(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0144192
(43) 공개일자 2020년12월29일

(51) 국제특허분류(Int. Cl.)
G06F 7/58 (2006.01) *H03K 3/84* (2006.01)
(52) CPC특허분류
G06F 7/588 (2013.01)
H03K 3/84 (2013.01)
(21) 출원번호 10-2019-0071664
(22) 출원일자 2019년06월17일
심사청구일자 없음

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
박성모
대전광역시 유성구 왕가봉로 23 1110-1201
박경환
대전광역시 유성구 어은동 어은로 57
(뒷면에 계속)
(74) 대리인
특허법인 고려

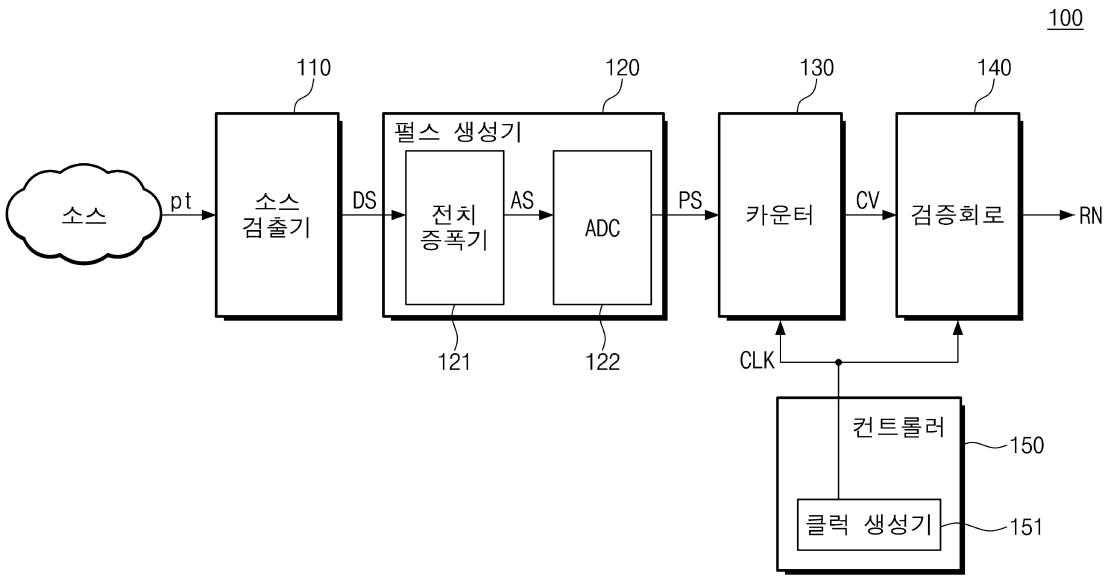
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **난수 생성 장치 및 이의 동작 방법**

(57) 요 약

본 발명은 난수 생성 장치 및 이의 동작 방법에 관한 것이다. 본 발명의 실시예에 따른 난수 생성 장치는 소스 검출기, 펄스 생성기, 카운터, 및 검증 회로를 포함한다. 소스 검출기는 소스로부터 방출된 입자들을 검출하여 검출 신호를 생성한다. 펄스 생성기는 검출 신호에 기초하여 검출된 입자들에 대응되는 펄스들을 생성한다. 카운터는 펄스들 사이의 시간 간격들에 각각 대응되는 이진 카운트 값들을 생성한다. 검증 회로는 이진 카운트 값들에 포함된 0 값들의 개수 및 1 값들의 개수에 기초하여 이진 카운트 값들의 출력을 결정한다.

대 표 도



(72) 발명자

강태욱

대전광역시 서구 도안북로 125 104동 701호 (도안동,금성백조예미지아파트)

최병건

대전광역시 서구 둔산동 둔산북로 160 한마루아파트 105-602

이 발명을 지원한 국가연구개발사업

과제고유번호	2018M2A8A1083094
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	원자력원천기술
연구과제명	난수 발생 회로 개발 및 집적화 기술 개발
기 여 율	1/1
과제수행기관명	한국원자력연구원
연구기간	2018.09.18 ~ 2019.04.30

명 세 서

청구범위

청구항 1

소스로부터 방출된 입자들을 검출하여 검출 신호를 생성하는 소스 검출기;

상기 검출 신호에 기초하여 상기 검출된 입자들에 대응되는 펄스들을 생성하는 펄스 생성기;

상기 펄스들 사이의 시간 간격들을 측정하고, 상기 시간 간격들에 각각 대응되는 이진 카운트 값들을 생성하는 카운터; 및

상기 이진 카운트 값들에 포함된 0 값들의 개수 및 1 값들의 개수에 기초하여 상기 이진 카운트 값들의 출력을 결정하는 검증 회로를 포함하는 난수 생성 장치.

청구항 2

제1 항에 있어서,

상기 검증 회로는,

상기 이진 카운트 값들에서 상기 0 값들 및 상기 1 값들을 추출하는 비교기;

상기 0 값들의 개수에 대응되는 제1 누적 값을 생성하고, 상기 1 값들의 개수에 대응되는 제2 누적 값을 생성하는 누적기;

상기 제1 누적 값 및 상기 제2 누적 값의 차이에 기초하여 상기 이진 카운트 값들의 유효성을 검증하기 위한 검증 신호를 생성하는 판단기; 및

상기 검증 신호에 기초하여 상기 이진 카운트 값들을 출력하는 멀티플렉서를 포함하는 난수 생성 장치.

청구항 3

제2 항에 있어서,

상기 차이가 기준 범위 이내인 경우, 상기 판단기는 활성화 값을 갖는 상기 검증 신호를 생성하고, 상기 멀티플렉서는 상기 활성화 값에 응답하여 상기 이진 카운트 값들을 출력하는 난수 생성 장치.

청구항 4

제2 항에 있어서,

상기 차이가 기준 범위를 벗어난 경우, 상기 판단기는 비활성화 값을 갖는 상기 검증 신호를 생성하고, 상기 멀티플렉서는 상기 비활성화 값에 응답하여 상기 이진 카운트 값들의 출력을 차단하는 난수 생성 장치.

청구항 5

제2 항에 있어서,

상기 판단기는,

상기 제1 누적 값 및 상기 제2 누적 값의 상기 차이를 계산하는 감산기; 및

상기 차이를 기준 범위와 비교하고, 비교 결과에 기초하여 상기 검증 신호를 생성하는 기준 값 비교기를 포함하는 난수 생성 장치.

청구항 6

제2 항에 있어서,

상기 누적기는,

상기 0 값들을 수신할 때 상기 제1 누적 값을 증가시키는 제1 누적기; 및

상기 1 값들을 수신할 때 상기 제2 누적 값을 증가시키는 제2 누적기를 포함하고,

상기 비교기는 상기 0 값들 및 상기 1 값들을 분리하고, 상기 0 값들을 상기 제1 누적기로 출력하고, 상기 1 값들을 상기 제2 누적기로 출력하는 난수 생성 장치.

청구항 7

제1 항에 있어서,

상기 카운터는,

상기 펄스들을 클럭 신호에 동기화하여 출력하는 플립플롭; 및

상기 동기화된 펄스들 사이의 시간 간격들 동안, 상기 클럭 신호에 포함된 클럭들의 개수를 카운트하여 상기 이진 카운트 값들을 생성하는 클럭 카운터를 포함하는 난수 생성 장치.

청구항 8

제1 항에 있어서,

기준 시간 동안 생성된 상기 펄스들에 기초하여 상기 이진 카운트 값들을 생성하도록 상기 카운터를 제어하고, 상기 이진 카운트 값들의 출력을 결정하도록 상기 검증 회로를 제어하는 컨트롤러를 더 포함하는 난수 생성 장치.

청구항 9

제1 항에 있어서,

상기 이진 카운트 값들의 총 비트 수가 기준 개수일 때까지 상기 이진 카운트 값들을 생성하도록 상기 카운터를 제어하고, 상기 이진 카운트 값들의 출력을 결정하도록 상기 검증 회로를 제어하는 컨트롤러를 더 포함하는 난수 생성 장치.

청구항 10

제1 항에 있어서,

상기 펄스 생성기는,

상기 검출 신호를 증폭하는 전치 증폭기; 및

상기 증폭된 검출 신호를 상기 펄스들로 변환하는 아날로그-디지털 변환기를 포함하는 난수 생성 장치.

청구항 11

제1 항에 있어서,

상기 소스는 베타선 소스이고, 상기 입자들 각각은 베타선에 대응되는 난수 생성 장치.

청구항 12

소스로부터 방출된 입자들을 검출하여 검출 신호를 생성하는 소스 검출기;

상기 검출 신호를 상기 검출된 입자들에 대응되는 펄스들로 변환하는 펄스 생성기;

상기 펄스들 사이의 시간 간격들 동안 클럭들의 개수를 카운트하여 이진 카운트 값들을 생성하는 카운터; 및

상기 이진 카운트 값들의 총 비트 수에 대한 타겟 값들의 개수의 비율에 기초하여 상기 이진 카운트 값들의 출력을 결정하는 검증 회로를 포함하는 난수 생성 장치.

청구항 13

제12 항에 있어서,

상기 타겟 값들의 개수는 상기 이진 카운트 값들에 포함된 0 값들의 개수이거나, 상기 이진 카운트 값들에 포함된 1 값들의 개수인 난수 생성 장치.

청구항 14

제12 항에 있어서,

상기 검증 회로는,

상기 이진 카운트 값들에서 상기 타겟 값들을 추출하는 비교기;

상기 타겟 값들의 개수에 대응되는 누적 값을 생성하는 누적기;

상기 누적 값에 기초하여 상기 비율을 계산하고, 상기 비율에 기초하여 상기 이진 카운트 값들의 유효성을 검증하기 위한 검증 신호를 생성하는 판단기; 및

상기 검증 신호에 기초하여 상기 이진 카운트 값들을 출력하는 멀티플렉서를 포함하는 난수 생성 장치.

