(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년05월04일
(11) 등록번호 10-1516114
(24) 등록일자 2015년04월22일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2014-0016718
(22) 출원일자 2014년02월13일
심사청구일자 2014년02월13일
(56) 선행기술조사문헌
KR1020120041904 A
JP2011055309 A

(73) 특허권자
부경대학교 산학협력단
부산광역시 남구 신선로 365 (용당동, 부경대학교)
(72) 발명자
이경현
부산광역시 해운대구 마린시티2로 33, 101동 2209호(두산위브더제니스)
신상욱
부산 남구 분포로 111, 134동 2204호 (용호동, 엘지메트로시티아파트)
(뒷면에 계속)
(74) 대리인
특허법인이상

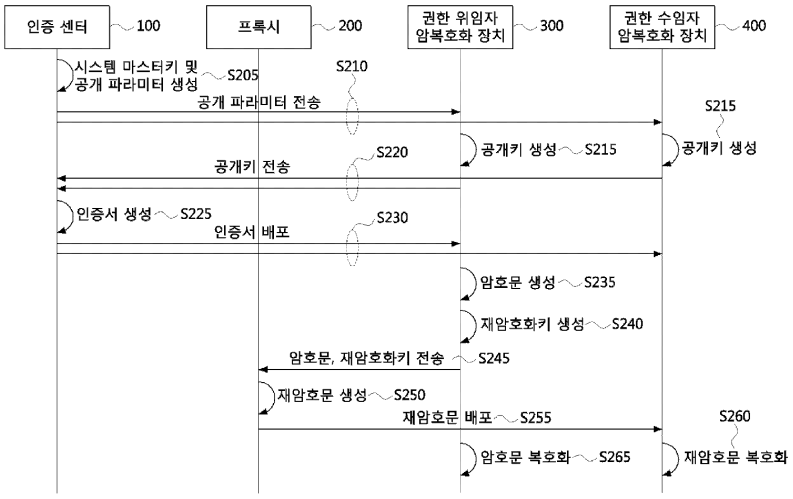
전체 청구항 수 : 총 20 항 심사관 : 문형섭

(54) 발명의 명칭 **인증서 기반 프록시 재암호화 방법 및 이를 위한 시스템**

(57) 요 약

인증서를 기반으로 암호화 및 복호화를 수행하는 장치들의 프록시 재암호화 방법, 시스템 및 암복호화 장치가 개시된다. 인증서 기반 프록시 재암호화 방법은, 인증 센터가 시스템 마스터키를 이용하여 공개 파라미터를 생성하는 초기화 단계와, 공개 파라미터, 평문 및 제1 사용자의 공개키를 입력값으로 하여 암호문을 생성하는 암호화 단계와, 공개 파라미터, 제1 사용자의 인증서, 제1 사용자의 공개키에 대응하는 개인키 및 제2 사용자의 공개키를 입력값으로 하여 재암호화키를 생성하는 재암호화키 생성 단계와, 프록시가 암호문에 기반하여 유효성 검증 파라미터를 산출하고, 암호문이 유효성 검증 파라미터에 관한 소정의 조건을 충족함에 따라, 공개 파라미터, 재암호화키 및 암호문을 입력값으로 하여 재암호문을 생성하는 재암호화 단계를 포함하여 구성될 수 있다.

대 표 도



(72) 발명자

박영호

부산광역시 사상구 모라로52번길 9(102호, 한양하이츠빌라3차)

서철

부산 해운대구 해운대로483번길 15-7, 가-301 (우동, 그린빌라)

이 발명을 지원한 국가연구개발사업

과제고유번호 2013R1A1A4A01009848

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 일반연구자지원 지역대학우수과학자

연구과제명 V-클라우드 기반 응용 서비스 모델 및 보안 메커니즘 개발

기 여 율 1/1

주관기관 부경대학교 산학협력단

연구기간 2013.06.01 ~ 2015.05.31

공지예외적용 : 있음

명 세 서

청구범위

청구항 1

인증서를 기반으로 암호화 및 복호화를 수행하는 장치들의 프록시(proxy) 재암호화(re-encryiption)에 있어서,

인증 센터(authentication center)가 시스템 마스터키를 이용하여 공개 파라미터(public parameter)를 생성하는 초기화 단계;

상기 공개 파라미터, 평문(plain text) 및 제1 사용자의 공개키(public key)를 입력값으로 하여 암호문(cipher text)을 생성하는 암호화 단계;

상기 공개 파라미터, 상기 제1 사용자의 인증서, 상기 제1 사용자의 공개키에 대응하는 개인키(private key) 및 제2 사용자의 공개키를 입력값으로 하여 재암호화키(re-encryption key)를 생성하는 재암호화키 생성 단계;

프록시는, 상기 암호문에 기반하여 유효성 검증 파라미터를 산출하고, 상기 암호문이 상기 유효성 검증 파라미터에 관한 소정의 조건을 충족함에 따라, 상기 공개 파라미터, 상기 재암호화키 및 상기 암호문을 입력값으로 하여 재암호문(re-ciphertext)을 생성하는 재암호화 단계를 포함하는 인증서 기반 프록시 재암호화 방법.

청구항 2

청구항 1에 있어서,

상기 공개 파라미터는,

겹선형 페어링(bilinear pairing), 적어도 하나의 해시 함수(hash function), 상기 시스템 마스터키(system master key)를 이용하여 생성된 시스템 공개키를 포함하여 구성되는 것을 특징으로 하는 인증서 기반 프록시 재암호화 방법.

청구항 3

청구항 1에 있어서,

상기 초기화 단계와 상기 재암호화키 생성 단계 사이에,

인증 센터가 상기 공개 파라미터, 상기 시스템 마스터키, 사용자의 공개키를 입력값으로 하여 상기 사용자의 인증서를 생성하고, 상기 사용자에게 상기 인증서를 배포하는 인증서 생성 단계를 더 포함하는 것을 특징으로 하는 인증서 기반 프록시 재암호화 방법.

청구항 4

청구항 1에 있어서,

상기 암호문은,

상기 유효성 검증 파라미터를 내재한 형태로 생성되는 것을 특징으로 하는 인증서 기반 프록시 재암호화 방법.

청구항 5

청구항 1에 있어서,

상기 재암호화키는,

엘가말 암호 방식(ElGamal Scheme)을 적용한 단방향(uni-directional) 재암호화키인 것을 특징으로 하는 인증서 기반 프록시 재암호화 방법.

청구항 6

청구항 1에 있어서,

상기 소정의 조건은,

상기 암호문이 변경되었는지 여부에 관한 검증식으로 표현되고,

상기 검증식은 상기 공개 파라미터에 포함된 해시 함수 중 적어도 하나를 이용하는 것을 특징으로 하는 인증서 기반 프록시 재암호화 방법.

청구항 7

청구항 1에 있어서,

상기 재암호화 단계 이후에,

상기 공개 파라미터, 상기 제2 사용자의 인증서 및 상기 제2 사용자의 공개키에 대응하는 개인키를 입력값으로 하여 상기 재암호문을 복호화하여 상기 평문을 출력하는 재암호문 복호화 단계를 더 포함하는 것을 특징으로 하는 인증서 기반 프록시 재암호화 방법.

청구항 8

청구항 7에 있어서,

상기 재암호문 복호화 단계는,

상기 재암호문이 상기 제2 사용자의 공개키 및 인증서에 관한 검증식 조건을 충족하는 경우에만 상기 재암호문을 복호화하여 상기 평문을 출력하는 것을 특징으로 하는 인증서 기반 프록시 재암호화 방법.

청구항 9

청구항 1에 있어서,

상기 암호화 단계 이후에,

상기 공개 파라미터, 상기 제1 사용자의 인증서 및 상기 제1 사용자의 공개키에 대응하는 개인키를 입력값으로 하여 상기 암호문을 복호화하여 상기 평문을 출력하는 암호문 복호화 단계를 더 포함하는 것을 특징으로 하는 인증서 기반 프록시 재암호화 방법.

청구항 10

청구항 9에 있어서,

상기 암호문 복호화 단계는,

상기 암호문이 상기 제1 사용자의 공개키 및 인증서에 관한 검증식 조건을 충족하는 경우에만 상기 암호문을 복호화하여 상기 평문을 출력하는 것을 특징으로 하는 인증서 기반 프록시 재암호화 방법.

청구항 11

평문, 제1 사용자의 공개키 및 인증 센터로부터 전달된 공개 파라미터를 입력값으로 하여 유효성 검증 파라미터를 내재한 형태로 암호문을 생성하는 암호화부;

상기 공개 파라미터, 상기 제1 사용자의 인증서, 상기 제1 사용자의 공개키에 대응하는 개인키 및 제2 사용자의 공개키를 입력값으로 하여 재암호화키를 생성하는 재암호화키 생성부;

프록시가 재암호문을 생성하도록 상기 재암호화키를 상기 프록시에 전달하는 재암호화키 전달부를 포함하는 제1 사용자 암복호화 장치.

