(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년01월02일
(11) 등록번호 10-2620784
(24) 등록일자 2023년12월28일

(51) 국제특허분류(Int. Cl.)
G06F 21/84 (2013.01) *G06F 21/71* (2013.01)
G06F 7/58 (2006.01)
(52) CPC특허분류
G06F 21/84 (2013.01)
G06F 21/71 (2013.01)
(21) 출원번호 10-2021-0189267
(22) 출원일자 2021년12월28일
심사청구일자 2021년12월28일
(65) 공개번호 10-2023-0099867
(43) 공개일자 2023년07월05일
(56) 선행기술조사문헌
JP2011107930 A*
Hadi Mardani Kamali 외 3인, 'SCRAMBLE: The State, Connectivity and Routing Augmentation Model for Building Logic Encryption', 2020 IEEE Computer Society Annual Symposium on VLSI, 2020.08.04.*
KR1020150079880 A
JP2009505059 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
강성호
서울특별시 마포구 양화로 45, 101동 2102호(서교동, 메세나폴리스)
장석준
서울특별시 서대문구 연희로 82, B동 201호(연희동)
(74) 대리인
특허법인(유한)아이시스

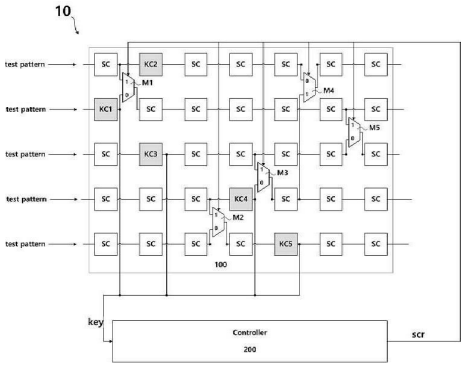
전체 청구항 수 : 총 11 항 심사관 : 구대성

(54) 발명의 명칭 **보안 스캔 체인 회로 및 스캔 체인 회로 보안 방법**

(57) 요 약

본 실시예에 의한 보안 스캔 체인 회로는: 각각 캐스케이드로 연결된 스캔 셀과 하나 이상의 키 셀(key cell)을 포함하는 복수의 스캔 체인들; 서로 다른 스캔 체인들 사이에서 데이터 경로를 스크램블하는 스크램블 다중화기(scramble MUX)들 및 골든 키(golden key)를 저장하고, 상기 키 셀이 제공하는 키와 상기 골든 키를 비교하고, 상기 비교 결과에 따라 상기 스크램블 다중화기(scramble MUX)들을 제어하되, 시프트 인 데이터는 정상 데이터 경로를 따라 전파하고, 캡쳐 데이터는 스크램블된 경로를 따라 전파하도록 제어하는 제어부를 포함한다. 본 실시예에 의하면, 인가되지 않은 사용자가 캡쳐된 데이터를 확인할 수 없어 높은 보안성을 가진다. 또한, 인가되지 않은 사용자가 테스트 패턴을 시프트 인하는 경우에는 경로 스크램블이 이루어지지 않도록 하여 보안 동작을 확인할 수 없어 높은 안전성을 가진다는 장점이 제공된다.

대 표 도



(52) CPC특허분류
G06F 7/58 (2018.05)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711131125
과제번호	2019R1A2C3011079
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	중견연구자지원사업
연구과제명	인-메모리 컴퓨팅의 로버스트니스 향상을 위한 반도체 설계 기술
기 여 율	1/1
과제수행기관명	연세대학교
연구기간	2021.03.01 ~ 2022.02.28

명 세 서

청구범위

청구항 1

각각 캐스케이드로 연결된 스캔 셀과 하나 이상의 키 셀(key cell)을 포함하는 복수의 스캔 체인들;

서로 다른 스캔 체인들 사이에서 데이터 경로를 스크램블하는 스크램블 다중화기(scramble MUX)들 및

골든 키(golden key)를 저장하고, 상기 키 셀이 제공하는 키와 상기 골든 키를 비교하고, 상기 비교 결과에 따라 상기 스크램블 다중화기(scramble MUX)들을 제어하되, 시프트 인 데이터는 정상 데이터 경로를 따라 전파하고, 캡쳐 데이터는 스크램블된 경로를 따라 전파하도록 제어하는 제어부를 포함하고,

상기 제어부는,

상기 키 셀이 제공하는 키를 제공받고, 난수를 생성하는 난수 생성부와,

상기 스크램블 다중화기들이 순차적으로 스크램블 해제되도록 순차 해제 코드를 생성하는 해제 코드 생성부 및

상기 난수와 상기 순차 해제 코드를 논리 연산하여 고장 주입 코드를 형성하는 로직부를 포함하는 보안 스캔 체인 회로.

청구항 2

제1항에 있어서,

상기 스크램블 다중화기는,

제1 스캔 체인에 포함된 스캔 셀과 제2 스캔 체인에 포함된 스캔셀로부터 입력 받고,

상기 제1 스캔 체인에 포함된 스캔 셀에서 제공된 입력을 상기 제2 스캔 체인에 포함된 스캔 셀에 출력하여 상기 데이터 경로를 스크램블하는 보안 스캔 체인 회로.

청구항 3

제1항에 있어서,

상기 보안 스캔 체인 회로는,

상기 스캔 체인에 테스트 패턴을 시프트 인(shift in) 할 때 상기 데이터 경로의 스크램블을 수행하지 않고,

테스트 대상 회로로부터 캡쳐된 데이터를 시프트 아웃(shift out) 할 때 상기 데이터 경로의 스크램블을 수행하는 보안 스캔 체인 회로.

청구항 4

제1항에 있어서,

상기 제어부는,

클록 신호와, 스캔 활성화 신호를 제공받고,

캡쳐 클록과 시프트 클록을 형성하는 클록 형성부를 포함하는 보안 스캔 체인 회로.

청구항 5

제4항에 있어서,

상기 제어부는,

상기 골든키를 저장하고, 상기 키 셀이 제공하는 키를 비교하되,

상기 캡쳐 클록에 따라 상기 골든 키와 상기 키 셀이 제공하는 키를 비트별로 비교하는 키 비교부를 포함하는

보안 스캔 체인 회로.

청구항 6

삭제

청구항 7

제1항에 있어서,

상기 난수 생성부는 리니어 피드백 시프트 레지스터(LFSR, linear feedback shift register)이고,

상기 해제 코드 생성부는 스캔 데이터가 입력되는 측으로부터 순차적으로 상기 스크램블 다중화기가 스크램블 해제되도록 스크램블 해제 코드를 생성하는 카운터인 보안 스캔 체인 회로.

청구항 8

제1항에 있어서,

상기 해제 코드 생성부는,

상기 순차적으로 스크램블 해제되는 상기 스크램블 다중화기들의 위치를 저장하는 보안 스캔 체인 회로.

청구항 9

제1항에 있어서,

상기 제어부는,

상기 로직부의 출력 값과

상기 스크램블 다중화기들의 스크램블을 해제하는 값이 입력되는 다중화기를 더 포함하며,

상기 다중화기는 상기 비교 결과에 따라 입력된 값 중 어느 하나를 출력하는 보안 스캔 체인 회로.

