(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0053801
(43) 공개일자 2017년05월17일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01) *H04L 9/30* (2006.01)
(52) CPC특허분류
H04L 9/14 (2013.01)
H04L 9/30 (2013.01)
(21) 출원번호 10-2015-0155981
(22) 출원일자 2015년11월06일
심사청구일자 2015년11월06일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
김효승
서울특별시 성북구 안암로9가길 56 206호 (안암동5가)
(74) 대리인
김등용, 김홍석

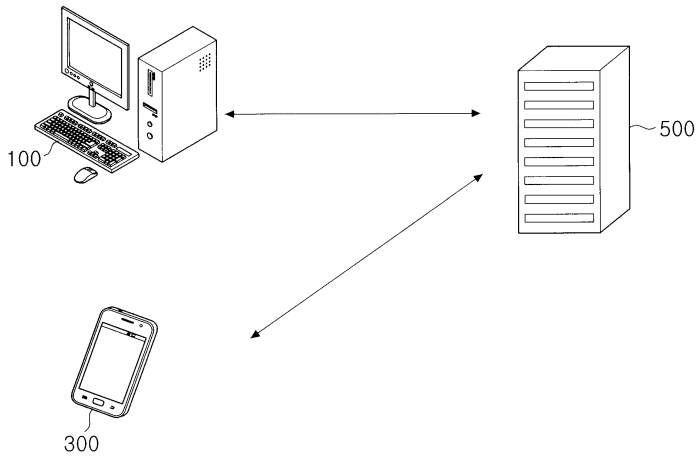
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 **암호 시스템 및 방법**

(57) 요 약

암호화 방법이 개시된다. 상기 암호화 방법은 수신 단말기에서 수행되고, 비밀키를 설정하는 단계, 상기 비밀키를 이용하여 공개키를 생성하는 단계, 및 서버로부터 수신된 부분 비밀키와 상기 비밀키를 이용하여 복호화키를 생성하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3066 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 R01261510900001002
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신방송연구개발사업
연구과제명 계층적 식별자를 가진 인터넷 개체의 공개키 인증 구조 연구
기 여 율 1/1
주관기관 고려대학교
연구기간 2015.03.01 ~ 2016.02.29

명 세 서

청구범위

청구항 1

수신 단말기에서 수행되는 암호화 방법에 있어서,

비밀키(sk_{ID})를 설정하는 단계;

상기 비밀키(sk_{ID})를 이용하여 공개키(pk_{ID})를 생성하는 단계; 및

서버로부터 수신된 부분 비밀키(psk_{ID})와 상기 비밀키(sk_{ID})를 이용하여 복호화키(dk_{ID})를 생성하는 단계를 포함하는,

암호화 방법.

청구항 2

제1항에 있어서,

상기 비밀키(sk_{ID})를 설정하는 단계는,

선택된 임의의 값($x \in Z_p^*$)을 상기 비밀키($sk_{ID} = x_{ID}$)로 설정하는,

암호화 방법.

청구항 3

제2항에 있어서,

상기 공개키(pk_{ID})는 수학식에 의해 결정되고,

상기 수학식은 $pk_{ID} = g^{x_{ID}}$ 이고,

상기 g 는 소수(p)를 위수로 갖는 곱셈군(G)의 생성원인,

암호화 방법.

청구항 4

제1항에 있어서,

상기 공개키(pk_{ID})를 이용하여 송신 단말기에 의해 암호화된 암호문(CT)을 상기 송신 단말기로부터 수신하고, 상기 복호화키(dk_{ID})를 이용하여 상기 암호문(pk_{ID})을 복호화하는 단계를 더 포함하는,

암호화 방법.

청구항 5

비밀키(sk_{ID})를 설정하는 비밀키 생성부;

상기 비밀키(sk_{ID})를 이용하여 공개키(pk_{ID})를 생성하는 공개키 생성부; 및

서버로부터 수신된 부분 비밀키(psk_{ID})와 상기 비밀키(sk_{ID})를 이용하여 복호화키(dk_{ID})를 생성하는 복호화키 생성부를 포함하는 수신 단말기.

