



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년05월02일
(11) 등록번호 10-1974345
(24) 등록일자 2019년04월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 12/40 (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/0866 (2013.01)
H04L 9/0825 (2013.01)
(21) 출원번호 10-2018-0155867
(22) 출원일자 2018년12월06일
심사청구일자 2018년12월06일
(56) 선행기술조사문헌
KR1020180065694 A*
(뒷면에 계속)

(73) 특허권자
동국대학교 산학협력단
서울특별시 중구 필동로1길 30 (필동3가, 동국대학교)
조선대학교 산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
임대운
서울특별시 은평구 진관2로 57-37, 243동 1001호
(진관동, 은평뉴타운우물골)
김영식
광주광역시 서구 풍암2로 66 금호2차아파트 201동 1005호
박경원
서울특별시 동대문구 장안벚꽃로 167 래미안장안 2차아파트 212동 101호
(74) 대리인
김효성

전체 청구항 수 : 총 10 항

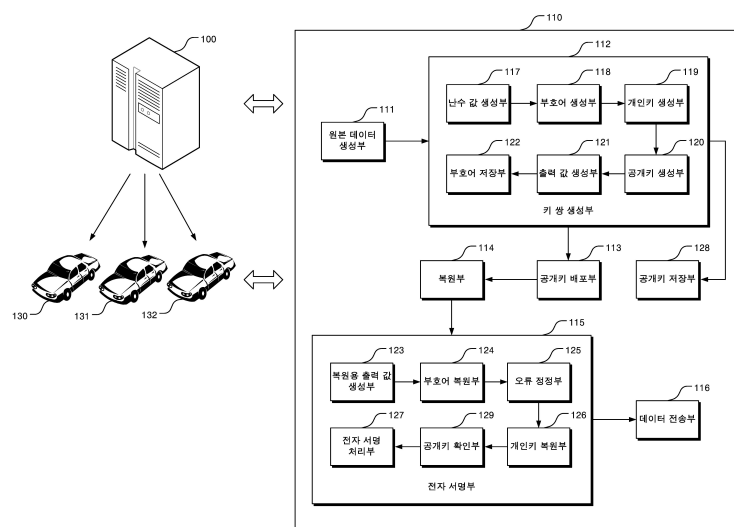
심사관 : 양종필

(54) 발명의 명칭 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치 및 그 동작 방법

(57) 요약

전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치 및 그 동작 방법이 개시된다. 본 발명은 사용자의 생체 정보에 기초하여 개인키가 생성되도록 함으로써, 별도의 저장 공간 상에 개인키를 저장하지 않더라도 전자 서명이 가능하도록 지원하고, 개인키를 생성하는데 사용되는 사용자의 생체 정보를 부호어(codeword)로 취급하여 오류 정정 기반의 디코딩을 수행하는 방식으로 상기 개인키의 생성을 처리하는 커넥티드 차량용 데이터 통신 장치 및 그 동작 방법을 제시함으로써, 차량 간의 데이터 통신에 있어 높은 보안성을 제공할 수 있다.

대표도 - 도1



(52) CPC특허분류

H04L 9/0869 (2013.01)
H04L 9/3236 (2013.01)
H04L 9/3247 (2013.01)
H04L 9/3278 (2013.01)
H04L 2012/40273 (2013.01)
H04L 2209/84 (2013.01)

(56) 선행기술조사문헌

KR1020180104363 A*
 US6363485 B1
 KR1020180059980 A
 KR1020180081108 A
 *는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업

과제고유번호	1711065844
부처명	과학기술정보통신부
연구관리전문기관	정보통신기술진흥센터
연구사업명	정보보호핵심원천기술개발(R&D)
연구과제명	자율 주행차를 위한 침입 감내 핵심 요소 기술 개발
기 여 율	1/1
주관기관	조선대학교 산학협력단
연구기간	2018.01.01 ~ 2018.12.31

명세서

청구범위

청구항 1

공개키 배포 서버로부터 복수의 차량들로의 공개키 배포를 수행하기 위한 공개키 발급 요청이 수신되면, 차량 내에 탑재되어 있는 생체 정보 인식기를 통해 사용자로부터 제1 생체 정보를 입력받고, 상기 제1 생체 정보를 구성하는 데이터를 t (t 는 자연수) 비트 코드에 대한 오류 정정 능력을 갖는 선정된(predetermined) 제1 생성 행렬에 기초하여 인코딩된 제1 부호어(codeword)로 취급하여, 상기 선정된 제1 생성 행렬을 기초로 상기 제1 부호어에 대한 오류 정정 기반의 디코딩을 수행함으로써, 상기 제1 부호어에 대한 원본 데이터를 생성하는 원본 데이터 생성부;

상기 원본 데이터를 기초로 제1 개인키를 생성하고, 상기 제1 개인키에 대응하는 제1 공개키를 생성하는 키 쌍 생성부;

상기 제1 공개키를 상기 공개키 배포 서버에 전송하여 상기 제1 공개키의 배포를 완료하는 공개키 배포부;

상기 제1 공개키의 배포가 완료된 이후, 상기 복수의 차량들 중 네트워크로 연결된 제1 차량의 데이터 통신 장치로부터 상기 제1 차량의 데이터 통신 장치로 전송될 제1 원본 메시지에 대한 전자 서명 요청이 수신되면, 상기 생체 정보 인식기를 통해 상기 사용자로부터 상기 제1 생체 정보를 입력받아, 상기 제1 생체 정보를 상기 제1 부호어로 취급하여 상기 제1 생체 정보에 대해 상기 선정된 제1 생성 행렬을 기초로 오류 정정 기반의 디코딩을 수행함으로써, 상기 원본 데이터를 복원하는 복원부;

상기 복원된 원본 데이터를 기초로 상기 제1 개인키를 복원하고, 상기 제1 원본 메시지를 선정된 제1 해시 함수에 입력으로 인가하여 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행함으로써, 제1 전자 서명 값을 생성하는 전자 서명부; 및

상기 제1 원본 메시지와 상기 제1 전자 서명 값을 상기 제1 차량의 데이터 통신 장치로 전송하는 데이터 전송부를 포함하고,

상기 키 쌍 생성부는

상기 원본 데이터가 생성되면, 난수 생성기를 통해 난수 값을 생성하는 난수 값 생성부;

상기 난수 값에 대해 n (n 는 자연수) 비트 코드에 대한 오류 정정 능력을 갖는 선정된 제2 생성 행렬을 기초로 인코딩을 수행함으로써, 제2 부호어를 생성하는 부호어 생성부;

두 종류의 데이터를 결합하여 출력 데이터를 생성하는 선정된 결합 함수에 상기 원본 데이터와 상기 제2 부호어를 입력으로 인가하여 제1 결합 데이터를 생성한 후 상기 제1 결합 데이터를 선정된 개인키 생성용 해시 함수에 입력으로 인가함으로써 연산되는 해시 값을 상기 제1 개인키로 생성하는 개인키 생성부;

상기 제1 개인키를 기초로 상기 제1 개인키에 대응하는 상기 제1 공개키를 생성하는 공개키 생성부;

SRAM(Static Random Access Memory) 기반의 물리적 복제 방지 함수(Physical Unclonable Function: PUF)에 선정된 제1 입력 값을 입력으로 인가하여 제1 출력 값을 생성하는 출력 값 생성부; 및

상기 제2 부호어와 상기 제1 출력 값을 배타적 논리합(XOR)하여 암호화된 제2 부호어를 생성하고, 상기 암호화된 제2 부호어를 부호어 저장소 상에 저장하는 부호어 저장부

를 포함하는 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 전자 서명부는

상기 복원부를 통해 상기 원본 데이터가 복원되면, 상기 SRAM 기반의 PUF에 상기 선정된 제1 입력 값을 입력으로 인가하여 상기 제1 출력 값을 생성하는 복원용 출력 값 생성부;

