



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0141783
(43) 공개일자 2020년12월21일

(51) 국제특허분류(Int. Cl.)
G06F 21/75 (2013.01) G06F 21/55 (2013.01)
(52) CPC특허분류
G06F 21/75 (2020.05)
G06F 21/55 (2013.01)
(21) 출원번호 10-2019-0068762
(22) 출원일자 2019년06월11일
심사청구일자 2019년06월11일

(71) 출원인
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
강성호
서울특별시 마포구 양화로 45, 101동 2102호(서교동, 메세나폴리스)
이영우
서울특별시 강남구 개포로109길 21, 301동 1207호(개포동, 대청아파트)
(74) 대리인
특허법인우인

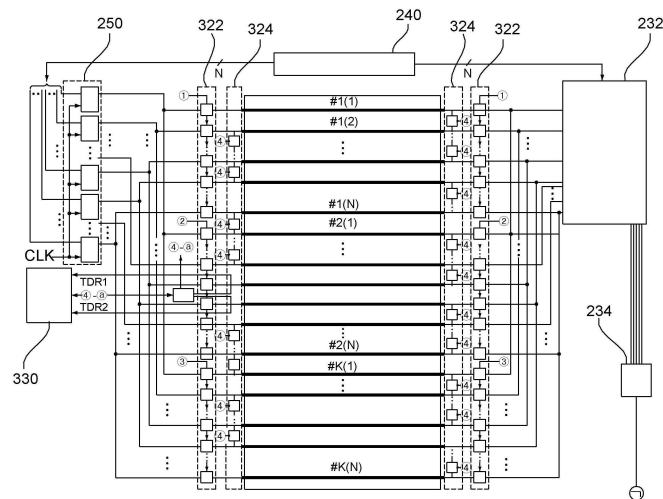
전체 청구항 수 : 총 19 항

(54) 발명의 명칭 침투 공격에 대해 검출 및 보호가 가능한 온칩 보안 회로

(57) 요약

본 실시예들은 쉘드의 와이어의 양단을 하이 임피던스 상태로 변경하여 와이어의 연결 상태를 변경하고 연결된 와이어 경로를 통해 반사된 테스트 신호를 분석하여 마이크로 프로브 공격을 감지하거나, 쉘드의 와이어의 양단을 하이 임피던스 상태로 변경하여 와이어의 연결 상태를 변경하고 그룹별로 선택된 와이어를 통과한 테스트 신호를 분석하여 집속 이온빔 공격을 감지하거나, 검출 회로를 통해 외부 공격을 감지하면 접근 가능한 신호 경로를 하이 임피던스 상태로 변경하여 물리적인 접근을 차단할 수 있는 보안 회로를 제공한다.

대표도



이 발명을 지원한 국가연구개발사업

과제고유번호	1711091198
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	(유형2)중견연구(연평균연구비 2억원~4억원 이내)
연구과제명	인-메모리 컴퓨팅의 로버스트니스 향상을 위한 반도체 설계 기술
기 여 율	1/1
과제수행기관명	연세대학교 산학협력단
연구기간	2019.03.01 ~ 2020.02.29

명세서

청구범위

청구항 1

M(상기 M은 2보다 큰 자연수) 개의 와이어를 포함하며 반도체 칩의 상부에 배치되는 설드; 및

상기 M 개의 와이어의 연결 상태를 변경하여 와이어 경로를 설정하고, 상기 와이어 경로를 이동한 테스트 신호를 분석하여 외부 공격을 감지하는 검출 회로를 포함하며,

상기 검출 회로는 상기 M 개의 와이어를 연결하여 복수의 와이어 경로를 생성하고, 상기 복수의 와이어 경로의 끝단을 상기 테스트 신호의 반사가 가능한 임피던스 값으로 변경하는 것을 특징으로 하는 보안 회로.

청구항 2

제1항에 있어서,

상기 검출 회로는 제어 신호를 전송하는 제어부, 상기 제어 신호에 따라 하이 임피던스 상태로 변경되어 상기 M 개의 와이어의 연결 상태를 변경하는 신호 경로 변경부, 및 상기 와이어 경로에 연결되며 상기 테스트 신호를 분석하는 신호 분석부를 포함하며,

상기 제어부가 상기 복수의 와이어 경로에 테스트 신호를 각각 인가하면, 상기 신호 분석부는 상기 복수의 와이어 경로의 끝단에서 각각 반사된 복수의 테스트 신호를 비교하여 시간 지연을 검출하는 것을 특징으로 하는 보안 회로.

청구항 3

제2항에 있어서,

상기 신호 분석부는 감지 증폭기(Sense Amplifier)로 구현되며,

상기 감지 증폭기는 (i) 상기 제어부가 상기 테스트 신호를 상기 복수의 와이어 경로에 인가하는 시점에 제1 크기를 갖는 신호들을 생성하고, (ii) 상기 반사된 복수의 테스트 신호가 인가되는 시점에 제2 크기를 갖는 신호들을 생성하여, 상기 제2 크기를 갖는 신호들의 차이를 비교하여 신호의 지연을 검출하는 것을 특징으로 하는 보안 회로.

청구항 4

제2항에 있어서,

상기 감지 증폭기는 상기 제1 크기를 갖는 신호들을 비교하지 않도록 상기 제1 크기보다 크고 상기 제2 크기보다 작게 설정된 임계치에서 동작하는 것을 비교하는 것을 특징으로 하는 보안 회로.

청구항 5

제2항에 있어서,

상기 신호 경로 변경부는 상기 M 개의 와이어의 입력단의 일부 또는 전부를 외부로부터 분리하고, 상기 M 개의 와이어의 출력단의 일부 또는 전부를 외부로부터 분리하여, 상기 입력단 및 상기 출력단에서 신호의 흐름을 차단하는 와이어 분리부를 포함하고,

상기 신호 경로 변경부는 상기 M 개의 와이어의 입력단의 일부를 상호 연결하고, 상기 M 개의 와이어의 출력단의 일부를 상호 연결하여, 와이어 경로를 형성하는 와이어 연결부를 포함하는 것을 특징으로 하는 보안 회로.

청구항 6

제5항에 있어서,

상기 신호 경로 변경부는 상기 와이어 분리부와 상기 와이어 연결부를 이용하여 동일한 캐패시터 값을 갖는 제1

와이어 경로와 제2 와이어 경로를 생성하는 것을 특징으로 하는 보안 회로.

청구항 7

제5항에 있어서,

상기 와이어 분리부는 3 상태 버퍼(3 State Buffer)로 구현되며,

상기 와이어 연결부는 트랜스미션 게이트(Transmission Gate)로 구현되는 것을 특징으로 하는 보안 회로.

청구항 8

제1항에 있어서,

상기 와이어 경로를 형성하는 와이어의 개수를 증가시켜 감지 가능한 캐패시터의 최소값을 감소시키는 것을 특징으로 하는 보안 회로.

청구항 9

M(상기 M은 2보다 큰 자연수) 개의 와이어를 포함하며 반도체 칩의 상부에 배치되는 절드; 및

상기 M 개의 와이어의 연결 상태를 변경하여 와이어 경로를 설정하고, 상기 와이어 경로를 이동한 테스트 신호를 분석하여 외부 공격을 감지하는 검출 회로를 포함하며,

상기 검출 회로는 상기 M 개의 와이어를 K(상기 K는 상기 M보다 작은 자연수) 개의 와이어 그룹으로 그룹핑하고, 상기 K 개의 와이어 그룹 중에서 선택된 와이어 그룹의 와이어 경로를 활성화하는 것을 특징으로 하는 보안 회로.

청구항 10

제9항에 있어서,

상기 검출 회로는 제어 신호를 전송하는 제어부, 상기 제어 신호에 따라 하이 임피던스 상태로 변경되어 상기 M 개의 와이어의 연결 상태를 변경하는 신호 경로 변경부, 및 상기 와이어 경로에 연결되며 상기 테스트 신호를 분석하는 신호 분석부를 포함하며,

상기 제어부는 상기 제어 신호를 기 설정된 시간 간격으로 상기 K 개의 와이어 그룹 중에서 일부의 와이어 그룹에 전송하여 상기 K 개의 와이어 그룹을 순차적으로 활성화하는 것을 특징으로 하는 보안 회로.

청구항 11

제9항에 있어서,

상기 검출 회로는 N(상기 N은 상기 M보다 작은 자연수) 개의 비트를 랜덤하게 생성하는 비트 생성부, 및 상기 비트 생성부로부터 상기 N 개의 비트를 수신하고 상기 N 개의 비트를 저장하는 비트 저장부를 포함하며,

상기 비트 저장부는 상기 K 개의 와이어 그룹에 연결되어 상기 N 개의 비트를 상기 테스트 신호로 제공하고,

상기 K 개의 와이어 그룹이 상기 비트 저장부를 공유하는 것을 특징으로 하는 보안 회로.

청구항 12

제11항에 있어서,

상기 신호 분석부는 상기 K 개의 와이어 그룹을 통과한 테스트 신호와 상기 비트 생성부로부터 수신한 N 개의 비트를 비교하여, 그룹별로 테스트 신호의 이상 여부를 판단하는 그룹 신호 비교부를 포함하는 것을 특징으로 하는 보안 회로.

청구항 13

제12항에 있어서,

상기 신호 분석부는 상기 그룹 신호 비교부로부터 신호를 수신하여 상기 N 개의 비트 중에서 적어도 하나의 이상 여부를 판단하는 통합 신호 비교부를 포함하는 것을 특징으로 하는 보안 회로.

청구항 14

M(상기 M은 2보다 큰 자연수) 개의 와이어를 포함하며 반도체 칩의 상부에 배치되는 설드; 및

상기 M 개의 와이어의 연결 상태를 변경하여 와이어 경로를 설정하고, 상기 와이어 경로를 이동한 테스트 신호를 분석하여 외부 공격을 감지하는 검출 회로를 포함하며,

상기 검출 회로는 상기 와이어 경로의 하이 임피던스 상태를 변경하여 마이크로 프로브 공격을 감지하는 제1 진단 모드 또는 집속 이온빔 공격을 감지하는 제2 진단 모드로 설정하는 것을 특징으로 하는 보안 회로.

