(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년02월15일
(11) 등록번호 10-1593673
(24) 등록일자 2016년02월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01)
(21) 출원번호 10-2014-0114173
(22) 출원일자 2014년08월29일
심사청구일자 2014년08월29일
(56) 선행기술조사문헌
Kee Sung Kim 외 1인, Springer-Verlag Berlin Heidelberg 2014, "Efficient verifiably encrypted signatures from lattices" (2014.01.11. 공개)

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
정익래
서울특별시 광진구 긴고랑로4길 53, 203호(중곡1동, 호동아파트)
김기성
서울특별시 성북구 안암로 145, 로봇융합관 404호 (안암동5가)
(74) 대리인
심경식, 홍성욱

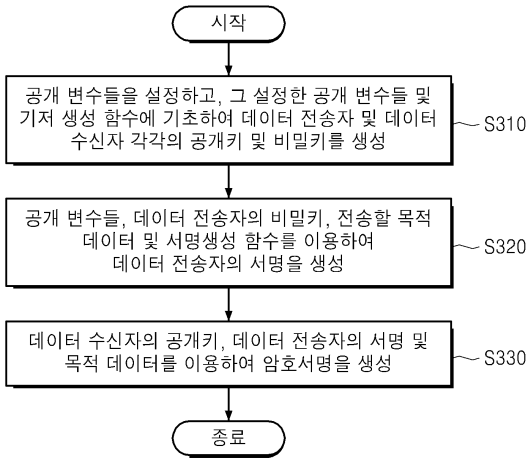
전체 청구항 수 : 총 13 항 심사관 : 문형섭

(54) 발명의 명칭 **래티스 기반의 암호서명 생성 방법 및 장치, 래티스 기반의 암호서명 복원 방법 및 장치**

(57) 요 약

래티스 기반의 암호서명 생성 방법이 개시된다. 본 발명의 일 실시예에 따른 래티스 기반의 암호서명 생성 방법은 공개 변수들을 설정하고, 상기 설정한 공개 변수들 및 기저 생성 함수에 기초하여 데이터 전송자 및 데이터 수신자 각각의 공개키 및 비밀키를 생성하는 단계; 상기 공개 변수들, 상기 데이터 전송자의 비밀키, 전송할 목적 데이터 및 서명생성 함수를 이용하여 상기 데이터 전송자의 서명을 생성하는 단계; 및 상기 데이터 수신자의 공개키, 상기 데이터 전송자의 서명 및 상기 목적 데이터를 이용하여 상기 전송할 데이터에 대한 암호문으로서 상기 데이터 전송자에 대한 서명값을 포함하는 암호서명을 생성하는 단계를 포함한다.

대 표 도 - 도3



이 발명을 지원한 국가연구개발사업
과제고유번호 R1309081
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 (이공)중견연구자지원_핵심연구
연구과제명 [1차년도]실용적인 래티스 기반 익명성 보장 및 연산 가능한 서명 기술 연구
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2013.12.01 ~ 2014.11.30

특허청구의 범위

청구항 1

공개 변수들을 설정하고, 상기 설정한 공개 변수들 및 기저 생성 함수에 기초하여 데이터 전송자 및 데이터 수신자 각각의 공개키 및 비밀키를 생성하는 단계;

상기 공개 변수들, 상기 데이터 전송자의 비밀키, 전송할 목적 데이터 및 서명생성 함수를 이용하여 상기 데이터 전송자의 서명을 생성하는 단계; 및

상기 데이터 수신자의 공개키, 상기 데이터 전송자의 서명 및 상기 목적 데이터를 이용하여 상기 전송할 데이터에 대한 암호문으로서 상기 데이터 전송자에 대한 서명값을 포함하는 암호서명을 생성하는 단계를 포함하고,

상기 암호서명은 수학식 3에 의거하여 생성되는 것을 특징으로 하는 래티스 기반의 암호서명 생성 방법.

[수학식 3]

$$c=(B^{T}s+2\sigma+M) \bmod q$$

이때, c는 암호서명을 나타내고, B^{T}는 상기 데이터 수신자의 공개키 B를 트랜스포즈한 값, s는 0에서 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터, σ는 데이터 전송자의 서명, modq는 괄호안의 값을 q로 나눈 나머지 값을 나타냄.

청구항 2

제1항에 있어서,

상기 데이터 전송자 및 데이터 수신자 각각의 공개키 및 비밀키가 행렬일 때,

상기 데이터 전송자의 공개키 행렬 A와 상기 데이터 전송자의 비밀키 행렬 S_A를 곱하여 생성된 제1 곱셈 행렬 및 상기 데이터 수신자의 공개키 행렬 B와 상기 데이터 수신자의 비밀키 행렬 S_B를 곱하여 생성된 제2 곱셈 행렬의 구성요소들 각각의 값은 0인 것을 특징으로 하는 래티스 기반의 암호서명 생성 방법.

청구항 3

제2항에 있어서,

상기 공개 변수들은 상호간에 관련성을 가지는 제1 변수 n, 제2 변수 m, 제3 변수 δ 및 제4 변수 q를 포함하고,

상기 데이터 전송자의 공개키 행렬 A와 상기 데이터 수신자의 공개키 행렬 B는 n * m의 크기를 가지고 0에서 q사이의 랜덤 값들을 구성요소로 가지고,

상기 데이터 전송자의 비밀키 행렬 S_A와 상기 데이터 수신자의 비밀키 행렬 S_B는 m * m의 크기를 가지고 0에서 q사이의 랜덤 값들을 구성요소로 가지는 것을 특징으로 하는 래티스 기반의 암호서명 생성 방법.

청구항 4

제3항에 있어서,

상기 데이터 전송자의 서명을 생성하는 단계는

0 내지 2사이의 값들을 구성요소로 하는 m차원의 벡터와 0 내지 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터를 입력으로 0 내지 q사이의 랜덤 해쉬 값들을 구성요소로 하는 n차원의 벡터를 출력하는 안전 해쉬 함수를 설정하는 단계;

0에서 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터 s를 생성하는 단계; 및

상기 안전 해쉬함수에 상기 목적 데이터에 대응되는 m차원의 벡터 및 상기 벡터 s를 입력하여 출력된 n차원의

해쉬 출력 벡터, 상기 데이터 전송자의 비밀키 S_A, 상기 제3 변수 δ 및 상기 서명생성 함수를 이용하여 m차원의 벡터 형태를 가진 상기 데이터 전송자의 서명 σ를 생성하는 단계를 포함하는 것을 특징으로 하는 래티스 기반의 암호서명 생성 방법.

청구항 5

삭제

청구항 6

데이터 수신자의 공개키, 데이터 전송자의 서명 및 전송하고자 하는 목적 데이터를 이용하여 생성된 상기 목적 데이터에 대한 암호문으로서 상기 데이터 전송자에 대한 서명값을 포함하는 암호서명을 수신하는 단계;

상기 데이터 수신자의 비밀키를 이용하여 상기 데이터 전송자의 서명과 상기 목적 데이터만이 결합된 형태를 가진 중간 연산값을 산출하는 단계;

상기 산출된 중간 연산값에 mod함수를 적용하여 상기 중간 연산값으로부터 상기 목적 데이터를 추출하는 단계; 및

상기 추출된 목적 데이터를 이용하여 상기 중간 연산값으로부터 상기 데이터 전송자의 서명을 추출하는 단계를 포함하고,

상기 데이터 수신자의 공개키 및 비밀키는 행렬 형태를 가지고, 상기 데이터 수신자의 공개키에 대응되는 행렬과 상기 데이터 수신자의 비밀키에 대응되는 행렬을 곱하여 생성된 행렬의 구성요소들 각각의 값은 0이 되고,

상기 수신된 암호서명은 수학식 3에 따른 형태를 가지는 것을 특징으로 하는 래티스 기반의 암호서명 복원 방법.

[수학식 3]

$$c=(B^{T}s+2\sigma+M) \bmod q$$

이때, c는 암호서명을 나타내고, B^{T}는 상기 데이터 수신자의 공개키 B를 트랜스포즈한 값, s는 0에서 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터, σ는 데이터 전송자의 서명, modq는 괄호안의 값을 q로 나눈 나머지 값을 나타냄.

