(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0087120
(43) 공개일자 2017년07월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 9/08* (2006.01)
H04L 9/14 (2006.01)
(52) CPC특허분류
H04L 9/30 (2013.01)
H04L 9/0869 (2013.01)
(21) 출원번호 10-2016-0006629
(22) 출원일자 2016년01월19일
심사청구일자 2016년01월19일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김송이
서울특별시 서초구 양재대로2길 90 209동 1105호 (우면동,서초힐스아파트)
박승환
서울특별시 동작구 노량진로6마길 8 (노량진동)
이광수
서울특별시 성북구 길음로 119, 221동 902호 (길음동, 길음뉴타운 대우푸르지오아파트)
(74) 대리인
김등용, 김홍석

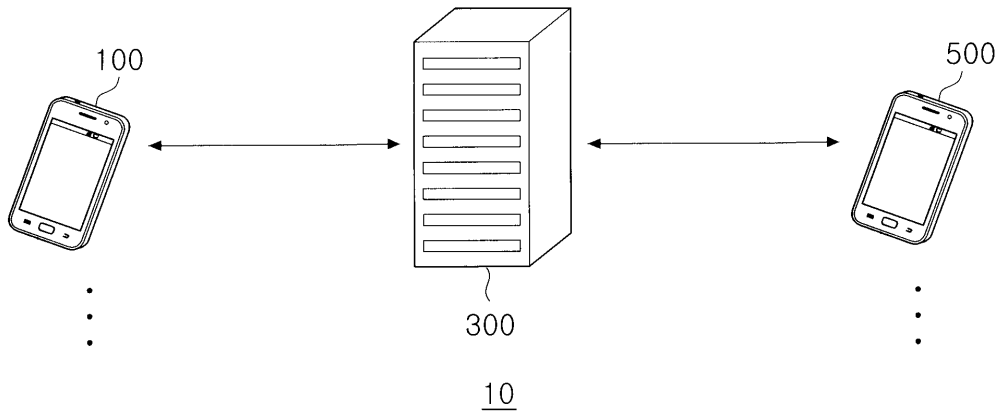
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **무인증서 공개키 암호 시스템 및 수신 단말기**

(57) 요 약

무인증서 공개키 암호 시스템이 개시된다. 상기 무인증서 공개키 암호 시스템은 수신 단말기, 송신 단말기, 및 서버를 포함하고, 상기 서버는 보안 상수를 입력받아 마스터키와 공개 상수를 생성하고, 상기 공개 상수를 공개하는 설정 모듈 및 상기 공개 상수와 상기 마스터키를 이용하여 상기 수신 단말기의 부분 개인키를 생성하고, 상기 부분 개인키를 상기 수신 단말기로 송신하는 부분 개인키 추출 모듈을 포함하고, 상기 수신 단말기는 상기 공개 상수, 상기 수신 단말기의 아이디 및 상기 수신 단말기의 상태 정보($st_{ID,i-1}$)를 이용하여 비밀값을 생성하는 비밀값 설정 모듈 및 상기 공개 상수, 상기 비밀값 및 상기 상태 정보($st_{ID,i}$)를 이용하여 공개키를 생성하는 공개키 설정 모듈을 포함하고, 상기 송신 단말기는 상기 공개 상수, 상기 수신 단말기의 아이디 및 상기 공개키를 메시지를 암호화하여 암호문을 생성하고, 생성된 암호문을 상기 수신 단말기로 송신한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/14 (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 단말기, 송신 단말기 및 서버를 포함하는 무인증서 공개키 암호 시스템에 있어서,

상기 서버는,

보안 상수를 입력받아 마스터키와 공개 상수를 생성하고, 상기 공개 상수를 공개하는 설정 모듈; 및

상기 공개 상수와 상기 마스터키를 이용하여 상기 수신 단말기의 부분 개인키를 생성하고, 상기 부분 개인키를 상기 수신 단말기로 송신하는 부분 개인키 추출 모듈을 포함하고,

상기 수신 단말기는,

상기 공개 상수, 상기 수신 단말기의 아이디 및 상기 수신 단말기의 상태 정보($st_{ID,i-1}$)를 이용하여 비밀값을 생성하는 비밀값 설정 모듈; 및

상기 공개 상수, 상기 비밀값 및 상기 상태 정보($st_{ID,i}$)를 이용하여 공개키를 생성하는 공개키 설정 모듈을 포함하고,

상기 송신 단말기는 상기 공개 상수, 상기 수신 단말기의 아이디 및 상기 공개키를 이용하여 메시지를 암호화하고, 생성된 암호문을 상기 수신 단말기로 송신하는,

무인증서 공개키 암호 시스템.

청구항 2

제1항에 있어서,

상기 수신 단말기는,

상기 공개 상수, 상기 부분 개인키 및 상기 비밀값을 이용하여 복호화키를 생성하는 복호화키 설정 모듈; 및

상기 공개 상수와 상기 복호화키를 이용하여 상기 암호문을 복호화하는 복호화 모듈을 더 포함하는,

무인증서 공개키 암호 시스템.

