



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0060588
(43) 공개일자 2018년06월07일

(51) 국제특허분류(Int. Cl.)
G06F 21/33 (2013.01) H04L 9/30 (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G06F 21/33 (2013.01)
H04L 9/30 (2013.01)
(21) 출원번호 10-2016-0160261
(22) 출원일자 2016년11월29일
심사청구일자 2016년11월29일

(71) 출원인
서울대학교산학협력단
서울특별시 관악구 관악로 1 (신림동)
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
노중선
서울특별시 강남구 광평로10길 15 상록수아파트 109동 406호
이위직
서울특별시 관악구 관악로17길 8, 1102호
김영식
광주광역시 서구 풍암2로 62 금호2차아파트 201동 1005호
(74) 대리인
김효성

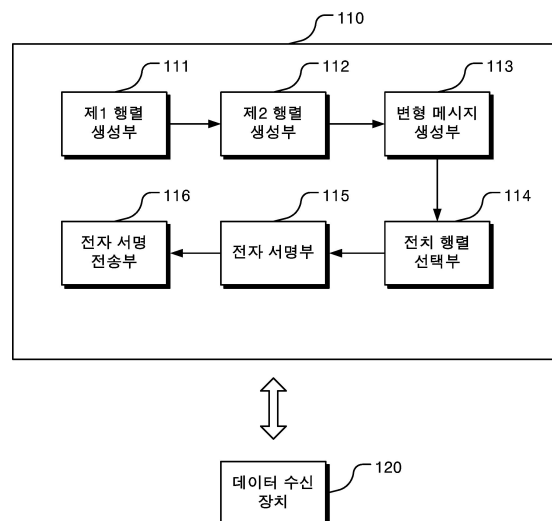
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 데이터 보안이 강화된 전자 서명 장치 및 방법

(57) 요약

데이터 보안이 강화된 전자 서명 장치 및 방법이 개시된다. 본 발명은 "1"과 "0"의 코드 값을 임의의 성분들로 포함하는 $(n-k) \times k$ 크기의 제1 부분 행렬(submatrix) R과 $(n-k) \times (n-k)$ 의 크기를 갖는 단위 행렬인 제2 부분 행렬 I가 열 방향으로 조합된 제1 행렬 H를 생성하고, "1"과 "0"의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q와 "1"과 "0"의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P를 생성한 후 상기 제1 행렬 H, 상기 스크램블링 행렬 Q 및 상기 순열 행렬 P를 개인키로 활용하여 전자 서명 값을 생성하고, 상기 스크램블링 행렬 Q, 상기 제1 행렬 H 및 상기 순열 행렬 P가 곱해진 QHP를 공개키로 사용하여 상기 전자 서명 값을 검증하는 새로운 방식의 전자 서명 생성 및 검증과 관련된 알고리즘을 제공할 수 있다.

대표도 - 도1



(52) CPC특허분류

H04L 9/3247 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711037819

부처명 미래창조과학부

연구관리전문기관 미래창조과학부

연구사업명 정보보호핵심원천기술개발

연구과제명 (창조씨앗 1단계) IoT 및 클라우드 컴퓨팅을 위한 경량 포스트 양자 암호 시스템 연구

기 여 율 1/1

주관기관 서울대학교 산학협력단

연구기간 2016.04.01 ~ 2016.12.31

명세서

청구범위

청구항 1

"1"과 "0"의 코드 값을 임의의 성분들로 포함하는 $(n-k) \times k - n$ 과 k 는 자연수이고 n 은 k 보다 큼 - 크기의 제1 부분 행렬(submatrix) R 과 $(n-k) \times (n-k)$ 의 크기를 갖는 제2 부분 행렬 I - 상기 제2 부분 행렬 I 는 $(n-k) \times (n-k)$ 의 크기를 갖는 단위 행렬임 - 가 열 방향으로 조합된 제1 행렬 H 를 생성하는 제1 행렬 생성부;

"1"과 "0"의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q 와 "1"과 "0"의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 를 생성하는 제2 행렬 생성부;

데이터 수신 장치로 전송할 평문 메시지 m 을 선정된(predetermined) 해시 함수인 $h(x)$ 에 입력으로 인가하여 해시 값 $h(m)$ - 상기 해시 값 $h(m)$ 은 크기가 $(n-k)$ 인 벡터로 $1 \times (n-k)$ 의 크기를 갖는 행렬로 표현됨 - 을 연산하고, 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 변형 메시지 m' - $m' = Q^{-1}h(m)^T$ 임 - 을 연산하는 변형 메시지 연산부;

$H z^T = m' - z^T$ 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐 - 을 만족하는 하나 이상의 z^T 들 중 어느 하나인 z_s^T 를 선택하는 전치 행렬 선택부;

상기 z_s^T 의 좌측 변에 상기 순열 행렬 P 의 역행렬인 P^{-1} 을 곱하여 $P^{-1}z_s^T$ 를 연산함으로써, 상기 연산된 $P^{-1}z_s^T$ 을 상기 평문 메시지 m 에 대한 전자 서명 값으로 생성하는 전자 서명부; 및

상기 데이터 수신 장치에 대해 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1}z_s^T$ 을 전송하는 전자 서명 전송부를 포함하는 데이터 보안이 강화된 전자 서명 장치.

청구항 2

제1항에 있어서,

상기 전치 행렬 선택부는

$H z^T = m'$ 을 만족하는 하나 이상의 z^T 들 중 상기 벡터 z 의 해밍 무게(Hamming Weight)가 기준치 이하로 연산되는 z^T 들로부터 상기 z_s^T 를 선택하는 데이터 보안이 강화된 전자 서명 장치.

청구항 3

제2항에 있어서,

상기 전치 행렬 선택부는

크기가 k 인 "0"의 코드 값으로만 구성된 제1 벡터 a 와 크기가 $(n-k)$ 인 m' 의 성분들로 구성된 제2 벡터 b 를 열 방향으로 나열하여 크기가 n 인 상기 벡터 z 의 초기값을 생성한 후 상기 벡터 z 의 초기값으로부터 상기 제1 부분 행렬 R 의 각 열의 성분 값들에 기초하여 상기 제1 벡터 a 와 상기 제2 벡터 b 의 성분 값을 조정하면서 $H z^T = m'$ 을 만족하는 z^T 들을 하나씩 연산하고, 상기 하나씩 연산되는 z^T 들 중 상기 벡터 z 의 해밍 무게가 상기 기준치 이하로 연산되는 z^T 가 발견되는 경우, 상기 발견된 z^T 를 상기 z_s^T 로 선택하는 데이터 보안이 강화된 전자 서명 장치.

