(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년12월05일
(11) 등록번호 10-2474628
(24) 등록일자 2022년12월01일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/14* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/0825 (2013.01)
H04L 9/14 (2022.08)
(21) 출원번호 10-2020-0161683
(22) 출원일자 2020년11월26일
심사청구일자 2020년11월26일
(65) 공개번호 10-2022-0073530
(43) 공개일자 2022년06월03일
(56) 선행기술조사문헌
Ioana Ivan, Functional Signatures, Massachusetts Institute of Technology 2013 (2013.06.)*
Elette Boyle 외 2명, Functional Signatures and Pseudorandom Functions, PKC 201, LNCS 8383 (2014.)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
신지선
서울특별시 광진구 능동로 209, 세종대학교 대양AI센터 708호(군자동)
조민재
서울특별시 동작구 사당로 180-6, 201호 (사당동)
(74) 대리인
두호특허법인

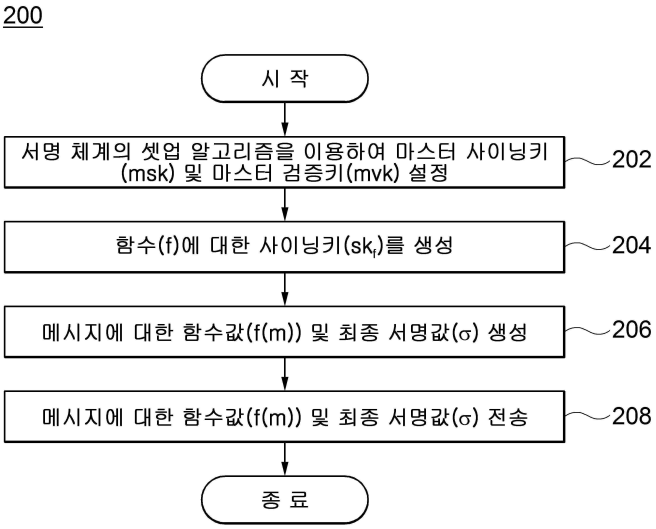
전체 청구항 수 : 총 15 항 심사관 : 양종필

(54) 발명의 명칭 **함수 서명을 이용한 서명 암호화 방법 및 이를 수행하기 위한 컴퓨팅 장치**

(57) 요 약

함수 서명을 이용한 서명 암호화 방법 및 이를 수행하기 위한 컴퓨팅 장치가 개시된다. 개시되는 일 실시예에 따른 서명 암호화 방법은, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서, 서명 체계(Signature Scheme)의 셋업 알고리즘을 이용하여 마스터 사이닝키(master signing key: msk) 및 마스터 검증키(master verification key: mvk)의 쌍을 설정하는 동작, 마스터 사이닝키(msk) 및 함수 서명(Functional Signature)의 함수(f)를 기반으로 함수(f)에 대한 사이닝키(sk_f)를 생성하는 동작, 및 함수 서명의 함수(f), 함수(f)에 대한 사이닝키(sk_f), 및 메시지(m)에 기반하여 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 동작을 포함한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 9/3263 (2013.01)
H04L 2209/72 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711116150
과제번호	2016-6-00599-005
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(R&D,정보화)
연구과제명	(함수암호 3세부) 함수서명 설계기법 및 응용기술 연구
기 여 율	1/1
과제수행기관명	고려대학교 산학협력단
연구기간	2020.02.01 ~ 2021.01.31

명 세 서

청구범위

청구항 1

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서,

서명 체계(Signature Scheme)의 셋업 알고리즘을 이용하여 마스터 사이닝키(master signing key: msk) 및 마스터 검증키(master verification key: mvk)의 쌍을 설정하는 동작;

상기 마스터 사이닝키(msk) 및 함수 서명(Functional Signature)의 함수(f)를 기반으로 함수(f)에 대한 사이닝키(sk_f)를 생성하는 동작; 및

상기 함수 서명의 함수(f), 상기 함수(f)에 대한 사이닝키(sk_f), 및 메시지(m)에 기반하여 상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 동작을 포함하고,

상기 함수 서명의 함수(f)는, 암호화를 위한 공개키 또는 대칭키로 설정되며,

공개키 또는 대칭키인 상기 함수(f)에 대한 사이닝키(sk_f)를 생성하는 동작은,

상기 서명 체계의 셋업 알고리즘을 이용하여 사이닝키(signing key: sk) 및 검증키(verification key: vk)의 쌍을 설정하는 동작;

상기 마스터 사이닝키(msk), 상기 함수 서명의 함수(f), 및 상기 검증키(vk)에 상기 서명 체계의 서명(Signature) 알고리즘을 적용하여 상기 검증키에 대한 서명값(σ_{vk})을 산출하는 동작;

상기 함수 서명의 함수(f), 상기 검증키(vk), 및 상기 검증키에 대한 서명값(σ_{vk})에 기초하여 인증서(c)를 생성하는 동작; 및

상기 사이닝키(sk) 및 상기 인증서(c)에 기반하여 상기 함수(f)에 대한 사이닝키(sk_f)를 생성하는 동작을 포함하고,

상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 동작은, 상기 함수(f)가 공개키인 경우 RSA(Rivest Shamir Adleman) 기반의 공개키 암호화 방식을 사용하고, 상기 함수(f)가 대칭키인 경우 AES(Advanced Encrytion Standard Algorithm) 기반의 대칭키 암호화 방식을 사용하며,

상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 동작은,

상기 메시지(m) 및 상기 사이닝키(sk)에 상기 서명 체계의 서명 알고리즘을 적용하여 상기 메시지에 대한 서명값(σ_m)을 산출하는 동작;

상기 메시지(m)를 상기 함수(f)에 적용하여 상기 메시지에 대한 함수 값(f(m))을 생성하는 동작; 및

상기 메시지(m), 상기 인증서(c), 및 상기 메시지에 대한 서명값(σ_m)에 기반하여 상기 최종 서명값(σ)을 생성하는 동작을 포함하는, 서명 암호화 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

청구항 1에 있어서,

상기 검증키에 대한 서명값(σ_{vk})을 산출하는 동작은,

상기 마스터 사이닝키(msk)로 상기 함수(f)에 상기 검증키(vk)를 연결한(Concatenated) 값(f|vk)을 서명하여 상기 검증키에 대한 서명값(σ_{vk})을 산출하는, 서명 암호화 방법.

청구항 5

삭제

청구항 6

청구항 1에 있어서,

상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 동작은,

상기 함수(f)에 대한 사이닝키(sk_f)를 상기 사이닝키(sk)와 상기 인증서(c)로 파싱하는 동작을 더 포함하는, 서명 암호화 방법.

