(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0089948
(43) 공개일자 2009년08월25일

(51) Int. Cl.
*H04L 9/32* (2006.01) *H04L 9/14* (2006.01)
*G06F 21/00* (2006.01)
(21) 출원번호 10-2008-0015128
(22) 출원일자 2008년02월20일
심사청구일자 2008년02월20일

(71) 출원인
**인하대학교 산학협력단**
인천 남구 용현동 253 인하대학교
(72) 발명자
**양대헌**
서울 서초구 서초동 삼풍 ATP 3동 405호
(74) 대리인
**특허법인태동**

전체 청구항 수 : 총 5 항

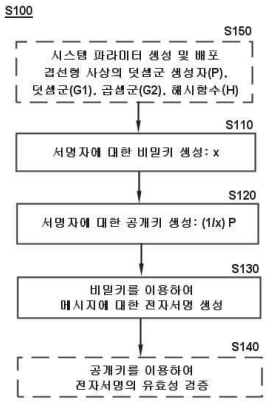
# (54) 겹선형 사상을 이용한 전자서명 방법

## (57) 요 약

본 발명은 전자서명 방법에 관한 것으로, 특히 겹선형 사상(Bilinear Mapping)을 이용한 전자서명 방법에 관한 것이다. 본 발명의 특징에 따른 겹선형 사상을 이용한 전자서명 방법은, (1) 서명자(signer)에 대한 비밀키 x를 생성하는 단계; (2) 상기 단계 (1)에서 생성된 상기 비밀키 x 및 겹선형 사상에 대한 덧셈군 생성자 P를 이용하여, 상기 서명자에 대한 공개키 $P_{pub}$를 (1/x)P로서 생성하는 단계; 및 (3) 상기 비밀키 x를 이용하여 메시지 m에 대한 전자서명 σ을 생성하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.

본 발명의 전자서명 방법에 따르면, 겹선형 사상에 대한 덧셈군 생성자 P를 이용하여, 서명자(signer)에 대한 비밀키와 공개키를 각각 x와 (1/x)P의 형태로 생성한 후, 이를 이용하여 메시지에 대한 전자서명 및 전자서명에 대한 유효성을 검증함으로써, 미리 계산해 놓을 수 있는 부분이 늘어나고 이에 따라 전체적인 계산량을 크게 줄일 수 있으며, 그 결과 전자서명 및 유효성 검증에 대한 효율성을 크게 향상시킬 수 있다.

*대 표 도* - 도1



## 특허청구의 범위

### 청구항 1

겹선형 사상(Bilinear Mapping)을 이용한 전자서명 방법으로서,

(1) 서명자(signer)에 대한 비밀키 x를 생성하는 단계;

(2) 상기 단계 (1)에서 생성된 상기 비밀키 x 및 겹선형 사상에 대한 덧셈군 생성자 P를 이용하여, 상기 서명자에 대한 공개키 $P_{pub}$를 (1/x)P로서 생성하는 단계; 및

(3) 상기 비밀키 x를 이용하여 메시지 m에 대한 전자서명 σ을 생성하는 단계

를 포함하는 전자서명 방법.

### 청구항 2

제1항에 있어서,

상기 단계 (3)에서, 다음 수학식에 의하여 상기 전자서명 σ을 생성하는 것을 특징으로 하는 전자서명 방법.

$\sigma = xH(m)$

여기서, 함수 H()는 full-domain 해시 함수로서 임의의 비트 스트링을 입력받아 겹선형 사상의 덧셈군 $G_1$의 한 원소로 변환하는 함수이며, 암호학적 해시 함수의 성질을 만족한다.

### 청구항 3

제1항에 있어서,

(4) 상기 공개키($P_{pub}$)를 이용하여, 전자서명의 유효성을 검증하는 단계를 더 포함하는 전자서명 방법.

### 청구항 4

제3항에 있어서,

상기 단계 (4)에서, 다음 수학식을 이용하여 전자서명의 유효성을 검증하는 것을 특징으로 하는 전자서명 방법.

