

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2014-0029040 (43) 공개일자 2014년03월10일
(51) 국제특허분류(Int. Cl.) H04L 9/12 (2006.01) (21) 출원번호 10-2012-0096673 (22) 출원일자 2012년08월31일 심사청구일자 2012년09월07일	(71) 출원인 고려대학교 산학협력단 서울시 성북구 안암로 145 (안암동) (72) 발명자 이동훈 서울 종로구 사직로8길 34, 1404호 (내수동, 경희 궁의아침3단지) 박승환 서울 동작구 노량진로6마길 8, (노량진동) 김태수 서울 성북구 안암로 145, 정보보호대학원 (안암동5가, 고려대학교) (74) 대리인 특허법인충현	

전체 청구항 수 : 총 10 항

(54) 발명의 명칭 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 시스템 및 방법

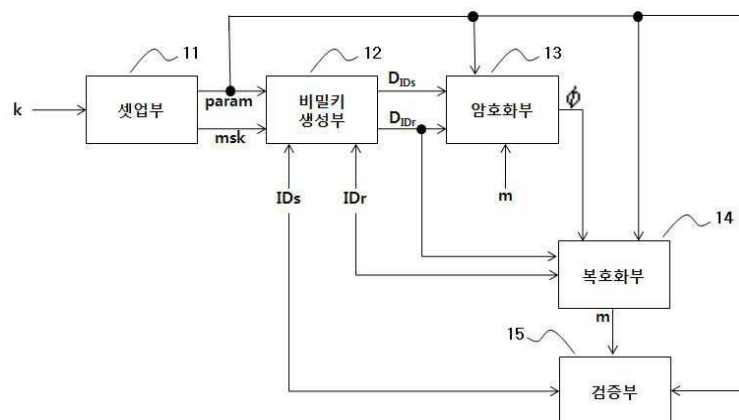
(57) 요약

본 발명은 ID 기반 사인크립션 암호화 기법으로 암호화된 메시지에 대한 외부 공격으로부터의 위변조를 방지하여 상기 메시지의 안전성을 유지시킬 수 있는 시스템에 관한 것이다.

안전성을 유지시키기 위해 개시되는 시스템은 ID 기반 사인크립션에 의한 메시지(m)의 암호화에 이용되는 값들 중 송신자만이 가질 수 있는 값에 대해 해시 함수(hash function)를 적용하여 상기 m의 암호화를 수행하는 암호화부와 상기 m을 복호화하는 복호화부를 포함하고, 상기 암호화부는 상기 복호화부만 획득할 수 있는 값을 암호화에 포함한다.

본 발명에 의한 ID 기반 사인크립션 기법에 따라 메시지를 암호화하는 경우, 암호화에 이용되는 값들 중 송신자만이 가질 수 있는 값에 대해 해시 함수를 적용하여 메시지의 암호화를 수행하고, 아울러 복호화 내지는 검증 과정에서 수신자만 획득할 수 있는 값을 암호화 과정에 포함시키기 때문에 외부 공격으로부터 메시지의 안전성을 유지할 수 있다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	ITAH0301120330070001000100100
부처명	정보통신산업진흥원
연구사업명	대학IT연구센터육성지원사업
연구과제명	스마트 그리드 보안 기술개발
기 여 율	1/1
주관기관	고려대학교 산학협력단
연구기간	2012.01.01 ~ 2012.12.31

특허청구의 범위

청구항 1

ID 기반 사인크립션(ID based signcryption)에 의한 메시지(m)의 암호화에 이용되는 값들 중 송신자만이 가질 수 있는 값에 대해 해시 함수(hash function)를 적용하여 상기 m의 암호화를 수행하는 암호화부를 포함하는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 시스템.

청구항 2

제 1 항에 있어서,

상기 m을 복호화하는 복호화부를 더 포함하고,

상기 암호화부가 상기 m을 암호화하는 경우에는, 상기 복호화부만 얻을 수 있는 값을 상기 m의 암호화에 포함시키는 것을 특징으로 하는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 시스템.

청구항 3

제 2 항에 있어서,

상기 해시 함수는 상기 복호화부만 얻을 수 있는 값에 대해 적용되는 것을 특징으로 하는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 시스템.

