(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0061194
(43) 공개일자 2021년05월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/3026 (2013.01)
H04L 9/3236 (2013.01)
(21) 출원번호 10-2019-0149105
(22) 출원일자 2019년11월19일
심사청구일자 2019년11월29일

(71) 출원인
기초과학연구원
대전광역시 유성구 엑스포로 55(도룡동)
(72) 발명자
심경아
대전광역시 유성구 지족북로 60, 201동401호(한화꿈에그린2블럭)
문현석
대전광역시 유성구 유성대로1689번길 26-6, 202호(도윤빌라)
(74) 대리인
윤재석

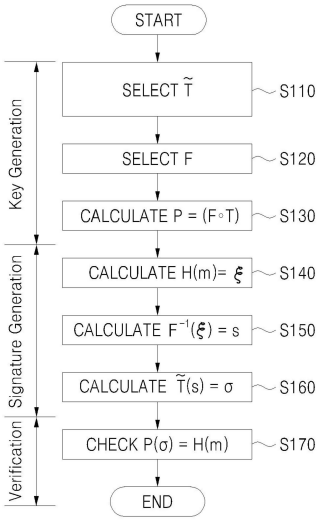
전체 청구항 수 : 총 21 항

(54) 발명의 명칭 **구조화된 행렬들에 기초한 공개키 암호를 위한 방법과 장치**

(57) 요 약

키 생성기를 이용하여 공개키와 비밀키를 생성하는 방법이 개시된다. 상기 방법은 아핀 맵과 비밀 센트럴 맵을 획득하고, 상기 아핀 맵과 상기 비밀 센트럴 맵을 이용하여 공개키와 비밀키를 생성하는 단계를 포함하고, 상기 비밀 센트럴 맵은 o개의 다변수 이차식들의 시스템으로 표현되고, 상기 o개의 다변수 이차식들의 시스템은, 유한체에서 정의된 v개의 일차식들과 v개의 변수들이 주어졌을 때, 구조화된 행렬 또는 구조화된 행렬의 부분 행렬과 벡터의 곱으로 표현 가능하다.

대 표 도 - 도2



(52) CPC특허분류
H04L 9/3247 (2013.01)
H04L 2209/26 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711099800
부처명	과학기술정보통신부
과제관리(전문)기관명	국가수리과학연구소
연구사업명	산업수학 기반연구
연구과제명	경량기기 전용 신규 난제 기반 고속공개키 암호알고리즘 연구
기 여 율	1/1
과제수행기관명	국가수리과학연구소
연구기간	2019.01.01 ~ 2019.12.31

명 세 서

청구범위

청구항 1

키 생성기를 이용하여 공개키와 비밀키를 생성하는 방법에 있어서,

아핀 맵($\widetilde{T}$)과 맵($\mathcal{F}:\mathbb{F}_q^n \to \mathbb{F}_q^m$)을 획득하는 단계; 및

상기 아핀 맵과 상기 맵을 이용하여 공개키($\mathcal{P}=\mathcal{F}\circ T$)와 비밀키 $(\mathcal{F},\widetilde{T})$를 생성하는 단계를 포함하고,

상기 맵($\mathcal{F}:\mathbb{F}_q^n \to \mathbb{F}_q^m$)은 o 개의 다변수 이차식들의 시스템 ($\mathcal{F}_V^{(1)},\cdots,\mathcal{F}_V^{(o)}$)으로 표현되고,

유한체($\mathbb{F}_q$)에서 정의된 v 개의 일차식들($L_1,\ldots,L_v$)과 v 개의 변수들 ($x_1,\ldots,x_v$)이 주어졌을 때,

상기 o 개의 다변수 이차식들의 시스템 ($\mathcal{F}_V^{(1)},\cdots,\mathcal{F}_V^{(o)}$)은 아래와 같이 표현되고,

$$\begin{pmatrix}\mathcal{F}_V^{(1)}\\ \mathcal{F}_V^{(2)}\\ \cdots\\ \mathcal{F}_V^{(o)}\end{pmatrix}=\begin{pmatrix}x_1\ x_2\cdots x_v\\ \cdots\cdots\cdots\\ \cdots\cdots\cdots\\ \cdots\cdots\cdots\end{pmatrix}\cdot\begin{pmatrix}L_1\\ L_2\\ \cdots\\ L_v\end{pmatrix}=M_V\cdot\begin{pmatrix}L_1\\ L_2\\ \cdots\\ L_v\end{pmatrix}$$

여기서, $T:\mathbb{F}_q^n \to \mathbb{F}_q^n$ 이고, $\widetilde{T}=T^{-1}$ 이고,

M_V 는 구조화된 행렬 또는 구조화된 행렬의 부분 행렬이고,

$m=o$ 이고,

$V=\{1,\cdots,v\}$

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

$|V|=v$ 이고, $|O|=o$ 이고, V 는 비니거(Vinegar) 변수들을 정의하기 위한 인덱스 집합이고, O 는 오일(Oil) 변수들을 정의하기 위한 인덱스 집합인 공개키와 비밀키를 생성하는 방법.

청구항 2

제1항에 있어서,

상기 o 개의 다변수 이차식들의 시스템($\mathcal{F}_V^{(1)},\cdots,\mathcal{F}_V^{(o)}$)이 아래와 같이 표현될 때,

$$\begin{pmatrix}\mathcal{F}_V^{(1)}\\ \mathcal{F}_V^{(2)}\\ \cdots\\ \mathcal{F}_V^{(o)}\end{pmatrix}=\begin{pmatrix}x_1 & x_2 & \cdots & x_v\\ x_v & x_1 & \cdots & x_{v-1}\\ \cdots & \cdots & \cdots & \cdots\\ x_{v-o+2} & x_{v-o+3} & \cdots & x_{v-o+1}\end{pmatrix}\cdot\begin{pmatrix}L_1\\ L_2\\ \cdots\\ L_v\end{pmatrix}=M_V\cdot\begin{pmatrix}L_1\\ L_2\\ \cdots\\ L_v\end{pmatrix}$$

여기서, M_V 는 순환 행렬 또는 순환 행렬의 부분 행렬인 공개키와 비밀키를 생성하는 방법.

청구항 3

제1항에 기재된 공개키와 비밀키를 생성하는 방법을 수행하기 위해 저장 매체에 저장된 컴퓨터 프로그램.

청구항 4

제1항에 기재된 공개키와 비밀키를 생성하는 방법을 수행하는 상기 키 생성기;

상기 아핀 맵($\widetilde{T}$), 상기 맵($\mathcal{F}$), 및 메시지(m)를 이용하여 상기 메시지(m)의 전자 서명(σ)을 생성하는 서명 생성기; 및

상기 메시지(m), 상기 전자 서명(σ), 및 상기 공개키($\mathcal{P}=\mathcal{F}\circ T$)를 이용하여 상기 전자 서명($\sigma$)을 검증하는 서명 검증기를 더 포함하고,

상기 서명 생성기는,

상기 메시지(m)에 대한 해시 메시지($H(m)=\xi$)를 계산하고,

$\xi=(\xi_1,\cdots,\xi_m)$가 주어질 때, $\mathcal{F}(\mathbf{x})=\xi$의 해($\mathbf{s}=(s_1,\cdots,s_n)$)를 $\mathcal{F}^{-1}(\xi)=\mathbf{s}$을 이용하여 계산하고,

$\widetilde{T}(\mathbf{s})=\sigma$를 계산하고,

상기 서명 검증기는 $P(\sigma)=H(m)$ 인지를 판단하고 판단 결과에 따라 상기 전자 서명(σ)을 검증하고,

$H:\{0,1\}^*\rightarrow\mathbb{F}_q^m$

$H(m)=\xi=(\xi_1,\cdots,\xi_m)\in\mathbb{F}_q^m$ 인 전자 서명기.

청구항 5

키 생성기를 이용하여 공개키와 비밀키를 생성하는 방법에 있어서,

아핀 맵($\widetilde{T}$)과 맵($\mathcal{F}:\mathbb{F}_q^n\rightarrow\mathbb{F}_q^m$)을 획득하는 단계; 및

상기 아핀 맵과 상기 맵을 이용하여 공개키($\mathcal{P}=\mathcal{F}\circ T$)와 비밀키 $(\mathcal{F},\widetilde{T})$를 생성하는 단계를 포함하고,

상기 맵($\mathcal{F}:\mathbb{F}_q^n\rightarrow\mathbb{F}_q^m$)은 o 개의 다변수 이차식들의 시스템 ($\mathcal{F}_{OV}^{(1)},\cdots,\mathcal{F}_{OV}^{(o)}$)으로 표현되고,

유한체($\mathbb{F}_q$)에서 정의된 v 개의 변수들($x_1,\ldots,x_v$)과 o 개의 변수들 ($x_{v+1},x_{v+2},\cdots,x_{v+o}$)이 주어졌을 때, 상기 o 개의 다변수 이차식들의 시스템 ($\mathcal{F}_{OV}^{(1)},\cdots,\mathcal{F}_{OV}^{(o)}$)은 아래와 같이 표현되고,

$$\begin{pmatrix} \mathcal{F}_{OV}^{(1)} \\ \mathcal{F}_{OV}^{(2)} \\ \vdots \\ \mathcal{F}_{OV}^{(o)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}^T\mathbf{a}_{11} & \mathbf{v}^T\mathbf{a}_{12} & \cdots & \mathbf{v}^T\mathbf{a}_{1o} \\ \mathbf{v}^T\mathbf{a}_{21} & \mathbf{v}^T\mathbf{a}_{22} & \cdots & \mathbf{v}^T\mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}^T\mathbf{a}_{o1} & \mathbf{v}^T\mathbf{a}_{o2} & \cdots & \mathbf{v}^T\mathbf{a}_{oo} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix} + B \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{v}^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}^T \end{pmatrix} \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{oo} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix} + B \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix}$$

여기서,

$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1o} \\ b_{21} & b_{22} & \cdots & b_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ b_{o1} & b_{o2} & \cdots & b_{oo} \end{pmatrix}, \quad M_{OV} = \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{oo} \end{pmatrix}$$ 이고,

$\mathbf{v}^T = [x_1 \quad x_2 \quad \cdots \quad x_v]$ 이고,

$T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ 이고, $\widetilde{T} = T^{-1}$ 이고,

각 열 벡터(a_{ij})를 하나의 행렬의 원소로 간주했을 때, M_{OV}가 구조화된 행렬이 되도록 각 열 벡터(a_{ij})가 선택되고, B도 M_{OV}와 동일한 형태의 구조화된 행렬이 되도록 원소 값들(b_{ij})이 선택되는 공개키와 비밀키를 생성하는 방법.

청구항 6

제5항에 있어서,

$o(=2k)$가 짝수일 때,

M_{OV}가 아래와 같이 표현될 때, M_{OV}는 벡터들의 블록 순환 행렬이고,

$$M_{OV} = \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o1} & \mathbf{a}_{o2} & \cdots & \mathbf{a}_{oo} \end{pmatrix} = \begin{pmatrix} \mathbf{p}_1 & \mathbf{p}_2 & \cdots & \mathbf{p}_k & \mathbf{q}_1 & \mathbf{q}_2 & \cdots & \mathbf{q}_k \\ \mathbf{p}_k & \mathbf{p}_1 & \cdots & \mathbf{p}_{k-1} & \mathbf{q}_k & \mathbf{q}_1 & \cdots & \mathbf{q}_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{p}_2 & \mathbf{p}_3 & \cdots & \mathbf{p}_1 & \mathbf{q}_2 & \mathbf{q}_3 & \cdots & \mathbf{q}_1 \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_k & \mathbf{s}_1 & \mathbf{s}_2 & \cdots & \mathbf{s}_k \\ \mathbf{r}_k & \mathbf{r}_1 & \cdots & \mathbf{r}_{k-1} & \mathbf{s}_k & \mathbf{s}_1 & \cdots & \mathbf{s}_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{r}_2 & \mathbf{r}_3 & \cdots & \mathbf{r}_1 & \mathbf{s}_2 & \mathbf{s}_3 & \cdots & \mathbf{s}_1 \end{pmatrix} = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}$$

$\mathbf{p}_i, \mathbf{q}_i, \mathbf{r}_i$ 와 $\mathbf{s}_i$ 각각은 크기(v)를 가지는 열 벡터이고,

P, Q, R, S 각각은 벡터들의 순환 행렬이고,

B 가 아래와 같이 표현될 때, B 는 블록 순환 행렬인,

$$B=\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1o} \\ b_{21} & b_{22} & \cdots & b_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ b_{o1} & b_{o2} & \cdots & b_{oo} \end{pmatrix} = \begin{pmatrix} t_1 & t_2 & \cdots & t_k & u_1 & u_2 & \cdots & u_k \\ t_k & t_1 & \cdots & t_{k-1} & u_k & u_1 & \cdots & u_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t_2 & t_3 & \cdots & t_1 & u_2 & u_3 & \cdots & u_1 \\ v_1 & v_2 & \cdots & v_k & w_1 & w_2 & \cdots & w_k \\ v_k & v_1 & \cdots & v_{k-1} & w_k & w_1 & \cdots & w_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ v_2 & v_3 & \cdots & v_1 & w_2 & w_3 & \cdots & w_1 \end{pmatrix}$$

공개키와 비밀키를 생성하는 방법.

청구항 7

제5항에 기재된 공개키와 비밀키를 생성하는 방법을 수행하기 위해 저장 매체에 저장된 컴퓨터 프로그램.

청구항 8

제5항에 기재된 공개키와 비밀키를 생성하는 방법을 수행하는 상기 키 생성기;

상기 아핀 맵($\widetilde{T}$), 상기 맵($\mathcal{F}$), 및 메시지(m)를 이용하여 상기 메시지(m)의 전자 서명(σ)을 생성하는 서명 생성기; 및

상기 메시지(m), 상기 전자 서명(σ), 및 상기 공개키($\mathcal{P}=\mathcal{F}\circ T$)를 이용하여 상기 전자 서명(σ)을 검증하는 서명 검증기를 더 포함하고,

상기 서명 생성기는,

상기 메시지(m)에 대한 해시 메시지($H(m)=\xi$)를 계산하고,

$\xi=(\xi_1,\cdots,\xi_m)$ 가 주어질 때, $\mathcal{F}(\mathbf{x})=\xi$ 의 해($\mathbf{s}=(s_1,\cdots,s_n)$)를 $\mathcal{F}^{-1}(\xi)=\mathbf{s}$ 을 이용하여 계산하고,

$\widetilde{T}(\mathbf{s})=\sigma$ 를 계산하고,

상기 서명 검증기는 $P(\sigma)=H(m)$ 인지를 판단하고 판단 결과에 따라 상기 전자 서명(σ)을 검증하고,

$H:\{0,1\}^*\rightarrow\mathbb{F}_q^m$

$H(m)=\xi=(\xi_1,\cdots,\xi_m)\in\mathbb{F}_q^m$ 인 전자 서명기.

청구항 9

키 생성기를 이용한 공개키와 비밀키를 생성하는 방법에 있어서,

제1아핀 맵($\widetilde{S}$), 제2아핀 맵($\widetilde{T}$)과 맵($\mathcal{F}:\mathbb{F}_q^n\rightarrow\mathbb{F}_q^m$)을 획득하는 단계; 및

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

상기 맵($\mathcal{F}:\mathbb{F}_q^n\rightarrow\mathbb{F}_q^m$)은 $m=o_1+o_2$ 개의 방정식들과 $n=v+m$ 개의 변수들을 갖는 다변수

이차식들의 시스템 ($\mathcal{F} = \mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$)으로 표현될 때,

$i=1, \ldots, o_1$ 에 대해 $\mathcal{F}^{(i)}$ 는 아래와 같이 표현되고,

$$\begin{cases} \mathcal{F}^{(1)}(x_1, \cdots, x_{v+o_1}) = \mathcal{F}_V^{(1)}(x_1, \cdots, x_v) + \mathcal{F}_{OV}^{(1)}(x_1, \cdots, x_{v+o_1}) + \delta_1, \\ \vdots \\ \mathcal{F}^{(o_1)}(x_1, \cdots, x_{v+o_1}) = \mathcal{F}_V^{(o_1)}(x_1, \cdots, x_v) + \mathcal{F}_{OV}^{(o_1)}(x_1, \cdots, x_{v+o_1}) + \delta_{o_1} \end{cases}$$

유한체($\mathbb{F}_q$)에서 정의된 v 개의 일차식들($L_1, \ldots, L_v$)과 v 개의 변수들 ($x_1, \ldots, x_v$)가 주어졌을 때,

$i=1, \ldots, o_1$ 에 대해 $\mathcal{F}_V^{(i)}$ 는 아래와 같이 표현되고,

$$\begin{pmatrix} \mathcal{F}_V^{(1)} \\ \mathcal{F}_V^{(2)} \\ \vdots \\ \mathcal{F}_V^{(o_1)} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_v \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix} = M_V \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix}$$

여기서, M_V^1 는 구조화된 행렬 또는 구조화된 행렬의 부분 행렬이고,

$i = o_1 + 1, \ldots, m$ 에 대해 $\mathcal{F}^{(i)}$ 는 아래와 같이 표현되고,

$$\begin{cases} \mathcal{F}^{(o_1+1)}(x_1, \cdots, x_n) = \mathcal{F}_V^{(o_1+1)}(x_1, \cdots, x_{v+o_1}) + \mathcal{F}_{OV}^{(o_1+1)}(x_1, \cdots, x_n) + \delta_{o_1+1}, \\ \vdots \\ \mathcal{F}^{(m)}(x_1, \cdots, x_n) = \mathcal{F}_V^{(o_1+o_2)}(x_1, \cdots, x_{v+o_1}) + \mathcal{F}_{OV}^{(m)}(x_1, \cdots, x_n) + \delta_m, \end{cases}$$

$v+o_1$ 의 변수를 갖는 일차식들($L'_1, \cdots, L'_{v+o_1}$)과 $v+o_1$ 개의 변수들이 주어졌을 때,

$i = o_1 + 1, \ldots, m$ 에 대해 $\mathcal{F}_V^{(i)}$ 는 아래와 같이 표현되고,

$$\begin{pmatrix} \mathcal{F}_V^{(o_1+1)} \\ \mathcal{F}_V^{(o_1+2)} \\ \vdots \\ \mathcal{F}_V^{(o_1+o_2)} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_{v+o_1} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix} \cdot \begin{pmatrix} L'_1 \\ L'_2 \\ \cdots \\ L'_{v+o_1} \end{pmatrix} = M_V^2 \cdot \begin{pmatrix} L'_1 \\ L'_2 \\ \cdots \\ L'_{v+o_1} \end{pmatrix}$$

여기서, M_V^2 는 구조화된 행렬 또는 구조화된 행렬의 부분 행렬이고,

$m=o_1+o_2$ 이고,

$S : \mathbb{F}_q^m \to \mathbb{F}_q^m$ 이고, $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ 이고, $\widetilde{S} = S^{-1}$ 이고, $\widetilde{T} = T^{-1}$ 이고,

$V = \{1, \cdots, v\}$,

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

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

여기서, $|V| = v$ 이고, i = 1과 2에 대해 $|O_i| = o_i$ 이고, V 는 비니거 변수들을 정의하기 위한 인덱스 집합이고, O_1 과 O_2 는 오일 변수들을 정의하기 위한 인덱스 집합들인 공개키와 비밀키를 생성하는 방법.

