

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2014-0109114 (43) 공개일자 2014년09월15일
(51) 국제특허분류(Int. Cl.) G06F 17/00 (2006.01) G06F 21/00 (2006.01)		(71) 출원인 고려대학교 산학협력단 서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(21) 출원번호 10-2013-0023408		(72) 발명자 정익래 서울 광진구 긴고랑로4길 53, 203호 (중곡동, 호동아파트)
(22) 출원일자 2013년03월05일 심사청구일자 2013년03월05일		천지영 서울 성북구 오패산로 46, 118동 104호 (하월곡동, 월곡두산위브아파트)
		노건태 서울 강남구 개포로 516, 707동 1304호 (개포동, 개포동주공아파트)
		(74) 대리인 특허법인엠에이피에스

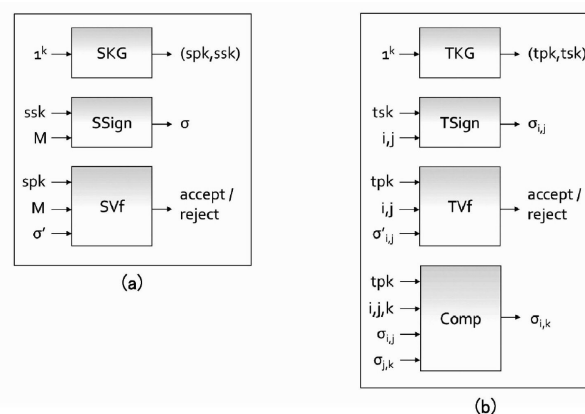
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **이행성 서명 처리 방법**

(57) 요약

무방향 그래프 형태로 이루어진 사용자 단말들을 포함하는 네트워크에서의 이행성 서명 처리 방법은 트랩도어 생성 알고리즘에 따라 생성된 랜덤 행렬 및 이에 대응되는 트랩 도어 행렬에 기초하여 제 1 사용자 단말에 대하여 생성된 공개키 및 서명키를 상기 제 1 사용자 단말이 수신하는 단계 및 제 1 사용자 단말의 공개키 및 서명키와 제 2 사용자 단말에 대한 연결선 정보에 기반하여, 상기 제 1 사용자 단말이 가우시안 샘플링 알고리즘에 따라 추출한 래티스 벡터를 상기 제 1 사용자 단말이 상기 제 2 사용자 단말에 전송하는 메시지에 대한 서명으로서 생성하는 단계를 포함한다.

대표도



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 고려대학교 산학협력단

연구기간 2012.05.01 ~ 2013.04.30

특허청구의 범위

청구항 1

무방향 그래프 형태로 이루어진 사용자 단말들을 포함하는 네트워크에서의 이행성 서명 처리 방법에 있어서,
트랩도어 생성 알고리즘에 따라 생성된 랜덤 행렬 및 이에 대응되는 트랩 도어 행렬에 기초하여 제 1 사용자 단말에 대하여 생성된 공개키 및 서명키를 상기 제 1 사용자 단말이 수신하는 단계 및
제 1 사용자 단말의 공개키 및 서명키와 제 2 사용자 단말에 대한 연결선 정보에 기반하여, 상기 제 1 사용자 단말이 가우시안 샘플링 알고리즘에 따라 추출한 래티스 벡터를 상기 제 1 사용자 단말이 상기 제 2 사용자 단말에 전송하는 메시지에 대한 서명으로서 생성하는 단계를 포함하는 이행성 서명 처리 방법.

청구항 2

제 1 항에 있어서,
상기 공개키는 상기 랜덤 행렬을 포함하고,
상기 서명키는 상기 트랩도어 행렬인 이행성 서명 처리 방법.

청구항 3

제 1 항에 있어서,
상기 제 2 사용자 단말의 공개키 및 서명키와 제 3 사용자 단말에 대한 연결선 정보에 기반하여, 상기 제 2 사용자 단말이 가우시안 샘플링 알고리즘에 따라 추출한 래티스 벡터를 상기 제 2 사용자 단말이 상기 제 3 사용자 단말에 전송하는 메시지에 대한 서명으로서 생성하는 단계를 더 포함하는 이행성 서명 처리 방법.