청구항 15

제14항에 있어서,

상기 검출 회로는 제어 신호를 전송하는 제어부, 상기 제어 신호에 따라 하이 임피던스 상태로 변경되어 상기 M 개의 와이어의 연결 상태를 변경하는 신호 경로 변경부, 및 상기 와이어 경로에 연결되며 상기 테스트 신호를 분석하는 신호 분석부를 포함하며,

상기 제어부는 (i) 제1 시점에 상기 제1 진단 모드를 동작시키는 제1 제어 신호를 상기 신호 경로 변경부로 전송하고, (ii) 제2 시점에 상기 제2 진단 모드를 동작시키는 제2 제어 신호를 상기 신호 경로 변경부로 전송하는 것을 특징으로 하는 보안 회로.

청구항 16

제15항에 있어서,

상기 신호 경로 변경부는 상기 M 개의 와이어의 입력단 및 출력단에 연결된 3 상태 버퍼들을 공유하며, 상기 제1 제어 신호 및 상기 제2 제어 신호에 따라 상기 M 개의 와이어의 입력단 및 출력단의 일부 또는 전부를 하이 임피던스 상태로 선택하는 것을 특징으로 하는 보안 회로.

청구항 17

제14항에 있어서,

상기 신호 분석부는 상기 제1 진단 모드에서 감지한 신호의 이상 여부 및 상기 제2 진단 모드에서 감지한 신호의 이상 여부를 모두 검출하는 것을 특징으로 하는 보안 회로.

청구항 18

복수의 와이어를 통과한 출력 신호를 분석하여 외부 공격을 감지하는 검출 회로; 및

상기 검출 회로가 상기 외부 공격을 감지하면, 보호 대상에 연결된 신호 경로를 하이 임피던스 상태로 변경하여 접근을 차단하는 보호 회로

를 포함하는 보안 회로.

청구항 19

제1항에 있어서,

상기 보호 대상의 신호 경로에 신호 경로 차단부가 연결되며,

상기 보호 회로는 안티 퓨즈(Anti Fuse) 방식으로 상기 보호 대상에 연결된 상기 신호 경로 차단부를 인에이블하는 것을 특징으로 하는 보안 회로.

발명의 설명

기술 분야

본 실시예가 속하는 기술 분야는 반도체 칩 내부의 정보를 보호하는 하드웨어 기반의 검출 및 보호 회로에 관한 것이다.

[0001]

배경 기술

- [0002] 이 부분에 기술된 내용은 단순히 본 실시예에 대한 배경 정보를 제공할 뿐 종래기술을 구성하는 것은 아니다.
- [0003] 반도체 칩에 대한 다양한 물리적 공격 및 소프트웨어 공격은 SoC(System on Chip)를 이용한 제품 및 이를 이용한 응용 서비스에 위협이 된다. 공격자들은 집적 회로에 관한 리버스 엔지니어링(Reverse Engineering)을 수행하고, 획득된 정보를 이용하여 회로의 동작 모드를 임의적으로 변경하거나 메모리 내에 저장된 데이터의 조작을 수행한다.
- [0004] 반도체 칩에 대한 물리적 침투(Invasive) 공격은 칩에 직접 접근하여 내부 구조를 관측하거나 분석하는 방식이다. 공격 방식은 크게 집속 이온빔(Focused Ion Beam, FIB) 장비를 이용한 칩 수정 방식과 마이크로 프로브(Micro Probe) 접근을 통한 회로 변형 방식이 있다. 집속 이온빔 공격 방식은 이온빔을 이용하여 메탈 라인을 임의적으로 단락하거나 연결한다. 마이크로 프로브 공격 방식은 특정 메탈 라인에 관한 상태값을 독출한다.
- [0005] 반도체 칩에 관한 침투 공격은 중요 데이터에 관한 해킹이나 출입 보안을 해체하는 현실적인 문제를 발생시킨다.

선행기술문헌

특허문헌

- [0006] (특허문헌 0001) 한국공개특허공보 제10-2017-0095155호 (2017.08.22.)

발명의 내용

해결하려는 과제

- [0007] 본 발명의 실시예들은 쉘드의 와이어의 양단을 하이 임피던스 상태로 변경하여 와이어의 연결 상태를 변경하고 연결된 와이어 경로를 통해 반사된 테스트 신호를 분석하여 마이크로 프로브 공격을 감지하는 것을 주된 목적으로 한다.
- [0008] 본 발명의 실시예들은 쉘드의 와이어의 양단을 하이 임피던스 상태로 변경하여 와이어의 연결 상태를 변경하고 그룹별로 선택된 와이어를 통과한 테스트 신호를 분석하여 집속 이온빔 공격을 감지하는 것을 다른 목적으로 한다.
- [0009] 본 발명의 실시예들은 쉘드의 와이어의 양단을 하이 임피던스 상태로 변경하는 3 상태 버퍼를 공유하고 선택적으로 제어하여 마이크로 프로브 공격 및 집속 이온빔 공격을 모두 진단하는 것을 다른 목적으로 한다.
- [0010] 본 발명의 실시예들은 검출 회로를 통해 외부 공격을 감지하면 접근 가능한 신호 경로를 하이 임피던스 상태로 변경하여 물리적인 접근을 차단하는 것을 다른 목적으로 한다.
- [0011] 본 발명의 명시되지 않은 또 다른 목적들은 하기의 상세한 설명 및 그 효과로부터 용이하게 추론할 수 있는 범위 내에서 추가적으로 고려될 수 있다.

과제의 해결 수단

- [0012] 본 실시예의 일 측면에 의하면, M (상기 M 은 2보다 큰 자연수) 개의 와이어를 포함하며 반도체 칩의 상부에 배치되는 쉘드, 및 상기 M 개의 와이어의 연결 상태를 변경하여 와이어 경로를 설정하고, 상기 와이어 경로를 이동한 테스트 신호를 분석하여 외부 공격을 감지하는 검출 회로를 포함하며, 상기 검출 회로는 상기 M 개의 와이어를 연결하여 복수의 와이어 경로를 생성하고, 상기 복수의 와이어 경로의 끝단을 상기 테스트 신호의 반사가 가능한 임피던스 값으로 변경하는 것을 특징으로 하는 보안 회로를 제공한다.
- [0013] 본 실시예의 다른 측면에 의하면, M (상기 M 은 2보다 큰 자연수) 개의 와이어를 포함하며 반도체 칩의 상부에 배치되는 쉘드, 및 상기 M 개의 와이어의 연결 상태를 변경하여 와이어 경로를 설정하고, 상기 와이어 경로를 이동한 테스트 신호를 분석하여 외부 공격을 감지하는 검출 회로를 포함하며, 상기 검출 회로는 상기 M 개의 와이어를 K (상기 K 는 상기 M 보다 작은 자연수) 개의 와이어 그룹으로 그룹핑하고, 상기 K 개의 와이어 그룹 중에서 선택된 와이어 그룹의 와이어 경로를 활성화하는 것을 특징으로 하는 보안 회로를 제공한다.

[0014] 본 실시예의 다른 측면에 의하면, M(상기 M은 2보다 큰 자연수) 개의 와이어를 포함하며 반도체 칩의 상부에 배치되는 쉘드, 및 상기 M 개의 와이어의 연결 상태를 변경하여 와이어 경로를 설정하고, 상기 와이어 경로를 이동한 테스트 신호를 분석하여 외부 공격을 감지하는 검출 회로를 포함하며, 상기 검출 회로는 상기 와이어 경로의 하이 임피던스 상태를 변경하여 마이크로 프로브 공격을 감지하는 제1 진단 모드 또는 집속 이온빔 공격을 감지하는 제2 진단 모드로 설정하는 것을 특징으로 하는 보안 회로를 제공한다.

[0015] 본 실시예의 다른 측면에 의하면, 복수의 와이어를 통과한 출력 신호를 분석하여 외부 공격을 감지하는 검출 회로, 및 상기 검출 회로가 상기 외부 공격을 감지하면, 보호 대상에 연결된 신호 경로를 하이 임피던스 상태로 변경하여 접근을 차단하는 보호 회로를 포함하는 보안 회로를 제공한다.

발명의 효과

[0016] 이상에서 설명한 바와 같이 본 발명의 실시예들에 의하면, 쉘드의 와이어의 양단을 하이 임피던스 상태로 변경하여 와이어의 연결 상태를 변경하고 연결된 와이어 경로를 통해 반사된 테스트 신호를 분석하여 마이크로 프로브 공격을 감지할 수 있는 효과가 있다.

[0017] 본 발명의 실시예들에 의하면, 쉘드의 와이어의 양단을 하이 임피던스 상태로 변경하여 와이어의 연결 상태를 변경하고 그룹별로 선택된 와이어를 통과한 테스트 신호를 분석하여 집속 이온빔 공격을 감지할 수 있는 효과가 있다.

[0018] 본 발명의 실시예들에 의하면, 쉘드의 와이어의 양단을 하이 임피던스 상태로 변경하는 3 상태 버퍼를 공유하고 선택적으로 제어하여 마이크로 프로브 공격 및 집속 이온빔 공격을 모두 진단할 수 있는 효과가 있다.

[0019] 본 발명의 실시예들에 의하면, 검출 회로를 통해 외부 공격을 감지하면 접근 가능한 신호 경로를 하이 임피던스 상태로 변경하여 물리적인 접근을 차단할 수 있는 효과가 있다.

[0020] 여기에서 명시적으로 언급되지 않은 효과라 하더라도, 본 발명의 기술적 특징에 의해 기대되는 이하의 명세서에서 기재된 효과 및 그 잠정적인 효과는 본 발명의 명세서에 기재된 것과 같이 취급된다.

도면의 간단한 설명

[0021] 도 1 및 도 2는 본 발명의 실시예들에 따른 보안 회로들을 예시한 블록도이다.

도 3은 본 발명의 일 실시예에 따른 보안 회로의 제1 검출 회로를 예시한 블록도이다.

도 4 및 도 5는 본 발명의 다른 실시예에 따른 보안 회로의 제2 검출 회로를 예시한 블록도이다.

도 6 및 도 7은 본 발명의 또 다른 실시예에 따른 보안 회로의 제3 검출 회로를 예시한 블록도이다.

도 8은 본 발명의 실시예들에 따른 보안 회로의 제1 제어부를 예시한 회로도이다.

도 9는 본 발명의 실시예들에 따른 보안 회로의 제1 검출 회로 및 제2 검출 회로를 예시한 회로도이다.

도 10은 본 발명의 실시예들에 따른 보안 회로의 제3 검출 회로를 예시한 회로도이다.

도 11은 본 발명의 실시예들에 따른 보안 회로의 제3 신호 분석부를 예시한 회로도이다.

도 12 및 도 13은 본 발명의 실시예들에 따른 보안 회로의 보호 회로를 예시한 회로도이다.