청구항 10

제9항에 있어서,

상기 맵($\mathcal{F}: \mathbb{F}_q^n \to \mathbb{F}_q^m$)이 $m=o_1+o_2$ 개의 방정식들과 $n = v + m$ 개의 변수들을 갖는 다변수 이차식들의 시스템($\mathcal{F} = \mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$)으로 표현될 때,

$i=1, \ldots, o_1$ 에 대해 $\mathcal{F}_V^{(i)}$ 는 아래와 같이 표현되고,

$$\begin{pmatrix} \mathcal{F}_V^{(1)} \\ \mathcal{F}_V^{(2)} \\ \cdots \\ \mathcal{F}_V^{(o_1)} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_v \\ x_v & x_1 & \cdots & x_{v-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{v-o_1+2} & x_{v-o_1+3} & \cdots & x_{v-o_1+1} \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix} = M_V^1 \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix}$$

여기서, M_V^1 는 순환 행렬 또는 순환 행렬의 부분 행렬이고,

$i = o_1 + 1, \ldots, m$ 에 대해 $\mathcal{F}^{(i)}$ 는 아래와 같이 표현되고,

$$\begin{cases} \mathcal{F}^{(o_1+1)}(x_1, \cdots, x_n) = \mathcal{F}_V^{(o_1+1)}(x_1, \cdots, x_{v+o_1}) + \mathcal{F}_{OV}^{(o_1+1)}(x_1, \cdots, x_n) + \delta_{o_1+1}, \\ \quad \vdots \\ \mathcal{F}^{(m)}(x_1, \cdots, x_n) = \mathcal{F}_V^{(o_1+o_2)}(x_1, \cdots, x_{v+o_1}) + \mathcal{F}_{OV}^{(m)}(x_1, \cdots, x_n) + \delta_m. \end{cases}$$

$i = o_1 + 1, \ldots, m$ 에 대해 $\mathcal{F}_V^{(i)}$ 는 아래와 같이 표현되고,

$$\begin{pmatrix} \mathcal{F}_V^{(o_1+1)} \\ \mathcal{F}_V^{(o_1+2)} \\ \cdots \\ \mathcal{F}_V^{(o_1+o_2)} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_{v+o_1} \\ x_v & x_1 & \cdots & x_{v+o_1-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{v+o_1-o_2+2} & x_{v+o_1-o_2+3} & \cdots & x_{v+o_1-o_2+1} \end{pmatrix} \cdot \begin{pmatrix} L'_1 \\ L'_2 \\ \cdots \\ L'_{v+o_1} \end{pmatrix} = M_V^2 \cdot \begin{pmatrix} L'_1 \\ L'_2 \\ \cdots \\ L'_{v+o_1} \end{pmatrix}$$

여기서, M_V^2 는 순환 행렬 또는 순환 행렬의 부분 행렬인 공개키와 비밀키를 생성하는 방법.

청구항 11

제9항에 기재된 공개키와 비밀키를 생성하는 방법을 수행하기 위해 저장 매체에 저장된 컴퓨터 프로그램.

청구항 12

제9항에 기재된 공개키와 비밀키를 생성하는 방법을 수행하는 상기 키 생성기;

상기 제1아핀 맵($\widetilde{S}$), 상기 제2아핀 맵($\widetilde{T}$), 상기 맵($\mathcal{F}$), 및 메시지(m)를 이용하여 상기 메시지(m)의 전자

서명(σ)을 생성하는 서명 생성기; 및

상기 메시지(m), 상기 전자 서명(σ), 및 상기 공개키($\mathcal{P} = S \circ \mathcal{F} \circ T$)를 이용하여 상기 전자 서명($\sigma$)을 검증하는 서명 검증기를 포함하고,

상기 서명 생성기는,

상기 메시지(m)에 대해 해시 메시지(H(m))를 계산하고,

$\widetilde{S}(H(\mathtt{m})) = \xi = (\xi_1, \cdots, \xi_m) \in \mathbb{F}_q^m$ 을 계산하고,

$\xi = (\xi_1, \cdots, \xi_m)$ 가 주어질 때, , $\mathcal{F}(\mathbf{x}) = \xi$ 의 해 ($\mathbf{s} = (s_1, \cdots, s_n)$)를 $\mathcal{F}^{-1}(\xi) = \mathbf{s}$ 을 이용하여 계산하고,

$\widetilde{T}(\mathbf{s}) = \sigma$ 를 계산하고,

상기 서명 검증기는,

$P(\sigma)=H(m)$ 인지를 판단하고 판단 결과에 따라 상기 전자 서명(σ)을 검증하고,

$H : \{0,1\}^* \rightarrow \mathbb{F}_q^m$ 인 전자 서명기.

청구항 13

제12항에 있어서, 상기 서명 생성기는,

$\mathbb{F}_q^m$ 의 벡터($\mathbf{h}$)와 상기 제1아핀 맵($\widetilde{S}$)의 곱($\widetilde{S} \cdot \mathbf{h}$)에서 상기 제1아핀 맵($\widetilde{S}$)의 랜덤화를 위해 주어진 행렬($R$)이 순환 행렬일 때,

$\widetilde{S}(H(\mathtt{m}))$ 을 아래의 수학식으로,

$\widetilde{S}(H(m)) = (\widetilde{S} + R)(H(m)) - R(H(m))$ 계산하는 전자 서명기.

청구항 14

제12항에 있어서, 상기 서명 생성기는,

$\mathbb{F}_q^m$ 의 벡터($\mathbf{h}$)와 상기 제1아핀 맵($\widetilde{S}$)의 곱($\widetilde{S} \cdot \mathbf{h}$)에서 상기 제1아핀 맵($\widetilde{S}$)의 랜덤화를 위해 주어진 행렬($R$)이 순환 행렬일 때,

$\widetilde{S}(H(\mathtt{m}))$ 을 아래의 수학식으로,

$\widetilde{S}(H(m)) = (\widetilde{S} \cdot R^{-1} \cdot R)(H(m))$ 계산하는 전자 서명기.

청구항 15

키 생성기를 이용한 공개키와 비밀키를 생성하는 방법에 있어서,

제1아핀 맵($\widetilde{S}$), 제2아핀 맵($\widetilde{T}$)과 맵 ($\mathcal{F} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$)을 획득하는 단계; 및

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

상기 맵($\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$)은 $m = o_1 + o_2$ 개의 다변수 이차식들의 시스템 ($\mathcal{F} = \mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$)으로 표현되고,

유한체($\mathbb{F}_q$)에서 정의된 v 개의 변수들($x_1, \ldots, x_v$)과 o_1개의 변수들($x_{v+1}, x_{v+2}, \ldots, x_{v+o_1}$)이 주어졌을 때, 상기 o_1 개의 다변수 이차식들의 시스템 ($\mathcal{F}_{OV}^{(1)}, \ldots, \mathcal{F}_{OV}^{(o_1)}$)은 아래와 같이 표현되고,

$$\begin{pmatrix} \mathcal{F}_{OV}^{(1)} \\ \mathcal{F}_{OV}^{(2)} \\ \vdots \\ \mathcal{F}_{OV}^{(o_1)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}^T\mathbf{a}_{11} & \mathbf{v}^T\mathbf{a}_{12} & \cdots & \mathbf{v}^T\mathbf{a}_{1o_1} \\ \mathbf{v}^T\mathbf{a}_{21} & \mathbf{v}^T\mathbf{a}_{22} & \cdots & \mathbf{v}^T\mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}^T\mathbf{a}_{o_1 1} & \mathbf{v}^T\mathbf{a}_{o_1 2} & \cdots & \mathbf{v}^T\mathbf{a}_{o_1 o_1} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix} + B_1 \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{v}^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}^T \end{pmatrix} \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o_1} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o_1 1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{o_1 o_1} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix} + B_1 \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix}$$

여기서,

$$M_{OV,1} = \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o_1} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o_1 1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{o_1 o_1} \end{pmatrix}$$ 와 $$B_1 = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1o_1} \\ b_{21} & b_{22} & \cdots & b_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{o_1 1} & b_{o_1 2} & \cdots & b_{o_1 o_1} \end{pmatrix}$$ 로 주어지고,

$\mathbf{v}^T = [x_1 \quad x_2 \quad \cdots \quad x_v]$ 이고,

각 열 벡터(a_{ij})를 하나의 행렬의 원소로 간주했을 때, $M_{OV,1}$가 구조화된 행렬이 되도록 각 열 벡터(a_{ij})가 선택되고, B_1도 $M_{OV,1}$와 동일한 형태의 구조화된 행렬이 되도록 원소 값들(b_{ij})이 선택되고,

$i = o_1 + 1, \ldots, m$ 에 대해 $\mathcal{F}_{OV}^{(i)}$는 아래와 같이 주어지고,

$$\begin{pmatrix} \mathcal{F}_{OV}^{(o_1+1)} \\ \mathcal{F}_{OV}^{(o_1+2)} \\ \vdots \\ \mathcal{F}_{OV}^{(o_1+o_2)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}'^T\mathbf{a}'_{11} & \mathbf{v}'^T\mathbf{a}'_{12} & \cdots & \mathbf{v}'^T\mathbf{a}'_{1o_2} \\ \mathbf{v}'^T\mathbf{a}'_{21} & \mathbf{v}'^T\mathbf{a}'_{22} & \cdots & \mathbf{v}'^T\mathbf{a}'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}'^T\mathbf{a}'_{o_2 1} & \mathbf{v}'^T\mathbf{a}'_{o_2 2} & \cdots & \mathbf{v}'^T\mathbf{a}'_{o_2 o_2} \end{pmatrix} \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix} + B_2 \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{v}'^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}'^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}'^T \end{pmatrix} \begin{pmatrix} \mathbf{a}'_{11} & \mathbf{a}'_{12} & \cdots & \mathbf{a}'_{1o_2} \\ \mathbf{a}'_{21} & \mathbf{a}'_{22} & \cdots & \mathbf{a}'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}'_{o_2 1} & \mathbf{a}'_{11} & \cdots & \mathbf{a}'_{o_2 o_2} \end{pmatrix} \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix} + B_2 \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix}$$

여기서,

$M_{OV,2} = \begin{pmatrix} \mathbf{a}'_{11} & \mathbf{a}'_{12} & \cdots & \mathbf{a}'_{1o_2} \\ \mathbf{a}'_{21} & \mathbf{a}'_{22} & \cdots & \mathbf{a}'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}'_{o_21} & \mathbf{a}'_{11} & \cdots & \mathbf{a}'_{o_2o_2} \end{pmatrix}$ 와 $B_2 = \begin{pmatrix} b'_{11} & b'_{12} & \cdots & b'_{1o_2} \\ b'_{21} & b'_{22} & \cdots & b'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ b'_{o_21} & b'_{o_22} & \cdots & b'_{o_2o_2} \end{pmatrix}$ 로 주어지고,

$\mathbf{v}'^T = [x_1 \; x_2 \; \cdots \; x_{v+o_1}]$ 이고,

각 열 벡터(a'_{ij})를 하나의 행렬의 원소로 간주했을 때, $M_{OV,2}$ 가 구조화된 행렬이 되도록 각 열 벡터(a'_{ij})가 선택되고, B_2 도 $M_{OV,2}$ 와 동일한 형태의 구조화된 행렬이 되도록 원소 값들(b'_{ij})이 선택되고,

$S : \mathbb{F}_q^m \to \mathbb{F}_q^m$ 이고, $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ 이고, $\widetilde{S} = S^{-1}$ 이고, $\widetilde{T} = T^{-1}$ 인 공개키와 비밀키를 생성하는 방법.

청구항 16

제15항에 있어서,

$o_1 = 2k_1$ 로 $o_2 = 2k_2$ 로 주어질 때,

$i = 1, \ldots, o_1$ 에 대해 $F_{OV}^{(i)}$ 는 아래와 같이 표현되고,

$$\begin{pmatrix} \mathcal{F}_{OV}^{(1)} \\ \mathcal{F}_{OV}^{(2)} \\ \vdots \\ \mathcal{F}_{OV}^{(o_1)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}^T\mathbf{a}_{11} & \mathbf{v}^T\mathbf{a}_{12} & \cdots & \mathbf{v}^T\mathbf{a}_{1o_1} \\ \mathbf{v}^T\mathbf{a}_{21} & \mathbf{v}^T\mathbf{a}_{22} & \cdots & \mathbf{v}^T\mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}^T\mathbf{a}_{o_11} & \mathbf{v}^T\mathbf{a}_{o_12} & \cdots & \mathbf{v}^T\mathbf{a}_{o_1o_1} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix} + B_1 \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{v}^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}^T \end{pmatrix} \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o_1} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o_11} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{o_1o_1} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix} + B_1 \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix}$$

여기서,

$$M_{OV,1} = \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o_1} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o_11} & \mathbf{a}_{o_12} & \cdots & \mathbf{a}_{o_1o_1} \end{pmatrix} = \begin{pmatrix} \mathbf{p}_1 & \mathbf{p}_2 & \cdots & \mathbf{p}_{k_1} & \mathbf{q}_1 & \mathbf{q}_2 & \cdots & \mathbf{q}_{k_1} \\ \mathbf{p}_{k_1} & \mathbf{p}_1 & \cdots & \mathbf{p}_{k_1-1} & \mathbf{q}_{k_1} & \mathbf{q}_1 & \cdots & \mathbf{q}_{k_1-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{p}_2 & \mathbf{p}_3 & \cdots & \mathbf{p}_1 & \mathbf{q}_2 & \mathbf{q}_3 & \cdots & \mathbf{q}_1 \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_{k_1} & \mathbf{s}_1 & \mathbf{s}_2 & \cdots & \mathbf{s}_{k_1} \\ \mathbf{r}_{k_1} & \mathbf{r}_1 & \cdots & \mathbf{r}_{k_1-1} & \mathbf{s}_{k_1} & \mathbf{s}_1 & \cdots & \mathbf{s}_{k_1-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{r}_2 & \mathbf{r}_3 & \cdots & \mathbf{r}_1 & \mathbf{s}_2 & \mathbf{s}_3 & \cdots & \mathbf{s}_1 \end{pmatrix} = \begin{pmatrix} P_1 & Q_1 \\ R_1 & S_1 \end{pmatrix}$$

이고,

$\mathbf{p}_i, \mathbf{q}_i, \mathbf{r}_i$ 와 $\mathbf{s}_i$ 각각은 크기(v)를 가지는 열 벡터이고,

P_1, Q_1, R_1, S_1 각각은 벡터들의 순환 행렬이고,

$M_{OV,1}$는 벡터들의 블록 순환 행렬이고,

$$B_1 = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1o_1} \\ b_{21} & b_{22} & \cdots & b_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{o_11} & b_{o_12} & \cdots & b_{o_1o_1} \end{pmatrix} = \begin{pmatrix} t_1 & t_2 & \cdots & t_{k_1} & u_1 & u_2 & \cdots & u_{k_1} \\ t_k & t_1 & \cdots & t_{k_1-1} & u_k & u_1 & \cdots & u_{k_1-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t_2 & t_3 & \cdots & t_1 & u_2 & u_3 & \cdots & u_1 \\ v_1 & v_2 & \cdots & v_{k_1} & w_1 & w_2 & \cdots & w_{k_1} \\ v_k & v_1 & \cdots & v_{k_1-1} & w_k & w_1 & \cdots & w_{k_1-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ v_2 & v_3 & \cdots & v_1 & w_2 & w_3 & \cdots & w_1 \end{pmatrix}$$

B_1은 블록 순환 행렬이고,

$i = o_1 + 1, \ldots, m$에 대해 $\mathcal{F}_{OV}^{(i)}$은 아래와 같이 표현되고,

$$\begin{pmatrix} \mathcal{F}_{OV}^{(o_1+1)} \\ \mathcal{F}_{OV}^{(o_1+2)} \\ \vdots \\ \mathcal{F}_{OV}^{(o_1+o_2)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}'^T\mathbf{a}'_{11} & \mathbf{v}'^T\mathbf{a}'_{12} & \cdots & \mathbf{v}'^T\mathbf{a}'_{1o_2} \\ \mathbf{v}'^T\mathbf{a}'_{21} & \mathbf{v}'^T\mathbf{a}'_{22} & \cdots & \mathbf{v}'^T\mathbf{a}'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}'^T\mathbf{a}'_{o_21} & \mathbf{v}'^T\mathbf{a}'_{o_22} & \cdots & \mathbf{v}'^T\mathbf{a}'_{o_2o_2} \end{pmatrix} \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix} + B_2 \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{v}'^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}'^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}'^T \end{pmatrix} \begin{pmatrix} \mathbf{a}'_{11} & \mathbf{a}'_{12} & \cdots & \mathbf{a}'_{1o_2} \\ \mathbf{a}'_{21} & \mathbf{a}'_{22} & \cdots & \mathbf{a}'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}'_{o_21} & \mathbf{a}'_{11} & \cdots & \mathbf{a}'_{o_2o_2} \end{pmatrix} \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix} + B_2 \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix}$$