청구항 7

청구항 1에 있어서,

상기 서명 암호화 방법은,

상기 메시지에 대한 함수 값(f(m)) 및 상기 최종 서명값(σ)을 다른 컴퓨팅 장치로 전송하는 동작을 더 포함하고,

상기 다른 컴퓨팅 장치는,

상기 마스터 검증키(mvk)에 기반하여 상기 메시지에 대한 함수 값(f(m)) 및 상기 최종 서명값(σ)을 검증하는 동작을 수행하는, 서명 암호화 방법.

청구항 8

청구항 7에 있어서,

상기 검증하는 동작은,

상기 최종 서명값(σ)을 상기 메시지(m), 상기 인증서($c = (f, vk, \sigma_{vk})$), 및 상기 메시지에 대한 서명값(σ_m)으로 파싱하는 동작;

상기 파싱한 메시지(m)를 상기 함수(f)에 적용하여 상기 메시지에 대한 함수 값(f(m))을 생성하는 동작; 및

상기 생성한 메시지에 대한 함수 값(f(m))이 상기 컴퓨팅 장치로부터 수신한 메시지에 대한 함수 값(f(m))과 일치하는지를 확인하는 동작을 포함하는, 서명 암호화 방법.

청구항 9

청구항 8에 있어서,

상기 검증하는 동작은,

상기 메시지(m) 및 상기 검증키(vk)를 상기 서명 체계의 검증 알고리즘에 적용하여 상기 파싱한 메시지에 대한

서명값(σ_m)을 검증하는 동작을 더 포함하는, 서명 암호화 방법.

청구항 10

청구항 9에 있어서,

상기 검증하는 동작은,

상기 마스터 검증키(mvk) 및 상기 검증키(vk)에 함수(f)를 연결한(Concatenated) 값(f|vk)을 상기 서명 체계의 검증 알고리즘에 적용하여 상기 파싱한 검증키에 대한 서명값(σ_{vk})을 검증하는 동작을 더 포함하는, 서명 암호화 방법.

청구항 11

하나 이상의 프로세서들;

메모리; 및

하나 이상의 프로그램들을 포함하고,

상기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행되도록 구성되며,

상기 하나 이상의 프로그램들은,

서명 체계(Signature Scheme)의 셋업 알고리즘을 이용하여 마스터 사이닝키(master signing key: msk) 및 마스터 검증키(master verification key: mvk)의 쌍을 설정하기 위한 명령;

상기 마스터 사이닝키(msk) 및 함수 서명(Functional Signature)의 함수(f)를 기반으로 함수(f)에 대한 사이닝키(sk_f)를 생성하기 위한 명령; 및

상기 함수 서명의 함수(f), 상기 함수(f)에 대한 사이닝키(sk_f), 및 메시지(m)에 기반하여 상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하기 위한 명령을 포함하고,

상기 함수 서명의 함수(f)는, 암호화를 위한 공개키 또는 대칭키로 설정되며,

공개키 또는 대칭키인 상기 함수(f)에 대한 사이닝키(sk_f)를 생성하기 위한 명령은,

상기 서명 체계의 셋업 알고리즘을 이용하여 사이닝키(signing key: sk) 및 검증키(verification key: vk)의 쌍을 설정하기 위한 명령;

상기 마스터 사이닝키(msk), 상기 함수 서명의 함수(f), 및 상기 검증키(vk)에 상기 서명 체계의 서명(Signature) 알고리즘을 적용하여 상기 검증키에 대한 서명값(σ_{vk})을 산출하기 위한 명령;

상기 함수 서명의 함수(f), 상기 검증키(vk), 및 상기 검증키에 대한 서명값(σ_{vk})에 기초하여 인증서(c)를 생성하기 위한 명령; 및

상기 사이닝키(sk) 및 상기 인증서(c)에 기반하여 상기 함수(f)에 대한 사이닝키(sk_f)를 생성하기 위한 명령을 포함하고,

상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)의 생성은, 상기 함수(f)가 공개키인 경우 RSA(Rivest Shamir Adleman) 기반의 공개키 암호화 방식을 사용하고, 상기 함수(f)가 대칭키인 경우 AES(Advanced Encrytion Standard Algorithm) 기반의 대칭키 암호화 방식을 사용하며,

상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하기 위한 명령은,

상기 메시지(m) 및 상기 사이닝키(sk)에 상기 서명 체계의 서명 알고리즘을 적용하여 상기 메시지에 대한 서명

값(σ_m)을 산출하기 위한 명령;

상기 메시지(m)를 상기 함수(f)에 적용하여 상기 메시지에 대한 함수 값(f(m))을 생성하기 위한 명령; 및

상기 메시지(m), 상기 인증서(c), 및 상기 메시지에 대한 서명값(σ_m)에 기반하여 상기 최종 서명값(σ)을 생성하기 위한 명령을 포함하는, 컴퓨팅 장치.

청구항 12

삭제

청구항 13

삭제

청구항 14

청구항 11에 있어서,

상기 검증키에 대한 서명값(σ_{vk})을 산출하기 위한 명령은,

상기 마스터 사이닝키(msk)로 상기 함수(f)에 상기 검증키(vk)를 연결한(Concatenated) 값(f|vk)을 서명하여 상기 검증키에 대한 서명값(σ_{vk})을 산출하는, 컴퓨팅 장치.

청구항 15

삭제

청구항 16

청구항 11에 있어서,

상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하기 위한 명령은,

상기 함수(f)에 대한 사이닝키(sk_f)를 상기 사이닝키(sk)와 상기 인증서(c)로 파싱하기 위한 명령을 더 포함하는, 컴퓨팅 장치.

청구항 17

청구항 11에 있어서,

상기 하나 이상의 프로그램들은,

상기 메시지에 대한 함수 값(f(m)) 및 상기 최종 서명값(σ)을 다른 컴퓨팅 장치로 전송하기 위한 명령을 더 포함하고,

상기 다른 컴퓨팅 장치는,

상기 마스터 검증키(mvk)에 기반하여 상기 메시지에 대한 함수 값(f(m)) 및 상기 최종 서명값(σ)을 검증하는, 컴퓨팅 장치.

청구항 18

청구항 17에 있어서,

상기 다른 컴퓨팅 장치는,

상기 최종 서명값(σ)을 상기 메시지(m), 상기 인증서(c = (f, vk, σ_{vk})), 및 상기 메시지에 대한 서명값(σ_m)으로 파싱하고, 상기 파싱한 메시지(m)를 상기 함수(f)에 적용하여 상기 메시지에 대한 함수 값(f(m))을 생성하며, 상기 생성한 메시지에 대한 함수 값(f(m))이 상기 컴퓨팅 장치로부터 수신한 메시지에 대한 함수 값(f(m))과 일치하는지를 확인하는, 컴퓨팅 장치.

