



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0045505
(43) 공개일자 2023년04월04일

(51) 국제특허분류(Int. Cl.)
G06F 21/75 (2013.01) G06F 21/73 (2013.01)
(52) CPC특허분류
G06F 21/75 (2020.05)
G06F 21/73 (2013.01)
(21) 출원번호 10-2021-0178879
(22) 출원일자 2021년12월14일
심사청구일자 없음
(30) 우선권주장
1020210128350 2021년09월28일 대한민국(KR)

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
우형일
경기도 수원시 영통구 삼성로 129 (매탄동, 삼성 전자)
박성철
경기도 수원시 영통구 삼성로 129 (매탄동, 삼성 전자)
박재현
경기도 수원시 영통구 삼성로 129 (매탄동, 삼성 전자)
(74) 대리인
리엔특허법인

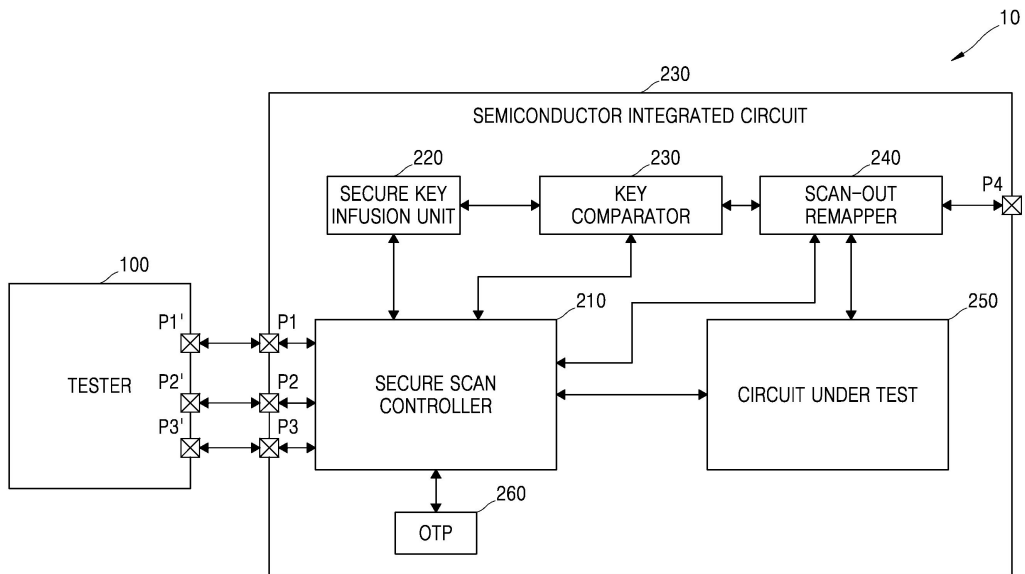
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 반도체 집적 회로, 반도체 집적 회로를 테스트하는 방법, 및 반도체 시스템

(57) 요약

반도체 집적 회로, 반도체 집적 회로를 테스트하는 방법, 및 반도체 시스템이 개시된다. 본 개시의 기술적 사상에 따른 반도체 집적 회로는, 테스트 스캔 입력 신호를 기초로 테스트 스캔 입력 신호로부터 서로 다르게 딜레이된 복수의 딜레이 입력 신호들을 생성하고, 테스트 클럭 신호에 응답하여 복수의 딜레이 입력 신호들을 캡처함으로써 입력 키 신호를 생성하는 보안 키 주입부, 기준 키를 이용해 입력 키를 검증하는 키 비교기, 스캔 출력 신호를 출력하는 칩, 검증 결과에 따라 스캔 출력 신호를 난독화하는 스캔 출력 리맵퍼, 및 보안 스캔 컨트롤러를 포함한다.

대표도



명세서

청구범위

청구항 1

외부로부터 테스트 스캔 입력 신호, 테스트 클릭 신호, 및 테스트 모드 신호를 수신하여, 보안 스캔 출력 신호를 출력하는 반도체 집적 회로에 있어서,

상기 테스트 스캔 입력 신호를 기초로 상기 테스트 스캔 입력 신호로부터 서로 다르게 딜레이된 복수의 딜레이 입력 신호들을 생성하고, 상기 테스트 클릭 신호에 응답하여 상기 복수의 딜레이 입력 신호들을 캡처함으로써 입력 키 신호를 생성하도록 구성된 보안 키 주입부;

상기 입력 키 신호에 따른 입력 키가 미리 설정된 기준 키와 일치하는지 여부를 나타내는 검증 결과 신호를 생성하도록 구성된 키 비교기;

상기 테스트 스캔 입력 신호를 기초로 스캔 출력 신호를 생성하도록 구성된 칩;

상기 검증 결과 신호에 의한 검증 결과에 따라 상기 스캔 출력 신호를 난독화하고, 난독화된 스캔 출력 신호를 상기 보안 스캔 출력 신호로 출력하도록 구성된 스캔 출력 리맵퍼; 및

상기 보안 키 주입부, 상기 키 비교기, 상기 칩 및 상기 스캔 출력 리맵퍼를 제어하도록 구성된 보안 스캔 컨트롤러를 포함하는, 반도체 집적 회로.

청구항 2

제1 항에 있어서,

상기 보안 스캔 컨트롤러는,

상기 테스트 스캔 입력 신호 및 상기 테스트 클릭 신호를 상기 보안 키 주입부에 제공하고,

상기 복수의 딜레이 입력 신호들은, 각각

제1 논리 값 또는 상기 제1 논리 값과 다른 제2 논리 값을 갖고,

상기 보안 키 주입부는,

상기 테스트 클릭 신호의 라이징 엣지에서의 상기 복수의 딜레이 입력 신호들의 논리 값들을 상기 입력 키 신호로 생성하여, 상기 입력 키 신호를 상기 키 비교기에 제공하는 것을 특징으로 하는, 반도체 집적 회로.

청구항 3

제1 항에 있어서,

상기 보안 스캔 컨트롤러는,

상기 기준 키를 나타내는 기준 키 신호 및 상기 테스트 클릭 신호를 상기 키 비교기에 제공하고,

상기 키 비교기는,

상기 입력 키가 상기 기준 키와 일치하면, 패스를 나타내는 신호를 상기 검증 결과 신호로서 상기 스캔 출력 리맵퍼에 제공하고,

상기 입력 키가 상기 기준 키와 다르면, 페일을 나타내는 신호를 상기 검증 결과 신호로서 상기 스캔 출력 리맵퍼에 제공하는 것을 특징으로 하는, 반도체 집적 회로.

청구항 4

제3 항에 있어서,

상기 보안 스캔 컨트롤러는,

상기 복수의 딜레이 입력 신호들이 캡처될 때마다, 상기 복수의 딜레이 입력 신호들을 캡처되는 횟수에 대응되는 스테이지를 카운트하고,

미리 저장된 복수의 키들 중 카운트된 스테이지에 대응되는 키를 상기 기준 키로 상기 키 비교기에 제공하는 것을 특징으로 하는, 반도체 집적 회로.

청구항 5

제3 항에 있어서,

상기 키 비교기는,

상기 입력 키가 상기 기준 키와 다르면, 비교 키 신호를 상기 스캔 출력 리맵퍼에 추가적으로 제공하고,

상기 스캔 출력 리맵퍼는,

상기 비교 키 신호를 기초로 상기 스캔 출력 신호를 난독화하기 위한 난독화 정보를 생성하고, 상기 난독화 정보에 따라 상기 스캔 출력 신호를 난독화하는 것을 특징으로 하는, 반도체 집적 회로.

청구항 6

제1 항에 있어서,

상기 스캔 출력 리맵퍼는,

상기 검증 결과 신호에 의한 검증 결과가 패스이면, 비난독화된 스캔 출력 신호를 상기 보안 스캔 출력 신호로 출력하는 것을 특징으로 하는, 반도체 집적 회로.

청구항 7

외부로부터 테스트 스캔 입력 신호, 테스트 클럭 신호, 및 테스트 모드 신호를 수신하여, 보안 스캔 출력 신호를 출력하는 반도체 집적 회로에 있어서,

상기 테스트 스캔 입력 신호를 입력받고 상기 테스트 스캔 입력 신호로부터 서로 다르게 딜레이된 $N(N \geq 1)$ 개의 정수)개의 딜레이 입력 신호들을 출력하는 N 개의 딜레이 회로들 및 상기 테스트 클럭 신호에 응답하여 상기 N 개의 딜레이 입력 신호들의 논리 값들을 래치하고, 래치된 논리 값들로 구성되는 입력 키 신호를 출력하는 N 개의 플립플롭들을 포함하는 보안 키 주입부;

상기 입력 키 신호에 의한 입력 키와 미리 설정된 기준 키의 일치 여부를 나타내는 검증 결과 신호를 출력하는 키 비교기;

상기 테스트 스캔 입력 신호를 기초로 스캔 출력 신호를 생성하는 칩;

상기 검증 결과 신호에 의한 검증 결과에 따라 상기 스캔 출력 신호를 난독화하고, 난독화된 스캔 출력 신호를 상기 보안 스캔 출력 신호로 출력하는 스캔 출력 리맵퍼; 및

상기 보안 키 주입부, 상기 키 비교기, 상기 칩 및 상기 스캔 출력 리맵퍼를 제어하도록 구성된 보안 스캔 컨트롤러를 포함하는, 반도체 집적 회로.

청구항 8

제7 항에 있어서,

상기 보안 스캔 컨트롤러는,

상기 테스트 스캔 입력 신호를 상기 N 개의 딜레이 회로들에 제공하고, 상기 테스트 클럭 신호를 상기 N 개의 플립플롭들에 제공하고,

상기 N 개의 플립플롭들은, 각각

상기 테스트 클럭 신호의 라이징 엣지에 응답하여, 상기 테스트 클럭 신호의 라이징 엣지에서의 상기 N 개의 딜레이 입력 신호들의 논리 값들을 래치하는 것을 특징으로 하는, 반도체 집적 회로.

청구항 9

제8 항에 있어서,

상기 N개의 딜레이 회로들 중 적어도 하나는, 하나 이상의 버퍼를 포함하고,

상기 N개의 딜레이 회로들 중 제i(i는 N 이하의 정수) 딜레이 회로에 포함된 버퍼의 개수는, 상기 N개의 딜레이 회로들 중 제j(j는 i와 다르고 N 이하의 정수) 딜레이 회로에 포함된 버퍼의 개수와 다른 것을 특징으로 하는, 반도체 집적 회로.

청구항 10

제9 항에 있어서,

상기 N개의 딜레이 회로들 중 어느 하나의 딜레이 회로는, 버퍼를 포함하지 않고, 상기 테스트 스캔 입력 신호를 상기 N개의 플립플롭들 중 상기 어느 하나의 딜레이 회로에 대응되는 플립플롭에 입력하는 것을 특징으로 하는, 반도체 집적 회로.

청구항 11

제7 항에 있어서,

상기 보안 스캔 컨트롤러는,

상기 N개의 딜레이 입력 신호들의 논리 값들이 래치된 헷수에 대응되는 스테이지를 카운트하여 카운트된 스테이지를 나타내는 스테이지 신호를 출력하고, 상기 스테이지가 카운트될 때마다 비교 동작을 지시하는 비교 신호를 출력하는 스테이지 카운터;

상기 스테이지 신호에 응답하여 미리 저장된 복수의 키들 중 상기 카운트된 스테이지에 따라 선택된 키를 상기 기준 키로서 상기 키 비교기에 제공하는 키 선택기; 및

상기 비교 신호 및 상기 테스트 클럭 신호의 논리곱 연산을 수행하여 그 결과를 상기 키 비교기에 제공하는 제1 논리곱 게이트를 포함하는 것을 특징으로 하는, 반도체 집적 회로.

청구항 12

제11 항에 있어서,

미리 저장된 인증 키 번호를 나타내는 키 선택 신호를 상기 키 선택기에 제공하는 원 타임 프로그래머블 메모리를 더 포함하고,

미리 저장된 복수의 키들은,

스테이지에 대응되는 스테이지 키들과 상기 인증 키 번호에 대응되는 인증 키 세트를 포함하고,

상기 키 선택기는,

상기 스테이지 키들 중 스테이지 신호에 따라 선택된 스테이지 키를 출력하는 제1 멀티플렉서;

상기 선택된 스테이지 키와 상기 인증 키 세트 중 상기 키 선택 신호에 따라 선택된 키를 상기 기준 키로서 출력하는 제2 멀티플렉서를 포함하는 것을 특징으로 하는, 반도체 집적 회로.

청구항 13

제7 항에 있어서,

상기 보안 스캔 컨트롤러는,

상기 테스트 클럭 신호를 상기 스캔 출력 리맵퍼에 제공하고,

상기 키 비교기는,

비교 키 신호를 상기 스캔 출력 리맵퍼에 추가적으로 제공하고,

상기 스캔 출력 리맵퍼는,

상기 스캔 출력 신호를 전달하고, 상기 테스트 클럭 신호 및 상기 비교 키 신호를 기초로 제1 클럭 신호 및 제2 클럭 신호를 출력하고, 제1 스캔 인에이블 신호를 출력하는 리맵 컨트롤러;

상기 제1 스캔 인에이블 신호를 반전시켜 제2 스캔 인에이블 신호를 출력하는 인버터;

상기 제1 스캔 인에이블 신호 및 상기 제1 클럭 신호에 응답하여 상기 스캔 출력 신호를 래치하고, 래치된 제1 스캔 출력 신호를 출력하는 제1 레지스터 세트;

상기 제2 스캔 인에이블 신호 및 상기 제2 클럭 신호에 응답하여 상기 스캔 출력 신호를 래치하고, 래치된 제2 스캔 출력 신호를 출력하는 제2 레지스터 세트;

상기 제1 스캔 출력 신호 및 상기 제2 스캔 출력 신호 중 상기 제2 스캔 인에이블 신호에 따라 어느 하나를 선택하는 제1 선택기; 및

상기 제1 선택기로부터 선택된 스캔 출력 신호와 상기 스캔 출력 신호 중 상기 검증 결과 신호에 따라 어느 하나를 상기 보안 스캔 출력 신호로 출력하는 제2 선택기를 포함하는 것을 특징으로 하는, 반도체 집적 회로.

청구항 14

제13 항에 있어서,

상기 제1 레지스터 세트는,

직렬로 케스케이드된 r 개의(r 은 1 이상의 정수) 제1 플립플롭들을 포함하고,

상기 제2 레지스터 세트는,

직렬로 케스케이드된 r 개의 제2 플립플롭들을 포함하는 것을 특징으로 하는, 반도체 집적 회로.

청구항 15

제13 항에 있어서,

제1 선택기는, 제1 멀티플렉서이고,

제2 선택기는, 제2 멀티플렉서인 것을 특징으로 하는, 반도체 집적 회로.

청구항 16

테스트 스캔 입력 신호를 서로 다른 딜레이 값을 갖는 복수의 딜레이 입력 신호들로 변경하는 단계;

테스트 클럭 신호에 응답하여 상기 복수의 딜레이 입력 신호들을 캡처함으로써 입력 키 신호를 생성하는 단계;

상기 입력 키 신호에 따른 입력 키가 미리 설정된 기준 키와 일치하는지 여부를 검증하는 단계; 및

검증 결과에 따라, 테스트 대상이 되는 칩으로부터 출력된 스캔 출력 신호를 난독화하는 단계를 포함하는, 반도체 집적 회로를 테스트하는 방법.

청구항 17

제16 항에 있어서,

상기 복수의 딜레이 입력 신호들은, 각각

제1 논리 값 또는 상기 제1 논리 값과 다른 제2 논리 값을 갖고,

상기 입력 키 신호를 생성하는 단계는,

상기 테스트 클럭 신호의 라이징 엣지에서의 상기 복수의 딜레이 입력 신호들의 논리 값들을 상기 입력 키 신호로 생성하는 것을 특징으로 하는, 반도체 집적 회로를 테스트하는 방법.

청구항 18

제16 항에 있어서,

상기 검증하는 단계는,

상기 입력 키가 상기 기준 키와 일치하면, 패스를 나타내는 신호를 출력하고,

상기 입력 키가 상기 기준 키와 다르면, 페일을 나타내는 신호를 출력하는 것을 특징으로 하는, 반도체 집적 회로를 테스트하는 방법.

청구항 19

제18 항에 있어서,

상기 검증 결과가 패스이면, 비난독화된 스캔 출력 신호를 보안 스캔 출력 신호로 출력하는 단계를 더 포함하는 것을 특징으로 하는, 반도체 집적 회로를 테스트하는 방법.

청구항 20

제18 항에 있어서,

상기 검증 결과가 페일이면, 난독화된 스캔 출력 신호를 보안 스캔 출력 신호로 출력하는 단계를 더 포함하는 것을 특징으로 하는, 반도체 집적 회로를 테스트하는 방법.