청구항 4

제 1 항에 있어서,
상기 래티스 벡터를 서명으로서 생성하는 단계는 상기 가우시안 샘플링 알고리즘에 따라 하기의 수학적 식 1을 만족하는 래티스 벡터(v)를 산출하는 이행성 서명 처리 방법.

[수학적 식 1]

$$Av = u \pmod{q}, \quad \|v\| \leq s\sqrt{m}$$

A: 랜덤 행렬, q: 양의 정수, s: 가우시안 파라미터, m: 차원

청구항 5

제 3 항에 있어서,
상기 제 1 사용자 단말이 상기 제 2 사용자 단말에 전송하는 메시지에 대한 서명과 상기 제 2 사용자 단말이 상기 제 3 사용자 단말에 전송하는 메시지에 대한 서명을 결합하여 상기 제 1 사용자 단말이 상기 제 3 사용자 단말에 전송하는 메시지에 대한 서명을 생성하는 단계를 더 포함하는 이행성 서명 처리 방법.

청구항 6

제 1 항에 있어서,
상기 제 1 사용자 단말의 공개키, 상기 제 1 사용자 단말과 제 2 사용자 단말 간의 연결선 정보 및 상기 제 1 사용자 단말이 상기 제 2 사용자 단말에 전송하는 메시지에 대한 서명 정보에 기초하여, 상기 서명의 정당성 여부를 검증하는 단계를 더 포함하는 이행성 서명 처리 방법.

청구항 7

제 6 항에 있어서,

상기 서명의 정당성 여부를 검증하는 단계는 하기 수학적식 2 및 3을 모두 만족하는 경우 해당 서명이 정당한 것으로 판단하는 이행성 서명 처리 방법.

[수학적식 3]

$$\|v_{i,j}\| \leq s \sqrt{m}$$

[수학적식 4]

$$A \cdot v_{i,j} = H(i) - H(j) \pmod{q}$$

A: 랜덤 행렬, i, j: 연결선 정보, q: 양의 정수, s: 가우시안 파라미터, m: 차원, H: 해시함수

청구항 8

청구항 1 내지 7 중 어느 한 항에 기재된 방법을 컴퓨터 상에서 수행하기 위한 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.

명세서

기술분야

[0001] 본 발명은 래티스 기반의 이행성 서명 처리 방법에 관한 것이다.

배경기술

[0002] 이행성 서명(Transitive Signature) 기법은 2002년, Micali와 Rivest에 의해 처음으로 개념이 정립되었다. 메시지에 대해 서명을 수행하는 일반 서명 기법과는 달리, 이행성 서명 기법은 이행적으로 닫혀있는 그래프 내 노드들간의 연결선(edge)에 대해 서명을 수행한다.

[0003] 이행성 서명 기법은 연결선(i, j)에 대한 서명($\sigma_{i,j}$)과 연결선(j, k)에 대한 서명($\sigma_{j,k}$)이 주어졌을 경우, 서명키 없이 공개키만을 가지고 연결선(i, k)에 대한 서명($\sigma_{i,k}$)을 계산해낼 수 있어야 한다는 특징을 가진다. 즉, 세개의 정점(i, j, k)으로 이루어진 그래프에서, 두 개의 연결선((i, j), (j,k))에 기초하여, 나머지 연결선(i,k)에 대한 서명을 획득할 수 있게 된다.

[0004] 정점과 연결선으로 이루어진 관계도는 객체들 간의 관계를 표현하는데 매우 효과적일 수 있다. 예를 들면, 특정 조직에 설치된 컴퓨터 네트워크 구조에서 관리자와 직원의 관계 등을 효율적으로 나타낼 수 있다. 이와 같은 관계도를 활용할 경우, 관계도의 동적인 특성 때문에 노드의 삭제/추가로 인하여 관계도가 변경되는 경우 전체 관계도를 재서명해야 하는 불편함이 있을 수 있다. 이행성 서명 기법은 이와 같은 경우에 관계도의 동적인 특성을 반영할 수 있는 방법인 것으로 알려져 있다.

[0005] 이행성 서명 기법은 서명의 대상이 되는 그래프가 무방향(undirected)인 경우와 방향(directed)인 경우로 구분되며, 본 발명은 무방향 그래프에서의 이행성 서명 처리 방법에 관한 것이다.

