

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2016-0055363 (43) 공개일자 2016년05월18일
(51) 국제특허분류(Int. Cl.) G06F 21/00 (2006.01) G06F 21/30 (2013.01) G06F 21/79 (2013.01)	(71) 출원인 고려대학교 산학협력단 서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)	
(21) 출원번호 10-2014-0154707	(72) 발명자 김현민 서울 성북구 길음로 118, 414동 1801호 (길음동, 길음뉴타운)	
(22) 출원일자 2014년11월07일 심사청구일자 2014년11월07일	홍석희 서울특별시 도봉구 마들로 859-19, 103동 107호 (도봉동, 한신아파트)	
	(74) 대리인 특허법인충현	

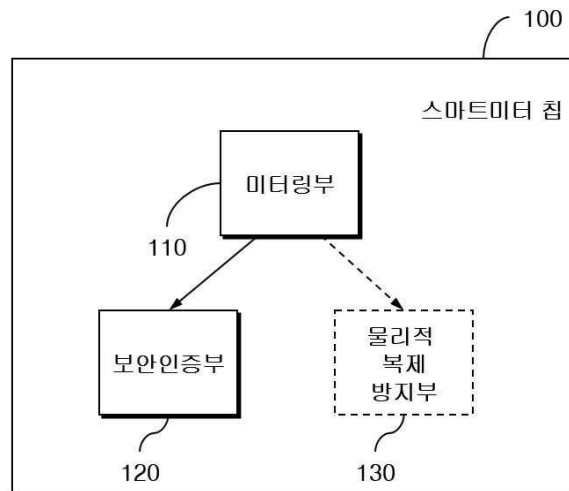
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 타원곡선 암호화 기반의 복제 불가능한 스마트미터 칩

(57) 요약

본 발명은 스마트미터 칩에 관한 것으로, 스마트그리드에 이용되는 스마트미터 칩에 있어서, 전력량을 측정하는 미터링부, 및 타원곡선암호를 이용하여 상기 측정된 전력량의 데이터를 암호화하거나 객체 인증을 수행하는 보안인증부를 포함하고, 하나의 칩 형태로 구현되는 것을 특징으로 함으로써, 스마트그리드 환경에서 안전한 제품 운용이 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

스마트그리드에 이용되는 스마트미터 칩에 있어서,

전력량을 측정하는 미터링부; 및

타원곡선암호를 이용하여 상기 측정된 전력량의 데이터를 암호화하거나 객체 인증을 수행하는 보안인증부를 포함하고,

하나의 칩 형태로 구현되는 것을 특징으로 하는 스마트미터 칩.

청구항 2

제 1 항에 있어서,

상기 보안인증부는,

이진체(Binary field) 상의 유한체 연산을 통해 동작하는 것을 특징으로 하는 스마트미터 칩.

청구항 3

제 1 항에 있어서,

상기 보안인증부는,

소체(Prime field) 상의 유한체 곱셈기 및 유한체 나눗셈기를 포함하는 것을 스마트미터칩.

청구항 4

제 1 항에 있어서,

상기 측정된 전력량의 데이터 및 객체정보에 물리적 복제 방지를 수행하는 물리적 복제 방지부를 더 포함하는 스마트미터 칩.

청구항 5

제 4 항에 있어서,

상기 물리적 복제 방지부는,

용량지연(Capacitance delay) 및 잡음변화(Noise variation)을 이용하여 동작하는 것을 특징으로 하는 스마트미터 칩.

청구항 6

제 4 항에 있어서,

상기 물리적 복제 방지부는,

링 오실레이터(Ring oscillator) 방식, 아비터(arbiter) 방식, 글리치(Glitch) 방식, 또는 고급 암호화 표준(AES)을 이용하여 동작하는 것을 특징으로 하는 스마트미터 칩.

청구항 7

정보를 자체적으로 처리하고 외부와 통신기능을 가지는 장치에 있어서,

정보를 처리하는 처리부;

타원곡선암호를 이용하여 상기 처리된 정보의 데이터를 암호화하거나 객체 인증을 수행하는 보안인증부; 및

상기 처리된 정보의 데이터 및 객체정보에 물리적 복제 방지를 수행하는 물리적 복제 방지부를 포함하는 장치.

