(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0071884
(43) 공개일자 2012년07월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/14* (2006.01)
(21) 출원번호 10-2010-0133610
(22) 출원일자 2010년12월23일
심사청구일자 없음
기술이전 희망 : **기술양도**, **실시권허여**, **기술지도**

전체 청구항 수 : 총 11 항

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
고려대학교 산학협력단
서울 성북구 안암동5가 1

(72) 발명자
홍도원
대전광역시 유성구 엑스포로 448, 212동 1704호 (전민동, 엑스포아파트)
정익래
서울특별시 성동구 성수동1가 709번지 성수2차 대우아파트 101동 1704호
노건태
서울특별시 강남구 개포로 516, 주공아파트 707동 1304호 (개포동)

(74) 대리인
김원준, **제일특허법인**

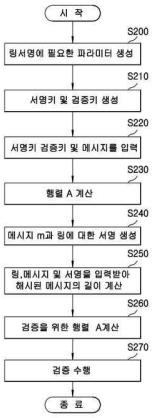
(54) 발명의 명칭 **래티스 기반의 링 서명 방법**

(57) 요 약

본 발명은 종래의 링 서명 기법이 가지는 안전성보다 강한 위조 불가능성 안전성을 만족하는 래티스 기반의 링 서명 방법에 관한 것이다.

이를 위하여 본 발명의 실시 예에 따른 래티스 기반의 링 서명 방법은 링 서명에 필요한 파라미터인 차원, 바운드, 해시된 메시지의 길이, 가우시안 파라미터 및 공개 파라미터를 생성하는 단계와, 링 서명에 필요한 파라미터를 이용하여 링을 구성한 사용자에 대한 서명키와 검증키를 생성하는 단계와, 서명키와 검증키를 이용하여 메시지와 링에 대한 서명을 생성하는 단계를 포함할 수 있다.

대 표 도 - 도2



특허청구의 범위

청구항 1

링 서명에 필요한 파라미터인 차원, 바운드, 해시된 메시지의 길이, 가우시안 파라미터 및 공개 파라미터를 생성하는 단계와,

상기 링 서명에 필요한 파라미터를 이용하여 링을 구성한 사용자에 대한 서명키와 검증키를 생성하는 단계와,

상기 서명키와 검증키를 이용하여 메시지와 상기 링에 대한 서명을 생성하는 단계를 포함하는

래티스 기반의 링 서명 방법.

청구항 2

제 1 항에 있어서,

상기 공개 파라미터를 생성하는 단계는,

상기 차원, 바운드 및 해시된 메시지 길이를 이용하여 링 서명의 차원을 생성하며,

상기 링 서명의 차원을 이용하여 가우시안 분포를 생성하고, 균등하게 랜덤하고 서로 독립적인 해시된 메시지 길이의 행렬을 이용하여 공개 파라미터를 생성하는 단계를 포함하는

래티스 기반의 링 서명 방법.

청구항 3

제 2 항에 있어서,

상기 링 서명의 차원은 충돌성-저항이 없는 해시 함수를 이용하여 생성하는 것을 특징으로 하는

래티스 기반의 링 서명 방법.

청구항 4

제 1 항에 있어서,

상기 링 서명에 필요한 파라미터는, Global Setup 알고리즘을 이용하여 생성하는 것을 특징으로 하는

래티스 기반의 링 서명 방법.

청구항 5

제 1 항에 있어서,

상기 검증키와 서명키를 생성하는 단계는,

상기 링을 구성하는 사용자i에 대해 GenBasis 알고리즘을 두 번씩 수행하여 상기 사용자i의 서명키와 검증키를 생성하는 것을 특징으로 하는

래티스 기반의 링 서명 방법.

청구항 6

제 5 항에 있어서,

상기 서명을 생성하는 단계는,

상기 서명키와 상기 링을 구성한 사용자들의 검증키 집합 및 메시지를 입력으로 하는 Sign 알고리즘을 이용하여 행렬 A를 계산하는 단계와,

상기 행렬 A를 사용하여 상기 메시지와 링에 대한 서명을 생성하는 단계를 포함하는 것을 특징으로 하는

래티스 기반의 링 서명 방법.

청구항 7

제 6 항에 있어서,

상기 행렬 A를 계산하는 단계는, 상기 링을 구성하는 사용자 수와 상기 해시된 메시지의 길이의 차이에 의거하여 상기 행렬 A를 계산하는 것을 특징으로 하는

래티스 기반의 링 서명 방법.

청구항 8

제 7 항에 있어서,

상기 해시된 메시지의 길이가 상기 링을 구성하는 사용자 수보다 큰 경우 "$A = A_1^{(\mu_1)} \| \cdots \| A_{|r|}^{(\mu_{|r|})} \| B_1^{(\mu_{|r+1|})} \| \cdots \| B_{|\mu|-|r|}^{(\mu_{|\mu|-|r|})} \in Z_q^{n \times m}$] "이고, 상기 해시된 메시지의 길이가 상기 링을 구성하는 사용자 수보다 작은 경우 "$A = A_1^{(\mu_1)} \| \cdots \| A_{|r|}^{(\mu_{|r| \bmod |\mu|+1})} \in Z_q^{n \times m}$ "이며, 상기 해시된 메시지의 길이와 상기 링을 구성하는 사용자 수가 같은 경우 "$A = A_1^{(\mu_1)} \| \cdots \| A_{|\mu|}^{(\mu_{|\mu|})} \in Z_q^{n \times m}$ "인 것을 특징으로 하는

래티스 기반의 링 서명 방법.

