



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0058834
(43) 공개일자 2019년05월30일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H03M 13/13 (2006.01)
H04L 1/00 (2006.01) H04L 9/06 (2006.01)
(52) CPC특허분류
H04L 9/3247 (2013.01)
H03M 13/136 (2013.01)
(21) 출원번호 10-2017-0156149
(22) 출원일자 2017년11월22일
심사청구일자 2017년11월22일

(71) 출원인
서울대학교산학협력단
서울특별시 관악구 관악로 1 (신림동)
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
노중선
서울특별시 강남구 광평로10길 15 상록수아파트 109동 406호
김영식
광주광역시 서구 풍암2로 66 금호2차아파트 201동 1005호
이위직
서울특별시 관악구 관악로17길 8, 1102호
(74) 대리인
김효성

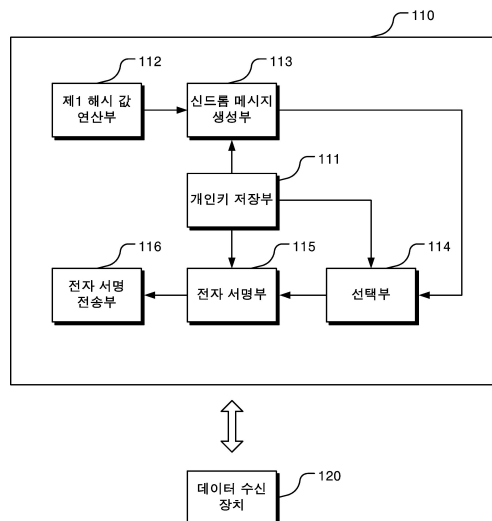
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치 및 방법

(57) 요약

패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치 및 방법이 개시된다. 본 발명은 데이터 수신 장치에 전송할 메시지를 기초로 임의의 신드롬 메시지를 생성한 후 패리티 검사 행렬을 이용하여 상기 신드롬 메시지에서 전자 서명용 오류 벡터를 검출한 후 상기 전자 서명용 오류 벡터를 기초로 전자 서명 값을 생성하여 상기 데이터 수신 장치로 전송함으로써, 기존의 비대칭키 기반의 전자 서명 기법과 전혀 다른 알고리즘에 따른 부인 방지 기능을 제공할 수 있다.

대표도 - 도1



(52) CPC특허분류

H04L 1/0061 (2013.01)

H04L 9/0618 (2013.01)

H04L 9/0643 (2013.01)

H04L 9/3236 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711054914

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보보호핵심원천기술개발

연구과제명 (창조씨앗 2단계) IoT 및 클라우드 컴퓨팅을 위한 경량 포스트 양자 암호 시스템 연구

기 여 율 1/1

주관기관 서울대학교 산학협력단

연구기간 2017.01.01 ~ 2017.12.31

명세서

청구범위

청구항 1

리드-물러(Reed-Muller: RM) 코드로 구성된 $(n-k) \times n$ - n 과 k 는 자연수이고 n 은 k 보다 큼 - 크기의 선형 부호에 대한 패리티 검사 행렬 H , '1'과 '0'의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스캐램블링 행렬 Q 및 '1'과 '0'의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 가 저장되어 있는 개인키 저장부;

데이터 수신 장치로 전송할 평문 메시지 m 을 선정된(predetermined) 해시 함수인 $h(x)$ - 상기 해시 함수 $h(x)$ 는 입력 값을 $(n-k)$ 비트 크기의 출력 값으로 변환시키는 일방향 함수임 - 에 입력으로 인가하여 제1 해시 값 $h(m)$ 을 연산하는 제1 해시 값 연산부;

상기 제1 해시 값 $h(m)$ 의 연산이 완료되면, 변수 i - 상기 변수 i 는 '0'이상인 정수임 - 를 '0'부터 '1'씩 증가시키면서, 상기 제1 해시 값 $h(m)$ 에 상기 변수 i 에 대한 비트 값을 연결한 결과 값 $h(m)||i$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 제2 해시 값인 $h(h(m)||i)$ 을 연산하고, 상기 제2 해시 값인 $h(h(m)||i)$ 의 전치 행렬인 $h(h(m)||i)^T$ 의 좌측 변에 상기 스캐램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 신드롬 메시지 s_i - $s_i = Q^{-1}h(h(m)||i)^T$ 임 - 를 생성하는 신드롬 메시지 생성부;

상기 변수 i 가 '0'을 시작으로 해서 '1'씩 증가되면서 상기 신드롬 메시지 s_i 가 생성될 때마다, 각 변수 i 에서의 상기 신드롬 메시지 s_i 에 대해 상기 패리티 검사 행렬 H 를 기초로 완전 복호화(Complete Decoding)를 수행하여 $H z^T = s_i$ - z 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐 - 를 만족하는 z^T 를 연산한 후 z^T 의 해밍 무게(Hamming Weight)가 선정된 해밍 무게인 w 이하로 연산되는 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 연산된 z^T 를 서명용 오류 벡터 z_s^T 로 선택하는 선택부;

상기 서명용 오류 벡터 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 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 를 전송하는 전자 서명 전송부

를 포함하는 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치.

청구항 2

제1항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 스캐램블링 행렬 Q 와 상기 패리티 검사 행렬 H 및 상기 순열 행렬 P 가 곱해진 행렬인 $(n-k) \times n$ 크기를 갖는 $K_{pub} = QHP$ 임 - 를 전자 서명에 대한 검증키로 저장하고 있고, 상기 평문 메시지 m

과 상기 전자 서명 값 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게

가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 검증키 K_{pub} 와 상기 서명용 변수 i_s 에 기초하여 상기 전자 서

명 값 $P^{-1}z_s^T$ 에 대한 검증을 수행하는 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치.

청구항 3

제2항에 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 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 평문 메시지 m 을 상기 메모리 상에 저장되어 있는 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 상기 제1 해시 값 $h(m)$ 을 연산하고,

상기 제1 해시 값 $h(m)$ 이 연산되면, 상기 제1 해시 값 $h(m)$ 에 상기 서명용 변수 i_s 에 대한 비트 값을 연접한 결과 값 $h(m)|i_s$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 검증용 해시 값인 $h(h(m)|i_s)$ 을 연산하며,

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 검증용 해시 값인 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는지 비교하여 상기 $K_{pub}P^{-1}z_s^T$ 가 상기 검증용 해시 값 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 성공으로 판단하는 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치.

청구항 4

리드-물러(Reed-Muller: RM) 코드로 구성된 $(n-k) \times n$ 과 k 는 자연수이고 n 은 k 보다 큰 크기의 선형 부호에 대한 패리티 검사 행렬 H , 상기 패리티 검사 행렬 H 에서 복수의 선정된(predetermined) 제1 행들에 위치하는 성분들이 랜덤한 코드 값으로 치환되고, 복수의 선정된 제2 열들에 위치하는 성분들이 '0'의 코드 값으로 치환된 변형 패리티 검사 행렬 H_1 , '1'과 '0'의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q 및 '1'과 '0'의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 가 저장되어 있는 개인키 저장부;

데이터 수신 장치로 전송할 평문 메시지 m 을 선정된 해시 함수인 $h(x)$ - 상기 해시 함수 $h(x)$ 는 입력 값을 $(n-k)$ 비트 크기의 출력 값으로 변환시키는 일방향 함수임 - 에 입력으로 인가하여 제1 해시 값 $h(m)$ 을 연산하는 제1 해시 값 연산부;

상기 제1 해시 값 $h(m)$ 의 연산이 완료되면, 변수 i - 상기 변수 i 는 '0'이상인 정수임 - 를 '0'부터 '1'씩 증가시키면서, 상기 제1 해시 값 $h(m)$ 에 상기 변수 i 에 대한 비트 값을 연접한 결과 값 $h(m)|i$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 제2 해시 값인 $h(h(m)|i)$ 을 연산하고, 상기 제2 해시 값인 $h(h(m)|i)$ 의 전치 행렬인 $h(h(m)|i)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 신드롬 메시지 s_i - $s_i = Q^{-1}h(h(m)|i)^T$ 임 - 를 생성하는 신드롬 메시지 생성부;

상기 변수 i 가 '0'을 시작으로 해서 '1'씩 증가되면서 상기 신드롬 메시지 s_i 가 생성될 때마다, 각 변수 i 에서의 상기 신드롬 메시지 s_i 에 대해 상기 패리티 검사 행렬 H 를 기초로 완전 복호화(Complete Decoding)를 수행하여 $Hz^T = s_i$ - z 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐 - 를 만족하는 z^T 를 연산하고, 상

기 변형 패리티 검사 행렬 H_t 에서 상기 복수의 선정된 제1 행들과 상기 복수의 선정된 제2 열들에 위치하는 코드 값에 기초하여 각 변수 i 마다 연산되는 z^T 의 성분을 조작함으로써, $H_t z_t^T = s_i$ 를 만족하는 z_t^T 를 검출한 후 z_t^T 의 해밍 무게(Hamming Weight)가 선정된 해밍 무게인 w 이하로 검출되는 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 검출된 z_t^T 를 서명용 오류 벡터 z_s^T 로 선택하는 선택부;

상기 서명용 오류 벡터 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 $P^{-1} z_s^T$ 및 상기 서명용 변수 i_s 를 전송하는 전자 서명 전송부를 포함하는 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치.

