



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년10월23일
(11) 등록번호 10-2593179
(24) 등록일자 2023년10월19일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 9/06 (2006.01)

(52) CPC특허분류
H04L 9/0838 (2013.01)
H04L 9/0662 (2013.01)

(21) 출원번호 10-2021-0131890

(22) 출원일자 2021년10월05일

심사청구일자 2021년10월05일

(65) 공개번호 10-2023-0048912

(43) 공개일자 2023년04월12일

(56) 선행기술조사문헌

JP2013156330 A*

KR102281265 B1*

Aleksejus Mihalkovich 외 2명, Key Exchange Protocol Defined over a Non-Computing Group Based on an NP-Complete Decisional Problem, symmetry (2020.08.20.)*

*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 20 항

심사관 : 양종필

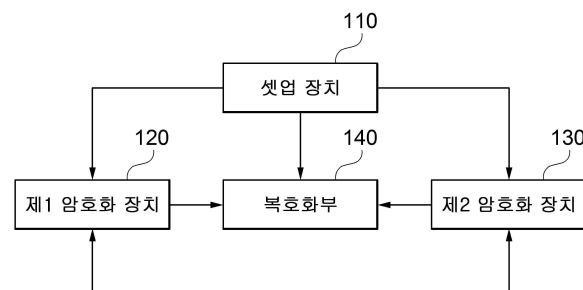
(54) 발명의 명칭 분산화된 키 발급을 지원하는 교집합 연산을 위한 효율적인 함수 암호 기술

(57) 요약

분산화된 키 발급을 지원하는 교집합 연산을 위한 효율적인 함수 암호 기술이 개시된다. 일 실시예에 따른 방법은, 각각 사전 정의된 정수 집합의 원소인 제1 비밀 값, 제2 비밀 값 및 제3 비밀 값을 포함하는 제1 사용자의 비밀키를 생성하는 단계; 상기 제3 비밀 값에 기초하여 제1 사용자의 공개키를 생성하는 단계; 상기 정수 집합의 원소인 제4 비밀 값에 기초하여 생성된 제2 사용자의 공개키를 획득하는 단계; 상기 제3 비밀 값 및 상기 제2 사용자의 공개키에 기초하여 상기 제1 사용자와 상기 제2 사용자가 공유할 공유키를 생성하는 단계; 및 상기 제1 비밀 값, 제2 비밀 값 및 상기 공유키에 기초하여, 상기 제1 사용자의 비밀키를 이용하여 암호화된 제1 데이터 집합과 상기 제2 사용자의 비밀키를 이용하여 암호화된 제2 데이터 집합 사이의 교집합을 생성하기 위해 이용될 함수키에 대한 부분키를 생성하는 단계를 포함한다.

대표도

100



(52) CPC특허분류

H04L 9/0825 (2013.01)

H04L 9/085 (2013.01)

H04L 2209/122 (2013.01)

H04L 2209/24 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711134706
과제번호	2021-0-00518-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	데이터경제를위한블록체인기술개발(R&D)
연구과제명	블록체인 데이터 암호화 기반의 프라이버시 보호 기술개발
기 여 율	1/1
과제수행기관명	한양대학교산학협력단
연구기간	2021.04.01 ~ 2021.12.31
공지예외적용	: 있음

명세서

청구범위

청구항 1

각각 사전 정의된 정수 집합의 원소인 제1 비밀 값, 제2 비밀 값 및 제3 비밀 값을 포함하는 제1 사용자의 비밀 키를 생성하는 단계;

상기 제3 비밀 값에 기초하여 제1 사용자의 공개키를 생성하는 단계;

상기 정수 집합의 원소인 제4 비밀 값에 기초하여 생성된 제2 사용자의 공개키를 획득하는 단계;

상기 제3 비밀 값 및 상기 제2 사용자의 공개키에 기초하여 상기 제1 사용자와 상기 제2 사용자가 공유할 공유 키를 생성하는 단계; 및

상기 제1 비밀 값, 제2 비밀 값 및 상기 공유키에 기초하여, 상기 제1 사용자의 비밀키를 이용하여 암호화된 제1 데이터 집합과 상기 제2 사용자의 비밀키를 이용하여 암호화된 제2 데이터 집합 사이의 교집합을 생성하기 위해 이용될 함수기에 대한 부분키를 생성하는 단계를 포함하고,

상기 제1 사용자의 공개키는, 아래의 수학적 식 1

[수학적 식 1]

$$PK_i = g^{y_i}$$

(이때, i는 상기 제1 사용자의 사용자 인덱스, PK_i 는 상기 제1 사용자의 공개키, g는 위수(order)가 소수 p인 곱셈형 군(bilinear group) G의 생성원, y_i 는 상기 제3 비밀 값)

을 만족하고,

상기 제2 사용자의 공개키는, 아래의 수학적 식 2

[수학적 식 2]

$$PK_j = g^{y_j}$$

(이때, j는 상기 제2 사용자의 사용자 인덱스, PK_j 는 상기 제2 사용자의 공개키, y_j 는 상기 제4 비밀 값)

를 만족하는, 방법.

청구항 2

삭제

청구항 3

청구항 1에 있어서,

상기 공유키는 아래의 수학적 식 3

[수학적 식 3]

$$K_{i,j} = PK_j^{y_i} = g^{y_i \cdot y_j}$$

(이때, $K_{i,j}$ 는 상기 공유키)

을 만족하는, 방법.

청구항 4

청구항 3에 있어서,

상기 부분키를 생성하는 단계는,

상기 공유키에 기초하여, 각각 상기 정수 집합의 원소인 제1 부분키 생성 요소, 제2 부분키 생성 요소 및 제3 부분키 생성 요소를 생성하는 단계; 및

상기 제1 비밀 값, 상기 제2 비밀 값, 상기 제1 부분키 생성 요소, 상기 제2 부분키 생성 요소 및 상기 제3 부분키 생성 요소에 기초하여 상기 부분키를 생성하는 단계를 포함하는, 방법.

청구항 5

청구항 4에 있어서,

상기 제1 부분키 생성 요소, 상기 제2 부분키 생성 요소 및 상기 제3 부분키 생성 요소는 아래의 수학식 4

[수학식 4]

$$r = PRF(K_{i,j}, 1)$$

$$s = PRF(K_{i,j}, 2)$$

$$t = PRF(K_{i,j}, 3)$$

(이때, r은 상기 제1 부분키 생성 요소, s는 상기 제2 부분키 생성 요소, t는 상기 제3 부분키 생성 요소,

$PRF: G \times [3] \rightarrow \mathbb{Z}_p$ 를 만족하는 의사 랜덤 함수(pseudo-random function), \mathbb{Z}_p 는 상기 정수 집합)

를 만족하는, 방법.

청구항 6

청구항 4에 있어서,

상기 부분키는, 제1 부분키 요소, 제2 부분키 요소 및 제3 부분키 요소를 포함하고,

상기 제1 부분키 요소는, 아래의 수학식 5

[수학식 5]

$$A_1 = \hat{g}^{a_i \cdot r}$$

(이때, A_1 은 상기 제1 부분키 요소, \hat{g} 는 위수가 상기 소수 p인 곱셈형 군 \hat{G} 의 생성원, r은 상기 제1 부분키 생성 요소, a_i 는 상기 제1 비밀 값)

를 만족하고,

상기 제2 부분키 요소는, 아래의 수학식 6

[수학식 6]

$$A_2 = \begin{cases} \hat{g}^{\beta_i \cdot s}, & \text{if } i < j \\ 1, & \text{if } i > j \end{cases}$$

(이때, A_2 는 상기 제2 부분키 요소, s 는 상기 제2 부분키 생성 요소, β_i 는 상기 제2 비밀 값)

을 만족하고,

상기 제3 부분키 요소는, 아래의 수학식 7

[수학식 7]

$$E = \begin{cases} s \cdot \alpha_i + t \bmod p, & \text{if } i < j \\ s \cdot \alpha_i - t \bmod p, & \text{if } i > j \end{cases}$$

(이때, E 는 상기 제3 부분키 요소, t 는 상기 제3 부분키 생성 요소)

을 만족하는, 방법.

청구항 7

제1 암호화 장치로부터 제1 사용자의 비밀키를 이용하여 암호화된 제1 데이터 집합과 제2 사용자의 비밀키를 이용하여 암호화된 제2 데이터 집합 사이의 교집합을 생성하기 위해 이용될 함수키에 대한 제1 부분 키를 획득하는 단계;

제2 암호화 장치로부터 상기 함수키에 대한 제2 부분 키를 획득하는 단계;

사전 정의된 정수 집합의 원소인 임의의 정수를 선택하는 단계; 및

상기 임의의 정수, 상기 제1 부분 키 및 상기 제2 부분 키에 기초하여 상기 함수키를 생성하는 단계를 포함하고,

상기 제1 부분 키는, 상기 제1 사용자의 비밀키 및 상기 제2 사용자의 공개키에 기초하여 생성되고,

상기 제2 부분 키는, 상기 제2 사용자의 비밀키 및 상기 제1 사용자의 공개키에 기초하여 생성되며,

상기 제1 사용자의 비밀키는 아래의 수학식 1

[수학식 1]

$$SK_i = \{\alpha_i, \beta_i, \gamma_i\}$$

(이때, i 는 상기 제1 사용자의 사용자 인덱스, SK_i 는 상기 제1 사용자의 비밀키, α_i , β_i 및 γ_i 는

$$\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}_p$$

를 만족하는 임의의 정수, \mathbb{Z}_p 는 상기 정수 집합)

을 만족하고,

상기 제1 사용자의 공개키는 아래의 수학식 2

[수학식 2]

$$PK_i = g^{\gamma_i}$$

(이때, PK_i 는 상기 제1 사용자의 공개키, g 는 위수(order)가 소수 p 인 곱셈형 군(bilinear group) G 의 생성원)

를 만족하고,

상기 제2 사용자의 비밀키는 아래의 수학식 3

[수학식 3]

$$SK_j = \{\alpha_j, \beta_j, \gamma_j\}$$

(이때, j 는 상기 제2 사용자의 사용자 인덱스, SK_j 는 상기 제2 사용자의 비밀키, α_j , β_j 및 γ_j 는

$$\alpha_j, \beta_j, \gamma_j \in \mathbb{Z}_p$$

를 만족하는 임의의 정수)

을 만족하고,

상기 제2 사용자의 공개키는, 아래의 수학식 4

[수학식 4]

$$PK_j = g^{\gamma_j}$$

(이때, PK_j 는 상기 제2 사용자의 공개키)

를 만족하는, 방법.

청구항 8

삭제

청구항 9

청구항 7에 있어서,

상기 제1 부분키는, 상기 γ_i 및 상기 제2 사용자의 공개키 PK_j 에 기초하여 제1 암호화 장치에 의해 생성된 공유 키에 기초하여 생성되고,

상기 제2 부분키는, 상기 γ_j 및 상기 제1 사용자의 공개키 PK_i 에 기초하여 제2 암호화 장치에 의해 생성된 상기 공유키에 기초하여 생성되는, 방법.

청구항 10

청구항 9에 있어서,

상기 공유키는, 아래의 수학식 5

[수학식 5]

$$K_{i,j} = PK_j^{\gamma_i} = PK_i^{\gamma_j} = g^{\gamma_i \cdot \gamma_j}$$

(이때, $K_{i,j}$ 는 상기 공유키)

를 만족하는, 방법.

청구항 11

청구항 10에 있어서,

상기 제1 부분키는 아래의 수학식 6

[수학식 6]

$$pDK_{i,(i,j)} = \{A_1 = \hat{g}^{a_i \cdot r}, A_2 = \hat{g}^{\beta_i \cdot s}, E = s \cdot \alpha_i + t \bmod p\}$$

을 만족하고,

상기 제2 부분키는 아래의 수학식 7

[수학식 7]

$$pDK_{j,(i,j)} = \{A'_1 = \hat{g}^{a_j \cdot r'}, A'_2 = 1, E' = s \cdot \alpha_j - t \bmod p\}$$

을 만족하는, 방법.

청구항 12

청구항 11에 있어서,

상기 함수키는, 아래의 수학식 8

[수학식 8]

$$DK_{(i,j)} = \{K_1 = (A_1)^{r'}, K_2 = (A'_1)^{r'}, K_3 = (A_2)^{1/(E+E')}\}$$

(이때, $DK_{(i,j)}$ 는 상기 함수키, r' 는 상기 선택된 임의의 정수)

을 만족하는, 방법.

