



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0076009
(43) 공개일자 2014년06월20일

(51) 국제특허분류(Int. Cl.)

H04L 9/30 (2006.01)

(21) 출원번호 10-2012-0144050

(22) 출원일자 2012년12월12일

심사청구일자 없음

(71) 출원인

한국전자통신연구원

대전광역시 유성구 가정로 218 (가정동)

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

조남수

대전 유성구 온천북로33번길 22-9, 정다운집 402호 (봉명동)

노건태

서울 강남구 개포로 516, 707동 1034호 (개포동, 개포동주공아파트)

정익래

서울 광진구 긴고랑로4길 53, 203호 (중곡동, 호동아파트)

(74) 대리인

특허법인이지

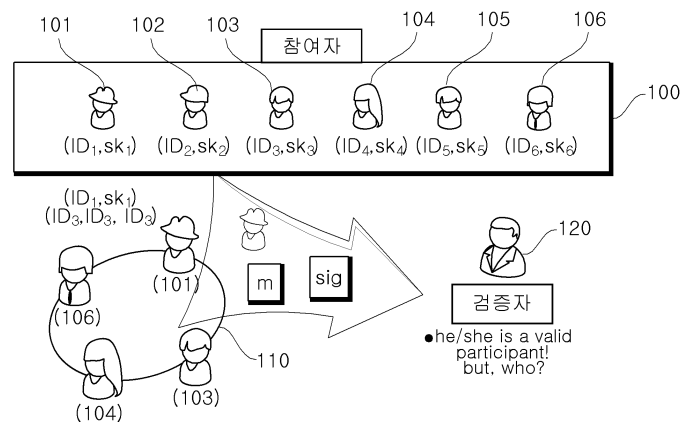
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 강한 위조 불가능성을 만족하는 ID 기반 링 서명 장치

(57) 요약

본 발명의 일실시예에 따른 강한 위조 불가능성을 만족하는 ID 기반 링 서명 장치는 시큐리티 파라미터, 래티스 구성 정보를 이용하여 서버의 마스터 비밀키와, 서명 장치의 공개 파라미터를 생성하는 파라미터 생성부; 상기 생성된 마스터 비밀키 및 공개파라미터와, 링 서명에 참여하는 참여자의 공개 ID(Identification)를 이용하여 참여자 비밀키를 생성하는 비밀키 생성부; 상기 참여자 중 한 명의 서명자가 자신의 비밀키와, 서명자가 임의로 구성한 참여자 ID 집합(링)과, 메시지를 이용하여 서명을 생성하는 서명 생성부; 및 상기 생성된 서명이 상기 참여자 ID 집합 및 참여자 메시지에 대한 정당한 서명인지를 검증하여 참 또는 거짓에 대한 결과를 출력하는 서명 검증부;를 포함하며, 강한 위조 불가능성을 만족한다.

대표도 - 도1



특허청구의 범위

청구항 1

링 서명 장치에 있어서,

시큐리티 파라미터 및 래티스 구성 정보를 이용하여 서버의 마스터 비밀키와, 서명 장치의 공개 파라미터를 생성하는 파라미터 생성부;

상기 생성된 마스터 비밀키 및 공개파라미터와, 링 서명에 참여하는 참여자의 공개 ID(Identification)를 이용하여 참여자 비밀키를 생성하는 비밀키 생성부;

상기 참여자 중 한 명의 서명자가 자신의 비밀키와, 서명자가 임의로 구성한 참여자 ID 집합(링)과, 메시지를 이용하여 서명을 생성하는 서명 생성부; 및

상기 생성된 서명이 상기 참여자 ID 집합 및 메시지에 대한 정당한 서명인지를 검증하여 참 또는 거짓에 대한 결과를 출력하는 서명 검증부;

를 포함하는 ID 기반 링 서명 장치.

명세서

기술 분야

[0001] 본 발명은 ID 기반 링 서명 장치에 관한 것으로서, 더욱 상세하게는 링 서명 참여자 ID를 이용한 강한 위조 불가능성을 만족하는 ID 기반 링 서명 장치에 관한 것이다.