청구항 4

제2항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 스크램블링 행렬 Q와 상기 제1 행렬 H 및 상기 순열 행렬 P가 곱해진 행렬인 $(n-k) \times n$ 크기를 갖는 $K_{pub} - K_{pub} = QHP$ 임 - 를 전자 서명에 대한 검증키로 저장하고 있고, 상기 평문 메시지 m과 상기 전자 서명 값 $P^{-1}z_s^T$ 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 기준치 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 기준치 이하인 것으로 확인되면, 상기 검증키 K_{pub} 에 기초하여 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 수행하는 데이터 보안이 강화된 전자 서명 장치.

청구항 5

제4항에 있어서,

상기 데이터 수신 장치는

상기 메모리 상에 상기 해시 함수 $h(x)$ 를 추가로 저장하고 있고, 상기 평문 메시지 m과 상기 전자 서명 값 $P^{-1}z_s^T$ 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 기준치 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 기준치 이하인 것으로 확인되면, 상기 평문 메시지 m을 상기 메모리 상에 저장되어 있는 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 상기 해시 값 $h(m)$ 을 연산한 후 상기 검증키 K_{pub} 에 상기 전자 서명 값 $P^{-1}z_s^T$ 을 곱한 결과 값인 $K_{pub}P^{-1}z_s^T$ 가 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 와 일치하는지 비교하여 상기 $K_{pub}P^{-1}z_s^T$ 가 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 성공으로 판단하는 데이터 보안이 강화된 전자 서명 장치.

청구항 6

"1"과 "0"의 코드 값을 임의의 성분들로 포함하는 $(n-k) \times k - n$ 과 k는 자연수이고 n은 k보다 큼 - 크기의 제1 부분 행렬(submatrix) R과 $(n-k) \times (n-k)$ 의 크기를 갖는 제2 부분 행렬 I - 상기 제2 부분 행렬 I는 $(n-k) \times (n-k)$ 의 크기를 갖는 단위 행렬임 - 가 열 방향으로 조합된 제1 행렬 H를 생성하는 단계;

"1"과 "0"의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q와 "1"과 "0"의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P를 생성하는 단계;

데이터 수신 장치로 전송할 평문 메시지 m을 선정된(predetermined) 해시 함수인 $h(x)$ 에 입력으로 인가하여 해시 값 $h(m)$ - 상기 해시 값 $h(m)$ 은 크기가 $(n-k)$ 인 벡터로 $1 \times (n-k)$ 의 크기를 갖는 행렬로 표현됨 - 을 연산하고, 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q의 역행렬인 Q^{-1} 을 곱하여 변형 메시지 $m' - m' = Q^{-1}h(m)^T$ 임 - 을 연산하는 단계;

$H z^T = m' - z^T$ 는 크기가 n인 벡터 z의 전치 행렬로 $n \times 1$ 의 크기를 가짐 - 을 만족하는 하나 이상의 z^T 들 중 어느 하나인 z_s^T 를 선택하는 단계;

상기 z_s^T 의 좌측 변에 상기 순열 행렬 P의 역행렬인 P^{-1} 을 곱하여 $P^{-1}z_s^T$ 를 연산함으로써, 상기 연산된 $P^{-1}z_s^T$ 을 상기 평문 메시지 m에 대한 전자 서명 값으로 생성하는 단계; 및

상기 데이터 수신 장치에 대해 상기 평문 메시지 m과 상기 전자 서명 값 $P^{-1}z_s^T$ 을 전송하는 단계

를 포함하는 데이터 보안이 강화된 전자 서명 방법.

청구항 7

제6항에 있어서,

상기 z_s^T 를 선택하는 단계는

$H z^T = m'$ 을 만족하는 하나 이상의 z^T 들 중 상기 벡터 z 의 해밍 무게(Hamming Weight)가 기준치 이하로 연산되는 z^T 들로부터 상기 z_s^T 를 선택하는 데이터 보안이 강화된 전자 서명 방법.

청구항 8

제7항에 있어서,

상기 z_s^T 를 선택하는 단계는

크기가 k 인 "0"의 코드 값으로만 구성된 제1 벡터 a 와 크기가 $(n-k)$ 인 m' 의 성분들로 구성된 제2 벡터 b 를 열 방향으로 나열하여 크기가 n 인 상기 벡터 z 의 초기값을 생성한 후 상기 벡터 z 의 초기값으로부터 상기 제1 부분 행렬 R 의 각 열의 성분 값들에 기초하여 상기 제1 벡터 a 와 상기 제2 벡터 b 의 성분 값을 조정하면서 $H z^T = m'$ 을 만족하는 z^T 들을 하나씩 연산하고, 상기 하나씩 연산되는 z^T 들 중 상기 벡터 z 의 해밍 무게가 상기 기준치 이하로 연산되는 z^T 가 발견되는 경우, 상기 발견된 z^T 를 상기 z_s^T 로 선택하는 데이터 보안이 강화된 전자 서명 방법.

청구항 9

제7항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 스크램블링 행렬 Q 와 상기 제1 행렬 H 및 상기 순열 행렬 P 가 곱해진 행렬인 $(n-k) \times n$ 크기를 갖는 $K_{pub} - K_{pub} = QHP$ 을 전자 서명에 대한 검증키로 저장하고 있고, 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1} z_s^T$ 가 수신되면, 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 기준치 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 기준치 이하인 것으로 확인되면, 상기 검증키 K_{pub} 에 기초하여 상기 전자 서명 값 $P^{-1} z_s^T$ 에 대한 검증을 수행하는 데이터 보안이 강화된 전자 서명 방법.

청구항 10

제9항에 있어서,

상기 데이터 수신 장치는

상기 메모리 상에 상기 해시 함수 $h(x)$ 를 추가로 저장하고 있고, 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1} z_s^T$ 가 수신되면, 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 기준치 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 기준치 이하인 것으로 확인되면, 상기 평문 메시지 m 을 상기 메모리 상에 저장되어 있는 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 상기 해시 값 $h(m)$ 을 연산한 후 상기 검증키 K_{pub} 에 상기 전자 서명 값 $P^{-1} z_s^T$ 를 곱한 결과 값인 $K_{pub} P^{-1} z_s^T$ 가 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 와 일치하는지 비교하여 상기 $K_{pub} P^{-1} z_s^T$ 가 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1} z_s^T$ 에 대한 검증을 성공으로 판단하는 데이터 보안이 강화된 전자 서명 방법.

청구항 11

제6항 내지 제10항 중 어느 한 항의 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 12

제6항 내지 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술 분야

[0001] 본 발명은 비대칭키를 활용하여 부인 방지를 수행하는 전자 서명 시스템에 활용될 수 있는 기술들과 관련된다.