발명의 설명

기술 분야

[0001] 본 발명은 스마트미터 칩에 관한 것으로서, 타원곡선 암호화 및 물리적 복제 방지 기반의 스마트미터 칩에 관한 것이다.

배경 기술

[0002] 스마트그리드 환경의 근간이 되는 스마트미터(한전형 및 민수형 전체) 보급을 2020년까지 완료하고자 하는 정부의 정책적 의지가 확고하고, 한전에서 사용중인 스마트미터(G-type, Advanced E-type 등)를 비롯하여, 민수용 등 수용가 프라이버시 등 보안 이슈에 대한 적절한 보안 솔루션 마련이 시급한 상황이다. 또한, 스마트그리드의 실시간 가용성 및 보안성 확보를 위해 HW 기반 보안 솔루션이 필요하다. 보안 IC와 Metering IC를 별개로 적용 시 스마트미터 개발에 대한 난이도 및 비용이 증가되는 문제가 있다. 현재 사용되고 있는 G-Type 스마트미터에 보안기능이 들어있지 않다. 스마트그리드 환경에서 수요자 측면의 보안이 중요한 이슈로 부각되면서 스마트미터에서의 보안성 확보가 최우선적인 과제로 부각되고 있고, 이에 대한 대책 마련이 시급하다.

[0003] 본 발명과 관련된 선행기술로는 '스마트 미터(한국공개특허: 10-2013-0131897)' 등이 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명이 해결하고자 하는 첫 번째 과제는 타원곡선 암호화 및 물리적 복제 방지 기반의 스마트미터 칩을 제공하는 것이다.

[0005] 본 발명이 해결하고자 하는 두 번째 과제는 타원곡선 암호화 및 물리적 복제 방지 기반의 스마트 장치를 제공하는 것이다.

과제의 해결 수단

[0006] 본 발명은 상기 첫 번째 과제를 해결하기 위하여, 스마트그리드에 이용되는 스마트미터 칩에 있어서, 전력량을 측정하는 미터링부; 및 타원곡선암호를 이용하여 상기 측정된 전력량의 데이터를 암호화하거나 객체 인증을 수행하는 보안인증부를 포함하고, 하나의 칩 형태로 구현되는 것을 특징으로 하는 스마트미터 칩을 제공한다.

[0007] 본 발명의 다른 실시예에 의하면, 상기 보안인증부는, 이진체(Binary field) 상의 유한체 연산을 통해 동작하거나, 소체(Prime field) 상의 유한체 곱셈기 및 유한체 나눗셈기를 포함하는 것을 스마트미터 칩일 수 있다.

[0008] 본 발명의 다른 실시예에 의하면, 상기 측정된 전력량의 데이터 및 객체정보에 물리적 복제 방지를 수행하는 물리적 복제 방지부를 더 포함하는 스마트미터 칩일 수 있다.

[0009] 본 발명의 다른 실시예에 의하면, 상기 물리적 복제 방지부는, 용량지연(Capacitance delay) 및 잡음변화(Noise variation)을 이용하여 동작하거나, 링 오실레이터(Ring oscillator) 방식, 아비터(arbiter) 방식, 글리치(Glitch) 방식, 또는 고급 암호화 표준(AES)을 이용하여 동작하는 것을 특징으로 하는 스마트미터 칩일 수 있다.

[0010] 본 발명은 상기 두 번째 과제를 해결하기 위하여, 정보를 자체적으로 처리하고 외부와 통신기능을 가지는 장치에 있어서, 정보를 처리하는 처리부; 타원곡선암호를 이용하여 상기 처리된 정보의 데이터를 암호화하거나 객체 인증을 수행하는 보안인증부; 및 상기 처리된 정보의 데이터 및 객체정보에 물리적 복제 방지를 수행하는 물리적 복제 방지부를 포함하는 장치를 제공한다.

발명의 효과

[0011] 본 발명에 따르면, 스마트미터칩에 ECC 암호알고리즘 모듈을 탑재하여 스마트그리드 환경에서 안전한 제품 운용이 가능하다. 스마트미터기는 물론이고, 스마트어댑터, 전기차, 스마트가전 등 IoT 장비 등에도 확장 및 이용 가능하다. PUFs 모듈이 탑재된 최초의 ECC 암호화 장비로써 CC 인증을 통한 제품의 상품성에도 기여할 수 있다.

