



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0002729  
(43) 공개일자 2012년01월09일

(51) Int. Cl.

G06F 17/30 (2006.01) H04L 9/14 (2006.01)

G06F 21/24 (2006.01) G06F 15/16 (2006.01)

(21) 출원번호 10-2010-0063390

(22) 출원일자 2010년07월01일

심사청구일자 2010년07월01일

(71) 출원인

고려대학교 산학협력단

서울특별시 성북구 종암로 1 (안암동5가, 고려대역)

(72) 발명자

정익래

서울특별시 노원구 공릉로34길 62, 1014동 1303호 (공릉동, 태강아파트)

김동민

서울특별시 동대문구 약령시로 154, 1동 505호 (청량리동, 미주아파트)

(뒷면에 계속)

(74) 대리인

특허법인엠에이피에스

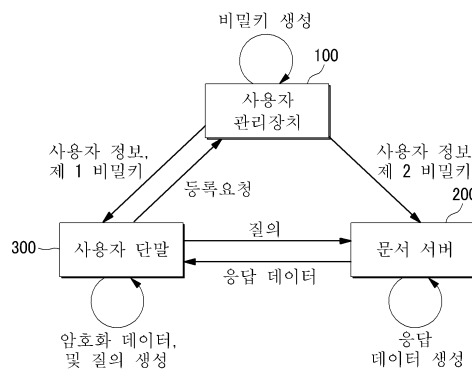
전체 청구항 수 : 총 17 항

#### (54) 암호화 문서에 대한 다자간 검색 시스템 및 그 방법

#### (57) 요약

다자간 검색 시스템은 사용자 등록 요청에 따라, 사용자 등록을 요청한 사용자의 사용자 단말에 제 1 비밀키를 발급하고, 제 1 비밀키가 포함되도록 생성한 제 2 비밀키 및 사용자의 식별정보를 문서 관리부에 제공하는 사용자 관리부, 사용자 단말로부터 수신한 난수 및 제 2 비밀키를 이용하여, 문서를 암호화하는 문서 암호화키의 생성에 사용되는 제 1 생성키 및 문서에 대한 키워드를 암호화하는 키워드 인덱스 생성키의 생성에 사용되는 제 2 생성키를 생성하여 사용자 단말에 제공하고, 사용자 단말로부터 수신한 암호화된 문서 및 암호화된 키워드를 저장하는 문서 관리부를 포함하되, 암호화된 문서는 제 1 생성키에 기초하여 생성된 문서 암호화키에 의하여 사용자 단말에서 암호화된 것이고, 암호화된 키워드는 제 2 생성키에 기초하여 생성된 키워드 인덱스 생성키에 의하여 사용자 단말에서 암호화된 것이다.

대표도 - 도1



(72) 발명자

**천지영**

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

**노건태**

서울특별시 강남구 개포로 516, - 707동 1304호 (개  
포동, 개포주공아파트706동)

이 발명을 지원한 국가연구개발사업

과제고유번호 1091205002100010000412098208298

부처명 (재)한국콘텐츠진흥원

연구관리전문기관

연구사업명 문화콘텐츠기술(CT)개발지원사업

연구과제명 저작권 보호 및 공정이용 연구센터

기여율

주관기관 고려대학교 산학협력단

연구기간 2009년 06월 26일 ~ 2010년 04월 25일

---

## 특허청구의 범위

### 청구항 1

다자간 검색 시스템에 있어서,

사용자 등록 요청에 따라, 상기 사용자 등록을 요청한 사용자의 사용자 단말에 제 1 비밀키를 발급하고, 상기 제 1 비밀키가 포함되도록 생성한 제 2 비밀키 및 상기 사용자의 식별정보를 문서 관리부에 제공하는 사용자 관리부 및

상기 사용자 단말로부터 수신한 난수 및 상기 제 2 비밀키를 이용하여, 문서를 암호화하는 문서 암호화키의 생성에 사용되는 제 1 생성키 및 상기 문서에 대한 키워드를 암호화하는 키워드 인덱스 생성키의 생성에 사용되는 제 2 생성키를 생성하여 상기 사용자 단말에 제공하고, 상기 사용자 단말로부터 수신한 상기 암호화된 문서 및 암호화된 키워드를 저장하는 문서 관리부를 포함하되,

상기 암호화된 문서는 상기 제 1 생성키에 기초하여 생성된 문서 암호화키에 의하여 상기 사용자 단말에서 암호화된 것이고, 상기 암호화된 키워드는 상기 제 2 생성키에 기초하여 생성된 키워드 인덱스 생성키에 의하여 상기 사용자 단말에서 암호화된 것인 다자간 검색 시스템.

### 청구항 2

제 1 항에 있어서,

상기 사용자 단말은 사용자의 키워드 입력에 따라 상기 키워드, 상기 사용자의 식별정보 및 상기 사용자 단말의 제 1 비밀키가 포함된 쿼리값을 생성하여 상기 문서 관리부로 전송하고, 상기 문서 관리부로부터 수신한 암호화된 문서를 복호화하는 것인 다자간 검색 시스템.

### 청구항 3

제 2 항에 있어서,

상기 문서 관리부는 상기 사용자가 사용자 리스트에 등록된 사용자인 경우, 상기 쿼리값 및 상기 사용자의 제 2 비밀키에 기초하여 키워드 인덱스 생성키를 산출하고, 상기 산출된 키워드 인덱스 생성키에 해당하는 암호화된 문서를 검색하여, 상기 암호화된 문서 및 상기 암호화된 문서에 대한 제 1 생성키를 상기 사용자 단말로 전송하는 것인 다자간 검색 시스템.

### 청구항 4

제 3 항에 있어서,

상기 사용자 단말은 상기 문서 관리부로부터 수신한 상기 제 1 생성키로부터 상기 암호화된 문서에 대한 문서 암호화키를 산출하고, 상기 산출한 문서 암호화키에 기초하여 상기 암호화된 문서를 복호화하는 것인 다자간 검색 시스템.

### 청구항 5

제 3 항에 있어서,

상기 문서 관리부는,

상기 사용자 등록을 요청한 사용자의 식별정보 및 상기 제 1 비밀키가 포함되도록 생성한 상기 제 2 비밀키를 사용자별로 관리하는 사용자 리스트 관리부,

상기 사용자 단말로부터 수신한 난수 및 상기 제 2 비밀키를 이용하여 상기 문서 암호화키의 생성에 사용되는 제 1 생성키 및 상기 키워드 인덱스 생성키의 생성에 사용되는 제 2 생성키를 생성하는 키 생성부,

상기 암호화된 문서 및 암호화된 키워드를 저장하는 암호화 데이터 저장부 및

상기 쿼리값 및 상기 사용자의 제 2 비밀키에 기초하여 상기 키워드 인덱스 생성키를 산출하고, 상기 산출된 키워드 인덱스 생성키에 해당하는 암호화된 문서를 검색하여, 상기 암호화된 문서 및 상기 암호화된 문서에 대한 제 1 생성키를 상기 사용자 단말로 전송하는 데이터 검색부를 포함하는 다자간 검색 시스템.

## 청구항 6

제 5 항에 있어서,

상기 사용자 리스트 관리부는,

사용자 탈퇴를 요청한 사용자의 식별정보 및 상기 사용자 탈퇴를 요청한 사용자의 제 2 비밀키를 상기 사용자 리스트로부터 제거하는 것인 다자간 검색 시스템.

## 청구항 7

제 3 항에 있어서,

상기 사용자 단말은,

상기 문서 암호화키를 생성하여 상기 문서 관리부에 저장할 문서를 암호화하고, 상기 키워드 인덱스 생성키를 생성하여 상기 문서에 대한 키워드를 암호화하는 데이터 암호화부,

상기 사용자의 키워드 입력에 따라 상기 키워드, 상기 사용자의 식별정보 및 상기 사용자 단말의 제 1 비밀키가 포함된 상기 쿼리값을 생성하는 쿼리 생성부 및

상기 문서 관리부로부터 수신한 상기 제 1 생성키로부터 상기 암호화된 문서에 대한 문서 암호화키를 산출하고, 상기 산출한 문서 암호화키에 기초하여 상기 암호화된 문서를 복호화하는 데이터 복호화부를 포함하는 다자간 검색 시스템.

## 청구항 8

제 1 항에 있어서,

상기 사용자 관리부는,

상기 사용자 등록을 요청한 사용자의 식별정보를 사용자 리스트로 관리하는 사용자 리스트 관리부 및

상기 사용자 관리부의 비밀키를 이용하여 상기 사용자 등록을 요청한 사용자의 사용자 단말에 발급할 상기 제 1 비밀키 및 상기 문서 관리부에 제공할 상기 제 1 비밀키가 포함되도록 생성한 상기 제 2 비밀키를 생성하는 키 생성부를 포함하는 다자간 검색 시스템.

## 청구항 9

다자간 검색 방법에 있어서,

사용자 관리장치가 사용자 등록 요청에 따라, 상기 사용자 등록을 요청한 사용자의 사용자 단말에 제 1 비밀키를 발급하고, 상기 제 1 비밀키가 포함되도록 생성한 제 2 비밀키 및 상기 사용자의 식별정보를 문서 서버에 제공하는 단계,

상기 문서 서버가 상기 사용자 단말로부터 수신한 난수 및 상기 제 2 비밀키를 이용하여, 문서를 암호화하는 문서 암호화키의 생성에 사용되는 제 1 생성키 및 상기 문서에 대한 키워드를 암호화하는 키워드 인덱스 생성키의

생성에 사용되는 제 2 생성키를 생성하여 상기 사용자 단말에 제공하는 단계 및

상기 문서 서버가 상기 문서 암호화키를 이용하여 암호화된 문서 및 상기 키워드 인덱스 생성키를 이용하여 암호화된 키워드를 상기 사용자 단말로부터 수신하여 저장하는 단계를 포함하되,

상기 문서 암호화키는 상기 제 1 생성키에 기초하여 생성되고, 상기 키워드 인덱스 생성키는 상기 제 2 생성키에 기초하여 생성된 것인

다자간 검색 방법.

