(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년03월07일
(11) 등록번호 10-1599996
(24) 등록일자 2016년02월26일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01)
(21) 출원번호 10-2014-0175081
(22) 출원일자 2014년12월08일
심사청구일자 2014년12월08일
(56) 선행기술조사문헌
Kwangsu Lee 외 2인, IACR Cryptology ePrint Archive, "Efficient revocable identity-based encryption via subset difference methods" (2014.02.24. 공개)
JP2007096751 A

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
박승환
서울 동작구 노량진로6마길 8
엄지은
서울 서대문구 가재울로 45, 102동 102호 (남가좌동, 현대아파트)
(뒷면에 계속)
(74) 대리인
김등용, 김홍석

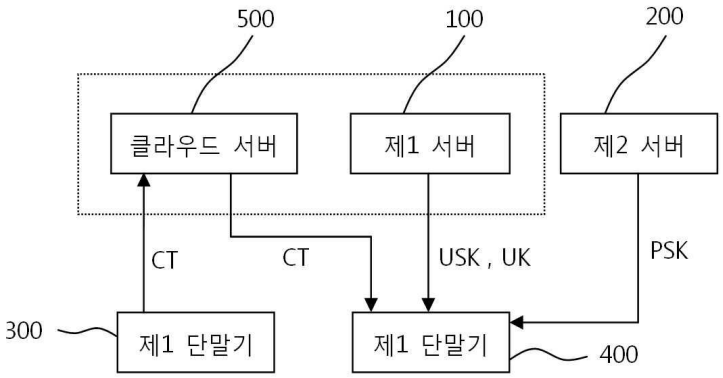
전체 청구항 수 : 총 4 항 심사관 : 문형섭

(54) 발명의 명칭 **폐기가능한 ID 기반 암호 서버 및 시스템**

(57) 요 약

ID(identity) 기반 암호 서버가 개시된다. 상기 ID 기반 암호 서버는, 보안 상수와 사용자 집합을 입력으로 받고, 공개 파라미터와 제1 마스터키를 생성하는 셋업 모듈, 상기 공개 파라미터, 이진트리의 상태 정보, 및 상기 제1 마스터키를 이용하여 개인키를 생성하고, 생성된 개인키를 단말기로 송신하는 개인키 생성 모듈, 및 상기 공개 파라미터, 폐기 목록, 상기 상태 정보, 및 상기 제1 마스터키를 이용하여 업데이트키를 생성하고, 생성된 업데이트키를 상기 단말기로 송신하는 업데이트키 생성 모듈을 포함한다.

대 표 도 - 도1



10

(72) 발명자

류금숙

서울 용산구 두텁바위로 96-8, 2층 (후암동)

이동훈

서울 종로구 사직로8길 34, 1404호 (내수동, 경희궁의아침 3단지)

이 발명을 지원한 국가연구개발사업

과제고유번호	NIPA-2014-H0301-14-1004
부처명	미래창조과학부
연구관리전문기관	정보통신산업진흥원
연구사업명	ITRC
연구과제명	제어시스템 보안 연구
기 여 율	1/1
주관기관	고려대학교 산학협력단
연구기간	2014.01.01 ~ 2014.12.31

명 세 서

청구범위

청구항 1

제1 서버와 제2 서버를 포함하는 ID(identity) 기반 암호 시스템에 있어서,

상기 제1 서버는,

보안 상수와 사용자 집합을 입력으로 받고, 공개 파라미터와 제1 마스터키를 생성하는 셋업 모듈;

상기 공개 파라미터, 이진트리의 상태 정보, 및 상기 제1 마스터키를 이용하여 개인키를 생성하고, 생성된 개인키를 단말기로 송신하는 개인키 생성 모듈; 및

상기 공개 파라미터, 폐기 목록, 상기 상태 정보, 및 상기 제1 마스터키를 이용하여 업데이트키를 생성하고, 생성된 업데이트키를 상기 단말기로 송신하는 업데이트키 생성 모듈을 포함하고,

상기 제2 서버는,

상기 보안 상수와 상기 사용자 집합을 입력으로 받고, 상기 공개 파라미터와 제2 마스터키를 생성하는 제2 셋업 모듈; 및

상기 공개 파라미터와 상기 제2 마스터키 및 상기 단말기의 ID를 이용하여 보조키를 생성하고, 생성된 보조키를 상기 단말기로 송신하는 보조키 생성 모듈을 포함하는,

ID 기반 암호 시스템.

