



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0081168

(43) 공개일자 2015년07월13일

(51) 국제특허분류(Int. Cl.)

H04N 21/6334 (2011.01) H04N 21/2543

(2011.01)

(21) 출원번호 10-2014-0000873

(22) 출원일자 2014년01월03일

심사청구일자 2014년01월03일

(71) 출원인

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

정익래

서울특별시 광진구 긴고랑로4길 53 203호(중곡1동, 호동아파트)

노건태

서울특별시 강남구 개포로 516 707동 1304호 (개포동, 주공아파트)

천지영

서울특별시 성북구 오패산로 46 118동 104호 (하월곡동, 월곡두산위브아파트)

(74) 대리인

심경식, 홍성욱, 한승범, 유병욱

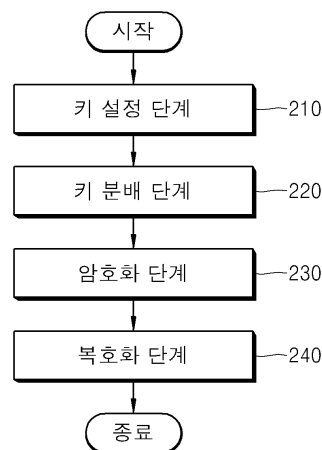
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 래티스에서의 아이디 기반 브로드캐스트 방법

(57) 요약

본 발명의 일 실시예에 따른 래티스에서의 아이디 기반 브로드캐스트 방법은 균일 분포를 가지는 랜덤 행렬 A_0 및 해시 함수 H 를 공개키로 설정하고, 상기 랜덤 행렬 A_0 에 대응되는 기저 B_0 를 비밀키로 설정하는 키 설정 단계; 상기 키 설정 단계에서 설정된 상기 공개키 및 상기 비밀키에 기초하여 사용자의 아이디(ID)에 대응되는 비밀키를 생성하고, 상기 생성된 비밀키를 상기 사용자에게 전송하는 키 분배 단계; 및 상기 공개키 및 상기 비밀키와 임의의 난수들을 이용하여 평문의 문자열 데이터를 암호화하여 암호문을 생성하고, 상기 생성된 암호문을 상기 평문 전송을 요청한 참여자에게 브로드캐스트 하는 암호화 단계를 포함한다.

대표도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호 2013026726

부처명 미래부

연구관리전문기관 한국연구재단

연구사업명 (이공)일반연구자-여성과학자

연구과제명 래티스 기반의 효율적인 서명 및 인증 기법 연구

기 여 율 1/1

주관기관 고려대학교산학협력단

연구기간 2013.05.01 ~ 2014.04.30

명세서

청구범위

청구항 1

균일 분포를 가지는 랜덤 행렬 A_0 및 해시 함수 H 를 공개키로 설정하고, 상기 랜덤 행렬 A_0 에 대응되는 기저 B_0 를 비밀키로 설정하는 키 설정 단계;

상기 키 설정 단계에서 설정된 상기 공개키 및 상기 비밀키에 기초하여 사용자의 아이디(ID)에 대응되는 비밀키를 생성하고, 상기 생성된 비밀키를 상기 사용자에게 전송하는 키 분배 단계; 및

상기 공개키 및 상기 비밀키와 임의의 난수들을 이용하여 평문의 문자열 데이터를 암호화하여 암호문을 생성하고, 상기 생성된 암호문을 상기 평문 전송을 요청한 참여자에게 브로드캐스트 하는 암호화 단계

를 포함하는 것을 특징으로 하는 래티스에서의 아이디 기반 브로드캐스트 방법.

청구항 2

제1항에 있어서,

상기 키 설정 단계는

보안 파라미터 n , 차원 $m=O(n \log q)$, 양의 정수 q 를 입력 파라미터로 하는 기저 생성 알고리즘을 이용하여, $-q/2 \sim q/2$ 범위 내의 랜덤 값을 행렬 값으로 가지는 $n \times m$ 행렬 각각을 상기 랜덤 행렬 A_0 및 상기 기저 B_0 로서 생성하는 단계;

상기 기저 생성 알고리즘의 입력 파라미터를 이용하여 상기 해시 함수 H 를 생성하는 단계; 및

상기 랜덤 행렬 A_0 및 상기 해시 함수 H 를 상기 공개키로 설정하고, 상기 기저 B_0 를 비밀키로 설정하는 단계

를 포함하는 것을 특징으로 하는 래티스에서의 아이디 기반 브로드캐스트 방법.

청구항 3

제2항에 있어서,

상기 해시 함수 H 는

0과 1로 이루어진 문자열을 행렬 값으로 가지는 $n \times m$ 행렬을 만드는 함수인 것을 특징으로 하는 래티스에서의 아이디 기반 브로드캐스트 방법.

