



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0135652
(43) 공개일자 2022년10월07일

(51) 국제특허분류(Int. Cl.)
G06F 7/58 (2006.01)

(52) CPC특허분류
G06F 7/588 (2013.01)

(21) 출원번호 10-2021-0041628

(22) 출원일자 2021년03월31일

심사청구일자 2021년03월31일

(71) 출원인
고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

김철우

서울특별시 강남구 선릉로 221

박윤수

서울특별시 성북구 안암로7길 44

전진우

서울특별시 강남구 선릉로112길 53(삼성동, 롯데캐슬킹덤아파트)

(74) 대리인

특허법인주연케이알피

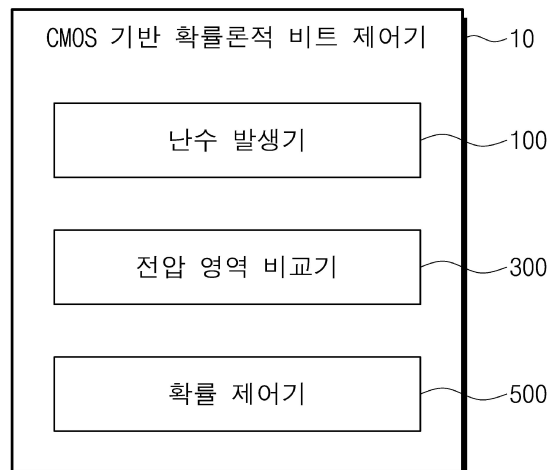
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 CMOS 기반의 난수 발생기를 이용한 확률론적 비트 제어기 및 그 동작방법

(57) 요약

본 발명은 CMOS 기반 확률론적 비트 제어기에 관한 것으로, 좀 더 자세하게는 CMOS 기반의 난수 발생기를 이용한 확률론적 비트 제어기에 관한 것이다. 본 발명의 일 실시예에 따른 확률론적 비트 제어기는 CMOS 기반의 적어도 하나의 적분기의 동작을 통해 노이즈 전압을 얻는 난수 발생기, 상기 노이즈 전압을 디지털화 하는 전압 영역 비교기, 및 상기 전압 영역 비교기의 문턱 전압에 기초하여, 상기 전압 영역 비교기의 디지털 출력의 확률을 제어하는 확률 제어기를 포함한다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	1711110467
과제번호	2019R1A2B5B03100756
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)(R&D)
연구과제명	레퍼런스 및 기생 성분에 둔감한 커패시턴스-디지털 변환기 구현
기 여 율	1/1
과제수행기관명	고려대학교
연구기간	2020.03.01 ~ 2021.02.28

명세서

청구범위

청구항 1

CMOS 기반의 적어도 하나의 적분기의 동작을 통해 노이즈 전압을 얻는 난수 발생기;

상기 노이즈 전압을 디지털화 하는 전압 영역 비교기; 및

상기 전압 영역 비교기의 문턱 전압에 기초하여, 상기 전압 영역 비교기의 디지털 출력의 확률을 제어하는 확률 제어기를 포함하는, 확률론적 비트 제어기.

청구항 2

제1항에 있어서,

상기 난수 발생기는,

상기 노이즈 전압을 생성하는 상기 CMOS 기반의 적어도 하나의 동적 노이즈 적분기;

일정한 클럭신호에 기반하여 상기 클럭신호에 따라 동기화된 상기 노이즈 전압을 출력하도록 동작하는 하나의 스위치; 및

상기 노이즈 전압을 저장하는 캐패시터를 포함하는, 확률론적 비트 제어기.

청구항 3

제2항에 있어서,

상기 노이즈 전압은 제1 및 제2 획득 방법 중 적어도 하나를 통해 노이즈 전압을 생성하고,

상기 제1 획득 방법은 상기 클럭신호에 따라 변하는 상기 CMOS의 노이즈 전압을 획득하는 방법이고,

상기 제2 획득 방법은 상기 클럭신호가 1에서 0으로 변화할 때의 노이즈와 그 시점에서의 노드 전압의 기울기에 비례한 노이즈 전압을 획득하는 방법인, 확률론적 비트 제어기.

청구항 4

제1항에 있어서,

상기 확률 제어기는 상기 전압 영역 비교기의 상기 문턱 전압을 변화시킴으로써 상기 디지털 출력의 확률을 제어하는, 확률론적 비트 제어기.

청구항 5

제1항에 있어서,

상기 난수 발생기는,

제1 및 제2 제거 방법을 통해 낮은 주파수 영역에 존재하는 노이즈를 제거하는, 확률론적 비트 제어기.

청구항 6

제5항에 있어서,

상기 제1 제거 방법은 추가 캐패시터를 통해 노이즈를 서로 빼줌으로써 낮은 주파수 영역의 노이즈를 제거하는 방법이고,

상기 제2 제거 방법은 상기 동적 노이즈 적분기를 복수개 사용함으로써, 인접한 두 노이즈의 연관성이 떨어뜨려, 상기 낮은 주파수 영역의 노이즈를 출력하는 않는 방법인, 확률론적 비트 제어기.

청구항 7

제6항에 있어서,

상기 제1 제거 방법은 상기 추가 캐패시터에 노이즈 전압을 저장하고, 기존의 캐패시터에 노이즈 전압을 저장하여, 두 캐패시터에 저장된 노이즈 전압의 차를 상기 전압 영역 비교기에 입력하는, 확률론적 비트 제어기.

