(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년06월16일
(11) 등록번호 10-2123435
(24) 등록일자 2020년06월10일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/06* (2006.01)
H04L 9/30 (2006.01)
(52) CPC특허분류
H04L 9/0838 (2013.01)
H04L 9/0643 (2013.01)
(21) 출원번호 10-2019-0100941
(22) 출원일자 2019년08월19일
심사청구일자 2019년08월19일
(56) 선행기술조사문헌
JP2014095847 A*
JP2016517243 A*
KR1020130136555 A*
KR1020150070383 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
이광수
서울특별시 광진구 능동로 209(군자동) 세종대학교 대양AI센터 726호
(74) 대리인
두호특허법인

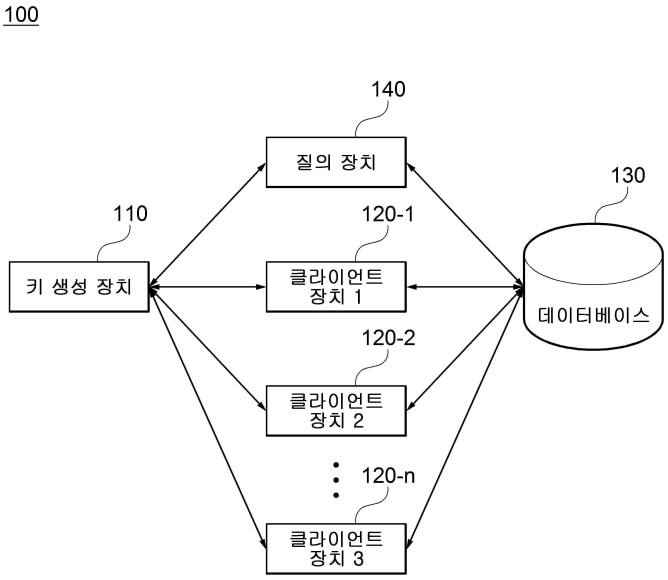
전체 청구항 수 : 총 24 항 심사관 : 양종필

(54) 발명의 명칭 **멀티 클라이언트 환경에서 동치 질의를 지원하는 암호화 방법 및 이를 이용한 장치**

(57) 요 약

멀티 클라이언트 환경에서 암호문들에 대한 동치 질의를 지원하는 암호화 방법 및 장치가 개시된다. 일 실시예에 따른 방법은, 키 생성 장치로부터 사용자 암호키를 획득하는 단계 및 속성 벡터에 대한 라벨(label) 및 상기 사용자 암호키에 기초하여 상기 속성 벡터에 대한 암호문을 생성하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0869 (2013.01)
H04L 9/3033 (2013.01)
H04L 9/3213 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711094110
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보보호핵심원천기술개발사업
연구과제명 (함수암호 1세부) 함수암호 기법 설계·분석 및 구현기술 연구
기 여 율 1/1
주관기관 상명대학교 산학협력단
연구기간 2019.04.01 ~ 2020.01.31

명 세 서

청구범위

청구항 1

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서,

키 생성 장치로부터 사용자 암호키를 획득하는 단계; 및

속성 벡터에 대한 라벨(label) 및 상기 사용자 암호키에 기초하여 상기 속성 벡터에 대한 암호문을 생성하는 단계를 포함하고,

상기 암호문을 생성하는 단계는,

상기 라벨에 대한 해시 값을 생성하는 단계;

상기 속성 벡터에 포함된 하나 이상의 속성 값 각각에 대한 의사 난수(pseudo-random number)를 생성하는 단계; 및

상기 해시 값, 상기 의사 난수 및 상기 사용자 암호키에 기초하여 상기 암호문을 생성하는 단계를 포함하고,

상기 암호문은, 상기 하나 이상의 속성 값 각각에 대한 의사 난수를 상기 해시 값의 지수로 이용하여 산출된 복수의 암호문 원소를 포함하는, 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

청구항 1에 있어서,

상기 사용자 암호키는, 아래의 수학식 1

[수학식 1]

$$EK_i = (z_i, w_{i,1}, w_{i,2}),$$

(이때, i는 사용자 인덱스, EK_i는 사용자 i에 대한 사용자 암호키, z_i는 $Z_p = \{0, 1, \ldots, p-1\}$의 원소, $w_{i,1}$ 및 $w_{i,2}$는 각각 임의의 정수, p는 소수(prime number))

을 만족하고,

상기 의사 난수를 생성하는 단계는, 아래의 수학식 2 및 3

[수학식 2]

$$z_{i,j} = PRF(z_i, j)$$

[수학식 3]

$$f_{i,j} = PRF(z_{i,j}, x_{i,j})$$

(이때, j 는 속성 카테고리 인덱스, PRF()는 의사 랜덤 함수, $x_{i,j}$ 는 상기 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, $f_{i,j}$ 는 상기 속성 값 $x_{i,j}$ 에 대한 의사 난수)

을 이용하여 상기 하나 이상의 속성 값 각각에 대한 의사 난수를 생성하는, 방법.

청구항 5

청구항 4에 있어서,

상기 암호문을 생성하는 단계는, 아래의 수학식 4

[수학식 4]

$$CT_{i,T} = \left(\left\{C_{1,j}^{(i)} = H(T)^{f_{i,j}}\right\}_{j=1}^{\ell}, C_2^{(i)} = H(T)^{w_{i,1}}, C_3^{(i)} = H(T)^{w_{i,2}}\right)$$

(이때, $CT_{i,T}$ 는 상기 암호문, ℓ 은 상기 속성 벡터에 포함된 속성 카테고리의 총 개수, T는 상기 라벨, $H(T)$ 는 상기 해시 값)

을 이용하여 상기 암호문을 생성하는, 방법.

청구항 6

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서,

복수의 사용자 각각에 대한 사용자 암호키 및 마스터 비밀키를 생성하는 단계;

상기 생성된 사용자 암호키를 상기 복수의 사용자 각각의 클라이언트 장치로 제공하는 단계;

질의 장치로부터 복수의 질의 벡터를 포함하는 질의 벡터 집합을 수신하는 단계;

상기 질의 벡터 집합 및 상기 마스터 비밀키를 이용하여 상기 질의 벡터 집합에 대한 토큰을 생성하는 단계; 및

상기 생성된 토큰을 상기 질의 장치로 제공하는 단계를 포함하는, 방법.

청구항 7

청구항 6에 있어서,

상기 토큰을 생성하는 단계는,

상기 질의 벡터 집합에 대한 의사 난수(pseudo-random number)를 생성하는 단계; 및

상기 의사 난수 및 상기 마스터 비밀키를 이용하여 상기 토큰을 생성하는 단계를 포함하는, 방법.

청구항 8

청구항 7에 있어서,

상기 사용자 암호키는 아래의 수학식 1

[수학식 1]

$$EK_i = (z_i, w_{i,1}, w_{i,2}),$$

(이때, i는 사용자 인덱스, EK_i는 사용자 i에 대한 사용자 암호키, z_i는 $Z_p = \{0, 1, \ldots, p-1\}$의 원소, $w_{i,1}$ 및 $w_{i,2}$는 각각 임의의 정수, p는 소수(prime number))을 만족하고,

상기 의사 난수를 생성하는 단계는, 아래의 수학식 2 및 3

[수학식 2]

$$z_{i,j} = PRF(z_i, j)$$

[수학식 3]

$$f_Y = \sum_{i=1}^{n} \sum_{j \in S_i} PRF(z_{i,j}, y_{i,j})$$

(이때, j는 속성 카테고리 인덱스, PRF()는 의사 랜덤 함수, f_Y는 상기 질의 벡터 집합에 대한 의사 난수, $y_{i,j}$는 질의 벡터 $\vec{y}_i$에 포함된 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, S_i는 상기 질의 벡터 $\vec{y}_i$에 포함된 하나 이상의 속성 값들 중 와일드 카드(wild card) 속성 값을 제외한 나머지 속성 값들 각각에 대한 속성 카테고리 인덱스들의 집합)

을 이용하여 상기 의사 난수를 생성하는, 방법.

청구항 9

청구항 8에 있어서,

상기 마스터 비밀키를 생성하는 단계는 아래의 수학식 4

[수학식 4]

$$MK = \left(\{z_i\}_{i=1}^{n}, \hat{v}, \hat{w}_1 = \hat{v}^{\sum_{i=1}^{n} w_{i,1}}, \hat{w}_2 = \hat{v}^{\sum_{i=1}^{n} w_{i,2}}\right)$$

(이때, MK는 상기 마스터 비밀키, n은 상기 복수의 사용자의 총수, $\hat{v}$는 위수가 p인 순환군(cyclic group) $\hat{G}$의 원소)

를 이용하여 상기 마스터 비밀키를 생성하고,

상기 토큰을 생성하는 단계는, 아래의 수학식 5

[수학식 5]

$$TK_Y = \left(K_0 = \hat{v}^{fy \cdot r_1} \cdot \hat{w}_1^{r_2} \cdot \hat{w}_2^{r_3}, K_1 = \hat{v}^{-r_1}, K_2 = \hat{v}^{-r_2}, K_3 = \hat{v}^{-r_3}\right)$$

(이때, TK_Y는 상기 질의 벡터 집합에 대한 토큰, r_1, r_2 및 r_3는 각각 Z_p의 원소)

를 이용하여 상기 토큰을 생성하는, 방법.

청구항 10

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서,

복수의 질의 벡터를 포함하는 질의 벡터 집합을 생성하는 단계;

키 생성 장치로부터 상기 질의 벡터 집합에 대한 토큰을 획득하는 단계; 및

상이한 사용자 암호키를 이용하여 암호화된 복수의 속성 벡터 각각에 대한 암호문, 상기 복수의 속성 벡터에 대한 라벨(label) 및 상기 토큰을 이용하여, 상기 복수의 속성 벡터를 포함하는 속성 벡터 집합과 상기 질의 벡터 집합 사이의 동치 관계 성립 여부를 판단하는 단계를 포함하는 방법.

청구항 11

청구항 10에 있어서,

상기 복수의 속성 벡터 각각에 대한 암호문은, 상기 라벨에 대한 해시 값, 상기 복수의 속성 벡터 각각에 포함된 하나 이상의 속성 값 각각에 대한 제1 의사 난수(pseudo-random number) 및 상기 사용자 암호키를 이용하여 생성되고,

상기 토큰은, 상기 질의 벡터 집합에 대한 제2 의사 난수 및 마스터 비밀키를 이용하여 생성되는 방법.