청구항 12

청구항 11에 있어서,

상기 재암호화키는,

엘가말 암호 방식을 적용한 단방향 재암호화키인 것을 특징으로 하는 제1 사용자 암복호화 장치.

청구항 13

청구항 11에 있어서,

상기 공개 파라미터, 상기 제1 사용자의 인증서 및 상기 제1 사용자의 공개키에 대응하는 개인키를 입력값으로 하여 상기 암호문을 복호화하여 상기 평문을 출력하는 암호문 복호화부를 더 포함하되,

상기 암호문 복호화부는 상기 암호문이 상기 제1 사용자의 공개키 및 인증서에 관한 검증식 조건을 충족하는 경우에만 상기 암호문을 복호화하여 상기 평문을 출력하는 것을 특징으로 하는 제1 사용자 암복호화 장치.

청구항 14

인증서 기반의 프록시 재암호화 시스템에 있어서,

시스템 마스터키를 이용하여 공개 파라미터를 생성하는 초기화부를 구비하고 있는 인증 센터;

상기 공개 파라미터, 제1 사용자의 인증서, 상기 제1 사용자의 공개키에 대응하는 개인키 및 제2 사용자의 공개키를 입력값으로 하여 재암호화키를 생성하는 재암호화키 생성부를 구비하고 있는 제1 사용자 암복호화 장치;

암호문에 기반하여 유효성 검증 파라미터를 산출하고, 상기 암호문이 상기 유효성 검증 파라미터에 관한 소정의 조건을 충족함에 따라, 상기 공개 파라미터, 상기 재암호화키 및 상기 암호문을 입력값으로 하여 재암호문을 생성하는 재암호화부를 구비하고 있는 프록시를 포함하는 인증서 기반 프록시 재암호화 시스템.

청구항 15

청구항 14에 있어서,

상기 공개 파라미터는,

겹선형 페어링, 적어도 하나의 해시 함수, 상기 시스템 마스터키를 이용하여 생성된 시스템 공개키를 포함하여 구성되는 것을 특징으로 하는 인증서 기반 프록시 재암호화 시스템.

청구항 16

청구항 14에 있어서,

상기 인증 센터는,

상기 공개 파라미터, 상기 시스템 마스터키, 사용자의 공개키를 입력값으로 하여 상기 사용자의 인증서를 생성하고, 상기 사용자에게 상기 인증서를 배포하는 인증서 생성부를 더 포함하는 것을 특징으로 하는 인증서 기반 프록시 재암호화 시스템.

청구항 17

청구항 14에 있어서,

상기 암호문은,

상기 유효성 검증 파라미터를 내재한 형태로 생성되는 것을 특징으로 하는 인증서 기반 프록시 재암호화 시스템.

청구항 18

청구항 14에 있어서,

상기 재암호화키는,

엘가말 암호 방식을 적용한 단방향 재암호화키인 것을 특징으로 하는 인증서 기반 프록시 재암호화 시스템.

청구항 19

청구항 14에 있어서,

상기 소정의 조건은,

상기 암호문이 변경되었는지 여부에 관한 검증식으로 표현되고,

상기 검증식은 상기 공개 파라미터에 포함된 해시 함수 중 적어도 하나를 이용하는 것을 특징으로 하는 인증서 기반 프록시 재암호화 시스템.

청구항 20

청구항 14에 있어서,

상기 공개 파라미터, 상기 제2 사용자의 인증서 및 상기 제2 사용자의 공개키에 대응하는 개인키를 입력값으로 하여 상기 재암호문을 복호화하여 평문을 출력하는 재암호문 복호화부를 구비하고 있는 제2 사용자 암복호화 장치를 더 포함하되,

상기 재암호문 복호화부는 상기 재암호문이 상기 제2 사용자의 공개키 및 인증서에 관한 검증식 조건을 충족하는 경우에만 상기 재암호문을 복호화하여 상기 평문을 출력하는 것을 특징으로 하는 인증서 기반 프록시 재암호화 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 인증서 기반의 암호화 기술(certificate-based encryption)을 이용한 프록시 재암호화(proxy re-encryption)에 관한 것으로, 더욱 상세하게는 프록시와 복호화 권한을 위임받은 권한 수임자 간의 공모 공격(collusion attack)과 선택 암호문 공격(chosen ciphertext attack)에 대한 안전성을 보장하기 위하여 단방향 프록시 재암호화키(uni-directional proxy re-encryption key)를 생성하고 사용하는 기술에 관한 것이다.

배 경 기 술

[0002] 데이터 전송 시, 타인의 불법적인 방법에 의해 데이터가 도청되거나 유출되는 것을 방지하기 위한 기술로서 데이터를 쉽게 해독할 수 없도록 다른 형태로 변환하여 전송하고 데이터를 수신하는 쪽에서는 이를 원래의 형태대로 복원하는 방법이 연구되어 왔다.

[0003] 이를 암호화 및 복호화라고 하며, 암호화 방식은 크게 대칭형 암호화 방식의 비밀키 암호화 기법(symmetric key cryptography)과 비대칭형 암호화 방식의 공개키 암호화 기법(asymmetric key cryptography)으로 나뉘어진다.

[0004] 비밀키(private key) 암호화 기법은 동일한 키로 암호화와 복호화를 수행하는 방법으로 보안 유지와 키 관리에 어려움이 있으나 알고리즘이 간단해 암호화 속도가 빠르고 용량이 작아 경제적이다.

[0005] 즉, 하나의 비밀키로 암호화 및 복호화를 해야 하므로 비밀 통신을 하는 당사자들만이 키를 안전하게 공유해야 한다. 그래서 이 방법을 비밀키 암호 시스템(secret key cryptosystem)이라고도 한다. 대표적인 알고리즘으로 DES(Data Encryption Standard)와, DES의 단점을 일부 보완한 Triple DES와 AES(Advanced Encryption Standard) 등이 있다.

[0006] 공개키(public Key) 암호화 기법은 공개되는 공개키와 본인만 사용하는 비밀키(private key)로 구성되는 것으로 공개키와 비밀키를 별도로 관리하기 때문에 키 관리가 용이하며 암호화와 사용자 인증이 동시에 이뤄진다는 특징이 있다. 이는 전자 문서의 디지털서명, 부인봉쇄에 사용된다. 그러나 알고리즘이 복잡해 속도가 느리다는 단점을 가지고 있다.

[0007] 즉, 각 사용자 주체마다 두 개의 키가 존재하여, 각 사용자마다 키쌍(key pair)인 공개키(public key)와 개인키(private key)를 유지해야 한다. 대표적인 알고리즘으로는 RSA(Rivest Shamir Adleman), ECC(Elliptic Curve Cryptosystem) 등이 있다.

[0008] 이 중 공개키 암호화(public key encryption) 기술은 특정 사용자의 공개키를 이용하여 메시지에 대한 암호화를 수행하여 암호문을 생성하고, 공개키에 대응하는 개인키로 암호문을 복호화하여 메시지를 획득하는 것이므로, 이와 같은 환경에서 다른 사용자에게 복호화 권한을 위임하기 위해서는 권한 위임자의 개인키를 권한 수임자(피위임자)에게 알려주거나, 모든 암호문에 대하여 복호화를 수행한 후 권한 수임자의 공개키로 메시지를 암호화하여야 한다. 하지만, 권한 위임자의 개인키를 알려주는 것은 많은 보안적인 위협들을 초래하므로 전자의 방법은 적절한 방법이 될 수 없으며, 후자의 방법은 실시간으로 복호화와 암호화를 수행해야 하므로 항상 권한 위임자에 대하여 온라인 상태일 것을 요구한다. 또한, 복호화와 암호화의 수행으로 인하여 권한 위임자의 추가적인 계

산 상의 오버헤드(overhead)를 초래한다.

[0009] 따라서, 기존의 공개키 암호화 기술은 암호학적 기능들 중의 가장 중요한 기술이지만, 위에서 언급한 복호화 권한위임에 관련된 키 관리의 문제와 추가적인 오버헤드로 인하여 상황에 따라 실용적인 적용에서 많은 제한점을 내포하고 있다.

[0010] 위와 같은 문제점들을 해결하기 위하여, 1998년 Blaze, Bleumer와 Starauss는 특정 사용자(권한 위임자)의 공개키로 암호화된 메시지를 복호화하지 않고, 프록시(proxy)가 재암호화키를 이용하여 암호문을 재암호화하여 새로운 암호문(재암호문)을 생성하고 복호화 권한을 획득한 권한 수임자(피위임자)의 개인키로 새로운 암호문(재암호문)을 복호화할 수 있는 프록시 재암호화 방법을 제안하였다.