청구항 4

제1항에 있어서,

상기 키 분배 단계는

상기 해시 함수 H 를 이용하여 상기 사용자의 아이디에 대한 행렬 A' 를 생성하는 단계;

상기 랜덤 행렬 A_0 와 상기 아이디에 대한 행렬 A' 의 논리합 행렬 $\bar{A}(A_0 | A')$ 에 대응하는 기저 $\bar{B}$ 를 상기 비밀키로서 생성하는 단계; 및

상기 생성된 비밀키 $\bar{B}$ 를 상기 사용자에게 전송하는 단계

를 포함하는 것을 특징으로 하는 래티스에서의 아이디 기반 브로드캐스트 방법.

청구항 5

제4항에 있어서,

상기 기저 $\bar{B}$ 를 상기 비밀키로서 생성하는 단계는

상기 논리합 행렬 $\bar{A}$ 및 상기 기저 B_0 를 입력 파라미터로 하는 기저 확장 알고리즘을 이용하여 상기 논리합 행렬 $\bar{A}$ 에 대응하는 상기 기저 B_0 를 상기 비밀키로서 생성하는 단계

를 포함하는 것을 특징으로 하는 래티스에서의 아이디 기반 브로드캐스트 방법.

청구항 6

제4항에 있어서,

상기 생성된 비밀키 $\bar{B}$ 를 상기 사용자에게 전송하는 단계는

상기 사용자, 및 상기 공개키 및 비밀키를 생성하는 주체인 키 생성 센터 간에 보안 채널을 형성하는 단계; 및

상기 보안 채널을 통해 상기 비밀키 B_i 를 상기 사용자에게 전송하는 단계

를 포함하는 것을 특징으로 하는 래티스에서의 아이디 기반 브로드캐스트 방법.

청구항 7

제1항에 있어서,

상기 암호화 단계는

상기 평문 전송을 요청한 참여자의 집합을 아이디를 기반으로 하여 구성하는 단계;

상기 공개키를 이용하여 상기 참여자의 집합에 대한 행렬 A 를 생성하는 단계;

상기 행렬 A 의 전치 행렬 A^T , 행렬 난수 및 가우시안 난수를 이용하여 상기 암호문을 생성하는 단계; 및

상기 생성된 암호문을 상기 참여자의 집합에게 브로드캐스트 하는 단계

를 포함하고,

상기 행렬 A 는

$-q/2 \sim q/2$ 범위 내의 랜덤 값을 행렬 값으로 가지는 $n \times k$ 행렬(상기 k 는 $2 \log n$ 이고, 상기 n 은 상기 참여자 집합의 크기)인 것을 특징으로 하는 래티스에서의 아이디 기반 브로드캐스트 방법.

청구항 8

제1항에 있어서,

상기 사용자의 아이디에 대응되는 비밀키를 이용하여 상기 암호문으로부터 상기 평문의 문자열 데이터를 복호화 하는 복호화 단계

를 더 포함하는 것을 특징으로 하는 래티스에서의 아이디 기반 브로드캐스트 방법.

청구항 9

제8항에 있어서,

상기 복호화 단계는

상기 평문 전송을 요청한 참여자의 집합에 대한 행렬 A에 대응되는 기저 B를 생성하는 단계;

상기 기저 B와 상기 암호문을 곱셈 연산하는 단계; 및

상기 곱셈 연산의 결과에 상기 기저 B의 역행렬 B^{-1} 을 곱셈 연산하여 상기 암호문으로부터 상기 평문의 문자열 데이터를 복호화하는 단계

를 포함하는 것을 특징으로 하는 래티스에서의 아이디 기반 브로드캐스트 방법.

청구항 10

제9항에 있어서,

상기 참여자의 집합에 대한 행렬 A에 대응되는 기저 B를 생성하는 단계는

상기 행렬 A 및 비밀키 B 를 입력 파라미터로 하는 기저 확장 알고리즘을 이용하여 상기 행렬 A에 대응하는 상기 기저 B를 상기 사용자의 아이디에 대응되는 비밀키로서 생성하는 단계

를 포함하는 것을 특징으로 하는 래티스에서의 아이디 기반 브로드캐스트 방법.

발명의 설명

기술 분야

[0001]

본 발명의 실시예들은 래티스에서의 브로드캐스트 방법에 관한 것으로, 더욱 상세하게는 사용자의 공개키를 난수 형태가 아닌 아이디 형태로 구성하여 공개키 저장을 위한 공간을 효율적으로 관리할 수 있도록 하는 래티스에서의 아이디 기반 브로드캐스트 방법에 관한 것이다.

배경 기술

[0002]

브로드캐스트 방법은 다수의 정당한 사용자에게 동일한 정보를 정확하고 안전하게 분배하는 환경에서 유용하게 사용될 수 있다. 이에 대한 가장 대표적인 환경은 케이블 TV이며, 이 환경에서 정당한 사용자는 비용을 지불하며, 서비스 제공자는 비용이 지불된 정당한 사용자에게만 콘텐츠를 제공한다. 이러한 기능을 요구하는 환경에 브로드캐스트 방법은 매우 유용하다.