청구항 12

청구항 11에 있어서,

상기 사용자 암호키는 아래의 수학식 1

[수학식 1]

$$EK_i = \left(z_i, w_{i,1}, w_{i,2}\right),$$

(i는 사용자 인덱스, EK_i는 사용자 i에 대한 사용자 암호키, z_i는 $Z_p = \{0, 1, \ldots, p-1\}$의 원소, $w_{i,1}$ 및 $w_{i,2}$는 각각 임의의 정수, p는 소수(prime number))

을 만족하고,

상기 제1 의사 난수는, 아래의 수학식 2

[수학식 2]

$$f_{i,j} = PRF(z_{i,j}, x_{i,j})$$

(이때, j 는 속성 카테고리 인덱스, PRF()는 의사 랜덤 함수, $x_{i,j}$ 는 사용자 i의 사용자 암호키를 이용하여 암호화된 속성 벡터 $\vec{x}_i$ 에 포함된 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, $f_{i,j}$ 는 상기 속성 값 $x_{i,j}$ 에 대한 제1 의사 난수)

을 이용하여 생성되고,

상기 제2 의사 난수는, 아래의 수학식 3

[수학식 3]

$$f_Y = \sum_{i=1}^{n} \sum_{j \in S_i} PRF(z_{i,j}, y_{i,j})$$

(이때, f_Y 는 상기 질의 벡터 집합에 대한 제2 의사 난수, $y_{i,j}$ 는 상기 속성 벡터 $\vec{x}_i$ 에 대한 질의 벡터 $\vec{y}_i$ 에 포함된 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, S_i는 상기 질의 벡터 $\vec{y}_i$ 에 포함된 하나 이상의 속성 값 중 와일드 카드(wild card) 속성 값을 제외한 나머지 속성 값들 각각에 대한 속성 카테고리 인덱스들의 집합)을 이용하여 생성되며,

상기 $z_{i,j}$ 는 아래의 수학식 4

[수학식 4]

$$z_{i,j} = PRF(z_i, j)$$

를 이용하여 생성되는 방법.

청구항 13

청구항 12에 있어서,

상기 마스터 비밀키는 아래의 수학식 5

[수학식 5]

$$MK = \left(\{z_i\}_{i=1}^{n}, \hat{v}, \hat{w}_1 = \hat{v}^{\sum_{i=1}^{n} w_{i,1}}, \hat{w}_2 = \hat{v}^{\sum_{i=1}^{n} w_{i,2}}\right)$$

(이때, MK는 상기 마스터 비밀키, n은 상기 복수의 사용자의 수, $\hat{v}$ 는 위수가 p인 순환군(cyclic group) $\hat{G}$ 의 원소)

를 만족하고,

상기 암호문은, 아래의 수학식 6

[수학식 6]

$$CT_{i,T} = \left(\left\{C_{1,j}^{(i)} = H(T)^{f_{i,j}}\right\}_{j=1}^{\ell}, C_2^{(i)} = H(T)^{w_{i1}}, C_3^{(i)} = H(T)^{w_{i2}}\right)$$

(이때, $CT_{i,T}$는 상기 암호문, ℓ은 상기 속성 벡터에 포함된 속성 카테고리의 총 개수, T는 상기 라벨, $H(T)$는 상기 해시 값)

을 만족하고,

상기 토큰은, 아래의 수학식 7

[수학식 7]

$$TK_Y = \left(K_0 = \hat{v}^{fy \cdot r_1} \cdot \hat{w}_1^{r_2} \cdot \hat{w}_2^{r_3}, K_1 = \hat{v}^{-r_1}, K_2 = \hat{v}^{-r_2}, K_3 = \hat{v}^{-r_3}\right)$$

(이때, TK_Y는 상기 토큰, r_1, r_2 및 r_3는 각각 Z_p의 원소)

을 만족하는, 방법.

청구항 14

청구항 13에 있어서,

상기 판단하는 단계는, 아래의 수학식 8

[수학식 8]

$$e(H(T), K_0) \cdot e\left(\prod_{i=1}^{n}\prod_{j \in S_i} C_{1,j}^{(i)}, K_1\right) \cdot e\left(\prod_{i=1}^{n} C_2^{(i)}, K_2\right) \cdot e\left(\prod_{i=1}^{n} C_3^{(i)}, K_3\right) = 1$$

(이때, e는 $e: G \times \hat{G} \rightarrow G_T$를 만족하는 겹선형 함수(bilinear map), G, $\hat{G}$ 및 G_T는 위수(order)가 소수 p인 순환군(cyclic group))

이 만족되는 경우, 상기 동치 관계가 성립하는 것으로 판단하는, 방법.

청구항 15

하나 이상의 프로세서;

메모리; 및

하나 이상의 프로그램을 포함하는 장치로서,

상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며,

상기 프로그램은,

키 생성 장치로부터 사용자 암호키를 획득하는 단계; 및

속성 벡터에 대한 라벨(label) 및 상기 사용자 암호키에 기초하여 상기 속성 벡터에 대한 암호문을 생성하는 단계를 실행하기 위한 명령어들을 포함하고,

상기 암호문을 생성하는 단계는,

상기 라벨에 대한 해시 값을 생성하는 단계;

상기 속성 벡터에 포함된 하나 이상의 속성 값 각각에 대한 의사 난수(pseudo-random number)를 생성하는 단계; 및

상기 해시 값, 상기 의사 난수 및 상기 사용자 암호키에 기초하여 상기 암호문을 생성하는 단계를 포함하고,

상기 암호문은, 상기 하나 이상의 속성 값 각각에 대한 의사 난수를 상기 해시 값의 지수로 이용하여 산출된 복수의 암호문 원소를 포함하는, 장치.

청구항 16

삭제

청구항 17

삭제

청구항 18

청구항 15에 있어서,

상기 사용자 암호키는, 아래의 수학식 1

[수학식 1]

$$EK_i = (z_i, w_{i,1}, w_{i,2}),$$

(이때, i는 사용자 인덱스, EK_i는 사용자 i에 대한 사용자 암호키, z_i는 $Z_p = \{0, 1, \ldots, p-1\}$의 원소, $w_{i,1}$ 및 $w_{i,2}$는 각각 임의의 정수, p는 소수(prime number)을 만족하고,

상기 의사 난수를 생성하는 단계는, 아래의 수학식 2 및 3

[수학식 2]

$$z_{i,j} = PRF(z_i, j)$$

[수학식 3]

$$f_{i,j} = PRF(z_{i,j}, x_{i,j})$$

(이때, j는 속성 카테고리 인덱스, PRF()는 의사 랜덤 함수, $x_{i,j}$는 상기 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, $f_{i,j}$는 상기 속성 값 $x_{i,j}$에 대한 의사 난수)

을 이용하여 상기 하나 이상의 속성 값 각각에 대한 의사 난수를 생성하는, 장치.

청구항 19

청구항 18에 있어서,

상기 암호문을 생성하는 단계는, 아래의 수학식 4

[수학식 4]

$$CT_{i,T} = \left(\left\{C_{1,j}^{(i)} = H(T)^{f_{i,j}}\right\}_{j=1}^{\ell}, C_2^{(i)} = H(T)^{w_{i,1}}, C_3^{(i)} = H(T)^{w_{i,2}}\right)$$

(이때, $CT_{i,T}$는 상기 암호문, ℓ은 상기 속성 벡터에 포함된 속성 카테고리의 총 개수, T는 상기 라벨, $H(T)$는 상기 해시 값)

을 이용하여 상기 암호문을 생성하는, 장치.

청구항 20

하나 이상의 프로세서;

메모리; 및

하나 이상의 프로그램을 포함하는 장치로서,

상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며,

상기 프로그램은,

복수의 사용자 각각에 대한 사용자 암호키 및 마스터 비밀키를 생성하는 단계;

상기 생성된 사용자 암호키를 상기 복수의 사용자 각각의 클라이언트 장치로 제공하는 단계;

질의 장치로부터 복수의 질의 벡터를 포함하는 질의 벡터 집합을 수신하는 단계;

상기 질의 벡터 집합 및 상기 마스터 비밀키를 이용하여 상기 질의 벡터 집합에 대한 토큰을 생성하는 단계; 및

상기 생성된 토큰을 상기 질의 장치로 제공하는 단계를 실행하기 위한 명령어들을 포함하는, 장치.

청구항 21

청구항 20에 있어서,

상기 토큰을 생성하는 단계는,

상기 질의 벡터 집합에 대한 의사 난수(pseudo-random number)를 생성하는 단계; 및

상기 의사 난수 및 상기 마스터 비밀키를 이용하여 상기 토큰을 생성하는 단계를 포함하는, 장치.

청구항 22

청구항 21에 있어서,

상기 사용자 암호키는 아래의 수학식 1

[수학식 1]

$$EK_i = (z_i, w_{i,1}, w_{i,2}),$$

(이때, i는 사용자 인덱스, EK_i는 사용자 i에 대한 사용자 암호키, z_i는 $Z_p = \{0, 1, \ldots, p-1\}$의 원소, $w_{i,1}$

$w_{i,2}$

및 는 각각 임의의 정수, p는 소수(prime number))을 만족하고,

상기 의사 난수를 생성하는 단계는, 아래의 수학식 2 및 3

[수학식 2]

$$z_{i,j} = PRF(z_i, j)$$

[수학식 3]

$$f_Y = \sum_{i=1}^{n} \sum_{j \in S_i} PRF(z_{i,j}, y_{i,j})$$

j f_Y

(이때, 는 속성 카테고리 인덱스, PRF()는 의사 랜덤 함수, 는 상기 질의 벡터 집합에 대한 의사 난수,

$y_{i,j}$ $\vec{y}_i$ $\vec{y}_i$

는 질의 벡터 에 포함된 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, S_i는 상기 질의 벡터

에 포함된 하나 이상의 속성 값들 중 와일드 카드(wild card) 속성 값을 제외한 나머지 속성 값들 각각에 대한 속성 카테고리 인덱스들의 집합)

을 이용하여 상기 의사 난수를 생성하는, 장치.

청구항 23

청구항 22에 있어서,

상기 마스터 비밀키를 생성하는 단계는 아래의 수학식 4

[수학식 4]

$$MK = \left(\{z_i\}_{i=1}^{n}, \hat{v}, \hat{w}_1 = \hat{v}^{\sum_{i=1}^{n} w_{i,1}}, \hat{w}_2 = \hat{v}^{\sum_{i=1}^{n} w_{i,2}}\right)$$

$\hat{v}$ $\hat{G}$

(이때, MK는 상기 마스터 비밀키, n은 상기 복수의 사용자의 총수, 는 위수가 p인 순환군(cyclic group)

의 원소)

를 이용하여 상기 마스터 비밀키를 생성하고,

상기 토큰을 생성하는 단계는, 아래의 수학식 5

[수학식 5]

$$TK_Y = \left(K_0 = \hat{v}^{f_Y \cdot r_1} \cdot \hat{w}_1^{r_2} \cdot \hat{w}_2^{r_3}, K_1 = \hat{v}^{-r_1}, K_2 = \hat{v}^{-r_2}, K_3 = \hat{v}^{-r_3}\right)$$

TK_Y r_1 r_2 r_3 Z_p

(이때, 는 상기 질의 벡터 집합에 대한 토큰, , 및 는 각각 의 원소)

를 이용하여 상기 토큰을 생성하는, 장치.

