

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2016-0058290 (43) 공개일자 2016년05월25일
(51) 국제특허분류(Int. Cl.) G06K 19/073 (2006.01) G06K 19/077 (2006.01)		(71) 출원인 고려대학교 산학협력단 서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(21) 출원번호 10-2014-0158701		(72) 발명자 김현민 서울 성북구 길음로 118, 414동 1801호 (길음동, 길음뉴타운) 홍석희 서울특별시 도봉구 마들로 859-19, 103동 107호 (도봉동, 한신아파트)
(22) 출원일자 2014년11월14일 심사청구일자 2014년11월14일		(74) 대리인 특허법인충현

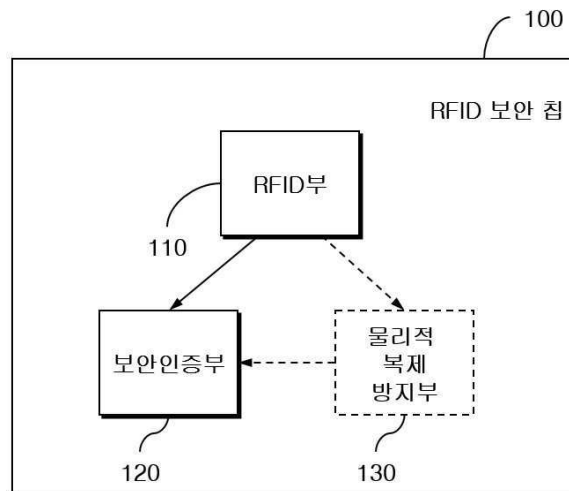
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 타원곡선 암호화 기반의 복제 불가능한 RFID 보안 칩

(57) 요약

본 발명은 RFID 칩에 관한 것으로, 장착된 장치의 식별정보를 저장하는 RFID부, 및 타원곡선암호를 이용하여 상기 식별정보를 암호화하거나 객체 인증을 수행하는 보안인증부를 포함함으로써, RFID 칩에 대한 안정적인 보안이 가능하다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호 NIPA-2014-H0301-14-1004

부처명 미래창조과학부

연구관리전문기관 정보통신산업진흥원

연구사업명 ITRC

연구과제명 제어시스템 보안 연구

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2014.01.01 ~ 2014.12.31

명세서

청구범위

청구항 1

RFID 칩에 있어서,
장착된 장치의 식별정보를 저장하는 RFID부; 및
타원곡선암호를 이용하여 상기 식별정보를 암호화하거나 객체 인증을 수행하는 보안인증부를 포함하는 RFID 칩.

청구항 2

제 1 항에 있어서,
상기 보안인증부는,
유한체 연산부, 모듈러 연산부, 및 산술 연산부를 포함하는 것을 특징으로 하는 RFID 칩.

청구항 3

제 1 항에 있어서,
상기 보안인증부는,
모듈레이터 산술논리연산장치부(MALU)를 포함하는 것을 특징으로 하는 RFID 칩.

청구항 4

제 1 항에 있어서,
상기 보안인증부는,
상기 RFID부에 저장된 타원곡선암호 파라미터를 이용하여 암호화를 수행하는 것을 특징으로 하는 RFID 칩.

청구항 5

제 1 항에 있어서,
상기 식별정보에 물리적 복제 방지를 수행하는 물리적 복제 방지부를 더 포함하는 RFID 칩.

청구항 6

제 5 항에 있어서,
상기 물리적 복제 방지부는,
난수, 난수를 위한 씨드(SEED), 또는 랜덤 노이즈 중 하나 이상을 발생시키는 것을 특징으로 하는 RFID 칩.

청구항 7

제 5 항에 있어서,
상기 물리적 복제 방지부는,
정적 램(SRAM) 방식, 글리치(Glitch) 방식, 또는 아비터(arbiter) 방식 중 하나 이상의 방식을 이용하여 동작하는 것을 특징으로 하는 RFID 칩.

발명의 설명

기술 분야

본 발명은 RFID 보안 칩에 관한 것으로서, 타원곡선 암호화 및 물리적 복제 방지 기반의 RFID 보안 칩에 관한

[0001]

것이다.

