(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0093764
(43) 공개일자 2016년08월09일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) *H04L 9/12* (2006.01)
(52) CPC특허분류
H04L 9/0656 (2013.01)
H04L 9/12 (2013.01)
(21) 출원번호 10-2015-0014151
(22) 출원일자 2015년01월29일
심사청구일자 2015년01월29일

(71) 출원인
주식회사 아나스타시스
서울특별시 마포구 양화로8길 32-17, 누가빌딩5층 (서교동)
(72) 발명자
김윤규
경기도 용인시 처인구 금령로40번길 15-8 108호 (김량장동,청광그린빌라)
(74) 대리인
송봉식, 정삼영

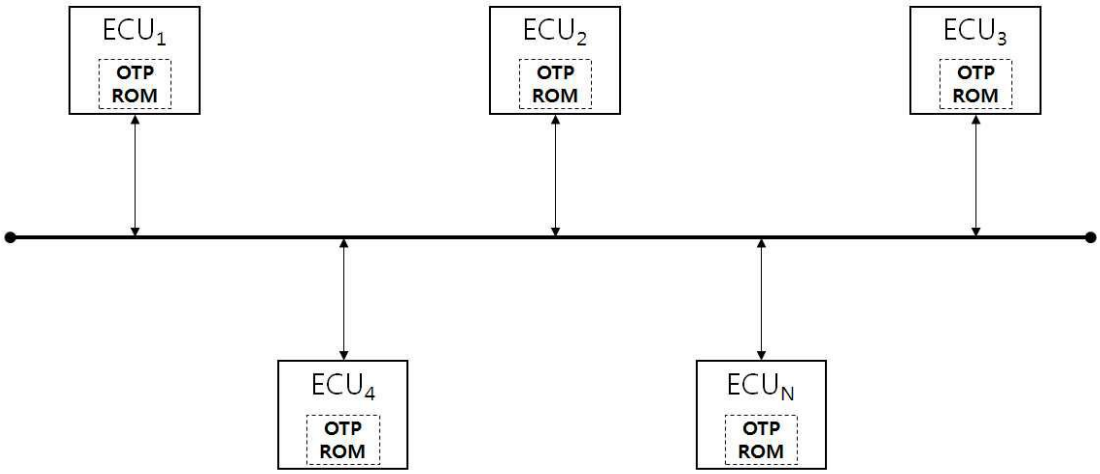
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **ＯＴＰ ＲＯＭ을 활용하는 ＥＣＵ 보안 통신 시스템**

(57) 요 약

ECU 보안 통신 시스템이 개시된다. 본 시스템은 하나 이상의 ECU를 포함하고, 각각의 ECU는 OTP ROM을 포함한다. 이러한 OTP ROM은 보안 통신을 위해 사용되는 비밀 데이터, 공개 데이터, 및 고정 데이터 등을 저장한다. 또한, OTP ROM은 상기 ECU에 장착되기 전에 데이터가 저장될 수도 있고, 장착된 후에 저장될 수도 있다.

대 표 도 - 도2



이 발명을 지원한 국가연구개발사업
과제고유번호 1711022465
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 방송통신융합미디어원천기술개발
연구과제명 자동차 전장 ECU간 보안전송기술 개발
기 여 율 1/1
주관기관 인포뱅크
연구기간 2014.04.01 ~ 2015.02.28

명 세 서

청구범위

청구항 1

ECU 보안 통신 시스템으로서,

하나 이상의 ECU를 포함하고,

상기 ECU 각각은 OTP ROM을 포함하는 것을 특징으로 하는 ECU 보안 통신 시스템.

청구항 2

제 1 항에 있어서, 상기 OTP ROM은 보안 통신을 위해 사용되는 비밀 데이터, 공개 데이터, 및 고정 데이터 등을 저장하는 것을 특징으로 하는 ECU 보안 통신 시스템.

청구항 3

제 1 항에 있어서, 상기 OTP ROM은 상기 ECU에 장착되기 전에 데이터가 저장되는 것을 특징으로 하는 ECU 보안 통신 시스템.

청구항 4

제 1 항에 있어서, 상기 OTP ROM은 상기 ECU에 장착된 후에 데이터가 저장되는 것을 특징으로 하는 ECU 보안 통신 시스템.

청구항 5

제 1 항에 있어서, 상기 ECU는 난수 생성기 및 암호화·복호화 알고리즘을 더 포함하고, 상기 난수 생성기는 암호키를 랜덤 생성하여 상기 OTP ROM에 저장하고, 상기 암호화·복호화 알고리즘은 상기 암호키를 이용하여 상기 OTP ROM에 저장되는 데이터를 암호화하고, 암호화된 데이터를 복호화하는 것을 특징으로 하는 ECU 보안 통신 시스템.

청구항 6

제 5 항에 있어서, 상기 OTP ROM, 상기 난수 생성기, 및 상기 암호화·복호화 알고리즘의 일부 또는 모두는 시스템온칩(SoC)에 실장되는 것을 특징으로 하는 ECU 보안 통신 시스템.

청구항 7

ECU의 보안 통신을 위한 시스템온칩(SoC)으로서,

암호키를 랜덤 생성하는 난수 생성기;

상기 암호키를 이용하여 비밀 데이터를 암호화하고, 암호화된 비밀 데이터를 복호화하는 암호화·복호화 알고리즘; 및

상기 암호화된 비밀 데이터, 및 상기 암호키를 저장하기 위한 OTP ROM을 포함하는 것을 특징으로 하는 ECU의 보안 통신을 위한 시스템온칩SoC.

청구항 8

제 7 항에 있어서, 상기 OTP ROM에 저장되는 데이터는 상기 암호화 키, 상기 암호화된 비밀 데이터, 공개 데이터, 및 고정 데이터 등을 포함하는 것을 특징으로 하는 ECU의 보안 통신을 위한 SoC.

청구항 9

OTP ROM을 포함하는 시스템온칩(SoC)에 비밀 데이터를 기록하는 방법으로서,

상기 SoC가 난수 생성기를 통해 랜덤하게 암호키를 생성하여 상기 OTP ROM에 저장하는 단계;

비밀 데이터가 입력된 때 상기 OTP ROM에 저장된 암호키를 이용하여 상기 비밀 데이터를 암호화하는 단계;

상기 암호화된 비밀 데이터를 상기 OTP ROM에 저장하는 단계를 포함하는 것을 특징으로 하는 OTP ROM을 포함하는 SoC에 비밀 데이터를 기록하는 방법.

청구항 10

OTP ROM을 포함하는 시스템온칩(SoC)으로부터 비밀 데이터를 판독하는 방법으로서,

상기 OTP ROM에 저장된 암호화된 비밀 데이터를 상기 OTP ROM에 저장된 암호키를 이용하여 복호화하는 단계를 포함하는 것을 특징으로 하는 OTP ROM을 포함하는 SoC으로부터 비밀 데이터를 판독하는 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 ECU 보안 통신 시스템에 관한 것이고, 더욱 상세하게는, OTP(One-Time Programmable) ROM을 이용한 ECU 보안 통신 시스템에 관한 것이다.

