(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0103081
(43) 공개일자 2014년08월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/20 (2006.01) *H04L 9/12* (2006.01)
(21) 출원번호 10-2014-0017453
(22) 출원일자 2014년02월14일
심사청구일자 없음
(30) 우선권주장
13305176.3 2013년02월15일
유럽특허청(EPO)(EP)
13305371.0 2013년03월26일
유럽특허청(EPO)(EP)

(71) 출원인
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 잔 다르크 뤼 1-5
(72) 발명자
좌, 마르끄
프랑스 쎄쏭 쎄비네 35 576 쎄 에스 176 16 자크 데 샹 블랑 아브뉘 데 샹 블랑 975 떼끄니꼴로르 에르 에 데 프랑스
리베르, 브누와
프랑스 쎄쏭 쎄비네 35 576 쎄 에스 176 16 자크 데 샹 블랑 아브뉘 데 샹 블랑 975 떼끄니꼴로르 에르 에 데 프랑스
(74) 대리인
백만기, 양영준, 전경석

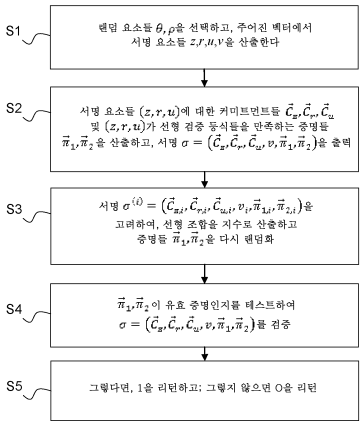
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **선형 준동형 구조-보존 서명을 생성 및 검증하기 위한 암호화 디바이스 및 방법**

(57) 요 약

벡터 $(M_1,\ldots,M_n)\in\mathbb{G}^n$ 에서 선형 준동형 구조-보존 서명 σ은, 프로세서(120)에서, 서명 키 $sk=\{x_i,y_i,\delta_i\}_{i=1}^n$를 사용하여, $z=\prod_{i=1}^n M_i^{-x_i}$, $r=\prod_{i=1}^n M_i^{-y_i}$, $u=\prod_{i=1}^n M_i^{-\delta_i}$를 계산함으로써 서명 요소들 (z,r,u)를 산출하고, 서명 요소들 (z,r,u)을 포함하는 서명 σ를 출력함으로써, 생성된다. 서명은, 프로세서(220)에서, $(M_1,\ldots,M_n)\neq(1_{\mathbb{G}},\ldots,1_{\mathbb{G}})$이고, (z,r,u)이 등식들 $1_{\mathbb{G}_T}=e(g_z,z)\cdot e(g_r,r)\cdot\prod_{i=1}^n e(g_i,M_i)$, $1_{\mathbb{G}_T}=e(h_z,z)\cdot e(h,u)\cdot\prod_{i=1}^n e(h_i,M_i)$을 만족하는지를 검증하고; 검증이 성공적인 경우에 서명은 성공적으로 검증된 것으로 결정하고 그렇지 않으면 서명은 성공적으로 검증되지 않은 것으로 결정함으로써 검증된다. 또한, 완전한 스킴(fully-fledged scheme)과 컨텍스트-은폐 스킴(context-hiding scheme)이 제공된다.

대 표 도 - 도2



특허청구의 범위

청구항 1

벡터 $(M_1,\ldots,M_n)\in\hat{\mathbb{G}}^n$ 에서 선형 준동형 서명(linearly homomorphic signature) σ을 생성하는 방법 - $\hat{\mathbb{G}}$는 제1 그룹을 나타냄 - 으로서,

디바이스(100)의 프로세서(120)에서,

서명 키 $sk=\{\chi_i,\gamma_i,\delta_i\}_{i=1}^n$ 를 사용하여, $z=\prod_{i=1}^n M_i^{-\chi_i}$, $r=\prod_{i=1}^n M_i^{-\gamma_i}$, $u=\prod_{i=1}^n M_i^{-\delta_i}$를 계산함으로써 서명 요소들(z,r,u)를 산출하는 단계, 및

상기 서명 요소들 (z,r,u)을 포함하는 상기 서명 σ를 출력하는 단계

를 포함하는 선형 준동형 서명 생성 방법.

청구항 2

제1항에 있어서, 상기 서명 키는 요소 $h_z^{\alpha_r}$ 를 더 포함하고,

상기 방법은,

랜덤 요소들 $\theta,\rho\xleftarrow{R}\mathbb{Z}_p$ 을 선택하는 단계; 및

추가 서명 요소 $v=h^{\rho}$를 산출하는 단계 - h는 제2 그룹의 요소임 -

를 더 포함하고,

z의 계산은 g_r^{θ}의 곱을 더 포함하고, r의 계산은 $g_z^{-\theta}$ 의 곱을 더 포함하고, u의 계산은 $(h_z^{\alpha_r})^{-\theta}$

의 곱을 더 포함하고, α^r은 정수이고, h, g_r 및 g_z는 상기 제2 그룹의 요소들이고;

상기 서명은 상기 서명 요소 v를 더 포함하고;

상기 제1 그룹 및 상기 제2 그룹은 동일한 선형 준동형 서명 생성 방법.

청구항 3

벡터 $(M_1,\ldots,M_n)\in\hat{\mathbb{G}}^n$ 에 대한 서명 요소들 (z,r,u)를 포함하는 선형 준동형 서명 σ를 검증하는 방법 - $\hat{\mathbb{G}}$는 제1 그룹을 나타냄 - 으로서,

디바이스(200)의 프로세서(220)에서,

$(M_1,\ldots,M_n)\neq(1_{\hat{\mathbb{G}}},\ldots,1_{\hat{\mathbb{G}}})$ 이고, (z,r,u)가 제1 등식 $1_{\mathbb{G}_T}=e(g_z,z)\cdot e(g_r,r)\cdot\prod_{i=1}^n e(g_i,M_i)$ 및 제2 등식 $1_{\mathbb{G}_T}=e(h_z,z)\cdot e(h,u)\cdot\prod_{i=1}^n e(h_i,M_i)$를 만족하는지를 검증 - $e(\cdot,\cdot)$는 대칭 및 가환성 페어링(symmetric and commutative pairing)을 나타내고, h, h_z, h_i, g_r, g_i 및 g_z는 제2 그룹의 요소들임 - 하는 단계; 및

상기 검증들이 성공적인 경우에 상기 서명이 성공적으로 검증된 것으로 결정하고 그렇지 않으면 상기 서명이 성공적으로 검증되지 않은 것으로 결정하는 단계

를 포함하는 선형 준동형 서명 검증 방법.

청구항 4

제3항에 있어서, 상기 제2 등식은 항 $e(H_G(\tau),v)$를 더 포함하는데, $H_G(\tau)$는 해시 함수를 나타내고, τ는 서명된 벡터들이 있는 서브스페이스의 식별자를 나타내는 것인 선형 준동형 서명 검증 방법.

청구항 5

벡터 $(M_1,\ldots,M_n)\in\hat{\mathbb{G}}^n$에 대한 선형 준동형 서명 σ를 생성하기 위한 디바이스(100) - $\hat{\mathbb{G}}$는 제1 그룹을 나타냄 - 로서,

프로세서(120)

를 포함하고,

상기 프로세서(120)는,

서명 키 $sk=\{x_i,y_i,\delta_i\}_{i=1}^n$를 사용하여, $z=\prod_{i=1}^n M_i^{-x_i}$, $r=\prod_{i=1}^n M_i^{-y_i}$, $u=\prod_{i=1}^n M_i^{-\delta_i}$를 계산함으로써 서명 요소들(z,r,u)를 산출하고,

상기 서명 요소들 (z,r,u)를 포함하는 상기 서명 σ를 출력하도록 구성되는 선형 준동형 서명 생성 디바이스.

청구항 6

제5항에 있어서, 상기 서명 키는 요소 $h_z^{\alpha_r}$를 더 포함하고, 상기 프로세서는:

랜덤 요소 $\theta,\rho\xleftarrow{R}\mathbb{Z}_p$를 선택하고;

추가 서명 요소 $v=h^{\rho}$를 계산 - h는 제2 그룹의 요소임 - 하도록 더 구성되며,

z의 계산은 g_r^{θ}의 곱을 더 포함하고, r의 계산은 $g_z^{-\theta}$의 곱을 더 포함하고, u의 계산은 $(h_z^{\alpha_r})^{-\theta}$의 곱을 더 포함하는데, α_r은 정수이고, h, g_r 및 g_z는 상기 제2 그룹의 요소들이고;

상기 서명은 상기 서명 요소 v를 더 포함하고;

상기 제1 그룹 및 상기 제2 그룹은 동일한 것인 선형 준동형 서명 생성 디바이스.