[0006] 현재까지 연구된 무방향 그래프에 대한 이행성 서명 기법들은 RSA 암호나 인수분해 문제의 어려움에 기반을 두고 설계되었다. RSA 암호나 인수분해 문제의 어려움에 기반을 두고 설계된 이행성 서명 기법들은 모두 지수 연산 등 효율성이 떨어지는 연산이 요구된다는 단점이 있다.

[0007] 이와 관련하여, 대한민국 공개특허 제2007-0082313호(발명의 명칭: 알에스에이 암호 가정에 기초한 추이적 서명 방법)는 강력한 RSA 가정에 기초한 추이적 서명방법으로서, 수학적 모델링을 통하여 안전성이 매우 엄밀하게 증명되고 있으며, 이에 따라 서명자의 서명방법을 만족시킬 수 있는 정확성을 확인할 수 있는 방법을 제시하고 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 전술한 종래 기술의 문제점을 해결하기 위한 것으로서, 본 발명의 일부 실시예는 래티스에 기반하여 이행성 서명을 처리할 수 있는 방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0009] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면에 따른 이행성 서명 처리 방법은 무방향 그래프 형태로 이루어진 사용자 단말들을 포함하는 네트워크에서 수행되는 것으로, 트랩도어 생성 알고리즘에 따라 생성된 랜덤 행렬 및 이에 대응되는 트랩 도어 행렬에 기초하여 제 1 사용자 단말에 대하여 생성된 공개키 및 서명키를 상기 제 1 사용자 단말이 수신하는 단계 및 제 1 사용자 단말의 공개키 및 서명키와 제 2 사용자 단말에 대한 연결선 정보에 기반하여, 상기 제 1 사용자 단말이 가우시안 샘플링 알고리즘에 따라 추출한 래티스 벡터를 상기 제 1 사용자 단말이 상기 제 2 사용자 단말에 전송하는 메시지에 대한 서명으로서 생성하는 단계를 포함한다.

발명의 효과

[0010] 전술한 본 발명의 과제 해결 수단에 의하면, 무방향 그래프 형태로 이루어진 네트워크에서의 이행성 서명 처리를 수행함에 있어서, 래티스에 기반을 두고 수행할 수 있도록 한다. 래티스에 기반을 두고 설계할 경우 선형 연산들로 이루어지기 때문에 높은 연산 효율성을 가지는 장점이 있다. 또한, 래티스에서 존재하는 어려운 문제들은 최악의 경우에도 어려운 문제들로 알려져 있으며, 이에 기반을 두는 경우 보다 높은 안전성을 제공한다는 장점을 가진다.

도면의 간단한 설명

[0011] 도 1 및 도 2는 본원 발명의 일 실시예에 사용되는 이행성 서명의 개념을 설명하기 위한 도면이다.
 도 3은 본원 발명의 일 실시예에 따른 이행성 서명을 제공하는 시스템을 도시한 도면이다.
 도 4는 본원 발명의 일 실시예에 따른 이행성 서명 처리 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0012] 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.

[0013] 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.

[0014] 도 1 및 도 2는 본원 발명의 일 실시예에 사용되는 이행성 서명의 개념을 설명하기 위한 도면이다.

[0015] 도 1의 (a)와 같은 일반적인 서명 방법에서는 각 사용자 단말(1~5) 간에 전송되는 메시지에 대하여, 해당 메시지를 전송하는 사용자 단말에 의하여 생성된 것임을 확인하는 서명이 생성된다. 즉, 서로 다른 두 단말(i, j)

사이에, 서명($\sigma_{i,j}$) 정보가 생성되어 메시지와 함께 전송될 수 있다.

[0016] 다만, 이러한 경우 네트워크를 구성하는 모든 단말별로 서명 정보가 생성되므로, 다수의 단말이 포함되거나, 단말의 유동적으로 추가 또는 삭제되는 네트워크에서는 서명 관리에 어려움이 있을 수 있다.

[0017] 이에, 도 1의 (b)와 같은 이행성 서명 처리 방법의 개념이 제시되었다. 즉, 제 1 사용자 단말이 제 2 사용자 단말에 대하여 생성한 서명과 제 2 사용자 단말이 제 3 사용자 단말에 대하여 생성한 서명에 기초하여, 제 1 사용자 단말의 제 3 사용자 단말에 대한 서명 정보를 생성할 수 있다.

