(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0050220
(43) 공개일자 2008년06월05일

(51) Int. Cl.
G06F 7/58 (2006.01)
(21) 출원번호 10-2007-0057400
(22) 출원일자 2007년06월12일
심사청구일자 2007년06월12일
(30) 우선권주장
1020060120454 2006년12월01일 대한민국(KR)

(71) 출원인
한국전자통신연구원
대전 유성구 가정동 161번지
(72) 발명자
박영수
대전 서구 탄방동 산호아파트 101-907
박지만
대전 유성구 송강동 청솔아파트 310-1208
전성익
대전 유성구 어은동 한빛아파트 107동 704호
(74) 대리인
특허법인 씨엔에스 · 로고스

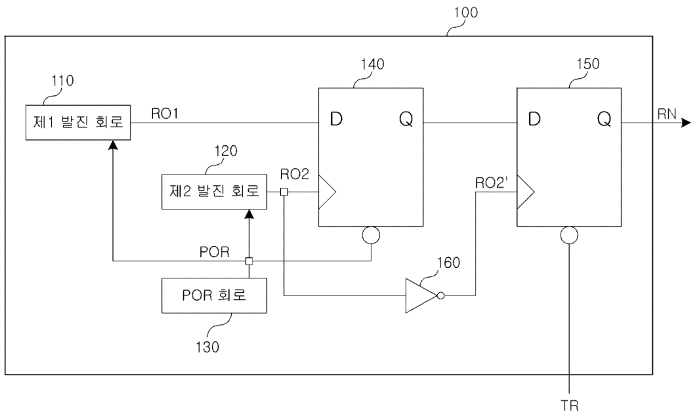
전체 청구항 수 : 총 11 항

(54) 오실레이터 샘플링 방법을 이용한 실난수 발생 장치

(57) 요 약

본 발명은 오실레이터 샘플링 방법을 이용한 실난수 발생 장치에 관한 것으로, 자체 출력을 데이터 입력으로 제공하는 제 1 발진 회로; 자체 출력을 클럭 입력으로 제공하는 제 2 발진 회로; 자체 출력을 리셋 입력으로 제공하는 POR(Power-On-Reset) 회로; 상기 데이터, 클럭 및 리셋을 입력으로 하여 동작하는 제 1 D-플립플롭; 상기 제 2 발진 회로의 출력을 인버팅하여 출력하는 인버터; 상기 제 1 D-플립플롭의 출력을 데이터 입력으로 하고, 상기 인버터의 출력을 클럭 입력으로 하며, 외부 인가되는 리셋 신호를 입력으로 동작하여 실난수를 발생시키는 제 2 D-플립플롭을 포함하여 구성되며, 이에 의하여 그 구현이 용이하며, 고속, 저소비전력 및 저가격의 실난수를 발생할 수 있는 효과를 가진다.

대표도



특허청구의 범위

청구항 1

자체 출력을 데이터 입력으로 제공하는 제 1 발진 회로;

자체 출력을 클럭 입력으로 제공하는 제 2 발진 회로;

자체 출력을 리셋 입력으로 제공하는 POR(Power-On-Reset) 회로;

상기 데이터, 클럭 및 리셋을 입력으로 하여 동작하는 제 1 D-플립플롭;

상기 제 2 발진 회로의 출력을 인버팅하여 출력하는 인버터; 및

상기 제 1 D-플립플롭의 출력을 데이터 입력으로 하고, 상기 인버터의 출력을 클럭 입력으로 하며, 외부 인가되는 리셋 신호를 입력으로 동작하여 실난수를 발생시키는 제 2 D-플립플롭을 포함하되,

상기 POR 회로는 상기 제 1 및 제 2 발진 회로에 동작 개시 신호를 제공하고, 상기 제 1 D-플립플롭에 리셋 신호를 제공하는 것을 특징으로 하는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치.

청구항 2

제1항에 있어서,

상기 제 1 및 제 2 발진 회로는,

입력을 반전시켜 출력하는 링발진기; 및

상기 링발진기의 출력과 외부 인가 신호를 입력으로 하여 발진 회로의 출력을 생성하는 NAND 게이트를 포함하되,

상기 NAND 게이트는 출력을 피드백하여 링발진기에 제공하는 것을 특징으로 하는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치.

청구항 3

제1항에 있어서,

상기 POR 회로는,

전원에 연결된 저항; 및

접지에 연결된 콘덴서를 포함하되,

상기 저항과 콘덴서는 직렬로 연결되어, 상기 직렬연결 지점을 출력 단자로 하는 것을 특징으로 하는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치.

청구항 4

제1항에 있어서,

상기 POR 회로는,

임의의 지연 시간을 갖고 출력이 저(Low) 수준에서 고(High) 수준 또는 이와 반대의 동작을 수행하는 논리 모듈을 포함하는 것을 특징으로 하는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치.

청구항 5

제1항에 있어서,

상기 실난수 발생 장치는,

반복된 구조로 병렬 구성되어 임의 비트 크기의 실난수를 발생시키는 것을 특징으로 하는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치.

청구항 6

제 1항에 있어서,

상기 실난수 발생 장치는,

상기 제 1 및 제 2 발진 회로, 상기 POR 회로 및 상기 인버터를 리소스 공유하고, 그 나머지가 반복된 구조로 병렬 구성되도록 하여, 임의 비트 크기의 실난수를 발생시키는 것을 특징으로 하는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치.

청구항 7

자체 출력을 데이터 입력으로 제공하는 지터 회로;

자체 출력을 클럭 입력으로 제공하는 제 2 발진 회로;

자체 출력을 리셋 입력으로 제공하는 POR 회로;

상기 POR 회로의 출력을 입력으로 하여 동작하고, 자체 출력을 상기 지터 회로의 동작 개시 신호로 제공하는 제 3 발진 회로;

상기 데이터, 클럭 및 리셋을 입력으로 하여 동작하는 제 1 D-플립플롭;

상기 제 2 발진 회로의 출력을 인버팅하여 출력하는 인버터; 및

상기 제 1 D-플립플롭의 출력을 데이터 입력으로 하고, 상기 인버터의 출력을 클럭 입력으로 하며, 외부 인가되는 리셋 신호를 입력으로 동작하여 실난수를 발생시키는 제 2 D-플립플롭을 포함하되,

상기 POR 회로는 상기 제 2 및 제 3 발진 회로에 동작 개시 신호를 제공하고, 상기 제 1 D-플립플롭에 리셋 신호를 제공하는 것을 특징으로 하는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치.

청구항 8

제7항에 있어서,

상기 지터 회로는,

반도체 집적회로 내에서 취득 가능한 열, 온도, 전류, 전압 및 주파수 중 적어도 하나를 입력하여 신호를 출력하는 잡음원;

상기 잡음원으로부터 출력된 신호를 증폭하여 디지털 신호를 생성하는 증폭기; 및

상기 증폭기에서 생성된 신호를 외부 입력 신호에 따라서 출력하는 버퍼를 포함하는 것을 특징으로 하는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치.