청구항 13

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 하나 이상의 프로그램은,

각각 사전 정의된 정수 집합의 원소인 제1 비밀 값, 제2 비밀 값 및 제3 비밀 값을 포함하는 제1 사용자의 비밀 키를 생성하는 단계;

상기 제3 비밀 값에 기초하여 제1 사용자의 공개키를 생성하는 단계;

상기 정수 집합의 원소인 제4 비밀 값에 기초하여 생성된 제2 사용자의 공개키를 획득하는 단계;

상기 제3 비밀 값 및 상기 제2 사용자의 공개키에 기초하여 상기 제1 사용자와 상기 제2 사용자가 공유할 공유 키를 생성하는 단계; 및

상기 제1 비밀 값, 제2 비밀 값 및 상기 공유키에 기초하여, 상기 제1 사용자의 비밀키를 이용하여 암호화된 제1 데이터 집합과 상기 제2 사용자의 비밀키를 이용하여 암호화된 제2 데이터 집합 사이의 교집합을 생성하기 위해 이용될 함수키에 대한 부분키를 생성하는 단계를 실행하기 위한 명령어들을 포함하고,

상기 제1 사용자의 공개키는, 아래의 수학식 1

[수학식 1]

$$PK_i = g^{y_i}$$

(이때, i 는 상기 제1 사용자의 사용자 인덱스, PK_i 는 상기 제1 사용자의 공개키, g 는 위수(order)가 소수 p 인 곱셈형 군(bilinear group) G 의 생성원, y_i 는 상기 제3 비밀 값)

을 만족하고,

상기 제2 사용자의 공개키는, 아래의 수학식 2

[수학식 2]

$$PK_j = g^{y_j}$$

(이때, j 는 상기 제2 사용자의 사용자 인덱스, PK_j 는 상기 제2 사용자의 공개키, y_j 는 상기 제4 비밀 값)

를 만족하는, 장치.

청구항 14

삭제

청구항 15

청구항 13에 있어서,

상기 공유키는 아래의 수학식 3

[수학식 3]

$$K_{i,j} = PK_j^{y_i} = g^{y_i \cdot y_j}$$

(이때, $K_{i,j}$ 는 상기 공유키)

을 만족하는, 장치.

청구항 16

청구항 15에 있어서,

상기 부분키를 생성하는 단계는,

상기 공유키에 기초하여, 각각 상기 정수 집합의 원소인 제1 부분키 생성 요소, 제2 부분키 생성 요소 및 제3 부분키 생성 요소를 생성하는 단계; 및

상기 제1 비밀 값, 상기 제2 비밀 값, 상기 제1 부분키 생성 요소, 상기 제2 부분키 생성 요소 및 상기 제3 부분키 생성 요소에 기초하여 상기 부분키를 생성하는 단계를 포함하는, 장치.

청구항 17

청구항 16에 있어서,

상기 제1 부분키 생성 요소, 상기 제2 부분키 생성 요소 및 상기 제3 부분키 생성 요소는 아래의 수학식 4

[수학식 4]

$$r = PRF(K_{i,j}, 1)$$

$$s = PRF(K_{i,j}, 2)$$

$$t = PRF(K_{i,j}, 3)$$

(이때, r은 상기 제1 부분키 생성 요소, s는 상기 제2 부분키 생성 요소, t는 상기 제3 부분키 생성 요소,

$PRF: G \times [3] \rightarrow \mathbb{Z}_p$ 를 만족하는 의사 랜덤 함수(pseudo-random function), \mathbb{Z}_p 는 상기 정수 집합)

를 만족하는, 장치.

청구항 18

청구항 16에 있어서,

상기 부분키는, 제1 부분키 요소, 제2 부분키 요소 및 제3 부분키 요소를 포함하고,

상기 제1 부분키 요소는, 아래의 수학식 5

[수학식 5]

$$A_1 = \hat{g}^{\alpha_i \cdot r}$$

(이때, A_1 은 상기 제1 부분키 요소, \hat{g} 는 위수가 상기 소수 p인 곱셈형 군 \hat{G} 의 생성원, r은 상기 제1 부분키 생성 요소, α_i 는 상기 제1 비밀 값)

를 만족하고,

상기 제2 부분키 요소는, 아래의 수학식 6

[수학식 6]

$$A_2 = \begin{cases} \hat{g}^{\beta_i \cdot s}, & \text{if } i < j \\ 1, & \text{if } i > j \end{cases}$$

(이때, A_2 는 상기 제2 부분키 요소, s는 상기 제2 부분키 생성 요소, β_i 는 상기 제2 비밀 값)

을 만족하고,

상기 제3 부분키 요소는, 아래의 수학식 7

[수학식 7]

$$E = \begin{cases} s \cdot \alpha_i + t \bmod p, & \text{if } i < j \\ s \cdot \alpha_i - t \bmod p, & \text{if } i > j \end{cases}$$

(이때, E는 상기 제3 부분키 요소, t는 상기 제3 부분키 생성 요소)

을 만족하는, 장치.

청구항 19

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 하나 이상의 프로그램은,

제1 암호화 장치로부터 제1 사용자의 비밀키를 이용하여 암호화된 제1 데이터 집합과 제2 사용자의 비밀키를 이용하여 암호화된 제2 데이터 집합 사이의 교집합을 생성하기 위해 이용될 함수키에 대한 제1 부분 키를 획득하는 단계;

제2 암호화 장치로부터 상기 함수키에 대한 제2 부분 키를 획득하는 단계;

사전 정의된 정수 집합의 원소인 임의의 정수를 선택하는 단계; 및

상기 임의의 정수, 상기 제1 부분 키 및 상기 제2 부분 키에 기초하여 상기 함수키를 생성하는 단계를 실행하기 위한 명령어들을 포함하고,

상기 제1 부분 키는, 상기 제1 사용자의 비밀키 및 상기 제2 사용자의 공개키에 기초하여 생성되고,

상기 제2 부분 키는, 상기 제2 사용자의 비밀키 및 상기 제1 사용자의 공개키에 기초하여 생성되며,

상기 제1 사용자의 비밀키는 아래의 수학식 1

[수학식 1]

$$SK_i = \{\alpha_i, \beta_i, \gamma_i\}$$

(이때, i 는 상기 제1 사용자의 사용자 인덱스, SK_i 는 상기 제1 사용자의 비밀키, α_i , β_i 및 γ_i 는

$\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}_p$ 를 만족하는 임의의 정수, \mathbb{Z}_p 는 상기 정수 집합)

을 만족하고,

상기 제1 사용자의 공개키는 아래의 수학식 2

[수학식 2]

$$PK_i = g^{\gamma_i}$$

(이때, PK_i 는 상기 제1 사용자의 공개키, g 는 위수(order)가 소수 p 인 곱셈형 군(bilinear group) G 의 생성원)

를 만족하고,

상기 제2 사용자의 비밀키는 아래의 수학식 3

[수학식 3]

$$SK_j = \{\alpha_j, \beta_j, \gamma_j\}$$

(이때, j 는 상기 제2 사용자의 사용자 인덱스, SK_j 는 상기 제2 사용자의 비밀키, α_j , β_j 및 γ_j 는

$\alpha_j, \beta_j, \gamma_j \in \mathbb{Z}_p$ 를 만족하는 임의의 정수)

을 만족하고,

상기 제2 사용자의 공개키는, 아래의 수학적식 4

[수학적식 4]

$$PK_j = g^{Y_j}$$

(이때, PK_j는 상기 제2 사용자의 공개키)

를 만족하는, 장치.

청구항 20

삭제

청구항 21

청구항 19에 있어서,

상기 제1 부분키는, 상기 x_i 및 상기 제2 사용자의 공개키 PK_j에 기초하여 제1 암호화 장치에 의해 생성된 공유키에 기초하여 생성되고,

상기 제2 부분키는, 상기 x_j 및 상기 제1 사용자의 공개키 PK_i에 기초하여 제2 암호화 장치에 의해 생성된 상기 공유키에 기초하여 생성되는, 장치.

청구항 22

청구항 21에 있어서,

상기 공유키는, 아래의 수학적식 5

[수학적식 5]

$$K_{i,j} = PK_j^{Y_i} = PK_i^{Y_j} = g^{Y_i \cdot Y_j}$$

(이때, K_{i,j}는 상기 공유키)

를 만족하는, 장치.

청구항 23

청구항 22에 있어서,

상기 제1 부분키는 아래의 수학적식 6

[수학적식 6]

$$pDK_{i,(i,j)} = \{A_1 = \hat{g}^{a_i \cdot r}, A_2 = \hat{g}^{\beta_i \cdot s}, E = s \cdot \alpha_i + t \bmod p\}$$

을 만족하고,

상기 제2 부분키는 아래의 수학적식 7

[수학적식 7]

$$pDK_{j,(i,j)} = \{A'_1 = \hat{g}^{a_j \cdot r}, A'_2 = 1, E' = s \cdot a_j - t \bmod p\}$$

을 만족하는, 장치.

청구항 24

청구항 23에 있어서,

상기 함수키는, 아래의 수학적식 8

[수학적식 8]

$$DK_{(i,j)} = \{K_1 = (A_1)^{r'}, K_2 = (A'_1)^{r'}, K_3 = (A_2)^{1/(E+E')}\}$$

(이때, $DK_{(i,j)}$ 는 상기 함수키, r' 는 상기 선택된 임의의 정수)

을 만족하는, 장치.

발명의 설명

기술 분야

[0001] 본 발명의 실시예들은 함수 암호(functional encryption) 기술과 관련된다.

배경 기술

[0002] 함수 암호(Functional Encryption, FE)는 암호화된 상태에서 연산을 수행하는 암호 기술로, 평문에 대한 암호문과 함수에 대한 함수키를 이용하여 복호화하면 함수 연산의 결과를 평문 형태로 출력한다. 임의의 함수에 대해 동작하는 함수 암호 기술은 구현이 매우 비효율적이기 때문에, 내적 연산 등 특정 함수에 대해서 효율적으로 연산 가능한 함수 암호 기술들이 제안되어 왔다.

[0003] 한편, 교집합 연산을 지원하는 종래 함수 암호 기술(Functional Encryption for Set Intersection, FE-SI)은 아래와 같은 문제점들이 존재한다.

[0004] 1. 시스템을 셋업(setup)하는 과정에서 연산을 수행하는 사용자가 고정된다. 즉, 사용자가 n 명인 경우, 시스템 셋업(set up)에서 오직 고정된 n 명의 사용자에게 대한 비밀키와 시스템 파라미터가 발급되며, 새로운 사용자가 추가되는 경우에는 전체 시스템을 다시 셋업 해야 한다.

[0005] 2. 시스템 셋업에 참여한 n 명의 사용자 전체가 연산에 참여해야만 하며, 그 중 일부 사용자들의 데이터 집합에 대한 교집합 연산은 수행할 수 없다.

[0006] 3. 교집합 연산을 수행하기 위한 비밀 정보가 존재하지 않으며, 따라서 누구나 암호문만을 이용하여 교집합을 연산할 수 있다.

[0007] 대한민국 등록특허 제10-2143525호에서는 이러한 종래 기술의 문제점을 해결할 수 있는 새로운 함수 암호 기술을 개시하고 있다.

[0008] 대한민국 등록특허 제10-2143525호에서 개시하고 있는 함수 암호 기술은 (1) 시스템을 셋업하는 과정에서 시스템 내의 모든 사용자에게 대한 비밀키와 시스템 파라미터가 발급되기 때문에 임의의 사용자들 간에 교집합 연산을 수행하더라도 초기 단계에서 한 번의 셋업만 수행하면 되고 (2) 신뢰 기관으로부터 교집합 연산을 위한 함수키를 발급받은 사용자(혹은 제 3의 서비스 제공자)만이 암호문으로부터 교집합 연산의 결과를 계산할 수 있으며 (3) 공모 공격(collusion)에 안전하도록 설계되었다. 그러나, 복호화 과정에서 집합의 개수(n)의 제곱에 비례한 연산이 필요하여, n 이 커질수록 복호화 시간이 제곱으로 증가한다.

[0009] 구체적으로, 대한민국 등록특허 제10-2143525호에서 개시하고 있는 함수 암호 기술에 따르면, 원소의 개수가 n_1 인 데이터 집합 X_1 에 대한 암호문, 원소의 개수가 n_2 인 데이터 집합 X_2 에 대한 암호문 및 복호화 키를 입력으로 이용하여 $X_1 \cap X_2$ 를 생성하기 위해 $n_1 \cdot n_2$ 에 비례하는 연산이 필요하게 된다. 즉, 대한민국 등록특허 제10-2143525호에서 개시하고 있는 함수 암호 기술은 $O(n^2)$ 의 복호화 난이도를 가지므로, 집합의 개수가 큰 환경에서

는 실시간으로 복호화를 할 수 없는 문제점이 발생할 수 있다.

[0010] 한편, 대한민국 등록특허 제10-2284877호에서는 대한민국 등록특허 제10-2143525호에서 개시하고 있는 함수 암호 기술의 효율성을 개선하여 원소의 개수가 n_1 인 데이터 집합 X_1 에 대한 암호문, 원소의 개수가 n_2 인 데이터 집합 X_2 에 대한 암호문 및 복호화 키를 입력으로 이용하여 $X_1 \cap X_2$ 를 생성하기 위해 n_1+n_2 에 비례하는 연산이 필요한 함수 암호 기술을 제시하였다.

[0011] 그러나, 대한민국 등록특허 제10-2284877호에서 개시하고 있는 함수 암호 기술의 경우, 암호화 과정에서 사용되는 사용자 비밀번호와 복호화 과정에서 필요한 함수키를 중앙의 신뢰 기관이 생성하기 때문에 신뢰 기관이 모든 암호문을 복호화할 수 있고, 각 사용자가 서비스 제공자에 대한 데이터 접근 권한을 직접 제어하지 못한다는 문제점이 있다.