청구항 10

각각 캐스케이드로 연결된 스캔 셀과 하나 이상의 키 셀(key cell)을 포함하는 복수의 스캔 체인들로부터 키를 제공받는 단계와,

저장된 골든 키(golden key)와 상기 키 셀이 제공하는 키를 비교하는 단계와,

상기 비교 결과에 따라 시프트 인 데이터는 정상 데이터 경로를 따라 전파하고, 캡처 데이터는 스크램블된 경로를 따라 전파하는 단계를 포함하고,

상기 캡처 데이터가 스크램블된 경로를 따라 전파하는 단계는 스크램블 다중화기에 의하여 이루어지며,

상기 스크램블 다중화기는,

제1 스캔 체인과 제2 스캔 체인에 포함된 스캔 셀들로부터 각각 입력을 제공받고,

상기 비교 결과에 따라 상기 제1 스캔 체인으로부터 제공된 입력을 상기 제2 스캔 체인에 출력하여 상기 데이터 경로를 스크램블하며,

상기 스크램블은,

상기 키 셀이 제공한 키로부터 난수를 형성하고, 상기 스크램블 다중화기들이 순차적으로 스크램블 해제되도록 순차 해제 코드를 생성하는 단계와,

상기 난수와 상기 순차 해제 코드를 로직 연산하여 고장 주입 코드를 형성하는 단계 및

상기 고장 주입 코드에 따라 상기 순차적으로 상기 스크램블 다중화기를 제어하여 수행하는 스캔 체인 회로 보안 방법.

청구항 11

삭제

청구항 12

삭제

청구항 13

제10항에 있어서,

상기 키를 제공받는 단계는,

상기 스캔 체인에 테스트 패턴을 시프트 인(shift in)이 완료된 후 수행되는 스캔 체인 회로 보안 방법.

청구항 14

제10항에 있어서,

상기 순차 해제 코드를 생성하는 단계는,

스캔 클록을 계수하여 저장된 상기 스크램블 다중화기의 위치와 비교하는 단계와,

서로 일치하면 상기 스크램블 다중화기가 스크램블 해제되도록 상기 순차 해제 코드를 형성하는 스캔 체인 회로 보안 방법.

발명의 설명

기 술 분 야

[0001] 본 기술은 보안 스캔 체인 회로 및 스캔 체인 회로 보안 방법과 관련된다.

배 경 기 술

[0002] 스캔 체인은 테스트 대상 소자를 간결하고, 신속하게 테스트할 수 있다는 장점이 있어 널리 사용되고 있다. 그러나, 스캔 체인은 테스트 대상 소자에 저장된 기밀 사항들을 획득할 수 있는 백도어(back-door)로 기능할 수 있어 그 보안이 요청된다.

[0003] 스캔 체인 내 저장되어 있는 데이터 추출을 막기 위한 보안 키 방식의 기존 기술들의 경우 보안 키를 활용하여 다양한 방식으로 스캔 데이터 출력을 보호하고 있으나, 기본적인 테스트 패턴을 이용한 단순 패턴 시프팅 동작을 통해서도 보안 동작이 이루어 지고 있음을 쉽게 파악할 수 있다.

발명의 내용

해결하려는 과제

[0004] 특정 입력 패턴에 대하여 보안 동작이 이루어 지고 있음이 파악되는 것은 보안 키 추론의 단서가 될 수 있어, 다수의 칩에 대한 많은 테스트 패턴 출력 결과를 분석하면 회로의 보안 기능을 상실할 수 있다.

[0005] 본 기술로 해결하고자 하는 과제 중 하나는, 테스트 대상 회로에서 형성되는 데이터를 파악하는 것을 곤란하게 하며, 나아가 보안 동작이 이루어지고 있는지 파악하는 것도 파악할 수 없도록 하여 보안성을 더욱 강화하기 위한 것이다. 이로부터

과제의 해결 수단

[0006] 본 실시예에 의한 보안 스캔 체인 회로는: 각각 캐스케이드로 연결된 스캔 셀과 하나 이상의 키 셀(key cell)을 포함하는 복수의 스캔 체인들; 서로 다른 스캔 체인들 사이에서 데이터 경로를 스크램블하는 스크램블 다중화기(scramble MUX)들 및 골든 키(golden key)를 저장하고, 상기 키 셀이 제공하는 키와 상기 골든 키를 비교하고, 상기 비교 결과에 따라 상기 스크램블 다중화기(scramble MUX)들을 제어하되, 시프트 인 데이터는 정상 데이터 경로를 따라 전파하고, 캡쳐 데이터는 스크램블된 경로를 따라 전파하도록 제어하는 제어부를 포함한다.

[0007] 본 실시예의 어느 한 측면에 의하면, 상기 스크램블 다중화기는, 제1 스캔 체인에 포함된 스캔 셀과 제2 스캔 체인에 포함된 스캔셀로부터 입력 받고, 상기 제1 스캔 체인에 포함된 스캔 셀에서 제공된 입력을 상기 제2 스캔 체인에 포함된 스캔 셀에 출력하여 상기 데이터 경로를 스크램블한다.

[0008] 본 실시예의 어느 한 측면에 의하면, 상기 보안 스캔 체인 회로는, 상기 스캔 체인에 테스트 패턴을 시프트 인(shift in) 할 때 상기 데이터 경로의 스크램블을 수행하지 않고, 상기 테스트 대상 회로로부터 캡처된 데이터를 시프트 아웃(shift out) 할 때 상기 데이터 경로의 스크램블을 수행한다.

[0009] 본 실시예의 어느 한 측면에 의하면, 상기 제어부는, 클록 신호와, 스캔 활성화 신호를 제공받고, 캡처 클록과 시프트 클록을 형성하는 클록 형성부를 포함한다.

[0010] 본 실시예의 어느 한 측면에 의하면, 상기 제어부는, 상기 골든키를 저장하고, 상기 키 셀이 제공하는 키를 비교하되, 상기 캡처 클록에 따라 상기 골든 키와 상기 키 셀이 제공하는 키를 비트별로 비교하는 키 비교부를 포함한다.

[0011] 본 실시예의 어느 한 측면에 의하면, 상기 제어부는, 상기 키 셀이 제공하는 키를 제공받고, 난수를 생성하는 난수 생성부와, 상기 스크램블 다중화기들이 순차적으로 스크램블 해제되도록 순차 해제 코드를 생성하는 해제 코드 생성부 및 상기 유사 난수와 상기 순차 해제 코드를 논리 연산하여 고장 주입 코드를 형성하는 로직부를 포함한다.

[0012] 본 실시예의 어느 한 측면에 의하면, 상기 난수 생성부는 리니어 피드백 시프트 레지스터(LFSR, linear feedback shift register)이고, 상기 해제 코드 생성부는 스캔 데이터가 입력되는 측으로부터 순차적으로 상기 스크램블 다중화기가 스크램블 해제되도록 스크램블 해제 코드를 생성하는 카운터이다.

[0013] 본 실시예의 어느 한 측면에 의하면, 상기 해제 코드 생성부는, 상기 순차적으로 스크램블 해제되는 상기 스크램블 다중화기들의 위치를 저장한다.