도면의 간단한 설명

- [0012] 도 1은 본 발명의 일 실시예에 따른 스마트미터 칩의 블록도이다.
- 도 2는 본 발명의 실시예에 따른 스마트미터 칩을 나타낸 것이다.
- 도 3은 본 발명의 실시예에 따른 스마트미터 칩이 사용되는 스마트미터 모듈을 나타낸 것이다.
- 도 4 및 5는 본 발명의 일 실시예에 따른 스마트미터 칩을 설계하는 과정 및 흐름도이다.
- 도 6은 본 발명의 일 실시예에 따른 스마트 장치의 블록도이다.

발명을 실시하기 위한 구체적인 내용

- [0013] 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자 하는 과제의 해결 방안의 개요 또는 기술적 사상의 핵심을 우선 제시한다.
- [0014] 본 발명의 일 실시예에 따른 스마트미터 칩은, 스마트그리드에 이용되는 스마트미터 칩에 있어서, 전력량을 측정하는 미터링부, 및 타원곡선암호를 이용하여 상기 측정된 전력량의 데이터를 암호화하거나 객체 인증을 수행하는 보안인증부를 포함하고, 하나의 칩 형태로 구현되는 것을 특징으로 한다.
- [0015] 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.
- [0016] 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 실시 예에 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.
- [0017] 도 1은 본 발명의 일 실시예에 따른 스마트미터 칩의 블록도이다.
- [0018] 본 발명의 일 실시예에 따른 스마트미터 칩은 스마트그리드에 이용되는 하나의 칩 형태로 구현되는 스마트미터 칩(100)으로, 미터링부(110) 및 보안인증부(120)를 포함하고, 물리적 복제 방지부(130)를 더 포함할 수 있다.
- [0019] 스마트미터 칩(100)은 장착된 디바이스의 전력량을 실시간으로 측정하고, 전력량의 데이터를 객체 정보와 함께 전력관리 서버로 송부하는 역할을 한다. 상기 정보들을 서버로 송부할 시, 보안상의 문제가 발생할 수 있는바, 이를 해결하기 위하여, 본 발명의 일 실시예에 따른 스마트미터 칩(100)은 타원곡선암호를 이용하는 ECC와 물리적 복제를 방지하는 PUFs를 하나의 칩 상에 탑재한다. 이를 통해, 기존에 중간에 신뢰기관이나, 서버(TC)에서 수행되던 인증 문제를 디바이스 자체적으로 장비내에서 자가 인증이 가능하게 하고, 서버나 신뢰기관으로의 인증 데이터 전송 시 발생할 수 있는 개인 정보 유출문제를 해결할 수 있다. 또한, 기존의 복잡한 이러한 인증 시스템을 매우 간소화할 수 있어서, 그 효율성 측면에서도 우수하다.
- [0020] 미터링부(110)는 전력량을 측정한다.
- [0021] 보다 구체적으로, 미터링부(110)는 스마트미터의 본래 목적을 수행하는 구성으로, 장착된 디바이스의 전력량 측정을 수행한다. 미터링부(110)는 기존의 스마트미터에서 수행되던 미터링(metering)을 수행하는 구성을 포함한다. 미터링부(110)는 시스템온칩의 특정 기능을 수행하는 IP(intellectual property)로 구현되어 칩 상에 탑재될 수 있다.
- [0022] 보안인증부(120)는 타원곡선암호를 이용하여 상기 측정된 전력량의 데이터를 암호화하거나 객체 인증을 수행한다.
- [0023] 보다 구체적으로, 스마트미터 칩(100) 상에서 보안과 인증을 자체적으로 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 스마트미터

칩(100)상에 수행하여 안전할 수 있으며, 인증을 수행함에 있어서, 효율성을 높일 수 있다.