청구항 2

제1항에 있어서,

상기 업데이트키 생성 모듈은 주기적으로 업데이트키를 생성하고, 생성된 업데이트키를 상기 단말기로 송신하는 ID 기반 암호 시스템.

청구항 3

제1항에 있어서,

상기 셋업 모듈에 의해 생성되는 상기 공개 파라미터는 겹선형 군, 상기 겹선형 군의 생성원, 임의의 난수를 이용하여 생성된 제1 공개 파라미터, 및 입력되는 임의의 스트링(string)을 타원곡선 위의 점으로 매핑하는 제1 매핑 함수와 제2 매핑 함수를 포함하는 ID 기반 암호 시스템.

청구항 4

제1항에 있어서,

상기 개인키, 상기 업데이트키, 및 상기 보조키를 수신하여 복호화키를 생성하고, 생성된 복호화키를 이용하여 암호문을 복호화하는 상기 단말기를 더 포함하는, ID 기반 암호 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 폐기가능한 ID 기반 암호 서버 및 시스템에 관한 것으로, 특히 효율적으로 만료된 사용자의 복호화키를 폐기할 수 있고, 서버의 마스터키로 사용자의 데이터를 복호화하는 것이 불가능한 폐기가능한 ID 기반 암호 서버 및 시스템에 관한 것이다.

배 경 기 술

[0002] 공개키 기반 구조(Public Key Infrastructure, PKI)에 기반한 공개키 암호(Public Key Encryption) 시스템에서

는 암호화키와 복호화키가 임의의 값(Random string or Random value)으로 존재하기 때문에 암호화키와 사용자의 관계를 인증할 수 있는 인증서(Certificate)가 필요하며, 인증서는 인증서 발급 기관(Central Authority)에 의해 발급된다. 데이터를 암호화하기 위해, 송신자는 수신자의 공개키와 공개키에 대한 인증서를 수신자로부터 미리 수신받아 키에 대한 검증을 수행한 후에 데이터를 암호화한다. 이와 같은 인증서 사용의 불편함을 해결하기 위하여 ID기반 암호 시스템(Identity Based Encryption, IBE)이 개발되었다.

[0003] ID기반 암호 시스템에서는 암호화 시 수신자를 식별할 수 있는 식별 정보, 예컨대 수신자의 이메일 주소, 사원번호, 전화번호 등이 공개키로 사용된다. 수신자를 바로 식별할 수 있는 값을 공개키로 사용하기 때문에 송신자는 별도의 키에 대해 인증할 필요가 없으며, 결과적으로 시스템 상에서 인증서를 사용하지 않아도 된다.

[0004] 그러나, 각 사용자가 발급받는 복호화키는 서버의 마스터키에 기초하여 만들어지기 때문에 서버는 암호 시스템 상에서 존재하는 모든 암호문에 대한 복호화가 가능하다. 수많은 사용자들의 데이터를 저장하는 클라우드 스토리지 환경에서 기존의 ID 기반 암호 시스템을 사용한다면, 클라우드 서버는 저장되어 있는 모든 데이터를 복호화할 수 있으므로 사용자의 프라이버시 침해 문제가 제기되게 된다.

[0005] 이와 같은 문제를 해결하기 위하여 저장 서버와 키 발급 서버를 따로 두고, ID 기반 암호 시스템을 사용할 수 있으나, 이 경우 클라우드 서버에 의한 사용자 관리(가입 및 탈퇴)가 불가능하게 되고, 외부 키 발급 서버에 의한 사용자 관리가 이루어지게 된다.

[0006] 따라서, 클라우드 스토리지 서비스 제공자에 의한 사용자 관리가 가능하면서 스토리지 서비스 제공자는 서버에 저장되어 있는 데이터를 복호화할 수 없는 ID 기반 암호 시스템이 필요하다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 대한민국 등록특허 제10-1382626호

발명의 내용

해결하려는 과제

[0008] 본 발명이 이루고자 하는 기술적인 과제는 서비스 제공자에 의한 사용자 관리가 가능하며, 서비스 제공 서버에 저장되어 있는 데이터를 서비스 제공자로부터 보호할 수 있는 폐기가능한 ID 기반 암호 서버 및 시스템을 제공하는 것이다.