#### 청구항 10

제 9 항에 있어서,

상기 문서 서버가 상기 사용자가 사용자 리스트에 등록된 사용자인 경우, 상기 사용자 단말로부터 수신한 쿼리 값 및 상기 사용자의 제 2 비밀키에 기초하여 키워드 인덱스 생성키를 산출하고, 상기 산출된 키워드 인덱스 생성키에 해당하는 암호화된 문서를 검색하여, 상기 암호화된 문서 및 상기 암호화된 문서에 대한 제 1 생성키를 상기 사용자 단말로 전송하는 단계를 더 포함하는 다자간 검색 방법.

#### 청구항 11

제 10 항에 있어서,

상기 사용자 단말은 사용자의 키워드 입력에 따라 상기 키워드, 상기 사용자의 식별정보 및 상기 사용자 단말의 제 1 비밀키가 포함된 상기 쿼리값을 생성하는 것인 다자간 검색 방법.

#### 청구항 12

제 10 항에 있어서,

상기 사용자 단말은 상기 문서 서버로부터 수신한 상기 제 1 생성키로부터 상기 암호화된 문서에 대한 문서 암호화키를 산출하고, 상기 산출한 문서 암호화키에 기초하여 상기 암호화된 문서를 복호화하는 것인 다자간 검색 방법.

#### 청구항 13

제 9 항에 있어서,

상기 문서 서버가 사용자 탈퇴를 요청한 사용자의 식별정보 및 상기 사용자 탈퇴를 요청한 사용자의 제 2 비밀키를 사용자 리스트로부터 제거하는 단계를 더 포함하는 다자간 검색 방법.

#### 청구항 14

다자간 검색 시스템에 있어서,

사용자 등록 요청에 따라, 상기 사용자 등록을 요청한 사용자의 사용자 단말에 제 1 비밀키를 발급하고, 상기 제 1 비밀키가 포함되도록 생성한 제 2 비밀키 및 상기 사용자의 식별정보를 문서 서버에 제공하는 사용자 관리 장치,

문서 암호화키를 생성하여 상기 문서 서버에 저장할 문서를 암호화하고, 키워드 인덱스 생성키를 생성하여 상기 문서에 대한 키워드를 암호화하며, 상기 암호화된 문서 및 상기 암호화된 키워드를 상기 문서 서버로 전송하는 사용자 단말 및

상기 사용자 단말로부터 수신한 난수 및 상기 제 2 비밀키를 이용하여 상기 문서 암호화키의 생성에 사용되는

제 1 생성키 및 상기 키워드 인덱스 생성키의 생성에 사용되는 제 2 생성키를 생성하여 상기 사용자 단말에 제공하고, 상기 사용자 단말로부터 수신한 상기 암호화된 문서 및 암호화된 키워드를 저장하는 문서 서버를 포함하되,

상기 사용자 단말은 상기 제 1 생성키에 기초하여 상기 문서 암호화키를 생성하고, 상기 제 2 생성키에 기초하여 상기 키워드 인덱스 생성키를 생성하는 것인 다자간 검색 시스템.

## 청구항 15

제 14 항에 있어서,

상기 사용자 단말은 사용자의 키워드 입력에 따라 상기 키워드, 상기 사용자의 식별정보 및 상기 사용자 단말의 제 1 비밀키가 포함된 쿼리값을 생성하여 상기 문서 서버로 전송하고, 상기 문서 서버로부터 수신한 암호화된 문서를 복호화하는 것인 다자간 검색 시스템.

## 청구항 16

제 15 항에 있어서,

상기 문서 서버는 상기 사용자가 사용자 리스트에 등록된 사용자인 경우, 상기 쿼리값 및 상기 사용자의 제 2 비밀키에 기초하여 키워드 인덱스 생성키를 산출하고, 상기 산출된 키워드 인덱스 생성키에 해당하는 암호화된 문서를 검색하여, 상기 암호화된 문서 및 상기 암호화된 문서에 대한 제 1 생성키를 상기 사용자 단말로 전송하는 것인 다자간 검색 시스템.

## 청구항 17

제 16 항에 있어서,

상기 사용자 단말은 상기 문서 서버로부터 수신한 상기 제 1 생성키로부터 상기 암호화된 문서에 대한 문서 암호화키를 산출하고, 상기 산출한 문서 암호화키에 기초하여 상기 암호화된 문서를 복호화하는 것인 다자간 검색 시스템.

## 명세서

### 기술분야

[0001] 본 발명은 보안성이 보장되고, 효율적인 키워드 검색을 제공하는 다자간 검색 시스템 및 그 방법에 관한 것이다.

### 배경기술

[0002] 최근 클라우드 컴퓨팅(cloud computing) 기술의 발달과 더불어 인터넷을 통해 자료를 공유할 수 있는 클라우드 기반 스토리지(storage) 서비스가 주목받고 있다. 스토리지 서비스를 통해 사용자 단말들은, 공공의 서버(public server)에 자신의 자료를 업로드(upload)하고, 관심있는 자료를 다운로드(download) 받을 수 있다.

[0003] 그러나, 공공의 서버를 통한 자료의 공유는 사용자 단말들의 편리성을 증가시킨 반면 사용자 단말들의 프라이버시에 대한 문제점이 있다. 공공의 서버에 저장된 자료는 사용자 단말들이 아닌 서비스 제공자에 의해 관리되므로 신뢰할 수 없는 서비스 제공자에 의한 데이터 노출은 단순한 접근통제만으로 해결하기 힘들다.

[0004] 또한, 신뢰할 수 없는 서비스 제공자에 대한 데이터 노출을 막기 위해서 데이터를 암호화하여 저장할 수도 있으나, 이러한 데이터 암호화는 검색의 효율을 급격히 저하시킨다.

[0005] 이러한 검색 문제를 해결하기 위해 대칭키(symetric key) 기반 및 공개키(public key) 기반으로 키워드를 이용하여 암호화된 문서를 검색하는 연구가 활발히 진행되고 있다. 대칭키 기반의 키워드 검색은 사용자 단말이 자신의 대칭키로 데이터를 암호화하여 서버에 저장한 후, 자신의 대칭키를 이용하여 문서를 검색하는 방법으로 데

이터 암호화에 사용한 대칭키를 소유한 사용자 단말만이 검색이 가능하다.

[0006] 그리고, 공개키 기반의 키워드 검색 기법은 암호화된 데이터와 함께 데이터검색 정보를 사용자 단말의 공개키로 암호화하여 서버에 저장한다. 이때, 암호화에 사용된 공개키에 대응되는 비밀키를 소유한 사람만이 검색이 가능한 기법이다. 그러나 대칭키 및 공개키 기반 검색 방법은, 특정 사용자 단말만이 검색이 가능하다. 따라서 이러한 기법은 여러 사용자 단말이 공공의 서버를 통해 데이터를 공유하는 환경에는 적합하지 않다.

[0007] 만약 N명의 사용자 단말이 서로의 데이터를 공유하는 환경이라면 데이터를 업로드하는 사용자 단말은 N명의 사용자 단말 모두에 대해서 문서 검색이 가능하도록 같은 데이터를 N번 암호화하여 저장하여야 한다. 이는 저장량 측면에서 매우 비효율적이다.

[0008] 한편, 최근에는 다자간 데이터 공유 환경에서 사용자 단말들의 프라이버시를 보호하면서도 문서 검색이 가능한 방법이 제안되었다. 그러나, 데이터를 업로드할 수 있는 사용자 단말이 특정한 한 명뿐이어서, 데이터 업로드가 가능한 사용자 단말은 데이터를 업로드 하기 전에 먼저 데이터를 다운로드 받을 다른 사용자 단말들을 정한 후, 해당 다른 사용자 단말들만이 데이터를 다운로드 받을 수 있도록 데이터를 암호화하여 저장한다. 따라서 이러한 방법은 여러 사용자 단말들이 자신의 데이터를 업로드하는 환경에는 적합하지 않다.

[0009] 또한 사전에 검색 가능한 사용자 단말들을 지정하기 때문에 추후 가입자나 탈퇴자가 발생하였을 경우 그에 따른 관리가 어렵다. 예를 들어, 탈퇴자 처리(revocation)를 위해 브로드캐스트 암호화(broadcast encryption)를 사용하기 때문에 탈퇴자 발생 시마다 다른 모든 사용자 단말들이 새로운 값을 갱신해야 하는 번거로움이 따른다. 또한 가입자나 탈퇴자 처리를 위해 모든 데이터에 대한 암호화된 인덱스를 수정해야 하므로 가입자나 탈퇴자 처리가 매우 비효율적이다.

[0010] 그리고, 암호화된 데이터에 대해 여러 사용자 단말들이 자신의 데이터를 업로드하고 다운로드받을 수 있는 환경으로 다자간 데이터 공유 환경에 적합한 방법도 있으나, 탈퇴자의 수동적 공격(passive attack)에 대해 안전하지 못한 측면이 있다. 즉, 기존 사용자 단말이 탈퇴할 경우 문서를 검색할 수는 없으나 다른 사용자 단말이 검색하는 데이터를 도청(eavesdropping)할 경우 도청한 모든 데이터에 대한 복호화가 가능하게 된다.

## 발명의 내용

### 해결하려는 과제

[0011] 본 발명의 일 실시예는 다자간 보안성이 보장될 수 있고, 효율적으로 암호화된 문서를 검색할 수 있는 다자간 검색 시스템 및 그 방법을 제공하는 데에 그 목적이 있다.

[0012] 또한, 본 발명의 일 실시예는 효과적이고 편리한 탈퇴자 처리 및 암호화된 문서에 대한 키워드 검색을 요청한 사용자의 쿼리에 대해, 해당 쿼리에 포함된 키워드에 관련된 암호화된 문서를 검색하여 전송하되, 암호화된 문서를 산출된 문서 암호화키를 이용하여 복호화시킬 수 있도록 함으로써, 외부 공격자에 의한 데이터 도청 문제를 해소시키는 다자간 검색 시스템 및 그 방법을 제공하는 데에 그 목적이 있다.