배 경 기 술

[0002] 최신 자동차들은 운전자와 승객에게 안전성과 편의성을 제공하기 위해 다양한 정보통신기술과 융합되고 있다. 자동차에 정보통신기술을 효율적으로 융합시키기 위해서는 ECU의 사용이 필수적으로 요구된다. 자동차 내부에 탑재되는 ECU는 도입 초기부터 지금까지 그 수요가 꾸준히 증가하여 최근에 개발되는 고급 자동차의 경우 약 70여개 이상의 ECU들이 자동차 내부에 탑재되고 있다. 이러한 ECU들은 서로 통신을 하며 데이터를 주고받는다. 이러한 통신에는 주로 CAN(Controller Area Network)이 사용되고 있으며, 최근에 CAN FD, FlexRay, LIN, MOST, Ethernet 등이 추가 되고 있다.

[0003] 도 1을 참조하면, 일반적으로 차량에 사용되는 ECU 통신 개념도가 도시되어 있다. 도시된 바와 같이, 여러 개의 ECU들은 하나의 네트워크로 구성되어 서로 데이터를 주고받는다. 그러나, 현재의 ECU 통신에는 어떠한 보안 기법이 적용되지 않고 있어 해킹에 취약하다. 이러한 ECU는 서로 간에 통신을 할 때 인증, 암호화 등의 보안 기능을 전혀 수행하지 않는다. 이렇기 때문에 ECU 통신을 해킹하는 것은 구조적으로 매우 간단하며 통신 패킷을 분석하는 작업만 완료되면 자동차는 순식간에 해킹이 된다. 따라서, 안전한 ECU 보안 통신 시스템에 대한 필요성이 존재한다.

[0004] 안전한 ECU 보안 통신을 하기 위해서는 암호 프로토콜이 설계되어야 하며, 암호 프로토콜은 하나 혹은 여러 개의 암호 알고리즘으로 구성되어진다. 이러한 암호 알고리즘은 각 알고리즘별로 사용하는 비밀 데이터(예: 비밀키), 공개데이터(예: 공개키)나 ECU마다 고유하게 사용하는 고정데이터(예: ID) 등이 있다. 이러한 데이터들은 외부에 유출되거나 수정, 삭제 등이 이루어지면 안 된다.

[0005] OTP ROM은 단 한번만 기록될 수 있는 형태의 ROM을 말한다. 데이터가 기록된 후에는 내부에 기록된 데이터는 안전하게 보관되며 외부에서는 읽을 수만 있게 된다. 따라서 OTP ROM을 ECU에서 암호 알고리즘의 비밀 데이터, 공개데이터나 고유하게 사용하는 고정데이터를 저장하는 보안 저장장치(Secure Storage)로 활용할 수 있다.

[0006] 예를 들어, 한국특허출원 제2012-0090279호는 CAN에서 데이터의 기밀성과 무결성을 보장하는 방법을 개시한다. 여기에, (a)CAN(Controller Area Networks)을 통해 데이터를 송신하는 ECU(Electronic Control Unit, 송신 ECU)와 상기 송신된 데이터를 수신하는 수신 ECU에 상기 데이터의 암호화키를 부여하는 단계; 및 (b)상기 송신 ECU와 상기 수신 ECU에 상기 데이터의 인증키를 부여하는 단계를 포함하는 CAN에서의 데이터의 기밀성과 무결성을 보장하는 방법이 개시되어 있다.

[0007] 한국특허출원 제2012-0070829호는 차량 네트워크의 메시지 무결성 체크 시스템 및 방법을 개시한다. 여기에, 각 ECU 간에 전송되는 메시지의 무결성 체크를 위한 체크섬 체크방법과 롤링카운트 체크방법을 결합할 수 있도록 메시지가 전송될 때마다 메시지 내에서 체크섬이 위치한 메시지 맵의 N번 바이트를 N+1번째 바이트로 위치 이동시킴으로써 메시지에서 무결성 체크를 위해 사용되는 비트를 감소시킬 수 있어 정해진 비트(예를 들면 64 bit)의 메시지에 보다 많은 정보를 담아 전송할 수 있는 차량 네트워크의 메시지 무결성 체크 시스템 및 방법이 개시되어 있다.

[0008] 한국특허출원 제2010-002137호는 CAN 프로토콜을 사용한 데이터 통신에서 데이터 메시지에 대한 무결성 확인 방법을 개시한다. 이는 하나의 제어 유니트에서 다른 제어 유니트로 CAN(Control Area Network) 통신 프로토콜을 사용하여 CAN 데이터를 송수신할 때 CAN 데이터의 무결성 체크 방법에 관한 것으로, 보다 상세하게는 송신측에서 동일한 전송 상태 데이터를 연속하여 보낸 후, 수신측에서 연속하여 수신한 상태 데이터를 비교하여 동일한 전송 상태 데이터가 수신되고 수신된 전송 상태 데이터가 상태의 변화를 의미할 때에만 수신된 데이터를 유효한 것으로 인식하는 CAN 프로토콜을 사용한 데이터 통신에서 데이터 메시지에 대한 무결성 확인 방법에 관한 것이다. 여기에, CAN 프로토콜을 사용한 데이터 통신에서 데이터 메시지에 대한 무결성 확인 방법은 타이머가 기설정된 타이머값의 3배 시간값에 이르렀는지를 확인하고, 상기 타이머가 기설정된 타이머값의 3배 시간값에 이르렀으면, 수신된 데이터 메시지를 CAN-Data-Array[2]에 저장하는 타이머값 3배수 종료 확인 단계와; 상기 타이머값 3배수 종료 확인 단계에서 타이머값 3배수가 종료되지 않았다면 타이머값 2배수가 종료되었는지를 확인하고, 상기 타이머가 기설정된 타이머값의 2배 시간값에 이르렀으면, 수신된 데이터 메시지를 CAN-Data-Array[1]에 저장하는 타이머값 2배수 종료 확인 단계와; 상기 타이머값 2배수 종료 확인 단계에서 타이머값 2배수가 종료되지 않았다면 타이머값이 종료되었는지를 확인하고,상기 타이머가 기설정된 타이머값에 이르렀으면, 수신된 데이터 메시지를 CAN-Data-Array[0]에 저장하는 타이머값 종료 확인 단계와; 상기 타이머값 3배수 종료 확인 단계에서 타이머값 3배수 종료가 확인되면, 상기 타이머값 3배수 종료 확인 단계에서 CAN-Data-Array[2]에 저장한 데이터 메시지와 상기 타이머값 2배수 종료 확인 단계에서 CAN-Data-Array[1]에 저장한 데이터 메시지가 같은지를 비교하고, 같은 메시지이면 CAN-Data-Array[1]에 저장한 데이터 메시지가 기설정된 데이터 값과 일치하는지를 확인하는 제 1 데이터 메시지 비교 단계와; 상기 제 1 데이터 메시지 비교 단계에서 비교하여 상호 다른 데이터 메시지 이면, 상기 타이머값 2배수 종료 확인 단계에서 CAN-Data-Array[1]에 저장한 데이터 메시지와 상기 타이머값 종료 확인 단계에서 CAN-Data-Array[0]에 저장한 데이터 메시지가 같은지를 비교하고, 같은 메시지이면 CAN-Data-Array[1]에 저장한 데이터 메시지가 기설정된 데이터 값과 일치하는지를 확인하는 제 2 데이터 메시지 비교 단계와; 상기 제 2 데이터 메시지 비교 단계에서 비교하여 상호 다른 데이터 메시지 이면, 상기 타이머값 3배수 종료 확인 단계에서 CAN-Data-Array[2]에 저장한 데이터 메시지와 상기 타이머값 종료 확인 단계에서 CAN-Data-Array[0]에 저장한 데이터 메시지가 같은지를 비교하고, 같은 메시지이면 CAN-Data-Array[0]에 저장한 데이터 메시지가 기설정된 데이터 값과 일치하는지를 확인하는 제 3 데이터 메시지 비교 단계와; 상기 제 1 데이터 메시지 비교 단계 또는 제 2 데이터 메시지 비교 단계 또는 제 3 데이터 메시지 비교 단계에서 데이터 메시지가 기설정된 데이터 값과 일치하는 경우에 데이터 메시지를 처리하는 데이터 메시지 처리 단계;를 포함하는 방법이 개시되어 있다. 이러한 AN 프로토콜을 사용한 데이터 통신에서 데이터 메시지에 대한 무결성 확인 방법은 CAN 프로토콜 통신을 사용하는 차량내 탑재 전자 제어 유니트간의 데이터 통신에서 송수신되는 데이터 메시지의 무결성을 보장할 수 있어, CAN 프로토콜 통신의 신뢰성을 높여 사고를 미연에 방지하는 효과가 있다.