청구항 4

제 1 항 내지 제 3 항 중 어느 한 항에 있어서,

상기 m의 암호화는 표준 모델(standard model)에서 적용되는 것을 특징으로 하는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 시스템.

청구항 5

제 4 항에 있어서,

상기 복호화부만 얻을 수 있는 값(T_1)은 다음의 식에 의한 것임을 특징으로 하는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 시스템.

$$e(g_1, g_2)^{s_1} = T_1$$

여기서 $e()$ 는 어드미서블 곱선형 함수(admissible bilinear map)이고, g_1, g_2 는 상기 곱선형 함수와 관련된 순

환군(cyclic group)에서 선택된 임의의 난수이며, s_1 은 소수 p 를 위수(位數)로 갖는 $\mathbb{Z}_p^*$ 의 임의의 한 원소이다.

청구항 6

ID 기반 사인크립션(ID based signcryption)에 의한 메시지(m)의 암호화에 이용되는 값들 중 송신자만이 가질 수 있는 값에 대해 해시 함수(hash function)를 적용하여 상기 m이 암호화되는 단계를 포함하는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 방법.

청구항 7

제 6 항에 있어서,

상기 m이 복호화되는 단계를 더 포함하고,

상기 m이 암호화되는 단계에는 상기 복호화 단계에서만 얻을 수 있는 값이 포함되는 것을 특징으로 하는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 방법.

청구항 8

제 7 항에 있어서,

상기 해시 함수는 상기 복호화 단계에서만 얻을 수 있는 값에 대해 적용되는 것을 특징으로 하는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 방법.

청구항 9

제 6 항 내지 제 8 항 중 어느 한 항에 있어서,

상기 m의 암호화는 표준 모델(standard model)에서 적용되는 것을 특징으로 하는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 방법.

청구항 10

제 9 항에 있어서,

상기 복호화 단계에서만 얻을 수 있는 값(T_1)은 다음의 식에 의한 것임을 특징으로 하는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 방법.

$$e(g_1, g_2)^{s_1} = T_1$$

여기서 $e()$ 는 어드미시블 곱선형 함수(admissible bilinear map)이고, g_1, g_2 는 상기 곱선형 함수와 관련된 순

환군(cyclic group)에서 선택된 임의의 난수이며, s_1 은 소수 p 를 위수(位數)로 갖는 $\mathbb{Z}_p^*$ 의 임의의 한 원소이다.

명세서

기술 분야

[0001] 본 발명은 ID 기반 사인크립션 암호화 메시지의 안전성(security)을 유지하는 시스템 및 방법에 관한 것으로, 보다 상세하게는 사인크립션 암호화 기법으로 암호화된 메시지에 대한 외부 공격으로부터의 위변조를 방지하여 상기 메시지의 안전성을 유지시킬 수 있는 시스템 및 방법에 관한 것이다.

배경 기술

[0002] 사인크립션(Signcrypt) 암호화 기법은 메시지의 암호화(encryption)와 메시지에 대한 서명(signature)을 동시에 제공할 수 있는 암호화 기법으로서, 암호화 스킴(scheme)과 서명 스킴을 독립적 내지는 별개로 적용해야 하는 하이브리드(hybrid) 암호화 기법보다 연산 및 통신비용 측면에서 효율적이다. 사인크립션 기법은 암호화 스킴과 서명 스킴이 같이 요구되는 서비스를 한꺼번에 제공하기 때문에 암호화 스킴에서 고려해야 하는 안전성인 선택 평문 공격(또는 선택 암호문 공격)에 대한 메시지 구분 불가능성(IND-CPA 또는 IND-CCA)과 서명 스킴에서 고려해야 하는 안전성인 선택 메시지 공격에 대한 위조 불가능성(EUF-CMA)을 제공하여야(보장하여야) 한다.

[0003] 사인크립션 기법은 공개키 구조(PKI) 기반의 암호화 시스템에서 연구가 시작되었으며, 이후 ID 기반(IDentity-based) 암호화 기법과 결합된 ID 기반 사인크립션 기법이 제안되었다.