발명의 설명

기술 분야

[0001] 본 개시의 기술적 사상은 전자 장치에 관한 것이며, 더욱 상세하게는, 반도체 집적 회로, 반도체 집적 회로를 테스트하는 방법, 및 반도체 시스템에 관한 것이다.

배경 기술

[0002] 테스트용 설계(DFT) 기술들은 이들이 디바이스 내부 컴포넌트들에 액세스할 뿐만 아니라 이들을 관독하고 변경하는 간단하고 효과적인 수단을 허용하기 때문에, 복합 집적 회로(IC) 및 시스템 온 칩(SoC)의 테스트에 기본적인 지원이다. 이러한 액세스는 스캔 체인들을 통해 제공된다. 그러나, 바람직하지 못하게, 테스트 동안 유익한 이러한 액세스는 제품이 판매/배치된 이후에 보안에 다수의 문제들을 초래할 수 있다. 즉, 이러한 동일한 액세스는 제품을 변경하고, 제품을 조작하고, 제품을 분해하여 모방하거나 다른 악의적인 활동들을 수행하기 위해 악의적인 이유들로 사용될 수 있다.

[0003] 테스트 이후에 시스템의 스캔 체인의 활용을 방지하는 통상의 솔루션은 외부로부터 테스트 스캔 입력 신호로 들어오는 입력 키가 미리 설정된 인증 키에 해당되는지 확인하는 것이다. 일반적으로 외부로부터 테스트 스캔 입력 신호를 클럭 신호에 응답하여 캡처하기 위해, 직렬 연결된 플립플롭들이 도입되고 있다. 그런데, 인증 키 입력을 직렬 연결된 플립플롭들을 이용하여 받는 경우, 미리 설정된 인증 키를 복잡하게 하는 등 보안성을 높이기 위해서는 플립플롭이 추가적으로 직렬 연결되어야 한다. 이러한 방법은 칩의 사이즈를 증가시킬뿐만 아니라, 보안성을 크게 높이는 데 기여하지 못한다는 문제점이 있다.

발명의 내용

해결하려는 과제

[0004] 본 개시의 기술적 사상은, 플립플롭 등의 엘리먼트를 추가하지 않고도 보안성을 더욱 강화하는 반도체 집적 회로, 반도체 집적 회로를 테스트하는 방법, 및 반도체 시스템을 제공한다.

과제의 해결 수단

[0005] 본 개시의 기술적 사상에 따른 반도체 집적 회로는, 테스트 스캔 입력 신호를 기초로 테스트 스캔 입력 신호로부터 서로 다르게 딜레이된 복수의 딜레이 입력 신호들을 생성하고, 테스트 클럭 신호에 응답하여 복수의 딜레이 입력 신호들을 캡처함으로써 입력 키 신호를 생성하도록 구성된 보안 키 주입부, 입력 키 신호에 따른 입력 키가 미리 설정된 기준 키와 일치하는지 여부를 나타내는 검증 결과 신호를 생성하도록 구성된 키 비교기, 테스트 스캔 입력 신호를 기초로 스캔 출력 신호를 생성하도록 구성된 칩, 검증 결과 신호에 의한 검증 결과에 따라 스캔 출력 신호를 난독화하고, 난독화된 스캔 출력 신호를 보안 스캔 출력 신호로 출력하도록 구성된 스캔 출력 리맵퍼, 및 보안 키 주입부, 키 비교기, 칩 및 스캔 출력 리맵퍼를 제어하도록 구성된 보안 스캔 컨트롤러를 포

함한다.

[0006] 또한, 본 개시의 기술적 사상에 따른 반도체 집적 회로는, 테스트 스캔 입력 신호를 입력받고 테스트 스캔 입력 신호로부터 서로 다르게 딜레이된 $N(N$ 은 1 이상의 정수)개의 딜레이 입력 신호들을 출력하는 N 개의 딜레이 회로 들 및 테스트 클럭 신호에 응답하여 N 개의 딜레이 입력 신호들의 논리 값들을 래치하고, 래치된 논리 값들로 구성되는 입력 키 신호를 출력하는 N 개의 플립플롭들을 포함하는 보안 키 주입부, 입력 키 신호에 의한 입력 키와 미리 설정된 기준 키의 일치 여부를 나타내는 검증 결과 신호를 출력하는 키 비교기, 테스트 스캔 입력 신호를 기초로 스캔 출력 신호를 생성하는 칩, 검증 결과 신호에 의한 검증 결과에 따라 스캔 출력 신호를 난독화하고, 난독화된 스캔 출력 신호를 보안 스캔 출력 신호로 출력하는 스캔 출력 리맵퍼, 및 보안 키 주입부, 키 비교기, 칩 및 스캔 출력 리맵퍼를 제어하도록 구성된 보안 스캔 컨트롤러를 포함한다.

[0007] 또한, 본 개시의 기술적 사상에 따른 반도체 집적 회로를 테스트하는 방법 은, 테스트 스캔 입력 신호를 서로 다른 딜레이 값을 갖는 복수의 딜레이 입력 신호들로 변경하는 단계, 테스트 클럭 신호에 응답하여 복수의 딜레이 입력 신호들을 캡처함으로써 입력 키 신호를 생성하는 단계, 입력 키 신호에 따른 입력 키가 미리 설정된 기준 키와 일치하는지 여부를 검증하는 단계, 검증 결과에 따라, 테스트 대상이 되는 칩으로부터 출력된 스캔 출력 신호를 난독화하는 단계를 포함한다.

[0008] 또한, 본 개시의 기술적 사상에 따른 반도체 시스템은, 테스트 스캔 입력 신호, 테스트 클럭 신호, 및 테스트 모드 신호를 출력하는 테스트 장치, 및 테스트 스캔 입력 신호, 테스트 클럭 신호, 및 테스트 모드 신호를 수신 하여, 보안 스캔 출력 신호를 출력하는 반도체 집적 회로를 포함하고, 반도체 집적 회로는, 테스트 스캔 입력 신호를 입력 받고 테스트 스캔 입력 신호로부터 서로 다르게 딜레이된 $N(N$ 은 1 이상의 정수)개의 딜레이 입력 신호들을 출력하는 N 개의 딜레이 회로들, 및 테스트 클럭 신호에 응답하여 N 개의 딜레이 입력 신호들의 논리 값 들을 래치하는 N 개의 플립플롭들을 포함한다.

발명의 효과

[0009] 본 개시의 기술적 사상에 의하면, 직렬 연결된 플립플롭들을 이용하여 인증 키를 입력 받는 방식을 사용하지 않아서 악의적 사용자로부터 시스템을 안전하게 보호하면서도, 플립플롭 등의 엘리먼트를 추가하지 않고도 보안성을 더욱 강화하는 효과가 있다.

도면의 간단한 설명

- [0010] 도 1은 본 개시의 일 실시예에 따른 반도체 시스템을 설명하기 위한 도면이다.
- 도 2는 본 개시의 일 실시예에 따른 반도체 집적 회로를 설명하기 위한 도면이다.
- 도 3은 본 개시의 일 실시예에 따른 보안 키 주입부를 설명하기 위한 도면이다.
- 도 4는 본 개시의 일 실시예에 따른 보안 키 주입부를 구현하기 위한 일 예시를 나타낸 도면이다.
- 도 5는 본 개시의 일 실시예에 따른 입력 키 신호로 생성하는 방법을 설명하기 위한 타이밍도이다.
- 도 6은 본 개시의 일 실시예에 따라 키 비교기를 제어하기 위한 보안 스캔 컨트롤러의 구현 예를 나타내는 도면이다.
- 도 7은 도 6에 도시된 키 선택기의 구현 예를 나타내는 도면이다.
- 도 8은 본 개시의 일 실시예에 따른 스캔 출력 리맵퍼를 설명하기 위한 도면이다.
- 도 9는 본 개시의 일 실시예에 따른 스캔 출력 리맵퍼를 구현하기 위한 일 예시를 나타낸 도면이다.
- 도 10은 본 개시의 일 실시예에 따른 리맵 컨트롤러의 구현 예를 나타내는 도면이다.
- 도 11은 테스트 모드에서 출력되는 보안 스캔 출력 신호를 설명하기 위한 도면이다.
- 도 12는 스캔 덤프 모드에서 출력되는 보안 스캔 출력 신호를 설명하기 위한 도면이다.
- 도 13은 본 개시의 다른 실시예에 따른 반도체 집적 회로를 설명하기 위한 도면이다.
- 도 14는 본 개시의 또 다른 실시예에 따른 반도체 집적 회로를 설명하기 위한 도면이다.
- 도 15는 본 개시의 일 실시예에 따른 반도체 집적 회로를 테스트하는 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0011] 이하, 첨부한 도면을 참조하여 본 개시의 실시예에 대해 상세히 설명한다.
- [0012] 도 1은 본 개시의 일 실시예에 따른 반도체 시스템을 설명하기 위한 도면이다.
- [0013] 도 1을 참조하면, 반도체 시스템(10)은 테스터(100) 및 반도체 집적 회로(200)를 포함할 수 있다.
- [0014] 테스터(100)는 반도체 집적 회로(200)를 테스트하는데 적합한 임의의 장치일 수 있다. 테스터(100)는 복수의 핀들을 구비할 수 있다. 도 1을 참조하여 예를 들면, 테스터(100)는 제1 핀(P1'), 제2 핀(P2'), 및 제3 핀(P3')을 구비할 수 있다. 하지만, 이에 한정되는 것은 아니다. 테스터(100)는 각 핀을 통해 특정 신호를 반도체 집적 회로(200) 전송할 수 있다. 예를 들면, 테스터(100)는 제1 핀(P1')을 통해 테스트 스캔 입력 신호를 출력하고, 제2 핀(P2')을 통해 테스트 클럭 신호를 출력하며, 제3 핀(P3')을 통해 테스트 모드 신호를 출력할 수 있다. 테스트 스캔 입력 신호는 테스트를 수행할 사용자가 테스트를 수행하기 위해 임의로 입력하는 신호일 수 있다. 또는 테스트 스캔 입력 신호는, 테스트를 수행할 사용자가 반도체 집적 회로(200)에 대한 테스트를 수행할 자격이 있는지 여부를 인증하기 위한 키를 포함하는 신호일 수 있다. 테스트 클럭 신호는 테스트 모드에서 사용되는 클럭 신호일 수 있다. 테스트 클럭 신호는 특정 주기로 일정하게 토글링(Toggling)될 수 있다. 이때, 특정 주기는 미리 설정된 사이클(cycle)들을 포함하는 경우, 테스트 클럭 신호는 특정 주기 내에서 사이클마다 반복적으로 토글링(Toggling)될 수 있다. 또는 테스트 클럭 신호는 한 주기 내에 포함된 복수의 사이클들 중 적어도 하나의 특정 사이클에서만 토글링될 수 있다. 예를 들면, 테스트 클럭 신호의 한 주기는 100개의 사이클을 포함하는 경우, 테스트 클럭 신호는 100개의 사이클 중 70번째 사이클, 81번째 내지 83번째 사이클, 및 99번째 사이클에서 토글링될 수 있다. 하지만, 이에 한정되는 것은 아니다. 테스트 모드 신호는 테스트 모드를 수행하기 위한 신호일 수 있다. 테스트 모드 신호의 논리 값이 제1 값(또는 제1 비트값, 로직 하이 레벨(Logic high level))이면, 이는 테스트 모드를 수행할 것을 지시하는 것일 수 있다. 반대로, 테스트 모드 신호의 논리 값이 제2 값(또는 제2 비트값, 로직 로우 레벨(Logic low level))이면, 이는 노멀 모드를 수행할 것을 지시하는 것일 수 있다. 하지만, 이에 한정되는 것은 아니다. 본 명세서에서의 테스터(100)는 테스트 장치, 테스트기 등으로 지칭될 수 있다.
- [0015] 일 실시예에서, 테스터(100)는 컴퓨터 시스템으로서, 예를 들어, 퍼스널 컴퓨터 등으로 구비되며 테스트를 위한 디버깅 프로그램(Debugging program)을 구비할 수 있다.
- [0016] 반도체 집적 회로(200)는 테스터(100)로부터 출력된 신호들을 수신하기 위해 복수의 핀들을 구비할 수 있다. 예를 들면, 반도체 집적 회로(200)는 제1 핀(P1), 제2 핀(P2), 및 제3 핀(P3)을 구비하며, 각 핀을 통해 테스트 스캔 입력 신호, 테스트 클럭 신호, 및 테스트 모드 신호를 수신할 수 있다. 하지만, 이에 한정되는 것은 아니다. 반도체 집적 회로(200)는 테스트 수행 결과 생성된 스캔 출력 신호를 출력하기 위한 핀을 더 구비할 수 있다. 예를 들면, 반도체 집적 회로(200)는 제4 핀(P4)을 구비할 수 있다.
- [0017] 일 실시예에서, 반도체 집적 회로(200)는 보안 스캔 컨트롤러(210), 보안 키 주입부(220), 키 비교기(230), 스캔 출력 리맵퍼(240), 서킷 언더 테스트(250), 및 원 타임 프로그래머블 메모리(One time programmable memory, 이하 OTP라고 함)(260)를 포함할 수 있다.
- [0018] 도 2는 본 개시의 일 실시예에 따른 반도체 집적 회로를 설명하기 위한 도면이다.
- [0019] 도 2를 참조하면, 반도체 집적 회로(200)는 테스트 스캔 입력 신호(TSI), 테스트 클럭 신호(TCK), 및 테스트 모드 신호(TMS)를 수신하여, 보안 스캔 출력 신호(SSO)를 출력할 수 있다. 이를 위하여 반도체 집적 회로(200)는 보안 스캔 컨트롤러(210), 보안 키 주입부(220), 키 비교기(230), 스캔 출력 리맵퍼(240), 서킷 언더 테스트(250), 및 OTP(260)를 포함할 수 있다.
- [0020] 보안 스캔 컨트롤러(210)는 보안 키 주입부(220), 키 비교기(230), 스캔 출력 리맵퍼(240), 및 서킷 언더 테스트(250) 각각을 제어할 수 있다. 보안 스캔 컨트롤러(210)는 제1 내지 제3 핀들(P1, P2, P3)를 통해 테스트 스캔 입력 신호(TSI), 테스트 클럭 신호(TCK), 및 테스트 모드 신호(TMS)를 수신할 수 있다. 일 실시예에서, 테스트 모드 신호가 제1 값을 갖는 경우, 보안 스캔 컨트롤러(210)는, 테스트 스캔 입력 신호(TSI)를 테스트 키 신호(TSI_KEY)로서 보안 키 주입부(220)에 전달하고, 보안 키 주입부(220)에 대한 테스트 클럭 신호(TCK_SKI)를 보안 키 주입부(220)에 전달할 수 있다. 일 실시예에서, 보안 스캔 컨트롤러(210)는, 키 비교기(230)에 대한 테스트 클럭 신호(TCK_KC)를 키 비교기(230)에 전달하고 미리 저장된 기준 키 신호(KEY_REF)를 키 비교기(230)에 전달할 수 있다. 일 실시예에서, 보안 스캔 컨트롤러(210)는, 스캔 출력 리맵퍼(240)에 대한 테스트 클럭 신호

(TCK_SR)를 스캔 출력 리맵퍼(240)에 전달할 수 있다. 일 실시예에서, 보안 스캔 컨트롤러(210)는, 스캔 컨트롤 신호(SC), 테스트 데이터(TSI_TD), 및 서킷 언더 테스트(250)에 대한 테스트 클럭 신호(TCK_CHIP)를 서킷 언더 테스트(250)에 전달할 수 있다.