[0011] 프록시 재암호화 방법에서 프록시는 특정 사용자(권한 위임자)의 공개키로 암호화된 암호문을 다른 사용자(권한 수임자)의 개인키로 복호화할 수 있도록 암호문을 변형하는 역할을 수행하지만, 이러한 변형단계(재암호화단계)에서 프록시는 암호문 또는 재암호문으로 부터 평문에 관한 정보를 알 수 없어야 한다는 조건을 만족시키는 것이 바람직하다. 이와 같은 조건으로 인하여, 프록시 재암호화 방법은 분산 파일 시스템, 안전한 메일 포워딩 및 호환 가능한 DRM(Digital Rights Management) 시스템과 같은 서비스에서 효율적인 키 관리를 위한 핵심 암호학적 기반기술로 각광받고 있고 있으며, 최근까지 많은 프록시 재암호화 방법들이 연구되고 있다.

[0012] 프록시 재암호화 방법의 기능적 측면을 고려할 때, 프록시 재암호화 방법은 재암호화키의 특성에 따라 양방향(bidirectional) 프록시 재암호화 방법과 단방향(unidirectional) 프록시 재암호화 방법으로 분류된다. 동일한 재암호화키를 이용하여 복호화 권한 위임자로부터 복호화 권한 수임자로의 암호문 변형뿐만 아니라, 역방향(권한 수임자로부터 권한 위임자)의 변형도 가능할 때 이를 양방향 프록시 재암호화 방법이라 하고, 역변환을 허용하지 않을 경우에 단방향 프록시 재암호화 방법이라 한다.

[0013] 일반적으로, 프록시 재암호화 방법의 설계시 단방향 프록시 재암호화 방법을 두 번 사용함으로써 양방향 프록시 재암호화 방법과 동일한 기능을 제공할 수 있기 때문에, 원천기술로써 단방향 프록시 재암호화 방법을 설계하는 것이 보다 더 유용하다. 더욱이, 양방향 프록시 재암호화 방법들은 권한 수임자와 프록시의 공모를 통하여 권한 위임자의 개인키 정보를 유출하는 공모 공격(collusion attack)에 취약성을 나타낸다.

[0014] 이를 위하여, Ateniese외 저자들은 겹선형 페어링(bilinear pairing)을 이용하여 처음으로 단방향 프록시 재암호화 방법을 설계하였다. 하지만, 그들이 제안한 방법은 공모 공격에는 안전하지만, 선택 평문 공격(CPA, Chosen Plaintext Attack)에 대한 안전성만을 보장한다. 이후, Canetti와 Hohenberger는 선택 평문 공격에만 안전한 기법은 다양한 응용기술로의 적용에 충분한 안정성을 제공하지 못함을 제시하고, 선택 암호문 공격(CCA, Chosen Ciphertext Attack)에 안전한 프록시 재암호화 방법을 제안하였다.

[0015] 하지만, Canetti와 Hohenberger의 방법은 양방향 방법으로써 기존의 양방향 프록시 재암호화 방법들처럼 여전히 공모 공격에 취약성을 가지고 있다. 최근, 선택 암호문 공격에 안전한 단방향 프록시 재암호화 기법이 Libert와 Vergnaud에 의하여 제안되었으며, Shao와 Cao는 겹선형 페어링 연산을 제거한 단방향 프록시 재암호화 방법을 제안하였다. 또한, Green과 Ateniese는 기존의 공개키 암호 기술을 이용한 방법들과 달리 신원기반 암호화(identity-based encryption) 기술을 이용한 프록시 재암호화 방법의 설계시 고려해야 할 점을 지적하고, 선택 암호문 공격에 안전한 신원기반 단방향 프록시 재암호화 방법을 설계하였다. 하지만, 제안 방법에 사용되는 재암호화키 생성 기술의 특성으로 인하여 여전히 공모 공격에 취약성을 가지고 있다.

[0016] 비록 최근까지 많은 프록시 재암호화 방법들이 제안되었지만, 이미 제안된 프록시 재암호화 방법들은 전통적인 공개키 암호화 기술 또는 신원기반 암호화 기술을 이용하여 설계되었다. 하지만, 전통적인 공개키 암호화 기술은 인증서 관리 문제의 어려움을 내포하고 있으며, 신원기반 암호화 기술은 키 위탁문제를 가지고 있다.

발명의 내용

해결하려는 과제

[0017] 본 발명은 위와 같은 종래의 문제점을 해결하기 위해 안출된 것으로, 본 발명의 목적은 인증서 기반 암호화(certificate-based encryption) 기술을 이용하여 프록시 재암호화 방법을 설계하여, 프록시 재암호화 기술의 기능적 특성인 안전한 복호화 권한 위임을 위한 효율적인 키 관리 방법을 제공하는 것에 있다. 더 나아가, 기존 공개키 암호화 기술을 이용한 프록시 재암호화 방법의 인증서(certificate) 관리 문제와 신원기반 암호화 기술의 키 위탁(key escrow) 문제를 해결할 수 있는 새로운 프록시 재암호화 방법을 제공하는 것이다.

[0018] 본 발명의 다른 목적은 재암호화키 생성 단계와 재암호화 단계를 통하여 프록시에 의해 메시지를 노출 당하는 공격 및 권한 위임자와 권한 수임자의 개인키 정보를 노출 당하는 공격에 안전성을 보장하는 동시에 현재 안전한 공개키 암호화 기술을 위한 표준 보안 모델(security model)로써 고려되고 있는 악의적인 공격자에 의한 임의의 암호문 변경을 통한 선택 암호문 공격(CCA, Chosen Ciphertext Attack)에 대하여 안전성을 보장하는 프록시 재암호화 방법을 제공하는 것이다.

[0019] 본 발명의 또 다른 목적은 복호화 권한을 위임받은 권한 수임자와 프록시 재암호화키를 소유하고 있는 프록시와의 공모 공격(collusion attack)을 통한 복호화 권한 위임자의 개인키 정보 유출을 방지하기 위해 단방향 재암호화키를 생성하여 사용하는 단방향 프록시 재암호화 방법을 제공하는 것이다. 또한 프록시 재암호화키 생성 단계에서 본 발명의 효율성 향상을 위하여 권한 위임자와 프록시 간의 비밀정보를 전송하는 추가적인 단계가 필요하지 않은 비대화식(non-interactive) 프록시 재암호화키 생성 방법을 제공하는 것이다.

과제의 해결 수단

[0020] 상술한 본 발명의 목적을 달성하기 위한 일 측면에 따른 인증서 기반 프록시 재암호화 방법은, 인증서를 기반으로 암호화 및 복호화를 수행하는 장치들의 프록시(proxy) 재암호화(re-encryiption)에 있어서, 인증 센터(authentication center)가 시스템 마스터키를 이용하여 공개 파라미터(public parameter)를 생성하는 초기화 단계와, 공개 파라미터, 평문(plain text) 및 제1 사용자의 공개키(public key)를 입력값으로 하여 암호문(cipher text)을 생성하는 암호화 단계와, 공개 파라미터, 제1 사용자의 인증서, 제1 사용자의 공개키에 대응하는 개인키(private key) 및 제2 사용자의 공개키를 입력값으로 하여 재암호화키(re-encryption key)를 생성하는 재암호화키 생성 단계와, 프록시는 상기 암호문에 기반하여 유효성 검증 파라미터를 산출하고, 암호문이 상기 유효성 검증 파라미터에 관한 소정의 조건을 충족함에 따라, 공개 파라미터, 재암호화키 및 암호문을 입력값으로 하여 재암호문(re-ciphertext)을 생성하는 재암호화 단계를 포함하여 구성될 수 있다.

[0021] 여기에서, 공개 파라미터는, 겹선형 페어링(bilinear pairing), 적어도 하나의 해시 함수(hash function), 시스템 마스터키(system master key)를 이용하여 생성된 시스템 공개키를 포함하여 구성될 수 있다.

[0022] 여기에서, 인증서 기반 프록시 재암호화 방법은, 초기화 단계와 재암호화키 생성 단계 사이에, 인증 센터가 공개 파라미터, 시스템 마스터키, 사용자의 공개키를 입력값으로 하여 사용자의 인증서를 생성하고, 사용자에게 상기 인증서를 배포하는 인증서 생성 단계를 더 포함하여 구성될 수 있다.

[0023] 여기에서, 상기 암호문은, 유효성 검증 파라미터를 내재한 형태로 생성될 수 있다.

[0024] 여기에서, 상기 재암호화키는, 엘가말 암호 방식(ElGamal Scheme)을 적용한 단방향(uni-directional) 재암호화키일 수 있다.

[0025] 여기에서, 상기 소정의 조건은, 암호문이 변경되었는지 여부에 관한 검증식으로 표현되고, 검증식은 공개 파라미터에 포함된 해시 함수 중 적어도 하나를 이용할 수 있다.

