



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0046425
(43) 공개일자 2018년05월09일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/30 (2013.01)
H04L 9/0819 (2013.01)
(21) 출원번호 10-2016-0141184
(22) 출원일자 2016년10월27일
심사청구일자 2016년10월27일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
최수리
서울특별시 동대문구 경동시장로 67-5 202호 (제기동)
(뒷면에 계속)
(74) 대리인
김동용, 김홍석

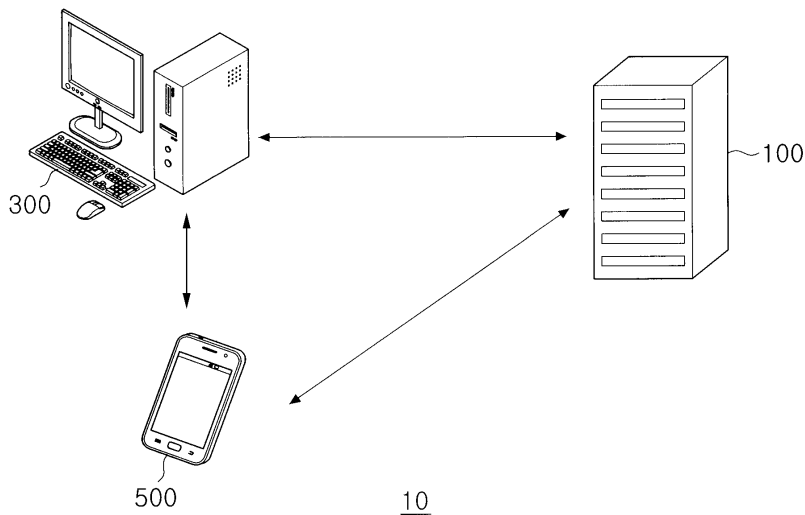
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 공개키 기반 암호화 방법 및 키 생성 서버

(57) 요약

공개키 기반 암호화 방법이 개시된다. 상기 공개키 기반 암호화 방법은 (a) 서버가 공개 상수와 마스터 비밀키를 생성하는 단계, (b) 상기 서버가 수신 단말의 부분 비밀키를 생성하고, 상기 부분 비밀키를 상기 수신 단말로 송신하는 단계, (c) 상기 수신 단말이 비밀값을 선택하는 단계, (d) 상기 수신 단말이 비밀키를 생성하는 단계, (e) 상기 수신 단말이 공개키를 생성하고, 상기 공개키를 상기 송신 단말로 송신하는 단계, (f) 상기 송신 단말이 메시지를 암호화하여 암호문을 생성하고, 상기 암호문을 상기 수신 단말로 송신하는 단계, 및 (g) 상기 수신 단말이 상기 암호문을 복호화하는 단계를 포함한다.

대표도 - 도1



(52) CPC특허분류

H04L 9/0861 (2013.01)

H04L 9/0869 (2013.01)

(72) 발명자

김효승

서울특별시 성북구 안암로9가길 56 206호 (안암동 5가)

김중현

서울특별시 강남구 학동로68길 29, 101동 1301호
(삼성동, 삼성동 힐스테이트)

이 발명을 지원한 국가연구개발사업

과제고유번호 R01261610900001002

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보통신방송연구개발사업

연구과제명 계층적 식별자를 가진 인터넷 개체의 공개키 인증 구조 연구

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2016.03.01 ~ 2017.02.28

명세서

청구범위

청구항 1

- (a) 서버가 공개 상수($params$)와 마스터 비밀키(msk)를 생성하는 단계;
- (b) 상기 서버가 수신 단말의 부분 비밀키(D_A)를 생성하고, 상기 부분 비밀키(D_A)를 상기 수신 단말로 송신하는 단계;
- (c) 상기 수신 단말이 비밀값($d_A \in Z_q^*$)을 선택하는 단계;
- (d) 상기 수신 단말이 비밀키(S_A)를 생성하는 단계;
- (e) 상기 수신 단말이 공개키(P_A)를 생성하고, 상기 공개키(P_A)를 상기 송신 단말로 송신하는 단계;
- (f) 상기 송신 단말이 메시지(M)를 암호화하여 암호문(CT)을 생성하고, 상기 암호문(CT)을 상기 수신 단말로 송신하는 단계; 및
- (g) 상기 수신 단말이 상기 암호문(CT)을 복호화하는 단계를 포함하고,
- 상기 (a) 단계는,
- 위수가 소수 q ($q > 2^\lambda$)인 순환 군(G), G 에 속하는 임의의 생성자 g, h ($g, h \in G$) 및 해쉬 함수 ($H: \{0,1\}^* \rightarrow Z_q^*$)를 선택하는 단계; 및
- 각각의 i ($i \in \{1, \dots, l+1\}$)에 대해 임의의 난수($s_i \in Z_q^*$)를 선택하고 계산값($g_i = g^{s_i}$)을 계산하는 단계를 포함하고,
- 상기 공개 상수($params$)는 수학식 1에 의해 정의되고,
- 상기 마스터 비밀키(msk)는 수학식 2에 의해 정의되고,
- 상기 수학식 1은 $params = (G, g, h, \{g_i\}_{i=1}^{l+1}, H)$ 이고,
- 상기 수학식 2는 $msk = \{s_i\}_{i=1}^{l+1}$ 이고,
- 상기 l 은 공모제한 상수인,
- 공개키 기반 암호화 방법.