[0013] 또한, 본 발명의 일 실시예는 키워드로 검색하고자 하는 암호화된 문서에 대해 사용자가 정당하게 발급받은 자신의 비밀키를 이용하여 쿼리를 생성함으로써, 외부 공격자가 악의적인 목적으로 정당한 쿼리를 생성할 수 없게 하여, 쿼리에 대한 안정성이 확보될 수 있는 다자간 검색 시스템 및 그 방법을 제공하는 데에 그 목적이 있다.

### 과제의 해결 수단

[0014] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면에 따른 다자간 검색 시스템은 사용자 등록 요청에 따라, 사용자 등록을 요청한 사용자의 사용자 단말에 제 1 비밀키를 발급하고, 제 1 비밀키가 포함되도록 생성한 제 2 비밀키 및 사용자의 식별정보를 문서 관리부에 제공하는 사용자 관리부, 사용자 단말로부터 수신한 난수 및 제 2 비밀키를 이용하여, 문서를 암호화하는 문서 암호화키의 생성에 사용되는 제 1 생성키 및 문서에 대한 키워드를 암호화하는 키워드 인덱스 생성키의 생성에 사용되는 제 2 생성키를 생성하여 사용자 단말에 제공하고, 사용자 단말로부터 수신한 암호화된 문서 및 암호화된 키워드를 저장하는 문서 관리부를 포함하되, 암호화된 문서는 제 1 생성키에 기초하여 생성된 문서 암호화키에 의하여 사용자 단말에서 암호화된 것이고, 암호화된 키워드는 제 2 생성키에 기초하여 생성된 키워드 인덱스 생성키에 의하여 사용자 단말에서 암호화된 것이다.

[0015] 여기서, 사용자 단말은 사용자의 키워드 입력에 따라 키워드, 사용자의 식별정보 및 사용자 단말의 제 1 비밀키

가 포함된 쿼리값을 생성하여 문서 관리부로 전송하고, 문서 관리부로부터 수신한 암호화된 문서를 복호화한다.

- [0016] 그리고, 문서 관리부는 사용자가 사용자 리스트에 등록된 사용자인 경우, 쿼리값 및 사용자의 제 2 비밀키에 기초하여 키워드 인덱스 생성키를 산출하고, 산출된 키워드 인덱스 생성키에 해당하는 암호화된 문서를 검색하여, 암호화된 문서 및 암호화된 문서에 대한 제 1 생성키를 사용자 단말로 전송한다.
- [0017] 또한, 사용자 단말은 문서 관리부로부터 수신한 제 1 생성키로부터 암호화된 문서에 대한 문서 암호화키를 산출하고, 산출한 문서 암호화키에 기초하여 암호화된 문서를 복호화한다.
- [0018] 또한, 문서 관리부는, 사용자 등록을 요청한 사용자의 식별정보 및 제 1 비밀키가 포함되도록 생성한 제 2 비밀키를 사용자별로 관리하는 사용자 리스트 관리부, 사용자 단말로부터 수신한 난수 및 제 2 비밀키를 이용하여 문서 암호화키의 생성에 사용되는 제 1 생성키 및 키워드 인덱스 생성키의 생성에 사용되는 제 2 생성키를 생성하는 키 생성부, 암호화된 문서 및 암호화된 키워드를 저장하는 암호화 데이터 저장부 및 쿼리값 및 사용자의 제 2 비밀키에 기초하여 키워드 인덱스 생성키를 산출하고, 산출된 키워드 인덱스 생성키에 해당하는 암호화된 문서를 검색하여, 암호화된 문서 및 암호화된 문서에 대한 제 1 생성키를 사용자 단말로 전송하는 데이터 검색부를 포함한다.
- [0019] 여기서, 사용자 리스트 관리부는, 사용자 탈퇴를 요청한 사용자의 식별정보 및 사용자 탈퇴를 요청한 사용자의 제 2 비밀키를 사용자 리스트로부터 제거한다.
- [0020] 또한, 사용자 단말은, 문서 암호화키를 생성하여 문서 관리부에 저장할 문서를 암호화하고, 키워드 인덱스 생성키를 생성하여 문서에 대한 키워드를 암호화하는 데이터 암호화부, 사용자의 키워드 입력에 따라 키워드, 사용자의 식별정보 및 사용자 단말의 제 1 비밀키가 포함된 쿼리값을 생성하는 쿼리 생성부 및 문서 관리부로부터 수신한 제 1 생성키로부터 암호화된 문서에 대한 문서 암호화키를 산출하고, 산출한 문서 암호화키에 기초하여 암호화된 문서를 복호화하는 데이터 복호화부를 포함한다.
- [0021] 또한, 사용자 관리부는, 사용자 등록을 요청한 사용자의 식별정보를 사용자 리스트로 관리하는 사용자 리스트 관리부 및 사용자 관리부의 비밀키를 이용하여 사용자 등록을 요청한 사용자의 사용자 단말에 발급할 제 1 비밀키 및 문서 관리부에 제공할 제 1 비밀키가 포함되도록 생성한 제 2 비밀키를 생성하는 키 생성부를 포함한다.
- [0022] 본 발명의 제 2 측면에 따른 다자간 검색 방법은 사용자 관리장치가 사용자 등록 요청에 따라, 사용자 등록을 요청한 사용자의 사용자 단말에 제 1 비밀키를 발급하고, 제 1 비밀키가 포함되도록 생성한 제 2 비밀키 및 사용자의 식별정보를 문서 서버에 제공하는 단계, 문서 서버가 사용자 단말로부터 수신한 난수 및 제 2 비밀키를 이용하여 문서를 암호화하는 문서 암호화키의 생성에 사용되는 제 1 생성키 및 문서에 대한 키워드를 암호화하는 키워드 인덱스 생성키의 생성에 사용되는 제 2 생성키를 생성하여 사용자 단말에 제공하는 단계 및 문서 서버가 문서 암호화키를 이용하여 암호화된 문서 및 키워드 인덱스 생성키를 이용하여 암호화된 키워드를 사용자 단말로부터 수신하여 저장하는 단계를 포함하되, 문서 암호화키는 제 1 생성키에 기초하여 생성되고, 키워드 인덱스 생성키는 제 2 생성키에 기초하여 생성된 것이다.
- [0023] 여기서, 문서 서버가 사용자가 사용자 리스트에 등록된 사용자인 경우, 사용자 단말로부터 수신한 쿼리값 및 사용자의 제 2 비밀키에 기초하여 키워드 인덱스 생성키를 산출하고, 산출된 키워드 인덱스 생성키에 해당하는 암호화된 문서를 검색하여, 암호화된 문서 및 암호화된 문서에 대한 제 1 생성키를 사용자 단말로 전송하는 단계를 더 포함한다.
- [0024] 이때, 사용자 단말은 사용자의 키워드 입력에 따라 키워드, 사용자의 식별정보 및 사용자 단말의 제 1 비밀키가 포함된 쿼리값을 생성한다.
- [0025] 또한, 사용자 단말은 문서 서버로부터 수신한 제 1 생성키로부터 암호화된 문서에 대한 문서 암호화키를 산출하고, 산출한 문서 암호화키에 기초하여 암호화된 문서를 복호화한다.
- [0026] 본 발명의 제 3 측면에 따른 다자간 검색 시스템은 사용자 등록 요청에 따라, 사용자 등록을 요청한 사용자의 사용자 단말에 제 1 비밀키를 발급하고, 제 1 비밀키가 포함되도록 생성한 제 2 비밀키 및 사용자의 식별정보를 문서 서버에 제공하는 사용자 관리장치, 문서 암호화키를 생성하여 문서 서버에 저장할 문서를 암호화하고, 키워드 인덱스 생성키를 생성하여 문서에 대한 키워드를 암호화하며, 암호화된 문서 및 암호화된 키워드를 문서 서버로 전송하는 사용자 단말, 사용자 단말로부터 수신한 난수 및 제 2 비밀키를 이용하여 문서 암호화키의 생성에 사용되는 제 1 생성키 및 키워드 인덱스 생성키의 생성에 사용되는 제 2 생성키를 생성하여 사용자 단말에 제공하고, 사용자 단말로부터 수신한 암호화된 문서 및 암호화된 키워드를 저장하는 문서 서버를 포함하되, 사

용자 단말은 제 1 생성키에 기초하여 문서 암호화키를 생성하고, 제 2 생성키에 기초하여 키워드 인덱스 생성키를 생성한다.

[0027] 여기서, 사용자 단말은 사용자의 키워드 입력에 따라 키워드, 사용자의 식별정보 및 사용자 단말의 제 1 비밀키가 포함된 쿼리값을 생성하여 문서 서버로 전송하고, 문서 서버로부터 수신한 암호화된 문서를 복호화한다.

[0028] 그리고, 문서 서버는 사용자가 사용자 리스트에 등록된 사용자인 경우, 쿼리값 및 사용자의 제 2 비밀키에 기초하여 키워드 인덱스 생성키를 산출하고, 산출된 키워드 인덱스 생성키에 해당하는 암호화된 문서를 검색하여, 암호화된 문서 및 암호화된 문서에 대한 제 1 생성키를 사용자 단말로 전송한다.

[0029] 또한, 사용자 단말은 문서 서버로부터 수신한 제 1 생성키로부터 암호화된 문서에 대한 문서 암호화키를 산출하고, 산출한 문서 암호화키에 기초하여 암호화된 문서를 복호화한다.

### 발명의 효과

[0030] 전술한 본 발명의 과제 해결 수단 중 어느 하나에 의하면, 다자간 보안성이 보장될 수 있으며, 효율적으로 암호화된 문서를 검색할 수 있다.