상기 부호어 저장소로부터 상기 암호화된 제2 부호어를 추출하고, 상기 암호화된 제2 부호어와 상기 제1 출력 값을 배타적 논리합하여 상기 제2 부호어를 복원하는 부호어 복원부;

상기 선정된 제2 생성 행렬을 기초로 상기 복원된 제2 부호어에 대해 오류 정정 기반의 디코딩을 수행함으로써, 오류 정정이 수행된 상기 제2 부호어를 생성하는 오류 정정부;

상기 복원부를 통해 복원된 상기 원본 데이터와 오류 정정이 수행된 상기 제2 부호어를 상기 선정된 결합 함수에 입력으로 인가하여 상기 제1 결합 데이터를 생성하고, 상기 제1 결합 데이터를 상기 선정된 개인키 생성용 해시 함수에 입력으로 인가함으로써 연산되는 해시 값을 상기 제1 개인키로 복원하는 개인키 복원부; 및

상기 제1 원본 메시지를 상기 선정된 제1 해시 함수에 입력으로 인가하여 상기 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행하여 상기 제1 전자 서명 값의 생성을 처리하는 전자 서명 처리부

를 포함하는 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치.

청구항 4

제3항에 있어서,

상기 키 쌍 생성부를 통해 상기 제1 공개키가 생성되면, 공개키 저장소에 상기 제1 공개키를 저장하는 공개키 저장부

를 더 포함하고,

상기 전자 서명부는

상기 개인키 복원부를 통해 상기 제1 개인키의 복원이 완료되면, 상기 복원된 제1 개인키에 대응하는 공개키로 검증용 공개키를 생성한 후 상기 검증용 공개키가 상기 공개키 저장소에 저장되어 있는 상기 제1 공개키와 일치하는지 여부를 확인하는 공개키 확인부

를 더 포함하며,

상기 전자 서명 처리부는

상기 검증용 공개키가 상기 공개키 저장소에 저장되어 있는 상기 제1 공개키와 일치하는 것으로 확인되면, 상기 제1 원본 메시지를 상기 선정된 제1 해시 함수에 입력으로 인가하여 상기 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행하여 상기 제1 전자 서명 값의 생성을 처리하는 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치.

청구항 5

제1항에 있어서,

상기 제1 차량의 데이터 통신 장치는

상기 공개키 배포 서버로부터 상기 제1 공개키가 상기 커넥티드 차량용 데이터 통신 장치에 대한 배포용 공개키로 수신되면, 메모리 상에 상기 제1 공개키를 저장하고,

상기 제1 공개키가 상기 메모리 상에 저장된 이후, 상기 커넥티드 차량용 데이터 통신 장치로부터 상기 제1 원본 메시지와 상기 제1 전자 서명 값이 수신되면, 상기 메모리 상에 저장되어 있는 상기 제1 공개키를 기초로 상기 제1 전자 서명 값에 대한 복호화를 수행하여 복호화 값을 생성하고, 상기 제1 원본 메시지를 상기 선정된 제1 해시 함수와 동일한 해시 함수에 입력으로 인가하여 검증용 해시 값을 생성한 후 상기 복호화 값과 상기 검증용 해시 값이 서로 동일한 것으로 확인되면, 상기 제1 전자 서명 값에 대한 검증이 성공인 것으로 판단하는 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치.

청구항 6

공개키 배포 서버로부터 복수의 차량들로의 공개키 배포를 수행하기 위한 공개키 발급 요청이 수신되면, 차량 내에 탑재되어 있는 생체 정보 인식기를 통해 사용자로부터 제1 생체 정보를 입력받고, 상기 제1 생체 정보를 구성하는 데이터를 t (t 는 자연수) 비트 코드에 대한 오류 정정 능력을 갖는 선정된(predetermined) 제1 생성 행렬에 기초하여 인코딩된 제1 부호어(codeword)로 취급하여, 상기 선정된 제1 생성 행렬을 기초로 상기 제1 부호어에 대한 오류 정정 기반의 디코딩을 수행함으로써, 상기 제1 부호어에 대한 원본 데이터를 생성하는 단계;

상기 원본 데이터를 기초로 제1 개인키를 생성하고, 상기 제1 개인키에 대응하는 제1 공개키를 생성함으로써, 개인키-공개키 쌍의 생성을 처리하는 단계;

상기 제1 공개키를 상기 공개키 배포 서버에 전송하여 상기 제1 공개키의 배포를 완료하는 단계;

상기 제1 공개키의 배포가 완료된 이후, 상기 복수의 차량들 중 네트워크로 연결된 제1 차량의 데이터 통신 장치로부터 상기 제1 차량의 데이터 통신 장치로 전송될 제1 원본 메시지에 대한 전자 서명 요청이 수신되면, 상기 생체 정보 인식기를 통해 상기 사용자로부터 상기 제1 생체 정보를 입력받아, 상기 제1 생체 정보를 상기 제1 부호어로 취급하여 상기 제1 생체 정보에 대해 상기 선정된 제1 생성 행렬을 기초로 오류 정정 기반의 디코딩을 수행함으로써, 상기 원본 데이터를 복원하는 단계;

상기 복원된 원본 데이터를 기초로 상기 제1 개인키를 복원하고, 상기 제1 원본 메시지를 선정된 제1 해시 함수에 입력으로 인가하여 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행함으로써, 제1 전자 서명 값을 생성하는 단계; 및

상기 제1 원본 메시지와 상기 제1 전자 서명 값을 상기 제1 차량의 데이터 통신 장치로 전송하는 단계

를 포함하고,

상기 개인키-공개키 쌍의 생성을 처리하는 단계는

상기 원본 데이터가 생성되면, 난수 생성기를 통해 난수 값을 생성하는 단계;

상기 난수 값에 대해 n (n 는 자연수) 비트 코드에 대한 오류 정정 능력을 갖는 선정된 제2 생성 행렬을 기초로 인코딩을 수행함으로써, 제2 부호어를 생성하는 단계;

두 종류의 데이터를 결합하여 출력 데이터를 생성하는 선정된 결합 함수에 상기 원본 데이터와 상기 제2 부호어를 입력으로 인가하여 제1 결합 데이터를 생성한 후 상기 제1 결합 데이터를 선정된 개인키 생성용 해시 함수에 입력으로 인가함으로써 연산되는 해시 값을 상기 제1 개인키로 생성하는 단계;

상기 제1 개인키를 기초로 상기 제1 개인키에 대응하는 상기 제1 공개키를 생성하는 단계;

SRAM(Static Random Access Memory) 기반의 물리적 복제 방지 함수(Physical Unclonable Function: PUF)에 선정된 제1 입력 값을 입력으로 인가하여 제1 출력 값을 생성하는 단계; 및

상기 제2 부호어와 상기 제1 출력 값을 배타적 논리합(XOR)하여 암호화된 제2 부호어를 생성하고, 상기 암호화된 제2 부호어를 부호어 저장소 상에 저장하는 단계

를 포함하는 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 동작 방법.