[0014] 본 실시예의 어느 한 측면에 의하면, 상기 제어부는, 상기 로직부의 출력 값과 상기 스크램블 다중화기들의 스크램블을 해제하는 값이 입력되는 다중화기를 더 포함하며, 상기 다중화기는 상기 비교 결과에 따라 입력된 값 중 어느 하나를 출력한다.

[0015] 본 실시예에 의한 스캔 체인 회로의 보안 방법은 각각 캐스케이드로 연결된 스캔 셀과 하나 이상의 키 셀(key cell)을 포함하는 복수의 스캔 체인들로부터 키를 제공받는 단계와, 저장된 골든 키(golden key)와 상기 키 셀이 제공하는 키를 비교하는 단계와, 상기 비교 결과에 따라 시프트 인 데이터는 정상 데이터 경로를 따라 전파하고, 캡처 데이터는 스크램블된 경로를 따라 전파하는 단계를 포함한다.

[0016] 본 실시예의 어느 한 측면에 의하면, 상기 캡처 데이터가 스크램블된 경로를 따라 전파하는 단계는 스크램블 다중화기에 의하여 이루어지며, 상기 스크램블 다중화기는, 제1 스캔 체인과 제2 스캔 체인에 포함된 스캔 셀들로부터 각각 입력을 제공받고, 상기 비교 결과에 따라 상기 제1 스캔 체인으로부터 제공된 입력을 상기 제2 스캔 체인에 출력하여 상기 데이터 경로를 스크램블한다.

[0017] 본 실시예의 어느 한 측면에 의하면, 상기 스크램블하는 단계는, 상기 키 셀이 제공한 키로부터 난수를 형성하고, 상기 스크램블 다중화기들이 순차적으로 스크램블 해제되도록 순차 해제 코드를 생성하는 단계와, 상기 난수와 상기 순차 해제 코드를 로직 연산하여 고장 주입 코드를 형성하는 단계 및 상기 고장 주입 코드에 따라 상기 순차적으로 상기 스크램블 다중화기를 제어하여 수행한다.

[0018] 본 실시예의 어느 한 측면에 의하면, 상기 키를 제공받는 단계는, 상기 스캔 체인에 테스트 패턴을 시프트 인(shift in)이 완료된 후 수행된다.

[0019] 본 실시예의 어느 한 측면에 의하면, 상기 순차 해제 코드를 생성하는 단계는, 스캔 클록을 계수하여 저장된 상기 스크램블 다중화기의 위치와 비교하는 단계와, 서로 일치하면 상기 스크램블 다중화기가 스크램블 해제되도록 상기 순차 해제 코드를 형성한다.

발명의 효과

[0020] 본 실시예에 의하면, 인가되지 않은 사용자가 캡처된 데이터를 확인할 수 없어 높은 보안성을 가진다. 또한, 인가되지 않은 사용자가 테스트 패턴을 시프트 인하는 경우에는 경로 스크램블이 이루어지지 않도록 하여 보안 동작을 확인할 수 없어 높은 안전성을 가진다는 장점이 제공된다.

도면의 간단한 설명

[0021] 도 1은 본 실시예에 의한 보안 스캔 체인 회로의 개요를 도시한 도면이다.

도 2는 본 실시예에 의한 스캔 체인 회로의 보안 방법의 개요를 도시한 순서도이다.

도 3은 본 실시예의 제어부 개요를 도시한 도면이다.

도 4는 해제 코드 생성부의 동작을 설명하기 위한 도면이다.

도 5는 본 실시예에 의한 보안 스캔 체인 회로의 동작을 설명을 위한 개요도이다.

도 6은 스캔 클록(s_clk)이 세 주기 제공된 경우 보안 스캔 체인 회로의 동작을 설명을 위한 개요도이다.

도 7은 시프트 인되는 데이터가 스캔 체인의 마지막 스캔 셀 까지 도달한 상태를 예시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하에서는 첨부된 도면들을 참조하여 본 실시예에 의한 보안 스캔 체인 회로(10)를 설명한다. 도 1은 본 실시예에 의한 보안 스캔 체인 회로(10)의 개요를 도시한 도면이다. 도 1을 참조하면, 본 실시예에 의한 보안 스캔 체인 회로(10)는 캐스케이드로 연결된 스캔 셀(SC)과 하나 이상의 키 셀(key cell, KC)을 포함하는 복수의 스캔 체인들(100)과, 서로 다른 스캔 체인들 사이에서 데이터 경로를 스크램블하는 스크램블 다중화기(scramble MUX, M1, M2, M3, M4, M5)들 및 골든 키(golden key)를 저장하고, 상기 키 셀이 제공하는 키와 상기 골든 키를 비교하고, 상기 비교 결과에 따라 상기 스크램블 다중화기(scramble MUX)들을 제어하는 제어부(200)를 포함한다.

[0023] 도 2는 본 실시예에 의한 스캔 체인 회로의 보안 방법의 개요를 도시한 순서도이다. 도 2를 참조하면, 본 실시예에 의한 스캔 체인 회로의 보안 방법은 각각 캐스케이드로 연결된 스캔 셀과 하나 이상의 키 셀(key cell)을 포함하는 복수의 스캔 체인들로부터 키를 제공받는 단계(S100)와, 저장된 골든 키(golden key)와 상기 키 셀이 제공하는 키를 비교하는 단계(S200)와, 상기 비교 결과에 따라 스크램블 다중화기(scramble MUX)들을 제어하여 상기 스캔 체인의 데이터 경로를 스크램블하는 단계(S300)를 포함한다.

[0024] 도 1 및 도 2를 참조하면, 스캔 체인(100)을 통하여 테스트 패턴(test pattern)을 입력받는다. 테스트 패턴은 스캔 체인(100)으로 순차적으로 시프트 인(shift in) 된다. 테스트 패턴은 일반적으로 스캔 체인(100)을 통하여 테스트 대상 소자(DUT, device under test, 미도시)에 제공된다. 테스트 대상 소자(DUT)는 입력된 테스트 패턴과 테스트 대상 소자의 내부 회로 및 테스트 대상 소자(DUT)에 발생한 고장에 상응하는 출력을 형성하여 출력한다. 테스트 대상 소자(DUT)가 형성한 출력은 스캔 체인(100)에 의하여 캡쳐(capture)되고, 스캔 체인(100)을 통하여 순차적으로 시프트 아웃(shift out)된다.

[0025] 도 3은 본 실시예의 제어부(200)의 개요를 도시한 도면이다. 도 3을 참조하면, 이하에서는 도 1 내지 도 3을 참조하여 본 실시예에 의한 보안 스캔 체인 회로(10)의 동작을 살펴본다. 스캔 체인(100)은 캐스케이드로 연결된 스캔 셀(SC)들을 포함한다. 스캔 체인(100)을 통해 입력된 테스트 패턴은 순차적으로 스캔 체인을 따라 전파된다. 본 실시예에서, 테스트 패턴은 키 셀들(KC1, KC2, KC3, KC4, KC5)에 제공되는 키를 포함한다. 키 셀들(KC1, KC2, KC3, KC4, KC5)에 제공되는 키들은 통상의 테스트 패턴과 마찬가지로 순차적으로 시프트 인(shift in)되어 목적하는 키 셀들(KC1, KC2, KC3, KC4, KC5)에 제공될 수 있다.