과제의 해결 수단

[0009] 본 발명의 실시 예에 따른 ID(identity) 기반 암호 서버는, 보안 상수와 사용자 집합을 입력으로 받고, 공개 파라미터와 제1 마스터키를 생성하는 셋업 모듈, 상기 공개 파라미터, 이진트리의 상태 정보, 및 상기 제1 마스터키를 이용하여 개인키를 생성하고, 생성된 개인키를 단말기로 송신하는 개인키 생성 모듈, 및 상기 공개 파라미터, 폐기 목록, 상기 상태 정보, 및 상기 제1 마스터키를 이용하여 업데이트키를 생성하고, 생성된 업데이트키를 상기 단말기로 송신하는 업데이트키 생성 모듈을 포함한다.

[0010] 또한, 본 발명의 실시 예에 따른 ID 기반 암호 시스템은, 상기 암호화 서버, 및 제2 서버를 포함하고, 상기 제2 서버는, 상기 보안 상수와 상기 사용자 집합을 입력으로 받고, 상기 공개 파라미터와 제2 마스터키를 생성하는 제2 셋업 모듈, 및 상기 공개 파라미터와 상기 제2 마스터키, 및 상기 단말기의 ID를 이용하여 보조키를 생성하고, 생성된 보조키를 상기 단말기로 송신하는 보조키 생성 모듈을 포함한다.

발명의 효과

[0011] 본 발명의 실시 예에 따른 폐기가능한 ID 기반 암호 서버 및 시스템에 의할 경우, 서비스 제공자에 의한 사용자 관리가 가능할 뿐아니라, 서버에 저장되어 있는 데이터를 서비스 제공자로부터 보호할 수 있는 효과가 있다.

도면의 간단한 설명

[0012] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 따른 ID 기반 암호 시스템을 도시한다.

도 2는 도 1에 도시된 제1 서버의 기능 블럭도이다.

도 3은 도 1에 도시된 제2 서버의 기능 블럭도이다.

도 4는 도 1에 도시된 제2 단말기의 기능 블럭도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0014] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0015] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0016] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0017] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0018] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0019] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0020] 도 1은 본 발명의 일 실시 예에 따른 ID 기반 암호 시스템을 도시한다. 도 1을 참조하면, 클라우드 스토리지 환경에서 활용가능한 ID(identity) 기반 암호 시스템(10)은 제1 서버(100), 제2 서버(200), 제1 단말기(300), 및 제2 단말기(400)를 포함한다. 실시 예에 따라, 암호 시스템(10)은 클라우드 서비스를 제공할 수 있는 클라우드 서버(500)를 더 포함할 수 있다.

[0021] 키 생성 기관(Key Generation Center) 또는 키 생성 서버로 불릴 수도 있는 제1 서버(100)는 개인키(USK)와 업데이트키(UK)를 생성하여, 생성된 개인키(USK)와 업데이트키(UK)를 제2 단말기(400)로 송신할 수 있다. 실시 예에 따라, 제1 서버(100)는 클라우드 서버(500)와 동일한 서버이거나, 클라우드 서버(500)와 물리적으로 분리된 서버이지만 클라우드 서버(500)의 운영자에 의해 운영되는 서버일 수도 있다.

[0022] 제2 서버(200)는 보조키(PSK)를 생성하여, 생성된 보조키(PSK)를 제2 단말기(400)로 송신할 수 있다. 제2 서버

(200)는 제1 서버(100)와 물리적으로 분리되어 있을 뿐만 아니라 제1 서버(100)의 운영자와는 다른 운영자에 의해 운영되는 서버임이 원칙이나, 본 발명이 이에 제한되는 것은 아니다. 제1 서버(100)와 제2 서버(200)가 상이한 주체에 의해 운영될 경우, 제1 서버(100)를 포함하는 클라우드 서버(500)에 저장된 암호문(CT)이 임의로 복호화될 가능성을 배제할 수 있다.

[0023] 암호문(CT)을 송신하는 송신자의 단말기인 제1 단말기(300)는 제2 단말기(400)의 사용자의 ID 또는 제2 단말기(400)의 ID를 이용하여 메시지를 암호화하여 암호문(CT)를 생성한다. 또한, 제1 단말기(300)는 생성된 암호문(CT)을 클라우드 서버(500)로 송신할 수 있다. 실시 예에 따라, 제1 단말기(300)은 생성된 암호문(CT)을 유무선 통신망을 통하여 제2 단말기(400)로 직접 송신할 수도 있다.