[0009] 상기 특허출원 또는 특허들은 CAN 프로토콜 통신에서의 데이터 무결성을 향상시키기 위한 솔루션을 제공한다. 이는 ECU간 통신에 있어서, 데이터 오류로 인한 오작동을 방지하는데 도움을 줄 수 있다. 그러나, 외부로부터의 의도적인 해킹에는 여전히 취약하다.

[0010] 한국특허출원 제2005-0121296호는 차량용 네트워크를 이용한 보안 시스템을 개시한다. 이 시스템은 차량용 네트워크를 이용한 보안 시스템에 관한 것으로, 차량 내에 포함 구비되는 다수 유형의 전자 컨트롤 유니트(ECU)들이, 차량용 네트워크를 통해 연결 접속됨과 아울러, 차량 시동시, 상기 각 전자 컨트롤 유니트들간에 상호 보안 승인 절차를 수행한 후, 그 수행 결과에 따라, 제어 동작을 정상 수행하거나, 또는 중지시키는 것을 특징으로 한다. 캔(CAN) 네트워크를 이용하여, 각종 전자 컨트롤 유니트들간의 상호 보안 승인 동작을 수행함으로써, 임의의 전자 컨트롤 유니트 교체시, 도난 차량으로 간주하여, 정상적인 동작이 수행되지 않도록 하여, 차량 도난을 효율적으로 예방할 수 있게 된다.

[0011] 한국특허출원 제2010-0044419호는 인체 통신을 이용한 텔레매틱스 시스템, 인체 통신을 이용한 텔레매틱스 기능을 구비한 휴대 장치 및 인체 통신을 이용한 텔레매틱스 서비스 제공 방법을 개시한다. 더욱 상세하게는, 보안성 및 사용 편의성을 향상시킬 수 있는 인체 통신을 이용한 텔레매틱스 시스템, 인체 통신을 이용한 텔레매틱스 기능을 구비한 휴대 장치 및 인체 통신을 이용한 텔레매틱스 서비스 제공 방법이 개시된다. 이러한 인체 통신을 이용한 텔레매틱스 시스템은, 인체를 매질로 사용하는 인체 통신을 이용하여 적어도 하나의 휴대 장치로부터 인증키를 제공받고, 제공받은 인증키의 유효성 여부에 기초하여 도어(door)의 개폐를 제어하는 차량, 차량에 접촉된 사용자의 신체를 통해 차량에 제1 인증키를 전송하는 제1 휴대 장치 및 상기 차량에 접촉된 사용자의 신체를 통해 상기 차량에 제2 인증키를 전송하는 제2 휴대 장치를 포함하며, 상기 차량은 상기 제1 인증키 및 상기 제2 인증키의 유효성을 검사한 후, 상기 제1 및 제2 인증키가 모두 유효한 경우 상기 차량의 도어를 개방함으로

써, 텔레매틱스 서비스의 보안성 및 사용 편의성을 향상시킬 수 있다.

[0012] 한국특허출원 제2009-0083602호는 저전력 알에프아이디 통신을 이용한 자동차 사용자의 인증장치를 개시한다. 이는 저전력 RFID 통신을 이용한 자동차 사용자의 인증장치 및 인증방법에 관한 것이다. 이 원격제어기 및 송수신제어기를 이용한 원격 제어 장치는 자동차의 내부에 설치되는 유닛으로, 상기 원격제어기로 웨이크업 데이터를 전송하여 원격제어기로부터 인증데이터를 수신하여 인증을 수행한 뒤, 설치된 자동차에 대한 보안을 해제 또는 설정하도록 하기 위한 송수신제어기; 및 상기 자동차 사용자가 소지하며 상기 송수신제어기와 RFID 통신을 수행하는 유닛으로, 상기 송수신제어기로부터 웨이크업 데이터를 수신하여 상기 웨이크업 데이터에 대한 응답데이터를 전송하며, 이에 따른 상기 송수신제어기로부터의 근접 여부 확인을 위한 데이터를 수신하여 상기 근접 여부 확인을 위한 데이터에 대한 인증데이터를 전송하여 인증을 수행하는 원격제어기를 포함할 수 있다. 이에 의해, 웨이크업 데이터 송출에 대한 원격제어기의 응답신호를 통해 반응하도록 구성됨으로서 차량의 송수신제어기가 최소 전력을 유지할 수 있으며, 송수신제어기에 사용되는 전원(Battery)을 낮은 용량으로 사용할 수 있으며, 사용자가 자동차에 근접할 경우 인증을 통해 자동적으로 보안 및 잠금이 해제되며, 멀어지면 자동적으로 보안 및 잠금이 설정되도록 함으로써, 자동차의 안전 및 사용자의 안전을 유지할 수 있다. 뿐만 아니라, 설정된 인증데이터(인증 ID)를 갖고 있는 사용자만 자동차에 대한 인증을 수행할 수 있어 자동차 유지 및 관리에 효율적일 수 있다.

[0013] 한국특허출원 제2007-0132841호는 텔레매틱스와 스마트카드를 이용한 차량 인증 시스템을 개시한다. 이 시스템은 텔레매틱스와 스마트카드를 이용한 차량 인증 시스템에 관한 것으로서, 그 텔레매틱스와 스마트카드를 이용한 차량 인증 시스템은 고유의 식별번호를 각각 구비하며 상호 캔 통신으로 연동되는 부품부, 텔레매틱스 통신을 위하여 차량에 마련되며, 사용자정보를 제공하기 위한 스마트카드를 구비하고, 부품부와 캔 통신으로 연결된 통신부, 및 전송받은 사용자정보를 저장된 사용자정보와 대조하고, 인증된 경우에는 작동신호를 차량의 통신부로 내려주고 캔 통신을 이용하여 부품부의 각 부품을 활성화시키며, 인증에 실패한 경우에는 오프신호를 내려주어 부품부의 캔버스를 오프시킴으로써 각 부품을 비활성화시키는 데이터베이스 서버로 구성된다.