청구항 9

제 6 항에 있어서,

상기 메시지와 링에 대한 서명을 계산하는 단계는,

상기 행렬 A를 ExtBasis 알고리즘과 SampleD 알고리즘에 적용한 결과값과 기반으로 상기 메시지와 링에 대한 서명을 계산하는 것을 특징으로 하는

래티스 기반의 링 서명 방법.

청구항 10

제 1 항에 있어서,

상기 링, 메시지 및 상기 계산된 서명을 입력받아 검증을 수행하는 단계를 더 포함하는 것을 특징으로 하는

래티스 기반의 링 서명 방법.

청구항 11

제 10 항에 있어서,

상기 검증을 수행하는 단계는,

상기 링, 메시지 및 상기 계산된 서명을 입력받아 해시된 메시지 길이를 계산하는 단계와,

상기 해시된 메시지 길이와 상기 서명키 및 검증키를 이용하여 검증을 위한 행렬 A를 생성하여 검증을 수행하는 단계를 포함하는 것을 특징으로 하는

래티스 기반의 링 서명 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 링 서명 방법에 관한 것으로, 더욱 상세하게는 종래의 링 서명 기법이 가지는 안전성보다 강한 위조 불가능성 안전성을 만족하는 래티스 기반의 링 서명 방법에 관한 것이다.

배 경 기 술

[0002] 링 서명은 1991년 David Chaum 등에 의해 소개된 그룹 서명의 변형된 형태이다. 그룹 서명은 어떤 그룹을 대표해서 한 명의 사용자가 서명하고, 다른 사람은 그 서명이 그룹 내의 누군가가 서명하였다는 사실만을 알며(익명성, anonymity), 문제가 생겼을 경우 그룹 매니저가 누구인지 찾아낼 수 있는 능력을 가진다(추적가능성, traceability). 따라서 그룹 서명은 서명을 추적할 수 있는 능력을 가진 그룹 매니저가 별도로 존재하며, 동적 그룹에 대해서는 그룹의 가입 및 탈퇴에 대한 처리 또한 요구된다.

[0003] 반면, 링 서명은 서명자가 다수의 참여자를 자유롭게 선택하여 링을 구성하고, 구성된 링을 대표하여 서명하는 것을 말한다. 링 서명은 그룹 서명과 유사하게 링 내의 누군가가 서명하였다는 사실을 알지만(익명성, anonymity), 그룹 서명과는 다르게 어느 누구도 서명자를 추적할 수 없다. 즉, 링의 멤버 중 누가 서명하였는지는 어느 누구도 결코 알 수 없다. 따라서 링 서명은 그룹 서명과는 다르게 그룹 매니저가 필요하지 않으며, 링의 가입이나 탈퇴에 대해서도 고려할 필요가 없는 것이 특징이라고 할 수 있다. 따라서 링 서명은 내부 고발자(whistle-blower) 시스템에서 유용하게 사용될 수 있다.

[0004] 링 서명은 2001년 Ronald L. Rivest 등에 의해 처음으로 소개되었으며, 인수분해 문제에 기반을 둔 링 서명, 겹선형 사상(bilinear map)에 기반을 둔 링 서명, 래티스에 기반을 둔 링 서명 등 다양한 문제에 기반을 두어 설계되어왔다. 이러한 링 서명은 주로 2006년 Adam Bender 등이 정립한 안전성 모델에 기반을 두어 설계되었는데, Adam Bender 등은 그 특성에 따라 익명성 모델을 basic anonymity, anonymity w.r.t. adversarially-chosen keys, anonymity against attribution attacks, anonymity against full key exposure의 네 가지로 분류하였으며, 위조 불가능성 모델은 unforgeability against fixed-ring attacks, unforgeability against chosen-subring attacks, unforgeability w.r.t. insider corruption 이렇게 세 가지로 분류하였다.

[0005] 하지만, 위조 불가능성에 대한 모델은 세 가지 모두 약한 위조 불가능성만을 만족하며, 강한 위조 불가능성에 대한 안전성 모델은 아직까지 정립되지 않았다. 그렇기 때문에 지금까지 제안된 모든 링 서명 기법은 약한 위조 불가능성만을 만족하게 설계되었으며, 강한 위조 불가능성을 만족하는 링 서명 기법은 존재하지 않는다.

[0006] 현재까지 제안된 일반적인 서명 기법들은 점차 강한 위조 불가능성을 만족하도록 설계되고 있으며, 앞으로 링 서명에서도 강한 위조 불가능성을 만족하는 안전성 모델의 정립 및 기법의 설계가 요구된다.

발명의 내용

해결하려는 과제

[0007] 상기와 같은 필요성에 의해 안출된 것으로서, 본 발명의 목적은 종래의 링 서명 기법이 가지는 안전성보다 강한 위조 불가능성 안전성을 만족하는 래티스 기반의 링 서명 방법을 제공하는데 있다.