도 14는 본 발명의 실시예들에 따른 보안 회로의 동작을 예시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하, 본 발명을 설명함에 있어서 관련된 공지기능에 대하여 이 분야의 기술자에게 자명한 사항으로서 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하고, 본 발명의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다.

[0023] 반도체 칩에 대한 다양한 물리적 공격 및 소프트웨어 공격은 반도체 칩의 보안 또는 안정성 측면에서 위협이 될 수 있다. 특히, 반도체 칩의 디패키징을 통해 반도체 칩 내부의 데이터 버스에 접근하는 경우 데이터가 해킹 등에 노출될 수 있으므로 이러한 경우 데이터 유출을 원천적으로 차단할 수 있는 구조가 필요하다.

[0024] IC(Integrated Circuit) 카드 등에 사용되는 집적 회로에 대해 공격자들은 집적 회로에 관한 리버스 엔지니어링

(Reverse Engineering)을 수행하고, 획득된 정보를 이용하여 회로의 동작 모드를 임의적으로 변경하거나 메모리 내에 저장된 데이터의 조작을 수행할 수 있다. 위와 같은 반도체 칩에 관한 공격은 중요 데이터에 관한 해킹이나 출입 보안을 해체하는 것과 같은 현실적인 문제들을 야기할 가능성이 존재한다.

- [0025] 공격자들은 FIB(Focused Ion Beam) 방법, 마이크로 프로빙(Probing) 방법 및 포싱(Forcing) 방법 등을 이용하여 집적회로 내의 설드를 회피하여 상기 집적회로에 관한 공격을 수행할 수 있다. FIB는 이온빔을 이용하여 메탈 라인을 임의적으로 단락 하거나 연결하는 방법을 나타낸다. 마이크로 프로빙 방법은 특정 메탈 라인에 관한 상태값을 독출하는 방법을 나타낸다. 포싱이란 FIB 방법에 의해 특정 메탈 라인을 절단하고, 절단된 메탈 라인에 대해 특정한 조작 신호를 제공하여 데이터를 조작하는 공격을 나타낸다.
- [0026] 도 1 및 도 2는 본 발명의 실시예들에 따른 보안 회로들을 예시한 블록도이다.
- [0027] 도 1에 도시된 바와 같이 보안 회로(10)는 검출 회로(12) 및 설드(14)를 포함한다. 도 2에 도시된 바와 같이 보안 회로(20)는 검출 회로(22), 설드(24), 및 보호 회로(26)를 포함할 수 있다.
- [0028] 설드(14, 24)는 메탈 라인을 포함하며, 프로세서의 상부에 배치되어 프로세서를 보호할 수 있다. 설드(14, 24)는 복수의 메탈 라인을 포함하는 액티브 설드와 같은 형태로 구현될 수 있다.
- [0029] 검출 회로(12, 22)는 설드(14, 24)의 와이어의 양단을 하이 임피던스 상태로 변경하는 3 상태 버퍼들을 공유하고 3 상태 버퍼들을 선택적으로 제어하여 마이크로 프로브 공격 및 집속 이온빔 공격을 모두 진단할 수 있다. 설드(14, 24)는 M (M 은 2보다 큰 자연수) 개의 와이어를 포함하며 반도체 칩의 상부에 배치된다. 검출 회로(12, 22)는 M 개의 와이어의 연결 상태를 변경하여 와이어 경로를 설정하고, 와이어 경로를 이동한 테스트 신호를 분석하여 외부 공격을 감지한다. 검출 회로(12, 22)는 와이어 경로의 하이 임피던스 상태를 변경하여 마이크로 프로브 공격을 감지하는 제1 진단 모드 또는 집속 이온빔 공격을 감지하는 제2 진단 모드로 설정할 수 있다. 제1 검출 회로(100)는 집속 이온빔 공격을 감지하는 제2 검출 회로(200)와 마이크로 프로브 공격을 감지하는 제3 검출 회로(300)를 선택적으로 동작시킨다.
- [0030] 검출 회로(12, 22)는 설드(14, 24)의 와이어의 양단을 하이 임피던스 상태로 변경하여 와이어의 연결 상태를 변경하고 그룹별로 선택된 와이어를 통과한 테스트 신호를 분석하여 집속 이온빔 공격을 감지한다. 설드(14, 24)는 M (M 은 2보다 큰 자연수) 개의 와이어를 포함하며 반도체 칩의 상부에 배치된다. 검출 회로(12, 22)는 M 개의 와이어의 연결 상태를 변경하여 와이어 경로를 설정하고, 와이어 경로를 이동한 테스트 신호를 분석하여 외부 공격을 감지한다. 검출 회로(12, 22)는 M 개의 와이어를 K (K 는 상기 M 보다 작은 자연수) 개의 와이어 그룹으로 그룹핑하고, K 개의 와이어 그룹 중에서 선택된 와이어 그룹의 와이어 경로를 활성화할 수 있다. 제2 검출 회로(200)는 집속 이온빔 공격을 감지한다.
- [0031] 검출 회로(12, 22)는 설드(14, 24)의 와이어의 양단을 하이 임피던스 상태로 변경하여 와이어의 연결 상태를 변경하고 연결된 와이어 경로를 통해 반사된 테스트 신호를 분석하여 마이크로 프로브 공격을 감지한다. 설드(14, 24)는 M (M 은 2보다 큰 자연수) 개의 와이어를 포함하며 반도체 칩의 상부에 배치된다. 검출 회로(12, 22)는 M 개의 와이어의 연결 상태를 변경하여 와이어 경로를 설정하고, 와이어 경로를 이동한 테스트 신호를 분석하여 외부 공격을 감지한다. 검출 회로(12, 22)는 M 개의 와이어를 연결하여 복수의 와이어 경로를 생성하고, 복수의 와이어 경로의 끝단을 하이 임피던스 상태로 변경할 수 있다. 제3 검출 회로(300)는 마이크로 프로브 공격을 감지한다.
- [0032] 보호 회로(26)는 검출 회로(22)를 통해 외부 공격을 감지하면 접근 가능한 신호 경로를 하이 임피던스 상태로 변경하여 물리적인 접근을 차단한다. 검출 회로(22)는 복수의 와이어를 통과한 출력 신호를 분석하여 외부 공격을 감지한다.
- [0033] 도 3은 본 발명의 일 실시예에 따른 보안 회로의 제1 검출 회로를 예시한 블록도이다.
- [0034] 제1 검출 회로(100)는 제1 제어부(110), 제1 신호 경로 변경부(120), 및 제1 신호 분석부(130)를 포함한다. 제1 검출 회로(100)는 제2 검출 회로(200) 및 제3 검출 회로(300)를 포함할 수 있다.
- [0035] 제1 제어부(110)는 제어 신호를 제1 신호 경로 변경부(120) 및 제1 신호 분석부(130)로 전송한다. 제1 신호 경로 변경부(120)는 수신한 제어 신호에 따라 하이 임피던스 상태로 변경되어 M 개의 와이어의 연결 상태를 변경하여 와이어 경로를 설정한다. 제1 신호 분석부(130)는 와이어 경로에 연결되며 테스트 신호를 분석한다.
- [0036] 제1 제어부(110)는 (i) 제1 시점에 제1 진단 모드를 동작시키는 제1 제어 신호를 제1 신호 경로 변경부(120)로 전송하고, (i) 제2 시점에 제2 진단 모드를 동작시키는 제2 제어 신호를 제1 신호 경로 변경부(120)로

전송한다. 제1 제어부(110)는 제2 제어부(210) 및 제3 제어부(310)를 포함한다.

- [0037] 제1 신호 경로 변경부(120)는 제2 신호 경로 변경부(120) 및 제3 신호 경로 변경부(120)를 포함하여, 제1 신호 경로 변경부(120)는 와이어 분리부(322)를 공유한다.
- [0038] 제1 신호 경로 변경부(120)는 M 개의 와이어의 입력단 및 출력단에 연결된 3 상태 버퍼들을 공유하며, 제1 제어 신호 및 제2 제어 신호에 따라 M 개의 와이어의 입력단 및 출력단의 일부 또는 전부를 하이 임피던스 상태로 선택한다.
- [0039] 제1 신호 분석부(130)는 제1 진단 모드에서 감지한 신호의 이상 여부 및 제2 진단 모드에서 감지한 신호의 이상 여부를 모두 검출할 수 있다. 제1 신호 분석부(130)는 제2 신호 분석부(230)에서 검출한 결과와 제3 신호 분석부(330)에서 검출한 결과를 종합하여 판단한다.
- [0040] 도 4 및 도 5는 본 발명의 다른 실시예에 따른 보안 회로의 제2 검출 회로를 예시한 블록도이다.
- [0041] 제2 검출 회로(200)는 제2 제어부(210), 제2 신호 경로 변경부(220), 제2 신호 분석부(230), 및 비트 생성부(240)를 포함한다. 제2 검출 회로(200)는 비트 저장부(250)를 추가로 포함할 수 있다.
- [0042] 제2 제어부(210)는 제어 신호를 제2 신호 경로 변경부(220), 제2 신호 분석부(230), 비트 생성부(240), 및 비트 저장부(250)로 전송한다. 제어 신호로 스텝 펄스 등이 인가될 수 있다. 제2 신호 경로 변경부(220)는 수신한 제어 신호에 따라 하이 임피던스 상태로 변경되어 M 개의 와이어의 연결 상태를 변경하여 와이어 경로를 설정한다. 제2 신호 분석부(230)는 와이어 경로에 연결되며 테스트 신호를 분석한다.
- [0043] 제2 제어부(210)는 제어 신호를 기 설정된 시간 간격으로 K 개의 와이어 그룹 중에서 일부의 와이어 그룹에 전송하여 K 개의 와이어 그룹을 순차적으로 활성화할 수 있다.
- [0044] 제2 신호 경로 변경부(220)는 와이어 분리부(322)를 포함한다.
- [0045] 제2 신호 분석부(230)는 그룹 신호 비교부(232) 및 통합 신호 비교부(234)를 포함할 수 있다. 그룹 신호 비교부(232)는 K 개의 와이어 그룹을 통과한 테스트 신호와 비트 생성부(240)로부터 수신한 N 개의 비트를 비교하여, 그룹별로 테스트 신호의 이상 여부를 판단한다. 통합 신호 비교부(234)는 그룹 신호 비교부로부터 신호를 수신하여 상기 N 개의 비트 중에서 적어도 하나의 이상 여부를 판단한다.
- [0046] 비트 생성부(240)는 N 개의 비트를 랜덤하게 생성한다.
- [0047] 비트 저장부(250)는 비트 생성부(240)로부터 N 개의 비트를 수신하고 N 개의 비트를 저장한다. 비트 저장부(250)는 K 개의 와이어 그룹에 연결되어 N 개의 비트를 테스트 신호로 제공한다. K 개의 와이어 그룹이 비트 저장부(240)를 공유한다.
- [0048] 도 6 및 도 7은 본 발명의 또 다른 실시예에 따른 보안 회로의 제3 검출 회로를 예시한 블록도이다.
- [0049] 제3 검출 회로(300)는 제3 제어부(310), 제3 신호 경로 변경부(320), 및 제3 신호 분석부(330)를 포함한다.
- [0050] 제3 제어부(310)는 제어 신호를 제3 신호 경로 변경부(320) 및 제3 신호 분석부(330)로 전송한다. 제어 신호로 스텝 펄스 등이 인가될 수 있다. 제3 신호 경로 변경부(320)는 수신한 제어 신호에 따라 하이 임피던스 상태로 변경되어 M 개의 와이어의 연결 상태를 변경하여 와이어 경로를 설정한다. 제3 신호 분석부(330)는 와이어 경로에 연결되며 테스트 신호를 분석한다. 테스트 신호로 스텝 펄스 등이 인가될 수 있다.
- [0051] 제3 제어부(310)가 복수의 와이어 경로에 테스트 신호를 각각 인가하면, 제3 신호 분석부(330)는 복수의 와이어 경로의 끝단에서 각각 반사된 복수의 테스트 신호를 비교하여 시간 지연을 검출한다.
- [0052] 제3 신호 경로 변경부(320)는 와이어 분리부(322) 및 와이어 연결부(324)를 포함한다.
- [0053] 와이어 분리부(322)는 M 개의 와이어의 입력단의 일부 또는 전부를 외부로부터 분리하고, M 개의 와이어의 출력단의 일부 또는 전부를 외부로부터 분리하여, 입력단 및 상기 출력단에서 신호의 흐름을 차단한다.
- [0054] 와이어 연결부(324)는 M 개의 와이어의 입력단의 일부를 상호 연결하고, M 개의 와이어의 출력단의 일부를 상호 연결하여, 와이어 경로를 형성한다.
- [0055] 제3 신호 경로 변경부(320)는 와이어 분리부(322)와 와이어 연결부(324)를 이용하여 동일한 캐패시터 값을 갖는 제1 와이어 경로와 제2 와이어 경로를 생성할 수 있다.

