(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년12월15일
(11) 등록번호 10-1809076
(24) 등록일자 2017년12월08일

(51) 국제특허분류(Int. Cl.)
G06F 21/75 (2013.01) *G06F 21/87* (2013.01)
H01L 23/00 (2006.01)
(52) CPC특허분류
G06F 21/75 (2013.01)
G06F 21/87 (2013.01)
(21) 출원번호 10-2016-0084835
(22) 출원일자 2016년07월05일
심사청구일자 2016년07월05일
(56) 선행기술조사문헌
KR1020050033780 A*
(뒷면에 계속)

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김승주
서울특별시 송파구 중대로 24, 201동 1401호(문정동, 올림픽훼밀리타운)
이경석
경기도 용인시 기흥구 동백5로 41 3008동 1001호 (중동,성산마을신영지웰아파트)
(74) 대리인
김등용, 김홍석

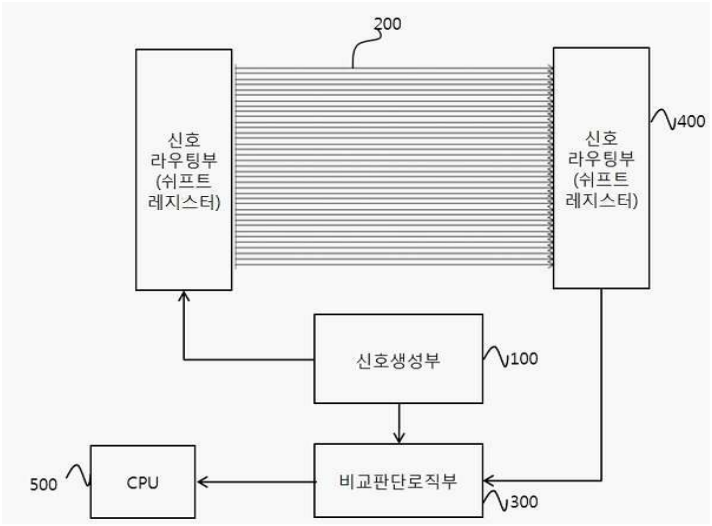
전체 청구항 수 : 총 6 항 심사관 : 구대성

(54) 발명의 명칭 **역설계 방지 집적회로칩**

(57) 요 약

본 발명의 실시예에 따른 역설계 방지 집적회로칩은 제1신호를 발생시키는 신호생성부, 상기 신호생성부에서 생성된 제1신호를 수신하여, 제2신호를 생성하는 메탈라인부, 상기 신호생성부에서 생성된 제1신호와 상기 메탈라인부에서 생성된 제2신호를 비교하는 비교판단로직부 및 상기 메탈라인부의 양측에 형성되어, 상기 일측은 상기 신호생성부와 상기 메탈라인부를 연결하고, 타측은 상기 메탈라인부와 상기 비교판단로직부를 연결하는 신호라우팅부를 포함하되, 상기 신호라우팅부는 시프트 레지스터(Shift Register)이다.

대 표 도 - 도4



(52) CPC특허분류
H01L 23/57 (2013.01)

(56) 선행기술조사문헌
JP11284612 A*
US20030132777 A1
KR1020080087542 A
JP2002296325 A
*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업
과제고유번호 R7117-16-0161
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신방송연구개발사업
연구과제명 자율주행 스마트자동차용 이상징후 탐지 핵심기술개발
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2016.04.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

제1신호를 발생시키는 신호생성부;

상기 신호생성부에서 생성된 제1신호를 수신하여, 제2신호를 생성하는 메탈라인부;

상기 신호생성부에서 생성된 제1신호와 상기 메탈라인부에서 생성된 제2신호를 비교하는 비교판단로직부; 및

상기 메탈라인부의 양측에 형성되어, 일측은 상기 신호생성부와 상기 메탈라인부를 연결하고, 타측은 상기 메탈라인부와 상기 비교판단로직부를 연결하는 신호라우팅부를 포함하되, 상기 신호라우팅부는 시프트 레지스터(Shift Register)이며,

상기 비교판단로직부는 상기 제1신호를 저장하는 제1신호 레지스터;

상기 제2신호를 저장하는 제2신호 레지스터;

상기 제1신호와 상기 제2신호를 비교하는 신호비교모듈;

제1비교데이터를 생성하는 비교데이터생성모듈;

상기 제1비교데이터를 인버팅하여 제2비교데이터를 생성하는 인버터;

상기 신호비교모듈에서의 비교결과, 상기 제1신호와 상기 제2신호가 동일한 경우, 상기 제2비교데이터를 출력하고, 상기 신호비교모듈의 비교결과, 상기 제1신호와 상기 제2신호가 상이한 경우, 상기 제1비교데이터를 출력하는 먹스를 포함하는 것을 특징으로 하는 역설계 방지 집적회로칩.