[0014] 한국특허출원 제2005-0120967호는 홍채 인식을 통한 차량 도난 방지 방법 및 그 시스템을 개시한다. 여기에, 홍채 인식을 통한 차량 도난 방지 방법 및 그 시스템에 관한 것으로, 운전자의 홍채 이미지를 추출하는 단계와, 상기 추출된 홍채 이미지를 인증 서버로 전달하는 단계와, 상기 전달된 홍채 이미지와 인증 서버에 미리 등록된 상기 운전자의 홍채 이미지를 비교하여 운전자 인증여부를 결정하는 단계와, 상기 결정된 운전자 인증여부를 텔레매틱스 장치에 전달하여 운행 가능 여부를 결정하는 단계를 포함하여 이루어지는 홍채 인식을 통한 차량 도난 방지 방법이 제공되어 있다.

[0015] 한국특허출원 제2005-0001452호는 전파식별시스템을 이용한 텔레매틱스 시스템의 도난 방지장치 및 방법을 개시한다. 이는 텔레매틱스 시스템에 관한 것으로, 특히 전파식별 시스템(Radio Frequency IDentification System: 이하 "RFID 시스템"이라 함)을 이용하여 차량의 도난을 감지하고 차량 소유주에게 차량의 도난을 알려주는 RFID 시스템을 이용한 텔레매틱스 시스템의 도난 방지 장치 및 방법에 관한 것이다. 이러한 텔레매틱스 시스템의 도난 방지 장치는 자동차키 시동 보안 암호를 가지는 전파식별 태그가 심어져 있는 자동차키와, 상기 자동차키의 삽입을 검출 시 상기 전파식별 태그의 자동차키 시동 보안 암호를 무선으로 읽어오는 전파식별 리더기를 구비하여 상기 읽혀진 상기 자동차키 시동보안 암호와 미리 저장되어 있는 자동차 시동 보안 암호를 비교하여 동일할 경우 시동을 걸 수 있는 시동 대기 모드를 설정하는 텔레매틱스 단말기를 포함한다.

[0016] 미국특허 US7,141,889는 생체 정보를 이용하는 자동차 컨트롤러 및 자동차 컨트롤러를 사용하는 시스템과 방법(Automobile controller using biological information, and system and method which use the automobile controller)를 개시한다. 이는 고도로 편리한 자동차 엔진 시작은 생체 정보를 이용하고, 엔진을 작동시킬 때 요구된 보안 기능을 제공하는 개별적 인증 기기를 사용함과 동시에, 생체 정보를 받기 위한 센서를 보호한다. 엔진 시동 시스템은 자동차의 상태를 제어하기 위한 점화 스위치; 점화 스위치의 상태를 바꾸기 위한 키; 생체 정보를 등록하기 위한 위치 정합 키; 엔진을 작동시키기 위한 스위치; 생체 정보를 입력하기 위한 센서; 생체 정보를 저장하기 위한 장치; 저장된 생물학적 정보를 가진 입력된 생체 정보를 대조하기 위한 순서맞춤 장치; 그리고 인증 기기의 센서를 커버링하기 위한 덮개를 포함한다.

[0017] 유럽특허출원 EP2005-106879는 차량을 위한 텔레메틱 보안 시스템(Telematic security system for a vehicle)을 개시한다. 이러한 차량을 위한 텔레메틱 보안 시스템이은 차량의 안에 배치될 수 있는 텔레메틱 장치 (10)를 포함하고, 규정된 통신 프로토콜에 따라 디지털 무선 통신을 수신하고 전송하기 위한 유닛(30) 및 식별 코드의 리더기(32), 외부 신원확인 장치로서 고정 장치 (100), 차량의 안에 배치될 수 있고 외부 인증 장치(120)에

의해 전송된 식별 신호를 수신하기 위한 수단 (111)과 연관된 전자 제어 장치 (110)를 포함한다. 제어 장치 (110)는 식별 신호를 수신하기 위한 장애의 결과로서, 차량의 출발 또는 구동을 방지할 수 있다. 송수신부(30)는 외부에게 경보 신호를 전송하기 위한 제어 장치(110)에 연결된다.

[0018] 상기 특허출원 또는 특허들은 자동차의 물리적 보안성을 강화하는 솔루션, 즉, 자동차 도난 방지를 위한 솔루션을 제공하고 있다. 그러나, 자동차 내부의 ECU간의 통신에 대한 외부로부터의 해킹에는 여전히 취약할 수 밖에 없다.

[0019] 미국특허출원 US2013-084495는 방법과 차량 그리고 무선 통신 기기 또는 키폽 사이의 보안 및 승인을 받은 커뮤니케이션을 위한 시스템(METHOD AND SYSTEM FOR SECURE AND AUTHORIZED COMMUNICATION BETWEEN A VEHICLE AND WIRELESS COMMUNICATION DEVICES OR KEY FOBS)을 개시한다. 더욱 상세하게는, 무선 통신 기기 (또는 단말 디바이스)과 중심 모듈을 가지는 차량과 키 프로비져닝 서버를 포함하는 시스템이 제공되어 있다. 키 프로비져닝 서버는 communicatively 무선 커넥션을 통해 무선 통신 기기와 중심 모듈에 결합된다. 중심 모듈은 현재 통신 세션을 초기화하기 위한 무선 통신 기기와의 무선 커넥션을 설치할 수 있다. 무선 커넥션이 중심 모듈로 설치될 때, 무선 통신 기기는 일시적 보안정보 (예를 들면, 공개 키 그리고/또는 전자 인증서)을 요구하기 위해 요구 메시지를 전달시킨다. 키 프로비져닝 서버는 후에 요구 메시지에 반응하여 일시적 보안정보를 무선 통신 기기 그리고/또는 중심 모듈에게 제공할 수 있다. 일시적 보안정보는 후에 무선 통신 기기와 중심 모듈 사이의 커뮤니케이션을 암호화하는데 사용될 수 있다.

[0020] 미국특허출원 US2011-985969는 외부 장치와 게이트웨이를 통해 모터 차량에서 통신망에서 장치에 접근하는 방법(Method of accessing a device in a communication network in a motor vehicle via an external device and gateway)을 개시한다. 여기에, 외부 장치를 통해 모터 차량에서 통신 네트워크에서 장치에 접근하는 방법은 기술되고, 여기서 소프트웨어적 요소는 외부 장치에 의해 통신 네트워크에서 장치의 컨트롤을 허용하기 위한 통신 네트워크에서 장치에 대한 승인된 액세스의 경우에 외부 장치로 전송된다. 게이트웨이는 액세스가 가능하고, 요구된 장치로 또는 시스템 매니저를 통해 또하나의 직접적으로 점검하는 것인지에 점검한다. 제어될 외부 장치와 장치 사이의 커뮤니케이션에서 보안은 외부 장치로 전사된 추가적 암호화 그리고/또는 소프트웨어적 요소의 규정된 유효기간에 의해 이루어질 수 있다. 제어되기 위한 장치를 위한 어떤 소프트웨어적 요소도 있지 않으면, 그러한 소프트웨어적 요소는 장치에서 저장된 제어 모듈과 데이터의 사용으로 생성될 수 있다. IEEE 1394에 따른, 버스 시스템은 예를 들어 통신 네트워크로서 사용될 수 있다.