배경 기술

[0002] 최근, 인터넷이 널리 보급됨에 따라, 온라인을 이용한 बैं킹 서비스나 결제 시스템의 도입이 활발하게 이루어지고 있다.

[0003] 이러한 온라인 बैं킹 서비스나 결제 시스템에서는 계좌 이체나 전자 결제를 하고자 하는 진정한 사람으로부터 계좌 이체 또는 전자 결제 요청이 있는지 여부를 정확하게 판단해야 할 필요가 있다.

[0004] 예컨대, A라는 사용자가 온라인 बैं킹 서비스를 통해서 B라는 사용자에게 계좌 이체를 한다고 했을 때, 온라인 बैं킹 서비스를 제공하는 시스템에서는 해당 계좌 이체 요청이 A라는 사용자에게 의해서 정말로 이루어진 것인지를 확인해야 할 필요가 있다.

[0005] 이렇게, 특정 사용자로부터 전달되는 메시지가 진정한 사용자에게 의해서 전달되는 것인지 여부를 확인하기 위한 보안 서비스를 부인 방지 서비스라고 칭한다.

[0006] 보통, 일반적인 온라인 बैं킹 서비스나 결제 시스템에서 도입하고 있는 부인 방지 서비스는 공개키 기반의 암호화 방식(Public Key Infrastructure: PKI)을 이용한 전자 서명 시스템이 주를 이루고 있다.

[0007] 공개키 기반의 암호화 방식의 전자 서명 시스템이란 메시지를 전달하는 측에서 해당 메시지에 대한 해시 값을 대해 자신의 개인키로 암호화를 수행하여 전자 서명 값을 생성한 후 해당 메시지와 상기 전자 서명 값을 메시지 수신측에 전달하면, 메시지 수신측에서 상기 개인키에 대응하는 공개키로 상기 전자 서명 값을 복호화하고, 메시지 전송측으로부터 수신한 상기 메시지에 대한 해시 값을 연산한 후 상기 공개키로 복호화한 값과 상기 메시지에 대한 해시 값을 비교하여 두 값이 서로 동일한 것으로 판단되면, 메시지 전송측으로부터 수신된 상기 전자 서명 값이 상기 메시지 전송측의 개인키에 의해서 정말로 암호화된 값임이 입증됨에 따라, 상기 메시지가 진정한 메시지 전송측으로부터 전달된 메시지임을 확인하는 시스템이다.

[0008] 이러한 공개키 기반의 암호화 방식의 전자 서명 시스템은 일반적으로 널리 알려진 DH(Diffie-Hellman) 알고리즘에 따른 키교환 방식 등을 활용해서, 개인키와 이에 대응하는 공개키를 생성한 후 상기 개인키로 전자 서명 값을 생성하고, 상기 공개키로 상기 전자 서명 값을 검증하는 형태로 운영되고 있다.

[0009] 이러한 기존의 전자 서명 생성 및 검증 알고리즘은 이미 관련 업계에서 널리 사용되고 있다는 점에서 전자 서명의 위변조 가능성이 높아 보안상 취약성을 가지고 있다.

[0010] 따라서, 기존의 전자 서명 생성 및 검증 알고리즘과 다른 새로운 방식의 전자 서명 생성 및 검증 알고리즘에 대한 연구가 필요하다.

발명의 내용

해결하려는 과제

[0011] 본 발명은 "1"과 "0"의 코드 값을 임의의 성분들로 포함하는 $(n-k) \times k$ 크기의 제1 부분 행렬(submatrix) R과 $(n-k) \times (n-k)$ 의 크기를 갖는 단위 행렬인 제2 부분 행렬 I가 열 방향으로 조합된 제1 행렬 H를 생성하고, "1"과 "0"의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스칼라블링 행렬 Q와 "1"과 "0"의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P를 생성한 후 상기 제1 행렬 H, 상기 스칼라블링 행렬 Q 및 상기 순열 행렬 P를 개인키로 활용하여 전자 서명 값을 생성하고, 상기 스칼라블링 행렬 Q, 상기 제1 행렬 H 및 상기 순열 행렬 P가 곱해진 QHP를 공개키로 사용하여 상기 전자 서명 값을 검증하는 새로운 방식의 전자 서명 생성 및 검증과 관련된 알고리즘을 제공하고자 한다.

과제의 해결 수단

[0012] 본 발명의 일실시예에 따른 데이터 보안이 강화된 전자 서명 장치는 "1"과 "0"의 코드 값을 임의의 성분들로 포함하는 $(n-k) \times k - n$ 과 k 는 자연수이고 n 은 k 보다 큰 크기의 제1 부분 행렬(submatrix) R 과 $(n-k) \times (n-k)$ 의 크기를 갖는 제2 부분 행렬 I - 상기 제2 부분 행렬 I 는 $(n-k) \times (n-k)$ 의 크기를 갖는 단위 행렬임 - 가 열 방향으로 조합된 제1 행렬 H 를 생성하는 제1 행렬 생성부, "1"과 "0"의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q 와 "1"과 "0"의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 를 생성하는 제2 행렬 생성부, 데이터 수신 장치로 전송할 평문 메시지 m 을 선정된(predetermined) 해시 함수인 $h(x)$ 에 입력으로 인가하여 해시 값 $h(m)$ - 상기 해시 값 $h(m)$ 은 크기가 $(n-k)$ 인 벡터로 $1 \times (n-k)$ 의 크기를 갖는 행렬로 표현됨 - 을 연산하고, 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 변형 메시지 $m' - m' = Q^{-1}h(m)^T$ 임 - 을 연산하는 변형 메시지 연산부, $H z^T = m' - z^T$ 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐 - 을 만족하는 하나 이상의 z^T 들 중 어느 하나인 z_s^T 를 선택하는 전치 행렬 선택부, 상기 z_s^T 의 좌측 변에 상기 순열 행렬 P 의 역행렬인 P^{-1} 을 곱하여 $P^{-1}z_s^T$ 를 연산함으로써, 상기 연산된 $P^{-1}z_s^T$ 을 상기 평문 메시지 m 에 대한 전자 서명 값으로 생성하는 전자 서명부 및 상기 데이터 수신 장치에 대해 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1}z_s^T$ 을 전송하는 전자 서명 전송부를 포함한다.

