

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2016-0039010 (43) 공개일자 2016년04월08일
(51) 국제특허분류(Int. Cl.) H04L 9/32 (2006.01)		(71) 출원인 고려대학교 산학협력단 서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(21) 출원번호 10-2014-0131565		
(22) 출원일자 2014년09월30일		(72) 발명자 김현민 서울 성북구 길음로 118, 414동 1801호 (길음동, 길음뉴타운) 홍석희 서울특별시 도봉구 마들로 859-19, 103동 107호 (도봉동, 한신아파트)
심사청구일자 2014년09월30일		(74) 대리인 특허법인충현

전체 청구항 수 : 총 9 항

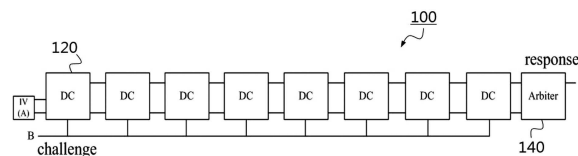
(54) 발명의 명칭 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로

(57) 요약

본 발명은 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로에 관한 것으로서, 보다 바람직하게는 복수 개가 서로 직렬 연결되어, 복수 개의 신호를 입력받고, 입력받은 복수 개의 신호에 각각 설정된 지연시간을 반영한 후 상기 복수 개의 신호를 출력하는 딜레이 셀; 및 상기 딜레이 셀의 끝단에 직렬 연결되어, 상기 딜레이 셀로부터 출력된 복수 개의 신호를 입력받고, 입력받은 복수 개의 신호 중 입력 시간 또는 각 레일의 전력 소비량에 기초하여 하나의 신호를 출력하는 아비터 로직;을 포함한다.

이러한 구성에 의해, 본 발명의 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로는 복수 개의 게이트들을 대신하여 듀얼 레일 딜레이 로직으로 이루어지는 딜레이 셀을 이용함으로써, 사용 면적이 감소함에 따라 제품을 소형화시킬 수 있고, 제품의 기능에 대한 처리를 고속화할 수 있는 효과가 있다.

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

복수 개가 서로 직렬 연결되어, 복수 개의 신호를 입력받고, 입력받은 복수 개의 신호에 각각 설정된 지연시간을 반영한 후 상기 복수 개의 신호를 출력하는 딜레이 셀; 및

상기 딜레이 셀의 끝단에 직렬 연결되어, 상기 딜레이 셀로부터 출력된 복수 개의 신호를 입력받고, 입력받은 복수 개의 신호 중 입력 시간 또는 각 레일의 전력 소비량에 기초하여 하나의 신호를 출력하는 아비터 로직;

을 포함하는 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로.

청구항 2

제1항에 있어서,

상기 딜레이 셀은

적어도 하나의 듀얼 레일 딜레이 로직을 포함하며, 서로 병렬 연결되는 것을 특징으로 하는 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로.

청구항 3

제2항에 있어서,

상기 듀얼 레일 딜레이 로직은

복수 개의 신호를 입력받는 것을 특징으로 하는 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로.

청구항 4

제3항에 있어서,

상기 듀얼 레일 딜레이 로직은

복수 개의 신호를 입력받는 경우, 상기 복수 개의 신호 중 하나의 신호를 챌린지 신호로서 입력받고, 나머지 신호들은 이전 배치된 데이터 셀의 출력값과, 상기 출력값의 보수값으로서 입력받는 것을 특징으로 하는 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로.

청구항 5

제4항에 있어서,

상기 딜레이 셀은

상기 입력받은 챌린지 신호에 응답하여 챌린지 비트 수에 해당하는 개수가 직렬 연결되는 것을 특징으로 하는 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로.

청구항 6

제1항에 있어서,

복수 개가 직렬 연결되는 딜레이 셀 사이에 직렬 연결되는 적어도 하나의 버퍼;
를 더 포함하는 것을 특징으로 하는 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로.

청구항 7

제1항에 있어서,

상기 아비터 로직은

상기 입력받은 복수 개의 신호 중 입력 시간이 가장 빠른 신호에 응답하여 하이 레벨의 신호를 출력하는 것을 특징으로 하는 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로.

청구항 8

제1항에 있어서,

상기 아비터 로직은

아날로그 비교기를 포함하여, 각 레일의 전력 소비량의 크기가 가장 큰 신호에 응답하여 하이 레벨의 신호를 출력하는 것을 특징으로 하는 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로.