청구항 3

제2항에 있어서,

상기 설정 모듈은,

위수가 소수 p 인 군(G_1 , G_2), 생성자($g \in G_1$), 및 겹선형 함수($e : G_1 \times G_1 \rightarrow G_2$)를 선택하고,

임의의 난수($\alpha \in Z_p^*$)와 상기 G_1 에 속하는 임의의 원소($g_1, h_1, h_2 \in G_1$)를 선택하고,

수학식 1에 의해 정의되는 상기 마스터키(MK)와 수학식 2에 의해 정의되는 상기 공개 상수(PP)를 생성하고,

상기 수학식 1은 $MK = g^{\alpha}$ 이고,

상기 수학식 2는 $PP=<e,g,g_1,h_1,h_2,\Omega=e(g,g)^{\alpha}>$ 인,

무인증서 공개키 암호 시스템.

청구항 4

제3항에 있어서,

상기 부분 개인키 추출 모듈은 임의의 난수($r_1 \in Z_p^*$)를 선택하고, 수학식 3에 의해 정의되는 상기 부분 개인키(PSK_{ID})를 생성하고,

상기 수학식 3은 $PSK_{ID}=<K_1=g^{\alpha}(g_1^{ID}h_1)^{r_1},K_2=g^{r_1}>$ 인,

무인증서 공개키 암호 시스템.

청구항 5

제4항에 있어서,

상기 비밀값 설정 모듈은 임의의 난수($\beta,r_2 \in Z_p^*$)를 선택하고,

상기 비밀값(S_{ID})은 수학식 4에 의해 정의되고,

상기 수학식 4는 $S_{ID}=<S_0=g^{\beta}(g_1^{ID||st_{ID,i}}h_2)^{r_2},S_1=g^{r_2}>$ 인,

무인증서 공개키 암호 시스템.

청구항 6

제5항에 있어서,

상기 복호화키 설정 모듈은,

임의의 난수($r'_1,r'_2 \in Z_p^*$)를 선택하고,

수학식 5를 계산하여 상기 복호화키(DK_{ID})를 생성하고,

$$DK_{ID}=<D_0=K_1 \cdot S_0 \cdot (g_1^{ID}h_1)^{r'_1} \cdot (g_1^{ID||st_{ID,i}}h_2)^{r'_2},$$

상기 수학식 5는 $$D_1=K_2 \cdot g^{r'_1},D_2=S_1 \cdot g^{r'_2}>$$ 인,

무인증서 공개키 암호 시스템.

청구항 7

제6항에 있어서,

상기 공개키 설정 모듈은 수학식 6을 이용하여 상기 공개키(PK_{ID})를 생성하고,

상기 수학식 6은 $PK_{ID} =< P = \Omega \cdot e(g,g)^{\beta} >$ 인,

무인증서 공개키 암호 시스템.

청구항 8

제7항에 있어서,

상기 송신 단말기는 임의의 난수($s \in Z_p^*$)를 선택하고, 수학식 7을 이용하여 상기 암호문(C)을 생성하고,

상기 수학식 7은 $C =< C_0 = M \cdot P^s, C_1 = (g_1^{ID} h_1)^s, C_2 = (g_1^{ID \| st_{ID,i}} h_2)^s, C_3 = g^s >$ 인,

무인증서 공개키 암호 시스템.

청구항 9

제8항에 있어서,

상기 복호화 모듈은 수학식 8을 이용하여 상기 암호문(C)을 복호화하고,

상기 수학식 8은 $M = C_0 \frac{e(C_1, D_1) e(C_2, D_2)}{e(D_0, C_3)}$ 인,

무인증서 공개키 암호 시스템.

청구항 10

무인증서 공개키 암호 시스템에 포함되는 수신 단말기에 있어서,

공개 상수, 상기 수신 단말기의 아이디 및 상기 수신 단말기의 상태 정보($st_{ID,i-1}$)를 이용하여 비밀값을 생성하는 비밀값 설정 모듈;

상기 공개 상수, 서버로부터 수신된 부분 개인키, 및 상기 비밀값을 이용하여 복호화키를 생성하는 복호화키 설정 모듈;

상기 공개 상수, 상기 비밀값 및 상기 상태 정보($st_{ID,i}$)를 이용하여 공개키를 생성하는 공개키 설정 모듈; 및

상기 공개 상수와 상기 복호화키를 이용하여 상기 암호문을 복호화하는 복호화 모듈을 포함하는,

수신 단말기.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 무인증서 공개키 암호 시스템에 관한 것으로, 특히 공개키가 교체된 이후 이전에 사용했던 비밀값과 복호화키가 노출되더라도 현재의 정당한 복호화키에 대한 어떠한 정보도 알아낼 수 없게 함으로써 안전성을 보장하는 무인증서 공개키 암호 시스템 및 수신 단말기에 관한 것이다.

배 경 기 술

[0003] 본 발명의 배경이 되는 기술은 다음과 같다.