- [0021] 다른 실시예에서, 보안 스캔 컨트롤러(210)는 OTP(260)로부터 키 선택 신호(KEY_SEL)를 수신하여 미리 저장된 복수의 키들 중 키 선택 신호(KEY_SEL)에 의해 선택된 어느 하나의 키를 기준 키 신호(KEY_REF)로서 출력할 수 있다.
- [0022] 다른 실시예에서, 보안 스캔 컨트롤러(210)는, 서킷 언더 테스트(250)로부터 스캔 덤프 인에이블 신호(SDE) 및 컨피규레이션 신호(CFG)를 수신하고, 노멀 모드에서 스캔 덤프 모드로 전환하기 위해, 덤프 모드 신호(DUMP_MODE)를 스캔 출력 리맵퍼(240)에 전달할 수 있다. 스캔 덤프 인에이블 신호(SDE)는 스캔 덤프 모드를 진입할 것을 지시하는 신호일 수 있다. 컨피규레이션 신호(CFG)는 스캔 덤프 모드 시 서킷 언더 테스트(250)의 내부 정보를 나타내는 신호일 수 있다.
- [0023] 또 다른 실시예에서, 보안 스캔 컨트롤러(210)는, 권한이 있는 사용자가 보안 스캔 출력 신호(SSO)를 해독하기 위한 맵 선택 신호(MAP_SEL)를 스캔 출력 리맵퍼(240)에 전달할 수 있다.
- [0024] 보안 키 주입부(220)는 테스트 스캔 입력 신호(TSI)를 기초로 복수의 딜레이 입력 신호들을 생성할 수 있다. 복수의 딜레이 입력 신호들은 테스트 스캔 입력 신호(TSI)로부터 서로 다르게 딜레이된 신호들일 수 있다. 보안 키 주입부(220)는 테스트 클럭 신호(TCK)에 응답하여 복수의 딜레이 입력 신호들을 캡처함으로써 입력 키 신호(KEY_CAP)를 생성할 수 있다. 보안 키 주입부(220)는 입력 키 신호(KEY_CAP)를 키 비교기(230)에 제공할 수 있다.
- [0025] 키 비교기(230)는 입력 키 신호(KEY_CAP)에 따른 입력 키가 기준 키 신호(KEY_REF)에 따른 기준 키와 일치하는지 여부를 검증할 수 있다. 그리고, 키 비교기(230)는 이러한 검증 결과를 나타내는 검증 결과 신호(P/F)를 생성할 수 있다. 구체적으로, 키 비교기(230)는, 키 비교기(230)에 대한 테스트 클럭 신호(TCK_KC)에 응답하여 입력 키 신호(KEY_CAP)의 값과 기준 키 신호(KEY_REF)의 값을 비교하고 패스(Pass) 또는 페일(Fail)을 나타내는 검증 결과 신호(P/F)를 출력할 수 있다.
- [0026] 일 실시예에서, 키 비교기(230)는 비교 키 신호(KEY_COMP)를 스캔 출력 리맵퍼(240)에 추가적으로 제공할 수 있다. 비교 키 신호(KEY_COMP)는, 예를 들어 테스트 클럭 신호(TCK_KC)가 마지막으로 토글링된 사이클에서 기준 키와 비교된 입력 키를 나타내는 신호일 수 있다.
- [0027] 스캔 출력 리맵퍼(240)는 검증 결과 신호(P/F)에 의한 검증 결과에 따라 스캔 출력 신호(PSO)를 난독화하고(obfuscate), 난독화된(obfuscated) 스캔 출력 신호를 보안 스캔 출력 신호(SSO)로 출력할 수 있다.
- [0028] 일 실시예에서, 검증 결과가 패스이면, 스캔 출력 리맵퍼(240)는 스캔 출력 신호(PSO)를 제4 핀(P4)을 통해 그대로 출력할 수 있다. 즉, 검증 결과가 패스이면, 스캔 출력 리맵퍼(240)는 스캔 출력 신호(PSO)를 비난독화하고, 비난독화된 스캔 출력 신호(PSO)를 보안 스캔 출력 신호(SSO)로 제4 핀(P4)을 통해 그대로 출력할 수 있다.
- [0029] 일 실시예에서, 검증 결과가 페일이면, 스캔 출력 리맵퍼(240)는 비교 키 신호(KEY_COMP)를 기초로 스캔 출력 신호(PSO)를 난독화하기 위한 난독화 정보를 생성할 수 있다. 그리고, 스캔 출력 리맵퍼(240)는 난독화 정보에 따라 스캔 출력 신호(PSO)를 난독화할 수 있다.
- [0030] 다른 실시예에서, 스캔 출력 리맵퍼(240)는 덤프 모드 신호(DUMP_MODE) 및 맵 선택 신호(MAP_SEL)를 기초로 스캔 출력 신호(PSO)를 난독화하기 위한 난독화 정보를 생성할 수 있다.
- [0031] 서킷 언더 테스트(250)는 테스트, 디버깅(Debugging) 대상이 되는 회로(circuit) 또는 칩(Chip)일 수 있다. 서킷 언더 테스트(250)는 하나의 스캔-체인(scan-chain)으로 접속된 복수의 동기 회로들을 포함할 수 있다. 서킷 언더 테스트(250)는 보안 스캔 컨트롤러(210)로부터 수신된 스캔 컨트롤 신호(SC), 테스트 데이터(TSI_TD), 및 서킷 언더 테스트(250)를 기초로 스캔 동작을 수행하고, 스캔 출력 신호(PSO)를 생성하며, 스캔 출력 신호(PSO)를 스캔 출력 리맵퍼(240)에 전송할 수 있다. 본 명세서의 서킷 언더 테스트(250)는 칩, 회로, 코어 로직(Core logic), 온-칩 로직(On-chip logic) 등으로 지칭될 수 있다.
- [0032] OTP(260)는 인증 키 데이터를 저장할 수 있다. 인증 키 데이터는 제조업자 등이 생성한 인증 키 번호를 나타내는 데이터일 수 있다. OTP(260)는 인증 키 데이터를 키 선택 신호(KEY_SEL)로서 보안 스캔 컨트롤러(210)에 출력할 수 있다. 보안 스캔 컨트롤러(210)는 미리 저장된 복수의 키들 중 키 선택 신호(KEY_SEL)에 의해 선택된 어느 하나의 키를 기준 키 신호(KEY_REF)로서 출력할 수 있다. 본 명세서의 OTP(260)는 퓨즈, 안티-퓨즈, 또는

e-퓨즈로 구현될 수 있다.

- [0033] 도 3은 본 개시의 일 실시예에 따른 보안 키 주입부를 설명하기 위한 도면이다.
- [0034] 도 3을 참조하면, 보안 키 주입부(220)는 N개의 딜레이 회로들 및 N개의 플립플롭들을 포함할 수 있다. N은 1 이상의 정수일 수 있다. 도 3을 참조하여 예를 들면, 보안 키 주입부(220)는 제1 내지 제6 딜레이 회로들(221_1, 221_2, 221_3, 221_4, 221_5, 221_6) 및 제1 내지 제6 플립플롭들(222_1, 222_2, 222_3, 222_4, 222_5, 222_6)을 포함할 수 있다. 하지만, 이에 한정되는 것은 아니다. 이하에서는 설명의 편의상 보안 키 주입부(220)에 포함된 딜레이 회로 및 플립플롭의 개수는 6개인 것으로 가정한다.
- [0035] 보안 스캔 컨트롤러(210)는 테스트 스캔 입력 신호(TSI)를 테스트 키 신호(TSI_KEY)로서 제1 내지 제6 딜레이 회로들(221_1, 221_2, 221_3, 221_4, 221_5, 221_6)에 전달할 수 있다. 이 경우, 제1 내지 제6 딜레이 회로들(221_1, 221_2, 221_3, 221_4, 221_5, 221_6)은 테스트 키 신호(TSI_KEY)를 딜레이하여 제1 내지 제6 딜레이 입력 신호들(D0, D1, D2, D3, D4, D5)을 출력할 수 있다. 제1 내지 제6 딜레이 입력 신호들(D0, D1, D2, D3, D4, D5) 각각이 갖는 딜레이 값들은 서로 다를 수 있다. 제1 내지 제6 딜레이 입력 신호들(D0, D1, D2, D3, D4, D5) 각각은 제1 내지 제6 플립플롭들(222_1, 222_2, 222_3, 222_4, 222_5, 222_6)에 전달될 수 있다.
- [0036] 보안 스캔 컨트롤러(210)는 보안 키 주입부(220)에 대한 테스트 클럭 신호(TCK_SKI)를 제1 내지 제6 플립플롭들(222_1, 222_2, 222_3, 222_4, 222_5, 222_6)에 전달할 수 있다. 이 경우, 제1 내지 제6 플립플롭들(222_1, 222_2, 222_3, 222_4, 222_5, 222_6)은, 테스트 클럭 신호(TCK_SKI)에 응답하여, 제1 내지 제6 딜레이 입력 신호들(D0, D1, D2, D3, D4, D5)의 논리 값들을 래치하고, 래치된 값들을 키 비교기(230)에 전달할 수 있다. 도 3을 참조하여 예를 들면, 테스트 클럭 신호(TCK_SKI)에 응답하여, 제1 플립플롭(222_1)은 제1 딜레이 입력 신호(D0)의 논리값을 래치하고, 제2 플립플롭(222_2)은 제2 딜레이 입력 신호(D1)의 논리 값을 래치하고, 제3 플립플롭(222_3)은 제3 딜레이 입력 신호(D2)의 논리 값을 래치할 수 있다. 마찬가지로, 제4 내지 제6 플립플롭들(222_4, 222_5, 222_6)도 제4 내지 제6 딜레이 입력 신호들(D3, D4, D5)의 논리 값을 각각 래치할 수 있다.
- [0037] 도 4는 본 개시의 일 실시예에 따른 보안 키 주입부를 구현하기 위한 일 예시를 나타낸 도면이다.
- [0038] 도 4를 참조하면, 제1 내지 제6 딜레이 회로들(221_1, 221_2, 221_3, 221_4, 221_5, 221_6) 중 적어도 하나는, 하나 이상의 버퍼를 포함할 수 있다. 이 경우, 6개의 제1 내지 제6 딜레이 회로들(221_1, 221_2, 221_3, 221_4, 221_5, 221_6) 중 제i(i는 N 이하의 정수, 예를 들면 1 내지 6) 딜레이 회로에 포함된 버퍼의 개수는, 6개의 제1 내지 제6 딜레이 회로들(221_1, 221_2, 221_3, 221_4, 221_5, 221_6) 중 제j(j는 i와 다르고 N 이하의 정수) 딜레이 회로에 포함된 버퍼의 개수와 다를 수 있다.
- [0039] 도 4를 참조하여 예를 들면, 제2 딜레이 회로(221_2)는 4개의 버퍼(223)를 포함하고, 제3 딜레이 회로(221_3)는 2개의 버퍼(223)를 포함하고, 제4 딜레이 회로(221_4)는 1개의 버퍼(223)를 포함하고, 제5 딜레이 회로(221_5)는 3개의 버퍼(223)를 포함하며, 제6 딜레이 회로(221_6)는 5개의 버퍼(223)를 포함할 수 있다. 하지만, 이에 한정되는 것은 아니며, 각 딜레이 회로에 포함된 버퍼의 개수는 서로 다르기만하면 어떤 조합이든지 본 실시예에 적용될 수 있다. 버퍼(223)의 개수가 많을수록, 딜레이 값은 더 커질 수 있다. 즉, 버퍼(223)의 개수가 많을수록, 테스트 키 신호(TSI_KEY)는 더 많이 딜레이될 수 있다.
- [0040] 일 실시예에서, 6개의 제1 내지 제6 딜레이 회로들(221_1, 221_2, 221_3, 221_4, 221_5, 221_6) 중 어느 하나의 딜레이 회로는, 버퍼를 포함하지 않을 수 있다. 이 경우, 제1 내지 제6 딜레이 회로들(221_1, 221_2, 221_3, 221_4, 221_5, 221_6) 중 어느 하나의 딜레이 회로는 테스트 키 신호(TSI_KEY)를 대응되는 플립플롭에 전달할 수 있다. 도 4를 참조하여 예를 들면, 제1 딜레이 회로(221_1)는 버퍼를 포함하지 않을 수 있고, 제1 딜레이 회로(221_1)는 제1 딜레이 회로(221_1)는 테스트 키 신호(TSI_KEY)를 제1 플립플롭(222_1)에 입력할 수 있다. 하지만, 이에 한정되는 것은 아니다.
- [0041] 도 5는 본 개시의 일 실시예에 따른 입력 키 신호로 생성하는 방법을 설명하기 위한 타이밍도이다.
- [0042] 도 4 및 도 5를 참조하면, 테스트 클럭 신호(TCK_SKI) 및 테스트 키 신호(TSI_KEY)가 보안 키 주입부(220)에 전달될 수 있다. 테스트 클럭 신호(TCK_SKI)는 한 주기 내에서 특정 사이클에서만 토글링될 수 있다. 테스트 키 신호(TSI_KEY)는 특정 시점부터 다른 특정 시점까지 제1 논리 값(예를 들면, 로직 하이 레벨)을 가질 수 있다. 테스트 클럭 신호(TCK_SKI) 및 테스트 키 신호(TSI_KEY)는 각각 제1 논리 값 또는 제2 논리 값을 가질 수 있다. 이하에서는 편의상 제1 논리 값은 로직 하이 레벨 또는 1 비트(Bit)이고 제2 논리 값은 로직 로우 레벨 또는 0 비트인 것으로 가정한다.

- [0043] 제1 내지 제6 딜레이 입력 신호들(D0, D1, D2, D3, D4, D5)은 테스트 키 신호(TSI_KEY)가 딜레이된 신호들일 수 있다. 제1 내지 제6 딜레이 입력 신호들(D0, D1, D2, D3, D4, D5)은 각각 제1 논리 값 또는 제2 논리 값을 가질 수 있다. 각 딜레이 회로에 포함된 버퍼(223)의 개수가 도 4에 도시된 바와 같은 경우를 가정하면, 제1 딜레이 입력 신호(D0), 제4 딜레이 입력 신호(D3), 제3 딜레이 입력 신호(D2), 제5 딜레이 입력 신호(D4), 제2 딜레이 입력 신호(D1), 및 제6 딜레이 입력 신호(D5)로 갈수록, 딜레이된 값이 커질 수 있다.
- [0044] 일 실시예에서, 제1 내지 제6 플립플롭들(222_1, 222_2, 222_3, 222_4, 222_5, 222_6)은 테스트 클럭 신호(TCK_SKI)의 라이징 엣지에 응답하여, 테스트 클럭 신호(TCK_SKI)의 라이징 엣지에서의 제1 내지 제6 딜레이 입력 신호들(D0, D1, D2, D3, D4, D5)의 논리 값들을 래치할 수 있다. 도 5를 참조하여 예를 들면, 제1 스테이지(STG1)에서, 테스트 클럭 신호(TCK_SKI)의 라이징 엣지가 발생할 수 있다. 이때, 제1 딜레이 입력 신호(D0)의 논리 값은 제1 논리 값(또는 로직 하이 레벨, 또는 1 비트(Bit)), 제2 딜레이 입력 신호(D1)의 논리 값은 제2 논리 값(또는 로직 로우 레벨, 또는 0 비트), 제3 딜레이 입력 신호(D2) 내지 제5 딜레이 입력 신호(D4)의 논리 값은 제1 논리 값, 및 제6 딜레이 입력 신호(D5)의 논리 값은 제2 논리 값일 수 있다. 제1 내지 제6 플립플롭들(222_1, 222_2, 222_3, 222_4, 222_5, 222_6)은 래치된 논리 값들로 구성되는 입력 키(KEY_CAP [D0:D5])를 캡처할 수 있으며, 이때 입력 키(KEY_CAP [D0:D5])는 "101110"일 수 있다. 도 5를 참조하여 다른 예를 들면, 제2 스테이지(STG2)에서, 테스트 클럭 신호(TCK_SKI)의 라이징 엣지가 발생할 수 있다. 이때, 제1 딜레이 입력 신호(D0)의 논리 값은 제2 논리 값, 제2 및 제3 딜레이 입력 신호들(D1, D2)의 논리 값은 제1 논리 값, 제4 딜레이 입력 신호(D3)의 논리 값은 제2 논리 값, 제5 및 제6 딜레이 입력 신호들(D4, D5)의 논리 값은 제1 논리 값일 수 있다. 이 경우, 래치된 논리 값들로 구성되는 입력 키(KEY_CAP [D0:D5])는 "011011"일 수 있다. 도 5를 참조하여 또 다른 예를 들면, 제3 스테이지(STG3)에서, 테스트 클럭 신호(TCK_SKI)의 라이징 엣지가 발생할 수 있다. 이때, 제1 내지 제5 딜레이 입력 신호들(D0, D1, D2, D3, D4)의 논리 값은 제1 논리 값이고 제6 딜레이 입력 신호(D5)의 논리 값은 제2 논리 값일 수 있다. 이 경우, 입력 키(KEY_CAP [D0:D5])는 "111110"일 수 있다.
- [0045] 보안 키 주입부(220)는 테스트 클럭 신호(TCK_SKI)의 라이징 엣지에서의 제1 내지 제6 딜레이 입력 신호들(D0, D1, D2, D3, D4, D5)의 논리 값들을 입력 키 신호(KEY_CAP)로 생성하여, 입력 키 신호(KEY_CAP)를 키 비교기(230)에 제공할 수 있다.
- [0046] 테스트 클럭 신호(TCK_SKI)가 제1 내지 제6 플립플롭들(222_1, 222_2, 222_3, 222_4, 222_5, 222_6)에 대하여 토글링되면, 제1 내지 제6 플립플롭들(222_1, 222_2, 222_3, 222_4, 222_5, 222_6)에 의해 캡처될 수 있는 입력 키(KEY_CAP [D0:D5])의 경우의 수는 2^6 이다. 사용자 등이 키 비교기(230)에 입력된 기준 키와 동일한 입력 키를 획득하기 위해서는, 사용자가 테스트 키 신호(TSI_KEY)의 트랜지션(Transition)이 제1 내지 제6 플립플롭들(222_1, 222_2, 222_3, 222_4, 222_5, 222_6) 각각에 도달하는 시간을 모두 알고 있어야 하며, 원하는 키 값을 캡처하기 위한 테스트 키 신호(TSI_KEY)의 트랜지션과 테스트 클럭 신호(TCK_SKI) 간의 스큐(Skew)를 정확히 입력하여야 한다. 따라서, 본 개시에 따른 실시예에 의하면, 악의적 사용자가 테스트 키 신호(TSI_KEY)의 트랜지션과 테스트 클럭 신호(TCK_SKI) 간의 스큐(Skew)를 정확히 입력하기 어렵게 되므로, 보안성이 강화되는 효과가 있다.
- [0047] 진술한 바에 의하면, 플립플롭을 추가하지 않고도 암호화 정도를 높일 수 있어서, 보다 더 높은 보안성 및 신뢰성을 도모하는 효과가 있다.
- [0048] 도 6은 본 개시의 일 실시예에 따라 키 비교기를 제어하기 위한 보안 스캔 컨트롤러의 구현 예를 나타내는 도면이다.
- [0049] 도 6을 참조하면, 보안 스캔 컨트롤러(210)는 기준 키 신호(KEY_REF) 및 테스트 클럭 신호(TCK_KC)를 키 비교기(230)에 제공할 수 있다. 보안 스캔 컨트롤러(210)는 복수의 딜레이 입력 신호들이 캡처될 때마다, 복수의 딜레이 입력 신호들을 캡처되는 횟수에 대응되는 스테이지를 카운트할 수 있다. 도 4 및 도 6을 참조하여 예를 들면, 보안 스캔 컨트롤러(210)는, 제1 내지 제6 딜레이 입력 신호들(D0, D1, D2, D3, D4, D5)이 제1 스테이지(STG1)에서 캡처될 때, 제1 스테이지(STG1)를 카운트할 수 있다. 그리고, 보안 스캔 컨트롤러(210)는, 제1 내지 제6 딜레이 입력 신호들(D0, D1, D2, D3, D4, D5)이 제2 스테이지(STG2)에서 캡처될 때, 제2 스테이지(STG2)를 카운트할 수 있다. 그리고, 보안 스캔 컨트롤러(210)는, 제1 내지 제6 딜레이 입력 신호들(D0, D1, D2, D3, D4, D5)이 제3 스테이지(STG3)에서 캡처될 때, 제3 스테이지(STG3)를 카운트할 수 있다. 보안 스캔 컨트롤러(210)는, 미리 저장된 복수의 키들 중 카운트된 스테이지에 대응되는 키를 기준 키로 키 비교기(230)에 제공할 수 있다.