[0056] 와이어 분리부(322)는 3 상태 버퍼(3 State Buffer)로 구현될 수 있고, 와이어 연결부(324)는 트랜스미션 게이트(Transmission Gate)로 구현될 수 있다.

[0057] 제3 신호 분석부(330)는 감지 증폭기(Sense Amplifier)로 구현될 수 있다.

[0058] 감지 증폭기는 (i) 제3 제어부(310)가 테스트 신호를 복수의 와이어 경로에 인가하는 시점에 제1 크기를 갖는 신호들을 생성하고, (ii) 반사된 복수의 테스트 신호가 인가되는 시점에 제2 크기를 갖는 신호들을 생성하여, 제2 크기를 갖는 신호들의 차이를 비교하여 신호의 지연을 검출한다. 감지 증폭기는 제1 크기를 갖는 신호들을 비교하지 않도록 제1 크기보다 크고 제2 크기 보다 작게 설정된 임계치에서 동작한다.

[0059] 제3 검출 회로(300)는 쉘드(14, 24)에서 와이어 경로를 형성하는 와이어의 개수를 증가시켜 감지 가능한 캐패시터의 최소값을 감소시킨다. 검출 가능한 캐패시터 값이 고정되면 더 작은 캐패시터 값을 갖는 마이크로 프로브 공격에 무력화된다. 본 실시예에 따른 보안 회로는 검출 가능한 최소 캐패시터 값을 설계 초기단계에서 동적으로 조정이 가능하여, 새로운 프로브에도 대응이 가능하다.

[0060] 프로브가 접촉되면 와이어의 캐패시터 값은 변경된다. 프로브의 기생 캐패시터(C_p)에 대한 알람 발생이 불가능한 조건은 수학적 식 1과 같이 표현된다.

수학적 식 1

$$C_p < \frac{t_{SATDR2} - t_{SATDR1} - t_H}{(N_{WIRE} - 1) \times (k_{PMOS} + k_{NMOS}) \times \Omega \times |\Delta N_{PROBE}|}$$

[0061]

[0062] t_{SATDR1} 및 t_{SATDR2} 는 두 개의 와이어 경로에서 각각 반사되어 검출된 왕복 시간이다. t_H 는 기 설정된 홀드 시간이다. N_{wire} 는 와이어 경로의 원래 와이어의 개수이다. Ω 는 공급 전압과 임계 전압에 따른 트랜지스터의 저항이다. $(k_{PMOS} + k_{NMOS})$ 는 PMOS 트랜지스터 및 NMOS 트랜지스터의 잔여 트랜지스터 파라미터에 따른 트랜스 저항(Trans-Resistance)이다. ΔN_{PROBE} 는 와이어 연결된 프로브의 개수이다.

[0063] 프로브의 기생 캐패시터(C_p)에 대한 알람 발생이 가능한 조건은 수학적 식 2과 같이 표현된다.

수학적 식 2

$$C_p > \frac{t_{SATDR2} - t_{SATDR1} + t_H}{(N_{WIRE} - 1) \times (k_{PMOS} + k_{NMOS}) \times \Omega \times |\Delta N_{PROBE}|}$$

[0064]

[0065] 프로브의 기생 캐패시터(C_p)는 와이어의 개수에서 1을 뺀 값에 반비례하므로 본 실시예에 따른 보안 회로는 와이어 경로를 형성하는 와이어의 개수를 증가시켜 감지 가능한 캐패시터의 최소값을 감소시킬 수 있다.

[0066] 도 8은 본 발명의 실시예들에 따른 보안 회로의 제1 제어부를 예시한 회로도이다.

[0067] 기존의 방식들은 복수의 공격 방법 중에서 한 가지 공격만 검출이 가능하며 나머지 다른 공격에는 취약한 단점이 있다. 제안 발명은 두 가지 공격 방법 모두 검출이 가능하여 적은 하드웨어 오버헤드를 갖고, 각각의 공격에 대해서도 빠른 검출 시간으로 검출이 가능하다.

[0068] 본 실시예에 따른 보안 회로는 침투 공격 검출을 위해서 칩 내부를 보호하기 위하여 메탈 상부에 와이어를 평행하게 구축한 쉘드(Shield)를 갖는다. 쉘드에 와이어의 수를 M 개라고 가정하면 M 개의 와이어에 대하여 침투 공격 여부를 실시간으로 계속해서 진단을 진행한다.

[0069] 제1 제어부(110)는 제2 제어부(210) 및 제3 제어부(310)를 포함하며, 제어 신호로 스텝 펄스 등이 인가될 수 있다. 제1 제어부(110)는 검출 부분 선택 및 모드를 자동적으로 선택한다.

- [0070] 제1 제어부(110) 또는 제2 제어부(220)는 집속 이온빔 공격을 감지하는 제2 검출 회로(200)를 동작시키는 제어 신호를 순차적으로 전송한다. 제1 제어부(110) 또는 제2 제어부(220)는 복수의 플립플롭(111, 112, 113, 114)을 이용하여 제어 신호의 시간 간격을 조절하거나 트랜지스터(115) 등을 이용하여 신호의 경로 또는 타이밍을 조절한다. 도 8의 ①, ②, 및 ③은 도 9의 ①, ②, ③에 연결된다. 제1 제어부(110) 또는 제2 제어부(220)는 도 8의 ①, ②, ③을 통하여 3 개의 와이어 그룹에 각각 대응하는 제어 신호를 와이어 분리부(322)에 전송한다.
- [0071] 제1 제어부(110) 또는 제3 제어부(320)는 마이크로 프로브 공격을 감지하는 제3 검출 회로(300)를 동작시키는 제어신호를 전송한다. 도 8의 ④ 및 ④-a는 도 9의 ④ 및 ④-a에 연결된다. 제1 제어부(110) 또는 제3 제어부(320)는 도 8의 ④를 통하여 제1 와이어 경로 및 제2 와이어 경로로 제어 신호를 전송하고, 도 8의 ④-a를 통하여 와이어 연결부(324) 및 제3 신호 분석부(330)로 제어 신호를 전송한다.
- [0072] 도 9는 본 발명의 실시예들에 따른 보안 회로의 제1 검출 회로 및 제2 검출 회로를 예시한 회로도이다.
- [0073] 비트 생성부(240)는 Block Cipher로 구현될 수 있으며, N 개의 랜덤(Random) 비트를 생성한다. 비트 저장부(250)는 N 개의 공유된 플립플롭으로 생성된 비트를 전달한다. 생성된 N 개의 비트는 N 개의 와이어를 동시에 모니터링이 가능하다. M 개의 와이어를 검증하기 위해서 총 M/N 번의 랜덤 비트 생성 및 검증을 진행한다. N 개의 생성된 비트는 공유된 플립플롭을 이용하여 하드웨어를 최소화할 수 있다.
- [0074] 비트 저장부(250)에 저장된 비트는 입력단에 위치하는 와이어 분리부(322)를 통하여 와이어를 통과한다. 그룹 신호 비교부(232)는 출력단에 위치하는 와이어 분리부(322)를 통하여 해당 비트의 변형 여부를 체크한다.
- [0075] 와이어 분리부(322)는 3 상태 버퍼를 이용하여 입력단과 출력단에서 N 개의 와이어만 순차적으로 활성화시켜서 공격 여부를 진단한다. 도 8의 제1 제어부(110) 또는 제2 제어부(210)을 통해 3 상태 버퍼로 구현된 와이어 분리부(322)를 제어한다.
- [0076] 제1 제어부(110) 또는 제2 제어부(210)는 3 상태 버퍼를 통하여 와이어 그룹을 선택하고, 해당하는 와이어 그룹의 N 개의 랜덤 비트를 비교하기 위해서 N 개의 XOR 게이트를 이용하여 원하는 데이터를 비교한다.
- [0077] 만약 N 개의 랜덤 비트 중 단 하나라도 비트에 이상이 있다면 N-입력 OR 게이트로 구성된 통합 신호 비교부(234)에서 알람 신호를 출력한다. 예컨대, 로직 로우(0)는 정상이고, 로직 하이(1)는 알람을 의미한다. 도 9의 ㉞는 도 12의 ㉞에 연결된다.
- [0078] M 개의 와이어에 대해서 순차적으로 모두 진단이 끝나면, 시간 영역 반사(Time Domain Reflection, TDR)을 통한 물리적 와이어 길이와 신호 지연 비교를 통한 FIB 공격 재검증 및 마이크로 프로빙 공격 검출 진단이 진행된다.
- [0079] 도 10a 및 도 10b는 본 발명의 실시예들에 따른 보안 회로의 제3 검출 회로를 예시한 회로도이다.
- [0080] TDR 검증을 위해서, 복수의 와이어 영역으로 구분한다. 예컨대, 도 10a는 2 개의 와이어 영역을 예시하고 있다. 칩을 2 영역으로 나누어 각 영역의 와이어는 와이어 분리부(324)를 이용하여 하나의 와이어로 길게 연결한다. 이때 필요에 따라 칩을 2등분이 아닌 수로 나누어도 무방하다. 와이어 분리부(324)는 트랜스미션 게이트(Transmission Gate)로 구현될 수 있다. 트랜스미션 게이트는 인에이블 신호가 로직 하이이면 입력에서 출력으로 신호를 전달하고, 로직 로우이면 하이 임피던스 상태가 될 수 있다. 인에이블 신호에 따른 동작을 반대로 설정할 수도 있다.
- [0081] 제1 제어부(110) 또는 제3 제어부(310)를 통하여 쉴드 바깥쪽에 위치한 모든 입력단과 출력단의 와이어 분리부(322)는 하이 임피던스 모드로 설정되어 완전히 격리(isolation) 상태로 만든다. 와이어 분리부(322)는 3 상태 버퍼로 구현될 수 있다. 3 상태 버퍼는 인에이블 신호가 로직 로우이면 입력에서 출력으로 신호를 전달하고, 로직 하이이면 하이 임피던스 상태가 될 수 있다. 인에이블 신호에 따른 동작을 반대로 설정할 수도 있다.
- [0082] 하나의 긴 와이어로 연결된 동일한 두 개의 와이어에서 갖고 있는 캐패시터는 동일하며, 제1 제어부(110) 또는 제3 제어부(310)에서 발생된 스텝 펄스(Step Pulse)를 동시에 인가한다.
- [0083] 도 10a를 참조하면 인가된 스텝 펄스 신호는 와이어 선을 따라 진행하고 양 끝단(322-1, 322-2)에 위치한 3 상태 버퍼를 만난다. 도 10b를 참조하면 3 상태 버퍼는 하이 임피던스 상태이므로 신호가 다시 반사되어 되돌아오게 된다. 반사된 신호가 스텝 펄스를 인가한 지점까지 다시 돌아오는데 걸리는 시간은 FIB 공격이나 프로브 시도(Probe Attempt)가 없다면 두 와이어 모두 반드시 동일하다.
- [0084] 도 11은 본 발명의 실시예들에 따른 보안 회로의 제3 신호 분석부를 예시한 회로도이다.