배경 기술

[0002] RFID 기술은 사물에 대한 식별 정보와 부가 정보를 저장하고, 또는 추가로 센서를 장착하여 상태 정보를 획득하여 RFID 리더의 요청에 의하거나 또는 상황에 따라 리더에게 무선접속 기술을 통해 정보를 전송하는 기술로서, RFID 태그 및 리더 기술, 미들웨어 기술, 정보보호 기술, 위치추적 기술, 모바일 RFID 기술, 디렉터리 서비스 기술, 응용 분야별 활용 및 적용 기술을 바탕으로 운용되는 기술이다. 차세대 RFID 기술은 이들 기술들에 대한 새로운 시장 요구를 반영하는 진일보 기술 영역들을 일컫는 말로 통용될 정도로 관련 분야 시장에 대한 기대가 많아 지고 있다. RFID 기술 중 태그 기술은 사물의 식별 정보 및 센싱 정보를 저장하고 리더의 요청에 의하거나 또는 상황에 따라 외부로 정보를 전송하는 기술이며, RFID 리더 기술은 태그의 정보를 인식하거나 태그에 정보를 기록하며, 태그로부터 수집된 정보를 미들웨어에 제공하는 장치에 관련된 기술이다. 태그는 송신하는 전파의 에너지를 얻는 방법에 따라 수동형(Passive), 배터리 지원 수동형(Battery-assisted Passive) 및 능동형(Active)으로 구분할 수 있으며, 수동형은 리더로부터 수신되는 전파에서 동작, 송신 에너지를 얻고, 배터리 지원 수동형은 수동형 방식에 배터리를 추가하여 인식거리를 향상시킬 수 있으며 능동형은 별도의 배터리에서 동작 송신에너지를 자체 송신기로 정보를 송신한다. 리더는 태그의 종류에 따라 수동형, 배터리 지원 수동형, 능동형으로 구분할 수 있으며, 리저의 형태에 따라 고정형, 이동형 등으로 나눌 수 있다.

[0003] 모바일 RFID기술은 UHF 대역의 RFID 리더를 모바일 휴대형 통신기기에 내장 연동하고, 이동통신 네트워크를 이용하여 사물에 부착된 태그를 통하여 콘텐츠 및 서비스를 제공하는 기술로 기존의 B2B 영역(유통, 물류 등)에서 활용되어 온 RFID 기술을 유비쿼터스(ubiquitous) 시대의 대표적인 개인 휴대단말로 부상하고 있는 휴대폰과 결합하여 B2C 영역의 서비스를 제공하는 기술로 다음과 같은 세부 기술 표준화 항목이 있다. 1)모바일 RFID 사용자 프라이버시 보호 프로토콜, 2)모바일 AIDC 서비스 브로커, 3)모바일 RFID 리더 제어 프로토콜, 4)코드 해석 프로토콜, 5)모바일 AIDC 응용 데이터 구조 및 인코딩 표준, 6)모바일 AIDC UII 식별코드 구조 및 인코딩 표준 등이 있다.

[0004] 기존의 RFID 시스템은 데이터 암호화 및 인증을 위하여 대칭키 암호 시스템이나 RSA 암호와 같은 무겁고 구현 비용이 많이 드는 알고리즘을 사용하였다. 또한, 암호시스템의 키 값이나 부채널 분석등의 물리적인 공격을 막기 위한 랜덤한 시드값으로 난수 발생기를 별도로 크게 구현하여 탑재하였다.

[0005] 본 발명과 관련된 선행기술로는 '알에프아이디 칩이 내장된 태그(한국등록특허: 10-1150704)' 등이 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명이 해결하고자 하는 과제는 타원곡선 암호화 및 물리적 복제 방지 기반의 RFID 칩을 제공하는 것이다.

과제의 해결 수단

[0007] 본 발명은 상기 과제를 해결하기 위하여, RFID 칩에 있어서, 장착된 장치의 식별정보를 저장하는 RFID부; 및 타원곡선암호를 이용하여 상기 식별정보를 암호화하거나 객체 인증을 수행하는 보안인증부를 포함하는 RFID 칩을 제공한다.

[0008] 본 발명의 다른 실시예에 의하면, 상기 보안인증부는, 유한체 연산부, 모듈러 연산부, 및 산술 연산부를 포함하거나, 모듈레이터 산술논리연산장치부(MALU)를 포함하는 것을 특징으로 하는 RFID 칩일 수 있다.

[0009] 본 발명의 다른 실시예에 의하면, 상기 보안인증부는, 상기 RFID부에 저장된 타원곡선암호 파라미터를 이용하여 암호화를 수행하는 것을 특징으로 하는 RFID 칩일 수 있다.

[0010] 본 발명의 다른 실시예에 의하면, 상기 식별정보에 물리적 복제 방지를 수행하는 물리적 복제 방지부를 더 포함하는 RFID 칩일 수 있다.

[0011] 본 발명의 다른 실시예에 의하면, 상기 물리적 복제 방지부는, 난수, 난수를 위한 씨드(SEED), 또는 랜덤 노이즈 중 하나 이상을 발생시키는 것을 특징으로 하는 RFID 칩일 수 있다.

[0012] 본 발명의 다른 실시예에 의하면, 상기 물리적 복제 방지부는, 정적 램(SRAM) 방식, 글리치(Glitch) 방식, 또는 아비터(arbiter) 방식 중 하나 이상의 방식을 이용하여 동작하는 것을 특징으로 하는 RFID 칩일 수 있다.