청구항 9

제1항에 있어서,

상기 아비터 로직은

비교기, 덧셈기, 나누셈기, 곱셈기 중 적어도 하나를 포함하는 것을 특징으로 하는 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로.

발명의 설명

기술 분야

[0001] 본 발명은 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로에 관한 것으로, 특히 적은 면적에서 후처리 없이 높은 안전성을 가지고 효율적으로 복제 방지가 용이한 디지털 장비에 대한 사용자 인증, 객체 인증 등을 수행할 수 있는 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로에 관한 것이다.

배경 기술

[0002] 최근 IT 기술의 급격한 발전으로 인해 빠른 속도로 새로운 최첨단 디바이스들이 등장하고 있지만, 다른 한 편으로는 불법 복제에 대한 피해와 위조로 인한 경제적, 산업적 손실이 날이 갈수록 커지고 있는 실정이다. 이러한 문제를 해결하고자 물리적 복제 방지(Physical Unclonable Function, 이하, PUF라고 한다.) 시스템이라는 새로운 기술이 등장하였다.

[0003] 이러한 PUF는 마치 인간의 지문 또는 홍채와 같은 생체 정보처럼 각각의 디바이스가 고유의 특성을 가질 수 있는 기술로서, 동일한 공정으로 만들어진 디바이스라 할지라도 다른 특성을 갖도록 하는 기술이다. 즉, PUF는 아무리 똑같은 방법으로 디바이스를 만들어도 절대로 그 고유한 특성만큼은 복제할 수 없는 기술을 나타낸다.

[0004] 이러한 PUF는 물리적으로 랜덤한 특성과 복제 불가능한 특성을 이용하여 현재 주로 안전한 키 스토리지와 객체 인증(ID authentication)에 사용되고 있다. 즉, PUF는 소프트웨어적으로 생성된 함수를 이용하여 랜덤한 시드(seed)를 추출하는 것이 아니라, 물리적으로 칩이나 장비가 제작될 때 각각의 칩과 장비가 동일하게 제작될 수 밖에 없는 물리적인 특성을 이용하여 진성 랜덤(true random)한 시드(seed)값을 추출하고, 추출한 시드값을 사용자 고유의 값으로 이용하여 객체 인증에 사용할 수 있으며, 진성 랜덤한 값이기 때문에 복제 불가능한 칩이나

장비에 적용할 수 있는 코드를 생성하는데 이용할 수 있다.

[0005] 특히, 스탠다드 셀과 메모리 등을 이용한 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 것으로서, 가장 대표적인 예로는 아비터 로직 PUF(Arbiter PUF)와 링 오실레이터 PUF(Ring Oscillator PUF)가 있다.

[0006] 또한 메모리 기반의 PUF의 구체적인 PUF 형태로는 SRAM 메모리 기반의 PUF가 있는데, 이러한 메모리 기반의 PUF는 SRAM메모리가 초기 상태에서의 불안정한 초기값을 이용한 PUF이다. 이러한 메모리 기반의 PUF는 PUF를 만들기 위해 추가적인 작업없이 기존의 메모리 프리미티브(primitive)를 그대로 사용하여 PUF를 만든다는 점에서 다른 PUF들 보다 생성하기 쉽고, 현실적으로 사용가능한 실용적인 PUF이다. 이러한 메모리 기반의 PUF는 SRAM 메모리의 초기값의 무작위성(randomness)은 메모리 제조단계에서 제작 시 모든 메모리들을 동일한 제작 조건하에서 동일한 제작 방식으로 제작하기 어려움에 따라 PUF 특성을 충분히 만족하는 SRAM 기반의 PUF를 쉽게 만들어 낼 수 있는 장점이 있다.

[0007] 나머지 딜레이 기반의 PUF 중 아비터 로직 PUF는 동일한 거리를 갖는 두 경로에 동일한 신호를 전송하여 어떤 신호가 먼저 아비터 로직에 도착하는지에 따라 출력이 결정되는 PUF이다. 하지만 이러한 PUF를 구성하기 위해서는 PUF의 1 bit 출력(response)마다 추가적인 PUF 모듈이 필요하며, 또한 기존 딜레이 기반의 PUF는 많은 수의 멀티 플렉서 및 래치를 사용해야 하므로, 높은 제조 비용이 소요되는 문제점이 발생했다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) KR 10-2013-0129334 (사물지능통신에서 PUF에 기반한 장치간 보안 인증 장치 및 방법, ㈜ 아이 씨터케어) 2013.11.28.