여기서,

$$M_{OV,2} = \begin{pmatrix} \mathbf{a}'_{11} & \mathbf{a}'_{12} & \cdots & \mathbf{a}'_{1o_2} \\ \mathbf{a}'_{21} & \mathbf{a}'_{22} & \cdots & \mathbf{a}'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}'_{o_21} & \mathbf{a}'_{o_22} & \cdots & \mathbf{a}'_{o_2o_2} \end{pmatrix} = \begin{pmatrix} \mathbf{p}'_1 & \mathbf{p}'_2 & \cdots & \mathbf{p}'_{k_2} & \mathbf{q}'_1 & \mathbf{q}'_2 & \cdots & \mathbf{q}'_{k_2} \\ \mathbf{p}'_{k_2} & \mathbf{p}'_1 & \cdots & \mathbf{p}'_{k_2-1} & \mathbf{q}'_{k_2} & \mathbf{q}'_1 & \cdots & \mathbf{q}'_{k_2-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{p}'_2 & \mathbf{p}'_3 & \cdots & \mathbf{p}'_1 & \mathbf{q}'_2 & \mathbf{q}'_3 & \cdots & \mathbf{q}'_1 \\ \mathbf{r}'_1 & \mathbf{r}'_2 & \cdots & \mathbf{r}'_{k_2} & \mathbf{s}'_1 & \mathbf{s}'_2 & \cdots & \mathbf{s}'_{k_2} \\ \mathbf{r}'_{k_2} & \mathbf{r}'_1 & \cdots & \mathbf{r}'_{k_2-1} & \mathbf{s}'_{k_2} & \mathbf{s}'_1 & \cdots & \mathbf{s}'_{k_2-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{r}'_2 & \mathbf{r}'_3 & \cdots & \mathbf{r}'_1 & \mathbf{s}'_2 & \mathbf{s}'_3 & \cdots & \mathbf{s}'_1 \end{pmatrix} = \begin{pmatrix} P_2 & Q_2 \\ R_2 & S_2 \end{pmatrix}$$

$\mathbf{p}'_i$, $\mathbf{q}'_i$, $\mathbf{r}'_i$, 와 $\mathbf{s}'_i$ 각각은 크기($v + o_1$)를 가지는 열 벡터이고,

P_2, Q_2, R_2, S_2 각각은 벡터들의 순환 행렬이고,

$M_{OV,2}$는 벡터들의 블록 순환 행렬이고,

$$B_2 = \begin{pmatrix} b'_{11} & b'_{12} & \cdots & b'_{1o_2} \\ b'_{21} & b'_{22} & \cdots & b'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ b'_{o_21} & b'_{o_22} & \cdots & b'_{o_2o_2} \end{pmatrix} = \begin{pmatrix} t'_1 & t'_2 & \cdots & t'_{k_2} & u'_1 & u'_2 & \cdots & u'_{k_2} \\ t'_k & t'_1 & \cdots & t'_{k_2-1} & u'_k & u'_1 & \cdots & u'_{k_2-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t'_2 & t'_3 & \cdots & t'_1 & u'_2 & u'_3 & \cdots & u'_1 \\ v'_1 & v'_2 & \cdots & v'_{k_2} & w'_1 & w'_2 & \cdots & w'_{k_2} \\ v'_k & v'_1 & \cdots & v'_{k_2-1} & w'_k & w'_1 & \cdots & w'_{k_2-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ v'_2 & v'_3 & \cdots & v'_1 & w'_2 & w'_3 & \cdots & w'_1 \end{pmatrix}$$

B_2은 블록 순환 행렬이고, $m = o_1 + o_2$인 공개키와 비밀키를 생성하는 방법.

청구항 17

제16항에 있어서,

상기 유한체에서 정의된 v 개의 일차식들($L_1, \ldots, L_v$)과 v 개의 변수들 ($x_1, \ldots, x_v$)가 주어졌을 때

$i=1, \cdots, o_1$에 대해 $\mathcal{F}_V^{(i)}$는 아래와 같이 표현되고,

$$\begin{pmatrix} \mathcal{F}_V^{(1)} \\ \mathcal{F}_V^{(2)} \\ \cdots \\ \mathcal{F}_V^{(o_1)} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_v \\ x_v & x_1 & \cdots & x_{v-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{v-o_1+2} & x_{v-o_1+3} & \cdots & x_{v-o_1+1} \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix} = M_V^1 \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix}$$

여기서, M_V^1는 순환 행렬 또는 순환 행렬의 부분 행렬이고,

$v+o_1$의 변수를 갖는 일차식들 ($L_1', \cdots, L_{v+o_1}'$)과 $v+o_1$개의 변수들이 주어졌을 때, $i = o_1 + 1, \ldots, m$에 대해 $\mathcal{F}_V^{(i)}$는 아래와 같이 표현되고,

$$\begin{pmatrix} \mathcal{F}_V^{(o_1+1)} \\ \mathcal{F}_V^{(o_1+2)} \\ \cdots \\ \mathcal{F}_V^{(o_1+o_2)} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_{v+o_1} \\ x_v & x_1 & \cdots & x_{v+o_1-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{v+o_1-o_2+2} & x_{v+o_1-o_2+3} & \cdots & x_{v+o_1-o_2+1} \end{pmatrix} \cdot \begin{pmatrix} L_1' \\ L_2' \\ \cdots \\ L_{v+o_1}' \end{pmatrix} = M_V^2 \cdot \begin{pmatrix} L_1' \\ L_2' \\ \cdots \\ L_{v+o_1}' \end{pmatrix}$$

여기서, M_V^2는 순환 행렬 또는 순환 행렬의 부분 행렬이고,

$i=1, \ldots, m$에 대해 $\mathcal{F}^{(i)}$는 아래와 같이,

$$\begin{cases} \mathcal{F}^{(1)}(x_1, \cdots, x_{v+o_1}) = \mathcal{F}_V^{(1)}(x_1, \cdots, x_v) + \mathcal{F}_{OV}^{(1)}(x_1, \cdots, x_{v+o_1}) + \delta_1, \\ \vdots \\ \mathcal{F}^{(o_1)}(x_1, \cdots, x_{v+o_1}) = \mathcal{F}_V^{(o_1)}(x_1, \cdots, x_v) + \mathcal{F}_{OV}^{(o_1)}(x_1, \cdots, x_{v+o_1}) + \delta_{o_1}, \end{cases}$$

$$\begin{cases} \mathcal{F}^{(o_1+1)}(x_1, \cdots, x_n) = \mathcal{F}_V^{(o_1+1)}(x_1, \cdots, x_{v+o_1}) + \mathcal{F}_{OV}^{(o_1+1)}(x_1, \cdots, x_n) + \delta_{o_1+1}, \\ \vdots \\ \mathcal{F}^{(o_1+o_2)}(x_1, \cdots, x_n) = \mathcal{F}_V^{(o_1+o_2)}(x_1, \cdots, x_{v+o_1}) + \mathcal{F}_{OV}^{(o_1+o_2)}(x_1, \cdots, x_n) + \delta_m, \end{cases}$$

표현되고, $m = o_1 + o_2$인 공개키와 비밀키를 생성하는 방법.

청구항 18

제15항에 기재된 공개키와 비밀키를 생성하는 방법을 수행하기 위해 저장 매체에 저장된 컴퓨터 프로그램.

청구항 19

제15항에 기재된 공개키와 비밀키를 생성하는 방법을 수행하는 상기 키 생성기;

상기 제1아핀 맵($\widetilde{S}$), 상기 제2아핀 맵($\widetilde{T}$), 상기 맵($\mathcal{F}$), 및 메시지(m)를 이용하여 상기 메시지(m)의 전자 서명(σ)을 생성하는 서명 생성기; 및

상기 메시지(m), 상기 전자 서명(σ), 및 상기 공개키($\mathcal{P} = S \circ \mathcal{F} \circ T$)를 이용하여 상기 전자 서명($\sigma$)을 검증하는 서명 검증기를 포함하고,

상기 서명 생성기는,

상기 메시지(m)에 대해 해시 메시지(H(m))를 계산하고,

$\widetilde{S}(H(\mathrm{m})) = \xi_=(\xi_1, \cdots, \xi_m) \in \mathbb{F}_q^m$ 을 계산하고,

$\xi = (\xi_1, \cdots, \xi_m)$ 가 주어질 때, , $\mathcal{F}(\mathbf{x}) = \xi$ 의 해 ($\mathbf{s} = (s_1, \cdots, s_n)$)를 $\mathcal{F}^{-1}(\xi) = \mathbf{s}$ 을 이용하여 계산하고,

$\widetilde{T}(\mathbf{s}) = \sigma$ 를 계산하고,

상기 서명 검증기는,

$P(\sigma)=H(m)$ 인지를 판단하고 판단 결과에 따라 상기 전자 서명(σ)을 검증하고,

$H : \{0,1\}^* \rightarrow \mathbb{F}_q^m$ 인 전자 서명기.

청구항 20

제19항에 있어서, 상기 서명 생성기는,

$\mathbb{F}_q^m$ 의 벡터($\mathbf{h}$)와 상기 제1아핀 맵($\widetilde{S}$)과의 곱($\widetilde{S} \cdot \mathbf{h}$)에서 상기 제1아핀 맵($\widetilde{S}$)의 랜덤화를 위해 주어진 행렬(R)이 순환 행렬일 때,

$\widetilde{S}(H(\mathbf{m}))$ 을 아래의 수학식으로,

$\widetilde{S}(H(m)) = (\widetilde{S} + R)(H(m)) - R(H(m))$ 계산하는 전자 서명기.

청구항 21

제19항에 있어서, 상기 서명 생성기는,

$\mathbb{F}_q^m$ 의 벡터($\mathbf{h}$)와 상기 제1아핀 맵($\widetilde{S}$)과의 곱($\widetilde{S} \cdot \mathbf{h}$)에서 상기 제1아핀 맵($\widetilde{S}$)의 랜덤화를 위해 주어진 행렬(R)이 순환 행렬일 때,

$\widetilde{S}(H(\mathbf{m}))$ 을 아래의 수학식으로,

$\widetilde{S}(H(m)) = (\widetilde{S} \cdot R^{-1} \cdot R)(H(m))$ 계산하는 전자 서명기.

발명의 설명

기 술 분 야

[0001] 본 발명은 공개키 암호에 관한 것으로, 특히 구조화된 행렬들에 기초한 다변수 이차식 기반 디지털 서명 알고리즘을 수행할 수 있는 방법과 장치에 관한 것이다.

배 경 기 술

[0002] 다변수 이차식 기반 디지털 서명(digital signature based on multivariate quadratic equations)은 다변수 암호(multivariate cryptography) 시스템에서 사용되는 디지털 서명(또는 '전자 서명'이라고도 함.)을 의미한다. 여기서, 다변수 암호 시스템은 유한체(finite field) 위에서 정의된 다변수 다항식들(multivariate polynomials)을 기반으로 하는 비대칭 암호 기본 요소들(asymmetric cryptographic primitives)을 갖는 시스템을 의미한다.

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

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 미국등록특허공보: US 9,191,199 B2 (2015.11.17)

(특허문헌 0002) 미국공개특허공보: US 2004/0258240 A1 (2004.12.23)

(특허문헌 0003) 미국공개특허공보: US 2007/0033417 A1 (2007.02.08)

발명의 내용

해결하려는 과제

[0005] 본 발명이 이루고자 하는 기술적인 과제는 구조화된 행렬들을 사용함으로써 비밀키의 길이를 크게 줄일 수 있으며, 계산의 효율성을 증대시켜 빠르게 서명 생성을 수행할 수 있는 다변수 이차식 기반 전자 서명 알고리즘을 수행할 수 있는 방법, 장치, 및 컴퓨터 프로그램을 제공하는 것이다.

과제의 해결 수단

[0006] 본 발명의 실시 예들에 따라, 키 생성기를 이용하여 공개키와 비밀키를 생성하는 방법은 아핀 맵($\widetilde{T}$)과 맵($\mathcal{F}:\mathbb{F}_q^n \to \mathbb{F}_q^m$)을 획득하는 단계와 상기 아핀 맵과 상기 맵을 이용하여 공개키($\mathcal{P}=\mathcal{F}\circ T$)와 비밀키 $(\mathcal{F},\tilde{T})$ 를 생성하는 단계를 포함하고, 상기 맵($\mathcal{F}:\mathbb{F}_q^n \to \mathbb{F}_q^m$)은 o 개의 다변수 이차식들의 시스템 $(\mathcal{F}_V^{(1)},\cdots,\mathcal{F}_V^{(o)})$ 으로 표현되고, 유한체($\mathbb{F}_q$)에서 정의된 v 개의 일차식들($L_1,\ldots,L_v$)과 v 개의 변수들 ($x_1,\ldots,x_v$)이 주어졌을 때, 상기 o 개의 다변수 이차식들의 시스템 ($\mathcal{F}_V^{(1)},\cdots,\mathcal{F}_V^{(o)}$)은 아래와 같이 표현되고,

[0007] $$\begin{pmatrix}\mathcal{F}_V^{(1)}\\ \mathcal{F}_V^{(2)}\\ \cdots\\ \mathcal{F}_V^{(o)}\end{pmatrix}=\begin{pmatrix}x_1\ x_2\cdots x_v\\ \cdots\cdots\cdots\\ \cdots\cdots\cdots\\ \cdots\cdots\cdots\end{pmatrix}\cdot\begin{pmatrix}L_1\\ L_2\\ \cdots\\ L_v\end{pmatrix}=M_V\cdot\begin{pmatrix}L_1\\ L_2\\ \cdots\\ L_v\end{pmatrix}$$

[0008] 여기서, $T:\mathbb{F}_q^n \to \mathbb{F}_q^n$ 이고, $\widetilde{T}=T^{-1}$ 이고, M_V 는 구조화된 행렬 또는 구조화된 행렬의 부분 행렬이고, $m=o$ 이고, $V=\{1,\cdots,v\}$, $O=\{v+1,\cdots,v+o\}$, $|V|=v$ 이고, $|O|=o$ 이고, V 는 비니거(Vinegar) 변수들을 정의하기 위한 인덱스 집합이고, O 는 오일(Oil) 변수들을 정의하기 위한 인덱스 집합이다.

[0009] 저장 매체에 저장된 컴퓨터 프로그램은 상기 키 생성기를 이용하여 공개키와 비밀키를 생성하는 방법을 저장한다.

[0010] 본 발명의 실시 예들에 따른 전자 서명기는 상기 공개키와 비밀키를 생성하는 방법을 수행하는 상기 키 생성기와, 상기 아핀 맵($\widetilde{T}$), 상기 맵($\mathcal{F}$), 및 메시지(m)를 이용하여 상기 메시지(m)의 전자 서명(σ)을 생성하는 서명 생성기와, 상기 메시지(m), 상기 전자 서명(σ), 및 상기 공개키($\mathcal{P}=\mathcal{F}\circ T$)를 이용하여 상기 전자

서명(σ)을 검증하는 서명 검증기를 포함하고, 상기 서명 생성기는 상기 메시지(m)에 대한 해시 메시지($H(m)=\xi$)를 계산하고, $\xi=(\xi_1,\cdots,\xi_m)$가 주어질 때, $\mathcal{F}(\mathbf{x})=\xi$의 해($\mathbf{s}=(s_1,\cdots,s_n)$)를 $\mathcal{F}^{-1}(\xi)=\mathbf{s}$을 이용하여 계산하고, $\widetilde{T}(\mathbf{s})=\sigma$를 계산하고, 상기 서명 검증기는 $P(\sigma)=H(m)$인지를 판단하고 판단 결과에 따라 상기 전자 서명(σ)을 검증하고, $H:\{0,1\}^*\rightarrow\mathbb{F}_q^m$이고, $H(m)=\xi=(\xi_1,\cdots,\xi_m)\in\mathbb{F}_q^m$이다.