발명의 효과

- [0013] 본 발명에 따르면, 적은 키 길이를 가지고도 기존에 탑재되었던 암호화방법과 동일한 안정성을 보장할 수 있는 ECC 암호화를 이용하여 구현 비용을 줄였다. 또한, ECC 암호화를 이용해 RFID 칩 자체적으로 인증을 수행할 수 있게 공개키 암호화의 특성을 이용한다. 추가적으로 난수를 생성하기 위하여 AES 등의 다른 경량 암호를 이용하여 주로 난수를 발생시키거나 아날로그적인 노이즈 데이터 등을 이용하여 난수를 발생시키는 기존 시스템에 비하여 PUFs를 이용한 난수 발생은 적은 구현비용으로 간단히 구현할 수 있어 기존에 추가적인 난수 발생기를 탑재하므로 인해서 전체적인 면적이 커지는 단점을 극복할 수 있다. 또한, PUFs의 복제 불가능한 특성을 이용하여 RFID 칩의 복제 불가능성을 부여할 수 있어 RFID 칩의 도난이나 복제를 통한 개인 정보유출 문제를 극복할 수 있다.

도면의 간단한 설명

- [0014] 도 1은 본 발명의 일 실시예에 따른 RFID 칩의 블록도이다.
- 도 2는 본 발명의 다른 실시예에 따른 RFID 칩의 블록도이다.
- 도 3은 본 발명의 다른 실시예에 따른 RFID 칩을 나타낸 것이다.

발명을 실시하기 위한 구체적인 내용

- [0015] 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자 하는 과제의 해결 방안의 개요 또는 기술적 사상의 핵심을 우선 제시한다.
- [0016] 본 발명의 일 실시예에 따른 RFID 칩에 있어서, 장착된 장치의 식별정보를 저장하는 RFID부, 및 타원곡선암호를 이용하여 상기 식별정보를 암호화하거나 객체 인증을 수행하는 보안인증부를 포함한다.
- [0017] 이하 첨부된 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있는 실시 예를 상세히 설명한다. 그러나 이들 실시예는 본 발명을 보다 구체적으로 설명하기 위한 것으로, 본 발명의 범위가 이에 의하여 제한되지 않는다는 것은 당업계의 통상의 지식을 가진 자에게 자명할 것이다.
- [0018] 본 발명이 해결하고자 하는 과제의 해결 방안을 명확하게 하기 위한 발명의 구성을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명의 바람직한 실시예에 대한 동작 원리를 상세하게 설명함에 있어 본 발명과 관련된 공지 기능 또는 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.
- [0019] 도 1은 본 발명의 일 실시예에 따른 RFID 칩의 블록도이다.
- [0020] 본 발명의 일 실시예에 따른 RFID 칩(100)은, RFID부(110) 및 보안인증부(120)를 포함하고, 물리적 복제 방지부(130)를 더 포함할 수 있다.
- [0021] 본 발명의 일 실시예에 따른 RFID 칩(100)은 RFID 보안기술에 대한 신뢰성을 높이기 위한 구성들이 포함된 칩으로, RFID 보안기술은 사용자의 요구사항을 만족시키기 위한 핵심기술 중 하나이다. RFID 태그의 기술발전 및 다양한 응용에 따라 태그 내에 저장된 데이터를 안전하게 관리하고, 리더에게 안전하게 전달하기 위해 암호화 및 인증, 키 관리, 프라이버시 보호 등의 보안 서비스를 제공하여 안전하고 신뢰성 있는 RFID 서비스를 가능하게 하는 것이 중요하다.
- [0022] RFID 보안기술은 다음과 같은 표준화 항목들이 있다. 첫 번째, 보안서비스 및 파일 관리를 위한 RFID air interface architecture로, 모든 주파수 대역의 RFID air interface에 대하여 보안 서비스와 파일 관리를 위한 공통 아키텍처를 정의하는 표준으로 보안 요구사항, 파일구조, 파일 접근제어, 공통 암호화 방식 등을 포함한다. 두 번째, 보안서비스 및 파일 관리를 위한 13.56 MHz RFID air interface로, 13.56 MHz HF 대역의 수동형 RFID 태그와 리더 사이의 보안 서비스 및 파일 관리를 위한 air interface 표준으로 공통 아키텍처 표준을 준수하며, 보다 구체적인 보안 프로토콜, 명령/응답 메시지 포맷, 암호화 방식, 파일 접근 제어 방식, 메모리 맵 구조 등을 정의한다. 세 번째, 보안 서비스 및 파일 관리를 위한 860-960 MHz RFID air interface로, 860-960

MHz UHF 대역의 수동형 RFID 태그와 리더 사이의 보안 서비스 및 파일 관리를 위한 air interface 표준으로 공통 아키텍처 표준을 준수하며, 보다 구체적인 보안 프로토콜, 명령/응답 메시지 포맷, 암호화 방식, 파일 접근 제어 방식, 메모리 맵 구조 등을 정의한다. 마지막으로, 보안 서비스 및 파일 관리를 위한 433 MHz RFID air interface로, 433MHz UHF 대역의 능동형 RFID 태그와 리더 사이의 보안 서비스 및 파일 관리를 위한 air interface 표준으로 공통 아키텍처 표준을 준수하며, 보다 구체적인 보안 프로토콜, 명령/응답 메시지 포맷, 암호화 방식, 파일 접근 제어 방식, 메모리 맵 구조등을 정의한다.