청구항 15

제14 항에 있어서,

상기 비율이 기준 범위 이내인 경우, 상기 판단기는 활성화 값을 갖는 상기 검증 신호를 생성하고, 상기 멀티플렉서는 상기 활성화 값에 응답하여 상기 이진 카운트 값들을 출력하는 난수 생성 장치.

청구항 16

제14 항에 있어서,

상기 비율이 기준 범위를 벗어난 경우, 상기 판단기는 비활성화 값을 갖는 상기 검증 신호를 생성하고, 상기 멀티플렉서는 상기 비활성화 값에 응답하여 상기 이진 카운트 값들의 출력을 차단하는 난수 생성 장치.

청구항 17

난수 생성 장치의 동작 방법에 있어서,

소스로부터 방출되는 입자들이 검출된 시간 간격들에 대응되는 이진 카운트 값들을 생성하는 단계;

상기 이진 카운트 값들에서 0 값들 및 1 값들을 추출하는 단계;

상기 0 값들의 개수에 대응되는 제1 누적 값을 생성하는 단계;

상기 1 값들의 개수에 대응되는 제2 누적 값을 생성하는 단계;

상기 제1 누적 값 및 상기 제2 누적 값의 차이에 기초하여 상기 이진 카운트 값들의 유효성을 검증하기 위한 검증 신호를 생성하는 단계; 및

상기 검증 신호에 기초하여 상기 이진 카운트 값들의 출력여부를 판단하는 단계를 포함하는 방법.

청구항 18

제17 항에 있어서,

상기 검증 신호를 생성하는 단계는,

상기 제1 누적 값 및 상기 제2 누적 값의 차이를 계산하는 단계;

상기 차이와 기준 범위를 비교하는 단계; 및

상기 차이가 상기 기준 범위 이내인지 판단하는 단계를 포함하는 방법.

청구항 19

제18 항에 있어서,

상기 이진 카운트 값들의 출력여부를 판단하는 단계는,

상기 차이가 상기 기준 범위 이내인 경우 상기 이진 카운트 값들을 난수로 출력하는 단계를 포함하는 방법.

청구항 20

제18 항에 있어서,

상기 이진 카운트 값들의 출력여부를 판단하는 단계는,

상기 차이가 상기 기준 범위를 벗어난 경우 상기 이진 카운트 값들의 출력을 차단하는 단계를 포함하는 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 난수 생성 장치 및 이의 동작 방법에 관한 것으로, 좀 더 구체적으로 진성 난수를 생성하는 장치 및 이의 동작 방법에 관한 것이다.

배 경 기 술

[0002] 난수(Random number)는 전자 상거래나 인증 등과 같은 다양한 분야에서 정보 보안을 위한 암호 시스템에서 사용된다. 이외에도, 난수는 게임, 복권, 표본화, 모의 실험 등 다양한 분야에서 사용되므로, 난수의 랜덤성을 확보하는 방안이 연구되고 있다. 현재 일반적으로 사용되는 의사 난수(Pseudo Random Number)는 컴퓨터 알고리즘으로 만들어 진다. 이러한 의사 난수는 일고리즘에 의하여 패턴이 존재하므로, 패턴이 알려지는 경우 보안에 취약할 수 있다.

[0003] 일례로, 씨드를 난수 생성 장치에 입력하여 의사 난수를 생성하는 장치가 사용될 수 있다. 씨드는 결정론적 난수 발생 장치에 입력으로 사용되는 비트열로, 난수의 안정성은 씨드에 의존한다. 일례로, 운영 체제에서 제공되는 잡음 또는 GPU(Graphical Processing Unit) 코어들 간의 메모리 접근 경쟁에 따른 잡음이 씨드로 이용될 수 있다. 다만, 상술한 바와 같이, 이러한 난수 발생 장치는 완전한 랜덤성을 갖지 않을 수 있다.

[0004] 이에 따라, 하드웨어 기반의 랜덤 현상으로부터 추출되는 진성 난수(True Random Number)가 각광받고 있다. 일례로, 진성 난수는 양자역학적 랜덤 현상을 이용하여 생성될 수 있다. 일례로, 방사성 동위원소의 알파선 베타선 등의 랜덤한 방출과 같은 양자역학적 랜덤 현상이 진성 난수를 생성하는데 이용될 수 있다. 진성 난수를 생성하는 장치에서, 소형화 및 난수의 품질 증가에 대한 요구가 제기되고 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 소형화되고, 생성된 난수의 품질을 향상시키는 난수 생성 장치 및 이의 동작 방법을 제공할 수 있다.

과제의 해결 수단

[0006] 본 발명의 실시예에 따른 난수 생성 장치는 소스 검출기, 펄스 생성기, 카운터, 및 검증 회로를 포함한다. 소스 검출기는 소스로부터 방출된 입자들을 검출하여 검출 신호를 생성한다. 펄스 생성기는 검출 신호에 기초하여 검출된 입자들에 대응되는 펄스들을 생성한다. 카운터는 펄스들 사이의 시간 간격들을 측정하고, 시간 간격들에 각각 대응되는 이진 카운트 값들을 생성한다. 검증 회로는 이진 카운트 값들에 포함된 0 값들의 개수 및 1 값들의 개수에 기초하여 이진 카운트 값들의 출력을 결정한다.

[0007] 일례로, 검증 회로는 이진 카운트 값들에서 0 값들 및 1 값들을 추출하는 비교기, 0 값들의 개수에 대응되는 제1 누적 값을 생성하고, 1 값들의 개수에 대응되는 제2 누적 값을 생성하는 누적기, 제1 누적 값 및 제2 누적 값의 차이에 기초하여 이진 카운트 값들의 유효성을 검증하기 위한 검증 신호를 생성하는 판단기, 및 검증 신호에 기초하여 이진 카운트들 값들을 출력하는 멀티플렉서를 포함할 수 있다. 상기 차이가 기준 범위 이내인 경우, 판단기는 활성화 값을 갖는 검증 신호를 생성하고, 멀티플렉서는 활성화 값에 응답하여 이진 카운트 값들을 출력할 수 있다. 상기 차이가 기준 범위를 벗어난 경우, 판단기는 비활성화 값을 갖는 검증 신호를 생성하고, 멀티플렉서는 비활성화 값에 응답하여 이진 카운트 값들의 출력을 차단할 수 있다.

[0008] 일례로, 판단기는 제1 누적 값 및 제2 누적 값의 차이를 계산하는 감산기, 및 차이를 기준 범위와 비교하고, 비교 결과에 기초하여 검증 신호를 생성하는 기준 값 비교기를 포함할 수 있다. 일례로, 누적기는 0 값들을 수신할 때 제1 누적 값을 증가시키는 제1 누적기 및 1 값들을 수신할 때 제2 누적 값을 증가시키는 제2 누적기를 포함할 수 있다. 비교기는 0 값들 및 1 값들을 분리하고, 0 값들을 제1 누적기로 출력하고, 1 값들을 제2 누적기로 출력할 수 있다.

[0009] 일례로, 카운터는 펄스들을 클럭 신호에 동기화하여 출력하는 플립플롭, 및 동기화된 펄스들 사이의 시간 간격들 동안, 클럭 신호에 포함된 클럭들의 개수를 카운트하여 이진 카운트 값들을 생성하는 클럭 카운터를 포함할 수 있다.

[0010] 일례로, 난수 생성 장치는 기준 시간 동안 생성된 펄스들에 기초하여 이진 카운트 값들을 생성하도록 카운터를 제어하고, 이진 카운트 값들의 출력을 결정하도록 검증 회로를 제어하는 컨트롤러를 더 포함할 수 있다. 일례로, 난수 생성 장치는 이진 카운트 값들의 총 비트 수가 기준 개수일 때까지 이진 카운트 값들을 생성하도록 카운터를 제어하고, 이진 카운트 값들의 출력을 결정하도록 검증 회로를 제어하는 컨트롤러를 더 포함할 수 있다.

[0011] 일례로, 펄스 생성기는 검출 신호를 증폭하는 전치 증폭기, 및 증폭된 검출 신호를 펄스들로 변환하는 아날로그-디지털 변환기를 포함할 수 있다. 일례로, 소스는 베타선 소스이고, 입자들 각각은 베타선에 대응될 수 있다.

[0012] 본 발명의 실시예에 따른 난수 생성 장치는 소스 검출기, 펄스 생성기, 카운터, 및 검증 회로를 포함한다. 소스 검출기는 소스로부터 방출된 입자들을 검출하여 검출 신호를 생성할 수 있다. 펄스 생성기는 검출 신호를 검출된 입자들에 대응되는 펄스들로 변환할 수 있다. 카운터는 펄스들 사이의 시간 간격들 동안 클럭들의 개수를 카운트하여 이진 카운트 값들을 생성할 수 있다. 검증 회로는 이진 카운트 값들의 총 비트 수에 대한 타겟 값들의 개수의 비율에 기초하여 이진 카운트 값들의 출력을 결정할 수 있다. 타겟 값들의 개수는 이진 카운트 값들에 포함된 0 값들의 개수이거나, 이진 카운트 값들에 포함된 1 값들의 개수일 수 있다.

[0013] 일례로, 검증 회로는 이진 카운트 값들에서 타겟 값들을 추출하는 비교기, 타겟 값들의 개수에 대응되는 누적 값을 생성하는 누적기, 누적 값에 기초하여 비율을 계산하고 비율에 기초하여 이진 카운트 값들의 유효성을 검증하기 위한 검증 신호를 생성하는 판단기, 및 검증 신호에 기초하여 이진 카운트 값들을 출력하는 멀티플렉서를 포함할 수 있다. 상기 비율이 기준 범위 이내인 경우, 판단기는 활성화 값을 갖는 검증 신호를 생성하고, 멀티플렉서는 활성화 값에 응답하여 이진 카운트 값들을 출력할 수 있다. 상기 비율이 기준 범위를 벗어난 경우, 판단기는 비활성화 값을 갖는 검증 신호를 생성하고, 멀티플렉서는 비활성화 값에 응답하여 이진 카운트 값들의 출력을 차단할 수 있다.

