(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년04월19일
(11) 등록번호 10-1136973
(24) 등록일자 2012년04월09일

(51) 국제특허분류(Int. Cl.)
H04L 9/18 (2006.01) *H04L 9/16* (2006.01)
H04L 9/12 (2006.01)
(21) 출원번호 10-2009-0028244
(22) 출원일자 2009년04월01일
심사청구일자 2009년04월01일
(65) 공개번호 10-2010-0067584
(43) 공개일자 2010년06월21일
(30) 우선권주장
1020080126109 2008년12월11일 대한민국(KR)
(56) 선행기술조사문헌
EP00615361 A1
Damith C. Ranasinghe, Daihyun Lim, Peter H. Cole and Srinivas Devadas, "A low cost solution to authentication in passive RFID systems," Technical Report, Auto-ID Lab University of Adelaide (2006)
기술이전 희망 : **기술양도**, **실시권허여**, **기술지도**

(73) 특허권자
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
최용제
대전광역시 유성구 배울2로 6, 한화꿈에그린 104동 2002호 (관평동)
최두호
충청남도 천안시 동남구 풍세로 770, 신도브래뉴아파트 101동 501호 (청당동)
조현숙
대전광역시 유성구 관평1로 12, 대덕테크노밸리7단지 금성백조아파트 701동 501호 (관평동)
(74) 대리인
팬코리아특허법인

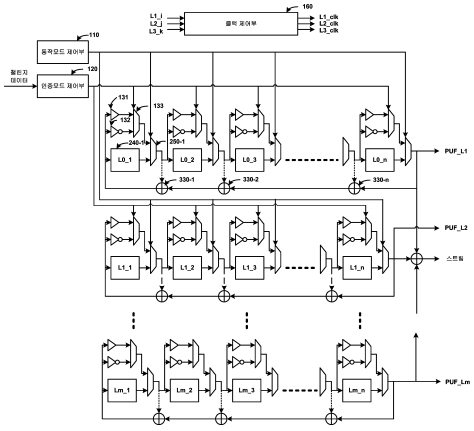
전체 청구항 수 : 총 9 항 심사관 : 이형일

(54) 발명의 명칭 **통합 보안 장치 및 통합 보안 방법**

(57) 요 약

PUF를 통한 기기 인증과 LFSR 기반의 데이터 암호화를 동시에 수행할 수 있는 통합 보안 장치 및 방법이 제공된다. 이를 위한 통합 보안 장치는 기기 인증을 수행하는 인증 모드와 스트림 암호화를 수행하는 암호화 모드를 결정하는 동작 모드 제어부와, 상기 인증 모드에서 입력 데이터에 의해 결정되는 데이터 경로의 차이를 이용하여 기기 인증을 수행하는 인증부 및 상기 암호화 모드에서 궤환 천이 연산을 통해 입력값을 스트림 암호화하는 암호부를 포함한다.

대 표 도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호	2005-S-088-04
부처명	지식경제부 및 정보통신연구지흥원
연구사업명	IT성장동력기술개발
연구과제명	안전한 RFID/USN을 위한 정보보호 기술 개발
주관기관	한국전자통신연구원
연구기간	2005.01.01~2009.02.28

특허청구의 범위

청구항 1

인증 모드와 암호화 모드를 결정하는 동작 모드 제어부;

복수의 출력 비트를 각각 생성하는 복수의 출력 비트 생성부; 및

상기 암호화 모드에서 상기 복수의 출력 비트를 이용하여 비밀키를 생성하는 비밀키 생성부를 포함하고,

상기 복수의 출력 비트 생성부의 각각은 복수의 레지스터를 포함하고,

상기 인증 모드에서 상기 동작 모드 제어부는 상기 복수의 출력 비트 생성부가 입력되는 데이터에 따라 결정되는 데이터 경로에 해당하는 경로 지연 특성에 따라 상기 복수의 출력 비트로 이루어진 챌린지 응답을 생성하도록 제어하고, 상기 챌린지 응답 생성시에 상기 결정되는 데이터 경로에 해당하는 경로 지연 특성에 따라 획득한 초기 값을 상기 복수의 레지스터에 저장하고,

상기 암호화 모드에서 상기 동작 모드 제어부는 상기 복수의 출력 비트 생성부가 상기 복수의 레지스터의 상기 초기 값에 기초하여 상기 복수의 출력 비트를 생성하도록 제어하는 통합 보안 장치.

