(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년08월31일
(11) 등록번호 10-2439195
(24) 등록일자 2022년08월29일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/06* (2006.01)
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)
(52) CPC특허분류
H04L 9/3255 (2013.01)
H04L 9/0643 (2013.01)
(21) 출원번호 10-2022-0055043
(22) 출원일자 2022년05월03일
심사청구일자 2022년05월03일
(56) 선행기술조사문헌
KR1020050042358 A
(뒷면에 계속)

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
이광수
서울특별시 광진구 능동로 209(군자동) 세종대학교 대양AI센터 726호
(74) 대리인
두호특허법인

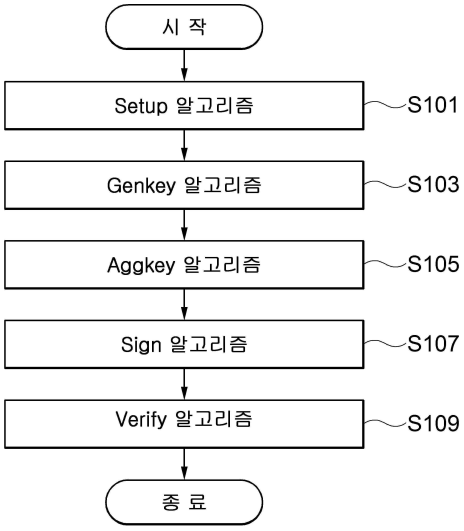
전체 청구항 수 : 총 21 항 심사관 : 양종필

(54) 발명의 명칭 **다중 서명 생성 방법 및 시스템과 이를 수행하기 위한 컴퓨팅 장치**

(57) 요 약

다중 서명 생성 방법과 시스템 및 이를 실행하기 위한 컴퓨팅 장치가 개시된다. 개시되는 일 실시예에 따른 다중 서명 생성 방법은, 관리 서버에서, 보안 상수를 입력으로 하여 공개 파라미터를 생성하고, 생성된 공개 파라미터를 송신하는 단계, 각 서명 단말에서, 공개 파라미터를 수신하고, 공개 파라미터를 이용하여 자신의 비밀키(SK_i)와 공개키(PK_i)를 생성하는 단계, 각 서명 단말에서, 자신의 공개키(PK_i)를 다른 서명 단말들과 상호 공유하여 공개키 리스트(LK)(LK = (PK_1, PK_2, 쩜, PK_n), n은 다중 서명을 수행하는 서명 단말의 전체 개수)를 생성하며, 공개키 리스트(LK) 및 공개 파라미터에 기반하여 합의된 공개키(AK)를 생성하는 단계, 및 각 서명 단말에서, 메시지(M), 공개 파라미터, 비밀키(SK_i), 공개키 리스트(LK), 및 합의된 공개키(AK)에 기반하여 다중 서명을 생성하는 단계를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 9/085 (2013.01)
H04L 9/30 (2013.01)

(56) 선행기술조사문헌
JP2011233943 A
KR1020210054146 A
KR101575030 B1
KR1020100018043 A
KR1020110070765 A
KR1020200003144 A*
*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152985
과제번호	2021-0-00518-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	데이터 경제를 위한 블록체인 기술개발(R&D)
연구과제명	블록체인 데이터 암호화 기반의 프라이버시 보호 기술개발
기 여 율	1/1
과제수행기관명	한양대학교산학협력단
연구기간	2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

관리 서버에서, 보안 상수를 입력으로 하여 공개 파라미터를 생성하고, 생성된 상기 공개 파라미터를 송신하는 단계;

각 서명 단말에서, 상기 공개 파라미터를 수신하고, 상기 공개 파라미터를 이용하여 자신의 비밀키(SK_i)와 공개키(PK_i)를 생성하는 단계;

각 서명 단말에서, 자신의 공개키(PK_i)를 다른 서명 단말들과 상호 공유하여 공개키 리스트(LK)(LK = (PK_1, PK_2, ..., PK_n), n은 다중 서명을 수행하는 서명 단말의 전체 개수)를 생성하며, 상기 공개키 리스트(LK) 및 상기 공개 파라미터에 기반하여 합의된 공개키(AK)를 생성하는 단계; 및

각 서명 단말에서, 메시지(M), 공개 파라미터, 비밀키(SK_i), 공개키 리스트(LK), 및 합의된 공개키(AK)에 기반하여 다중 서명을 생성하는 단계를 포함하고,

상기 공개 파라미터를 생성하는 단계는,

상기 보안 상수를 입력으로 하여 차수(order)가 p인 순환 그룹($\mathbb{G}$)을 생성하는 단계;

상기 순환 그룹($\mathbb{G}$)에서 한 쌍의 제1 생성원(generator)(g, h)를 각각 랜덤하게 선택하는 단계;

상기 순환 그룹($\mathbb{G}$) 중 지수(exponent) α($\alpha \in \mathbb{Z}_p$, $\mathbb{Z}$는 정수)를 랜덤하게 선택하고, 상기 선택된 지수 α 및 상기 한 쌍의 제1 생성원(g, h)에 기반하여 한 쌍의 제2 생성원(g_2, h_2)을 설정하는 단계;

기 설정된 입력에 대해 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하는 하나 이상의 해시 함수(hash function)를 설정하는 단계; 및

상기 순환 그룹($\mathbb{G}$), 순환 그룹의 차수(p), 한 쌍의 제1 생성원(g,h), 한 쌍의 제2 생성원(g_2, h_2), 및 해시 함수를 포함하는 공개 파라미터를 생성하는 단계를 포함하는, 다중 서명 생성 방법.

청구항 2

삭제

청구항 3

청구항 1에 있어서,

상기 한 쌍의 제2 생성원(g_2, h_2)을 설정하는 단계는,

상기 지수 α를 갖는 제1-1 생성원(g)을 제2-1 생성원(g_2)으로 설정($g_2 = g^{\alpha}$)하는 단계; 및

상기 지수 α를 갖는 제1-2 생성원(h)을 제2-2 생성원(h_2)으로 설정($h_2 = h^{\alpha}$)하는 단계를 포함하는, 다중 서명 생성 방법.

청구항 4

청구항 3에 있어서,

상기 해시 함수를 설정하는 단계는,

랜덤한 비트열을 입력으로 하여 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하도록 하는 제1 해시 함수(H_1)를 설정하는 단계;

랜덤한 비트열을 입력으로 하여 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하도록 하는 제2 해시 함수(H_2)를 설정하는 단계; 및

랜덤한 비트열을 입력으로 하여 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하도록 하는 제3 해시 함수(H_3)를 설정하는 단계를 포함하는, 다중 서명 생성 방법.

청구항 5

청구항 4에 있어서,

상기 비밀키(SK_i)를 생성하는 단계는,

상기 공개 파라미터에 포함된 순환 그룹($\mathbb{G}$) 중 제1 지수(x_{i1}) 및 제2 지수(x_{i2})를 랜덤하게 선택하는 단계; 및

상기 제1 지수(x_{i1}) 및 제2 지수(x_{i2})를 자신의 비밀키(SK_i)로 설정($SK_i = (x_{i1}, x_{i2})$)하는 단계를 포함하는, 다중 서명 생성 방법.

청구항 6

청구항 5에 있어서,

상기 공개키(PK_i)를 생성하는 단계는,

상기 제1 지수(x_{i1}) 및 상기 제2 지수(x_{i2})와 상기 공개 파라미터 중 한 쌍의 제1 생성원(g,h) 및 한 쌍의 제2 생성원(g_2, h_2)에 기반하여 제1 공개키 원소(X_i) 및 제2 공개키 원소(Y_i)를 포함하는 공개키($PK_i = (X_i, Y_i)$)를 생성하는, 다중 서명 생성 방법.

청구항 7

청구항 6에 있어서,

상기 공개키(PK_i)를 생성하는 단계는,

상기 제1-1 생성원(g) 및 제2-1 생성원(g_2)이 각각 제1 지수(x_{i1}) 및 제2 지수(x_{i2})를 갖도록 하여 제1 공개키 원소($X_i = g^{x_{i1}} g_2^{x_{i2}}$)를 생성하는 단계; 및

상기 제1-2 생성원(h) 및 제2-2 생성원(h_2)이 각각 제1 지수(x_{i1}) 및 제2 지수(x_{i2})를 갖도록 하여 제2 공개키 원소($Y_i = h^{x_{i1}} h_2^{x_{i2}}$)를 생성하는 단계를 포함하는, 다중 서명 생성 방법.

청구항 8

청구항 7에 있어서,

상기 합의된 공개키(AK)를 생성하는 단계는,

상기 공개키(PK_i), 공개키 리스트(LK), 및 공개 파라미터 중 해시 함수에 기반하여 자신의 합의 공개키 지수(a_i)를 산출하는 단계; 및

상기 공개키 리스트(LK) 및 자신의 합의 공개키 지수(a_i)에 기반하여 제1 합의된 공개키 원소(AX) 및 제2 합의된 공개키 원소(AY)를 포함하는 합의된 공개키(AK = (AX, AY))를 생성하는 단계를 포함하는, 다중 서명 생성 방법.