청구항 8

CMOS 기반의 적어도 하나의 적분기의 동작을 통해 노이즈 전압을 얻는 단계;

전압 영역 비교기가 상기 노이즈 전압을 디지털화 하는 단계; 및

상기 전압 영역 비교기의 문턱 전압에 기초하여, 상기 디지털화된 노이즈 전압의 확률을 제어하는 단계를 포함하는, 확률론적 비트 제어기의 동작방법.

청구항 9

제8항에 있어서,

상기 노이즈 전압을 얻는 단계는,

캐패시터의 상단 전압을 VDD로 충전하는 단계;

상기 캐패시터의 상단 전압을 클럭신호에 맞춰 상기 동적 노이즈 적분기의 전류로 방전하는 단계; 및

상기 클럭신호가 1에서 0이 될 때 방전을 멈추는 단계를 포함하는, 확률론적 비트 제어기의 동작방법.

청구항 10

제9항에 있어서,

상기 클럭신호가 1에서 0이 될 때 방전을 멈추는 단계 이후에,

상기 캐패시터에 저장된 노이즈 전압을 획득하는 단계 및 상기 클럭신호의 변화 시점에서의 노이즈와 상기 클럭신호의 변화 시점에서의 V_n 노드 전압의 기울기에 비례한 노이즈 전압을 획득하는 단계 중 적어도 하나를 동작하는, 확률론적 비트 제어기의 동작방법.

청구항 11

제8항에 있어서,

상기 디지털 출력의 확률을 제어하는 단계는, 상기 디지털화된 노이즈 전압의 문턱 전압을 변화시킴으로써 상기 디지털 출력의 확률을 제어하는, 확률론적 비트 제어기의 동작방법.

발명의 설명

기술 분야

[0001] 본 발명은 CMOS 기반 확률론적 비트 제어기에 관한 것으로, 좀 더 자세하게는 CMOS 기반의 난수 발생기를 이용한 확률론적 비트 제어기에 관한 것이다.

배경 기술

[0002] 정보 통신 기술의 발전에 따라서, 정보의 암호화 및 복호화 기술은 해당 정보의 보안 유지를 위하여 매우 중요시되고 있다. 난수(random number)는 보안 시스템(security system)의 비밀키(secret key)를 비롯한 여러 곳에서 사용된다. 따라서, 보안이 중요시되는 시스템은 난수 발생기(random number generator)가 구비되며, 상기 난수 발생기는 예측 불가능한 값을 갖는 난수를 발생시켜야만 한다. 보안이 중요시되는 시스템에 있어서, 난수는 주기성과 규칙성을 가져서는 안 된다. 즉, 보안 시스템에서는 예측이 불가능하고 어떠한 주기성도 갖지 않는 완전한 난수를 발생시킬 필요가 있는 것이다.

[0003] 또한, 난수 발생기에 인가되는 전원 전압 및/또는 접지 전압에 노이즈가 포함되는 경우에는 발생된 난수의 랜덤

성이 악화되는 문제가 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명은 CMOS 공정을 통한 난수 발생기를 이용한 확률론적 비트를 구현하는 CMOS 기반 확률론적 비트 제어기를 제공하는 것에 목적이 있다.

과제의 해결 수단

[0005] 본 발명의 일 실시예에 따른 확률론적 비트 제어기는 CMOS 기반의 적어도 하나의 적분기의 동작을 통해 노이즈 전압을 얻는 난수 발생기, 상기 노이즈 전압을 디지털화 하는 전압 영역 비교기, 및 상기 전압 영역 비교기의 문턱 전압에 기초하여, 상기 전압 영역 비교기의 디지털 출력의 확률을 제어하는 확률 제어기를 포함한다.

[0006] 본 발명의 일 실시예에 있어서, 상기 난수 발생기는, 상기 노이즈 전압을 생성하는 상기 CMOS 기반의 적어도 하나의 동적 노이즈 적분기, 일정한 클럭신호에 기반하여 상기 클럭신호에 따라 동기화된 상기 노이즈 전압을 출력하도록 동작하는 하나의 스위치, 및 상기 노이즈 전압을 저장하는 캐패시터를 포함할 수 있다.

[0007] 본 발명의 일 실시예에 있어서, 상기 노이즈 전압은 제1 및 제2 획득 방법 중 적어도 하나를 통해 노이즈 전압을 생성하고, 상기 제1 획득 방법은 상기 클럭신호에 따라 변하는 상기 CMOS의 노이즈 전압을 획득하는 방법이고, 상기 제2 획득 방법은 상기 클럭신호가 1에서 0으로 변화할 때의 노이즈과 그 시점에서의 노드 전압의 기울기에 비례한 노이즈 전압을 획득하는 방법일 수 있다.

[0008] 본 발명의 일 실시예에 있어서, 상기 확률 제어기는 상기 전압 영역 비교기의 상기 문턱 전압을 변화시킴으로써 상기 디지털 출력의 확률을 제어할 수 있다.

[0009] 본 발명의 일 실시예에 있어서, 상기 난수 발생기는 제1 및 제2 제거 방법을 통해 낮은 주파수 영역에 존재하는 노이즈를 제거할 수 있다.

[0010] 본 발명의 일 실시예에 있어서, 상기 제1 제거 방법은 추가 캐패시터를 통해 노이즈를 서로 빼줌으로써 낮은 주파수 영역의 노이즈를 제거하는 방법이고, 상기 제2 제거 방법은 상기 동적 노이즈 적분기를 복수개 사용함으로써, 인접한 두 노이즈의 연관성이 떨어뜨려, 상기 낮은 주파수 영역의 노이즈를 출력하는 않는 방법일 수 있다.