청구항 6

제5항에 있어서,

상기 비밀키 생성부는

선택된 임의의 값($x \in Z_p^*$)을 상기 비밀키($sk_{ID} = x_{ID}$)로 설정하는,

수신 단말기.

청구항 7

제6항에 있어서,

상기 공개키(pk_{ID})는 수학식에 의해 결정되고,

상기 수학식은 $pk_{ID} = g^{x_{ID}}$ 이고,

상기 g 는 소수(p)를 위수로 갖는 곱셈군(G)의 생성원인,

수신 단말기.

청구항 8

제5항에 있어서,

상기 공개키(pk_{ID})를 이용하여 송신 단말기에 의해 암호화된 암호문(CT)을 상기 송신 단말기로부터 수신하고, 상기 복호화키(dk_{ID})를 이용하여 상기 암호문(pk_{ID})을 복호화하는 복호화부를 더 포함하는,

수신 단말기.

청구항 9

제5항 내지 제8항 중 어느 하나의 항에 기재된 상기 수신 단말기;

상기 송신 단말기; 및

상기 서버를 포함하는 암호 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 암호 시스템 및 방법에 관한 것으로, 특히 인증서 없이 효율적으로 데이터를 암호화할 수 있는 암호 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 현재 널리 사용하는 PKI(Public-Key Infrastructure)에서는 사용자 장치 내에서 공개키와 비밀키 쌍이

생성된다. 이러한 키 쌍은 임의의 난수로 구성되어 있기 때문에 신뢰기관에서 발행하는 인증서(certificate)를 통하여 신원 정보와 난수를 결합(binding)시킨다. 하지만, 인증서를 이용할 경우, 인증서 소유자는 주기적으로 인증서를 갱신해야 하고 검증자는 인증서 폐기 리스트(Certificate Revocation List)를 체크하여 상대방의 공개키가 정당한지 검증하는 과정을 수행하여야 한다. 이는 암/복호화 알고리즘의 효율성과는 별개로 부가적인 페이로드를 송/수신자 모두에게 발생시킨다.

[0003] 인증서의 문제를 해결하고자 ID 기반 암호(ID-based Encryption) 시스템이 제안되었다. ID 기반 암호 시스템은 학번, 메일주소, 전화번호와 같이 사용자를 특정 지을 수 있는 고유 ID를 직접 공개키로 사용하므로 별도의 공개키 인증 과정이 필요하지 않는다. 인증서가 없으므로 사용자 키 쌍을 직접 생성하는 PKI와 달리 사용자는 ID의 소유권을 키 생성 기관(Key Generation Center)에게 인증받은 후 ID에 대응하는 비밀키를 전달받는 과정을 수행하는데, 이 과정에서 키 생성 기관이 모든 사용자들의 개인키를 알게 되는 막강한 권한을 가지게 된다.

[0004] 2003년, 신뢰기관의 권한이 다소 약한 PKI와 인증서를 사용하지 않는 ID 기반 암호 시스템의 장점을 융합한 무인증서 기반 암호(Certificateless-based Encryption)가 제안되었다. 무인증서 기반 암호 시스템은 ID 기반 암호 시스템과 같이 키 생성 기관을 시스템 구성에 포함하고 있으나, PKI처럼 사용자가 직접 생성하는 키 쌍이 존재하기 때문에 이 값을 모르는 키 생성 기관은 사용자 ID에 대한 암호문을 복호화할 수 없다. 최근까지 학계에서 무인증서 기반 암호에 대한 연구가 활발히 진행되고 있으나, 다음과 같은 이유로 인하여 상용화 단계에 도달하지 못하고 있다.

