



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년12월21일
(11) 등록번호 10-1811228
(24) 등록일자 2017년12월15일

(51) 국제특허분류(Int. Cl.)
G06F 21/72 (2013.01) G06F 11/07 (2006.01)
G06F 21/50 (2013.01)
(52) CPC특허분류
G06F 21/725 (2013.01)
G06F 1/04 (2013.01)
(21) 출원번호 10-2015-7027594
(22) 출원일자(국제) 2014년03월10일
심사청구일자 2017년06월05일
(85) 번역문제출일자 2015년10월05일
(65) 공개번호 10-2015-0128834
(43) 공개일자 2015년11월18일
(86) 국제출원번호 PCT/US2014/022655
(87) 국제공개번호 WO 2014/164512
국제공개일자 2014년10월09일
(30) 우선권주장
13/801,375 2013년03월13일 미국(US)
(56) 선행기술조사문헌
US20080080658 A1*
(뒷면에 계속)

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
티리, 크리스
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
맥그리거, 매튜 스코트
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
타오, 유콩
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

전체 청구항 수 : 총 43 항

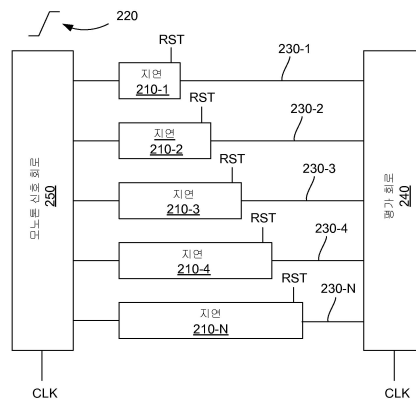
심사관 : 김병균

(54) 발명의 명칭 클록 탬퍼링을 검출하기 위한 장치 및 방법

(57) 요약

클록 탬퍼링(clock tampering)을 검출하기 위한 방법이 개시된다. 상기 방법에서, 복수의 재설정 가능한 지연 라인 세그먼트들이 제공된다. 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 클록과 연관된 클록 평가 시간 기간 동안에 모노톤 신호(monotone signal)가 제공된다. 모노톤 신호는 각각의 복수의 지연된 모노톤 신호들을 생성하기 위해 복수의 재설정 가능한 지연 라인 세그먼트들 각각을 사용하여 지연된다. 클록은 클록 결함을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용하는 평가 회로를 트리거링하는데 사용된다.

대표도



(52) CPC특허분류

G06F 11/0721 (2013.01)

G06F 11/076 (2013.01)

G06F 21/50 (2013.01)

(56) 선행기술조사문헌

US20100109721 A1*

US20070274434 A1*

W02004092932 A1

US5521499 A

*는 심사관에 의하여 인용된 문헌

명세서

청구범위

청구항 1

클록 탬퍼링(clock tampering)을 검출하기 위한 방법으로서,

복수의 재설정 가능한 지연 라인 세그먼트(delay line segment)들을 제공하는 단계 - 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로(discretely) 증가하는 지연 시간들과 연관됨 -;

클록과 연관된 클록 평가 시간 기간 동안에 모노톤 신호(monotone signal)를 제공하는 단계;

각각의 복수의 지연된 모노톤 신호들을 생성하기 위해 상기 복수의 재설정 가능한 지연 라인 세그먼트들 각각을 사용하여 상기 모노톤 신호를 지연시키는 단계 - 상기 복수의 지연된 모노톤 신호들 각각은 1 또는 0 로직 값 중 어느 하나를 가짐 -; 및

클록 결함을 검출하기 위해 상기 복수의 지연된 모노톤 신호들을 사용하는 평가 회로를 트리거링하기 위해 상기 클록을 사용하는 단계를 포함하는,

클록 탬퍼링을 검출하기 위한 방법.

청구항 2

제 1 항에 있어서,

상기 방법은 재설정 시간 기간 동안에 상기 재설정 가능한 지연 라인 세그먼트들을 재설정하는 단계를 더 포함하고,

상기 재설정 시간 기간은 상기 클록 평가 시간 기간 전에 있는,

클록 탬퍼링을 검출하기 위한 방법.

청구항 3

제 1 항에 있어서,

상기 평가 회로를 트리거링하기 위해 상기 클록을 사용하는 단계는, 상기 평가 회로를 트리거링하기 위해 상기 클록 평가 시간 기간의 끝에서 클록 에지를 사용하는 단계를 포함하는,

클록 탬퍼링을 검출하기 위한 방법.

청구항 4

제 1 항에 있어서,

상기 평가 회로는, 상기 복수의 지연된 모노톤 신호들 내의 1들의 갯수가 미리 결정된 임계치보다 더 많이 수위 갯수(water level number)와 상이한지를 결정하는,

클록 탬퍼링을 검출하기 위한 방법.

청구항 5

제 4 항에 있어서,

상기 수위 갯수는 하나 이상의 이전의 클록 평가 시간으로부터 지연된 모노톤 신호들에 기초하여 결정되는,

클록 탬퍼링을 검출하기 위한 방법.

청구항 6

제 1 항에 있어서,

상기 복수의 재설정 가능한 지연 라인 세그먼트들은 지연 라인을 따라 탭들(taps)을 포함하는,
클록 탬퍼링을 검출하기 위한 방법.

청구항 7

제 1 항에 있어서,

상기 복수의 재설정 가능한 지연 라인 세그먼트들은 병렬의 지연 라인들을 포함하는,
클록 탬퍼링을 검출하기 위한 방법.

청구항 8

클록 탬퍼링을 검출하기 위한 장치로서,

클록과 연관된 클록 평가 시간 기간 동안에 모노톤 신호를 제공하기 위한 수단;

최소 지연 시간과 최대 지연 시간 사이에서 이산적으로 증가하는 지연 시간들을 갖는 복수의 지연된 모노톤 신호들을 생성하기 위해 상기 모노톤 신호를 지연시키기 위한 수단 — 상기 복수의 지연된 모노톤 신호들 각각은 1 또는 0 로직 값 중 어느 하나를 가짐 —;

클록 결함을 검출하기 위해 상기 복수의 지연된 모노톤 신호들을 사용하는, 평가하기 위한 수단; 및

상기 평가하기 위한 수단을 트리거링하기 위한 수단을 포함하는,

클록 탬퍼링을 검출하기 위한 장치.

청구항 9

제 8 항에 있어서,

상기 장치는 재설정 시간 기간 동안에 상기 모노톤 신호를 지연시키기 위한 수단을 재설정하기 위한 수단을 더 포함하고,

상기 재설정 시간 기간은 상기 클록 평가 시간 기간 전에 있는,

클록 탬퍼링을 검출하기 위한 장치.

청구항 10

제 8 항에 있어서,

상기 평가하기 위한 수단을 트리거링하기 위한 수단은, 상기 평가하기 위한 수단을 트리거링하기 위해 상기 클록 평가 시간 기간의 끝에서 클록 에지를 사용하는,

클록 탬퍼링을 검출하기 위한 장치.

청구항 11

제 8 항에 있어서,

상기 평가하기 위한 수단은, 상기 복수의 지연된 모노톤 신호들 내의 1들의 갯수가 미리 결정된 임계치보다 더 많이 수위 갯수와 상이한지를 결정하는,

클록 탬퍼링을 검출하기 위한 장치.