청구항 2

제1항에 있어서,

상기 비교판단로직부는 상기 제1신호와 서로 대응되는 상기 제2신호를 비교하여, 외부침입여부를 판단하는 것을 특징으로 하는 역설계 방지 집적회로칩.

청구항 3

제2항에 있어서,

상기 비교판단로직부는 외부침입으로 판단되는 경우, 집적회로칩의 초기화 신호 또는 기능차단 신호를 생성하여 중앙처리장치(CPU)에 전송하는 것을 특징으로 하는 역설계 방지 집적회로칩.

청구항 4

삭제

청구항 5

제1항에 있어서,

상기 비교데이터생성모듈은 토글신호를 발생시키는 오실레이터 또는 랜덤신호를 발생시키는 랜덤신호발생기인 것을 특징으로 하는 역설계 방지 집적회로칩.

청구항 6

제1항에 있어서,

상기 비교판단로직부는 상기 먹스로부터 입력되는 데이터가 제1비교데이터인 경우, 외부침입으로 판단하여 집적회로의 초기화 신호 또는 기능차단 신호를 생성하는 판단모듈을 더 포함하는 것을 특징으로 하는 역설계 방지 집적회로칩.

청구항 7

제1항에 있어서,

상기 시프트 레지스터는 단일의 데이터를 입력받아 다수의 데이터를 출력하는 SIPO(Serial-in to Parallel-out) 시프트 레지스터인 것을 특징으로 하는 역설계 방지 집적회로칩.

발명의 설명

기 술 분 야

[0001] 본 발명은 역설계 방지 집적회로칩에 관한 것으로서, 보다 상세하게는 역설계를 방지하기 위한 보안성은 높이면서, 회로의 크기는 최소화 할 수 있는 집적회로칩에 관한 것이다.

배 경 기 술

[0003] 일반적으로 집적회로를 구성하는 실리콘 칩의 구조는 트랜지스터와 금속층으로 이루어져 있다. 금속층은 실리콘 칩이 프로세서 또는 암호엔진으로 동작할 수 있도록 하는 디지털 로직으로서 트랜지스터를 연결하고 있다. 실리콘 칩으로부터 칩에 관한 정보를 얻기 위해서는 다양한 방법이 사용되는데, 특히 스마트 카드에 사용되는 집적회로에서는 공격자가 집적회로의 분석, 소위 역설계(reverse engineering)를 수행하여 얻어진 정보로 회로의 동작 모드를 변동시키거나 메모리 내의 데이터를 조작한다.

[0004] 이러한 방법은 특히 현금 카드 기능 또는 출입 허가 기능을 가진 보안 관련 회로에서 원치 않는 결과를 야기할 수 있다.

[0005] 공격자는 FIB(Focused Ion Beam) 방법과 프로빙(probing) 방법 또는 포싱(forcing) 방법에 의하여 집적회로의 액티브 쉴드를 피하여 집적회로를 해킹한다. FIB(Focused Ion Beam)란 메탈 라인을 임의적으로 단락하거나 연결하는 방법이다. 프로빙(probing) 방법이란 FIB 방법에 의하여 액티브 쉴드의 특정 메탈 라인을 절단하고, 절단된 메탈 라인의 상태값을 독출하는 것을 의미한다. 포싱(forcing)이란 FIB 방법에 의하여 액티브 쉴드의 특정 메탈 라인을 절단하고, 절단된 메탈 라인에 특정한 신호가 제공함으로써 데이터를 조작하는 것을 의미한다.

[0006] 이러한 실리콘 칩의 역설계를 이용하여 칩 내부의 보안구조는 파악이 가능하며, 개인정보나 암호키로서 유용한 정보를 얻기 위해 프로브 공격을 사용할 수 있다. 이 때문에 데이터 암호화 표준(DES), 고급암호화 표준(AES) 및 RSA와 같은 보안관련 블록 엔진 프로빙 공격을 방지하기 위해 칩의 하층에 칩의 보안구조가 위치한다.

[0007] 실리콘 칩의 보안구조에 대한 프로브 공격을 막기 위해서 칩의 표면에 실리콘 표면 보호층을 추가하는 것은 매우 중요하게 되었다. 그러나 실리콘 칩에 별도의 층을 구비하는 것은 전체적인 생산비용 증가, 제조자체의 난해성 등으로 인해서 제조사에 큰 부담이 되고 있으며, 칩의 크기 또한 증가하게 되어, 최소 사이즈로 구현되어야 하는 칩의 특성에 반하고, 칩의 효율성 측면에서도 어려움이 있다.

[0008] 도 1은 종래 집적회로칩의 개념도이다.

[0009] 도 2는 실제 프로브에 탐침을 진행하는 SEM사진이다.

[0010] 도 1과 도 2에 도시된 바와 같이 실리콘 칩의 역설계를 위한 프로브 공격을 방지하기 위해서 실리콘 칩의 상부층에 복수의 메탈라인을 형성하고, 그 하부층에 복수의 메탈라인과 연결되는 라우팅 영역이 존재하게 된다.

