(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년04월07일
(11) 등록번호 10-1382626
(24) 등록일자 2014년04월01일

(51) 국제특허분류(Int. Cl.)
*H04L 9/30* (2006.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2013-0000754
(22) 출원일자 2013년01월03일
심사청구일자 2013년01월03일
(56) 선행기술조사문헌
[이지선 외 2인, '키 노출 공격에 안전한 ID-기반의 강한 지정된 검증자 서명 기법', 한국콘텐츠학회논문지 제9권제10호, 59~66페이지, 2009.10.
US20070165843 A1
KR1020120071884 A

(73) 특허권자
**고려대학교 산학협력단**
서울시 성북구 안암로 145 (안암동)
(72) 발명자
**정익래**
서울 광진구 긴고랑로4길 53, 203호 (중곡동, 호동아파트)
**노건태**
서울 강남구 개포로 516, 707동 1304호 (개포동, 개포동주공아파트)
**천지영**
서울 성북구 오패산로 46, 118동 104호 (하월곡동, 월곡두산위브아파트)
(74) 대리인
**특허법인엠에이피에스**

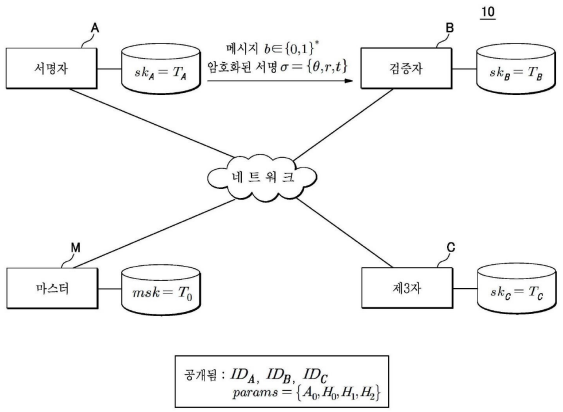
전체 청구항 수 : 총 17 항 심사관 : 이병수

(54) 발명의 명칭 **ID 기반의 강한 지정된 검증자 서명 시스템 및 방법**

## (57) 요 약

본 발명은 사용자 개체의 공개된 식별 정보를 상기 사용자 개체의 사용자 공개키로 사용하여, 상기 사용자 공개키에 대응되는 사용자 비밀키를 생성하여 상기 사용자 개체에게 할당하는 마스터 개체;를 포함하되, 상기 사용자 개체는 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 검증자 개체의 공개된 식별 정보를 사용하여 서명한 메시지를 상기 검증자 개체에게 전송하는 서명자 개체; 및 상기 서명자 개체로부터 수신한 서명을 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 상기 서명자 개체의 공개된 식별 정보를 사용하여 검증하는 검증자 개체;를 포함하는 전자 서명 시스템을 제공한다.

## 대 표 도



이 발명을 지원한 국가연구개발사업

| | |
|---|---|
| 과제고유번호 | 1345188176 |
| 부처명 | 교육과학기술부 |
| 연구사업명 | 여성과학자지원사업 |
| 연구과제명 | 래티스 기반의 효율적인 서명 및 인증 기법 연구 |
| 기 여 율 | 1/1 |
| 주관기관 | 고려대학교산학협력단 |
| 연구기간 | 2012.05.01 ~ 2013.04.30 |

## *특허청구의 범위*

**청구항 1**

전자 서명 시스템에 있어서,

사용자 개체의 공개된 식별 정보를 상기 사용자 개체의 사용자 공개키로 사용하여, 상기 사용자 공개키에 대응되는 사용자 비밀키를 생성하여 상기 사용자 개체에게 할당하는 마스터 개체;를 포함하되,

상기 사용자 개체는

자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 검증자 개체의 공개된 식별 정보를 사용하여 서명한 메시지를 상기 검증자 개체에게 전송하는 서명자 개체; 및

상기 서명자 개체로부터 수신한 서명을 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 상기 서명자 개체의 공개된 식별 정보를 사용하여 검증하는 검증자 개체;를 포함하며,

상기 마스터 개체는 래티스(lattice) 상에서의 SIS(small integer solution) 문제의 어려움에 기반하여, 마스터 비밀키로 사용할 트랩도어(trapdoor)를 생성하고, 상기 사용자 공개키를 사용하여 상기 트랩도어를 더 큰 차원(dimension)을 갖도록 확장하여 상기 확장된 트랩도어를 상기 사용자 비밀키로 출력하되,

상기 트랩도어는 일련의 래티스 벡터가 모인 행렬인 전자 서명 시스템.

**청구항 2**

삭제

**청구항 3**

제 1 항에 있어서,

상기 트랩도어는

행렬 차원 파라미터, 크기 파라미터를 포함하는 보안 파라미터에 기초하여 균일한 분포(uniform distribution)에서 선택된 랜덤(random)한 값을 가지도록 생성되는 행렬인 제 1 행렬에 대응 관계를 가지며, 역행렬이 존재하고, 모든 행의 크기가 특정 임계값보다 작은 행렬이며,

상기 대응 관계는 상기 제 1 행렬과 상기 트랩도어의 곱은 상기 크기 파라미터와의 나머지 연산이 0이 되는 것인 전자 서명 시스템.

**청구항 4**

제 1 항에 있어서,

상기 서명자 개체는 상기 확장된 트랩도어에서 추출한 래티스 벡터를 상기 서명에 사용하는 전자 서명 시스템.

**청구항 5**

제 4 항에 있어서,

상기 서명자 개체는 상기 추출한 래티스 벡터를 난수 및 에러 벡터를 사용하여 가공하여 서명을 생성하는 전자 서명 시스템.

**청구항 6**

제 1 항에 있어서,

상기 트랩도어에서 래티스 벡터를 추출하는 데에 가우시안 샘플링(Gaussian Sampling)이 사용되는 전자 서명 시스템.

**청구항 7**

제 3 항에 있어서,

상기 마스터 개체는 상기 보안 파라미터에 기초하여 일련의 해시(hash) 함수를 선택하며,

상기 제 1 행렬과 상기 일련의 해시 함수는 공개되는 전자 서명 시스템.

**청구항 8**

제 1 항에 있어서,

상기 검증자 개체는

자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 상기 서명자 개체의 공개된 식별 정보를 사용하여 상기 서명자 개체로부터 수신한 서명을 생성할 수 있는 전자 서명 시스템.

**청구항 9**

전자 서명 방법에 있어서,

(a) 마스터 개체가 서명자 개체 및 검증자 개체를 포함하는 사용자 개체의 공개된 식별 정보를 상기 사용자 개체의 사용자 공개키로 사용하여, 상기 사용자 공개키에 대응되는 사용자 비밀키를 생성하여 상기 사용자 개체에게 할당하는 단계;

(b) 서명자 개체가 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 검증자 개체의 공개된 식별 정보를 사용하여 서명한 메시지를 상기 검증자 개체에게 전송하는 단계; 및

(c) 검증자 개체가 상기 서명자 개체로부터 수신한 서명을 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 상기 서명자 개체의 공개된 식별 정보를 사용하여 검증하는 단계;를 포함하며,

상기 (a) 단계는

래티스(lattice) 상에서의 SIS(small integer solution) 문제의 어려움에 기반하여, 마스터 비밀키로 사용할 트랩도어(trapdoor)를 생성하는 단계; 및 상기 사용자 공개키를 사용하여 상기 트랩도어를 더 큰 차원(dimension)을 갖도록 확장하여 상기 확장된 트랩도어를 상기 사용자 비밀키로서 출력하는 단계;를 포함하되,

상기 트랩도어는 일련의 래티스 벡터가 모인 행렬인 전자 서명 방법.

**청구항 10**

삭제

**청구항 11**

제 9 항에 있어서,

(b) 단계는 상기 확장된 트랩도어에서 가우시안 샘플링(Gaussian Sampling)을 사용하여 상기 서명에 사용할 래티스 벡터를 추출하는 단계;를 포함하는 전자 서명 방법.