[0023] 이 보안 부분들의 핵심 기능들을 공개키 암호인 ECC 암호화를 이용하여 인증 및 키 관리를 수행하고, PUFs를 이용하여 프라이버시 보호 및 복제 불가능성 확보한다. ECC 암호화를 RFID의 보안에 이용함으로써 무선환경에 필수적인 경량화된 환경에 최적화시킬 수 있고, 적은 키 사이즈를 가지고도 강력한 암호학적 안전도를 제공할 수 있다. 기존의 홀로그램 ID 기술을 통해 위변조가 불가능하고 대용량의 정보를 저장할 수 있었고, 또한 Global Identification System 기술은 최근 이슈가 되고 있는 Internet of Things (IoT), Machine to Machine (M2M) 등의 환경에서 필요한 식별체계에 대한 기술로 식별을 위한 코드체계 및 코드의 할당, 관리, 해석까지 포함하는 기술이나 이를 구현하는데 복잡한 문제가 있었다. 하지만, PUFs를 이용하여 이러한 복잡한 프로토콜과 구조를 단순화하고, 더 물리적으로 안전하고, 무선환경에 맞게 경량화할 수 있고, 그 효율성 또한 높다. 이러한 PUFs가 적용된 RFID 칩은 기존의 방식들이 상당한 추가적인 비용을 발생시켰던 데에 비해 매우 적은 비용으로도 구현이 가능하여 유용하다.

[0024] RFID부(110)는 장착된 장치의 식별정보를 저장한다.

[0025] 보다 구체적으로, RFID부(110)는 RFID 칩의 본래 기능을 수행하는 부분으로, 칩이 장착된 장치에 대한 식별 정보와 부가 정보를 저장하거나, 부가적으로 센서의 센싱을 통해 상태 정보를 획득하여 RFID 리더의 요청에 의하거나 또는 상황에 따라 RFID 리더에게 무선접속 기술을 통해 정보를 전송하는 역할을 수행한다.

[0026] 보안인증부(120)는 타원곡선암호를 이용하여 상기 식별정보를 암호화하거나 객체 인증을 수행한다.

[0027] 보다 구체적으로, RFID 칩(100)의 보안과 인증을 수행하기 위해 보안인증부(120)를 탑재한다. 보안인증부(120)는 타원곡선암호를 이용하여 보안과 인증을 수행한다. 보안을 데이터를 외부로 전송시 데이터를 암호화를 수행하며, 디바이스 정보 또는 사용자 정보에 대한 서명 또는 인증을 외부가 아닌 RFID 칩(100)상에 수행하여 안전할 수 있으며, 인증을 수행함에 있어서, 효율성을 높일 수 있다.

[0028] 타원곡선암호를 이용한 암호화방법(Elliptic Curve Cryptography, ECC)은 이산대수의 난해성에 기반을 둔 공개키 방식의 암호화방법으로 RSA 방법에 이어 전자 상거래의 핵심기술로 최근 주목받고 있다. 이산대수의 난해성에 기반을 둔 타원곡선 암호화방법은 DSA 방법과 소인수분해 기반의 RSA 등과 함께 공개키 방식의 일종이다. ECC는 지난 85년 N.Koblitz와 V.S.Miller 가 RSA 암호화방식에 대한 대안으로 처음 제안하였으며, 현재 보안시스템 및 전자상거래 솔루션업체들에 의해 폭넓게 채용되고 있는 추세이다. ECC는 타원곡선을 이용, 유한체 위에서 새로운 공개키 암호화방법을 만들지는 않지만 기존의 공개키 암호화방법을 타원곡선을 이용해 구현하는 특징을 지니고 있다. 엄밀하게 말하면 ECC는 특정 암호화방법이 아니라 암호화방법을 구현해 볼 수 있는 수학적 장소를 제공하고 있는 것으로 RSA, Diffie-Hellman, Elgamal 등의 방법을 기존의 정수공간이 아닌 타원 곡선위에서 구현할 수 있다. 타원 곡선위에서의 암호 구현은 수학적 복잡도 때문에 동일한 키 크기의 정수 위에서 구현하는 것보다 훨씬 강도가 강하다. 타원곡선 암호화방법은 유한체의 곱셈 군에 근거한 시스템으로서 다음의 장점을 갖는다.