청구항 24

하나 이상의 프로세서;

메모리; 및

하나 이상의 프로그램을 포함하는 장치로서,

상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며,

상기 프로그램은,

복수의 질의 벡터를 포함하는 질의 벡터 집합을 생성하는 단계;

키 생성 장치로부터 상기 질의 벡터 집합에 대한 토큰을 획득하는 단계; 및

상이한 사용자 암호키를 이용하여 암호화된 복수의 속성 벡터 각각에 대한 암호문, 상기 복수의 속성 벡터에 대한 라벨(label) 및 상기 토큰을 이용하여, 상기 복수의 속성 벡터를 포함하는 속성 벡터 집합과 상기 질의 벡터 집합 사이의 동치 관계 성립 여부를 판단하는 단계를 실행하기 위한 명령어들을 포함하는, 장치.

청구항 25

청구항 24에 있어서,

상기 복수의 속성 벡터 각각에 대한 암호문은, 상기 라벨에 대한 해시 값, 상기 복수의 속성 벡터 각각에 포함된 하나 이상의 속성 값 각각에 대한 제1 의사 난수(pseudo-random number) 및 상기 사용자 암호키를 이용하여 생성되고,

상기 토큰은, 상기 질의 벡터 집합에 대한 제2 의사 난수 및 마스터 비밀키를 이용하여 생성되는 장치.

청구항 26

청구항 25에 있어서,

상기 사용자 암호키는 아래의 수학식 1

[수학식 1]

$$EK_i = (z_i, w_{i,1}, w_{i,2}),$$

(i 는 사용자 인덱스, EK_i 는 사용자 i에 대한 사용자 암호키, z_i 는 $Z_p = \{0, 1, \ldots, p-1\}$ 의 원소, $w_{i,1}$ 및 $w_{i,2}$ 는 각각 임의의 정수, p는 소수(prime number))을 만족하고,

상기 제1 의사 난수는, 아래의 수학식 2

[수학식 2]

$$f_{i,j} = PRF(z_{i,j}, x_{i,j})$$

(이때, j 는 속성 카테고리 인덱스, PRF()는 의사 랜덤 함수, $x_{i,j}$ 는 사용자 i의 사용자 암호키를 이용하여 암호화된 속성 벡터 $\vec{x}_i$ 에 포함된 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, $f_{i,j}$ 는 상기 속성 값 $x_{i,j}$ 에 대한 제1 의사 난수)

을 이용하여 생성되고,

상기 제2 의사 난수는, 아래의 수학식 3

[수학식 3]

$$f_Y = \sum_{i=1}^{n} \sum_{j \in S_i} PRF(z_{i,j}, y_{i,j})$$

(이때, f_Y 는 상기 질의 벡터 집합에 대한 제2 의사 난수, $y_{i,j}$ 는 상기 속성 벡터 $\vec{x}_i$ 에 대한 질의 벡터 $\vec{y}_i$ 에 포함된 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, S_i는 상기 질의 벡터 $\vec{y}_i$ 에 포함된 하나 이상의 속성 값 중 와일드 카드(wild card) 속성 값을 제외한 나머지 속성 값들 각각에 대한 속성 카테고리 인덱스들의 집합)을 이용하여 생성되며,

상기 $z_{i,j}$ 는 아래의 수학식 4

[수학식 4]

$$z_{i,j} = PRF(z_i, j)$$

를 이용하여 생성되는 장치.

청구항 27

청구항 26에 있어서,

상기 마스터 비밀키는 아래의 수학식 5

[수학식 5]

$$MK = \left(\{z_i\}_{i=1}^{n}, \hat{v}, \hat{w}_1 = \hat{v}^{\sum_{i=1}^{n} w_{i,1}}, \hat{w}_2 = \hat{v}^{\sum_{i=1}^{n} w_{i,2}}\right)$$

(이때, MK는 상기 마스터 비밀키, n은 상기 복수의 사용자의 수, $\hat{v}$ 는 위수가 p인 순환군(cyclic group) $\hat{G}$ 의 원소)

를 만족하고,

상기 암호문은, 아래의 수학식 6

[수학식 6]

$$CT_{i,T} = \left(\left\{C_{1,j}^{(i)} = H(T)^{f_{i,j}}\right\}_{j=1}^{\ell}, C_2^{(i)} = H(T)^{w_{i,1}}, C_3^{(i)} = H(T)^{w_{i,2}}\right)$$

(이때, $CT_{i,T}$ 는 상기 암호문, ℓ 은 상기 속성 벡터에 포함된 속성 카테고리의 총 개수, T는 상기 라벨, $H(T)$ 는 상기 해시 값)

을 만족하고,

상기 토큰은, 아래의 수학식 7

[수학식 7]

$$TK_Y = \left(K_0 = \hat{v}^{fy \cdot r_1} \cdot \hat{w}_1^{r_2} \cdot \hat{w}_2^{r_3}, K_1 = \hat{v}^{-r_1}, K_2 = \hat{v}^{-r_2}, K_3 = \hat{v}^{-r_3}\right)$$

(이때, TK_Y는 상기 토큰, r_1, r_2 및 r_3는 각각 Z_p의 원소)

을 만족하는, 장치.

청구항 28

청구항 27에 있어서,

상기 판단하는 단계는, 아래의 수학식 8

[수학식 8]

$$e(H(T), K_0) \cdot e\left(\prod_{i=1}^{n} \prod_{j \in S_i} C_{1,j}^{(i)}, K_1\right) \cdot e\left(\prod_{i=1}^{n} C_2^{(i)}, K_2\right) \cdot e\left(\prod_{i=1}^{n} C_3^{(i)}, K_3\right) = 1$$

$e: G \times \hat{G} \rightarrow G_T$ G $\hat{G}$ G_T

(이때, e는 를 만족하는 겹선형 함수(bilinear map), , 및 는 위수(order)가 소수 p인 순환군(cyclic group))

이 만족되는 경우, 상기 동치 관계가 성립하는 것으로 판단하는, 장치.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 암호화 기술과 관련된다.

배 경 기 술

[0002] 술어-기반 암호(Predicate Encryption)는 암호화된 메시지의 속성과 속성 벡터 간의 동치 연산을 가능하게 하는 비밀키 암호 기술이다. 기존 술어-기반 암호 기법들은 다수의 클라이언트가 생성한 다수의 암호문들을 모두 한 번에 비교하기가 어려웠다. 일부 다수 술어-기반 암호 기법은 다수의 클라이언트가 생성한 다수의 암호문에 대한 비교를 지원했으나 다수 암호문에 대한 질의(또는 복호화) 연산을 수행하는 과정이 처리하는 암호문의 개수에 선형적으로 늘어나는 단점을 가져서 비효율적이었다.

선행기술문헌

특허문헌

[0003] (특허문헌 0001) 대한민국 등록특허공보 제10-1695361호 (2017. 01. 11. 공고)

발명의 내용

해결하려는 과제

[0004] 본 발명의 실시예들은 멀티 클라이언트 환경에서 동치 질의를 지원하는 암호화 방법 및 이를 이용한 장치를 제공하기 위한 것이다.

과제의 해결 수단

[0005] 본 발명의 일 실시예에 따른 방법은, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서, 키 생성 장치로부터 사용자 암호키를 획득하는 단계; 및 속성 벡터에 대한 라벨(label) 및 상기 사용자 암호키에 기초하여 상기 속성 벡터에 대한 암호문을 생성하는 단계를 포함한다.

[0006] 상기 암호문을 생성하는 단계는, 상기 라벨에 대한 해시 값을 생성하는 단계;

[0007] 상기 속성 벡터에 포함된 하나 이상의 속성 값 각각에 대한 의사 난수(pseudo-random number)를 생성하는 단계; 및 상기 해시 값, 상기 의사 난수 및 상기 사용자 암호키에 기초하여 상기 암호문을 생성하는 단계를 포함할 수 있다.

[0008] 상기 암호문은, 상기 하나 이상의 속성 값 각각에 대한 의사 난수를 상기 해시 값의 지수로 이용하여 산출된 복수의 암호문 원소를 포함할 수 있다.

[0009] 상기 사용자 암호키는, 아래의 수학식 1

[0010] [수학식 1]

$$EK_i = (z_i, w_{i,1}, w_{i,2}),$$

[0011]

[0012] (이때, i는 사용자 인덱스, EK_i는 사용자 i에 대한 사용자 암호키, z_i는 $Z_p = \{0, 1, \ldots, p-1\}$의 원소, $w_{i,1}$ 및 $w_{i,2}$는 각각 임의의 정수, p는 소수(prime number)을 만족하고, 상기 의사 난수를 생성하는 단계는, 아래의 수학식 2 및 3

[0013] [수학식 2]

$$z_{i,j} = PRF(z_i, j)$$

[0014]

[0015] [수학식 3]

$$f_{i,j} = PRF(z_{i,j}, x_{i,j})$$

[0016]

[0017] (이때, j는 속성 카테고리 인덱스, PRF()는 의사 랜덤 함수, $x_{i,j}$는 상기 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, $f_{i,j}$는 상기 속성 값 $x_{i,j}$에 대한 의사 난수)을 이용하여 상기 하나 이상의 속성 값 각각에 대한 의사 난수를 생성할 수 있다.

[0018] 상기 암호문을 생성하는 단계는, 아래의 수학식 4

[0019] [수학식 4]

$$CT_{i,T} = \left(\left\{ C_{1,j}^{(i)} = H(T)^{f_{i,j}} \right\}_{j=1}^{\ell}, C_2^{(i)} = H(T)^{w_{i,1}}, C_3^{(i)} = H(T)^{w_{i,2}} \right)$$

[0020]

[0021] (이때, $CT_{i,T}$는 상기 암호문, ℓ은 상기 속성 벡터에 포함된 속성 카테고리의 총 개수, T는 상기 라벨, $H(T)$는 상기 해시 값)을 이용하여 상기 암호문을 생성할 수 있다.

[0022] 본 발명의 일 실시예에 따른 방법은, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서, 복수의 사용자 각각에 대한 사용자 암호키 및 마스터 비밀키를 생성하는 단계; 상기 생성된 사용자 암호키를 상기 복수의 사용

자 각각의 클라이언트 장치로 제공하는 단계; 질의 장치로부터 복수의 질의 벡터를 포함하는 질의 벡터 집합을 수신하는 단계; 상기 질의 벡터 집합 및 상기 마스터 비밀키를 이용하여 상기 질의 벡터 집합에 대한 토큰을 생성하는 단계; 및 상기 생성된 토큰을 상기 질의 장치로 제공하는 단계를 포함한다.

[0023] 상기 토큰을 생성하는 단계는, 상기 질의 벡터 집합에 대한 의사 난수(pseudo-random number)를 생성하는 단계; 및 상기 의사 난수 및 상기 마스터 비밀키를 이용하여 상기 토큰을 생성하는 단계를 포함할 수 있다.