[0011] 본 발명의 일 실시예에 있어서, 상기 제1 제거 방법은 상기 추가 캐패시터에 노이즈 전압을 저장하고, 기존의 캐패시터에 노이즈 전압을 저장하여, 두 캐패시터에 저장된 노이즈 전압의 차를 상기 전압 영역 비교기에 입력할 수 있다.

[0012] 본 발명의 일 실시예에 따른 확률론적 비트 제어기의 동작 방법은, CMOS 기반의 적어도 하나의 적분기의 동작을 통해 노이즈 전압을 얻는 단계, 전압 영역 비교기가 상기 노이즈 전압을 디지털화 하는 단계, 및 상기 전압 영역 비교기의 문턱 전압에 기초하여, 상기 디지털화된 노이즈 전압의 확률을 제어하는 단계를 포함한다.

[0013] 본 발명의 일 실시예에 있어서, 상기 노이즈 전압을 얻는 단계는 캐패시터의 상단 전압을 VDD로 충전하는 단계, 상기 캐패시터의 상단 전압을 클럭신호에 맞춰 상기 동적 노이즈 적분기의 전류로 방전하는 단계, 및 상기 클럭신호가 1에서 0이 될 때 방전을 멈추는 단계를 포함할 수 있다.

[0014] 본 발명의 일 실시예에 있어서, 상기 클럭신호가 1에서 0이 될 때 방전을 멈추는 단계 이후에, 상기 캐패시터에 저장된 노이즈 전압을 획득하는 단계 및 상기 클럭신호의 변화 시점에서의 노이즈와 상기 클럭신호의 변화 시점에서의 V_n 노드 전압의 기울기에 비례한 노이즈 전압을 획득하는 단계 중 적어도 하나를 동작할 수 있다.

[0015] 본 발명의 일 실시예에 있어서, 상기 디지털 출력의 확률을 제어하는 단계는, 상기 디지털화된 노이즈 전압의 문턱 전압을 변화시킴으로써 상기 디지털 출력의 확률을 제어할 수 있다.

발명의 효과

[0016] 본 발명의 CMOS 기반 확률론적 비트 제어기는 CMOS 공정을 통한 난수 발생기를 이용한 확률론적 비트를 구현할 수 있다.

[0017] 본 발명의 CMOS 기반 확률론적 비트 제어기는 CMOS 공정을 이용한 난수 발생기를 구현함으로써 에너지 효율을

높일 수 있다.

도면의 간단한 설명

- [0018] 도 1은 본 발명의 일 실시예에 따른 CMOS 기반 확률론적 비트 제어기를 나타낸 블록도이다.
- 도 2는 본 발명의 일 실시예에 따른 난수 발생기를 나타낸 회로도이다.
- 도 3은 본 발명의 일 실시예에 따른 제1 획득 방법으로 노이즈 전압을 생성하는 방법을 도시한 회로도이다.
- 도 4는 본 발명의 일 실시예에 따른 제2 획득 방법으로 노이즈 전압을 생성하는 방법을 도시한 회로도이다.
- 도 5는 본 발명의 일 실시예에 따른 제1 제거 방법을 도시한 회로도이다.
- 도 6은 본 발명의 일 실시예에 따른 제2 제거 방법을 도시한 회로도이다.
- 도 7은 본 발명의 일 실시예에 따른 확률 제어기의 동작을 나타낸 도면이다.
- 도 8은 본 발명의 일 실시예에 따른 CMOS 기반 확률론적 비트 제어기의 동작 방법을 도시한 순서도이다.
- 도 9는 본 발명의 일 실시예에 따른 난수 발생기의 동작방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0019] 이하, 첨부된 도면을 참조하여 본 개시(present disclosure)를 설명한다. 본 개시는 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들이 도면에 예시되고 관련된 상세한 설명이 기재되어 있다. 그러나, 이는 본 개시를 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 개시의 사상 및 기술 범위에 포함되는 모든 변경 및/또는 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 도면의 설명과 관련하여, 유사한 구성요소에 대해서는 유사한 참조 부호가 사용되었다.
- [0020] 본 개시 가운데 사용될 수 있는 "포함한다" 또는 "포함할 수 있다" 등의 표현은 개시된 해당 기능, 동작 또는 구성요소 등의 존재를 가리키며, 추가적인 하나 이상의 기능, 동작 또는 구성요소 등을 제한하지 않는다. 또한, 본 개시에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0021] 본 개시에서 "또는" 등의 표현은 함께 나열된 단어들의 어떠한, 그리고 모든 조합을 포함한다. 예를 들어, "A 또는 B"는, A를 포함할 수도, B를 포함할 수도, 또는 A 와 B 모두를 포함할 수도 있다.
- [0022] 본 개시 가운데 "제 1," "제2," "첫째," 또는 "둘째," 등의 표현들이 본 개시의 다양한 구성요소들을 수식할 수 있지만, 해당 구성요소들을 한정하지 않는다. 예를 들어, 상기 표현들은 해당 구성요소들의 순서 및/또는 중요도 등을 한정하지 않는다. 상기 표현들은 한 구성요소를 다른 구성요소와 구분 짓기 위해 사용될 수 있다. 예를 들어, 제1 사용자 기기와 제 2 사용자 기기는 모두 사용자 기기이며, 서로 다른 사용자 기기를 나타낸다. 예를 들어, 본 개시의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다.
- [0023] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해될 수 있어야 할 것이다.
- [0024] 본 개시에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 개시를 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.
- [0025] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 개시에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

