(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0074017
(43) 공개일자 2022년06월03일

(51) 국제특허분류(Int. Cl.)
G06F 21/75 (2013.01) *G06F 21/72* (2013.01)
(52) CPC특허분류
G06F 21/75 (2020.05)
G06F 21/72 (2013.01)
(21) 출원번호 10-2020-0162047
(22) 출원일자 2020년11월27일
심사청구일자 2020년11월27일

(71) 출원인
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
강성호
서울특별시 마포구 양화로 45, 101동 2102호 (서교동, 메세나폴리스)
이영광
경기도 안산시 상록구 삼리로 24, 107동 1301호 (사동, 숲속마을아파트)
(74) 대리인
특허법인(유한)아이시스

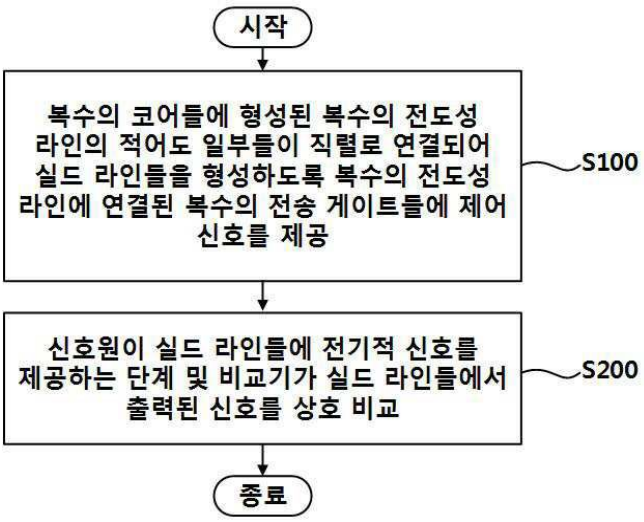
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **칩의 보안 회로**

(57) 요 약

본 실시예에 의한 칩의 보안 회로는 복수의 코어들과 코어의 전기적 연결을 수행하는 복수의 전도성 라인들과, 복수의 전도성 라인의 적어도 일부들이 직렬로 연결되어 실드 라인들을 형성하도록 복수의 전도성 라인에 연결된 복수의 전송 게이트들(transmission gate)과, 실드 라인들에 신호를 제공하는 신호원 및 실드 라인들에서 출력된 신호를 상호 비교하는 비교기를 포함한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	1711110267
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	2020.03.01 ~ 2021.02.28

명 세 서

청구범위

청구항 1

복수의 코어들과 상기 코어의 전기적 연결을 수행하는 복수의 전도성 라인들;

상기 복수의 전도성 라인의 적어도 일부들이 직렬로 연결되어 실드 라인들을 형성하도록 상기 복수의 전도성 라인에 연결된 복수의 전송 게이트들(transmission gate);

상기 실드 라인들에 신호를 제공하는 신호원;

상기 실드 라인들에서 출력된 신호를 상호 비교하는 비교기를 포함하는 보안회로.

청구항 2

제1항에 있어서,

상기 복수의 코어들은 제1 코어 및 제2 코어를 포함하고,

상기 신호원은 상기 제1 코어에 형성된 제1 실드 라인과, 상기 제2 코어에 형성된 제2 실드 라인에 상기 신호를 제공하는 보안 회로.

청구항 3

제2항에 있어서,

상기 제1 실드 라인과, 상기 제2 실드 라인은 서로 동일한 전기적 특성을 가지는 보안 회로.

청구항 4

제1항에 있어서,

상기 보안 회로는,

상기 비교기의 비교 결과를 제공받고, 상기 코어들의 동작을 제어하는 제어기를 더 포함하는 보안 회로.

청구항 5

제1항에 있어서,

상기 신호원은 상기 실드 라인들의 제1 지점에 신호를 인가하고,

상기 비교기는 상기 실드 라인들의 상기 제1 지점에서 출력된 신호를 서로 비교하는 보안 회로.

청구항 6

제5항에 있어서,

상기 비교기는,

상기 신호원이 상기 제1 지점에 인가한 신호가 상기 실드 라인의 단부에서 반사되어 상기 제1 지점에 형성된 신호를 서로 비교하는 보안 회로.