청구항 2

- 제1항에 있어서,
- 상기 (b) 단계는,

각각의 i 에 대하여 $\sum_{i=1}^l t_i = 0$ 을 만족하는 $t_i \in Z_q^*$ 를 선택하는 단계;

수학식 3에 의해 정의되는 벡터 $\vec{x}$ 를 생성하는 단계; 및

수학식 4를 이용하여 상기 수신 단말의 부분 비밀키(D_A)를 생성하는 단계를 포함하고,

상기 수학식 3은,

$$\vec{x} = (H(ID_A)^{t_l}, H(ID_A)^{l-1}t_{l-1}, \dots, H(ID_A)^2t_2, H(ID_A)t_1, 1) = (x_1, \dots, x_{l+1}) \in Z_q^{*l+1} \text{ 이고,}$$

$$D_A = (s_x, \vec{x}) = \left(\sum_{i=1}^{l+1} s_i \cdot x_i, \vec{x} \right) = (\langle \vec{s}, \vec{x} \rangle, \vec{x})$$

상기 수학식 4는 이고,

상기 ID_A 는 상기 수신 단말의 아이디인,

공개키 기반 암호화 방법.

청구항 3

제2항에 있어서,

상기 비밀키(S_A)는 수학식 5에 의해 정의되고,

$$S_A = (s_x, \vec{x}, d_A) \text{ 인,}$$

상기 수학식 5는

공개키 기반 암호화 방법.

청구항 4

제3항에 있어서,

상기 공개키(P_A)는 수학식 6에 의해 정의되고,

$$P_A = h^{d_A} \text{ 인,}$$

상기 수학식 6은

공개키 기반 암호화 방법.

청구항 5

제4항에 있어서,

상기 단계 (f)는,

임의의 난수 $a, b, r \in Z_q^*$ 를 선택하는 단계; 및

수학식 7을 이용하여 암호문(CT)을 생성하는 단계를 포함하고,

상기 수학식 7은,

$$CT = \langle g^r, (P_A)^a \cdot M, \{h^{y_i} \cdot g_i^r\}_{i=1}^{l+1} \rangle = \langle A, B, \{C_i\}_{i=1}^{l+1} \rangle \text{ 이고,}$$

상기 벡터 $\vec{y}$ 는 수학식 8에 의해 정의되고,

상기 수학식 8은,

$$\vec{y} = (bH(ID_A), bH(ID_A)^2, \dots, bH(ID_A)^l, a) = (y_1, \dots, y_{l+1}) \in Z_q^{*l+1} \text{ 인,}$$

공개키 기반 암호화 방법.

청구항 6

제5항에 있어서,

상기 수신 단말은 수학식 9를 이용하여 상기 암호문(CT)을 복호화하고,

$$M = B \times \left(\frac{A^{s_x}}{\prod_{i=1}^{l+1} C_i^{x_i}} \right)^{d_A} \text{ 인,}$$

상기 수학식 9는

공개키 기반 암호화 방법.

청구항 7

위수가 소수 q ($q > 2^\lambda$)인 순환 군(G), G 에 속하는 임의의 생성자 g, h ($g, h \in G$) 및 해쉬 함수 ($H: \{0,1\}^* \rightarrow Z_q^*$)를 선택하고, 각각의 i ($i \in \{1, \dots, l+1\}$)에 대해 임의의 난수($s_i \in Z_q^*$)를 선택하고 계산값($g_i = g^{s_i}$)을 계산하고, 수학식 1에 의해 정의되는 공개 상수($params$)와 수학식 2에 의해 정의되는 마스터 비밀키(msk)를 생성하는 설정부; 및

각각의 i 에 대하여 $\sum_{i=1}^l t_i = 0$ 을 만족하는 $t_i \in Z_q^*$ 를 선택하고, 수학식 3에 의해 정의되는 벡터 $\vec{x}$ 를 생

성하고, 수학식 4를 이용하여 수신 단말의 부분 비밀키(D_A)를 생성하는 부분 비밀키 생성부를 포함하고,

상기 수학식 1은 $params = (G, g, h, \{g_i\}_{i=1}^{l+1}, H)$ 이고,

상기 수학식 2는 $msk = \{s_i\}_{i=1}^{l+1}$

상기 수학식 3은,

$$\vec{x} = (H(ID_A)^{t_l}, H(ID_A)^{l-1}t_{l-1}, \dots, H(ID_A)^2t_2, H(ID_A)t_1, 1) = (x_1, \dots, x_{l+1}) \in Z_q^{*l+1} \text{ 이고,}$$

$$D_A = (s_x, \vec{x}) = \left(\sum_{i=1}^{l+1} s_i \cdot x_i, \vec{x} \right) = (\langle \vec{s}, \vec{x} \rangle, \vec{x})$$

상기 수학식 4는

이고,

상기 ID_A 는 상기 수신 단말의 아이디이고,

상기 l 은 공모제한 상수인,

키 생성 서버.