[0014] 본 발명의 실시예에 따른 난수 생성 장치의 동작 방법은, 소스로부터 방출되는 입자들이 검출된 시간 간격들에 대응되는 이진 카운트 값들을 생성하는 단계, 이진 카운트 값들에서 0 값들 및 1 값들을 추출하는 단계, 0 값들의 개수에 대응되는 제1 누적 값을 생성하는 단계, 1 값들의 개수에 대응되는 제2 누적 값을 생성하는 단계, 제1 누적 값 및 제2 누적 값의 차이에 기초하여 이진 카운트 값들의 유효성을 검증하기 위한 검증 신호를 생성하는 단계, 및 검증 신호에 기초하여 이진 카운트 값들의 출력여부를 판단하는 단계를 포함한다.

[0015] 일례로, 검증 신호를 생성하는 단계는, 제1 누적 값 및 제2 누적 값의 차이를 계산하는 단계, 차이와 기준 범위를 비교하는 단계, 및 차이가 기준 범위 이내인지 판단하는 단계를 포함할 수 있다. 일례로, 이진 카운트 값들의 출력여부를 판단하는 단계는, 차이가 기준 범위 이내인 경우 이진 카운트 값들을 난수로 출력하는 단계를 포함할 수 있다. 일례로, 이진 카운트 값들의 출력여부를 판단하는 단계는, 차이가 기준 범위를 벗어난 경우 이진 카운트 값들의 출력을 차단하는 단계를 포함할 수 있다.

발명의 효과

[0016] 본 발명의 실시예에 따른 난수 생성 장치 및 이의 동작 방법은 소형화에 적합한 아날로그 증폭기 및 디지털 신호 처리 회로를 이용하여 진성 난수를 생성할 수 있다.

[0017] 또한, 본 발명의 실시예에 따른 난수 생성 장치 및 이의 동작 방법은 검증 회로를 이용하여, 난수의 랜덤성이 증가하고 난수의 품질이 향상될 수 있다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 실시예에 따른 난수 생성 장치를 도시한 도면이다.

도 2는 도 1의 펄스 생성기의 동작에 따른 증폭 신호 및 펄스 신호의 예시적인 파형을 도시한 그래프이다.

도 3은 도 1의 카운터의 예시적인 블록도이다.

도 4는 도 1 및 도 3의 카운터의 동작을 설명하기 위한 그래프이다.

도 5는 도 1의 검증 회로의 예시적인 블록도이다.

도 6은 도 5의 판단기의 예시적인 블록도이다.

도 7은 도 5의 판단기의 예시적인 블록도이다.

도 8은 도 1의 난수 생성 장치의 동작 방법의 예시적인 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 아래에서는, 본 발명의 기술 분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있을 정도로, 본 발명의 실시 예들이 명확하고 상세하게 기재된다.

[0020] 도 1은 본 발명의 실시예에 따른 난수 생성 장치를 도시한 도면이다. 도 1을 참조하면, 난수 생성 장치(100)는 소스 검출기(110), 펄스 생성기(120), 카운터(130), 검증 회로(140), 및 컨트롤러(150)를 포함한다. 도 1 이하의 난수 생성 장치(100)는 소스로부터 방출된 이벤트, 엔트로피, 또는 입자 등으로부터 진성 난수를 생성한다. 일례로, 난수 생성 장치(100)는 양자역학적 랜덤 현상을 이용하여 난수를 생성할 수 있고, 특히 방사성 동위원소의 자연붕괴 현상을 이용하여 난수를 생성할 수 있다. 이하, 예시적으로 소스가 베타 소스와 같은 방사성 동위원소인 것으로 가정하여 설명된다. 다만, 이에 제한되지 않고, 난수 생성 장치(100)는 빛의 랜덤 현상 또는 자연 발생적 잡음을 소스로 이용할 수 있다.

[0021] 방사성 동위원소는 원자핵의 양성자 및 중성자의 조합이 불안정하여 안정한 상태로 바뀌는 과정에서 입자들(pt)을 방출하는 동위원소를 의미한다. 방사성 동위원소는 안정화를 위하여, 알파 입자 또는 베타 입자 (알파선 또는 베타선) 등과 같은 에너지를 갖는 입자들(pt)을 자발적으로 방출하며, 이는 자연붕괴 현상으로 정의된다. 방사성 동위원소의 자연붕괴 현상은 붕괴 이벤트의 랜덤성, 이전 이벤트와의 무상관성, 및 물리적 환경 조건에 무관성을 갖고 있어, 진성 난수를 생성하기 위하여 사용될 수 있다.

[0022] 소스 검출기(110)는 방사성 동위원소와 같은 소스로부터 방출된 입자들(pt)을 검출한다. 소스 검출기(110)가 입자들(pt)을 검출하는 방식은 제한되지 않는다. 일례로, 소스 검출기(110)는 기체 방사선 검출기(gas filled radiation detector), 반도체 방사선 검출기(semiconductor radiation detector), 또는 자기출력형 방사선 검출기(self—powered radiation detector) 등을 포함할 수 있다. 소스 검출기(110)는 검출된 입자들(pt)에 기초하여 검출 신호(DS)를 생성할 수 있다. 검출 신호(DS)는 전압 또는 전류와 같은 아날로그 전기 신호이고, 펄스 생성기(120)로 제공된다. 일례로, 검출 신호(DS)에서 입자들(pt)이 검출된 시간과 검출되지 않은 시간이 구별될 수 있다.

[0023] 펄스 생성기(120)는 검출 신호(DS)에 기초하여 펄스 신호(PS)를 생성할 수 있다. 펄스 신호(PS)는 검출된 입자들(pt)에 각각 대응되는 펄스들을 포함할 수 있다. 즉, 펄스 신호(PS)에 포함된 펄스들의 개수는 검출된 입자들(pt)의 개수에 대응될 수 있다. 펄스 신호(PS)를 생성하기 위하여, 펄스 생성기(120)는 전치 증폭기(121) 및 아날로그-디지털 변환기(122)를 포함할 수 있다.

[0024] 전치 증폭기(121)는 검출 신호(DS)를 증폭하여 증폭 신호(AS)를 생성한다. 전치 증폭기(121)는 검출 신호(DS)의 크기를 증폭함으로써, 입자들(pt)이 검출된 시간과 입자들(pt)이 검출되지 않은 시간이 용이하게 구별될 수 있도록 한다. 증폭 신호(AS)는 아날로그-디지털 변환기(122)로 제공된다.

[0025] 아날로그-디지털 변환기(122)는 아날로그 전기 신호인 증폭 신호(AS)를 디지털 신호인 펄스 신호(PS)로 변환할 수 있다. 아날로그-디지털 변환기(122)는 증폭 신호(AS)에 기초하여 입자들(pt)에 각각 대응되는 펄스들을 포함하는 펄스 신호(PS)를 생성할 수 있다. 아날로그-디지털 변환기(122)는 검출 신호(DS)의 크기에 기초하여 입자들(pt)이 검출된 것으로 판단되는 시간들을 판별할 수 있다. 아날로그-디지털 변환기(122)는 해당 시간들에 대응되는 펄스들을 생성하고, 이러한 펄스들을 포함하는 펄스 신호(PS)를 카운터(130)로 출력할 수 있다.

[0026] 카운터(130)는 펄스 신호(PS)에 포함된 펄스들 사이의 시간 간격들을 측정할 수 있다. 카운터(130)에 하나의 펄스가 입력되면, 카운터(130)는 다음 펄스가 입력될 때까지의 시간 동안 클럭 신호(CLK)에 포함된 클럭들을 카운트할 수 있다. 카운터(130)는 펄스 신호(PS)에서 인접한 두 개의 펄스들 사이의 시간 간격 동안 클럭들의 개수

를 카운트한다. 카운터(130)는 클럭들을 카운트하기 위하여 클럭 신호(CLK)를 수신할 수 있다. 클럭 신호(CLK)는 컨트롤러(150)로부터 제공될 수 있다. 다만, 이에 제한되지 않고, 클럭 신호(CLK)는 카운터(130) 내부에서 직접 생성할 수 있다.

[0027] 카운터(130)는 복수의 펄스들 사이의 시간 간격들 각각의 카운트 결과, 이진 카운트 값들(CV)을 생성할 수 있다. 이진 카운트 값들(CV) 각각은 설정된 비트 수의 0 값 또는 1 값들을 포함할 수 있다. 설정된 비트 수를 갖는 이진 카운트 값들(CV)의 개수는 측정된 시간 간격들의 개수에 대응된다. 이진 카운트 값들(CV) 각각은 측정된 시간 간격의 길이에 의존한다. 즉, 측정된 시간 간격의 길이가 길수록, 이진 카운트 값들(CV) 중 해당 시간 간격에 대응되는 이진 카운트 값은 큰 값을 가질 수 있다.

[0028] 검증 회로(140)는 카운터(130)로부터 생성된 이진 카운트 값들(CV)의 유효성을 검증할 수 있다. 검증 회로(140)는 이진 카운트 값들(CV) 전체에 포함된 0 값들의 개수 및 1 값들의 개수에 기초하여 이진 카운트 값들(CV)의 유효성을 검증할 수 있다. 진성 난수의 표본이 클수록, 난수 (이진 카운트 값)가 특정 값을 가질 확률은 일정해진다. 예를 들어, 이진 카운트 값이 n개의 비트 수를 갖는 경우, 그들 중 어느 하나의 값을 가질 확률은 $1/2^n$으로 수렴할 수 있다. 즉, 표본이 클수록, 이진 카운트 값들(CV)은 난수 범위에서 골고루 분포된 값을 가질 수 있고, 0 값들의 개수 및 1 값들의 개수는 거의 동일해질 수 있다.