[0005] 일반적으로 무인증서 기반 암호는 겹선형 함수(bilinear map)를 이용한 ID 기반 암호 설계 방법과 동일한 방법을 이용한다. 즉, 대부분의 무인증서 기반 암호 기법은 ID 기반 암호의 비밀키 구조와 매우 유사하다. 이때, 겹선형 함수 연산은 일반 지수 연산보다 최소 10배 최대 50배 정도 느려 하드웨어 성능 제약사항이 있는 디바이스에서 연산하기 부담스럽다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 공개특허공보 제10-2011-0035573호(2011.04.06.)

발명의 내용

해결하려는 과제

[0007] 본 발명이 이루고자 하는 기술적인 과제는 인증서 없이 효율적으로 데이터를 암호화하는 방법과 키 생성 기관의 권한을 제한할 수 있는 암호 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0008] 본 발명의 일 실시 예에 따른 암호화 방법은 수신 단말기에서 수행되고, 비밀키를 설정하는 단계, 상기 비밀키를 이용하여 공개키를 생성하는 단계, 및 서버로부터 수신된 부분 비밀키와 상기 비밀키를 이용하여 복호화키를 생성하는 단계를 포함한다.

[0009] 또한, 본 발명의 일 실시 예에 따른 수신 단말기는 비밀키를 설정하는 비밀키 생성부, 상기 비밀키를 이용하여 공개키를 생성하는 공개키 생성부, 및 서버로부터 수신된 부분 비밀키와 상기 비밀키를 이용하여 복호화키를 생성하는 복호화키 생성부를 포함한다.

[0010] 또한, 본 발명의 일 실시 예에 따른 암호 시스템은 상기 수신 단말기, 상기 송신 단말기, 및 상기 서버를 포함한다.

발명의 효과

[0011] 본 발명의 실시 예에 따른 암호 시스템 및 방법에 의할 경우, 인증서를 사용하지 않음으로써 인증서 저장, 관리, 폐기 등으로부터 발생하는 문제를 근본적으로 해결할 수 있다.

[0012] 또한, 키 생성 기관은 ID에 대응하는 부분 비밀키만 생성하므로 암호문으로부터 어떠한 정보도 얻을 수 없으며,

결과적으로 사용자 프라이버시를 보호할 수 있다.

[0013] 또한, 겹선형 함수 없이 일반 곱셈 순환군(multiplicative cyclic group)을 이용하여 기법을 설계하여 타원곡선군(eliptic curve group)을 이용할 경우, 구현시 성능을 향상시킬 수 있다.

도면의 간단한 설명

[0014] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 따른 암호 시스템을 도시한다.

도 2는 도 1에 도시된 서버의 기능 블럭도이다.

도 3은 도 1에 도시된 제1 단말기의 기능 블럭도이다.

도 4는 도 1에 도시된 암호 시스템을 이용한 암호화 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0015] 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.

[0016] 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.

[0017] 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.

[0018] 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.

[0019] 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.

[0020] 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.

[0021] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0023] 도 1은 본 발명의 일 실시 예에 따른 암호 시스템을 도시한다.

[0024] 도 1을 참조하면, 암호 시스템(10)은 제1 단말기(100), 제2 단말기(300) 및 서버(500)를 포함한다.

[0025] 키 생성 기관 또는 키 생성 서버로 명명될 수도 있는 서버(500)는 공개 파라미터(pp)와 마스터키(msk)를 생성하고, 생성된 공개 파라미터(pp)를 공개할 수 있다. 또한, 서버(500)는 사용자의 ID에 대한 부분 비밀키(psk_{ID})를 생성하고, 생성된 부분 비밀키(psk_{ID})를 대응되는 단말기로 송신할 수 있다.

[0026] 제1 단말기(100) 또는 제2 단말기(300)는 서버(500)로부터 수신된 부분 비밀키(psk_{ID})와 자신의 비밀키(sk_{ID})를 이용하여 공개키(pk_{ID})와 복호화키(dk_{ID})를 생성할 수 있다. 이때 생성된 공개키(pk_{ID})는 공개될 수 있다.

[0027] 제1 단말기(100) 및/또는 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.