[0004] ID 기반 암호화 기법은 PKI 기반의 암호화 기법에서 인증서 관리에 대한 문제를 해결하기 위하여 제안되었다. PKI 기반 암호화 기법에서는 사용자가 생성한 임의의 공개키에 대하여 신뢰할 수 있는 인증기관이 발급해주는 공개키 인증서가 필요한데, ID 기반 암호화 기법은 사용자의 이름, 전화번호, 이메일 등과 같은 사용자의 신원 정보를 공개키로 사용하므로 이러한 사용자 공개키에 대응하는 비밀키를 안전하게 발급해주는 신뢰할 수 있는 제3의 기관인 키 발급 기관(KGC : Key Generation Center)이 필요하다. ID 기반 암호화 기법은 송신자와 수신자

의 메시지 송수신 과정에서 인증서 교환이나 확인 등의 작업이 필요하지 않기 때문에 PKI 기반의 암호 시스템보다 편리하고 효율적이라 볼 수 있다. 이와 같은 이유로 ID 기반 암호화 기법은 암호화와 전자서명 분야 및 기타의 다양한 분야에서 적용되고 있다.

[0005] 한편 해시 함수(Hash function)가 제공하는 안전성에 의존하는 랜덤 오라클 모델(Random oracle model)에서 증명 가능한 안전성을 갖는 ID 기반 사인크립션 기법이 제안된바 있으며, 랜덤 오라클 모델을 사용하지 않은 표준 모델(Standard model)에서 증명 가능한 안전성을 갖는 ID 기반 사인크립션 기법이 제안되기도 하였다. 하지만, 지금까지 제안된 여러 ID 기반 사인크립션 기법 중에 표준 모델에서 메시지의 안전성을 보장할 수 있는 ID 기반 사인크립션 기법은 없음이 밝혀지기도 하였다(S. S. D. Selvi, S. S. Vivek, D. Vinayagamurthy, and C. P. Rangan On the Security of ID Based Signcryption Schemes. <http://eprint.iacr.org/2011/664>, 2011).

[0006] 한편 암호학에서는 안전성을 증명(보장)하기 위해 공격자에게 주어지는 환경과 목적을 정의하여 안전성 모델(security model)을 설정하고, 대수적 어려움에 기반하여 안전성을 증명해왔다. 안전성 증명은 용이하지 않기 때문에 타당하게 잘 정의된 안전성 모델을 조금 변화시키던가 증명이 가능한 다른 어려운 문제를 찾는다면가 해서 암호 기법들을 설계하고 안전성을 증명해왔다. 여기서 일반적으로 많이 사용되는 어려운 문제(hard problem)에 기반하여 수정되지 않은 본래 정의된 안전성 모델을 이용하면 안전성 모델의 표준 모델(standard model)에서 안전하다고 말할 수 있다. 랜덤 오라클 모델은 공격자에게 해시 오라클이 추가되어 있는 모델로서 안전성 증명을 하기에 조금 더 수월한 모델이지만, 랜덤 오라클에서 증명된 기법보다 표준 모델에서 증명되는 암호화 기법이 더 안전하고 암호학적으로 의미가 있다고 볼 수 있다.

[0007] 표준 모델에서 적용되는 기존의 ID 기반 사인크립션 기법들은 서명 질의(sign query)를 통해 얻은 암호문 조장을 통해서 서명을 위조하거나 구분 불가능성 또는 위조 불가능성 게임에서 챌린지 메시지에 대한 검증 테스트를 통해 공격자가 메시지를 구분할 수 있었다. 즉, 구분 불가능성과 위조 불가능성이 보장되지 아니하여 결국 메시지에 대한 기밀성과 무결성이 보장되지 아니하여 메시지의 안전성(security)이 훼손될 수 있는 심각한 문제를 내포하고 있다.

발명의 내용

해결하려는 과제

[0008] 따라서 본 발명은 상기와 같은 문제를 해결하기 위해 창안된 것으로, 본 발명이 해결하고자 하는 과제는 표준 모델에서 ID 기반 사인크립션 기법에 의해 암호화된 메시지의 기밀성과 무결성을 확보하여 메시지의 안전성 훼손을 방지할 수 있는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 방안을 제시하는 것이다.