[0026] 일 실시예로, 각각의 키 셀(KC1, KC2, KC3, KC4, KC5)에 미리 정해진 키가 시프트 인되어 제공된 후, 캡쳐 단계에서 테스트 대상 회로(DUT)에서 형성된 데이터를 스캔 체인(100)으로 입력받는다. 또한, 캡쳐 단계에서 키 셀(KC1, KC2, KC3, KC4, KC5)들에 형성된 키는 키 비교부(210)에 제공된다.

[0027] 키 비교부(210)는 키 셀(KC1, KC2, KC3, KC4, KC5)로부터 제공된 키(key)와 미리 정해진 골든 키(golden key)를 비교하고, 비교 결과에 상응하는 비교 신호(comp.)를 출력한다. 키 비교부(210)는 캡쳐 클록(c_clk)을 제공받고, 골든 키와 입력된 키를 순차적으로 비교하여 비교 결과에 상응하는 비교 신호(comp.)를 출력한다. 비교 신호(comp.)는 다중화기(MUX)에 제공되고, 다중화기(MUX)를 제어한다.

[0028] 일 실시예로, 키 비교부(210)가 키 셀(KC1, KC2, KC3, KC4, KC5)로부터 제공된 키(key)와 미리 정해진 골든 키(golden key)를 비교하여 서로 일치하면 논리 로우의 비교 신호(comp.)를 출력한다. 다중화기(MUX)는 비교 신호(comp.)에 상응하는 논리 로우 상태의 고장 주입 신호(FI)를 출력한다.

[0029] 논리 로우의 고장 주입 신호(FI)가 스크램블 다중화기(M1, M2, M3, M4, M5)에 제공됨에 따라 스크램블 다중화기

(M1, M2, M3, M4, M5)들은 캡처된 데이터가 전송되는 경로를 스크램블하지 않는다. 따라서, 각 스캔 체인에 형성된 캡처 데이터는 정상적인 경로를 따라 출력된다.

[0030] 이하에서는 키 셀들(KC1, KC2, KC3, KC4, KC5)로부터 제공된 키(key)와 미리 정해진 골든 키(golden key)가 서로 상이한 경우의 보안 스캔 체인 회로(10)의 동작을 살펴본다. 키 비교부(210)는 저장된 골든 키와 입력된 키(key)가 상이하면 논리 하이 상태의 비교 신호(comp.)를 출력하여 다중화기(MUX)가 고장 주입 신호(FI)를 출력하도록 제어한다.

[0031] 캡처 단계 이후, 테스트 대상 소자(DUT)에 새로운 테스트 패턴을 입력하기 위하여 시프트 인 단계가 수행될 수 있으며, 이때, 스캔 활성화(SE) 신호가 활성화된다. 따라서 캡처 클록(c_clk)은 논리 로우 상태를 유지하고, 클록 비교부(210)에 의하여 비교 신호(comp.)는 논리 하이 상태를 유지한다.

[0032] 스캔 클록(s_clk)이 제공됨에 따라 난수 발생기(240)는 난수(R)를 발생하여 출력한다. 일 실시예로, 키 비교부(210)는 키 셀(KC1, KC2, KC3, KC4, KC5)이 제공한 키(key)를 시드(seed)로 난수 발생기(240)에 제공한다. 난수 발생기(240)는 키 비교부(210)가 출력한 시드(seed)를 난수 발생의 시드로 삼아 난수(R)를 형성하여 출력한다. 일 실시예로, 난수 발생기(240)는 선형 피드백 시프트 레지스터(LFSR, linear feedback shift register)일 수 있다. 또한, 난수 발생기(240)는 스캔 클록(s_clk)이 제공될 때마다 이전에 형성하였던 난수(R)를 시드로 삼아 새로이 난수(R)를 형성하여 출력한다.

[0033] 도 4는 해제 코드 생성부(230)의 동작을 설명하기 위한 도면이다. 도 1 내지 도 4를 참조하면, 해제 코드 생성부(230)는 스크램블 다중화기들(M1, M2, M3, M4, M5)이 순차적으로 스크램블 해제되도록 순차 해제 코드(clr)를 생성한다. 해제 코드 생성부(230)는 스캔 체인(100) 내 스크램블 다중화기(M1, M2, M3, M4, M5)의 위치에 상응하는 값을 저장할 수 있다. 일 예로, 시프트인 된 데이터가 해당 다중화기에 도달하는데 필요한 클록의 개수를 저장할 수 있다. 일 예로, 스크램블 다중화기(M1)의 위치로 1, 스크램블 다중화기(M2)의 위치로 3, 스크램블 다중화기(M3)의 위치로 4의 값을 저장할 수 있다.

[0034] 해제 코드 생성부(230)는 입력된 스캔 클록(s_clk)의 개수가 저장된 값에 상응하면 미리 정해진 비트에서 인접한 비트로 값을 천이하는 카운터일 수 있다. 일 예로, 미리 정해진 비트는 MSB 일 수 있으며, 미리 저장된 회수의 스캔 클록이 제공되면 LSB 측으로 인접한 비트를 논리 하이에서 논리 로우로 천이하여 출력할 수 있다. 다른 예로 미리 정해진 비트는 LSB 일 수 있으며, 미리 저장된 회수의 스캔 클록이 제공되면 MSB 측으로 인접한 비트를 논리 로우에서 논리 하이로 천이하여 출력할 수 있다.

[0035] 해제 코드 생성부(230)는 스캔 클록(s_clk)이 입력된 회수와 저장된 값을 비교한다. 스크램블 다중화기(M1)의 위치와 입력된 스캔 클록(s_clk_)의 주기가 서로 상응하므로, 해제 코드 생성부(230)는 스크램블 다중화기(M1)가 스크램블 해제되도록 순차 해제 코드(clr)를 생성하여 출력한다.

[0036] 도 4로 예시된 실시예에서, 캡처시 이진수 [11111]로 형성된 순차 해제 코드(clr)는 스캔 클록(s_clk)이 한 주기 제공됨에 따라 MSB가 0으로 전환되어 이진수 [01111]로 전환된다. 순차 해제 코드(clr)는 난수(R)와 AND 연산되어 고장 주입 코드(FI)를 형성한다.

[0037] 도 5는 본 실시예에 의한 보안 스캔 체인 회로의 동작을 설명을 위한 개요도이다. 도 5를 참조하면, 고장 주입 코드(FI)의 MSB는 순차 해제 코드(clr)의 MSB가 0으로 형성됨에 따라 반드시 0으로 제한된다. 이와 같이 형성된 고장 주입 코드(FI)의 MSB는 상응하는 위치의 스크램블 다중화기(M1)에 제공된다. 따라서, 캡처 단계 이후 시프트인 되는 데이터들은 스크램블 다중화기(M1)가 데이터 경로를 스크램블 하지 않아 정상적인 경로를 따라 시프트 인 된다.

[0038] 그러나, 고장 주입 코드(FI)의 MSB 이외의 비트가 제공되는 스크램블 다중화기(M2, M3, M4, M5)는 순차 해제 코드(clr)와 난수(R)와의 논리 연산 결과에 따라 동작한다. 도 5로 예시된 실시예에 의하면 스크램블 다중화기(M2, M3, M5)는 논리 하이 상태의 고장 주입 코드(FI)가 제공되므로, 스크램블 다중화기(M2, M3, M5)는 캡처된 데이터가 전송되는 데이터 경로를 스크램블한다. 따라서, 스캔 체인(100)의 외부에서는 테스트 대상 소자(DUT)에서 캡처된 데이터를 파악할 수 없다.