[0031] 또한, 전술한 본 발명의 과제 해결 수단 중 어느 하나에 의하면, 효과적이고 편리한 탈퇴자 처리 및 암호화된 문서에 대한 키워드 검색을 요청한 사용자의 쿼리에 대해, 해당 쿼리에 포함된 키워드에 관련된 암호화된 문서를 검색하여 전송하되, 암호화된 문서를 산출된 문서 암호화키를 이용하여 복호화시킬 수 있도록 함으로써, 외부 공격자에 의한 데이터 도청 문제를 해소시킬 수 있다.

[0032] 또한, 전술한 본 발명의 과제 해결 수단 중 어느 하나에 의하면, 키워드로 검색하고자 하는 암호화된 문서에 대해 사용자가 정당하게 발급받은 자신의 비밀키를 이용하여 쿼리를 생성함으로써, 외부 공격자가 악의적인 목적으로 정당한 쿼리를 생성할 수 없게 하여, 쿼리에 대한 안정성이 확보될 수 있다.

### 도면의 간단한 설명

[0033] 도 1은 본 발명의 일 실시예에 따른 다자간 검색 시스템의 구성을 도시한다.

도 2는 본 발명의 일 실시예에 따른 사용자 관리장치의 블록도이다.

도 3은 본 발명의 일 실시예에 따른 문서 서버의 블록도이다.

도 4는 본 발명의 일 실시예에 따른 사용자 단말의 블록도이다.

도 5는 본 발명의 일 실시예에 따른 다자간 검색 시스템의 셋업, 등록, 탈퇴 과정을 나타낸다.

도 6은 본 발명의 일 실시예에 따른 다자간 검색 시스템의 저장 과정을 나타낸다.

도 7은 본 발명의 일 실시예에 따른 다자간 검색 시스템의 쿼리 및 검색 과정을 나타낸다.

도 8은 본 발명의 일 실시예에 따른 다자간 검색 방법의 순서도이다.

### 발명을 실시하기 위한 구체적인 내용

[0034] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0035] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0036] 도 1은 본 발명의 일 실시예에 따른 다자간 검색 시스템의 구성을 도시한다.

[0037] 도 1에 도시된 바와 같이, 다자간 검색 시스템은 사용자 관리장치(이하, “UM” 라고도 함)(100), 문서 서버(이하 “S” 라고도 함)(200) 및 사용자 단말(이하, “U” 라고도 함)(300)를 포함한다.

- [0038] 사용자 관리장치(100)는 사용자 등록 요청에 따라, 사용자 등록을 요청한 사용자의 사용자 단말(300)에 제 1 비밀키를 발급하고, 제 1 비밀키가 포함되도록 생성한 제 2 비밀키 및 사용자의 식별정보를 문서 서버(200)에 제공한다.
- [0039] 문서 서버(200)는 사용자 관리장치(100)로부터 수신한 사용자의 식별정보 및 제 2 비밀키를 저장한다. 또한, 문서 서버(200)는 암호화된 문서 및 해당 문서에 대한 암호화된 키워드를 포함하는 암호화된 데이터를 사용자 단말(300)로부터 수신하여 저장한다. 구체적으로, 암호화된 데이터는 다수의 속성들로 구성된  $m$ 개의 데이터  $(d_1, \dots, d_m)$ 가 암호화된 형태이며, 속성 중의 하나는 문서를 검색하기 위한 키워드를 포함할 수 있다.
- [0040] 또한, 문서 서버(200)는 문서 암호화키를 생성하기 위한 제 1 생성키 및 문서에 대한 키워드를 암호화하는 키워드 인덱스 생성키를 생성하기 위한 제 2 생성키를 사용자 단말(300)로부터 수신한 난수 및 제 2 비밀키를 이용하여 생성하여 사용자 단말(300)로 제공할 수 있다.
- [0041] 또한, 문서 서버(200)는 사용자가 사용자 리스트에 등록된 사용자인 경우, 사용자 단말(300)로부터 수신한 쿼리 값 및 사용자의 제 2 비밀키에 기초하여 키워드 인덱스 생성키를 산출하고, 산출된 키워드 인덱스 생성키에 해당하는 암호화된 문서를 검색하여, 암호화된 문서 및 암호화된 문서에 대한 생성키를 사용자 단말(300)로 전송한다.
- [0042] 사용자 단말(300)은 문서 암호화키를 생성하여 문서 서버(200)에 저장할 문서를 암호화하고, 키워드 인덱스 생성키를 생성하여 문서에 대한 키워드를 암호화하며, 암호화된 문서 및 암호화된 키워드를 문서 서버(200)로 전송한다. 이때, 사용자 단말(300)은 문서 서버(200)로부터 수신한 제 1 생성키에 기초하여 문서 암호화키를 생성하고, 제 2 생성키에 기초하여 키워드 인덱스 생성키를 생성할 수 있다.
- [0043] 또한, 사용자 단말(300)은 사용자의 키워드 입력에 따라 키워드, 사용자의 식별정보 및 사용자 단말(300)의 제 1 비밀키가 포함된 쿼리값을 생성하여 문서 서버(200)로 전송하고, 문서 서버(200)로부터 수신한 암호화된 문서를 복호화할 수 있다.
- [0044] 여기서, 사용자 단말(300)은 암호화된 문서 및 암호화된 문서에 대한 생성키를 문서 서버(200)로부터 수신하고, 해당 생성키로부터 암호화된 문서에 대한 문서 암호화키를 산출하고, 산출한 문서 암호화키에 기초하여 암호화된 문서를 복호화할 수 있다.
- [0045] 이하, 도 2 내지 도 4를 통해 다자간 검색 시스템의 각 구성요소에 대해서 보다 자세히 설명하기로 한다.
- [0046] 도 2는 본 발명의 일 실시예에 따른 사용자 관리장치의 블록도이다.
- [0047] 도 2에 도시된 바와 같이, 사용자 관리장치(100)는 사용자 리스트 관리부(110) 및 키 생성부(120)를 포함한다.
- [0048] 사용자 리스트 관리부(110)는 사용자 등록을 요청한 사용자의 식별정보를 사용자 리스트로 관리한다. 예컨대, 사용자 리스트 관리부(110)는 사용자 등록을 요청한 사용자의 식별정보를 사용자 관리장치(100)의 사용자 리스트에 포함시키거나, 사용자 탈퇴를 요청한 사용자의 식별정보를 사용자 관리장치(100)의 사용자 리스트로부터 제거할 수 있다.
- [0049] 키 생성부(120)는 사용자 관리장치(100)의 비밀키를 이용하여 사용자 등록을 요청한 사용자의 사용자 단말(300)에게 발급할 제 1 비밀키 및 문서 서버(200)에 제공할 제 1 비밀키가 포함되도록 생성한 제 2 비밀키를 생성한다.
- [0050] 도 3은 본 발명의 일 실시예에 따른 문서 서버의 블록도이다.
- [0051] 도 3에 도시된 바와 같이, 문서 서버(200)는 사용자 리스트 관리부(210), 암호화 데이터 저장부(220), 키 생성부(230) 및 데이터 검색부(240)를 포함한다.
- [0052] 사용자 리스트 관리부(210)는 사용자 등록을 요청한 사용자의 식별정보 및 제 1 비밀키가 포함되도록 생성한 제 2 비밀키를 사용자별로 관리한다. 여기서 사용자 리스트 관리부(210)는, 사용자 탈퇴를 요청한 사용자의 식별정보 및 사용자 탈퇴를 요청한 사용자의 제 2 비밀키를 사용자 리스트로부터 제거할 수 있다.
- [0053] 따라서, 탈퇴한 사용자의 식별정보 및 비밀키가 삭제되므로, 탈퇴한 외부 사용자로부터 문서를 안전하게 보호할 수 있다.
- [0054] 암호화 데이터 저장부(220)는 사용자 단말(300)로부터 수신한 암호화된 문서 및 암호화된 키워드를 저장한다.