과제의 해결 수단

[0009] 상기와 같은 과제를 해결하기 위해 개시되는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 시스템은 ID 기반 사인크립션에 의한 메시지(m)의 암호화에 이용되는 값들 중 송신자만이 가질 수 있는 값에 대해 해시 함수(hash function)를 적용하여 상기 m의 암호화를 수행하는 암호화부를 포함하여 상기한 과제를 해결한다. 아울러 개시되는 시스템은 상기 m을 복호화하는 복호화부를 더 포함하고, 상기 암호화부는 상기 복호화부만 획득할 수 있는 값을 암호화에 포함시켜 상기한 과제를 해결한다.

[0010] 상기한 과제를 해결하기 위해 개시되는 ID 기반 사인크립션 암호화 메시지의 안전성을 유지하는 방법은 ID 기반 사인크립션에 의한 메시지(m)의 암호화에 이용되는 값들 중 송신자만이 가질 수 있는 값에 대해 해시 함수(hash function)를 적용하여 상기 m이 암호화되는 단계를 포함하여 상기한 과제를 해결한다. 아울러 개시되는 방법은 상기 m이 복호화되는 단계를 더 포함하고, 상기 복호화되는 단계에서만 획득할 수 있는 값이 상기 암호화되는 단계에 포함되어 상기한 과제를 해결한다.

발명의 효과

[0011] 본 발명에 의한 ID 기반 사인크립션 기법에 따라 메시지를 암호화하는 경우, 암호화에 이용되는 값들 중 송신자만이 가질 수 있는 값에 대해 해시 함수를 적용하여 메시지의 암호화를 수행하고, 아울러 복호화 내지는 검증 과정에서 수신자만 획득할 수 있는 값을 암호화 과정에 포함시키기 때문에 외부 공격으로부터 메시지의 안전성을 유지할 수 있다.

도면의 간단한 설명

- [0012] 도 1은 본 시스템 발명의 구성을 제시한 도면이다.
도 2는 본 방법 발명의 구성을 제시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0013] 본 발명을 실시하기 위한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하려는 과제의 해결 방안의 개요를 우선 제시한다.
- [0014] 본 발명은 외부 공격으로부터 안전하며, 표준 모델에서 메시지의 안전성을 확보할 수 있는(안전성의 훼손이 발생할 수 없는) ID 기반 사인크립션 기법을 제안하는 것으로, 선택 메시지 공격에 대한 위조 불가능성(EUF-CMA)을 확보할 수 있으며, 선택 평문 공격에 대한 메시지 구분 불가능성(IND-CPA)을 확보할 수 있도록 하는 것이다.
- [0015] 이는 메시지 m 의 암호화에 이용되는 값들 중 송신자만이 가질 수 있는 값에 대해 해시 함수(hash function)를 적용하여 메시지 m 의 암호화를 수행하고, 아울러 복호화 내지는 검증 과정에서 수신자만 획득할 수 있는 값을 암호화 과정에 포함시키는 것으로써 메시지의 안전성을 유지하는 것이다.
- [0016] 이하, 본 발명을 실시하기 위한 구체적인 내용을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면 상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.
- [0017] ID 기반 사인크립션 기법은 크게 셋업 단계, 비밀키 생성(발급) 단계, 암호화 단계, 복호화 단계, 검증 단계인 5단계로 구현된다. 본 발명은 이 중에서 특히 암호화 단계에서 요구되는 값에 소정의 조작을 행하고, 복호화 단계에서 수신자만이 얻을 수 있는 값을 암호화 단계에 포함시켜 표준 모델에서 적용되는 기존의 ID 기반 사인크립션 기법이 가진 문제점인 안전성 훼손의 우려를 제거하고자 한다.

[0018] <셋업 단계: $\text{Setup}(1^k)$ >

[0019] 본 단계는 메시지의 암호화 및 복호화, 서명의 유효성을 검증하는데 필요한 값들을 생성하는 단계(s21)로, 이를 위해 셋업부(11)는 보안 상수 k 를 입력으로 받아 마스터 비밀키 msk 와 공개 상수 param 을 생성(출력)하여 메시지의 암호화 및 복호화, 서명의 유효성을 검증하는데 필요한 값들을 생성한다. 이때 생성은 다음과 같이 이루어질 수 있다.

