다.
- [0063] 즉, 시스템 파라미터, 본 서명자의 ID, ID에 대응하는 사용자 비밀키, 메시지를 입력받아(S17_100), 메시지에 대한 서명을 출력한다(S17_200).
- [0064] 서명 검증 기능 제공부(19)는 사용자 ID를 사용해 서명을 검증하는 L.Verify를 제공한다.
- [0065] 즉, 시스템 파라미터, 본 서명자의 ID, 메시지, 메시지에 대한 서명을 입력받아(S19_100), 정당한 서명이면 (S19_200), 1을 출력하고(S19_300), 아니면 0을 출력한다(S19_400).
- [0066] 도 7은 본 발명의 일실시예에 따른 마스터 개체를 도시하고 있다.
- [0067] 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 사용자 공개키 및 사용자 비밀키를 생성한다.
- [0068] 도 8을 통해 자세히 살펴보면, 시스템 설정부(100)의 PS.Setup는 일반 서명 기능 제공부(10)가 제공하는 L.Setup를 사용하여 시스템을 설정한다.
- [0069] 즉, L.Setup에 안전성 레벨 파라미터를 넘긴 후, 그 출력값으로 시스템 파라미터를 설정한다(S100_100).
- [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.
- [0071] 즉, L.KeyGen가 출력한 결과를 본 서명자(a)를 위한 사용자 공개키 및 사용자 비밀키로 출력하고(S200_100), L.KeyGen가 출력한 결과를 대리 서명자(b)를 위한 사용자 공개키 및 사용자 비밀키로 출력한다(S200_200). 본 서명자(a)를 위한 단계와 대리 서명자(b)를 위한 단계만이 도시되어 있으나, 이는 일반 서명 기능 제공부(10)가 제공하는 마스터 공개키 및 마스터 비밀키를 어떻게 각 사용자 개체의 사용자 공개키 및 사용자 비밀키로 사용하는지를 설명하기 위한 예시일 뿐으로, 다른 사용자에 대해서도 이러한 단계를 수행한다.
- [0072] 도 9은 본 발명의 일실시예에 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] 도 10을 통해 자세히 살펴보면, 본 서명자(a)에 의해 사용되는 위임 생성부(300)의 PS.DeIGen는 일반 서명 기능 제공부(10)의 L.Extract를 사용하여 위임을 생성한다.
- [0075] 즉, L.Extract의 ID 입력 부분에 보증서를, 마스터 비밀키 입력 부분에 본 서명자의 사용자 비밀키를 입력하고, 출력되는 ID에 대응되는 사용자 비밀키를 위임으로 사용한다(S300_100).
- [0076] 대리 서명자(b)에 의해 사용되는 대리 서명 생성부(400)의 PS.ProxySign는 일반 서명 기능 제공부(10)의 L.Sign을 사용하여 대리 서명을 생성한다.
- [0077] 즉, 먼저, L.Sign의 ID 입력 부분에 보증서를, 사용자 비밀키 입력 부분에 위임을 입력하여 제 1 서명을 생성한다(S400_100).
- [0078] 다음, 난수를 뽑아 제 1 서명과 연결한 값을 해시하여 제 1 보증서를 생성한다(S400_200).
- [0079] 다음, L.Extract의 ID 입력 부분에 제 1 보증서를, 마스터 비밀키 입력 부분에 대리 서명자(b)의 비밀키를 입력하여 제 1 위임을 생성한다(S400_300).
- [0080] 다음, L.Sign의 ID 입력 부분에 제 1 보증서를, 사용자 비밀키 입력 부분에 제 1 위임을 입력하여 제 2 서명을 생성한다(S400_400).
- [0081] 다음, 제 1 서명과 제 2 서명, 및 난수의 결합을 대리 서명으로 출력한다(S400_500).
- [0082] 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.
- [0083] 즉, 먼저, 제 1 서명의 정당성을 L.Verify의 마스터 공개키 입력 부분에 본 서명자(a)의 사용자 공개키를, ID 입력 부분에 보증서를, 서명 입력 부분에 제 1 서명을 입력하여 확인한다(S500_100).