- [0055] 키 생성부(230)는 사용자 단말(300)로부터 수신한 난수 및 제 2 비밀키를 이용하여 문서 암호화키의 생성에 사용되는 제 1 생성키 및 키워드 인덱스 생성키의 생성에 사용되는 제 2 생성키를 생성한다.
- [0056] 여기서, 제 1 생성키 및 제 2 생성키는 사용자 단말(300)로 전달되어, 각각 문서를 암호화하는 문서 암호화키 및 문서에 대한 키워드를 암호화하는 키워드 인덱스 생성키를 생성하는 데에 이용될 수 있다.
- [0057] 데이터 검색부(240)는 사용자 단말(300)로부터 수신한 쿼리값 및 사용자의 제 2 비밀키에 기초하여 키워드 인덱스 생성키를 산출하고, 산출된 키워드 인덱스 생성키에 해당하는 암호화된 문서를 검색하여, 검색된 암호화된 문서 및 암호화된 문서에 대한 생성키를 사용자 단말(300)로 전송한다.
- [0058] 여기서, 사용자 단말(300)은 검색된 암호화된 문서 및 암호화된 문서에 대한 생성키를 문서 서버(200)로부터 수신하고, 해당 생성키로부터 암호화된 문서에 대한 문서 암호화키를 산출하고, 산출한 문서 암호화키에 기초하여 암호화된 문서를 복호화할 수 있게 된다.
- [0059] 따라서, 암호화된 문서에 대한 키워드 검색을 요청한 사용자의 쿼리에 대해, 해당 쿼리에 포함된 키워드에 관련된 암호화된 문서를 검색하여 전송하되, 암호화된 문서를 산출된 문서 암호화키를 이용하여 복호화시킬 수 있도록 함으로써, 외부 공격자에 의한 데이터 도청 문제를 해소시킬 수 있게 된다.
- [0060] 도 4는 본 발명의 일 실시예에 따른 사용자 단말의 블록도이다.
- [0061] 도 4에 도시된 바와 같이, 사용자 단말(300)은 식별정보 관리 요청부(310), 데이터 암호화부(320), 쿼리 생성부(330) 및 데이터 복호화부(340)를 포함한다.
- [0062] 식별정보 관리 요청부(310)는 사용자 관리장치(100)로 사용자의 식별정보를 전송하여 식별정보에 대한 등록 또는 탈퇴 요청을 수행한다.
- [0063] 데이터 암호화부(320)는 문서 암호화키를 생성하여 문서 서버(200)에 저장할 문서를 암호화하고, 키워드 인덱스 생성키를 생성하여 문서에 대한 키워드를 암호화한다. 이때, 제 1 생성키에 기초하여 문서 암호화키를 생성하고, 제 2 생성키에 기초하여 키워드 인덱스 생성키를 생성할 수 있다.
- [0064] 쿼리 생성부(330)는 사용자의 키워드 입력에 따라 키워드, 사용자의 식별정보 및 사용자 단말(300)의 제 1 비밀키가 포함된 쿼리값을 생성한다.
- [0065] 데이터 복호화부(340)는 암호화된 문서 및 암호화된 문서에 대한 생성키를 문서 서버(200)로부터 수신하고, 해당 생성키로부터 암호화된 문서에 대한 문서 암호화키를 산출하고, 산출한 문서 암호화키에 기초하여 암호화된 문서를 복호화한다.
- [0066] 한편 이하의 본 발명의 실시예에서, 예컨대  $x \in_R X$  표기는 집합  $X$ 의 원소  $x$ 를 랜덤하게 선택하는 것을 나타내며,  $|X|$ 는 집합  $X$ 의 크기를 나타낸다. 또한,  $x \leftarrow A$  표기는 알고리즘  $A$ 에서  $x$ 를 출력하는 것을 나타낸다. 그리고  $v(k): N \rightarrow R$  표기는 모든 양의 정수  $c$ 에 대하여 정수  $N_c$ 가 존재하고,  $k > N_c, |v(k)| < 1/k^c$ 를 만족할 때 무시할 수 있을 만큼 작은 값으로 수렴하는 함수(negligible function)로 정의된다.
- [0067] 또한, 본 발명의 실시예에서 이용되는 의사난수 함수(pseudorandom function)는 난수 함수(random function)의 출력 값과 효율적으로 구별이 불가능한 출력 값을 가지는 함수로 정의된다. 구체적으로 의사난수 함수는  $f: \{0,1\}^j \times \{0,1\}^m \rightarrow \{0,1\}^n$
- [0068] 로 정의될 수 있으며, 여기서  $j$ 는 시드(seed) 값의 비트수,  $m$ 은 입력 값의 비트수,  $n$ 은 출력 값의 비트수를 나타낸다.
- [0069] 또한, 본 발명의 실시예에서 이용되는 암호학적 해시 함수(예컨대, 후술될  $H, h$ )는 일반적으로 의사난수 함수로부터 모델링된다. 이때, 의사난수 함수 중에서 입력 값의 비트수와 출력 값의 비트수가 같을 경우, 이것을

의사난수 치환(pseudorandom permutation)이라고 정의한다. 구체적으로 의사난수 치환은

$$p: f: \{0,1\}^j \times \{0,1\}^n \rightarrow \{0,1\}^n$$

[0070] 로 정의될 수 있다. 일반적으로 안전한 대칭키 암호화 기법은 의사난수 치환을 이용하여 모델링된다. 예컨대, 후술될  $E(\cdot)$ 가 의사 난수 치환으로,  $h_s(\cdot)$ 가 의사 난수 함수로 모델링될 수 있다.

[0071] 또한, 본 발명의 실시예에서는 곱선형 사상(bilinear maps)을 제공하는 소수 위수의 어떤 유한군을 이용한다. 예컨대  $G$ 와  $G_1$ 이 소수 위수  $P$ 를 가지는 두 개의 군이라 하고, 곱선형 사상을

$$e: G \times G \rightarrow G_1$$

라고 하면, 이하의 (가) 내지 (다)를 만족한다.

[0072] (가) 모든  $g, g' \in G$ 와 모든  $a, b \in \mathbb{Z}_P^*$ 에 대해  $e(g^a, g'^b) = e(g, g')^{ab}$  를 만족한다. 참고로,  $e$ 는 암호화에 이용되는 대칭키를 나타내고,  $g$ 는 상수를 나타낸다.

[0073] (나) 만약  $g$ 가 군  $G$ 의 생성자이면,  $e(g, g)$ 는 군  $G_1$ 의 생성자이다.

[0074] (다) 임의의 원소  $g, g' \in G$ 에 대해  $e(g, g')$ 는 계산하기 쉬워야 한다.

[0075] 또한, 본 발명의 실시예에서 이용되는 BLS 짧은 서명(short signature)은, Boneh 등에 의해 제안된 곱선형 사상에 기반을 둔 서명 기법이다. 예컨대, 후술될 BLS 짧은 서명의 변수들인  $(G, G_1, e)$ 를 곱선형 사상과 동일하게

$$h: \{0,1\}^* \rightarrow G$$

정의하고,  $g$ 를 군  $G$ 의 생성자, 충돌 저항성 해시 함수를, 사용자 단말의 서명키를  $k \in \mathbb{Z}_P^*$ , 검증키를  $y = g^k \in G$ 라고 정의한다.

[0076] 여기서, 메시지  $m$ 에 대한 서명을  $\sigma = h(m)^k$ 라고 하면, 이에 대한 검증은

$$e(g, \sigma) = e(y, h(m))$$

을 통해 가능하다. BLS 짧은 서명은 CDH(Computational Diffie-Hellman) 문제의 어려움에 기반하여 랜덤 오라클 모델에서 서명 위조 불가능성을 만족한다.

[0077] 이하 도 5 내지 도 7을 통해 각 과정에 따른 다자간 키워드 검색을 제공하는 다자간 검색 시스템의 동작에 대해서 구체적으로 설명하기로 한다.

[0078] 도 5는 본 발명의 일 실시예에 따른 다자간 검색 시스템의 셋업, 사용자 등록, 사용자 탈퇴 과정을 나타낸다.

[0079] 도 5에 도시된 바와 같이, 셋업(Setup) 과정에 있어서, 사용자 관리장치(100)는 공개 파라미터( $params$ )와 자신의 비밀키( $sk_{UM}$ )를 생성한다.

[0080] 구체적으로 설명하자면, 사용자 관리장치(100)는 시큐리티 파라미터(security parameter)(예컨대  $1^k$ )를 이용하여 공개 파라미터( $params$ )를 설정하고, 자신의 비밀키( $k_m \in \mathbb{Z}_P^*$ )를 랜덤하게 선택한다.

[0081] 그리고 안전한 대칭키 암호화 기법( $E$ ), 충돌 저항성(collision resistance) 해시함수

$$H: G_1 \rightarrow K$$

( $H$ ), 해시함수의 시드값( $s \in_R S$ )을 랜덤하게 선택하고, 시드를 포함하는 충돌 저항성 해시함수( $h_s: S \times W \rightarrow G$ )를 설정한다. 여기서  $K$ 는 키들의 집합,  $S$ 는 시드들의

집합,  $W$ 는 키워드들의 집합을 나타낸다.

[0082] 다음으로 사용자 등록(Join) 과정에 있어서, 사용자가 사용자 관리장치(100)로 사용자 등록을 요청하면, 사용자 관리장치(100)는 자신의 비밀키 값( $sk_{um}$ )을 이용하여 사용자 등록을 요청한 사용자에게 제공할 비밀키( $qk_u$ )를 생성하여 발급한다.

[0083] 보다 자세히 설명하자면, 사용자 등록을 원하는 사용자가 사용자 관리장치(100)로 식별정보( $u$ )(또는 고유정보)를 전송하면, 사용자 관리장치(100)은 해당 식별정보( $u$ )를 사용자 관리장치측 사용자 리스트( $U_{list}$ )에 포함시킨다.

[0084] 그리고 사용자 관리장치(100)는 사용자의 비밀키  $k_u \in \mathbb{Z}_P^*$  (제 1 비밀키)를 랜덤하게 선택하고, 자신의 비밀키( $sk_{um}$ ) 및 제 1 비밀키를 이용하여 문서 서버(200)에 제공할 비밀키  $s_u$  (제 2 비밀키)를 생성한다. 여기서, 제 2 비밀키는 사용자의 식별정보( $u$ )에 대응된 정보일 수 있다.

[0085] 또한, 사용자 관리장치(100)는 사용자 단말(300)에 제 1 비밀키 및 해시함수의 시드값( $\{k_u, s\}$ ), 문서 서버(200)에 사용자의 식별정보 및 제 2 비밀키( $\{u, s_u\}$ )를 각각 전송한다. 여기서, 문서 서버(200)는 자신의 사용자 리스트( $SU_{list}$ )에 사용자의 식별정보 및 제 2 비밀키를 포함시킨다.

[0086] 다음으로 사용자 탈퇴(Revoke) 과정에 있어서, 사용자 관리장치(100)는 사용자 탈퇴를 요청한 사용자( $u$ )를 사용자 리스트( $U_{list}$ )에서 제거하고, 문서 서버(200)에 해당 사용자의 식별정보( $u$ )를 전송한다. 그러면, 문서 서버(200)는 자신의 사용자 리스트( $SU_{list}$ )에서 사용자 탈퇴를 요청한 사용자의 식별정보 및 제 2 비밀키( $\{u, s_u\}$ )를 제거하게 된다.

[0087] 도 6은 본 발명의 일 실시예에 따른 다자간 검색 시스템의 저장 과정을 나타낸다.

[0088] 도 6에 도시된 바와 같이, 데이터 저장(Store) 과정에 있어서, 사용자 단말(300)는 사용자 관리장치(100)로부터 수신한  $qk_u$  (즉,  $\{k_u, s\}$ )를 이용하여 문서( $d$ )와 상기 문서에 대한 키워드( $w$ )를 암호화한 암호화된 데이터( $El_i$ )를 문서 서버(200)로 전송한다.