$e(P_{pub}, \sigma) = e(P, H(m))$

여기서, 함수 e()는 겹선형 사상의 덧셈군 $G_1$의 두 원소를 입력받아 겹선형 사상의 곱셈군 $G_2$로 사상시키는 겹선형 사상을 나타내며, 함수 H()는 full-domain 해시 함수로서 임의의 비트 스트링을 입력받아 겹선형 사상의 덧셈군 $G_1$의 한 원소로 변환하는 함수이며, 암호학적 해시 함수의 성질을 만족한다.

### 청구항 5

제1항에 있어서,

(5) 시스템 파라미터로서, 덧셈군 생성자(P), 덧셈군($G_1$), 곱셈군($G_2$), 해시 함수(H)를 생성하여 모든 사용자에게 공개하는 단계를 더 포함하는 전자서명 방법.

## 명 세 서

## 발명의 상세한 설명

### 기 술 분 야

<1> 본 발명은 전자서명 방법에 관한 것으로, 특히 겹선형 사상을 이용한 전자서명 방법에 관한 것이다. 보다 구체적으로는, 겹선형 사상에 대한 덧셈군 생성자 P를 이용하여, 서명자(signer)에 대한 비밀키와 공개키를 각각 x와 (1/x)P의 형태로 생성한 후, 이를 이용하여 메시지에 대한 전자서명 및 전자서명에 대한 유효성을 검증하는 전자서명 방법에 관한 것이다.

## 배 경 기 술

<2> 전자서명(electronic signature)이란, 자료 메시지에 부착되거나 논리적으로 결합된 전자적 형태의 서명으로서, 서명자의 신원을 확인하고 자료 메시지의 내용에 대한 그 사람의 승인을 나타낼 목적으로 사용된다. 전자서명은, 손으로 하는 수기 서명(manual signature) 또는 날인의 전자적인 대체물로서, 펜 대신에 컴퓨터를 매개로 하여 생성되는 서명 정보라고 할 수 있다.

<3> 전자서명은 송신자가 작성한 전자문서 자체를 암호화하는 것이 아니므로 제3자가 문서 내용을 열람하는 데에는 아무런 지장이 없다. 다만, 그 전자서명에 작성자로 기재된 자가 그 전자문서를 작성하였다는 사실과 작성 내용이 송수신 과정에서 위조·또는 변조되지 않았다는 사실을 증명하고, 작성자가 그 전자문서 작성 사실을 나중에 부인할 수 없게 하는 역할을 한다.

<4> 전자서명은 인터넷 쇼핑이나 사이버 금융거래 등에서 생길 수 있는 정보 유출 등의 위험을 줄일 수 있는 효과적인 도구로서, 전자서명을 활용하면 개인정보 도용이나 변조를 원천적으로 차단할 수 있다.

<5> 전자서명의 대표적인 용도는 인터넷 뱅킹 등의 금융거래, 인터넷 민원서비스, 인터넷 쇼핑 등이 있으며, 앞으로 국제 간 전자상거래, 전자투표 등으로 확대될 수 있다. 인터넷 뱅킹이나 온라인 주식거래에 필요한 공인인증서는 국가가 지정한 공인인증기관에서 발행하고 공개키를 관리하는 대표적인 전자서명이다.

<6> 겹선형 쌍들, 즉, 대수 곡선상의 베일(Weil) 쌍과 테이트(Tate) 쌍은 대수기하학 연구에서 매우 중요한 도구들이다. 암호에서 겹선형 쌍의 초기 응용은 이산대수문제(Discrete Logarithm Problem)의 평가를 위한 것이었다. 예를 들면, 베일 쌍을 이용한 엠오브이(MOV) 공격이나 테이트 쌍을 이용한 에프아르(FR) 공격은 특정 타원 곡선이나 초타원 곡선에서의 이산대수문제를 유한체에서의 이산대수문제로 간단히 축약할 수 있게 한다.