청구항 12

제 11 항에 있어서,

상기 수위 갯수는 하나 이상의 이전의 클록 평가 시간으로부터 지연된 모노톤 신호들에 기초하여 결정되는,

클록 탬퍼링을 검출하기 위한 장치.

청구항 13

제 8 항에 있어서,
상기 모노톤 신호를 지연시키기 위한 수단은 지연 라인을 따라 탭들을 포함하는,
클록 탬퍼링을 검출하기 위한 장치.

청구항 14

제 8 항에 있어서,
상기 모노톤 신호를 지연시키기 위한 수단은 병렬의 지연 라인들을 포함하는,
클록 탬퍼링을 검출하기 위한 장치.

청구항 15

클록 탬퍼링을 검출하기 위한 장치로서,
클록과 연관된 클록 평가 시간 기간 동안에 모노톤 신호를 제공하는 회로;
각각의 복수의 지연된 모노톤 신호들을 생성하기 위해 상기 모노톤 신호를 지연시키는 복수의 재설정 가능한 지연 라인 세그먼트들 - 상기 복수의 지연된 모노톤 신호들 각각은 1 또는 0 로직 값 중 어느 하나를 가지고, 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관됨 -; 및
클록 결함을 검출하기 위해 상기 복수의 지연된 모노톤 신호들을 사용하는, 상기 클록에 의해 트리거링되는, 평가 회로를 포함하는,
클록 탬퍼링을 검출하기 위한 장치.

청구항 16

제 15 항에 있어서,
상기 재설정 가능한 지연 라인 세그먼트들은 재설정 시간 기간 동안에 재설정되고,
상기 재설정 시간 기간은 상기 클록 평가 시간 기간 전에 있는,
클록 탬퍼링을 검출하기 위한 장치.

청구항 17

제 15 항에 있어서,
상기 평가 회로는 상기 클록 평가 시간 기간의 끝에서 클록 에지에 의해 트리거링되는,
클록 탬퍼링을 검출하기 위한 장치.

청구항 18

제 15 항에 있어서,
상기 평가 회로는, 클록 결함을 검출하기 위해, 상기 복수의 지연된 모노톤 신호들 내의 1들의 갯수가 미리 결정된 임계치보다 더 많이 수위 갯수와 상이한지를 결정하는,
클록 탬퍼링을 검출하기 위한 장치.

청구항 19

제 18 항에 있어서,
상기 수위 갯수는 하나 이상의 이전의 클록 평가 시간으로부터 지연된 모노톤 신호들에 기초하여 결정되는,

클록 탬퍼링을 검출하기 위한 장치.

청구항 20

제 15 항에 있어서,

상기 복수의 재설정 가능한 지연 라인 세그먼트들은 지연 라인을 따라 탭들을 포함하는,

클록 탬퍼링을 검출하기 위한 장치.

청구항 21

제 15 항에 있어서,

상기 복수의 재설정 가능한 지연 라인 세그먼트들은 병렬의 지연 라인들을 포함하는,

클록 탬퍼링을 검출하기 위한 장치.

청구항 22

클록 탬퍼링을 검출하기 위한 장치로서,

클록과 연관된 제 1 클록 평가 시간 기간 동안에 제 1 모노톤 신호를 제공하는 제 1 회로;

제 1 복수의 재설정 가능한 지연 라인 세그먼트들 — 상기 제 1 복수의 재설정 가능한 지연 라인 세그먼트들 각각은 각각의 제 1 복수의 지연된 모노톤 신호들을 생성하기 위해 상기 제 1 모노톤 신호를 지연시키고, 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관됨 —;

상기 클록과 연관된 제 2 클록 평가 시간 기간 동안에 제 2 모노톤 신호를 제공하는 제 2 회로 — 상기 제 2 클록 평가 시간 기간은 상기 제 1 클록 평가 시간 기간과 상이한 시간을 커버함 —;

제 2 복수의 재설정 가능한 지연 라인 세그먼트들 — 상기 제 2 복수의 재설정 가능한 지연 라인 세그먼트들 각각은 각각의 제 2 복수의 지연된 모노톤 신호들을 생성하기 위해 상기 제 2 모노톤 신호를 지연시키고, 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관됨 —; 및

클록 결합을 검출하기 위해 상기 제 1 복수의 지연된 모노톤 신호들 또는 상기 제 2 복수의 지연된 모노톤 신호들을 사용하는, 상기 클록에 의해 트리거링되는, 평가 회로를 포함하는,

클록 탬퍼링을 검출하기 위한 장치.

청구항 23

전압 탬퍼링을 검출하기 위한 방법으로서,

복수의 재설정 가능한 지연 라인 세그먼트들을 제공하는 단계 — 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관됨 —;

평가 시간 기간 동안에 모노톤 신호를 제공하는 단계;

각각의 복수의 지연된 모노톤 신호들을 생성하기 위해 상기 복수의 재설정 가능한 지연 라인 세그먼트들 각각을 사용하여 상기 모노톤 신호를 지연시키는 단계 — 상기 복수의 지연된 모노톤 신호들 각각은 1 또는 0 로직 값 중 어느 하나를 가짐 —; 및

전압 결합을 검출하기 위해 상기 복수의 지연된 모노톤 신호들을 사용하는 평가 회로를 트리거링하기 위해 클록을 사용하는 단계를 포함하는,

전압 탬퍼링을 검출하기 위한 방법.

청구항 24

제 23 항에 있어서,

상기 방법은 재설정 시간 기간 동안에 상기 재설정 가능한 지연 라인 세그먼트들을 재설정하는 단계를 더 포함하고,

상기 재설정 시간 기간은 상기 평가 시간 기간 전에 있는,

전압 탭퍼링을 검출하기 위한 방법.

청구항 25

제 23 항에 있어서,

상기 평가 회로를 트리거링하기 위해 상기 클록을 사용하는 단계는, 상기 평가 회로를 트리거링하기 위해 상기 평가 시간 기간의 끝에서 클록 에지를 사용하는 단계를 포함하는,

전압 탭퍼링을 검출하기 위한 방법.

청구항 26

제 23 항에 있어서,

상기 평가 회로는, 상기 복수의 지연된 모노톤 신호들 내의 1들의 갯수가 미리 결정된 임계치보다 더 많이 수위 갯수와 상이한지를 결정하는,

전압 탭퍼링을 검출하기 위한 방법.

청구항 27

제 26 항에 있어서,

상기 수위 갯수는 하나 이상의 이전의 평가 시간으로부터 지연된 모노톤 신호들에 기초하여 결정되는,

전압 탭퍼링을 검출하기 위한 방법.

청구항 28

제 23 항에 있어서,

상기 복수의 재설정 가능한 지연 라인 세그먼트들은 지연 라인을 따라 탭들을 포함하는,

전압 탭퍼링을 검출하기 위한 방법.

청구항 29

제 23 항에 있어서,

상기 복수의 재설정 가능한 지연 라인 세그먼트들은 병렬의 지연 라인들을 포함하는,

전압 탭퍼링을 검출하기 위한 방법.