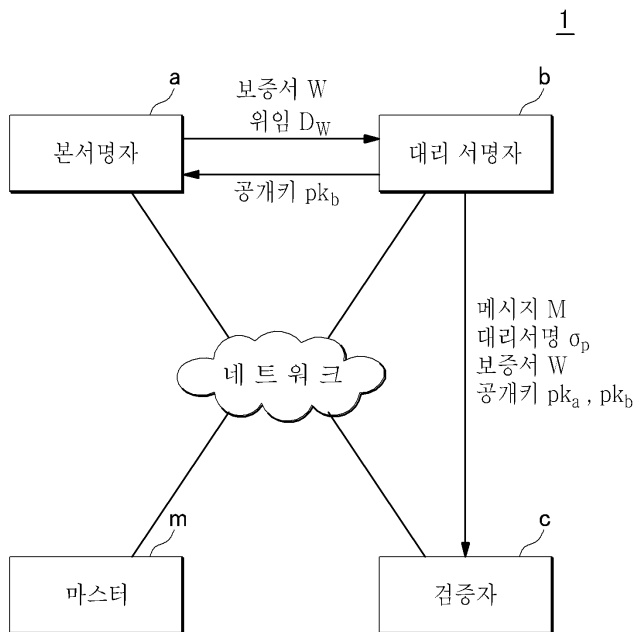
- [0084] 다음, 제 2 서명의 정당성을 L.Verify의 마스터 공개키 입력 부분에 대리 서명자(b)의 사용자 공개키를, ID 입력 부분에 제 1 보증서를, 서명 입력 부분에 제 2 서명을 입력하여 확인한다(S500_200). 이때 제 1 보증서는 난수와 제 1 서명을 연결한 값을 해시한 것이다.
- [0085] 도 11은 본 발명의 일실시예에 따른 대리 서명 방법의 흐름을 도시하고 있다.
- [0086] 마스터(m)가 자신과 기능적으로 연결된 일반 서명 기능 제공부(10)의 시스템 설정 기능 제공부(11)를 사용하여 시스템을 설정하고(S110), 마스터 키 생성 기능 제공부(13)를 사용하여 각 사용자의 사용자 공개키 및 사용자 비밀키를 생성하고 분배한다(S120).
- [0087] 다음, 본 서명자(a)가 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 위임을 생성하여 대리 서명자(b)에게 전송한다(S130).
- [0088] 대리 서명자(b)가 위임, 보증서, 메시지, 자신의 비밀키 및 자신과 기능적으로 연결된 일반 서명 기능 제공부(10)의 서명 생성 기능 제공부(17)를 사용하여 대리 서명을 생성하여 검증자(c)에게 전송한다(S140).
- [0089] 검증자(c)가 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(S150).
- [0090] 진술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.
- [0091] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

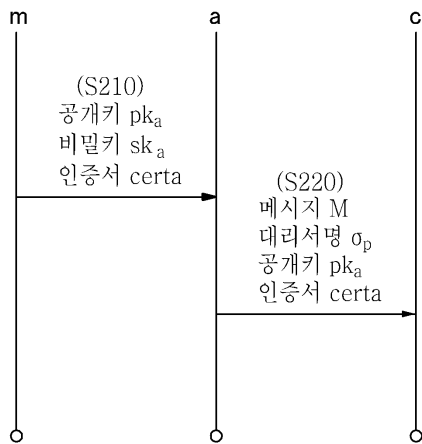
- [0092] a: 본 서명자
b: 대리 서명자
c: 검증자
m: 마스터
10: 일반 서명 기능 제공부