[0026] 여기에서, 인증서 기반 프록시 재암호화 방법은, 재암호화 단계 이후에, 공개 파라미터, 제2 사용자의 인증서 및 제2 사용자의 공개키에 대응하는 개인키를 입력값으로 하여 재암호문을 복호화하여 평문을 출력하는 재암호문 복호화 단계를 더 포함하여 구성될 수 있다.

[0027] 나아가, 상기 재암호문 복호화 단계는, 재암호문이 제2 사용자의 공개키 및 인증서에 관한 검증식 조건을 충족하는 경우에만 재암호문을 복호화하여 평문을 출력할 수 있다.

[0028] 여기에서, 인증서 기반 프록시 재암호화 방법은, 암호화 단계 이후에, 공개 파라미터, 제1 사용자의 인증서 및 제1 사용자의 공개키에 대응하는 개인키를 입력값으로 하여 암호문을 복호화하여 평문을 출력하는 암호문 복호화 단계를 더 포함하여 구성될 수 있다.

[0029] 나아가, 상기 암호문 복호화 단계는, 암호문이 제1 사용자의 공개키 및 인증서에 관한 검증식 조건을 충족하는 경우에만 암호문을 복호화하여 평문을 출력할 수 있다.

[0030] 상술한 본 발명의 목적을 달성하기 위한 다른 측면에 따른 제1 사용자 암복호화 장치는, 평문, 제1 사용자의 공개키 및 인증 센터로부터 전달된 공개 파라미터를 입력값으로 하여 유효성 검증 파라미터를 내재한 형태로 암호문을 생성하는 암호화부와, 공개 파라미터, 제1 사용자의 인증서, 제1 사용자의 공개키에 대응하는 개인키 및 제2 사용자의 공개키를 입력값으로 하여 재암호화키를 생성하는 재암호화키 생성부와, 프록시가 재암호문을 생성하도록 재암호화키를 프록시에 전달하는 재암호화키 전달부를 포함하여 구성될 수 있다.

[0031] 여기에서, 상기 재암호화키는, 엘가말 암호 방식을 적용한 단방향 재암호화키일 수 있다.

[0032] 여기에서, 제1 사용자 암복호화 장치는, 공개 파라미터, 제1 사용자의 인증서 및 제1 사용자의 공개키에 대응하는 개인키를 입력값으로 하여 암호문을 복호화하여 평문을 출력하는 암호문 복호화부를 더 포함하되, 암호문 복호화부는 암호문이 제1 사용자의 공개키 및 인증서에 관한 검증식 조건을 충족하는 경우에만 암호문을 복호화하여 상기 평문을 출력할 수 있다.

[0033] 상술한 본 발명의 목적을 달성하기 위한 또다른 측면에 따른 인증서 기반 프록시 재암호화 시스템은, 인증서 기반의 프록시 재암호화 시스템에 있어서, 시스템 마스터키를 이용하여 공개 파라미터를 생성하는 초기화부를 구비하고 있는 인증 센터와, 공개 파라미터, 제1 사용자의 인증서, 제1 사용자의 공개키에 대응하는 개인키 및 제2 사용자의 공개키를 입력값으로 하여 재암호화키를 생성하는 재암호화키 생성부를 구비하고 있는 제1 사용자 암복호화 장치와, 암호문에 기반하여 유효성 검증 파라미터를 산출하고, 암호문이 유효성 검증 파라미터에 관한 소정의 조건을 충족함에 따라, 공개 파라미터, 재암호화키 및 암호문을 입력값으로 하여 재암호문을 생성하는 재암호화부를 구비하고 있는 프록시를 포함하여 구성될 수 있다.

[0034] 여기에서, 상기 공개 파라미터는, 겹선형 페어링, 적어도 하나의 해시 함수, 시스템 마스터키를 이용하여 생성된 시스템 공개키를 포함하여 구성될 수 있다.

[0035] 여기에서, 상기 인증 센터는, 공개 파라미터, 시스템 마스터키, 사용자의 공개키를 입력값으로 하여 사용자의 인증서를 생성하고, 사용자에게 인증서를 배포하는 인증서 생성부를 더 포함하여 구성될 수 있다.

[0036] 여기에서, 상기 암호문은, 유효성 검증 파라미터를 내재한 형태로 생성될 수 있다.

[0037] 여기에서, 상기 재암호화키는, 엘가말 암호 방식을 적용한 단방향 재암호화키일 수 있다.

[0038] 여기에서, 상기 소정의 조건은, 암호문이 변경되었는지 여부에 관한 검증식으로 표현되고, 검증식은 공개 파라미터에 포함된 해시 함수 중 적어도 하나를 이용할 수 있다.

[0039] 여기에서, 인증서 기반 프록시 재암호화 시스템은, 공개 파라미터, 제2 사용자의 인증서 및 제2 사용자의 공개키에 대응하는 개인키를 입력값으로 하여 재암호문을 복호화하여 평문을 출력하는 재암호문 복호화부를 구비하고 있는 제2 사용자 암복호화 장치를 더 포함하되, 재암호문 복호화부는 재암호문이 제2 사용자의 공개키 및 인증서에 관한 검증식 조건을 충족하는 경우에만 재암호문을 복호화하여 평문을 출력할 수 있다.

발명의 효과

[0040] 상기와 같은 본 발명에 따른 인증서 기반 프록시 재암호화 방법 및 시스템, 제1 사용자 암복호화 장치를 사용하면, 특정 사용자(권한 위임자)의 공개키로 암호화된 메시지를 프록시에 의해서 다른 사용자(권한 수임자)의 개인키로 복호화할 수 있는 새로운 암호문을 생성하는 프록시 재암호화 방법에 있어서, 인증서를 복호화 단계에서 암호문을 복호화하기 위한 부분 복호화키로 사용함으로써 사용자의 공개키에 대한 묵시적 인증(implicit certification)을 제공하여 기존의 공개키 암호화 기술을 이용한 프록시 재암호화 방법의 인증서 관리 문제를 해결할 수 있다는 장점이 있다.

[0041] 또한, 사용자의 개인키를 복호화 단계에서 암호문을 복호화하기 위한 부분 복호화키로 사용함으로써 기존의 신원기반 암호화 기술을 이용한 프록시 재암호화 방법의 키 위탁 문제를 해결할 수 있다.

[0042] 또한, 본 발명은 암호화 단계에서 생성되는 암호문 및 재암호화 단계에서 생성되는 재암호문에 관하여 공개키 암호화 기술의 표준 보안 모델인 선택 암호문 공격(CCA, Chosen Cihpertext Attack)에 대하여 암호학적 증명 가능한 안전성을 제공할 수 있다.

[0043] 재암호화키 생성 단계에서는 단방향 재암호화키를 생성하여 재암호화 단계에서 재암호문 생성을 위해 사용되므로 복호화 권한을 위임받은 권한 수임자와 프록시 간의 공모 공격에 대한 안전성을 제공할 수 있다. 또한, 재암호화키 생성단계에서 복호화 권한 위임자와 프록시 간의 비밀정보를 전송하는 추가적인 단계가 필요로 하지 않는 비대화식 재암호화키 생성 방법을 제공하므로 효율성을 높일 수 있다는 효과가 있다.

도면의 간단한 설명

[0044] 도 1은 본 발명의 일 실시예에 따른 사용자 암복호화 장치와 인증 서버의 일반적인 환경을 설명하기 위한 개념도이다.

도 2는 본 발명의 일 실시예에 따른 인증서 기반 프록시 재암호화 방법과 그 세부 구성요소를 설명하기 위한 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 인증서 기반 프록시 재암호화 시스템과 그 세부 구성요소, 제1 사용자 암복호화 장치와 그 세부 구성요소를 설명하기 위한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0045] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0046] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0047] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0048] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0049] 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 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0050] 먼저, 본 출원에서 사용되는 용어를 간략히 설명하면 다음과 같다.

[0051] 신원기반 암호화(IBE, Identity-Based Encryption)란 공개키 암호화 방식의 또 다른 일종으로 사용자의 정보를 공개키로 사용한다. 이때 공개키로 사용할 수 있는 정보는 사용자의 이메일 주소나 전화번호 등 그 사용자에게만 해당하는 유일한 정보여야 한다.

[0052] 공개키 암호 방식이란, 이전에 서로 만나서 키를 나누어가지지 않은 사용자라도 안전하게 통신할 수 있도록 한다. 다만, 이때 상대방이 공개키가 정말로 그 사용자의 공개 열쇠인지 확인할 수 있는 방법이 반드시 필요하다. 흔히 이것은 전자인증서와 같은 public key infrastructure를 통해서 확인하지만, 이 과정이 번거롭고 비용도 많이 든다. 신원 기반암호는 상대방의 신원을 공개 열쇠로 사용하므로 이런 과정이 불필요하다. 즉, 인증서가 필요하지 않다.