[0013] 또한, 본 발명의 일실시예에 따른 데이터 보안이 강화된 전자 서명 방법은 "1"과 "0"의 코드 값을 임의의 성분들로 포함하는 $(n-k) \times k - n$ 과 k 는 자연수이고 n 은 k 보다 큰 크기의 제1 부분 행렬 R 과 $(n-k) \times (n-k)$ 의 크기를 갖는 제2 부분 행렬 I - 상기 제2 부분 행렬 I 는 $(n-k) \times (n-k)$ 의 크기를 갖는 단위 행렬임 - 가 열 방향으로 조합된 제1 행렬 H 를 생성하는 단계, "1"과 "0"의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q 와 "1"과 "0"의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 를 생성하는 단계, 데이터 수신 장치로 전송할 평문 메시지 m 을 선정된 해시 함수인 $h(x)$ 에 입력으로 인가하여 해시 값 $h(m)$ - 상기 해시 값 $h(m)$ 은 크기가 $(n-k)$ 인 벡터로 $1 \times (n-k)$ 의 크기를 갖는 행렬로 표현됨 - 을 연산하고, 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 변형 메시지 $m' - m' = Q^{-1}h(m)^T$ 임 - 을 연산하는 단계, $H z^T = m' - z^T$ 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐 - 을 만족하는 하나 이상의 z^T 들 중 어느 하나인 z_s^T 를 선택하는 단계, 상기 z_s^T 의 좌측 변에 상기 순열 행렬 P 의 역행렬인 P^{-1} 을 곱하여 $P^{-1}z_s^T$ 를 연산함으로써, 상기 연산된 $P^{-1}z_s^T$ 을 상기 평문 메시지 m 에 대한 전자 서명 값으로 생성하는 단계 및 상기 데이터 수신 장치에 대해 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1}z_s^T$ 을 전송하는 단계를 포함한다.

발명의 효과

[0014] 본 발명은 "1"과 "0"의 코드 값을 임의의 성분들로 포함하는 $(n-k) \times k$ 크기의 제1 부분 행렬(submatrix) R 과 $(n-k) \times (n-k)$ 의 크기를 갖는 단위 행렬인 제2 부분 행렬 I 가 열 방향으로 조합된 제1 행렬 H 를 생성하고, "1"과 "0"의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q 와 "1"과 "0"의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 를 생성한 후 상기 제1 행렬 H , 상기 스크램블링 행렬 Q 및 상기 순열 행렬 P 를 개인키로 활용하여 전자 서명 값을 생성하고, 상기 스크램블링 행렬 Q , 상기 제1 행렬 H 및 상기 순열 행렬 P 가 곱해진 QHP를 공개키로 사용하여 상기 전자 서명 값을 검증하는 새로운 방식의 전자 서명 생성 및 검증과 관련된 알고리즘을 제공할 수 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명의 일실시예에 따른 데이터 보안이 강화된 전자 서명 장치의 구조를 도시한 도면이다.
 도 2는 본 발명의 일실시예에 따른 데이터 보안이 강화된 전자 서명 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0016] 이하에서는 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명하기로 한다. 이러한 설명은 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경,

균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였으며, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 본 명세서 상에서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 사람에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[0017] 도 1은 본 발명의 일실시예에 따른 데이터 보안이 강화된 전자 서명 장치의 구조를 도시한 도면이다.

[0018] 도 1을 참조하면, 본 발명에 따른 데이터 보안이 강화된 전자 서명 장치(110)는 제1 행렬 생성부(111), 제2 행렬 생성부(112), 변형 메시지 연산부(113), 전치 행렬 선택부(114), 전자 서명부(115) 및 전자 서명 전송부(116)를 포함한다.

[0019] 제1 행렬 생성부(111)는 "1"과 "0"의 코드 값을 임의의 성분들로 포함하는 $(n-k) \times k$ 크기의 제1 부분 행렬(submatrix) R과 $(n-k) \times (n-k)$ 의 크기를 갖는 제2 부분 행렬 I가 열 방향으로 조합된 제1 행렬 H를 생성한다.

[0020] 여기서, n과 k는 자연수이고 n은 k보다 큰 수이며, 상기 제2 부분 행렬 I는 $(n-k) \times (n-k)$ 의 크기를 갖는 단위 행렬이다.

[0021] 이때, 상기 제1 행렬 H는 상기 제1 부분 행렬 R과 상기 제2 부분 행렬 I가 열 방향으로 조합된 행렬이므로, 하기의 수학식 1과 같이 표현할 수 있다.

수학식 1

$$H = [R | I]$$

[0023]

[0025] 제2 행렬 생성부(112)는 "1"과 "0"의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스칼라블링 행렬 Q와 "1"과 "0"의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P를 생성한다.

[0026] 여기서, 제2 행렬 생성부(113)는 "1"과 "0"의 코드 값을 성분으로 갖는 $(n-k) \times (n-k)$ 크기의 상기 스칼라블링 행렬 Q와 $n \times n$ 크기의 상기 순열 행렬 P를 랜덤하게 생성할 수 있다.

[0027] 변형 메시지 연산부(113)는 데이터 수신 장치(120)로 전송할 평문 메시지 m을 선정된(predetermined) 해시 함수인 $h(x)$ 에 입력으로 인가하여 해시 값 $h(m)$ 을 연산하고, 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 의 좌측 변에 상기 스칼라블링 행렬 Q의 역행렬인 Q^{-1} 을 곱하여 변형 메시지 m'을 연산한다.

[0028] 여기서, 상기 해시 값 $h(m)$ 은 크기가 $(n-k)$ 인 벡터로 $1 \times (n-k)$ 의 크기를 갖는 행렬로 표현될 수 있고, 상기 변형 메시지 m'은 하기의 수학식 2에 따라 연산될 수 있다.

수학식 2

$$m' = Q^{-1}h(m)^T$$

[0030]

[0032] 전치 행렬 선택부(114)는 하기의 수학식 3에 따라 $Hz^T = m'$ 을 만족하는 하나 이상의 z^T 들 중 어느 하나인 z_s^T 를 선택한다.

[0033] 여기서, z^T 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 갖는 행렬을 의미한다.

수학식 3

$$Hz^T = m'$$

[0035]

[0037] 이때, 상기 제1 행렬 H 는 "1"과 "0"의 코드 값을 임의의 성분들로 포함하는 $(n-k) \times k$ 크기의 제1 부분 행렬 R 과 $(n-k) \times (n-k)$ 의 크기를 갖는 단위 행렬인 제2 부분 행렬 I 로 구성되어 있어서, 상기 수학식 3의 조건을 만족하는 $n \times 1$ 의 크기를 갖는 행렬인 z^T 는 행렬의 대수적 특성상 "1"과 "0"의 코드 값을 성분들로 포함하는 서로 다른 행렬들이 다수개 존재할 수 있다.

[0038] 그리고 나서, 전자 서명부(114)는 상기 z_s^T 의 좌측 변에 상기 순열 행렬 P 의 역행렬인 P^{-1} 을 곱하여 $P^{-1}z_s^T$ 를 연산함으로써, 상기 연산된 $P^{-1}z_s^T$ 을 상기 평문 메시지 m 에 대한 전자 서명 값으로 생성한다.