[0021] 미국특허 US8,819,414는 차량 대 차량 통신망에서 위협 완화 방법(Threat mitigation in a vehicle-to-vehicle communication network)을 개시한다. 차량에 대한 인증서 폐지 목록 (CRL)를 차량 대 차량 통신 시스템에서 획득하기 위한 방법이 제공된다. 휴대용 보안 유니트는 차량을 위한 보안 오퍼레이션에 접근하기 위해 제공된다. 휴대용 보안 유니트는 통신망에 접속하는 장치에 연결된다. 통신망은 업데이트된 CRL을 공개하기 위한 인증 기관과 연결된다. 업데이트된 CRL은 인증 기관에서부터 휴대용 보안 유니트까지 다운로드된다. 나중에, 사용자가 차량에 엔터링할 때, 통신 링크는 휴대용 보안 유니트와 차량 프로세서 유니트 사이에 설치된다. 상호 인증은 휴대용 보안 유니트와 차량 처리부 사이에 교환된다. 휴대용 보안 유니트에서 저장된 업데이트된 CRL은 성공적 상호 인증에 반응하여 차량 통화 시스템의 메모리로 다운로딩된다.

[0022] 미국특허 US8,230,215는 차량 대 차량 통신망에서 차량에 다중 인증 증명서를 할당하기 위한 방법(Method for allocating multiple authentication certificates to vehicles in a vehicle-to-vehicle communication network)을 개시한다. 더욱 상세하게는, 커뮤니케이션을 보호하기 위해 PKI 보안 방법을 이용하는 차량 대 차량 통신망에서 그리고 PKI 암호화가 어느 것을 이용하는 것에서 양쪽 비밀 키와 공개적으로 배포키를 가지는 인증 기관, 통신망에서 각각 차량에 할당되는 각각 차량을 위한 다중 인증서를 배정하는 방법이 제공된다. 이 방법은 통신망에서 유일한 비밀키 k를 각각 차량에 할당하는 단계를 포함한다. 인증 기관은 후에 다수의 공개 키를 생성하고 각각 차량과 각각 암호화 쌍을 위한 개인키 암호화 쌍은 인덱스 i와 관련된다. 다수의 증명서는 후에. 특별한 차량에 할당된 모든 암호화 쌍이 그 차량에 해당한 비밀키 k에 의해 리보크되도록 비밀키를 포함하는 폐지 목록은 인증 기관에 의해 유지된다.

[0023] 상기 특허출원 또는 특허들은 차량과 차량, 또는 차량 내부 시스템과 외부 장치간의 통신에 관한 것이다. 따라서, 이들은 차량 내부의 ECU간의 통신 보안에 대한 솔루션이 되지 못한다.

[0024] 한국특허출원 제2012-0148579호는 차량용 통신 네트워크의 보안 강화 장치 및 방법을 개시한다. 수신 장치 및 게이트웨이 모듈을 포함하는 차량용 네트워크의 보안 강화 장치로서, 상기 게이트웨이 모듈은, 수신 장치가 연결된 채널을 통하여 수신된 제1 메시지 및 상기 제1 메시지가 암호화된 제2 메시지 중 수신 장치의 유효성을 판

단하기 위하여 상기 제2 메시지를 복호화하여 제3 메시지를 생성하는 복호화부; 상기 제1 메시지와 상기 제3 메시지의 동일성 여부를 판단하여 상기 제1 메시지와 상기 제3 메시지의 동일성이 인정되면 상기 수신 장치가 유효성이 있는 설정된 수신 장치임을 확인한 후, 보안성을 검증하기 위하여 상기 제1 메시지가 설정된 메시지인지 여부를 판단하는 제어부; 및 상기 제1 메시지가 설정된 메시지로 확인되어 상기 보안성이 검증되면 상기 제1 메시지를 연결된 복수의 채널 중 설정된 어느 하나의 채널로 라우팅하는 라우팅부를 포함하는 차량용 통신 네트워크의 보안 강화를 위한 장치 및 방법이 개시되어 있다.

[0025] 한국특허출원 제2012-0148223호는 차량용 네트워크의 보안 메시지 송수신 장치 및 방법을 개시한다. 여기에, 적어도 둘 이상의 ECU를 포함하는 차량용 네트워크의 보안 메시지 송수신 장치로서, 상기 적어도 둘 이상의 ECU 중 제1 ECU는, 상기 적어도 둘 이상의 ECU 중 제2 ECU로 전송하고자 하는 제1 데이터 중 암호화하고자 하는 제2 데이터를 제1 테이블에 입력하기 위하여, 상기 제2 데이터의 비트 수 만큼의 난수를 발생하는 난수 발생부; 상기 발생된 난수를 이용하여 상기 제2 데이터를 설정된 순서에 따라 상기 제1 테이블의 설정된 위치에 입력하여 제2 테이블을 생성하는 테이블 생성부; 상기 발생된 난수를 암호화하는 암호화부; 및 상기 제2 테이블과 상기 암호화된 난수를 상기 제2 ECU로 전송하는 통신부를 포함하는 차량용 네트워크의 보안 메시지 송수신 장치 및 방법이 개시되어 있다.

[0026] 상기 특허출원 또는 특허들은 차동자 내의 통신 네트워크에 대한 보안 방법을 제공하고 있다. 그러나, 외부로부터의 접근성 차단 및 내부 데이터의 완벽한 보안이 보장되지 않아서, 외부로부터의 해킹에 대한 완벽한 솔루션이 되지 못하고 있는 실정이다.

[0027] 따라서, 외부로부터의 해킹에 안전한 ECU 보안 통신 솔루션에 대한 필요성이 존재한다.

발명의 내용

해결하려는 과제

[0028] 본 발명은 해킹에 안전한 ECU 보안 통신 시스템을 구축하고자 한다.

과제의 해결 수단

[0029] 본 발명의 하나의 형태로서, ECU 보안 통신 시스템이 제공된다. 본 시스템은 하나 이상의 ECU를 포함하고, 각각의 ECU는 OTP ROM을 포함한다.

[0030] 이러한 OTP ROM은 보안 통신을 위해 사용되는 비밀 데이터, 공개 데이터, 및 고정 데이터 등을 저장할 수 있다.

[0031] 이러한 OTP ROM은 ECU에 장착되기 전에 데이터가 저장될 수 도 있고, 장착된 후에 저장될 수도 있다.

[0032] 또한, ECU는 난수 생성기 및 암호화·복호화 알고리즘을 더 포함하는 것이 바람직할 수 있다. 난수 생성기는 암호키를 랜덤 생성하여 OTP ROM에 저장하고, 암호화·복호화 알고리즘은 상기 암호키를 이용하여 OTP ROM에 저장되는 데이터를 암호화하고, 암호화된 데이터를 복호화한다.

[0033] 바람직하게는, OTP ROM, 난수 생성기, 및 암호화·복호화 알고리즘은 시스템온칩(SoC)에 실장될 수 있다.

