(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
*G06F 15/00* (2006.01)

(45) 공고일자 2007년05월16일
(11) 등록번호 10-0718489
(24) 등록일자 2007년05월09일

(21) 출원번호 10-2005-0017472
(22) 출원일자 2005년03월02일
심사청구일자 2005년03월02일

(65) 공개번호 10-2006-0043347
(43) 공개일자 2006년05월15일

(30) 우선권주장 04290558.8 2004년03월02일 유럽특허청(EPO)(EP)

(73) 특허권자 프랑스 텔레콤
프랑스, 에프-75015 파리, 프라스 달러레, 6

(72) 발명자 까나르드 세바스티엥
프랑스 14000 쌩 알렉산드레 비조 15번가

가우드 마티
18 뀌 데 잘레 14470 꾸셀레 수 메 프랑스

떼라우레 자뀌
프랑스 61100 새인트 조지 데 그로셀레즈 23 아비뉴데라 쉬제 노르망디

(74) 대리인 심서래
정순옥

(56) 선행기술조사문헌
EPO 조사보고서
JP2000242170 A
KR1020000033345 A
KR1020010108919 A
KR1020030095751 A
JP2000235341 A
KR1019990053065 A
KR1020010017358 A
KR1020020003059 A

심사관 : 여원현

전체 청구항 수 : 총 15 항

# (54) 신규의 공정한 은닉 서명을 위한 서명 방법, 컴퓨터 프로그램, 장치 및 서명 시스템

(57) 요약

공정한 은닉 서명 방법에서, 사용자는 $A^e = a_0 a_1^x a_2^m a_3^{x_u} a_4^t a_5^s \pmod n$과 같은 7개의 요소로 된 집합 (A,e,s,t,$x_u$,x,m)을 완성시키기 위해 서명자와 상호작용을 한다. 여기서 $a_0$, $a_1$, $a_2$, $a_3$, $a_4$와 $a_5$ 및 n은 서명자의 공개키($PUBK_S$:Signer's public key)의 요소들이다. 서명-발행 단계 동안, 사용자(U:user)는 서명자(S:signer)에게 신뢰기관(TA:trusted authority)에 알려진

키(f)에 따라 암호화된 데이터 요소($a_1^x$)를 제공한다. 그리고 이 데이터 요소($a_1^x$)는 서명된 메시지가 전송되는 동안에 나타난다. 마찬가지로, 서명된 메시지는 신뢰기관(TA)에 알려진 키(f)에 따라 암호화된 두 번째 데이터 요소($a_3^{x_u}$)를 구성하는 두 번째 암호화된 데이터와 결합되어 전송된다. 그리고 이 두번째 데이터 요소($a_3^{x_u}$)는 서명-발행 단계 동안에 서명자에게 나타난다. 따라서, 신뢰기관(TA)은 디지털 서명의 익명성을 취소할 수 있다.

대표도

도 1

## 특허청구의 범위

### 청구항 1.

서명-발행 단계에서 사용자 장치가 다수의 서명자 장치로 이루어진 서명자 장치군과 상호작용하는 공정한 은닉 서명 설계, 메시지에 있는 공정한 은닉 디지털 서명을 얻기 위해 공개키를 가지고 있는 상기 서명자 장치군과 디지털 서명의 익명성을 취소할 수 있는 다수의 신뢰기관 장치로 이루어진 신뢰기관 장치군이 있는 공정한 은닉 서명 방법에 있어서,

사용자 장치는 식(1)을 만족시키는 첫번째 내지 일곱번째 요소 A, e, s, t, $x_u$, x와 m으로 구성되는 7개의 요소로 된 집합을 완성시키기 위해 상기 서명자 장치군으로부터 데이터를 전송받고,

식(1) $$A^e = a_0 a_1^x a_2^m a_3^{x_u} a_4^t a_5^s \pmod{n}$$

여기서 $a_0$, $a_1$, $a_2$, $a_3$, $a_4$와 $a_5$ 및 n은 상기 서명자 장치군의 공개키의 요소들이며 상기 서명자 장치군에 의해 생성되고,

m은 서명된 상기 메시지이고,

e와 s는 상기 서명자 장치군에 의해 항상 임의로 선택되는 매개변수들이고,

t와 $x_u$는 사용자 장치에 의해 항상 임의로 선택되는 매개변수들이고,

x는 상기 서명자 장치군에 의해 항상 임의로 선택되는 매개변수와 사용자 장치에 의해 항상 임의로 선택되는 매개변수에 기초하여 사용자 장치에 의해 계산되는 중개값이며,

A는 식(2)에 따라 계산되는 매개변수이고,

식(2) $$A = (a_0 C_2 a_5^s Id_U)^{1/e} \pmod{n}$$

여기서 $C_2$는 식(3)에 따라 사용자 장치에 의해 계산되는 매개 변수이며,

식(3) $$C_2 = a_1^x a_2^m a_4^t \pmod{n}$$

$Id_U$는 상기 사용자 장치와 연관된 사용자를 확인하기 위해 사용자 장치에 의해 계산되는 코드인 것을 특징으로 하는 공정한 은닉 서명 방법.

### 청구항 2.

제 1 항에 있어서,

사용자 장치가 공정한 은닉 서명 설계에 따라 서명된 메시지 m을 제3자 장치에 전송하는 서명 제출 단계로 구성되고, 서명-제출 단계에서 사용자 장치는 제3자 장치에

- 암호화된 형식에 있는 적어도 하나의 첫번째 데이터 요소 $a_3^{x_u}$ 를 포함하는 암호화된 데이터 $E_3$, $E_4$

- A에 있는 약속과

- 식(1)과 같이 정의되는 지식 서명 P를 제출하며,

$$P=SK(\alpha,\beta,\gamma,\delta,\eta,\zeta,\theta,\iota,\varepsilon,\mu : I_{sig} = a_1^{\alpha} \wedge E_3 = a_3^{\varepsilon} f^{\gamma} \wedge E_4 = g^{\gamma} \wedge a_0 I_{sig} a_2^{m} = D_1^{\beta} / (a_3^{\varepsilon} a_4^{\delta} a_5^{\mu} h^{\eta}) \wedge D_2 = g^{\zeta} h^{\theta} \wedge 1 = D_2^{\beta} / (g^{\eta} h^{\iota}) \wedge \beta \in ]2^{l_e-1}; 2^{l_e}[ \wedge \mu \in I_{2^{l_s}} \wedge \alpha \in I_N \wedge \varepsilon \in I_N \wedge \delta \in I_N)(m).$$

식(1)

여기서 $I_{sig}$는 $I_{sig} = a_1^{x} \pmod n$ 에 따라 사용자 장치에 의해 계산되는 매개변수이고,

f는 상기 신뢰기관 장치군의 공개키이고,

g와 h는 상기 서명자 장치군의 공개키의 추가된 요소들이고,

$D_1$은 $w_1$이 사용자 장치에 의하여 항상 임의로 선택되는 매개 변수인 $D_1 = A h^{w_1} \pmod n$ 에 따라 정의되는 매개변수이고,

$D_2$는 $w_2$가 사용자 장치에 의하여 항상 임의로 선택되는 매개 변수인 $D_2 = g^{w_1} h^{w_2} \pmod n$ 에 따라 정의되는 매개변수이고,

$l_e$는 $l_e \geq l_r + 2$ 에 따라 정의되는 길이 매개변수이고, 여기서 $l_r = \max(l_m, l_N)$, $l_m$은 메시지 m의 비트 길이, $l_N$은 $N = \lfloor n/4 \rfloor$ 인 매개변수 N의 비트길이이며,

$l_s$는 $l_s \geq l_n + l_r + l + 3$ 에 따라 정의되는 길이 매개변수이고, 여기서 $l_n$은 n의 비트 길이이고, l은 공정한 은닉 서명 설계에 따라 정의되는 보안 매개변수인 것을 특징으로 하는 공정한 은닉 서명 방법.

## 청구항 3.

제 1 항 또는 제 2 항에 있어서,

공정한 은닉 서명 설계에서 서명-발행 단계 동안 사용자 장치는 상기 신뢰기관 장치군에 알려진 키에 따라 암호화된 적어도 하나의 두번째 데이터 요소로 이루어지는 두번째 암호화된 데이터를 상기 서명자 장치군에 제공하고, 상기 두번째 데이터 요소는 서명된 메시지가 전송되는 동안 나타나며, 공정한 은닉 서명 설계에 의해 상기 신뢰기관 장치군은 서명-발행 과정의 번역으로부터 어떤 디지털 서명이 그것으로부터 생긴 것인지 결정할 수 있는 것을 특징으로 하는 공정한 은닉 서명 방법.

## 청구항 4.

제 2 항에 있어서,

공정한 은닉 서명 설계에서 암호화된 데이터 $E_3$, $E_4$는 상기 신뢰기관 장치군에 알려진 키에 따라 암호화된 적어도 하나의 상기 첫번째 데이터 요소 $a_3^{x_u}$ 로 이루어지고, 적어도 하나의 상기 첫번째 데이터 요소 $a_3^{x_u}$ 는 서명-발행 단계 동안 상기 서명자 장치군에 공개되며, 공정한 은닉 서명 설계에 의해 상기 신뢰기관 장치군은 전송된 서명으로부터 상기 서명이 발행된 서명-발행 과정을 결정할 수 있는 것을 특징으로 하는 공정한 은닉 서명 방법.

