(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년07월22일
(11) 등록번호 10-2281265
(24) 등록일자 2021년07월19일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06F 17/10* (2006.01)
H04L 9/06 (2006.01) *H04L 9/12* (2006.01)
(52) CPC특허분류
H04L 9/0822 (2013.01)
G06F 17/10 (2013.01)
(21) 출원번호 10-2020-0127100
(22) 출원일자 2020년09월29일
심사청구일자 2020년09월29일
(56) 선행기술조사문헌
KR101599996 B1*
(뒷면에 계속)

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

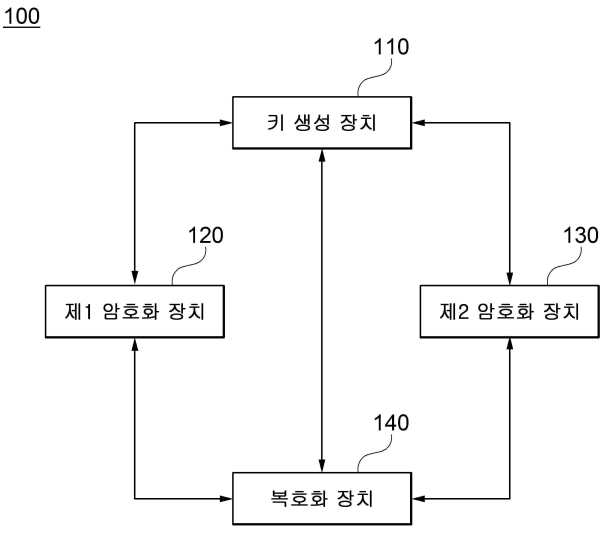
전체 청구항 수 : 총 8 항 심사관 : 양종필

(54) 발명의 명칭 **시간 제약을 지원하는 교집합 연산을 위한 함수 암호 기술**

(57) 요 약

교집합 연산을 지원하는 함수 암호를 위한 방법 및 이를 이용한 장치가 개시된다. 일 실시예에 따른 방법은, 마스터 키에 기초하여 복수의 사용자 각각에 대한 사용자 비밀 키를 생성하는 단계; 및 상기 복수의 사용자 중 제1 사용자에 대한 제1 사용자 비밀 키, 상기 복수의 사용자 중 제2 사용자에 대한 제2 사용자 비밀 키 및 시간 정보에 기초하여, 상기 제1 사용자 비밀 키 및 상기 시간 정보를 이용하여 암호화된 제1 데이터 집합과 상기 제2 사용자 비밀 키 및 상기 시간 정보를 이용하여 암호화된 제2 데이터 집합에 대한 교집합을 생성하기 위한 함수 키를 생성하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0643 (2013.01)
H04L 9/12 (2013.01)

(56) 선행기술조사문헌
KR102143525 B1*
KR1020180003106 A*
JP2013128235 A
KR1020040097717 A
*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업

과제고유번호	1711116146
과제번호	2016-6-00600-005
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발사업
연구과제명	(함수암호 1세부) 함수암호 기법 설계·분석 및 구현기술 연구
기 여 율	1/1
과제수행기관명	상명대학교산학협력단
연구기간	2020.02.01 ~ 2021.01.31

명 세 서

청구범위

청구항 1

마스터 키에 기초하여 복수의 사용자 각각에 대한 사용자 비밀 키를 생성하는 단계; 및

상기 복수의 사용자 중 제1 사용자에 대한 제1 사용자 비밀 키, 상기 복수의 사용자 중 제2 사용자에 대한 제2 사용자 비밀 키 및 시간 정보에 기초하여, 상기 제1 사용자 비밀 키 및 상기 시간 정보를 이용하여 암호화된 제1 데이터 집합과 상기 제2 사용자 비밀 키 및 상기 시간 정보를 이용하여 암호화된 제2 데이터 집합에 대한 교집합을 생성하기 위한 함수 키를 생성하는 단계를 포함하고,

상기 사용자 비밀키를 생성하는 단계는, 아래의 수학식 1

[수학식 1]

$$EK_u = PRF(z, 0 \| u)$$

(이때, u는 $u \in [n]$을 만족하는 사용자 인덱스, n은 상기 복수의 사용자의 총 수, EK_u는 상기 사용자 인덱스가 u인 사용자 대한 사용자 비밀키, z는 상기 마스터 키, PRF()는 의사 랜덤 함수(pseudo-random function))

을 이용하여 상기 복수의 사용자 각각에 대한 사용자 비밀 키를 생성하고,

상기 함수 키를 생성하는 단계는, 아래의 수학식 2

[수학식 2]

$$SK_{i,j,T} = \hat{g}^{\frac{\beta_{i,T}}{(\alpha_{i,T}+\alpha_{j,T})}} = \hat{g}^{\frac{PRF(EK_i,2\|T)}{(PRF(EK_i,1\|T)+PRF(EK_j,1\|T))}}$$

(이때, $SK_{i,j,T}$는 상기 함수 키, i는 상기 제1 사용자의 사용자 인덱스, j는 상기 제2 사용자의 사용자 인덱스, T는 상기 시간 정보, $\hat{g}$는 위수가 소수 p인 순환군 $\hat{G}$의 생성원)

를 이용하여 상기 함수 키를 생성하는, 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

키 생성 장치로부터 사용자에 대한 사용자 비밀 키를 획득하는 단계;

시간 정보 및 상기 사용자 비밀 키에 기초하여, 데이터 집합에 포함된 각 원소에 대한 제1 암호문 요소 및 제2 암호문 요소를 생성하는 단계; 및

상기 각 원소에 대한 제1 암호문 요소 및 제2 암호문 요소를 포함하는 암호문을 생성하는 단계를 포함하고,

상기 제1 암호문 요소 및 제2 암호문 요소를 생성하는 단계는, 상기 시간 정보 및 상기 사용자 비밀 키에 기초하여 상기 각 원소에 대한 제1 암호문 요소를 생성하는 단계;

상기 시간 정보, 사용자 비밀 키 및 상기 각 원소에 기초하여 상기 각 원소에 대한 대칭 키를 생성하는 단계; 및

상기 각 원소에 대한 대칭 키를 암호화 키로 이용한 대칭 키 암호 알고리즘을 이용하여 상기 각 원소에 대한 제2 암호문 요소를 생성하는 단계를 포함하고,

상기 제1 암호문 요소를 생성하는 단계는, 아래의 수학식 1

[수학식 1]

$$C_{u,k} = H_1(x_{u,k})^{PRF(EK_u, 1 \| T)}$$

(이때, u는 $u \in [n]$을 만족하는 상기 사용자의 사용자 인덱스, $H_1()$은 $H_1:\{0,1\}^* \rightarrow G$를 만족하는 제1 해시 함수, G는 위수가 소수 p인 순환군, $x_{u,k}$는 상기 데이터 집합에 포함된 k번째 원소, PRF()는 의사 랜덤 함수(pseudo-random function), EK_u는 상기 사용자 비밀 키, T는 상기 시간 정보, $C_{u,k}$는 상기 k번째 원소에 대한 제1 암호문 요소)

을 이용하여 상기 각 원소에 대한 제1 암호문 요소를 생성하는, 방법.

청구항 5

삭제

청구항 6

청구항 4에 있어서,

상기 대칭 키를 생성하는 단계는, 아래의 수학식 2

[수학식 2]

$$TK_{u,k} = H_2\left(e\left(H_1(x_{u,k}), \hat{g}\right)^{PRF(EK_u, 2 \| T)}\right)$$

(이때, $TK_{u,k}$는 상기 k번째 원소에 대한 대칭 키, $H_2()$는 보안 상수 1^λ에 대해 $H_2:G_T \rightarrow \{0,1\}^\lambda$를 만족하는 제2 해시 함수, e는 $e: G \times \hat{G} \rightarrow G_T$를 만족하는 겹선형 함수(bilinear map), $\hat{G}$ 및 G_T는 위수가 소수 p인 순환군)

를 이용하여 상기 각 원소에 대한 대칭 키를 생성하고,

상기 제2 암호문 요소를 생성하는 단계는, 아래의 수학식 3

[수학식 3]

$$D_{u,k} = Enc(T \| x_{u,k}, TK_{u,k})$$

(이때, $D_{u,k}$는 상기 k번째 원소에 대한 제2 암호문 요소, Enc()는 대칭 키 암호 알고리즘을 이용한 암호화)

을 이용하여 상기 각 원소에 대한 제2 암호문 요소를 생성하는, 방법.

청구항 7

청구항 6에 있어서,

상기 암호문은 아래의 수학식 4

[수학식 4]

$$CT_{u,T} = \{(C_{u,\pi(k)}, D_{u,\pi(k)})\}_{k=1}^{\ell}$$

(이때, π는 랜덤한 순열(permutation), ℓ은 상기 데이터 집합에 포함된 원소의 개수)

를 만족하는, 방법.