[0011] 복수의 메탈라인을 통해서 신호가 일측에서 타측으로 전송되며, 프로브 공격이 있는 경우 메탈라인에서 신호의 이상이 발생하게 되어 공격을 검출하는 방식인데, 이 때 다중신호를 유입해야 하는 메탈라인의 특성상 메탈라인의 하부에는 메탈라인의 양단부를 연결하는 라우팅 영역이 존재하고 되고, 라우팅 영역 사이에는 집적회로가 배치된다.

[0012] 도 3은 라우팅 영역으로 인한 집적회로영역의 감소를 도시한 도면이다.

[0013] 최근 프로브에 의한 탐침기술의 발달로 인하여 역설계를 위한 침입이 가능한데, 이를 막고, 칩 자체의 보안레벨을 높이기 위해서는 메탈라인을 보다 조밀하게 구성해야 한다. 메탈라인을 조밀하게 구성하게 되는 경우 도 3과 같이 라우팅 영역 또한, 차지하는 영역이 넓어지게 되어 라우팅 영역 사이에 놓이게 되는 집적회로의 크기가 줄어들거나 전체적인 칩 사이즈가 커져야 하는 문제점이 있어왔다.(N1은 신호갯수)

선행기술문헌

특허문헌

[0015] (특허문헌 0001) 대한민국 공개특허 제10-2008-0087542호(2008.10.01)

발명의 내용

해결하려는 과제

[0016] 본 발명의 목적은 역설계를 방지하기 위한 집적회로칩에서 보안레벨을 증가시켜 보안성을 강화한 집적회로칩을 제공하는 것이다.

[0017] 본 발명의 목적은 보안성이 강화됨에도 불구하고 집적회로 칩의 크기가 증가하지 않도록 하는 집적회로칩을 제공하는 것이다.

과제의 해결 수단

[0019] 본 발명의 실시예에 따른 역설계 방지 집적회로칩은 제1신호를 발생시키는 신호생성부, 상기 신호생성부에서 생성된 제1신호를 수신하여, 제2신호를 생성하는 메탈라인부, 상기 신호생성부에서 생성된 제1신호와 상기 메탈라인부에서 생성된 제2신호를 비교하는 비교판단로직부 및 상기 메탈라인부의 양측에 형성되어, 상기 일측은 상기 신호생성부와 상기 메탈라인부를 연결하고, 타측은 상기 메탈라인부와 상기 비교판단로직부를 연결하는 신호라우팅부를 포함하되, 상기 신호라우팅부는 시프트 레지스터(Shift Register)이다.

발명의 효과

[0021] 본 발명의 실시예에 따른 역설계 방지 집적회로 칩은 칩의 크기가 커지거나 집적도를 떨어뜨리지 않고도 칩 자체의 보안레벨을 증가시켜 보안성이 증가될 수 있다.

[0022] 또한, 칩 자체의 보안레벨이 증가함에도 면적이 증가하지 않아 칩 자체의 가격상승이 줄어들게 된다.

도면의 간단한 설명

[0024] 도 1은 종래 집적회로칩의 개념도이다.

도 2는 실제 프로브에 탐침을 진행하는 SEM사진이다.

도 3은 라우팅 영역으로 인한 집적회로영역의 감소를 도시한 도면이다.

도 4는 본 발명의 실시예에 따른 역설계 방지 집적회로칩의 기능 블록도이다.

도 5는 본 발명의 실시예에 따른 비교판단로직부의 상세기능블록도이다.

도 6은 SIPO 시프트 레지스터의 회로도이다.

도 7은 SIPO 시프트 레지스터의 시간차트이다.

발명을 실시하기 위한 구체적인 내용

[0025] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0026] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0027] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로

만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0028] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0029] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0030] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0031] 이하 도면을 참고하여 본 발명의 실시예에 따른 역설계 방지 집적회로칩에 대해서 상세히 설명한다.

[0032] 도 4는 본 발명의 실시예에 따른 역설계 방지 집적회로칩의 기능 블록도이다.

[0033] 도 4에 도시된 바와 같이 본 발명의 실시예에 따른 역설계 방지 집적회로칩은 제1신호를 발생시키는 신호생성부(100), 상기 신호생성부(100)에서 생성된 제1신호를 수신하여, 제2신호를 생성하는 메탈라인부(200), 상기 신호생성부(100)에서 생성된 제1신호와 상기 메탈라인부(200)에서 생성된 제2신호를 비교하는 비교판단로직부(300) 및 상기 메탈라인부(200)의 양측에 형성되어, 상기 일측은 상기 신호생성부(100)와 상기 메탈라인부(200)를 연결하고, 타측은 상기 메탈라인부(200)와 상기 비교판단로직부(300)를 연결하는 신호라우팅부(400)를 포함하되, 상기 신호라우팅부(400)는 시프트 레지스터(Shift Register)일 수 있다.