배경 기술

[0002] 2001년, Ronald L. Rivest 등에 의해 링 서명 기법에 대한 개념이 처음으로 소개되었다. 링 서명 기법은 서명자가 다수의 참여자를 자신이 원하는 대로 선택하고, 서명자가 자신이 선택한 다수의 참여자를 대표하여 메시지에 서명하는 것을 의미한다.

[0003] 여기서, 서명자가 선택한 다수의 참여자를 포함하는 집합을 링이라고 한다. 링 서명 기법에서 검증자는 링 서명을 통하여 링에 포함된 참여자 중의 한 명이 서명하였다는 사실만을 알 수 있으며, 링에 포함된 참여자 중에서 누가 링 서명을 했는지에 대한 정보는 알 수 없다. 다시 말하면, 링 서명 기법은 기본적으로 서명자의 익명성을 제공해야 하며, 서명 기법이 기본적으로 제공해야 하는 위조 불가능성 또한 제공해야 한다.

[0004] 기존의 링 서명 기법에서는 서명을 검증하기 위한 공개키 인증을 위해서 PKI(공개키 기반 구조, Public Key Infrastructure)가 요구된다. 또한 기존의 링 서명 기법의 공개키는 사용자 측면에서 볼 때 난수 형태로 구성된다. 반면 ID 기반 링 서명 기법에서는 사용자의 ID가 공개키의 역할을 하여 PKI가 요구되지 않는다.

[0005] 위조 불가능성은 약한 위조 불가능성과 강한 위조 불가능성으로 나눌 수 있다. 약한 위조 불가능성 모델에서 공격자는 위조하고자 하는 링-메시지 쌍을 서명 오라클에 물어볼 수 없지만, 강한 위조 불가능성 모델에서는 이것을 허용한다. 즉, 강한 위조 불가능성은 약한 위조 불가능성과 비교하여 공격자에게 보다 많은 능력을 허용하는 강한 안전성 요구 조건이다.

[0006] 최근에 설계되고 있는 일반 서명 기법들은 강한 위조 불가능성을 만족하도록 설계되는 추세이지만, 강한 위조 불가능성을 만족하는 ID 기반 링 서명 기법은 아직까지 설계되지 못하였다.

발명의 내용

해결하려는 과제

[0007] 본 발명의 목적은, 강한 위조 불가능성을 만족하는 ID 기반 링 서명 장치를 제공하는 데 있다.

과제의 해결 수단

[0008] 본 발명의 일실시예에 따른 ID 기반 링 서명 장치는 초기 설정된 시큐리티 파라미터 및 래티스 구성 정보를 이

용하여 서버의 마스터 비밀키와, 서명 장치의 공개 파라미터를 생성하는 파라미터 생성부; 상기 생성된 마스터 비밀키 및 공개파라미터와, 링 서명에 참여하는 참여자의 공개 ID(Identification)를 이용하여 참여자 비밀키를 생성하는 비밀키 생성부; 상기 참여자 중 한 명의 서명자가 자신의 비밀키와, 서명자가 임의로 구성한 참여자 ID 집합(링)과, 메시지를 이용하여 서명을 생성하는 서명 생성부; 및 상기 생성된 서명이 상기 참여자 ID 집합 및 메시지에 대한 정당한 서명인지를 검증하여 참 또는 거짓에 대한 결과를 출력하는 서명 검증부를 포함한다.

[0009] 상기 파라미터 생성부는, 상기 시큐리티 파라미터, 래티스의 구성 정보에 기초한 GenBasis 알고리즘을 이용하여 패리티 검사행렬과 래티스의 트랩도어 행렬을 생성하는 것이 가능하다.

[0010] 상기 비밀키 생성부는, 상기 링 서명에 참여하는 모든 참여자의 ID를 공개키로 사용하여, 이에 대응되는 상기 참여자 비밀키를 생성하는 것이 가능하다.

[0011] 상기 서명 생성부는, SampleD(ExtBasis) 알고리즘을 이용하여 상기 래티스에 대응되는 코셋의 원소를 가우시안 샘플링하는 것이 가능하다.

[0012] 상기 서명 검증부는, $\|v\| < s \cdot \sqrt{(|R|+2)m}$ 과 $A_{R,u}v = u \pmod{q}$ 를 둘 다 만족하는 경우에는 검증 성공값을 출력하고, 그렇지 않은 경우에는 검증 실패값을 출력하는 것이 가능하다.