도면

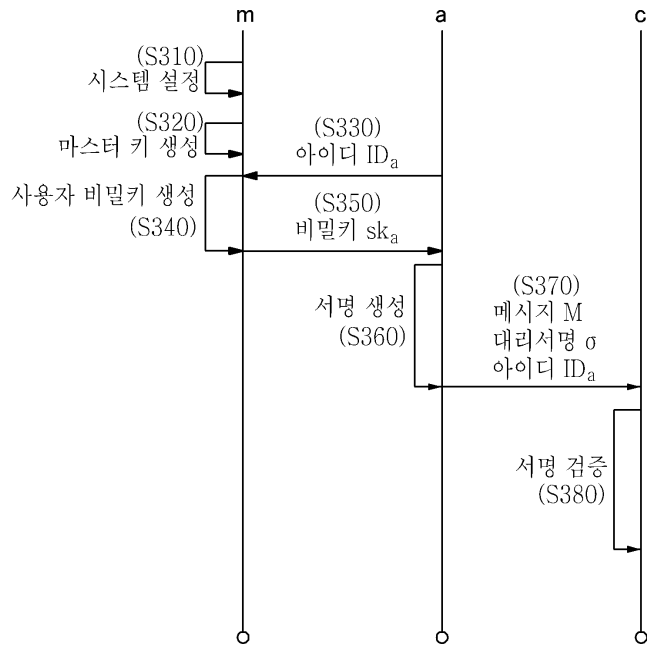
도면1



도면2

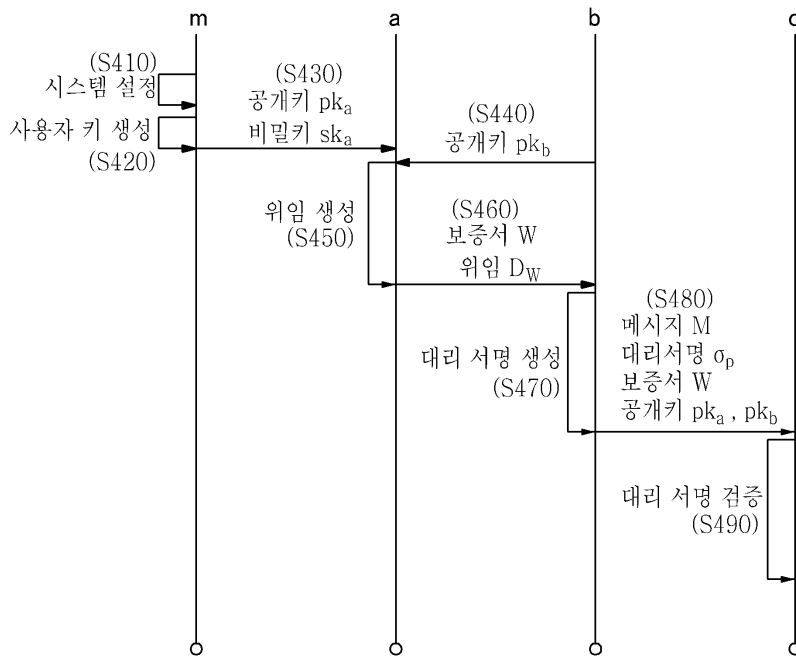


도면3



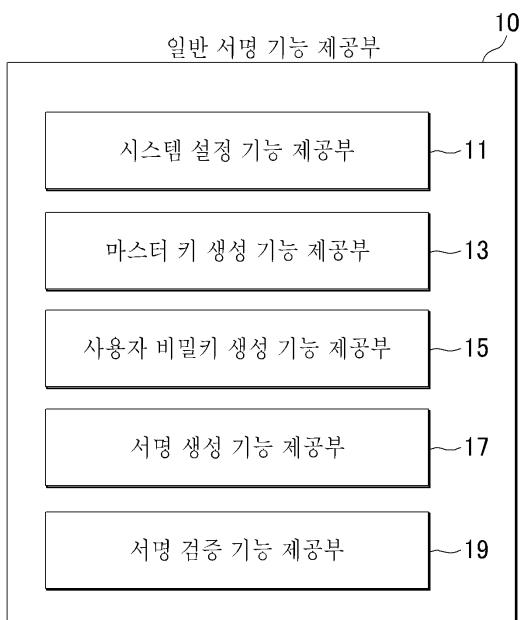
시스템 설정(S310): $\Gamma \leftarrow \text{Setup}(\lambda)$
 마스터 키 생성(S320): $(mpk, msk) \leftarrow \text{KeyGen}(\Gamma)$
 사용자 비밀키 생성(S340): $sk_{ID} \leftarrow \text{Extract}(\Gamma, ID, msk)$
 서명 생성(S360): $\sigma \leftarrow \text{Sign}(\Gamma, ID, sk_{ID}, M)$
 서명 검증(S380): $1 \text{ 또는 } 0 \leftarrow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