**청구항 12**

전자 서명 방법에 있어서,

(a) 마스터 개체가 보안 파라미터에 기초하여 일련의 해시(hash) 함수를 선택하는 단계;

(b) 상기 마스터 개체가 상기 보안 파리미터에 기초하여 자신의 비밀키로 사용할 트랩도어(trapdoor)를 생성하는 단계;

(c) 상기 일련의 해시 함수를 공개하는 단계; 및

(d) 사용자 개체의 공개된 식별 정보를 상기 사용자 개체의 사용자 공개키로 사용하여, 상기 사용자 공개키에 기초하여 상기 트랩도어를 더 큰 차원(dimension)을 갖도록 확장하고, 상기 확장된 트랩도어를 상기 사용자 비밀키로 출력하는 단계;를 포함하되,

상기 마스터 개체는 래티스(lattice) 상에서의 SIS(small integer solution) 문제의 어려움에 기반하여, 상기

트랩도어를 생성하며,

상기 트랩도어는 일련의 래티스 벡터가 모인 행렬인 전자 서명 방법.

**청구항 13**

제 12항에 있어서,

상기 (b) 단계는 상기 트랩도어에 대응되는 제 1 행렬을 생성하는 단계;를 포함하고,

상기 (c) 단계는 상기 제 1 행렬을 상기 일련의 해시 함수와 함께 공개하는 전자 서명 방법.

**청구항 14**

제 13 항에 있어서,

상기 보안 파라미터는 행렬 차원 파라미터, 크기 파라미터를 포함하고,

제 1 행렬은 상기 보안 파리미터에 기초하여 균일한 분포(uniform distribution)에서 선택된 랜덤(random)한 값을 가지도록 생성되며,

상기 트랩도어는

상기 제 1 행렬에 대응 관계를 가지며, 역행렬이 존재하고, 모든 행의 크기가 특정 임계값보다 작은 행렬이되,

상기 대응 관계는 상기 제 1 행렬과 상기 트랩도어의 곱은 상기 크기 파라미터와의 나머지 연산이 0이 되는 것인 전자 서명 방법.

**청구항 15**

제 12 항에 있어서,

상기 확장된 트랩도어에서 추출한 래티스 벡터는 상기 사용자 개체가 자신의 서명을 생성하는 데 사용되는 전자 서명 방법.

**청구항 16**

제 12 항에 있어서,

래티스(lattice) 상에서의 LWE(learning with errors) 문제의 어려움에 기반하여, 상기 확장된 트랩도어에서 추출한 래티스 벡터는 상기 사용자 개체가 자신의 서명을 생성할 때 난수 및 에러 벡터를 사용하여 가공되는 전자 서명 방법.

**청구항 17**

제 12 항에 있어서,

상기 트랩도어에서 래티스 벡터를 추출하는 데에 가우시안 샘플링(Gaussian Sampling)이 사용되는 전자 서명 방법.

**청구항 18**

제 12 항에 있어서,

상기 사용자 개체는

자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 검증자 개체의 공개된 식별 정보를 사용하여 서명한 메시지를 상기 검증자 개체에게 전송하는 서명자 개체; 및

상기 서명자 개체로부터 수신한 서명을 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 상기 서명자 개체의 공개된 식별 정보를 사용하여 검증하는 검증자 개체;를 포함하는 전자 서명 방법.

**청구항 19**

제 18 항에 있어서,

상기 검증자 개체는

자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 상기 서명자 개체의 공개된 식별 정보를 사용하여 상기 서명자 개체로부터 수신한 서명을 생성할 수 있는 전자 서명 방법.

# 명 세 서

## 기 술 분 야

[0001] 본 발명은 전자 서명 시스템 및 방법에 관한 것이다.

## 배 경 기 술

[0002] 전자 거래 등 사용자의 신원이 위조되면 곤란한 온라인 활동이 활성화됨에 따라 전자 서명의 중요성이 점점 커지고 있다. 이에 따라, 생성된 서명을 수신한 검증자는 서명자가 해당 서명을 생성하였음을 확인할 수 있어야 한다는 기본적인 요건 뿐 아니라, 제 3 자가 서명을 위조하기 어려워야 하고 서명자는 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] 또한, 서명자가 특정 검증자를 지정하여 서명을 생성하면, 지정된 검증자 이외에는 해당 서명을 검증할 수 없게 하는 지정된 검증자 서명 기법(designated verifier signature scheme)도 소개되었다. 이때, 검증이라 함은 서명이 서명자에 의해 생성된, 유효한 서명임을 확인하는 것이다. 서명자와 지정된 검증자 이외의 어느 누구도 서명이 서명자에 의해 생성되었다는 것을 확인할 수 없으며, 서명자와 지정된 검증자 중의 한 명이 생성했다는 것만을 알 수 있으므로, 지정된 검증자 서명 기법은 서명자와 지정된 검증자 사이의 익명성을 제공한다.

[0005] 이 기법을 더 발전시킨 것이 강한 지정된 검증자 서명 기법(strong designated verifier signature scheme)이다. 강한 지정된 검증자 서명 기법을 통해 생성된 서명은 서명자와 지정된 검증자 이외의 어느 누구도 어떤 서명자가 어떤 지정된 검증자를 대상으로 생성한 서명인지를 알아낼 수 없으므로, 더욱 강력한 익명성을 제공하며, 따라서 안전성이 더욱 높다.

[0006] 한편, 서명의 안전성을 높이기 위해 기반이 되는 수학적 난제에 대한 연구도 많이 이루어졌다. 예를 들어, 이산 대수 문제의 어려움, 겹선형 함수의 어려움 등 평균적인 경우 어려운 문제들에서 최악의 경우에도 어려운 문제로 알려진 래티스(lattice) 상에서의 SIS(small integer solution) 문제와 LWE(learning with errors) 문제의 어려움에 기반을 두는 서명 기법들로 발전하고 있다.

[0007] 안전성 요건과 효율성 요건을 동시에 충족시키는 전자 서명 시스템을 개발하는 것은 어려운 일이다. 따라서 각각 안전성 또는 효율성 측면에서 장점을 가지고 있는 ID 기반 서명 기법, 강한 지정된 검증자 서명 기법, 및 래티스 상에서의 SIS 문제의 어려움에 기반을 둔 서명 기법을 적절히 통합하여 안전성이 높으면서도 효율적인 전자 서명 시스템 및 방법을 제공할 필요가 있다.

[0008] 지정된 검증자 서명과 관련하여 한국등록특허 제10-0369408호("이동 통신에서의 수신자 지정 대리 서명 방법")에는 이산 대수 문제의 어려움에 기반을 둔 서명 생성 방법이 개시되어 있다. 하지만 이는 강한 지정된 검증자 서명은 아니다.

[0009] 또한, 한국공개특허 제10-2005-0128506호("겹선형 사상을 이용한 한정적 검증자 서명 방법")는 겹선형 사상을 이용한 지정된 검증자 서명 생성 방법이 개시되어 있다. 역시 이는 강한 지정된 검증자 서명은 아니다.

## 발명의 내용

### 해결하려는 과제

[0010] 본 발명은 전술한 문제를 해결하기 위한 것으로서, 그 목적은 안전성과 효율성이 높은 전자 서명 시스템 및 방법을 제공하는 것이다.

## 과제의 해결 수단

[0011] 상기와 같은 목적을 달성하기 위한 본 발명의 제 1 측면에 따른 전자 서명 시스템은 사용자의 공개된 식별 정보를 상기 사용자의 사용자 공개키로 사용하여, 상기 사용자 공개키에 대응되는 사용자 비밀키를 생성하여 상기 사용자에게 할당하는 마스터;를 포함하되, 상기 사용자는 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 검증자의 공개된 식별 정보를 사용하여 서명한 메시지를 상기 검증자에게 전송하는 서명자; 및 상기 서명자로부터 수신한 서명을 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 상기 서명자의 공개된 식별 정보를 사용하여 검증하는 검증자;를 포함하는 것을 특징으로 한다.

[0012] 상기와 같은 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 전자 서명 방법은 (a) 마스터가 서명자 및 검증자를 포함하는 사용자의 공개된 식별 정보를 상기 사용자의 사용자 공개키로 사용하여, 상기 사용자 공개키에 대응되는 사용자 비밀키를 생성하여 상기 사용자에게 할당하는 단계; (b) 서명자가 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 검증자의 공개된 식별 정보를 사용하여 서명한 메시지를 상기 검증자에게 전송하는 단계; 및 (c) 검증자가 상기 서명자로부터 수신한 서명을 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 상기 서명자의 공개된 식별 정보를 사용하여 검증하는 단계;를 포함하는 것을 특징으로 한다.