청구항 9

청구항 8에 있어서,

상기 자신의 합의 공개키 지수(a_i)를 산출하는 단계는,

상기 공개키(PK_i) 및 공개키 리스트(LK)를 상기 제3 해시 함수(H_3)에 입력하여 자신의 합의 공개키 지수(a_i)를 산출하는, 다중 서명 생성 방법.

청구항 10

청구항 8에 있어서,

상기 합의된 공개키(AK)를 생성하는 단계는,

상기 공개키 리스트(LK)의 모든 제1 공개키 원소(X_i)들에 자신의 합의 공개키 지수(a_i)를 갖도록 하고 이를 곱하여 제1 합의된 공개키 원소($AX = \prod_{i=1}^{n} X_i^{a_i}$)를 산출하는 단계; 및

상기 공개키 리스트(LK)의 모든 제2 공개키 원소(Y_i)들에 자신의 합의 공개키 지수(a_i)를 갖도록 하고 이를 곱하여 제2 합의된 공개키 원소($AY = \prod_{i=1}^{n} Y_i^{a_i}$)를 산출하는 단계를 포함하는, 다중 서명 생성 방법.

청구항 11

청구항 9에 있어서,

상기 다중 서명을 생성하는 단계는,

상기 메시지(M), 공개키 리스트(LK), 합의된 공개키(AK), 및 공개 파라미터의 해시 함수에 기반하여 메시지 관련 해시 값(c)을 산출하는 단계;

상기 공개 파라미터, 자신의 합의 공개키 지수(a_i), 자신의 비밀키(SK_i), 및 메시지 관련 해시 값(c)에 기반하여 제1 부분 서명(s_{i1}) 및 제2 부분 서명(s_{i2})을 포함하는 자신의 한 쌍의 부분 서명(s_{i1}, s_{i2})을 생성하는 단계;

상기 자신의 한 쌍의 부분 서명(s_{i1}, s_{i2})을 다른 서명 단말들과 공유하는 단계;

상기 자신의 한 쌍의 부분 서명(s_{i1}, s_{i2}) 및 다른 서명 단말들의 한 쌍의 부분 서명$\{(s_{j1}, s_{j2})\}_{1\le j\ne i\le n}$에 기반하여 제1 전체 부분 서명($s_1$) 및 제2 전체 부분 서명($s_2$)을 각각 생성하는 단계; 및

상기 메시지 관련 해시 값(c), 제1 전체 부분 서명(s_1), 및 제2 전체 부분 서명(s_2)에 기반하여 다중 서명을 생성하는 단계를 포함하는, 다중 서명 생성 방법.

청구항 12

청구항 11에 있어서,

상기 메시지 관련 해시 값(c)을 산출하는 단계는,

상기 메시지(M) 및 상기 공개 파라미터에 기반하여 자신의 랜덤 약속 값(R_i)을 산출하는 단계;

상기 자신의 랜덤 약속 값(R_i)을 다른 서명 단말들과 공유하는 단계;

상기 자신의 랜덤 약속 값(R_i)과 다른 서명 단말들의 랜덤 약속 값$\{R_j\}_{1\le j\neq i\le n}$에 기반하여 전체 랜덤 약속 값(AR)을 산출하는 단계; 및

상기 메시지(M), 공개키 리스트(LK), 합의된 공개키(AK), 전체 랜덤 약속 값(AR)을 상기 제2 해시 함수(H_2)에 입력하여 메시지 관련 해시 값(c)을 산출하는 단계를 포함하는, 다중 서명 생성 방법.

청구항 13

청구항 12에 있어서,

상기 자신의 랜덤 약속 값(R_i)을 산출하는 단계는,

상기 공개 파라미터에 포함된 순환 그룹($\mathbb{G}$)에서 제1 랜덤 약속 지수(r_{i1}) 및 제2 랜덤 약속 지수(r_{i2})를 각각 랜덤하게 선택하는 단계; 및

상기 메시지(M), 한 쌍의 제1 생성원(g,h), 한 쌍의 제2 생성원(g_2, h_2), 상기 제1 해시 함수(H_1), 제1 랜덤 약속 지수(r_{i1}), 및 제2 랜덤 약속 지수(r_{i2})에 기반하여 자신의 랜덤 약속 값(R_i)을 산출하는 단계를 포함하는, 다중 서명 생성 방법.

청구항 14

청구항 13에 있어서,

하기의 수학식에 의해 자신의 랜덤 약속 값(R_i)을 산출하는, 다중 서명 생성 방법.

(수학식)

$$R_i = (g^{H_1(M)}h)^{ri1}(g_2{}^{H_1(M)}h_2)^{ri2}$$

청구항 15

청구항 13에 있어서,

상기 전체 랜덤 약속 값(AR)을 산출하는 단계는,

상기 자신의 랜덤 약속 값(R_i)과 다른 서명 단말들의 랜덤 약속 값$\{R_j\}_{1\le j\neq i\le n}$을 곱하여 전체 랜덤 약속 값($AR = \prod_{i=1}^{n} R_i$)을 산출하는, 다중 서명 생성 방법.

청구항 16

청구항 13에 있어서,

상기 자신의 한 쌍의 부분 서명(s_{i1}, s_{i2})을 생성하는 단계는,

상기 제1 랜덤 약속 지수(r_{i1}), 비밀키(SK_i)의 제1 지수(x_{i1}), 자신의 합의 공개키 지수(a_i), 및 메시지 관련 해시 값(c)에 기반하여 제1 부분 서명(s_{i1})을 생성하는 단계; 및

상기 제2 랜덤 약속 지수(r_{i2}), 비밀키(SK_i)의 제2 지수(x_{i2}), 자신의 합의 공개키 지수(a_i), 및 메시지 관련 해시 값(c)에 기반하여 제2 부분 서명(s_{i2})을 생성하는 단계를 포함하는, 다중 서명 생성 방법.

청구항 17

청구항 16에 있어서,

상기 제1 부분 서명(s_{i1})은, 하기의 수학식에 의해 생성하고,

(수학식)

$s_{i1} = r_{i1} + x_{i1}a_ic$

상기 제2 부분 서명(s_{i2})은, 하기의 수학식에 의해 생성하는, 다중 서명 생성 방법.

(수학식)

$s_{i2} = r_{i2} + x_{i2}a_ic$

청구항 18

청구항 16에 있어서,

상기 제1 전체 부분 서명(s_1)을 생성하는 단계는,

상기 자신의 제1 부분 서명과 다른 서명 단말들의 제1 부분 서명들을 합산하여 제1 전체 부분 서명($s_1 = \sum_{i=1}^{n} s_{i1}$)을 생성하고,

상기 제2 전체 부분 서명(s_2)을 각각 생성하는 단계는,

상기 자신의 제2 부분 서명과 다른 서명 단말들의 제2 부분 서명들을 합산하여 제2 전체 부분 서명($s_2 = \sum_{i=1}^{n} s_{i2}$)을 생성하는, 다중 서명 생성 방법.

청구항 19

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되고, 다중 서명을 생성하기 위한 방법으로서,

다중 서명을 위한 공개 파라미터를 수신하는 단계;

상기 공개 파라미터를 이용하여 자신의 비밀키(SK_i)와 공개키(PK_i)를 생성하는 단계;

상기 자신의 공개키(PK_i)를 상기 다중 서명을 수행하는 다른 서명 단말들과 상호 공유하여 공개키 리스트(LK)(LK = (PK_1, PK_2, ..., PK_n), n은 다중 서명을 수행하는 서명 단말의 전체 개수)를 생성하며, 상기 공개키 리스트(LK) 및 상기 공개 파라미터에 기반하여 합의된 공개키(AK)를 생성하는 단계; 및

기 설정된 메시지(M), 공개 파라미터, 비밀키(SK_i), 공개키 리스트(LK), 및 합의된 공개키(AK)에 기반하여 다중 서명을 생성하는 단계를 포함하고,

상기 공개 파라미터의 생성은,

보안 상수를 입력으로 하여 차수(order)가 p인 순환 그룹($\mathbb{G}$)을 생성하고, 상기 순환 그룹($\mathbb{G}$)에서 한 쌍의 제1 생성원(generator)(g, h)를 각각 랜덤하게 선택하며, 상기 순환 그룹($\mathbb{G}$) 중 지수(exponent) α($\alpha \in \mathbb{Z}_p$, $\mathbb{Z}$는 정수)를 랜덤하게 선택하고 상기 선택된 지수 α 및 상기 한 쌍의 제1 생성원(g, h)에 기반하여 한 쌍의 제2 생성원(g_2, h_2)을 설정하며, 기 설정된 입력에 대해 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하는 하나 이상의 해시 함수(hash function)를 설정하고, 상기 순환 그룹($\mathbb{G}$), 순환 그룹의 차수(p), 한 쌍의 제1 생성원(g,h), 한 쌍의 제2 생성원(g_2, h_2), 및 해시 함수를 포함하여 공개 파라미터를 생성하는, 다중 서명 생성 방법.