발명의 내용

해결하려는 과제

[0009] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 듀얼 레일 로직을 포함하는 딜레이 셀을 이용하여 물리적 복제 방지 회로를 구현함으로써, 적은 면적뿐만 아니라, 후속 처리 없이 고속의 높은 신뢰성을 가질 수 있는 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로를 제공하고자 한다.

과제의 해결 수단

[0010] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로는 복수 개가 서로 직렬 연결되어, 복수 개의 신호를 입력받고, 입력받은 복수 개의 신호에 각각 설정된 지연시간을 반영한 후 상기 복수 개의 신호를 출력하는 딜레이 셀; 및 상기 딜레이 셀의 끝단에 직렬 연결되어, 상기 딜레이 셀로부터 출력된 복수 개의 신호를 입력받고, 입력받은 복수 개의 신호 중 입력 시간 또는 각 레일의 전력 소비량에 기초하여 하나의 신호를 출력하는 아비터 로직;을 포함한다.

[0011] 보다 바람직하게는 적어도 하나의 듀얼 레일 딜레이 로직을 포함하며, 서로 병렬 연결되는 딜레이 셀을 포함할 수 있다.

[0012] 특히, 복수 개의 신호를 입력받는 듀얼 레일 딜레이 로직을 포함할 수 있다.

[0013] 보다 바람직하게는 복수 개의 신호를 입력받는 경우, 상기 복수 개의 신호 중 하나의 신호를 챌린지 신호로서 입력받고, 나머지 신호들은 이전 배치된 데이터 셀의 출력값과, 상기 출력값의 보수값으로서 입력받는 듀얼 레일 딜레이 로직을 포함할 수 있다.

- [0014] 보다 바람직하게는 상기 입력받은 챌린지 신호에 응답하여 챌린지 비트 수에 해당하는 개수가 직렬 연결되는 딜레이 셀을 포함할 수 있다.
- [0015] 보다 바람직하게는 복수 개가 직렬 연결되는 딜레이 셀 사이에 직렬 연결되는 적어도 하나의 버퍼;를 더 포함할 수 있다.
- [0016] 보다 바람직하게는 상기 입력받은 복수 개의 신호 중 입력 시간이 가장 빠른 신호에 대하여 하이 레벨의 신호를 출력하는 아비터 로직을 포함할 수 있다.
- [0017] 보다 바람직하게는 아날로그 비교기를 포함하여, 입력받은 복수 개의 신호 중 크기가 가장 큰 신호에 대하여 하이 레벨의 신호를 출력하는 아비터 로직을 포함할 수 있다.
- [0018] 보다 바람직하게는 비교기, 덧셈기, 나누셈기, 곱셈기 중 적어도 하나를 포함하는 아비터 로직을 포함할 수 있다.

발명의 효과

- [0019] 본 발명의 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로는 복수 개의 게이트들을 대신하여 듀얼 레일 딜레이 로직으로 이루어지는 딜레이 셀을 이용함으로써, 사용 면적이 감소함에 따라 제품을 소형화시킬 수 있고, 제품의 기능에 대한 처리를 고속화할 수 있는 효과가 있다.
- [0020] 또한, 본 발명의 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로는 듀얼 레일 로직을 갖는 딜레이 셀을 통해 각 레일의 경쟁 조건이 외부의 환경적인 조건에 의해 불가피하게 변화하는 경우에도 후처리 없이 우수한 특성을 가짐에 따라, 후처리 과정에 소요되는 비용을 크기 절감할 수 있는 효과가 있다.
- [0021] 더불어, 본 발명의 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로는 듀얼 레일 로직을 포함하는 복수 개의 딜레이 셀 사이에 버퍼를 삽입하여, 출력 전류에 대한 신호 감쇠 현상을 보상함으로써, 제품의 신뢰성을 향상시킬 수 있는 효과가 있다.

도면의 간단한 설명

- [0022] 도 1은 본 발명의 일 실시 예에 따른 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로의 블록도이다.
- 도 2는 본 발명의 다른 실시 예에 따른 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로의 딜레이 셀 부분을 나타낸 도면이다.
- 도 3은 듀얼 레일 딜레이 로직의 입력 신호를 나타낸 도면이다.
- 도 4는 듀얼 레일 딜레이 로직의 내부 기본 구조를 나타낸 회로도이다.
- 도 5는 듀얼 레일 딜레이 로직의 XOR/XNOR 게이트 구조를 나타낸 회로도이다.

