(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0051305
(43) 공개일자 2020년05월13일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/3066 (2013.01)
H04L 9/0825 (2013.01)
(21) 출원번호 10-2018-0134507
(22) 출원일자 2018년11월05일
심사청구일자 2018년11월23일

(71) 출원인
기초과학연구원
대전광역시 유성구 엑스포로 55(도룡동)
(72) 발명자
심경아
대전광역시 유성구 유성대로 1689번길 70 (전민동)
(74) 대리인
윤재석

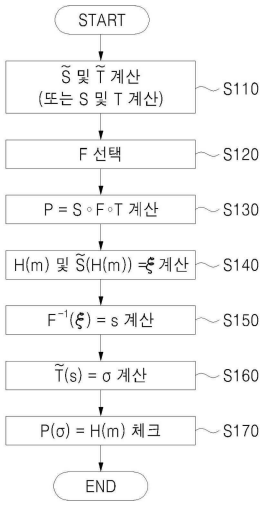
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **오일-오일 이차항을 갖는 센트럴 맵에 기초한 양자 컴퓨터에 안전한 다변수 이차식 전자서명 스킴**

(57) 요 약

키 생성 장치를 포함하는 전자 장치가 개시된다. 상기 상기 키 생성 장치는 제1아핀 맵, 제2아핀 맵, 및 제3맵을 획득하고, 상기 제1아핀 맵, 상기 제2아핀 맵, 및 상기 제3맵를 이용하여 공개키를 생성하고, 상기 제3맵은 n개의 변수들과 m개의 방정식들을 갖는 다변수 이차 다항식들의 시스템이고, 상기 다변수 이차 다항식들 중에서 적어도 하나는 0이 아닌 계수의 오일-오일 이차항을 갖고, 상기 제3맵은 오일과 비니거 방식에서 사용되는 비니거 변수들을 정의하기 위한 적어도 하나의 집합과 상기 오일과 비니거 방식에서 사용되는 오일 변수들을 정의하기 위한 인덱스 집합들을 포함하고, 상기 제1아핀 맵, 상기 제2아핀 맵, 및 상기 제3맵 각각은 유한체이다.

대 표 도 - 도5



(52) CPC특허분류
H04L 9/3247 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 B18120000
부처명 과학기술정보통신부
연구관리전문기관 국가수리과학연구소
연구사업명 정보수학기반 핵심기술 연구
연구과제명 경량기기 전용 신규 난제 기반 고속 공개키 암호알고리즘 연구
기 여 율 1/1
주관기관 국가수리과학연구소
연구기간 2018.01.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

키 생성 장치를 포함하는 전자 장치에 있어서,

상기 키 생성 장치는 제1아핀 맵($S : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^m$), 제2아핀 맵 ($T : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$), 및 제3맵 ($\mathcal{F} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$)을 획득하고, 상기 제1아핀 맵, 상기 제2아핀 맵, 및 상기 제3맵를 이용하여 공개키 ($\mathcal{P} = S \circ \mathcal{F} \circ T$)를 생성하고,

상기 제3맵($\mathcal{F}$)은 n개의 변수들과 m개의 방정식들을 갖는 다변수 이차 다항식들($\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$)의 시스템이고,

상기 다변수 이차 다항식들 중에서 적어도 하나는 0이 아닌 계수의 오일-오일 이차항을 갖고,

상기 제3맵($\mathcal{F}$)은 오일과 비니거 방식에서 사용되는 비니거 변수들을 정의하기 위한 적어도 하나의 제1인덱스 집합과 상기 오일과 비니거 방식에서 사용되는 오일 변수들을 정의하기 위한 적어도 하나의 제2인덱스 집합을 포함하고,

$\mathbb{F}_q$ 는 원소들의 개수가 q인 유한체인 전자 장치.

청구항 2

제1항에 있어서,

레이어의 개수를 나타내는 u가 1 이상일 때, $v_1, \cdots, v_{u+1}$ 는 정수들(integers)이고, $0 < v_1 < v_2 < \cdots < v_u < v_{u+1} = n$이고,

상기 적어도 하나의 제1인덱스 집합은 정수들의 집합들 ($V_i = \{1, \cdots, v_i\}$)이고,

상기 적어도 하나의 제2인덱스 집합은 정수들의 집합들 ($O_i = \{v_i + 1, \cdots, v_{i+1}\}$)이고,

$o_i = v_{i+1} - v_i$ 이고,

$|V_i| = v_i$ 이고, $|O_i| = o_i$ 이고,

$i = 1, \cdots, u$ 이고,

$m = o_1 + \cdots + o_u$ 고, $n = v_1 + m$ 인 전자 장치.

청구항 3

제2항에 있어서,

$k = 1, \cdots, m-1$ 에 대해 상기 n개의 변수들($x_1, \cdots, x_n$)을 갖는 다변수 이차 다항식들은 아래와 같이 정의되고,

$$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_l, j\in V_l} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V_l, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V_l\cup O_l} \gamma_i^{(k)} x_i + \eta^{(k)}$$

l 은 $k \in O_l$ 을 만족하는 유일한 정수이고,

$\mathbf{x} = (x_1, \cdots, x_n)$ 이고,

k = m일 때, 다변수 이차 다항식들은 아래와 같이 정의되고,

$$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_u, j\in V_u} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V_u, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i,j\in O_u, i\le j} \delta_{ij}^{(k)} x_i x_j + \sum_{i\in V_u\cup O_u} \gamma_i^{(k)} x_i + \eta^{(k)}$$

1≤ k ≤m인 전자 장치.

청구항 4

제1항에 있어서,

상기 적어도 하나의 제1인덱스 집합은 $V = \{1, \cdots, v\}$ 이고,

상기 적어도 하나의 제2인덱스 집합은 $O_1 = \{v+1, \cdots, v+o_1\}$, $O_2 = \{v+o_1+1, \cdots, v+o_1+o_2\}$ 이고,

$|V| = v$ 이고, $|O_i| = o_i$ 이고, i = 1과 2이고,

상기 다변수 이차 다항식들($\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$) 중에서 마지막 다항식 ($\mathcal{F}^{(m)}$)은 0이 아닌 계수의 오일-오일 이차항을 갖고,

상기 m = o_1 + o_2이고, 상기 n = v + m인 전자 장치.

청구항 5

제1항에 있어서, $\mathcal{F}^{(k)}$ 에 관련된 레이어가 제1레이어와 제2레이어를 포함할 때,

상기 제1레이어에서, $k = 1, \cdots, o_1$ 에 대해 $\mathcal{F}^{(k)}$ 는 아래와 같이 정의되고,

$$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_1, j\in V} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O_1} \gamma_i^{(k)} x_i + \eta^{(k)}$$

상기 제2레이어에서, $k = o_1+1, \cdots, m-1$ 에 대해 $\mathcal{F}^{(k)}$ 는 아래와 같이 정의되고,

$$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_2, j\in V\cup O_1} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V\cup O_1, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O_1\cup O_2} \gamma_i^{(k)} x_i + \eta^{(k)}$$

상기 제2레이어에서, k = m에 대해 $\mathcal{F}^{(k)}$ 는 아래와 같이 정의되고,

$$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_2, j\in V\cup O_1} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V\cup O_1, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i,j\in O_2, i\le j} \delta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O_1\cup O_2} \gamma_i^{(k)} x_i + \eta^{(m)},$$

여기서, 벡터 $\mathbf{x} = (x_1, \cdots, x_n)$ 인 전자 장치.

청구항 6

제1항에 있어서,

상기 적어도 하나의 제1인덱스 집합은 $V = \{1, \cdots, v\}$이고,

상기 적어도 하나의 제2인덱스 집합은 $O = \{v+1, \cdots, v+o\}$ 이고,

$|V| = v$이고, $|O| = o$ 이고,

$k = 1, \cdots, m-1$ 에 대해 $\mathcal{F}^{(k)}$는 아래와 같이 정의되고,

$$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i \in O, j \in V} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j \in V, i \leq j} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V \cup O} \gamma_i^{(k)} x_i + \eta^{(k)}$$

k = m에 대해 $\mathcal{F}^{(k)}$는 아래와 같이 정의되고,

$$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i \in O, j \in V} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j \in V, i \leq j} \beta_{ij}^{(k)} x_i x_j + \sum_{i,j \in O, i \leq j} \delta_{ij}^{(k)} x_i x_j + \sum_{i \in V \cup O} \gamma_i^{(k)} x_i + \eta^{(k)}$$

여기서, 벡터 $\mathbf{x} = (x_1, \cdots, x_n)$인 전자 장치.

청구항 7

제1항에 있어서,

디지털서명 생성 장치와 검증 장치를 더 포함하고,

상기 디지털서명 생성 장치는,

메시지(m)를 수신하고,

상기 키 생성 장치로부터 상기 제1아핀 맵(S), 상기 제2아핀 맵(T), 상기 제3맵($\mathcal{F}$), 및 상기 공개키($\mathcal{P}$)를 수신하고,

상기 제1아핀 맵(S)의 역변환($\widetilde{S}$)과 상기 제2아핀 맵(T)의 역변환($\widetilde{T}$)을 계산하고,

상기 역변환($\widetilde{S}$), 상기 역변환($\widetilde{T}$), 및 상기 제3맵 ($\mathcal{F}$)을 이용하여 상기 메시지(m)에 대한 서명(σ)을 생성하고,

상기 공개키($\mathcal{P}$), 상기 서명(σ), 및 상기 메시지(m)를 상기 검증 장치로 동시에 출력하고,

상기 검증 장치는 상기 공개키($\mathcal{P}$), 상기 서명(σ), 및 상기 메시지(m)를 이용하여 $\mathcal{P}(\sigma) = H(\mathrm{m})$인지를 검증하는 전자 장치.