청구항 30

전압 탭퍼링을 검출하기 위한 장치로서,

평가 시간 기간 동안에 정상 상태(steady-state) 모노톤 신호를 제공하기 위한 수단;

최소 지연 시간과 최대 지연 시간 사이에서 이산적으로 증가하는 지연 시간들을 갖는 복수의 지연된 모노톤 신호들을 생성하기 위해 상기 모노톤 신호를 지연시키기 위한 수단 — 상기 복수의 지연된 모노톤 신호들 각각은 1 또는 0 로직 값 중 어느 하나를 가짐 —;

전압 결함을 검출하기 위해 상기 복수의 지연된 모노톤 신호들을 사용하는, 평가하기 위한 수단; 및

상기 평가하기 위한 수단을 트리거링하기 위한 수단을 포함하는,

전압 탭퍼링을 검출하기 위한 장치.

청구항 31

제 30 항에 있어서,

상기 장치는 재설정 시간 기간 동안에 상기 모노톤 신호를 지연시키기 위한 수단을 재설정하기 위한 수단을 더 포함하고,

상기 재설정 시간 기간은 상기 평가 시간 기간 전에 있는,

전압 탬퍼링을 검출하기 위한 장치.

청구항 32

제 30 항에 있어서,

상기 평가하기 위한 수단을 트리거링하기 위한 수단은, 상기 평가하기 위한 수단을 트리거링하기 위해 상기 평가 시간 기간의 끝에서 클록 에지를 사용하는,

전압 탬퍼링을 검출하기 위한 장치.

청구항 33

제 30 항에 있어서,

상기 평가하기 위한 수단은, 상기 복수의 지연된 모노톤 신호들 내의 1들의 갯수가 미리 결정된 임계치보다 더 많이 수위 갯수와 상이한지를 결정하는,

전압 탬퍼링을 검출하기 위한 장치.

청구항 34

제 33 항에 있어서,

상기 수위 갯수는 하나 이상의 이전의 평가 시간으로부터 지연된 모노톤 신호들에 기초하여 결정되는,

전압 탬퍼링을 검출하기 위한 장치.

청구항 35

제 30 항에 있어서,

상기 모노톤 신호를 지연시키기 위한 수단은 지연 라인을 따라 탭들을 포함하는,

전압 탬퍼링을 검출하기 위한 장치.

청구항 36

제 30 항에 있어서,

상기 모노톤 신호를 지연시키기 위한 수단은 병렬의 지연 라인들을 포함하는,

전압 탬퍼링을 검출하기 위한 장치.

청구항 37

전압 탬퍼링을 검출하기 위한 장치로서,

평가 시간 기간 동안에 모노톤 신호를 제공하는 회로;

각각의 복수의 지연된 모노톤 신호들을 생성하기 위해 상기 모노톤 신호를 지연시키는 복수의 재설정 가능한 지연 라인 세그먼트들 — 상기 복수의 지연된 모노톤 신호들 각각은 1 또는 0 로직 값 중 어느 하나를 가지고, 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관됨 —; 및

전압 결함을 검출하기 위해 상기 복수의 지연된 모노톤 신호들을 사용하는, 클록에 의해 트리거링되는, 평가 회로를 포함하는,

전압 탬퍼링을 검출하기 위한 장치.

청구항 38

제 37 항에 있어서,

상기 재설정 가능한 지연 라인 세그먼트들은 재설정 시간 기간 동안에 재설정되고,

상기 재설정 시간 기간은 상기 평가 시간 기간 전에 있는,

전압 탬퍼링을 검출하기 위한 장치.

청구항 39

제 37 항에 있어서,

상기 평가 회로는 상기 평가 시간 기간의 끝에서 클록 에지에 의해 트리거링되는,

전압 탬퍼링을 검출하기 위한 장치.

청구항 40

제 37 항에 있어서,

상기 평가 회로는, 상기 전압 결함을 검출하기 위해, 상기 복수의 지연된 모노톤 신호들 내의 1들의 갯수가 미리 결정된 임계치보다 더 많이 수위 갯수와 상이한지를 결정하는,

전압 탬퍼링을 검출하기 위한 장치.

청구항 41

제 40 항에 있어서,

상기 수위 갯수는 하나 이상의 이전의 평가 시간으로부터 지연된 모노톤 신호들에 기초하여 결정되는,

전압 탬퍼링을 검출하기 위한 장치.

청구항 42

제 37 항에 있어서,

상기 복수의 재설정 가능한 지연 라인 세그먼트들은 지연 라인을 따라 탭들을 포함하는,

전압 탬퍼링을 검출하기 위한 장치.

청구항 43

제 37 항에 있어서,

상기 복수의 재설정 가능한 지연 라인 세그먼트들은 병렬의 지연 라인들을 포함하는,

전압 탬퍼링을 검출하기 위한 장치.

발명의 설명

기술 분야

[0001] 본 발명은 일반적으로 프로세서의 클록 및/또는 공급 전압에서 탬퍼링(tampering)을 검출하는 것에 관한 것이다.

배경 기술

[0002] 계산 시스템의 암호 계산은, 클록 및/또는 전력 공급 전압 상의 일시적인 스파이크(또는 글리치)를 받

생시켜 결함들을 계산 결과들에 도입함으로써 공격받을 수 있다. 또한, 공격은, 불완전한 계산의 잘못된 값이 계산 시스템의 레지스터들에서 샘플링되도록 계산 기간을 충분히 단축시키기 위해 클록 주파수를 증가시킬 수 있다. 또한, 공격은 시스템을 더 용이하게 공격하기 위해 계산 시스템의 버스를 둔화시킬 수 있다.

- [0003] [0003] 따라서, 프로세서의 클록 및/또는 공급 전압에서 템퍼링을 효율적이고 비용 효율적인 방식으로 검출하기 위한 기술에 대한 필요성이 존재한다.

발명의 내용

- [0004] [0004] 본 발명의 양상은 클록 템퍼링을 검출하기 위한 방법에 상주할 수 있다. 상기 방법에서, 복수의 재설정 가능한 지연 라인 세그먼트들이 제공된다. 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 클록과 연관된 클록 평가 시간 기간 동안에 모노톤 신호(monotone signal)가 제공된다. 모노톤 신호는 각각의 복수의 지연된 모노톤 신호들을 생성하기 위해 복수의 재설정 가능한 지연 라인 세그먼트들 각각을 사용하여 지연된다. 클록은 클록 결함을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용하는 평가 회로를 트리거링하는데 사용된다.

- [0005] [0005] 본 발명의 더 상세한 양상들에서, 상기 방법은 재설정 시간 기간 동안에 재설정 가능한 지연 라인 세그먼트들을 재설정하는 단계를 더 포함할 수 있다. 재설정 시간 기간은 클록 평가 시간 기간 전에 있을 수 있다. 평가 회로를 트리거링하기 위해 클록을 사용하는 것은, 평가 회로를 트리거링하기 위해 클록 평가 시간 기간의 끝에서 클록 에지를 사용할 수 있다.

- [0006] [0006] 본 발명의 다른 더 상세한 양상들에서, 복수의 지연된 모노톤 신호들 각각은 1 또는 0 중 어느 하나일 수 있다. 평가 회로는, 복수의 지연된 모노톤 신호들 내의 1들의 갯수가 미리 결정된 임계치보다 더 많이 수위 갯수(water level number)와 상이한지를 결정할 수 있다. 수위 갯수는 하나 이상의 이전의 클록 평가 시간으로부터 지연된 모노톤 신호들에 기초하여 결정될 수 있다. 복수의 재설정 가능한 지연 라인 세그먼트들은 지연 라인을 따라 탭들(taps)을 포함할 수 있다. 대안적으로, 복수의 재설정 가능한 지연 라인 세그먼트들은 병렬의 지연 라인들을 포함한다.