발명을 실시하기 위한 구체적인 내용

- [0023] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 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 실시 예에 한정되는 것은 아니다.
- [0024] 일반적으로 사용되는 물리적 복제 방지 회로(PUF)는 소형의 저전력 회로로서, 표준형 실리콘 칩에 부착되어, 동일한 입력에 대한 출력이 고유한 값이 쌍을 이루는 특성(CRP, Challenge-Response Pair)을 이용하여 칩의 ID를 인증할 수 있다. 즉, 물리적 복제 방지 회로를 이용하여 특정 기기에 대한 인증 방법을 간략히 살펴보면, 인증 서버가 입력값과 이에 대응하는 고유한 출력값(CRPs)를 저장하고, 상기 인증서버에서 인증하고자 하는 해당 기기로 챌린지 값을 전송하면, 물리적 복제 방지 회로를 포함하는 상기 해당 기기는 상기 물리적 복제 방지 회로를 통해 출력값(response)를 전송하고 전송된 출력값과 상기 인증서버에 기저장된 출력값이 일치하는지 여부를 확인함으로써 상기 해당 기기를 인증한다.
- [0025] 이하에서는 상술한 물리적으로 랜덤한 특성과 복제 불가능한 특성을 이용하여 안전한 키 스토리지와 객체 인증

에 사용될 수 있는 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로(PUF)에 대하여 보다 자세히 살펴볼도록 한다.