발명의 효과

[0013] 본 발명의 실시예들에 따른 강한 위조 불가능성을 만족하는 ID 기반 링 서명 장치는 래티스를 기반으로 설계되어, 기존의 접전형 사상을 기반으로 하여 설계된 대부분의 링 서명 기법들과 비교하여 보다 안전하며 연산이 효율적인 효과가 있다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 일실시예에 따른 ID 기반 링 서명 기법에 대한 기본 구조도이고,

도 2는 본 발명의 일실시예에 따른 ID 기반 링 서명 장치의 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0015] 본 발명의 실시예들의 설명을 위한 각 도면의 구성 요소들에 참조 부호를 부가함에 있어서, 동일한 구성 요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략하며, 단수로 기재된 용어도 복수의 개념을 포함할 수 있다. 또한, 이하에서 본 발명의 바람직한 실시예를 설명할 것이나, 본 발명의 기술적 사상은 이에 한정하거나 제한되지 않고 당업자에 의해 변형되어 다양하게 실시될 수 있음은 물론이다.

[0016] 첨부된 블록도의 각 블록과 흐름도의 각 단계의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수도 있다. 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다. 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 블록도의 각 블록 또는 흐름도 각 단계에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다. 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 블록도의 각 블록 및 흐름도의 각 단계에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0017] 또한, 각 블록 또는 각 단계는 특정된 논리적 기능을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 실시 예들에서는 블록들 또는 단계들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 블록들 또는 단계

들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

[0018] ID 기반 링 서명 기법은 ID 기반 서명 기법과 링 서명 기법의 성질을 결합한 개념이다. ID 기반 암호 시스템에 대한 개념은 1984년, Adi Shamir에 의해 이 처음으로 소개되었다.

[0019] 이하, 첨부된 도면들을 참조하여 본 발명의 실시예들을 상세히 설명한다.

[0020] 도 1은 본 발명의 일실시예에 따른 ID 기반의 링 서명 방법이 적용되는 기본 구조를 도시한 것이다.

[0021] 도 1을 참조하면, 본 발명의 실시예에 적용되는 ID 기반의 링 서명 방법에서 서명자(101)는 다수의 참여자 그룹(100) 중 임의의 참여자들을 선택한 후 선택한 참여자들(101,103,104,106)을 이용하여 자신을 포함한 링(110)을 형성하고, 구성된 링(110)을 대표하여 메시지에 대한 서명을 수행할 수 있다. ID 기반 링 서명 방법에 있어서, 서명을 검증하는 검증자(120)는 링(110)의 멤버 중 한 명이 서명하였다는 것만 알 수 있으며, 링(110)의 멤버 중 누가 서명했는지를 결코 알 수 없다.

[0022] 본 발명의 실시예들을 기술하기에 앞서, 본 발명의 실시예들에서 사용될 표기들을 정리한다. 시큐리티 파라미터는 n 으로 표기하며, 정수 $q \geq 1$ 로 모듈러(modulo)한 정수들의 집합은 Z_q 로 나타낸다. 특별한 설명이 없는 한, 벡터(vector)는 소문자로 표시하고, 행렬(matrix)은 대문자로 표시하기로 한다. 예를 들면, 벡터는 v 로 표기하고, 행렬은 V 로 표기한다. 임의의 벡터 v 에 대해 $\|v\|$ 는 v 의 길이를 의미하고, 임의의 집합 R 에 대해 $|R|$ 은 R 에 포함된 원소의 개수를 나타낸다. 행렬 $A \parallel B$ 는 행렬 A 와 B 가 순차적으로 결합한 것을 의미한다. $\tilde{S}$ 는 행렬 S 의 그램-슈미트 직교화를 나타낸다.

[0023] 본 발명의 실시예들은 $SampleD$, $GenBasis$, $ExtBasis$ 알고리즘을 사용하여 수행된다. 이 알고리즘들은 모두 m 차원의 풀-랭크 정수 래티스에서 정의된다. m 차원의 풀-랭크 정수 래티스는 다음과 같다. 여기서 $n \geq 1$ 과 $q \geq 2$ 는 모두 정수이며, m 은 본 실시예에서 사용되는 시큐리티 파라미터이고, 모든 다른 파라미터들은 m 으로부터 파생된다.