[0003]

브로드캐스트 방법은 1997년 이후 다수의 학자로부터 연구되기 시작하였으며, 기본적으로 이것은 의미론적 안전성을 만족해야 한다. 즉, 정당한 사용자만이 정보를 얻어볼 수 있어야 하며, 그렇지 않은 사용자는 정보를 얻어낼 수 없어야 한다. 추가적으로, 정당한 사용자들은 모두 동일한 정보를 획득해야만 한다. 이를 복호화 일관성이라고 한다.

[0004]

래티스에서의 설계는 지수 연산 등이 요구되지 않아 매우 효율적이며, 양자 컴퓨팅 환경에도 안전할 정도로 안전성이 매우 높다. 이러한 연구의 흐름으로 의미론적 안전성과 복호화 일관성을 두루 만족하는 래티스에서의 브로드캐스트 방법은 공개키가 난수 형태로 존재하며, 이에 따라 공개키의 크기가 매우 크다. 공개키를 난수 형태가 아니라 이메일(e-mail) 주소와 같은 간단한 아이디(ID) 형태로 바꿀 수만 있다면, 공간적인 절약 측면에서 매우 도움이 되며, 따라서 이러한 설계는 반드시 필요하다.

발명의 내용

해결하려는 과제

- [0005] 본 발명의 일 실시예는 래티스에서 사용자의 공개키를 난수 형태가 아닌 아이디 형태로 구성함으로써 의미론적 안전성 및 복호화 일관성을 만족할 뿐만 아니라 공개키 저장을 위한 공간을 효율적으로 관리할 수 있는 래티스에서의 아이디 기반 브로드캐스트 방법을 제공한다.
- [0006] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제(들)로 제한되지 않으며, 언급되지 않은 또 다른 과제(들)는 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

- [0007] 본 발명의 일 실시예에 따른 래티스에서의 아이디 기반 브로드캐스트 방법은 균일 분포를 가지는 랜덤 행렬 A_0 및 해시 함수 H 를 공개키로 설정하고, 상기 랜덤 행렬 A_0 에 대응되는 기저 B_0 를 비밀키로 설정하는 키 설정 단계; 상기 키 설정 단계에서 설정된 상기 공개키 및 상기 비밀키에 기초하여 사용자의 아이디(ID)에 대응되는 비밀키를 생성하고, 상기 생성된 비밀키를 상기 사용자에게 전송하는 키 분배 단계; 및 상기 공개키 및 상기 비밀키와 임의의 난수들을 이용하여 평문의 문자열 데이터를 암호화하여 암호문을 생성하고, 상기 생성된 암호문을 상기 평문 전송을 요청한 참여자에게 브로드캐스트 하는 암호화 단계를 포함한다.
- [0008] 상기 키 설정 단계는 보안 파라미터 n , 차원 $m=O(n \log q)$, 양의 정수 q 를 입력 파라미터로 하는 기저 생성 알고리즘을 이용하여, $-q/2 \sim q/2$ 범위 내의 랜덤 값을 행렬 값으로 가지는 $n \times m$ 행렬 각각을 상기 랜덤 행렬 A_0 및 상기 기저 B_0 로서 생성하는 단계; 상기 기저 생성 알고리즘의 입력 파라미터를 이용하여 상기 해시 함수 H 를 생성하는 단계; 및 상기 랜덤 행렬 A_0 및 상기 해시 함수 H 를 상기 공개키로 설정하고, 상기 기저 B_0 를 비밀키로 설정하는 단계를 포함할 수 있다.
- [0009] 상기 해시 함수 H 는 0과 1로 이루어진 문자열을 행렬 값으로 가지는 $n \times m$ 행렬을 만드는 함수일 수 있다.
- [0010] 상기 키 분배 단계는 상기 해시 함수 H 를 이용하여 상기 사용자의 아이디에 대한 행렬 A' 를 생성하는 단계; 상기 랜덤 행렬 A_0 와 상기 아이디에 대한 행렬 A' 의 논리합 행렬 $\bar{A}(A_0 | A')$ 에 대응하는 기저 $\bar{B}$ 를 상기 비밀키로서 생성하는 단계; 및 상기 생성된 비밀키 $\bar{B}$ 를 상기 사용자에게 전송하는 단계를 포함할 수 있다.
- [0011] 상기 기저 $\bar{B}$ 를 상기 비밀키로서 생성하는 단계는 상기 논리합 행렬 $\bar{A}$ 및 상기 기저 B_0 를 입력 파라미터로 하는 기저 확장 알고리즘을 이용하여 상기 논리합 행렬 $\bar{A}$ 에 대응하는 상기 기저 B_0 를 상기 비밀키로서 생성하는 단계를 포함할 수 있다.
- [0012] 상기 생성된 비밀키 $\bar{B}$ 를 상기 사용자에게 전송하는 단계는 상기 사용자, 및 상기 공개키 및 비밀키를 생성하는 주체인 키 생성 센터 간에 보안 채널을 형성하는 단계; 및 상기 보안 채널을 통해 상기 비밀키 B_1 를 상기 사용자에게 전송하는 단계를 포함할 수 있다.
- [0013] 상기 암호화 단계는 상기 평문 전송을 요청한 참여자의 집합을 아이디를 기반으로 하여 구성하는 단계; 상기 공개키를 이용하여 상기 참여자의 집합에 대한 행렬 A 를 생성하는 단계; 상기 행렬 A 의 전치 행렬 A^T , 행렬 난수 및 가우시안 난수를 이용하여 상기 암호문을 생성하는 단계; 및 상기 생성된 암호문을 상기 참여자의 집합에게 브로드캐스트 하는 단계를 포함하고, 상기 행렬 A 는 $-q/2 \sim q/2$ 범위 내의 랜덤 값을 행렬 값으로 가지는 $n \times k$ 행렬(상기 k 는 $2 \ln m$ 이고, 상기 l 은 상기 참여자 집합의 크기)일 수 있다.
- [0014] 본 발명의 일 실시예에 따른 래티스에서의 아이디 기반 브로드캐스트 방법은 상기 사용자의 아이디에 대응되는 비밀키를 이용하여 상기 암호문으로부터 상기 평문의 문자열 데이터를 복호화하는 복호화 단계를 더 포함할 수