[0008] 본 발명의 목적은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 본 발명이 속하는 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0009] 본 발명의 일 측면에 따르면, 본 발명의 실시 예에 따른 래티스 기반의 링 서명 방법은, 링 서명에 필요한 파라미터인 차원, 바운드, 해시된 메시지의 길이, 가우시안 파라미터 및 공개 파라미터를 생성하는 단계와, 상기 링 서명에 필요한 파라미터를 이용하여 링을 구성한 사용자에 대한 서명키와 검증키를 생성하는 단계와, 상기 서명키와 검증키를 이용하여 메시지와 상기 링에 대한 서명을 생성하는 단계를 포함할 수 있다.

[0010] 본 발명의 실시 예에 따른 래티스 기반의 링 서명 방법에서 상기 공개 파라미터를 생성하는 단계는, 상기 차원, 바운드 및 해시된 메시지 길이를 이용하여 링 서명의 차원을 생성하며, 상기 링 서명의 차원을 이용하여 가우시안 분포를 생성하고, 균등하게 랜덤하고 서로 독립적인 해시된 메시지 길이의 행렬을 이용하여 공개 파라미터를 생성하는 단계를 포함할 수 있다.

[0011] 본 발명의 실시 예에 따른 래티스 기반의 링 서명 방법에서 상기 링 서명의 차원은 충돌성-저항이 없는 해시 함수를 이용하여 생성하는 것을 특징으로 한다.

[0012] 본 발명의 실시 예에 따른 래티스 기반의 링 서명 방법에서 상기 링 서명에 필요한 파라미터는, *Global Setup* 알고리즘을 이용하여 생성하는 것을 특징으로 한다.

[0013] 본 발명의 실시 예에 따른 래티스 기반의 링 서명 방법에서 상기 검증키와 서명키를 생성하는 단계는, 상기 링을 구성하는 사용자i에 대해 GenBasis 알고리즘을 두 번씩 수행하여 상기 사용자i의 서명키와 검증키를 생성하는 것을 특징으로 한다.

[0014] 본 발명의 실시 예에 따른 래티스 기반의 링 서명 방법에서 상기 서명을 생성하는 단계는, 상기 서명키와 상기 링을 구성한 사용자들의 검증키 집합 및 메시지를 입력으로 하는 Sign 알고리즘을 이용하여 행렬 A를 계산하는 단계와, 상기 행렬 A를 사용하여 상기 메시지와 링에 대한 서명을 생성하는 단계를 포함하는 것을 특징으로 한다.

[0015] 본 발명의 실시 예에 따른 래티스 기반의 링 서명 방법에서 상기 행렬 A를 계산하는 단계는, 상기 링을 구성하는 사용자 수와 상기 해시된 메시지의 길이의 차이에 의거하여 상기 행렬 A를 계산하는 것을 특징으로 한다.

[0016] 본 발명의 실시 예에 따른 래티스 기반의 링 서명 방법은 상기 해시된 메시지의 길이가 상기 링을 구성하는 사용자 수보다 큰 경우 "$A = A_1^{(\mu_1)} \| \cdots \| A_{|r|}^{(\mu_{|r|})} \| B_1^{(\mu_{|r+1|})} \| \cdots \| B_{|\mu|-|r|}^{(\mu_{|\mu|})} \in Z_q^{n \times m'}$]"이고, 상기 해시된 메시지의 길이가 상기 링을 구성하는 사용자 수보다 작은 경우 "$A = A_1^{(\mu_1)} \| \cdots \| A_{|r|}^{(\mu_{|r|-1 \bmod |\mu|+1|})} \in Z_q^{n \times m'}$ "이며, 상기 해시된 메시지의 길이와 상기 링을 구성하는 사용자 수가 같은 경우 "$A = A_1^{(\mu_1)} \| \cdots \| A_{|\mu|}^{(\mu_{|\mu|})} \in Z_q^{n \times m'}$ "인 것을 특징으로 한다.

[0017] 본 발명의 실시 예에 따른 래티스 기반의 링 서명 방법에서 상기 메시지와 링에 대한 서명을 계산하는 단계는, 상기 행렬 A를 ExtBasis 알고리즘과 SampleD 알고리즘에 적용한 결과값과 기반으로 상기 메시지와 링에 대한 서명을 계산하는 것을 특징으로 한다.

[0018] 본 발명의 실시 예에 따른 래티스 기반의 링 서명 방법은 상기 링, 메시지 및 상기 계산된 서명을 입력받아 검증을 수행하는 단계를 더 포함하는 것을 특징으로 한다.

[0019] 본 발명의 실시 예에 따른 래티스 기반의 링 서명 방법에서 상기 검증을 수행하는 단계는, 상기 링, 메시지 및 상기 계산된 서명을 입력받아 해시된 메시지 길이를 계산하는 단계와, 상기 해시된 메시지 길이와 상기 서명키 및 검증키를 이용하여 검증을 위한 행렬 A를 생성하여 검증을 수행하는 단계를 포함하는 것을 특징으로 한다.

발명의 효과

[0020] 본 발명은 래티스를 사용한 링 서명 방법을 제공함으로써, 강한 위조 불가능성을 만족한 링 서명 방법을 제공할 수 있다.