## 청구항 5.

제 4 항에 있어서,

공정한 은닉 서명 설계는 사용자-등록 단계로 이루어지고, 상기 사용자-등록 단계 동안 사용자 장치는 사용자 장치와 연관된 사용자를 확인하기 위해 이용하는 매개변수로서 적어도 하나의 상기 첫번째 데이터 요소 $a_3^{x_u}$ 를 상기 신뢰기관 장치군에 제공하는 것을 특징으로 하는 공정한 은닉 서명 방법.

## 청구항 6.

제 1 항 내지 제 5 항 중 어느 한 항에 있어서,

공정한 은닉 서명 설계에서 상기 서명자 장치군은 다수의 서명자 장치들로 구성되고, 상기 서명자 장치의 집합의 협력은 상기 7개의 원소로 된 집합을 완성하는 데이터를 사용자 장치에 제공하기 위해 필요한 것을 특징으로 하는 공정한 은닉 서명 방법.

## 청구항 7.

제 1 항 내지 제 6 항 중 어느 한 항에 있어서,

공정한 은닉 서명 설계에서 상기 신뢰기관 장치군은 다수의 신뢰기관 장치들로 구성되고, 디지털 서명의 익명성의 취소는 상기 신뢰기관 장치들의 집합의 협력에 의해 얻을 수 있는 것을 특징으로 하는 공정한 은닉 서명 방법.

## 청구항 8.

적어도 하나의 사용자 전산 장치, 서명자 전산 장치와 신뢰기관 전산 장치를 포함하는 전산 시스템을 사용할 때, 상기 전산 시스템에 제 1 항 내지 제 7 항 중 어느 한 항에 따르는 공정한 은닉 서명 설계를 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 매체.

## 청구항 9.

사용자가 서명-발행 단계에서 서명자와 상호작용하는 공정한 은닉 서명 설계를 실행하기 위해 사용상 적용된 서명 시스템과, 메시지에 공정한 은닉 디지털 서명을 얻기 위해, 공개키를 가지고 있는 서명자, 디지털 서명의 익명성을 취소할 수 있는 신뢰기관이 있고, 서명 시스템은 적어도 하나의 사용자 장치, 서명자 장치 및 신뢰기관 장치로 구성되며,

여기서 상기 또는 각각의 사용자 장치는 서명-발행 프로토콜을 수행하기 위해 상기 서명자 장치와 협력하도록 적용되고,

신뢰기관 장치와 서명자 장치는 적어도 하나의 추적 프로토콜을 수행하기 위해 협력하도록 적용되는 서명 시스템에 있어서,

상기 서명-발행 프로토콜의 실행은 상기 사용자 장치로 하여금 식(1)을 만족시키는 첫번째 내지 일곱번째 요소 A, e, s, t, $x_u$, x 및 m으로 구성되는 7개의 요소로 된 집합을 완성시키도록 하는 서명자 장치로부터 사용자 장치에 데이터를 제공하고,

식(1) $$A^e = a_0 a_1^x a_2^m a_3^{x_u} a_4^t a_5^s \pmod{n}$$

여기서 $a_0$, $a_1$, $a_2$, $a_3$, $a_4$와 $a_5$ 및 n은 서명자의 공개키의 요소들이며 서명자 장치에 의해 생성되고,

m은 서명된 상기 메시지이고,

e와 s는 서명자 장치에서 항상 임의로 선택되는 매개변수들이고,

t와 $x_u$는 사용자 장치에서 항상 임의로 선택되는 매개변수들이고,

x는 서명자 장치에서 항상 임의로 선택되는 매개변수와 사용자 장치에서 항상 임의로 선택되는 매개변수에 기초하여 사용자 장치에서 계산되는 중개값이며,

A는 식(2)에 따라 계산되는 매개변수이고,

식(2) $$A = (a_0 C_2 a_5^s Id_U)^{1/e} \pmod{n}$$

여기서 $C_2$는 식(3)에 따라 사용자 장치에서 계산되는 매개 변수이며,

식(3) $$C_2 = a_1^x a_2^m a_4^t \pmod{n}$$

$Id_U$는 상기 사용자를 확인하기 위해 사용자 장치에서 계산되는 코드인 것을 특징으로 하는 서명 시스템.

## 청구항 10.

사용자가 서명-발행 단계에서 서명자와 상호작용하는 공정한 은닉 서명 설계에 참여하기 위해 사용상 적용된 사용자 장치와, 메시지에 공정한 은닉 디지털 서명을 얻기 위해, 공개키를 가지고 있는 서명자, 디지털 서명의 익명성을 취소할 수 있는 신뢰기관이 있고, 사용자 장치는 메시지 m을 제공하기 위한 메시지 제공 수단과 선결된 서명-발행 프로토콜에 따라 상기 메시지 m의 서명에 대한 요구를 서명자 장치에 내기 위한 서명 요구 수단으로 구성되며,

여기서 사용자 장치는 서명-발행 프로토콜을 수행하기 위해 서명자 장치와 협력하도록 적용되는 사용자 장치에 있어서,

상기 서명-발행 프로토콜의 실행은 상기 사용자 장치로 하여금 식(1)을 만족시키는 첫번째 내지 일곱번째 요소 A, e, s, t, $x_u$, x 및 m으로 구성되는 7개의 요소로 된 집합을 완성시키도록 하는 서명자 장치로부터 사용자 장치에 데이터를 제공하고,

식(1) $$A^e = a_0 a_1^x a_2^m a_3^{x_u} a_4^t a_5^s \pmod{n}$$

여기서 $a_0$, $a_1$, $a_2$, $a_3$, $a_4$와 $a_5$ 및 n은 서명자의 공개키의 요소들이며 서명자 장치에서 생성되고,

m은 서명된 상기 메시지이고,

e와 s는 서명자 장치에서 항상 임의로 선택되는 매개변수들이고,

t와 $x_u$는 사용자 장치에서 항상 임의로 선택되는 매개변수들이고,

x는 서명자 장치에서 항상 임의로 선택되는 매개변수와 사용자 장치에서 항상 임의로 선택되는 매개변수에 기초하여 사용자 장치에서 계산되는 중개값이며,

A는 식(2)에 따라 계산되는 매개변수이고,

식(2) $$A = (a_0 C_2 a_5^s Id_U)^{1/e} (\mathrm{mod}\ n)$$

여기서 $C_2$는 식(3)에 따라 사용자 장치에서 계산되는 매개 변수이며,

식(3) $$C_2 = a_1^x a_2^m a_4^t \ (\mathrm{mod}\ n)$$

$Id_U$는 상기 사용자를 확인하기 위해 사용자 장치에서 계산되는 코드인 것을 특징으로 하는 사용자 장치.

## 청구항 11.

컴퓨터 장치를 사용할 때, 상기 컴퓨터 장치를 제 10 항에 따르는 사용자 장치를 구성하는 수단으로 기능시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 매체.

## 청구항 12.

사용자가 서명-발행 단계에서 서명자와 상호작용하는 공정한 은닉 서명 설계에 참여하기 위해 사용상 적용된 서명자 장치와, 메시지에 공정한 은닉 디지털 서명을 얻기 위해, 공개키를 가지고 있는 서명자, 디지털 서명의 익명성을 취소할 수 있는 신뢰기관이 있고, 서명자 장치는 메시지 m의 서명에 대한 요구를 사용자 장치로부터 받기 위한 요구 수신 수단과 선결된 서명-발행 프로토콜을 수행하기 위해 상기 사용자 장치와 협력하기 위한 서명-프로토콜-실행 수단으로 구성되는 서명자 장치에 있어서,

상기 서명-발행 프로토콜의 실행은 상기 사용자 장치로 하여금 식(1)을 만족시키는 첫번째 내지 일곱번째 요소 A, e, s, t, $x_u$, x 및 m으로 구성되는 7개의 요소로 된 집합을 완성시키도록 하는 서명자 장치로부터 사용자 장치에 데이터를 제공하고,

식(1) $$A^e = a_0 a_1^x a_2^m a_3^{x_u} a_4^t a_5^s \ (\mathrm{mod}\ n)$$

여기서 $a_0$, $a_1$, $a_2$, $a_3$, $a_4$와 $a_5$ 및 n은 서명자의 공개키의 요소들이며 서명자 장치에서 생성되고,

m은 서명된 상기 메시지이고,

e와 s는 서명자 장치에서 항상 임의로 선택되는 매개변수들이고,

t와 $x_u$는 사용자 장치에서 항상 임의로 선택되는 매개변수들이고,

x는 서명자 장치에서 항상 임의로 선택되는 매개변수와 사용자 장치에서 항상 임의로 선택되는 매개변수에 기초하여 사용자 장치에서 계산되는 중개값이며,

A는 식(2)에 따라 계산되는 매개변수이고,

식(2) $A = (a_0 C_2 a_5^s Id_U)^{1/e} (\mathrm{mod}\ n)$

여기서 $C_2$는 식(3)에 따라 사용자 장치에서 계산되는 매개 변수이며,

식(3) $C_2 = a_1^x a_2^m a_4^t \ (\mathrm{mod}\ n)$

$Id_U$는 상기 사용자를 확인하기 위해 사용자 장치에서 계산되는 코드인 것을 특징으로 하는 서명자 장치.

