(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) Int. Cl.[6]
G06F 17/60

(45) 공고일자 2000년02월15일
(11) 등록번호 10-0244852
(24) 등록일자 1999년11월24일

(21) 출원번호 10-1997-0035930
(22) 출원일자 1997년07월29일
(65) 공개번호 특1999-0012517
(43) 공개일자 1999년02월25일

(73) 특허권자 엘지전자주식회사 구자홍
서울특별시 영등포구 여의도동 20번지송주석
(72) 발명자 서울특별시 강남구 압구정동 현대아파트 73-703호
송주석
서울특별시 강남구 압구정동 현대아파트 73-703호
양대헌
인천광역시 남동구 간석 4동 579-1
(74) 대리인 김영호

심사관 : 이은철

(54) 디지탈 서명 생성방법 및 장치

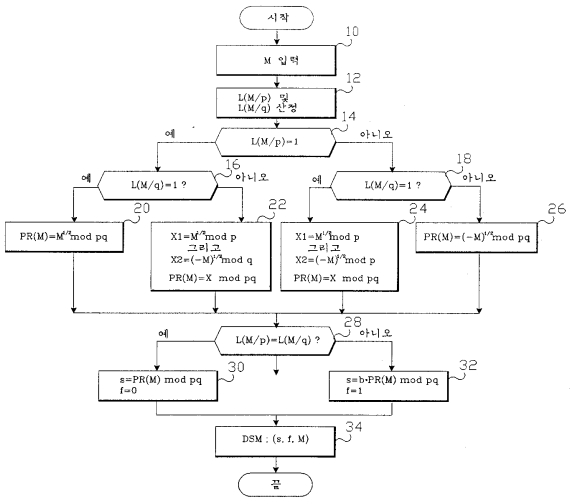
요약

본 발명의 목적은 디지탈 서명의 생성과정의 불확정성이 제거된 디지탈 서명 생성방법 및 장치에 관한 것이다.

본 발명에서는 브름 수인 제1 및 제2 키원소(p, q)를 가지는 비밀키를 마련하고, 디지탈 문서(M)의 제곱근(R(M))과 디지탈 문서(M)의 부의 값에 대한 제곱근(R(-M))을 산출한다. 제1 키원소(p)와 제2 키원소(q)의 곱에 해당하는 크기의 유한체와 디지탈 문서(M)의 제곱근과의 포함관계에 따라 디지탈 문서(M)의 제곱근(R(M))과 디지탈 문서(M)의 부의 값에 대한 제곱근 (R(-M) 중 어느 하나가 연산됨으로써 서명코드(S)가 산출된다.

이에 따라, 본 발명에서는 디지탈 서명을 효율적으로 생성할 수 있고 아울러 디지탈 서명이 소인수 분해와 같은 수준의 안정성을 가지게 한다.

대표도



명세서

도면의 간단한 설명

제1도는 본 발명의 실시예에 따른 디지탈서명 생성방법을 설명하는 흐름도.

제2도는 본 발명의 실시예에 따른 디지탈 서명 확인방법을 설명하는 흐름도.

제3도는 본 발명의 실시예에 따른 디지탈서명 생성장치의 블럭도.

제4도는 본 발명의 실시예에 따른 디지탈 서명 생성방법 및 장치가 적용된 통신망 시스템을 계략적으로 도시하는 도면.

* 도면의 주요부분에 대한 부호의 설명

60, 62 : 르잔드르심볼발생기　　64내지70 : 래치

72, 74, 96 : 멀티플렉서　　76, 78 : 제곱근모듈로모듈

80, 98 : 어드레스어블디코더　　82 : 나머지정리모듈

84 : 비고기　　86 : 모듈로승산기

88 : 인버터　　90, 92 : AND 게이트

100 : 레지스터　　110 : 통신망

120, 130, 140 : 데이타스테이션　　122, 132, 142 : 데이타종단장치

126, 134, 144 : 데이타회선정합장치　　124 : 디지탈서명생성장치

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 공개키 암호화 방식에 관한 것으로, 특히 디지탈 문서의 무결성과 인증을 제공하기 위한 디지탈 서명을 생성하는 디지탈 서명 생성방법 및 장치에 관한 것이다. 그리고 본 발명은 디지탈 서명을 그 생성과정에 따라 디코딩하는 디지탈 서명 확인방법에 관한 것이다.

최근 통신망과 컴퓨터 기술의 급속한 발달로 디지탈 문서에 대한 무결성의 보장과 인증을 제공하는 디지탈 서명 방법이 요구되게 되었다. 이 디지탈 서명은 공개키 암호화 방식에서만 사용될 수 있는 것으로, 디지탈 문서에 대한 비밀키를 알고 있는 서명자만이 할 수 있다. 또한, 디지탈 서명은 서명자의 공개키를 의해서 확인된다. 그러므로, 디지탈 서명의 생성과 그의 확인을 위해서는 비밀키와 공개키가 필요하다.

이러한 디지탈 서명을 생성하는 방법에는 RSA(Rivest Shamir Adleman) 공개키 암호화 시스템을 이용한 디지탈 서명 생성방법(이하, "RSA디지탈 서명 생성방법"이라 함), 엘가말(Elgamal)의 디지탈 서명 생성방법 및 디지탈 서명 생성방법 등이 알려져 있다. 하지만, 이들 서명 생성방법들은 서명이 생성되기까지 많은 양의 연산을 수행하여야 함은 물론이거니와 생성된 서명의 확인시에도 많은 양의 연산이 수행되도록 하므로 효율성이 떨어진다. 이들 디지탈 서명 생성방법들의 비효율성을 개선하기 위한 방안으로서 로빈(Robin) 방식의 디지탈 서명 생성방법이 제안되었다. 이 로빈방식의 디지탈 서명 생성방법은 서명의 확인에 있어서는 상기의 서명 생성방법들 보다 매우 뛰어난 효율을 가지긴 하나 서명의 생성과정이 불확정적이라는 단점을 안고 있다. 이로 인하여, 로빈방식의 디지탈 서명 생성방법은 상기의 서명 생성방법들과 마찬가지로 현제 실용화되고 있는 집적회로카드 등의 형태로 구현되기 곤란하였다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명의 목적은 디지탈 서명의 생성과정의 불확정성이 제거된 디지탈 서명 생성방법 및 장치를 제공함에 있다.

본 발명의 다른 목적은 디지탈 서명이 효율적으로 수행되도록 할 수있는 디지탈 서명 생성방법 및 장치를 제공함에 있다.

본 발명의 또 다른 목적은 디지탈 서명이 소인수 분해와 같은 수준의 안정성을 가지도록 하는 디지탈 서명 생성방법 및 장치를 제공함에 있다.

본 발명의 또 다른 목적은 공개키의 길이를 짧게 할 수 있는 디지탈 서명 생성방법 멎 장치를 제공함에 있다.

발명의 구성 및 작용

상기 목적을 달성하기 위하여, 본 발명에 따른 디지탈 서명 생성방법은 임의의 브름 수의 크기를 가지는 유한체에서 연산을 수행하여 디지탈 문서(M)에 대한 서명코드를 생성한다.

본 발명에 따른 디지탈 서명 생성방법은 승산값이 임의의 브름 수가 되는 제1 및 제2 키원소(p, q)를 가지는 비밀키를 마련하는 단계와, 디지탈문서(M)의 제곱근(R(M))을 산출하는 단계와, 디지탈 문서(M)의 부의 값에 대한 제곱근(R(-M))을 산출하는 단계와, 제1 키원소(p)와 제2 키원소(q)의 곱에 해당하는 크기의 유한체와 디지탈 문서(M)의 제곱근과의 포함관계를 판단하는 단계와, 유한체와 디지탈 문서(M)의 제곱근(PR(M))과의 포함관계에 따라 디지탈 문서(M)의 제곱근(R(M))과 디지탈 문서(M)의 부의 값에 대한 제곱근(R(-M) 중 어느 하나를 이용하여 서명코드(S)를 산출하는 단계를 포함한다.

본 발명에 따른 디지탈 서명 생성방법은 승산값이 임의의 브름 수가 되는 제1 및 제2 키원소(p, q)를 가지는 비밀키를 마련하는 단계와, 디지탈문서(M)의 제곱근(R(M))이 제1 키원소(p)의 크기를 가지는 제1 유한체(Zp)와 제2 키원소의 크기를 가지는 제2 유한체(Zq)와의 포함관계를 판단하는 단계와, 유한체들(Zp, Zq)과 디지탈 문서(M)의 제곱근(R(M))과의 포함관계에 따라 상이한 연산식을 이용하여 디지탈 문서(M)의 가상제곱근(PR(M))을 산출하는 단계와, 가상제곱근(PR(M))을 이용하여 서명코드(S)를 산출하는 단계를 포

함한다.