<7> 최근에 겹선형 쌍들이 암호에서 다양한 응용 분야가 있다는 것이 밝혀졌다. 예들 들면, 보네-프랭클린(Boneh-Franklin)의 개인 식별정보 기반 암호 시스템, 스마트카드의 개인 식별정보 기반 인증 키 관리와 몇 가지 개인 식별정보 기반 전자서명 기법을 들 수 있다. 개인 식별정보 기반의 원형서명은 일반 원형서명과 개인 식별 기반 기법을 결합한 형태로 검증을 하기 위한 공개키가 서명자의 개인 식별정보가 되는 것이다. 즉, 개인 식별정보 기반의 원형서명은 서명자의 공개키가 단순히 그의 개인 식별정보이기 때문에 서명 과정이 대단히 효율적이다.

<8> 크립토 2001 학회에서 최초로 보네와 프랭클린에 의해서 겹선형 사상을 갖는 군(Group)의 특성을 사용한 암호 시스템이 제안된 이후, 암호 및 복호화 기법, 키 합의 및 키 동의 기법, 서명기법 등이 제안되었으나 겹선형 사상 함수는 많은 계산량을 요구한다는 문제점이 있었으며, 이에 따라 계산량을 줄일 수 있는 개선 방안이 요구되었다.

## 발명의 내용

### 해결 하고자하는 과제

<9> 본 발명은 기존에 제안된 방법들의 상기와 같은 문제점들을 해결하기 위해 제안된 것으로서, 겹선형 사상에 대한 덧셈군 생성자 P를 이용하여, 서명자(signer)에 대한 비밀키와 공개키를 각각 x와 (1/x)P의 형태로 생성한 후, 이를 이용하여 메시지에 대한 전자서명 및 전자서명에 대한 유효성을 검증함으로써, 전체적인 계산량을 크게 줄일 수 있는 전자서명 방법을 제공하는 것을 그 목적으로 한다.

### 과제 해결수단

<10> 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 겹선형 사상(Bilinear Mapping)을 이용한 전자서명 방법은,

<11> (1) 서명자(signer)에 대한 비밀키 x를 생성하는 단계;

<12> (2) 상기 단계 (1)에서 생성된 상기 비밀키 x 및 겹선형 사상에 대한 덧셈군 생성자 P를 이용하여, 상기 서명자에 대한 공개키 $P_{pub}$를 (1/x)P로서 생성하는 단계; 및

<13> (3) 상기 비밀키 x를 이용하여 메시지 m에 대한 전자서명 σ을 생성하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.

<14> 바람직하게는, 상기 단계 (3)에서, 다음 수학식 1에 의하여 상기 전자서명 σ을 생성하는 것을 특징으로 한다.

### 수학식 1

<15> $\sigma = xH(m)$

<16> 여기서, 함수 H()는 full-domain 해시 함수로서 임의의 비트 스트링을 입력받아 겹선형 사상의 덧셈군 $G_1$의 한 원소로 변환하는 함수이며, 암호학적 해시 함수의 성질을 만족한다.

<17> 바람직하게는, (4) 상기 공개키($P_{pub}$)를 이용하여, 전자서명의 유효성을 검증하는 단계를 더 포함한다.

<18> 더욱 바람직하게는, 상기 단계 (4)에서, 다음 수학식 2을 이용하여 전자서명의 유효성을 검증하는 것을 특징으로 한다.

### 수학식 2

<19> $e(P_{pub}, \sigma) = e(P, H(m))$

<20> 여기서, 함수 e()는 겹선형 사상의 덧셈군 $G_1$의 두 원소를 입력받아 겹선형 사상의 곱셈군 $G_2$로 사상시키는 겹선형 사상을 나타내며, 함수 H()는 full-domain 해시 함수로서 임의의 비트 스트링을 입력받아 겹선형 사상의 덧셈군 $G_1$의 한 원소로 변환하는 함수이며, 암호학적 해시 함수의 성질을 만족한다.

<21> 바람직하게는, (5) 시스템 파라미터로서, 덧셈군 생성자(P), 덧셈군($G_1$), 곱셈군($G_2$), 해시 함수(H)를 생성하여 모든 사용자에게 공개하는 단계를 더 포함한다.