- [0050] 일 실시예에서, 보안 스캔 컨트롤러(210)는 키 선택기(211), 스테이지 카운터(212), 제1 논리곱 게이트(213), 제1 논리합 게이트(214), 제2 논리합 게이트(215), 제2 논리곱 게이트(216)를 포함할 수 있다.
- [0051] 키 선택기(211)는 스테이지 신호(STG)에 응답하여 미리 저장된 복수의 키들 중 카운트된 스테이지에 따라 어느 하나의 키를 기준 키로서 선택하여, 기준 키 신호(KEY_REF)를 키 비교기(230)에 전달할 수 있다. 일 실시예에서, 키 선택기(211)는 OTP(260)로부터 수신된 키 선택 신호(KEY_SEL)에 응답하여 기준 키 신호(KEY_REF)를 키 비교기(230)에 전달할 수도 있다.
- [0052] 스테이지 카운터(212)는 N개의 딜레이 입력 신호들의 논리 값들이 래치된 횟수에 대응되는 스테이지를 카운트하여 카운트된 스테이지를 나타내는 스테이지 신호(STG)를 출력할 수 있다. 도 5 및 도 6을 참조하여 예를 들면, 스테이지 카운터(212)는 제1 스테이지(STG1), 제2 스테이지(STG2), 제3 스테이지(STG3)를 순차적으로 나타내는 스테이지 신호(STG)를 출력할 수 있다. 스테이지 카운터(212)는, 스테이지가 카운트될 때마다 비교 동작을 지시하는 비교 신호(COMP)를 출력할 수 있다. 비교 신호(COMP)는 제1 논리 값 또는 제2 논리 값을 가질 수 있으며, 스테이지가 카운트되는 동안, 비교 신호(COMP)는 제1 논리 값을 가질 수 있다. 키 비교기(230)의 비교 동작이 완료된 경우 또는 미리 설정된 스테이지 카운트 수가 충족된 경우, 스테이지 카운터(212)는 비교 완료 신호(COMP_DONE)를 제1 논리합 게이트(214)에 출력할 수 있다. 비교 완료 신호(COMP_DONE)는 제1 논리 값 또는 제2 논리 값을 가질 수 있다. 키 비교기(230)의 비교 동작이 완료된 경우, 비교 신호(COMP)는 제2 논리 값을 가지고 비교 완료 신호(COMP_DONE)는 제1 논리 값을 가질 수 있다.
- [0053] 제1 논리곱 게이트(213)는 비교 신호(COMP) 및 테스트 클럭 신호(TCK)의 논리곱 연산을 수행하여 그 결과를 키 비교기(230)에 대한 테스트 클럭 신호(TCK_KC)로서 키 비교기(230)에 제공할 수 있다. 제1 논리곱 게이트(213)는 앤드 게이트(And gate)로 지칭될 수 있다.
- [0054] 제1 논리합 게이트(214)는 비교 완료 신호(COMP_DONE) 및 덤프 모드 신호(DUMP_MODE)의 논리합 연산을 수행하여 그 결과를 시스템 리셋 신호(SYS_nRESET)로서 서킷 언더 테스트(250)에 제공할 수 있다. 덤프 모드 신호(DUMP_MODE)는 제1 논리 값 또는 제2 논리 값을 가질 수 있다. 덤프 모드 신호(DUMP_MODE)가 제1 논리 값을 갖는 경우, 이는 스캔 덤프 모드가 진입되는 것을 의미할 수 있다. 시스템 리셋 신호(SYS_nRESET)는 서킷 언더 테스트(250)가 리셋되는 것을 지시하는 신호일 수 있다.
- [0055] 제2 논리합 게이트(215)는 비교 완료 신호(COMP_DONE) 및 덤프 모드 신호(DUMP_MODE)의 논리합 연산을 수행하여 그 결과를 제2 논리곱 게이트(216)에 제공할 수 있다.
- [0056] 제2 논리곱 게이트(216)는 제2 논리합 게이트(215)의 출력과 외부로부터 제공된 테스트 클럭 신호(TCK)의 논리곱 연산을 수행하여 그 결과를 서킷 언더 테스트(250)에 대한 테스트 클럭 신호(TCK_CHIP)로 출력할 수 있다.
- [0057] 키 비교기(230)는, 입력 키 신호(KEY_CAP)에 의한 입력 키가 기준 키 신호(KEY_REF)에 의한 기준 키와 일치하면, 패스를 나타내는 신호를 검증 결과 신호(P/F)로서 출력할 수 있다. 이 경우, 패스를 나타내는 신호는, 예를 들어 제1 논리 값을 갖는 신호일 수 있다. 한편, 키 비교기(230)는, 입력 키가 기준 키와 다르면, 페일을 나타내는 신호를 검증 결과 신호(P/F)로서 출력할 수 있다 이 경우, 페일을 나타내는 신호는, 예를 들어 제2 논리 값을 갖는 신호일 수 있다. 하지만, 이에 한정되는 것은 아니다.
- [0058] 도 7은 도 6에 도시된 키 선택기의 구현 예를 나타내는 도면이다.
- [0059] 도 5, 도 6 및 도 7을 참조하면, 키 선택기(211)는 스테이지에 대응되는 스테이지 키들(211_1)과 인증 키 번호에 대응되는 인증 키 세트(211_2)를 미리 저장할 수 있다. 이러한 키 선택기(211)는 제1 멀티플렉서(211_3) 및 제2 멀티플렉서(211_4)를 포함할 수 있다. 스테이지 키들(211_1)의 개수는 m개일 수 있으나 이에 한정되는 것은 아니다. 여기서, m은 2 이상 정수일 수 있다.
- [0060] 제1 멀티플렉서(211_3)는 스테이지 키들(211_1) 중 스테이지 신호(STG)에 따라 선택된 스테이지 키를 출력할 수 있다. 도 5 및 도 7을 참조하여 예를 들면, 스테이지 신호(STG)가 제1 스테이지(STG1)을 가리키는 경우, 제1 멀티플렉서(211_3)는 제1 스테이지 키(KEY_0)를 출력할 수 있다.
- [0061] 제2 멀티플렉서(211_4)는 제1 멀티플렉서(211_3)에 의해 선택된 스테이지 키와 인증 키 세트(211_2) 중 키 선택 신호(KEY_SEL)(또는 인증 키 데이터)에 따라 키를 선택하여, 기준 키 신호(KEY_REF)를 출력할 수 있다.
- [0062] 도 8은 본 개시의 일 실시예에 따른 스캔 출력 리맵퍼를 설명하기 위한 도면이다.
- [0063] 도 8을 참조하면, 스캔 출력 리맵퍼(240)는 리맵 컨트롤러(241), 제1 레지스터 세트(242), 제2 레지스터 세트

(243), 제1 선택기(244), 및 제2 선택기(245)를 포함할 수 있다.

- [0064] 리맵 컨트롤러(241)는, 스캔 출력 리맵퍼(240)에 대한 테스트 클럭 신호(TCK_SR), 스캔 출력 신호(PSO), 검증 결과 신호(P/F), 덤프 모드 신호(DUMP_MODE), 및 비교 키 신호(KEY_COMP)를 수신할 수 있다. 실시예에 따라, 리맵 컨트롤러(241)는 맵 선택 신호(MAP_SEL)를 더 수신할 수 있다. 리맵 컨트롤러(241)는 스캔 출력 신호(PSO)를 제1 및 제2 레지스터 세트들(242, 243)에 전달할 수 있다. 리맵 컨트롤러(241)는, 테스트 클럭 신호(TCK_SR) 및 비교 키 신호(KEY_COMP)를 기초로, 제1 클럭 신호(TCK_1)를 제1 레지스터 세트(242)에 출력하고 제2 클럭 신호(TCK_2)를 제2 레지스터 세트(243)에 출력할 수 있다. 리맵 컨트롤러(241)는 제1 스캔 인에이블 신호(SE_1)를 제1 레지스터 세트(242)에 출력하고 제2 스캔 인에이블 신호(SE_2)를 제2 레지스터 세트(243)에 제공하고 출력할 수 있다. 실시예에 따라, 제2 스캔 인에이블 신호(SE_2)는 제1 스캔 인에이블 신호(SE_1)가 반전된 신호일 수 있다.
- [0065] 제1 레지스터 세트(242)는 제1 스캔 인에이블 신호(SE_1) 및 제1 클럭 신호(TCK_1)에 응답하여 스캔 출력 신호(PSO)를 래치하고, 래치된 제1 스캔 출력 신호(OSO1)를 출력할 수 있다. 제1 레지스터 세트(242)는 그라운드(GND)와 연결될 수 있다.
- [0066] 제2 레지스터 세트(243)는 제2 스캔 인에이블 신호(SE_2) 및 제2 클럭 신호(TCK_2)에 응답하여 스캔 출력 신호(PSO)를 래치하고, 래치된 제2 스캔 출력 신호(OSO2)를 출력할 수 있다. 제2 레지스터 세트(243)는 그라운드(GND)와 연결될 수 있다.
- [0067] 제1 선택기(244)는 제1 스캔 출력 신호(OSO1) 및 제2 스캔 출력 신호(OSO2) 중 제2 스캔 인에이블 신호(SE_2)에 따라 어느 하나를 선택할 수 있다.
- [0068] 제2 선택기(245)는 제1 선택기(244)로부터 선택된 스캔 출력 신호(OSO_SEL)와 스캔 출력 신호(PSO) 중 검증 결과 신호(P/F)에 따라 어느 하나를 보안 스캔 출력 신호(SSO)로 출력할 수 있다.
- [0069] 도 9는 본 개시의 일 실시예에 따른 스캔 출력 리맵퍼를 구현하기 위한 일 예시를 나타낸 도면이다.
- [0070] 도 9를 참조하면, 제1 레지스터 세트(242)는, 직렬로 케스케이드된 r개의(r은 1 이상의 정수) 제1 플립플롭들을 포함할 수 있다. 직렬로 케스케이드된 것은 현재 플립플롭의 출력 단자가 다음 플립플롭의 입력 단자에 접속된 형태인 것일 수 있다. 도 9를 참조하여 예를 들면, 제1 레지스터 세트(242)는 현재 플립플롭의 출력과 다음 플립플롭의 입력이 연결된 4개의 제1 플립플롭들(242_1, 242_2, 242_3, 242_4)을 포함할 수 있다. 하지만, 이에 한정되는 것은 아니다. 이하에서는 제1 플립플롭의 개수는 4개인 것으로 가정한다. 제1 플립플롭들(242_1, 242_2, 242_3, 242_4) 각각은 4개의 제1 클럭 신호들(TCK_11, TCK_12, TCK_13, TCK_14)의 라이징 엣지에 응답하여 스캔 출력 신호(PSO)를 래치할 수 있다. 제1 플립플롭들(242_1, 242_2, 242_3, 242_4)에서 제1 플립플롭(242_1)은 그라운드(GND)를 스캔 입력 단(SI)으로 입력 받고, 3개의 제1 플립플롭들(242_2, 242_3, 242_4)은 이전 플립플롭의 스캔 출력 단(SO)이 다음 플립플롭의 스캔 입력 단(SI)에 연결될 수 있다. 제1 플립플롭들(242_4)이 MSB(Most Significant Bit)에 대응되고, 제1 플립플롭(242_1)이 LSB(Least Significant Bit)에 대응될 수 있다.
- [0071] 제2 레지스터 세트(243)는, 직렬로 케스케이드된 r개의 제2 플립플롭들을 포함할 수 있다. 도 9를 참조하여 예를 들면, 제2 레지스터 세트(243)는 현재 플립플롭의 출력과 다음 플립플롭의 입력이 연결된 4개의 제2 플립플롭들(243_1, 243_2, 243_3, 243_4)을 포함할 수 있다. 하지만, 이에 한정되는 것은 아니다. 이하에서는 제2 플립플롭의 개수는 4개인 것으로 가정한다. 제2 플립플롭들(243_1, 243_2, 243_3, 243_4) 각각은 4개의 제2 클럭 신호들(TCK_21, TCK_22, TCK_23, TCK_24)의 라이징 엣지에 응답하여 스캔 출력 신호(PSO)를 래치할 수 있다. 제2 플립플롭들(243_1, 243_2, 243_3, 243_4)에서 제2 플립플롭(243_1)은 그라운드(GND)를 스캔 입력 단(SI)으로 입력 받고, 3개의 제2 플립플롭들(243_2, 243_3, 243_4)은 이전 플립플롭의 스캔 출력 단(SO)이 다음 플립플롭의 스캔 입력 단(SI)에 연결될 수 있다. 제2 플립플롭들(243_4)이 MSB(Most Significant Bit)에 대응되고, 제2 플립플롭(243_1)이 LSB(Least Significant Bit)에 대응될 수 있다.
- [0072] 리맵 컨트롤러(241)는 4개의 제1 클럭 신호들(TCK_11, TCK_12, TCK_13, TCK_14)을 제1 레지스터 세트(242)에 출력할 수 있다. 리맵 컨트롤러(241)는 4개의 제2 클럭 신호들(TCK_21, TCK_22, TCK_23, TCK_24)을 제2 레지스터 세트(243)에 출력할 수 있다. 리맵 컨트롤러(241)는 제1 스캔 인에이블 신호(SE_1)를 제1 레지스터 세트(242)에 출력할 수 있다.
- [0073] 스캔 출력 리맵퍼(240)는 인버터(246)를 더 포함할 수 있다. 인버터(246)는 제1 스캔 인에이블 신호(SE_1)를 반

전시켜 제2 스캔 인에이블 신호(SE_2)를 제2 레지스터 세트(243)에 출력할 수 있다.