[0029] 먼저, 다양한 암호시스템 설계가 가능하다. 군(group)을 제공할 수 있는 다양한 타원곡선을 활용할 수 있다. 즉, 다양한 암호시스템 설계가 용이하다. 또한, 모든 사용자가 같은 기저체 K 를 사용한다 할지라도 각 사용자가 다른 곡선 I 를 선택할 수 있다. 즉, 모든 사용자는 연산을 수행하기 위해 같은 H/W 를 사용할 수 있으며, 추가 보안을 위해 주기적으로 곡선 I 를 바꿀 수 있다.

[0030] 두 번째로 안전성이 높다. 공개키 암호시스템의 이론적 안전도를 조사하기 위해서는 먼저 시스템을 공격하는 데에 있어 그 시스템의 기반이 되는 수학적 문제를 푸는 것이 어느정도 요구되는가를 분석하는 것이다. 실제 소인수문제에 기반을 둔 공개키 암호시스템 RSA, 이산대수문제에 기반을 둔 공개키 암호시스템 DSA 및 타원곡선 암호시스템 모두 수년간 정밀한 분석이 있어왔고, 그러한 시스템 공격방법은 그 기반이 되는 수학적 문제를 푸는 것이라고 알려져 있다. 그러므로, 이제 “기반이 되는 어려운 문제”가 무엇인지를 분석하여야 한다. 타원곡선 이산대수문제는 타원곡선의 작은 클래스인 초 특이 타원곡선일 때 상대적으로 쉽다. 그러나 이러한 취약점은 쉽게 확인될 수 있으며, 그러므로 쉽게 피할 수도 있다. 모듈러 p 에서의 소인수 분해 문제와 이산대수문제는 일반

적으로 Sub-exponential time 알고리즘이 알려져 있다. Sub-exponential time 알고리즘이란 여전히 어려운 문제이나, 완전지수복잡도(fully exponential time) 알고리즘만을 허용하는 문제보다는 쉽다. 이 알고리즘의 수행 시간은 상수 c 에 대하여 그러나(초 특이 타원곡선을 피하면서) 이 군에서의 sub-exponential time algorithms 이 존재하지 않는다. 즉, 안전한 암호시스템을 설계하는 것이 용이하다. RSA와 DSA가 1024비트의 모듈러를 사용하는 반면, ECC는 160비트 모듈러로도 충분함을 보여준다. 더욱이 키 크기가 증가할수록 그 비율은 더욱 증가한다.