[0053] 암호 기술에서 공모 공격이란 다수의 사용자가 공모하여, 암호 시스템 혹은 일반 사용자가 소유한 비밀값 혹은 정보를 획득하는 공격 방법이다.

[0054] 선택 평문 공격(CPA, Chosen Plaintext Attack)은, 암호 분석가가 임의로 선택한 평문과 그것에 대응한 암호문을 이용하는 공격 방법이다.

[0055] 선택 암호문 공격(CCA, Chosen Ciphertext Attack)은, 암호 분석가가 임의로 선택된 암호문과 일치하는 평문으로부터 공격하고자 하는 암호문과 일치하는 평문을 알아내기 위해 시도하는 공격이다. 이는 선택 평문 공격보다

더욱 강력한 공격 방법으로써 현재 안전한 공개키 암호화 기술을 위한 표준 보안 모델로써 고려되고 있다.

[0056] 해시 함수(hash function)란 주어진 원문에서 고정된 길이의 난수를 생성하는 연산기법이다. 생성된 값은 해시값 혹은 해시코드라고 한다. 통신회선을 통해서 데이터를 주고받을 때, 송신측과 수신측의 양쪽 끝에서 데이터의 해쉬값을 구해서 비교하면, 전송 도중 조작 여부를 확인할 수 있다.

[0057] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명하기에 앞서 본 발명의 구성을 간략하게 정리하면 다음과 같다.

[0058] 인증서 기반 암호화 기술을 이용한 단방향 프록시 재암호화 방법은, ① 인증 센터가 시스템 마스터키와 공개파라미터를 생성하는 초기화단계, ② 공개파라미터를 입력 값으로, 사용자(복호화 권한 위임자와 수임자를 모두 포함) 측에서 자신의 공개키와 개인키 쌍을 생성하는 키 생성단계, ③ 인증 센터가 공개파라미터, 마스터키와 사용자의 신원정보, 공개키를 입력 값으로 인증서를 생성하는 인증서 생성단계, ④ 암호화하고자 하는 메시지와 공개파라미터, 사용자의 신원정보, 공개키를 입력 값으로, 암호문을 생성하게 되는 암호화 단계, ⑤ 공개파라미터, 복호화 권한 위임자(④ 단계에서 암호문을 생성한 사용자)의 인증서, 개인키와 권한 수임자의 신원정보, 공개키를 입력 값으로, 권한 위임자 측에서 단방향 재암호화키를 생성하는 재암호화키 생성단계, ⑥ 공개파라미터, 재암호화키와 권한 위임자를 위한 암호문을 입력 값으로, 프록시 측에서 권한 수임자를 위해 재암호화된 새로운 암호문(재암호문)을 생성하게 되는 재암호화 단계, ⑦ 공개파라미터, 암호문과 권한 위임자의 인증서, 개인키를 입력 값으로, 암호화 단계에서 암호화된 암호문을 복호화 하여 출력하게 되는 암호문 복호화 단계와, 공개파라미터, 재암호문과 권한 수임자의 인증서, 개인키를 입력 값으로, 재암호화 단계에서 암호화된 재암호문을 복호화 하여 출력하게 되는 재암호문 복호화 단계로 이루어지는 것을 기술적 요지로 한다.

[0059] 본 발명의 상기 초기화단계에서 인증센터가 겹선형 그룹(bilinear group)상에서 정의되는 수학적 연산을 기반으로 하여 시스템 마스터키와 인증센터의 공개키 및 암호학적 해시함수(cryptographic hash function)들을 포함하는 공개파라미터을 생성하는 특징을 갖는다.

[0060] 암호화 단계에서는, 사용자의 신원정보와 공개키에 대한 암호화뿐만 아니라 복호화 권한을 위임받은 권한 수임자를 위한 재암호화를 가능하게 하는 암호문 생성을 가능케 하며, 악의적인 공격자에 의한 임의의 암호문 변경을 통한 선택 암호문 공격에 안전성을 보장할 수 있는 암호문을 생성하는 특징을 갖는다.

[0061] 재암호화키 생성 단계에서는, 프록시와 권한 수임자간의 공모를 통한 권한 위임자의 개인키 정보를 유출하는 공모 공격에 안전성을 보장하기 위하여 ElGamal 암호 기술이 적용된 단방향 재암호화키를 생성하며, 재암호화키 생성을 위하여 권한 위임자와 프록시 간의 비밀정보의 전송이 필요로 하지 않는 비대화식 프록시 재암호화키를 생성하는 특징을 갖는다.

[0062] 재암호화 단계에서는, 권한 위임자의 신원정보와 공개키에 대한 암호문을 프록시가 재암호화키 생성 단계에서 생성된 단방향 재암호화키를 사용하여 복호화 권한을 위임받은 권한 수임자를 위한 재암호문을 생성하고, 악의적인 공격자에 의한 임의의 암호문 변경을 통한 선택 암호문 공격에 대한 안전성을 보장하기 위해 권한 위임자를 위한 암호문에 대한 유효성 검증식을 포함하는 특징을 갖는다.

[0063] 복호화 단계에서는, 암호화 단계에서 생성된 암호문에 대한 복호화와 재암호화 단계에서 생성된 재암호문에 대한 복호화를 수행하여 메시지를 복원하고, 악의적인 공격자에 의한 임의의 암호문 변경을 통한 선택 암호문 공격에 대한 안전성을 보장하기 위해 암호문 및 재암호문에 대한 유효성 검증식을 포함하는 특징을 갖는다.

[0064] 도 1은 본 발명의 일 실시예에 따른 사용자 암복호화 장치와 인증 서버의 일반적인 환경을 설명하기 위한 개념도이다. 도 1을 참조하여 인증서 기반 프록시 재암호화 환경을 살펴보면 다음과 같다.

[0065] 암복호화 장치는 일반적으로 컴퓨팅이 가능한 적어도 하나의 프로세서와 기록 매체를 포함하여 구성될 수 있고, 다양한 접속망(access network)을 통하여 인증 서버 및 프록시에 접근할 수 있다. 접속망의 종류는 제한되지 않는다. 유무선 통신망이 모두 포함될 수 있다. 일반적으로 인증서버와 프록시는 코어망(core network)에 위치할 수 있다.

[0066] 그러나 인증서 기반 프록시 재암호화에 있어서, 각 구성요소들이 반드시 도 1의 형태로 물리적으로 분리되어 있어야 하는 것은 아니다. 예를 들어 프록시는 암복호화 장치를 포함한 컴퓨팅 장치 내에 위치하는 것도

가능하다.

[0067] 도 2는 본 발명의 일 실시예에 따른 인증서 기반 프록시 재암호화 방법과 그 세부 구성요소를 설명하기 위한 흐름도이다. 도 2를 참조하여 인증서 기반 프록시 재암호화 방법을 살펴보면 다음과 같다.

[0068] 인증서 기반 프록시 재암호화 방법은, 인증서를 기반으로 암호화 및 복호화를 수행하는 장치들의 프록시(proxy) 재암호화(re-encryiption)에 있어서, 인증 센터(authentication center)가 시스템 마스터키를 이용하여 공개 파라미터(public parameter)를 생성하는 초기화 단계(S205)와, 공개 파라미터, 평문(plain text) 및 제1 사용자의 공개키(public key)를 입력값으로 하여 암호문(cipher text)을 생성하는 암호화 단계(S235)와, 공개 파라미터, 제1 사용자의 인증서, 제1 사용자의 공개키에 대응하는 개인키(private key) 및 제2 사용자의 공개키를 입력값으로 하여 재암호화키(re-encryption key)를 생성하는 재암호화키 생성 단계(S240)와, 프록시는 상기 암호문에 기반하여 유효성 검증 파라미터를 산출하고, 암호문이 유효성 검증 파라미터에 관한 소정의 조건을 충족함에 따라, 공개 파라미터, 재암호화키 및 암호문을 입력값으로 하여 재암호문(re-ciphertext)을 생성하는 재암호화 단계(S250)를 포함하여 구성될 수 있다.

[0069] 공개 파라미터는 겹선형 페어링(bilinear pairing), 적어도 하나의 해시 함수(hash function), 시스템 마스터키(system master key)를 이용하여 생성된 시스템 공개키를 포함하여 구성될 수 있다.

[0070] 인증서 기반 프록시 재암호화 방법은, 초기화 단계(S205)와 재암호화키 생성 단계(S240) 사이에, 인증 센터가 공개 파라미터, 시스템 마스터키, 사용자의 공개키를 입력값으로 하여 사용자의 인증서를 생성하고, 사용자에게 인증서를 배포하는 인증서 생성 단계(S225, S230)를 더 포함하여 구성될 수 있다.