본 발명에 따른 디지탈 서명 생성방법은 승산값이 임의의 브름 수가 되는 제1 및 제2 키원소(p, q)와 임의의 정수인 제3 키원소(b)를 가지는 비밀키를 마련하는 단계와, 디지탈 문서(M)의 제곱근(R(M))이 제1 키원소(p)의 크기를 가지는 제1 유한체(Zp)와 제2 키원소의 크기를 가지는 제2 유한체(Zq)와의 포함관계를 판단하는 단계와, 유한체들(Zp, Zq)과 디지탈 문서(M)의 제곱근(R(M))과의 포함관계에 따라 상이한 연산식을 이용하여 디지탈문서(M)의 가상제곱근(PR(M))을 산출하는 단계와, 유한체들(Zp, Zq)과 디지탈 문서(M)의 제곱근(R(M))과의 포함관계에 따라 제3 키원소(b)와 가상제곱근(PR(M))와의 연산을 선택적으로 수행하여 서명코드(S)를 산출하는 단계를 포함한다.

본 발명에 따른 디지탈 서명 생성장치는 임의의 브름 수의 크기를 가지는 유한체에서 연산을 수행하여 디지탈 문서(M)에 대한 서명코드를 생성한다.

본 발명에 따른 디지탈 서명 생성장치는 승산값이 임의의 브름 수가 되는 제1 및 제2 키원소(p, q)를 가지는 비밀키와 디지탈 문서(M)를 입력하는 입력수단과, 디지탈 문서(M)의 제곱근(R(M))을 산출하는 제1 연산수단과, 디지탈 문서(M)의 부의 값에 대한 제곱근(R(-M))을 산출하는 제2 연산수단과, 제1 키원소(p)와 제2 키원소(q)의 곱에 해당하는 크기의 유한체와 디지탈 문서(M)의 제곱근(R(M))과의 포함관계를 검출하는 포함관계검출수단과, 유한체와 디지탈 문서(M)의 제곱근(PR(M))과의 포함관계에 따라 디지탈문서(M)의 제곱근(R(M))과 디지탈 문서(M)의 부의 값에 대한 제곱근(R(-M)중 어느 하나를 이용하여 서명코드(S)를 산출하는 제3 연산수단을 구비한다.

본 발명에 따른 디지탈 서명 생성장치는 승산값이 임의의 브름 수가 되는 제1 및 제2 키원소(p, q)를 가지는 비밀키와 디지탈문서(M)를 입력하는 입력수단과, 디지탈 문서(M)의 제곱근(R(M))이 제1 키원소(p)의 크기를 가지는 제1 유한체(Zp)와 제2 키원소의 크기를 가지는 제2 유한제(Zq)와의 포함관계를 검출하는 포함관계검출수단과, 유한체들(Zp, Zq)과 디지탈 문서(M)의 제곱근(R(M))과의 포함관계에 따라 상이한 연산식을 이용하여 디지탈 문서(M)의 가상제곱근(PR(M))을 산출하는 제1 연산수단과, 가상제곱근(PR(M))을 이용하여 서명코드(S)를 산출하는 제2 연산수단을 구비한다.

본 발명에 따른 디지탈 서명 생성장치는 승산값이 임의의 브름 수가 되는 제1 및 제2 키원소(p, q)와 임의의 정수인 제3 키원소(b)를 가지는 비밀키와 디지탈 문서(M)를 입력하는 단계와, 디지탈 문서(M)의 제곱근(R(M))이 제1 키원소(p)의 크기를 가지는 제1 유한체(Zp)와 제2 키원소의 크기를 가지는 제2 유한체(Zq)와의 포함관계를 검출하는 포함관계검출수단과, 유한체들(Zp, Zq)과 디지탈 문서(M)의 제곱근(R(M))과의 포함관계에 따라 상이한 연산식을 이용하여 디지탈 문서(M)의 가상제곱근(PR(M))을 산출하는 제1 연산수단과, 유한체들(Zp, Zq)과 디지탈 문서(M)의 제곱근(R(M))과의 포함관계에 따라 제3 키원소(b)와 가상제곱근(PR(M))와의 연산을 선택적으로 수행하여 서명코드(S)를 산출하는제2 연산수단을 구비한다.

본 발명에 따른 디지탈 서명 확인방법은 임의의 브롬 수인 키원소(pq)를 가지는 공개키를 마련하는 단계와, 브름 수(pq)의 크기를 가지는 유한체에서의 연산에 의해 생성되어진 디지탈 문서(M)에 대한 서명코드(S)의 4제곱값을 산출하는 단계와, 디지탈 문서(M)의 가상제곱값(PS(M))을 수식 $PS(M) = M^2 \bmod pq$ 에 의해 산출하는 단계와, 서명코드(S)의 4제곱값과 가상제곱값(PS(M))을 비교하는 단계를 포함한다.

본 발명에 따른 디지탈 서명 확인방법은 승산값이 임의의 브름 수가 되는 제1 및 제2 키원소(p,q)와 임의의 정수인 제3 키원소(b)를 가지는 비밀키중 제1 및 제2 키원소(p,q)의 곱값의 크기를 가지는 유한체에서의 제곱근연산함과 아울러 상기 그 제곱근을 제3 키원소(b)와 선택적으로 연산함에 의해 생성되어진 서명코드(S)와 디지탈 문서(M)를 디코딩플래그(f)와 함께 수신하는 단계와, 제1 및 제2 키원소(p,q)의 곱값의 제4 키원소(pq)와 제3 키원소(b)의 4제곱값의 제5 키원소(B)를 마련하는 단계와, 서명코드(S)의 4제곱값을 산출하는 단계와, 제4 키원소에 의한 모듈로연산을 포함하는 디지탈 문서(M)의 제곱연산에 디코딩플래 그에 따라 제5 키원소(B)를 선택적으로 적용하여 디지탈 문서(M)의 가상제곱값(PS(M))을 산출하는 단계와, 서명코드(S)의 4제곱값과 가상제곱값(PS(M))을 비교하는 단계를 포함한다.

상기 목적들 외에 본 발명의 다른 목적 및 잇점들은 첨부한 도면을 참조한 실시예에 대한 상세한 설명을 통하여 명백하게 드러나게 될 것이다.

이하, 본 발명의 실시예를 첨부한 도1 및 도2 를 참조하여 상세히 설명하기로 한다.

본 발명의 실시예를 설명하기 전에 먼저 본 발명의 디지탈 서명 생성방법에서 사용될 비밀키와 본 발명에 의해 생성되어진 디지탈 서명의 확인에 사용될 공개키에 관하여 살펴보기로 한다.

비밀키는 제1 내지 제3 키원소(p, q, b)로 구성된다. 이들 키원소들(p, q, b) 중 제1 및 제2 키원소(p, q)는 서로 승산한 값이 브름 수(Blum Number)가 되도록 4n+3 의 형태를 가지는 임의의 소수로 설정된다. 여기서, n 은 정수이다. 나머지 제3 키원소(b)는 임의의 정수로 랜덤하게 설정된다.

또한, 공개키는 제1 및 제2 키원소(pq, B)로 구성된다. 제1 키원소(pq)는 두 소수(p, q)의 곱값(즉, pq)으로서 브름 수이다. 제2 키원소(B)는 비밀키의 제3 키원소(b)를 4제곱한 다음 공개키의 제1 키원소(pq)에 의해 모듈러 연산됨에 의해 산출되는 정수로 설정된다.