[0024] 상기 사용자 암호키는 아래의 수학식 1

[0025] [수학식 1]

$$EK_i = (z_i, w_{i,1}, w_{i,2}),$$

[0026]

[0027] (이때, i는 사용자 인덱스, EK_i는 사용자 i에 대한 사용자 암호키, z_i는 $Z_p = \{0, 1, \ldots, p-1\}$의 원소, $w_{i,1}$ 및 $w_{i,2}$는 각각 임의의 정수, p는 소수(prime number))을 만족하고, 상기 의사 난수를 생성하는 단계는, 아래의 수학식 2 및 3

[0028] [수학식 2]

$$z_{i,j} = PRF(z_i, j)$$

[0029]

[0030] [수학식 3]

$$f_Y = \sum_{i=1}^{n} \sum_{j \in S_i} PRF(z_{i,j}, y_{i,j})$$

[0031]

[0032] (이때, j는 속성 카테고리 인덱스, PRF()는 의사 랜덤 함수, f_Y는 상기 질의 벡터 집합에 대한 토큰, $y_{i,j}$는 질의 벡터 i에 포함된 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, S_i는 상기 질의 벡터 i에 포함된 하나 이상의 속성 값들 중 와일드 카드(wild card) 속성 값을 제외한 나머지 속성 값들 각각에 대한 속성 카테고리 인덱스들의 집합)을 이용하여 상기 의사 난수를 생성할 수 있다.

[0033] 상기 마스터 비밀키를 생성하는 단계는 아래의 수학식 4

[0034] [수학식 4]

$$MK = \left(\{z_i\}_{i=1}^{n}, \hat{v}, \hat{w}_1 = \hat{v}^{\sum_{i=1}^{n} w_{i,1}}, \hat{w}_2 = \hat{v}^{\sum_{i=1}^{n} w_{i,2}}\right)$$

[0035]

[0036] (이때, MK는 상기 마스터 비밀키, n은 상기 복수의 사용자의 총수, $\hat{v}$는 위수가 p인 순환군(cyclic group) $\hat{G}$의 원소)를 이용하여 상기 마스터 비밀키를 생성하고, 상기 토큰을 생성하는 단계는, 아래의 수학식 5

[0037] [수학식 5]

$$TK_Y = \left(K_0 = \hat{v}^{f_Y \cdot r_1} \cdot \hat{w}_1^{r_2} \cdot \hat{w}_2^{r_3}, K_1 = \hat{v}^{-r_1}, K_2 = \hat{v}^{-r_2}, K_3 = \hat{v}^{-r_3}\right)$$

[0038]

[0039] (이때, TK_Y는 상기 질의 벡터 집합에 대한 토큰, r_1, r_2 및 r_3는 각각 Z_p의 원소)를 이용하여 상기 토큰을 생성할 수 있다.

[0040] 본 발명의 일 실시예에 따른 방법은, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서, 복수의 질의 벡

터를 포함하는 질의 벡터 집합을 생성하는 단계; 키 생성 장치로부터 상기 질의 벡터 집합에 대한 토큰을 획득하는 단계; 및 상이한 사용자 암호키를 이용하여 암호화된 복수의 속성 벡터 각각에 대한 암호문, 상기 복수의 속성 벡터에 대한 라벨(label) 및 상기 토큰을 이용하여, 상기 복수의 속성 벡터를 포함하는 속성 벡터 집합과 상기 질의 벡터 집합 사이의 동치 관계 성립 여부를 판단하는 단계를 포함한다.

[0041] 상기 복수의 속성 벡터 각각에 대한 암호문은, 상기 라벨에 대한 해시 값, 상기 복수의 속성 벡터 각각에 포함된 하나 이상의 속성 값 각각에 대한 제1 의사 난수(pseudo-random number) 및 상기 사용자 암호키를 이용하여 생성되고, 상기 토큰은, 상기 질의 벡터 집합에 대한 제2 의사 난수 및 상기 마스터 비밀키를 이용하여 생성될 수 있다.

[0042] 상기 사용자 암호키는 아래의 수학식 1

[0043] [수학식 1]

$$EK_i = (z_i, w_{i,1}, w_{i,2}),$$

[0044]

[0045] (i 는 사용자 인덱스, EK_i 는 사용자 i에 대한 사용자 암호키, z_i 는 $Z_p = \{0, 1, \ldots, p-1\}$ 의 원소, $w_{i,1}$ 및 $w_{i,2}$ 는 각각 임의의 정수, p는 소수(prime number))을 만족하고, 상기 제1 의사 난수는, 아래의 수학식 2

[0046] [수학식 2]

$$f_{i,j} = PRF(z_{i,j}, x_{i,j})$$

[0047]

[0048] (이때, j 는 속성 카테고리 인덱스, PRF()는 의사 랜덤 함수, $x_{i,j}$ 는 사용자 i의 사용자 암호키를 이용하여 암호화된 속성 벡터 $\vec{x}_i$ 에 포함된 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, $f_{i,j}$ 는 상기 속성 값 $x_{i,j}$ 에 대한 제1 의사 난수)을 이용하여 생성되고, 상기 제2 의사 난수는, 아래의 수학식 3

[0049] [수학식 3]

$$f_Y = \sum_{i=1}^{n} \sum_{j \in S_i} PRF(z_{i,j}, y_{i,j})$$

[0050]

[0051] (이때, f_Y 는 상기 질의 벡터 집합에 대한 토큰, $y_{i,j}$ 는 상기 속성 벡터 $\vec{x}_i$ 에 대한 질의 벡터 $\vec{y}_i$ 에 포함된 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, S_i는 상기 질의 벡터 i에 포함된 하나 이상의 속성 값 중 와일드 카드(wild card) 속성 값을 제외한 나머지 속성 값들 각각에 대한 속성 카테고리 인덱스들의 집합)을 이용하여 생성되며, 상기 $z_{i,j}$ 는 아래의 수학식 4

[0052] [수학식 4]

$$z_{i,j} = PRF(z_i, j)$$

[0053]

[0054] 를 이용하여 생성될 수 있다.

[0055] 상기 마스터 비밀키는 아래의 수학식 5

[0056] [수학식 5]

$$MK = \left(\{z_i\}_{i=1}^{n}, \hat{v}, \hat{w}_1 = \hat{v}^{\sum_{i=1}^{n} w_{i,1}}, \hat{w}_2 = \hat{v}^{\sum_{i=1}^{n} w_{i,2}}\right)$$

[0057]

[0058] (이때, MK는 상기 마스터 비밀키, n은 상기 복수의 사용자의 수, $\hat{v}$ 는 위수가 p인 순환군(cyclic group) $\hat{G}$ 의 원소)를 만족하고,

[0059] 상기 암호문은, 아래의 수학식 6

[0060] [수학식 6]

$$CT_{i,T} = \left(\left\{C_{1,j}^{(i)} = H(T)^{f_{i,j}}\right\}_{j=1}^{\ell}, C_2^{(i)} = H(T)^{w_{i,1}}, C_3^{(i)} = H(T)^{w_{i,2}}\right)$$

[0061]

[0062] (이때, $CT_{i,T}$ 는 상기 암호문, ℓ 은 상기 속성 벡터에 포함된 속성 카테고리의 총 개수, T는 상기 라벨, $H(T)$ 는 상기 해시 값)을 만족하고,

[0063] 상기 토큰은, 아래의 수학식 7

[0064] [수학식 7]

$$TK_Y = \left(K_0 = \hat{v}^{fy \cdot r_1} \cdot \hat{w}_1^{r_2} \cdot \hat{w}_2^{r_3}, K_1 = \hat{v}^{-r_1}, K_2 = \hat{v}^{-r_2}, K_3 = \hat{v}^{-r_3}\right)$$

[0065]

[0066] (이때, TK_Y 는 상기 토큰, r_1 , r_2 및 r_3 는 각각 Z_p 의 원소)을 만족할 수 있다.

[0067] 상기 판단하는 단계는, 아래의 수학식 8

[0068] [수학식 8]

$$e(H(T), K_0) \cdot e\left(\prod_{i=1}^{n} \prod_{j \in S_i} C_{1,j}^{(i)}, K_1\right) \cdot e\left(\prod_{i=1}^{n} C_2^{(i)}, K_2\right) \cdot e\left(\prod_{i=1}^{n} C_3^{(i)}, K_3\right) = 1$$

[0069]

$e: G \times \hat{G} \rightarrow G_T$ G $\hat{G}$ G_T

[0070] (이때, e는 를 만족하는 겹선형 함수(bilinear map), , 및 는 위수(order)가 소수 p인 순환군(cyclic group))이 만족되는 경우, 상기 동치 관계가 성립하는 것으로 판단할 수 있다.

[0071] 본 발명의 일 실시예에 따른 장치는, 메모리; 및 하나 이상의 프로그램을 포함하는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 키 생성 장치로부터 사용자 암호키를 획득하는 단계; 및 속성 벡터에 대한 라벨(label) 및 상기 사용자 암호키에 기초하여 상기 속성 벡터에 대한 암호문을 생성하는 단계를 실행하기 위한 명령어들을 포함한다.

[0072] 상기 암호문을 생성하는 단계는, 상기 라벨에 대한 해시 값을 생성하는 단계; 상기 속성 벡터에 포함된 하나 이상의 속성 값 각각에 대한 의사 난수(pseudo-random number)를 생성하는 단계; 및 상기 해시 값, 상기 의사 난수 및 상기 사용자 암호키에 기초하여 상기 암호문을 생성할 수 있다.

[0073] 상기 암호문은, 상기 하나 이상의 속성 값 각각에 대한 의사 난수를 상기 해시 값의 지수로 이용하여 산출된 복수의 암호문 원소를 포함할 수 있다.

[0074] 상기 사용자 암호키는, 아래의 수학식 1

[0075] [수학식 1]

$$EK_i = (z_i, w_{i,1}, w_{i,2}),$$

[0076]

[0077] (이때, i 는 사용자 인덱스, EK_i 는 사용자 i에 대한 사용자 암호키, z_i 는 $Z_p = \{0, 1, \ldots, p-1\}$ 의 원소, $w_{i,1}$ 및 $w_{i,2}$ 는 각각 임의의 정수, p는 소수(prime number)을 만족하고, 상기 의사 난수를 생성하는 단계는, 아래의 수학식 2 및 3

[0078] [수학식 2]

$$z_{i,j} = PRF(z_i, j)$$

[0079]

[0080] [수학식 3]

$$f_{i,j} = PRF(z_{i,j}, x_{i,j})$$

[0081]

[0082] (이때, j 는 속성 카테고리 인덱스, PRF()는 의사 랜덤 함수, $x_{i,j}$ 는 상기 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, $f_{i,j}$ 는 상기 속성 값 $x_{i,j}$ 에 대한 의사 난수)을 이용하여 상기 하나 이상의 속성 값 각각에 대한 의사 난수를 생성할 수 있다.

[0083] 상기 암호문을 생성하는 단계는, 아래의 수학식 4

[0084] [수학식 4]

$$CT_{i,T} = \left(\left\{ C_{1,j}^{(i)} = H(T)^{f_{i,j}} \right\}_{j=1}^{\ell}, C_2^{(i)} = H(T)^{w_{i,1}}, C_3^{(i)} = H(T)^{w_{i,2}} \right)$$

[0085]

[0086] (이때, $CT_{i,T}$ 는 상기 암호문, ℓ 은 상기 속성 벡터에 포함된 속성 카테고리의 총 개수, T는 상기 라벨, $H(T)$ 는 상기 해시 값)을 이용하여 상기 암호문을 생성할 수 있다.