[0013] 상기와 같은 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 전자 서명 방법은 (a) 마스터 개체가 보안 파라미터에 기초하여 일련의 해시(hash) 함수를 선택하는 단계; (b) 상기 마스터 개체가 상기 보안 파리미터에 기초하여 자신의 비밀키로 사용할 트랩도어(trapdoor)를 생성하는 단계; (c) 상기 일련의 해시 함수를 공개하는 단계; 및 (d) 사용자 개체의 공개된 식별 정보를 상기 사용자 개체의 사용자 공개키로 사용하여, 상기 사용자 공개키에 기초하여 상기 트랩도어를 더 큰 차원(dimension)을 갖도록 확장하고, 상기 확장된 트랩도어를 상기 사용자 비밀키로 출력하는 단계;를 포함하되, 상기 마스터 개체는 래티스(lattice) 상에서의 SIS(small integer solution) 문제의 어려움에 기반하여, 상기 트랩도어를 생성하며, 상기 트랩도어는 일련의 래티스 벡터가 모인 행렬인 것을 특징으로 한다.

## 발명의 효과

[0014] 본 발명은 전자 서명 시스템 및 방법에 있어, 전자 서명의 안전성과 효율성을 동시에 향상시키는 효과를 얻는다.

[0015] 구체적으로, 본 발명은 공개키 기반 환경에서 사용자의 공개키로 사용자의 공개된 식별 정보를 사용하는 ID 기반 서명 기법을 사용하므로, 효율성이 높다.

[0016] 또한, 본 발명은 서명자와 지정된 검증자 이외의 어느 누구도 서명을 생성한 것이 누구인지 알 수 없다는 강한 지정된 검증자 서명 기법을 사용하므로, 완벽한 익명성을 제공하고, 따라서 안전성이 높다.

[0017] 또한, 본 발명은 최악의 경우에도 어려운 수학적 난제인 래티스 상에서의 SIS 문제의 어려움에 기반을 두고 있으므로, 안전성이 높다.

## 도면의 간단한 설명

[0018] 도 1은 본 발명의 일실시예에 따른 전자 서명 시스템의 구조를 도시함.

도 2는 도 1의 시스템의 구조를 다른 관점에서 도시함.

도 3은 본 발명의 일실시예에 따른 트랩도어 생성 방법의 흐름을 도시함.

도 4는 본 발명의 일실시예에 따른 트랩도어 확장 방법의 흐름을 도시함.

도 5는 본 발명의 일실시예에 따른 가우시안 샘플링 방법의 흐름을 도시함.

도 6은 본 발명의 일실시예에 따른 전자 서명 방법의 흐름을 도시함.

도 7은 본 발명의 일실시예에 따른 마스터 키 생성 방법의 흐름을 도시함.

도 8은 본 발명의 일실시예에 따른 사용자 키 생성 방법의 흐름을 도시함.

도 9는 본 발명의 일실시예에 따른 서명 생성 방법의 흐름을 도시함.

도 10은 본 발명의 일실시예에 따른 서명 검증 방법의 흐름을 도시함.

## *발명을 실시하기 위한 구체적인 내용*

[0019] 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.

[0020] 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.

[0021] 도 1 및 도 2는 본 발명의 일실시예에 따른 전자 서명 시스템의 구조를 도시하고 있다.

[0022] 본 발명의 일실시예에 따른 전자 서명 시스템(10)에는 네트워크를 통해 연결된 서명자(A), 검증자(B), 및 제3자(C)를 포함하는 사용자와 마스터(M) 등의 개체(entity)가 참여한다.

[0023] 사용자 중, 서명자(A)는 메시지에 서명하여 검증자(B)에게 전송하는 개체이며, 검증자(B)는 서명자(A)로부터 수신한 서명을 검증하는 개체이다. 이때, 검증이란 전술한 바와 같이, 수신한 서명이 서명자(A)에 의해 생성된, 유효한 서명임을 확인하는 것이다.

[0024] 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 전술한 바와 같이, 강한 지정된 검증자 서명(strong designated verifier signature)을 사용하므로, 서명자(A)는 메시지에 서명할 때, 특정 검증자(B)를 지정하여 해당 검증자(B)만이 검증할 수 있도록 가공된 서명을 생성한다. 다른 개체가 해당 서명을 읽어볼 수 없음을 강조하기 위해, 도면에는 서명자(A)가 특정 검증자(B)를 지정해 생성하고 해당 검증자(B)에게 전송하는 서명을 암호화된 서명으로 도시하였다. 그러나 이는 이해를 돕기 위한 것일 뿐, 서명 데이터가 반드시 암호화되고 복호화되어야 하는 것은 아니다.

[0025] 따라서, 서명을 생성하여 전송한 서명자(A)와 서명을 수신한 검증자(B) 이외의 다른 사용자인 제3자(C)는 해당 서명을 검증할 수 없으며, 심지어 전술한 바와 같이, 누가 생성한 서명인지도 전혀 알 수 없다.

[0026] 도면에는 각각 하나의 서명자(A), 검증자(B), 및 제3자(C) 개체만을 도시되어 있고, 이들이 서로 다른 개체인 것처럼 도시되어 있다. 그러나 서명자(A), 검증자(B), 및 제3자(C)는 모두 사용자 개체로서, 이들의 역할은 고정적이지 않으며, 전자 서명 시스템(10)에 참여하는 사용자 개체의 수에도 제한이 없을 것임을 쉽게 이해할 수 있을 것이다. 또한, 이들 각 사용자 개체는 사용자가 사용하는 기기나 소프트웨어 등의 실체를 의미할 수 있다. 이는 통용되는 개념이므로 본 명세서에서 이에 대한 명시적 기재는 생략한다. 예를 들어, 이하 기술에서 사용자라 함은 서명자(A), 검증자(B), 제3자(C) 등의 사용자 개체를 나타낼 수 있다.

[0027] 전술한 바와 같이, 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 공개키 기반 환경에서 사용자의 식별 정보를 공개키로 사용하는 ID 기반 서명 기법을 사용한다. 따라서 본 발명의 일실시예에 따른 전자 서명 시스템(10)에는 각 사용자의 비밀키를 생성하여 해당 사용자에게 배포하는 마스터(M) 개체가 참여한다. 여기에서 마스터(M)는 키 생성 기관(Key Generation Center), 인증 기관(Certification Authority) 등 다양한 이름으로 불릴 수 있으며, 전자 서명 시스템(10)이 원할하게 운영되도록 관리하는 기관들을 통칭하는 개념으로 사용하였다.

[0028] 종래의 공개키 기반 환경에서는 전술한 바와 같이, 마스터(M)가 각 사용자에게 공인 인증서를 발급해야 하지만, 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 사용자의 공개된 식별정보를 공개키로 사용하므로 이 과정이 필요없어, 효율적이고 안전성 또한 높을 수 있다. 공인 인증서, 즉 공개 키 인증서(public key certificate)는 각 사용자의 공개키가 해당 사용자의 것임을 보증하기 위해, 인증 기관이 자신의 비밀키로 각 사용자의 공개키에 서명한 것이다. ID 기반 서명은 ID, 이메일 등의 이미 공개되어 있는 사용자 식별정보를 사용하여 이러한 과정을 없앤 것이다.

[0029] 도면은 사용자 식별정보($ID_A$, $ID_B$, $ID_C$)가 사용자 공개키로서 공개되어 있고, 대응되는 사용자 비밀키($sk_A$ 등)는 각 사용자만이 가지고 있음을 도시하고 있다.

[0030] 공개키 기반 방식은 서로 대응되는 키 쌍을 생성하여, 이중 공개키는 암호화 또는 서명 확인용으로, 비밀키는 복호화 또는 서명용으로 사용하는 비대칭형 암호화 또는 서명 방식이다.

[0031] 해당 메시지를 보낸 사용자가 누구인가를 증명하기 위한 것이므로, 어떤 메시지에 서명할 때는 비밀키로 서명하

고 대응되는 공개키로 이를 확인한다. 즉, 비밀키는 문서에 찍는 도장의 기능을 한다. 따라서 종래의 공개키 기반 환경에서는 메시지를 주고 받는 당사자 이외의 사용자도 누가 메시지에 서명했는지 알 수 있다.

[0032] 그러나, 전술한 바와 같이, 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 강한 지정된 검증자 서명 기법을 사용하므로, 메시지를 주고 받는 당사자인 서명자(A)와 검증자(B) 이외의 사용자, 즉 제3자(C)는 메시지와 서명을 가로채더라도 서명을 검증할 수 없으며, 메시지에 서명한 것이 누구인지 전혀 알 수 없다. 이렇게 강력한 익명성을 보장하므로 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 높은 안전성을 제공한다.