도 1 은 퍼스널 컴퓨터(Personal Computer)와 같은 통상의 연산처리장치에 의해 수행될 수 있는 본 발명에 따른 디지탈 서명 생성방법을 상세하게 설명한다. 도1의 제10 단계에서 디지탈 문서(M)이 연산처리장치에 입력되면, 그 연산처리장치는 디지탈 문서(M)에 대한 제1 및 제2 르잔드르심볼(L(M/p), L(M/q))를 산출한다 (제12 단계). 이 제1 르잔드르심볼(L(M/p))은 디지탈 문서(M)의 논리값이 비밀키의 제1 키원소(p)의 크기를 가지는 제1 숫자링(Zp^*)내의 임의의 한 원소의 제곱한 값과 동일한가의 여부를 나타낸다. 디지탈 문서(M)의 논리값이 제1 숫자링(Zp^*)내의 임의의 한원소의 제곱한 값과 동일한 경우에 "1"의 논리값을 가진다. 비슷하게, 제2르잔드르심볼(L(M/q))은 디지탈 문서(M)의 논리값이 비밀키의 제2 키원소(p)의 크기를 가지는 제2 숫자링(Zq^*)내의 임의의 한 원소의 제곱한 값과 동일한가의 여부를 나타낸다. 디지탈 문서(M)의 논리값이 제2 숫자링(Zq^*)내의 임의의 한 원소의 제곱한 값과 동일한 경우에 &

quot;1"의 논리값을 가진다.

이어서, 연산처리장치는 제14 단계 내지 제16 단계에서 제1 및 제2 르잔드르심볼(L(M/p), L(M/q))들의 논리값을 검사하여 그 검사결과에 따라 가상제곱근(PR(M)) 연산식을 결정한다. 이를 상세히 하면, 연산처리장치는 제1 및 제2 르잔드르심볼(L(M/p), L(M/q))의 논리값에 따라 디지탈 문서가 상기 두개의 숫자링들(Zp^*, Zq^*) 중 어느 숫자링에서 연산 가능한가를 판단하고 그 판단결과에 의해 가상제곱근(PR(M)) 연산식을 결정하게 된다.

제14 및 제16 단계에서 제1 및 제2 르잔드르심볼(L(M/p), L(M/q))이 모두 "1"의 논리값을 가지는 경우, 즉 디지탈문서(M)가 제1 및 제2 숫자링(Zp^*, Zq^*) 모두에서 연산될 수 있는 경우에 연산처리장치는 수식1 에서와 같이 디지탈 문서(M)의 제곱근을 산출하고 그 산출된 제곱근을 브름수, 즉 비밀키의 제1 및 제2 키원소(p,q)의 승산값으로 모듈러 연산함으로써 가상제곱근(PR(M))을 산출한다 (제20 단계).

[수식1]

$$PR(M) = M^{1/2} \bmod pq$$

제14 및 제16 단계에서 제1 르잔드르심볼(L(M/p))이 "1"이고 제2 르잔드르심볼(L(M/q))이 "0"인 경우, 즉 디지탈문서(M)가 제1 숫자링(Zp^*)에서만 연산될 수 있는 경우에 연산처리장치는 수식2 내지 수식4 에 따라 가상제곱근(PR(M))을 산출한다 (제22 단계).

[수식2]

$$x1 = M^{1/2} \bmod p$$

[수식3]

$$x2 = (-M)^{1/2} \bmod q$$

[수식4]

$$PR(M) = x \bmod pq$$

$$=x1 + p(x2 - x1^2) \cdot p^{q^{-1}} \bmod pq$$

$$=Mp^{1/2} + p((-Mq)^{1/2} - Mp^{1/2}) \cdot p^{q^{-1}} \bmod pq$$

수식4 에서 pq^{-1} 은 비밀키의 제1 키원소(p)와 승산하여 "1"을 산출시킬 수 있는 제2 숫자링(Zq^*)에 포함되어진 임의의 원소이다.

제14 및 제18 단계에서 제1 르잔드르심볼(L(M/p))이 "0"이고 제2 르잔드르심볼(L(M/q))이 "1"인 경우, 즉 디지탈문서(M)가 제2 숫자링(Zp^*)에서만 연산될 수 있는 경우에 연산처리장치는 수식5 내지 수식7 에 따라 가상제곱근(PR(M))을 산출한다 (제24 단계).

[수식5]

$$x1 = M^{1/2} \bmod q$$

[수식6]

$$x2 = (-M)^{1/2} \bmod p$$

[수식7]

$$PR(M) = x \bmod pq$$

$$=x1 + p(x2 - x1) \cdot p^{q^{-1}} \bmod pq$$

$$=Mp^{1/2} + q((-Mq)^{1/2} \_ Mp^{1/2}) \cdot q^{q^{-1}} \bmod pq$$

수식4 에서 $q^{q^{-1}}$ 은 비밀키의 제2 키원소(q)와 승산하여 "1"을 산출시킬 수있는 제1 숫자링(Zp^*)에 포함되어진 임의의 원소이다.

제14 및 제18 단계에서 제1 및 제2 르잔드르심볼(L(M/p), L(M/q))이 모두 "0"의 논리값을 가지는 경우, 즉 디지탈문서(M)가 제1 및 제2 숫자링(Zp^*, Zq^*) 모두에서 연산될 수 없는 경우에 연산처리장치는 수식8 에서와 같이 디지탈 문서(M)의 대수 · 제곱근을 산출하고 그 산출된 결과를 브름수, 즉 비밀키의 제1 및 제2 키원소(p, q)의 승산값으로 모듈러 연산함으로써 가상제곱근(PR(M))을 산출한다 (제26 단계).

[수식8]

$$PR(M) = -M^{1/2} \bmod pq$$

제20 내지 제26 단계들 중 어느 한 단계를 수행한 후, 연산처리장치는 제1 및 제2 르잔드르심볼(L(M/p), L(M/q))이 동일한 논리값을 가지는가를 판단한다 (제28 단계). 즉, 연산처리장치는 디지탈 문서(M)이 제1 숫자링(Zp^*)에 포함된 임의의 원소의 제곱값임과 동시에 제2 숫자링(Zq^*)에 포함된 임의의 원소의 제곱값인가를 판단한다.

제28 단계에서 두 르잔드르심볼(L(M/p), L(M/q))이 동일한 것으로 판단된 경우, 즉 디지탈 문서(M)이 제1 숫자링(Zp^*)에 포함된 임의의 원소의 제곱값임과 동시에 제2 숫자링(Zq^*)에 포함된 임의의 원소의 제곱값이거나 또는 디지탈 문서(M)의 논리값이 제1 및 제2 숫자링(Zp^*, Zq^*)에 포함된 어느원소의 제곱값과도 같지 않은 경우에, 연산처리장치는 수식9 에서와 같이 가상제곱근(PR(M))을 비밀키의 제1 및 제2 키원소들간의 승산값에 의해 모듈러 연산함으로써 서명코드(S)를 생성한다 (제30 단계).

[수식9]

$$S = PR(M) \bmod pq$$

이와 더불어, 연산처리장치는 서명코드(S)의 디코딩방법을 지시하는 디코딩플래그(f)를 발생한다. 이 때, 디코딩플래그(f)는 비밀키의 제3 키원소(b)가 서명코드의 생성에 사용되지 않았음을 나타내는 "0"의 논리값으로 세트된다.

이와는 달리, 두 르잔드르심볼(L(M/p), L(M/q))의 논리값이 동일하지않은 경우, 즉 디지탈 문서(M)의 논리값이 제1 숫자링(Zp^*)에 포함된 임의의 원소의 제곱값과 제2 숫자링(Zq^*)에 포함된 임의의 원소의 제곱값 중 어느하나와 같은 경우에 연산처리장치는 수식10 에서와 같이 가상제곱근(PR(M))과 비밀키의 제3 키원소(b)와의 승산값을 비밀키의 제1 및 제2 키원소들(p, q)간의 승산값(pq)에 의해 모듈러 연산함으로써 서명코드(S)를 생성한다(제32 단계).

[수식10]

$$S = b \cdot PR(M) \bmod pq$$

더불어, 연산처리장치는 디코딩플래그(f)를 비밀키의 제3 키원소(b)가 서명코드의 생성에 사용되었음을 나타내는 "1"의 논리값으로 세트한다.

제30 또는 제32 단계의 수행 후, 연산처리장치는 디지탈 문서(M)에 서명코드(S) 및 디코딩플래그(f)를 부가하여 디지탈 서명 메세지(DSM)를 형성하고 그 디지탈 서명 메세지(DSM)를 통신채널을 통해 송출하게 된다 (제34 단계).

도 2 는 퍼스널 컴퓨터(Personal Computer)와 같은 통상의 연산처리장치에 의해 수행될 수 있는 본 발명에 따른 디지탈 서명 확인방법을 상세하게 설명한다. 도2 의 제40 단계에서 연산처리장치는 통신채널로부터 디지탈 문서(M), 서명코드(S) 및 디코딩플래그(f)을 포함하는 디지탈 서명 메세지(DSM)을 수신한다. 또한, 연산처리장치는 디지탈 서명 메세지(DSM)에 포함된 디코딩플래그(f)의 논리값을 검사하여 서명코드의 생성에 서명자의 비밀키의 제3 키원소(b)의 사용여부를 판단하여 서명코드의 확인방법을 결정한다 (제42 단계).

