(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0068163
(43) 공개일자 2025년05월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3263 (2013.01)
H04L 9/0825 (2013.01)
(21) 출원번호 10-2023-0154311
(22) 출원일자 2023년11월09일
심사청구일자 2023년11월09일

(71) 출원인
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
이광수
서울특별시 광진구 능동로 209 세종대학교 대양AI센터 726호
(74) 대리인
특허법인린

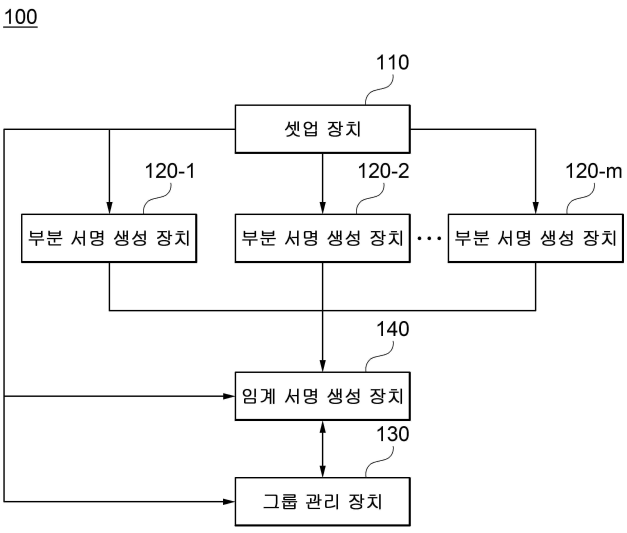
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **효율적인 가중치를 지원하는 분산화된 비상호적 임계 서명 방법 및 장치**

(57) 요 약

효율적인 가중치를 지원하는 분산화된 비상호적 임계 서명 방법 및 장치가 개시된다. 개시되는 실시예들에 따르면, 별도의 신뢰 기관 없이 각 사용자가 자신의 사용자 공개키 및 사용자 비밀키를 스스로 생성하되, 사용자 공개키 및 사용자 비밀키를 생성과 사용자 그룹 설정 과정에서 사용자 사이의 어떠한 상호작용도 요구하지 않으므로 비상호적이고 탈중앙화된 임계 서명을 가능케 하며, 이를 통해 사용자 공개키, 사용자 비밀키 및 사용자 그룹 설정을 위해 요구되는 통신량과 연산량을 줄일 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3218 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711194271
과제번호	2021-0-00518-003
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	데이터경제를위한블록체인기술개발사업
연구과제명	블록체인 데이터 암호화 기반의 프라이버시 보호 기술개발
기 여 율	1/1
과제수행기관명	한양대학교산학협력단
연구기간	2023.01.01 ~ 2023.12.31

명 세 서

청구범위

청구항 1

하나 이상의 프로세서를 포함하는 컴퓨팅 장치에 의해 수행되는 방법으로서,

사용자 그룹에 참여한 복수의 사용자 각각의 사용자 공개키 및 등록키를 검증하는 단계;

라그랑주 보간법(Lagrange interpolation)을 이용하여 상기 복수의 사용자 각각의 사용자 인덱스 및 사용자 가중치에 기초한 가중치 기반 인덱스에 대응하는 n(이때, n은 상기 복수의 사용자 각각의 사용자 가중치의 총합)개의 포인트를 지나고 차수가 n-1인 다항식을 정의하는 단계;

상기 다항식에 대한 라그랑주 기저 다항식(Lagrange basis polynomial)을 이용하여, 상기 n개의 포인트를 제외한 상기 다항식 상의 n-t(이때, t는 t≤n인 사전 설정된 양의 정수)개의 포인트 및 상기 다항식의 y절편 각각에 대한 라그랑주 계수(Lagrange coefficient)를 산출하는 단계;

상기 n-t개의 포인트 각각에 대한 라그랑주 계수, 상기 복수의 사용자 각각의 사용자 공개키 및 등록키를 이용하여, 상기 복수의 사용자 중 상기 사용자 가중치의 합이 t 이상인 하나 이상의 사용자가 각각 자신의 사용자 비밀키를 이용하여 생성한 부분 서명으로부터 임계 서명을 생성하기 위한 결합키를 생성하는 단계; 및

상기 y절편에 대한 라그랑주 계수, 상기 하나 이상의 사용자 각각의 사용자 공개키 및 상기 사용자 그룹의 그룹 식별자를 이용하여 상기 임계 서명에 대한 검증키를 생성하는 단계를 포함하는, 방법.

청구항 2

청구항 1에 있어서,

상기 복수의 사용자 중 상기 사용자 인덱스가 i(이때, i는 1≤i≤m인 정수, m은 상기 복수의 사용자의 총 수이고, 2≤m≤n를 만족함)인 사용자 P_i의 공개키는, 상기 사용자 P_i의 사용자 비밀키를 이용하여 생성되고,

상기 사용자 P_i의 등록키 RK_i는, 상기 그룹 식별자, 상기 사용자 P_i의 사용자 비밀키를 이용하여 생성된 상기 그룹 식별자에 대한 서명 및 상기 사용자 P_i의 사용자 비밀키에 대한 영지식 증명(zero knowledge proof)을 위한 증명 값을 포함하는, 방법.

청구항 3

청구항 2에 있어서,

상기 사용자 P_i의 공개키는, 아래의 수학식 1

[수학식 1]

$$X_i = g^{s_i}$$

(이때, X_i는 상기 사용자 P_i의 사용자 공개키, g는 위수(order)가 소수 p인 순환 군(cyclic group) $\mathbb{G}$의 생성원(generator), s_i는 $s_i \in \mathbb{Z}_p^*$를 만족하는 상기 사용자 P_i의 사용자 비밀키, $\mathbb{Z}_p^*$는 사전 정의된 정수 집합)

을 만족하고,

상기 그룹 식별자에 대한 서명은, 아래의 수학식 2

[수학식 2]

$$Y_i = H_0(GID)^{s_i}$$

(이때, GID는 상기 그룹 식별자, Y_i는 상기 그룹 식별자에 대한 서명, H_0는 $H_0: \{0,1\}^* \rightarrow \hat{\mathbb{G}}$ 를 만족하는 해시 함수, $\hat{\mathbb{G}}$ 는 위수가 소수 p인 순환 군)

를 만족하고,

$\mathbb{G}$ $\hat{\mathbb{G}}$

p, g, H_0, 및 는 공개 파라미터인, 방법.

청구항 4

청구항 3에 있어서,

상기 증명 값은 제1 증명 요소 및 제2 증명 요소를 포함하고,

상기 제1 증명 요소는, 아래의 수학식 3

[수학식 3]

$$R_i = g^{r_i}$$

(이때, R_i는 상기 제1 증명 요소, r_i은 $r_i \in \mathbb{Z}_p$ 를 만족하는 임의의 정수, $\mathbb{Z}_p$ 는 사전 정의된 정수 집합)

을 만족하고,

상기 제2 증명 요소는, 아래의 수학식 4

[수학식 4]

$$z_i = r_i + s_i \cdot H_z(g, X_i, R_i)$$

$$H_z: \mathbb{G}^3 \rightarrow \mathbb{Z}_p$$

(이때, z_i는 상기 제2 증명 요소, H_z는 를 만족하는 해시 함수)

를 만족하고,

상기 공개 파라미터는 H_z를 더 포함하는, 방법.

청구항 5

청구항 4에 있어서,

상기 검증하는 단계는,

상기 등록키에 포함된 그룹 식별자와 상기 사용자 그룹의 그룹 식별자가 일치하고 아래의 수학식 5

[수학식 5]

$$e(g, Y_i) = e\left(X_i, H_0(GID)\right)$$

(이때, e는 각각 위수가 소수 p인 순환 군 $\mathbb{G}$, $\hat{\mathbb{G}}$ 및 $\mathbb{G}_T$에 대해 $e: \mathbb{G} \times \hat{\mathbb{G}} \rightarrow \mathbb{G}_T$를 만족하는 페어링(pairing) 함수)

가 만족되는지 여부를 판단하는 단계;

아래의 수학식 6

[수학식 6]

$$h = H_z(g, X_i, R_i)$$

을 이용하여 h를 산출하는 단계; 및

아래의 수학식 7

[수학식 7]

$$g^{z_i} = R_i \cdot (X_i)^h$$

이 만족되는지 여부를 판단하는 단계를 포함하고,

상기 공개 파라미터는 e 및 $\mathbb{G}_T$를 더 포함하는, 방법.

청구항 6

청구항 3에 있어서,

상기 다항식은, 아래의 수학식 8

[수학식 8]

$$f(x) = \sum_{j \in [n]} f(j) \cdot L_j(x) = \sum_{j \in [n]} s_{\psi(j)} \cdot y_j \cdot L_j(x)$$

(이때, f(x)는 상기 다항식, j는 상기 가중치 기반 인덱스, ψ(j)는 $j \in [\bar{w}_{i-1} + 1 : \bar{w}_{i-1} + w_i]$인 각 j에 대해 $\bar{w}_i = \sum_{k=1}^{i} w_k$, ψ(j)=i인 j∈[n]에서 i∈[m]로의 사상(mapping), w_i는 상기 사용자 P_i의 사용자 가중치, , L_j(x)는 라그랑주 기저 다항식(Lagrange basis polynomial))

을 만족하고,

y_j는, 아래의 수학식 9

[수학식 9]

$y_j = H_2(GD \| j)$

(이때, GD는 상기 사용자 그룹에 대한 그룹 기술(group description) 정보로서

$$GD = (GID, \{PK_i, RK_i, P_i, w_i\}_{i=1}^{m}, n, t)$$

)

를 만족하고,

$L_j(x)$는, 아래의 수학식 10

[수학식 10]

$$L_j(x) = \prod_{k \in [n], k \neq j} \frac{x-k}{j-k}$$

을 만족하는, 방법.

청구항 7

청구항 6에 있어서,

상기 결합키는, 상기 n-t개의 포인트 각각에 대한 제1 결합키 요소 및 제2 결합키 요소를 포함하고,

상기 결합키를 생성하는 단계는, $k \in [-(n-t):-1]$인 각 k에 대해,

아래의 수학식 11

[수학식 11]

$$V_k = \prod_{j \in [n]} X_{\psi(j)}^{H_2(GD \| j) \cdot L_j(k)}$$

(이때, V_k는 상기 제1 결합키 요소, $L_j(k)$는 상기 n-t개의 포인트 각각에 대한 라그랑주 계수)

을 이용하여 상기 제1 결합키 요소를 생성하고,

아래의 수학식 12

[수학식 12]

$$W_k = \prod_{j \in [n]} Y_{\psi(j)}^{H_2(GD \| j) \cdot L_j(k)}$$

(이때, W_k는 상기 제2 결합키 요소)

를 이용하여 상기 제2 결합키 요소를 생성하는, 방법.

청구항 8

청구항 6에 있어서,

상기 검증키는, 제1 검증키 요소 및 제2 검증키 요소를 포함하고,

상기 검증키를 생성하는 단계는, 아래의 수학식 13

[수학식 13]

$$V_0 = \prod_{j \in [n]} X_{\psi(j)}^{H_2(GD \| j) \cdot L_j(0)}$$

(이때, V_0는 상기 제1 검증키 요소, $L_j(0)$는 상기 y절편에 대한 라그랑주 계수)

을 이용하여 상기 제1 검증키 요소를 생성하고,

아래의 수학식 14

[수학식 14]

$$W = H_0(GID)$$

(이때, W는 상기 제2 검증키 요소)

를 이용하여 상기 제2 검증키 요소를 생성하는, 방법.