청구항 5

제4항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 스크램블링 행렬 Q 와 상기 변형 패리티 검사 행렬 H_t 및 상기 순열 행렬 P 가 곱해진 행렬인 $(n-k) \times n$ 크기를 갖는 $K_{pub} = QH_tP$ 임 - 를 전자 서명에 대한 검증키로 저장하고 있고, 상기 평문

메시지 m 과 상기 전자 서명 값 $P^{-1} z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1} z_s^T$ 의

해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 검증키 K_{pub} 와 상기 서명용 변수 i_s 에 기초하여 상기

전자 서명 값 $P^{-1} z_s^T$ 에 대한 검증을 수행하는 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치.

청구항 6

제5항에 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 $P^{-1} z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 선정된 해밍

무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 평문 메시지 m 을 상기 메모리 상에 저장되어 있는 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 상기 제1 해시 값 $h(m)$ 을 연산하고,

상기 제1 해시 값 $h(m)$ 이 연산되면, 상기 제1 해시 값 $h(m)$ 에 상기 서명용 변수 i_s 에 대한 비트 값을 연결한 결과 값 $h(m)|i_s$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 검증용 해시 값인 $h(h(m)|i_s)$ 을 연산하며,

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 검증용 해시 값인 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는지 비교하여 상기 $K_{pub}P^{-1} z_s^T$ 가 상기 검증용 해

시 값 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 성공으로 판단하는 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치.

청구항 7

리드-물러(Reed-Muller: RM) 코드로 구성된 $(n-k) \times n$ 과 k 는 자연수이고 n 은 k 보다 큰 크기의 선형 부호에 대한 패리티 검사 행렬 H , '1'과 '0'의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스캐램블링 행렬 Q 및 '1'과 '0'의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 가 저장되어 있는 개인키 저장부를 유지하는 단계;

데이터 수신 장치로 전송할 평문 메시지 m 을 선정된(predetermined) 해시 함수인 $h(x)$ - 상기 해시 함수 $h(x)$ 는 입력 값을 $(n-k)$ 비트 크기의 출력 값으로 변환시키는 일방향 함수임 - 에 입력으로 인가하여 제1 해시 값 $h(m)$ 을 연산하는 단계;

상기 제1 해시 값 $h(m)$ 의 연산이 완료되면, 변수 i - 상기 변수 i 는 '0'이상인 정수임 - 를 '0'부터 '1'씩 증가시키면서, 상기 제1 해시 값 $h(m)$ 에 상기 변수 i 에 대한 비트 값을 연결한 결과 값 $h(m)|i$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 제2 해시 값인 $h(h(m)|i)$ 을 연산하고, 상기 제2 해시 값인 $h(h(m)|i)$ 의 전치 행렬인 $h(h(m)|i)^T$ 의 좌측 변에 상기 스캐램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 신드롬 메시지 s_i - $s_i = Q^{-1}h(h(m)|i)^T$ 임 - 를 생성하는 단계;

상기 변수 i 가 '0'을 시작으로 해서 '1'씩 증가되면서 상기 신드롬 메시지 s_i 가 생성될 때마다, 각 변수 i 에서의 상기 신드롬 메시지 s_i 에 대해 상기 패리티 검사 행렬 H 를 기초로 완전 복호화(Complete Decoding)를 수행하여 $H z^T = s_i$ - z 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐 - 를 만족하는 z^T 를 연산한 후 z^T 의 해밍 무게(Hamming Weight)가 선정된 해밍 무게인 w 이하로 연산되는 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 연산된 z^T 를 서명용 오류 벡터 z_s^T 로 선택하는 단계;

상기 서명용 오류 벡터 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 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 를 전송하는 단계

를 포함하는 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법.

청구항 8

제7항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 스캐램블링 행렬 Q 와 상기 패리티 검사 행렬 H 및 상기 순열 행렬 P 가 곱해진 행렬인 $(n-k) \times n$ 크기를 갖는 K_{pub} - $K_{pub} = QHP$ 임 - 를 전자 서명에 대한 검증키로 저장하고 있고, 상기 평문 메시지 m

과 상기 전자 서명 값 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게

가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선

정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 검증키 K_{pub} 와 상기 서명용 변수 i_s 에 기초하여 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 수행하는 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법.

청구항 9

제8항에 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 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 평문 메시지 m 을 상기 메모리 상에 저장되어 있는 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 상기 제1 해시 값 $h(m)$ 을 연산하고,

상기 제1 해시 값 $h(m)$ 이 연산되면, 상기 제1 해시 값 $h(m)$ 에 상기 서명용 변수 i_s 에 대한 비트 값을 연접한 결과 값 $h(m)|i_s$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 검증용 해시 값인 $h(h(m)|i_s)$ 을 연산하며,

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 검증용 해시 값인 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는지 비교하여 상기 $K_{pub}P^{-1}z_s^T$ 가 상기 검증용 해시 값 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 성공으로 판단하는 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법.

청구항 10

리드-물러(Reed-Muller: RM) 코드로 구성된 $(n-k) \times n - n$ 과 k 는 자연수이고 n 은 k 보다 큼 - 크기의 선형 부호에 대한 패리티 검사 행렬 H , 상기 패리티 검사 행렬 H 에서 복수의 선정된(predetermined) 제1 행들에 위치하는 성분들이 랜덤한 코드 값으로 치환되고, 복수의 선정된 제2 열들에 위치하는 성분들이 '0'의 코드 값으로 치환된 변형 패리티 검사 행렬 H_t , '1'과 '0'의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q 및 '1'과 '0'의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 가 저장되어 있는 개인키 저장부를 유지하는 단계;

데이터 수신 장치로 전송할 평문 메시지 m 을 선정된 해시 함수인 $h(x)$ - 상기 해시 함수 $h(x)$ 는 입력 값을 $(n-k)$ 비트 크기의 출력 값으로 변환시키는 일방향 함수임 - 에 입력으로 인가하여 제1 해시 값 $h(m)$ 을 연산하는 단계;

상기 제1 해시 값 $h(m)$ 의 연산이 완료되면, 변수 i - 상기 변수 i 는 '0'이상인 정수임 - 를 '0'부터 '1'씩 증가시키면서, 상기 제1 해시 값 $h(m)$ 에 상기 변수 i 에 대한 비트 값을 연접한 결과 값 $h(m)|i$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 제2 해시 값인 $h(h(m)|i)$ 을 연산하고, 상기 제2 해시 값인 $h(h(m)|i)$ 의 전치 행렬인 $h(h(m)|i)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 신드롬 메시지 s_i - $s_i = Q^{-1}h(h(m)|i)^T$ 임 - 를 생성하는 단계;

상기 변수 i 가 '0'을 시작으로 해서 '1'씩 증가되면서 상기 신드롬 메시지 s_i 가 생성될 때마다, 각 변수 i 에서의 상기 신드롬 메시지 s_i 에 대해 상기 패리티 검사 행렬 H 를 기초로 완전 복호화(Complete Decoding)를 수행하

여 $H_z^T = s_i - z^T$ 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가진 $-$ 를 만족하는 z^T 를 연산하고, 상기 변형 패리티 검사 행렬 H_t 에서 상기 복수의 선정된 제1 행들과 상기 복수의 선정된 제2 열들에 위치하는 코드 값에 기초하여 각 변수 i 마다 연산되는 z^T 의 성분을 조작함으로써, $H_t z_t^T = s_i$ 를 만족하는 z_t^T 를 검출한 후 z_t^T 의 해밍 무게(Hamming Weight)가 선정된 해밍 무게인 w 이하로 검출되는 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 검출된 z_t^T 를 서명용 오류 벡터 z_s^T 로 선택하는 단계;

상기 서명용 오류 벡터 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 $P^{-1} z_s^T$ 및 상기 서명용 변수 i_s 를 전송하는 단계

를 포함하는 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법.

청구항 11

제10항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 스크램블링 행렬 Q 와 상기 변형 패리티 검사 행렬 H_t 및 상기 순열 행렬 P 가 곱해진 행렬인 $(n-k) \times n$ 크기를 갖는 $K_{pub} = QH_t P$ 임 - 를 전자 서명에 대한 검증키로 저장하고 있고, 상기 평문

메시지 m 과 상기 전자 서명 값 $P^{-1} z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1} z_s^T$ 의

해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 검증키 K_{pub} 와 상기 서명용 변수 i_s 에 기초하여 상기

전자 서명 값 $P^{-1} z_s^T$ 에 대한 검증을 수행하는 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법.

청구항 12

제11항에 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 $P^{-1} z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 선정된 해밍

무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1} z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 평문 메시지 m 을 상기 메모리 상에 저장되어 있는 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 상기 제1 해시 값 $h(m)$ 을 연산하고,

상기 제1 해시 값 $h(m)$ 이 연산되면, 상기 제1 해시 값 $h(m)$ 에 상기 서명용 변수 i_s 에 대한 비트 값을 연결한 결과 값 $h(m)|i_s$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 검증용 해시 값인 $h(h(m)|i_s)$ 을 연산하며,

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 검증용 해시 값인

$h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는지 비교하여 상기 $K_{pub}P^{-1}z_s^T$ 가 상기 검증용 해시 값 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 성공으로 판단하는 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법.

청구항 13

제7항 내지 제12항 중 어느 한 항의 방법을 컴퓨터로 하여금 수행하도록 하는 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 14

제7항 내지 제12항 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 बैंक 서비스나 결제 시스템의 도입이 활발하게 이루어지고 있다.