- [0026] 도 1은 본 발명의 일 실시 예에 따른 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로의 블록도이다.
- [0027] 도 1에 도시된 바와 같이, 본 발명의 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로(100)는 딜레이 셀(120, delay cell) 및 아비터 로직(140, arbiter)를 포함한다.
- [0028] 딜레이 셀(120)은 복수 개가 서로 직렬 연결되어, 복수 개의 신호를 입력받고, 입력받은 복수 개의 신호에 각각 미리 설정된 지연시간을 반영하여, 지연시간이 반영된 복수 개의 신호를 출력한다. 이러한 딜레이 셀(120)은 서로 병렬 연결된 적어도 하나의 듀얼 레일 딜레이 로직(122)을 포함한다.
- [0029] 듀얼 레일 딜레이 로직(122)은 외부로부터 복수 개의 신호를 입력받는데, 입력받은 복수 개의 신호 중 하나의 신호는 챌린지(challenge) 신호로서 입력받고, 나머지 신호들은 상기 듀얼 레일 딜레이 로직(122)이 포함된 데이터 셀이 아닌 이전 배치된 데이터 셀의 출력값과, 상기 출력값의 보수값으로서 입력받는다.
- [0030] 또한 이러한 딜레이 셀(120)은 무작위성(randomness)과 신뢰도(reliability) 특성을 분석에 따른 챌린지 비트에 대응하는 챌린지 신호에 응답하여 챌린지 비트 수에 해당하는 개수가 직렬 연결된다. 예를 들어, 8 비트의 챌린지 비트가 필요하여 2^8 정도의 출력(response) 데이터에 대한 특성을 검증하려면 상기 챌린지 비트 수와 동일한 총 8개의 딜레이 셀을 직렬로 연결하여 물리적 복제 방지 회로를 구성한다.
- [0031] 이때, 상기 딜레이 셀은 내부에 기본적으로 두 개의 듀얼 레일 로직(DCVSL)을 포함할 수 있지만 하나의 듀얼 레일 로직만을 포함하더라도 본 발명을 구현할 수 있다.
- [0032] 특히, 상기 딜레이 셀 내 듀얼 레일 로직을 구성하는 내부 노드의 커패시턴스들은 그 크기가 서로 다르고, 각각의 커패시턴스에 저장될 수 있는 전류의 양 또한 서로 다르다. 따라서, 상기 듀얼 레일 로직으로 입력되는 입력값에 따라 VDD에서 VCC까지의 내부 노드에 충전 또는 방전되는 전류의 양에 의해 듀얼 레일의 두 출력 노드(out과 out bar) 중 각 레일에 해당하는 출력 노드에서 전력 소비량의 차이가 발생한다. 그러므로, 이와 같은 전력 소비량의 차이를 발생시키는 VDD에서 VCC까지의 전력 소비 딜레이 차이를 이용하는 특성을 갖는 듀얼 레일 로직을 포함하는 딜레이 셀(cell)이 구성될 수 있다.
- [0033] 아비터 로직(140)은 복수 개가 직렬 연결되는 딜레이 셀(120)의 끝단에 직렬 연결되어, 앞단에 연결된 상기 딜레이 셀(120)로부터 출력된 복수 개의 신호를 입력받고, 각각의 레일에 대한 경쟁 조건을 판단한 후, 입력받은 복수 개의 신호 중 입력 시간 또는 전력 소비량에 기초하여 하나의 신호(Response)를 출력한다. 이러한 아비터 로직(140)은 복수 개의 입력 신호 중 입력 시간이 가장 빠른 신호에 대하여 하이 레벨(1)의 신호를 출력하고, 상기 입력 시간이 가장 빠른 신호를 제외한 나머지 입력 신호들에 대해서는 로우 레벨(0)의 신호를 출력한다.
- [0034] 또는 상기 아비터 로직(140)이 내부에 아날로그 비교기를 구비하여 각 레일에서 소비되는 전력 소비량을 비교하여 크기가 가장 큰 레일을 통해 입력된 신호에 대하여 하이 레벨(1)의 신호를 출력하고, 나머지 레일을 통해 입력된 신호에 대하여 로우 레벨(0)의 신호를 출력한다.
- [0035] 이에 따라, 상기 아비터 로직(140)이 각 레일에 대한 경쟁 조건(race condition)을 판단하여 신호(Response)를 출력하는데, 예를 들어, 상기 아비터 로직으로 입력된 복수 개의 신호 중 제1 딜레이 레일을 통해 입력된 신호의 입력 시간이 제2 딜레이 레일을 통해 입력된 신호의 입력시간 보다 빠른 경우, 하이 레벨(1)에 해당하는 신호(response)를 출력하고, 그렇지 않는 경우에는 로우 레벨(0)에 해당하는 신호(response)를 출력한다. 이때, 상기 아비터 로직(140)은 비교기, 덧셈기, 나누셈기, 곱셈기 중 적어도 하나를 포함하여 이루어질 수 있다.
- [0036] 뿐만 아니라, 상기 아비터 로직(140)이 각 레일에 대한 경쟁 조건이 아닌 각 레일에서 사용되는 전력 소비량을 비교하여 각 레일의 전력 소비량 중 가장 큰 전력 소비량을 갖는 딜레이 레일을 통해 입력되는 신호에 응답하여 하이 레벨(1)에 해당하는 신호(response)를 출력하고, 전체 레일 중 가장 큰 전력 소비량을 갖는 레일을 제외한 나머지 레일을 통해 입력된 신호에 대해서는 로우 레벨(0)에 해당하는 신호(response)를 출력할 수 있다. 특히, 이처럼 상기 아비터 로직(140)이 각 레일의 전력 소비량을 비교 기준으로 사용하는 경우에는 센스 증폭기(sense amplifier)와 같은 아날로그 비교기를 포함하여 신호를 출력할 수 있다. 이때, 사용되는 센스 증폭기는 컴퓨터 기억 장치에 있어서의 판독 신호를 논리 레벨로 증폭하고, 논리 신호로 변환하기 위해 쓰이는 고이득, 광대역의 증폭기. 판독 증폭기를 나타낸다. 기억 장치에서 미약한 출력 신호를 증폭할 수 있는 이득 대역폭을 가지며, 또 기록 사이클에서 침입하는 잡음에 대한 양호한 잡음 배제성과 과부하 내력, 나아가서는 급속한 성능 회복 능력이 요구된다. 또한 입력 레벨의 판정을 하는 안정적인 임계값 검출기와 올바른 파형을 올바른 시점에서 송출하

기 위한 스트로브 게이트를 가지며, 기록 사이클에서 센스 증폭기에 나타나는 잡음 전압은 거의 동상분 전압이므로, 동상분 배제비가 큰 차동 증폭기가 사용된다.