[0021] 또한, 본 발명의 실시 예에 다른 강한 위조 불가능성을 만족하는 링 서명 기법을 사용하여 내부 고발자 시스

템을 구성하는 경우, 종래의 방법들에 비해 보다 안전한 구성이 가능하다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 실시 예에 따른 링 서명 방법이 적용되는 기본 구조를 도시한 도면,

도 2는 본 발명의 실시 예에 따른 래티스 기반의 링 서명 및 검증 과정을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0023] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시 예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시 예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시 예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야에서 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 구성 요소를 지칭한다.

[0024] 본 발명의 실시 예들을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명의 실시 예에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0025] 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.

[0026] 또한, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 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 단계들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

[0027] 이하, 첨부된 도면을 참조하여 본 발명의 실시 예를 상세히 설명하기로 한다.

[0028] 도 1은 본 발명의 실시 예에 따른 링 서명 방법이 적용되는 기본 구조를 도시한 도면이다.

[0029] 도 1에 도시된 바와 같이, 본 발명의 실시 예에 적용되는 링 서명은 다수의 참여자들(100) 중 임의의 참여자들을 선택한 후 선택한 참여자들을 이용하여 링(110)을 구성하고, 정당한 참여자는 구성된 링(110)을 대표하여 메시지에 대한 서명을 수행할 수 있다. 링 서명에서 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.

[0030] 본 발명의 실시 예에 따른 링 서명에 앞서, 본 발명의 실시 예에서 사용되는 변수는 아래와 같다.

[0031] 본 발명의 실시 예에서 n은 시큐리티 파라미터로 사용되며, 모든 알고리즘(공격자도 포함)에 동일한 시큐리티 파라미터 n이 내포되었다고 가정한다. 정수 $q \geq 1$로 모듈러한(modulo) 정수들의 집합은 Z_q로 나타내며, 어떤 문자열 x에 대해 $|x|$는 x의 길이를 나타내고, 어떤 집합 K에 대해 $|K|$는 K의 원소의 개수를 나타낸다.

n의 함수에 대해, n의 어떤 다항식의 역보다 더 빠르게 사라지는 경우에 $negl(n)$이라고 나타낸다. 두 개의 분포(또는 분포를 가지는 두 개의 랜덤 변수) X와 Y 사이의 통계적인 거리(statistical distance)는 셀 수 있는 정의역 D 상의 함수 관점에서 보는 경우 $\max_{A \subseteq D}|X(A)-Y(A)|$로 정의한다.

[0032] 열 벡터(column vector)는 소문자로 표시하고(예를 들면, x), 행렬(matrix)은 대문자로 표시한다(예를 들면, X). 행렬 X는 순서를 가지는 열 벡터의 집합 $\{x_i\}$이며, $X \| X'$는 집합 X와 X'의 순서를 가지는 접합(concatenation)을 나타낸다. 선형 독립 벡터들의 어떤 순서를 가지는 집합 $S=\{s_1,\cdots s_k\} \subset R^m$에 대해 Gram-Schmidt 직교화는 $\tilde{S}=\{\tilde{s_1},\cdots,\tilde{s_k}\}$로 나타낸다.

[0033] 본 발명의 실시 예에서 링 서명은 래티스를 기반으로 한다. 본 발명의 실시 예에서의 메시지 공간 M과 링 공간 R에 대한 링 서명 기법은 *Gen, Sign, Vrfy*의 세 알고리즘의 튜플로 구성된다. 여기에서 링 공간 $R=\{vk_1,\cdots,vk_t\}$은 순서를 가지는 검증키 집합을 의미한다. 링 서명(RS)에서 Gen은 서명키 sk와 검증키 vk를 출력하며, $Sign(sk,r,m)$은 서명키 sk와 링 $r \in R$, 그리고 메시지 $m \in M$가 주어지면, 서명 $\sigma \in \{0,1\}^*$를 출력한다. 또한, $Vrfy(r,m,\sigma)$은 링 r과 메시지 m, 그리고 서명 σ가 주어지면, 1 또는 0을 출력한다. 여기서 1은 정당한 서명이라는 의미이며, 0은 정당하지 않은 서명이라는 의미이다.

[0034] 이러한 링 서명이 정확성을 만족한다는 것은, 어떤 메시지 $m \in M$, 링 $r \in R$, 서명키/검증키 $(sk,vk) \leftarrow Gen$, 그리고 정당한 서명 $\sigma \leftarrow Sign(sk,r,m)$에 대해, $Vrfy(r,m,\sigma)$ 알고리즘이 극단적인 확률(overwhelming probability)을 가지고 정확한 검증을 수행하는, 즉 1을 출력하는 것을 의미한다. 이때 확률은 링 서명을 구성하는 각각의 알고리즘 내부에서 사용하는 모든 난수에 대해 계산한다.

[0035] 한편, 본 발명의 실시 예에 따른 링 서명은 래티스를 기반으로 이루어지는데, 이러한 래티스에 대한 설명은 아래와 같다.