[0034] 본 발명의 실시예에 따른 신호생성부(100)는 제1신호를 발생시킨다. 여기서 제1신호는 임의의 디지털신호일 수 있으며, 집적회로칩의 상부에 형성되어 있는 메탈라인부(200)를 통한 외부침입을 탐지할 수 있는 식별신호로서 기능한다.

[0035] 메탈라인부(200)는 하부에 놓여 있는 집적회로를 보호하기 위한 복수의 금속라인들이 형성되어 있는 구성부분이다. 메탈라인부(200)에 입력된 제1신호는 제2신호로 출력된다. 물론, 메탈라인부(200)에 외부의 침입이 작용하지 않는 경우는 제1신호와 제2신호가 모두 같고, 외부의 침입이 작용하는 경우에는 제1신호와 제2신호가 서로 상이하게 된다. 이러한 점을 이용하여 메탈라인부(200)를 프로브의 침입에 대비하기 위해 촘촘하게 구성하는 것이 바람직하며, 본 발명의 실시예에 따른 메탈라인부(200)는 전체 칩 사이즈를 $1mm^2$ 이고, 전체 라인의 수가 1000개라고 가정하면 1000개의 다른 신호들이 메탈라인부(200)를 통해서 전송된다.

[0036] 1000개의 다른 신호들이 메탈라인부(200)를 통과하는 과정에서 프로브 침입 등을 탐지하는 경우 메탈라인부(200)의 일부 라인에서 신호의 변화가 발생하게 되고, 발생된 신호의 변화는 앞서 설명한 바와 같이 제1신호와 제2신호가 상이한 상태임을 확인한다.

[0037] 비교판단로직부(300)는 신호생성부(100)에서 생성된 제1신호와 메탈라인부(200)에서 출력되는 제2신호를 비교판단한다. 비교판단로직부(300)는 제1신호와 서로 대응되는 제2신호를 비교하여 외부침입여부를 판단하고, 외부침입으로 판단되는 경우 집적회로 칩의 초기화 신호 또는 기능차단 신호를 생성하여 중앙처리장치(CPU)(500)에 전송한다.

[0038] 중앙처리장치(500)는 칩의 초기화 신호 또는 기능차단 신호를 수신하여 집적회로에 침입탐지에 따른 조치를 취하게 된다.

[0039] 도 5는 본 발명의 실시예에 따른 비교판단로직부의 상세기능블록도이다.

[0040] 도 5에 도시된 바와 같이 상기 비교판단로직부(300)는 상기 제1신호를 저장하는 제1신호 레지스터(310), 상기 제2신호를 저장하는 제2신호 레지스터(320), 상기 제1신호와 상기 제2신호를 비교하는 신호비교모듈(330), 제1비교데이터를 생성하는 비교데이터생성모듈(340), 상기 제1비교데이터를 인버팅하여 제2비교데이터를 생성하는 인버터(350), 상기 신호비교모듈(330)에서의 비교결과, 상기 제1신호와 상기 제2신호가 동일한 경우, 상기 제2비교데이터를 출력하고, 상기 신호비교모듈(330)의 비교결과, 상기 제1신호와 상기 제2신호가 상이한 경우, 상기 제1비교데이터를 출력하는 먹스(360)를 포함한다.

[0041] 본 발명의 실시예에 따른 비교판단로직부(300)의 제1신호레지스터(310)는 신호생성부(100)에서 생성된 제1신호를 저장한다. 제2신호 레지스터(320)는 메탈라인부(200)를 통과한 제2신호를 저장한다. 제1신호 레지스터(310)와 제2신호 레지스터(320)에 저장된 제1신호와 제2신호를 신호비교모듈(330)에서 비교한다.

[0042] 신호비교모듈(330)에서의 제1신호와 제2신호 비교에 의해서 제1신호와 제2신호가 동일한 경우에는 메탈라인부(200)를 통한 프로브 침입이 없는 경우이고, 제1신호와 제2신호가 상이한 경우는 메탈라인부(200)를 통한 프로브 침입 등이 감지된 경우이다.

[0043] 비교데이터 생성모듈(340)은 제1비교데이터를 생성한다. 비교데이터 생성모듈(340)은 토글신호를 발생시키는 오실레이터 이거나 랜덤신호를 발생시키는 랜덤신호발생기일 수 있다. 제1비교데이터로 토글신호가 발생한 경우 제1비교데이터를 인버팅하는 인버터(350)에서는 제2비교데이터로 제1비교데이터와 위상이 다른 토글신호를 생성하게 된다.

[0044] 비교데이터 생성모듈(340)에서 생성되는 제1비교데이터는 신호비교모듈(330)에 의해서 판단된 침입결과에 대한 시간대별 침입탐지결과를 제공하기 위한 클럭신호(CLK신호)일 수 있다.