선행기술문헌

특허문헌

[0012] (특허문헌 0001) 대한민국 등록특허 제10-2143525호 (2020. 08. 11. 공고)

(특허문헌 0002) 대한민국 등록특허 제10-2284877호 (2021. 07. 30. 공고)

발명의 내용

해결하려는 과제

[0013] 본 발명의 실시예들은 교집합 연산을 지원하는 함수 암호를 위한 방법 및 이를 이용한 장치를 제공하기 위한 것이다.

과제의 해결 수단

[0014] 일 실시예에 따른 방법은, 각각 사전 정의된 정수 집합의 원소인 제1 비밀 값, 제2 비밀 값 및 제3 비밀 값을 포함하는 제1 사용자의 비밀키를 생성하는 단계; 상기 제3 비밀 값에 기초하여 제1 사용자의 공개키를 생성하는 단계; 상기 정수 집합의 원소인 제4 비밀 값에 기초하여 생성된 제2 사용자의 공개키를 획득하는 단계; 상기 제3 비밀 값 및 상기 제2 사용자의 공개키에 기초하여 상기 제1 사용자와 상기 제2 사용자가 공유할 공유키를 생성하는 단계; 및 상기 제1 비밀 값, 제2 비밀 값 및 상기 공유키에 기초하여, 상기 제1 사용자의 비밀키를 이용하여 암호화된 제1 데이터 집합과 상기 제2 사용자의 비밀키를 이용하여 암호화된 제2 데이터 집합 사이의 교집합을 생성하기 위해 이용될 함수키에 대한 부분키를 생성하는 단계를 포함한다.

[0015] 상기 제1 사용자의 공개키는, 아래의 수학적 식 1

[0016] [수학적 식 1]

$$PK_i = g^{Y_i}$$

[0017]

[0018] (이때, i 는 상기 제1 사용자의 사용자 인덱스, PK_i 는 상기 제1 사용자의 공개키, g 는 위수(order)가 소수 p 인 곱셈형 군(bilinear group) G 의 생성원, Y_i 는 상기 제3 비밀 값을 만족하고, 상기 제2 사용자의 공개키는, 아래의 수학적 식 2

[0019] [수학적 식 2]

$$PK_j = g^{Y_j}$$

[0020]

[0021] (이때, j 는 상기 제2 사용자의 사용자 인덱스, PK_j 는 상기 제2 사용자의 공개키, Y_j 는 상기 제4 비밀 값을 만족할 수 있다.

[0022] 상기 공유키는 아래의 수학적 식 3

[0023] [수학식 3]

$$K_{i,j} = PK_j^{Y_i} = g^{Y_i \cdot Y_j}$$

[0024]

[0025] (이때, $K_{i,j}$ 는 상기 공유키)을 만족할 수 있다.

[0026] 상기 부분키를 생성하는 단계는, 상기 공유키에 기초하여, 각각 상기 정수 집합의 원소인 제1 부분키 생성 요소, 제2 부분키 생성 요소 및 제3 부분키 생성 요소를 생성하는 단계; 및 상기 제1 비밀 값, 상기 제2 비밀 값, 상기 제1 부분키 생성 요소, 상기 제2 부분키 생성 요소 및 상기 제3 부분키 생성 요소에 기초하여 상기 부분키를 생성하는 단계를 포함할 수 있다.

[0027] 상기 제1 부분키 생성 요소, 상기 제2 부분키 생성 요소 및 상기 제3 부분키 생성 요소는 아래의 수학식 4

[0028] [수학식 4]

$$r = PRF(K_{i,j}, 1)$$

[0029]

$$s = PRF(K_{i,j}, 2)$$

[0030]

$$t = PRF(K_{i,j}, 3)$$

[0031]

[0032] (이때, r은 상기 제1 부분키 생성 요소, s는 상기 제2 부분키 생성 요소, t는 상기 제3 부분키 생성 요소,

$$PRF: G \times [3] \rightarrow \mathbb{Z}_p$$

PRF()는 를 만족하는 의사 랜덤 함수(pseudo-random function), 는 상기 정수 집합)를 만족할 수 있다.

[0033] 상기 부분키는, 제1 부분키 요소, 제2 부분키 요소 및 제3 부분키 요소를 포함하고, 상기 제1 부분키 요소는, 아래의 수학식 5

[0034] [수학식 5]

$$A_1 = \hat{g}^{\alpha_i \cdot r}$$

[0035]

$$\hat{g} \quad \hat{G}$$

[0036] (이때, A_1 은 상기 제1 부분키 요소, 는 위수가 상기 소수 p인 곱셈형 군 의 생성원, r은 상기 제1 부분키 생성 요소, α_i 는 상기 제1 비밀 값)를 만족하고, 상기 제2 부분키 요소는, 아래의 수학식 6

[0037] [수학식 6]

$$A_2 = \begin{cases} \hat{g}^{\beta_i \cdot s}, & \text{if } i < j \\ 1, & \text{if } i > j \end{cases}$$

[0038] 삭제

[0039] (이때, A_2 는 상기 제2 부분키 요소, s는 상기 제2 부분키 생성 요소, β_i 는 상기 제2 비밀 값)을 만족하고, 상기 제3 부분키 요소는, 아래의 수학식 7

[0040] [수학식 7]

$$E = \begin{cases} s \cdot \alpha_i + t \bmod p, & \text{if } i < j \\ s \cdot \alpha_i - t \bmod p, & \text{if } i > j \end{cases}$$

[0041]

[0042] (이때, E는 상기 제3 부분키 요소, t는 상기 제3 부분키 생성 요소)을 만족할 수 있다.

[0043] 일 실시예에 따른 방법은, 제1 암호화 장치로부터 제1 사용자의 비밀키를 이용하여 암호화된 제1 데이터 집합과 제2 사용자의 비밀키를 이용하여 암호화된 제2 데이터 집합 사이의 교집합을 생성하기 위해 이용될 함수키에 대한 제1 부분 키를 획득하는 단계; 제2 암호화 장치로부터 상기 함수키에 대한 제2 부분 키를 획득하는 단계; 사전 정의된 정수 집합의 원소인 임의의 정수를 선택하는 단계; 및 상기 임의의 정수, 상기 제1 부분 키 및 상기 제2 부분 키에 기초하여 상기 함수키를 생성하는 단계를 포함하고, 상기 제1 부분 키는, 상기 제1 사용자의 비밀키 및 상기 제2 사용자의 공개키에 기초하여 생성되고, 상기 제2 부분 키는, 상기 제2 사용자의 비밀키 및 상기 제1 사용자의 공개키에 기초하여 생성된다.

[0044] 상기 제1 사용자의 비밀키는 아래의 수학식 1

[0045] [수학식 1]

$$SK_i = \{\alpha_i, \beta_i, \gamma_i\}$$

[0046]

[0047] (이때, i는 상기 제1 사용자의 사용자 인덱스, SK_i는 상기 제1 사용자의 비밀키, α_i, β_i 및 γ_i 는 $\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}_p$ \mathbb{Z}_p 를 만족하는 임의의 정수, \mathbb{Z}_p 는 상기 정수 집합)을 만족하고, 상기 제1 사용자의 공개키는 아래의 수학식 2

[0048] [수학식 2]

$$PK_i = g^{\gamma_i}$$

[0049]

[0050] (이때, PK_i는 상기 제1 사용자의 공개키, g는 위수(order)가 소수 p인 곱선형 군(bilinear group) G의 생성원)를 만족하고, 상기 제2 사용자의 비밀키는 아래의 수학식 3

[0051] [수학식 3]

$$SK_j = \{\alpha_j, \beta_j, \gamma_j\}$$

[0052]

[0053] (이때, j는 상기 제2 사용자의 사용자 인덱스, SK_j는 상기 제2 사용자의 비밀키, α_j, β_j 및 γ_j 는 $\alpha_j, \beta_j, \gamma_j \in \mathbb{Z}_p$ \mathbb{Z}_p 를 만족하는 임의의 정수)을 만족하고, 상기 제2 사용자의 공개키는, 아래의 수학식 4

[0054] [수학식 4]

$$PK_j = g^{\gamma_j}$$

[0055]

[0056] (이때, PK_j는 상기 제2 사용자의 공개키)를 만족할 수 있다.

[0057] 상기 제1 부분키는, 상기 γ_i 및 상기 제2 사용자의 공개키 PK_j에 기초하여 제1 암호화 장치에 의해 생성된 공유키에 기초하여 생성되고, 상기 제2 부분키는, 상기 γ_j 및 상기 제1 사용자의 공개키 PK_i에 기초하여 제2 암호화 장치에 의해 생성된 상기 공유키에 기초하여 생성될 수 있다.

[0058] 상기 공유키는, 아래의 수학식 5

[0059] [수학식 5]

$$K_{i,j} = PK_j^{\gamma_i} = PK_i^{\gamma_j} = g^{\gamma_i \cdot \gamma_j}$$

[0060]

[0061] (이때, K_{i,j}는 상기 공유키)할 수 있다.

[0062] 상기 제1 부분키는 아래의 수학식 6

[0063] [수학식 6]

$$pDK_{i,(i,j)} = \{A_1 = \hat{g}^{a_i \cdot r}, A_2 = \hat{g}^{\beta_i \cdot s}, E = s \cdot \alpha_i + t \bmod p\}$$

[0064]

[0065] 을 만족하고, 상기 제2 부분키는 아래의 수학식 7

[0066] [수학식 7]

$$pDK_{j,(i,j)} = \{A'_1 = \hat{g}^{a_j \cdot r}, A'_2 = 1, E' = s \cdot a_j - t \bmod p\}$$

[0067] 삭제

[0068] 을 만족할 수 있다.

[0069] 상기 함수키는, 아래의 수학식 8

[0070] [수학식 8]

$$DK_{(i,j)} = \{K_1 = (A_1)^{r'}, K_2 = (A'_1)^{r'}, K_3 = (A_2)^{\frac{1}{E+E'}}\}$$

[0071]

[0072] (이때, $DK_{(i,j)}$ 는 상기 함수키, r' 는 상기 선택된 임의의 정수)을 만족할 수 있다.

[0073] 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 하나 이상의 프로그램은, 각각 사전 정의된 정수 집합의 원소인 제1 비밀 값, 제2 비밀 값 및 제3 비밀 값을 포함하는 제1 사용자의 비밀키를 생성하는 단계; 상기 제3 비밀 값에 기초하여 제1 사용자의 공개키를 생성하는 단계; 상기 정수 집합의 원소인 제4 비밀 값에 기초하여 생성된 제2 사용자의 공개키를 획득하는 단계; 상기 제3 비밀 값 및 상기 제2 사용자의 공개키에 기초하여 상기 제1 사용자와 상기 제2 사용자가 공유할 공유키를 생성하는 단계; 및 상기 제1 비밀 값, 제2 비밀 값 및 상기 공유키에 기초하여, 상기 제1 사용자의 비밀키를 이용하여 암호화된 제1 데이터 집합과 상기 제2 사용자의 비밀키를 이용하여 암호화된 제2 데이터 집합 사이의 교집합을 생성하기 위해 이용될 함수키에 대한 부분키를 생성하는 단계를 실행하기 위한 명령어들을 포함한다.

[0074] 상기 제1 사용자의 공개키는, 아래의 수학식 1

[0075] [수학식 1]

$$PK_i = g^{Y_i}$$

[0076]

[0077] (이때, i 는 상기 제1 사용자의 사용자 인덱스, PK_i 는 상기 제1 사용자의 공개키, g 는 위수(order)가 소수 p 인 곱셈형 군(bilinear group) G 의 생성원, Y_i 는 상기 제3 비밀 값)을 만족하고, 상기 제2 사용자의 공개키는, 아래의 수학식 2

[0078] [수학식 2]

$$PK_j = g^{Y_j}$$

[0079]

[0080] (이때, j 는 상기 제2 사용자의 사용자 인덱스, PK_j 는 상기 제2 사용자의 공개키, Y_j 는 상기 제4 비밀 값)를 만족할 수 있다.

[0081] 상기 공유키는 아래의 수학식 3

[0082] [수학식 3]

$$K_{i,j} = PK_j^{Y_i} = g^{Y_i \cdot Y_j}$$

[0083]

[0084] (이때, $K_{i,j}$ 는 상기 공유키)을 만족할 수 있다.

[0085] 상기 부분키를 생성하는 단계는, 상기 공유키에 기초하여, 각각 상기 정수 집합의 원소인 제1 부분키 생성 요소, 제2 부분키 생성 요소 및 제3 부분키 생성 요소를 생성하는 단계; 및 상기 제1 비밀 값, 상기 제2 비밀 값, 상기 제1 부분키 생성 요소, 상기 제2 부분키 생성 요소 및 상기 제3 부분키 생성 요소에 기초하여 상기 부분키를 생성하는 단계를 포함할 수 있다.