[0034] 본 발명의 다른 형태로서, ECU의 보안 통신을 위한 시스템온칩(SoC)이 개시된다. 본 SoC는 암호키를 랜덤 생성하는 난수 생성기; 상기 암호키를 이용하여 데이터를 암호화하고, 암호화된 데이터를 복호화하는 암호화·복호화 알고리즘; 및 상기 암호화된 데이터 및 상기 암호키를 저장하기 위한 OTP ROM을 포함한다.

[0035] OTP ROM에 저장되는 데이터는 보안 통신을 위해 사용되는 비밀 데이터, 공개 데이터, 및 고정 데이터 등을 포함할 수 있다.

[0036] 본 발명의 또 다른 형태로서, OTP ROM을 포함하는 시스템온칩(SoC)에 비밀 데이터를 기록하는 방법이 제공된다. 본 방법은 SoC가 난수 생성기를 통해 랜덤하게 암호키를 생성하여 OTP ROM에 저장하는 단계; 비밀 데이터가 입력된 때 상기 OTP ROM에 저장된 암호키를 이용하여 비밀 데이터를 암호화하는 단계; 암호화된 비밀 데이터를 OTP ROM에 저장하는 단계를 포함한다.

[0037] 본 발명의 또 다른 형태로서, OTP ROM을 포함하는 시스템온칩(SoC)으로부터 비밀 데이터를 판독하는 방법이 제공된다. 본 방법은 OTP ROM에 저장된 암호화된 비밀 데이터를 OTP ROM에 저장된 암호키를 이용하여 복호화하는 단계를 포함한다.

발명의 효과

[0038] 현재 생산되는 차량은 각종 전자제어 시스템을 운영하기 위해 ECU간 통신을 수행한다. 하지만 차량 내부의 통신은 어떠한 보안 기법도 적용되어 있지 않기 때문에 해킹에 무방비 상태로 노출되어있다. 악의적인 공격자는 이런 특성을 이용하여 차량을 임의로 제어할 수 있다.

[0039] 본 발명은 OTP ROM을 활용한 ECU 보안 통신 시스템을 제공하여, 해킹으로부터 안전한 차량 내부 네트워크 구축을 가능하게 한다.

도면의 간단한 설명

[0040] 이제, 아래의 도면을 참조하여 상세한 설명이 제공된다.

도 1은 종래기술의 ECU 통신 개념도이다.

도 2는 본 발명의 하나의 실시예에 따른 ECU 통신 개념도이다.

도 3은 본 발명의 하나의 실시예에 따른 ECU 보안 통신 시스템용 SoC를 개략적으로 도시하는 블록도이다.

도 4는 도 3에 도시된 SoC를 이용하는 본 발명의 다른 실시예에 따른 ECU 통신 개념도이다.

발명을 실시하기 위한 구체적인 내용

[0041] 도 2는 본 발명의 하나의 실시예에 따른 ECU 통신 개념도이다. 본 실시예에서, 각각의 ECU는 OTP ROM를 포함한다. 각 ECU 내부에 장착된 OTP ROM에는 보안 통신을 하기 위해 사용되는 비밀 데이터, 공개데이터, 고정데이터 등이 저장될 수 있다.

[0042] OTP ROM은 ECU에 장착되기 전 또는 장착된 후에 데이터가 기록될 수 있다. 이 때 기록되는 데이터는 ECU에서 보안 통신을 하기 위해 사용되는 데이터들로써 비밀 데이터(예: 비밀키 등), 공개데이터(예: 공개키 등), 고정데이터(예: ID 등) 등이 있다.

[0043] 이러한 OTP ROM은 ECU에 장착된다. OTP ROM 내부에 저장된 데이터는 ECU 내부 프로그램(예: 펌웨어(firmware))을 통해서만 접근이 가능하며, 외부에서는 접근이 불가능하다. 또한 OTP ROM은 물리적으로 한 번만 기록이 가능하기 때문에 재기록(Re-writing)이 될 수 없다. 따라서, 이러한 ECU를 이용한 통신은 외부의 해킹으로부터 안전하다.

[0044] OTP ROM에 저장된 비밀 데이터(또는 암호화된 비밀 데이터), 공개데이터, 고정데이터 등을 활용하여 ECU간 보안 통신이 수행된다. 이 때 보안 통신 프로토콜에는, 제한하지 않는 예로서, 공개키암호 알고리즘(예: RSA 등), 대칭키암호 알고리즘(예: AES 등), 일방향해시 알고리즘(예: SHA-1 등), MAC(Message Authentication Code) 알고리즘(예: HMAC 등) 등이 사용될 수 있다.

[0045] 도 3은 본 발명의 하나의 실시예에 따른 ECU 보안 통신 시스템용 SoC를 개략적으로 도시하는 블록도이다. 도시된 바와 같이, SoC는 난수 생성기, 암호화·복호화 알고리즘, 및 OTP ROM을 포함한다.

[0046] 본 실시예에서는, 추가적으로 OTP ROM에 저장되는 데이터 중에서 비밀 데이터가 암호화되어 저장 될 수 있다. 이 때 사용되는 암호키(대칭키)는 난수생성기에 의해 랜덤하게 생성되어 OTP ROM에 저장된다. 암호화·복호화 알고리즘은 OTP ROM에 저장된 이러한 암호키를 이용하여 비밀 데이터를 암호화한다. 암호화된 비밀 데이터는 OTP ROM에 저장된다.

[0047] 도 4는 도 3에 도시된 SoC를 이용하는 본 발명의 다른 실시예에 따른 ECU 통신 개념도이다. 도시된 바와 같이, 각각의 ECU는 도 3에 도시된 SoC를 포함한다. 앞서 설명한 바와 같이, SoC 내의 OTP ROM은 암호키, 암호화된 비밀 데이터(예: 비밀키 등), 공개데이터(예: 공개키 등), 고정데이터(예: ID 등)를 포함한다. 각각의 ECU는 이러한 데이터를 이용하여 서로 보안 통신할 수 있다. 이 때 보안 통신 프로토콜에는, 제한하지 않는 예로서, 공개키암호 알고리즘(예: RSA 등), 대칭키암호 알고리즘(예: AES 등), 일방향해시 알고리즘(예: SHA-1 등), MAC(Message Authentication Code) 알고리즘(예: HMAC 등) 등이 사용될 수 있다. 본 실시예에 따른 도 3의 SoC를 포함하는 ECU 간의 통신은 비밀 데이터가 암호화되어 있으므로 도 2의 경우에 비해 한층 더 높은 보안 수준을 달성할 수 있다.

[0048] 이러한 알고리즘은 컴퓨터 소프트웨어, 프로그램 코드, 및/또는 명령어를 포함할 수 있다. 또한 이러한 컴퓨터

소프트웨어, 프로그램 코드는 임의의 시간 간격 동안 계산하기 위해 사용되는 디지털 데이터를 포함하는 컴퓨터 컴포넌트, 디바이스, 및 기록 매체; 램(RAM)으로 알려진 반도체 저장부; 보통 하드 디스크, 테이프, 드럼, 카드 및 다른 타입과 같은 자기 저장부의 형태의 광 디스크와 같은 보다 영구 저장을 위한 대용량 저장부; 프로세서 레지스터, 캐시 메모리, 휘발성 메모리, 비휘발성 메모리; CD, DVD와 같은 광학 저장부; 플래시 메모리(예를 들어, USB 스택 또는 키), 플로피 디스크, 자기 테이프, 페이퍼 테이프, 펀치 카드, 독립형 램 디스크, 집드라이브, 외장형 대용량 저장부, 오프라인등과 같은 이동식 매체; 동적 메모리, 정적 메모리, 기록/쓰기 저장부, 변하기 쉬운(mutable) 저장부, 읽기 전용 저장부, 램, 순차 접근 저장부, 로케이션 어드레스어블, 파일 어드레스어블, 콘텐츠 어드레스어블, 네트워크 부착 저장부, 샌(storage area network), 바코드, 자기 잉크등과 같은 다른 컴퓨터 메모리를 포함할 수 있는 기계 판독가능 매체에 저장되고 및/또는 접근될 수 있다.