청구항 9

제7항에 있어서,

상기 제 2 및 제 3 발진 회로는,

입력을 반전시켜 출력하는 기능을 하는 링발진기; 및

상기 링발진기의 출력과 외부 인가 신호를 입력으로 하여 발진 회로의 출력을 생성하는 NAND 게이트를 포함하되,

상기 NAND 게이트는 출력을 피드백하여 링발진기에 제공하는 것을 특징으로 하는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치.

청구항 10

제7항에 있어서,

상기 실난수 발생 장치는,

반복된 구조로 병렬 구성되어 임의 비트 크기의 실난수를 발생시키는 것을 특징으로 하는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치.

청구항 11

제7항에 있어서,

상기 실난수 발생 장치는,

상기 제 2 및 제 3 발진 회로, 상기 POR 회로, 상기 지터 회로 및 상기 인버터를 리소스 공유하고, 그 나머지가 반복된 구조로 병렬 구성되도록 하여, 임의 비트 크기의 실난수를 발생시키는 것을 특징으로 하는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<16> 본 발명은 오실레이터 샘플링 방법을 이용한 실난수 발생 장치에 관한 것으로, 특히 IC 칩에 집적이 가능하며 오실레이터 샘플링 방법을 이용한 고속 동작 및 저전력 특성의 실난수 생성이 가능한 실난수 발생 장치에 관한 것이다.

<17> 일반적으로 난수 발생 장치는 실난수 발생 장치와 의사난수 발생 장치로 분류된다.

<18> 통상적으로 의사난수 발생 장치는, 퍼스널 컴퓨터의 조립 난수 생성과 같이 논리 회로와 소프트웨어에 의하여 난수를 생성하는 방법을 사용하며, 소형 회로로 그 구현이 간단한 장점이 있으나, 동일한 시드(seed)는 동일 난수 생성시키므로 초기 상태가 알려지는 경우 용이하게 난수 예측이 가능하여 기밀보호의 관점에서 불충분한 단점을 가진다.

<19> 실난수 발생 장치는 물리적 현상 즉, 전기적으로는 저항체의 열잡음, 반도체에서의 쇼트 잡음(노이즈), 광학적으로 방사선의 발생파 등을 이용하여 난수를 생성하는 방법을 사용함으로, 의사난수 발생 방법보다 안전한 난수 생성을 보장하며, 증폭, 오실레이터 샘플링, 카오스 등과 같은 방법 및 기술로 구현되어 기밀보호가 뛰어난 장점을 가진다.

<20> 그러나, 실난수 발생 장치는 상기 잡음 수준이 작아 난수 추출을 위해 잡음 수준을 높여야하는 경우, IC 미세화로 낮아지는 동작 전압 등으로 IC 칩 구현 적합성 등을 해결해야 하는 단점을 가진다.

<21> 이와 같은 실난수 발생 장치의 구현 방법에 대해 살펴보면, 먼저 증폭 방법은 통상적으로 신호 증폭 수단과 AD 변환 수단으로 구성되어, 낮은 신호 수준을 증폭하는 기능을 수행한다.

<22> 그런데, 증폭 방법은 낮은 신호 수준을 높이기 위해 높은 게인(gain)의 증폭기를 필요로 하여, 신호 증폭에 의한 증폭기 회로 규모의 증가로 소비 전력 증가를 초래하며, 디지털 회로와의 격리 및 전원으로부터의 스파이크 노이즈 제어를 위한 큰 저항 및 커패시터를 필요로 하여 집적도를 저하시키는 문제점을 가진다.

<23> 다음으로, 오실레이터 샘플링 방법은 신호 발진 수단과 신호 샘플링 수단으로 구성된다. 여기서, 신호 발진 수단은 링 발진기와 같이 루프 상에 접속되는 복수 개의 지연 회로로 구성되며, 일예로 전압 제어 발진(VCO), 크리스탈 발진 등이 있으나 발진 회로의 특성으로 인한 소비전력의 증가와 난수 데이터의 주기성이 노출될 우려가 있다.

<24> 카오스 방법은, 카오스 처리 방법과 신호 이론을 적용한 수단으로 구성된다.

<25> 실제로 난수 발생에 있어서 잡음의 수준은 낮기 때문에 매우 큰 감쇄 간섭은 난수 발생 장치의 출력 또는 엔트로피(통계적인 독립) 모두를 빼앗아 간다.

<26> 이에, 잡음 신호의 증폭과 샘플링은 증폭기가 피할 수 없는 대역 제한과 경계가 일반적으로 바이어스 되어 더욱 엔트로피를 감소시키며 고-엔트로피 비트의 고속 및 저 가격의 실현이 어렵다. 이러한 문제를 극복하기 위하여 카오스 처리 방법과 신호 이론을 적용한다.

<27> 그러나, 카오스 방법은 실난수 발생 장치의 잡음이 아날로그로 구현됨에 의해 아날로그 신호를 디지털화한 후 적용 알고리즘으로 후 처리하는 디지털 로직으로 구현된다. 따라서, 카오스 방법은 완전한 디지털 설계를 구현하지 못하는 단점과 함께 신속한 시스템 프로토타입 및 적은 규모의 제품 제작과 신기술로의 전이 용이의 가능성이 방해되어 하드웨어로의 구현 갭을 포함하여, 실난수 발생 장치를 제조함에 있어서 상기 갭에 의해 난수 발생 장치의 단가를 상승시키는 문제점을 가진다.

<28> 만약, 실난수 생성에 이용되는 물리적인 현상의 공통적인 문제인 복잡한 회로와 물리적/회로 크기를 해결하기 위하여 취약한 회로를 사용하지 않고 랜덤 특성을 가지는 불완전 전송(meta-stability), 위상 및/또는 주파수(phase and/or frequency) 이용 지터(jitter) 등을 적용할 경우, 전압 및 주파수(voltage & frequency) 변화 결합, 물리적 소스 검증과 전기적인 공격에 대한 저항 검증이 필요하다. 또한 서멀(thermal) 또는 산탄 잡음(shot noise)을 적용하여 개별적으로 또는 집적한 형태로 구현 가능하므로 진공관 산탄 잡음(vacuum tube shot noise), 방사성붕괴(radioactive decay), 네온 발광관(neon lamp discharge), 클럭 지터(clock jitter) 및 PC 하드 드라이버 변동(hard drive fluctuations) 등이 잡음원으로 사용 가능하나 실제 잡음원의 신호 수준은 매우 낮기 때문에 큰 감쇄 간섭은 엔트로피를 감소시킨다. 엔트로피를 향상시키기 위하여 디지털 비선형 필터링 또는 감쇄 압축(lossy compression) 등을 적용할 수 있으나 처리 속도(bit-rate)가 감소한다.

<29> 한편, 상기와 같은 난수 발생 장치의 단점을 극복하고자, 증폭, 오실레이터 샘플링, 카오스 방법을 이용한 난수 발생 장치를 구현하려는 노력이 계속되고 있다.

<30> 이러한 노력 중에서의 하나가 Fairfield, Mortenson and Coulthart[참고 문헌 1]으로 고/저(high/low) 주파수의 샘플링하는 발진기, 바이어스를 제거하기 위한 패리티 필터, 스크램블하는 LFSR로 구성되었다.