[0036] 본 발명에서는 m차원의 풀-랭크(full-rank) 정수 래티스를 사용하며, 이것은 유한개의 인덱스(finite index)를 가지는 Z^m의 이산 가산 부분군(discrete additive subgroup)이다. 즉, 쿼션트 그룹(quotient group) Z^m/Λ이 유한하다. 하나의 래티스 $\Lambda \subseteq Z^m$은 아래의 수학식 1과 같이 m개의 선형 독립 기저(basis) 벡터 $B=\{b_1,\cdots b_m\} \subset Z^m$의 모든 정수 선형 결합의 집합과 동일하게 정의될 수 있다.

[0037] [수학식 1]

[0038] $$\Lambda = L(B) = \left\{ Bc = \sum_{i \in \{1,\cdots,m\}} c_i b_i : c \in Z^m \right\}$$

[0039] 상기의 수학식 1에서 $m \geq 2$일 경우, 동일한 래티스를 생성하는 기저들은 무수히 많다.

[0040] 모든 래티스 $\Lambda \subseteq Z^m$는 유일한 표준 기저(canonical basis) $H = HNF(\Lambda) \in Z^{m \times m}$를 가지며, 이것을 HNF(hermite normal form)라고 한다. 래티스에서 임의의 기저 B가 주어졌을 경우, HNF를 효율적으로 계산할 수 있다는 사실 때문에 HNF기저를 사용한다. 기저 B로 생성된 래티스의 HNF를 $HNF(B)$로 표시한다.

[0041] 본 발명의 실시 예에서는 정수 래티스의 특정한 형태를 사용하며, $n \geq 1$과 $q \geq 2$는 정수이며, 차원 n은 본 발명의 실시 예에서 사용되는 시큐리티 파라미터이고, 모든 다른 파라미터들은 n의 함수들로 내포되었다고 가정한다. 여기에서, m차원 하드 래티스는 패리티 검사 행렬(parity check matrix), $A \in Z_q^{n \times m}$에 아래의 수학식2에 의해 생성될 수 있다.

[0042] [수학식 2]

[0043] $$\Lambda^{\perp}(A) = \left\{ x \in Z^m : Ax = \sum_{i \in \{1,\cdots,m\}} x_i \cdot a_i = 0 \in Z_q^n \right\} \subseteq Z^m$$

[0044] 한편, 어떤 y에 대해서, 패리티 검사 행렬 $A \in Z_q^{n \times m}$에 의해 생성되는 코셋(coset)은 아래의 수학식3으로 정의될 수 있다.

[0045] [수학식 3]

[0046] $$\Lambda_y^{\perp}(A) = \{x \in Z^m : Ax = y \in Z_q^n\} = \Lambda^{\perp}(A) + \bar{x}$$

[0047] 상기의 수학식 3에서 $\bar{x} \in Z^m$는 $\Lambda_y^{\perp}$의 임의의 원소이다.

[0048] 임의의 고정된 상수 $C > 1$과 어떤 $m \geq Cn \lg q$에 대해, 균등하게 랜덤한(uniformly random) $A \in Z_q^{n \times m}$의 열벡터는 Z_q^n 상의 모두를 ($2^{-\Omega(n)} = negl(n)$ 확률을 제외하고) 생성할 수 있다. 따라서 본 발명의 실시 예에서는 균등하게 랜덤한 A를 사용한다.

[0049] 다음으로 하드 래티스의 SIS(short integer solution, 이하, SIS라고 함) 문제에 대해서 살펴보자. 이 문제는 평균적인 경우에 어려운 문제(average-case hardness problems)에 속해있으며, Miklos Ajtai는 이 문제를 최악의 경우에도 어려운 문제(worst-case hardness problems)로 커넥션(connection)하는 방법을 발견하였다.

[0050] SIS **문제**. (l_2 norm에서의) $SIS_{q,\beta}$ 문제는 어떤 $m = poly(n)$에 대해 균등하게 랜덤한 행렬 $A \in Z_q^{n \times m}$를 입력으로 받아 $\| v \|_2 \leq \beta$와 $Av = 0 \in Z_q^n$(즉, $v \in \Lambda^{\perp}(A)$)을 만족하는 영이 아닌(nonzero) 정수 벡터 $v \in Z^m$를 찾는 것이다.

[0051] 래티스에서의 가우시안 분포는 어떤 $s > 0$과 차원 $m \geq 1$에 대해, 가우시안 함수(Gaussian function) $\rho_s : R^m \rightarrow (0,1]$는 $\rho_s(x) = \exp(-\pi \| x \|^2 / s^2)$로 정의될 수 있다. 또한, 어떤 코셋 $\Lambda_y^{\perp}(A)$에 대해, 코셋 상의 (중심이 0인) 이산 가우시안 분포(discrete Gaussian distribution) $D_{\Lambda_y^{\perp}(A),s}$는 각각의 $x \in \Lambda_y^{\perp}(A)$에서 $\rho_s(x)$에 비례하는 확률을 가진다.

[0052] 본 발명의 실시 예에서 사용되는 래티스에서의 가우시안 분포와 관련되는 성질들은 아래의 수학식 4와 같다.

[0053] [수학식 4]

[0054] $$\Pr_{x \leftarrow D_{\Lambda^{\perp}(A),s}}[\| x \| > s \cdot \sqrt{m}] \leq negl(n)$$

[0055] $$\Pr_{x \leftarrow D_{\Lambda^{\perp}(A),s}}[x = 0] \leq negl(n)$$

[0056] 상기의 수학식 4에서, S는 어떤 $A \in Z_q^{n \times m}$에 대한 $\Lambda^{\perp}(A)$의 기저를 말하며, $s \geq \| \tilde{S} \| \cdot w(\sqrt{\log n})$이다.