[0039] 도 6은 스캔 클록(s_clk)이 세 주기 제공된 경우 보안 스캔 체인 회로의 동작을 설명을 위한 개요도이다. 도 1 내지 도 6을 참조하면, 스캔 클록(s_clk)이 세 주기 제공된 경우 스크램블 다중화기(M3)의 위치와 입력된 스캔 클록(s_clk_)의 주기가 서로 상응하므로, 해제 코드 생성부(230)는 스크램블 다중화기(M1, M2)가 스크램블 해제되도록 순차 해제 코드(clr) [00111]를 생성하여 출력한다.

[0040] 순차 해제 코드(clr)는 난수(R)와 논리 연산되어 고장 주입 코드(FI)를 형성한다. 고장 주입 코드(FI)의 MSB측 두 비트는 항상 0이므로, 스크램블 다중화기들(M1, M2)는 시프트 인 데이터가 전파되는 경로를 스크램블하지 않는다. 따라서 시프트 인되는 데이터들은 정상적인 경로를 따라 시프트인된다.

[0041] 그러나, MSB 측 두 비트 이외의 고장 주입 코드(FI)가 제공되는 스크램블 다중화기(M3, M4, M5)는 순차 해제 코드(clr)와 난수(R)와의 논리 연산 결과에 따라 동작한다. 도 5로 예시된 실시예에 의하면 스크램블 다중화기(M2, M3, M5)는 논리 하이 상태의 고장 주입 코드(FI)가 제공되므로, 스크램블 다중화기(M3, M4)는 캡처된 데이터가 전송되는 데이터 경로를 스크램블한다.

[0042] 도 7은 시프트 인되는 데이터가 스캔 체인의 마지막 스캔 셀 까지 도달한 상태를 예시한 도면이다. 도 7을 참조하면, 해제 코드 생성부(230)가 생성한 순차 해제 코드(clr)는 [00000]으로 형성된다. 따라서, 난수(R)와 논리 연산을 수행하여도 모두 0으로 형성되므로 스크램블 다중화기(M1, M2, M3, M4, M5)는 데이터 전송 경로를 스크램블하지 않고, 모두 정상적인 경로를 따라 시프트 인되는 데이터를 전송한다.

[0043] 또한, 캡처된 데이터는 난수(R)와 순차 해제 코드(clr)와의 논리 연산에 의하여 형성된 고장 주입 코드에 따라 제어되는 스크램블 다중화기(M1, M2, M3, M4, M5)에 의하여 스크램블된 데이터 경로를 따라 전파된다. 따라서, 스캔 체인 회로의 외부에서 테스트 대상 회로에 저장된 기밀 데이터, 테스트 대상 회로의 주요한 구성을 파악할 수 없다.

[0045] 본 발명에 대한 이해를 돕기 위하여 도면에 도시된 실시 예를 참고로 설명되었으나, 이는 실시를 위한 실시예로, 예시적인 것에 불과하며, 당해 분야에서 통상적 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위에 의해 정해져야 할 것이다.