청구항 9

청구항 6에 있어서,

상기 복수의 사용자 중 적어도 일부 사용자 각각이 자신의 사용자 비밀키를 이용하여 메시지에 대해 생성한 부분 서명을 획득하는 단계;

상기 적어도 일부 사용자 각각의 사용자 공개키를 이용하여 상기 적어도 일부 사용자 각각의 부분 서명을 검증하고, 상기 적어도 일부 사용자 중 부분 서명이 검증된 각 사용자 및 상기 검증된 각 사용자의 사용자 가중치를 포함하는 집합 Q를 생성하는 단계;

상기 검증된 각 사용자의 사용자 가중치의 합이 t 이상인 경우, 상기 집합 Q에 포함된 각 사용자의 가중치 기반 인덱스 중 t개의 가중치 기반 인덱스에 기초하여 아래의 수학식 15

[수학식 15]

$$f(0) = \sum_{j \in X_Q \cup [-(n-t):-1]} f(j) \cdot L_j(0)$$

$\{L_j(0)\}_{j \in X_Q \cup [-(n-t):-1]}$

를 만족하는 라그랑주 계수 (이때, X_Q는 상기 집합 Q에 포함된 각 사용자의 가중치 기반 인덱스 중 t개의 가중치 기반 인덱스를 포함하는 집합)를 생성하는 단계;

$\{L_j(0)\}_{j \in X_Q \cup [-(n-t):-1]}$

상기 라그랑주 계수 , 상기 집합 Q에 포함된 각 사용자의 부분 서명 및 상기 결합키를 이용하여 상기 메시지에 대한 임계 서명을 생성하는 단계를 더 포함하는, 방법.

청구항 10

청구항 9에 있어서,

상기 임계 서명은, 제1 서명 요소, 제2 서명 요소 및 제3 서명 요소를 포함하고,

상기 임계 서명을 생성하는 단계는, 아래의 수학식 16

[수학식 16]

$$S_0 = \prod_{j \in X_Q} \sigma_i^{H_2(GD \| j) \cdot L_j(0)}$$

(이때, S_0는 상기 제1 서명 요소)

을 이용하여 상기 제1 서명 요소를 생성하고,

아래의 수학식 17

[수학식 17]

$$S_1 = \prod_{j \in [-(n-t):-1]} V_j^{L_j(0)}$$

(이때, S_1은 상기 제2 서명 요소)

을 이용하여 상기 제2 서명 요소를 생성하고,

아래의 수학식 18

[수학식 18]

$$S_2 = \prod_{j \in [-(n-t):-1]} W_j^{L_j(0)}$$

(이때, S_2는 상기 제3 서명 요소)

을 이용하여 상기 제3 서명 요소를 생성하는, 방법.

청구항 11

하나 이상의 프로세서; 및

상기 하나 이상의 프로세서에 의해 실행되는 하나 이상의 프로그램을 저장하는 메모리를 포함하고,

상기 하나 이상의 프로세서는,

사용자 그룹에 참여한 복수의 사용자 각각의 사용자 공개키 및 등록키를 검증하고,

라그랑주 보간법(Lagrange interpolation)을 이용하여 상기 복수의 사용자 각각의 사용자 인덱스 및 사용자 가중치에 기초한 가중치 기반 인덱스에 대응하는 n(이때, n은 상기 복수의 사용자 각각의 사용자 가중치의 총합)개의 포인트를 지나고 차수가 n-1인 다항식을 정의하고,

상기 다항식에 대한 라그랑주 기저 다항식(Lagrange basis polynomial)을 이용하여, 상기 n개의 포인트를 제외한 상기 다항식 상의 n-t(이때, t는 t≤n인 사전 설정된 양의 정수)개의 포인트 및 상기 다항식의 y절편 각각에 대한 라그랑주 계수(Lagrange coefficient)를 산출하고,

상기 n-t개의 포인트 각각에 대한 라그랑주 계수, 상기 복수의 사용자 각각의 사용자 공개키 및 등록키를 이용하여, 상기 복수의 사용자 중 상기 사용자 가중치의 합이 t 이상인 하나 이상의 사용자가 각각 자신의 사용자 비밀키를 이용하여 생성한 부분 서명으로부터 임계 서명을 생성하기 위한 결합키를 생성하고,

상기 y절편에 대한 라그랑주 계수, 상기 하나 이상의 사용자 각각의 사용자 공개키 및 상기 사용자 그룹의 그룹 식별자를 이용하여 상기 임계 서명에 대한 검증키를 생성하는, 장치.

청구항 12

청구항 11에 있어서,

상기 복수의 사용자 중 상기 사용자 인덱스가 i(이때, i는 1≤i≤m인 정수, m은 상기 복수의 사용자의 총 수이고, 2≤m≤n를 만족함)인 사용자 P_i의 공개키는, 상기 사용자 P_i의 사용자 비밀키를 이용하여 생성되고,

상기 사용자 P_i의 등록키 RK_i는, 상기 그룹 식별자, 상기 사용자 P_i의 사용자 비밀키를 이용하여 생성된 상기 그

룹 식별자에 대한 서명 및 상기 사용자 P_i의 사용자 비밀키에 대한 영지식 증명(zero knowledge proof)을 위한 증명 값을 포함하는, 장치.

청구항 13

청구항 12에 있어서,

상기 사용자 P_i의 공개키는, 아래의 수학식 1

[수학식 1]

$$X_i = g^{s_i}$$

(이때, X_i는 상기 사용자 P_i의 사용자 공개키, g는 위수(order)가 소수 p인 순환 군(cyclic group) $\mathbb{G}$ 의 생성원(generator), s_i는 $s_i \in \mathbb{Z}_p^*$ 를 만족하는 상기 사용자 P_i의 사용자 비밀키, $\mathbb{Z}_p^*$ 는 사전 정의된 정수 집합)

을 만족하고,

상기 그룹 식별자에 대한 서명은, 아래의 수학식 2

[수학식 2]

$$Y_i = H_0(GID)^{s_i}$$

(이때, GID는 상기 그룹 식별자, Y_i는 상기 그룹 식별자에 대한 서명, H_0는 $H_0: \{0,1\}^* \rightarrow \hat{\mathbb{G}}$ 를 만족하는 해시 함수, $\hat{\mathbb{G}}$ 는 위수가 소수 p인 순환 군)

를 만족하고,

p, g, H_0, $\mathbb{G}$ 및 $\hat{\mathbb{G}}$ 는 공개 파라미터인, 장치.

청구항 14

청구항 13에 있어서,

상기 증명 값은 제1 증명 요소 및 제2 증명 요소를 포함하고,

상기 제1 증명 요소는, 아래의 수학식 3

[수학식 3]

$$R_i = g^{r_i}$$

(이때, R_i는 상기 제1 증명 요소, r_i은 $r_i \in \mathbb{Z}_p$ 를 만족하는 임의의 정수, $\mathbb{Z}_p$ 는 사전 정의된 정수 집합)

을 만족하고,

상기 제2 증명 요소는, 아래의 수학식 4

[수학식 4]

$$z_i = r_i + s_i \cdot H_z(\mathrm{g}, X_i, R_i)$$

$$H_z: \mathbb{G}^3 \rightarrow \mathbb{Z}_p$$

(이때, z_i는 상기 제2 증명 요소, H_z는 를 만족하는 해시 함수)

를 만족하고,

상기 공개 파라미터는 H_z를 더 포함하는, 장치.

청구항 15

청구항 14에 있어서,

상기 하나 이상의 프로세서는,

상기 등록키에 포함된 그룹 식별자와 상기 사용자 그룹의 그룹 식별자가 일치하고 아래의 수학식 5

[수학식 5]

$$e(\mathrm{g}, Y_i) = e\left(X_i, H_0(GID)\right)$$

$\mathbb{G}$ $\hat{\mathbb{G}}$ $\mathbb{G}_T$ $e: \mathbb{G} \times \hat{\mathbb{G}} \rightarrow \mathbb{G}_T$

(이때, e는 각각 위수가 소수 p인 순환 군 , 및 에 대해 겹선형 사상(bilinear map) 를 만족하는 페어링(pairing) 함수)

가 만족되는지 여부를 판단하고,

아래의 수학식 6

[수학식 6]

$$h = H_z(\mathrm{g}, X_i, R_i)$$

을 이용하여 h를 산출하고,

아래의 수학식 7

[수학식 7]

$$\mathrm{g}^{z_i} = R_i \cdot (X_i)^h$$

이 만족되는지 여부를 판단하고,

$\mathbb{G}_T$

상기 공개 파라미터는 e 및 를 더 포함하는, 장치.

청구항 16

청구항 13에 있어서,

상기 다항식은, 아래의 수학식 8

[수학식 8]

$$f(x) = \sum_{j\in[n]} f(j)\cdot L_j(x) = \sum_{j\in[n]} s_{\psi(j)}\cdot y_j \cdot L_j(x)$$

(이때, f(x)는 상기 다항식, j는 상기 가중치 기반 인덱스, ψ(j)는 $j \in [\bar{w}_{i-1}+1:\bar{w}_{i-1}+w_i]$ 인 각 j에 대해 $\bar{w}_i = \sum_{k=1}^{i} w_k$ ψ(j)=i인 j∈[n]에서 i∈[m]로의 사상(mapping), w_i는 상기 사용자 P_i의 사용자 가중치, , L_j(x)는 라그랑주 기저 다항식(Lagrange basis polynomial))

을 만족하고,

y_j는, 아래의 수학식 9

[수학식 9]

$y_j=H_2(GD \| j)$

(이때, GD는 상기 사용자 그룹에 대한 그룹 기술(group description) 정보로서 $GD = (GID, \{PK_i, RK_i, P_i, w_i\}_{i=1}^{m}, n, t)$)

를 만족하고,

$L_j(x)$는, 아래의 수학식 10

[수학식 10]

$$L_j(x) = \prod_{k\in[n],k\neq j} \frac{x-k}{j-k}$$

을 만족하는, 장치.

청구항 17

청구항 16에 있어서,

상기 결합키는, 상기 n-t개의 포인트 각각에 대한 제1 결합키 요소 및 제2 결합키 요소를 포함하고,

상기 하나 이상의 프로세서는, k∈[-(n-t):-1]인 각 k에 대해,

아래의 수학식 11

[수학식 11]

$$V_k = \prod_{j\in[n]} X_{\psi(j)}^{H_2(GD\|j)\cdot L_j(k)}$$

(이때, V_k는 상기 제1 결합키 요소, $L_j(k)$는 상기 n-t개의 포인트 각각에 대한 라그랑주 계수)

을 이용하여 상기 제1 결합키 요소를 생성하고,

아래의 수학식 12

[수학식 12]

$$W_k = \prod_{j\in[n]} Y_{\psi(j)}^{H_2(GD\|j)\cdot L_j(k)}$$

(이때, W_k는 상기 제2 결합키 요소)

를 이용하여 상기 제2 결합키 요소를 생성하는, 장치.

청구항 18

청구항 16에 있어서,

상기 검증키는, 제1 검증키 요소 및 제2 검증키 요소를 포함하고,

상기 하나 이상의 프로세서는, 아래의 수학식 13

[수학식 13]

$$V_0 = \prod_{j\in[n]} X_{\psi(j)}^{H_2(GD\|j)\cdot L_j(0)}$$

(이때, V_0는 상기 제1 검증키 요소, $L_j(0)$는 상기 y절편에 대한 라그랑주 계수)

을 이용하여 상기 제1 검증키 요소를 생성하고,

아래의 수학식 14

[수학식 14]

$$W = H_0(GID)$$

(이때, W는 상기 제2 검증키 요소)

를 이용하여 상기 제2 검증키 요소를 생성하는, 장치.