청구항 8

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,

마스터 키에 기초하여 복수의 사용자 각각에 대한 사용자 비밀 키를 생성하는 단계; 및

상기 복수의 사용자 중 제1 사용자에 대한 제1 사용자 비밀 키, 상기 복수의 사용자 중 제2 사용자에 대한 제2 사용자 비밀 키 및 시간 정보에 기초하여, 상기 제1 사용자 비밀 키 및 상기 시간 정보를 이용하여 암호화된 제1 데이터 집합과 상기 제2 사용자 비밀 키 및 상기 시간 정보를 이용하여 암호화된 제2 데이터 집합에 대한 교집합을 생성하기 위한 함수 키를 생성하는 단계를 실행하기 위한 명령어들을 포함하고,

상기 사용자 비밀키를 생성하는 단계는, 아래의 수학식 1

[수학식 1]

$$EK_u = PRF(z, 0 \| u)$$

(이때, u는 u∈[n]을 만족하는 사용자 인덱스, n은 상기 복수의 사용자의 총 수, EK_u는 상기 사용자 인덱스가 u인 사용자 대한 사용자 비밀키, z는 상기 마스터 키, PRF()는 의사 랜덤 함수(pseudo-random function))

을 이용하여 상기 복수의 사용자 각각에 대한 사용자 비밀 키를 생성하고,

상기 함수 키를 생성하는 단계는, 아래의 수학식 2

[수학식 2]

$$SK_{i,j,T} = \hat{g}^{\frac{\beta_{i,T}}{(\alpha_{i,T}+\alpha_{j,T})}} = \hat{g}^{\frac{PRF(EK_i,2\|T)}{(PRF(EK_i,1\|T)+PRF(EK_j,1\|T))}}$$

(이때, $SK_{i,j,T}$는 상기 함수 키, i는 상기 제1 사용자의 사용자 인덱스, j는 상기 제2 사용자의 사용자 인덱스, T는 상기 시간 정보, $\hat{g}$는 위수가 소수 p인 순환군 $\hat{G}$의 생성원)

를 이용하여 상기 함수 키를 생성하는, 장치.

청구항 9

삭제

청구항 10

삭제

청구항 11

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 사용자에 대한 사용자 비밀 키를 획득하는 단계;

시간 정보 및 상기 사용자 비밀 키에 기초하여, 데이터 집합에 포함된 각 원소에 대한 제1 암호문 요소 및 제2 암호문 요소를 생성하는 단계; 및

상기 각 원소에 대한 제1 암호문 요소 및 제2 암호문 요소를 포함하는 암호문을 생성하는 단계를 실행하기 위한 명령어들을 포함하고,

상기 제1 암호문 요소 및 제2 암호문 요소를 생성하는 단계는, 상기 시간 정보 및 상기 사용자 비밀 키에 기초하여 상기 각 원소에 대한 제1 암호문 요소를 생성하는 단계;

상기 시간 정보, 사용자 비밀 키 및 상기 각 원소에 기초하여 상기 각 원소에 대한 대칭 키를 생성하는 단계; 및

상기 각 원소에 대한 대칭 키를 암호화 키로 이용한 대칭 키 암호 알고리즘을 이용하여 상기 각 원소에 대한 제2 암호문 요소를 생성하는 단계를 포함하고,

상기 제1 암호문 요소를 생성하는 단계는, 아래의 수학식 1

[수학식 1]

$$C_{u,k} = H_1(x_{u,k})^{PRF(EK_u, 1\|T)}$$

(이때, u는 $u \in [n]$을 만족하는 상기 사용자의 사용자 인덱스, $H_1()$은 $H_1:\{0,1\}^* \rightarrow G$를 만족하는 제1 해시 함수, G는 위수가 소수 p인 순환군, $x_{u,k}$는 상기 데이터 집합에 포함된 k번째 원소, PRF()는 의사 랜덤 함수(pseudo-random function), EK_u는 상기 사용자 비밀 키, T는 상기 시간 정보, $C_{u,k}$는 상기 k번째 원소에 대한 제1 암호문 요소)

을 이용하여 상기 각 원소에 대한 제1 암호문 요소를 생성하는, 장치.

청구항 12

삭제

청구항 13

청구항 11에 있어서,

상기 대칭 키를 생성하는 단계는, 아래의 수학식 2

[수학식 2]

$$TK_{u,k} = H_2\left(e\left(H_1(x_{u,k}), \hat{g}\right)^{PRF(EK_u, 2\|T)}\right)$$

(이때, $TK_{u,k}$는 상기 k번째 원소에 대한 대칭 키, $H_2()$는 보안 상수 1^{λ}에 대해 $H_2: G_T \rightarrow \{0,1\}^{\lambda}$를 만족하는 제2 해시 함수, e는 $e: G \times \hat{G} \rightarrow G_T$ 를 만족하는 겹선형 함수(bilinear map), $\hat{G}$ 및 G_T 는 위수가 소수 p인 순환군)

를 이용하여 상기 각 원소에 대한 대칭 키를 생성하고,

상기 제2 암호문 요소를 생성하는 단계는, 아래의 수학식 3

[수학식 3]

$$D_{u,k} = Enc\left(T \| x_{u,k}, TK_{u,k}\right)$$

(이때, $D_{u,k}$ 는 상기 k번째 원소에 대한 제2 암호문 요소, Enc()는 대칭 키 암호 알고리즘을 이용한 암호화)

을 이용하여 상기 각 원소에 대한 제2 암호문 요소를 생성하는, 장치.

청구항 14

청구항 13에 있어서,

상기 암호문은 아래의 수학식 4

[수학식 4]

$$CT_{u,T} = \left\{\left(C_{u,\pi(k)}, D_{u,\pi(k)}\right)\right\}_{k=1}^{\ell}$$

(이때, π는 랜덤한 순열(permutation), ℓ은 상기 데이터 집합에 포함된 원소의 개수)

를 만족하는, 장치.

발명의 설명

기 술 분 야

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

배 경 기 술

[0002] 함수 암호(Functional Encryption, FE)는 암호화된 상태에서 연산을 수행하는 암호 기술로, 평문에 대한 암호문과 함수에 대한 함수 키를 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 n명인 경우, 시스템 셋업(set up)에서 오직 고정된 n명의 사용자에 대한 비밀 키와 시스템 파라미터가 발급되며, 새로운 사용자가

추가되는 경우에는 전체 시스템을 다시 셋업해야 한다.

[0005] 2. 시스템 셋업에 참여한 n명의 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 사용자에 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, 함수 키가 한 번 발급되면 특정 사용자 2명의 (동일한 시간에 대해 생성된) 모든 암호문에 대하여 교집합 연산이 가능하기 때문에, 함수키를 발급받은 사용자(혹은 제 3의 서비스 제공자)는 한 번의 함수 키 발급으로 인해 막대한 권한을 획득하게 되며 암호문에 대한 세밀한 접근 제어가 이루어지지 않는 문제점이 발생한다.

[0009] 예를 들어, 사용자 i와 j가 임의의 서비스를 신청하여 제 3의 서비스 제공자가 함수 키를 발급받은 상황을 생각해보자. 이후 특정 시점에 사용자 i와 j가 서비스를 해지하는 경우, 서비스 제공자는 해당 시점 이후부터는 더 이상 사용자들의 데이터에 대한 정보를 얻을 수 없어야 한다. 하지만 대한민국 등록특허 제10-2143525호에서 제안한 기술을 이용하면, 서비스 제공자는 처음 발급받은 함수 키를 이용하여 서비스 해지 시점 이후의 암호문에 대해서도 교집합 연산을 수행하여 사용자들에 대한 유의미한 정보를 얻을 수 있다. 이를 방지하기 위해서는 일부 사용자들이 서비스를 해지할 때마다 전체 시스템을 다시 셋업해야 하기 때문에 매우 비효율적이다.

선행기술문헌

특허문헌

[0010] (특허문헌 0001) 대한민국 등록특허 제10-2143525호 (2020. 08. 11. 공고)

발명의 내용

해결하려는 과제

[0011] 본 발명의 실시예들은 교집합 연산을 지원하는 함수 암호를 위한 방법 및 이를 이용한 장치를 제공하기 위한 것이다.

과제의 해결 수단

[0012] 일 실시예에 따른 방법은, 마스터 키에 기초하여 복수의 사용자 각각에 대한 사용자 비밀 키를 생성하는 단계; 및 상기 복수의 사용자 중 제1 사용자에 대한 제1 사용자 비밀 키, 상기 복수의 사용자 중 제2 사용자에 대한 제2 사용자 비밀 키 및 시간 정보에 기초하여, 상기 제1 사용자 비밀 키 및 상기 시간 정보를 이용하여 암호화된 제1 데이터 집합과 상기 제2 사용자 비밀 키 및 상기 시간 정보를 이용하여 암호화된 제2 데이터 집합에 대한 교집합을 생성하기 위한 함수 키를 생성하는 단계를 포함한다.

[0013] 상기 사용자 비밀키를 생성하는 단계는, 아래의 수학식 1

[0014] [수학식 1]

$$EK_u = PRF(z, 0 \| u)$$

[0015]

[0016] (이때, u는 $u \in [n]$을 만족하는 사용자 인덱스, n은 상기 복수의 사용자의 총 수, EK_u는 상기 사용자 인덱스가 u인 사용자 대한 사용자 비밀키, z는 상기 마스터 키, PRF()는 의사 랜덤 함수(pseudo-random function))을 이

용하여 상기 복수의 사용자 각각에 대한 사용자 비밀 키를 생성할 수 있다.