부호의 설명

[0046] 10: 보안 스캔 체인 회로

100: 스캔 체인

M1, M2, M3, M4, M5: 스크램블 다중화기

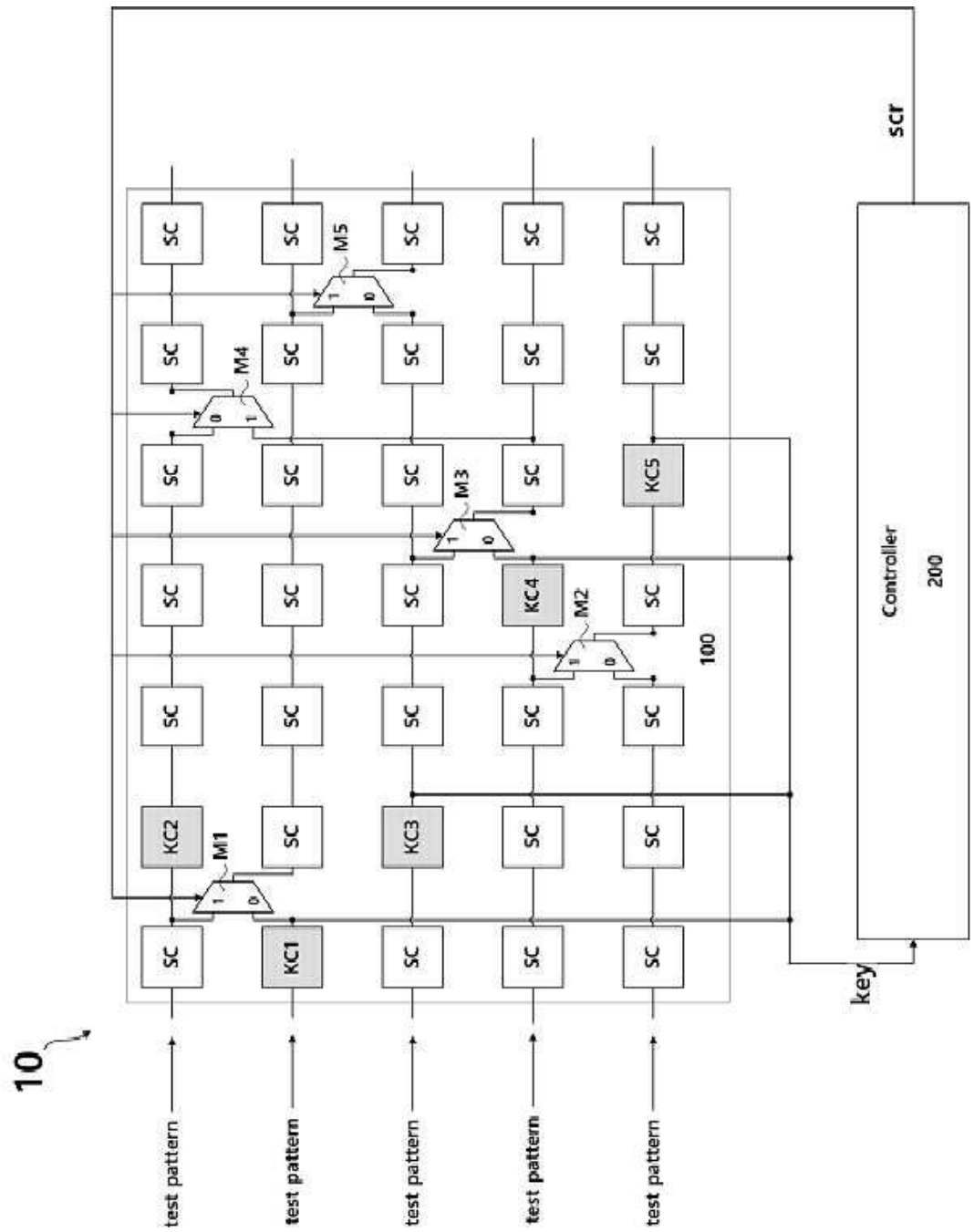
200: 제어부 210: 키 비교부

220: 클록 형성부 230: 해제 코드 생성부

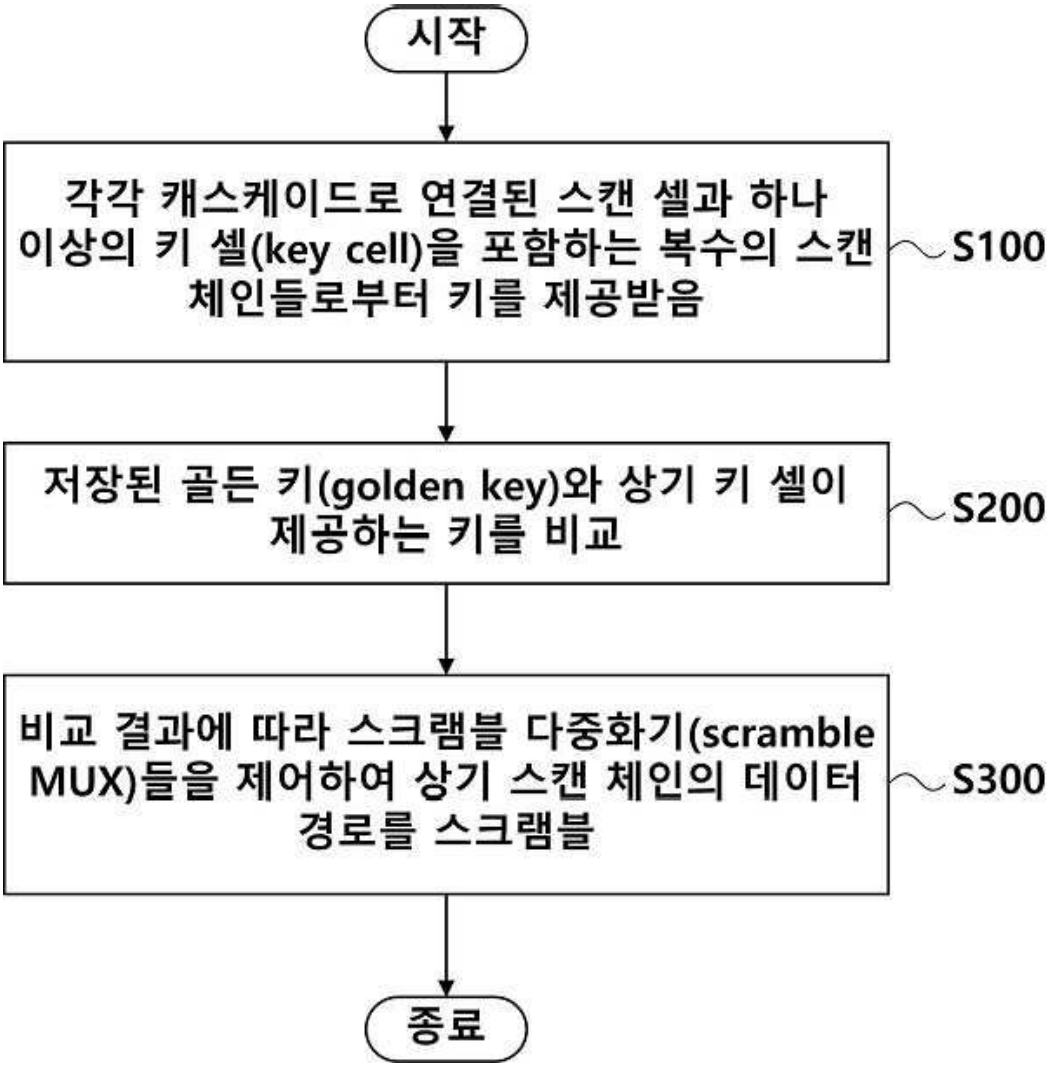
240: 난수 발생기

도면

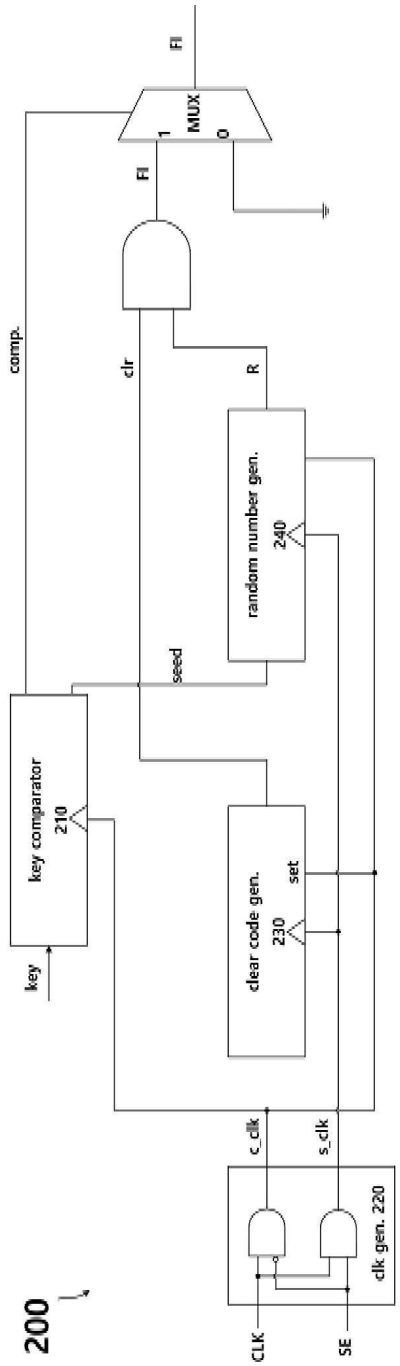
도면1


10
test pattern
test pattern
test pattern
test pattern
test pattern
SC
KC1
KC2
KC3
KC4
KC5
M1
M2
M3
M4
M5
100
Controller
200
scr
key