## 효 과

<22> 본 발명의 전자서명 방법에 따르면, 겹선형 사상에 대한 덧셈군 생성자 P를 이용하여, 서명자(signer)에 대한 비밀키와 공개키를 각각 x와 (1/x)P의 형태로 생성한 후, 이를 이용하여 메시지에 대한 전자서명 및 전자서명에 대한 유효성을 검증함으로써, 미리 계산해 놓을 수 있는 부분이 늘어나고 이에 따라 전체적인 계산량을 크게 줄일 수 있으며, 그 결과 전자서명 및 유효성 검증에 대한 효율성을 크게 향상시킬 수 있다.

## 발명의 실시를 위한 구체적인 내용

<23> 이하에서는 첨부된 도면들을 참조하여, 본 발명에 따른 실시예에 대하여 상세하게 설명하기로 한다.

<24> 도 1은 본 발명의 일 실시예에 따른 전자서명 방법의 구성을 나타내는 도면이다. 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 전자서명 방법(S100)은, 서명자에 대한 비밀키 x를 생성하는 단계(S110), 서명자에 대한 공개키 (1/x)P를 생성하는 단계(S120), 및 생성된 비밀키를 이용하여 메시지에 대한 전자서명을 생성하는 단계(S130)를 포함한다. 또한, 본 발명의 일 실시예에 따른 전자서명 방법(S100)은, 수신된 전자서명을 공개키를 이용하여 그 유효성을 검증하는 단계(S140)를 더 포함할 수 있으며, 또한 겹선형 사상의 덧셈군 생성자(P), 덧셈군($G_1$), 곱셈군($G_2$), 및 해시함수(H())와 같은 시스템 파라미터를 생성 및 배포하는 단계(S150)를 더 포함할 수도 있다.

<25> 단계 S110에서는, 서명자에 대한 비밀키 x를 생성하는 역할을 한다. 비밀키 x는 $x \in_R Z_q^*$을 만족하는 값으로 선택된다.

<26> 단계 S120에서는, 단계 S110에서 생성된 비밀키 x 및 겹선형 사상의 덧셈군 생성자 P를 이용하여 공개키($P_{pub}$)를 (1/x)P로서 생성하는 역할을 한다.

<27> 단계 S130에서는, 단계 S110에서 생성된 비밀키 x를 이용하여 메시지 m에 대한 전자서명 σ을 생성하는 역할을 한다. 메시지 m은 $m \in 0,1^*$을 만족한다. 바람직하게는, 단계 S130에서, 앞서 설명한 수학식 1을 이용하여 전자서명을 생성할 수 있다.

<28> 단계 S140에서는, 수신된 전자서명에 대하여, 단계 S120에서 생성된 공개키($P_{pub}$)를 이용하여 해당 전자서명의 유효성을 검증하는 역할을 한다. 바람직하게는, 단계 S140에서, 앞서 설명한 수학식 2를 이용하여 전자서명의

유효성을 검증할 수 있다.

<29> 단계 S150에서는, 본 발명에 따른 전자서명 방법을 위한 시스템 파라미터를 생성 및 배포하는 역할을 한다. 시스템 파라미터로는, 겹선형 사상의 덧셈군 생성자(P), 덧셈군($G_1$), 곱셈군($G_2$), 및 해시함수(H())가 포함될 수 있다.

<30> 이하에서는, 겹선형 사상에 대해서 살펴본 후, 본 발명에서 제안하고 있는 전자서명 방법을 상세히 살펴보기로 한다.

<31> 1. 겹선형 사상

<32> 동일한 위수 q를 갖는 겹선형 사상의 덧셈군 $G_1$과 곱셈군 $G_2$를 가정하자. 이 그룹 내에서 이산대수문제를 푸는 것은 계산상 불가능하다고 가정한다. P를 덧셈군 $G_1$의 생성자(generator)라고 하자. 이때 aP는 P를 a번 더한 것을 의미한다. $e : G_1 \times G_1 \rightarrow G_2$ 가 다음 3가지 속성을 만족할 경우, 이를 겹선형 사상(Bilinear Mapping)이라고 한다.