[0033] 이는 서명자(A)가 메시지에 서명할 때, 자신의 공개된 식별 정보 및 자신의 사용자 비밀키 이외에도 서명한 메시지가 전송될 검증자(B)의 공개된 식별 정보를 사용하기 때문에 가능하다. 이에 따라, 검증자(B)는 서명자(A)로부터 수신한 서명을 검증할 때, 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 서명자(A)의 공개된 식별 정보를 사용한다. 제3자(C)는 서명을 검증하기 위해 필요한 정보를 가지고 있지 못하기 때문에 해당 서명이 어떤 사용자에 의해 생성된 것인지 알아낼 수 없는 것이다.

[0034] 전술한 바와 같이, 암호화 및 전자 서명 시스템은 특정 정보가 없으면 풀기 어려운 수학적 난제에 기반하여 구축되는데, 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 래티스(lattice) 상에서의 SIS(small integer solution) 문제와 LWE(learning with errors) 문제의 어려움에 기반하고 있다.

[0035] 특정 정보가 없으면 풀기 어렵다는 것은 연산이 일방향성이라는 의미이다. 일방향성은 연산은 쉬워도 연산의 역을 구하는 것은 어렵우며, 이때 특정 정보를 갖고 있는 경우에는 쉽게 역을 구할 수 있음을 나타낸다. 이러한 특정 정보를 트랩도어(trapdoor)라고 부른다.

[0036] 예를 들어, 공개키 기반 환경에서 암호화 연산은 암호화는 쉽지만 그 역변환인 복호화는 암호화시 사용한 암호화 키에 대응되는 복호화 키가 없는 경우 매우 어려운 일방향성 연산을 사용하여 수행된다. 즉, 암호화시 사용한 암호화 키에 대응되는 복호화 키가 트랩도어이다. 일단 메시지를 암호화하고 나면 암호화 키가 있어도 이를 복호화할 수 없으므로, 암호화 키는 공개되어도 된다. 반면, 트랩도어 또는 복호화 키는 공개되면 안된다. 따라서, 공개키 기반 환경에서 트랩도어를 생성하는 데 사용된 정보는 공개키로서 공개되고, 트랩도어는 비밀키로서 공개되지 않는다.

[0037] 따라서 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 사용자의 공개된 식별 정보를 사용하여, 각 사용자의 비밀키로 사용할 트랩도어를 생성하는데, 본 발명의 일실시예에 따른 전자 서명 시스템(10)에서 사용하는 트랩도어는 일련의 래티스 벡터가 모인 행렬이다.

[0038] 래티스에 기반한 SIS 문제와 LWE 문제는 전술한 바와 같이 최악의 경우에서도 풀기 어려운 수학적 난제 중 하나이므로, 최근 암호화 및 전자 서명 시스템에 이를 적용하려는 시도가 많이 이루어지고 있는 추세이다. 래티스는 공간에서 2개의 기저의 선형 결합을 통해 만들어지는 모든 점의 집합이다. 기저를 모르면 제3자(C)가 어떤 점을 알아내었다고 해도 해당 점으로부터 가장 가까운 래티스 점이 어딘지 알아내는 것은 매우 어렵다는 장점이 있다. 또한, 기저를 모르면 제3자(C)는 특정 길이 이내의 래티스 점을 찾는 것이 매우 어렵다는 장점이 있다.

[0039] 본 발명의 일실시예에 따른 전자 서명 시스템(10)은 마스터(M)가 자신의 마스터 비밀키(msk)로 사용할 트랩도어를 생성하고, 이 트랩도어를 확장하여 사용자 비밀키를 생성하며, 서명자(A)는 자신의 비밀키, 즉 트랩도어로부터 추출한 래티스 벡터를 서명 생성에 사용함으로써, 래티스를 활용한다. 트랩도어에서 래티스 벡터를 추출하는 데에는 가우시안 샘플링(Gaussian Sampling)이 사용될 수 있다.

[0040] 도 2에 도시되어 있는 바와 같이, 이를 위해 마스터(M)는 트랩도어 생성부(100) 및 트랩도어 확장부(200)를 포함하며, 각 사용자(A, B, C)는 가우시안 샘플링부(300)를 포함한다. 트랩도어 생성부(100), 트랩도어 확장부(200), 및 가우시안 샘플링부(300)가 수행하는 동작은 도 3 내지 도 5에 도시되어 있다.

[0041] 도 3은 본 발명의 일실시예에 따른 트랩도어 생성 방법의 흐름을 도시하고 있다.

[0042] 전술한 바와 같이, 트랩도어는 마스터 비밀키(msk)로 사용되는 행렬이다. 도시되어 있는 바와 같이, 트랩도어 생성부(100)는 트랩도어 생성 방법을 사용하여 임의의 행렬 A 및 이에 대응되는 트랩도어 T를 생성한다.

[0043] 먼저, 보안 파라미터를 입력받는다(S1100). 보안 파라미터는 전자 서명 시스템(10)의 안전성 레벨을 결정하는 파라미터이다. 상수 n 및 m은 트랩도어 행렬의 차수(dimension)을 결정하는 파라미터이다. 즉, 트랩도어 생성에 쓰이는 임의의 행렬 A의 행 또는 열의 개수를 결정한다. 상수 q는 양의 정수이며, 이후 행렬 A에 대응되는 트랩도어 T를 생성하는데 사용되는 나머지 연산(mod)에 사용되는 충분히 큰 값으로, 트랩도어 T의 각 요소의 값의

크기를 결정하는 데 사용된다. 도시되어 있는 바와 같이, m은 n과 q에 기초하여 결정된다.

[0044] 다음, 균일한 분포(uniform distribution)를 가지는 임의의 행렬 A를 생성하고, 이에 대응하는 트랩도어를 생성하여(S1200), 출력한다(S1300). 행렬 A는 랜덤(random)한 값을 갖는다. 이에 대응하는 트랩도어 T는 역행렬을 가지고, 모든 행의 크기가 특정 임계값보다 작은 행렬이다.

[0045] 도시된 바와 같이 행렬 A와 트랩도어 T의 곱은 q와의 나머지 연산이 0이 된다. 양의 정수 q로 나눈 나머지가 0이 되어야 하므로, 이에 따라 트랩도어 T의 각 요소는 매우 작은 값을 가지게 된다. 즉, 본 발명에 따른 트랩도어는 SIS(small integer solution) 문제에 기반하여 생성되게 된다. 즉, 생성되는 트랩도어는 래티스 벡터가 모인 행렬이 된다.

[0046] 도 4는 본 발명의 일실시예에 따른 트랩도어 확장 방법의 흐름을 도시하고 있다.

[0047] 전술한 바와 같이, 마스터 비밀키로 사용되는 트랩도어는 각 사용자의 비밀키를 생성하기 위하여 확장된다. 확장된다는 뜻은 행렬의 차수가 커진다는 뜻, 즉, 트랩도어의 행 또는 열의 개수가 늘어난다는 뜻이다. 마스터(M)는 이를 위해 각 사용자의 공개된 식별 정보를 사용한다.

[0048] 먼저, 도 3에서 생성된 행렬 A 및 대응되는 트랩도어 T 및 추가적인 행렬 A'를 입력받는다(S2100). A'는 각 사용자의 공개된 식별 정보를 사용하여 생성되는 행렬이다(도 8 참조).

[0049] 행 또는 열의 개수가 늘어난 행렬 A'' 및 이에 대응되는 확장된 트랩도어 T''를 생성하고(S2200), 출력한다(S2300). 전술한 바와 같이, 확장된 트랩도어 T''는 해당 사용자의 비밀키로 사용된다.

[0050] 도 5는 본 발명의 일실시예에 따른 가우시안 샘플링 방법의 흐름을 도시하고 있다.

[0051] 전술한 바와 같이, 가우시안 샘플링은 서명자(A)가 자신의 비밀키, 즉 확장된 트랩도어에서 서명에 사용할 래티스 벡터를 추출하기 위해 사용한다.

[0052] 먼저, 필요한 정보를 입력받는다(S3100). 입력받는 행렬 및 트랩도어는 각각 A 및 T로 도시되어 있으나, 도 3에서 마스터 비밀키용으로 생성한 A 및 T를 의미하지 않는다. 임의의 행렬 및 대응되는 트랩도어를 입력받는다는 뜻으로 쓰였으며, 실제 입력되는 것은 도 4에서 생성되어 서명자(A)에게 할당된 A'' 및 T''가 될 것이다(도 9 참조).