<31> 또한 Intel[참고 문헌 2]은 열잡음의 증폭 수단으로 VCO와 샘플링하는 발진기로 구성되었다.

<32> 그리고 Stojanovski[참고 문헌 3] 등은 스위치 전류(switched current) 기술로 실난수 발생 장치를 구성하여 난수를 발생하도록 만드는 기술이다.

<33> [참고문헌 1] R.C. Fair_eld, R.L. Mortenson, and K.B. Coulthart. An LSI Random Number Generator (RNG). In Advances in Cryptography: Proceedings of Crypto 84, pages 203.230. LNCS 0196, Springer-Verlag, 1984.

<34> [참고문헌 2] B. Jun and P. Kocher. The intel random number generator. White paper by Cryptographic Research Inc., 1999.

<35> ftp://download.intel.com/design/security/rng/CRIwp.pdf.

<36> [참고문헌 3] T. Stojanovski, J. Pil, and L. Kocarev. Chaos-based random number generators. Part II: practical realization. IEEE Transactions on Circuits and Systems . I: fundamental Theory and Application, 48(3):382.385, March 2001.

<37> 그러나 상기 노력 예에 따른 기술은 LFSR의 스크램블러로의 적용, 증폭과 샘플링의 복합사용과 SHA-1 기반 혼합 기능의 소프트웨어 구조, 아날로그 기반의 설계 등의 단점을 가진다.

<38> 또한, 상기 예들에 따른 기술은 성능면에서도 저속임에 따라, 상기 노력 예에 따른 기술은 모바일 기기 등에서 요구되는 저전력 실난수 발생 장치에는 적용되기 어려운 문제점이 있다.

발명이 이루고자 하는 기술적 과제

<39> 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은 구현이 용이하고, 저전력 난수를 발생할 수 있는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치를 제공하는데 있다.

<40> 그리고, 상기와 같은 문제점을 해결하기 위한 본 발명의 다른 목적은 병렬형 실난수를 발생하는 오실레이터 샘플링 방법을 이용한 실난수 발생 장치를 제공하는데 있다.

발명의 구성 및 작용

<41> 상기와 같은 목적을 달성하기 위한 본 발명의 일 실시예에 따른 오실레이터 샘플링 방법을 이용한 실난수 발생 장치는, 자체 출력을 데이터 입력으로 제공하는 제 1 발진 회로; 자체 출력을 클럭 입력으로 제공하는 제 2 발진 회로; 자체 출력을 리셋 입력으로 제공하는 POR(Power-On-Reset) 회로; 상기 데이터, 클럭 및 리셋을 입력으

로 하여 동작하는 제 1 D-플립플롭; 상기 제 2 발진 회로의 출력을 인버팅하여 출력하는 인버터; 상기 제 1 D-플립플롭의 출력을 데이터 입력으로 하고, 상기 인버터의 출력을 클럭 입력으로 하며, 외부 인가되는 리셋 신호를 입력으로 동작하여 실난수를 발생시키는 제 2 D-플립플롭을 포함하되, 상기 POR 회로는 상기 제 1 및 제 2 발진 회로에 동작 개시 신호를 제공하고, 상기 제 1 D-플립플롭에 리셋 신호를 제공하는 것을 특징으로 한다.

<42> 상기 제 1 및 제 2 발진 회로는, 입력을 반전시켜 출력하는 링발진기; 상기 링발진기의 출력과 외부 인가 신호를 입력으로 하여 발진 회로의 출력을 생성하는 NAND 게이트를 포함하되, 상기 NAND 게이트는 출력을 피드백하여 링발진기에 제공하는 것을 특징으로 한다.

<43> 상기 POR 회로는, 전원에 연결된 저항; 접지에 연결된 콘덴서를 포함하되, 상기 저항과 콘덴서는 직렬로 연결되어, 상기 직렬연결 지점을 출력 단자로 하는 것을 특징으로 한다.

<44> 상기 POR 회로는, 임의의 지연 시간을 갖고 출력이 저(Low) 수준에서 고(High) 수준 또는 이와 반대의 동작을 수행하는 논리 모듈을 포함하는 것을 특징으로 한다.

<45> 바람직하게 상기 실난수 발생 장치는, 반복된 구조로 병렬 구성되어 임의 비트 크기의 실난수를 발생시키는 것을 특징으로 한다.

<46> 바람직하게 상기 실난수 발생 장치는, 상기 제 1 및 제 2 발진 회로, 상기 POR 회로 및 상기 인버터를 리소스 공유하고, 그 나머지가 반복된 구조로 병렬 구성되도록 하여, 임의 비트 크기의 실난수를 발생시키는 것을 특징으로 한다.

<47> 상기와 같은 목적을 달성하기 위한 본 발명의 다른 실시예에 따른 오실레이터 샘플링 방법을 이용한 실난수 발생 장치는, 자체 출력을 데이터 입력으로 제공하는 지터 회로; 자체 출력을 클럭 입력으로 제공하는 제 2 발진 회로; 자체 출력을 리셋 입력으로 제공하는 POR 회로; 상기 POR 회로의 출력을 입력으로 하여 동작하고, 자체 출력을 상기 지터 회로의 동작 개시 신호로 제공하는 제 3 발진 회로; 상기 데이터, 클럭 및 리셋을 입력으로 하여 동작하는 제 1 D-플립플롭; 상기 제 2 발진 회로의 출력을 인버팅하여 출력하는 인버터; 상기 제 1 D-플립플롭의 출력을 데이터 입력으로 하고, 상기 인버터의 출력을 클럭 입력으로 하며, 외부 인가되는 리셋 신호를 입력으로 동작하여 실난수를 발생시키는 제 2 D-플립플롭을 포함하되, 상기 POR 회로는 상기 제 2 및 제 3 발진 회로에 동작 개시 신호를 제공하고, 상기 제 1 D-플립플롭에 리셋 신호를 제공하는 것을 특징으로 한다.

<48> 상기 지터 회로는, 반도체 집적회로 내에서 취득 가능한 열, 온도, 전류, 전압 및 주파수 중 적어도 하나를 입력하여 신호를 출력하는 잡음원; 상기 잡음원으로부터 출력된 신호를 증폭하여 디지털 신호를 생성하는 증폭기; 상기 증폭기에서 생성된 신호를 외부 입력 신호에 따라서 출력하는 버퍼를 포함하는 것을 특징으로 한다.

<49> 상기 제 2 및 제 3 발진 회로는, 입력을 반전시켜 출력하는 기능을 하는 링발진기; 상기 링발진기의 출력과 외부 인가 신호를 입력으로 하여 발진 회로의 출력을 생성하는 NAND 게이트를 포함하되, 상기 NAND 게이트는 출력을 피드백하여 링발진기에 제공하는 것을 특징으로 한다.

<50> 바람직하게 상기 실난수 발생 장치는, 반복된 구조로 병렬 구성되어 임의 비트 크기의 실난수를 발생시키는 것을 특징으로 한다.