청구항 7

삭제

청구항 8

제6항에 있어서,

상기 제1 전자 서명 값을 생성하는 단계는

상기 원본 데이터를 복원하는 단계를 통해 상기 원본 데이터가 복원되면, 상기 SRAM 기반의 PUF에 상기 선정된 제1 입력 값을 입력으로 인가하여 상기 제1 출력 값을 생성하는 단계;

상기 부호어 저장소로부터 상기 암호화된 제2 부호어를 추출하고, 상기 암호화된 제2 부호어와 상기 제1 출력 값을 배타적 논리합하여 상기 제2 부호어를 복원하는 단계;

상기 선정된 제2 생성 행렬을 기초로 상기 복원된 제2 부호어에 대해 오류 정정 기반의 디코딩을 수행함으로써,

오류 정정이 수행된 상기 제2 부호어를 생성하는 단계;

상기 원본 데이터를 복원하는 단계를 통해 복원된 상기 원본 데이터와 오류 정정이 수행된 상기 제2 부호어를 상기 선정된 결합 함수에 입력으로 인가하여 상기 제1 결합 데이터를 생성하고, 상기 제1 결합 데이터를 상기 선정된 개인키 생성용 해시 함수에 입력으로 인가함으로써 연산되는 해시 값을 상기 제1 개인키로 복원하는 단계; 및

상기 제1 원본 메시지를 상기 선정된 제1 해시 함수에 입력으로 인가하여 상기 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행하여 상기 제1 전자 서명 값의 생성을 처리하는 단계

를 포함하는 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 동작 방법.

청구항 9

제8항에 있어서,

상기 개인키-공개키 쌍의 생성을 처리하는 단계를 통해 상기 제1 공개키가 생성되면, 공개키 저장소에 상기 제1 공개키를 저장하는 단계

를 더 포함하고,

상기 제1 전자 서명 값을 생성하는 단계는

상기 제1 개인키로 복원하는 단계를 통해 상기 제1 개인키의 복원이 완료되면, 상기 복원된 제1 개인키에 대응하는 공개키로 검증용 공개키를 생성한 후 상기 검증용 공개키가 상기 공개키 저장소에 저장되어 있는 상기 제1 공개키와 일치하는지 여부를 확인하는 단계

를 더 포함하며,

상기 제1 전자 서명 값의 생성을 처리하는 단계는

상기 검증용 공개키가 상기 공개키 저장소에 저장되어 있는 상기 제1 공개키와 일치하는 것으로 확인되면, 상기 제1 원본 메시지를 상기 선정된 제1 해시 함수에 입력으로 인가하여 상기 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행하여 상기 제1 전자 서명 값의 생성을 처리하는 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 동작 방법.

청구항 10

제6항에 있어서,

상기 제1 차량의 데이터 통신 장치는

상기 공개키 배포 서버로부터 상기 제1 공개키가 상기 커넥티드 차량용 데이터 통신 장치에 대한 배포용 공개키로 수신되면, 메모리 상에 상기 제1 공개키를 저장하고,

상기 제1 공개키가 상기 메모리 상에 저장된 이후, 상기 커넥티드 차량용 데이터 통신 장치로부터 상기 제1 원본 메시지와 상기 제1 전자 서명 값이 수신되면, 상기 메모리 상에 저장되어 있는 상기 제1 공개키를 기초로 상기 제1 전자 서명 값에 대한 복호화를 수행하여 복호화 값을 생성하고, 상기 제1 원본 메시지를 상기 선정된 제1 해시 함수와 동일한 해시 함수에 입력으로 인가하여 검증용 해시 값을 생성한 후 상기 복호화 값과 상기 검증용 해시 값이 서로 동일한 것으로 확인되면, 상기 제1 전자 서명 값에 대한 검증이 성공인 것으로 판단하는 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 동작 방법.

청구항 11

제6항, 제8항, 제9항 또는 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 컴퓨터 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 12

제6항, 제8항, 제9항 또는 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술 분야

[0001] 본 발명은 차량 간의 데이터 통신에 있어서 보안성을 강화할 수 있는 전자 서명 기술에 대한 것이다.

배경 기술

[0002] 특정 사용자로부터 전달되는 메시지가 진정한 사용자에게 의해서 전달되는 것인지 여부를 확인하기 위한 보안 서비스를 부인 방지 서비스라고 칭한다.

[0003] 보통, 일반적인 온라인 뱅킹 서비스나 결제 시스템에서 도입하고 있는 부인 방지 서비스는 공개키 기반의 암호화 방식(Public Key Infrastructure: PKI)을 이용한 전자 서명 시스템이 주를 이루고 있다.

[0004] 공개키 기반의 암호화 방식의 전자 서명 시스템이란 메시지를 전달하는 측에서 해당 메시지를 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, 상기 공개키로 복호화한 값과 상기 메시지를 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.

[0005] 최근에는 차량 간에 네트워크로 연결되어 데이터를 송수신할 수 있는 커넥티드 차량에 대한 연구가 활발히 진행되고 있다. 차량 간의 데이터 통신에 있어서는 차량의 특성상 외부로부터 위조나 변조된 데이터가 수신되는 경우, 교통사고를 일으키는 등의 심각한 문제를 발생시킬 수 있다는 점에서 데이터 송수신 과정에서 보안 프로토콜이 반드시 적용되어야 한다.

[0006] 특히, 차량 간의 통신에 있어서는 상대측 차량으로부터 전송되는 데이터가 신뢰할 수 있는 진정한 상대방으로부터 수신된 데이터가 맞는지를 판단할 수 있는 부인 방지 기술이 적용되어야 할 필요성이 높다.

[0007] 차량에서 기존의 전자 서명 방식을 사용하는 경우, 데이터 전송측이 소정의 물리적 저장소에 개인키를 보관하고 있어야 하는데, 물리적 저장소에 개인키를 보관하는 방식은 이동성이 보장되어야 하는 차량에 있어서 많은 불편을 초래하고, 개인키의 노출 가능성이 매우 높아지는 문제를 발생시킬 수 있다.

[0008] 따라서, 차량 간 데이터 통신에서 공개키 기반의 암호화 방식의 전자 서명 방식을 도입함에 있어서, 데이터 전송측이 소정의 개인키 저장소 상에 별도로 개인키를 저장하지 않더라도 전자 서명을 수행할 수 있도록 지원하기 위한 새로운 방식의 보안 알고리즘이 도입될 필요가 있다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 사용자의 생체 정보에 기초하여 개인키가 생성되도록 함으로써, 별도의 저장 공간 상에 개인키를 저장하지 않더라도 전자 서명이 가능하도록 지원하고, 개인키를 생성하는데 사용되는 사용자의 생체 정보를 부호어(codeword)로 취급하여 오류 정정 기반의 디코딩을 수행하는 방식으로 상기 개인키의 생성을 처리하는 커넥티드 차량용 데이터 통신 장치 및 그 동작 방법을 제시함으로써, 차량 간의 데이터 통신에 있어 높은 보안성을 제공할 수 있도록 한다.

과제의 해결 수단

[0010] 본 발명의 일 실시예에 따른 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치는 공개키 배포 서버로부터 복수의 차량들로의 공개키 배포를 수행하기 위한 공개키 발급 요청이 수신되면, 차량 내에 탑재되어 있는 생체 정보 인식기를 통해 사용자로부터 제1 생체 정보를 입력받고, 상기 제1 생체 정보를 구성하는 데이터를 t (t 는 자연수) 비트 코드에 대한 오류 정정 능력을 갖는 선정된(predetermined) 제1 생성 행렬에 기초하여 인코딩된 제1 부호어(codeword)로 취급하여, 상기 선정된 제1 생성 행렬을 기초로 상기 제1 부호어에 대한 오류 정정 기반의 디코딩을 수행함으로써, 상기 제1 부호어에 대한 원본 데이터를 생성하는 원본 데이터 생성부, 상기 원본 데이터를 기초로 제1 개인키를 생성하고, 상기 제1 개인키에 대응하는 제1 공개키를 생성하는 키 쌍 생성부, 상기 제1 공개키를 상기 공개키 배포 서버에 전송하여 상기 제1 공개키의 배포를 완료

하는 공개키 배포부, 상기 제1 공개키의 배포가 완료된 이후, 상기 복수의 차량들 중 네트워크로 연결된 제1 차량의 데이터 통신 장치로부터 상기 제1 차량의 데이터 통신 장치로 전송될 제1 원본 메시지에 대한 전자 서명 요청이 수신되면, 상기 생체 정보 인식기를 통해 상기 사용자로부터 상기 제1 생체 정보를 입력받아, 상기 제1 생체 정보를 상기 제1 부호어로 취급하여 상기 제1 생체 정보에 대해 상기 선정된 제1 생성 행렬을 기초로 오류 정정 기반의 디코딩을 수행함으로써, 상기 원본 데이터를 복원하는 복원부, 상기 복원된 원본 데이터를 기초로 상기 제1 개인키를 복원하고, 상기 제1 원본 메시지를 선정된 제1 해시 함수에 입력으로 인가하여 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행함으로써, 제1 전자 서명 값을 생성하는 전자 서명부 및 상기 제1 원본 메시지와 상기 제1 전자 서명 값을 상기 제1 차량의 데이터 통신 장치로 전송하는 데이터 전송부를 포함한다.