청구항 19

청구항 18에 있어서,

상기 다른 컴퓨팅 장치는,

상기 메시지(m) 및 상기 검증키(vk)를 상기 서명 체계의 검증 알고리즘에 적용하여 상기 파싱한 메시지에 대한 서명값(σ_m)을 검증하는, 컴퓨팅 장치.

청구항 20

청구항 19에 있어서,

상기 다른 컴퓨팅 장치는,

상기 마스터 검증키(mvk) 및 상기 검증키(vk)에 함수(f)를 연결한(Concatenated) 값(f|vk)을 상기 서명 체계의 검증 알고리즘에 적용하여 상기 파싱한 검증키에 대한 서명값(σ_{vk})을 검증하는, 컴퓨팅 장치.

청구항 21

비일시적 컴퓨터 판독 가능한 저장 매체(non-transitory computer readable storage medium)에 저장된 컴퓨터 프로그램으로서,

상기 컴퓨터 프로그램은 하나 이상의 명령어들을 포함하고, 상기 명령어들은 하나 이상의 프로세서들을 갖는 컴퓨팅 장치에 의해 실행될 때, 상기 컴퓨팅 장치로 하여금,

서명 체계(Signature Scheme)의 셋업 알고리즘을 이용하여 마스터 사이닝키(master signing key: msk) 및 마스터 검증키(master verification key: mvk)의 쌍을 설정하는 동작;

상기 마스터 사이닝키(msk) 및 함수 서명(Functional Signature)의 함수(f)를 기반으로 함수(f)에 대한 사이닝키(sk_f)를 생성하는 동작; 및

상기 함수 서명의 함수(f), 상기 함수(f)에 대한 사이닝키(sk_f), 및 메시지(m)에 기반하여 상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 동작을 수행하도록 하고,

상기 함수 서명의 함수(f)는, 암호화를 위한 공개키 또는 대칭키로 설정되며,

공개키 또는 대칭키인 상기 함수(f)에 대한 사이닝키(sk_f)를 생성하는 동작은,

상기 서명 체계의 셋업 알고리즘을 이용하여 사이닝키(signing key: sk) 및 검증키(verification key: vk)의 쌍을 설정하는 동작;

상기 마스터 사이닝키(msk), 상기 함수 서명의 함수(f), 및 상기 검증키(vk)에 상기 서명 체계의 서명(Signature) 알고리즘을 적용하여 상기 검증키에 대한 서명값(σ_{vk})을 산출하는 동작;

상기 함수 서명의 함수(f), 상기 검증키(vk), 및 상기 검증키에 대한 서명값(σ_{vk})에 기초하여 인증서(c)를 생성하는 동작; 및

상기 사이닝키(sk) 및 상기 인증서(c)에 기반하여 상기 함수(f)에 대한 사이닝키(sk_f)를 생성하는 동작을 포함

하고,

상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 동작은, 상기 함수(f)가 공개키인 경우 RSA(Rivest Shamir Adleman) 기반의 공개키 암호화 방식을 사용하고, 상기 함수(f)가 대칭키인 경우 AES(Advanced Encrytion Standard Algorithm) 기반의 대칭키 암호화 방식을 사용하며,

상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 동작은,

상기 메시지(m) 및 상기 사이닝키(sk)에 상기 서명 체계의 서명 알고리즘을 적용하여 상기 메시지에 대한 서명값(σ_m)을 산출하는 동작;

상기 메시지(m)를 상기 함수(f)에 적용하여 상기 메시지에 대한 함수 값(f(m))을 생성하는 동작; 및

상기 메시지(m), 상기 인증서(c), 및 상기 메시지에 대한 서명값(σ_m)에 기반하여 상기 최종 서명값(σ)을 생성하는 동작을 포함하는, 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예는 서명 암호화 기술과 관련된다.

배 경 기 술

[0003] 최근, 통신 기술이 발달하면서 디지털 메시지의 사용이 증가하고 있다. 즉, 인터넷의 발달로 언제 어디서나 이메일 또는 SNS 메시지 등을 주고 받고 있으며 인터넷을 통해 정보 수집 활동을 하고 있다. 이러한 인터넷의 이용으로 생활의 편익과 경제성 및 효율성은 증대되고 있으나, 인터넷의 개방성으로 인해 전자거래 정보의 위변조 및 개인 정보 유출 등의 위험성이 상존하고 있다.

[0004] 그에 따라, 보안 및 인증 통신을 위한 암호문이 사용되고 있는데 이는 메시지의 위조를 방지하고 메시지의 기밀성을 유지하기 위한 것이다. 또한, 이러한 암호화 기술과 함께 전자 서명(Electronic Signature)이 도입되고 있다. 전자 서명은 인터넷 등 통신망을 통하여 컴퓨터 시스템 간에 교환 및 전송되는 메시지 무결성을 보증하기 위한 메시지 인증과 해당 메시지에 대한 생성, 처리, 전송, 저장, 및 수신 등의 행위를 한 사용자를 보증하기 위한 사용자 인증의 기능을 겸하는 보안 기술 또는 수단으로 정의될 수 있다.

[0005] 한편, 전자 서명과 관련한 많은 연구들이 수행되고 있으나, 안전하면서도 편리하고 신뢰할 수 있으며 새롭고 효율적인 전자 서명의 검증과 이를 통한 전자 서명 방안이나 대책은 지속적으로 요구되고 있는 실정이다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 한국등록특허공보 제10-1253683호(2013.04.11)

발명의 내용

해결하려는 과제

[0008] 본 발명의 실시예는 새로운 기법의 함수 서명을 이용한 서명 암호화 방법 및 이를 수행하기 위한 컴퓨팅 장치를 제공하기 위한 것이다.

과제의 해결 수단

[0010] 개시되는 일 실시예에 따른 서명 암호화 방법은, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서, 서명 체계(Signature Scheme)의 셋업 알고리즘을 이용하여 마스터 사이닝키(master signing key: msk) 및 마스터

검증키(master verification key: mvk)의 쌍을 설정하는 동작; 상기 마스터 사이닝키(msk) 및 함수 서명(Functional Signature)의 함수(f)를 기반으로 함수(f)에 대한 사이닝키(sk_f)를 생성하는 동작; 및 상기 함수 서명의 함수(f), 상기 함수(f)에 대한 사이닝키(sk_f), 및 메시지(m)에 기반하여 상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 동작을 포함한다.