- [0007] [0007] 본 발명의 다른 양상은 클록 템퍼링을 검출하기 위한 장치에 상주할 수 있고, 상기 장치는 클록과 연관된 클록 평가 시간 기간 동안에 모노톤 신호를 제공하기 위한 수단, 최소 지연 시간과 최대 지연 시간 사이에서 이산적으로 증가하는 지연 시간들을 갖는 각각의 복수의 지연된 모노톤 신호들을 생성하기 위해 복수의 재설정 가능한 지연 라인 세그먼트들을 사용하여 모노톤 신호를 지연시키기 위한 수단, 및 클록 결함을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용하는 평가 회로를 트리거링하기 위해 클록을 사용하기 위한 수단을 포함한다.

- [0008] [0008] 본 발명의 다른 양상은 클록 템퍼링을 검출하기 위한 장치에 상주할 수 있고, 상기 장치는 모노톤 신호를 제공하는 회로, 복수의 재설정 가능한 지연 라인 세그먼트들 및 평가 회로를 포함한다. 회로는 클록과 연관된 클록 평가 시간 기간 동안에 모노톤 신호를 제공한다. 복수의 재설정 가능한 지연 라인 세그먼트들은 각각의 복수의 지연된 모노톤 신호들을 생성하기 위해 모노톤 신호를 지연시킨다. 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 평가 회로는 클록에 의해 트리거링되고, 클록 결함을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용한다.

- [0009] [0009] 본 발명의 다른 양상은 클록 템퍼링을 검출하기 위한 장치에 상주할 수 있고, 상기 장치는 제 1 회로, 제 1 복수의 재설정 가능한 지연 라인 세그먼트들, 제 2 회로, 제 2 복수의 재설정 가능한 지연 라인 세그먼트들 및 평가 회로를 포함한다. 제 1 회로는 클록과 연관된 제 1 클록 평가 시간 기간 동안에 제 1 모노톤 신호를 제공한다. 제 1 복수의 재설정 가능한 지연 라인 세그먼트들은 각각의 제 1 복수의 지연된 모노톤 신호들을 생성하기 위해 제 1 모노톤 신호를 각각 지연시킨다. 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 제 2 회로는 클록과 연관된 제 2 클록 평가 시간 기간 동안에 제 2 모노톤 신호를 제공한다. 제 2 클록 평가 시간 기간은 제 1 클록 평가 시간 기간과 상이한 시간을 커버한다. 제 2 복수의 재설정 가능한 지연 라인 세그먼트들은 각각의 제 2 복수의 지연된 모노톤 신호들을 생성하기 위해 제 1 모노톤 신호를 각각 지연시킨다. 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트

트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 평가 회로는 클록에 의해 트리거링되고, 클록 결합을 검출하기 위해 제 1 복수의 지연된 모노톤 신호들 또는 제 2 복수의 지연된 모노톤 신호들을 사용한다.

[0010] 본 발명의 양상은 전압 탬퍼링을 검출하기 위한 방법에 상주할 수 있다. 상기 방법에서, 복수의 재설정 가능한 지연 라인 세그먼트들이 제공된다. 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 평가 시간 기간 동안에 모노톤 신호가 제공된다. 모노톤 신호는, 각각의 복수의 지연된 모노톤 신호들을 생성하기 위해 복수의 재설정 가능한 지연 라인 세그먼트들 각각을 사용하여 지연된다. 클록은 전압 결합을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용하는 평가 회로를 트리거링하는데 사용된다.

[0011] 본 발명의 더 상세한 양상들에서, 상기 방법은 재설정 시간 기간 동안에 재설정 가능한 지연 라인 세그먼트들을 재설정하는 단계를 더 포함할 수 있다. 재설정 시간 기간은 평가 시간 기간 전에 있을 수 있다. 평가 회로를 트리거링하기 위해 클록을 사용하는 것은, 평가 회로를 트리거링하기 위해 평가 시간 기간의 끝에서 클록 에지를 사용할 수 있다.

[0012] 본 발명의 다른 더 상세한 양상들에서, 복수의 지연된 모노톤 신호들 각각은 1 또는 0 중 어느 하나를 포함한다. 평가 회로는, 복수의 지연된 모노톤 신호들 내의 1들의 갯수가 미리 결정된 임계치보다 더 많이 수 위 갯수와 상이한지를 결정할 수 있다. 수위 갯수는 하나 이상의 이전의 평가 시간으로부터 지연된 모노톤 신호들에 기초하여 결정될 수 있다. 복수의 재설정 가능한 지연 라인 세그먼트들은 지연 라인을 따라 탭들을 포함할 수 있다. 대안적으로, 복수의 재설정 가능한 지연 라인 세그먼트들은 병렬의 지연 라인들을 포함할 수 있다.

[0013] 본 발명의 다른 양상은 전압 탬퍼링을 검출하기 위한 장치에 상주할 수 있고, 상기 장치는 평가 시간 기간 동안에 모노톤 신호를 제공하기 위한 수단, 최소 지연 시간과 최대 지연 시간 사이에서 이산적으로 증가하는 지연 시간들을 갖는 각각의 복수의 지연된 모노톤 신호들을 생성하기 위해 복수의 재설정 가능한 지연 라인 세그먼트들 각각을 사용하여 모노톤 신호를 지연시키기 위한 수단, 및 전압 결합을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용하는 평가 회로를 트리거링하기 위해 클록을 사용하기 위한 수단을 포함한다.

[0014] 본 발명의 다른 양상은 전압 탬퍼링을 검출하기 위한 장치에 상주할 수 있고, 상기 장치는 모노톤 신호를 제공하는 회로, 복수의 재설정 가능한 지연 라인 세그먼트들 및 평가 회로를 포함한다. 회로는 평가 시간 기간 동안에 모노톤 신호를 제공한다. 복수의 재설정 가능한 지연 라인 세그먼트들은 각각의 복수의 지연된 모노톤 신호들을 생성하기 위해 모노톤 신호를 지연시킨다. 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 평가 회로는 클록에 의해 트리거링되고, 전압 결합을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용한다.

도면의 간단한 설명

[0015] 도 1은 본 발명에 따른, 클록 탬퍼링을 검출하기 위한 방법의 흐름도이다.

[0016] 도 2는 클록 탬퍼링 또는 전압 탬퍼링을 검출하기 위한 장치의 블록도이다.

[0017] 도 3은 클록 신호 및 재설정 신호의 개략도이다.

[0018] 도 4는 병렬의 지연 라인 세그먼트들의 개략도이다.

[0019] 도 5는 직렬의 지연 라인 세그먼트들의 개략도이다.

[0020] 도 6은 평가 회로 내의 검출 회로의 개략도이다.

[0021] 도 7은 불균일한 듀티 사이클을 갖는 클록을 검출하기 위한 듀얼 지연 라인들을 갖는 회로의 개략도이다.