[0017] 상기 함수 키를 생성하는 단계는, 아래의 수학식 2

[0018] [수학식 2]

$$SK_{i,j,T} = \hat{g}^{\frac{\beta_{i,T}}{(\alpha_{i,T}+\alpha_{j,T})}} = \hat{g}^{\frac{PRF(EK_i,2\|T)}{(PRF(EK_i,1\|T)+PRF(EK_j,1\|T))}}$$

[0019]

[0020] (이때, $SK_{i,j,T}$는 상기 함수 키, i는 상기 제1 사용자의 사용자 인덱스, j는 상기 제2 사용자의 사용자 인덱스, T는 상기 시간 정보, $\hat{g}$는 위수가 소수 p인 순환군 $\hat{G}$의 생성원)를 이용하여 상기 함수 키를 생성할 수 있다.

[0021] 일 실시예에 따른 방법은, 키 생성 장치로부터 사용자에 대한 사용자 비밀 키를 획득하는 단계; 시간 정보 및 상기 사용자 비밀 키에 기초하여, 데이터 집합에 포함된 각 원소에 대한 제1 암호문 요소 및 제2 암호문 요소를 생성하는 단계; 및 상기 각 원소에 대한 제1 암호문 요소 및 제2 암호문 요소를 포함하는 암호문을 생성하는 단계를 포함한다.

[0022] 상기 제1 암호문 요소 및 제2 암호문 요소를 생성하는 단계는, 상기 시간 정보 및 상기 사용자 비밀 키에 기초하여 상기 각 원소에 대한 제1 암호문 요소를 생성하는 단계; 상기 시간 정보, 사용자 비밀 키 및 상기 각 원소에 기초하여 상기 각 원소에 대한 대칭 키를 생성하는 단계; 및 상기 각 원소에 대한 대칭 키를 암호화 키로 이용한 대칭 키 암호 알고리즘을 이용하여 상기 각 원소에 대한 제2 암호문 요소를 생성하는 단계를 포함할 수 있다.

[0023] 상기 제1 암호문 요소를 생성하는 단계는, 아래의 수학식 1

[0024] [수학식 1]

$$C_{u,k} = H_1(x_{u,k})^{PRF(EK_u,1\|T)}$$

[0025]

[0026] (이때, u는 $u \in [n]$을 만족하는 상기 사용자의 사용자 인덱스, $H_1()$은 $H_1:\{0,1\}^* \rightarrow G$를 만족하는 제1 해시 함수, G는 위수가 소수 p인 순환군, $x_{u,k}$는 상기 데이터 집합에 포함된 k번째 원소, PRF()는 의사 랜덤 함수(pseudo-random function), EK_u는 상기 사용자 비밀 키, T는 상기 시간 정보, $C_{u,k}$는 상기 k번째 원소에 대한 제1 암호문 요소)을 이용하여 상기 각 원소에 대한 제1 암호문 요소를 생성하고, 상기 대칭 키를 생성하는 단계는, 아래의 수학식 2

[0027] [수학식 2]

$$TK_{u,k} = H_2\left(e\left(H_1(x_{u,k}),\hat{g}\right)^{PRF(EK_u,2\|T)}\right)$$

[0028]

[0029] (이때, $TK_{u,k}$는 상기 k번째 원소에 대한 대칭 키, $H_2()$는 보안 상수 1^λ에 대해 $H_2:G_T \rightarrow \{0,1\}^\lambda$를 만족하는 제2 해시 함수, e는 $e: G \times \hat{G} \rightarrow G_T$를 만족하는 겹선형 함수(bilinear map), $\hat{G}$ 및 G_T는 위수가 소수 p인 순환군)를 이용하여 상기 각 원소에 대한 대칭 키를 생성하고, 상기 제2 암호문 요소를 생성하는 단계는, 아래의 수학식 3

[0030] [수학식 3]

$$D_{u,k} = Enc(T \| x_{u,k}, TK_{u,k})$$

[0031]

[0032] (이때, $D_{u,k}$는 상기 k번째 원소에 대한 제2 암호문 요소, Enc()는 대칭 키 암호 알고리즘을 이용한 암호화)을

이용하여 상기 각 원소에 대한 제2 암호문 요소를 생성할 수 있다.

[0033] 상기 암호문은 아래의 수학식 4

[0034] [수학식 4]

$$CT_{u,T} = \{(C_{u,\pi(k)}, D_{u,\pi(k)})\}_{k=1}^{\ell}$$

[0035]

[0036] (이때, π는 랜덤한 순열(permutation), ℓ은 상기 데이터 집합에 포함된 원소의 개수)를 만족할 수 있다.

[0037] 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, 마스터 키에 기초하여 복수의 사용자 각각에 대한 사용자 비밀 키를 생성하는 단계; 및 상기 복수의 사용자 중 제1 사용자에 대한 제1 사용자 비밀 키, 상기 복수의 사용자 중 제2 사용자에 대한 제2 사용자 비밀 키 및 시간 정보에 기초하여, 상기 제1 사용자 비밀 키 및 상기 시간 정보를 이용하여 암호화된 제1 데이터 집합과 상기 제2 사용자 비밀 키 및 상기 시간 정보를 이용하여 암호화된 제2 데이터 집합에 대한 교집합을 생성하기 위한 함수 키를 생성하는 단계를 실행하기 위한 명령어들을 포함한다.

[0038] 상기 사용자 비밀키를 생성하는 단계는, 아래의 수학식 1

[0039] [수학식 1]

$$EK_u = PRF(z, 0 \| u)$$

[0040]

[0041] (이때, u는 u∈[n]을 만족하는 사용자 인덱스, n은 상기 복수의 사용자의 총 수, EK_u는 상기 사용자 인덱스가 u인 사용자 대한 사용자 비밀키, z는 상기 마스터 키, PRF()는 의사 랜덤 함수(pseudo-random function))을 이용하여 상기 복수의 사용자 각각에 대한 사용자 비밀 키를 생성할 수 있다.

[0042] 상기 함수 키를 생성하는 단계는, 아래의 수학식 2

[0043] [수학식 2]

$$SK_{i,j,T} = \hat{g}^{\frac{\beta_{i,T}}{(\alpha_{i,T}+\alpha_{j,T})}} = \hat{g}^{\frac{PRF(EK_i,2\|T)}{(PRF(EK_i,1\|T)+PRF(EK_j,1\|T))}}$$

[0044]

[0045] (이때, $SK_{i,j,T}$는 상기 함수 키, i는 상기 제1 사용자의 사용자 인덱스, j는 상기 제2 사용자의 사용자 인덱스, T는 상기 시간 정보, $\hat{g}$는 위수가 소수 p인 순환군 $\hat{G}$의 생성원)를 이용하여 상기 함수 키를 생성할 수 있다.

[0046] 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, 키 생성 장치로부터 사용자에 대한 사용자 비밀 키를 획득하는 단계; 시간 정보 및 상기 사용자 비밀 키에 기초하여, 데이터 집합에 포함된 각 원소에 대한 제1 암호문 요소 및 제2 암호문 요소를 생성하는 단계; 및 상기 각 원소에 대한 제1 암호문 요소 및 제2 암호문 요소를 포함하는 암호문을 생성하는 단계를 실행하기 위한 명령어들을 포함한다.

[0047] 상기 제1 암호문 요소 및 제2 암호문 요소를 생성하는 단계는, 상기 시간 정보 및 상기 사용자 비밀 키에 기초하여 상기 각 원소에 대한 제1 암호문 요소를 생성하는 단계; 상기 시간 정보, 사용자 비밀 키 및 상기 각 원소에 기초하여 상기 각 원소에 대한 대칭 키를 생성하는 단계; 및 상기 각 원소에 대한 대칭 키를 암호화 키로 이용한 대칭 키 암호 알고리즘을 이용하여 상기 각 원소에 대한 제2 암호문 요소를 생성하는 단계를 포함할 수 있다.

[0048] 상기 제1 암호문 요소를 생성하는 단계는, 아래의 수학식 1

[0049] [수학식 1]

$$C_{u,k} = H_1(x_{u,k})^{PRF(EK_u, 1\|T)}$$

[0050]

[0051] (이때, u는 u∈[n]을 만족하는 상기 사용자의 사용자 인덱스, $H_1()$은 $H_1:\{0,1\}^* \rightarrow G$를 만족하는 제1 해시 함수, G는 위수가 소수 p인 순환군, $x_{u,k}$는 상기 데이터 집합에 포함된 k번째 원소, PRF()는 의사 랜덤 함수(pseudo-random function), EK_u는 상기 사용자 비밀 키, T는 상기 시간 정보, $C_{u,k}$는 상기 k번째 원소에 대한 제1 암호문 요소)을 이용하여 상기 각 원소에 대한 제1 암호문 요소를 생성하고, 상기 대칭 키를 생성하는 단계는, 아래의 수학식 2

[0052] [수학식 2]

$$TK_{u,k} = H_2\left(e\left(H_1(x_{u,k}), \hat{g}\right)^{PRF(EK_u, 2\|T)}\right)$$

[0053]

[0054] (이때, $TK_{u,k}$는 상기 k번째 원소에 대한 대칭 키, $H_2()$는 보안 상수 1^λ에 대해 $H_2:G_T \rightarrow \{0,1\}^\lambda$를 만족하는 제2 해시 함수, e는 $e: G \times \hat{G} \rightarrow G_T$를 만족하는 겹선형 함수(bilinear map), $\hat{G}$ 및 G_T는 위수가 소수 p인 순환군)를 이용하여 상기 각 원소에 대한 대칭 키를 생성하고, 상기 제2 암호문 요소를 생성하는 단계는, 아래의 수학식 3

[0055] [수학식 3]

$$D_{u,k} = Enc(T \| x_{u,k}, TK_{u,k})$$

[0056]

[0057] (이때, $D_{u,k}$는 상기 k번째 원소에 대한 제2 암호문 요소, Enc()는 대칭 키 암호 알고리즘을 이용한 암호화)을 이용하여 상기 각 원소에 대한 제2 암호문 요소를 생성할 수 있다.