[0024] 또한, 차원 하드 래티스 $\Lambda^\perp(A)$ 는 패리티 검사 행렬 $A \in Z_q^{n \times m}$ 로부터 다음과 같이 정의된다.

[0025]
$$\Lambda^\perp(A) = \{v \in Z_q^m : Av = 0 \in Z_q^n\} \subseteq Z_q^m$$

[0026] 그리고 어떤 u 에 대해서, $A \in Z_q^{n \times m}$ 에 의해 생성되는 m 차원 하드 래티스 $\Lambda^\perp(A)$ 에 대응되는 코셋 $\Lambda_u^\perp(A)$ 은 다음과 같이 정의 된다.

[0027]
$$\Lambda_u^\perp(A) = \{v \in Z_q^m : Av = u \in Z_q^n\} = \Lambda^\perp(A) + \overline{v}$$

[0028] 여기서 $\overline{v} \in Z_q^m$ 는 $\Lambda^\perp(A)$ 에 속하는 임의의 원소이다.

[0029] *SampleD* 알고리즘:

[0030] 본 발명의 실시예에서는 *SampleD* 알고리즘을 사용한다. 하지만 이와 동일한 결과를 가지는 다른 알고리즘들을 사용해도 발명을 구성하는 것에 영향을 받지 않음을 미리 밝힌다. 여기서 $T \in \mathbb{Z}_q^{m \times m}$ 는 어떤 패리티 검사 행렬 $A \in \mathbb{Z}_q^{n \times m}$ 로부터 생성되는 m 차원 하드 래티스 $\Lambda^\perp(A)$ 의 트랩도어 행렬을 나타내며, 가우시안 파라미터는 $s \geq \|T\| \cdot \omega(\sqrt{\log n})$ 이다. 그러면 트랩도어 행렬 T 를 사용하여 래티스 $\Lambda^\perp(A)$ 에 대응되는 코셋 $\Lambda_u^\perp(A)$ 으로부터 가우시안 샘플링을 할 수 있는 알고리즘 $\text{SampleD}(T, u, s)$ 이 존재한다. 그리고 트랩도어 행렬 T 를 알지 못하는 경우, 래티스 $\Lambda^\perp(A)$ 에 대응되는 코셋 $\Lambda_u^\perp(A)$ 으로부터 가우시안 샘플링을 할 수 있는 방법은 존재하지 않는다. 여기서 $\text{SampleD}(T, u, s)$ 알고리즘으로부터 샘플링된 v 의 출력 범위는 극단적인 확률로 $\|v\| \leq s\sqrt{m}$ 이다.

[0031] *GenBasis* 알고리즘:

[0032] 본 발명에서는 *GenBasis* 알고리즘을 사용한다. 하지만 이와 동일한 결과를 가지는 다른 알고리즘들을 사용해도 발명을 구성하는 것에 영향을 받지 않음을 미리 밝힌다. *GenBasis* 알고리즘은 입력으로 $(1^n, 1^m, q)$ 를 받으며, 여기서 차원 m 의 범위는 $m \geq Cn \log q$ 이다 (C 는 상수이다.). 그러면 패리티 검사 행렬 $A \in \mathbb{Z}_q^{n \times m}$ 와 래티스 $\Lambda^\perp(A)$ 의 트랩도어 행렬 $T \in \mathbb{Z}_q^{m \times m}$ 를 동시에 생성할 수 있는 알고리즘 $\text{GenBasis}(1^n, 1^m, q)$ 이 존재한다. 여기서 $\|T\| \leq O(\sqrt{n \log q})$ 이다.

[0033] *ExtBasis* 알고리즘:

[0034] 본 발명에서는 *ExtBasis* 알고리즘을 사용한다. 하지만 이와 동일한 결과를 가지는 다른 알고리즘들을 사용해도 발명을 구성하는 것에 영향을 받지 않음을 미리 밝힌다. *ExtBasis* 알고리즘은 입력으로 $(T, A' = A \text{PVER} \overline{A})$ 을 받으며, 여기서 $T \in \mathbb{Z}_q^{m \times m}$ 는 래티스 $\Lambda^\perp(A)$ 의 트랩도어 행렬이며, $\Lambda^\perp(A)$, $\overline{A} \in \mathbb{Z}_q^{m \times m}$ 이다. 그러면 래티스 $\Lambda^\perp(A')$ 의 트랩도어 행렬 $T' \in \mathbb{Z}_{(m+\overline{m}) \times (m+\overline{m})}$ 을 생성할 수 있는 알고리즘 $\text{ExtBasis}(T, A' = A \parallel \overline{A})$ 이 존재한다. 여기서 $\|T'\| = \|T\|$ 이다.