있다.

[0015] 상기 복호화 단계는 상기 평문 전송을 요청한 참여자의 집합에 대한 행렬 A 에 대응되는 기저 B 를 생성하는 단계; 상기 기저 B 와 상기 암호문을 곱셈 연산하는 단계; 및 상기 곱셈 연산의 결과에 상기 기저 B 의 역행렬 B^{-1} 을 곱셈 연산하여 상기 암호문으로부터 상기 평문의 문자열 데이터를 복호화하는 단계를 포함할 수 있다.

[0016] 상기 참여자의 집합에 대한 행렬 A 에 대응되는 기저 B 를 생성하는 단계는 상기 행렬 A 및 비밀키 $\mathbf{B}\mathbf{B}$ 를 입력 파라미터로 하는 기저 확장 알고리즘을 이용하여 상기 행렬 A 에 대응하는 상기 기저 B 를 상기 사용자의 아이디에 대응되는 비밀키로서 생성하는 단계를 포함할 수 있다.

[0017] 기타 실시예들의 구체적인 사항들은 상세한 설명 및 첨부 도면들에 포함되어 있다.

발명의 효과

[0018] 본 발명의 일 실시예에 따르면, 래티스에서 난수 형태인 공개키를 아이디 형태로 변경하여 설계함으로써 의미론적 안전성 및 복호화 일관성을 만족할 뿐만 아니라 공개키 저장을 위한 공간을 효율적으로 관리할 수 있다.

[0019] 따라서, 본 발명의 일 실시예에 따르면 케이블 TV 환경 등 다수의 정당한 사용자가 안전하고 정확하게 정보를 제공받아야만 하는 환경에서 유용하게 사용될 수 있다.

도면의 간단한 설명

[0020] 도 1은 본 발명의 일 실시예에 따른 래티스에서의 아이디 기반 브로드캐스트 방법을 수행하는 동작 주체들(참여자)의 네트워크 구성을 도시한 도면이다.

도 2는 본 발명의 일 실시예에 따른 래티스에서의 아이디 기반 브로드캐스트 방법을 설명하기 위해 도시한 흐름도이다.

도 3은 도 2의 키 설정 단계를 상세히 설명하기 위해 도시한 흐름도이다.

도 4는 도 2의 키 분배 단계를 상세히 설명하기 위해 도시한 흐름도이다.

도 5는 도 2의 암호화 단계를 상세히 설명하기 위해 도시한 흐름도이다.

도 6은 도 2의 복호화 단계를 상세히 설명하기 위해 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0021] 본 발명의 이점 및/또는 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 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 구성요소를 지칭한다.

[0022] 본 발명에서 제안하는 방법을 설계하기 위해 기저 생성 알고리즘과 기저 확장 알고리즘을 사용한다. 상기 두 가지 알고리즘들에서 사용되는 파라미터들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 사용이 가능하다. 이러한 알고리즘들의 간략한 설명은 다음과 같다.

[0023] 먼저, 상기 기저 생성 알고리즘 $GenBasis(1^n, 1^m, q)$ 은 보안 파라미터 n , 차원 $m = O(n \log q)$, 양의 정수 q 를 입력받아서 균일한 분포를 가지는 랜덤 행렬 $A_0 \in \mathbb{Z}_q^{n \times m}$ 와 이에 대응되는 기저 $B_0 \in \mathbb{Z}^{m \times m}$ 를 생성하는 알고리즘

증이다. 여기서 B_0 는 역행렬이 존재하며, 길이는 짧다.

[0024] 다음으로, 상기 기저 확장 알고리즘 $ExtBasis(\overline{A}=A_0|A', B_0)$ 는 균일한 분포를 가지는 랜덤 행렬 $A_0 \in \mathbb{Z}_q^{n \times m}$ 와 이에 대응되는 기저 $B_0 \in \mathbb{Z}^{m \times m}$, 그리고 균일한 분포를 가지는 또 다른 랜덤 행렬 $A' \in \mathbb{Z}_q^{n \times m'}$ 을 입력받아서 $\overline{A}=A_0|A' \in \mathbb{Z}_q^{n \times (m+m')}$ 에 대응되는 기저 $\overline{B} \in \mathbb{Z}^{(m+m') \times (m+m')}$ 를 생성하는 알고리즘이다.