[0089] 그러면, 문서 서버(200)는 해당 사용자의 식별정보( $u$ )가 사용자 리스트( $SU_{list}$ )에 등록되었는지 여부를 검사하고,  $El_i$ 를  $El_D$ 에 저장한다. 참고로, 문서 서버(200)에  $i$  (양의 정수) 번째 저장되는 문서와 키워드를 각각  $(d_i, w_i)$ 라고 하면,  $(d_i, w_i)$ 를 암호화한 암호화된 데이터는  $El_{d_i}$ 로 표기되고, 이러한  $El_d$ 들의 집합은  $El_D$ 로 표기된다.

[0090] 보다 구체적으로 설명하자면, 사용자 단말(300)는 문서( $d$ )를 암호화하기 위한 문서 암호화키( $k_{d_i}$ ) 및 키워드( $w$ )에 대한 키워드 인덱스 생성키( $k_{w_i}$ )를 생성하기 위해, 먼저 난수( $r_i \in \mathbb{Z}_R^*$ )와 난수( $t_i \in \mathbb{Z}_R^*$ )를 랜덤하게 선택하고, 난수화된 키워드( $w$ ) 정보를 포함하는  $\{u, g^{t_i}, h_s(w)^{r_i}\}$ 를 생성하여 문서 서버(200)로 전송한다. 여기서,  $r_i$  및  $t_i$ 는 난수화 값으로 각각  $k_{d_i}$  및  $k_{w_i}$ 를 생성할 때 사용될 수 있다.

[0091] 그러면 문서 서버(200)는 해당 사용자의 식별정보( $u$ )가 등록되어 있는지 여부를 검사하고, 문서 암호화키 및

키워드 인덱스 생성키( $k_{d_i}$  및  $k_{w_i}$ )를 생성하기 위한 제 1 및 제 2 생성키 값( $\overline{k_{d_i}}$  및  $\overline{k_{w_i}}$ )을 상술된 곱선형 사상 함수를 이용하여 아래 수학식 (1) 및 (2)와 같이 생성해서 사용자 단말(300)로 전송한다.

[수학식 1]

$$\overline{k_{d_i}} = e(g^{t_i}, s_u) = e(g^{t_i}, g^{k_m/k_u})$$

[수학식 2]

$$\overline{k_{w_i}} = e(h_s(w)^{r_i}, s_u) = e(h_s(w)^{r_i}, g^{k_m/k_u})$$

여기서, 상술된 사용자 관리장치(100)로부터 수신한 사용자의 식별정보에 대응되는 제 2 비밀키 값( $s_u$ ) 및 난수

화된 키워드( $w$ ) 정보를 포함하는  $\{u, g^{t_i}, h_s(w)^{r_i}\}$  정보가 이용될 수 있다.

그리고, 상술된 탈퇴한 사용자 단말은 해당 사용자 단말의 제 2 비밀키( $s_u$ ) 정보가 사용자 리스트( $SU_{list}$ )에서 삭제되어 있으므로, 근본적으로 문서를 검색하기 위한 키워드에 대한 키워드 인덱스 생성키가 생성될 수 없다.

그리고, 사용자 단말(300)은 문서 서버(200)로부터 수신한 제 1 및 제 2 생성키 값( $\overline{k_{d_i}}$  및  $\overline{k_{w_i}}$ )을 이용하여 문서( $d$ )를 암호화하기 위한 문서 암호화키( $k_{d_i}$ ) 및 키워드( $w$ )에 대한 키워드 인덱스 생성키( $k_{w_i}$ )를 아래 수학식 (3) 및 (4)와 같이 생성할 수 있다. 이때, 사용자 관리장치(100)로부터 수신한 제 1 비밀키가 이용될 수 있다.

[수학식 3]

$$k_{d_i} = H((\overline{k_{d_i}})^{k_u}) = H(e(g^{t_i}, g^{k_m/k_u})^{k_u}) = H(e(g^{t_i}, g^{k_m}))$$

[수학식 4]

$$k_{w_i} = H((\overline{k_{w_i}})^{k_u/r_i}) = H(e(h_s(w)^{r_i}, g^{k_m/k_u})^{k_u/r_i}) = H(e(h_s(w), g^{k_m}))$$

여기서, 사용자 단말(300)은 저장하기 원하는 문서( $d_i$ )를 문서 암호화키 값( $k_{d_i}$ )을 이용하여  $E_{k_{d_i}}(d_i)$ 로 암호화 하고,  $E_{k_{d_i}}(d_i)$ 를 검색하기 위한 키워드를 인덱스 생성키 값( $k_{w_i}$ )을 이용하여 암호화한다. 이때, 랜덤한 난수 ( $R_i \in Z^*_p$ )를 선택하고, 해당 난수( $R_i \in Z^*_p$ ) 및 키워드 인덱스 생성키 값( $k_{w_i}$ )을 이용하여 암호화된 키워드 ( $E_{k_{w_i}}(R_i)$ )를 생성할 수 있다.

여기서, 난수( $R_i$ )를 적용시킴으로써, 같은 키워드에도 다른 인덱스 값을 생성하게 되어 외부 공격자에 의한 정보 노출의 위험을 막을 수 있게 된다.

다음으로, 사용자 단말(300)은 수학식 5와 같이 암호화된 데이터에 대한 집합을 생성하여 문서 서버(200)에 저장한다. 여기서, 인덱스( $I_i$ )에 난수( $R_i$ ) 및 해당 난수가 적용된 암호화된 키워드( $E_{k_{w_i}}(R_i)$ )가 문서 서버(200)에 전송되어진다.

[0106] [수학식 5]

$$EI_i = \{T_i = g^{t_i}, C_i = E_{k_{d_i}}(d_i), I_i = \{I_i[1], I_i[2]\} = \{R_i, E_{k_{w_i}}(R_i)\}\}$$

[0107] 도 7은 본 발명의 일 실시예에 따른 다자간 검색 시스템의 쿼리 및 검색 과정을 나타낸다.

[0108] 도 7에 도시된 바와 같이, 조회(Query) 과정에 있어서, 사용자 단말(300)은 사용자의 식별정보, 키워드 및 자신의 제 1 비밀키를 이용하여, 문서 서버(200)에 요청할 쿼리( $q_u(w)$ )를 생성한다.

$$q_u(w) = \{u, h_s(w)^{k_u}\}$$

[0110] 즉, 을 생성하여 문서 서버(200)로 전송한다.

[0111] 여기서, 사용자 관리장치(100)로부터 수신한 해당 사용자의 제 1 비밀키를 통해 쿼리가 생성되므로, 외부 공격자가 정당한 쿼리를 생성할 수 없게 되어, 쿼리에 대한 안정성이 확보될 수 있다.

[0112] 검색(Search) 과정에 있어서, 사용자 단말(300)은 문서 서버에 쿼리( $q_u(w)$ )를 전송하고 그에 대응되는 응답 데이터( $ans_d(w)$ )를 수신한다. 그리고, 사용자 단말(300)은 응답 데이터로부터 암호화된 문서를 복호화하게 된다.

[0113] 보다 구체적으로 설명하자면, 사용자 단말(300)로부터 쿼리( $q_u(w)$ )를 수신한 문서 서버(200)는, 사용자 리스트( $SU_{list}$ )에 해당 식별정보가 등록되어 있는지 여부를 확인하고, 만약 등록된 정보가 존재하지 않으면 정당한 사용자 단말이 아니므로 종료한다. 만약 해당 사용자에 대한 등록된 정보가 존재할 경우, 문서 서버(200)는 사용자 단말(300)로부터 수신한 쿼리값 및 해당 사용자의 제 2 비밀키에 기초하여 키워드 인덱스 생성키( $k_w$ )를 다음과 같이 산출한다.

$$k_w = H(e(h_s(w)^{k_u}, s_u)) = H(e(h_s(w)^{k_u}, g^{k_m/k_u})) = H(e(h_s(w), g^{k_m}))$$

[0114] 그리고 문서 서버(200)는,

$$EI_i = \{g^{t_i}, E_{k_{d_i}}(d_i), R, E_{k_{w_i}}(R)\}$$

[0115] 의 집합( $EI_D$ )중에서 키워드 인덱스 생성키에 대응되는 암호화된 문서를 검색한다.

[0116] 그리고, 검색된 암호화된 문서( $E_{k_{d_i}}(d_i)$ ) 및 암호화된 문서에 대한 제 1 생성키

$$\overline{k_{d_i}} = e(g^{t_i}, s_u)$$

[0117] ( )을 생성하여 사용자 단말(300)로 전송한다.

[0118] 그러면, 사용자 단말(300)은 제 1 생성키를 이용하여 암호화된 문서에 대한 문서 암호화키( $k_{d_i}$ )를 아래와 같이 산출하고, 산출한 문서 암호화키에 기초하여 암호화된 문서를 복호화하게 된다.

$$k_{d_i} = H((\overline{k_{d_i}})^{k_u}) = H(e(g^{t_i}, g^{k_m})^{k_u}) = H(e(g^{t_i}, g^{k_m/k_u})^{k_u}) = H(e(g^{t_i}, g^{k_m}))$$

[0119] 도 8은 본 발명의 일 실시예에 따른 다자간 검색 방법의 순서도이다.

[0120] 사용자 단말(300)이 사용자 관리장치(100)에 사용자 등록 요청을 수행한다(S801).

[0121] 다음으로, 사용자 관리장치(100)가 사용자 등록 요청에 따라, 사용자 등록을 요청한 사용자의 사용자 단말(300)에 제 1 비밀키를 발급한다(S802).