[0004] 공개키 암호 시스템(Public Key Encryption System)

[0005] 공개키 암호 시스템에서 메시지 암호화 통신을 위해 사용되는 공개키는 식별이 불가능한 난수 형태이기 때문에 공개키만으로는 그 키에 대한 소유자가 누구인지 알 수 없다. 따라서, 메시지 전송 방식이 안전하기 위해서는 공개키와 소유자 사이를 인증해주는 새로운 매개체가 필요하다. 공개키 암호 시스템에서는 인증서를 통해 공개키의 소유 여부를 인증하며, 이 인증서는 제3의 신뢰기관(trusted third authority)을 통해 발급된다. 인증서를 기반으로 공개키를 인증하기 때문에 공개키에 대한 신뢰는 보장할 수 있지만, 인증서 저장, 폐기 및 분배 등 관리차원의 문제가 발생한다. 따라서 이러한 공개키 암호 기법의 문제를 해결하기 위해서 ID기반 암호 시스템이 개발되었다.

[0007] ID기반 암호 시스템(Identity Based Encryption System)

[0008] ID기반 암호 시스템에서는 이메일 주소나 IP 주소와 같은 식별 가능한 문자열인 사용자의 ID가 공개키가 되어 그 자체로 사용자의 공개키 소유 권한이 입증된다. 별도의 공개키 인증 과정이 필요하지 않아 공개키 기반 구조의 인증서 관리 문제가 발생하지 않지만, 키 생성 기관(key generation center)이 모든 개인키를 생성하여 사용자에게 발급해주는 방식이기 때문에 키 생성 기관이 모든 개인키를 알게 되는 키 위탁(key escrow) 문제가 발생한다. 이를 해결하기 위하여 무인증서 공개키 암호 시스템이 개발되었다.

[0010] 무인증서 공개키 암호 시스템(Certificateless Public Key Encryption System)

[0011] 무인증서 공개키 암호 시스템은 난수성을 갖는 공개키와 사용자의 ID를 함께 공개키로 사용하는 암호 시스템으로써, 인증서를 사용하지 않으면서 ID기반 암호의 키 위탁 문제를 해결하였다. 무인증서 공개키 암호 시스템에서는 메시지를 복호화하기 위해 사용자가 선택한 비밀값과 키 생성 기관이 발급한 부분 개인키를 이용하여 연산된 복호화키를 사용한다. 여기서 난수성을 가지는 공개키는 사용자가 선택한 비밀값을 이용하여 계산된 값이다. 이때, 한 번이라도 공개키가 교체된 이후에 이전의 비밀값과 복호화키가 노출되더라도 공격자가 현재의 공개키로 암호화된 암호문에 대하여 어떠한 정보도 얻을 수 없어야 한다. 이러한 무인증서 공개키 암호 시스템에 대한 안전성을 보장하는 기법을 비밀값과 복호화키 노출 공격에 안전한 무인증서 공개키 암호 기법이라 한다.

[0013] 겹선형 함수(Bilinear Map)

[0014] 위수를 소수 p 로 갖는 곱셈 군 G_1 과 G_2 가 있고, G_1 의 생성원(generator)이 g 라고 가정하자. 다음과 같은 조건을 만족하는 함수 $e: G_1 \times G_1 \rightarrow G_2$ 를 겹선형 함수라 한다.

[0015] 1) 겹선형성(bilinearity): 임의의 두 원소 $g,h \in G_1$ 와 $a,b \in Z_p^*$ 에 대해 $e(g^a,h^b) = e(g,h)^{ab}$ 가 된다.

[0016] 2) 비소실성(non-degeneracy): $e(g,g) \neq 1$ 을 만족하는 $g \in G_1$ 가 존재한다.

[0017] 3) 계산 가능성(computability): 임의의 $g,h \in G_1$ 에 대해서 $e(g,h)$ 를 효율적으로 계산할 수 있는 알고리즘이 존재한다.

[0019] DBDH 가정(Decisional Bilinear Diffie-Hellman assumption)

[0020] 위수를 소수 p 로 갖는 군 G_1 가 있고 겹선형 함수 $e: G_1 \times G_1 \rightarrow G_2$ 가 있을 때 $g \in G_1$을 G_1의 생성원이라고 가정하자. 이 때, DBDH 문제는 지수 부분의 $a,b,c \in Z_p^*$ 가 이와 같이 Z_p^* 상의 원소이고 집합

(g, g^a, g^b, g^c, T)가 주어졌을 때, $e(g,g)^{abc} = ? T$ 인지를 결정하는 것이다.

[0021] 알고리즘 B는 $e(g,g)^{abc} = T$ 혹은 $e(g,g)^{abc} \neq T$에 따라 비트 $b \in \{0,1\}$을 출력하는 알고리즘이다. 이 때, 다항식 시간 안에 의미 있는(non-negligible) 확률로 계산할 수 있는 알고리즘 B가 존재하지 않는다면 DBDH 문제는 풀기 어렵다고 정의하며, 알고리즘 B가 DBDH 문제를 풀 수 있을

[0022] 이점(advantage) ϵ는 다음과 같다.

[0023] $$Adv(B) = \left| \begin{matrix} \Pr[B(g,g^a,g^b,g^c,e(g,g)^{abc}) = 0] \\ -\Pr[B(g,g^a,g^b,g^c,T) = 0] \end{matrix} \right| \geq \epsilon$$

발명의 내용

해결하려는 과제

[0025] 본 발명이 이루고자 하는 기술적인 과제는 공개키가 교체된 이후 이전의 비밀값과 복호화키가 노출되더라도 이를 이용하여 부분 개인키를 연산할 수 없고 현재의 공개키로 암호화된 암호문에 대한 어떠한 정보도 얻을 수 없게 함으로써 높은 안전성을 보장할 수 있는 무인증서 공개키 암호 시스템 및 수신 단말기를 제공하는 것이다.