청구항 2

제1항에 있어서,

상기 복수의 출력 비트 생성부의 각각은,

경로 지연 특성에 따른 출력 값을 생성하는 복수의 단위 경로 세트; 및

상기 복수의 단위 경로 세트 및 상기 복수의 레지스터에 각각 대응하고, 대응하는 단위 경로 세트의 출력 값과 대응하는 레지스터의 출력 값 중 어느 하나를 선택하는 복수의 제1 다중화기를 더 포함하고,

상기 인증 모드에서 상기 복수의 제1 다중화기에 의해 상기 복수의 단위 경로 세트는 체인을 형성하고,

상기 암호화 모드에서 상기 복수의 제1 다중화기에 의해 상기 복수의 레지스터는 체인을 형성하는

통합 보안 장치.

청구항 3

제2항에 있어서,

상기 복수의 단위 경로 세트의 각각은,

경로 지연 특성이 서로 상이한 복수의 버퍼와,

상기 버퍼들의 출력 중 어느 하나를 선택하기 위한 제2 다중화기를 포함하는

통합 보안 장치.

청구항 4

제3항에 있어서,

상기 복수의 출력 비트 생성부의 각각은

상기 복수의 제1 다중화기의 출력 값 중 일부 또는 전부를 연산하여 연산된 값을 첫번째 단위 경로 세트와 첫번째 레지스터에 제공하는 하나 이상의 연산기를 더 포함하는

통합 보안 장치.

청구항 5

제4항에 있어서,

상기 하나 이상의 연산기는 XOR 연산기에 해당하는 통합 보안 장치.

청구항 6

삭제

청구항 7

제3항에 있어서,

챌린지 모드에서 챌린지 데이터를 상기 제2 다중화기를 제어하는 제어 신호로서 상기 제2 다중화기에 제공하는 인증 모드 제어부를 더 포함하는 통합 보안 장치.

청구항 8

제3항에 있어서,

상기 복수의 출력 비트 생성부의 복수의 레지스터 중 일부의 값에 기초하여 복수의 클럭 신호를 생성하는 클럭 제어부를 더 포함하고,

상기 복수의 클럭 신호는 상기 복수의 출력 비트 생성부에 각각 대응하고,

상기 복수의 클럭 신호의 각각은 대응하는 출력 비트 생성부의 복수의 레지스터를 위한 클럭 신호에 해당하는 통합 보안 장치.

청구항 9

통합 보안 장치가 수행하는 통합 보안 방법에 있어서,

인증 모드에서, 입력되는 데이터에 따라 결정되는 데이터 경로에 해당하는 경로 지연 특성에 따라 복수의 출력 포트에 챌린지 응답을 출력하는 단계;

상기 인증 모드에서 상기 챌린지 응답 출력시 상기 결정되는 데이터 경로에 해당하는 경로 지연 특성에 따라 획득한 초기 값을 복수의 레지스터에 저장하는 단계;

상기 인증 모드에서 암호화 모드로 모드를 변경하는 단계;

상기 암호화 모드에서 상기 복수의 레지스터의 상기 초기 값에 기초하여 상기 복수의 출력 포트에 복수의 출력 비트를 출력하는 단계;

상기 암호화 모드에서 상기 복수의 출력 비트를 연산하여 비밀키를 생성하는 단계를 포함하는 통합 보안 방법.

청구항 10

제9항에 있어서,

상기 암호화 모드에서 상기 복수의 레지스터 중 일부에 저장된 값에 기초하여 상기 복수의 레지스터를 위한 클럭 신호를 생성하는 단계를 더 포함하는 통합 보안 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명의 실시예는 PUF를 통한 기기 인증과 LFSR 기반의 데이터 암호화를 동시에 수행할 수 있는 통합 보안 장치 및 방법에 관한 것이다.

[0002] 본 발명은 지식경제부 및 정보통신연구진흥원의 IT성장동력기술개발사업의 일환으로 수행한 연구로부터 도출된 것이다[과제관리번호: 2005-S-088-04, 과제명: 안전한 RFID/USN을 위한 정보보호 기술 개발].

배 경 기 술

[0003] PUF(Physical Unclonable Function)는 계산하기는 쉬우나 특성화하기는 어려운 물리 구조물에 구현되는 함수로서, 디지털 로직의 하드웨어 구현 시 각 공정의 특성, 선로 지연(wire delay), 게이트 지연(gate delay) 등이

생산품에 미치는 영향을 이용하여 복제 여부를 알아내는 기술이다.

[0004] PUF 회로는 일종의 난수 발생 회로로서 집적회로의 예측 불가능한 지연 성분을 이용한다. 통상 집적회로의 지연 성분의 편차는 임의적(random)이고 이를 측정하는 것도 거의 불가능하므로 집적회로의 복제를 원천적으로 봉쇄하는 기술로 각광을 받고 있다.