[0011] 상기 함수 서명의 함수(f)는, 암호화를 위한 공개키 또는 대칭키로 설정될 수 있다.

[0012] 상기 함수(f)에 대한 사이닝키(sk_f)를 생성하는 동작은, 상기 서명 체계의 셋업 알고리즘을 이용하여 사이닝키(signing key: sk) 및 검증키(verification key: vk)의 쌍을 설정하는 동작; 상기 마스터 사이닝키(msk), 상기 함수 서명의 함수(f), 및 상기 검증키(vk)에 상기 서명 체계의 서명(Signature) 알고리즘을 적용하여 상기 검증키에 대한 서명값(σ_{vk})을 산출하는 동작; 상기 함수 서명의 함수(f), 상기 검증키(vk), 및 상기 검증키에 대한 서명값(σ_{vk})에 기초하여 인증서(c)를 생성하는 동작; 및 상기 사이닝키(sk) 및 상기 인증서(c)에 기반하여 상기 함수(f)에 대한 사이닝키(sk_f)를 생성하는 동작을 포함할 수 있다.

[0013] 상기 검증키에 대한 서명값(σ_{vk})을 산출하는 동작은, 상기 마스터 사이닝키(msk)로 상기 함수(f)에 상기 검증키(vk)를 연결한(Concatenated) 값(f|vk)을 서명하여 상기 검증키에 대한 서명값(σ_{vk})을 산출할 수 있다.

[0014] 상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 동작은, 상기 메시지(m) 및 상기 사이닝키(sk)에 상기 서명 체계의 서명 알고리즘을 적용하여 상기 메시지에 대한 서명값(σ_m)을 산출하는 동작; 상기 메시지(m)를 상기 함수(f)에 적용하여 상기 메시지에 대한 함수 값(f(m))을 생성하는 동작; 및 상기 메시지(m), 상기 인증서(c), 및 상기 메시지에 대한 서명값(σ_m)에 기반하여 상기 최종 서명값(σ)을 생성하는 동작을 포함할 수 있다.

[0015] 상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 동작은, 상기 함수(f)에 대한 사이닝키(sk_f)를 상기 사이닝키(sk)와 상기 인증서(c)로 파싱하는 동작을 더 포함할 수 있다.

[0016] 상기 서명 암호화 방법은, 상기 메시지에 대한 함수 값(f(m)) 및 상기 최종 서명값(σ)을 다른 컴퓨팅 장치로 전송하는 동작을 더 포함하고, 상기 다른 컴퓨팅 장치는, 상기 마스터 검증키(mvk)에 기반하여 상기 메시지에 대한 함수 값(f(m)) 및 상기 최종 서명값(σ)을 검증하는 동작을 수행할 수 있다.

[0017] 상기 검증하는 동작은, 상기 최종 서명값(σ)을 상기 메시지(m), 상기 인증서($c = (f, vk, \sigma_{vk})$), 및 상기 메시지에 대한 서명값(σ_m)으로 파싱하는 동작; 상기 파싱한 메시지(m)를 상기 함수(f)에 적용하여 상기 메시지에 대한 함수 값(f(m))을 생성하는 동작; 및 상기 생성한 메시지에 대한 함수 값(f(m))이 상기 컴퓨팅 장치로부터 수신한 메시지에 대한 함수 값(f(m))과 일치하는지를 확인하는 동작을 포함할 수 있다.

[0018] 상기 검증하는 동작은, 상기 메시지(m) 및 상기 검증키(vk)를 상기 서명 체계의 검증 알고리즘에 적용하여 상기 파싱한 메시지에 대한 서명값(σ_m)을 검증하는 동작을 더 포함할 수 있다.

[0019] 상기 검증하는 동작은, 상기 마스터 검증키(mvk) 및 상기 검증키(vk)에 함수(f)를 연결한(Concatenated) 값(f|vk)을 상기 서명 체계의 검증 알고리즘에 적용하여 상기 파싱한 검증키에 대한 서명값(σ_{vk})을 검증하는 동작을 더 포함할 수 있다.

[0020] 개시되는 일 실시예에 따른 컴퓨팅 장치는, 하나 이상의 프로세서들; 메모리; 및 하나 이상의 프로그램들을 포함하고, 상기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행되도록 구성되며, 상기 하나 이상의 프로그램들은, 서명 체계(Signature Scheme)의 셋업 알고리즘을 이용하여 마스터 사이닝키(master signing key: msk) 및 마스터 검증키(master verification key: mvk)의 쌍을 설정하기 위한 명령; 상기 마스터 사이닝키(msk) 및 함수 서명(Functional Signature)의 함수(f)를 기반으로 함수(f)에 대한 사이닝키(sk_f)를 생성하기 위한 명령; 및 상기 함수 서명의 함수(f), 상기 함수(f)에 대한 사이닝키(sk_f), 및 메시지(m)에 기반하여 상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하기 위한 명령을 포함한다.

[0021] 상기 함수 서명의 함수(f)는, 암호화를 위한 공개키 또는 대칭키로 설정될 수 있다.

[0022] 상기 함수(f)에 대한 사이닝키(sk_f)를 생성하기 위한 명령은, 상기 서명 체계의 셋업 알고리즘을 이용하여 사이닝키(signing key: sk) 및 검증키(verification key: vk)의 쌍을 설정하기 위한 명령; 상기 마스터 사이닝키(msk), 상기 함수 서명의 함수(f), 및 상기 검증키(vk)에 상기 서명 체계의 서명(Signature) 알고리즘을 적용하여 상기 검증키에 대한 서명값(σ_{vk})을 산출하기 위한 명령; 상기 함수 서명의 함수(f), 상기 검증키(vk), 및 상기 검증키에 대한 서명값(σ_{vk})에 기초하여 인증서(c)를 생성하기 위한 명령; 및 상기 사이닝키(sk) 및 상기 인증서(c)에 기반하여 상기 함수(f)에 대한 사이닝키(sk_f)를 생성하기 위한 명령을 포함할 수 있다.

[0023] 상기 검증키에 대한 서명값(σ_{vk})을 산출하기 위한 명령은, 상기 마스터 사이닝키(msk)로 상기 함수(f)에 상기 검증키(vk)를 연결한(Concatenated) 값(f|vk)을 서명하여 상기 검증키에 대한 서명값(σ_{vk})을 산출할 수 있다.