[0029] 일례로, 검증 회로(140)는 0 값들의 개수와 1 값들의 개수의 차이가 기준 범위 이내인지를 판단하여 이진 카운트 값들(CV)의 유효성을 검증할 수 있다. 여기에서, 기준 범위는 이진 카운트 값들(CV)이 난수(RN)로 사용될 수 있을 정도의 랜덤성을 확보한 것으로 인정되는 허용 오차 범위일 수 있다. 예를 들어, 기준 범위는 이진 카운트 값들(CV)의 총 비트 수의 -0.05%와 +0.05% 사이일 수 있다.

[0030] 이 경우, 검증 회로(140)는 이진 카운트 값들(CV)에서 0 값들 및 1 값들을 추출할 수 있다. 검증 회로(140)는 0 값이 추출될 때마다 0 값에 대응되는 누적 값(제1 누적 값)을 증가시키고, 1 값이 추출될 때마다 1 값에 대응되는 누적 값(제2 누적 값)을 증가시킬 수 있다. 검증 회로(140)는 제1 누적 값과 제2 누적 값의 차이를 계산하여 기준 범위와 비교할 수 있다. 이러한 차이가 기준 범위 이내인 경우, 이진 카운트 값들(CV)은 난수(RN)로 출력된다. 차이가 기준 범위를 벗어난 경우, 이진 카운트 값들(CV)의 출력이 차단되어 난수(RN)로 사용되지 않을 수 있다.

[0031] 일례로, 검증 회로(140)는 이진 카운트 값들(CV)에 포함된 총 비트 수에 대한 0 값들의 개수의 비율 또는 총 비트 수에 대한 1 값들의 개수의 비율이 기준 범위 이내인지를 판단하여 이진 카운트 값들(CV)의 유효성을 검증할 수 있다. 여기에서, 기준 범위는 이진 카운트 값들(CV)이 난수(RN)로 사용될 수 있을 정도의 랜덤성을 확보한 것으로 인정되는 허용 오차 범위일 수 있다. 예를 들어, 기준 범위는 49.95%와 50.05% 사이일 수 있다.

[0032] 이 경우, 검증 회로(140)는 이진 카운트 값들(CV)에서 0 값들 또는 1 값들을 추출할 수 있다. 검증 회로(140)는 0 값 또는 1 값이 추출될 때 누적 값을 증가시킬 수 있다. 검증 회로(140)는 이진 카운트 값들(CV)의 총 비트 수에 대한 누적 값의 비율을 계산하여 기준 범위와 비교할 수 있다. 이러한 차이가 기준 범위 이내인 경우, 이진 카운트 값들(CV)은 난수(RN)로 출력된다. 차이가 기준 범위를 벗어난 경우, 이진 카운트 값들(CV)의 출력이 차단되어 난수(RN)로 사용되지 않을 수 있다.

[0033] 컨트롤러(150)는 난수 생성 장치(100)의 동작을 제어할 수 있다. 일례로, 컨트롤러(150)는 펄스 생성기(120)로부터 생성된 펄스 신호(PS)에 기초하여 이진 카운트 값들(CV)을 생성하도록 카운터(130)를 제어할 수 있다. 일례로, 컨트롤러(150)는 이진 카운트 값들(CV)의 유효성을 검증하여 이진 카운트 값들(CV)을 난수(RN)로 사용할지 여부를 결정하도록 검증 회로(140)를 제어할 수 있다. 이외에도, 컨트롤러(150)는 입자들(pt)을 검출하도록 소스 검출기(110)를 제어하거나, 펄스 신호(PS)를 생성하도록 펄스 생성기(120)를 제어할 수 있다.

[0034] 이진 카운트 값들(CV)의 유효성을 검증하기 위하여, 상술된 바와 같이, 표본이 요구될 수 있다. 컨트롤러(150)는 표본에 대응되는 이진 카운트 값들(CV)의 개수를 결정할 수 있다. 검증 회로(140)는 해당 개수의 카운트 값들(CV)을 이용하여 유효성을 검증할 수 있다. 일례로, 컨트롤러(150)는 기준 시간 동안 생성된 입자들(pt)에 대응되는 펄스들에 기초하여 이진 카운트 값들(CV)을 생성하도록 카운터(130)를 제어할 수 있다. 여기에서, 기준 시간은 유효성을 검증하기에 충분한 표본을 획득할 것으로 예상되는 입자들(pt)의 방출 시간으로 정의될 수 있다. 일례로, 컨트롤러(150)는 설정된 기준 개수의 총 비트 수만큼 이진 카운트 값들(CV)을 생성하도록 난수 생성 장치(100)를 제어할 수 있다. 여기에서, 기준 개수는 유효성을 검증하기에 충분한 표본으로 인정되는 비트 수로 정의될 수 있다.

[0035] 컨트롤러(150)는 카운터(130) 및 검증 회로(140)에 제공될 클럭 신호(CLK)를 생성하는 클럭 생성기(151)를 포함

할 수 있다. 클럭 신호(CLK)는 카운터(130)가 펄스들 사이의 시간 간격들을 카운트하는데 이용될 수 있다. 클럭 신호(CLK)는 검증 회로(140)의 유효성 검증을 위한 0 값들 또는 1 값들의 추출, 제1 누적 값 및 제2 누적 값의 계산을 위한 동기화 등에 사용될 수 있다. 도 1에 도시된 바와 달리, 클럭 생성기(151)는 카운터(130) 또는 검증 회로(140)에 포함될 수 있다.

[0036] 도 2는 도 1의 펄스 생성기의 동작에 따른 증폭 신호 및 펄스 신호의 예시적인 파형을 도시한 그래프이다. 도 2를 참조하면, 가로축은 시간으로 정의되고, 세로축은 증폭 신호(AS) 및 펄스 신호(PS)의 크기 (전압 또는 전류 레벨)로 정의된다. 증폭 신호(AS) 및 펄스 신호(PS) 각각은 도 1의 증폭 신호(AS) 및 펄스 신호(PS)에 대응된다. 설명의 편의상 도 1의 도면 부호를 참조하여, 도 2가 설명된다.

[0037] 증폭 신호(AS)는 소스 검출기(110)로부터 수신된 검출 신호(DS)를 전치 증폭기(121)를 이용하여 증폭한 신호일 수 있다. 증폭 신호(AS)는 5개의 피크 값을 가지므로, 방사성 동위원소로부터 5개의 입자들이 검출된 경우의 파형으로 이해될 것이다. 5개의 피크 값들 중 인접한 피크 값들 사이에 4개의 시간 간격들, 즉 제1 내지 제4 시간 간격들(i1~i4)이 존재한다. 제1 내지 제4 시간 간격들(i1~i4)은 난수(RN) 또는 이진 카운트 값들(CV)을 생성하는데 이용되며, 난수(RN)의 크기는 제1 내지 제4 시간 간격들(i1~i4) 각각의 길이에 의존한다.

[0038] 펄스 신호(PS)는 아날로그-디지털 변환기(122)를 이용하여 증폭 신호(AS)의 파형들을 디지털 신호인 사각 펄스로 처리한 신호일 수 있다. 일례로, 아날로그-디지털 변환기(122)는 증폭 신호(AS)로부터 5개의 극대값들을 추출할 수 있고, 제1 내지 제4 시간 간격들(i1~i4)로 분포된 펄스들을 생성할 수 있다. 5개의 펄스들 각각은 입자들(pt)이 검출된 시간에 대응된다. 이러한 펄스들은 카운터(130)에 입력된다. 카운터(130)는 제1 내지 제4 시간 간격들(i1~i4) 각각에 대응되는 카운트 값들을 생성할 수 있다.

[0039] 도 3은 도 1의 카운터의 예시적인 블록도이다. 도 3의 카운터(130)는 펄스들 사이의 시간 간격들 각각을 측정하여 이진 카운트 값들(CV)을 생성하는 예시적인 구성으로 이해될 것이다. 도 3을 참조하면, 카운터(130)는 플립플롭(131) 및 클럭 카운터(132)를 포함할 수 있다.

[0040] 플립플롭(131)은 펄스 신호(PS)에 포함된 펄스들을 클럭 신호(CLK)에 동기화하여 출력할 수 있다. 플립플롭(131)은 펄스 도 1의 펄스 생성기(120)로부터 생성된 펄스 신호(PS)를 수신한다. 상술한 바와 같이, 펄스 신호(PS)는 입자(pt)들 각각의 검출 시점에 대응되는 복수의 펄스들을 포함한다. 플립플롭(131)은 비동기적으로 생성된 펄스들을 클럭 신호(CLK)에 포함된 클럭들의 상승 엣지 또는 하강 엣지에 맞출 수 있다. 플립플롭(131)은 동기화된 펄스 신호(PSa)를 클럭 카운터(132)로 출력할 수 있다.

[0041] 클럭 카운터(132)는 동기화된 펄스 신호(PSa)에 포함된 펄스들 사이의 시간 간격들 동안, 클럭들의 개수를 카운트할 수 있다. 클럭 카운터(132)에 하나의 펄스가 입력되면, 클럭 카운터(132)는 다음 펄스가 입력될 때까지의 시간 동안 입력되는 클럭들을 카운트할 수 있다. 클럭 카운터(132)는 카운트된 클럭들의 개수에 대응되는 이진 카운트 값(CV)을 생성할 수 있다. 이진 카운트 값(CV)은 0 값 또는 1 값을 갖는 비트열을 포함할 수 있다. 이진 카운트 값(CV)의 크기는 카운트된 클럭들의 개수에 의존한다. 즉, 카운트된 클럭들의 개수가 클수록, 이진 카운트 값(CV)의 크기는 증가한다. 펄스들은 소스의 랜덤한 입자(pt) 방출에 기초하여 생성되므로, 카운트된 클럭들의 개수는 랜덤할 수 있다. 따라서, 이진 카운트 값(CV)이 상술된 검증 회로(140)에 의하여 유효한 것으로 판단되는 경우, 이진 카운트 값(CV)은 난수로 사용된다.