[0028] 또한, 겹선형 함수($e: G_1 \times G_1 \rightarrow G_2$)란 겹선형 성질($e(g_1^a, g_1^b) = e(g_1^b, g_1^a) = e(g_1, g_1)^{ab} = g_2^{ab}$)을 만족하는 함수를 의미한다. Super Singular 곡선(SS-curve)를 이용하여 겹선형 함수를 구현할 경우 $e(g_1^a, g_1^b) = g_2^{ab}$ 를 계산하는 시간은 일반 지수 연산 $g_1 \wedge \{a\} = g_1^a$ 를 계산하는 시간보다 10배 ~ 50배 정도 느리다(Xavier Boyen, "A tapestry of Identity-based encryption: practical frameworks compared", 2008). 따라서, 본 발명에서는 겹선형 함수 없이 일반 곱셈 순환군(multiplicative cyclic group)을 이용하여 기법을 설계하여 타원곡선 군(elliptic curve group)을 이용할 경우, 구현 시 매우 효율적인 성능 평가를 기대할 수 있다.

[0029] 이하에서, 제1 단말기(100)는 제1 단말기(100)의 공개키(pk_{ID})를 이용하여 암호화된 암호문(CT)을 수신하고, 암호문(CT)을 복호화하는 수신 단말기로, 제2 단말기(300)는 제1 단말기(100)의 공개키(pk_{ID})를 이용하여 메시지(m)를 암호화하여 암호문(CT)을 생성한 후 제1 단말기(100)로 송신하는 송신 단말기로 가정한다.

[0031] 도 2는 도 1에 도시된 서버의 기능 블럭도이다.

[0032] 도 1과 도 2를 참조하면, 서버(500)는 셋업부(510)와 비밀키 생성부(530)를 포함한다.

[0033] 셋업부(510)는 셋업 알고리즘($pp, msk \leftarrow Setup(\lambda)$)을 수행하여 공개 파라미터(pp)와 마스터키(msk)를 생성하고, 공개 파라미터(pp)를 공개할 수 있다. 실시 예에 따라, 공개 파라미터(pp)는 유무선 통신망을 통하여 제1 단말기(100) 및/또는 제2 단말기(300)로 송신될 수도 있다.

[0034] 구체적으로, 셋업부(510)는 안전성 파라미터(λ)에 상응하는 소수(p)를 선택하고, 위수를 p 로 갖는 곱셈군(G)을 선택한다. 또한, 셋업부(510)는 (k+1) 개의 임의의 값($\{x_i\}_{i=0}^{k-1},\ y \in Z_p^*$)을 선택한 후 $\{x_i\}_{i=0}^{k-1},\ y \in Z_p^*$ 를 계산한다. 이때, g 는 곱셈군(G)의 생성원을 의미할 수 있다. 또한, 셋업부(510)는 임의의 길이의 문자열을 입력받아 k-비트의 바이너리 문자열을 출력하는 암호학적 해쉬함수

($H: \{0,1\}^* \rightarrow \{0,1\}^k$)를 선택한다. 선택된 값들과 계산된 값들을 이용하여 생성된 공개 파라미터(pp)와 마스터키(msk)는 다음과 같다.

[0035] $$pp = \left(g, g^{x_0}, g^{x_1}, \ldots, g^{x_{k-1}}, g^{y}, H\right),\ msk = \left(x_0, x_1, \ldots, x_{k-1}, y\right)$$

[0037] 비밀키 생성부(530)는 부분 비밀키 생성 알고리즘($psk_{ID} \leftarrow Partial-Private-Key-Extract(msk, ID)$)을 수행하여 부분 비밀키(psk_{ID})를 생성하고 생성된 부분 비밀키(psk_{ID})를 제1 단말기(100)로 송신할 수 있다.