[0024] 상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하기 위한 명령은, 상기 메시지(m) 및 상기 사이닝키(sk)에 상기 서명 체계의 서명 알고리즘을 적용하여 상기 메시지에 대한 서명값(σ_m)을 산출하기 위한 명령; 상기 메시지(m)를 상기 함수(f)에 적용하여 상기 메시지에 대한 함수 값(f(m))을 생성하기 위한 명령; 및 상기 메시지(m), 상기 인증서(c), 및 상기 메시지에 대한 서명값(σ_m)에 기반하여 상기 최종 서명값(σ)을 생성하기 위한 명령을 포함할 수 있다.

[0025] 상기 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하기 위한 명령은, 상기 함수(f)에 대한 사이닝키(sk_f)를 상기 사이닝키(sk)와 상기 인증서(c)로 파싱하기 위한 명령을 더 포함할 수 있다.

[0026] 상기 하나 이상의 프로그램들은, 상기 메시지에 대한 함수 값(f(m)) 및 상기 최종 서명값(σ)을 다른 컴퓨팅 장치로 전송하기 위한 명령을 더 포함하고, 상기 다른 컴퓨팅 장치는, 상기 마스터 검증키(mvk)에 기반하여 상기 메시지에 대한 함수 값(f(m)) 및 상기 최종 서명값(σ)을 검증할 수 있다.

[0027] 상기 다른 컴퓨팅 장치는, 상기 최종 서명값(σ)을 상기 메시지(m), 상기 인증서($c = (f, vk, \sigma_{vk})$), 및 상기 메시지에 대한 서명값(σ_m)으로 파싱하고, 상기 파싱한 메시지(m)를 상기 함수(f)에 적용하여 상기 메시지에 대한 함수 값(f(m))을 생성하며, 상기 생성한 메시지에 대한 함수 값(f(m))이 상기 컴퓨팅 장치로부터 수신한 메시지에 대한 함수 값(f(m))과 일치하는지를 확인할 수 있다.

[0028] 상기 다른 컴퓨팅 장치는, 상기 메시지(m) 및 상기 검증키(vk)를 상기 서명 체계의 검증 알고리즘에 적용하여 상기 파싱한 메시지에 대한 서명값(σ_m)을 검증할 수 있다.

[0029] 상기 다른 컴퓨팅 장치는, 상기 마스터 검증키(mvk) 및 상기 검증키(vk)에 함수(f)를 연결한(Concatenated) 값(f|vk)을 상기 서명 체계의 검증 알고리즘에 적용하여 상기 파싱한 검증키에 대한 서명값(σ_{vk})을 검증할 수 있다.

발명의 효과

[0031] 개시되는 실시예에 의하면, 함수 서명의 함수(f)를 공개키 또는 대칭키로 설정하고, 함수(f)에 대한 사이닝키(sk_f)로 메시지(m)를 서명하여 메시지에 대한 함수 값(f(m))(즉, 메시지(m)를 공개키 또는 대칭키인 함수(f)로 암호화한 값) 및 최종 서명값(σ)을 생성함으로써, 메시지를 암호화함과 동시에 서명을 수행할 수 있게 된다.

도면의 간단한 설명

[0033] 도 1은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

도 2는 본 발명의 일 실시예에 따른 암호화 서명 처리 방법을 설명하기 위한 흐름도

도 3은 개시되는 일 실시예에서, 함수에 대한 사이닝키를 생성하는 과정을 나타낸 흐름도

도 4는 개시되는 일 실시예에서, 메시지에 대한 함수 값 및 최종 서명값을 생성하는 과정을 나타낸 흐름도

도 5는 일 실시예에 따른 다른 컴퓨팅 장치에서 마스터 검증키에 기반하여 메시지에 대한 함수 값 및 최종 서명값을 검증하는 과정을 나타낸 흐름도

발명을 실시하기 위한 구체적인 내용

[0034] 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.

[0035] 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.

[0036] 이하의 설명에 있어서, 신호 또는 정보의 "전송", "통신", "송신", "수신" 기타 이와 유사한 의미의 용어는 일 구성요소에서 다른 구성요소로 신호 또는 정보가 직접 전달되는 것뿐만이 아니라 다른 구성요소를 거쳐 전달되는 것도 포함한다. 특히 신호 또는 정보를 일 구성요소로 "전송" 또는 "송신"한다는 것은 그 신호 또는 정보의 최종 목적지를 지시하는 것이고 직접적인 목적지를 의미하는 것이 아니다. 이는 신호 또는 정보의 "수신"에 있어서도 동일하다. 또한 본 명세서에 있어서, 2 이상의 데이터 또는 정보가 "관련"된다는 것은 하나의 데이터(또는 정보)를 획득하면, 그에 기초하여 다른 데이터(또는 정보)의 적어도 일부를 획득할 수 있음을 의미한다.

[0037] 또한, 제1, 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로 사용될 수 있다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성 요소는 제2 구성 요소로 명명될 수 있고, 유사하게 제2 구성 요소도 제1 구성 요소로 명명될 수 있다.

[0039] 도 1은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 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.

[0040] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 본 발명의 일 실시예에 따른 암호화 서명 처리를 수행하기 위한 장치일 수 있다.

[0041] 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.

[0042] 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.

[0043] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0044] 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.

[0046] 도 2는 본 발명의 일 실시예에 따른 암호화 서명 처리 방법(200)을 설명하기 위한 흐름도이다. 전술한 바와 같이, 본 발명의 일 실시예에 따른 암호화 서명 처리 방법(200)은 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치(12)에서 수행될 수 있다. 이를 위하여, 암호화 서명 처리 방법(200)은 하나 이상의 컴퓨터 실행 가능 명령어를 포함하는 프로그램 내지 소프트웨어의 형태로 구현되어 상기 메모리상에 저장될 수 있다.

[0047] 또한, 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 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.

[0048] 단계 202에서, 컴퓨팅 장치(12)는 서명 체계(Signature Scheme)를 이용하여 마스터 키 쌍을 설정한다. 서명 체계는 기 공지된 기술이므로 이에 대한 자세한 설명은 생략하기로 한다. 여기서, 마스터 키 쌍은 마스터 사이닝키(master signing key: msk) 및 마스터 검증키(master verification key: mvk)를 포함할 수 있다.

[0049] 예시적인 실시예에서, 컴퓨팅 장치(12)는 서명 체계의 셋업(Setup) 알고리즘을 이용하여 마스터 사이닝키 및 마스터 검증키의 쌍을 설정할 수 있다. 이때, 단계 202의 과정은 아래 수학식 1로 표현할 수 있다.

[0050] (수학식 1)

[0051] $(msk, mvk) \leftarrow Sig.Setup(1^k)$

[0052] 단계 204에서, 컴퓨팅 장치(12)는 마스터 사이닝키(msk) 및 함수 서명의 함수(f)를 기반으로 함수(f)에 대한 사이닝키(sk_f)를 생성한다.