<51> 바람직하게 상기 실난수 발생 장치는, 상기 제 2 및 제 3 발진 회로, 상기 POR 회로, 상기 지터 회로 및 상기 인버터를 리소스 공유하고, 그 나머지가 반복된 구조로 병렬 구성되도록 하여, 임의 비트 크기의 실난수를 발생시키는 것을 특징으로 한다.

<52> 이하 첨부된 도면을 참조하여 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있는 바람직한 실시 예를 상세히 설명한다. 다만, 본 발명의 바람직한 실시 예에 대한 동작 원리를 상세하게 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략한다.

<53> 또한, 도면 전체에 걸쳐 유사한 기능 및 작용을 하는 부분에 대해서는 동일한 도면 부호를 사용한다.

<54> 도 1은 본 발명의 바람직한 일실시예에 따른 실난수 발생 장치의 구성을 나타낸 블록도이다.

<55> 도 1을 참조하면, 본 발명의 실난수 발생 장치(100)는 제 1 및 제 2 발진 회로(110, 120), POR(Power-On-Reset) 회로(130), 제 1 및 제 2 D-플립플롭(140, 150) 및 인버터(160)를 기본 요소로 구성될 수 있으며, TR(Test Reset) 신호를 입력으로, RN(Random Number) 신호를 출력으로 한다.

<56> 이와 같은 구성을 갖는 실난수 발생 장치(100)에서 POR 회로(130)는 전원이 투입되고 일정한 시간이 지난 후에 POR 신호를 발생하여, 발생되는 POR 신호를 제 1 및 제 2 발진회로(110, 120)와 제 1 D-플립플롭(140)에 제공하는 기능을 수행한다.

<57> 이에, 제 1 발진 회로(110)는 POR 회로(130)의 출력 신호인 POR 신호를 입력으로 하고, 출력(RO1((Ring-oscillator Output 1))을 제 1 D-플립플롭(140)의 데이터 입력으로 제공한다.

<58> 그리고, 제 2 발진 회로(120)는 POR 회로(130)의 출력 신호인 POR 신호를 입력으로 하고, 출력(RO2)을 제 1 D-플립플롭(140)의 클럭으로 제공한다.

<59> 제 1 D-플립플롭(140)은 제 2 발진 회로(120)의 출력(RO2)을 클럭으로 하고 제 1 발진 회로(110) 출력(RO)을 데이터 입력으로 하여, 클럭이 상승 에지 트리거일 때 출력 단자 Q로 데이터를 출력한다. 또한, 제 1 D-플립플롭(140)은 리셋 단자에 입력되는 POR 신호 값에 따라서 제 1 D-플립플롭(140)의 값을 초기화된다.

<60> 제 2 D-플립플롭(150)은 제 1 D-플립플롭(140)의 출력을 데이터 입력으로 하고, 제 2 발진 회로(120)의 출력이 반전된 신호(RO2')를 클럭으로 하여 난수(RN)를 출력하는 기능을 수행한다. 또한, 제 2 D-플립플롭(150)은 리셋 단자에 입력되는 TR 신호 값에 따라서 상기 제 2 D-플립플롭(150)의 값을 초기화된다.

<61> 한편, 인버터(160)는 제 2 발진 회로(120)의 출력을 반전하여 제 2 D-플립플롭(150)의 클럭으로 제공하는 기능을 수행한다.

<62> 도 2는 본 발명의 바람직한 다른 실시예에 따른 실난수 발생 장치의 구성을 나타낸 블록도이다.

<63> 도 2를 참조하면, 본 발명의 실난수 발생 장치(100)는 지터 회로(170), 제 2 및 제 3 발진 회로(120, 180), POR 회로(130), 제 1 및 제 2 D-플립플롭(140,150) 및 인버터(160)를 기본 요소로 구성될 수 있으며, TR 신호를 입력으로, RN 신호를 출력으로 한다.

<64> 먼저, 이와 같은 구성을 갖는 실난수 발생 장치(100)에서 POR 회로(130)는 전원이 투입되고 일정한 시간이 지난 후에 POR 신호를 발생하여, 제 2 및 제 3 발진 회로(120, 180)와 제 1 D-플립플롭(140)에 제공하는 기능을 수행한다.

<65> 이에, 제 2 발진 회로(120)는 POR 회로(130)의 출력 신호인 POR을 입력으로 하고, 출력(RO2)을 제 1 D-플립플롭(140)의 클럭으로 제공하는 기능을 수행한다.

<66> 그리고, 제 3 발진 회로(180)는 POR 회로(130)의 출력 신호인 POR을 입력으로 하고, 출력을 지터 회로(170)의 입력으로 제공하는 기능을 수행한다.

<67> 지터 회로(170)는 제 3 발진 회로(180)의 출력 신호를 입력으로 하고, 출력(JO)을 제 1 D-플립플롭(140)의 데이터 입력으로 제공한다. 이때, 출력(JO)은 통상적으로 상기 제 2 발진 회로(120)의 출력보다 빠른 주기의 파형이다.

<68> 제 1 D-플립플롭(140)은 제 2 발진 회로(120)의 출력(RO2)을 클럭으로 하고 지터 회로(170)의 출력(JO)을 데이터 입력으로 하여, 클럭이 상승 에지 트리거일 때 출력 단자 Q로 데이터를 출력한다. 또한, 제 1 D-플립플롭(140)은 리셋 단자에 입력되는 POR 신호 값에 따라서 제 1 D-플립플롭(140)의 값을 초기화된다.

<69> 제 2 D-플립플롭(150)은 제 1 D-플립플롭(140)의 출력을 데이터 입력으로 하고, 제 2 발진 회로(120)의 출력이 반전된 신호(RO2')를 클럭으로 하여 난수(RN)를 출력하는 기능을 수행한다. 또한, 제 2 D-플립플롭(150)은 리셋 단자에 입력되는 TR 신호 값에 따라서 상기 제 2 D-플립플롭(150)의 값을 초기화된다.

<70> 한편, 인버터(160)는 제 2 발진 회로(120)의 출력을 반전하여 제 2 D-플립플롭(150)의 클럭으로 제공하는 기능을 수행한다.

<71> 다음으로, 도 1 및 도 2를 통해 살펴본 실난수 발생 장치(100)의 각 구성에 대해 도면을 참조하여 자세히 살펴보도록 한다.

<72> 도 3은 본 발명의 바람직한 일 실시예에 따라 실난수 발생 장치의 지터 회로를 도시한 블록도이다.

<73> 도 3에 도시된 바와 같이, 도 2의 실난수 발생 장치(100)가 구성하는 지터 회로(170)는, 잡음원(171), 증폭기(172) 및 버퍼(173)로 구성될 수 있으며, 제 3 발진 회로의 출력 신호인 'Enable' 신호를 입력으로, JO(Jitter Output) 신호를 출력으로 한다.

<74> 지터 회로(170)에서 잡음원(171)은 칩내의 집적이 가능한 열(온도), 전류, 전압, 주파수 등을 입력하여 신호를 출력하는 기능을 수행하며, 증폭기(172)는 잡음원(171)으로부터 출력된 낮은 수준의 신호를 증폭하여 디지털 신호를 생성하는 기능을 수행한다.