## 청구항 13.

컴퓨터 장치 사용시, 상기 컴퓨터 장치를 제 12 항에 따르는 서명자 장치를 구성하는 수단으로 기능시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 매체.

## 청구항 14.

사용자가 서명-발행 단계에서 서명자와 상호작용하는 공정한 은닉 서명 설계에 참여하기 위해 사용상 적용된 신뢰기관 장치와, 메시지에 공정한 은닉 디지털 서명을 얻기 위해, 공개키를 가지고 있는 서명자가 있는 신뢰기관 장치에 있어서,

상기 신뢰기관 장치는 상기 사용자로 하여금 식(1)을 만족시키는 첫번째 내지 일곱번째 요소 A, e, s, t, $x_u$, x 및 m으로 구성되는 7개의 요소로 된 집합을 완성시키도록 하는 서명자로부터 사용자에게 데이터를 제공하도록 실행되는 서명-발행 프로토콜에 따라 발행된 디지털 서명의 익명성을 취소하도록 적용되고,

식(1) $A^e = a_0 a_1^x a_2^m a_3^{x_u} a_4^t a_5^s \ (\mathrm{mod}\ n)$

여기서 $a_0$, $a_1$, $a_2$, $a_3$, $a_4$와 $a_5$ 및 n은 서명자의 공개키의 요소들이며 서명자에 의해 생성되고,

m은 서명된 상기 메시지이고,

e와 s는 서명자에 의해 항상 임의로 선택되는 매개변수들이고,

t와 $x_u$는 사용자에 의해 항상 임의로 선택되는 매개변수들이고,

x는 서명자에 의해 항상 임의로 선택되는 매개변수와 사용자에 의해 항상 임의로 선택되는 매개변수에 기초하여 사용자에 의해 계산되는 중개값이며,

A는 식(2)에 따라 계산되는 매개변수이고,

식(2) $A = (a_0 C_2 a_5^s Id_U)^{1/e} (\mathrm{mod}\ n)$

여기서 $C_2$는 식(3)에 따라 사용자에 의해 계산되는 매개 변수이며,

식(3) $C_2 = a_1^x a_2^m a_4^t \ (\mathrm{mod}\ n)$

$Id_U$는 상기 사용자를 확인하기 위해 사용자에 의해 계산되는 코드인 것을 특징으로 하는 신뢰기관 장치.

## 청구항 15.

컴퓨터 장치 사용시, 상기 컴퓨터 장치를 제 14 항에 따르는 신뢰기관 장치를 구성하는 수단으로 기능시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 매체.

명세서

# 발명의 상세한 설명

## 발명의 목적

### 발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 전자 상거래의 보안에 관계된다. 특히, 본 발명은 디지털 서명의 기술적인 분야에 관련된다.

디지털 서명 설계는 사용자와 서명자를 포함하는 공개키 암호 프로토콜이다. 서명자는 비밀 키 및 결합된 공개키를 소유한다. 사용자는 일반적으로 인터넷과 같은 네트워크로 전송을 하기 위하여 메시지를 만든다. 서명자는 메시지의 유효성 또는 신뢰성의 표시로서 메시지의 디지털 서명을 만들기 위해 그의 비밀(또는 개인) 키를 사용한다. 서명의 신뢰성을 확인하기를 바라는 사람은 오직 서명자의 공개키를 사용함으로써 그렇게 할 수 있다.

전통적인 디지털 서명 설계들에서 서명자는 디지털 서명이 사용된 메시지의 내용을 알고 있다. 그리고 서명 알고리즘(예를 들면, 유명한 RSA 알고리즘)은 위조하기에 어렵거나 불가능한 디지털 서명을 생성시키기 위해 사용된다.

은닉 서명 설계에서, 사용자는 서명자로 하여금 메시지의 내용에 대해 정보를 가지고 있도록 하지 않으면서 그의 메시지에 대해 디지털 서명을 얻을 수 있다. Dr. David Chaum 교수에 의해 개발된 유명한 은닉 서명 설계는 EP-A-0 139 313에 설명되어 있다. 은닉 서명 설계들은 금융 기관이 현금의 다음 용도를 추적할 수 있는 것을 막는 방법으로 개인이 금융 기관으로부터 디지털 현금을 구입하는 것을 가능케 하기 위하여 디지털 현금 신청서에의 사용을 위하여 자주 제안된다.

일반적인 은닉 서명 설계에서, 만약 서명자가 다른 사용자들을 위해 많은 서류들에 서명한다면, 그에게 그가 서명한 특정 서류가 주어졌을 때, 그는 언제 또는 누구를 위해 그 서류에 서명했는지 알 수 없을 것이다. 대조적으로, 공정한 은닉 서명 설계(FBSS : fair blind signature scheme)에서는, 한 추가적인 참여자, 즉 하나 또는 그 이상의 신뢰기관들(또는 “심사원들”)이 있다. 그리고 서명자는 어떤 서명이 주어진 서명 과정에서 기인하였는지 신뢰기관(또는 만약 하나 이상이라면 신뢰기관들의 단체)의 도움으로 확인할 수 있다.

만약 서명자가 특정 서명 과정의 기록을 가지고 있으면, 신뢰기관의 도움으로, 그는 그 과정에서 기인하는 서명-메시지 쌍을 확인할 수 있다 : 이것은 "서명 추적"이라고 불린다. 반대로, 만약 서명자가 유효한 특정 메시지-서명 쌍을 가지고 있으면, 신뢰기관의 도움으로, 그는 이것이 생성된 서명 과정을 정할 수 있다 : 이것은 "과정 추적"이라고 불린다.

공정한 은닉 서명 설계들에 사용된 한 구성요소는 "지식의 0-지식 증명"이다. 한 존재("입증자")는 또 다른 존재("확인자")에게 어떤 진술(또는 서술)이 진정하다는 것을 증명할 필요가 있을 지도 모른다. 만약 입증자와 확인자가 알맞은 상호작용식 프로토콜(지식의 상호작용식 입증)을 수행할 수 있으면, 확인자는 진술의 진실성을 확신할 수 있다. 만약, 지식 증명에 참가한 후에도, 확인자가 진술이 무엇인지 전혀 알지 못한다면(확인자는 단지 그것이 진실하거나 또는 “유효”하다는 것만 알고 있다면), 지식 프로토콜의 증명은 "0 지식"이라고 불린다. 후자의 경우에, 확인자는 다른 사람들에게 진술의 유효성을 스스로 입증할 수 없다.

비록 공정한 은닉 서명 설계들이 주어진 디지털 서명을 주어진 사용자에 연결되도록 하더라도, 사용자의 메시지는 여전히 비밀 상태로 있다. 공정한 은닉 서명 설계들은 전자 경매 같이 취소할 수 있는 익명성이 바람직한 경우와, 조직적인 범죄와의 싸움(예를 들어, 돈세탁의 예방)에 주로 제안되었다.

보안을 위하여, 공정한 은닉 서명 설계는 하나 이상 위조불가성, 은닉성 및 추적성(엄격한 취소) 같은 특성들을 가지고 있어야 한다.

"하나 이상 위조불가성"은 비록 고의적인 위조자가 서명자와 k번 상호 작용하였을지라도 공정한 은닉 서명 설계 하에서는 k+ 1번째 유효한 서명을 만드는 것이 계산적으로 어렵다는 사실을 의미한다 (이것은 "(k,k+ 1)-위조불가성"으로 불릴 수 있다). 이 특성은 비록 고의적인 위조자와 서명자 사이의 상호작용이 적합하고 배차 배치하는 방법으로 수행될지라도 지켜져야 한다.
"은닉성"은 특정 유효 디지털 서명을 제공받은 사람(신뢰기관을 제외한)이, 서명을 생기게 한 서명 과정을 처리하였던 사용자의 식별 정보를 생성하는 것이 계산적으로 어렵다는 특성을 의미한다. 마찬가지로, 특정 서명 과정의 기록을 제공받은 사람(신뢰기관을 제외한)이 그 과정에서 만들어진 서명을 확인하는 것은 계산적으로 어렵다.

삭제

삭제

"추적성(엄격한 취소)"은 어떤 사람(서명자를 제외한)이 공정한 은닉 서명 설계로 만들어진 추적 절차를 회피하는 것이 어렵다는 특성을 의미한다. 특히, 모든 사람(서명자를 제외한)이, 신뢰기관에 의하여 추적될 수 없는 또는 신뢰기관에 의하여 유사 사용자에게 맞춰질 수 없는 유효한 서명을 산출하는 것은 계산적으로 어렵다.