[0053] 여기서, 함수 서명(Functional Signature)은 비밀키의 복호화 권한을 제한하여 비밀키를 가진 사람이 암호문의 모든 정보에 접근할 수 있는 것이 아니라 암호문의 특정 함수 값에만 접근할 수 있도록 하고, 데이터에 대한 함수 연산의 무결성 기능을 제공하며, 메시지가 정당한 함수를 사용하여 연산이 수행되었음을 검증할 수 있는 서명 기법의 일종이다.

[0054] 개시되는 실시예에서, 함수 서명의 함수(f)는 암호화를 위한 공개키 또는 대칭키로 설정될 수 있다. 이때, 단계 204는 공개키 또는 대칭키인 함수(f)에 대응하는 사이닝키를 생성하는 과정이 된다. 함수(f)에 대한 사이닝키(sk_f)를 생성하는 구체적인 과정은 도 3을 참조하여 후술하기로 한다.

[0055] 도 3은 개시되는 일 실시예에서, 함수(f)에 대한 사이닝키(sk_f)를 생성하는 과정을 나타낸 흐름도이다.

[0056] 단계 302에서, 컴퓨팅 장치(12)는 서명 체계(Signature Scheme)의 셋업 알고리즘를 이용하여 새로운 키 쌍(즉, 사용자의 키 쌍)을 설정한다. 즉, 컴퓨팅 장치(12)는 마스터 사이닝키 및 마스터 검증키의 쌍을 설정할 때 사용한 서명 체계의 셋업 알고리즘를 이용하여 새로운 키 쌍을 설정할 수 있다.

[0057] 여기서, 새로운 키 쌍은 사이닝키(signing key: sk) 및 검증키(verification key: vk)를 포함할 수 있다. 단계 302의 과정은 아래 수학식 2로 표현할 수 있다.

[0058] (수학식 2)

[0059] $(sk, vk) \leftarrow Sig.Setup(1^k)$

[0060] 단계 304에서, 컴퓨팅 장치(12)는 마스터 사이닝키(msk), 함수 서명(Functional Signature)의 함수(f), 및 검증키(vk)에 서명 체계의 서명(Signature) 알고리즘을 적용하여 검증키에 대한 서명값(σ_{vk})을 산출한다.

[0061] 예시적인 실시예에서, 컴퓨팅 장치(12)는 마스터 사이닝키(msk)로 함수(f)에 검증키(vk)를 연결한(Concatenated) 값(f|vk)을 서명(Signature)하여 검증키에 대한 서명값(σ_{vk})을 산출할 수 있다. 여기서, 함수

(f)는 공개키 또는 대칭키로 사용될 수 있다. 이 경우, 공개키 또는 대칭키에 검증키(vk)를 연결한 값을 마스터 사이닝키(msk)로 서명하여 검증키에 대한 서명값(σ_{vk})을 산출할 수 있다. 단계 304의 과정은 아래 수학식 3으로 표현할 수 있다.

[0062] (수학식 3)

[0063] $\sigma_{vk} \leftarrow Sig.Sign(msk, f|vk)$

[0064] 단계 306에서, 컴퓨팅 장치(12)는 함수 서명의 함수(f), 검증키(vk), 및 검증키에 대한 서명값(σ_{vk})에 기초하여 인증서(c)를 생성한다. 단계 306의 과정은 아래 수학식 4로 표현할 수 있다.

[0065] (수학식 4)

[0066] $c = (f, vk, \sigma_{vk})$

[0067] 단계 308에서, 컴퓨팅 장치(12)는 사이닝키(sk) 및 인증서(c)에 기반하여 함수(f)에 대한 사이닝키(sk_f)를 생성한다. 단계 308의 과정은 아래 수학식 5로 표현할 수 있다.

[0068] (수학식 5)

[0069] $sk_f = (sk, c)$

[0070] 다시 도 2를 참조하면, 단계 206에서 컴퓨팅 장치(12)는 함수 서명의 함수(f), 함수(f)에 대한 사이닝키(sk_f), 및 메시지(m)에 기반하여 메시지에 대한 함수 값(f(m))(즉, 메시지(m)를 공개키 또는 대칭키인 함수(f)로 암호화한 값) 및 최종 서명값(σ)을 생성한다.

[0071] 여기서, 함수(f)가 공개키인 경우, RSA(Rivest Shamir Adleman) 기반의 공개키 암호화 방식을 사용할 수 있다. 또한, 함수(f)가 대칭키인 경우, AES(Advanced Encryption Standard Algorithm) 기반의 대칭키 암호화 방식을 사용할 수 있다.

[0072] 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 구체적인 과정은 도 4를 참조하여 후술하기로 한다. 도 4는 개시되는 일 실시예에서, 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 생성하는 과정을 나타낸 흐름도이다.

[0073] 단계 402에서, 컴퓨팅 장치(12)는 메시지(m) 및 사이닝키(sk)에 서명 체계의 서명(Signature) 알고리즘을 적용하여 메시지에 대한 서명값(σ_m)을 산출한다. 여기서, 컴퓨팅 장치(12)는 함수(f)에 대한 사이닝키(sk_f)를 사이닝키(sk)와 인증서(c)로 파싱할 수 있다.

[0074] 예시적인 실시예에서, 컴퓨팅 장치(12)는 사이닝키(sk)로 메시지(m)를 서명(Signature)하여 메시지에 대한 서명값(σ_m)을 산출할 수 있다. 단계 402의 과정은 아래 수학식 6으로 표현할 수 있다.

[0075] (수학식 6)

[0076] $\sigma_m \leftarrow Sig.Sign(sk, m)$

[0077] 단계 404에서, 컴퓨팅 장치(12)는 메시지(m)를 함수(f)에 적용하여 메시지에 대한 함수 값(f(m))을 생성하고, 메시지(m), 인증서(c), 및 메시지에 대한 서명값(σ_m)에 기반하여 최종 서명값(σ)을 생성한다. 여기서, 최종 서명값(σ)은 아래 수학식 7로 표현될 수 있다.

[0078] (수학식 7)

[0079] $\sigma = (m, c, \sigma_m)$

[0080] 다시 도 2를 참조하면, 단계 208에서 컴퓨팅 장치(12)는 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 다른 컴퓨팅 장치(12)로 전송한다. 그러면, 다른 컴퓨팅 장치(12)는 마스터 검증키(mvk)에 기반하여 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 검증할 수 있다.