[0024] 암호문(CT)을 수신하는 수신자의 단말기인 제2 단말기(400)는 제1 서버(100)로부터 개인키(USK)와 업데이트키(UK)를 수신하고, 제2 서버(200)로부터 보조키(PSK)를 수신할 수 있다. 제2 단말기는 수신된 개인키(USK), 업데이트키(UK), 및 보조키(PSK)를 이용하여 복호화키를 생성한다. 제2 단말기는 상기 복호화키를 이용하여 제1 단말기(300) 또는 클라우드 서버(500)로부터 수신한 암호문(CT)을 복호화할 수 있다.

[0025] 제1 단말기(300) 또는 제2 단말기(400)는 PC(personal computer), 태블릿 PC, 노트북(notebook), 넷-북(net-book), e-리더(e-reader), PDA(personal digital assistant), PMP(portable multimedia player), MP3 플레이어, 또는 MP4 플레이어와 같은 데이터 처리 장치로 구현되거나, 모바일폰(mobile phone) 또는 스마트폰(smart phone)과 같은 핸드헬드 장치(handheld device)로 구현될 수 있다.

[0026] 클라우드 서버(500)는 클라우드 서비스를 제공하는 서버일 수 있다.

[0027] 도 2는 도 1에 도시된 제1 서버의 기능 블럭도이다. 도 1과 도 2를 참조하면, 제1 서버(100)는 셋업 모듈(110), 개인키 생성 모듈(130), 및 업데이트키 생성 모듈(150)을 포함한다. 실시 예에 따라, 제1 서버(100)는 폐기 모듈(170)을 더 포함할 수 있다.

[0028] 셋업 모듈(110)은 보안 상수(1^{λ})와 사용자의 집합(N)을 입력으로 하는 셋업 알고리즘($Setup(1^{\lambda},N)$)을 수행하여 공개 파라미터(PP)와 제1 마스터키(MK_{Server})를 생성한다.

[0029] 구체적으로, 셋업 모듈(110)은 소수(prime number) p를 위수로 갖는 겹선형 군(p, G, G_T, e)을 생성하고, g를 겹선형 군(G)의 정규 생성원으로 한다.

[0030] 또한, 셋업 모듈(110)은 임의의 난수($\beta \in Z_p^*$)를 선택하여 제1 공개 파라미터($e(g,g)^{\beta}$)를 생성한다. 또한, 셋업 모듈(110)은 임의의 스트링(string)에 해당하는 입력값을 타원곡선 위의 점으로 매핑하는 매핑 함수($F:\mathcal{I} \rightarrow G$)와 매핑 함수($H:\mathcal{T} \rightarrow G$)를 선택한다.

[0031] 셋업 모듈(110)은 정규 생성원(g), 겹선형 군(G), 제1 공개 파라미터($\Omega_2 = e(g,g)^{\beta}$), 매핑 함수($F$), 및 매핑 함수($H$)를 포함하는 공개 파라미터(PP)를 공개한다. 본 발명에서 이용되는 공개 파라미터($PP=(g,G,\Omega_1=e(g,g)^{\alpha},\Omega_2=e(g,g)^{\beta},F,H)$) 중 제2 공개 파라미터($\Omega_1 = e(g,g)^{\alpha}$)는 제2 서버(200)에 의해 생성된 파라미터일 수 있다.

[0032] 또한, 셋업 모듈(110)은 제1 마스터키($MK_{Server} = g^{\beta}$)를 생성한다. 생성된 제1 마스터키는 사용자의 개인키와 업데이트키를 생성하는 과정에서 이용될 수 있다.

[0033] 개인키 생성 모듈(130)은 시간(T), ID, 제1 마스터키, 이진트리(BT)의 상태 정보(ST), 및 공개 파라미터를 입력으로 하는 개인키 생성 알고리즘($KeyPrivate(T,ID,MK_{Server},ST,PP)$)을 실행하여, 개인

키를 생성하고, 생성된 개인키를 제2 단말기(400)로 송신한다.

[0034] 구체적으로, 개인키 생성 모듈(130)은 이진트리(BT)의 말단 노드들 중 사용자가 할당되지 않은 임의의 말단 노드(η)를 선택하고, 선택된 말단 노드(η)에 ID를 할당한다. 그리고 개인키 생성 모듈(130)은 각각의 노드($\theta \in Path(\eta)$)에 대해 다음과 같은 과정을 수행한다. 여기서, $Path(\eta)$ 은 노드(η)에서부터 루트 노드(최상위 노드)까지의 경로에 포함되어 있는 노드들의 집합을 의미한다.

[0035] 1. 노드(θ)에 대응하는 임의의 난수(β_θ)가 정의되어 있지 않는 경우, 임의의 난수($\beta_\theta \in Z_p$)를 선택하여 선택된 난수를 노드(θ)에 할당 또는 정의한다.