<33> (1) 겹선형성(Bilinearity)

<34> 모든 $P,Q \in G_1$과 모든 $a,b \in Z$에 대하여, $e(aP,bQ) = e(P,Q)^{ab}$ 이다.

<35> (2) 비퇴보성(Non-degeneracy)

<36> 모든 $Q \in G_1$에 대하여, $e(P,Q)=1$이면 $P=O$이다.

<37> (3) 계산성(Computability)

<38> 모든 $P,Q \in G_1$에 대하여, $e(P,Q)$를 계산하기 위한 효율적인 알고리즘이 존재한다.

<39> 겹선형 사상의 덧셈군 $G_1$과 곱셈군 $G_2$를 이용해서 다음과 같은 문제를 정의할 수 있으며, 이는 아직까지 계산하기 어려운 것으로 알려져 있다.

<40> (1) 이산대수 문제(Discrete Logarithm Problem)

<41> $P,P' \in G_1$이 주어졌을 때, $P=nP'$을 만족하는 정수 n을 구한다.

<42> (2) CDH 문제(Computational Diffie-Hellman Problem)

<43> $a,b \in Z_q^*$에 대하여 $(P,aP,bP) \in G_1$이 주어졌을 때, abP를 구한다.

<44> (3) DDH 문제(Decisional Diffie-Hellman)

<45> $a,b,c \in Z_q^*$에 대하여 $(P,aP,bP,cP) \in G_1$이 주어졌을 때, $c=abP \pmod q$인지 여부를 결정한다.

<46> (4) Gap Diffie-Hellman 문제

<47> CDH는 풀기 어려우나 DDH 문제는 쉬운 문제들을 의미한다.

<48> 겹선형 쌍을 구현하기 위하여, Weil pairing 또는 Tate pairing을 이용할 수 있다.

<49> 2. 전사서명 방법

<50> (1) 시스템 파라미터

<51> 겹선형 사상의 덧셈군 생성자 P, 덧셈군 $G_1$, 곱셈군 $G_2$ 및 해시 함수 H() 등은 공개되어 있고, 모든 사용자가 공유한다.

<52> (2) 비밀키 및 공개키 생성

<53> $x \in_R Z_q^*$ 를 만족하는 임의의 x를 비밀키로 생성한다.

<54> 생성된 비밀키 x 및 덧셈군 생성자 P를 이용하여, 공개키($P_{pub}$)를 (1/x)P로서 생성한다.

<55> (3) 전자서명 생성

<56> 주어진 메시지 $m \in 0,1^*$와 비밀키 x를 이용하여 전자서명 σ를 앞서 설명한 바 있는 다음 수학식 1과 같이 계산한다.

<57> <수학식 1>

<58> $\sigma = xH(m)$

<59> (4) 전자서명 검증

<60> 공개키 $P_{pub}$, 덧셈군 생성자 P, 메시지 m, 해시 함수 H()를 이용하여, 앞서 설명한 바 있는 다음 수학식 2에 의하여 전자서명 σ의 유효성을 검증한다.

<61> <수학식 2>

<62> $e(P_{pub}, \sigma) = e(P, H(m))$

<63> 본 발명에서 제안한 전자서명 방법의 응용예로서, 전자서명 일괄 검증 방법 및 동일 사용자가 생성한 전자서명 일괄 검증 방법에 대하여 이하에서 설명한다.

<64> 3. 전자서명 일괄 검증 방법

<65> n명의 사용자에 대한 공개키가 $P_{pub1}$, $P_{pub2}$, , $P_{pubn}$이라고 하자. 각각의 사용자에 대한 메시지가 $m_1$, $m_2$, , $m_n$이고, 이 각각의 메시지에 대한 전자서명이 $\sigma_1$, $\sigma_2$, , $\sigma_n$이라고 할 경우, 다음 수학식 3과 같이 전자서명을 검증할 수 있다.