- [0018] 이와 같은 이행성 서명 처리 방법에서는 도 2에 도시된 바와 같이, 키 생성 모듈(TKG)을 이용하여 공개키(tpk) 및 비밀키(tsk)를 생성하는 단계, 서명 생성 모듈(TSign)을 이용하여 서로 다른 두 사용자 단말간의 서명 ($\sigma_{i,j}$)을 생성하는 단계, 서명 검증 모듈(TVf)을 이용하여 서명($\sigma_{i,j}$)을 검증하는 단계, 서명 결합 모듈(Comp)을 이용하여 서로 다른 두 서명을 결합하여 새로운 서명을 생성하는 단계를 수행할 수 있다.
- [0019] 즉, 종전의 일반적인 서명 방법과는 달리, 이행성을 만족하는 서로 다른 두 서명의 결합을 통해 새로운 서명을 생성할 수 있다.
- [0020] 도 3은 본원 발명의 일 실시예에 따른 이행성 서명을 제공하는 시스템을 도시한 도면이다.
- [0021] 이행성 서명 제공 시스템(10)은 키 생성 서버(110) 및 복수의 사용자 단말(120~140)을 포함한다.
- [0022] 사용자 단말은 네트워크를 통해 키 생성 서버(110)에 접속할 수 있는 컴퓨터나 휴대용 단말기로 구현될 수 있다. 여기서, 컴퓨터는 예를 들어, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(desktop), 랩톱(laptop), 태블릿 PC 등을 포함하고, 휴대용 단말기는 예를 들어, 휴대성과 이동성이 보장되는 무선 통신 장치로서, PCS(Personal Communication System), GSM(Global System for Mobile communications), PDC(Personal Digital Cellular), PHS(Personal Handyphone System), PDA(Personal Digital Assistant), IMT(International Mobile Telecommunication)-2000, CDMA(Code Division Multiple Access)-2000, W-CDMA(W-Code Division Multiple Access), Wibro(Wireless Broadband Internet) 단말, 스마트 폰 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다.
- [0023] 참고로, 본 발명의 실시예에 따른 도 3에 도시된 구성 요소들은 소프트웨어 또는 FPGA(Field Programmable Gate Array) 또는 ASIC(Application Specific Integrated Circuit)와 같은 하드웨어 구성 요소를 의미하며, 소정의 역할들을 수행한다.
- [0024] 그렇지만 '구성 요소들'은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니며, 각 구성 요소는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다.
- [0025] 따라서, 일 예로서 구성 요소는 소프트웨어 구성 요소들, 객체지향 소프트웨어 구성 요소들, 클래스 구성 요소들 및 태스크 구성 요소들과 같은 구성 요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다.
- [0026] 구성 요소들과 해당 구성 요소들 안에서 제공되는 기능은 더 작은 수의 구성 요소들로 결합되거나 추가적인 구성 요소들로 더 분리될 수 있다.
- [0027] 키 생성 서버(110)는 사용자 단말(120~140)의 요청에 따라 공개키(pk) 및 서명키(sk)를 생성하여 사용자 단말에 제공한다. 예를 들면, 키 생성 서버(110)는 PKI(Public Key Infrastructure) 기반의 키 생성 기관에 설치될 수 있으나, 이에 한정되는 것은 아니다. 이때, 공개키 기반의 키 생성 방식은 서로 대응되는 키 쌍을 생성하여, 이중 공개키는 암호화 또는 서명 확인용으로, 비밀키는 복호화 또는 서명용으로 사용하는 비대칭형 암호화 또는 서명 방식이다. 해당 메시지를 보낸 사용자가 누구인가를 증명하기 위한 것이므로, 어떤 메시지에 서명할 때는 비밀키로 서명하고 대응되는 공개키로 이를 확인할 수 있다. 즉, 비밀키는 문서에 찍는 도장의 기능을 한다. 따라서 종래의 공개키 기반 환경에서는 메시지를 주고 받는 당사자 이외의 사용자도 누가 메시지에 서명했는지 확인할 수 있다.
- [0028] 키 생성 서버(110)는 트랩도어 생성 알고리즘에 따라 생성된 랜덤 행렬 및 이에 대응되는 트랩도어 행렬에 기초하여 공개키 및 서명키를 생성한다.
- [0029] 암호화 및 전자 서명 시스템은 특정 정보가 없으면 풀기 어려운 수학적 난제에 기반하여 구축되는데, 본 발명의 일 실시예에 따른 이행성 서명 시스템(10)은 래티스(lattice) 상에서의 SIS(small integer solution) 문제와 LWE(learning with errors) 문제의 어려움에 기반하고 있다.
- [0030] 특정 정보가 없으면 풀기 어렵다는 것은 연산이 일방향성이라는 의미이다. 일방향성은 연산은 쉬워도 연산의 역을 구하는 것은 매우 어려우며, 이때 특정 정보를 갖고 있는 경우에는 쉽게 연산의 역을 구할 수 있음을 나타낸다. 이러한 특정 정보를 트랩도어(trapdoor)라고 부른다.
- [0031] 예를 들어, 공개키 기반 환경에서 암호화 연산은 암호화는 쉽지만 그 역변환인 복호화는 암호화시 사용한 암호