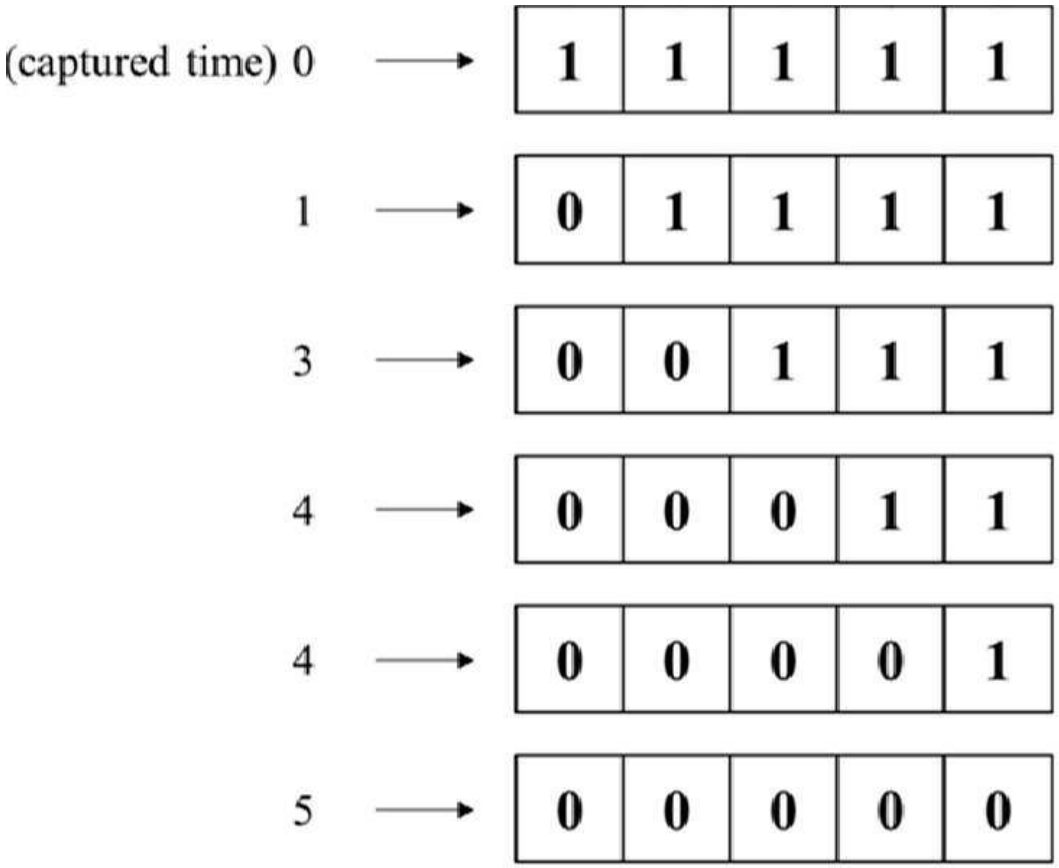
도면2


시작
각각 캐스케이드로 연결된 스캔 셀과 하나 이상의 키 셀(key cell)을 포함하는 복수의 스캔 체인들로부터 키를 제공받음
S100
저장된 골든 키(golden key)와 상기 키 셀이 제공하는 키를 비교
S200
비교 결과에 따라 스크램블 다중화기(scramble MUX)들을 제어하여 상기 스캔 체인의 데이터 경로를 스크램블
S300
종료

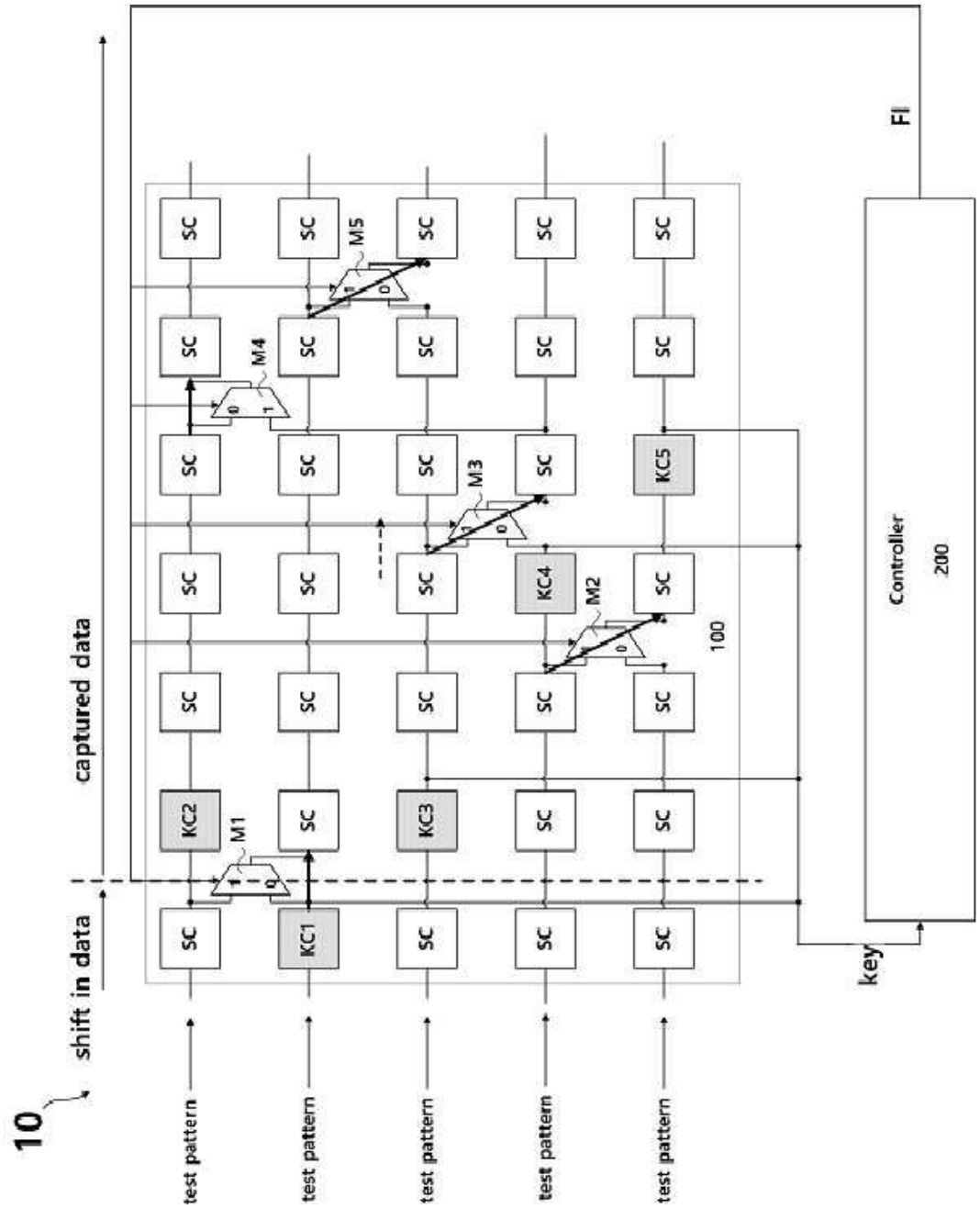
도면3


FI
MUX
1
0
FI
comp.
clr
R
random number gen.
240
seed
key comparator
210
key
clear code gen.
230
set
c_clk
s_clk
clk gen. 220
CLK
SE
200