[0087] 본 발명의 일 실시예에 따른 장치는, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 복수의 사용자 각각에 대한 사용자 암호키 및 마스터 비밀키를 생성하는 단계; 상기 생성된 사용자 암호키를 상기 복수의 사용자 각각의 클라이언트 장치로 제공하는 단계; 질의 장치로부터 복수의 질의 벡터를 포함하는 질의 벡터 집합을 수신하는 단계; 상기 질의 벡터 집합 및 상기 마스터 비밀키를 이용하여 상기 질의 벡터 집합에 대한 토큰을 생성하는 단계; 및 상기 생성된 토큰을 상기 질의 장치로 제공하는 단계를 실행하기 위한 명령어들을 포함한다.

[0088] 상기 토큰을 생성하는 단계는, 상기 질의 벡터 집합에 대한 의사 난수(Pseudo-random number)를 생성하는 단계; 및 상기 의사 난수 및 상기 마스터 비밀키를 이용하여 상기 토큰을 생성하는 단계를 포함할 수 있다.

[0089] 상기 사용자 암호키는 아래의 수학식 1

[0090] [수학식 1]

$$EK_i = (z_i, w_{i,1}, w_{i,2}),$$

[0091]

[0092] (이때, i 는 사용자 인덱스, EK_i 는 사용자 i에 대한 사용자 암호키, z_i 는 $Z_p = \{0, 1, \ldots, p-1\}$ 의 원소, $w_{i,1}$

$w_{i,2}$

및 는 각각 임의의 정수, p는 소수(prime number))을 만족하고, 상기 의사 난수를 생성하는 단계는, 아래의 수학식 2 및 3

[0093] [수학식 2]

$$z_{i,j} = PRF(z_i, j)$$

[0094]

[0095] [수학식 3]

$$f_Y = \sum_{i=1}^{n} \sum_{j \in S_i} PRF(z_{i,j}, y_{i,j})$$

[0096]

j f_Y $y_{i,j}$

[0097] (이때, 는 속성 카테고리 인덱스, PRF()는 의사 랜덤 함수, 는 상기 질의 벡터 집합에 대한 토큰, 는 질의 벡터 i에 포함된 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, S_i는 상기 질의 벡터 i에 포함된 하나 이상의 속성 값들 중 와일드 카드(wild card) 속성 값을 제외한 나머지 속성 값들 각각에 대한 속성 카테고리 인덱스들의 집합)을 이용하여 상기 의사 난수를 생성할 수 있다.

[0098] 상기 마스터 비밀키를 생성하는 단계는 아래의 수학식 4

[0099] [수학식 4]

$$MK = \left(\{z_i\}_{i=1}^{n}, \hat{v}, \hat{w}_1 = \hat{v}^{\sum_{i=1}^{n} w_{i,1}}, \hat{w}_2 = \hat{v}^{\sum_{i=1}^{n} w_{i,2}}\right)$$

[0100]

$\hat{v}$ $\hat{G}$

[0101] (이때, MK는 상기 마스터 비밀키, n은 상기 복수의 사용자의 총수, 는 위수가 p인 순환군(cyclic group)의 원소)를 이용하여 상기 마스터 비밀키를 생성하고, 상기 토큰을 생성하는 단계는, 아래의 수학식 5

[0102] [수학식 5]

$$TK_Y = \left(K_0 = \hat{v}^{f_Y \cdot r_1} \cdot \hat{w}_1^{r_2} \cdot \hat{w}_2^{r_3}, K_1 = \hat{v}^{-r_1}, K_2 = \hat{v}^{-r_2}, K_3 = \hat{v}^{-r_3}\right)$$

[0103]

TK_Y r_1 r_2 r_3 Z_p

[0104] (이때, 는 상기 질의 벡터 집합에 대한 토큰, , 및 는 각각 의 원소)를 이용하여 상기 토큰을 생성할 수 있다.

[0105] 본 발명의 일 실시예에 따른 장치는, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 복수의 질의 벡터를 포함하는 질의 벡터 집합을 생성하는 단계; 키 생성 장치로부터 상기 질의 벡터 집합에 대한 토큰을 획득하는 단계; 및 상이한 사용자 암호키를 이용하여 암호화된 복수의 속성 벡터 각각에 대한 암호문, 상기 복수의 속성 벡터에 대한 라벨(label) 및 상기 토큰을 이용하여, 상기 복수의 속성 벡터를 포함하는 속성 벡터 집합과 상기 질의 벡터 집합 사이의 동치 관계 성립 여부를 판단하는 단계를 실행하기 위한 명령어들을 포함한다.

[0106] 상기 복수의 속성 벡터 각각에 대한 암호문은, 상기 라벨에 대한 해시 값, 상기 복수의 속성 벡터 각각에 포함된 하나 이상의 속성 값 각각에 대한 제1 의사 난수(pseudo-random number) 및 상기 사용자 암호키를 이용하여 생성되고, 상기 토큰은, 상기 질의 벡터 집합에 대한 제2 의사 난수 및 상기 마스터 비밀키를 이용하여 생성될 수 있다.

[0107] 상기 사용자 암호키는 아래의 수학식 1

[0108] [수학식 1]

$$EK_i = (z_i, w_{i,1}, w_{i,2}),$$

[0109]

[0110] (i 는 사용자 인덱스, EK_i 는 사용자 i에 대한 사용자 암호키, z_i 는 $Z_p = \{0, 1, \ldots, p-1\}$ 의 원소, $w_{i,1}$ 및 $w_{i,2}$ 는 각각 임의의 정수, p는 소수(prime number))을 만족하고, 상기 제1 의사 난수는, 아래의 수학식 2

[0111] [수학식 2]

$$f_{i,j} = PRF(z_{i,j}, x_{i,j})$$

[0112]

[0113] (이때, j 는 속성 카테고리 인덱스, PRF()는 의사 랜덤 함수, $x_{i,j}$ 는 사용자 i의 사용자 암호키를 이용하여 암호화된 속성 벡터 $\vec{x}_i$ 에 포함된 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, $f_{i,j}$ 는 상기 속성 값 $x_{i,j}$ 에 대한 제1 의사 난수)을 이용하여 생성되고, 상기 제2 의사 난수는, 아래의 수학식 3

[0114] [수학식 3]

$$f_Y = \sum_{i=1}^{n} \sum_{j \in S_i} PRF(z_{i,j}, y_{i,j})$$

[0115]

[0116] (이때, f_Y 는 상기 질의 벡터 집합에 대한 토큰, $y_{i,j}$ 는 상기 속성 벡터 $\vec{x}_i$ 에 대한 질의 벡터 $\vec{y}_i$ 에 포함된 하나 이상의 속성 값 중 속성 카테고리 j에 대한 속성 값, S_i는 상기 질의 벡터 i에 포함된 하나 이상의 속성 값 중 와일드 카드(wild card) 속성 값을 제외한 나머지 속성 값들 각각에 대한 속성 카테고리 인덱스들의 집합)을 이용하여 생성되며, 상기 $z_{i,j}$ 는 아래의 수학식 4

[0117] [수학식 4]

$$z_{i,j} = PRF(z_i, j)$$

[0118]

[0119] 를 이용하여 생성될 수 있다.

[0120] 상기 마스터 비밀키는 아래의 수학식 5

[0121] [수학식 5]

$$MK = \left(\{z_i\}_{i=1}^{n}, \hat{v}, \hat{w}_1 = \hat{v}^{\sum_{i=1}^{n} w_{i,1}}, \hat{w}_2 = \hat{v}^{\sum_{i=1}^{n} w_{i,2}}\right)$$

[0122]

[0123] (이때, MK는 상기 마스터 비밀키, n은 상기 복수의 사용자의 수, $\hat{v}$ 는 위수가 p인 순환군(cyclic group) $\hat{G}$ 의 원소)를 만족하고, 상기 암호문은, 아래의 수학식 6

[0124] [수학식 6]

$$CT_{i,T} = \left(\left\{C_{1,j}^{(i)} = H(T)^{f_{i,j}}\right\}_{j=1}^{\ell}, C_2^{(i)} = H(T)^{w_{i,1}}, C_3^{(i)} = H(T)^{w_{i,2}}\right)$$

[0125]

[0126] ($CT_{i,T}$, ℓ, $H(T)$) (이때, $CT_{i,T}$는 상기 암호문, ℓ은 상기 속성 벡터에 포함된 속성 카테고리의 총 개수, T는 상기 라벨, $H(T)$는 상기 해시 값)을 만족하고, 상기 토큰은, 아래의 수학식 7

[0127] [수학식 7]

$$TK_Y = \left(K_0 = \hat{v}^{fy \cdot r_1} \cdot \hat{w}_1^{r_2} \cdot \hat{w}_2^{r_3}, K_1 = \hat{v}^{-r_1}, K_2 = \hat{v}^{-r_2}, K_3 = \hat{v}^{-r_3}\right)$$

[0128]

[0129] (TK_Y, r_1, r_2, r_3, Z_p) (이때, TK_Y는 상기 토큰, r_1, r_2 및 r_3는 각각 Z_p의 원소)을 만족할 수 있다.

[0130] 상기 판단하는 단계는, 아래의 수학식 8

[0131] [수학식 8]

$$e(H(T), K_0) \cdot e\left(\prod_{i=1}^{n} \prod_{j \in S_i} C_{1,j}^{(i)}, K_1\right) \cdot e\left(\prod_{i=1}^{n} C_2^{(i)}, K_2\right) \cdot e\left(\prod_{i=1}^{n} C_3^{(i)}, K_3\right) = 1$$

[0132]

[0133] ($e: G \times \hat{G} \rightarrow G_T$, G, $\hat{G}$, G_T) (이때, e는 $e: G \times \hat{G} \rightarrow G_T$를 만족하는 겹선형 함수(bilinear map), G, $\hat{G}$ 및 G_T는 위수(order)가 소수 p인 순환군(cyclic group))이 만족되는 경우, 상기 동치 관계가 성립하는 것으로 판단할 수 있다.

발명의 효과

[0134] 본 발명의 실시예들에 따르면, 멀티 클라이언트 환경에서 상이한 클라이언트에 의해 생성된 다수의 암호문에 대한 효율적인 동치 연산이 가능하게 된다..

도면의 간단한 설명

[0135] 도 1은 도 1은 본 발명의 일 실시예에 따른 암호화 시스템의 구성도

도 2는 본 발명의 일 실시예에 따른 암호화 과정을 설명하기 위한 순서도

도 3은 본 발명의 일 실시예에 따른 질의 벡터 집합과 속성 벡터 집합 사이의 동치 관계 성립 여부를 판단하는 과정을 설명하기 위한 순서도

도 4는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0136] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0137] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 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. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0138] 도 1은 본 발명의 일 실시예에 따른 암호화 시스템의 구성도이다.

[0139] 도 1을 참조하면, 본 발명의 일 실시예에 따른 암호화 시스템(100)은 키 생성 장치(110), 복수의 클라이언트 장치(120-1, 120-2, 120-n), 데이터베이스(130) 및 질의 장치(140)를 포함한다.

[0140] 키 생성 장치(110)는 암호화 시스템(100)에서 사용할 마스터 비밀키, 사용자 암호키 및 공개 파라미터를 생성하기 위한 장치로서 예를 들어, 신뢰 기관(Trusted Third Party)와 같이 신뢰할 수 있는 개체에 의해 운영될 수 있다.