청구항 7

벡터 $(M_1,\ldots,M_n)\in\hat{\mathbb{G}}^n$에 대한 서명 요소들 (z,r,u)를 포함하는 선형 준동형 서명 σ를 검증하기 위한 디바이스(200) - $\hat{\mathbb{G}}$는 제1 그룹을 나타냄 - 로서,

프로세서(220)

를 포함하고,

상기 프로세서(220)는,

$(M_1,\ldots,M_n)\neq(1_{\hat{\mathbb{G}}},\ldots,1_{\hat{\mathbb{G}}})$이고 (z,r,u)가 제1 등식 $1_{\mathbb{G}_T}=e(g_z,z)\cdot e(g_r,r)\cdot\prod_{i=1}^n e(g_i,M_i)$ 및 제2 등식 $1_{\mathbb{G}_T}=e(h_z,z)\cdot e(h,u)\cdot\prod_{i=1}^n e(h_i,M_i)$를 만족하는지를 검증 - $e(\cdot,\cdot)$는 대칭 및 가환성 페어링(symmetric and commutative pairing)을 나타내고, h, h_z, h_i, g_r, g_i 및 g_z는 제2 그룹의 요소들임 - 하고;

상기 검증들이 성공적인 경우에 상기 서명이 성공적으로 검증된 것으로 결정하고 그렇지 않으면 상기 서명이 성공적으로 검증되지 않은 것으로 결정하도록 구성된 선형 준동형 서명 검증 디바이스.

청구항 8

제7항에 있어서, 상기 제2 등식은 항 e($H_G(\tau)$,v)를 더 포함하는데, $H_G(\tau)$은 해시 함수를 나타내고, τ는 서명된 벡터들이 있는 서브스페이스의 식별자를 나타내는 것인 선형 준동형 서명 검증 디바이스.

청구항 9

벡터 $(M_1,\ldots,M_n)\in\hat{\mathbb{G}}^n$ 에 대한 선형 준동형 서명 σ를 생성하기 위한 디바이스(100) - $\hat{\mathbb{G}}$는 제1 그룹을 나타냄 - 로서,

프로세서(120)

를 포함하고,

상기 프로세서(120)는,

서명 키 $\mathrm{sk}=\{h_z^{\alpha_r},\chi_i,\gamma_i,\delta_i\}_{i=1}^n$ 를 사용 - h_z는 제2 그룹의 멤버이고, α_r은 정수임 - 하여, $z=g_r^{\theta}\cdot\prod_{i=1}^n M_i^{-\chi_i}$, $r=g_z^{-\theta}\cdot\prod_{i=1}^n M_i^{-\gamma_i}$, $u=(h_z^{\alpha_r})^{-\theta}\cdot\prod_{i=1}^n M_i^{-\delta_i}$, $v=h^{\rho}$ 를 계산함으로써 서명 요소들 (z,r,u,v)을 산출 - $H_G(\tau)$는 해시 함수를 나타내고, τ는 서명된 벡터들이 있는 서브스페이스의 식별자를 나타냄 - 하고;

z, r 및 u에 대한 커미트먼트들(commitments)을 각각 생성하고;

z, r 및 u에 대한 상기 커미트먼트들을 사용하여, z, r 및 u는 미리 결정된 검증 알고리즘들을 만족한다는 증명들을 생성하고;

상기 서명 요소 v와, z, r 및 u에 대한 상기 커미트먼트들, 및 상기 증명들을 포함하는 상기 서명 σ를 출력하도록 구성된 선형 준동형 서명 생성 디바이스.

청구항 10

벡터 $(M_1,\ldots,M_n)\in\hat{\mathbb{G}}^n$ 에 대한 선형 준동형 서명 σ를 검증하기 위한 디바이스(200) - $\hat{\mathbb{G}}$는 제1 그룹을 나타내고, 상기 선형 준동형 서명 σ는 제1 서명 요소 v, 벡터들 $\vec{f}_1,\vec{f}_2,\vec{f}_3$을 사용하여 생성된, 추가 서명 요소들 z, r 및 u 각각에 대한 커미트먼트들 $\vec{C}_z,\vec{C}_r,\vec{C}_u$, 및 z, r 및 u가 미리 결정된 검증 알고리즘들을 만족한다는 증명들 $\vec{\pi}_1,\vec{\pi}_2$을 포함함 - 로서,

프로세서(220)

를 포함하고,

상기 프로세서(220)는,

$(M_1,\ldots,M_n)\neq(1_{\hat{\mathbb{G}}},\ldots,1_{\hat{\mathbb{G}}})$ 와 상기 검증들 $\prod_{i=1}^n E(g_i,(1_{\hat{\mathbb{G}}},1_{\hat{\mathbb{G}}},M_i))^{-1}=E(g_z,\vec{C}_z)\cdot E(g_r,\vec{C}_r)\cdot E(\pi_{1,1},\vec{f}_1)\cdot E(\pi_{1,2},\vec{f}_2)\cdot E(\pi_{1,3},\vec{f}_3)$ 및 $\prod_{i=1}^n E(h_i,(1_{\hat{\mathbb{G}}},1_{\hat{\mathbb{G}}},M_i))^{-1}\cdot E(H_{\hat{\mathbb{G}}}(\tau),(1_{\hat{\mathbb{G}}},1_{\hat{\mathbb{G}}},v))^{-1}=E(h_z,\vec{C}_z)\cdot E(h,\vec{C}_u)\cdot E(\pi_{2,1},\vec{f}_1)\cdot E(\pi_{2,2},\vec{f}_2)\cdot E(\pi_{2,3},\vec{f}_3)$ 를 검증 - $E(\cdot,\cdot)$는 좌표-별 페어링(coordinate-wise pairing)을 나타내고, h, h_z, h_i, g_r, g_i 및 g_z는 제2 그룹의 요소들임 - 하고;

상기 검증이 성공적인 경우에 상기 서명이 성공적으로 검증된 것으로 결정하고 그렇지 않으면 상기 서명이 성공적으로 검증되지 않은 것으로 결정하도록 구성된 선형 준동형 서명 검증 디바이스.

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 암호화에 관한 것으로, 특히, 선형 준동형 구조-보존 서명(linearly homomorphic structure-preserving signatures)에 관한 것이다.

배 경 기 술

[0002] 이 섹션은, 아래 설명 및/또는 청구되는 본 발명의 다양한 양태와 관련될 수 있는 기술의 다양한 양태를 독자에게 소개하도록 의도된다. 이러한 논의는 본 발명의 다양한 양태의 보다 나은 이해를 용이하게 하기 위하여 배경 정보를 독자에게 제공하는 데 도움이 될 것으로 여겨진다. 따라서, 이러한 진술들은, 종래 기술을 인정하는 것이 아니라, 이러한 견지에서 읽혀져야 한다는 것을 이해해야 한다.

[0003] 선형 준동형 서명(linearly homomorphic signatures)은 암호화에 대한 기술 분야에서 잘 알려져 있다. 이는, *PKC'09, Lecture Notes in Computer Science*, 5443권, 68-87페이지(2009)에 있는, D. Boneh, D. Freeman, J. Katz, B. Waters에 의한, Signing a Linear Subspace: Signature Schemes for Network Coding에 정의되어 있다.

[0004] 다음에 있는 선형 준동형 서명에 대한 다른 예들이 사용가능하다:

[0005] ● 2010년 6월 22일 발행된, US 7743253; D.-X. Charles, K. Jain, K. Lauter에 의한, Digital signature for network coding.

[0006] ● *PKC'09, Lecture Notes in Computer Science*, 5443권, 68-87페이지(2009)에 있는, D. Boneh, D. Freeman, J. Katz, B. Waters에 의한, Signing a Linear Subspace: Signature Schemes for Network Coding.

[0007] ● *PKC'10, Lecture Notes in Computer Science*, 6056권, 142-160페이지(2010)에 있는, R. Gennaro, J. Katz, H. Krawczyk, T. Rabin에 의한, Secure Network Coding over the Integers.

[0008] ● *PKC'11, Lecture Notes in Computer Science*, 6571권, 17-34페이지(2011)에 있는, N. Attrapadung, B. Libert에 의한, Homomorphic Network Coding Signatures in the Standard Model.

[0009] ● *PKC'11, Lecture Notes in Computer Science*, 6571권, 1-16페이지(2011)에 있는, D. Boneh, D. Freeman에 의한, Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures.

[0010] ● *Eurocrypt'11, Lecture Notes in Computer Science*, 6632권, 149-168페이지(2011)에 있는, D. Boneh, D. Freeman에 의한, Homomorphic Signatures for Polynomial Functions.