[0003] 이러한 온라인 बैंक 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 बैंक 서비스를 통해서 B라는 사용자에게 계좌 이체를 한다고 했을 때, 온라인 बैंक 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 बैंक 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 값에 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 데이터 수신 장치에 전송할 메시지를 기초로 임의의 신드롬 메시지를 생성한 후 패리티 검사 행렬을 이용하여 상기 신드롬 메시지에서 전자 서명용 오류 벡터를 검출한 후 상기 전자 서명용 오류 벡터를 기초로 전자 서명 값을 생성하여 상기 데이터 수신 장치로 전송함으로써, 기존의 비대칭키 기반의 전자 서명 기법과 전혀 다른 알고리즘에 따른 부인 방지 기능을 제공하고자 한다.

과제의 해결 수단

[0012] 본 발명의 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치는 리드-물러(Reed-Muller: RM) 코드로 구성된 $(n-k) \times n - n$ 과 k 는 자연수이고 n 은 k 보다 큼 - 크기의 선형 부호에 대한 패리티 검사 행렬 H , '1'과 '0'의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q 및 '1'과 '0'의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 가 저장되어 있는 개인키 저장부, 데이터 수신 장치로 전송할 평문 메시지 m 을 선정된(predetermined) 해시 함수인 $h(x)$ - 상기 해시 함수 $h(x)$ 는 입력 값을 $(n-k)$ 비트 크기의 출력 값으로 변환시키는 일방향 함수임 - 에 입력으로 인가하여 제1 해시 값 $h(m)$ 을 연산하는 제1 해시 값 연산부, 상기 제1 해시 값 $h(m)$ 의 연산이 완료되면, 변수 i - 상기 변수 i 는 '0'이상인 정수임 - 를 '0'부터 '1'씩 증가시키면서, 상기 제1 해시 값 $h(m)$ 에 상기 변수 i 에 대한 비트 값을 연결한 결과 값 $h(m)|i$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 제2 해시 값인 $h(h(m)|i)$ 를 연산하고, 상기 제2 해시 값인 $h(h(m)|i)$ 의 전치 행렬인 $h(h(m)|i)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 신드롬 메시지 s_i - $s_i = Q^{-1}h(h(m)|i)^T$ 임 - 를 생성하는 신드롬 메시지 생성부, 상기 변수 i 가 '0'을 시작으로 해서 '1'씩 증가되면서 상기 신드롬 메시지 s_i 가 생성될 때마다, 각 변수 i 에서의 상기 신드롬 메시지 s_i 에 대해 상기 패리티 검사 행렬 H 를 기초로 완전 복호화(Complete Decoding)를 수행하여 $Hs_i^T = z_i$ - z_i 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐 - 를 만족하는 z^T 를 연산한 후 z^T 의 해밍 무게(Hamming Weight)가 선정된 해밍 무게인 w 이하로 연산되는 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 연산된 z^T 를 서명용 오류 벡터 z_s^T 로 선택하는 선택부, 상기 서명용 오류 벡터 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 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 를 전송하는 전자 서명 전송부를 포함한다.

[0013] 또한, 본 발명의 다른 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치는 RM 코드로 구성된 $(n-k) \times n - n$ 과 k 는 자연수이고 n 은 k 보다 큼 - 크기의 선형 부호에 대한 패리티 검사 행렬 H , 상기 패리티 검사 행렬 H 에서 복수의 선정된 제1 행들에 위치하는 성분들이 랜덤한 코드 값으로 치환되고, 복수의 선정된 제2 열들에 위치하는 성분들이 '0'의 코드 값으로 치환된 변형 패리티 검사 행렬 H_t , '1'과 '0'의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q 및 '1'과 '0'의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 가 저장되어 있는 개인키 저장부, 데이터 수신 장치로 전송할 평문 메시지 m 을 선정된 해시 함수인 $h(x)$ - 상기 해시 함수 $h(x)$ 는 입력 값을 $(n-k)$ 비트 크기의 출력 값으로 변환시키는 일방향 함수임 - 에 입력으로 인가하여 제1 해시 값 $h(m)$ 을 연산하는 제1 해시 값 연산부, 상기 제1 해시 값 $h(m)$ 의 연산이 완료되면, 변수 i - 상기 변수 i 는 '0'이상인 정수임 - 를 '0'부터 '1'씩 증가시키면서, 상기 제1 해시 값 $h(m)$ 에 상기 변수 i 에 대한 비트 값을 연결한 결과 값 $h(m)|i$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 제2 해시 값인 $h(h(m)|i)$ 를 연산하고, 상기 제2 해시 값인 $h(h(m)|i)$ 의 전치 행렬인

$h(h(m)|i)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 신드롬 메시지 $s_i - s_i = Q^{-1}h(h(m)|i)^T$ 임 - 를 생성하는 신드롬 메시지 생성부, 상기 변수 i 가 '0'을 시작으로 해서 '1'씩 증가되면서 상기 신드롬 메시지 s_i 가 생성될 때마다, 각 변수 i 에서의 상기 신드롬 메시지 s_i 에 대해 상기 패리티 검사 행렬 H 를 기초로 완전 복호화를 수행하여 $H z^T = s_i - z^T$ 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐 - 를 만족하는 z^T 를 연산하고, 상기 변형 패리티 검사 행렬 H_t 에서 상기 복수의 선정된 제1 행들과 상기 복수의 선정된 제2 열들에 위치하는 코드 값에 기초하여 각 변수 i 마다 연산되는 z^T 의 성분을 조합함으로써, $H_t z_t^T = s_i$ 를 만족하는 z_t^T 를 검출한 후 z_t^T 의 해밍 무게가 선정된 해밍 무게인 w 이하로 검출되는 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 검출된 z_t^T 를 서명용 오류 벡터 z_s^T 로 선택하는 선택부, 상기 서명용 오류 벡터 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 $P^{-1} z_s^T$ 및 상기 서명용 변수 i_s 를 전송하는 전자 서명 전송부를 포함한다.

[0014] 또한, 본 발명의 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법은 RM 코드로 구성된 $(n-k) \times n - n$ 과 k 는 자연수이고 n 은 k 보다 큼 - 크기의 선형 부호에 대한 패리티 검사 행렬 H , '1'과 '0'의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q 및 '1'과 '0'의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 가 저장되어 있는 개인키 저장부를 유지하는 단계, 데이터 수신 장치로 전송할 평문 메시지 m 을 선정된 해시 함수인 $h(x)$ - 상기 해시 함수 $h(x)$ 는 입력 값을 $(n-k)$ 비트 크기의 출력 값으로 변환시키는 일방향 함수임 - 에 입력으로 인가하여 제1 해시 값 $h(m)$ 을 연산하는 단계, 상기 제1 해시 값 $h(m)$ 의 연산이 완료되면, 변수 i - 상기 변수 i 는 '0'이상인 정수임 - 를 '0'부터 '1'씩 증가시키면서, 상기 제1 해시 값 $h(m)$ 에 상기 변수 i 에 대한 비트 값을 연접한 결과 값 $h(m)|i$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 제2 해시 값인 $h(h(m)|i)$ 을 연산하고, 상기 제2 해시 값인 $h(h(m)|i)$ 의 전치 행렬인 $h(h(m)|i)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 신드롬 메시지 $s_i - s_i = Q^{-1}h(h(m)|i)^T$ 임 - 를 생성하는 단계, 상기 변수 i 가 '0'을 시작으로 해서 '1'씩 증가되면서 상기 신드롬 메시지 s_i 가 생성될 때마다, 각 변수 i 에서의 상기 신드롬 메시지 s_i 에 대해 상기 패리티 검사 행렬 H 를 기초로 완전 복호화를 수행하여 $H z^T = s_i - z^T$ 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐 - 를 만족하는 z^T 를 연산한 후 z^T 의 해밍 무게가 선정된 해밍 무게인 w 이하로 연산되는 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 연산된 z^T 를 서명용 오류 벡터 z_s^T 로 선택하는 단계, 상기 서명용 오류 벡터 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 $P^{-1} z_s^T$ 및 상기 서명용 변수 i_s 를 전송하는 단계를 포함한다.

[0015] 또한, 본 발명의 다른 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법은 RM 코드로 구성된 $(n-k) \times n - n$ 과 k 는 자연수이고 n 은 k 보다 큼 - 크기의 선형 부호에 대한 패리티 검사 행렬 H , 상기 패리티 검사 행렬 H 에서 복수의 선정된 제1 행들에 위치하는 성분들이 랜덤한 코드 값으로 치환되고, 복수의 선정된 제2 열들에 위치하는 성분들이 '0'의 코드 값으로 치환된 변형 패리티 검사 행렬 H_t ,

'1'과 '0'의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q 및 '1'과 '0'의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 가 저장되어 있는 개인키 저장부를 유지하는 단계, 데이터 수신 장치로 전송할 평문 메시지 m 을 선정된 해시 함수인 $h(x)$ - 상기 해시 함수 $h(x)$ 는 입력 값을 $(n-k)$ 비트 크기의 출력 값으로 변환시키는 일방향 함수임 - 에 입력으로 인가하여 제1 해시 값 $h(m)$ 을 연산하는 단계, 상기 제1 해시 값 $h(m)$ 의 연산이 완료되면, 변수 i - 상기 변수 i 는 '0'이상인 정수임 - 를 '0'부터 '1'씩 증가시키면서, 상기 제1 해시 값 $h(m)$ 에 상기 변수 i 에 대한 비트 값을 연결한 결과 값 $h(m)||i$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 제2 해시 값인 $h(h(m)||i)$ 을 연산하고, 상기 제2 해시 값인 $h(h(m)||i)$ 의 전치 행렬인 $h(h(m)||i)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 신드롬 메시지 s_i - $s_i = Q^{-1}h(h(m)||i)^T$ 임 - 를 생성하는 단계, 상기 변수 i 가 '0'을 시작으로 해서 '1'씩 증가되면서 상기 신드롬 메시지 s_i 가 생성될 때마다, 각 변수 i 에서의 상기 신드롬 메시지 s_i 에 대해 상기 패리티 검사 행렬 H 를 기초로 완전 복호화를 수행하여 $H z^T = s_i - z^T$ 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐 - 를 만족하는 z^T 를 연산하고, 상기 변형 패리티 검사 행렬 H_t 에서 상기 복수의 선정된 제1 행들과 상기 복수의 선정된 제2 열들에 위치하는 코드 값에 기초하여 각 변수 i 마다 연산되는 z^T 의 성분을 조작함으로써, $H_t z_t^T = s_i$ 를 만족하는 z_t^T 를 검출한 후 z_t^T 의 해밍 무게가 선정된 해밍 무게인 w 이하로 검출되는 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 검출된 z_t^T 를 서명용 오류 벡터 z_s^T 로 선택하는 단계, 상기 서명용 오류 벡터 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 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 를 전송하는 단계를 포함한다.