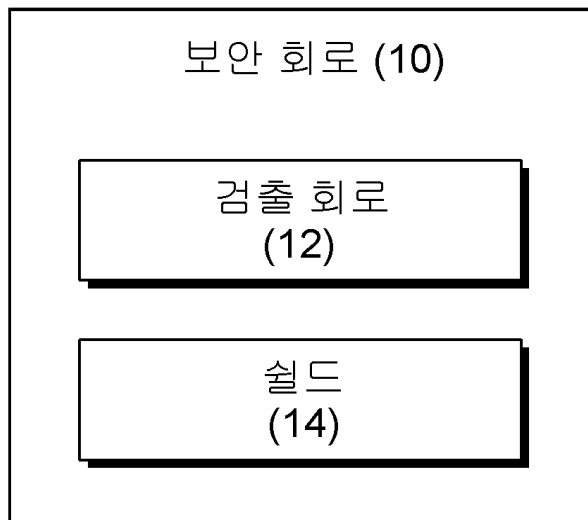
- [0085] 제3 신호 분석부(330)는 두 개의 반사된 신호의 도착 시간을 비교하기 위하여 감지 증폭기(Sense Amplifier)를 사용할 수 있다. 감지 증폭기를 통하여 두 개의 반사된 신호의 미세한 차이를 비교한다.
- [0086] 스텝 펄스가 인가되는 시점에는 VDD의 절반의 크기(Amplitude)가 생성되고 2T 즉 신호가 반사되어 되돌아오는 시간 이후에는 VDD와 동일한 크기가 생성된다. 반사되어 돌아오는 신호가 아닌 처음 인가되는 스텝 펄스의 차이를 비교하지 않도록 감지 증폭에 사용되는 입력의 트랜지스터는 고 임계 전압을 갖는 것으로 사용한다.
- [0087] 반사된 두 신호가 정확하게 일치한다면 감지 증폭기 내부의 PMOS와 NMOS들의 온 저항(On-Resistance)에 따른 전압으로 분배되어 감지 증폭기의 두 개의 출력 모두 미드밴드보다 높은 하이 값을 출력한다. 두 신호 중에서 한 신호에 지연이 발생되어 먼저 도착한다면 해당 출력이 로직 하이에서 로직 로우로 먼저 변경된다. 결국 두 신호의 도착 시간이 다르다면 한쪽은 로직 하이를 다른 한쪽은 로직 로우를 출력한다.
- [0088] 따라서 SA 출력단에 XOR 게이트를 이용한 알람부를 통하여 알람 신호를 출력한다. 예컨대, 로직 로우(0)는 정상이고, 로직 하이(1)는 알람을 의미한다. 도 11의 ㉠은 도 12의 ㉠에 연결된다.
- [0089] 본 실시예에 따른 TDR 검증 방식은 연결된 와이어의 물리적 길이 비교가 가능하므로, 이전 단계에서 시행하였던 랜덤 비트 생성을 통한 암호 통신(Encrypted Communication) 기반의 검증 방법을 통한 FIB 공격에 대한 재검증이 가능하고, 프로브 침투를 통한 미세한 캐패시터 변화에 의한 신호 지연 검출이 가능하다.
- [0090] 도 12 및 도 13은 본 발명의 실시예들에 따른 보안 회로의 보호 회로를 예시한 회로도이다.
- [0091] 검출 회로에서 물리 공격을 감지한다면, 알람부에서 발생된 알람 신호는 동기화부(27)를 거쳐 보호 회로(26)로 전달된다. 동기화부(27)는 클럭 신호에 따라 동기화되고, 출력 신호에 따라 초기화될 수 있다. 도 8의 ㉠-㉠을 통해 제어 신호를 수신하여 보호 회로(26)를 동작시킨다. 도 9의 ㉠과 도 11의 ㉠을 통하여, 두 개의 공격 여부를 판단한다.
- [0092] 보호 회로(26)는 안티 퓨즈(Anti Fuse, 29) 방식으로 보호 대상에 연결된 신호 경로 차단부를 인에이블한다. 안티 퓨즈(29)는 두 개의 트랜지스터가 연결된 구조를 가질 수 있다. 보호 대상의 신호 경로에 신호 경로 차단부, 예컨대, 3 상태 버퍼들(28)이 연결된다.
- [0093] 보호 회로(26)는 알람 신호가 발생하면 멀티플렉서의 신호 제어를 통하여 안티 퓨즈 입력에 하이 VDD를 인가하여 상단의 트랜지스터를 블로잉(Blowing)시킨다.
- [0094] 멀티플렉서의 제어 신호는 초기값으로 바뀌어 일반 크기의 VDD를 인가한다. 안티 퓨즈(29)가 블로잉을 통하여 프로그래밍이 되면 3 상태 버퍼의 제어 신호에 항상 하이 값이 입력된다. 즉 하이 임피던스 상태가 유지되어 중요 정보에 접근이 가능한 모든 경로를 물리적으로 차단할 수 있다. 안티 퓨즈 내부의 하단 트랜지스터 입력은 관련 칩을 회수하여 디버깅이 필요할 경우에는 디버깅 포트 생성이 가능하다. 또는 VDD나 공격 알람 발생 신호의 반전으로 연결할 수 있다.
- [0095] 도 14는 본 발명의 실시예들에 따른 보안 회로의 동작을 예시한 흐름도이다.
- [0096] 본 발명의 실시예들에 따른 보안 회로는 크게 검출 회로와 보호 회로로 구성되며, 검출 회로는 블록 암호(Block Cipher)를 통한 암호(Encrypted Communication) 기반의 FIB 공격 검출하는 제1 진단 모드와 시간 영역 반사(Time Domain Reflection, TDR)을 통한 물리적 와이어 길이와 신호 지연 비교를 통한 FIB 공격 재검증 및 마이크로 프로빙 공격을 검출하는 제2 진단 모드를 진행한다.
- [0097] 각 진단 모드에서 요구되는 환경과 조건은 3 상태 버퍼를 이용하여 구현될 수 있고, 보안 회로는 각 진단 모드에서 3 상태 버퍼를 공유하여 하드웨어 오버헤드를 줄일 수 있다.
- [0098] 단계 S410에서 보안 회로는 설정을 초기화한다. 예컨대, 캐패시터 값을 조절하기 위한 와이어의 개수를 설정한다.
- [0099] 단계 S420에서 보안 회로는 제1 진단 모드에서 N 개의 랜덤 비트를 생성한다. 비트 생성부(240)를 통해 N 개의 랜덤 비트를 생성한다.
- [0100] 단계 S430에서 보안 회로는 N 개의 3 상태 버퍼 쌍의 상태를 일반 상태로 설정하고 나머지의 3 상태 버퍼 쌍의 상태를 하이 임피던스 상태로 설정한다. 와이어의 입력단의 3 상태 버퍼와 출력단의 3 상태 버퍼는 하나의 쌍을 형성한다.
- [0101] 단계 S440에서 보안 회로는 생성된 N 개의 랜덤 비트와 와이어를 통과한 N 개의 랜덤 비트를 비교하여 비트 오

류를 검출한다.