- [0024] 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, 유한체위에서 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 수학적인 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.
- [0025] 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.
- [0026] 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 일반적으로 Sub-exponential time 알고리즘이 알려져 있다. Sub-exponential time 알고리즘이란 여전히 어려운 문제이나, 완전지수복잡도(fully exponential time) 알고리즘만을 허용하는 문제보다는 쉽다. 이 알고리즘의 수행시간은 상수 c 에 대하여 그러나(초 특이 타원곡선을 피하면서) 이 군에서의 sub-exponential time algorithms이 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.
- [0027] 보안인증부(120)는, 이진체(Binary field) 상의 유한체 연산을 통해 동작할 수 있다. 스마트미터 칩(100)의 경량화 및 저전력 환경에서 구동하기 위하여 이진체 상의 유한체 연산을 통해 보안인증을 수행할 수 있다.
- [0028] 보안인증부(120)는 소체(Prime field) 상의 유한체 곱셈기 및 유한체 나눗셈기를 포함할 수 있다. 이진체 뿐만 아니라 소체 상의 연산이 가중하도록 소체(Prime field) 상의 유한체 곱셈기 및 유한체 나눗셈기를 추가로 탑재하여 확장가능하게 구성할 수 있다. 상기 유한체 곱셈기는 몽고메리 곱셈기일 수 있다.
- [0029] 물리적 복제 방지부(130)는 상기 측정된 전력량의 데이터 및 객체정보에 물리적 복제 방지를 수행한다.
- [0030] 보다 구체적으로, 미터링부(110)에서 측정된 전력량의 데이터 및 객체정보에 대한 공격 및 복제, 스마트미터의 도난 등으로 인해서 발생할 수 있는 정보 유출과 데이터 조작을 방지하기 위하여 물리적 복제 방지부(130)는 전력량의 데이터 및 객체정보에 물리적 복제 방지를 수행한다.
- [0031] 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.
- [0032] 또는 물리적 복제 방지부(130)는 링 오실레이터(Ring oscillator) 방식, 아비터(arbiter) 방식, 글리치(Glitch) 방식, 또는 고급 암호화 표준(AES)을 이용하여 동작할 수 있다. 기존 물리적 복제 방지 방식들을 이용하여 물리적 복제 방지를 수행할 수도 있다.
- [0033] 물리적 복제 방지(Physically Unclonable Functions, PUFs)는 칩의 복제를 방지하는 방법으로, 칩이 내장될 때 나타나는 미세한 차이를 이용한다. PUF관련 많은 기술 문서들이 있지만, PUF라는 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 나뉘어진다. 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 PUF가 있다. 메모리 기반의 PUF는 대표적으로 SRAM 메모리 기반의 PUF가 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.

[0034] 상기와 같이, 스마트미터 칩(100)은 보안을 위하여 보안인증부(120)에 ECC암호화방법을 탑재하고, 물리적 복제 방지부(130)에 PUFs를 또한 탑재하여 기존의 서버 및 다른 추가 장비에서 행해지던 객체 인증 및 사용자 인증을 디바이스 자체내에서 할 수 있고, 또한 복제 불가능한 PUFs의 특성을 이용하여 개인 정보 유출 방지를 위한 하드웨어 디지털 펌웨어프린트 기능을 할 수 있다. 기존의 스마트미터 칩을 구성하는미터링부(110) 등의 각종 IP들과 하나의 SoC로 구성하여 저전력 및 고속의 성능을 낼 수 있게 한다. 나아가, MCU부분에 firmware upgrade를 할 수 있게 구성하여, 기존의 스마트미터 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.

[0035] 도 2는 본 발명의 실시예에 따른 스마트미터 칩을 나타낸 것이다.

[0036] 스마트미터 칩의 구체적인 구성도를 나타낸 것으로, 기존의 metering IP는 IP를 도입해서 사용하고, security IP를 두어 다양한 ECC 응용모듈(210)과 interface 및 PUFs(220)를 설계하여 IP로 구성한다. 기존에 AES IP를 HW로 구성하여 운용한 부분은 SW로 변경하여 추가적인 필요시에만 firmware updata를 통해 장비에 탑재하여 사용하게 할 수 있다.

[0037] 도 3은 본 발명의 실시예에 따른 스마트미터 칩이 사용되는 스마트미터 모듈을 나타낸 것이다.

[0038] 스마트미터 칩을 실제 스마트미터기에 적용하였을 경우로, 전력량 측정, 저장장치, 전원, 디스플레이 등의 주변 장치들과 연결을 통해 스마트미터를 구현하는 모듈을 나타낸 것이다. 물론, 스마트미터기뿐만 아니라, 다른 다양한 플랫폼 및 장비에도 동일하게 구성하여 이용할 수 있다.

[0039] 도 4 및 5는 본 발명의 일 실시예에 따른 스마트미터 칩을 설계하는 과정 및 흐름도이다.