[0020] 곱선형 함수(Bilinear Maps)와 관련된 순환군(cyclic group)들 (G_1, G_T, e) 을 생성한다. 이때 G_1 과 G_T 는 소수 (prime number) p 를 위수(位數)로 가지며, g 는 G_1 의 생성원이다. $e: G_1 \times G_1 \rightarrow G_T$ 는 어드미서블 곱선형 함수(admissible bilinear map)이다. G_1 의 임의의 생성원 g 를 선택한다.

[0021] 임의의 난수 $a(\in \mathbb{Z}_p^*)$ 를 선택하여($\mathbb{Z}_p^*$ 는 $\mathbb{Z}_p$ 에서 0을 제외한 값의 집합으로 예를 들어, 소수 p 가 7

이면 $\mathbb{Z}_p$ 는 $\{0, 1, 2, 3, 4, 5, 6\}$ 이고, $\mathbb{Z}_p^*$ 는 $\{1, 2, 3, 4, 5, 6\}$ 이다) $g_1 = g^a$ 를 만족하는 g_1 을 생성하고, G_1 에서 임의의 난수들 g_2, u', m', t' 를 선택하고, G_1 에서 원소가 임의의 난수로 이루어진 각각 길이 n_u, n_m, n_t 를 갖는 벡터 $u = (u_i), m = (m_i), t = (t_i)$ 를 선택한다. 또한 암호화적인 해시 함수 $H_1: G_T \rightarrow \mathbb{Z}_p^*$ 와

$H_2: G_T \times G_1 \rightarrow \{0, 1\}^*$ 를 선택한다. 이로부터 공개 상수 param 와 마스터 비밀키 msk 를 다음과 같이 생성

한다.

$$param = (g, g_1, g_2, u', m', t', u, m, t, H_1, H_2) \quad msk = g_2^a$$

[0022]

<비밀키 생성(발급) 단계: Extract(param, msk, ID)>

[0023]

이 단계는 메시지 m의 송신자의 서명용 비밀키(D_{ID_s})와 수신자의 메시지 복호화 비밀키(D_{ID_r})를 생성하여 각각 송신자(암호화부(11))와 수신자(복호화부(12))에 발급하는 단계(s22)이다. 비밀키 생성부(12)는 두 비밀키를 다음과 같이 생성할 수 있다.

[0024]

셋업 단계에서 생성된 공개 상수 param, 마스터 비밀키 msk 및 송신자와 수신자 각각의 ID(ID_s , ID_r)를 입력으로 받는다. u를 ID를 표현하는 길이 n_u 인 비트 문자열(bit string)로 정의하며 $u[i]$ 를 u의 i번째 비트 값으로 정의

[0025]

하고, $U \subset \{1, 2, \dots, n_u\}$ 를 $u[i]=1$ 인 i의 집합이라 정의한다. 한편 u에 대해서는 두 개가 정의되는데 u_r 은 수신자의 ID를, u_s 는 송신자의 ID를 표현하는 비트 문자열(비트 문장)이다.

임의의 난수 $r_1, r_2 (\in Z_p^*)$ 를 선택하고, 송신자의 서명용 비밀키(D_{ID_s})와 수신자의 복호화 비

[0026]

밀키(D_{ID_r})는 다음과 같이 생성될 수 있다.

$$D_{ID_s} = (ssk_1, ssk_2) = (g_2^a (u' \prod_{i \in U_s} u_i)^{r_2}, g^{r_2}), \quad D_{ID_r} = (d_1, d_2) = (g_2^a (u' \prod_{i \in U_r} u_i)^{r_1}, g^{r_1})$$

[0027]

$$Signcrypt(param, m, D_{ID_s}, ID_r)$$

<암호화 단계:>

[0028]

이 단계는 메시지(m)을 사인크립션 기법으로 암호화한 암호문 Φ 을 생성하는 단계(s23)로, 암호화부(13)는

[0029]

암호문 Φ 를 다음과 같이 생성할 수 있다. 암호화부(13)는 본 발명에서 송신자의 핵심 구성 요소에 해당하는 것으로 이하 두 용어를 혼용하기로 하며, 후술할 복호화부(14)도 본 발명에서 수신자의 핵심 구성 요소에 해당되기 때문에 두 용어를 혼용하기로 한다.