청구항 7

복수의 코어들에 형성된 복수의 전도성 라인의 적어도 일부들이 직렬로 연결되어 실드 라인들을 형성하도록 상기 복수의 전도성 라인에 연결된 복수의 전송 게이트들에 제어 신호를 제공하는 단계;

신호원이 상기 실드 라인들에 전기적 신호를 제공하는 단계 및

비교기가 상기 실드 라인들에서 출력된 신호를 상호 비교하는 단계를 포함하는 칩의 보안 방법.

청구항 8

제7항에 있어서,

상기 복수의 코어들은 제1 코어 및 제2 코어를 포함하고,

상기 신호원은 상기 제1 코어에 형성된 제1 실드 라인과, 상기 제2 코어에 형성된 제2 실드 라인에 상기 신호를 제공하는 보안 방법.

청구항 9

제8항에 있어서,

상기 제1 실드 라인과, 상기 제2 실드 라인은 서로 동일한 전기적 특성을 가지는 보안 방법.

청구항 10

제7항에 있어서,

상기 보안 방법은,

상기 비교기의 비교 결과를 제공받고,

제어기가 상기 코어들의 동작을 제어하는 단계를 더 포함하는 보안 방법.

청구항 11

제7항에 있어서,

상기 신호원은 상기 실드 라인들의 제1 지점에 신호를 인가하고,

상기 비교기는 상기 실드 라인들의 상기 제1 지점에서 출력된 신호를 서로 비교하는 보안 방법.

청구항 12

제11항에 있어서,

상기 비교기는,

상기 신호원이 상기 제1 지점에 인가한 신호가 상기 실드 라인의 단부에서 반사되어 상기 제1 지점에 형성된 신호를 서로 비교하는 보안 방법.

발명의 설명

기 술 분 야

[0001] 본 기술은 칩의 보안 회로와 관련된다.

배 경 기 술

[0002] 반도체 회로가 형성된 칩의 역설계(reverse engineering) 또는 칩에 형성된 중요한 정보를 탈취를 위한 공격이 수행된다. 이러한 공격의 대표적인 예로는 마이크로 프로빙(micro probing)등이 있다. 마이크로 프로빙은 칩에 형성된 실드(shield)의 메탈 라인 사이의 공간을 통해 아래 레이어(layer)의 와이어에 접촉해 신호를 탐지하는 형태로 수행된다.

발명의 내용

해결하려는 과제

[0003] 이러한 마이크로 프로빙으로부터 보안을 유지하여 칩에 형성된 주요한 정보를 지키기 위해서는 여러 층에 걸쳐서 액티브 실드(active shield)를 배치하는 멀티 레이어 액티브 실드(Multi-layer Active Shield)등의 기법을 이용할 수 있다.

[0004] 그러나, 멀티 레이어 액티브 실드는 하드웨어 오버헤드가 크기 때문에 칩 설계에 부담이 된다. 따라서 적은 하

드웨어 오버헤드로 충분한 보안 성능을 얻을 수 있는 보안회로가 필요하다.

[0005] 본 실시예는 상기한 종래 기술의 난점을 해소하기 위한 것이다. 즉, 하드웨어의 추가적 부담을 줄이고 이로부터 충분한 보안을 얻을 수 있는 보안 회로를 제공하는 것이 본 실시예로 해결하고자 하는 과제 중 하나이다.

과제의 해결 수단

[0006] 본 실시예에 의한 칩의 보안 회로는 복수의 코어들과 코어의 전기적 연결을 수행하는 복수의 전도성 라인들과, 복수의 전도성 라인의 적어도 일부들이 직렬로 연결되어 실드 라인들을 형성하도록 복수의 전도성 라인에 연결된 복수의 전송 게이트들(transmission gate)과, 실드 라인들에 신호를 제공하는 신호원 및 실드 라인들에서 출력된 신호를 상호 비교하는 비교기를 포함한다.

[0007] 본 실시예의 일 태양에 의하면, 복수의 코어들은 제1 코어 및 제2 코어를 포함하고, 신호원은 제1 코어에 형성된 제1 실드 라인과, 제2 코어에 형성된 제2 실드 라인에 신호를 제공한다.

[0008] 본 실시예의 일 태양에 의하면, 제1 실드 라인과, 제2 실드 라인은 서로 동일한 전기적 특성을 가진다.