[0058] 상기 암호문은 아래의 수학식 4

[0059] [수학식 4]

$$CT_{u,T} = \{(C_{u,\pi(k)}, D_{u,\pi(k)})\}_{k=1}^{\ell}$$

[0060]

[0061] (이때, π는 랜덤한 순열(permutation), ℓ은 상기 데이터 집합에 포함된 원소의 개수)를 만족할 수 있다.

발명의 효과

[0062] 본 발명의 실시예들에 따르면, 특정한 시간 정보에 대응되는 함수 키를 발급받은 사용자는 동일한 시간 정보에 대해 생성된 암호문들에 대해서만 복호화를 통해 교집합 연산을 수행할 수 있으며, 다른 시간 정보에 대해 생성된 암호문들에 대해서는 정당한 연산의 결과를 얻을 수 없도록 함으로써, 대한민국 등록특허 제10-2143525호에 개시된 함수 암호 기술이 가진 문제점을 해소할 수 있다.

도면의 간단한 설명

[0063] 도 1은 일 실시예에 따른 암호 시스템의 구성도

도 2는 일 실시예에 따른 교집합 생성 절차를 나타낸 절차도

도 3은 일 실시예에 따른 암호화 과정을 나타낸 순서도

도 4는 일 실시예에 따른 교집합 생성 과정을 나타낸 순서도

도 5는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위

한 블록도

발명을 실시하기 위한 구체적인 내용

[0064] 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.

[0065] 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.

[0066] 도 1은 일 실시예에 따른 암호 시스템의 구성도이다.

[0067] 도 1을 참조하면, 본 발명의 일 실시예에 따른 암호 시스템(100)은 키 생성 장치(110), 제1 암호화 장치(120), 제2 암호화 장치(130) 및 복호화 장치(140)를 포함한다.

[0068] 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.

[0069] 키 생성 장치(110)는 암호 시스템(100)에 대한 셋업(setup)을 수행하고, 암호 시스템(100) 내에서 사용할 마스터 키, 사용자 비밀 키, 함수 키 및 공개 파라미터를 생성하기 위한 장치이다.

[0070] 일 실시예에서, 키 생성 장치(110)는 예를 들어, 신뢰 기관(Trusted Third Party)와 같이 신뢰할 수 있는 개체(entity)에 의해 운영될 수 있으나, 키 생성 장치(110)의 운영 주체는 반드시 특정한 개체로 한정되는 것은 아니다.

[0071] 구체적으로, 키 생성 장치(110)는 마스터 키 및 공개 파라미터를 생성하여 마스터 키는 안전하게 저장하고, 공개 파라미터는 암호 시스템(100) 내에 공개할 수 있다.

[0072] 또한, 키 생성 장치(110)는 암호 시스템(100) 내에서 암호화에 참여할 복수의 사용자 각각에 대한 사용자 비밀 키를 생성하고, 생성된 각 사용자에 대한 사용자 비밀 키를 암호화를 위해 각 사용자에 의해 이용되는 암호화 장치(120, 130)로 제공할 수 있다.

[0073] 또한, 키 생성 장치(110)는 복호화 장치(140)의 요청에 따라 각각 상이한 사용자 비밀 키를 이용하여 암호화되되 동일한 시간 정보를 이용하여 암호화된 두 데이터 집합에 대한 교집합 생성을 위해 이용될 함수 키를 생성하여 복호화 장치(140)로 제공할 수 있다.

[0074] 이때, 시간 정보는 암호 시스템(100) 내에서 미리 설정되거나 암호화에 참여할 복수의 사용자 사이에 사전 합의된 방식 내지는 규칙에 따라 결정될 수 있다. 예를 들어, 시간 정보는 암호화 대상인 데이터 집합의 생성 시점, 암호화 시점, 데이터 집합에 대한 암호화를 통해 생성된 암호문의 유효 기간 등일 수 있다. 그러나, 시간 정보는 반드시 상술한 예에 한정되는 것은 아니며, 시간 정보의 종류, 형태 및 결정 방식은 실시예에 따라 다양하게 변경될 수 있다.

[0075] 제1 암호화 장치(120) 및 제2 암호화 장치(130)는 각각 키 생성 장치(110)로부터 사용자 비밀 키를 발급받고, 사용자 비밀 키 및 시간 정보를 이용하여 데이터 집합을 암호화하기 위해 이용되는 장치이다.

[0076] 구체적으로, 제1 암호화 장치(120)는 제1 사용자에 의해 이용될 수 있으며, 키 생성 장치(110)로부터 제공받은 제1 사용자에 대한 사용자 비밀 키 및 시간 정보를 이용하여 제1 데이터 집합에 대한 암호문을 생성할 수 있다. 또한, 제2 암호화 장치(130)는 제2 사용자에 의해 이용될 수 있으며, 키 생성 장치(110)로부터 제공받은 제2 사용자에 대한 사용자 비밀 키 및 시간 정보를 이용하여 제2 데이터 집합에 대한 암호문을 생성할 수 있다.

[0077] 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.

[0078] 복호화 장치(140)는 제1 사용자에 대한 사용자 비밀 키 및 시간 정보를 이용하여 제1 암호화 장치(120)에 의해 암호화된 제1 데이터 집합에 대한 암호문, 제2 사용자에 대한 사용자 비밀 키 및 시간 정보를 이용하여 제2 암호화 장치(130)에 의해 암호화된 제2 데이터 집합에 대한 암호문 및 키 생성 장치(110)로부터 제공받은 함수 키를 이용하여 제1 데이터 집합과 제2 데이터 집합에 대한 교집합을 생성한다.

[0079] 한편, 도 1에 도시된 암호 시스템(100)에 의해 수행되는 동작을 상세히 설명하면 아래와 같다.

[0080] 셋업(setup)

[0081] 키 생성 장치(110)는 보안 상수(Security Parameter) 1^{λ} 및 암호 시스템(100) 내에서 암호화에 참여할 사용자의 총수(n, 이때, n은 2 이상인 정수)에 기초하여, 마스터 키(master key) 및 공개 파라미터를 생성한다.

[0082] 구체적으로, 키 생성 장치(110)는 각각 위수(order)가 소수(prime number) p인 겹선형 군(bilinear group) G, $\hat{G}$ 및 G_T를 생성한 후, $e: G \times \hat{G} \rightarrow G_T$를 만족하는 겹선형 함수(bilinear map) e 및 $\hat{G}$의 생성원(generator) $\hat{g}$를 생성할 수 있다.

[0083] 또한, 키 생성 장치(110)는 $z \in \{0,1\}^{\lambda}$를 만족하는 랜덤 스트링(random string) z, $H_1: \{0,1\}^{*} \rightarrow G$를 만족하는 제1 해시 함수(hash function) H_1 및 $H_2: G_T \rightarrow \{0,1\}^{\lambda}$를 만족하는 제2 해시 함수 H_2를 선택할 수 있다.

[0084] 이후, 키 생성 장치(110)는 선택된 랜덤 스트링 z를 마스터 키로서 안전하게 저장하고, 공개 파라미터 $PP = \left((p, G, \hat{G}, G_T, e), \hat{g}, H_1, H_2\right)$를 암호 시스템(100) 내에 공개할 수 있다.

[0085] 이때, 대칭 키 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 대칭 키 암호 알고리즘이 이용될 수 있다.

[0086] 사용자 비밀 키 생성

[0087] 키 생성 장치(110)는 암호화에 참여할 복수의 사용자 각각에 대한 사용자 비밀 키를 생성한다.

[0088] 일 실시예에 따르면, 키 생성 장치(110)는 암호화에 참여할 복수의 사용자 각각에 대한 사용자 인덱스(index) 및 마스터 키에 기초하여 복수의 사용자 각각에 대한 사용자 비밀 키를 생성할 수 있다.

[0089] 구체적으로, 키 생성 장치(110)는 아래의 수학식 1을 이용하여 복수의 사용자 중 사용자 인덱스가 u(이때, $u \in [n]$)인 사용자에 대한 사용자 비밀 키 EK_u를 생성할 수 있다.

[0090] [수학식 1]

$$EK_u = PRF(z, 0 \| u)$$

[0091]

$$PRF: \{0,1\}^{\lambda} \times \{0,1\}^{*} \rightarrow \mathbb{Z}_p$$

[0092] 수학식 1에서, PRF()는 를 만족하는 의사 랜덤 함수(pseudo-random function), "‖"는 두 값 사이의 연결(concatenation)을 나타내며, 이하 동일한 의미로 사용된다.