삭제

다양한 공정한 은닉 서명 설계들이 제안되었다. 예를 들면, 베를린, Springer-Verlag, 컴퓨터 과학 강의 노트 921호, pp 209– 219, Eurocrypt '95에 있는 '암호학 진보'에서 M. Stadler 등에 의한 "공정한 은닉 서명들"을 보십시오. 그러나, 제안된 설계들의 대부분은 비능률적이고 불안전하거나, 비표준 가정들이 만들어지면 안전하다고 증명될 뿐이다.

삭제

삭제

한 효과적인 공정한 은닉 서명 설계는 Abe와 Ohkubo에 의하여 제안되었다(베를린, Springer-Verlag, 컴퓨터 과학 강의 노트 2248호, pp 583-601, Asiacrypt '01 회보에 있는 "엄격한 취소를 가진 아마도 안전한 공정한 은닉 서명들"을 보십시오).

## 발명이 이루고자 하는 기술적 과제

이 설계의 보안(즉, 서명들의 위조불가성)은 이산 대수 문제에 의존한다. 비록 이 설계가 다항식 보안을 제공하도록 요구될지라도, 사실상 그것은 오직 복대수 보안을 제공한다(즉, 오직 서명들의 복대수 수만 안전하게 발행될 수 있으며, 이 복대수 수는 보안 매개변수의 관점에서 정의가 내려진다).

삭제

본 발명의 제출된 구체적 설명은, 능률적이며 서명들의 다항식 수가 안전하게 발행되도록 하는 공정한 은닉 서명 설계를 제공한다.

본 발명은 첨부한 청구항에 규정된 것처럼 공정한 은닉 서명 설계를 제공한다.

본 발명의 그 이상의 특징과 이점들은, 예로서 주어지고, 제출된 구체적 설명의 공정한 은닉 서명 설계의 주요한 요소들을 가리킨 첨부 도면에 의해 설명되어, 그것에 대해 제출된 구체적 설명인 다음 설명으로부터 명백하게 될 것이다.

본 발명의 제출된 구체적 설명에 따라 공정한 은닉 서명 방법의 상세한 설명을 제공하기 전에, 공정한 은닉 서명 설계들의 기본적인 원리들과 약간의 수학적인 기호법을 상기하는 것은 유용하다.

이것이 이 분야에 유명하기 때문에 여기에서 공정한 은닉 서명 설계(FBSS : fair blind signature scheme)의 공식적인 정의를 내리는 것은 불필요하다고 생각된다. 그러나, 원한다면, 흥미를 가지고 있는 독자는 그러한 정의에 대해 상기에 인용된 Abe와 Ohkubo의 논문을 참조할 수 있다.

삭제

여기서 FBSS가 3가지 유형의 참여자들을 포함하는 것을 상기하는 것은 충분하다고 생각된다 : 메시지들이 서명되기를 바라는 사용자들 U(users), 은닉 디지털 서명들을 생성시키는 서명자(S : signer ), 그리고 "심사원"이라고 불릴 수 있는 신뢰기관(TA : trusted authority ). 본 발명의 공정한 은닉 서명 설계에는 3가지 다른 종류의 프로토콜들이 사용된다 : 사용자가 그가 선택한 메시지의 서명을 얻을 수 있도록 하는, 사용자와 서명자 사이에서 처리되는 서명-발행 프로토콜, 사용자가 메시지와 함께 서명을 제출할 수 있도록 하는, 사용자와 일반인 사이에서 처리되는 서명 제출 프로토콜, 그리고 서명자 S와 신뢰기관 TA 사이에서 처리되는 서명-추적 프로토콜 및/또는 과정-추적 프로토콜이 있는 추적 프로토콜들.

본 발명의 제출된 구체적 설명에 사용된 과정-추적 프로토콜이 신뢰기관으로 하여금 특정한 메시지-서명 쌍으로부터 그 쌍을 만든 서명과정을 처리한 사용자의 동일성을 확인할 수 있게 한다는 것은 주목되어야 한다. 따라서, 이 제출된 프로토콜은 "사용자-추적" 프로토콜로 부를 수 있다. 실제로, 사용자의 추적은 특정한 메시지-서명 쌍을 생성한 서명 과정을 단순히 확인하는 것보다 더 유용하다. (어떤 설계들에서는, 어떤 사용자가 진정한 과정-추적 프로토콜에 의해 확인된 서명 과정을 처리하였는지를 결정하기 위하여 광범위한 데이터 베이스를 통하여 찾는 것이 필요하다.)

삭제

삭제

삭제

아래 설명에서 다음과 같은 수학 표기법이 사용될 것이다 :
$x \in_R E$는 x가 집합 E로부터 항상 임의로 선택됨을 의미한다 - 바꾸어 말하면, x는 균등 분포에 따라 집합 E로부터 임의로 선택된다.

만약 x가 정수이면, |x| 는 x의 이원 크기(또는 길이)를 표시한다.

집합 $I_d$는 0부터 d-1까지의 정수들의 집합을 의미한다. 바꾸어 말하면, 그것은 집합 {0,1,2,..., d-1} 과 같다.

정수 n에 대해, $Z_n$은 n을 법으로 하는 나머지 종류 환을 표시한다. 그리고 $Z_n^*$는 $Z_n$에서 역 요소들의 곱셈 그룹을 표시한다.

집합 $Z_n$에 항상 임의로 선택되는 요소 α에 대해(바꾸어 말하면, $\alpha \in_R Z_n$에 대해), $Z_n^*$에서 α의 차수는 ord(α)로 표시된다.

$Z_n^*$에서 항상 임의로 선택된 요소α에 의하여 생성된(바꾸어 말하면, $\alpha \in_R Z_n^*$에 의하여 생성된) $Z_n^*$의 하위집단은 <α>로 표시된다.

집합 QR(n)은 n을 법으로 하는 모든 이차 방정식 나머지들의 집합을 표시한다.
기호 ‖ 는 2(이진수) 문자열들의(또는 정수들과 그룹 요소들의 2진수 표현들의) 연결을 표시한다.

기호 H는 어떤 편리한 해시 함수를 표시한다.

SK(α : f(α,...))(m)은 메시지 m에 있는 "지식 서명"을 표시한다. 지식 서명 SK(signature of knowledge)를 제공하는 것에 의해, 입증자는 제 3 자("확인자")에게 그가 술어 f을 규정하는 방정식을 만족시키는 값 α를 알고 있다는 것을 증명한다.

삭제

SK(α,β:f(α,...) ∧ g(β,...))(M)은 입증자가, f를 규정하는 방정식과 g를 규정하는 방정식을 만족시키는 값들인 α와 β를 알고 있다는 것을 증명함으로써, 메시지 M(message)에 있는 "지식 서명"을 표시한다.

"지식 서명"은 유명한 Fiat-Shamir의 경험적 지식을 사용하는 지식의 0 지식 증명으로부터 시작된 서명이다 (베를린, Springer-Verlag, 1987, 컴퓨터 과학 강의 노트 263호, pp186-194, Crypto '86 회보에 있는 A. Fiat과 A. Shamir의 "당신 자신을 증명하는 방법 : 확인와 서명 문제들의 실제적인 해결책"을 보십시오). 만약 지식의 근원적인 증명이 안전하면, 거기서부터 획득된 지식 서명은 임의 신탁 모델에서 안전하다고 보여질 수 있다.
지식 서명에 참조된 술어(들) f, g 등의 성질에 따라, 입증자는 지식의 0 지식 증명을 수립하기 위하여 확인자에게 다른 정보를 전송할 필요가 있을 것이다. 19쪽에서 시작하여, 몇몇 예들에는 전형적인 술어들과, 관련 술어를 만족시키는 값의 소유를 증명하기 위하여 입증자에 의하여 전송될 수 있는 정보가 주어질 것이다.

삭제

삭제

발명의 제출된 구체적 설명에 따라 공정한 은닉 서명 설계는 도 1을 참조하여 지금부터 설명될 것이다. 이 시스템은, 디지털 서명들을 발행하는 서명자 S, 그들의 각 메시지들에 대해 (공정한 은닉) 디지털 서명들을 얻으려고 노력하는 사용자들의 복수 U 그리고 디지털 서명들의 익명성을 취소시킬 수 있는 하나 이상의 신뢰기관들 TA를 포함한다는 것이 상기될 것이다.