청구항 7

제6항에 있어서,

상기 중간 연산값을 산출하는 단계는

수학식 4 및 수학식 5에 의거하여 상기 중간 연산값을 2σ+M으로서 산출하는 것을 특징으로 하는 래티스 기반의 암호서명 복원 방법.

[수학식 4]

$$(S_B)^{T}c=(BS_B)^{T}s+(S_B)^{T}(2\sigma+M) \bmod q=(S_B)^{T}(2\sigma+M) \bmod q=(S_B)^{T}(2\sigma+M)$$

[수학식 5]

$$(S_B)^{-T}(S_B)^{T}(2\sigma+M)=2\sigma+M$$

이때, $(S_B)^{T}$ 는 데이터 수신자의 비밀키에 대응되는 행렬 S_B를 트랜스포즈한 행렬이고, $(S_B)^{-T}$ 는 $(S_B)^{T}$ 행렬의 역행렬임.

청구항 8

제7항에 있어서,

상기 목적 데이터를 추출하는 단계는

수학식 6에 의거하여 수행되는 것을 특징으로 하는 래티스 기반의 암호서명 복원 방법.

[수학식 6]

$$(2\sigma+M) \bmod 2 = M$$

청구항 9

제7항에 있어서,

상기 데이터 전송자의 서명을 추출하는 단계는

수학식 7에 의거하여 수행되는 것을 특징으로 하는 래티스 기반의 암호서명 복원 방법.

[수학식 7]

$$(2\sigma+M-M)/2 = \sigma$$

청구항 10

제7항에 있어서,

상기 목적 데이터의 무결성을 검증하는 단계를 더 포함하고,

상기 무결성을 검증하는 단계는 수학식 8에서 랜덤 값들을 구성요소로 하는 n차원의 벡터 s를 산출한 후, 수학식 9를 만족하는지 여부에 기초하여 수행되는 것을 특징으로 하는 래티스 기반의 암호서명 복원 방법.

[수학식 8]

$$c-(2\sigma+M) = B^{T}s \bmod q$$

[수학식 9]

$$\sigma \neq 0,\ \|\sigma\| \leq \delta\sqrt{m},\ A\sigma = H(M,s)$$

이때, δ 는 제1 변수 n, 제2 변수 m, 제3 변수 δ 및 제4 변수 q를 포함하는 공개 변수들 중 제3 변수이고, H는 0 내지 2사이의 값들을 구성요소로 하는 m차원의 벡터와 0 내지 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터를 입력으로 0 내지 q사이의 랜덤 해쉬 값들을 구성요소로 하는 n차원의 벡터를 출력하는 안전 해쉬 함수를 나타냄.

청구항 11

공개 변수들을 설정하고, 상기 설정한 공개 변수들 및 기저 생성 함수에 기초하여 데이터 전송자 및 데이터 수신자 각각의 공개키 및 비밀키를 생성하는 키 생성부;

상기 공개 변수들, 상기 데이터 전송자의 비밀키, 전송할 목적 데이터 및 서명생성 함수를 이용하여 상기 데이터 전송자의 서명을 생성하는 서명 생성부; 및

상기 데이터 수신자의 공개키, 상기 데이터 전송자의 서명 및 상기 목적 데이터를 이용하여 상기 전송할 데이터에 대한 암호문으로서 상기 데이터 전송자에 대한 서명값을 포함하는 암호서명을 생성하는 암호서명 생성부를 포함하고,

상기 암호서명은

수학식 3에 의거하여 생성되는 것을 특징으로 하는 래티스 기반의 암호서명 생성 장치.

[수학식 3]

$$c=(B^{T}s+2\sigma+M) \bmod q$$

이때, c는 암호서명을 나타내고, B^{T}는 상기 데이터 수신자의 공개키 B를 트랜스포즈한 값, s는 0에서 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터, σ는 데이터 전송자의 서명, modq는 괄호안의 값을 q로 나눈 나머지 값을 나타냄.

청구항 12

제11항에 있어서,

상기 서명 생성부는

0 내지 2사이의 값들을 구성요소로 하는 m차원의 벡터와 0 내지 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터를 입력으로 0 내지 q사이의 랜덤 해쉬 값들을 구성요소로 하는 n차원의 벡터를 출력하는 안전 해쉬 함수를 설정하는 해쉬 함수 생성부;

0에서 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터 s를 생성하는 벡터 생성부; 및

상기 안전 해쉬함수에 상기 목적 데이터에 대응되는 m차원의 벡터 및 상기 벡터 s를 입력하여 출력된 n차원의 해쉬 출력 벡터, 상기 데이터 전송자의 비밀키 S_A, 제3 변수 δ 및 상기 서명생성 함수를 이용하여 m차원의 벡터 형태를 가진 상기 데이터 전송자의 서명 σ를 생성하는 서명 처리부를 포함하는 것을 특징으로 하는 래티스 기반의 암호서명 생성 장치.

청구항 13

데이터 수신자의 공개키, 데이터 전송자의 서명 및 전송하고자 하는 목적 데이터를 이용하여 생성된 상기 목적 데이터에 대한 암호문으로서 상기 데이터 전송자에 대한 서명값을 포함하는 암호서명을 수신하는 수신부;

상기 암호서명에 기초하여 상기 데이터 수신자의 비밀키를 이용하여 상기 데이터 전송자의 서명과 상기 목적 데이터만이 결합된 형태를 가진 중간 연산값을 산출하는 중간 연산 산출부;

상기 산출된 중간 연산값에 mod함수를 적용하여 상기 중간 연산값으로부터 상기 목적 데이터를 추출하는 데이터 추출부; 및

상기 추출된 목적 데이터를 이용하여 상기 중간 연산값으로부터 상기 데이터 전송자의 서명을 추출하는 서명 추출부를 포함하고,

상기 데이터 수신자의 공개키 및 비밀키는 행렬 형태를 가지고, 상기 데이터 수신자의 공개키에 대응되는 행렬과 상기 데이터 수신자의 비밀키에 대응되는 행렬을 곱하여 생성된 행렬의 구성요소들 각각의 값은 0이 되고,

상기 암호서명은 수학식 3에 따른 형태를 가지는 것을 특징으로 하는 래티스 기반의 암호서명 복원 장치.

[수학식 3]

$$c=(B^{T}s+2\sigma+M) \bmod q$$

이때, c는 암호서명을 나타내고, B^{T}는 상기 데이터 수신자의 공개키 B를 트랜스포즈한 값, s는 0에서 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터, σ는 데이터 전송자의 서명, modq는 괄호안의 값을 q로 나눈 나머지 값을 나타냄.

청구항 14

제13항에 있어서,

상기 목적 데이터의 무결성을 검증하는 무결성 검증부를 더 포함하고,

상기 무결성을 검증부는 수학식 8에서 랜덤 값들을 구성요소로 하는 n차원의 벡터 s를 산출한 후, 수학식 9를

만족하는지 여부에 기초하여 무결성을 검증하는 것을 특징으로 하는 래티스 기반의 암호서명 복원 장치.

[수학식 8]

$$c-(2\sigma+M)=B^{T}s \bmod q$$

[수학식 9]

$$\sigma \neq 0,\ \|\sigma\| \leq \delta\sqrt{m},\ A\sigma = H(M,s)$$

이때, δ 는 제1 변수 n, 제2 변수 m, 제3 변수 δ 및 제4 변수 q를 포함하는 공개 변수들 중 제3 변수이고, H는 0 내지 2사이의 값들을 구성요소로 하는 m차원의 벡터와 0 내지 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터를 입력으로 0 내지 q사이의 랜덤 해쉬 값들을 구성요소로 하는 n차원의 벡터를 출력하는 안전 해쉬 함수를 나타냄.

명 세 서

기 술 분 야

[0001] 본 발명은 래티스 기반의 암호서명에 관한 것으로, 특히 래티스 기반의 암호서명 생성 방법 및 장치, 래티스 기반의 암호서명 복원 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 암호 기술은 데이터에 대한 기밀성을 보장하기 위해 사용되며 암호 분야에서 가장 널리 사용되는 기술 중 하나이다. 이러한 암호 기술은 보통 대칭키 암호 기술과 공개키 암호 기술로 분류되며, 본 특허에서는 공개키 암호 기술에 관해 다룬다. 공개키 암호 기술은 데이터를 암호화하기 위해 필요한 암호화키와 암호문을 복호화하기 위해 필요한 복호화키로 구성되며 암호화키는 누구나 접근할 수 있게 공개하고, 복호화키는 사용자가 개인적으로 보관한다. 누구든 해당 암호화키로 데이터를 암호화할 수 있으며, 해당 암호문을 복호화하여 원본 데이터를 볼 수 있는 것은 복호화키를 가지고 있는 사용자만이 해당된다.