청구항 8

제7항에 있어서,

상기 디지털서명 생성 장치는,

상기 메시지(m)에 대한 해시 함수(H(m))를 계산하고,

$\xi = (\xi_1, \cdots, \xi_m)$가 주어졌을 때 $\widetilde{S}(H(\mathbb{m})) = \xi$을 계산하고,

$\mathcal{F}^{-1}(\xi) = \mathbf{s}$을 만족하는 벡터($\mathbf{s}$)를 계산하고,

상기 서명(σ)을 생성하기 위해 $\widetilde{T}(\mathbf{s}) = \sigma$을 계산하는 전자 장치.

청구항 9

제1항에 있어서,

디지털서명 생성 장치와 검증 장치를 더 포함하고,

상기 키 생성 장치는,

상기 제1아핀 맵(S)의 역변환($\widetilde{S}$)과 상기 제2아핀 맵(T)의 역변환($\widetilde{T}$)을 계산하고,

상기 역변환($\widetilde{S}$), 상기 역변환($\widetilde{T}$), 상기 제3맵($\mathcal{F}$), 및 상기 공개키 ($\mathcal{P}$)를 상기 디지털서명 생성 장치로 전송하고,

상기 디지털서명 생성 장치는,

메시지(m)를 수신하고,

상기 키 생성 장치로부터 상기 역변환($\widetilde{S}$), 상기 역변환($\widetilde{T}$), 상기 제3맵($\mathcal{F}$), 및 상기 공개키($\mathcal{P}$)를 수신하고,

상기 역변환($\widetilde{S}$), 상기 역변환($\widetilde{T}$), 및 상기 제3맵($\mathcal{F}$)을 이용하여 상기 메시지(m)에 대한 서명(σ)을 생성하고,

상기 공개키($\mathcal{P}$), 상기 서명(σ), 및 상기 메시지(m)를 상기 검증 장치로 동시에 출력하고,

상기 검증 장치는 상기 공개키($\mathcal{P}$), 상기 서명(σ), 및 상기 메시지(m)를 이용하여 $\mathcal{P}(\sigma) = H(\mathbb{m})$인지를 검증하는 전자 장치.

청구항 10

제9항에 있어서,

상기 디지털서명 생성 장치는,

상기 메시지(m)에 대한 해시 함수(H(m))를 계산하고,

$\xi = (\xi_1, \cdots, \xi_m)$가 주어졌을 때 $\widetilde{S}(H(\mathbb{m})) = \xi$을 계산하고,

$\mathcal{F}^{-1}(\xi) = \mathbf{s}$을 만족하는 벡터($\mathbf{s}$)를 계산하고,

상기 서명(σ)을 생성하기 위해 $\widetilde{T}(\mathbf{s}) = \sigma$을 계산하는 전자 장치.

청구항 11

제1아핀 맵($S : \mathbb{F}_q^m \to \mathbb{F}_q^m$), 제2아핀 맵 ($T : \mathbb{F}_q^n \to \mathbb{F}_q^n$), 및 제3맵

($\mathcal{F}: \mathbb{F}_q^n \to \mathbb{F}_q^m = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$)을 획득하는 단계; 및

상기 제1아핀 맵, 상기 제2아핀 맵, 및 상기 제3맵를 이용하여 공개키 ($\mathcal{P} = S \circ \mathcal{F} \circ T$)를 생성하는 단계를 포함하고,

상기 제3맵($\mathcal{F}$)은 n개의 변수들과 m개의 방정식들을 갖는 다변수 이차 다항식들($\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$)의 시스템이고,

상기 다변수 이차 다항식들 중에서 적어도 하나는 0이 아닌 계수의 오일-오일 이차항을 갖고,

상기 제3맵($\mathcal{F}$)은 오일과 비니거 방식에서 사용되는 비니거 변수들을 정의하기 위한 적어도 하나의 제1인덱스 집합과 상기 오일과 비니거 방식에서 사용되는 오일 변수들을 정의하기 위한 적어도 하나의 제2인덱스 집합을 포함하고,

$\mathbb{F}_q$ 는 원소들의 개수가 q인 유한체인 전자 장치를 이용한 전자 서명 방법.

청구항 12

제11항에 있어서,

레이어의 개수 u가 1 이상일 때, $v_1, \cdots, v_{u+1}$ 는 정수들(integers)이고, $0 < v_1 < v_2 < \cdots < v_u < v_{u+1} = n$이고,

상기 적어도 하나의 제인덱스 집합은 정수들의 집합들 ($V_i = \{1, \cdots, v_i\}$)이고,

상기 적어도 하나의 제2인덱스 집합은 정수들의 집합들 ($O_i = \{v_i + 1, \cdots, v_{i+1}\}$)이고,

$o_i = v_{i+1} - v_i$ 이고,

$|V_i| = v_i$ 이고, $|O_i| = o_i$ 이고,

$i = 1, \cdots, u$ 이고,

$m = o_1 + \cdots + o_u$ 고, $n = v_1 + m$ 인 전자 장치를 이용한 전자 서명 방법.

청구항 13

제12항에 있어서,

$k = 1, \cdots, m-1$ 에 대해 상기 n개의 변수들($x_1, \cdots, x_n$)을 갖는 다변수 이차 다항식들은 아래와 같이 정의되고,

$$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i \in O_l, j \in V_l} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j \in V_l, i \leq j} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V_l \cup O_l} \gamma_i^{(k)} x_i + \eta^{(k)}$$

l 은 $k \in O_l$ 을 만족하는 유일한 정수이고,

$\mathbf{x} = (x_1, \cdots, x_n)$ 이고,

k = m일 때, 다변수 이차 다항식들은 아래와 같이 정의되고,

$$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_u, j\in V_u} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V_u, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i,j\in O_u, i\le j} \delta_{ij}^{(k)} x_i x_j + \sum_{i\in V_u\cup O_u} \gamma_i^{(k)} x_i + \eta^{(k)}$$

1≤ k ≤m인 전자 장치를 이용한 전자 서명 방법.

청구항 14

제11항에 있어서,

상기 적어도 하나의 제1인덱스 집합은 $V = \{1, \cdots, v\}$이고,

상기 적어도 하나의 인덱스 집합은 $O_1 = \{v+1, \cdots, v+o_1\}$, $O_2 = \{v+o_1+1, \cdots, v+o_1+o_2\}$이고,

$|V| = v$ 이고, $|O_i| = o_i$ 이고, i = 1과 2이고,

상기 다변수 이차 다항식들($\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$) 중에서 마지막 다항식 ($\mathcal{F}^{(m)}$)은 0이 아닌 계수의 오일-오일 이차항을 갖고,

상기 m = o_1 + o_2이고, 상기 n = v + m인 전자 장치를 이용한 전자 서명 방법.

청구항 15

제11항에 있어서,

상기 적어도 하나의 제1인덱스 집합은 $V = \{1, \cdots, v\}$이고,

상기 적어도 하나의 제2인덱스 집합은 $O = \{v+1, \cdots, v+o\}$ 이고,

$|V| = v$ 이고, $|O| = o$ 이고,

$k = 1, \cdots, m-1$ 에 대해 $\mathcal{F}^{(k)}$는 아래와 같이 정의되고,

$$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O, j\in V} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O} \gamma_i^{(k)} x_i + \eta^{(k)}$$

k = m에 대해 $\mathcal{F}^{(k)}$는 아래와 같이 정의되고,

$$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O, j\in V} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i,j\in O, i\le j} \delta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O} \gamma_i^{(k)} x_i + \eta^{(k)}$$

여기서, 벡터 $\mathbf{x} = (x_1, \cdots, x_n)$인 전자 장치를 이용한 전자 서명 방법.

청구항 16

제11항에 있어서,

상기 전자 장치의 외부로부터 메시지(m)를 수신하는 단계;

상기 제1아핀 맵(S)의 제1역변환($\widetilde{S}$)과 상기 제2아핀 맵(T)의 제2역변환 ($\widetilde{T}$)을 계산하는 단계;

상기 제1역변환($\widetilde{S}$), 상기 제2역변환($\widetilde{T}$), 및 상기 제3맵($\mathcal{F}$)을 이용하여 상기 메시지(m)에 대한 서명(σ)을 생성하는 단계; 및

상기 공개키($\mathcal{P}$), 상기 서명(σ), 및 상기 메시지(m)를 이용하여 $\mathcal{P}(\sigma) = H(\mathrm{m})$인지를 검증하는 단계를 포함하는 전자 장치를 이용한 전자 서명 방법.

청구항 17

전자 장치를 이용한 전자 서명 방법에 있어서,

제1아핀 맵($S : \mathbb{F}_q^m \to \mathbb{F}_q^m$), 제2아핀 맵 ($T : \mathbb{F}_q^n \to \mathbb{F}_q^n$), 및 제3맵 ($\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$)을 획득하는 단계;

상기 제1아핀 맵, 상기 제2아핀 맵, 및 상기 제3맵를 이용하여 공개키 ($\mathcal{P} = S \circ \mathcal{F} \circ T$)를 생성하는 단계; 및

상기 공개 키($\mathcal{P}$)를 상기 전자 장치의 외부로 전송한 후, 상기 전자 장치의 외부로부터 상기 공개 키($\mathcal{P}$)에 대한 인증서를 수신하는 단계를 포함하고,

상기 제3맵($\mathcal{F}$)은 n개의 변수들과 m개의 방정식들을 갖는 다변수 이차 다항식들($\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$)의 시스템이고,

상기 다변수 이차 다항식들 중에서 적어도 하나는 0이 아닌 계수의 오일-오일 이차항을 갖고,

상기 제3맵($\mathcal{F}$)은 오일과 비니거 방식에서 사용되는 비니거 변수들을 정의하기 위한 적어도 하나의 제1인덱스 집합과 상기 오일과 비니거 방식에서 사용되는 오일 변수들을 정의하기 위한 적어도 하나의 제2인덱스 집합을 포함하고,

$\mathbb{F}_q$는 원소들의 개수가 q인 유한체인 전자 장치를 이용한 전자 서명 방법.