- [0031] 보안인증부(120)는 도 2와 같이, 유한체 연산부(121), 모듈러 연산부(122), 및 산술 연산부(123)를 포함할 수 있다. 보안인증부(120)의 타원곡선암호화를 수행하는 프로세서(125)에서 이용되는 유한체 연산을 수행하는 부분으로, 보안인증부(120)에 포함될 수 있다. 산술 연산부(123)는 일반 산술 연산기일 수 있다.
- [0032] 또한, 보안인증부(120)는 모듈레이터 산술논리연산장치부(Modulator Arithmetic Logic Unit, MALU)를 포함할 수 있다. 모듈레이터 산술논리연산장치부(124)는 유한체 연산부(121), 모듈러 연산부(122), 및 산술 연산부(123)와 함께 타원곡선암호에 필요한 연산을 수행할 수 있고, 몽고메리 곱셈기, 역원기 및 나눗셈기, field conversion 등의 특수 연산을 수행할 수 있다.
- [0033] 보안인증부(120)는 RFID부(110)에 저장된 타원곡선암호 파라미터를 이용하여 암호화를 수행할 수 있다. 암호화의 안정성을 높이기 위해, RFID부(110)에 저장된 타원곡선암호 파라미터들을 이용하여 주기적인 또는 랜덤하게 업데이트하고, 곡선 또한 변경할 수 있고, 다양한 ECC연산이 가능하도록 유한체도 변경할 수 있도록 할 수 있다.
- [0034] 보안인증부(120)는, 이진체(Binary field) 상의 유한체 연산을 통해 동작할 수 있다. RFID 칩(100)의 경량화 및 저전력 환경에서 구동하기 위하여 이진체 상의 유한체 연산을 통해 보안인증을 수행할 수 있다. 이진체뿐만 아니라 소체 상의 연산이 가능하도록 소체(Prime field) 상의 유한체 곱셈기 및 유한체 나눗셈기를 추가로 탑재하여 확장가능하게 구성할 수 있다. 상기 유한체 곱셈기는 몽고메리 곱셈기일 수 있다.
- [0035] 물리적 복제 방지부(130)는 상기 식별정보에 물리적 복제 방지를 수행한다.
- [0036] 보다 구체적으로, RFID부(110)에 저장된 식별정보에 대한 공격 및 복제, 정보 유출과 데이터 조작을 방지하기 위하여 물리적 복제 방지부(130)는 식별정보에 물리적 복제 방지를 수행한다.
- [0037] 물리적 복제 방지부(130)는 난수, 난수를 위한 씨드(SEED), 또는 랜덤 노이즈 중 하나 이상을 발생시킬 수 있다. 물리적 복제 방지를 위해 난수를 발생시키거나, 난수를 위한 씨드를 발생시킬 수 있고, 랜덤 노이즈를 발생시킬 수 있다.
- [0038] 물리적 복제 방지부(130)는 정적 램(SRAM) 방식, 글리치(Glitch) 방식, 또는 아비터(arbiter) 방식 중 하나 이상의 방식을 이용하여 동작할 수 있다. 물리적 복제 방지부(130)는 정적 램(SRAM) 방식, 글리치(Glitch) 방식, 아비터(arbiter) 방식에 대한 각각의 물리적 복제 방지부로 구성될 수 있고, 정적 램(SRAM) 방식, 글리치(Glitch) 방식, 아비터(arbiter) 방식을 한번에 동작하거나, 또는 각각 하나씩 따로 동작할 수 있다. 적용 환경, 플랫폼, 및 응용환경에 맞도록 동작할 수 있다.
- [0039] 물리적 복제 방지부(130)는 용량지연(Capacitance delay) 및 잡음변화(Noise variation)을 이용하여 동작할 수 있다. 스마트미터 칩의 아날로그 블록의 용량지연 및 잡음변화를 이용하여 적은 비용으로 효과적으로 동작할 수 있다.
- [0040] 또는 물리적 복제 방지부(130)는 링 오실레이터(Ring oscillator) 방식, 또는 고급 암호화 표준(AES)을 이용하여 동작할 수 있다. 기존 물리적 복제 방지 방식들을 이용하여 물리적 복제 방지를 수행할 수도 있다.
- [0041] 물리적 복제 방지(Physically Unclonable Functions, PUFs)는 칩의 복제를 방지하는 방법으로, 칩이 내장될 때 나타나는 미세한 차이를 이용한다. PUF관련 많은 기술 문서들이 있지만, PUFs라는 개념이 나오기전 주로 TRNG(True Random Number Generator) or Digital Fingerprint 라는 개념으로 사용되었다. 처음 PUF의 개발이 이루어졌을 때 PUF의 랜덤한 특성에 맞추어서 개발이 이루어졌다. 이후 임베디드 PUF(기존에 개발되어 있는 스탠다드셀(standard cell)과 메모리등을 이용한)가 소개되면서, 이 임베디드 PUF분야의 많은 후속 연구들이 진행되어왔다. 임베디드 PUF는 크게 메모리기반의 PUF와 딜레이 기반의 PUF로 나누어진다. 메모리기반의 PUF는 현재 개발되어 사용되고 있는 메모리에서 PUF의 주요 특성을 만족하는 부분만을 추출하여 PUF로 이용한 것이고, 딜레이 기반의 PUF는 하드웨어의 물리적특성을 통해서 발생할 수 있는 딜레이 특성을 PUF로 이용한 것으로 가장 대표적인 Arbiter PUF와 Ring Oscillator PUF 가 있다. 메모리 기반의 PUF는 대표적으로 SRAM 메모리 기반의 PUF

가 있다. 이 PUF는 SRAM메모리가 초기 상태에서의 불안정한 초기값을 이용한 PUF이다. 본 PUF는 PUF를 만들기 위해 추가적인 작업이 없이 기존의 메모리 primitive를 그대로 사용하여 PUF를 만든다는 점에서 다른 PUF들보다 생성하기 쉽고, 현실적으로 사용가능한 실용적인 PUF이다. 그리고, 무엇보다도 SRAM 메모리의 초기값의 randomness는 메모리 제조단계에서 제작 시 모든 메모리들을 동일한 제작 조건하에서 동일한 제작 방식으로 이루어질 수 없으므로 PUF 특성을 충분히 만족하는 SRAM 기반의 PUF를 쉽게 만들어 낼 수 있는 장점이 있다. Arbiter PUF는 신호의 경쟁 조건(race condition)을 이용하여 신호 도착의 우선순위를 판단하는 arbiter이 마지막에 판단하여 PUF의 출력(response)를 만들어 낸다. 이때, 신호의 경쟁 조건을 만들어 내기 위하여 다양한 입력신호들(challenge)을 이용하고, 이 입력신호들의 랜덤한 입력 또한 arbiter PUF의 랜덤한 출력 값을 형성하는데 중요한 요소로 작용한다. Ring Oscillator PUF는 Ring oscillator를 연결하여 발생하는 주파수의 변화를 비교하여 랜덤한 출력값을 생성하는 PUF이다.