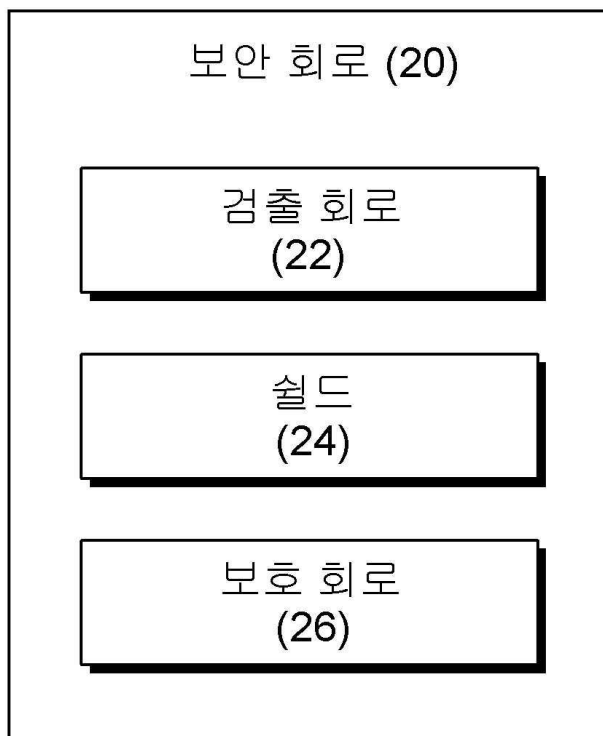
- [0102] 단계 S450에서 보안 회로는 비교한 결과에 따라 랜덤 비트가 일치하지 않으면, 보호 회로를 활성화한다(S560).
- [0103] 단계 S460에서 보안 회로는 와이어 그룹을 선택적으로 진단하고, 마지막 와이어 해당 여부를 판단한다. 마지막 와이어가 아니면 다른 와이어 그룹을 진단하고, 마지막 와이어이면 제2 진단 모드로 변경한다.
- [0104] 단계 S510에서 보안 회로는 M 개의 3 상태 버퍼 쌍의 상태를 하이 임피던스 상태로 설정한다. 즉, 입력단과 출력단을 신호 라인으로부터 격리한다.
- [0105] 단계 S520에서 보안 회로는 복수의 와이어를 연결하여 두 개의 단일 와이어 경로들을 생성한다. 단계 S530에서 보안 회로는 두 개의 단일 와이어 경로들로 스텝 펄스 신호를 인가한다. 단계 S540에서 보안 회로는 두 개의 단일 와이어 경로들을 각각 왕복한 신호들의 이동 시간을 비교한다.
- [0106] 단계 S550에서 보안 회로는 왕복한 신호들의 이동 시간의 일치 여부 판단하여, 왕복한 신호들의 이동 시간이 일치하면 제2 진단 모드를 종료한다. 왕복한 신호들의 이동 시간이 일치하지 않으면, 보호 회로를 활성화한다(S560).
- [0107] 보안 회로에 포함된 복수의 구성요소들은 상호 결합되어 적어도 하나의 모듈로 구현될 수 있다. 구성요소들은 장치 내부의 소프트웨어적인 모듈 또는 하드웨어적인 모듈을 연결하는 통신 경로에 연결되어 상호 간에 유기적으로 동작한다. 이러한 구성요소들은 하나 이상의 통신 버스 또는 신호선을 이용하여 통신한다.
- [0108] 보안 회로는 하드웨어, 펌웨어, 소프트웨어 또는 이들의 조합에 의해 로직회로 내에서 구현될 수 있고, 범용 또는 특정 목적 컴퓨터를 이용하여 구현될 수도 있다. 장치는 고정배선형(Hardwired) 기기, 필드 프로그램 가능한 게이트 어레이(Field Programmable Gate Array, FPGA), 주문형 반도체(Application Specific Integrated Circuit, ASIC) 등을 이용하여 구현될 수 있다. 또한, 장치는 하나 이상의 프로세서 및 컨트롤러를 포함한 시스템온칩(System on Chip, SoC)으로 구현될 수 있다.
- [0109] 보안 회로는 하드웨어적 요소가 마련된 컴퓨팅 디바이스에 소프트웨어, 하드웨어, 또는 이들의 조합하는 형태로 탑재될 수 있다. 컴퓨팅 디바이스는 각종 기기 또는 유무선 통신망과 통신을 수행하기 위한 통신 모듈 등의 통신장치, 프로그램을 실행하기 위한 데이터를 저장하는 메모리, 프로그램을 실행하여 연산 및 명령하기 위한 마이크로프로세서 등을 전부 또는 일부 포함한 다양한 장치를 의미할 수 있다.
- [0110] 도 14에서는 각각의 과정을 순차적으로 실행하는 것으로 기재하고 있으나 이는 예시적으로 설명한 것에 불과하고, 이 분야의 기술자라면 본 발명의 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 도 14에 기재된 순서를 변경하여 실행하거나 또는 하나 이상의 과정을 병렬적으로 실행하거나 다른 과정을 추가하는 것으로 다양하게 수정 및 변형하여 적용 가능할 것이다.
- [0111] 본 실시예들에 따른 동작은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능한 매체에 기록될 수 있다. 컴퓨터 판독 가능한 매체는 실행을 위해 프로세서에 명령어를 제공하는 데 참여한 임의의 매체를 나타낸다. 컴퓨터 판독 가능한 매체는 프로그램 명령, 데이터 파일, 데이터 구조 또는 이들의 조합을 포함할 수 있다. 예를 들면, 자기 매체, 광기록 매체, 메모리 등이 있을 수 있다. 컴퓨터 프로그램은 네트워크로 연결된 컴퓨터 시스템 상에 분산되어 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수도 있다. 본 실시예를 구현하기 위한 기능적인(Functional) 프로그램, 코드, 및 코드 세그먼트들은 본 실시예가 속하는 기술분야의 프로그래머들에 의해 용이하게 추론될 수 있을 것이다.
- [0112] 본 실시예들은 본 실시예의 기술 사상을 설명하기 위한 것이고, 이러한 실시예에 의하여 본 실시예의 기술 사상의 범위가 한정되는 것은 아니다. 본 실시예의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 실시예의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