[0042] 도 4는 도 1 및 도 3의 카운터의 동작을 설명하기 위한 그래프이다. 도 4를 참조하면, 가로축은 시간으로 정의되고, 세로축은 펄스 신호(PS) (또는 동기화된 펄스 신호(PSa)) 및 클럭 신호(CLK)의 크기 (전압 또는 전류 레벨)로 정의된다. 펄스 신호(PS), 동기화된 펄스 신호(PSa), 및 클럭 신호(CLK)는 도 3의 펄스 신호(PS), 동기화된 펄스 신호(PSa), 및 클럭 신호(CLK)에 대응된다.

[0043] 펄스 신호(PS)는 도 1의 입자들(pt) 각각에 대응되는 펄스들을 포함한다. 동기화된 펄스 신호(PSa)는 도 3의 플립플롭(131)을 이용하여, 펄스들을 클럭 신호(CLK)의 상승 엣지 (또는 하강 엣지)에 동기화한 펄스들을 포함한다. 펄스들은 랜덤한 시간 간격으로 분포될 수 있다. 도 3의 클럭 카운터(132)는 펄스들 사이의 시간 간격들 동안, 클럭들의 개수를 카운트할 수 있다.

[0044] 도 4에서, 첫번째 펄스 및 두번째 펄스 사이의 시간 간격 동안 3개의 클럭들이 카운트될 수 있다. 설정된 이진 카운트 값의 비트 수가 4인 것으로 가정하면, 제1 이진 카운트 값(CV1)은 0011_2일 수 있다. 두번째 펄스 및 세번째 펄스 사이의 시간 간격 동안 4개의 클럭들이 카운트되고, 제2 이진 카운트 값(CV2)은 0100_2일 수 있다. 세번째 펄스 및 네번째 펄스 사이의 시간 간격 동안 10개의 클럭들이 카운트된다면, 제3 이진 카운트 값(CV3)은

1010_2일 수 있다.

[0045] 다만, 이에 제한되지 않고, 제1 내지 제3 이진 카운트 값들(CV1~CV3)은 카운트된 클럭들의 개수와 동일한 값을 갖지 않을 수 있다. 일례로, 제1 이진 카운트 값(CV1)은 3개의 클럭들이 카운트될 때의 설정된 값을 가질 수 있다. 예를 들어, 설정된 값은 카운트된 클럭들의 개수에 비례하거나, 이진 카운트 값의 설정된 비트 수로 표현되는 범위 내로 보정된 값일 수 있다.

[0046] 펄스들이 랜덤한 시간 간격으로 분포되므로, 제1 내지 제3 이진 카운트 값들(CV1~CV3)은 도 1의 난수(RN)로 사용될 수 있다. 다만, 제1 내지 제3 이진 카운트 값들(CV1~CV3)은 신호의 전달, 변환, 변형 과정 등에서 노이즈 등이 포함된 결과일 수 있다. 일예로, 도 1에서 소스 검출기(110)가 입자(pt)를 검출하는 과정, 펄스 생성기(120)가 아날로그 신호를 증폭하고 디지털 펄스로 변환하는 과정 등에서 노이즈가 신호에 포함될 수 있다. 이 경우, 이진 카운트 값들의 신뢰성이 감소하고, 편향성을 가질 수 있다. 도 1의 검증 회로(140)는 카운터(130)로부터 생성된 이진 카운트 값들의 유효성을 검증할 수 있다.

[0047] 도 5는 도 1의 검증 회로의 예시적인 블록도이다. 도 5의 검증 회로(140)는 이진 카운트 값들(CV)의 분포를 판단하여 진성 난수에 가까운지 판단하는 예시적인 구성으로 이해될 것이다. 도 5를 참조하면, 검증 회로(140)는 비교기(141), 누적기(142), 판단기(145), 및 멀티플렉서(MUX)를 포함할 수 있다.

[0048] 비교기(141)는 이진 카운트 값들(CV)에서 0 값들(C0) 및 1 값들(C1)을 추출한다. 이진 카운트 값들(CV)은 복수의 시간 간격들에 각각 대응된다. 하나의 이진 카운트 값은 하나의 시간 간격에 대응되고, 0 값 또는 1 값을 갖는 비트열을 포함한다. 이진 카운트 값들(CV)은 복수의 비트열들을 포함한다. 비교기(141)는 이진 카운트 값들(CV)의 비트들 각각의 크기를 기준 값과 비교하여 0 값들(C0)과 1 값들(C1)을 분리할 수 있다. 일례로, 기준 값은 0 값에 대응되는 디지털 신호의 크기와 1 값에 대응되는 디지털 신호의 크기 사이의 값일 수 있다. 0 값들(C0) 및 1 값들(C1)은 서로 분리되어 누적기(142)로 출력될 수 있다. 비교기(141)는 클럭 신호(CLK)에 동기화되어 동작할 수 있다.

[0049] 누적기(142)는 수신된 0 값들(C0) 및 1 값들(C1)을 각각 누적할 수 있다. 누적기(142)는 0 값들(C0)을 누적하여 0 값들(C0)의 개수에 대응되는 제1 누적 값(A1)을 생성할 수 있다. 누적기(142)는 1 값들(C1)을 누적하여 1 값들(C1)의 개수에 대응되는 제2 누적 값(A2)을 생성할 수 있다. 누적기(142)는 0 값들(C0)을 누적하여 제1 누적 값(A1)을 생성하는 제1 누적기(143), 및 1 값들(C1)을 누적하여 제2 누적 값(A2)을 생성하는 제2 누적기(144)를 포함할 수 있다. 제1 누적기(143)는 0 값들(C0)을 수신할 때마다 제1 누적 값(A1)을 증가시킬 수 있다. 제2 누적기(144)는 1 값들(C1)을 수신할 때마다 제2 누적 값(A2)을 증가시킬 수 있다.

[0050] 판단기(145)는 제1 누적 값(A1) 및 제2 누적 값(A2)의 차이에 기초하여 검증 신호(VS)를 생성할 수 있다. 판단기(145)는 클럭 신호(CLK)에 동기화되어 동작할 수 있다. 판단기(145)는 제1 누적 값(A1)과 제2 누적 값(A2)을 감산할 수 있다. 이러한 감산 값은 0 값들(C0)의 개수와 1 값들(C1)의 개수의 차이일 수 있다. 판단기(145)는 감산 값이 기준 범위 이내인지 판단할 수 있다. 여기에서, 기준 범위는 이진 카운트 값들(CV)이 난수(RN)로 사용될 수 있을 정도의 랜덤성을 확보한 것으로 인정되는 허용 오차 범위일 수 있다. 이상적으로, 표본이 충분히 크다면, 진성 난수에 대응되는 감산 값은 0에 수렴할 것이다.

[0051] 감산 값이 기준 범위 이내인 경우, 판단기(145)는 이진 카운트 값들(CV)이 유효한 것으로 판단하고, 활성화 값(일례로, 1 값)을 갖는 검증 신호(VS)를 생성할 수 있다. 감산 값이 기준 범위를 벗어난 경우, 판단기(145)는 이진 카운트 값들(CV)이 유효한 진성 난수가 아닌 것으로 판단하고, 비활성화 값 (일례로, 0 값)을 갖는 검증 신호(VS)를 생성할 수 있다. 검증 신호(VS)는 멀티 플렉서(MUX)를 제어하는데 사용될 수 있다.

[0052] 멀티플렉서(MUX)는 검증 신호(VS)에 기초하여, 이진 카운트 값들(CV)을 난수(RN)로 출력하거나 출력하지 않을 수 있다. 검증 신호(VS)가 활성화 값 (일례로, 1 값)을 갖는 경우, 멀티플렉서(MUX)는 이진 카운트 값들(CV)을 난수(RN)로 출력할 수 있다. 출력된 난수(RN)는 암호 시스템과 같이, 난수(RN)가 요구되는 전자 시스템으로 제공될 수 있다. 검증 신호(VS)가 비활성화 값 (일례로, 0 값)을 갖는 경우, 멀티플렉서(MUX)는 이진 카운트 값들(CV)의 출력을 차단할 수 있다. 즉, 검증 회로(140)는 이진 카운트 값들(CV)의 유효성을 판단하여 난수(RN)로의 사용여부를 판단할 수 있다.

[0053] 도 5의 검증 회로(140)는 상술된 0 값들 및 1 값들의 차이를 이용하여 이진 카운트 값들(CV)의 유효성을 판단하는 방식 이외에, 0 값들 또는 1 값들의 개수와 총 비트 수의 비율을 이용하여 이진 카운트 값들(CV)의 유효성을 판단할 수 있다. 이 경우, 비교기(141)는 이진 카운트 값들(CV)에서 0 값들(C0) 및 1 값들(C1) 중 어느 하나를 추출할 수 있다. 누적기(142)는 0 값들(C0)의 개수 또는 1 값들(C1)의 개수에 대응되는 누적 값을 생성할 수 있

다. 그리고, 누적기(142)는 이진 카운트 값들(CV) 전체의 비트 수를 누적하여 누적 값을 생성할 수 있다. 예를 들어, 비교기(141)는 0 값들(C0)을 제1 누적기(143)로 출력하고, 제1 누적기(143)는 0 값들(C0)의 개수에 대응되는 제1 누적 값(A1)을 생성할 수 있다. 예를 들어, 비교기(141)는 이진 카운트 값들(CV) 전체를 제2 누적기(144)로 출력하고, 제2 누적기(144)는 이진 카운트 값들(CV)의 총 비트 수에 대응되는 제2 누적 값(A2)을 생성할 수 있다.