[0039] 이렇게, 상기 전자 서명 값 $P^{-1}z_s^T$ 가 생성되면, 전자 서명 전송부(116)는 데이터 수신 장치(120)에 대해 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1}z_s^T$ 을 전송한다.

[0040] 이렇게, 데이터 보안이 강화된 전자 서명 장치(110)로부터 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1}z_s^T$ 가 데이터 수신 장치(120)로 전송되면, 데이터 수신 장치(120)는 상기 전자 서명 값 $P^{-1}z_s^T$ 가 데이터 보안이 강화된 전자 서명 장치(110)에서 생성된 상기 스크램블링 행렬 Q , 상기 제1 행렬 H 및 상기 순열 행렬 P 에 기반하여 정상적으로 생성된 것인지 여부를 검증하는 과정을 수행하게 된다.

[0041] 이를 위해서, 데이터 수신 장치(120)는 메모리 상에 상기 스크램블링 행렬 Q 와 상기 제1 행렬 H 및 상기 순열 행렬 P 가 곱해진 행렬인 $(n-k) \times n$ 크기를 갖는 $K_{pub} = K_{pub}QHP$ 를 전자 서명에 대한 검증키로 저장하고 있고, 이와 동시에 상기 해시 함수 $h(x)$ 도 저장하고 있다.

[0042] 이때, 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1}z_s^T$ 가 데이터 수신 장치(120)로 수신되면, 데이터 수신 장치(120)는 상기 평문 메시지 m 을 상기 메모리 상에 저장되어 있는 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 상기 해시 값 $h(m)$ 을 연산한 후 상기 검증키 K_{pub} 에 상기 전자 서명 값 $P^{-1}z_s^T$ 을 곱한 결과 값인 $K_{pub}P^{-1}z_s^T$ 을 연산할 수 있다.

[0043] 그리고 나서, 데이터 수신 장치(120)는 상기 $K_{pub}P^{-1}z_s^T$ 가 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 와 일치하는지 여부를 비교하여 상기 $K_{pub}P^{-1}z_s^T$ 가 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 성공으로 판단하여 상기 평문 메시지 m 이 진정한 소유자로부터 전송된 평문 메시임을 확인할 수 있다.

[0044] 관련해서, 상기 전자 서명 값 $P^{-1}z_s^T$ 가 상기 스크램블링 행렬 Q , 상기 제1 행렬 H 및 상기 순열 행렬 P 에 의해 정상적으로 생성된 전자 서명 값이라고 한다면, 상기 $K_{pub}P^{-1}z_s^T$ 는 하기의 수학식 4에 따라 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 로 연산될 수 있다.

수학식 4

$$\begin{aligned}
 K_{pub}P^{-1}z_s^T &= (QHP)P^{-1}z_s^T \\
 \Rightarrow (QHP)P^{-1}z_s^T &= QHz_s^T \\
 \Rightarrow QHz_s^T &= Q(m') \\
 \Rightarrow Q(m') &= Q(Q^{-1}h(m)^T) \\
 \Rightarrow Q(Q^{-1}h(m)^T) &= h(m)^T
 \end{aligned}$$

[0046]

[0048]

이렇게, 본 발명에 따른 데이터 보안이 강화된 전자 서명 장치(110)는 상기 수학식 2에 따라 m' 을 연산한 후 상기 수학식 3의 연산을 만족하는 하나 이상의 z^T 들을 찾고, 이러한 하나 이상의 z^T 들 중 어느 하나의 값에 해당되는 z_s^T 를 선택하여 상기 z_s^T 에 대해 상기 순열 행렬 P 의 역행렬인 P^{-1} 을 곱한 결과 값인 $P^{-1}z_s^T$ 를 상기 평문 메시지 m 에 대한 전자 서명 값으로 생성한 후 데이터 수신 장치(120)에 대해 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1}z_s^T$ 을 전송하는 방식으로 전자 서명 과정을 완료함으로써, 결국, 상기 전자 서명 값 $P^{-1}z_s^T$ 를 생성하기 위해서, 상기 스크램블링 행렬 Q , 상기 제1 행렬 H 및 상기 순열 행렬 P 를 전자 서명을 위한 개인키로 활용하게 되는 것이다. 그리고, 데이터 수신 장치(120)는 상기 전자 서명 값 $P^{-1}z_s^T$ 을 검증하기 위해서, 상기 스크램블링 행렬 Q , 상기 제1 행렬 H 및 상기 순열 행렬 P 가 곱해진 QHP 를 공개키로 사용하게 되는 것이다.

[0049]

본 발명의 일실시예에 따르면, 전치 행렬 선택부(114)는 상기 전자 서명 값 $P^{-1}z_s^T$ 를 생성할 때, 제3자에 의한 상기 전자 서명 값 $P^{-1}z_s^T$ 의 예측을 방지하기 위해서, Hm^T 을 만족하는 하나 이상의 z^T 들 중 어느 하나인 z_s^T 를 선택하는 과정에서 추가적인 보안 조건을 설정할 수 있다.

[0050]

관련해서, 본 발명의 일실시예에 따르면, 전치 행렬 선택부(114)는 Hm^T 을 만족하는 하나 이상의 z^T 들 중 상기 벡터 z 의 해밍 무게(Hamming Weight)가 기준치 이하로 연산되는 z^T 들로부터 상기 z_s^T 를 선택할 수 있다.

[0051]

여기서, 해밍 무게란 "0"과 "1"로 구성된 코드 값들의 집합에서 "1"이라는 코드 값의 개수를 의미한다.

[0052]

예컨대, Hm^T 을 만족하는 하나 이상의 z^T 들이 10개 존재한다고 하고, 상기 10개의 z^T 들 중 상기 벡터 z 의 해밍 무게가 상기 기준치 이하로 연산되는 z^T 가 3개 존재한다고 하면, 전치 행렬 선택부(114)는 상기 10개의 z^T 들 중에서 상기 z_s^T 를 선택하는 것이 아니라, 상기 벡터 z 의 해밍 무게가 상기 기준치 이하로 연산되는 상기 3개의 z^T 들 중에서 상기 z_s^T 를 선택함으로써, 상기 z_s^T 가 선택되는 조건을 "해밍 무게가 상기 기준치 이하일 것"이라는 추가 조건을 설정할 수 있다.