[0005] PUF는 주로 챌린지-응답 인증(challenge-response authentication) 메커니즘을 통해 순정 집적회로의 접근만을 허용한다. PUF를 포함하는 전자 장치에 물리적 자극이 가해지면 PUF는 랜덤 함수에 의해 예측불허의 방식으로 반응하는데, 상기 가해지는 자극을 챌린지(challenge)라 하고, 그에 대한 PUF의 반응을 응답(response)이라 한다.

[0006] 한편, 무한의 임의 이진수열 또는 무한 난수를 이용하여 이진수열로 변환된 평문을 암호화하는 기법을 스트림 암호(stream cipher)라 한다. 스트림 암호는 선형 궤환 쉬프트 레지스터(LFSR; Linear Feedback ShiftRegister) 또는 비선형 궤환 쉬프트 레지스터(nLFSR; Non-linear Feedback ShiftRegister) 등의 하드웨어를 통해 구현된다.

[0007] 전술한 바와 같이 PUF 회로는 디지털 회로의 지문과 같은 역할을 담당하므로 전자 장치를 인증하는 데 주로 이용되고 있다. 그러나, 전자 장치가 인증된 후에도 전자 장치의 데이터를 보호하기 위해서는 별도의 암호 알고리즘을 적용할 필요가 있으며 이를 위해 별도의 하드웨어를 구비해야 한다.

발명의 내용

해결 하고자하는 과제

[0008] 본 발명의 실시예는 PUF를 통한 기기 인증과 스트림 암호화를 통한 데이터 보안을 동시에 수행하는 통합 보안 장치 및 방법을 제공하는 데에 그 목적이 있다.

과제 해결수단

[0009] 위와 같은 목적을 달성하기 이한 본 발명의 일 양태의 통합 보안 장치는, 기기 인증을 수행하는 인증 모드와 스트림 암호화를 수행하는 암호화 모드를 결정하는 동작 모드 제어부와, 상기 인증 모드에서, 입력 데이터에 의해 결정되는 데이터 경로의 차이를 이용하여 기기 인증을 수행하는 인증부 및 상기 암호화 모드에서, 궤환 천이 연산을 통해 입력값을 스트림 암호화하는 암호부를 포함한다.

[0010] 여기서, 상기 인증부는, 경로 지연 특성이 서로 상이한 복수의 버퍼와, 상기 버퍼들의 출력 중 어느 하나를 선택하기 위한 제2 다중화기를 포함하는 복수의 단위 경로 세트 및 랜덤 특성을 구현하기 위해 비트 연산을 수행하는 연산기를 복수 개 포함할 수 있고, 상기 인증부의 마지막 단위 경로 세트의 출력은 상기 연산기를 거쳐 첫 번째 단위 경로 세트의 입력으로 연결될 수 있다.

[0011] 또한, 상기 암호부는 궤환 천이 과정에서 비트 연산을 수행하는 연산기 및 상기 궤환 천이 과정에서 스트림 암호를 위한 비밀키의 각 비트값을 저장하는 복수의 레지스터를 복수 개 포함할 수 있고, 이때 상기 암호부의 마지막 레지스터의 출력은 상기 연산기를 거쳐 첫 번째 레지스터의 입력으로 연결될 수 있다.

[0012] 또한, 상기 동작 모드 제어부는 상기 인증부의 출력과 상기 암호부의 출력 중 어느 하나를 선택하는 제1 다중화기를 제어하여 인증 모드 또는 암호화 모드를 결정할 수 있다..

[0013] 또한, 인증 모드의 하위 모드로서, 입력 데이터의 각 비트값으로 상기 제2 다중화기를 제어하여 복수의 경로 중 어느 하나를 결정하는 챌린지 모드와, 랜덤 함수로 동작하는 랜덤 모드를 결정하는 인증 모드 제어부를 더 포함할 수 있다.

[0014] 또한, 상기 레지스터로부터 입력된 신호로 클럭 신호를 제어하는 클럭 제어부를 더 포함할 수 있다.

[0015] 본 발명의 다른 일 양태는 기기 인증을 수행하는 인증 모드와 스트림 암호화를 수행하는 암호화 모드 중 어느 하나를 선택받는 단계와, 상기 인증 모드에서, 입력 데이터에 의해 결정되는 데이터 경로의 차이를 이용하여 기기 인증을 수행하는 단계 및 상기 암호화 모드에서, 궤환 천이 연산을 통해 입력값을 스트림 암호화하는 단계를 포함한다.