화 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 공개되어서는 안된다. 따라서, 공개키 기반 환경에서 트랩도어를 생성하는 데 사용된 정보는 공개키로서 공개되고, 트랩도어는 비밀키로서 공개되지 않는다.

[0032] 따라서 본 발명의 일실시예에 따른 이행성 서명 시스템(10)은 각 사용자의 서명키로 사용할 트랩도어를 생성하며, 이때 트랩도어는 래티스의 기저이다.

[0033] 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 기저 내 벡터들의 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.

[0034] 예를 들어, 키 생성 서버(110)는 보안 파라미터 n , 차원 $m = O(n \log q)$, 양의 정수 q 를 입력 받아서 트랩도어 생성 알고리즘($TrapGen(1^n, 1^m, q)$)을 통해, 균일한 분포를 가지는 랜덤 행렬($A \in Z_q^{n \times m}$)을 생성하고, 이에 대응되는 트랩도어 행렬($T \in Z_q^{m \times m}$)을 생성한다. 그리고, 키 생성 서버(110)는 해시함수 $H: \{0,1\}^* \rightarrow Z_q^n$ 를 선택한다. 그리고, 이에 기초하여 공개키 및 서명키를 생성하는데, 공개키는 랜덤 행렬 및 해시함수를 포함하고 $pk = \{A, H\}$, 서명키는 트랩도어 행렬($sk = T$)이다.

[0035] 한편, 각각의 사용자 단말(120~140)은 서명을 생성하는 서명 생성부(122, 132, 142), 서명을 검증하는 서명 검증부(124, 134, 144) 및 서명 결합부(126, 136, 146)를 포함한다. 설명의 간단을 위하여 제 1 사용자 단말(120)을 기준으로 각각의 세부 구성 요소를 설명하기로 한다.

[0036] 서명 생성부(122)는 키 생성 서버(110)로부터 수신한 사용자 단말의 공개키 및 서명키와 연결선 정보에 기반하여, 가우시안 샘플링 알고리즘에 따라 서명을 생성한다. 예를 들어, 제 1 사용자 단말(120)이 제 2 사용자 단말(130)에 대해서 전송한 메시지에 대하여 서명을 생성하는 경우, 자신의 공개키($pk = \{A, H\}$), 자신의 서명키($sk = T$) 및 제 1 사용자 단말(120)과 제 2 사용자 단말(130) 사이의 연결선(i, j) 정보에 기반하여, 가우시안 샘플링 알고리즘($SampleD(A, T, H(i) - H(j), s)$)을 사용하여 래티스 벡터($v_{i,j} \in Z^m$)를 샘플링한다. 이때, 가우시안 샘플링 알고리즘은 랜덤 행렬($A \in Z_q^{n \times m}$), 트랩도어 행렬($T \in Z_q^{m \times m}$), 벡터($u \in Z_q^n$), 가우시안 파라미터 s 를 입력받아서, 미리 설정된 아래 수학식 1 및 2를 만족시키는 래티스 벡터를 샘플링한다.

[0037] [수학식 1]

$$Av = u \pmod{q}$$

[0038]

[0039] [수학식 2]

$$\|v\| \leq s \sqrt{m}$$

[0040]

[0041] 이와 같이, 추출된 래티스 벡터는 제 1 사용자 단말(120)이 제 2 사용자 단말(130)에 대해서 전송한 메시지에 대한 서명으로서 사용된다. 이때, 서명은 $\sigma_{i,j} = v_{i,j}$ 이다.