[0003] 전자서명 기술은 데이터에 대한 인증 및 무결성 보장 등에 사용되며 암호 분야에서 암호 기술과 함께 가장 널리 사용되는 기술 중 하나이다. 이러한 전자서명 기술에서 서명자는 주어진 데이터에 대해 자신의 서명키를 사용해 서명을 생성하며, 확인자는 서명키와 쌍을 이루는 확인키를 사용하여 해당 서명의 정당성을 판단한다.

[0004] 만일, 데이터에 대해 무결성과 기밀성을 동시에 보장하기 위해서는 위의 두 기술을 동일한 데이터에 사용하면 된다. 하지만 그러한 경우 암호문과 서명을 동시에 생성, 저장 및 관리해야하는 단점이 생긴다. 이러한 문제점을 해결하기 위해 개발된 기술이 암호서명기술이다. 하나의 암호문만으로 해당 데이터에 대한 기밀성과 무결성을 동시에 제공하는 기술이다. 암호서명 기술은 일반적으로 데이터와 그에 대한 서명을 암호문에 포함시키는 기술로 이를 본 제 3자는 데이터 및 서명에 대한 어떠한 정보도 얻어볼 수 없다. 생성된 암호서명은 오직 그에 대응하는 비밀키를 가진 사용자만이 그 안에 들어있는 서명과 데이터 쌍을 복구할 수 있으며 해당 서명이 정당한지를 판단하는 과정을 거침으로써 데이터에 대한 기밀성과 무결성을 동시에 보장하게 된다.

[0005] 현재까지 제안된 대부분의 암호서명 기술의 경우 인수 분해, 이산 대수, 페어링(pairing)을 기반으로 설계되었다. 하지만 풀기 어렵다고 여겨지던 이러한 문제들은 최근 양자 알고리즘의 발전으로 더 이상 안전성의 신뢰성을 보장할 수 없으며, 실제 양자 알고리즘을 이용해 인수분해 문제를 해결하는 논문이 제안되었다. 이러한 환경에서 래티스에 대한 관심이 점차 높아지고 있다. 기존의 래티스 기반의 암호 시스템의 경우 안전성 증명이 결여되어 많은 문제점이 있었으나, 최근 worst-case 문제에 기반하여 증명되는 래티스 기반의 암호 시스템들이 등장하고 있다. 기존의 암호 시스템이 average-case 문제에 기반하여 설계된 점을 비추어 볼 때 매우 높은 안전성을 제공한다는 것을 알 수 있다. 이 뿐만 아니라 래티스 암호 시스템은 기존의 기법에 비해 매우 효율적이다. 인수 분해, 이산 대수, pairing등의 연산 복잡도는 이지만, 래티스에서의 연산 복잡도는 으로 훨씬 효율적이다. 또한, 래티스 암호 시스템은 양자 알고리즘에 안전하다. 이러한 다양한 이유 때문에 최근 래티스 환경에서 다양한 암호 시스템이 설계되고 있으며, 이러한 작업은 매우 의미 있는 일로 여겨지고 있다. 따라서 래티스 환경에서의 효율적이고 안전한 암호서명 기술의 개발 필요성이 대두되고 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 일 실시예의 목적은 래티스 기반 암호 시스템이 갖는 연산 효율성, 높은 안전성, 양자 컴퓨터 분석에 대한 내성의 장점을 가지면서 데이터에 대해 무결성과 기밀성을 동시에 보장하는 래티스 기반의 암호서명 생성 방법 및 장치, 래티스 기반의 암호서명 복원 방법 및 장치를 제공하는 것이다.

과제의 해결 수단

[0007] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 래티스 기반의 암호서명 생성 방법은 공개 변수들을 설정하고, 상기 설정한 공개 변수들 및 기저 생성 함수에 기초하여 데이터 전송자 및 데이터 수신자 각각의 공개키 및 비밀키를 생성하는 단계; 상기 공개 변수들, 상기 데이터 전송자의 비밀키, 전송할 목적 데이터 및 서명 생성 함수를 이용하여 상기 데이터 전송자의 서명을 생성하는 단계; 및 상기 데이터 수신자의 공개키, 상기 데이터 전송자의 서명 및 상기 목적 데이터를 이용하여 상기 전송할 데이터에 대한 암호문으로서 상기 데이터 전송자에 대한 서명값을 포함하는 암호서명을 생성하는 단계를 포함한다.

[0008] 바람직하게는, 상기 데이터 전송자 및 데이터 수신자 각각의 공개키 및 비밀키가 행렬일 때, 상기 데이터 전송자의 공개키 행렬 A와 상기 데이터 전송자의 비밀키 행렬 S_A를 곱하여 생성된 제1 곱셈 행렬 및 상기 데이터 수신자의 공개키 행렬 B와 상기 데이터 수신자의 비밀키 행렬 S_B를 곱하여 생성된 제2 곱셈 행렬의 구성요소들 각각의 값은 0일 수 있다.

[0009] 바람직하게는, 상기 공개 변수들은 상호간에 관련성을 가지는 제1 변수 n, 제2 변수 m, 제3 변수 δ 및 제4 변수 q를 포함하고, 상기 데이터 전송자의 공개키 행렬 A와 상기 데이터 수신자의 공개키 행렬 B는 n * m의 크기를 가지고 0에서 q사이의 랜덤 값들을 구성요소로 가지고, 상기 데이터 전송자의 비밀키 행렬 S_A와 상기 데이터 수신자의 비밀키 행렬 S_B는 m * m의 크기를 가지고 0에서 q사이의 랜덤 값들을 구성요소로 가질 수 있다.

[0010] 바람직하게는, 상기 데이터 전송자의 서명을 생성하는 단계는 0 내지 2사이의 값들을 구성요소로 하는 m차원의 벡터와 0 내지 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터를 입력으로 0 내지 q사이의 랜덤 해쉬 값들을 구성요소로 하는 n차원의 벡터를 출력하는 안전 해쉬 함수를 설정하는 단계; 0에서 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터 s를 생성하는 단계; 및 상기 안전 해쉬함수에 상기 목적 데이터에 대응되는 m차원의 벡터 및 상기 벡터 s를 입력하여 출력된 n차원의 해쉬 출력 벡터, 상기 데이터 전송자의 비밀키 S_A, 상기 제3 변수 δ 및 상기 서명생성 함수를 이용하여 m차원의 벡터 형태를 가진 상기 데이터 전송자의 서명 σ를 생성하는 단계를 포함할 수 있다.

[0011] 바람직하게는, 상기 암호서명은 수학식 3에 의거하여 생성될 수 있다.

[0012] [수학식 3]

[0013] $$c=(B^{T}s+2\sigma+M) \bmod q$$

[0014] 이때, c는 암호서명을 나타내고, B^{T}는 상기 데이터 수신자의 공개키 B를 트랜스포즈한 값, s는 0에서 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터, σ는 데이터 전송자의 서명, modq는 괄호안의 값을 q로 나눈 나머지 값을 나타낸다.

[0015] 또한, 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 래티스 기반의 암호서명 복원 방법은 데이터 수신자의 공개키, 데이터 전송자의 서명 및 전송하고자 하는 목적 데이터를 이용하여 생성된 상기 목적 데이터에 대한 암호문으로서 상기 데이터 전송자에 대한 서명값을 포함하는 암호서명을 수신하는 단계; 상기 데이터 수신자의 비밀키를 이용하여 상기 데이터 전송자의 서명과 상기 목적 데이터만이 결합된 형태를 가진 중간 연산값을 산출하는 단계; 상기 산출된 중간 연산값에 mod함수를 적용하여 상기 중간 연산값으로부터 상기 목적 데이터를 추출하는 단계; 및 상기 추출된 목적 데이터를 이용하여 상기 중간 연산값으로부터 상기 데이터 전송자의 서명을 추출하는 단계를 포함하고, 상기 데이터 수신자의 공개키 및 비밀키는 행렬 형태를 가지고, 상기 데이터 수신자의 공개키에 대응되는 행렬과 상기 데이터 수신자의 비밀키에 대응되는 행렬을 곱하여 생성된 행렬의 구성요소들 각각의 값은 0이 된다.