<75> 버퍼(173)는 외부 입력 신호(Enable)에 따라서 증폭기(172)에서 생성된 디지털 신호를 출력하는 기능을 수행한다. 여기서, 외부 입력 신호인 'Enable'은 실난수 발생 장치(100)의 동작에서 지터 회로(170)의 출력을 발생시키고, 실난수 발생 장치(100)의 동작 완료시에 지터 회로(170)의 출력을 차단시키는 특징을 갖는다.

<76> 도 4는 본 발명의 바람직한 일 실시예에 따라 실난수 발생 장치의 발진 회로를 도시한 블록도이다.

<77> 도 4에 도시된 바와 같이, 상기 도 1 내지 도 2에서의 제 1, 제 2 및 제 3 발진 회로(120, 130, 180)는 링발진기(121)와 NAND 게이트(122)로 구성될 수 있으며, 'Enable' 신호를 입력으로, 'RO' 신호를 출력으로 한다.

<78> 여기서, 링발진기(121)는 입력을 반전시켜 출력하는 기능을 수행한다.

<79> 링발진기(121)의 입력은 NAND 게이트(122)의 출력 신호를 입력으로 하며, 링발진기(121)의 출력은 상기 NAND 게이트(122)의 입력 중 하나에 공급한다.

<80> 이와 같은 링발진기(121)는 입력을 반전시킬 수 있는 기능을 가진 짝수 개의 논리 게이트, 일예로 인버터, NAND 게이트, NOR 게이트 등으로 구성될 수 있으나, 칩 내에 차지하는 면적, 전력 소비 등이 적은 인버터를 주로 구성한다.

<81> 한편, NAND 게이트(122)는 링발진기(121)의 출력과 외부 'Enable' 신호를 입력으로 하여 해당 발진회로의 출력(RO)을 생성한다.

<82> 그리고, NAND 게이트는 상기 'Enable' 신호에 따라서 링발진기(121)의 동작을 제어하는 기능을 수행한다. 일예로, NAND 게이트는 'Enable = 1' 인 경우에 다른 입력 신호를 반전시키며, 'Enable = 0' 인 경우에 항상 출력이 '1'로 유지되도록 하여 링발진기(121)의 동작을 제어할 수 있다.

<83> 이와 같은 NAND 게이트는 'Enable' 신호의 값이 '1' 또는 '0' 일때 각각 신호 반전 또는 이전 출력 값 유지, 이와 반대로 이전 값 유지 또는 신호 반전의 결과를 출력하는 임의의 논리 게이트로 대체 가능할 수 있다.

<84> 도 5는 본 발명의 바람직한 일 실시예에 따라 실난수 발생 장치의 POR 회로의 회로 구성도이다.

<85> 도 5에 도시된 바와 같이, 상기 도 1 내지 도 2에서의 POR 회로(130)는 직렬로 연결된 저항(R)과 콘덴서(C)로 구성되어, 전원 투입 후 상기 저항(R)과 콘덴서(C)의 값에 의해 정해지는 시간(t)이 되면, 저항(R)과 콘덴서(C) 사이의 출력 POR이 저(Low) 수준에서 고(High) 수준으로 전환되도록 하는 기능을 수행한다.

<86> 여기서, 저항(R)과 콘덴서(C)의 값에 의해 정해지는 시간(t)은, 다른 실시예로 다른 회로를 이용하여 변경이 가능하다. 그 일예로서 수 비트의 카운터를 사용하여 특정한 값이 카운팅되는 시점까지를 't' 시간으로 정할 수 있으며, 임의의 지연 시간을 갖고 저수준에서 고수준 또는 이와 반대의 동작을 수행하는 논리 모듈을 직렬 연결된 저항(R)과 콘덴서(C) 구성으로 대체 가능하다.

<87> 도 6은 본 발명의 바람직한 일 실시예에 따른 실난수 발생 장치의 신호별 타이밍도이다.

<88> 도 6을 참조하면, 도 1, 도 2 내지 도 5에서 전원(전원 전압 Vdd) 투입 후 실난수 발생 장치(100)로부터 발생되는 신호는, POR 회로(130)의 출력 POR, 지터 회로(170)의 출력 JO, 제 1 및 제 2 발진 회로(110, 120)의 출력 RO1, RO2 그리고 최종 출력 RN 신호를 포함한다.

<89> 도 6에서 시간 't'는 POR 회로(130)에 의하여 정해지는 시간이다.

<90> 그리고, 시간 't' 이후의 시간에서 제 1 발진 회로(120) 출력 'RO1'는 자체 회로 구성에 의하여 값이 정해지고, 지터 회로(170) 출력 'JO' 또한 제 3 발진 회로(180)의 출력에 따라서 그 값이 결정되기 때문에 타이밍도로 나타낼 수 없다.

<91> 하지만, 제 2 발진 회로(120)의 출력인 'RO2'는 도 6의 클럭으로 발생되어 제 1 D-플립플롭(140)으로 제공되며, 제 2 D-플립플롭(150)의 출력인 'RN'은 상기 'RO2'의 하강 천이 구간에서 발생되는 난수 값으로 발생된다.

<92> 한편, 이와 같은 구성 및 구성 동작을 갖는 실난수 발생 장치(100)는 반복 구현되어 사용자가 원하는 크기의 실난수를 발생시킬 수 있다.

<93> 도 7은 본 발명의 바람직한 일 실시예에 따른 반복 구조형의 병렬형 실난수 발생 장치를 도시한 블록도이다.

<94> 도 7을 참조하면, 병렬형 실난수 발생 장치(100)는 전술된 도 1 내지 도 2의 실난수 발생 장치(100)를 반복적으로 이용하여 구현함으로써 사용자가 원하는 크기의 실난수를 생성할 수 있다.

<95> 즉, 병렬형 실난수 발생 장치(100)는 일예로, 8개의 병렬 실난수 발생 장치(100)를 이용하여 도 7과 같이 8비트의 난수 RN0~RN7 값을 생성할 수 있다.

<96> 그리고, 전술된 도 1 내지 도 2의 실난수 발생 장치(100)는 임의의 구성 요서들만이 리소스 공유되어 사용자가 원하는 크기의 실난수가 발생되도록 할 수 있다.

<97> 도 8은 본 발명의 바람직한 일 실시예에 따른 리소스 공유형 실난수 발생 장치를 개념적으로 설명하기 위한 블록도이다.

<98> 도 8을 참조하면, 리소스 공유형의 실난수 발생 장치(200)는 각각 하나의 제 1 및 제 2 발진 회로(110, 120), POR 회로(130) 및 인버터(160)를 공유하여 사용하며, 상기 도 1 내지 도 7에서 나머지 회로의 구성 요소가 다수 블록(210)으로 구현되도록 함으로써 사용자가 원하는 크기의 실난수를 생성할 수 있다.

<99> 즉, 리소스 공유형 실난수 발생 장치(100)는 도 8과 같이, 제 1 및 제 2 발진 회로(110, 120), POR 회로(130) 및 인버터(160)를 제외한 나머지 구성 요소들이 출력 신호 RN0 ~ RN7 별로 각각 서로 다른 블록으로 구현되도록 하여, 원하는 크기의 실난수를 생성한다.