제42 단계에서 디코딩플래그(f)의 논리값이 "0"인 경우, 즉 서명코드(S)의 생성시 서명자 비밀키의 제3 키원소(b)가 사용되지 않은 경우에, 연산처리장치는 서명코드(S)와 디지탈 문서(M)가 수식11 을 만족시키는가를 검사하여 디지탈 서명 메세지(DSM)에 포함된 서명코드(S)를 확인한다 (제44

[수식11]

$$S^4 = M^2 \bmod pq$$

단계). 즉, 서명코드(S)가 4제곱된 값과 디지탈 문서(M)이 제곱연산된 다음 서명자 공개키의 제1 키원소(pq)에 의해 모듈러연산된 값과 동일한가에 따라연산처리장치는 서명코드(S)이 서명자의 것인지를 판단한다 (제44 단계).

이와는 달리, 디코딩플래그(f)의 논리값이 "1"인 경우, 즉 서명코드(S)의 생성시 서명자 비밀키의 제3 키원소(b)가 사용된 경우에, 연산처리장치는 서명코드(S)와 디지탈 문서(M)이 수식12 를 만족시키는가를 검사하여 디지탈 서명 메세지(DSM)에 포함된 서명코드(S)를 확인한다 (제46 단계).

즉, [수식12]

$$S^4 = B \cdot M^2 \bmod pq$$

서명코드(S)의 4제곱값이 디지탈 문서(M)의 제곱값과 서명자 공개키의 제2키원소(B)와의 승산값이 서명자 공개키의 제1 키원소(pq)에 의해 모듈러 연산된 값과 동일한가를 따라 연산처리장치는 서명코드(S)이 서명자의 것인지를 판단한다.

디지탈 서명 메세지(DSM)에 포함된 서명코드(S)와 디지탈 문서(M)이 수식11 또는 수식12 를 만족시키는 경우에 연산처리장치는 서명코드(S)가 서명자의 것임을 확인자에게 통보하게 된다 (제48 단계). 반면, 디지탈 서명 메세지(DSM)에 포함된 서명코드(S)와 디지탈 문서(M)가 수식11 및 수식12 모두를 만족시키지 못하는 경우에 연산처리장치는 서명코드(S)가 서명자가 행한 것이 아님을 확인자에게 통보한다 (제50 단계).

도 3 은 본 발명의 실시예에 따른 디지탈 서명 생성장치의 블럭도이다. 도3 에 있어서, 디지탈 서명 생성장치는 디지탈 문서(M)를 공통적으로 입력하는 제1 및 제2 르잔드르심볼발생기(60, 62)을 구비한다. 제1 르잔드르심볼발생기(60)에 서명자 비밀키의 제1 키원소(p)가 그리고 제2 르잔드르심볼발생기(62)에는 서명자 비밀키의 제2 키원소(q)가 추가로 입력된다. 제1 르잔드르심볼발생기(60)는 디지탈 문서(M)의 논리

값을 비밀키의 제1 키원소(p)의 크기를 가지는 제1 숫자링(Zp^*)내의 원소들의 제곱한 값들과 순차적으로 비교함으로써 제1 르잔드르심볼(L(M/p))를 발생한다 (제12 단계). 이 제1 르잔드르심볼(L(M/p))은 디지탈 문서(M)의 논리값이 제1 숫자링(Zp^*)의 어느 한 원소의 제곱값과 동일한 경우에 "1"의 논리값을 가지게 된다. 비슷하게, 제2 르잔드르심볼발생기(62)도 디지탈 문서(M)의 논리값을 비밀키의 제2 키원소(q)의 크기를 가지는 제2 숫자링(Zq^*)내의 원소들의 제곱한값들과 순차적으로 비교함으로써 제2 르잔드르심볼(L(M/q))를 발생한다. 이 제2 르잔드르심볼(L(M/q))은 디지탈 문서(M)의 논리값이 제2 숫자링(Zq^*)의 어느 한 원소의 제곱값과 동일한 경우에 "1"의 논리값을 가지게 된다.

디지탈 서명 생성장치는 디지탈 문서(M)와 비밀키의 키원소를 래치하기 위한 제1 내지 제4 래치(64 내지 70)를 구비한다. 제1 래치(64)는 디지탈 문서(M)와 비밀키의 제1 키원소(p)를 제1 멀티플렉서(72)쪽으로 전달하고, 제2 래치(66)은 반전된 디지탈 문서(-M)와 비밀키의 제1 키원소(p)를 제1 멀티플렉서(72)쪽으로 래치한다. 마찬가지로, 제3 래치(68)는 디지탈문서(M)와 비밀키의 제2 키원소(q)를 제2 멀티플렉서(74)쪽으로 전달하고, 제4 래치(70)은 반전된 디지탈 문서(-M)와 비밀키의 제2 키원소(q)를 제2 멀티플렉서(74)쪽으로 래치한다. 이들 래치들(64 내지 70)은 제1 및 제2 르잔드르심볼발생기들 (60, 62)로부터의 제 1 및 제 2 르잔드르심볼(L(M/p), L(M/q)를 입력하는 어드레스어블 디코더(80)의 제어를 받는다. 이 어드레스어블 디코더(80)는 제1 및 제2 르잔드르심볼(L(M/p), L(M/q)들의 논리값에 따라 제1 내지 제4 래치(64 내지 70) 중 하나 또는 두개의 래치들이 래치동작을 행하도록 한다. 이를 상세히 하면, 제1 및 제2 르잔드르심볼(L(M/p), L(M/q)이 모두 "1"의 논리값을 가지는 경우에 제1 래치(64)만이 래치동작을 수행함으로써 제1 모듈러 제곱근 모듈(76)에만 디지탈 문서(M)와 비밀키의 제1 키원소(p)가 공급되게 된다. 이 때, 나머지정리모듈(82)에는 수식2 과 같이 비밀키의 제1 키원소(p)에 의해 모듈러연산된 디지탈 문서(M)의 제곱근이 제1 모듈러 제곱근 모듈(76)로부터 공급된다. 반대로, 제1및 제2 르잔드르심볼(L(M/p), L(M/q)이 모두 "0"의 논리값을 가지는 경우에는 제4 래치(70)만이 래치동작을 수행함으로써 제2 모듈러 제곱근 모듈(78)에만 반전된 디지탈 문서(-M)와 비밀키의 제2 키원소(q)가 공급되게 된다. 이 경우, 제2 모듈러 제곱근 모듈(78)은 나머지정리모듈(82)에 수식3 과 같이 비밀키의 제2 키원소(p)에 의해 모듈러연산된 반전된 디지탈 문서(M)의 제곱근이 공급된다. 이와는 달리, 제1 및 제2 르잔드르심볼(L(M/p), L(M/q)의 논리값이 "10"인 경우에 제1 및 제4 래치(64, 70)가 래치동작을 수행함으로써 제1 및 제2 모듈러 제곱근 모듈(76, 78) 각각에 디지탈 문서(M)와 비밀키의 제1 키원소(p)와 그리고 반전된 디지탈 문서(-M)와 비밀키의 제2 키원소(q)가 각각 공급되게 된다. 이 때, 제1 모듈러 제곱근 모듈(76)은 수식2와 같이 연산되어진 제곱근을 그리고 제2 모듈러 제곱근 모듈(78)은 수식3과 같이 연산되어진 제곱근을 나머지정리모듈(82)에 공급한다. 반대로, 제1 및 제2 르잔드르심볼(L(M/p), L(M/q)의 논리값이 "1"인 경우에 제2 및 제3 래치(66, 68)가 래치동작을 수행함으로써 제1 및 제2 모듈러 제곱근 모듈(76, 78) 각각에 반전된 디지탈 문서(-M)와 비밀키의 제1 키원소(p)와 그리고 디지탈 문서(M)와 비밀키의 제2 키원소(q)가 각각 공급되게 된다. 이 경우에 제1 모듈러 제곱근 모듈(76)은 수식6 와 같이 연산되어진 제곱근을 그리고 제2 모듈러 제곱근 모듈(78)은 수식5 과 같이 연산되어진 제곱근을 나머지정리모듈(82)에 공급하게 된다. 그러면, 나머지정리모듈(82)는 제1 및 제2 모듈러 제곱근 모듈(76, 78) 중 어느 한쪽에서만 디지탈 문서(M)의 제곱근이 입력될 경우에는 그 입력된 제곱근을 가상제곱근(PR(M))으로써 제1 출력단자(82A)를 통해 송출한다. 이와는 달리, 제1 및 제2 모듈러 제곱근 모듈들(76, 78) 각각으로부터 두개의 제곱근이 입력되는 경우에 나머지정리모듈(82)은 두개의 제곱근을 수식4 또는 수식7 에 적용하여 가상제곱근(PR(M))을 산출한다. 수식4 또는 수식7 에 의해 산출되어진 가상제곱근(PR(M))은 나머지정리모듈(82)의 제2 출력단자(82B)를 통해 출력된다.