[0016] 여기서, 상기 기기 인증 단계는, 상기 챌린지 정보의 각 비트값을 이용하여 복수의 데이터 경로 중 어느 하나를 결정하는 단계 및 상기 결정된 데이터 경로에 따른 제1 결과값을 상기 입력 데이터에 대해 미리 정해진 제2 결

과값과 비교하여 기기 인증을 수행하는 단계를 포함할 수 있다.

효 과

[0017] 본 발명의 실시예에 따르면 PUF 회로와 FSR 회로의 중복되는 소자를 공동으로 이용하되 동작 모드만을 변경하여 기기 인증 및 스트림 암호화를 모두 수행할 수 있으므로 전자 기기의 제작 단가를 낮추고 보안 모듈을 소형화할 수 있다.

발명의 실시를 위한 구체적인 내용

[0018] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0019] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "…부", "…기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0020] 도 1은 본 발명의 일 실시예에 의한 통합 보안 장치(100)의 구성을 간략하게 도시한 블록도이다. 본 발명의 일 실시예에 의한 통합 보안 장치는 동작 모드 제어부(110), 인증 모드 제어부(120), 인증부(130), 암호부(140), 저장부(150) 및 클럭 제어부(160)를 포함한다.

[0021] 동작 모드 제어부(110)는 통합 보안 장치가 기기 인증을 수행하는 인증 모드와 스트림 암호화를 수행하는 암호화 모드 중 어느 하나로 동작하도록 통합 보안 장치를 제어한다.

[0022] 인증 모드 제어부(120)는 챌린지-응답(challenge-response) 메커니즘에 의해 기기 인증(authentication)을 수행하는 챌린지 모드와, 무작위 값을 출력하는 랜덤 모드 중 어느 하나로 동작하도록 통합 보안 장치를 제어한다. 챌린지 모드 및 랜덤 모드는 상기 인증 모드의 하위 모드이다.

[0023] 인증부(130)는 통합 보안 장치가 인증 모드로 동작할 때 입력 데이터에 의해 결정되는 데이터 경로의 차이를 이용하여 기기 인증을 수행한다.

[0024] 인증부(130)는 챌린지 모드에서 물리적 복제 불능 함수(Physical Unclonable Function, 이하 'PUF'라 함)의 챌린지-응답 인증(challenge-response authentication) 메커니즘을 이용하여 기기 인증을 수행한다. 따라서, 인증부(130)는 챌린지 데이터가 입력되면 저장부(150)로부터 미리 저장된 챌린지-응답 쌍을 불러오고, 불러온 응답 값을 상기 챌린지 데이터에 대한 처리 결과값과 비교한다. 만약, 두 값이 동일하면 통합 보안 장치에 접근하려는 전자 기기는 순정(genuine)인 것으로 인증된다.

[0025] 암호화 모드에서, 암호부(140)는 궤환 천이 연산을 통해 원본 데이터에 대한 스트림 암호화를 수행한다. 궤환 천이 연산을 위해 선형 궤환 천이 레지스터(Linear Feedback Shift Register, LFSR) 또는 비선형 궤환 천이 레지스터(non-Linear Feedback Shift Register, nLFSR)가 사용될 수 있다.

[0026] 통합 보안 장치의 구성을 보다 상세하게 살펴보면 다음과 같다. 도 2는 통합 보안 장치의 구성을 보다 상세하게 도시하는 블록도이고, 도 3은 도 2의 각 블록을 전자 소자들로 간략하게 표현한 회로 구성도이다.

[0027] 동작 모드 제어부(110)는 제1 다중화기(150)를 제어하여 인증부(130)의 출력과 암호부(140)의 출력 중 어느 하나를 인가함으로써 인증 모드 또는 암호화 모드를 선택할 수 있다.

[0028] 인증부(130)는 경로 지연 특성이 서로 상이한 복수의 버퍼(131, 132)와, 버퍼들(131, 132)의 출력 중 어느 하나를 선택하기 위한 제2 다중화기(133)와, PUF의 랜덤 특성을 구현하기 위해 비트 연산을 수행하는 연산기(300-1 내지 300-n 중 하나)를 포함한다.

[0029] 복수의 버퍼(131, 132)와 제2 다중화기(133)를 묶어 하나의 경로 결정 유닛이라 정의할 때, 인증부(130)는 복수의 경로 결정 유닛(230-1 ~ 230-n)과 연산기(300-1 내지 300-n 중 하나)를 포함한다. 이때, 마지막 번째 경로 결정 유닛(230-n)의 출력은 연산기(300-1 내지 300-n 중 하나)를 거쳐 첫 번째 경로 결정 유닛(230-1)으로 입력

되는 궤환 구조를 가질 수 있다.