[0038] 구체적으로, 비밀키 생성부(530)는 인증된 사용자의 ID에 대한 부분 비밀키를 생성하기 위하여 $H(ID)$를 계산한다. $H(ID) = h_0 h_1 \cdots h_{k-1} \quad (h_i \in \{0,1\})$ 이라 할 때, 비밀키 생성부(530)는 임의의 난수인 비밀키 태그값($tag_{ID} \in Z_p^*$)을 선택한 뒤, ID에 대한 부분 비밀키($psk_{ID} = (psk_{ID,0}, psk_{ID,1})$)를 생성한다. 부분 비밀키(psk_{ID})의 각 구성 요소는 다음과 같다.

[0039] $$psk_{ID,0} = x_0 h_0 + x_1 h_1 ID + x_2 h_2 ID^2 + \cdots + x_{k-1} h_{k-1} ID^{k-1} + y tag_{ID}$$

[0040] $$psk_{ID,1} = tag_{ID}$$

[0042] 도 3은 도 1에 도시된 제1 단말기의 기능 블럭도이다.

[0043] 도 1 내지 도 3을 참조하면, 제1 단말기(100)는 비밀키 생성부(110), 공개키 생성부(130), 복호화키 생성부(150) 및 복호화부(190)를 포함한다. 실시 예에 따라 제1 단말기(100)는 암호화부(170)를 더 포함할 수 있다.

[0044] 비밀키 생성부(110)는 비밀키 생성 알고리즘($sk_{ID} \leftarrow Set-Secret-Key(pp, ID)$)을 수행하여 제1 단말기(100)만의 독립적인 비밀키(sk_{ID})를 생성할 수 있다.

[0045] 구체적으로, 비밀키 생성부(110)는 임의의 값($x \in Z_p^*$)을 선택한 후, 서버(500)로부터 수신된 부분 비밀키(psk_{ID})와는 독립적인 자신의 비밀키($sk_{ID} = x_{ID}$)를 생성(또는 설정)할 수 있다.

[0047] 공개키 생성부(130)는 공개키 생성 알고리즘($pk_{ID} \leftarrow Set-Secret-Key(pp, sk_{ID})$)을 수행하여 공개키(pk_{ID})를 생성(또는 설정)하고, 생성된 공개키(pk_{ID})를 공개할 수 있다.

[0048] 구체적으로, 공개키 생성부(130)는 자신의 비밀키인 비밀값(sk_{ID})를 이용하여 공개키($pk_{ID} = g^{x_{ID}}$)를 생성할 수 있다.

[0050] 복호화키 생성부(150)는 복호화키 생성 알고리즘

($dk_{ID} \leftarrow Set-Decrypt-Key(psk_{ID}, sk_{ID})$)을 수행하여 복호화키($dk_{ID}$)를 생성(또는 설정)할 수 있다.

[0051] 구체적으로, 복호화키 생성부(150)는 부분 비밀키(psk_{ID})와 비밀키(sk_{ID})를 이용하여 복호화키($dk_{ID} = (dk_{ID,0}, dk_{ID,1})$)를 생성할 수 있다. 복호화키($dk_{ID}$)의 각 구성 요소는 아래와 같다.

[0052] $$dk_{ID,0} = psk_{ID,0} + sk_{ID}$$

[0053] $$dk_{ID,0} = psk_{ID,0} + sk_{ID}$$

[0054] 실시 예로, $H(ID)$가 4비트 바이너리 문자열을 출력한다고 가정하고($k=4$), $H(ID_1) = 1101$이고 $H(ID_2) = 0011$일 때, ID_1에 대응하는 복호화키(dk_{ID_1})와 ID_2에 대응하는 복호화키(dk_{ID_2})는 다음과 같다.

[0055] $$dk_{ID_1} = (x_{ID_1} + x_0 + x_1 ID_1 + x_3 ID_1^3 + ytag_{ID_1},\ tag_{ID_1})$$

[0056] $$dk_{ID_2} = (x_{ID_2} + x_2 ID_2^2 + x_3 ID_2^3 + ytag_{ID_2},\ tag_{ID_2})$$

[0058] 암호화부(170)는 암호화 알고리즘($CT \leftarrow Enc(pp, ID, pk_{ID}, m)$)을 수행하여 메시지($m$)를 암호화할 수 있다.