- [0074] 일 실시예에서, 제1 선택기(244)는 제1 멀티플렉서(244_1)로 구현될 수 있다. 하지만, 이에 한정되는 것은 아니다. 제1 멀티플렉서(244_1)는 제2 스캔 인에이블 신호(SE_2)의 논리 값에 따라 제1 스캔 출력 신호(OS01) 또는 제2 스캔 출력 신호(OS02)를 선택 및 출력할 수 있다. 예를 들면, 제2 스캔 인에이블 신호(SE_2)의 논리 값이 제1 논리값(예를 들어, 로직 하이 레벨)인 경우, 제1 멀티플렉서(244_1)는 제2 스캔 출력 신호(OS02)를 출력할 수 있다. 다른 예를 들면, 제2 스캔 인에이블 신호(SE_2)의 논리 값이 제2 논리값(예를 들어, 로직 로우 레벨)인 경우, 제1 멀티플렉서(244_1)는 제1 스캔 출력 신호(OS01)를 출력할 수 있다.
- [0075] 일 실시예에서, 제2 선택기(245)는 제2 멀티플렉서(245_1)로 구현될 수 있다. 하지만, 이에 한정되는 것은 아니다. 제2 멀티플렉서(245_1)는 검증 결과 신호(P/F)의 논리 값에 따라 선택된 스캔 출력 신호(OSO_SEL) 또는 스캔 출력 신호(PSO)를 선택 및 출력할 수 있다. 예를 들면, 검증 결과 신호(P/F)의 논리 값이 제1 논리값(예를 들어, 패스 또는 로직 하이 레벨)인 경우, 제2 멀티플렉서(245_1)는 스캔 출력 신호(PSO)를 보안 스캔 출력 신호(SSO)로 출력할 수 있다. 다른 예를 들면, 검증 결과 신호(P/F)의 논리 값이 제2 논리값(예를 들어, 페일 또는 로직 로우 레벨)인 경우, 제2 멀티플렉서(245_1)는 선택된 스캔 출력 신호(OSO_SEL)를 보안 스캔 출력 신호(SSO)로 출력할 수 있다.
- [0076] 도 10은 본 개시의 일 실시예에 따른 리맵 컨트롤러의 구현 예를 나타내는 도면이다.
- [0077] 도 10을 참조하면, 리맵 컨트롤러(241)는 비교 키 신호(KEY_COMP)를 기초로 스캔 출력 신호(PSO)를 난독화하기 위한 난독화 정보를 생성하고, 난독화 정보에 따라 스캔 출력 신호(PSO)를 난독화할 수 있다. 이러한 난독화 정보는 r개의 제1 클럭 신호들(TCK_1 [r-1:0]) 또는 r개의 제2 클럭 신호들(TCK_2 [r-1:0])의 라이징 엣지 타이밍으로 나타낼 수 있다.
- [0078] 리맵 컨트롤러(241)는 리니어-피드백 시프트 레지스터(241_1), 원-핫 인코더(241_2), 제1 멀티플렉서(241_3), 제2 멀티플렉서(241_4), 제3 멀티플렉서(241_5), r개의 제1 논리곱 게이트들(241_6), 및 r개의 제2 논리곱 게이트들(241_7)을 포함할 수 있다.
- [0079] 리니어-피드백 시프트 레지스터(241_1)는 비교 키 신호(KEY_COMP)를 기초로 r개의 리니어 신호들(L0)을 출력할 수 있다. 여기서, 리니어 신호들(L0)의 개수는 제1 및 제2 레지스터 세트들(242, 243)에 포함된 플립플롭의 개수와 동일할 수 있다.
- [0080] 원-핫 인코더(241_2)는 맵 선택 신호(MAP_SEL)를 기초로 r개의 인코딩 신호들(E0)을 출력할 수 있다. 여기서, 인코딩 신호들(E0)의 개수는 제1 및 제2 레지스터 세트들(242, 243)에 포함된 플립플롭의 개수와 동일할 수 있다.
- [0081] r개의 리니어 신호들(L0) 및 r개의 인코딩 신호들(E0)은 전술한 난독화 정보에 대응될 수 있다.
- [0082] 제1 멀티플렉서(241_3)는 덤프 모드 신호(DUMP_MODE)의 논리 값에 따라 r개의 리니어 신호들(L0) 또는 r개의 인코딩 신호들(E0)을 출력할 수 있다. 예를 들면, 덤프 모드 신호(DUMP_MODE)의 논리 값이 제1 논리값인 경우, 제1 멀티플렉서(241_3)는 r개의 인코딩 신호들(E0)을 출력할 수 있다. 다른 예를 들면, 덤프 모드 신호(DUMP_MODE)의 논리 값이 제2 논리값인 경우 제1 멀티플렉서(241_3)는 r개의 리니어 신호들(L0)을 출력할 수 있다.
- [0083] 제2 멀티플렉서(241_4)는, 제1 스캔 인에이블 신호(SE_1)의 논리 값에 따라, 미리 저장된 제1 논리 값을 갖는 제1 데이터(241_8) 또는 제1 멀티플렉서(241_3)의 출력 신호를 출력할 수 있다. 예를 들면, 제1 스캔 인에이블 신호(SE_1)의 논리 값이 제1 논리값인 경우, 제2 멀티플렉서(241_4)는 제1 데이터(241_8)를 출력할 수 있다. 다른 예를 들면, 제1 스캔 인에이블 신호(SE_1)의 논리 값이 제2 논리값인 경우, 제2 멀티플렉서(241_4)는 제1 멀티플렉서(241_3)의 출력 신호를 출력할 수 있다.
- [0084] 제3 멀티플렉서(241_5)는 제1 스캔 인에이블 신호(SE_1)의 논리 값에 따라, 미리 저장된 제1 논리 값을 갖는 제2 데이터(241_9) 또는 제1 멀티플렉서(241_3)의 출력 신호를 출력할 수 있다. 예를 들면, 제1 스캔 인에이블 신호(SE_1)의 논리 값이 제1 논리값인 경우, 제3 멀티플렉서(241_5)는 제1 멀티플렉서(241_3)의 출력 신호를 출력할 수 있다. 다른 예를 들면, 제1 스캔 인에이블 신호(SE_1)의 논리 값이 제2 논리값인 경우, 제3 멀티플렉서(241_5)는 제2 데이터(241_9)를 출력할 수 있다.
- [0085] 실시예에 따라, 제1 데이터(241_8)와 제2 데이터(241_9)는, 같은 저장 공간에 하나의 데이터로 저장되거나 서로

다른 저장 공간에 각각 저장될 수 있다.

- [0086] r개의 제1 논리곱 게이트들(241_6)은, 각각 테스트 클럭 신호(TCK_SR) 및 제2 멀티플렉서(241_4)의 출력 신호의 논리곱 연산을 수행할 수 있다.
- [0087] r개의 제2 논리곱 게이트들(241_7)은, 각각 테스트 클럭 신호(TCK_SR) 및 제3 멀티플렉서(241_5)의 출력 신호의 논리곱 연산을 수행할 수 있다.
- [0088] 도 11은 테스트 모드에서 출력되는 보안 스캔 출력 신호를 설명하기 위한 도면이다.
- [0089] 도 9, 도 10 및 도 11을 참조하면, 편의상 테스트 클럭 신호(TCK_SR)의 사이클의 개수는 12개이고, r은 4이고, 리니어 신호들(L0)의 논리 값(또는 비트 값)은, 각 사이클 마다 순차적으로, "0011", "0001", "1000", "0100", "0010", "1001", "1100", "0110", "1011", "0101", "1010", "1101"이며, "-"은 제1 클럭 신호들(TCK_11, TCK_12, TCK_13, TCK_14) 및 제2 클럭 신호들(TCK_21, TCK_22, TCK_23, TCK_24)이 게이트드(Gated) 되는 것으로 가정한다. "En"은 제1 클럭 신호들(TCK_11, TCK_12, TCK_13, TCK_14) 및 제2 클럭 신호들(TCK_21, TCK_22, TCK_23, TCK_24)이 인에이블드(Enabled), 라이징 엣지를 갖는 것 또는 각 플립플롭에 입력되며, "SR_A [3:0]"은 제1 스캔 출력 신호(OS01)이고 "SR_B [3:0]"는 제2 스캔 출력 신호(OS02)인 것으로 가정한다.
- [0090] 4개의 사이클마다 제1 스캔 인에이블 신호(SE_1)의 논리 값과 제2 스캔 인에이블 신호(SE_2)의 논리 값이 서로 교번하는 것으로 가정한다. 예를 들면, 첫 번째 사이클부터 네 번째 사이클까지(즉, 0번 사이클 카운트부터 3번 사이클 카운트까지) 제1 스캔 인에이블 신호(SE_1)의 논리 값은 로직 로우 레벨이고, 제2 스캔 인에이블 신호(SE_2)의 논리 값은 로직 하이 레벨일 수 있다. 이 경우, 보안 스캔 출력 신호(SS0)는 4개의 제2 플립플롭들(243_1, 243_2, 243_3, 243_4)로부터 출력된 신호일 수 있다. 그리고, 다섯 번째 사이클부터 여덟 번째 사이클까지(즉, 4번 사이클 카운트부터 7번 사이클 카운트까지) 제1 스캔 인에이블 신호(SE_1)의 논리 값은 로직 하이 레벨이고, 제2 스캔 인에이블 신호(SE_2)의 논리 값은 로직 로우 레벨일 수 있다. 이 경우, 이 경우, 보안 스캔 출력 신호(SS0)는 4개의 제1 플립플롭들(242_1, 242_2, 242_3, 242_4)로부터 출력된 신호일 수 있다.
- [0091] 첫 번째 사이클 즉, 사이클 카운트가 0인 경우, 스캔 출력 신호(PS0)의 값은 "p0"이고, 제1 클럭 신호들(TCK_11, TCK_12)만 인에이블된다. 제1 플립플롭들(242_1, 242_2)은 제1 클럭 신호들(TCK_13, TCK_14)의 라이징 엣지에 응답하여 "p0"를 래치할 수 있다. 두 번째 사이클 즉, 사이클 카운트가 1인 경우, 스캔 출력 신호(PS0)의 값은 "p1"이고, 제1 클럭 신호(TCK_11)만 인에이블된다. 제1 플립플롭(242_1)은 제1 클럭 신호(TCK_11)의 라이징 엣지에 응답하여 "p1"를 래치할 수 있다. 세 번째 사이클 즉, 사이클 카운트가 2인 경우, 제1 클럭 신호(TCK_14)만 인에이블되며, 제1 플립플롭(242_4)은 제1 클럭 신호(TCK_14)의 라이징 엣지에 응답하여 "p2"를 래치할 수 있다. 사이클 카운트가 3인 경우, 제1 클럭 신호(TCK_13)만 인에이블되며, 제1 플립플롭(242_3)은 제1 클럭 신호(TCK_13)의 라이징 엣지에 응답하여 "p3"를 래치할 수 있다.
- [0092] 사이클 카운트가 4 내지 7인 경우, 보안 스캔 출력 신호(SS0)는, MSB에 대응되는 제1 플립플롭(242_4)부터 LSB에 대응되는 제1 플립플롭(242_1)까지, 각 플립플롭의 출력 값을 순차적으로 출력할 수 있다. 사이클 카운트가 4인 경우에 보안 스캔 출력 신호(SS0)는 "p2"이고 사이클 카운트가 5인 경우에 보안 스캔 출력 신호(SS0)는 "p3"이고, 사이클 카운트가 6인 경우에 보안 스캔 출력 신호(SS0)는 "p0"이며, 사이클 카운트가 7인 경우에 보안 스캔 출력 신호(SS0)는 "p1"일 수 있다.
- [0093] 사이클 카운트가 4인 경우, 제2 클럭 신호(TCK_22)만 인에이블된다. 제2 플립플롭(243_2)은 제2 클럭 신호(TCK_22)의 라이징 엣지에 응답하여 "p4"를 래치할 수 있다. 사이클 카운트가 5인 경우, 제2 플립플롭들(243_1, 243_4)은 제2 클럭 신호(TCK_21, TCK_24)의 라이징 엣지에 응답하여 "p5"를 래치할 수 있다. 마찬가지로, 사이클 카운트가 6인 경우, 제2 플립플롭들(243_3, 243_4)은 "p6"를 래치할 수 있다. 사이클 카운트가 7인 경우, 제2 플립플롭들(243_2, 243_3)은 "p7"를 래치할 수 있다.
- [0094] 사이클 카운트가 8 내지 11인 경우, MSB에 대응되는 제2 플립플롭(243_4)부터 LSB에 대응되는 제2 플립플롭(243_1)까지, 순차적으로, "p6", "p7", "p7", 또는 "p5"을 갖는 보안 스캔 출력 신호(SS0)가 출력될 수 있다.
- [0095] 도 12는 스캔 덤프 모드에서 출력되는 보안 스캔 출력 신호를 설명하기 위한 도면이다.
- [0096] 도 9, 도 10, 도 11 및 도 12를 참조하면, 도 11과 유사하게, 편의상 테스트 클럭 신호(TCK_SR)의 사이클의 개수는 8개이고, r은 4이고, 맵 선택 신호(MAP_SEL)의 값은 {2'b00, 2'b10, 2'b11, 2'b01}(또는 "00101101")인 것으로 가정한다. 이때 맵 선택 신호(MAP_SEL)의 값을 나타내는 {A, B, C, D}는, MSB에 대응되는 플립플롭부터 LSB에 대응되는 플립플롭까지의 우선순위를 나타낸다. 예를 들면, {A, B, C, D}에서 첫 번째 비트 자리(즉,

"A")는 MSB에 대응되는 플립플롭(예를 들면, 제1 플립플롭(242_4) 및 제2 플립플롭(243_4))의 우선 순위를 나타내고, 두 번째 비트 자리(즉, "B")는 (MSB-1)에 대응되는 플립플롭(예를 들면, 제1 플립플롭(242_3) 및 제2 플립플롭(243_3))의 우선 순위를 나타내고, 세 번째 비트 자리(즉, "C")는 (MSB-2)에 대응되는 플립플롭(예를 들면, 제1 플립플롭(242_2) 및 제2 플립플롭(243_2))의 우선 순위를 나타내고, 네 번째 비트 자리(즉, "D")는 LSB에 대응되는 플립플롭(예를 들면, 제1 플립플롭(242_1) 및 제2 플립플롭(243_1))의 우선 순위를 나타낼 수 있다. 그리고, 괄호("{}")안의 값이 낮을수록 래치되는 순서가 빠르다. 예를 들면, {2'b00, 2'b10, 2'b11, 2'b01}의 경우, 래치하는 순서가 MSB에 대응되는 플립플롭, LSB에 대응되는 플립플롭, (MSB-1)에 대응되는 플립플롭, 및 (MSB-2)에 대응되는 플립플롭일 수 있다. 이 경우, 인코딩 신호들(E0)의 논리 값은, "1000", "0001", "0100", "0010"으로 4개의 사이클마다 반복될 수 있다.