[0011] ● *PKC'12, Lecture Notes in Computer Science*, 7293권, 697-714페이지(2012)에 있는, D. Freeman에 의한, Improved security for linearly homomorphic signatures: A generic framework.

[0012] ● *Eurocrypt'11, Lecture Notes in Computer Science*, 6632권, 207-223페이지(2011)에 있는, D. Catalano, D. Fiore, B.Warinschi에 의한, Adaptive Pseudo-free Groups and Applications.

[0013] ● *PKC'12, Lecture Notes in Computer Science*, 7293권, 680-696페이지(2012)에 있는, D. Catalano, D. Fiore, B.Warinschi에 의한, Efficient Network Coding Signatures in the Standard Model.

[0014] 표준 가정 하에 표준 모델에서 안전하다고 입증된 스킴들 중에서, 가장 효율적인 스킴은 *Asiacrypt'12,* LNCS, 7658권, 367-385페이지(2012)에 있는, N. Attrapadung, B. Libert, T. Peters에 의한, Computing on Authenticated Data: New Privacy Definitions and Constructions에 있는 것으로 나타났다.

[0015] 컨스트럭션(construction)은 가법 그룹(additive group)(Z_p,+)에 걸쳐 준동형이다. 즉, 근본적인 순환 그룹(underlying cyclic group)은 $G=Z_p$이고, 서명된 메시지는 파일 식별자 $\tau\in\{0,1\}^L$ 및 벡터 Z_p^n으로 구성되어 있다. 스킴은 프라임 오더(prime order) p의 그룹들 $(\mathbb{G},\hat{\mathbb{G}},\mathbb{G}_T)$ 사이에 정의된 바이리니어 맵(bilinear map) $e:\mathbb{G}x\hat{\mathbb{G}}\rightarrow\mathbb{G}_T$을 이용한다.

[0016] Keygen(λ,n): 서명할 벡터의 차원(dimension)을 나타내는 정수 $n\in poly(\lambda)$ 및 보안 파라미터 $\lambda\in N$을 고려하여, 프라임 오더 $p>2^\lambda$의 바이리니어 그룹(bilinear groups) $(\mathbb{G},\hat{\mathbb{G}},\mathbb{G}_T)$을 선택한다. 일부 $L\in poly(\lambda)$에 대한 $\alpha\xleftarrow{R}\mathbb{Z}_p,\hat{g}\xleftarrow{R}\hat{\mathbb{G}},v\xleftarrow{R}\mathbb{G}$ 및 $u_0,u_1,\ldots,u_L\xleftarrow{R}\mathbb{G}$를 선택한다. 이러한 요소들 $(u_0,u_1,\ldots,u_L)\in\mathbb{G}^{L+1}$은 수 이론적 해시 함수 $H_G:\{0,1\}^L\rightarrow G$를 구현하는 데 사용되어, 임의의 L-비트 스트링 m=m[1]...m[L]$\in\{0,1\}^L$은 해시 값 $H_G(m)=u_0\cdot\prod_{i=1}^{L}u_i^{m[i]}$를 갖는다. $g_i\xleftarrow{R}\mathbb{G}$(i=1내지 n)를 선택한다. 마지막으로, 식별자 공간 $T:=\{0,1\}^L$를 정의한

다. 개인 키는 sk:=α이고, 공개 키는 다음과 같이 구성된다.

[0017] $$pk := \left((\mathbb{G},\mathbb{G}_T),\hat{g},\hat{g}^{\alpha},v,\{g_i\}_{i=1}^{n},\{u_i\}_{i=0}^{L}\right)$$

[0018] $\mathbf{Sign}(sk,\tau,\vec{v})$: 벡터 $\vec{v}=(v_1,\ldots v_n)\in\mathbb{Z}_p^n$, 파일 식별자 $\tau:=\{0,1\}^L$ 및 개인 키 sk = $\alpha\in Z_p$를 고려하여, $r,s\overset{R}{\leftarrow}\mathbb{Z}_p$를 선택한다. 그 다음, 서명 $\sigma=(\sigma_1,\sigma_2,s)\in\mathbb{G}\times\hat{\mathbb{G}}\times\mathbb{Z}_p$를 다음과 같이 산출한다.

[0019] $$\sigma_1=(g_1^{v_1}\cdots g_n^{v_n}\cdot v^{s})^{\alpha}\cdot H_{\mathbb{G}}(\tau)^{r},\qquad \sigma_2=\hat{g}^{r}$$

[0020] $SignDerive(pk,\tau,\{(\beta_i,\sigma^{(i)})\}_{i=1}^{l})$: pk, 파일 식별자 τ 및 l 투플 $(\beta_i,\sigma^{(i)})$를 고려하여, 각각의 $\sigma^{(i)}$를 $\sigma^{(i)}=(\sigma_{i,1},\sigma_{i,2},s_i)$(i=1 내지 l)로서 분석(parse)한다. $\hat{r}\overset{R}{\leftarrow}\mathbb{Z}_p$를 선택한다. 그 다음, (σ_1,σ_2,s)를 산출 및 출력하는데, 여기서

[0021] $$\sigma_1=\prod_{i=1}^{l}\sigma_{i,1}^{\beta_i}\cdot H_{\mathbb{G}}(\tau)^{\hat{r}}\qquad \sigma_2=\prod_{i=1}^{l}\sigma_{i,2}^{\beta_i}\cdot\hat{g}^{\hat{r}}\qquad s=\sum_{i=1}^{l}\beta_i\cdot s_i$$

[0022] $\mathbf{Verify}(pk,\tau,\vec{y},\sigma)$: pk, 서명 $\sigma=(\sigma_1,\sigma_2,s)$ 및 메시지 $(\tau,\vec{y})$를 고려하여 - 여기서 $\tau\in\{0,1\}^L$이고 $\vec{y}=(y_1,\ldots,y_n)\in(\mathbb{Z}_p)^n$임 - , $\vec{y}=\vec{0}$인 경우, ⊥를 리턴한다. 그렇지 않으면, $e(\sigma_1,\hat{g})=e(g_1^{y_1}\cdots g_n^{y_n}\cdot v^{s},\hat{g}^{\alpha})\cdot e(H_{\mathbb{G}}(\tau),\sigma_2)$이기만 한다면 1을 리턴한다.

[0023] 컨스트럭션에서, 올-제로 벡터(all-zero vector) $\vec{0}$에 대한 서명은 허용되지 않는다는 것을 이해할 수 있을 것이다. 선형 준동형 서명의 모든 애플리케이션에서, 적당한 길이의 단위 벡터 (0,...,1,...,0)가 서명된 벡터들에 첨부되므로 이것은 제한이 아니다.

[0024] Attrapadung 등에 의한 논문에서, 위의 스킴은 디피-헬만 가정의 변형 하에 위조불가능한 것으로 입증되었다. 이 가정은, 랜덤으로 선택된 a,b ∈ Zp에 대해 $(g,\hat{g},g^{a},\hat{g}^{b})\in(\mathbb{G}\times\hat{\mathbb{G}})^2$ - 여기서, $(\mathbb{G},\hat{\mathbb{G}})$는 오더 p의 순환 바이리니어 그룹임 - 를 고려할 때, 어떠한 PPT(Probabilistic Polynomial Time) 알고리즘도 g^{ab}를 산출할 수 없음을 상정한다. 앞선 버전에서, 스킴은 컨텍스트를 완전히 은폐하고 있지 않다(즉, 파생된 서명이 원래 서명에 통계적으로 독립적이지 않다). Attrapadung 등은, 서명 길이를 증가하는 비용으로 컨텍스트를 완전히 은폐하게 할 수 있도록 스킴을 수정하는 방법을 보여 주었다[*PKC'13*, LNCS, 7778권, 386-404페이지(2013)에 있는, N. Attrapadung, B. Libert, T. Peters에 의한, Efficient Completely Context-Hiding Quotable Signatures and Linearly Homomorphic Signatures 참고].

[0025] 종래 기술에서의 선형 준동형 서명은 각각의 벡터의 좌표가 $(Z_p,+)$와 같은 그룹에 속하는 벡터 공간에 대해서만 존재하는데, 이는 이산 대수를 산출하기 쉽다. 따라서, 유한 오더 p의 이산-대수-하드 그룹(discrete-logarithm-hard group) G에 좌표가 있는 벡터 $\vec{M}_1\in\mathbb{G}^n$를 처리할 수 있는 스킴을 갖는 것이 바람직한 것임을 알 수 있을 것이다. 하나의 주요 어려움은, 이러한 그룹에서, 보통, 복수의 벡터 $\vec{M}_1,\ldots,\vec{M}_{n-1}\in\mathbb{G}^n$가 선형 종속적인지 여부를 결정하는 것이 어렵다는 점이다. 일반적으로, n>2에 대해, 이를 수행하는 유일한 알려진 방법은 Z_p에서 모든 좌표의 이산 대수를 산출하는 것이다.