[0030] 또한, 복수의 경로 결정 유닛(230-1 ~ 230-n)과 연산기(300-1 내지 300-n 중 하나)를 묶어 하나의 단위 경로 세트라 할 때, 인증부(130)는 복수의 단위 경로 세트(도면에 미도시)를 포함한다.

[0031] 도 3에서, 제2 다중화기(133)에 연결되는 각 버퍼(131, 132)의 경로 지연 특성은 서로 상이하므로 동일한 신호가 입력되더라도 각 버퍼(131, 132)를 경과하는 시간(이를 '경로 지연'이라 한다) 역시 서로 상이하다. 인증 모드 제어부(120)는 인증 모드의 하위 모드 중 챌린지 모드에서 챌린지 데이터의 각 비트값으로 제2 다중화기(133)를 제어하여 데이터 경로를 결정한다.

[0032] 각 단위 경로 세트마다 하나의 데이터 경로가 결정되고 그에 따라 하나의 PUF 결과 비트(예를 들어 PUF_L1)가 결정된다. 따라서, 전체 단위 경로 세트의 결과 비트(PUF_L1 ~ PUF_Lm)를 조합하면 챌린지 데이터에 대한 응답 데이터를 결정할 수 있다.

[0033] 암호부(140)는 복수의 레지스터(240-1 ~ 240-n)와 궤환 스트림 암호화를 위한 비트 연산을 수행하는 연산기(도면에 미도시)를 포함한다. 본 실시예에서 암호부(140)는 LFSR을 이용한 암호화를 수행한다고 가정한다.

[0034] 암호부(140)의 연산기(도면에 미도시)와 인증부의 연산기(300-1 내지 300-n 중 하나)는 공용되는 것이 바람직하다. 암호부(140)의 마지막 레지스터(240-n)의 출력은 연산기(300-1 내지 300-n 중 하나)를 거쳐 첫 번째 레지스터(240-1)로 입력되는 궤환 구조를 가질 수 있다.

[0035] 복수의 레지스터(240-1 ~ 240-n))를 하나의 스트림 세트로 정의할 때, 암호부(140)는 복수의 스트림 세트(도면에 미도시)를 포함할 수 있다. 이때, 암호부(140)는 클럭 제어부(160)에 선택된 하나의 스트림 세트에서 출력되는 비트 스트림(또는 복수의 스트림 세트에서 출력되는 비트 스트림을 XOR 연산한 값)과 입력된 원본 데이터를 XOR 연산하여 암호화된 데이터를 생성한다. 여기서 상기 비트 스트림은 스트림 암호화를 위한 비밀키가 된다.

[0036] 인증 모드에서, 연산기(300-1 ~ 300-n)는 복수의 경로 결정 유닛들(230-1 ~ 230-(n-1)) 중 미리 정해진 경로 결정 유닛의 출력값(도 3에서 점선으로 표시되어 있음)과 마지막 경로 결정 유닛(230-n)의 출력값에 대해 미리 정해진 비트 연산을 수행한다. 비트 연산의 결과값은 첫 번째 경로 결정 유닛(230-1)으로 궤환(feedback)된다.

[0037] 또한 암호화 모드에서, 연산기(300-1 내지 300-n 중 어느 하나)는 복수의 레지스터들(230-1 ~ 230-(n-1)) 중 미리 정해진 레지스터의 출력값(도 3에서 점선으로 표시되어 있음)과 마지막 레지스터(230-n)의 출력값에 대해 미리 정해진 비트 연산을 수행한다. 비트 연산의 결과값이 첫 번째 레지스터(230-1)로 궤환되면서 각 레지스터(132)의 저장값들은 상기 궤환 방향으로 한 비트씩(또는 미리 정해진 비트씩) 천이(shift)된다. 이와 같은 비트 연산 방식을 궤환 천이 연산이라 부른다. 위와 같은 비트 연산으로 AND, OR, XOR 중 어느 하나가 사용될 수 있고, 이 중에서 적어도 둘 이상이 조합되어 사용될 수도 있다. 연산부의 연산은 통합 보안 장치에 적용되는 최소 다항함수에 따라 결정된다.

[0038] 클럭 제어부(160)는 복수의 단위 경로 세트 또는 복수의 스트림 세트 중에서 어떤 세트에 클럭을 인가할 것인지를 결정한다.

[0039] 클럭 제어부(160)는 암호부(140)가 스트림 암호화를 수행함에 있어서 LFSR이 최대 주기를 가지게 하는 소정의 폴리노미얼 함수(polynomial function)에 따라 클럭 인가를 제어하는 것이 바람직하다. 특히, 인증 모드의 하위 모드 중 랜덤 모드에서 클럭 제어부(160)는 소정의 랜덤 함수(random function)에 따라 클럭 인가를 제어하여 무작위 값이 생성되도록 한다.