[0022] 도 8은 본 발명에 따른, 전압 탬퍼링을 검출하기 위한 방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0016] 단어 "예시적인"은 "예, 사례 또는 예시로서 기능하는 것"을 의미하도록 본원에 사용된다. "예시적인

것"으로서 본원에 설명된 임의의 실시예는 반드시 다른 실시예들에 비해 선호되거나 유리한 것으로 해석되지는 않는다.

- [0017] [0024] 도 1, 도 2 및 도 3을 참조하면, 본 발명의 양상은 클록 탬퍼링을 검출하기 위한 방법(100)에 상주할 수 있다. 상기 방법에서, 복수의 재설정 가능한 지연 라인 세그먼트들(210)이 제공된다(단계 110). 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트(210-1) 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트(210-N) 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 클록 CLK와 연관된 클록 평가 시간 기간(310) 동안에 모노톤 신호(220)가 제공된다(단계 120). 모노톤 신호는, 각각의 복수의 지연된 모노톤 신호들(230)을 생성하기 위해 복수의 재설정 가능한 지연 라인 세그먼트들 각각을 사용하여 지연된다(단계 130). 클록은, 클록 결함을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용하는 평가 회로(240)를 트리거링하는데 사용된다(단계 140).
- [0018] [0025] 본 발명의 더 상세한 양상들에서, 방법(100)은 재설정 시간 기간(320) 동안에 재설정 신호 RST를 사용하여 재설정 가능한 지연 라인 세그먼트들(210)을 재설정하는 것을 더 포함할 수 있다. 재설정 시간 기간은 클록 평가 시간 기간(310) 전에 있을 수 있다. 평가 회로(240)를 트리거링하기 위한 클록 CLK를 사용하는 것은 평가 회로를 트리거링하기 위해 클록 평가 시간 기간의 끝에서 클록 에지를 사용할 수 있다.
- [0019] [0026] 본 발명의 다른 더 상세한 양상들에서, 복수의 지연된 모노톤 신호들(230) 각각은 1 또는 0 중 어느 하나일 수 있다. 평가 회로(240)는, 복수의 지연된 모노톤 신호들 내의 1들의 수가 미리 결정된 임계치보다 더 많이 수위 갯수와 상이한지를 결정할 수 있다. 수위 갯수는 하나 이상의 이전 클록 평가 시간(310)으로부터의 지연 모노톤 신호들에 기초하여 결정될 수 있다.
- [0020] [0027] 도 4를 참조하면, 복수의 재설정 가능한 지연 라인 세그먼트들(210)은 병렬의 세그먼트 지연 라인들을 포함할 수 있다. 하나의 지연 라인 세그먼트는 최소의 지연된 모노톤 신호를 생성하는 단지 하나의 지연 엘리먼트를 가질 수 있다. 다른 지연 라인 세그먼트는 최대의 지연된 모노톤 신호(230-N)를 생성하는 N 개의 지연 엘리먼트들을 가질 수 있다. 지연 라인들 내의 AND 게이트들 각각은 지연 라인을 초기의 알려진 상태로 설정하도록 지연 엘리먼트들 사이의 라인을 재설정하는 재설정 입력 RST를 가질 수 있다.
- [0021] [0028] 도 5를 참조하면, 복수의 재설정 가능한 지연 라인 세그먼트들(310)은 지연 라인을 따라 탬들을 포함할 수 있다. 세그먼트 지연 라인은 각각의 지연된 모노톤 신호들(230)을 생성하기 위해 라인을 따라 탬들을 가질 수 있다. 평가 신호 EVAL은 지연 엘리먼트들 사이에 AND 게이트를 사용하여 라인 세그먼트들을 재설정할 수 있다. 평가 신호는 클록 신호 CLK, 예를 들면, 1/2 클록 신호로부터 형성될 수 있다.
- [0022] [0029] 도 6을 참조하면, 평가 회로는, 클록에 응답하여, 각각의 재설정 가능한 지연 라인 세그먼트에 대한 각각의 지연된 모노톤 신호(230-N)를 래칭하기 위한 플립-플롭 또는 플립-플롭들의 쌍을 각각 갖는 검출 회로들을 사용할 수 있다.
- [0023] [0030] 모노톤 0-1 전환은 재설정 연산자들을 도입함으로써 달성될 수 있다. 각각의 재설정 연산자는 재설정 단계 동안에 감지 회로의 각각의 지연 라인을 임의의 설정-위반들과 독립적인 알려진 상태로 재설정할 수 있고, 반면에 회로는 평가 단계 동안에 감지한다. 재설정 연산자들 없이, 예상된 것보다 더 느린 주파수들을 검출하는 감지 회로는 미지의 상태에 있을 수 있다. 재설정 연산자를 구현하기 위한 몇몇의 방법들이 존재한다. 도 4 및 도 5에 도시된 바와 같이, AND-게이트들이 지연 라인(들)에 삽입될 수 있다. AND 게이트의 하나의 입력은 모노톤 0-1 신호에 의해 구동될 수 있고, 다른 입력은 부정(negated) 재설정 신호에 의해 구동될 수 있다. 각각의 AND-게이트는, 평가 기간 동안에 모노톤 0-1 신호를 전파하면서, 지연 라인의 자신의 부분이 재설정 기간 내에서 재설정되도록 허용한다.
- [0024] [0031] 본 발명의 기술은 예상된 것보다 더 빠른 및 더 느린 클록 주파수들을 검출할 수 있다. 이것은 또한 예상된 것보다 더 빠른 주파수들 또는 글리치들을 감지하기 위해 모노톤 신호의 설정-시간 위반을 검출할 수 있다. 설정-시간 위반들의 갯수에서의 실질적인 변화는 적응형 환경 무감각 센서를 제공하도록 검출될 수 있다. 온도와 같은 정상 환경적 변화들로 인한 작은 차이는 미리 결정된 검출 임계치 내에 있을 것이다. 탬퍼링(주파수 및/또는 전압)으로 인한 위반들의 큰 차이는 미리 결정된 검출 임계치를 넘어있을 것이다.
- [0025] [0032] 최장 전파 지연을 갖는 회로가 트리거링될 때, 클록 부재 조건(no-clock-present condition)이 검출될 수 있다. 이러한 트리거는 즉시 반응하기 위한 비동기 회로들에 의해 사용될 수 있거나, 클록이 다시 등장하고 난 이후에, 시스템이 반응하도록 상태 비트가 설정될 수 있다.
- [0026] [0033] 매우 높은 정상 상태 주파수 검출은 최단 지연 라인의 재설정 연산자들 사이의 지연에 의존한다. 이러

한 지연 라인을 재설정하는데 요구되는 시간이 더 짧을수록, 지연 라인을 재설정하기 위해 실제 할당되는 시간이 더 짧을 수 있다. 다른 감지 회로들의 재설정 연산자들 사이의 지연은 덜 긴박할 수 있고, 최고의 수용 가능한 동작 주파수에 의해 결정될 수 있다.

[0027] [0034] 변하는 설정 위반들의 갯수가 상당한지를 검출하기 위한 몇몇의 기술들이 사용될 수 있다. 하나의 방법은 각각의 검출 회로의 상태와 회로의 이전 상태를 XOR하고, 1들의 수와 임계치를 비교하는 것이다. 다른 방법은 STA(static timing analysis)를 사용하여 또는 교정 단계 동안에 예상된 주파수에 대응하는 특정 검출 회로를 결정하는 것이다. 이러한 특정 회로는 수위로서 작동하고, 더 짧은 지연 라인들과 연관된 회로들은 '0'을 측정할 것이고, 반면에 더 긴 지연 라인들과 연관된 회로들은 '1'을 측정할 것이다. 높은 수위 마크 및 낮은 수위 마크는 트리거로서 기능할 수 있다.