삭제

## 발명의 구성

도 1은 본 발명의 제출된 구체적 설명에 따라 공정한 은닉 서명 설계를 실행하기 위해 사용된 주요 처리들과 프로토콜들을 가리키는 도표이다.
도 1에서 볼 수 있는 것처럼, 어떤 설계 매개 변수들의 값들이 정해지는 초기 설정 단계가 있다. 이 설정 단계 동안, 값들은 첫번째와 두번째 보안 매개 변수들 l과 $l_p$를 위해 (시스템 설계자에 의해) 선택된다. 그러면, 서명자(S)는 각자가 보안 매개 변수 $l_p$와 동등한 많은 비트들을 가진 임의의 비밀 소수들 p'와 q'를 선택한다. p'와 q'는 값 p = 2p'+ 1 과 q = 2q'+ 1 이 둘 다 소수들인 것으로 선택된다. 서명자는 $PRK_S$=(p', q')를 그의 개인키(또는 "비밀키")로 사용할 것이다. 계수 n은 n = pq 값에 설정된다. 그리고 그 이상의 매개 변수들 N과 $l_n$은 다음 방정식들에 따라 결정된다 :

삭제

삭제

삭제

삭제

삭제

$$N = \lfloor n/4 \rfloor = p'q' + \frac{p'+q'}{2}$$ 그리고 $l_n = 2\, l_p$

서명자 S는, 다른 것들에 관한 이 임의 생성원들의 각각의 이산 대수가 알려지지 않은 QR(n)의 임의 생성원들 $(a_0,a_1,a_2,a_3,a_4,a_5,g,h)$를 또한 선택한다.

설정 단계에서, 신뢰기관은 $y \in_R I_N$을 선택한다 ( 바꾸어 말하면, TA는 집합 {0,1,...,N-1}에서 항상 임의로 선택하는 것에 의해 매개 변수 y를 위한 값을 선택한다). 이 매개 변수 y는 신뢰기관의 개인키가 될 것이다. 그 다음 TA는 다음과 같이 그것의 공개키 f를 계산한다 : $f = g^y \pmod n$.

삭제

삭제

전체적인 공정한 은닉 서명 시스템의 공개키는 PUBK = $(n,a_0,a_1,a_2,a_3,a_4,a_5,f,g,h)$ 이다. 서명자의 공개키는 값 f는 없이 전체적인 시스템의 것과 동일할 것이다 : 즉 그것은 $(n,a_0,a_1,a_2,a_3,a_4,a_5,g,h)$ 와 같다.

삭제

아래 표 1은 설정 단계 동안에 값들이 규정되도록 하는 일부 매개 변수들을 요약한 것이다.

표 1

| 매개 변수 | 기호 | 값 |
|---|---|---|
| 첫번째 보안 매개 변수 | l | (일반적으로) 160 |
| 두번째 보안 매개 변수 | $l_p$ | (일반적으로) 1024 |
| 계수 | n | pq |
| 서명자의 개인키 | $PRK_S$ | $(p',q')$ |
| 서명자의 공개키 | $PUBK_S$ | $(n,a_0,a_1,a_2,a_3,a_4,a_5,g,h)$ |
| 서명자에 의하여 선택된 QR(n)의 임의 생성원들 | $(a_0,a_1,a_2,a_3,a_4,a_5,g,h)$ | |
| 신뢰기관의 개인키 | $PRK_{TA}$ | (0부터 N-1까지의 정수들 집합에서 항상 임의로 선택된) y |
| 신뢰기관의 공개키 | $PUBK_{TA}$ | $f=g^y \pmod n$ |
| 전체적인 FBSS의 공개키 | PUBK | $(n,a_0,a_1,a_2,a_3,a_4,a_5,f,g,h)$ |

설정 단계 후에, 본 발명의 공정한 은닉 서명 시스템은 사용할 준비가 된다. 즉, 서명자는 사용자들을 위해 디지털적으로 메시지들에 서명할 준비가 된다.

비록 본 발명에 필수적이지 않을지라도, 사용자들이 시스템에 등록하는 것은 유용할 수 있다. 이것은 시스템으로 하여금 단순한 과정-추적보다 사용자 추적을 수행할 수 있게 한다. 따라서, 본 발명의 제출된 구체적 설명의 FBSS는 도 1에서 점선으로 된 박스에 의해 표시된 것처럼, 등록 단계를 포함한다.

등록 단계에서, 사용자 U는 비밀 값 $x_u \in_R I_N$을 선택한다 ( 바꾸어 말하면, U는 집합 {0,1,...,N-1}에서 항상 임의로 선택하는 것에 의해 매개 변수 $x_u$를 위한 값을 선택한다). U는 그 다음에 그 자신을 확인하기 위하여 코드 $Id_U$를 계산한다 :

삭제

$$Id_U = a_3^{x_u} \pmod n.$$

사용자는 그 다음에 그가 밑 $a_3$에 대해 $Id_U$의 이산 대수를 알고 있다는 것을 신뢰기관에 증명한다. 이것은 어떤 편리한 처리를 사용하여 수행될 수 있다 (예를 들어, 베를린, Springer-Verlag 1998, 컴퓨터 과학 강의 노트 1403호, pp 422 - 436, Eurocrypt '98 의 회보에 있는 G. Poupard와 J. Stern에 의한 "빈틈없는 인증과 서명 생성에서의 실제 보안 분석" ; 또는 베를린, Springer-Verlag, 컴퓨터 과학 강의 노트 473호, pp 481-486, Eurocrypt 1990의 회보에 있는 M. Girault에 의한 "합성수를 법으로 하는 이산 대수들에 기초한 동일성-근거 확인 설계"를 보십시오). 그 다음에 신뢰기관이 사용자에 의해 제공된 $Id_U$와 증명 모두를 발행한다. 따라서 서명-발행 프로토콜이 실행되는 동안(아래를 보십시오) 사용자가 인증될 수 있도록 한다. 등록 단계는 이제 완비되었다.

삭제

삭제

삭제

도 1이 표시하는 것처럼, 제출된 구체적 설명의 공정한 은닉 서명 설계는 서명-발행 프로토콜, 서명 제출 프로토콜 그리고 서명-추적 프로토콜 및/또는 과정-추적 프로토콜(여기서는, 사용자-추적 프로토콜)을 포함하는 추적 프로토콜들을 포함한다. 분명히 서명-발행 프로토콜은 사용자가 메시지의 서명을 위하여 서명자와 교신할 때마다 사용된다. 그리고 서명 제출 프로토콜은 사용자가 서명된 메시지를 제3자에게 제공할 때마다 사용된다. 반면에 서명-추적과 과정-추적 프로토콜들은 디지털 서명의 익명성을 취소하는 것이 바람직한 경우에 인용될 뿐이다 (예를 들면, 온라인 경매에서 낙찰자의 세목을 검색하는 것이 바람직하기 때문에). 이 프로토콜들은 이제 차례로 고려될 것이다.

삭제

삭제

서명-발행 프로토콜

4개의 길이 매개 변수들 $l_r$, $l_m$, $l_e$ 그리고 $l_s$는 다음 3 관계식을 만족시키도록 규정된다 :

$l_r = \max(l_m, l_N)$

$l_e \geq l_r + 2$

$l_s \geq l_n + l_r + l + 3$

여기서 l은 첫번째 보안 매개 변수이고, $l_n$은 계수 n의 비트-길이이다. 그리고 $l_N$은 설정 단계의 상기 검토에 언급된 매개 변수 N의 비트-길이이다. 서명되어야 하는 메시지 m은 비트-길이 $l_m$의 메시지이다. 바꾸어 말하면 m은 집합 $\{0, 1, \ldots, (2^{l_m}-1)\}$에 있는 정수일 수 있다. 발명의 제출된 구체적 설명에서, 이 길이 매개 변수들의 값을 고정시키는 사람은 서명자이다. 하지만 본 발명은 이 가능성에 제한되지 않는다. 발명의 다른 구체적 설명에서, 다른 상대방들, 예를 들면 신뢰 기관은, 이 길이 매개 변수들의 값을 지정할 수 있다.

삭제

삭제

사용자와 서명자에 의해 상호 작용하여 수행되는 서명-발행 프로토콜은 2성분형 프로토콜로 생각될 수 있다. 서명-발행 프로토콜의 첫번째 부분에서, 사용자와 서명자는 상호작용하고, 사용자는 서명자로부터 어떤 매개 변수 데이터(명료하게는, $\hat{x}$, A, e와 s)를 얻는다. 서명-발행 프로토콜의 두번째 부분에서, 사용자는 서명자로부터 얻어진 매개 변수 데이터를 이용하는 원하던 디지털 서명을 생성시킨다.

삭제

삭제

서명-발행 프로토콜의 첫번째 부분에서, 다음 단계들이 수행된다 :

사용자는 집합 {0, 1, ..., N-1}로부터 항상 임의로 한 매개 변수 $\tilde{x}$와 한 매개 변수 $\tilde{r}$을 선택한다 - 다시 말하면, $\tilde{x} \in_R I_N$ 과 $\tilde{r} \in_R I_N$.

사용자는 다음과 같이 매개 변수 $C_1$과 두 개의 지식 서명들 $U_0$와 $U_1$을 만든다 :

$$C_1 = g^{\tilde{x}} h^{\tilde{r}} \pmod{n},$$

$U_0$ = SK (α,β:$C_1 = g^{\alpha}h^{\beta}(\text{mod } n) \wedge \alpha \in I_N$), 그리고

$U_1$ = SK (α: $Id_U = a_3^{\alpha}(\text{mod } n) \wedge \alpha \in I_N$),

그 다음에, 사용자는 서명자에게 $C_1$, 사용자의 확인 코드 $Id_U$, 그리고 두 개의 지식 서명 $U_0$ 와 $U_1$을 전송한다.