[0011] 또한, 본 발명의 일실시예에 따른 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 동작 방법은 공개키 배포 서버로부터 복수의 차량들로의 공개키 배포를 수행하기 위한 공개키 발급 요청이 수신되면, 차량 내에 탑재되어 있는 생체 정보 인식기를 통해 사용자로부터 제1 생체 정보를 입력받고, 상기 제1 생체 정보를 구성하는 데이터를 t (t 는 자연수) 비트 코드에 대한 오류 정정 능력을 갖는 선정된 제1 생성 행렬에 기초하여 인코딩된 제1 부호어로 취급하여, 상기 선정된 제1 생성 행렬을 기초로 상기 제1 부호어에 대한 오류 정정 기반의 디코딩을 수행함으로써, 상기 제1 부호어에 대한 원본 데이터를 생성하는 단계, 상기 원본 데이터를 기초로 제1 개인키를 생성하고, 상기 제1 개인키에 대응하는 제1 공개키를 생성함으로써, 개인키-공개키 쌍의 생성을 처리하는 단계, 상기 제1 공개키를 상기 공개키 배포 서버에 전송하여 상기 제1 공개키의 배포를 완료하는 단계, 상기 제1 공개키의 배포가 완료된 이후, 상기 복수의 차량들 중 네트워크로 연결된 제1 차량의 데이터 통신 장치로부터 상기 제1 차량의 데이터 통신 장치로 전송될 제1 원본 메시지에 대한 전자 서명 요청이 수신되면, 상기 생체 정보 인식기를 통해 상기 사용자로부터 상기 제1 생체 정보를 입력받아, 상기 제1 생체 정보를 상기 제1 부호어로 취급하여 상기 제1 생체 정보에 대해 상기 선정된 제1 생성 행렬을 기초로 오류 정정 기반의 디코딩을 수행함으로써, 상기 원본 데이터를 복원하는 단계, 상기 복원된 원본 데이터를 기초로 상기 제1 개인키를 복원하고, 상기 제1 원본 메시지를 선정된 제1 해시 함수에 입력으로 인가하여 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행함으로써, 제1 전자 서명 값을 생성하는 단계 및 상기 제1 원본 메시지와 상기 제1 전자 서명 값을 상기 제1 차량의 데이터 통신 장치로 전송하는 단계를 포함한다.

발명의 효과

[0012] 본 발명은 사용자의 생체 정보에 기초하여 개인키가 생성되도록 함으로써, 별도의 저장 공간 상에 개인키를 저장하지 않더라도 전자 서명이 가능하도록 지원하고, 개인키를 생성하는데 사용되는 사용자의 생체 정보를 부호어(codeword)로 취급하여 오류 정정 기반의 디코딩을 수행하는 방식으로 상기 개인키의 생성을 처리하는 커넥티드 차량용 데이터 통신 장치 및 그 동작 방법을 제시함으로써, 차량 간의 데이터 통신에 있어 높은 보안성을 제공할 수 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 일실시예에 따른 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 구조를 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 동작 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 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.

[0015] 본 문서에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다. 또한, 본 발명의 다양한

실시예들에 있어서, 각 구성요소들, 기능 블록들 또는 수단들은 하나 또는 그 이상의 하부 구성요소로 구성될 수 있고, 각 구성요소들이 수행하는 전기, 전자, 기계적 기능들은 전자회로, 집적회로, ASIC(Application Specific Integrated Circuit) 등 공지된 다양한 소자들 또는 기계적 요소들로 구현될 수 있으며, 각각 별개로 구현되거나 2 이상이 하나로 통합되어 구현될 수도 있다.

[0016] 한편, 첨부된 블록도의 블록들이나 흐름도의 단계들은 범용 컴퓨터, 특수용 컴퓨터, 휴대용 노트북 컴퓨터, 네트워크 컴퓨터 등 데이터 프로세싱이 가능한 장비의 프로세서나 메모리에 탑재되어 지정된 기능들을 수행하는 컴퓨터 프로그램 명령들(instructions)을 의미하는 것으로 해석될 수 있다. 이들 컴퓨터 프로그램 명령들은 컴퓨터 장치에 구비된 메모리 또는 컴퓨터에서 판독 가능한 메모리에 저장될 수 있기 때문에, 블록도의 블록들 또는 흐름도의 단계들에서 설명된 기능들은 이를 수행하는 명령 수단을 내포하는 제조물로 생산될 수도 있다. 아울러, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 명령들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 가능한 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 정해진 순서와 달리 실행되는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 실질적으로 동시에 수행되거나, 역순으로 수행될 수 있으며, 경우에 따라 일부 블록들 또는 단계들이 생략된 채로 수행될 수도 있다.

[0017] 도 1은 본 발명의 일실시예에 따른 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 구조를 도시한 도면이다.

[0018] 도 1을 참조하면, 본 발명에 따른 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치(110)는 원본 데이터 생성부(111), 키 쌍 생성부(112), 공개키 배포부(113), 복원부(114), 전자 서명부(115) 및 데이터 전송부(116)를 포함한다.

[0019] 우선, 공개키 배포 서버(100)는 커넥티드 차량용 데이터 통신 장치(110)로부터 복수의 차량들(130, 131, 132)로 데이터가 전자 서명되어 전송되면, 복수의 차량들(130, 131, 132)이 전자 서명의 검증을 수행할 수 있도록 하기 위한 공개키의 배포 처리를 수행하는 서버로, 공개키 배포 서버(100)는 커넥티드 차량용 데이터 통신 장치(110)와 복수의 차량들(130, 131, 132)이 본격적인 데이터 통신을 수행하기에 앞서, 공개키 배포 과정을 수행하기 위해 커넥티드 차량용 데이터 통신 장치(110)에 공개키 발급 요청을 전송하게 된다.

[0020] 이때, 원본 데이터 생성부(111)는 공개키 배포 서버(100)로부터 복수의 차량들(130, 131, 132)로의 공개키 배포를 수행하기 위한 공개키 발급 요청이 수신되면, 차량 내에 탑재되어 있는 생체 정보 인식기를 통해 사용자로부터 제1 생체 정보를 입력받고, 상기 제1 생체 정보를 구성하는 데이터를 t (t 는 자연수) 비트 코드에 대한 오류 정정 능력을 갖는 선정된(predetermined) 제1 생성 행렬에 기초하여 인코딩된 제1 부호어(codeword)로 취급하여, 상기 선정된 제1 생성 행렬을 기초로 상기 제1 부호어에 대한 오류 정정 기반의 디코딩을 수행함으로써, 상기 제1 부호어에 대한 원본 데이터를 생성한다.