[0011] 본 발명의 실시 예들에 따라, 키 생성기를 이용하여 공개키와 비밀키를 생성하는 방법은 아핀 맵($\widetilde{T}$)과 맵($\mathcal{F}:\mathbb{F}_q^n\rightarrow\mathbb{F}_q^m$)을 획득하는 단계와, 상기 아핀 맵과 상기 맵을 이용하여 공개키($\mathcal{P}=\mathcal{F}\circ T$)와 비밀키($(\mathcal{F},\widetilde{T})$)를 생성하는 단계를 포함하고, 상기 맵($\mathcal{F}:\mathbb{F}_q^n\rightarrow\mathbb{F}_q^m$)은 o개의 다변수 이차식들의 시스템($\mathcal{F}_{OV}^{(1)},\cdots,\mathcal{F}_{OV}^{(o)}$)으로 표현되고, 유한체($\mathbb{F}_q$)에서 정의된 v개의 변수들($x_1,\ldots,x_v$)과 o개의 변수들 ($x_{v+1},x_{v+2},\cdots,x_{v+o}$)이 주어졌을 때, 상기 o개의 다변수 이차식들의 시스템($\mathcal{F}_{OV}^{(1)},\cdots,\mathcal{F}_{OV}^{(o)}$)은 아래와 같이 표현되고,

[0012]
$$\begin{pmatrix}\mathcal{F}_{OV}^{(1)}\\ \mathcal{F}_{OV}^{(2)}\\ \vdots\\ \mathcal{F}_{OV}^{(o)}\end{pmatrix}=\begin{pmatrix}\mathbf{v}^T\mathbf{a}_{11} & \mathbf{v}^T\mathbf{a}_{12} & \cdots & \mathbf{v}^T\mathbf{a}_{1o}\\ \mathbf{v}^T\mathbf{a}_{21} & \mathbf{v}^T\mathbf{a}_{22} & \cdots & \mathbf{v}^T\mathbf{a}_{2o}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{v}^T\mathbf{a}_{o1} & \mathbf{v}^T\mathbf{a}_{o2} & \cdots & \mathbf{v}^T\mathbf{a}_{oo}\end{pmatrix}\begin{pmatrix}x_{v+1}\\ x_{v+2}\\ \vdots\\ x_{v+o}\end{pmatrix}+B\begin{pmatrix}x_{v+1}\\ x_{v+2}\\ \vdots\\ x_{v+o}\end{pmatrix}$$

[0013]
$$=\begin{pmatrix}\mathbf{v}^T & 0 & \cdots & 0\\ 0 & \mathbf{v}^T & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \mathbf{v}^T\end{pmatrix}\begin{pmatrix}\mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o}\\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{a}_{o1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{oo}\end{pmatrix}\begin{pmatrix}x_{v+1}\\ x_{v+2}\\ \vdots\\ x_{v+o}\end{pmatrix}+B\begin{pmatrix}x_{v+1}\\ x_{v+2}\\ \vdots\\ x_{v+o}\end{pmatrix}$$

여기서,

[0014]
$$B=\begin{pmatrix}b_{11} & b_{12} & \cdots & b_{1o}\\ b_{21} & b_{22} & \cdots & b_{2o}\\ \vdots & \vdots & \ddots & \vdots\\ b_{o1} & b_{o2} & \cdots & b_{oo}\end{pmatrix},\quad M_{OV}=\begin{pmatrix}\mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o}\\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{a}_{o1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{oo}\end{pmatrix}$$ 이고,

[0015] $\mathbf{v}^T=[x_1\quad x_2\quad\cdots\quad x_v]$이고, $T:\mathbb{F}_q^n\rightarrow\mathbb{F}_q^n$이고, $\widetilde{T}=T^{-1}$이고,

[0016] 각 열 벡터(a_{ij})를 하나의 행렬의 원소로 간주했을 때, M_{OV}가 구조화된 행렬이 되도록 각 열 벡터(a_{ij})가 선택되고, B도 M_{OV}와 동일한 형태의 구조화된 행렬이 되도록 원소 값들(b_{ij})이 선택된다.

[0017] 저장 매체에 저장된 컴퓨터 프로그램은 상기 키 생성기를 이용하여 공개키와 비밀키를 생성하는 방법을 저장한다.

[0018] 본 발명의 실시 예들에 따른 전자 서명기는 상기 공개키와 비밀키를 생성하는 방법을 수행하는 상기 키 생성기와, 상기 아핀 맵($\widetilde{T}$), 상기 맵($\mathcal{F}$), 및 메시지(m)를 이용하여 상기 메시지(m)의 전자 서명(σ)을 생성하는

서명 생성기와, 상기 메시지(m), 상기 전자 서명(σ), 및 상기 공개키($\mathcal{P}=\mathcal{F}\circ T$)를 이용하여 상기 전자 서명($\sigma$)을 검증하는 서명 검증기를 포함하고, 상기 서명 생성기는 상기 메시지(m)에 대한 해시 메시지($H(m)=\xi$)를 계산하고, $\xi=(\xi_1,\cdots,\xi_m)$가 주어질 때, $\mathcal{F}(\mathbf{x})=\xi$의 해($\mathbf{s}=(s_1,\cdots,s_n)$)를 $\mathcal{F}^{-1}(\xi)=\mathbf{s}$을 이용하여 계산하고, $\widetilde{T}(\mathbf{s})=\sigma$를 계산하고, 상기 서명 검증기는 $P(\sigma)=H(m)$ 인지를 판단하고 판단 결과에 따라 상기 전자 서명(σ)을 검증하고, $H:\{0,1\}^*\rightarrow\mathbb{F}_q^m$ 이고, $H(m)=\xi=(\xi_1,\cdots,\xi_m)\in\mathbb{F}_q^m$ 이다.

[0019] 본 발명의 실시 예들에 따라, 키 생성기를 이용한 공개키와 비밀키를 생성하는 방법은 제1아핀 맵($\widetilde{S}$), 제2아핀 맵($\widetilde{T}$)과 맵($\mathcal{F}:\mathbb{F}_q^n\rightarrow\mathbb{F}_q^m$)을 획득하는 단계와, 상기 제1아핀 맵, 상기 제2아핀 맵, 및 상기 맵을 이용하여 공개키 ($\mathcal{P}=S\circ\mathcal{F}\circ T$)와 비밀키($(\widetilde{S},\mathcal{F},\widetilde{T})$)를 생성하는 단계를 포함하고, 상기 맵($\mathcal{F}:\mathbb{F}_q^n\rightarrow\mathbb{F}_q^m$)은 $m=o_1+o_2$ 개의 방정식들과 $n=v+m$ 개의 변수들을 갖는 다변수 이차식들의 시스템 ($\mathcal{F}=\mathcal{F}^{(1)},\cdots,\mathcal{F}^{(m)}$)으로 표현될 때, $i=1,\ldots,o_1$ 에 대해 $\mathcal{F}^{(i)}$ 는 아래와 같이 표현되고,

[0020]
$$\begin{cases}\mathcal{F}^{(1)}(x_1,\cdots,x_{v+o_1})=\mathcal{F}_V^{(1)}(x_1,\cdots,x_v)+\mathcal{F}_{OV}^{(1)}(x_1,\cdots,x_{v+o_1})+\delta_1,\\ \vdots\\ \mathcal{F}^{(o_1)}(x_1,\cdots,x_{v+o_1})=\mathcal{F}_V^{(o_1)}(x_1,\cdots,x_v)+\mathcal{F}_{OV}^{(o_1)}(x_1,\cdots,x_{v+o_1})+\delta_{o_1}\end{cases}$$

[0021] 유한체($\mathbb{F}_q$)에서 정의된 v 개의 일차식들($L_1,\ldots,L_v$)과 v 개의 변수들 ($x_1,\ldots,x_v$)가 주어졌을 때, $i=1,\ldots,o_1$ 에 대해 $\mathcal{F}_V^{(i)}$ 는 아래와 같이 표현되고,

[0022]
$$\begin{pmatrix}\mathcal{F}_V^{(1)}\\ \mathcal{F}_V^{(2)}\\ \vdots\\ \mathcal{F}_V^{(o_1)}\end{pmatrix}=\begin{pmatrix}x_1 & x_2 & \cdots & x_v\\ \cdots & \cdots & \cdots & \cdots\\ \cdots & \cdots & \cdots & \cdots\\ \cdots & \cdots & \cdots & \cdots\end{pmatrix}\cdot\begin{pmatrix}L_1\\ L_2\\ \cdots\\ L_v\end{pmatrix}=M_V\cdot\begin{pmatrix}L_1\\ L_2\\ \cdots\\ L_v\end{pmatrix}$$

[0023] 여기서, M_V^1 는 구조화된 행렬 또는 구조화된 행렬의 부분 행렬이고,

[0024] $i=o_1+1,\ldots,m$ 에 대해 $\mathcal{F}^{(i)}$ 는 아래와 같이 표현되고,

[0025]
$$\begin{cases}\mathcal{F}^{(o_1+1)}(x_1,\cdots,x_n)=\mathcal{F}_V^{(o_1+1)}(x_1,\cdots,x_{v+o_1})+\mathcal{F}_{OV}^{(o_1+1)}(x_1,\cdots,x_n)+\delta_{o_1+1},\\ \vdots\\ \mathcal{F}^{(m)}(x_1,\cdots,x_n)=\mathcal{F}_V^{(o_1+o_2)}(x_1,\cdots,x_{v+o_1})+\mathcal{F}_{OV}^{(m)}(x_1,\cdots,x_n)+\delta_m,\end{cases}$$

[0026] $v+o_1$ 의 변수를 갖는 일차식들($L_1',\cdots,L_{v+o_1}'$)과 $v+o_1$ 개의 변수들이 주어졌을 때, $i=o_1+1,\ldots,m$ 에 대해 $\mathcal{F}_V^{(i)}$ 는 아래와 같이 표현되고,

$$\begin{pmatrix} \mathcal{F}_V^{(o_1+1)} \\ \mathcal{F}_V^{(o_1+2)} \\ \vdots \\ \mathcal{F}_V^{(o_1+o_2)} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_{v+o_1} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix} \cdot \begin{pmatrix} L'_1 \\ L'_2 \\ \cdots \\ L'_{v+o_1} \end{pmatrix} = M_V^2 \cdot \begin{pmatrix} L'_1 \\ L'_2 \\ \cdots \\ L'_{v+o_1} \end{pmatrix}$$

[0027]

[0028] 여기서, M_V^2는 구조화된 행렬 또는 구조화된 행렬의 부분 행렬이고, $m=o_1+o_2$이고, $S:\mathbb{F}_q^m \to \mathbb{F}_q^m$이고, $T:\mathbb{F}_q^n \to \mathbb{F}_q^n$이고, $\widetilde{S}=S^{-1}$이고, $\widetilde{T}=T^{-1}$이고, $V=\{1,\cdots,v\}$, $O_1=\{v+1,\cdots,v+o_1\}$, $O_2=\{v+o_1+1,\cdots,v+o_1+o_2\}$, 여기서, $|V|=v$이고, i = 1과 2에 대해 $|O_i|=o_i$이고, V는 비니거 변수들을 정의하기 위한 인덱스 집합이고, O_1과 O_2는 오일 변수들을 정의하기 위한 인덱스 집합들이다.

[0029] 본 발명의 실시 예들에 따라, 키 생성기를 이용한 공개키와 비밀키를 생성하는 방법은 제1아핀 맵($\widetilde{S}$), 제2아핀 맵($\widetilde{T}$)과 맵 ($\mathcal{F}:\mathbb{F}_q^n \to \mathbb{F}_q^m$)을 획득하는 단계와, 상기 제1아핀 맵, 상기 제2아핀 맵, 및 상기 맵을 이용하여 공개키 ($\mathcal{P}=S\circ\mathcal{F}\circ T$)와 비밀키($(\widetilde{S},\mathcal{F},\widetilde{T})$)를 생성하는 단계를 포함하고, 상기 맵 ($\mathcal{F}:\mathbb{F}_q^n \to \mathbb{F}_q^m$)은 $m=o_1+o_2$개의 다변수 이차식들의 시스템 ($\mathcal{F}=\mathcal{F}^{(1)},\cdots,\mathcal{F}^{(m)}$)으로 표현되고, 유한체($\mathbb{F}_q$)에서 정의된 v개의 변수들($x_1,\ldots,x_v$)과 o_1개의 변수들($x_{v+1},x_{v+2},\ldots,x_{v+o_1}$)이 주어졌을 때, 상기 o_1개의 다변수 이차식들의 시스템 ($\mathcal{F}_{OV}^{(1)},\ldots,\mathcal{F}_{OV}^{(o_1)}$)은 아래와 같이 표현되고,

$$\begin{pmatrix} \mathcal{F}_{OV}^{(1)} \\ \mathcal{F}_{OV}^{(2)} \\ \vdots \\ \mathcal{F}_{OV}^{(o_1)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}^T\mathbf{a}_{11} & \mathbf{v}^T\mathbf{a}_{12} & \cdots & \mathbf{v}^T\mathbf{a}_{1o_1} \\ \mathbf{v}^T\mathbf{a}_{21} & \mathbf{v}^T\mathbf{a}_{22} & \cdots & \mathbf{v}^T\mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}^T\mathbf{a}_{o_11} & \mathbf{v}^T\mathbf{a}_{o_12} & \cdots & \mathbf{v}^T\mathbf{a}_{o_1o_1} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix} + B_1 \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{v}^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}^T \end{pmatrix} \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o_1} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o_11} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{o_1o_1} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix} + B_1 \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix}$$

[0030]

[0031] 여기서,

[0032] $$M_{OV,1} = \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o_1} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o_11} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{o_1o_1} \end{pmatrix}$$ 와 $$B_1 = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1o_1} \\ b_{21} & b_{22} & \cdots & b_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{o_11} & b_{o_12} & \cdots & b_{o_1o_1} \end{pmatrix}$$ 로 주어지고, $\mathbf{v}^T=[x_1 \quad x_2 \quad \cdots \quad x_v]$이고, 각 열 벡터($a_{ij}$)를 하나의 행렬의 원소로 간주했을 때, $M_{OV,1}$가 구조화된 행렬이 되도록 각 열 벡터(a_{ij})가 선택되고, B_1도 $M_{OV,1}$와 동일한 형태의 구조화된 행렬이

되도록 원소 값들(b_{ij})이 선택되고,

[0033] $i = o_1 + 1, \ldots, m$ 에 대해 $\mathcal{F}_{OV}^{(i)}$ 는 아래와 같이 주어지고,

[0034]
$$\begin{pmatrix} \mathcal{F}_{OV}^{(o_1+1)} \\ \mathcal{F}_{OV}^{(o_1+2)} \\ \vdots \\ \mathcal{F}_{OV}^{(o_1+o_2)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}'^T\mathbf{a}'_{11} & \mathbf{v}'^T\mathbf{a}'_{12} & \cdots & \mathbf{v}'^T\mathbf{a}'_{1o_2} \\ \mathbf{v}'^T\mathbf{a}'_{21} & \mathbf{v}'^T\mathbf{a}'_{22} & \cdots & \mathbf{v}'^T\mathbf{a}'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}'^T\mathbf{a}'_{o_21} & \mathbf{v}'^T\mathbf{a}'_{o_22} & \cdots & \mathbf{v}'^T\mathbf{a}'_{o_2o_2} \end{pmatrix} \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix} + B_2 \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix}$$
$$= \begin{pmatrix} \mathbf{v}'^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}'^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}'^T \end{pmatrix} \begin{pmatrix} \mathbf{a}'_{11} & \mathbf{a}'_{12} & \cdots & \mathbf{a}'_{1o_2} \\ \mathbf{a}'_{21} & \mathbf{a}'_{22} & \cdots & \mathbf{a}'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}'_{o_21} & \mathbf{a}'_{11} & \cdots & \mathbf{a}'_{o_2o_2} \end{pmatrix} \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix} + B_2 \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix}$$

[0035] 여기서,

[0036]
$$M_{OV,2} = \begin{pmatrix} \mathbf{a}'_{11} & \mathbf{a}'_{12} & \cdots & \mathbf{a}'_{1o_2} \\ \mathbf{a}'_{21} & \mathbf{a}'_{22} & \cdots & \mathbf{a}'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}'_{o_21} & \mathbf{a}'_{11} & \cdots & \mathbf{a}'_{o_2o_2} \end{pmatrix}$$ 와 $$B_2 = \begin{pmatrix} b'_{11} & b'_{12} & \cdots & b'_{1o_2} \\ b'_{21} & b'_{22} & \cdots & b'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ b'_{o_21} & b'_{o_22} & \cdots & b'_{o_2o_2} \end{pmatrix}$$ 로 주어지고,

[0037] $\mathbf{v}'^T = [x_1\ x_2\ \cdots\ x_{v+o_1}]$ 이고, 각 열 벡터(a'_{ij})를 하나의 행렬의 원소로 간주했을 때, $M_{OV,2}$ 가 구조화된 행렬이 되도록 각 열 벡터(a'_{ij})가 선택되고, B_2 도 $M_{OV,2}$ 와 동일한 형태의 구조화된 행렬이 되도록 원소 값들(b'_{ij})이 선택되고, $S : \mathbb{F}_q^m \to \mathbb{F}_q^m$ 이고, $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ 이고, $\widetilde{S} = S^{-1}$ 이고, $\widetilde{T} = T^{-1}$ 이다.

발명의 효과

[0039] 본 발명의 실시 예에 따른 다변수 이차식 기반 전자 서명 알고리즘을 수행하는 방법, 장치 또는 컴퓨터 프로그램은 구조화된 행렬들을 사용함으로써 비밀키의 길이를 크게 줄일 수 있으며, 계산의 효율성을 증대시켜 빠르게 서명 생성을 수행할 수 있는 효과가 있다.

도면의 간단한 설명

[0040] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 실시 예들에 따른 레이어가 1개인 다변수 이차식 기반 전자 서명기의 블록도이다.

도 2는 도 1에 도시된 다변수 이차식 기반 전자 서명기의 동작을 설명하기 위한 플로우 차트이다.

도 3은 본 발명의 실시 예들에 따른 레이어가 2개인 다변수 이차식 기반 전자 서명기의 블록도이다.

도 4는 도 3에 도시된 다변수 이차식 기반 전자 서명기의 동작을 설명하기 위한 플로우 차트이다.

발명을 실시하기 위한 구체적인 내용

[0041] 본 명세서에서는 적당한 연산(또는 연산들)을 수행한 후에, 구조화된 행렬 (structured matrix) 또는 구조화된 행렬의 부분 행렬(submatrix)과 벡터(vector)의 곱으로 표현할 수 있는 다변수 이차식들의 시스템(systems of multivariate quadratic equations)의 생성에 기반한 전자 서명 알고리즘(또는 상기 전자 서명 알고리즘을 수행할 수 있는 장치, 방법, 및/또는 저장 매체에 저장된 컴퓨터 프로그램)이 개시된다.

[0043] 1. v (여기서, v 는 자연수)개의 일차식들과 v 개의 변수들(여기서, x_i , $1 \leq i \leq v$)을 이용하여 구조화된 행렬(structured matrix) 또는 구조화된 행렬의 부분 행렬(submatix)과 벡터(vector)의 곱으로 표현 가능한 o (여기서, o 는 자연수)개의 이차식들을 생성.