[0009] 본 실시예의 일 태양에 의하면, 보안 회로는, 비교기의 비교 결과를 제공받고, 코어들의 동작을 제어하는 제어기를 더 포함한다.

[0010] 본 실시예의 일 태양에 의하면, 신호원은 실드 라인들의 제1 지점에 신호를 인가하고, 비교기는 실드 라인들의 제1 지점에서 출력된 신호를 서로 비교한다.

[0011] 본 실시예의 일 태양에 의하면, 비교기는, 신호원이 제1 지점에 인가한 신호가 실드 라인의 단부에서 반사되어 제1 지점에 형성된 신호를 서로 비교한다.

[0012] 본 실시예에 의한 칩의 보안 방법은, 복수의 코어들에 형성된 복수의 전도성 라인의 적어도 일부들이 직렬로 연결되어 실드 라인들을 형성하도록 복수의 전도성 라인에 연결된 복수의 전송 게이트들에 제어 신호를 제공하는 단계와, 신호원이 실드 라인들에 전기적 신호를 제공하는 단계 및 비교기가 실드 라인들에서 출력된 신호를 상호 비교하는 단계를 포함한다.

[0013] 본 실시예의 일 태양에 의하면, 복수의 코어들은 제1 코어 및 제2 코어를 포함하고, 신호원은 제1 코어에 형성된 제1 실드 라인과, 제2 코어에 형성된 제2 실드 라인에 신호를 제공한다.

[0014] 본 실시예의 일 태양에 의하면, 제1 실드 라인과, 제2 실드 라인은 서로 동일한 전기적 특성을 가진다.

[0015] 본 실시예의 일 태양에 의하면, 보안 방법은, 비교기의 비교 결과를 제공받고, 제어기가 코어들의 동작을 제어하는 단계를 더 포함한다.

[0016] 본 실시예의 일 태양에 의하면, 신호원은 실드 라인들의 제1 지점에 신호를 인가하고, 비교기는 실드 라인들의 제1 지점에서 출력된 신호를 서로 비교한다.

[0017] 본 실시예의 일 태양에 의하면, 비교기는, 신호원이 제1 지점에 인가한 신호가 실드 라인의 단부에서 반사되어 제1 지점에 형성된 신호를 서로 비교한다.

발명의 효과

[0018] 본 실시예에 의하면 하드웨어의 추가적 부담 없이 충분한 보안을 얻을 수 있다는 장점이 제공된다.

도면의 간단한 설명

[0019] 도 1은 본 실시예에 의한 칩의 보안 방법의 각 단계들을 개요적으로 도시한 순서도이다.

도 2는 본 실시예에 의한 칩의 보안 회로를 개요적으로 도시한 도면이다.

도 3은 복수의 전송 게이트(T1a, ..., Tna, T1b, ..., Tnb)들 중 어느 한 전송 게이트(T1a)의 개요를 도시한 도면이다.

도 4는 제어부(120)가 전송 게이트들(T1a, ..., Tna, T1b, ..., Tnb)이 도통되도록 제어 신호를 제공하여 실드 라인이 형성된 상태에서 신호원(100)이 신호를 제공한 상태를 도시한 도면이다.

도 5는 신호원(100)이 제공한 신호가 실드 라인의 단부에서 반사되어 전파되는 것을 예시한 도면이다.

도 6(a)와 도 6(b)는 각각 마이크로 프로빙 공격이 없을 때와 있을 때 실드 라인에서 전파되는 신호의 형태를 개요적으로 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0020] 이하에서는 첨부된 도면들을 참조하여 본 실시예에 의한 칩의 보안 방법 및 칩의 보안 회로를 설명한다. 도 1은 본 실시예에 의한 칩의 보안 방법의 각 단계들을 개요적으로 도시한 순서도이다. 도 1을 참조하면, 본 실시예에 의한 칩의 보안 방법은: 복수의 코어들에 형성된 복수의 전도성 라인의 적어도 일부들이 직렬로 연결되어 실드 라인들을 형성하도록 복수의 전도성 라인에 연결된 복수의 전송 게이트들에 제어 신호를 제공하는 단계(S100)와, 신호원이 실드 라인들에 전기적 신호를 제공하는 단계 및 비교기가 실드 라인들에서 출력된 신호를 상호 비교하는 단계(S200)를 포함한다.