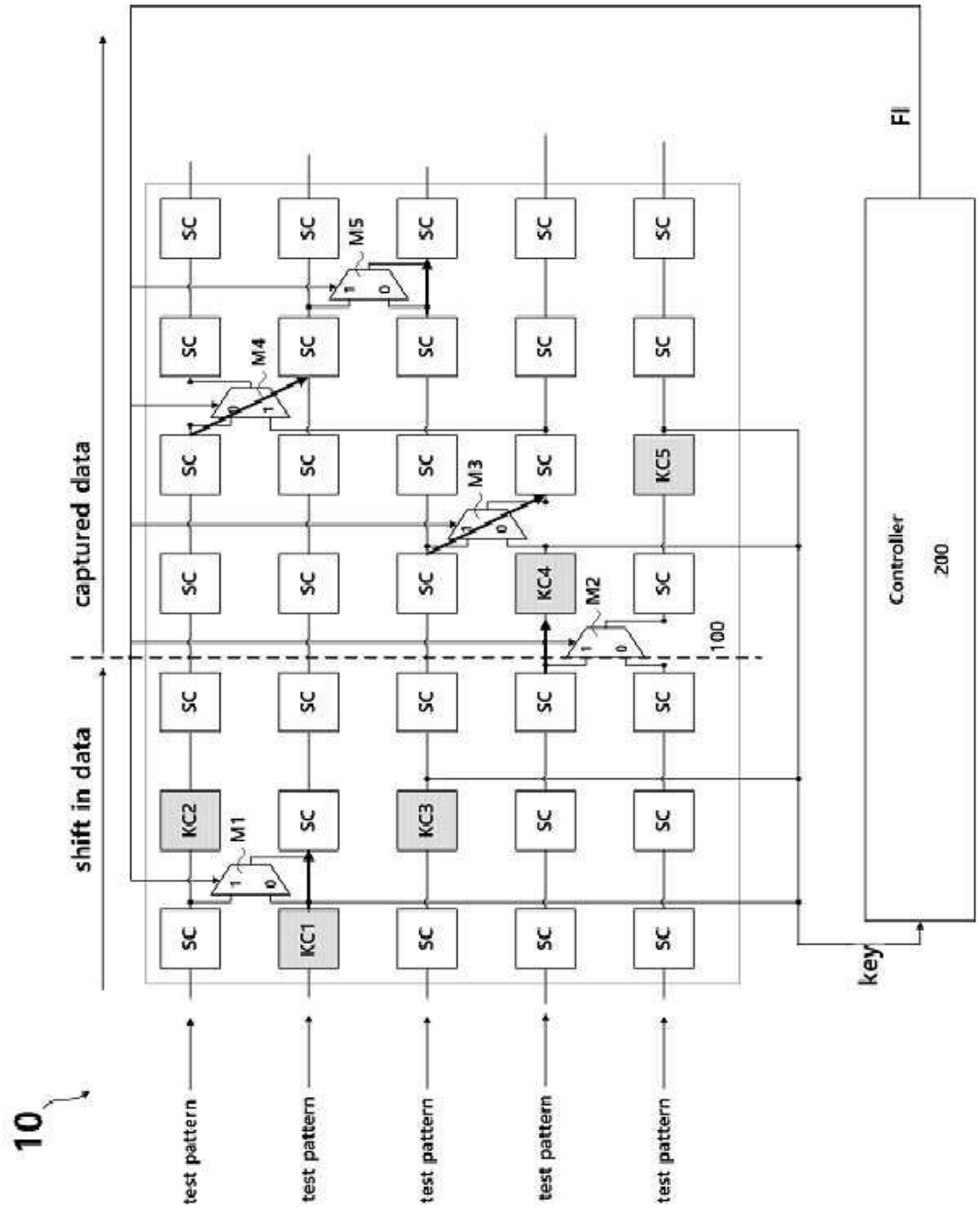
도면4



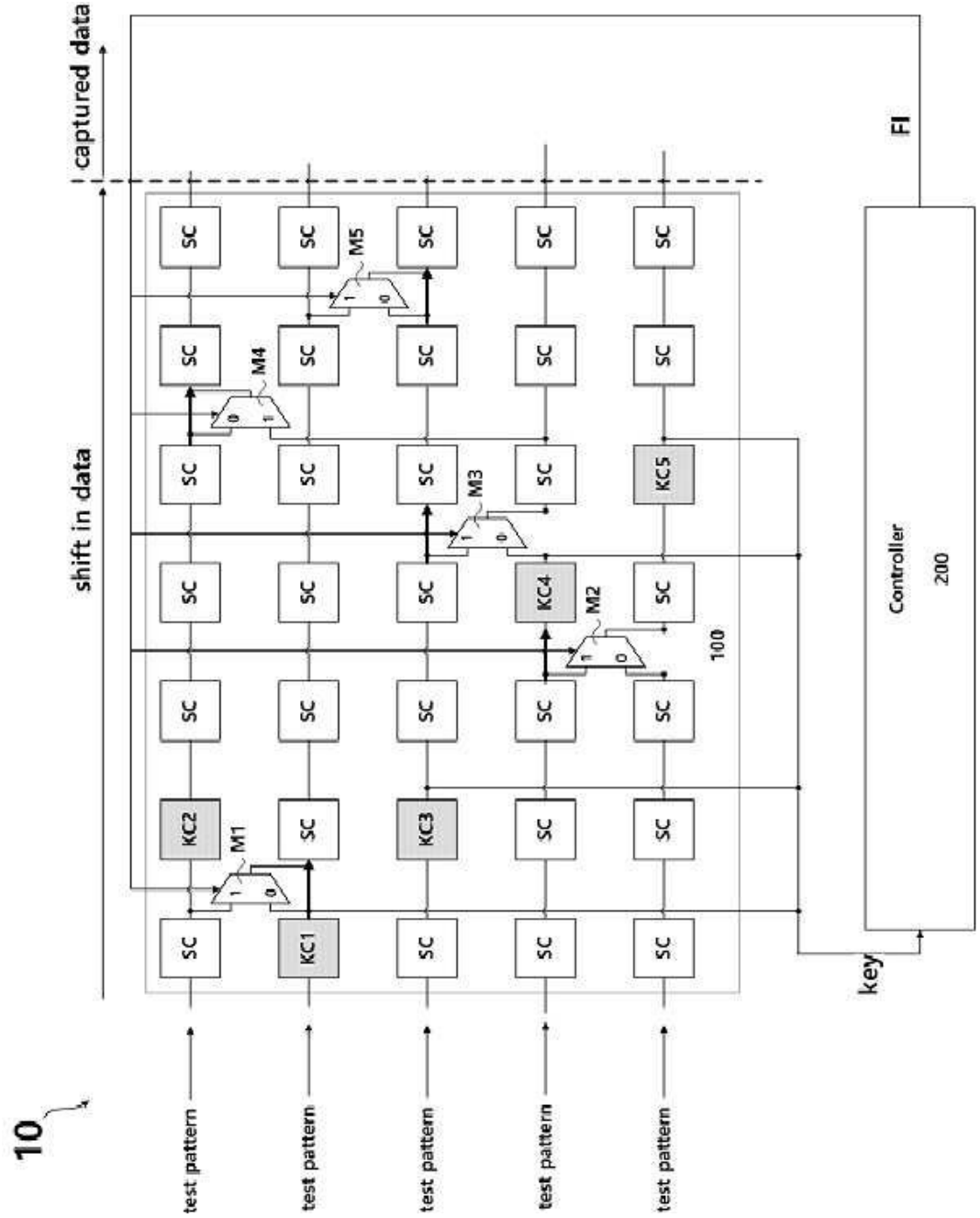
도면5


10
shift in data
captured data
test pattern
test pattern
test pattern
test pattern
test pattern
SC
KC1
KC2
KC3
KC4
KC5
M1
M2
M3
M4
M5
100
FI
key
Controller
200

도면6


10
test pattern
test pattern
test pattern
test pattern
test pattern
shift in data
captured data
SC
KC1
KC2
KC3
KC4
KC5
M1
M2
M3
M4
M5
100
FI
key
Controller
200

도면7


captured data
shift in data
FI
SC
KC1
KC2
KC3
KC4
KC5
M1
M2
M3
M4
M5
100
Controller
200
key
10
test pattern
test pattern
test pattern
test pattern
test pattern