[0081] 다른 컴퓨팅 장치(12)가 메시지에 대한 함수 값(f(m)) 및 최종 서명값(σ)을 검증하는 과정은 도 5를 참조하여 후술하기로 한다. 도 5는 일 실시예에 따른 다른 컴퓨팅 장치(12)에서 마스터 검증키(mvk)에 기반하여 메시지에

대한 함수 값(f(m)) 및 최종 서명값(σ)을 검증하는 과정을 나타낸 흐름도이다.

[0082] 단계 502에서, 다른 컴퓨팅 장치(12)는 최종 서명값(σ)을 메시지(m), 인증서(c = (f, vk, σ_{vk})), 및 메시지에 대한 서명값(σ_m)으로 파싱한다. 단계 502의 과정은 아래 수학식 8로 표현할 수 있다.

[0083] (수학식 8)

[0084] $\sigma = (m, c = (f, vk, \sigma_{vk}), \sigma_m)$

[0085] 단계 504에서, 다른 컴퓨팅 장치(12)는 파싱한 메시지(m)를 함수(f)에 적용하여 메시지에 대한 함수 값(f(m))을 생성하며, 생성한 메시지에 대한 함수 값(f(m))이 컴퓨팅 장치(12)로부터 수신한 메시지에 대한 함수 값(f(m))과 일치하는지를 확인하여 검증한다.

[0086] 단계 506에서, 다른 컴퓨팅 장치(12)는 메시지(m) 및 검증키(vk)를 서명 체계의 검증 알고리즘에 적용하여 상기 파싱한 메시지에 대한 서명값(σ_m)을 검증한다. 단계 506의 과정은 아래 수학식 9로 표현할 수 있으며, 수학식 9의 값이 1이면 상기 파싱한 메시지에 대한 서명값(σ_m)이 유효함을 확인하게 된다.

[0087] (수학식 9)

[0088] $Sig.Verify(vk, m, \sigma_m) \rightarrow 1$

[0089] 단계 508에서, 다른 컴퓨팅 장치(12)는 마스터 검증키(mvk), 검증키(vk), 및 함수(f)를 서명 체계의 검증 알고리즘에 적용하여 상기 파싱한 검증키에 대한 서명값(σ_{vk})을 검증한다. 구체적으로, 다른 컴퓨팅 장치(12)는 마스터 검증키(mvk) 및 검증키(vk)에 함수(f)를 연결한(Concatenated) 값(f|vk)을 서명 체계의 검증 알고리즘에 적용하여 상기 파싱한 검증키에 대한 서명값(σ_{vk})을 검증할 수 있다. 단계 508의 과정은 아래 수학식 10로 표현할 수 있으며, 수학식 10의 값이 1이면 상기 파싱한 검증키에 대한 서명값(σ_{vk})이 유효함을 확인하게 된다.

[0090] 개시되는 실시예에서, 서명 알고리즘은 DSA(Digital Signature Algorithm), ECDSA(Elliptic Curve Digital Signature Algorithm), RSA(Rivest Shamir Adleman), ElGamal 등이 사용될 수 있다.

[0091] 개시되는 실시예에 의하면, 함수 서명의 함수(f)를 공개키 또는 대칭키로 설정하고, 함수(f)에 대한 사이닝키(sk_f)로 메시지(m)를 서명하여 메시지에 대한 함수 값(f(m))(즉, 메시지(m)를 공개키 또는 대칭키인 함수(f)로 암호화한 값) 및 최종 서명값(σ)을 생성함으로써, 메시지를 암호화함과 동시에 서명을 수행할 수 있게 된다.

[0093] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 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