발명의 효과

[0016] 본 발명은 데이터 수신 장치에 전송할 메시지를 기초로 임의의 신드롬 메시지를 생성한 후 패리티 검사 행렬을 이용하여 상기 신드롬 메시지로부터 전자 서명용 오류 벡터를 검출한 후 상기 전자 서명용 오류 벡터를 기초로 전자 서명 값을 생성하여 상기 데이터 수신 장치로 전송함으로써, 기존의 비대칭키 기반의 전자 서명 기법과 전혀 다른 알고리즘에 따른 부인 방지 기능을 제공할 수 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치의 구조를 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 변형 패리티 검사 행렬 H_t 의 형태에 대한 예시를 도시한 도면이다.

도 3은 본 발명의 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법을 도시한 순서도이다.

도 4는 본 발명의 또 다른 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 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 상

에서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 사람에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

- [0019] 도 1은 본 발명의 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치의 구조를 도시한 도면이다.
- [0020] 도 1을 참조하면, 본 발명의 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치(110)는 개인키 저장부(111), 제1 해시 값 연산부(112), 신드롬 메시지 생성부(113), 선택부(114), 전자 서명부(115) 및 전자 서명 전송부(116)를 포함한다.
- [0021] 개인키 저장부(111)에는 리드-몰러(Reed-Muller: RM) 코드로 구성된 $(n-k) \times n$ 크기의 선형 부호에 대한 패리티 검사 행렬 H , '1'과 '0'의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스캐램블링 행렬 Q 및 '1'과 '0'의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 가 저장되어 있다.
- [0022] 여기서, n 과 k 는 자연수이고 n 은 k 보다 큰 수이다.
- [0023] RM 코드는 오류 정정 코드로 사용되는 선형 코드를 의미하는 것으로, $RM(r, m)$ 으로 표현되는 RM 코드는 길이가 2^m 이고, m 개의 기본 코드를 가지게 되며, 상기 m 개의 기본 코드들 간의 곱을 갖는 코드 역시 RM의 기본 코드가 될 수 있다. 그리고, r 은 기본 코드들 간의 곱에 사용될 수 있는 기본 코드의 최대 개수를 의미한다. 예컨대, $m=4$, $r=4$ 라고 할 때, RM 코드의 길이는 16이 되고, 이때, 상기 RM 코드는 2^4 으로 표시되므로, 4개의 기본 코드 R_1, R_2, R_3, R_4 (각 기본 코드의 길이는 16임)를 가지게 된다. 이때, 4개의 기본 코드 R_1, R_2, R_3, R_4 간의 곱을 연산한 RM 코드 역시 기본 코드가 될 수 있다. 여기서, $r=4$ 이기 때문에 4개의 기본 코드 R_1, R_2, R_3, R_4 에 대해서는 또 다른 추가 기본 코드를 생성하기 위해서 상기 4개의 기본 코드들 간의 곱에 사용 가능한 최대 개수가 4개가 되기 때문에, 4개의 기본 코드 R_1, R_2, R_3, R_4 상호 간의 곱을 최대 4개까지 조합하여 연산함으로써, 추가적인 기본 코드들을 생성할 수 있다. 관련해서, $RM(4, 4)$ 에 대해서는 R_1, R_2, R_3, R_4 에 해당되는 4개의 기본 코드와 $R_1R_2, R_1R_3, R_1R_4, R_2R_3, R_2R_4, R_3R_4, R_1R_2R_3, R_1R_2R_4, R_1R_3R_4, R_2R_3R_4, R_1R_2R_3R_4$ 로 구성된 11개의 기본 코드를 생성할 수 있고, RM 코드의 특성상 비트 값이 모두 '1'로 구성된 코드도 기본 코드로 가져야 하기 때문에 결과적으로 총 16개의 기본 코드들이 생성될 수 있다. 이러한 RM 코드는 데이터 수신측으로 전송할 메시지를 부호어(codeword)로 인코딩하기 위한 생성 행렬을 구성하는데 사용될 수 있고, 데이터 수신측에 수신된 부호어에 오류가 발생하였는지 여부를 검증하기 위한 패리티 검사 행렬을 구성하는데 사용될 수 있다.
- [0024] 패리티 검사 행렬은 데이터 수신측에 수신된 부호어에 오류가 발생하였는지 여부를 검증하기 위한 행렬로 $k \times n$ 크기의 생성 행렬 G 가 있을 때, 이에 대응하는 패리티 검사 행렬을 'H'라고 하면, 상기 패리티 검사 행렬 H 의 크기는 $(n-k) \times n$ 이 되며, 상기 패리티 검사 행렬 H 와 상기 생성 행렬 G 사이에는 하기의 수학식 1과 같은 특성이 존재한다.

수학식 1

[0026] $GH^T = 0$

[0028] 여기서, H^T 는 패리티 검사 행렬 H 의 전치 행렬을 의미한다.

[0029] 만약, 데이터 전송측이 생성 행렬 G 를 이용해서 부호어 c 를 생성하여 데이터 수신측으로 전송함에 따라 데이터 수신측에 수신된 부호어를 'r'이라고 한다면, 상기 부호어 r 에 오류가 발생하지 않은 경우, 상기 부호어 r 에 대해서는 패리티 검사 행렬 H 와의 관계에서 하기의 수학식 2와 같은 특성이 존재한다.

수학식 2

$$Hr^T = Hc^T = 0$$

여기서, r^T 는 부호어 r 의 전치 행렬을 의미한다.

하지만, 데이터 전송측이 전송한 부호어 c 에 오류 e 가 발생하였다고 한다면, 데이터 수신측이 수신한 상기 부호어 r 은 ' $c+e$ '가 될 것이고, 이로 인해 패리티 검사 행렬 H 와 상기 부호어 r 사이에는 하기의 수학식 3과 같은 특성을 가지게 된다.

수학식 3

$$\begin{aligned} Hr^T &= H(c+e)^T \\ &= Hc^T + He^T \quad (Hc^T = 0 \text{ 이므로}) \\ &= He^T \\ &= s \end{aligned}$$

상기 수학식 3에서의 연산과 같이, 데이터 수신측에서는 패리티 검사 행렬을 이용해서 데이터 수신측에 수신된 데이터에 오류가 존재하는지 여부를 검출할 수 있다. 그리고, 상기 수학식 3에서 ' s '를 신드롬(Syndrome)이라고 한다.

패리티 검사 행렬 H 가 RM 코드로 구성되는 경우, 상기 수학식 3에서 표현한 신드롬 s 에 대해 상기 패리티 검사 행렬 H 를 기초로 한 완전 복호(Complete Decoding) 알고리즘을 이용하게 되면, $He^T = s$ 의 수식을 만족하는 복수의 e 들 중 해밍 무게(Hamming Weight)가 최소인 e 를 찾아낼 수 있다.

상기 완전 복호 알고리즘이란 $r \times n$ 크기의 패리티 검사 행렬과 신드롬 $s \in 0, 1^r$ 가 있을 때, $He^T = s$ 를 만족하는 e 들 중 해밍 무게가 최소인 e 를 찾아내는 복호화 알고리즘이다. 완전 복호 알고리즘을 이용하면, 데이터 전송측이 부호어를 생성하기 위해 사용한 생성 행렬에 지정되어 있는 오류 정정 능력을 초과하는 오류에 대해서도 복호가 가능하며, RM 코드의 복호 방법 중 하나인 채귀 복호는 완전 복호가 가능한 특징이 있다.

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

이렇게, 개인키 저장부(111) 상에 패리티 검사 행렬 H , 스크램블링 행렬 Q 및 순열 행렬 P 가 저장되어 있는 상태에서, 데이터 수신 장치(120)로 전송할 평문 메시지를 m 이라고 한다면, 제1 해시 값 연산부(112)는 상기 평문 메시지 m 을 선정된(predetermined) 해시 함수인 $h(x)$ 에 입력으로 인가하여 제1 해시 값 $h(m)$ 을 연산한다.

여기서, 상기 해시 함수 $h(x)$ 는 입력 값을 $(n-k)$ 비트 크기의 출력 값으로 변환시키는 일방향 함수이다.

신드롬 메시지 생성부(113)는 상기 제1 해시 값 $h(m)$ 의 연산이 완료되면, 변수 i (상기 변수 i 는 '0'이상인 정수임)를 '0'부터 '1'씩 증가시키면서, 상기 제1 해시 값 $h(m)$ 에 상기 변수 i 에 대한 비트 값을 연결한 결과 값 $h(m)||i$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 제2 해시 값인 $h(h(m)||i)$ 을 연산하고, 상기 제2 해시 값인 $h(h(m)||i)$ 의 전치 행렬인 $h(h(m)||i)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 신드롬 메시지 s_i 를 생성한다.