[0021] 여기서, 상기 제1 생체 정보란 상기 사용자로부터 획득할 수 있는 지문 정보, 홍채 정보 등 상기 사용자를 식별하기 위한 고유의 생체적 특성을 드러내는 정보를 의미한다. 예컨대, 상기 제1 생체 정보가 상기 사용자의 지문 정보라고 하는 경우, 원본 데이터 생성부(111)는 소정의 지문 인식기를 통해 상기 사용자로부터 상기 사용자의 지문 정보를 획득할 수 있다.

[0022] 이렇게, 원본 데이터 생성부(111)는 상기 사용자로부터 상기 제1 생체 정보를 입력받으면, 상기 제1 생체 정보를 구성하는 데이터를 t 비트 코드에 대한 오류 정정 능력을 갖는 상기 선정된 제1 생성 행렬에 기초하여 인코딩된 제1 부호어로 취급하여, 상기 선정된 제1 생성 행렬을 기초로 상기 제1 부호어에 대한 오류 정정 기반의 디코딩을 수행함으로써, 상기 제1 부호어에 대한 원본 데이터를 생성할 수 있다.

[0023] 생성 행렬이란 데이터 송수신 과정에서 데이터 전송측이 원본 데이터를 소정의 부호어로 인코딩하는데 사용되는 행렬을 의미하는 것으로, 데이터 전송측에서 원본 데이터가 생성 행렬을 기초로 부호어로 인코딩되어 데이터 수신측으로 전송되면, 데이터 수신측에서는 수신 데이터에 대해 상기 생성 행렬을 기초로 오류 정정을 수행함으로써, 상기 원본 데이터를 복원할 수 있게 된다.

[0024] 관련해서, t 비트 코드에 대한 오류 정정 능력을 갖는 $k \times n$ 크기의 생성 행렬을 'G', 데이터 전송측이 데이터 수신측으로 전송할 길이가 k 인 원본 데이터를 'd'라고 하는 경우, 데이터 전송측은 하기의 수학식 1의 연산에 따라 데이터 수신측으로 전송할 부호어 c 를 생성할 수 있다.

수학식 1

$$c = dG$$

데이터 전송측이 상기 수학식 1의 연산에 따라 상기 부호어 c 를 생성하여 데이터 수신측으로 상기 부호어 c 를 전송하였을 때, 데이터 수신측에 수신된 부호어를 ' r '이라고 한다면, 데이터 수신측에서는 상기 수신된 부호어 r 로부터 상기 생성 행렬 G 을 기초로 오류 정정 기반의 디코딩을 수행함으로써, 원본 데이터 d 를 복원할 수 있다. 여기서, 상기 생성 행렬 G 의 오류 정정 능력은 ' t '이기 때문에, 데이터 수신측에서는 상기 수신된 부호어 r 에 오류가 t 비트 이하로 발생한 경우에 한해서 상기 원본 데이터 d 를 복원할 수 있다.

참고로, 상기 생성 행렬 G 에 대응하는 $(n-k) \times n$ 크기의 패리티 검사 행렬을 ' H '라고 하는 경우, 상기 패리티 검사 행렬 H 와 상기 생성 행렬 G 사이에는 하기의 수학식 2와 같은 특성이 존재한다.

수학식 2

$$GH^T = 0$$

여기서, H^T 는 패리티 검사 행렬 H 의 전치 행렬을 의미한다.

만약, 데이터 수신측에 수신된 상기 부호어 r 에 오류가 발생하지 않은 경우, 상기 부호어 r 에 대해서는 패리티 검사 행렬 H 와의 관계에서 하기의 수학식 3과 같은 특성이 존재한다.

수학식 3

$$rH^T = cH^T = 0$$

하지만, 데이터 전송측이 전송한 부호어 c 에 오류 e 가 발생하였다고 한다면, 데이터 수신측이 수신한 상기 부호어 r 은 ' $c \oplus e$ '($\oplus$ 는 배타적 논리합임)가 될 것이고, 이로 인해 패리티 검사 행렬 H 와 상기 부호어 r 사이에는 하기의 수학식 4와 같은 특성을 가지게 된다.

수학식 4

$$\begin{aligned} rH^T &= (c \oplus e)H^T \\ &= cH^T \oplus eH^T \quad (cH^T = 0 \text{ 이므로}) \\ &= eH^T \\ &= s \end{aligned}$$

상기 수학식 4에서의 연산과 같이, 데이터 수신측에서는 패리티 검사 행렬을 이용해서 데이터 수신측에 수신된 데이터에 오류가 존재하는지 여부를 검출할 수 있다. 그리고, 상기 수학식 4에서 ' s '를 신드롬(Syndrome)이라고 한다. 이러한 신드롬을 기반으로 오류 정정을 수행하여 원본 데이터를 복호화할 수 있는데, 이를 신드롬 디코딩이라고 칭한다.

이러한 오류 정정 기법을 활용해서, 원본 데이터 생성부(111)는 상기 제1 생체 정보를 이용하여 개인키를 생성하기 위한 원본 데이터를 생성할 수 있는데, 원본 데이터 생성부(111)는 상기 사용자로부터 상기 제1 생체 정보가 입력되면, 상기 제1 생체 정보를 상기 수학식 1에서 나타낸 c 와 같이, 제1 생성 행렬에 기초하여 인코딩된 제1 부호어로 취급하여, 상기 선정된 제1 생성 행렬을 기초로 상기 제1 부호어에 대한 오류 정정 기반의 디코딩을 수행함으로써, 상기 제1 부호어에 대한 원본 데이터를 생성할 수 있다.