[0053] 도시된 조건을 만족하는 트랩도어에서 벡터 v를 샘플링, 즉 추출하고(S3200), 출력한다(S3300). 도시되어 있는 두번째 조건은 공간에서의 벡터의 크기, 즉 벡터가 공간에서 어떤 점을 나타낸다고 생각했을 때의 그 벡터의 길이가 임계값보다 짧음을 의미한다.

[0054] 도 6은 본 발명의 일실시예에 따른 전자 서명 방법의 흐름을 도시하고 있다.

[0055] 먼저, 마스터(M)는 도 3의 방법을 사용하여, 마스터 비밀키를 생성한다(S110). 전술한 바와 같이, 마스터 비밀키는 래티스 벡터가 모인 행렬인 트랩도어이다.

[0056] 다음, 마스터(M)는 도 4의 방법을 사용하여, 각 사용자에 대해 각 사용자의 공개된 식별 정보를 사용하여 사용자 비밀키를 생성한다(S120). 전술한 바와 같이, 사용자 비밀키는 마스터 비밀키가 확장된 트랩도어이다.

[0057] 서명자(A)가 메시지 및 서명을 생성하여 검증자(B)에게 전송하면(S130), 검증자(B)는 수신한 서명을 검증(S140)한다. 전술한 바와 같이, 서명자(A)는 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 검증자(B)의 공개된 식별 정보를 사용하여 서명한 메시지를 검증자(B)에게 전송하며, 검증자(B)는 서명자(A)로부터 수신한 서명을 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 서명자(A)의 공개된 식별 정보를 사용하여 검증한다.

[0058] 필요한 경우, 검증자(B)는 서명 생성을 시뮬레이션할 수 있다(S150). 이는 검증자(B)가 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 서명자(A)의 공개된 식별 정보를 사용하여 서명자(A)로부터 수신한 서명을 생성할 수 있음을 의미한다.

[0059] 도 7 내지 도 10은 도 6의 각 단계를 자세히 설명하고 있다.

[0060] 먼저, 도 7은 본 발명의 일실시예에 따른 마스터 키 생성 방법의 흐름을 도시하고 있다.

[0061] 마스터(M)는 도 3에서 설명한 트랩도어 생성 방법을 사용하여, 제 1 행렬 A0 및 대응하는 트랩도어 T0를 생성하고(S210), 생성한 트랩도어를 마스터 비밀키로 설정한다(S220).

[0062] 이외에도 마스터(M)는 전자 서명 시스템(10)에 사용될 일련의 해시(hash) 함수들을 생성하고(S230), 제 1 행렬

A0와 함께 공개 파라미터로서 공개한다(S240). 따라서, 도 1에 도시되어 있는 바와 같이, 본 발명의 일실시예에 따른 전자 서명 시스템(10)에서는 각 사용자의 공개된 식별 정보 뿐 아니라, 해시 함수 등의 공개 파라미터도 공개되어 있다.

[0063] 도 8은 본 발명의 일실시예에 따른 사용자 키 생성 방법의 흐름을 도시하고 있다.

[0064] 도면에서 user는 각 사용자를 나타내며, 이는 도 1에 도시된 바와 같은 각 사용자의 공개된 식별 정보를 사용하여 각 사용자에 대해 사용자 비밀키를 각각 생성함을 의미한다.

[0065] 마스터(M)가 각 사용자의 비밀키를 생성하는 데에 필요한 것은 마스터 비밀키, 즉 트랩도어 T0 및 사용자의 공개된 식별 정보이다(S210). 전술한 바와 같이, 사용자의 공개된 식별 정보로 사용자의 ID 이외에도 이메일 등 다양한 형태의 식별 정보가 사용될 수 있다.

[0066] 마스터(M)는 도 4에서 설명한 트랩도어 확장 방법을 사용하여 생성한 확장된 트랩도어를(S220) 사용자의 비밀키로 설정한다(S230).

[0067] 도 9는 본 발명의 일실시예에 따른 서명 생성 방법의 흐름을 도시하고 있다.

[0068] 서명자(A)가 메시지에 서명하기 위해서는 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 검증자(B)의 공개된 식별 정보가 필요하다(S310). 전술한 바와 같이, 서명자(A)가 서명에 검증자B)의 공개된 식별 정보를 사용하기 때문에, 검증자(B) 이외의 제3자(C)는 해당 서명이 서명자(A)에 의해 생성되었음을 알 수 없다.

[0069] 난수 및 벡터의 크기가 임계값보다 작은 벡터를 선택하여(S320), 이를 기초로 도 5에서 설명한 가우시안 샘플링을 사용하여 자신의 사용자 비밀키, 즉 확장된 트랩도어로부터 서명에 사용할 래티스 벡터를 추출한다(S330).

[0070] 다음, 난수 및 에러 분포로부터 샘플링되는 에러 벡터를 사용하여(S340), 래티스 벡터를 가공한다(S350, S360). 에러 분포는 정규 분포를 일반화한 분포이다. 여기서 이렇게 생성된 벡터는 LWE(learning with errors) 문제에 기반하여 생성하게 된다.

[0071] 다음, 가공된 서명을 출력한다(S370). 도시되어 있는 바와 같이, 본 발명의 일실시예에 따른 서명 생성 방법은 트랩도어에서 추출한 래티스 벡터를 서명으로 사용하지 않고 가공하여 사용하므로, 안전성이 좀더 높아진다.

[0072] 도 10은 본 발명의 일실시예에 따른 서명 검증 방법의 흐름을 도시하고 있다.

[0073] 검증자(B)가 서명자(A)로부터 수신한 서명을 검증하기 위해서는 자신의 공개된 식별 정보, 자신의 사용자 비밀키, 및 서명자(A)의 공개된 식별 정보가 필요하다(S410).

[0074] 이후 단계들에서 서명 검증에 필요한 정보들을 산출하여(S420 내지 S440), 세가지 조건이 모두 만족되는지 확인한다(S450). 세가지 조건이 모두 만족되면 서명이 유효한 것이므로 받아들이고(S460), 그렇지 않으면 서명이 유효하지 않다고 판단한다(S470).

[0075] 본 발명의 일실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0076] 본 발명의 방법 및 시스템은 특정 실시예와 관련하여 설명되었지만, 그것들의 구성 요소 또는 동작의 일부 또는 전부는 범용 하드웨어 아키텍처를 갖는 컴퓨터 시스템을 사용하여 구현될 수 있다. 본 발명의 일실시예의 하나 이상의 구성 요소 또는 동작을 실시하기 위하여 사용될 수 있는 컴퓨터 시스템 아키텍처의 일례를 설명하면, 하드웨어 시스템은 프로세서, 캐쉬, 메모리 및 상술한 기능에 관련된 하나 이상의 소프트웨어 어플리케이션 및 드라이버를 포함할 수 있다.

[0077] 전술한 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.