청구항 8

제7항에 있어서,

상기 설정부는 상기 공개 상수($params$)를 공개하고,

상기 부분 비밀키 생성부는 상기 부분 비밀키(D_A)를 상기 수신 단말로 송신하는,

키 생성 서버.

발명의 설명

기술 분야

[0001]

본 발명의 개념에 따른 실시 예는 공개키 기반 암호화 방법 및 키 생성 서버에 관한 것으로서, 특히 사용자 단말이 키 생성 서버로부터 수신한 부분 비밀키를 이용하여 비밀키와 공개키를 생성하도록 하여 키 위탁 문제를 해결할 수 있는 공개키 기반 암호화 방법 및 키 생성 서버에 관한 것이다.

배경 기술

[0003]

공개키 암호 시스템은 사용자의 정보와 난수 값인 공개키를 결합하는 인증서를 필요로 한다. 이와 달리 ID(identity) 기반 암호 시스템은 사용자의 메일주소와 같은 ID를 공개키로 사용하여 별도의 인증 없이 암호화를 가능하게 하였다. 그러나, ID 기반 암호 시스템에서 모든 사용자의 비밀키가 키 생성 기관(Key Generation Center, KGC)에 의해 생성되기 때문에 악의적인 목적을 가진 키 생성 기관에 의해 모든 암호문이 복호화될 수 있는 키 위탁 문제가 존재한다.

[0004]

본 발명에서는 키 생성 기관과 사용자가 함께 참여하여 비밀키를 생성하는 방식을 사용하여 상술한 키 위탁 문제를 해결하고자 한다.

선행기술문헌

특허문헌

[0006]

(특허문헌 0001) 대한민국 등록특허 제10-1652846호 (2016.09.02. 공개)

(특허문헌 0002) 대한민국 등록특허 제10-1327980호 (2013.07.29. 공개)

발명의 내용

해결하려는 과제

[0007] 본 발명이 이루고자 하는 기술적인 과제는 키 생성 서버로부터 수신된 부분 비밀키와 수신 단말이 선택한 비밀값을 이용하여 비밀키 및 공개키를 생성하도록 하여 인증서를 사용하지 않으면서 키 위탁 문제를 해결할 수 있는 무인증서 공개키 기반 암호화 방법 및 키 생성 서버를 제공하는 것이다.

과제의 해결 수단

[0009] 본 발명의 실시 예에 따른 공개키 기반 암호화 방법은 (a) 서버가 공개 상수와 마스터 비밀키를 생성하는 단계, (b) 상기 서버가 수신 단말의 부분 비밀키를 생성하고, 상기 부분 비밀키를 상기 수신 단말로 송신하는 단계, (c) 상기 수신 단말이 비밀값을 선택하는 단계, (d) 상기 수신 단말이 비밀키를 생성하는 단계, (e) 상기 수신 단말이 공개키를 생성하고, 상기 공개키를 상기 송신 단말로 송신하는 단계, (f) 상기 송신 단말이 메시지를 암호화하여 암호문을 생성하고, 상기 암호문을 상기 수신 단말로 송신하는 단계, 및 (g) 상기 수신 단말이 상기 암호문을 복호화하는 단계를 포함한다.

[0010] 또한, 본 발명의 실시 예에 따른 키 생성 서버는 위수가 소수 $q (q > 2^\lambda)$ 인 순환 군(G), G 에 속하는 임의의 생성자 $g, h (g, h \in G)$ 및 해쉬 함수($H: \{0,1\}^* \rightarrow Z_q^*$)를 선택하고, 각각의 $i (i \in \{1, \dots, l+1\})$ 에 대해 임의의 난수($s_i \in Z_q^*$)를 선택하고 계산값($g_i = g^{s_i}$)을 계산하고, 수학적 1에 의해 정의되는 공개 상수($params$)와 수학적 2에 의해 정의되는 마스터 비밀키를 생성하는 설정부 및 각각의 i 에 대하여 $\sum_{i=1}^l t_i = 0$ 을 만족하는 $t_i \in Z_q^*$ 를 선택하고, 수학적 3에 의해 정의되는 벡터 $\vec{x}$ 를 생성하고, 수학적 4를 이용하여 수신 단말의 부분 비밀키(D_A)를 생성하는 부분 비밀키 생성부를 포함한다.

발명의 효과

[0012] 본 발명의 실시 예에 따른 공개키 기반 암호화 방법 및 키 생성 서버에 의할 경우 인증서를 필요로 하지 않으며, 페어링 연산을 수행하지 않기 때문에 효율적인 암호화 기법을 제공할 수 있다.

[0013] 또한, 본 발명에 의할 경우 키 생성 기관이 사용자의 비밀키를 알지 못하기 때문에 키 위탁 문제를 해결할 수 있다.

도면의 간단한 설명

[0015] 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 블록도이다.

도 3은 도 1에 도시된 수신 단말의 기능 블록도이다.

도 4는 도 1에 도시된 암호 시스템 상에서 수행되는 암호화 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0016] 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.

[0017] 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.

[0018] 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.

[0019] 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.

[0020] 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.

[0021] 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.

[0022] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0024] 우선 본 발명에 의한 무인증서 공개키 암호 기법에 대하여 설명하기로 한다.