도면4

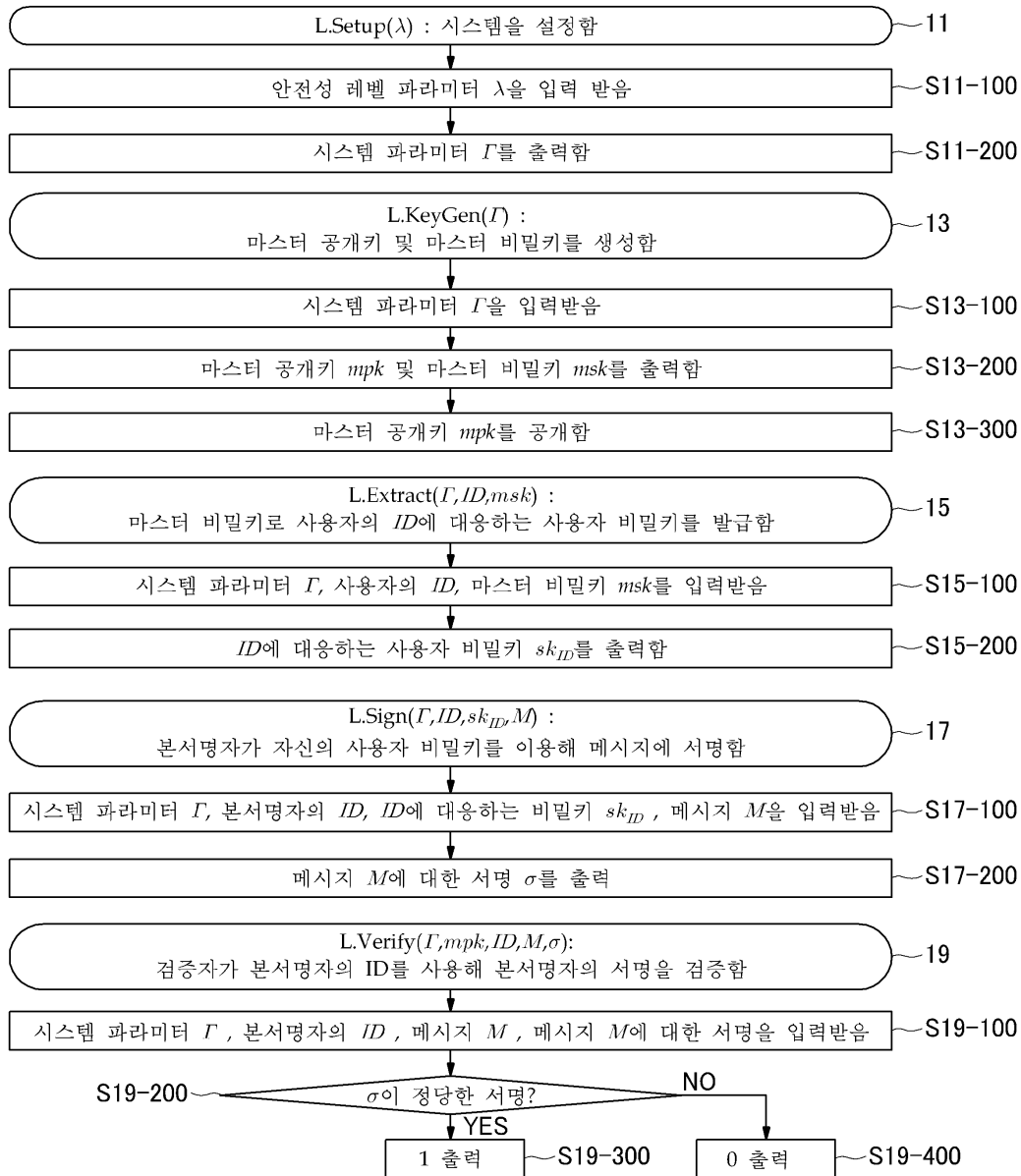


시스템 설정(S410): $\Gamma \leftarrow \text{Setup}(\lambda)$
 사용자 키 생성(S420): $(pk_a, sk_a), (pk_b, sk_b) \leftarrow \text{KeyGen}(\Gamma)$
 위임 생성(S450): $D_W \leftarrow \text{DelGen}(\Gamma, W, pk_b, sk_a)$
 대리 서명 생성(S470): $\sigma_p \leftarrow \text{ProxySign}(\Gamma, W, D_W, sk_b, M)$
 대리 서명 검증(S490):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