[0040] 스마트미터 칩의 전체 설계는 HW와 SW의 통합설계 방식으로 이루어진다. HW부분에서는 기존의 스마트미터 칩의 기능을 하는 IP를 도입하고, 본 발명의 실시예에 따른 ECC와 PUFs모듈을 HW IP로 설계하여 기존에 도입한 IP들과 One-chip SoC 형태로 구성한다. 이렇게 metering IC와 Security IC가 결합된 단일칩에 국제 표준에 적합한 security 모듈을 이용한 다양한 응용(서명, 인증, 암호화 등등)을 할 수 있게 프로토콜을 설계하고, 기존의 metering IC와 security IC와의 통신을 위한 프로토콜도 이 부분에 설계한다. SW 파트에는 기존에 HW로 구현되었던 AES 암호알고리즘을 소프트웨어로 설계하고, 또한, ECC에 적용될 각종 파라미터들의 저장공간을 두어 주기적으로 파라미터 변경을 통한 보안성 강화에 기여할 수 있다. 이외에도 개발한 스마트미터칩을 다양한 장비 및 플랫폼에 적용(전력량계, micro grid, 스마트가전, IoT, EMS, 수요반응, EV car 등)하기 위하여 SW에 firmware upgrade를 할 수 있게 구성한다. 전체적인 설계 플로우는 도 5와 같고, ECC와 PUFs가 포함된 security IP를 기존의 metering IP와 같이 합성한다.

[0041] 도 6은 본 발명의 일 실시예에 따른 스마트 장치의 블록도이다.

[0042] 본 발명의 일 실시예에 따른 스마트 장치(600)는 정보를 자체적으로 처리하고 외부와 통신기능을 가지는 장치로, 정보를 처리하는 처리부(610), 타원곡선암호를 이용하여 상기 처리된 정보의 데이터를 암호화하거나 객

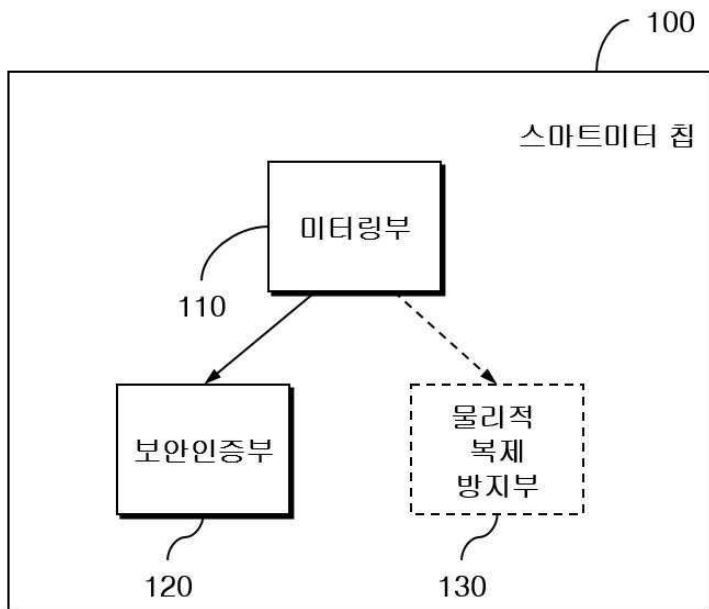
체 인증을 수행하는 보안인증부(620), 및 상기 처리된 정보의 데이터 및 객체정보에 물리적 복제 방지를 수행하는 물리적 복제 방지부(630)를 포함한다. 스마트어댑터, 전기차, 스마트가전 등 IoT 장비들이 본 발명의 실시예에 따른 스마트 장치일 수 있다. 스마트 장치(600)에 대한 상세한 설명은 도 1의 스마트미터 칩(100)에 대한 상세한 설명에 대응하는바, 도 1의 스마트미터 칩(100)에 대한 상세한 설명으로 대신한다.

[0043] 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.