[0053]

또한, 본 발명의 일실시예에 따르면, 전치 행렬 선택부(114)는 Hm^T 을 만족하는 하나 이상의 z^T 들 중 상기 벡터 z 의 해밍 무게가 상기 기준치 이하로 연산되는 z_s^T 를 선택하는 방법으로, 크기가 k 인 "0"의 코드 값으로만 구성된 제1 벡터 a 와 크기가 $n-k$ 인 m' 의 성분들로 구성된 제2 벡터 b 를 열 방향으로 나열하여 크기가 n 인 상기 벡터 z 의 초기값을 생성한 후 상기 벡터 z 의 초기값으로부터 상기 제1 부분 행렬 R 의 각 열의 성분 값들에 기초하여 상기 제1 벡터 a 와 상기 제2 벡터 b 의 성분 값을 조정하면서 Hm^T 을 만족하는 z^T 들을 하나씩 연산하고, 상기 하나씩 연산되는 z^T 들 중 상기 벡터 z 의 해밍 무게가 상기 기준치 이하로 연산되는 z^T 가 발견되는 경우, 상기

발견된 z^T 를 상기 z_s^T 로 선택할 수 있다.

[0054] 관련해서, 상기 벡터 z 는 상기 제1 벡터 a 와 상기 제1 벡터 b 가 열 방향으로 나열된 벡터라고 하였으므로, 상기 벡터 z 는 하기의 수학식 5와 같이 표현할 수 있다.

수학식 5

$$z = [a|b]$$

[0056]

[0058] 이때, 전치 행렬 선택부(114)는 우선 상기 제1 벡터 a 의 성분을 모두 "0"의 코드 값으로 채우고, 상기 제2 벡터 b 의 성분을 모두 m' 의 성분들로 채움으로써, 상기 벡터 z 의 초기값을 생성할 수 있다.

[0059] 만약, 상기 벡터 z 의 초기값의 해밍 무게가 상기 기준치 이하가 된다면, 전치 행렬 선택부(114)는 상기 벡터 z 의 초기값에 대한 전치 행렬을 상기 z_s^T 로 선택할 수 있다.

[0060] 하지만, 상기 벡터 z 의 초기값의 해밍 무게가 상기 기준치를 초과한다면, " $w*v$ "의 연산을 하기의 수학식 6에 따라 정의하였을 때, " $r_i * m' \geq 2$ "의 조건을 만족하는 경우에 한해서 전치 행렬 선택부(114)는 상기 제1 벡터 a 의 성분과 상기 제2 벡터 b 의 성분을 하기의 수학식 7에 따라 변경할 수 있다.

수학식 6

$$w^*v = \sum_{j=1}^{n-k} c_j$$

$$c_j = \begin{cases} 1 & a_j = b_j = 1 \\ -1 & a_j = 1, b_j = 1 \\ 0 & else \end{cases}$$

[0062]

수학식 7

$$a_i \leftarrow 1 - a_i, b_e \leftarrow b_e + r_i$$

[0064]

[0066] 여기서, r_i 는 상기 제1 부분 행렬 R 에 존재하는 k 개의 열들 중 i 번째 열에 위치하는 $(n-k)$ 개의 성분들을 의미하고, a_i 는 상기 제1 벡터 a 를 구성하는 k 개의 성분들 중 i 번째 열에 위치하는 성분을 의미하며, b_e 는 상기 제2 벡터 b 를 구성하는 $(n-k)$ 개의 성분 전체를 의미한다.

- [0067] 이러한 상황 하에서 상기 벡터 z 의 초기값의 해밍 무게가 상기 기준치를 초과하는 경우, 전치 행렬 선택부(114)는 $i=1$ 일 때, " $r_1 * m$ "을 연산하고, 해당 연산 결과 값이 2보다 크거나 같은지 여부를 판단할 수 있다.
- [0068] 관련해서, r_1 은 상기 제1 부분 행렬 R 에 존재하는 k 개의 열들 중 첫 번째 열에 위치하는 $(n-k)$ 개의 성분들이고, m '의 성분들의 개수도 $(n-k)$ 개이므로, 전치 행렬 선택부(114)는 상기 수학식 6에 따라 $(n-k)$ 개의 r_1 의 성분들과 $(n-k)$ 개의 m '의 성분들을 각각 하나씩 서로 비교하여 각 성분들의 비교 결과 값의 합인 " $r_1 * m$ "을 연산할 수 있다.
- [0069] 그리고 나서, 상기 연산된 " $r_1 * m$ "이 2보다 크거나 같은 것으로 확인되면, 전치 행렬 선택부(114)는 상기 수학식 7의 연산에 따라 상기 제1 벡터 a 를 구성하는 k 개의 성분들 중 첫 번째 열에 위치하는 성분인 a_1 을 $1-a_1$ 으로 대체할 수 있다. 예컨대, a_1 의 성분이 "0"이라는 코드 값인 경우, 전치 행렬 선택부(114)는 a_1 의 성분을 " $1-0=1$ "인 "1"이라는 코드 값으로 변경할 수 있다.
- [0070] 이와 동시에 전치 행렬 선택부(114)는 상기 수학식 7의 연산에 따라, 상기 제2 벡터 b 를 구성하는 $(n-k)$ 개의 성분 전체인 b_e 에 대해 b_e 와 $(n-k)$ 개의 r_1 의 성분들을 "+"연산(논리 연산임)함으로써, $b_e + r_1$ 으로 대체할 수 있다. 여기서, 상기 제2 벡터 b 를 구성하는 $(n-k)$ 의 성분은 m '의 성분으로 구성되어 있기 때문에 전치 행렬 선택부(114)는 상기 제2 벡터 b 를 구성하는 m '의 성분들을 $m' + r_1$ 으로 대체할 수 있다.
- [0071] 이러한 방식으로 "0"의 코드 값으로 구성된 상기 제1 벡터 a 와 m '의 코드 값으로 구성된 상기 제2 벡터 b 가 열 방향으로 나열됨으로써 생성된 상기 벡터 z 의 초기값은 전치 행렬 선택부(114)에 의해서, "0"의 코드 값으로 구성된 상기 제1 벡터 a 가 a_1 이 $1-a_1$ 로 대체된 벡터로 변경되고, m '의 성분으로 구성된 상기 제2 벡터 b 가 $m' + r_1$ 으로 대체된 벡터로 변경될 수 있다.
- [0072] 이렇게 상기 벡터 z 가 새롭게 변경 완료되면, 전치 행렬 선택부(114)는 상기 새롭게 변경된 벡터 z 의 해밍 무게가 상기 기준치 이하로 연산되는지 확인한 후 상기 새롭게 변경된 벡터 z 의 해밍 무게가 상기 기준치 이하로 연산된다면, 상기 새롭게 변경된 벡터 z 의 전치 행렬인 z^T 를 상기 z_s^T 로 선택할 수 있다.
- [0073] 여기서, 상기 새롭게 변경된 벡터 z 의 전치 행렬인 z^T 는 행렬의 대수적 특성에 따라 $H z^T = m'$ 의 조건을 만족하게 된다.
- [0074] 지금까지 설명한 방식으로, 전치 행렬 선택부(114)는 i 를 1부터 k 까지 변경하면서, " $r_i * m' \geq 2$ "의 조건을 만족하는 경우, 상기 수학식 7에 따라 상기 벡터 z 의 성분들을 변경하여 상기 벡터 z 를 새롭게 갱신하고, 새롭게 갱신된 벡터 z 의 해밍 무게가 상기 기준치 이하가 되는지 확인해서, 해밍 무게가 상기 기준치 이하로 연산되는 벡터 z 가 발견되는 경우, 상기 벡터 z 의 갱신을 중단하고, 해밍 무게가 상기 기준치 이하로 연산되는 벡터 z 의 전치 행렬인 z^T 를 상기 z_s^T 로 선택할 수 있다.
- [0075] 이렇게, 벡터 z 의 해밍 무게가 기준치 이하가 될 것이라는 조건이 추가됨에 따라 상기 z_s^T 가 선택되어, 전자 서명부(115)에 의해 상기 전자 서명 값 $P^{-1} z_s^T$ 가 연산되고, 전자 서명 전송부(116)에 의해 데이터 수신 장치(120)로 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1} z_s^T$ 가 전송되면, 데이터 수신 장치(120)는 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 기준치 이하인지 여부를 우선 확인할 수 있다.
- [0076] 여기서, z_s^T 는 상기 벡터 z 의 전치 행렬이고, P^{-1} 은 상기 순열 행렬 P 의 역행렬이기 때문에 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게는 상기 벡터 z 의 해밍 무게와 동일하다.
- [0077] 이로 인해, 만약, 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 기준치를 초과한다면, 상기 전자 서명 값 $P^{-1} z_s^T$ 가 정상적으로 생성된 전자 서명 값으로 볼 수 없기 때문에 데이터 수신 장치(120)는 상기 전자 서명 값 $P^{-1} z_s^T$