청구항 20

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되고, 다중 서명을 생성하기 위한 방법으로서,

보안 상수를 입력으로 하여 공개 파라미터를 생성하는 단계; 및

상기 공개 파라미터를 다중 서명을 수행하는 복수 개의 서명 단말로 각각 송신하는 단계를 포함하며,

상기 공개 파라미터를 생성하는 단계는,

상기 보안 상수를 입력으로 하여 차수(order)가 p인 순환 그룹($\mathbb{G}$)을 생성하는 단계;

상기 순환 그룹($\mathbb{G}$)에서 한 쌍의 제1 생성원(generator)(g, h)를 각각 랜덤하게 선택하는 단계;

상기 순환 그룹($\mathbb{G}$) 중 지수(exponent) α($\alpha \in \mathbb{Z}_p$, $\mathbb{Z}$는 정수)를 랜덤하게 선택하고, 상기 선택된 지수 α 및 상기 한 쌍의 제1 생성원(g, h)에 기반하여 한 쌍의 제2 생성원(g_2, h_2)을 설정하는 단계;

기 설정된 입력에 대해 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하는 하나 이상의 해시 함수(hash function)를 설정하는 단계; 및

상기 순환 그룹($\mathbb{G}$), 순환 그룹의 차수(p), 한 쌍의 제1 생성원(g,h), 한 쌍의 제2 생성원(g_2, h_2), 및 해시 함수를 포함하는 공개 파라미터를 생성하는 단계를 포함하는, 다중 서명 생성 방법.

청구항 21

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,

다중 서명을 위한 공개 파라미터를 수신하기 위한 명령;

상기 공개 파라미터를 이용하여 자신의 비밀키(SK_i)와 공개키(PK_i)를 생성하기 위한 명령;

상기 자신의 공개키(PK_i)를 상기 다중 서명을 수행하는 다른 서명 단말들과 상호 공유하여 공개키 리스트(LK)(LK = (PK_1, PK_2, ..., PK_n), n은 다중 서명을 수행하는 서명 단말의 전체 개수)를 생성하며, 상기 공개키

리스트(LK) 및 상기 공개 파라미터에 기반하여 합의된 공개키(AK)를 생성하기 위한 명령; 및

기 설정된 메시지(M), 공개 파라미터, 비밀키(SK_i), 공개키 리스트(LK), 및 합의된 공개키(AK)에 기반하여 다중 서명을 생성하기 위한 명령을 포함하고,

상기 공개 파라미터의 생성을 위한 명령은,

보안 상수를 입력으로 하여 차수(order)가 p인 순환 그룹($\mathbb{G}$)을 생성하기 위한 명령;

상기 순환 그룹($\mathbb{G}$)에서 한 쌍의 제1 생성원(generator)(g, h)를 각각 랜덤하게 선택하기 위한 명령;

상기 순환 그룹($\mathbb{G}$) 중 지수(exponent) α(α∈$\mathbb{Z}_p$, $\mathbb{Z}$는 정수)를 랜덤하게 선택하고, 상기 선택된 지수 α 및 상기 한 쌍의 제1 생성원(g, h)에 기반하여 한 쌍의 제2 생성원(g_2, h_2)을 설정하기 위한 명령;

기 설정된 입력에 대해 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하는 하나 이상의 해시 함수(hash function)를 설정하기 위한 명령; 및

상기 순환 그룹($\mathbb{G}$), 순환 그룹의 차수(p), 한 쌍의 제1 생성원(g,h), 한 쌍의 제2 생성원(g_2, h_2), 및 해시 함수를 포함하는 공개 파라미터를 생성하기 위한 명령을 포함하는, 컴퓨팅 장치.

청구항 22

보안 상수를 입력으로 하여 공개 파라미터를 생성하고, 생성된 상기 공개 파라미터를 송신하는 관리 서버; 및

상기 공개 파라미터를 수신하여 다중 서명을 생성하는 복수 개의 서명 단말을 포함하며,

상기 복수 개의 서명 단말 각각은,

상기 공개 파라미터를 이용하여 자신의 비밀키(SK_i)와 공개키(PK_i)를 생성하고, 자신의 공개키(PK_i)를 다른 서명 단말들과 상호 공유하여 공개키 리스트(LK)(LK = (PK_1, PK_2, ..., PK_n), n은 다중 서명을 수행하는 서명 단말의 전체 개수)를 생성하며, 상기 공개키 리스트(LK) 및 상기 공개 파라미터에 기반하여 합의된 공개키(AK)를 생성하며, 메시지(M), 공개 파라미터, 비밀키(SK_i), 공개키 리스트(LK), 및 합의된 공개키(AK)에 기반하여 다중 서명을 생성하고,

상기 관리 서버는,

상기 보안 상수를 입력으로 하여 차수(order)가 p인 순환 그룹($\mathbb{G}$)을 생성하고, 상기 순환 그룹($\mathbb{G}$)에서 한 쌍의 제1 생성원(generator)(g, h)를 각각 랜덤하게 선택하며, 상기 순환 그룹($\mathbb{G}$) 중 지수(exponent) α(α∈$\mathbb{Z}_p$, $\mathbb{Z}$는 정수)를 랜덤하게 선택하고, 상기 선택된 지수 α 및 상기 한 쌍의 제1 생성원(g, h)에 기반하여 한 쌍의 제2 생성원(g_2, h_2)을 설정하며, 기 설정된 입력에 대해 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하는 하나 이상의 해시 함수(hash function)를 설정하고, 상기 순환 그룹($\mathbb{G}$), 순환 그룹의 차수(p), 한 쌍의 제1 생성원(g,h), 한 쌍의 제2 생성원(g_2, h_2), 및 해시 함수를 포함하는 공개 파라미터를 생성하는, 다중 서명 생성 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예는 다중 서명 생성 기술과 관련된다.

배 경 기 술

[0003] 한 명의 서명자가 하나의 정당한 서명을 생성하는 기존의 전자 서명(Digital Signature) 기법과는 달리 다중 서

명(Multi Signature) 기법은 여러 명의 공동 서명자들이 함께 여러 라운드에 걸쳐 서명 프로토콜을 수행하여 하나의 완성된 서명을 생성해낸다. 서명 프로토콜이 진행되는 라운드 수(n)에 따라 n 라운드 다중 서명으로 명시된다.

[0004] 다중 서명 기법에서는 모든 사용자의 비밀키가 사용되어야 하나의 정당한 서명이 생성될 수 있다. 다중 서명 기법에서는 공격자가 서명을 위조하려 할 때, 서명에 참여하는 n명의 공동 서명자의 비밀키 중 (n-1)개의 비밀키를 알아도 단 한 명의 비밀키를 알지 못한다면 정당한 서명을 위조해낼 수 없어야 한다.

[0005] 대표적인 전자 서명 기법 중 하나인 Schnorr 전자 서명 기법을 확장해 다중 서명으로 설계하는 다양한 연구들이 수행되어 왔으나, Schnorr 전자 서명 기법을 단순하게 확장할 경우 단 한 명의 서명키만 알더라도 정당한 다중 서명을 생성할 수 있는 로그 키 공격(Rouge Key Attack)에 취약하게 된다. 그리고, Schnorr 전자 서명을 기반으로 설계된 다중 서명 기법들은 확장이 용이하지만, 특정 비트 사이즈의 안정성을 보장하려면 4배의 비트 사이즈에 해당하는 파라미터를 사용해야 하는데, 큰 사이즈의 파라미터를 사용할수록 그 효율성은 낮아지게 된다.

[0006] 이에 Schnorr 서명 구조가 아닌 Okamoto 서명 구조를 이용하여 특정 비트 사이즈의 안전성이 필요할 때 2배의 비트 사이즈에 해당하는 파라미터를 사용하는 기법이 제안되었으나, 이러한 기법은 서명 알고리즘의 중간 출력값인 부분 서명과 최종 서명이 같은 수학적 구조를 가지고 있어 Wagner 알고리즘에 취약하다는 문제점이 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 한국등록특허공보 제10-1849920호(2018.04.19)

발명의 내용

해결하려는 과제

[0009] 개시되는 실시예는 새로운 기법의 다중 서명 생성 기술을 제공하기 위한 것이다.

과제의 해결 수단

[0011] 개시되는 일 실시예에 따른 다중 서명 생성 방법은, 관리 서버에서, 보안 상수를 입력으로 하여 공개 파라미터를 생성하고, 생성된 상기 공개 파라미터를 송신하는 단계; 각 서명 단말에서, 상기 공개 파라미터를 수신하고, 상기 공개 파라미터를 이용하여 자신의 비밀키(SK_i)와 공개키(PK_i)를 생성하는 단계; 각 서명 단말에서, 자신의 공개키(PK_i)를 다른 서명 단말들과 상호 공유하여 공개키 리스트(LK)(LK = (PK_1, PK_2, ..., PK_n), n은 다중 서명을 수행하는 서명 단말의 전체 개수)를 생성하며, 상기 공개키 리스트(LK) 및 상기 공개 파라미터에 기반하여 합의된 공개키(AK)를 생성하는 단계; 및 각 서명 단말에서, 메시지(M), 공개 파라미터, 비밀키(SK_i), 공개키 리스트(LK), 및 합의된 공개키(AK)에 기반하여 다중 서명을 생성하는 단계를 포함한다.