과제의 해결 수단

[0027] 본 발명의 일 실시 예에 따른 무인증서 공개키 암호 시스템은 수신 단말기, 송신 단말기 및 서버를 포함하고, 상기 서버는 보안 상수를 입력받아 마스터키와 공개 상수를 생성하고, 상기 공개 상수를 공개하는 설정 모듈 및 상기 공개 상수와 상기 마스터키를 이용하여 상기 수신 단말기의 부분 개인키를 생성하고, 상기 부분 개인키를 상기 수신 단말기로 송신하는 부분 개인키 추출 모듈을 포함하고, 상기 수신 단말기는 상기 공개 상수, 상기 수신 단말기의 아이디 및 상기 수신 단말기의 상태 정보($st_{ID,i-1}$)를 이용하여 비밀값을 생성하는 비밀값 설정 모듈 및 상기 공개 상수, 상기 비밀값 및 상기 상태 정보($st_{ID,i}$)를 이용하여 공개키를 생성하는 공개키 설정 모듈을 포함하고, 상기 송신 단말기는 상기 공개 상수, 상기 수신 단말기의 아이디 및 상기 공개키로 메시지를 암호화하여 암호문을 생성하고, 생성된 암호문을 상기 수신 단말기로 송신한다.

[0029] 본 발명의 일 실시 예에 따른 수신 단말기는 상기 무인증서 공개키 암호 시스템에 포함될 수 있고, 공개 상수, 상기 수신 단말기의 아이디 및 상기 수신 단말기의 상태 정보($st_{ID,i-1}$)를 이용하여 비밀값을 생성하는 비밀값 설정 모듈, 상기 공개 상수, 서버로부터 수신된 부분 개인키, 및 상기 비밀값을 이용하여 복호화키를 생성하는 복호화키 설정 모듈, 상기 공개 상수, 상기 비밀값 및 상기 상태 정보($st_{ID,i}$)를 이용하여 공개키를 생성하는 공개키 설정 모듈, 및 상기 공개 상수와 상기 복호화키를 이용하여 상기 암호문을 복호화하는 복호화 모듈을 포함한다.

발명의 효과

[0031] 본 발명의 실시 예에 따른 무인증서 공개키 암호 시스템에 의할 경우, 공개키가 교체된 이후 이전의 사용자 비밀값과 복호호키가 악의적인 공격자에게 노출되더라도 노출된 키 정보를 연산하여 부분 개인키 값을 구한다거나 현재의 공개키로 암호화된 암호문을 해독하는 것은 불가능하다. 즉, 공격자가 이러한 키 정보를 이용하여 어떠한 의미있는 정보도 알아낼 수 없다.

[0032] 또한, 클라이언트가 비밀값을 생성할 때마다 상태정보가 갱신되고, 갱신된 상태정보를 이용하여 공개키가 생성

되기 때문에, 공격자가 악의적으로 공개키를 교체하더라도 공개키로 암호화된 암호문의 상태정보와 복호화키의 상태정보가 다르기 때문에 공격자는 암호문에 대한 어떠한 정보도 알아낼 수 없다. 또한, 수학적으로 계산이 어려운 문제에 기반을 두어 설계되었으므로 무인증서 암호 기법의 안전성이 보장된다.

도면의 간단한 설명

[0034] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 의한 무인증서 공개키 암호 시스템을 도시한다.

도 2는 도 1에 도시된 서버의 기능 블럭도이다.

도 3은 도 1에 도시된 수신 단말기의 기능 블럭도이다.

발명을 실시하기 위한 구체적인 내용

[0035] 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.

[0036] 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.

[0037] 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.

[0038] 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.

[0039] 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.

[0040] 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.

[0042] 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명하기 전에 본 발명에서 이용되는 알고리즘에 대해 설명하면 다음과 같다.

[0043] 본 발명에 따른 무인증서 암호 기법은 설정 알고리즘(Setup), 부분 개인키 추출 알고리즘(ExtractPartialPrivateKey), 비밀값 설정 알고리즘(SetSecretValue), 복호화키 설정 알고리즘

(SetDecryptionKey), 공개키 설정 알고리즘(SetPublicKey), 암호화 알고리즘(Encrypt), 복호화 알고리즘(Decrypt)을 이용하며, 이용되는 각 알고리즘은 다음과 같이 구성된다.

[0045] 1. 설정 알고리즘(Setup)

[0046] 설정 알고리즘 또는 설정 단계에서는 보안 상수 k 를 입력받아 마스터키 MK와 공개 상수(공개 파라미터라고도 함) PP 를 출력한다. 상기 설정 알고리즘은 서버에 의해 수행되며 설정 단계가 완료되면 상기 서버는 마스터키 MK 를 저장하고 공개 상수 PP 를 공개한다.