또한, 디지탈 서명 생성장치는 제1 및 제2 르잔드르심볼(L(M/p),L(M/q)을 비교하는 비교기(84)와, 나머지정리모듈(82)의 제2 출력단자(82B)로부터의 가상제곱근(PR(M))을 모듈러승산하기 위한 모듈로 승산기(86)를 구비한다. 비교기(84)는 제1 및 제2 르잔드르심볼(L(M/p), L(M/q)의 논리값들이 같은 경우에 "1"의 논리값을 반대로 제1 및 제2 르잔드르심볼(L(M/p), L(M/q)의 논리값이 서로 다른 경우에는 "0"의 논리값을 각각 가지는 비교신호를 발생한다. 비교기(84)에서 발생되는 비교신호는 인버터(88)에 의해 반전되어 디코딩플래그로써 레지스터(100)에 저장된다. 모듈로 승산기(86)는 수식12와 같이 나머지정리모듈(82)로부터의 가상제곱근(PR(M))을 비밀키의 제3 키원소(b)와 승산하고 공개키의 제1 키원소(pq)에 의해 모듈러 연산하고 그 연산된 결과를 제1 AND 게이트(90)에 공급한다. 제1 AND 게이트(90)는 제2 AND 게이트(92)와 함께 제2 어드레스어블 디코더(98)의 제어를 받는다. 제2 어드레스어블 디코더(98)는 비교기(84)로부터의 비교신호의 논리값에 따라 제1 및 제2 AND 게이트(90, 92) 중 어느 한쪽에만 하이논리의 논리신호를 제공한다. 이를 상세히 하면, 비교신호가 "0"의 논리값을 가지는 경우에 제1 AND 게이트(90)에 하이논리의 논리신호가 공급된다. 이 때, 모듈러 승산기(86)의 연산결과는 제1 AND 게이트(90) 및 제3멀티플렉서(96)을 경유하여 레지스터(100)에 서명코드(S)로서 저장된다. 반대로, 비교신호가 "1"의 논리값을 가지는 경우에는 제2 AND 게이트(92)에 하이논리의 논리신호가 공급되게 된다. 이 경우, 나머지정리모듈(82)의 제1 출력단자(82A)에서 출력되는 가상제곱근(PR(M))은 제2 AND 게이트(92) 및 제3 멀티플렉서(96)를 경유하여 레지스터(100)에 서명코드(S)로서 저장된다. 레지스터(100)에는 디코딩플래그(f)와 서명코드(S) 외에도 디지탈 문서(M)을 비트순대로 저장함으로써 디지탈 서명 메세지(DSM)을 형성하게 된다. 이 레지스터(100)에 저장되어진 디지탈 서명 메세지(DSM)은 도시하지 않은 통신채널을 통해 송출되게 된다.

도4 은 본 발명의 실시예에 따른 디지탈 서명 생성장치 및 그 장치가 적용된 통신망 시스템을 개략적으로 도시한다. 도4 에 도시된 통신망 시스템은 통신망(110)에 접속되어진 제1 내지 제3 데이타 스테이션(120, 130, 140)을 구비한다. 제1 데이타 스테이션(120)은 제1 데이타종단장치(122)와 통신망(110) 사이에 직렬 접속된 디지탈 서명 생성장치(124) 및 제1 데이타회선정합장치(126)로 구성되어 있다. 제1 데이타종단장치(122)는 통신망(110)쪽으로 전송될 디지탈 문서 또는 통신망(110)으로부터의 디지탈 문서를 처리한다. 디지탈 서명 생성장치(124)는 제1 데이타종단장치(122)로부터의 비밀키를 이용하여 제1 데이타종단장치(122)로부터 제1 데이타회선정합장치(126)쪽으로 전송될 디지탈 문서에 대한 서명코드를 생성하고 그 서명코드를 디지탈 문서와 함께 제1 데이타회선정합장치(126)에 공급한다. 이를 위하여, 디지탈 서명 생성장치(124)는 도3 에 도시된 바와 같은 회로구성을 가진다. 제1 데이타회선정합장치(126)는 디지탈 서명 생성 장치(124)로부터의 서명코드와 디지탈문서를 통신망쪽으로 전송하게 된다. 아울러, 제1 데이타회

선정합장치(126)는 통신망(110)과 제1 데이타종단장치(122) 간의 디지탈 문서를 중계한다.

제2 데이타 스테이션(130)은 통신망(110)에 직렬 접속된 제2 데이타종단장치(132)와 제2 데이타회선정합장치(134)로 구성된다. 제2 데이타종단장치(132)는 제1 데이타종단장치(122)와 마찬가지로 통신망(110)쪽으로 전송될 디지탈 문서 또는 통신망(110)으로부터의 디지탈 문서를 처리한다. 이와 더불어, 제2 데이타종단장치(132)는 비밀키를 이용하여 통신망(110)쪽으로 전송될 디지탈 문서에 대한 서명코드와 서명코드의 디코딩방법을 지시하는 디코딩 플래그를 생성하고 그 서명코드 및 디코딩플래그를 디지탈 문서와 함께 제2 데이타회선정합장치(134)을 경유하여 통신망(110)쪽으로 전송한다. 이를 위하여, 제2 데이타종단장치(132)는 디지탈 서명 생성 프로그램(132A)를 구비한다. 제2 데이타회선정합장치(134)는 제2 데이타종단장치(132)와 통신망(110)과의 디지탈 문서를 중계한다.

제3 데이타 스테이지(140)도 제2 데이타 스테이지(130)과 마찬가지로 통신망(110)과 직렬 접속되어진 제3 데이타종단장치(142)와 제3 데이타회선정합장치(144)로 구성된다. 이들 제3 데이타종단장치(142)와 제3 데이타회선정합장치(144)는 제2 데이타종단장치(132)와 제2 데이타회선정합장치(134)와 동일한 기능을 수행하므로 상세한 설명은 생략하기로 한다.

발명의 효과

상술한 바와 같이, 본 발명에 따른 디지탈 서명 생성방법 및 장치는 브름수, 즉4n+3 형태의 두 소수의 곱에 해당하는 크기의 숫자링(Zpq^*)에서의 연산에 의해서 디지탈 서명을 생성함으로써 디지탈 서명에 소인수 분해와 같은 수준의 안정성을 부여할 수 있고 공개키의 길이를 짧게 할 수 있다. 이 결과, 본 발명의 디지탈 서명 생성방법 및 장치에서는 연산량이 대폭적으로 감소됨은 물론 효율이 극대화 된다. 이와 더불어, 본 발명에 따른 디지탈 서명 생성방법 및 장치는 디지탈 서명의 생성시에 비밀키의 일부 키원소의 사용여부를 지시함으로써 디지탈 서명의 확인시의 연산량을 대폭적으로 감소시키고 디지탈 서명의 확인 효율을 높일 수 있다.

또한, 본 발명에 따른 디지탈 서명 확인방법은 디지탈 서명의 생성과정에 따라 디지탈 서명을 디코딩함으로써 연산량을 대폭적으로 줄일 수 있고 확인 효율을 극대화 할 수 있다.

이상 설명한 내용을 통해 당업자라면 본 발명의 기술사상을 일탈하지아니하는 범위에서 다양한 변경 및 수정이 가능함을 알 수 있을 것이다. 따라서, 본 발명의 기술적 범위는 실시예에 기재된 내용으로 한정되는 것이 아니라 특허 청구의 범위에 의하여 정하여져야만 한다.

(57) 청구의 범위

청구항 1

임의의 브름 수의 크기를 가지는 유한체에서 연산을 수행하여 디지탈문서(M)에 대한 서명코드를 생성하는 것을 특징으로 하는 디지탈 서명 생성방법.