[0071] 암호문은 유효성 검증 파라미터를 내재한 형태로 생성될 수 있고, 재암호화키는 엘가말 암호 방식(ElGamal Scheme)을 적용한 단방향(uni-directional) 재암호화키일 수 있다.

[0072] 소정의 조건은, 암호문이 변경되었는지 여부에 관한 검증식으로 표현되고, 검증식은 공개 파라미터에 포함된 해시 함수 중 적어도 하나를 이용할 수 있다.

[0073] 인증서 기반 프록시 재암호화 방법은, 재암호화 단계 이후에, 공개 파라미터, 제2 사용자의 인증서 및 제2 사용자의 공개키에 대응하는 개인키를 입력값으로 하여 재암호문을 복호화하여 평문을 출력하는 재암호문 복호화 단계(S260)를 더 포함하여 구성될 수 있다. 재암호문 복호화 단계(S260)는 재암호문이 제2 사용자의 공개키 및 인증서에 관한 검증식 조건을 충족하는 경우에만 재암호문을 복호화하여 평문을 출력할 수 있다.

[0074] 인증서 기반 프록시 재암호화 방법은, 암호화 단계(S235) 이후에, 공개 파라미터, 제1 사용자의 인증서 및 제1 사용자의 공개키에 대응하는 개인키를 입력값으로 하여 암호문을 복호화하여 평문을 출력하는 암호문 복호화 단계(S265)를 더 포함하여 구성될 수 있고, 암호문 복호화 단계(S265)는 암호문이 제1 사용자의 공개키 및 인증서에 관한 검증식 조건을 충족하는 경우에만 암호문을 복호화하여 평문을 출력할 수 있다.

[0075] ① 초기화 단계(S205)

[0076] 초기화 단계(S205)는 인증 센터가 시스템 마스터키 mk와 공개파라미터 params를 생성하는 단계이다. 이를 위하여, 보안 매개변수 k와 k_0를 입력 값으로 k비트 소수 q를 선택하고, 상기 위수 q를 갖는 군 G, G_T과 겹선형 페어링 e: $G\times G\rightarrow G_T$을 생성한 후 임의의 생성자 g,h∈G을 선택할 수 있다. 그리고 시스템 마스터키로 임의의 $s\in Z_q^*$를 선택하고 시스템 공개키 $g_1=g^s\in G$를 계산할 수 있다. 그리고 암호학적 해시 함수들 H_1: $\{0,1\}^*\rightarrow G$, H_2: $\{0,1\}^*\rightarrow G$, H_3: $\{0,1\}^{n+k0}\rightarrow Z_q^*$, H_4: $G_T^2\rightarrow\{0,1\}^{n+k0}$, H_5: $\{0,1\}^*\rightarrow G$, H_6: $\{0,1\}^*\rightarrow G$ 을 선택할 수 있다.

[0077] 즉, 시스템 마스터키는 mk=s로 정의되고 공개파라미터는 params={G, G_T, e, g, h, g_1, H_1, H_2, H_3, H_4, H_5, H_6}로 정의할 수 있다.

[0078] ② 키 생성 단계(S215)

[0079] 키 생성 단계(S215)에서는 공개파라미터 params를 입력 값으로, 사용자 A가 임의의 $x_A\in Z_q^*$를 선택하여 자신의

개인키 sk_A로 설정하고 이에 대응하는 공개키로 $pk_A=g^{xA}\in G$을 생성하여 출력할 수 있다.

[0080] ③ 인증서 생성 단계(S225)

[0081] 인증서 생성 단계에서는 공개파라미터 params, 마스터키 s와 사용자 A의 신원정보 λ_A, 공개키 pk_A를 입력 값으로, 인증 센터 측에서 $h_A=H_1(g_1 \| \lambda_A \| pk_A)$를 계산한 후 사용자의 인증서 $Cert_A=h_A^S\in G$를 생성하여 출력할 수 있다.

[0082] ④ 암호화 단계(S235)

[0083] 암호화 단계(S235)에서는 임의의 사용자가 메시지 m에 대해 암호화를 수행하고자 하는 경우 사용자는 다음과 같은 단계를 수행한 후 암호문 C를 출력할 수 있다. 메시지 m, 공개파라미터 params와 사용자 A의 신원정보 λ_A, 공개키 pk_A를 입력 값으로, $h_A=H_1(g_1 \| \lambda_A \| pk_A)$와 $h_A'=H_2(\lambda_A \| pk_A)$를 계산한 후, 임의의 $\sigma\in\{0,1\}^{k0}$를 선택하고 $r=H_3(m \| \sigma)\in Z_q^*$을 계산할 수 있다. 이후 $C_1=g^r$, $C_2=h^r$, $C_3=(m \| \sigma)\oplus H_4(e(g_1,h_A)^r \| e(pk_A,h_A')^r)$, $C_4=u^r$을 생성하⑥고 암호문으로 $C=(C_1,C_2,C_3,C_4)$를 설정하고 출력할 수 있다. 암호문에서 u는 $H_5(C_1 \| C_2 \| C_3)$의 수행결과로써 후술할 재암호화 단계(S250)에서 암호문의 유효성을 검증하기 위하여 사용될 수 있다.

[0084] ⑤ 재암호화키 생성 단계(S240)

[0085] 재암호화키 생성 단계(S240)에서는 복호화 권한 위임자인 A가 다음과 같은 단계를 수행한 후 단방향 재암호화키 $rk_{A\to B}$를 생성하여 출력할 수 있다. 공개파라미터 params와 복호화 권한 수임자 B의 신원정보 λ_B, 공개키 pk_B와 권한 위임자 A의 인증서 $Cert_A$, 개인키 sk_A를 입력 값으로, $h_B=H_1(g_1 \| \lambda_B \| pk_B)$와 $h_B'=H_2(\lambda_B \| pk_B)$를 계산한 후 임의의 $t\in Z_q^*$를 선택할 수 있다. 이후 $rk_{A\to B}^{(1)}=h^t \cdot H_6(e(g_1,h_B)^t)\cdot Cert_A$, $rk_{A\to B}^{(2)}=h^t \cdot H_6(e(pk_B,h_B')^t)\cdot h_A'^{xA}$, $rk_{A\to B}^{(3)}=g^t$을 생성하고 단방향 재암호화키로 $rk_{A\to B}=(rk_{A\to B}^{(1)},rk_{A\to B}^{(2)},rk_{A\to B}^{(3)})$을 설정하고 출력할 수 있다.

[0086] 재암호화키는 복호화 권한 수임자(사용자 B)와 프록시의 공모를 통하여 권한 위임자 (사용자 A)의 개인키 정보를 유출하는 공모 공격에 안전성을 보장하기 위하여 ElGamal 암호 기술이 적용된 단방향 재암호화키로 생성되며, 재암호화키를 생성하기 위하여 권한 위임자와 프록시간의 비밀정보의 전송이 필요하지 않는 것을 특징으로 한다.

[0087] ⑥ 재암호화 단계(S250)

[0088] 재암호화 단계(S250)에서는 프록시가 권한 위임자 A에 대한 암호문 C를 다음과 같은 단계를 수행한 후 권한 수임자 B에 대한 재암호문 C'을 생성하여 출력할 수 있다. 공개파라미터 params, 재암호화키 $rk_{A\to B}$와 권한 위임자 A에 대한 암호문 $C=(C_1,C_2,C_3,C_4)$를 입력 값으로, 먼저 $u=H_5(C_1 \| C_2 \| C_3)$을 계산한 후 아래와 같은 검증식 1과 2를 통하여 입력된 암호문의 유효성을 검증할 수 있다.

[0089] [검증식 1]

[0090] $$e(C_1, u)=e(g,C_4)$$

[0091] [검증식 2]

[0092] $$e(C_2, u)=e(h,C_4)$$

[0093] 검증식 1과 2가 성립하면 $C_1'=rk_{A\to B}^{(3)}$을 설정하고 $C_2'=e(C_1,rk_{A\to B}^{(1)})/e(C_2,rk_{A\to B}^{(3)})$와 $C_2''=e(C_1,rk_{A\to B}^{(2)})/e(C_2,rk_{A\to B}^{(3)})$을 계산할 수 있다. 이후 재암호문으로 $C'=(C_1,C_1',C_2',C_2'',C_3)$을 설정하고 출력할 수 있다. 검증식 1과 2를 통하여 공격자에 의한 임의의 암호문 변경을 통한 악의적인 공격을 예방할 수 있다.

[0094] ⑦ 복호화 단계(S260, S265)

[0095] 복호화 단계는 재암호화되지 않은 암호문 C에 대한 암호문 복호화 단계(S265)와 재암호문 C'에 대한 재암호문 복호화 단계(S260)로 구성될 수 있다. 재암호화되지 않은 암호문 C를 복호화하기 위해서 사용자 A는 다음과 같은 단계를 수행한 후 상기 메시지 m을 출력할 수 있다.