- [0026] 도 1은 본 발명의 일 실시예에 따른 CMOS 기반 확률론적 비트 제어기를 나타낸 블록도이다.
- [0027] 도 1을 참조하면, CMOS 기반 확률론적 비트 제어기(10)는 난수 발생기(100), 전압 영역 비교기(300), 및 확률 제어기(500)를 포함한다.
- [0028] 난수 발생기(100)는 적어도 하나의 적분기의 동작을 통해 노이즈 전압을 획득할 수 있다. 이때, 적어도 하나의 적분기는 CMOS 기반의 동적 노이즈 적분기일 수 있다.
- [0029] 즉, 난수 발생기(100)는 CMOS 기반의 적어도 하나의 동적 노이즈 적분기의 동작을 통해 노이즈 전압을 획득할 수 있다. 이때, 난수 발생기(100)는 랜덤한 출력인 노이즈 전압을 제공하기 위해서 노이즈가 심한 소자를 이용하거나 CMOS 소자를 이용할 수 있다. 일 실시예에 있어서, 난수 발생기(100)는 CMOS 기반의 동적 노이즈 적분기, 스위치, 및 캐패시터(150)로 구현될 수 있으며, 구체적인 내용은 도 2에서 후술될 것이다.
- [0030] 난수 발생기(100)는 두 가지의 방법을 통해 노이즈 전압을 획득할 수 있다. 이와 관련된 구체적인 내용은 도 3 및 도 4에서 후술될 것이다.
- [0031] 전압 영역 비교기(300)는 난수 발생기(100)에서 획득한 노이즈 전압을 디지털화 하여 디지털 출력을 생성할 수 있다. 즉, 전압 영역 비교기(300)는 난수 발생기(100)에서 출력된 노이즈 전압을 0 또는 1 중 적어도 하나로 디지털화할 수 있다.
- [0032] 확률 제어기(500)는 전압 영역 비교기(300)의 문턱 전압에 기초하여, 전압 영역 비교기(300)의 출력인 디지털 출력의 확률을 제어할 수 있다. 즉, 확률 제어기(500)는 0 또는 1의 출력 확률을 조절할 수 있다. 예를 들어, 확률 제어기(500)는 전압 영역 비교기(300)의 문턱 전압을 변화시킴으로써, 디지털 출력의 확률을 조절할 수 있다. 이와 관련된 구체적인 내용은 도 7에서 후술될 것이다.
- [0033] 상술한 바와 같이, CMOS 기반 확률론적 비트 제어기(10)는 CMOS 기반의 적어도 하나의 동적 노이즈 적분기의 동작을 통해 노이즈 전압을 획득할 수 있다. 또한, 난수 발생기(100)에서 획득한 노이즈 전압을 디지털화 하여 디지털 출력을 생성하고, 생성된 디지털 출력의 확률을 제어할 수 있다.
- [0034] 상기와 같은 구조를 가지는 CMOS 기반 확률론적 비트 제어기(10)는 CMOS 공정을 통한 난수 발생기(100)를 이용한 확률론적 비트를 구현할 수 있다. 또한, CMOS 기반 확률론적 비트 제어기(10)는 CMOS 공정을 이용한 난수 발생기(100)를 구현함으로써 에너지 효율을 높일 수 있다.
- [0035] 도 2는 본 발명의 일 실시예에 따른 난수 발생기(100)를 나타낸 회로도이다.
- [0036] 도 2를 참조하면, 난수 발생기(100)는 적어도 하나의 동적 노이즈 적분기(110), 스위치(130), 및 캐패시터(150)를 포함할 수 있다.
- [0037] 적어도 하나의 동적 노이즈 적분기(110)는 노이즈 전압을 생성할 수 있다. 적어도 하나의 동적 노이즈 적분기(110)는 NMOS 트랜지스터로 구성되어 있을 수 있다. 예를 들어, 적어도 하나의 동적 노이즈 적분기(110)는 NMOS 트랜지스터의 전류원, 노이즈 전류, 및 내부 저항을 포함할 수 있다.
- [0038] 적어도 하나의 동적 노이즈 적분기(110)는 동적 적분 과정에서, V_n 노드를 NMOS의 베이스 전류로 방전하는 동시에, 노이즈 전류를 통해 캐패시터(150)에 노이즈를 저장할 수 있다. 이에 대한 자세한 설명은 도 3에서 후술될 것이다.
- [0039] 동적 노이즈 적분기(110)는 두 가지의 방법을 통해 노이즈 전압을 획득할 수 있다. 제1 획득 방법은 클럭신호에 따라 변하는 CMOS의 노이즈 전압을 획득하는 방법이고, 제2 획득 방법은 클럭신호가 1에서 0으로 변화할 때의 노이즈와 그 시점에서의 노드 전압의 기울기에 비례한 노이즈 전압을 획득하는 방법일 수 있다. 이와 관련된 자세한 내용은 도 3 및 도 4에서 후술될 것이다.
- [0040] 난수 발생기(100)를 CMOS 공정을 통해 구현함으로써, MJT 공정을 사용하는 기존의 공정보다 복잡도를 낮출 수 있다. 또한, 난수 발생기(100)가 동적 동작을 수행함으로써, 저전력 및 저면적 구현이 가능하도록 할 수 있다.
- [0041] 스위치(130)는 일정한 클럭신호에 기반하여 클럭신호에 따라 동기화된 상기 노이즈 전압을 출력하도록 동작할 수 있다. 예를 들어, 동적 노이즈 적분기(110)가 두 개일 때, 스위치(130) 클럭은 입력 클럭이 제1 동적 노이즈 적분기(111) 및 제2 동적 노이즈 적분기(113)에 입력됨과 동시에 1이 되어, 입력단과 출력단을 연결해줌으로써, 난수 발생기(100)가 동작되도록 할 수 있다. 반면, 클럭이 0이 되는 순간, 스위치(130) 클럭 또한 0이 되어, 난수 발생기(100)의 동작이 멈추도록 동작될 수 있다.