[0016] 바람직하게는, c는 암호서명을 나타내고, B^T는 상기 데이터 수신자의 공개키 B를 트랜스포즈한 값, s는 0에서 q 사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터, σ는 데이터 전송자의 서명, modq는 괄호안의 값을 q로 나눈 나머지 값을 나타낼 때, 상기 암호서명은 수학식 3에 따른 형태를 가지고,

[0017] [수학식 3]

[0018] $$c=(B^{T}s+2\sigma+M)\bmod q$$

[0019] 상기 중간 연산값을 산출하는 단계는

[0020] 수학식 4 및 수학식 5에 의거하여 상기 중간 연산값을 2σ+M으로서 산출할 수 있다.

[0021] [수학식 4]

[0022] $$(S_B)^{T}c=(BS_B)^{T}s+(S_B)^{T}(2\sigma+M)\bmod q=(S_B)^{T}(2\sigma+M)\bmod q=(S_B)^{T}(2\sigma+M)$$

[0023] [수학식 5]

[0024] $$(S_B)^{-T}(S_B)^{T}(2\sigma+M)=2\sigma+M$$

[0025] 이때, $(S_B)^T$ 는 데이터 수신자의 비밀키에 대응되는 행렬 S_B를 트랜스포즈한 행렬이고, $(S_B)^{-T}$ 는 $(S_B)^T$ 행렬의 역행렬이다.

[0026] 바람직하게는, 상기 목적 데이터를 추출하는 단계는 수학식 6에 의거하여 수행될 수 있다.

[0027] [수학식 6]

[0028] $$(2\sigma+M)\bmod 2=M$$

[0029] 바람직하게는, 상기 데이터 전송자의 서명을 추출하는 단계는 수학식 7에 의거하여 수행될 수 있다.

[0030] [수학식 7]

[0031] $$(2\sigma+M-M)/2=\sigma$$

[0032] 바람직하게는, 상기 목적 데이터의 무결성을 검증하는 단계를 더 포함하고, 상기 무결성을 검증하는 단계는 수학식 8에서 랜덤 값들을 구성요소로 하는 n차원의 벡터 s를 산출한 후, 수학식 9를 만족하는지 여부에 기초하여 수행될 수 있다.

[0033] [수학식 8]

[0034] $$c-(2\sigma+M)=B^{T}s\bmod q$$

[0035] [수학식 9]

[0036] $$\sigma\neq 0,\ \|\sigma\|\leq\delta\sqrt{m},A\sigma=H(M,s)$$

[0037] 이때, δ 는 제1 변수 n, 제2 변수 m, 제3 변수 δ 및 제4 변수 q를 포함하는 공개 변수들 중 제3 변수이고, H는 0 내지 2사이의 값들을 구성요소로 하는 m차원의 벡터와 0 내지 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터를 입력으로 0 내지 q사이의 랜덤 해쉬 값들을 구성요소로 하는 n차원의 벡터를 출력하는 안전 해쉬 함수를 나타낸다.

[0038] 또한, 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 래티스 기반의 암호서명 생성 장치는 공개 변수들을 설정하고, 상기 설정한 공개 변수들 및 기저 생성 함수에 기초하여 데이터 전송자 및 데이터 수신자 각각의 공개키 및 비밀키를 생성하는 키 생성부; 상기 공개 변수들, 상기 데이터 전송자의 비밀키, 전송할 목적 데

이터 및 서명생성 함수를 이용하여 상기 데이터 전송자의 서명을 생성하는 서명 생성부; 및 상기 데이터 수신자의 공개키, 상기 데이터 전송자의 서명 및 상기 목적 데이터를 이용하여 상기 전송할 데이터에 대한 암호문으로서 상기 데이터 전송자에 대한 서명값을 포함하는 암호서명을 생성하는 암호서명 생성부를 포함한다.

[0039] 바람직하게는, 상기 서명 생성부는 0 내지 2사이의 값들을 구성요소로 하는 m차원의 벡터와 0 내지 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터를 입력으로 0 내지 q사이의 랜덤 해쉬 값들을 구성요소로 하는 n차원의 벡터를 출력하는 안전 해쉬 함수를 설정하는 해쉬 함수 생성부; 0에서 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터 s를 생성하는 벡터 생성부; 및 상기 안전 해쉬함수에 상기 목적 데이터에 대응되는 m차원의 벡터 및 상기 벡터 s를 입력하여 출력된 n차원의 해쉬 출력 벡터, 상기 데이터 전송자의 비밀키 S_A, 상기 제3 변수 δ 및 상기 서명생성 함수를 이용하여 m차원의 벡터 형태를 가진 상기 데이터 전송자의 서명 σ를 생성하는 서명 처리부를 포함한다.

[0040] 또한, 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 래티스 기반의 암호서명 복원 장치는 데이터 수신자의 공개키, 데이터 전송자의 서명 및 전송하고자 하는 목적 데이터를 이용하여 생성된 상기 목적 데이터에 대한 암호문으로서 상기 데이터 전송자에 대한 서명값을 포함하는 암호서명을 수신하는 수신부; 상기 암호서명에 기초하여 상기 데이터 수신자의 비밀키를 이용하여 상기 데이터 전송자의 서명과 상기 목적 데이터만이 결합된 형태를 가진 중간 연산값을 산출하는 중간 연산 산출부; 상기 산출된 중간 연산값에 mod함수를 적용하여 상기 중간 연산값으로부터 상기 목적 데이터를 추출하는 데이터 추출부; 및 상기 추출된 목적 데이터를 이용하여 상기 중간 연산값으로부터 상기 데이터 전송자의 서명을 추출하는 서명 추출부를 포함하고, 상기 데이터 수신자의 공개키 및 비밀키는 행렬 형태를 가지고, 상기 데이터 수신자의 공개키에 대응되는 행렬과 상기 데이터 수신자의 비밀키에 대응되는 행렬을 곱하여 생성된 행렬의 구성요소들 각각의 값은 0이 된다.

[0041] 바람직하게는, 본 발명의 일 실시예에 따른 래티스 기반의 암호서명 복원 장치는 상기 목적 데이터의 무결성을 검증하는 무결성 검증부를 더 포함하고, 상기 무결성을 검증부는 수학식 8에서 랜덤 값들을 구성요소로 하는 n차원의 벡터 s를 산출한 후, 수학식 9를 만족하는지 여부에 기초하여 무결성을 검증한다.

[0042] [수학식 8]

[0043] $$c-(2\sigma+M)=B^{T}s \bmod q$$

[0044] [수학식 9]

[0045] $$\sigma \neq 0,\ \|\sigma\| \leq \delta\sqrt{m},\ A\sigma = H(M,s)$$

[0046] 이때, δ 는 제1 변수 n, 제2 변수 m, 제3 변수 δ 및 제4 변수 q를 포함하는 공개 변수들 중 제3 변수이고, H는 0 내지 2사이의 값들을 구성요소로 하는 m차원의 벡터와 0 내지 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터를 입력으로 0 내지 q사이의 랜덤 해쉬 값들을 구성요소로 하는 n차원의 벡터를 출력하는 안전 해쉬 함수를 나타낸다.

발명의 효과

[0047] 본 발명의 일 실시예에 따른 암호 서명 기술은 래티스 기반으로 설계되었기 때문에 래티스 기반 암호 시스템이 갖는 연산 효율성, 높은 안전성, 양자 컴퓨터 분석에 대한 내성의 장점을 가지면서 데이터에 대해 무결성과 기밀성을 동시에 보장할 수 있는 효과가 있다.

도면의 간단한 설명

[0048] 도 1은 본 발명의 일실시예에 따른 래티스 기반의 암호서명 생성 장치를 설명하기 위하여 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 서명 생성부를 설명하기 위하여 도시한 도면이다.

도 3은 본 발명의 일실시예에 따른 래티스 기반의 암호서명 생성 방법을 설명하기 위하여 도시한 흐름도이다.