*수학식 3*

<66> $$e(P_{pub_1},\sigma_1)*e(P_{pub_2},\sigma_2)*\cdots*e(P_{pub_n},\sigma_n) = e(P,H(m_1)+H(m_2)+\cdots+H(m_n))$$

<67> 상기 수학식 3에서 확인할 수 있는 바와 같이, 우변의 겹선형 사상 계산이 1번으로 줄기 때문에 겹선형 사상의 연산 횟수를 절반으로 줄일 수 있다. 이는, 다음 수학식 4에서 확인할 수 있는 바와 같이, 각각의 메시지의 해시 함수 값에 대한 덧셈군 생성자와의 겹선형 사상의 곱을 각각의 메시지의 해시 함수 값의 합과 덧셈군 생성자와의 한 번의 겹선형 사상으로 변환할 수 있기 때문이다.

*수학식 4*

<68> $$e(P,H(m_1))*e(P,H(m_2))*\cdots*e(P,H(m_n)) = e(P,H(m_1)+H(m_2)+\cdots+H(m_n))$$

<69> 4. 동일 사용자가 생성한 전자서명의 일괄 검증 방법

<70> 한 명의 사용자가 다수개의 메시지($m_1$, $m_2$, , $m_n$)에 대한 전자서명($\sigma_1$, $\sigma_2$, , $\sigma_n$)을 생성했을 때 다음 수학식 5와 같이 전자서명을 검증할 수 있다.

*수학식 5*

<71> $$e(P_{pub},\sigma_1+\sigma_2+\cdots+\sigma_n) = e(P,H(m_1)+H(m_2)+\cdots+H(m_n))$$

<72> 상기 수학식 5에서 확인할 수 있는 바와 같이, 좌변과 우변의 겹선형 사상 계산이 각각 1번으로 줄기 때문에 겹선형 사상의 계산 횟수를 2번으로 줄일 수 있다. 이는 앞서 설명한 바와 같이, 우변에서, 각각의 메시지의 해시 함수 값에 대한 덧셈군 생성자와의 겹선형 사상의 곱을 각각의 메시지의 해시 함수 값의 합과 덧셈군 생성자와의 한 번의 겹선형 사상으로 변환할 수 있기 때문이며, 또한 다음 수학식 6에서 확인할 수 있는 바와 같이, 좌변에서, 각각의 대응하는 공개키와 전자서명 간의 겹선형 사상의 곱을 하나의 공개키와 각각의 전자서명들의 합 간의 한 번의 겹선형 사상으로 변환할 수 있기 때문이다.

### 수학식 6

<73> $$e(P_{pub_1},\sigma_1)*e(P_{pub_2},\sigma_2)*\cdots*e(P_{pub_n},\sigma_n)=e(P_{pub},\sigma_1+\sigma_2+\cdots+\sigma_n)$$

<74> 이상 살펴본 바와 같이, 본 발명에서 제안하는 전자서명 방법은, 특히 하나의 인증서 발행기관(Certificate Authority)에서 발행한 여러 개의 인증서를 검증하거나, 전자화폐에서 사용하는 전자서명 등을 검증할 때 계산량을 많이 줄여줄 수 있다.

<75> 이상 설명한 본 발명은 본 발명이 속한 기술분야에서 통상의 지식을 가진 자에 의하여 다양한 변형이나 응용이 가능하며, 본 발명에 따른 기술적 사상의 범위는 아래의 특허청구범위에 의하여 정해져야 할 것이다.

## 도면의 간단한 설명

<76> 도 1은 본 발명의 일 실시예에 따른 전자서명 방법의 구성을 나타내는 도면.

<77> <도면 중 주요 부분에 대한 부호의 설명>

<78> S100: (본 발명의 일 실시예에 따른) 전자서명 방법

<79> S110: 서명자에 대한 비밀키 x를 생성하는 단계

<80> S120: 서명자에 대한 공개키 (1/x)P를 생성하는 단계

<81> S130: 비밀키를 이용하여 메시지에 대한 전자서명을 생성하는 단계

<82> S140: 공개키를 이용하여 전자서명의 유효성을 검증하는 단계

<83> S150: 시스템 파라미터를 생성 및 배포하는 단계

## 도면

### 도면1