[0047] 구체적으로, 상기 서버는 위수가 소수 p 인 군 G_1, G_2, 생성자 $g \in G_1$, 겹선형 함수 $e: G_1 \times G_1 \rightarrow G_2$ 를 선택한다. 또한, 상기 서버는 임의의 난수 $\alpha \in Z_p^*$ 와 G_2에 포함되는 임의의 원소 $g_1, h_1, h_2 \in G_1$를 선택한다. 결국, 서버에 의해 생성된 마스터키 MK 는 g^{α} 이고, 공개 파라미터 PP는 다음과 같다.

[0048] $$PP = < e, g, g_1, h_1, h_2, \Omega = e(g,g)^{\alpha} >$$

[0050] 2. 부분 개인키 추출 알고리즘(ExtractPartialPrivateKey)

[0051] 부분 개인키 추출 알고리즘 또는 부분 개인키 추출 단계에서는 공개 상수 PP, 마스터키 MK, 및 사용자(수신자)의 아이디 ID 를 입력받아 부분 개인키 PSK_{ID} 를 출력한다. 상기 부분 개인키 추출 알고리즘은 상기 서버에 의해 각각의 사용자 별로 1회씩 수행될 수 있으며, 생성된 부분 개인키 PSK_{ID}는 대응하는 사용자(또는 사용자의 단말기)에게 전달된다.

[0052] 구체적으로, 상기 서버는 임의의 난수 $r_1 \in Z_p^*$ 를 선택하고, 상기 서버에 의해 생성된 부분 개인키 PSK_{ID}는 다음과 같다.

[0053] $$PSK_{ID} = < K_1 = g^{\alpha}(g_1^{ID} h_1)^{r_1}, K_2 = g^{r_1} >$$

[0055] 3. 비밀값 설정 알고리즘(SetSecretValue)

[0056] 비밀값 설정 알고리즘 또는 비밀값 설정 단계에서는 공개 상수 PP 와 사용자의 아이디 ID를 입력받고 상기 사용자의 상태정보 $st_{ID,i-1}$를 이용하여 비밀값 S_{ID} 을 출력할 수 있다. 비밀값 설정 알고리즘은 상기 사용자의 단말기인 수신 단말기에 의해 수행될 수 있다.

[0057] 구체적으로, 상기 수신 단말기는 임의의 난수 $\beta, r_2 \in Z_p^*$ 를 선택한다. 이때, 난수 β는 상기 수신 단말기가 공개키를 생성하는 과정에서 이용될 수 있으며 상기 수신 단말기에 의해 상기 수신 단말기 내에 저장된다. 상태정보 $st_{ID,i}$ 는 임의의 정수, 예컨대 "1"을 초기값으로 갖으며(즉, $st_{ID,1} = 1$), 비밀값 S_{ID}이 생성될 때마다 상기 수신 단말기에 의해 그 값이 갱신될 수 있다(즉, $st_{ID,i} = st_{ID,i-1} + 1$). 상기 수신 단말기에 의해 생성된 비밀값 S_{ID} 는 다음과 같다.

[0058] $$S_{ID} = < S_0 = g^{\beta}(g_1^{ID \| st_{ID,i}} h_2)^{r_2}, S_1 = g^{r_2} >$$

[0060] 4. 복호화키 설정 알고리즘(SetDecryptionKey)

[0061] 복호화키 설정 알고리즘 또는 복호화키 설정 단계에서는 공개 상수 PP, 부분 개인키 PSK_{ID}, 및 비밀값 S_{ID}을 입력받고 상기 사용자의 복호화키 DK_{ID}를 출력할 수 있다. 상기 복호화키 설정 알고리즘은 상기 수신 단말기에 의해 수행된다.

[0062] 구체적으로, 상기 수신 단말기는 임의의 난수 $r'_1, r'_2 \in Z_p^*$를 선택하고, 아래 수학식을 연산하여 복호화키 DK_{ID}를 생성한다.

[0063]
$$DK_{ID} = < D_0 = K_1 \cdot S_0 \cdot (g_1^{ID} h_1)^{r'_1} \cdot (g_1^{ID \| st_{ID,i}} h_2)^{r'_2},$$
$$D_1 = K_2 \cdot g^{r'_1}, D_2 = S_1 \cdot g^{r'_2} >$$

[0064] 생성된 복호화키 DK_{ID}는 다음과 같다.

[0065]
$$DK_{ID} = < D_0 = g^{\alpha+\beta} (g_1^{ID} h_1)^{\hat{r_1}} (g_1^{ID \| st_{ID,i}} h_2)^{\hat{r_2}},$$
$$D_1 = g^{\hat{r_1}}, D_2 = g^{\hat{r_2}} >$$

[0066] 이때, $\hat{r_1}$과 $\hat{r_2}$는 아래와 같이 정의될 수 있다.

[0067] $\hat{r_1} = r_1 + r'_1$, $\hat{r_2} = r_2 + r'_2$

[0069] 5. 공개키 설정 알고리즘(SetPublicKey)

[0070] 공개키 설정 알고리즘 또는 공개키 설정 단계에서는 공개 상수 PP와 사용자의 비밀값 S_{ID}을 입력받고 상기 사용자의 상태정보 $st_{ID,i}$를 이용하여 공개키 PK_{ID}를 출력할 수 있다. 상기 공개키 설정 알고리즘은 수신 단말기에 의해 수행될 수 있다.

[0071] 구체적으로, 상기 수신 단말기에 의해 생성된 공개키 PK_{ID}는 다음과 같다.