[0093] 한편, 키 생성 장치(110)는 생성한 사용자 비밀 키 EK_u 각각을 대응되는 사용자에 의해 이용되는 암호화 장치(120, 130)로 제공할 수 있다.

[0094] 예를 들어, 키 생성 장치(110)는 사용자 인덱스가 i(이때, $j \in [n]$)인 제1 사용자에 대한 사용자 비밀 키 EK_i를 제1 사용자에 의해 이용되는 제1 암호화 장치(120)로 제공하고, 사용자 인덱스가 j(이때, $j \in [n]$ 및 $j \neq i$)인 제

2 사용자에 대한 사용자 비밀 키 EK_j를 제2 사용자에 의해 이용되는 제2 암호화 장치(130)로 제공할 수 있다.

[0095] 암호화

[0096] 제1 암호화 장치(120) 및 제2 암호화 장치(130)는 각각 키 생성 장치(110)로부터 제공받은 사용자 비밀 키 및 시간 정보에 기초하여 데이터 집합에 대한 암호문을 생성한다.

[0097] 이때, 시간 정보는 암호 시스템(100) 내에서 미리 설정되거나 암호화에 참여할 복수의 사용자 사이에 사전 합의된 방식 내지는 규칙에 따라 결정될 수 있다.

[0098] 한편, 본 발명의 실시예에서, 교집합은 동일한 시간 정보를 이용하여 암호화된 두 데이터 집합에 대해서만 생성될 수 있다.

[0099] 구체적으로, 키 생성 장치(110)로부터 사용자 인덱스가 i인 제1 사용자에 대한 사용자 비밀 키 EK_i를 제공받은 제1 암호화 장치(120)는 데이터 집합 $X_i = \{x_{i,1}, \ldots, x_{i,\ell_i}\}$ (이때, $|X_i| = \ell_i$, ℓ_i는 2 이상인 정수)에 포함된 각 원소 x_{i,k_i} ($k_i \in [\ell_i]$)에 대한 제1 암호문 요소 C_{i,k_i} 및 제2 암호문 요소 D_{i,k_i}를 생성할 수 있다.

[0100] 구체적으로, 제1 암호화 장치(120)는 우선, 시간 정보 T 및 제1 사용자의 사용자 비밀 키 EK_i에 기초하여 데이터 집합 X_i에 포함된 각 원소 x_{i,k_i}에 대한 제1 암호문 요소 C_{i,k_i}를 생성할 수 있다.

[0101] 이때, 제1 암호문 요소 C_{i,k_i}는 예를 들어, 아래의 수학식 2를 이용하여 생성될 수 있다.

[0102] [수학식 2]

$$C_{i,k_i} = H_1(x_{i,k_i})^{PRF(EK_i, 1\|T)}$$

[0103]

[0104] 또한, 제1 암호화 장치(120)는 시간 정보 T, 제1 사용자의 사용자 비밀 키 EK_i 및 데이터 집합 X_i에 포함된 각 원소 x_{i,k_i}에 기초하여 각 원소 x_{i,k_i}에 대응되는 대칭 키 TK_{i,k_i}를 생성할 수 있다.

[0105] 이때, 대칭 키 TK_{i,k_i}는 예를 들어, 아래의 수학식 3을 이용하여 생성될 수 있다.

[0106] [수학식 3]

$$TK_{i,k_i} = H_2\left(e(H_1(x_{i,k_i}), \hat{g})^{PRF(EK_i, 2\|T)}\right)$$

[0107]

[0108] 이후, 제1 암호화 장치(120)는 x_{i,k_i}에 대응되는 대칭 키 TK_{i,k_i}를 암호화 키로 이용한 대칭 키 암호 알고리즘을 이용하여 각 원소 x_{i,k_i}에 대한 제2 암호문 요소 D_{i,k_i}를 생성할 수 있다.

[0109] 이때, 제2 암호문 요소 D_{i,k_i}는 예를 들어, 아래의 수학식 4를 이용하여 생성될 수 있다.

[0110] [수학식 4]

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

[0111]

[0112] 수학식 4에서, Enc ()는 대칭 키 암호 알고리즘을 이용한 암호화를 나타내며, $Enc(T \parallel x_{i,k_i}, TK_{i,k_i})$는 TK_{i,k_i}를 암호화 키로 이용하여 $T \parallel x_{i,k_i}$를 암호화함을 의미한다.

[0113] 이후, 제1 암호화 장치(120)는 데이터 집합 X_i에 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 포함하고, 시간 정보 T에 대응되는 암호문 $CT_{i,T}$를 생성할 수 있다.

[0114] 구체적으로, 데이터 집합 X_i에 대한 암호문 $CT_{i,T}$는 아래의 수학식 5를 만족할 수 있다.

[0115] [수학식 5]

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

[0116]

[0117] 이때, π는 랜덤한 순열(permutation)을 의미한다.

[0118] 한편, 키 생성 장치(110)로부터 제2 사용자에 대한 사용자 비밀 키 EK_j를 제공받은 제2 암호화 장치(130)는 데이터 집합 $X_j = \{x_{j,1}, \ldots, x_{i,\ell_j}\}$ (이때, $|X_j| = \ell_j$, ℓ_j는 2 이상인 정수)에 포함된 각 원소 x_{j,k_j} (이때, $k_j \in [\ell_j]$)에 대한 제1 암호문 요소 C_{j,k_j} 및 제2 암호문 요소 D_{j,k_j}를 생성할 수 있다.

[0119] 구체적으로, 제2 암호화 장치(130)는 시간 정보 T' 및 사용자 비밀 키 EK_j에 기초하여 데이터 집합 X_j에 포함된 각 원소 x_{j,k_j}에 대한 제1 암호문 요소 C_{j,k_j}를 생성할 수 있다.

[0120] 이때, 제1 암호문 요소 C_{j,k_j}는 예를 들어, 아래의 수학식 6을 이용하여 생성될 수 있다.

[0121] [수학식 6]

$$C_{j,k_j} = H_1\left(x_{j,k_j}\right)^{PRF\left(EK_j, 1 \| T'\right)}$$

[0122]

[0123] 또한, 제2 암호화 장치(130)는 시간 정보 T', 제2 사용자의 사용자 비밀 키 EK_j 및 데이터 집합 X_j에 포함된 각 원소 x_{j,k_j}에 기초하여 각 원소 x_{j,k_j}에 대응되는 대칭 키 TK_{j,k_j}를 생성할 수 있다.

[0124] 이때, 대칭 키 TK_{j,k_j}는 예를 들어, 아래의 수학식 7를 이용하여 생성될 수 있다.

[0125] [수학식 7]

$$TK_{j,k_j} = H_2\left(e\left(H_1(x_{j,k_j}),\hat{g}\right)^{PRF(EK_j,2\|T')}\right)$$

[0126]

[0127] 이후, 제2 암호화 장치(130)는 각 원소 x_{j,k_j}에 대응되는 대칭 키 TK_{j,k_j}를 암호화 키로 이용한 대칭 키 암호 알고리즘을 이용하여 각 원소 x_{j,k_j}에 대한 제2 암호문 요소 D_{j,k_j}를 생성할 수 있다.

[0128] 이때, 제2 암호문 요소 D_{j,k_j}는 예를 들어, 아래의 수학식 8을 이용하여 생성될 수 있다.

[0129] [수학식 8]

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

[0130]

[0131] 이후, 제2 암호화 장치(130)는 데이터 집합 X_j에 포함된 각 원소 x_{j,k_j}에 대한 제1 암호문 요소 C_{j,k_j} 및 제2 암호문 요소 D_{j,k_j}을 포함하고, 시간 정보 T'에 대응되는 암호문 $CT_{j,T'}$를 생성할 수 있다.

[0132] 구체적으로, 암호문 $CT_{j,T'}$는 아래의 수학식 9를 만족할 수 있다.

[0133] [수학식 9]

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

[0134]

[0135] 함수 키 생성

[0136] 키 생성 장치(110)는 각각 상이한 사용자 비밀 키를 이용하여 암호화되되, 동일한 시간 정보를 이용하여 암호화된 두 데이터 집합에 대한 교집합을 생성하기 위한 함수 키를 생성하고, 생성된 함수 키를 복호화 장치(140)로 제공한다.

[0137] 일 실시예에 따르면, 함수 키는 두 데이터 집합 각각에 대한 암호화를 위해 이용된 사용자 비밀 키 및 시간 정보에 기초하여 생성될 수 있다.

[0138] 구체적으로, 제1 사용자에 대한 사용자 비밀 키 EK_i 및 시간 정보 T를 이용하여 암호화된 데이터 집합 X_i와 제2 사용자에 대한 사용자 비밀 키 EK_j 및 시간 정보 T를 이용하여 암호화된 데이터 집합 X_j에 대한 교집합을 생성하기 위한 함수 키 $Sk_{i,j,T}$는 아래의 수학식 10을 이용하여 생성될 수 있다.