[0021] 도 2는 본 실시예에 의한 칩의 보안 회로를 개요적으로 도시한 도면이다. 도 2를 참조하면, 본 실시예에 의한 칩의 보안 회로는: 복수의 코어들(10, 20)과 코어의 전기적 연결을 수행하는 복수의 전도성 라인들(L1a, L2a, L3a, ... LNa, L1b, L2b, L3b, ... LNb)과, 복수의 전도성 라인(L1a, L2a, L3a, ... LNa, L1b, L2b, L3b, ... LNb)의 적어도 일부들이 직렬로 연결되어 실드 라인들을 형성하도록 복수의 전도성 라인에 연결된 복수의 전송 게이트들(transmission gate, T1a, ..., Tka, T1b, ..., Tkb)과, 실드 라인들에 신호를 제공하는 신호원(signal generator, 100) 및 실드 라인들에서 출력된 신호를 상호 비교하는 비교기(comparator, 110)를 포함한다. 일 실시예로, 칩의 보안 회로는 비교기(110)rk 출력한 신호에 따라 회로의 동작을 제어하는 제어부(120)를 더 포함할 수 있다.

[0022] 도 1 및 도 2를 참조하면, 복수의 코어들(10a, 10b)의 상부에는 코어 내부의 배선을 위하여 전도성 라인들이 층을 이루어 배치된다. 일 실시예에서 실드 라인을 형성하는 전도성 라인들은 최상부 레이어에 배치된 전도성 라인들일 수 있다. 다른 실시예에서, 실드 라인을 형성하는 전도성 라인들은 각 코어들의 최상부 몇 몇 레이어에 배치된 전도성 라인들 일 수 있다.

[0023] 도 3은 복수의 전송 게이트(T1a, ..., Tna, T1b, ..., Tnb)들 중 어느 한 전송 게이트(T1a)의 개요를 도시한 도면이다. 도 3을 참조하면, 전송 게이트(T1a)는 NMOS 트랜지스터와 PMOS 트랜지스터 및 인버터(INV)를 포함하며, NMOS 트랜지스터의 소스 전극은 PMOS 트랜지스터의 드레인 전극과 연결되고, NMOS 트랜지스터의 드레인 전극은 PMOS 트랜지스터의 소스 전극과 연결된다. NMOS 트랜지스터의 게이트 전극과 PMOS 트랜지스터의 게이트 전극은 인버터(INV)에 의하여 서로 반전된 신호가 제공된다.

[0024] 일 실시예로, 전송 게이트(T1a)에 논리 로우 신호가 제공되면 NMOS 트랜지스터의 게이트 전극과 PMOS 트랜지스터의 게이트 전극에는 각각 논리 로우 신호와 논리 하이 신호가 제공되어 전송 게이트(T1a)는 차단된다. 그러나, 전송 게이트(T1a)에 논리 하이 신호가 제공되면 NMOS 트랜지스터의 게이트 전극과 PMOS 트랜지스터의 게이트 전극에는 논리 하이 신호가 제공되어 NMOS 트랜지스터는 도통되고, PMOS 트랜지스터의 게이트 전극에는 논리 로우 신호가 제공되어 PMOS 트랜지스터는 도통된다. NMOS 트랜지스터와 PMOS 트랜지스터가 모두 도통되므로 전류(i)는 양방향으로 흐를 수 있다.

[0025] 전송 게이트들에는 제어 신호가 제공되며, 복수의 전송 게이트(T1a, ..., Tna, T1b, ..., Tnb)들의 도통 및 차단을 제어하는 제어 신호는 제어부(120)가 제공할 수 있다.

[0026] 도 4는 제어부(120)가 전송 게이트들(T1a, ..., Tna, T1b, ..., Tnb)이 도통되도록 제어 신호를 제공하여 실드 라인이 형성된 상태에서 신호원(100)이 신호를 제공한 상태를 도시한 도면이다. 도 4를 참조하면, 제어부(120)가 전송 게이트들(T1a, ..., Tna, T1b, ..., Tnb)이 도통되도록 제어 신호를 제공하면 복수의 전도성 라인들(L1a, L2a, L3a, ... LNa)은 전송 게이트(T1a, ..., Tka)에 의하여 서로 직렬로 연결되어 실드 라인(shield line)을 형성한다. 마찬가지로 제어부(120)가 전송 게이트(T1b, ..., Tnb)들이 도통되도록 제어 신호를 제공하면 전도성 라인들(L1b, L2b, L3b, ... LNb)들은 서로 직렬로 연결되어 실드 라인을 형성한다.