[0025] 본 발명에서는 결정적 디피-헬만 가정(Decisional Diffie-Hellman Assumption, DDH) 문제를 이용하여 안전성을 증명하였으며 자세한 내용은 다음과 같다. 소수 q 를 위수로 가지는 순환 군(cyclic group) G 에서 DDH는 다음의 두 분포가 주어졌을 때 D_0 과 D_1 을 의미 있는 확률로 구별하는 알고리즘이 존재하지 않는다는 가정이다.

$$D_0 = \{(g, g^a, g^b, g^{ab}) | g \in G, a, b \in \mathbb{Z}_q^*\}$$

$$D_1 = \{(g, g^a, g^b, g^c) | g \in G, a, b, c \in \mathbb{Z}_q^*\}$$

[0029] 본 발명에 의한 무인증서 공개키 암호 기법은 설정 알고리즘(Setup), 부분 비밀키 생성 알고리즘(Partial Private Key Extract), 비밀값 설정 알고리즘(Set Secret Value), 비밀키 생성 알고리즘(Set Private Key), 공개키 생성 알고리즘(Set Public Key), 암호화 알고리즘(Encrypt) 및 복호화 알고리즘(Decrypt)의 일곱 개의 알고리즘으로 구성되어 있으며, 각 알고리즘에 대한 상세한 설명은 다음과 같다.

[0031] 1. 설정 알고리즘($Setup(\lambda, l)$)

[0032] 설정 알고리즘은 보안 상수 λ 와 공모제한 상수 l 을 입력받고 마스터 비밀키 msk 와 공개 상수 $params$ 를 출력한다. 설정 알고리즘은 KGC에 의해 수행되며, 공개 상수 $params$ 는 KGC에 의해 공개되고, 마스터 비밀키 msk 는 안전하게 KGC에 보관된다. 여기서, 공모제한 상수 l 은 KGC가 부분 비밀키를 발급해 줄 수 있는 사용자의 수를 의미할 수 있다.

[0033] 구체적으로, 설정 알고리즘에서는 위수가 소수 q ($q > 2^\lambda$)인 순환 군 G 를 선택하고 G 에 속하는 임의의 생성자 g, h ($g, h \in G$)를 선택한다. 또한, 암호학적 해쉬 함수 H ($H: \{0,1\}^* \rightarrow Z_q^*$)를 선택한다. 각각의 $i \in \{1, \dots, l+1\}$ 에 대해 $s_i \in Z_q^*$ 를 임의로 선택하고, $g_i = g^{s_i}$ 를 계산한다. 여기서, 공개 상수 $params$ 와 마스터 비밀키 msk 를 다음과 같이 생성한다.

$$[0034] \quad params = (G, g, h, \{g_i\}_{i=1}^{l+1}, H)$$

$$[0035] \quad msk = \{s_i\}_{i=1}^{l+1}$$

[0037] 2. 부분 비밀키 생성 알고리즘($Partial\ Private\ Key\ Extract(params, msk, ID_A)$)

[0038] 부분 비밀키 생성 알고리즘은 공개 상수 $params$, 마스터 비밀키 msk 및 사용자 A 의 아이디 $ID_A \in \{0,1\}^*$ 를 입력받아 사용자 A 의 부분 비밀키 D_A 를 출력한다. 부분 비밀키 생성 알고리즘은 KGC에 의해 수행되며, 부분 비밀키 D_A 는 안전한 채널을 통해 사용자 A 의 단말기로 전달된다.

[0039] 즉, 키 생성 기관은 ID 기반 암호 시스템의 비밀키를 생성하는 과정과 동일하게 사용자의 부분 비밀키를 생성할 수 있다. 그러나, 부분 비밀키 생성 알고리즘에서 생성된 사용자의 부분 비밀키 D_A 는 ID 기반 암호 시스템의 비밀키와는 다르게 사용자의 비밀키로 쓰이지 않는다.

[0040] 부분 비밀키 생성 알고리즘의 구체적인 동작을 살펴보면 다음과 같다.

[0041] $\sum_{i=1}^l t_i = 0$ 을 만족하는 $t_i \in Z_q^*$ 를 i ($i = 1, \dots, l$)에 대해 임의로 고른다. 벡터 $\vec{x} = (H(ID_A)^l t_l, H(ID_A)^{l-1} t_{l-1}, \dots, H(ID_A)^2 t_2, H(ID_A) t_1, 1) = (x_1, \dots, x_{l+1}) \in Z_q^{*l+1}$ 를 생성한다. 사용자 A 의 ID_A 에 대한 부분 비밀키 D_A 를 다음과 같이 생성한다.

$$[0042] \quad D_A = (s_x, \vec{x}) = \left(\sum_{i=1}^{l+1} s_i \cdot x_i, \vec{x} \right) = (\langle \vec{s}, \vec{x} \rangle, \vec{x})$$

[0044] 3. 비밀값 설정 알고리즘($Set\ Secret\ Value(params, ID_A)$)

[0045] 비밀값 설정 알고리즘은 공개 상수 $params$ 와 사용자 A 의 아이디 ID_A 를 입력받아 사용자 A 의 비밀값

d_A 를 출력한다. 비밀값 설정 알고리즘은 사용자 A 의 단말기에 의해 수행된다. 즉, 사용자 A 의 단말기는 키 생성 기관이 마스터 비밀키 msk 라는 비밀값을 부분 비밀키를 생성하기 위해 사용한 것처럼 사용자 A 의 비밀값 d_A ($d_A \in Z_q^*$)을 생성한다.