청구항 18

제17항에 있어서,

레이어의 개수 u가 1 이상일 때, $v_1, \cdots, v_{u+1}$는 정수들(integers)이고, $0 < v_1 < v_2 < \cdots < v_u < v_{u+1} = n$이고,

상기 적어도 하나의 제1인덱스 집합은 정수들의 집합들($V_i = \{1, \cdots, v_i\}$)이고,

상기 적어도 하나의 제2인덱스 집합은 정수들의 집합들 ($O_i = \{v_i + 1, \cdots, v_{i+1}\}$)이고,

$o_i = v_{i+1} - v_i$이고,

$|V_i| = v_i$이고, $|O_i| = o_i$이고,

$i = 1, \cdots, u$이고,

$m = o_1 + \cdots + o_u$ 고, $n = v_1 + m$ 인 전자 장치를 이용한 전자 서명 방법.

청구항 19

제17항에 있어서

상기 적어도 하나의 제1인덱스 집합은 $V = \{1, \cdots, v\}$ 이고,

상기 적어도 하나의 제2인덱스 집합은 $O_1 = \{v+1, \cdots, v+o_1\}$, $O_2 = \{v+o_1+1, \cdots, v+o_1+o_2\}$ 이고,

$|V| = v$ 이고, $|O_i| = o_i$ 이고, i = 1과 2인 전자 장치를 이용한 전자 서명 방법.

청구항 20

제17항에 있어서,

상기 적어도 하나의 제1인덱스 집합은 $V = \{1, \cdots, v\}$ 이고,

상기 적어도 하나의 제2인덱스 집합은 $O = \{v+1, \cdots, v+o\}$ 이고,

$|V| = v$ 이고, $|O| = o$ 인 전자 장치를 이용한 전자 서명 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 전자서명에 관한 것으로, 특히 0이 아닌 계수의 오일-오일 이차항을 갖는 센트럴 맵에 기초한 양자 컴퓨터에 안전한 다변수 이차식 전자서명 스킴을 수행할 수 있는 방법과 상기 방법을 실행할 수 있는 전자 장치에 관한 것이다.

배 경 기 술

[0002] 다변수 이차식 서명(multivariate quadratic signature)은 다변수 암호 (multivariate cryptography) 시스템에서 사용되는 전자서명(또는 '디지털 서명'이라고도 함.)을 의미한다. 여기서, 다변수 암호 시스템은 유한체(finite field) 위에서 정의된 다변수 다항식들을 기반으로 하는 비대칭(asymmetric) 암호 시스템을 의미한다.

[0003] 특히, 다변수 암호 시스템에서 사용되는 다변수 다항식들의 차수(degree)가 2인 경우, 상기 다변수 암호 시스템을 다변수 이차식 암호 시스템이라고 한다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 미국등록공보 US 8,811,608 B2 (2014. 08. 19.)

(특허문헌 0002) 미국등록공보 US 7,158,636 B2 (2007. 01. 02.)

발명의 내용

해결하려는 과제

[0005] 본 발명이 이루고자 하는 기술적인 과제는 0이 아닌 계수의 오일-오일 이차항을 갖는 다항식을 다변수 이차 다항식들 중에서 적어도 하나에 추가하여 오일-오일 이차항이 없는 구조를 파괴하고, 다변수 이차 다항식들 중에

서 0이 아닌 계수의 오일-오일 이차항을 갖는 다항식이 적어도 하나가 존재함에도 불구하고 다변수 이차식 센트럴 맵을 역변환하여 메시지에 대한 전자서명을 생성할 수 있는 다변수 이차식 전자서명 스킴을 이용하는 방법과 상기 방법을 실행할 수 있는 전자 장치를 제공하는 것이다.

과제의 해결 수단

[0006] 본 발명의 실시 예에 따른 키 생성 장치를 포함하는 전자 장치에서, 상기 키 생성 장치는 제1아핀 맵($S : \mathbb{F}_q^m \to \mathbb{F}_q^m$), 제2아핀 맵 ($T : \mathbb{F}_q^n \to \mathbb{F}_q^n$), 및 제3맵($\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$)을 획득하고, 상기 제1아핀 맵, 상기 제2아핀 맵, 및 상기 제3맵를 이용하여 공개키 ($\mathcal{P} = S \circ \mathcal{F} \circ T$)를 생성하고, 상기 제3맵($\mathcal{F}$)은 n개의 변수들과 m개의 방정식들을 갖는 다변수 이차 다항식들($\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$)의 시스템이고, 상기 다변수 이차 다항식들 중에서 적어도 하나는 0이 아닌 계수의 오일-오일 이차항을 갖고, 상기 제3맵($\mathcal{F}$)은 오일과 비니거 방식에서 사용되는 비니거 변수들을 정의하기 위한 적어도 하나의 제1인덱스 집합과 상기 오일과 비니거 방식에서 사용되는 오일 변수들을 정의하기 위한 적어도 하나의 제2인덱스 집합을 포함하고, $\mathbb{F}_q$는 원소들의 개수가 q이다.

[0007] 본 발명의 실시 예에 따른 전자 장치를 이용한 전자서명 방법은 제1아핀 맵 ($S : \mathbb{F}_q^m \to \mathbb{F}_q^m$), 제2아핀 맵 ($T : \mathbb{F}_q^n \to \mathbb{F}_q^n$), 및 제3맵 ($\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$)을 획득하는 단계; 상기 제1아핀 맵, 상기 제2아핀 맵, 및 상기 제3맵를 이용하여 공개키 ($\mathcal{P} = S \circ \mathcal{F} \circ T$)를 생성하는 단계를 포함하고, 상기 제3맵($\mathcal{F}$)은 n개의 변수들과 m개의 방정식들을 갖는 다변수 이차 다항식들($\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$)의 시스템이고, 상기 다변수 이차 다항식들 중에서 적어도 하나는 0이 아닌 계수의 오일-오일 이차항을 갖고, 상기 제3맵($\mathcal{F}$)은 오일과 비니거 방식에서 사용되는 비니거 변수들을 정의하기 위한 적어도 하나의 제1인덱스 집합과 상기 오일과 비니거 방식에서 사용되는 오일 변수들을 정의하기 위한 적어도 하나의 제2인덱스 집합을 포함하고, $\mathbb{F}_q$는 원소들의 개수는 q이다.

[0008] 본 발명의 실시 예에 따른 전자 장치를 이용한 전자서명 방법은 제1아핀 맵 ($S : \mathbb{F}_q^m \to \mathbb{F}_q^m$), 제2아핀 맵 ($T : \mathbb{F}_q^n \to \mathbb{F}_q^n$), 및 제3맵 ($\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$)을 획득하는 단계; 상기 제1아핀 맵, 상기 제2아핀 맵, 및 상기 제3맵를 이용하여 공개키 ($\mathcal{P} = S \circ \mathcal{F} \circ T$)를 생성하는 단계; 및 상기 공개키($\mathcal{P}$)를 상기 전자 장치의 외부로 전송한 후, 상기 전자 장치의 외부로부터 상기 공개 키($\mathcal{P}$)에 대한 인증서를 수신하는 단계를 포함하고, 상기 제3맵($\mathcal{F}$)은 n개의 변수들과 m개의 방정식들을 갖는 다변수 이차 다항식들($\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$)의 시스템이고, 상기 다변수 이차 다항식들 중에서 적어도 하나는 0이 아닌 계수의 오일-오일 이차항을 갖고, 상기 제3맵($\mathcal{F}$)은 오일과 비니거 방식에서 사용되는 비니거 변수들을 정의하기 위한 적어도 하나의 제1인덱스 집합과 상기 오일과 비니거 방식에서 사용되는 오일 변수들을 정의하기 위한 적어도 하나의 제2인덱스 집합을 포함하고, $\mathbb{F}_q$는 원소들의 개수는 q이다.

발명의 효과

[0009] 본 발명의 실시 예에 따른 다변수 이차식 전자서명 스킴은 0이 아닌 계수의 오일-오일 이차항을 갖는 센트럴 맵에 기초하여 상기 0이 아닌 계수의 오일-오일 이차항이 존재함에도 불구하고 상기 센트럴 맵을 역변환하여 메시지에 대한 전자서명을 안전하게 생성할 수 있는 갖는 효과가 있다.

도면의 간단한 설명

[0010] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명에 따른 센트럴 맵의 이차항 부분에 관련된 대칭 행렬의 실시 예이다.

도 2는 본 발명의 실시 예들에 따른 전자 장치의 블록도이다.

도 3은 본 발명의 실시 예들에 따른 전자 장치의 블록도이다.

도 4는 본 발명의 실시 예들에 따른 전자 장치의 블록도이다.

도 5는 도 2, 도 3, 또는 도 4에 도시된 전자 장치의 작동을 설명하는 플로우 차트이다.