청구항 19

청구항 16에 있어서,

상기 하나 이상의 프로세서는,

상기 복수의 사용자 중 적어도 일부 사용자 각각이 자신의 사용자 비밀키를 이용하여 메시지에 대해 생성한 부분 서명을 획득하고,

상기 적어도 일부 사용자 각각의 사용자 공개키를 이용하여 상기 적어도 일부 사용자 각각의 부분 서명을 검증하고, 상기 적어도 일부 사용자 중 부분 서명이 검증된 각 사용자 및 상기 검증된 각 사용자의 사용자 가중치를 포함하는 집합 Q를 생성하고,

상기 검증된 각 사용자의 사용자 가중치의 합이 t 이상인 경우, 상기 집합 Q에 포함된 각 사용자의 가중치 기반 인덱스 중 t개의 가중치 기반 인덱스에 기초하여 아래의 수학식 15

[수학식 15]

$$f(0) = \sum_{j\in X_Q \cup [-(n-t):-1]} f(j)\cdot L_j(0)$$

$\{L_j(0)\}_{j\in X_Q\cup[-(n-t):-1]}$

를 만족하는 라그랑주 계수 (이때, X_Q는 상기 집합 Q에 포함된 각 사용자의 가중치 기반 인덱스 중 t개의 가중치 기반 인덱스를 포함하는 집합)를 생성하고,

$\{L_j(0)\}_{j\in X_Q\cup[-(n-t):-1]}$

상기 라그랑주 계수 , 상기 집합 Q에 포함된 각 사용자의 부분 서명 및 상기 결합키를 이용하여 상기 메시지에 대한 임계 서명을 생성하는, 장치.

청구항 20

청구항 19에 있어서,

상기 임계 서명은, 제1 서명 요소, 제2 서명 요소 및 제3 서명 요소를 포함하고,

상기 하나 이상의 프로세서는, 아래의 수학식 16

[수학식 16]

$$S_0 = \prod_{j\in X_Q} \sigma_i^{H_2(GD\|j)\cdot L_j(0)}$$

(이때, S_0는 상기 제1 서명 요소)

을 이용하여 상기 제1 서명 요소를 생성하고,

아래의 수학식 17

[수학식 17]

$$S_1 = \prod_{j\in[-(n-t):-1]} V_j^{L_j(0)}$$

(이때, S_1은 상기 제2 서명 요소)

을 이용하여 상기 제2 서명 요소를 생성하고,

아래의 수학식 18

[수학식 18]

$$S_2 = \prod_{j\in[-(n-t):-1]} W_j^{L_j(0)}$$

(이때, S_2는 상기 제3 서명 요소)

을 이용하여 상기 제3 서명 요소를 생성하는, 장치.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 전자 서명 기술과 관련된다.

배 경 기 술

[0002] 임계 서명 기법은 시스템에 포함된 여러 사용자들이 각각의 비밀키를 소유하고 있고, 각각의 비밀키로 서명을

생성할 수 있도록 하는 서명 기법이다. 임계 서명 기법에서는 임계치보다 많은 수의 (정당하게 생성된)서명을 가지고 있어야 검증 알고리즘을 통과할 수 있다. 이러한 임계 서명 기법은 블록체인 또는 전자 서명 프리미티브(primitive)에서 권한을 분산시킬 때 사용할 수 있다. 그러나 실제 블록체인 환경에서 모두가 동일한 사용자 그룹에 포함된 임계 서명을 사용하는 것은 단순하지 않다. 다양한 사용자들이 같은 응용환경을 이용하려면 각기 다른 임계치를 가지는 각자의 사용자 그룹이 존재하고, 각각의 사용자 그룹에 속하는 서명자의 서명을 결합하여 한 번에 검증할 수 있어야 한다. 기존에 알려진 방식으로 다중 사용자 그룹을 지원하는 임계 서명 기법을 설계하는 접근 방식은 여러 가지가 존재한다.

[0003] 첫 번째는 단순하게 기존의 임계 서명 기법들을 여러 개 붙이는 방식이다. 결합은 쉬워 보이지만, 사용자 그룹이 많아질수록 파라미터의 크기 및 서명의 크기, 그리고 연산의 비용이 증가하기 때문에 효율적으로 사용하기 어렵다.

[0004] 두 번째 방식은 SNARK (Succinct non-interactive argument of knowledge)를 이용하는 방식이다. 부분 서명을 결합하는 사람이 SNARK의 특성을 이용한다면 결합에 사용된 서명의 수를 숨긴 채로 올바른 서명이라는 것을 증명할 수 있다. 그러나 이 방식은 검증하는 방식에서 너무 많은 연산이 필요하다.

[0005] 세 번째 방식은 다중 서명을 이용하는 방식이다. 다중 서명을 이용하는 방식에서 각 사용자 그룹에 포함된 사용자들은 사용자 그룹의 공개키와 비밀키를 자신의 공개키 및 비밀키로 갖는다. 올바르게 검증되는 서명을 결합하려면 모든 사용자 그룹의 서명이 하나 이상씩 필요하게 된다는 점이 있다. 최초 설정 단계가 따로 필요 없다는 점이나 결합하는 사람의 연산량이 임계치와 상관없다는 점도 있지만 전체적인 연산효율이 매우 비효율적이다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 등록특허 제10-2439195호 (2022.08.31. 공고)

발명의 내용

해결하려는 과제

[0007] 본 발명의 실시예들은 효율적인 가중치를 지원하는 분산화된 비상호적인 임계 서명 방법 및 장치를 제공하기 위한 것이다.

과제의 해결 수단

[0008] 일 실시예에 따른 방법은, 사용자 그룹에 참여한 복수의 사용자 각각의 사용자 공개키 및 등록키를 검증하는 단계; 라그랑주 보간법(Lagrange interpolation)을 이용하여 상기 복수의 사용자 각각의 사용자 인덱스 및 사용자 가중치에 기초한 가중치 기반 인덱스에 대응하는 n(이때, n은 상기 복수의 사용자 각각의 사용자 가중치의 총합)개의 포인트를 지나고 차수가 n-1인 다항식을 정의하는 단계; 상기 다항식에 대한 라그랑주 기저 다항식(Lagrange basis polynomial)을 이용하여, 상기 n개의 포인트를 제외한 상기 다항식 상의 n-t(이때, t는 t≤n인 사전 설정된 양의 정수)개의 포인트 및 상기 다항식의 y절편 각각에 대한 라그랑주 계수(Lagrange coefficient)를 산출하는 단계; 상기 n-t개의 포인트 각각에 대한 라그랑주 계수, 상기 복수의 사용자 각각의 사용자 공개키 및 등록키를 이용하여, 상기 복수의 사용자 중 상기 사용자 가중치의 합이 t 이상인 하나 이상의 사용자가 각각 자신의 사용자 비밀키를 이용하여 생성한 부분 서명으로부터 임계 서명을 생성하기 위한 결합키를 생성하는 단계; 및 상기 y절편에 대한 라그랑주 계수, 상기 하나 이상의 사용자 각각의 사용자 공개키 및 상기 사용자 그룹의 그룹 식별자를 이용하여 상기 임계 서명에 대한 검증키를 생성하는 단계를 포함한다.

[0009] 상기 복수의 사용자 중 상기 사용자 인덱스가 i(이때, i는 $1 \leq i \leq m$인 정수, m은 상기 복수의 사용자의 총 수이고, $2 \leq m \leq n$를 만족함)인 사용자 P_i의 공개키는, 상기 사용자 P_i의 사용자 비밀키를 이용하여 생성되고, 상기 사용자 P_i의 등록키 RK_i는, 상기 그룹 식별자, 상기 사용자 P_i의 사용자 비밀키를 이용하여 생성된 상기 그룹 식별자에 대한 서명 및 상기 사용자 P_i의 사용자 비밀키에 대한 영지식 증명(zero knowledge proof)을 위한 증명 값

을 포함할 수 있다.

[0010] 상기 사용자 P_i의 공개키는, 아래의 수학식 1

[0011] [수학식 1]

$$X_i = g^{s_i}$$

[0012]

[0013] (이때, X_i는 상기 사용자 P_i의 사용자 공개키, g는 위수(order)가 소수 p인 순환 군(cyclic group) $\mathbb{G}$의 생성원(generator), s_i는 $s_i \in \mathbb{Z}_p^*$를 만족하는 상기 사용자 P_i의 사용자 비밀키, $\mathbb{Z}_p^*$는 사전 정의된 정수 집합)을 만족하고, 상기 그룹 식별자에 대한 서명은, 아래의 수학식 2

[0014] [수학식 2]

$$Y_i = H_0(GID)^{s_i}$$

[0015]

[0016] (이때, GID는 상기 그룹 식별자, Y_i는 상기 그룹 식별자에 대한 서명, H_0는 $H_0: \{0,1\}^* \rightarrow \hat{\mathbb{G}}$를 만족하는 해시 함수, $\hat{\mathbb{G}}$는 $\mathbb{G}$와 $\hat{\mathbb{G}}$는 위수가 소수 p인 순환 군)를 만족하고, p, g, H_0, $\mathbb{G}$ 및 $\hat{\mathbb{G}}$는 공개 파라미터일 수 있다.

[0017] 상기 증명 값은 제1 증명 요소 및 제2 증명 요소를 포함하고, 상기 제1 증명 요소는, 아래의 수학식 3

[0018] [수학식 3]

$$R_i = g^{r_i}$$

[0019]

[0020] (이때, R_i는 상기 제1 증명 요소, r_i은 $r_i \in \mathbb{Z}_p$를 만족하는 임의의 정수, $\mathbb{Z}_p$는 사전 정의된 정수 집합)을 만족하고, 상기 제2 증명 요소는, 아래의 수학식 4

[0021] [수학식 4]

$$z_i = r_i + s_i \cdot H_z(g, X_i, R_i)$$

[0022]

[0023] (이때, z_i는 상기 제2 증명 요소, H_z는 $H_z: \mathbb{G}^3 \rightarrow \mathbb{Z}_p$를 만족하는 해시 함수)

[0024] 를 만족하고, 상기 공개 파라미터는 H_z를 더 포함할 수 있다.

[0025] 상기 검증하는 단계는, 상기 등록키에 포함된 그룹 식별자와 상기 사용자 그룹의 그룹 식별자가 일치하고 아래의 수학식 5

[0026] [수학식 5]

$$e(g, Y_i) = e\left(X_i, H_0(GID)\right)$$

[0027]

[0028] (이때, e는 각각 위수가 소수 p인 순환 군 $\mathbb{G}$, $\hat{\mathbb{G}}$ 및 $\mathbb{G}_T$에 대해 겹선형 사상(bilinear map) $e: \mathbb{G} \times \hat{\mathbb{G}} \rightarrow \mathbb{G}_T$를 만족하는 페어링(pairing) 함수)가 만족되는지 여부를 판단하는 단계; 아래의 수학식 6

[0029] [수학식 6]

$$h = H_z(\mathrm{g}, X_i, R_i)$$

[0030]

[0031] 을 이용하여 h를 산출하는 단계; 및 아래의 수학식 7

[0032] [수학식 7]

$$\mathrm{g}^{x_i} = R_i \cdot (X_i)^h$$

[0033]

[0034] 이 만족되는지 여부를 판단하는 단계를 포함하고, 상기 공개 파라미터는 e 및 $\mathbb{G}_T$ 를 더 포함할 수 있다.

[0035] 상기 다항식은, 아래의 수학식 8

[0036] [수학식 8]

$$f(x) = \sum_{j\in[n]} f(j)\cdot L_j(x) = \sum_{j\in[n]} s_{\psi(j)}\cdot y_j \cdot L_j(x)$$

[0037]

[0038] (이때, f(x)는 상기 다항식, j는 상기 가중치 기반 인덱스, $\psi(j)$는 $j \in [\bar{w}_{i-1}+1 : \bar{w}_{i-1}+w_i]$ 인 각 j에 대해 $\bar{w}_i = \sum_{k=1}^{i} w_k$ $\psi(j)=i$인 $j\in[n]$에서 $i\in[m]$로의 사상(mapping), w_i는 상기 사용자 P_i의 사용자 가중치, , $L_j(x)$는 라그랑주 기저 다항식(Lagrange basis polynomial))을 만족하고, y_j는, 아래의 수학식 9

[0039] [수학식 9]

[0040] $y_j=H_2(GD \| j)$

[0041] (이때, GD는 상기 사용자 그룹에 대한 그룹 기술(group description) 정보로서 $GD = (GID, \{PK_i, RK_i, P_i, w_i\}_{i=1}^{m}, n, t)$)을 만족하고, $L_j(x)$는, 아래의 수학식 10

[0042] [수학식 10]

$$L_j(x) = \prod_{k\in[n],k\neq j} \frac{x-k}{j-k}$$

[0043]

[0044] 을 만족할 수 있다.