- [0042] 캐패시터(150)는 동적 노이즈 적분기(110)의 노이즈 전류로부터 노이즈 전압을 저장할 수 있다. 캐패시터(150)에 저장된 전압은 V_n 전압일 수 있으며, 난수 발생기(100)는 이 전압을 전압 영역 비교기로 전달할 수 있다.
- [0043] 도 3은 본 발명의 일 실시예에 따른 제1 획득 방법으로 노이즈 전압을 생성하는 방법을 도시한 회로도이다.
- [0044] 도 3을 참조하면, 제1 획득 방법은 클럭신호에 따라 변하는 CMOS의 노이즈 전압을 획득하는 방법일 수 있다.
- [0045] 구체적으로, 제1 획득 방법은 캐패시터(150) 상단 전압 V_n 을 VDD로 미리 충전시켜 놓고, 클럭신호가 0에서 1로 되는 순간에 동적 노이즈 적분기(110)의 전류로 캐패시터를 방전시킨다. 클럭신호가 1에서 0이 되는 순간, 스위치(130)가 꺼지면서 방전이 멈추게 된다. 그때 캐패시터(150)에 저장된 전압을 획득함으로써, 노이즈 전압을 획득할 수 있다. 이때, 동적 노이즈 적분기(110)의 전류는 CMOS의 베이스 전류(I_B)와 노이즈 전류($\bar{I}_n$)의 합일 수 있다.
- [0046] 이때, 제1 획득 방법은 클럭신호가 0에서 1로 되는 동작시 시간에 따라 변하는 CMOS의 노이즈 전류에 의해 V_n 은 각 시행마다 다른 값을 가질 수 있다.
- [0047] 도 4는 본 발명의 일 실시예에 따른 제2 획득 방법으로 노이즈 전압을 생성하는 방법을 도시한 회로도이다.
- [0048] 도 4를 참조하면, 제2 획득 방법은 클럭신호가 1에서 0으로 변화할 때의 노이즈와 그 시점에서의 노드 전압의 기울기에 비례한 노이즈 전압을 획득할 수 있다.
- [0049] 구체적으로, 제2 획득 방법은 캐패시터 상단 전압 V_n 을 VDD로 미리 충전시켜 놓고, 클럭신호가 0에서 1로 되는 순간에 동적 노이즈 적분기의 전류로 캐패시터를 방전시킨다. 클럭신호가 1에서 0이 되는 순간 방전이 멈춘다. 그 때, 노이즈로 인하여 시간 영역에서 클럭신호에 노이즈가 발생하게 된다. 예를 들어, 클럭신호의 변화 시점의 시간 영역에서 σ_t 의 노이즈를 갖고 있다면, σ_t 와 그 시점에서의 V_n 노드 전압의 기울기에 비례한 노이즈가 캐패시터에 저장된다. 이때, 동적 노이즈 적분기의 전류는 CMOS의 베이스 전류와 노이즈 전류의 합일 수 있다.
- [0050] 즉, 제2 획득 방법은 클럭신호가 1에서 0이 되는 순간의 노이즈(σ_t)와 그 순간에서의 시간에 따른 V_n 의 변화량을 곱한 값일 수 있다.
- [0051] 도 5는 본 발명의 일 실시예에 따른 제1 제거 방법을 도시한 회로도이다.
- [0052] 도 5를 참조하면, 제1 제거 방법은 추가 캐패시터(151)를 통해 노이즈를 서로 빼줌으로써 낮은 주파수 영역의 노이즈를 제거하는 방법일 수 있다.
- [0053] 제1 제거 방법은 기존의 캐패시터(152)외에 같은 캐패시턴스를 갖는 캐패시터(151)를 추가하여, 하나의 캐패시터가 연결될 경우 다른 캐패시터는 플로팅 상태로 동작하도록 한다. 즉, 하나의 노이즈 전압을 생성하기 위하여 노이즈 전압 획득 동작을 두 번 하도록 한다.
- [0054] 제1 제거 방법은 추가 캐패시터(151)에 노이즈 전압을 저장하고, 기존의 캐패시터(152)에 노이즈 전압을 저장하여, 두 캐패시터에 저장된 노이즈 전압의 차를 전압 영역 비교기에 입력한다.
- [0055] 구체적으로, 스위치 S1(131)을 턴 온(Turn On) 한 동안에는 위쪽의 캐패시터(151)인 C1에 노이즈를 저장하고, 밑쪽의 캐패시터(152)인 C2는 플로팅 상태를 유지한다. 그 후, 스위치(132) S2를 턴 온하여 C2에 노이즈를 저장하게 된다. 그 결과, $V_{n,1f}$ 는 두 캐패시터에 저장된 전압의 차이를 갖게됨으로써, 낮은 주파수 영역에 존재하는 노이즈를 제거할 수 있다.
- [0056] 도 6은 본 발명의 일 실시예에 따른 제2 제거 방법을 도시한 회로도이다.
- [0057] 도 6을 참조하면, 제2 제거 방법은 복수개의 동적 노이즈 적분기(110_1~110_n)를 사용함으로써, 인접한 두 노이즈의 연관성이 떨어뜨려, 낮은 주파수 영역의 노이즈를 출력하는 않는 방법일 수 있다.
- [0058] 낮은 주파수의 노이즈는 시간영역에서 느리게 변화하므로, 한 개의 동적 노이즈 적분기를 통하여 난수를 발생시켰을 경우, 연속되는 출력들에 동일한 노이즈 성분이 포함되게 된다. 즉, 인접한 비트의 연관성이 생기게 된다.
- [0059] 따라서, 복수개의 동적 노이즈 적분기(110_1~110_n)를 통해 여러개의 노이즈 전압을 생성하고, 여러개의 노이즈 전압이 순차적으로 섞이면서 낮은 주파수 영역의 노이즈를 출력하지 않을 수 있다.
- [0060] 도 7은 본 발명의 일 실시예에 따른 확률 제어기의 동작을 나타낸 도면이다.