[0086] 상기 제1 부분키 생성 요소, 상기 제2 부분키 생성 요소 및 상기 제3 부분키 생성 요소는 아래의 수학식 4

[0087] [수학식 4]

$$r = PRF(K_{i,j}, 1)$$

[0088]

$$s = PRF(K_{i,j}, 2)$$

[0089]

$$t = PRF(K_{i,j}, 3)$$

[0090]

[0091] (이때, r은 상기 제1 부분키 생성 요소, s는 상기 제2 부분키 생성 요소, t는 상기 제3 부분키 생성 요소,

$$PRF: G \times [3] \rightarrow \mathbb{Z}_p$$

PRF()는 를 만족하는 의사 랜덤 함수(pseudo-random function), 는 상기 정수 집합)를 만족할 수 있다.

[0092] 상기 부분키는, 제1 부분키 요소, 제2 부분키 요소 및 제3 부분키 요소를 포함하고, 상기 제1 부분키 요소는, 아래의 수학식 5

[0093] [수학식 5]

$$A_1 = \hat{g}^{\alpha_i \cdot r}$$

[0094]

$$\hat{g} \quad \hat{G}$$

[0095] (이때, A_1 은 상기 제1 부분키 요소, 는 위수가 상기 소수 p인 곱셈형 군 의 생성원, r은 상기 제1 부분키 생성 요소, α_i 는 상기 제1 비밀 값)를 만족하고, 상기 제2 부분키 요소는, 아래의 수학식 6

[0096] [수학식 6]

$$A_2 = \begin{cases} \hat{g}^{\beta_i \cdot s}, & \text{if } i < j \\ 1, & \text{if } i > j \end{cases}$$

[0097] 삭제

[0098] (이때, A_2 는 상기 제2 부분키 요소, s는 상기 제2 부분키 생성 요소, β_i 는 상기 제2 비밀 값)을 만족하고, 상기 제3 부분키 요소는, 아래의 수학식 7

[0099] [수학식 7]

$$E = \begin{cases} s \cdot \alpha_i + t \bmod p, & \text{if } i < j \\ s \cdot \alpha_i - t \bmod p, & \text{if } i > j \end{cases}$$

[0100]

[0101] (이때, E는 상기 제3 부분키 요소, t는 상기 제3 부분키 생성 요소)을 만족할 수 있다.

[0102] 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 하나 이상의 프로그램은, 제1 암호화 장치로부터 제1 사용자의 비밀키를 이용하여 암호화된 제1 데이터 집합과 제2 사용자의 비밀키를 이용하여 암호화된 제2 데이터 집합 사이의 교집합을 생성하기 위해 이용될 함수키에 대한 제1 부분 키를 획득하는 단계; 제2 암호화 장치로부터 상기 함수키에 대한 제2 부분 키를 획득하는 단계; 사전 정의된 정수 집합의 원소인 임의의 정수를 선택하는 단계; 및 상기 임의의 정수, 상기 제1 부분 키 및 상기 제2 부분 키에 기초하여 상기 함수키를 생성하는 단계를 실행하기 위한 명령어들을 포함하고, 상기 제1 부분 키는, 상기 제1 사용자의 비밀키 및 상기 제2 사용자의 공개키에 기초하여 생성되고, 상기 제2 부분 키는, 상기 제2 사용자의 비밀키 및 상기 제1 사용자의 공개키에 기초하여 생성된다.

[0103] 상기 제1 사용자의 비밀키는 아래의 수학적 식 1

[수학적 식 1]

$$SK_i = \{\alpha_i, \beta_i, \gamma_i\}$$

[0105]

[0106] (이때, i는 상기 제1 사용자의 사용자 인덱스, SK_i는 상기 제1 사용자의 비밀키, α_i , β_i 및 γ_i 는 $\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}_p$ 를 만족하는 임의의 정수, \mathbb{Z}_p 는 상기 정수 집합)을 만족하고, 상기 제1 사용자의 공개키는 아래의 수학적 식 2

[수학적 식 2]

$$PK_i = g^{\gamma_i}$$

[0108]

[0109] (이때, PK_i는 상기 제1 사용자의 공개키, g는 위수(order)가 소수 p인 곱셈형 군(bilinear group) G의 생성원)를 만족하고, 상기 제2 사용자의 비밀키는 아래의 수학적 식 3

[수학적 식 3]

$$SK_j = \{\alpha_j, \beta_j, \gamma_j\}$$

[0111]

[0112] (이때, j는 상기 제2 사용자의 사용자 인덱스, SK_j는 상기 제2 사용자의 비밀키, α_j , β_j 및 γ_j 는 $\alpha_j, \beta_j, \gamma_j \in \mathbb{Z}_p$ 를 만족하는 임의의 정수)을 만족하고, 상기 제2 사용자의 공개키는, 아래의 수학적 식 4

[수학적 식 4]

$$PK_j = g^{\gamma_j}$$

[0114]

[0115] (이때, PK_j는 상기 제2 사용자의 공개키)를 만족할 수 있다.

[0116] 상기 제1 부분키는, 상기 γ_i 및 상기 제2 사용자의 공개키 PK_j에 기초하여 제1 암호화 장치에 의해 생성된 공유키에 기초하여 생성되고, 상기 제2 부분키는, 상기 γ_j 및 상기 제1 사용자의 공개키 PK_i에 기초하여 제2 암호화 장치에 의해 생성된 상기 공유키에 기초하여 생성될 수 있다.

[0117] 상기 공유키는, 아래의 수학적 식 5

[수학적 식 5]

$$K_{i,j} = PK_j^{\gamma_i} = PK_i^{\gamma_j} = g^{\gamma_i \cdot \gamma_j}$$

[0119]

[0120] (이때, $K_{i,j}$ 는 상기 공유키)할 수 있다.

[0121] 상기 제1 부분키는 아래의 수학식 6

[0122] [수학식 6]

$$pDK_{i,(i,j)} = \{A_1 = \hat{g}^{a_i \cdot r}, A_2 = \hat{g}^{\beta_i \cdot s}, E = s \cdot \alpha_i + t \bmod p\}$$

[0123]

[0124] 을 만족하고, 상기 제2 부분키는 아래의 수학식 7

[0125] [수학식 7]

$$pDK_{j,(i,j)} = \{A'_1 = \hat{g}^{a_j \cdot r}, A'_2 = 1, E' = s \cdot a_j - t \bmod p\}$$

[0126] 삭제

[0127] 을 만족할 수 있다.

[0128] 상기 함수키는, 아래의 수학식 8

[0129] [수학식 8]

$$DK_{(i,j)} = \{K_1 = (A_1)^{r'}, K_2 = (A'_1)^{r'}, K_3 = (A_2)^{\frac{1}{E+E'}}\}$$

[0130]

[0131] (이때, $DK_{(i,j)}$ 는 상기 함수키, r' 는 상기 선택된 임의의 정수)을 만족할 수 있다.

발명의 효과

[0132] 본 발명의 실시예들에 따르면, 암호문을 생성하는 각 사용자가 자신의 비밀키를 직접 생성하고, 각 사용자가 생성한 부분키를 결합하여 함수키를 생성함으로써 기존 교집합 연산을 지원하는 다중 사용자 함수 암호의 키 발급 과정에서 신뢰 기관이 필요한 문제점을 해결할 수 있다. 이를 통해 사용자는 신뢰 기관이 모든 암호문을 복호화하는 것으로부터 안전해질 수 있으며, 사용자가 교집합을 생성하는 서비스 제공자에 대한 데이터 접근 권한을 직접 제어할 수 있게 된다.

도면의 간단한 설명

[0133] 도 2는 일 실시예에 따른 부분키 및 함수키 생성 절차를 나타낸 절차도

도 3은 일 실시예에 따른 부분키 생성 과정을 나타낸 순서도

도 4는 일 실시예에 따른 함수키 생성 과정을 나타낸 순서도

도 5에 일 실시예에 따른 암호화 과정을 나타낸 순서도

도 6은 일 실시예에 따른 교집합 생성 과정을 나타낸 순서도

도 7은 일 실시예에 따른 교집합 S의 원소를 결정하는 과정을 나타낸 순서도

도 8은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0134] 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.

[0135] 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.

- [0136] 도 1은 일 실시예에 따른 암호 시스템의 구성도이다.
- [0137] 도 1을 참조하면, 본 발명의 일 실시예에 따른 암호 시스템(100)은 셋업(setup) 장치(110), 제1 암호화 장치(120), 제2 암호화 장치(130) 및 복호화 장치(140)를 포함한다.
- [0138] 암호 시스템(100)은 암호화된 두 데이터 집합을 암호화된 상태로 연산하여 해당 두 데이터 집합에 대한 교집합을 생성하는 함수 암호(Functional encryption)를 지원하기 위한 시스템이다.
- [0139] 셋업 장치(110)는 암호 시스템(100)에 대한 셋업(setup)을 수행하고, 암호 시스템(100) 내에서 사용할 공개 파라미터를 생성하기 위한 장치이다.
- [0140] 일 실시예에서, 셋업 장치(110)는 예를 들어, 신뢰 기관(Trusted Third Party)과 같이 신뢰할 수 있는 개체(entity)에 의해 운영될 수 있으나, 셋업 장치(110)의 운영 주체는 반드시 특정한 개체로 한정되는 것은 아니다.
- [0141] 제1 암호화 장치(120)는 제1 사용자에게 의해 이용되는 장치로서, 제1 사용자의 비밀키 및 공개키를 생성하고, 생성한 제1 사용자의 비밀키를 이용하여 암호화를 수행하기 위한 장치이다. 또한, 제2 암호화 장치(130)는 제2 사용자에게 의해 이용되는 장치로서, 제2 사용자의 비밀키 및 공개키를 생성하고, 생성한 제2 사용자의 비밀키를 이용하여 암호화를 수행하기 위한 장치이다.
- [0142] 제1 암호화 장치(120) 및 제2 암호화 장치(130)는 각각 제1 사용자의 비밀키를 이용하여 제1 암호화 장치(120)에 의해 암호화된 제1 데이터 집합과 제2 사용자의 비밀키를 이용하여 제2 암호화 장치(130)에 의해 암호화된 제2 데이터 집합 사이의 교집합을 생성하기 위해 이용될 함수키에 대한 부분키를 생성한 후 복호화 장치(140)로 제공한다.
- [0143] 한편, 도 1에 도시된 예에서는 설명의 편의를 위해 암호 시스템(100)에 포함된 암호화 장치(120, 130)가 2개인 것으로 예시하고 있으나, 암호화 장치(120, 130)의 개수는 실시예에 따라 변경될 수 있다.
- [0144] 복호화 장치(140)는 제1 사용자의 비밀키를 이용하여 제1 암호화 장치(120)에 의해 암호화된 제1 데이터 집합 및 제2 사용자의 비밀키를 이용하여 제2 암호화 장치(130)에 의해 암호화된 제2 데이터 집합을 이용하여 제1 데이터 집합과 제2 데이터 집합에 대한 교집합을 생성하기 위한 장치이다. 이를 위해, 복호화 장치(140)는 제1 암호화 장치(120) 및 제2 암호화 장치(130) 각각에 의해 생성된 부분키를 이용하여 함수키를 생성하고, 생성한 함수키를 이용하여 제1 데이터 집합과 제2 데이터 집합에 대한 교집합을 생성한다.
- [0145] 한편, 도 1에 도시된 암호 시스템(100)에 의해 수행되는 동작을 상세히 설명하면 아래와 같다.
- [0146] 셋업(setup)
- [0147] 셋업 장치(110)는 보안 상수(Security Parameter) 1^λ 및 암호 시스템(100) 내에서 암호화에 참여할 사용자의 총수 n (이때, n 은 2 이상인 정수)에 기초하여 공개 파라미터를 생성한다.
- [0148] 구체적으로, 셋업 장치(110)는 각각 위수(order)가 소수(prime number) p 인 곱선형 군(bilinear group) G , \hat{G} , G_T 및 $e: G \times \hat{G} \rightarrow G_T$ 를 만족하는 곱선형 함수(bilinear map) e , G 의 생성원(generator) g 및 \hat{G} 의 생성원 \hat{g} 를 생성할 수 있다.
- [0149] 또한, 셋업 장치(110)는 $H_1: \{0,1\}^* \rightarrow G$ 를 만족하는 제1 해시 함수(hash function) H_1 및 $H_2: G_T \rightarrow K$ (이때, K 는 대

칭키 암호 알고리즘의 키 공간(key space))를 만족하는 제2 해시 함수 H_2 를 선택할 수 있다.

[0150] 이때, 대칭키 암호 알고리즘은 예를 들어, AES(Advanced Encryption Standard) 알고리즘일 수 있으나, AES 알고리즘 외에도 암호화를 위한 암호화 키와 복호화를 위한 복호화 키가 동일하며, 선택 평문 공격(CPA, Chosen Plaintext Attack)에 대한 안전성을 제공하는 공지된 다양한 종류의 대칭키 암호 알고리즘이 이용될 수 있다.

$$PP = ((p, G, \hat{G}, G_T, e), g, \hat{g}, H_1, H_2, n)$$

[0151] 이후, 셋업 장치(110)는 공개 파라미터를 암호 시스템(100) 내에 공개할 수 있다.