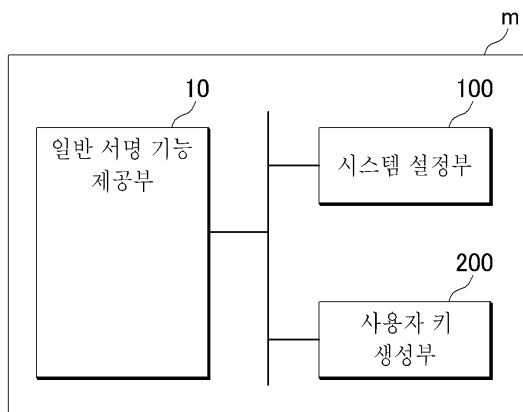
도면5



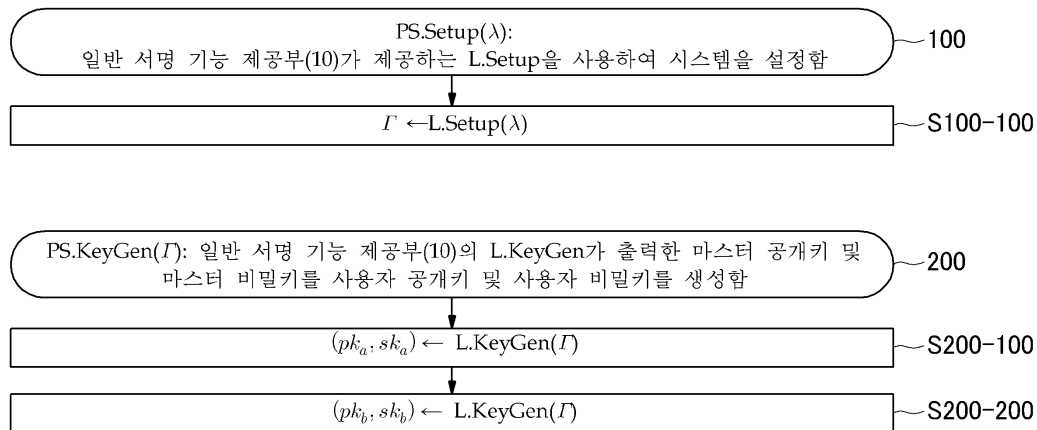
도면6