[0025] 본 발명의 일 실시예에 따른 래티스에서의 아이디 기반 브로드캐스트 방법은 위에 설명한 기저 생성 알고리즘과 기저 확장 알고리즘을 사용하며, 세 가지 타입의 참여자가 다음과 같이 존재한다.

[0026] 도 1은 본 발명의 일 실시예에 따른 래티스에서의 아이디 기반 브로드캐스트 방법을 수행하는 동작 주체들(참여자)의 네트워크 구성을 도시한 도면이다.

[0027] 도 1에 도시된 바와 같이, 상기 세 가지 타입의 참여자(100)는 키를 생성해서 분배하는 역할을 수행하는 키 생성 센터(KGC)(110), 서비스 제공자(120), 그리고 다수의 사용자들(130)을 포함하여 구성된다. 여기서, 적용하는 환경에 따라서 상기 키 생성 센터(110)와 상기 서비스 제공자(120)는 동일한 참여자가 역할을 수행할 수도 있다. 이들(110, 120)은 키 설정 단계, 키 분배 단계, 암호화 단계 그리고 복호화 단계를 통해 k비트 문자열 데이터 $d \in \mathbb{Z}_2^k$ 를 브로드캐스트한다. 여기서 $k=2lm$ 이다.

[0028] 이하에서는 첨부된 도면을 참조하여 본 발명의 실시예들을 더욱 구체적으로 설명한다.

[0029] 도 2는 본 발명의 일 실시예에 따른 래티스에서의 아이디 기반 브로드캐스트 방법을 설명하기 위해 도시한 흐름도이다.

[0030] 도 1 및 도 2를 참조하면, 본 발명의 일 실시예에 따른 래티스에서의 아이디 기반 브로드캐스트 방법은 키 설정 단계(210), 키 분배 단계(220), 암호화 단계(230), 및 복호화 단계(240)를 포함하여 구성될 수 있다.

[0031] 먼저, 상기 키 설정 단계(210)에서, 상기 키 생성 센터(110)는 균일 분포를 가지는 랜덤 행렬 A_0 및 해시 함수 H 를 공개키로 설정하고, 상기 랜덤 행렬 A_0 에 대응되는 기저 B_0 를 비밀키로 설정한다.

[0032] 여기서, 상기 랜덤 행렬 A_0 및 상기 랜덤 행렬 A_0 에 대응되는 기저 B_0 는 상기 기저 생성 알고리즘을 이용하여 생성될 수 있으며, 상기 해시 함수 H 는 상기 기저 생성 알고리즘의 입력 파라미터를 이용하여 생성될 수 있다.

[0033] 즉, 상기 키 생성 센터(110)는 상기 기저 생성 알고리즘 $GenBasis(1^n, 1^m, q)$ 을 수행하여 (A_0, B_0) 를 생성하고, 해시 함수 $H: \{0,1\}^* \rightarrow \mathbb{Z}_q^{n \times m}$ 를 선택한다. 상기 키 생성 센터(110)의 공개키는 $pk = \{A_0, H\}$ 이고, 비밀키는 $sk = B_0$ 이다.

[0034] 상기 키 설정 단계(210)에 대해서는 도 3을 참조하여 후술하기로 한다.

[0035] 다음으로, 상기 키 분배 단계(220)에서, 상기 키 생성 센터(110)는 상기 키 설정 단계(210)에서 설정된 상기 공개키 및 상기 비밀키에 기초하여 사용자(130)의 아이디(ID)에 대응되는 비밀키를 생성하고, 상기 생성된 비밀키를 상기 사용자(130)에게 전송한다.

[0036] 여기서, 상기 사용자(130)의 아이디에 대응되는 비밀키는 상기 기저 확장 알고리즘을 이용하여 생성될 수 있다. 상기 키 생성 센터(110)는 상기 생성된 비밀키를 안전한 채널을 통해 상기 사용자(130)에게 전송할 수 있다.

[0037] 즉, 상기 키 생성 센터(110)는 i번째 사용자의 ID ID_i 를 입력으로 받아서 $A'_i = H(ID_i)$ 를 계산한다. 그리고, 상기 키 생성 센터(110)는 상기 기저 확장 알고리즘 $ExtBasis(\overline{A}_i = A_0|A'_i, B_0)$ 을 수행하여 $\overline{B}_i$ 를 생성한다. 그러면, i번째 사용자(130)의 ID ID_i 에 대응되는 비밀키는 $\overline{B}_i$ 이며, 상기 키 생성 센터(110)는 이 비밀키를 안전한 보안 채널(secure channel)을 통해 i번째 사용자(130)에게 전송한다.

[0038] 상기 키 분배 단계(220)에 대한 자세한 설명은 도 4를 참조하여 후술하기로 한다.