[0054] 제1 누적 값(A1)이 0 값들 또는 1 값들의 개수에 대응되고 제2 누적 값(A2)이 이진 카운트 값들(CV)의 총 비트 수에 대응되는 경우, 판단기(145)는 제2 누적 값(A2)에 대한 제1 누적 값(A1)의 비율에 기초하여 검증 신호(VS)를 생성할 수 있다. 판단기(145)는 제2 누적 값(A2)에 대한 제1 누적 값(A1)의 비율을 계산할 수 있다. 이러한 비율은 이진 카운트 값들(CV)의 총 비트 수에 대한 0 값들(C0) (또는 1 값들(C1))의 개수의 비율일 수 있다. 판단기(145)는 해당 비율이 기준 범위 이내인지 판단할 수 있다. 여기에서, 기준 범위는 이진 카운트 값들(CV)이 난수(RN)로 사용될 수 있을 정도의 랜덤성을 확보한 것으로 인정되는 허용 오차 범위일 수 있다. 이상적으로, 표본이 충분히 크다면, 진성 난수에 대응되는 비율은 50%에 수렴할 것이다.

[0055] 해당 비율이 기준 범위 이내인 경우, 판단기(145)는 이진 카운트 값들(CV)이 유효한 것으로 판단하고, 활성화 값 (일례로, 1 값)을 갖는 검증 신호(VS)를 생성할 수 있다. 해당 비율이 기준 범위를 벗어난 경우, 판단기(145)는 이진 카운트 값들(CV)이 유효한 진성 난수가 아닌 것으로 판단하고, 비활성화 값 (일례로, 0 값)을 갖는 검증 신호(VS)를 생성할 수 있다. 검증 신호(VS)가 활성화 값 (일례로, 1 값)을 갖는 경우, 멀티플렉서(MUX)는 이진 카운트 값들(CV)을 난수(RN)로 출력할 수 있다. 검증 신호(VS)가 비활성화 값 (일례로, 0 값)을 갖는 경우, 멀티플렉서(MUX)는 이진 카운트 값들(CV)의 출력을 차단할 수 있다.

[0056] 도 6은 도 5의 판단기의 예시적인 블록도이다. 도 6의 판단기(145_1)는 이진 카운트 값들(CV)에서 0 값들의 개수 및 1 값들의 개수의 차이에 기초하여 유효성을 판단하는 예시적인 구성으로 이해될 것이다. 도 6을 참조하면, 판단기(145_1)는 제1 레지스터(146_1), 제2 레지스터(147_1), 감산기(148_1), 및 기준 값 비교기(149_1)를 포함할 수 있다.

[0057] 제1 레지스터(146_1)는 제1 누적 값(A1)을 임시 저장하고, 제2 레지스터(147_1)는 제2 누적 값(A2)을 임시 저장한다. 제1 레지스터(146_1) 및 제2 레지스터(147_1)는 클럭 신호(CLK)에 동기화되어 동작할 수 있다. 제1 누적 값(A1)은 도 5의 0 값들(C0)의 개수에 대응되고, 제2 누적 값(A2)은 도 5의 1 값들(C1)의 개수에 대응된다. 제1 레지스터(146_1) 및 제2 레지스터(147_1)는 클럭 신호(CLK)에 기초하여, 제1 누적 값(A1) 및 제2 누적 값(A2)을 감산기(148_1)로 출력할 수 있다.

[0058] 감산기(148_1)는 제1 누적 값(A1) 및 제2 누적 값(A2)의 차이를 계산할 수 있다. 이러한 차이는 0 값들(C0)의 개수와 1 값들(C1)의 개수의 차이일 수 있다. 감산기(148_1)는 이진 카운트 값들(CV)의 0 개수와 1 개수의 차이에 대응되는 감산 값(SU)을 생성하여, 기준 값 비교기(149_1)로 출력할 수 있다.

[0059] 기준 값 비교기(149_1)는 감산 값(SU)이 기준 범위(RR1) 이내인지 판단할 수 있다. 여기에서, 기준 범위(RR1)는 이진 카운트 값들(CV)이 난수(RN)로 사용될 수 있을 정도의 랜덤성을 확보한 것으로 인정되는 허용 오차 범위일 수 있다. 일례로, 기준 범위(RR1)는 0을 기준으로 허용 오차 범위만큼 대칭된 상한 및 하한을 가질 수 있다. 감산 값(SU)이 기준 범위(RR1) 이내인 경우, 기준 값 비교기(149_1)는 활성화 값 (일례로, 1 값)을 갖는 검증 신호(VS)를 생성할 수 있다. 감산 값(SU)이 기준 범위(RR1)를 벗어난 경우, 기준 값 비교기(149_1)는 비활성화 값 (일례로, 0 값)을 갖는 검증 신호(VS)를 생성할 수 있다.

[0060] 도 7은 도 5의 판단기의 예시적인 블록도이다. 도 7의 판단기(145_2)는 이진 카운트 값들(CV)의 총 비트 수에 대한 0 값들의 개수 (또는 1 값들의 개수)의 비율에 기초하여 유효성을 판단하는 예시적인 구성으로 이해될 것이다. 도 7을 참조하면, 판단기(145_2)는 제1 레지스터(146_2), 제2 레지스터(147_2), 비율 계산기(148_2), 및 기준 값 비교기(149_2)를 포함할 수 있다.

[0061] 제1 레지스터(146_2)는 제1 누적 값(A1)을 임시 저장하고, 제2 레지스터(147_2)는 제2 누적 값(A2)을 임시 저장한다. 제1 레지스터(146_2) 및 제2 레지스터(147_2)는 클럭 신호(CLK)에 동기화되어 동작할 수 있다. 제1 누적 값(A1)은 이진 카운트 값들(CV)에 포함된 0 값들의 개수 또는 1 값들의 개수에 대응될 수 있다. 제2 누적 값(A2)은 이진 카운트 값들(CV)의 총 비트 수에 대응될 수 있다. 제1 레지스터(146_2) 및 제2 레지스터(147_2)는 클럭 신호(CLK)에 기초하여, 제1 누적 값(A1) 및 제2 누적 값(A2)을 비율 계산기(148_2)로 출력할 수 있다.

[0062] 비율 계산기(148_2)는 제2 누적 값(A2)에 대한 제1 누적 값(A1)의 비율을 계산할 수 있다. 이러한 비율은 이진 카운트 값들(CV)의 총 비트 수에 대한 0 값들(C0) (또는 1 값들(C1))의 개수의 비율일 수 있다. 비율 계산기

(148_2)는 제1 누적 값(A1)을 제2 누적 값(A2)으로 나누어 비율 값(RA)을 생성할 수 있다.

[0063] 기준 값 비교기(149_2)는 비율 값(RA)이 기준 범위(RR2) 이내인지 판단할 수 있다. 여기에서, 기준 범위(RR2)는 이진 카운트 값들(CV)이 난수(RN)로 사용될 수 있을 정도의 랜덤성을 확보한 것으로 인정되는 허용 오차 범위일 수 있다. 일례로, 기준 범위(RR2)는 0.5(50%)를 기준으로 허용 오차 범위만큼 대칭된 상한 및 하한을 가질 수 있다. 비율 값(RA)이 기준 범위(RR2) 이내인 경우, 기준 값 비교기(149_2)는 활성화 값 (일례로, 1 값)을 갖는 검증 신호(VS)를 생성할 수 있다. 비율 값(RA)이 기준 범위(RR2)를 벗어난 경우, 기준 값 비교기(149_2)는 비활성화 값 (일례로, 0 값)을 갖는 검증 신호(VS)를 생성할 수 있다.

[0064] 도 8은 도 1의 난수 생성 장치의 동작 방법의 예시적인 순서도이다. 도 8의 단계들은 도 1 내지 도 7에서 설명된 난수 생성 장치(100)에서 수행될 수 있다. 설명의 편의상 도 1의 도면 부호를 참조하여, 도 8이 설명된다.

[0065] S110 단계에서, 난수 생성 장치(100)는 초기화 동작을 수행한다. 일례로, 초기화 동작 이전에 수행된 난수 생성 과정에서 저장된 값들, 신호들 등이 리셋될 수 있다.

[0066] S120 단계에서, 난수 생성 장치(100)의 카운터(130)는 이진 카운트 값들(CV)을 생성한다. 이를 위하여, 소스 검출기(110)는 소스로부터 방출된 입자들(pt)을 검출하여 검출 신호(DS)를 생성할 수 있다. 펄스 생성기(120)는 검출된 입자들(pt) 각각의 검출 시간에 대응되는 펄스들을 생성할 수 있다. 카운터(130)는 펄스들 사이의 시간 간격들 동안 클럭들의 개수를 카운트하여 이진 카운트 값들(CV)을 생성할 수 있다.

[0067] S130 단계에서, 난수 생성 장치(100)의 검증 회로(140)는 이진 카운트 값들(CV)에서 0 값들 및/또는 1 값들을 추출한다. S130 단계는 도 5의 비교기(141)에서 수행될 수 있다. 0 값들의 개수 및 1 값들의 개수의 차이에 기초하여 유효성을 판단하는 실시예에서, 비교기(141)는 0 값들 및 1 값들을 추출할 수 있다. 이진 카운트 값들(CV)의 총 비트 수에 대한 0 값들의 개수 (또는 1 값들의 개수)의 비율에 기초하여 유효성을 판단하는 실시예에서, 비교기(141)는 0 값들을 추출하거나 1 값들을 추출할 수 있다.

[0068] S140 단계에서, 난수 생성 장치(100)의 검증 회로(140)는 추출된 0 값들 및/또는 1 값들을 누적할 수 있다. S140 단계는 도 5의 누적기(142)에서 수행될 수 있다. 0 값들의 개수 및 1 값들의 개수의 차이에 기초하여 유효성을 판단하는 실시예에서, 누적기(142)는 0 값들의 개수에 대응되는 제1 누적 값을 생성하고, 1 값들의 개수에 대응되는 제2 누적 값을 생성할 수 있다. 총 비트 수에 대한 0 값들의 개수 (또는 1 값들의 개수)의 비율에 기초하여 유효성을 판단하는 실시예에서, 누적기(142)는 0 값들의 개수 또는 1 값들의 개수에 대응되는 제1 누적 값을 생성하고, 이진 카운트 값들(CV)의 총 비트 수에 대응되는 제2 누적 값을 생성할 수 있다.