[0027] 코어 1(10a)에 형성된 실드라인의 단부와 코어 2(10b)에 형성된 실드라인의 단부는 신호원(100)과 전기적으로 연결된다. 신호원(100)은 각 실드라인의 단부에 전기적 신호를 제공한다. 일 예로, 신호원(100)이 제공하는 신호는 미리 정해진 진폭을 가지는 단일한 펄스(pulse), 펄스열(pulse train), 정현파 펄스(sinusoidal pulse) 및 스텝 신호(step signal) 중 어느 하나일 수 있다.

[0028] 일 실시예로, 신호원(100)은 동시에 각 실드라인에 신호를 제공할 수 있다. 다른 실시예로, 신호원(100)은 어느 한 코어가 아이들(idle) 상태에 있을 때 해당 코어에 형성된 실드 라인에 신호를 제공하고, 다른 코어가 아이들

(idle) 상태에 있을 때 해당 코어에 형성된 실드 라인에 신호를 제공하는 방식으로 신호를 제공할 수 있다.

[0029] 도 5는 신호원(100)이 제공한 신호가 실드 라인의 단부에서 반사되어 전파되는 것을 예시한 도면이다. 도 5를 참조하면, 신호원(100)이 제공한 신호는 실드 라인의 단부에서 반사되고, 양방향 전도성을 가지는 전송 게이트들을 통하여 전파된다. 비교기(110)는 각 실드 라인에서 반사된 신호들을 검출하고, 두 신호들 사이의 진폭, 지연(delay)를 비교하여 마이크로 프로빙 공격 여부를 파악한다.

[0030] 도 6(a)와 도 6(b)는 각각 마이크로 프로빙 공격이 없을 때와 있을 때 실드 라인에서 전파되는 신호의 형태를 개요적으로 도시한 도면이다. 도 6(a)를 참조하면, 코어 1(10a)에 형성되는 전도성 라인(L1a, L2a, L3a, ... LNa)과 코어 2(10b)에 형성되는 전도성 라인(L1b, L2b, L3b, ... LNb)들의 전기적 특성은 동일하다. 도시된 예에서, 신호원(100)은 단일한 사각 펄스를 제공하는 것을 예시한다. 다만, 이는 용이한 이해를 위한 예시이며, 상술한 바와 같이 신호원은 폭을 가지는 단일한 펄스(pulse), 펄스열(pulse train), 정현파 펄스(sinusoidal pulse) 및 스텝 신호(step signal) 중 어느 하나를 제공할 수 있다.

[0031] 일 예로, 전도성 라인(L1a, L2a, L3a, ... LNa)과 전도성 라인(L1b, L2b, L3b, ... LNb)은 전도성 라인을 형성하는 재질, 전도성 라인의 전도도, 전도성 라인의 저항및 전도성 라인의 길이가 동일하다. 따라서, 코어 1(10a)에서 전도성 라인(L1a, L2a, L3a, ... LNa)이 전송 게이트(T1a, ..., Tka)를 통하여 직렬로 연결되어 형성된 실드 라인(Sa)와 코어 2(10b)에서 전도성 라인(L1b, L2b, L3b, ... LNb)이 전송 게이트(T1b, ..., Tkb)를 통하여 직렬로 연결되어 형성된 실드 라인(Sb)는 전기적 특성이 동일하다. 따라서, 실드라인(Sa)의 단부에서 반사되어 형성된 신호와 실드라인(Sb)의 단부에서 반사되어 형성된 신호는 서로 동일한 개형을 가지며 비교기(120)에 동일한 시간에 도달한다.

[0032] 도 6(b)는 코어 1(10a)에 마이크로 프로빙 공격이 있는 경우의 개요도이다. 도 6(b)를 참조하면, 마이크로 프로빙 공격에 의하여 마이크로 프로브(미도시)가 실드라인(Sa)과 전기적으로 연결된다. 따라서, 실드라인(Sa)에는 마이크로 프로브와의 접촉에 의하여 커패시턴스 성분(C)가 형성된다. 실드라인(Sa)에 형성된 커패시턴스 성분에 의하여 펄스에 지연(delay)가 발생한다. 따라서, 비교기는 실드라인(Sa)와 실드라인(Sb)에서 형성된 신호를 입력받고 두 신호의 진폭 변화, 지연(delay)등을 검출하여 칩에 대한 공격여부를 파악할 수 있다.