[0042] 서명 검증부(124)는 다른 사용자 단말에 의하여 생성된 서명을 검증한다. 즉, 다른 사용자 단말의 공개키 ($pk = \{A, H\}$), 연결선 정보 및 메시지에 대한 서명 정보에 기초하여 서명의 정당성 여부를 검증할 수 있다. 예를 들어, 서명 검증부(124)는 제 2 사용자 단말(130)의 공개키 및 제 2 사용자 단말(130)이 제 3 사용자 단말(140)에 전송한 메시지에 대한 서명 정보에 기초하여, 해당 서명이 제 2 사용자 단말(130)에 의하여 수행된 것임을 검증한다.

[0043] 서명 검증부(124)는 서명자의 공개키($pk = \{A, H\}$), 검증 대상 서명이 전달된 연결선(i, j)에 대한 정보 및 서명 정보($\sigma_{i,j} = v_{i,j}$)를 입력 받아, 미리 설정된 아래 수학식 3 및 4를 만족시키는지 여부에 기초하여 서명을 검증한다.

[0044] [수학식 3]

$$\|v_{i,j}\| \leq s \sqrt{m}$$

[0045]

[0046] [수학식 4]

$$A \cdot v_{i,j} = H(i) - H(j) \pmod{q}$$

[0047]

[0048] 즉, 수학식 3 및 4를 모두 만족하면, 서명 정보($\sigma_{i,j} = v_{i,j}$)가 정당한 서명인 것으로 판단한다.

[0049] 서명 결합부(126)는 이행성을 만족하는 서로 다른 둘 이상의 서명을 결합하여 새로운 서명을 생성할 수 있다. 즉, 도 1의 (b)와 같이 서명이 생성되지 않은 사용자 단말(1)과 사용자 단말(3) 사이에서, 사용자 단말(1)에 의하여 생성된 서명과 사용자 단말(2)에 의하여 생성된 서명을 결합하여, 사용자 단말(1)과 사용자 단말(3) 사이의 서명을 생성할 수 있다.

[0050] 예를 들어, 각 서명자의 공개키($pk = \{A, H\}$), 연결선 (i, j)와 연결선(j, k)에 대한 정보, 연결선 각각에 대한 서명($\sigma_{i,j} = v_{i,j}$, $\sigma_{j,k} = v_{j,k}$)를 입력 받아, 하기 수학식 5에 따라 새로운 서명을 생성한다.

[0051] [수학식 5]

$$v_{i,k} = v_{i,j} + v_{j,k}$$

[0052]

[0053] 상기 수학식 5와 같이 서로 다른 두 서명의 결합을 통해 새로운 서명을 생성할 수 있는 배경은 아래 수학식 6과 같다.

[0054] [수학식 6]

$$A \cdot v_{i,j} = H(i) - H(j) \pmod{q}$$

$$A \cdot v_{j,k} = H(j) - H(k) \pmod{q}$$

$$A \cdot (v_{i,j} + v_{j,k}) = H(i) - H(k) \pmod{q} = A \cdot v_{i,k}$$

[0055]

[0056] 이때, 결합된 서명은 $\sigma_{i,k} = v_{i,k}$ 이다.

[0057] 이와 같이, 본 발명의 이행성 서명 시스템(10)에 포함된 각각의 사용자 단말은 래티스 기반의 이행성 서명 처리 방법에 따라, 서명, 서명 검증, 서명 결합을 수행할 수 있다.

[0058] 도 4는 본원 발명의 일 실시예에 따른 이행성 서명 처리 방법을 도시한 순서도이다.

[0059] 먼저, 키 생성 서버(110)가 사용자 단말의 요청에 따라 공개키와 서명키를 생성한다(S410). 앞서 설명한 바와 같이, 트랩도어 생성 알고리즘에 따라 생성된 랜덤 행렬 및 이에 대응되는 트랩도어 행렬에 기초하여 공개키 및 서명키를 생성한다. 공개키는 랜덤 행렬 및 해시함수를 포함하고, 서명키는 트랩도어 행렬인데, 이 트랩도어 행렬은 일련의 래티스 벡터가 모인 행렬이다.