[0139] [수학식 10]

$$SK_{i,j,T} = \hat{g}^{\frac{\beta_{i,T}}{(\alpha_{i,T}+\alpha_{j,T})}} = \hat{g}^{\frac{PRF(EK_i,2\|T)}{(PRF(EK_i,1\|T)+PRF(EK_j,1\|T))}}$$

[0140]

[0141] 이때, 사용자 인덱스들의 인덱스 집합 {i,j}는 암호화 시스템(100)에서 사전에 정해진 규칙에 따라 배열될 수 있으며, 동일한 집합에 대해서는 동일한 순서로 배열될 수 있다. 따라서, 함수 키 생성을 위한 키 생성 알고리즘은 결정적(deterministic) 알고리즘에 해당한다.

[0142] 복호화

[0143] 복호화 장치(140)는 함수 키 $SK_{i,j,T}$, 암호문 $CT_{i,T}$ 및 암호문 $CT_{j,T'}$을 이용하여 데이터 집합 X_i와 데이터 집합 X_j에 대한 교집합 $S=(X_i \cap X_j)$을 생성한다.

[0144] 구체적으로, 복호화 장치(140)는 아래 수학식 11을 이용하여 모든 k_i 및 k_j에 대해 k_i 및 k_j의 조합 (k_i, k_j) 각각에 대한 대칭 키 TK_{k_i,k_j}를 생성할 수 있다.

[0145] [수학식 11]

$$TK_{k_i,k_j} = H_2\left(e(C_{i,k_i} \times C_{j,k_j}, SK_{i,j,T})\right)$$

[0146]

[0147] 또한, 복호화 장치(140)는 생성된 각 대칭 키 TK_{k_i,k_j}을 복호화 키로 이용한 대칭 키 암호 알고리즘을 이용하여 암호문 $CT_{i,T}$에 포함된 제2 암호문 요소 D_{i,k_i} 각각을 복호화할 수 있다.

[0148] 구체적으로, 복호화 장치(140)는 아래의 수학식 12를 이용하여 암호문 $CT_{i,T}$에 포함된 제2 암호문 요소 D_{i,k_i} 각각을 복호화하고, $A_{k_i,k_j} = T$ 인 경우, B_{k_i,k_j}를 집합 S에 포함시킬 수 있다.

[0149] [수학식 12]

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

[0150]

[0151] 수학식 12에서, Dec()는 대칭 키 암호 알고리즘을 이용한 복호화를 나타내며, $Dec\left(D_{i,k_i}, TK_{k_i,k_j}\right)$는 TK_{k_i,k_j}를 복호화 키로 이용하여 D_{i,k_i}를 복호화함을 의미한다.

[0152] 한편, 복호화 장치(140)는 모든 k_i 및 k_j의 조합에 대해 상술한 복호화가 수행된 경우, 집합 S를 데이터 집합 X_i와 데이터 집합 X_j에 대한 교집합으로 출력할 수 있다.

[0153] 도 2는 일 실시예에 따른 교집합 생성 절차를 나타낸 절차도이다.

[0154] 도 2를 참조하면, 우선 키 생성 장치(110)는 셋업 절차를 수행하여 마스터 키 z와 공개 파라미터 $PP = \left((p, G, \hat{G}, G_T, e), \hat{g}, H_1, H_2\right)$를 생성한다(201).

[0155] 이때, 키 생성 장치(110)는 마스터 키 z는 안전하게 저장하고, 공개 파라미터 PP를 암호 시스템(100) 내에 공개할 수 있다.

[0156] 이후, 제1 암호화 장치(120)는 키 생성 장치(110)로 사용자 인덱스가 i인 제1 사용자에 대한 사용자 비밀 키 EK_i를 요청한다(202).

[0157] 이후, 키 생성 장치(110)는 마스터 키 z 및 제1 사용자에 대한 사용자 인덱스 i에 기초하여 사용자 비밀 키 EK_i를 생성하고(203), 생성된 사용자 비밀 키 EK_i를 제1 암호화 장치(120)로 제공한다(204).

[0158] 한편, 제2 암호화 장치(130)는 키 생성 장치(110)로 사용자 인덱스가 j인 제2 사용자에 대한 사용자 비밀 키 EK_j를 요청한다(205).

[0159] 이후, 키 생성 장치(110)는 마스터 키 z 및 제2 사용자에 대한 사용자 인덱스 j에 기초하여 사용자 비밀 키 EK_j를 생성하고(206), 생성된 사용자 비밀 키 EK_j를 제2 암호화 장치(130)로 제공한다(207).

[0160] 이후, 제1 암호화 장치(120)는 시간 정보 T 및 사용자 비밀 키 EK_i를 이용하여 데이터 집합 X_i를 암호화하고(208), 데이터 집합 X_i에 대한 암호문 $CT_{i,T}$를 복호화 장치(140)로 제공한다(209).

[0161] 또한, 제2 암호화 장치(130)는 시간 정보 T 및 사용자 비밀 키 EK_j를 이용하여 데이터 집합 X_j를 암호화하고(210), 데이터 집합 X_j에 대한 암호문 $CT_{j,T}$를 복호화 장치(140)로 제공한다(211).

[0162] 이후, 복호화 장치(140)는 키 생성 장치(110)로 제1 사용자의 비밀 키 EK_i, 사용자 비밀 키 EK_j 및 시간 정보 T에 기초하여 생성된 함수 키 $SK_{i,j,T}$를 요청한다(212).

[0163] 이후, 키 생성 장치(110)는 제1 사용자의 사용자 비밀 키 EK_i, 제2 사용자의 사용자 비밀 키 EK_j 및 시간 정보 T에 기초하여 함수 키 $SK_{i,j,T}$를 생성하고(213), 생성된 함수 키 $SK_{i,j,T}$를 복호화 장치(140)로 제공한다(214).

[0164] 이후, 복호화 장치(140)는 데이터 집합 X_i에 대한 암호문 $CT_{i,T}$, 데이터 집합 X_j에 대한 암호문 $CT_{j,T}$ 및 함수 키 $SK_{i,j,T}$를 이용하여 데이터 집합 X_i와 데이터 집합 X_j에 대한 교집합 S를 생성한다(215).

[0165] 한편, 도 2에 도시된 절차도에서 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.

[0166] 도 3은 일 실시예에 따른 암호화 과정을 나타낸 순서도이다.

[0167] 도 3에 도시된 암호화 과정은 예를 들어, 도 2에 도시된 208 단계에서 제1 암호화 장치(120)에 의해 수행되거나, 210 단계에서 제2 암호화 장치(130)에 의해 수행될 수 있으나, 이하에서는, 설명의 편의를 위해 제1 암호화 장치(120)에서 암호화 과정을 수행하는 것으로 가정하여 설명한다.

[0168] 도 3을 참조하면, 우선, 제1 암호화 장치(120)는 인덱스 값 k_i를 1로 초기화한다(301).

[0169] 이후, 제1 암호화 장치(120)는 시간 정보 T 및 사용자 비밀 키 EK_i에 기초하여, 데이터 집합 X_i에 포함된 원소들 중 인덱스 값이 k_i인 원소 x_{i,k_i}에 대한 제1 암호문 요소 C_{i,k_i}를 생성한다(302).

[0170] 이후, 제1 암호화 장치(120)는 시간 정보 T 및 사용자 비밀 키 EK_i에 기초하여, x_{i,k_i}에 대응되는 대칭 키 TK_{i,k_i}를 생성한다(303).

[0171] 이후, 제1 암호화 장치(120)는 대칭 키 TK_{i,k_i}를 암호화 키로 이용한 대칭 키 암호 알고리즘을 이용하여 x_{i,k_i}에 대한 제2 암호문 요소 D_{i,k_i}를 생성한다(304).

[0172] 이후, 제1 암호화 장치(120)는 인덱스 값 k_i가 데이터 집합 X_i에 포함된 원소들의 개수 ℓ_i와 동일한지 여부를 판단한다(305).

[0173] 이때, $k_j \neq \ell_j$인 경우, 제1 암호화 장치(140)는 k_i를 1만큼 증가시킨 후(306), 302 단계로 되돌아 간다.

[0174] 반면, $k_i = \ell_i$인 경우, 제1 암호화 장치(120)는 데이터 집합 X_i에 대한 암호문 $CT_{i,T}$를 생성한다(307).

[0175] 이때, 암호문 $CT_{i,T}$는 상술한 수학식 5와 같이 데이터 집합 X_i에 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.

[0176] 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 부가되어 수행될 수 있다.

[0177] 도 4는 일 실시예에 따른 교집합 생성 과정을 나타낸 순서도이다.

[0178] 도 4에 도시된 교집합 생성 과정은 예를 들어, 도 2에 도시된 215 단계에서 복호화 장치(140)에 의해 수행될 수 있다.

[0179] 도 4를 참조하면, 우선, 복호화 장치(140)는 복호화 장치(140)는 공집합 $S = \emptyset$를 설정하고(401), 인덱스 값 k_i 및 k_j를 각각 1로 초기화한다(402, 403).

[0180] 이후, 복호화 장치(140)는 암호문 $CT_{i,T}$에 포함된 제1 암호문 요소 C_{i,k_i} 및 암호문 $CT_{j,T'}$에 포함된 제1 암호문 요소 C_{j,k_j} 및 함수 키 함수 키 $SK_{i,j,T}$에 기초하여, 인덱스 값 k_i 및 k_j의 조합 (k_i, k_j)에 대응되는 대칭 키 TK_{k_i,k_j}를 생성한다(404).