공개 상수 param, 메시지 $m (\in Z_p^*)$, 송신자의 서명용 비밀키 D_{ID_s} 와 수신자의 아이디 ID_r 를 입력으로 받는다. t를 해시(hash)를 표현하는 길이 n_t 인 비트 문자열로 정의하며 $t[i]$ 를 t의 i번째 비트 값으로 정의

[0030]

하고, $T(\subset \{1, 2, \dots, n_t\})$ 을 $t[i]=1$ 인 i 의 집합이라 정의한다. 아울러 메시지 m 이 길이 n_m 인 비트 문자열

일 때 $m[i]$ 를 m 의 i 번째 비트 값으로 정의하고, $M(\subset \{1, 2, \dots, n_m\})$ 를 $m[i]=1$ 인 i 의 집합이라 정의한다.

[0031] 임의의 난수 $s_1, s_2 (\in Z_p^*)$ 를 선택한 후 메시지 m 에 사인크립션 기법을 적용하여 암호화되는 암호문

Φ 을 다음과 같이 생성할 수 있다.

$$e(g_1, g_2)^{s_1} = T_1, H_1(T_1) = T_2, H_2(T_1, g^{s_2}) = T_3 \quad \text{--- 식(1).}$$

$$\Phi = (\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6) \quad \text{--- 식(2).}$$

[0034] 여기에서, $H_1()$ 과 $H_2()$ 는 해시 함수(hash function)를 의미하며, ϕ_1 내지 ϕ_6 은 각각 다음과 같다.

$$\phi_1 = (u' \prod_{i \in U_r} u_i)^{s_1}, \quad \phi_2 = T_2 \cdot m, \quad \phi_3 = g^{s_1}.$$

$$\phi_4 = ssk_1 \cdot (t' \prod_{i \in T} t_i)^{s_1} \cdot (m' \prod_{i \in M} m_i)^{s_2}, \quad \phi_5 = ssk_2, \quad \phi_6 = g^{s_2}.$$

[0036] 본 발명에 의한 ID 기반 사인크립션 기법이 기존의 ID 기반 사인크립션 기법과 뚜렷이 구별되는 점 중의 하나는

바로 외부 공격으로부터 암호문 Φ 의 조작 가능성을 원천적으로 불가능하도록 하는 점인데, 이는 암호화에 이용되는 값에 해시 함수를 적용한 결과를 암호화에 이용하기 때문이다(암호화 과정에 해시 함수를 적용하기 때문이다). 위의 경우에는 식(1)과 식(2)에 제시된 바와 같이 해시 함수를 적용한 결과값인 T_2, T_3 을 암호화에 이

용하였으며, ϕ_2 와 ϕ_4 의 $(t' \prod_{i \in T} t_i)^{s_1}$ 에 반영되어 있다.

[0037] 해시 함수는 일 방향 함수(one-side function)의 성질을 갖고 있는 것으로, 일 방향 함수는 함수의 출력이 주어 지더라도 입력을 알아낼 수 없는 성질을 가지고 있다. 이러한 성질을 식(1)과 식(2)에 적용하면 입력은 $T_1(g_1,$

$g_2, s_1)$ 과 g^{s_2} 이고 출력은 T_2, T_3 이며, $T_1(g_1, g_2, s_1)$ 과 g^{s_2} 는 송신자(암호화부(13))만 가지고 있

는 고유한 값이기 때문에 제3자가 $T_1(g_1, g_2, s_1)$ 과 g^{s_2} 을 알 수 없으므로 암호문 Φ 의 조작이 원천 적으로 불가능한 것이다.

[0038] 아울러, 자세한 사항은 후술하겠지만, 상기한 T_1 은 암호문 Φ 이 수신자에 의해 복호화될 때 수신자(복호화

$$H_1(T_1)=T_2$$

부(14))만 얻을 수 있게 할 값으로서 해시 함수가 이에 적용되는 것(

$H_2(T_1, g^{s_2})=T_3$)이 메시지 m (암호문 Φ)의 안전성을 유지함에 있어 가장 바람직할 것이다. 왜냐하면 T_1 은 수신자(복호화부(14))만 얻을 수 있도록 해야 하는 값이기 때문에 이 값에 대해서는 나머지 제3자에 대해 기밀성을 확보해야 할 필요성이 보다 더 높기 때문이다.