[0152] 비밀키 및 공개키 생성

[0153] 제1 암호화 장치(120)는 사용자 인덱스가 i (이때, $i \in [n]$)인 제1 사용자의 비밀키 및 공개키를 생성하고, 제2 암호화 장치(130)는 사용자 인덱스가 j (이때, $i \in [n]$, $i \neq j$)인 제2 사용자의 비밀키 및 공개키를 생성한다.

[0154] 구체적으로, 제1 암호화 장치(120)는 공개 파라미터 PP 에 포함된 소수 p 에 의해 사전 정의된 정수 집합 $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ 에서 임의의 정수 α_i, β_i 및 γ_i 를 선택한 후(즉, $\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}_p$), 제1 사용자의 비밀키

$$SK_i = \{\alpha_i, \beta_i, \gamma_i\}$$

$$PK_i = g^{\gamma_i}$$

및 제1 사용자의 공개키를 생성할 수 있다. 이후, 제1 암호화 장치(120)는 제1 사용자의 비밀키 SK_i 는 안전하게 보관하고, 공개키 PK_i 는 암호화 시스템(100) 내에 공개할 수 있다.

[0155] 또한, 제2 암호화 장치(130)는 정수 집합 \mathbb{Z}_p 에서 임의의 정수 α_j, β_j 및 γ_j 를 선택한 후(즉, $\alpha_j, \beta_j, \gamma_j \in \mathbb{Z}_p$), 제2 사용자의 비밀키 $SK_j = \{\alpha_j, \beta_j, \gamma_j\}$ 및 제2 사용자의 공개키 $PK_j = g^{\gamma_j}$ 를 생성할 수 있다. 이후, 제2 암호화 장치(130)는 제2 사용자의 비밀키 SK_j 는 안전하게 보관하고, 공개키 PK_j 는 암호화 시스템(100) 내에 공개할 수 있다.

[0156] 암호화

[0157] 제1 암호화 장치(120) 및 제2 암호화 장치(130)는 각각 하나 이상의 데이터를 포함하는 데이터 집합에 대한 라벨(label) 및 사용자 비밀키에 기초하여 데이터 집합에 대한 암호문을 생성한다.

[0158] 이때, 데이터 집합에 대한 라벨은 암호 시스템(100) 내에서 미리 설정되거나 암호화에 참여할 복수의 사용자 사이에 사전 합의된 방식 내지는 규칙에 따라 암호화 대상인 데이터 집합에 부여되는 정보로서, 예를 들어, 데이터 집합에 대한 분류 정보, 데이터 집합과 관련된 시간 등과 관련된 정보일 수 있으나 반드시 특정한 정보로 한정되는 것은 아니다.

[0159] 한편, 본 발명의 실시예에서, 교집합은 라벨이 동일한 두 데이터 집합에 대해서만 생성될 수 있다.

[0160] 제1 암호화 장치(120)는 사용자 인덱스가 i 인 제1 사용자의 비밀키 SK_i 를 이용하여 데이터 집합 $X_i = \{x_{i,1}, \dots, x_{i,\ell_i}\}$ (이때, $|X_i| = \ell_i$, ℓ_i 는 2 이상인 정수)에 포함된 각 원소 x_{i,k_i} (이때, $k_i \in [\ell_i]$)에 대한 제

$$C_{i,k_i}$$

$$D_{i,k_i}$$

1 암호문 요소 및 제2 암호문 요소를 생성할 수 있다.

[0161] 구체적으로, 제1 암호화 장치(120)는 우선, 암호화할 데이터 집합 X_i 에 대한 라벨 T 및 제1 사용자의 비밀키 SK_i 에 포함된 비밀 값 α_i 에 기초하여 데이터 집합 X_i 에 포함된 각 원소 x_{i,k_i} 에 대한 제1 암호문 요소 C_{i,k_i} 를 생성할 수 있다.

[0162] 이때, 제1 암호문 요소 C_{i,k_i} 는 예를 들어, 아래의 수학식 1을 이용하여 생성될 수 있다.

[0163] [수학식 1]

$$C_{i,k_i} = H_1(T \parallel x_{i,k_i})^{\alpha_i}$$

[0164]

[0165] 여기서, " \parallel "는 두 값 사이의 연결(concatenation)을 나타내며, 이하 동일한 의미로 사용된다.

[0166] 또한, 제1 암호화 장치(120)는 데이터 집합 X_i 에 대한 라벨 T 및 제1 사용자의 비밀키 SK_i 에 포함된 비밀 값 β_i

에 기초하여 데이터 집합 X_i 에 포함된 각 원소 x_{i,k_i} 에 대응되는 대칭키 TK_{i,k_i} 를 생성할 수 있다.

[0167] 이때, 대칭키 TK_{i,k_i} 는 예를 들어, 아래의 수학식 2를 이용하여 생성될 수 있다.

[0168] [수학식 2]

$$TK_{i,k_i} = H_2(e(H_1(T, x_{i,k_i}), \hat{g})^{\beta_i})$$

[0169]

[0170] 이후, 제1 암호화 장치(120)는 x_{i,k_i} 에 대응되는 대칭키 TK_{i,k_i} 를 암호화 키로 이용한 대칭키 암호 알고리즘을 이

용하여 각 원소 x_{i,k_i} 에 대한 제2 암호문 요소 D_{i,k_i} 를 생성할 수 있다.

[0171] 이때, 제2 암호문 요소 D_{i,k_i} 는 예를 들어, 아래의 수학식 3을 이용하여 생성될 수 있다.

[0172] [수학식 3]

$$D_{i,k_i} = Enc(TK_{i,k_i}, T \parallel x_{i,k_i})$$

[0173]

[0174] 수학식 3에서, $Enc()$ 는 대칭키 암호 알고리즘을 이용한 암호화를 나타내며, $Enc(TK_{i,k_i}, T \parallel x_{i,k_i})$ 는 TK_{i,k_i} 를 암호

화 키로 이용하여 $T \parallel x_{i,k_i}$ 를 암호화함을 의미한다.

[0175] 이후, 제1 암호화 장치(120)는 데이터 집합 X_i 에 대한 라벨 T , 데이터 집합 X_i 에 포함된 각 원소 x_{i,k_i} 에 대한 제

1 암호문 요소 C_{i,k_i} 및 제2 암호문 요소 D_{i,k_i} 를 포함하는 암호문 $CT_{i,T}$ 를 생성할 수 있다.

[0176] 구체적으로, 데이터 집합 X_i 에 대한 암호문 $CT_{i,T}$ 는 아래의 수학식 4를 만족할 수 있다.

[0177] [수학식 4]

$$CT_{i,T} = (T, \{C_{i,k_i}, D_{i,k_i}\}_{k_i=1}^{\ell_i})$$

[0178]

[0179] 한편, 제2 암호화 장치(130)는 사용자 인덱스가 j 인 제2 사용자의 비밀키 SK_j 를 이용하여 데이터 집합

$X_j = \{x_{j,1}, \dots, x_{i,\ell_j}\}$ (이때, $|X_j| = \ell_j$, ℓ_j 는 2 이상인 정수)에 포함된 각 원소 x_{j,k_j} ($k_j \in [\ell_j]$)에 대한 제

1 암호문 요소 C_{j,k_j} 및 제2 암호문 요소 D_{j,k_j} 를 생성할 수 있다.

[0180] 구체적으로, 제2 암호화 장치(130)는 암호화할 데이터 집합 X_j 에 대한 라벨 T' 및 제2 사용자의 비밀키 SK_j 에 포함된 비밀 값 α_j 에 기초하여 데이터 집합 X_j 에 포함된 각 원소 x_{j,k_j} 에 대한 제1 암호문 요소 C_{j,k_j} 를 생성할 수 있다.

[0181] 이때, 제1 암호문 요소 C_{j,k_j} 는 예를 들어, 아래의 수학식 5를 이용하여 생성될 수 있다.

[0182] [수학식 5]

$$C_{j,k_j} = H_1(T' \parallel x_{j,k_j})^{\alpha_j}$$

[0183]

[0184] 또한, 제2 암호화 장치(130)는 데이터 집합 X_j 에 대한 라벨 T' 및 사용자 비밀키 SK_j 에 포함된 비밀 값 β_j 에 기

초하여 데이터 집합 X_j 에 포함된 각 원소 x_{j,k_j} 에 대응되는 대칭키 TK_{j,k_j} 를 생성할 수 있다.

[0185] 이때, 대칭키 TK_{j,k_j} 는 예를 들어, 아래의 수학식 6을 이용하여 생성될 수 있다.

[0186] [수학식 6]

$$TK_{j,k_j} = H_2(e(H_1(T', x_{j,k_j}), \hat{g}))^{\beta_j}$$

[0187]

[0188] 이후, 제2 암호화 장치(130)는 각 원소 x_{j,k_j} 에 대응되는 대칭키 TK_{j,k_j} 를 암호화 키로 이용한 대칭키 암호 알고

리즘을 이용하여 각 원소 x_{j,k_j} 에 대한 제2 암호문 요소 D_{j,k_j} 를 생성할 수 있다.

[0189] 이때, 제2 암호문 요소 D_{j,k_j} 는 예를 들어, 아래의 수학식 7을 이용하여 생성될 수 있다.

[0190] [수학식 7]

$$D_{j,k_j} = Enc(TK_{j,k_j}, T' \parallel x_{j,k_j})$$

[0191]

[0192] 이후, 제2 암호화 장치(130)는 데이터 집합 X_j 에 대한 라벨 T' , 데이터 집합 X_j 에 포함된 각 원소 x_{j,k_j} 에 대한

제1 암호문 요소 C_{j,k_j} 및 제2 암호문 요소 D_{j,k_j} 를 포함하는 암호문 $CT_{j,T'}$ 를 생성할 수 있다.

[0193] 구체적으로, 암호문 $CT_{j,T'}$ 는 아래의 수학식 8을 만족할 수 있다.

[0194] [수학식 8]

$$CT_{j,T'} = \left(T', \{C_{j,k_j}, D_{j,k_j}\}_{k_j=1}^{\ell_j} \right)$$

[0195]

[0196] 부분키 생성

[0197] 제1 암호화 장치(120) 및 제2 암호화 장치(130)는 각각 제1 암호화 장치(120)에 의해 생성된 데이터 집합 X_i 에 대한 암호문 $CT_{i,T}$ 와 제2 암호화 장치(130)에 의해 생성된 데이터 집합 X_j 에 대한 암호문 $CT_{j,T'}$ 를 이용하여 데이터 집합 X_i 과 데이터 집합 X_j 사이의 교집합을 생성하기 위해 이용될 함수키 $DK_{(i,j)}$ 에 대한 부분키를 생성한다.

[0198] 일 실시예에 따르면, 제1 암호화 장치(120)는 제1 사용자의 비밀키 SK_i 및 제2 사용자의 공개키 PK_j 에 기초하여 함수키 $DK_{(i,j)}$ 에 대한 제1 부분키 $pDK_{i,(i,j)}$ 를 생성하고, 제2 암호화 장치(130)는 제2 사용자의 비밀키 SK_j 및 제1 사용자의 공개키 PK_i 에 기초하여 함수키 $DK_{(i,j)}$ 에 대한 제2 부분키 $pDK_{j,(i,j)}$ 를 생성할 수 있다.

[0199] 구체적으로, 제1 암호화 장치(120)는 제1 사용자 비밀키 SK_i 에 포함된 비밀 값 y_i 와 제2 사용자의 공개키 PK_j 에 기초하여 제1 사용자와 제2 사용자가 공유할 공유키 $K_{i,j}$ 를 생성하고, 제2 암호화 장치(130)는 제2 사용자 비밀키 SK_j 에 포함된 비밀 값 y_j 와 제1 사용자의 공개키 PK_i 에 기초하여 공유키 $K_{i,j}$ 를 생성할 수 있다. 이때, 제1 암호화 장치(120)는 아래의 수학식 9를 이용하여 공유키 $K_{i,j}$ 를 생성하고, 제2 암호화 장치(130)는 아래의 수학식 10을 이용하여 공유키 $K_{i,j}$ 를 생성할 수 있다.

[0200] [수학식 9]

$$K_{i,j} = PK_j^{y_i} = g^{y_i \cdot y_j}$$

[0201]

[0202] [수학식 10]

$$K_{i,j} = PK_i^{y_j} = g^{y_i \cdot y_j}$$

[0203]

[0204] 이후, 제1 암호화 장치(120) 및 제2 암호화 장치(130)는 각각 공유키 $K_{i,j}$ 를 이용하여 \mathbb{Z}_p 의 원소인 부분키 생성

$$r, s, t \in \mathbb{Z}_p$$

요소 r, s 및 t (즉,)를 생성할 수 있다. 이때, 부분키 생성 요소 r, s 및 t 는 각각 아래의 수학식 11 내지 13을 통해 생성될 수 있다.