[0042] 상기와 같이, RFID 칩(100)은 보안을 위하여 보안인증부(120)에 ECC암호화방법을 탑재하고, 물리적 복제 방지부(130)에 PUFs를 또한 탑재하여 인증 및 보안을 강화할 수 있고, 또한 복제 불가능한 PUFs의 특성을 이용하여 개인 정보 유출 방지를 위한 하드웨어 디지털 핑거프린트 기능을 할 수 있다. RFID 부분은 RFID IP를 도입하여 사용하고, RFID IP와 연동하기 위한 firmware는 MCU에 따로 구현하여 구성하여, 칩의 기능 업그레이드는 물론이고, 보안 모듈들에 대한 파라미터 등의 업그레이드를 통한 보안성 강화 및 구동 드라이버의 업그레이드를 용이하게 할 수 있다. 소프트웨어와의 연동이 가능하도록 하여 다양한 플랫폼에 적용이 가능하다.

[0043] 도 3은 본 발명의 다른 실시예에 따른 RFID 칩을 나타낸 것이다.

[0044] 본 발명의 실시예에 따른 RFID 칩은 ECC(Elliptic Curve Cryptography)에 기반하고, PUFs를 탑재한 보안 SoC 솔루션으로 전체적인 구성은 도 3과 같다. RFID의 보안시스템의 핵심은 ECC co-processor(220)이고, ECC는 유한체 연산기, 모듈러 연산기, 일반 산술연산 모듈을 지원할 수 있게 각각의 연산 프리미티브 모듈을 각각 포함하여 구현한다. 특수한 연산들(역원기, 나눗셈기, 필드 변환)과 많이 사용하는 연산(square and multiplication)은 따로 연산 모듈을 만들어 ECC co-processor와 같이 동작하게 한다. 상단의 연산모듈(221)은 ECC co-processor(220)를 동작시키기 위한 핵심적인 부분으로, 각각의 연산 모듈(221)은 유한체 연산기와 모듈러 연산기, 일반 산술 연산기 등으로 나누어 구성된다. Cell_S1, Cell_S2, Cell_M으로 구성하고, MALU_register도 특수한 연산 모듈을 동일하게 포함하고, 특히 이 레지스터는 위의 연산들을 제대로 동작할 수 있게 하는 프로토콜을 탑재하여 그 기능을 주로 수행한다. ECC co-processor(220)를 동작시키기 위한 드라이버 firmware 및 프로토콜은 Micro controller상에 구현한다. Micro controller가 ECC-coprocessor를 RFID 기존 시스템에 제대로 적용될 수 있게 하는 프로토콜을 가지고 있으며, 동작 명령을 내린다. 또한, micro controller의 주된 기능은 IP block 형태로 ROM에 탑재시키는 ECC parameter들(유한체, ECC 커브, 연산 포인트 등)을 ECC coprocessor로 로드하여 제대로 동작할 수 있게 하고, 보안성 강화를 위하여 수시로 업데이트되는 이러한 파라미터들에 대한 통신을 수행할 수 있게 한다. ECC 파라미터는 RAM or ROM에 탑재하여 수시로 업데이트 가능하게 하고, 또한 커브를 바꿀수 있게도 하며, 다양한 ECC연산이 가능할 수 있게 유한체도 바꿔서 업로드 할 수 있게 구성한다. MCU를 통해 ECC coprocessor와 통신한다. ECC를 이용한 ECDHA등의 다양한 응용 프로그램을 형성하고 구동하기 위한 프로토콜은 micro controller와 함께 bus manager에도 구현하여 구성한다. BUS manager에는 ECC coprocessor를 이용하여 ECDHA같은 전자서명 알고리즘을 구현할 수 있게끔 프로토콜을 구현하여 사용자 인증 등에 PUFs와 더불어 사용할 수 있게 하고, RFID 가 무선통신에 이용하는 만큼 자체적으로 서명 값을 생성할 수 있게 하여, 향후 보안시스템 설계 시 추가적인 비용이 발생하지 않도록 한다.

[0045] MALU 모듈(222)에는 위에 언급한 연산모듈과 함께 유한체 연산, 모듈러 연산, 일반 산술 연산기를 구현하되 몽고메리 곱셈기, 역원기 및 나눗셈기, field conversion 등의 특수 연산기능을 갖춘 모듈로 구성한다.