4. 비밀키 생성 알고리즘($Set\ Private\ Key(params, D_A, d_A)$)

비밀키 생성 알고리즘은 공개 상수 $params$, 부분 비밀키 D_A 및 비밀값 d_A 를 입력받아 비밀키 S_A 를 출력한다. 비밀키 생성 알고리즘은 사용자 A 의 단말기에 의해 수행된다. 사용자 A 의 비밀키 S_A 는 다음과 같다.

$$S_A = (\langle \vec{s}, \vec{x} \rangle, \vec{x}, d_A) = (s_x, \vec{x}, d_A)$$

5. 공개키 생성 알고리즘($Set\ Public\ Key(params, d_A)$)

공개키 생성 알고리즘은 공개 상수 $params$ 와 비밀값 d_A 를 입력받아 사용자 A 의 공개키 P_A 를 출력한다. 공개키 생성 알고리즘은 사용자 A 의 단말기에 의해 수행된다. 즉, 사용자 A 의 단말이 비밀키 S_A 를 생성하기 위해 사용한 비밀값 d_A 를 암호화 과정에서 사용해야만 사용자를 위해 암호화된 암호문을 키 생성 기관이 복호화할 수 없게 되며, 이로 인해 키 위탁 문제를 해결할 수 있다. 따라서, 사용자 A 의 단말기는 암호화를 위한 자신의 공개키 P_A 를 자신의 비밀값 d_A 를 사용하여 생성한 후에 공개한다. 사용자 A 의 공개키 P_A 는 다음과 같다.

$$P_A = h^{d_A}$$

6. 암호화 알고리즘($Encrypt(params, M, P_A, ID_A)$)

암호화 알고리즘은 공개 상수 $params$, 사용자 A 의 공개키 P_A , 사용자 A 의 아이디 ID_A 및 메시지 M 을 입력받는다. 만약 P_A 가 정당하다면 암호문 CT 를 출력하고, 그렇지 않다면 $\perp$ 를 출력한다.

구체적으로, 암호화 알고리즘은 임의의 난수 a, b, r ($a, b, r \in Z_q^*$)를 선택하고, 다음과 같이 암호문 CT 을 생성한다.

$$CT = \langle g^r, (P_A)^a \cdot M, \{h^{y_i} \cdot g_i^r\}_{i=1}^{l+1} \rangle = \langle A, B, \{C_i\}_{i=1}^{l+1} \rangle$$

이때 사용된 벡터 $\vec{y}$ 는 다음과 같다.

$$\vec{y} = (bH(ID_A), bH(ID_A)^2, \dots, bH(ID_A)^l, a) = (y_1, \dots, y_{l+1}) \in Z_q^{*l+1}$$

7. 복호화 알고리즘($Decrypt(params, CT, S_A)$)

복호화 알고리즘은 암호문 CT , 공개 상수 $params$ 및 비밀키 S_A 를 입력받는다. 만약 암호문 CT 가 정당하다면 메시지 M 을 출력하고, 그렇지 않다면 $\perp$ 를 출력한다. 암호문 CT 는 다음 수학적식을 이용하여 복호화된다.

$$M = B \times \left(\frac{A^{s_x}}{\prod_{i=1}^{l+1} C_i^{x_i}} \right)^{d_A}$$

본 발명에 의한 암호화 기법이 정확성을 가짐은 다음 수학적식을 통하여 알 수 있다.

$$\left(\frac{A^{s_x}}{\prod_{i=1}^{l+1} C_i^{x_i}} \right)^{d_A} = \left(\frac{g^{rs_x}}{\prod_{i=1}^{l+1} h^{x_i y_i} \cdot (g^{s_i})^{rx_i}} \right)^{d_A} = \left(\frac{g^{rs_x}}{\prod_{i=1}^{l+1} h^{x_i y_i} \prod_{i=1}^{l+1} g^{rx_i s_i}} \right)^{d_A} = \left(\frac{1}{h^{\langle \vec{x}, \vec{y} \rangle}} \right)^{d_A} = \frac{1}{(P_A)^a}$$

도 1은 본 발명의 일 실시 예에 따른 암호 시스템을 도시한다.

도 1을 참조하면, 암호 시스템(10)은 서버(100), 수신 단말(300) 및 송신 단말(500)을 포함한다.

키 생성 서버 등으로 불릴 수도 있는 서버(100)는 설정 알고리즘과 부분 비밀키 생성 알고리즘을 수행한다.

구체적으로, 서버(100)는 설정 알고리즘 또는 설정 단계를 수행하여 공개 상수 $params$ 와 마스터 비밀키 msk 를 생성할 수 있다. 공개 상수 $params$ 는 서버(100)에 의해 공개되거나 수신 단말(300) 및 송신 단말(500)로 전송될 수 있다.