[0059] 구체적으로 암호화부(170)는 메시지(m)를 암호화하기 위하여 우선 임의의 난수($s \in Z_p^*$)와 난수인 암호문 태그값($tag_c \in Z_p^*$)을 선택한다. 또한, 암호화부(170)는 $H(ID) = h_0 h_1 \cdots h_{k-1}$를 계산한 후 공개 파라미터($pp$)와 공개키($sk_{ID}$)를 이용하여 암호문($CT = (CT_0, CT_1, CT_2, CT_3)$)을 생성할 수 있다. 암호문($CT$)의 각 구성 요소는 다음과 같다.

[0060] $$CT_0 = g^s$$

[0061] $$CT_1 = g^{(x_{ID} + x_0 h_0 + x_1 h_1 ID + \cdots + x_{k-1} h_{k-1} ID^{k-1} + ytag_c)s} \quad \left(x_i = \begin{matrix} 0 \text{ if } h_i = 0 \\ 1 \text{ if } h_i = 1 \end{matrix} \right)$$

[0062] $$CT_2 = tag_c$$

[0063] $$CT_3 = g^{ys} m$$

[0064] 실시 예로, $H(ID_3) = 1001$일 때, ID_3에 대응하는 공개키($g^{x_{ID_3}}$)를 이용하여 암호화한 암호문(CT)은 다음과 같다.

[0065] $$CT=(g^{s},g^{s(x_{ID_3}+x_0+x_3ID_3^3+ytag_c)},tag_c,g^{ys}m)$$

[0066] 상기 암호문(CT)을 생성하는 송신자는 자신이 선택한 s, tag_c와 공개 상수(pp)의 원소 g^{x_0}, g^{x_3}, g^{y}, 그리고 사용자 공개키($g^{x_{ID_3}}$)를 이용하여 암호문(CT)의 두 번째 원소를 계산할 수 있다.

[0068] 복호화부(190)는 복호화 알고리즘($m \leftarrow Dec(pp,dk_{ID},CT)$)을 수행하여 암호문($CT$)을 복호화하여 메시지($m$)를 계산할 수 있다.

[0069] 구체적으로, 복호화부(190)는 아래 3 개의 수학식을 순차적으로 연산함으로써 암호문(CT)을 복호화할 수 있다.

[0070] $$c=\frac{CT_1}{CT_0^{dk_{ID,0}}}$$

[0071] $$c'=c^{\frac{1}{CT_2-dk_{ID,1}}}$$

[0072] $$m=CT_3\times c'^{-1}$$

[0074] 복호화 수식에 대한 정확도(correctness)는 아래와 같다.

$$m=g^{ys}m\times\left(\frac{CT_1}{CT_0^{dk_{ID,0}}}\right)^{\frac{-1}{CT_2-dk_{ID,1}}}$$

$$=g^{ys}m\times\left(\frac{g^{(x_{ID}+x_0h_0+x_1h_1ID+\cdots+x_{k-1}h_{k-1}ID^{k-1}+ytag_c)s}}{g^{s(x_0h_0+x_1h_1ID+\cdots+x_{k-1}h_{k-1}ID^{k-1}+ytag_{ID}+x_{ID})}}\right)^{\frac{-1}{tag_c-tag_{ID}}}$$

$$=g^{ys}m\times g^{ys(tag_c-tag_{ID})\times\frac{-1}{tag_c-tag_{ID}}}$$

$$=g^{ys}m\times g^{-ys}$$

[0075]

[0076] 만약, $tag_c=tag_{ID}$ 이면, 복호화가 불가능하다. 하지만, 각각이 임의의 난수인 tag_c와 tag_{ID}가 같은 값이 될 확률은 $\frac{1}{|Z_p^*|}$ 이므로, 안전성 파라미터(λ)에 의하여 충분한 p가 선택된다면 거의 0에 가까운 의미 없는(negligible) 값이 된다.