[0060] 다음으로, 공개키 및 서명키에 기초하여 각 사용자 단말에서 서명을 생성한다(S420). 예를 들어, 제 1 사용자 단말(120)은 자신의 공개키 및 서명키에 기초하여, 제 2 사용자 단말(130)로 전송하는 메시지에 대한 서명을 생성한다. 이때, 가우시안 샘플링 알고리즘에 따라 수학식 1 및 2를 만족하는 래티스 벡터를 추출하고, 이를 서명으로서 사용한다.

[0061] 다른 사용자 단말에서도 이와 같은 과정을 통해 각자의 서명을 생성할 수 있다.

[0062] 다음으로, 서로 다른 서명을 결합하여 새로운 서명을 생성한다(S430).

[0063] 즉, 제 1 사용자 단말(120)이 제 2 사용자 단말(130)로 전송한 메시지에 대한 서명과 제 2 사용자 단말(130)이 제 3 사용자 단말(140)로 전송한 메시지에 대한 서명을 결합하여, 제 1 사용자 단말(120)이 제 3 사용자 단말(140)로 전송한 메시지에 대한 서명을 생성할 수 있다.

[0064] 한편, 이와 같이 생성된 각각의 서명에 대해서는 래티스 벡터의 추출과정을 활용하여 서명에 대한 검증을 수행할 수 있다. 즉, 서명자의 공개키 및 서명 정보에 기초하여, 수학식 3 및 4를 만족하는지 여부를 확인하는 과정을 통해 검증을 수행한다.

[0065] 본 발명의 일 실시예는 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.

[0066] 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.

[0067] 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.

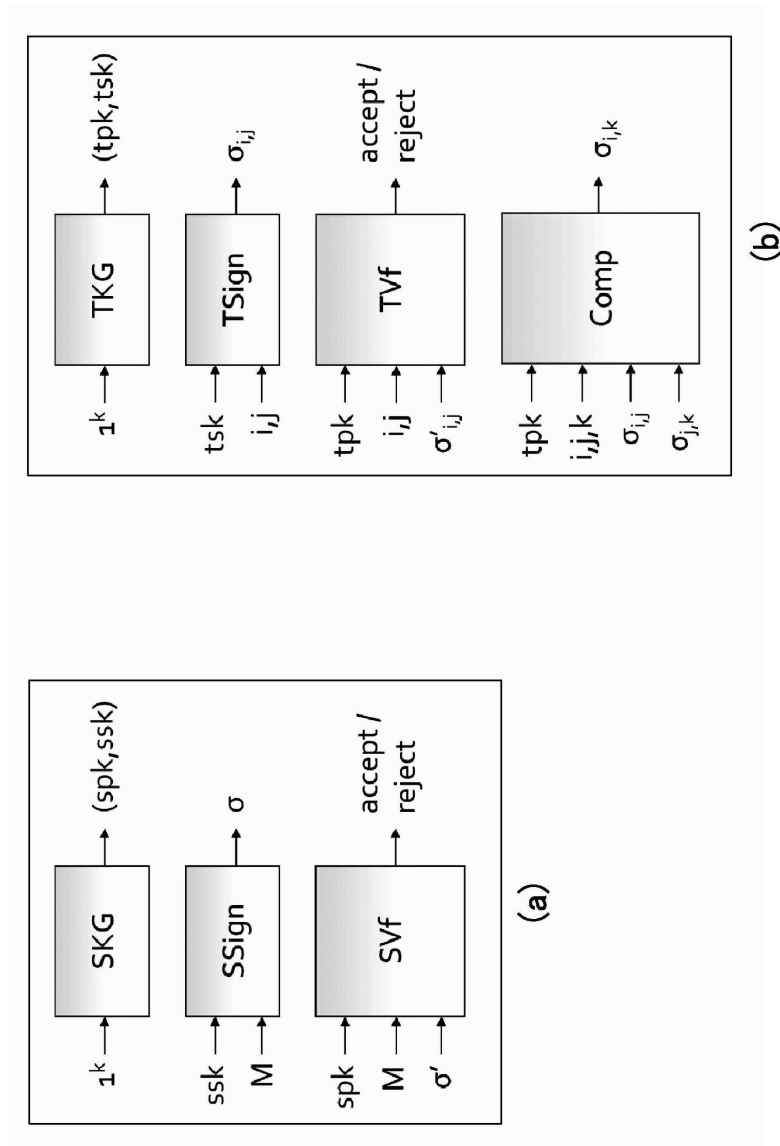
부호의 설명

[0068]