[0012] 상기 공개 파라미터를 생성하는 단계는, 상기 보안 상수를 입력으로 하여 차수(order)가 p인 순환 그룹($\mathbb{G}$)을 생성하는 단계; 상기 순환 그룹($\mathbb{G}$)에서 한 쌍의 제1 생성원(generator)(g, h)를 각각 랜덤하게 선택하는 단계; 상기 순환 그룹($\mathbb{G}$) 중 지수(exponent) α(α$\in \mathbb{Z}_p$, $\mathbb{Z}$는 정수)를 랜덤하게 선택하고, 상기 선택된 지수 α 및 상기 한 쌍의 제1 생성원(g, h)에 기반하여 한 쌍의 제2 생성원(g_2, h_2)을 설정하는 단계; 기 설정된 입력에 대해 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하는 하나 이상의 해시 함수(hash function)를 설정하는 단계; 및 상기 순환 그룹($\mathbb{G}$), 순환 그룹의 차수(p), 한 쌍의 제1 생성원(g,h), 한 쌍의 제2 생성원(g_2, h_2), 및 해시 함수를 포함하는 공개 파라미터를 생성하는 단계를 포함할 수 있다.

[0013] 상기 한 쌍의 제2 생성원(g_2, h_2)을 설정하는 단계는, 상기 지수 α를 갖는 제1-1 생성원(g)을 제2-1 생성원(g_2)으로 설정($g_2 = g^{\alpha}$)하는 단계; 및 상기 지수 α를 갖는 제1-2 생성원(h)을 제2-2 생성원(h_2)으로 설정(h_2 =

h^{α})하는 단계를 포함할 수 있다.

[0014] 상기 해시 함수를 설정하는 단계는, 랜덤한 비트열을 입력으로 하여 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하도록 하는 제1 해시 함수(H_1)를 설정하는 단계; 랜덤한 비트열을 입력으로 하여 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하도록 하는 제2 해시 함수(H_2)를 설정하는 단계; 및 랜덤한 비트열을 입력으로 하여 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하도록 하는 제3 해시 함수(H_3)를 설정하는 단계를 포함할 수 있다.

[0015] 상기 비밀키(SK_i)를 생성하는 단계는, 상기 공개 파라미터에 포함된 순환 그룹($\mathbb{G}$) 중 제1 지수(x_{i1}) 및 제2 지수(x_{i2})를 랜덤하게 선택하는 단계; 및 상기 제1 지수(x_{i1}) 및 제2 지수(x_{i2})를 자신의 비밀키(SK_i)로 설정($SK_i = (x_{i1}, x_{i2})$)하는 단계를 포함할 수 있다.

[0016] 상기 공개키(PK_i)를 생성하는 단계는, 상기 제1 지수(x_{i1}) 및 상기 제2 지수(x_{i2})와 상기 공개 파라미터 중 한 쌍의 제1 생성원(g,h) 및 한 쌍의 제2 생성원(g_2, h_2)에 기반하여 제1 공개키 원소(X_i) 및 제2 공개키 원소(Y_i)를 포함하는 공개키($PK_i = (X_i, Y_i)$)를 생성할 수 있다.

[0017] 상기 공개키(PK_i)를 생성하는 단계는, 상기 제1-1 생성원(g) 및 제2-1 생성원(g_2)이 각각 제1 지수(x_{i1}) 및 제2 지수(x_{i2})를 갖도록 하여 제1 공개키 원소($X_i = g^{x_{i1}} g_2^{x_{i2}}$)를 생성하는 단계; 및 상기 제1-2 생성원(h) 및 제2-2 생성원(h_2)이 각각 제1 지수(x_{i1}) 및 제2 지수(x_{i2})를 갖도록 하여 제2 공개키 원소($Y_i = h^{x_{i1}} h_2^{x_{i2}}$)를 생성하는 단계를 포함할 수 있다.

[0018] 상기 합의된 공개키(AK)를 생성하는 단계는, 상기 공개키(PK_i), 공개키 리스트(LK), 및 공개 파라미터 중 해시 함수에 기반하여 자신의 합의 공개키 지수(a_i)를 산출하는 단계; 및 상기 공개키 리스트(LK) 및 자신의 합의 공개키 지수(a_i)에 기반하여 제1 합의된 공개키 원소(AX) 및 제2 합의된 공개키 원소(AY)를 포함하는 합의된 공개키($AK = (AX, AY)$)를 생성하는 단계를 포함할 수 있다.

[0019] 상기 자신의 합의 공개키 지수(a_i)를 산출하는 단계는, 상기 공개키(PK_i) 및 공개키 리스트(LK)를 상기 제3 해시 함수(H_3)에 입력하여 자신의 합의 공개키 지수(a_i)를 산출할 수 있다.

[0020] 상기 합의된 공개키(AK)를 생성하는 단계는, 상기 공개키 리스트(LK)의 모든 제1 공개키 원소(X_i)들에 자신의 합의 공개키 지수(a_i)를 갖도록 하고 이를 곱하여 제1 합의된 공개키 원소($AX = \prod_{i=1}^{n} X_i^{a_i}$)를 산출하는 단계; 및 상기 공개키 리스트(LK)의 모든 제2 공개키 원소(Y_i)들에 자신의 합의 공개키 지수(a_i)를 갖도록 하고 이를 곱하여 제2 합의된 공개키 원소($AY = \prod_{i=1}^{n} Y_i^{a_i}$)를 산출하는 단계를 포함할 수 있다.

[0021] 상기 다중 서명을 생성하는 단계는, 상기 메시지(M), 공개키 리스트(LK), 합의된 공개키(AK), 및 공개 파라미터의 해시 함수에 기반하여 메시지 관련 해시 값(c)을 산출하는 단계; 상기 공개 파라미터, 자신의 합의 공개키 지수(a_i), 자신의 비밀키(SK_i), 및 메시지 관련 해시 값(c)에 기반하여 제1 부분 서명(s_{i1}) 및 제2 부분 서명(s_{i2})을 포함하는 자신의 한 쌍의 부분 서명(s_{i1}, s_{i2})을 생성하는 단계; 상기 자신의 한 쌍의 부분 서명(s_{i1}, s_{i2})을 다른 서명 단말들과 공유하는 단계; 상기 자신의 한 쌍의 부분 서명(s_{i1}, s_{i2}) 및 다른 서명 단말들의 한 쌍의 부분 서명$\{(s_{j1}, s_{j2})\}_{1\le j\ne i\le n}$에 기반하여 제1 전체 부분 서명($s_1$) 및 제2 전체 부분 서명($s_2$)을 각각 생성하는 단계; 및 상기 메시지 관련 해시 값(c), 제1 전체 부분 서명(s_1), 및 제2 전체 부분 서명(s_2)에 기반하여 다중 서명을 생성하는 단계를 포함할 수 있다.

[0022] 상기 메시지 관련 해시 값(c)을 산출하는 단계는, 상기 메시지(M) 및 상기 공개 파라미터에 기반하여 자신의 랜덤 약속 값(R_i)을 산출하는 단계; 상기 자신의 랜덤 약속 값(R_i)을 다른 서명 단말들과 공유하는 단계; 상기 자신의 랜덤 약속 값(R_i)과 다른 서명 단말들의 랜덤 약속 값$\{R_j\}_{1\le j\ne i\le n}$에 기반하여 전체 랜덤 약속 값(AR)을 산

출하는 단계; 및 상기 메시지(M), 공개키 리스트(LK), 합의된 공개키(AK), 전체 랜덤 약속 값(AR)을 상기 제2 해시 함수(H_2)에 입력하여 메시지 관련 해시 값(c)을 산출하는 단계를 포함할 수 있다.

[0023] 상기 자신의 랜덤 약속 값(R_i)을 산출하는 단계는, 상기 공개 파라미터에 포함된 순환 그룹($\mathbb{G}$)에서 제1 랜덤 약속 지수(r_{i1}) 및 제2 랜덤 약속 지수(r_{i2})를 각각 랜덤하게 선택하는 단계; 및 상기 메시지(M), 한 쌍의 제1 생성원(g,h), 한 쌍의 제2 생성원(g_2, h_2), 상기 제1 해시 함수(H_1), 제1 랜덤 약속 지수(r_{i1}), 및 제2 랜덤 약속 지수(r_{i2})에 기반하여 자신의 랜덤 약속 값(R_i)을 산출하는 단계를 포함할 수 있다.