[0035] 도 2는 본 발명의 일실시예에 따른 ID 기반 링 서명 장치의 구성도이다

[0036] 도 2를 참조하면, 본 발명의 일실시예에 따른 ID 기반 링 서명 장치는 서버의 마스터 비밀키와, 서명 장치의 공개 파라미터를 생성하는 파라미터 생성부(210); 참여자 비밀키를 생성하는 비밀키 생성부(220); ID 기반의 링 서명을 생성하는 서명 생성부(230); 및 서명이 참 또는 거짓에 대한 결과를 출력하는 서명 검증부(240)를 포함한다.

[0037] 제안하는 강한 위조 불가능성을 만족하는 ID 기반 링 서명 기법은 앞서 설명한 *SampleD*, *GenBasis*, *ExtBasis* 알고리즘을 사용하여 구성된다. 시큐리티 파라미터 n , 차원 m , 가우시안 파라미터 s 등은 기본적으로 위에서 설정한 범위를 그대로 따르지만, 본 발명의 기술 사상 범위 내에서 다양하게 변형이 가능하다.

[0038] 파라미터 생성부(210)는 $KeyGen(1^n, 1^m, q)$ 알고리즘을 이용하여 시큐리티 파라미터, 래티스 구성 정보를 이용하여 서버의 마스터 비밀키와, 서명 장치의 공개 파라미터를 생성한다.

[0039] 구체적으로, $GenBasis(1^n, 1^m, q)$ 알고리즘을 사용하여 행렬 $A_0 \in Z_q^{n \times m}$ 와 래티스 $\Lambda^\perp(A_0)$ 의 트랩도어 행렬 $T_0 \in Z_q^{m \times m}$ 를 생성한다. T_0 는 마스터 비밀키 msk 로 사용된다. 공개 파라미터 $params$ 는 $\{A_0, E_0, E_1, C_0, \dots, C_h, u, H(\cdot, \cdot), E(\cdot)\}$ 이며, 여기서 행렬 $E_0, E_1 \in Z_q^{n \times m}$, 행렬 $C_0, \dots, C_h \in Z_q^{n \times m}$, 벡터 $u \in Z_q^n$, h -비트의 출력 값을 가지는 해시 함수 $H(\cdot, \cdot)$, 그리고 인코딩 함수 $E(\cdot): Z_q^n \rightarrow Z_q^{n \times n}$ 이다.

[0040] 비밀키 생성부(220)는 $Extract(params, msk, ID_i)$ 알고리즘을 이용하여 링 서명에 참여하는 모든 참여자의 ID를 공개키로 사용하여, 이에 대응되는 상기 참여자 비밀키를 생성한다.

[0041] 구체적으로, 링 서명에 참여하는 모든 참여자들은 자신의 아이디인 $ID_i \in Z_q^n$ 을 공개키로 사용하며, 이것에 대응되는 비밀키 $sk_i = T_i$ 을 발급받아 서명을 생성하는 데 사용한다. T_i 은 래티스 $\Lambda^\perp(A_0 \parallel E_0 + E(ID_i)E_1)$ 의 트랩도어 행렬이며, $ExtBasis(T_0, A_0 \parallel E_0 + E(ID_i)E_1)$ 알고리즘을 사용하여 생성한다.

[0042] 서명 생성부(230)는 $Sign(sk_i, R, m)$ 알고리즘을 이용하여 상기 생성된 서명자의 비밀키 sk_i 와, 서명자가 임의로 구성한 참여자 ID 집합 R 에 대해 주어진 메시지 m 의 서명을 생성한다.