도 4는 본 발명의 일실시예에 따른 서명 생성 방법을 설명하기 위하여 도시한 흐름도이다.

도 5는 본 발명의 일실시예에 따른 래티스 기반의 암호서명 복원 장치를 설명하기 위하여 도시한 도면이다.

도 6은 본 발명의 일실시예에 따른 래티스 기반의 암호서명 복원 방법을 설명하기 위하여 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0049] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0050] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0051] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0052] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0053] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0054] 본 발명의 실시예들을 설명하기에 앞서, 본 발명의 기반이 되는 기술인 래티스(lattices)에 대해 설명하고, 이를 통해 본 발명의 일 실시예에서 사용되는 알고리즘들에 대해서도 상세히 살펴보기로 한다.

[0055] **- 래티스 (lattices)**

[0056] 본 발명에서는 m차원의 풀-랭크(full-rank) 정수 래티스를 사용하며, 이것은 유한개의 지수(finite index)를 가지는 $\mathbb{Z}^m$의 이산 가산 서브그룹(discrete additive subgroup)이다. 즉, 퀴션트 그룹(quotient group) $\mathbb{Z}^m/\Lambda$이 유한하다. 하나의 래티스 $\Lambda\subseteq\mathbb{Z}^m$은 m개의 선형 독립 기저(basis) 벡터 $B=\{b_1,\cdots b_m\}\subset\mathbb{Z}^m$의 모든 정수 선형 결합의 집합과 동일하게 정의된다.

[0057] $$\Lambda=L(B)=\left\{Bc=\sum_{i\in\{1,\cdots,m\}}c_i b_i : c\in\mathbb{Z}^m\right\}$$

[0058] 여기서 $m\geq 2$일 경우, 동일한 래티스를 생성하는 기저들은 무수히 많다.

[0059] **- 하드 래티스와 SIS, LWE 문제**

[0060] 본 발명에서는 다음과 같은 정수 래티스의 특정한 형태를 사용한다. 여기서 $n\geq 1$과 $q\geq 2$는 정수이며, 차원 n은 본 발명에서 사용되는 보안 파라미터이고, 모든 다른 파라미터들은 n의 함수들로 내포되었다고 가정한다. 여기

서 m차원 하드 래티스는 패리티 검사 행렬(parity check matrix) $A \in Z_q^{n \times m}$에 의해 생성되며, 다음과 같이 정의된다.

[0061] $$\Lambda^{\perp}(A)=\left\{x \in Z^m : Ax=\sum_{j \in \{1,\cdots,m\}} x_j \cdot a_j = 0 \in Z_q^n\right\} \subseteq Z^m$$

[0062] 그리고 어떤 y에 대해서, 패리티 검사 행렬 $A \in Z_q^{n \times m}$에 의해 생성되는 코셋(coset)은 다음과 같이 정의된다.

[0063] $$\Lambda_y^{\perp}(A)=\{x \in Z^m : Ax=y \in Z_q^n\}$$

[0064] 어떤 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 열 벡터는 Z_q^n 상의 모두를 ($2^{-\Omega(n)}=negl(n)$ 확률을 제외하고) 생성할 수 있다. 따라서 본 발명에서는 균등하게 랜덤한 A를 사용한다.

[0065] 다음으로 하드 래티스의 SIS(Short Integer Solution) 문제에 대해서 살펴보자. 이 문제는 평균적인 경우에 어려운 문제(average-case hardness problems)에 속해 있으며, 이 문제를 최악의 경우에 어려운 문제(worst-case hardness problems)로 커넥션(connection)하는 방법에 대해서도 공지된 바 있다.

[0066] 참고로, $SIS_{q,\beta}$ 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. SIS 문제에서 알고리즘 A의 성공 확률은 $Adv_{SIS_{q,\beta}}$로 나타낸다.

[0067] 또한, LWE 문제는 정수 n,q와 Z_q상의 특정 분포 χ에 대해, $LWE_{n,q,\chi}$ 문제는 주어진 다수의 $(a,a^T s+x) where\ a,s \leftarrow Z_q^n, x \leftarrow \chi$에서 벡터 s를 찾는 것으로 정의된다.

[0068] 특히, LWE 문제에서 x가 분포 $\overline{\Psi_\alpha}(q)^m$을 따르는 경우, 이 역시 SIS 문제와 마찬가지로 최악의 경우에 어려운 문제(worst-case hardness problems)로 커넥션(connection)할 수 있다. 여기서 분포 $\overline{\Psi_\alpha}$란 $0<\alpha<1$, 소수 q에 대해 X가 평균 0, 표준편차 $\alpha/\sqrt{2\pi}$을 따르는 정규분포라고 할 때, qX에 가장 가까운 정수를 나타내는 확률변수를 의미한다.

[0069] **- 래티스에서의 가우시안 분포**

[0070] 본 발명에서 제안된 내용을 바탕으로 래티스에서의 가우시안 분포에 대해서 살펴본다. 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 정의된다. 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.

[0071] 다음으로 본 발명에서 사용되는 래티스에서의 가우시안 분포와 관련되는 성질들을 살펴본다. 여기에서 S는 어

떤 $A \in Z_q^{n \times m}$ 에 대한 $\Lambda^{\perp}(A)$의 기저를 말하며, $s \geq \|\tilde{S}\| \cdot \omega(\sqrt{\log n})$이다.

[0072] $$\Pr_{x \leftarrow D_{\Lambda_y^{\perp}(A),s}}[\|x\| > s \cdot \sqrt{m}] \leq negl(n)$$

[0073] $$\Pr_{x \leftarrow D_{\Lambda^{\perp}(A),s}}[x=0] \leq negl(n)$$

[0074] ($negl(n)$ 통계적인 거리를 가지는) $D_{\Lambda_y^{\perp}(A),s}$로부터 샘플링을 할 수 있는 PPT(probabilistic polynomial time) 알고리즘 SampleD(S,y,s)이 존재한다.

[0075] **- 기저와 트랩도어 (basis and trapdoors)**

[0076] 본 발명에서는 균등한 분포에서 임의로 선택된 매트릭스 $A \in Z_q^{n \times m}$ 와 이러한 매트릭스로 생성되는 래티스 $\Lambda^{\perp}(A)$의 짧은 기저 T_A를 생성하는 알고리즘 $(A \in Z_q^{n \times m}, T_A \in Z^{m \times m}) \leftarrow \mathrm{GBasis}\ (1^n, 1^m, q)$을 사용한다. 위의 알고리즘에서 파라미터들은 $m = O(n \log q)$을 만족하며, 기저 T_A의 길이는 $\|\widetilde{T_A}\| = O(\sqrt{n \log q})$만큼 짧다. 임의의 래티스의 짧은 기저를 찾는 문제는 결국 SIS 문제이기 때문에 알고리즘 $GBasis(1^n, 1^m, q)$은 임의의 래티스와 그것의 트랩도어 (SIS 문제에 대한) 즉, 짧은 기저를 생성하게 된다.

[0077] **- 특별한 성질을 만족하는 기저와 트랩도어**

[0078] 본 발명에서는 위의 트랩도어 생성 알고리즘을 변형한 특별한 성질을 만족하는 변형 트랩도어 생성 알고리즘으로서 SuperSamp$(1^n, 1^m, q, B)$ 알고리즘을 사용한다. 해당 알고리즘은 위의 GBasis의 입력값에 추가적으로 매트릭스 $B \in Z_q^{n \times m}$ 를 입력받아 위의 알고리즘과 동일한 분포의 결과값 즉, 래티스 및 그것의 짧은 기저 쌍 $(A \in Z_q^{n \times m} T_A \in Z^{m \times m})$을 출력한다.

[0079] 여기서 중요한 성질은 입력값으로 받은 매트릭스 B와 출력 매트릭스인 A 사이에는 $AB^T = 0$을 만족한다는 것이다. SuperSamp의 입력 파라미터는 수식 $n, q \geq 2, m \geq n + 8n \log q$을 만족해야 한다.