[0028] [0035] 몇몇의 변동들이 용이하게 구현될 수 있다는 것을 유의하라. 예로서, 검출/감지 회로는 모노톤 0-1 전환에 의존할 수 있고, 회로는 1로 재설정될 수 있다. 다른 예로서, 회로는 모노톤 1-0 및 0-1 전환들을 인터리빙할 수 있다. 다른 예로서, 재설정 연산자는, 재설정 신호에 기초하여 모노톤 신호와 재설정 값 사이에서 선택하는 MUX로 구현될 수 있다. 다른 예로서, 지연 라인은, 버퍼들, 페어링된 인버터들 또는 모노톤 신호 전환을 보장하는 임의의 회로로 구성될 수 있다. 다른 예로서, 무-클록 검출이 생략될 수 있다. 다른 예로서, '빠른'-라인(또는 임의의 다른 라인)은, 회로가 완전히 재설정된 것을 확인하기 위해 재설정-단계의 끝에서 샘플링될 수 있다. 다른 예로서, 검출 회로는 단지 2 개의 지연 라인 세그먼트들을 갖도록 감소될 수 있고, 하나는 높은 수위 마크에 대응하고, 다른 것은 낮은 수위 마크에 대응한다.

[0029] [0036] 본 발명의 다른 양상은 클록 탬퍼링을 검출하기 위한 장치에 상주할 수 있고, 상기 장치는 클록 CLK와 연관된 클록 평가 시간 기간(310) 동안에 모노톤 신호(220)를 제공하기 위한 수단(250), 최소 지연 시간과 최대 지연 시간 사이에서 이산적으로 증가하는 지연 시간들을 갖는 각각의 복수의 지연된 모노톤 신호들(230)을 생성하기 위해 복수의 재설정 가능한 지연 라인 세그먼트들을 사용하여 모노톤 신호를 지연시키기 위한 수단(210), 및 클록 결함을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용하는 평가 회로(240)를 트리거링하기 위해 클록 CLK를 사용하기 위한 수단(240)을 포함한다.

[0030] [0037] 본 발명의 다른 양상은 클록 탬퍼링을 검출하기 위한 장치에 상주할 수 있고, 상기 장치는 모노톤 신호(220)를 제공하는 회로(250), 복수의 재설정 가능한 지연 라인 세그먼트들(210) 및 평가 회로(240)를 포함한다. 회로(250)는 클록 CLK와 연관된 클록 평가 시간 기간(310) 동안에 모노톤 신호를 제공한다. 복수의 재설정 가능한 지연 라인 세그먼트들은 각각의 복수의 지연된 모노톤 신호들(230)을 생성하기 위해 모노톤 신호를 지연시킨다. 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트들(210-1) 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트들(210-N) 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 평가 회로(240)는 클록 CLK에 의해 트리거링되고, 클록 결함을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용한다.

[0031] [0038] 불균일한 듀티 사이클들을 갖는 클록-신호들은 듀얼 회로들: 클록 신호에 의해 구동되는 하나 및 부정 클록 신호에 의해 구동되는 다른 것을 사용함으로써 검출될 수 있다. 듀얼 회로들 없이, 재설정 기간을 증가시키지만 평가 기간을 일정하게 유지함으로써 주파수가 검출 불가하게 둔화될 수 있다. 듀얼 회로 접근법을 통해, 하나의 회로는 이러한 장시간 간격 동안에 평가 단계에 있는 것으로 보장될 것이다.

[0032] [0039] 또한 도 7을 참조하면, 본 발명의 다른 양상은 클록 탬퍼링을 검출하기 위한 장치에 상주할 수 있고, 상기 장치는 제 1 회로(750A), 제 1 복수의 재설정 가능한 지연 라인 세그먼트들(710), 제 2 회로(750B), 제 2 복수의 재설정 가능한 지연 라인 세그먼트들(720) 및 평가 회로(240)를 포함한다. 제 1 회로는 클록과 연관된 제 1 클록 평가 시간 기간 동안에 제 1 모노톤 신호를 제공한다. 제 1 복수의 재설정 가능한 지연 라인 세그먼트들 각각은 각각의 제 1 복수의 지연된 모노톤 신호들을 생성하기 위해 제 1 모노톤 신호를 지연시킨다. 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 제 2 회로는 클록과 연관된 제 2 클록 평가 시간 기간 동안에 제 2 모노톤 신호를 제공한다. 제 2 클록 평가 시간 기간은, 인버터(730)에 의해 강제될 수 있듯이, 제 1 클록 평가 시간 기간과 상이한 시간을 커버한다. 제 2 복수의 재설정 가능한 지연 라인 세그먼트들 각각은 각각의 제 2 복수의 지연된 모노톤 신호들을 생성하기 위해 제 1 모노톤 신호를 지연시킨다. 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 평가 회로는 클록(예를 들면, EVAL)에 의해 트리거링되고, 클록 결함을

검출하기 위해 제 1 복수의 지연된 모노톤 신호들 또는 제 2 복수의 지연된 모노톤 신호들을 사용한다. 멀티플렉서(760)는 제 1 또는 제 2 복수의 지연된 모노톤 신호들 중 어느 것이 평가 회로에 제공되도록 활성인지를 선택할 수 있다.

[0033] [0040] 본 발명의 기술은 정적 CMOS를 사용하는 결합 로직(combinatorial logic)에 기초하여 구현될 수 있고, 이것은 프로세서의 기존의 회로 통합에 기초하여 비교적 비용 효율적이다. 지연 라인들의 프로세스, 전압 및 온도 변동들에 대한 검출 보상은, 지연 라인들의 수 및 다중-주파수 계획 지원을 적응시킴으로써 달성될 수 있다. 결합 공격에 사용되는 전압 스파이크들이 검출될 수 있다. 이러한 전압 스파이크들은 전압을 감소시키고, 회로를 둔화시키고, 레지스터들에서 샘플링되는 불완전한 계산을 발생시킬 수 있다. 대안적으로, 전압의 증가는 회로 속도를 높이고, 레지스터들에서 샘플링되는 예상하지 않은 계산 또는 결과를 발생시킨다.

[0034] [0041] 도 2, 도 3 및 도 8을 참조하면, 본 발명의 다른 양상은 전압 탬퍼링을 검출하기 위한 방법(800)에 상주할 수 있다. 상기 방법에서, 복수의 재설정 가능한 지연 라인 세그먼트들(210)이 제공된다(단계 810). 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트(210-1) 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트(210-N) 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 클록 평가 시간 기간(310) 동안에 모노톤 신호(220)가 제공된다(단계 820). 모노톤 신호는, 각각의 복수의 지연된 모노톤 신호들(230)을 생성하기 위해 복수의 재설정 가능한 지연 라인 세그먼트들 각각을 사용하여 지연된다(단계 830). 클록은, 전압 결합을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용하는 평가 회로(240)를 트리거링하는데 사용된다(단계 840).