[0045] 이로 인해, 상기 신드롬 메시지 s_i 는 하기의 수학식 4와 같이 표현될 수 있다.

수학식 4

[0047]
$$s_i = Q^{-1}h(h(m)|i)^T$$

[0049] 선택부(114)는 상기 변수 i 가 '0'을 시작으로 해서 '1'씩 증가되면서 상기 신드롬 메시지 s_i 가 생성될 때마다, 각 변수 i 에서의 상기 신드롬 메시지 s_i 에 대해 상기 패리티 검사 행렬 H 를 기초로 완전 복호화(Complete Decoding)를 수행하여 $H z^T = s_i$ (z 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐)를 만족하는 z^T 를 연산한 후 z^T 의 해밍 무게가 선정된 해밍 무게인 w 이하로 연산되는 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 연산된 z^T 를 서명용 오류 벡터 z_s^T 로 선택한다.

[0050] 즉, 선택부(114)는 상기 수학식 4에서 나타낸 s_i 에 대해 상기 변수 i 를 '0'을 시작으로 해서 '1'씩 증가시키면서 완전 복호화를 수행하여 $H z^T = s_i$ 를 만족하는 z^T 를 연산해 보고, z^T 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하로 연산되는 시점에서, z^T 를 찾는 연산을 중단한 후 해당 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 연산된 z^T 를 서명용 오류 벡터 z_s^T 로 선택할 수 있다.

[0051] 그 이후, 전자 서명부(115)는 상기 서명용 오류 벡터 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.

[0052] 그리고, 전자 서명 전송부(116)는 데이터 수신 장치(120)에 대해 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1} z_s^T$ 및 상기 서명용 변수 i_s 를 전송할 수 있다.

[0053] 이때, 본 발명의 일실시예에 따르면, 데이터 수신 장치(120)는 메모리 상에 상기 스크램블링 행렬 Q 와 상기 패리티 검사 행렬 H 및 상기 순열 행렬 P 가 곱해진 행렬인 $(n-k) \times n$ 크기를 갖는 K_{pub} 를 전자 서명에 대한 검증키로 저장하고 있을 수 있다.

[0054] 여기서, 상기 검증키 K_{pub} 는 하기의 수학식 5와 같이 나타낼 수 있다.

수학식 5

[0056]
$$K_{pub} = QHP$$

[0058] 만약, 데이터 수신 장치(120)에 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1} z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 데이터 수신 장치(120)는 상기 전자 서명 값 $P^{-1} z_s^T$ 가 진정한 데이터 전송측에 의해서 전송된 데이

터인지 여부를 검증하기 위해, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 검증키 K_{pub} 와 상기 서명용 변수 i_s 에 기초하여 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 수행할 수 있다.

[0059] 관련해서, 데이터 수신 장치(120)는 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 수행하기 위한 구체적 구성으로, 상기 메모리 상에 상기 해시 함수 $h(x)$ 를 저장하고 있고, 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인할 수 있다.

[0060] 앞서, 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치(110)의 선택부(114)는 해밍 무게가 상기 선정된 해밍 무게인 w 이하를 갖는 서명용 오류 벡터 z_s^T 를 선택한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 을 생성하여 데이터 수신 장치(120)로 전송하였기 때문에, 데이터 수신 장치(120)에 수신된 전자 서명 값인 $P^{-1}z_s^T$ 의 해밍 무게도 상기 선정된 해밍 무게인 w 이하가 되어야 데이터 수신 장치(120)에 정상적으로 데이터가 수신되었다고 볼 수 있을 것이다.

[0061] 따라서, 데이터 수신 장치(120)는 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 먼저 확인하게 된다.

[0062] 만약, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 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 제1 해시 값 $h(m)$ 을 연산할 수 있다.

[0063] 그리고 나서, 데이터 수신 장치(120)는 상기 제1 해시 값 $h(m)$ 에 상기 서명용 변수 i_s 에 대한 비트 값을 연접한 결과 값 $h(m)|i_s$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 검증용 해시 값인 $h(h(m)|i_s)$ 을 연산할 수 있다.

[0064] 그 이후, 데이터 수신 장치(120)는 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 검증용 해시 값인 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는지 비교하여 상기 $K_{pub}P^{-1}z_s^T$ 가 상기 검증용 해시 값 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 성공으로 판단할 수 있다.

[0065] 관련해서, 상기 검증키 K_{pub} 에 상기 전자 서명 값 $P^{-1}z_s^T$ 을 곱한 결과 값인 $K_{pub}P^{-1}z_s^T$ 은 하기의 수학식 6과 같이 나타낼 수 있다.

수학식 6

$$\begin{aligned} & K_{pub}P^{-1}z_s^T \\ &= QHPP^{-1}z_s^T \\ &= QHz_s^T \end{aligned}$$

[0067]

[0069] 그리고, 상기 검증용 해시 값 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 는 하기의 수학식 7과 같이 나타낼 수 있다.

수학식 7

$$\begin{aligned} & h(h(m)|i_s)^T \\ &= QQ^{-1}h(h(m)|i_s)^T \end{aligned}$$

[0071]

[0073] 상기 수학식 7에서 $Q^{-1}h(h(m)|i_s)^T$ 는 상기 서명용 변수 i_s 가 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치(110)로부터 데이터 수신 장치(120)로 위조나 변조 없이 정상적으로 수신되었다면, Hz_s^T 와 동일한 값이 될 것이다.

[0074]

이로 인해, 상기 전자 서명 값 $P^{-1}z_s^T$ 가 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치(110)로부터 데이터 수신 장치(120)로 위조나 변조 없이 정상적으로 수신되었다면, 상기 수학식 6에 따른 $K_{pub}P^{-1}z_s^T$ 와 상기 수학식 7에 따른 $h(h(m)|i_s)^T$ 는 하기의 수학식 8에서 나타낸 것처럼 동일한 값이 되어야 할 것이다.

수학식 8

$$\begin{aligned} & K_{pub}P^{-1}z_s^T \\ &= QHPP^{-1}z_s^T \\ &= QHz_s^T \\ &= QQ^{-1}h(h(m)|i_s)^T \\ &= h(h(m)|i_s)^T \end{aligned}$$

[0076]

[0078] 따라서, 데이터 수신 장치(120)는 상기 $K_{pub}P^{-1}z_s^T$ 가 상기 검증용 해시 값 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 성공으로 판단할

수 있다.

[0079] 이상, 도 1을 참조하여 본 발명의 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치(110)를 설명하였다.

[0080] 지금까지 설명한 실시예에서는 RM 코드로 구성된 패리티 검사 행렬을 기초로 전자 서명을 수행하는 구성을 포함하고 있다는 점에서, 제3자가 RM 코드의 구조적 특성을 기반으로 상기 패리티 검사 행렬을 추측해낼 가능성을 배제할 수 없는 보안상의 약점이 존재할 수 있다. 따라서, 본 발명은 전자 서명의 보안성을 더욱 높이기 위해서, 전술한 실시예와는 다른 변형된 실시예로 전자 서명에 사용되는 패리티 검사 행렬의 구조를 변경함으로써, 제3자가 RM 코드의 구조적 특성을 기반으로 패리티 검사 행렬을 추측해낼 수 없도록 구성될 수도 있다. 관련해서, 이하에서는 도 1을 참조하여 본 발명의 변형된 실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치(110)에 대해 추가적으로 설명하기로 한다.

[0081] 개인키 저장부(111)에는 RM 코드로 구성된 $(n-k) \times n$ 크기의 선형 부호에 대한 패리티 검사 행렬 H , 상기 패리티 검사 행렬 H 에서 복수의 선정된 제1 행들에 위치하는 성분들이 랜덤한 코드 값으로 치환되고, 복수의 선정된 제2 열들에 위치하는 성분들이 '0'의 코드 값으로 치환된 변형 패리티 검사 행렬 H_t , '1'과 '0'의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스�크램블링 행렬 Q 및 '1'과 '0'의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P 가 저장되어 있다.

[0082] 여기서, n 과 k 는 자연수이고 n 은 k 보다 큰 수이다.

[0083] 보통, 상기 패리티 검사 행렬 H 는 하기의 수학식 9에서 표현한 것처럼, 패리티 비트들로 구성된 $k \times (n-k)$ 크기의 패리티 부(sub) 행렬 P_s 에 대한 전치 행렬인 P_s^T 와 $(n-k) \times (n-k)$ 크기의 단위 행렬 I 가 서로 연결된 형태를 가지고 있다.

수학식 9

$$H = [P_s^T | I] = \begin{bmatrix} p_{11} & p_{21} & \dots & p_{k1} & 1 & 0 & \dots & 1 \\ p_{12} & p_{22} & \dots & p_{k2} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ p_{1(n-k)} & p_{2(n-k)} & & p_{k(n-k)} & 0 & 0 & \dots & 1 \end{bmatrix}$$

[0087] 이때, 개인키 저장부(110) 상에 저장되어 있는 상기 변형 패리티 검사 행렬 H_t 는 상기 수학식 9의 형태를 갖는 상기 패리티 검사 행렬 H 에서 복수의 선정된 제1 행들에 위치하는 성분들이 랜덤한 코드 값으로 치환되고, 복수의 선정된 제2 열들에 위치하는 성분들이 '0'의 코드 값으로 치환된 형태를 가지도록 구성될 수 있다.