[0080] **- 위임 방법 (delegation method)**

[0081] 본 발명에서는 래티스의 짧은 기저를 위임하는 기법인 BasisDel 알고리즘을 사용한다. 우선 다음과 같이 짧은 길이의 벡터를 열벡터로 갖는 매트릭스 $R^{m \times m}$을 정의한다. $R^{m \times m}$의 열벡터의 분포는 가우시안 분포 $D_{z^m, \sqrt{n \log q}\omega(\sqrt{\log m})}$를 따른다.

[0082] BasisDel (A, R, T_A, s) 알고리즘은 매트릭스 $A \in Z_q^{n \times m}$, 래티스 $\Lambda^{\perp}(A)$의 짧은 기저 T_A, 위에서 정의한 짧은 매트릭스 $R \in R^{m \times m}$ 그리고 파라미터 $s \geq m\|\widetilde{T_A}\|\omega(\sqrt{\log m})^4$을 입력값으로 받아, 매트릭스 AR^{-1}와 이로 생성되는 래티스 $\Lambda^{\perp}(AR^{-1})$의 짧은 기저 $T_{AR^{-1}}$을 출력한다. 특히, 생성된 기저의 길이는 $\|T_{AR^{-1}}\| \leq \|T_A\| m^{3/2} \omega(\sqrt{\log m})^4$ 만큼 증가 비율을 갖는다.

[0083] **- 매트릭스 변환 방법(matirx transformation method)**

[0084] 본 발명에서는 다음과 같은 매트릭스(래티스) 변환 알고리즘, Transform 알고리즘을 제안한다. 해당 알고리즘 $\mathrm{Transform}^{(A,T_A,B,s)}$은 매트릭스 $A,B\in Z_q^{n\times m}$, 래티스 $\Lambda^{\perp}(A)$의 짧은 기저 T_A, 그리고 파라미터 $s\geq\|\widetilde{T_A}\|\omega(\sqrt{\log m})$을 입력값으로 받아, 위에서 정의한 짧은 매트릭스 분포 $R^{m\times m}$을 따르는 매트릭스 $K\in Z^{m\times m}$을 출력한다.

[0085] 출력된 매트릭스 K는 수식 $AK=B,\|K\|\leq s\sqrt{m}$을 만족한다. 해당 알고리즘을 설계하는 방법은 k_i,b_i를 각각 매트릭스 K,B의 i번째 열이라고 했을 때, $k_i\leftarrow\mathrm{SamplePre}^{(T_A,b_i,s)}$을 이용하여 생성할 수 있다. 해당 방법을 m번 사용하면 매트릭스를 완성할 수 있으며, SamplePre의 성질에 따라 $AK=B \bmod q$임을 확인할 수 있다.

[0086] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0087] 도 1은 본 발명의 일실시예에 따른 래티스 기반의 암호서명 생성 장치를 설명하기 위하여 도시한 도면이다.

[0088] 도 1을 참조하면, 본 발명의 일실시예에 따른 래티스 기반의 암호서명 생성 장치는 키 생성부(110), 서명 생성부(120) 및 암호서명 생성부(130)를 포함한다.

[0089] 키 생성부(110)는 공개 변수들을 설정하고, 설정한 공개 변수들 및 기저 생성 함수에 기초하여 데이터 전송자 및 데이터 수신자 각각의 공개키 및 비밀키를 생성한다.

[0090] 이때, 공개 변수들은 상호간에 관련성을 가지는 제1 변수 n, 제2 변수 m, 제3 변수 δ 및 제4 변수 q를 포함할 수 있으며, 제1 변수 n은 보안 파라미터로서 값이 높을수록 보안성이 높아진다.

[0091] 제1 변수 n, 제2 변수 m, 제3 변수 δ 및 제4 변수 q는 n=k, m=10nlogq, $\delta=\sqrt{m}w(\sqrt{\log m})$, q=(2δ+1)^{2}m과 같이 정의될 수 있다.

[0092] 한편, 래티스 암호화 시스템에서 데이터 전송자 및 데이터 수신자 각각의 공개키 및 비밀키는 기저 생성 함수 GBasis를 이용하여 수학식 1과 같이 정의될 수 있다.

수학식 1

$$(A\in Z_q^{n\times m},S_A\in Z_q^{m\times m})\leftarrow GBasis(1^n,1^m,q)$$

$$(B\in Z_q^{n\times m},S_B\in Z_q^{m\times m})\leftarrow GBasis(1^n,1^m,q)$$

[0093]

[0094] 이때, A는 행렬로서 데이터 전송자의 공개키를 나타내고, S_A는 행렬로서 데이터 전송자의 비밀키를 나타내고, B는 행렬로서 데이터 수신자의 공개키를 나타내고, S_B는 행렬로서 데이터 전송자의 비밀키를 나타내는데, 데이터 전송자의 공개키 행렬 A와 데이터 수신자의 공개키 행렬 B는 n * m의 크기를 가지고 0에서 q사이의 랜덤 값들을 구성요소로 가지고, 데이터 전송자의 비밀키 행렬 S_A와 데이터 수신자의 비밀키 행렬 S_B는 m * m의 크기를 가지고 0에서 q사이의 랜덤 값들을 구성요소로 가진다.

[0095] 한편, 데이터 전송자의 공개키 A, 데이터 전송자의 비밀키 S_A, 데이터 수신자의 공개키 B, 데이터 수신자의 비밀키 S_B 각각은 기저 생성 함수 GBasis에 기초하여 생성되므로, 데이터 전송자의 공개키 행렬 A와 데이터 전송자의 비밀키 행렬 S_A를 곱하여 생성된 제1 곱셈 행렬 및 데이터 수신자의 공개키 행렬 B와 데이터 수신자의 비밀키 행렬 S_B를 곱하여 생성된 제2 곱셈 행렬의 구성요소들 각각의 값은 0이 되는 성질을 가지게 된다.

[0096] 본 발명의 일실시예에 따른 래티스 기반의 암호서명 복원 방법은 이와 같은 성질을 이용하여 암호서명을 복원하게 된다.

[0097] 서명 생성부(120)는 공개 변수들, 데이터 전송자의 비밀키, 전송할 목적 데이터 및 서명생성 함수를 이용하여 데이터 전송자의 서명을 생성한다.

[0098] 이때, 서명 생성부(120)는 데이터 전송자의 비밀키를 이용하여 데이터 전송자의 서명을 생성하므로 데이터 전송자만이 데이터 전송자의 서명을 생성할 수 있게 된다.

[0099] 서명 생성부(120)가 데이터 전송자의 서명을 생성하는 구체적인 프로세스에 대해서는 도 2를 참조하여 후술한다.

[0100] 암호서명 생성부(130)는 데이터 수신자의 공개키, 데이터 전송자의 서명 및 목적 데이터를 이용하여 전송할 데이터에 대한 암호문으로서 데이터 전송자에 대한 서명값을 포함하는 암호서명을 생성한다.

[0101] 이와 같이, 본 발명의 일 실시예는 래티스 암호화 시스템의 기저 생성 함수 및 서명생성 함수를 이용하여 암호서명을 생성하므로 래티스 기반 암호 시스템이 갖는 연산 효율성, 높은 안전성, 양자 컴퓨터 분석에 대한 내성의 장점을 가지면서 데이터에 대해 무결성과 기밀성을 동시에 보장할 수 있는 효과가 잇다.

[0102] 도 2는 본 발명의 일실시예에 따른 서명 생성부를 설명하기 위하여 도시한 도면이다.

[0103] 도 2를 참조하면, 본 발명의 일실시예에 따른 서명 생성부(120)는 해쉬 함수 생성부(122), 벡터 생성부(124) 및 서명 처리부(126)를 포함한다.

[0104] 해쉬 함수 생성부(122)는 0 내지 2사이의 값들을 구성요소로 하는 m차원의 벡터와 0 내지 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터를 입력으로 0 내지 q사이의 랜덤 해쉬 값들을 구성요소로 하는 n차원의 벡터를 출력하는 안전 해쉬 함수 $H: Z_2^m \times Z_q^n \rightarrow Z_q^n$ 를 설정한다.

[0105] 벡터 생성부(124)는 0에서 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터 $s \leftarrow Z_q^n$ 를 생성한다.