- [0061] 도 7을 참조하면, 확률 제어기는 상기 전압 영역 비교기의 문턱 전압을 변화시킴으로써 상기 디지털 출력의 확률을 제어할 수 있다.
- [0062] 구체적으로, 노이즈 전압이 평균 m 과 표준편차 σ 의 전압을 갖는다면, 전압 영역 비교기의 문턱 전압을 변화시킴으로써, 디지털 출력이 가능할 수 있다.
- [0063] 예를 들어, 문턱 전압이 1σ 의 전압을 가질 경우, 문턱전압의 오른쪽 부분의 경우는 출력 1을 가지는 경우이고, 왼쪽 부분의 경우는 출력 0을 가지는 경우일 수 있다. 즉, 이 경우에는 출력이 0이 나올 확률이 많다.

표 1

Voff(D)	0이 나올 확률	1이 나올 확률
-3σ	0.001	0.999
-2σ	0.022	0.978
-1σ	0.158	0.842
0	0.500	0.500
1σ	0.842	0.158
2σ	0.978	0.022
3σ	0.999	0.001

- [0065] 표 1은 문턱 전압에 따른 확률의 예시를 나타낸 표이다.
- [0066] 표를 참조하면, 문턱 전압이 왼쪽으로 갈수록 1이 나올 확률이 높아지고, 문턱 전압이 오른쪽으로 갈수록 0이 나올 확률이 높아지게 된다.
- [0067] 도 8은 본 발명의 일 실시예에 따른 CMOS 기반 확률론적 비트 제어기의 동작 방법을 도시한 순서도이다.
- [0068] 도 8을 참조하면, S100 단계는 난수 발생기가 동적 노이즈 적분기의 동작을 통해 노이즈 전압을 획득하는 단계일 수 있다. 예를 들어, 동적 노이즈 적분기는 동적 적분 과정에서, V_n 노드를 NMOS의 베이스 전류로 방전하는 동시에, 노이즈 전류를 통해 캐패시터에 노이즈를 저장할 수 있다.
- [0069] S300 단계는 전압 영역 비교기가 획득된 노이즈 전압을 디지털화하는 단계일 수 있다. 예를 들어, 난수 발생기에서 출력된 노이즈 전압을 0 또는 1 중 적어도 하나로 디지털화할 수 있다.
- [0070] S500 단계는 확률 제어기가 전압 영역 비교기의 문턱 전압에 기초하여, 디지털화된 노이즈 전압의 확률을 제어하는 단계일 수 있다. 예를 들어, 전압 영역 비교기의 문턱 전압을 변화시킴으로써, 디지털 출력의 확률을 조절할 수 있다.
- [0071] 도 9는 본 발명의 일 실시예에 따른 난수 발생기의 동작방법을 도시한 순서도이다.
- [0072] 도 9를 참조하면, S110 단계는 캐패시터의 상단 전압을 VDD로 충전하는 단계일 수 있다.
- [0073] S130 단계는 캐패시터의 전압을 클럭 신호에 맞춰 방전하는 단계일 수 있다. 예를 들어, 클럭신호가 0에서 1로 되는 순간에 동적 노이즈 적분기의 전류로 캐패시터를 방전시킬 수 있다. 이때, 동적 노이즈 적분기의 전류는 CMOS의 베이스 전류와 노이즈 전류의 합일 수 있다.
- [0074] S150 단계는 클럭신호가 1에서 0이될 때 방전을 멈추는 단계일 수 있다.
- [0075] S171 단계는 캐패시터에 저장된 노이즈 전압을 획득하는 단계일 수 있다. 예를 들어, 클럭신호가 1에서 0이 되는 순간에 캐패시터에 저장된 노이즈 전압을 획득할 수 있다. 이때, 클럭신호가 0에서 1로 되는 동작시 시간에 따라 변하는 CMOS의 노이즈 전류에 의해 V_n 은 각 시행마다 다른 값을 가질 수 있다.
- [0076] S173 단계는 S150 단계에서 클럭신호가 1에서 0으로 변화되는 순간의 노이즈와 그 시점에서의 V_n 노드 전압의 기울기에 비례한 노이즈 전압을 획득할 수 있다. 예를 들어, 클럭신호의 변화 시점의 시간 영역에서 σ_t 의 노이즈를 갖고 있다면, σ_t 와 그 시점에서의 V_n 노드 전압의 기울기에 비례한 노이즈가 캐패시터에 저장된다. 즉, 클럭신호가 1에서 0이 되는 순간의 노이즈(σ_t)와 그 순간에서의 시간에 따른 V_n 의 변화량을 곱한 값일 수 있다.
- [0077] 상술한 바와 같이, CMOS 기반 확률론적 비트 제어기의 동작 방법은 CMOS 기반의 적어도 하나의 동적 노이즈 적분기의 동작을 통해 노이즈 전압을 획득하고, 난수 발생기에서 획득한 노이즈 전압을 디지털화 하여 디지털 출

력을 생성하고, 생성된 디지털 출력의 확률을 제어할 수 있다.