<100> 도 9는 본 발명의 바람직한 다른 실시예에 따른 리소스 공유형 실난수 발생 장치를 개념적으로 설명하기 위한 블록도이다.

<101> 도 9를 참조하면, 리소스 공유형의 실난수 발생 장치(200)는 각각 하나의 지터 회로(170), POR 회로(130), 제 2 및 제 3 발진 회로(110, 120) 및 인버터(160)를 공유하여 사용하며, 상기 도 2 내지 도 7에서 나머지 회로의 구성 요소가 다수 블록(220)으로 구현되도록 함으로써 사용자가 원하는 크기의 실난수를 생성할 수 있다.

<102> 이상에서 설명한 본 발명은 전술한 실시 예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경할 수 있다는 것은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 당업자에게 있어 명백할 것이다.

발명의 효과

<103> 상기한 바와 같은 본 발명에 따른 오실레이터 샘플링 방법을 이용한 실난수 발생 장치는, 디지털 설계되고 발진기 제어 기능을 이용함으로, 그 구현이 용이하며, 고속, 저소비전력 및 저가격의 실난수를 발생할 수 있는 효과를 가진다.

<104> 그리고, 상기한 바와 같은 본 발명에 따른 오실레이터 샘플링 방법을 이용한 실난수 발생 장치는, 반복 구조의 병렬형 또는 리소스 공유형으로 응용됨으로, 사용자가 원하는 크기의 실난수를 생성할 수 있는 효과를 가진다.

도면의 간단한 설명

<1> 도 1은 본 발명의 바람직한 일실시예에 따른 실난수 발생 장치의 구성을 나타낸 블록도,

<2> 도 2는 본 발명의 바람직한 다른 실시예에 따른 실난수 발생 장치의 구성을 나타낸 블록도,

<3> 도 3은 본 발명의 바람직한 일 실시예에 따라 실난수 발생 장치의 지터 회로를 도시한 블록도,

<4> 도 4는 본 발명의 바람직한 일 실시예에 따라 실난수 발생 장치의 발진 회로를 도시한 블록도,

<5> 도 5는 본 발명의 바람직한 일 실시예에 따라 실난수 발생 장치의 POR 회로의 회로 구성도,

<6> 도 6은 본 발명의 바람직한 일 실시예에 따른 실난수 발생 장치의 신호별 타이밍도,

<7> 도 7은 본 발명의 바람직한 일 실시예에 따른 반복 구조형의 병렬형 실난수 발생 장치를 도시한 블록도,

<8> 도 8은 본 발명의 바람직한 일 실시예에 따른 리소스 공유형 실난수 발생 장치를 개념적으로 설명하기 위한 블록도, 그리고

<9> 도 9는 본 발명의 바람직한 다른 실시예에 따른 리소스 공유형 실난수 발생 장치를 개념적으로 설명하기 위한

블록도이다.