[0033] 다시 도 1 및 도 2를 참조하면, 비교기(110)는 실드라인(Sa)과 실드라인(Sb)로부터 각각 입력된 신호를 비교하고, 비교 결과를 제어부(120)에 제공한다. 제어부(120)는 비교기(110)로부터 비교 결과를 제공받고, 비교 결과에 따라 제어 신호(con)을 제공하여 코어의 활성화를 제어할 수 있다.

[0034] 일 실시예로, 코어 1(10a)에 형성된 전도성 라인(L1a, L2a, L3a, ... LNa)의 각 단부와, 코어 2(10b)에 형성된 전도성 라인(L1b, L2b, L3b, ... LNb)의 각 단부에는 제어 가능한 버퍼(B)들이 위치한다. 따라서, 제어부(120)는 비교기(110)가 제공한 비교 신호에 따라 외부로부터의 침입이 발생한 경우에는 제어 신호(con)을 제공하여 버퍼(B)들을 불활성화(disable)할 수 있다. 따라서, 칩에 형성된 주요한 정보를 보호할 수 있다.

[0035] 두 개의 코어를 가지는 칩에 대한 공격을 탐지하는 실시예를 들어 본 발명을 설명하였다. 그러나, 통상의 기술자는 위에서 설명된 바를 기초로 3개 이상의 코어들에 대한 공격을 탐지하도록 용이하게 변형 실시할 수 있을 것이다.