청구항 2

제 1 항에 있어서,

상기 서명코드는 상기 유한체에서의 제곱근 연산에 의해 생성되는 것을 특징으로 하는 디지탈 서명 생성방법.

청구항 3

승산값이 임의의 브름 수가 되는 제1 및 제2 키원소(p, q)를 가지는 비밀키를 마련하는 단계와,

디지탈 문서(M)의 제곱근 (R(M))을 산출하는 단계와,

상기 디지탈 문서(M)의 부의 값에 대한 제곱근 (R(-M))을 산출하는 단계와,

상기 제1 키원소(p)와 상기 제2 키원소(q)의 곱에 해당하는 크기의 유한체와 디지탈 문서(M)의 제곱근과의 포함관계를 판단하는 단계와,

상기 유한체와 상기 디지탈 문서(M)의 제곱근(PR(M))과의 포함관계에 따라 상기 디지탈 문서(M)의 제곱근(R(M))과 상기 디지탈 문서(M)의 부의값에 대한 제곱근 (R(-M) 중 어느 하나를 이용하여 서명코드(S)를 산출하는 단계를 포함하는 것을 특징으로 하는 디지탈 서명 생성방법.

청구항 4

제 3 항에 있어서,

상기 서명코드(S)는 수식 $S = R \bmod pq$ 에 의해 산출된 것을 특징으로 하는 디지탈 서명 생성방법.

청구항 5

제 3 항에 있어서,

상기 디지탈 문서 (M)의 제곱근 (R(M))은 수식 $R = M^{1/2} \bmod pq$ 에 의해 산출된 것을 특징으로 하는 디지탈 서명 생성방법.

청구항 6

제 3 항에 있어서,

상기 디지탈 문서(M)의 부의 값에 대한 제곱근 (R(-M))은 수식 $R = (-M)^{1/2} \bmod pq$ 에 의해 산출된 것을 특징으로 하는 디지탈 서명 생성방법.

청구항 7

승산값이 임의의 브름 수가 되는 제1 및 제2 키원소(p, q)를 가지는 비밀키를 마련하는 단계와,

디지탈 문서(M)의 제곱근(R(M))이 상기 제1 키원소 (p)의 크기를 가지는 제1 유한체 (Zp)와 상기 제2 키원소의 크기를 가지는 제2 유한체 (Zq)와의 포함관계를 판단하는 단계와,

상기 유한체들 (Zp, Zq)과 상기 디지탈 문서 (M)의 제곱근 (R(M))과의 포함관계에 따라 상이한 연산식을 이용하여 상기 디지탈 문서 (M)의 가상제곱근 (PR(M))을 산출하는 단계와,

상기 가상제곱근 (PR(M))을 이용하여 서명코드 (S)를 산출하는 단계를 포함하는 것을 특징으로 하는 디지탈 서명 생성방법.

청구항 8

제 7 항에 있어서,

상기 서명코드 (S)는 수식 $S = PR(M) \bmod pq$ 에 의해 산출된 것을 특징으로 하는 디지탈 서명 생성방법.

청구항 9

제 7 항에 있어서,

상기 디지탈 문서 (M)의 가상제곱근 (PR (M))은,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 유한체들 (Zp, Zq) 모두에 속하면 수식 $PR(M) = M^{1/2} \bmod pq$ 에 의해 산출되고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 유한체들 (Zp, Zq) 모두에 속하지 않으면 수식 $PR(M) = (-M)^{1/2} \bmod pq$ 에 의해 산출되고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 제1 유한체 (Zp)에만 속하면 수식들 $x1 = M^{1/2} \bmod p$, $x2 = (-M)^{1/2} \bmod q$ 및 $PR(M) = x1 + p(x2 - x1^2) \cdot pq^{-1} \bmod pq$ 에 의해 산출되고, 여기서 $p^{q^{-1}}$ 상기 제1 키원소(p)와 승산하여 "1"을 산출하는 제2 유한체 (Zq)의 한 원소이고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 제2 유한체 (Zq)에만 속하면 수식들 $x1 = M^{1/2} \bmod q$, $x2 = (-M)^{1/2} \bmod p$ 및 $PR(M) = x1 + p(x2 - x1^2) \cdot q_p^{-1} \bmod pq$ 에 의해 산출되고, 여기서 q_p^{-1} 는 상기 제2 키원소 (q)와 승산하여 "1"을 산출하는 제1 유한체 (Zq)의 한 원소임을 특징으로 하는 디지탈 서명 생성방법.

청구항 10

승산값이 임의의 브름 수가 되는 제1 및 제2 키원소 (p,q)와 임의의 정수인 제3 키원소 (b)를 가지는 비밀키를 마련하는 단계와,

디지탈 문서 (M)의 제곱근 (R (M))이 상기 제1 키원소 (p)의 크기를 가지는 제1 유한체 (Zp)와 상기 제2 키원소의 크기를 가지는 제2 유한체 (Zq)와의 포함관계를 판단하는 단계와,

상기 유한체들 (Zp, Zq)과 상기 디지탈 문서 (M)의 제곱근 (R (M))과의 포함관계에 따라 상이한 연산식을 이용하여 상기 디지탈 문서 (M)의 가상제곱근 (PR (M))을 산출하는 단계와,

상기 유한체들 (Zp, Zq)과 상기 디지탈 문서 (M)의 제곱근 (R (M))과의 포함관계에 따라 상기 제3 키원소 (b)와 상기 가상제곱근 (PR (M))와의 연산을 선택적으로 수행하여 서명코드 (S)를 산출하는 단계를 포함하는 것을 특징으로 하는 디지탈 서명 생성방법.

청구항 11

제 10 항에 있어서,

상기 서명코드 (S)는,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 유한체들 (Zp, Zq) 모두에 속하는 경우와 상기 유한체들 (Zp, Zq) 모두에 속하지 않는 경우에는 수식 $S = PR(M) \bmod pq$ 에 의해 산출되고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 유한체들 (Zp, Zq)) 중 어느 한쪽의 유한체에만 속하면 수식 $S = b \times PR(M) \bmod pq$ 에 의해 산출되는 것을 특징으로 하는 디지탈 서명 생성방법.

청구항 12

제 11 항에 있어서,

상기 서명코드 (S)의 연산과정에서의 상기 제3 키원소 (b)의 사용여부를 나타내는 디코딩플래그 (f)를 생성하는 단계를 추가로 포함하는 것을 특징으로 하는 디지탈 서명 생성방법.

청구항 13

제 12 항에 있어서,

상기 디지탈 문서 (M)의 가상제곱근 (PR (M))은,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 유한체들 (Zp, Zq) 모두에 속하면 수식 $PR(M) = M^{1/2} \bmod pq$ 에 의해 산출되고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 유한체들 (Zp, Zq) 모두에 속하지 않으면 수식 $PR(M) = (-M)^{1/2} \bmod pq$ 에 의해 산출되고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 제1 유한체 (Zp)에만 속하면 수식들 $x1 = M^{1/2} \bmod p$, $x2 = (-M)^{1/2} \bmod q$ 및 $PR(M) = x1 + p\,(x2-x1^2) \cdot p_q^{-1} \bmod pq$ 에 의해 산출되고, 여기서 p_q^{-1} 상기 제1 키원소 (p)와 승산하여 "1"을 산출하는 제2 유한체 (Zq)의 한 원소이고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 제2 유한체 (Zq)에만 속하면 수식들 $x1 = M^{1/2} \bmod q$, $x2 = (-M)^{1/2} \bmod p$ 및 $PR(M) = x1 + p(x2-x1^2) \cdot q_p^{-1} \bmod pq$ 에 의해 산출되고, 여기서 q_p^{-1} 는 상기 제2 키원소 (q)와 승산하여 "1"을 산출하는 제1 유한체 (Zq)의 한 원소임을 특징으로 하는 디지탈 서명 생성방법.

청구항 14

임의의 브름 수의 크기를 가지는 유한체에서 연산을 수행하여 디지탈문서 (M)에 대한 서명코드를 생성하는 것을 특징으로 하는 디지탈 서명 생성장치.

청구항 15

제 14 항에 있어서,

상기 서명코드는 상기 유한체에서의 제곱근 연산에 의해 생성되는 것을 특징으로 하는 디지탈 서명 생성장치.