또한, 서버(100)는 부분 비밀키 생성 알고리즘 또는 부분 비밀키 생성 단계를 수행하여 수신 단말(300)의 부분 비밀키 D_A 를 생성하고 생성된 부분 비밀키 D_A 를 수신 단말(300)로 송신할 수 있다. 부분 비밀키 D_A 를 생성하는 과정에서 사용되는 수신 단말(300)의 아이디 ID_A 는 수신 단말(300)로부터 수신될 수 있다.

수신 단말(300)은 비밀값 설정 알고리즘, 비밀키 생성 알고리즘, 공개키 생성 알고리즘 및 복호화 알고리즘을 수행할 수 있다.

구체적으로, 수신 단말(300)은 비밀값 설정 알고리즘 또는 비밀값 설정 단계를 수행하여 수신 단말(300) 또는 수신 단말(300)의 사용자의 비밀값 d_A ($d_A \in Z_q^*$)을 선택할 수 있다. 선택된 비밀값 d_A 는 비밀키 S_A 생성 과정과 공개키 P_A 생성 과정에서 이용될 수 있다.

- [0077] 또한, 수신 단말(300)은 비밀키 생성 알고리즘 또는 비밀키 생성 단계를 수행하여 수신 단말(300) 또는 수신 단말(300)의 사용자의 비밀키 S_A 를 생성할 수 있다. 생성된 비밀키 S_A 는 암호문 CT 을 복호화하는 과정에서 이용될 수 있다.
- [0078] 또한, 수신 단말(300)은 공개키 생성 알고리즘 또는 공개키 생성 단계를 수행하여 수신 단말(300) 또는 수신 단말(300)의 사용자의 공개키 P_A 를 생성할 수 있다.
- [0079] 또한, 수신 단말(300)은 복호화 알고리즘 또는 복호화 단계를 수행하여 송신 단말(500)로부터 수신된 암호문 CT 을 복호화할 수 있다.
- [0081] 송신 단말(500)은 암호화 알고리즘을 수행하여 암호문 CT 를 생성할 수 있다. 구체적으로, 송신 단말(500)은 암호화 알고리즘 또는 암호화 단계를 수행하여 메시지 M 에 대한 암호문 CT 를 생성할 수 있다. 생성된 암호문 CT 은 송신 단말(500)에 의해 수신 단말(300)로 송신될 수 있다.
- [0083] 수신 단말(300)과 송신 단말(500)은 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) 등과 같은 핸드헬드 장치(handheld device)로 구현될 수 있다.
- [0085] 도 2는 도 1에 도시된 서버의 기능 블록도이다.
- [0086] 도 1과 도 2를 참조하면, 서버(100)는 설정부(110)와 부분 비밀키 생성부(130)를 포함한다.
- [0087] 설정부(110)는 설정 알고리즘 또는 설정 단계를 수행하여 공개 상수 $params$ 와 마스터 비밀키 msk 를 생성한다.
- [0088] 구체적으로, 설정부(110)는 위수가 소수 $q (q > 2^\lambda)$ 인 순환 군 G , G 에 속하는 임의의 생성자 $g, h (g, h \in G)$, 및 암호학적 해쉬 함수 $H (H: \{0,1\}^* \rightarrow Z_q^*)$ 를 선택한다. 또한, 설정부(110)는 각각의 $i \in \{1, \dots, l+1\}$ 에 대해 $s_i \in Z_q^*$ 를 임의로 선택하고, $g_i = g^{s_i}$ 를 계산한다. 여기서, 공개 상수 $params$ 와 마스터 비밀키 msk 는 다음 수학식을 이용하여 생성된다.
- [0089]
$$params = (G, g, h, \{g_i\}_{i=1}^{l+1}, H)$$
- [0090]
$$msk = \{s_i\}_{i=1}^{l+1}$$
- [0091] 생성된 공개 상수 $params$ 는 설정부(110)에 의해 공개되거나 수신 단말(300) 및 송신 단말(500)로 송신될 수 있다.
- [0092]
- [0093] 부분 비밀키 생성부(130)는 부분 비밀키 생성 알고리즘 또는 부분 비밀키 생성 단계를 수행하여 수신 단말(300)의 부분 비밀키 D_A 를 생성하고, 생성된 부분 비밀키 D_A 를 수신 단말(300)로 송신할 수 있다. 이때, 부분

비밀키 D_A 생성 과정에서 필요한 수신 단말(300)의 아이디 ID_A 는 수신 단말(300)로부터 수신될 수 있다.

[0094] 구체적으로, 부분 비밀키 생성부(130)는 $\sum_{i=1}^l t_i = 0$ 을 만족하는 $t_i \in Z_q^*$ 를 $i (i = 1, \dots, l)$ 에 대해 임의로 선택하고, 벡터 $\vec{x} = (H(ID_A)^{t_l}, H(ID_A)^{t_{l-1}}, \dots, H(ID_A)^{t_2}, H(ID_A)^{t_1}, 1) = (x_1, \dots, x_{l+1}) \in Z_q^{*l+1}$ 를 생성한다. 또한, 부분 비밀키 생성부(130)는 아래 수학적식을 이용하여 수신 단말(300)의 아이디 또는 수신 단말(300)의 사용자의 아이디 ID_A 에 대한 부분 비밀키 D_A 를 생성할 수 있다.

$$D_A = (s_x, \vec{x}) = \left(\sum_{i=1}^{l+1} s_i \cdot x_i, \vec{x} \right) = (\langle \vec{s}, \vec{x} \rangle, \vec{x})$$

[0096] 부분 비밀키 생성부(130)는 생성된 부분 비밀키 D_A 를 안전한 채널을 통해 수신 단말(300)로 송신할 수 있다.