[0036] 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

[0037] S100~S200: 본 실시예에 의한 칩의 보안 방법의 개요적 각 단계

10a: 제1 코어 10b: 제2 코어

100: 신호원 110: 비교기

120: 제어부

L1a, L2a, L3a, ... LNa, L1b, L2b, L3b, ... LNb: 전도성 라인

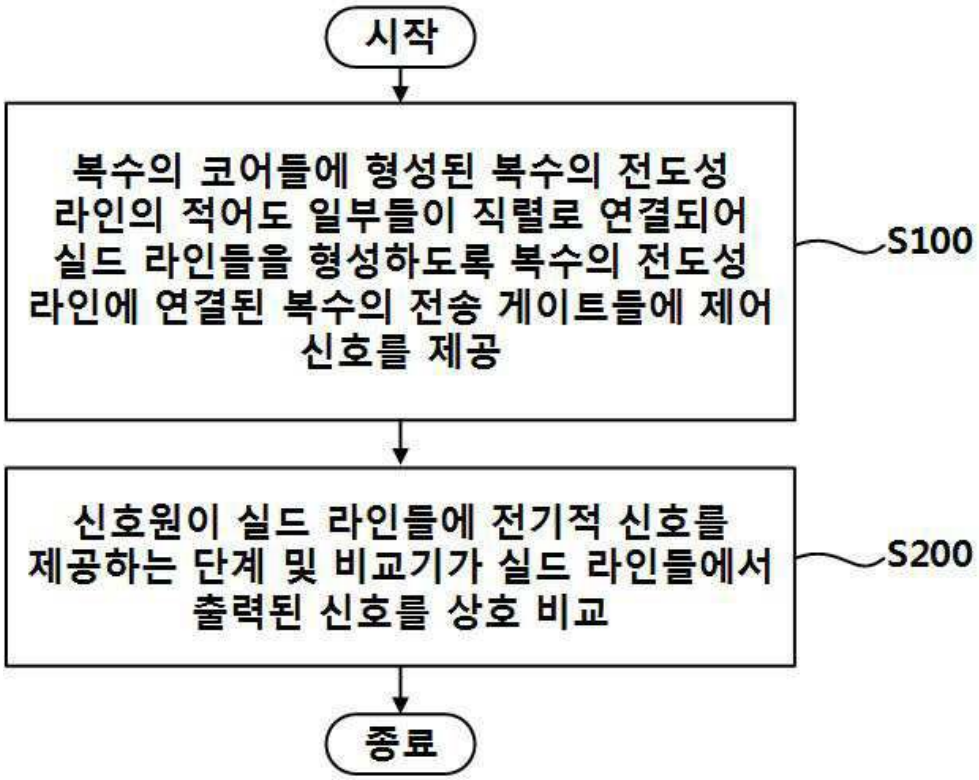
T1a, ..., Tna, T1b, ..., Tnb: 전송 게이트

B: 제어 가능한 버퍼 NMOS: NMOS 트랜지스터

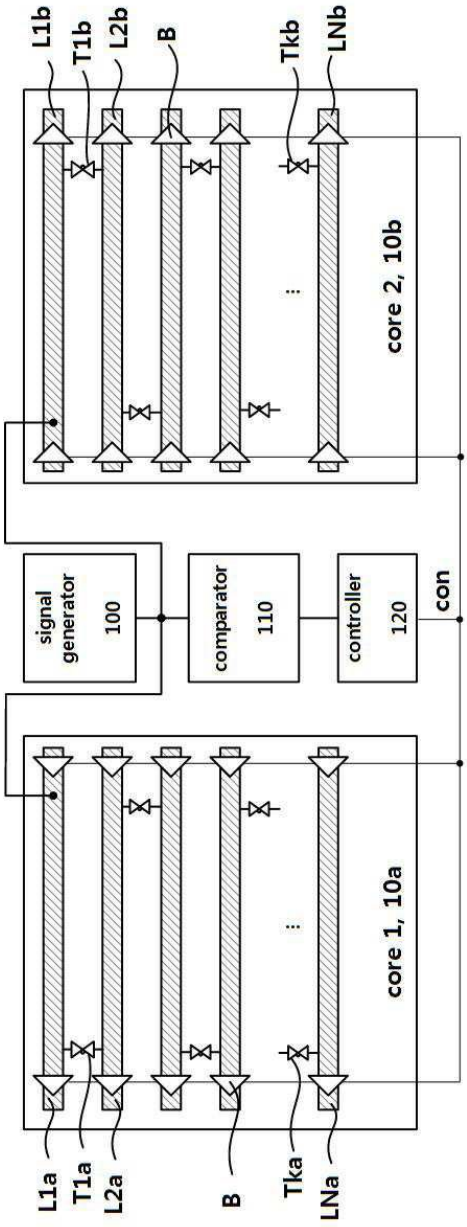
PMOS: PMOS 트랜지스터 INV: 인버터

도면

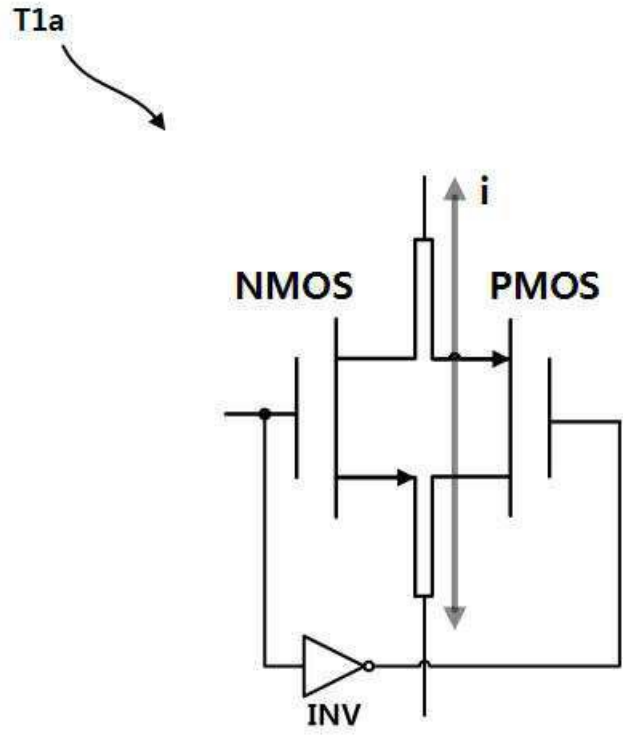
도면1