[0045] 먹스(MUX)(360)는 신호비교모듈(330)에서의 비교결과 제1신호와 제2신호가 동일한 경우에는 제2비교데이터를 출력하고, 신호비교모듈(330)의 비교결과 제1신호와 제2신호가 상이한 경우에는 제1비교데이터를 출력한다.

[0046] 비교판단로직부(300)는 먹스(360)로부터 입력되는 데이터가 제1비교데이터인 경우 외부침입으로 판단하여 집적회로의 초기화 신호 또는 기능차단 신호를 생성하는 판단모듈(370)을 더 포함할 수 있다.

[0047] 비교판단로직부(300)의 데이터 흐름에 대해서 도 5를 통해서 설명하면, 비교판단로직부(300)로 입력되는 제1신호와 제2신호를 비교하는 신호비교모듈(330)은 비교결과정보를 먹스(360)로 입력한다. 동시에 비교데이터 생성모듈(340)은 제1비교데이터를 인버터(350)로 입력시키고 인버터(350)는 제1비교데이터를 인버팅한 신호인 제2비교데이터를 생성하여 먹스(360)로 입력시킨다.

[0048] 비교데이터생성모듈(340)의 제1비교데이터는 먹스(360)와 판단모듈(370)로 동시에 전송되고, 먹스(360)는 신호비교모듈(330)에서 전송된 비교결과정보를 통해서 제1비교데이터를 판단모듈(370)로 출력할 것인지 제2비교데이터를 판단모듈(370)로 출력할 것인지를 결정하여 침입이 탐지되었다는 비교결과정보가 전송된 경우 제1비교데이터를 판단모듈(370)로 전송하고, 그렇지 않은 경우는 제2비교데이터를 판단모듈(370)로 전송한다.

[0049] 판단모듈(370)로 들어온 비교데이터가 각각 제1비교데이터, 제2비교데이터인 경우에는 침입이 탐지되지 않은 경우이므로, 그 시간대에 집적회로의 프로세싱은 정상적으로 동작하도록 유지시키고, 판단모듈(370)로 들어온 비교데이터가 각각 제1비교데이터, 제1비교데이터인 경우에는 침입이 탐지된 경우로서, 판단모듈(370)은 앞서 설명한 바와 같이 중앙처리장치(CPU)(500)에 집적회로 초기화 신호 또는 기능차단신호를 생성하여 전송한다.

[0050] 본 발명의 실시예에 따른 신호라우팅부(400)는 메탈라인부(200)의 양측에 형성되어 일측은 신호생성부(100)와 메탈라인부(200)를 연결하고, 타측은 메탈라인부(200)와 비교판단로직부(300)를 연결한다. 특히 본 발명의 실시예에 따른 신호라우팅부(200)는 시프트 레지스터(shift register)일 수 있다.

[0051] 또한, 본 발명의 실시예에 따른 시프트 레지스터는 단일의 데이터를 입력받아 다수의 데이터를 출력하는 SIPO(Serial-in to Parallel-out) 시프트 레지스터일 수 있으며, 다수의 데이터를 입력받아 다수의 데이터를 출력하는 PIPO(Parallel-in Parallel-out) 시프트 레지스터일 수 있으나 반드시 이에 제한되는 것은 아니다.

[0052] 도 6은 SIPO 시프트 레지스터의 회로도이다.

[0053] 본래 시프트 레지스터는 데이터를 저장하거나 데이터를 옆으로 이동할 때 사용하는 회로로서, 데이터 시스템에서 시프트 레지스터와 같이 데이터 및 정보를 저장하고 이동하는 기능을 발전시켜 메모리라는 부품이 개발된 것

이다.

[0054] 도 7은 SIPO 시프트 레지스터의 시간차트이다.

[0055] 도 6, 도 7을 통해 SIPO시프트 레지스터의 동작상태를 살펴보면, SIPO 시프트 레지스터는 단일의 데이터가 시프트 레지스터를 거쳐 다수의 출력으로 나타내는 구조로서 데이터가 입력으로 들어오면 클록이 rising이 되기 전까지 대기하고 있다가 rising edge가 검출되면 Q0으로 데이터를 출력한다(a). 두번째 클록이 들어오면 DATA에 들어오는 새로운 입력이 Q0로 출력되고, Q0에 저장되어 있던 데이터는 Q1으로 출력된다(b). 이러한 방식으로 클록이 발생할 때마다 순차적으로 데이터를 이동시키며(c, d), 클록이 발생하지 않는 동안은 데이터를 유지시켜주는 기능을 가진 회로가 SIPO 시프트 레지스터이다.