[0205] [수학식 11]

$$r = PRF(K_{i,j}, 1)$$

[0206]

[0207] [수학식 12]

$$s = PRF(K_{i,j}, 2)$$

[0208]

[0209] [수학식 13]

$$t = PRF(K_{i,j}, 3)$$

[0210]

$$PRF: G \times [3] \rightarrow \mathbb{Z}_p$$

[0211] 수학식 11 내지 13에서, $PRF()$ 는 을 만족하는 의사 랜덤 함수(pseudo-random function)를

나타내며, 이하 동일한 의미로 사용된다.

[0212] 이후, 제1 암호화 장치(120)는 제1 사용자의 비밀키 SK_i 에 포함된 비밀 값 α_i , β_i 와 부분키 생성 요소 r , s , t 를 이용하여 함수키 $DK_{(i,j)}$ 에 대한 제1 부분키 $pDK_{i,(i,j)}$ 를 생성할 수 있다.

[0213] 예를 들어, 제1 부분키 $pDK_{i,(i,j)}$ 는 $i < j$ 인 경우, 아래의 수학식 14를 이용하여 생성될 수 있고, $i > j$ 인 경우, 아래의 수학식 15를 이용하여 생성될 수 있다.

[0214] [수학식 14]

$$pDK_{i,(i,j)} = \{A_1 = \hat{g}^{\alpha_i \cdot r}, A_2 = \hat{g}^{\beta_i \cdot s}, E = s \cdot \alpha_i + t \bmod p\}$$

[0215]

[0216] [수학식 15]

$$pDK_{j,(i,j)} = \{A_1 = \hat{g}^{\alpha_j \cdot r}, A_2 = 1, E = s \cdot \alpha_j - t \bmod p\}$$

[0217] 삭제

[0218] 한편, 제2 암호화 장치(130)는 제2 사용자의 비밀키 SK_j 에 포함된 비밀 값 α_j , β_j 와 부분키 생성 요소 r , s , t 를 이용하여 함수키 $DK_{(i,j)}$ 에 대한 제2 부분키 $pDK_{j,(i,j)}$ 를 생성할 수 있다.

[0219] 예를 들어, 제2 부분키 $pDK_{j,(i,j)}$ 는 $i < j$ 인 경우, 아래의 수학식 16을 이용하여 생성될 수 있고, $i > j$ 인 경우, 아래의 수학식 17을 이용하여 생성될 수 있다.

[0220] [수학식 16]

$$pDK_{j,(i,j)} = \{A'_1 = \hat{g}^{\alpha_j \cdot r}, A'_2 = 1_{\hat{G}}, E' = s \cdot \alpha_j - t \bmod p\}$$

[0221]

[0222] [수학식 17]

$$pDK_{j,(i,j)} = \{A'_1 = \hat{g}^{\alpha_j \cdot r}, A'_2 = 1, E' = s \cdot \alpha_j - t \bmod p\}$$

[0223] 삭제

[0224] 함수키 생성

[0225] 복호화 장치(140)는 제1 암호화 장치(120)로부터 제1 부분키 $pDK_{i,(i,j)}$ 를 획득하고, 제2 암호화 장치(130)로부터 제2 부분키 $pDK_{j,(i,j)}$ 를 획득한다. 이후, 복호화 장치(140)는 제1 부분키 $pDK_{i,(i,j)}$ 및 제2 부분키 $pDK_{j,(i,j)}$ 에 기초하여 함수키 $DK_{(i,j)}$ 를 생성한다.

$$r' \in \mathbb{Z}_p$$

[0226] 구체적으로, 복호화 장치(140)는 $r' \in \mathbb{Z}_p$ 를 만족하는 임의의 정수 r' 를 선택한 후, r' , $pDK_{i,(i,j)}$ 및 $pDK_{j,(i,j)}$ 에 기초하여 함수키 $DK_{(i,j)}$ 를 생성할 수 있다. 예를 들어, 함수키 $DK_{(i,j)}$ 는 아래의 수학식 18을 이용하여 생성될 수 있다.

[0227] [수학식 18]

$$DK_{(i,j)} = \{K_1 = (A_1)^{r'}, K_2 = (A'_1)^{r'}, K_3 = (A_2)^{1/(E+E')}\}$$

[0228]

[0229] 복호화

[0230] 복호화 장치(140)는 함수키 $DK_{(i,j)}$, 암호문 $CT_{i,T}$ 및 암호문 $CT_{j,T'}$ 을 이용하여 데이터 집합 X_i 와 데이터 집합 X_j

사이의 교집합 $S=(X_i \cap X_j)$ 을 생성한다.

[0231] 구체적으로, 복호화 장치(140)는 우선, 암호문 $CT_{i,T}$ 에 포함된 라벨 T와 암호문 $CT_{j,T'}$ 에 포함된 라벨 T'가 동일
한지 여부를 판단할 수 있다.

[0232] 이때, $T \neq T'$ 인 경우, 복호화 장치(140)은 교집합 생성이 불가능함을 나타내는 오류 메시지를 생성할 수 있다.

[0233] 반면, $T=T'$ 인 경우, 복호화 장치(140)는 암호문 $CT_{i,T}$ 에 포함된 모든 제1 암호문 요소 C_{i,k_i} 에 대해 아래의 수학
식 19를 이용한 제1 페어링(pairing) 연산을 수행하고, 암호문 $CT_{j,T}$ 에 포함된 모든 제1 암호문 요소 C_{j,k_j} 에 대
해 아래의 수학식 20을 이용한 제2 페어링 연산을 수행할 수 있다.

[0234] [수학식 19]

$$E_{i,k_i} = e(C_{i,k_i}, K_2)$$

[0235]

[0236] [수학식 20]

$$E_{j,k_j} = e(C_{j,k_j}, K_1)$$

[0237]

[0238] 이후, 복호화 장치(140)는 암호문 $CT_{i,T}$ 에 포함된 모든 제1 암호문 요소 C_{i,k_i} 에 대해 수행된 제1 페어링 연산의

$$E_i = \{E_{i,k_i}\}_{k_i=1}^{\ell_i}$$

결과들을 포함하는 제1 결과 집합

및 암호문 $CT_{j,T}$ 에 포함된 모든 제1 암호문 요소 C_{j,k_j} 에 대해

$$E_j = \{E_{j,k_j}\}_{k_j=1}^{\ell_j}$$

수행된 제2 페어링 연산의 결과들을 포함하는 제2 결과 집합 E_j 을 생성하고, 제1 결과 집합과 상
기 제2 결과 집합 사이의 교집합인 제3 결과 집합 $F=E_i \cap E_j$ 을 생성할 수 있다.

[0239] 이후, 복호화 장치(140)는 제3 결과 집합 F가 공집합인지 여부를 판단하고, 공집합인 경우(즉, $F = \emptyset$), 데이터

$$S = \emptyset$$

집합 X_i 와 데이터 집합 X_j 사이의 교집합 S가 공집합인 것으로 판단할 수 있다(즉, $S = \emptyset$).

$$F \neq \emptyset$$

[0240] 반면, 제3 결과 집합 F가 공집합이 아닌 경우(즉, $F \neq \emptyset$), 복호화 장치(140)는 제3 결과 집합 F에 기초하여 데
이터 집합 X_i 와 데이터 집합 X_j 사이의 교집합 S를 생성할 수 있다.

[0241] 구체적으로, 복호화 장치(140)는 제3 결과 집합 F에 포함된 각 원소에 대해 아래의 수학식 21을 만족하는

$$C_{j,k_j}$$

를 선택할 수 있다.

[0242] [수학식 21]

$$F_k = E_{i,k_i} = E_{j,k_j}$$

[0243]

[0244] 수학식 21에서, F_k 는 제3 결과 집합 F에 포함된 k(이때, k는 $1 \leq k \leq |F|$ 을 만족하는 자연수) 번째 원소를 나타낸

다.

[0245] 이후, 복호화 장치(140)는 선택된 C_{i,k_i} 에 대응되는 D_{i,k_i} 를 복호화하기 위한 복호화 키 TK_{k_i,k_j} 를 생성하고, 생성된 복호화 키 TK_{k_i,k_j} 를 이용하여 D_{i,k_i} 를 복호화할 수 있다.

[0246] 구체적으로, 복호화 장치(140)는 아래의 수학적식 22를 이용하여 복호화 키 TK_{k_i,k_j} 를 생성할 수 있다.

[0247] [수학적식 22]

$$TK_{k_i,k_j} = H_2(e(C_{i,k_i} \cdot C_{j,k_j}, K_3))$$

[0248]

[0249] 또한, 복호화 장치(140)는 아래의 수학적식 23을 이용하여 D_{i,k_i} 를 복호화할 수 있다.

[0250] [수학적식 23]

$$Dec(TK_{k_i,k_j}, D_{i,k_i}) = (A_{k_i,k_j} \parallel B_{k_i,k_j})$$

[0251]

[0252] 수학적식 23에서, Dec()는 대칭키 암호 알고리즘을 이용한 복호화를 나타내며, $Dec(TK_{k_i,k_j}, D_{i,k_i})$ 는 TK_{k_i,k_j} 를 복호화 키로 이용하여 D_{i,k_i} 를 복호화함을 의미한다.

[0253] 한편, 복호화 장치(140)는 D_{i,k_i} 를 복호화한 결과 $A_{k_i,k_j} = T$ 인 경우, B_{k_i,k_j} 를 데이터 집합 X_i 와 데이터 집합 X_j 사이의 교집합 S의 원소로 결정할 수 있다.

[0254] 도 2는 일 실시예에 따른 부분키 및 함수키 생성 절차를 나타낸 절차도이다.

[0255] 도 2를 참조하면, 우선, 셋업 장치(110)는 상술한 셋업 절차를 수행하여 공개 파라미터 PP를 생성한다(201).

[0256] 이후, 셋업 장치(110)는 생성한 공개 파라미터 PP를 제1 암호화 장치(120), 제2 암호화 장치(130) 및 복호화 장치(140)로 제공한다(202, 203, 204).

[0257] 이후, 제1 암호화 장치(120)는 제1 사용자의 비밀키 SK_i 및 공개키 PK_i 를 생성하고(205), 제2 암호화 장치(130)는 제2 사용자의 비밀키 SK_j 및 공개키 PK_j 를 생성한다(206).

[0258] 이후, 제1 암호화 장치(120)는 제1 사용자의 공개키 PK_i 를 제2 암호화 장치(130)로 제공하고(207), 제2 암호화 장치(130)는 제2 사용자의 공개키 PK_j 를 제1 암호화 장치로 제공한다(208).

[0259] 이후, 제1 암호화 장치(120)는 함수키 $DK_{(i,j)}$ 에 대한 제1 부분키 $pDK_{i,(i,j)}$ 를 생성하고(209), 제2 암호화 장치(130)는 함수키 $DK_{(i,j)}$ 에 대한 제2 부분키 $pDK_{j,(i,j)}$ 를 생성한다(210).

[0260] 이후, 제1 암호화 장치(120)는 제1 부분키 $pDK_{i,(i,j)}$ 를 복호화 장치(140)로 제공하고(211), 제2 암호화 장치(130)는 제2 부분키 $pDK_{j,(i,j)}$ 를 복호화 장치(140)로 제공한다(212).

[0261] 이후, 복호화 장치(140)는 제1 부분키 $pDK_{i,(i,j)}$ 및 제2 부분키 $pDK_{j,(i,j)}$ 를 이용하여 함수키 $DK_{(i,j)}$ 를 생성한다(213).

[0262] 한편, 도 2에 도시된 절차도에서 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함

게 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 추가되어 수행될 수 있다.

[0263] 도 3은 일 실시예에 따른 부분키 생성 과정을 나타낸 순서도이다.

[0264] 도 3에 도시된 부분키 생성 과정은 예를 들어, 도 2에 도시된 209 단계에서 제1 암호화 장치(120)에 의해 수행되거나, 210 단계에서 제2 암호화 장치(130)에 의해 수행될 수 있다. 이하에서는, 설명의 편의를 위해 제1 암호화 장치(120)에서 부분키 생성 과정을 수행하는 것으로 가정하여 설명한다.

[0265] 도 3을 참조하면, 우선, 제1 암호화 장치(120)는 제1 사용자의 비밀키 SK_i 에 포함된 비밀 값인 x_i 와 제2 사용자의 공개키 PK_j 에 기초하여 공유키 $K_{i,j}$ 를 생성한다 (310).

[0266] 이후, 제1 암호화 장치(120)는 생성한 공유키 $K_{i,j}$ 를 이용하여, 부분키 생성 요소 r , s 및 t 를 생성한다(320).

[0267] 이후, 제1 암호화 장치(120)는 각각 제1 사용자의 비밀키 SK_i 에 포함된 비밀 값인 α_i 및 β_i 와 생성한 부분키 생성 요소 r , s 및 t 에 기초하여 부분키 요소 A_1 , A_2 및 E 를 생성하고, 부분키 요소 A_1 , A_2 및 E 를 포함하는 제1 부분키 $pDK_{i,(i,j)}$ 를 생성한다(330).

[0268] 한편, 도 3에 도시된 순서도에서 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 추가되어 수행될 수 있다.

[0269] 도 4는 일 실시예에 따른 함수키 생성 과정을 나타낸 순서도이다.