z_s^{-1T} 에 대한 검증이 실패한 것으로 판단할 수 있다.

[0078] 하지만, 상기 전자 서명 값 $P^{-1}z_s^{-1T}$ 의 해밍 무게가 상기 기준치 이하인 것으로 확인되면, 데이터 수신 장치(120)는 상기 평문 메시지 m 을 상기 메모리 상에 저장되어 있는 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 상기 해시 값 $h(m)$ 을 연산한 후 상기 검증키 K_{pub} 에 상기 전자 서명 값 $P^{-1}z_s^{-1T}$ 을 곱한 결과 값인 $K_{pub}P^{-1}z_s^{-1T}$ 가 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 와 일치하는지 비교하여 상기 $K_{pub}P^{-1}z_s^{-1T}$ 가 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^{-1T}$ 에 대한 검증을 성공으로 판단할 수 있다.

[0079] 지금까지 설명한 본 발명의 실시예에서는 데이터 보안이 강화된 전자 서명 장치(110)가 상기 전자 서명 값 $P^{-1}z_s^{-1T}$ 와 상기 평문 메시지 m 을 데이터 수신 장치(120)로 전송하는 예에 대해 설명하였지만, 본 발명의 다른 실시예에 따르면, 데이터 보안이 강화된 전자 서명 장치(110)는 상기 전자 서명 값 $P^{-1}z_s^{-1T}$ 의 생성이 완료되면, 상기 전자 서명 값 $P^{-1}z_s^{-1T}$ 와 상기 평문 메시지 m 을 데이터 수신 장치(120)로 전송하는 것이 아니라, 상기 전자 서명 값 $P^{-1}z_s^{-1T}$ 와 상기 해시 값 $h(m)$ 을 데이터 수신 장치(120)로 전송하도록 구성될 수 있다.

[0080] 이때, 데이터 수신 장치(120)는 상기 전자 서명 값 $P^{-1}z_s^{-1T}$ 와 상기 해시 값 $h(m)$ 이 수신되면, 상기 메모리 상에 저장되어 있는 K_{pub} 에 상기 전자 서명 값 $P^{-1}z_s^{-1T}$ 을 곱한 결과 값인 $K_{pub}P^{-1}z_s^{-1T}$ 가 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 와 일치하는지 여부를 바로 비교함으로써, 상기 전자 서명 값 $P^{-1}z_s^{-1T}$ 에 대한 검증을 완료할 수 있다.

[0081] 도 2는 본 발명의 일실시예에 따른 데이터 보안이 강화된 전자 서명 방법을 도시한 순서도이다.

[0082] 단계(S210)에서는 "1"과 "0"의 코드 값을 임의의 성분들로 포함하는 $(n-k) \times k - n$ 과 k 는 자연수이고 n 은 k 보다 큼 - 크기의 제1 부분 행렬 R 과 $(n-k) \times (n-k)$ 의 크기를 갖는 제2 부분 행렬 I - 상기 제2 부분 행렬 I 는 $(n-k) \times (n-k)$ 의 크기를 갖는 단위 행렬임 - 가 열 방향으로 조합된 제1 행렬 H 를 생성한다.

[0083] 단계(S220)에서는 "1"과 "0"의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q 와 "1"과 "0"의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 를 생성한다.

[0084] 단계(S230)에서는 데이터 수신 장치로 전송할 평문 메시지 m 을 선정된 해시 함수인 $h(x)$ 에 입력으로 인가하여 해시 값 $h(m)$ - 상기 해시 값 $h(m)$ 은 크기가 $(n-k)$ 인 벡터로 $1 \times (n-k)$ 의 크기를 갖는 행렬로 표현됨 - 을 연산하고, 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 변형 메시지 $m' - m' = Q^{-1}h(m)^T$ 임 - 을 연산한다.

[0085] 단계(S240)에서는 $Hz^T = m' - z^T$ 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐 - 을 만족하는 하나 이상의 z^T 들 중 어느 하나인 z_s^T 를 선택한다.

[0086] 단계(S250)에서는 상기 z_s^T 의 좌측 변에 상기 순열 행렬 P 의 역행렬인 P^{-1} 을 곱하여 $P^{-1}z_s^T$ 를 연산함으로써, 상기 연산된 $P^{-1}z_s^T$ 을 상기 평문 메시지 m 에 대한 전자 서명 값으로 생성한다.

[0087] 단계(S260)에서는 상기 데이터 수신 장치에 대해 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1}z_s^T$ 을 전송한다.

[0088] 이때, 본 발명의 일실시예에 따르면, 단계(S240)에서는 $Hz^T = m'$ 을 만족하는 하나 이상의 z^T 들 중 상기 벡터 z 의 해밍 무게가 기준치 이하로 연산되는 z^T 들로부터 상기 z_s^T 를 선택할 수 있다.