[0141] 구체적으로, 키 생성 장치(110)는 암호화 시스템(100)에 참여한 복수의 사용자 각각에 대한 사용자 암호키를 생성하고, 생성된 각 사용자에 대한 사용자 암호키를 암호화를 위해 각 사용자에 의해 이용되는 클라이언트 장치(120-1, 120-2, 120-n)로 제공할 수 있다.

[0142] 또한, 키 생성 장치(110)는 마스터 비밀키 및 공개 파라미터를 생성하여 마스터 비밀키는 안전하게 저장하고, 공개 파라미터는 암호화 시스템(100) 내에 공개할 수 있다.

[0143] 한편, 키 생성 장치(110)는 질의 장치(140)의 요청에 따라 질의 벡터 집합에 대한 토큰을 생성하여 질의 장치(140)로 제공할 수 있다.

[0144] 클라이언트 장치(120-1, 120-2, 120-n)는 암호문 생성을 위해 키 생성 장치(110)로부터 사용자 암호키를 발급받은 각 사용자에 의해 이용되는 장치로서, 클라이언트 장치(120-1, 120-2, 120-n)의 개수는 실시예에 따라 변경될 수 있다.

[0145] 데이터베이스(130)는 각 클라이언트 장치(120-1, 120-2, 120-n)에 의해 생성된 암호문을 저장하기 위한 것으로, 각 클라이언트 장치(120-1, 120-2, 120-n) 및 질의 장치(140)에 의해 접근 가능한 하나 이상의 서버 또는 클라우드(cloud) 환경 내에 구현될 수 있다.

[0146] 질의 장치(140)는 키 생성 장치(110)로부터 제공받은 질의 벡터 집합에 대한 토큰과 각 클라이언트 장치(120-1, 120-2, 120-n)에 의해 생성되어 데이터베이스(130)에 저장된 복수의 속성 벡터 각각에 대한 암호문을 이용하여, 복수의 속성 벡터를 포함하는 속성 벡터 집합과 질의 벡터 집합 사이의 동치 관계 성립 여부를 판단한다.

[0147] 한편, 도 1에 도시된 암호화 시스템(100)에서 수행되는 암호화 기법은 다음과 같은 4개의 알고리즘으로 구성될 수 있다.

[0148] 셋업(setup) 알고리즘

[0149] 셋업 알고리즘은 보안 상수(Security Parameter) 1^{λ} 및 암호화 시스템(100)에 참여할 사용자의 총수(n)을 입력 받아 각각 위수(order)가 소수(prime number) p인 순환군(cyclic group) G, $\hat{G}$ 및 G_T를 생성할 수 있다.

[0150] 또한, 셋업 알고리즘은 $e: G \times \hat{G} \rightarrow G_T$를 만족하는 겹선형 함수(bilinear map) e, $g \in G$를 만족하는 G의 생성원(generator) g 및 $\hat{g} \in \hat{G}$를 만족하는 $\hat{G}$의 생성원 $\hat{g}$를 생성할 수 있다.

[0151] 이후, 셋업 알고리즘은 모든 i(이때, i는 사용자 인덱스로서 $i \in [n]$인 정수)에 대해 $z_i \in Z_p = \{0, 1, \ldots, p-1\}$를 만족하는 z_i, 임의의 정수 $w_{i,1}$ 및 $w_{i,2}$를 선택하여 각 사용자에 대한 사용자 암호키 $EK_i = (z_i, w_{i,1}, w_{i,2})$를 생성할 수 있다.

[0152] 또한, 셋업 알고리즘은 $\hat{v} \in \hat{G}$를 만족하는 $\hat{v}$를 선택하고, 마스터 비밀키 $MK = \left(\{z_i\}_{i=1}^n, \hat{v}, \hat{w}_1 = \hat{v}^{\sum_{i=1}^n w_{i,1}}, \hat{w}_2 = \hat{v}^{\sum_{i=1}^n w_{i,2}}\right)$를 생성할 수 있다.

[0153] 한편, 본 발명의 일 실시예에서, 셋업 알고리즘은 키 생성 장치(110)에 의해 수행될 수 있다. 이 경우, 키 생성 장치(110)는 셋업 알고리즘을 수행하여 생성한 각 사용자의 사용자 암호키 EK_i를 각 사용자의 클라이언트 장치

(120-1, 120-2, 120-n)로 제공할 수 있다.

[0154] 또한, 키 생성 장치(110)는 마스터 비밀키 MK는 안전하게 저장하고, 공개 파라미터 $PP = \left((p, G, \hat{G}, G_T, e), g, \hat{g}, H\right)$ H G 는 공개할 수 있다. 이때, 는 임의의 문자 열을 로 맵핑시키는 해시 함수 $H: \{0,1\}^* \rightarrow G$ (hash function)(즉,)를 나타낸다.

[0155] 암호화 알고리즘

[0156] 암호화 알고리즘은 사용자 암호키, 공개 파라미터 및 속성 벡터에 대한 라벨(label)에 기초하여 속성 벡터에 대한 암호문을 생성할 수 있다.

[0157] 이때, 속성 벡터는 예를 들어, 특정 학생 또는 학급의 성적 데이터에 대한 속성, 특정인의 생체 데이터에 대한 속성 등과 같이 특정한 속성을 나타내기 위한 벡터로서 하나 이상의 속성 카테고리 각각에 대한 속성 값을 포함할 수 있다. 예를 들어, 속성 벡터가 특정 학급의 성적 데이터인 경우, 속성 카테고리는 예를 들어, 성적 평균, 최고 점수, 최저 점수 등일 수 있다.

[0158] 한편, 속성 벡터에 대한 라벨은 암호화 시스템(100) 내에서 기 설정된 방식에 따라 속성 벡터에 부여되는 정보로서 예를 들어, 속성 벡터에 대한 분류 정보, 속성 벡터와 관련된 시점에 관한 정보 등일 수 있으나, 반드시 특정한 정보로 한정되는 것은 아니다.

[0159] 구체적인 예로, 속성 벡터가 특정인의 홍체 데이터, 지문 데이터 및 유전자 데이터 중 유전자 데이터에 대한 속성 벡터인 경우, 해당 속성 벡터에 대한 라벨은 유전자 데이터에 대한 속성 벡터임을 나타내는 정보일 수 있다. 다른 예로, 속성 벡터가 특정 학급의 1학기 성적 데이터 및 2학기 성적 데이터 중 1학기 성적 데이터에 대한 속성 벡터인 경우, 해당 속성 벡터에 대한 라벨은 1학기 성적 데이터임을 나타내는 정보일 수 있다.

[0160] 한편, 암호화 알고리즘은 암호화할 속성 벡터 $\vec{x}_i = (x_{i,1}, \ldots, x_{i,\ell})$ (이때, ℓ 은 속성 벡터에 포함될 속성 카테고리의 총 개수)에 포함된 각 속성 값 $x_{i,j}$ (이때, j는 속성 카테고리의 인덱스로서 $j \in [\ell]$ 인 정수)에 대한 의사 난수(pseudo-random number)를 생성할 수 있다.

[0161] 구체적으로, 암호화 알고리즘은 아래의 수학식 1을 이용하여 속성 벡터 $\vec{x}_i$ 에 포함된 각 속성 값 $x_{i,j}$ 에 대한 의사 난수 $f_{i,j}$ 를 생성할 수 있다.

[0162] [수학식 1]

$$f_{i,j} = PRF(z_{i,j}, x_{i,j})$$

[0163]

[0164] 수학식 1에서, PRF()는 의사 랜덤 함수(pseudo-random function)를 나타내며, $z_{i,j}$ 는 아래의 수학식 2를 이용하여 산출될 수 있다.

[0165] [수학식 2]

$$z_{i,j} = PRF(z_i, j)$$

[0166]

[0167] 이후, 암호화 알고리즘은 속성 벡터 $\vec{x}_i$ 의 라벨 T에 대한 해시 값 H(T), 의사 난수 $f_{i,j}$ 및 사용자 암호키 EK_i에 기초하여 속성 벡터 $\vec{x}_i$ 에 대한 암호문을 생성할 수 있다.

[0168] 구체적으로, 암호화 알고리즘은 아래의 수학식 3을 이용하여 속성 벡터 $\vec{x}_i$ 에 대한 암호문 $CT_{i,T}$ 를 생성할 수 있다.

[0169] [수학식 3]

$$CT_{i,T} = \left(\left\{C_{1,j}^{(i)} = H(T)^{f_{i,j}}\right\}_{j=1}^{\ell}, C_2^{(i)} = H(T)^{w_{i1}}, C_3^{(i)} = H(T)^{w_{i2}}\right)$$

[0170]

[0171] 한편, 본 발명의 일 실시예에서, 암호화 알고리즘은 키 생성 장치(110)로부터 사용자 암호키를 발급받은 각 클라이언트 장치(120-1, 120-2, 120-n)에 의해 수행될 수 있다.

[0172] 이 경우, 각 클라이언트 장치(120-1, 120-2, 120-n)는 암호화 알고리즘을 수행하여 생성한 암호문 $CT_{i,T}$ 를 데이터베이스(130)에 저장할 수 있다. 이때, 각 클라이언트 장치(120-1, 120-2, 120-n)는 속성 벡터의 라벨 T 및 사용자의 인덱스 정보 i를 해당 속성 벡터에 대한 암호문 $CT_{i,T}$ 와 함께 데이터베이스(130)에 저장할 수 있다.

[0173] 토큰(Token) 생성 알고리즘

$$Y = (\vec{y}_1, \ldots, \vec{y}_n)$$

[0174] 토큰 생성 알고리즘은 질의 벡터 집합 에 대한 토큰을 생성할 수 있다. 이때, 질의 벡터 집합은 암호화 알고리즘을 이용하여 각 클라이언트 장치(120-1, 120-2, 120-n)에 의해 암호화된 속성 벡터들 각각에 대한 질의 벡터 $\vec{y}_i = (y_{i,1}, \ldots, y_{i,\ell})$ 를 포함할 수 있다.

[0175] 이때, 질의 벡터 $\vec{y}_i$ 에 포함된 각 속성 카테고리의 속성 값 $y_{i,j}$ 는 속성 벡터 $\vec{x}_i$ 에 포함된 속성 값들 중 $y_{i,j}$ 와 동일한 인덱스 튜플(tuple) (i, j)를 가지는 속성 값 $x_{i,j}$ 가 만족하여야 할 값을 의미할 수 있다.

[0176] 한편, 실시예에 따라, 각 질의 벡터 $\vec{y}_i$ 에 포함된 속성 값 중 하나 이상은 와일드 카드(wild card) 속성 값을 가질 수 있다. 이때, 와일드 카드 속성 값은 속성 벡터 $\vec{x}_i$ 포함된 속성 값들 중 와일드 카드 속성 값과 동일한 인덱스 튜플을 가지는 속성 값이 어떠한 값을 가지더라도 무관함을 의미할 수 있다.