- [0039] 다음으로, 상기 암호화 단계(230)에서, 상기 서비스 제공자(120)는 상기 공개키 및 상기 비밀키와 임의의 난수들을 이용하여 평문의 문자열 데이터를 암호화하여 암호문을 생성하고, 상기 생성된 암호문을 상기 평문 전송을 요청한 참여자에게 브로드캐스트 한다.
- [0040] 여기서, 상기 평문 전송을 요청한 참여자는 자신이 정당하다고 판단하는 사용자(130)들의 집합을 의미한다.
- [0041] 즉, 상기 서비스 제공자(120)는 자신이 정당하다고 판단하는 사용자들의 집합을 구성한다. 이를 $L = \{ID_1, \dots, ID_t\}$ 이라 나타낸다. 그리고, 상기 서비스 제공자(120)가 선택한 k비트 문자열 데이터를 $d \in \mathbb{Z}_2^k$ 라고 한다. 상기 서비스 제공자(120)는 $A = [\overline{A_1} | \dots | \overline{A_t}] \in \mathbb{Z}_q^{n \times k}$ 를 계산하고, $c = As + 2x + d \pmod{q}$ 를 계산해서 정당하다고 판단하는 사용자들에게 모두 전송한다. 여기서 $s \xleftarrow{\$} \mathbb{Z}_q^n$ 이고, $\$$ 는 k차원 에리 벡터이다.
- [0042] 상기 암호화 단계(230)에 대해서는 도 5를 참조하여 뒤에서 자세히 살펴보기로 한다.
- [0043] 다음으로, 상기 복호화 단계(240)에서, 상기 사용자(130)는 상기 사용자(130)의 아이디에 대응되는 비밀키를 이용하여 상기 암호문으로부터 상기 평문의 문자열 데이터를 복호화한다.
- [0044] 여기서, 상기 평문의 문자열 데이터에 대한 복호화를 위해 상기 기저 확장 알고리즘이 사용될 수 있다.
- [0045] 즉, i번째 정당한 사용자(130)는 자신의 아이디 ID_i 에 대응되는 비밀키 $\overline{B_i}$ 를 사용하여 상기 서비스 제공자(120)로부터 받은 암호문(c)으로부터 평문의 문자열 데이터(d)를 복호화한다.
- [0046] 이를 위해, 먼저 상기 사용자(130)는 상기 기저 확장 알고리즘 $ExtBasis(A = \overline{A_1} | \dots | \overline{A_t}, \overline{B_i})$ 를 수행하여 $A = [\overline{A_1} | \dots | \overline{A_t}] \in \mathbb{Z}_q^{n \times k}$ 에 대응되는 기저 $B \in \mathbb{Z}^{k \times k}$ 를 계산한다. 그리고, 상기 사용자(130)는 $e = Bc \pmod{q}$ 를 계산한 다음에 $d = B^{-1}e \pmod{2}$ 를 계산하여 상기 서비스 제공자(120)가 선택한 k비트 문자열 데이터 d를 복호화한다.
- [0047] 상기 복호화 단계(240)에 대한 자세한 설명은 도 6을 참조하여 후술하기로 한다.
- [0048] 이와 같이, 본 발명의 일 실시예에서는 래티스에서 난수 형태인 공개키를 아이디 형태로 변경하여 설계함으로써 의미론적 안전성 및 복호화 일관성을 만족할 뿐만 아니라 공개키 저장을 위한 공간을 효율적으로 관리할 수 있다. 따라서, 케이블 TV 환경 등 다수의 정당한 사용자가 안전하고 정확하게 정보를 제공받아야만 하는 환경에서 유용하게 사용될 수 있다.
- [0049] 도 3은 도 2의 키 설정 단계(210)를 상세히 설명하기 위해 도시한 흐름도이다.
- [0050] 도 1 및 도 3을 참조하면, 단계(310)에서 상기 키 생성 센터(110)는 보안 파라미터 n, 차원 $m = O(n \log q)$, 양의 정수 q를 입력 파라미터로 하는 기저 생성 알고리즘을 이용하여, $-q/2 \sim q/2$ 범위 내의 랜덤 값을 행렬 값으로 가지는 $n \times m$ 행렬 각각을 상기 랜덤 행렬 A_0 및 상기 기저 B_0 로서 생성한다.
- [0051] 다음으로, 단계(320)에서 상기 키 생성 센터(110)는 상기 기저 생성 알고리즘의 입력 파라미터를 이용하여 상기 해시 함수 H를 생성한다($H: \{0,1\}^* \rightarrow \mathbb{Z}_q^{n \times m}$).
- [0052] 다음으로, 단계(330)에서 상기 키 생성 센터(110)는 상기 랜덤 행렬 A_0 및 상기 해시 함수 H를 상기 공개키로 설정한다($pk = \{A_0, H\}$).
- [0053] 여기서, 상기 해시 함수 H는 0과 1로 이루어진 문자열을 행렬 값으로 가지는 $n \times m$ 행렬을 만드는 함수일 수 있다. 다만, 상기 해시 함수 H는 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 사용 가능하다.
- [0054] 다음으로, 단계(340)에서 상기 키 생성 센터(110)는 상기 기저 B_0 를 비밀키로 설정한다($sk = B_0$).