[0057] 또한, $negl(n)$ 통계적인 거리를 가지는 $D_{\Lambda_y^{\perp}(A),s}$로부터 트랩도어 S를 가지고 샘플링을 할 수 있는 PPT 알고리즘 $SampleD(S,y,s)$이 존재하는데 반해 트랩도어 S 없이 샘플링을 할 수 있는 PPT 알고리즘은 존재하지 않는다.

[0058] 그리고 $SampleD(S,y,s)$ 알고리즘의 정의역을 가우시안 분포로부터 샘플링할 수 있는 $SampleDom$ 알고리즘도 존재한다. 즉, $SampleDom$ 알고리즘으로 샘플링된 x의 범위는 $\| x \| \leq s\sqrt{m}$이다. x의 범위에서 $s \geq \sigma_1(S) \cdot w(\sqrt{\log n})$이고, $\sigma_1(S)$는 S의 가장 큰 특이점(largest singular value)이며, $\| \tilde{S} \|$보다 절대 짧지 않지만, 대부분의 중요한 경우에 대해서 크지 않다.

[0059] 또한, 본 발명의 실시 예에서 사용되는 래티스의 짧은 기저를 만들기 위한 $GenBasis$ 알고리즘은 아래와 같다.

[0060] $GenBasis$ 알고리즘은 입력으로 $(1^n, 1^m, q)$를 받는데, 이를 $GenBasis(1^m, 1^n, q)$로 표현할 수 있다. 여기에서, n에 대한 다항식 바운드(poly(n)-bounded) $m \geq Cn \lg q$이며, 이에 따라 $GenBasis$ 알고리즘은 다음의 조건

을 만족하는 $A \in Z_q^{n \times m}$와 $S \in Z^{m \times m}$를 출력한다. A의 분포는 $negl(n)$ 통계적인 거리를 가지며, S는 $\Lambda^{\perp}(A)$의 기저이며, $\| \tilde{S} \| \leq \tilde{L} = O(\sqrt{n \log q})$이다.

[0061] $GenBasis$ 알고리즘을 사용하여 생성된 S는 본 발명의 실시 예에 따른 링 서명 기법에서 서명을 생성하기 위한 트랩도어, 즉 서명키로 사용될 수 있다.

[0062] 본 발명의 실시 예에서 사용되는 래티스의 짧은 기저를 위임하기 위해서 $ExtBasis$ 알고리즘을 사용하는데, $ExtBasis$ 알고리즘에 대한 설명은 아래와 같다.

[0063] $ExtBasis$ 알고리즘은 입력으로 $(S, A' = A \| \overline{A})$를 받는데, 이를 $ExtBasis(S, A' = A \| \overline{A})$으로 표현할 수 있다. 여기서 S는 $\Lambda^{\perp}(A)$의 기저이고, $A \in Z_q^{n \times m}$, $\overline{A} \in Z_q^{n \times \overline{m}}$이며, 이에 따라 $ExtBasis$ 알고리즘은 다음의 조건을 만족하는 $S' \in Z^{m' \times m'}$을 출력한다. 여기에서, $m' = m + \overline{m}$이고, S'은 $\Lambda^{\perp}(A')$의 기저이며, $\| \tilde{S'} \| = \| \tilde{S} \|$ 이다. 또한, $\Lambda^{\perp}(A'P)$의 기저는 PS'이다. 여기서 P는 퍼뮤테이션 행렬(permutation matrix)이다.

[0064] 래티스 기반의 링 서명은 상기에서 설명한 세가지 알고리즘, 즉 $SampleD$, $GenBasis$, $ExtBasis$ 알고리즘을 사용하여 구성함으로써, 강한 위조 불가능성을 만족하는 링 서명을 생성할 수 있다.

[0065] 도 2는 본 발명의 실시 예에 따른 래티스 기반의 링 서명 과정을 도시한 흐름도이다.

[0066] 먼저, 링 서명에 앞서, 신뢰할 수 있는 키 설정 기관(setup authority)은 아래와 같은 $Global\ Setup$ 알고리즘을 수행하여 본 발명의 실시 예에서 사용할 추가적인 파라미터들을 생성(S200)한다.

[0067] 키 설정 기관(setup authority)이 $Global\ Setup$ 알고리즘을 이용하여 생성하는 파라미터들은 아래와 같다.

[0068] 차원 $m = O(n \lg q)$, 바운드(bound) $\tilde{L} = O(\sqrt{n \lg q})$. 해시된 메시지의 길이 $|\mu|$를 정의하며, 이에 따라 링 서명의 차원이 $m' = m \cdot \max(|r|, |\mu|)$이 될 수 있다. 여기에서, $|r|$은 링 r에 포함된 참여자들의 수를 의미한다.

[0069] 또한, 본 발명의 실시 예에 따른 링 서명 기법에서는 아래의 수학식 5와 같은 충돌성-저항(collision-resistant) 해시 함수를 사용하여 해시된 메시지의 길이를 생성할 수 있다.