[0072]
$$PK_{ID} = < P = e(g,g)^{\alpha+\beta}, st_{ID,i} >$$

[0073] 상기 공개키 PK_{ID}에 포함된 P는 아래 수학식을 이용하여 계산될 수 있다.

[0074]
$$P = \Omega \cdot e(g,g)^{\beta}$$

[0076] 6. 암호화 알고리즘(Encrypt)

[0077] 암호화 알고리즘 또는 암호화 단계에서는 공개 상수 PP, 수신자(또는 수신 단말기)의 아이디 ID, 공개키 PK_{ID}, 및 메시지 M를 입력받아 암호문 C을 출력한다. 상기 암호화 알고리즘은 송신 단말기에 의해 수행될 수 있다.

[0078] 구체적으로 상기 송신 단말기는 임의의 난수 $s \in Z_p^*$를 선택하고, 아래 수학식에 의해 정의되는 암호문 C을 생성할 수 있다.

[0079] $$C=< C_0 = M \bullet P^s, C_1 = (g_1^{ID} h_1)^s, C_2 = (g_1^{ID\|st_{ID,i}} h_2)^s, C_3 = g^s >$$

[0081] 7. 복호화 알고리즘(Decrypt)

[0082] 복호화 알고리즘 또는 복호화 단계에서는 공개 상수 PP, 복호화키 DK_{ID}, 및 암호문 C을 입력받아 메시지 M 또는 에러 기호 $\perp$를 출력할 수 있다. 상기 복호화 알고리즘은 수신 단말기에 의해 수행될 수 있으며, 메시지 M는 아래 수학식을 이용하여 생성(또는 복호화)될 수 있다.

[0083] $$C_0 \frac{e(C_1, D_1)e(C_2, D_2)}{e(D_0, C_3)} = M$$

[0085] 상술된 무인증서 암호 기법은 아래와 같이 평문 메시지 M를 구하는 과정으로부터 그 정확성이 입증될 수 있다.

$$C_0 \frac{e(C_1, D_1)e(C_2, D_2)}{e(D_0, C_3)}$$

$$= M \bullet P^s \frac{e((g_1^{ID} h_1)^s, g^{\hat{r_1}})e((g_1^{ID\|st_{ID,i}} h_2)^s, g^{\hat{r_2}})}{e(g^{\alpha+\beta}(g_1^{ID} h_1)^{\hat{r_1}}(g_1^{ID\|st_{ID,i}} h_2)^{\hat{r_2}}, g^s)}$$

$$= M \bullet P^s \frac{e((g_1^{ID} h_1)^s, g^{\hat{r_1}})e((g_1^{ID\|st_{ID,i}} h_2)^s, g^{\hat{r_2}})}{e(g^{\alpha+\beta}, g^s)e((g_1^{ID} h_1)^{\hat{r_1}}, g^s)e((g_1^{ID\|st_{ID,i}} h_2)^{\hat{r_2}}, g^s)}$$

$$= M \bullet P^s \frac{e(g_1^{ID} h_1, g)^{\hat{r_1} s} e(g_1^{ID\|st_{ID,i}} h_2, g)^{\hat{r_2} s}}{e(g^{\alpha+\beta}, g^s)e(g_1^{ID} h_1, g)^{\hat{r_1} s} e(g_1^{ID\|st_{ID,i}} h_2, g)^{\hat{r_2} s}}$$

$$= M \bullet (e(g,g)^{\alpha} e(g,g)^{\beta})^s \frac{1}{e(g^{\alpha+\beta}, g^s)}$$

$$= M \bullet e(g,g)^{s(\alpha+\beta)} \frac{1}{e(g,g)^{s(\alpha+\beta)}}$$

[0086] $$= M$$

[0088] 도 1은 본 발명의 일 실시 예에 의한 무인증서 공개키 암호 시스템을 도시한다.

[0089] 도 1을 참조하면, 무인증서 공개키 암호 시스템(10)은 수신 단말기(100), 서버(300) 및 송신 단말기(500)를 포함한다.

[0090] 수신 단말기(100)는 서버(300)로부터 부분 개인키 PSK_{ID}를 수신하고, 비밀값 S_{ID}을 생성하며, 수신된 부분 개인키 PSK_{ID}와 생성된 비밀값 S_{ID}을 이용하여 복호화키 DK_{ID}를 생성하며, 설정된 비밀값 S_{ID}을 이용하여 공개키 PK_{ID}를 설정할 수 있다.

[0091] 또한, 수신 단말기(100)는 송신 단말기(300)로부터 암호문 C을 수신하고, 생성된 복호화키 DK_{ID}를 이용하여 암호문 C을 복호화할 수 있다.

[0093] 무인증서 공개키 암호 서버, 무인증서 암호 서버, 암호 서버, 키 생성 서버 또는 키 발급 서버 등으로 명명될

수 있는 서버(300)는 마스터키 MK 와 공개 상수 PP 를 생성하고, 생성된 공개 상수 PP를 공개할 수 있다. 또한, 서버(300)는 사용자(또는 수신 단말기(100))의 아이디 ID 에 대응하는 부분 개인키 PSK_{ID}를 생성하고 생성된 부분 개인키 PSK_{ID} 를 수신 단말기(100)로 송신할 수 있다.