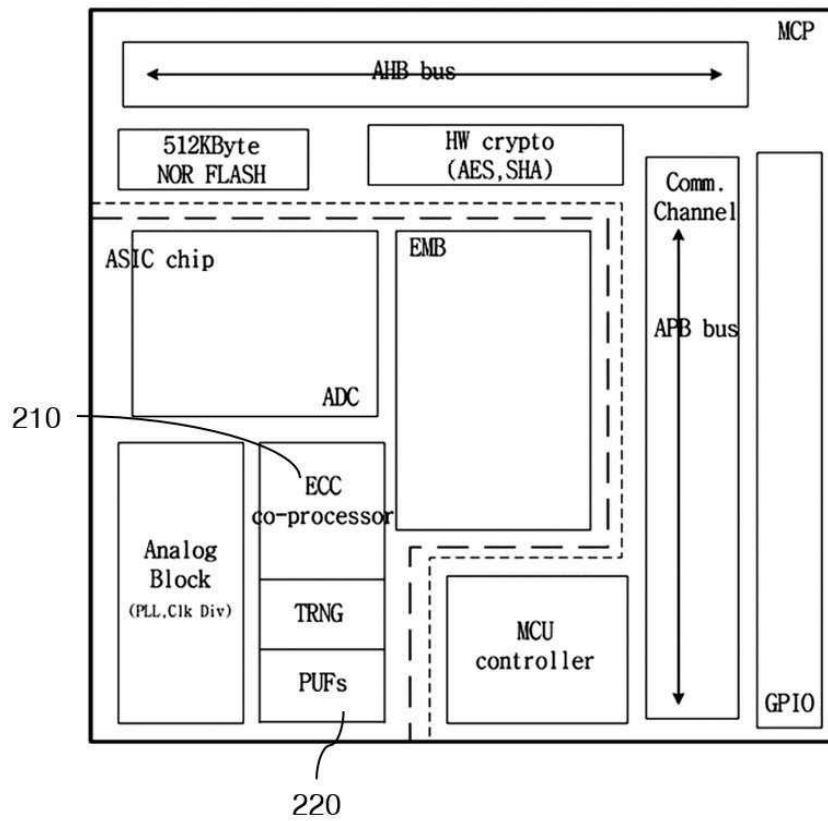
[0044] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면

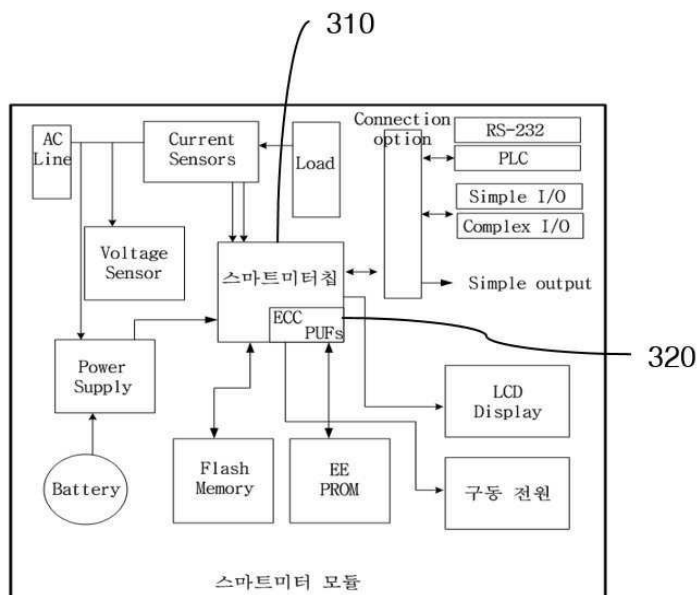
도면1



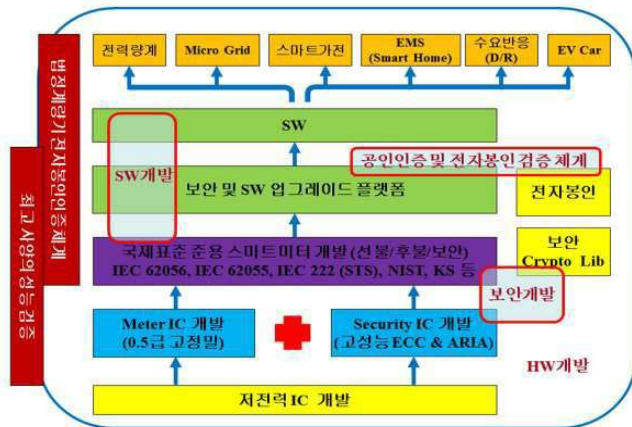
도면2



도면3



도면4



도면5



도면6