- [0124] 그리고, 제 1 비밀키가 포함되도록 생성한 제 2 비밀키 및 사용자의 식별정보를 문서 서버(200)에 제공한다(S803).
- [0125] 다음으로, 사용자 단말(300)이 사용자 관리장치(100)에 난수를 전송한다(S804).
- [0126] 다음으로, 문서 서버(200)가 사용자 단말(300)로부터 수신한 난수 및 제 2 비밀키를 이용하여 문서 암호화키의 생성에 사용되는 제 1 생성키 및 키워드 인덱스 생성키의 생성에 사용되는 제 2 생성키를 생성하여 사용자 단말(300)에 제공한다(S805).
- [0127] 다음으로, 사용자 단말(300)이 제 1 생성키에 기초하여 문서 암호화키를 생성하고, 제 2 생성키에 기초하여 키워드 인덱스 생성키를 생성한다(S806).
- [0128] 그리고, 사용자 단말(300)이 제 1 생성키에 기초하여 생성된 문서 암호화키를 이용하여 문서를 암호화하고, 제 2 생성키에 기초하여 생성된 키워드 인덱스 생성키를 이용하여 키워드를 암호화하여 문서 서버(200)로 전송한다(S807, S808).
- [0129] 다음으로, 문서 서버(200)가 암호화된 문서 및 암호화된 키워드를 사용자 단말(300)로부터 수신하여 저장한다(S809).
- [0130] 다음으로, 사용자 단말(300)이 쿼리값을 생성하여 문서 서버(200)에 전송한다(S810, S811). 여기서, 사용자 단말(300)은 사용자의 키워드 입력에 따라 키워드, 사용자의 식별정보 및 사용자 단말(300)의 제 1 비밀키가 포함된 쿼리값을 생성할 수 있다.
- [0131] 다음으로, 문서 서버(200)가 해당 사용자가 사용자 리스트에 등록된 사용자인지 여부를 판단한다(S812).
- [0132] 다음으로, 사용자가 사용자 리스트에 등록된 사용자인 경우, 문서 서버(200)가 사용자 단말(300)로부터 수신한 쿼리값 및 사용자의 제 2 비밀키에 기초하여 키워드 인덱스 생성키를 산출하고, 산출된 키워드 인덱스 생성키에 해당하는 암호화된 문서를 검색한다(S813).
- [0133] 다음으로, 문서 서버(200)가 암호화된 문서 및 암호화된 문서에 대한 제 1 생성키를 사용자 단말(300)로 전송한다(S814).
- [0134] 다음으로, 사용자 단말(300)은 문서 서버(200)로부터 수신한 제 1 생성키로부터 암호화된 문서에 대한 문서 암호화키를 산출하고, 산출한 문서 암호화키에 기초하여 암호화된 문서를 복호화한다(S815).
- [0135] 이후, 문서 서버(200)는 사용자 단말(300)로부터 사용자 탈퇴 요청을 수신한 경우에는, 사용자 탈퇴를 요청한 사용자의 식별정보 및 사용자 탈퇴를 요청한 사용자의 제 2 비밀키를 사용자 리스트로부터 제거하게 된다.
- [0136] 상술된 과정(S801~S809)를 이용하여, 예를 들어, 다른 정당한 사용자( $u'$ )가 동일한 키워드( $w$ )를 이용하여 생성한 쿼리

[0137] 즉,  $q_{u'}(w) = \{u', h_s(w)^{k_{u'}}\}$  을 문서 서버(200)로 전송하면, 문서 서버(200)는

[0138]  $k_w' = H(e(h_s(w)^{k_{u'}}, g^{k_m/k_{u'}})) = H(e(h_s(w), g^{k_m}))$  을 생성한다.

[0139] 그러면,  $k_w = k_w'$  이므로, 다른 사용자는 사용자가 저장한 데이터를 암호화된 상태로 전송받을 수 있다. 그리고,

다른 사용자는 문서 서버(200)로부터 전송받은  $ans_{u'}(w)$ 로부터  $k_{d_i}'$ 를 생성하고,  $k_{d_i} = k_{d_i}'$ 이므로, 다른 사용자는 사용자가 저장한 암호화된 문서를 정당하게 복호화할 수 있게 된다.

[0140] 따라서, 다수의 사용자들이 안전하고 효율적으로 암호화된 문서에 대한 검색을 수행할 수 있게 된다.

[0141] 한편, 상술된 사용자 관리장치(100) 및 문서 서버(200)는 다자간 검색 시스템에 각각 모듈로 구현될 수 있음은 물론이다. 예컨대, 사용자 관리장치(100)는 사용자 관리부, 문서 서버(200)는 문서 관리부로 다자간 검색 시스템에 구성요소로 포함될 수 있다.

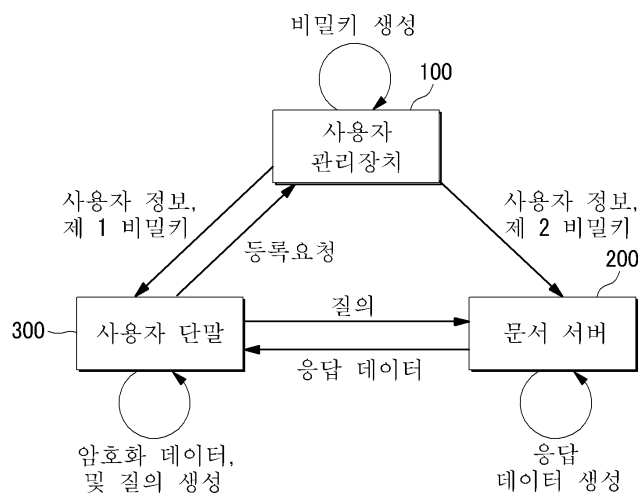
- [0142] 또한, 상술된 도 3의 암호화 데이터 저장부(220)는 캐쉬, ROM(Read Only Memory), PROM(Programmable ROM), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM) 및 플래쉬 메모리(Flash memory)와 같은 비휘발성 메모리 소자 또는 RAM(Random Access Memory)과 같은 휘발성 메모리 소자 또는 하드디스크 드라이브(HDD, Hard Disk Drive), CD-ROM과 같은 저장 매체 중 적어도 하나로 구현될 수 있으나 이에 한정되지는 않는다.
- [0143] 그리고 도 2 내지 도 4에서 도시된 각각의 구성요소는 일종의 '모듈'로 구성될 수 있다. 상기 '모듈'은 소프트웨어 또는 Field Programmable Gate Array(FPGA) 또는 주문형 반도체(ASIC, Application Specific Integrated Circuit)와 같은 하드웨어 구성요소를 의미하며, 모듈은 어떤 역할들을 수행한다. 그렇지만 모듈은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. 모듈은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 실행시키도록 구성될 수도 있다. 구성요소들과 모듈들에서 제공되는 기능은 더 작은 수의 구성요소들 및 모듈들로 결합되거나 추가적인 구성요소들과 모듈들로 더 분리될 수 있다.
- [0144] 또한 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.
- [0145] 그리고 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

### 부호의 설명

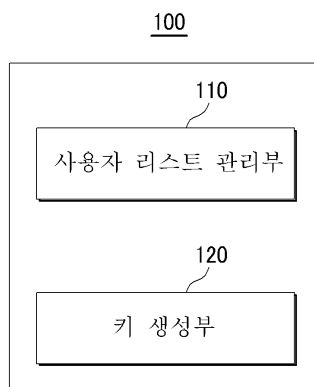
- [0146]
- |                  |                  |
|------------------|------------------|
| 100: 사용자 관리장치    | 110: 사용자 리스트 관리부 |
| 120: 키 생성부       | 200: 문서 서버       |
| 210: 사용자 리스트 관리부 | 220: 암호화 데이터 저장부 |
| 230: 키 생성부       | 240: 데이터 검색부     |
| 300: 사용자 단말      | 310: 식별정보 관리 요청부 |
| 320: 데이터 암호화부    | 330: 쿼리 생성부      |
| 340: 데이터 복호화부    |                  |