청구항 16

승산값이 임의의 브름 수가 되는 제1 및 제2 키원소 (p, q)를 가지는 비밀키와 디지탈 문서 (M)를 입력하는 입력수단과,

상기 디지탈 문서 (M)의 제곱근 (R (M))을 산출하는 제1 연산수단과,

상기 디지탈 문서 (M)의 부의 값에 대한 제곱근 (R (-M))을 산출하는 제2 연산수단과,

상기 제1 키원소 (p)와 상기 제2 키원소 (q)의 곱에 해당하는 크기의 유한체와 상기 디지탈 문서 (M)의 상기 제곱근 (R (M))과의 포함관계를 검출하는 포함관계 검 출수단과,

상기 유한체와 상기 디지탈 문서 (M)의 제곱근 (PR (M))과의 포함관계에 따라 상기 디지탈 문서 (M)의 제곱근 (R (M))과 상기 디지탈 문서 (M)의 부의 값에 대한 제곱근 (R (-M) 중 어느 하나를 이용하여 서명코드 (S)를 산출하는 제3 연산수단을 구비하는 것을 특징으로 하는 디지탈 서명 생성장치.

청구항 17

제 16 항에 있어서,

상기 제3 연산수단은 수식 $S = R \bmod pq$ 에 의해 상기 서명코드 (S)를 산출하는 것을 특징으로 하는 디지탈 서명 생성장치.

청구항 18

제 16 항에 있어서,

상기 제1 연산수단은 수식 $R = M^{1/2} \bmod pq$ 에 의해 상기 디지탈 문서 (M)의 상기 제곱근 (R (M))을 산출하는 것을 특징으로 하는 디지탈 서명 생성장치.

청구항 19

제 16 항에 있어서,

상기 제2 연산수단은 수식 $R = (-M)^{1/2} \bmod pq$ 에 의해 상기 디지탈문서 (M)의 부의 값에 대한 상기 제곱근 (R (-M))을 산출하는 것을 특징으로 하는 디지탈 서명 생성장치.

청구항 20

승산값이 임의의 브름 수가 되는 제1 및 제2 키원소 (p, q)를 가지는 비밀키와 디지탈문서 (M)를 입력하는 입력수단과,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 제1 키원소 (p)의 크기를 가지는 제1 유한체 (Zp)와 상기 제2 키원소의 크기를 가지는 제2 유한체 (Zq)와의 포함관계를 검출하는 포함관계검출수단과,

상기 유한체들 (Zp, Zq)과 상기 디지탈 문서 (M)의 상기 제곱근 (R (M))과의 포함관계에 따라 상이한 연산식을 이용하여 상기 디지탈 문서 (M)의 가상제곱근 (PR (M))을 산출하는 제1 연산수단과,

상기 가상제곱근 (PR (M))을 이용하여 서명코드 (S)를 산출하는 제2 연산수단을 구비하는 것을 특징으로 하는 디지탈 서명 생성장치.

청구항 21

제 20 항에 있어서,

상기 제2 연산수단은 수식 S = PR(M) mod pq 에 의해 상기 서명코드 (S)는 산출하는 것을 특징으로 하는 디지탈 서명 생성장치.

청구항 22

제 20 항에 있어서,

상기 제1 연산수단은,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 유한체들 (Zp, Zq) 모두에 속하면 수식 PR (M) = $M^{1/2}$ mod pq 에 의해 상기 디지탈 문서 (M)의 상기 가상제곱근 (PR (M)) 을 산출하고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 유한체들 (Zp, Zq) 모두에속하지 않으면 수식 PR (M) = $(-M)^{1/2}$ mod pq 에 의해 상기 디지탈 문서 (M)의 상기 가상제곱근 (PR (M))을 산출하고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 제1 유한체 (Zp)에만 속하면 수식들 x1 = $M^{1/2}$ mod p, x2 = $(-M)^{1/2}$ mod q 및 PR (M) = x1 + $p(x2-x1^2)\cdot p_q^{-1}$ mod pq 에 의해 상기 디지탈 문서(M)의 상기 가상제곱근 (PR (M))을 산출하고, 여기서 p_q^{-1} 상기 제1 키원소 (p)와 승산하여 "1"을 산출하는 제2 유한체 (Zq)의 한 원소이고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 제2 유한체 (Zq)에만 속하면 수식들 x1 = $M^{1/2}$ mod q, x2 = $(-M)^{1/2}$ mod p 및 PR (M) = x1 + $p(x2-x1^2)\cdot q_p^{-1}$ mod pq 에 의해 상기 디지탈 문서 (M)의 상기 가상제곱근 (PR (M))을 산출하고, 여기서 q_p^{-1} 는 상기 제2 키원소(q)와 승산하여 "1"을 산출하는 제1 유한체 (Zq)의 한 원소임을 특징으로 하는 디지탈 서명 생성장치.

청구항 23

승산값이 임의의 브름 수가 되는 제1 및 제2 키원소 (p, q)와 임의의 정수인 제3 키원소 (b)를 가지는 비밀키와 디지탈 문서 (M)를 입력하는 단계와,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 제1 키원소 (p)의 크기를 가지는 제1 유한체 (Zp)와 상기 제2 키원소의 크기를 가지는 제2 유한체 (Zq)와의 포함관계를 검출하는 포함관계검출수단과,

상기 유한체들 (Zp, Zq)과 상기 디지탈 문서 (M)의 제곱근 (R (M))과의 포함관계에 따라 상이한 연산식을 이용하여 상기 디지탈 문서 (M)의 가상제곱근 (PR (M))을 산출하는 제1 연산수단과,

상기 유한체들 (Zp, Zq)과 상기 디지탈 문서 (M)의 제곱근 (R (M))과의 포함관계에 따라 상기 제3 키원소 (b)와 상기 가상제곱근 (PR (M))와의 연산을 선택적으로 수행하여 서명코드 (S)를 산출하는제2 연산수단을 구비하는 것을 특징으로 하는 디지탈 서명 생성장치.

청구항 24

제 23 항에 있어서,

상기 제2 연산수단은,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 유한체들 (Zp, Zq) 모두에 속하는 경우와 상기 유한체들 (Zp, Zq) 모두에 속하지 않는 경우에는 수식 S=PR (M) mod pq 에 의해 상기 서명코드 (S)를 산출하고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 유한체들 (Zp, Zq)) 중 어느 한쪽의 유한체에만 속하면 수식 S = b × PR (M) mod pq 에 의해 상기 서명코드 (S)를 산출하는 것을 특징으로 하는 디지탈 서명 생성장치.

청구항 25

제 24 항에 있어서,

상기 서명코드 (S)의 연산과정에서의 상기 제3 키원소 (b)의 사용여부를 나타내는 디코딩플래그 (f)를 생성하는 플래그생성수단을 추가로 구비하는 것을 특징으로 하는 디지탈 서명 생성장치.

청구항 26

제 25 항에 있어서,

상기 제1 연산수단은,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 유한체들 (Zp, Zq) 모두에 속하면 수식 PR (M) = $M^{1/2}$ mod pq 에 의해 상기 디지탈 문서 (M)의 상기 가상제곱근 (PR (M)) 을 산출하고,

상기 디지탈 문서 (M)의 제곱근 (R(M))이 상기 유한체들 (Zp, Zq) 모두에 속하지 않으면 수식 PR (M) =

$(-M)^{1/2}$ mod pq 에 의해 상기 디지탈 문서 (M)의 상기 가상제곱근 (PR (M))을 산출하고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 제1 유한체 (Zp)에만 속하면 수식들 $x1 = M^{1/2}$ mod p, $x2 = (-M)^{1/2}$ mod q 및 $PR(M) = x1 + p(x2-x1^{2}) \cdot p_{q}^{-1}$ mod pq 에 의해 상기 디지탈 문서 (M)의 상기 가상제곱근 (PR (M))을 산출하고, 여기서 p_q^{-1} 상기 제1 키원소 (p)와 승산하여 "1"을 산출하는 제2 유한체 (Zq)의 한 원소이고,

상기 디지탈 문서 (M)의 제곱근 (R (M))이 상기 제2 유한체 (Zq)에만 속하면 수식들 $x1 = M^{1/2}$ mod q, $x2 = (-M)^{1/2}$ mod p 및 $PR(M) = x1 + p(x2-x1^{2}) \cdot q_{p}^{-1}$ mod pq 에 의해 상기 디지탈 문서 (M)의 상기 가상제곱근 (PR (M))을 산출하고, 여기서 q_p^{-1} 는 상기 제2 키원소 (q)와 승산하여 "1"을 산출하는 제1 유한체 (Zq)의 한 원소임을 특징으로 하는 디지탈 서명 생성장치.