[0044] $\mathbb{F}_q$ 가 원소의 개수가 q (여기서, q 는 자연수)개인 유한체(finite field)일 때, 유한체($\mathbb{F}_q$)에서 정의된 v 개의 일차식들($L_1, \ldots, L_v$)과 v 개의 변수들 ($x_1, \ldots, x_v$)이 주어졌을 때, 수학식 1과 같이 구조화된 행렬(또는 구조화된 행렬의 부분 행렬)과 벡터의 곱의 형태로 표현할 수 있는 o 개의 이차식들의 시스템 ($\mathcal{F}_V^{(1)}, \cdots, \mathcal{F}_V^{(o)}$)이 생성된다.

[0045] 이차식들의 시스템($\mathcal{F}_V^{(1)}, \cdots, \mathcal{F}_V^{(o)}$)은 수학식 1로 표현되며, 이때, M_V 는 구조화된 행렬(또는 구조화된 행렬의 부분 행렬)로 정의된다.

[0046] [수학식 1]

$$\begin{pmatrix} \mathcal{F}_V^{(1)} \\ \mathcal{F}_V^{(2)} \\ \cdots \\ \mathcal{F}_V^{(o)} \end{pmatrix} = \begin{pmatrix} x_1 \; x_2 \cdots x_v \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix} = M_V \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix}$$

[0047]

[0048] 여기서, 구조화된 행렬은 구조화된 행렬(또는 구조화된 행렬의 부분 행렬)과 벡터의 곱의 복잡도가 $O(v^2)$ 보다 작거나 같은 경우도 포함한다.

[0050] **1-1. 구조화된 행렬는 순환 행렬(circulant matrix)이다.**

[0051] v 개의 일차방정식들($L_1, \ldots, L_v$)과 v 개의 변수들($x_1, \ldots, x_v$)이 장치 또는 컴퓨터 프로그램에게 주어졌을 때, 수학식 2와 같이 o 개의 이차 방정식들을 포함하는 이차식들의 시스템($\mathcal{F}_V^{(1)}, \cdots, \mathcal{F}_V^{(o)}$)이 생성된다. 여기서, o 는 이차 방정식들의 개수로, 레이어(layer)가 한 개인 경우에는 o 로 표현되고, 레이어가 두 개일 때 첫 번째 레이어는 o_1 으로 표현되고 두 번째 레이어는 o_2 로 표현된다.

[0052] [수학식 2]

$$\begin{aligned} \mathcal{F}_V^{(1)} &= x_1 \cdot L_1 + x_2 \cdot L_2 + \cdots + x_v \cdot L_v, \\ \mathcal{F}_V^{(2)} &= x_v \cdot L_1 + x_1 \cdot L_2 + \cdots + x_{v-1} \cdot L_v, \\ &\cdots, \\ \mathcal{F}_V^{(o)} &= x_{v-o+2} \cdot L_1 + x_{v-o+3} \cdot L_2 + \cdots + x_{v-o+1} \cdot L_v \end{aligned}$$

[0053]

[0055] 수학식 2의 이차식들의 시스템은 수학식 3과 같이 순환 행렬(또는 순환 행렬의 부분 행렬)와 벡터와의 곱의 형태로 표현될 수 있어야 한다. 즉, 수학식 3에서 M_V 는 순환 행렬 또는 순환 행렬의 부분 행렬이 된다.

[0056] [수학식 3]

[0057] $$\begin{pmatrix} \mathcal{F}_V^{(1)} \\ \mathcal{F}_V^{(2)} \\ \cdots \\ \mathcal{F}_V^{(o)} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_v \\ x_v & x_1 & \cdots & x_{v-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{v-o+2} & x_{v-o+3} & \cdots & x_{v-o+1} \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix} = M_V \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix}$$

[0059] **1-2. 블록 순환 행렬(block circulant matrix)로 표현되는 이차식들의 시스템을 추가로 생성**

[0060] 1-1에서 설명한 바와 같이 변수들($x_1, \ldots, x_v$)에 대한 이차식들이 선택된 후, 추가로 $o(=2k)$(여기서, k는 자연수)개의 변수($x_{v+1}, x_{v+2}, \cdots, x_{v+o}$)에 대한 이차식의 시스템($\mathcal{F}_{OV}^{(1)}, \cdots, \mathcal{F}_{OV}^{(o)}$)이 수학식 4와 같이 생성된다.

[0061] [수학식 4]

$$\begin{pmatrix} \mathcal{F}_{OV}^{(1)} \\ \mathcal{F}_{OV}^{(2)} \\ \vdots \\ \mathcal{F}_{OV}^{(o)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}^T\mathbf{a}_{11} & \mathbf{v}^T\mathbf{a}_{12} & \cdots & \mathbf{v}^T\mathbf{a}_{1o} \\ \mathbf{v}^T\mathbf{a}_{21} & \mathbf{v}^T\mathbf{a}_{22} & \cdots & \mathbf{v}^T\mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}^T\mathbf{a}_{o1} & \mathbf{v}^T\mathbf{a}_{o2} & \cdots & \mathbf{v}^T\mathbf{a}_{oo} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix} + B \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{v}^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}^T \end{pmatrix} \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{oo} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix} + B \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix}$$

$$M_{OV} = \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o1} & \mathbf{a}_{o2} & \cdots & \mathbf{a}_{oo} \end{pmatrix} = \begin{pmatrix} \mathbf{p}_1 & \mathbf{p}_2 & \cdots & \mathbf{p}_k & \mathbf{q}_1 & \mathbf{q}_2 & \cdots & \mathbf{q}_k \\ \mathbf{p}_k & \mathbf{p}_1 & \cdots & \mathbf{p}_{k-1} & \mathbf{q}_k & \mathbf{q}_1 & \cdots & \mathbf{q}_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{p}_2 & \mathbf{p}_3 & \cdots & \mathbf{p}_1 & \mathbf{q}_2 & \mathbf{q}_3 & \cdots & \mathbf{q}_1 \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_k & \mathbf{s}_1 & \mathbf{s}_2 & \cdots & \mathbf{s}_k \\ \mathbf{r}_k & \mathbf{r}_1 & \cdots & \mathbf{r}_{k-1} & \mathbf{s}_k & \mathbf{s}_1 & \cdots & \mathbf{s}_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{r}_2 & \mathbf{r}_3 & \cdots & \mathbf{r}_1 & \mathbf{s}_2 & \mathbf{s}_3 & \cdots & \mathbf{s}_1 \end{pmatrix} = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}$$

$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1o} \\ b_{21} & b_{22} & \cdots & b_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ b_{o1} & b_{o2} & \cdots & b_{oo} \end{pmatrix} = \begin{pmatrix} t_1 & t_2 & \cdots & t_k & u_1 & u_2 & \cdots & u_k \\ t_k & t_1 & \cdots & t_{k-1} & u_k & u_1 & \cdots & u_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t_2 & t_3 & \cdots & t_1 & u_2 & u_3 & \cdots & u_1 \\ v_1 & v_2 & \cdots & v_k & w_1 & w_2 & \cdots & w_k \\ v_k & v_1 & \cdots & v_{k-1} & w_k & w_1 & \cdots & w_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ v_2 & v_3 & \cdots & v_1 & w_2 & w_3 & \cdots & w_1 \end{pmatrix}$$

[0062]

[0063] 여기서, $\mathbf{v}^T = [x_1 \quad x_2 \quad \cdots \quad x_v]$ 이고, P, Q, R, S 각각은 벡터들의 순환 행렬이고, M_{OV}는 벡터들의 블록 순환 행렬이고, B 도 M_{OV}와 같은 구조를 가지는 블록 순환 행렬이다.

[0064] 수학식 4의 이차식들의 시스템과 수학식 2의 이차식들의 시스템이 합쳐져서 $x_i x_j, i, j = v+1, \ldots, v+o$ (여기서, i와 j 각각은 자연수)를 만족하는 이차항들(quadratic terms)이 없는 수학식 5와 같은 이차식들의 시스템이 생성된다. 여기서, δ_i 는 유한체($\mathbb{F}_q$)에서 선택된 상수항이다.

[0065] [수학식 5]

$$\begin{cases} \mathcal{F}^{(1)}(x_1,\cdots,x_{v+o}) = & \mathcal{F}_V^{(1)}(x_1,\cdots,x_v)+\mathcal{F}_{OV}^{(1)}(x_1,\cdots,x_{v+o})+\delta_1 \\ & \vdots \\ \mathcal{F}^{(o)}(x_1,\cdots,x_{v+o}) = & \mathcal{F}_V^{(o)}(x_1,\cdots,x_v)+\mathcal{F}_{OV}^{(o)}(x_1,\cdots,x_{v+o})+\delta_o \end{cases}$$

[0066]

[0068] 2. 계수 행렬이 구조화된 행렬(structured matrix) 구조를 갖는 이차식들의 시스템을 생성

[0069] 수학식 6과 같이 표현될 수 있는 $n = v + o$ (n은 자연수)개의 변수들을 가지는 이차식들의 시스템에서, v 개의 변수들($x_1,\ldots,x_v$)과 O 개의 변수들 ($x_{v+1},x_{v+2},\cdots,x_{v+o}$)에 대한 이차식들의 시스템($\mathcal{F}_{OV}^{(i)}$)이 있다고 가정한다.

[0070] [수학식 6]

$$\begin{pmatrix} \mathcal{F}_{OV}^{(1)} \\ \mathcal{F}_{OV}^{(2)} \\ \vdots \\ \mathcal{F}_{OV}^{(o)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}^T\mathbf{a}_{11} & \mathbf{v}^T\mathbf{a}_{12} & \cdots & \mathbf{v}^T\mathbf{a}_{1o} \\ \mathbf{v}^T\mathbf{a}_{21} & \mathbf{v}^T\mathbf{a}_{22} & \cdots & \mathbf{v}^T\mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}^T\mathbf{a}_{o1} & \mathbf{v}^T\mathbf{a}_{o2} & \cdots & \mathbf{v}^T\mathbf{a}_{oo} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix} + B \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{v}^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}^T \end{pmatrix} \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{oo} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix} + B \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix}$$

[0071]

[0072] 여기서, $\mathbf{v}^T = \begin{bmatrix} x_1 & x_2 & \cdots & x_v \end{bmatrix}$ 이고,

[0073] B 와 M_{OV} 는 수학식 7과 같이 표현된다.

[0074] [수학식 7]

$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1o} \\ b_{21} & b_{22} & \cdots & b_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ b_{o1} & b_{o2} & \cdots & b_{oo} \end{pmatrix}, \quad M_{OV} = \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{oo} \end{pmatrix}$$

[0075]

[0076] 이때, 각 열 벡터(a_{ij})를 하나의 행렬의 원소로 간주했을 때, M_{OV} 가 구조화된 행렬이 되도록 각 열 벡터(a_{ij})가 선택되고, B 도 M_{OV} 와 동일한 형태의 구조화된 행렬이 되도록 원소 값들(b_{ij})이 선택되면 원하는 이차식들의 시스템이 생성된다.

[0077] 여기서, 구조화된 행렬이란 기존의 구조화된 행렬 또는 역행렬을 구하거나 구조화된 행렬을 계수 행렬로 갖는 일차식의 시스템의 해를 찾는 복잡도가 $O(n^2)$ 보다 작거나 같은 경우를 포함한다. 이때, 일차식의 시스템의 계수 행렬의 크기는 $n \times n$ 이다.

[0079] **2-1. M_{OV} 와 B 는 블록 순환 행렬(block circulant matrix(BC))이다.**

[0080] $o(=2k)$ 가 짝수일 때, 수학식 8과 수학식 9와 같이 M_{OV} 와 B 각각이 블록 순환 행렬이 되도록, M_{OV}와 B 각각이 선택된다.

[0081] [수학식 8]

$$M_{OV}=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1o} \\ a_{21} & a_{22} & \cdots & a_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ a_{o1} & a_{o2} & \cdots & a_{oo} \end{pmatrix}=\begin{pmatrix} p_1 & p_2 & \cdots & p_k & q_1 & q_2 & \cdots & q_k \\ p_k & p_1 & \cdots & p_{k-1} & q_k & q_1 & \cdots & q_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_2 & p_3 & \cdots & p_1 & q_2 & q_3 & \cdots & q_1 \\ r_1 & r_2 & \cdots & r_k & s_1 & s_2 & \cdots & s_k \\ r_k & r_1 & \cdots & r_{k-1} & s_k & s_1 & \cdots & s_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ r_2 & r_3 & \cdots & r_1 & s_2 & s_3 & \cdots & s_1 \end{pmatrix}=\begin{pmatrix} P & Q \\ R & S \end{pmatrix}$$

[0082]

[0083] 여기서, P, Q, R, S 각각은 벡터들의 순환 행렬이고, M_{OV} 는 벡터들의 블록 순환 행렬이다.

[0084] [수학식 9]

$$B=\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1o} \\ b_{21} & b_{22} & \cdots & b_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ b_{o1} & b_{o2} & \cdots & b_{oo} \end{pmatrix}=\begin{pmatrix} t_1 & t_2 & \cdots & t_k & u_1 & u_2 & \cdots & u_k \\ t_k & t_1 & \cdots & t_{k-1} & u_k & u_1 & \cdots & u_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t_2 & t_3 & \cdots & t_1 & u_2 & u_3 & \cdots & u_1 \\ v_1 & v_2 & \cdots & v_k & w_1 & w_2 & \cdots & w_k \\ v_k & v_1 & \cdots & v_{k-1} & w_k & w_1 & \cdots & w_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ v_2 & v_3 & \cdots & v_1 & w_2 & w_3 & \cdots & w_1 \end{pmatrix}$$

[0085]

[0086] 여기서, B 는 블록 순환 행렬이다.

[0088] **2-2. 주어진 블록 순환 행렬(BC)의 역행렬(BC^{-1})을 효율적으로 계산하는 방법**

[0089] 주어진 블록 순환 행렬($BC=\begin{pmatrix} P & Q \\ R & S \end{pmatrix}$)의 블록 행렬식($K=PS-QR$)이 구해진다. P, Q, R, S모두가 순환 행렬이므로, K 도 역시 순환 행렬이다.

[0090] 먼저, K 의 역행렬(K^{-1})이 구해지고, BC 의 역행렬(BC^{-1})은 $\begin{pmatrix} K^{-1}S & -K^{-1}Q \\ -K^{-1}R & K^{-1}P \end{pmatrix}$ 을 계산해서 구해진다. 이때, K 의 역행렬을 구하기 위해 확장 유클리드 알고리즘(Extended Euclidean Algorithm) 등의 효율적인 알고리즘이 이용된다.

[0092] **3. 구조화된 행렬을 이용한 랜덤화(randomization)**

[0093] 부채널(side-channel) 공격 등 다양한 공격들에 대응하기 위한 메시지 랜덤화나 비밀키 랜덤화의 실시 예들은 아래와 같다.

[0094] (i) 행렬과 메시지(또는 비밀키)를 더하여 제1연산 결과를 생성한 후, 상기 제1연산 결과로부터 상기 행렬을 빼기, 또는

[0095] (ii) 행렬과 메시지(또는 비밀키)를 곱하여 제2연산 결과를 생성한 후, 상기 제2연산 결과에 상기 행렬의 역행

렬을 곱하기.

[0096] 이때, 행렬이 구조화된 행렬로 선택되면, 계산 효율이 높아지는 효과가 있다.

[0098] **3-1. 순환 행렬 또는 블록 순환 행렬을 이용한 랜덤화(randomization)**

[0099] 부채널(side-channel) 공격 등 다양한 공격들에 대응하기 위한 메시지 랜덤화나 비밀키 랜덤화의 실시 예들은 아래와 같다.

[0100] (i) 행렬과 메시지(또는 비밀키)를 더하여 제1연산 결과를 생성한 후, 상기 제1연산 결과로부터 상기 행렬을 빼기, 또는

[0101] (ii) 행렬과 메시지(또는 비밀키)를 곱하여 제2연산 결과를 생성한 후, 상기 제2연산 결과에 상기 행렬의 역행렬을 곱하기.

[0102] 이때, 랜덤 행렬이 순환 행렬 또는 블록 순환 행렬로 선택되면, 계산 효율이 높아지는 효과가 있다.

[0104] 3-2. $\mathbb{F}_q$가 원소의 개수가 q개인 유한체(finite field)일 때, $\mathbb{F}_q^m$의 벡터 (h)와 비밀키($\tilde{S}$)와의 곱 ($\tilde{S} \cdot \mathbf{h}$)에서 비밀키($\tilde{S}$)의 랜덤화를 위해, 수학식 10과 같이 랜덤 행렬(R)이 순환 행렬로 선택되면, 계산 효율은 높아지는 효과가 있다.

[0105] [수학식 10]

[0106] $\tilde{S}(H(m)) = (\tilde{S} + R)(H(m)) - R(H(m))$ 또는

[0107] $\tilde{S}(H(m)) = (\tilde{S} \cdot R^{-1} \cdot R)(H(m))$

[0108] 여기서, $\tilde{S} = S^{-1}$이고, $H(m)$은 메시지(m)에 대한 해시 값으로 $H(m) = \xi = (\xi_1, \cdots, \xi_m) \in \mathbb{F}_q^m$으로 표현된다.

[0110] 본 발명에 따른 다변수 이차식 기반 전자(또는 디지털) 서명 알고리즘은 키 생성 알고리즘, 서명 생성 알고리즘, 및 서명 검증 알고리즘을 포함한다. 상기 다변수 이차식 기반 전자 서명 알고리즘은 전자 장치(또는 디지털 서명 장치)에 의해 실행되거나 상기 전자 장치에서 실행되는 컴퓨터 프로그램에 의해 실행된다.

[0111] 저장 매체에 저장된 컴퓨터 프로그램은 구조화된 행렬에 기초한 전자 서명 알고리즘(인증(authentication), 부인 방지(non-repudiation), 및/또는 메시지(또는 데이터)의 무결성(integrity)를 보호하는 알고리즘)를 위한 방법을 수행하기 위한 프로그램 코드를 갖고, 상기 프로그램 코드는 컴퓨팅 장치에서 실행된다.