[0056] 본 발명의 실시예에 따른 시프트 레지스터를 역설계 방지 집적회로칩의 신호라우팅부(400)에 포함시킴으로서, 종래 신호라우팅 기능을 담당했던 라우팅 영역이 넓어질 필요가 없이 고정된 상태에서 메탈라인부(200)로 제1신호를 전달할 수 있게 된다.

표 1

[0057]

구분	메탈라인부의 신호개수(라인개수) (32line to 128 line)			실시예
N1	32	64	128	1000
Co	6.4%	12.8%	25.6%	0.4%

[0059] 위 표 1에서 N1은 메탈라인부(200)의 라인개수 또는 신호개수를 의미하고, Co는 라우팅 영역의 오버헤드, 다시 말하면 전체 칩의 크기($1mm^2$)에서 라우팅 영역이 차지하는 비율을 의미하고, 종래기술과 같이 라우팅 영역으로 내부금속층을 형성하는 경우(도 1 참고) 32개의 신호를 메탈라인부(200)를 통해서 전송할 때는 6.4%, 62개의 신호를 전송할 때는 12.8%, 128개의 신호를 전송할 때는 25.6%의 면적을 라우팅 영역에서 차지하고 있어, 나머지 영역에 집적회로를 구성해야 하나, 본 발명의 실시예에 따른 집적회로칩의 경우에는 1000개의 신호를 메탈라인부(200)를 통해서 전송할 때 차지하는 신호라우팅부(400)의 할당면적은 전체면적대비 0.4%에 불과하여 나머지 영역에 집적회로를 구성할 수 있는 영역이 넓어지면서 동시에 보안의 강도가 높아짐을 확인할 수 있다.

부호의 설명

[0061]