청구항 27

임의의 브름 수 (pq)의 크기를 가지는 유한체에서의 연산에 의해 생성되어진 디지탈 문서 (M)에 대한 서명코드 (S)를 확인하는 방법에 있어서,

상기 브롬 수의 키원소 (pq)를 가지는 공개키를 마련하는 단계와,

상기 서명코드 (S)의 4제곱값을 산출하는 단계와,

상기 디지탈 문서 (M)의 가상제곱값 (PS (M))을 수식 $PS(M) = M^{2}$ mod pq에 의해 산출하는 단계와,

상기 서명코드 (S)의 4제곱값과 상기 가상제곱값 (PS (M))을 비교하는 단계를 포함하는 것을 특징으로 하는 디지탈 서명 확인방법.

청구항 28

승산값이 임의의 브름 수가 되는 제1 및 제2 키원소 (p, q)와 임의의 정수인 제3 키원소 (b)를 가지는 비밀키중 디지탈 문서 (M)을 상기 제1 및 제2 키원소 (p, q)의 곱값의 크기를 가지는 유한체에서의 제곱근 연산함과 아울러 상기 그 제곱근을 제3 키원소 (b)와 선택적으로 연산함에 의해 생성되어진 서명코드 (S)를 확인하는 방법에 있어서,

상기 디지탈 문서 (M)와 상기 서명코드 (S)를 디코딩플래그 (f)와 함께 수신하는 단계와,

상기 브름 수의 제4 키원소 (pq)와 상기 제3 키원소 (b)의 4제곱값의 제5 키원소 (B)를 마련하는 단계와,

상기 서명코드 (S)의 4제곱값을 산출하는 단계와,

상기 키원소예 의한 모듈로연산을 포함하는 상기 디지탈 문서 (M)의 제곱연산에 상기 디코딩플래그에 따라 상기 제5 키원소 (B)를 선택적으로 적용하여 상기 디지탈 문서(M)의 가상제곱값 (PS (M))을 산출하는 단계와,

상기 서명코드 (S)의 4제곱값과 상기 가상제곱값 (PS (M))을 비교하는 단계를 포함하는 것을 특징으로 하는 디지탈 서명 확인방법.

청구항 29

제 28 항에 있어서,

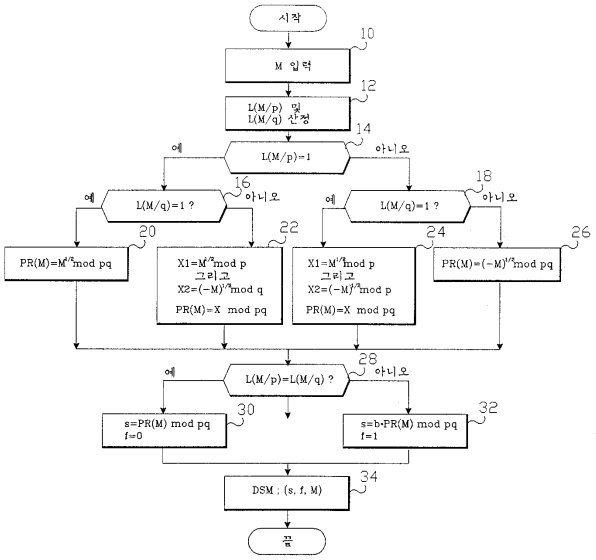
상기 가상제곱값은,

상기 디코딩플래그가 "1"의 논리값을 가지면 수식 $PS(M) = M^{2}$ mod pq에 의해 산출되고,

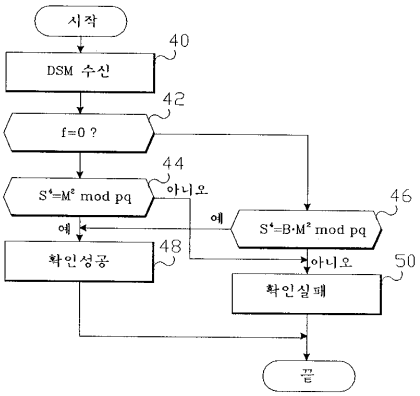
상기 디코딩플래그가 "0의 논리값을 가지면 수식 $PS(M) = B \times M^{2}$ mod pq 에 의해 산출되는 것을 특징으로 하는 디지탈 서명 확인방법.

도면

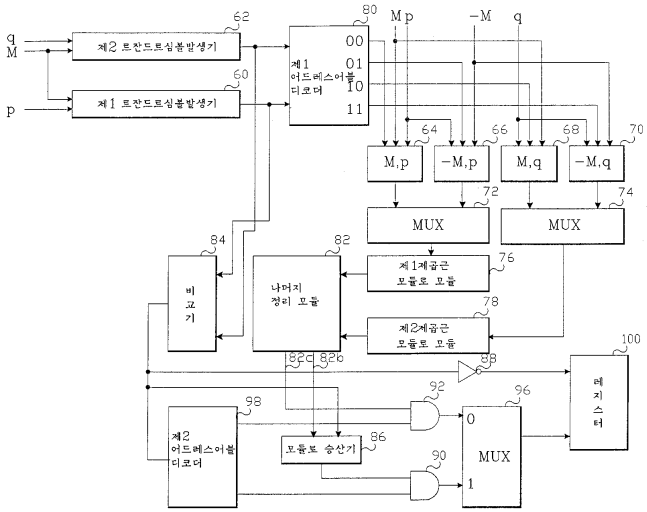
도면1


시작
10
M 입력
12
L(M/p) 및
L(M/q) 산정
14
L(M/p)=1
예
아니오
16
L(M/q)=1 ?
18
L(M/q)=1 ?
20
PR(M)=M^(1/2) mod pq
22
X1=M^(1/2) mod p
그리고
X2=(-M)^(1/2) mod q
PR(M)=X mod pq
24
X1=M^(1/2) mod p
그리고
X2=(-M)^(1/2) mod p
PR(M)=X mod pq
26
PR(M)=(-M)^(1/2) mod pq
28
L(M/p)=L(M/q) ?
30
s=PR(M) mod pq
f=0
32
s=b·PR(M) mod pq
f=1
34
DSM ; (s, f, M)
끝

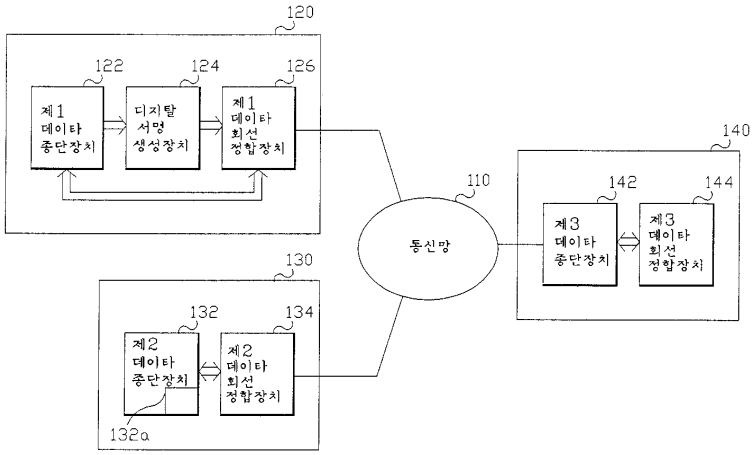
도면2


시작
40
DSM 수신
42
f=0 ?
44
S=M² mod pq
아니오
예
46
S=B·M² mod pq
48
확인성공
아니오
50
확인실패
끝

도면3


q
M
p
62
제2 로잔드르심볼발생기
60
제1 로잔드르심볼발생기
80
제1
어드레스어블
디코더
00
01
10
11
Mp
-M
q
64
66
68
70
M,p
-M,p
M,q
-M,q
72
74
MUX
MUX
84
82
비
교
기
나머지
정리 모듈
76
제1제곱근
모듈로 모듈
78
제2제곱근
모듈로 모듈
100
레
지
스
터
88
92
96
98
제2
어드레스어블
디코더
모듈로 승산기
86
90
0
1
MUX

도면4


120
122
124
126
제1
데이타
종단장치
디지탈
서명
생성장치
제1
데이타
회선
정합장치
110
통신망
140
142
144
제3
데이타
종단장치
제3
데이타
회선
정합장치
130
132
134
제2
데이타
종단장치
제2
데이타
회선
정합장치
132a