[0089] 이때, 본 발명의 일실시예에 따르면, 단계(S240)에서는 크기가 k 인 "0"의 코드 값으로만 구성된 제1 벡터 a 와 크기가 $(n-k)$ 인 m' 의 성분들로 구성된 제2 벡터 b 를 열 방향으로 나열하여 크기가 n 인 상기 벡터 z 의 초기값을

생성한 후 상기 벡터 z 의 초기값으로부터 상기 제1 부분 행렬 R 의 각 열의 성분 값들에 기초하여 상기 제1 벡터 a 와 상기 제2 벡터 b 의 성분 값을 조정하면서 $H z^T = m'$ 을 만족하는 z^T 들을 하나씩 연산하고, 상기 하나씩 연산되는 z^T 들 중 상기 벡터 z 의 해밍 무게가 상기 기준치 이하로 연산되는 z^T 가 발견되는 경우, 상기 발견된 z^T 를 상기 z_s^T 로 선택할 수 있다.

[0090] 또한, 본 발명의 일실시예에 따르면, 상기 데이터 수신 장치는 메모리 상에 상기 스크램블링 행렬 Q 와 상기 제1 행렬 H 및 상기 순열 행렬 P 가 곱해진 행렬인 $(n-k) \times n$ 크기를 갖는 $K_{pub} - K_{pub} = QHP^T$ 를 전자 서명에 대한 검증키로 저장하고 있고, 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1} z_s^T$ 가 수신되면, 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 기준치 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 기준치 이하인 것으로 확인되면, 상기 검증키 K_{pub} 에 기초하여 상기 전자 서명 값 $P^{-1} z_s^T$ 에 대한 검증을 수행할 수 있다.

[0091] 이때, 본 발명의 일실시예에 따르면, 상기 데이터 수신 장치는 상기 메모리 상에 상기 해시 함수 $h(x)$ 를 추가로 저장하고 있고, 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1} z_s^T$ 가 수신되면, 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 기준치 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 기준치 이하인 것으로 확인되면, 상기 평문 메시지 m 을 상기 메모리 상에 저장되어 있는 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 상기 해시 값 $h(m)$ 을 연산한 후 상기 검증키 K_{pub} 에 상기 전자 서명 값 $P^{-1} z_s^T$ 을 곱한 결과 값인 $K_{pub} P^{-1} z_s^T$ 가 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 와 일치하는지 비교하여 상기 $K_{pub} P^{-1} z_s^T$ 가 상기 해시 값 $h(m)$ 의 전치 행렬인 $h(m)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1} z_s^T$ 에 대한 검증을 성공으로 판단할 수 있다.

[0092] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 데이터 보안이 강화된 전자 서명 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 데이터 보안이 강화된 전자 서명 방법은 도 1을 이용하여 설명한 데이터 보안이 강화된 전자 서명 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0093] 본 발명의 일실시예에 따른 데이터 보안이 강화된 전자 서명 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0094] 또한, 본 발명의 일실시예에 따른 데이터 보안이 강화된 전자 서명 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0095] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0096] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

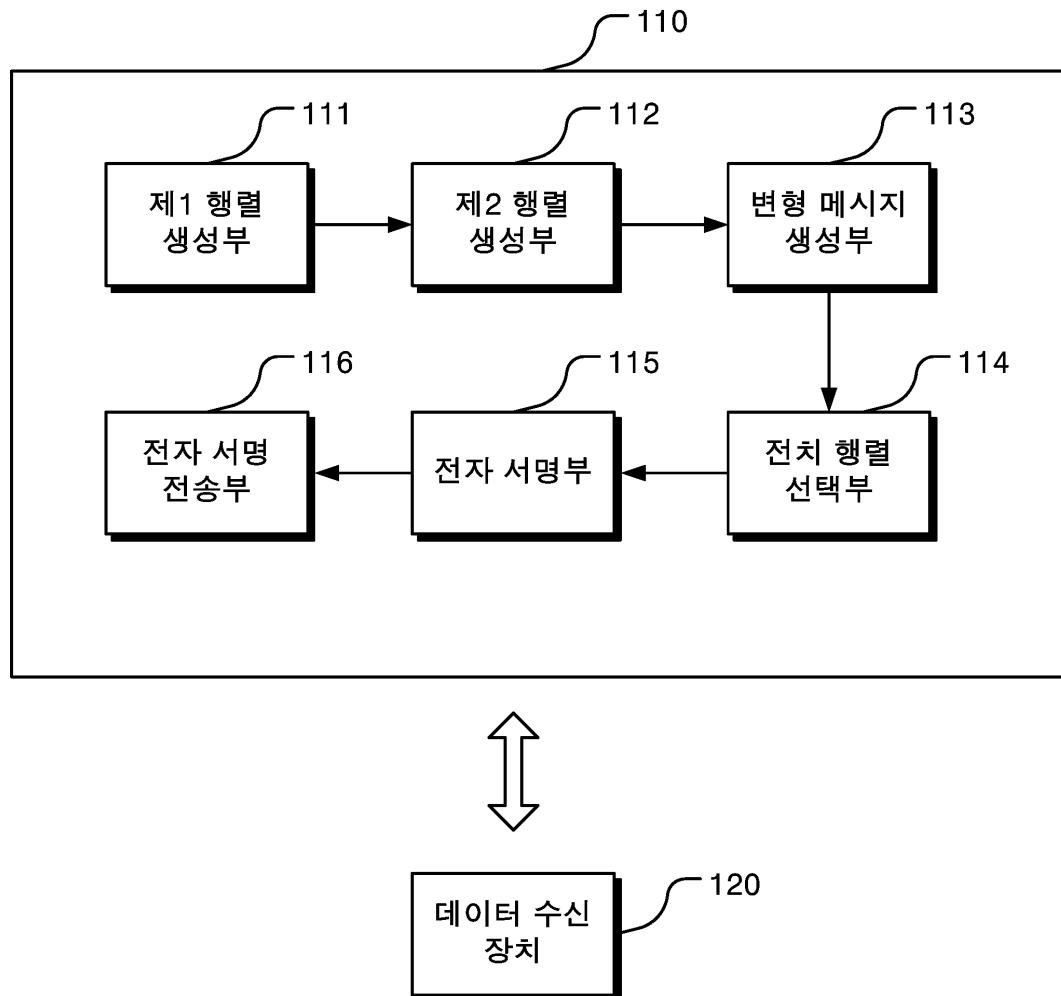
부호의 설명

[0097]

110: 데이터 보안이 강화된 전자 서명 장치
 111: 제1 행렬 생성부 112: 제2 행렬 생성부
 113: 변형 메시지 생성부 114: 전치 행렬 선택부
 115: 전자 서명부 116: 전자 서명 전송부
 120: 데이터 수신 장치

도면

도면1



도면2