[0024] 상기 수학식에 의해 자신의 랜덤 약속 값(R_i)을 산출할 수 있다.

[0025] (수학식)

[0026] $$R_i = (g^{H_1(M)}h)^{ri1}(g_2{}^{H_1(M)}h_2)^{ri2}$$

[0027] 상기 전체 랜덤 약속 값(AR)을 산출하는 단계는, 상기 자신의 랜덤 약속 값(R_i)과 다른 서명 단말들의 랜덤 약속 값$\{R_j\}_{1\le j\neq i\le n}$을 곱하여 전체 랜덤 약속 값($AR = \prod_{i=1}^{n} R_i$)을 산출할 수 있다.

[0028] 상기 자신의 한 쌍의 부분 서명(s_{i1}, s_{i2})을 생성하는 단계는, 상기 제1 랜덤 약속 지수(r_{i1}), 비밀키(SK_i)의 제1 지수(x_{i1}), 자신의 합의 공개키 지수(a_i), 및 메시지 관련 해시 값(c)에 기반하여 제1 부분 서명(s_{i1})을 생성하는 단계; 및 상기 제2 랜덤 약속 지수(r_{i2}), 비밀키(SK_i)의 제2 지수(x_{i2}), 자신의 합의 공개키 지수(a_i), 및 메시지 관련 해시 값(c)에 기반하여 제2 부분 서명(s_{i2})을 생성하는 단계를 포함할 수 있다.

[0029] 상기 제1 부분 서명(s_{i1})은, 하기의 수학식에 의해 생성하고,

[0030] (수학식)

[0031] $s_{i1} = r_{i1} + x_{i1}a_ic$

[0032] 상기 제2 부분 서명(s_{i2})은, 하기의 수학식에 의해 생성할 수 있다.

[0033] (수학식)

[0034] $s_{i2} = r_{i2} + x_{i2}a_ic$

[0035] 상기 제1 전체 부분 서명(s_1)을 생성하는 단계는, 상기 자신의 제1 부분 서명과 다른 서명 단말들의 제1 부분 서명들을 합산하여 제1 전체 부분 서명($s_1 = \sum_{i=1}^{n} s_{i1}$)을 생성하고, 상기 제2 전체 부분 서명($s_2$)을 각각 생성하는 단계는, 상기 자신의 제2 부분 서명과 다른 서명 단말들의 제2 부분 서명들을 합산하여 제2 전체 부분 서명($s_2 = \sum_{i=1}^{n} s_{i2}$)을 생성할 수 있다.

[0036] 개시되는 다른 실시예에 따른 다중 서명 생성 방법은, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되고, 다중 서명을 생성하기 위한 방법으로서, 다중 서명을 위한 공개 파라미터를 수신하는 단계; 상기 공개 파라미터를 이용하여 자신의 비밀키(SK_i)와 공개키(PK_i)를 생성하는 단계; 상기 자신의 공개키(PK_i)를 상기 다중 서명을 수행하는 다른 서명 단말들과 상호 공유하여 공개키 리스트(LK)(LK = (PK_1, PK_2, ..., PK_n), n은 다중 서명을 수행하는 서명 단말의 전체 개수)를 생성하며, 상기 공개키 리스트(LK) 및 상기 공개 파라미터에 기반하여 합의된 공개키(AK)를 생성하는 단계; 및 기 설정된 메시지(M), 공개 파라미터, 비밀키(SK_i), 공개키 리스트(LK), 및 합의된 공개키(AK)에 기반하여 다중 서명을 생성하는 단계를 포함한다.

[0037] 개시되는 또 다른 실시예에 따른 다중 서명 생성 방법은, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되고, 다중 서명을 생성하기 위한 방법으로서, 보안 상수를 입력으로 하여 공개 파라미터를 생성하는 단계; 및 상기 공개 파라미터를 다중 서명을 수행하는 복수 개의 서명 단말로 각각 송신하는 단계를 포함하며, 상기 공개 파라미터를

생성하는 단계는, 상기 보안 상수를 입력으로 하여 차수(order)가 p인 순환 그룹($\mathbb{G}$)을 생성하는 단계; 상기 순환 그룹($\mathbb{G}$)에서 한 쌍의 제1 생성원(generator)(g, h)를 각각 랜덤하게 선택하는 단계; 상기 순환 그룹($\mathbb{G}$) 중 지수(exponent) α(α∈$\mathbb{Z}_p$, $\mathbb{Z}$는 정수)를 랜덤하게 선택하고, 상기 선택된 지수 α 및 상기 한 쌍의 제1 생성원(g, h)에 기반하여 한 쌍의 제2 생성원(g_2, h_2)을 설정하는 단계; 기 설정된 입력에 대해 상기 순환 그룹($\mathbb{G}$)의 지수를 출력하는 하나 이상의 해시 함수(hash function)를 설정하는 단계; 및 상기 순환 그룹($\mathbb{G}$), 순환 그룹의 차수(p), 한 쌍의 제1 생성원(g,h), 한 쌍의 제2 생성원(g_2, h_2), 및 해시 함수를 포함하는 공개 파라미터를 생성하는 단계를 포함한다.

[0038] 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, 다중 서명을 위한 공개 파라미터를 수신하기 위한 명령; 상기 공개 파라미터를 이용하여 자신의 비밀키(SK_i)와 공개키(PK_i)를 생성하기 위한 명령; 상기 자신의 공개키(PK_i)를 상기 다중 서명을 수행하는 다른 서명 단말들과 상호 공유하여 공개키 리스트(LK)(LK = (PK_1, PK_2, ..., PK_n), n은 다중 서명을 수행하는 서명 단말의 전체 개수)를 생성하며, 상기 공개키 리스트(LK) 및 상기 공개 파라미터에 기반하여 합의된 공개키(AK)를 생성하기 위한 명령; 및 기 설정된 메시지(M), 공개 파라미터, 비밀키(SK_i), 공개키 리스트(LK), 및 합의된 공개키(AK)에 기반하여 다중 서명을 생성하기 위한 명령을 포함한다.

[0039] 개시되는 일 실시예에 따른 다중 서명 생성 시스템은, 보안 상수를 입력으로 하여 공개 파라미터를 생성하고, 생성된 상기 공개 파라미터를 송신하는 관리 서버; 및 상기 공개 파라미터를 수신하여 다중 서명을 생성하는 복수 개의 서명 단말을 포함하며, 상기 복수 개의 서명 단말 각각은, 상기 공개 파라미터를 이용하여 자신의 비밀키(SK_i)와 공개키(PK_i)를 생성하고, 자신의 공개키(PK_i)를 다른 서명 단말들과 상호 공유하여 공개키 리스트(LK)(LK = (PK_1, PK_2, ..., PK_n), n은 다중 서명을 수행하는 서명 단말의 전체 개수)를 생성하며, 상기 공개키 리스트(LK) 및 상기 공개 파라미터에 기반하여 합의된 공개키(AK)를 생성하며, 메시지(M), 공개 파라미터, 비밀키(SK_i), 공개키 리스트(LK), 및 합의된 공개키(AK)에 기반하여 다중 서명을 생성한다.

발명의 효과

[0041] 개시되는 실시예에 의하면, 관리 서버는 공개 파라미터를 생성한 후 별도의 비밀 정보를 관리하지 않으며, 각 서명 단말은 신뢰 기관의 도움 없이 공개 파라미터를 이용하여 비밀키와 공개키를 생성할 수 있으며, 다중 서명의 안전성을 높일 수 있게 된다. 그리고, 다중 서명은 블록체인 기반의 시스템에 적용할 수 있으며, 블록체인 기반의 시스템의 보안성을 높일 수 있게 된다.

도면의 간단한 설명

[0043] 도 1은 본 발명의 일 실시예에 따른 다중 서명 생성 시스템의 구성을 나타낸 도면

도 2는 본 발명의 일 실시예에 따른 다중 서명 생성 방법을 나타낸 흐름도

도 3은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0044] 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.

[0045] 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 사

용되지 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.

[0046] 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.

[0047] 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.

[0049] 도 1은 본 발명의 일 실시예에 따른 다중 서명 생성 시스템의 구성을 나타낸 도면이다. 도 1을 참조하면, 다중 서명 생성 시스템(100)은 관리 서버(102), 서명 단말(104), 및 검증 단말(106)을 포함할 수 있다.

[0050] 관리 서버(102), 서명 단말(104), 및 검증 단말(106)은 각각 통신 네트워크(150)를 통해 상호 통신 가능하게 연결된다. 여기서, 통신 네트워크(150)는 인터넷, 하나 이상의 로컬 영역 네트워크(local area networks), 광역 네트워크(wide area networks), 셀룰러 네트워크, 모바일 네트워크, 그 밖에 다른 종류의 네트워크들, 또는 이러한 네트워크들의 조합을 포함할 수 있다.