[0177] 한편, 토큰 생성 알고리즘은 질의 벡터 집합 Y 및 마스터 비밀 키 MK를 이용하여 질의 벡터 집합 Y에 대한 토큰 TK_Y를 생성할 수 있다.

[0178] 구체적으로, 토큰 생성 알고리즘은 질의 벡터 집합 Y에 대한 의사 난수 f_Y 를 생성할 수 있다. 이때, 토큰 생성 알고리즘은 아래의 수학식 4를 이용하여 의사 난수 f_Y 를 생성할 수 있다.

[0179] [수학식 4]

$$f_Y = \sum_{i=1}^{n} \sum_{j \in S_i} PRF(z_{i,j}, y_{i,j})$$

[0180]

[0181] 수학식 4에서, S_i는 질의 벡터 집합 Y에 포함된 각 질의 벡터 $\vec{y}_i$ 의 속성 값들 중 와일드 카드(wild card) 속성

값을 제외한 나머지 속성 값들 각각에 대한 속성 카테고리 인덱스들을 포함하는 집합을 나타내며, $z_{i,j}$ 는 상술한 수학식 2를 이용하여 산출될 수 있다.

[0182] 이후, 토큰 생성 알고리즘은 생성된 의사 난수 f_Y 및 마스터 비밀키 MK를 이용하여 질의 벡터 집합 Y에 대한 토큰 TK_Y을 생성할 수 있다.

[0183] 구체적으로, 토큰 생성 알고리즘은 아래의 수학식 5를 이용하여 토큰 TK_Y를 생성할 수 있다.

[0184] [수학식 5]

$$TK_Y = \left(K_0 = \hat{v}^{f_Y \cdot r_1} \cdot \hat{w}_1^{r_2} \cdot \hat{w}_2^{r_3}, K_1 = \hat{v}^{-r_1}, K_2 = \hat{v}^{-r_2}, K_3 = \hat{v}^{-r_3}\right)$$

[0185]

[0186] 한편, 본 발명의 일 실시예에서, 토큰 생성 알고리즘은 키 생성 장치(110)에 의해 수행될 수 있다.

[0187] 이 경우, 키 생성 장치(110)는 질의 장치(140)로부터 질의 벡터 집합 Y에 대한 토큰 생성 요청이 있는 경우, 토큰 생성 알고리즘을 수행하여 질의 벡터 집합 Y에 대한 토큰 TK_Y를 생성할 수 있다. 또한, 키 생성 장치(110)는 생성된 토큰 TK_Y를 질의 장치(140)로 제공할 수 있다.

[0188] 쿼리(query) 알고리즘

[0189] 쿼리 알고리즘은 각 클라이언트 장치(120-1, 120-2, 120-n)에 의해 생성된 속성 벡터 $\vec{x}_i = (x_{i,1}, \ldots, x_{i,\ell})$ 에 대한 암호문 $CT_{i,T}$, 라벨 T 및 질의 벡터 집합 $Y = (\vec{y}_1, \ldots, \vec{y}_n)$ 에 대한 토큰 TK_Y를 이용하여 질의 벡터 집합 Y와 속성 벡터 집합 $X = (\vec{x}_1, \ldots, \vec{x}_n)$ 사이의 동치 관계 성립 여부를 판단할 수 있다.

[0190] 구체적으로, 쿼리 알고리즘은 아래의 수학식 6이 만족되는 경우, 질의 벡터 집합 Y와 속성 벡터 집합 X 사이의 동치 관계가 성립하는 것으로 판단할 수 있다.

[0191] [수학식 6]

$$e(H(T), K_0) \cdot e\left(\prod_{i=1}^{n} \prod_{j \in S_i} C_{1,j}^{(i)}, K_1\right) \cdot e\left(\prod_{i=1}^{n} C_2^{(i)}, K_2\right) \cdot e\left(\prod_{i=1}^{n} C_3^{(i)}, K_3\right) = 1$$

[0192]

[0193] 한편, 본 발명의 일 실시예에서, 쿼리 알고리즘은 질의 장치(140)에 의해 수행될 수 있다.

[0194] 이 경우, 질의 장치(110)는 쿼리 알고리즘을 수행하여 질의 벡터 집합 Y와 속성 벡터 집합 X 사이의 동치 관계가 성립하는 것으로 판단된 경우, 1을 출력하고, 성립하지 않는 것으로 판단된 경우, 0을 출력할 수 있다.

[0195] 도 2는 본 발명의 일 실시예에 따른 암호화 과정을 설명하기 위한 순서도이다.

[0196] 도 2에 도시된 순서도에서는 설명의 편의를 위해 암호화 시스템(100) 내에 각각 상이한 사용자에 의해 이용되는 3개의 클라이언트 장치(120-1, 120-2, 120-3)가 있는 것으로 가정하나, 사용자 및 클라이언트 장치의 개수가 반드시 도시된 예에 한정되는 것은 아니다.

[0197] 도 2를 참조하면, 우선, 키 생성 장치(110)는 셋업 알고리즘을 수행하여, 각 사용자의 사용자 암호키 $\{EK_i = (z_i, w_{i,1}, w_{i,2})\}_{i=1}^{3}$, 마스터 비밀키 $MK = \left(\{z_i\}_{i=1}^{3}, \hat{v}, \hat{w}_1 = \hat{v}^{\sum_{i=1}^{3} w_{i,1}}, \hat{w}_2 = \hat{v}^{\sum_{i=1}^{3} w_{i,2}}\right)$ 및 공개 파라미터 $PP = \left((p, G, \hat{G}, G_T, e), g, \hat{g}, H\right)$ 를 생성한다(201).

[0198] 이후, 키 생성 장치(110)는 사용자 1의 사용자 암호키 EK_1을 사용자 1에 의해 이용되는 클라이언트 장치 1(120-1)로 제공한다(202).

[0199] 또한, 키 생성 장치(110)는 사용자 2의 사용자 암호키 EK_2을 사용자 2에 의해 이용되는 클라이언트 장치 2(120-2)로 제공한다(203).

[0200] 또한, 키 생성 장치(110)는 사용자 3의 사용자 암호키 EK_3을 사용자 3에 의해 이용되는 클라이언트 장치 3(120-3)로 제공한다(204).

[0201] 한편, 키 생성 장치(110)로부터 사용자 암호키 EK_1를 획득한 클라이언트 장치 1(120-1)은 암호화 알고리즘을 수행하여 라벨이 T인 속성 벡터 $\vec{x}_1 = (x_{1,1}, \ldots, x_{1,\ell})$에 대한 암호문

$$CT_{1,T} = \left(\left\{C_{1,j}^{(1)} = H(T)^{f_{1,j}}\right\}_{j=1}^{\ell}, C_2^{(1)} = H(T)^{w_{1,1}}, C_3^{(1)} = H(T)^{w_{1,2}}\right)$$

을 생성한다(205).

[0202] 이후, 클라이언트 장치 1(120-1)은 생성한 암호문 $CT_{1,T}$을 데이터베이스(130)에 저장한다(206).

[0203] 또한, 키 생성 장치(110)로부터 사용자 암호키 EK_2를 획득한 클라이언트 장치 2(120-2)는 암호화 알고리즘을 수행하여 라벨이 T인 속성 벡터 $\vec{x}_2 = (x_{2,1}, \ldots, x_{2,\ell})$에 대한 암호문

$$CT_{2,T} = \left(\left\{C_{1,j}^{(2)} = H(T)^{f_{2,j}}\right\}_{j=1}^{\ell}, C_2^{(2)} = H(T)^{w_{2,1}}, C_3^{(2)} = H(T)^{w_{2,2}}\right)$$

을 생성한다(207).

[0204] 이후, 클라이언트 장치 2(120-2)는 생성한 암호문 $CT_{2,T}$을 데이터베이스(130)에 저장한다(208).

[0205] 또한, 키 생성 장치(110)로부터 사용자 암호키 EK_3를 획득한 클라이언트 장치 3(120-3)은 암호화 알고리즘을 수행하여 라벨이 T인 속성 벡터 $\vec{x}_3 = (x_{3,1}, \ldots, x_{3,\ell})$에 대한 암호문

$$CT_{3,T} = \left(\left\{C_{1,j}^{(3)} = H(T)^{f_{3,j}}\right\}_{j=1}^{\ell}, C_2^{(3)} = H(T)^{w_{3,1}}, C_3^{(3)} = H(T)^{w_{3,2}}\right)$$

을 생성한다(209).

[0206] 이후, 클라이언트 장치 3(120-3)는 생성한 암호문 $CT_{3,T}$을 데이터베이스(130)에 저장한다(210).

[0207] 도 3은 본 발명의 일 실시예에 따른 질의 벡터 집합과 속성 벡터 집합 사이의 동치 관계 성립 여부를 판단하는 과정을 설명하기 위한 순서도이다.

[0208] 도 3에 도시된 과정은 도 2에 도시된 암호화 과정 이후에 수행될 수 있다.

[0209] 도 3을 참조하면, 우선, 질의 장치(140)는 속성 벡터 집합 $X = (\vec{x}_1, \vec{x}_2, \vec{x}_3)$에 대한 질의 벡터 집합 $Y = (\vec{y}_1, \vec{y}_2, \vec{y}_3)$를 생성한다(301).

[0210] 이후, 질의 장치(140)는 키 생성 장치(110)로 질의 벡터 집합 Y에 대한 토큰 생성을 요청한다(302).

[0211] 이후, 키 생성 장치(110)는 토큰 생성 알고리즘을 수행하여 질의 벡터 집합 Y에 대한 토큰

$$TK_Y = \left(K_0 = \hat{v}^{fy \cdot r_1} \cdot \hat{w}_1^{r_2} \cdot \hat{w}_2^{r_3}, K_1 = \hat{v}^{-r_1}, K_2 = \hat{v}^{-r_2}, K_3 = \hat{v}^{-r_3}\right)$$

를 생성한다(303).

[0212] 이후, 키 생성 장치(110)는 생성한 토큰 TK_Y를 질의 장치(140)로 제공한다(304).

[0213] 이후, 질의 장치(140)는 데이터베이스(130)에 저장된 암호문들 중 속성 벡터 집합 X에 포함된 속성 벡터 $\vec{x}_1$, $\vec{x}_2$, $\vec{x}_3$ 및 $CT_{1,T}$, $CT_{2,T}$, $CT_{3,T}$ 각각에 대한 암호문과 토큰 TK_Y를 이용하여 질의 벡터 집합 Y와 속성 벡터 집합 X 사이의 동치 관계 성립 여부를 판단한다(305).

$$e(H(T),K_0)\cdot e\left(\prod_{i=1}^{3}\prod_{j\in S_i}C_{1,j}^{(i)},K_1\right)\cdot e\left(\prod_{i=1}^{3}C_2^{(i)},K_2\right)\cdot e\left(\prod_{i=1}^{3}C_3^{(i)},K_3\right)=1$$

[0214] 이때, 질의 장치(140)는 이 만족된 경우, 질의 벡터 집합 Y와 속성 벡터 집합 X 사이의 동치 관계가 성립하는 것으로 판단하고, 만족되지 않은 경우, 동치 관계가 성립하지 않는 것으로 판단할 수 있다.