[0040] 이상에서 설명한 통합 보안 장치를 통해 기기 인증 및 데이터 암호화를 수행하는 방법을 설명하면 다음과 같다.

[0041] 도 4는 본 발명의 일 실시예에 따른 통합 보안 방법의 각 단계를 순차적으로 도시한 순서도이다.

[0042] 인증 모드의 하위 모드 중 챌린지 모드가 선택된 후(S101), 기기 인증을 위한 챌린지 데이터가 입력되면(S102), 통합 보안 장치는 챌린지 데이터의 각 비트값을 이용하여 복수의 데이터 경로 중 어느 하나를 결정한다(S103). 복수의 단위 경로 세트가 존재하므로 결정된 데이터 경로 역시 복수로 존재한다.

[0043] 통합 보안 장치는 데이터베이스로부터 미리 저장된 챌린지-응답 쌍들의 테이블로부터 상기 입력받은 챌린지 데이터에 상응하는 챌린지-응답 쌍을 불러온다(S104). 그리고, 불러온 챌린지-응답 쌍의 응답 데이터를 상기 결정된 데이터 경로에 따른 출력 비트값들(PUF_L1 ~ PUF_Lm)을 결합한 데이터와 비교한다(S105). 만약, 두 데이터가 동일하다면 상기 기기는 순정으로 인증된다.

[0044] 상기 과정들을 통해 기기 인증이 성공적으로 완료되면(S106), 이후로 입력되는 데이터에 대해 암호화를 수행하는 암호화 모드로 전환된다(S107). 암호화 모드에서, 통합 보안 장치는 전술한 궤환 천이 연산을 통해 비밀키를 생성하고(S108), 생성된 비밀키를 입력값과 XOR 연산하여 암호화된 데이터를 생성한다(S109).

[0045] 한편, 인증 모드의 하위 모드 중 랜덤 모드가 선택되면(S110) 클럭 제어부는 복수의 단위 경로 세트 중 미리 정해진 수의 단위 경로 세트를 랜덤하게 선택하여(S111) 해당 단위 경로 세트에만 클럭이 인가되도록 한다. 이를 통해 통합 보안 장치는 랜덤 함수로 동작하게 된다(S112).

[0046] 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 쉽게 구현할 수 있는 것이다.

[0047] 또한, 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면의 간단한 설명

[0048] 도 1은 본 발명의 일 실시예에 의한 통합 보안 장치의 구성을 간략하게 도시한 블록도이다.

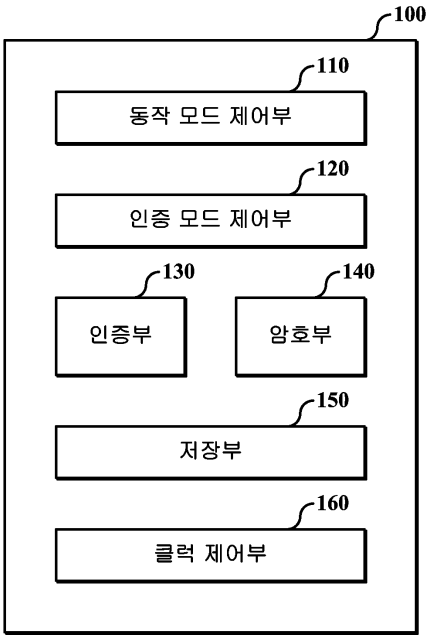
[0049] 도 2는 통합 보안 장치의 구성을 보다 상세하게 도시하는 블록도이다.

[0050] 도 3은 도 2의 각 블록을 전자 소자들로 간략하게 표현한 회로 구성도이다.