[0077] 제2 단말기(300)의 구성 및 기능은 제1 단말기(100)의 구성 및 기능과 동일할 수 있으므로 이에 관한 상세한 설

명은 생략하기로 한다.

[0079] 도 2와 도 3에 도시된 서버(500)의 구성들 각각과 제1 단말기(100)의 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.

[0080] 또한, 본 명세서에서 "~부"라 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.

[0082] 도 4는 도 1에 도시된 암호 시스템을 이용한 암호화 방법을 설명하기 위한 흐름도이다.

[0083] 도 1 내지 도 4를 참조하면, 서버(500)의 셋업부(510)는 공개 파라미터(pp)와 마스터키(msk)를 생성할 수 있다(S100). 생성된 공개 파라미터(pp)는 셋업부(510)에 의해 공개될 수 있다.

[0084] S200 단계에서, 서버(500)의 비밀키 생성부(530)는 사용자의 ID에 대한 부분 비밀키(psk_{ID})를 생성하고, 생성된 부분 비밀키(psk_{ID})를 상기 사용자의 단말기, 예컨대 제1 단말기(100)로 송신한다.

[0085] 서버(500)로부터 부분 비밀키(psk_{ID})를 수신한 제1 단말기(100)는 자신의 비밀키(sk_{ID})와 공개키(pk_{ID})를 생성하고, 생성된 공개키(pk_{ID})를 공개할 수 있다. 이때 제1 단말기(100)는 암호문(CT)을 수신하는 수신 단말기를 의미할 수 있다.

[0086] 또한, 제1 단말기(100)는 부분 비밀키(psk_{ID})와 비밀키(sk_{ID})를 이용하여 복호화키(dk_{ID})를 생성할 수 있다(S400).

[0087] S500 단계에서, 제2 단말기(300)는 제1 단말기(100)의 공개키(pk_{ID})를 이용하여 메시지(m)를 암호화하여 암호문(CT)을 생성하고, 생성된 암호문(CT)을 제1 단말기(100)로 송신할 수 있다. 이때, 제2 단말기(300)는 암호문(CT)을 송신하는 송신 단말기를 의미할 수 있다.

[0088] 암호문(CT)을 수신한 수신 단말기인 제1 단말기(100)는 복호화키(dk_{ID})를 이용하여 암호문(CT)을 복호화할 수 있다(S600).

[0089] 상술된 암호화 방법에서 단계 S400과 단계 S500은 수행 주체가 상이한 단계로서, 그 순서가 반드시 정해진 것은 아니며 실시 예에 따라 수행 순서가 달리 진행될 수도 있다.