[0095] 송신 단말기(500)는 암호화 알고리즘을 수행하여 메시지 M 를 암호화하고 생성된 암호문 C 을 수신 단말기(100)로 송신할 수 있다.

[0096] 구체적으로 송신 단말기(500)는 임의의 난수 $s \in Z_p^*$ 를 선택하고, 아래 수학식에 의해 정의되는 암호문 C 을 생성할 수 있다.

[0097] $$C=< C_0 = M \bullet P^s, C_1 = (g_1^{ID} h_1)^s, C_2 = (g_1^{ID \| st_{ID,i}} h_2)^s, C_3 = g^s >$$

[0098] 생성된 암호문 C 은 수신 단말기(100)로 송신될 수 있다.

[0100] 수신 단말기(100)는 및/또는 송신 단말기(300)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), 스마트폰(smart phone)과 같은 핸드헬드 장치(handheld device)로 구현될 수 있다.

[0102] 도 2는 도 1에 도시된 서버의 기능 블럭도이다.

[0103] 도 1과 도 2를 참조하면, 서버(300)는 설정 모듈(310)과 부분 개인키 추출 모듈(330)을 포함한다.

[0104] 설정 모듈(310)은 설정 알고리즘을 수행할 수 있다. 즉, 설정 모듈(310)은 보안 상수 k를 입력받고 마스터키 MK 와 공개 상수 PP 를 생성하고, 공개 상수 PP 를 공개할 수 있다.

[0105] 구체적으로, 설정 모듈(310)은 위수가 소수 p 인 군 G_1, G_2, 생성자 $g \in G_1$, 겹선형 함수 $e : G_1 \times G_1 \rightarrow G_2$ 를 선택한다. 또한, 설정 모듈(310)은 임의의 난수 $\alpha \in Z_p^*$와 G_2에 포함되는 임의의 원소 $g_1, h_1, h_2 \in G_1$ 를 선택한다. 결국, 설정 모듈(310)에 의해 생성된 마스터키 MK는 g^α 이고, 공개 파라미터 PP 는 다음과 같다.

[0106] $$PP=< e, g, g_1, h_1, h_2, \Omega = e(g,g)^\alpha >$$

[0108] 부분 개인키 추출 모듈(330)은 부분 개인키 추출 알고리즘을 수행할 수 있다. 즉, 부분 개인키 추출 모듈(330)은 공개 상수 PP , 마스터키 MK , 및 사용자의 아이디 ID 를 이용하여 부분 개인키 PSK_{ID}를 생성하고, 생성된 부분 개인키 PSK_{ID} 를 대응하는 수신 단말기(100)로 송신할 수 있다.

[0109] 구체적으로, 부분 개인키 추출 모듈(330)은 임의의 난수 $r_1 \in Z_p^*$ 를 선택하고, 아래 수학식에 의해 정의되는 부분 개인키 PSK_{ID} 를 생성한다.

[0110] $$PSK_{ID} =< K_1 = g^\alpha (g_1^{ID} h_1)^{r_1}, K_2 = g^{r_1} >$$

[0111] 생성된 부분 개인키 PSK_{ID}는 수신 단말기(100)로 송신될 수 있다.

[0113] 도 3은 도 1에 도시된 수신 단말기의 기능 블럭도이다.

[0114] 도 1 내지 도 3을 참조하면, 수신 단말기(100)는 비밀값 설정 모듈(110), 복호화키 설정 모듈(130), 공개키 설정 모듈(150), 및 복호화 모듈(170)을 포함한다.

[0116] 비밀값 설정 모듈(110)은 비밀값 설정 알고리즘을 수행할 수 있다. 즉, 비밀값 설정 모듈(110)은 공개 상수 PP, 사용자의 아이디 ID, 및 상기 사용자의 상태정보 $st_{ID,i-1}$를 이용하여 비밀값 S_{ID}을 생성할 수 있다.

[0117] 구체적으로, 비밀값 설정 모듈(110)은 임의의 난수 $\beta, r_2 \in Z_p^*$ 를 선택한다. 이때, 난수 β는 상기 수신 단말기(100)가 공개키를 생성하는 과정에서 이용될 수 있으며 수신 단말기(100)에 의해 수신 단말기(100) 내에 저장된다. 상태정보 $st_{ID,i}$는 임의의 정수, 예컨대 "1"을 초기값으로 갖으며(즉, $st_{ID,1}=1$), 비밀값 S_{ID}이 생성될 때마다 비밀값 설정 모듈(110)에 의해 그 값이 갱신될 수 있다(즉, $st_{ID,i}=st_{ID,i-1}+1$). 비밀값 설정 모듈(110)에 의해 생성된 비밀값 S_{ID}는 다음과 같다.

[0118] $$S_{ID} =< S_0 = g^{\beta}(g_1^{ID\|st_{ID,i}} h_2)^{r_2}, S_1 = g^{r_2} >$$

[0120] 복호화키 설정 모듈(130)은 복호화키 설정 알고리즘을 수행할 수 있다. 즉, 복호화키 설정 모듈(130)은 공개 상수 PP, 부분 개인키 PSK_{ID}, 및 비밀값 S_{ID}을 이용하여 사용자(또는 수신 단말기(100))의 복호화키 DK_{ID}를 생성할 수 있다.