[0112] 컴퓨팅 장치는 PC, 서버, 또는 모바일 장치를 의미하고, 상기 모바일 장치는 이동 전화기, 스마트폰, 인터넷 모바일 장치(internet mobile device(MID)), 랩탑 컴퓨터 등을 의미하나 이에 한정되는 것은 아니다.

[0113] 도 1은 본 발명의 실시 예들에 따른 레이어가 1개인 다변수 이차식 기반 전자 서명기의 블록도이고, 도 2는 도 1에 도시된 다변수 이차식 기반 전자 서명기의 동작을 설명하기 위한 플로우 차트이다.

[0114] 도 1의 전자 서명기(100)는 1개의 레이어(layer)를 갖는 비밀 센트럴 맵 (security central map)을 구성하고, 이를 이용하여 다변수 이차식 기반 전자 서명 알고리즘을 실행하고, 키 생성기(110), 서명 생성기(120), 및 서명 검증기(130)를 포함한다.

[0115] 본 명세서에서 전자 서명기(100 또는 200)는 하드웨어 컴포넌트 또는 소프트웨어 컴포넌트로 구현될 수 있다. 전자 서명기(100 또는 200)가 하드웨어 컴포넌트로 구현될 때 구성 요소들(110, 120, 및 130) 각각은 하드웨어 컴포넌트로 구현되고, 전자 서명기(100)가 소프트웨어 컴포넌트로 구현될 때 구성 요소들(110, 120, 및 130) 각

각은 소프트웨어 컴포넌트로 구현된다.

[0117] **키 생성(key generation) 알고리즘**

[0118] 키 생성기(110)는 공개키(public key)를 계산하는 키 생성(key generation) 알고리즘을 수행하기 위해 단계들(S110~S130)을 수행한다.

[0119] 보안 파라미터(λ)에 대해, 공개키(PK)와 비밀키(SK)의 쌍($< PK, SK >=< \mathcal{P}, (\mathcal{F}, \tilde{T}) >$)은 다음과 같이 생성된다. 보안 파라미터(λ)는 비도(security level)를 나타낸다.

[0120] 1. 한 개의 아핀 맵($\tilde{T}$)이 랜덤하게 선택된다(S110). 아핀 맵($\tilde{T}$)이 역변환 가능(invertable)하지 않다면, 새로운 아핀 맵이 랜덤하게 다시 선택된다. 여기서, $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ 이고, $\tilde{T} = T^{-1}$ 이다. 아핀 맵들과 비밀 센트럴 맵 ($\mathcal{F} = \mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$)은 키 생성기(110)가 액세스할 수 있는 장치(예컨대, 데이터 저장장치)에 안전하게 저장되어 있다고 가정한다.

[0122] 2. 비밀 센트럴 맵($\mathcal{F} = \mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$)은 아래와 같이 선택된다(S120).

[0123] 구조화된 행렬을 이용한 다변수 이차식 기반 전자서명 알고리즘으로의 응용을 위해, 본 발명에 따른 새로운 센트럴 맵의 구성은 레이어(layer)가 한(1) 개인 경우 2개의 인덱스 집합들(V, O)이 필요하다. $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ 이고, n 과 m 각각은 자연수이다.

[0124] $$V = \{1, \cdots, v\}$$

[0125] $$O = \{v+1, \cdots, v+o\}$$

[0126] 여기서, $|V| = v$ 이고, $|O| = o$ 이다. V 는 비니거(Vinegar) 변수들을 정의하기 위한 인덱스 집합이고, O 는 오일(Oil) 변수들을 정의하기 위한 인덱스 집합이다.

[0127] 비밀 센트럴 맵($\mathcal{F} = \mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$), 즉 $m = o$ 개의 방정식들과 $n = v + m$ 개의 변수들을 갖는 다변수 이차식들의 시스템에서,

[0128] $i = 1, \cdots, o$ 에 대해 $\mathcal{F}^{(i)}$ 는 수학식 11과 같이 정의된다.

[0129] [수학식 11]

[0130] $$\begin{cases} \mathcal{F}^{(1)}(x_1, \cdots, x_{v+o}) = \mathcal{F}_V^{(1)}(x_1, \cdots, x_v) + \mathcal{F}_{OV}^{(1)}(x_1, \cdots, x_{v+o}) + \delta_1 \\ \vdots \\ \mathcal{F}^{(o)}(x_1, \cdots, x_{v+o}) = \mathcal{F}_V^{(o)}(x_1, \cdots, x_v) + \mathcal{F}_{OV}^{(o)}(x_1, \cdots, x_{v+o}) + \delta_o \end{cases}$$

[0131] $i = 1, \cdots, o$ 에 대해 $\mathcal{F}_V^{(i)}$ 는 수학식 12와 같이 정의되고,

[0132] [수학식 12]

$$\begin{pmatrix} \mathcal{F}_V^{(1)} \\ \mathcal{F}_V^{(2)} \\ \cdots \\ \mathcal{F}_V^{(o)} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_v \\ x_v & x_1 & \cdots & x_{v-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{v-o+2} & x_{v-o+3} & \cdots & x_{v-o+1} \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix} = M_V \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix}$$

[0133]

[0134] 여기서, M_v 는 순환 행렬 또는 순환 행렬의 부분 행렬이다.

[0135] $i = 1, \cdots, o$ 에 대해 $\mathcal{F}_{OV}^{(i)}$ 는 수학식 13과 같이 정의되고,

[0136] [수학식 13]

$$\begin{pmatrix} \mathcal{F}_{OV}^{(1)} \\ \mathcal{F}_{OV}^{(2)} \\ \vdots \\ \mathcal{F}_{OV}^{(o)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}^T\mathbf{a}_{11} & \mathbf{v}^T\mathbf{a}_{12} & \cdots & \mathbf{v}^T\mathbf{a}_{1o} \\ \mathbf{v}^T\mathbf{a}_{21} & \mathbf{v}^T\mathbf{a}_{22} & \cdots & \mathbf{v}^T\mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}^T\mathbf{a}_{o1} & \mathbf{v}^T\mathbf{a}_{o2} & \cdots & \mathbf{v}^T\mathbf{a}_{oo} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix} + B \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{v}^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}^T \end{pmatrix} \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{oo} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix} + B \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o} \end{pmatrix}$$

[0137]

[0138] 여기서, B 는 수학식 9의 B 와 같고, M_{OV} 는 수학식 8의 M_{OV} 와 같다.

$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1o} \\ b_{21} & b_{22} & \cdots & b_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ b_{o1} & b_{o2} & \cdots & b_{oo} \end{pmatrix}, \quad M_{OV} = \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{oo} \end{pmatrix}$$

[0139]

$$M_{OV} = \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o1} & \mathbf{a}_{o2} & \cdots & \mathbf{a}_{oo} \end{pmatrix} = \begin{pmatrix} \mathbf{p}_1 & \mathbf{p}_2 & \cdots & \mathbf{p}_k & \mathbf{q}_1 & \mathbf{q}_2 & \cdots & \mathbf{q}_k \\ \mathbf{p}_k & \mathbf{p}_1 & \cdots & \mathbf{p}_{k-1} & \mathbf{q}_k & \mathbf{q}_1 & \cdots & \mathbf{q}_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{p}_2 & \mathbf{p}_3 & \cdots & \mathbf{p}_1 & \mathbf{q}_2 & \mathbf{q}_3 & \cdots & \mathbf{q}_1 \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_k & \mathbf{s}_1 & \mathbf{s}_2 & \cdots & \mathbf{s}_k \\ \mathbf{r}_k & \mathbf{r}_1 & \cdots & \mathbf{r}_{k-1} & \mathbf{s}_k & \mathbf{s}_1 & \cdots & \mathbf{s}_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{r}_2 & \mathbf{r}_3 & \cdots & \mathbf{r}_1 & \mathbf{s}_2 & \mathbf{s}_3 & \cdots & \mathbf{s}_1 \end{pmatrix} = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}$$

$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1o} \\ b_{21} & b_{22} & \cdots & b_{2o} \\ \vdots & \vdots & \ddots & \vdots \\ b_{o1} & b_{o2} & \cdots & b_{oo} \end{pmatrix} = \begin{pmatrix} t_1 & t_2 & \cdots & t_k & u_1 & u_2 & \cdots & u_k \\ t_k & t_1 & \cdots & t_{k-1} & u_k & u_1 & \cdots & u_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t_2 & t_3 & \cdots & t_1 & u_2 & u_3 & \cdots & u_1 \\ v_1 & v_2 & \cdots & v_k & w_1 & w_2 & \cdots & w_k \\ v_k & v_1 & \cdots & v_{k-1} & w_k & w_1 & \cdots & w_{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ v_2 & v_3 & \cdots & v_1 & w_2 & w_3 & \cdots & w_1 \end{pmatrix}$$

[0140]

[0141] 상수항(δ_i)는 유한체($\mathbb{F}_q$)에서 랜덤하게 선택된다.

[0143] 3. 공개키($\mathcal{P} = \mathcal{F} \circ T$)가 계산된다(S130). 여기서, 원(circle)은 합성 (composition)을 의미하고, 공개키

($\mathcal{P} = \mathcal{F} \circ T$)는 서명 검증을 위해 필요하고, 비밀키($SK = (\mathcal{F}, \tilde{T})$)는 서명 검증을 위해 필요하다.

[0145] **서명 생성(signature generation) 알고리즘**

[0146] 서명 생성기(120)는 서명 생성(signature generation) 알고리즘, 즉 본 발명에 따른 새로운 센트럴 맵을 역변환하는 방법(how to invert the central map)을 수행하기 위해 단계들(S140 내지 S160)을 수행한다.

[0147] 서명 생성기(120)는 아핀 맵 ($\tilde{T}$), 비밀 센트럴 맵($\mathcal{F}$), 및 메시지(m)를 수신한다. 메시지(m)는 원문(plaintext) 그대로 통신 매체(예컨대, 유선 또는 무선)를 통해 전송될 메시지를 의미한다.

[0149] 1. 메시지(m)에 대해 해시(hash) 메시지(H(m)=ξ)가 계산된다(S140). 여기서, $H : \{0,1\}^* \rightarrow \mathbb{F}_q^m$ 는 충돌 방지 해시 함수(collision resistant hash function)이다. $H(m) = \xi = (\xi_1, \cdots, \xi_m) \in \mathbb{F}_q^m$ 이 계산된다.

[0151] 2. $\xi = (\xi_1, \cdots, \xi_m)$ 가 주어질 때, $\mathcal{F}^{-1}(\xi) = \mathbf{s}$, 즉 $\mathcal{F}(\mathbf{x}) = \xi$ 의 해 (solution) $\mathbf{s} = (s_1, \cdots, s_n)$ 를 찾는 과정들은 아래와 같다(S150).

[0152] 랜덤 값들의 벡터, $\mathbf{s_v} = (s_1, \cdots, s_v) \in \mathbb{F}_q^v$ 를 선택한다. 벡터($\mathbf{s_v}$)를 $i = 1, \cdots, m$ 에 대한 $\mathcal{F}_V^{(i)}$ 에 대입(plug)하여, $v \times v$ 순환 행렬의 $o \times v$ 부분 행렬과 벡터($(L_1(s_v), \cdots, L_v(s_v))$)의 전치 행렬(transpose)의 곱을 계산하고, 그 결과로 $(c_1, \cdots, c_o)$ 를 얻는다. 이때, $o \times v$ 부분 행렬은 수학식 3의 M_V 이다.

[0153] 벡터($\mathbf{s_v}$)를 $i = 1, \cdots, m$ 에 대한 $\mathcal{F}_{OV}^{(i)}$ 에 대입하여 o 개의 변수들 $(x_{v+1}, \cdots, x_n)$ 을 갖는 o 개의 일차 방정식들의 시스템을 구하면, 계수 행렬의 형태는 블록 순환 행렬(BC)로 된다.

[0154] 여기서, 블록 순환 행렬(BC)은 벡터($\mathbf{s_v}$)를 수학식 13의 $\mathbf{v}^T$ 로 구성된 행렬에 대입해서 얻어진 행렬에 M_{OV} 를 곱해서 얻어진 행렬이다.

[0155] 앞에서 설명한 2-2에서 정의한 방법으로 구한 역행렬(BC^{-1})에 $(\xi_1 - c_1 - \delta_1, \cdots, \xi_o - c_o - \delta_o)$ 의 전치 행렬(transpose)을 곱하여 해 $(s_{v+1}, \cdots, s_n)$ 를 구한다. 그러면, 벡터 $\mathbf{s} = (s_1, \cdots, s_n)$ 는 $\mathcal{F}(\mathbf{x}) = \xi$ 의 해이다.

[0156] 만약, 블록 순환 행렬(BC)의 역행렬(BC^{-1})이 존재하지 않으면, 서명 생성 알고리즘의 처음으로 돌아가 새로운 랜덤 값들의 벡터($\mathbf{s_v}' = (s_1', \cdots, s_v')$)를 선택하여 앞에서 설명한 방법들(또는 과정들)을 다시 수행

한다.

[0158] 3. $\widetilde{T}(\mathbf{s})=\sigma$ 가 계산된다(S160). σ 는 메시지(m)의 서명(여기서, 서명은 디지털 서명(digital signature) 또는 전자 서명(electronic signature)을 의미함)이다.

[0160] **서명 검증 또는 검증 알고리즘**

[0161] 서명 검증기(130)는 서명 검증 또는 검증 알고리즘을 수행하기 위해 단계 (S170)을 수행한다. 서명 검증기(130)는 서명 생성기(120)로부터 공개키($\mathcal{P}$)와 공개키($\mathcal{P}$)를 포함하는 인증서 중에서 어느 하나, 메시지(m), 및 서명(σ)을 수신하고, 즉 메시지(m)에 대한 서명(σ)과 공개키($\mathcal{P}$)가 주어지면, $P(\sigma)=H(m)$ 인지가 확인된다. $P(\sigma)=H(m)$ 이면 서명(σ)이 수락되고, 그렇지 않으면 서명(σ)은 거절된다.

[0163] 도 3은 본 발명의 실시 예들에 따른 레이어가 2개인 다변수 이차식 기반 전자 서명기의 블록도이고, 도 4는 도 3에 도시된 다변수 이차식 기반 전자 서명기의 동작을 설명하기 위한 플로우 차트이다.

[0164] 도 3의 전자 서명기(200)는 2개의 레이어들(layers)을 갖는 비밀 센트럴 맵을 구성하고 처리한다.

[0165] 키 생성기(210)는 공개키를 계산하는 키 생성 알고리즘을 수행하기 위해 단계들(S210~S230)을 수행한다.

[0167] **키생성 알고리즘**:

[0168] 보안 파라미터(λ)에 대해, 공개키(PK)와 비밀키(SK)의 쌍($<PK,SK>=<\mathcal{P},(\widetilde{S},\mathcal{F},\widetilde{T})>$)이 다음과 같이 생성된다. 보안 파라미터($\lambda$)는 비도를 나타낸다.

[0169] 1. 두 개의 아핀 맵들($\widetilde{S}$와 $\widetilde{T}$)이 랜덤하게 선택된다(S210). $\widetilde{S}$와 $\widetilde{T}$가 역변환가능(invertable)하지 않다면, 두 개의 (새로운) 아핀 맵들($\widetilde{S}$와 $\widetilde{T}$)이 랜덤하게 다시 선택된다. 여기서, $S:\mathbb{F}_q^m\rightarrow\mathbb{F}_q^m$ 와 $\widetilde{S}=S^{-1}$ 이고, $T:\mathbb{F}_q^n\rightarrow\mathbb{F}_q^n$ 와 $\widetilde{T}=T^{-1}$ 이다. 아핀 맵들($\widetilde{S}$와 $\widetilde{T}$)을 포함하는 아핀 맵들과 비밀 센트럴 맵 ($\mathcal{F}=\mathcal{F}^{(1)},\cdots,\mathcal{F}^{(m)}$)은 키 생성기(210)에 의해 액세스 가능한 장치에 안전하게 저장될 수 있다.

[0171] 2. 비밀 센트럴 맵($\mathcal{F}=\mathcal{F}^{(1)},\cdots,\mathcal{F}^{(m)}$)을 아래와 같이 선택한다 (S220).

[0172] 구조화된 행렬을 이용한 다변수 이차식 기반 전자서명 알고리즘으로의 응용을 위해, 본 발명에 따른 새로운 센트럴 맵의 구성은 레이어들이 두개인 경우 3개의 인덱스 집합들(V, O_1, 및 O_2)이 필요하다.

[0173] $V=\{1,\cdots,v\}$,

[0174] $O_1=\{v+1,\cdots,v+o_1\}$,

[0175] $O_2=\{v+o_1+1,\cdots,v+o_1+o_2\}$

[0176] 여기서, $|V| = v$ 이고, $i = 1, 2$ 에 대해 $|O_i| = o_i$ 이다. V는 비니거 변수들을 정의하기 위한 인덱스 집합이고, O_1 과 O_2는 오일 변수들을 정의하기 위한 인덱스 집합들이다.

[0177] 비밀 센트럴 맵($\mathcal{F} = \mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)}$) , 즉 $m = o_1 + o_2$ (여기서, o_1과 o_2 각각은 자연수)개의 방정식들과 $n = v + m$ 개의 변수들을 갖는 이차식들의 시스템에서, $i = 1, \ldots, o_1$ 에 대해 $\mathcal{F}^{(i)}$는 수학식 14와 같이 정의된다.