[0026] 따라서, 메시지들이 특정 대수 구조(special algebraic structure), 즉, "구조-보존(structure-preserving)" 서명 스킴을 갖는 요소들일 수 있는 선형 준동형 서명 스킴을 갖는 것이 바람직하다는 것을 이해할 수 있을 것이다. 본 발명은 그러한 스킴을 제공한다.

발명의 내용

[0027] 제1 양태에서, 본 발명은 벡터 $(M_1,\ldots,M_n)\in\hat{\mathbb{G}}^n$에 대한 선형 준동형 서명 σ를 생성하기 위한 방법에 관한 것으

로, 여기서, $\mathbb{G}$는 제1 그룹을 나타낸다. 디바이스의 프로세서는, 서명 키 $sk = \{\chi_i, \gamma_i, \delta_i\}_{i=1}^{n}$를 사용하여, $z = \prod_{i=1}^{n} M_i^{-\chi_i}$, $r = \prod_{i=1}^{n} M_i^{-\gamma_i}$, $u = \prod_{i=1}^{n} M_i^{-\delta_i}$를 계산함으로써 서명 요소들 (z,r,u)을 산출하고, 서명 요소들 (z,r,u)을 포함하는 서명 σ를 출력한다.

[0028] 바람직한 실시예에서, 서명 키는 요소 $h_z^{\alpha_r}$를 더 포함하고, 프로세서는 또한 랜덤 요소 $\theta, \rho \xleftarrow{R} \mathbb{Z}_n$를 선택하고; 추가 서명 요소 $v = h^{\rho}$를 계산하고, 여기서, h는 제2 그룹의 요소이고; 여기서, z의 계산은 g_r^{θ}의 곱을 더 포함하고, r의 계산은 $g_z^{-\theta}$의 곱을 더 포함하고, u의 계산은 $(h_z^{\alpha_r})^{-\theta}$의 곱을 더 포함하고, 여기서, α_r은 정수이고, h, g_r 및 g_z는 제2 그룹의 요소들이고; 여기서, 서명은 서명 요소 v를 더 포함하고; 여기서, 제1 그룹 및 제2 그룹은 동일하다.

[0029] 제2 양태에서, 본 발명은 벡터 $(M_1, \ldots, M_n) \in \mathbb{G}^n$에 대한 서명 요소들 (z,r,u)를 포함하는 선형 준동형 서명 σ를 검증하는 방법에 관한 것으로, 여기서, $\mathbb{G}$는 제1 그룹을 나타낸다. 디바이스의 프로세서는, $(M_1, \ldots, M_n) \neq (1_{\mathbb{G}}, \ldots, 1_{\mathbb{G}})$이고 (z,r,u)가 제1 등식 $1_{G_T} = e(g_z, z) \cdot e(g_r, r) \cdot \prod_{i=1}^{n} e(g_i, M_i)$ 및 제2 등식 $1_{G_T} = e(h_z, z) \cdot e(h, u) \cdot \prod_{i=1}^{n} e(h_i, M_i)$를 만족하는지를 검증 - 여기서, $e(\cdot,\cdot)$는 대칭 및 가환성 페어링(symmetric and commutative pairing)을 나타내고, 여기서 h, h_z, h_i, g_r, g_i 및 g_z는 제2 그룹의 요소들임 - 하고; 검증이 성공적인 경우에 서명이 성공적으로 검증된 것으로 결정하고 그렇지 않으면 서명이 성공적으로 검증되지 않은 것으로 결정한다.

[0030] 제1 실시예에서, 제2 등식은 항 $e(H_G(\tau), v)$를 더 포함하는데, 여기서, $H_G(\tau)$는 해시 함수를 나타내고, τ는 서명된 벡터가 있는 서브스페이스의 식별자를 나타낸다.

[0031] 제3 양태에서, 본 발명은 벡터 $(M_1, \ldots, M_n) \in \mathbb{G}^n$에 대한 선형 준동형 서명 σ를 생성하기 위한 디바이스에 관한 것으로, 여기서, $\mathbb{G}$는 제1 그룹을 나타낸다. 디바이스는, 서명 키 $sk = \{\chi_i, \gamma_i, \delta_i\}_{i=1}^{n}$를 사용하여, $z = \prod_{i=1}^{n} M_i^{-\chi_i}$, $r = \prod_{i=1}^{n} M_i^{-\gamma_i}$, $u = \prod_{i=1}^{n} M_i^{-\delta_i}$를 계산함으로써 서명 요소들 (z,r,u)을 산출하고, 서명 요소들 (z,r,u)을 포함하는 서명 σ를 출력하도록 구성된 프로세서를 포함한다.

[0032] 제1 실시예에서, 서명 키는 요소 $h_z^{\alpha_r}$를 더 포함하고, 프로세서는 또한 랜덤 요소 $\theta, \rho \xleftarrow{R} \mathbb{Z}_n$를 선택하고; 추가 서명 요소 $v = h^{\rho}$를 계산 - 여기서, h는 제2 그룹의 요소임 - 하도록 구성되는데; 여기서, z의 계산은 g_r^{θ}의 곱을 더 포함하고, r의 계산은 $g_z^{-\theta}$의 곱을 더 포함하고, u의 계산은 $(h_z^{\alpha_r})^{-\theta}$의 곱을 더 포함하고, 여기서, α_r은 정수이고, h, g_r 및 g_z는 제2 그룹의 요소들이고; 여기서, 서명은 서명 요소 v를 더 포함하고; 여기서, 제1 그룹 및 제2 그룹은 동일하다.

[0033] 제4 양태에서, 본 발명은 벡터 $(M_1, \ldots, M_n) \in \mathbb{G}^n$에 대한 서명 요소들 (z,r,u)를 포함하는 선형 준동형 서명 σ를 검증하기 위한 디바이스에 관한 것으로, 여기서, $\mathbb{G}$는 제1 그룹을 나타낸다. 디바이스는, $(M_1, \ldots, M_n) \neq (1_{\mathbb{G}}, \ldots, 1_{\mathbb{G}})$이고 (z,r,u)가 제1 등식 $1_{G_T} = e(g_z, z) \cdot e(g_r, r) \cdot \prod_{i=1}^{n} e(g_i, M_i)$ 및 제2 등식 $1_{G_T} = e(h_z, z) \cdot e(h, u) \cdot \prod_{i=1}^{n} e(h_i, M_i)$를 만족하는지를 검증 - 여기서, $e(\cdot,\cdot)$는 대칭 및 가환성 페어링(symmetric and commutative pairing)을 나타내고, 여기서, h, h_z, h_i, g_r, g_i 및 g_z는 제2 그룹의 요소들임 - 하고; 검증이 성

공적인 경우에 서명이 성공적으로 검증된 것으로 결정하고 그렇지 않으면 서명이 성공적으로 검증되지 않은 것으로 결정하도록 구성된 프로세서를 포함한다.

[0034] 제1 실시예에서, 제2 등식은 항 $e(H_G(\tau),v)$를 더 포함하는데, 여기서, $H_G(\tau)$는 해시 함수를 나타내고, τ는 서명된 벡터가 있는 서브스페이스의 식별자를 나타낸다.

[0035] 제5 양태에서, 본 발명은 벡터 $(M_1,\ldots,M_n)\in\mathbb{G}^n$에 대한 선형 준동형 서명 σ를 생성하기 위한 디바이스에 관한 것으로, 여기서, $\mathbb{G}$는 제1 그룹을 나타낸다. 디바이스는, 서명 키 $sk=\{h_z^{\alpha_r},\chi_i,\gamma_i,\delta_i\}_{i=1}^n$를 사용 - 여기서, h_z는 제2 그룹의 멤버이고, α_r은 정수임 - 하여, $z=g_r^{\theta}\cdot\prod_{i=1}^n M_i^{-\chi_i}$, $r=g_z^{-\theta}\cdot\prod_{i=1}^n M_i^{-\gamma_i}$, $u=(h_z^{\alpha_r})^{-\theta}\cdot\prod_{i=1}^n M_i^{-\delta_i}$, $v=h^{\rho}$를 계산함으로써 서명 요소들 (z,r,u,v)을 산출 - 여기서, $H_G(\tau)$는 해시 함수를 나타내고, τ는 서명된 벡터가 있는 서브스페이스의 식별자를 나타냄 - 하고; z, r 및 u에 대한 커미트먼트를 각각 생성하고; z, r 및 u에 대한 커미트먼트를 사용하여, z, r 및 u는 미리 결정된 검증 알고리즘을 만족한다는 증명(proof)을 생성하고; 서명 요소 v, z, r 및 u에 대한 커미트먼트, 및 증명을 포함하는 서명 σ를 출력하도록 구성된 프로세서를 포함한다.