[0078] 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

[0079] 10: 전자 서명 시스템

M: 마스터

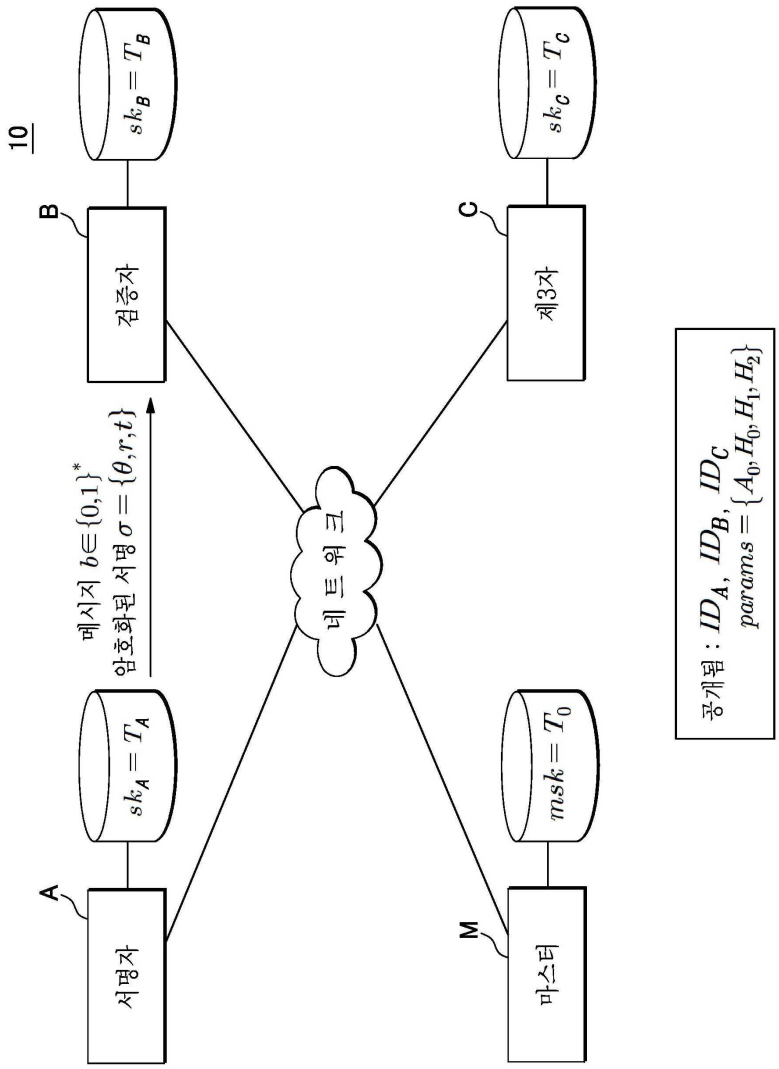
A: 서명자

B: 검증자

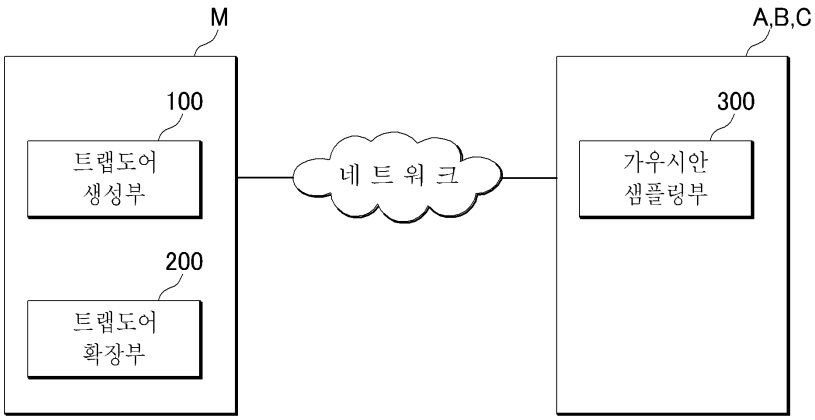
C: 제3자

## 도면

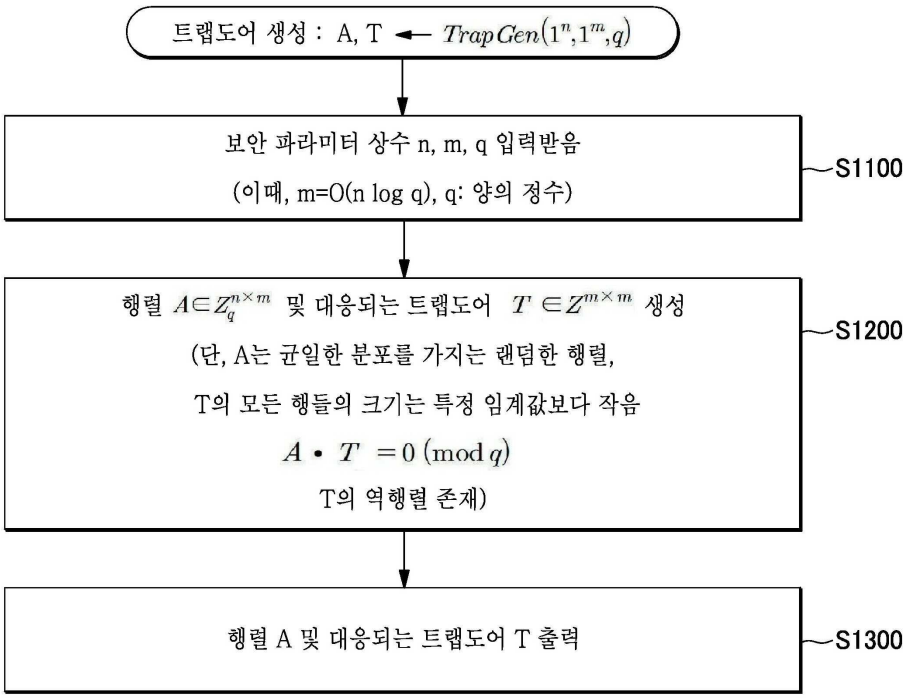
### 도면1



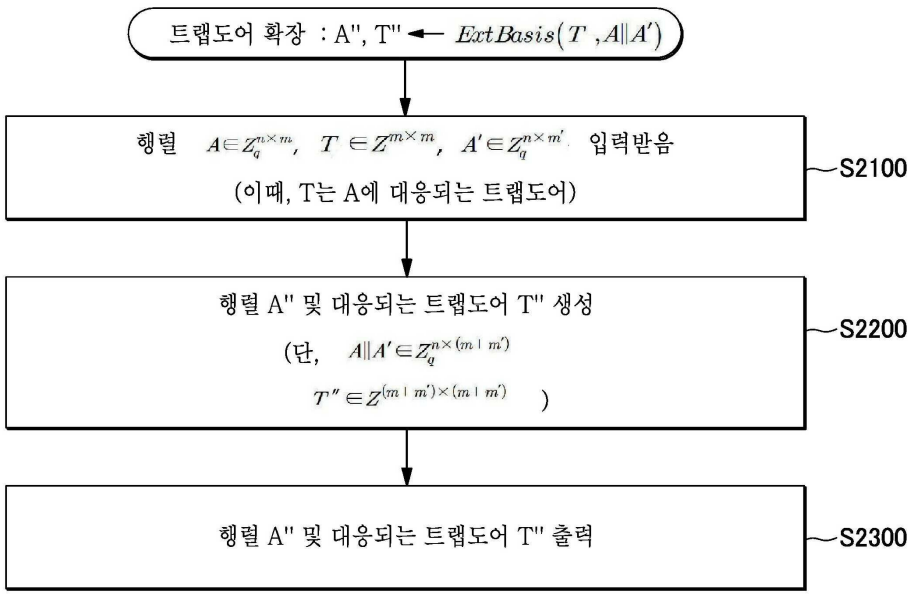
도면2


M
A,B,C
100
트랩도어
생성부
200
트랩도어
확장부
네 트 워 크
300
가우시안
샘플링부

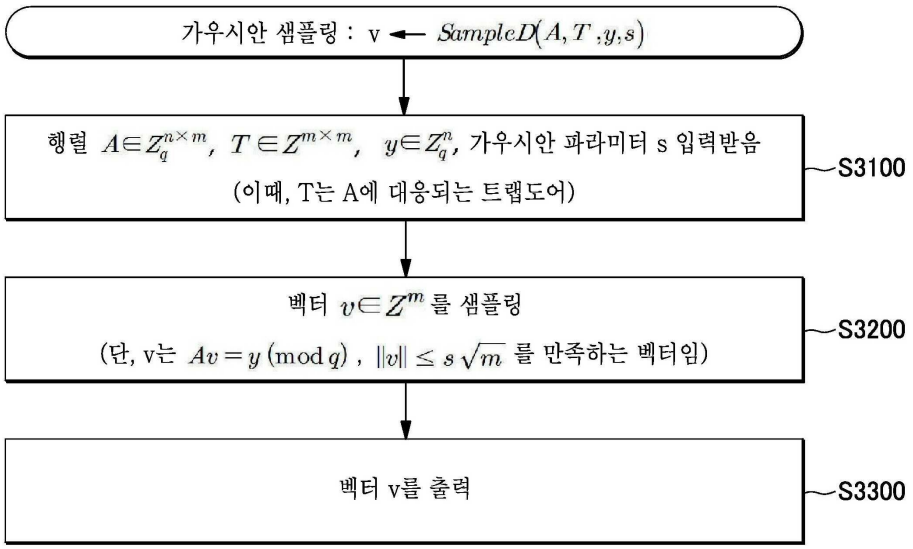
도면3


트랩도어 생성 : A, T ← $TrapGen(1^n,1^m,q)$
보안 파라미터 상수 n, m, q 입력받음
(이때, m=O(n log q), q: 양의 정수)
S1100
행렬 $A \in Z_q^{n \times m}$ 및 대응되는 트랩도어 $T \in Z^{m \times m}$ 생성
(단, A는 균일한 분포를 가지는 랜덤한 행렬,
T의 모든 행들의 크기는 특정 임계값보다 작음
$A \cdot T = 0 \pmod q$
T의 역행렬 존재)
S1200
행렬 A 및 대응되는 트랩도어 T 출력
S1300