[0091] 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

[0092] 10 : 암호 시스템

100 : 제1 단말기

110 : 비밀키 생성부

130 : 공개키 생성부

150 : 복호화키 생성부

170 : 암호화부

190 : 복호화부

300 : 제2 단말기

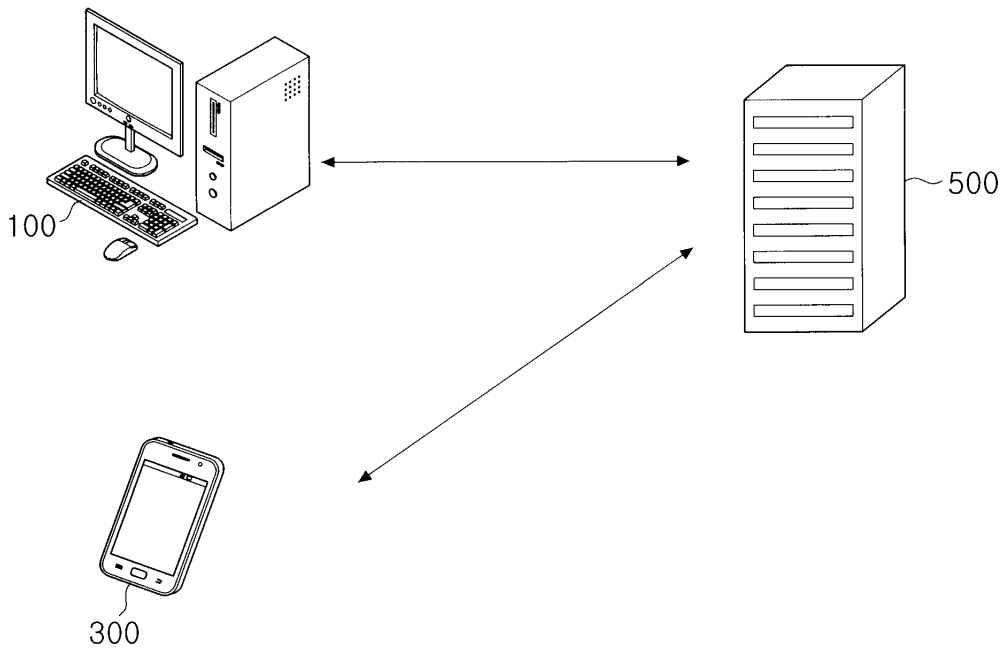
500 : 서버

510 : 셋업부

530 : 비밀키 생성부

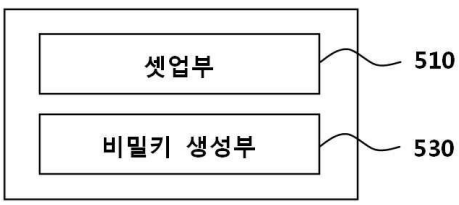
도면

도면1



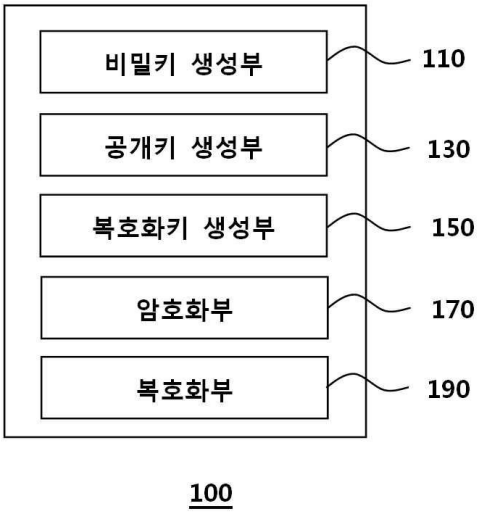
10

도면2

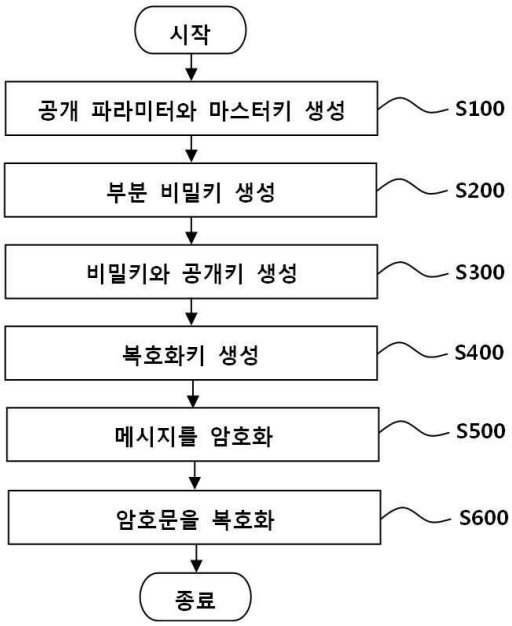


500

도면3


비밀키 생성부
110
공개키 생성부
130
복호화키 생성부
150
암호화부
170
복호화부
190
100

도면4


시작
공개 파라미터와 마스터키 생성
S100
부분 비밀키 생성
S200
비밀키와 공개키 생성
S300
복호화키 생성
S400
메시지를 암호화
S500
암호문을 복호화
S600
종료