[0270] 도 4에 도시된 함수키 생성 과정은 예를 들어, 도 2에 도시된 213 단계에서 복호화 장치(140)에 의해 수행될 수 있다.

[0271] 도 4를 참조하면, 우선, 복호화 장치(140)는 \mathbb{Z}_p 의 원소인 임의의 정수 r' (즉, $r' \in \mathbb{Z}_p$)를 선택한다(410).

[0272] 이후, 복호화 장치(140)는 제1 암호화 장치(120)로부터 획득한 제1 부분키 $pDK_{i,(i,j)}$, 제2 암호화 장치(130)로부터 획득한 제2 부분키 $pDK_{j,(i,j)}$ 및 r' 에 기초하여 함수키 $DK_{(i,j)}$ 를 생성한다(420).

[0273] 한편, 도 4에 도시된 순서도에서 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 추가되어 수행될 수 있다.

[0274] 도 5에 일 실시예에 따른 암호화 과정을 나타낸 순서도이다.

[0275] 도 5에 도시된 암호화 과정은 제1 암호화 장치(120) 또는 제2 암호화 장치(130)에 의해 수행될 수 있으나, 이하에서는, 설명의 편의를 위해 제1 암호화 장치(120)에서 암호화 과정을 수행하는 것으로 가정하여 설명한다.

[0276] 도 5를 참조하면, 우선, 제1 암호화 장치(120)는 데이터 집합 X_i 에 포함된 각 원소에 대한 인덱스 값 k_i 를 1로 초기화한다(501).

[0277] 이후, 제1 암호화 장치(120)는 데이터 집합 X_i 에 대한 라벨 T 및 제1 사용자의 비밀키 SK_i 에 포함된 비밀 값 α_i

에 기초하여, 데이터 집합 X_i 에 포함된 원소들 중 인덱스 값이 k_i 인 원소 x_{i,k_i} 에 대한 제1 암호문 요소 c_{i,k_i} 를 생성한다(502).

[0278] 이후, 제1 암호화 장치(120)는 데이터 집합 X_i 에 대한 라벨 T 및 비밀키 SK_i 에 포함된 비밀 값 β_i 에 기초하여,

x_{i,k_i} 에 대응되는 대칭키 TK_{i,k_i} 를 생성한다(503).

[0279] 이후, 제1 암호화 장치(120)는 생성된 대칭키 TK_{i,k_i} 를 암호화 키로 이용한 대칭키 암호 알고리즘을 이용하여

x_{i,k_i} 에 대한 제2 암호문 요소 D_{i,k_i} 를 생성한다(504).

[0280] 이후, 제1 암호화 장치(120)는 인덱스 값 k_i 가 데이터 집합 X_i 에 포함된 원소들의 개수 ℓ_i 와 동일한지 여부를 판단한다(505).

[0281] 이때, $k_i \neq \ell_i$ 인 경우, 제1 암호화 장치(120)는 k_i 를 1만큼 증가시킨 후(506), 502 단계로 되돌아 간다.

[0282] 반면, $k_i = \ell_i$ 인 경우, 제1 암호화 장치(120)는 데이터 집합 X_i 에 대한 암호문 $CT_{i,T}$ 를 생성한다(507).

[0283] 이때, 암호문 $CT_{i,T}$ 는 데이터 집합 X_i 에 대한 라벨 T , 데이터 집합 X_i 에 포함된 각 원소 x_{i,k_i} 에 대한 제1 암호문 요소 C_{i,k_i} 및 제2 암호문 요소 D_{i,k_i} 를 포함할 수 있다.

[0284] 한편, 도 5에 도시된 순서도에서 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 추가되어 수행될 수 있다.

[0285] 도 6은 일 실시예에 따른 교집합 생성 과정을 나타낸 순서도이다.

[0286] 도 6을 참조하면, 우선, 복호화 장치(140)는 데이터 집합 X_i 에 대한 암호문 $CT_{i,T}$ 에 포함된 라벨 T 와 데이터 집합 X_j 에 대한 암호문 $CT_{j,T'}$ 에 포함된 라벨 T' 가 동일한지 여부를 판단한다(610).

[0287] 이때, $T \neq T'$ 인 경우, 복호화 장치(140)은 교집합 생성이 불가능한 것으로 판단하고, 교집합 생성 절차를 종료한다. 이 경우, 실시예에 따라, 복호화 장치(140)는 교집합 생성이 불가능함을 나타내는 오류 메시지를 생성할 수 있다.

[0288] 반면, $T = T'$ 인 경우, 복호화 장치(140)는 교집합 S 를 공집합으로 설정한 후 (620), 암호문 $CT_{i,T}$ 에 포함된 모든

제1 암호문 요소 C_{i,k_i} 에 대해 상술한 수학식 19를 이용한 제1 페어링(pairing) 연산을 수행하고, 암호문 $CT_{j,T'}$

에 포함된 모든 제1 암호문 요소 C_{j,k_j} 에 대해 상술한 수학식 20을 이용한 제2 페어링 연산을 수행하여, 제1 결

과 집합 $E_i = \{E_{i,k_i}\}_{k_i=1}^{\ell_i}$ 및 제2 결과 집합 $E_j = \{E_{j,k_j}\}_{k_j=1}^{\ell_j}$ 를 생성한다(630).

[0289] 이후, 복호화 장치(140)는 제1 결과 집합 E_i 과 상기 제2 결과 집합 E_j 사이의 교집합인 제3 결과 집합 $F = E_i \cap E_j$ 을 생성한다(640).

[0290] 이후, 복호화 장치(140)는 제3 결과 집합 F 가 공집합인지 여부를 판단하고(650), 공집합이 아닌 경우(즉, $F \neq \emptyset$), 제3 결과 집합 F 에 기초하여 교집합 S 의 원소를 결정한다(660).

[0291] 반면, 제3 결과 집합 F 가 공집합인 경우(즉, $F = \emptyset$), 복호화 장치(140)는 교집합 S 를 출력한다(670). 즉, 이 경우, 복호화 장치(140)는 공집합인 S (즉, $S = \emptyset$)를 출력할 수 있다.

[0292] 한편, 도 6에 도시된 순서도에서 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 추가되어 수행될 수 있다.

- [0293] 도 7은 일 실시예에 따른 교집합 S의 원소를 결정하는 과정을 나타낸 순서도이다.
- [0294] 도 7에 도시된 과정은 예를 들어, 도 6에 도시된 660 단계에서 복호화 장치(140)에 의해 수행될 수 있다.
- [0295] 도 6을 참조하면, 우선, 복호화 장치(140)는 제3 결과 집합 F의 원소에 대한 인덱스 값 k를 1로 초기화한다(661).
- [0296] 이후, 복호화 장치(140)는 $F_k = E_{i,k_i} = E_{j,k_j}$ 를 만족하는 C_{i,k_i} 및 C_{j,k_j} 를 선택한다(662).
- [0297] 이후, 복호화 장치(140)는 선택된 C_{i,k_i} 에 대응되는 D_{i,k_i} 를 복호화하기 위한 복호화 키 TK_{k_i,k_j} 를 선택된 C_{j,k_j} 를 이용하여 생성한다(663).
- [0298] 이후, 복호화 장치(140)는 선택된 C_{i,k_i} 에 대응되는 D_{i,k_i} 를 복호화 키 TK_{k_i,k_j} 를 이용하여 복호화한다(664).
- [0299] 이후, 복호화 장치(140)는 D_{i,k_i} 를 복호화한 결과인 $(A_{k_i,k_j} \parallel B_{k_i,k_j})$ 에 기초하여, $A_{k_i,k_j} = T$ 를 만족하는지 여부를 판단한다(665).
- [0300] 이때, $A_{k_i,k_j} = T$ 인 경우, 복호화 장치(140)는 B_{k_i,k_j} 를 교집합 S의 원소로 추가한다(666).
- [0301] 이후, 복호화 장치(140)는 인덱스 값 k가 제3 결과 집합 F에 포함된 원소들의 개수 |F|와 동일한지 여부를 판단한다(667).
- [0302] 이때, $k \neq |F|$ 인 경우, 복호화 장치(140)는 k를 1만큼 증가시킨 후(668), 662 단계로 되돌아 간다.
- [0303] 반면, $k = |F|$ 인 경우, 복호화 장치(140)는 S를 두 데이터 집합 X_i 와 X_j 에 대한 교집합(즉, $S = (X_i \cap X_j)$)으로 출력한다(670).
- [0304] 한편, 도 7에 도시된 순서도에서 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 추가되어 수행될 수 있다.
- [0305] 도 8은 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 않은 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.
- [0306] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 암호 시스템(100)에 포함되는 하나 이상의 컴포넌트일 수 있다.
- [0307] 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.
- [0308] 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.

[0309] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0310] 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.

[0311] 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.

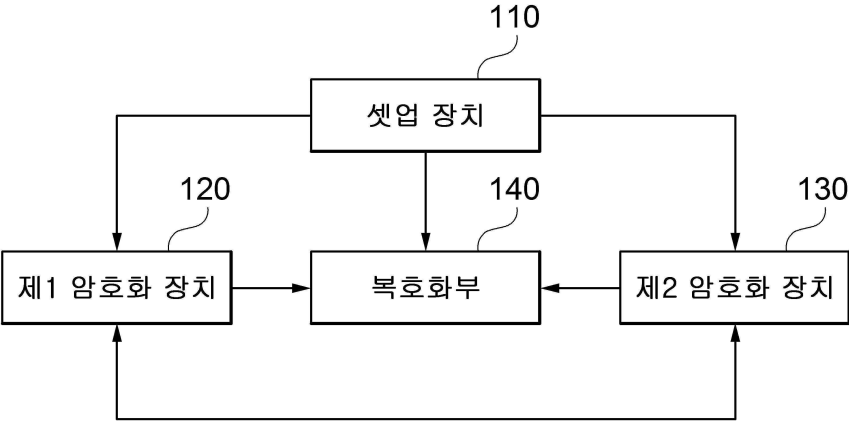
부호의 설명

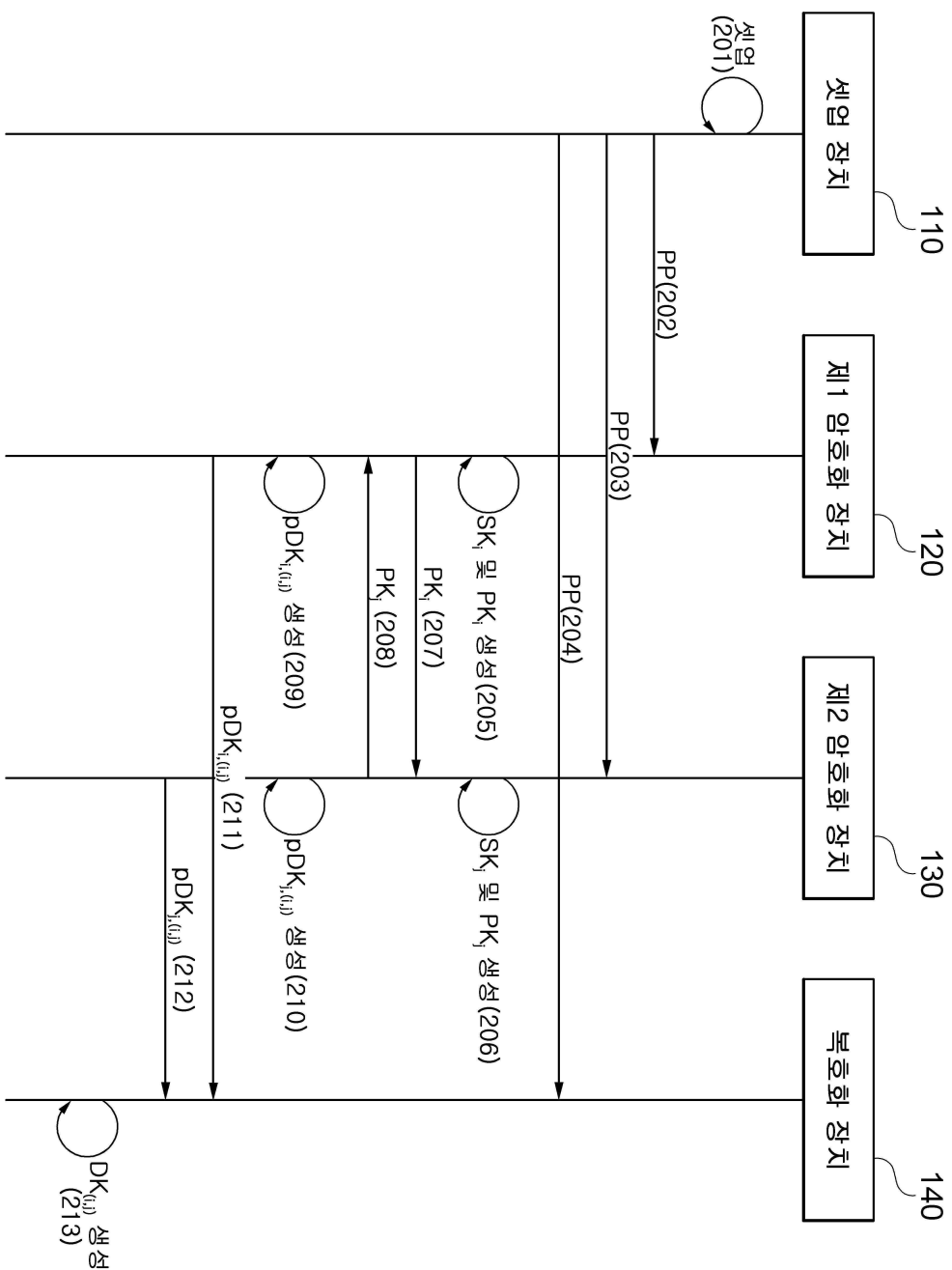
- [0312]
- 10: 컴퓨팅 환경
 - 12: 컴퓨팅 장치
 - 14: 프로세서
 - 16: 컴퓨터 판독 가능 저장 매체
 - 18: 통신 버스
 - 20: 프로그램
 - 22: 입출력 인터페이스
 - 24: 입출력 장치
 - 26: 네트워크 통신 인터페이스
 - 100: 암호 시스템
 - 110: 셋업 장치
 - 120: 제1 암호화 장치
 - 130: 제2 암호화 장치
 - 140: 복호화 장치