[0039] 한편 식(1)과 식(2)은 암호화에 이용되는 값들 중 특정한 값을 선택하여 해시 함수를 적용한 일례에 불과하며, 다른 값을 선택하여 해시 함수를 적용할 수 있음은 당업자의 입장에서 자명하다 할 것이다. 본 발명에 의한 암호화 단계에서의 핵심은 궁극적으로 송신자(암호화부(13))만이 가질 수 있는 고유한 값에 대해 해시 함수를 적용하는 것이다.

$$Unsigncrypt(param, \phi, D_{ID_r})$$

[0040] <복호화 단계:

[0041] 수신자(복호화부(14))는 공개 상수 $param$, 암호문 Φ 과 수신자의 복호화용 비밀키 D_{ID_r} 를 입력으로

받아 암호문 Φ 를 다음과 같이 복호화하여 메시지 m 을 얻는다(s24).

$$\phi_2 / H_1 \left(\frac{e(d_1, \phi_3)}{e(\phi_1, d_2)} \right)$$

[0042]

$$= T_2 \cdot m / H_1 \left(\frac{e(g_2^a (u' \prod_{i \in U_r} u_i)^{r_1}, g^{s_1})}{e((u' \prod_{i \in U_r} u_i)^{s_1}, g^{r_1})} \right)$$

[0043]

$$= H_1(e(g_1, g_2)^{s_1}) \cdot m / H_1 \left(\frac{e(g_2^a (u' \prod_{i \in U_r} u_i)^{r_1}, g^{s_1})}{e((u' \prod_{i \in U_r} u_i)^{s_1}, g^{r_1})} \right)$$

[0044]

[0045] = m --- 식(3).

[0046] 사인크립션은 암호에 관한 값, 서명에 관한 값, 암호와 서명 둘 다 연관되어 있는 값의 모임으로 암호문이 표현되는 암호화 기법이므로(암호화 스킴과 서명 스킴이 하나의 알고리즘으로 구현되므로), 복호화된 메시지 m 과 남은 암호문 값들이 그 자체로 서명으로 취급된다. 즉, 서명이 별도로 출력되는 것이 아니다. 따라서 메시지 m ,

암호문 $\phi_3, \phi_4, \phi_5, \phi_6$ 및 복호화 단계에서 정당한 수신자만에 의해 추출되는

$$T_1 = \frac{e(d_1, \phi_3)}{e(\phi_1, d_2)} \text{ 이 서명이라고 볼 수 있다.}$$

[0047] 수신자가 복호화용 비밀키 $\phi_2 = T_2 \cdot m$ D_{ID_r} 를 이용하여 암호문 Φ 를 복호화하는 경우에는, 위에서 본 바와 같이, $\phi_2 = T_2 \cdot m$ 이므로 Φ_2 를 T_2 로 나누어 준다. T_2 는 T_1 의 해시 함수의 출력 값이므로 T_1 은

정당한 수신자만이 자신의 복호화용 비밀키 D_{ID_r} 로 추출해낼 수 있게 되는 것이다. 후술할 서명의 유효성

검증 단계에 T_1 을 추출하는 과정이 제시되어 있는데, $e(t' \prod_{i \in T} t_i, \phi_3)$ 에서 T 가 T_1 이다.

[0048] <검증 단계: Verify(param, m, σ , ID_s)>

[0049] 공개 상수 param, 메시지 m, 서명 σ 과 송신자의 아이디 ID_s 를 입력으로 받아 서명 σ 의 유효성을 검증하는 단계이다(s25). 위에서 복호화된 메시지(m)가 서명으로 취급된다고 하였으므로 본 단계는 메시지의 유효성을 검증하는 단계로도 언급될 수 있다. 검증부(15)는 그 유효성을 다음 식이 만족하는지를 보이는 것으로 검증할 수 있다.