[0045] 상기 결합키는, 상기 n-t개의 포인트 각각에 대한 제1 결합키 요소 및 제2 결합키 요소를 포함하고, 상기 결합키를 생성하는 단계는, $k\in[-(n-t):-1]$인 각 k에 대해, 아래의 수학식 11

[0046] [수학식 11]

$$V_k = \prod_{j\in[n]} X_{\psi(j)}^{H_2(GD\|j)\cdot L_j(k)}$$

[0047]

[0048] (이때, V_k는 상기 제1 결합키 요소, $L_j(k)$는 상기 n-t개의 포인트 각각에 대한 라그랑주 계수)을 이용하여 상기 제1 결합키 요소를 생성하고, 아래의 수학식 12

[0049] [수학식 12]

$$W_k = \prod_{j\in[n]} Y_{\psi(j)}^{H_2(GD\|j)\cdot L_j(k)}$$

[0050]

[0051] (이때, W_k는 상기 제2 결합키 요소)를 이용하여 상기 제2 결합키 요소를 생성할 수 있다.

[0052] 상기 검증키는, 제1 검증키 요소 및 제2 검증키 요소를 포함하고, 상기 검증키를 생성하는 단계는, 아래의 수학식 13

[0053] [수학식 13]

$$V_0 = \prod_{j\in[n]} X_{\psi(j)}^{H_2(GD\|j)\cdot L_j(0)}$$

[0054]

[0055] (이때, V_0는 상기 제1 검증키 요소, $L_j(0)$는 상기 y절편에 대한 라그랑주 계수)을 이용하여 상기 제1 검증키 요소를 생성하고, 아래의 수학식 14

[0056] [수학식 14]

$$W = H_0(GID)$$

[0057]

[0058] (이때, W는 상기 제2 검증키 요소)를 이용하여 상기 제2 검증키 요소를 생성할 수 있다.

[0059] 상기 방법은, 상기 복수의 사용자 중 적어도 일부 사용자 각각이 자신의 사용자 비밀키를 이용하여 메시지에 대해 생성한 부분 서명을 획득하는 단계; 상기 적어도 일부 사용자 각각의 사용자 공개키를 이용하여 상기 적어도 일부 사용자 각각의 부분 서명을 검증하고, 상기 적어도 일부 사용자 중 부분 서명이 검증된 각 사용자 및 상기 검증된 각 사용자의 사용자 가중치를 포함하는 집합 Q를 생성하는 단계; 상기 검증된 각 사용자의 사용자 가중치의 합이 t 이상인 경우, 상기 집합 Q에 포함된 각 사용자의 가중치 기반 인덱스 중 t개의 가중치 기반 인덱스에 기초하여 아래의 수학식 15

[0060] [수학식 15]

$$f(0) = \sum_{j\in X_Q\cup[-(n-t):-1]} f(j)\cdot L_j(0)$$

[0061]

$\{L_j(0)\}_{j\in X_Q\cup[-(n-t):-1]}$

[0062] 를 만족하는 라그랑주 계수 (이때, X_Q는 상기 집합 Q에 포함된 각 사용자의 가중치 기반 인덱스 중 t개의 가중치 기반 인덱스를 포함하는 집합)를 생성하는 단계; 상기 라그랑주 계수 $\{L_j(0)\}_{j\in X_Q\cup[-(n-t):-1]}$, 상기 집합 Q에 포함된 각 사용자의 부분 서명 및 상기 결합키를 이용하여 상기 메시지에 대한 임계 서명을 생성하는 단계를 더 포함할 수 있다.

[0063] 상기 임계 서명은, 제1 서명 요소, 제2 서명 요소 및 제3 서명 요소를 포함하고, 상기 임계 서명을 생성하는 단계는, 아래의 수학식 16

[0064] [수학식 16]

$$S_0 = \prod_{j\in X_Q} \sigma_i^{H_2(GD\|j)\cdot L_j(0)}$$

[0065]

[0066] (이때, S_0는 상기 제1 서명 요소)을 이용하여 상기 제1 서명 요소를 생성하고, 아래의 수학식 17

[0067] [수학식 17]

$$S_1 = \prod_{j\in[-(n-t):-1]} V_j^{L_j(0)}$$

[0068]

[0069] (S_1은 상기 제2 서명 요소)을 이용하여 상기 제2 서명 요소를 생성하고, 아래의 수학식 18

[0070] [수학식 18]

$$S_2 = \prod_{j\in[-(n-t):-1]} W_j^{L_j(0)}$$

[0071]

[0072] (S_2는 상기 제3 서명 요소)을 이용하여 상기 제3 서명 요소를 생성할 수 있다.

[0073] 일 실시예에 따른 장치는, 하나 이상의 프로세서; 및 상기 하나 이상의 프로세서에 의해 실행되는 하나 이상의 프로그램을 저장하는 메모리를 포함하고, 상기 하나 이상의 프로세서는, 사용자 그룹에 참여한 복수의 사용자 각각의 사용자 공개키 및 등록키를 검증하고, 라그랑주 보간법(Lagrange interpolation)을 이용하여 상기 복수의 사용자 각각의 사용자 인덱스 및 사용자 가중치에 기초한 가중치 기반 인덱스에 대응하는 n(이때, n은 상기 복수의 사용자 각각의 사용자 가중치의 총합)개의 포인트를 지나고 차수가 n-1인 다항식을 정의하고, 상기 다항식에 대한 라그랑주 기저 다항식(Lagrange basis polynomial)을 이용하여, 상기 n개의 포인트를 제외한 상기 다항식 상의 n-t(이때, t는 t≤n인 사전 설정된 양의 정수)개의 포인트 및 상기 다항식의 y절편 각각에 대한 라그랑주 계수(Lagrange coefficient)를 산출하고, 상기 n-t개의 포인트 각각에 대한 라그랑주 계수, 상기 복수의 사용자 각각의 사용자 공개키 및 등록키를 이용하여, 상기 복수의 사용자 중 상기 사용자 가중치의 합이 t 이상인 하나 이상의 사용자가 각각 자신의 사용자 비밀키를 이용하여 생성한 부분 서명으로부터 임계 서명을 생성하기 위한 결합키를 생성하고, 상기 y절편에 대한 라그랑주 계수, 상기 하나 이상의 사용자 각각의 사용자 공개키 및 상기 사용자 그룹의 그룹 식별자를 이용하여 상기 임계 서명에 대한 검증키를 생성한다.

[0074] 상기 복수의 사용자 중 상기 사용자 인덱스가 i(이때, i는 1≤i≤m인 정수, m은 상기 복수의 사용자의 총 수이고, 2≤m≤n를 만족함)인 사용자 P_i의 공개키는, 상기 사용자 P_i의 사용자 비밀키를 이용하여 생성되고, 상기 사용자 P_i의 등록키 RK_i는, 상기 그룹 식별자, 상기 사용자 P_i의 사용자 비밀키를 이용하여 생성된 상기 그룹 식별자에 대한 서명 및 상기 사용자 P_i의 사용자 비밀키에 대한 영지식 증명(zero knowledge proof)을 위한 증명 값을 포함할 수 있다.

[0075] 상기 사용자 P_i의 공개키는, 아래의 수학식 1

[0076] [수학식 1]

$$X_i = g^{s_i}$$

[0077]

[0078] (X_i는 상기 사용자 P_i의 사용자 공개키, g는 위수(order)가 소수 p인 순환 군(cyclic group) $\mathbb{G}$ 의 생성원 (generator), s_i는 $s_i \in \mathbb{Z}_p^*$ 를 만족하는 상기 사용자 P_i의 사용자 비밀키, $\mathbb{Z}_p^*$ 는 사전 정의된 정수 집합)을 만족하고, 상기 그룹 식별자에 대한 서명은, 아래의 수학식 2

[0079] [수학식 2]

$$Y_i = H_0(GID)^{s_i}$$

[0080]

[0081] (이때, GID는 상기 그룹 식별자, Y_i는 상기 그룹 식별자에 대한 서명, H_0는 $H_0: \{0,1\}^* \rightarrow \widehat{\mathbb{G}}$ 를 만족하는 해시 함

$\hat{\mathbb{G}}$ $\mathbb{G}$ $\hat{\mathbb{G}}$

수, 는 위수가 소수 p인 순환 군)를 만족하고, p, g, H_0, 및 는 공개 파라미터일 수 있다.

[0082] 상기 증명 값은 제1 증명 요소 및 제2 증명 요소를 포함하고, 상기 제1 증명 요소는, 아래의 수학식 3

[0083] [수학식 3]

$$R_i = g^{r_i}$$

[0084]

$r_i \in \mathbb{Z}_p$ $\mathbb{Z}_p$

[0085] (이때, R_i는 상기 제1 증명 요소, r_i은 를 만족하는 임의의 정수, 는 사전 정의된 정수 집합)을 만족하고, 상기 제2 증명 요소는, 아래의 수학식 4

[0086] [수학식 4]

$$z_i = r_i + s_i \cdot H_z(g, X_i, R_i)$$

[0087]

$H_z: \mathbb{G}^3 \rightarrow \mathbb{Z}_p$

[0088] (이때, z_i는 상기 제2 증명 요소, H_z는 를 만족하는 해시 함수)를 만족하고, 상기 공개 파라미터는 H_z를 더 포함할 수 있다.

[0089] 상기 하나 이상의 프로세서는, 상기 등록키에 포함된 그룹 식별자와 상기 사용자 그룹의 그룹 식별자가 일치하고 아래의 수학식 5

[0090] [수학식 5]

$$e(g, Y_i) = e\left(X_i, H_0(GID)\right)$$

[0091]

$\mathbb{G}$ $\hat{\mathbb{G}}$ $\mathbb{G}_T$ $e: \mathbb{G} \times \hat{\mathbb{G}} \rightarrow \mathbb{G}_T$

[0092] (이때, e는 각각 위수가 소수 p인 순환 군 , 및 에 대해 겹선형 사상(bilinear map) 를 만족하는 페어링(pairing) 함수)가 만족되는지 여부를 판단하고, 아래의 수학식 6

[0093] [수학식 6]

$$h = H_z(g, X_i, R_i)$$

[0094]

[0095] 을 이용하여 h를 산출하고, 아래의 수학식 7

[0096] [수학식 7]

$$g^{z_i} = R_i \cdot (X_i)^h$$

[0097]

$\mathbb{G}_T$

[0098] 이 만족되는지 여부를 판단하고, 상기 공개 파라미터는 e 및 를 더 포함할 수 있다.

[0099] 상기 다항식은, 아래의 수학식 8

[0100] [수학식 8]

$$f(x) = \sum_{j \in [n]} f(j) \cdot L_j(x) = \sum_{j \in [n]} s_{\psi(j)} \cdot y_j \cdot L_j(x)$$

[0101]

$j \in [\bar{w}_{i-1} + 1 : \bar{w}_{i-1} + w_i]$

[0102] (이때, f(x)는 상기 다항식, j는 상기 가중치 기반 인덱스, $\psi(j)$는 인 각 j에 대해

$\bar{w}_i = \sum_{k=1}^{i} w_k$

ψ(j)=i인 j∈[n]에서 i∈[m]로의 사상(mapping), w_i는 상기 사용자 P_i의 사용자 가중치, , L_j(x)는 라그랑주 기저 다항식(Lagrange basis polynomial))을 만족하고, y_j는, 아래의 수학식 9

[0103] [수학식 9]

[0104] $y_j=H_2(GD \| j)$

[0105] (이때, GD는 상기 사용자 그룹에 대한 그룹 기술(group description) 정보로서 $GD = (GID, \{PK_i, RK_i, P_i, w_i\}_{i=1}^{m}, n, t)$)를 만족하고, L_j(x)는, 아래의 수학식 10

[0106] [수학식 10]

$$L_j(x) = \prod_{k\in[n],k\neq j} \frac{x-k}{j-k}$$

[0107]

[0108] 을 만족할 수 있다.