<10> *도면의 주요 부분에 대한 부호의 설명*

<11> 100 : 실난수 발생 장치 110 : 제 1 발진 회로

<12> 120 : 제 2 발진 회로 130 : POR(Power-On-Reset) 회로

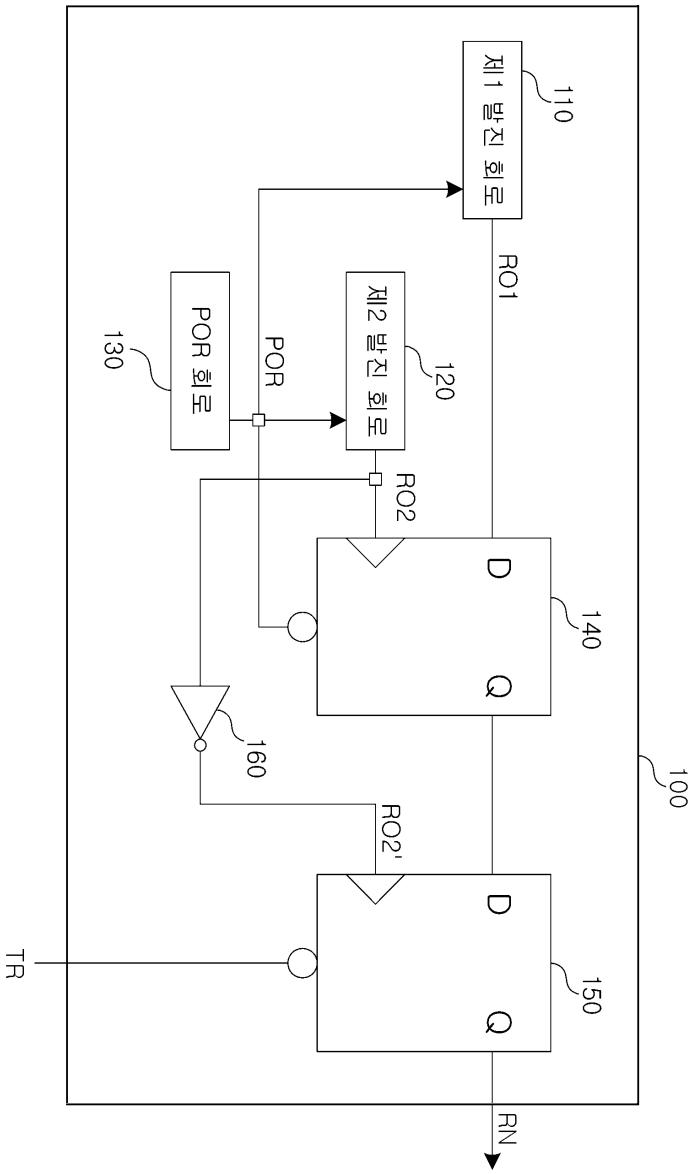
<13> 140 : 제 1 D-플립플롭 150 : 제 2 D-플립플롭

<14> 160 : 인버터 170 : 지터 회로

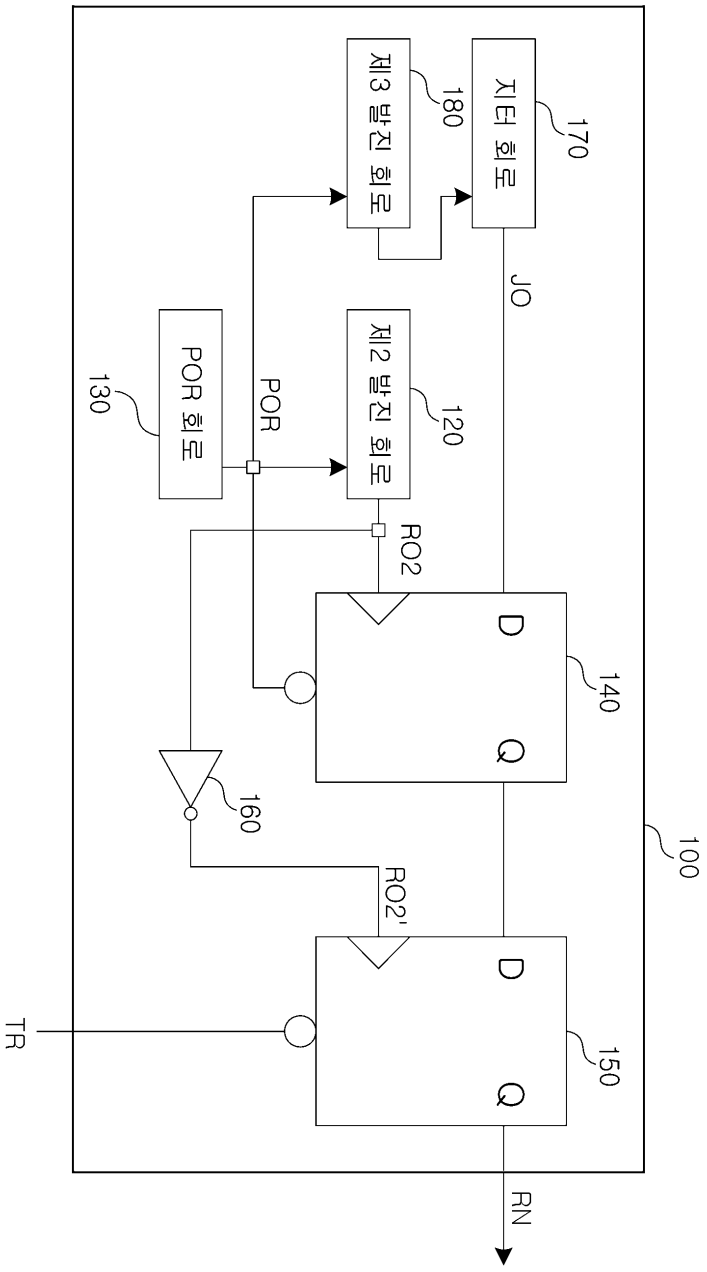
<15> 180 : 제 3 발진 회로

도면

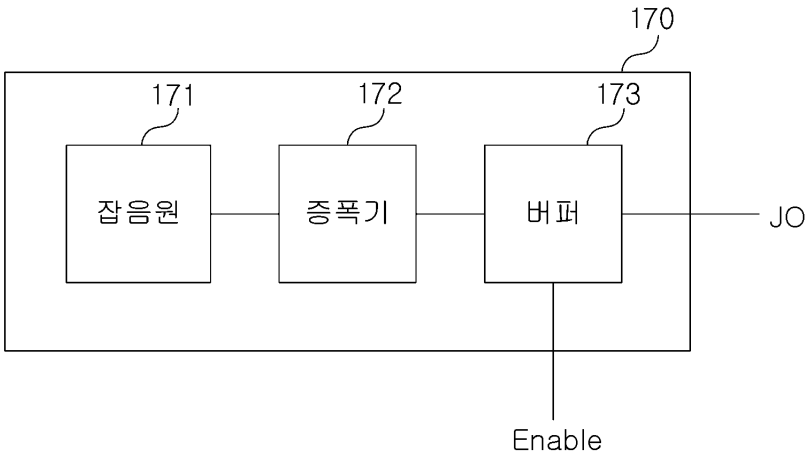
도면1



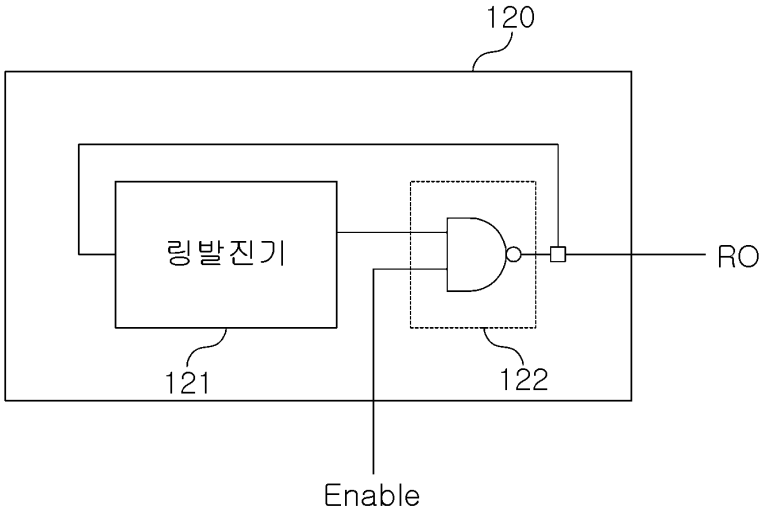
도면2


지터 회로
170
제3 발진 회로
180
JO
POR 회로
130
POR
제2 발진 회로
120
RO2
D
Q
140
160
RO2'
D
Q
150
100
TR
RN