- [0037] 또한, 상기 아비터 로직으로부터 출력된 출력신호에 해당하는 출력값에 해쉬함수를 적용하여 비밀키를 생성하는데 사용할 수 있다.
- [0038] 이외에도, 상술한 본 발명의 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로는 내부 구성에 딜레이 셀과 아비터 로직 외에도 버퍼(buffer)를 더 포함할 수 있다.
- [0039] 도 2는 본 발명의 다른 실시 예에 따른 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로의 딜레이 셀 부분을 나타낸 도면이다.
- [0040] 도 2에 도시된 바와 같이, 본 발명의 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로는 앞서 도 1을 통해 설명한 딜레이 셀, 아비터 로직 외에도 복수 개의 딜레이 셀(120) 사이에 적어도 하나의 버퍼(130)가 직렬 연결될 수 있는데, 이와 같이 연결되는 버퍼를 통해 8, 16, 24, 32 또는 그 이상에 해당하는 8 비트 기반의 위드단위로 연결하여 챌린지 비트(Challenge bit)를 구성할 수 있다.
- [0041] 뿐만 아니라, 복수 개의 딜레이 셀 사이에 적어도 하나의 버퍼가 직렬 연결되어, 출력 전류에 대한 신호 감쇠(degradation)를 보상해 줌으로써 사용자 신뢰도를 향상시킬 수 있다.
- [0042] 도 3은 듀얼 레일 딜레이 로직의 입력 신호를 나타낸 도면이다.
- [0043] 도 3(a)에 도시된 바와 같이, 본 발명에서 사용되는 듀얼 레일 딜레이 로직은 두 개의 입력 신호를 가지나, 사용자 설정에 의해 도 3(b)에 도시된 바와 같이 3개의 입력 신호 또는 그 이상의 입력 신호를 가질 수 있다.
- [0044] 이처럼, 상기 듀얼 레일 딜레이 로직이 두 개 이상의 입력 신호를 입력받는 경우에는 복수 개의 입력 신호 중 하나의 입력 신호가 챌린지 신호로서 사용될 수 있다. 이후, 상기 챌린지 신호로 사용되는 입력 신호를 제외한 나머지 입력 신호에 대해서는 현재 듀얼 레일 딜레이 로직이 포함된 딜레이 셀의 이전에 배치된 딜레이 셀의 출력값을 나타내는 출력신호와 상기 출력값의 보수값에 해당하는 출력신호가 각각 현재 듀얼 레일 딜레이 로직의 입력신호로서 입력된다.
- [0045] 이러한 듀얼 레일 딜레이 로직의 내부구조는 도 4에 도시된 바와 같이, 딜레이 블록이 하나의 기본 게이트와 동일한 한 개의 듀얼 레일 로직으로 이루어지며, 특히 듀얼 레일 로직의 XOR/XNOR 게이트의 구조는 도 5를 통해 확인할 수 있다. 특히 이때, 상기 듀얼 레일 딜레이 로직을 이루는 PMOS 트랜지스터와 NMOS 트랜지스터의 폭(Width)을 변화시켜 각각의 딜레이 블록을 설계하는 경우, 복수 개의 PUF ID가 설계될 수 있다.
- [0046] 즉, 본 발명의 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로의 동일한 입력에 대한 출력이 고유한 값으로서, 이러한 입력값과 출력값이 쌍을 이루는 특성(CRP, Challenge-Response Pair)을 이용하여 PUF를 기반으로 하는 인증을 용이하게 수행할 수 있다.
- [0047] 상술한 바와 같이 구현된 물리적 복제 방지 회로(PUF)는 다양한 분야에서 사용될 수 있는데, 복제가 불가능해야 하는 신용카드와 같은 금융 IC 또는 자동차 키에 대한 복제 방지를 위한 ID에도 적용할 수 있다. 또한, 상술한 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로는 객체 인증에 대한 초경량화 모듈로도 사용할 수 있는데 예를 들면, 전자 여권과 같이 각 개인의 유일한 ID를 PUF 칩으로 부여함으로써, 매우 작은 크기의 인증모듈을 전자여권상에 탑재할 수 있고, 또한 랜덤한 키를 생성하기 위한 활성화 키(activation key)로도 사용할 수 있어, 기존의 암호화 알고리즘에서의 비밀키로도 안전하게 사용할 수 있다.
- [0048] 본 발명의 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로는 복수 개의 게이트들을 대신하여 듀얼 레일 딜레이 로직으로 이루어지는 딜레이 셀을 이용함으로써, 사용 면적이 감소함에 따라 제품을 소형화시킬 수 있고, 제품의 기능에 대한 처리를 고속화할 수 있는 효과가 있다.
- [0049] 또한, 본 발명의 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로는 듀얼 레일 로직을 갖는 딜레이 셀을 통해 각 레일의 경쟁 조건이 주변 온도 변화 같이 외부의 환경적인 조건에 의해 불가피하게 변화하는 경우에도 후처리 없이 우수한 특성을 가짐에 따라, 후처리 과정에 소요되는 비용을 크기 절감할 수 있는 효과가 있다.
- [0050] 더불어, 본 발명의 듀얼 레일 딜레이 로직을 이용한 물리적 복제 방지 회로는 듀얼 레일 로직을 포함하는 복수 개의 딜레이 셀 사이에 버퍼를 삽입하여, 출력 전류에 대한 신호 감쇠 현상을 보상함으로써, 제품의 신뢰성을 향상시킬 수 있는 효과가 있다.