- [0044] 이렇게, 상기 원본 데이터가 생성되면, 키 쌍 생성부(112)는 상기 원본 데이터를 기초로 제1 개인키를 생성하고, 상기 제1 개인키에 대응하는 제1 공개키를 생성한다.
- [0045] 이때, 본 발명의 일실시예에 따르면, 키 쌍 생성부(112)는 난수 값 생성부(117), 부호어 생성부(118), 개인키 생성부(119), 공개키 생성부(120), 출력 값 생성부(121) 및 부호어 저장부(122)를 포함할 수 있다.
- [0046] 난수 값 생성부(117)는 상기 원본 데이터가 생성되면, 난수 생성기를 통해 난수 값을 생성한다.
- [0047] 부호어 생성부(118)는 상기 난수 값에 대해 n (n 는 자연수) 비트 코드에 대한 오류 정정 능력을 갖는 선정된 제2 생성 행렬을 기초로 인코딩을 수행함으로써, 제2 부호어를 생성한다.
- [0048] 관련해서, 부호어 생성부(118)는 상기 수학식 1에서 나타낸 수식에 따라 상기 난수 값을 'd'로 취급하여 상기 난수 값에 대해 상기 선정된 제2 생성 행렬을 기초로 인코딩을 수행함으로써, 상기 제2 부호어를 생성할 수 있다.
- [0049] 개인키 생성부(119)는 두 종류의 데이터를 결합하여 출력 데이터를 생성하는 선정된 결합 함수에 상기 원본 데이터와 상기 제2 부호어를 입력으로 인가하여 제1 결합 데이터를 생성한 후 상기 제1 결합 데이터를 선정된 개인키 생성용 해시 함수에 입력으로 인가함으로써 연산되는 해시 값을 상기 제1 개인키로 생성한다.
- [0050] 관련해서, 상기 선정된 결합 함수는 'a'와 'b'라고 하는 두 종류의 데이터가 존재할 때, 'a'와 'b'를 배타적 논리합(XOR) 연산하도록 하는 함수일 수도 있고, 'a'에 'b'를 연접하도록 하는 함수일 수도 있는 것처럼, 두 종류의 데이터를 결합해서 소정의 출력 데이터를 생성하도록 설정된 함수를 의미한다.
- [0051] 이렇게, 상기 선정된 결합 함수에 상기 원본 데이터와 상기 제2 부호어가 입력으로 인가되어 상기 제1 결합 데이터가 생성되면, 개인키 생성부(119)는 선정된 개인키 생성용 해시 함수에 상기 제1 결합 데이터를 입력으로 인가함으로써, 해시 값을 연산하고, 상기 연산된 해시 값을 전자 서명을 위한 상기 제1 개인키로 결정할 수 있다.
- [0052] 이렇게, 상기 제1 개인키가 생성되면, 공개키 생성부(120)는 상기 제1 개인키를 기초로 상기 제1 개인키에 대응하는 상기 제1 공개키를 생성한다.
- [0053] 이때, 본 발명의 일실시예에 따르면, 공개키 생성부(120)는 RSA(Rivest-Shamir-Adleman) 알고리즘과 같이 다양한 개인키-공개키 생성 알고리즘에 기초하여 상기 제1 개인키에 대응하는 상기 제1 공개키를 생성할 수 있다.
- [0054] 출력 값 생성부(121)는 SRAM(Static Random Access Memory) 기반의 물리적 복제 방지 함수(Physical Unclonable Function: PUF)에 선정된 제1 입력 값을 입력으로 인가하여 제1 출력 값을 생성한다.
- [0055] PUF란 소자의 제조 공정상의 물리적 편차를 이용하여 전자기적으로 소정의 고유 식별정보를 생성해 내는 방식을 의미하는 것으로, PUF의 입력은 요청(challenge)이라 하고 출력은 응답(response)이라고 한다. PUF의 출력은 동일한 제조 공정, 동일한 회로로 구현하더라도 제조 공정상의 편차로 인하여 결과를 예측할 수 없는 특징이 있다. 관련해서, 메모리 기반의 SRAM PUF는 SRAM이 가지고 있는 불안정한 상태를 이용하는데, 출력 값 생성부(121)는 이러한 SRAM 기반의 PUF에 선정된 제1 입력 값을 입력으로 인가함으로써, 고유의 제1 출력 값을 생성할 수 있다.
- [0056] 부호어 저장부(122)는 상기 제1 출력 값이 생성되면, 부호어 생성부(118)에서 생성된 상기 제2 부호어와 상기 제1 출력 값을 배타적 논리합하여 암호화된 제2 부호어를 생성하고, 상기 암호화된 제2 부호어를 부호어 저장소(미도시) 상에 저장한다.
- [0057] 이러한 방식으로 키 쌍 생성부(112)에서 상기 제1 개인키와 상기 제1 공개키의 생성이 완료되면, 공개키 배포부(113)는 상기 제1 공개키를 공개키 배포 서버(100)에 전송하여 상기 제1 공개키의 배포를 완료한다.
- [0058] 이때, 공개키 배포 서버(100)는 상기 제1 공개키가 수신되면, 복수의 차량들(130, 131, 132)로 상기 제1 공개키를 전송하여 상기 제1 공개키의 배포를 처리할 수 있다.
- [0059] 이때, 복수의 차량들(130, 131, 132) 각각에 탑재되어 있는 데이터 통신 장치는 공개키 배포 서버(100)로부터 상기 제1 공개키가 커넥티드 차량용 데이터 통신 장치(110)에 대한 배포용 공개키로 수신되면, 메모리 상에 상기 제1 공개키를 저장할 수 있다.
- [0060] 이렇게, 상기 제1 공개키의 배포가 완료된 이후, 본 발명에 따른 커넥티드 차량용 데이터 통신 장치(110)가 복수의 차량들(130, 131, 132) 중 네트워크로 연결된 제1 차량(130)의 데이터 통신 장치로 제1 원본 메시지를 전

송해야 하는 상황이 발생함에 따라, 제1 차량(130)의 데이터 통신 장치로부터 상기 제1 원본 메시지에 대한 전자 서명 요청이 수신되면, 복원부(114)는 상기 생체 정보 인식기를 통해 상기 사용자로부터 상기 제1 생체 정보를 입력받아, 상기 제1 생체 정보를 상기 제1 부호어로 취급하여 상기 제1 생체 정보에 대해 상기 선정된 제1 생성 행렬을 기초로 오류 정정 기반의 디코딩을 수행함으로써, 상기 원본 데이터를 복원한다.

[0061] 상기 사용자로부터 입력되는 상기 제1 생체 정보는 앞서 언급한 바와 같이, 지문 정보, 홍채 정보 등과 같은 사용자의 고유 생체 정보를 의미하는 것으로, 생체 정보 인식기의 인식 상의 오류로 인해 항상 동일한 데이터가 획득되지 않을 수 있다. 하지만, 상기 제1 생체 정보 상에 오류가 t 비트 이하로 발생하였다면 복원부(114)는 상기 제1 생체 정보를 상기 제1 부호어로 취급하여 상기 선정된 제1 생성 행렬을 기초로 오류 정정 기반의 디코딩을 수행함으로써, 앞서 원본 데이터 생성부(111)에서 생성되었던 상기 원본 데이터와 동일한 데이터를 복원해 낼 수 있다.

[0062] 이렇게, 상기 원본 데이터의 복원이 완료되면, 전자 서명부(115)는 상기 복원된 원본 데이터를 기초로 상기 제1 개인키를 복원하고, 상기 제1 원본 메시지를 선정된 제1 해시 함수에 입력으로 인가하여 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행함으로써, 제1 전자 서명 값을 생성한다.

[0063] 이때, 본 발명의 일실시예에 따르면, 전자 서명부(115)는 상기 제1 전자 서명 값의 생성을 위한 구체적 구성으로 복원용 출력 값 생성부(123), 부호어 복원부(124), 오류 정정부(125), 개인키 복원부(126) 및 전자 서명 처리부(127)를 포함할 수 있다.

[0064] 복원용 출력 값 생성부(123)는 복원부(114)를 통해 상기 원본 데이터가 복원되면, 상기 SRAM 기반의 PUF에 상기 선정된 제1 입력 값을 입력으로 인가하여 상기 제1 출력 값을 생성한다.

[0065] 부호어 복원부(124)는 상기 부호어 저장소로부터 상기 암호화된 제2 부호어를 추출하고, 상기 암호화된 제2 부호어와 상기 제1 출력 값을 배타적 논리합하여 상기 제2 부호어를 복원한다.

[0066] 관련해서, 상기 부호어 저장소에는 부호어 저장부(122)를 통해 상기 제2 부호어와 상기 제1 출력 값이 배타적 논리합 연산된 상기 암호화된 제2 부호어가 저장되어 있기 때문에, 부호어 복원부(124)는 상기 암호화된 제2 부호어에 대해 복원용 출력 값 생성부(123)에서 생성된 상기 제1 출력 값을 다시 배타적 논리합함으로써, 상기 제2 부호어를 복원해 낼 수 있다.

[0067] 오류 정정부(125)는 상기 선정된 제2 생성 행렬을 기초로 상기 복원된 제2 부호어에 대해 오류 정정 기반의 디코딩을 수행함으로써, 오류 정정이 수행된 상기 제2 부호어를 생성한다.

[0068] 관련해서, 부호어 복원부(124)에서 상기 제2 부호어가 복원되었지만, SRAM 기반의 PUF의 특성상 동일한 제1 입력 값이 입력으로 인가되었다고 하더라도 복원용 출력 값 생성부(123)에서 생성된 상기 제1 출력 값이 출력 값 생성부(121)에서 생성되었던 제1 출력 값과 완전히 일치하지 않을 수 있어, 부호어 복원부(124)에서 복원된 상기 제2 부호어는 부호어 생성부(118)에서 생성되었던 제2 부호어와 완전히 일치하지 않을 수 있다.

[0069] 따라서, 오류 정정부(125)는 부호어 복원부(124)에서 복원된 상기 제2 부호어에 소정의 오류가 발생할 수 있음을 예상하여 상기 선정된 제2 생성 행렬을 기초로 오류 정정 기반의 디코딩을 수행함으로써, 오류 정정이 수행된 상기 제2 부호어를 생성할 수 있다.