[0098] 도 3은 도 1에 도시된 수신 단말의 기능 블록도이다.

[0099] 도 1 내지 도 3을 참조하면, 수신 단말(300)은 비밀값 설정부(310), 비밀키 생성부(330), 공개키 생성부(350) 및 복호화부(370)를 포함한다.

[0100] 비밀값 설정부(310)는 비밀값 설정 알고리즘 또는 비밀값 설정 단계를 수행하여 수신 단말(300)의 비밀값 d_A 를 생성할 수 있다. 구체적으로, 비밀값 설정부(310)는 공개 상수 $params$ 와 수신 단말 또는 사용자의 아이디 ID_A 를 입력받아 비밀값 d_A 를 출력한다.

[0102] 비밀키 생성부(330)는 비밀키 생성 알고리즘 또는 비밀키 생성 단계를 수행하여 수신 단말(300) 또는 수신 단말(300)의 사용자의 비밀키 S_A 를 생성할 수 있다.

[0103] 구체적으로, 비밀키 생성부(330)는 공개 상수 $params$, 부분 비밀키 D_A 및 비밀값 d_A 를 입력받아 아래 수학적식에 의해 정의되는 비밀키 S_A 를 생성한다.

$$S_A = (\langle \vec{s}, \vec{x} \rangle, \vec{x}, d_A) = (s_x, \vec{x}, d_A)$$

[0106] 공개키 생성부(350)는 공개키 생성 알고리즘 또는 공개키 생성 단계를 수행하여 수신 단말(300) 또는 수신 단말(300)의 사용자의 공개키 P_A 를 생성할 수 있다.

[0107] 구체적으로, 공개키 생성부(350)는 공개 상수 $params$ 와 비밀값 d_A 을 입력받아 아래 수학적식에 의해 정의되는 공개키 P_A 를 생성한다. 생성된 공개키 P_A 는 공개키 생성부(350)에 의해 공개되거나 송신 단말(500)로 송신될 수 있다.

$$P_A = h^{d_A}$$

[0110] 복호화부(370)는 복호화 알고리즘 또는 복호화 단계를 수행하여 송신 단말(500)로부터 수신된 암호문 CT 을 복호화할 수 있다.

[0111] 구체적으로, 복호화부(370)는 암호문 CT , 공개 상수 $params$ 및 비밀키 S_A 를 입력받고, 아래 수학적식을 이용하여 암호문 CT 를 복호화한다.

$$M = B \times \left(\frac{A^{s_x}}{\prod_{i=1}^{l+1} C_i^{x_i}} \right)^{d_A}$$

[0112]

[0114] 도 2와 도 3에 도시된 서버(100)와 수신 단말(300)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 전문가가 용이하게 추론할 수 있을 것이다.

[0115] 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 "~부"는 소정의 코드로 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것이 아니다.

[0117] 도 4는 도 1에 도시된 암호 시스템 상에서 수행되는 암호화 방법을 설명하기 위한 흐름도이다.

[0118] 도 1 내지 도 4를 참조하면, 서버(100)의 설정부(110)는 보안 상수 λ 와 l 를 입력받고 마스터 비밀키 msk 와 공개 상수 $params$ 를 생성한다(S100). 생성된 공개 상수 $params$ 는 설정부(110)에 의해 공개되거나 수신 단말(300)과 송신 단말(500)로 송신되고, 마스터 비밀키 msk 는 안전하게 서버(100) 내에 보관된다.

[0119] 또한, 서버(100)의 부분 비밀키 생성부(130)는 공개 상수 $params$, 마스터 비밀키 msk 및 수신 단말(300) 또는 사용자의 아이디 ID_A 를 입력받아 부분 비밀키 D_A 를 생성한다(S200). 생성된 부분 비밀키 D_A 는 부분 비밀키 생성부(130)에 의해 안전한 채널을 통하여 수신 단말(300)로 송신될 수 있다.

[0121] 수신 단말(300)의 비밀값 설정부(310)는 공개 상수 $params$ 와 수신 단말(300)의 아이디 ID_A 를 이용하여 비밀값 d_A 를 선택한다(S300).

[0122] 또한, 수신 단말(300)은 공개 상수 $params$, 부분 비밀키 D_A 및 비밀값 d_A 을 이용하여 비밀키 S_A 를 생성하고, 공개 상수 $params$ 와 비밀값 d_A 을 이용하여 공개키 P_A 를 생성한다(S400). 즉, 수신 단말(300)의 비밀키 생성부(330)는 비밀키 S_A 를 생성하고, 수신 단말(300)의 공개키 생성부(350)는 공개키 P_A 를 생성한다. 생성된 공개키 P_A 는 공개키 생성부(350)에 의하여 공개되거나 송신 단말(500)로 송신될 수 있다.