[0070] [수학식 5]

[0071] $$h(\cdot,\cdot): \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^{|\mu|}$$

[0072] 그리고, 가우시안 파라미터 $s = \tilde{L} \cdot w(\sqrt{\log m'})$, 공개 파라미터 $params = \{B_1^{(0)}, B_1^{(1)}, \cdots, B_{|\mu|}^{(0)}, B_{|\mu|}^{(1)}, y\}$를 생성할 수 있는데, 여기에서, $B_i^{(b)} \in Z_q^{n \times m}$는 균등하게 랜덤하고(uniformly random) 서로 독립적인(independent) $2|\mu|$개의 $n \times m$ 행렬이고, $y \in Z_q^n$는 균등하게 랜덤한 $n \times 1$ 열 벡터이다.

[0073] 각각의 사용자는 $Global\ Setup$ 알고리즘을 통해 생성한 공개 파라미터들을 사용하여 링 서명 기법 $RS = \{Gen, Sign, Vrfy\}$을 아래와 같이 구성한다.

[0074] Gen은 i번째 사용자에 대해 $GenBasis(1^m, 1^n, q)$ 알고리즘을 두 번씩 수행하여 $A_i^{(0)} \in Z_q^{n \times m}$, $A_i^{(1)} \in Z_q^{n \times m}$과 $S_i^{(0)} \in Z_q^{m \times m}$, $S_i^{(1)} \in Z_q^{m \times m}$을 얻는다. 여기서 $S_i^{(0)}$는 $\Lambda^{\perp}(A_i^{(0)})$의 짧은 기저($\| \widetilde{S_i^{(0)}} \| \leq \tilde{L}$)이고, $S_i^{(1)}$는 $\Lambda^{\perp}(A_i^{(1)})$의 짧은 기저($\| \widetilde{S_i^{(1)}} \| \leq \tilde{L}$)이다. 결과적으로 i번째 사용자의 서명키"$sk_i = \{S_i^{(0)}, S_i^{(1)}\}$"와 검증키는 "$vk_i = \{A_i^{(0)}, A_i^{(1)}\}$"를 생성(S210)할 수 있다.

[0075] 그런 다음, $Sign(sk_i, r, m)$은 $Sign$ 알고리즘의 입력으로 서명키 $sk_i = \{S_i^{(0)}, S_i^{(1)}\}$, 링 $r = \{vk_1, \cdots, vk_{|r|}\}$, 메시지 $m \in \{0,1\}^*$를 받는다(S220). 여기에서, $i \in \{1, \cdots, |r|\}$이다.

[0076] 랜덤한 값 $\gamma \in \{0,1\}^*$을 선택하고, $\mu = h(m,\gamma) = \mu_1 \| \cdots \| \mu_{|\mu|}$을 계산한다. 그리고, $|\mu|$와 $|r|$의 길이의 차이에 따라 아래의 수학식 6과 같이 세 가지 경우를 고려하여 행렬 A를 계산(S230)한다.

[0077] [수학식 6]

[0078] $|\mu| = |r|$인 경우, $A = A_1^{(\mu_1)} \| \cdots \| A_{|\mu|}^{(\mu_{|\mu|})} \in Z_q^{n \times m}$

[0079] $|\mu| > |r|$인 경우, $A = A_1^{(\mu_1)} \| \cdots \| A_{|r|}^{(\mu_{|r|})} \| B_1^{(\mu_{|r|+1})} \| \cdots \| B_{|\mu|-|r|}^{(\mu_{|\mu|})} \in Z_q^{n \times m}$]

[0080] $|\mu| < |r|$인 경우, $A = A_1^{(\mu_1)} \| \cdots \| A_{|r|}^{(\mu_{|r| \bmod |\mu|+1})} \in Z_q^{n \times m}$

[0081] 상기의 수학식 6에서, $j \in \{1,\cdots,|\mu|\}$는 임의의 값이다. 쉽게 말하면, μ의 마지막 값 $\mu_{|r|}$까지 링 r의 검증키 값들을 순차적으로 반복하여 A를 구성한다.

[0082] 위와 같이 구성된 A을 아래와 같은 수학식 7에 적용, 즉 SampleD 및 ExtBasis 알고리즘에 적용하여 v를 계산한다.

[0083] [수학식 7]

[0084] $v \leftarrow SampleD(ExtBasis(S_i^{(\mu)}, A), y, s)$

[0085] 위의 수학식 7의 결과로부터 메시지 m과 링 r에 대한 서명"$\sigma = (v,\gamma)$"을 생성(S240)할 수 있다.

[0086] 그런 다음, 생성된 서명에 대한 검증 단계를 수행할 수 있는데, 즉 $Vrfy(r,m,\sigma)$는 $Vrfy$ 알고리즘의 입력으로 링 r, 메시지 m, 서명 $\sigma = (v,\gamma)$를 입력받아 해시된 메시지의 길이"$\mu = h(m,\gamma)$"를 계산(S250)한다.