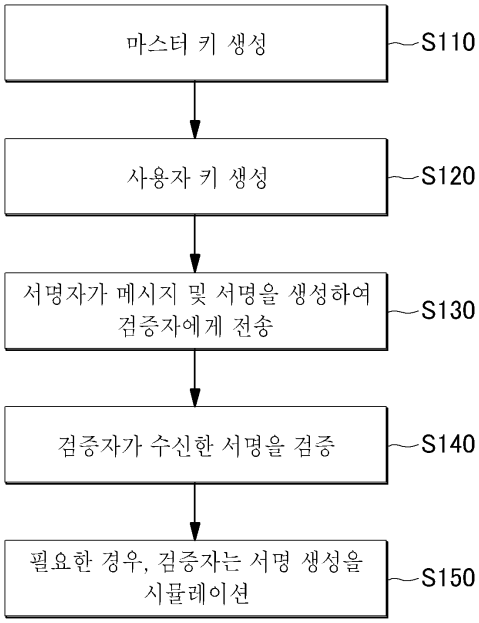
도면4


트랩도어 확장 : A'', T'' ← $ExtBasis(T, A\|A')$
행렬 $A \in Z_q^{n \times m}$, $T \in Z^{m \times m}$, $A' \in Z_q^{n \times m'}$ 입력받음
(이때, T는 A에 대응되는 트랩도어)
S2100
행렬 A'' 및 대응되는 트랩도어 T'' 생성
(단, $A\|A' \in Z_q^{n \times (m+m')}$
$T'' \in Z^{(m+m') \times (m+m')}$ )
S2200
행렬 A'' 및 대응되는 트랩도어 T'' 출력
S2300

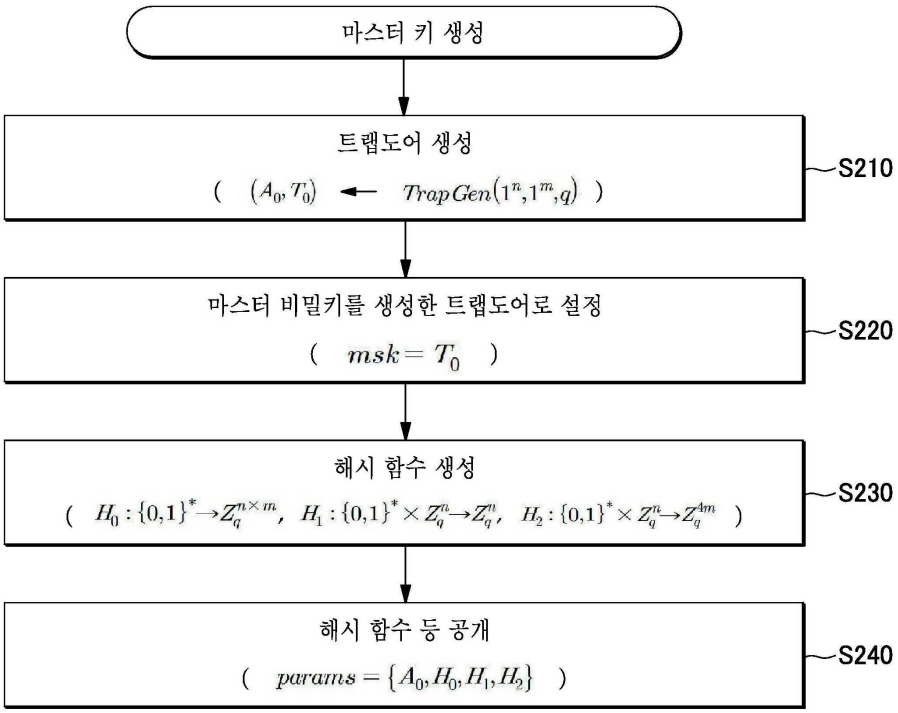
도면5


가우시안 샘플링 : v ← $SampleD(A, T, y, s)$
행렬 $A \in Z_q^{n \times m}$, $T \in Z^{m \times m}$, $y \in Z_q^n$, 가우시안 파라미터 s 입력받음
(이때, T는 A에 대응되는 트랩도어)
S3100
벡터 $v \in Z^m$ 를 샘플링
(단, v는 $Av = y \pmod q$ , $\|v\| \le s\sqrt{m}$ 를 만족하는 벡터임)
S3200
벡터 v를 출력
S3300

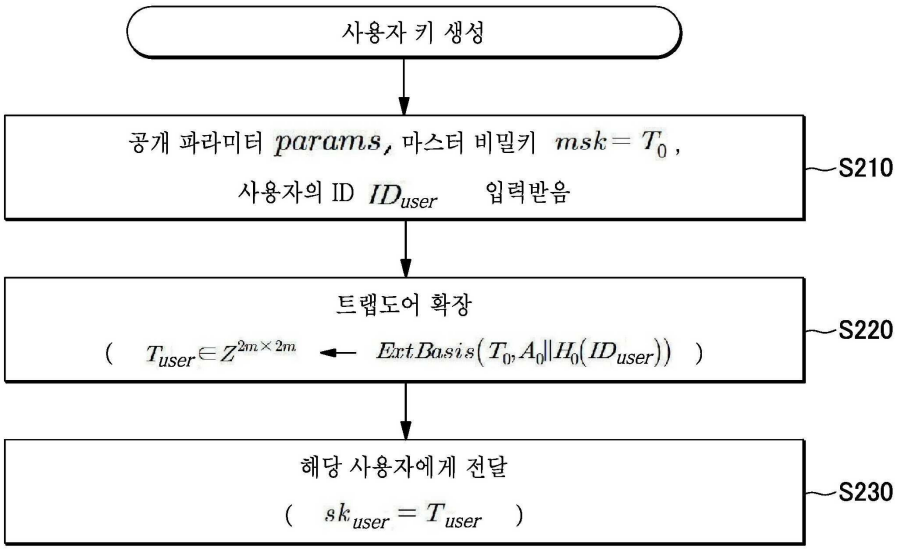
도면6


마스터 키 생성
S110
사용자 키 생성
S120
서명자가 메시지 및 서명을 생성하여 검증자에게 전송
S130
검증자가 수신한 서명을 검증
S140
필요한 경우, 검증자는 서명 생성을 시뮬레이션
S150