[0036] 2. 임의의 난수($r_\theta \in Z_p$)를 선택한다.

[0037] 3. 아래의 수학식으로 정의되는 제1 개인키($usk_{\Theta,0}$)와 제2 개인키($usk_{\Theta,1}$)를 생성한다.

[0038]
$$usk_{\theta,0} = g^{\beta_\theta} \cdot F(ID)^{r_\theta}$$
$$usk_{\theta,1} = g^{r_\theta}$$

[0039] 개인키 생성 모듈(130)은 위의 과정들을 수행한 후에 각각의 노드(Θ)에 대응하는 제1 개인키와 제2 개인키를 포함하는 개인키($USK_{ID} = (\theta, usk_{\theta,0}, usk_{\theta,1})_{\theta \in Path(\eta)}$)를 생성하고, 생성된 개인키를 제2 단말기(400)로 송신할 수 있다.

[0040] 업데이트키 생성 모듈(150)은 시간(T), 제1 마스터키, 이진트리(BT)의 상태 정보(ST), 및 공개 파라미터(PP)를 입력으로 하는 업데이트키 생성 알고리즘($UpdateKey(T, RL, MK_{Server}, ST, PP)$)을 실행하여 업데이트키를 생성하고, 생성된 업데이트키를 제2 단말기(400)로 송신한다.

[0041] 즉, 업데이트키 생성 모듈(150)은 주기적으로 업데이트키를 생성하고, 생성된 업데이트키를 제2 단말기(400)로 송신한다. 제2 단말기(400)는 수신된 업데이트키를 이용하여 복호화키를 생성할 수 있다.

[0042] 업데이트키를 생성하기에 앞서, 업데이트키 생성 모듈(150)은 이진트리(BT) 상에서, 대응되는 업데이트키가 생성될 노드들의 집합(Y)을 구할 수 있다.

[0043] 상기 노드들의 집합(Y)은 이진트리(BT), 폐기 목록(RL), 및 시간(T)을 입력으로 하는 노드 생성 알고리즘(KUNode)을 이용하여 구할 수 있다. 알고리즘에 관한 구체적인 내용은 다음과 같다.

$$KUNode(BT, RL, T):$$
$$X, Y \leftarrow \varnothing;$$
$$\forall (\eta_i, T_i) \in RL$$
$$If\ T_i \leq T\ then\ add\ Path(\eta_i)\ to X$$
$$\forall x \in X$$
$$If x_{left} \notin X\ then\ add\ x_{left}\ to\ Y$$
$$If x_{right} \notin X\ then\ add\ x_{right}\ to\ Y$$
$$If\ Y = \varnothing\ then\ add\ root\ to\ Y$$
$$Return\ Y$$

[0044]

[0045] 상기 알고리즘 상에서 T_i 는 노드(η_i)의 폐기 시간을 의미하고, 노드(x_{left})는 노드(x)의 왼쪽 자식 노드를 의미하고, 노드(x_{right})는 노드(x)의 오른쪽 자식 노드를 의미한다. 이진트리(BT) 상에서 각각의 사용자는 말단 노드에 할당된다. $Path(\eta_i)$ 는 노드(η_i)에서부터 루트 노드, 즉 최상위 노드까지 경로상에 위치한 노드들의 집합을 의미한다.

[0046] 따라서, 시간(T)에 집합(Y)에 포함된 노드들에 대응되는 업데이트키만이 생성되고, 폐기되지 않은 사용자들은, 자신의 노드로부터 루트 노드까지의 경로상에 포함된 노드들 중 어느 하나의 노드가 집합(Y)에 포함되어 있으므로 시간(T)에 복호화키를 생성할 수 있다.

[0047] 업데이트키 생성 모듈(150)은 업데이트키를 생성할 노드들의 집합(Y)을 생성한 후, 이진트리(BT) 상의 노드($\theta \in KUNode(BT, RL, T)$), 즉 집합(Y)에 포함된 노드(Θ)에 대해 다음과 같은 과정을 수행한다.

[0048] 1. 이진트리(BT)의 노드(Θ)에 정의된 임의의 난수(β_θ)를 가지고 온다.

[0049] 2. 임의의 지수($s_\theta \in Z_p$)를 선택한다.

[0050] 3. 제1 업데이트키($uk_{\theta,0} = g^{\beta - \beta_\theta} \cdot H(T)^{s_\theta}$)와 제2 업데이트키($uk_{\theta,1} = g^{s_\theta}$)를 생성한다.