[0096] 먼저 $h_A'=H_2(\lambda_A \| pk_A)$와 $w=e(C_1,Cert_A) \| e(C_1,h_A')^{xA}$를 계산한 후, $(m \| \sigma)=C_3 \oplus H_4(w)$를 계산할 수 있다. 이후 아래와 같은 검증식 3과 4를 통하여 암호문의 유효성을 검증할 수 있다.

[0097] [검증식 3]

[0098] $$C_1 = g^r$$

[0099] [검증식 4]

[0100] $$C_2 = h^r$$

[0101] 검증식 3과 4에서 r은 $r=H_3(m \| \sigma)$의 수행 결과이다. 검증식 3과 4가 성립하면 메시지 m을 출력할 수 있다. 검증식 3과 4를 통하여 본 발명은 공격자에 의한 임의의 암호문 변경을 통한 악의적인 공격을 예방할 수 있다. 암호문 복호화 단계의 올바름의 증명은 다음과 같은 검증식 5에 의하여 증명되어질 수 있다.

[0102] [검증식 5]

[0103] $$\begin{aligned} e(C_1, Cert_A) \| e(C_1, h_A')^{x_A} &= e(g^r, h_A^s) \| e(g^r, h_A')^{x_A} \\ &= e(g^s, h_A)^r \| e(g^{x_A}, h_A')^r \\ &= e(g_1, h_A)^r \| e(pk_A, h_A')^r \end{aligned}$$

[0104] 재암호문 C'를 복호화하기 위해서 권한 수임자 B는 다음과 같은 단계를 수행한 후 메시지 m을 출력할 수 있다. 먼저 $h_B'=H_2(\lambda_B \| pk_B)$를 계산하고 $w_1=C_2'/e(C_1,H_6(e(C_1',Cert_B)))$와 $w_2=C_2''/e(C_1,H_6(e(C_1',h_B')^{xB}))$를 계산한 후, $(m \| \sigma)=C_3 \oplus H_4(w_1 \| w_2)$을 계산할 수 있다. 이후 아래와 같은 검증식 6을 통하여 재암호문의 유효성을 검증할 수 있다.

[0105] [검증식 6]

[0106] $$C_1 = g^r$$

[0107] 검증식 6에서 r은 $r=H_3(m \| \sigma)$의 수행결과이다. 검증식 6이 성립하면 상기 메시지 m을 출력할 수 있다. 검증식 6을 통하여 본 발명은 공격자에 의한 임의의 암호문 변경을 통한 악의적인 공격을 예방할 수 있다. 재암호문 복호화 단계(S260)의 올바름의 증명은 다음과 같은 검증식 7과 8에 의하여 검증될 수 있다.

[0108] [검증식 7]

[0109] $$\begin{aligned} C_2'/e(C_1, H_6(e(C_1', Cert_B))) &= \frac{e(g^r, H_6(e(g_1, h_B)^t)) \cdot e(g^r, h_A^s)}{e(g^r, H_6(e(g^t, h_B^s))} \\ &= \frac{e(g^r, H_6(e(g^s, h_B)^t)) \cdot e(g^s, h_A)^r}{e(g^r, H_6(e(g^s, h_B)^t))} \\ &= e(g_1, h_A)^r \end{aligned}$$

[0110] [검증식 8]

[0111]
$$C_2''/e(C_1, H_6(e(C_1', h_B')^{x_B})) = \frac{e(g^r, H_6(e(pk_B, h_B')^t)) \cdot e(g^r, h_A'^{x_A})}{e(g^r, H_6(e(g^t, h_B')^{x_B}))} = \frac{e(g^r, H_6(e(g^{x_B}, h_B')^t)) \cdot e(g^{x_A}, h_A')^r}{e(g^r, H_6(e(g^{x_B}, h_B')^t))} = e(pk_A, h_A')^r$$

[0112] 도 3은 본 발명의 일 실시예에 따른 인증서 기반 프록시 재암호화 시스템(10)과 그 세부 구성요소, 제1 사용자 암복호화 장치(300)와 그 세부 구성요소를 설명하기 위한 블록도이다. 도 3을 참조하여 제1 사용자 암복호화 장치(300)를 살펴보면 다음과 같다.

[0113] 제1 사용자 암복호화 장치(300)는, 평문, 제1 사용자의 공개키 및 인증 센터(100)로부터 전달된 공개 파라미터를 입력값으로 하여 유효성 검증 파라미터를 내재한 형태로 암호문을 생성하는 암호화부(320)와, 공개 파라미터, 제1 사용자의 인증서, 제1 사용자의 공개키에 대응하는 개인키 및 제2 사용자의 공개키를 입력값으로 하여 재암호화키를 생성하는 재암호화키 생성부(330)와, 프록시(200)가 재암호문을 생성하도록 재암호화키를 프록시(200)에 전달하는 재암호화키 전달부(350)를 포함하여 구성될 수 있다.

[0114] 재암호화키는 엘가말 암호 방식을 적용한 단방향 재암호화키일 수 있다. 제1 사용자 암복호화 장치(300)는 공개 파라미터, 제1 사용자의 인증서 및 제1 사용자의 공개키에 대응하는 개인키를 입력값으로 하여 암호문을 복호화하여 평문을 출력하는 암호문 복호화부(340)를 더 포함하되, 암호문 복호화부(340)는 암호문이 제1 사용자의 공개키 및 인증서에 관한 검증식 조건을 충족하는 경우에만 암호문을 복호화하여 평문을 출력할 수 있다.

[0115] 제1 사용자 암복호화 장치(300)와 세부 구성요소에 대한 설명은 앞서 설명한 인증서 기반 프록시 재암호화 방법에 대한 설명에서 상술한 바 있으므로 중복하여 기재하지는 않는다. 다만, 제1 사용자 암복호화 장치(300)는 복호화 권한을 위임하고자 하는 사용자, 즉 복호화 권한 위임자의 암복호화 장치를 의미할 수 있다. 이 때, 제1, 제2 등의 용어는 권한 위임자와 권한 수임자의 암복호화 장치를 구분하기 위해 임의로 붙여진 것이다. 따라서 제1 사용자 암복호화 장치(300)와 제2 사용자 암복호화 장치(400)의 구성은 실제로는 동일할 수 있다.

[0116] 도 3을 계속 참조하여 인증서 기반 프록시 재암호화 시스템(10)과 그 세부구성요소를 살펴보면 다음과 같다.

[0117] 인증서 기반 프록시 재암호화 시스템(10)은, 시스템 마스터키를 이용하여 공개 파라미터를 생성하는 초기화부(110)를 구비하고 있는 인증 센터(100)와, 공개 파라미터, 제1 사용자의 인증서, 제1 사용자의 공개키에 대응하는 개인키 및 제2 사용자의 공개키를 입력값으로 하여 재암호화키를 생성하는 재암호화키 생성부(330)를 구비하고 있는 제1 사용자 암복호화 장치(300)와, 암호문에 기반하여 유효성 검증 파라미터를 산출하고, 암호문이 유효성 검증 파라미터에 관한 소정의 조건을 충족함에 따라, 공개 파라미터, 재암호화키 및 암호문을 입력값으로 하여 재암호문을 생성하는 재암호화부(210)를 구비하고 있는 프록시(200)를 포함하여 구성될 수 있다.

[0118] 공개 파라미터는, 겹선형 페어링, 적어도 하나의 해시 함수, 시스템 마스터키를 이용하여 생성된 시스템 공개키를 포함하여 구성될 수 있다.

[0119] 인증 센터(100)는 공개 파라미터, 시스템 마스터키, 사용자의 공개키를 입력값으로 하여 사용자의 인증서를 생성하고, 사용자에게 인증서를 배포하는 인증서 생성부(120)를 더 포함하여 구성될 수 있다.

[0120] 암호문은 유효성 검증 파라미터를 내재한 형태로 생성될 수 있고, 재암호화키는 엘가말 암호 방식을 적용한 단방향 재암호화키일 수 있다.

[0121] 소정의 조건은 암호문이 변경되었는지 여부에 관한 검증식으로 표현되고, 검증식은 공개 파라미터에 포함된 해시 함수 중 적어도 하나를 이용할 수 있다.

[0122] 인증서 기반 프록시 재암호화 시스템(10)은, 공개 파라미터, 제2 사용자의 인증서 및 제2 사용자의 공개키에 대응하는 개인키를 입력값으로 하여 재암호문을 복호화하여 평문을 출력하는 재암호문 복호화부(340)를 구비하고 있는 제2 사용자 암복호화 장치(400)를 더 포함하되, 재암호문 복호화부(340)는 재암호문이 제2 사용자의 공개

키 및 인증서에 관한 검증식 조건을 충족하는 경우에만 재암호문을 복호화하여 평문을 출력할 수 있다.