[0049] OTP ROM이 포함된 SoC에 비밀 데이터가 기록되는 단계는 다음과 같다. SoC 내부의 OTP ROM에 비밀 데이터를 기록할 때에 SoC는 내부 난수생성기를 통해 랜덤한 암호키를 생성하여 OTP ROM에 저장한다. 암호키가 생성된 후에 입력된 비밀 데이터를 암호키로 암호화하여 생성된 암호화된 비밀 데이터를 OTP ROM에 저장한다.

[0050] OTP ROM이 포함된 SoC에서 비밀 데이터를 읽는 단계는 다음과 같다. ECU 내부 프로그램에서 SoC 내부 OTP ROM에 기록된 비밀 데이터를 읽을 때에 SoC는 OTP ROM에 저장된 암호키로 암호화된 비밀 데이터를 복호화하여 생성된 비밀 데이터를 ECU 내부 프로그램에 전달한다.

[0051] 상술된 실시예는 예로서 제공된 것일 뿐이며, 본 발명은 본 명세서에 도시되고 서술된 것으로 한정되지 않음을 이해해야 한다.

[0052] 예컨대, 상기 설명에서는 난수생성기, 암호화·복호화 알고리즘, OTP ROM이 SoC에 포함된 구성이 설명되었다. 그러나, 난수생성기, 암호화·복호화 알고리즘, OTP ROM는 ECU 내에서 별도의 부품으로서 포함될 수도 있다. 또한, 난수생성기, 암호화·복호화 알고리즘, OTP ROM 중 일부는 ECU 내부의 임의의 회로 내에 포함되고, 나머지는 SoC에 포함될 수도 있다. 또한, 난수생성기, 암호화·복호화 알고리즘, 및 OTP ROM 중 일부 또는 모두가 하나의 모듈로 제공될 수도 있다. 예컨대, 난수 생성기 및 암호화·복호화 알고리즘이 하나의 모듈로 제공될 수 있다.

[0053] 또한, 소프트웨어 또는 하드웨어 엔지니어링 실시에 따라, 묘사된 요소 및 그 기능은 모놀리식 소프트웨어 구조로서, 독립형 소프트웨어 모듈로서, 또는 외부 루틴, 코드, 서비스등을 채용하는 모듈로서 저장된 프로그램 명령어를 실행할 수 있는 프로세서를 갖는 컴퓨터 실행가능 매체를 통해 기계에서 구현될 수 있고, 이러한 모든 구현은 본 발명의 범위 안에 있을 수 있다. 이러한 기계의 예는 퍼스널 디지털 어시스턴트, 랩탑, 퍼스널 컴퓨터, 모바일 폰, 다른 휴대형 컴퓨팅 장치, 의료 기기, 유무선 통신 장치, 트랜스듀서, 챕, 계산기, 위성, 태블릿 PC, 전자책, 개지트(gadget), 전자 장치, 인공 지능을 갖는 장치, 컴퓨팅 장치, 네트워킹 기기, 서버, 라우터등을 포함할 수 있지만 이에 제한되는 것은 아니다. 또한, 블록도 또는 임의의 다른 논리 컴포넌트에 표현된 요소는 프로그램 명령어를 실행할 수 있는 기계에서 구현될 수 있다. 따라서, 상기 도면 및 설명이 개시된 시스템의 기능적 특징을 제시하고 있지만, 분명히 언급하거나 본문으로부터 분명하지 않으면 이러한 기능적 특징을 구현하기 위한 소프트웨어의 특정 설계도 이러한 설명으로부터 추론되어서는 안된다. 마찬가지로, 상술된 다양한 단계는 변하될 수 있고 이러한 단계의 순서는 여기에 개시된 기술의 특정 적용에 따라 조정될 수 있다. 이러한 변형 및 수정은 본 발명의 범위에 포함되어 있다. 따라서, 다양한 단계를 위한 순서의 설명은 특정 적용에 의해 요구되거나, 분명히 언급하거 본문으로부터 분명하지 않으면, 이러한 단계를 위한 특정 실행 순서를 필요로 하지 않는 것으로 이해해야 한다.

[0054] 상술된 방법 및/또는 이와 연관된 단계는 하드웨어, 소프트웨어 또는 특정 적용에 적절한 하드웨어 및 소프트웨어의 임의의 조합으로 구현될 수 있다. 이러한 하드웨어는 범용 컴퓨터 및/또는 전용 컴츄팅 장치 또는 특정 컴퓨팅 장치 또는 특정 컴퓨팅 장치의 특정 특징 또는 컴포넌트를 포함할 수 있다. 이러한 프로세스는 내부 및/외부 메모리와 함께, 마이크로프로세서, 마이크로컨트롤러, 내장된 마이크로컨트롤러, 프로그래머블 디지털 신호 프로세서 또는 다른 프로그래머블 장치중 하나 이상에서 구현될 수 있다. 이러한 프로세스는 또한, 또는 대신에 주문형 집적 회로, 프로그래머블 게이트 어레이, 프로그래머블 어레이 로직, 또는 전자 신호를 처리하도록 구성될 수 있는 임의의 다른 장치 또는 장치의 조합에서 구현될 수 있다. 또한, 이러한 프로세스의 하나 이상은 기계 판독가능 매체에서 실행될 수 있는 컴퓨터 실행가능 코드로서 구현될 수 있다는 것을 이해할 것이다.

[0055] 컴퓨터 실행가능 코드는 C와 구조적 프로그래밍 언어, C++와 같은 객체 지향 프로그래밍 언어, 또는, 프로세서, 프로세서 구조의 이질적인 조합은 물론 상기 장치중 하나, 또는 상이한 하드웨어 및 소프트웨어의 조합, 또는

프로그램 명령어를 실행할 수 있는 임의의 다른 기계에 저장되거나, 컴파일링되거나, 해석되어 실행될 수 있는 (어셈블리 언더, 하드웨어 기술 언어, 및 데이터베이스 프로그래밍 언어 및 기술을 포함하는) 임의의 다른 고레벨 또는 저레벨의 프로그래밍 언어를 사용하여 생성될 수 있다.