[0106] 서명 처리부(126)는 안전 해쉬함수 H에 벡터 생성부(120)가 생성한 벡터 s와 목적 데이터에 대응되는 m차원의 벡터 M을 입력하여 출력된 n차원의 해쉬 출력 벡터, 데이터 전송자의 비밀키 S_A, 제3 변수 δ 및 서명생성 함수 SampleD를 이용하여 m차원의 벡터 형태를 가진 데이터 전송자의 서명 σ를 생성한다.

[0107] 즉, 서명 처리부(126)는 수학식 2에 의하여 데이터 전송자의 서명 σ를 생성한다.

수학식 2

[0108] $$\sigma \in Z^m \leftarrow SampleD(S_A, H(M,s), \delta)$$

[0109] 이때, 해쉬함수 H에 입력으로 표시되어 있는 M은 전송할 목적 데이터를 나타내고 M의 데이터 공간은 Z_2^m 이다. 즉, M은 m차원의 벡터로서 0부터 2사이의 값들을 구성요소로 한다.

[0110] 한편, 서명생성 함수 SampleD는 래티스 암호화 시스템에서 일반적으로 사용되는 함수이므로 자세한 설명은 생략한다.

[0111] 도 3은 본 발명의 일실시예에 따른 래티스 기반의 암호서명 생성 방법을 설명하기 위하여 도시한 흐름도이다.

[0112] 단계 310에서는, 래티스 기반의 암호서명 생성 장치가 공개 변수들을 설정하고, 그 설정한 공개 변수들 및 기저 생성 함수에 기초하여 데이터 전송자 및 데이터 수신자 각각의 공개키 및 비밀키를 생성한다.

[0113] 단계 320에서는, 래티스 기반의 암호서명 생성 장치가 공개 변수들, 데이터 전송자의 비밀키, 전송할 목적 데이터 및 서명생성 함수를 이용하여 데이터 전송자의 서명을 생성한다.

[0114] 단계 330에서는, 래티스 기반의 암호서명 생성 장치가 데이터 수신자의 공개키, 데이터 전송자의 서명 및 목적 데이터를 이용하여 전송할 데이터에 대한 암호문으로서 데이터 전송자에 대한 서명값을 포함하는 암호서명을 생성한다.

[0115] 보다 구체적으로는, 래티스 기반의 암호서명 생성 장치는 암호서명을 수학식 3과 같이 생성하게 된다.

수학식 3

[0116] $$c=(B^{T}s+2\sigma+M) \bmod q$$

[0117] 이때, c는 암호서명을 나타내고, B^{T}는 데이터 수신자의 공개키 B를 트랜스포즈한 값, s는 0에서 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터, σ는 데이터 전송자의 서명, modq는 괄호안의 값을 q로 나눈 나머지 값을 나타낸다.

[0118] 도 4는 본 발명의 일실시예에 따른 서명 생성 방법을 설명하기 위하여 도시한 흐름도이다.

[0119] 단계 410에서는, 래티스 기반의 암호서명 생성 장치가 0 내지 2사이의 값들을 구성요소로 하는 m차원의 벡터와 0 내지 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터를 입력으로 0 내지 q사이의 랜덤 해쉬 값들을 구성요소로 하는 n차원의 벡터를 출력하는 안전 해쉬 함수를 설정한다.

[0120] 단계 420에서는, 래티스 기반의 암호서명 생성 장치가 0에서 q사이의 랜덤 값들을 구성요소로 하는 n차원의 벡터 s를 생성한다.

[0121] 단계 430에서는, 래티스 기반의 암호서명 생성 장치가 안전 해쉬함수에 목적 데이터에 대응되는 m차원의 벡터 및 벡터 s를 입력하여 출력된 n차원의 해쉬 출력 벡터, 데이터 전송자의 비밀키 S_A, 제3 변수 δ 및 서명생성 함수를 이용하여 m차원의 벡터 형태를 가진 데이터 전송자의 서명 σ를 생성한다.

[0122] 도 5는 본 발명의 일실시예에 따른 래티스 기반의 암호서명 복원 장치를 설명하기 위하여 도시한 도면이다.

[0123] 도 5를 참조하면, 본 발명의 일 실시예에 따른 래티스 기반의 암호서명 복원 장치는 수신부(510), 중간 연산 산출부(520), 데이터 추출부(530) 및 서명 추출부(540)를 포함한다.

[0124] 수신부(510)는 데이터 수신자의 공개키, 데이터 전송자의 서명 및 전송하고자하는 목적 데이터를 이용하여 생성된 목적 데이터에 대한 암호문으로서 데이터 전송자에 대한 서명값을 포함하는 암호서명을 수신한다.

[0125] 중간 연산 산출부(520)는 데이터 수신자의 비밀키를 이용하여 데이터 전송자의 서명과 목적 데이터만이 결합된 형태를 가진 중간 연산값을 산출한다.

[0126] 예컨대, 중간 연산 산출부(520)는 수학식 4 및 수학식 5에 기초하여 중간 연산값을 산출할 수 있다.

수학식 4

[0127] $$(S_B)^{T}c=(BS_B)^{T}s+(S_B)^{T}(2\sigma+M) \bmod q=(S_B)^{T}(2\sigma+M) \bmod q=(S_B)^{T}(2\sigma+M)$$

[0128] 이때, $(S_B)^{T}$ 는 데이터 수신자의 비밀키에 대응되는 행렬 S_B를 트랜스포즈한 행렬로서, 수학식 4에서는 $(S_B)^{T}$ 를 암호서명 c에 곱해주게 되는데, 전술한 바와 같이 데이터 수신자의 공개키 B 행렬과 데이터 수신자의 비밀키 S_B 행렬을 곱하여 생성된 제2 곱셈 행렬의 구성요소들 각각의 값은 0이 되는 성질이 있으므로 수학식 4의 최우측과 같이 $(S_B)^{T}(2\sigma+M)$ 이 산출된다.

수학식 5

[0129] $$(S_B)^{-T}(S_B)^{T}(2\sigma+M)=2\sigma+M$$

[0130] 이때, $(S_B)^{-T}$ 는 $(S_B)^{T}$ 행렬의 역행렬로서, 수학식 4에서 산출된 값에 $(S_B)^{-T}$를 곱해줌으로써 중간 연산값 2σ+M이 산출된다.

[0131] 데이터 추출부(530)는 그 산출된 중간 연산값에 mod함수를 적용하여 중간 연산값으로부터 목적 데이터를 추출한다.

[0132] 예컨대, 데이터 추출부(530)는 수학식 6에 기초하여 목적 데이터를 추출할 수 있다.

수학식 6

[0133] $$(2\sigma+M)\bmod 2=M$$

[0134] 수학식 6에서 중간 연산값 2σ+M에 mod2 함수를 적용하여 목적 데이터만을 추출할 수 있는 이유는 2σ가 짝수 값이고, M의 데이터 공간이 Z_2^m 이기 때문이다.

[0135] 서명 추출부(540)는 그 추출된 목적 데이터를 이용하여 중간 연산값으로부터 데이터 전송자의 서명을 추출한다.

[0136] 예컨대, 서명 추출부(540)는 수학식 7에 기초하여 데이터 전송자의 서명을 추출할 수 있다

수학식 7

[0137] $$(2\sigma+M-M)/2=\sigma$$

[0138] 수학식 7에서는 중간 연산값 2σ+M에서 M을 빼준 후에, 그 연산 결과를 2로 나눠줌으로써 간단하게 데이터 전송자의 서명 σ를 추출할 수 있게 된다.

[0139] 바람직하게는, 본 발명의 일 실시예에 따른 래티스 기반의 암호서명 복원 장치는 목적 데이터의 무결성을 검증하는 무결성 검증부(미도시)를 더 포함할 수 있다.

[0140] 무결성 검증부는 수학식 8 및 수학식 9에 의하여 목적 데이터의 무결성을 검증할 수 있다.

[0141] [수학식 8]

[0142] $$c-(2\sigma+M)=B^{T}s\bmod q$$

[0143] 수학식 8에 의하여 무결성 검증부는 랜덤 값들을 구성요소로 하는 n차원의 벡터 s를 산출하게 된다.