발명을 실시하기 위한 구체적인 내용

[0011] 이하, 첨부된 도면들을 참조하여 본 발명을 실시하기 위한 구체적인 내용을 설명한다.

[0012] 본 명세서에서는, 오일-오일 이차항을 갖는 센트럴 맵(또는 '비밀 센트럴 맵'이라고도 함.)에 기초한 양자 컴퓨터에 안전한 다변수 이차식 전자서명 스킴이 개시된다.

[0013] 다변수 이차식(multivariate quadratic(MQ)) 전자서명 스킴의 구성에 대한 주요 아이디어는 n개의 변수들을 갖는 m개의 다변수 이차 다항식들의 가역변환 맵 (invertable map; $\mathcal{F}:\mathbb{F}_q^n \to \mathbb{F}_q^m$)을 찾는 것이다. 그 후에 공개키($\mathcal{P}$)로 센트럴 맵(cental map; $\mathcal{F}$)의 특별한 구조를 감추기 위해 2 개의 가역 아핀 맵들 (invertable affine maps) 또는 2 개의 가역 선형 맵들(linear invertable maps; $S:\mathbb{F}_q^m \to \mathbb{F}_q^m$ 와 $T:\mathbb{F}_q^n \to \mathbb{F}_q^n$)이 선택된다. 본 명세서에서, i, j, n, m, k, q, 및 v 각각은 1 이상의 자연수이다.

[0014] 공개키($\mathcal{P}$)는 이차 맵(quadratic map; $\mathcal{P} = S \circ \bar{\mathcal{F}} \circ T$)으로 구성되고, 공개키($\mathcal{P}$), 즉 이차 맵($\mathcal{P} = S \circ \bar{\mathcal{F}} \circ T$)은 랜덤 시스템과 거의 구별되지 않으므로 역변환하기(invert) 어렵다. 여기서, 원(circle)은 합성(composition)을 의미한다. 비밀키는 공개키($\mathcal{P}$)를 역변환시킬 수 있는 ($S, \mathcal{F}, T$)로 구성된다.

[0015] 공개키($\mathcal{P}$)는 수학식 1에 의해 정의되고, m개의 방정식들과 n개의 변수들을 갖는 다변수 다항식들의 시스템($\mathcal{P} = (\mathcal{P}^{(1)}, \cdots, \mathcal{P}^{(m)})$)이다.

[0016] [수학식 1]

[0017]
$$\mathcal{P}^{(k)}(x_1, \cdots, x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(k)} x_i x_j + \sum_{i=1}^{n} p_i^{(k)} x_i + p_0^{(k)}$$

[0018] 여기서, k = 1, …, m이고, $p_{ij}^{(k)}$ 과 $p_i^{(k)}$ 은 해당 항(corresponding term)의 계수(coefficient)를 나타내고, $p_0^{(k)}$ 는 상수(constant)를 나타내고, 각 값은 원소들의 개수가 q개인 유한체(finite field) $\mathbb{F}_q$ 내에서 랜덤하게 선택된다.

[0020] 본 발명의 주요 아이디어들은,

[0021] i) 0이 아닌 계수의 오일-오일 이차항을 갖는 다항식을 다변수 이차 다항식들 중에 적어도 하나에 추가하여 상기 0이 아닌 계수의 오일-오일 이차항이 없는 종래의 다변수 이차 다항식들의 구조를 파괴하고,

[0022] ii) 다변수 이차 다항식들 중에서 0이 아닌 계수의 오일-오일 이차항을 갖는 다항식이 적어도 하나가 존재함에도 불구하고 센트럴 맵의 새로운 역변환 방법을 제공하는 것이다.

[0024] 본 발명에 따른 새로운 센트럴 맵(New Cenral Map):

[0025] 0(zero)이 아닌 계수를 갖는 오일-오일 이차항을 갖는 본 발명에 따른 새로운 센트럴 맵을 구성하기 위해, 본 발명에서 레이어가 1인 경우, 2개의 인텍스 집합들(V와 O)이 필요하다. 예컨대, 오일과 비니거(Oil and Vinegar) 방식에서 사용되는 오일 변수들을 정의하기 위한 인덱스 집합의 개수는 레이어의 개수에 따라 결정되거나 상기 레이어의 개수에 종속적이다.

[0026] $$V = \{1, \cdots, v\}$$

[0027] $$O = \{v+1, \cdots, v+o\}$$

[0028] 여기서, $|V| = v$이고, $|O| = o$ 이다. V는 오일 및 비니거 방식에서 사용되는 비니거 변수들을 정의하기 위한 인덱스 집합이고, O 는 상기 오일 및 비니거 방식에서 사용되는 오일 변수들을 정의하기 위한 인덱스 집합이다.

[0029] 센트럴 맵 $\mathcal{F} = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$, 즉 m = o 개의 방정식들과 n = v + m 개의 변수들을 갖는 다변수 이차 다항식들의 시스템은 수학식 2와 수학식 3와 같이 정의된다.

[0030] $k = 1, \cdots, m-1$ 에 대해 $\mathcal{F}^{(k)}$는 수학식 2와 같이 정의된다.

[0031] [수학식 2]

[0032] $$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i \in O, j \in V} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j \in V, i \le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V \cup O} \gamma_i^{(k)} x_i + \eta^{(k)}$$

[0033] k = m에 대해 $\mathcal{F}^{(k)}$는 수학식 3과 같이 정의된다.

[0034] [수학식 3]

[0035] $$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i \in O, j \in V} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j \in V, i \le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i,j \in O, i \le j} \delta_{ij}^{(k)} x_i x_j + \sum_{i \in V \cup O} \gamma_i^{(k)} x_i + \eta^{(k)}$$

[0036] 여기서, 벡터 $\mathbf{x} = (x_1, \cdots, x_n)$이고, $\alpha_{ij}^{(k)}$, $\beta_{ij}^{(k)}$, $\delta_{ij}^{(k)}$, 및 $\gamma_i^{(k)}$은 해당 항의 계수를 나타내고, $\eta^{(k)}$는 상수를 나타내고, 각 값은 원소의 개수가 q개인 유한체 $\mathbb{F}_q$ 내에서 랜덤하게 선택된다.

[0037] 레이어(layer)가 1일 때, 본 발명에 따른 스킴의 파라미터 세트는 $\mathbb{F}_q, v, o$ 이다.

[0038] 본 발명에 따른 새로운 센트럴 맵을 역변환하는 방법(How to Invert the Cental Map):

[0039] $\xi = (\xi_1, \cdots, \xi_m)$가 주어질 때, $\mathcal{F}^{-1}(\xi) = \mathbf{s}$, 즉 $\mathcal{F}(\mathbf{x}) = \xi$의 해들(solutions) $\mathbf{s}$를 찾는 과정들은 아래와 같다.

[0040] - 제1레이어에서, 비니거 값들(Vinegar values)의 랜덤 벡터, $\mathbf{s_v} = (s_1, \cdots, s_v) \in \mathbb{F}_q^v$가 선택된다. 벡터($\mathbf{s_v}$)가 $i = 1, \cdots, m$에 대한 $\mathcal{F}^{(i)}$에 대입(plug)되면, 0이 아닌 계수를 갖는 하나의 오일-오일 이차 방정식과 o 개의 변수들 $(x_{v+1}, \cdots, x_n)$을 갖는 $o-1$ 개의 방정식들의 선형 시스템이 구해진다.

[0041] - 상기 선형 시스템에 가우스 소거법을 이용하면, $i = v+1, \cdots, n-1$에 대한 각 변수 x_i는 변수 x_n의 방정식에 의해 표현될 수 있다.

[0042] - $i = v+1, \cdots, n-1$에 대한 x_i는 x_n의 이차 방정식이 얻어짐에 따라 $\mathcal{F}^{(m)}$으로부터 획득된 이차 방정식에 대입된다.

[0043] - x_n의 이차 방정식의 해(s_n)가 얻어진 후, $x_n = s_n$으로부터 $i = v+1, \cdots, n-1$에 대한 $x_i = s_i$가 계산된다.

[0044] - 그러면, 벡터 $\mathbf{s} = (s_1, \cdots, s_n)$는 $\mathcal{F}(\mathbf{x}) = \xi$의 해이다.

[0045] 만약, 제1레이어의 선형 시스템 또는 이차 방정식이 해를 갖지 않는다면, 새로운 랜덤 비니거 값들의 벡터($\mathbf{s_v}' = (s_1', \cdots, s_v')$)를 새롭게 선택하여 앞에서 설명한 방법들(또는 과정들)을 다시 수행한다.

[0046] 레이어가 2인 경우, 0이 아닌 계수의 오일-오일 이차항을 갖는 본 발명에 따른 새로운 센트럴 맵을 구성하기 위해, 본 발명에서는 3개의 인덱스 집합들(V, O_1, 및 O_2)이 필요하다.

[0047] $V = \{1, \cdots, v\}$,

[0048] $O_1 = \{v+1, \cdots, v+o_1\}$,

[0049] $O_2 = \{v+o_1+1, \cdots, v+o_1+o_2\}$

[0050] 여기서, $|V| = v$이고, i = 1과 2에 대해 $|O_i| = o_i$이다. V는 오일 및 비니거 방식에서 사용되는 비니거 변수들을 정의하기 위한 인덱스 집합이고, O_1과 O_2는 상기 오일 및 비니거 방식에서 사용되는 오일 변수들을 정의하기 위한 인덱스 집합들이다.