[0070] 오류 정정부(125)를 통해 상기 제2 부호어에 대해 오류 정정이 수행되면, 오류 정정이 수행된 제2 부호어는 부호어 생성부(118)에서 생성되었던 제2 부호어와 동일해지기 때문에, 개인키 복원부(126)는 개인키 생성부(119)와 동일한 방식으로, 복원부(114)를 통해 복원된 상기 원본 데이터와 오류 정정이 수행된 상기 제2 부호어를 상기 선정된 결합 함수에 입력으로 인가하여 상기 제1 결합 데이터를 생성하고, 상기 제1 결합 데이터를 상기 선정된 개인키 생성용 해시 함수에 입력으로 인가함으로써 연산되는 해시 값을 상기 제1 개인키로 복원한다.

[0071] 전자 서명 처리부(127)는 상기 제1 원본 메시지를 상기 선정된 제1 해시 함수에 입력으로 인가하여 상기 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행하여 상기 제1 전자 서명 값의 생성을 처리한다.

[0072] 이때, 본 발명의 일실시예에 따르면, 커넥티드 차량용 데이터 통신 장치(110)는 키 쌍 생성부(112)를 통해 상기 제1 공개키가 생성되면, 공개키 저장소(미도시)에 상기 제1 공개키를 저장하는 공개키 저장부(128)를 더 포함할 수 있다.

[0073] 이때, 전자 서명부(115)는 개인키 복원부(126)를 통해 상기 제1 개인키의 복원이 완료되면, 상기 복원된 제1 개인키

인키에 대응하는 공개키로 검증용 공개키를 생성한 후 상기 검증용 공개키가 상기 공개키 저장소에 저장되어 있는 상기 제1 공개키와 일치하는지 여부를 확인하는 공개키 확인부(129)를 더 포함할 수 있다.

[0074] 이때, 전자 서명 처리부(127)는 상기 검증용 공개키가 상기 공개키 저장소에 저장되어 있는 상기 제1 공개키와 일치하는 것으로 확인되면, 상기 제1 원본 메시지를 상기 선정된 제1 해시 함수에 입력으로 인가하여 상기 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행하여 상기 제1 전자 서명 값의 생성을 처리할 수 있다.

[0075] 이렇게, 전자 서명부(115)를 통해 상기 제1 전자 서명 값이 생성되면, 데이터 전송부(116)는 상기 제1 원본 메시지와 상기 제1 전자 서명 값을 제1 차량(130)의 데이터 통신 장치로 전송한다.

[0076] 이때, 본 발명의 일실시예에 따르면, 제1 차량(130)의 데이터 통신 장치는 커넥티드 차량용 데이터 통신 장치(110)로부터 상기 제1 원본 메시지와 상기 제1 전자 서명 값이 수신되면, 상기 제1 공개키의 배포에 따라 제1 차량(130)의 데이터 통신 장치의 메모리 상에 기 저장되어 있는 상기 제1 공개키를 기초로 상기 제1 전자 서명 값에 대한 복호화를 수행하여 복호화 값을 생성하고, 상기 제1 원본 메시지를 상기 선정된 제1 해시 함수와 동일한 해시 함수에 입력으로 인가하여 검증용 해시 값을 생성한 후 상기 복호화 값과 상기 검증용 해시 값이 서로 동일한 것으로 확인되면, 상기 제1 전자 서명 값에 대한 검증이 성공인 것으로 판단할 수 있다.

[0077] 결국, 본 발명에 따른 커넥티드 차량용 데이터 통신 장치(110)는 사용자의 생체 정보에 기초하여 개인키가 생성되도록 함으로써, 별도의 저장 공간 상에 개인키를 저장하지 않더라도 전자 서명이 가능하도록 지원하고, 개인키를 생성하는데 사용되는 사용자의 생체 정보를 부호어로 취급하여 오류 정정 기반의 디코딩을 수행하는 방식으로 상기 개인키의 생성을 처리한다는 점에서, 사용자로부터 인식되는 생체 정보가 조금씩 달라지더라도 항상 동일한 개인키가 생성되도록 지원할 수 있다.

[0078] 도 2는 본 발명의 일실시예에 따른 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 동작 방법을 도시한 순서도이다.

[0079] 단계(S210)에서는 공개키 배포 서버로부터 복수의 차량들로의 공개키 배포를 수행하기 위한 공개키 발급 요청이 수신되면, 차량 내에 탑재되어 있는 생체 정보 인식기를 통해 사용자로부터 제1 생체 정보를 입력받고, 상기 제1 생체 정보를 구성하는 데이터를 t (t 는 자연수) 비트 코드에 대한 오류 정정 능력을 갖는 선정된 제1 생성 행렬에 기초하여 인코딩된 제1 부호어로 취급하여, 상기 선정된 제1 생성 행렬을 기초로 상기 제1 부호어에 대한 오류 정정 기반의 디코딩을 수행함으로써, 상기 제1 부호어에 대한 원본 데이터를 생성한다.

[0080] 단계(S220)에서는 상기 원본 데이터를 기초로 제1 개인키를 생성하고, 상기 제1 개인키에 대응하는 제1 공개키를 생성함으로써, 개인키-공개키 쌍의 생성을 처리한다.

[0081] 단계(S230)에서는 상기 제1 공개키를 상기 공개키 배포 서버에 전송하여 상기 제1 공개키의 배포를 완료한다.

[0082] 단계(S240)에서는 상기 제1 공개키의 배포가 완료된 이후, 상기 복수의 차량들 중 네트워크로 연결된 제1 차량의 데이터 통신 장치로부터 상기 제1 차량의 데이터 통신 장치로 전송될 제1 원본 메시지에 대한 전자 서명 요청이 수신되면, 상기 생체 정보 인식기를 통해 상기 사용자로부터 상기 제1 생체 정보를 입력받아, 상기 제1 생체 정보를 상기 제1 부호어로 취급하여 상기 제1 생체 정보에 대해 상기 선정된 제1 생성 행렬을 기초로 오류 정정 기반의 디코딩을 수행함으로써, 상기 원본 데이터를 복원한다.

[0083] 단계(S250)에서는 상기 복원된 원본 데이터를 기초로 상기 제1 개인키를 복원하고, 상기 제1 원본 메시지를 선정된 제1 해시 함수에 입력으로 인가하여 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행함으로써, 제1 전자 서명 값을 생성한다.

[0084] 단계(S260)에서는 상기 제1 원본 메시지와 상기 제1 전자 서명 값을 상기 제1 차량의 데이터 통신 장치로 전송한다.

[0085] 이때, 본 발명의 일실시예에 따르면, 단계(S220)에서는 상기 원본 데이터가 생성되면, 난수 생성기를 통해 난수 값을 생성하는 단계, 상기 난수 값에 대해 n (n 는 자연수) 비트 코드에 대한 오류 정정 능력을 갖는 선정된 제2 생성 행렬을 기초로 인코딩을 수행함으로써, 제2 부호어를 생성하는 단계, 두 종류의 데이터를 결합하여 출력 데이터를 생성하는 선정된 결합 함수에 상기 원본 데이터와 제2 부호어를 입력으로 인가하여 제1 결합 데이터를 생성한 후 상기 제1 결합 데이터를 선정된 개인키 생성용 해시 함수에 입력으로 인가함으로써 연산되는 해시 값을 상기 제1 개인키로 생성하는 단계, 상기 제1 개인키를 기초로 상기 제1 개인키에 대응하는 상기 제1 공개키를 생성하는 단계, SRAM 기반의 PUF에 선정된 제1 입력 값을 입력으로 인가하여 제1 출력 값을 생성하는 단계

및 상기 제2 부호어와 상기 제1 출력 값을 배타적 논리합(XOR)하여 암호화된 제2 부호어를 생성하고, 상기 암호화된 제2 부호어를 부호어 저장소 상에 저장하는 단계를 포함할 수 있다.