- [0055] 도 4는 도 2의 키 분배 단계(220)를 상세히 설명하기 위해 도시한 흐름도이다.
- [0056] 도 1 및 도 4를 참조하면, 단계(410)에서 상기 키 생성 센터(110)는 상기 해시 함수 H를 이용하여 상기 사용자의 아이디에 대한 행렬 A'를 생성한다($A'_i = H(ID_i)$).
- [0057] 다음으로, 단계(420)에서 상기 키 생성 센터(110)는 상기 랜덤 행렬 A_0 와 상기 아이디에 대한 행렬 A'의 논리합 행렬 $\bar{A}(A_0|A')$ 에 대응하는 기저 $\bar{B}$ 를 상기 비밀키로서 생성한다.
- [0058] 이를 위해, 상기 키 생성 센터(110)는 상기 논리합 행렬 $\bar{A}$ 및 상기 기저 B_0 를 입력 파라미터로 하는 기저 확장 알고리즘을 이용할 수 있다. 즉, 상기 키 생성 센터(110)는 상기 기저 확장 알고리즘을 이용하여 상기 논리합 행렬 $\bar{A}$ 에 대응하는 상기 기저 B_0 를 상기 비밀키로서 생성할 수 있다. 따라서, i번째 사용자의 아이디 ID_i 에 대응되는 비밀키는 $\bar{B}_i$ 이 된다.
- [0059] 다음으로, 단계(430)에서 상기 키 생성 센터(110)는 상기 생성된 비밀키 $\bar{B}$ 를 상기 사용자에게 전송한다.
- [0060] 이때, 상기 키 생성 센터(110)는 안전한 데이터 전송을 위해 상기 사용자(130)와 보안 채널을 형성할 수 있다. 상기 키 생성 센터(110)는 상기 보안 채널을 통해 상기 비밀키 B_i 를 상기 사용자(130)에게 전송할 수 있다.
- [0061] 도 5는 도 2의 암호화 단계(230)를 상세히 설명하기 위해 도시한 흐름도이다.
- [0062] 도 1 및 도 5를 참조하면, 단계(510)에서 상기 서비스 제공자(120)는 상기 평문 전송을 요청한 참여자의 집합을 아이디를 기반으로 하여 구성한다. 상기 집합은 $L=\{ID_1, \dots, ID_l\}$ 로 나타낼 수 있으며, 이때 상기 l은 상기 평문 전송을 요청한 참여자의 수, 즉 상기 집합의 크기를 나타낼 수 있다.
- [0063] 다음으로, 단계(520)에서 상기 서비스 제공자(120)는 상기 공개키를 이용하여 상기 참여자의 집합에 대한 행렬 A를 생성한다. 여기서, 상기 행렬 A는 $-q/2 \sim q/2$ 범위 내의 랜덤 값을 행렬 값으로 가지는 $n \times k$ 행렬(상기 k는 $2l \ln m$)일 수 다($A = [\bar{A}_1 | \dots | \bar{A}_l] \in \mathbb{Z}_q^{n \times k}$).
- [0064] 다음으로, 단계(530)에서 상기 서비스 제공자(120)는 상기 행렬 A의 전치 행렬 A^T , 행렬 난수(s) 및 가우시안 난수(x)를 이용하여 상기 암호문(c)을 생성한다($c = As + 2x + d \pmod{q}$, $s \leftarrow \mathbb{Z}_q^n$, x 는 k차원 에러 벡터).
- [0065] 다음으로, 단계(540)에서 상기 서비스 제공자(120)는 상기 생성된 암호문을 상기 참여자의 집합에게 브로드캐스트 한다.
- [0066] 도 6은 도 2의 복호화 단계(240)를 상세히 설명하기 위해 도시한 흐름도이다.
- [0067] 도 1 및 도 6을 참조하면, 단계(610)에서 상기 사용자(130)는 상기 평문 전송을 요청한 참여자의 집합에 대한 행렬 A에 대응되는 기저 B를 생성한다(행렬 $A = [\bar{A}_1 | \dots | \bar{A}_l] \in \mathbb{Z}_q^{n \times k}$, 기저 $B \in \mathbb{Z}^{k \times k}$).
- [0068] 이때, 상기 사용자(130)는 상기 행렬 A 및 비밀키 $\bar{B}$ 를 입력 파라미터로 하는 기저 확장 알고리즘을 이용하여 상기 행렬 A에 대응하는 상기 기저 B를 상기 사용자(130)의 아이디에 대응되는 비밀키로서 생성한다.
- [0069] 다음으로, 단계(620)에서 상기 사용자(130)는 상기 기저 B와 상기 암호문을 곱셈 연산한다($e = Bc \pmod{q}$).
- [0070] 다음으로, 단계(630)에서 상기 사용자(130)는 상기 곱셈 연산의 결과에 상기 기저 B의 역행렬 B^{-1} 을 곱셈 연산하여 상기 암호문(c)으로부터 상기 평문(d)의 문자열 데이터를 복호화한다($d = B^{-1}e \pmod{2}$).