[0181] 이후, 복호화 장치(140)는 대칭 키 TK_{k_i,k_j}를 복호화 키로 이용한 대칭 키 암호 알고리즘을 이용하여 암호문 $CT_{i,T}$에 포함된 제2 암호문 요소 D_{i,k_i}를 복호화한다(405).

[0182] 이후, 복호화 장치(140)는 복호화를 통해 생성된 값 $(A_{k_i,k_j} \| B_{k_i,k_j})$ 중 A_{k_i,k_j}가 시간 정보 T와 동일한지 여부를 판단한다(406).

[0183] 이때, $A_{k_i,k_j} = T$인 경우, 복호화 장치(140)는 B_{k_i,k_j}를 집합 S의 원소로 추가한다(407).

[0184] 이후, 복호화 장치(140)는 인덱스 값 k_j가 데이터 집합 X_j에 포함된 원소들의 개수 ℓ_j(즉, 암호문 $CT_{j,T'}$에 포함된 제1 암호문 요소 C_{j,k_j} 또는 제2 암호문 요소 D_{j,k_j}의 개수)와 동일한지 여부를 판단한다(408).

[0185] 이때, $k_j \neq \ell_j$인 경우, 복호화 장치(140)는 k_j를 1만큼 증가시킨 후(409), 405 단계로 되돌아 간다.

[0186] 반면, $k_j = \ell_j$인 경우, 복호화 장치(140)는 인덱스 값 k_i가 데이터 집합 X_i에 포함된 원소들의 개수 ℓ_i(즉, 암호문 $CT_{i,T}$에 포함된 제1 암호문 요소 C_{i,k_i} 또는 제2 암호문 요소 D_{i,k_i}의 개수)와 동일한지 여부를 판단한다(410).

[0187] 이때, $k_i \neq \ell_i$인 경우, 복호화 장치(140)는 k_i를 1만큼 증가시킨 후(411), 403 단계로 되돌아 간다.

[0188] 반면, $k_i = \ell_i$인 경우, 복호화 장치(140)는 집합 S를 두 데이터 집합 X_i와 X_j에 대한 교집합(즉, $S=(X_i \cap X_j)$)으로 출력한다(412).

[0189] 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 부가되

어 수행될 수 있다.

[0190] 도 5는 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.

[0191] 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.

[0192] 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.

[0193] 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.

[0194] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0195] 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.