[0051] 모든 노드($\theta \in KUNode(BT, RL, T)$)에 관하여, 위의 과정이 완료되면, 업데이트키 생성 모듈(150)은 제1 업데이트키와 제2 업데이트키를 포함하는 업데이트키($UK_T = (\theta, uk_{\theta,0}, uk_{\theta,1})_{\theta \in KUNode(BT, RL, T)}$)를 제2 단말기(400)로 송신한다.

[0052] 폐기 모듈(170)은 폐기될 ID, 시간(T), 폐기 목록(RL), 이진트리(BT)의 상태(state) 정보(ST)를 입력으로 하는 폐기 알고리즘($Revoke(ID, T, RL, ST)$)을 수행함으로써, ID에 대한 폐기 동작을 수행할 수 있다.

[0053] 즉, ID가 할당된 말단 노드가 η 라면, $RL \cup \{(\eta, T)\}$ 를 새로운 폐기 목록으로 갱신함으로써, ID에 대한 폐기 동작을 수행할 수 있다.

[0054] 도 3은 도 1에 도시된 제2 서버의 기능 블럭도이다. 도 1 내지 도 3을 참조하면, 제2 서버(200)는 셋업 모듈(210)과 보조키 생성 모듈(230)을 포함한다.

[0055] 셋업 모듈(210)은 보안 상수(1^{λ})와 사용자의 집합(N)을 입력으로 하는 셋업 알고리즘($Setup(1^{\lambda},N)$)을 수행하여 공개 파라미터(PP)와 제2 마스터키(MK_{PKG})를 생성한다. 이때, 보안 상수(1^{λ})와 사용자의 집합(N)은 제1 서버(100)와 제2 서버(200) 간에 미리 공유된 값일 수 있다.

[0056] 구체적으로, 셋업 모듈(210)은 소수(prime number) p를 위수로 갖는 겹선형 군(p, G, G_T, e)을 생성하고, g를 겹선형 군(G)의 정규 생성원으로 한다.

[0057] 또한, 셋업 모듈(210)은 임의의 난수($\alpha \in Z_p^*$)를 선택하여 제2 공개 파라미터($e(g,g)^{\alpha}$)를 생성한다. 또한, 셋업 모듈(210)은 임의의 스트링(string)에 해당하는 입력값을 타원곡석 위의 점으로 매핑하는 매핑 함수($F:\mathcal{I} \rightarrow G$)와 매핑 함수($H:\mathcal{T} \rightarrow G$)를 선택한다.

[0058] 셋업 모듈(210)은 정규 생성원(g), 겹선형 군(G), 제2 공개 파라미터($\Omega_1 = e(g,g)^{\alpha}$), 매핑 함수($F$), 및 매핑 함수($H$)를 포함하는 공개 파라미터를 공개한다. 본 발명에서 이용되는 공개 파라미터($PP = (g, G, \Omega_1 = e(g,g)^{\alpha}, \Omega_2 = e(g,g)^{\beta}, F, H)$) 중 제1 공개 파라미터($\Omega_2 = e(g,g)^{\beta}$)는 제1 서버(100)에 의해 생성된 파라미터일 수 있다.

[0059] 또한, 셋업 모듈(210)은 제2 마스터키($MK_{PKG} = g^{\alpha}$)를 생성한다. 생성된 제2 마스터키는 제2 단말기(400)로 송신할 보조키를 생성하는 과정에서 이용될 수 있다.

[0060] 상술된 셋업 모듈(210)의 동작 중 제1 서버(100)의 셋업 모듈(110)의 동작과 중복되는 동작은 셋업 모듈(210)과 셋업 모듈(110) 중 어느 하나에 의해 수행되어 공유될 수도 있고, 두 개의 셋업 모듈 각각에서 수행될 수도 있다.

[0061] 보조키 생성 모듈(230)은 ID, 제2 마스터키, 및 공개 파라미터(PP)를 입력으로 하는 보조키 생성 알고리즘($KeySub(ID, MK_{PKG}, PP)$)을 수행하여 보조키를 생성하고, 생성된 보조키를 제2 단말기(400)로 송신한다.

[0062] 구체적으로, 보조키 생성 모듈(230)은 임의의 난수($r \in Z_p$)를 선택하고, 선택된 임의의 난수($r \in Z_p$)를 이용하여 제1 보조키(psk_0)와 제2 보조키(psk_1)를 포함하는 보조키($PSK_{ID}=(psk_0, psk_1)$)생성할 수 있다.