[0071]

본 발명의 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터 판독 가능 매체를 포함한다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크와 같은 자기-광 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0072]

지금까지 본 발명에 따른 구체적인 실시예에 관하여 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서는 여러 가지 변형이 가능함은 물론이다. 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허 청구의 범위뿐 아니라 이 특허 청구의 범위와 균등한 것들에 의해 정해져야 한다.

[0073]

이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 이는 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명 사상은 아래에 기재된 특허청구범위에 의해서만 파악되어야 하고, 이의 균등 또는 등가적 변형 모두는 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0074]

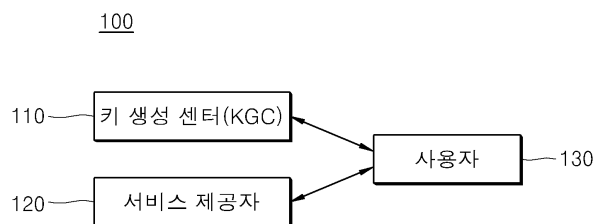
110: 키 생성 센터(KGC)

120: 서비스 제공자

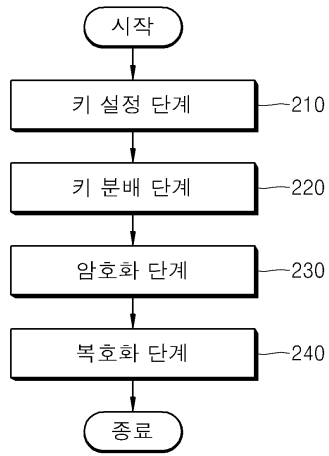
130: 사용자

도면

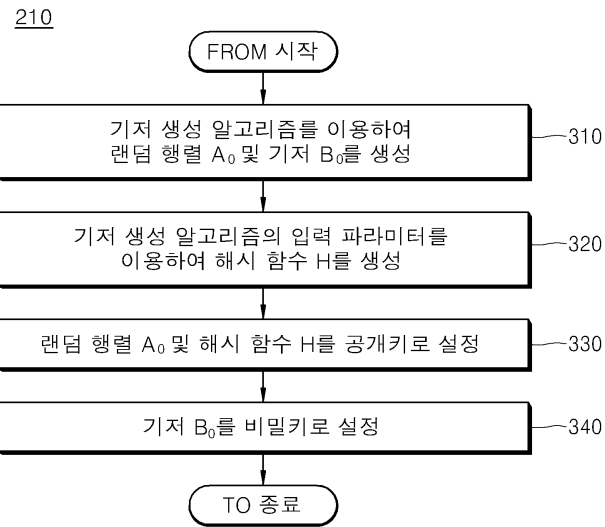
도면1



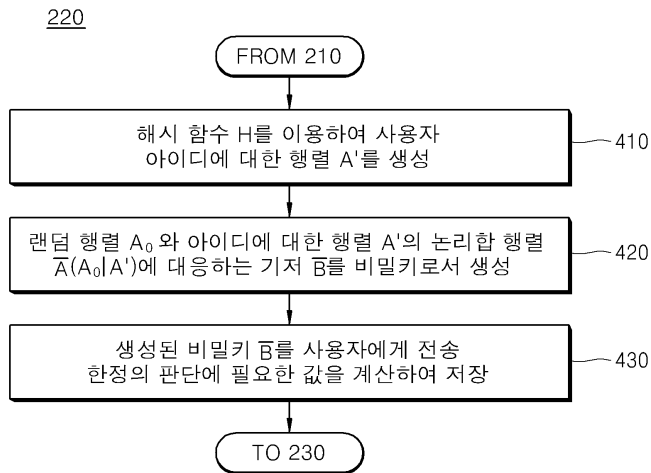
도면2



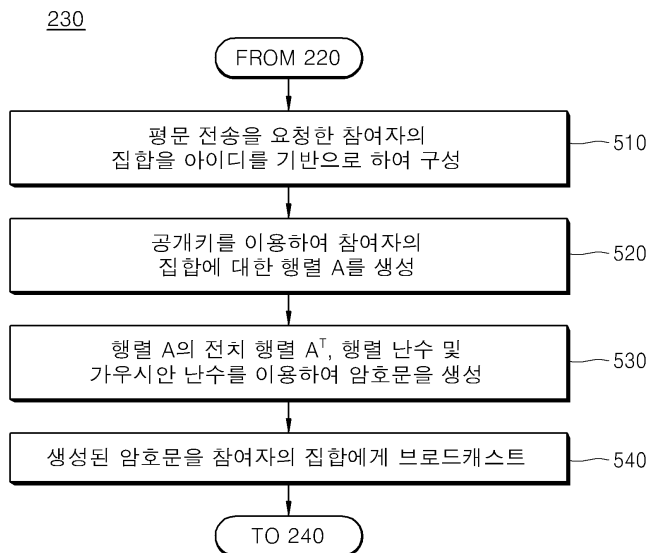
도면3



도면4



도면5



도면6