[0121] 구체적으로, 복호화키 설정 모듈(130)은 임의의 난수 $r'_1, r'_2 \in Z_p^*$ 를 선택하고, 아래 수학식을 연산하여 복호화키 DK_{ID}를 생성한다.

[0122] $$DK_{ID} =< D_0 = K_1 \cdot S_0 \cdot (g_1^{ID} h_1)^{r'_1} \cdot (g_1^{ID\|st_{ID,i}} h_2)^{r'_2},$$
$$D_1 = K_2 \cdot g^{r'_1}, D_2 = S_1 \cdot g^{r'_2} >$$

[0123] 생성된 복호화키 DK_{ID}는 다음과 같다.

[0124] $$DK_{ID} =< D_0 = g^{\alpha+\beta}(g_1^{ID} h_1)^{\hat{r_1}} (g_1^{ID\|st_{ID,i}} h_2)^{\hat{r_2}},$$
$$D_1 = g^{\hat{r_1}}, D_2 = g^{\hat{r_2}} >$$

[0125] 이때, $\hat{r_1}$과 $\hat{r_2}$는 아래와 같이 정의될 수 있다.

[0126] $\hat{r_1} = r_1 + r'_1$, $\hat{r_2} = r_2 + r'_2$

[0128] 공개키 설정 모듈(150)은 공개키 설정 알고리즘을 수행할 수 있다. 즉, 공개 상수 PP와 비밀값 S_{ID}, 및 상태정보 $st_{ID,i}$를 이용하여 공개키 PK_{ID}를 생성할 수 있다.

[0129] 구체적으로, 공개키 설정 모듈(150)에 의해 생성된 공개키 PK_{ID} 는 다음과 같다.

[0130] $$PK_{ID} = < P = e(g,g)^{\alpha+\beta}, st_{ID,i} >$$

[0131] 공개키 PK_{ID} 에 포함된 P 는 아래 수학식을 이용하여 계산될 수 있다.

[0132] $$P = \Omega \cdot e(g,g)^{\beta}$$

[0134] 복호화 모듈(170)은 복호화 알고리즘을 수행할 수 있다. 즉, 복호화 모듈(170)은 공개 상수 PP, 및 복호화키 DK_{ID} 를 이용하여 암호문 C 을 복호화함으로써 메시지 M 를 출력할 수 있다. 메시지 M 는 아래 수학식을 이용하여 생성(또는 복호화)될 수 있다.

[0135] $$C_0 \frac{e(C_1, D_1)e(C_2, D_2)}{e(D_0, C_3)} = M$$

[0137] 도 2 및 도 3에 도시된 서버(300)와 수신 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.

[0138] 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.

[0140] 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

[0141] 100 : 수신 단말기

110 : 비밀값 설정 모듈

130 : 복호화키 설정 모듈

150 : 공개키 설정 모듈

170 : 복호화 모듈

300 : 서버

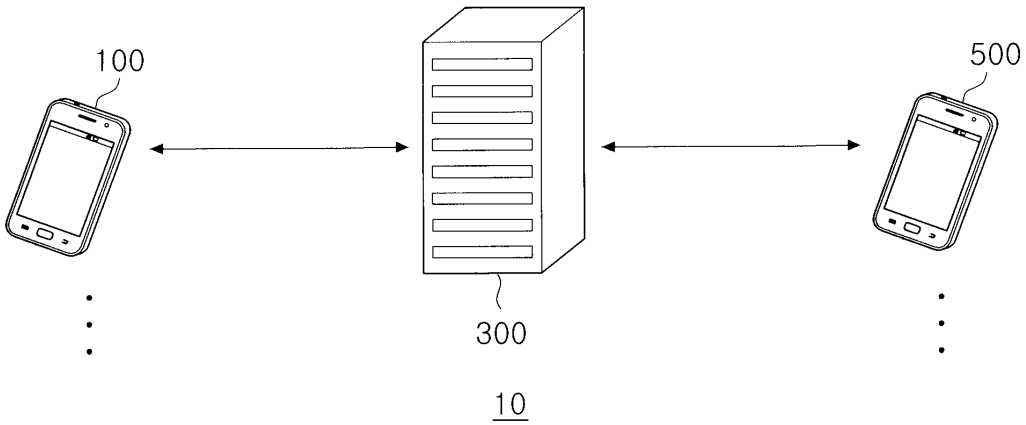
310 : 설정 모듈

330 : 부분 개인키 추출 모듈

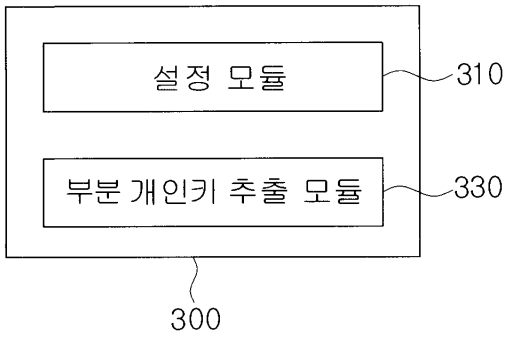
500 : 송신 단말기

도면

도면1



도면2



도면3