[0051] 관리 서버(102)는 신뢰 기관(인증 기관)의 서버로서, 다중 서명을 위한 공개 파라미터를 설정할 수 있다. 관리 서버(102)는 기 설정된 보안 상수(security parameter)를 입력 받아 공개 파라미터(public parameter)(PP)를 생성할 수 있다. 관리 서버(102)는 공개 파라미터(PP)를 서명 단말(104) 및 검증 단말(106)로 각각 송신할 수 있다.

[0052] 서명 단말(104)은 공동으로 서명을 하는 각 사용자들의 단말일 수 있다. 각 서명 단말(104)은 공개 파라미터를 이용하여 자신의 비밀키(SK)와 공개키(PK)를 각각 생성할 수 있다. 또한, 각 서명 단말(104)은 공개키 리스트(LK)(즉, 각 서명 단말(104)들의 공개키들의 목록)를 이용하여 합의된 공개키(AK)를 생성할 수 있다.

[0053] 각 서명 단말(104)은 기 설정된 서명 알고리즘에 의하여 다중 서명(σ)을 생성할 수 있다. 각 서명 단말(104)은 메시지(M), i번째 서명자의 비밀키(SK_i), 공개키 리스트(LK), 및 공개 파라미터(PP)를 입력으로 하여 다중 서명(σ)을 생성할 수 있다. 예시적인 실시예에서, 각 서명 단말(104)은 2라운드 방식을 통해 다중 서명(σ)을 생성할 수 있다.

[0054] 검증 단말(106)은 서명 단말(104)에 의해 생성된 다중 서명(σ)을 검증하도록 마련될 수 있다. 검증 단말(106)은 다중 서명(σ), 메시지(M), 공개키 리스트(LK), 및 공개 파라미터(PP)를 획득하고 이를 기반으로 다중 서명(σ)을 검증할 수 있다. 검증 단말(106)은 다중 서명(σ)이 정당한 서명이면 검증 값 1을 출력하고, 다중 서명(σ)이 정당한 서명이 아닌 경우 검증 값 0을 출력할 수 있다. 여기서, 검증 단말(106)은 서명 단말(104)과는 별개의 단말일 수 있으나, 이에 한정되는 것은 아니며 복수 개의 서명 단말(104) 중 어느 하나의 단말일 수도 있다.

[0056] 도 2는 본 발명의 일 실시예에 따른 다중 서명 생성 방법을 나타낸 흐름도이다. 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.

[0057] 도 2를 참조하면, 다중 서명 생성 방법은 Setup(셋업)(S 101), Genkey(키생성)(S 103), AggKey(키합의)(S 105), Sign(서명)(S 107), 및 Verify(검증)(S 109)과 같은 5개의 알고리즘으로 구성될 수 있다.

[0058] Setup(셋업) 알고리즘: S 101

[0059] 셋업 알고리즘에서, 관리 서버(102)는 보안 상수(1^{λ})를 입력으로 하여 순환 그룹(cyclic group: $\mathbb{G}$)을 생성할

수 있다. 이때, 관리 서버(102)는 차수(또는 위수)(order)가 소수 p인 순환 그룹($\mathbb{G}$)을 생성할 수 있다. 즉, 관리 서버(102)는 보안 상수(1^{λ})를 입력으로 하여 원소의 개수가 p인 순환 그룹($\mathbb{G}$)을 생성할 수 있다. 여기서, 순환 그룹($\mathbb{G}$) = $\mathbb{Z}_p$ = {0, 1, 2, ..., p-1}으로 나타낼 수 있다.

[0060] 관리 서버(102)는 생성된 순환 그룹($\mathbb{G}$)에서 한 쌍의 제1 생성원(generator) g, h를 각각 랜덤하게 선택할 수 있다(g,h $\in \mathbb{G}$). 여기서, 한 쌍이라는 것은 g,h 간에 특별한 연관성이 있다는 의미가 아니라, 랜덤하게 선택된 생성원이 2개라는 의미이다. 한 쌍의 제1 생성원 중 g는 제1-1 생성원이라 하고, h는 제1-2 생성원이라 지칭할 수 있다.

[0061] 또한, 관리 서버(102)는 순환 그룹($\mathbb{G}$) 중 지수(exponent) α(α $\in \mathbb{Z}_p$)를 랜덤하게 선택하고, 지수 α를 이용하여 순환 그룹($\mathbb{G}$)에서 한 쌍의 제2 생성원 g_2, h_2를 설정할 수 있다. 한 쌍의 제2 생성원 중 g_2는 제2-1 생성원이라 하고, h_2는 제2-2 생성원이라 지칭할 수 있다. 여기서, 지수 α를 갖는 제1-1 생성원(g)을 제2-1 생성원(g_2)으로 설정하고, 지수 α를 갖는 제1-2 생성원(h)을 제2-2 생성원(h_2)으로 설정할 수 있다. 즉, $g_2 = g^{\alpha}$이고, $h_2 = h^{\alpha}$으로 설정할 수 있다.

[0062] 또한, 관리 서버(102)는 기 설정된 입력(예를 들어, 메시지 또는 랜덤 비트 등)에 대해 순환 그룹($\mathbb{G}$)의 지수를 출력하는 하나 이상의 해시 함수(hash function)를 설정할 수 있다. 예시적인 실시예에서, 관리 서버(102)는 제1 해시 함수(H_1), 제2 해시 함수(H_2), 및 제3 해시 함수(H_3)를 설정할 수 있다. 예를 들어, 제1 해시 함수(H_1), 제2 해시 함수(H_2), 및 제3 해시 함수(H_3)는 랜덤 비트를 입력 받아 순환 그룹($\mathbb{G}$)의 지수를 출력하도록 마련된 것일 수 있다. 여기서, $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_p$, $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_p$, $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_p$으로 나타낼 수 있다. $\{0,1\}^*$는 0과 1로 이루어지는 임의의 비트열을 의미할 수 있다. 제1 해시 함수(H_1), 제2 해시 함수(H_2), 및 제3 해시 함수(H_3)에서 "제1", "제2", "제3" 등의 용어는 서로를 구별하기 위해 사용된 것이다.

[0063] 관리 서버(102)는 순환 그룹($\mathbb{G}$), 순환 그룹의 차수(p), 한 쌍의 제1 생성원(g,h), 한 쌍의 제2 생성원(g_2, h_2), 및 해시 함수(H_1, H_2, H_3)를 포함하는 공개 파라미터(Public Parameter : PP)를 생성할 수 있다. 즉, 공개 파라미터(PP) = ($\mathbb{G}$, p, g, h, g_2, h_2, H_1, H_2, H_3)일 수 있다.

[0064] 관리 서버(102)는 공개 파라미터(PP)를 서명 단말(104) 및 검증 단말(106)로 각각 송신할 수 있다. 관리 서버(102)는 공개 파라미터(PP)를 생성한 후 이를 공개하고 별도의 비밀 정보를 관리하지 않게 된다.

[0066] Genkey(키생성) 알고리즘: S 103

[0067] 키생성 알고리즘에서, 각 서명 단말(104)은 공개 파라미터(PP)에 기반하여 자신의 비밀키(SK)와 공개키(PK)를 각각 생성할 수 있다. 구체적으로, 각 서명 단말(104)은 공개 파라미터(PP)에 포함된 순환 그룹($\mathbb{G}$) 중 2개의 지수(exponent)를 랜덤하게 선택할 수 있다. 이때, 제1 지수는 x_{i1}으로 나타내고, 제2 지수는 x_{i2}로 나타낼 수 있다(x_{i1}, $x_{i2} \in \mathbb{Z}_p$). 여기서 i는 복수 개의 서명 단말(104) 중 i번째 서명 단말(104)을 의미할 수 있다. 각 서명 단말(104)은 제1 지수 및 제2 지수를 자신의 비밀키(SK_i)로 설정할 수 있다. 즉, 비밀키(SK_i) = (x_{i1}, x_{i2})으로 설정할 수 있다. 여기서, 비밀키가 2개의 지수를 포함함에 따라 공격에 대한 안전성을 높일 수 있게 된다.

[0068] 또한, 각 서명 단말(104)은 공개 파라미터(PP) 중 한 쌍의 제1 생성원(g,h) 및 한 쌍의 제2 생성원(g_2, h_2)과 제1 지수(x_{i1}) 및 제2 지수(x_{i2})에 기반하여 공개키(PK_i)를 생성할 수 있다. 각 서명 단말(104)은 제1 공개키 원소(X_i) 및 제2 공개키 원소(Y_i)를 포함하는 공개키(PK_i)를 생성할 수 있다. 즉, 공개키(PK_i) = (X_i, Y_i)일 수 있다.

[0069] 구체적으로, 각 서명 단말(104)은 제1-1 생성원(g) 및 제2-1 생성원(g_2)이 각각 제1 지수(x_{i1}) 및 제2 지수(x_i

$_2$)를 갖도록 하여 제1 공개키 원소(X_i)를 생성하고, 제1-2 생성원(h) 및 제2-2 생성원(h_2)이 각각 제1 지수(x_{i1}) 및 제2 지수(x_{i2})를 갖도록 하여 제2 공개키 원소(Y_i)를 생성할 수 있다. 즉, 제1 공개키 원소(X_i) = $g^{xi1} g_2^{xi2}$이고, 제2 공개키 원소(Y_i) = $h^{xi1} h_2^{xi2}$ 일 수 있다.