[0069] S150 단계에서, 난수 생성 장치(100)의 검증 회로(140)는 0 값들의 개수 및 1 값들의 개수의 차이가 기준 범위 이내인지 판단할 수 있다. 이러한 동작은 도 6의 판단기(145_1)에서 수행될 수 있다. 판단기(145_1)는 제1 누적 값과 제2 누적 값을 감산하고 감산 값이 기준 범위 이내인지 판단할 수 있다.

[0070] 또는, S150 단계에서, 검증 회로(140)는 이진 카운트 값들(CV)의 총 비트 수에 대한 0 값들의 개수 (또는 1 값들의 개수)의 비율이 기준 범위 이내인지 판단할 수 있다. 이러한 동작은 도 7의 판단기(145_2)에서 수행될 수 있다. 판단기(145_2)는 제2 누적 값에 대한 제1 누적 값의 비율을 계산하고, 비율 값이 기준 범위 이내인지 판단할 수 있다.

[0071] 감산 값 또는 비율 값이 기준 범위 이내인 경우, S160 단계가 진행된다. S160 단계에서, 검증 회로(140)는 이진 카운트 값들(CV)을 난수(RN)로 출력한다. 감산 값 또는 비율 값이 기준 범위 이내인 경우, 검증 회로(140)는 이진 카운트 값들(CV)이 유효한 것으로 판단하고, 활성화 값 (일례로, 1 값)을 갖는 검증 신호(VS)를 생성할 수 있다. 검증 신호(VS)는 도 5의 멀티플렉서(MUX)에 입력되고, 멀티플렉서(MUX)는 활성화 값에 기초하여 이진 카운트 값들(CV)을 난수(RN)로 출력할 수 있다.

[0072] 감산 값 또는 비율 값이 기준 범위를 벗어난 경우, S170 단계가 진행된다. S170 단계에서, 검증 회로(140)는 이진 카운트 값들(CV)의 출력을 차단한다. 감산 값 또는 비율 값이 기준 범위를 벗어난 경우, 검증 회로(140)는 이진 카운트 값들(CV)이 유효한 진성 난수가 아닌 것으로 판단하고, 비활성화 값 (일례로, 0 값)을 갖는 검증 신호(VS)를 생성할 수 있다. 검증 신호(VS)는 도 5의 멀티플렉서(MUX)에 입력되고, 멀티플렉서(MUX)는 비활성화 값에 기초하여 이진 카운트 값들(CV)을 출력하지 않을 수 있다.

[0073] 위에서 설명한 내용은 본 발명을 실시하기 위한 구체적인 예들이다. 본 발명에는 위에서 설명한 실시 예들뿐만 아니라, 단순하게 설계 변경하거나 용이하게 변경할 수 있는 실시 예들도 포함될 것이다. 또한, 본 발명에는 상술한 실시 예들을 이용하여 앞으로 용이하게 변형하여 실시할 수 있는 기술들도 포함될 것이다.