[0036] 제6 양태에서, 본 발명은 벡터 $(M_1,\ldots,M_n)\in\mathbb{G}^n$에 대한 선형 준동형 서명 σ를 검증하기 위한 디바이스에 관한 것으로, 여기서, $\mathbb{G}$는 제1 그룹을 나타내고, 선형 준동형 서명 σ는 제1 서명 요소 v, 추가 서명 요소들 z, r 및 u 각각에 대한 커미트먼트들 $\vec{C}_z,\vec{C}_r,\vec{C}_u$, 벡터 $\vec{f}_1,\vec{f}_2,\vec{f}_3$를 사용하여 생성된 커미트먼트들, 및 z, r 및 u가 미리 결정된 검증 알고리즘을 만족한다는 증명들 $\vec{\pi}_1,\vec{\pi}_2$을 포함한다. 디바이스는 $(M_1,\ldots,M_n)\neq(1_{\mathbb{G}},\ldots,1_{\mathbb{G}})$와 검증들 $\prod_{i=1}^n E(g_i,(1_{\mathbb{G}},1_{\mathbb{G}},M_i))^{-1}=E(g_z,\vec{C}_z)\cdot E(g_r,\vec{C}_r)\cdot E(\pi_{1,1},\vec{f}_1)\cdot E(\pi_{1,2},\vec{f}_2)\cdot E(\pi_{1,3},\vec{f}_3)$ 및 $\prod_{i=1}^n E(h_i,(1_{\mathbb{G}},1_{\mathbb{G}},M_i))^{-1}\cdot E(H_{\mathbb{G}}(\tau),(1_{\mathbb{G}},1_{\mathbb{G}},v))^{-1}=E(h_z,\vec{C}_z)\cdot E(h,\vec{C}_u)\cdot E(\pi_{2,1},\vec{f}_1)\cdot E(\pi_{2,2},\vec{f}_2)\cdot E(\pi_{2,3},\vec{f}_3)$를 검증 - 여기서, $E(\cdot,\cdot)$는 좌표-별 페어링(coordinate-wise pairing)을 나타내고, 여기서, h, h_z, h_i, g_r, g_i 및 g_z는 제2 그룹의 요소들임 - ; 검증이 성공적인 경우에 서명이 성공적으로 검증된 것으로 결정하고 그렇지 않으면 서명이 성공적으로 검증되지 않은 것으로 결정하도록 구성된 프로세서를 포함한다.

도면의 간단한 설명

[0037] 본 발명의 바람직한 특징들은 이제 첨부 도면을 참조하여 비 제한적인 예로서 설명될 것이다.

도 1은 본 발명의 바람직한 실시예에 따른 구조-보존 선형 준동형 서명 시스템을 도시한다.

도 2는 본 발명의 바람직한 실시예에 따른 컨텍스트-은폐 선형 준동형 구조-보존 서명을 생성 및 검증하기 위한 방법을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0038] 본 발명의 구조-보존 선형 준동형 서명 스킴은, Cryptology ePrint Archive: Report 2010/133(2010)에서, M. Abe, K. Haralambiev, M. Ohkubo에 의한, Signing on Elements in Bilinear Groups for Modular Protocol Design 및 *Crypto'10*, *Lecture Notes in Computer Science*, 6223권, 209-236페이지(2010)에서, M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, M. Ohkubo에 의한, Structure-Preserving Signatures and Commitments to Group Elements[설명을 위한 첫 번째 문서의 부록 C를 참조]에 제안된 구조-보존 서명 스킴의 변형을 기반으로 한다. 스킴은 준동형인 것으로 여겨지지 않고 여겨지지도 않았으며, 그것은 단지 주어진 공개 키에 대하여 하나의 메시지를 서명하는 것을 허용하는 것임을 이해할 수 있을 것이다.

[0039] 따라서, ($\mathbb{G}^n$인 n-1 선형 독립 벡터에 의해 스팬된) 단지 하나의 선형 서브스페이스가 주어진 키 페어(sk;pk)를 사용하여 서명되는 한, 이산 대수 하드 그룹(discrete-logarithm-hard group)에 대해 선형 준동형 서명 스킴을 얻기 위해 제1 변형이 이루어진다. 이러한 제1 스킴은 다음과 같이 설명될 수 있다. 다음 표기법에서, pp는 프라임 오더 $p>2^{\lambda}$의 그룹 $(\mathbb{G},\hat{\mathbb{G}},\mathbb{G}_T)$으로 구성된 공개 파라미터들의 세트를 나타내는데, 여기서, $\lambda\in\mathbb{N}$은 보안 파

라미터이고, 그에 대해 효율적으로 산출가능한 바이리니어 맵 $e:\mathbb{G}\times\hat{\mathbb{G}}\to\mathbb{G}_T$이 정의된다.

[0040] 도 1은 본 발명의 바람직한 실시예에 따른 준동형 서명을 생성하기 위한 암호화 서명 디바이스(100) 및 준동형 서명의 검증을 위한 암호화 서명 디바이스(200)를 도시한다. 디바이스(100, 200) 각각은 통신을 위해 구성된 적어도 하나의 인터페이스 유닛(110, 210), 적어도 하나의 프로세서("프로세서")(120, 220), 및 누산기와 중개 계산 결과와 같은 데이터를 저장하기 위해 구성된 적어도 하나의 메모리(130, 230)를 포함한다. 도면은 또한, 프로세서(120, 220)에 의해 실행될 때, 각각 본 발명에 따른 서명을 생성 및 검증하는 명령어들이 저장된 CD-ROM 또는 DVD와 같은 제1 및 제2 컴퓨터 프로그램 제품(비 일시적 저장 매체)(140, 240)을 도시한다.

[0041] **1 회용 스킴(One-time scheme):**

[0042] Keygen(pp,n): pp 및 서명할 서브스페이스의 차원 n∈N을 고려하여, 제너레이터 $h,g_z,g_r,z_z\xleftarrow{R}\mathbb{G}$를 선택한다. $\chi_i,\gamma_i,\delta_i\xleftarrow{R}\mathbb{Z}_p$를 선택한다(i=1 내지 n). 그 다음, 각각의 i∈{1,...,n}에 대해, $g_i=g_z^{\chi_i}g_r^{\gamma_i}$, $h_i=h_z^{\chi_i}h^{\delta_i}$를 산출한다. 공개 키는 $\mathrm{pk}=(g_z,h_r,h_z,h,\{g_i,h_i\}_{i=1}^n)\in\mathbb{G}^{2n+4}$로서 정의되고, 개인 키는 $sk=\{\chi_i,\gamma_i,\delta_i\}_{i=1}^n$로서 정의된다.

[0043] Sign(sk,τ(M1,...,Mn)): $sk=\{\chi_i,\gamma_i,\delta_i\}_{i=1}^n$를 사용하여 식별자 τ=ε와 관련된 벡터 $(M_1,\ldots,M_n)\in\hat{\mathbb{G}}^n$에 서명하기 위해,

[0044] $$z=\prod_{i=1}^{n}M_i^{-\chi_i},\quad r=\prod_{i=1}^{n}M_i^{-\gamma_i},\quad u=\prod_{i=1}^{n}M_i^{-\delta_i}$$

[0045] 를 산출한다.

[0046] 서명은 $\sigma=(z,r,u)\in\hat{\mathbb{G}}^3$를 포함한다.

[0047] $SignDerive(pk,\tau,\{(\omega_i,\sigma^{(i)})\}_{i=1}^{l})$: pk, 파일 식별자 τ 및 l 투플 $(\omega_i,\sigma^{(i)})$를 고려하여, 각각의 서명 $\sigma^{(i)}$를 $\sigma^{(i)}=(z_i,r_i,u_i)\in\hat{\mathbb{G}}^3$ (i=1 내지 l)로서 분석한다.

[0048] $$z=\prod_{i=1}^{\ell}z_i^{\omega_i}\quad r=\prod_{i=1}^{\ell}r_i^{\omega_i}\quad u=\prod_{i=1}^{\ell}u_i^{\omega_i}$$

[0049] 를 산출하고, σ = (z,r,u)를 리턴한다.

[0050] Verify(pk,σ,τ(M1,...,Mn)): 서명 $\sigma=(z,r,u)\in\hat{\mathbb{G}}^3$, 벡터 (M1,...,Mn) 및 파일 식별자 τ=ε를 고려하여, $(M_1,\ldots,M_n)\neq(1_{\hat{\mathbb{G}}},\ldots,1_{\hat{\mathbb{G}}})$이고, (z,r,u)가 등식 $1_{\mathbb{G}_T}=e(g_z,z)\cdot e(g_r,r)\cdot\prod_{i=1}^{n}e(g_i,M_i)$, $1_{\mathbb{G}_T}=e(h_z,z)\cdot e(h,u)\cdot\prod_{i=1}^{n}e(h_i,M_i)$를 만족하기만 하면 1을 리턴한다.