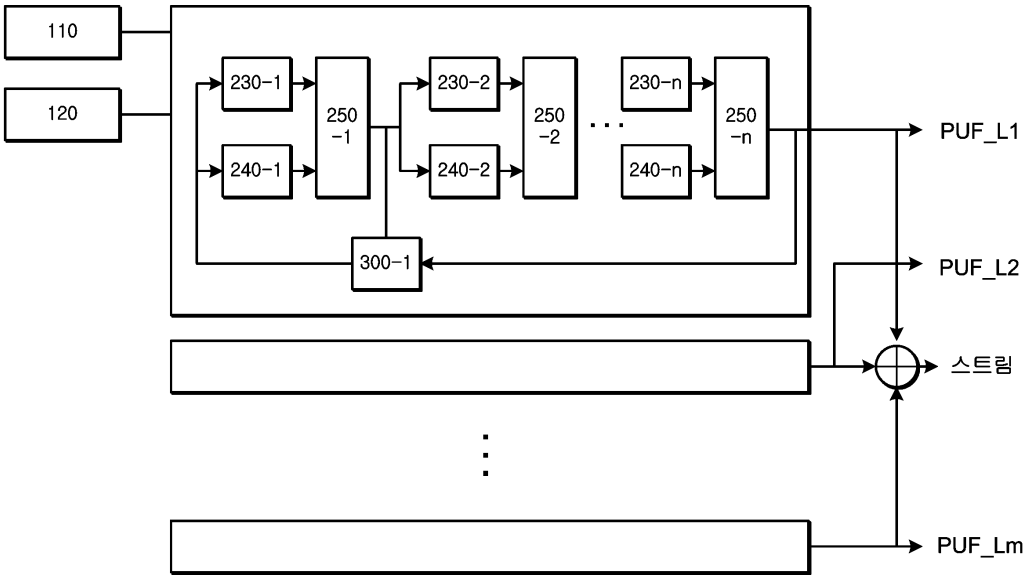
[0051] 도 4는 본 발명의 일 실시예에 따른 통합 보안 방법의 각 단계를 순차적으로 도시한 순서도이다.