도면

도면1

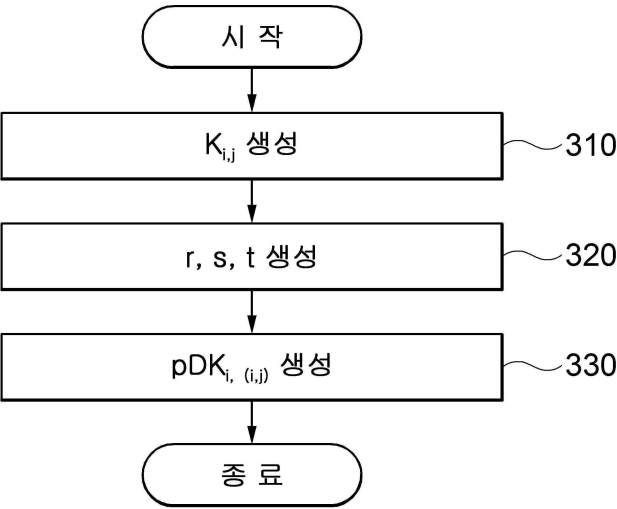
100



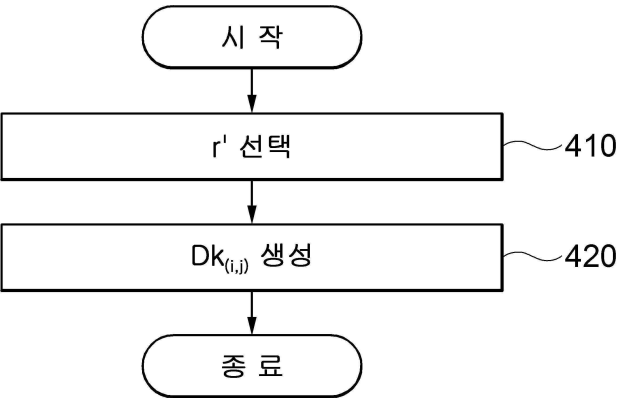


도면2

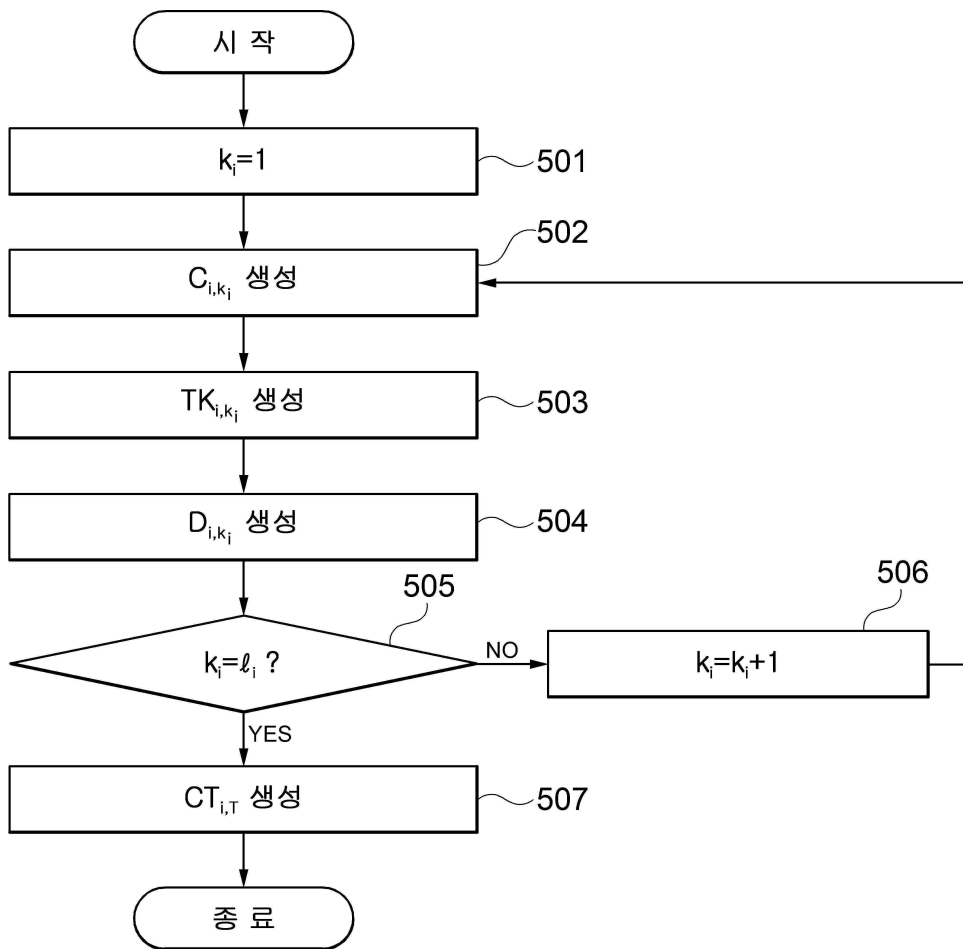
도면3



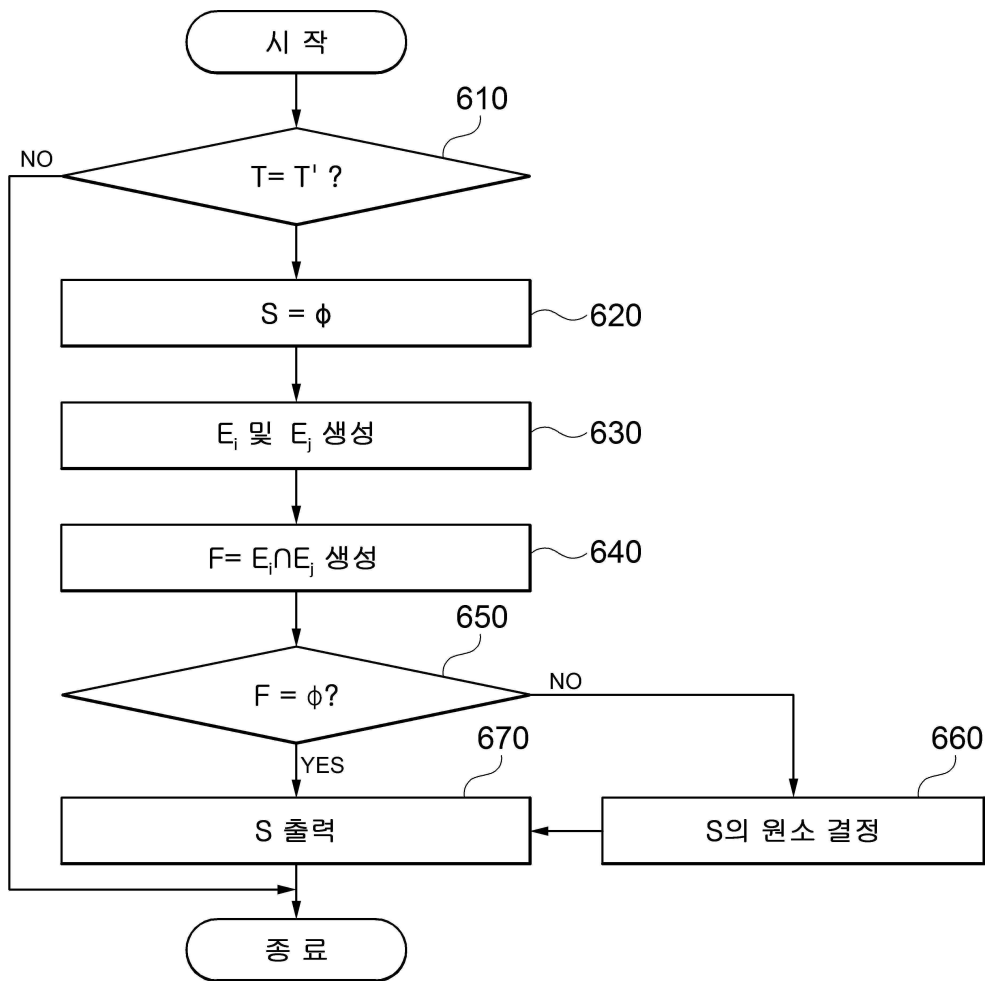
도면4



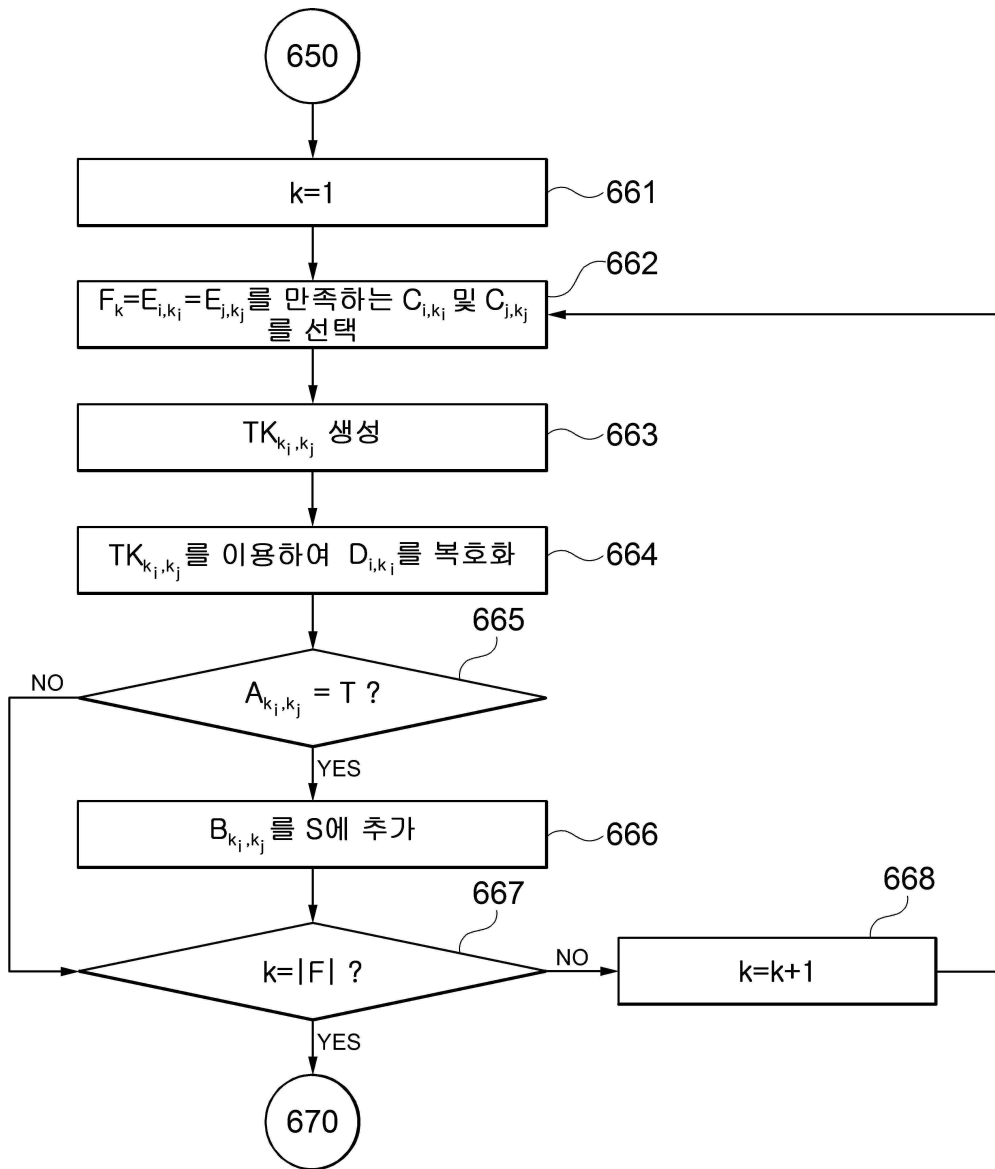
도면5



도면6



도면7



도면8

10