[0051] 센트럴 맵 $\mathcal{F} = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$, 즉 m = o_1 + o_2 개의 방정식들과 n = v + m 개의 변수들을 갖는 다변수 다항식들의 시스템은 수학식 4 내지 수학식 6과 같이 정의된다.

[0052] $k = 1, \cdots, o_1$에 대해 $\mathcal{F}^{(k)}$는 수학식 4와 같이 정의된다.

[0053] [수학식 4]

[0054] $$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_1, j\in V} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O_1} \gamma_i^{(k)} x_i + \eta^{(k)}$$

[0055] $k = o_1 + 1, \cdots, m-1$에 대해 $\mathcal{F}^{(k)}$는 수학식 5와 같이 정의된다.

[0056] [수학식 5]

[0057] $$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_2, j\in V\cup O_1} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V\cup O_1, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O_1\cup O_2} \gamma_i^{(k)} x_i + \eta^{(k)}$$

[0058] k = m에 대해 $\mathcal{F}^{(k)}$는 수학식 6과 같이 정의된다.

[0059] [수학식 6]

[0060] $$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_2, j\in V\cup O_1} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V\cup O_1, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i,j\in O_2, i\le j} \delta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O_1\cup O_2} \gamma_i^{(k)} x_i + \eta^{(m)}$$

[0061] 여기서, 벡터 $\mathbf{x} = (x_1, \cdots, x_n)$이고, $\alpha_{ij}^{(k)}$, $\beta_{ij}^{(k)}$, $\delta_{ij}^{(k)}$, 및 $\gamma_i^{(k)}$은 해당 항(corresponding term)의 계수를 나타내고, $\eta^{(k)}$은 상수를 나타내고, 각 값은 원소의 개수가 q개인 유한체 $\mathbb{F}_q$내에서 랜덤하게 선택된다.

[0062] i = 1, …, o_1에 대한 $\mathcal{F}^{(i)}$는 제1레이어에서의 비밀 다항식(secret polynomial)이라 불리고, i = o_1 + 1, …, m에 대한 $\mathcal{F}^{(i)}$는 제2레이어에서의 비밀 다항식이라 불린다.

[0063] 레이어의 개수가 2일 때, 본 발명에 따른 스킴의 파라미터 세트는 $\mathbb{F}_q, v, o_1, o_2$이다.

[0065] 본 발명에 따른 새로운 센트럴 맵을 역변환하는 방법(How to Invert the Cental Map):

[0066] $\xi = (\xi_1, \cdots, \xi_m)$가 주어질 때, $\mathcal{F}^{-1}(\xi) = \mathbf{s}$, 즉 $\mathcal{F}(\mathbf{x}) = \xi$의 해들(solutions) $\mathbf{s}$를 찾는 과정들은 아래와 같다.

[0067] - 제1레이어에서, 비니거 값들(Vinegar values)의 랜덤 벡터, $\mathbf{s_v} = (s_1, \cdots, s_v) \in \mathbb{F}_q^v$가 선택된다. 벡터($\mathbf{s_v}$)가 $i = 1, \cdots, o_1$에 대한 제1레이어($\mathcal{F}^{(i)}$)에 대입(plug)되면, o_1개의 변수들을 갖는 o_1개의 방정식들의 선형 시스템이 얻어진다. 가우스 소거법(Gaussian elimination)을 사용하여 상기 선형 시스템의 해($s_{v+1}, \cdots, s_{v+o_1}$)가 얻어진다.

[0068] - 제2레이어에서, 비니거 값들의 벡터($\mathbf{s_v}$)와 선형 시스템의 해 ($s_{v+1}, \cdots, s_{v+o_1}$)로 구성된 값 ($s_1, \cdots, s_{v+o_1}$)이 $j = o_1+1, \cdots, m$에 대한 $\mathcal{F}^{(j)}$로 대입된다. 0이 아닌 계수를 갖는 하나의 오일-오일 이차 방정식과 o_2개의 변수들 ($x_{v+o_1+1}, \cdots, x_n$)을 갖는 $o_2 - 1$개의 방정식들의 선형 시스템이 구해진다.

[0069] - 선형 시스템에서 가우스 소거법을 이용하면, $i = v + o_1 + 1, \cdots, n-1$에 대한 각 변수 x_i는 변수 x_n의 방정식에 의해 표현될 수 있다.

[0070] - $i = v + o_1 + 1, \cdots, n-1$에 대한 x_i는 x_n의 이차 방정식이 얻어짐에 따라 $\mathcal{F}^{(m)}$으로부터 획득된 이차 방정식에 대입된다.

[0071] - x_n의 이차 방정식의 해(s_n)가 얻어진 후, $x_n = s_n$으로부터 $i = v + o_1 + 1, \cdots, n-1$에 대한 $x_i = s_i$가 계산된다.

[0072] - 그러면, 벡터 $\mathbf{s} = (s_1, \cdots, s_n)$는 $\mathcal{F}(\mathbf{x}) = \xi$의 해이다.

[0073] 만약, 제1레이어의 선형 시스템 또는 이차 방정식이 해를 갖지 않는다면, 새로운 랜덤 비니거 값들의 벡터($\mathbf{s_v}' = (s_1', \cdots, s_v')$)를 새롭게 선택하여 앞에서 설명한 방법들(또는 과정들)을 다시 수행한다.

[0075] 키 생성(Key Generation) 또는 키 생성 단계:

[0076] 보안 파라미터(λ)에 대해, 공개키와 비밀키의 쌍 ($< PK, SK >=< \mathcal{P}, (\widetilde{S}, \mathcal{F}, \widetilde{T}) >$)이 다음과 따라 생성된다. 보안 파라미터(λ)는 비도(security level)를 나타낼 수 있다.

[0077] 1. 두 개의 아핀 맵들($\widetilde{S}$와 $\widetilde{T}$)이 랜덤하게 선택된다. $\widetilde{S}$와 $\widetilde{T}$가 역변환 가능하지 않다면(invertable), 두 개의 (새로운) 아핀 맵들($\widetilde{S}$와 $\widetilde{T}$)이 랜덤하게 다시 선택된다. 여기서, $\widetilde{S} = S^{-1}$이고, $\widetilde{T} = T^{-1}$이다.

[0078] 2. 앞에서 설명된 센트럴 맵 $\mathcal{F} = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$이 랜덤하게 선택된다.

[0079] 3. 공개키($\mathcal{P} = S \circ \mathcal{F} \circ T$)가 계산된다.

[0081] 서명 생성(Signature Generation) 또는 서명 생성 단계:

[0082] 메시지(m)에 대해 해시 메시지(H(m))가 계산된다.

[0083] 여기서, $H : \{0,1\}^* \rightarrow \mathbb{F}_q^m$는 충돌 방지 해시 함수(collision resistant hash function)이다.

[0084] 1. $\widetilde{S}(H(\mathrm{m})) = \xi$가 계산된다.

[0085] 2. $\mathcal{F}^{-1}(\xi) = \mathbf{s}$ 즉 $\mathcal{F}(\mathbf{s}) = \xi$에 대한 벡터($\mathbf{s}$)가 구해진다.

[0086] 새로운 센트럴 맵을 역변환하는 방법에서 설명한 바와 같이,

[0087] (1) 비니거 값들의 랜덤 벡터 $\mathbf{s_v} = (s_1, \cdots, s_v) \in \mathbb{F}_q^v$가 선택된다.

[0088] (2) 벡터($\mathbf{s_v}$)는 $i = 1, \cdots, o_1$에 대한 제1레이어($\mathcal{F}^{(i)}$)에 대입되고,

[0089] (3) o_1 개의 변수들을 갖는 o_1 개의 방정식들의 선형 시스템이 구해진다.

[0090] (4) 가우스 소거법을 사용하여 상기 선형 시스템의 해 ($s_{v+1}, \cdots, s_{v+o_1}$)가 구해진다.

[0091] - 벡터($\mathbf{s_v}$)와 선형 시스템의 해 $(s_1, \cdots, s_{v+o_1})$ 로 구성된 값($s_1, \cdots, s_{v+o_1}$)이 $i = o_1 + 1, \cdots, m$ 에 대한 $\mathcal{F}^{(i)}$ 로 대입되고, 변수들 $(x_{v+o_1+1}, \cdots, x_n)$ 을 갖는 하나의 이차 방정식과 o_2 개의 변수들을 갖는 $o_2 - 1$ 개의 방정식들의 선형 시스템이 얻어진다.

[0092] 선형 시스템에서,

[0093] 변수 x_n 의 방정식에 의해 표현되는 $x_i \ (i = v + o_1 + 1, \cdots, n-1)$ 가 얻어진다.

[0094] $i = v + o_1 + 1, \cdots, n-1$ 에 대한 x_i 는 x_n 의 이차 방정식이 얻어짐에 따라 $\mathcal{F}^{(m)}$ 으로부터 획득된 이차 방정식에 대입된다.

[0095] x_n 의 이차 방정식의 해(s_n)가 얻어진 후, $x_n = s_n$ 으로부터 $i = v + o_1 + 1, \cdots, n-1$ 에 대한 $x_i = s_i$ 가 계산된다.

[0096] 그러면, $\mathbf{s} = (s_1, \cdots, s_n)$ 는 $\mathcal{F}(\mathbf{x}) = \xi$ 의 해이다.

[0097] 만일, 제1레이어의 선형 시스템과 제2레이어의 이차 방정식 중에서 어느 하나가 해를 갖고 있지 않으면, 비니거 값들의 다른 벡터 $\mathbf{s_v}' = (s'_1, \cdots, s'_v)$ 가 선택되고, 앞에서 설명된 과정들이 다시 수행된다.