[0109] 상기 결합키는, 상기 n-t개의 포인트 각각에 대한 제1 결합키 요소 및 제2 결합키 요소를 포함하고, 상기 하나 이상의 프로세서는, k∈[-(n-t):-1]인 각 k에 대해, 아래의 수학식 11

[0110] [수학식 11]

$$V_k = \prod_{j\in[n]} X_{\psi(j)}^{H_2(GD\|j)\cdot L_j(k)}$$

[0111]

[0112] (V_k는 상기 제1 결합키 요소, L_j(k)는 상기 n-t개의 포인트 각각에 대한 라그랑주 계수)을 이용하여 상기 제1 결합키 요소를 생성하고, 아래의 수학식 12

[0113] [수학식 12]

$$W_k = \prod_{j\in[n]} Y_{\psi(j)}^{H_2(GD\|j)\cdot L_j(k)}$$

[0114]

[0115] (W_k는 상기 제2 결합키 요소)를 이용하여 상기 제2 결합키 요소를 생성할 수 있다.

[0116] 상기 검증키는, 제1 검증키 요소 및 제2 검증키 요소를 포함하고, 상기 하나 이상의 프로세서는, 아래의 수학식 13

[0117] [수학식 13]

$$V_0 = \prod_{j\in[n]} X_{\psi(j)}^{H_2(GD\|j)\cdot L_j(0)}$$

[0118]

[0119] (V_0는 상기 제1 검증키 요소, L_j(0)는 상기 y절편에 대한 라그랑주 계수)을 이용하여 상기 제1 검증키 요소를 생성하고, 아래의 수학식 14

[0120] [수학식 14]

$$W = H_0(GID)$$

[0121]

[0122] (이때, W는 상기 제2 검증키 요소)를 이용하여 상기 제2 검증키 요소를 생성할 수 있다.

[0123] 상기 하나 이상의 프로세서는, 상기 복수의 사용자 중 적어도 일부 사용자 각각이 자신의 사용자 비밀키를 이용

하여 메시지에 대해 생성한 부분 서명을 획득하고, 상기 적어도 일부 사용자 각각의 사용자 공개키를 이용하여 상기 적어도 일부 사용자 각각의 부분 서명을 검증하고, 상기 적어도 일부 사용자 중 부분 서명이 검증된 각 사용자 및 상기 검증된 각 사용자의 사용자 가중치를 포함하는 집합 Q를 생성하고, 상기 검증된 각 사용자의 사용자 가중치의 합이 t 이상인 경우, 상기 집합 Q에 포함된 각 사용자의 가중치 기반 인덱스 중 t개의 가중치 기반 인덱스에 기초하여 아래의 수학식 15

[0124] [수학식 15]

[0125] $$f(0) = \sum_{j \in X_Q \cup [-(n-t):-1]} f(j) \cdot L_j(0)$$

[0126] 를 만족하는 라그랑주 계수 $\{L_j(0)\}_{j \in X_Q \cup [-(n-t):-1]}$ (이때, X_Q는 상기 집합 Q에 포함된 각 사용자의 가중치 기반 인덱스 중 t개의 가중치 기반 인덱스를 포함하는 집합)를 생성하고, 상기 라그랑주 계수 $\{L_j(0)\}_{j \in X_Q \cup [-(n-t):-1]}$, 상기 집합 Q에 포함된 각 사용자의 부분 서명 및 상기 결합키를 이용하여 상기 메시지에 대한 임계 서명을 생성할 수 있다.

[0127] 상기 임계 서명은, 제1 서명 요소, 제2 서명 요소 및 제3 서명 요소를 포함하고, 상기 하나 이상의 프로세서는, 아래의 수학식 16

[0128] [수학식 16]

[0129] $$S_0 = \prod_{j \in X_Q} \sigma_i^{H_2(GD \| j) \cdot L_j(0)}$$

[0130] (이때, S_0는 상기 제1 서명 요소)을 이용하여 상기 제1 서명 요소를 생성하고, 아래의 수학식 17

[0131] [수학식 17]

[0132] $$S_1 = \prod_{j \in [-(n-t):-1]} V_j^{L_j(0)}$$

[0133] (이때, S_1은 상기 제2 서명 요소)을 이용하여 상기 제2 서명 요소를 생성하고, 아래의 수학식 18

[0134] [수학식 18]

[0135] $$S_2 = \prod_{j \in [-(n-t):-1]} W_j^{L_j(0)}$$

[0136] (이때, S_2는 상기 제3 서명 요소)을 이용하여 상기 제3 서명 요소를 생성할 수 있다.

발명의 효과

[0137] 개시되는 실시예들에 따르면, 별도의 신뢰 기관 없이 각 사용자가 자신의 사용자 공개키 및 사용자 비밀키를 스스로 생성하되, 사용자 공개키 및 사용자 비밀키를 생성과 사용자 그룹 설정 과정에서 사용자 사이의 어떠한 상호작용도 요구하지 않으므로 비상호적이고 탈중앙화된 임계 서명을 가능케 하며, 이를 통해 사용자 공개키, 사용자 비밀키 및 사용자 그룹 설정을 위해 요구되는 통신량과 연산량을 줄일 수 있다.

[0138] 또한, 개시되는 실시예들에 따르면, 사용자 그룹에 포함된 각 사용자마다 상이한 가중치를 가지도록 하여, 가중치 기반의 임계 서명 생성 및 검증이 가능토록 할 수 있다.

도면의 간단한 설명

[0139] 도 1은 일 실시예에 따른 시스템의 구성도이다.

도 2는 일 실시예에 따른 부분 서명 생성 과정을 나타낸 순서도이다.

도 3은 일 실시예에 따른 결합키 및 검증키 생성 과정을 나타낸 순서도이다.

도 4는 일 실시예에 따른 임계 서명 생성 및 검증 과정을 나타낸 순서도이다.

도 5는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0140] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0141] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0142] 도 1은 일 실시예에 따른 임계 서명 기법이 적용되는 시스템의 예시적인 구성도이다.

[0143] 도 1을 참조하면, 본 발명의 일 실시예에 따른 시스템(100)은 셋업 장치(110), 부분 서명 생성 장치(120-1, 120-2, 120-m), 그룹 관리 장치(130) 및 임계 서명 생성 장치(140)를 포함한다.

[0144] 셋업 장치(110)는 시스템(100)에 대한 셋업(setup)을 수행하고, 시스템(100) 내에서 사용할 공개 파라미터를 생성하기 위한 장치이다. 일 실시예에서, 셋업 장치(110)는 예를 들어, 신뢰 기관(Trusted Third Party)과 같이 신뢰할 수 있는 개체(entity)에 의해 운영될 수 있으나, 셋업 장치(110)의 운영 주체는 반드시 특정한 개체로 한정되는 것은 아니다.

[0145] 부분 서명 생성 장치(120-1, 120-2, 120-m)는 시스템(100) 내 각 사용자가 메시지에 대한 부분 서명을 생성하기 위해 이용되는 장치이다. 한편, 시스템(100) 내에는 하나 이상의 사용자 그룹이 존재할 수 있고, 각 사용자는 시스템(100) 내 하나 이상의 사용자 그룹에 참여할 수 있다.

[0146] 한편, 각 부분 서명 생성 장치(120-1, 120-2, 120-m)는 각 부분 서명 생성 장치(120-1, 120-2, 120-m)를 이용하는 사용자의 사용자 비밀키, 사용자 공개키를 생성할 수 있다. 이후, 각 부분 서명 생성 장치(120-1, 120-2, 120-m)는 사용자 공개키를 시스템(100) 내에 공개하고 사용자 비밀키를 이용하여 메시지에 대한 부분 서명(partial signature)을 생성할 수 있다. 또한, 각 부분 서명 생성 장치(120-1, 120-2, 120-m)는 시스템(100) 내 사용자 그룹에 대한 사용자의 등록키를 생성하고, 생성한 등록키를 그룹 관리 장치(130)로 제공할 수 있다.

[0147] 그룹 관리 장치(130)는 사용자 그룹에 참여한 사용자들이 생성한 메시지에 대한 부분 서명을 이용하여 메시지에 대한 임계 서명을 생성하기 위한 결합키 및 임계 서명에 대한 검증키를 생성하기 위한 장치이다.

[0148] 임계 서명 생성 장치(140)는 사용자 그룹에 참여한 사용자들 중 적어도 일부의 사용자들이 생성한 부분 서명과 그룹 관리 장치(130)가 생성한 결합키를 이용하여 메시지에 대한 임계 서명을 생성하기 위한 장치이다.

[0149] 한편, 도 1에 도시된 시스템(100)의 구성은 예시적인 것이므로, 시스템(100)의 구성이 반드시 도 1에 도시된 예에 한정되는 것은 아니다. 예를 들어, 도 1에 도시된 예에서는 그룹 관리 장치(130)와 임계 서명 생성 장치(140)가 분리된 별도의 장치인 것으로 도시하고 있으나, 실시예에 따라 그룹 관리 장치(130)와 임계 서명 생성 장치(140)는 하나의 장치로 구현될 수 있다.

[0150] 이하에서는 설명의 편의를 위해 각 부분 서명 생성 장치(120-1, 120-2, 120-m)의 사용자가 동일한 사용자 그룹에 참여한 것으로 가정하여 설명하나 반드시 이에 한정되는 것은 아님을 유의하여야 한다. 또한, 이하에서 임의

의 정수 a>0 및 b<a에 대해 [a]은 정수들의 집합 {1,...,a}을 나타내며, [b:a]은 정수들의 집합 {b, b+1,...,a-1,a}을 나타낸다.

[0151] 한편, 일 실시예에 따른 임계 서명 기법은 셋업 알고리즘, 키 생성 알고리즘, 등록키 생성 알고리즘, 그룹 셋업 알고리즘, 서명 알고리즘, 부분 서명 검증 알고리즘, 결합 알고리즘, 임계 서명 검증 알고리즘을 포함할 수 있고, 각 알고리즘에 대한 설명은 아래와 같다.

[0153] 셋업 알고리즘

[0154] 셋업 알고리즘은 보안 상수(security parameter) 1^{λ}를 입력 받고, 겹선형 군(bilinear group) $(p, \mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, e, g, \hat{g})$ $\mathbb{G}$ $\hat{\mathbb{G}}$ $\mathbb{G}_T$ 를 생성한다. 이때, , 및 는 각각 위수(order)가 소수(prime number) p인 순환 군 $\mathbb{G}$ $\hat{g}$ $\hat{\mathbb{G}}$ (cyclic group), g는 의 생성원(generator), 는 의 생성원이다. 또한, e는 겹선형 사상(bilinear map) $e: \mathbb{G} \times \hat{\mathbb{G}} \rightarrow \mathbb{G}_T$ $e(g^a, \hat{g}^b) = e(g, \hat{g})^{ab}$ 를 만족하는 페어링(pairing) 함수이다. 즉, e는 를 만족한다.

[0155] 이후, 셋업 알고리즘은 $H_0: \{0,1\}^* \rightarrow \hat{\mathbb{G}}$ 를 만족하는 해시(hash) 함수 H_0, $H_1: \{0,1\}^* \rightarrow \hat{\mathbb{G}}$ 를 만족하는 해시 함수 H_1, 및 $H_2: \{0,1\}^* \rightarrow \mathbb{Z}_p^*$ 를 만족하는 해시 함수 H_2 $H_z: \mathbb{G}^3 \rightarrow \mathbb{Z}_p$ 를 만족하는 해시 함수 H_z를 선택하고, 공개 파라미터 $PP = ((p, \mathbb{G}, \hat{\mathbb{G}}, \mathbb{G}_T, e, g, \hat{g}), H_0, H_1, H_2, CRS)$ 를 시스템(100) 내에 공개한다. 이때, CRS는 영지식 증명(zero knowledge proof)를 위한 공개 파라미터이며, $CRS = (p, \mathbb{G}, g, H_z)$ 이다.

[0156] 한편, 일 실시예에서, 셋업 알고리즘은 예를 들어, 도 1에 도시된 셋업 장치(110)에 의해 수행될 수 있다.