서명자는 두 지식 서명들 $U_0$와 $U_1$을 확인한다. 그 다음, 만약 지식 서명들이 성공적으로 확인되었으면, 서명자는 집합 {0, 1, ..., N-1}에서 항상 임의로 선택하는 것에 의해 매개 변수 $\hat{x}$를 위한 값을 설정한다 - 다시 말하면, $\hat{x} \in_R I_N$. 이 매개 변수는 사용자에게 다시 전송된다.

삭제

삭제

다음으로, 사용자는 매개 변수 $x = \tilde{x} + \hat{x} \ (\text{mod } n)$을 만들기 위하여 서명자로부터 받은 매개 변수 $\hat{x}$를 이용한다.

그 다음에 사용자는 집합 {0, 1, ..., N-1}로부터 항상 임의로 매개 변수 t와 매개 변수 r을 선택한다 - 다시 말하면, $t \in_R I_N$과 $r \in_R I_N$.

그 다음으로 사용자는 다음과 같이 3개의 매개 변수들 $C_2$, $E_1$과 $E_2$, 그리고 2개의 지식 서명 V와 W를 계산한다 :

$$C_2 = a_1^x a_2^m a_4^t \ (\text{mod } n),$$

$$E_1 = a_1^x f^r \ (\text{mod } n),$$

$$E_2 = g^r \ (\text{mod } n),$$

$$V = SK(\alpha,\beta,\gamma,\delta : C_2 = a_1^{\alpha} a_2^{\beta} a_4^{\gamma} \wedge E_1 = a_1^{\alpha} f^{\delta} \wedge E_2 = g^{\delta} \wedge \beta \in I_{2^{l_m}} \wedge \gamma \in I_N),$$ 그리고

삭제

삭제

삭제

삭제

$$W = SK(\alpha,\beta,\gamma,\delta,\theta : C_2 = a_1^{\alpha} a_2^{\theta} a_4^{\delta} \wedge C_1 g^{\hat{x}} = (g^N)^{\beta} g^{\alpha} h^{\gamma} \wedge \alpha \in I_N \wedge$$

$\delta \in I_N \wedge \theta \in I_{2^{l_m}})$.

매개 변수 $E_1$이 신뢰기관의 공개키 f에 따라 암호화된 데이터 $a_1^x$와 일치하는 것이 인지될 것이다. 사용자는 서명자에게 이 세 매개 변수들과 두 지식 서명들($C_2$, $E_1$, $E_2$, V, W)을 전송한다.

삭제

서명자는 2개의 지식 서명, V 와 W를 확인한다. 만약 이 지식 서명 모두가 유효하면, 서명자는 집합 $\{0, 1, .., (I_{2^{l_s}} - 1)\}$에서 항상 임의로 첫번째 매개 변수 s를 선택하고, $2^{l_e - 1}$ 와 $2^{l_e}$ 사이의 소수로 이루어진 집합에서 항상 임의로 두 번째 매개 변수 e를 선택한다. - 바꾸어 말하면 :

삭제

$s \in_R I_{2^{l_s}}$

$e \in_R ]2^{l_e-1}, 2^{l_e}[$ 소수

삭제

그런 후 서명자는 다음과 같이 매개 변수 A를 계산한다 :

$A = (a_0 C_2 a_5^{s} Id_U)^{1/e} \pmod n$

서명자는 다음 관계식이 참인 것을 확인하는 사용자에게 A, e와 s를 전송한다 :

$A^e = a_0 a_1^x a_2^m a_3^{x_u} a_4^t a_5^s \pmod n$

$e \in ]2^{l_e-1}, 2^{l_e}[$

삭제

이 뒤쪽 2개의 확인은 서명-발행 프로토콜의 첫번째 부분을 끝낸다.

서명-발행 프로토콜의 두번째 부분에서 사용자는 그의 메시지 m의 진정한 디지털 서명을 생성시킨다. 이것은 (FBSS에 따라 집합 $\{0, 1, \ldots, (2^{l_m}-1)\}$에서 정수인 메시지 m을 위해 유효한 디지털 서명을 성립시키는) 다음 요소를 만드는 것을 포함한다 :

삭제

삭제

- $I_{sig}$ 값

- ElGamal 암호문 $E = (E_3, E_4)$

- U가 집합$(A, e, s, t, x_u, x)$를 다음과 같이 아는 것을 입증하는 지식 서명, P :

o $(P_1)$ : $I_{sig} = (a_1^{x} \bmod n)$ 그리고 $x \in I_N$

o $(P_2)$ : $A^e = a_0 I_{sig} a_2^m a_4^t a_5^s a_3^{x_u} \pmod n$ 그리고 $x_u$와 t는 $I_N$에 속하며, s 는 $I_{2^{l_s}}$에 속한다.

o $(P_3)$ : E는 $a_3^{x_u} \pmod n$의 암호화

ElGamal 암호문의 특성은 이 분야에 숙련된 사람에게 잘 알려져 있으므로 여기에서 상세하게 설명되지 않을 것이다. 그러나 원하다면, 그 이상의 정보는 Springer-Verlag 1985, 컴퓨터 과학 강의 노트 196호 p 10-18, Crypto'84의 회보에 있는 T. El Gamal, G.R. Blakley와 D. Chaum에 의한 "이산 대수에 기초한 공개키 암호 체계와 서명 설계"에서 찾을 수 있다.

삭제

만약 지식 증명 PK(proof of knowledge)가 유효하면 m에 있는 서명 SK는 유효하다. 비록 사용자가 몇몇 다른 지식 서명들 SK를 만들 수 있을지라도, 메시지 m에 있는 디지털 서명은 사용자와 서명자에 의하여 연합하여 계산되었던 $I_{sig}$값에 의하여 유일하게 결정된다. 만약 m에 있는 두 개의 서명이 각각 다른 $I_{sig}$ 값을 가진다면 이 서명들은 다르다고 생각될 것이다. 만약 m에 있는 두 개의 서명이 같은 $I_{sig}$값을 가지고 있으면 비록 각각의 지식 서명들인 SK가 다를지라도 그것들은 같다고 생각될 것이다.

삭제

삭제

삭제

본 발명의 제출된 구체적 설명에 의하면, 알맞은 지식 서명 SK는 다음과 같이 구성될 수 있다 :
사용자는 $I_{sig} = a_1^{x} \pmod n$을 계산한다.

사용자는 집합 {0, 1, ..., $I_N$-1}에서 항상 임의로 세 개의 매개 변수 w, $w_1$과 $w_2$를 선택한다, 다시 말하면, w, $w_1$, $w_2 \in_R I_N$.

그 다음에 사용자는 다음과 같이 ElGamal 암호문 $E_3$, $E_4$, 그리고 두 개의 다른 매개 변수들 $D_1$과 $D_2$를 계산한다 :

$$E_3 = a_3^{x_u} \; f^{w} \pmod n$$

$$E_4 = g^{w} \pmod n$$

$$D_1 = A h^{w_1} \pmod n$$

$$D_2 = g^{w_1} \; h^{w_2} \pmod n$$

삭제

삭제

삭제

삭제

그리고 지식 서명 SK는 다음과 같이 정의가 내려진다 :

$$P=SK(\alpha,\beta,\gamma,\delta,\eta,\zeta,\theta,\iota,\varepsilon,\mu : I_{sig} = a_1^{\alpha} \wedge E_3 = a_3^{\varepsilon} \; f^{\gamma} \wedge E_4 = g^{\gamma} \wedge a_0 I_{sig} \; a_2^{m} =$$

$$D_1^{\beta} / (a_3^{\varepsilon} \, a_4^{\delta} \, a_5^{\mu} \, h^{\eta}) \wedge D_2 = g^{\zeta} \; h^{\theta} \wedge 1 = D_2^{\beta} / (g^{\eta} \, h^{\iota}) \wedge \beta \in ]2^{l_\varepsilon - 1}; 2^{l_\varepsilon}[ \wedge \mu \in I_{2^{l_\varepsilon}} \wedge$$

$$\alpha \in I_N \wedge \varepsilon \in I_N \wedge \delta \in I_N)(m).$$

삭제

비록 상기 지식 서명이 외관상으로 복잡해 보일지라도, 숙련된 사람은 그것이 상기 정의에서 콜론의 오른쪽에 있는 11개의 술어를 만족시키는 $\alpha$, $\beta$, $\gamma$, $\delta$, $\eta$, $\zeta$, $\theta$, $\iota$, $\varepsilon$와 $\mu$ 값을 사용자가 안다는 것을 보여주는 지식 서명이 된다는 것을 쉽게 이해할 것이다.
숙련된 사람은 이 분야의 일반적인 지식으로부터 지식 서명 SK로부터 특정 술어를 입증하기 위하여 어떤 데이터가 확인자에게 전송되어야 하는지 쉽게 이해할 것이다. 실제로, 이 분야에는 다른 타입 지식의 비밀 부분 소유를 입증하는 지식 서명을 생성시키는 방법에 관해 자세히 알려주는 많은 수의 기술 논문들이 있다, 예를 들어, Springer Verlag 1997, 컴퓨터 과학 강의 노트 1294호, pp.410-424, CRYPTO '97, '암호학 진보'에서 J. Camenisch와 M.Stadler에 의한 "큰 그룹을 위한 능률적인 그룹 서명 설계들"을 보십시오.