[0088] 관련해서, 상기 변형 패리티 검사 행렬 H_t 는 도 2에 도시된 그림과 같은 형태를 가지도록 구성될 수 있다.

[0089] 도 2에 도시된 그림과 같이, 상기 변형 패리티 검사 행렬 H_t 는 도면부호 211로 표시한 것처럼 상기 패리티 검사 행렬 H 의 최하단 행으로부터 p 개의 행까지에 존재하는 코드들이 랜덤한 코드 값으로 치환되고, 도면부호 212에 표시한 것처럼 상기 패리티 검사 행렬 H 의 최우측 열으로부터 p 개의 열까지에 존재하는 코드들이 '0'으로 치환된 형태를 가지도록 구성될 수 있다.

[0090] 이때, 도 2에서 I_p 로 표시한 $p \times p$ 크기의 부분에 위치하는 코드들에 대해서는 변형을 수행하지 않음으로써, 상기 변형 패리티 검사 행렬 H_t 가 I_p 부분에 대해 단위 행렬의 형태를 갖도록 구성될 수 있다.

[0091] 이렇게, 개인키 저장부(111) 상에 패리티 검사 행렬 H , 변형 패리티 검사 행렬 H_t , 스�크램블링 행렬 Q 및 순열 행렬 P 가 저장되어 있는 상태에서, 데이터 수신 장치(120)로 전송할 평문 메시지를 m 이라고 한다면, 제1 해시 값 연산부(112)는 상기 평문 메시지 m 을 선정된 해시 함수인 $h(x)$ 에 입력으로 인가하여 제1 해시 값 $h(m)$ 을 연

산한다.

[0092] 여기서, 상기 해시 함수 $h(x)$ 는 입력 값을 $(n-k)$ 비트 크기의 출력 값으로 변환시키는 일방향 함수이다.

[0093] 신드롬 메시지 생성부(113)는 상기 제1 해시 값 $h(m)$ 의 연산이 완료되면, 변수 i (상기 변수 i 는 '0'이상인 정수임)를 '0'부터 '1'씩 증가시키면서, 상기 제1 해시 값 $h(m)$ 에 상기 변수 i 에 대한 비트 값을 연결한 결과 값 $h(m)||i$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 제2 해시 값인 $h(h(m)||i)$ 을 연산하고, 상기 제2 해시 값인 $h(h(m)||i)$ 의 전치 행렬인 $h(h(m)||i)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 신드롬 메시지 s_i 를 생성한다.

[0094] 이로 인해, 상기 신드롬 메시지 s_i 는 하기의 수학식 10과 같이 표현될 수 있다.

수학식 10

[0096]
$$s_i = Q^{-1}h(h(m)||i)^T$$

[0098] 선택부(114)는 상기 변수 i 가 '0'을 시작으로 해서 '1'씩 증가되면서 상기 신드롬 메시지 s_i 가 생성될 때마다, 각 변수 i 에서의 상기 신드롬 메시지 s_i 에 대해 상기 패리티 검사 행렬 H 를 기초로 완전 복호화를 수행하여

$H_z^T = s_i$ (z^T 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐)를 만족하는 z^T 를 연산하고, 상기 변형 패리티 검사 행렬 H_t 에서 상기 복수의 선정된 제1 행들과 상기 복수의 선정된 제2 열들에 위치하는 코드 값에 기초하여 각 변수 i 마다 연산되는 z^T 의 성분을 조작함으로써, $H_t z_t^T = s_i$ 를 만족하는 z_t^T 를 검출한 후 z_t^T 의 해밍 무게가 선정된 해밍 무게인 w 이하로 검출되는 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 검출된 z_t^T 를 서명용 오류 벡터 z_s^T 로 선택한다.

[0099] 관련해서, 선택부(114)는 상기 수학식 10에서 나타낸 s_i 에 대해 상기 변수 i 를 '0'을 시작으로 해서 '1'씩 증가시키면서 완전 복호화를 수행하여 $H_z^T = s_i$ 를 만족하는 z^T 를 연산할 수 있다.

[0100] 그리고, 선택부(114)는 도 2의 형태를 갖는 상기 변형 패리티 검사 행렬 H_t 에서 도면부호 211과 도면부호 212로 표시한 치환된 코드 값에 기초하여 각 변수 i 마다 연산되는 z^T 의 성분을 조작함으로써, $H_t z_t^T = s_i$ 를 만족하는 z_t^T 를 검출할 수 있다. 관련해서, 상기 변형 패리티 검사 행렬 H_t 는 상기 패리티 검사 행렬 H 에서 도면부호 211과 도면부호 212로 표시된 부분의 코드 값만 변경된 행렬이므로, $H_z^T = s_i$ 를 만족하는 z^T 가 연산되면, $n \times 1$ 의 크기를 갖는 행렬인 z^T 에 포함되어 있는 성분들 중 도면부호 211과 도면부호 212의 성분들이 변경됨에 따라 H_z^T 의 연산에 영향을 받는 성분들의 코드 값만을 조작함으로써, $H_t z_t^T = s_i$ 의 연산을 만족하는 z_t^T 를 찾아낼 수 있다.

[0101] 이러한 방식으로 선택부(114)는 상기 변수 i 를 '1'씩 증가시키면서 각 변수에 대응하는 z_t^T 를 찾으면서, z_t^T 의 해밍 무게가 선정된 해밍 무게인 w 이하로 검출되는 시점에서, z_t^T 를 찾는 연산을 중단한 후 해당 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 연산된 z_t^T 를 서명용 오류 벡터 z_s^T 로

선택할 수 있다.

[0102] 그 이후, 전자 서명부(115)는 상기 서명용 오류 벡터 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 생성한다.

[0103] 그리고, 전자 서명 전송부(116)는 데이터 수신 장치(120)에 대해 상기 평문 메시지 m과 상기 전자 서명 값 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 를 전송할 수 있다.

[0104] 이때, 본 발명의 일실시예에 따르면, 데이터 수신 장치(120)는 메모리 상에 상기 스크램블링 행렬 Q와 상기 변형 패리티 검사 행렬 H_t 및 상기 순열 행렬 P가 곱해진 행렬인 $(n-k) \times n$ 크기를 갖는 K_{pub} 를 전자 서명에 대한 검증키로 저장하고 있을 수 있다.

[0105] 여기서, 상기 검증키 K_{pub} 는 하기의 수학적 식 11과 같이 나타낼 수 있다.

수학적 식 11

[0107]
$$K_{pub} = QH_tP$$

[0109] 만약, 데이터 수신 장치(120)에 상기 평문 메시지 m과 상기 전자 서명 값 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 데이터 수신 장치(120)는 상기 전자 서명 값 $P^{-1}z_s^T$ 가 진정한 데이터 전송측에 의해서 전송된 데이터인지 여부를 검증하기 위해, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 검증키 K_{pub} 와 상기 서명용 변수 i_s 에 기초하여 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 수행할 수 있다.

[0110] 관련해서, 데이터 수신 장치(120)는 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 수행하기 위한 구체적인 구성으로, 상기 메모리 상에 상기 해시 함수 $h(x)$ 를 저장하고 있고, 상기 평문 메시지 m과 상기 전자 서명 값 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인할 수 있다.

[0111] 앞서, 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치(110)의 선택부(114)는 해밍 무게가 상기 선정된 해밍 무게인 w 이하를 갖는 서명용 오류 벡터 z_s^T 를 선택한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 을 생성하여 데이터 수신 장치(120)로 전송하였기 때문에, 데이터 수신 장치(120)에 수신된 전자 서명 값인 $P^{-1}z_s^T$ 의 해밍 무게도 상기 선정된 해밍 무게인 w 이하가 되어야 데이터 수신 장치(120)에 정상적으로 데이터가 수신되었다고 볼 수 있을 것이다.

[0112] 따라서, 데이터 수신 장치(120)는 상기 평문 메시지 m과 상기 전자 서명 값 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 먼저 확인하게 된다.

[0113] 만약, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 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 제1 해시 값 $h(m)$ 을 연산할 수 있다.

[0114] 그리고 나서, 데이터 수신 장치(120)는 상기 제1 해시 값 $h(m)$ 에 상기 서명용 변수 i_s 에 대한 비트 값을 연결한 결과 값 $h(m)|i_s$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 검증용 해시 값인 $h(h(m)|i_s)$ 을 연산할 수 있다.

[0115] 그 이후, 데이터 수신 장치(120)는 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 검증용 해시 값인 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는지 비교하여 상기 $K_{pub}P^{-1}z_s^T$ 가 상기 검증용 해시 값 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 성공으로 판단할 수 있다.

[0116] 관련해서, 상기 검증키 K_{pub} 에 상기 전자 서명 값 $P^{-1}z_s^T$ 을 곱한 결과 값인 $K_{pub}P^{-1}z_s^T$ 은 하기의 수학적 식 12와 같이 나타낼 수 있다.

수학적 식 12

$$\begin{aligned} & K_{pub}P^{-1}z_s^T \\ &= QH_tPP^{-1}z_s^T \\ &= QH_tz_s^T \end{aligned}$$

[0118]

[0120] 그리고, 상기 검증용 해시 값 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 는 하기의 수학적 식 13과 같이 나타낼 수 있다.

수학적 식 13

$$\begin{aligned} & h(h(m)|i_s)^T \\ &= QQ^{-1}h(h(m)|i_s)^T \end{aligned}$$

[0122]

[0124] 상기 수학적 식 13에서 $Q^{-1}h(h(m)|i_s)^T$ 는 상기 서명용 변수 i_s 가 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치(110)로부터 데이터 수신 장치(120)로 위조나 변조 없이 정상적으로 수신되었다면, $H_tz_s^T$ 와 동일한 값이 될 것이다.