[0098] 3. $\widetilde{T}(\mathbf{s}) = \sigma$ 가 계산된다. σ 는 메시지(m)의 전자서명을 의미한다.

[0100] 검증(Verify) 또는 검증 단계:

[0101] 메시지(m)에 대한 전자서명(σ)과 공개키($\mathcal{P}$)가 주어지면, $\mathcal{P}(\sigma) =$ H(m)인지가 체크된다. $\mathcal{P}(\sigma) =$ H(m) 이면 전자서명(σ)이 수락되고, 그렇지 않으면 전자서명(σ)은 거절된다.

[0102] 도 1은 본 발명에 따른 센트럴 맵의 이차항 부분에 관련된 대칭 행렬의 실시 예이다. 도 1을 참조하면, $F^{(k)} \ (1 \le k \le m)$ 은 본 발명의 실시 예에 따른 센트럴 맵($\mathcal{F}$)의 k-번째 다항식의 호모지니어스 이차항 부분(homogeneous quadratic part)에 해당하는 대칭 행렬들(symmetric matrices)이다.

[0103] 도 1에 도시된 대칭 행렬들($F^{(i)}$)을 참조하면, 백색 부분들(white parts)은 0인 원소들을 나타내고, 그레이 부분들(gray parts 또는 사각형)은 0이 아닌 원소들을 나타낸다. $P^{(k)} \ (1 \le k \le m)$ 는 공개키($\mathcal{P}$)의 k-번째 다항식의 이차항 부분(quadratic part)에 해당하는 대칭 행렬들이다. 도 1을 참조하면 k = m일 때 $o_2 \times o_2$ 항들(또는 오일-오일 이차항)에 0이 아닌 원소들이 존재한다. $1 \le k \le m$일 때, k가 어떤 값을 갖더라도 오일-오일 이차항을 갖는 $\mathcal{F}^{(k)}$ 는 존재할 수 있다.

[0105] 예컨대, 레이어가 2개인 경우,

[0106] 제1레이어에서, $k = 1, \cdots, o_1$ 에 대해 $\mathcal{F}^{(k)}$ 는 수학식 7과 같이 정의된다.

[0107] [수학식 7]

[0108] $$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_1, j\in V} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O_1} \gamma_i^{(k)} x_i + \eta^{(k)}$$

[0109] 제2레이어에서, $k = o_1 + 1, \cdots, m-1$에 대해 $\mathcal{F}^{(k)}$는 수학식 8과 같이 정의된다.

[0110] [수학식 8]

[0111] $$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_2, j\in V\cup O_1} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V\cup O_1, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O_1\cup O_2} \gamma_i^{(k)} x_i + \eta^{(k)}$$

[0112] 상기 제2레이어에서, k = m에 대해 $\mathcal{F}^{(k)}$는 수학식 9와 같이 정의된다.

[0113] [수학식 9]

[0114] $$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_2, j\in V\cup O_1} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V\cup O_1, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i,j\in O_2, i\le j} \delta_{ij}^{(k)} x_i x_j + \sum_{i\in V\cup O_1\cup O_2} \gamma_i^{(k)} x_i + \eta^{(m)}$$

[0116] 일반적인 경우(General Case)를 설명하면 아래와 같다.

[0117] u≥1일 때, $v_1, \cdots, v_{u+1}$는 정수들(integers)이고, $0 < v_1 < v_2 < \cdots < v_u < v_{u+1} = n$이다. 여기서 u는 레이어의 개수를 나타낸다.

[0118] $i = 1, \cdots, u$에 대한 정수들의 집합들($V_i = \{1, \cdots, v_i\}$)과, $i = 1, \cdots, u$일 때 집합($o_i = v_{i+1} - v_i$)과 집합 ($O_i = \{v_i + 1, \cdots, v_{i+1}\}$)이 정의된다. 그러면, $|V_i| = v_i$이고, $|O_i| = o_i$이고, $m = o_1 + \cdots + o_u$이고, $n = v_1 + m$이고, $v_1 = v$이다.

[0119] $k = 1, \cdots, m-1$에 대해, n개의 변수들($x_1, \cdots, x_n$)을 갖는 다항식들($F^{(k)}$)은 수학식 10에 의해 정의된다.

[0120] [수학식 10]

[0121] $$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_l, j\in V_l} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V_l, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V_l\cup O_l} \gamma_i^{(k)} x_i + \eta^{(k)}$$

[0122] 여기서, l이 $k \in O_l$을 만족하는 유일한 정수이고, $\mathbf{x} = (x_1, \cdots, x_n)$이다.

[0123] k = m일 때, 다항식들($F^{(k)}$)은 수학식 11에 의해 정의된다.

[0124] [수학식 11]

[0125] $$\mathcal{F}^{(k)}(\mathbf{x}) = \sum_{i\in O_u, j\in V_u} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j\in V_u, i\le j} \beta_{ij}^{(k)} x_i x_j + \sum_{i,j\in O_u, i\le j} \delta_{ij}^{(k)} x_i x_j + \sum_{i\in V_u\cup O_u} \gamma_i^{(k)} x_i + \eta^{(k)}$$

[0127] 도 2는 본 발명의 실시 예들에 따른 전자 장치의 블록도이다. 도 2를 참조하면, 전자 장치(100A)는 키 생성 장치(200A), 디지털서명 생성 장치(300A), 및 검증 장치(400)를 포함할 수 있다. 본 명세서에서 설명될 전자 장치(100A, 100B, 또는 100C, 집합적으로 100)는 0이 아닌 계수의 오일-오일(또는 오일×오일) 이차항을 갖는 센트

럴 맵 ($\mathcal{F}=(\mathcal{F}^{(1)},\cdots,\mathcal{F}^{(m)})$)에 근거한 다변수 이차식 전자서명 스킴에 따라 전자서명(σ)을 생성하고 검증하는 전자 시스템(또는 양자 컴퓨터)을 의미할 수 있다.

[0128] 비록, 도 2 내지 도 4에서는 키 생성 장치, 디지털서명(또는 전자서명) 생성 장치, 및 검증 장치 각각이 서로 분리된 하드웨서에서 구현된 형태로 도시되어 있으나, 키 생성 장치에 해당하는 구성, 디지털서명 생성 장치에 해당하는 구성, 및 검증 장치에 해당하는 구성 모두는 컴퓨터 프로그램(또는 컴퓨터 프로그램 코드)으로 작성될 수 있다.

[0129] 키 생성 장치(200A)는 앞에서 설명된 키 생성(또는 키 생성 단계)을 수행할 수 있다. 예컨대, 키 생성 장치(200A)는 제1아핀 맵(S), 제2아핀 맵(T), 및 제3맵(예컨대, 센트럴 맵($\mathcal{F}$))을 이용하여 공개키($\mathcal{P}=(\mathcal{P}^{(1)},\cdots,\mathcal{P}^{(m)})=S\circ\mathcal{F}\circ T$)를 생성할 수 있다.

[0130] 키 생성 장치(200A)는 프로세서(210)와 메모리 장치(220)를 포함할 수 있다. 메모리 장치(220)는 제1아핀 맵(S), 제2아핀 맵(T), 및 제3맵(즉, 센트럴 맵 ($\mathcal{F}$))을 포함하는 맵들을 저장하는 불휘발성 메모리 장치로 구현될 수 있다.

[0131] 프로세서(210)는 메모리 장치(220)에 저장된 맵들(S, T, 및 $\mathcal{F}$)을 이용하여 공개키($\mathcal{P}=(\mathcal{P}^{(1)},\cdots,\mathcal{P}^{(m)})=S\circ\mathcal{F}\circ T$)를 생성하고, 보안 파라미터(λ)는 키 생성 장치(200A)의 외부로부터 입력될 수 있다.

[0132] 키 생성 장치(200A)는 맵들(S, T, 및 $\mathcal{F}$) 및 공개키 ($\mathcal{P}=(\mathcal{P}^{(1)},\cdots,\mathcal{P}^{(m)})= S\circ\mathcal{F}\circ T$)를 제1통신 네트워크를 통해 디지털서명 생성 장치(300A)로 전송할 수 있다.

[0133] 실시 예들에 따라, 키 생성 장치(200A)는 공개키($\mathcal{P}$)를 인증서 생성장치(또는 인증기관)으로 전송하면, 상기 인증서 생성장치는 공개키($\mathcal{P}$)에 대한 인증서를 생성하고, 생성된 인증서를 키 생성 장치(200A)로 전송할 수 있다. 따라서, 키 생성 장치(200A)는 공개키($\mathcal{P}$) 및/또는 상기 인증서를 디지털서명 생성 장치(300A)로 전송할 수 있다. 본 명세서와 청구항에서 공개키($\mathcal{P}$)는 공개키($\mathcal{P}$)와 공개키 ($\mathcal{P}$)에 대한 인증서를 총칭하는 의미로 이해될 수 있다.

[0134] 디지털서명 생성 장치(300A)는 앞에서 설명한 서명 생성(또는 서명 생성 단계)을 수행할 수 있다. 예컨대, 디지털서명 생성 장치(300A)의 프로세서(310)는 키 생성 장치(200A)로부터 전송된 맵들(S, T, 및 $\mathcal{F}$)을 수신하고, 맵들(S와 T)의 역변환들($\widetilde{S}=S^{-1}$와 $\widetilde{T}=T^{-1}$)을 계산하고, 계산된 역변환들($\widetilde{S}=S^{-1}$와 $\widetilde{T}=T^{-1}$)을 메모리 장치(320)에 저장하고, 메모리 장치(320)에 저장된 맵들 ($\widetilde{S}=S^{-1}$, $\mathcal{F}$, 및 $\widetilde{T}=T^{-1}$)을 이용하여 서명 생성(또는 서명 생성 단계)을 수행할 수 있다.