[0158] 키 생성 알고리즘

[0159] 키 생성 알고리즘은 공개 파라미터 PP를 입력 받고, 부분 서명을 생성할 사용자의 사용자 비밀키 및 사용자 공개키를 생성한다.

[0160] 구체적으로, 키 생성 알고리즘은 포함된 소수 p에 기초하여 정의되는 정수 집합 $\mathbb{Z}_p^*$ 에 포함된 임의의 원소 s(즉, $s \in \mathbb{Z}_p^*$)를 선택하여 사용자 비밀키 SK=s를 생성하고, 수학식 1을 이용하여 사용자 공개키 PK=X를 생성한다.

[0161] [수학식 1]

$$X = g^s$$

[0162]

[0163] 한편, 일 실시예에서, 키 생성 알고리즘은 예를 들어, 도 1에 도시된 각 부분 서명 생성 장치(120-1, 120-2, 120-m)에 의해 수행될 수 있다.

[0165] 등록키 생성 알고리즘

[0166] 등록키 생성 알고리즘은 공개 파라미터 PP, 사용자 그룹의 그룹 식별자 GID$\in\{0,1\}^*$, 사용자 비밀키 SK=s 및 사용자 공개키 PK=X를 입력 받고, 그룹 식별자 GID, 그룹 식별자 GID에 대한 서명 Y 및 사용자 비밀키 s에 대한

영지식 증명을 위한 증명 값 π을 포함하는 등록키 RK=(GID, Y, π)를 생성한다. 이때, 그룹 식별자 GID는 예를 들어, 그룹 관리 장치(130)에 의해 사전에 생성되어 시스템(100) 내에 공개될 수 있다.

[0167] 구체적으로, 등록키 생성 알고리즘은 수학식 2를 이용하여 그룹 식별자 GID에 대한 서명 Y를 생성할 수 있다.

[0168] [수학식 2]

$$Y = H_0(GID)^s$$

[0169]

[0170] 또한, 등록키 생성 알고리즘은 제1 증명 요소 R 및 제2 증명 요소 z를 포함하는 증명 값 π=(R, z)를 생성할 수 있다. 구체적으로, 등록키 생성 알고리즘은 정수 집합 $\mathbb{Z}_p$ 에 포함된 임의의 원소 r(즉, $r \in \mathbb{Z}_p$)를 선택한 후 수학식 3을 이용하여 제1 증명 요소 R을 생성할 수 있다.

[0171] [수학식 3]

$$R = \mathbf{g}^r$$

[0172]

[0173] 이후, 등록키 생성 알고리즘은 수학식 4를 이용하여 제2 증명 요소 z를 생성할 수 있다.

[0174] [수학식 4]

$$z = r + s \cdot H_z(\mathbf{g}, X, R)$$

[0175]

[0176] 한편, 일 실시예에서, 등록키 생성 알고리즘은 예를 들어, 도 1에 도시된 각 부분 서명 생성 장치(120-1, 120-2, 120-m)에 의해 수행될 수 있다.

[0178] 그룹 셋업 알고리즘

[0179] 그룹 셋업 알고리즘은 사용자 그룹에 대한 그룹 기술(group description) 정보 $GD = (GID, \{PK_i, RK_i, P_i, w_i\}_{i=1}^m, n, t)$ 및 공개 파라미터 PP를 입력받고, 사용자 그룹에 대한 결합키 CK 및 검증키 VK를 생성한다.

[0180] 이때, w_i, m, n 및 t는 각각 양의 정수이며, m은 사용자 그룹에 참여한 사용자들의 총 수, w_i는 사용자 그룹에 참여한 각 사용자들에 대한 사용자 가중치, n은 사용자 그룹에 참여한 각 사용자들에 대한 사용자 가중치의 총합(즉, $n = \sum_{i=1}^m w_i$), t는 사전 설정된 임계 값을 나타낸다. 또한, n 및 m는 $2 \le m \le n$를 만족하고, t는 $t \le n$를 만족한다. 한편, 각 사용자의 사용자 가중치 w_i는 사전 설정된 가중치 결정 기준에 따라 결정될 수 있으며, 이때, 가중치 결정 기준은 반드시 실시예에 따라 다양하게 설정될 수 있다.

[0181] 한편, 사용자 그룹에 참여한 각 사용자들은 사전 설정된 정규화된 순서(canonical ordering)을 통해 인덱싱될 수 있으며, $i \in [1:m]$는 각 사용자에 대한 사용자 인덱스를 나타낸다. 또한, P_i는 사용자 그룹에 참여한 m명의 사용자 중 사용자 인덱스가 i인 사용자를 나타내며, PK_i 및 RK_i는 각각 사용자 인덱스가 i인 사용자의 사용자 공개키 및 등록키를 나타낸다.

[0182] 한편, 그룹 셋업 알고리즘은 그룹 기술 정보 GD에 포함된 각 사용자의 공개키 $PK_i=X_i$ 및 등록키 $RK_i=(GID', Y_i, \pi_i)$를 검증한다. 구체적으로, 그룹 셋업 알고리즘은 그룹 기술 정보에 포함된 그룹 식별자 GID와 각 사용자의 등록키 RK_i에 포함된 그룹 식별자 GID'가 일치하는지 여부 및 수학식 5가 만족되는지 여부를 판단한다.

[0183] [수학식 5]

$$e(g, Y_i) = e(X_i, H_0(GID))$$

[0184]

[0185] 또한, 그룹 셋업 알고리즘은 수학식 6을 이용하여 h를 산출한 후 수학식 7이 만족되는지 여부를 판단한다.

[0186] [수학식 6]

$$h = H_z(g, X_i, R_i)$$

[0187]

[0188] [수학식 7]

$$g^{z_i} = R_i \cdot (X_i)^h$$

[0189]

[0190] 한편, 그룹 셋업 알고리즘은 GID≠GID'이거나, 수학식 5 및 7 중 적어도 하나가 만족되지 않는 경우, 검증에 실패한 것으로 판단한다. 반면, 그룹 셋업 알고리즘은 GID=GID'이고 수학식 5 및 7이 모두 만족되는 경우, 검증에 성공한 것으로 판단한다.

[0191] 검증에 성공한 경우, 그룹 셋업 알고리즘은 라그랑주 보간법(Lagrange interpolation)을 이용하여 사용자 그룹에 참여한 각 사용자의 사용자 인덱스 및 사용자 가중치에 기초한 각 사용자의 가중치 기반 인덱스 j∈[1:n]에 대응하는 n개의 포인트 $\{(j, f(j))\}_{j\in[1:n]}$를 지나고 차수가 n-1인 다항식 $f \in \mathbb{Z}_p[X]$을 정의한다.

$j \in [\bar{w}_{i-1} + 1 : \bar{w}_{i-1} + w_i]$ $\bar{w}_i = \sum_{k=1}^{i} w_k$)

[0192] 이때, 각 사용자의 가중치 기반 인덱스 j는 (이때, 인 각 j에 대해 아래의 수학식 8과 같이 정의되는 j∈[n]에서 i∈[m]로의 사상(mapping) ψ:[n]→[m]에 의해 결정될 수 있다.

[0193] [수학식 8]

$$\psi(j) = i$$

[0194]

$X_1 = g^{s_1}$ $X_2 = g^{s_2}$ $X_3 = g^{s_3}$

[0195] 예를 들어, (, P_1, w_1=3), (, P_2, w_2=1), (, P_3, w_3=2)이고, m=3, n=6, t=4인 것으로 가정하면, 수학식 8에 따라 ψ(1)=1, ψ(2)=1, ψ(3)=1, ψ(4)=2, ψ(5)=3, ψ(6)=3이므로, 사용자 P_1의 가중치 기반 인덱스는 {1, 2, 3}이고, 사용자 P_2의 가중치 기반 인덱스는 {4}이며, 사용자 P_3의 가중치 기반 인덱스는 {5, 6}으로 결정될 수 있다.

[0196] 한편, 다항식 f(x)는 아래의 수학식 9와 같이 정의될 수 있다.

[0197] [수학식 9]

$$f(x) = \sum_{j\in[n]} f(j) \cdot L_j(x)$$

[0198]

[0199] 수학식 9에서 f(j)는 j∈[1:n]인 각 j에 대해 $s_{\psi(j)}=d\log_g(X_{\psi(j)})$이고, $y_j=H_2(GD \| j)$일 때, 아래의 수학식 10과 같이 정의될 수 있다.

[0200] [수학식 10]

$$f(j) = s_{\psi(j)} \cdot y_j$$

[0201]

$X_1 = g^{s_1}$ $X_2 = g^{s_2}$ $X_3 = g^{s_3}$

[0202] 예를 들어, (, P_1, w_1=3), (, P_2, w_2=1), (, P_3, w_3=2)이고, m=3, n=6, t=4인 것으로

가정하면, $\psi(1)=1$, $\psi(2)=1$, $\psi(3)=1$, $\psi(4)=2$, $\psi(5)=3$, $\psi(6)=3$이고, $f(1)=s_1 \cdot y_1$, $f(2)=s_1 \cdot y_2$, $f(3)=s_1 \cdot y_3$, $f(4)=s_2 \cdot y_4$, $f(5)=s_3 \cdot y_5$, $f(6)=s_3 \cdot y_6$이다.

[0203] 한편, 수학식 9에서 $L_i(x)$는 수학식 11과 같이 정의되는 라그랑주 기저 다항식(Lagrange basis polynomial)이다.

[0204] [수학식 11]

$$L_j(x) = \prod_{k\in[n],k\neq j} \frac{x-k}{j-k}$$

[0205]

[0206] 이후, 그룹 셋업 알고리즘은 라그랑주 기저 다항식 $L_j(x)$을 이용하여 $\{(j,f(j))\}_{j\in[1:n]}$ 를 제외한 다항식 f(x) 상의 n-t개의 포인트 및 다항식 f(x)의 y절편 각각에 대한 라그랑주 계수(Lagrange interpolation)를 산출한다.

[0207] 구체적으로, 그룹 셋업 알고리즘은 라그랑주 기저 다항식 $L_j(x)$을 이용하여 다항식 f(x) 상의 n-t개의 포인트 $\{(k,f(k)\}_{k\in[-(n-t):-1]}$ 각각에 대한 라그랑주 계수 $\{L_j(k)\}_{j\in[n]}$ 를 생성하고, 다항식 f(x)의 y절편 f(0)에 대한 라그랑주 계수 $\{L_j(0)\}_{j\in[n]}$ 를 생성할 수 있다.

[0208] 이후, 그룹 셋업 알고리즘은 수학식 12 및 13을 이용하여 각 k에 대한 제1 결합키 요소 V_k 및 제2 결합키 요소 W_k를 생성한다.

[0209] [수학식 12]

$$V_k = \prod_{j\in[n]} X_{\psi(j)}^{H_2(GD\|j)\cdot L_j(k)} = g^{f(k)}$$

[0210]

[0211] [수학식 13]

$$W_k = \prod_{j\in[n]} Y_{\psi(j)}^{H_2(GD\|j)\cdot L_j(k)} = H_0(GID)^{f(k)}$$

[0212]

[0213] 또한, 그룹 셋업 알고리즘은 수학식 14 및 15를 이용하여 제1 검증키 요소 V_0 및 제2 검증키 요소 W를 생성한다.

[0214] [수학식 14]

$$V_0 = \prod_{j\in[n]} X_{\psi(j)}^{H_2(GD\|j)\cdot L_j(0)}$$

[0215]

[0216] [수학식 15]

$$W = H_0(GID)$$

[0217]

[0218] 이후, 그룹 셋업 알고리즘은 각 k에 대한 제1 결합키 요소 V_k 및 제2 결합키 요소 W_k를 포함하는 결합키 $CK=(\{V_k\}_{k\in[-(n-t):-1]},\{W_k\}_{k\in[-(n-t):-1]})$ 및 제1 검증키 요소 V_0 및 제2 검증키 요소 W를 포함하는 검증키 $VK=(V_0,W)$를 출력한다.