도면

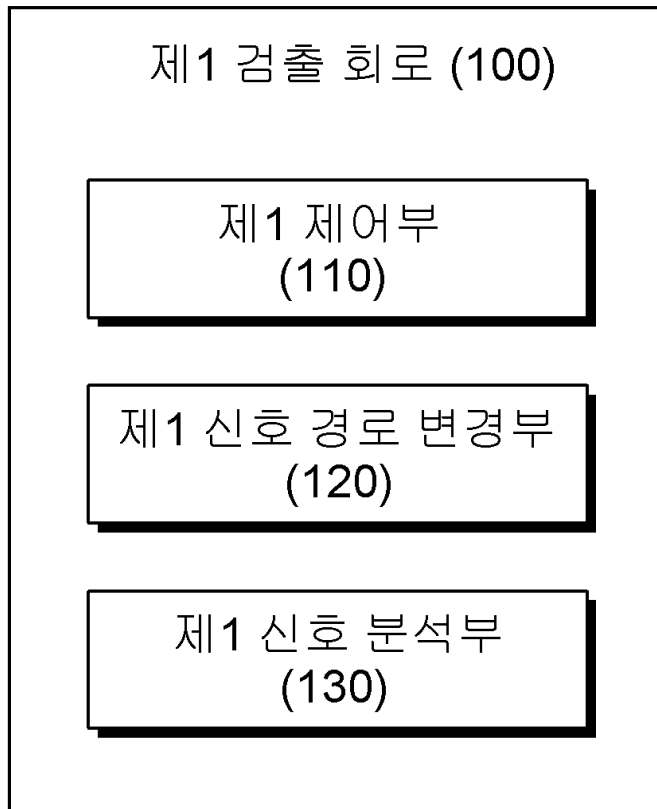
도면1



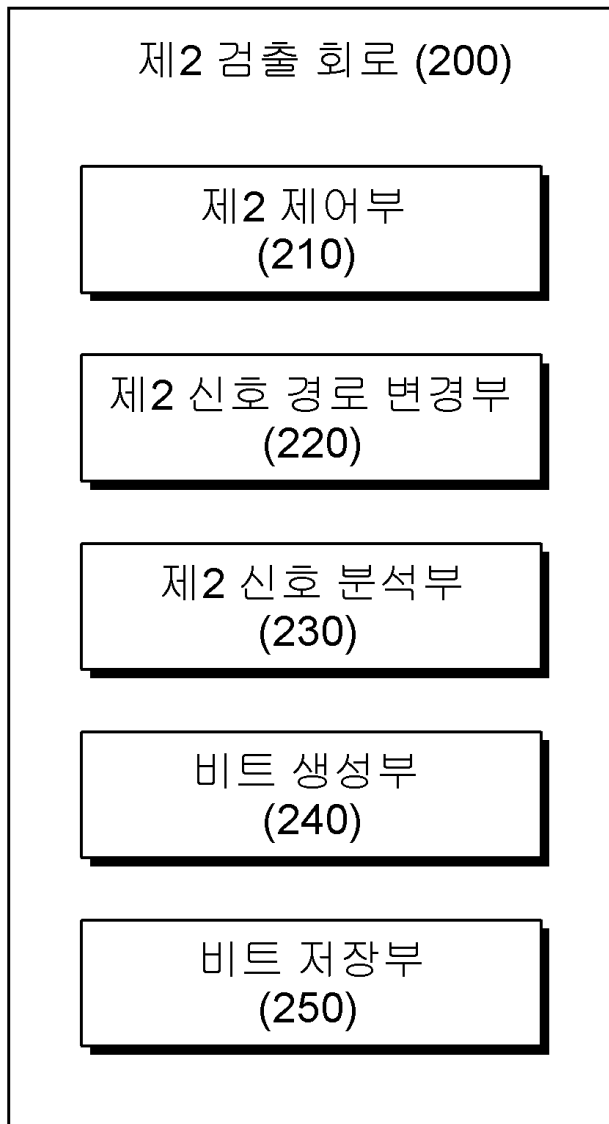
도면2



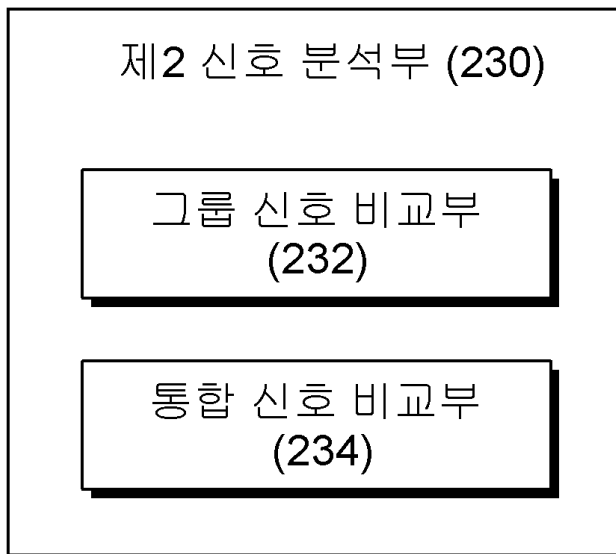
도면3



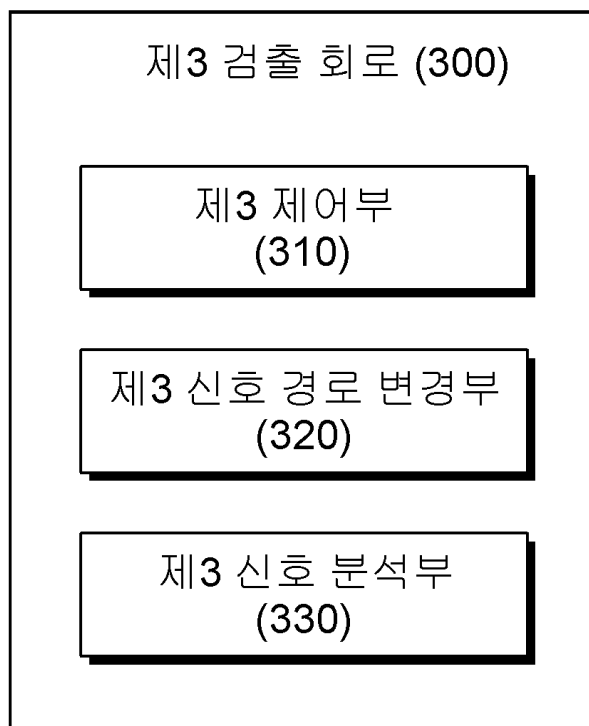
도면4



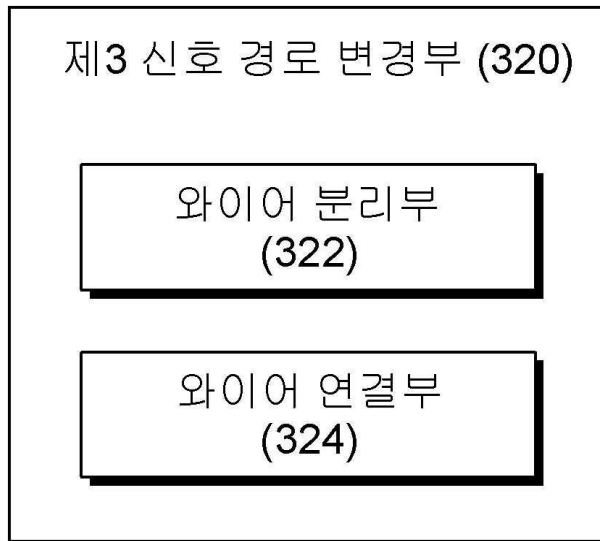
도면5



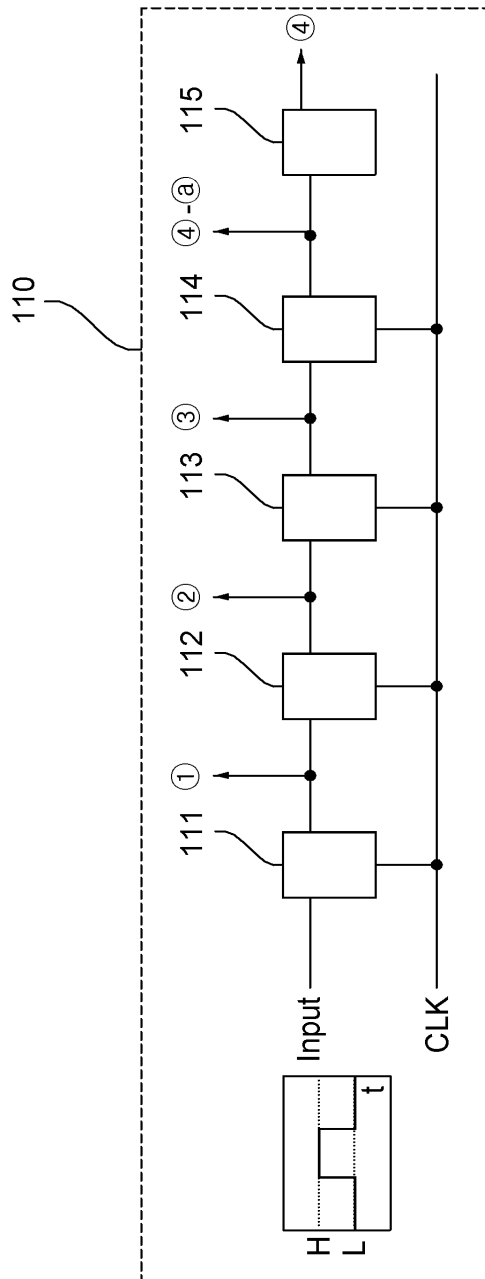
도면6