[0123] 인증서 기반 프록시 재암호화 시스템(10)과 세부 구성요소에 대한 설명은 앞서 설명한 인증서 기반 프록시 재암호화 방법에 대한 설명에서 상술한 바 있으므로 중복하여 기재하지는 않는다. 다만, 인증서 기반 프록시 재암호화 시스템(10)과 그 구성요소들은 논리적으로 구분 가능한 요소일 뿐, 물리적인 위치가 반드시 서로 다름을 의미하지는 않는다. 즉, 예를 들면, 프록시(200)는 데이터 센터 내의 코어망에 위치하는 것이 일반적인 구성이지만, 사용자의 암복호화 장치를 포함하는 컴퓨팅 장치 내에 존재하는 것도 가능한 구성이다.

[0124] 비록 몇몇의 측면들은 방법의 관점에서 설명되었지만, 이러한 측면들은 상응하는 장치의 설명을 나타내는 것이 명확하며, 여기서 방법의 단계는 장치에 대응한다. 특정 구현 요구들에 따르면, 발명의 실시예들은 하드웨어 또는 소프트웨어에서 구현될 수 있다. 본 발명의 실시예들은 프로그램 코드, 방법들 중 하나의 수행을 위해 동작하는 프로그램 코드를 가지는 컴퓨터 프로그램 제품으로서 수행될 수 있다.

[0125] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시 예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시 예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

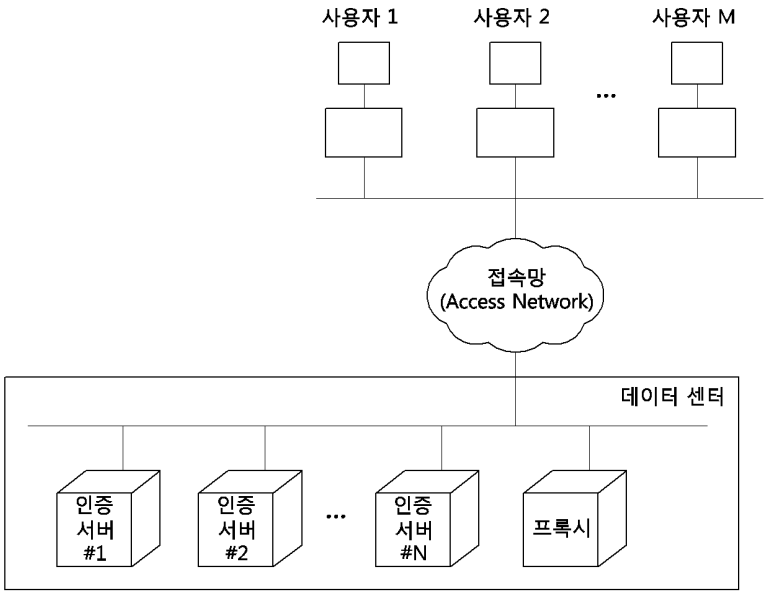
부호의 설명

[0126] 10: 인증서 기반 프록시 재암호화 시스템

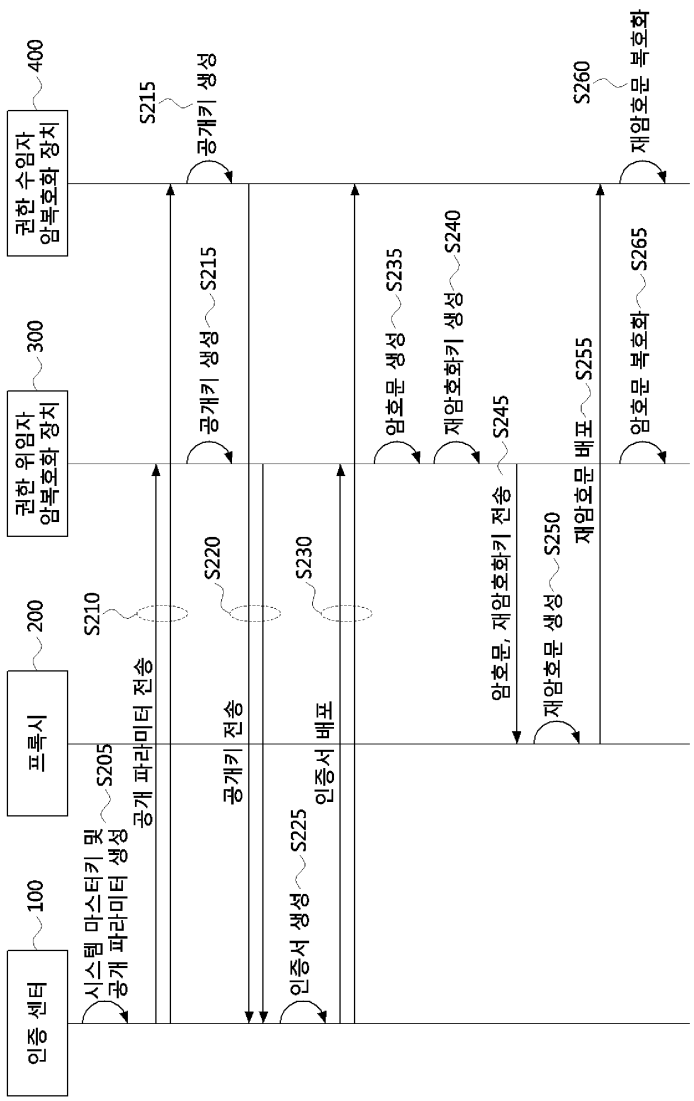
100: 인증 센터	110: 초기화부
120: 인증서 생성부	200: 프록시
210: 재암호화부	300: 제1 사용자 암복호화 장치
310: 키 생성부	320: 암호화부
330: 재암호화키 생성부	340: 암호문 복호화부
350: 재암호화키 전달부	400: 제2 사용자 암복호화 장치
410: 키 생성부	420: 재암호문 복호화부

도면

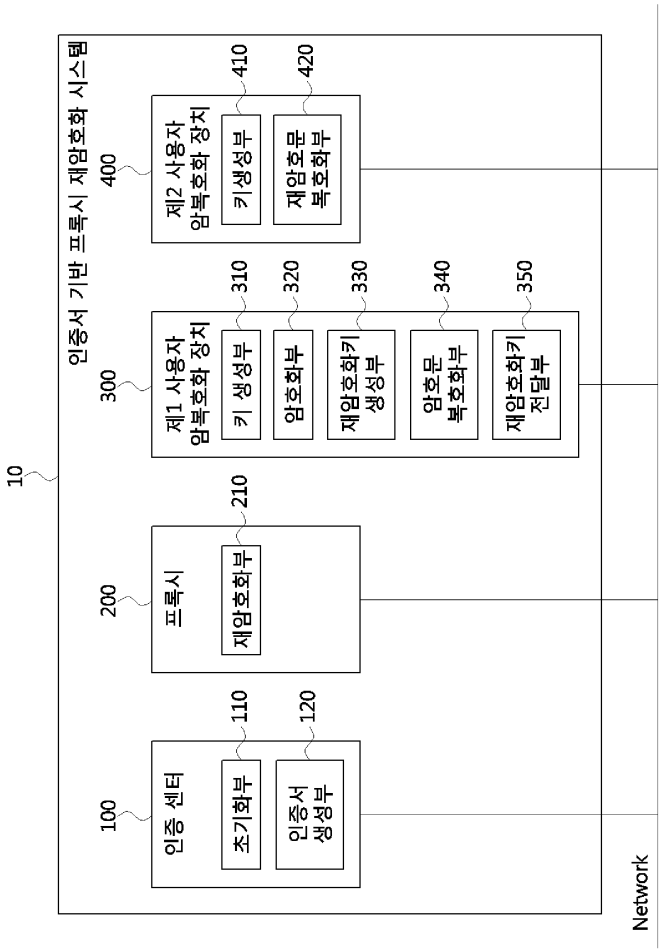
도면1


사용자 1
사용자 2
사용자 M
...
접속망
(Access Network)
데이터 센터
인증
서버
#1
인증
서버
#2
...
인증
서버
#N
프록시

도면2


인증 센터
100
프록시
200
권한 위임자 암복호화 장치
300
권한 수임자 암복호화 장치
400
시스템 마스터키 및 공개 파라미터 생성
S205
공개 파라미터 전송
S210
공개키 생성
S215
공개키 전송
S220
인증서 생성
S225
인증서 배포
S230
공개키 생성
S215
암호문 생성
S235
재암호화키 생성
S240
암호문, 재암호화키 전송
S245
재암호문 생성
S250
재암호문 배포
S255
암호문 복호화
S265
재암호문 복호화
S260

도면3



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 20

【변경전】

출력는

【변경후】

출력하는