도면

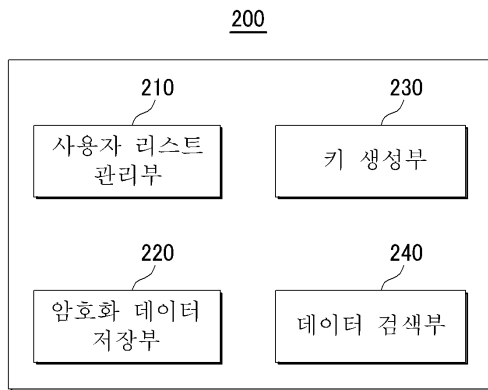
도면1



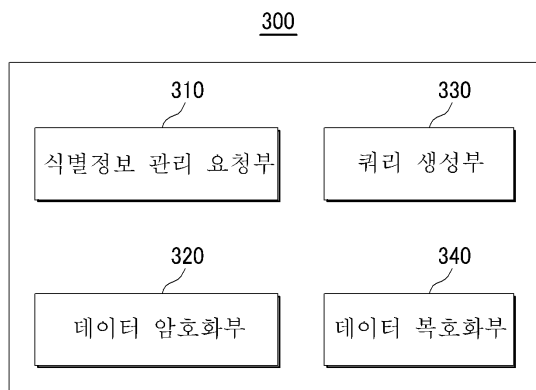
도면2



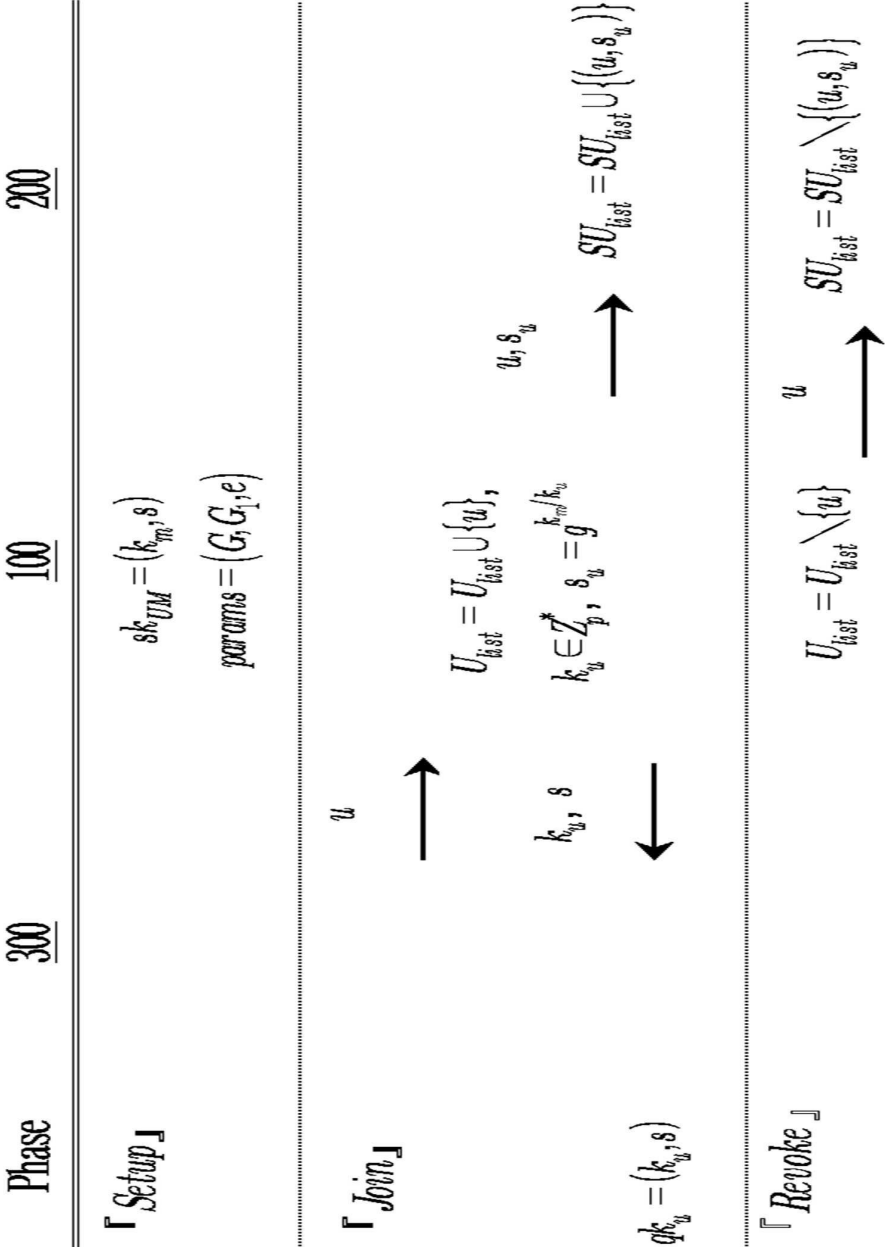
도면3



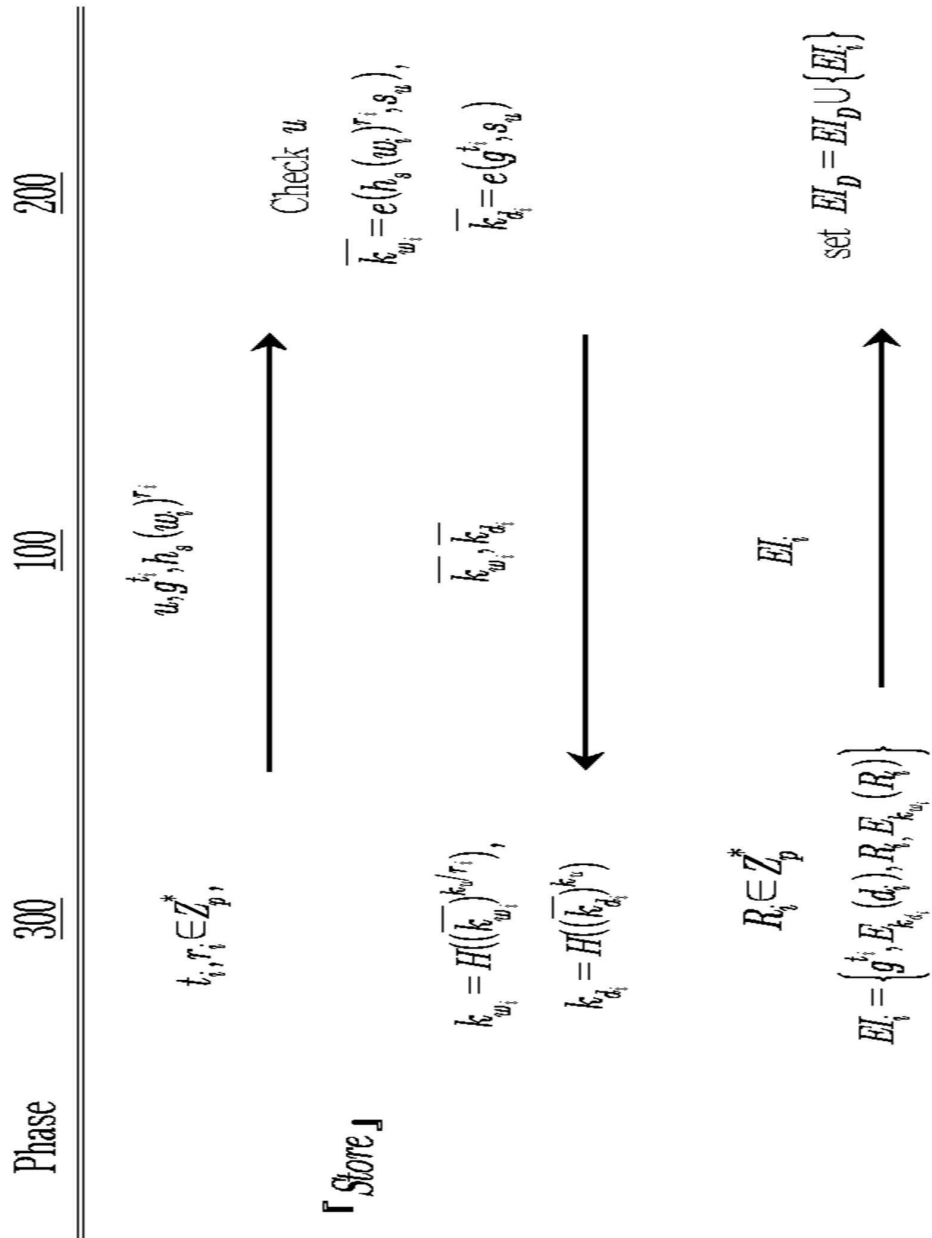
도면4



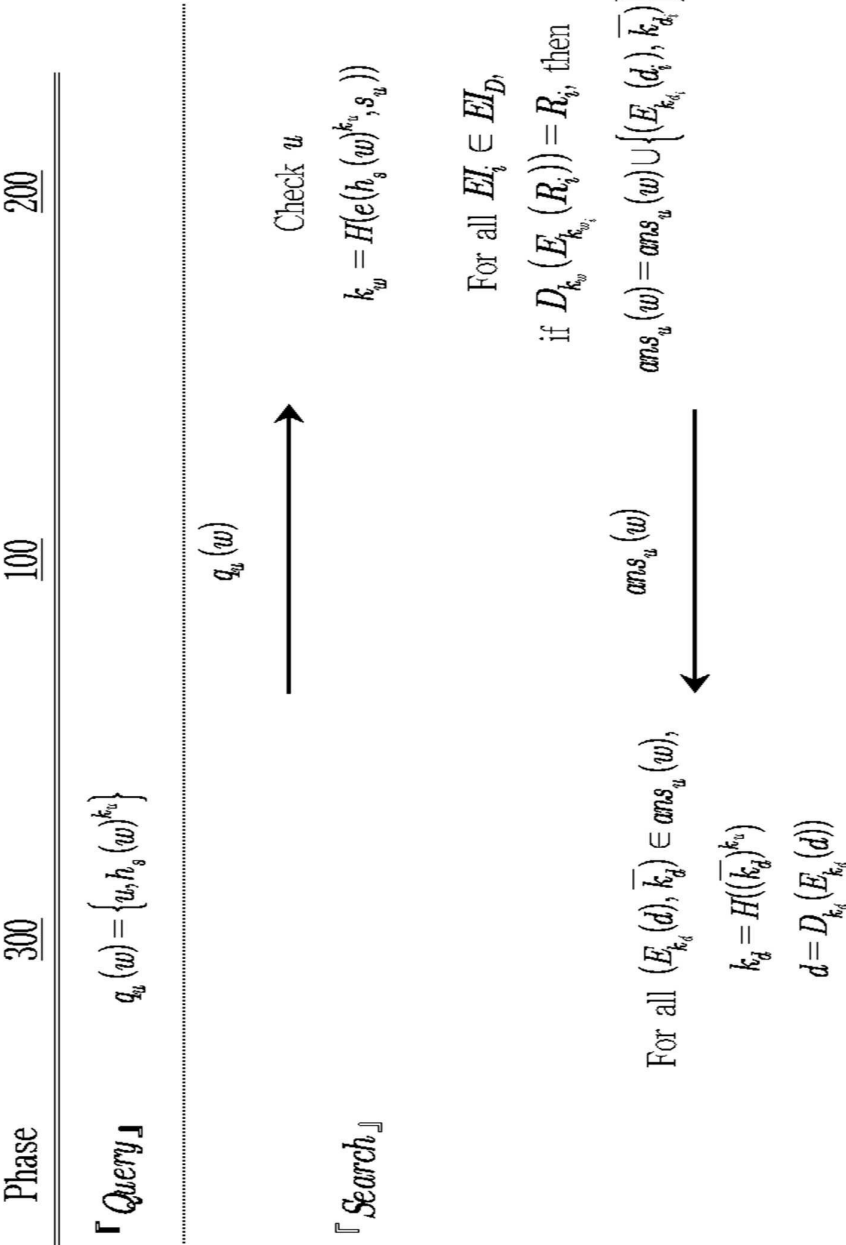
도면5



도면6



도면7



도면8