삭제

하지만 지금 지식의 비밀 부분이 어떤 특정 형식(아래를 보십시오)을 따를 때, 입증자가 지식의 결합된 비밀 부분을 소유하고 있다는 것을 입증하기에 적합한 지식 서명들을 상기하는 것은 도움이 될 것이다. 이것은 본 발명의 제출된 구체적 설명에 사용된 구조 블록들이라고 생각될 수 있다.

구조 블록 1 - 사용자는 밑 g에 대한 y의 이산 대수인 x를 알고 있다.

사용자가 밑 g에 대한 y의 이산 대수 x를 알고 있는 경우를 생각해 보십시오 (즉, $y = g^x$), g와 y는 모두 그룹 G의 원소들이다.

만약 사용자가 그가 값 x를 누설하지 않고 (밑 g에 대한 y의 이산 대수인) x를 알고 있는 것을 입증하기를 바란다면, 그는 다음과 같이 그렇게 할 수 있다. 우선 그는 집합 $\{0,1,\ldots, I_{\epsilon(l_G+k)}-1\}$에서 항상 임의로 매개 변수 r을 선택한다. 그 다음에 그는 $c = H(g \| y \| g^r \| m)$과 (Z에서) $s = r-cx$에 따라 두 증거 매개 변수 c와 s의 값을 정한다. 만약 입증자가 참으로 이산 대수 값 x를 알고 있고, 증거 매개 변수 c와 s를 만들 때 적합한 값을 사용하였다면, 데이터 쌍 (c,s)는 c와 s가 각각 집합 $I_k \times I_{\epsilon(l_G+k)+1}$의 원소인 방정식 $c = H(g \| y \| y^c g^s \| m)$을 만족시킬 것이다.

삭제

삭제

따라서 만약 사용자가 $c = H(g \| y \| y^c g^s \| m)$을 만족시킨 데이터 쌍 (c,s)의 값을 포함하는 지식 서명을 생성시키면, 이것은 사용자가 메시지 $m \in \{0,1\}^*$에 대하여 밑 g에 관한 y의 이산 대수를 알고 있다는 것을 증명한다. 관계되는 지식 서명은 $SK(\alpha : y= g^{\alpha})(m)$으로 나타낼 수 있다.

구조 블록 2 - 사용자는 밑 g에 관한 $y_1$의 이산 대수이며, 밑 h에 관한 $y_2$의 이산 대수인 x를 알고 있다.

이 경우에 사용자는 $y_1 = g^x$인 것과 $y_2 = h^x$인 것을 알고 있다. 사용자는 다음과 같이 x를 누설하지 않고 이 지식의 소유를 증명할 수 있다.

삭제

삭제

우선 그는 집합 $\{0,1,\ldots, I_{\epsilon(l_G+k)}-1\}$에서 항상 임의로 매개 변수 r을 선택한다. 그 다음 그는 $c = H(g \| h \| y_1 \| y_2 \| g^r \| h^r \| m)$, (Z에 있는) $s = r-cx$ 에 따라 두 증거 매개 변수, c와 s의 값을 정한다. 만약 입증자가 참으로 이산 대수 값 x를 알고 있고, 밑 g에 대한 $y_1$의 이 이산 대수가 밑 h에 대한 $y_2$의 이산 대수와 동일하며, 증거 매개 변수 c와 s을 만들 때 입증자가 x의 적합한 값을 사용하였다면, 각각 집합 $I_k \times I_{\epsilon(l_G+k)+1}$의 원소인 데이터 쌍 (c, s)는 방정식 $c = H(g \| h \| y_1 \| y_2 \| y_1^c g^s \| y_2^c h^s \| m)$을 만족시킬 것이다.

삭제

따라서 만약 사용자가 $c = H(g \| h \| y_1 \| y_2 \| y_1^c g^s \| y_2^c h^s \| m)$을 만족시키는 이 데이터 쌍(c, s)의 값을 포함하는 지식 서명을 만들면, 이것은 사용자가 메시지 $m \in \{0,1\}^*$에 있는 밑 g에 대한 $y_1$의 이산 대수와 밑 h에 대한 $y_2$의 이산 대수를 모두 알고 있다는 것을 증명한다. 대응하는 지식 서명은 $SK(\alpha,\beta:y_1=g_1^{\alpha} \wedge y_2=g_2^{\beta})(m)$으로 표시할 수 있다.

구조 블록 3 - 사용자는 밑 g와 밑 h에 대한 y의 표시인 $x_1$, $x_2$를 알고 있다.

이 경우에 사용자는 $y = g^{x_1}h^{x_2}$ 인 것을 알고 있다. 사용자는 다음과 같이 $x_1$과 $x_2$을 누설하지 않고 이 지식의 소유를 나타낼 수 있다.

삭제

삭제

우선 그는 집합 $\{0,1,\ldots, I_{\epsilon(l_G+k)}-1\}$에서 항상 임의로 두 매개 변수 $r_1$, $r_2$를 선택한다. 그 다음에 그는 $c = H(g \| h \| y \| g^{x_1}h^{x_2} \| m)$, (Z에 있는) $s_1 = r_1 - cx_1$과 $s_2 = r_2 - cx_2$에 따라서 세 증거 매개 변수 c, $s_1$과 $s_2$의 값을 정한다. 만약 입증자가 참으로 밑 g와 밑 h에 대한 y의 표시를 알고 있고, 증거 매개 변수 c, $s_1$과 $s_2$를 만들 때 적합한 값을 사용하였다면, c, $s_1$과 $s_2$는 각각 집합 $I_k \times I_{\epsilon(l_G+k)+1} \times I_{\epsilon(l_G+k)+1}$ 의 원소인 데이터 집합 (c, $s_1$, $s_2$)는 방정식 $c = H(g \| h \| y \| y^c g^{s_1}h^{s_2} \| m)$ 을 만족시킬 것이다.

삭제

따라서 만약 사용자가 $c = H(g \| h \| y \| y^c g^{s_1}h^{s_2} \| m)$ 을 만족시키는 이 데이터 집합 (c, $s_1$, $s_2$)의 값을 포함하는 지식 서명을 만들면, 이것은 사용자가 메시지 $m \in \{0,1\}^*$에 있는 밑 g와 밑 h에 대한 y의 표시를 알고 있다는 것을 증명한다. 대응하는 지식 서명은 $SK(\alpha,\beta : y=g^{\alpha}h^{\beta})(m)$으로 표시될 수 있다.

<u>구조 블록 4 - 사용자는 밑 g에 대한 y의 이산 대수를 알고 있고, 이 이산 대수는 특정한 구간에 있다.</u>

이 경우 사용자는 $y = g^x$인 것과 x가 간격 $]X-2^{\varepsilon(l+k)}, X+2^{\varepsilon(l+k)}[$에 있다는 것을 알고 있다. 사용자는 다음과 같이 x를 누설하지 않고 이 지식의 소유를 증명할 수 있다.

삭제

우선 그는 집합 $\{0,1,\ldots, I_{\epsilon(l_G+k)}-1\}$에서 항상 임의로 매개 변수 r을 선택한다. 그 다음에 그는 $c = H(g \| y \| g^r \| m)$, (Z에 있는) $s = r - c(x-X)$에 따라 두 증거 매개 변수 c와 s의 값을 정한다. 만약 입증자가 밑 g에 대한 y의 이산 대수와 이것이 있는 구간을 참으로 알고 있고, 증거 매개 변수 c와 s을 만들 때 적합한 값을 사용하였다면, 데이터 쌍(c, s)는 c와 s가 각각 집합 $I_k \times I_{\epsilon(l_G+k)+1}$의 원소인 방정식 $c = H(g \| y \| y^c g^{s-cX} \| m)$을 만족시킬 것이다.

삭제

따라서 만약 사용자가 $c = H(g \| y \| y^c g^{s-cX} \| m)$을 만족시키는 이 데이터 쌍(c, s)의 값을 포함하는 지식 서명을 만든다면, 이것은 사용자가 메시지 $m \in \{0,1\}^*$에 있는 밑 g에 대한 y의 이산 대수와 이것이 있는 구간을 알고 있다는 것을 증명한다. 대응하는 지식 서명은 표시될 수 있다 :

$$SK(\alpha : y = g^{\alpha} \wedge \alpha \in ]X-2^{\epsilon(l+k)}, X+2^{\epsilon(l+k)}[\,)(m)$$

<u>서명-제출 프로토콜</u>

공정한 은닉 서명 시스템 FBSS로 돌아가서, 발명의 제출된 구체적 설명에 따라, 일단 사용자가 서명된 메시지의 생성을 완료하면, 그는 원하는 대로 그것을 다른 사람에게 제출할 수 있다. 서명된 메시지가 공급되는 (서명자와 같은) 존재는 이

FBSS를 사용하여 만들어진 특정 서명의 유효성을 확신하기를 바랄 지도 모른다. 그러므로, 그는 서명된 메시지와 결합된 지식 서명 P의 유효성을 검증하기를 바랄 지도 모른다. 지식 서명(P)은 상기에 언급된 모든 구조 블록들의 결합체이고, 그것은 사용자(입증자)와 확인자(예를 들면, 서명자)를 포함하는 상호작용 절차를 이용하여 검증될 수 있다.