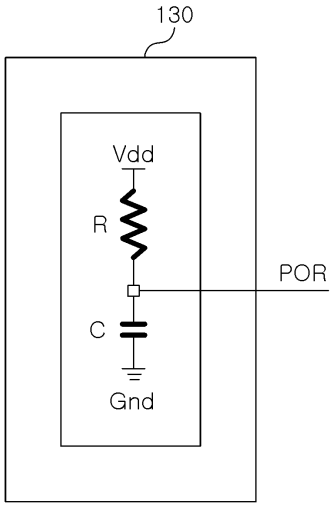
도면3



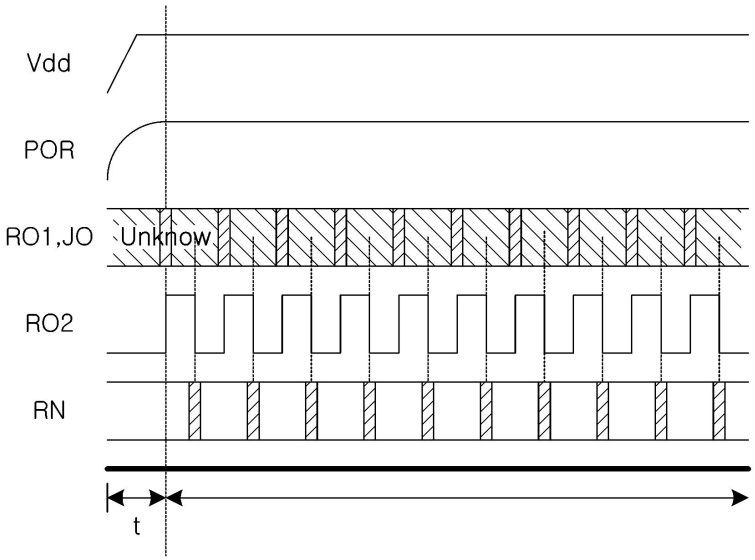
도면4



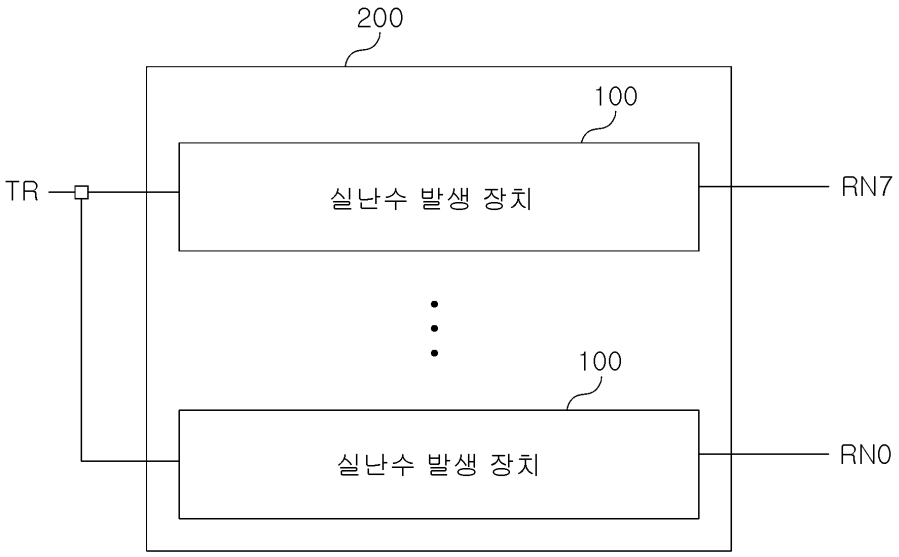
도면5



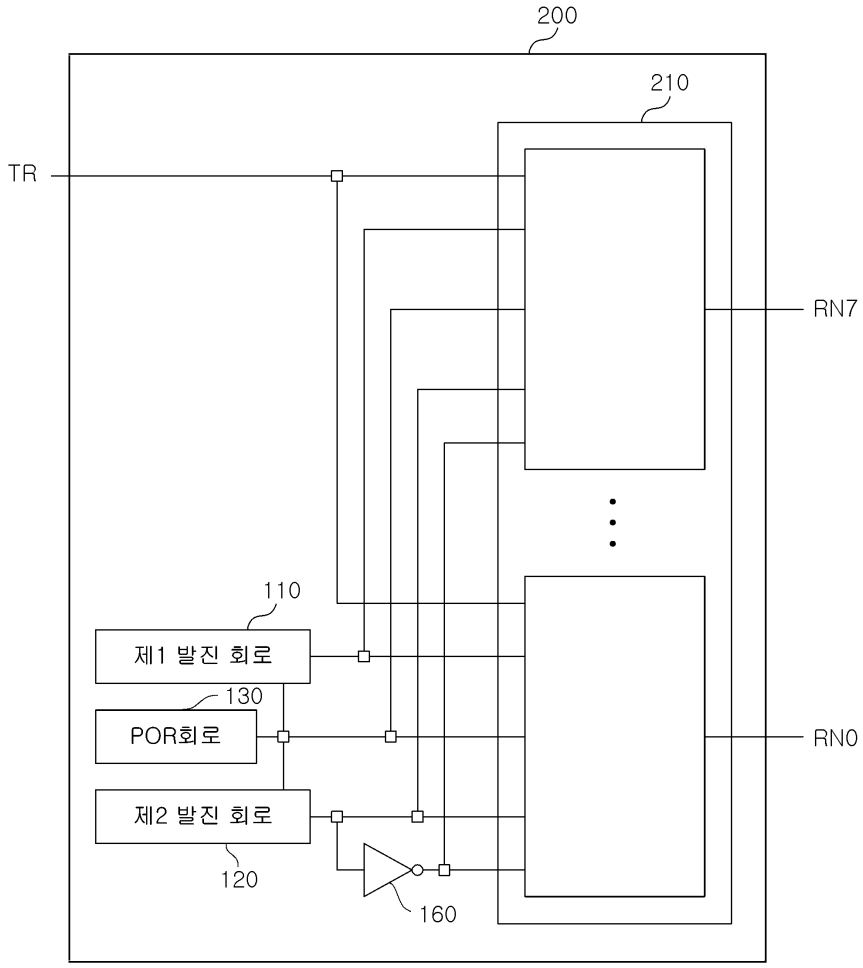
도면6



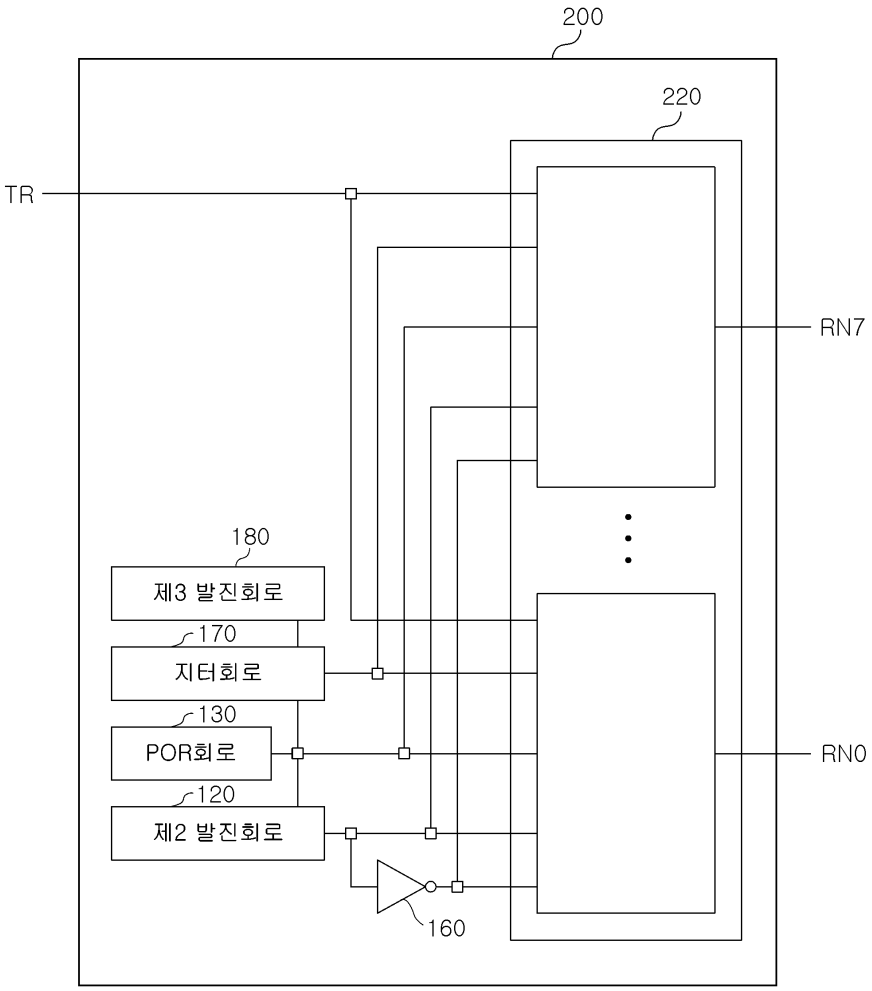
도면7


200
100
TR
실난수 발생 장치
RN7
100
실난수 발생 장치
RN0

도면8


200
210
TR
RN7
110
제1 발진 회로
130
POR회로
RN0
제2 발진 회로
120
160

도면9


200
220
TR
RN7
180
제3 발진회로
170
지터회로
130
POR회로
120
제2 발진회로
160
RN0