[0125] 이로 인해, 상기 전자 서명 값 $P^{-1}z_s^T$ 가 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장

치(110)로부터 데이터 수신 장치(120)로 위조나 변조 없이 정상적으로 수신되었다면, 상기 수학적 식 12에 따른 $K_{pub}P^{-1}z_s^T$ 와 상기 수학적 식 13에 따른 $h(h(m)|i_s)^T$ 는 하기의 수학적 식 14에서 나타난 것처럼 동일한 값이 되어야 할 것이다.

수학적 식 14

$$\begin{aligned} & K_{pub}P^{-1}z_s^T \\ &= QH_tPP^{-1}z_s^T \\ &= QH_tz_s^T \\ &= QQ^{-1}h(h(m)|i_s)^T \\ &= h(h(m)|i_s)^T \end{aligned}$$

[0127]

[0129] 따라서, 데이터 수신 장치(120)는 상기 $K_{pub}P^{-1}z_s^T$ 가 상기 검증용 해시 값 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 성공으로 판단할 수 있다.

[0130] 도 3은 본 발명의 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법을 도시한 순서도이다.

[0131] 단계(S310)에서는 RM 코드로 구성된 $(n-k) \times n$ 크기의 선형 부호에 대한 패리티 검사 행렬 H, '1'과 '0'의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스캐램블링 행렬 Q 및 '1'과 '0'의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P가 저장되어 있는 개인키 저장부를 유지한다.

[0132] 여기서, n과 k는 자연수이고 n은 k보다 큰 수이다.

[0133] 단계(S320)에서는 데이터 수신 장치로 전송할 평문 메시지 m을 선정된 해시 함수인 h(x)에 입력으로 인가하여 제1 해시 값 h(m)을 연산한다.

[0134] 상기 해시 함수 h(x)는 입력 값을 $(n-k)$ 비트 크기의 출력 값으로 변환시키는 일방향 함수이다.

[0135] 단계(S330)에서는 상기 제1 해시 값 h(m)의 연산이 완료되면, 변수 i(상기 변수 i는 '0'이상인 정수임)를 '0'부터 '1'씩 증가시키면서, 상기 제1 해시 값 h(m)에 상기 변수 i에 대한 비트 값을 연결한 결과 값 $h(m)|i$ 를 상기 해시 함수 h(x)에 입력으로 인가하여 제2 해시 값인 $h(h(m)|i)$ 을 연산하고, 상기 제2 해시 값인 $h(h(m)|i)$ 의 전치 행렬인 $h(h(m)|i)^T$ 의 좌측 변에 상기 스캐램블링 행렬 Q의 역행렬인 Q^{-1} 을 곱하여 신드롬 메시지 $s_i(s_i = Q^{-1}h(h(m)|i)^T)$ 임)를 생성한다.

[0136] 단계(S340)에서는 상기 변수 i가 '0'을 시작으로 해서 '1'씩 증가되면서 상기 신드롬 메시지 s_i 가 생성될 때마다, 각 변수 i에서의 상기 신드롬 메시지 s_i 에 대해 상기 패리티 검사 행렬 H를 기초로 완전 복호화를 수행하여 $Hz^T = s_i$ (z^T 는 크기가 n인 벡터 z의 전치 행렬로 $n \times 1$ 의 크기를 가짐)를 만족하는 z^T 를 연산한 후 z^T 의 해밍 무게가 선정된 해밍 무게인 w 이하로 연산되는 시점에서의 변수 i를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 연산된 z^T 를 서명용 오류 벡터 z_s^T 로 선택한다.

- [0137] 단계(S350)에서는 상기 서명용 오류 벡터 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 생성한다.
- [0138] 단계(S360)에서는 상기 데이터 수신 장치에 대해 상기 평문 메시지 m과 상기 전자 서명 값 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 를 전송한다.
- [0139] 이때, 본 발명의 일실시예에 따르면, 상기 데이터 수신 장치는 메모리 상에 상기 스크램블링 행렬 Q와 상기 패리티 검사 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 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 검증키 K_{pub} 와 상기 서명용 변수 i_s 에 기초하여 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 수행할 수 있다.
- [0140] 이때, 본 발명의 일실시예에 따르면, 상기 데이터 수신 장치는 상기 메모리 상에 상기 해시 함수 $h(x)$ 를 추가로 저장하고 있고, 상기 평문 메시지 m과 상기 전자 서명 값 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 평문 메시지 m을 상기 메모리 상에 저장되어 있는 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 상기 제1 해시 값 $h(m)$ 을 연산하고, 상기 제1 해시 값 $h(m)$ 이 연산되면, 상기 제1 해시 값 $h(m)$ 에 상기 서명용 변수 i_s 에 대한 비트 값을 연접한 결과 값 $h(m)|i_s$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 검증용 해시 값인 $h(h(m)|i_s)$ 을 연산하며, 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 검증용 해시 값인 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는지 비교하여 상기 $K_{pub}P^{-1}z_s^T$ 가 상기 검증용 해시 값 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 성공으로 판단할 수 있다.
- [0141] 도 4는 본 발명의 또 다른 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법을 도시한 순서도이다.
- [0142] 단계(S410)에서는 RM 코드로 구성된 $(n-k) \times n$ 크기의 선형 부호에 대한 패리티 검사 행렬 H, 상기 패리티 검사 행렬 H에서 복수의 선정된 제1 행들에 위치하는 성분들이 랜덤한 코드 값으로 치환되고, 복수의 선정된 제2 열들에 위치하는 성분들이 '0'의 코드 값으로 치환된 변형 패리티 검사 행렬 H_t , '1'과 '0'의 코드 값을 성분으로 포함하는 $(n-k) \times (n-k)$ 크기의 스크램블링 행렬 Q 및 '1'과 '0'의 코드 값을 성분으로 포함하는 $n \times n$ 크기의 순열 행렬 P가 저장되어 있는 개인키 저장부를 유지한다.
- [0143] 여기서, n과 k는 자연수이고 n은 k보다 큰 수이다.
- [0144] 단계(S420)에서는 데이터 수신 장치로 전송할 평문 메시지 m을 선정된 해시 함수인 $h(x)$ 에 입력으로 인가하여 제1 해시 값 $h(m)$ 을 연산한다.
- [0145] 상기 해시 함수 $h(x)$ 는 입력 값을 $(n-k)$ 비트 크기의 출력 값으로 변환시키는 일방향 함수이다.

- [0146] 단계(S430)에서는 상기 제1 해시 값 $h(m)$ 의 연산이 완료되면, 변수 i (상기 변수 i 는 '0'이상인 정수임)를 '0'부터 '1'씩 증가시키면서, 상기 제1 해시 값 $h(m)$ 에 상기 변수 i 에 대한 비트 값을 연접한 결과 값 $h(m)|i$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 제2 해시 값인 $h(h(m)|i)$ 을 연산하고, 상기 제2 해시 값인 $h(h(m)|i)$ 의 전치 행렬인 $h(h(m)|i)^T$ 의 좌측 변에 상기 스크램블링 행렬 Q 의 역행렬인 Q^{-1} 을 곱하여 신드롬 메시지 $s_i(s_i = Q^{-1}h(h(m)|i)^T)$ 임을 생성한다.
- [0147] 단계(S440)에서는 상기 변수 i 가 '0'을 시작으로 해서 '1'씩 증가되면서 상기 신드롬 메시지 s_i 가 생성될 때마다, 각 변수 i 에서의 상기 신드롬 메시지 s_i 에 대해 상기 패리티 검사 행렬 H 를 기초로 완전 복호화를 수행하여 $H z^T = s_i$ (z^T 는 크기가 n 인 벡터 z 의 전치 행렬로 $n \times 1$ 의 크기를 가짐)를 만족하는 z^T 를 연산하고, 상기 변형 패리티 검사 행렬 H_t 에서 상기 복수의 선정된 제1 행들과 상기 복수의 선정된 제2 열들에 위치하는 코드 값에 기초하여 각 변수 i 마다 연산되는 z^T 의 성분을 조합함으로써, $H_t z_t^T = s_i$ 를 만족하는 z_t^T 를 검출한 후 z_t^T 의 해밍 무게가 선정된 해밍 무게인 w 이하로 검출되는 시점에서의 변수 i 를 서명용 변수 i_s 로 선택함과 동시에 상기 서명용 변수 i_s 에 대응하여 검출된 z_t^T 를 서명용 오류 벡터 z_s^T 로 선택한다.
- [0148] 단계(S450)에서는 상기 서명용 오류 벡터 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.
- [0149] 단계(S460)에서는 상기 데이터 수신 장치에 대해 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 를 전송한다.
- [0150] 이때, 본 발명의 일실시예에 따르면, 상기 데이터 수신 장치는 메모리 상에 상기 스크램블링 행렬 Q 와 상기 변형 패리티 검사 행렬 H_t 및 상기 순열 행렬 P 가 곱해진 행렬인 $(n-k) \times n$ 크기를 갖는 $K_{pub}(K_{pub} = QH_tP)$ 을 전자 서명에 대한 검증키로 저장하고 있고, 상기 평문 메시지 m 과 상기 전자 서명 값 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 검증키 K_{pub} 와 상기 서명용 변수 i_s 에 기초하여 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 수행할 수 있다.
- [0151] 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 $P^{-1}z_s^T$ 및 상기 서명용 변수 i_s 가 수신되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인지 여부를 확인한 후 상기 전자 서명 값 $P^{-1}z_s^T$ 의 해밍 무게가 상기 선정된 해밍 무게인 w 이하인 것으로 확인되면, 상기 평문 메시지 m 을 상기 메모리 상에 저장되어 있는 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 상기 제1 해시 값 $h(m)$ 을 연산하고, 상기 제1 해시 값 $h(m)$ 이 연산되면, 상기 제1 해시 값 $h(m)$ 에 상기 서명용 변수 i_s 에 대한 비트 값을 연접한 결과 값 $h(m)|i_s$ 를 상기 해시 함수 $h(x)$ 에 입력으로 인가하여 검증용 해시 값인 $h(h(m)|i_s)$ 을 연산하며, 상기 검

증키 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 검증용 해시 값인 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는지 비교하여 상기 $K_{pub}P^{-1}z_s^T$ 가 상기 검증용 해시 값 $h(h(m)|i_s)$ 의 전치 행렬인 $h(h(m)|i_s)^T$ 와 일치하는 것으로 판단되면, 상기 전자 서명 값 $P^{-1}z_s^T$ 에 대한 검증을 성공으로 판단할 수 있다.