100 신호생성부 200 메탈라인부

300 비교판단로직부 310 제1신호레지스터

320 제2신호레지스터 330 신호비교모듈

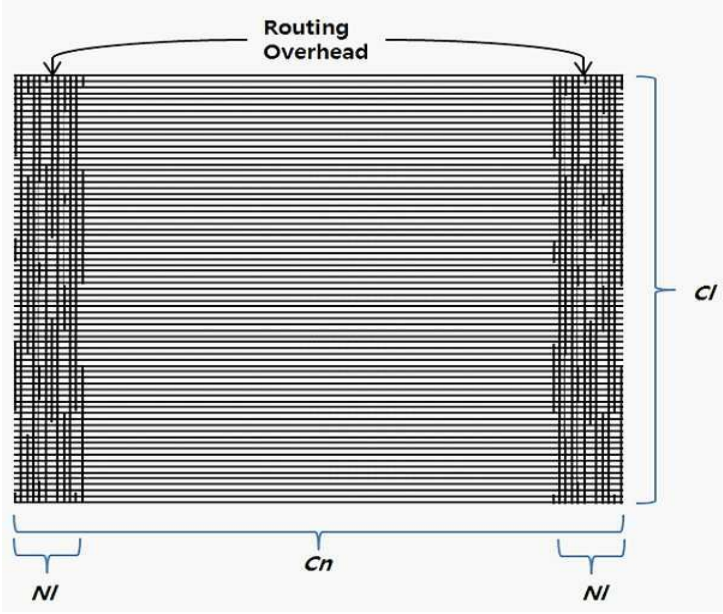
340 비교데이터생성모듈 350 인버터

360 MUX(먹스) 370 판단모듈

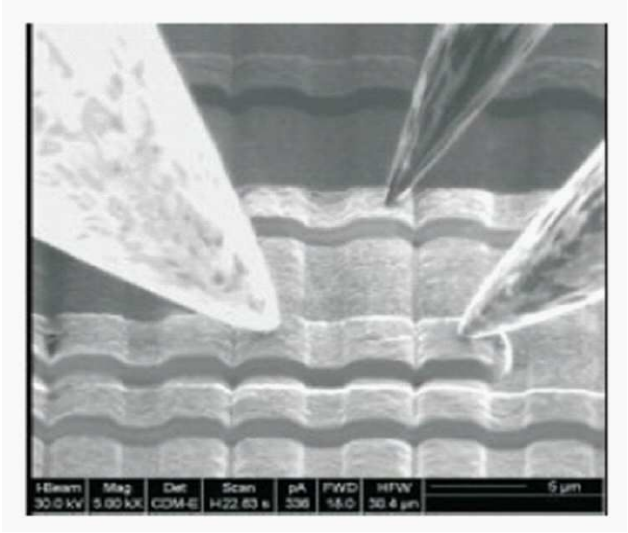
400 신호라우팅부 500 CPU

도면

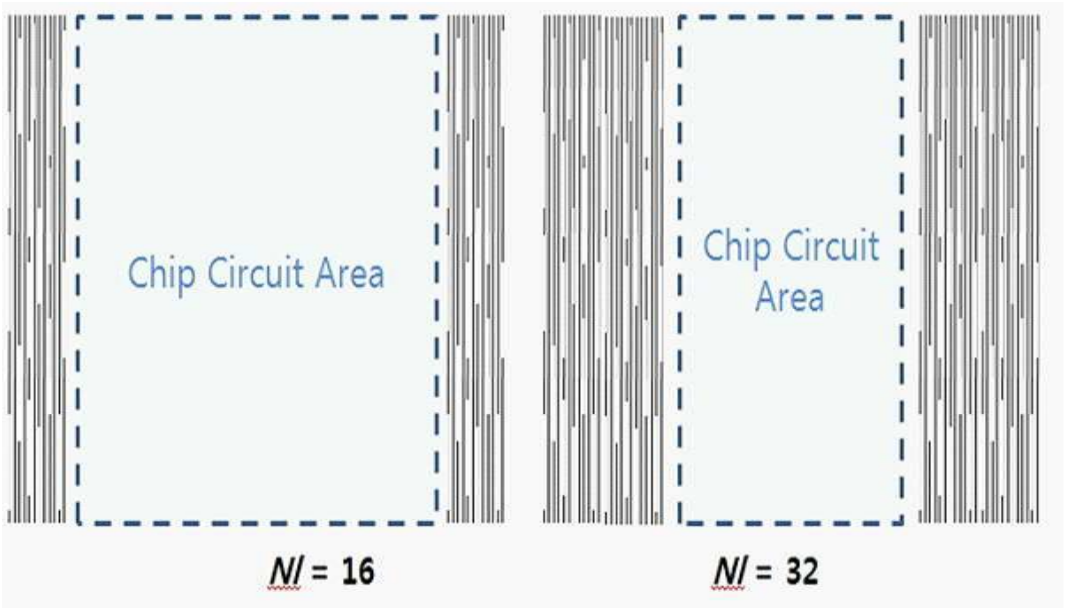
도면1



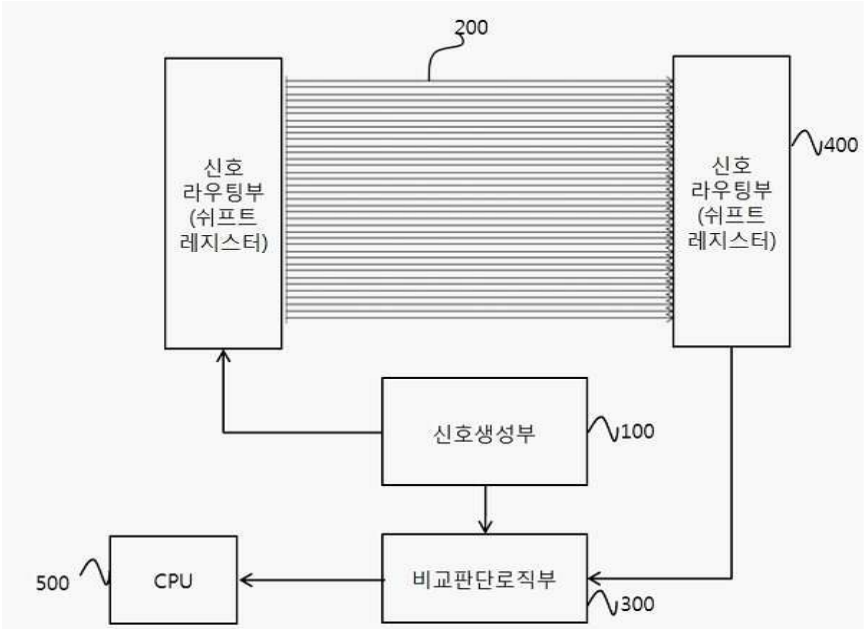
도면2



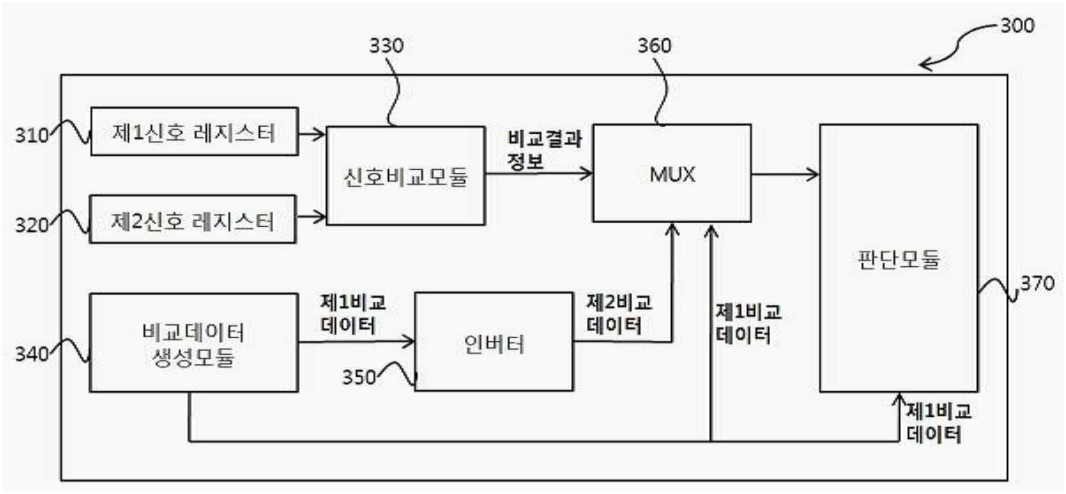
도면3


Chip Circuit Area
N/ = 16