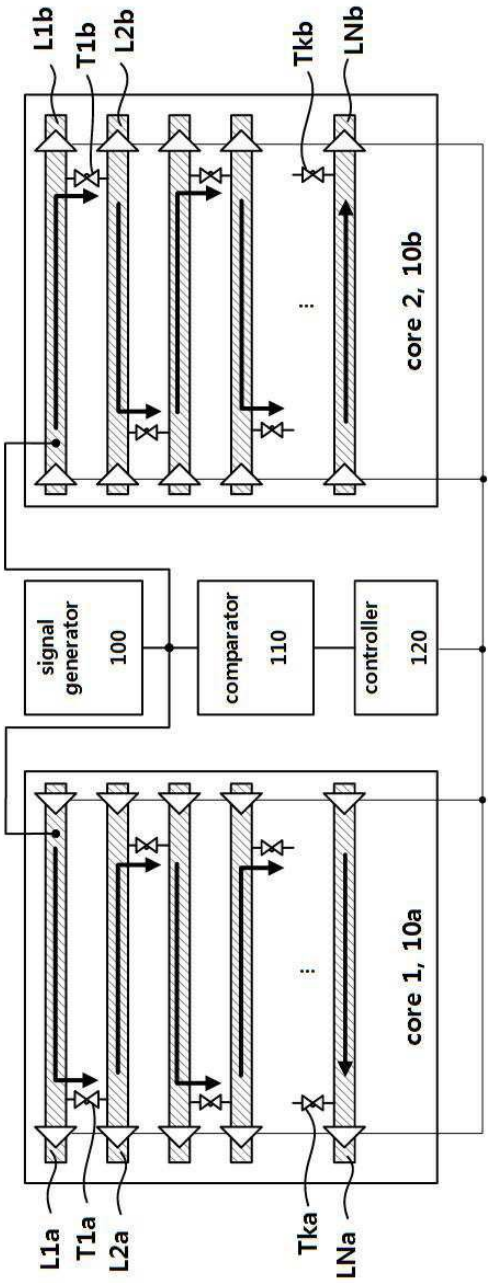
도면2


L1b
T1b
L2b
B
Tkb
LNb
core 2, 10b
signal generator 100
comparator 110
controller 120
con
core 1, 10a
L1a
T1a
L2a
B
Tka
LNa

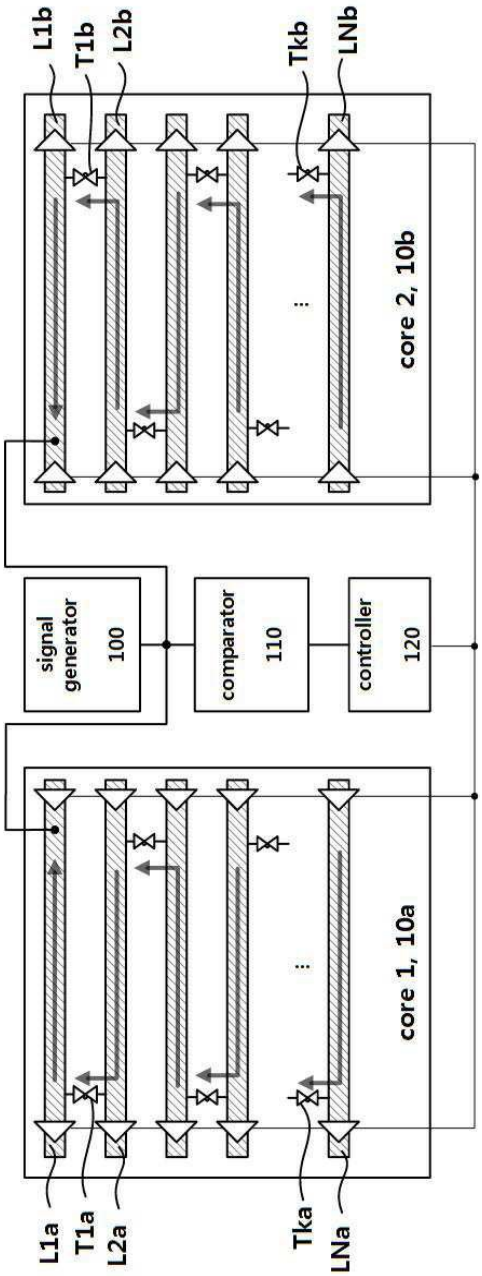
도면3



도면4


L1b
T1b
L2b
Tkb
LNb
core 2, 10b
signal generator 100
comparator 110
controller 120
core 1, 10a
L1a
T1a
L2a
Tka
LNa

도면5


L1b
T1b
L2b
Tkb
LNb
core 2, 10b
signal generator 100
comparator 110
controller 120
core 1, 10a
L1a
T1a
L2a
Tka
LNa

도면6