[0219] 한편, 일 실시예에서, 그룹 셋업 알고리즘은 도 1에 도시된 그룹 관리 장치(130) 각각에 의해 수행될 수 있다.

[0221] 서명 알고리즘

[0222] 서명 알고리즘은 공개 파라미터 PP 및 사용자의 비밀키 SK를 이용하여 메시지 $M \in \{0,1\}^*$에 대한 사용자의 부분 서명 σ을 생성한다. 구체적으로, 서명 알고리즘은 수학식 16을 이용하여 부분 서명 σ을 생성할 수 있다.

[0223] [수학식 16]

$$\sigma = H_1(M)^s$$

[0224]

[0225] 한편, 일 실시예에서, 서명 알고리즘은 도 1에 도시된 부분 서명 생성 장치(120-1, 120-2, 120-m) 각각에 의해 수행될 수 있다.

[0227] 부분 서명 검증 알고리즘

[0228] 부분 서명 검증 알고리즘은 공개 파라미터 PP, 메시지 M, 사용자 공개키 PK를 이용하여, 메시지 M에 대한 사용자의 부분 서명을 검증한다. 구체적으로, 부분 서명 검증 알고리즘은 사용자의 부분 서명 σ이 수학식 17을 만족하는지 여부를 판단함으로써 부분 서명 σ을 검증할 수 있다.

[0229] [수학식 17]

$$e(g,\sigma) = e\left(X, H_1(M)\right)$$

[0230]

[0231] 한편, 부분 서명 검증 알고리즘은 수학식 17이 만족된 경우 부분 서명에 대한 검증이 성공한 것으로 판단하여 1을 출력하고, 만족되지 않은 경우 부분 서명에 대한 검증이 실패한 것으로 판단하여 0을 출력할 수 있다.

[0232] 한편, 일 실시예에서, 부분 서명 검증 알고리즘은 도 1에 도시된 임계 서명 생성 장치(140)에 의해 수행될 수 있다.

[0234] 결합 알고리즘

[0235] 결합 알고리즘은 사용자 그룹에 대한 그룹 기술 정보 GD, 메시지 M, 사용자 그룹에 참여한 m명의 사용자 중 적어도 일부 사용자 각각이 생성한 메시지 M에 대한 부분 서명 집합 $\{\sigma_i\}$ 및 사용자 그룹에 대한 결합키 CK 및 공개 파라미터 PP를 이용하여 메시지 M에 대한 임계 서명을 생성한다.

[0236] 구체적으로, 사용자 그룹에 참여한 사용자들의 집합이 $P_G=\{P_1,\ldots,P_m\}$이고, 부분 서명을 생성한 사용자들의 집합이 P_o라고 할 때, 결합 알고리즘은 우선 P_G와 P_o의 교집합에 속한 각 사용자 P_i(즉, $P_i \in P_G \cap P_o$) 중 부분 서명 검증 알고리즘을 통한 검증을 통과한 부분 서명을 생성한 사용자 및 해당 사용자에 대한 사용자 가중치를 포함하는 집합 Q를 생성한다.

[0237] 이후, 결합 알고리즘은 집합 Q에 포함된 사용자들에 대한 사용자 가중치의 합 w_Q 가 $w_Q < t$인 경우, 임계 서명 생성에 실패한 것으로 판단한다.

[0238] 한편, $w_Q \geq t$인 경우, 결합 알고리즘은 집합 Q에 포함된 각 사용자의 가중치 기반 인덱스 중 t개의 가중치 기반 인덱스에 기초하여 아래의 수학식 18을 만족하는 라그랑주 계수 $\{L_j(0)\}_{j \in X_Q \cup [-(n-t):-1]}$를 도출한다.

[0239] [수학식 18]

$$f(0) = \sum_{j \in X_Q \cup [-(n-t):-1]} f(j) \cdot L_j(0)$$

[0240]

[0241] 수학식 18에서, X_Q는 집합 Q에 포함된 각 사용자의 가중치 기반 인덱스 중 t개의 가중치 기반 인덱스를 포함하는 집합을 나타낸다. 예를 들어, 집합 Q에 포함된 사용자 및 사용자 가중치가 Q={(P_1, w_1=3), (P_3, w_3=2)}인 것으로 가정하면, 사용자 P_1의 가중치 기반 인덱스는 {1, 2, 3}이고, 사용자 P_3의 가중치 기반 인덱스는 {5, 6}이다. 이 경우, t=4인 것으로 가정하면, X_Q는 P_1 및 P_3의 가중치 기반 인덱스 중 작은 수대로 선택된 4개의 가중치 기반 인덱스를 포함할 수 있다(즉, X_Q={1, 2, 3}∪{5}).

[0242] 한편, 결합 알고리즘은 라그랑주 계수 $\{L_j(0)\}_{j\in X_Q\cup[-(n-t):-1]}$, 집합 Q에 포함된 각 사용자의 부분 서명 σ_i 및 사용자 그룹의 결합키 CK를 이용하여 메시지 M에 대한 임계 서명 σ_τ을 생성한다.

[0243] 구체적으로, 결합알고리즘은 수학식 19 내지 21을 이용하여 제1 서명 요소 S_0, 제2 서명 요소 S_1 및 제3 서명 요소 S_2를 생성한 후, 임계 서명 σ_τ=(S_0, S_1, S_2)를 출력한다.

[0244] [수학식 19]

$$S_0 = \prod_{j\in X_Q} \sigma_i^{H_2(GD\|j)\cdot L_j^{par}} = \prod_{j\in X_Q} \sigma_i^{H_2(GD\|j)\cdot L_j(0)}$$

[0245]

[0246] [수학식 20]

$$S_1 = \prod_{j\in[-(n-t):-1]} V_j^{L_j^{pub}} = \prod_{j\in[-(n-t):-1]} V_j^{L_j(0)}$$

[0247]

[0248] [수학식 21]

$$S_2 = \prod_{j\in[-(n-t):-1]} W_j^{L_j^{pub}} = \prod_{j\in[-(n-t):-1]} W_j^{L_j(0)}$$

[0249]

[0250] 한편, 일 실시예에서, 결합 알고리즘은 도 1에 도시된 임계 서명 생성 장치(140)에 의해 수행될 수 있다.

[0252] 임계 서명 검증 알고리즘

[0253] 임계 서명 검증 알고리즘은 사용자 그룹의 검증키 VK=(V_0,W), 메시지 M 및 공개 파라미터 PP를 이용하여 메시지 M에 대한 임계 서명 σ_τ=(S_0, S_1, S_2)를 검증한다.

[0254] 구체적으로, 임계 서명 검증 알고리즘은 수학식 22 및 23이 모두 만족되는 경우 임계 서명 σ_τ에 대한 검증이 성공한 것으로 판단하고, 수학식 22 및 23 중 적어도 하나가 만족되지 않는 경우 임계 서명 σ_τ에 대한 검증이 실패한 것으로 판단할 수 있다.

[0255] [수학식 22]

$$e(g, S_0) = e\left(V_0/S_1, H_1(M)\right)$$

[0256]

[0257] [수학식 23]

$$e(S_1, W) = e(g, S_2)$$

[0258]

[0259] 한편, 일 실시예에서, 임계 서명 검증 알고리즘은 도 1에 도시된 그룹 관리 장치(130) 또는 임계 서명 생성 장치(140)에 의해 수행될 수 있다.

[0260] 도 2는 일 실시예에 따른 부분 서명 생성 과정을 나타낸 순서도이다.

[0261] 도 2에 도시된 부분 서명 생성 과정은 예를 들어, 도 1에 도시된 각 부분 서명 생성 장치(120-1, 120-2, 120-m)에 의해 수행될 수 있다.

[0262] 도 2를 참조하면, 사용자 인덱스가 i인 사용자 P_i의 부분 서명 생성 장치(120-i)는 P_i의 사용자 비밀키 $SK_i=s_i$ 및 사용자 공개키 $PK_i=X_i$를 생성한다(210).

[0263] 이후, 부분 서명 생성 장치(120-i)는 사용자 비밀키 SK_i, 사용자 공개키 PK_i 및 사용자가 참여할 사용자 그룹의 그룹 식별자 GID를 이용하여 사용자 그룹에 대한 P_i의 등록키 RK_i를 생성한다(220).

[0264] 이후, 부분 서명 생성 장치(120-i)는 사용자 비밀키 Sk_i를 이용하여 메시지 M에 대한 P_i의 부분 서명 σ_i을 생성한다(230).

[0265] 한편, 도 2에 도시된 순서도에서 210 단계는 상술한 키 생성 알고리즘을 통해 수행될 수 있고, 220 단계는 상술한 등록키 생성 알고리즘을 통해 수행될 수 있으며, 230 단계는 상술한 서명 알고리즘을 통해 수행될 수 있다.

[0266] 또한, 도 2에 도시된 순서도에서 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0267] 도 3은 일 실시예에 따른 결합키 및 검증키 생성 과정을 나타낸 순서도이다.

[0268] 도 3에 도시된 과정은 예를 들어, 도 1에 도시된 그룹 관리 장치(130)에 의해 수행될 수 있다.

[0269] 도 3을 참조하면, 우선, 그룹 관리 장치(130)는 사용자 그룹에 참여한 복수의 사용자 각각의 사용자 공개키 $PK_i=X_i$ 및 등록키 RK_i를 검증한다(310).

[0270] 이후, 그룹 관리 장치(130)는 라그랑주 보간법을 이용하여 복수의 사용자 각각의 사용자 인덱스 및 사용자 가중치에 기초한 가중치 기반 인덱스 $j\in[1:n]$에 대응하는 n개의 포인트 $\{(j,f(j))\}_{j\in[1:n]}$ 를 지나고 차수가 n-1인 다항식 f를 정의한다(320).

[0271] 이후, 그룹 관리 장치(130)는 정의된 다항식 f에 대한 라그랑주 기저 다항식을 이용하여, 가중치 기반 인덱스 $j\in[1:n]$에 대응하는 n개의 포인트 $\{(j,f(j))\}_{j\in[1:n]}$ 를 제외한 다항식 f 상의 n-t개의 포인트 각각에 대한 라그랑주 계수 및 다항식 f의 y절편에 대한 라그랑주 계수를 산출한다(330).

[0272] 이때, n-t개의 포인트는 $\{(k,f(k))\}_{k\in[-(n-t):-1]}$ 일 수 있고, n-t개의 포인트 각각에 대한 라그랑주 계수는 $\{L_j(k)\}_{j\in[n]}$ 일 수 있다. 다항식의 y 절편은 (0, f(0))이고, y절편에 대한 라그랑주 계수는 $\{L_j(0)\}_{j\in[n]}$ 일 수 있다.

[0273] 이후, 그룹 관리 장치(130)는 n-t개의 포인트 각각에 대한 라그랑주 계수, 복수의 사용자 각각의 사용자 공개키 PK_i 및 등록키 RK_i를 이용하여 결합키 CK를 생성하고, 다항식 f의 y절편에 대한 라그랑주 계수, 복수의 사용자 각각의 사용자 공개키 PK_i 및 사용자 그룹의 그룹 식별자 GID를 이용하여 임계 서명에 대한 검증키 VK를 생성한다(340).

[0274] 한편, 도 3에 도시된 순서도에서 각 단계는 상술한 그룹 셋업 알고리즘을 통해 수행될 수 있다.

[0275] 또한, 도 3에 도시된 순서도에서 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0276] 도 4는 일 실시예에 따른 임계 서명 생성 및 검증 과정을 나타낸 순서도이다.

[0277] 도 4에 도시된 과정은 예를 들어, 도 1에 도시된 임계 서명 생성 장치(140)에 의해 수행될 수 있다.

[0278] 도 4를 참조하면, 임계 서명 생성 장치(140)는 사용자 그룹에 참여한 복수의 사용자 중 적어도 일부 사용자 각각이 자신의 사용자 비밀키를 이용하여 메시지 M에 대해 생성한 부분 서명 집합 $\{\sigma_i\}$을 획득한다(410).