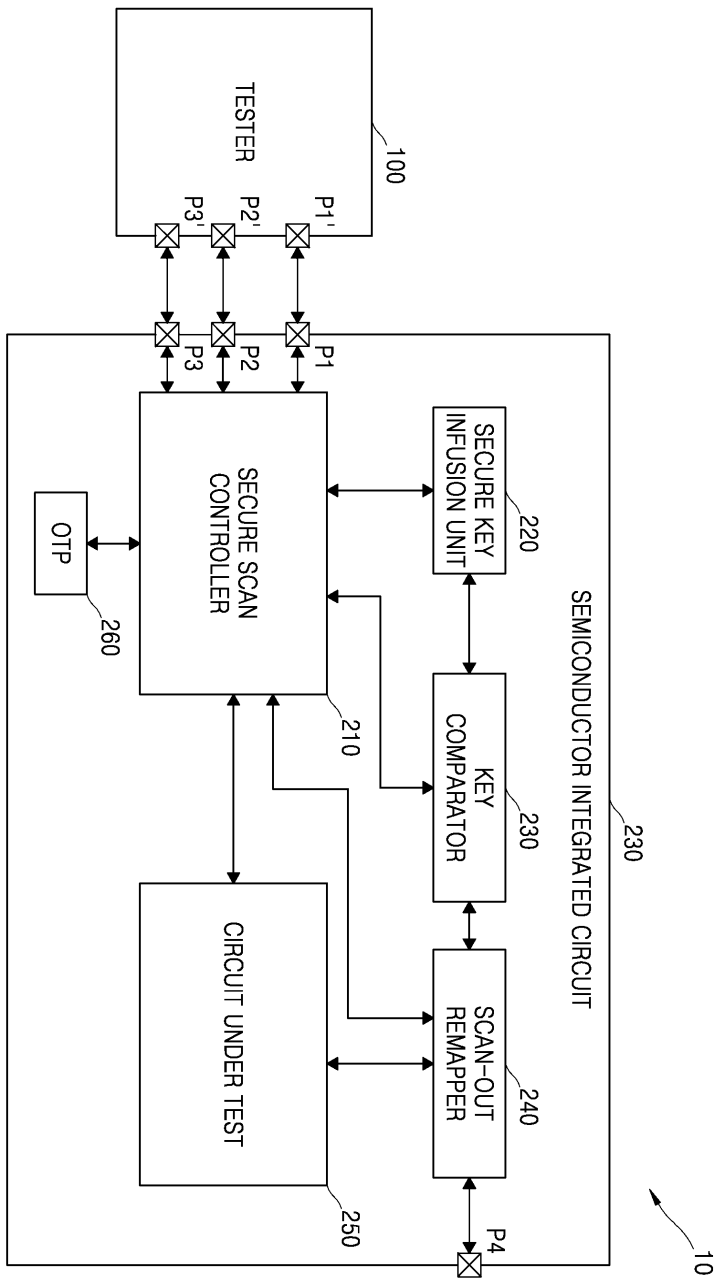
- [0097] 한편, 도 11에 도시된 바와 같이, 4개의 사이클마다 제1 스캔 인에이블 신호(SE_1)의 논리 값과 제2 스캔 인에이블 신호(SE_2)의 논리 값이 서로 교번하는 것으로 가정한다.
- [0098] 사이클 카운트가 0일 때, 제1 플립플롭(242_4)은 "p0"를 래치할 수 있다. 사이클 카운트가 1일 때, 제1 플립플롭(242_1)은 "p1"를 래치할 수 있다. 사이클 카운트가 2일 때, 제1 플립플롭(242_3)은 "p2"를 래치할 수 있다. 사이클 카운트가 3일 때, 제1 플립플롭(242_2)은 "p3"을 래치할 수 있다. 보안 스캔 출력 신호(SS0)의 값은 "0"일 수 있다.
- [0099] 사이클 카운트가 4일 때, 제2 플립플롭(243_4)은 "p4"를 래치할 수 있다. 사이클 카운트가 5일 때, 제2 플립플롭(243_1)은 "p5"를 래치할 수 있다. 사이클 카운트가 6일 때, 제2 플립플롭(243_3)은 "p6"를 래치할 수 있다. 사이클 카운트가 7일 때, 제2 플립플롭(243_2)은 "p7"을 래치할 수 있다. 보안 스캔 출력 신호(SS0)의 값은 순차적으로, "p0", "p2", "p3", "p1"일 수 있다.
- [0100] 도 13은 본 개시의 다른 실시예에 따른 반도체 집적 회로를 설명하기 위한 도면이다.
- [0101] 도 13을 참조하면, 반도체 직접 회로(400)는, 도 1을 참조하여 기술한 바와 같이, 제1 내지 제4 핀들(P1, P2, P3, P4)을 구비할 수 있다. 반도체 직접 회로(400)는 싱글 락 키 회로(410) 및 복수의 칩들(420_1, 420_2, ..., 420_n)을 포함할 수 있다. n은 2 이상의 정수일 수 있다.
- [0102] 싱글 락 키 회로(410)는 도 1에 도시된 보안 스캔 컨트롤러(210), 보안 키 주입부(220), 키 비교기(230), 스캔 출력 리맵퍼(240), 서킷 언더 테스트(250), 및 OTP(260)를 포함할 수 있다.
- [0103] 싱글 락 키 회로(410)는 도 1에 도시된 보안 스캔 컨트롤러(210), 보안 키 주입부(220), 키 비교기(230), 스캔 출력 리맵퍼(240), 및 OTP(260)를 포함할 수 있다.
- [0104] 복수의 칩들(420_1, 420_2, ..., 420_n) 각각은 도 1에 도시된 서킷 언더 테스트(250)에 대응될 수 있다. 이러한 복수의 칩들(420_1, 420_2, ..., 420_n)은 복수의 테스트 인터페이스들(421_1, 421_2, ..., 421_n)을 포함할 수 있다. 복수의 테스트 인터페이스들(421_1, 421_2, ..., 421_n)은, 테스트 모드 또는 스캔 덤프 모드 시, 싱글 락 키 회로(410)와 통신하기 위한 인터페이스일 수 있다. 실시예에 따라, 복수의 칩들(420_1, 420_2, ..., 420_n)은 복수의 회로로 구현될 수 있다.
- [0105] 도 14는 본 개시의 또 다른 실시예에 따른 반도체 집적 회로를 설명하기 위한 도면이다.
- [0106] 도 14를 참조하면, 반도체 집적 회로(500)는 제1 및 제2 핀들(P1', P2')을 구비할 수 있다. 반도체 집적 회로(500)는, 제1 핀(P1')을 통해, 테스트 스캔 입력 신호(TSI) 또는 테스트 클럭 신호(TCK)를 수신할 수 있다. 반도체 집적 회로(500)는, 제2 핀(P2')을 통해, 보안 스캔 출력 신호(SS0)를 출력할 수 있다.
- [0107] 반도체 집적 회로(500)는 싱글 락 키 회로 그룹(510), 복수의 칩들(520_1, 520_2, ..., 520_n), 및 디멀티플렉서(530)를 포함할 수 있다.
- [0108] 싱글 락 키 회로 그룹(510)은 복수의 싱글 락 키 회로들(510_1, 510_2, ..., 510_n)을 포함할 수 있다. 복수의 싱글 락 키 회로들(510_1, 510_2, ..., 510_n) 각각은 도 13을 참조하여 기술한 싱글 락 키 회로(410)에 대응될 수 있다.
- [0109] 복수의 칩들(520_1, 520_2, ..., 520_n)은 도 13을 참조하여 기술한 복수의 칩들(420_1, 420_2, ..., 420_n)에 대응될 수 있다.
- [0110] 일 실시예에서, 제1 싱글 락 키 회로(510_1)는 제1 칩(520_1)에 포함된 제1 테스트 인터페이스(521_1)와 통신할 수 있다. 제2 싱글 락 키 회로(510_2)는 제2 칩(520_2)에 포함된 제2 테스트 인터페이스(521_2)와 통신할 수 있다.

다. 제 n 싱글 락 키 회로(510 $_n$)는 제 n 칩(520 $_n$)에 포함된 제 n 테스트 인터페이스(521 $_n$)와 통신할 수 있다.

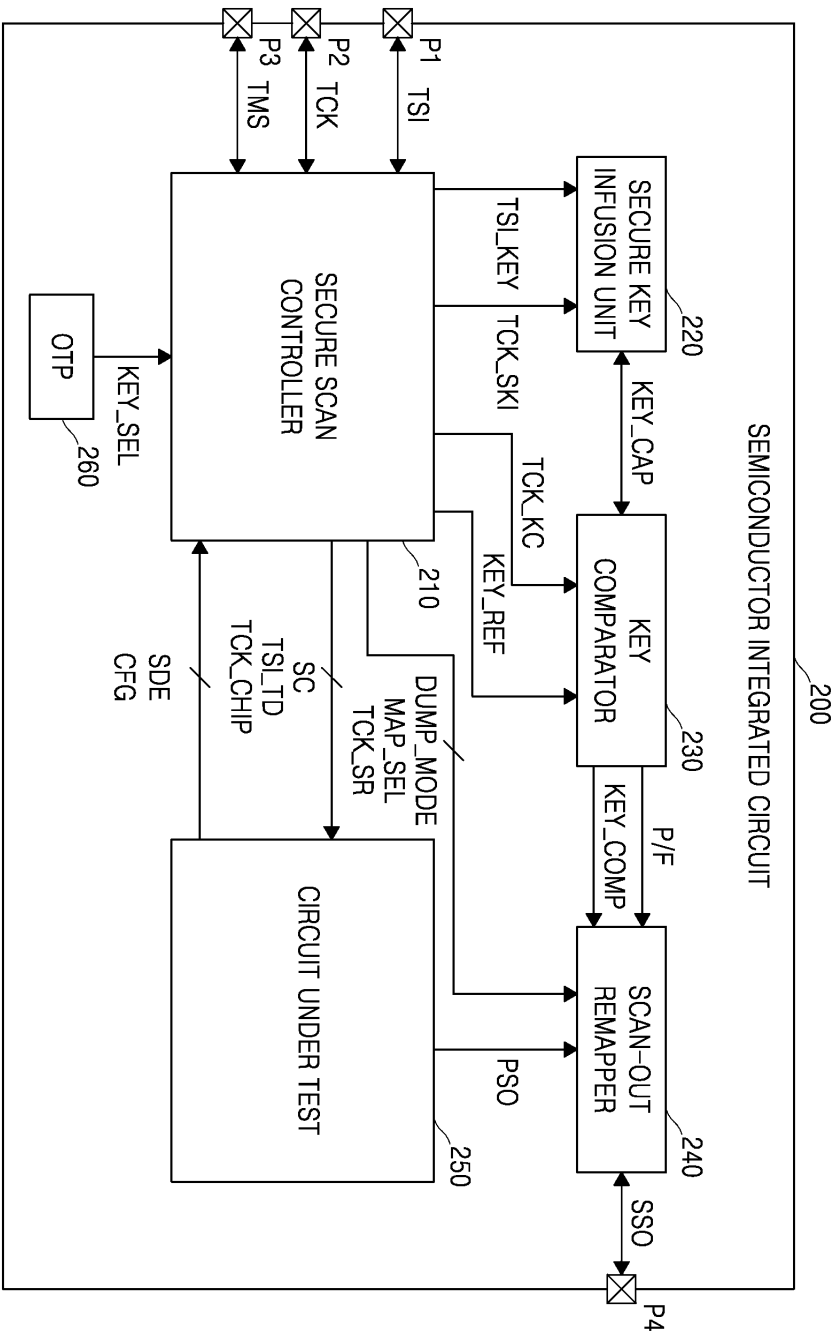
- [0111] 디멀티플렉서(530)는 제1 핀(P1')을 통해, 외부로부터 수신된 신호를 복수의 싱글 락 키 회로들(510 $_1$, 510 $_2$, ..., 510 $_n$)에 전달할 수 있다.
- [0112] 도 15는 본 개시의 일 실시예에 따른 반도체 집적 회로를 테스트하는 방법을 설명하기 위한 흐름도이다.
- [0113] 도 15를 참조하면, 반도체 집적 회로를 테스트하는 방법은, 테스트 스캔 입력 신호를 서로 다른 딜레이 값을 갖는 복수의 딜레이 입력 신호들로 변경하는 단계(S310), 테스트 클럭 신호에 응답하여 복수의 딜레이 입력 신호들을 캡처함으로써 입력 키 신호를 생성하는 단계(S320), 입력 키 신호에 따른 입력 키가 미리 설정된 기준 키와 일치하는지 여부를 검증하는 단계(S330), 칩으로부터 스캔 출력 신호를 획득하는 단계(S340), 및 검증 결과에 따라, 테스트 대상이 되는 칩으로부터 출력된 스캔 출력 신호를 난독화하는 단계(S350, S360, S370, S380)를 포함할 수 있다.
- [0114] 검증 결과에 따라, 테스트 대상이 되는 칩으로부터 출력된 스캔 출력 신호를 난독화하는 단계(S350, S360, S370, S380)의 경우, 검증 패스인지 여부를 확인하는 단계(S350), 검증 결과가 패스이면(S350, YES), 스캔 출력 신호를 출력 핀을 통해 외부에 출력하는 단계(S360), 검증 결과가 페일이면(S350, NO), 스캔 출력 신호를 난독화하는 단계(S370) 및 난독화된 스캔 출력 신호를 출력 핀을 통해 외부에 출력하는 단계(S380)가 수행될 수 있다.
- [0115] 일 실시예에서, 복수의 딜레이 입력 신호들은, 각각 제1 논리 값 또는 제1 논리 값과 다른 제2 논리 값을 가질 수 있다. 이 경우, 입력 키 신호를 생성하는 단계(S320)는, 테스트 클럭 신호의 라이징 엣지에서의 복수의 딜레이 입력 신호들의 논리 값들을 입력 키 신호로 생성할 수 있다.
- [0116] 일 실시예에서, 입력 키 신호에 따른 입력 키가 미리 설정된 기준 키와 일치하는지 여부를 검증하는 단계(S330)에서, 입력 키가 기준 키와 일치하면, 패스를 나타내는 신호가 출력될 수 있다. 한편, 입력 키가 기준 키와 다르면, 페일을 나타내는 신호가 출력될 수 있다.
- [0117] 일 실시예에서, 스캔 출력 신호를 출력 핀을 통해 외부에 출력하는 단계(S360)에서, 비난독화된 스캔 출력 신호가 보안 스캔 출력 신호로 출력될 수 있다.
- [0118] 일 실시예에서, 난독화된 스캔 출력 신호를 출력 핀을 통해 외부에 출력하는 단계(S380)에서, 난독화된 스캔 출력 신호가 보안 스캔 출력 신호로 출력될 수 있다.
- [0119] 전술한 바에 의하면, 테스트를 수행하기 위한 회로를 악의적으로 사용하는 것으로부터 방지함으로써, 신뢰성 및 보안성이 개선되는 효과가 있다.
- [0120] 또한, 전술한 바에 의하면, 테스트 스캔 입력을 페러럴라이즈드 인풋(Parallelized input) 방식으로 플립플롭에 입력시킴으로써, 보안 키의 입력의 경우의 수를 기하급수적으로 늘릴 수 있고, 이에 따라 보안성을 더욱 증대시키는 효과가 있다.
- [0121] 또한, 전술한 바에 의하면, 보안성을 강화하기 위해 시리얼라이즈드 인풋(Serialized input) 방식으로 구현된 플립플롭을 추가하는 대신에 페러럴라이즈드 인풋(Parallelized input) 방식으로 플립플롭에 입력되는 테스트 스캔 인풋을 한번 더 입력시킴으로써, 제조 비용을 절감하고 제품을 집적화하는 효과가 있다.
- [0122] 이상에서와 같이 도면과 명세서에서 예시적인 실시예들이 개시되었다. 본 명세서에서 특정한 용어를 사용하여 실시예들을 설명되었으나, 이는 단지 본 개시의 기술적 사상을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 개시의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 개시의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