[0095] 10 : 컴퓨팅 환경

12 : 컴퓨팅 장치

14 : 프로세서

16 : 컴퓨터 판독 가능 저장 매체

18 : 통신 버스

20 : 프로그램

22 : 입출력 인터페이스

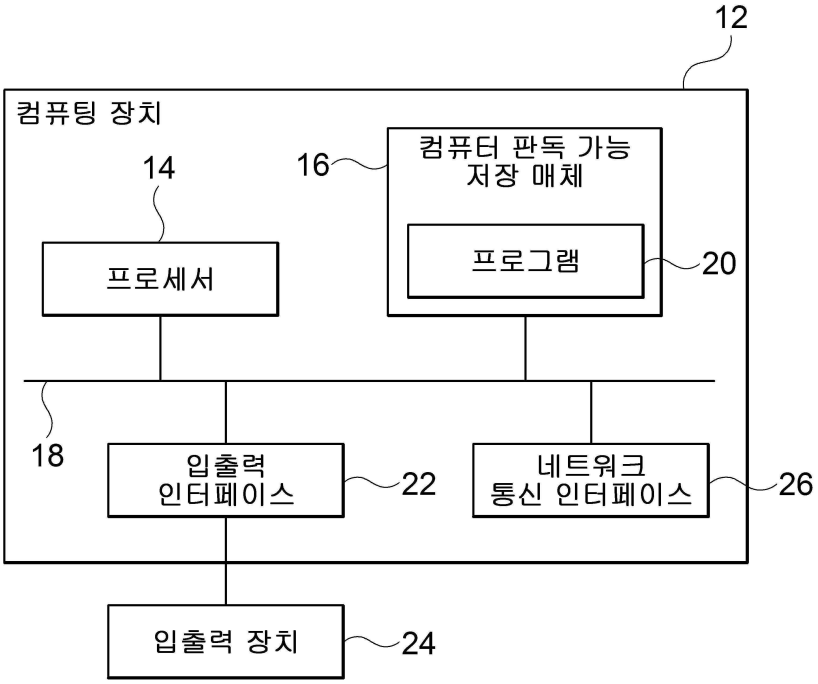
24 : 입출력 장치

26 : 네트워크 통신 인터페이스

도면

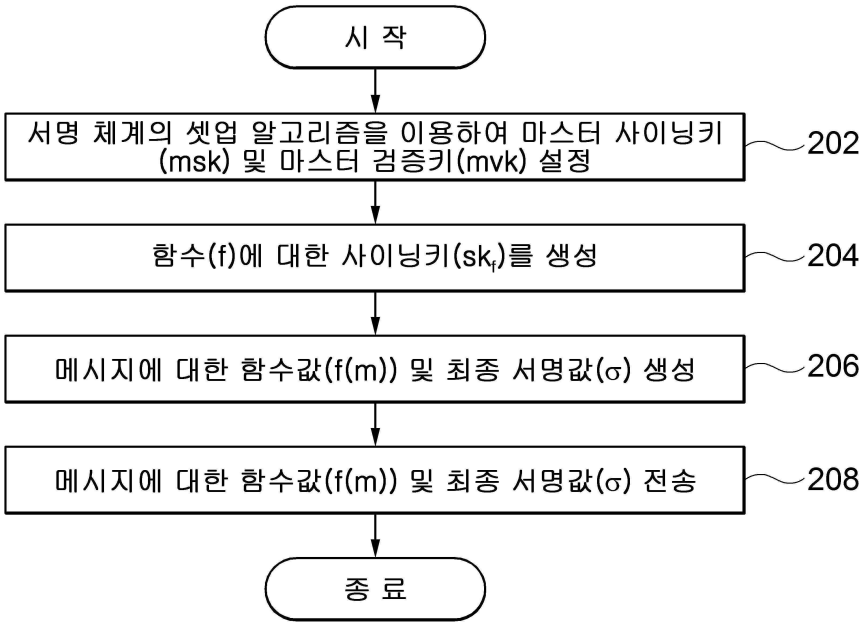
도면1

10

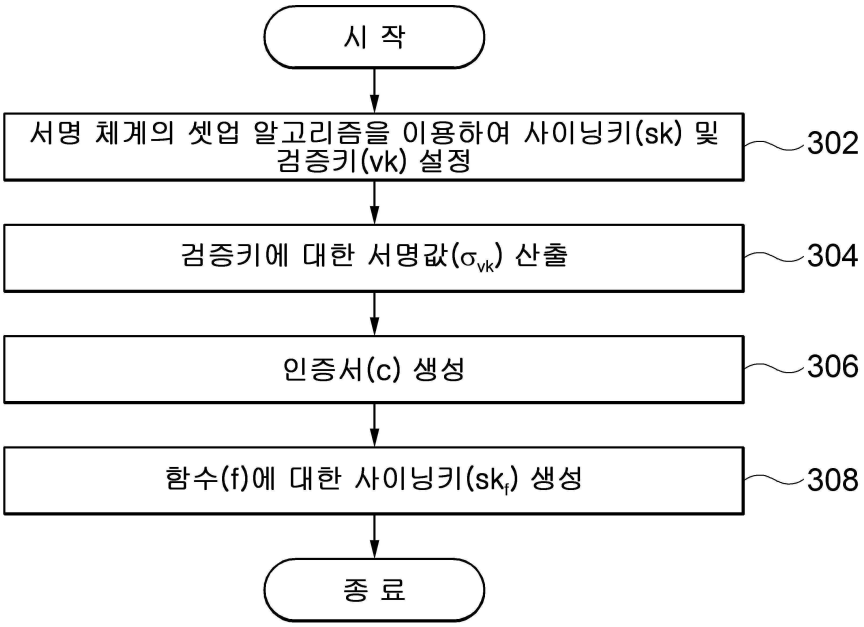


도면2

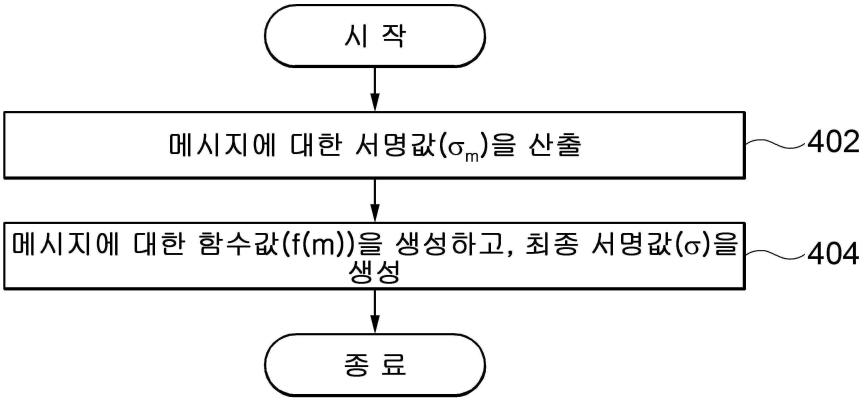
200



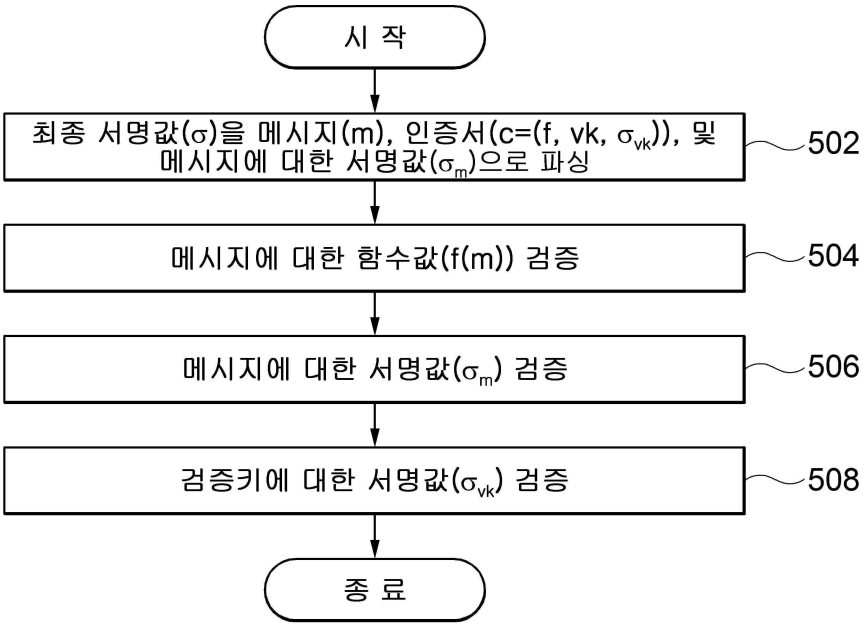
도면3


시 작
서명 체계의 셋업 알고리즘을 이용하여 사이닝키(sk) 및 검증키(vk) 설정
302
검증키에 대한 서명값(σ_{vk}) 산출
304
인증서(c) 생성
306
함수(f)에 대한 사이닝키(sk_f) 생성
308
종 료

도면4


시 작
메시지에 대한 서명값(σ_m)을 산출
402
메시지에 대한 함수값(f(m))을 생성하고, 최종 서명값(σ)을 생성
404
종 료

도면5


시 작
최종 서명값(σ)을 메시지(m), 인증서(c=(f, vk, σ_{vk})), 및 메시지에 대한 서명값(σ_m)으로 파싱
502
메시지에 대한 함수값(f(m)) 검증
504
메시지에 대한 서명값(σ_m) 검증
506
검증키에 대한 서명값(σ_{vk}) 검증
508
종 료