[0035] [0042] 본 발명의 더 상세한 양상들에서, 방법(800)은 재설정 시간 기간(320) 동안에 재설정 신호 RST를 사용하여 재설정 가능한 지연 라인 세그먼트들(210)을 재설정하는 것을 더 포함할 수 있다. 재설정 시간 기간은 클록 평가 시간 기간(310) 전에 있을 수 있다. 평가 회로(240)를 트리거링하기 위한 클록 CLK를 사용하는 것은 평가 회로를 트리거링하기 위해 클록 평가 시간 기간의 끝에서 클록 에지를 사용할 수 있다.

[0036] [0043] 본 발명의 다른 더 상세한 양상들에서, 복수의 지연된 모노톤 신호들(230) 각각은 1 또는 0 중 어느 하나를 포함할 수 있다. 평가 회로(240)는, 복수의 지연된 모노톤 신호들 내의 1들의 수가 미리 결정된 임계치보다 더 많이 수위 갯수와 상이한지를 결정할 수 있다. 수위 갯수는 하나 이상의 이전 클록 평가 시간(310)으로부터의 지연 모노톤 신호들에 기초하여 결정될 수 있다. 복수의 재설정 가능한 지연 라인 세그먼트들은 지연 라인을 따라 탭들을 포함할 수 있다. 대안적으로, 복수의 재설정 가능한 지연 라인 세그먼트들은 병렬의 지연 라인들을 포함한다.

[0037] [0044] 본 발명의 다른 양상은 전압 탬퍼링을 검출하기 위한 장치에 상주할 수 있고, 상기 장치는 평가 시간(310) 동안에 모노톤 신호(220)를 제공하기 위한 수단(250), 최소 지연 시간과 최대 지연 시간 사이에서 이산적으로 증가하는 지연 시간들을 갖는 각각의 복수의 지연된 모노톤 신호들(230)을 생성하기 위해 복수의 재설정 가능한 지연 라인 세그먼트들을 사용하여 모노톤 신호를 지연시키기 위한 수단(210), 및 전압 결합을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용하는 평가 회로(240)를 트리거링하기 위해 클록을 사용하기 위한 수단(240)을 포함한다.

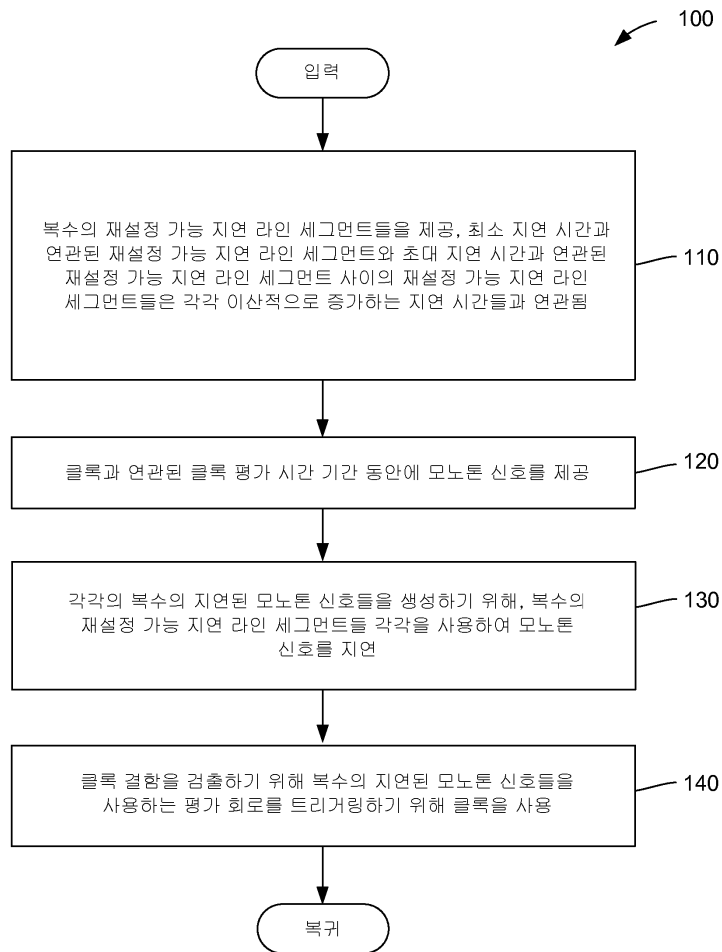
[0038] [0045] 본 발명의 다른 양상은 전압 탬퍼링을 검출하기 위한 장치에 상주할 수 있고, 상기 장치는 모노톤 신호(220)를 제공하는 회로(250), 복수의 재설정 가능한 지연 라인 세그먼트들(210) 및 평가 회로(240)를 포함한다. 회로(250)는 평가 시간 기간(310) 동안에 모노톤 신호를 제공한다. 복수의 재설정 가능한 지연 라인 세그먼트들은 각각의 복수의 지연된 모노톤 신호들(230)을 생성하기 위해 모노톤 신호를 지연시킨다. 최소 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트(210-1) 및 최대 지연 시간과 연관된 재설정 가능한 지연 라인 세그먼트(210-N) 사이의 재설정 가능한 지연 라인 세그먼트들 각각은 이산적으로 증가하는 지연 시간들과 연관된다. 평가 회로(240)는 클록 CLK에 의해 트리거링되고, 전압 결합을 검출하기 위해 복수의 지연된 모노톤 신호들을 사용한다.

[0039] [0046] 상기 설명 전체에 걸쳐 개시된 회로들은 데스크톱 또는 랩톱 컴퓨터, 태블릿, 모바일 디바이스, 셀룰러 텔레폰 등과 같은 컴퓨팅 시스템에 포함될 수 있다. 본원에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들 및 알고리즘 단계들이 전자 하드웨어 또는 하드웨어 및 컴퓨터 소프트웨어의 조합들로서 구현될 수 있다는 것을 당업자들은 또한 인지할 것이다. 그러한 기능이 하드웨어로 구현되는지 또는 소프트웨어로 구현되는지는 특정 애플리케이션 및 전체 시스템 상에 부여된 설계 제약들에 의존한다. 당업자들은 각각의 특정 애플리케이션에 대해 설명된 기능을 다양한 방식으로 구현할 수 있지만, 그러한 구현 결정은 본 발명의 범위에서 벗어나게 하는 것으로 해석되지 않아야 한다.