도면

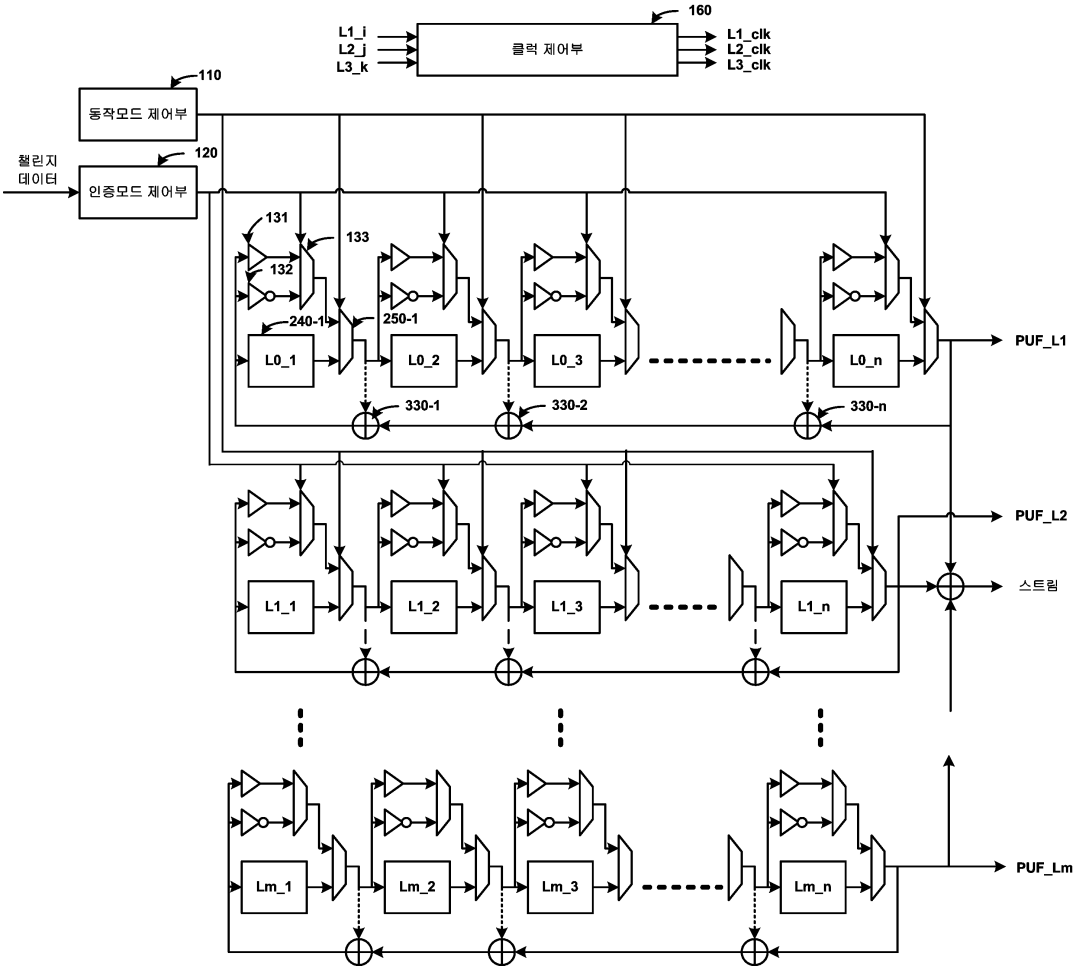
도면1



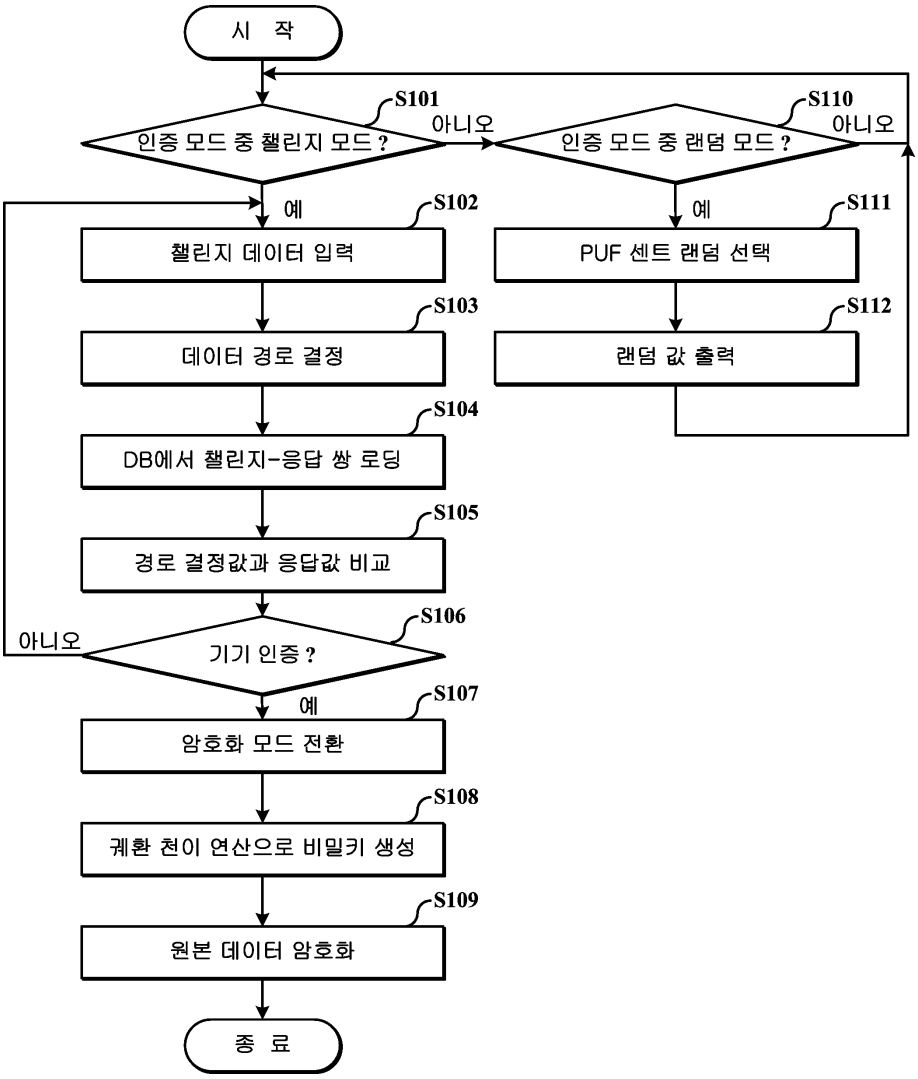
도면2


110
120
230-1
240-1
250-1
230-2
240-2
250-2
230-n
240-n
250-n
300-1
PUF_L1
PUF_L2
스트림
PUF_Lm

도면3


160
L1_i
L2_j
L3_k
클럭 제어부
L1_clk
L2_clk
L3_clk
110
동작모드 제어부
120
챌린지 데이터
인증모드 제어부
131
133
132
240-1
250-1
L0_1
L0_2
L0_3
L0_n
330-1
330-2
330-n
PUF_L1
PUF_L2
스트림
L1_1
L1_2
L1_3
L1_n
Lm_1
Lm_2
Lm_3
Lm_n
PUF_Lm

도면4


시 작
S101
인증 모드 중 챌린지 모드 ?
아니오
예
S102
챌린지 데이터 입력
S103
데이터 경로 결정
S104
DB에서 챌린지-응답 쌍 로딩
S105
경로 결정값과 응답값 비교
S106
기기 인증 ?
아니오
예
S107
암호화 모드 전환
S108
궤환 천이 연산으로 비밀키 생성
S109
원본 데이터 암호화
종 료
S110
인증 모드 중 랜덤 모드 ?
아니오
예
S111
PUF 센트 랜덤 선택
S112
랜덤 값 출력