[0178] [수학식 14]

[0179]
$$\begin{cases} \mathcal{F}^{(1)}(x_1, \cdots, x_{v+o_1}) = \mathcal{F}_V^{(1)}(x_1, \cdots, x_v) + \mathcal{F}_{OV}^{(1)}(x_1, \cdots, x_{v+o_1}) + \delta_1, \\ \vdots \\ \mathcal{F}^{(o_1)}(x_1, \cdots, x_{v+o_1}) = \mathcal{F}_V^{(o_1)}(x_1, \cdots, x_v) + \mathcal{F}_{OV}^{(o_1)}(x_1, \cdots, x_{v+o_1}) + \delta_{o_1} \end{cases}$$

[0180] 여기서, $\mathcal{F}_V^{(i)}$ 는 수학식 2와 같이 정의되고, $\mathcal{F}_{OV}^{(i)}$ 는 수학식 4와 같이 정의된다. 이때, 앞에서 설명한 1-2에서 처럼 o 가 o_1 ($o_1 = 2k_1$, 여기서 k_1 은 자연수)으로 대체되면, 수학식 3은 수학식 15로 되고, 수학식 6은 수학식 16으로 되고, 수학식 8과 수학식 9는 수학식 17로 된다.

[0181] [수학식 15]

[0182]
$$\begin{pmatrix} \mathcal{F}_V^{(1)} \\ \mathcal{F}_V^{(2)} \\ \cdots \\ \mathcal{F}_V^{(o_1)} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_v \\ x_v & x_1 & \cdots & x_{v-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{v-o_1+2} & x_{v-o_1+3} & \cdots & x_{v-o_1+1} \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix} = M_V^1 \cdot \begin{pmatrix} L_1 \\ L_2 \\ \cdots \\ L_v \end{pmatrix}$$

[0183] 여기서, M_V^1 는 순환 행렬 또는 순환 행렬의 부분 행렬이고,

[0184] $i=1, \ldots, o_1$ 에 대해 $\mathcal{F}_{OV}^{(i)}$ 는 수학식 16과 같다.

[0185] [수학식 16]

[0186]
$$\begin{pmatrix} \mathcal{F}_{OV}^{(1)} \\ \mathcal{F}_{OV}^{(2)} \\ \vdots \\ \mathcal{F}_{OV}^{(o_1)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}^T\mathbf{a}_{11} & \mathbf{v}^T\mathbf{a}_{12} & \cdots & \mathbf{v}^T\mathbf{a}_{1o_1} \\ \mathbf{v}^T\mathbf{a}_{21} & \mathbf{v}^T\mathbf{a}_{22} & \cdots & \mathbf{v}^T\mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}^T\mathbf{a}_{o_1 1} & \mathbf{v}^T\mathbf{a}_{o_1 2} & \cdots & \mathbf{v}^T\mathbf{a}_{o_1 o_1} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix} + B_1 \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix}$$
$$= \begin{pmatrix} \mathbf{v}^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}^T \end{pmatrix} \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o_1} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o_1 1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{o_1 o_1} \end{pmatrix} \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix} + B_1 \begin{pmatrix} x_{v+1} \\ x_{v+2} \\ \vdots \\ x_{v+o_1} \end{pmatrix}$$

[0187] 여기서,

[0188] $\mathbf{v}^T = \begin{bmatrix} x_1 & x_2 & \cdots & x_v \end{bmatrix}$ 이고,

[0189] $M_{OV,1} = \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o_1} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o_1 1} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{o_1 o_1} \end{pmatrix}$ 이고, $B_1 = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1o_1} \\ b_{21} & b_{22} & \cdots & b_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{o_1 1} & b_{o_1 2} & \cdots & b_{o_1 o_1} \end{pmatrix}$

[0190] 이다.

[0191] 여기서, $M_{OV,1}$ 은 각각이 크기(v)를 갖는 열 벡터들($\mathbf{a}_{ij}$)을 원소로 하는 블록 순환 행렬이고, B_1은 블록 순환 행렬이다.

[0192] 벡터들의 블록 순환 행렬($M_{OV,1}$)과 블록 순환 행렬(B_1)은 수학식 17과 같다.

[0193] [수학식 17]

$$M_{OV,1} = \begin{pmatrix} \mathbf{a}_{11} & \mathbf{a}_{12} & \cdots & \mathbf{a}_{1o_1} \\ \mathbf{a}_{21} & \mathbf{a}_{22} & \cdots & \mathbf{a}_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{o_1 1} & \mathbf{a}_{o_1 2} & \cdots & \mathbf{a}_{o_1 o_1} \end{pmatrix} = \begin{pmatrix} \mathbf{p}_1 & \mathbf{p}_2 & \cdots & \mathbf{p}_{k_1} & \mathbf{q}_1 & \mathbf{q}_2 & \cdots & \mathbf{q}_{k_1} \\ \mathbf{p}_{k_1} & \mathbf{p}_1 & \cdots & \mathbf{p}_{k_1-1} & \mathbf{q}_{k_1} & \mathbf{q}_1 & \cdots & \mathbf{q}_{k_1-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{p}_2 & \mathbf{p}_3 & \cdots & \mathbf{p}_1 & \mathbf{q}_2 & \mathbf{q}_3 & \cdots & \mathbf{q}_1 \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_{k_1} & \mathbf{s}_1 & \mathbf{s}_2 & \cdots & \mathbf{s}_{k_1} \\ \mathbf{r}_{k_1} & \mathbf{r}_1 & \cdots & \mathbf{r}_{k_1-1} & \mathbf{s}_{k_1} & \mathbf{s}_1 & \cdots & \mathbf{s}_{k_1-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{r}_2 & \mathbf{r}_3 & \cdots & \mathbf{r}_1 & \mathbf{s}_2 & \mathbf{s}_3 & \cdots & \mathbf{s}_1 \end{pmatrix} = \begin{pmatrix} P_1 & Q_1 \\ R_1 & S_1 \end{pmatrix}$$

$$B_1 = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1o_1} \\ b_{21} & b_{22} & \cdots & b_{2o_1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{o_1 1} & b_{o_1 2} & \cdots & b_{o_1 o_1} \end{pmatrix} = \begin{pmatrix} t_1 & t_2 & \cdots & t_{k_1} & u_1 & u_2 & \cdots & u_{k_1} \\ t_k & t_1 & \cdots & t_{k_1-1} & u_k & u_1 & \cdots & u_{k_1-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t_2 & t_3 & \cdots & t_1 & u_2 & u_3 & \cdots & u_1 \\ v_1 & v_2 & \cdots & v_{k_1} & w_1 & w_2 & \cdots & w_{k_1} \\ v_k & v_1 & \cdots & v_{k_1-1} & w_k & w_1 & \cdots & w_{k_1-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ v_2 & v_3 & \cdots & v_1 & w_2 & w_3 & \cdots & w_1 \end{pmatrix}$$

[0194]

[0195] 여기서, P_1, Q_1, R_1, S_1은 벡터들의 순환 행렬이고, $M_{OV,1}$는 벡터들의 블록 순환 행렬이다.

[0196] 마지막으로, 상수항(δ_i)은 유한체($\mathbb{F}_q$)에서 랜덤하게 선택된다.

[0197] $i = o_1 + 1, \ldots, m$ 에 대해 $\mathcal{F}^{(i)}$는 수학식 18과 같이 정의된다.

[0198] [수학식 18]

$$\begin{cases} \mathcal{F}^{(o_1+1)}(x_1, \cdots, x_n) = \mathcal{F}_V^{(o_1+1)}(x_1, \cdots, x_{v+o_1}) + \mathcal{F}_{OV}^{(o_1+1)}(x_1, \cdots, x_n) + \delta_{o_1+1}, \\ \qquad \vdots \\ \mathcal{F}^{(m)}(x_1, \cdots, x_n) = \mathcal{F}_V^{(o_1+o_2)}(x_1, \cdots, x_{v+o_1}) + \mathcal{F}_{OV}^{(m)}(x_1, \cdots, x_n) + \delta_m, \end{cases}$$

[0199]

[0200] 여기서, $\mathcal{F}_V^{(i)}$는 수학식 2와 같이 정의된다. 이때, 앞에서 설명한 1-1의 L_i가 L_i'으로 대체되고, v가 $v+o_1$으로 대체되면, $\mathcal{F}_V^{(i)}$는 수학식 19와 같다.

[0201] [수학식 19]

$$\mathcal{F}_V^{(o_1+1)} = x_1 \cdot L'_1 + x_2 L'_2 + \cdots + x_{v+o_1} L'_{v+o_1},$$

$$\mathcal{F}_V^{(o_1+2)} = x_v \cdot L'_1 + x_1 L'_2 + \cdots + x_{v+o_1-1} L'_{v+o_1},$$

$$\cdots,$$

$$\mathcal{F}_V^{(o_1+o_2)} = x_{v+o_1-o_2+2} \cdot L'_1 + x_{v+o_1-o_2+3} L'_2 + \cdots + x_{v+o_1-o_2+1} L'_{v+o_1},$$

[0202]

[0203] $\mathcal{F}_{OV}^{(i)}$는 수학식 4와 같이 정의된다. 이때, 1-2에서 설명한 v가 $v+o_1$으로 대체되고, o가 o_2($o_2 = 2k_2$, 여기서 k_2는 자연수)로 대체되면, 수학식 3은 수학식 20으로 되고, 수학식 6은 수학식 21로 되고, 수학식 8과 수학식 9는 수학식 22로 된다.

[0204] [수학식 20]

$$\begin{pmatrix} \mathcal{F}_V^{(o_1+1)} \\ \mathcal{F}_V^{(o_1+2)} \\ \cdots \\ \mathcal{F}_V^{(o_1+o_2)} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_{v+o_1} \\ x_v & x_1 & \cdots & x_{v+o_1-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{v+o_1-o_2+2} & x_{v+o_1-o_2+3} & \cdots & x_{v+o_1-o_2+1} \end{pmatrix} \cdot \begin{pmatrix} L'_1 \\ L'_2 \\ \cdots \\ L'_{v+o_1} \end{pmatrix} = M_V^2 \cdot \begin{pmatrix} L'_1 \\ L'_2 \\ \cdots \\ L'_{v+o_1} \end{pmatrix}$$

[0205]

[0206] 여기서, M_V^2는 순환 행렬 또는 순환 행렬의 부분 행렬이고, $i=o_1+1, \ldots, o_1+o_2$에 대해 $\mathcal{F}_{OV}^{(i)}$는 수학식 21과 같이 정의된다.

[0207] [수학식 21]

$$\begin{pmatrix} \mathcal{F}_{OV}^{(o_1+1)} \\ \mathcal{F}_{OV}^{(o_1+2)} \\ \vdots \\ \mathcal{F}_{OV}^{(o_1+o_2)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}'^T \mathbf{a}'_{11} & \mathbf{v}'^T \mathbf{a}'_{12} & \cdots & \mathbf{v}'^T \mathbf{a}'_{1o_2} \\ \mathbf{v}'^T \mathbf{a}'_{21} & \mathbf{v}'^T \mathbf{a}'_{22} & \cdots & \mathbf{v}'^T \mathbf{a}'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}'^T \mathbf{a}'_{o_2 1} & \mathbf{v}'^T \mathbf{a}'_{o_2 2} & \cdots & \mathbf{v}'^T \mathbf{a}'_{o_2 o_2} \end{pmatrix} \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix} + B_2 \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{v}'^T & 0 & \cdots & 0 \\ 0 & \mathbf{v}'^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{v}'^T \end{pmatrix} \begin{pmatrix} \mathbf{a}'_{11} & \mathbf{a}'_{12} & \cdots & \mathbf{a}'_{1o_2} \\ \mathbf{a}'_{21} & \mathbf{a}'_{22} & \cdots & \mathbf{a}'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}'_{o_2 1} & \mathbf{a}'_{11} & \cdots & \mathbf{a}'_{o_2 o_2} \end{pmatrix} \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix} + B_2 \begin{pmatrix} x_{v+o_1+1} \\ x_{v+o_1+2} \\ \vdots \\ x_{v+o_1+o_2} \end{pmatrix}$$

[0208]

[0209] 여기서,

[0210] $\mathbf{v}'^T = [x_1 \quad x_2 \quad \cdots x_{v+o_1}]$ 이고,

[0211] $M_{OV,2} = \begin{pmatrix} \mathbf{a}'_{11} & \mathbf{a}'_{12} & \cdots & \mathbf{a}'_{1o_2} \\ \mathbf{a}'_{21} & \mathbf{a}'_{22} & \cdots & \mathbf{a}'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}'_{o_2 1} & \mathbf{a}'_{11} & \cdots & \mathbf{a}'_{o_2 o_2} \end{pmatrix}$ 이고, $B_2 = \begin{pmatrix} b'_{11} & b'_{12} & \cdots & b'_{1o_2} \\ b'_{21} & b'_{22} & \cdots & b'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ b'_{o_2 1} & b'_{o_2 2} & \cdots & b'_{o_2 o_2} \end{pmatrix}$ 이다.

[0212] 여기서, $M_{OV,2}$는 크기(v)를 갖는 열 벡터(a'_{ij})를 원소로 하는 블록 순환 행렬이고, B_2는 블록 순환 행렬이다.

[0213] 벡터들의 블록 순환 행렬($M_{OV,2}$)과 블록 순환 행렬 B_2은 수학식 22과 같다.

[0214] [수학식 22]

$$M_{OV,2}=\begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1o_2} \\ a'_{21} & a'_{22} & \cdots & a'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ a'_{o_21} & a'_{o_22} & \cdots & a'_{o_2o_2} \end{pmatrix}=\begin{pmatrix} p'_1 & p'_2 & \cdots & p'_{k_2} & q'_1 & q'_2 & \cdots & q'_{k_2} \\ p'_{k_2} & p'_1 & \cdots & p'_{k_2-1} & q'_{k_2} & q'_1 & \cdots & q'_{k_2-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p'_2 & p'_3 & \cdots & p'_1 & q'_2 & q'_3 & \cdots & q'_1 \\ r'_1 & r'_2 & \cdots & r'_{k_2} & s'_1 & s'_2 & \cdots & s'_{k_2} \\ r'_{k_2} & r'_1 & \cdots & r'_{k_2-1} & s'_{k_2} & s'_1 & \cdots & s'_{k_2-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ r'_2 & r'_3 & \cdots & r'_1 & s'_2 & s'_3 & \cdots & s'_1 \end{pmatrix}=\begin{pmatrix} P_2 & Q_2 \\ R_2 & S_2 \end{pmatrix}$$

$$B_2=\begin{pmatrix} b'_{11} & b'_{12} & \cdots & b'_{1o_2} \\ b'_{21} & b'_{22} & \cdots & b'_{2o_2} \\ \vdots & \vdots & \ddots & \vdots \\ b'_{o_21} & b'_{o_22} & \cdots & b'_{o_2o_2} \end{pmatrix}=\begin{pmatrix} t'_1 & t'_2 & \cdots & t'_{k_2} & u'_1 & u'_2 & \cdots & u'_{k_2} \\ t'_k & t'_1 & \cdots & t'_{k_2-1} & u'_k & u'_1 & \cdots & u'_{k_2-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t'_2 & t'_3 & \cdots & t'_1 & u'_2 & u'_3 & \cdots & u'_1 \\ v'_1 & v'_2 & \cdots & v'_{k_2} & w'_1 & w'_2 & \cdots & w'_{k_2} \\ v'_k & v'_1 & \cdots & v'_{k_2-1} & w'_k & w'_1 & \cdots & w'_{k_2-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ v'_2 & v'_3 & \cdots & v'_1 & w'_2 & w'_3 & \cdots & w'_1 \end{pmatrix}$$

[0215]

[0216] 여기서, $p_i^{'}$, $q_i^{'}$, $r_i^{'}$, 와 $s_i^{'}$ 는 각각 크기($\mathcal{V}$)를 가지는 열 벡터들이고, P_2, Q_2, R_2, S_2 각각은 벡터들의 순환 행렬이고, $M_{OV,2}$ 은 벡터들의 블록 순환 행렬이다.

[0217] 마지막으로, 상수항(δ_i)은 유한체($\mathbb{F}_q$)에서 랜덤하게 선택된다.

[0219] 3. 공개키($\mathcal{P}=S\circ\mathcal{F}\circ T$)가 계산된다(S230).

[0220] **서명 생성 알고리즘**

[0221] 서명 생성기(220)는 서명 생성 알고리즘, 즉 본 발명에 따른 새로운 센트럴 맵을 역변환하는 방법을 수행하기 위해 단계들(S240 내지 S260)을 수행한다. 서명 생성기(220)는 아핀 맵들($\tilde{S}$와 $\tilde{T}$), 비밀 센트럴 맵($\mathcal{F}$), 및 메시지(m)을 수신한다.

[0223] 1. 메시지(m)에 대해 해시 메시지(H(m))가 계산된다(S240).

[0224] 여기서, $H:\{0,1\}^*\rightarrow\mathbb{F}_q^m$ 는 충돌 방지 해시 함수(collision resistant hash function)이다.

[0226] 2. $\tilde{S}(H(\mathrm{m}))=\xi=(\xi_1,\cdots,\xi_m)\in\mathbb{F}_q^m$ 을 계산한다(S240). 랜덤 행렬 (R), 즉 순환 행렬이 주어지면(또는 제공되면), 3-2에서 설명한 바와 같이, $\tilde{S}(H(m))$ 는 수학식 10에 따라 계산된다.

[0228] 3. $\xi=(\xi_1,\cdots,\xi_m)$ 가 주어질 때, $\mathcal{F}^{-1}(\xi)=\mathbf{s}$, 즉 $\mathcal{F}(\mathbf{x})=\xi$ 의 해 (solutions) $\mathbf{s}=(s_1,\cdots,s_n)$ 를 찾는 과정들은 아래와 같다(S250).

[0229] 제1 레이어에서,

[0230] 랜덤 벡터, $\mathbf{s_v} = (s_1, \cdots, s_v) \in \mathbb{F}_q^v$ 가 랜덤하게 선택된다.

[0231] 벡터($\mathbf{s_v}$)를 $i = 1, \cdots, o_1$ 에 대한 제1레이어($\mathcal{F}_V^{(i)}$)에 대입(plug)하여 $v \times v$순환 행렬의 $o_1 \times v$ 부분 행렬과 벡터 $(L_1(s_v), \cdots, L_v(s_v))$ 의 전치 행렬의 곱을 계산하고 그 결과로서 $(c_1, \cdots, c_{o_1})$ 을 얻는다. 이때, 벡터($\mathbf{s_v}$)를 대입한 $o_1 \times v$ 부분 행렬은 M_V^1 이다.