[0152] 본 발명의 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 방법은 컴퓨터와 의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0153] 또한, 본 발명의 일실시예에 따른 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 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.

[0154] 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.

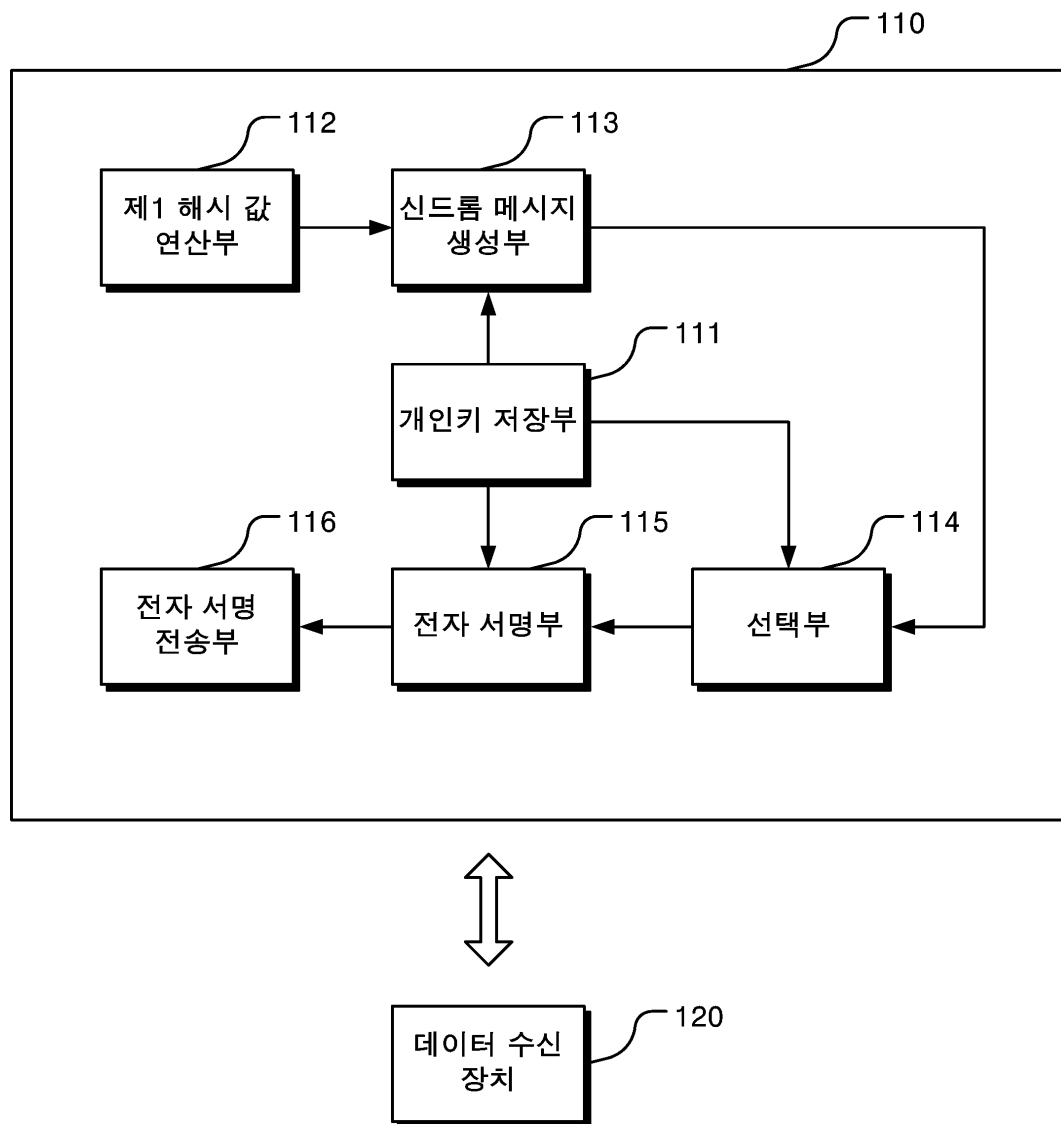
[0155] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0156] 110: 패리티 검사 행렬에 기초한 오류 복원 기법을 이용하는 전자 서명 장치
111: 개인키 저장부 112: 제1 해시 값 연산부
113: 신드롬 메시지 생성부 114: 선택부
115: 전자 서명부 116: 전자 서명 전송부
120: 데이터 수신 장치

도면

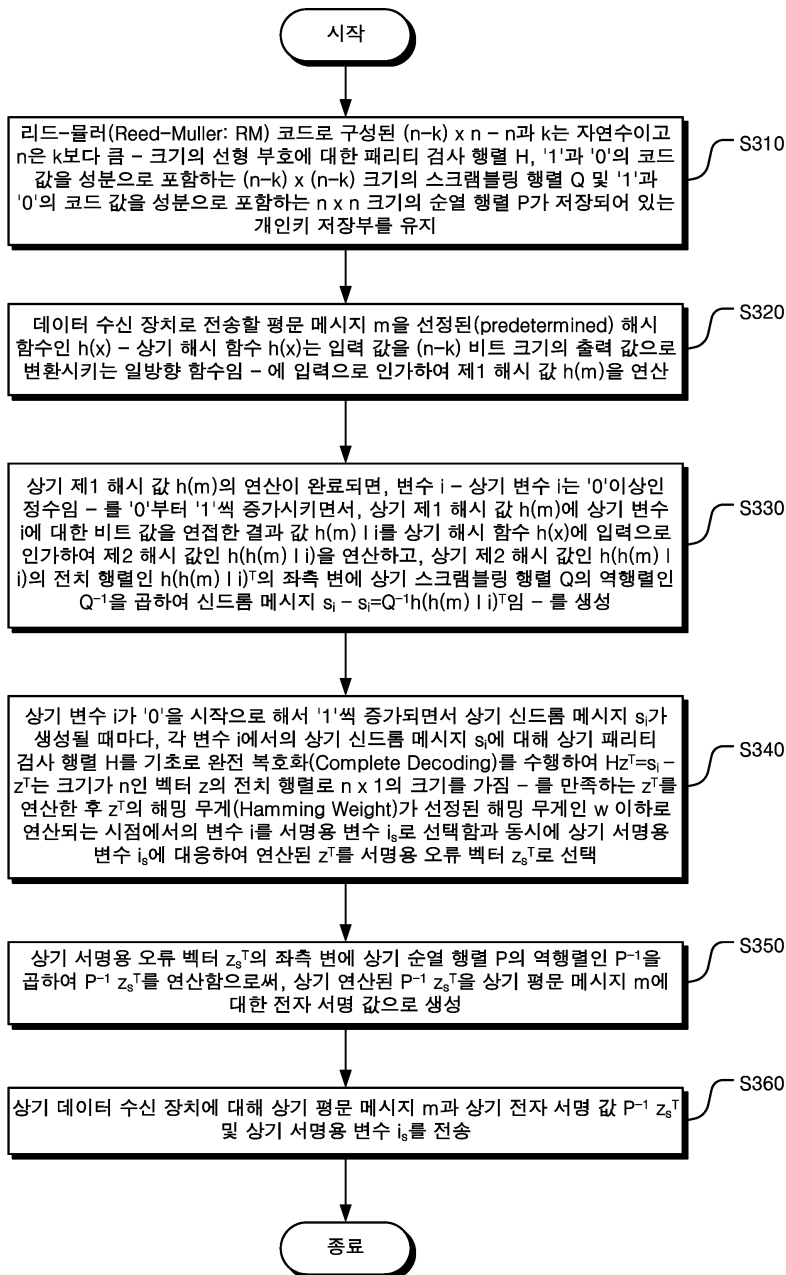
도면1



도면2

$$H_t = \left[\begin{array}{ccc|c} \overbrace{\hspace{1.5cm}}^k & \overbrace{\hspace{1.5cm}}^{n-k-p} & \overbrace{\hspace{1.5cm}}^p & \\ \hline \underbrace{\hspace{1.5cm}}_{n-k-p} & P_s'^T & I_{n-k-p} & 0 \\ \hline \underbrace{\hspace{1.5cm}}_p & R & I_p & \end{array} \right] \begin{array}{l} \left. \vphantom{\begin{array}{c} P_s'^T \\ I_{n-k-p} \\ 0 \end{array}} \right\} 212 \\ \left. \vphantom{\begin{array}{c} R \\ I_p \end{array}} \right\} 211 \end{array}$$

도면3



도면4