[0279] 이후, 임계 서명 생성 장치(140)는 부분 서명 집합 $\{\sigma_i\}$에 포함된 각 부분 서명을 생성한 사용자의 사용자 공개키 PK_i를 이용하여 각 사용자의 부분 서명을 검증하고, 부분 서명이 검증된 각 사용자 및 검증된 각 사용자의 사용자 가중치를 포함하는 집합 Q를 생성한다(420).

[0280] 이후, 임계 서명 생성 장치(140)는 집합 Q에 포함된 각 사용자의 사용자 가중치의 합 W_Q 이 임계 값 t 이상인지 여부를 판단한다(430).

[0281] $W_Q \geq t$인 경우, 임계 서명 생성 장치(140)는 집합 Q에 포함된 각 사용자의 가중치 기반 인덱스 중 t개의 가중치 기반 인덱스에 기초하여 라그랑주 계수 $\{L_j(0)\}_{j \in X_Q \cup [-(n-t):-1]}$를 생성한다(440).

[0282] 이후, 임계 서명 생성 장치(140)는 라그랑주 계수 $\{L_j(0)\}_{j \in X_Q \cup [-(n-t):-1]}$, 집합 Q에 포함된 각 사용자의 부분 서명 및 결합키 CK를 이용하여 메시지 M에 대한 임계 서명 σ_τ을 생성한다(450).

[0283] 이후, 임계 서명 생성 장치(140)는 사용자 그룹의 검증키 VK를 이용하여 메시지 M에 대한 임계 서명 σ_τ을 검증한다(460).

[0284] 한편, 도 4에 도시된 순서도에서 420 단계는 상술한 부분 서명 검증 알고리즘을 통해 수행될 수 있고, 430 단계 내지 450 단계는 상술한 결합 알고리즘을 통해 수행될 수 있으며, 460 단계는 상술한 임계 서명 검증 알고리즘을 통해 수행될 수 있다.

[0285] 또한, 도 4에 도시된 순서도에서 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0286] 도 5는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0287] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 도 1에 도시된 시스템(100)에 포함되는 하나 이상의 컴포넌트일 수 있다.

[0288] 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0289] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0290] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0291] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(12)와 연결될 수도 있다.

[0292] 이상에서 대표적인 실시예를 통하여 본 발명에 대하여 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 전술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0293] 10: 컴퓨팅 환경

12: 컴퓨팅 장치

14: 프로세서

16: 컴퓨터 판독 가능 저장 매체

18: 통신 버스

20: 프로그램

22: 입출력 인터페이스

24: 입출력 장치

26: 네트워크 통신 인터페이스

100: 시스템

110: 셋업 장치

120-1, 120-2, 120-m: 부분 서명 생성 장치

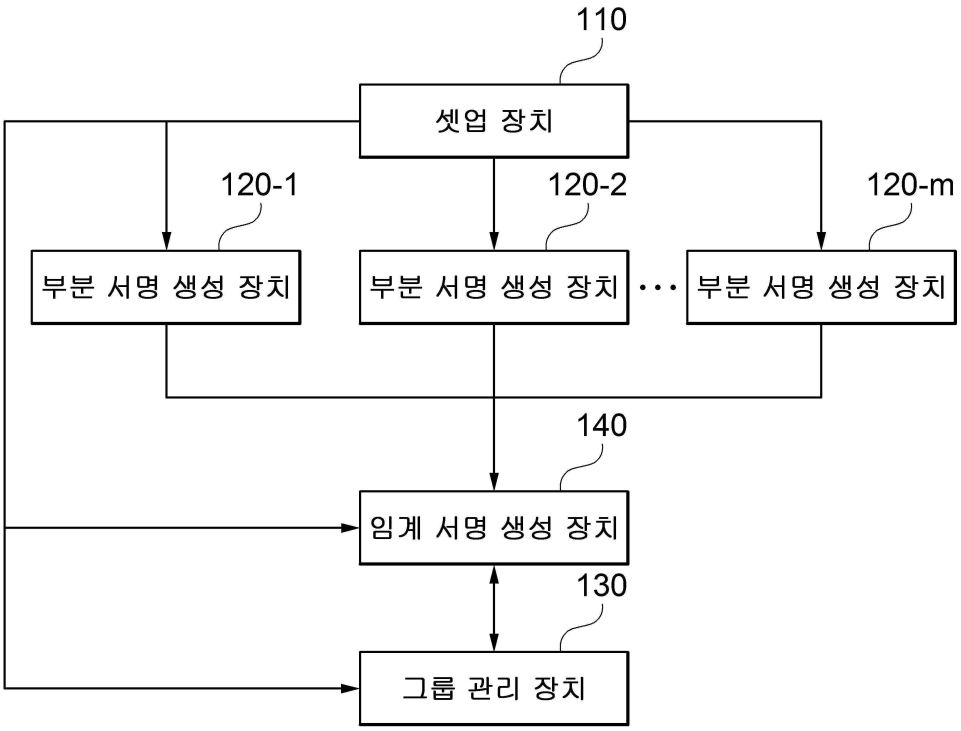
130: 그룹 관리 장치

140: 임계 서명 생성 장치

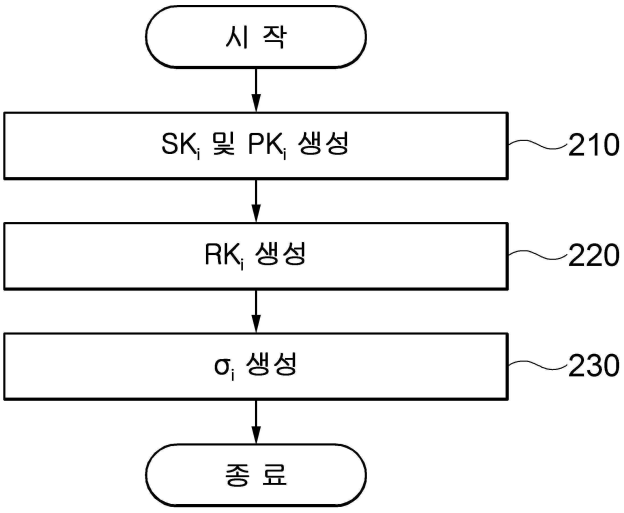
도면

도면1

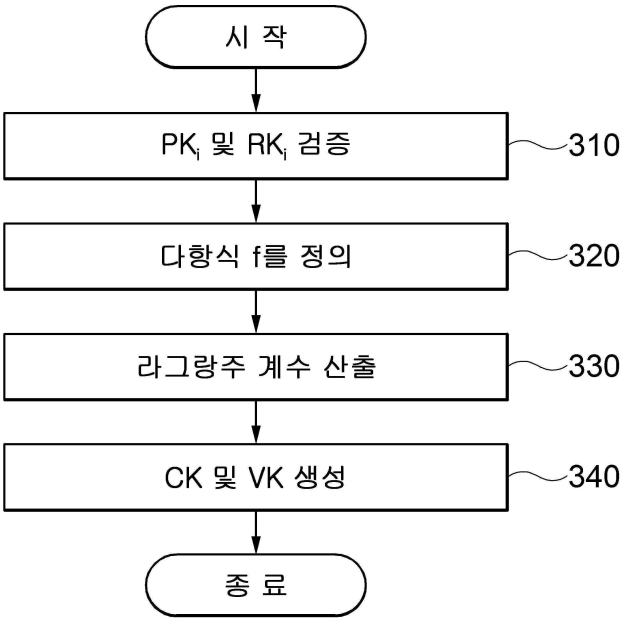
100



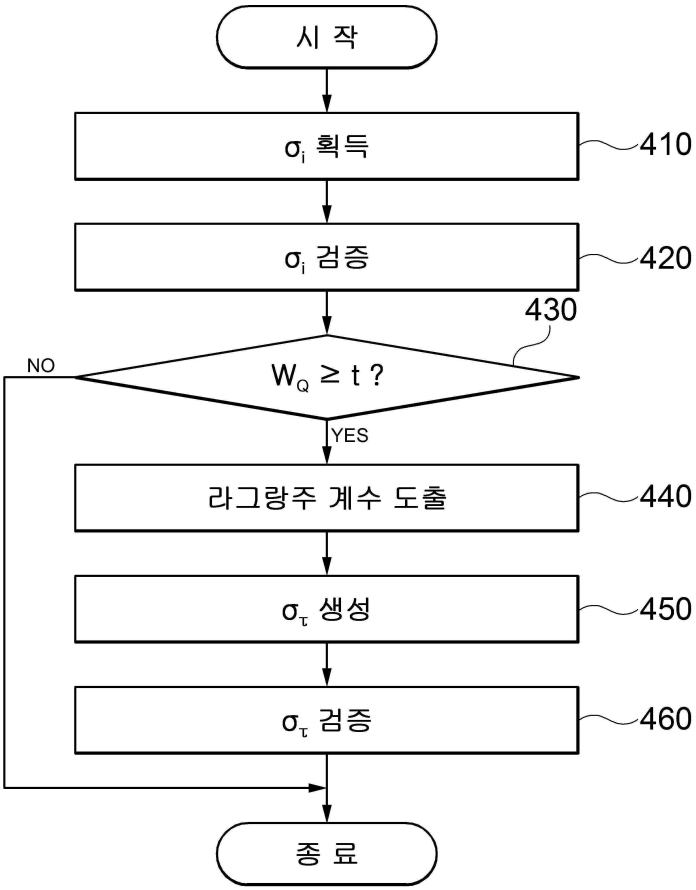
도면2



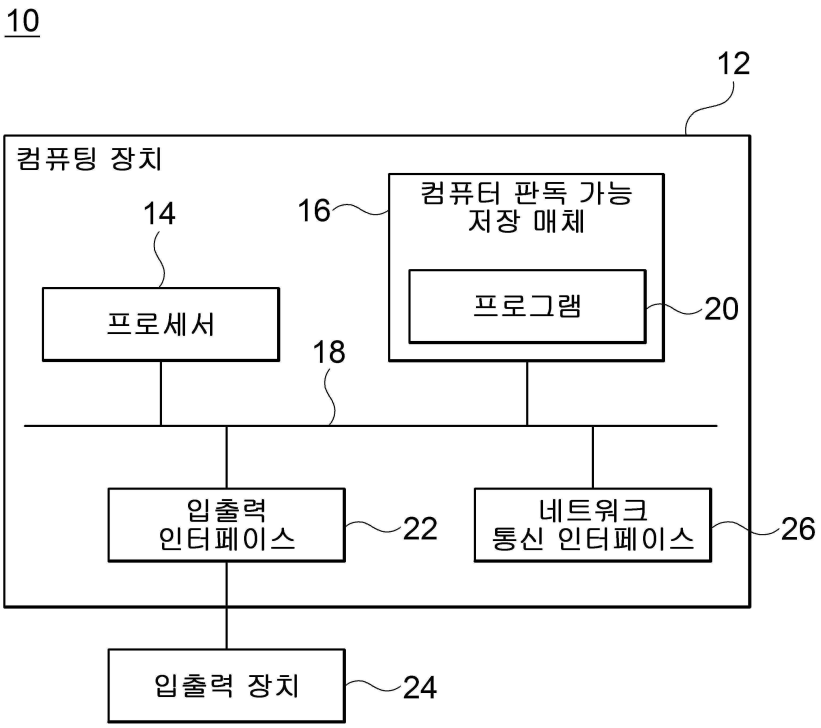
도면3


시 작
PKi 및 RKi 검증
310
다항식 f를 정의
320
라그랑주 계수 산출
330
CK 및 VK 생성
340
종 료

도면4


시 작
σi 획득
410
σi 검증
420
430
WQ ≥ t ?
NO
YES
라그랑주 계수 도출
440
στ 생성
450
στ 검증
460
종 료

도면5


10
12
컴퓨팅 장치
14
프로세서
16
컴퓨터 판독 가능
저장 매체
프로그램
20
18
입출력
인터페이스
22
네트워크
통신 인터페이스
26
입출력 장치
24