[0063] 제1 보조키(psk_0)와 제2 보조키(psk_1)는 아래의 수학식에 의해 생성될 수 있다.

[0064]
$$psk_0 = g^{\alpha} \cdot F(ID)^r$$
$$psk_1 = g^r$$

[0065] 상기 수학식에서 ID는 제2 단말기(400)의 식별 정보를 의미할 수 있다. 생성된 보조키(PSK_{ID})는 제2 단말기(400)로 송신될 수 있다.

[0066] 도 4는 도 1에 도시된 제2 단말기의 기능 블럭도이다. 도 1 내지 도 4를 참조하면, 제2 단말기(400)는 복호화키 생성 모듈(410)과 복호화 모듈(430)을 포함한다.

[0067] 복호화키 생성 모듈(410)은 보조키, 개인키, 업데이트키, 및 공개 파라미터를 입력으로 하는 복호화키 생성 알

고리즘($DeriveKey(PSK_{ID}, USK_{ID}, KU_T, PP)$)을 수행하여 복호화키를 생성할 수 있다.

[0068] 구체적으로, 복호화키 생성 모듈(410)은 제2 서버(200)로부터 보조키(PSK_{ID})를 수신하고, 제1 서버(100)로부터 개인키(USK_{ID})와 업데이트키(UK_T)를 수신할 수 있다. 또한, 복호화키 생성 모듈(410)은 보조키(PSK_{ID}), 개인키(USK_{ID}), 업데이트키(UK_T), 공개 파라미터(PP)를 이용하여 복호화키를 생성할 수 있다.

[0069] 복화키 생성 과정을 구체적으로 설명하면 다음과 같다.

[0070] 복호화키 생성 모듈(410)은 $PSK_{ID} = (psk_0, psk_1)$, $USK_{ID} = \{(\theta, usk_{\theta,0}, usk_{\theta,1})\}_{\theta \in I}$, 및 $KU_T = \{(\theta, ku_{\theta,0}, ku_{\theta,1})\}_{\theta \in J}$ 을 이용하여 복호화키를 생성할 수 있다. 이때, 집합(I)는 이진트리 상에서 제2 단말기(400)의 개인키에 속해있는 노드들의 집합, 즉 제2 단말기(400)의 ID가 할당된 말단 노드로부터 루트 노드까지의 경로에 포함된 노드들의 집합을 의미하고, 집합(S)는 이진트리 상에서 업데이트키에 속해있는 노드들의 집합을 의미한다.

[0071] 집합(I)와 집합(J)의 교집합이 공집합인 경우, 즉 $I \cap J = \Phi$ 인 경우, 복호화키 생성 모듈(410)은 복호화키를 생성할 수 없다. 제2 단말기(400)의 ID가 T 시간에 폐기되었거나 탈퇴되었다고 볼 수 있기 때문이다.

[0072] 집합(I)와 집합(J)의 교집합이 공집합이 아닌 경우, 즉 $I \cap J \neq \Phi$ 인 경우, 복호화키 생성 모듈(410)은 집합(I)와 집합(J)의 교집합의 원소인 노드($\Theta \in I \cap J$)를 이용하여 복호화키($DK_{ID,T} = (D_1, D_2, D_3)$)를 생성할 수 있다. 이때, $D_1 = psk_0 \cdot usk_{\theta,0} \cdot ku_{\theta,0}$ 이고, $D_2 = psk_1 \cdot usk_{\theta,1}$ 이고, $D_3 = ku_{\theta,1}$ 이다.

[0073] 복호화 모듈(430)은 암호문, 복호화키, 및 공개 파라미터를 입력으로 하는 복호화 알고리즘($Decrypt(CT_{ID,T}, DK_{ID',T'}, PP)$)을 수행하여 암호문을 복호화할 수 있다.

[0074] 구체적으로, 복호화 모듈(430)은 생성된 복호화키($DK_{ID,T}$)와 공개 파라미터(PP)를 이용하여 제1 단말기(300) 또는 클라우드 서버(500)로부터 수신한 암호문(CT_{ID})을 복호화할 수 있다. 암호문(CT)은 (C, C_1, C_2, C_3)이고, 복호화키(DK)는 (D_1, D_2, D_3) 이므로, 암호문(CT)는 다음 수식을 이용하여 복호화될 수 있다.

$$M = C \cdot \prod_{i=1}^{3} e(C_i, D_i)$$

[0075]

[0076] 이때, 제1 단말기(300)에 의한 암호화 과정은 다음과 같다. 제1 단말기(300)는 제2 단말기(400)의 ID, 시간(T), 메시지(M), 및 공개 파라미터(PP)를 입력으로 하는 암호화 알고리즘을 수행함으로써, 메시지(M)에 대한 암호문($CT = (\Omega^t \cdot M, g^{-t}, F(ID)^t, H(T)^t)$)을 생성할 수 있다. 이때, $\Omega = \Omega_1 \cdot \Omega_2$ 을 만족한다.