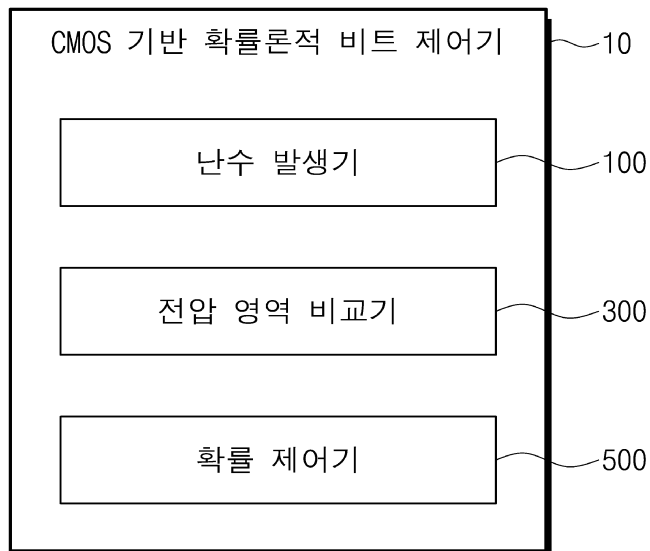
[0078] 상기와 같은 구조를 가지는 CMOS 기반 확률론적 비트 제어기는 CMOS 공정을 통한 난수 발생기를 이용한 확률론적 비트를 구현할 수 있다. 또한, CMOS 기반 확률론적 비트 제어기는 CMOS 공정을 이용한 난수 발생기를 구현함으로써 에너지 효율을 높일 수 있다.

부호의 설명

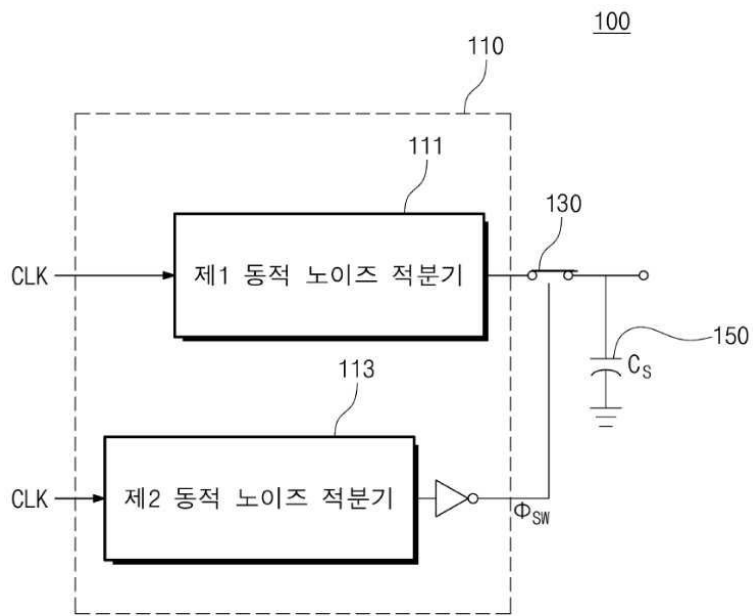
[0079] 10 : CMOS 기반 확률론적 비트 제어기
 100 : 난수 발생기
 110 : 동적 노이즈 적분기
 111 : 제1 동적 노이즈 적분기
 113 : 제2 동적 노이즈 적분기
 130, 131, 132 : 스위치
 150, 151, 152 : 캐패시터
 200 : 전압 영역 비교기
 300 : 전압 영역 비교기
 500 : 확률 제어기