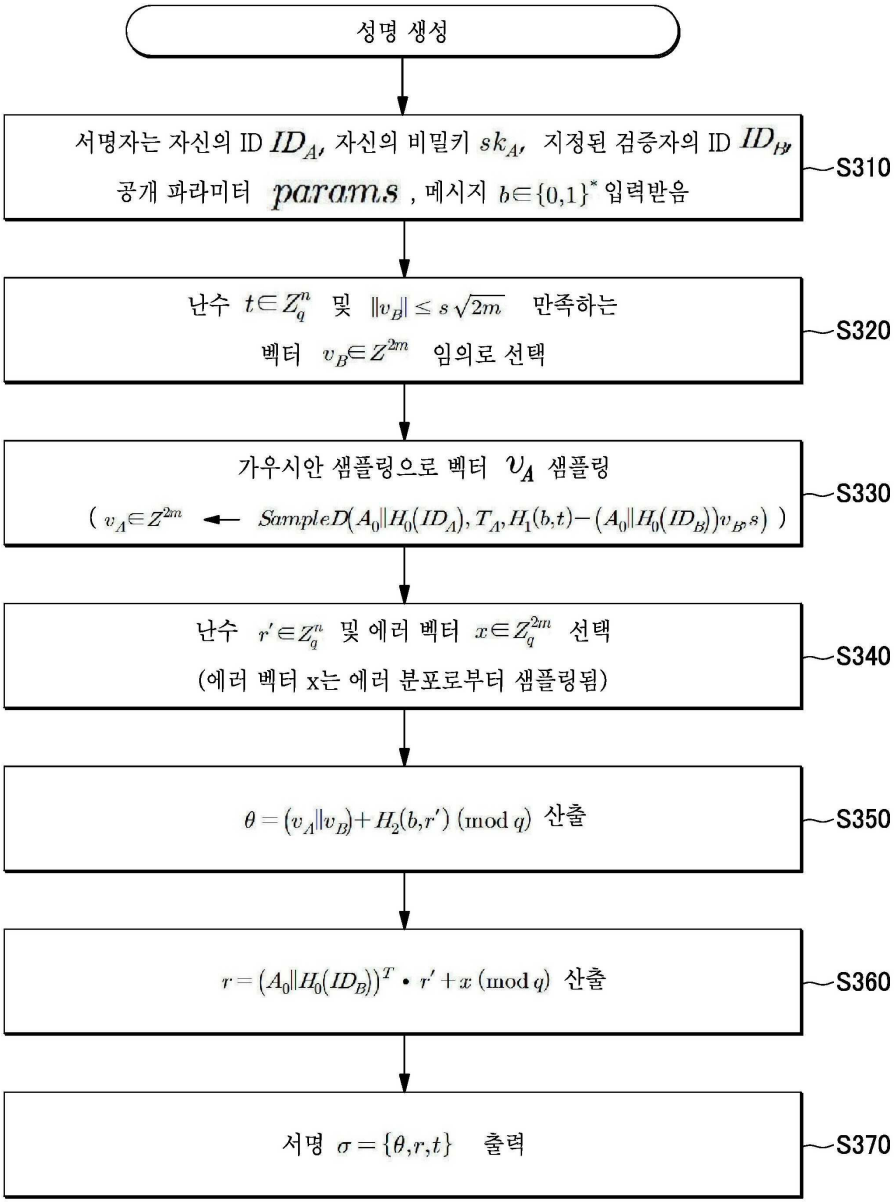
도면7


마스터 키 생성
트랩도어 생성
( $(A_0, T_0) \leftarrow TrapGen(1^n, 1^m, q)$ )
S210
마스터 비밀키를 생성한 트랩도어로 설정
( $msk = T_0$ )
S220
해시 함수 생성
( $H_0 : \{0,1\}^* \rightarrow Z_q^{n \times m}$, $H_1 : \{0,1\}^* \times Z_q^n \rightarrow Z_q^n$, $H_2 : \{0,1\}^* \times Z_q^n \rightarrow Z_q^{4m}$ )
S230
해시 함수 등 공개
( $params = \{A_0, H_0, H_1, H_2\}$ )
S240

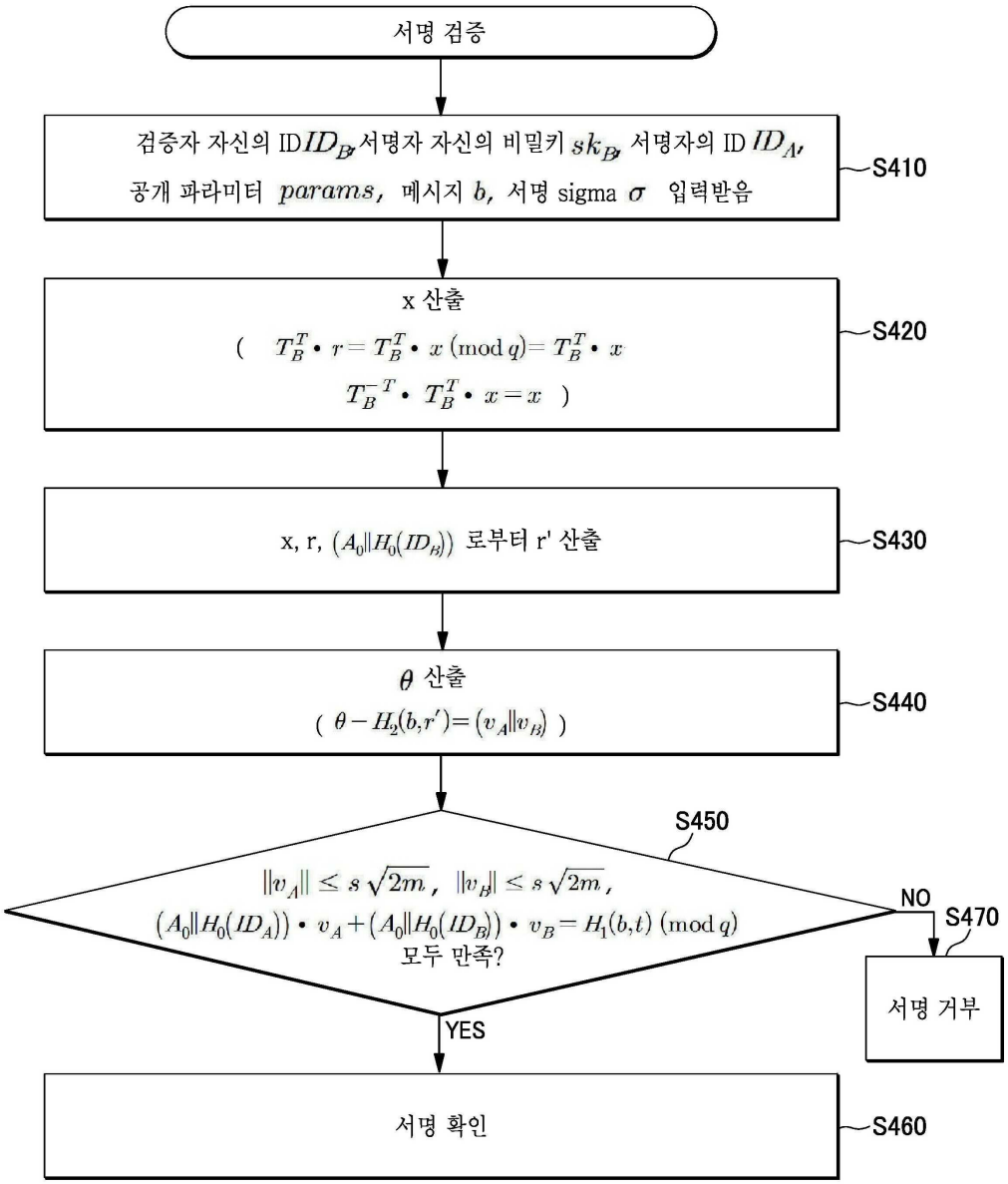
도면8


사용자 키 생성
공개 파라미터 $params$, 마스터 비밀키 $msk = T_0$,
사용자의 ID $ID_{user}$ 입력받음
S210
트랩도어 확장
( $T_{user} \in Z^{2m \times 2m} \leftarrow ExtBasis(T_0, A_0 \| H_0(ID_{user}))$ )
S220
해당 사용자에게 전달
( $sk_{user} = T_{user}$ )
S230

도면9


성명 생성
서명자는 자신의 ID $ID_A$, 자신의 비밀키 $sk_A$, 지정된 검증자의 ID $ID_B$
공개 파라미터 $params$ , 메시지 $b \in \{0,1\}^*$ 입력받음
S310
난수 $t \in Z_q^n$ 및 $\|v_B\| \le s\sqrt{2m}$ 만족하는
벡터 $v_B \in Z^{2m}$ 임의로 선택
S320
가우시안 샘플링으로 벡터 $v_A$ 샘플링
( $v_A \in Z^{2m} \leftarrow SampleD(A_0 \| H_0(ID_A), T_A, H_1(b,t) - (A_0 \| H_0(ID_B))v_B, s)$ )
S330
난수 $r' \in Z_q^n$ 및 에러 벡터 $x \in Z_q^{2m}$ 선택
(에러 벡터 x는 에러 분포로부터 샘플링됨)
S340
$\theta = (v_A \| v_B) + H_2(b,r') \pmod q$ 산출
S350
$r = (A_0 \| H_0(ID_B))^T \cdot r' + x \pmod q$ 산출
S360
서명 $\sigma = \{\theta, r, t\}$ 출력
S370

도면10


서명 검증
검증자 자신의 ID $ID_B$ 서명자 자신의 비밀키 $sk_B$ 서명자의 ID $ID_A$, 공개 파라미터 $params$, 메시지 $b$, 서명 sigma $\sigma$ 입력받음
S410
x 산출
( $T_B^T \cdot r = T_B^T \cdot x \pmod q = T_B^T \cdot x$
$T_B^{-T} \cdot T_B^T \cdot x = x$ )
S420
x, r, $(A_0 \| H_0(ID_B))$ 로부터 r' 산출
S430
$\theta$ 산출
( $\theta - H_2(b,r') = (v_A \| v_B)$ )
S440
S450
$\|v_A\| \le s\sqrt{2m}$, $\|v_B\| \le s\sqrt{2m}$,
$(A_0 \| H_0(ID_A)) \cdot v_A + (A_0 \| H_0(ID_B)) \cdot v_B = H_1(b,t) \pmod q$
모두 만족?
NO
S470
서명 거부
YES
서명 확인
S460