[0124] 암호화된 메시지를 수신 단말(300)로 송신하고자 하는 송신 단말(500)은 공개 상수 $params$, 수신 단말

(300) 또는 수신 단말(300)의 사용자의 공개키 P_A , 및 수신 단말(300) 또는 수신 단말(300)의 사용자의 아이디 ID_A 를 이용하여 메시지 M 을 암호화함으로써 암호문 CT 를 생성할 수 있다(S500). 생성된 암호문 CT 은 송신 단말(500)에 의하여 수신 단말(300)로 송신될 수 있다.

[0126] 송신 단말(500)로부터 암호문 CT 을 수신한 수신 단말(300)의 복호화부(370)는 공개 상수 $params$ 와 비밀키 S_A 를 이용하여 암호문 CT 을 복호화함으로써 메시지 M 을 획득할 수 있다.

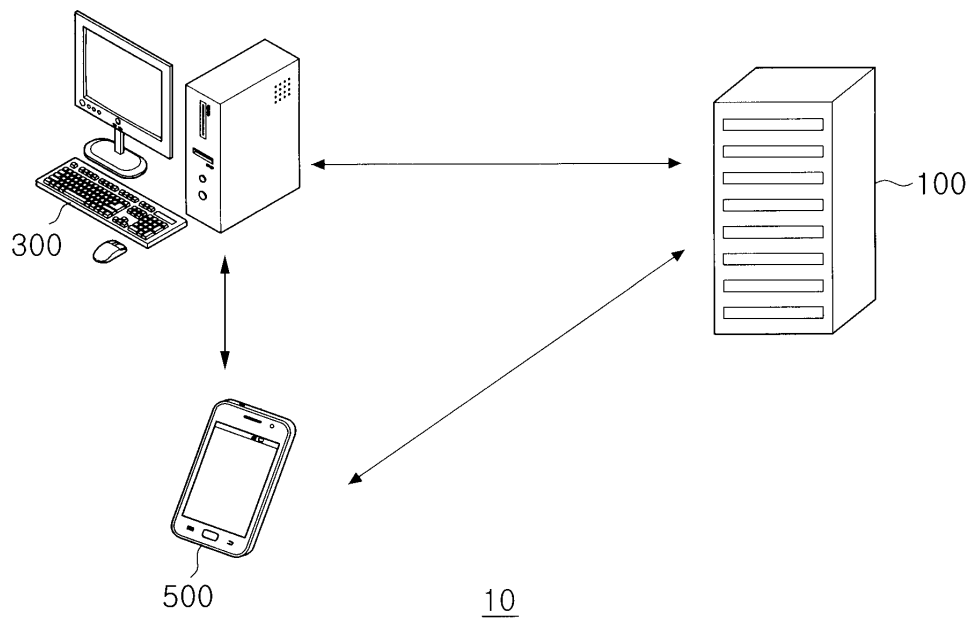
[0128] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

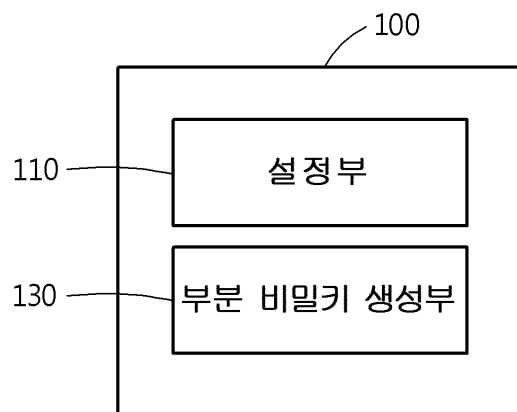
[0130] 10 : 암호 시스템
100 : 서버
110 : 설정부
130 : 부분 비밀키 생성부
300 : 수신 단말
310 : 비밀값 설정부
330 : 비밀키 생성부
350 : 공개키 생성부
370 : 복호화부
500 : 송신 단말

도면

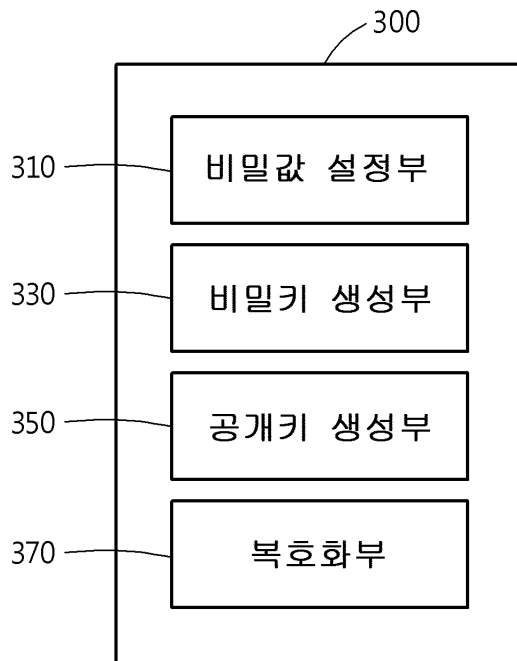
도면1



도면2



도면3



도면4