도면

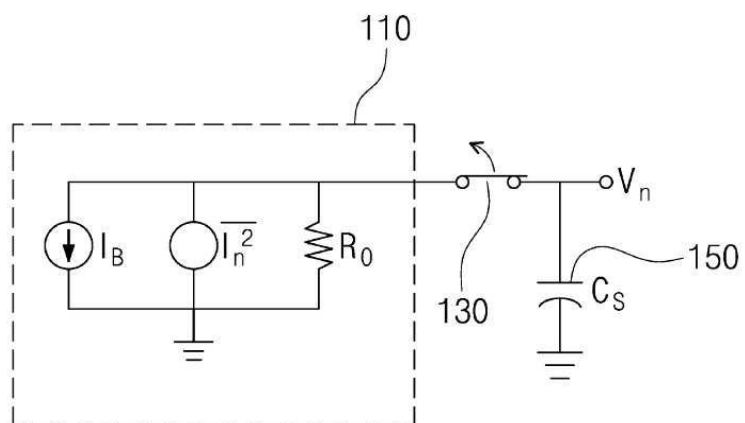
도면1



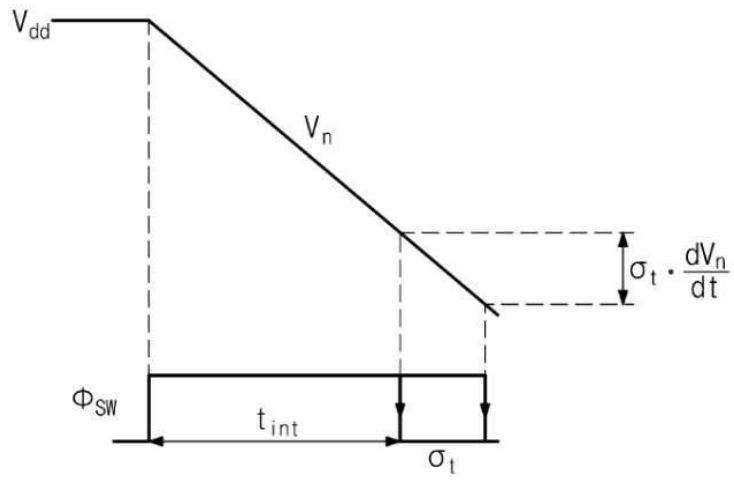
도면2



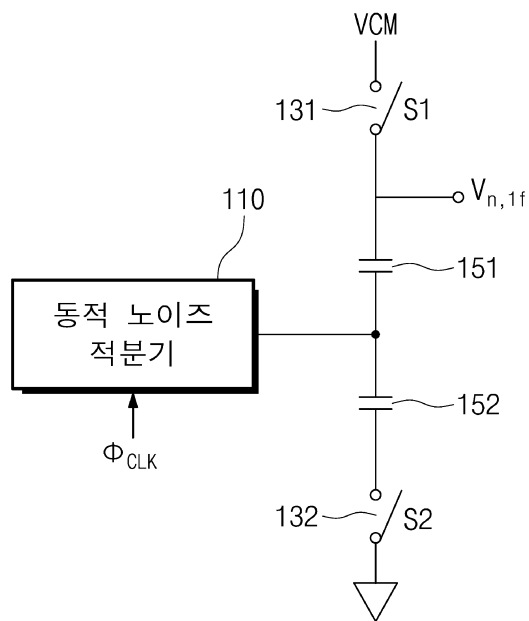
도면3



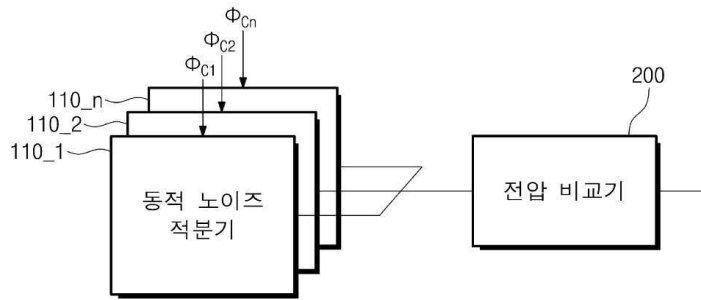
도면4



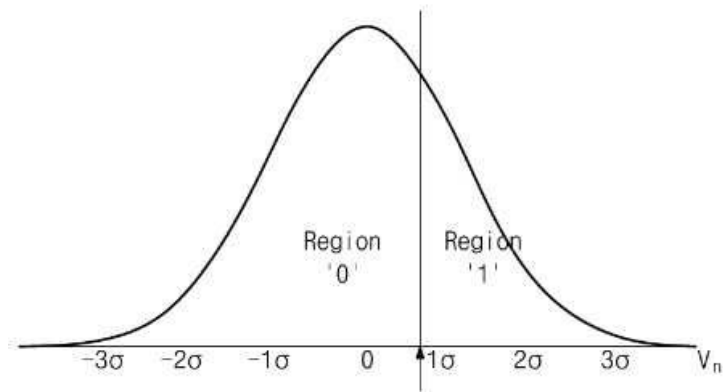
도면5



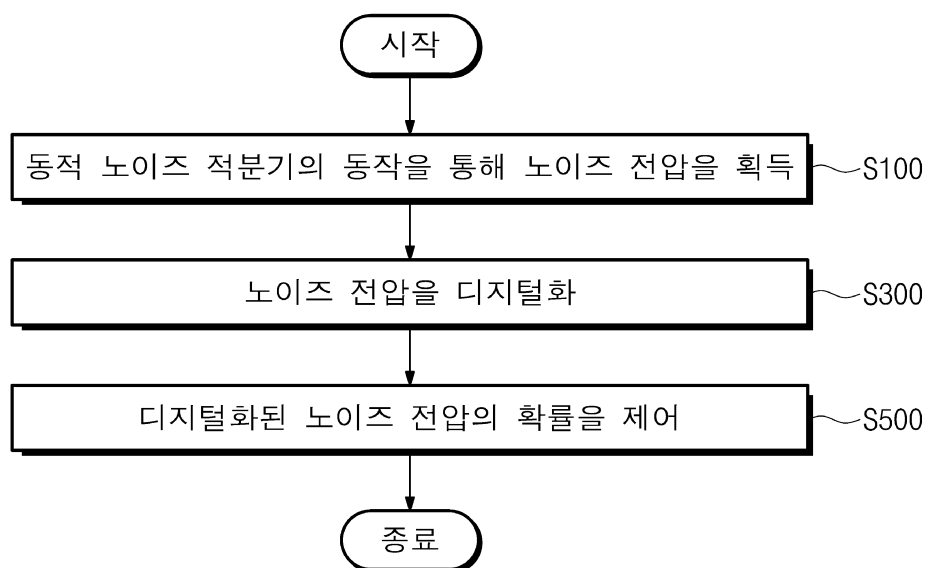
도면6



도면7



도면8



도면9