[0087] 그런 다음, 상기의 $Sign$ 알고리즘에서 행렬 A를 계산하는 방법과 동일하게 검증을 위한 행렬 A를 계산(S260)한다. 다시말해서, $|\mu|$와 $|r|$의 길이의 차이에 따라 상기와 같은 수학식 6과 같이 세 가지 경우를 고려하여 검증을 위한 행렬 A를 계산하고, 계산된 검증을 위한 행렬 A를 SampleD 및 ExtBasis 알고리즘에 적용하여 v를 계산하여 검증을 수행(S270)할 수 있다. 즉, 계산된 v가 "$\|v\| \le s\sqrt{m}$"이고 $Av = y$이면 1을 출력하고, 그렇지 않으면 0을 출력한다.

[0088] 본 발명의 실시 예에 따른 링 서명 기법 $RS = \{Gen, Sign, Vrfy\}$의 정확성은 다음과 같다.

[0089] 링 r의 검증키 중에 서명키를 아는 사람만 $ExtBasis$ 알고리즘을 통해 행렬 A의 짧은 기저를 계산할 수 있고, 짧은 기저를 아는 사람만 $SampleD$ 알고리즘을 통해 $\|v\| \le s\sqrt{m}$를 만족하는 v를 샘플링할 수 있다. 이렇게 구한 v는 가우시안 분포 $D_{\Lambda_y^\perp(A),s}$를 따르며, 즉 $y \equiv Av \bmod q$이다.

[0090] 이상 첨부된 도면을 참조하여 본 발명의 실시 예를 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 개시된 실시형태들을 조합 또는 치환하여 본 발명의 실시예에 명확하게 개시되지 않은 형태로 실시할 수 있으나, 이 역시 본 발명의 범위를 벗어나지 않는 것이다. 그러므로 이상에서 기술한 실시 예들은 모든 면에서 예시적인 것으로 한정적인 것으로 이해해서는 안 되며, 이러한 변형된 실시 예들은 본 발명의 특허청구범위에 기재된 기술사상에 포함된다고 하여야 할 것이다.

부호의 설명

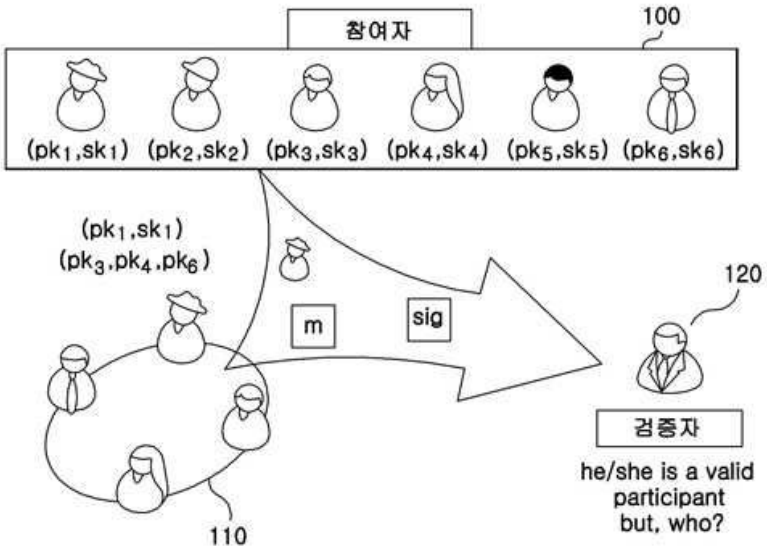
[0091] 100 : 참여자

110 : 링

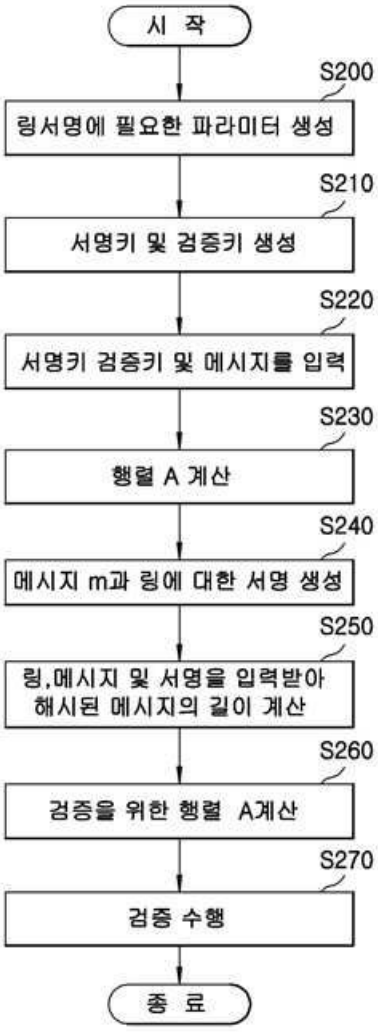
120 : 검증자

도면

도면1


참여자
100
(pk1,sk1) (pk2,sk2) (pk3,sk3) (pk4,sk4) (pk5,sk5) (pk6,sk6)
(pk1,sk1)
(pk3,pk4,pk6)
m
sig
120
검증자
he/she is a valid participant but, who?
110

도면2


시 작
S200
링서명에 필요한 파라미터 생성
S210
서명키 및 검증키 생성
S220
서명키 검증키 및 메시지를 입력
S230
행렬 A 계산
S240
메시지 m과 링에 대한 서명 생성
S250
링,메시지 및 서명을 입력받아 해시된 메시지의 길이 계산
S260
검증을 위한 행렬 A계산
S270
검증 수행
종 료