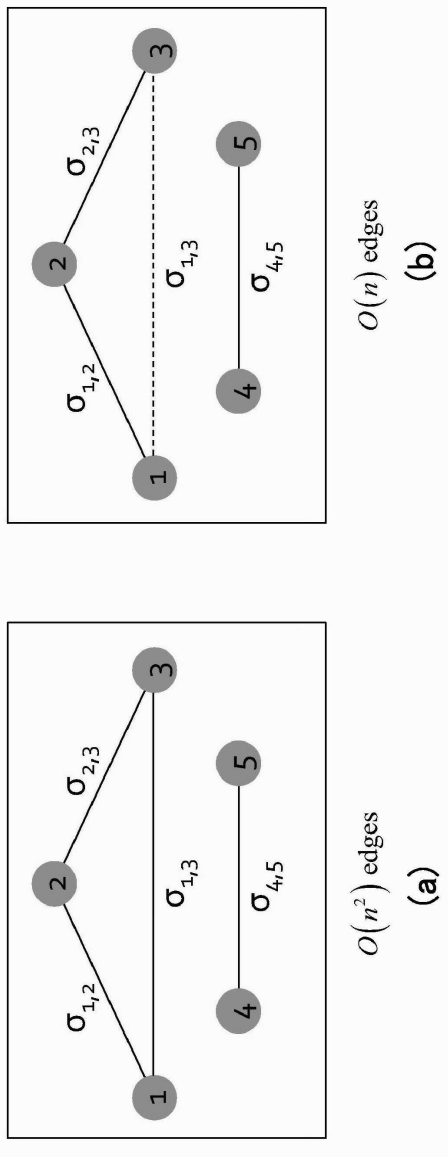
10: 이행정 서명 시스템 110: 키 생성 서버
120: 사용자 단말 122: 서명 생성부
124: 서명 검증부 126: 서명 결합부

도면

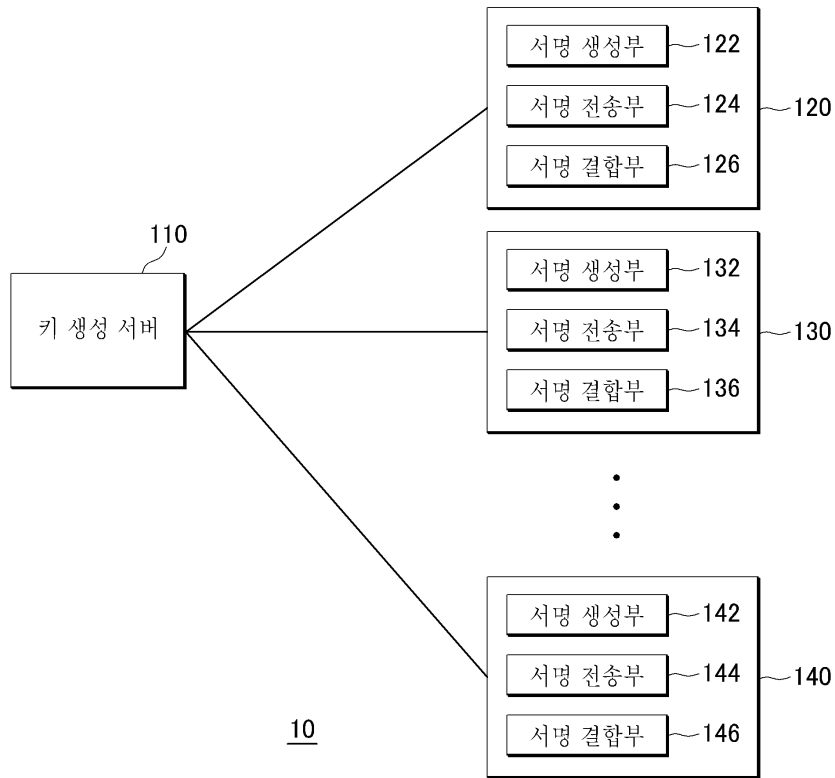
도면1



도면2



도면3



도면4