[0232] 벡터($\mathbf{s_v}$)를 $i = 1, \cdots, o_1$ 에 대한 $\mathcal{F}_{OV}^{(i)}$에 대입하여 o_1 개의 변수들을 갖는 o_1 개의 방정식들의 일차 방정식들의 시스템을 얻는다. 이때, 일차 방정식들의 시스템의 계수 행렬은 블록 순환 행렬(BC_1)이 된다.

[0233] 여기서, 블록 순환 행렬(BC_1)은 벡터($\mathbf{s_v}$)를 수학식 16의 $\mathbf{v}^T$로 구성된 행렬에 대입해서 얻어진 행렬에 $M_{OV,1}$를 곱해서 얻어진 행렬이다.

[0234] 앞에서 설명한 2-2에서 정의한 방법으로 구한 역행렬(BC_1^{-1})을 $(\xi_1 - c_1 - \delta_1, \cdots, \xi_{o_1} - c_{o_1} - \delta_{o_1})$ 의 전치 행렬에 곱하여 해 ($s_{v+1}, \cdots, s_{v+o_1}$)를 구한다.

[0235] 제2 레이어에서,

[0236] 벡터 $s_{v+o_1} = (s_1, \cdots, s_{v+o_1})$ 를 $i = o_1 + 1, \cdots, m$ 에 대한 제2레이어($\mathcal{F}_V^{(i)}$)에 대입하여, $(v + o_1) \times (v + o_1)$ 순환 행렬의 $o_2 \times (v + o_1)$ 부분 행렬과 벡터 ($(L_1'(s_{v+o_1}), \cdots, L_{v+o_1}'(s_{v+o_1}))$)의 전치 행렬의 곱을 계산하여 $(c_{o_1+1}, \cdots, c_m)$ 를 얻는다.

[0237] 이때, 벡터(s_{v+o_1})를 대입한 $o_2 \times (v + o_1)$ 부분 행렬은 M_V^2 이다.

[0238] 벡터($\mathbf{s}_{v+o_1}$)를 $i = o_1 + 1, \cdots, m$ 에 대한 $\mathcal{F}_{OV}^{(i)}$에 대입하여, o_2 개의 변수들을 갖는 o_2 개의 방정식들의 일차방정식의 시스템을 구한다. 이때, 일차 방정식들의 시스템의 계수 행렬은 블록 순환 행렬 (BC_2)이 된다.

[0239] 여기서, 블록 순환 행렬(BC_2)은 벡터(S_{v+o_1})를 수학식 21의 $\mathbf{v}^T$로 구성된 행렬에 대입해서 얻어진 행렬에 $M_{OV,2}$를 곱해서 얻어진 행렬이다.

[0240] 앞에서 설명한 2-2에서 정의한 방법으로 구한 역행렬(BC_2^{-1})을 $(\xi_{o_1+1} - c_{o_1+1} - \delta_{o_1+1}, \cdots, \xi_m - c_m - \delta_m)$ 의 전치 행렬에 곱해 해($(s_{v+o_1+1}, \cdots, s_{v+m})$)를 구한다. 그러면, 벡터 $\mathbf{s} = (s_1, \cdots, s_n)$ 는 $\mathcal{F}(\mathbf{x}) = \xi$의 해이다.

[0241] 만약, 블록 순환 행렬(BC_1)의 역행렬(BC_1^{-1})이 존재하지 않거나 블록 순환 행렬(BC_2)의 역행렬(BC_2^{-1})이 존재하지 않으면, 전자 서명 알고리즘의 처음으로 돌아가 새로운 랜덤 값들의 벡터($\mathbf{s_v}' = (s_1', \cdots, s_v')$)를 선택하여 앞에서 설명한 방법들(또는 과정들)을 다시 수행한다.

[0243] 4. $\widetilde{T}(\mathbf{s}) = \sigma$가 계산된다(S260). σ는 메시지(m)의 서명(여기서, 서명은 디지털 서명 또는 전자 서명)이다.

[0245] **서명 검증 또는 검증 단계:**

[0246] 서명 검증기(230)는 메시지(m), 서명(σ), 및 공개키($\mathcal{P}$)를 수신하고, 즉 메시지(m)에 대한 서명(σ)과 공개키($\mathcal{P}$)가 주어지면, $P(\sigma)=H(m)$ 인지가 확인한다(S270). $P(\sigma)=H(m)$ 이면 서명(σ)이 수락되고, 그렇지 않으면 서명(σ)은 거절된다.

[0247] 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

[0248] 100, 200: 전자 서명기

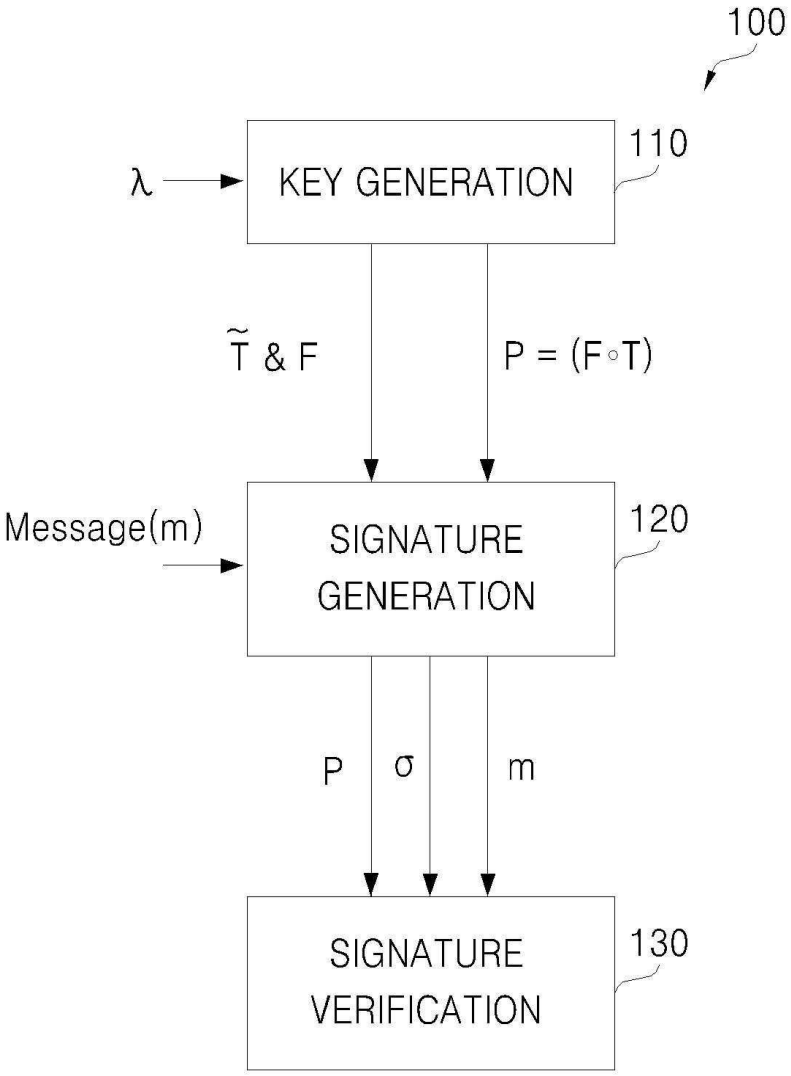
110, 210: 키 생성기

120, 220: 서명 생성기

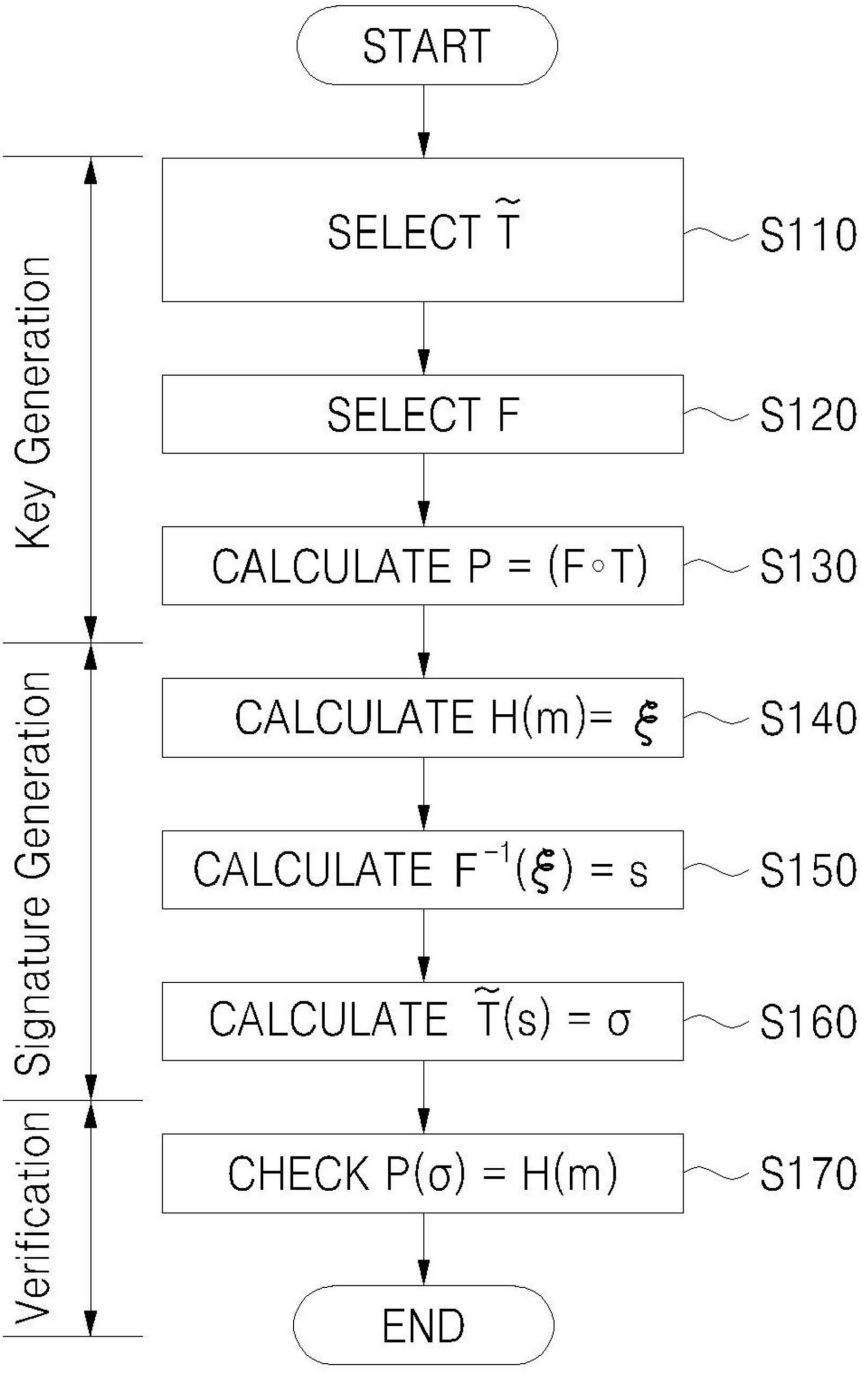
130, 230: 서명 검증기

도면

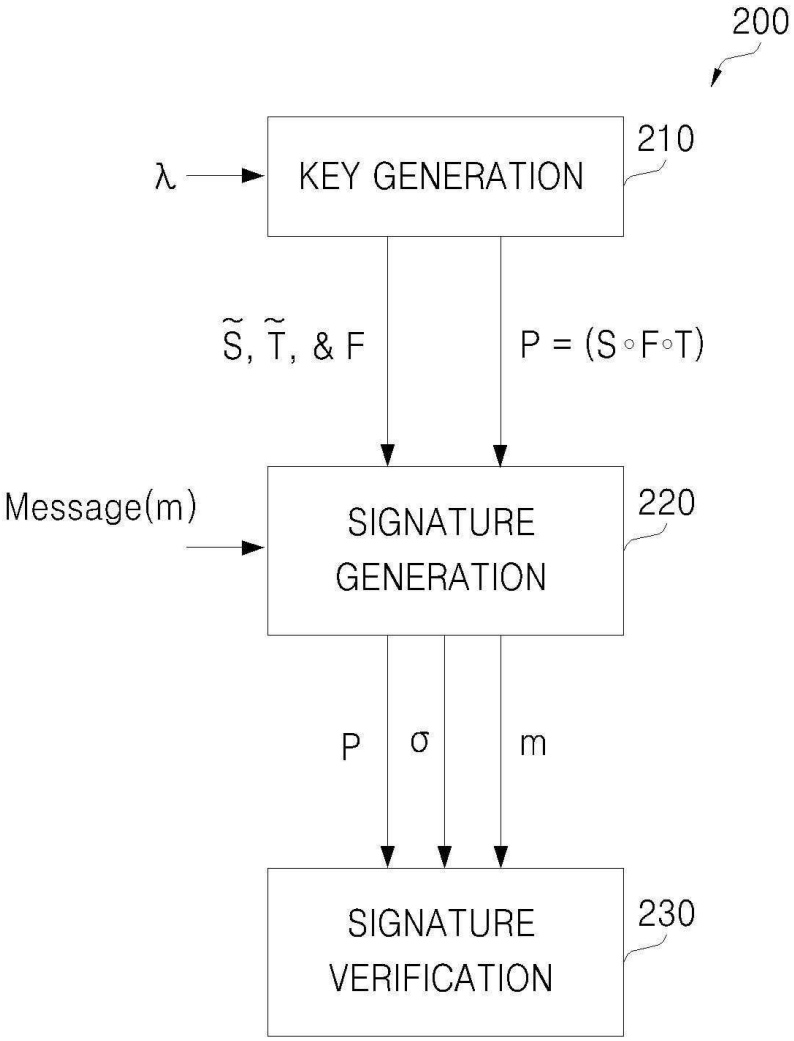
도면1


100
λ
KEY GENERATION
110
T̃ & F
P = (F∘T)
Message(m)
SIGNATURE GENERATION
120
P
σ
m
SIGNATURE VERIFICATION
130

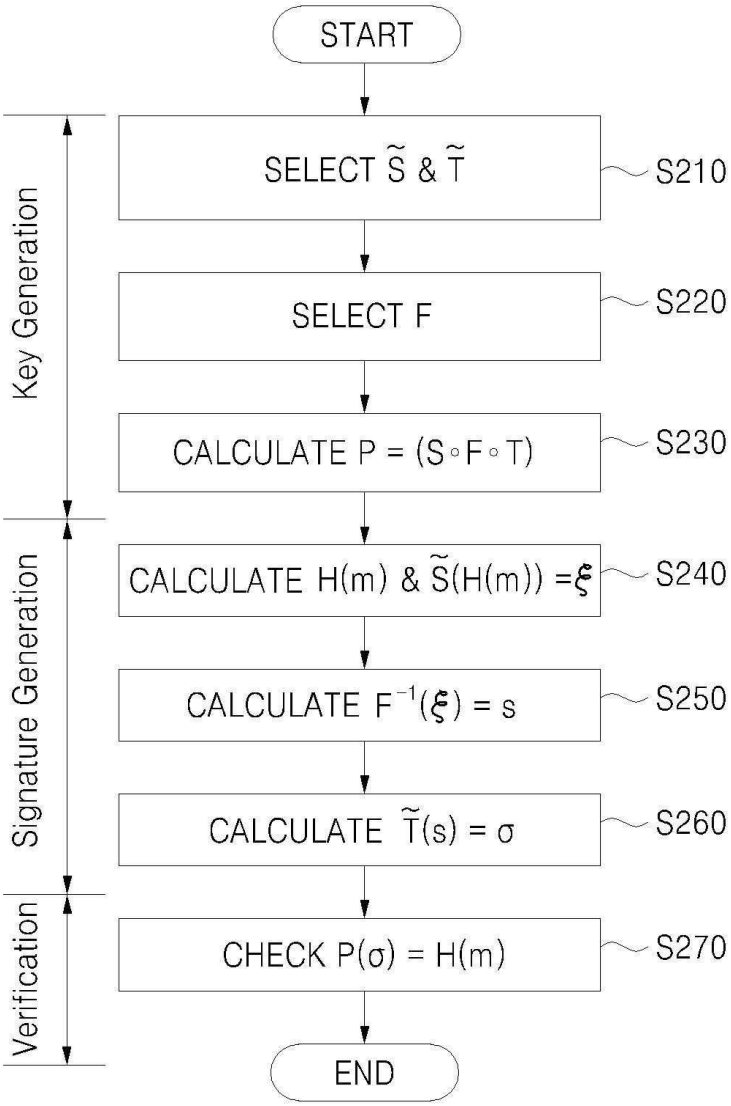
도면2


START
SELECT $\tilde{T}$
S110
SELECT F
S120
CALCULATE P = (F∘T)
S130
CALCULATE H(m)= ξ
S140
CALCULATE $F^{-1}(\xi)$ = s
S150
CALCULATE $\tilde{T}$(s) = σ
S160
CHECK P(σ) = H(m)
S170
END
Key Generation
Signature Generation
Verification

도면3


200
λ
KEY GENERATION
210
S̃, T̃, & F
P = (S∘F∘T)
Message(m)
SIGNATURE GENERATION
220
P
σ
m
SIGNATURE VERIFICATION
230

도면4


START
SELECT $\widetilde{S}$ & $\widetilde{T}$
S210
SELECT F
S220
CALCULATE P = (S∘F∘T)
S230
CALCULATE H(m) & $\widetilde{S}$(H(m)) =ξ
S240
CALCULATE F^{-1}(ξ) = s
S250
CALCULATE $\widetilde{T}$(s) = σ
S260
CHECK P(σ) = H(m)
S270
END
Key Generation
Signature Generation
Verification