부호의 설명

[0074] 100: 난수 생성 장치 110: 소스 검출기

120: 펄스 생성기 121: 전치 증폭기

122: 아날로그-디지털 변환기 130: 카운터

131: 플립플롭 132: 클럭 카운터

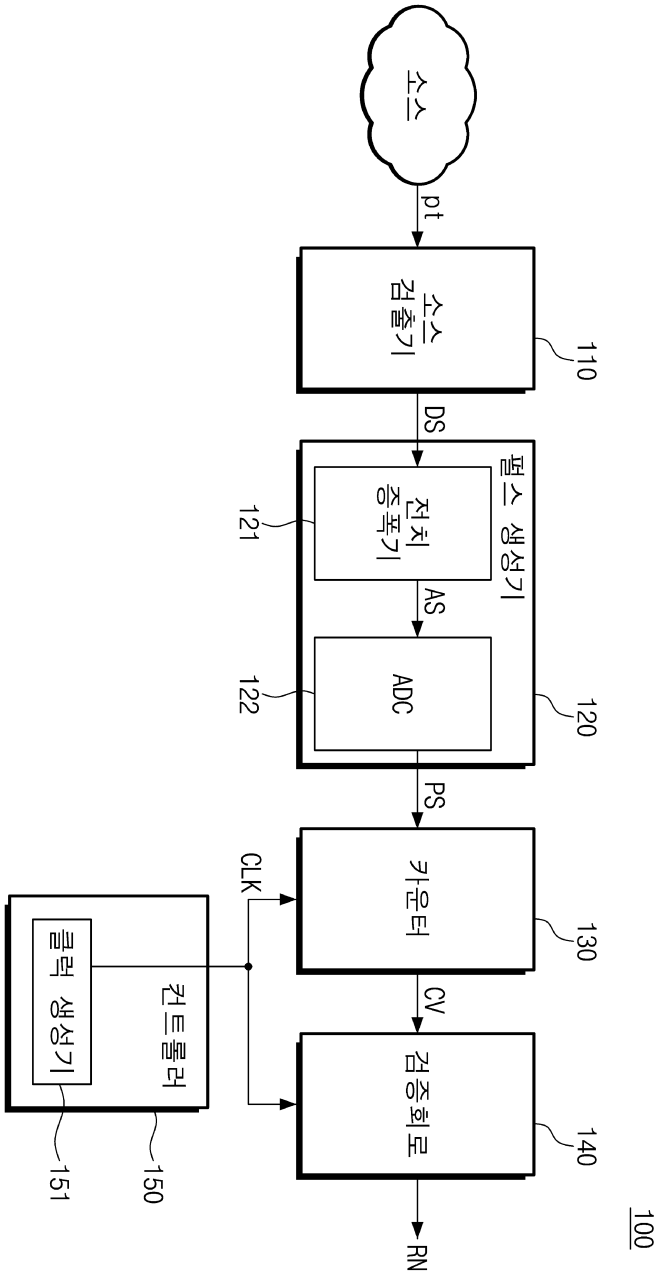
140: 검증 회로 141: 비교기

142: 누적기 145, 145_1, 145_2: 판단기

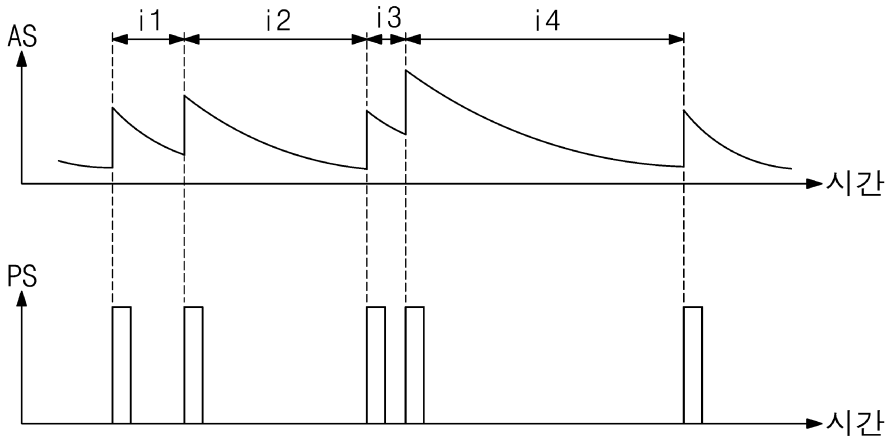
150: 컨트롤러 MUX: 멀티플렉서

도면

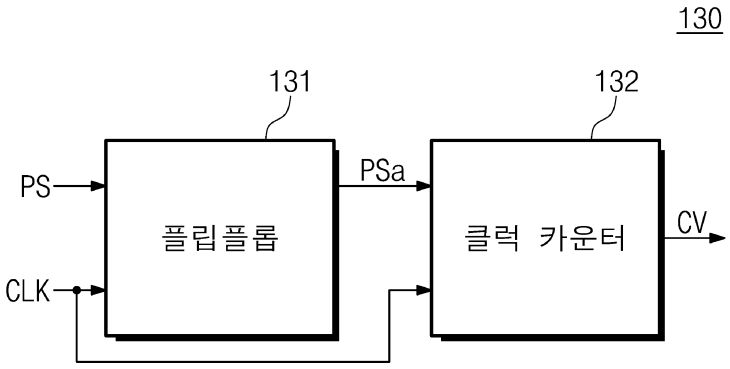
도면1



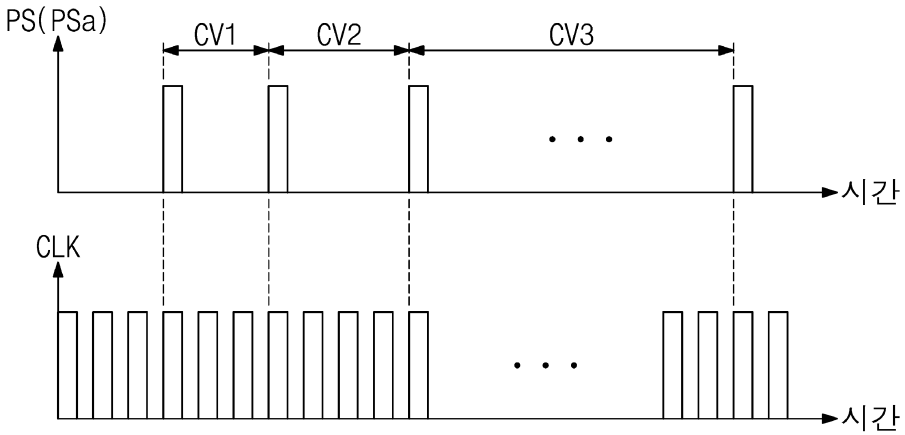
도면2


AS
i1
i2
i3
i4
시간
PS
시간

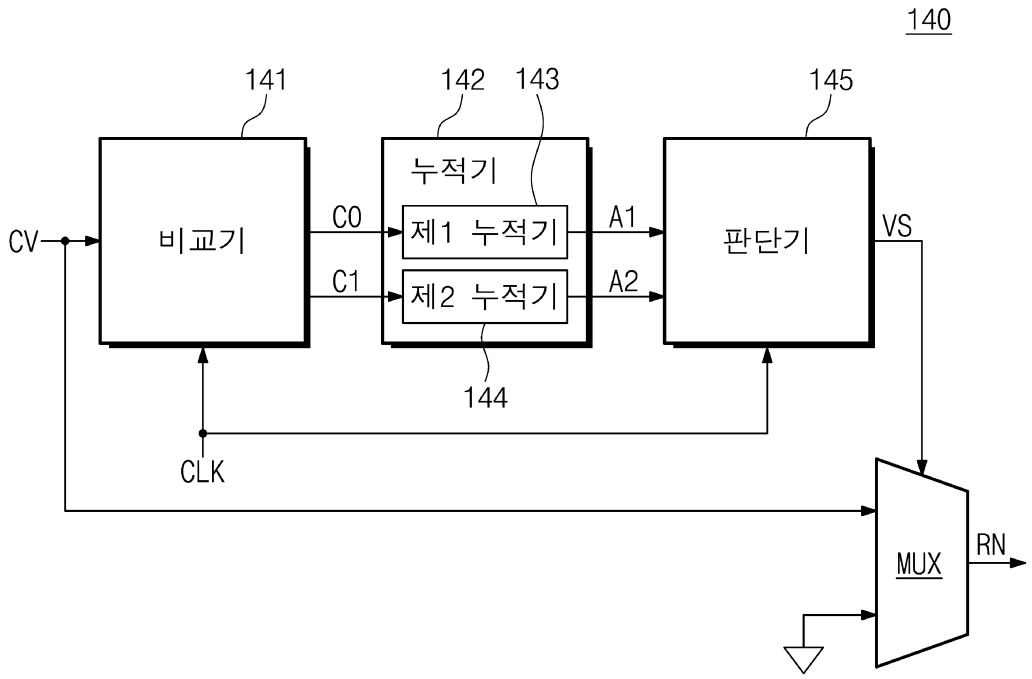
도면3


130
131
132
PS
PSa
CV
CLK
플립플롭
클럭 카운터

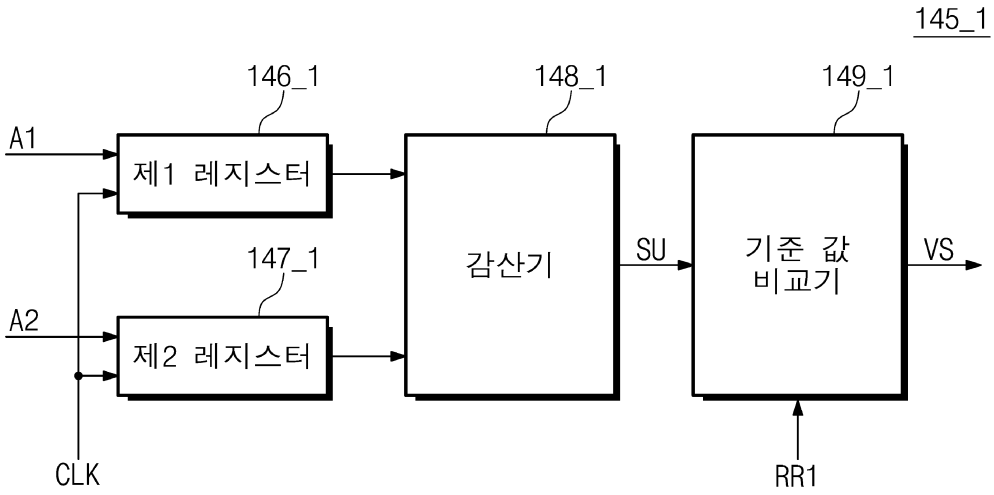
도면4


PS(PSa)
CV1
CV2
CV3
시간
CLK
시간

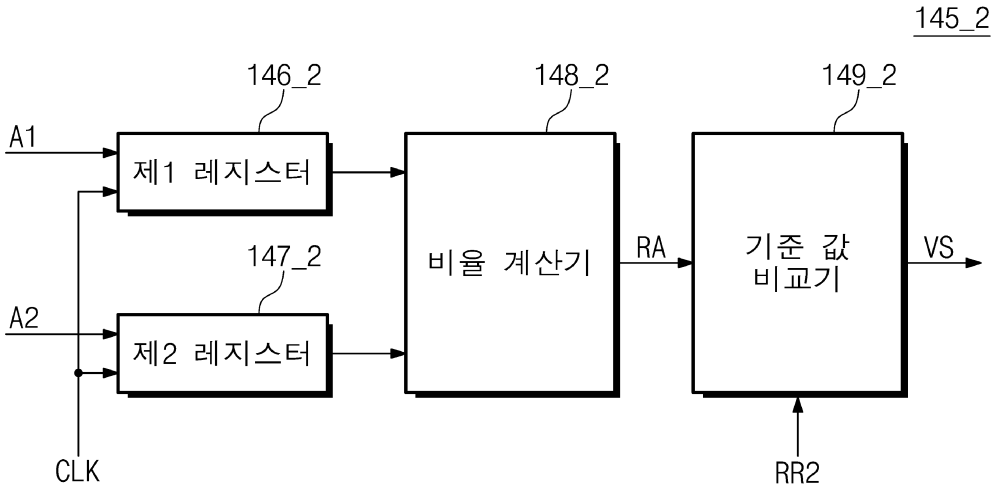
도면5


140
141
142
143
145
CV
비교기
C0
C1
누적기
제1 누적기
제2 누적기
A1
A2
판단기
VS
144
CLK
MUX
RN

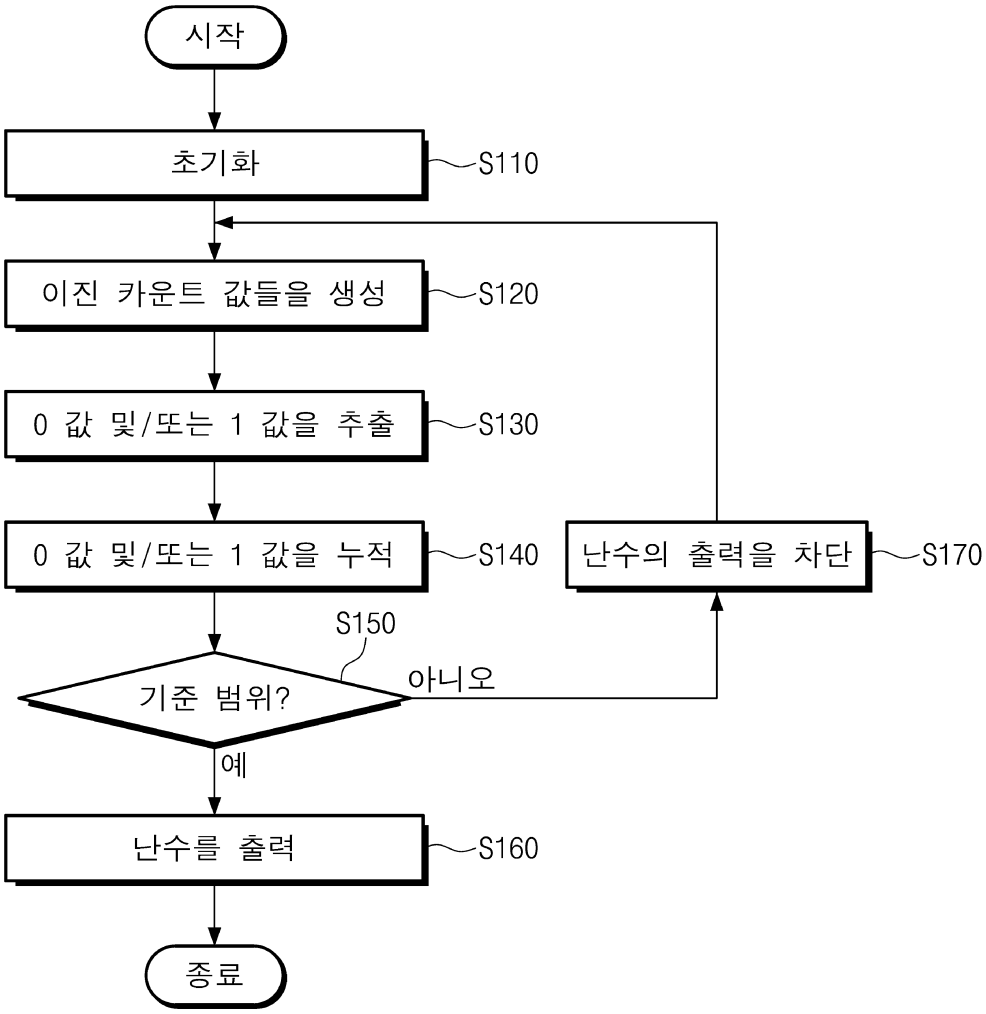
도면6


145_1
146_1
148_1
149_1
A1
제1 레지스터
147_1
A2
제2 레지스터
감산기
SU
기준 값
비교기
VS
CLK
RR1

도면7


145_2
146_2
148_2
149_2
A1
제1 레지스터
147_2
A2
제2 레지스터
CLK
비율 계산기
RA
기준 값
비교기
VS
RR2

도면8


시작
초기화
S110
이진 카운트 값들을 생성
S120
0 값 및/또는 1 값을 추출
S130
0 값 및/또는 1 값을 누적
S140
난수의 출력을 차단
S170
S150
기준 범위?
아니오
예
난수를 출력
S160
종료