[0086] 이때, 본 발명의 일실시예에 따르면, 단계(S250)에서는 단계(S240)을 통해 상기 원본 데이터가 복원되면, 상기 SRAM 기반의 PUF에 상기 선정된 제1 입력 값을 입력으로 인가하여 상기 제1 출력 값을 생성하는 단계, 상기 부호어 저장소로부터 상기 암호화된 제2 부호어를 추출하고, 상기 암호화된 제2 부호어와 상기 제1 출력 값을 배타적 논리합하여 상기 제2 부호어를 복원하는 단계, 상기 선정된 제2 생성 행렬을 기초로 상기 복원된 제2 부호어에 대해 오류 정정 기반의 디코딩을 수행함으로써, 오류 정정이 수행된 상기 제2 부호어를 생성하는 단계, 단계(S240)을 통해 복원된 상기 원본 데이터와 오류 정정이 수행된 상기 제2 부호어를 상기 선정된 결합 함수에 입력으로 인가하여 상기 제1 결합 데이터를 생성하고, 상기 제1 결합 데이터를 상기 선정된 개인키 생성용 해시 함수에 입력으로 인가함으로써 연산되는 해시 값을 상기 제1 개인키로 복원하는 단계 및 상기 제1 원본 메시지를 상기 선정된 제1 해시 함수에 입력으로 인가하여 상기 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행하여 상기 제1 전자 서명 값의 생성을 처리하는 단계를 포함할 수 있다.

[0087] 또한, 본 발명의 일실시예에 따르면, 상기 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 동작 방법은 단계(S220)을 통해 상기 제1 공개키가 생성되면, 공개키 저장소에 상기 제1 공개키를 저장하는 단계를 더 포함할 수 있다.

[0088] 이때, 단계(S250)에서는 상기 제1 개인키로 복원하는 단계를 통해 상기 제1 개인키의 복원이 완료되면, 상기 복원된 제1 개인키에 대응하는 공개키로 검증용 공개키를 생성한 후 상기 검증용 공개키가 상기 공개키 저장소에 저장되어 있는 상기 제1 공개키와 일치하는지 여부를 확인하는 단계를 더 포함할 수 있다.

[0089] 이때, 상기 제1 전자 서명 값의 생성을 처리하는 단계는 상기 검증용 공개키가 상기 공개키 저장소에 저장되어 있는 상기 제1 공개키와 일치하는 것으로 확인되면, 상기 제1 원본 메시지를 상기 선정된 제1 해시 함수에 입력으로 인가하여 상기 제1 해시 값을 생성한 후 상기 제1 해시 값에 대해 상기 복원된 제1 개인키로 암호화를 수행하여 상기 제1 전자 서명 값의 생성을 처리할 수 있다.

[0090] 또한, 본 발명의 일실시예에 따르면, 상기 제1 차량의 데이터 통신 장치는 상기 공개키 배포 서버로부터 상기 제1 공개키가 상기 커넥티드 차량용 데이터 통신 장치에 대한 배포용 공개키로 수신되면, 메모리 상에 상기 제1 공개키를 저장할 수 있다.

[0091] 그리고, 상기 제1 차량의 데이터 통신 장치는 상기 제1 공개키가 상기 메모리 상에 저장된 이후, 상기 커넥티드 차량용 데이터 통신 장치로부터 상기 제1 원본 메시지와 상기 제1 전자 서명 값이 수신되면, 상기 메모리 상에 저장되어 있는 상기 제1 공개키를 기초로 상기 제1 전자 서명 값에 대한 복호화를 수행하여 복호화 값을 생성하고, 상기 제1 원본 메시지를 상기 선정된 제1 해시 함수와 동일한 해시 함수에 입력으로 인가하여 검증용 해시 값을 생성한 후 상기 복호화 값과 상기 검증용 해시 값이 서로 동일한 것으로 확인되면, 상기 제1 전자 서명 값에 대한 검증이 성공인 것으로 판단할 수 있다.

[0092] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 동작 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 동작 방법은 도 1을 이용하여 설명한 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0093] 본 발명의 일실시예에 따른 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 동작 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0094] 또한, 본 발명의 일실시예에 따른 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치의 동작 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 수행하

록 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.

[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 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0097] 100: 공개키 배포 서버

110: 전자 서명을 통한 차량 간 보안 통신을 지원하는 커넥티드 차량용 데이터 통신 장치

111: 원본 데이터 생성부 112: 키 쌍 생성부

113: 공개키 배포부 114: 복원부

115: 전자 서명부 116: 데이터 전송부

117: 난수 값 생성부 118: 부호어 생성부

119: 개인키 생성부 120: 공개키 생성부

121: 출력 값 생성부 122: 부호어 저장부

123: 복원용 출력 값 생성부 124: 부호어 복원부

125: 오류 정정부 126: 개인키 복원부

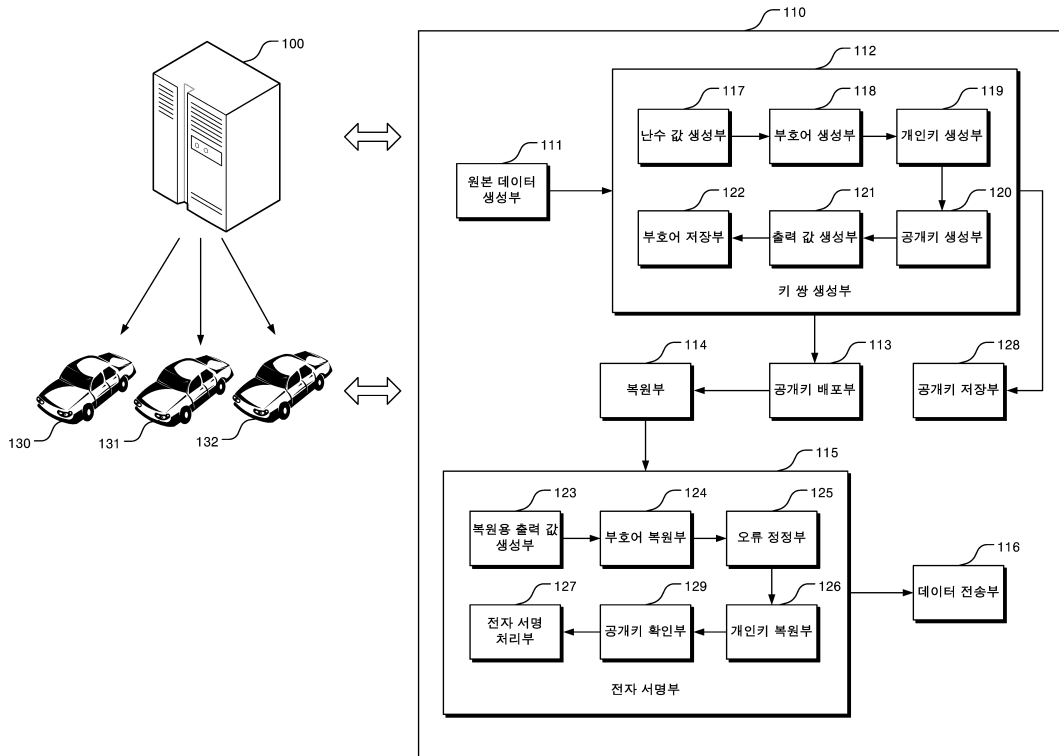
127: 전자 서명 처리부 128: 공개키 저장부

129: 공개키 확인부

130, 131, 132: 복수의 차량들

도면

도면1



도면2