[0144] [수학식 9]

[0145] $$\sigma\neq 0,\ \|\sigma\|\leq\delta\sqrt{m},A\sigma=H(M,s)$$

[0146] 무결성 검증부는 수학식 8에서 산출된 벡터 s를 수학식 9에 적용하고, 수학식 9의 3개의 조건이 모두 만족되는지에 기초하여 목적 데이터의 무결성을 검증하게 된다. 만일, 수학식 9의 3개의 조건이 모두 만족되면 목적 데이터의 무결성이 인정되고, 수학식 9의 3개의 조건 중에 하나라도 만족되지 않으면 목적 데이터의 무결성은 인

정되지 않게 된다.

[0147] 이와 같이, 본 발명의 일 실시예에 따른 래티스 기반의 암호서명 복원 장치에 따르면 수신된 암호서명으로부터 목적 데이터 및 데이터 전송자의 서명 σ를 추출할 수 있으므로, 데이터 전송자와 데이터 수신자가 암호서명을 이용하여 데이터를 송수신하는 것만으로도 데이터에 대해 무결성과 기밀성을 동시에 보장할 수 있게 되는 효과가 있다.

[0148] 도 6은 본 발명의 일실시예에 따른 래티스 기반의 암호서명 복원 방법을 설명하기 위하여 도시한 흐름도이다.

[0149] 단계 610에서는, 래티스 기반의 암호서명 복원 장치가 데이터 수신자의 공개키, 데이터 전송자의 서명 및 전송하고자 하는 목적 데이터를 이용하여 생성된 목적 데이터에 대한 암호문으로서 데이터 전송자에 대한 서명값을 포함하는 암호서명을 수신한다.

[0150] 단계 620에서는, 래티스 기반의 암호서명 복원 장치가 그 수신된 암호서명에 기초하여 데이터 수신자의 비밀키를 이용하여 데이터 전송자의 서명과 목적 데이터만이 결합된 형태를 가진 중간 연산값을 산출한다.

[0151] 단계 630에서는, 래티스 기반의 암호서명 복원 장치가 그 산출된 중간 연산값에 mod함수를 적용하여 중간 연산값으로부터 목적 데이터를 추출한다.

[0152] 단계 640에서는, 래티스 기반의 암호서명 복원 장치가 추출된 목적 데이터를 이용하여 중간 연산값으로부터 데이터 전송자의 서명을 추출한다.

[0153] 마지막으로, 래티스 기반의 암호서명 복원 장치는 그 추출된 목적 데이터와 데이터 전송자의 서명을 이용하여 목적 데이터의 무결성을 검증할 수 있다.

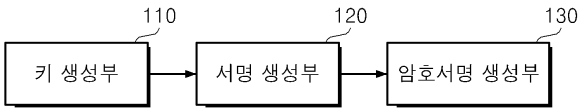
[0154] 한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[0155] 상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 를 포함한다.

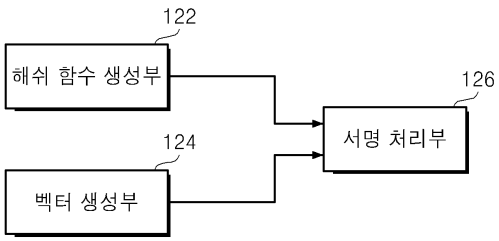
[0156] 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

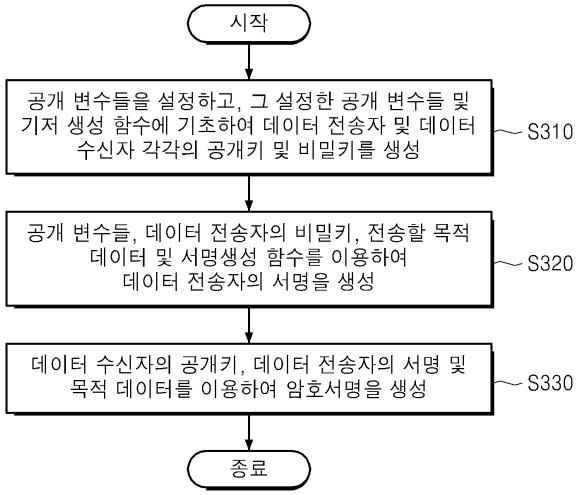
도면1



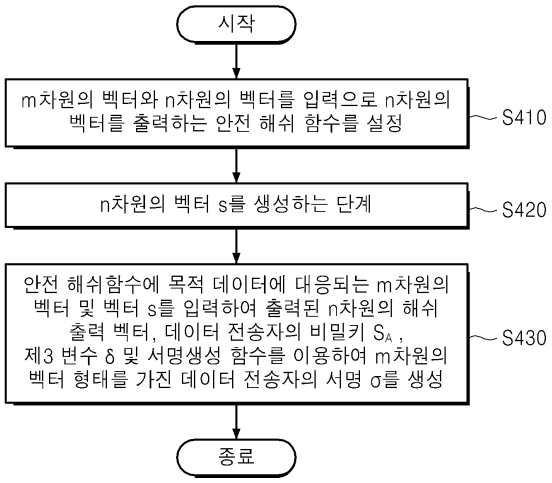
도면2



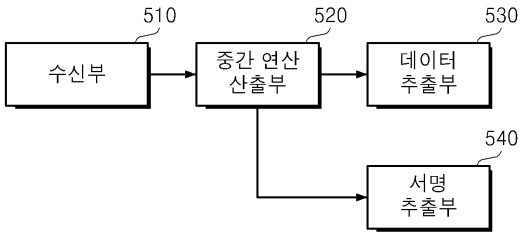
도면3


시작
공개 변수들을 설정하고, 그 설정한 공개 변수들 및 기저 생성 함수에 기초하여 데이터 전송자 및 데이터 수신자 각각의 공개키 및 비밀키를 생성
S310
공개 변수들, 데이터 전송자의 비밀키, 전송할 목적 데이터 및 서명생성 함수를 이용하여 데이터 전송자의 서명을 생성
S320
데이터 수신자의 공개키, 데이터 전송자의 서명 및 목적 데이터를 이용하여 암호서명을 생성
S330
종료

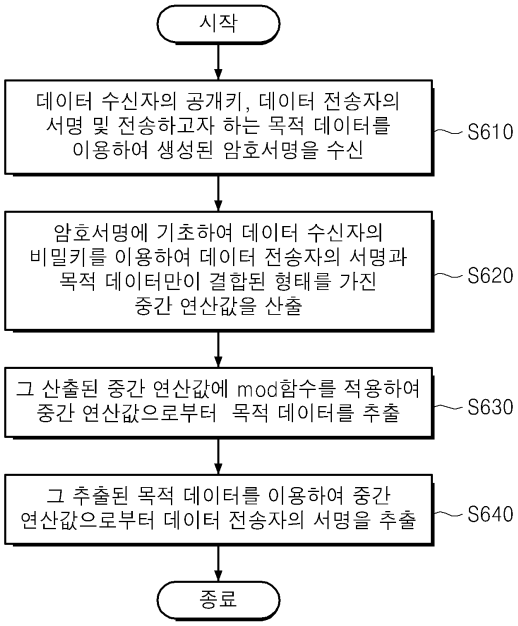
도면4


시작
m차원의 벡터와 n차원의 벡터를 입력으로 n차원의 벡터를 출력하는 안전 해쉬 함수를 설정
S410
n차원의 벡터 s를 생성하는 단계
S420
안전 해쉬함수에 목적 데이터에 대응되는 m차원의 벡터 및 벡터 s를 입력하여 출력된 n차원의 해쉬 출력 벡터, 데이터 전송자의 비밀키 S_A, 제3 변수 δ 및 서명생성 함수를 이용하여 m차원의 벡터 형태를 가진 데이터 전송자의 서명 σ를 생성
S430
종료

도면5


510
520
530
수신부
중간 연산 산출부
데이터 추출부
540
서명 추출부

도면6


시작
데이터 수신자의 공개키, 데이터 전송자의 서명 및 전송하고자 하는 목적 데이터를 이용하여 생성된 암호서명을 수신
S610
암호서명에 기초하여 데이터 수신자의 비밀키를 이용하여 데이터 전송자의 서명과 목적 데이터만이 결합된 형태를 가진 중간 연산값을 산출
S620
그 산출된 중간 연산값에 mod함수를 적용하여 중간 연산값으로부터 목적 데이터를 추출
S630
그 추출된 목적 데이터를 이용하여 중간 연산값으로부터 데이터 전송자의 서명을 추출
S640
종료