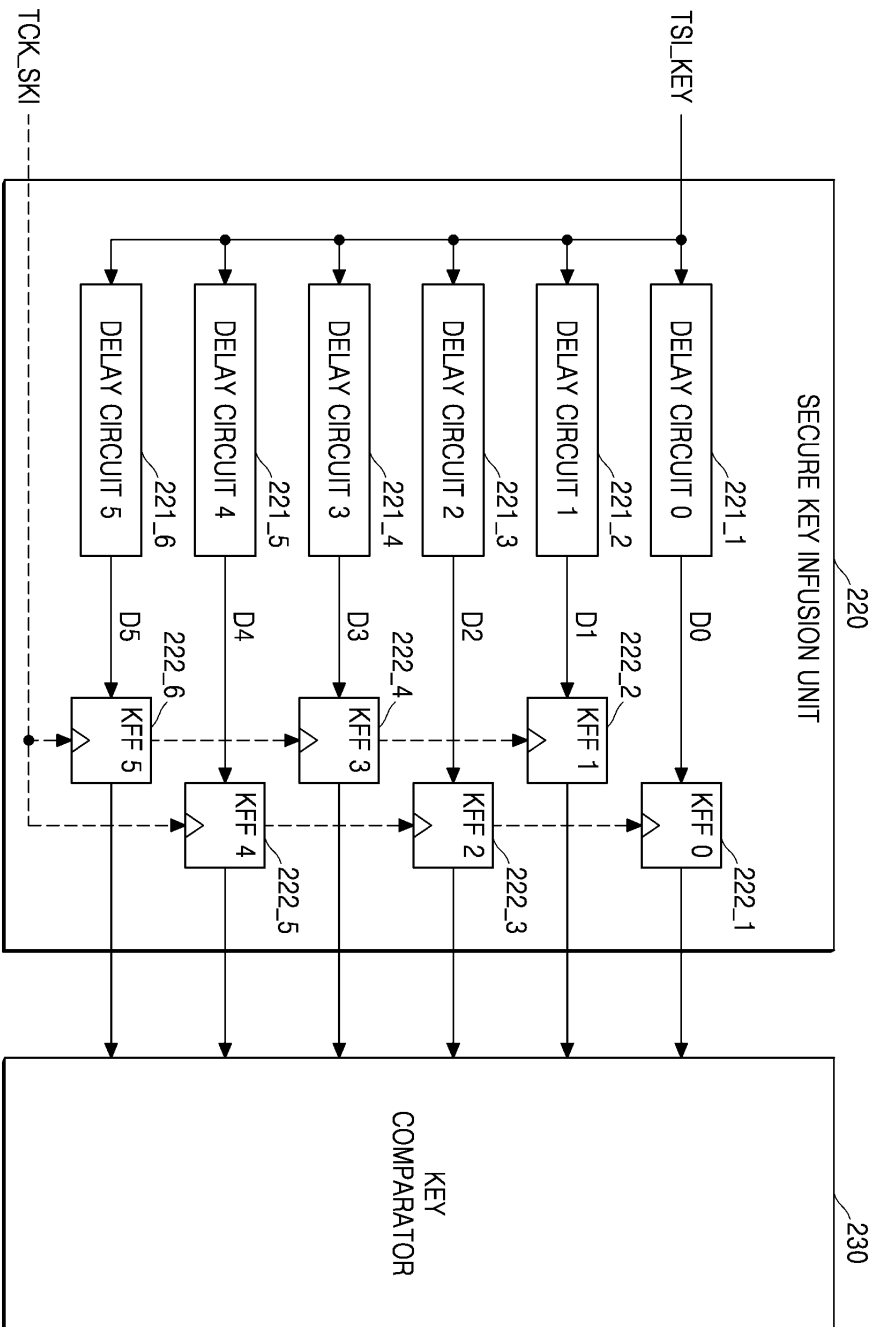
도면1



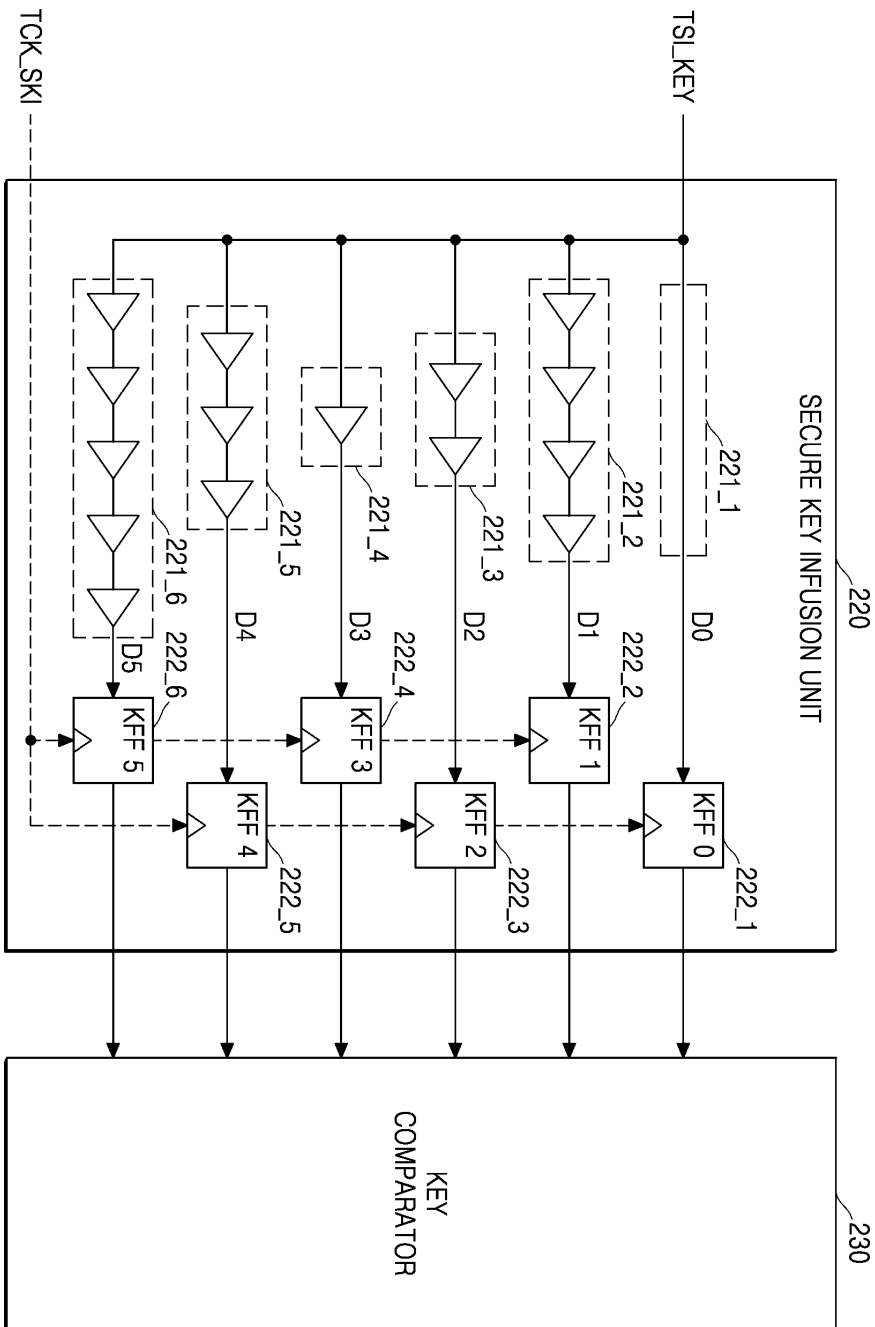
도면2



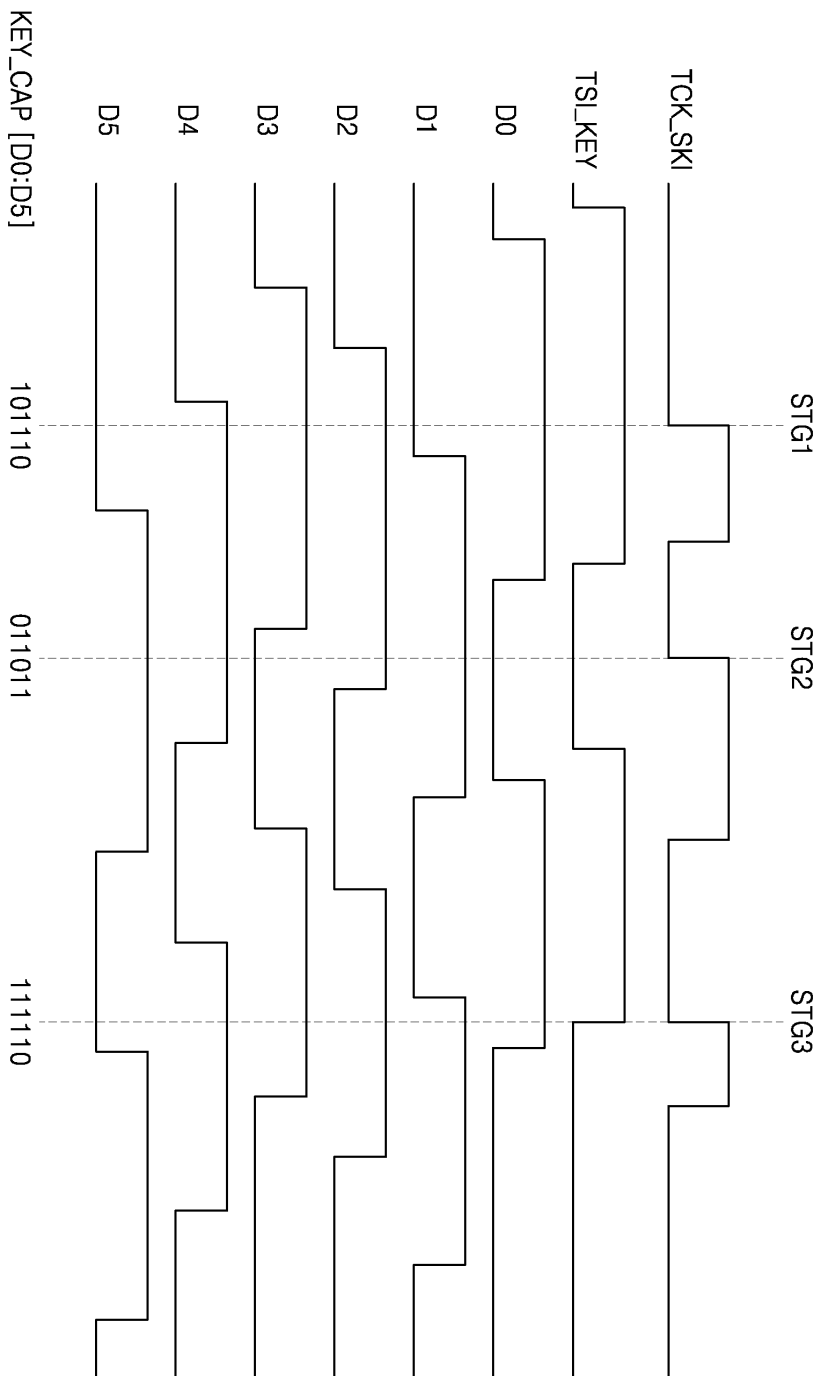
도면3



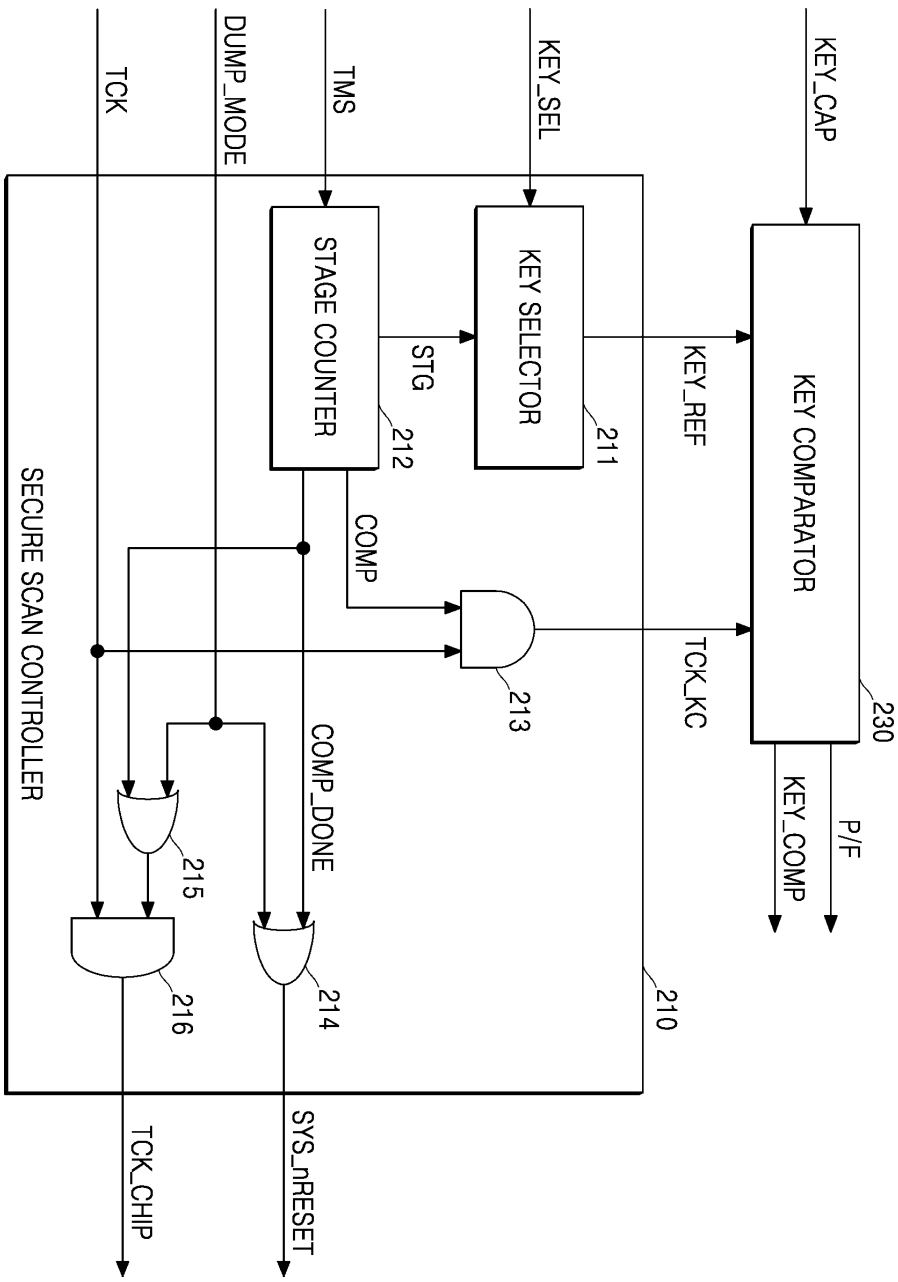
도면4



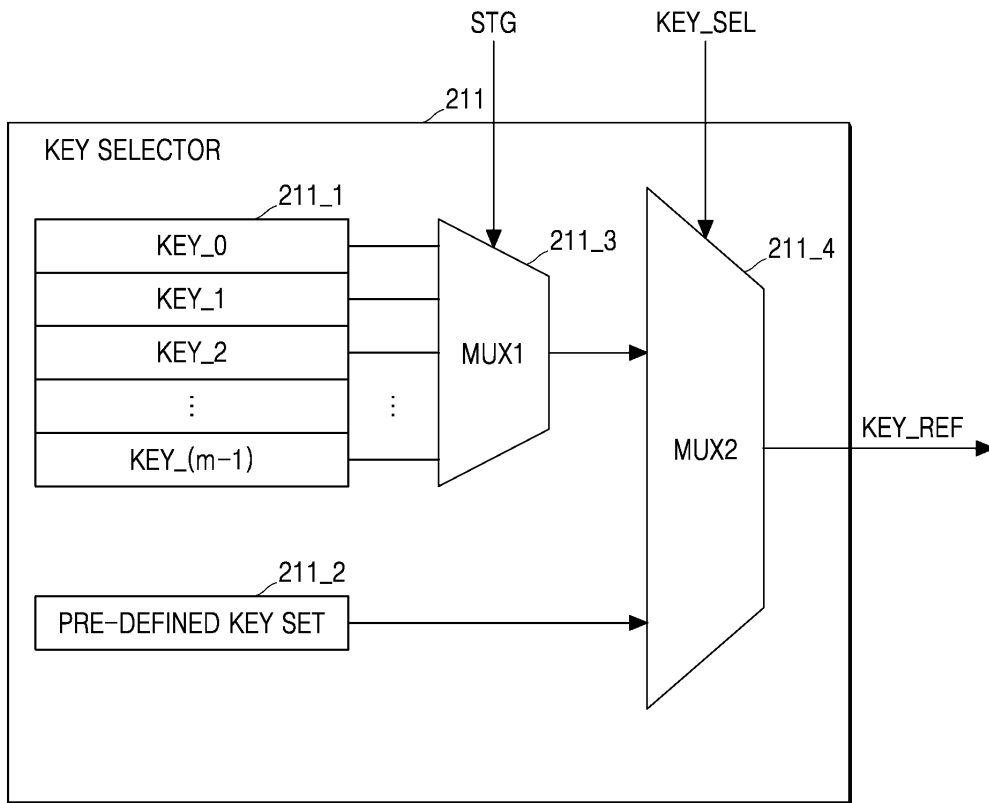
도면5



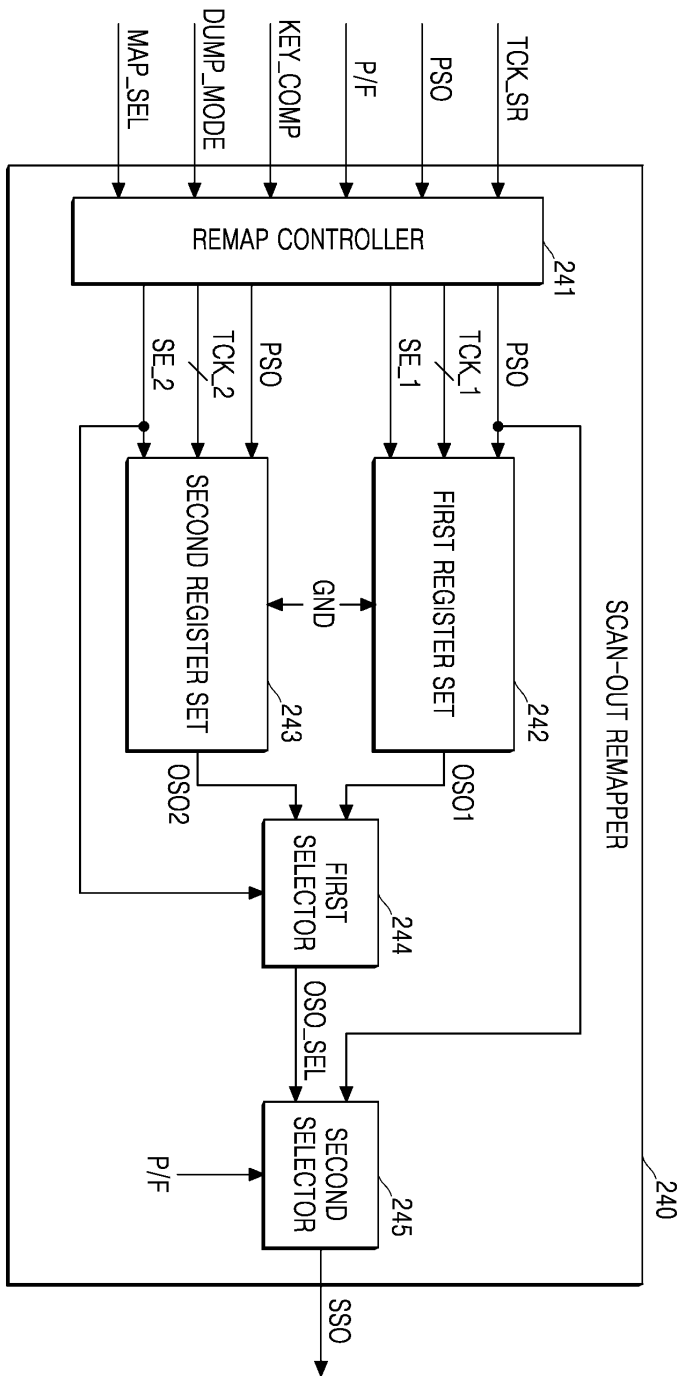
도면6



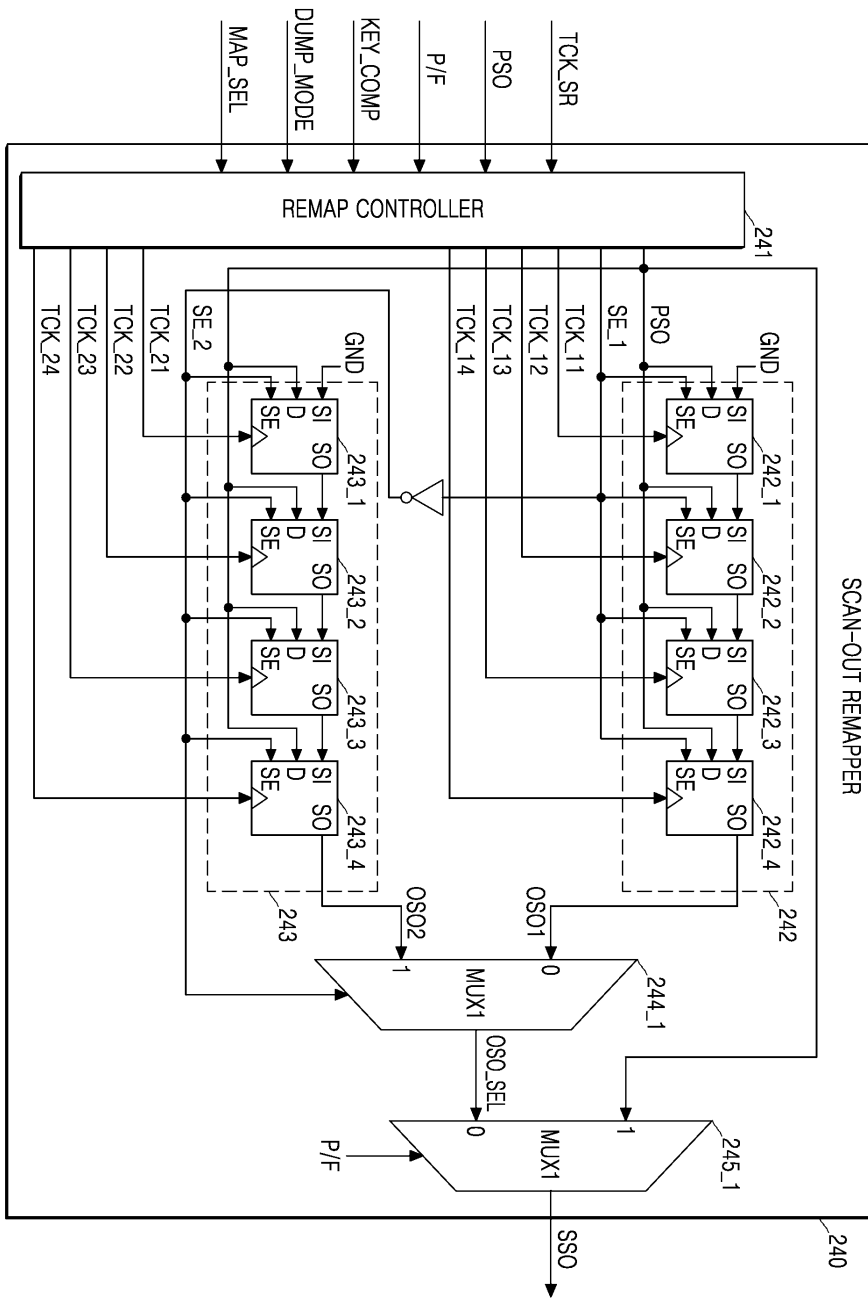
도면7



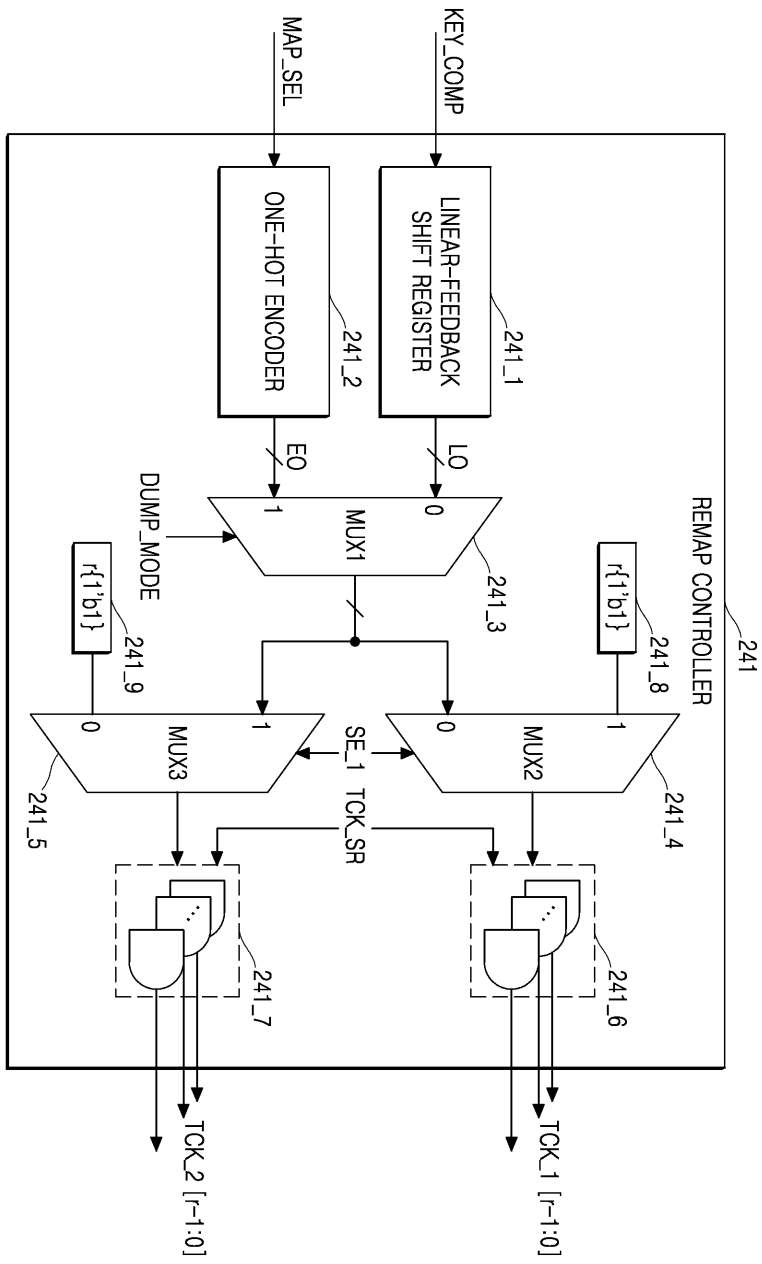
도면8



도면9



도면10



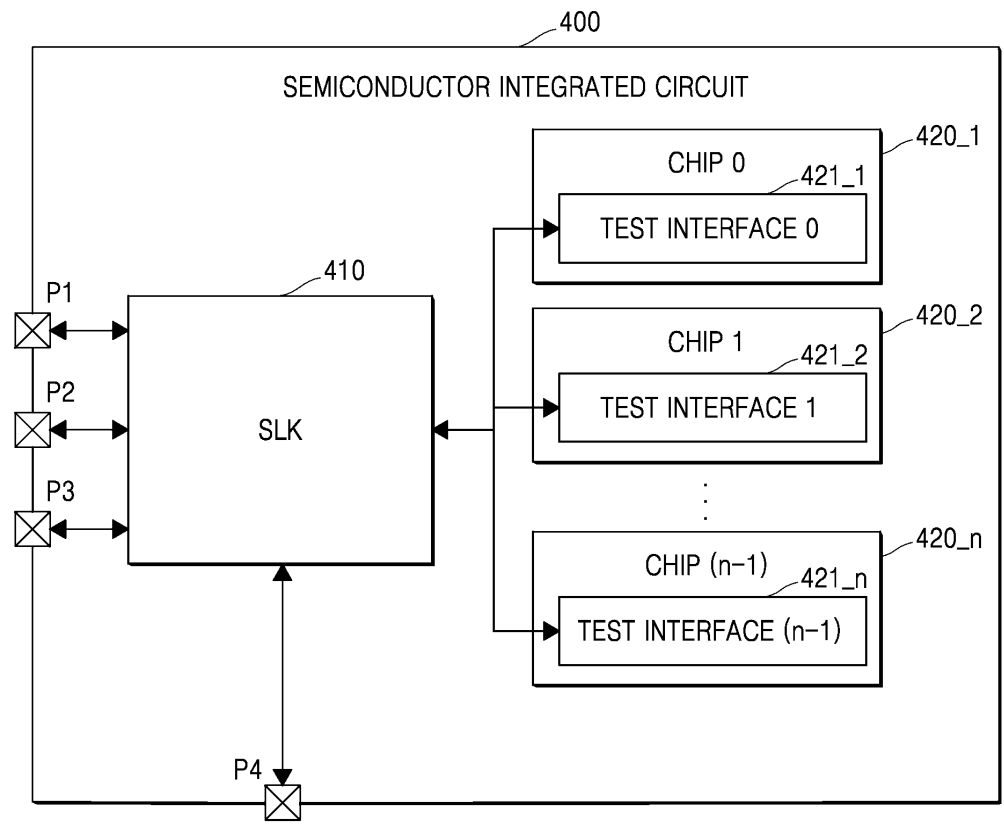
도면11

Cycle count	PSO	LO	SE_1	TCK_14	TCK_13	TCK_12	TCK_11	SR_A [3:0]	SE_2	TCK_24	TCK_23	TCK_22	TCK_21	SR_B [3:0]	SSO
0	p0	0011	0	-	-	En	En	X, X, 0, 0	1	En	En	En	En	4'b0	0
1	p1	0001	0	-	-	En	En	X, X,p0,p1	1	En	En	En	En	4'b0	0
2	p2	1000	0	En	-	-	-	p0, X,p0,p1	1	En	En	En	En	4'b0	0
3	p3	0100	0	-	En	-	-	p2,p3,p0,p1	1	En	En	En	En	4'b0	0
4	p4	0010	1	En	En	En	En	p3,p0,p0,0	0	-	-	En	-	0,0,p4,0	p2
5	p5	1001	1	En	En	En	En	p0,p1,0,0	0	En	-	-	En	p5,0,p4,p5	p3
6	p6	1100	1	En	En	En	En	p1,0,0,0	0	En	En	-	-	p6,p6,p4,p5	p0
7	p7	0110	1	En	En	En	En	4'b0	0	-	En	En	-	p6,p7,p7,p5	p1