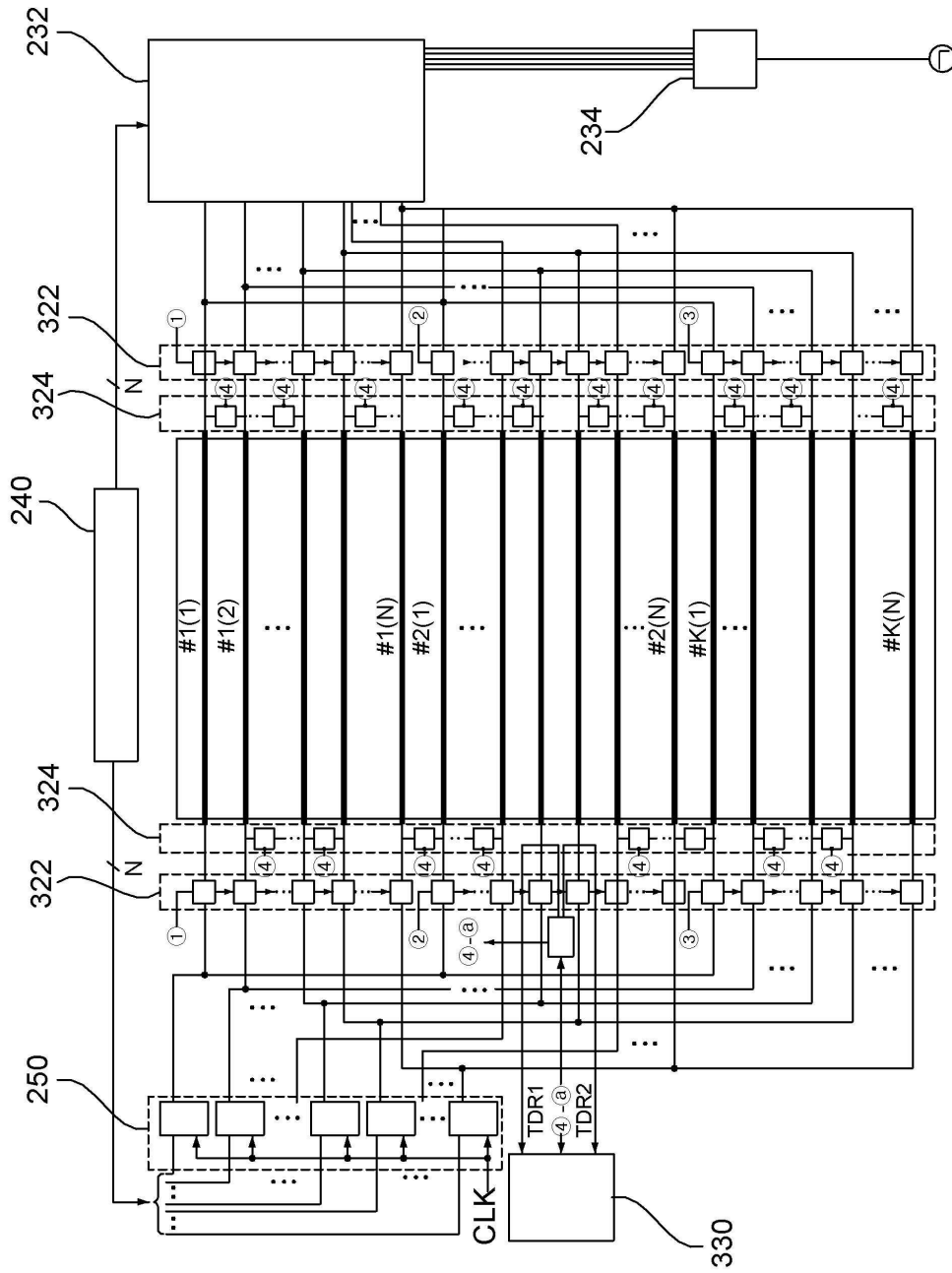
도면7



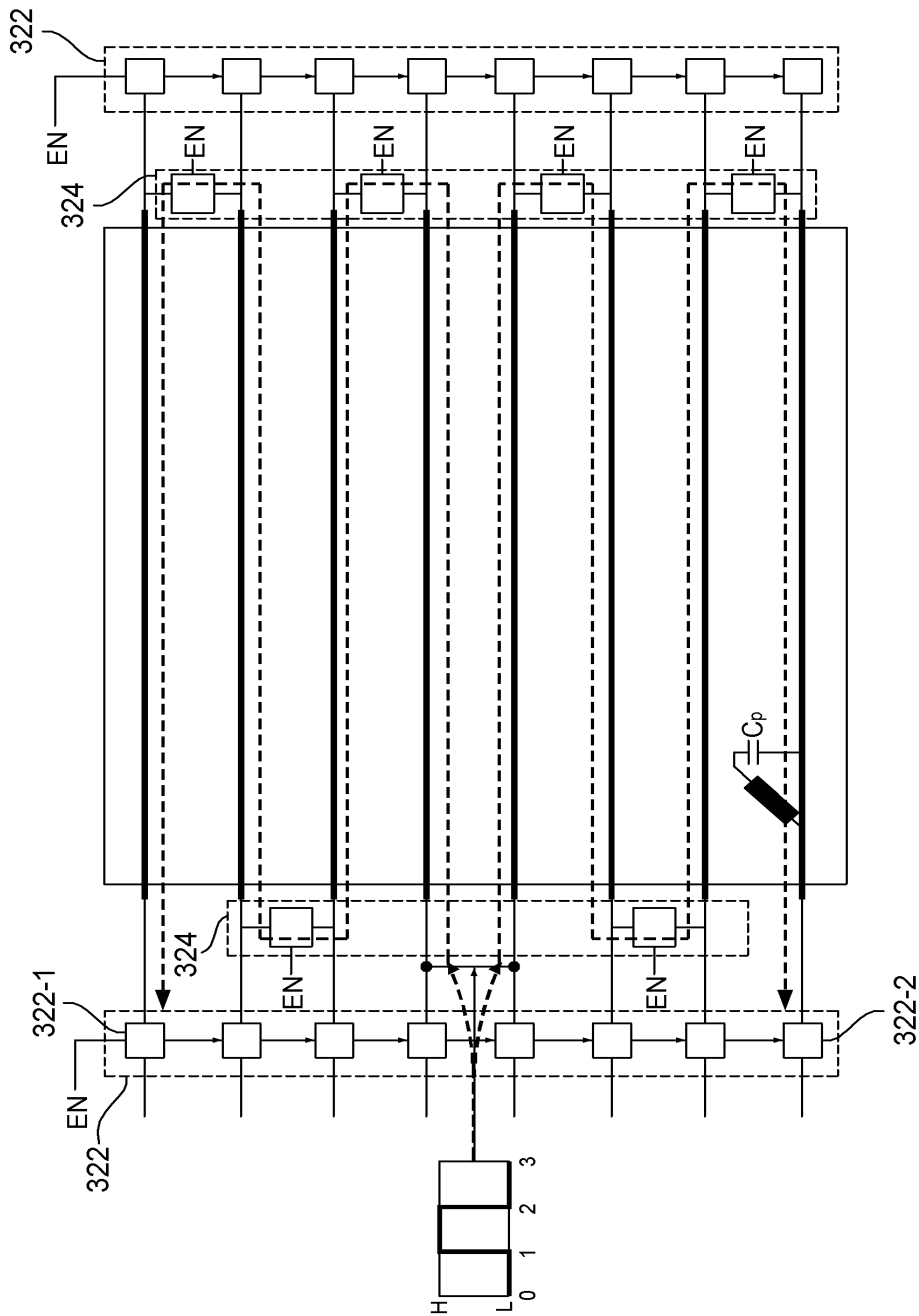
도면8



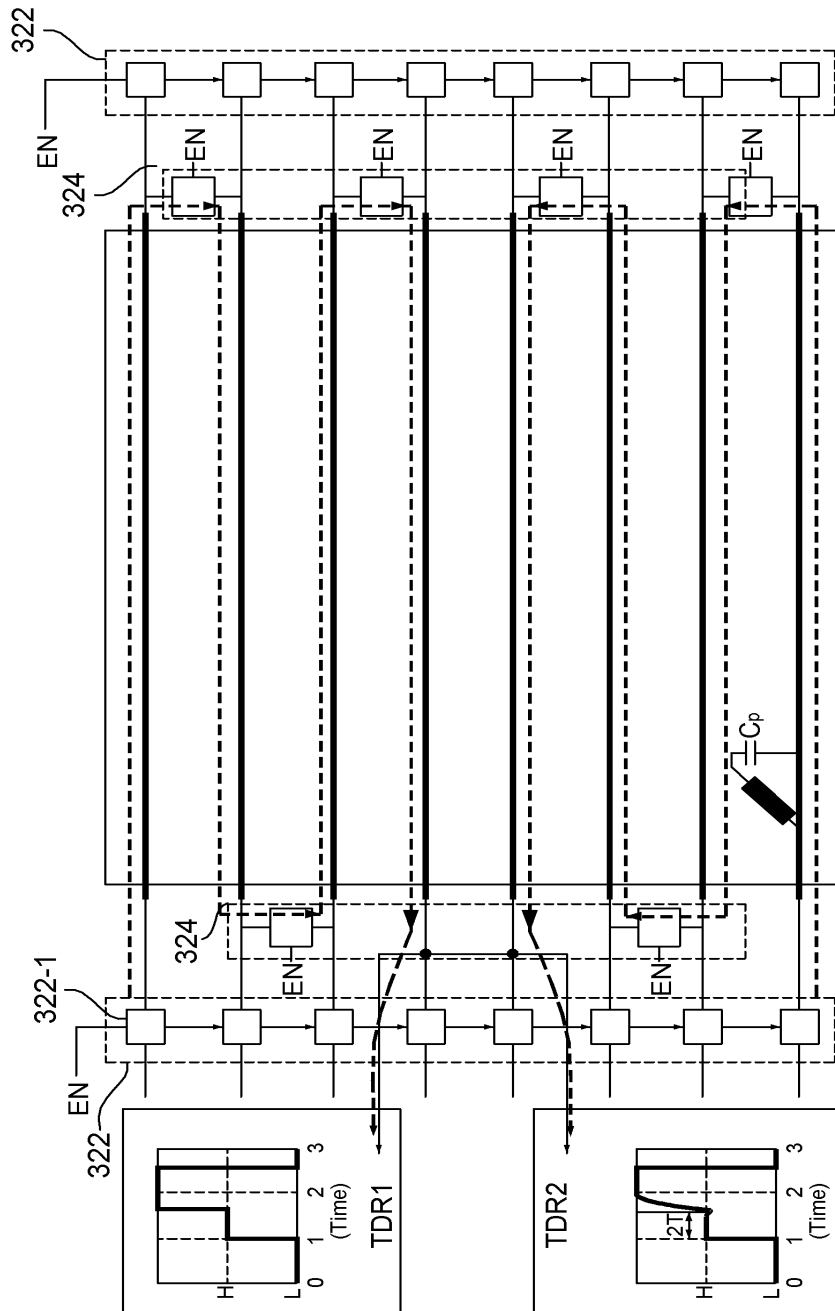
도면9



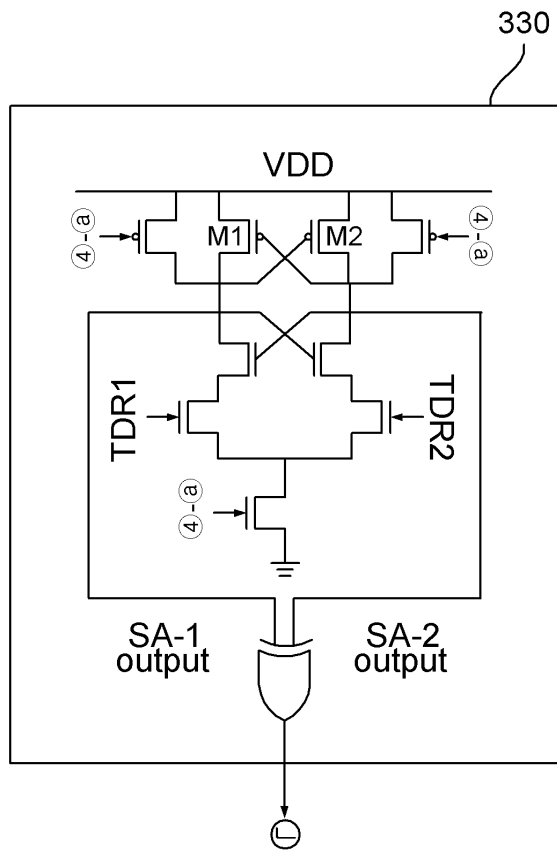
도면10a



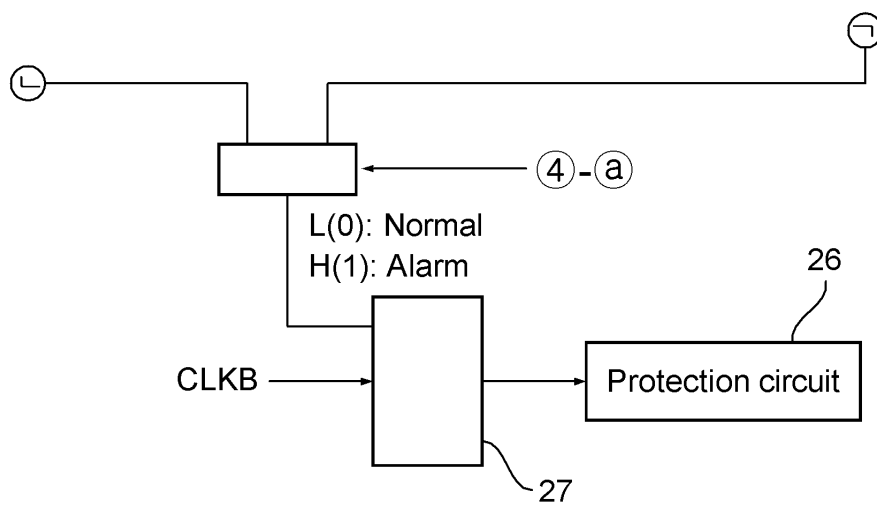
도면10b



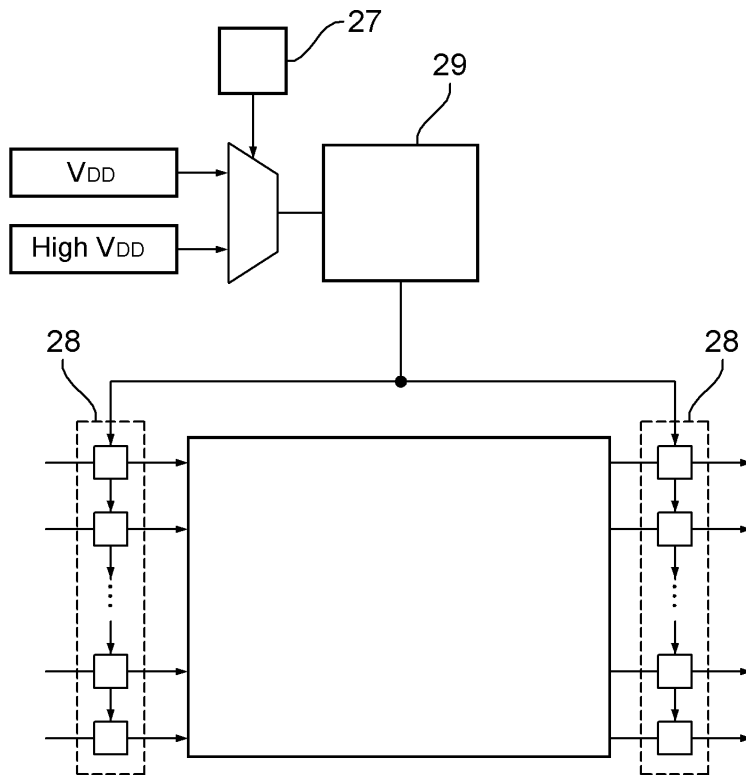
도면11



도면12



도면13



도면14