[0051] 최대 n-1개의 선형 독립 벡터 $\vec{M}_1,\ldots,\vec{M}_{n-1}$에 대한 서명을 얻는 상대는 SDP(Simultaneous Double Pairing) 가정이 유지되는 한은 벡터 $\vec{M}\notin\mathrm{span}(\vec{M}_1,\ldots,\vec{M}_{n-1})$에 대한 서명을 위조할 수 없다는 것이 증명될 수 있다. Abe, Haralambiev 및 Ohkubo에 의한 논문에서 설명된 SDP 가정은, $(\mathbb{G},\hat{\mathbb{G}})$에서, 요소들 $(g_z,g_r,h_z,h_u)\in G^4$의 투플을 고려하여, $e(g_z\cdot z)\cdot e(g_r\cdot r)=1_{\mathbb{G}_T}$ 및 $e(h_z\cdot z)\cdot e(h_u\cdot u)=1_{\mathbb{G}_T}$이도록 비단순 투플(non-trivial tuple) $(z,r,u)\in\hat{\mathbb{G}}^3\backslash\{(1_{\hat{\mathbb{G}}},1_{\hat{\mathbb{G}}},1_{\hat{\mathbb{G}}})\}$을 찾는 것이다.

[0052] **완전한 스킴(Full-fledged scheme):**

[0053] 1 회용 스킴은 임의의 수의 선형 서브스페이스에 서명하도록 허용하는 선형 컨스트럭션으로 업그레이드될 수 있다. 이렇게 하려면, $\mathbb{G}=\hat{\mathbb{G}}$인 바이리니어 그룹 $(\mathbb{G},\hat{\mathbb{G}})$의 구성이 필요하다. 즉, 바이리니어 맵 e: G×G→G_T는, 대칭 및 가환성이어야 하기 때문에 동일한 그룹 G에서 그의 인수를 모두 가지고 있어야 한다.

[0054] 컨스트럭션에서, 각각의 파일 식별자 τ는, 일부 L∈poly(λ)에 대해, L-비트 스트링으로 구성된다. 각각의 서명의 u 컴포넌트는 파일 식별자 τ에 대해 워터스 서명 $\left(h_z^{\alpha_r}\cdot H_{\mathbb{G}}(\tau)^{-\rho},h^{\rho}\right)$을 갖는 1 회용 스킴의 서명의 집합(aggregation)으로 볼 수 있다[*Eurocrypt'05, Lecture Notes in Computer Science*, 3494권, 114-127페이지(2005)에 있는, B. Waters에 의한, Efficient Identity-Based Encryption Without Random Oracles 참조]. 본 스킴에서, 이러한 워터스 서명은 서명 랜더마이저 Θ∈Z_p에 대한 지원으로 사용된다.

[0055] Keygen(pp,n): pp 및 서명할 서브스페이스의 차원 n∈N을 고려하여, 다음 단계를 수행한다:

[0056] 1. $h\overset{R}{\leftarrow}\mathbb{G}$ 및 $\alpha_z,\alpha_r,\beta_z\overset{R}{\leftarrow}\mathbb{Z}_p$ 선택. $g_z=h^{\alpha_z}$, $g_r=h^{\alpha_r}$ 및 $h_z=h^{\beta_z}$ 정의.

[0057] 2. i= 1 내지 n에 대해, $\chi_i,\gamma_i,\delta_i\overset{R}{\leftarrow}\mathbb{Z}_p$ 를 선택하고, $g_i=g_z^{\chi_i}g_r^{\gamma_i}$, $h_i=h_z^{\chi_i}h^{\delta_i}$ 를 산출.

[0058] 3. τ=τ[1]...τ[L]∈$\{0,1\}^L$를 $H_{\mathbb{G}}(\tau)=w_0\cdot\prod_{k=1}^{L}w_k^{\tau[k]}$에 매핑하는 해시 함수 H_G:$\{0,1\}^L$ → G를 정의하는 랜덤 벡터 $\vec{w}=(w_0,w_1,\ldots,w_L)\overset{R}{\leftarrow}\mathbb{G}^{L+1}$ 를 선택.

[0059] 공개 키는

[0060] $pk=(g_z,g_r,h_z,h,\{g_i,h_i\}_{i=1}^{n},\vec{w})\in\mathbb{G}^{2n+4}\times\mathbb{G}^{L+1}$ 로 구성되는 한편,

[0061] 개인 키는 $sk=\left(h_z^{\alpha_r},\{\chi_i,\gamma_i,\delta_i\}_{i=1}^{n}\right)$이다.

[0062] Sign(sk,τ(M_1,...,M_n)): $sk=\left(h_z^{\alpha_r},\{\chi_i,\gamma_i,\delta_i\}_{i=1}^{n}\right)$를 사용하여 파일 식별자 τ과 관련하여 벡터 (M_1,...,M_n)∈G^n에 서명하기 위해, $\theta,\rho\overset{R}{\leftarrow}\mathbb{Z}_p$를 선택하고,

$z=g_r^{\theta}\cdot\prod_{i=1}^{n}M_i^{-\chi_i}$, $r=g_z^{-\theta}\cdot\prod_{i=1}^{n}M_i^{-\gamma_i}$, $u=(h_z^{\alpha_r})^{-\theta}\cdot\prod_{i=1}^{n}M_i^{-\delta_i}\cdot H_{\mathbb{G}}(\tau)^{-\rho}$, $v=h^{\rho}$

를 산출한다.

[0063] 서명은 σ = (z,r,u,v) ∈ G^4를 포함한다.

[0064] $SignDerive(pk,\tau,\{(\omega_i,\sigma^{(i)})\}_{i=1}^{l})$: pk, 파일 식별자 τ 및 l 투플 ($\omega_i$,$\sigma^{(i)}$)을 고려하여, 각각의 서명 $\sigma^{(i)}$을 $\sigma^{(i)}$ = (z_i,r_i,u_i,v_i) ∈ G^4(i = 1 내지 l)로서 분석한다. 그 다음, $\rho'\overset{R}{\leftarrow}\mathbb{Z}_p$를 선택하고,

[0065] $z=\prod_{i=1}^{l}z_i^{\omega_i}$ $r=\prod_{i=1}^{l}r_i^{\omega_i}$ $u=\prod_{i=1}^{l}u_i^{\omega_i}\cdot H_{\mathbb{G}}(\tau)^{-\rho'}$ $v=\prod_{i=1}^{l}v_i^{\omega_i}\cdot h^{\rho'}$

[0066] 를 산출하고, σ = (z,r,u,v)를 리턴한다.

[0067] Verify(pk, σ, τ(M1,...,Mn): 서명 σ = (z,r,u,v) ∈ G^4, 파일 식별자 τ 및 벡터 (M1,...,Mn)를 고려하여, $(M_1,\ldots,M_n) \neq (\mathbf{1}_{\mathbb{G}},\ldots,\mathbf{1}_{\mathbb{G}})$ 이고, (z,r,u,v)가 등식들

$$\mathbf{1}_{\mathbb{G}_T} = e(g_z,z)\cdot e(g_r,r)\cdot\prod_{i=1}^{n} e(g_i,M_i),$$

[0068] $$\mathbf{1}_{\mathbb{G}_T} = e(h_z,z)\cdot e(h,u)\cdot e(H_{\mathbb{G}}(\tau),v)\cdot\prod_{i=1}^{n} e(h_i,M_i)$$

[0069] 을 만족하기만 하면 1을 리턴한다.

[0070] 1 회용 스킴은, 각각의 서명에서 Θ=ρ=0인 특정 경우의 완전한 스킴(full-fledged scheme)이라는 것을 이해할 수 있을 것이다.

[0071] **컨텍스트-은폐 스킴(Context-hiding scheme):**

[0072] 서명 도출 동작은 개인 키를 알지 못하고 근본적인 Θ를 다시 랜덤화할 수 없기 때문에, 완전한 스킴은 완전한 컨텍스트-은폐 보안을 제공하지 않는다는 것을 이해할 수 있을 것이다. 일부 애플리케이션에서, 계산상 무한한 관찰자의 관점에서조차, 도출된 서명 및 원래의 서명은 불연계성을 갖도록 보장하는 것이 바람직할 수 있다 .