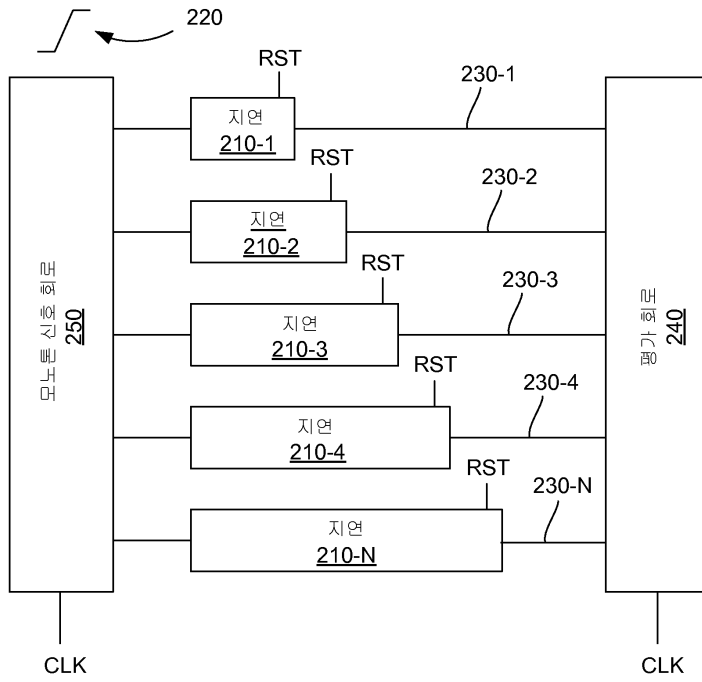
- [0040] [0047] 본원에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들 및 회로들은 범용 프로세서, 디지털 신호 프로세서(DSP), 주문형 집적 회로(ASIC), 필드 프로그래밍 가능 게이트 어레이(FPGA), 또는 다른 프로그래밍 가능 논리 디바이스, 이산 게이트 또는 트랜지스터 논리, 이산 하드웨어 컴포넌트들, 또는 본원에 설명된 기능들을 수행하도록 설계된 이들의 임의의 조합과 통합될 수 있다. 범용 프로세서는 마이크로 프로세서일 수 있지만, 대안적으로, 프로세서는 임의의 종래의 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수 있다. 프로세서는 또한 컴퓨팅 디바이스들의 조합, 예를 들면, DSP 및 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 함께 하나 이상의 마이크로프로세서들, 또는 임의의 다른 그러한 구성으로 구현될 수 있다.
- [0041] [0048] 본원에 개시된 실시예들과 관련하여 설명된 방법 또는 알고리즘의 단계들은 직접적으로 하드웨어로, 또는 프로세서에 의해 실행되는 하드웨어 및 소프트웨어 모듈의 조합으로 구현될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 착탈식 디스크, CD-ROM, 또는 당분야에 알려진 임의의 다른 형태의 저장 매체에 상주할 수 있다. 예시적인 저장 매체는, 프로세서가 저장 매체로부터 정보를 관독하고 정보를 저장 매체에 기록할 수 있도록 프로세서에 커플링된다. 대안적으로, 저장 매체는 프로세서에 통합될 수 있다. 프로세서 및 저장 매체는 ASIC에 상주할 수 있다. ASIC는 사용자 단말에 상주할 수 있다. 대안적으로, 프로세서 및 저장 매체는 컴퓨팅 시스템/사용자 단말 내의 이산 컴포넌트들로서 상주할 수 있다.
- [0042] [0049] 개시된 실시예들의 이전 설명이 임의의 당업자가 본 발명을 실시 또는 사용하는 것을 가능하게 하도록 제공된다. 이러한 실시예들의 다양한 수정들은 당업자들에게 용이하게 명백할 것이고, 본원에 정의된 일반적인 원리들은 본 발명의 사상 또는 범위에서 벗어나지 않고 다른 실시예들에 적용될 수 있다. 따라서, 본 발명은 본원에 도시된 실시예들로 제한되도록 의도되지 않지만, 본원에 개시된 원리들 및 신규한 특징들과 일치하는 최광의 범위를 따른다.

도면

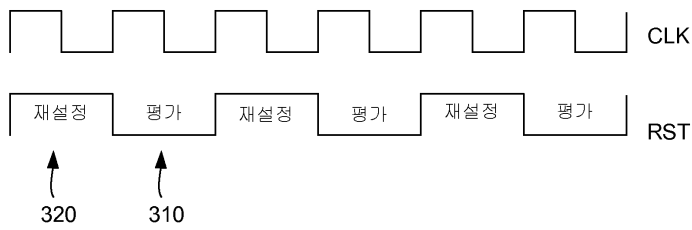
도면1



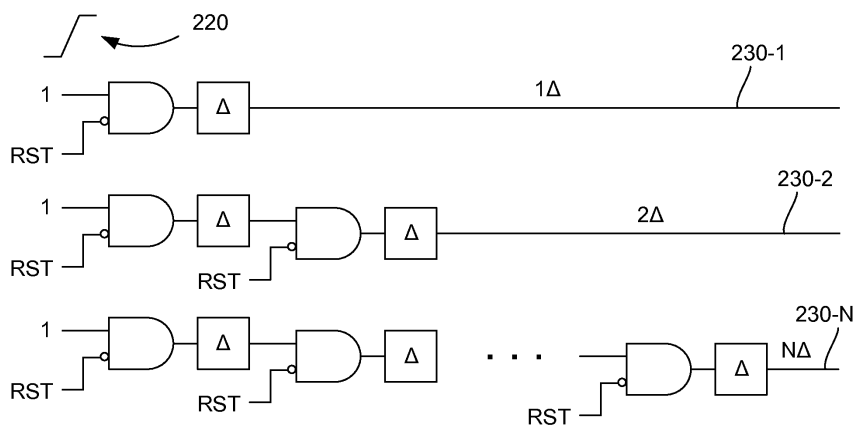
도면2



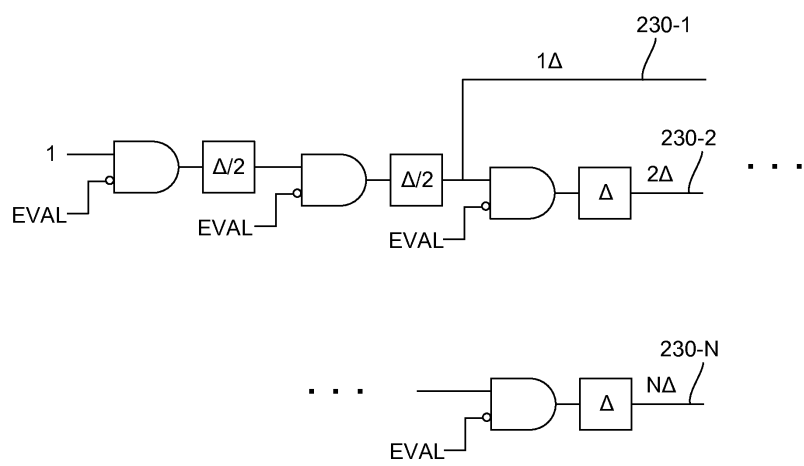
도면3



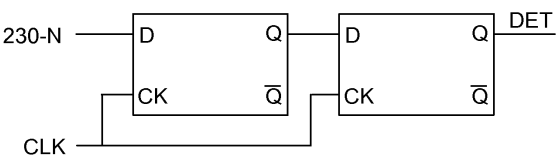
도면4



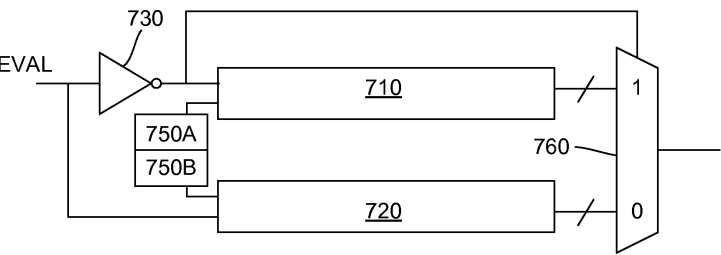
도면5



도면6



도면7



도면8