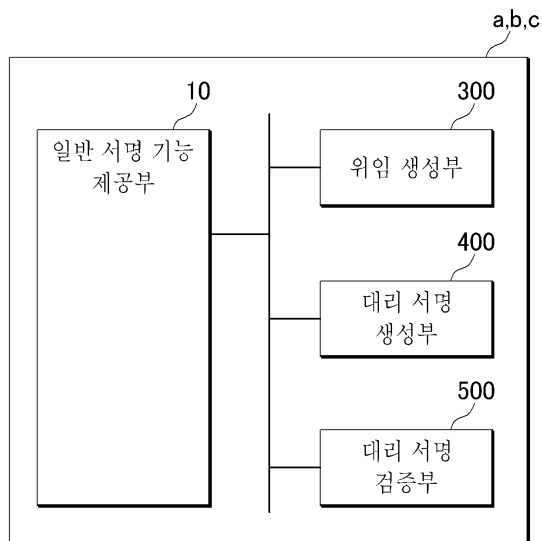
도면7



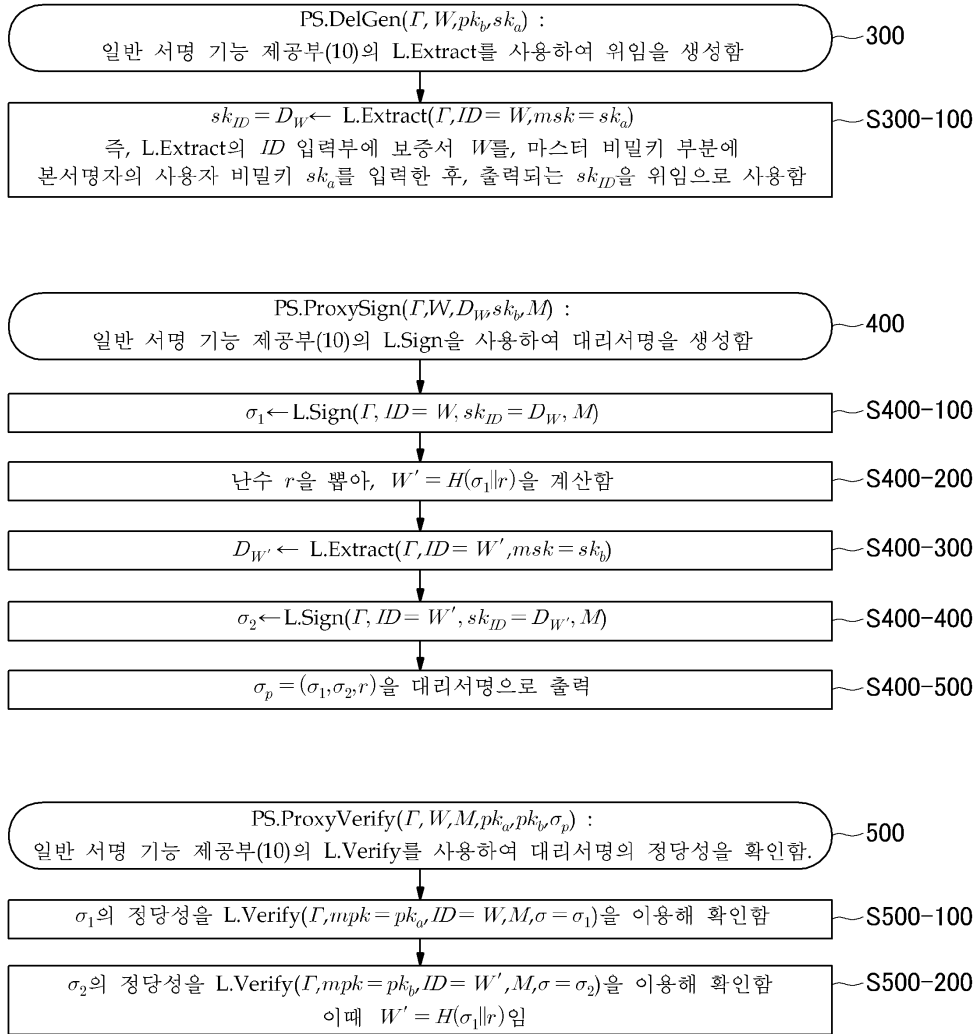
도면8



도면9



도면10



도면11