[0046] PUFs 모듈은 Random number generator(230)에 탑재하여, PUFs를 이용한 난수 발생을 물론이고, 각각의 RFID 칩에 대한 인증기능 및 복제불가능성을 부여하기 위한 아날로그 및 디지털 핑거프린트(fingerprint)의 역할을 하게 한다. PUFs모듈은 암호모듈 및 시스템(ECDHA)을 위한 난수 또는 난수를 위한 SEED로 생성한다. PUFs모듈은 총 3가지 형태로 구성하고 추가할 수 있게 한다. 기본적인 3가지 형태의 PUFs는 SRAM PUFs, Glitch PUFs, Arbiter PUFs로 한다. 각각의 PUFs는 한꺼번에 동작할 수 있고, 각각 하나씩 따로 동작할 수 있게 한다. 즉, 한 번에 예를 들어, 난수, 난수를 위한 SEED, 랜덤 노이즈 생성기로 각각 동작할 수 있고, 이중 한가지 동작을 위해 적용 환경 및 플랫폼, 응용환경에 맞게 동작할 수 있게 한다. 각각의 PUFs들은 추가적인 구현 비용이 발생하지 않게 기존에 Standard Cell을 이용하여 구현하고, 기존의 RFID 칩의 리소스를 사용한다.

[0047] PUFs와 ECC coprocessor는 서로 통신이 가능하게 하여 ECC에 대한 랜덤 노이즈나 랜덤 클럭 분주기 등을 추가할 수 있게 하여 부채널 분석에 안전하게 설계할 수 있다. PUFs와 ECC가 탑재한 RFID 칩은 부채널 분석에 안전한 카운터매저 및 복제불가능성을 모두 가지고 있다.

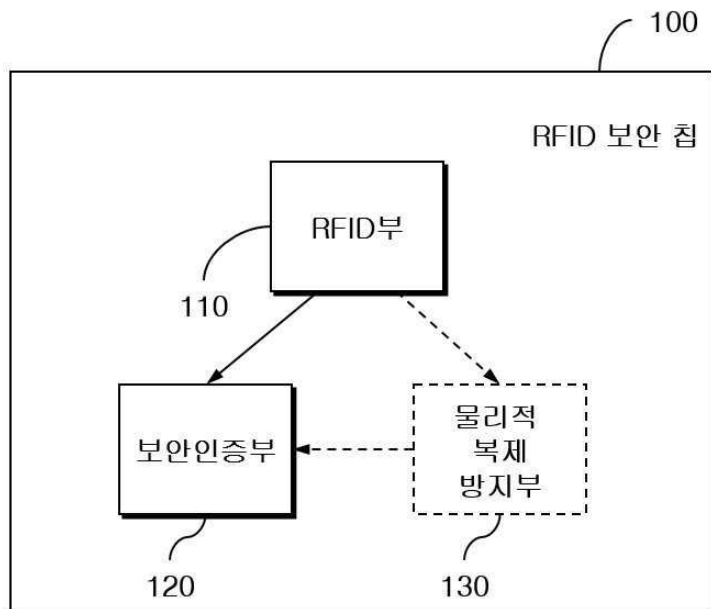
[0048] RFID의 시스템은 기존의 RFID IP를 도입하여 사용하고, 기존의 IP와 연동하기 위한 firmware는 MCU에 따로 구현하여 구성한다.

[0049] 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.

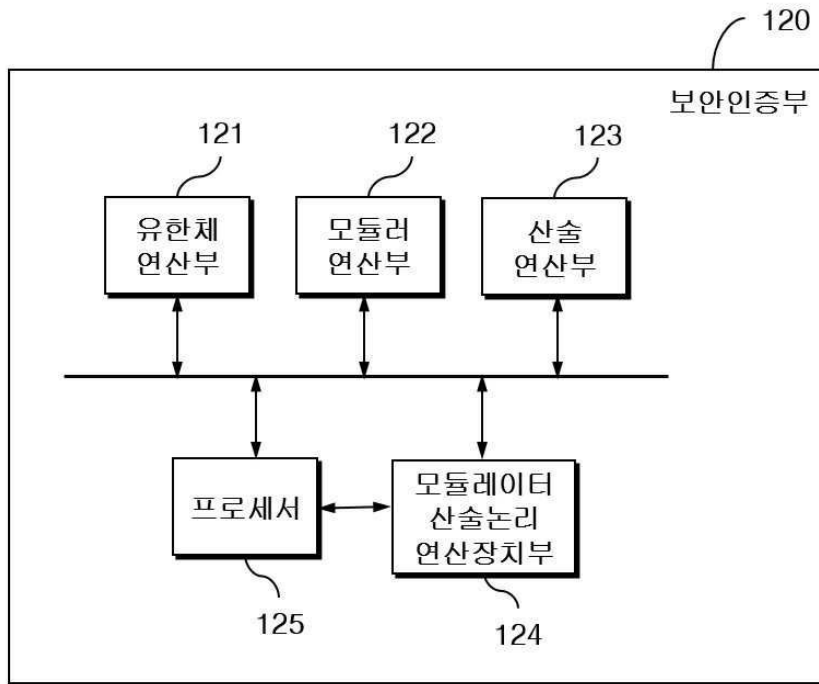
[0050] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면

도면1



도면2



도면3