[0050] 암호문 Φ 의 복호화는 식(3)에 의하면 결국 다음의 식으로 단순화될 것이다.

$$\phi_2 / H_1 \left(\frac{e(d_1, \phi_3)}{e(\phi_1, d_2)} \right) = m$$

[0051]

[0052] 한편 상기한 암호화 단계에서 $\phi_2 = T_2 \cdot m$, $H_1(T_1) = T_2$, $e(g_1, g_2)^{s_1} = T_1$ 이므로 수신자측에서 아래의 두 식이 모두 만족하는지 검증되면 서명 σ 은 유효한(valid) 것으로 검증된 것이다.

$$\frac{e(d_1, \phi_3)}{e(\phi_1, d_2)} = T_1$$

[0053]

$$\frac{e(\phi_4, g)}{e(u' \prod_{i \in U} u_i, \phi_5) \cdot e(t' \prod_{i \in T} t_i, \phi_3) \cdot e(m' \prod_{i \in M} m_i, \phi_6)} = e(g_1, g_2)$$

[0054]

[0055] [검증]

[0056]

[0057]

[0058]

[0059]

[0060]

[0061]

[0062]

[0063]

[0064]

$$\frac{e(d_1, \phi_3)}{e(\phi_1, d_2)} = \frac{e(g_2^a(u' \prod_{i \in U_r} u_i)^{r_1}, g^{s_1})}{e((u' \prod_{i \in U_r} u_i)^{s_1}, g^{r_1})} = \frac{e(g_2^a, g^{s_1})e((u' \prod_{i \in U_r} u_i)^{r_1}, g^{s_1})}{e((u' \prod_{i \in U_r} u_i)^{s_1}, g^{r_1})}$$

$$= e(g_1, g_2)^{s_1} = T_1$$

$$\frac{e(\phi_4, g)}{e(u' \prod_{i \in U_s} u_i, \phi_5) \cdot e(t' \prod_{i \in T} t_i, \phi_3) \cdot e(m' \prod_{i \in M} m_i, \phi_6)}$$

$$= \frac{e(g_2^a(u' \prod_{i \in U_s} u_i)^{r_2}(t' \prod_{i \in T} t_i)^{s_1}(m' \prod_{i \in M} m_i)^{s_2}, g)}{e(u' \prod_{i \in U_s} u_i, g^{r_2})e(t' \prod_{i \in T} t_i, g^{s_1})e(m' \prod_{i \in M} m_i, g^{s_2})}$$

$$= e(g_2^a, g)e((u' \prod_{i \in U_s} u_i)^{r_2}, g) \cdot \frac{e((t' \prod_{i \in T} t_i)^{s_1}, g)e((m' \prod_{i \in M} m_i)^{s_2}, g)}{e(u' \prod_{i \in U_s} u_i, g^{r_2})e(t' \prod_{i \in T} t_i, g^{s_1})e(m' \prod_{i \in M} m_i, g^{s_2})}$$

$$= e(g_2^a, g)$$

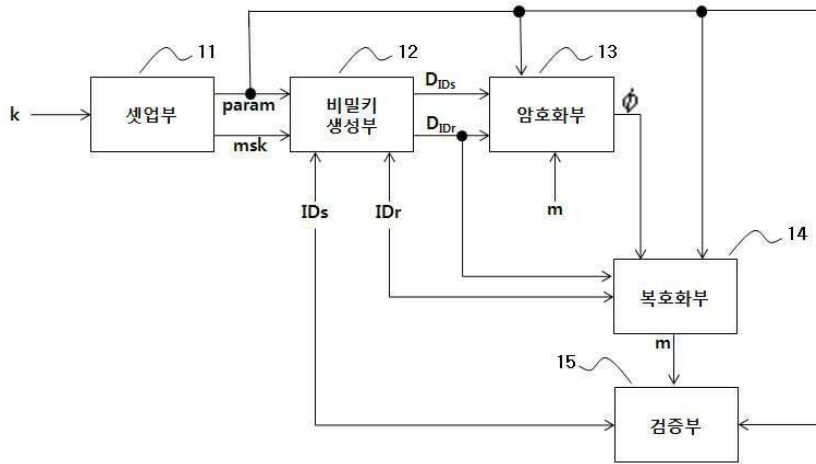
접선형 함수의 성질에 의해 $e(g_2^a, g) = e(g_1, g_2)$. 따라서 서명 σ 의 유효성이 검증되었다.

본 방법발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 유무선 네트워크를 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예는 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

도면1



도면2