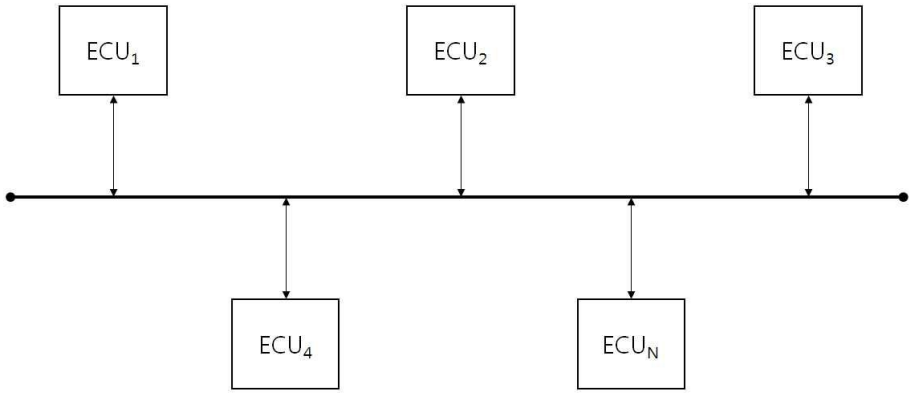
[0056] 따라서, 하나의 특징에서, 상술된 방법 및 그 조합은 하나 이상의 컴퓨팅 장치에서 실행될 때 단계를 실행하는 컴퓨터 실행가능 코드로 구현될 수 있다. 다른 특징에서, 이러한 방법은 단계를 실행하는 시스템에서 구현될 수 있고, 다수의 방식으로 장치들에 분산될 수 있거나, 이러한 기능 모두가 전용, 독립형 장치 또는 다른 하드웨어에 통합될 수 있다. 다른 특징에서, 상술된 프로세스와 연관된 단계를 실행하기 위한 수단은 상술된 하드웨어 및/또는 소프트웨어중 하나를 포함할 수 있다. 이러한 모든 치환 및 조합은 본 발명의 범위 내에 있다.

[0057] 또한, 본 명세서(특히 청구범위)의 용어는 달리 특별히 지시하지 않으면 단수 및 복수 모두를 포함하도록 되어 있다. 용어 "포함하는"은 달리 언급하지 않으면 개방형 용어(즉, "포함하지만 이에 제한되지 않는" 의미를 갖는다)로 이해해야 한다. 여기의 값의 범위의 설명은 달리 언급되지 않으면, 단지 범위 내에 있는 각 별개의 값을 개별적으로 언급하는 약기 방법으로서 되어 있고, 각 개별적인 값은 개별적인 여기에 열거되는 것처럼 본 명세서에 통합되어 있다. 여기에 기술된 모든 방법은 달리 언급되거나 달리 분명히 말하지 않으면 임의의 적절한 순서로 실행될 수 있다. 여기에 제공된, 임의의 예 및 모든 예, 또는 예시 언어(예를 들어, "와 같은")는 본 명세서를 보다 잘 설명하기 위해 사용되었고 달리 언급되지 않으면 본 명세서의 범위를 제한하지 않는다. 본 명세서의 어떤 언어도 임의의 청구되지 않은 요소를 본 발명의 실시에 필수적인 것을 가리키는 것으로 해석해서는 안된다.

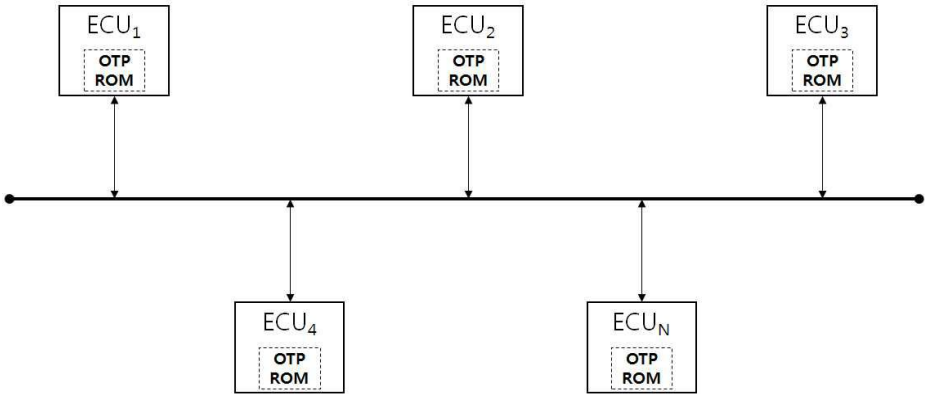
[0058] 상기 기록된 설명에 의해 당업자가 최상의 모드로 생각되는 것을 사용할 수 있지만, 당업자는 그 변형, 조합, 및 특정 실시예, 방법, 및 예의 등가를 이해할 것이다. 따라서, 본 명세서는 상술된 실시예, 방법, 및 예에 의해 제한되지 않고, 본 발명의 범위 및 정신 내의 모든 실시예 및 방법에 의해 한정되어야 한다.

도면

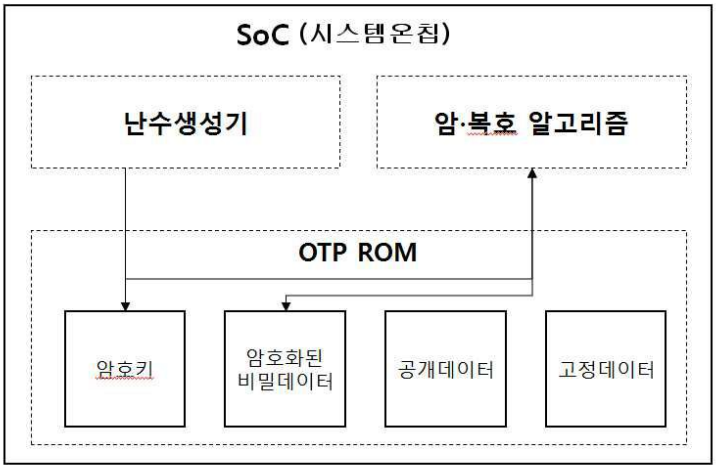
도면1



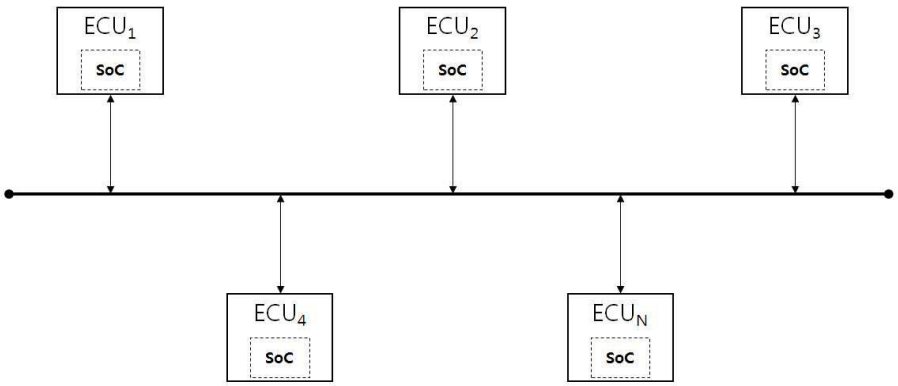
도면2


ECU1
OTP ROM
ECU2
OTP ROM
ECU3
OTP ROM
ECU4
OTP ROM
ECUN
OTP ROM

도면3


SoC (시스템온칩)
난수생성기
암·복호 알고리즘
OTP ROM
암호키
암호화된 비밀데이터
공개데이터
고정데이터

도면4


ECU1
SoC
ECU2
SoC
ECU3
SoC
ECU4
SoC
ECUN
SoC