[0071] AggKey(키합의) 알고리즘 : S 105

[0072] 키합의 알고리즘에서, 각 서명 단말(104)은 자신의 공개키(PK_i=(X_i, Y_i))를 상호 공유할 수 있다. 이를 통해, 각 서명 단말(104)은 공개키 리스트(LK)를 생성할 수 있다. 공개키 리스트(LK) = (PK_1, PK_2, ..., PK_n)(n은 서명 단말(104)의 전체 개수)으로 나타낼 수 있다.

[0073] 각 서명 단말(104)은 자신의 공개키(PK_i), 공개키 리스트(LK), 및 공개 파라미터(PP) 중 해시 함수에 기반하여 자신의 합의 공개키 지수(a_i)를 각각 산출할 수 있다. 각 서명 단말(104)은 공개키 리스트(LK) 및 자신의 공개키(PK_i)를 해시 함수에 입력하여 자신의 합의 공개키 지수(a_i)를 산출할 수 있다. 여기서, 합의 공개키 지수(a_i) = H_3(LK, PK_i)로 나타낼 수 있다. 여기서는 제3 해시 함수(H_3)를 사용하는 것으로 나타내었으나, 이에 한정되는 것은 아니며 제1 해시 함수(H_1) 또는 제2 해시 함수(H_2)를 사용할 수도 있다.

[0074] 각 서명 단말(104)은 공개키 리스트(LK) 및 자신의 합의 공개키 지수(a_i)에 기반하여 합의된 공개키(AK)를 생성할 수 있다. 여기서, 합의된 공개키(AK)는 제1 합의된 공개키 원소(AX) 및 제2 합의된 공개키 원소(AY)를 포함할 수 있다. 즉, 합의된 공개키(AK) = (AX, AY)로 나타낼 수 있다.

[0075] 각 서명 단말(104)은 공개키 리스트(LK)의 모든 제1 공개키 원소(X_i)들에 자신의 합의 공개키 지수(a_i)를 갖도록 하고 이를 곱하여 제1 합의된 공개키 원소(AX)를 산출할 수 있다. 즉, 제1 합의된 공개키 원소(AX) = $\prod_{i=1}^{n} X_i^{a_i}$으로 나타낼 수 있다.

[0076] 각 서명 단말(104)은 공개키 리스트(LK)의 모든 제2 공개키 원소(Y_i)들에 자신의 합의 공개키 지수(a_i)를 갖도록 하고 이를 곱하여 제2 합의된 공개키 원소(AY)를 산출할 수 있다. 즉, 제2 합의된 공개키 원소(AY) = $\prod_{i=1}^{n} Y_i^{a_i}$으로 나타낼 수 있다.

[0078] Sign(서명) 알고리즘 : S 107

[0079] 서명 알고리즘에서, 각 서명 단말(104)은 메시지(M), 공개 파라미터(PP), 비밀키(SK_i), 공개키 리스트(LK), 및 합의된 공개키(AK)에 기반하여 다중 서명을 생성할 수 있다.

[0080] 각 서명 단말(104)은 공개 파라미터(PP)에 포함된 순환 그룹($\mathbb{G}$) 중 2개의 지수(exponent)를 랜덤하게 선택할 수 있다. 이때, 2개의 선택된 지수 한 쌍의 랜덤 약속 지수로서, 그 중 하나는 제1 랜덤 약속 지수(r_{i1})라 하고, 다른 하나는 제2 랜덤 약속 지수(r_{i2})라 할 수 있다.

[0081] 각 서명 단말(104)은 메시지(M), 한 쌍의 제1 생성원(g,h), 한 쌍의 제2 생성원(g_2, h_2), 해시 함수, 제1 랜덤 약속 지수(r_{i1}), 및 제2 랜덤 약속 지수(r_{i2})에 기반하여 자신의 랜덤 약속 값(R_i)을 각각 산출할 수 있다. 여기서, 메시지(M)는 다중 서명의 대상이 되는 메시지일 수 있다. 각 서명 단말(104)은 하기 수학식 1에 의해 자신의 랜덤 약속 값(R_i)을 산출할 수 있다.

[0082] (수학식 1)

[0083] $$R_i = (g^{H_1(M)} h)^{ri1} (g_2{}^{H_1(M)} h_2)^{ri2}$$

[0084] 각 서명 단말(104)은 자신의 랜덤 약속 값(R_i)을 다른 서명 단말(104)로 각각 송신할 수 있다. 즉, 각 서명 단말(104)은 다른 서명 단말(104)들의 랜덤 약속 값$\{R_j\}_{1\le j\ne i\le n}$을 수신할 수 있다.

[0085] 각 서명 단말(104)은 자신의 랜덤 약속 값(R_i)과 다른 서명 단말(104)들의 랜덤 약속 값$\{R_j\}_{1\le j\ne i\le n}$에 기반하여

전체 랜덤 약속 값(AR)을 산출할 수 있다. 각 서명 단말(104)은 자신의 랜덤 약속 값(R_i)과 다른 서명 단말(104)들의 랜덤 약속 값$\{R_j\}_{1\le j\neq i\le n}$을 곱하여 전체 랜덤 약속 값(AR)을 산출할 수 있다. 즉, 전체 랜덤 약속 값(AR) = $\prod_{i=1}^{n} R_i$로 나타낼 수 있다.

[0086] 각 서명 단말(104)은 메시지(M), 공개키 리스트(LK), 합의된 공개키(AK), 전체 랜덤 약속 값(AR), 및 공개 파라미터(PP)의 해시 함수에 기반하여 메시지 관련 해시 값(c)을 산출할 수 있다.

[0087] 각 서명 단말(104)은 메시지(M), 공개키 리스트(LK), 합의된 공개키(AK), 전체 랜덤 약속 값(AR)을 공개 파라미터(PP)의 해시 함수(예를 들어, 제2 해시 함수(H_2))에 입력하여 메시지 관련 해시 값(c)을 산출할 수 있다. 메시지 관련 해시 값(c) = H_2(LK, AK, AR, M)으로 나타낼 수 있다.

[0088] 각 서명 단말(104)은 한 쌍의 랜덤 약속 지수(r_{i1}, r_{i2}), 자신의 합의 공개키 지수(a_i), 자신의 비밀키(SK_i = (x_{i1}, x_{i2})), 및 메시지 관련 해시 값(c)에 기반하여 자신의 한 쌍의 부분 서명을 생성할 수 있다. 자신의 한 쌍의 부분 서명은 제1 부분 서명(s_{i1}) 및 제2 부분 서명(s_{i2})을 포함할 수 있다.

[0089] 여기서, 각 서명 단말(104)은 제1 랜덤 약속 지수(r_{i1}), 비밀키의 제1 지수(x_{i1}), 자신의 합의 공개키 지수(a_i), 및 메시지 관련 해시 값(c)에 기반하여 제1 부분 서명(s_{i1})을 생성할 수 있다. 예를 들어, 각 서명 단말(104)은 하기의 수학식 2에 의해 제1 부분 서명(s_{i1})을 생성할 수 있다.

[0090] (수학식 2)

[0091] $$s_{i1} = r_{i1} + x_{i1}a_i c$$

[0092] 각 서명 단말(104)은 제2 랜덤 약속 지수(r_{i2}), 비밀키의 제2 지수(x_{i2}), 자신의 합의 공개키 지수(a_i), 및 메시지 관련 해시 값(c)에 기반하여 제2 부분 서명(s_{i2})을 생성할 수 있다. 예를 들어, 각 서명 단말(104)은 하기의 수학식 3에 의해 제2 부분 서명(s_{i2})을 생성할 수 있다.

[0093] (수학식 3)

[0094] $$s_{i2} = r_{i2} + x_{i2}a_i c$$

[0095] 각 서명 단말(104)은 자신의 한 쌍의 부분 서명(s_{i1}, s_{i2})을 다른 서명 단말(104)로 송신할 수 있다. 즉, 각 서명 단말(104)은 다른 서명 단말(104)들의 한 쌍의 부분 서명$\{(s_{j1}, s_{j2})\}_{1\le j\neq i\le n}$을 수신할 수 있다.