[0043] 구체적으로, 링 서명을 생성하고자 하는 서명자(여기서는 i 번째 참여자로 가정한다)는 먼저 난수 $r \in \{0, 1\}^n$ 을 생성하고, $\mu = \mu_1 \parallel \dots \parallel \mu_h = H(m, r)$ 을 계산한다. 여기서 μ 은 h 비트

문자열이다. 그리고 $C = \sum_{i=0}^h (-1)^{\mu_i} C_i$ 을 계산하며, 여기서 $\mu_0 = 0$ 이다. 그 다음으로 $A_{R,\mu} = [A_0 \parallel E_0 + E(ID_1)E_1 \parallel E_0 + E(ID_2)E_1 \parallel \cdots \parallel C]$ 을 계산하고, $SampleD(ExtBasis(T_i, A_{R,\mu}), u, s)$ 알고리즘들을 수행하여 v 를 가우시안 샘플링한다. 여기서 $R = \{ID_1, ID_2, \dots\}$ 이다. 그리고 링 서명으로 (v, r) 을 출력한다. 여기서 v 는 래티스 $\Lambda^\perp(A_{R,\mu})$ 에 대응되는 코셋 $\Lambda_u^\perp(A_{R,\mu})$ 의 원소이다.

[0044] 서명 검증부(240)는 $Vrfy(R, m, (v, r))$ 알고리즘을 이용하여 상기 생성된 서명이 상기 참여자 ID 집합 및 메시지에 대한 정당한 서명인지를 검증하여 참 또는 거짓에 대한 결과를 출력한다.

[0045] 구체적으로, 검증자는 $\|v\| < s \cdot \sqrt{(|R| + 2)m}$ 과 $A_{R,\mu}v = u \pmod{q}$ 를 만족하는지를 확인하고, 둘 다 만족하면 1(검증 성공)을 출력하고, 그렇지 않으면 0(검증 실패)을 출력한다.

[0046] 제안하는 강한 위조 불가능성을 만족하는 ID 기반 링 서명 기법 $\{KeyGen, Extract, Sign, Vrfy\}$ 의 정확성은 다음과 같다:

[0047] 링 R 에 포함된 ID_i 중에서 서명키를 아는 사람만이 $ExtBasis$ 알고리즘을 통해 행렬 $A_{R,\mu}$ 의 트랩도어 행렬을 생성할 수 있고, 이것을 생성할 수 있는 사람만이 검증과정을 통과할 수 있는 서명을 생성할 수 있다.

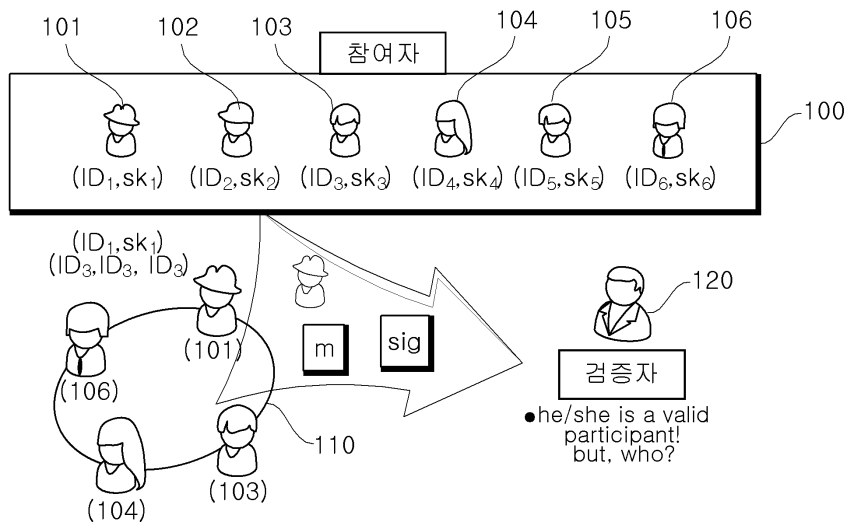
[0048] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위 내에서 다양한 수정, 변경 및 치환이 가능할 것이다. 따라서, 본 발명에 개시된 실시예 및 첨부된 도면들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예 및 첨부된 도면에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다. 또한, 특허청구범위에서 명시적인 인용 관계가 있지 않은 청구항들을 결합하여 실시예를 구성하거나 출원 후의 보정에 의해 새로운 청구항으로 포함시킬 수 있다.

부호의 설명

[0049] 210 : 파라미터 생성부
220 : 비밀키 생성부
230 : 서명 생성부
240 : 서명 검증부

도면

도면1



도면2