Chip Circuit Area
N/ = 32

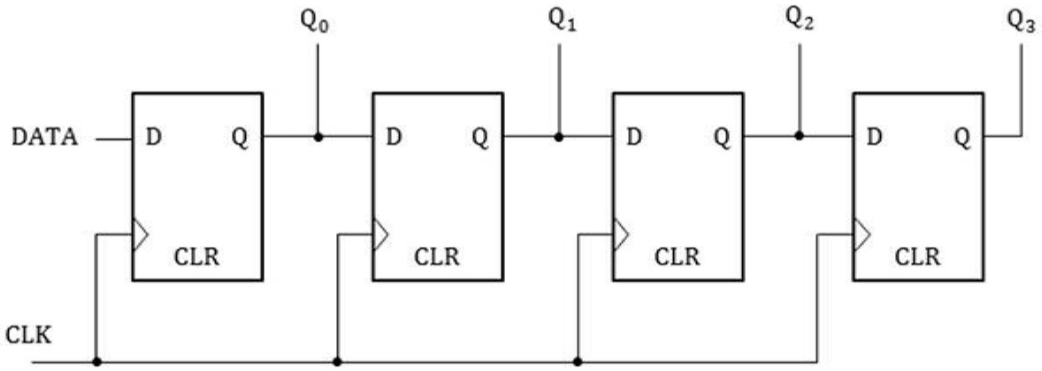
도면4


200
신호 라우팅부 (쉬프트 레지스터)
400
신호 라우팅부 (쉬프트 레지스터)
신호생성부
100
500
CPU
비교판단로직부
300

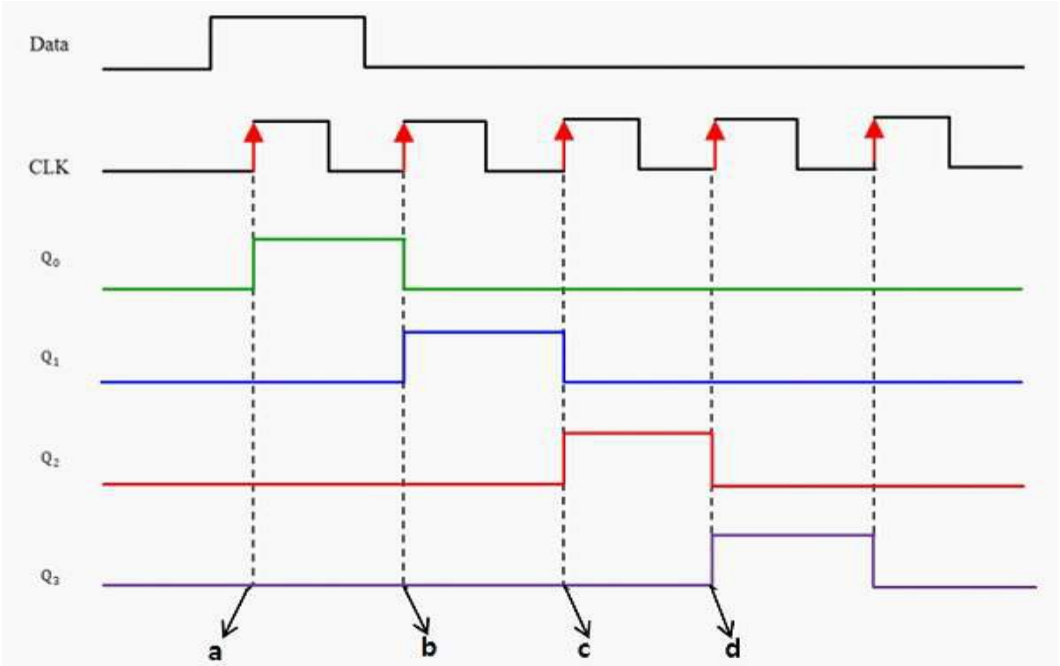
도면5


300
330
360
310
제1신호 레지스터
320
제2신호 레지스터
신호비교모듈
비교결과 정보
MUX
판단모듈
370
340
비교데이터 생성모듈
제1비교 데이터
350
인버터
제2비교 데이터
제1비교 데이터
제1비교 데이터

도면6


Q0
Q1
Q2
Q3
DATA
D
Q
CLR
CLK

도면7


Data
CLK
Q0
Q1
Q2
Q3
a
b
c
d