[0073] 이러한 이유로, 바람직한 실시예는 완전한 컨텍스트-은폐가 입증될 수 있는 스킴이다. 이러한 스킴은 완전한 스킴을 수정하여 얻어진다. 기본적으로, 서명자는 먼저 서명 σ = (z,r,u,v)를 완전한 스킴에서와 같이 산출한다. 요소 (z,r,u)는 공개적으로 다시 랜덤화될 수 없기 때문에, 서명자는 그들이 단지 Groth-Sahai 커미트먼트 내에 나타나게 하고[*Eurocrypt'08*, *Lecture Notes in Computer Science*, 4965권, 415-432페이지(2008)에 있는, J. Groth, A. Sahai에 의한, Efficient non-interactive proof systems for bilinear groups 참조], 커미트된 값들이 검증 등식을 만족한다는 비-대화형 증명(non-interactive proof)을 추가한다. Groth-Sahai 증명의 완벽한 랜덤화가능 속성(*Crypto'09*, *Lecture Notes in Computer Science*, 5677권, 108-125페이지(2009)에 있는, M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, H. Shacham에 의한, Randomizable Proofs and Delegatable Anonymous Credentials에 나타남)은, 도출된 서명이 새로 생성된 서명으로서 배포될 것이라는 점을 보장한다.

[0074] 이하의 설명에서, 바이리니어 맵 e:G×G → G_T는 대칭적(즉, $\mathbb{G}=\hat{\mathbb{G}}$)이도록 다시 요구된다. 다음 표기법에서, 좌표별 페어링 $E:\mathbb{G}\times\hat{\mathbb{G}}^3\rightarrow\mathbb{G}_T^3$는, 임의의 요소 h∈G 및 임의의 벡터 $\vec{g}=(g_1,g_2,g_3)$에 대해, $E(h,\vec{g})=\left(e(h,g_1),e(h,g_2),e(h,g_3)\right)$이도록 정의된다.

[0075] 도 2는 이하의 스킴의 Sign, SignDerive 및 Verify를 도시한다.

[0076] Keygen(pp,n): pp 및 서명할 서브스페이스의 차원 n∈N을 고려하여, 다음 단계를 수행한다:

[0077] 1. $h\xleftarrow{R}\mathbb{G}$ 및 $\alpha_z,\alpha_r,\beta_z\xleftarrow{R}\mathbb{Z}_p$를 선택한다. $g_z=h^{\alpha_z}$, $g_r=h^{\alpha_r}$ 및 $h_z=h^{\beta_z}$를 정의한다.

[0078] 2. 각각의 i∈{1,...,n}에 대해, $\chi_i,\gamma_i,\delta_i\xleftarrow{R}\mathbb{Z}_p$를 선택하고, $g_i=g_z^{\chi_i}g_r^{\gamma_i}$, $h_i=h_z^{\chi_i}h^{\delta_i}$를 산출한다.

[0079] 3. $f_1,f_2\xleftarrow{R}\mathbb{G}$를 선택하고 벡터들 $\vec{f_1}=(f_1,1,g)\in\mathbb{G}^3$, $\vec{f_2}=(1,f_2,g)\in\mathbb{G}^3$ 및 $\vec{f_3}\xleftarrow{R}\mathbb{G}^3$을 정의하여 Groth-Sahai 공통 기준 스트링을 선택한다.

[0080] 공개 키는

[0081] $$\mathrm{pk}=\left(g_z,g_r,h_z,h,\{g_i,h_i\}_{i=1}^n,\mathbf{f}=(\vec{f_1},\vec{f_2},\vec{f_3})\right)$$

[0082] 로 구성되는 한편, 개인 키는 $sk=(h_z^{\alpha_r},\{\chi_i,\gamma_i,\delta_i\}_{i=1}^n)$이다.

[0083] Sign(sk, τ ,(M_1,...,M_n)): $sk=(h_z^{\alpha_r}, \{\chi_i, \gamma_i, \delta_i\}_{i=1}^{n})$ 를 사용하여 파일 식별자 τ과 관련하여 벡터 (M_1,...,M_n)∈G^n에 서명하기 위해, 다음을 수행한다:

[0084] 1. $\theta, \rho \xleftarrow{R} \mathbb{Z}_p$ 를 선택하고,

[0085] $$z = g_r^{\theta} \cdot \prod_{i=1}^{n} M_i^{-\chi_i}, \quad r = g_z^{-\theta} \cdot \prod_{i=1}^{n} M_i^{-\gamma_i}$$

$$u = (h_z^{\alpha_r})^{-\theta} \cdot \prod_{i=1}^{n} M_i^{-\delta_i} \cdot H_{\mathbb{G}}(\tau)^{-\rho}, \quad v = h^{\rho}$$

[0086] 를 산출한다(S1).

[0087] 2. 벡터 $\mathbf{f} = (\vec{f_1}, \vec{f_2}, \vec{f_3})$를 사용하여, z,r 및 u에 대해 각각 커미트먼트들

[0088] $$\vec{C}_z = (\mathbf{1}_{\mathbb{G}}, \mathbf{1}_{\mathbb{G}}, z) \cdot \vec{f_1}^{v_{z,1}} \cdot \vec{f_2}^{v_{z,2}} \cdot \vec{f_3}^{v_{z,3}}$$

$$\vec{C}_r = (\mathbf{1}_{\mathbb{G}}, \mathbf{1}_{\mathbb{G}}, r) \cdot \vec{f_1}^{v_{r,1}} \cdot \vec{f_2}^{v_{r,2}} \cdot \vec{f_3}^{v_{r,3}}$$

$$\vec{C}_u = (\mathbf{1}_{\mathbb{G}}, \mathbf{1}_{\mathbb{G}}, u) \cdot \vec{f_1}^{v_{u,1}} \cdot \vec{f_2}^{v_{u,2}} \cdot \vec{f_3}^{v_{u,3}}$$

[0089] 를 산출한다(S2). 이러한 커미트먼트들의 랜덤성을 사용하여, (z,r,u)가 완전한 스킴의 검증 등식, 즉,

[0090] $$\mathbf{1}_{\mathbb{G}_T} = e(g_z, z) \cdot e(g_r, r) \cdot \prod_{i=1}^{n} e(g_i, M_i),$$
$$\mathbf{1}_{\mathbb{G}_T} = e(h_z, z) \cdot e(h, u) \cdot e(H_{\mathbb{G}}(\tau), v) \cdot \prod_{i=1}^{n} e(h_i, M_i)$$

[0091] 를 만족한다는 증명들 $\vec{\pi}_1 = (\pi_{1,1}, \pi_{1,2}, \pi_{1,3}) \in \mathbb{G}^3$ 및 $\vec{\pi}_2 = (\pi_{2,1}, \pi_{2,2}, \pi_{2,3}) \in \mathbb{G}^3$ 을 생성한다.

[0092] 이러한 증명들은

[0093] $$\vec{\pi}_1 = (\pi_{1,1}, \pi_{1,2}, \pi_{1,3}) = (g_z^{-v_{z,1}} \cdot g_r^{-v_{r,1}}, g_z^{-v_{z,2}} \cdot g_r^{-v_{r,2}}, g_z^{-v_{z,3}} \cdot g_r^{-v_{r,3}})$$

$$\vec{\pi}_2 = (\pi_{2,1}, \pi_{2,2}, \pi_{2,3}) = (h_z^{-v_{z,1}} \cdot h_r^{-v_{u,1}}, h_z^{-v_{z,2}} \cdot h_r^{-v_{u,2}}, h_z^{-v_{z,3}} \cdot h_r^{-v_{u,3}})$$

[0094] 로서 얻어지고, 검증 등식들

[0095] $$\prod_{i=1}^{n} E(g_i, (\mathbf{1}_{\mathbb{G}}, \mathbf{1}_{\mathbb{G}}, M_i))^{-1} = E(g_z, \vec{C}_z) \cdot E(g_r, \vec{C}_r) \cdot E(\pi_{1,1}, \vec{f_1}) \cdot E(\pi_{1,2}, \vec{f_2}) \cdot E(\pi_{1,3}, \vec{f_3})$$

$$\prod_{i=1}^{n} E(h_i, (\mathbf{1}_{\mathbb{G}}, \mathbf{1}_{\mathbb{G}}, M_i))^{-1} \cdot E(H_{\mathbb{G}}(\tau), (\mathbf{1}_{\mathbb{G}}, \mathbf{1}_{\mathbb{G}}, v))^{-1} = E(h_z, \vec{C}_z) \cdot E(h, \vec{C}_u) \cdot E(\pi_{2,1}, \vec{f_1}) \cdot E(\pi_{2,2}, \vec{f_2}) \cdot E(\pi_{2,3}, \vec{f_3})$$

[0096] 을 만족한다.

[0097] 서명은 $\sigma = (\vec{C}_z, \vec{C}_r, \vec{C}_u, v, \vec{\pi}_1, \vec{\pi}_2) \in \mathbb{G}^{16}$ 를 포함한다.