[0196] 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

[0197] 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: 키 생성 장치

120: 제1 암호화 장치

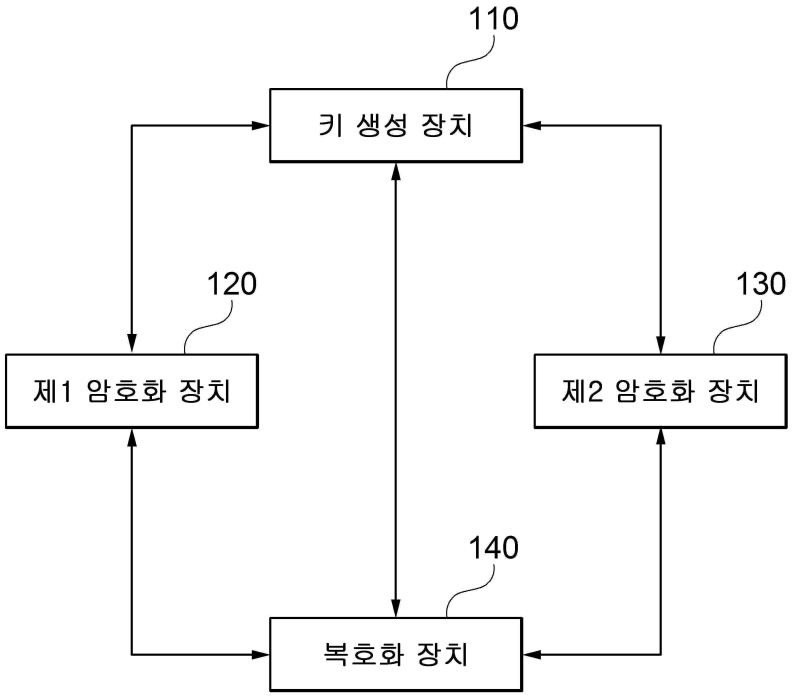
130: 제2 암호화 장치

140: 복호화 장치

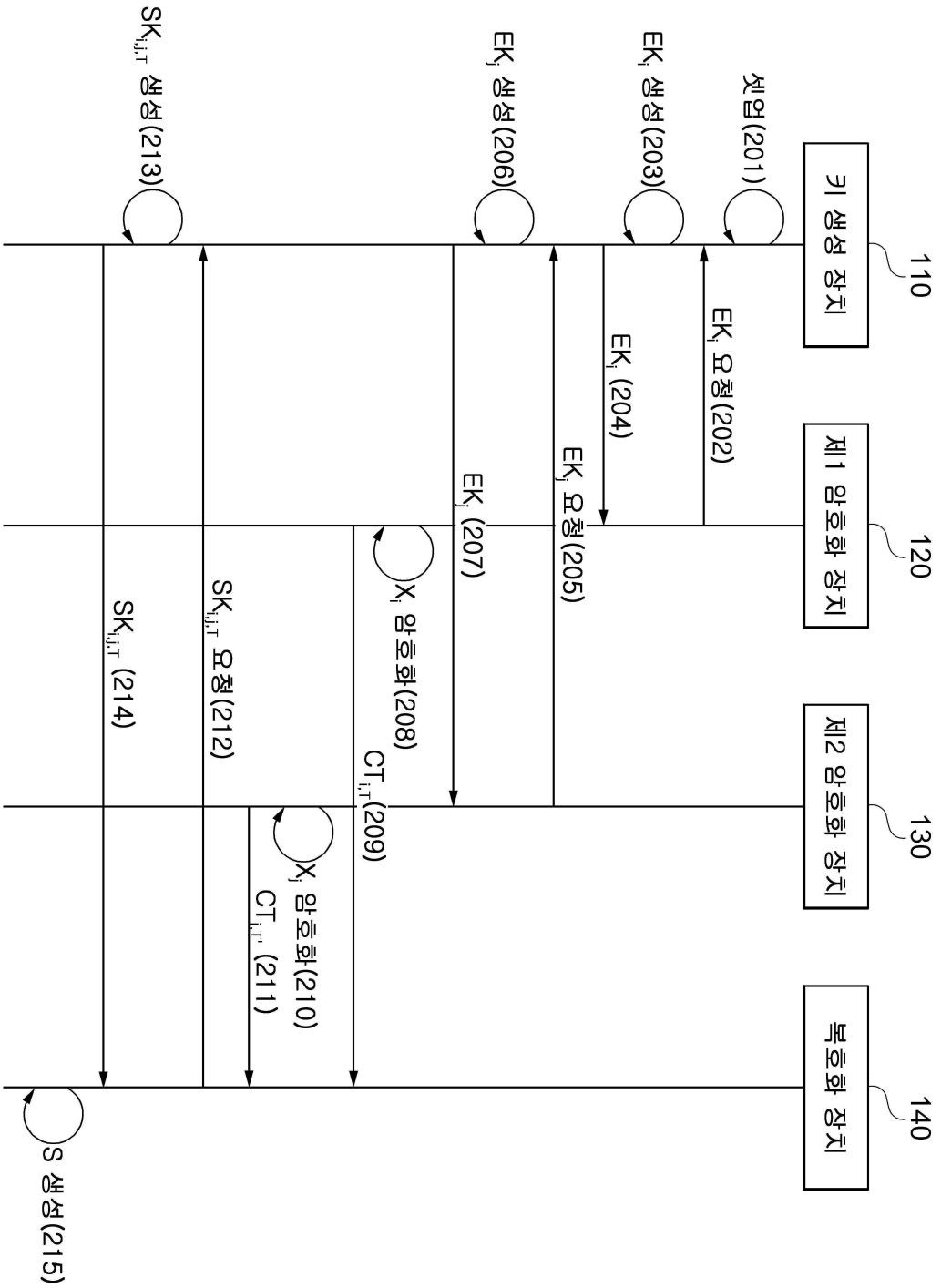
도면

도면1

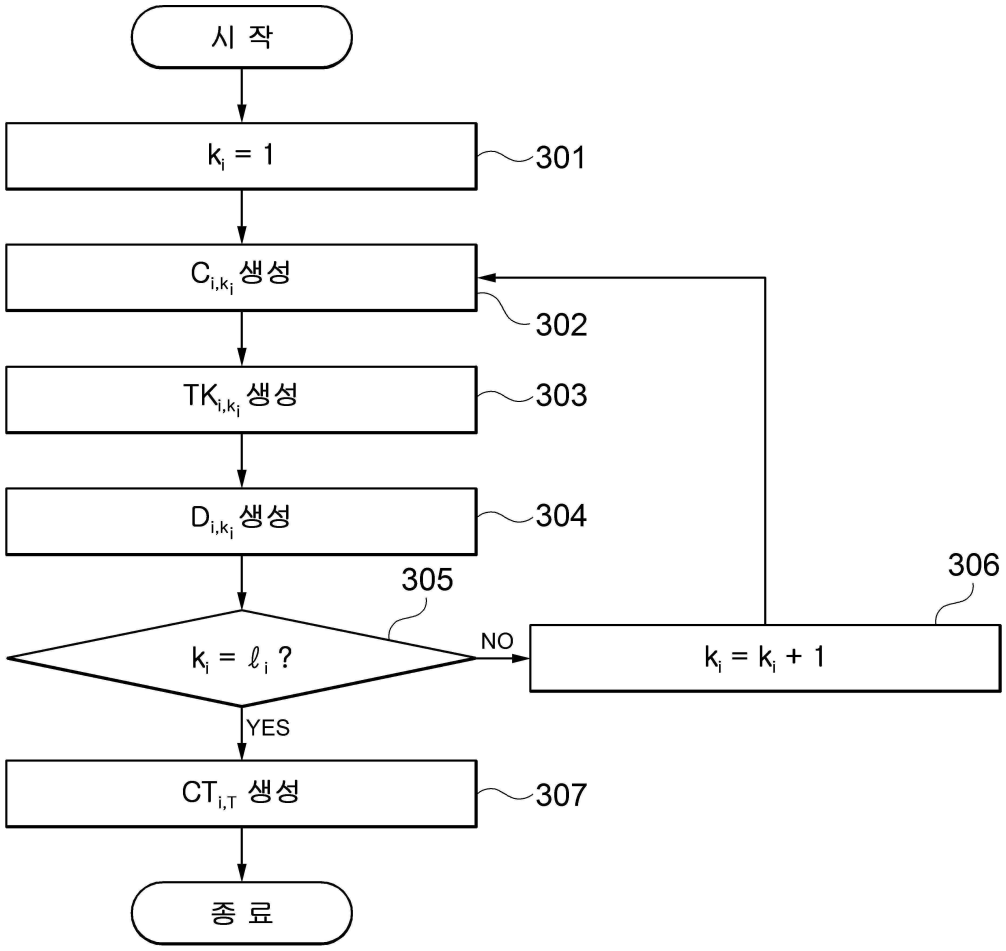
100



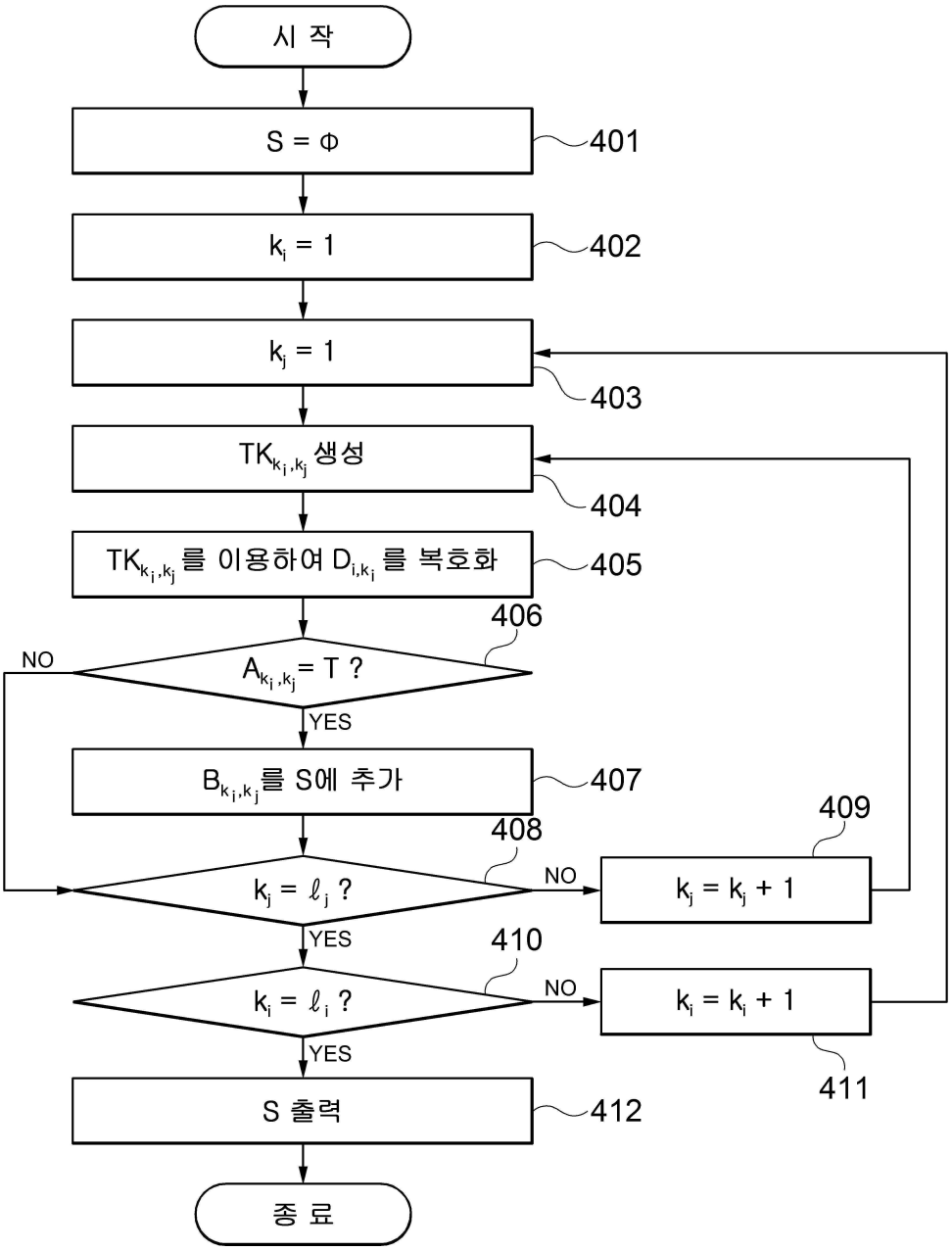
도면2


키 생성 장치
110
제1 암호화 장치
120
제2 암호화 장치
130
복호화 장치
140
셋업(201)
EKi 생성(203)
EKj 생성(206)
SKi,j,T 생성(213)
EKi 요청(202)
EKi (204)
EKj 요청(205)
EKj (207)
Xi 암호화(208)
CTi,T (209)
SKi,j,T 요청(212)
SKi,j,T (214)
Xj 암호화(210)
CTi,T' (211)
S 생성(215)

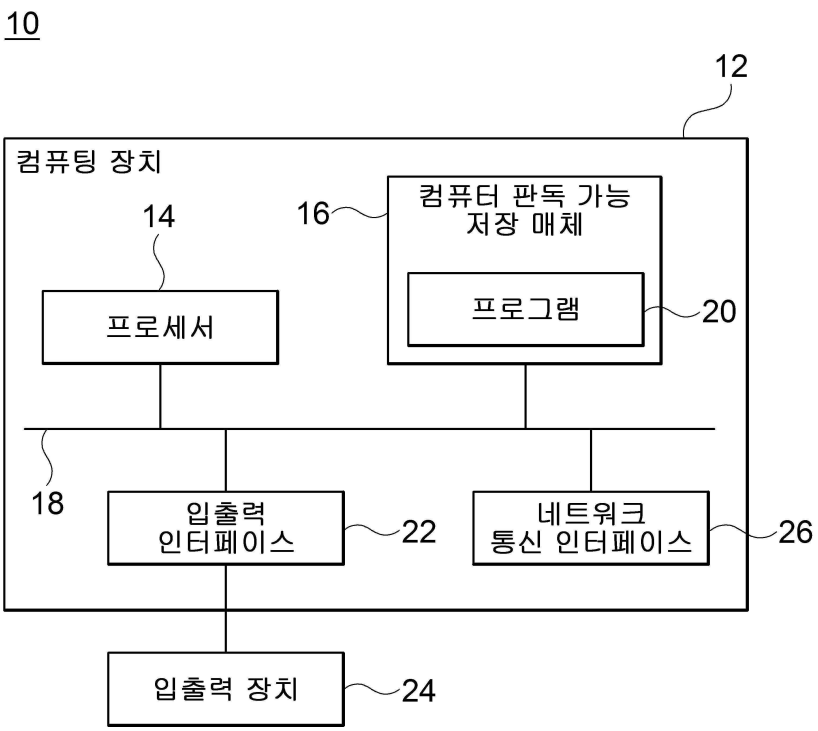
도면3


시 작
$k_i = 1$
301
C_{i,k_i} 생성
302
TK_{i,k_i} 생성
303
D_{i,k_i} 생성
304
305
$k_i = \ell_i$?
NO
306
$k_i = k_i + 1$
YES
$CT_{i,T}$ 생성
307
종 료

도면4


시 작
S = Φ
401
k_i = 1
402
k_j = 1
403
TK_{k_i,k_j} 생성
404
TK_{k_i,k_j}를 이용하여 D_{i,k_i}를 복호화
405
406
A_{k_i,k_j} = T ?
NO
YES
B_{k_i,k_j}를 S에 추가
407
409
408
k_j = ℓ_j ?
NO
k_j = k_j + 1
YES
410
k_i = ℓ_i ?
NO
k_i = k_i + 1
YES
411
S 출력
412
종 료

도면5


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