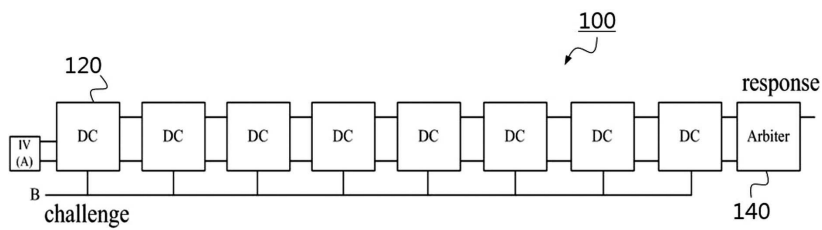
[0051] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

부호의 설명

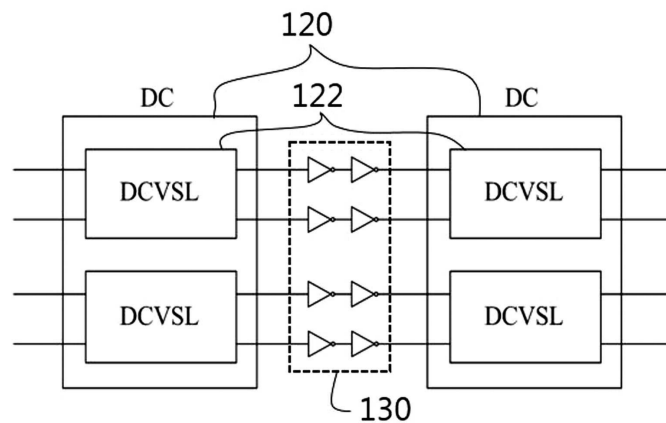
[0052] 120: 딜레이 셀 140: 아비터 로직

도면

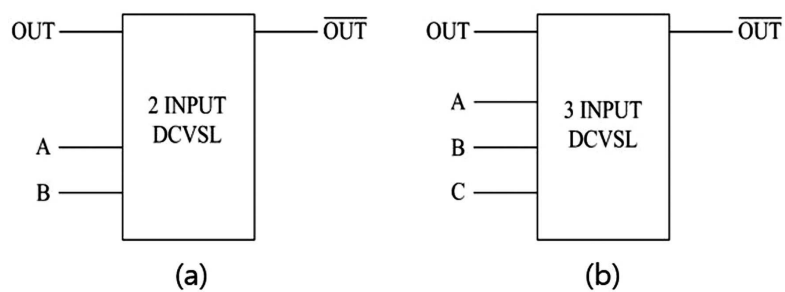
도면1



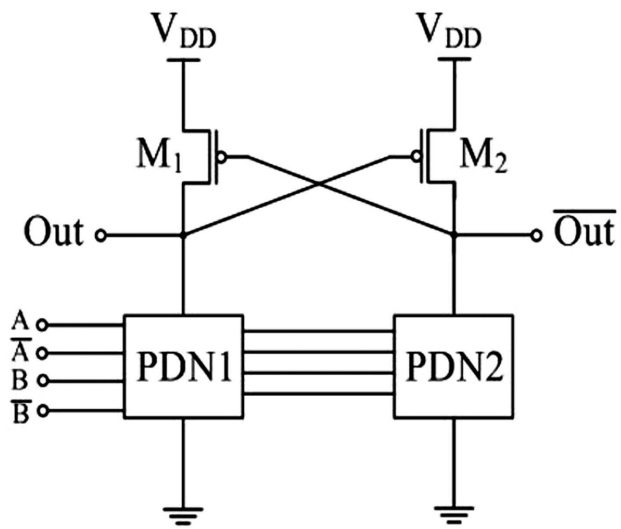
도면2



도면3



도면4



도면5