[0215] 한편, 도 2 및 도 3에 도시된 순서도에서는 상기 과정을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0216] 도 4는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술되지 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0217] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 암호화 시스템(100)에 포함되는 하나 이상의 컴포넌트일 수 있다.

[0218] 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0219] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0220] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0221] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(12)와 연결될 수도 있다.

[0222] 이상에서 대표적인 실시예를 통하여 본 발명에 대하여 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 전술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0223] 10: 컴퓨팅 환경

12: 컴퓨팅 장치

14: 프로세서

16: 컴퓨터 판독 가능 저장 매체

18: 통신 버스

20: 프로그램

22: 입출력 인터페이스

24: 입출력 장치

26: 네트워크 통신 인터페이스

100: 암호화 시스템

110: 키 생성 장치

120-1, 120-2, 120-3, 120-n: 클라이언트 장치

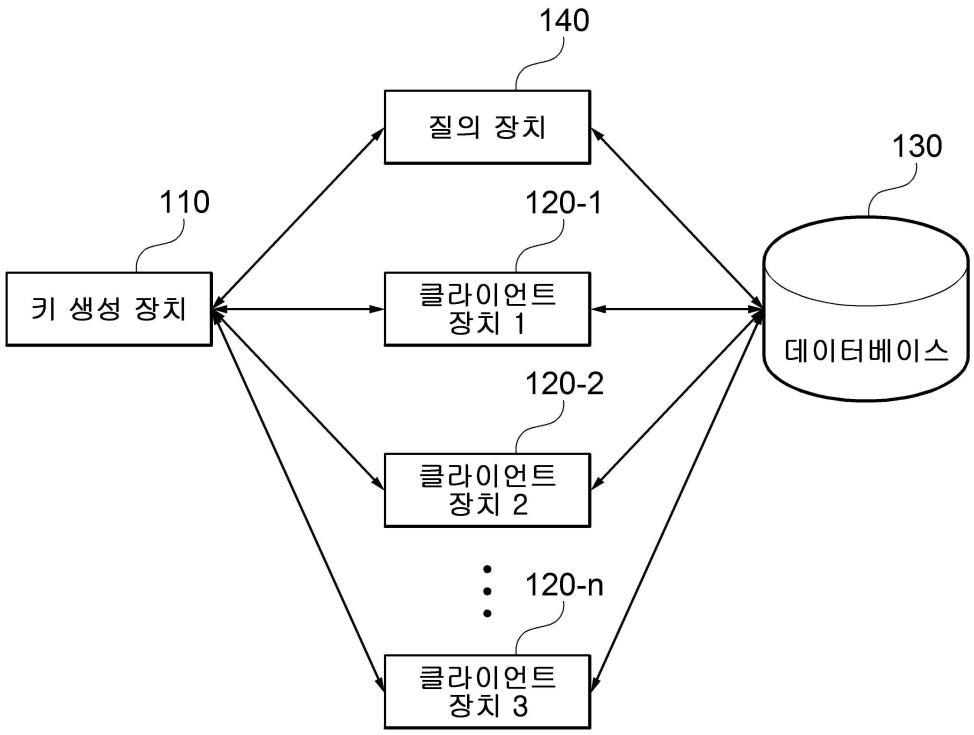
130: 데이터베이스

140: 질의 장치

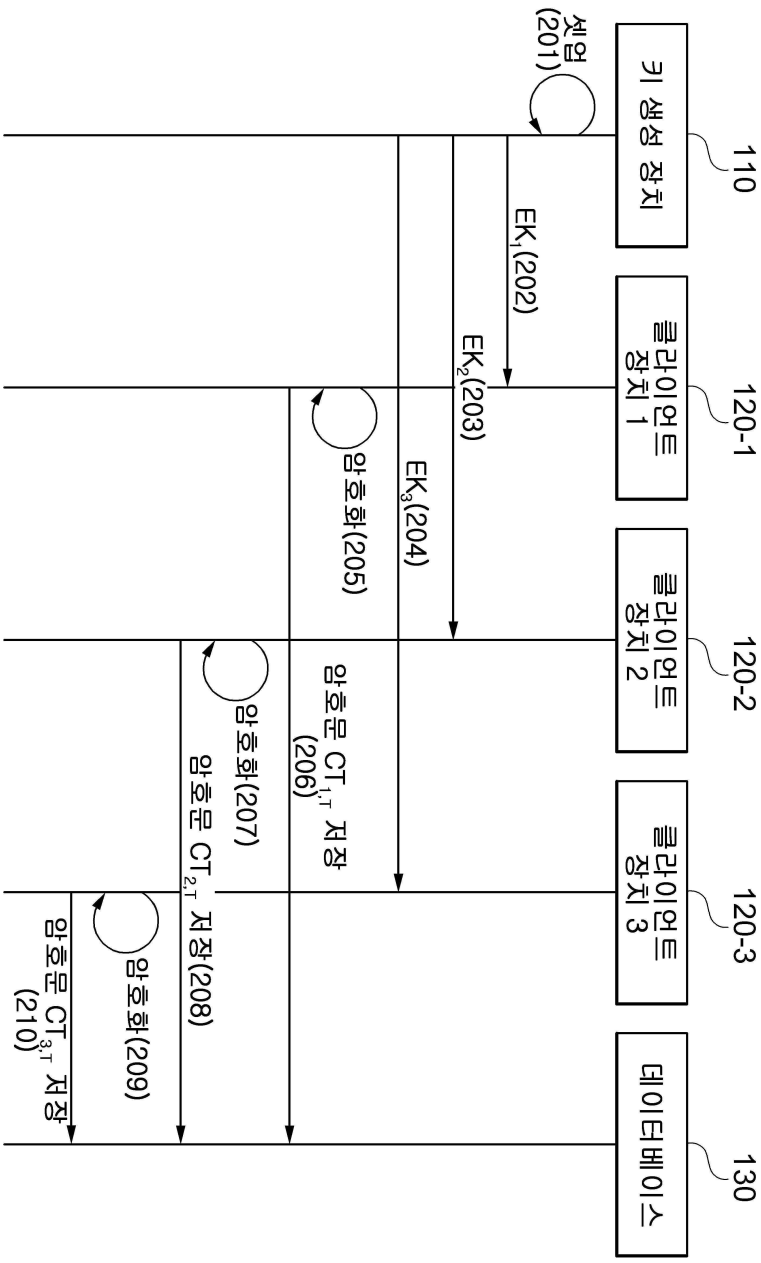
도면

도면1

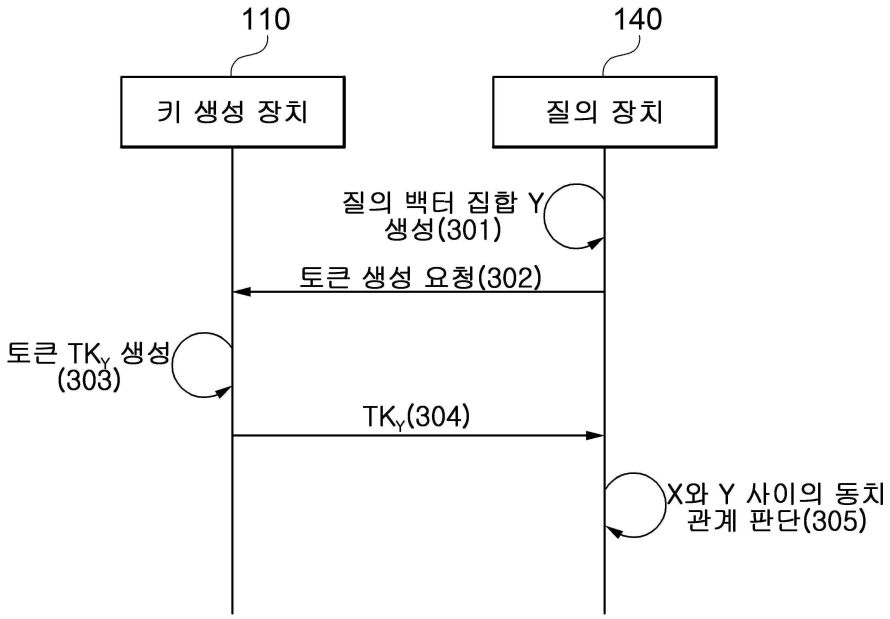
100



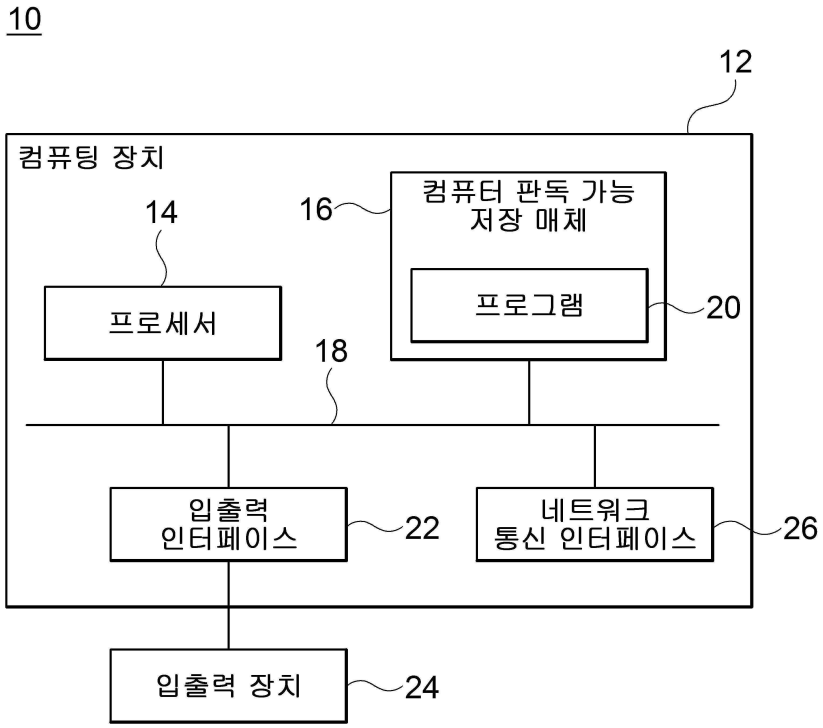
도면2


키 생성 장치
110
셋업 (201)
EK1(202)
EK2(203)
EK3(204)
클라이언트 장치 1
120-1
암호화(205)
클라이언트 장치 2
120-2
암호문 CT1,T 저장 (206)
암호화(207)
클라이언트 장치 3
120-3
암호문 CT2,T 저장(208)
암호화(209)
암호문 CT3,T 저장 (210)
데이터베이스
130

도면3


110
140
키 생성 장치
질의 장치
질의 백터 집합 Y 생성(301)
토큰 생성 요청(302)
토큰 TK_Y 생성 (303)
TK_Y(304)
X와 Y 사이의 동치 관계 판단(305)

도면4


10
12
컴퓨팅 장치
14
프로세서
16
컴퓨터 판독 가능 저장 매체
프로그램
20
18
입출력 인터페이스
22
네트워크 통신 인터페이스
26
입출력 장치
24