[0077] 도 2 내지 도 4에 도시된 제1 서버, 제2 서버, 및 제2 단말기의 구성들 각각은 기능 및 논리적으로 분리될 수 있음으로 나타내는 것이며, 반드시 각각의 구성이 별도의 물리적 장치로 구분되거나 별도의 코드로 작성됨을 의미하는 것이 아님을 본 발명의 기술분야의 평균적 전문가는 용이하게 추론할 수 있을 것이다.

[0078] 또한, 본 명세서에서 모듈이라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 모듈은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된

코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것이 아니다.

[0079] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0080] 100 : 제1 서버

110 : 셋업 모듈

130 : 개인키 생성 모듈

150 : 업데이트키 생성 모듈

170 : 폐기 모듈

200 : 제2 서버

210 : 셋업 모듈

230 : 보조키 생성 모듈

300 : 제1 단말기

400 : 제2 단말기

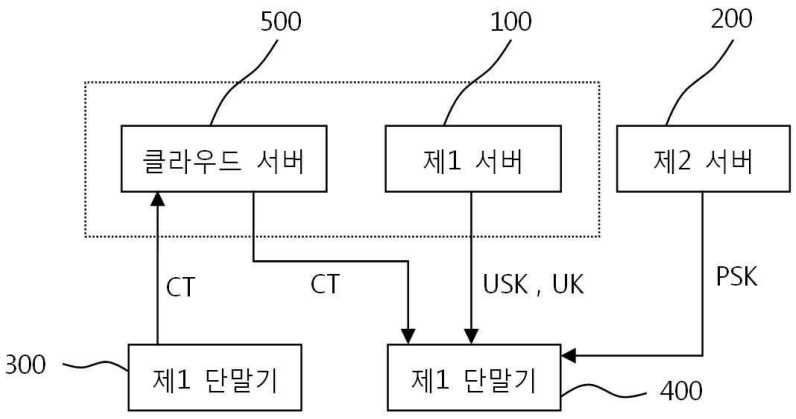
410 : 복호화키 생성 모듈

430 : 복호화 모듈

500 : 클라우드 서버

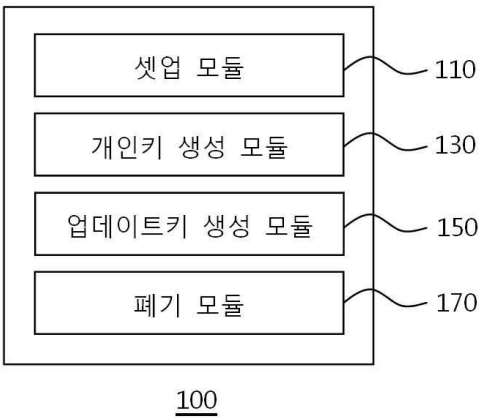
도면

도면1

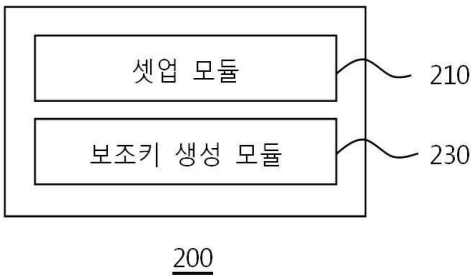


10

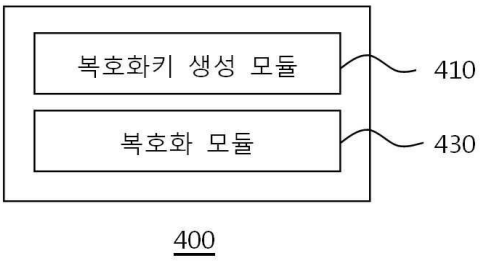
도면2


셋업 모듈
110
개인키 생성 모듈
130
업데이트키 생성 모듈
150
폐기 모듈
170
100

도면3


셋업 모듈
210
보조키 생성 모듈
230
200

도면4


복호화키 생성 모듈
410
복호화 모듈
430
400