[0096] 각 서명 단말(104)은 자신의 한 쌍의 부분 서명(s_{i1}, s_{i2}) 및 다른 서명 단말(104)들의 한 쌍의 부분 서명$\{(s_{j1}, s_{j2})\}_{1\le j\neq i\le n}$에 기반하여 제1 전체 부분 서명($s_1$) 및 제2 전체 부분 서명($s_2$)을 각각 생성할 수 있다. 각 서명 단말(104)은 자신의 제1 부분 서명과 다른 서명 단말(104)들의 제1 부분 서명들을 합산하여 제1 전체 부분 서명(s_1)을 생성할 수 있다. 즉, 제1 전체 부분 서명(s_1) = $\sum_{i=1}^{n} s_{i1}$으로 나타낼 수 있다. 각 서명 단말(104)은 자신의 제2 부분 서명과 다른 서명 단말(104)들의 제2 부분 서명들을 합산하여 제2 전체 부분 서명(s_2)을 생성할 수 있다. 즉, 제2 전체 부분 서명(s_2) = $\sum_{i=1}^{n} s_{i2}$으로 나타낼 수 있다. 제1 전체 부분 서명(s_1)과 제2 전체 부분 서명(s_2)은 한 쌍의 전체 부분 서명으로 지칭될 수 있다.

[0097] 각 서명 단말(104)은 메시지 관련 해시 값(c), 제1 전체 부분 서명(s_1), 및 제2 전체 부분 서명(s_2)에 기반하여 다중 서명(σ)을 생성할 수 있다. 예시적인 실시예에서, 다중 서명(σ) = (c, s_1, s_2)으로 나타낼 수 있다.

[0099] Verify(검증) 알고리즘 : S 109

[0100] 검증 알고리즘에서, 검증 단말(106)은 다중 서명(σ), 메시지(M), 및 공개키 리스트(LK)를 입력 받아 AggKey(키 합의) 알고리즘 수행하여 합의된 공개키(AK=(AX, AY))를 획득할 수 있다. 검증 단말(106)은 다중 서명(σ), 메시지(M), 한 쌍의 제1 생성원(g,h), 한 쌍의 제2 생성원(g_2, h_2), 해시 함수, 및 합의된 공개키(AK=(AX, AY))에 기반하여 하기의 수학식 4에 나타낸 바와 같이 전체 랜덤 약속 값(AR)을 산출할 수 있다.

[0101] (수학식 4)

[0102] $$AR = (g^{H_1(M)}h)^{s_1}(g_2{}^{H_1(M)}h_2)^{s_2}/(AX^{H_1(M)}AY)^c$$

[0103] 검증 단말(106)은 메시지(M), 합의된 공개키(AK), 전체 랜덤 약속 값(AR), 및 공개키 리스트(LK)에 기반하여 메시지 관련 해시 값(c) = H_2(LK, AK, AR, M)을 산출할 수 있다. 검증 단말(106)은 산출한 메시지 관련 해시 값(c)이 다중 서명(σ)에 포함된 메시지 관련 해시 값(c)과 일치하는지 여부를 확인하여 다중 서명(σ)을 검증할 수 있다.

[0105] 도 3은 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.

[0106] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 관리 서버(102)일 수 있다. 또한, 컴퓨팅 장치(12)는 서명 단말(104)일 수 있다. 또한, 컴퓨팅 장치(12)는 검증 단말(106)일 수 있다.

[0107] 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.

[0108] 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.

[0109] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0110] 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.

[0112] 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

[0114] 100 : 다중 서명 시스템

102 : 관리 서버

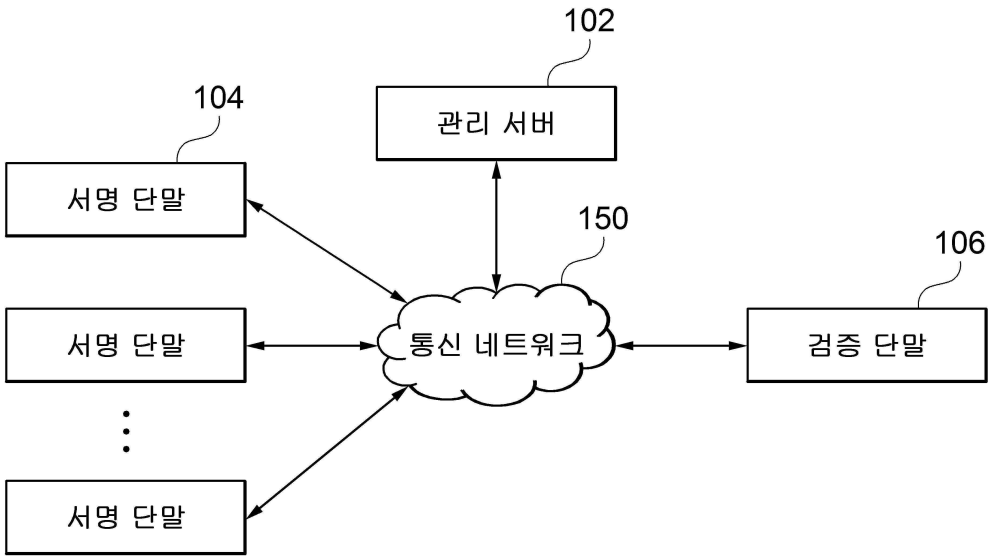
104 : 서명 단말

106 : 검증 단말

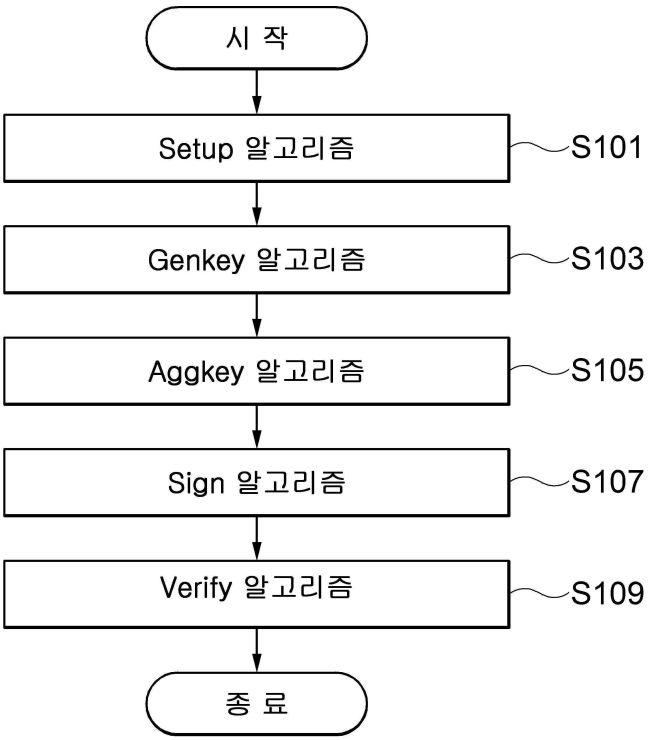
도면

도면1

100

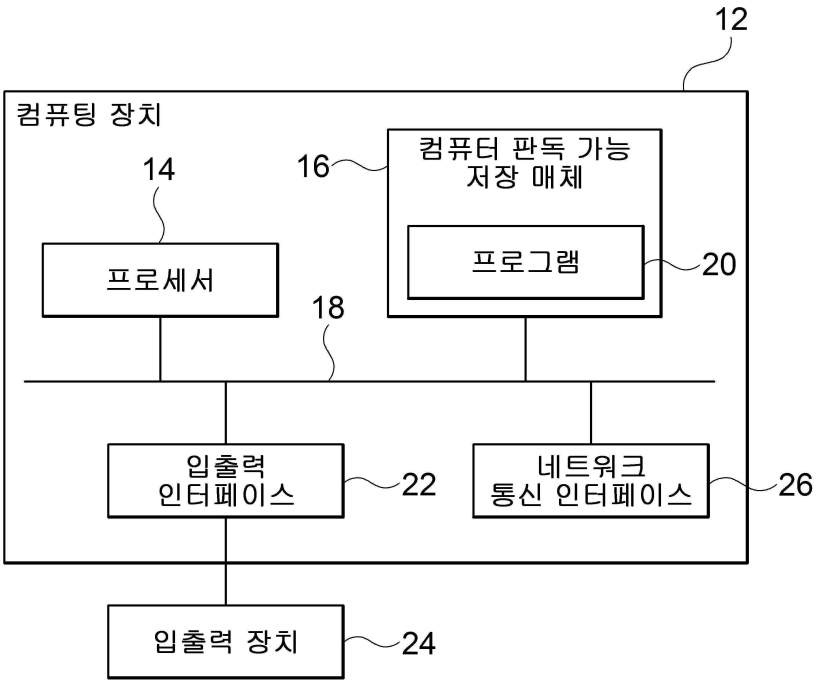


도면2



도면3

10



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 14

【변경전】

청구항 13에 있어서,

상기 수학식에 의해 자신의 랜덤 약속 값(R_i)을 산출하는, 다중 서명 생성 방법.

(수학식)

$$R_i = (g^{H_1(M)}h)^{ri1}(g_2{}^{H_1(M)}h_2)^{ri2}$$

【변경후】

청구항 13에 있어서,

하기의 수학식에 의해 자신의 랜덤 약속 값(R_i)을 산출하는, 다중 서명 생성 방법.

(수학식)

$$R_i = (g^{H_1(M)}h)^{ri1}(g_2{}^{H_1(M)}h_2)^{ri2}$$