[0135] 프로세서(310)는 주어진 메시지(m)에 해시 함수를 적용하여 해시 메시지 (H(m))를 생성하고, 서명 생성(또는 서명 생성 단계)에서 설명한 내용에 기초하여 해시 메시지(H(m))에 대한 전자서명(σ)을 생성하고, 공개키($\mathcal{P}$)와 공개키($\mathcal{P}$)를 포함하는 인증서 중에서 어느 하나, 메시지(m), 및 전자서명(σ)을 제3통신 네트워크를 통해 검증 장치(400)로 동시에 전송할 수 있다.

[0136] 상기 제1통신 네트워크, 상기 제2통신 네트워크, 및 상기 제3통신 네트워크 각각은 동일한 통신 네트워크일 수도 있고 서로 다른 통신 네트워크일 수 있으나 이에 한정되는 것은 아니다. 예컨대, 메시지(m)는 디지털서명 생성 장치(300A)의 외부로부터 입력될 수 있다.

[0137] 검증 장치(400)는 앞에서 설명한 검증(또는 검증 단계)을 수행할 수 있다. 예컨대, 검증 장치(400)는 디지털서

명 장치(300A)로부터 전송된 공개키($\mathcal{P}$)와 공개키($\mathcal{P}$)를 포함하는 인증서 중에서 어느 하나, 메시지(m), 및 전자서명(σ)을 이용하여 P(σ)=H(m) 인지를 체크하고, 체크의 결과에 따라 전자서명(σ)을 수락 (accept)할지 또는 거부(reject)할지를 결정할 수 있다. 예컨대, 검증 장치(400)는 공개키($\mathcal{P}$) 대신에 공개키($\mathcal{P}$)에 대한 인증서를 수신하더라도 상기 인증서로부터 공개키($\mathcal{P}$)를 추출하여 검증 단계를 수행할 수 있다.

[0138] 도 3은 본 발명의 실시 예들에 따른 전자 장치의 블록도이다. 도 3을 참조하면, 전자 장치(100B)는 키 생성 장치(200B), 디지털서명 생성 장치(300B), 및 검증 장치(400)를 포함할 수 있다.

[0139] 키 생성 장치(200B)는 앞에서 설명된 키 생성(또는 키 생성 단계)을 수행할 수 있다. 키 생성 장치(200B)의 메모리 장치(220)는 제1아핀 맵(S), 제2아핀 맵 (T), 및 제3맵(즉, 센트럴 맵($\mathcal{F}$))을 포함하는 맵들과, 각 맵(S와 T)의 각 역변환($\widetilde{S}=S^{-1}$ 및 $\widetilde{T}=T^{-1}$)를 계산하는 기능과 맵들(S, T, 및 $\mathcal{F}$)을 이용하여 공개키($\mathcal{P}=(\mathcal{P}^{(1)},\cdots,\mathcal{P}^{(m)})=S\circ\mathcal{F}\circ T$)를 생성하는 기능을 수행하는 컴퓨터 프로그램을 저장한다.

[0140] 프로세서(210)는 상기 컴퓨터 프로그램을 실행시켜 공개키 ($\mathcal{P}=(\mathcal{P}^{(1)},\cdots,\mathcal{P}^{(m)})=S\circ\mathcal{F}\circ T$)를 생성할 수 있다. 예컨대, 보안 파라미터(λ)는 키 생성 장치(200A)의 외부로부터 입력될 수 있다.

[0141] 키 생성 장치(200B)는 역변환들($\widetilde{S}$와 $\widetilde{T}$)을 계산하고, 역변환들($\widetilde{S}$와 $\widetilde{T}$)과 제3맵($\mathcal{F}$), 그리고 공개키($\mathcal{P}$)를 디지털서명 생성 장치(300B)로 안전하게 전송한다.

[0142] 실시 예들에 따라, 키 생성 장치(200B)가 공개키($\mathcal{P}$)를 인증서 생성장치(또는 인증기관)으로 전송하면, 상기 인증서 생성장치는 공개키($\mathcal{P}$)에 대한 인증서를 생성하고, 생성된 인증서를 키 생성 장치(200B)로 전송할 수 있다. 그러면, 키 생성 장치(200B)는 역변환들($\widetilde{S}$와 $\widetilde{T}$)과 제3맵($\mathcal{F}$), 그리고 상기 인증서를 디지털서명 생성 장치(300B)로 안전하게 전송한다.

[0143] 디지털서명 생성 장치(300B)는 앞에서 설명한 서명 생성(또는 서명 생성 단계)을 수행할 수 있다. 예컨대, 디지털서명 생성 장치(300B)의 프로세서(310)는 키 생성 장치(200B)로부터 전송된 맵들($\widetilde{S}$, $\widetilde{T}$, 및 $\mathcal{F}$)을 수신하여 메모리 장치 (320)에 저장하고, 메모리 장치(320)에 저장된 맵들($\widetilde{S}=S^{-1}$, $\mathcal{F}$, 및 $\widetilde{T}=T^{-1}$)을 이용하여 서명 생성(또는 서명 생성 단계)을 수행할 수 있다. 실시 예들에 따라 키 생성 장치(200B)가 공개키($\mathcal{P}$)에 대한 인증서를 전송하면, 상기 인증서는 프로세서(310)의 제어에 따라 메모리 장치(320)에 저장될수 있다.

[0144] 디지털서명 생성 장치(300B)의 프로세서(310)는 주어진 메시지(m)에 해시 함수를 적용하여 해시 메시지 (H(m))를 생성하고, 서명 생성(또는 서명 생성 단계)에서 설명한 내용에 기초하여 해시 메시지(H(m))에 대한 전자서명(σ)을 생성하고, 공개키($\mathcal{P}$)와 공개키($\mathcal{P}$)를 포함하는 인증서 중에서 어느 하나, 메시지(m), 및 전자서명(σ)을 제3통신 네트워크를 통해 검증 장치(400)로 동시에 전송할 수 있다.

[0145] 검증 장치(400)는 앞에서 설명한 검증(또는 검증 단계)을 수행할 수 있다. 예컨대, 검증 장치(400)는 디지털서명 장치(300B)로부터 전송된 공개키($\mathcal{P}$)와 공개키($\mathcal{P}$)를 포함하는 인증서 중에서 어느 하나, 메시지(m), 및 전자서명(σ)을 이용하여 P(σ)=H(m) 인지를 체크하고, 체크의 결과에 따라 전자서명(σ)을 수락할지 또는 거부할지를 결정할 수 있다.

[0146] 도 4는 본 발명의 실시 예들에 따른 전자 장치의 블록도이다. 도 2와 도 3을 참조하면, 키 생성 장치(200A 또는 200B)와 디지털서명 생성 장치(300A 또는 300B)는 하나의 시스템 보드 또는 하나의 실리콘 기판을 공유하지 않는 장치들로 구현될 수 있으나, 도 4의 전자 장치(100C)에서 키 생성 장치(200)와 디지털서명 생성 장치(300)는 하나의 전자 장치(500) 내에서 하나의 시스템 보드 또는 하나의 실리콘 기판(501)을 공유할 수 있다. 시스템 보

드(501)는 전자 장치 또는 컴퓨터에서 메인 회로 보드(main circuit board), 메인 PCB(main printed circuit board), 또는 시스템 보드(system board)를 의미할 수 있다.

[0147] 키 생성을 수행하는 키 생성 장치(200)는 정보((S, T, $\mathcal{F}$, 및 $\mathcal{P}$) 또는 ($\tilde{S}$, $\tilde{T}$, $\mathcal{F}$, 및 $\mathcal{P}$))를 디지털 서명 생성 장치(300)로 전송한다. 앞에서 설명한 바와 같이 키 생성 장치(200)는 정보((S, T, 및 $\mathcal{F}$), 또는 ($\tilde{S}$, $\tilde{T}$, $\mathcal{F}$))와 공개키($\mathcal{P}$)를 포함하는 인증서를 디지털서명 생성 장치(300)로 전송한다.

[0148] 서명 생성을 수행하는 디지털서명 생성 장치(300)는 정보((S, T, $\mathcal{F}$, 및 $\mathcal{P}$), 또는 ($\tilde{S}$, $\tilde{T}$, $\mathcal{F}$, 및 $\mathcal{P}$))를 이용하여 전자서명(σ)을 생성하고, 공개키($\mathcal{P}$)와 공개키($\mathcal{P}$)를 포함하는 인증서 중에서 어느 하나, 메시지(m), 및 전자서명(σ)을 제3통신 네트워크를 통해 검증 장치(400)로 동시에 전송할 수 있다. 검증 장치(400)는 검증을 수행할 수 있다.

[0149] 도 5는 도 2, 도 3, 또는 도 4에 도시된 전자 장치의 작동을 설명하는 플로우 차트이다. 도 2부터 도 5를 참조하면, 맵들(S와 T) 또는 역변환($\tilde{S}$와 $\tilde{T}$)이 계산된다(S110). 역변환($\tilde{S}$와 $\tilde{T}$)은 도 2의 디지털서명 생성 장치(300A)에서 계산될 수도 있고, 도 3의 키 생성 장치(200B)에서 계산될 수도 있고, 도 4의 키 생성 장치(200)에서 생성 또는 계산될 수 있다.