[0098] $SignDerive(pk, \tau, \{(\omega_i, \sigma^{(i)})\}_{i=1}^{l})$: pk, 파일 식별자 τ 및 l 투플 (ω_i, $\sigma^{(i)}$)를 고려하여, 각

각의 서명 $\sigma^{(i)}$을 $\sigma^{(i)} = (\vec{C}_{g,i}, \vec{C}_{r,i}, \vec{C}_{u,i}, v_i, \vec{\pi}_{1,i}, \vec{\pi}_{2,i}) \in \mathbb{G}^{16}$ (i= 1 내지 l) 형태의 투플로서 분석한다. $\rho' \xleftarrow{R} \mathbb{Z}_p$를 선택하고,

$$\vec{C}_g = \prod_{i=1}^{\ell} \vec{C}_{g,i}^{\omega_i} \quad \vec{C}_r = \prod_{i=1}^{\ell} \vec{C}_{r,i}^{\omega_i} \quad \vec{C}_u = \prod_{i=1}^{\ell} \vec{C}_{u,i}^{\omega_i} \cdot H_{\mathbb{G}}(\tau)^{-\rho'}$$

$$v = \prod_{i=1}^{\ell} v_i^{\omega_i} \cdot h^{\rho'} \quad \vec{\pi}_1 = \prod_{i=1}^{\ell} \vec{\pi}_{1,i}^{\omega_i} \quad \vec{\pi}_2 = \prod_{i=1}^{\ell} \vec{\pi}_{2,i}^{\omega_i}$$

[0099]

[0100] 를 산출한다.

[0101] 그 다음, S3는 커미트먼트들 및 증명들을 다시 랜덤화하고, $\sigma = (\vec{C}_g, \vec{C}_r, \vec{C}_u, v, \vec{\pi}_1, \vec{\pi}_2)$를 리턴한다.

[0102] Verify(pk, σ, τ, $(M_1, \ldots, M_n)$): 페어 (τ, $(M_1, \ldots, M_n)$) 및 알려진 서명 σ을 고려하여, 서명을 $(\vec{C}_g, \vec{C}_r, \vec{C}_u, v, \vec{\pi}_1, \vec{\pi}_2)$로서 분석한다. 그 다음, S5는 $(M_1, \ldots, M_n) \neq (1_G, \ldots, 1_G)$이고 Sign 검증들이 만족(S4), 즉,

$$\prod_{i=1}^{n} E(g_i, (1_{\mathbb{G}}, 1_{\mathbb{G}}, M_i))^{-1} = E(g_g, \vec{C}_g) \cdot E(g_r, \vec{C}_r) \cdot E(\pi_{1,1}, \vec{f}_1) \cdot E(\pi_{1,2}, \vec{f}_2) \cdot E(\pi_{1,3}, \vec{f}_3)$$

$$\prod_{i=1}^{n} E(h_i, (1_{\mathbb{G}}, 1_{\mathbb{G}}, M_i))^{-1} \cdot E(H_{\mathbb{G}}(\tau), (1_{\mathbb{G}}, 1_{\mathbb{G}}, v))^{-1} = E(h_g, \vec{C}_g) \cdot E(h, \vec{C}_u) \cdot E(\pi_{2,1}, \vec{f}_1) \cdot E(\pi_{2,2}, \vec{f}_2) \cdot E(\pi_{2,3}, \vec{f}_3)$$

[0103]

[0104] 이기만 하면 1을 리턴한다.

[0105] 스킴의 위조불가는, 차원 3의 그룹 요소들의 3개의 벡터가 선형적으로 종속적인지 아닌지 여부를 결정하는 것이 실현 불가능하다고 비공식적으로 말하는 선형 결정 가정(Decision Linear assumption) 하에 입증될 수 있다. 또한, 스킴은 무조건 컨텍스트-은폐형이다.

[0106] 본 발명의 장점은, 서명자가 자신의 이산 대수를 알지 못하더라도 그룹 요소로 구성된 벡터들을 서명하는 것을 허용할 수 있다는 것이다. 예를 들어, 서명 스킴은 서명자가 근본적인 평문(underlying plaintext)을 반드시 알 필요없이 암호문에 서명할 수 있도록 한다.

[0107] 본 발명의 스킴은 클라우드 컴퓨팅 서비스에서 암호화된 데이터세트를 아웃소싱하는데 사용될 수 있다는 것을 이해할 수 있을 것이다. 또한, 선형 준동형 서명은 또한 익명 추천 시스템에서 정확한 집합의 증거 역할을 할 수 있다.

[0108] 설명 및 (적절한 경우) 청구항 및 도면에 개시된 각각의 특징은 독립적으로 또는 임의의 적절한 조합으로 제공될 수 있다. 하드웨어로 구현되는 것으로 기술된 특징들은 또한 소프트웨어로 구현될 수도 있고, 그 반대일 수도 있다. 청구항에 나타나는 참조 번호는 단지 예시로서, 청구항의 범위에 아무런 제한 효과가 없다.

부호의 설명

[0109] 100 : 서명 디바이스

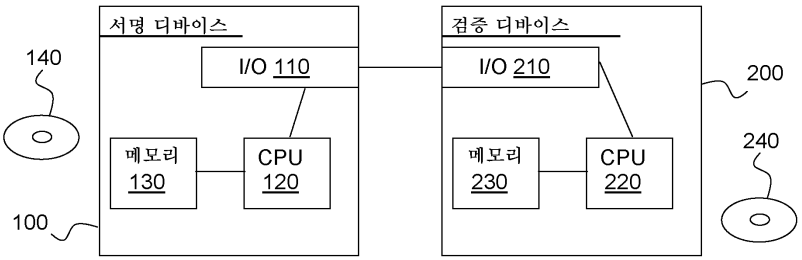
200 : 검증 디바이스

120, 220: 프로세서

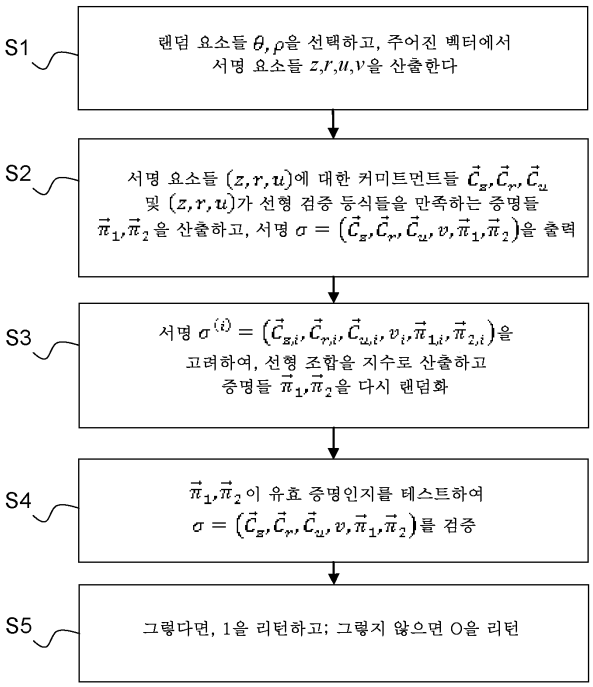
130, 230: 메모리

도면

도면1


서명 디바이스
I/O 110
메모리 130
CPU 120
140
100
검증 디바이스
I/O 210
메모리 230
CPU 220
200
240

도면2


S1
랜덤 요소들 θ, ρ을 선택하고, 주어진 벡터에서 서명 요소들 z,r,u,v을 산출한다
S2
서명 요소들 (z,r,u)에 대한 커미트먼트들 $\vec{C}_z, \vec{C}_r, \vec{C}_u$ 및 (z,r,u)가 선형 검증 등식들을 만족하는 증명들 $\vec{\pi}_1, \vec{\pi}_2$을 산출하고, 서명 $\sigma = (\vec{C}_z, \vec{C}_r, \vec{C}_u, v, \vec{\pi}_1, \vec{\pi}_2)$을 출력
S3
서명 $\sigma^{(i)} = (\vec{C}_{z,i}, \vec{C}_{r,i}, \vec{C}_{u,i}, v_i, \vec{\pi}_{1,i}, \vec{\pi}_{2,i})$을 고려하여, 선형 조합을 지수로 산출하고 증명들 $\vec{\pi}_1, \vec{\pi}_2$을 다시 랜덤화
S4
$\vec{\pi}_1, \vec{\pi}_2$이 유효 증명인지를 테스트하여 $\sigma = (\vec{C}_z, \vec{C}_r, \vec{C}_u, v, \vec{\pi}_1, \vec{\pi}_2)$를 검증
S5
그렇다면, 1을 리턴하고; 그렇지 않으면 0을 리턴