삭제

삭제

삭제

추적 프로토콜들

서명-추적 프로토콜

주어진 서명-발행 과정에서 기인한 특정 서명을 추적하는 것이 요구될 때, 서명자는 신뢰기관에 서명-발행 과정 동안 알게 된 $(E_1, E_2)$ 쌍을 제공할 수 있고, 신뢰기관은 $I_{sig}$를 정하기 위하여 이 암호문을 해독할 수 있다. 따라서, 신뢰기관은 어떤 암호가 문제의 서명-발행 과정에서 기인하였는지 확인할 수 있다.

삭제

삭제

과정-추적 프로토콜

특정 서명을 만든 서명-발행 과정을 추적하는 것이 요구될 때, 서명자는 신뢰기관에 유효한 서명으로부터 $(E_3, E_4)$ 쌍을 제공하고, 신뢰기관은 이 서명을 얻은 사용자를 확인하는 $Id_u$ 값을 정하기 위하여 이 암호문을 해독할 수 있다.

실시예

본 발명의 공정한 은닉 서명 설계는 다양하게 적용될 수 있다. 가능한 실시예의 몇몇 예는 (비록 본 발명이 이 예들에 제한되지 않지만) 다음을 포함한다 : 전자 경매, 불법 금융거래의 추적, 그리고 본 출원과 동시에 제출되어 "공정한 은닉 서명을 이용한 전자 투표 방법"이라는 명칭을 가진 출원인의 공동 보류 유럽 특허 출원에 설명된 것과 같은 온라인 선거 방법.

본 발명은 공정한 은닉 서명 설계를 실현하는데 사용될 특정 소프트웨어와 하드웨어에 대해 특별히 제한되지 않는다. 숙련된 사람은 이 분야에 대한 그의 일반적인 지식으로부터 발명을 실시하기 위한 알맞은 소프트웨어 처리 순서들과 하드웨어를 선택하는 방법을 쉽게 이해할 것이다.

그러나, 본 발명이 개인용 컴퓨터, 웹 서버, 개인 디지털 보조기, 네트워크 컴퓨터, 알맞게 설비를 갖춘 이동 전화 등과 같이, 협력하며 적절하게 프로그램된 다목적 계산 장치들의 세트를 사용하여 실시될 수 있다는 것은 주목되어야 한다. 선택적으로 서명 설계의 일부 또는 전부는 특정 목적 데이터 처리 장치를 사용하여 실시될 수 있다. 일반적으로, (각각의) 서명자, (각각의) 신뢰기관 및 각각의 사용자를 위한 하나의 데이터 처리/전산 장치가 있을 것이다. 그러나, 서명 설계에 포함된 여러 존재는 하부 루틴 또는 프로그램 모듈이 하나의 집중화된 장치보다 분산된 유닛에서 수행되는 분산된 전산 시스템을 이용할 것으로 이해될 것이다.

삭제

삭제

비록 본 발명이 그것에 대해 제출된 특정한 구체적 설명에서 설명되었을지라도, 이 기술에 숙련된 사람은 제출된 구체적 설명의 다양한 특성들이, 수반하는 청구항에 규정된 것과 같은 본 발명으로부터 출발하지 않고, 다른 것들에 의해 변화하고, 적용되며 그리고/또는 대체될 수 있다는 것을 쉽게 이해할 것이다.

예를 들면, 비록 본 발명에 따라 FBSS의 상기 기술된 구체적 설명이 사용자-등록 단계를 포함할 지라도, 이것은 만약 과정 기록에 기초한 대상 서명의 발행 시간을 충분히 정할 수 있다고 생각되면 생략될 수 있다. 바꾸어 말하면, 만약 "사용자-추적"보다 "과정-추적"을 충분히 수행할 수 있다면, 사용자-등록 단계는 생략될 수 있다.
더 나아가서, 비록 제출된 구체적 설명이 단일 신뢰기관을 이용하는 FBSS의 관점에서 상기에 설명되었을지라도, 숙련된 사람은 일련의 신뢰기관들이 대신 사용될 수 있다는 것과 익명성은 이 신뢰기관의 단체가 협력할 때에만 취소될 수 있다(바꾸어 말하면, 서명-추적과 과정-추적 프로토콜들은 하나보다는 일련의 신뢰기관들에 의하여 실시된다)는 것을 쉽게 이해할 것이다. 여러 신뢰기관들이 있다는 지금의 경우에 대한 상기 기술된 FBSS의 확장은 숙련된 사람에게 수월하므로, 그것에 대해 여기서 자세한 설명이 주어지지 않을 것이다. 원하다면, 여러 신뢰기관들이 있는 경우에 대해 이 기술을 확장하는 한 가지 방법에 대한 안내는 ACM의 통신 회보, pp. 612-613, 1979에 있는 A. Shamir에 의한 "비밀을 공유하는 방법"을 참조하여 얻을 수 있다.

삭제

삭제

삭제

게다가, 비록 제출된 구체적 설명이 서명자로 단일 존재를 사용하는 FBSS의 관점에서 상기에 설명되었을지라도, 숙련된 사람은 일련의 존재들이 대신 서명자를 구성하는데 사용될 수 있다는 것과 유효한 서명을 만들기 위해 사용자에 의하여 요구되는 데이터는 서명자를 구성하는 존재들의 단체의 협력에 의하여 얻어진다는 것을 쉽게 이해할 것이다. 바꾸어 말하면, 본 발명은 임계 공정한 은닉 서명 설계으로서 실시될 수 있다. 서명자가 일련의 존재들에 의해 구성되는 지금의 경우에 대한 상기 기술된 FBSS의 확장은 숙련된 사람에게 수월하므로, 그것에 대한 자세한 설명은 여기에 주어지지 않을 것이다. 원하다면, 이 확장을 수행하는 방법에 대한 안내는 Springer-Verlag, 컴퓨터 과학 강의 노트 2248호 pp.310-330, Asiacrypt '01 회보에 있는 P-A Fouque와 J. Stern에 의한 "표준 가정하에 완전히 분산된 임계값 RSA" 에서 찾을 수 있다.

삭제

삭제

삭제

그리고 본 발명은, 데이터가 서명 설계에 포함된 여러 존재 사이를 통과하는 방법과 관련하여 특별히 제한되지 않는다. 비록 많은 출원에서, 이 데이터 전송이 인터넷으로 수행될 것이지만, 이것은 본 발명의 요구 사항이 아니다. 특별히, (LAN, WAN 등을 포함하는) 다른 통신 네트워크들이 사용될 것이다.

## 발명의 효과

공정한 은닉 서명 방법에서, 사용자는 $A^e = a_0 a_1^x a_2^m a_3^{x_u} a_4^t a_5^s \pmod n$과 같은 7개의 요소로 된 집합 (A,e,s,t,$x_u$,x,m)을 완성시키기 위해 서명자와 상호작용을 한다. 여기서 $a_0$, $a_1$ , $a_2$ , $a_3$, $a_4$ , $a_5$와 n은 서명자의 공개키($PUBK_S$:Signer's public key)의 구성 요소들이다. 서명-발행 단계 동안, 사용자(U:user)는 서명자(S:signer)에게 신뢰기관(TA:trusted authority)에 알려진 키(f)에 따라 암호화된 데이터 요소($a_1^x$)를 제공한다. 그리고 이 데이터 요소($a_1^x$)는 서명된 메시지가 전송되는 동안에 나타난다. 마찬가지로, 서명된 메시지는 신뢰기관(TA)에 알려진 키(f)에 따라 암호화된 두 번째 데이터 요소($a_3^{x_u}$)를 구성하는 두 번째 암호화된 데이터와 결합되어 전송된다. 그리고 이 두번째 데이터 요소($a_3^{x_u}$)는 서명-발행 단계 동안에 서명자에게 나타난다. 따라서, 신뢰기관(TA)은 디지털 서명의 익명성을 취소할 수 있다.

삭제

삭제

삭제

## 도면의 간단한 설명

도 1은 본 발명의 제출된 구체적 설명에 따라 공정한 은닉 서명 설계를 실행하기 위해 사용되는 주요 과정들과 프로토콜들을 가리키는 도표이다. 도 1이 표시하는 것처럼, 제출된 구체적 설명의 공정한 은닉 서명 설계는 서명-발행 프로토콜, 서명 제출 프로토콜과 서명 추적 프로토콜 및/또는 과정-추적 프로토콜을 포함하는 추적 프로토콜을 포함한다.

도면

도면1