[0150] 도 2 내지 도 5를 참조하여 각 장치(100)의 작동을 간단히 설명하면 아래와 같다.

[0151] 키 생성 장치(200A, 200B, 또는 200; 집합적으로(collectively) 200)는 제3맵($\mathcal{F}$)을 랜덤하게 선택한다(S120).

[0152] 키 생성 장치(200)는 공개키($\mathcal{P} = S \circ \bar{\mathcal{F}} \circ T$)를 계산한다(S130).

[0153] 메시지(m)가 주어지면, 디지털서명 생성 장치(300A, 300B, 또는 300; 집합적으로 300)는 H(m)과 $\tilde{S}$(H(m))=ξ을 계산한다(S140).

[0154] 디지털서명 생성 장치(300)는 $\mathcal{F}^{-1}(\xi) = \mathbf{s}$을 계산한다(S150).

[0155] 디지털서명 생성 장치(300)는 $\tilde{T}(\mathbf{s}) = \sigma$을 계산한다(S160).

[0156] 검증 장치(400)는 디지털서명 생성 장치(300)로부터 전송된 공개키 ($\mathcal{P} = S \circ \bar{\mathcal{F}} \circ T$)와 공개키 ($\mathcal{P} = S \circ \bar{\mathcal{F}} \circ T$)를 포함하는 인증서 중에서 어느 하나, 메시지(m), 및 전자서명(σ)을 이용하여, P(σ)=H(m))인지를 체크한다(S170).

[0157] 본 명세서에서 설명된 키 생성, 서명 생성, 및 검증은 각 장치(100A, 100B, 또는 100C)에서 실행되는 컴퓨터 프로그램(또는 프로그램 코드들)에 의해 수행될 수 있다. 컴퓨터(예컨대, 각 장치(100A, 100B, 또는 100C)와 결합되어 상기 컴퓨터에 의해 읽을 수 있는 컴퓨터 프로그램(또는 프로그램 코드들)은 기록 매체에 저장될 수 있다. 상기 저장 매체(예컨대, 210 또는 220)는 비-일시적인 저장 매체(non-transitory storage medium)을 의미한다.

[0158] 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

[0159] 100A, 100B, 및 100C: 전자 장치 또는 디지털서명 검증 시스템

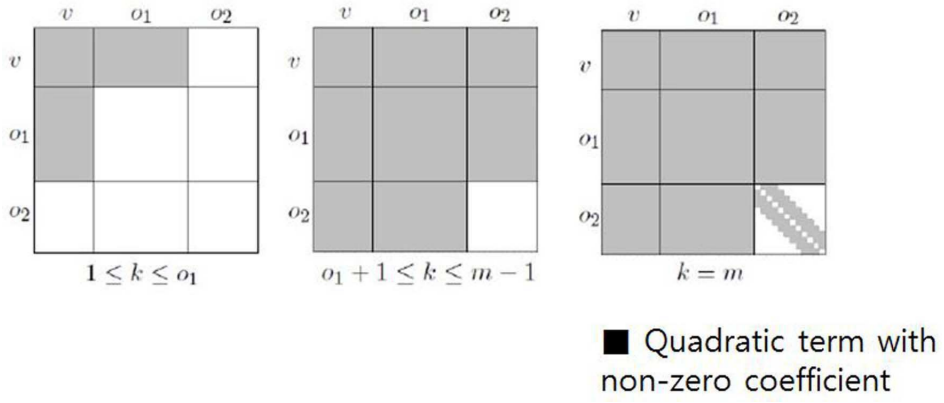
200A, 200B, 및 200: 키 생성 장치

300A, 300B, 및 300: 디지털서명 생성 장치

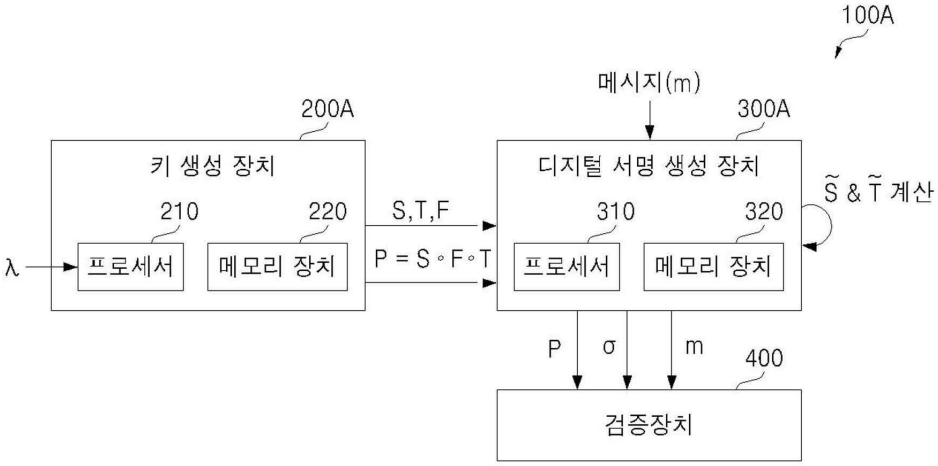
400: 검증 장치

도면

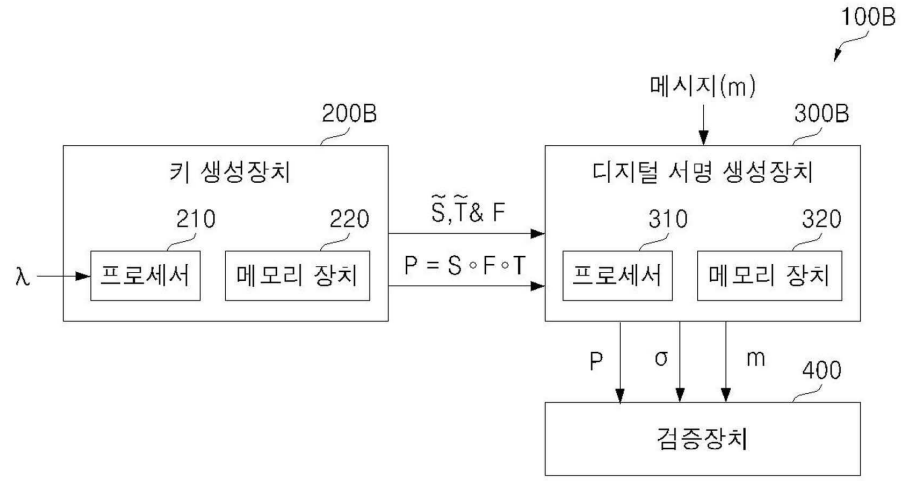
도면1



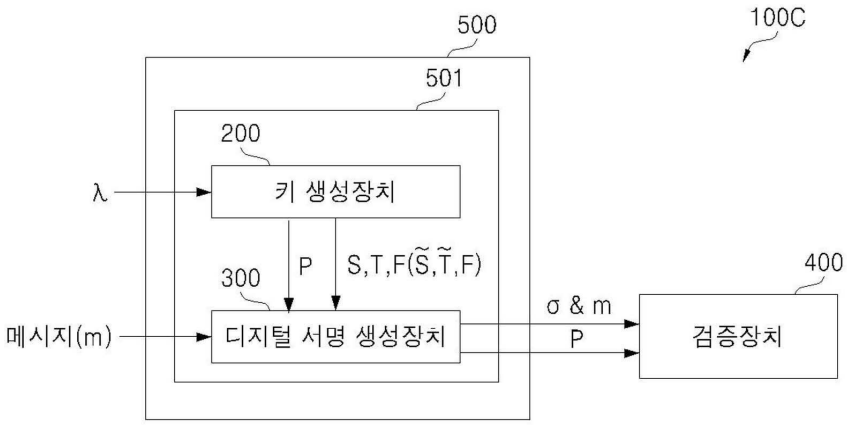
도면2



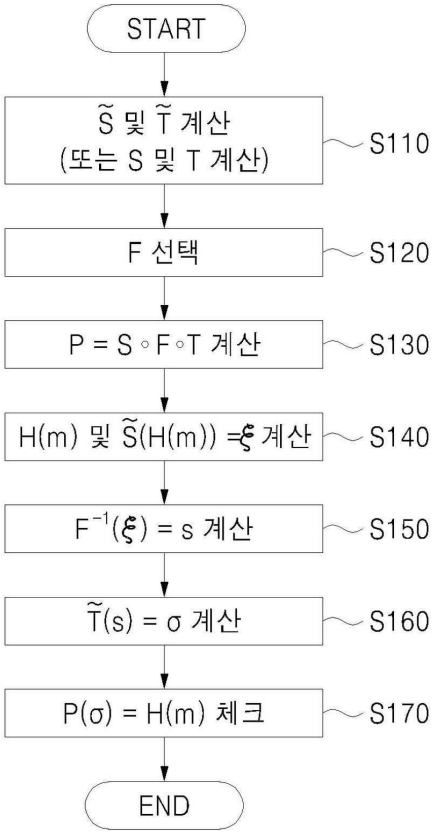
도면3



도면4


500
100C
501
200
λ
키 생성장치
P
S,T,F(S̃,T̃,F)
300
400
σ & m
메시지(m)
디지털 서명 생성장치
P
검증장치

도면5


START
S̃ 및 T̃ 계산
(또는 S 및 T 계산)
S110
F 선택
S120
P = S ◦ F ◦ T 계산
S130
H(m) 및 S̃(H(m)) =ξ 계산
S140
F⁻¹(ξ) = s 계산
S150
T̃(s) = σ 계산
S160
P(σ) = H(m) 체크
S170
END