8	p8	1011	0	En	-	En	En	p8,0,p8,p8	1	En	En	En	En	p7,p7,p5,0	p6
9	p9	0101	0	-	En	-	En	p8,p9,p8,p9	1	En	En	En	En	p7,p5,0,0	p7
10	pa	1010	0	En	-	En	-	pa,p9,pa,p9	1	En	En	En	En	p5,0,0,0	p7
11	pb	1101	0	En	En	-	En	pb,pb,pa,pb	1	En	En	En	En	4'b0	p5

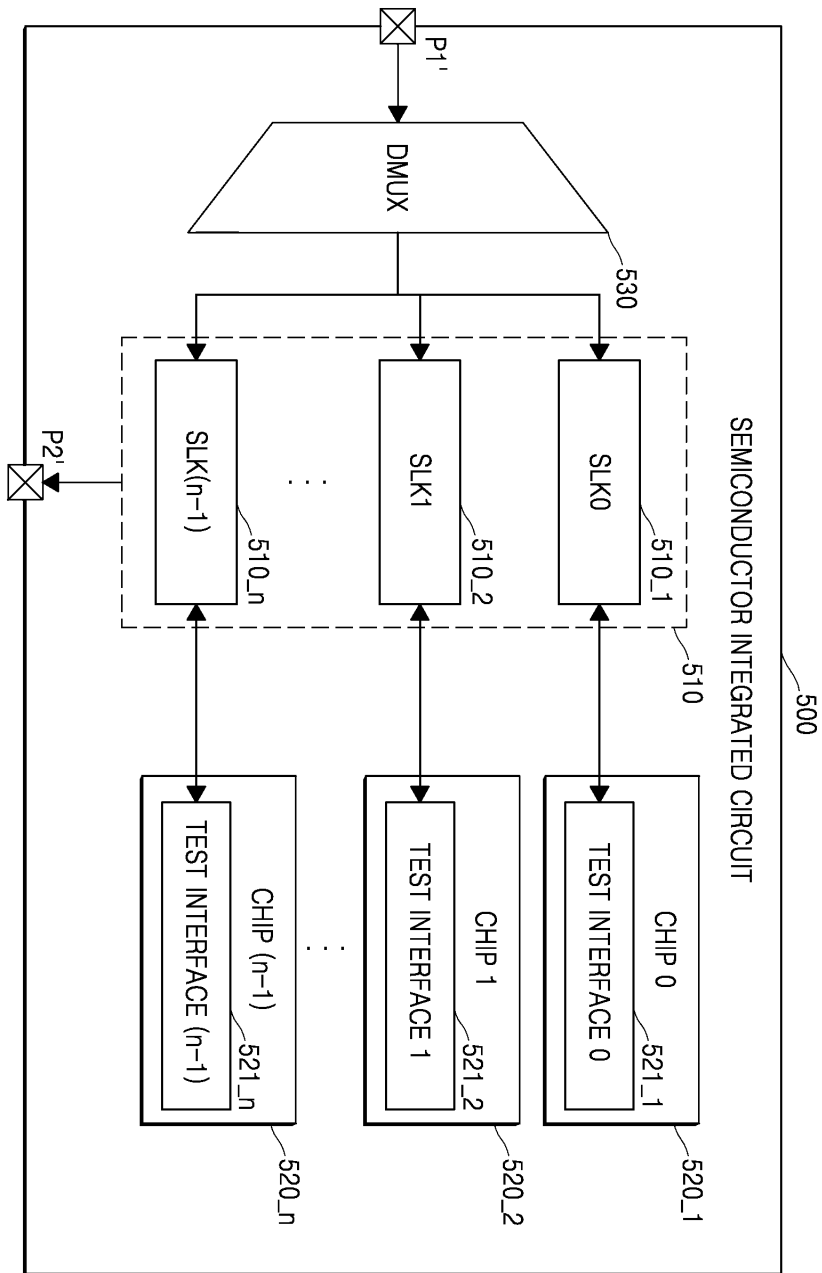
도면12

Cycle count	PS0	MAP_SEL	SE_1	TCK_14	TCK_13	TCK_12	TCK_11	SR_A [3:0]	SE_2	TCK_24	TCK_23	TCK_22	TCK_21	SR_B [3:0]	SSO
0	p0	$\left. \begin{array}{l} 2'b00, \\ 2'b10, \\ 2'b11, \\ 2'b01, \end{array} \right\}$	0	En	-	-	-	p0, 0, 0, 0	1	En	En	En	En	4'b0	0
1	p1		0	-	-	-	En	p0, 0, 0, p1	1	En	En	En	En	4'b0	0
2	p2		0	-	En	-	-	p0, p2, 0, p1	1	En	En	En	En	4'b0	0
3	p3		0	-	-	En	-	p0, p2, p3, p1	1	En	En	En	En	4'b0	0
4	p4		1	En	En	En	En	p2, p3, p1, 0	0	En	-	-	-	p4, 0, 0, 0	p0
5	p5		1	En	En	En	En	p3, p1, 0, 0	0	-	-	-	En	p4, 0, 0, p5	p2
6	p6		1	En	En	En	En	p1, 0, 0, 0	0	-	En	-	-	p4, p6, 0, p5	p3
7	p7	1	En	En	En	En	4'b0	0	-	-	En	-	p4, p6, p7, p5	p1	

도면13



도면14



도면15

